M_036

ヒステリシス署名を利用したデジタル画像の長期保証に関する一考察

A Study on Long-Term Verification of Digital Images Based on Hysteresis Signature

辰己 卓矢† 岩田 基† 汐崎 陽†
Takuya Tatsumi Motoi Iwata Akira Shiozaki

1. まえがき

デジタル技術の普及に伴い，カメラで撮影されたデジタル画像を証拠写真として用いる要求が高まっている．デジタル画像は，痕跡を残さずに変更が可能という性質があるため，デジタル画像を証拠写真として用いるには正当性を保証する必要がある．正当性を保証する方法として電子透かしを画像に埋め込む方法があり，誰でも検証可能な公開鍵暗号を用いた方式が提案されている [1]．しかし，公開鍵には有効期限があるため長期に渡ってその正当性を保証することは困難である．

電子文書に用いられているデジタル署名にも公開鍵暗号が用いられているため，有効期限の問題がある．デジタル署名に対しては正当性を長期間保証する方法がいくつか提案されている [2]．そこで，本研究では画像に透かしとして署名を埋め込み，デジタル署名を長期保証する対応策を用いることにより画像の正当性を長期保証することを目的とする．長期保証に必要な要件について述べ，それらを満たすシステムを提案する．そして，提案したシステムの問題点とその対応策について考察する．

2. 電子文書と証拠写真の用途の違い

電子文書の正当性は，署名者によるデジタル署名によって保証されている．署名者以外の第三者が署名だけ変えたとしても，保証している人が代わるため有益でないと考えられる．一方，デジタル証拠写真では，どのカメラで撮影されたかも重要となるため，署名を証拠写真に付与して正当性を保証しようとすると，署名の変更により，どのカメラで撮影されたかを改ざんできる．そのため，証拠写真では画像とその正当性を表す署名を一体化する必要がある．そこで，画像と署名の一体化に電子透かしを利用する．撮影者が透かしを埋め込んで正当性を保証する場合は，撮影後に画像を改ざんし，透かしを埋め込むことにより撮影者に有益な改ざんが可能となる．そのため，カメラ内で透かしを自動的に埋め込む必要がある．

署名を長期保証する代表的な方法に再署名方式とヒステリシス署名がある [3][4]．再署名方式は有効期限が切れる前に新たな署名を追加付与する方式である．ヒステリシス署名は過去に生成した署名に関する情報を含めて署名を作成する方式であり，過去に作成した署名に関する情報は署名生成記録として署名生成履歴に追加されていく．再署名方式を証拠写真に用いるとすると，(1) 再署名の際に人の手が加わり改ざんの可能性が生じる，(2) 再署名するごとに画質が劣化する，(3) 透かしを埋め込める量には限界がある，といった問題がある．それに対してヒステリシス署名を用いると，署名した画像に対して新たな処理をすることなく長期保証できるため，再署名のような問題は起こらない．よって，本研究ではヒステリシス署名を用いた方式を検討していく．

† 大阪府立大学大学院工学研究科

3. システムの要件

ヒステリシス署名を用いて証拠写真の正当性を保証するためには，(1) どのカメラから，誰によっていつ撮影されたかがわかる，(2) 署名が透かしとして埋め込まれる過程や秘密鍵の更新に人の手が加わる余地がない，といった要件があげられる．しかし，カメラの使用者を認識するには生体認証のような仕組みが必要であり，また現状では，秘密鍵の更新には人の手が必要である．そのため本研究では，(1) に関してはカメラに ID を設定し，カメラのみを識別する．(2) に関しては秘密鍵の更新の自動化は今後の課題とする．

4. 提案システム

本章では，3 章の要件を満たすシステムを提案する．要件を満たすためには，透かし情報として，(1) 撮影した画像の情報，(2) 撮影時刻，(3) カメラの ID，(4) 一つ前に撮影された写真の署名生成記録の情報，が必要である．署名生成記録は，撮影するたびに増加するため，全てをカメラ内で保管するのは困難だと考えられる．そこで，署名生成記録をカメラごとに保管する保管サーバを考える．また，秘密鍵を更新する機能，公開鍵証明書を保管する機能も保管サーバにあるものとする．今，撮影された画像が $N-1$ 枚あるとし，新たに撮影した N 番目の画像にヒステリシス署名を埋め込む過程を以下に示す．ここで，ヒステリシス署名が埋め込まれる前の N 番目の画像情報を M_N，ヒステリシス署名が埋め込まれた画像を S_N，署名生成記録を R_N とする．カメラには保管サーバとのセキュアな通信機能があり，固有の ID が設定されているものとする．なお，保管サーバは不正をしない第三者機関とする．

Step1 撮影者は，カメラのシャッターを押す．

Step2 カメラは，画像情報 M_N を生成する．そして，通信機能を用いて保管サーバにアクセスし，ID を保管サーバに送信する．このときの時刻を t_N とする．

Step3 保管サーバは，ID に対応する署名生成履歴 H_{ID} の最新の署名生成記録 R_{N-1} をカメラに送信する．

Step4 カメラは，画像情報 M_N を M_{N0} と M_{N1} に分離する．そして，M_{N0} のハッシュ値 $h(M_{N0})$ と署名生成記録 R_{N-1} のハッシュ値 $h(R_{N-1})$ を求めた後に秘密鍵 SK_N を用いてヒステリシス署名 $\mathrm{Sign}(h(M_{N0}) \,||\, h(R_{N-1}) \,||\, t_N \,||\, \mathrm{ID})_{\mathrm{SK}_N}$ を作成する．

Step5 カメラは，署名生成記録

$$R_N = h(M_{N0}) \,||\, h(R_{N-1}) \,||\, \mathrm{Sign}(h(M_{N0}) \,||\, h(R_{N-1}) \,||\, t_N \,||\, \mathrm{ID})_{\mathrm{SK}_N} \quad (1)$$

を求め，保管サーバに送信する．そして，M_{N1} に透かし情報を埋め込んで，ヒステリシス署名付き画像

$$S_N = M_{N0} \cup M'_{N1} \quad (2)$$

$$M'_{N1} = M_{N1} + (h(R_{N-1}) \,||\, t_N|| \,\mathrm{Sign}(h(M_{N0}) \,||\, h(R_{N-1}) \,||\, t_N \,||\, \mathrm{ID})_{\mathrm{SK}_N}) \quad (3)$$

を生成する．ここで + は埋め込み処理を表す．

Step6 保管サーバは，署名生成記録 R_N を署名生成履歴 H_{ID} に追加する．

次にヒステリシス署名付き画像 S_j の検証手順について述べる．画像を検証する者を検証者とし，画像 S_j と S_j の生成に用いられた秘密鍵 SK_j に対応する公開鍵証明書は持っているものとする．署名履歴には N 個の署名生成記録があり，N 番目の署名に用いられた秘密鍵は漏洩していないとする．また j 番目から N 番目に使用されたハッシュ関数は危殆化していないとする．j 番目の署名の公開鍵証明書の有効期限が切れていない場合は，以下の手順を行う．

Step1 検証者は，公開鍵証明書から公開鍵 PK_j を取り出し，S_j に埋め込まれたヒステリシス署名 $\mathrm{Sign}(h(M_{j0}) \,||\, h(R_{j-1}) \,||\, t_j \,||\, \mathrm{ID})_{\mathrm{SK}_j}$ を復号する．

Step2 検証者は，復号して得られた t_j, $h(M_{j0})$ とヒステリシス署名付き画像 S_j に埋め込まれていた t_j, M_{j0} 部のハッシュ値 $h(M_{j0})$ を比較する．

両者が一致していれば正当性を確認でき，一致していなければ偽造されたことを確認できる．

j 番目の署名の公開鍵証明書の有効期限が切れている場合は上記の手順に加えて以下の手順を行う．

Step3 検証者は，Step1 で得られた ID を保管サーバに送信する．

Step4 保管サーバは，ID に対応する署名生成履歴 H_{ID} と，署名生成記録 R_N に対応する公開鍵証明書を検証者に送信する．

Step5 検証者は，署名生成履歴 H_{ID} から署名生成記録 R_N を，公開鍵証明書から公開鍵 PK_N を取り出す．

Step6 検証者は，公開鍵 PK_N を用いて R_N の署名部を復号する．そして，復号して得られた $h(M_{N0})$, $h(R_{N-1})$, t_N, ID と R_N に含まれていた $h(M_{N0})$, $h(R_{N-1})$, t_N および Step3 で用いた ID を比較する．比較した値が全て一致していれば，$i = N$ として次のステップに進む．一致していなければ，画像 S_j の正当性は確認できなかったものとして終了する．

Step7 検証者は署名生成履歴 H_{ID} から R_{i-1} を取り出し，R_i に含まれる $h(R_{i-1})$ と R_{i-1} から求まる $h(R_{i-1})$ とを比較する．比較した値が一致していれば，次のステップへ進む．一致しなければ，画像 S_j の正当性は確認できなかったものとして終了する．

Step8 $i = j$ でない場合は，$i = i - 1$ として署名生成履歴 H_{ID} から R_i を取り出して Step7 へ戻る．$i = j$ の場合は画像 S_j の正当性を保証できたとして，署名記録の整合性検証を終了する．

5. 考察

考察すべき項目は，(1) 不要な画像の削除がシステムに影響を与えるか，(2) 検証時に公開鍵証明書をどのように入手するか，(3) 署名検証の Step6, Step7 で値が一致するような偽造が可能となる条件は何か，である．

(1) について，本提案システムでは，検証したい画像と署名生成記録を用いて正当性を検証している．そのため，不要な画像が削除されても署名生成記録を残しておけば検証ができる．

(2) について，本提案システムでは，公開鍵証明書を持っていることを前提としており，どのようにして入手するかについては述べていない．前提が成り立たないこともあるため，どのようにして公開鍵証明書を入手するか検討する必要がある．画像の特徴量を署名生成記録に追加して，検証の際には，その値を用いて保管サーバが公開鍵証明書を検索するといった方法が考えられる．

(3) について，署名検証の Step6 で値が一致するような偽造を成立させるためには，署名生成記録 R_N を偽造する必要がある．署名生成記録 R_N の生成に用いた秘密鍵 SK_N は漏洩していない．そのため，署名生成記録 R_N を偽造するのは困難である．よって，署名検証の Step6 で偽造は起こらないと考えられる．署名検証の Step7 で値が一致するような偽造を成立させるためには，署名生成記録 R_j 以降に生成された署名生成記録全てを偽造する必要がある．署名検証の Step6 のときと同様，N 番目の署名生成記録 R_N の偽造は困難である．よって，署名検証の Step7 でも偽造は起こらないと考えられる．以上より，(3) に示した偽造が起こることはないと考えられる．

6. まとめ

ヒステリシス署名を用いてデジタル証拠写真を長期保証するための要件について述べ，保管サーバを用いて証拠写真を長期保証するシステムを提案した．また，どのような問題点があるかについて述べ，それらを解決するための対応策について考察した．

謝辞 本研究の一部は，(財) 柏森情報科学振興財団の研究助成を受けて行われた．

参考文献

[1] 汐崎 陽，“公開鍵暗号を用いた JPEG 圧縮デジタル写真の改ざん位置特定可能な電子透かし法，”FIT2006, 2006.
[2] 宇根正志，“デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策，” IMES Discussion Paper Series, no. 2002-J-32, 日本銀行金融研究所, 2002.
[3] 伊東信治，宮崎邦彦，本多義則，谷川嘉伸，“電子署名の長期保証に関する一考察，” 2004 年暗号と情報セキュリティシンポジウム予稿集, pp. 527–532, 2004.
[4] 洲崎誠一，松本勉，“電子署名アリバイ実現機構-ヒステリシス署名と履歴交差，” 情報処理学会論文誌, vol.43, no.8, pp. 2381–2393, 2002.