I-013

コンテンツ再生時に画質制御可能なスクランブル効果制御方式

A Digital Video Scrambling Method with Variable Concealed Level for Stored Content

西本 友成† 藤津 智† 木村 武史† 今泉 浩幸† 三田 長久‡
Yusei Nishimoto† Satoshi Fujitsu† Takeshi Kimura† Hiroyuki Imaizumi† Nagahisa Mita‡

1. まえがき

有料放送では、契約者のみに放送サービスを提供するために、受信契約の状態に応じて、視聴の可否を制御できるアクセス制御システム[1]を用いる。このアクセス制御システムは、視聴可否制御という観点から２つに大別できる。一つは、コンテンツの視聴可と不可の２段階制御方式であり、デジタル放送で採用されている。もう一つは、番組の購入意欲を高めることを目的として、未契約者にも劣化させた映像を視聴させるために、コンテンツの映像画質を制御するスクランブル効果制御方式である。スクランブル効果制御方式は、未契約者に対する番組宣伝効果を持つため、２段階制御方式に比べて、デジタル放送で新たなビジネスモデルを創造できると期待される。

一方、近年、ワンセグやデジタルラジオと呼ばれる携帯受信機向けのリアルタイム受信の放送サービスが開始された。さらに、携帯受信機に一旦番組を蓄積してから再生視聴するダウンロード型の放送サービスが検討されている。そのため、携帯受信機向け放送において、蓄積後の再生視聴を前提とするダウンロード型放送用のスクランブル効果制御方式が望まれる。

しかし、携帯受信機向け放送で採用される H.264/AVC 符号化[2]コンテンツ用に最適化したスクランブル効果制御方式がない。また、従来方式[3]は、可変長符号を処理するので画質制御のための処理量が大きく、携帯受信機上の実装に適していない。また、これまで放送受信時のスクランブル効果制御方式は検討されてきたが、コンテンツ再生時のスクランブル効果制御方式は検討されていないという課題がある。

本稿では、携帯受信機向けのダウンロード型放送のための H.264/AVC 符号化コンテンツのスクランブル効果制御方式の要求条件について述べ、開発したスクランブル効果制御方式の概要を説明し、本方式の実装評価結果について報告する。

2. スクランブル効果制御方式の要求条件

携帯受信機向けダウンロード型放送では、携帯受信機にコンテンツを蓄積し、再生視聴や外部コピーを行う。そのため、再生回数、利用期間やコピー回数に応じて画質制御できるスクランブル効果制御方式が望まれる。さらに、有料放送の場合、不正な再生視聴や不正コピーを防止できる技術的手段を必須とする。また、携帯受信機への実装であることを考慮して、画質制御のための処理量をできる限り小さくする必要がある。

今回、以下に示す要求条件を設定し、それを満足するスクランブル効果制御方式を開発した。

(1) スクランブル効果制御を実現しながら、不正な視聴を防止できる技術的手段を持つこと
(2) 再生時およびコピー時に、スクランブル効果を制御できること
(3) デスクランブラの構成規模が小さく、処理負荷が小さいこと
(4) H.264/AVC 符号化方式に対応できること

3. スクランブル効果制御方式の設計

本方式では、再生時およびコピー時のスクランブル効果を実現するために、コンテンツをスライスレイヤーで暗号化し、その復号鍵をライセンスとして配布する。暗号化技術により不正視聴を防止し、スライスレイヤーでの暗号化により多段階の画質制御を行う。本方式が持つ暗号化による画質制御技術と、スライスレイヤーの暗号化技術について述べる。

3.1 暗号化による画質制御技術

図 1 に、暗号化による画質制御技術の概要を示す。スライス単位で暗号化することを基本とし、各々のスライスをスライス種別やスライス番号(スライス開始位置)毎に、ブロック化し、それぞれのブロックを異なる暗号鍵で暗号化する。そして、含まれる暗号鍵の数が異なる複数のライセンスを用意する。これにより、受信側では、所持するライセンスに応じて、復号できるスライスが異なるため、画質の劣化度が異なる映像を再生させることができる。さらに、再生後やコピー時に、ライセンスに含まれる暗号鍵を減らしていくことで、再生回数やコピー回数に応じて画質を多段階で制御できる。

全てのスライスは暗号化されるため、不正視聴に対する本方式の安全性は、採用する共通鍵暗号の強度に依存する。

3.2 スライスレイヤーの暗号化技術

単純にスライスレベルで暗号化した場合、H.264/AVC 符号化の規定にないデータが存在することになり、受信側の映像デコーダをハングアップさせてしまう恐れがある。今回、映像デコーダのハングアップを防止するスライスの暗号化技術を開発した。

図 2 に、開発したスライスの暗号化技術の概要を示す。暗号化処理は、信号処理の負荷を軽くするために、H.264/AVC 符号化方式の伝送レイヤである NAL(Network Abstraction Layer)レベルで行う。対象のスライスを暗号化する際、スライスヘッダおよびスライスデータ部を暗号化し、NAL ヘッダの NAL_unit_type を、新規に導入する暗号化 NAL unit に変更する。また、暗号化したスライスデータの最後尾に、1Byte の暗号化情報を付加する。暗号化情報は、スライスデータ部の暗号化情報であると同時に、スライスデータの終わりを示す RBSP Trailing bits としての機能も持つ。暗号化したスライスデータ部にスタートコード（エミュレーションコード含む）が発生した場合は、

†NHK 放送技術研究所, Science and Technical Research Labs.
‡熊本大学, Kumamoto University

再度暗号化を繰り返す。そのため、暗号化情報として、スライスデータの暗号化回数を記録する。

さらに、暗号化 NAL unit の直前に、効果制御用のスライスデータである NAL unit(非暗号)を追加する。効果制御用スライスは、できる限り小さいデータ量としたいため、I スライスの場合は、グレースケール表示のマクロブロックで構成し、P スライスと B スライスは、動きベクトル情報を持たないスキップトマクロブロックで構成する。

次に、受信機動作について説明する。暗号化 NAL unit の NAL_unit_type は、現行規格のリザーブ値を使う。そのため、従来技術の映像デコーダで処理した場合や暗号化 NAL unit の暗号を復号できない場合は、暗号化 NAL unit は無視され、効果制御用スライスが処理される。暗号を復号できる場合は、効果制御用スライスを読み飛ばし、暗号化 NAL unit を復号して映像を表示する。

これにより、暗号化したスライスによる映像デコーダのハングアップを防止でき、かつ、固定長符号である NAL_unit_type の判別のみで復号処理できるため可変長符号処理を不要とし、スクランブル効果制御の処理を低負荷で実現できる。

4. 実装評価

本方式で暗号化したコンテンツをデコードして映像を再生し、画質の評価を行った。

図 3 に、オリジナル画像、図 4 に、スクランブル効果制御を加えた画像を示す。表 1 に、評価したコンテンツの符号化パラメータと暗号化パラメータを示す。図 4 の画像は、ブロック C と D の復号鍵である Key C と Key D を含むライセンスを所持している場合を示している。つまり、ブロック A と B が暗号化されている時の画質を示している。映像を劣化させながらも、ある程度番組内容を把握できる映像となっている。これは、効果制御用スライスとして付加したスキップトマクロブロックによる効果であり、暗号化されている領域でも、その周りの映像に近いものが表示されるためである。

一方、本方式では、スライスを暗号化する際に、効果制御用のスライスデータと暗号化情報を付与するため、暗号化によりコンテンツのデータ量が増加する。12 本のスライスで構成されるコンテンツを暗号化した場合、コンテンツのデータ量は、約 2%増加する。しかし、ダウンロード型放送においては、データ量の増加により伝送の所要時間が若干長くなるだけなので、問題とならない。

5. まとめ

H.264/AVC 符号化コンテンツに適用でき、画質制御のための処理量が非常に小さく、コンテンツ再生時に多段階で画質制御可能なスクランブル効果制御方式を提案した。今後は、本方式の有効性を示すために、劣化映像の主観評価実験を行っていく。

【参考文献】

[1]電波産業会:“デジタル放送におけるアクセス制御方式標準規格,” ARIB STD-B25 (2006)
[2]矢ヶ崎ほか:“次世代動画像符号化方式MPEG-4 AVC/H.264,” トリケップス(2004)
[3]勝田ほか:“圧縮画像に適したディジタルスクランブルの一方式,” 信学技報ISEC92-59(1992)

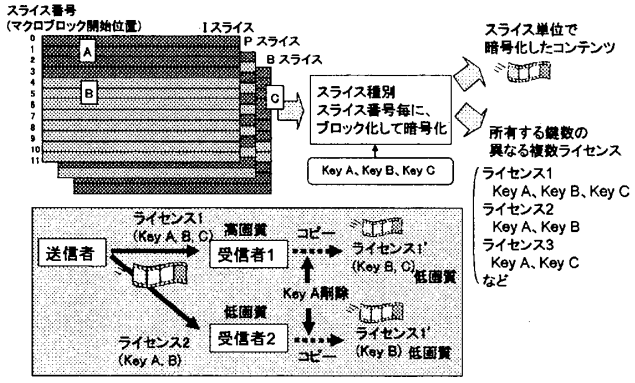

図 1 暗号化による画質制御技術

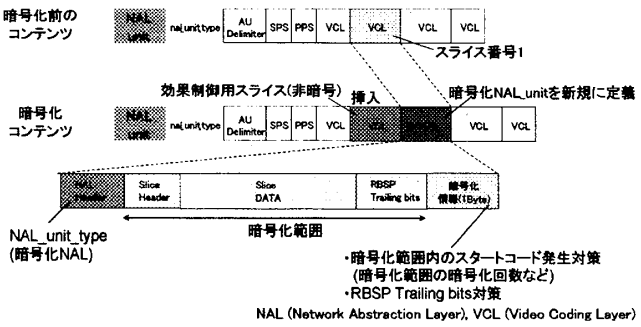

図 2 スライスの暗号化技術

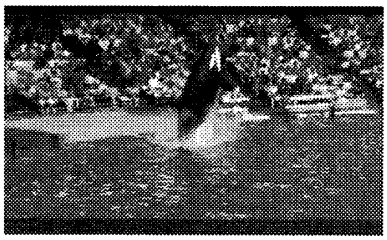

図 3 オリジナル画像

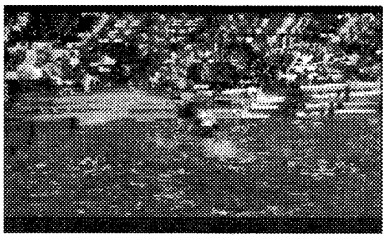

図 4 スクランブル効果制御を加えた画像

表 1 評価コンテンツのパラメータ

評価映像		ITE HDTV 標準画像 (番号 16 Whale show)
H.264/AVC符号化	プロファイル	Main Profile
	レベル	1.2
	画像サイズ	320×180
	スライス数	12
	フレームレート	15 [fps]
	スライス種別	I、P、Bを含む
暗号化	共通鍵暗号	AES, 鍵長256bit
	スライス[0～11まで]のブロック化	・ブロックA スライス番号が5のBスライスを KeyAで暗号化 ・ブロックB スライス番号が偶数のPスライスと スライス番号が1,3,7,9,11のBスライスを KeyBで暗号化 ・ブロックC 全Iスライスを KeyCで暗号化 ・ブロックD スライス番号が奇数のPスライスと スライス番号が偶数のBスライスを KeyDで暗号化