情報処理学会論文誌 Vol.55 No.1 300–310 (Jan. 2014)

コンテンツ保護機構を備えたインターネット生放送システムの実現可能性の評価

津田 侑[1,a)] 黄 亮錦[2] 森村 吉貴[3] 侯 書会[4] 上原 哲太郎[5] 上田 浩[6]

受付日 2013年4月10日, 採録日 2013年10月9日

概要：インターネット上でのユーザ間の情報共有は CGM と呼ばれるユーザ主体の情報発信基盤を通じて文字，写真，動画など様々な形で行われている．その中でもインターネット生放送は情報を映像とともにリアルタイムに伝える手段として注目を集めている．本論文ではユーザが創造したコンテンツを保護しつつ情報を発信できるインターネット生放送システムを提案しそのプロトタイプを構築した．そして，そのプロトタイプを用いて操作性，映像の品質，コンテンツ保護の効果の 3 つの項目を評価するために被験者実験を実施した．操作性では 83.3%の被験者から高い評価を得られた．映像の品質は画質，音質，映像と音声の同期性の 3 つの指標でそれぞれ 70%以上の被験者から高い評価を得られた．コンテンツ保護の効果では 100%の被験者に映像の視認性について効果が見られた．また，94.4%の被験者から映像の横流しに対する抑止力があるという評価を得た．

キーワード：インターネット生放送，消費者生成メディア（CGM），コンテンツ保護，暗号化，電子指紋

A Feasibility Study of an Internet Live Broadcasting System with Contents Protection

Yu Tsuda[1,a)] Liangjin Huang[2] Yoshitaka Morimura[3] Shuhui Hou[4]
Tetsutaro Uehara[5] Hiroshi Ueda[6]

Received: April 10, 2013, Accepted: October 9, 2013

Abstract: Information sharing among internet users has many formats on services which information is created by users called CGM; for instance, letters, pictures, movies and so on. Among the CGM services, internet live broadcasting has attracting attention as the service for broadcasting movie and voice in real time. In this paper, the authors proposed an internet live broadcasting system for protecting users' unique contents and implemented the prototype system. Thus, the authors evaluated the system by subjective experience about three points; usability, quality of contents and efficiency of contents-protection methods. In result, of the 18 examinees, 15 (83.3%) highly valued about usability. About quality of contents, more than 70% highly evaluated in quality of movie, sound, and synchronism between movie and sound. Furthermore, contents protection effective on all examinees. In addition, of the 18 examinees, 17 (94.4%) highly valued against contents piracy.

Keywords: internet live broadcasting, consumer generated media (CGM), contents protection, encryption, digital fingerprinting

[1] 独立行政法人情報通信研究機構サイバー攻撃対策総合研究センター
Cybersecurity Research Center, National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan
[2] 京都大学大学院情報学研究科
Graduate School of Informatics, Kyoto University, Kyoto 606–8501, Japan
[3] 京都大学物質–細胞統合システム拠点
iCeMS, Kyoto University, Kyoto 606–8501, Japan
[4] 北京科技大学信息与計算科学系
Department of Information and Computing Science, University of Science and Technology Beijing, Haidian District, Beijing, 100083, P.R. China
[5] 立命館大学情報理工学部
College of Information Science and Engineering, Ritsumeikan University, Kusatsu, Shiga 525–8577, Japan
[6] 京都大学学術情報メディアセンター
Academic Center of Computing and Media Studies, Kyoto University, Kyoto 606–8501, Japan
[a)] tsuda@nict.go.jp

1. はじめに

インターネットの普及により，人々は単なる情報の消費者から発信者へと変化しつつある．ブログや写真・動画の投稿サイトといったWebサービスが手軽に利用できるようになったことにより，今までコンテンツを受信することが主体であったユーザの一部は，自らコンテンツを生成し発信する側に変化してきた．このようにユーザ主体となってコンテンツを生成していくメディアは消費者生成メディア（CGM: Consumer Generated Media）と呼ばれている．

CGMに分類されるサービスの上で流通するコンテンツは文書，画像，動画などがあるが，その中でも2010年頃に登場した**インターネット生放送**と呼ばれるWebサービスではインターネットを介して自ら撮影した映像を生中継することができる．インターネット生放送の代表的なものとしてUSTREAM[*1]やニコニコ生放送[*2]がある．インターネット生放送を通じてコンテンツを配信するために必要な機材は一般の家電量販店で容易に購入可能なPCやWebカメラなどの機器とインターネット回線のみで，特殊な装置はいっさい使用しない．それゆえ誰でも簡単に自身の「放送局」を持つことができるため，自由にコンテンツを生放送できる基盤として多くの利用者を集めている．インターネット生放送で流通しているコンテンツのジャンルはニュースやスポーツ，音楽といった従来のテレビ放送と同様の形式の番組や，視聴者と対話しながら放送を作り上げていく視聴者参加型の番組など多岐にわたる．これらのコンテンツの中には放送者の創意工夫によって非常に高い品質に達したものも数多くあり，これらは多くの視聴者を集めている．このように，インターネット上の新たな創作活動の場としてインターネット生放送サービスは機能し始めている．

一般に，インターネット上で発信されたコンテンツは人気を博するにつれて利用者によって多くの複製が作られ，広く流通することが多い．インターネット生放送においても，一度放送したコンテンツの録画が複製されて二次流通し，多くのユーザに視聴されることがある．多くの視聴者を集めることは，放送者にとって創作活動を続けるための動機付けにつながりうる．しかし一方で，いったん複製によって広く流通したコンテンツを削除することは非常に困難である．そのため，放送中の手違いや事故によりコンテンツ内に不都合な映像が紛れ込んだ場合，これをインターネット上に複製，拡散されると放送者に不利益が生じる危険がある．このような問題は放送者当人だけでなく放送コンテンツ中に登場する人物や場所にまで影響が及ぶ可能性もある．よって，一般にインターネット生放送においても必要に応じてコンテンツの二次流通を抑止できることが望ましい．すなわち，放送者の意図に応じて視聴者を制限する機構，複製を禁止する機構や，万一二次流通した場合にコンテンツの流出経路を追跡できるようなトレーサビリティを確保するといったコンテンツ保護機構を備えることにより，放送者にとってよりコンテンツ作成を安全にし，コンテンツの作成と流通をより活発にする効果が期待できる．

我々は，放送者の創作したコンテンツの流通管理を実現し，放送者が安心・安全に利用できるインターネット生放送システムの実現を目指してきた．これまでの研究により，1) 意図しないユーザには視聴させないためのコンテンツの暗号化，2) ユーザの海賊行為を抑止するためのコンテンツトレーサビリティの確保，の2点によってコンテンツの流通を管理し，その保護を実現する手法については提案されている [1]．本論文では，提案手法が実際にインターネット生放送コンテンツの発展に資することを示すため，システムを実装するとともに被験者実験を実施する．評価項目は操作性，映像の品質，コンテンツ保護の効果の3つである．操作性の評価では従来のインターネット生放送と近い操作性を確保できているか，映像の品質の評価ではコンテンツ保護によって画質や音質が劣化しないかを評価する．これら2つの評価項目をあわせて，インターネット生放送のCGMとしての利便性を評価指標とする．さらにコンテンツ保護の効果の評価指標として，本論文では提案システムにおける映像の暗号化による映像コンテンツの内容の視認性の低下，および電子指紋による海賊行為の抑止力を評価する．

大規模な数のユーザが利用することが想定されるCGMでは通信の帯域資源や暗号化・復号の処理で使われる計算資源の評価も重要であるが，ユーザが実際にそのCGMのサービスを利用するかどうかはユーザビリティや放送されるコンテンツの品質といった主観的な評価は最も必要とされるべきことである．本論文ではユーザによる主観的な評価を基に本論文における提案システムが実世界のCGMサービスとして適用できるのかを議論する．

2. 先行研究

先行研究として森村らによりインターネット生放送のコンテンツを保護し，そのコンテンツのトレーサビリティを確保する仕組みが提案されている [1]．森村らの研究におけるコンテンツ保護は以下の2つである．

- 映像の暗号化：一部の映像フレームを暗号化することによりコンテンツを部分的に劣化させ，視聴を困難にさせる．
- 映像への電子指紋の埋め込み：視聴者固有のIDを視聴時にコンテンツに埋め込み，それを検出可能にすることでコンテンツの横流しを抑止する．

図1は森村らにより提案されたコンテンツ保護機能を備えたインターネット生放送の利用想定モデルである．放送

[*1] http://www.ustream.tv/
[*2] http://live.nicovideo.jp/

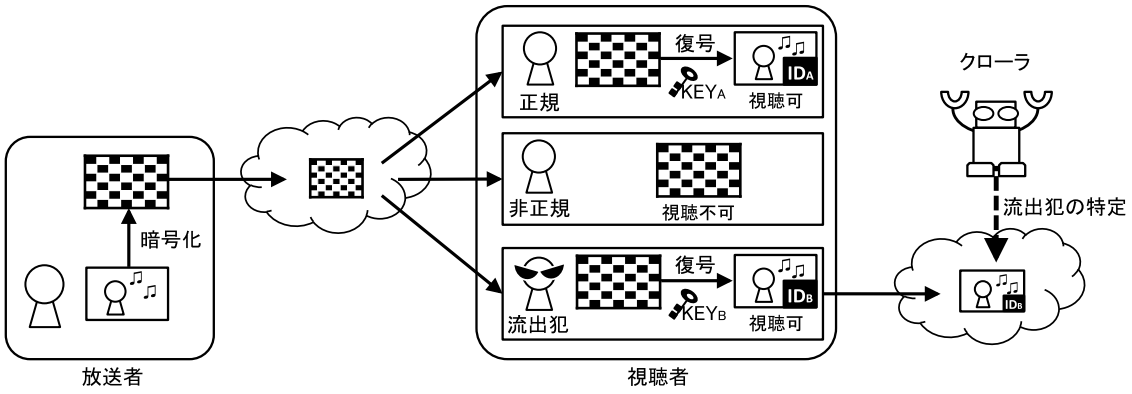


図 1 先行研究で提案されたインターネット生放送
Fig. 1 Overview of live broadcasting system proposed in previous research.

者によって暗号化され放送されたコンテンツはそのコンテンツの視聴権限がある視聴者にのみ復号可能となる．復号時には視聴したコンテンツには電子指紋としてその視聴者固有の ID が埋め込まれ，コンテンツを検査すればその視聴者を特定することを可能とする．これにより海賊行為をしてインターネットにコンテンツを横流ししようとする流出犯が現れればそれを検知するような仕組みを作ることができる．

森村らが提案したシステムでは Hou らによって提案された結託耐性符号 [2] と HomePage 暗号 [3] に基づいたコンテンツ保護手法を利用している [4]．このコンテンツ保護手法は JFD（Joint Fingerprint and Decryption）[5], [6] と呼ばれる方式を採用している．JFD を用いることによって，コンテンツの暗号化とコンテンツへの電子指紋の埋め込みを同時に行うことができる．

森村らが提案したシステムの評価実験では帯域資源と計算資源のオーバヘッドを計測し生放送に十分に適用可能であることが示された．ただし，先行研究では操作性や映像の品質を主観的に評価するような被験者実験が実施されておらず，提案したインターネット生放送が CGM の基盤として放送者の創作活動を支援できると判断できない．

また，先行研究で提案されたシステムは性能評価を目的とした実装のため，そのまま利用するためにはいくつかの既存ソフトウェアの導入や専門的な知識を必要とする．そこで本論文では森村らが提案したシステムを基に Web アプリケーションとしてインターネット生放送システムを実装する．Web アプリケーションとして実装することで，これらのソフトウェアや知識がなくても容易に視聴者や放送者が利用できるようになる．そのうえで，被験者実験を行い，提案するコンテンツ保護機能を備えたインターネット生放送の操作性，映像の品質，コンテンツ保護の効果が確保できるのかを示す．

3. 生放送映像のためのコンテンツ保護

本章では被験者実験の実施に向け，森村らのコンテンツ保護機能の実装からの変更点について述べる．本論文における実装はリアルタイム性を損なわずに被験者実験を実施するための実行性能を重視した実装である．

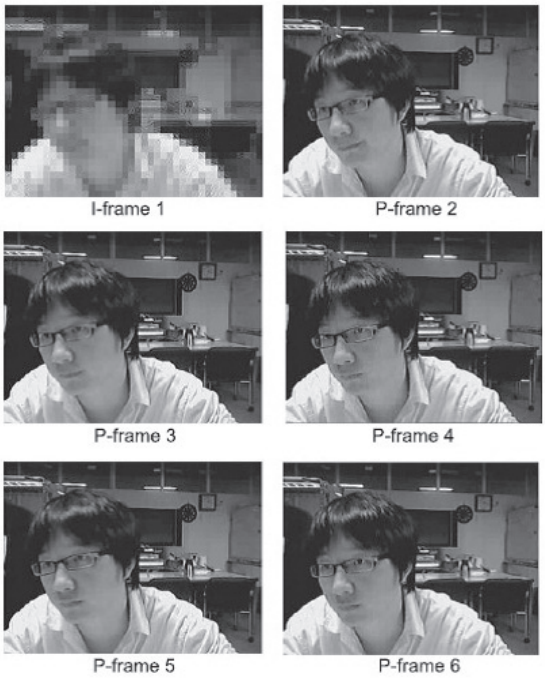
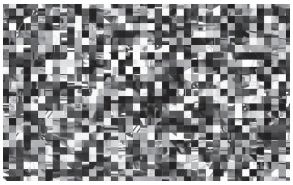


図 2 森村らのシステムで暗号化された映像フレーム
Fig. 2 Flames encrypted by the Morimura's system.

3.1 交換アルゴリズムによる映像フレームの暗号化

森村らの実装で用いられた映像の暗号化手法は，暗号化時に多少の映像の劣化はあるもののその映像の内容を判別することは容易であった．これは，MPEG 形式の映像は I フレームと複数の P フレームの組が連続することで構成されており，そのうち I フレームにのみ暗号化の処理を施しているためである（図 2）．I フレームにのみ暗号化の処理が施されることで，一定の時間間隔で映像が点滅する程度の映像の劣化にとどまる．このように内容の判別が容易であるのは，森村らの実装では放送型暗号 [7] により別途暗


(a) 未暗号化映像 (Non-encrypted)


(b) 暗号化済映像 (Encrypted)


(c) 復号済映像 (Decrypted)

図 3 コンテンツ保護を施した映像フレーム
Fig. 3 Flames encrypted by the authors' system.

号化処理を行うことを想定しているためである．

放送型暗号をインターネット生放送に適用すると，現状普及している計算機では計算資源を多く消費してしまい生放送の利点であるリアルタイム性が損なわれる可能性があるが，これは計算機の性能が向上することで将来的に解決されると考えられる．本論文では操作性の評価を行うことが主な目的の 1 つであるため，ここでは暗号化の処理は実行性能を重視した仮の実装とする．

森村らの実装からの変更点として，本論文では全フレームを暗号化することで映像の内容の判別を困難にする．これは，将来的に別途暗号化処理でコンテンツ保護が施されることを想定してユーザの行動を検証する被験者実験を実施するためである．先に述べたように放送型暗号によりコンテンツを暗号化することは現状ではリアルタイム性が損なわれる恐れがあるため，実装の軽量化を優先して交換アルゴリズム [8] を用いた映像の暗号化で代替する．暗号化前の映像（以下，未暗号化映像）を**図 3** (a) に，交換アルゴリズムにより暗号化された映像（以下，暗号化済映像）を図 3 (b) に示す．交換アルゴリズムを用いた暗号化は様々な攻撃手法が存在することで知られており堅牢な暗号化手法とはいえない [9]．その一方で，交換アルゴリズムは映像フレーム中のビット列を入れ替えて映像の暗号化を実現する軽量な手法であり，被験者実験を想定した仮の実装に適している．

この交換アルゴリズムによる暗号化は，映像フレームの色空間の形式である YUV フォーマットのうち，輝度 Y のバイト列を交換することで実現する．バイト列は映像フレームを格子状に 8 × 8 バイトの区切った単位を 1 ブロックとし，このブロックを交換する．交換リストは**図 4** の手順で生成した．

3.2 JFD を用いた映像フレームへの電子指紋の埋め込み

前節の手法で暗号化された映像を復号する際には同時に

```
procedure GenaratePermutationList
    count ← 0
    while true do
        r ← rand(BLOCK_NUM)
        temp[r] ← temp[r] + 1
        if temp[r] <= 1 then
            permutation_list[count] ← r
            count ← count + 1
            if count = BLOCK_NUM then
                break
            end if
        end if
    end while
end procedure
```

図 4 交換リストの生成アルゴリズム
Fig. 4 Algorithm for generating a permutation list.

電子指紋を埋め込む．これは視聴時に視聴者が固有に持つ ID を埋め込むことで，映像の不正な再配布といった海賊行為がされたときにその視聴者を特定可能にすることを目的としている．そしてこの機能があることを視聴者に周知することによって，海賊行為を未然に防ぐ狙いがある．

電子指紋の埋め込みには Hou らの JFD（Joint Fingerprinting and Decryption）[4] を利用する．電子指紋は交換アルゴリズムにより区切られた 8 × 8 バイトのブロックのうち任意の場所に埋め込まれる．電子指紋が埋め込まれた復号後の映像フレーム（以下，復号済映像）を図 3 (c) に示す．

4. コンテンツ保護機能を備えたインターネット生放送システムの実装

前節では被験者実験に向けたコンテンツ保護方法の改良について提案した．本章では，前節で述べた手法を森村らのシステムを基に実装したシステムの構成およびそのユーザインタフェースについて述べる．

4.1 システム構成

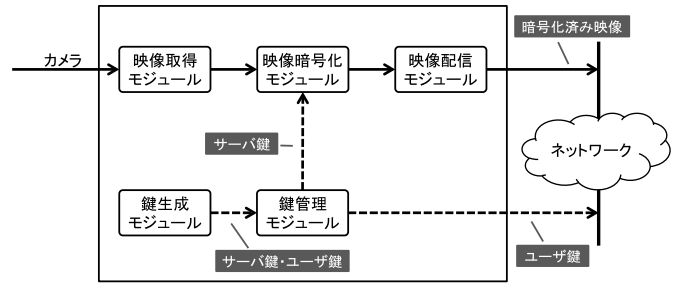
本提案システムは生放送の映像を配信するための**放送システム**と生放送の映像を受信するための**視聴システム**からなる．これらは DirectShow API [10]，Windows Media Format SDK [11] を用いた Microsoft ActiveX コントロール [12] として実装した．以下にこれら 2 つのシステムの詳細を述べる．

4.1.1 放送システム

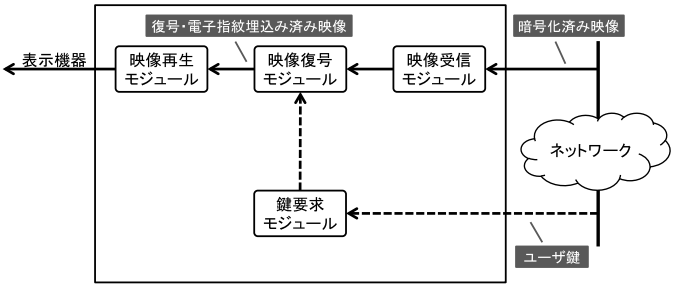
図 5 (a) に放送者が利用するシステムの構成を示す．

放送システムでは，映像の暗号化をする鍵（**サーバ鍵**）と視聴者ごとに配布される復号する鍵（**ユーザ鍵**）の組を生成，管理する鍵生成モジュールと鍵管理モジュールがある．サーバ鍵は放送システム内で利用し，ユーザ鍵は生放送の視聴者に向けて配信される．

放送者が生放送する際には，まず映像取得モジュールに



(a) 放送システム (Broadcasting system)



(b) 視聴システム (Viewing system)

図 5 コンテンツ保護機能を備えたインターネット生放送システム
Fig. 5 A live broadcasting system with contents protection.

よってカメラから映像が取得される．次にその映像は鍵管理モジュールから渡されたサーバ鍵を用いて映像暗号化モジュールで暗号化される．そして映像配信モジュールを用いてネットワーク上に暗号化された映像が配信される．

4.1.2 視聴システム

図 5 (b) に視聴者が利用するシステムの構成を示す．

視聴システムでは，鍵要求モジュールを用いて放送システムにユーザ鍵を要求する．ユーザ鍵は放送者が許可した視聴者のみ要求できる．

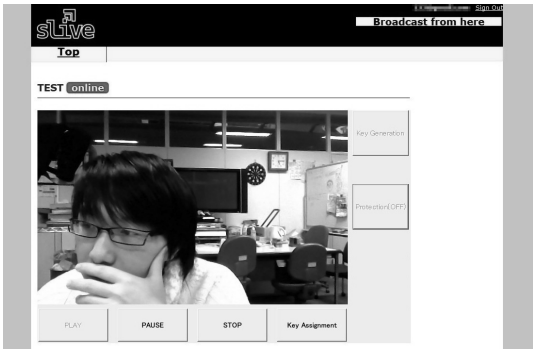
暗号化された映像は映像受信モジュールによって取得される．さきに要求したユーザ鍵を用いて映像復号モジュールで復号される．このとき復号された映像には電子指紋として視聴者を特定する ID が埋め込まれる．最後にこの映像を映像再生モジュールによって再生することができる．

4.2 Web アプリケーションとしての実装

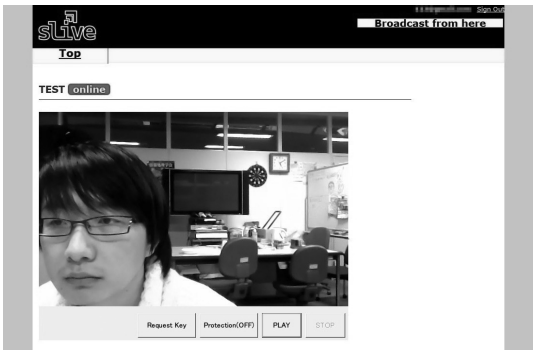
4.1 節で述べたシステムのフロントエンドは Ruby on Rails [13] を用いた Web アプリケーションとして構築した．これは広く利用されている USTREAM やニコニコ生放送が Web サービスとして提供されているためである．その画面の一例を**図 6** に示す．

また，コンテンツ保護に関する操作性を評価するため，コンテンツ保護に関わる操作のユーザインタフェースや画面遷移以外は USTREAM のものを模して作成した．

ここで，コンテンツ保護に関する操作を図 6 (a) を用いて説明する．まず，“Key Generation” ボタンを押すことでサーバ鍵を設定できる．サーバ鍵の設定完了後に “Protection” ボタンを押すことでコンテンツ保護が実施され，こ



(a) 放送システム (Broadcasting system)



(b) 視聴システム (Viewing system)

図 6 提案システムの Web インタフェース
Fig. 6 Web interfaces of the authors' system.

の後に “PLAY” ボタンを押すことで暗号化済映像を配信することができる．このとき，視聴者がユーザ鍵を所持していなければ映像を復号できない．“Key Assignment” ボタンは特定の視聴者と生成されたユーザ鍵を紐付け，ユーザ鍵を視聴者に配信する．放送者がこの操作を行うことで，視聴者はユーザ鍵を入手し暗号化済映像を復号でき，復号と同時に視聴者固有の ID が電子指紋として埋め込まれる．

5. 評価実験

本提案システムの実現可能性を評価するために評価実験を実施した．評価項目は，1) システムの操作性，2) 生放送で配信される映像の品質，3) 映像のコンテンツ保護の効果の 3 つである．本章ではその実験内容および実験結果について述べる．

5.1 実験内容

評価実験には京都大学に所属する 18 人の学生が参加した．実験は 2 人一組で行った．被験者は放送者と視聴者の役割を与えられ，それぞれの役割で本提案システムを利用する．システムの利用のために放送者には PC とヘッドホンとマイク，視聴者には PC とヘッドホンを与える．上にあげた 3 つの項目を評価するために，被験者には未暗号化映像，暗号化済映像，復号済映像の 3 種類の映像を順番に，時間は 3 分ずつ放送・視聴する．

(a) 未暗号化映像 (Non-encrypted) (b) 暗号化済映像 (Encrypted) (c) 復号済映像 (Decrypted)

図 7 実験の手順
Fig. 7 Steps of the evaluation experiment.

実験の手順を**図 7** に示す．視聴者が放送されるコンテンツの内容を判別できているかを確認するために，日本漢字能力検定[*3]の 1 級の問題に相当する難読漢字を用いた漢字の書き取り問題を放送者が出題する．出題方法は，漢字が記入された A4 サイズの用紙をカメラに向かって掲げ，放送者はその漢字の読みを発声する．視聴者は画面に表示されるコンテンツの内容を判別できれば指定の用紙に「漢字」を記入し，内容を判別できなければその「漢字の読み」を記入する．

まず, 放送者は未暗号化映像を放送し, 視聴者は図 6 (b) 中の “PLAY” ボタンを押すことでそれを視聴する（図 7 (a)）．このとき, 映像にはコンテンツ保護はいっさい施されていない状態である．次に，放送者は暗号化を施す操作をした後に放送を開始する．先ほどと同様に図 6 (b) 中の “PLAY” ボタンを押すことで視聴者は暗号化済映像を視聴することになる（図 7 (b)）．最後に視聴者は暗号化済映像を復号するための操作をする．まず，図 6 (b) 中の “Request Key” ボタンを押すことで映像を復号に必要なユーザ鍵を入手する．次に “Protection” ボタンを押した後に “PLAY” ボタンを押すことで視聴者は復号済映像を視聴する．この復号済映像には電子指紋が埋め込まれた状態となっている（図 7 (c)）．この手順がひととおり終われば 2 人の役割を入れ替えて同じ手順で本提案システムを利用する．

放送・視聴する映像の解像度は 640 × 400，フレームレートは 24 fps，ビットレートは 2,000 kbps に設定した．視聴者と放送者が使用するコンピュータは同一のサブネットに配置され，通信はユニキャストで行った．

実験終了後に評価項目を検証するためにアンケート調査を実施した．アンケート項目は付録 A.1 に示す．アンケート項目は放送担当用，視聴担当用のものをそれぞれ用意した．

5.2 実験結果

5.2.1 操作性についての評価

図 8 にコンテンツ保護に関する操作性についてのアンケート結果を示す．コンテンツ保護に関する操作はサーバ鍵の設定，特定の視聴者へのユーザ鍵の生成，コンテンツ保護の実施の 3 つで，それぞれボタンをクリックすることによって実行できる．

[*3] http://www.kanken.or.jp/kanken/

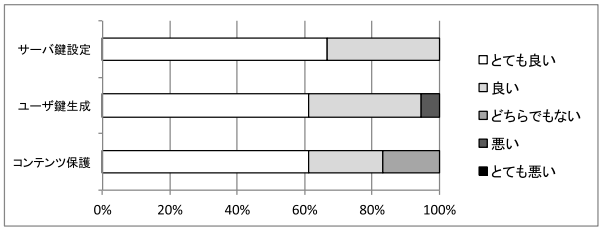
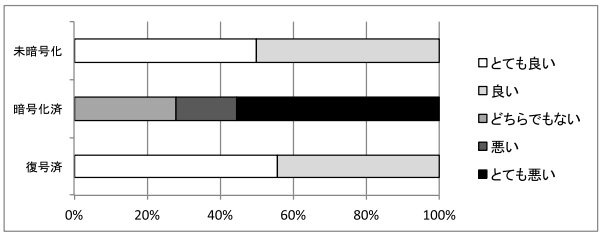
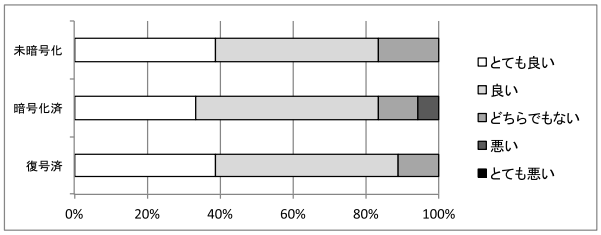


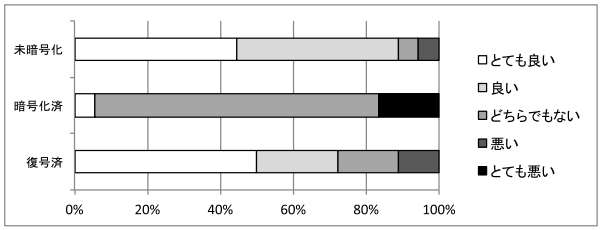
図 8 コンテンツ保護に関する操作性について
Fig. 8 Usability for contents protection.



(a) 画質 (Movie)



(b) 音質 (Sound)



(c) 映像と音声の同期性 (Synchronism between movie and sound)

図 9 生放送の映像の品質について
Fig. 9 Quality of live broadcasting contents.

サーバ鍵の設定については放送者のうち 12 人（66.7%）が「とても良い」，6 人（33.3%）が「良い」と評価し，すべての放送者が高い評価をした．ユーザ鍵の生成は 11 人（61.1%）が「とても良い」，6 人（33.3%）が「良い」と評価し，17 人（94.6%）の放送者が高い評価をしたものの，1 人の放送者のみ「悪い」と低い評価をした．コンテンツ保護の実施については 11 人（61.1%）の放送者が「とても良い」，4 人（22.2%）の被験者が「良い」と 15 人（83.3%）の放送者から高い評価を得られた．

5.2.2 映像の品質についての評価

図 9 に映像の品質についてのアンケート結果を示す．本論文での映像の品質とは画質，音質，映像と音声の同期性のことを指す．

画質については未暗号化映像は 9 人（50%）の視聴者が「とても良い」，9 人（50%）が「良い」とすべての視聴者が高く評価した．復号済映像ともに 10 人（55.6%）の視聴者が「とても良い」，8 人（44.4%）が「良い」と全視聴者が高く評価した．一方で，暗号済映像は 3 人（16.7%）の視聴者が「悪い」，10 人（55.6%）が「とても悪い」と 13 人（72.3%）の視聴者が低い評価をし，高い評価をした視聴者はいなかった（図 9 (a)）．

音質については未暗号化映像は 7 人（38.9%）が「とても良い」，8 人（44.4%）が「良い」と 15 人（83.3%）が高い評価をした．暗号化済映像については 6 人（33.3%）が「とても良い」，9 人（50%）が「良い」と 15 人（83.3%）が高い評価をし，1 人のみ「悪い」と低い評価をした．復号済映像は 7 人（38.9%）が「とても良い」，9 人（50%）が「良い」と 16 人（88.9%）が高い評価をした．暗号化・復号の処理を行わない音質については各種映像での結果の差異はほとんど見られなかった（図 9 (b)）．

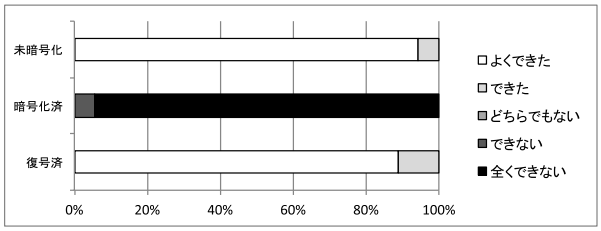
映像と音声の同期性について図 9 (c) に示す．未暗号化映像では 8 人（44.4%）が「とても良い」，8 人（44.4%）が「良い」と 16 人（88.8%）の視聴者が高い評価をしたが，1 人の視聴者のみに「悪い」と低い評価であった．暗号化済映像では 1 人（5.6%）が「とても良い」，3 人（16.7%が「とても悪い」），それ以外が「どちらでもない」と回答した．映像の視認性が下がっているため，ほとんどの視聴者が評価できなかった．復号済映像では 9 人（50%）が「とても良い」，4 人（22.2%）が「良い」と 13 人（72.2%）の視聴者が高い評価をし，2 人（11.1%）の視聴者が「悪い」と低い評価をした．

5.2.3 コンテンツ保護の効果についての評価

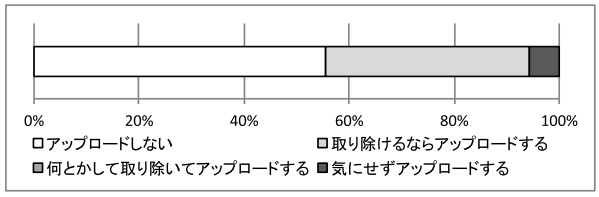
図 10 に本論文で提案した映像の暗号化および電子指紋の埋め込みによるコンテンツ保護の効果についての結果を示す．

図 10 (a) はそれぞれの映像の視認性についての結果である．未暗号化映像の内容の判別については 17 人（94.4%）の視聴者が「よくできた」，1 人（5.6%）が「できた」と回答し，全視聴者が高い評価をした．復号済映像については 16 人（88.9%）が「よくできた」，2 人（11.1%）が「できた」と回答し，未暗号化映像同様に全員の視聴者から視認性があるとの回答を得た．一方で，暗号化済映像は 1 人（5.6%）の視聴者がその内容の判別を「できない」，17 人（94.4%）の視聴者が「まったくできない」と評価し，全員が視認性がないと回答した．

図 10 (b) は映像に埋め込まれた電子指紋によって視聴者を特定できる場合にその映像をインターネット上に横流しするかどうかを質問した結果である．10 人（55.6%）の視聴者は「アップロードしない」と回答した．7 人（38.8%）の視聴者は「(電子指紋を）取り除けるならアップロードする」と回答した．そして，1 人の視聴者のみが「気にせずアップロードする」と回答した．この結果から，電子指紋を取り除くことが困難な場合に限り，17 人（94.4%）の視聴者が電子指紋の埋め込みが海賊行為の抑止に効果があることが分かった．



(a) 映像の暗号化による視認性 (Recognition of contents)



(b) 電子指紋埋込みの横流しの抑止力 (Deterrent against piracy)

図 10 生放送のコンテンツ保護の効果について
Fig. 10 Effectiveness at contents protection.

6. 考察

本章ではプロトタイプ実装を用いた評価実験の結果から得た知見とその考察を述べる．

まず操作性についての考察を述べる．構築したプロトタイプ実装のユーザインタフェースは既存の Web サービスである USTREAM を模して作成し，ユーザインタフェースの違いはコンテンツ保護に関する操作である．放送者の操作であるサーバ鍵の設定，ユーザ鍵の生成，コンテンツ保護の実施のすべてにおいて高評価を得られた．ユーザ鍵の生成では 1 人のみから低い評価を受けた．これは視聴者がユーザ鍵を放送者に要求する際に数秒時間がかかり，それによって放送者が待機させられることに起因している．これについては鍵の管理方法を変え，視聴者が意識せずにユーザ鍵を取得できるような仕組みを構築することで対応することが可能であると考えられる．

映像の品質については画質の点で未暗号化映像と復号済映像ともに 100%の視聴者が高く評価していた．このうち，未暗号化映像から復号済映像への画質が劣化したと評価した視聴者は 1 人のみで，その他の視聴者は変化していないと評価していた．このことから，電子指紋を埋め込むことでは視聴者にとって映像の画質は劣化していないと判断されたと考えられる．

本論文では音声情報について暗号化をするといった処理をしていないが，その結果は各種映像で差異が見られなかったことにも表れている．映像と音声の同期性については未暗号化映像よりも復号済映像のほうが悪い結果となっ

た．これは映像を暗号化・復号する処理時間が影響していると考えられる．また，未暗号化映像の視聴時においても悪い評価をしている視聴者が存在するため，映像の配信方法も検討する必要がある．このように森村らの研究における評価実験ではリアルタイムな映像の配信が可能であると考えられていたが，本論文での実験では視聴者によっては悪い評価をしている者もいた．今回の実験では放送者 1 人と視聴者 1 人で実施したが，実際の利用モデルを考えると 1 つの放送番組に対して放送者と視聴者が 1 対多となる．現状はユニキャストを利用する実装で，視聴者が多くなるとネットワークの帯域資源の枯渇による映像配信の遅延がより多く起こりうる．そのため，オーバレイネットワークやマルチキャストを用いた多人数への配信に適したプラットフォームを構築する必要がある．

最後にコンテンツ保護の効果についての考察を述べる．暗号化映像について 100%の視聴者がコンテンツの内容を判別できなかったことから，提案した手法による映像の暗号化は映像の視認性を低下させることができるといえる．一方で交換リストを用いた暗号化は被験者実験のための実行性能を重視した簡素な手法であるため，交換の規則性が分かれば暗号化済映像を復元されうる．これについては，先行研究での実装と同様に放送型暗号で別途暗号化することで解決できる．また，削除困難な電子指紋の埋め込み手法が用いられていることを視聴者に示すことができれば横流しに対する高い抑止力が見込める．これも電子指紋が削除困難であることが前提であるため，より高い抑止力を得るためにはより削除困難な電子指紋の埋め込み手法を検討し，横流しした視聴者を特定できること視聴者全体に示す方法を検討しなければならない．

本論文の実験では，システムの操作性および映像の品質の点では新たな課題が生じたものの被験者からはおおむね高い評価を得ることができた．コンテンツ保護機能である映像コンテンツの暗号化ではすべての被験者がコンテンツの内容を判別することができず，提案手法は高い効果があることが示された．また，電子指紋の埋め込みについては条件付きではあるが，コンテンツの不正な横流しのような海賊行為に対する抑止力として効果があることが分かった．不正な横流しに対する抑止力をより強めるためにはその不正を検知できる仕組みが求められる．そのためにはコンテンツのトレーサビリティの確保だけでなく，コンテンツの流通を制御し不正に横流しされたコンテンツを流通経路上で検知する機能やインターネット上を巡回して横流しされたコンテンツをクローリングする機能を実装する必要がある．

本論文で提案したシステムの実装では映像の暗号化と電子指紋の埋め込みがユーザにどのような影響を及ぼすかを検証するための実装である．そのため，暗号化済映像を復元する攻撃への耐性，復号済映像から埋め込まれた電子指紋を削除する攻撃に対する抑止力には課題がある．この課題については，将来実用可能になると考えられる放送型暗号を用いた別途の暗号化処理や複数箇所に電子指紋を埋め込むといった運用で対処できると考えられる．

7. おわりに

本論文ではコンテンツの暗号化とコンテンツへの電子指紋の埋め込みによるコンテンツ保護を可能としたインターネット生放送システムを実装した．評価実験では操作性，映像の品質，コンテンツ保護の効果の 3 つの評価軸を設け，18 人の被験者実験を実施した．その結果，すべての評価軸について高い評価を受けた．

一方で先行研究では実施しなかった被験者実験より新たな課題が生じた．1 つは映像を暗号化・復号する処理によって視聴者に及ぼす影響が映像と音声の同期性に少なからず表れるということと，もう 1 つはユニキャストでは多人数への映像の配信に耐えられない可能性があるということである．

今後は構築したシステムをインターネット上で公開し大規模なユーザ数でも利用可能なことを示す必要がある．そのためには本論文では実現できなかったユーザおよび暗号化・復号に用いられる鍵の管理，インターネット上に横流しされた映像コンテンツの検知機構を組み込むことに加え，上にあげた今回の実験で明らかになった課題を解決しなければならない．そのうえで今回の実験を拡張してインターネット上での大規模なユーザでの実証実験を行う予定である．

参考文献

[1] 森村吉貴，上原哲太郎，侯　書会，美濃導彦：インターネット放送のための同報性と導入容易性を両立する JFD システムの構築と評価，電子情報通信学会論文誌 B，通信，Vol.94, No.10, pp.1427–1439 (2011).

[2] Boneh, D. and Shaw, J.: Collusion-secure Fingerprinting for Digital Data, *IEEE Trans. Information Theory*, No.5, pp.1897–1905 (1998).

[3] 笠原正雄，村上恭通：公開鍵暗号の二，三の構成法，信学技報 ISEC 99 (208)，pp.33–39 (1999).

[4] Hou, S., Uehara, T., Satoh, T., Morimura, Y. and Minoh, M.: Fingerprinting Codes for Internet-Based Live Pay-TV System Using Balanced Incomplete Block Designs, *IEICE Trans. Information and Systems*, Vol.92, No.5, pp.876–887 (online), DOI: 10.1587/transinf.E92.D.876 (2009).

[5] Kundur, D. and Karthik, K.: Video Fingerprinting and Encryption Principles for Digital Rights Management, *Proc. IEEE*, Vol.92, No.6, pp.918–932 (2004).

[6] Lian, S., Liu, Z., Ren, Z. and Wang, H.: Joint Fingerprint Embedding and Decryption for Video Distribution, *2007 IEEE International Conference on Multimedia and Expo*, pp.1523–1526 (2007).

[7] Boneh, D., Gentry, C. and Waters, B.: Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys, *Proc. Crypto '05*, pp.258–275 (2005).

[8] Tang, L.: Methods for Encrypting and Decrypting MPEG Video Data Efficiently, *Proc. 4th ACM International Multimedia Conference* (*ACM Multimedia'96*), pp.219–229 (1996).
[9] Slagell, A.J.: Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm, available from ⟨http://eprint.iacr.org/2004/011.pdf⟩ (accessed 2013-04-10).
[10] Microsoft: DirectShow (Windows), available from ⟨http://msdn.microsoft.com/library/windows/desktop/dd375454(v=vs.85).aspx⟩ (accessed 2013-04-10).
[11] Microsoft: Windows Media Format 11 SDK (Windows), available from ⟨http://msdn.microsoft.com/library/windows/desktop/dd757738(v=vs.85).aspx⟩ (accessed 2013-04-10).
[12] Microsoft: ActiveX Controls, available from ⟨http://msdn.microsoft.com/library/aa751968(v=vs.85).aspx⟩ (accessed 2013-04-10).
[13] Rails Core Team: Ruby on Rails, available from ⟨http://rubyonrails.org/⟩ (accessed 2013-04-10).

付　　録

A.1 アンケート項目

A.1.1 放送者に対する質問

Q1 【単一回答】放送にコンテンツ保護を施すことに関して以下の問いにお答えください.

(a) 放送するための鍵の設定の操作性について
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

(b) 視聴者のための鍵の生成の操作性について
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

(c) 放送にコンテンツ保護を施すときの操作性について
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

A.1.2 視聴者に対する質問

Q1 【単一回答】**コンテンツ保護なし** 最初に視聴した放送の品質について以下の問いにお答えください.

(a) 映像の内容を判別できましたか
- ○ よくできた
- ○ できた
- ○ どちらでもない
- ○ できない
- ○ まったくできない

(b) 映像の画質と滑らかさはどうでしたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

(c) 音声の音質と滑らかさはどうでしたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

(d) 映像と音声は同期していましたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

Q2 【単一回答】**コンテンツ保護あり（復号前）** コンテンツ保護中に視聴した放送の品質について以下の問いにお答えください.

(a) 映像の内容を判別できましたか
- ○ よくできた
- ○ できた
- ○ どちらでもない
- ○ できない
- ○ まったくできない

(b) 映像の画質と滑らかさはどうでしたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

(c) 音声の音質と滑らかさはどうでしたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

(d) 映像と音声は同期していましたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

Q3【単一回答】コンテンツ保護あり（復号後）鍵を使って正しく視聴した放送の品質について以下の問いにお答えください．

(a) 映像の内容を判別できましたか
- ○ よくできた
- ○ できた
- ○ どちらでもない
- ○ できない
- ○ まったくできない

(b) 映像の画質と滑らかさはどうでしたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

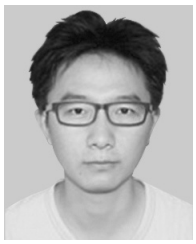
(c) 音声の音質と滑らかさはどうでしたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

(d) 映像と音声は同期していましたか
- ○ とても良い
- ○ 良い
- ○ どちらでもない
- ○ 悪い
- ○ とても悪い

Q4【単一回答】視聴した映像にはあなたのことを特定できるIDが埋め込まれています．そのため，あなたが視聴した映像をYouTubeやニコニコ動画にアップロードすると映像の権利者（放送者）に訴えられる可能性があります．それでもアップロードしたいとき，あなたはどうしますか？
- ○ やっぱり訴えられたくないのでアップロードしない
- ○ 簡単にIDを取り除けるなら取り除いてアップロードする（無理なら諦める）
- ○ IDを取り除くのが難しくても，どうにかして取り除いてアップロードする
- ○ 気にせずそのままアップロードする

津田 侑 （正会員）

平成20年立命館大学情報理工学部卒業．平成22年京都大学大学院情報学研究科修士課程修了．平成25年同大学院情報学研究科博士後期課程研究指導認定退学．同年情報通信研究機構サイバー攻撃対策総合研究センター研究員．サイバー攻撃対策に関する研究に従事．人工知能学会，社会情報学会各会員．

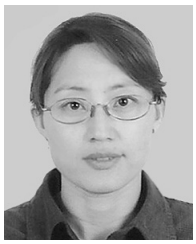


黄 亮錦

平成22年中山大学ソフトウェア工学部卒業．平成25年京都大学大学院情報学研究科修士課程修了．

森村 吉貴 （正会員）

平成16年京都大学工学部情報工学科卒業．平成21年同大学大学院情報学研究科博士後期課程研究指導認定退学．平成22年同大学物質–細胞統合システム拠点特定拠点助教．インターネット映像放送のDRMとQoSの研究，教育目的の映像処理の研究に従事．京都大学博士（情報学）．電子情報通信学会会員．



侯 書会

平成21年京都大学大学院情報学研究科博士後期課程修了．平成21年北京科技大学数力学系講師．平成25年同大学信息与計算科学系准教授．情報セキュリティ，デジタルフォレンジクスの研究に従事．京都大学博士（情報学）．

上原 哲太郎 （正会員）

平成 2 年京都大学工学部情報工学科卒業．平成 7 年同大学大学院博士課程研究指導認定退学．同年同大学院工学研究科助手，平成 8 年和歌山大学システム工学部講師，平成 15 年京都大学大学院工学研究科附属報センター助教授，平成 18 年同大学術情報メディアセンター助教授，平成 19 年同准教授．平成 23 年総務省技官（標準化推進官）．平成 25 年立命館大学情報理工学部教授．システム管理，情報セキュリティ関係の研究に従事．京都大学博士（工学）．IEEE，電気学会，日本ソフトウェア科学会，情報ネットワーク法学会，社会情報学会，CIEC 各会員．

上田 浩 （正会員）

平成 11 年豊橋技術科学大学工学部知識情報工学課程卒業．平成 16 年同大学大学院博士後期課程修了．博士（工学）．同年東北大学電気通信研究所博士研究員．平成 18 年群馬大学総合情報メディアセンター助教授．平成 19 年同准教授．平成 23 年京都大学学術情報メディアセンター准教授．ネットワークトラフィック等の確率過程モデル，自然・社会現象の数理モデル，情報倫理教育に関する研究に従事．電子情報通信学会，日本数理生物学会各会員．