W3 指紋照合技術とそのヒューマンインタフェースへの応用

Fingerprint identification and its application to human interface

内田 薫 (NEC C&C メディア研究所)

Kaoru UCHIDA, NEC Corporation, Miyamae, Kawasaki, 216-8555

Fingerprint matching has proved to be an effective technology for identifying persons, since it is highly accurate while the system can be inexpensive and compact. This paper covers the state-of-the-art of fingerprint-based personal identification, including principles and implementation of an input sensor and identification algorithms, system design and its applications. It also discusses an enhanced user interface "Fingerprint User Interface" that enables users to assign commands, data objects, or personalization settings to individual fingers for user-friendly direct manipulation.

Key Words : Fingerprint, Biometrics, Identification, User interface

1 指紋照合の特徴と認証への応用

情報機器の進歩と普及と共に、情報の電子化と、ネットワークで結ばれたシステム上でのさまざまな価値の非対面での交換が日常化しつつある。このような応用における、データの盗聴・改竄や「なりすまし」といった不正・犯罪に対抗するセキュリティの確保のために、各人に固有な生体情報を用いて個人を識別する、バイオメトリクスによる認証が注目されつつある⁽¹⁾⁽²⁾⁽³⁾。

人間の指先の皮膚紋様である指紋は、「万人不同」・「終生不変」という特徴を持つとされ、精密な個人の同定を可能にするバイオメトリクスとして広く知られている(指紋は一卵性双生児でも同一ではなく、さらに各人の指ごとに異なる。また表皮が損傷を受けてもその奥の不変な真皮から同じ指紋が復元される)。指紋による個人同定は、19世紀の終わりにインドで実用化されたのを皮切りに、警察・司法分野でおおよそ1世紀に渡り本格的に活用されている。そしてその自動化への取り組みも1960年代からと比較的長い歴史を持ち、現在では高い精度で個人を自動識別する方式・システムが実現され実用に供されている。

情報システムでの認証用途に一般の人々が使用することを考えると、「指紋を採られる」ことへの抵抗を感じる人がいることや、皮膚の乾燥・発汗や傷・摩耗などによって必要な品質で指紋画像を得られない場合があることは事実である。しかし指紋は他のバイオメトリクスと比較した場合、

- 高精度な照合方式が確立している。特に従来大規模なシステムでのみ利用可能であった照合技術がパーソナルユース向けに使えるレベルに達している、
 - 入力センサが接触型で小型化できるために、パソコンや携帯端末に搭載するという形態で使用しやすい、
- という点で、低価格・小型な情報セキュリティを実現するには最も適しており、いくつかの会社で商品化されるなどとも実用化が進んでいるバイオメトリクスである。

本稿ではまず指紋識別(認証)システムを可能にする要素技術について説明する。ついで実際のシステム構成例、応用について解説し、システムの実例を挙げる。最後に、情報システムにおけるバイオメトリクスの新しい可能性を示す例として、指紋識別技術のユーザーインタフェースへの応用を紹介する。

2 指紋認証の技術動向

指紋により個人を認証するシステムは基本的に、(1)「入力センサ」でユーザが提示した指紋を取得し、(2)そこから「特徴を抽出」し、(3)あらかじめ登録しておいた「テンプレート」と比較し同一人物であるか否かを決定するという動作を行う。

2.1 指紋の入力センサ

指紋の入力センサとしては、従来ほぼ光学方式、特に高コントラストな画像を得るための全反射法のみが用いられてきた。これはLED光源で発した光をプリズムに当ててからCCDのような受光素子で受け、プリズムの反射面に置いた指の凹凸(盛り上がった部分がなす線を「隆線(ridge)」、その間を「谷(valley)」と呼ぶ)を反射率の違いに反映させ、デジタル画像化するというものである(図1)。

近年はこれに加え、半導体チップの表面に直接接触させた指紋から静電容量などを用いてその凹凸をセンスする素子も実用化されてきている。このような半導体素子では、比較的低価格でありながらワンチップで指紋イメージの取得ができ、指紋入力部の小型化・薄型化により、システムの応用範囲を広げることが可能になる。

Fig.1 Optical sensing of a fingerprint image

2.2 指紋照合アルゴリズム

指紋の照合の実現には大きく分けて、画像から隆線の構造など照合用の特徴を抽出して登録側と入力側の抽出特徴同士を比較する「特徴照合」による方式と、2つの画像の間の類似度を直接評価する「画像マッチング」による方式とがある。

前者の代表として、指紋隆線及びその端点と分岐点 (ridge-ending と bifurcation: この 2 者をまとめて「マニユーシャ (minutia)」と呼ぶ) を抽出し、それらの位置関係を元に 2 つの指紋特徴間の一致を調べる方式がある。この方式ではマニユーシャ間の距離など詳細な情報を用い、2 つの指紋の類似度を評価することで照合を行う。一方画像マッチングの方法としては、例えば 2 値画像としての隆線パターンの単純な一致を調べる方法、あるいはフーリエ変換した指紋画像同士の位相相関を評価する位相限定相関方式や光相関を用いた方法などが提案されている。

これらを比較すると、画像マッチングによるほうが大局的な位置合わせだけのため指紋画像同士 1 対 1 の照合は高速であるが、画像の局所的な変形に弱いという傾向がある。特徴照合方式は一般には特徴抽出処理の計算量が大きい反面、指紋押捺の際に避けられない指紋画像の歪みなどの局所的な変形に強いという特長を持つ。

2.3 指紋画像からのマニユーシャ抽出

実用化されている特徴照合方式における処理の一例を挙げて動作を説明する。入力センサから濃淡画像が与えられると、まずノイズ除去や、隆線と谷とのコントラストを高めるための前処理が実行され、その後二値化及び細線化と言った画像処理により隆線パターンを表す細線化画像が抽出される。指紋押捺の画像においては、センサの感度や指の固さ、発汗の程度や乾燥度合い、押捺の強さなどが場所によりばらつく。このようなさまざまな外乱に起因する画像の不安定性に対応するため、隆線方向を強調する空間フィルタや適応的閾値の適用など、指紋に特化した画質改善処理が各段階で必要とされ、高精度の照合を可能にするためにはこの部分の計算量がかなり大きくなることが多い。

得られた細線化隆線パターンに対して隆線の端点・分岐点に対応するマスクフィルタを施すことにより、照合に用いる特徴点であるマニユーシャを抽出する。ここで得られる特徴点候補には、指紋入力の際のノイズや二値化・細線化処理などに起因する疑似マニユーシャが含まれることがあるため、さまざまなルールを用いて真のマニユーシャのみを選択する処理を加えることも多い。

2.4 マニユーシャ・リレーション方式

マニユーシャを用いる特徴照合方式において、基本となる特徴量はマニユーシャの位置関係やそこに接する隆線方向であるが、これらを求め、照合するだけでは例えば図 2 の 2 つを区別できない。さらには、マニユーシャ間の距離や角度は、本来 3 次元で弾性がある指を押捺した際に、つねに安定して 2 次元画像にマッピングされるとは限らず、照合のエラーの原因となる。そこでマニユーシャ間を結ぶ線分に交差する隆線数の関係を特徴量とする「マニユーシャ・リレーション方式」が開発された⁽⁴⁾⁽⁵⁾。図 3 に入力画像、隆線とマニユーシャの抽出結果、マニユーシャ・リレーションを表すマップ表現の例を示す。

登録指紋と認証用入力指紋の 2 つのマニユーシャ特徴データが与えられたとき、それらの一致を判定するのが「マニユーシャ照合処理」である。照合においては、まず例えば隆線のマクロな流れにおける湾曲の中心部を基準にして 2 つの特徴データの位置合わせを行う。ついで似たリレーション特徴を持ったマニユーシャの対応を見つけだすために、中心位置や回転角を微調整しながら対応マニユーシャ対を決定し、その対応強度の総和を計算する。図 4 のように登録側と入力側の両マニユーシャを比較し、両方の画像に対

応マニユーシャがあれば加点し、一方にしかなければ減点するというスコアリングが基本である。

Fig.2 Minutia and Relation

Fig.3 Minutiae-Relation matching

Fig.4 Search for corresponding minutiae

得られたスコアは 2 つの指紋の類似度を表し、これがあらかじめ定められた閾値 T より大きければ両指紋は「一致」、そうでなければ「不一致」と判定することになる。認証システムの動作特性を決定するのがこの T の値であり、例えば高いセキュリティを必要とする応用ではこれを高くすることで他人を誤って受理するというエラー率 ($FAR = \text{False Acceptance Rate}$: 他人受理率) を小さくするよう設計することになる。この場合、本人を誤って拒絶するというエラーの発生率 ($FRR = \text{False Rejection Rate}$: 本人拒否率) は必然的に高くなる (これと対極的な例として、誤った一致候

補は多数生じたとしても本人を見逃すことがないよう、Tを低くすることで本人拒否を許さないような設定をするという、鑑識用途のようなケースもある。)

以上説明したような特徴抽出及び照合処理を施すことで、指紋押捺によって引き起こされる画像の歪みを吸収しながら安定して動作する、高精度な指紋識別の実現が可能になる。NECが開発した本方式に基づいて大規模な指紋識別を行うシステム(AFIS = Automated Fingerprint Identification System)は、1982年以来日本の警察庁で稼働しているのを始めとして、世界の警察・官庁分野で約6割のシェア(登録データ数ベース)を持つに至っている。

2.5 1対N照合によるID不要認証

多くのバイオメトリクス認証においては、ユーザが認証を要求する際、何らかの識別名や番号の入力、あるいはIDカードの提示によって自分の名前(ユーザ識別情報)を名乗った後に、その名前で登録してあるバイオメトリクスデータと入力されたデータを「1対1照合」することにより認証している。これに対し、ユーザがバイオメトリクスを入力するだけで、あらかじめ登録しておいた複数の(時には多数の)登録データの中からそれと一致するものを探索し、このユーザ識別の結果が権限のあるユーザであれば認証成功と判定するという方法がある。この場合、あらかじめユーザ識別情報の提示はないため、指紋だけによるいわば「1対N照合」によりユーザを探索することでID入力不要な認証が実現される。

前述の特徴照合方式による識別の実現では、指紋特徴の抽出は一般に(画像マッチング法による実現に比べ)計算量が大きい、一度抽出した特徴同士は高速に照合できる。従ってその高い精度とあいまって、このような1対N照合を十分実用的な速度と信頼性で実現するには適していると言える。

3 指紋認証システムの構成と動作

代表的な指紋認証システムの構成と動作の例を説明する。

3.1 スタンドアロン基本機能

まず基本となるスタンドアロン型の認証装置の構成においては、あらかじめサービスを許可されているユーザから入力されて登録されている指紋情報と、サービスを要求する人間によって認証時に入力される入力指紋情報が照合され、一致と判定されるときに認証成功とすることになる。このとき登録指紋情報の保持方法として、(a)装置内に登録者人数分が保持され、ユーザがユーザ識別子を提示するとそのユーザの指紋情報が取り出され、ユーザが入力した指紋情報と照合される、という形態と、(b)ユーザが持参するICカードなどの提示物内に本人の指紋情報が保持され、認証時には読み出されたこの登録情報とユーザが入力した指紋が照合される、という2つの実現法がある。

また識別処理をどこで実行するかについても、この識別処理を入力センサと一体化した独立のユニットで実現するというシステム構成(このタイプを「インテリジェントタイプ」と呼ぶことがある)と、入力センサ部は指紋の入力だけを行い(「ノン・インテリジェントタイプ」)、識別処理は接続されたPCなどで行うという実現法の2つがある。

前者のインテリジェント型は、PCがない場合でも実現でき、指紋処理部が閉じたシステムであるためセキュリティを実現しやすいという特長を持つ。一方ノン・インテリジェント型には、ユニットに内蔵するマイクロプロセッサでは識別処理の時間がかかるという前者のケースに比べ、PC

の高速なCPUを識別処理に使えるというメリットがあり、PCなどをベースとした通常のコンピュータシステムにおける情報セキュリティ用途では有効な実現法である(もちろん識別処理をPCのソフトで実行するに当たっては、ソフトの改造に対抗するためその部分のセキュリティを高めるよう注意を払う必要がある。)

3.2 ネットワーク対応認証

一方ネットワークを介した情報サービスなどの応用では、ユーザがどの端末をクライアントとしてサービスを要求しても認証を実行できるように、サーバ側でユーザ情報を管理する場合がある。このようなシステムの構成例と動作を示すのが図5の(a)である。ユーザが入力した指紋情報からクライアントで抽出されたマニユエラ特徴がネットワークを介してサーバに送られ、サーバに保存されているそのユーザの登録指紋情報と照合される。指紋画像そのものよりは抽出した指紋の特徴情報の方がはるかにデータサイズが小さいため、クライアントーサーバ間のデータ交換には適している。ネットワークの安全性が比較的高い、イントラネットを主体とした社内システムのような場合、このようにして登録情報のサーバにおける集中管理をする方が現実的である。

逆に一般ユーザを対象としインターネット上で用いるような場合などでは、サーバに登録側指紋を置かずに、ユーザが保持・持参するICカードなどに登録した指紋情報と入力指紋をクライアント側で照合し、結果をサーバに送る図5(b)のような形態をとることもできる。

ネットワーク上に指紋情報を流すかあるいは指紋照合結果を流すかいずれの場合も、発信者と受信者の相互認証と通信内容の秘匿、改竄の防止のため、通信メッセージを暗号化し電子署名をつける必要がある。

Fig.5 Fingerprint authentication over network

3.3 指紋認証の応用・用途

まず基本となるスタンドアロン形態での指紋認証の用途としては、Windowsへログインする際のユーザー認証や、席を外すときのスクリーンセーバーによる端末ロック、ワープロなど一般アプリケーションのファイル内容秘匿のためのパスワード代替などがある。

さらにPCの盗難への対策として、BIOSと連携することで本人の指紋がなければPCの起動ができないように設定するBIOSロック機能も有用である。この場合、指紋識別機能とPCのBIOSレベルのアクセス制御が直接連動するよう実現されている必要がある。

一方、情報セキュリティへの適用という意味でバイオメトリクスの本領を発揮するネットワークサービスへの応用としては、イントラネットによるオフィス情報システムへのログイン、さらには電話回線を介したもののも含め、社外などからの情報システム、データベースへのアクセス管理がまず考えられる。さらにインターネットを通じての会員向け情報サービスや電子商取引(EC)での本人確認などがある。

3.4 指紋認証システムの実例

指紋識別に基づいたユーザー認証システムの一つの実例として、NECで開発された指紋認証ユニットについて説明する。中心技術となる指紋照合部には、2.4節で説明したマニュージャ・リレーション方式の照合アルゴリズムが利用されている⁽⁴⁾⁽⁵⁾。これはAFIS(大規模指紋照合システム)応用で実績ある特徴抽出及び照合処理のコア部分をマイクロプロセッサでのソフトとして動かせるようにしたもので、1~2秒程度と高速な照合でありながら、非常に高い照合精度が実現されている。この高精度の照合機能によって、複数の人が登録してあっても指紋を提示するだけでその人物が登録済みかどうか、さらにはそれが登録済みの誰であるかを識別する1対N認証動作が可能となっており、「指を置くだけ」というワンタッチの使い易さを実現している点が大きな特長となっている。指紋の入力センサ部としては、Veridicom社の静電容量方式のセンサチップ⁽⁶⁾を利用することで外形部の形状は光学方式を用いる場合に比べ大幅に薄型化・小型化が可能になった(図6)。

使用形態としては、ユニット内で指紋入力、特徴抽出を行った後にユニット内に記憶された登録指紋との照合を行い、結果をサービスを行うPCに送る、というインテリジェントタイプとして使える。PCとのインタフェースはRS-232CのものとPCMCIAのものがあ、いずれの場合もPCとの通信は暗号化することでセキュリティを保証している。内部での照合に加え、特徴情報をPCに送ることで、PCでの照合や、さらにはその先のネットワークで結ばれたサーバでの照合に対応することもでき、また指紋認証開発用のSDK(Software Development Kit)を利用することで広範囲な情報システムへの対応が可能となる。

また、今後セキュリティ意識の高まりと共に要求が高まると予想される、インテリジェント化されていくデジタル家電やドア、ロボットなどを含むさまざまな機器への、ユーザー認証・識別機能の組み込みを容易にするため、単独で指紋入力から照合までを行う組込用認証モジュールも用意されている(図6(c))。

Fig.6 "SecureFinger" identification unit
【 see: <http://www.sw.nec.co.jp/pid> 】

4 指紋識別技術の新たな応用展開

情報システムにおける指紋照合技術の新しい可能性を示す例として、指紋識別技術のユーザーインタフェースへの応用に関して論じる。

4.1 1対N照合の応用 —— 「指先ユーザーインタフェース」

2.5節で説明した「1対N照合」機能を利用することで、登録指紋の中で入力指紋と一致するものを探索し、この識別機能によって得られた「誰の」「どの指」かの判定結果に応じて認証以外の処理を行うこともできる(因みに指紋は全ての指で異なる)。本機能の最も基本的な応用が、指紋識別による自動ログインである。通常必要なユーザ名とパスワードのキーボード入力に対し、この方式では指紋の提示のみで本人としてのログインが可能で、なりすましを防ぐ認証と両立させながら、手軽さの面で優れたユーザーインタフェース(UI)を提供している。

このような、「指紋はそれだけでUIの一手段として利用できる」というアイデアを拡張することで、「指先UI」(あるいは「指紋UI」)とでも言うべき新しいコンセプトを展開することができる⁽⁷⁾⁽⁸⁾⁽⁹⁾。これは指紋の提示を入力の一環として、ユーザがセンサに触れた指に割り当てられたコマンドやデータオブジェクトを利用する処理を行うものである(図7)。例えば次のような応用が考えられる。

Fig.7 Fingerprint User Interface

指紋によるコマンド実行（「指先コマンド」）

個人の各指に仮想的にコマンドを割り当てる。従来の「ボタンを押す」と言うアクションは実行のトリガーだけであったのに比べ、この UI では「どの指で押すか」をも動作決定の入力としている。ボタン数削減、ボタン部を見ないでの操作が可能になるなどの効果がある。

指紋による状態設定（「指先セーブ」）

指紋によるログインと同時に、ユーザごとに用意された個別環境（ショートカットなど）を設定すること、さらにはどの指をログインに使うかに応じ異なる環境設定の中から選択できるようにすることが可能である。また設定するものとして、静的な環境だけでなく、前回そのユーザがシステムを使用したセッションの最後の状態を復元するという機能を提供することもできる。

このような「指先一本で各ユーザ固有の状態を復帰する」という機能は、オフィスにおけるパソコン上でよりは、小型端末において、あるいは子供・高齢者・身障者など従来型の UI に不慣れなユーザの使用するデジタル家電などにおいて、より大きなメリットを示す。一例を挙げると、TV ゲーム機や電子絵本を共用する際、各ユーザがどこまで進んだかを指紋と共に覚えさせ、後にその指一本で続きを再開できるという、誰にでも使い易いいわば「指先しおり」を実現することができる。

指先へのデータオブジェクト記憶（「指先メモ」）

上述の「状態の記憶」という考え方を進めると、指先をあたかも記憶媒体のように使用して、様々なデータオブジェクトを仮想的に記憶させ、呼び出すという UI が実現できる。例えば Web の URL を各指に割り当てることで、指を変えるだけで WWW をブラウズすることが可能になる。あるいは指ごとによく使う文字列（例えばシグニチャや定型文）を覚えさせ、メールなど文章を書くときに文字列を手軽に挿入する、という使い方ができる。またこの「記憶→呼び出し」という動作対を動的に使用すれば、指ごとに異なる複数のカットバッファ（クリップボード）を使ったカットアンドペーストを実現することができる。

さらにこれをネットワーク環境での動作に拡張し、図 8 のように一方の装置で仮想的に指先にデータを指先にコピーし、他の機器でペーストすることも可能である。この動作は、機器 A でコピーの際に指紋 P2 と関連づけて記憶されたデータ Obj2 を、他の機器 B から指紋 P2 をキーに探索し、B に送ることで実現される。

Fig. 8 Implementation of fingertip memo

認証によるパーソナリ化

以上の UI の例ではいずれも個人の複数の指の違いを用いているが、全ての UI 動作はもちろん「自分専用であり他人では実行できない」という特徴を持つ。従ってそのまま、動作区別の隠蔽から記憶内容の秘匿までの幅広いセキュリティを保証した、情報の自己管理とパーソナリ化を実現する手段を提供することになる。

5 おわりに

バイオメトリクス照合技術の中で最も実用化が進み、今後の応用の広がりについても期待の高い指紋識別技術について解説した。

指紋照合は、精度が高いことに加え、コンパクトで携帯に適した実現が可能であることで、さまざまな機器のセキュア化のための確かな認証手段であることがわかる。また従来から知られた認証用途に加え、4 章で論じた「指先ユーザインタフェース」のようにその識別性能を積極的に利用することで、幅広い情報機器の知能化や、ユーザフレンドリなマンマシンインタフェースが実現できる。機械系研究者・技術者の皆さんがバイオメトリクスに興味を持ち、本稿が今後のセキュアでインテリジェントな情報機器の実現の一助となれば幸いである。

参考文献

- (1) Jain et al: BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.
- (2) 坂野: “バイオメトリック個人認証技術の動向と課題,” 信学技報, PRMU99-29, pp. 75—82, 1999.6.
- (3) ここまで来たバイオメトリクスによる本人認証システム, 情報処理, Vol.40, No.11, 1999.
- (4) 浅井 他: マニユーシャネットワーク特徴による自動指紋照合 —特徴抽出過程—, 信学論, Vol.J72-D-II, No.5, pp.724—732, 1989.
- (5) 浅井 他: “マニユーシャネットワーク特徴による自動指紋照合 —照合過程—,” 信学論, Vol.J72-D-II, No.5, pp. 733—740, 1989.
- (6) Inglis et al: “A Robust, 1.8V, 250μW, Direct Contact 500dpi Fingerprint Sensor,” IEEE ISSCC98, SA 17.7, pp.285—285, 1998.2.
- (7) 内田 他: “指紋識別を用いた情報システム,” 信学技報, OFS98-26, IE98-52, pp. 13—18, 1998.9.
- (8) 杉浦 他: “指紋識別に基づくユーザインタフェース,” 情報処理学会 インタラクション'99, p.169—176, 1999.3.
- (9) 内田 他: “指紋による携帯向け個人識別端末とそのセキュリティ,” 信学技報, PRMU99-21, pp. 13—20, 1999.6.