2-2 指紋による個人認証の最前線

内田 薫[†]

キーワード：バイオメトリクス，個人認証，指紋照合，ユーザインタフェース

1. 指紋による個人識別

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。

歴史的には先史時代から中国などで個人を示すのに使われていたのが知られており，また，1874年に来日した英国人ヘンリー・フォールズが，日本の拇印の習慣から指紋に興味を持ち，指紋による個人識別の研究成果をイギリスの科学雑誌「Nature」（1880年10月）で報告したのが，指紋に関する世界初の論文とされている。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・司法分野でおよそ1世紀にわたり本格的に活用されている。そしてその自動化への取組みも，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，皮膚の乾燥や・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形化できるために，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・小形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もっとも実用化が進んでいるバイオメトリクスである¹⁾²⁾。

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，応用の最新の状況について解説し，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) ユーザが提示した指紋をシステム側で取得する「入力センサ」
- (2) 入力されたデータを処理し照合用の特徴を求める「特徴抽出部」
- (3) あらかじめ求め，記憶しておく正規ユーザについての登録（「テンプレート」）
- (4) 登録データと入力データ（の特徴同士）を比較し同一人物であるか否かを決定する「照合・判定部」

から構成される。照合の結果，特徴が十分類似し，指紋の提示者が登録ユーザであると判定されれば，認証成功ということで認証要求者は要求するサービスを受けられる。本節では，システムを実現するための要素技術の動向を紹介する。

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。しかしこの方式では，プリズムを配置し，さらに反射光を受光素子で受ける縮小光学系実現のための光路長をとる必要があることから，装置の小形化には限界があり，コンパクトなシステムをめざす際のネックとなっていた。

これに対しここ数年，光学方式以外のセンシングを可能とする素子の実用化が進んできている。半導体チップの表面に直接接触させた指紋からその凹凸をセンスするもので，例えば静電容量方式のもの，温度や電界の差を検知する方式のものなどがある。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，指紋入力部の小形化・薄形化により，システムの

^{*} 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。

[†] NEC 情報通信メディア研究本部

"The State-of-the-art of Fingerprint-Based Personal Identification." by Uchida Kaoru (NEC Corporation, Kawasaki)

応用範囲を広げることが可能になる。

なお、入力画像の解像度は20画素/mm (500dpi)、8ビット/画素のものが標準的であり、画像サイズは1.5cm角から2.5cm角程度のものが多い。

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」による方式がある。

前者の代表として、指紋隆線およびその端点と分岐点 (Ridge-EndingとBifurcation: この2者をまとめて「マニューシャ (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、マニュ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、指紋画像どうし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ューシャ抽出

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。入力センサから指紋の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る。その後二値化および細線化により隆線パターンが抽出され、さらにそこから照合に用いる特徴点であるマニューシャが抽出される。

これらのマニューシャ間の位置関係を用いて指紋を比較すればよいわけであるが、本来3次元で弾性がある指を押捺した際、マニューシャ間の位置関係は一意的に2次元画像にマッピングされるとは限らず、それら相互の距離や角度を用いるだけでは安定した照合は難しい。そこで精度向上のため、マニューシャ間を結ぶ線分に交差する隆線数の関係をも特徴とする「マニューシャ・リレーション方式」が考案された³⁾。図1に入力画像、隆線とマニューシャの抽出結果、マニューシャ・リレーションを表すマップ表現の例を示す。

2.4 マニューシャ・リレーション方式による指紋照合

登録指紋と認証用入力指紋の2つの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照合処理である。マニューシャ・リレーションによる照合においては、まず2つのマニューシャのマップ表現の位置を合わせ、似たり

図1 マニューシャ・リレーション照合方式

リレーション特徴を持ったマニュ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ューシャ対を決定し、その対応強度の総和からスコアを計算する⁴⁾。

得られたスコアは2つの指紋の類似度を表し、これと閾値との大小により一致、不一致を判定する (この閾値を高く設定すれば、他人受入エラー (FAR) は少なくなり、本人拒否エラー (FRR) が増すことになる)。

以上説明したような特徴抽出および照合処理を利用することで、指紋押捺によって必然的に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*。

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形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 (テンプレート) 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なる。この識別処理をどこで実行するかについては、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。

このような形態での用途としては、OSなどへログインする際のユーザ認証や、席を外すときのスクリーンセーバー

* 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・官庁分野で広く採用されている。

図2 サーバに登録した指紋と照合するネットワーク対応認証

図3 ユーザが持参する登録指紋と照合するネットワーク対応認証

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。

3.2 ネットワーク対応認証

ネットワークを介した情報サービスなどの応用のシステムにおいては、図2に示すように、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指紋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テンプレートと照合される、という構成が考えられる。ネットワークの安全度が比較的高い、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ことが可能である。

一方、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、ユーザが保持・持参するICカード上のテンプレート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3のような形態をとることもできる。

このようなネットワークサービスでの指紋認証の応用としては、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挙げられる。さらに、インターネットを通じての会員向け情

図4 指紋認証ユニット「SecureFinger」

【詳しくは <http://www.sw.nec.co.jp/pid> を参照】

図4 指紋認証ユニット「SecureFinger」

報サービスや電子商取引（EC）での本人確認などで、今後実用化が進むと考えられる。

3.3 指紋認証システムの実例

バイオメトリクス技術の応用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、先に説明したマニユーシャ・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。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およ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、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。指紋の入力センサ部としては、静電容量方式のセンサチップ⁵⁾を利用することにより、外形部の形状は光学方式を用いる場合に比べ大幅に薄形化・小形化が可能になった（図4）。

ユニット内部での照合に加え、特徴情報をPCに送ることによって、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ともに要求が高まると予想される、デジタル家電などさまざまな機器へ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4(c)）。

4. 指紋識別技術の応用と展開

最後に、情報システムにおける、認証以外のバイオメトリクス応用の新しい可能性を示す例として、指紋識別のユーザインタフェース（UI）への応用を紹介する。

上述の高精度な「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ができる。本機能の最も基本的な応用が、指紋の提示のみによる自動ログインであり、なりすましを防ぐ認証と両立させながら、手軽さの点で優れたユーザインタフェース（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」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⁹⁾。これは指紋の提示を入力の一形態として、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。例えば、次のような応用が考えられる。

4.1 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」というアクションは、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。

4.2 指紋による状態設定（指先セーブ）

前述の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、小形端末において、あるいは子供・高齢者・身障者など従来形の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、テレビ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。

4.3 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、さまざま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）と指紋を関連づけて登録しておき、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

図5 指を仮想的記憶媒体とする「指先メモ」

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5のように一方の装置でデータ仮想的に指先にコピーし、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で指紋P2をキーに探索し、Bに送ることによって実現される。

4.4 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。これにより、情報の自己管理とパーソナリ化が指紋認証に基づきセキュアに実現されることになる。

以上、バイオメトリクス認証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の最前線について解説した。読者の皆さんが指紋を含むバイオメトリクス技術に興味を持ち、本稿が安全でユーザに優しい情報化社会実現の一助となれば幸いである。

(2000年11月2日受付)

〔文 献〕

- 1) Anil Jain et al.: "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers (1999)
- 2) "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, 40, 11 (1999)
- 3) 浅井紘, 他: "マニピュレータネットワーク特徴による自動指紋照合一特徴抽出過程一", 信学論誌, J72-D-II, 5, pp.724-732 (1989)
- 4) 浅井紘, 他: "マニピュレータネットワーク特徴による自動指紋照合一照合過程一", 信学論誌, J72-D-II, 5, pp. 733-740 (1989)
- 5) D.Inglis et al.: "A Robust, 1.8V, 250 (W, Direct Contact 500dpi Fingerprint Sensor", IEEE ISSCC98, SA 17.7, pp.285-285 (1998.2)
- 6) 内田薫, 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)