コンピュータセキュリティ　5－7
（1999．5．21）

多重バイオメトリックスによる個人認証

坂野 鋭，劉偉傑
（株）NTTデータ マルチメディア技術センタ

あらまし

コンピューターの物理的セキュリティのためのバイオメトリック個人認証技術は，近年のデバイスの低価格化に伴い，急速な進展を見せている．しかしながら，バイオメトリック個人認証技術には，認証確率が100%ではない，傷害などで使用できないケースがある，などの導入の障害がある．本報告では，こうした課題に応えるための多重バイオメトリック個人認証技術について，複数のデバイスからの認証結果を用いて統計的パターン認識の方法で高精度化する手法を提案し，実験で有効性を確認した．

和文キーワード　生体学的個人認証，統計的パターン認識，情報統合

Person Authentication by Multiple Biometrics

Hitoshi Sakano , WeiJie Liu
Multi Media Technology Center, NTT Data Corporation

Abstract

Biometric person authentication is emerging with needs for real world computer security. However, biometrics has a couple of shortcomings. low relierbility , some people cannot use since injure, lost of organ etc. Multiple biometric technique is one of solution of the short comings. We propose novel integrate method for high acculate person identification based on statistical pattern recognition. Experimental results shows effectiveness of proposed method.

英文 key words　Biometrics,Statistical pattern recognition,information integration

1 はじめに

本報告では, 複数のバイオメトリック個人認証技術を組み合わせた多重バイオメトリックスにおいて, 統計的パターン認識の方法を用いて多重化後の認証精度を最適化する方法を提案する.

インターネットなどのオープンネットワークの発達とともに, ネットワーク上での不法アクセスを防止するための技術がコンピューターセキュリティの中心的な課題として論じられてきた. 暗号技術が成熟し, 公開鍵暗号などの技術や第3者認証局などの仕組の提案でコンピューター社会の秩序を保つ枠組みは一応整備されたかに見える.

しかしながら, 暗号鍵や電子署名情報は多くの場合, 端末の記憶装置やICカードなどの媒体に記憶されており, これらの装置に物理的に不正アクセスが行われた場合の対策は, 現在のところパスワードだけという状況がある.

現実のコンピューター犯罪の多くは端末の不正使用などの物理世界で発生しており, 犯行主体も組織に不満を持つ社員など, 内部の状況に知識を持った主体である. 内部犯行の場合, 他人のパスワードを推測することは容易であり, また,ICカードなどの所有物による認証を組み合わせた場合でも盗用することは比較的容易と言える. つまり, パスワード/ICカードによる本人認証は極めて脆弱なセキュリティであると言わざるを得ない.

こうした問題を解決できる方法として現在注目されているのが, 指紋認識に代表される生体学的個人認証技術である. * 生体学的個人認証の方法は, 人間の生物学的な個性を自動識別することにより個人認証を行う方法であるため, 盗用が極めて困難である. また, パスワードと異なり忘却などで失われる可能性も低いために, セキュリティレベルの向上とともにユーザビリティの向上を図ることも出来る.

しかし, 現時点では生体学的個人認証技術は必ずしも完成した技術とはいえない. 例えば, 生体学的個人認証技術はパターン認識技術に基づくため, 100%確実に動作する保証がないし, 傷害や障害などの理由で全てのユーザーに適用可能な訳ではない. こうした問題を解決するために現在検討が進んでいるのが, 複数の生体学的個人認証方式を組み合わせる多重バイオメトリックス† である. 複数の生体学的個人認証技術を組み合わせて用いることにより, 精度, 適用可能性が向上すると考えられ, 特にハイセキュアな領域には魅力的な方法と考えられる.

本報告では, **2.** で現在の生体学的個人認証技術を概説したあと, 多重バイオメトリックスに関する従来の研究を概観する. **3.** で我々の手法を提案し, **4.** で実験によって提案手法の有効性を検証する. **5.** で今後の課題を述べる.

2 生体学的個人認証技術

2.1 生体学的個人認証技術

2.1.1 生体学的個人認証の一般論‡

生体学的な特徴を計算機によって自動的に認識する技術の研究は1960年代に開始され,80年代にはFBIが指紋認識技術を採用した.80年代後半には年金受給者の認証に用いるなど, 犯罪捜査以外の目的への応用も始まっている. しかしながら, 近年に至るまでは指紋をはじめとした生体学的個人認証製品は高価で扱いづらいものであったため, 特殊な目的以外には用いられることが少なかった.90年代に入り, 計算機の処理能力が飛躍的に向上し, 個人認識技術はその多くをソフトウェアで実装出来るようになった. その結果, 劇的なコストの低減が実現し, 導入実例は着々と増えつつある.

現代的な意味での生体学的本人認証技術は

定義 人間の生物学的な特徴を用いて自動的に個人を特定する技術.

のように定義される.

生体学的本人認証技術には, 指紋など, 生体の形状を計算機で自動認識する技術と, 書字動作などの意識的な動作を認識する技術に大別されるが, どちらの方法でも, 認証は基本的にはテンプレートと呼ばれる個人個人の生体の特徴を記録したデータと使用時の入力データを比較することで行われる. 比較の際には何らかの尺度に基づく類似度が算出され, これが事前に設定された敷居値を上回るかどうかを判断することで認証が行われる. 敷居値の設定は低すぎれば他人の侵入を許し, 高すぎれば本人を排除する傾向がある. 生体学的個人認証技術は認識誤りは本人排除率 (FRR:False Rejection Rate), 他人受入率 (FAR:False Acceptance Rate) の二つの指標で評価される. これは当然敷居値により変化するが, 敷居値を上げるとFARは減少していき,FRRは増加していく, この交叉点での認証誤り率を交叉誤り率 (XER:Cross over Error Rate) と呼び, 評価の指標として用いている. この様な前提の上で, 以下, 個別の技術について概説する.

---

* 英語では **Biometric person authentication** であるが, 現在 **Autherize** された訳語は存在しない. 直訳は「生体計測による個人認証」であるが, 本報告では「生体学的個人認証」もしくは「バイオメトリックス」という言葉を用いる

† 英語では **Multiple biometrics** , もしくは **Multimodal biometrics** であるが, 当然この訳語も固定していない.「多重生体学的個人認証」という訳語が考えられるが, 語感が悪いので本報告では「多重バイオメトリックス」という言葉を用いる

‡ 本項で紹介する技術の詳細については [1] に詳しい. また, 適用実例等については [2] を, 最新の情報は常に [3] で紹介されている.

2.1.2 指紋認識技術

犯罪捜査の実績から，現在最も進んだバイオメトリック個人認証技術である．指紋は指の先端にある線状のパターンであり，個人ごと，指ごとに異なる形状であるとともに生涯不変であることが知られている．

代表的な指紋認識装置では光学的スキャンにより指紋表面の凹凸を陰影の形で取り込み，テンプレートと照合する．照合方式にはさまざまな方法があるが，大きくパターンマッチング方式と特徴点解析法式に分類できる．パターンマッチング方式は文字どおり記憶している指紋画像を入力画像と重ね合わせることで比較を行う方式で，アルゴリズムが単純であることから初期の研究ではよく用いられていたが，テンプレートサイズが大きくなる，多大な処理が必要であるなどの理由から現在はあまり用いられていない．特徴点解析法式は，指紋の分岐点，端点などの特徴的な部分に注目し，特徴点の位置，特徴点における指紋の畝の方向を比較することにより照合を行う．この方式では特徴点の座標，性質だけをテンプレートに保存すればよいのでテンプレートサイズが小さく，また指紋画像を記憶しないことから個人のプライバシーの保護の観点からも優れており，現在の製品の殆どはこの方式となっている．

指紋認識技術における課題は，乾燥肌など指紋が消失もしくは劣化しているユーザーが時として存在することである．現在のところこの問題に対する本質的な解決策はなく，そのユーザーがセキュリティホールにならないために運用を工夫することで対処が行われている．

2.1.3 虹彩

虹彩，つまり瞳の周辺の黒目部分に沈着する脂肪のパターンを用いて個人を識別する方式である．虹彩の脂肪沈着はほぼランダムで，しかも2歳くらいで固定し生涯不変であるとされている．

標準的な虹彩認識系では目に赤外線を投射し，その反射で得られた画像を入力とする．入力画像に対しては虹彩部分を同心円状に分割し，その上で濃淡の変化をコード化したものをテンプレートもしくは比較のための信号とする．照合処理は単純に上記のコード列を比較することで行われる．虹彩による本人認証は指紋と同程度の精度があることが実験的に確認されつつある．しかしながら，極端に虹彩の大きさが平常と異なる個人の場合には虹彩のコード化が不可能であるという問題もある．

2.1.4 網膜

網膜上の血管パターンを用いて本人を認証する方式である．網膜に限らず，殆どの血管の分布はほぼ乱数的であることが知られており，これを画像として取り込むことが出来れば本人の認証に用いることが出来る．

標準的な網膜認識系では，網膜が目の際奥部に位置するために比較的強い赤外線を用いて血管パターンの画像を撮影する．そのため，虹彩の場合とは異なり，部屋を暗くするか，特定の装置を覗き込む形で実装されることが多い．網膜による本人認証は少なくとも指紋，虹彩と同程度に高精度であるが，緑内障などの病気があった場合には用いることが出来ないという問題がある．

2.1.5 手形状

手の3次元的な形状を利用した個人識別技術．人間の手には指の長さ，太さ，手そのものの大きさなどのさまざまな特徴がある．これを利用して個人の認識を行う技術である．

手形状を用いた認証方式は，ユーザーの受容性が高く，テンプレートサイズが9バイトしかないという，利点からアトランタオリンピックで入退室管理に使われてから広く使用されるようになった．しかし，交叉誤り率が0.1%から0.2%と指紋や虹彩に比較すると認証誤りの確率が高いという問題もある．

2.1.6 サイン

サインなどの特定の図形を書くときのペンの動き方を利用した個人識別技術．現在実用になっているサインによる本人認証技術は，タブレットなどの時系列計測が可能な装置の上で行われたサインを照合する．

標準的なサイン認識装置では汎用のタブレットなどの装置の上で書字動作を行った際のペンのアップダウンのタイミング，描画された線の形状を比較することで認証を行う．不法傍受などの方法でデータが盗まれた場合でもテンプレートの変更が容易であるというメリットを持つためオープンネットワークでの利用に適していると言える．

問題は，書字動作をコピーした攻撃者の排除がどの程度可能であるかについて具体的な評価が殆ど行われていないことである．小規模の実験では交叉誤り率0.2%程度との報告があるが，現実的にどの程度の認証精度が得られるかは保証されていない．

2.1.7 声紋

音声が個々人で異なることはよく知られているが, これを本人の認証に用いる技術である. 基本的な技術は音声認識技術と酷似している.

音声による本人認証技術は通常のマイクロフォンを用いることが出来るため, 非常に安価に実装でき, さらに電話を経由して用いることが出来るという点でネットワークでの利用に既に対応しているとも言える. 大きな問題は人間の音声は数ヶ月のゆっくりしたスケールで変動しているために, 登録から時間を経過すると認証精度が徐々に落ちていくことである. また, 認証精度も交叉誤り率 1%程度と, 指紋などの精度と比較すると低い.

2.1.8 顔

顔による本人の認証は人間にとって最も自然な認証方式であるため, 早期から研究が進められていたが 90 年代に入って部分的に実用化した. 顔は 3 次元的な物体であるため, 姿勢や光源により大きく見え方が変化するという大きな技術的な問題がある. 現在製品化されているものはこれらの問題を本質的に解決したものではないが, 技術的な工夫により, ある程度の頑健性を確保している.

しかし一方で, 交叉誤り率が 1%程度と精度が低い. 光源条件が極端に変わる状況では利用できないなどの制約も多く, 今後の研究が期待される.

2.1.9 生体学的個人認証技術の課題

いくつかの生体学的個人認証技術を紹介してきたが, これらに共通する課題は, 前述の通り

1. 認証精度が 100%ではない
2. 傷害などにより, 特定のユーザーが使えない場合がある

の 2 点である.

認証精度の問題は各分野で常に改良の努力が続けられているが, 生体が必ずしも不変ではないこと, 信号入力時の雑音を完全に防ぐことが不可能であることから完全な信頼性は得られない. また, 社会で生活する以上, 全ての人間が事故を回避できるわけでもないため, 全ユーザーが使用可能な認証系は存在し得ない.

多重バイオメトリックスは, この二つの問題を完全に解決するものではないが, 特に適用可能性を大幅に拡大する. 一方でどのような組み合わせ方をすると認証精度が向上するかは必ずしも自明ではなく, 主としてパターン認識分野で活発な研究が行われている. 次節では多重バイオメトリックスに関する従来の研究を概観する.

2.2 多重バイオメトリックスに関する従来の研究

複数の生体学的個人認証技術を組み合わせること自体は運用/精度向上などの観点から自然な発想であり, 既に米国では製品も発表されている. 本節では多重バイオメトリックスを用いた認証精度向上に関する従来の研究を概観する.

2.2.1 論理的手法

論理的統合手法の最も簡単な例は, 認証機械が 2 つの場合でその出力の AND もしくは OR をとって認証精度の向上を図る. ただし, 容易に想像できる通り, AND を取った場合は FAR のみが減少し FRR は増加する. OR を用いた場合は逆である. また,3 つ以上の認証機械が組み合わされた場合には, 多数決を用いる例もある. このタイプの論理で興味深いのは Dieckman[4] らの実験結果である. 彼らは 3 種類の個人認証機械のうち,2 つの判定が一致することを条件として, 顔, 音声, 唇の動きを用いた認証実験を行った. その結果として,3 つの認証機械の一致を条件とした場合より総合性能が向上することを示した.

2.2.2 統計的手法

n 個の個人認証機械から出力される類似度 $s_i(i = 1,\ldots,n)$ に対して, 実験データから与えられる分布関数 $P(s_i|$ 本人$), P(s_i|$ 他人$)$ を用いて統合確率密度関数 $p(s_1,\ldots,s_n|$ 本人$), p(s_1,\ldots,s_n|$ 他人$)$ を計算することにより, 本人認証を行う手法である.

通常, 生体学的な個人情報は独立事象と考えてよいため, 単純な積, 和の規則で統合確率密度関数が計算でき, 精度の向上を図ることが出来る [6][5].

しかしながら, 分布関数 $P(s_i|\cdot)$ を計算するためには分布形状に関する仮定が必要であり, この仮定が誤った場合には正確な推定を与えないという問題がある.

また, 統計データに基づいて , 複数の論理と敷居値の双方を最適化するという手法も提案されている [7].

3 識別的手法に基づく多重バイオメトリックス

前節までに, これまでの統合手法では, 必ずしも統合後に最適な個人認証メカニズムを構築できないということ

を示してきた. 論理的手法の場合には, 結局個々の認証機械の認証結果をそのまま用いるため, 認証結果が矛盾したときには結局どちらかの出力を信用するかを考える問題になってしまい, ハイセキュアなシステムで多少の FRR の増加が問題にならない応用場面などを除くと殆ど利点がないと言ってよい.

一方, 統計的手法では, 分布関数の正確な推定が困難であるために, 結果的に統合結果も不安定なものになってしまう. 統計的手法の問題点は, 従来パターン認識分野で研究されていた識別器の設計問題と類似している§.

統計的パターン認識では, あるカテゴリωに対して, 確率密度関数 $P(\vec{x}|\omega)$ を計算し, 入力された特徴ベクトル$\vec{x}$に対して, 最大の確率を与えるカテゴリを認識結果として出力する. この問題の場合も, 最適な密度関数を推定することが困難であるために, 識別器械の設計が困難であるという問題があった.

近年, こうした困難を回避するために発展してきた方法が, 「密度関数を推定せず, 密度関数で与えられる識別境界のみを推定する」という, パラダイムである.

我々は, 多重バイオメトリックスにおける情報統合問題を, 上記のパラダイムで定式化し, 識別器を用いて統合結果を計算する手法を提案する.

問題の定式化自体は, 統計的統合手法と基本的には類似している. n 個の認証機械からの類似度の出力を $s_i, i = 1, \ldots, n$ としたとき, これを n 次元のベクトル$\vec{s}$と考える. 本報告ではこのベクトルの存在する空間をスコア空間と呼ぶことにする. すると, 統合後の認証問題は学習に用いるデータ群$\vec{s}_{correct}$ $\vec{s}_{false}$ の識別問題と考えることが出来る. 以下, この定式化に基づいて, 個人認証実験を行っていく.

4 認証実験

4.1 実験で用いる識別器

上記の定式化を実験のために具体化する. 図 1 に示すように, 二つの認証機械 A,B のスコア s_A, s_Bで作られるスコア空間には, 3 種類の領域が作られる. つまり認証機械 A,B の出力がともに個々の認証機械の敷居値 T_A, T_Bを超えており, 双方とも受理となる領域 I , A,B の出力がともに棄却となる領域IV, A,B の出力が矛盾する領域II, III である. 統合において問題となるのは領域II, IIIであるから, 領域II, IIIに識別器を適用することを考える. 今回は統計的識別器としてユークリッド距離に基づく最近接規則を用いる. つまり, 領域II, IIIにおいて, 受理となるデータ, 棄却となるデータそれぞれを平均して, それぞれ受理, 棄却の標準データとする. 認証時には個々の識別器のスコアに対して, 標準データからのユークリッド距離を計算し, 近い方の結果を統合出力とする.

§ 本項で用いるパターン認識技術については良書が多数あるが, 日本語の物では [8] が優れている

表 1: Closed 実験の結果

	声紋	顔	提案手法
FAR	15.7%	1.0 %	1.2%
FRR	11.0%	18.0%	5.0%

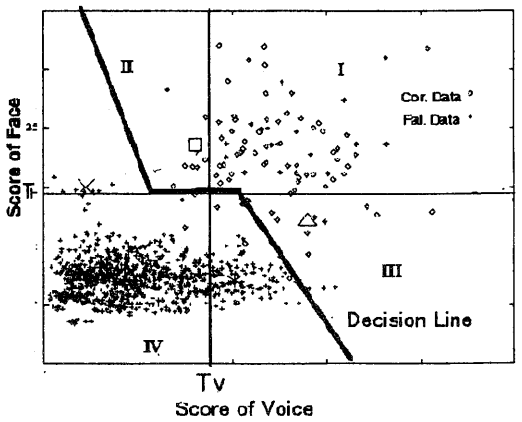

図 1: Closed 実験の識別面

4.2 実験で用いる認証機械

今回の実験では個別の認証機械として, 顔及び声紋の認識機械を採用する. 顔認識機械としては Turk の固有顔法 [9] を赤池情報量基準で最適化した [10] アルゴリズムを採用した. 声紋認識機械としては, 音声から LPC ケプストラム特徴を抽出し, 隠れマルコフモデルでマッチングする手法 [11] を採用した.

4.3 Close 実験

提案手法の有効性を示すための個人認証実験を行った. 最初の実験は, 識別面を作るために用いた個人と認証の対象となる個人が同じ場合である. 10 人の被験者について, 顔画像, 音声を 10 回収録し, うち 5 つを平均値を作るための学習データ, 残り 5 つを評価データとして用いた. 実験結果を表 1 . に, その時に作られた識別面を図 1 に示す. 提案手法によって劇的に認証精度があがったことがわかる.

表 2: Open 実験の結果

	声紋	顔	提案手法
FAR	14.3%	14.6 %	10.0%
FRR	6.0%	14.7%	9.7%

4.4 Open 実験

次に, スコア空間で識別器の設計に用いた個人と, 認証対象が異なる場合について実験を行った. Open 実験と同様, 79 人の被験者から, それぞれ 10 の顔画像, 音声を収録し, 50 人を識別器の設計に用い, 29 人を評価用データとして用いた. 実験結果を表 2. に示す. Closed 実験の場合ほど顕著ではないが, 認証精度の向上が見られる.

5 まとめと今後の課題

本報告では多重バイオメトリックスにおいて, 識別的手法を導入することを提案し, 顔と声紋を用いた個人認証実験で提案手法の有効性を検証した. 提案手法は極めて簡便に高精度な個人認証を提供する意味で有力であるが, セキュリティレベルの設定が困難であるなどの問題点を残している. また, スコア空間でどのような識別器械を用いるのがよいかは応用場面の状況に依存する側面もあり, 最適な技術を選択することは困難である. 今後はこうした問題点を実験的に検証し, 提案手法の有効性を確認していく.

謝辞

本研究の貴重な機会を頂いた当社マルチメディア技術センタ, 鈴木達郎所長, 林誠一郎部長, 桜井洋一部長, 坂本弘章課長, オープンシステム開発センタ武川直樹博士に感謝致します. また, 日頃討論頂いている当社技術開発本部同僚諸氏, 文献調査などに協力していただいた理化学研究所 坂野貴子博士に感謝します.

参考文献

[1] A. Jain and R Bolle, S. Pankanti ed. "Biometrics Personal Identification in Networked Society", Kluwer, (1999)

[2] "Biometric report 1999", sjb reserch, (1998)

[3] Biometric consortium homepage, http://www.biometrics.org

[4] U. Dieckman, et. al. "SESAMI: A Biometric Person Identification System Sensor Fusion", *Proc. 1st conf on AVBPA*, pp. 301-310, (1997)

[5] E. S. Bigun , et. al. "Expert conciliation for multi modal person authentication systems by Bayesian Statisticas" In Proc 1st conf of AVBPA, pp.327-334,(1997)

[6] J. Kittler, et.al. "Combining evidence in multimodal perspn identity recognition system", In Proc. 1st AVBPA,(1997)

[7] Weijie Liu, et. al. submitted to *Fusion 99*

[8] 例えば, 石井, 上田, 前田, 村瀬,「わかりやすいパターン認識」, オーム社,(1998)

[9] M. Turk and A. Pentland, "Face recognition Using Eigenfaces", Proc. CVPR, pp.568-591(1991)

[10] 坂野, 武川,「AIC による部分空間次元数の決定法」, 信学技報, PRMU97-173,(1997)

[11] 松井知子,「HMM による話者認識」, 信学技報,SP95-111,(1996)

[12] 坂野, 磯部, 劉, 春山, 武川,「顔と音声のスコア統合による個人認証」, 信学総大, D-12-60, (1997)

[13] 山口, 福井, 前田,「動画像を用いた顔認識システム」, 信学技報, PRMU97-50, (1997)