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

2006－DBS－138（33）
2006－GN－58（33）
2006／1／27

乱数放送を利用した撮影時刻の証明方式の提案

青野正宏*　小嶋徹也*
*東京工業高等専門学校

文字情報と異なり，一般に映像や音声の記録は，真実を表わしており，証拠能力もあるとされている．監視カメラの記録も映されたものは真実と考えられる．しかし，実際は編集やその他の手段で，事実と異なる記録を作り出すことが可能である．そのため，本稿で，監視カメラ記録を例に挙げ，乱数放送を用いて，撮影された時刻が正しいものであるか否かを証明する方法を提案する．

A Proof Method of Filming Time by Random Numbers Broadcasting

Masahiro Aono*　Tetsuya Kojima*
*Tokyo National College of Tecknology

Video and/or sound records are assumed to display truth and to be evidence of the event in general, but letters don't. Records of the watching camera are assumed to be true, too. However, really, it is possible to create the record of false event by the watching camera. In this paper we propose a method to proof filming time by random numbers broadcasting.

１．はじめに

一般に，文書に関しては，それが正当なものかどうかを判断するのに，相当な注意が払われる．紙に書かれたアナログ的な文書であれば署名・捺印で正当性が保証されているものとされる．署名は筆跡から他人には偽造は困難であるとみなされており，捺印に使用する印鑑も印影が同じものを作れないとみなして成り立っている．現実には必ずしも偽造が不可能なものであるかどうかは疑問なところもあるが，社会的には大きな混乱もなく成立している．これがデジタル文書となると，文書データそのものには正当性を保証する要素がないため，電子署名などの技術が用いられている[1]．いずれにせよ，なんらかの形で証明する機能が付加されている．しかも，これは作成者を証明するだけで，その内容が真実と判断できるかどうかは別問題である．

ところが，音声・写真・映像の形で記録された情報は，それだけで，それ(例えば，話であれば，話の内容ではなくそれを話したということ)が真実であると一般に認識されている．ある出来事があったということを文書の形で公開しても，それが真実であるか捏造であるかは，その文書のみからは信用しない．文書を作成した者が，信用がおけるかどうかで判断しているのみである．しかし，写真がついていれば真実であると信用してしまう．スキャンダルを例にとれば，A と B が会っているところを目撃したということを信用してよいかわからない人が第 3 者に伝えても，半信半疑の状態程度である．しかし，その者が写真を撮っており，その写真を示されれば，動かぬ証拠として信用してしまう．写真週刊誌がその是非は別として成り立つ所以である．また，利害が対立しその調整を行う会議を想定する．会議の記録を一方の当事者や第三者がメモの形で筆記しておいたものや，記憶をたどって議事録を，後で書き起こして議事録を作成し，会議関係者の承認を得る方法が成り立つのは当事者間で信頼関係が成り立って

いる場合のみである．社会的事件にからむような場合において，一方の当事者がその議事録を否定すれば, 記録としての信頼性は揺るいでしまう. しかし，ここに音声のレコーダを持ち込んで記録するとその内容が真実とされる．音声で記録されるとわかっている場合は発言が慎重となるし，まして相手に黙って音声記録をとることはルール違反とされるのは，音声記録に絶対性があるとみられるためである．写真や音声記録は，従来はアナログフィルムやテープレコーダであったが, デジタルカメラやデジタル IC 録音機に変わっても，法学的に厳密な判断は別としても，一般には証拠性はアナログ記録と同様の証拠性を持つものと受け止められていると考えてよさそうである．デジタルデータによる写真・音声・映像のデータ量は多く，これを作成するのは困難であると認識されているからである．

しかし，現実には，例えばコンピュータグラフックスの発展により，実写と見間違うようなリアルな画面を合成することも可能となってきており，無条件にこれらの情報が真実であるということは言えなくなってきている．このような状況を踏まえ，デジタルで記録した記録，特に監視カメラによる映像記録を取り上げて，その記録がその時点で撮られた真実の記録であることを証明する方法を検討する．

２．監視カメラの記録について

近年，世情の不安定化とカメラの低廉化に伴い，監視カメラの設置が目立つようになってきた．監視カメラによる記録により犯罪の防止や犯人の追求に効果を挙げる反面，プライバシーの侵害も懸念されている．ここではその是非については議論しない．

監視カメラは目的とする箇所の状況を把握するために設置している．監視員が目の行き届かない場所を常時リアルタイムに監視する目的で設置されているものもあるが，多くは記録装置に自動的に監視画面をコマ落としの方法で動画画像つまり映像を記録し，特にそのときの状況を把握したい場合は記録した映像を取り出して確認する．一定期間の間に特に問題がなければ古い記録から消去し，繰り返しその記憶領域を新しい記録のために再使用するという使い方が一般的である．この記録から犯罪者を見つけたり，その足取りを追ったりしたりしている．逆にこの記録からアリバイ証明にも使用できる．ある監視カメラの記録のある時刻にある人物が写っているとすれば，その時刻にその人物がその場所に存在していたとの証明となる．しかし，実際にその監視カメラの記録がその時刻に撮影されたものであるかどうかの確実な証明はしていない．監視カメラの設置管理者は善意であるとみなされている．必要があって監視カメラの映像記録を参照する場合，映像記録とその記録時刻は管理者の提供された情報を特に問題ない限りそのまま信用している．それがこれまで問題になったようなことはない.

ところが，やたらに監視カメラが増えてくると，これを逆用して監視カメラの記録を改ざんして偽のアリバイ証明を企てる者が現れるかもしれない．監視カメラには改ざん防止のための機能がついている装置が多いが設置管理者に初めから改ざんの意図があれば，撮影時刻を改ざんすることは難しくない．ここでは，監視カメラの設置管理者が悪意を持っていたとしても，監視カメラの映像と時刻の記録の信用性を高める方法を提案する．

３．事後の偽造の防止

撮影がある時刻より後で撮影されたものでないことを証明する方法としては，撮影された直後に映像記録またはそのコピーを信頼できる機関(認証機関)に預けることである．そうすれば，少なくとも預けた時刻より前であることは自明である．しかし，これは非現実的である．そのため，映像の代わりに映像データについてハッシュ関数を用いてダイジェスト値で代替させる．期間を区切り一定期間内の映像記録について証明の対象とする．対象となるデータは圧縮されたデータとするが，全データをリアルタ

イムでハッシュ値を求めるか一定間隔で抜き出したデータのみについてハッシュ値を求める．このハッシュ値の情報を認証機関に送れば，送信データ量はわずかで済む．それでも，ハッシュ値を保存すると管理に負担がかかる．要はその時刻に認証機関がそのハッシュ値を受け取ったということを証明できれば良い．送られてきたハッシュ値にタイムスタンプを付加して認証機関で電子署名をつけて，証明を求めてきた機関やシステムに送り直せば良い．撮影機関またはシステムは映像記録とともに証明書を保存する．撮影時刻を証明する場合は，記録時と同じ方法で映像記録のハッシュ値を再計算し，保存してある証明書のハッシュ値と一致すればその証明書に記録してあるタイムスタンプより前の時刻であること

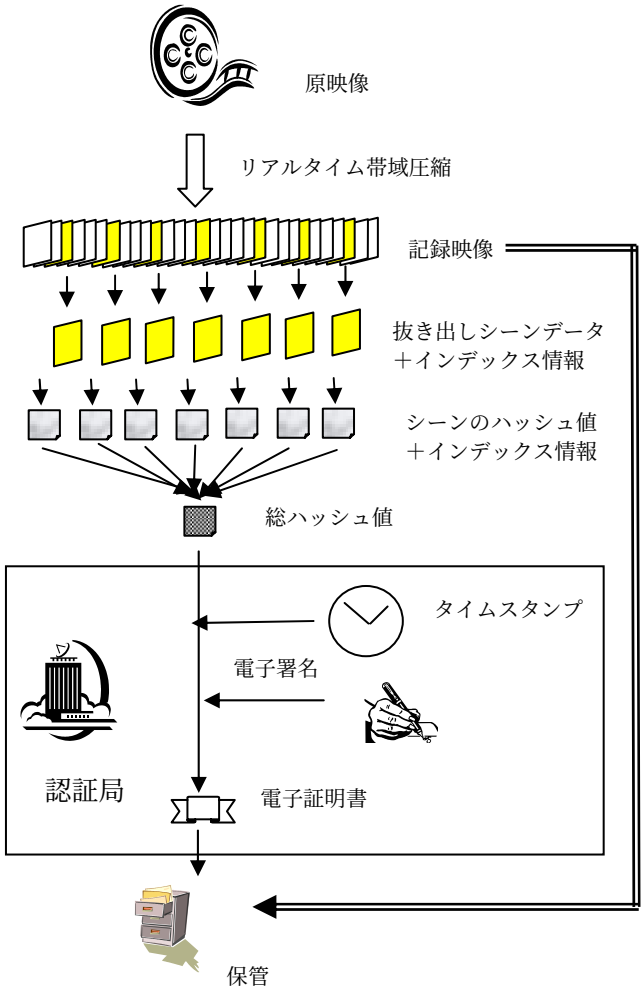

図 1　撮影時刻の証明

が保証される．これで事後のアリバイ作りなどは防止できる．この方法は一般の文書の原本性保証と同じ方法であり，特に難しい課題はない．

４．事前の偽造防止

４．１　事前の偽造防止の必要要件

事後の偽造防止のみでは，事前に準備されたアリバイ作りは防止できない．撮影が，ある時刻より後で記録されたものであることを証明する方法を検討する．ある時刻より後で記録されたことを証明する方法としては，その時刻にならないと判明しない情報を記録に加えることである．TV やラジオの放送局が放送している番組が生放送であることを示す一番良い方法は，出演者がその日のニュースを話題に取り上げることである．視聴者は生放送であることを信用する．しかし，監視カメラで撮影している映像にはニュースなど流せない．仮に TV ニュース画面が監視カメラの撮影映像に写っていたとしても，その TV カメラ画像自身が録画であるかもしれない．また，TV やラジオにしても，生放送中に一部を録画や録音を挿入しても視聴者はわからない．ごまかす気になればいくらでもごまかす方法はある．つまり，ここで考慮すべき点は，

- その時点でしかわからない最新の情報を記録に加えること
- 記録済みの映像に最新の情報を加えることが困難であること
- 最新の記録と古い記録を合成することが困難であること

の 3 点である．

４．２　最新情報の付加

まず，その時刻にならないと判明しない情報を作り出す方法を示す．一般的なニュースは常に発生するわけではないから，模擬的にニュースに代わる情報を作り出す．公正な信頼できる機関を想定する．この機関において，乱数を定期的に発生させる．乱

数は，過去の乱数を観測しても次に発生する乱数は予測することが困難なアルゴリズムを採用し，偏りが少ないものが望ましい．この乱数発生の計算式は非公開でその秘密は洩れないことを前提とする．このような乱数を発生させる機関を複数置き，それぞれの機関が発生した乱数を代表する機関にリアルタイムに送信し，代表機関が，それらの乱数からひとつの乱数を合成するようにすれば,乱数の秘密性は高くなる．少なくともひとつの機関の乱数発生のメカニズムが秘密であれば，最終的に出力される乱数の値を予測することはできない．最終的に出力される乱数とその時刻情報は，改ざんされないよう管理を厳密にして記録時刻を保証する期間は保存する．作成された乱数を代表機関が，利用対象者に向けて放送する．

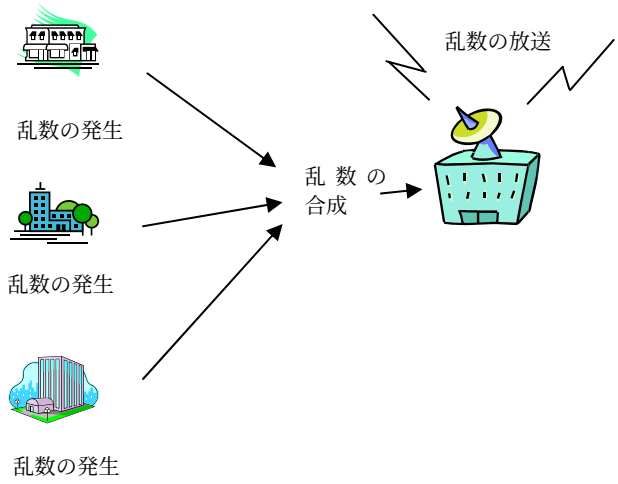

図 2.　乱数の発生と放送

４．３　記録済み映像の利用防止

次に記録済みの映像に最新の情報を加えることが困難とする方法を示す．撮影による映像記録と同時に，受信した乱数情報を記録情報のなかに，単純に織り込む方法では，時刻の証明にはならない．あらかじめ，撮影した記録データに乱数情報を織り込むことは容易にできるからである．事前に準備ができない方法でなければならない．その方法として，放送された乱数データが撮影方法を指定しているものとし，指定された方法で撮影する手法を提案する．

まず，カメラはズーム・パン・チルド機能を備えているものとする．撮影システムは乱数を受信すると，あらかじめ定めておいたルールに従い，カメラの撮影角度を変更する．例えば，4 桁の数字を乱数で与えられるものとして，ある時刻 t に乱数 xxyy が与えられるものとすると，カメラの角度を標準の設定位置より(xx-50)*0.2 度左(マイナスの場合右)，(yy-50)*0.1 度上(マイナスの場合下)，にずらすという方法である．一定時間毎に受信した乱数の値により撮影角度をずらす．ずらした角度により撮影された映像を記録する．

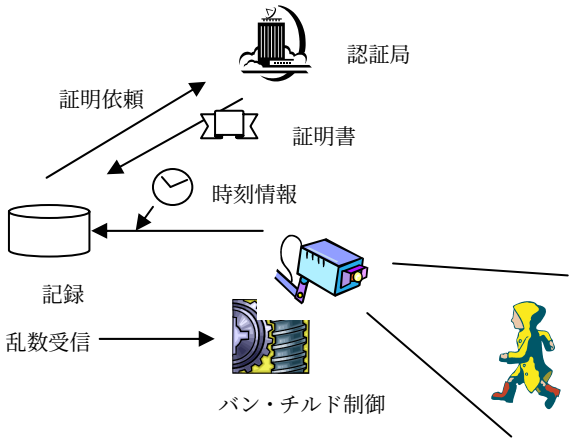

図３　撮影と記録の方法

カメラの種類，撮影対象となる距離などから撮影される範囲は限定される．撮影角度がずれることにより,乱数の情報を反映していることは証明できる．この方法に対抗し，事前に映像データを本来の撮影対象範囲よりも広く撮影しておき，乱数を受信したとき，乱数に合わせて撮影角度がずれた映像のみを取り出し，カメラの角度をずらした撮影を模擬するという方法が考えられる．そのような画像処理のプログラムを作成し，乱数受信に合わせて，リアルタイムで模擬画像を作成すれば，ある程度は同じように見える画面を模擬することは可能であるかもしれない．しかし，鑑定のレベルからすると模擬することはかなり難しい．まず，事前に作成する映像デー

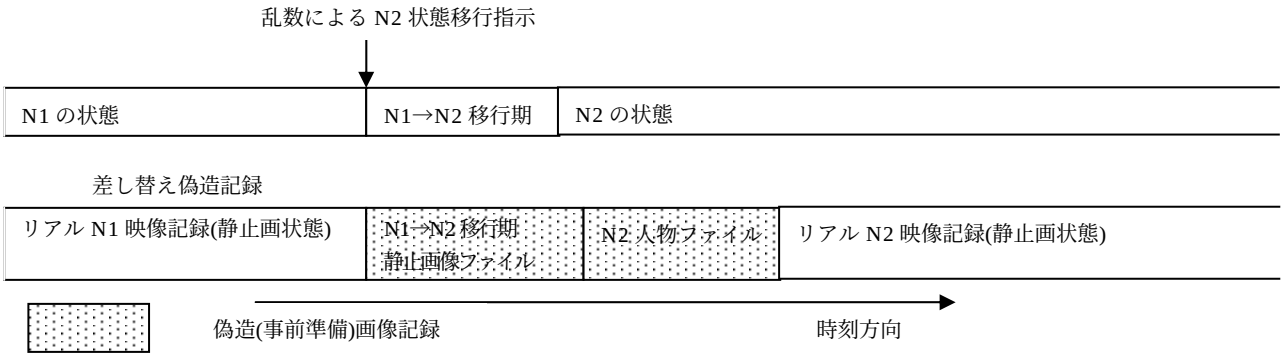

図 3　過去の映像記録と最新記録を合成する方法

タを作るためには，ターゲットとするカメラより広い画面を必要とする．撮影方法や撮影位置，カメラの種類などを変えなくてはならない．また，画面に映る固定的な対象物については情報量がまったく同じでなければならない．また 2 次元的に 3 次元対象物を撮影するため，周辺部ではゆがみが生じるが，異なる方法で撮影したものを同じように歪めるのは難しいと考えられる．

４．４　記録の合成

最新の記録と古い記録を合成することが困難とすることは少し難しい．次のような場合を想定する．ある人物 A が実際にはある時刻 B にある場所 C にいたが，いろいろな都合で場所 C にいなかったということにしておきたいとする．つまりアリバイ作りをしたいとする．その時刻 B に，全く別の場所 D にある監視カメラに写っていたとすれば，C にいなかったということが証明できる．監視カメラの管理者 E も共犯ということにする．人物 A は，あらかじめ，管理者 E の協力を得て，撮影方法の各種類にカメラを設定して，それぞれの撮影方法の種類に応じて，人物 A が撮影範囲内を通り過ぎる映像を作っておく．作った映像データは，映像ファイルとして準備する．アリバイ作りをしたい時間帯になったとき，人物 A は場所 C にいる．A に協力する管理者 E は，乱数放送で撮影方法の指定がなされたとき，その時点の映像データからでなく，指定された撮影方法に対応する映像ファイルを撮影記録として代替する．アリバイ証明が必要となったとき，この監視カメラの記録を証拠として提出し，時刻 B の前後には場所 D にいたことが監視カメラの記録から明らかなので場所 C にいたことを否認する．

これに対して，撮影方法の変更は断続的に行われるものではなく，撮影方法の移行過程がそのなかに入ってくる．撮影方法の変更指定があってから，カメラが移動する．記録としては変更前と変更後の両方の状態が必要となる．つまり，撮影方法としてNとおりの種類があるとすれば，N^2とおりの撮影データが必要となるから事前準備は難しいのではないかと考えることもできる．しかし，実際には楽観的には考えられない．人物などが写っていなければ，監視カメラの撮影画面の大部分は静止画に近いと考えても良い．人間が表示されている場合にN^2とおりの映像を作成するのが困難であっても，静止画の場合，時間をかけて自動的にN^2とおりの映像を作成することは，それほど困難でない．N1 の状態のとき，リアルタイムの監視カメラの画像の状態としておく．乱数放送によりN2 の撮影方法への移行の指示があったとき，あらかじめ用意したN1→N2 移行期ファイルを読み出し，リアルタイムの監視映像の代わりにこのファイルのデータを記録する．静止画同士を接続するのであるから，継ぎ目を見せなくすることは比較的容易である．

そのため，映像角度やズーム範囲など，乱数でで

きる撮影法の種類はできるだけ多い方が良い．あるいは常にカメラの所定の速度で移動していることが望ましい. 乱数受信の間隔が一定であったとしても，受信する乱数にカメラ撮影方法の間隔指定の意味も含ませ，撮影方法間隔はランダムであることが望ましい．N の数が小さいと事前準備により改ざんができやすくなってしまうからである．

原映像そのものは，ビット単位に情報を作れば作れないことはないから，はめ込み合成やその他の手段を組み合わせれば，原理的に偽造は不可能であるという厳密性までは有していない．数学的に解を見つけるのに莫大な時間がかかるから安全性が保証されるという暗号や署名の場合とは性質が異なっている．しかし，どのような用途に使われるか，偽造のコストとそれから得られる利益を考慮すると，証拠能力としては高いものと考えて良い．

これより，ある時刻より前に記録されたものであるということは認証により証明できるから，この両者を合わせると，ある一定時刻の範囲内に記録された情報であることを証明できる．

４．５　乱数放送について

乱数そのもの通信負荷はほとんど問題にならない[2]．放送される乱数は，諸般の事情により必ず受信できるとは限らない．誤って受信する場合も，受信できない場合もある．誤って受信し，異なる種類の撮影方式を選択すると正しい映像であっても偽造と判定されてしまう．乱数情報そのものは情報量としてわずかの情報であるから，冗長度をきわめて大きくして，誤った情報を正しいと判定することがないようにしなければならない．正しく受信できなかった場合は乱数による撮影方式選択はあきらめて，標準の撮影方式を選択する．過去の映像を用いた映像記録ではないとの証明はできないが，タイムスタンプのついた証明書が得られれば，少なくとも後から撮影した情報でないことだけは証明できる．限定された範囲での証明能力は残せる．また，必ずしも常に完全な証明が必要とは限らないから，有効性は残る．

直接本題に関係はないが，乱数放送の応用としては，ワンタイムパスワードへの利用が考えられる．ワンタイムパスワードは，通信の途中でパスワードを盗まれることがないよう時間に応じてパスワードを変更する方式であるが，利用者側で，サーバ側が認識できるよう同期してパスワードを変更するような機構が必要である．乱数放送のデータをサーバ側と利用者側で同時に受信できれば，利用者側は固定的なパスワードであっても，受信した乱数で変換を行い，それに一方向性関数を経由してサーバ側に送れば，毎回値が変更される．攻撃者は乱数データは公開された放送であるから知ることはできるが，途中で送信パスワードデータを盗聴しても，オリジナルのパスワード値を知ることはできない．

５．まとめ

５．１　従来研究との相違

従来の映像記録の保護に関する技術は，映像の撮影者や著作権者の権利を保護するため，不正コピーや不正視聴，第三者による改ざん防止などにテーマの中心がおかれている[3]．市販されている映像の監視装置では，改ざんの検出機能がついた製品が多く出ている．映像中に改変判定コードを埋め込み，再生時に判定できるようにするものである．これは一般に，第三者が改ざんすることを想定している．撮影されたものは真実を反映しているという世間の通念を利用して，最初から意図的に撮影者や監視カメラ管理者自身が，真実と異なる映像を作り出し，これを証拠として利用しようとする目的に対しては，その防御策は余り考えられていない．完全な証明という意味では無理であるが，撮影された記録が事実を表しているか否かについての方策の検討[4]を始めた．本稿では，監視カメラ記録の意図的な記録偽造を防止することに絞って述べた．

５．２　具体的検討への展開予定

映像の質は目的により，また今後の映像，データ記録密度，演算速度の技術とコストにより，求められるレベルが異なるのは当然であるが，一般に，それぞれ，どの程度の品質が求められるか検討しておくことが必要である．

- 映像の画質はどの程度必要か．
- 映像のサンプリング周期はどの程度必要か
- 映像の原本性保証のためのハッシュ値計算はどの程度の頻度でデータをサンプリングすべきか
- リアルタイムでハッシュ計算を行うとどの程度の演算負荷がかかるか
- 総ハッシュ値計算を行い，認証機関でタイムスタンプを押して認証するとすれば，映像記録が終わった時刻とタイムスタンプに押された時刻との時間差はどの程度あるか

乱数受信により，カメラをどの程度まで，動かすかという問題が課題のひとつとなる．乱数受信による制御に関する情報量が小さいと，あらかじめ偽造できる確率が大きくなり,信頼度が下がってしまう．カメラを動かす頻度やその角度が大きいと，必要あって画面を再生するとき，見辛くなる．また，カメラの動きをどの程度制御するか．複雑な制御はカメラシステムのコストを上げてしまう．これらの問題はトレードオフであるが，最適解を求めるには次の問題を調べる必要がある．

- カメラの動きにより，カメラをどう操作したかという分解能はどの程度まで可能か．
- カメラの動作方法は，どの方法がコスト的な面や分解能の面で最適か．例えばカメラを左右・上下に角度を変えるよう動作させるのが良いか．
- 画面を再生したとき，どの程度の画面変動に抑えるなら，画面を見ている者にとって容認できるか．
- 画面の動きを明確にするために固定目標を表示しておく必要があるのか．

謝辞

本研究は，独立行政法人日本学術振興会による科学研究補助金による研究「圧縮の疎密による余剰帯域を利用したマルチメディア統合放送方式に関する研究」の一部として，その応用利用方式を研究するために行った．

[1]電子情報通信学会編，”情報セキュリティハンドブック，オーム社，2004 年 11 月

[2]青野正宏，大森大将，小嶋徹也 "圧縮の疎密による余剰帯域の考察"，　情報処理学会研究報告 2005-BCCgr-10，2005 年 1 月

[3]松野良一，” 地域映像ネットワーク(Japan Film Net)の構築に関する実証的研究－デジタル時代における独自コンテンツの重要性－”，電子情報通信学会通信方式研究会　第 17 回ワーショップ 2004 年 10 月

[4] 青野正宏，上野健太，小嶋徹也，“マルチメディア記録の改ざん防止方式”,東京工業高等専門学校研究報告書　37(2)号　2006 年 1 月