レイヤ構造を利用したJPEG2000符号化画像の暗号化法

安藤　勝俊[†]　　貴家　仁志[††a)]

An Encryption Method for JPEG2000 Images Using Layer Function

Katsutoshi ANDO[†] and Hitoshi KIYA[††a)]

あらまし　本論文では，JPEG2000 または Motion JPEG2000 により符号化された画像の暗号化方式を提案する．提案法は，JPEG2000 の機能の一つであるレイヤ構造を利用して，JPEG2000 符号列の一部を選択的に暗号化するものである．この暗号化処理では，暗号化に要する演算を効果的に低減することが可能となる．また，JPEG2000 のデータ構造が保持されるため，暗号化された符号列は，スケーラビリティや誤り耐性機能等の JPEG2000 符号が本来もつ多様な機能を引き継ぐことができる．実際の画像を用いたシミュレーションにより，提案法の有効性を確認する．

キーワード　JPEG2000, 画像符号化，暗号化，レイヤ

1. まえがき

コンピュータの高性能化，ネットワークの広帯域化に伴い，ディジタル画像・映像コンテンツの流通が増加してきている．しかし，ディジタルデータは品質の劣化なくコピーできるため，その著作権保護が問題であり，ディジタルコンテンツ流通の発展において重要な課題となっている [1]．また，画像の用途によっては，その内容や所有者に関するプライバシー保護も問題となる．これらの問題を改善するための手法として，一般に次の 3 種類の方式が存在する．すなわち，(a) 電子透かし [2], [3]，(b) 情報半開示 [4]〜[6]，(c) 画像データの暗号化 [7], [8] である．

これらのうち，画像データの暗号化は，画像情報の保護のための方式として最も堅牢であり，高度な機密性の保持やプライバシー保護を行うことができる．また，必要な保護の程度に応じて，ほかの方式と組み合わせて利用することもできる．本論文では，この画像データの暗号化を取り扱い，JPEG2000 と Motion JPEG2000 に基づく，新しい画像データの暗号化手法を提案する．

[†] ソニー株式会社，東京都
Sony Corporation, Tokyo, 141–0001 Japan
[††] 東京都立大学大学院工学研究科，八王子市
Graduate School of Engineering, Tokyo Metropolitan University, 1–1 Minami-osawa, Hachioji-shi, 192–0397 Japan
a) E-mail: kiya@eei.metro-u.ac.jp

画像データの暗号化は，符号化されていない画像情報に直接適用する場合と，符号化画像に適用する場合の 2 種類が考えられる．本論文が対象とするのは後者である．ディジタル画像・映像コンテンツの流通において扱われる画像情報は，一般に符号化画像であるためである．更に，符号化画像の暗号化は，符号化された画像を単純なデータとみなして暗号化する方式と，画像符号化方式を考慮しつつ暗号化を適用する方式に大別できる．従来研究の多くは，前者に属し，暗号化方式と画像符号化方式の研究は独立に行われてきた．一方，本論文で提案する方式は，後者に属し，暗号化方式と画像符号化方式を同時に考慮する．これは，画像符号化方式のもつ様々な機能を暗号化後も保持し，かつ効率的な暗号化を行うために，この考慮が不可欠であると考えるからである．

提案法では，以下の三つの特徴が同時に考慮されている．(a) 汎用 JPEG2000 エンコーダ及びデコーダが使用可能で，その前後で暗号化・復号処理が実行できること．(b) 符号化画像としての形式を保持すること．(c) 処理に必要な演算量が小さいこと．

すなわち，(a) の特徴は，提案法のための専用エンコーダ及びデコーダの使用の回避を可能とするため，暗号化処理の普及や低コスト化に有利となる．(b) の特徴は，符号のもつ様々な機能（スケーラビリティ機能など）を維持する．(c) の特徴として，演算量が小さいことは，暗号化処理システムのコスト低減や高速

化に貢献し，特に動画像への適用において有用となる．

JPEG2000 では，レイヤという階層的符号構造をもつことができる．JPEG2000 符号列は，画質への貢献の大きい成分ほど上位のレイヤに含まれ，上位から下位まで順次画質を改善するよう構成される．提案法は，このレイヤ構造を利用し，JPEG2000 符号列の上位レイヤを選択的に暗号化する．このとき，JPEG2000 符号のデータ構造は保持され，下位レイヤの符号列はそのまま保存される．このような方式では，符号列の一部のみ選択的に暗号化するため，暗号化に要する演算量は小さい．一方で，暗号化後の符号列は，JPEG2000 符号が本来もつ様々な機能を引き継ぐことになる．また，JPEG2000 符号化方式では下位レイヤを復号するために上位レイヤの復号結果が必要となることから，提案法は，符号化画像を単純なデータとみなして暗号化した場合と同等に画像情報の保護を行うことができる．

以上，本論文の新規性について，次のように考えている．まず第 1 に，符号列のデータ構造を保持した形式で暗号化することが画像の流通において重要であることを指摘したことである．第 2 点は，この特徴をもちかつ処理負担の少ない暗号化方式を，JPEG2000 符号化画像に対して具体的に提案したことにある．

2. JPEG2000 符号化 [9]〜[11]

まず準備として，本論文が対象とする JPEG2000 Part1 符号化方式について簡単に説明する．更に，提案法が利用するレイヤ構造とその特徴について述べる．

2.1 符号化の概要

JPEG2000 Part1 の符号化処理の構成を図 1 に示す．まず，入力画像がウェーブレット変換によりサブバンド分解される．次にサブバンドのウェーブレット係数列は，必要に応じて量子化処理（オプション）され，EBCOT（Embedded Block Coding with Optimized Truncation）アルゴリズム [12] により符号化される．EBCOT アルゴリズムは，各サブバンドを一定サイズのコードブロックに分割する．そしてコードブロックはそれぞれ独立にビットプレーンに基づく係数ビットモデリングが実行され，更に算術符号化される．コードブロックごとに生成された算術符号は，それぞれの一部を廃棄することにより，全体として目的のビットレートに調整される．また，必要に応じてレイヤという単位にグループ分けされる．この後，更にヘッダ情報などを付加したものが，最終的な JPEG2000 符号列となる．

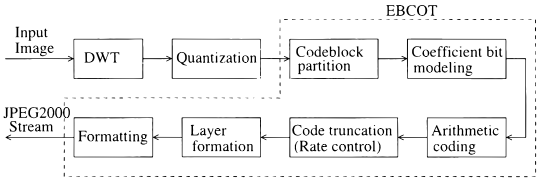
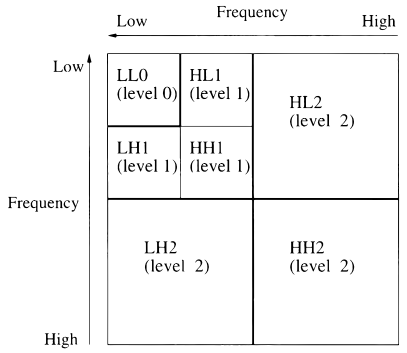
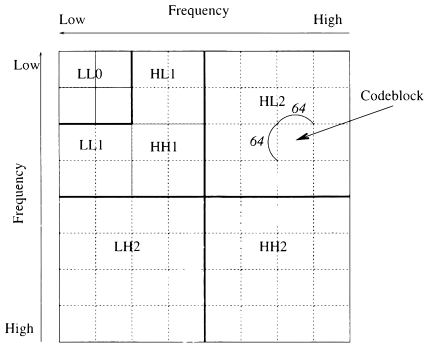


図 1 JPEG2000 エンコーダ
Fig. 1 JPEG2000 encoder.



(a) サブバンド分解



(b) コードブロック分割

図 2 ウェーブレット係数（サブバンド分解レベルが 2，コードブロックが 64 × 64 の場合）
Fig. 2 Sub-bands and code-blocks (where decomposition level was 2 and code-block size was 64 × 64).

サブバンド分解及びコードブロック分割の例を，それぞれ図 2 (a)，(b) に示す．すべてのレベルとすべての帯域を，一定のサイズで分割するように，コードブロックは構成される．JPEG2000 では，64 × 64 の分割サイズをデフォルトとしている．

このような JPEG2000 Part1 符号化方式は静止画を対象としたものであるが，各フレームに対してこの方式を適用した，動画像符号化のための Motion

JPEG2000（JPEG2000 Part3）[13], [14] が規格化されている．

2.2 レイヤ構造とその特徴

レイヤとは，複数の画質で順次再生できるように，算術符号を明示的にグループ分けしたものである．

図 3 にこのレイヤ構造が形成された JPEG2000 符号列の例を示す．符号列は，最上位から最下位までのいくつかのレイヤと，各レイヤの位置，長さを記録したヘッダ部からなる．そして，各レイヤは，各コードブロックの算術符号の一部と，その位置と長さを記録したヘッダ部から構成される．このとき，画質への寄与が高い情報ほど，上位のレイヤに含まれるようなる．すなわち，一般に各コードブロックにおいて上位ビットの情報ほど，上位レイヤに含まれるよう構成される．

このレイヤ構造により，デコーダでは，上位のレイヤから順番に復号し，複数の画質で順次再生することができる．

また，レイヤ構造が形成された JPEG2000 符号列は，階層的に様々なレートで復号処理を行うことができる．これは，符号列のうち下位レイヤを廃棄することにより実行され，もとの符号列より低いビットレートの符号列を得るものである．もし上位レイヤが廃棄されると，下位レイヤの情報が常に上位レイヤの情報に従属して生成されているため，それ以降の下位レイヤの正常な復号ができなくなることに注意する必要がある．

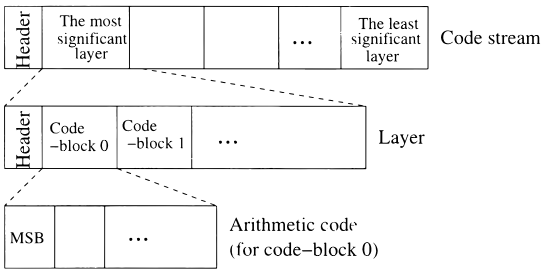


図 3　JPEG2000 符号列
Fig. 3　Structure of a JPEG2000 bit stream.

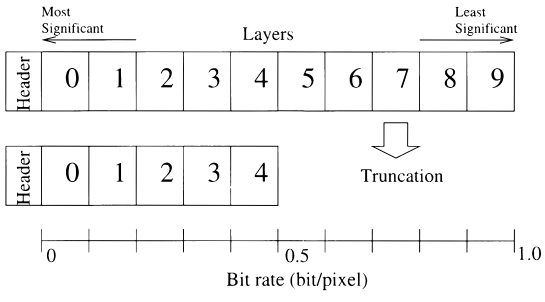


図 4　レイヤを用いたレート制御例
Fig. 4　An example of rate control using layer function.

図 4 に，0.1（bits/pixel）ごと 10 層のレイヤをもつ 1.0（bits/pixel）の符号列から，0.5（bits/pixel）の符号列を生成する例を示す．この例では，10 層あるレイヤのうち，下位レイヤ 5 層を廃棄し，上位レイヤ 5 層を保存することにより，半分のビットレートの符号列を生成している．これにより生成された 0.5（bits/pixel）の符号列は，JPEG2000 エンコーダにより最初から 0.5（bits/pixel）をターゲットレートとして符号化された場合の符号列とほぼ同一（ヘッダ部を除く）となる．

3. 提　案　法

ここでは，まず，提案法の概要について述べる．更に，JPEG2000 符号化画像の暗号化及び復号方式を具体的に説明する．

3.1 提案法の概要

提案法では，図 3 に示されるようなレイヤによりグループ分けされた JPEG2000 符号列から，最上位レイヤを選択し，その算術符号を暗号化する．一方，暗号化する最上位レイヤに続く下位レイヤの算術符号は暗号化しない．しかし，算術符号の性質上，上位区間を暗号化すると，その区間を復号しない限り，それ以降の非暗号化区間も復号できなくなる．提案法では，この最上位レイヤの暗号化によってすべての算術符号の復号が不可能となる性質に注目し，それを利用している．

このような最上位レイヤの暗号化には，最上位のみを暗号化する場合と，最上位を含むいくつかのレイヤを暗号化する場合の 2 通りが考えられる．以降では議論を簡単にするために，最上位レイヤのみを暗号化する場合について説明する．

図 5 は，JPEG2000 符号化での暗号化処理と復号処理の流れを説明したものである．同図に示すように，提案法における暗号化処理と復号処理は，JPEG2000 のエンコーダ，デコーダと独立に行われる．

まず，入力画像は JPEG2000 エンコーダにより符号化され，JPEG2000 符号列が生成される．そして，提案法により暗号化処理を施される．暗号化処理を施された符号列は，復号鍵を用い復号処理を行った後に，

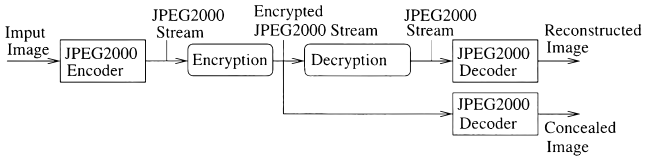


図 5　JPEG2000 符号と暗号化処理
Fig. 5　Encryption of a JPEG2000 bit-stream.

JPEG2000 デコーダによって正常に復元された画像を再生する．

このとき，JPEG2000 符号のデータ構造及び長さに影響を与えないような暗号化処理を行えば，暗号化にあたって，復号鍵以外のデータ量は増加しない．また，暗号化された符号列は，JPEG2000 符号のデータ構造を保持することができ，そのまま JPEG2000 デコーダでデコードすることができる．このとき，非開示画像が出力として得られる．更に JPEG2000 符号のデータ構造の保持は，JPEG2000 のもつ多様な機能を引き継ぐことを可能にする．

以下では，これらのことを詳細に説明する．

3.2　暗号化処理

図 6 は，0 から L までのレイヤ構造をもつ JPEG2000 符号列を例示している．各レイヤの位置と長さの情報がヘッダ部に記録されている．このような，JPEG2000 符号列に対して，まず，最上位であるレイヤ 0（図 6 の網線部）の算術符号の位置と長さの情報を，ヘッダ部から読み取る．

次に，得られた位置と長さの情報を用い最上位レイヤの算術符号の暗号化を行う．このとき，下位レイヤ 1 から L はそのまま状態に保存される．

このとき，算術符号の暗号化に，入力データのサイズと出力される暗号データのサイズが同一となる暗号アルゴリズムを用いれば，暗号化の前後で算術符号のデータ量が変化しない．JPEG2000 符号列のヘッダ部に各コードブロック，レイヤの算術符号の長さが記録されていることから，符号列の長さが変わらなければ，復号の同期が保証される．したがって，暗号化された符号列は，JPEG2000 デコーダに入力し非開示画像として再生することが可能となる．

一方，暗号化された符号列を非開示画像として再生する必要がないとき，用いる暗号アルゴリズムにこのような制約は必要ない．以下では，簡単のため，入力データのサイズと出力される暗号データのサイズが同一の暗号アルゴリズムを用いた場合について議論を展開する．

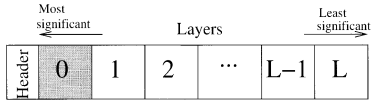


図 6　最上位レイヤ（網掛け部分）の暗号化
Fig. 6　Encryption of the most significant layer (shaded parts).

3.3　復 号 処 理

暗号化の解除は，図 5 のように，暗号化された算術符号を復号することにより行う．まず，JPEG2000 符号化列のヘッダ部から最上位レイヤの算術符号の位置と長さの情報を抽出する．次に，復号鍵を用い暗号化されている算術符号を復号する．これにより，JPEG2000 符号列は暗号化処理を行う前の状態に完全に復元する．

また，先に述べたように復号を行わなくても，デコードすることは可能であり，その場合は非開示画像が生成される．

以上では，最上位レイヤのみを暗号化する場合について議論したが，最上位を含むいくつかのレイヤを暗号化する場合も，同様の暗号化処理及び復号処理が実行可能である．ただし，最上位以外のどのレイヤを暗号化したかを示すパラメータを，暗号化処理において生成し，復号時に利用する必要がある．

3.4　マーカコードの取り扱い

提案法により暗号化処理を行う際には，偽のマーカコードが生成される可能性があることに注意する必要がある．マーカコードは，JPEG2000 おいて特別な意味を保つ符号であり（例えば符号の終端を意味する 0xFFD9），暗号化により偽のマーカコードが生成されると，非開示画像の正常な再生が妨げられることがある．

提案法は，JPEG2000 符号列のうち一部を選択的に暗号化するため，このような偽のマーカコードの出現する確率は極めて低い．しかし，暗号化の後，偽の

マーカコードが発生しないことを確認する必要がある．そして，もしマーカコードの発生がある場合，それを回避する必要がある．回避の方法は，次のようなものが考えられる．

(a) 符号列のレイヤ構造を変更し，マーカコードの発生しないよう最上位レイヤの区間を設定する

(b) 最上位レイヤの中で，暗号化を行う区間を選択する

(c) 暗号鍵を変更する

ただし，(b) の方法では，暗号化処理を行う際に，暗号化区間の選択情報をパラメータとして保存し，復号処理において利用する必要がある．

4. 提案法の特徴

ここでは，提案法のもつ特徴を要約する．

4.1 汎用のエンコーダ，デコーダが利用可能

図 5 に示したように，提案法の暗号化及び復号処理は，JPEG2000 のエンコーダとデコーダの処理の前後で実行される．これは，JPEG2000 のヘッダ情報から最上位レイヤの位置と長さの情報が抽出でき，その情報に基づいて算術符号の暗号化を施すからである．その結果，提案法では暗号化処理を前提としない汎用エンコーダ，デコーダを利用することができる．この特徴は，提案法の普及において重要であると考えている．

4.2 レート制御に影響を与えない

3.2 で述べたように，入力と出力のデータ量が同じとなる暗号アルゴリズムを用いる限り，この暗号化処理によって JPEG2000 符号のデータ構造，長さが変化することはない．またデコード後の再生画像の画質も変化しない．この特徴は，メディアの伝送速度や容量に厳しい制約がある応用において有用であると考えられる．

4.3 JPEG2000 符号のデータ構造の保持

提案法の暗号化処理は，JPEG2000 符号のデータ構造や長さに影響を与えない．したがって，暗号化された JPEG2000 符号列は復号の同期が保持され，そのまま JPEG2000 デコーダで破綻なく再生することができる．このとき，再生画像として非開示画像を得る．この特徴は，**4.5** で説明するスケーラビリティ機能においても重要となる．

4.4 演算処理量の低減

図 5 に示すように，提案法は，JPEG2000 符号列の算術符号の一部のみを暗号化する．したがって，符号列全部を暗号化の対象とする場合に比べて，暗号化及びその復号に必要な演算処理量が小さい．JPEG2000 のエンコード時に，最上位レイヤに含まれる算術符号を少なくするよう設定すれば，暗号化される算術符号の量を非常に小さくすることも可能である．

このような特徴は，暗号化システムの低コスト化や高速化に貢献すると考えられる．

4.5 スケーラビリティ・誤り耐性機能の維持

前述のように，提案法は JPEG2000 符号のデータ構造を保持する．この特性により，JPEG2000 のもつスケーラビリティ機能が維持される．その結果，暗号化された符号列から直接，下位レイヤを廃棄することによって，より低いビットレートの符号列を生成することが可能である．これは，提案法の暗号化が，下位レイヤ廃棄の影響を受けないためである．

図 7 に，等分割な 10 層のレイヤ構造をもつ JPEG2000 符号列を提案法により暗号化し（図中レイヤ 0 を暗号化），より低いビットレートの暗号化された JPEG2000 符号列を生成する例を示す．図 7 (a) は，0.1（bits/pixel）ごと 10 層のレイヤをもち，その最上位レイヤが暗号化された符号列を示している．この符号列から，下位レイヤを廃棄することにより，より低いビットレートの符号列の図 7 (b)，(c) を生成している．このような処理は，符号中の暗号化部分（図の網掛け部分）と無関係に行われる．図 7 (a)，(b)，(c) の符号列は，それぞれビットレートは異なるものの，同じ復号鍵を使用し，最上位レイヤの暗号化を解除することができる．

このような特徴によって，暗号化された符号化画像を一つの用意するだけで，再エンコード，再暗号化を行うことなく，要求画質の違う複数の受け手に，様々なビットレートの符号化画像を配信することができる．また，プログレッシブ伝送に対応することができ，受信者は符号全体の到着を待つことなく，最上位レイヤを受け取った時点で復号を行って，画像を再生することができる．詳細は割愛するが，スケーラビリティ機能と同様に，更に JPEG2000 のもつ誤り耐性機能の保持に対しても提案する暗号化法は有用となる．

4.6 Motion JPEG2000 での応用

4.4 で述べたように，提案法により暗号化された JPEG2000 符号列は，そのまま JPEG2000 デコーダで非開示画像として再生できる．この特徴により，Motion JPEG2000 符号化画像の一部のフレームを選択的に暗号化することが可能である．これは，動画像中に，暗号化されたフレームが存在しても非開示画像と

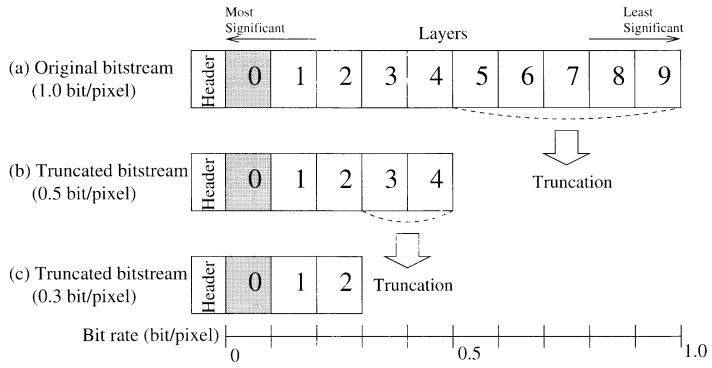


図 7　暗号化された符号列のスケーラビリティ（図の網掛け部分を暗号化）
Fig. 7　Scalability of an encrypted bit-stream. (Shaded parts are encrypted.)

して再生でき，動画像全体のデコードが破綻せずに行えるためである．これにより，後述のシミュレーションで示すような，例えばフレームを飛び飛びに暗号化する処理も可能となる．このような処理は，リアルタイム性の制約が強くかつデータ量の膨大な動画像の暗号化において，演算量削減の観点からも有効であると考えている．

5. シミュレーション

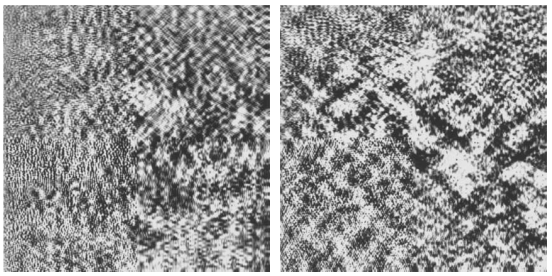
提案法の効果を確認するため，実際の画像に提案法を適用した結果を示す．シミュレーションには，図 8 に示す Lena の画像（512 × 512 画素，8 ビットグレースケール）を用いた．JPEG2000 符号化アルゴリズムとしては，JPEG2000 Verification Model 7.0 [15] を用い，Daubechies 9-7 フィルタによる 5 レベル分解，圧縮率 1（bits/pixel）の符号化を行った．暗号化には，Blowfish アルゴリズム [16] を使用した．暗号化は，**3.4** で述べたように偽マーカコードの発生を確認しつつ実行したが，実際に偽マーカコードが発生することはなかった．

（1） 暗号化された符号列の非開示画像としての再生

提案法の暗号化処理を施された JPEG2000 符号列を，そのままデコーダで再生した例を図 9 (a) に示す．これは，図 7 (a) のように 0.1（bits/pixel）ごと 10 層のレイヤをもち，そのうち最上位のレイヤ 0 を暗号化したものである．これに対して，図 9 (b) は，10 層のレイヤすべてを暗号化した場合である．

提案法では，復号鍵による復号なしでも，符号列を非開示画像として再生することができることがわかる．

図 8　原　画　像
Fig. 8　The original image.



(a) レイヤ 0 のみ　　(b) 全レイヤ

図 9　非開示画像
Fig. 9　Concealed images.

また，暗号化処理が符号列の一部のみを暗号化するにもかかわらず，全部を暗号化した場合と同様の，非開示画像が再生されることが確認される．

（2） スケーラビリティ機能の利用

図 9 (a) の場合と同様な暗号化を行い，それを復号した上でデコーダで再生した画像を図 10 に示す．この画像は，同じ条件による JPEG2000 符号化を行い，

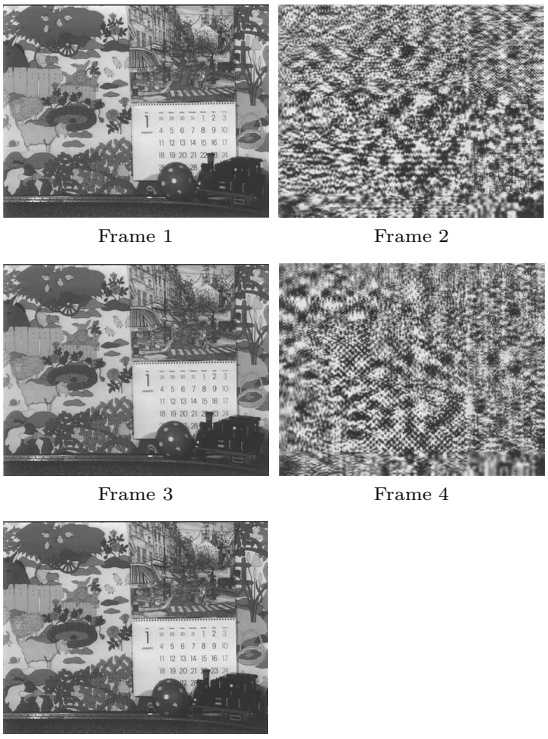
1.0 (bits/pixel), PSNR: 40.38 (dB)

図 10　復元画像
Fig. 10　A reconstructed image.

(a) 0.5 (bits/pixel)
PSNR: 37.30 (dB)

(b) 0.3 (bits/pixel)
34.87 (dB)

図 11　低ビットレートの復元画像
Fig. 11　Reconstructed images have lower bit-rate.



Frame 1　Frame 2
Frame 3　Frame 4
Frame 5

図 12　1 フレームおき飛び飛びに暗号化された動画像の例
Fig. 12　An example of image sequence encrypted every other frame.

暗号化を行わなかったときに得られる画像と同一である．

一方で，提案法の暗号化処理を施された JPEG2000 符号列に対し，下位レイヤ廃棄によるレート制御を適用した例を図 11 に示す．これは，図 9 (a) の場合と同様に暗号化された符号列（図 7 (a) 参照）から，図 7 (b), (c) に示されるようなレート制御を施された上で，復号された画像である．図 11 (a)，(b) はそれぞれ，0.5（bits/pixel），0.3（bits/pixel）となっている．このとき，図 11 (a)，(b) は，最初から 0.5（bits/pixel），0.3（bits/pixel）をターゲットレートとして JPEG2000 エンコーダで生成され，暗号化を行わなかったときの画像と同一である．

（3） 動画像への応用

図 12 は，フレームが 1 枚ごと交互に提案法により暗号化された Motion JPEG2000 動画像の例である．暗号化されたフレームが非開示画像として再生されることがわかる．このようなことが可能であるのは，提案法の暗号化処理が施された JPEG2000 符号列が，そのまま JPEG2000 デコーダで非開示画像として再生可能であるためである．すなわち Motion JPEG2000 動画像の連続するフレーム中に，暗号化された符号列が存在したとしても，デコーダでは動画像として破綻なく再生することできるのである．

このようなフレームごとの暗号化を，実際の動画像に適用した例を添付データに示す．ただし，添付可能なデータ形式の制約により，添付データは，いずれも MPEG 形式に変換したものとなっている．

添付データ 1 mobile.mpg は原画像であり，40 フレームで構成される．これに対して，添付データ 2 alt.mpg は，1 枚ごと交互に，原画像 40 フレームのうち 20 フレームを暗号化したものである．また，添付データ 3 partial.mpg は，原画像 40 フレームの 11 フレーム目から 20 フレーム目を連続して暗号化したものである．これらの結果から，提案法は MotionJPEG 2000 動画像符号化において，時間方向の情報半開示を実現できることが確認される．

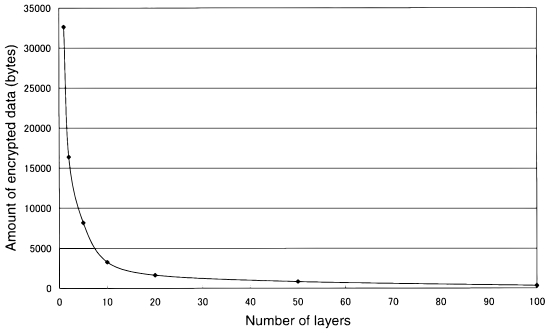


図 13 レイヤ数と暗号化データ量（等分割のレイヤをもつ 1.0 bits/pixel の画像 Lena の場合）

Fig. 13 Number of layers versus amount of encrypted data (where encryption was applied to 1.0 bits/pixel "Lena" which has equally divided layers).

（4） 演算量の低減

提案法では，最上位レイヤのみを暗号化するので，最上位レイヤに含まれる算術符号を制御することにより，暗号化に要する演算量を制御することができる．

図 13 は，1.0（bits/pixel）の符号化で，レイヤを 1〜100 層まで変えた場合の，最上位レイヤのデータサイズである．例えば，0.01（bits/pixel）ごとに 100 層のレイヤを形成した場合，レイヤが 1 層の場合の 1/100 となる．すなわち，暗号化されるデータ量は，符号化前の画像の約 1/800 であり，1.0（bits/pixel）で符号化された画像の約 1/100 となる．

このことは，最上位レイヤのみを暗号化するという提案法が，約 1/800 あるいは 1/100 の処理負担で暗号化を実現できることを示している．

6. むすび

本論文では，レイヤ構造を利用することにより，JPEG 2000 符号化画像を効果的に暗号化する手法を提案した．提案法は，暗号化と画像符号化を同時に考慮した暗号化方式であり，ディジタル画像の流通に有用な様々な特徴をもつ．また，シミュレーションにより，提案法の効果を確認した．

謝辞 本研究を進めるにあたり有益な助言を頂いたソニー株式会社 S&S アーキテクチャセンター・デジタルシステム開発室福原隆浩氏，木村青司氏に感謝する．また，本研究の一部は，日本学術振興会科学研究費補助金（萌芽的研究，課題番号 11875088）の援助によるものである．

文　献

[1] 松岡達雄，“ブロードバンド時代の映像コンテンツ流通，”映像情報メディア学会年次大会講演予稿集，pp.423–426, Aug. 2001.

[2] G.C. Langelaar, I. Setyawan, and R.L. Lagendijk, “Watermarking digital image and video data,” IEEE Signal Processing Magazine, vol.17, no.5, pp.20–46, Sept. 2000.

[3] 松井甲子雄，電子透かしの基礎—マルチメディアのニュープロテクト技術，森北出版，1998.

[4] 藤井　寛，阿部剛仁，西原祐一，串間和彦，“情報半開示方式，” NTT R&D, vol.47, no.6, pp.705–710, June 1998.

[5] 藤井　寛，山中康史，“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，” 情処学論，vol.38, no.10, pp.1945–1955, Oct. 1997.

[6] 安藤勝俊，渡邊　修，貴家仁志，“JPEG2000 符号化画像の情報半開示方式，” 信学論（D-II），vol.J85-D-II, no.2, pp.282–290, Feb. 2002.

[7] 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-I, no.5, pp.314–321, May 1992.

[8] 安藤勝俊，渡邊　修，貴家仁志，“伝送路誤りを考慮した JPEG2000 画像の暗号化法，” 信学技報，IE2000-152, Jan. 2001.

[9] ISO/IEC 15444-1, JPEG2000 Part1 final draft international standard, Aug. 2000.

[10] B.E. Usevirch, “A tutorial on modern Lossy wavelet image compression: Foundation of JPEG2000,” IEEE Signal Processing Magazine, vol.18, no.5, pp.22–35, Sept. 2001.

[11] A. Skodras, C. Christopoulos, and T. Ebrahimi, “The JPEG2000 still image compression standard,” IEEE Signal Processing Magazine, vol.18, no.5, pp.36–58, Sept. 2001.

[12] D. Taubman, “High performance scalable image compression with EBCOT,” IEEE Trans. Image Processing, vol.9, no.7, pp.1158–1170, July 2000.

[13] ISO/IEC 15444-3, Motion JPEG2000 Committe Draft 1.0, Dec. 2000.

[14] T. Fukuhara, K. Katoh, S. Kimura, K. Hosaka, and A. Leung, “Motion-JPEG 2000 standardization and target market,” Proc. IEEE ICIP2000, Sept. 2000.

[15] ISO/IEC JTC 1/SC 29/WG 1 WG1N1684, JPEG 2000 Verification Model 7.0, April 2000.

[16] B. Schneier, “Description of a new variable-length key, 64-bit block cipher (blowfish),” Fast Software Encryption, Cambridge Security Workshop Proceedings (Dec. 1993), pp.191–204, Springer-Verlag, 1994.

付　　録

添付ディジタルデーター覧

添付データ 1

ファイル名	**mobile.mpg**
保存場所	~/DATA/
データ種類	動画像
データ形式	MPEG1
説明	原画像（40 フレーム）

添付データ 2

ファイル名	**alt.mpg**
保存場所	~/DATA/
データ種類	動画像
データ形式	MPEG1
説明	1 枚ごと交互に暗号化した例

添付データ 3

ファイル名	**partial.mpg**
保存場所	~/DATA/
データ種類	動画像
データ形式	MPEG1
説明	途中のフレームを連続して暗号化した例

（平成 14 年 1 月 23 日受付，4 月 1 日再受付，
6 月 3 日最終原稿受付）

安藤　勝俊　（正員）

平 12 東京都立大・工・電子情報卒．平 14 同大大学院修士課程了．同年，ソニー（株）入社．在学中，マルチレート信号処理，画像処理の研究に従事．

貴家　仁志　（正員）

1980 長岡技科大・工・電気電子システム卒．1982 同大大学院修士課程了．同年東京都立大工学部電気工学科助手．2000 同大学大学院電気工学専攻教授．工博．1995〜1996 シドニー大（オーストラリア）客員研究員．マルチレート信号処理，画像符号化及びメディアセキュア技術に関する研究に従事．IEEE 論文誌 Signal Processing 編集委員（1998〜2000）．本会和文論文誌 A 編集委員（1998〜）．著書「高速フーリエ変換とその応用」,「ディジタル信号処理」,「マルチレート信号処理」．電子画像学会，映像情報メディア学会，IEEE シニア各会員．