社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－SLDM－136（15）
2008 / 10 / 7

暗号化されたビットストリームを用いたディジタルシネマ向けJPEG 2000符号化画像の同定法

飯田 知教† 渡邊 修†† 福原 隆浩††† 貴家 仁志†

† 首都大学東京大学院システムデザイン研究科情報通信システム工学専修 〒191–0065 東京都日野市旭が丘 6–6
†† 拓殖大学工学部情報エレクトロニクス学科 〒193–0985 東京都八王子市館町 815–1
††† ソニー株式会社 B2B ソリューション事業本部 〒243–0014 神奈川県厚木市旭町 4–14–1
E-mail: †{iida-tomonori@sd.tmu.ac.jp, kiya@eei.metro-u.ac.jp}, ††owatanab@es.takushoku-u.ac.jp,
†††Takahiro.Fukuhara@jp.sony.com

あらまし 本稿は，暗号化したJPEG 2000符号化画像を，暗号を解除することなく画像同定する方法を提案している．ここで，同定とは，同一の圧縮符号化方式で生成された符号化画像中から，原画像が同一の画像を判定することと定義する．提案法する同定法は，ビットストリーム中に存在するゼロビットプレーン数に着目しているため，ヘッダ以外のパケットボディなどを暗号化することを可能としている．さらに提案法は，画像の伸張処理と暗号の解除を必要とせず，セキュリティを確保した状態で高速に同定を実行することができる．

キーワード JPEG 2000，画像同定，暗号化，画像圧縮，スクランブル，画像検索

Identification of Encrypted JPEG 2000 Coded Images for Digital Cinema

Tomonori IIDA†, Osamu WATANABE††, Takahiro FUKUHARA†††, and Hitoshi KIYA†

† Dept. of Information and Communication Systems Engineering, Tokyo Metropolitan University
6–6 Asahigaoka, Hino-shi, Tokyo, 191–0065 Japan
†† Dept. of Electronics and Computer Systems, Takushoku University
815–1 Tatemachi, Hachioji-shi, Tokyo, 193–0985 Japan
††† B2B Solutions Business Group, Sony Corporation
4–14–1 Asahi-cho, Atsugi-shi, Kanagawa, 243–0014 Japan
E-mail: †{iida-tomonori@sd.tmu.ac.jp, kiya@eei.metro-u.ac.jp}, ††owatanab@es.takushoku-u.ac.jp,
†††Takahiro.Fukuhara@jp.sony.com

Abstract We propose an identification method for encrypted JPEG 2000 coded images. The proposed identification method provides a judgment whether the query image is the same as the original image of encrypted JPEG 2000 coded images without decryption. Packet-body can be encrypted due to the use of the number of zero-bitplanes in the proposed identification method. The images can be efficiently identified without decoding and decrypting for secure data management.

Key words JPEG 2000, Image identification, Encryption, Image compression, Scrambling, Image search

1. はじめに

本稿は，暗号化された符号化画像から画像を同定する方法を提案する．ここで，同定とは，同一の圧縮符号化方式で生成された符号化画像中から，原画像が同一の画像を判定することと定義する．ただし，圧縮率は同一であることを条件としない [1–3]．提案法は，圧縮方式として，JPEG 2000 符号化 [4] を対象として，パケットヘッダに格納されているゼロビットプレーン情報を特徴量とし，暗号化された符号化画像中から高速な画像同定を行うものである．

近年，大量のディジタル画像を取り扱う必要が高まり，所望する画像を高速かつ高精度に画像群の中から検索・特定する技術が求められている．特に JPEG 2000 はディジタルシネマ規格 (DCI:Digital Cinema Initiatives) [5] の画像コーデックとして正式採用され，大量の高精細画像を扱う必要性が生じている．JPEG 2000 符号化画像の同定法として，DWT(Discrete Wavelet Transform) 係数の正負符号を特徴量とする手法 [6,7] やゼロビットプレーン数を特徴量とする手法 [1,2] が提案されている．

一方，ディジタルシネマや医用画像などは，著作権保護を目的としたセキュリティやプライバシーを考慮する必要がある．この目的に対しては，画像のスクランブル法や暗号化法 [8–16] が提案されている．しかし，暗号化された画像群から所望画像を特定することは考慮されておらず，同定をおこなう際には，画像群の暗号を一旦解除し処理する必要があった．これは暗号化解除のための処理時間や鍵の管理などのセキュリティ面から問題があると考えられる．

提案法では，文献 [1,2] の画像同定手法を基本として，暗号化された JPEG 2000 符号化画像群の中から所望画像を特定する手法を提案する．同定法は，文献 [1,2] の方法と同様に，JPEG 2000 ビットストリームからヘッダ解析によって抽出したゼロビットプレーン情報を用いるため，高速な画像同定をおこなうことが可能である．また，暗号化法は，ゼロビットプレーン情報に影響を及ぼさない手法であれば，さまざまな従来の暗号化手法が適用可能である．例えば，DWT 係数の正負符号を反転する手法 [15] や，パケットボディの値を別の値へ変換する手法 [8–13] が直接適用可能である．一方，手法 [16] を用いると，正しいゼロビットプレーン数が抽出できなくなるため，コードブロックを交換する手法を用いることはできない．

2. JPEG 2000 符号化の概要と特徴

ここでは，JPEG 2000 について，その符号化手順，ビットストリーム構成にふれ，本研究で重要となるパラメータについて述べる．

2.1 JPEG 2000 符号化の概要

JPEG 2000 の典型的な符号化手順を図 1 に示す．入力画像は DWT が施されると分割レベルに応じて，複数個のサブバンド (subband) が生成される．サブバンド内の DWT 係数は量子化によって量子化係数に変換される．量子化係数はコードブロックと呼ばれる矩形領域に区切られ，各コードブロックはさらにビットプレーンに分解される（図 2）．EBCOT(Embedded Block Coding with Optimized Truncation) ではビットプレーン単位に，ビットモデリングと MQ 符号化をおこない，符号を生成する．レート制御は，EBCOT の構成単位である符号化パス (coding-pass) ごとに切り捨て処理 (Truncation) によって実現する．最後にヘッダを付加してパケット生成後，JPEG 2000 規格の符号化コードストリームを出力する．

2.2 ビットプレーン

ビットプレーンは係数データを従来の二次元から三次元に拡張して表現したものである（図 2）．同図に示すように，量子化係数を正負符号と係数の絶対値に分割し，係数の絶対値の部分を MSB(Most Significant Bit) から LSB(Least Significant Bit) に分割しそれぞれを 2 値信号として表現している．

ビットプレーンの大きさは以下のようにサブバンド毎に定義される．

$$K_b^{max} \triangleq \max\{0, \varepsilon_b + G - 1\} \quad (1)$$

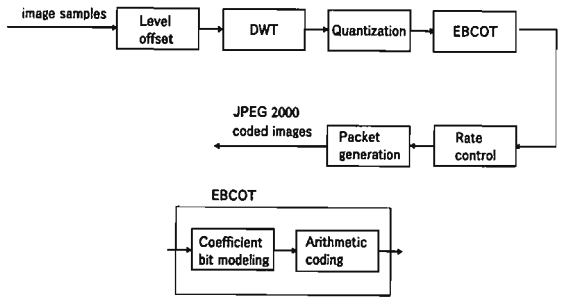


図 1　JPEG 2000 符号化手順.

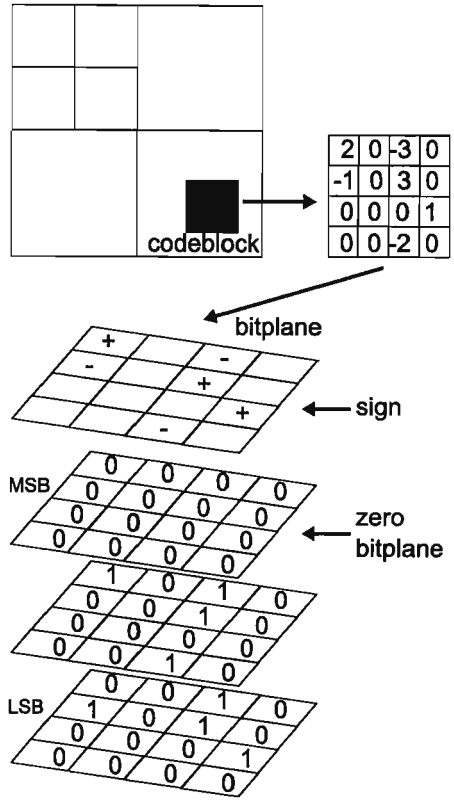


図 2　コードブロックとビットプレーンの関係.

K_b^{max} はビットプレーン数，G は保護ビット (guard bits) 数，ε_b は量子化ステップサイズのための指数パラメータである．

量子化係数をビットプレーンに分割した際，MSB からみていくと係数がすべて 0 となるビットプレーンが存在する．このビットプレーンをゼロビットプレーンという（図 2）．

ゼロビットプレーン数は式 (1) で定められるビットプレーンの大きさと量子化係数の大きさによって決まるため，異なる画像であれば，異なる数値となる可能性がある．なお，同一原画像から生成されるビットストリームのゼロビットプレーン数は，DWT 分解数，量子化ステップサイズ，コードブロックサイズ等の符号化パラメータが同じであれば同じ数値となる．

図 3 に，3 つのコードブロックをビットプレーン表現した際

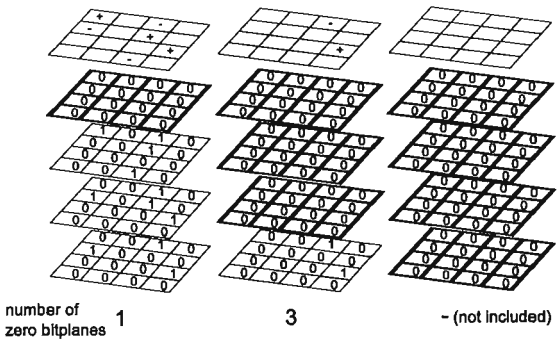


図3　ゼロビットプレーン数.

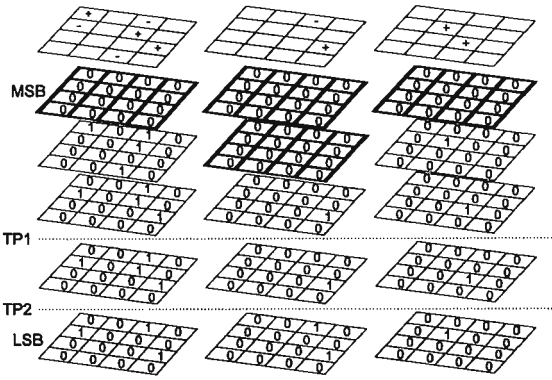


図4　レート制御.

の例を示す．左端のビットプレーンは最上位ビットプレーンのみがゼロビットプレーンなので，ゼロビットプレーン数は 1 となる．同様に，左端から 2 番目のビットプレーンは最上位ビットプレーンから数えて 3 個がゼロビットプレーンなので，ゼロビットプレーン数は 3 となる．左から 3 番目のビットプレーンはすべてのビットプレーンがゼロビットプレーンとなっている．この場合，JPEG 2000 ではこの場合，"not included"（ゼロビットプレーン数が未定義）と定め，そのコードブロックには符号化対象に含めるデータがないものとして取り扱う．

JPEG 2000 の圧縮時のレート制御は，通常最下位ビットプレーンから最上位ビットプレーン方向の順に，符号化コードストリームを切り捨てる手法を用いるので，ゼロビットプレーン数による同定法は圧縮率による影響を受けにくい利点を持っている（図 4）．図 4 は，3 つのコードブロックをビットプレーン表現した際の例である．同図の，TP1(Truncation Point 1)，TP2(Truncation Point 2) はそれぞれレート制御時のビットプレーン切り捨て位置を示している．同図を見てもらえれば分かるように，TP1，TP2 のどちらで切り捨ててもゼロビットプレーン数は同じである．以上のことから，圧縮率が変化しても，ゼロビットプレーン数には原理的に影響がないことがわかる．

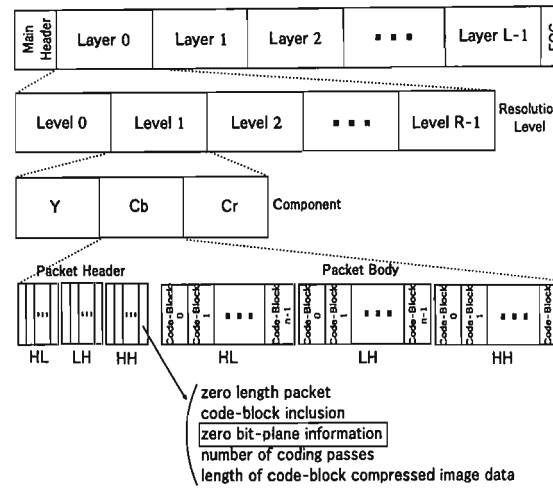


図5　JPEG 2000 ビットストリーム構造例.

2.3　ビットストリーム構造

JPEG 2000 のビットストリーム構造を図 5 に示す．ビットストリームは複数のパケットから構成される．パケットはパケットヘッダとパケットボディから構成され，パケットヘッダには各コードブロックの符号化パス数，ゼロビットプレーン数などの情報が格納されている．すなわち，コードブロックのゼロビットプレーン数は，パケットヘッダを解析することで得ることができる．

3. 提 案 法

提案法は，暗号化されたデータベース画像の中から，クエリ画像と原画像が同一の画像を特定する．ここで，データベース画像は DCI 規格準拠の JPEG 2000 方式で符号化されている圧縮ファイル群を指し，クエリ画像はデータベース中から特定したい画像の原画像を指す．データベース画像は DCI 規格準拠であることから，同一の符号化パラメータ（DWT 分解数，量子化ステップサイズ，コードブロックサイズなど）を用いて符号化されているため，クエリ画像も同じ符号化パラメータで符号化することにより，ゼロビットプレーン数の比較が可能となる．

以下に，同定法と暗号化法について述べ，最後に提案法の構成について述べる．

3.1　同定法の基本原理

ここでは，提案法で用いる同定法について述べる．同定法は，既に DCI 規格準拠の JPEG 2000 方式で符号化されている符号化画像群がデータベースに保存されていて，原画像がクエリ画像と同一である画像をデータベース中から特定することを指す．なお，提案法で用いる同定法は文献 [1,2] に基づくものである．本手法は以下に示す特徴を持っている．

- 計算負荷が小さいく，高速処理が可能．
- 圧縮率の変化に影響を受けにくい．
- 同定漏れがない．

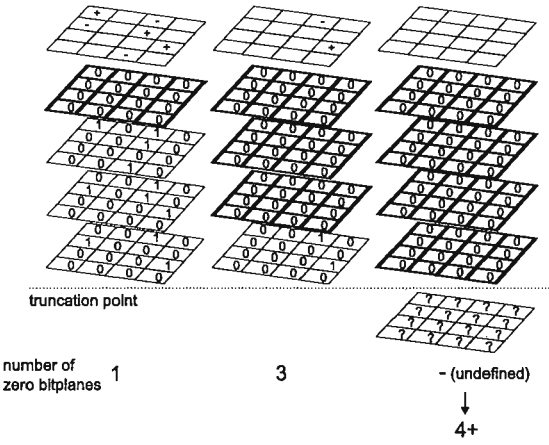


図 6　コードブロックの再定義.

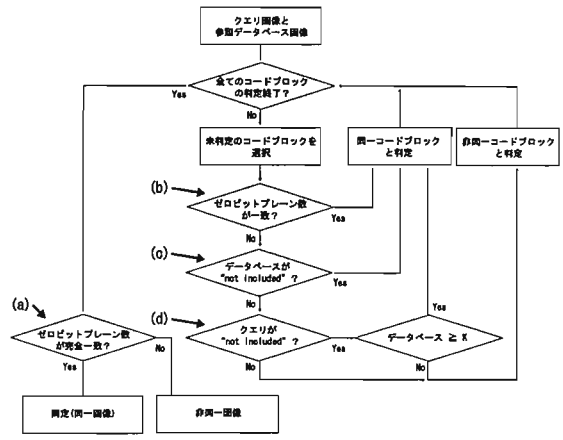


図 7　判定のフローチャート.

A. ゼロビットプレーン数の再定義

同定には JPEG 2000 ビットストリーム上に格納されているゼロビットプレーン数を画像の特徴とし処理をする．ただし，ゼロビットプレーン数は "not included" となる場合があり，単純な比較ができないため，図 6 のように再定義する．ただし，再定義はクエリ画像にのみ適用される．この再定義をクエリ画像に限定するのは，すでに符号化されているデータベース画像からは，"not included" となったゼロビットプレーン数を確認することができないためである．

図 6 の左から 3 番目のコードブロックでは，MSB 方向から数えて 4 番目のビットプレーンの位置で切り捨てがおこなわれたために，4 つのビットプレーンがゼロビットプレーンとなった．このコードブロックは，切り捨ての位置が更に LSB 方向であれば，下位のビットプレーンは非ゼロビットプレーンの可能性がある．従って，ゼロビットプレーン数は 4 以上の値となることから，ゼロビットプレーン数=4+と再定義する．

B. 同定規範

以下の条件により，データベース中の画像に対して 1 フレーム毎に同定を判定する．

(a)　クエリ画像とすべてのコードブロックのゼロビットプレーン数が完全一致するデータベース画像を同定とする．

ゼロビットプレーン数の一致，不一致は次の判定手順により，コードブロック毎に順に判定される．

(b)　クエリ画像とデータベース画像で，同じ位置のコードブロックのゼロビットプレーン数が一致ならばそれを同一のコードブロックと判定する．

(c)　データベースが "not included" の場合には，クエリ画像のゼロビットプレーン数に関係なく同一のコードブロックと判定する．

(d)　クエリ画像が "not included" の場合は，その時のゼロビットプレーン数 (K) を用いて，クエリ画像のゼロビットプレーン数を K+と定義し，データベース画像が K 以上の値のときに限り，両者は同一コードブロックと判定する．

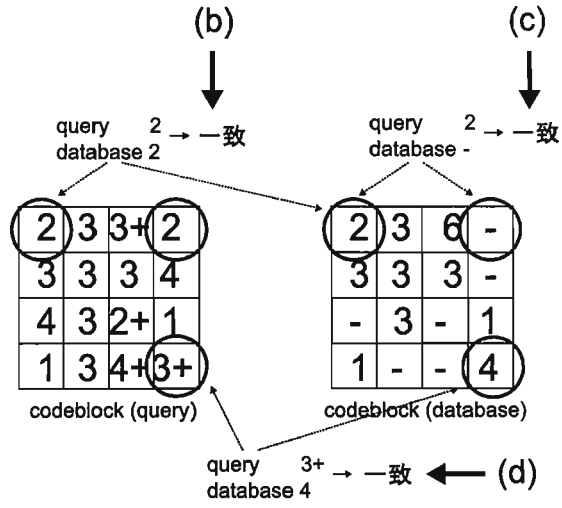


図 8　判定条件.

以上の手順を図 7 にまとめる．また，条件 (b)〜(d) の判定例を図 8 に示す．条件 (d) は，図 8 に示す様に，クエリ画像の 3+とデータベース画像の 4 とでは，＞K の奸計が成立しているので，同一のコードブロックと判定される．

3.2　JPEG 2000 符号列の暗号化

ここでは，提案法で用いる暗号化法について述べる．

JPEG 2000 符号化画像の暗号化法を，暗号化対象となるデータの種類によって以下の 3 種類に分類する．

- （方法 1）JPEG 2000 符号化過程のデータを暗号化
- （方法 2）JPEG 2000 ビットストリームを部分的に暗号化
- （方法 3）JPEG 2000 ファイル全体を暗号化

(方法 3) はビットストリーム上のヘッダ部とボディ部の両方に対し，暗号化処理を施す方式である．(方式 2) はビットスト

リーム上のボディ部のみを暗号化する方式である [8–13]. (方法 1) は符号化過程で生成される量子化係数等のデータに対し暗号処理を施す方式である [14, 15]. 例えば, 量子化係数の正負符号を反転や暗号化する手法などが挙げられる.

(方法 3) の方法はデータの暗号化と同じで, 暗号化後のデータを直接伸張したり, 画像として確認することができず, 画像の一部を確認する場合でも一般に全体を復号しなければならない. 故に, 画像データとしての取扱いが大きく制限される.

(方法 1), (方法 2) の方法は画像データを部分的に暗号化することにより, 暗号化後のデータの一部を画像として確認することが可能であり, 半開示なども可能となる. 画像同定を考えた際, 画像データの特徴の一部を確認する必要がある. そこで, 本研究で使用する暗号化処理は, (方法 1) や (方法 2) の手法を前提とする.

提案法で使用する同定法は, パケットヘッダに格納されているゼロビットプレーン数に着目し, 処理をおこなう. よって暗号化処理によってパケットヘッダの値が書き換わらなければ, 暗号化した JPEG 2000 符号化画像に対して同定処理をおこなうことが可能である.

情報半開示法などのように, 暗号化後のデータを直接デコードし閲覧する場合, 符号化データのパラメータが格納されているパケットヘッダに対し処理を実行すると, 暗号化データがデコード不可となってしまう場合があるため, 符号化データが格納されているパケットボディに対してのみ処理をおこなう場合が多い. よって, 多くの暗号化法が提案法で使用可能であると考えられる.

3.3 暗号化された符号列からの同定

データベースに格納されている符号化画像は暗号化されているものとし, この画像群に対し同定処理をおこなう. なお, クエリ画像はデータベース中から特定したい画像の原画像である. 同定処理の流れは以下のようになる.

- (手順 1) 符号化パラメータ (DWT 分解数, 量子化ステップサイズ, コードブロックサイズなど) をデータベース画像より抽出.
- (手順 2) 抽出した符号化パラメータを用いクエリ画像を符号化.
- (手順 3) クエリ画像と暗号化されたデータベース画像に対し, 同定処理を実行.

(手順 1) ではクエリ画像を符号化するために必要な符号化パラメータをデータベース画像より抽出する. データベース画像は DCI 規格準拠の JPEG 2000 方式で符号化されているため, 同一の符号化パラメータを用いて符号化されたものである. ただし, 可変ビットレートで符号化されているため, フレームごとの圧縮率は同一ではない.

(手順 2) では, 抽出した符号化パラメータを用いてクエリ画像を符号化する. データベース画像は同一の符号化パラメータを用いて符号化しているため, クエリ画像は符号化を一度実行すればよい.

(手順 3) では, クエリ画像と暗号化されたデータベース画像に対し, 同定処理を実行する. 3.2 で説明した暗号化方式であれば, 暗号解除の必要なくゼロビットプレーン数を抽出できる. よって, 3.1 で説明した同定処理がそのまま適用可能である.

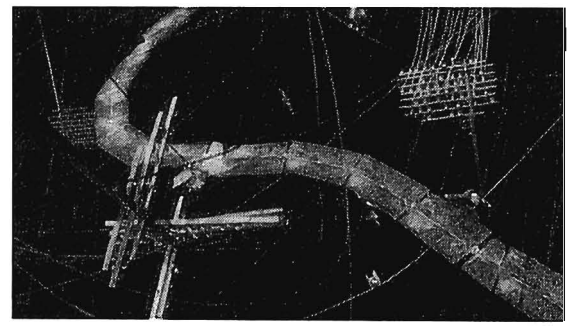


図 9 原画像 (3,000 フレーム目).

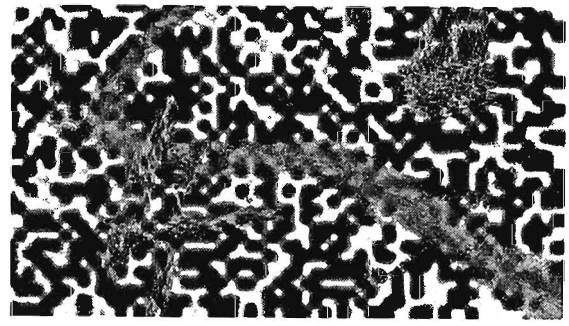


図 10 正負符号を反転 (3,000 フレーム目).

4. シミュレーション

4.1 シミュレーション条件

シミュレーションで用いた条件を表 1 に示す. 使用する動画として Elephants Dream の 15,691 フレームを用いた. シミュレーションでは, 表 2 に示すパラメータでデータベース画像のエンコードを行った. レート制御は固定レートであり, DCI 規格である VBR(Variable Bit Rate) 方式ではないが, 前に説明したように用いる同定法は圧縮率の影響を受けにくいため, シミュレーションとして有効であると考えられる. なお, 表 2 の符号化パラメータで処理をおこなった場合, 1 フレームあたり 6,321 個のコードブロックが発生する.

データベース画像には, DWT 係数の正負符号を確率 50[%] で反転処理を施し, シミュレーションをおこなった. なお, クエリ画像は, 3,000 フレーム目の画像を用いた. 図 9 に 3,000 フレーム目の画像を示す. また, 図 10 に量子化係数の正負符号を判定した画像を示す.

4.2 シミュレーション結果

シミュレーション結果を図 11 に示す. 横軸はフレームを表し, 縦軸はゼロビットプレーン数の一致率を表している. 使用した符号化画像には 6,321 個のコードブロックがあるので, 一致率は "同一コードブロックと判定された数/6,321" となる. 同

表1　シミュレーション条件.

動画	Elephants Dream
解像度	1,920(H)x1,080(V)
フォーマット	RGB 各 8 ビット
フレーム数	15,691 フレーム

表2　エンコード条件.

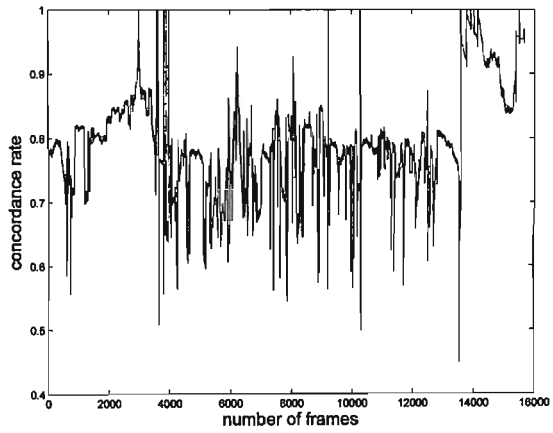
DWT 分解レベル数	5 (9 x 7 フィルタ使用)
コードブロックサイズ	32 x 32
レート制御	1 bpp

図に示すように，データベース画像の暗号化していても，同定結果に影響を及ぼしていないことが確認できる．

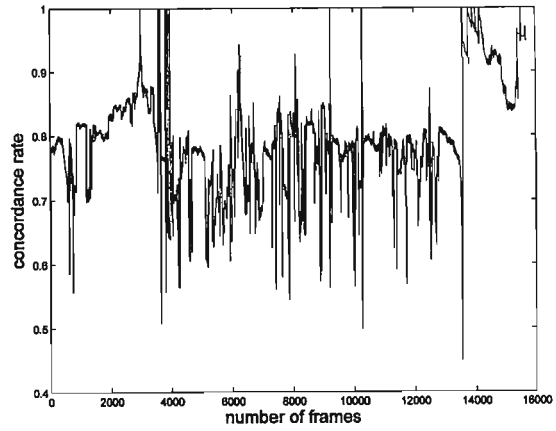
同定と判断された画像は，15,691 フレーム中 132 フレームあった．クエリと同じ原画像である 3,000 フレーム目の画像も同定されている．誤同定した残りの 131 フレームは，真っ黒や真っ白などの単一な輝度値しか持たない画像であったため，大半のコードブロックのゼロビットプレーン数が，"not included" となったものである．この場合，同定規範 (c) によりゼロビットプレーン数一致と判断され，同定と誤認識したものと考えられる．

5. おわりに

暗号化された JPEG 2000 符号化画像に対し，暗号化を解除することなく同定をおこなうことのできる手法を提案し，その有効性を示した．提案法は，暗号の解除の必要や，データベース画像の複号処理が必要でないため，高速な処理が可能である．また，データ漏洩などのセキュリティを確保した状態で，同定漏れを原理的に発生させることなく，高効率に同定することが可能である．



(a) 暗号化されたデータベース.



(b) 非暗号化のデータベース.

図 11　シミュレーション結果.

文　献

[1] 福原隆浩, 保坂和寿, 貴家仁志, "ディジタルシネマ向け JPEG2000 符号化画像のビットストリームレベル同定法, " 信学論 (D), vol.J91-D, no.9, pp.2305-2313, 2008.

[2] T. Fukuhara, K. Hosaka, and H. Kiya, "Accurate Identifying Method of JPEG2000 Images for Digital Cinema," Proc. of The 14th International Multimedia Modeling Conference, Jan. 2008.

[3] Fitri Arnia, I. Iizuka, M. Fujiyoshi, and H. Kiya, " Fast image identification methods for JPEG images with different compression ratios, " IEICE Trans. Fundamentals, vol.E89-A, no.6, pp.1585-1593, Jun. 2006.

[4] ISO/IEC 15444-1: JPEG2000 image coding system", 2000.

[5] Digital Cinema Initiatives, LLC Member Representatives Committee, "Digital cinema system specification V1.0, " Final Approval July 2005.

[6] 渡邊修, 川名明夫, 貴家仁志, "DWT 係数符号を用いた JPEG2000 符号化画像の同定法, " 2006 信学ソ大, no.A-4-8, p.75, 2006.

[7] 渡邊修, 川名明夫, 貴家仁志, "DWT 係数の正負符号を用いた JPEG2000 符号化画像の同定法" 信学信号処理シンポジウム, No.B2-1, Nov. 2006.

[8] 貴家仁志, 今泉祥子, 渡邊修, "マーカコードの発生を考慮した JPEG2000 符号化画像の情報開示法, " 信学論 (D-II), vol.J86-D-II, no.11, pp.1628–1636, Nov. 2003.

[9] 岩村恵市, 林淳一, "JPEG2000 符号化画像のマーカコード発生を回避できる暗号化方式, " 信学論 (A), Vol.J90-A No.11, pp.839–850, Nov. 2007.

[10] 安藤勝俊, 渡邊修, 貴家仁志, "JPEG2000 符号化画像の情報半開示法, " 信学論 (D-II), vol.J85-D-II, no.2, pp.282–290, Feb. 2002.

[11] 安藤勝俊, 貴家仁志, "レイヤ構造を利用した JPEG2000 符号化画像の暗号化法, " 信学論 (A), vol.J85-A, no.10, pp.1091–1099, Oct. 2002.

[12] S. Imaizumi, O.Watanabe, M.Fujiyoshi, H.Kiya, "Generalized Hierarchical Encryption of JPEG 2000 Codestreams for Access Control, " IEEE ICIP, vol.II, pp.1094–1097, Sep. 2005.

[13] S.Imaizumi, M.Fujiyoshi, Y.Abe, H.Kiya, "Collusion Attack-Resilient Hierarchical Encryption of JPEG 2000 Codestreams with Scalable Access Control, " IEEE ICIP, vol.II, pp.137–140, Sep. 2007.

[14] 高山真, 田中滑, 米山暁夫, 中島康之, "MPEG 圧縮ドメインでのスケーラブルなスクランブル方式, " 信学 PCSJ, no.P-2.10, pp.53–54, Nov. 2006.

[15] Raphaël Grosbois, Pierre Gerbelot and Touradj Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain," Proc. SPIE, vol.4472, pp.95–104, San Diego, CA, U.S., Jul.–Aug. 2001.

[16] 飯田知教, 藤吉正明, 貴家仁志, "マーカコード発生の回避を考慮した JPEG 2000 符号化画像のビットストリームレベル情報半開示法, " 信学技報, no.SIP2007-76, vol.107, no.181, pp.25–30, Aug. 2006.