マルチメディア通信と分散処理　97－31
コンピュータセキュリティ　8－31
（2000．3．22）

指紋データの原本性保証技術の開発

石田　修一†　　森藤　元†　　瀬戸　洋一†
†（株）日立製作所　システム開発研究所

本研究ではライブスキャナ（電子的指掌紋入力装置）で取得した指掌紋画像の原本性と証拠性を保全する技術の開発を行った．既開発の著作権保護機能つきデジタルカメラの技術を用いて，ライブスキャナにデジタル署名機能を実装し，取得した指掌紋画像とその登録情報に対してライブスキャナ内部でデジタル署名を作成することで，指掌紋画像の原本性と証拠性を保全するモデルを提案する．また，このモデルのプロトタイプシステムの開発を行い，指掌紋画像の原本性を保証するシステムの実現可能性を確認した結果について報告する．

Originality authentication technique for fingerprint images

Shuichi Ishida†　　Hajime Morito†　　Yoichi Seto†
†Systems Development Lab., Hitachi, Ltd.

We developed how to authenticate an originality of fingerprint images got from digital scanners. In this paper, using our digital camera technique that has authentication functions, we propose a model that keeps originality and validness of the fingerprint image by putting digital signature functions into fingerprint scanners. And we propose a result of developing a prototype to check this model.

1．はじめに

近年，指紋などを用いた生体認証技術が発達し，入退出管理やシステムへのログイン管理など，さまざまなアプリケーションが実際に運用されている[1]．また，電子政府などで，公的文書の電子化による行政フローの自動化が進められていることから，今後，裁判などで証拠として用いられる指紋にも，電子的に採取されたものが用いられるようになることが考えられる．

このように指紋画像が電子的に採取され，利用されるようになると，その画像の原本性や証拠性が保全されているかどうかが問題になる．デジタルデータは加工が容易であり，基本的に加工の痕跡も残らないため，改ざんが行われていないことを証明することは難しい．

そこで本報告では，既開発の著作権保護機能付きデジタルカメラで用いた技術を適用し，ライブスキャナにデジタル署名機能を搭載したモデルを提案する．具体的にはライブスキャナ内部で指紋画像に対して撮影者やライブスキャナを特定する情報と共にデジタル署名を作成し，画像と一緒に出力することで，指紋画像の原本性を保全する．

まずライブスキャナ内部で指紋画像のデジタル署名を作成する方式を述べる．さらに，プロトタイプとして，端末内でデジタル署名作成を

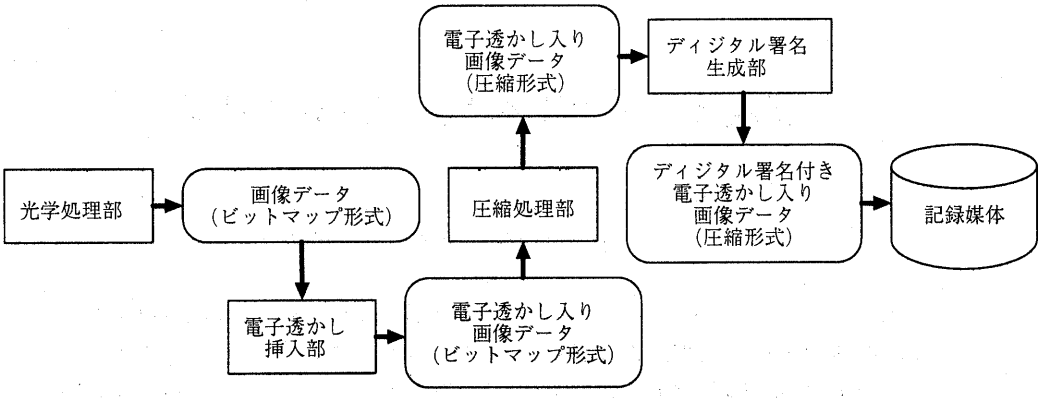

図1. デジタルカメラの機能ブロック図

行うシステムを開発した結果に関して報告する.

2. 著作権保護機能付きデジタルカメラ

図1は既開発である著作権保護機能付きデジタルカメラ[2]の概要を示す.

まず, 光学処理部においてデジタル化したビットマップ形式の画像データにカメラ内部のROM に保持されているカメラの識別子や日付など画像の著作権に属するデータを電子透かしとして挿入する. 続いて, 圧縮処理部において画像データを圧縮する. 次に, 圧縮形式となった画像データ (ヘッダ部を含む) に対してデジタル署名を生成・付加する.

署名の検証はデジタルカメラの公開鍵をあらかじめ配布しておいた計算機などを用いて行う.

以上のように、デジタルカメラの撮影画像に対して、著作権情報を埋め込み、カメラ内部で署名作成を行うことによって撮影画像の著作権の保護を実現している

3. 原本保証機能付きライブスキャナ

3.1 設計方針

2 章で説明したデジタルカメラ署名処理をライブスキャナに搭載し, 同じくライブスキャナの内部に格納した秘密鍵を用いて, 指紋画像に対してライブスキャナ内部でデジタル署名を作成することにより, 指紋画像の原本性を保証するモデルを述べる.

3.2 指紋登録処理

図3にライブスキャナを用いて取得した指紋画像を指紋の付加情報とともに登録するシステムのモデルを示す. まず, ライブスキャナは指紋をビットマップ形式の画像データとして取得した後で, 圧縮などの必要な画像処理を施す. 次に, ライブスキャナに接続された端末から登録者名や指紋の所有者名, 指の種別など指紋を特定するのに必要な情報を取得し, ライブスキャナの識別番号などを加えて登録情報とする. ライブスキャナは取得した登録情報と指紋画像をマージしてまとめ, これらに対して, 内部に格納しているライブスキャナ固有の秘密鍵を用いてデジタル署名を作成する. その後, 端末はライブスキャナとの間で相互認証と暗号通信を行い, 指紋画像とデジタル署名を取得する. 端末では, 指紋画像と登録情報とデジタル署名を指紋情報ファイルとしてまとめ, データベースに保存する.

3.3 指紋検証処理

図4は指紋登録処理において登録した指紋データの正当性を検証する処理を示す. 指紋登録処理では, データベースから指紋情報ファイルを取得し, 指紋情報ファイル内の指紋画像と登

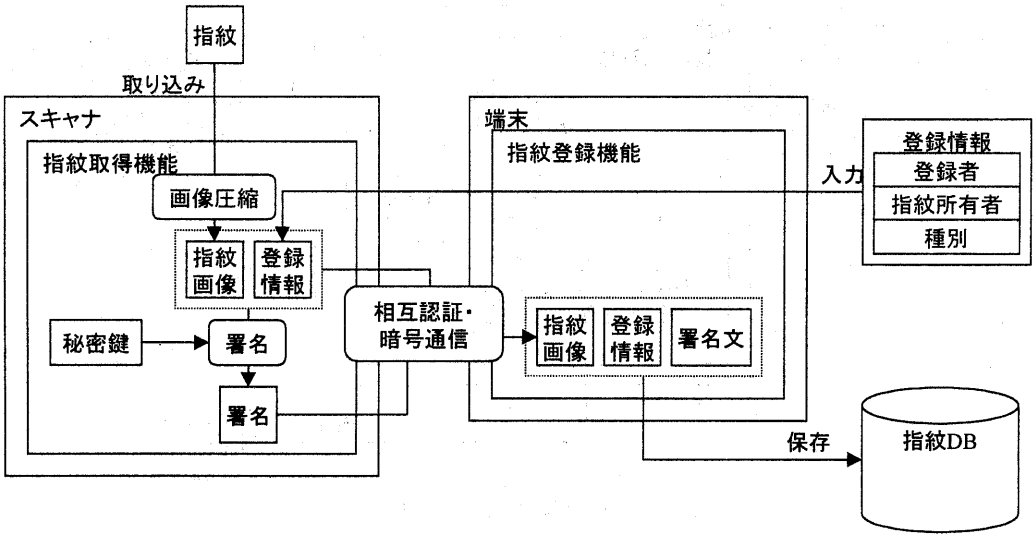

図3. 指紋登録処理

録情報をマージしてまとめ，次に指紋を採取したライブスキャナの秘密鍵に対応する公開鍵を用いて，デジタル署名の検証処理を行う．以上の処理により，指紋画像の原本性が保証されているかが検証できる．

4. プロトタイプシステムの開発

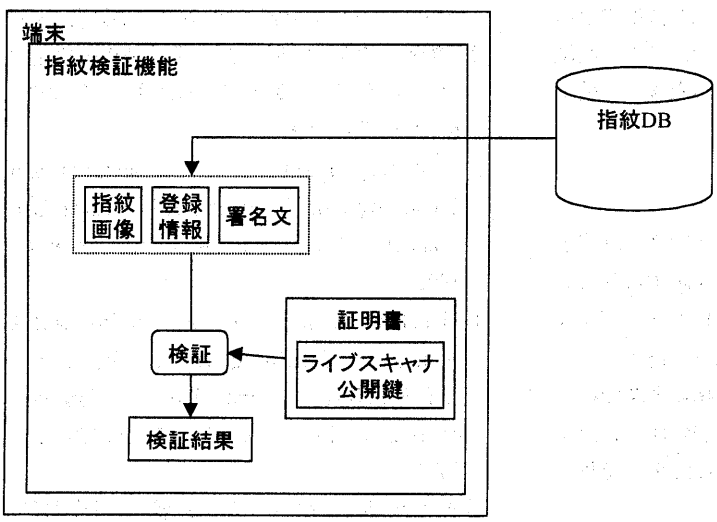

図4. 指紋検証処理

3 章で説明したシステムのプロトタイプとしてデジタル署名作成処理を端末で行うシステムを開発した．

図5は今回作成したプロトタイプの指紋登録処理を示す．本プロトタイプでは，まず，ライブスキャナが取得したビットマップ形式の指紋画像を端末に送信する．次に，ライブスキャナから取得した指紋画像と，端末は登録者の入力により取得した登録情報をマージしてまとめ，これらに対して，端末内に格納している秘密鍵を用いて，デジタル署名を作成する．次に，指紋画像と登録情報，デジタル署名を指紋情報ファイルとしてまとめる．作成したデータは HDD などの外部記憶装置に保管される．

本プロトタイプでは，原本性保証を行うためのデジタル署名の作成には，メッセージダイジェストを作成する一方向性ハッシュ関数として SHA[3] を使用し，デジタル署名作成用公開鍵アル

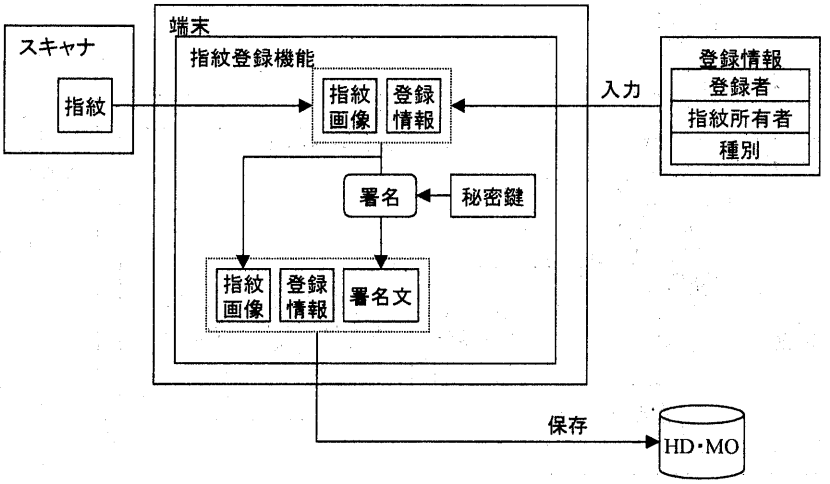

図5. 指紋登録プロトタイプ

ゴリズムとしてRSA署名方式[4]を採用した．ここで，デジタル署名用の秘密鍵はあらかじめ端末に登録されているものとし，暗号化用の暗号鍵は登録者からの入力によるものとした．また，画像はビットマップ形式で扱うものとしたため，画像の圧縮処理は省略した．

デジタル署名の検証処理は，図4と同じモデルで実現できる．

本プロトタイプ開発により，指紋画像を取得後，指紋の付加情報とともに登録を行い．その後，検証処理により，登録した指紋画像の原本性が保たれていることが確認した．また，画像や登録情報に対して改ざんを行った場合，検証処理での検出を確認した．

5. おわりに

デジタル署名をライブスキャナ内部に実装することで，指紋画像の原本性を保証するシステムを提案し，このシステムのプロトタイプシステムを開発した．この結果，以下を達成した．

(1) ライブスキャナで取得した指紋画像に対して，ライブスキャナ内部で署名作成を行うことで，指紋画像の原本性保証を可能とした．

(2) 指紋の登録情報を指紋画像に付加してデジタル署名作成を行うことにより，指紋の属性を含めた保証を可能とした．

(3) プロトタイプシステムの作成により，上記システムの実現可能性を確認した．

以上により，ライブスキャナで取得した指掌紋画像の原本性を保証するシステムの実現可能性を示した．

参考文献

1) D.Russell, G.T.Gangemi Sr.: コンピュータセキュリティの基礎，アスキー出版局，1994

2) 森藤，安細，吉浦，金野: 著作権保護機能付きディジタルカメラの試作，CSEC'99, pp.273-276, 1999

3) National Institute of Standards and Technology, NIST FIPS PUB 185: Secure Hash Standard, U.S. Department of Commerce, 1994

4) R.L.Rivest, A.Shamir, and L.M.Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, v.35, n.7, pp.120-126, 1978

5) W.Ford, M.Baum: ディジタル署名と暗号技術，プレンティスホール出版，1997