2008－CSEC－42（6）
2008/7/24

動画像・音声データに対する部分完全性保証技術 PIAT の実現(II)

吉岡 孝司† 武仲 正彦†

†株式会社富士通研究所 〒211-8588 神奈川県川崎市中原区上小田中 4-1-1
E-mail: †{yoshioka, takenaka}@labs.fujitsu.com

あらまし MPEG 等の動画像・音声データに対する部分完全性保証技術 PIAT を改良したので報告する。PIAT は、墨塗りや一部追加等を行っても、変更部分以外の完全性を保証可能な署名方式である。SCIS2008 では、この PIAT を利用し、動画像・音声データの一部切り出しと原本性保証を両立可能な方式の提案に加え、プロトタイプ作成による評価結果を報告した。本稿では、第三者が保証する時刻情報と連動させ、任意分割された動画像・音声データの原本性、連続性、時系列性を保証可能な改良方式について提案する。本提案方式を用いれば、任意分割された動画像・音声データにも適用でき、監視カメラ等の実際のシステムで、高い証拠性と利便性を備えた証跡管理が可能となる。

キーワード 動画像，音声，MPEG，部分完全性保証技術，署名，墨塗り

An Implementation of Partial Integrity Assurance Technology : PIAT for Audio and Video Data (II)

Takashi YOSHIOKA† Masahiko TAKENAKA†

†FUJITSU LABORATORIES LTD. 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, 211-8588, Japan
E-mail: †{yoshioka, takenaka}@labs.fujitsu.com

Abstract The Partial Integrity Assurance Technology (PIAT) is a signature scheme that guarantees the integrity even if an original document is sanitized or revised. In SCIS 2008, the authors proposed an efficient method for applying PIAT to the audio and video data such as MPEG, and evaluated our prototype. This article discusses how to guarantee the originality, continuity, and the time series of arbitrary divided audio and video data by using the time information issued by the trusted third-party. Since recorded data by actual surveillance video systems are divided, the proposed system enables to provide the trace management with high evidence and convenience.

Keyword Video data, Audio data, MPEG, Partial Integrity Assurance Technology, Signature, Sanitize

1. はじめに

店舗や繁華街、集合住宅等での監視カメラ設置や業務車両へのドライブレコーダ設置等が一般化し、動画像を証拠物件として取り扱う事例が増加している。また、電話による取引やサポート業務のトラブル対策として、顧客とオペレータとの会話を録音し証拠として保持することも常識となりつつある。

現在、動画像や音声を証拠とする場合、ビデオテープや画像・音声ファイルをそのまま提供している。しかし、画像・音声保存のデジタル化が進めば、それらの改ざんや編集は容易になり、証拠として取り扱う場合は署名やタイムスタンプといった第三者証明が必要となる。現に電話オペレータの音声をタイムスタンプ付で録音・記録するサービスや製品が販売されており[1],[2]、今後このような技術のニーズが高まることが予想される。

一方で、増加する監視カメラ等に対して、撮影された映像の利用に対するプライバシの保護が問題となり、議論が行われている[3]。また、個人情報保護法の施行等により、個人のプライバシ情報の利用が厳しく制限され、本人の要求があれば、開示や部分的な削除等が必要である。

こういった証拠性とプライバシ保護の両立という課題に対して、電子文書の一部に対する部分的な原本性(完全性)の保証や秘匿(墨塗り)する墨塗り署名技術の研究が進んでいる[4]～[11]。特に部分完全性保証技術 PIAT[6]は電子署名を施した文書の原本性を保証しながら、一部を追加や変更、墨塗り(秘匿)、削除が可能な署名技術で、幅広い応用が可能である。

本稿では、SCIS2008[10]で提案した動画像・音声データに対する PIAT 適用方法について述べる。更に、前回方式を改良し、第三者が保証する時刻情報と連動させ、任意分割された動画像・音声データの原本性、連続性、時系列性を保証可能な方式について提案する。

2. 部分完全性保証技術 PIAT

部分完全性保証技術 PIAT は、吉岡らが 2004 年に提案した署名応用技術[6]である。本章では、動画像・音声データに PIAT を適用することを前提に、データの切り出し・抽出を行う場合の PIAT が対象とするモデルとアルゴリズムについて述べる。

2.1. 三者モデル

PIAT では、対象の電子データに対して署名を行う署名者と、そのデータを抽出する抽出者、および開示データの検証を行う検証者からなる三者モデルを対象とし、署名者、抽出者、検証者に対して以下のような条件を設けている。

署名者は、署名することで署名対象の電子データの内容を保証する。対象データのうちどの部分が抽出されるかわからないという条件下で署名を行う必要がある。

抽出者は、署名者が署名した電子データから、部分的にデータを抽出して、検証者に開示する。抽出方法には、抽出者の情報を同時に開示し、誰がその抽出処理を行ったかを明示する顕名抽出と、抽出者が抽出処理を匿名で行う匿名抽出の 2 種類ある。本稿では、顕名抽出を行うことを前提に議論を行う。

検証者は、開示された電子データが署名者によって保証されているかどうかを検証する。匿名抽出の場合は、開示された抽出データは署名者が署名をした電子データの一部であることを検証する。顕名抽出の場合には、開示された抽出データは、署名者が署名をした電子データの一部であることに加え、その抽出が抽出者によって行われたことを検証する。

2.2. PIAT アルゴリズム

PIAT のアルゴリズムの概要を示す(図 1)。アルゴリズムの詳細は、[6],[7],[11]を参照。

署名者は、署名対象データを部分データに分割し、各部分データのハッシュ値を計算して、ハッシュ値集合を生成する。なお部分データのハッシュ値が同じ値にならないようにするために、各部分データに乱数を付加してハッシュ値を計算する場合がある。その後、生成したハッシュ値集合に対して署名者の電子署名を行い、ハッシュ値集合と電子署名をあわせて PIAT 署名とする。

抽出者は、署名者が PIAT 署名を施したデータから、部分データを抽出する(それ以外の部分データは消去する)。その後、署名者と同様の操作を行って、抽出者の PIAT 署名を生成する。ここで、抽出ではなく削除部分を明確にしたい場合には、墨塗り処理となり、削除後の部分文書を“XXXXXXX”といった墨塗りであることが区別可能な部分文書に変更する。

検証者は、まず、署名者と抽出者の PIAT 署名から、ハッシュ値集合の完全性を検証する。次に、開示された部分データからハッシュ値集合を生成し、抽出者の PIAT 署名に含まれるハッシュ値集合と同一であることを検証する。最後に、署名者と抽出者のハッシュ値集合を比較することで、ハッシュ値が同じ部分が元のデータからの抽出位置であることがわかる。もし、抽出データのハッシュ値が署名者の PIAT 署名のハッシュ値に含まれていない場合は、その部分データは改ざんされていることになる。

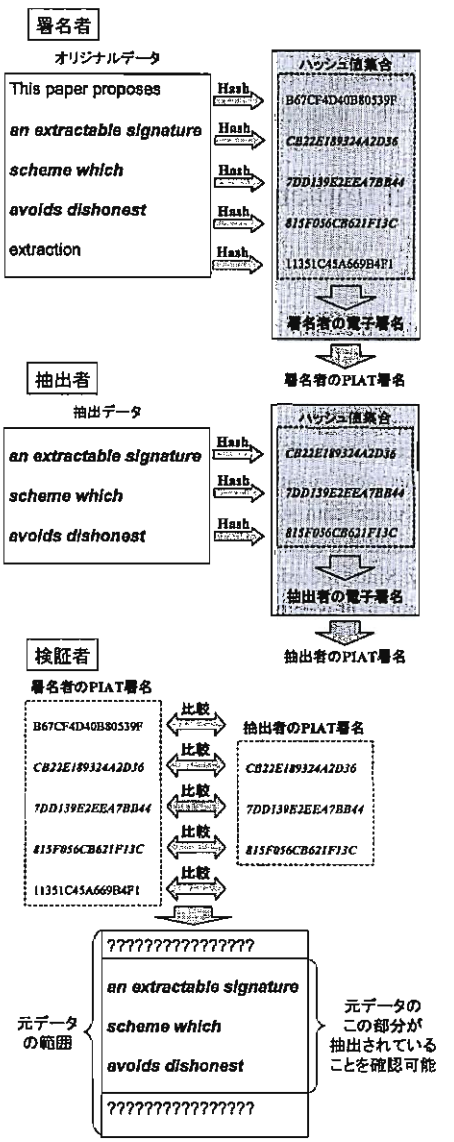

図 1. PIAT アルゴリズムの概略

3. 動画像・音声データへの PIAT 適用

本章では、動画像・音声データへの PIAT 適用について検討する。代表的な動画フォーマットとしては、MPEG-1[12]/2/4、音声フォーマットは、MP3(MPEG-1 Audio Layer-3)[13], WAV(RIFF waveform Audio Format, Microsoft)[14]等が存在する。本稿では、最も構造が単純な MPEG-1 の画像に対する適用方法を示すが、それ以外のフォーマットでも、基本的な構造は同じであり、PIAT は容易に適用できる。

MPEG-1 フォーマットには様々なものがあるが、本稿では、単純化のために、音声部分を除去した MPEG-1 の Video フレームを対象とし、CBR(Constant Bit Rate: 固定ビットレート)方式、MPEG-1 符号化された画像のみを扱う ES(Elementary Stream)への適用を検討する。これ以降対象とするフォーマットを単に MPEG-1 と記述する。

3.1. MPEG-1

MPEG-1 は、ISO/IEC 11172-2[12]で標準化されている動画像符号化技術である。動画像は、静止画像を高速に表示することによって実現される。例えば、テレビジョンでは秒間 30 枚程度の画像を表示している。この毎秒表示される画像の枚数をフレームレートと呼ぶ。

動画像の符号化技術では、データ量を削減するために符号化による(静止)画像圧縮と、フレーム間予測符号化による圧縮を行っている。MPEG-1 では静止画像圧縮に DCT 技術、フレーム間予測に双方向予測技術を採用している。双方向予測のために MPEG-1 では、静止画像の保持方法が 3 タイプ存在する。図 2に MPEG-1 の画像タイプとその並びを示す。I ピクチャは、表示に必要な全ての画像データを圧縮して保持している。P ピクチャは、フレーム間予測画像と呼ばれ、直近にデコードされた I ピクチャ、もしくは P ピクチャの画像を参照画像とし、そこからの差分等の値だけを保持する。B ピクチャは、直近にデコードされた未来と過去の I ピクチャ、P ピクチャの画像を参照画像として、その差分値等を保持する。P ピクチャや B ピクチャでは、前後の画像との差分をとることで、時間方向の冗長度を除去し、高いデータ圧縮を実現している。

また、MPEG-1 では、図 2のように何枚かの画像をまとめて GOP(Group of Pictures)と呼ばれる動画像の最小単位で構成される。GOP はその単位での独立再生が可能で、動画像を途中から再生・編集可能な構造となっている。

更に、MPEG-1 の Video フレームの構成を詳細化すると、図 3のように、Sequence Header(SH)、GOP Header(GH)、Picture Header(PH)、Picture Data(PD: PH 以下のレイヤデータ)から構成される。特に SH は、画像サイズやアスペクト比、フレームレート等、ビデオシーケンス全体に渡る共通のパラメータを記録しており、シーケンス中、変化しない情報となる。更に SH には、ユーザが自由にデータを格納できる領域が確保されており、撮影場所や天候・気温等の付加情報を記録可能である。

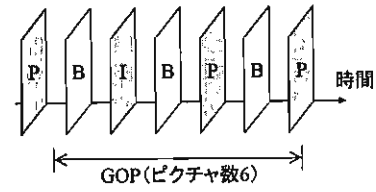

図 2. MPEG-1 の画像構成と GOP

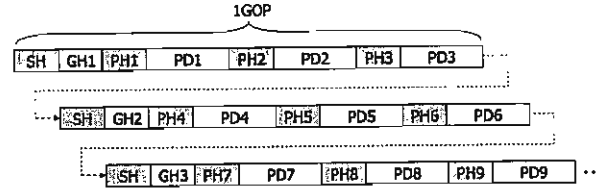

図 3. MPEG-1 の Video フレーム構成例

3.2. MPEG-1 への PIAT 適用

MPEG-1 への PIAT 適用を検討する。PIAT では、まず、部分データに分割するところから始まる。MPEG-1 のデータを抽出可能なように部分データに分割する場合、画像単位と GOP 単位が考えられる。しかし、フレーム間予測技術が用いられているため、P、B ピクチャ(PD)では、画像単位の独立性がなく、抽出が制限されることが考えられる。また、動画像データ全体の原本性保証を考えた場合、SH 等のヘッダ情報も含めて署名を付加する必要があると考えられる。そこで、本稿では、図 3のフレーム構成において、SH を先頭とし、次の SH が始まる直前の PD までを 1GOP とし、これを分割単位とする。更に、記録時間が長い動画像やフレームレートの高い動画像へ適用した場合の署名関連データ量の増大対策として、[15](以下、二分木手法)を利用する。なお、この署名関連データ量の削減手法・効果の詳細は、[9]を参照。

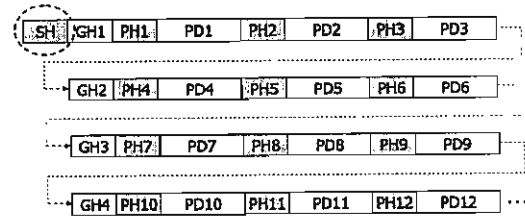

図 4. SH が付加されてない場合のフレーム構成例

また、図 3の MPEG-1 フレーム構成では、SH は全 GOP の先頭に付加されているが、SH は必ずしも GOP 毎に付加される必要がないため[1]、GOP 単位で見た場合、先頭 GOP に SH が付加されており、以降の GOP には SH が付加されていないフレーム構成も存在する(図 4)。

GOP が SH から始まる場合は、SH を検出することで GOP の開始と認識可能である。更に、GOP が GH から始まる場合でも、GH を検出することで GOP の開始と認識可能である。しかしながら、プライバシ保護のための切り出しを考慮すると、図 4のようなフレーム構成を持つ MPEG-1 への適用にはやや課題が残る。つまり、GH2～GH4 のいずれかで切り出されると、切り出された動画像が再生不能に陥る場合がある。これは、再生動作保証のために、先頭 GOP には必ず SH を含まなければならないという MPEG-1 規格の決まりがあるために生じる。

上記検討を踏まえ、2章の PIAT アルゴリズムを適用する。なお、動画像データの抽出が目的のため、本稿では、全データのうち連続するひとつの箇所の動画像を切り出すことを前提とする。以降、署名者が原本として扱う動画像データのことを原動画、抽出者が生成する動画像データのことを切り出し動画と記述する。

3.2.1. 原動画の署名生成方法

署名者は、原動画を GOP で分割し、署名時点では、どの位置で切り出されるかわからないため、SH が付加されていない GOP には直近の SH の内容を付与し、SH を含めた形で各 GOP のハッシュ値を計算。これらハッシュ値集合を用いて、二分木手法により、ひとつのルートハッシュ値を生成する。その後、生成したルートハッシュ値に対して、署名者の電子署名を生成し、ルートハッシュ値と電子署名をあわせて、署名者の PIAT 署名とする (図 5)。

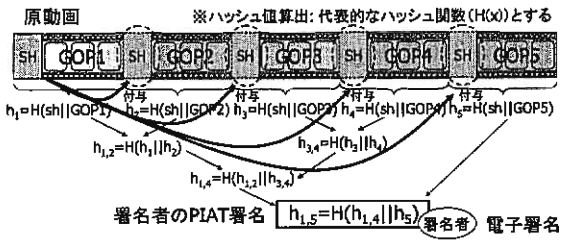

図 5. 原動画の署名生成方法

3.2.2. 切り出し動画の生成・署名生成方法

抽出者は、原動画から必要な部分を抽出し、切り出し動画を生成する。この時、切り出し動画が再生できない状態を回避するため、SH が付加されていない GOP には直近の SH の内容を付与し、SH を含めた形で切り出し動画を生成する(図 6)。この時、SH は、切り出し動画の実体に付加することで再生不能を回避する。また、切り出し動画の情報量削減のため、先頭 GOP のみ SH を付加する。

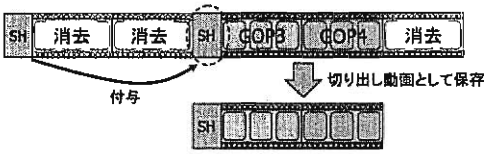

図 6. 切り出し動画の生成方法

続けて、原動画の署名生成同様に、消去部分に SH が付加されていない GOP には直近の SH の内容を付与し、SH を含めた形で各 GOP のハッシュ値を計算。抽出で消去する GOP だけからなる複数のルートハッシュ値(以下、消去ルートハッシュ値リスト)を生成する。更に、生成した消去ルートハッシュ値リストに対して、抽出者の電子署名を生成し、消去ルートハッシュ値リストと電子署名をあわせて、抽出者の PIAT 署名とする(図 7)。その後、切り出し動画と署名者、および抽出者の PIAT 署名を開示する。

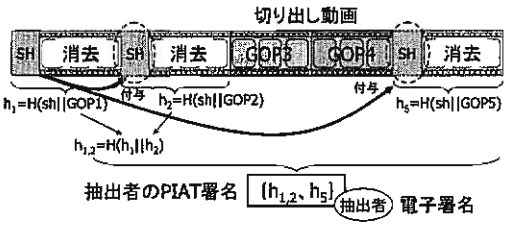

図 7. 切り出し動画の署名生成方法

3.2.3. 切り出し動画の署名検証方法

検証者は、開示された切り出し動画を用いて、SH が付加されていない GOP には直近の SH の内容を付与し、SH を含めた形でハッシュ値を生成する。続けて、抽出者の PIAT 署名に含まれる消去ルートハッシュ値リストと共に原動画のルートハッシュ値を復元し、署名者の PIAT 署名と比較・検証を行う(図 8)。一致していれば、原動画の一部であり、改変がないことを確認可能である。また、抽出者の電子署名を検証することで、誰が切り出しを行ったかを確認可能である。

図 17は、[10]で提案したプロトタイプによる切り出し動画の署名検証結果の画面である。この検証画面では、原動画のどの部分が切り出されたかを示す切り出し範囲と、切り出し動画の改変有無が明示される。

[1] MPEG-1 規格では、先頭 GOP に SH がひとつ付加されていれば、ストリーミングデータの再生は可能としている。

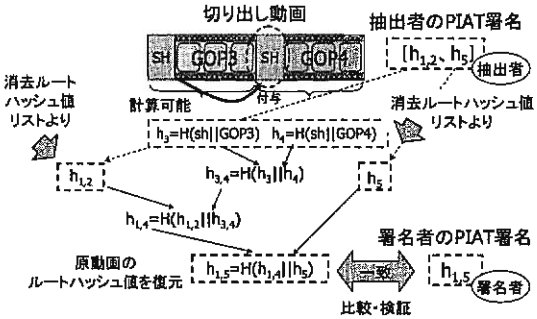

図 8. 切り出し動画の署名検証方法

3.3. 改良方式

3.3.1. 従来方式の課題

動画像・音声データの証拠性確保を実現する場合、コンテンツの原本性保証に加え、そのコンテンツがいつの時点で撮影・記録されたかについて言及される必要がある。しかし、3.2節の方式では、コンテンツ内における切り出し位置や範囲(フレーム時間)の特定は可能なものの、いつの時点で撮影・記録されたかを示す実際の時刻の特定までは考慮されていなかった。この対策として、撮影時刻の保証も同時に行うため、「いつ、何を」に対して証明可能なタイムスタンプの利用や、時刻配信機関から時刻情報を取得し、電子署名と共に保存することが考えられる。しかしながら、監視カメラ等では、24時間常時撮影等、長時間撮影が必要となり、検索性向上の観点から、記録映像を任意の単位(例えば、1時間単位と想定)で複数に分割して管理することが要求される。この場合、1 時間毎に時刻情報を取得しなければならず、コストがかかる。更に、次の 1 時間分の記録・保存が完了するまでに内部者や第三者による改ざんや中抜き等の不正が発生する可能性がある。また、過去に記録・保存された分についても、同様の脅威が発生する可能性がある。

3.3.2. 要件

上記課題の解決するため、以下 4 つの要件を満足する方式を検討する。

要件 1: 時刻配信機関が発行する時刻情報を記録開始時のみ取得し、原動画と関連付けて管理できること

要件 2: 記録映像を任意の単位で分割管理でき、その原本性、連続性、時系列性を保証できること

要件 3: 原動画、および切り出し動画の実時間の算出・確認が行えること

要件 4: 切り出し動画が正しく再生できることに加え、原動画の一部であり、改変がないことを保証できること

要件 4 については、[9],[10]で報告済みである。本稿では、要件 1～3 を中心に、動画像データの原本性、連続性、時系列性を考慮した任意分割生成方法と切り出し方法、および署名生成・検証方法について検討する。

3.3.3. 条件・前提

本節では、方式検討のための事前定義を行う。まず、ビデオカメラ等の映像記録端末が原動画を記録し、署名を付加する形態を考える。また、この映像記録端末は、時刻配信機関の専用サーバとインターネット等のネットワーク回線を通じて接続されていることを想定し、原動画の記録開始と同時に、時刻配信機関にアクセス。続けて、時刻配信機関によって保証されている時刻情報をリアルタイムに、かつ誤差なく受信・取得できること、また、記録された映像は任意の時間単位に分割して管理することを想定し、1 時間単位での保存を行うことを前提に検討を行う。

3.3.4. 原動画の生成・署名生成方法

本節では、3.3.2節で示した要件を満足するための、映像記録端末による原動画の任意分割生成方法、および任意分割された原動画の署名生成方法について述べる。本稿では、簡略化のために 5 つの GOP を 1 時間[2]と想定し、これら 5 つの GOP によりひとつの原動画が形成されるものとして述べる。

最初の 1 時間分の原動画 1 と、それ以降の原動画 2～N により、生成方法が異なる。まず、原動画 1 の記録開始と同時に、時刻配信機関から署名付き時刻情報を取得し、原動画 1 の SH 内に存在するユーザデータ領域(SHU)に格納する。SH は、再生等に必要なデータを格納する領域(SHM)と、ユーザが自由にデータを格納できる領域(SHU)に分かれ、本方式では、時刻配信機関から取得した署名付き時刻情報を SHU 内に格納する。続けて、SHU に格納された時刻配信機関の署名付き時刻情報を含む SH の内容を付与して、3.2.1節の方法で、映像記録端末の PIAT 署名(原動画 1 の PIAT 署名)を生成する(図 9)。

原動画 1 の記録完了と同時に、次の 1 時間分の原動画 2 の記録を継続する。この時、原動画 1 の SHM の内容を原動画 2 の SHM に継承・付与する。更に、直前の原動画 1 と時系列に連続(連結)していることを示すため、直前の原動画 1 の最後の部分情報に相当する GOP5 の内容から特徴値(例えば、GOP5 の内容から得られるハッシュ値等)を生成し、原動画 2 の SHU に格

[2] フレームレート=29.97 fps(frames par second)、1GOP あたり約 500 ミリ秒、1GOP に含まれるピクチャ数が 18 枚程度と想定すると、ストリーミングデータの生成条件によっても異なるが、1 時間分の実際の GOP 数は、おおよそ 6,000 個程度である。

納する。この時、連続性、時系列性を確保するための特徴値として原動画1のPIAT署名を用いてもよい。

続けて、原動画2のSHUに格納された特徴値を含めたSHの内容を付与して、3.2.1節の方法で、映像記録端末のPIAT署名(原動画2のPIAT署名)を生成する(図10)。以降の原動画についても、原動画2と同様の方法で順次生成する。図11は、原動画をN個に任意分割し、署名生成した後の保存形態を示している。

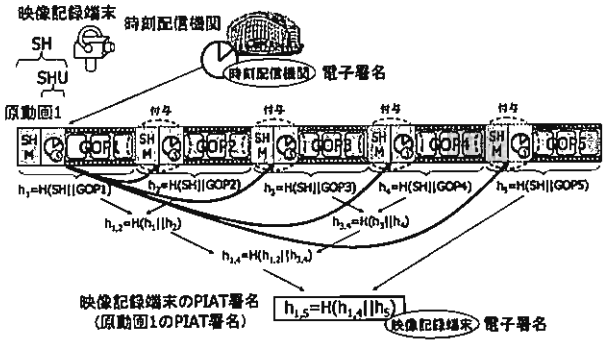

図 9. 原動画1の生成・署名生成方法

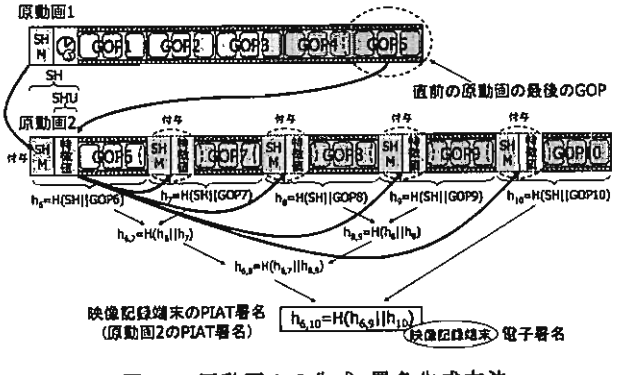

図 10. 原動画2の生成・署名生成方法

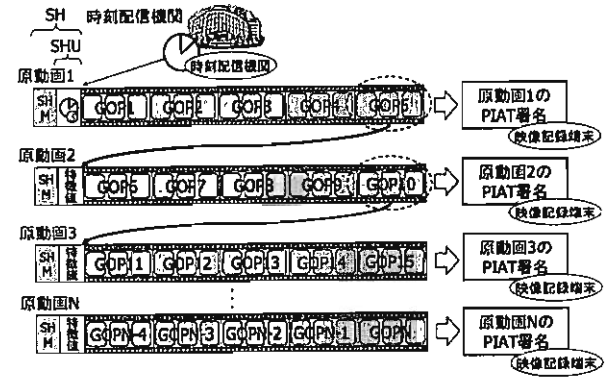

図 11. 原動画の任意分割保存形態

3.3.5. 切り出し動画の生成・署名生成方法

本節では、3.3.2節で示した要件を満足するための、抽出者による切り出し動画の生成方法、および署名生成方法について述べる。切り出し方法として、1つの原動画範囲内で完結する切り出しと、複数の原動画に渡る切り出しの2とおりの方法が考えられる。更に、原動画1を切り出すか、原動画2以降を切り出すかによってPIAT署名の生成方法が異なる。本稿では、図11で保存された原動画のうち、最も単純な、原動画2の中間部(GOP8,GOP9の2つのGOP)を切り出すことを想定して述べる。

まず、切り出し対象となる原動画2から切り出し範囲(GOP8,GOP9)を指定する。続けて、時刻情報が格納された原動画1のSHの内容を切り出し動画のSHとして継承・付与し、更に、原動画2のSHUに格納された特徴値の内容を継承・付与して、切り出し動画を生成する(図12)。この時、新たに生成された切り出し動画のSHUには、時刻配信機関の署名付き時刻情報、直前の原動画との連続性、時系列性を確保するための特徴値が格納される。

続けて、原動画2のSHUに格納された特徴値を含めたSHの内容を付与して、3.2.2節の方法で、抽出者のPIAT署名(切り出し動画のPIAT署名)を生成する(図13)。

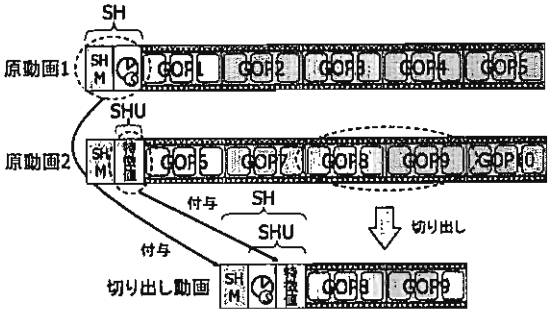

図 12. 切り出し動画の生成方法

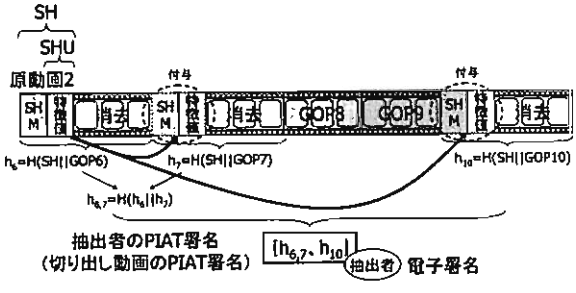

図 13. 切り出し動画の署名生成方法

図 14は、生成された抽出者の PIAT 署名の内容例を示している。切り出し動画に対する検証データとして、原動画の総 GOP 数(a)、切り出し開始位置の GOP 番号(b)、切り出し GOP 数(c)、切り出し動画の先頭 GOP が原動画 1 の先頭から数えて何個目の GOP に相当するかを示す累計 GOP 番号(d)、最後に消去ルートハッシュ値リストを順に記録する。また、上記検証データに対して抽出者の電子署名を付加する。

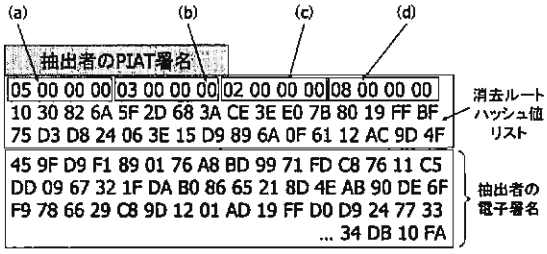

図 14. 抽出者の PIAT 署名の内容例

3.3.6. 切り出し動画の署名検証方法

本節では、3.3.2節で示した要件を満足するための、検証者による切り出し動画の署名検証方法について述べる。検証時には、切り出し動画、抽出者の PIAT 署名、原動画 2 の PIAT 署名の 3 つの情報を用いて、原動画の一部であり、改変がないことを検証する。続けて、SHU に記録された時刻情報から、切り出し動画に対する実時間の算出を行う。具体的には、切り出し動画の SHU に格納された時刻情報を除き、特徴値を含めた SH の内容を付与して、3.2.3節の方法で、原動画 2 のルートハッシュ値を復元し、原動画 2 の PIAT 署名と比較・検証を行う(図 15)。一致していれば、原動画の一部であり、改変がないことを確認可能である。また、抽出者の電子署名を検証することで、誰が切り出しを行ったかを確認可能である。

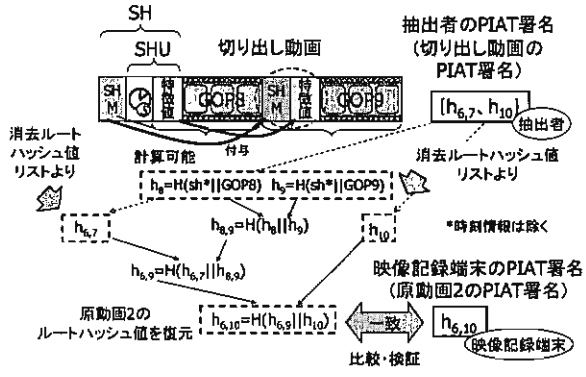

図 15. 切り出し動画の署名検証方法

続けて、抽出者の PIAT 署名に記録された情報(図 14 中、(b), (c), (d))を用いて、切り出し動画の実時間の算出を行う。具体的には、例えば、フレームレートが 29.97 fps とすると、原動画 1 の先頭 GOP に格納される最初のピクチャ(GOP1-P1)のフレーム時間を 0 秒とし、これを始点に GOP1-P2 のフレーム時間=1/29.97 秒、GOP1-P3 のフレーム時間=2/29.97 秒...と経過する。つまり、任意の GOP に格納されるピクチャ N のフレーム時間は、(N-1)/29.97 秒の計算式で算出することができる。よって、切り出し動画の先頭ピクチャ(GOP8-P1)は、原動画 1 の先頭ピクチャ(GOP1-P1)から数えて、152,848 枚目と想定すると、フレーム時間=152,847/29.97 秒と算出することができる。同様に、切り出し動画の最終ピクチャ(GOP9-PN)は、原動画 1 の先頭ピクチャ(GOP1-P1)から数えて、197,803 枚目と想定すると、フレーム時間=197,802/29.97 秒と算出することができる。

このフレーム時間の算出結果を参考にして、切り出し動画の開始実時間と終了実時間の算出を行う。例えば、時刻配信機関から取得した時刻情報が、2008 年 6 月 1 日 AM9:00:00.000 の場合、切り出し動画の開始実時間は、切り出し動画の先頭ピクチャ(GOP8-P1)のフレーム時間である 152,847/29.97 秒(5,100 秒=85 分)を加算し、2008 年 6 月 1 日 AM10:25:00.000 となる。切り出し動画の終了実時間も同様に、切り出し動画の最終ピクチャ(GOP9-PN)のフレーム時間である 197,802/29.97 秒(6,600 秒=110 分)を加算し、2008 年 6 月 1 日 AM10:50:00.000 となる。よって、2008 年 6 月 1 日 AM9:00:00.000 に映像記録が開始され、2008 年 6 月 1 日 AM10:25:00.000～2008 年 6 月 1 日 AM10:50:00.000 の約 25 分間の映像が切り出されたことを確認可能である(図 16)。

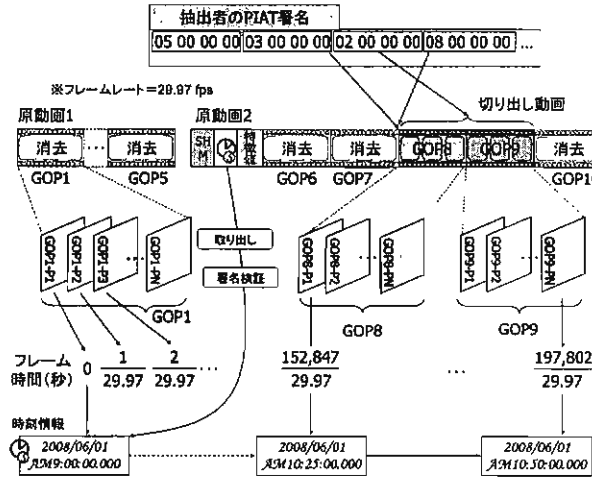

図 16. 切り出し動画の実時間の算出方法

3.4. 効果

本提案方式により、任意分割された動画像データに対してもPIAT署名の効果を実現できる。本提案では、時刻配信機関から取得した署名付き時刻情報と、直前の原動画の最後のGOPから生成した特徴値を、動画像に関連付けて管理することに加え、これら情報を含めてPIAT署名生成を行う方式を追加した。これにより、前回方式で実現した、プライバシ保護のための一部切り出しを行っても、切り出し箇所(位置)の検出、および切り出し動画の原本性検証が可能となる効果に加え、撮影時刻と連動した原本管理、ならびに動画像の原本性、連続性、時系列性を考慮した任意分割管理が可能となった。

4. まとめ

本稿では、任意分割されたMPEG-1形式の動画像データに対して、部分完全性保証技術(PIAT)を適用する方式について検討し、第三者が保証する時刻情報と連動させ、任意分割された動画像・音声データの原本性、連続性、時系列性を保証可能な改良方式について提案した。本提案方式を用いれば、任意分割された動画像・音声データにも適用でき、監視カメラ等の実際のシステムで、高い証拠性と利便性を備えた証跡管理が可能となる。

文　献

[1] PFU,"コールセンターにおける商品販売(音声データの存在・原本証明)", http://www.pfu.fujitsu.com/tsa/casestudies/case2.html

[2] 有限会社シーモス,"通話録音製品(テレコーダー)","http://www.999.co.jp/telecoder/index.html

[3] ユビキタスセンサーネットワーク技術に関する調査研究会,"ユビキタスセンサーネットワークの実現に向けて最終報告, 参考6 監視カメラ設置とプライバシ問題,"2004. Available at http://www.soumu.go.jp/s-news/2004/pdf/040806_4_b2_s6.pdf

[4] R. Steinfeld, L. Bull, and Y. Zheng. "Content Extraction Signatures," In International Conference on Information Security and Cryptology ICICS2001, LNCS 2288, pp. 285.304, 2001.

[5] 宮崎, 須崎, 岩村, 松本, 佐々木, 吉浦,"電子文書墨塗り問題,"電子情報通信学会技術研究報告書, ISEC2003-20, pp.61-68, 2003.

[6] 吉岡, 武仲,"電子文書の訂正・流通を考慮した部分完全性保証技術の提案,"第3回情報科学技術フォーラム(FIT 2004), M-066, pp.231-232, 2004.

[7] T. Izu, N. Kanaya, M. Takenaka, T. Yoshioka, "PIATS:A Partially Sanitizable Signature Scheme," In International Conference on Information Security and Cryptology ICICS 2005, LNCS 3783, pp.72.83, 2005. (Preliminary version was published at CSS 2004.)

[8] 武仲, 吉岡,"画像ファイルに対する部分完全性保証技術の実現,"電子情報通信学会技術研究報告書,ISEC2005-69, pp.183-188, 2005年7月.

[9] 吉岡, 武仲, 伊豆,"部分完全性保証技術 PIAT: 動画像・音声への適用,"暗号と情報セキュリティシンポジウム SCIS 2007, 1B2-2, 2007年1月.

[10] 吉岡, 武仲, 大橋, 山下,"動画像・音声データに対する部分完全性保証技術 PIAT の実現,"暗号と情報セキュリティシンポジウム SCIS 2008, 1D1-1, 2008年1月.

[11] 伊豆, 金谷, 武仲, 吉岡,"墨塗り者を特定可能な墨塗り署名方式,"情報処理学会論文誌, Vol. 48, No. 9, pp.2957-2965, September 2007.

[12] "Coding of moving pictures and associated audio for digital storage media at upto about 1.5 Mbit/s — Part 2 : Video," International Standard ISO/IEC11172-2, 1993.

[13] "Coding of moving pictures and associated audio for digital storage media at upto about 1.5 Mbit/s — Part 3 : Audio," International Standard ISO/IEC11172-2, 1993.

[14] マイクロソフト株式会社, "マルチメディアプログラマーズガイドマイクロソフトウィンドウズソフトウェア開発キット," 翔泳社, 1993.

[15] A. Menezes, P. Oorschot, and S. Vanstone,"Handbook of Applied Cryptography, 13.4.1 Authentication Tree," pp.556-559,CRC Press, 1997.

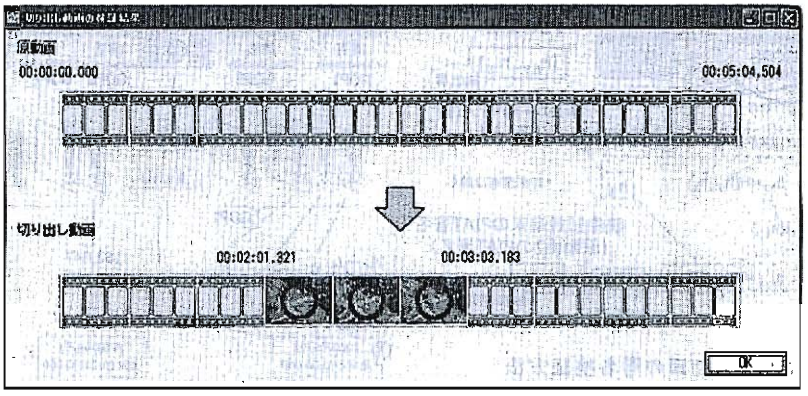

図 17. 切り出し動画の署名検証結果画面