

推薦論文

多重仮説における逐次確率比検定を用いた ID レス生体認証の高精度化

村上 隆夫^{†1} 高橋 健太^{†1}

近年、ユーザが生体情報のみを入力することで認証が行われる ID レス認証の利便性の高さが注目されており、様々なアプリケーションへの適用が進んでいる。しかしながら、ID レス認証では登録ユーザ数の増加にともない認証精度が劣化し、これが ID レス認証を大規模ユーザシステムに適用するうえでの大きな課題となっている。この問題を解決するために、複数の生体情報を用いるマルチモーダル認証技術を用いることで精度を高める手法が提案されているが、ユーザに複数の生体情報を入力させることで利便性が低下する。本稿では、多重仮説においてデータの平均観測回数を最小化する逐次確率比検定を基に、生体情報の入力回数を最小限にとどめつつ、精度を高める手法を提案する。従来手法との比較実験を通して、その有効性を示す。

Accuracy Improvement of Biometric Identification Using Multihypothesis Sequential Probability Ratio Test

TAKAO MURAKAMI^{†1} and KENTA TAKAHASHI^{†1}

Biometric identification has lately attracted attention because of its high convenience; it does not require the user to enter the user ID. The identification accuracy, however, decreases as the number of the enrollees increases. Although many multimodal biometric techniques have been proposed to improve the identification accuracy, it requires the user to input the multiple biometric data and makes the application less convenient. In this paper, we propose a new multimodal biometric technique that reduces the number of inputs by adopting the multihypothesis sequential test that minimizes the expected sample size. The results of the comparison experiment showed its effectiveness.

1. はじめに

ユーザが (ID を入力せず) 生体情報のみを入力し、システムが DB に登録されている N 人のユーザと順次スコア (類似度, あるいは距離) を求めることで、ユーザを一意に特定する生体認証を ID レス生体認証 (または ID レス認証, $1:N$ 認証) と呼ぶ。この認証手段を用いた場合、ユーザは自分の生体情報のみを入力すればよいため、利便性の非常に高い認証システムを実現することができる。この利便性の高さを活かして、近年では ID レス認証の情報アクセス制御、ログイン管理、勤怠管理など様々な分野への適用が進んでいる¹⁾。

しかしながら、ID レス認証では登録ユーザ数 N の増加にともない、認証精度が劣化するという問題があり、これが ID レス認証を大規模ユーザシステムに適用するうえでの大きな課題となっている。この問題を解決するために、複数の生体情報 (指紋, 顔, 音声など) を融合してユーザを判定することで認証精度を高めるマルチモーダル認証技術が、ID レス認証において提案されている^{2)–6)}。しかしこの場合、ユーザに複数の生体情報を入力させることで、ID レス認証の本来の長所である利便性が低下してしまう。文献 7) も、ユーザ数の大規模な ID レス認証システムにおいて、今後はマルチモーダル認証技術の適用が進むようになる、と予想しており、その際に利便性の低下が問題になることを指摘している。したがって、必要な生体情報の入力回数を最小限にとどめたまま、認証精度を高めることが重要な課題となる。

従来より研究されているマルチモーダル認証技術のほとんどは、ユーザがすべての生体情報を入力してからユーザの判定を行う一括融合判定方式である^{2)–5)}。この場合、ユーザは必ずすべての生体情報を入力する必要があるため、利便性の低下が引き起こされる。これに対して、ユーザが生体情報を入力するたびに、それまで得られた生体情報を融合して判定を行う手法は逐次的融合判定方式と呼ばれる⁸⁾。この方式では、必要な生体情報の入力回数が少ないほど利便性の低下が抑えられることになる。文献 6) は音声を用いた ID レス認証における逐次的融合判定方式を提案しているが、これによって生体情報の入力回数が最小化される、という理論的な最適性までは示されていない。

本稿では、多重仮説においてデータの平均観測回数を最小化する逐次確率比検定 (MSPRT :

^{†1} 株式会社日立製作所システム開発研究所

Systems Development Laboratory, Hitachi, Ltd.

本稿の内容は 2008 年 10 月のコンピュータセキュリティシンポジウム 2008 にて報告され、同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である。

Multihypothesis Sequential Probability Ratio Test)⁹⁾を用いることで、ID レス認証において、生体情報の入力回数を最小限に抑えた逐次的融合判定方式を提案する。また、その際にスコアを観測データとして用い、さらに本人/他人同士のスコアがそれぞれ独立に同一の分布（以下、本人/他人分布）に従うと仮定することで、あらゆる種類の生体情報に適用可能な、汎用性の高いアルゴリズムを定式化する。その有効性を、顔と指紋のスコアセット NIST BSSR1 (Biometric Scores Set - Release 1) Set1¹⁰⁾を用いた評価実験を通して示す。

2. ID レス生体認証

2.1 生体認証の種類

生体認証は、検証 (verification)¹⁾と識別 (identification) の 2 種類に大別される^{11),12)}。検証とは、入力された生体情報と登録されている生体情報とのスコアを求め、それを基に両者が同一人物のものか否かを判定することである。DB に複数人の生体情報が登録されているとき、ユーザが ID と生体情報を入力し、システムがその ID に紐付いた生体情報とのスコアを求めることで、本人か否かを判定できる。このような生体認証を ID 付き生体認証（または ID 付き認証、1:1 認証）と呼ぶ。ID 付き認証は検証の一例である。

これに対して識別とは、入力された生体情報と DB に登録されている $N (> 1)$ 個の生体情報とのスコアを順次求め、それを基に入力された生体情報と類似する (0 あるいは 1 人以上の) 候補者のリストを求めることである。識別は、従来より犯罪捜査における指紋のスクリーニングなどにおいて用いられてきたが、ユーザが生体情報のみを入力し、それを基にシステムがユーザを一意に特定する ID レス認証も、識別の一例である。この場合、候補者数は 0 あるいは 1 人である^{*2}。

2.2 ID レス認証における精度の評価指標

検証では、システムが誤って本人を拒否する FRR (False Reject Rate) と、誤って他人を受け入れる FAR (False Accept Rate) の 2 つの誤り率が、精度の評価指標として定義されている。FRR の増加は利便性の低下を、FAR の増加は安全性の低下を引き起こす。

一方、識別では CMC (Cumulative Match Characteristic) カーブや、FNIR (False Neg-

ative Identification Rate)/FPIR (False Positive Identification Rate) が従来より定義されている¹¹⁾。CMC カーブは、入力された生体情報を持つ個人がスコア (以後、類似度とする) の高い上位 r 人までにランクインされる確率を r の関数として描いた曲線である。FNIR は DB に登録されている個人の生体情報が入力されたときに、候補者リストに該当者が含まれない誤り率、FPIR は DB に登録されていない個人の生体情報が入力されたときに、1 人以上の候補者リストが出力される誤り率である。たとえば、指紋のスクリーニングにおいては、FNIR および FPIR を低減させることが課題になると考えられる。

ところが ID レス認証では、情報アクセス制御、ログイン管理、勤怠管理など、システムがユーザを一意に特定し、そのユーザに応じたサービスを提供する適用先を想定する。このとき、登録を行ったユーザ (以下、登録ユーザ) が認証を試みたときの認証誤りには、誤って他の登録ユーザと判定する誤りと、誤って認証失敗とする誤りの 2 つに分類できる。両者とも、認証を試みたユーザは本来のサービスを利用できないので利便性の低下が引き起こされるが、前者においては他のユーザに応じたサービスが提供されてしまうので、さらに安全性の低下も引き起こされる。

本稿では上記を考慮したうえで、ID レス認証における精度の評価指標として以下の 3 つの誤り率を新たに定義する。

EFRR (Enrollee False Reject Rate : 登録者本人拒否率):

登録ユーザが認証を試みたときに、システムが認証失敗としてしまう誤り率。

EFAR (Enrollee False Accept Rate : 登録者他人受入率):

登録ユーザが認証を試みたときに、システムが他の登録ユーザとして認証成功としてしまう誤り率。

NFAR (Non-Enrollee False Accept Rate : 非登録者他人受入率):

非登録ユーザが認証を試みたときに、システムがある登録ユーザとして認証成功としてしまう誤り率。

ログイン管理を例にとると、EFRR は登録ユーザがログインに失敗する誤り率、EFAR は登録ユーザが他のユーザアカウントでログインしてしまう誤り率、NFAR は非登録ユーザ (すなわち、攻撃者) がログインに成功してしまう誤り率を意味する。EFRR の増加は利便性の低下を、EFAR の増加は利便性および安全性の低下を、NFAR の増加は安全性の低下を引き起こす。図 1 に ID 付き認証、ID レス認証のそれぞれにおける精度の評価指標

*1 狭義の認証として訳されることもある¹²⁾。

*2 入退室管理においては、ユーザが登録されているか否か (入退室が許可されている否か) のみを判定すればよい場合もある。この場合は、候補者を 1 人に絞り込む必要はない。ただし、入退室を行ったユーザが誰なのかを記録する場合や、勤怠管理を兼ねる場合などにおいては、候補者を 1 人に絞り込む必要がある。

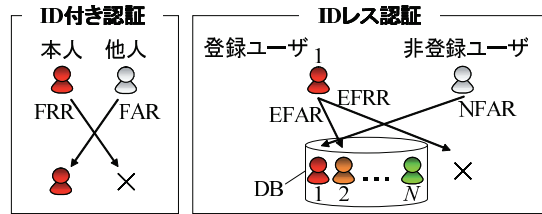


図 1 ID 付き/ID レス認証における精度の評価指標
Fig. 1 Performance metrics for biometric verification/identification systems.

を示す。

2.3 ID レス認証における精度の問題

ID レス認証では登録ユーザ数 N が増加するほど、誤識別の対象となるユーザが増加するため、認証精度は劣化するものと考えられる。たとえば、ID レス認証の判定方式として、認証閾値を上回るスコアが存在すれば、そのうち最大値を実現した登録ユーザを判定結果として出力し、そうでなければ認証失敗とする方式を考える。ここで、本人/他人同士のスコアが閾値を下回る/上回る確率は FRR/FAR に相当する。したがって、各登録ユーザに対して得られたスコアがそれぞれ独立であると仮定すると、 $N \times FAR \ll 1$ のとき、

$$\begin{aligned} EFRR &= FRR \times (1 - FAR)^{N-1} \\ &\approx FRR \times [1 - (N - 1) \times FAR] \\ &\approx FRR \end{aligned} \tag{1}$$

$$EFAR \approx (N - 1) \times \left[FRR \times FAR + \int_{s_{th}}^{\infty} f(s)(1 - G(s)) ds \right] \tag{2}$$

$$\begin{aligned} NFAR &= 1 - (1 - FAR)^N \\ &\approx N \times FAR \end{aligned} \tag{3}$$

と表せる(式(2)の導出は付録 A.1 を参照)。ただし、 $f()$ は本人分布、 $G()$ は他人分布 $g()$ の累積分布関数である。式(2)および式(3)より、 $EFAR$ および $NFAR$ は登録ユーザ数 N におおよそ比例して増加することが分かる。したがって、ID レス認証では登録ユーザ数 N の増加にともない、認証精度の問題が顕著となる。

3. ID レス認証におけるマルチモーダル認証技術の現状

3.1 マルチモーダル認証技術の種類

生体認証における精度を高めるための手段としては、複数の生体情報を融合して判定を行うマルチモーダル認証技術が従来より研究されている。マルチモーダル認証技術は、以下の5種類の方式に分類することができる⁷⁾。

- (1) 複数のセンサで取得した同一生体情報(複数のカメラで撮影した顔など)を融合する方式(Multiple sensors)
- (2) 複数種類の生体情報(顔, 指紋, 音声など)を融合する方式(Multiple biometrics)
- (3) 同一種類の部位が異なる生体情報(人差指, 中指, 薬指の指紋など)を融合する方式(Multiple units)
- (4) 複数回にわたって取得した同一生体情報を融合する方式(Multiple snapshots)
- (5) 同一生体情報に適用した複数の特徴量抽出, あるいは複数の照合アルゴリズムを融合する方式(Multiple matchers)¹⁾

(1), (4) および (5) の方式では同一の生体情報を用いて融合判定を行っているが、この場合、融合する対象同士の相関が非常に高いため、大きな精度向上は実現できないと考えられる。したがって、本稿では異なる生体情報を用いて融合判定を行う(2) および (3) の方式に焦点を絞って話を進める。これらは狭義のマルチモーダル認証技術でもある¹²⁾。

3.2 ID レス認証における一括融合判定方式

ID レス認証における認証精度を高めるため、上記のマルチモーダル認証技術(Multiple biometrics あるいは Multiple units)を適用した研究例はいくつか存在するが、そのほとんどはすべての生体情報が入力されてから判定を行う一括融合判定方式である。文献 3) では、ユーザから顔, 唇の動き, 音声の3つの生体情報を取得し、それぞれに対してID レス認証を行い、その結果が同一のものが2つ以上あれば、そのユーザを判定結果とする多数決方式を採用している。文献 4) では、ユーザに顔, 指紋を入力させ、顔で候補者を上位 n 人に絞り込んだうえで、顔と指紋のスコアを FAR 値に正規化し、それらの積を基準としてユーザの判定を行っている。文献 5) では、ユーザに複数の生体情報を入力させ、それを基に各クラスに属する事後確率を算出し、それを基準としてユーザの判定を行っている。

以上の研究例はいずれも、ユーザにすべての生体情報を入力させる必要があり、その場合

*1 この方式では用いる生体情報は1つのみであるが、文献 7) はこの方式もマルチモーダル認証技術に含めている。

における利便性の低下については考慮されていない。

3.3 ID レス認証における逐次的融合判定方式

一括融合判定方式に対して、生体情報が入力されるたびにユーザの判定を行う手法は逐次的融合判定方式と呼ばれる⁸⁾。文献 8) では、逐次確率比検定 (SPRT: Sequential Probability Ratio Test) に基づいた ID 付き認証における逐次的融合判定方式を提案し、その有効性を実験的に示している。SPRT は、観測データが i.i.d. (independent and identically distributed) であり、かつ十分多くの観測データが得られるときに、判定を終了するために必要な平均観測回数を最小化する検定手法である¹³⁾。これを適用することで、ID 付き認証における生体情報の入力回数を最小限にとどめる逐次的融合判定を実現できる。

ただし、SPRT はあくまでも帰無仮説 H_0 と対立仮説 H_1 のいずれかを判定する仮説検定 (すなわち、2 クラス判別) において、データの平均観測回数を最小化するアルゴリズムである。これに対して、ID レス認証は生体情報を入力したユーザがどの登録ユーザかを判定する (あるいは認証失敗とする) ものであり、多クラス判別に相当する。文献 6) は SPRT を多クラス判別に拡張し、それを用いた話者識別における逐次的融合判定方式を提案しているが、この手法がデータの平均観測回数を最小化する (すなわち、ID レス認証において生体情報の平均入力回数を最小化する)、という理論的な最適性は示されていない。

本稿は、多重仮説においてデータの平均観測回数を最小化する MSPRT を基に、ID レス認証において生体情報の入力回数を最小化する逐次的融合判定を実現することを目的とする。

4. MSPRT に基づく ID レス認証

本章では、多重仮説において平均観測回数を最小化する検定手法である MSPRT について述べ、ID レス認証においてこれに基づいた新しい逐次的融合判定方式を提案する。

4.1 MSPRT

SPRT は統計的仮説 H_0, H_1 に対し、観測データ s_t が得られるたびに、今までに得られた観測データの集合 $S_t = \{s_\tau | 1 \leq \tau \leq t\}$ を用いて、

$$Z_t = \frac{P(S_t|H_1)}{P(S_t|H_0)} \quad (4)$$

で表される尤度比を計算し、これがある閾値 A を上回れば H_1 を受理、別の閾値 B を下回れば H_0 を受理、どちらでもなければ観測を続ける手法である。文献 9) は、多重仮説 H_0, H_1, \dots, H_N に対しても、SPRT 同様に平均入力回数を最小化する検定が存在することを示し、そのような検定を MSPRT と呼んでいる。

以下、MSPRT について詳述する。仮説 H_i ($0 \leq i \leq N$) を受理したときに、それが誤りである確率 α_i は、

$$\alpha_i = \sum_{j \neq i} P(H_j) \alpha_{ji} \quad (5)$$

と表せる。ここで、 $P(H_j)$ は仮説 H_j が真である事前確率、 α_{ji} ($j \neq i$) は仮説 H_j が真であるときに仮説 H_i を誤って受理する確率である。各仮説に対する α_i ($0 \leq i \leq N$) が、それぞれ所定の値以下となるようなすべての検定を考える。そのような検定の中で、以下の検定 (MSPRT) を用いた場合に、判定終了までに必要なデータの平均観測回数が最小となることが証明されている⁹⁾。

MSPRT :

各仮説 H_i ($0 \leq i \leq N$) に対し、観測データ s_t が得られるたびに、今までに得られた観測データの集合 $S_t = \{s_\tau | 1 \leq \tau \leq t\}$ を用いて、

$$P(H_i|S_t) = \frac{P(H_i)Z_{ti}}{\sum_{n=0}^N P(H_n)Z_{tn}} \quad (6)$$

で表される事後確率を算出する。ただし、 Z_{ti} は、

$$Z_{ti} = \frac{P(S_t|H_i)}{P(S_t|H_0)} \quad (7)$$

で表される尤度比である。閾値 A を上回る事後確率があれば、そのうち最大値を実現した H_i を受理し、閾値 A を上回る事後確率がなければ観測を続ける。

SPRT や文献 6) では尤度比を判定基準としているが、上記の検定手法の特徴は、尤度比を事後確率に正規化後、事後確率を判定基準とする点にある。

4.2 スコアを観測データとした MSPRT の ID レス認証への適用

MSPRT を適用することで、ID レス認証において平均入力回数を最小化する逐次的融合判定方式を提案する。この際、観測データとして何を用いるか、に注意が必要である。文献 6) では、入力された生体情報から抽出した特徴量を観測データとし、あらかじめ学習しておいた各登録ユーザおよび全登録ユーザ共通の特徴量分布を用いて尤度比を算出している。しかしながら、たとえば虹彩認証では特徴量 (アイリスコード) の次元数は数千次元と非常に高く、またマニキュア方式を用いた指紋認証では、指紋を取得するたびに特徴量の次元数 (マニキュアの数) が変化する恐れがある²⁾。このような場合、特徴量分布の学習

は非常に困難である．したがって，文献 6) の手法は限られた種類の生体情報にしか適用できず，汎用性が低いという問題がある．

本稿ではこのことを考慮して，全登録ユーザに対して求めたスコアを観測データとして用いる手法を提案する．認証を試みるユーザ（以下，認証ユーザ）が t 回目の生体情報の入力を行ったとき， i 番目の登録ユーザに対して得られたスコアを s_{ti} とし，

$$s_t = (s_{t1}, s_{t2}, \dots, s_{tN}) \tag{8}$$

とおく．すなわち，各入力において得られる N 個のスコアで構成されるベクトルを観測データとする．このとき， t 回目の入力までに得られた観測データ（スコアベクトル）の集合は，

$$S_t = \{s_\tau | 1 \leq \tau \leq t\} \tag{9}$$

と表せる．式 (6) において S_t に S_t をあてはめ，

仮説 H_i : 「認証ユーザが i 番目の登録ユーザである」 ($1 \leq i \leq N$)

仮説 H_0 : 「認証ユーザが非登録ユーザである」

とすることで，MSPRT を ID レス認証における逐次的融合判定に適用することが可能となる．このとき尤度比 Z_{ti} の導出方法が問題となるが，Multiple biometrics や Multiple units では，各入力における生体情報の種類，あるいは部位が異なるため，各入力において得られたスコアベクトル s_τ ($1 \leq \tau \leq t$) は，互いに独立であると考えられる．したがって，尤度比 Z_{ti} は，

$$Z_{ti} = \frac{P(S_t|H_i)}{P(S_t|H_0)} = \frac{\prod_{\tau=1}^t P(s_\tau|H_i)}{\prod_{\tau=1}^t P(s_\tau|H_0)} \tag{10}$$

と分解できる．これは，各仮説 H_i が真であるときにスコアベクトル $s_\tau = (s_{\tau 1}, s_{\tau 2}, \dots, s_{\tau N})$ が得られる確率密度分布 $P(s_\tau|H_i)$ ($0 \leq i \leq N$) をあらかじめ学習しておけば，求めることができる．

提案方式では以下のようにしてユーザの判定を行う．生体情報が入力されるたびに，それまでに得られたスコアベクトル s_τ ($1 \leq \tau \leq t$) を用いて尤度比 Z_{ti} を算出し，この尤度比を認証ユーザが各登録ユーザである，あるいは非登録ユーザであるという事後確率 $P(H_i|S_t)$ に正規化する．そして，認証閾値 A を上回る事後確率 $P(H_i|S_t)$ があれば，そのうち最大値を実現した仮説を受理し，受理した仮説に対応する登録ユーザ ID（仮説 H_0 であれば，認証失敗）を判定結果として出力する．認証閾値 A を上回る事後確率がなければ次の生体情報を入力させる．ただし，入力できる生体情報の種類・部位には限りがあるため，生体情報の入力回数が上限値 T に到達した場合は，認証閾値 λ と比較し，これを上回る事後確率

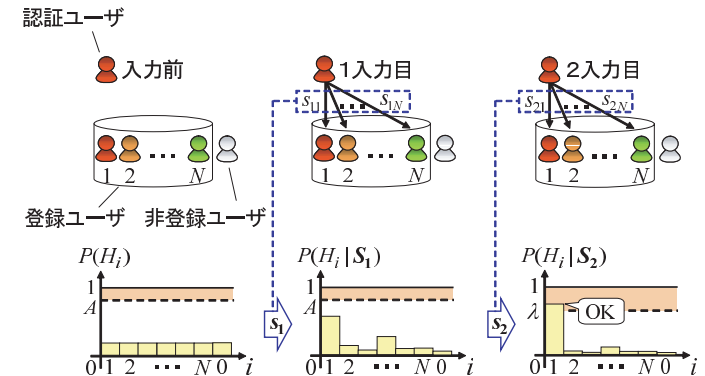


図 2 スコアを観測データとした MSPRT に基づく逐次的融合判定アルゴリズム

Fig. 2 The sequential decision fusion algorithm based on MSPRT using scores as observed data.

がなければ認証失敗とする．

ここで λ を動かすと， T 回目の入力における判定結果（認証成功/認証失敗）が変化する．しかしながら， $T - 1$ 回目までに判定が終了する場合は，その判定結果は何も変わらず， T 回目に判定が終了する場合も入力回数は T のまま変わらない．したがって， λ を動かしても生体情報の入力回数は変化しない．これを利用して， A を動かして平均入力回数を所定の値に変化させた後， λ を動かすことで，その値を固定したまま EFRR と EFAR/NFAR のトレードオフを制御することができる．MSPRT に基づいて逐次的融合判定を行う様子を図 2 に示す（ただし， $T = 2$ の場合）． $P(H_i)$ はスコアベクトル s_1 が得られる前段階（すなわち，生体情報の入力前）において，仮説 H_i が真である事前確率である．これはシステム側であらかじめ設定しておく．

4.3 スコアの独立同一性を仮定した分布の学習

前節では，確率密度分布 $P(s_\tau|H_i)$ ($0 \leq i \leq N$) を用いて尤度比が算出できることを説明した．しかしながら，この確率密度分布は N 次元分布であり，かつ計 $N + 1$ 個存在するため，登録ユーザ数 N が大きいときは分布学習のために大量のデータが必要となり，分布学習が困難になってしまう．また，ユーザの追加登録を行うと登録ユーザ数 N が変化してしまうため，そのつど，分布学習をし直す必要が生じるという問題もある．

そこで，本稿ではスコアの独立同一性を仮定することにより，分布の学習を容易にする手法を提案する．具体的には，すべてのスコアが独立であると仮定し（独立性の仮定），本人

同士のスコアはすべて本人分布 $f()$ 、他人同士のスコアはすべて他人分布 $g()$ にそれぞれ従うものとする（同一性の仮定）。本人/他人同士のスコアは厳密にはユーザに依存する*1のため、上記の仮定は実際には成立しない恐れがある。しかしながら、このときスコアベクトル s_τ の各要素はすべて独立であり、確率密度 $P(s_{\tau i}|H_j)$ は、

$$P(s_{\tau i}|H_j) = \begin{cases} f(s_{\tau i}) & (\text{if } i = j) \\ g(s_{\tau i}) & (\text{if } i \neq j) \end{cases} \quad (11)$$

と表すことができるので、式 (10) の尤度比 Z_{ti} は、

$$\begin{aligned} Z_{ti} &= \frac{\prod_{\tau=1}^t \prod_{n=1}^N P(s_{\tau n}|H_i)}{\prod_{\tau=1}^t \prod_{n=1}^N P(s_{\tau n}|H_0)} \\ &= \frac{\prod_{\tau=1}^t P(s_{\tau i}|H_i) \prod_{n \neq i} P(s_{\tau n}|H_i)}{\prod_{\tau=1}^t P(s_{\tau i}|H_0) \prod_{n \neq i} P(s_{\tau n}|H_0)} \\ &= \begin{cases} \prod_{\tau=1}^t f(s_{\tau i})/g(s_{\tau i}) & (\text{if } i \neq 0) \\ 1 & (\text{if } i = 0) \end{cases} \quad (12) \end{aligned}$$

と変形でき、本人分布 $f()$ および他人分布 $g()$ を学習しておけば、求めることができるようになる。本稿で提案する分布学習の枠組みを図 3 に示す。この場合、学習すべき分布の数はつねに本人分布 $f()$ および他人分布 $g()$ の 2 つであり、またこれらの分布は生体情報の種類や、登録ユーザ数 N に依存せずつねに 1 次元分布である。したがって、どのような場合においても分布の学習が容易であり、その結果、汎用性の高い逐次的融合判定を実現することができる。

本人分布 $f()$ および他人分布 $g()$ は、あらかじめ収集しておいた生体情報から本人/他人同士のスコア（以下、本人/他人スコア）を求め、それらを訓練データとして学習しておく。たとえば、分布のモデルとして正規分布などを仮定し、そのパラメータを最尤推定などによって求める方法が考えられる。あるいは、式 (12) より尤度比 Z_{ti} は、本人分布と他人分布の比 $f()/g()$ の積で表されるので、 $f()/g()$ をロジスティック回帰^{8),14)} を用いて学習してもよい。ロジスティック回帰では、 $\log f(s_{\tau i})/g(s_{\tau i})$ がスコア $s_{\tau i}$ に関する一次関数 $as_{\tau i} + b$

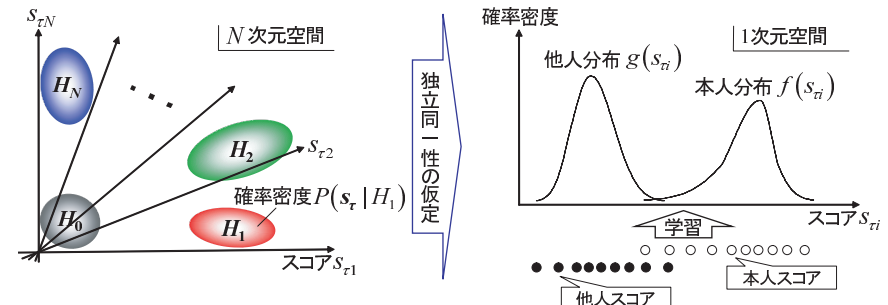


図 3 スコアの独立同一性を仮定したスコア分布の学習
Fig. 3 Training of score distributions supposing independency and identity of scores.

で表されるものと仮定し、そのパラメータ a と b を推定する。

本人分布 $f()$ や他人分布 $g()$ は、生体情報の種類や照合アルゴリズムによってその形状が異なる。したがって、これらを学習する場合は虹彩認証においては二項分布¹⁵⁾、静脈認証においてはベータ二項分布¹⁶⁾ というように、個々の事例ごとにどの分布モデルを用いるのが適切かを検討する必要がある。ただし、事例によっては分布の形状が複雑で、本人分布 $f()$ および他人分布 $g()$ を適切にモデル化すること自体が困難な場合もある。これに対して、ロジスティック回帰を用いて本人分布と他人分布の比 $f()/g()$ を推定する手法では、本人分布 $f()$ や他人分布 $g()$ に対する制約が緩いため、上記のような場合においても適切にモデル化できる可能性がある。たとえば文献 8), 14) が、ID 付き認証でのマルチモーダル認証技術においてロジスティック回帰を用いることの有効性を示している。

5. 提案方式の評価

5.1 評価実験の概要

提案方式の認証精度、および生体情報の入力回数に関する性能を調べるために評価実験を行った。ここでは比較のため、提案方式の他に逐次的融合判定方式として OR 判定方式¹⁷⁾、および文献 6) と同様に尤度比を判定基準とする方式（以下、尤度比判定方式）を用いた場合の評価も行った。OR 判定方式は、生体情報が入力されるたびに、各登録ユーザに対して新たに得られるスコア（FAR 値に正規化したもの）を閾値と比較し、閾値よりも小さいものがあれば、そのうち最小値を実現した登録ユーザを判定結果として出力し、そうでなければ次の生体情報を入力させる方式である（過去の入力において得られたスコアは、今回の判

*1 これは、指紋認証において指が乾燥している人は認証されにくい、顔認証において双子同士では誤認証が起きやすい、といった例を考えれば納得できる。

定に用いない). 尤度比判定方式は, 入力たびにそれまで得られたすべてのスコアを用いて, 式 (12) により各登録ユーザに対する尤度比 Z_{ti} ($1 \leq i \leq N$) を算出し, 閾値よりも大きいものがあれば, そのうち最大値を実現した登録ユーザを判定結果として出力し, そうでなければ次の生体情報を入力させる方式である. OR 判定方式では, t 回目の判定において過去のスコアを考慮せず, t 回目に得られたスコアのみを用いて判定を行うが, 尤度比判定方式と提案方式では, 過去のスコアと t 回目に得られたスコアをすべて考慮して判定を行う.

本実験で用いたデータは, NIST BSSR1 (Biometric Scores Set - Release 1) Set1¹⁰⁾ である. これは, 517 人の被験者からそれぞれ顔, 左手の指紋, 右手の指紋の 3 種類の生体情報 (登録用, 認証用に 1 つずつ) を収集し, その各々の生体情報を総当りに照合することで得られたスコアのセット (各生体情報につき, スコアの数は 517×517 個) である. ただし, 顔に関しては照合アルゴリズム C および G を用いて求めた 2 つのスコアセットが用意されており, このうち前者を使用した. この際, アルゴリズム C では 0 から 1 までの類似度がスコアとして用いられているが, 全被験者に対するスコアが不適切な (値が -1 となる) 被験者が 1 人存在していたので, その被験者は評価実験から除外した.

516 人の被験者のうち, 116 人の生体情報を総当りに照合して得られるスコア (各生体情報につき, 本人スコアは 116 個, 他人スコアは 116×115 個) を本人/他人分布, あるいはその比の学習に用いた. 学習は, 本人/他人分布として正規分布を仮定し, その分布パラメータを最尤推定によって求める場合 (以下, 正規分布モデル) と, 本人/他人分布の比をロジスティック回帰によって求める場合 (以下, ロジスティックモデル) の 2 通りを試みた.

残りの 400 人の被験者のうち, 200 人を登録ユーザ, 残りの 200 人を非登録ユーザとし, 各登録ユーザおよび非登録ユーザが 3 つの生体情報を逐次に入力する実験を行った. このときの生体情報の入力順序は $6 (= 3!)$ 通りあるが, そのすべてを試みた. また, 516 人の被験者を学習用の被験者, 登録ユーザ, および非登録ユーザに分ける方法として 100 通りの方法をランダムに選び, それぞれの場合において上記の実験を行った. 本実験において, 登録ユーザによる認証試行数, および非登録ユーザによる認証試行数はともに計 120,000 ($= 200 \times 6 \times 100$) 回である. この際, EFRR が 2% に固定されるように認証閾値 A および λ を制御し, そのときの EFAR/NFAR と平均入力回数の関係を評価した. なお, 提案方式における事前確率は $P(H_i) = 1/(N + 1)$ ($0 \leq i \leq N$) とした.

5.2 評価結果

評価結果を図 4 に示す. 「OR」は OR 判定方式, 「尤度比」は尤度比判定方式, 「MSPRT」は MSPRT に基づく逐次的融合判定方式 (提案方式) である. また, 括弧内の 「Gaussian」

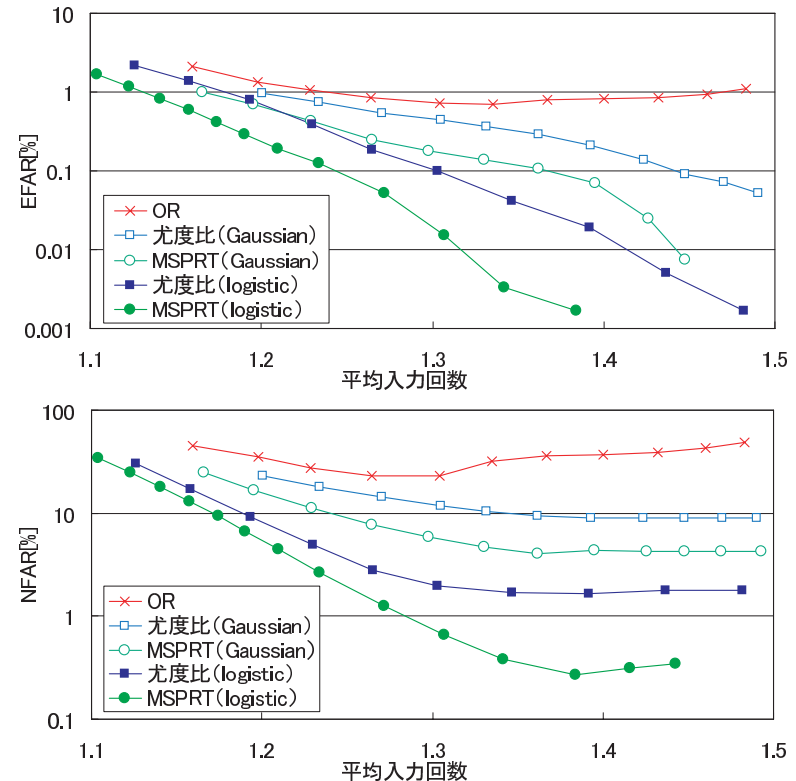


図 4 EFAR/NFAR と平均入力回数との関係
Fig. 4 Relationship between EFAR/NFAR and the average number of inputs.

は学習モデルとして正規分布モデルを用いた場合の結果, 「logistic」はロジスティックモデルを用いた場合の結果である. ただし, 「MSPRT(Gaussian)」では平均入力回数が 1.45 回以上のとき, 「MSPRT(logistic)」では 1.40 回以上のとき, 登録ユーザが他の登録ユーザと判定されることはなかった (すなわち, $EFAR = 0\%$).

図 4 から, EFAR/NFAR および平均入力回数の両面において, 提案方式が OR 判定方式や尤度比判定方式よりも優れていることが分かる. これは, 多重仮説においてデータの平均観測回数を最小化する MSPRT を用いたことによる効果であると考えられる. 提案方式では, 生体情報の入力回数に上限値 T (本実験では $T = 3$) を設けており, また分布学習を容易に

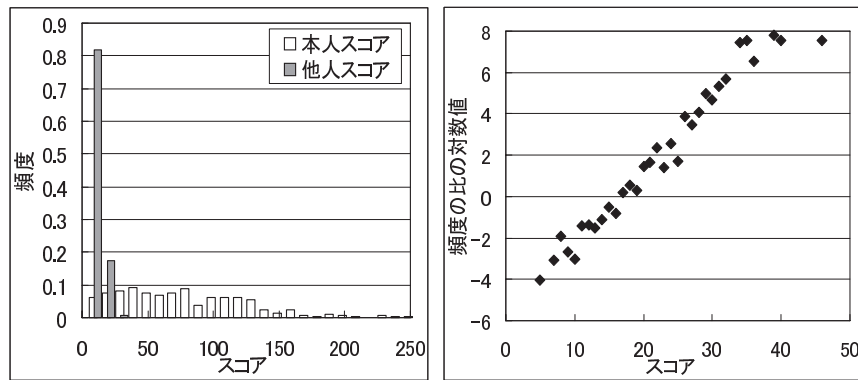


図 5 左手の指紋の本人/他人スコアの頻度分布とその比の対数値

Fig. 5 The frequency distribution of the genuine / imposter scores of the left hand fingerprints and the logarithm of their ratio.

するためにスコアの独立同一性を仮定している。しかしながら MSPRT では、いずれかの事後確率が閾値 A を上回るまでデータの観測を続けることを前提としており、またスコアの独立同一性の仮定も、前述したように厳密には成立しない恐れがある。それにもかかわらず提案方式は優れた性能を実現しており、入力回数の上限值 T の導入や、スコアの独立同一性の仮定が適切であることが実験的に示されたと考えている。

また、提案方式と尤度比判定方式では、ロジスティックモデルを用いた場合の方が、正規分布モデルを用いた場合よりも良い性能を実現している。この理由を説明するために、左手の指紋における本人スコア (516 個) と他人スコア (516 × 515 個) の頻度、およびその比の対数値のスコアに対する特性を図 5 に示す。頻度分布は複雑な形状をしているのに対して、その比の対数値はおおよそ直線的な特性が得られている。このような傾向は、顔、右手の指紋においても見られた。ロジスティック回帰を用いて学習を行う場合、スコア分布が複雑な形状をしていても適切にモデル化が行える可能性があることを前述したが、これが本実験においても表れたものとする。

なお、ユーザに 1 本目の指のみを入力させた場合 (すなわち、平均入力回数が 1 回するとき) の性能を調べてみたところ、 $EFAR = 7.3\%$ 、 $NFAR = 86\%$ であった。これに対して、たとえば、平均入力回数 < 1.35 回という要求値を設けたとき、OR 判定方式では $EFAR = 0.70\%$ 、 $NFAR = 32\%$ 、尤度比判定方式 (ロジスティックモデル) では

$EFAR = 0.042\%$ 、 $NFAR = 1.7\%$ であるのに対して、提案方式 (ロジスティックモデル) では $EFAR = 0.0033\%$ 、 $NFAR = 0.39\%$ という性能が得られている。以上より、提案方式の有効性が示された。

6. ま と め

本稿では MSPRT に基づき、ID レス認証において生体情報の平均入力回数を最小限にとどめつつ、認証精度を高める逐次的融合判定方式を提案した。その際、スコアを観測データとして使い、さらにスコアの独立同一性を仮定することで、生体情報の種類によらず容易に分布 (本人/他人分布) の学習が可能で、汎用性の高いアルゴリズムを定式化した。NIST BSSR1 (Biometric Scores Set - Release 1) Set1 を用いた評価実験を行い、平均入力回数および認証精度の両面において、提案方式は OR 判定方式や尤度比判定方式よりも優れた性能を持っていることを示した。

IC カードなどの持ち物の提示や、ユーザ ID/パスワードなどの文字列の入力が不要な ID レス認証は、あらゆる認証手段の中で最も利便性の高いものといえる。ログイン管理や入退室管理などの様々なアプリケーションに対して、このような認証手段の適用を今後さらに進めていくためには、いかに利便性と安全性を保ったまま、登録ユーザ数を拡大するかが課題になる。本稿では、このような問題に対する 1 つの最適解を提示したものと考えている。

参 考 文 献

- 1) 独立行政法人情報処理推進機構: バイオメトリクス製品データベース | IPA 情報処理推進機構 (オンライン). 入手先 <https://isec.ipa.go.jp/biodb/index.html>
- 2) Jain, A., Bolle, R. and Pankanti, S.: *BIOMETRICS Personal Identification in Networked Society*, Kluwer Academic Publishers (1999).
- 3) Frischholz, R.W. and Dieckmann, U.: BioID: A Multimodal Biometric Identification System, *IEEE Computer*, Vol.33, No.2, pp.64-68 (2000).
- 4) Hong, L. and Jain, A.: Integrating Faces and Fingerprints for Personal Identification, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.20, No.12, pp.1295-1307 (1998).
- 5) Kittler, J., Li, Y.P., Matas, J. and Sanchez, M.U.: Combining Evidence in Multimodal Personal Identity Recognition Systems, *Proc. AVBPA*, pp.327-344 (1997).
- 6) 野田秀樹, 浜崎 武, 河口英二: 逐次確率比検定を用いた適応的活者識別, 電子情報通信学会論文誌, Vol.J84-D-II, No.1, pp.211-213 (2001).
- 7) Jain, A.K., Ross, A. and Prabhakar, S.: An Introduction to Biometric Recognition, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.14, No.1, pp.4-20

(2004).

- 8) 高橋健太, 三村昌弘, 磯部義明, 宇都宮洋, 瀬戸洋一: 逐次確率比検定とロジスティック回帰を用いたマルチモーダル生体認証, 電子情報通信学会論文誌, Vol.J89-D, No.5, pp.1061-1065 (2006).
- 9) Dragalin, V.P., Tartakovsky, A.G. and Veeravalli, V.V.: MULTIHYPOTHESIS SEQUENTIAL PROBABILITY RATIO TESTS, PART I: ASYMPTOTIC OPTIMALITY, *IEEE Trans. Information Theory*, Vol.45, Issue 7, pp.2448-2461 (1999).
- 10) National Institute of Standards and Technology: NIST Biometric Scores Set (online). available from <http://www.itl.nist.gov/iad/894.03/biometricscores/~index.html>
- 11) ISO/IEC19795-1, Information Technology — Biometric Performance Testing and Reporting — Part 1: Principles and Framework (2006).
- 12) 瀬戸洋一: サイバーセキュリティにおける生体認証技術, 共立出版 (2002).
- 13) Wald, A.: *Sequential Analysis*, John Wiley & Sons, New York (1947).
- 14) Verlinde, P. and Acheroy, M.: A Contribution to Multi-Modal Identity Verification Using Decision Fusion, *Proc. PROMOPTICA* (2000).
- 15) Daugman, J. and Downing, C.: Epigenetic randomness, complexity and singularity of human iris patterns, *Proc. Royal Soc.: Biological Sciences*, Vol.268, pp.1737-1740 (2001).
- 16) Yanagawa, T. and Aoki, S. and Ohyama, T.: Human finger vein images are diverse and its patterns are useful for personal identification, MHF2007-12, MHF preprint series, Kyushu University 21st Century COE Program, Development of Dynamic Mathematics with High Functionality (2007).
- 17) Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K. and Senior, A.W.: *Guide to Biometrics*, Springer (2003).

付 録

A.1 式 (2) の導出

EFAR は登録ユーザが認証を試みたとき, 最も大きいスコアが他人スコアであり, かつそれが閾値を上回る確率値である. これを, 本人スコアが閾値を下回る場合と上回る場合に分けて考える. このとき, EFAR は前者において閾値を上回る他人スコアが存在する確率値, 後者において本人スコアを上回る他人スコアが存在する確率値の和に分解することができる. ここで FRR および FAR は, 本人分布 $f()$, 他人分布 $g()$ の累積分布関数 $G()$, および認証閾値 s_{th} を用いて,

$$FRR = \int_{-\infty}^{s_{th}} f(s) ds \quad (13)$$

$$FAR = \int_{s_{th}}^{\infty} g(s) ds = 1 - G(s_{th}) \quad (14)$$

と表せるので, スコアがすべて独立であり, $N \times FAR \ll 1$ のとき,

$$\begin{aligned} EFAR &= \int_{-\infty}^{s_{th}} f(s) \{1 - [G(s_{th})]^{N-1}\} ds + \int_{s_{th}}^{\infty} f(s) \{1 - [G(s)]^{N-1}\} ds \\ &= \int_{-\infty}^{s_{th}} f(s) ds \times \{1 - [1 - (1 - G(s_{th}))]^{N-1}\} \\ &\quad + \int_{s_{th}}^{\infty} f(s) \{1 - [1 - (1 - G(s))]^{N-1}\} ds \\ &\approx \int_{-\infty}^{s_{th}} f(s) ds \times \{1 - [1 - (N-1) \times (1 - G(s_{th}))]\} \\ &\quad + \int_{s_{th}}^{\infty} f(s) \{1 - [1 - (N-1) \times (1 - G(s))]\} ds \\ &= (N-1) \times \left[FRR \times FAR + \int_{s_{th}}^{\infty} f(s) (1 - G(s)) ds \right] \quad (15) \end{aligned}$$

と求めることができる.

(平成 21 年 4 月 9 日受付)

(平成 21 年 9 月 11 日採録)

推 薦 文

マルチモーダル認証の新しい手法を提案している. 本提案の認証手法における精度評価の指標を定義する際 ID レス認証特有の条件を考慮したうえで定義を行っており, この部分に新規性があると考えられる. 論文の採録にあたっては提案で示したモデルの厳密性を踏み込んで検討することが必要であるが, 全体を通して理論から検証の展開が論理的であり正確である. よって本提案を推薦したい.

(コンピュータセキュリティシンポジウム 2008 プログラム委員長 吉浦 裕)



村上 隆夫 (正会員)

平成 16 年東京大学工学部電子情報工学科卒業．平成 18 年同大学院修士課程修了．同年 (株) 日立製作所入社．以来，同システム開発研究所にて生体認証技術の研究開発に従事．平成 20 年 CSS2008 優秀論文賞受賞．



高橋 健太 (正会員)

平成 10 年東京大学理学部情報科学科卒業．平成 12 年同大学院修士課程修了．同年 (株) 日立製作所入社．以来，同システム開発研究所にて生体認証技術の研究開発に従事．平成 13 年情報処理学会高度交通システム研究会優秀論文賞受賞．平成 20 年度情報処理学会論文賞受賞．