Vol.2009-AVM-66 No.8
2009/9/24

自己動画コンテンツチェックによるコンテンツ正当性検証方式

児玉 明[†,††]

近年、ネットワークのブロードバンド化を背景に、ネットワークを利用したコンテンツサービスが普及し始めている。一方、コンテンツプロバイダーの立場からすると、貴重な資産コンテンツの安心安全利用の観点から、十分にサービス提供できない状況がある。コンテンツデータの保護方法として，主にデータ処理の暗号化方法，著作権管理方法などが検討されてきた．また、コンテンツプロバイダーと利用者との利用契約環境を考慮して，個々の送信情報に利用者情報を埋め込む方法やオリジナルを示す透かし情報を挿入する方法などが検討されている．そこで我々は，コンテンツの安心・安全利用を背景として，統合的なコンテンツ流通システムの実現を目指し，コンテンツ自身の情報を利用した配信，認証方法について検討してきた．本研究では，特に，動画コンテンツの配信時に着目したコンテンツの不正利用対策として，受信コンテンツ自信の情報を利用したチェック機能によるコンテンツ正当性検証システムを提案し、その有効性を評価する．

A Contents Correctness Verification Method by Checking Own Video Contents

Mei Kodama[†,††]

In video delivery systems over high-speed network, it is important to protect to use video contents against the law according to DRM technologies. We propose a contents correctness verification system using amount of video characteristics. The video data structure and authentication are focused on. In this study, the quantization parameter (MQ) of video coding as key information is used. After the system procedure is indicated, we consider the effect of utilization in this system and video characteristics for verification. By the experimental results, the accuracy of the key information is shown using the relationship between the coding rate and the MQ value. Moreover, the original information is also shown and the processing time is indicated in some hash methods. Finally, encryption functionality, see protection functionality and data verification functionality are organized.

1. はじめに

近年，ネットワークの高速化と低廉化を背景に，急速にインターネットを利用した動画や音楽などのコンテンツサービスが変貌を遂げようとしている．反面，コンテンツのネットワーク利用に対して，各種 DRM 技術を利用し，アクセス利用制限を設けることで，コンテンツの不正流通に対する耐性を考慮したコンテンツ配信を実現しており,ネットワークの利便性に対するコンテンツ不正利用の拡大が課題として有する．言い替えると，コンテンツの普及とコンテンツ不正防止の要求関係が相反し，ビジネスモデル実現のために，様々な課題を有していると言える．例えば，メディア販売やネットワーク提供での動画コンテンツの高画質化が進んでいるが，不正流通に対する対応策を考慮すると，ネットワーク提供時の動画品質が蓄積媒体と比較して品質が不十分で，高品質を要求する利用者はメディア販売からネット利用へと進まない傾向がある．所謂，コンテンツ利用の利便性やコストとの関係の中で，利用者はコストや利便性，品質などの自分の目的にあった様々な動画コンテンツサービスを模索しているのが現状である．利用拡大とコンテンツ保護というトレードオフの関係の中で，ビジネスモデルの拡大を阻害していると考えることもできる．また，これからの様々なアーカイブサービスにおいてネットワーク利用は不可欠であり，コンテンツ保護や利用促進に対する研究は重要な課題となっている．

これまで，コンテンツデータの保護方法として，主にデータ処理の暗号化方法，著作権管理方法などが検討されてきた．また，利用環境の多様化に伴い，不正流通を考慮してコンテンツ流通時の発信元・受信元の特定が要求されはじめている．ここで，コンテンツプロバイダーと利用者との利用契約環境を考慮して，個々の送信情報に利用者情報を埋め込む方法や，オリジナルを示す透かし情報を挿入する方法などが検討されている[1]-[5].

そこで我々は，コンテンツの安心・安全利用を背景として，統合的なコンテンツ流通システムの実現を目指し，コンテンツ自身の情報を利用した配信，認証方法について検討してきた[6]-[10]．本研究では，特に，動画コンテンツの配信時に着目したコンテンツの不正利用対策として，コンテンツ正当性検証機能を有するコンテンツ流通システムを提案する．本研究では，データの暗号化観点ではなく，送受信時のデータ抽出･データ分離によるコンテンツ正当性保証の有効性について明かにする.はじめに，提案システムの概要について説明し，システムで利用するデータ処理方法およびデータ抽出方式について説明する．本研究では，動画コンテンツに着目する．評価実験と

† 広島大学大学院総合科学研究科
Graduate School of Integrated Arts and Sciences, Hiroshima University
†† 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University

して，データ検証方法とシステム実現性について考察する．

2. 提案システム

2.1 システム概要

サーバに映像コンテンツが蓄積されており，利用者からのオンデマンド要求により，映像配信するモデルを想定する．本モデルにおいて，コンテンツ情報の正当性検証を実現するために，予めコンテンツ DB サーバに，検証処理用の情報を蓄積しておく．

利用者が受け取った情報に対して検証情報を生成し，情報検証することで正当性検証機能を実現する方法を提案する．提案システムでは配信サーバにアクセスする際に利用者認証を行うとする．言い換えると，動画像構造に着目した特徴情報を生成し，その情報をコンテンツデータの正当性検証に利用する動画配信システムである．

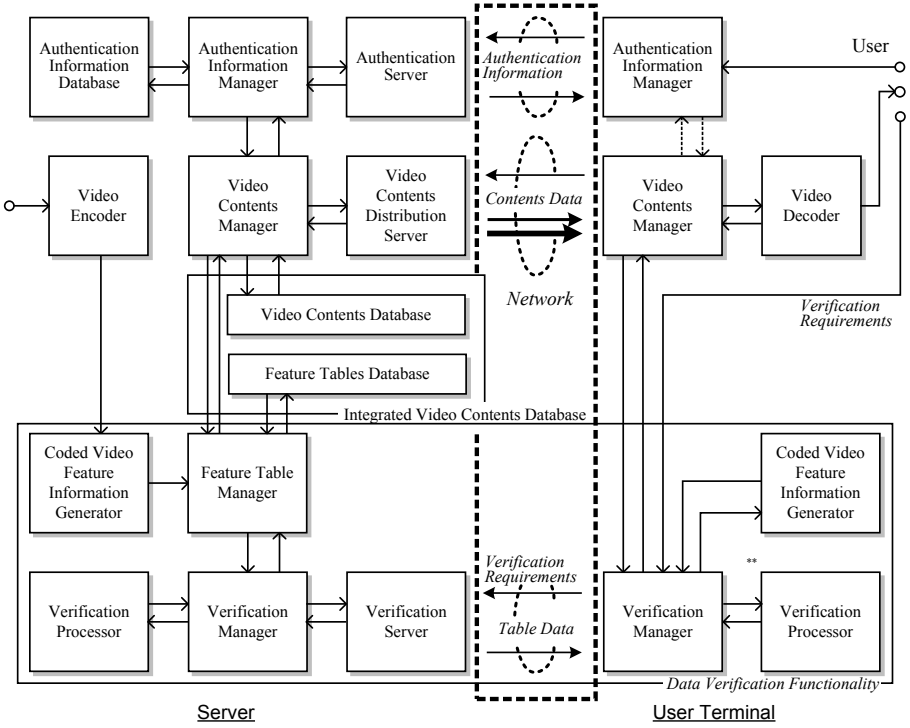


図 1　提案システム

動画コンテンツとして汎用的な符号化方式の利用を考える．図 1 に提案システムの概要を示す．符号化情報からコンテンツ検証情報を生成し DB 化し，また送信したメディア情報自身から特徴情報を生成し，特徴情報間で検証判定する．検証判定を受け，復号器を制御することで，正当性検証を実現する．検証精度への対策として，これまで検討してきた画像検索手法[11][12]を利用することで，動画像コンテンツの時間特性により検証精度が向上すると考えられる．さらに，定期的な検証を行うことで，コンテンツ長への対処が可能となる．また一度の検証に利用する特徴情報をグループ表現とすることで，さらに検証処理時間を高速化することが可能となる．図 1 中の**は，クライアント(利用者側端末)において，検証機能がある場合であるが，基本的には，受け取ったコンテンツ情報から生成された検証用情報はサーバに転送して検証する方法が，有用であると考えられる．

また，秘匿性制御のための拡張方法として，分割・合成データの利用が可能であり，合成情報を利用した配信システムを図 2 に示す．

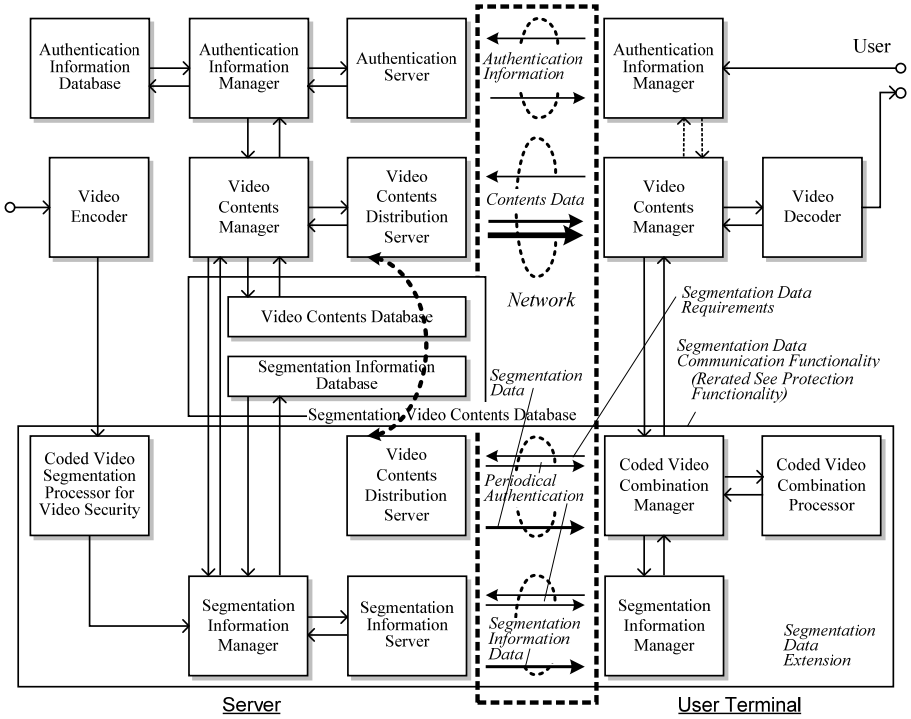


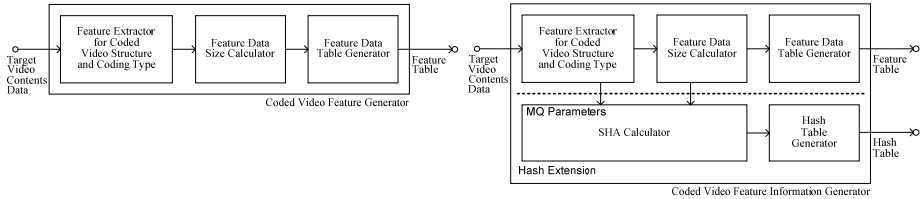
図 2 合成情報を利用した配信システム

2.2 正当性検証処理方法

正当性検証処理として，データ生成器とその情報検証処理器から成る（図 3,4）．それぞれ，符号化情報の構造を特異情報として，特徴量テーブルを作成する処理と，サーバで管理されている真の特徴量テーブルとの照合により，データ検証を行う処理を示す．図 3 に基本構造を(i)に拡張構造を(ii)に示す．

(i)では，符号化構造情報，実データなどからの特徴量抽出を行う場合を示している．(ii)ではさらに下段に，SHA 算出処理を加えた拡張処理を示した．例えば，符号化レート，符号化モードなどが異なる場合，量子化制御に対応した MB 量子化パラメタが変動することが知られている．これらの情報をフレーム内の局所範囲，例えばスライス単位など利用し時間拡張することで，その検証精度は保持可能となる．一方，これらの特徴情報をさらに，SHA ハッシュ値として利用することで，飛躍的に検証，即ち，同定を目的とした場合，処理速度の向上が期待される．図 4 のデータ検証器において，特徴情報検査処理を実行し，DB 情報と受信後のデータから生成したデータ間との同一性を検証する．

図 3,4 で扱う情報として，構造情報利用したインデックス情報処理，或いは，分離情報として扱うことができる．無論，インデックス情報も分離情報として扱うことも可能である．さらにスケーラブル符号化等を利用した分離データ拡張のデータ生成器を図 5 に示す．



(i) 基本　　(ii)拡張

図 3　符号化動画特徴情報生成器

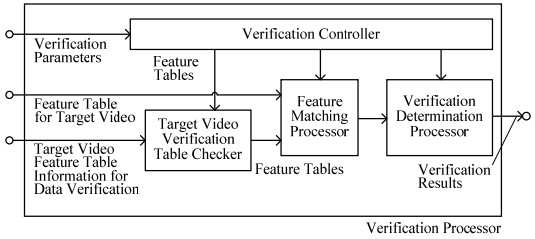


図 4 データ検証器(基本)

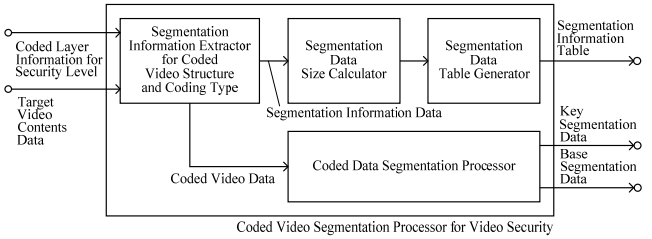


図 5 符号化動画情報分割データ生成器

2.3 キー情報の生成

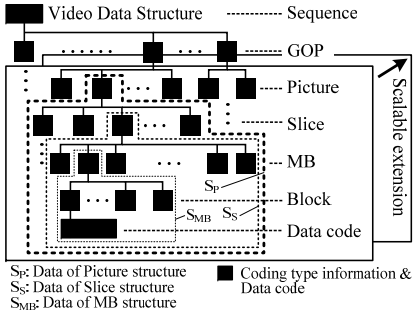


図 6 符号化動画構造の例

現在，多くの動画符号化方式で利用されている変換・予測のハイブリッド符号化方式では，符号化効率に繋がることから，圧縮効率が高いデータであればあるほど，局所領域間相関を利用した符号化データ構造であると考えることができる．

分離データ或いはチェックデータに利用する符号化動画構造例を図 6 に示す．ここでは，空間方向の矩形ブロックの集合とフレーム集合から構成される一般的な符号化構造の例を挙げた．図 6 に示した構造に基づいた場合，S_P,S_S,S_{MB} などの構造情報とそれに付随するデータ値がキー情報として生成される．加えて，各種スケーラブル拡張も可能であり，これまで我々が提案してきた更新型ストリーム構造を分離情報として扱うことも可能である[13].

3. 評価実験

3.1 キー情報の検証

検証情報として，実データレベル，符号化構造レベルなどが考えられるが，検証精度と情報量との関係が正当性検証としての課題となる．ここでは，符号化パラメタに

Vol.2009-AVM-66 No.8
2009/9/24

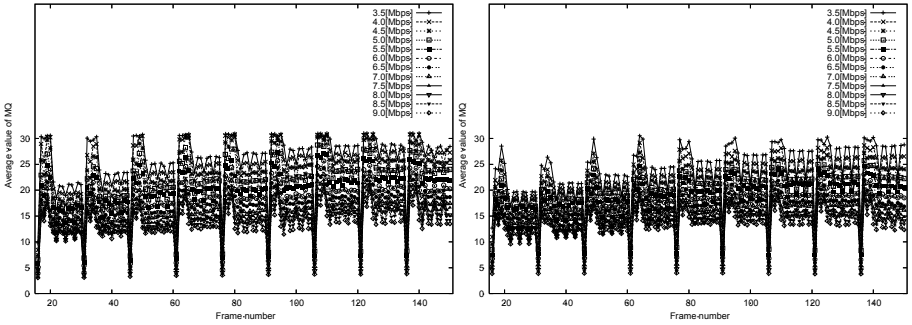
着目し，キー情報としての有効性を精度の観点から評価する．ここでは MB 量子化パラメタ MQ に着目し，符号化シミュレーション実験に MPEG-2 TM5 MP@ML を利用する．実験条件を表 1 に示す．ただし，画像フォーマットは 704[pel]x480[line]，色差フォーマット 4:2:0 を利用する．但し，安定した MQ 評価を目標とし，先頭 GOP は符号化するが評価には利用しない．

表 1 実験条件

テストシーケンス	Flower garden(flow), Mobile & calendar(mobl), Table Tennis(tabl), popl, Bus (5 sequences)
フレーム数	150[frame], 10[GOP]
符号化方式	TM5(MPEG-2)
MQ	全ての MB，中央スライス MB
符号量	3.5-9.0[Mbps](0.5[Mbps] 間隔)
ハッシュ化方法	非使用，SHA-1, SHA-256, SHA-384, SHA-512
評価方法	MQ 値，ハッシュ値

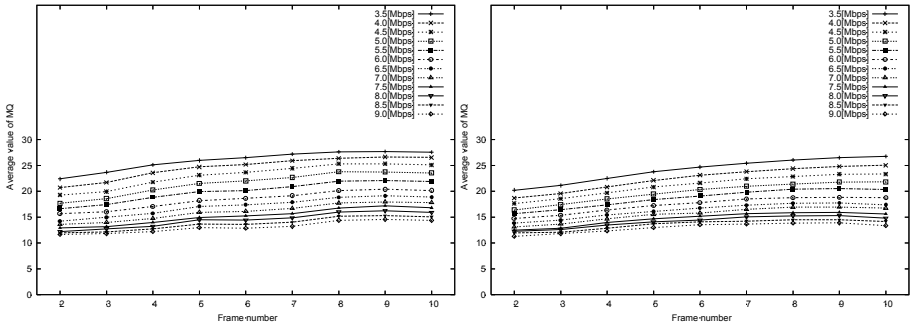
ここでは，テストシーケンスの中で，代表的な flow, mobl についての MQ 値の変動について，シミュレーション実験結果を図 7-10 に示す．また，フレーム内すべての MB において，MQ を利用した場合と，中央スライスライン(Slince 番号 16 番目とした)の MB において，MQ を利用した場合をそれぞれ示した．

無論，全ての MQ 値を利用する方が MQ 値による相違判定確率が増し精度が向上するのは明らかであるが，ここでは多くのテストシーケンスではないが，同一シーケンスのレート品質に対する性能評価も含めてその変動を示すこととした．図において，フレーム単位では，符号化フレーム順での MQ 値変動を示している．一方，GOP 単位では，全 150 フレームに対応する GOP9 個のデータに対する結果を示している．



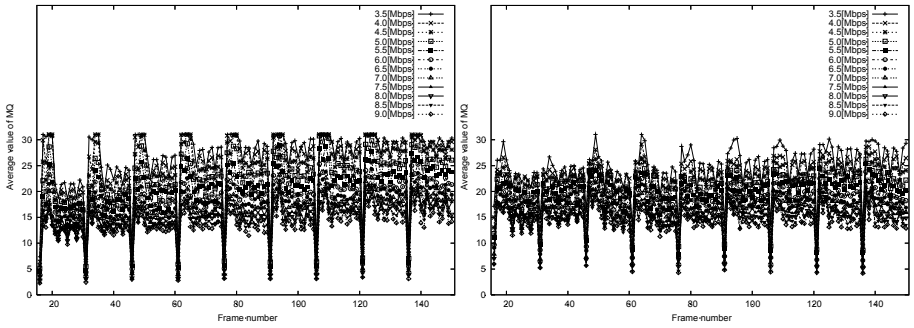
(i) flow (ii) mobl

図 7 全ての MB を利用した MQ 値の平均(フレーム単位)



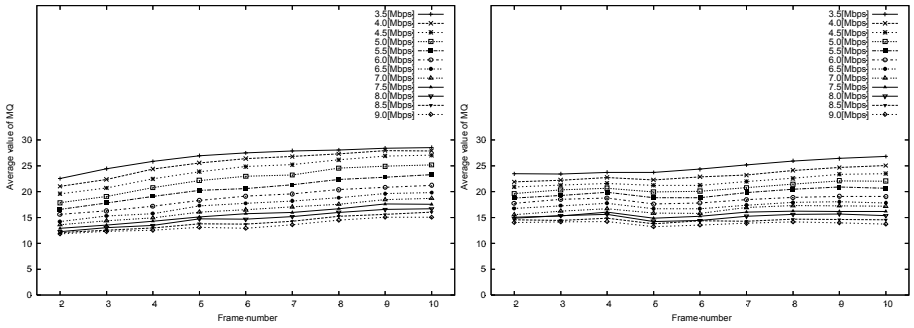
(i) flow (ii) mobl

図 8 全ての MB を利用した MQ 値の平均(GOP 単位)



(i) flow (ii) mobl

図 9 中央スライスの MB を利用した MQ 値の平均(フレーム単位)



(i) flow (ii) mobl

図 10 中央スライスの MB を利用した MQ 値の平均(GOP 単位)

ここで，テストシーケンスの先頭の GOP は符号化制御が安定しないので，ここでは扱わないで考える．

各符号量に対して量子化幅 MQ の変動が確認され，シーケンス及び異なる符号量によっての固有情報として利用可能なことを示している．ここでは，MQ の整数値をそのままキー情報として利用しても，平均値として利用してもよいと考えられる．H.264/AVC などでも同様に考えることができる．

3.2 ハッシュ演算

表 2 MQ 値から算出されたハッシュ値

方式	ハッシュ値
SHA-1	5d1b79640bf642da3a75dc6b4ea5f9321befc0db 5e85125333d023e77788d683b9eb4c3280f0df68 58fb8779ac0bb8fb69def79a74f37b3ae73a5ada 373c8986f6cf744f8a9d9e548b90314f1bd35ffa 25135897edf5d14ede80b2b514cbcc6fa74f3c42 69182ed18bb11ea29c49cb7b1e2ca47ec9ab9ff5 e2b8641f42fb1f2f8686c542f84e8cc0cdd224f4 9af49ca87302f4a4aca21c3a9fe919b8e7624bca db598567f695a1a6afb41d7b78104583c2b0e811 4acfc362383cc08571855ffa62236800442efb0d

表 3 ハッシュ計算処理時間

方式	処理時間平均 ($x10^{-5}$ [s])
SHA-1 & 全ての MQ	6.40
SHA-1 & スライス MQ	6.24
SHA-256 & 全ての MQ	6.12
SHA-256 & スライス MQ	6.12
SHA-384 & 全ての MQ	5.98
SHA-384 & スライス MQ	5.92
SHA-512 & 全ての MQ	6.12
SHA-512 & スライス MQ	5.86

次に，図 3(ii)に示した拡張方式として，MQ 値をさらにハッシュ化した場合について考察する．SHA-1,256,384,512 の中で SHA-1 の結果を表 2 に示す．但し，ここではシーケンス flow,mobl, tabl,popl, bus の順とし，MQ 全て，MQ スライスの計 10 個の値の順に示した．ここで機器とツールとして,それぞれ CPU Pentium 4 2.0GHz, Memory 1GB, shasum を利用した．次に，SHA 処理時間を表 3 に示す．但し，処理 1 万回平均として示す．

今回の実験では，サンプル数が少ないのでハッシュ値の衝突はなかった．また，データ量と処理方式に殆ど顕著な処理の差がなかった．これは元となる入力情報量が MQ 値のみで扱ったためであると考えられ，全 MQ，スライス MQ を考えると，処理的な観点からは相違はなく，ハッシュ化して扱う場合，精度から考えると全 MQ が有効と考える．

これらの実験結果より，キー情報を SHA ハッシュ値やグループ代表値などを利用することで，飛躍的に検証，即ち，同定を目的とした場合，処理速度の向上が期待される．

4. 考察

提案システムにおいて，データチェック機能，データ分離拡張，DRM 機能を考慮して，システム構成について考える．但し，ここでは認証システムは必須と考える．

ログイン認証，DRM 機能によるコンテンツ不正利用制御を利用したコンテンツ利用要求に合わせた基本モデルに対して，提案する正当性検証機能，分離データ型，内部情報チェック型方式について整理する．

(i) データチェック機能付き基づいた動画情報配信システム(図 1)
(ii) 分割情報に基づいた動画情報配信システム(図 2)
(iii) DRM 機能及びデータチェック機能付き分割情報に基づいた動画情報配信システム(図 11)

(i)の基本的なデータ検証処理は，DRM 機能も含めて，サーバから利用者へ利用者の要求に合わせて送信した動画情報について，データ検証要求があると，利用者からサーバに検証用データ送信要求を送り，その検証データとの整合性を利用者端末内で行い，許可の有無により，再生器を制御する方法である．サーバから利用者へ利用者の要求に合わせて送信した動画情報について，データ検証要求があると，利用者からサーバに検証用データ送信要求を送り，その検証データとの整合性を利用者端末内で行い，許可の有無により，再生器を制御する方法である．

(ii)のモデルは，分離情報利用により，秘匿性を踏まえた閲覧制御を実現する．分割情報に核情報が含まれている場合，有意な情報再生ができない特性を利用する．DRM 機能とは異なり，暗号化を後で追加することは可能であるが，データ自身の暗号ではないことが特徴である．分離情報では，DRM 機能も含めて，データ分割型で利用者へデータを提供し，利用者側でデータ合成して，再生する基本的なモデルを示している．符号化情報を秘匿性制御，閲覧制御を考慮して，データ分割型で利用者へデータを提供し，利用者側でデータ合成して，再生する基本的なモデルを示している．

(iii)のモデルは，図 11 に示すように，DRM 機能を含み，分割情報を利用した秘匿

性制御，閲覧制御の機能を有する配信システムであり，さらに，利用者側のデータ検証要求に合わせて，サーバ，利用者間で検証情報のやりとりを行い，検証結果に基づき，分割情報を合成利用するシステムを示している．ここでは，DRM を暗号化機能，分離合成処理を秘匿性機能，データ検証処理機能をインデックス情報と分離情報による検証処理として示した．

このように，複数の秘匿性，不正利用方式を融合することが可能であり，本方式は拡張性に優れていると言える．

5. まとめ

本研究では，動画像コンテンツの正当性検証機能を有する動画配信システムを提案した．また精度の観点から MQ を特徴情報としたキー情報生成方法を示し，その正当性保証についてシミュレーション実験を行った．また，高速化の観点からさらにハッシュ化による効果を検証し，提案方式の有効性を明らかにした．今後は，システムモデルにおける処理効率について検討する．

参考文献

1) 渡辺, 三部, 中村, 酒井:"超解像の原理を応用した動画像向け電子透かし方式",信学論誌 D-II, J88-D-II, 5, pp.833-843 (2005).
2) 藤本, 鈴木, 中山, 竹下, ラムザン, ジェントリィ, ジェイン:"環境適応型コンテンツ配信におけるコンテンツ正当性保証の実現", 信学論誌 B, J89-B, 3, pp.324-336 (2006).
3) 今井編著:"ユビキタス時代の著作権管理技術", 東京電機大学出版局 (2006).
4) 稲葉, 山本:"プライバシーと著作権を考慮したコンテンツ配信に関する提案", 信学論誌 D, J89-D, 12, pp.2536-2542 (2006).
5) 釜江, 沼田, 曽根原:"ディジタルコンテンツ販売のための開示度と料金の設定", 信学論誌 D, J91-D, 1, pp.12-22 (2008).
6) M. Kodama, S. Suzuki:“Consideration of Contents Utilization Time in Multi-Quality Video Content Delivery Methods with Scalable Transcoding”, IEICE Trans. on IS, E88-D,7, pp.1587-1597 (2005).
7) 児玉:"情報処理装置， 配信管理サーバ，配信要求方法，配信管理方法，コンテンツ配信システム，配信要求方法，配信管理方法，配信要求プログラム， 配信管理プログラムおよび記録媒体", 特願 2005-024554 (2005).
8) 児玉:"コンテンツ利用認証を用いた動画配信システムの一検討", 画電研報, 07-05-12, pp.73-78 (2008).
9) 児玉:"動画像配信システムおよび動画像配信方法", 特願 2008-138025 (2008).
10) 児玉:"コンテンツ正当性検証機能付き動画像配信システムの一検討", 映メ学冬大, 7-6 (2008).
11) 児玉:"動画特徴量を利用したコンテンツ正当性検証システムの一検討", 画電年大, R2-6 (2009).
12) 児玉, 池田:"MSP 動画像検索システムの提案とその一評価", 画電学誌, 30, 5, pp.600-612 (2001).
13) M. Kodama:"Comparison of Coding Efficiency in Updatable Scalable Video Coding for Multi-quality", IEVC 2007, IP-4, pp.1-4 (2007).

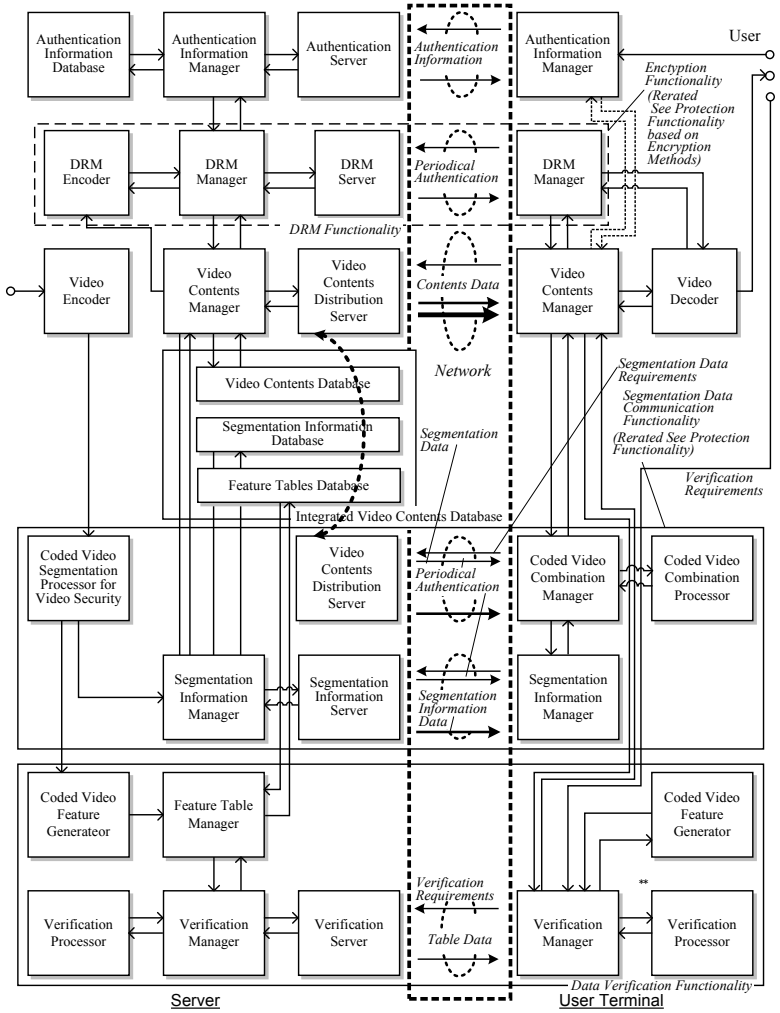


図 11 DRM 機能及びデータチェック機能付き分割情報に基づいた動画情報配信システム