

バイオメトリクス認証技術

Biometric Authentication Technology

あらまし

バイオメトリクス認証は、人の身体に備わる特徴を利用して本人認証を行う。認証のキーとなる情報の忘失、盗難、偽造の心配の少ない、本質的に安全性の高い認証である。

指紋認証は高識別を特長に早くから実用化が進んでおり、PC用をはじめ広範囲に適用されている。富士通研究所は、高性能と導入しやすさを両立させた小型のネットワーク認証装置を開発した。手のひら認証（静脈パターン認証）は高精度認証技術として新しく製品化を目指している。静脈パターンはセンサに手をかざすだけの非接触入力が可能であり、柔軟で使いやすい認証システムが期待される。顔や声による認証は更に利用者の負担の少ない自然な認証を実現でき、照合を行っていることを意識させない認証も可能となる。

本稿では、富士通研究所におけるこれらのバイオメトリクス認証技術の最新の研究開発成果を紹介する。

Abstract

Biometric authentication is a technology for identifying a person from the person's physical characteristics. It is essentially a high-security authentication technology that is free from the problems of forgotten, lost, and stolen authentication keys. Fingerprint authentication, which features high identifiability, has already been put to extensive practical use with personal computers and other applications. Fujitsu Laboratories has developed a compact network authentication server that combines both high performance and easy installation. Fujitsu Laboratories is also striving to commercialize a palm authentication device that ensures highly accurate authentication. This device enables contactless input of palm vein patterns (users simply place a hand over a sensor) and is expected to be a flexible, user-friendly authentication system. Face recognition and voice authentication systems that are also being developed will perform "natural" authentication: that is, users will be authenticated without being aware of the authentication process. This paper describes the biometric authentication work that has recently been carried out at Fujitsu Laboratories.



森 雅博（もり まさひろ）
ペリフェラルシステム研究所 所属
現在、情報システム向け個人認証技術の研究開発に従事。



新崎 卓（しんざき たかし）
ペリフェラルシステム研究所 所属
現在、指紋認証技術の研究開発に従事。



佐々木繁（ささき しげる）
ITメディア研究所メディアソリューション研究部 所属
現在、画像処理、音声処理、バイオ認証の技術開発に従事。

まえがき

Biometrics (バイオメトリクス) は、Biology (生物学) とMetrics (計測) の合成語であり、人の身体特徴量を用いて個人を同定する技術である。この技術は、情報システムへのアクセスが本人かどうかの認証 (本人認証) に利用されている。

今日までに様々な身体特徴量を使用したバイオメトリクス認証が研究および実用化されており、その一例を図-1に示す。バイオメトリクス認証はセキュリティの高さがよく強調されるが、高精度を確保するには利用する身体情報がある程度複雑で、かつ他人との差異が大きいことが本質的に必要である。指紋や虹彩、富士通が新しく製品化を目指す静脈紋様などがこの要件を満たす。バイオメトリクス認証は人におのずと付随する特徴量を利用し、記憶や物の所持などを利用者に要求しないことも大きな特長で、利便性や安全性が高い。顔や声による認証は、人が行う最も自然な識別方法であり、意識させずに認証することも可能で、今後の応用が期待される。

バイオメトリクス認証の特性

本人認証

本人認証には表-1に示す3種類がある。記憶による認証や持ち物認証は、提示されたものの正しさは

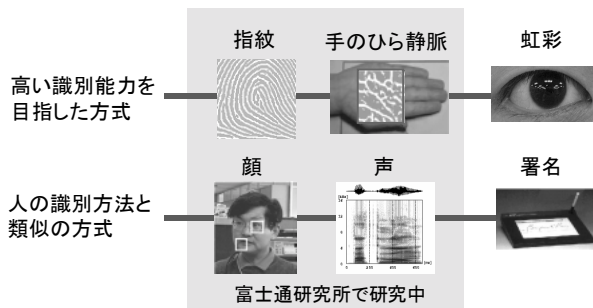


図-1 各種バイオメトリクス認証方式
Fig.1-Biometric authentication technologies.

表-1 本人認証方式

種類	例	長所	短所
記憶による認証	パスワード	正確な認証 低コスト	忘失・盗難・ 類推の恐れ
持ち物認証	IDカード 印鑑	正確な認証	紛失・盗難・ 偽造の恐れ
バイオメトリクス認証	指紋, 顔, 声, 署名, 静脈	忘失・盗難・紛失 なし, 偽造困難	認証精度が確 率的

正確に認証できる反面、提示したのが本人かどうかの確認は困難である。盗んだり拾ったりした情報による「なりすまし」に弱い。

バイオメトリクス認証は本人の身体情報を用いるので、原理的に他人による「なりすまし」を排除できる。認証に際しても特別なものを必要とせず、かつ、本人の行為であることを併せて確認できる特長がある。しかし、人の身体情報は採取するごとに多少変動するので、認証に際し本人が本人でないと判定されたり、また他人を誤認して受入れてしまったりする確率が存在する。このため、バイオメトリクス認証では、認証精度への正しい理解が重要である。

バイオメトリクス認証の精度

バイオメトリクス認証では一般に、あらかじめ登録してある特徴データと照合時に採取した特徴データとの類似度から本人判定が行われる。同一人からの特徴データは高い類似度を示し、別人のデータでは類似度は低い。判定のためのしきい値は両者の中間に設定される。

実際の集団の類似度分布をグラフ化したものを図-2に示す。同一人データの類似度は1 (=完全一致) 近くにピークのある分布となり、別人との類似度分布は0近くにピークを持つ。両方の分布が完全に分離していることが理想であるが、現実の身体特徴量では多くの場合、分布のすそ野の部分にオーバーラップが生じる。これは同一人でも採取ごとに特徴データが変動して類似度が低くなることもあり、また、別人でも差が小さい場合があることによる。ここで、しきい値を設定して判定を行うと、同一人でも別人として判定される場合 (本人拒否率FRR:

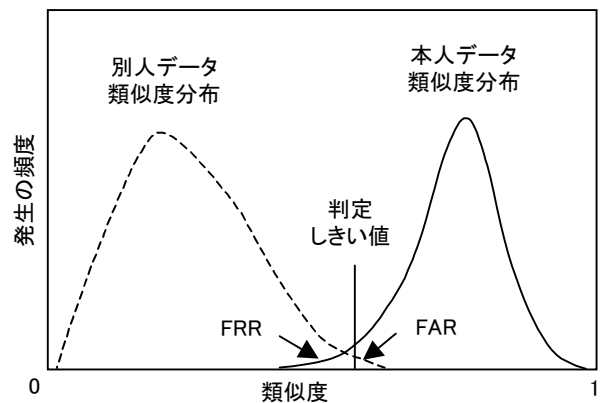


図-2 バイオメトリクス認証の精度
Fig.2-Accuracy of biometric authentication.

False Rejection Rate) や、別人が誤って本人として判定される場合 (他人受入率 FAR : False Acceptance Rate) が発生する。FRRとFARはトレードオフの関係にあり、単純に一方だけ良くすることはできない。

なお、分布グラフ交点のエラー率を等価エラー率 (EER : Equal Error Rate) と呼び、認証技術の精度性能の目安とする。小さいほど精度が高い。

高い認証精度の実現には適切な判定しきい値の設定が必要であるが、人の身体情報を対象としているので、しきい値は実験を通してしか得られない。偏りのない大きな母集団を対象にした実験評価を重ねて最適値を導き出すことになる。技術の開発途上や実用化初期には十分な精度でないこともあるが、フィールドからの積極的なフィードバックによって、より適切な値になっていく。

指紋認証

指紋認証は早くから実用化され、現時点で最も普及しているバイOMETRICS認証技術である。指紋には「万人不同」、「終生不変」という特徴があり、紋様を比較することで人の同定が可能である。指紋認証は高精度な識別を特長とする。

原理

指紋は、隆線 (りゅうせん) と呼ばれる皮膚が線状に隆起した構造が多数集まって紋様を成したものである。全体は同心円状であるが、個々の隆線はところどころで分岐したり終端したりしており複雑な紋様を形成する。隆線の分岐や終端部分を指紋特徴点 (マニューシャ) と呼び、この特徴点の位置・種類・方向の一致性比較が指紋認証の基本的な原理である (図-3)。指紋紋様のほかの特徴量として、渦や流れといった紋様全体の形、隆線の幅・ピッチなども利用される。

指紋センサ

指紋像の入力には光学的方法と静電容量を利用する方法がある。富士通研究所では、指紋認証の実用化当初は光学式指紋センサを開発、利用した。現在はサイズとコスト面から静電容量式の半導体指紋センサを用いている (図-4)。半導体指紋センサは入力面が硬く、低温や乾燥で指表面も硬くなっている場合には入力像がかすれやすくなる。自動画質補正技術やノイズ除去技術を開発して、認証への影響を

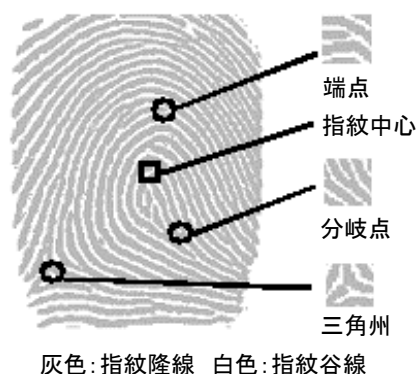


図-3 指紋特徴点
Fig.3-Fingerprint minutiae.

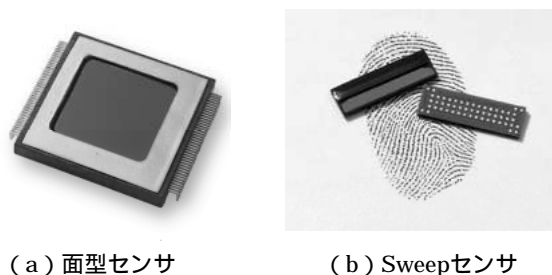


図-4 静電容量式半導体指紋センサ
Fig.4-Semiconductor fingerprint sensors.

防止している。

最近、モバイル向けに短冊状のSweep (Swipe) タイプの半導体指紋センサの実用化が始まっている。センサ上を指で走査することにより指紋全体像を採取する。実用化に向けて使いやすさや認証性能への影響の調査を進めている。

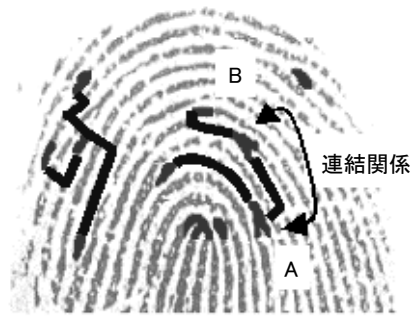
照合方式

2種類の照合方式を開発、実用化している。

(1) マニューシャ方式

マニューシャ方式は、指紋特徴点の位置・種類・向きを比較して判定する。認証精度の向上、とくに他人受入率を低減するため、特徴点情報に加え、特徴点間の連結関係なども評価する特徴相関 (Connected Minutiae Relation) 法と呼ぶ独自の改良型マニューシャ方式を開発して実用化した (図-5)。

多くの特徴量を判定に利用することで、本人受入率 99.96 % (2回以内の試行) と他人受入率 0.0001 % (100万分の1) 以下の高い認証精度を実現している (表-2)。登録データ量も1指あたり平均 300バイトと小さい。特徴点抽出 (約0.1秒) 後の



特徴点の位置・種類 + 特徴点の連結関係

図-5 特徴相関法

Fig.5-Connected Minutiae Relation method.

表-2 照合方式と性能

照合方式	特徴相関法 (マニューシャ方式)	形状相関法 (パターンマッチング方式)
他人受入率	0.0001%	0.01%
本人受入率 (2回試行)	99.96%	99.99%
照合時間	約0.1秒 Pentium4 2.4 GHz	1秒以内 ARM 約100 MHz
登録データ量	平均300バイト (最大600バイト)	約4 Kバイト

判定時間が数msと短いため、多数の判定を行うクライアント/サーバ型の認証システムや1対N認証(IDレス認証)にも適する。

(2) パターンマッチング方式

モバイル機器などへの組込用途では、搭載されるCPUの性能も限られ、コンパクトな照合方式が求められる。持ち主の認証ができればよい場合も多く、要求精度はあまり高くない。

パターンマッチング方式は紋様像全体を比較して同一性を判定する。処理が簡素で高速であるが、精度ではマニューシャ方式に及ばない。富士通研究所では、パターンマッチング方式に特徴点比較を加味した照合方式の形状相関法をモバイル用途向けに開発した。本人拒否の原因である不鮮明な特徴点の指紋に強く、他人受入率0.01%までの範囲ではマニューシャ方式より高い本人受入率を示す。プログラムも小さく、動作クロックが100 MHz程度の低速CPUでも認証時間は1秒と短い(表-2)。

精度

実用化している認証技術の精度を表-2に示す。認証精度を上げるため、10歳代から70歳代の一般の人数百人から実際に指紋を採取して評価している。

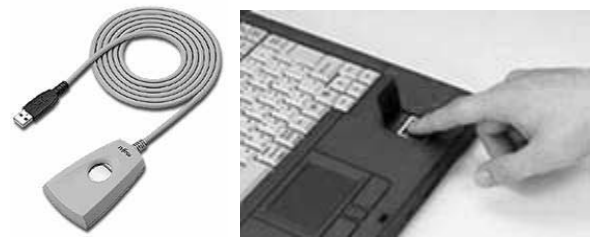


図-6 PC用指紋センサユニット
Fig.6-Fingerprint sensor units for PC.



最大500ユーザ
本人受入率:99.96%
他人受入率:0.0002%
照合時間:3秒

図-7 バイオ認証装置Secure Login Box
Fig.7-Secure Login Box.

指表面の状態は気温など環境の影響を受けやすい。同一人から季節ごとに指紋を採取して、環境の影響を受けにくい像処理の方法や判定条件を採用している。

指紋認証装置

PC用指紋センサユニットと認証ソフトを製品化している。センサユニットには、単体ユニット(USBおよびパラレルI/F)、キーボード組込型、ノートPC組込型がある(図-6)。認証ソフトによりWindowsログオンやスクリーンロック解除が実現でき、PC自体を高セキュリティ化できる。認証システム開発用のソフトウェアキットも製品化されている。

バイオ認証装置Secure Login Box

指紋認証をより手軽に利用できるように、導入のしやすさ、使いやすさを考慮し、低価格化したオフィス向けソリューションとして図-7に示すバイオ認証装置Secure Login Boxを開発、製品化した。LANで接続されたPC環境を対象に、指紋認証機能と登録情報の管理機能、データベースを組み込んだ小型の専用装置とし、従来システムと比較して約1/10の価格を実現した。以下の機能と特長を備える。

(1) アプリケーションとの自動連携

既存の業務アプリケーションやシステムに変更を加えることなく、指紋認証の導入を可能とした

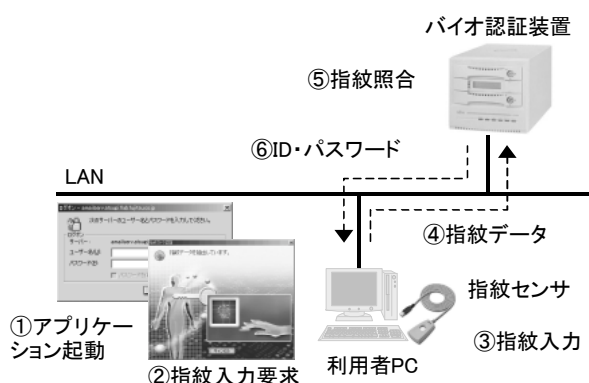


図-8 アプリケーションと指紋認証の自動連携
Fig.8-Authentication operation flow.



図-9 指紋認証付ICカードリーダー
Fig.9-IC-card reader with fingerprint authentication.

(図-8)。ID・パスワード認証を要求するアプリケーションを登録しておく、認証が必要な場面で自動的に指紋入力が要求され、照合に成功するとアプリケーションへのログインが行われる。ユーザは画面要求に応じて指をセンサに置くだけで認証されて、アプリケーションが利用可能となる。各種WindowsアプリケーションやWebページの認証に対応している。

(2) 簡単な導入・運用

必要なハード・ソフトを内蔵した専用装置にすることで、簡単な設定で指紋認証システムを構築できるようにした。運用管理はネットワーク内のどのPCからでもWebブラウザを用いて行える。登録データは2重化 (RAID-1) とバックアップ機能により高い信頼度で保護される。また、暗号化と独自プロトコルで、通信路や格納データのセキュリティを強化した。

(3) 高速・高精度指紋照合

指紋照合エンジンを高速化して、従来困難であったIDレス認証 (最大100人) を実現した。認証時は単に指を置くだけでよく、ID入力の煩わしさがなく、使いやすさが大幅に向上した。指紋の類似度に応じた処理を行い、はっきりと異なる場合は短時間で処理を打ち切り、本人の可能性が高い場合のみ精密な照合を行うことで、100人200指の中から本人を3秒以内に特定する。装置はIDレス認証対象者を含め500人分の登録データを収容できる。

指紋認証付きICカードリーダー

本人認証を含むシステム動作全体のセキュリティ向上のため、高機能ICカードリーダーと指紋認証を組み合わせた装置を開発した (図-9)。

手のひら静脈認証

手のひら静脈認証は、静脈パターンに基づく認証の一つである。静脈パターンに基づく認証では、静脈の網目のように見える模様をパターンとして扱い、あらかじめ登録しておいたパターンと認証時に読み取ったパターンを照合することにより本人を確認する。

静脈を含めて血管のパターンは、一般的に、双子を含めて万人不同といわれている。また、胎内で定まった後、大きな怪我などがなければ、大きさが変化する以外、トポロジー的に経年変化がないともいわれ、大変安定した情報である。さらに、体の中の情報であるため、体の外からの攻撃 (盗み見、変形) を受けにくく、信頼性が高い。

静脈パターンに基づく認証には、ほかに、手の甲の静脈認証、指の静脈認証がある。手のひらは、手の甲に比べると、メラニンが少ない、毛が生えないという性質があり、静脈を読み取る障害が少ない。そしてなにより手のひらを用いた認証は、手の甲の静脈、指の静脈の認証と比べて、認証時のユーザの動作が最も自然な動きであると言え、幅広いソリューションに適用できる可能性が大きい。

原理

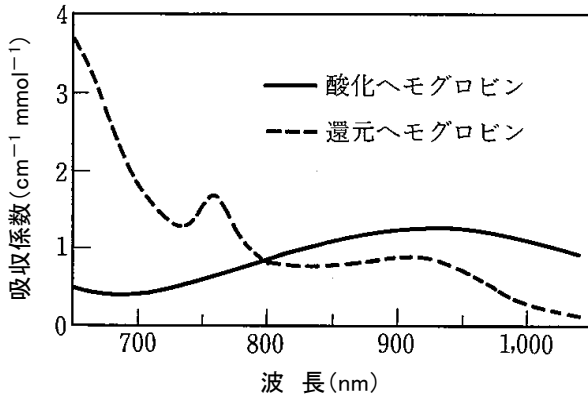
静脈には還元ヘモグロビンが流れている。動脈中の酸化ヘモグロビンに対して、静脈中の還元ヘモグロビンは酸素を失ったヘモグロビンである。この2種のヘモグロビンは吸収係数が異なる (図-10)。とくに、還元ヘモグロビンは近赤外光領域の約760 nmの波長の光を吸収する。そのため、手のひらに近赤外光を当てると、静脈が存在する部分だけ

光の反射が少なく、画像上、暗く映る（図-11）。画像処理により抽出した静脈部分を図-12に示す。

装置

接触型（図-13）と非接触型（図-14）の二つのタイプの装置を試作し、有効性を実証した。

接触型はオフィス環境への適用を目指したもので



出典：コロナ社生体情報の可視化技術編集委員会編「生体情報の可視化技術」(1997)

図-10 ヘモグロビンの吸光スペクトル
Fig.10-Absorbing spectrum of hemoglobin.



図-11 近赤外画像
Fig.11-Near-infrared image.

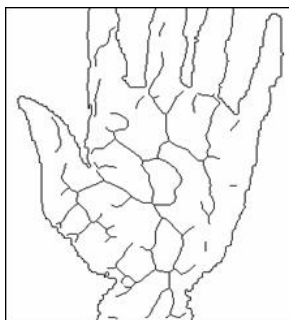


図-12 静脈抽出画像
Fig.12-Extracted vein pattern.

あり、マウスの形をしている。マウス型装置は、手のひら静脈認証とマウスの二つの機能を同時に実現する。マウスを握ったとき、手のひらが当たるところの窓から近赤外光の照射、および撮影を行う。

非接触型は、公共の場や医療業務など、心理的に違和感を抱かれないように個人を認証する場面や、衛生面の要求の高い場面への適用を目指したものである。装置の表面から近赤外光の照射、および撮影を行う。登録時も認証時も、装置の表面へ手のひらをかざすだけで使用できる。

照合方式

静脈パターンの照合処理は、画像処理に基づくパターン認識技術を使用している。静脈パターン中の特徴に基づくマッチング方式により、手のひらの様々なかざされ方に柔軟かつ高速に追従する。

非接触型は接触型に比べ、手が装置にかざされるたびに、手の位置、向きが大きく変動したり、手が撮影部分を完全に覆わないため、背景が映り込む。



図-13 接触型（マウス型）装置
Fig.13-Contact-type (Mouse-type) unit.



図-14 非接触型装置
Fig.14-Contactless-type unit.

そのため、様々な背景画像の中から安定して手の位置を検出できる技術を開発した。

精度

手のひら静脈パターンの個人識別力については、まず、良好な照明状態のもと、手のひらを固定して撮影した700名の手のひら画像を用いた実験により、すべての人を登録し、かつ、すべての人を識別できることを確認した。これは、使用したデータ数の統計的な限界性能として、等価エラー率0.5%（本人拒否率と他人受入率が等しくなるエラー率）に相当する。

また、非接触型装置に対する実験では、10代から70代、年齢・性別均等、就業・非就業および事務職、労務職比率は総務省統計局統計センター発表の統計に従った計700人、のべ1,400の手のひらデータを用いて本装置を評価した。その結果、2回登録の場合、理論的に、等価エラー率0.78%を確認した。また、本人受入率99%のとき、他人棄却率99.5%以上であることも確認した。

応用

手のひら静脈認証装置の照明機器、撮像機器およびその制御部は光学モジュールとして取り出し、様々な装置に組み込むことができる。光学モジュールは、壁や専用端末などに組み込むことで、入退室管理などの高セキュリティ市場分野、衛生面で非接触型の要求が高い医療システム分野でのソリューションが期待できる。

顔 認 証

顔認証とは、人の顔面の映像からその人が誰なのかを認証する技術である。人が個人を認証する場合でも顔面を見て判断することが極めて多い。それは、人の顔面が外見から誰でも容易に観察することができる唯一の特徴であることが大きな理由である。このように、顔認証では、ほかの個人認証と異なり、接触また近接で認証するのではなく、離れた場所からでも認証できるというメリットがある。

原理

顔認証では、指紋や虹彩のように模様ではなく、ある時刻での顔の状態を特徴として使う。しかし、顔は極端に変貌へんぼうすることは稀まれではあるが、常に変化している。時間の経過のほか、例えば、喜怒哀楽を示す表情も変化の代表例である。また、化粧や変

装のように人為的に変化を加えることも容易である。

さらに、顔に変化を与えるものとして、照明がある。メリットとして、遠方から認証できることを前述したが、離れているために、顔には外乱光の影響を受けやすく、髪や鼻梁びりょうの影などの陰影を差すことが多い。

このように、特徴そのものの変化や外乱光による変化を含む顔の映像から、いかに安定な認証を実現するかが、顔認証の大きな課題となっている。

照合方式

富士通研究所では、顔の変化のうち、とくに、遠方から撮影した際、顔の向きが変わり、顔の見え方が変化する問題に取り組んでいる。開発した手法は、局所パターン照合法と名付けた方法で、図-15のように、窓と呼ぶ目、鼻、口の周りの小さな領域ごとに、あらかじめ登録したデータと照合する方法である。具体的には、映像の全画面から顔の部分を探し、顔の中で明るさの変化の大きい部分を窓とする。それぞれの窓に対して、離散コサイン変換に基づいた類似度を算出し、その類似度から個人を同定する。本手法では、多数の窓を用いて独立に類似度を算定するため、見え方が多少変化する場合においても安定した認証が可能である。

精度

拡散光源を使うなど理想的な撮影条件のもとで700名を対象に評価した結果、正面顔では、認証能力を示す等価エラー率が0.9%、±15度の姿勢変動では1.6%という世界でトップクラスの顔認証エンジンと同等の性能を実現していることを確認した。

応用

顔認証に使う顔の映像は目視でも確認可能である。そのため、映像を認証結果とともに記録することで



図-15 局所パターン照合法
Fig.15-Local feature-based matching.

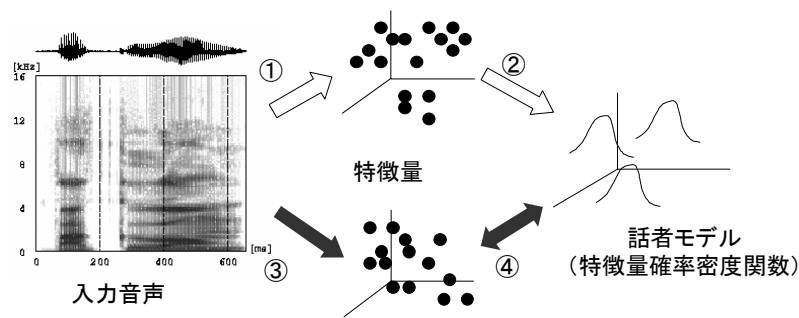


図-16 確率モデルを用いた声紋認証
Fig.16-Voice verification using probabilistic model.

結果の確認や認証失敗へのフォローアップの可能性など、顔認証はシステム構築面でメリットがある。

今後は、表情の変動、照明変動など、いわゆる環境変化への取組みを引き続き行い、顔認証のメリットを生かしたシステム展開を進めていく。

声 紋 認 証

声紋認証とは、人間が発する声を分析して得られる特徴を用いて、あらかじめ登録した本人であるか否かを判定する技術である。声紋認証は、マイクに向かって話すという自然な行為によって認証するので、抵抗感も少なく簡便であり、マイク以外の特別なハードウェアを追加する必要がないというメリットもある。

原理

声紋認証は、発声するという行動によって観測される情報を用いての認証である。登録時と認証時の時期・場所・雑音環境の差に伴い、発声の仕方に違いが出てくることもある。声紋認証では、そのような違いに影響されることなく、認証精度を向上させることが課題となっている。

照合方式

富士通研究所では、声紋認証の精度向上のために、登録時と認証時の声の差を確率モデルで吸収する方式を開発した。確率モデルを用いた声紋認証の流れを図-16に示し、その手順を以下に述べる。

(1) 登録時の手順

入力音声から特徴量を計算

特徴量の分布から、正規分布の確率密度関数の複合体として話者モデル作成

(2) 認証時の手順

入力音声から特徴量を計算

話者モデルと照合して類似度を計算し、しきい値以上なら本人と判定

特徴量の時系列パターンをそのまま話者モデルとする従来方式に比べ、本方式は、確率モデルを話者モデルとするので、発声のゆらぎを表現でき、登録時と認証時の発声の変動に対する頑健性が向上している。

応用

声紋認証は、テレフォンサービスや、電話で声による各種情報サービスを提供する音声ポータルサービスへの応用などに適している。音声認識、音声合成、そして声紋認証を組み合わせることにより、利用者に対し、セキュリティやプライバシーに関わるサービス、また個人別にカスタマイズしたサービスの提供が可能となる。

む す び

本稿では富士通研究所で研究開発を行っているバイオメトリクス認証技術から四つの方式を紹介した。

情報システムにおける人の認証はますます重要となっている。確実さ(精度)だけでなく、利用者への負担、認証の自然さ、本人の意思の確認または逆に無意識な認証など、提供するサービスに応じ要求は多様化している。バイオメトリクス認証技術は、利用する身体情報により様々な特徴を備え、しかも本質的に利用者への負担が少ない。今後、多様な特徴を生かした広い応用が期待される。