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

2006－DPS－126（9）
2006－CSEC－32（9）
2006／3／16

電子指紋により不正複製を抑止するインターネット放送システム

大西 宏樹 *1　　上原 哲太郎 *2　　佐藤 敬 *3　　山岡 克式 *4

*1 京都大学大学院工学研究科　　*2 京都大学学術情報メディアセンター
*3 北九州市立大学国際環境工学部　　*4 東京工業大学大学院理工学研究科

概要

インターネットの広帯域化に伴い，インターネット放送サービスが開始されている．本論文では同時視聴者数が数万人規模の有料インターネット放送システムを対象とし，コンテンツ保護のための電子指紋について考察した．fingerprint 系列としては，結託に対して耐性のある TA 符号を選択した．コンテンツは配信側でスクランブルされ，受信側で元に戻す．しかしながら，一部スクランブルされたままとし，その位置情報を fingerprint とする．このように配信側と受信側が一体となって fingerprint を埋め込むことにより，ユーザが fingerprint が埋め込まれていないコンテンツを入手できなくすることができる．また，提案手法を電子指紋に適用した放送システムを実装し，動作を確認することにより実用性を示した．

Internet Broadcasting System with Fingerprint for Detterrence of Unauthorized Duplication

Hiroki Onishi*1　　Tetsutaro Uehara*2　　Takashi Satoh*3　　Katsunori Yamaoka*4

*1 Graduate School of Engineering, Kyoto University
*2 Academic Center for Computing and Media Studies, Kyoto University
*3 Faculty of Environmental Engineering, The University of Kitakyushu
*4 Graduate School of Science and Engineering, Tokyo Institute of Technology

abstract

Internet-based content distribution systems are now providing new business opportunities. Given this background, this paper discusses the fingerprinting, which act as a psychological deterrent to illegal copying and distribution of copyrighted contents. As a fingerprint code, this paper assumes the use of TA code because it is superior in term of tolerance for collusion. We also present fingerprinting method to prevent leakage of content that has not yet had watermarks embedded. In proposed method, content are scrambled at the server and are descrambled at the receiver. However, some are left scrambled. The scrambled positions in the content constitute the fingerprint. Implementation of an application system is also described. We demonstrate that an Internet-based pay broadcasting system can be implemented efficiently using proposed fingerprinting to protect copyrighted contents.

1　はじめに

近年インターネットは広帯域化が進んでおり，音楽や映像などのコンテンツを提供するビジネスがインターネットを介して実現されるようになってきている．一方現在，人々の嗜好の多様化によりテレビなどは多チャンネル化が進んでおり，1 チャンネルあたりの視聴者数が減少している．よって，今後は広告収入により無料の放送ビジネスを行うことは困難になると予想され，インターネット放送においては有料放送が中心となると思われる．

このような背景により，本論文ではインターネット有料放送システムについて考察した．特に，放送ビジネスにおいて大きな問題となる，コンテンツを保護する仕組みについて考察した．サーバとクライアントが一体となってコンテンツに電子指紋を埋め込む手法を提案し，これにより不正コピーを抑止できることを示す．また，実際に放送システムを構築し，評価することによりその実用性を示す．

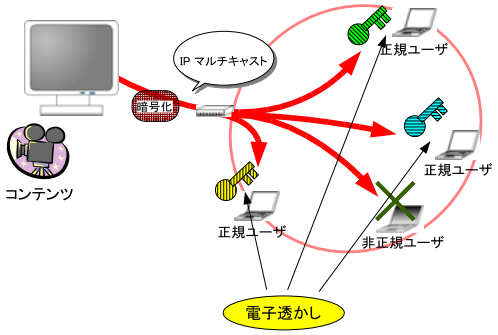

図 1　システムのモデル

2　対象とする放送システム

ここでは，本論文が対象とするインターネット放送システムについて述べる．

2.1　ユーザ数とコンテンツの種類

現在のインターネット放送は主に 1 対 1 のユニキャストによる通信のため，例えば数万人のような多数のクライアントが同時に同一のコンテンツを見るためには，サーバを冗長化，分散化する必要があり，コンテンツ配信者に大きな負担となる．本論文では既存のインターネットインフラストラクチャを用い，コンテンツ配信者に負担をかけることなく，数万人のユーザが同時に同一のコンテンツを視聴可能なシステムを目指す．また，本システムで配信するコンテンツは動画像や音声といったストリーム通信向けのデータとし，ライブ放送に対応できるシステムとする．

2.2　セキュリティ

有料コンテンツ放送ビジネスを実現するためには，受信を制限すること，受信後のコンテンツの複製を制限することが必須である．受信の制限は文献 [1] の考察より文献 [2] のユーザ認証方式により実現するとし，本論文ではコンテンツ複製の制限に焦点を当てる．

デジタルコンテンツはいくらコピーしても品質が劣化しないという特徴があり，容易に不正コピーされてしまうリスクを負っている．そこで，著作権の保護，主張，不正コピーの防止といったことが必要となる．このような問題を解決する手段として電子透かし [3] が有効である．

2.3　システムのモデル

我々の想定するシステムを図 1 に示す．課金を行った正規ユーザには予め鍵を配布しておく．セッションが開始すると，コンテンツサーバはコンテンツをリアルタイムに処理しながら，暗号化して IP マルチキャストにより配信する．正規ユーザは鍵を用いてコンテンツを復号・再生する．その際，コンテンツには電子透かしが埋め込まれる．

3　不正複製抑止方式

ユーザ認証を用いることで，鍵の不正な受け渡しは抑止できる．しかしながら，正規ユーザが受信したコンテンツを不正コピーし，流用することを防ぐことはできない．そこで，本システムではコンテンツ作成者の署名を埋め込む電子透かし (watermarking) と，受信者のユーザ情報を埋め込む電子透かし (fingerprinting) の 2 種類の電子透かしをコンテンツに埋め込む．本論文では watermarking に関しては既存方式を適用するとし，以下では fingerprinting について考える．

3.1　本システムにおける電子透かしの要件

一般に電子透かしは，頑健であること，知覚的にほとんど変化しないことが要求される．これに加えて，本システムではライブ放送への対応や，再生しながらの埋め込みを考えているためリアルタイムに電子透かしを埋め込むことができる必要がある．また，動画像においては，今日の放送番組が最低でも数分以上であることを考慮し，キャプチャした静止画像や 1 分以内の短い動画像といったものには価値がないと考え，1 分以上の動画像には電子透かしが埋め込まれていることを必要とするが，それより短い動画像に対してはなんの保証もなくてもよいと考える．また，fingerprinting では埋め込み後のコンテンツにユーザごとに異なる部分が発生する．そのため，ユーザ間の比較によって埋め込み箇所が判明する可能性があるが，これに対処する必要がある．

3.2　fingerprint 系列の選択

ここでは，本システムが埋め込むユーザ情報，すなわち fingerprint 系列について述べる．

3.2.1　結託耐性のある符号

結託に対して耐性のある fingerprint を埋め込むために，各ユーザの fingerprint 系列を符号語として表現する手法がいくつか提案されている [4][5][6] .

文献 [4] では c-secure frameproof codes(以下 SFP 符号) という 2 元符号が提案された．c-SFP 符号では，c 人以下の相異なる 2 つの結託者集合は同一の符号語を生成することができない，という性質を持つ．SFP 符号を用いることで，結託により無実のユーザが罪を着せられることを防ぐことができ，また，結託により生成された符号語から不正者をある範囲に限定可能である．文献 [5] では次のことが証明されている．

> c を 2 以上の整数とする．$\gcd(2d+1,(c^2)!)=1$ である $d>c$, 任意の j に対して, 符号長 $2\binom{2d-1}{d-1}\cdot(c^2+1)^j$, 符号語数 $(2d+1)^{2j}$ である c-SFP 符号が存在する．

また，文献 [6] では w-traceability codes (以下 TA 符号) という q 元符号が提案された．結託により生成可能な系列は，その i 番目の値を結託に関わったユーザの系列の i 番目の値から選択することにより生成可能な系列とする．この場合に，TA 符号では結託により生成された符号語から結託に関わった符号語を少なくとも 1 つ特定することができる．文献 [6] では次のことが証明されている．

> N,q,w が与えられ，q は素数であり，$N\leq q+1$ であ

るとする．このとき，$n = q^{\lceil N/w^2 \rceil}$ である符号長 N，符号語数 n，アルファベット q の w 人までの結託に耐える TA 符号が存在する．

TA 符号を 2 元系列である fingerprint 系列とするには，TA 符号での q 元の値 i を q 個のビット値で表現し，その $i+1$ 番目の値を 1，その他を 0 とすればよい．

3.2.2 符号の選択

本論文が前提としている 1 万人以上のユーザをサポートすることができ，1 分以内の動画像に fingerprint を埋め込み可能な符号とすることを考える．すなわち，符号語数を 1 万語以上とする．また，後に提案する fingerprinting は I フレームの 1 ブロックに 1 ビット埋め込むことから，1 分間の動画像における I フレームのブロック数を考え，符号長は 216000 以下とする．この条件で最も結託に耐えることができる符号とすると，それぞれ 3-SFP 符号，21-TA 符号となる．ただし，TA 符号は q 元符号を 2 元符号として扱っており，結託により生成可能な系列には，先に述べたように前提がある．その条件を前提にするならば，結託に関わったユーザを少なくとも 1 人追跡可能である．その条件を前提にしなければ，frameproof ではあるが，結託攻撃により fingerprint が消える可能性がある．しかしながら，21-TA 符号は，3 人までの結託であれば不正者をある範囲に限定可能であり，3-SFP 符号よりも優れていると考えられる．

次に，fingerprint が埋め込まれた動画像の画質について考える．TA 符号の符号語は 0 が多く，SFP 符号は 0 と 1 がほぼ同じである．後で述べる fingerprint を埋め込むことを考えると，0 が多いほど画質が向上するため，TA 符号の方が優れていると考えられる．

以上より，fingerprint 系列として TA 符号を選択する．

3.2.3 w-TA 符号

ここでは本論文で適用する，w 人までの結託に耐えることが可能である w-TA 符号と呼ばれる符号の定義とその生成方法について述べる．なお，本項では符号長 N，アルファベット Q，ただし $|Q| = q$ である符号を C とする．

TA 符号を定義するにあたり，任意の部分集合 $C_0 \subseteq C$ に対して，$\mathbf{desc}(C_0)$ と表される以下の符号語の集合を定義する．

$$\mathbf{desc}(C_0) = \{x \in Q^N : x_i \in \{a_i : a \in C_0\}, 1 \le i \le N\}$$

$\mathbf{desc}(C_0)$ は集合 C_0 の符号語から生成することが可能な符号語の集合である．そして，w-TA 符号は次のように定義される．

定義 3.1. $w \ge 2$ を整数とし，符号 $C_i \subseteq C, i = 1, 2, \cdots, t$ を $|C_i| \le w$ とする．また，任意の $x, y \in Q^N$ に対して，$I(x,y) = \{i : x_i = y_i\}$ を定義する．すべての i，$x \in \mathbf{desc}(C_i)$ に対して，任意の $z \in C \backslash C_i$ において $|I(x,y)| > |I(x,z)|$ となる符号語 $y \in C_i$ が少なくとも一つ存在するとき，符号 C は w-TA 符号という．

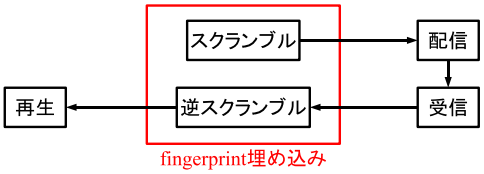

図 2　fingerprint 埋め込み手法

w-TA 符号は，次元 $t = \lceil N/w^2 \rceil$ の q 元リードソロモン符号として生成することができる．また不正者の追跡は，不正に生成された符号語を x，C を TA 符号としたとき，$c_i \in C$ の中で $|I(x, c_i)|$ が最大となる c_i を求めればよい．

3.3 提案する fingerprinting

3.3.1 埋め込みに関する考え方

fingerprinting 手法として，ユーザが鍵を用いてコンテンツを復号し，直ちに fingerprint を埋め込む手法がある．この手法では fingerprinting の処理をスキップすることで，fingerprint の埋め込まれていないコンテンツを入手される危険性がある．これを防ぐため，文献 [7] に提案されている以下の手法と同様の手法を用いる．

> コンテンツは鍵 K_{SSK}(Server Scramble Key) を用いてスクランブルすることにより，ぼやけた動画像として配信する．受信側ではユーザごとに固有の鍵 K_{CSK}(Client Scramble Key) を用いてスクランブルを元に戻す．しかしながら，$K_{\mathrm{SSK}} \neq K_{\mathrm{CSK}}$ であるため，いくつかの部分はスクランブルされたまま残る．このスクランブルされたままの位置情報が fingerprint となる．これを図 2 に示す．

この手法を用いることで，fingerprint の埋め込みをスキップしたとしても得られるコンテンツはぼやけた動画像であり，コンテンツとしての価値は低下するため，そのような攻撃に対して大きな効果がある．また，スクランブルされたコンテンツを著しく乱れたものとすることができたならば，暗号化としての意味を持つことになる．また，コンテンツ復号と fingerprint 埋め込みの処理を同時に行うことが可能となり，それぞれの処理を別個に行う場合に比べ高速な処理が期待できる．

3.3.2 提案手法

本システムではライブ放送などリアルタイムに処理しながらコンテンツを MPEG 圧縮して配信することを前提としている．そこで，fingerprint 埋め込みの処理速度を向上させるために，コンテンツサーバでは MPEG 圧縮の過程でスクランブル処理を，クライアントでは MPEG 伸長の過程で逆スクランブル処理を行う．MPEG 圧縮ではフレームを 8×8 画素 のブロックに分割し，DCT を施した後，量子化を行う．スクランブル，逆スクランブルはこの量子化を行った後の DCT 係数の内，DC 係数を除いた

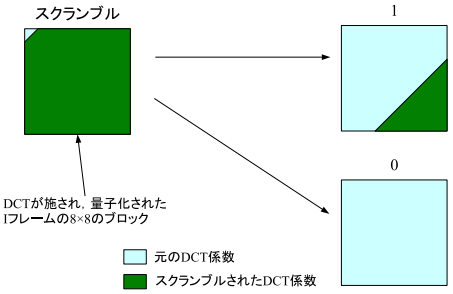

図 3　提案する fingerprinting の概念図

AC 係数に対して行う．ただし，スクランブルの対象は I フレームのみとする．また，動画像の長さの許す限り繰り返し fingerprint を埋め込む．

本システムでは，スクランブルされた動画像は品質が大きく低下し，fingerprint が埋め込まれた動画像は一定以上の品質が保たれていることを目指す．これを，スクランブルを施す周波数領域を変化させることで実現する手法を提案する．量子化後のブロックを 1 単位とし，スクランブルはブロックの AC 係数全体に施す．fingerprint 系列として 1 を埋め込むには低・中周波数成分のスクランブルを元に戻す．fingerprint 系列として 0 を埋め込むには全周波数成分のスクランブルを元に戻す．これを図 3 に示す．

3.3.3　SSK，CSK の生成

K_{SSK}，K_{CSK} は fingerprint 系列の長さを N として，N 個の鍵の集合と考えることができる．以下，K_{SSK}，K_{CSK} それぞれの i 番目の鍵を $K_{\mathrm{SSK},i}$，$K_{\mathrm{CSK},i}$ と表し，fingerprint 系列の i 番目の値を $K_{\mathrm{FP},i}$ と表す．fingerprint を埋め込むには，次のようにすればよい．$K_{\mathrm{FP},i}=1$ ならば $K_{\mathrm{SSK},i}\neq K_{\mathrm{CSK},i}$ とし，$K_{\mathrm{FP},i}=0$ ならば $K_{\mathrm{SSK},i}=K_{\mathrm{CSK},i}$ とする．ただし，$K_{\mathrm{SSK},i}\neq K_{\mathrm{CSK},i}$ である場合においても，低・中周波数成分に対応する部分は同一とする．

3.3.4　スクランブル・逆スクランブル

コンテンツサーバでは K_{SSK} に従って，DCT 係数をスクランブルする．ただし，MPEG のジグザグスキャン順で閾値以降の DCT 係数がすべて同一である場合は意味を成さないため，そのブロックはスクランブルは施すが fingerprint が埋め込まれないブロックとなる．クライアントでのスクランブルを元に戻す処理はサーバでのスクランブル処理と逆の処理とする．こうして，所望の fingerprint を埋め込むことができる．

3.3.5　fingerprint の検出

クライアントで MPEG 伸長された非圧縮動画像と，原動画像を用いて行う．それぞれ MPEG 圧縮時と同様に，1 フレームをブロック分割，DCT，量子化を行う．この量子化を行った後の DCT 係数について 2 つの動画像の間で比較する．スクランブルされているならば，そのブロックに対応する fingerprint の値を 1，原動画像と一致しているならば，そのブロックに対応する fingerprint の値を 0 とする．また，一定時間以上の動画像では，同一の fingerprint が繰り返し埋め込まれている．そこで，検出された fingerprint 系列をビットごとに多数決とることにより検出確率を上げる．

4　fingerprinting の実装と評価

提案手法を評価分析するため，fingerprint の埋め込み処理と検出処理を実装した．

4.1　fingerprinting の実装

実験には，TV 放送よりキャプチャしたサイズ 320 × 240 画素の RGB 形式の動画像を用いた．再生時間 60.00 秒，1799 フレーム，405 メガバイトである．

fingerprint 系列としては，3.2.3 項で述べた TA 符号を用いる．$w=10, n\geq 10000$ を満たすという条件で N,q を探索した結果，$N=101, q=103$ とした．103 元リードソロモン符号は符号長 102 となるが，TA 符号としては各符号語について最後の一つを除いた長さ 101 の系列とする．fingerprint 系列へ変換すると，系列の長さは $101\times 103=10403$ となる．

K_{SSK}，K_{SSK} のサイズを小さくするため，$K_{\mathrm{SSK},i}$，$K_{\mathrm{CSK},i}$ は 1 ビット値とした．K_{SSK} は乱数により生成し，K_{CSK} は K_{SSK} と K_{FP} の排他的論理和とする．

スクランブル処理は，MPEG のジグザグスキャン順である特定の周波数成分までは K_{SSK} のビット値 0 と 1 に関わらず同一のスクランブルを施し，その後の周波数成分に対しては，0 と 1 で異なるスクランブルを施す．逆スクランブル処理はサーバでのスクランブル処理と逆の処理とする．このようにすることで，$K_{\mathrm{SSK}}=K_{\mathrm{CSK}}$ であればスクランブルが元に戻るが，$K_{\mathrm{SSK}}\neq K_{\mathrm{CSK}}$ であれば後半部分がスクランブルされることになる．

検出は fingerprint が埋め込まれた動画像と原動画像それぞれについて，量子化を行った後の DCT 係数をテキストファイルとして書き出し，その 2 者間で比較することにより行う．

4.2　fingerprinting の評価

実装した fingerprinting を評価するために行った実験結果と考察・評価を述べる．以下では，MPEG1 圧縮された動画像を MPEG 動画像，スクランブル処理を行った動画像をスクランブル動画像，fingerprint が埋め込まれた動画像を埋め込み動画像と呼ぶ．

4.2.1　実験結果

原動画像に対してサンプルレート 400 kbps と 1500 kbps で MPEG 圧縮，スクランブル，逆スクランブル処理を行った．図 4 に原動画像を，図 5，6 に実験により得られた動画像をキャプチャした画像を示す．

基準となるデータとして，MPEG 動画像の PSNR(信号対雑音比) を測定したところ，400 kbps で 37.64dB，1500kbps で 43.26dB となった．次に，fingerprint 系列が 1 の場合にどの程度の周波数までスクランブルを元に戻す

図 4　原動画像

図 5　埋め込み動画像 (上) とスクランブル動画像 (下) (400kbps, partition = 5)

図 6　埋め込み動画像 (上) とスクランブル動画像 (下) (400kbps, partition = 45)

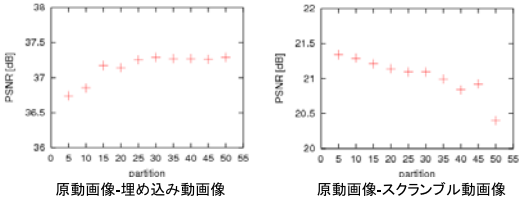

図 7　PSNR 測定結果 (400kbps)

のが望ましいかを判断するため，スクランブルを元に戻す周波数領域を変化させ，埋め込み動画像とスクランブル動画像の PSNR を測定した．結果を図 7，8 に示す．なお，fingerprint 系列が 1 の場合にスクランブルされたままとなる DCT 係数の範囲を表すのに，partition と呼ばれる変数を用いた．partition は MPEG のジグザグスキャン順で partition 番目以降の DCT 係数がスクランブルされたままとなることを示す．

また，同一の fingerprint を繰り返し埋め込んでいるが，何回繰り返し fingerprint の埋め込みが行われたかを測定した．結果を図 9 に示す．

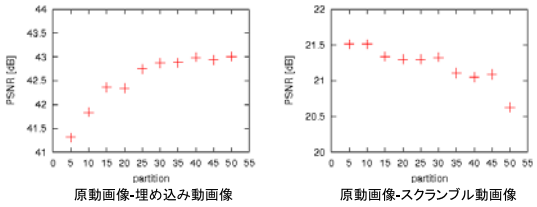

図 8　PSNR 測定結果 (1500kbps)

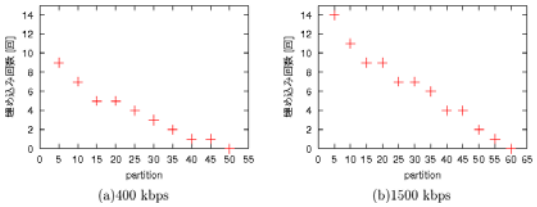

図 9　fingerprint 埋め込み回数

fingerprint が埋め込まれた動画像について，検出処理を行った．埋め込み動画像に対して何も攻撃をしなければ，正しく検出することができた．

4.2.2　評価・考察

主観的評価である見た目の点から評価する．埋め込み動画像は，fingerprint 系列が 1 である部分は高周波成分がスクランブルされたままとなっている．400 kbps では partition $\leq$ 30，1500 kbps では partition $\leq$ 40 である場合に，ブロックノイズが目についた．これは，fingerprint が埋め込まれている位置を判断することができることを意味し，望ましくない．400 kbps では partition $\geq$ 35，1500 kbps では partition $\geq$ 45 であれば，見た目には分からない．

次に，客観的評価である PSNR の点から評価する．スクランブル動画像では partition を大きくするほど PSNR が悪くなり，埋め込み動画像では partition を大きくするほど PSNR が良くなっている．一般的に，PSNR が 40dB 以上であれば視覚的には劣化がほとんど分からなくなるといわれており，スクランブル動画像では 40dB を下回り，埋め込み動画像では 40dB を上回ることが望まれる．1500kbps ではこの条件は満たされているが，400kbps では埋め込み動画像の PSNR が 40dB を下回っている．しかしながら，埋め込み動画像の PSNR の落ち込みは MPEG 動画像に対して 1dB 以内であり，問題はないと思われる．

最後に，同一の動画像に対して fingerprint 系列が何回埋め込まれたかという点で評価する．当然ながら partition を大きくするほど回数は減少している．400kbps では partition $\leq$ 45，1500kbps では partition $\leq$ 55 であれば 1 分の動画像に対して fingerprint を埋め込むことが可能であることが分かった．

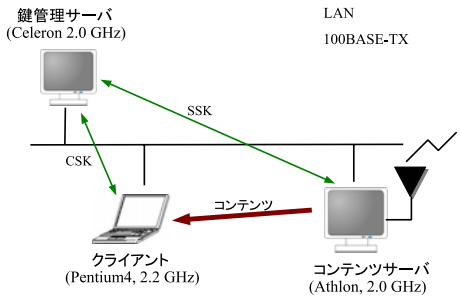

図 10　実装したシステム

以上より，提案手法は 400kbps では $35 \leq$ partition ≤ 45，1500kbps では $45 \leq$ partition ≤ 55 とすることで要件を満たすことが分かった．その範囲で用途に応じて partition の値を設定すればよい．

5　システムの実装と評価

提案手法を電子指紋として適用したインターネット有料放送システムを試作した．

5.1　システムの実装

実装したシステムを図 10 に示す．コンテンツを配信するコンテンツサーバ，受信再生するクライアント，鍵の管理を行う鍵管理サーバから構成され，PC 上でソフトウェアのみを用いて放送・再生するシステムとする．運用実験としては京都大学内の LAN 環境をそのまま利用した．

コンテンツはテレビ放送をそのまま利用し，サンプルレート 400 kbps，ネットワーク上で 650 kbps で配信した．コンテンツサーバではテレビ放送をキャプチャし，SSK に基づきスクランブル処理を行い，誤り訂正による制御データを追加し，IP マルチキャストにより配信する．クライアントではコンテンツを復号し，CSK に基づきスクランブルを取り除き，再生する．

TA 符号のパラメータは $N = 101$，$q = 103$，$w = 10$ とした．また，第 4 章の結果をふまえて partition の値を 35 とした．

5.2　システムの評価

SSK・CSK のサイズは共に 10403 bits となる．コンテンツ配信者に比べコンテンツ受信者の方が大幅に多いことから，CSK の配布についてのみ考えると，全ユーザに CSK を配布する場合で約 13 MBytes となる．現在一般に存在する通信速度が 10Mbps の Web サーバで 15 秒以内に送信可能なことや，CSK の配布は時間的に分散されることからこの程度のデータ量であれば問題ないと考えられる．

先に述べたシステムを実際に動作させたところ，サンプルレート 800 kbps 以内であれば複数台の PC から同時に同一のコンテンツを視聴することができ，リアルタイムに動作することが確認された．以後は 650 kbps で配信した結果について述べる．CPU 使用率はコンテンツサーバ (Athlon 2 GHz, 主メモリ 1 GB) で 62%，クライアント (Pentium4 2.2 GHz, 主メモリ 1 GB) で 6% であった．また，ネットワーク上でのパケットの欠落についても調べたが，同一 VLAN での運用ということもありほとんどパケット落ちは見られなかった．長時間連続で運用するとクライアントプログラムで単独の 1 パケットもしくは連続する 2 パケットの欠落が見られたが，これは誤り訂正符号により補完されていることが確認できた．

6　結論

有料インターネット放送を対象とし，コンテンツ保護のための電子指紋について考察した．

埋め込む fingerprint 系列について，結託に対する耐性や fingerprint として埋め込む場合の画質の面などから比較検討し，TA 符号が最も本システムに適していることを示した．また，TA 符号を fingerprint として埋め込むために，配信側と受信側で一体となって実現する電子透かしを提案した．そして，画質の面や埋め込みに必要なフレーム数の面から評価した．

提案手法を適用した有料インターネット放送システムのプロトタイプを実装し，運用実験によりそのシステムの実用性を示した．

参考文献

[1] 大西 宏樹, 上原 哲太郎, 佐藤 敬, 山岡 克式, IP マルチキャスト映像放送システムのためのユーザ認証方式に関する検討, 2005 画像電子学会年次大会予稿集, (2005), pp. 181–182.

[2] Y. Dodis, N. Fazio, A. Kiayias, and M. Yung, Scalable Public-Key Tracing and Revoking, *Principles of Distributed Computing*, (2003), pp. 190–199.

[3] 小野 束, 電子透かしとコンテンツ保護, オーム社, (2001).

[4] D. Boneh and J. Shaw, Collusion-Secure Fingerprinting for Digital Data, *Lecture Notes in Computer Science*, Vol. 963, (1995), pp. 452–465.

[5] D. R. Stinson, T. van Trung, and R. Wei, Secure Frameproof Codes, Key Distribution Patterns, Group Testing Algorithms and Related Structures, *Journal of Statistical Planning and Inference*, Vol. 86, (2000), pp. 595–617.

[6] J. N. Staddon, D. R. Stinson, and R. Wei, Combinatorial Properties of Frameproof and Traceability Codes , *IEEE Transactions on Information Theory*, Vol. 43, (2001), pp. 1042–1049.

[7] D. Kundur and K. Karthik, Video Fingerprinting and Encryption Principles for Digital Rights Management, *Proceedings of the IEEE*, Vol. 92, (2004), pp. 918–932.