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

2005－ＣＳＥＣ－30 (61)
2005／7／22

画像ファイルに対する部分完全性保証技術の実現

武仲 正彦† 吉岡 孝司†

†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: †{takenaka, yoshioka}@labs.fujitsu.com

あらまし JPEG 等の圧縮画像ファイルに対する部分完全性保証技術を実現したので報告する。本技術は、我々が FIT2004 等で提案した電子文書の訂正・流通を考慮した部分完全性保証方式を画像に対して適用したもので、画像への墨塗りを行っても、それ以外の部分の完全性を保証可能である。また、我々は本技術のプロトタイプを作成した。それを用いて実際にスキャナから取り込んだ画像に署名を行い、墨塗りを行うと、墨塗り箇所が検出でき、それ以外の部分の完全性を保証できることを実証した。

キーワード JPEG，部分完全性保証技術，墨塗り，署名

An Implementation of Partial Integrity Assurance Technology for Image Data

Masahiko TAKENAKA† Takashi YOSHIOKA†

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

Abstract We report that the Partial Integrity Assurance Technology (PIAT), proposed in FIT2004 by us, can be applied to compressed image files such as JPEG. In this paper, we propose the technology for the assurance of partial integrity of the image data. And even if the part of the image is changed or is sanitized, the integrity of the other parts can be assured. In addition, we implement a prototype of this technology. Images that are put on a paper scanner are signed with our prototype, and a part of the image is sanitized. Therefore, we can detect and indicate the changed part and can confirm constancy in other parts.

Keyword JPEG, Partial Integrity Assurance Technology, Sanitize, Signature

1. はじめに

2005 年 4 月に個人情報保護法と e-文書法が施行された。個人情報保護法は、個人の同意無く、収集した目的以外での個人情報の利用を厳しく制限する法律で、5000 人分を越える個人情報を扱う事業者は、規制の対象となる。また、個人情報保護法では、本人の求めに応じて情報の開示を行わなければならない。さらに公的機関では情報公開法により、公開要求があれば個人情報等のプライバシ情報や機密情報を除いて情報の公開を行わなければならない。

一方 e-文書法は、従来、紙で保存しなければならなかった一部の文書が、スキャナによる取り込みと電子署名、タイムスタンプを付加することで、電子文書として保管が可能となった。

これらの法律の施行により、今後発生しうる事例として、スキャナで取り込んで電子化したファイルの個人情報部分を削除して公開するということが考えられる。しかし、現在の e-文書法では取り込んだデータ全体に電子署名とタイムスタンプを施すため、個人情報部分の削除を行うとデータの改竄となり署名、タイムスタンプ共に無効となってしまう。その場合、個人情報部分の削除と同時にその他の部分を変更（改竄）することはきわめて容易で、且つ紙文書と異なりその検出は困難である。

そのため、スキャナで取り込んだ電子データの一部分を改変・削除するとその部分が変更されたことが識別可能で、その他の部分の完全性・原本性が保証できるような技術が必要となると考えられる。

本論文では、スキャナで取り込んで電子化した圧縮画像ファイル、特に JPEG[1]ファイルに対して、部分完全性保証技術（PIAT）[2][3][4]を適用する方法を提案する。また、スキャナで取り込んだ JPEG ファイルに対して、PIAT で署名、署名確認を行うプロトタイプを作成することで実現可能性検証を行う。さらに、このプロトタイプツールを実際に使用して、提案方式の評価と問題点を検討する。

2. 関連研究

XML 等の電子文書に対して部分的な完全性・原本性を保証する技術は、CES（Content Extract Signature）

[5][6]や電子文書の墨塗り技術（SUMI-1～5）[7][8]、部分完全性保証技術（PIAT）等として以前から研究されてきた。これらの技術では、部分的な変更・削除・墨塗りを行ってもそれ以外の部分の完全性を保証可能である。また、電子文書墨塗り技術（SUMI-4）を画像ファイルへ適用する方法について検討されている[9]。本章では、本論文で使用する PIAT と、画像ファイルの墨塗り技術[9]について簡単に紹介する。

2.1. 電子文書の部分完全性保証技術（PIAT）

PIAT は我々が FIT2004, CSEC2004-7, SCIS2005 で提案した XML 等の電子文書に対して部分的な完全性を保証する技術である。PIAT で XML 文書を署名、訂正・墨塗り、署名確認する場合の一例を示す。PIAT の詳細については、文献[2][3][4]を参照。

署名:

XML タグ毎に乱数を追加し、これを第 1 版の文書とする。次に各タグのハッシュ値を計算し、それらのハッシュ値に電子署名を行い、別ファイルに格納する。これを第 1 版の PIAT 署名とする。第 1 版の文書と PIAT 署名をペアで保存する。

変更・墨塗り:

第 1 版文書の任意の箇所を変更し、そこに対応するタグの乱数も変更する。これを第 2 版文書とする。そして署名時と同様の処理で第2版の PIAT 署名を行う。そして、第 2 版の文書と PIAT 署名、第 1 版の PIAT 署名を公開する。

署名確認:

まず第 1 版と第 2 版の PIAT 署名の電子署名をそれぞれ確認する。次に、第 2 版の文書から生成したハッシュ値と第 2 版の PIAT 署名のハッシュ値が一致するか検証を行う。さらに、第1版と第 2 版の PIAT 署名を比較し、変更・墨塗り箇所を特定する。これにより、第 1 版の文書を公開せずに第 2 版の変更箇所を確認することが可能となる。

PIAT の適用対象は XML 等の電子文書に限らず、電子データ一般に適用可能である。しかし、一般の電子データに適用する場合は、そのデータのフォーマットを解析し、XML 適用時のタグのような「部分」を識別する必要がある。

2.2. 画像データの墨塗り技術

スキャナで取り込んで電子化したデータは JPEG 等の圧縮画像フォーマットに変換される場合が多い。これに部分的な完全性を保証する技術を適用する場合、圧縮伸張後にフォーマット解析を行う必要がある。文献[9]で秦野等は、JPEG ファイルのフォーマットを解析し、電子文書の墨塗り技術を適用する方法を検討している。JPEG ではビットマップ画像を矩形に分割して処理を行っているため、これを「部分」の単位とすることが考えられる。しかし JPEG フォーマットではこれらの複数のブロックに対してエントロピ圧縮処理を行ってデータを保持するため、単純に墨塗り技術を適用することはできない。そこで文献[9]ではエントロピ圧縮伸張後のデータに対して墨塗り技術（SUMI-4）を適用する方法が提案されている。

しかし、文献[9]の方式では、エントロピ圧縮伸張後のデータ（中間データ）の置き換えを行う必要があるなど、複雑な墨塗り処理、検証処理を必要とする。

3. JPEG への部分完全性保証技術の適用

本章では JPEG ファイルへの PIAT 適用について述べる。本論文では、JPEG ファイルの最も単純な構造に対して PIAT の適用方法を示すが、それ以外の構造に対しても、PIAT は容易に適用可能である。

3.1. JPEG

JPEG の圧縮方式やフォーマットには様々なものがあるが、本論文では単純化のために、基本 DCT 方式を使用した JFIF[10]フォーマットを前提とし、縦横と輝度対色差のサンプリングファクタを 2:1 に固定、リスタートインターバルを無効、サムネイル不使用のデータ形式を利用する。これ以降対象とするフォーマットを単に JPEG と記述する。

図 1に JPEG データの構造を示す。図 1においてMCU（最小符号化ユニット）が画像の 1 ブロックにあたる。MCU フォーマットと画像の関係を図 2に示す。図 2では、画像の 16×16 ドットを 1 つの MCU が構成し、1 つの MCU は 8×8 ドットの輝度・色差成分 6 個から構成される。これは、色差成分を間引くことでデータ量を圧縮しているためである。

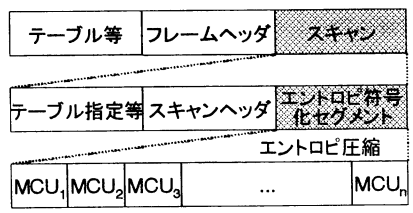


図 1. JPEG のデータ構造

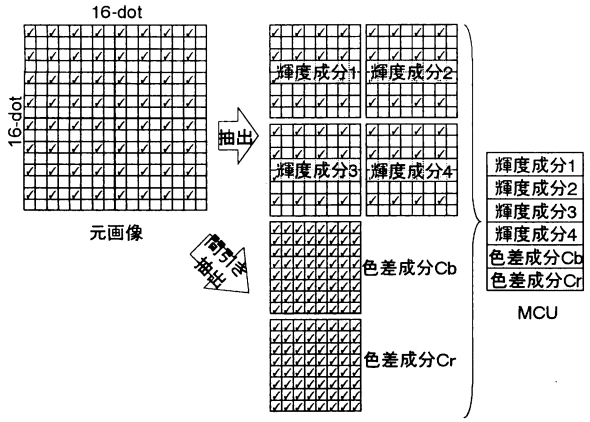


図 2. MCU の構造と画像の関係

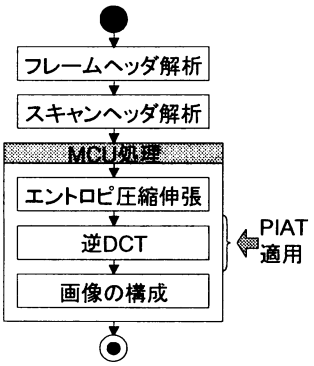


図 3. JPEG のデコードプロセス

3.2. JPEG 画像への PIAT 適用

JPEG へ PIAT を適用する。図 3に JPEG のデコードプロセスを示す。図 1に示すように JPEG ファイルでは複数の MCU がエントロピ圧縮されて格納されている。そのため、MCU 単位や輝度・色差成分単位で完全性保証を行うには、図 3のエントロピ圧縮伸張後に PIAT を適用する。以下に JPEG 画像に対する PIAT を適用する方法の一例を示す。(図 4参照)

署名:

JPEGファイルを第1版の画像とする。これに対し、エントロピ圧縮伸張を行い、輝度・色差成分を抽出する。そして各成分に対してハッシュ値を計算し、それらのハッシュ値に電子署名を行い、別ファイルに格納する。これを第 1 版の PIAT 署名とする。第 1 版の画像と PIAT 署名をペアで保存する。

変更・墨塗り:

画像エディタ等で第 1 版文書の任意の箇所を変更・墨塗りする。これを第 2 版の画像とする。そして署名時と同様の処理で第 2 版の PIAT 署名を行う。そして、第 2 版の画像と PIAT 署名、第 1 版の PIAT 署名を公開する。

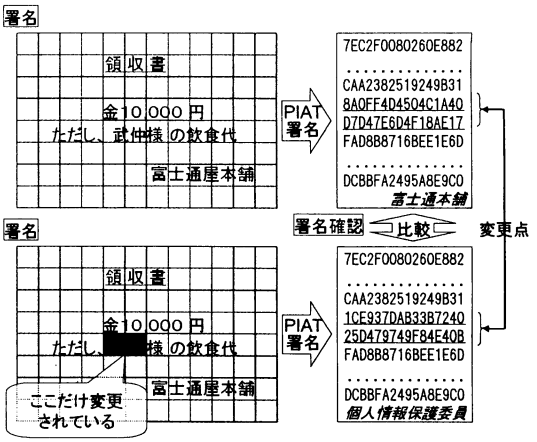


図 4. JPEG の PIAT 署名・墨塗り・署名確認

署名確認:

まず第 1 版と第 2 版の PIAT 署名の電子署名をそれぞれ確認する。次に、署名時と同様の処理で第 2 版の画像から生成したハッシュ値と第 2 版の PIAT 署名のハッシュ値が一致するかを検証する (第 2 版の PIAT 署名確認)。さらに、第 1 版と第 2 版の PIAT 署名を比較し、変更・墨塗り箇所を特定する。これにより、第 1 版の画像を公開せずに第 2 版の変更・墨塗り箇所を確認することが可能となる。

3.3. 効果

提案方式により、画像に対しても PIAT 署名の効果を実現できる。提案方式では、XML 文書に対する PIAT 署名と同様に、墨塗り時に墨塗り箇所の特定と、それ以外の部分の完全性保証が可能となる。また墨塗り者は PIAT 署名に対する電子署名から明らかとなるため、仮に墨塗り者が墨塗り以外の修正を行った場合でも、その追跡が可能である。

4. 試験実装

プロトタイプ実装により本方式の実現可能性検証を行った。文献[11]のサンプルプログラム JPEG_reader を改造して PIAT 署名作成と PIAT 署名検証機能を追加した。これらの機能の実装において、Hash 関数に MD5、署名に RSA を使用した。

4.1. PIAT 署名機能の実装

JPEG_reader の JPEG でコード処理部の改造を行った。エントロピ圧縮伸張後、輝度・色差成分毎にハッシュ値を計算する機能を追加した。作成したハッシュ値は署名ファイル（画像ファイル名.PIAT）に出力し、全てのハッシュ値が出力された後に RSA 署名を付加する。

4.2. PIAT 署名確認機能の実装

提案方式では本来、墨塗り画像およびその署名と原本の署名の 3 つを比較して署名検証を行う。しかしプロトタイプでは、簡単化のために署名確認時に第 1 版と第 2 版の署名を確認することはせずに、第 2 版の画像と第 1 版の署名ファイル（第 2 版の署名ファイルとしてコピーしたもの）との比較を行っている。署名機能と同様に第 2 版の画像のエントロピ圧縮伸張直後に輝度・色差の成分毎にハッシュ値を作成し、それを署名ファイル内のハッシュ値と比較する。もし画像のハッシュ値とファイルのハッシュ値が等しければ、そのブロックはそのまま表示する。もしそれらの 2 値が異なっていれば表示画像に重ねて「×」を表示する。

5. 評価と問題点

実際にスキャナから取り込んだ画像に対して、プロトタイプで PIAT 署名・署名確認を行うことで、試験実装を評価、問題点の抽出を行った。

5.1. 試験実装の評価

まず、以下の 3 種類の画像と PIAT 署名を作成した。（図 5, 図 6, 図 7左側参照）

1. ScanSnap （e-文書法対応）[12]で領収書のスキャンを行い、JPEG ファイルを作成する。その JPEG 画像に本方式で PIAT 署名を行う。
2. 1.の JPEG 画像を Windows Bitmap （BMP ファイル）に変換し、個人情報（個人名）部分に Windows 標準添付の画像ツールであるペイントで墨塗りを行った後、JPEG ファイルとして保存する。1.の PIAT 署名を本画像の PIAT 署名としてコピーする。
3. 2.と同様の方法で、領収書の個人情報の墨塗りに加えて、金額を修正する。その後 JPEG 画像で保存、1.の PIAT 署名を本画像の PIAT 署名としてコピーする。

次にこれら 3 種類の画像に対して PIAT 署名検証を行った。（図 5, 図 6, 図 7右側参照）

1. 全ての部分で署名検証に成功する。その結果、検証画像は通常の表示と同じで、何処にも「×」は表示されない。
2. 墨塗りした部分にだけ「×」が表示される。
3. 墨塗りした部分と修正した金額部分に「×」が表示される。

以上のように本方式では、墨塗り部分と金額の修正部分が明示されるので、墨塗り以外の改竄が検出可能であることが実証できた。また墨塗り者は PIAT 署名に施された電子署名から明らかとなるため、墨塗り以外の修正を行った者の追跡も可能である。さらに、墨塗りを一般の画像エディタで簡単に行える。

5.2. 問題点・課題

評価の結果、いくつかの問題点が明らかとなった。これらの解決は今後の課題である。

JPEG の直接編集を行うと全体の変更と検出

評価画像 2 の作成方法では、JPEG 画像を一旦 BMP に変換している。これは、直接 JPEG 画像を画像エディタで開いて墨塗りを行うと、PIAT 署名検証で画像全体が変更されたと判断されてしまうためである。原因としては正規化の誤差や正規化テーブルの変更等が考えられる。

JPEG ヘッダの変更の検証を行っていない

今回試験実装に利用したサンプルプログラムはヘッダ部分のテーブルを固定している。しかし、一般的にはこれらのテーブルは可変であり、正規化テーブル等が変更された場合、PIAT 署名検証で差異が無くても、画像としては全く異なる場合がありうる。

署名サイズが大きい

JPEG は非常に圧縮効率のよいフォーマットであるが、PIAT 署名データはハッシュ値で構成されるため圧縮が不可能である。そのため画像ファイルの種類にもよるが、評価データの場合、PIAT 署名ファイルは JPEG ファイルのサイズ 3 倍程度となってしまう。これに対する改良案としては、成分単位で署名を行わず、MCU 単位とすることで、PIAT 署名データ量を 1/6 程度とすることが可能である。また複数の MCU を単位とするとさらに PIAT 署名データ量が削減できる。

6. まとめ

本論文では、スキャナで取り込んだ JPEG 等の圧縮画像に対して、部分完全性保証技術（PIAT）を適用する方法を提案した。提案方式では、画像に対して PIAT の効果を適用できた。画像に対して PIAT 署名を施すことで、墨塗り時に墨塗り箇所の特定と、それ以外の部分の完全性保証が可能となった。また墨塗り者は PIAT 署名に対する電子署名から明らかとなるため、仮に墨塗り者が墨塗り以外の修正を行った場合でも、その追跡が可能である。

さらに、スキャナで取り込んだ JPEG ファイルに対して、PIAT で署名・署名確認を行うプロトタイプツー

ルを作成し、実際にスキャナで取り込んだ JPEG ファイルに使用して、提案方式の評価と問題点を検討した。その結果、提案方式では、墨塗り部分と金額の修正部分が明示されるので、墨塗り以外の改竄が検出可能であることが実証できた。さらに、墨塗りを一般の画像エディタで簡単に行えることも検証できた。

文　献

[1] ISO/IEC 10918-1, "Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines," 1994

[2] 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," FIT2004, M-066, 2004.

[3] 武仲, 吉岡, 金谷, "検証者が署名者と墨塗り者を識別可能な電子文書の墨塗り方式," CSS2004, pp. 475-480, 2004.

[4] 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方式の改良," SCIS2005, pp. 421-426, 2005.

[5] R. Steinfeld, L. Bull, Y. Zheng, "Content Extraction Signatures", ICISC 2001, LNCS 2288, pp.285--304, 2001.

[6] L. Bull, P. Stanski, D.M. Squire, "Content extraction signatures using XML digital signatures and custom transforms on-demand", WWW2003, pp.170-177, 2003.

[7] 宮崎, 洲崎, 岩村, 松本, 佐々木, 吉浦, "電子文書墨塗り問題," 信学技法, ISEC2003-20, pp.61-67, 2003.

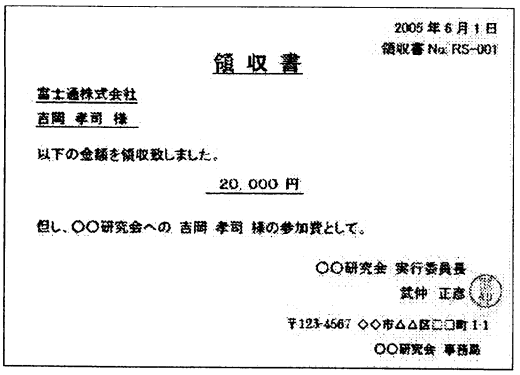
[8] 宮崎, 岩村, 松本, 佐々木, 吉浦, 手塚, 今井, "開示条件を制御可能な電子文書墨塗り技術," SCIS2004, pp.515-520, 2004.

[9] 秦野, 宮崎, "電子文書墨塗り技術の画像ファイルへの適用に関する一考察," SCIS2005, pp. 577-582, 2005.

[10] Eric Hamilton, "JPEG File Interchange Format Version 1.02," 1992, http://www.w3.org/Graphics/JPEG/jfif3.pdf

[11] 橋本晋之介, "JPEG 概念から C++での実装まで 第2版," ソフトバンクパブリッシング,2005.

[12] 富士通, カラーイメージスキャナ ScanSnap, http://scansnap.fujitsu.com/jp/



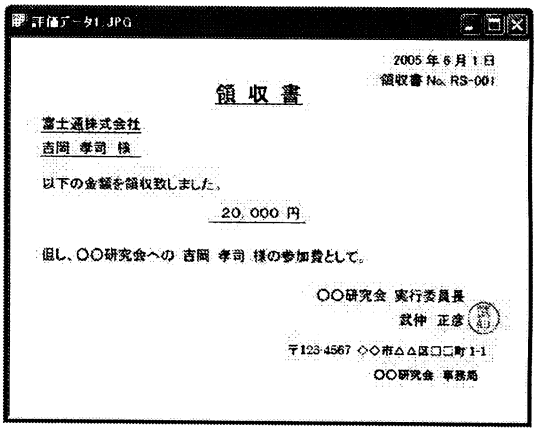


図 5. スキャナで取り込んだ領収書画像とその PIAT 署名検証画面

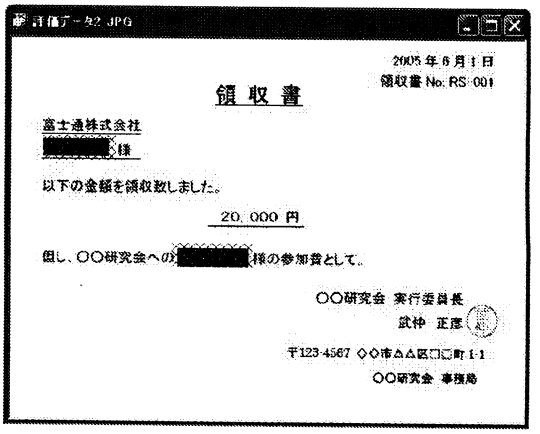


図 6. 個人情報に墨塗りをした証明書画像とその PIAT 署名検証画面

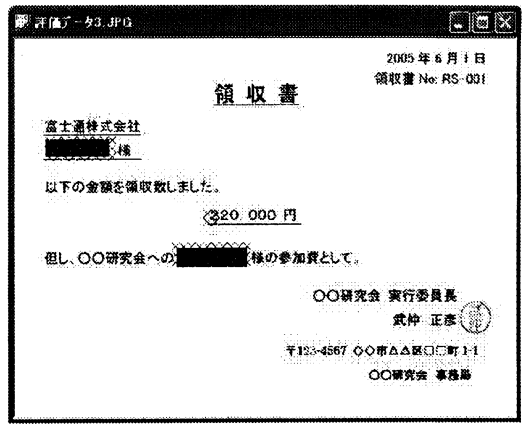


図 7. 個人情報の墨塗りに加え金額を訂正した証明書画像とその PIAT 署名検証画面