コンピュータセキュリティ 3－6
（1998. 11. 27）

電子透かしの理論的枠組に関する一考察

野見山 寛之　　満保 雅浩　　静谷 啓樹

東北大学大学院情報科学研究科
〒980-8576 仙台市 青葉区川内

Abstract

従来の電子透かし法が持っていた否認不可に係わる問題を解決するために、非対称電子透かし法が考案され、理論的な定義と、その具体的な構成例が示されている。しかし、最初に提案された非対称電子透かし法にはサーバの不正の余地が残されており、完全に安全だと言い切れないことが指摘されている。これに対応して、サーバの不正への対策を意図した具体的な電子透かし法が幾つか提案されている。

ところが、非対称電子透かし法の定義自体の矛盾はまだ修正されていないため、本論文では、この修正を行う。加えて、今までに見過ごされているサーバの不正が存在することを指摘し、その一解決策を示す。このサーバの不正は、著者の知る限りにおいて、サーバの不正を考慮した各種の方式を含む、既存の全ての方式に共通に存在する不正である。

A Study on the Theoretical Framework of Digital Watermarking

Hiroyuki Nomiyama　　Masahiro Mambo　　Hiroki Shizuya
Graduate School of Information Sciences, Tohoku University
Kawauchi Aoba Sendai, 980-8576 Japan

Abstract

In order to solve the problem of non-repudiation in ordinary fingerprinting, asymmetric fingerprinting has been introduced in [10], and its definition and concrete examples are shown. However, it is pointed out in [8] that concrete asymmetric fingerprinting schemes shown in [10] have a problem of server's deviation. Accordingly, several concrete asymmetric fingerprinting schemes supposedly solving this problem have been proposed in [10] and other papers. In this paper, we change a part of the definition of asymmetric fingerprinting in [8] since it is not well defined on the buyer's security. Moreover, we point out that there is a server's deviation overlooked in the previous papers, and show a scheme secure against the deviation.

1 はじめに

近年, 計算機の計算能力の向上とネットワークの発達に伴い、電子産業は活況を呈している。誰もが安価なコンピュータを購入できるようになり、ネットワーク上のディジタルコンテンツが充実してきていることも、電子産業が発展する原因となっている。この様な状況において、ネットワークを利用したディジタルコンテンツの取引が盛んに行われている。

本などの印刷物と異なり、画像やソフトウェア、文書などのディジタルデータはコピーが簡単にできるという特徴を持ち、不正コピーの問題がある. ディジタルデータを入手した正規購入者は、コピーを行うことにより、ディジタルデータを不特定多数に容易に配布できてしまう。そこで、不正コピーを抑止するために、電子透かし法 (Watermarking) が盛んに研究されている [11, 1, 2, 10, 4]。

電子透かし法は、当初、透かしの埋め込みと検出の両方に同一の秘密情報を利用することが一般的であった [11, 1, 2, 4]。しかし、この種の電子透かし法では、不正コピーと疑わしきディジタルデータをみつけたとしても、正規購入者がデータを横流したのか、サーバが故意に不当なデータを作り出したのか判別が付かない。よって、(a) 購入時には購入者のみが透かしの埋め込まれたデータを入手でき、(b) もし、サーバが透かしの埋め込まれたデータを入手できると、購入者を特定でき、第三者に対して、特定された購入者がデータを購入したことを示せるという性質を持つ非対称な電子透かし法が必要なことが指摘され、非対称電子透かし法の理論的な定義と具体的な構成例が示された [10]。

しかし、非対称電子透かしを理論的に考察したこの文献 [10] にはサーバの不正の余地が残されており、完全に安全であるとは言い切れないことが文献 [8] で指摘されている. このため、文献 [8] やその後の文献の幾つか [5] では、サーバの不正への対策を意図した電子透かし法が提案されている。

これらいずれの文献においても文献 [10] で提示された定義自体の矛盾を修正していないため、本論文では、文献 [10] の定義の修正を行う。加えて、今までに見過ごされているサーバの不正が存在することを指摘し、その一解決策を示す。このサーバの不正は、著者の知る限りにおいて、サーバの不正を考慮した各種の方式を含む、既存の全ての方式に共通に存在する不正である。

2 語句の解説

電子透かし法: 電子透かし法の用途には、所有権の主張 (Ownership assertion)、フィンガープリンティング (Fingerprinting)、作成者の認証と不変性の確認 (Authentication and integrity verification)、内容のラベル付け (Content labeling)、使用法の制御 (Usage control)、内容の保護 (Content protection) が挙げられる [7]。用途に依存して、方式も異なり、必ずしも全ての用途に利用できる方式が存在する訳ではない。

フィンガープリンティングとは、第 1節で述べたディジタルデータの不正コピーの抑止を目的とした方式を指す。本論文では不正コピー対策について取り扱うため、電子透かし法と表現した場合は、フィンガープリンティングを指すこととする。

否認不可署名: 否認不可署名 (Undeniable digital signature)[3] では、署名の正当性確認を署名のみでは行えず、署名者にゼロ知識証明を用いて証明してもらわなければいけない。このため、署名者が署名の正当性を示す相手を選択できる。署名者が自己のものでないと主張した場合には、不当な署名であることをゼロ知識証明を用いて証明してもらう。

非転移署名: 非転移署名 (Non-transitive digital signature)[9] では、否認不可署名と同様に、(i) 署名者本人のみが自己のメッセージの正当性を証明でき、否認不可署名と異なり、(ii) 署名の検証者はメッセージの出所を証明できない。否認不可署名にプライバシー保護機能を加えたものともみなすことができる。

3 非対称電子透かしの定義

文献 [10] において、非対称電子透かしは、鍵生成プロトコル key_gen、フィンガープリンティング・プロトコル $fing$、ユーザ特定用のプロトコル $identify$、論争解決用のプロトコル $dispute$ の 4 つのプロトコル $(key_gen, fing, identify, dispute)$ から構成されると定義される。安全性に関しては、ディジタルデータの品質に関する条件、サーバの安全性と購入者の安全性について、定義がなされている。定義の詳細は省略するが、定義で利用さられた記号を以下に用いるので、これらの記号の意味は文献 [10] を参考して下さい。

安全性の定義のうち、購入者の安全性についての定義が十分でない。文献 [10] において、購入済みの Pic_{bought} に対して、本来あるべき値と異なる $text(, proof(forpk_B))$ を付けられないとして購入者の安全性を定義している。しかし、実際には未購入の Pic_{bought} に対しても、$text(, proof(forpk_B))$ および $text(, proof(forotheruser))$ を付けられないとして考察しなければいけない。

4 サーバの不正

サーバの不正を考慮した電子透かし方式が幾つか提案されているが、いずれも以下の不正への対策が施されていない。

- サーバが正当なユーザにディジタルデータの検査を申し出て、署名などの所有権に関する証明を得た後に、別のユーザから不正なディジタルデータを発見したとして、罪を擦り付ける行為。

5 プロトコル

1. ユーザがサーバにディジタルデータ A を要求. この内容に対してユーザは ID をもとにした否認不可署名 id_U を生成し, id_U が否認不可署名であることをサーバに示し, id_U をサーバへ送る.
2. サーバは id_U の確認後, ユーザ名 U_{name} を生成し, ディジタルデータ A に U_{name} と id_U を s_{embed}S を使って埋め込み, A_W としてユーザへ送る. その際, $s_{extract}$ を生成しユーザへ送る.
3. ユーザは受けとった A_W と $s_{extract}$ を使って, A_W に id_U とユーザ名 U_{name} が埋まっていることを確認し, その後それを受理する.

ただし, 埋め込みはサーバのみが可能だとする. また, $s_{extract}$ の計算もサーバのみが可能とする.

検証

では, このプロトコルでの検証部分について述べる. (表 1)
ここで T とは検証対照者 U と U_{name}, id_U が一致することを示し F は一致しないことを示す.

不正についての考察

サーバが A_W を生成しユーザ U へ罪を擦りつける　サーバが A_W を生成できるのは当然であり, A_W がサーバの所にあれば, サーバの不正になる.

場合	U_{name}	id_U	判定	証明すること
A	T	T	不正なし	U は id_U が U の署名であることを証明
B	T	F	サーバの不正	U は id_U が U の署名でないことを証明
C	F	T	サーバの不正	U_{name} と実際の ID との比較 U は id_U が U の署名であることを証明
D	F	F	ユーザの不正	U_{name} と実際の ID との比較 U は id_U が U の署名でないことを証明

表 1: 検証方法

サーバが A_W を生成し他のユーザ U'へ配布する　ユーザ U'への配布時にプロトコルの step 3 にてチェックが可能であり, この不正は未然に防ぐことが可能.

ユーザ U が他の U'へ配布　これは表 1の場合 D にあたる.

ユーザ U がユーザ U'になりすます　$id_{U'}$ が生成不可能 (否認不可署名のプロトコルを実行したところでチェックが可能)

今回示した方式で非転移署名を利用すると、シュミレートできる署名しか受け取ることができないので、方式が成立しなくなるので、注意が必要である。

6　まとめ

非対称電子透かし法の定義自体に修正すべき点があることを指摘した。加えて、今までに見過ごされているサーバの不正が存在することを指摘し、その一解決策を示す。このサーバの不正は、著者の知る限りにおいて、サーバの不正を考慮した各種の方式を含む、既存の全ての方式に共通に存在する不正である。

参考文献

[1] G.R. Blakley, C. Meadow, G.B. Purdy, "Fingerprinting Long Forgiving Messages," Crypto'85, LNCS 218, Springer-Verlag, pp.180-189, 1986.

[2] Dan Boneh, James Shaw, "Collusion-Secure Fingerprinting for Digital Data," Crypto '95, LNCS 963, Springer-Verlag, pp.452-465, 1995.

[3] David Chaum, "Zero-Knowledge Undeniable Signatures," Eurocrypt'89, LNCS 473, Springer-Verlag, pp.458-464, 1991.

[4] Ingemar J. Cox, Joe Kilian, Tom Leighton, Talal Shamoon, "A Secure, Robust Watermarking for Multimedia," Information Hiding, LNCS 1174, Springer-Verlag, pp.183-206, 1997.

[5] 岩村 恵市, 桜井 幸一, 今井 秀樹, "ブラインド電子透かしの提案," 電子情報通信学会技術研究報告 ISEC97-35, pp.63-74, 1997.

[6] 岩村 恵市, 山口 和彦, 今井 秀樹, "公開抽出情報を用いる電子透かし手法の提案," コンピュータセキュリティシンポジウム'98, 情報処理学会シンポジウムシリーズ Vol.98, No.12, pp.33-38, 1998.

[7] Nasir Memon, Ping Wah Wong, "Protecting Digital Media Content," Communications of the ACM, Vol.41, No.7, 1998.

[8] 三浦 信治, 渡辺 創, 嵩 忠雄, "サーバの不正も考慮した電子透かしについて," 1997 年暗号と情報セキュリティシンポジウム, SCIS'97-31C, 1998.

[9] Tatsuaki Okamoto, Kazuo Ohta, "How to Utilize the Randomness of Zero-Knowledge Proofs," Crypto'90, LNCS 537, Springer-Verlag, pp.456-475, 1991.

[10] Birgit Pfitzmann, Matthias Schunter, "Asymmetric Fingerprinting," EUROCRYPT '96, LNCS 1070, Springer-Verlag, pp.85-95, 1996.

[11] Neal R. Wagner, "Fingerprinting," IEEE Symposium on Security and Privacy, pp.18-22, 1983.

捕捉

ここでは、文献 [8] のサーバの不正を考慮した電子透かしについて簡単に触れる。

プロトコル [8]

1. ユーザが原画像サーバにディジタルデータを要求. この内容に対してユーザは秘密鍵を用いて署名する.
2. 原画像サーバがその要求内容をユーザの署名から確認する. これを受理した後, 原画像データをスクランブルして, 自らが選択した埋め込みサーバへ送る. 原画像サーバはこのときのユーザ名及び委託内容に対する署名をつける. 同時にスクランブル復号関数をユーザへ送る.
3. 埋め込みサーバは受けとったスクランブルデータと署名の内容を確認. このユーザ情報を元に電子透かしを埋め込む. そして, ユーザへ電子透かし付きスクランブルデータを送る.
4. ユーザはスクランブル復号関数を用いて電子透かし付きスクランブルデータを復号する.

ただし埋め込んだ透かし情報は削除, 破壊できないとする.

不正に関する考察

この方法の特徴は, 原画像サーバと埋め込みサーバの 2 つのサーバに分けて非対称電子透かしのサーバの不正を防ぐために提案されたものである.

これで不正できるかは, ユーザ署名の内容と原画サーバが埋め込みサーバへ送る内容による.

もし, ユーザ署名の内容に宛先がない場合は, 原画サーバの方に送信するように原画サーバは仕組むことができる. またユーザが送って欲しい画像を指定して署名しないと希望と異なるデータが送れるように原画サーバは仕組むことができる.

つまり, ユーザは署名内容にユーザ名, 画像の名前, 転送先を入れ, 原画サーバは原画サーバの署名と一緒にユーザの署名も埋め込みサーバへ送るようにしなければならない.