手指形状認識による 画像認証手法のイントラネットへの応用

中村孔明† 髙橋雅隆† 納富一宏† 斎藤恵一††

本研究では，手指形状より得た特徴点情報を利用し，トーラス型自己組織化マップを用いた個人認証手法について述べる．各利用者の手指形状の特徴点間距離を属性ベクトルとして自己組織化マップを作成する．前実験では，被験者から抽出した特徴点に対して主成分分析を行い，その結果から特徴点の削減を行った．その後，平均の区間推定を行った結果，99%信頼区間で誤認識率は約 4.4%であった．以上の結果を踏まえ，本稿ではサンプル数を増やし，より一般化された特徴点の決定と，サンプルの分析を行う．また，会社や学校などで利用されるイントラネットへの本手法の応用例について検討する．

Application of image authentication method for intranet by hand shape recognition

YOSHIAKI NAKAMURA† MASATAKA TAKAHASHI†
KAZUHIRO NOTOMI† KEIITI SAITO††

In this article, we propose a personal authentication method by using characteristic information obtained from the hand shape, and using the torus type Self-Organizing Maps (SOM). The self-organizing maps are trained and generated with attribute vectors, which are characteristics from each user's hand shape. In the pre-experiment, we extracted a part of dimensions of characteristics by Principal Component Analysis (PCA). As the result, the error recognition rate was about 4.4% in the 99% confidence interval by interval estimation of the average. Based on the above result, it will be necessary to increase sample data, to determine more general feature points. In addition, we discuss to apply our authentication method for intranet used by companies and schools.

† 神奈川工科大学大学院工学研究科情報工学専攻
Dept. of Information and Computer Sciences, Kanagawa Institute of Technology
†国際医療福祉大学情報教育センター†
Education Center of Medical Informatics,International University of Health and Welfare

1. はじめに

従来のパスワード認証は，数桁の数字や記号を用いて認証を行うのが一般的であるが，偽造，盗難が容易であり，漏洩などの安全性に疑問が残る．対策として，インターネット上ではリモートアクセスなら鍵認証，ブラウザアクセスなら証明書での認証などがある．同様に，現実でも物理的な所持物による認証方法が存在する．しかし、所持物による認証方法は、その所持物を本人が持っていることが前提であるため，紛失時の本人拒否，盗難時の他人受容などが問題となる．これらの解決策として近年実用化され，銀行や ATM などでの個人認証や，入退室管理などに利用されているのがバイオメトリクス認証である [1]．バイオメトリクス認証において重要なのは，利用者への負担の軽減と利便性の向上である．利用者への負担には心理的負担と，身体的負担の二つがある．心理的負担とは指紋や虹彩など身体の情報を読み取られることへの抵抗感であり，身体的負担とは普段行わないような動作を強いられることへの抵抗感である．

そこで，利用者への負担の少ない認証方法として，キーボード上に置かれた手指形状により個人を特定する方法を提案する．固定したキーボードの真上からカメラで手指形状を撮影し，特徴点を抽出することで個人の特定を可能とする．提案手法は Web カメラがあれば認証が可能であるため，導入費用が数千円程度であり，低コストで導入できるという利点がある．キーボードに手を置くという日常的な動作のため，心理的負担，および身体的負担が共に少ないと考えられる．

2. 自己組織化マップ

2.1 自己組織化マップ

自己組織化マップ（SOM : Self-Organizing Maps）とは，1982 年に Kohonen が提案したトポロジカルマッピングを拡張した教師なし競合学習型のニューラルネットワークモデルの一つであり，出力層と入力層の 2 層から成る [2]．ニューラルネットワークモデルとは脳の中の神経細胞の情報処理の仕組みをコンピュータ内で実現しようとしたものである．SOM は n 次元属性ベクトルにより表現された入力データを，属性の類似度に従って二次元平面上にマッピングする能力を持ち，属性ベクトルの持つ各属性の値によってマップに着色することも可能である．

2.2 トーラス型自己組織化マップ

トーラス型自己組織化マップ(Torus SOM)[2]とはマップの上下左右のノードが相互に結合された SOM である．2.1 節で説明した通常の SOM には，勝者ノードがマップの端に配置されている場合，学習範囲が限られてしまう問題がある．本来学習すべき範囲にノードが存在しないことで学習量が減少するため，勝者ノードの位置によって学習量に差が生じてしまう．Torus SOM を使うことでこの問題は解決可能である．

2.3 本研究における自己組織化マップの役割

本研究では，手指形状より得た特徴点情報を利用し，トーラス型自己組織化マップを用いて個人の認証を行う．各利用者の手指形状の特徴点間距離を属性ベクトルとして自己組織化マップを作成する．あらかじめ学習された本人ノードが配置されている自己組織化マップに，認証用画像から計測した特徴点間距離を属性ベクトルとして投入する.学習済みノードと投入された認証用ノードのユークリッド距離の平均を求め，認証を行う．投入する認証用ノードとは，学習済みのマップに新たな入力ノードを加えることで正しく分類がなされているかを確認するためのものである．

このとき閾値(Threshold)を設定し，学習済みノードと投入されたノードのユークリッド距離の平均が閾値より低い値なら本人，高いなら他人と判断する．自己組織化マップに登録する被験者数と入力される次元数が多く，学習回数が少ないと完全にノードの位置が定まらないまま終了してしまうため，本実験で作成したマップは，すべて総ユニット数 4,900(70×70)，学習回数 50,000 回とする．

3. キーボード上に置かれた手指形状認識による画像認証手法の提案

本研究ではキーボード上のホームポジションに置かれた手指形状を Web カメラで撮影し，その画像から個人を特定する認証手法を提案する．Web カメラは固定されているため，利用者がキーボードに手を置く位置や手の角度が変わると計測する距離も変化する．そのため，手を置く場所をホームポジションに指定している．本研究で使用した Web カメラは最大 800 万画素の静止画を撮影することができる．個人を特定するために必要となる特徴点として 20 個所の手指形状距離を測定した [3]．測定した特徴点データを属性ベクトルとして SOM に投入し，学習を行った．表 3.1 に測定個所を示す．測定単位はピクセルを用いた．

表 3.1　SOM 作成に用いる特徴点間距離

番号	測定個所
1	両手の第 1 指指先点の間隔
2	両手の第 2 指指先点の間隔
3	右手尺側中手点から右手橈側中手点の間隔
4	左手尺側中手点から左手橈側中手点の間隔
5	右手第 1 指先端から右手第 2 指の間隔
6	左手第 1 指先端から左手第 2 指の間隔
7	右手第 2 指基節骨の長さ
8	左手第 2 指基節骨の長さ
9	右手第 3 指基節骨の長さ
10	左手第 3 指基節骨の長さ
11	右手第 4 指基節骨の長さ
12	左手第 4 指基節骨の長さ
13	右手第 5 指基節骨の長さ
14	左手第 5 指基節骨の長さ
15	右手第 2 指中手指節関節から第 3 指中手指節関節の間隔
16	左手第 2 指中手指節関節から第 3 指中手指節関節の間隔
17	右手第 2 指近位指節間関節から第 3 指近位指節間関節の間隔
18	左手第 2 指近位指節間関節から第 3 指近位指節間関節の間隔
19	両手の第 1 指中手指節関節の間隔
20	両手の第 1 指近位指節間関節の間隔

4. 実験

4.1 実験条件

手指形状の特徴点間距離を用いた個人認証実験の評価を行う．本学の学生 30 名(男性 15 名，女性 15 名)を被験者として，認証精度の検証実験を行った．被験者には実験前に予め実験方法の説明を行った．

被験者 30 名に対して，ホームポジションに手を置いた状態でキーボードの真上 40cm から Web カメラで手指形状の撮影を行った．手指形状の撮影は 1 人 5 回行ったが，1 枚撮影する毎にキーボードから手を離してもらい，再度撮影を行った．特徴点間距離の計測は，画像中の距離、面積を計算できるフリーソフトウェアである画像ビューアソフト [4]を用いて手作業で行った．実験機器の配置図を図 4.1 に示す．

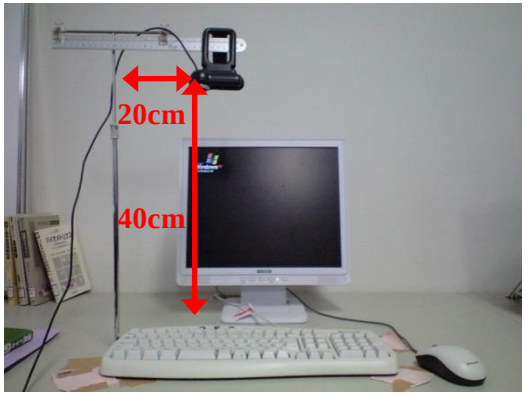

図 4.1　実験機器の配置図

4.2 主成分分析

各被験者から得られた5枚の手指形状画像から､20個所の特徴点間距離を計測した．計測データを多変量統計法の1つである主成分分析によって評価した[5]．主成分分析の目的は，より少ない成分でデータの情報を反映することである．各データは標準化し，相関行列による分析を行った．各主成分軸に対する累積寄与率を表4.1に示す．第1主成分と第2主成分の主成分得点に基づいて計測データをプロットしたグラフを図4.2に示す．第1主成分と第2主成分の主成分負荷量に基づいて各成分をプロットしたグラフを図4.3に示す．

図4.2では，第2主成分得点までで2つのグループに分類されているが，多くは第1主成分によって分類されている．図4.3から，最も寄与率の大きい主成分は各基節骨の長さ，尺側中手点から右手橈側中手点の間隔といった身体的特徴の指標であるということが読み取れる．第2位の主成分は，第2指と第3指の開き具合や親指の置き方といった，行動的特徴の指標ということが読み取れる．このことから図4.2で分類された2つのグループは男女の手の大きさの違いによって分類された結果と言える．

表4.1　上位8主成分の累積寄与率

主成分	1	2	3	4	5	6	7	8
累積寄与率	37.123	56.473	70.786	76.209	80.877	84.75	87.333	89.639

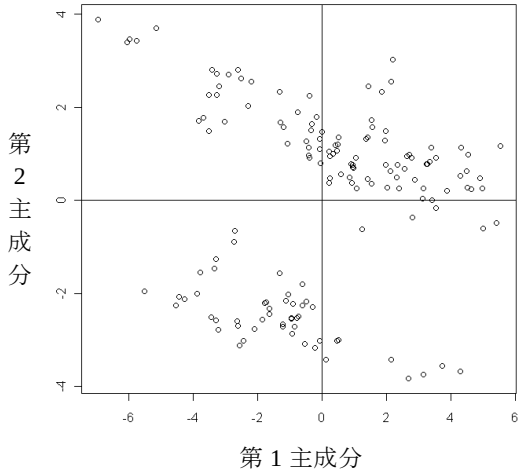

図4.2　第1主成分得点，第2主成分得点に基づく計測データの配置

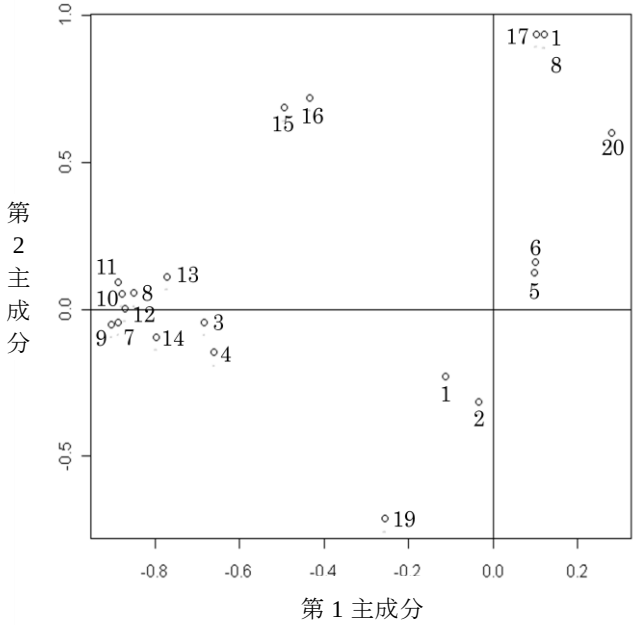

図4.3　第1主成分，第2主成分の主成分負荷量に基づく成分の配置

4.3 評価方法

他人受容率（FAR：False Accept Rate）と本人拒否率（FRR：False Reject Rate）を用いて評価を行った．FARとは本人ではないのにもかかわらず本人と判断してしまう失敗率のことであり，FRRとは本人を本人と判断できない失敗率のことである．FAR曲線とFRR曲線の交点をEER(Equal Error Rate)と呼ぶ．EERは誤り率であり，認証成功率は1 – EERとなる．FAR，FRRの定義式を以下に示す．

$$FAR = \frac{\text{他人受容回数}}{\text{試行回数}}, \quad FRR\frac{\text{本人拒否回数}}{\text{試行回数}}$$

SOMから，学習済みノードと投入ベクトルのノード間の距離を，2次元座標におけるユークリッド距離を用いて求めた．ユークリッド距離に閾値nを設け，nよりもユークリッド距離が小さければ本人，n以上ならば他人と判断する．

4.4 実験結果

主成分分析によって評価された指標のうち多くの変動を説明できる指標のみを，属性ベクトルとして SOM に投入した．主成分の数は，累積寄与率が 0.8 以上となることが一つの基準であるため，投入する特徴点データを第 5 主成分から第 8 主成分までに変化させ，それぞれで SOM を作成し，特徴点削減前の誤認識率と比較した．なお，SOM は初期値が乱数を利用して決定されるため，作成するたびに毎回異なるマップとなる．そのため主成分の数を変える毎に 30 枚の SOM を作成し，その平均の誤認識率を比較した．結果を表 4.2 に示す．

表 4.2　属性ベクトル数による誤認識率の変化

属性ベクトル数	5	6	7	8	20
平均 EER	0.0949	0.0854	0.0822	0.0852	0.0557

4.2 節では 5 つの主成分で累積寄与率 0.8 となったので多くの主成分は必要ないと思えたが，表 4.2 から次元圧縮を行わずに SOM を作ることで，最も誤認識率が低下するという結果が得られた．男性被験者 10 名で行った前実験 [6]では，次元圧縮を行って属性ベクトル数を 7 つにすることで誤認識率が最も低下したが，今回の実験では異なる結果となった．前実験では男性被験者のみであったが，今回は女性被験者も含まれるため各データの変動が大きくなり，各被験者の判別に必要な属性ベクトルが増えたのではないかと考えられる．

5. イントラネットへの応用事例

本研究の応用例としてイントラネットでの個人認識を提案する．本稿では，具体的な事例を取り上げて実用化に向けて考察し，ここでは定量的な分析は扱わない．

イントラネットでバイオメトリクスセキュリティを使用する利点として，個人の識別以外にも確実に本人が利用したという証明が可能というメリットがある．利用環境は社内限定であるため，利用者は自分のデスクと PC を持っていると仮定する．利用人数は社員数となるので，不特定多数の利用者を想定する必要はない．手指形状から個人を特定するため，経年変化によって誤識別率は上昇すると考えられるが，イントラネットへの応用例では利用者は成人しているため経年変化は少ない．本認証システムは初回のみ数分の登録作業が必要だが，認証は高速である．また，認証動作もキーボードに手を置くだけなので習熟する必要はない．サーバ側が手指形状データを保持し，認証処理はクライアント側で行うことで負荷の分散を図る．また，サーバ側が身体情報と認証に用いる SOM の情報を持つことで管理を一元化し，更新などの手間を少なくする．本人拒否率と他人受容率はトレードオフの関係であるためどちらを重視するかによって利便性と安全性が変化する．今回想定する事例では安全性が重視されると思われる．何らかの理由によって」認証が失敗した場合，バックアップとしてパスワードによる認証を行わず，システム管理者に連絡することとする．

以上のような背景での本認証手法を社内サーバのログインに利用した場合の事例を考察する．提案システムを導入する場合，認証に必要な機器はキーボードとカメラであり，設置スペースは確保できると思われる．想定される脅威として，成りすまし，サーバ上の身体情報の搾取，照合に用いる身体情報の改ざん，照合結果の改ざんの 4 つが考えられる．成りすましの方法として，写真の貼り付け，認証する対象の偽造が考えられる．指紋のように認証の対象物を偽造するのは難しい，写真を張り付けて偽る場合はホームポジションに構えられた手指を決められた角度，距離から撮影する必要があり困難だと思われる．サーバ上の身体情報の搾取への対策はデータを暗号化が考えられるが，クラッキングされた場合の対策としてバックアップを取り，他のサービスを行うサーバと分けることで被害の軽減が可能である．身体情報や照合結果の改ざんは，クライアントとサーバがネットワーク上でやり取りをする場合に想定される脅威である．サーバに送る認証結果の改ざんと，サーバからクライアントへ送る身体情報のテンプレートの改ざんが想定される．これらへの対策はネットワークから物理的に隔離するか，SSL（Secure Socket Layer）によるトンネリングがある．

以上の考察結果から，イントラネットへの応用事例では利用者の利便性を損なうことなく経年変化を考慮する必要がないと思われる．安全性を重視する場合本認証システムとパスワードとの認証の組合せが考えられる．

6. おわりに

検討した手法による被験者 30 名の場合の誤識別率は約 5.56%であった．5 章で提案した事例に本認証システムを使用する場合，更なる誤認識率の低減が必要となる．本認証方法は特徴空間の類似度をニューラルネットワークで学習し，本人であるかを判断するため，識別精度は 100%にはならない．そのため，今後は他の判別方法との比較検討や，新たな特徴点の追加によってより高い認識率の実現を目指す．

参考文献

1) バイオメトリックセキュリティ・ハンドブック，オーム社(2006).
2) 徳高平蔵，岸田悟，藤村喜久朗：自己組織化マップの応用，海文堂出版株式会社(1999).
3) Arne Sch affler，Sabine Schdmidt：からだの構造と機能，西村書店(2002).
4) pickmap，http://fishers.homeunix.net/software/pickmap/index.html#3(2011.1.27).
5) 浜田義彦：統計的パターン認識入門，森北出版株式会社(2009).
6) 中村孔明，髙橋雅隆，納富一宏，斎藤 恵一:手指形状認識による画像認証手法を行うための特徴軸決定-主成分分析による次元圧縮-，情報処理学会第 73 回全国大会 3Y-1, pp.503-504, (2011).