

圧力センサ搭載ヘルメットを用いた個人識別手法

藤井 敦寛¹ 村尾 和哉^{1,2}

概要: ヘルメットは社会生活において広く利用されている。本研究では 32 個の圧力センサを搭載したヘルメットを装着することで、頭部形状から個人を識別する手法を提案する。提案手法によって、ヘルメット上部に取り付けたディスプレイに名前を表示したり、視線情報などのデータを記録する際に手間なく作業者のラベルを付与できる。また、工場などで役職などにより入室できる部屋が制限されている場合に扉の鍵としても使用できる。提案手法は、あらかじめデータが登録された複数の人物のうちの 1 人がヘルメットを装着したときにその人物を識別する個人識別と、ヘルメットを装着した人物が登録者であれば認証し、登録者でなければ拒否する本人認証の 2 つの機構を備える。プロトタイプデバイスと解析用のソフトウェアを実装した後、被験者 9 人データを採取し、個人識別では精度が 100%, 本人認証では被験者全員の平均 EER が約 7.6%という結果を得た。

1. はじめに

ヘルメットは、スポーツやレジャー、バイク乗車時、工場、災害現場など、社会生活において広く利用されている。これらはいずれも、事故発生時に頭部を保護する目的で着用 [1] するものであり、頭部との隙間がないことが安全面において重要だとされている。

特に、工場や災害現場ではほぼ全員がヘルメットを装着して作業し、短期労働者や業者など、互いに顔を知らないさまざまな人間が出入りしている。一人 1 個のヘルメットを所有している場合はヘルメットに氏名がテープ等で表示されていたため、ヘルメットを装着したままでも遠くからあるいは頭上からでも識別できる。また、作業者によって所持している資格や従事可能な作業が異なるため、所有資格を示すステッカーが販売されており、そのような作業者のヘルメットに貼り付けて識別できるようにしている。しかし、貸与されたヘルメットの場合、ヘルメットに名前が表示されておらず、現場にいる者どうしも誰であるかを判断できず、不審者が容易に侵入できる可能性がある。また、仮に名前が表示されていたとしても、取り間違いによって、作業者とヘルメットの氏名が異なる場合もある。

本研究ではヘルメットの内部に圧力センサを搭載することで、頭部形状から個人を識別する手法を提案する。提案手法によって、ヘルメット上部に取り付けたディスプレイに名前や資格情報を表示できるため、ヘルメットが共用でも互いに認識でき、取り違えることもない。また、ヘル

メットに取り付けられたカメラや視線計測装置、各種センサのデータを自動で作業者と紐づけることができる。さらに、GPS モジュールとアンテナ [2] を取り付けることで、リアルタイムに作業員の名前と位置情報を送信することができれば、現場の全体の状況が把握しやすくなる。さらには、頭部形状を取得することによりヘルメットと頭部の隙間や圧迫の情報を取得できるため、ヘルメットと頭部形状が合っているかを確認することもできる。

このほか、工場などで役職や資格により入室できる部屋が制限されている場合の扉の鍵としての使用や、バイクの鍵としても使用できる。ヘルメットでの本人識別を行うため、鍵の盗難による侵入、車両盗難のリスクの減少にも繋がる。

個人を識別する手法として、パスワードや PIN、ストロークパターンなどの本人がカギを自由に設定できる手法、顔、指紋や筆跡、声紋、光彩などの身体的特徴を用いる手法、筆跡や歩容などの行動的特徴を用いる手法がある。個人が自由に設定できるパスワードや PIN、ストロークパターンのみを用いて、本研究で想定するような多数の人間の識別を行うことは、パスワードの重複や総当たり攻撃によるなりすましの危険性がある。

身体的特徴に関して、Chen ら [3] はスマートフォンなどの端末のフロントカメラとリアカメラから得られる顔と指先のビデオ映像からユーザ本人を認証する手法を提案している。ヘルメットの外部にあらかじめカメラを取り付けておくことで装着者を識別できると考えられるが、暗所や雨天では認識精度が低下する恐れがある。また、毎回ヘルメットを被る前に、ヘルメットを持って自身の顔を撮影す

¹ 立命館大学大学院情報理工学研究科

² 国立研究開発法人科学技術振興機構さきがけ

ることは面倒である。指紋認証 [4] は、指紋が写真などから容易に複製されるリスクがある。本研究で用いた頭部形状は、個人ごとに身体的特徴を持つ。また、立体形状であるため複製が困難であると考えられる。

行動的特徴を使うアプローチの場合、ヘルメットを装着する時点で個人が識別されている必要があるため、ヘルメットを被る動作を特徴とすることも考えられる。筆者らはこれまでにスマートフォンをポケットから取り出す際の加速度センサデータから認証する手法 [5] を提案した。スマートフォンはポケットや机の上など取る場面が限定されるが、ヘルメットを取る場面は様々であり、この手法をヘルメットに適用することは困難であると考えられる。

以降本稿では、2 節で関連研究を紹介する。3 節で提案手法を説明し、4 節で提案手法の評価実験と結果の考察を行い、最後に 5 節で本研究をまとめる。

2. 関連研究

本節では個人認証手法、身体部位装着型デバイス、頭部状態の認識に関する研究を紹介する。

2.1 個人認証手法

Bednarik ら [6] は、瞳孔の大きさや変化、視線速度、目の赤外線反射の距離などの眼球運動を使用した生体認証を提案した。Chen ら [3] はモバイルデバイスのフロントカメラとリアカメラで顔と指先のビデオ映像を同時に撮影し、個別の映像から抽出された 2 つのフォトプレチスモグラムを比較することにより、その一貫性から認証を行う手法を提案している。Siddharth ら [7] は掌紋と掌静脈を用いた生体認証システムを提案している。このシステムでは、可視光線と赤外線を使用して掌紋と掌静脈の画像を取得し、データベース内の登録データと照合することで認証を行っている。Sayo ら [8] は、身体的特徴である口唇の形状と、行動的特徴である発話に伴う口唇の動きをカメラで撮影して認証する手法を提案した。また、口元を用いた他の手法として、Kim ら [9] は歯の画像と音声を組み合わせた認証手法を提案している。

このようなカメラを使用したアプローチの場合、カメラをヘルメットの外側に取り付けておけば、ヘルメットを装着する前にカメラの方を向くことで個人を識別できるが、わざわざカメラで自身の顔を撮影する煩雑さがある。掌紋と掌静脈での認証の場合はヘルメットの側頭部にカメラを取り付け、着用時に握ることで実装が可能であるが、こちらの手法も装着するたびカメラを握らなければならない。フルフェイス型ヘルメットであれば、ヘルメットの口元にカメラを取り付けることで、口唇の形状、動きや歯の画像を取得できるが、ヘルメット内部の口元の空間は限られるため、口とカメラの距離が近くなってしまい、1 個のカメラで口唇の形状や動きを判別することは困難である。また、

すべてのヘルメットにカメラを装着する手間や経済的な問題がある。悪天候による水没や暗所での使用も考慮しなければならない、現実的ではない。

Guerra-Casanova ら [10] は加速度センサを内蔵したモバイルデバイスを用いて、ユーザが手を動かすジェスチャーによって認証する手法を提案している。

加速度センサを用いたジェスチャー認証の場合、ヘルメットに加速度センサを搭載することで、ヘルメットを装着するまでの動作の加速度の特徴量を用いて認証できる可能性がある。しかしながら、急いでいて動作が速くなる場合や、雨天時にヘルメットの内装が濡れないように気をつけながら装着する場合など、ヘルメットを装着する動作は多様であり、さまざまな状況において装着する可能性のある人全員のデータを採取して学習しておくことは現実的ではない。

Nogueira ら [4] は、畳み込みニューラルネットワーク (CNN) を用いて指紋認証を行うことで、高い分類精度を実現している。しかし、指紋は写真などから容易に複製できるリスクがある。

2.2 身体部位装着型デバイス

Ham ら [11] はスマートグラス用の入力デバイスとして、リストバンド型のデバイスを提案している。このデバイスはタッチパネルと慣性計測ユニットを搭載しており、タッチや手首をひねるなどのモーションで操作ができる。手首にデバイスを装着することで使用できるため、ユーザは動きを制限されず、自由度が高い。また、ポインティングにはタッチパネルを使用することで、入力の実用性を向上させた。Hernandez ら [12] は頭部装着型のウェアラブルデバイスである、Google Glass に内蔵された加速度センサ、ジャイロセンサ、カメラから脈拍数と呼吸数を認識する手法を提案している。Nishajith ら [13] は、視覚障害者の状況認識を支援するウェアラブルデバイスとして、スマートキャップの設計と実装を行った。デバイスは Raspberry Pi 3, Raspberry Pi NoIR Camera V2, イヤホン、電源から構成される。Raspberry Pi NoIR (No Infrared) Camera V2 とは Raspberry Pi の赤外線カメラモジュールである。この赤外線カメラで得られる画像から検出された対象物について、イヤホンを通して音声で説明する。

これらはいずれも身体部位に装着するウェアラブルデバイスに関する研究であり、さまざまな形状のデバイスを用いた研究が行われている。特に、頭部装着型のウェアラブルデバイスとしては帽子型や眼鏡型などが存在するが、ヘルメットを用いた研究は筆者らの知る限り存在しない。

2.3 頭部状態の認識

Electroencephalogram (EEG) ヘッドセットは脳波の計測に用いられるが、頭皮に電極を配置して計測を行うため、

局所的に筋信号が検出される。多くの場合はノイズとして除去されるが、Toth ら [14] はこの筋信号に注目し、安価な Electroencephalogram (EEG) ヘッドセットから得られる筋信号とジャイロセンサの値を用いて、6 種類の表情の分類を行った。表情の分類に既存の脳波デバイスを使用することで、別途追加で筋電位 (EMG) センサを用意する必要がなくなり、よりハイブリッドな脳コンピュータインタフェース (BCI) システムを構築できる。Kwon ら [15] は顔の表情と生理反応を利用して、利用者の感情を検出するメガネ型ウェアラブルデバイスを設計している。設計したデバイスは、内蔵したカメラで顔の表情が取得できる。また、フォトプレチスモグラム (PPG) や皮膚電気活動 (EDA) などの生理的反応を取得できる。これらを用いて利用者の感情を検出する。

これらの研究は、表情や顔部分の身体的反応などの動的な情報を取得するものであり、対して本研究は静的な頭部形状の特徴を取得するという点で異なる。

本研究では内装に圧力センサを搭載したヘルメットを装着することで、頭部形状を取得して個人識別する手法を提案する。提案手法は個人識別のために特別な動作を必要とせず、デバイスの搭載によって動作が制限されることもない。さらに、認証に用いる頭部形状を複製するには立体形状を正確に把握する必要がある、複製が困難である。

3. 提案手法

本節では提案手法の詳細を述べる。

3.1 概要

提案手法は、被験者が圧力センサを搭載したヘルメットを装着することで、頭部形状を取得し、装着者が事前に登録された人物であるかを識別する。本研究では2つの利用環境を想定する。一つ目は図 1 に示すように、複数の人物が登録されており、登録された人物（登録者）のうちのいずれかがヘルメットを装着した際に、その人物が登録者のうち誰かを認識する環境である。二つ目は、図 2 に示すように、1人以上の人物が登録されており、登録された人物以外を含む人物がヘルメットを装着した際に、その人物が登録者であれば認証し、登録者でなければ拒否する環境である。前者の環境を個人識別、後者の環境を本人認証と呼ぶ。

ヘルメットの内側には 32 個の圧力センサが搭載されており、32 次元のデータを取得する。提案システムでは、業務などでヘルメットを装着すると想定される人物を登録者として事前にヘルメットを装着してもらい、圧力センサデータを学習データとして収集しておく。個人識別では、識別したい利用者全員にヘルメットを複数回装着してもらうことで頭部の 32 次元の圧力センサデータ群を収集し、Support Vector Machine (SVM) を用いて学習データか

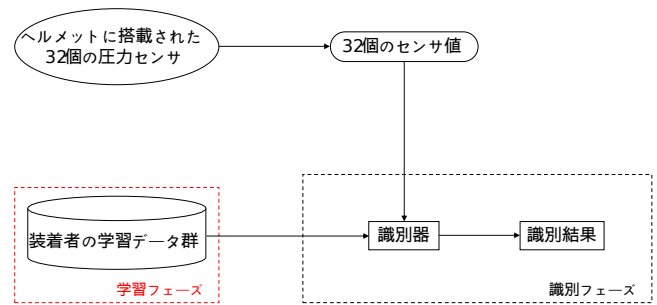


図 1 個人識別システムの構成

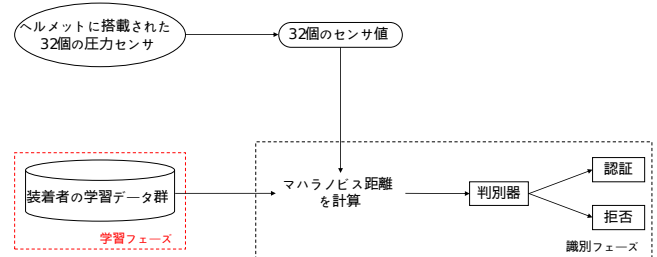


図 2 本人認証システムの構成

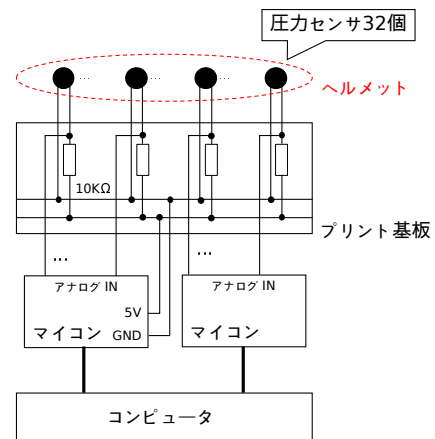


図 3 デバイスの構成

ら認識モデルを構築しておく。そして、識別フェーズで未知の登録者の入力データの特徴から識別結果を求める。一方、本人認証では、認証したい利用者にヘルメットを複数回装着してもらうことで頭部の 32 次元の圧力センサデータ群を収集しておく。そして、識別フェーズで登録者以外も含む人物の入力データと学習データ群とのマハラノビス距離を計算し、距離が閾値以下であれば本人であるとして認証する。

3.2 ハードウェア

提案手法に用いる圧力センサを搭載したヘルメットを実装した。デバイスの構成を図 3 に、デバイスの外観を図 4 に示す。

圧力値を正しく取得するには、センサとヘルメット装着者の頭部が密着している必要があるため、密着度の高いフルフェイス型ヘルメット (B&B 社製 BB100) を用いた。

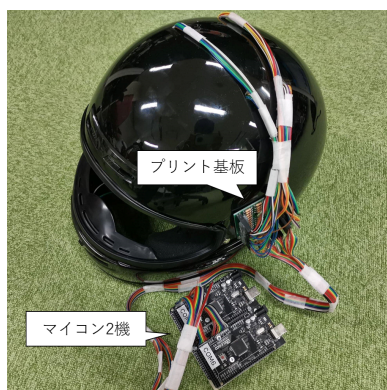


図 4 デバイスの外観



図 5 デバイスの内部



図 6 圧力センサの実装方法

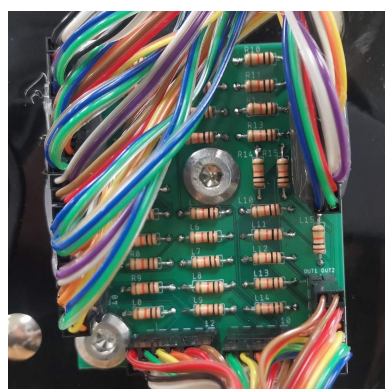


図 7 32 個の圧力センサと接続するプリント基板

圧力センサとしてインターリンクエレクトロニクス社製の FSR402 および FSR402 ShortTail を合計 32 個使用した。マイコンとして Arduino MEGA2560 R3 を使用した。使用したヘルメットはフリーサイズであり、内装の脱着が困難であったため、図 5 に示すように頭頂部の内装を取り外して、新たに厚みのあるウレタンスポンジを取り付けた。また、図 6 に示すようにウレタンスポンジの中央部に切り込みを入れて圧力センサを挿し込んだ。圧力センサは頭頂部に 4 個、頭頂部周囲に 16 個、後頭部に 6 個、左右チークパッド部に 6 個の合計 32 個を搭載した。配線はヘルメットの頭頂部にドリルで開けた穴から、ヘルメット外部に取り付けた 10KΩ の抵抗を配線してあるプリント基板を経由して、Arduino MEGA2560 R3 の 5V 電源、GND、アナログ入力ポートに接続した。ヘルメット外部に取り付けたプリント基板を図 7 に示す。プリント基板はヘルメットのシールド固定用に使われたネジ穴を用いて左頬部分にボルトで固定しており、取り外しが可能である。

3.3 個人識別手法

複数人がシステムに登録されており、その中からヘルメットを装着した人物を識別する手法では、機械学習アルゴリズムの一つである Support Vector Machine (SVM) を用いる。SVM は分類や回帰へ適用できる教師あり学習を用いるパターン認識モデルである。提案手法では登録者で

ラベル付けしたデータを事前に収集して SVM を学習させておき、その後、登録者のうち 1 名のデータを入力して登録者を識別する。

データの取得はユーザがヘルメットを装着することで開始する。ヘルメットを装着していない状態ではすべての圧力センサの電圧値がほぼ 5V である。ヘルメットの装着時に圧力センサの電圧値が下降し、値が安定した時刻 $t = T_s[s]$ から 2 秒間の 32 個の圧力センサデータ $p(t) = [p_{0,t}, \dots, p_{31,t}]$ を取得する。この 32 次元のデータから次元ごとに 2 秒間に得られたデータの N サンプルの平均値 $x(t) = \frac{1}{N} \sum_{t=T_s}^{T_s+N-1} p(t)$ を計算し、1 つの 32 次元のベクトルを特徴量として得る。事前に m 回ヘルメットを被って学習データ $[x_i, y_i]$ ($i = 1, \dots, m$) を収集し、SVM を学習させる。ただし、 y は登録者ラベル (登録者名や登録者番号など) である。そして、識別したいユーザの入力データ x を SVM に入力し、識別結果 $\hat{y}$ を得る。本手法では線形 SVM を使用し、パラメータは初期値である $C = 1.0$ とした。

3.4 本人認証

3.4.1 登録データとの距離計算

本人認証とは、1 人以上の利用者がシステムに登録されており、登録されている人がヘルメットを装着した場合は本人であると認証し、登録されていない人がヘルメットを

装着した場合は他人であるとして拒否する手法である。提案手法では、本人認証したい利用者の学習データと未知の装着者の入力データの距離計算方法として、マハラノビス距離を用いる。マハラノビス距離とは多変数間の距離計算手法のひとつであり、データの分布を考慮して正規化した距離を計算できる。

データの取得は個人識別の場合と同様に、ヘルメットの装着時に圧力センサの電圧値が下降し、値が安定した時刻 $t = T_s[s]$ から 2 秒間の 32 個の圧力センサデータ $p(t) = [p_{0,t}, \dots, p_{31,t}]$ を取得する。この 32 次元のデータから次元ごとに 2 秒間に得られたデータの N サンプルの平均値 $x(t) = \frac{1}{N} \sum_{t=T_s}^{T_s+N-1} p(t)$ を計算し、1 つの 32 次元のベクトルを特徴量として得る。

事前に m 回ヘルメットを被って学習データ $[x_i, y_i]$ ($i = 1, \dots, m$) を収集する。ただし、 y は登録者ラベル（登録者名や登録者番号など）である。学習データの平均値ベクトル μ と分散共分散行列 Σ を次式で求める。

$$\mu = \frac{1}{m} \sum_{i=1}^m x_i \quad (1)$$

$$\Sigma = \frac{1}{m} \sum_{i=1}^m (x_i - \mu)(x_i - \mu)^T \quad (2)$$

識別したいユーザの入力データ x とする。このとき、入力データが事前に登録された本人のデータであれば、入力データ x と学習データ x_i は同じ分散共分散行列 Σ の確率分布に従うため、入力データ x と学習データ x_i のマハラノビス距離は

$$d(x, x_i) = \sqrt{(x - x_i)^T \Sigma^{-1} (x - x_i)} \quad (3)$$

と定義できる。

3.4.2 認証判定

閾値を θ とおき、

$$\theta \geq \min_i (d(x, x_i)) \quad (i = 1, \dots, m) \quad (4)$$

を満たす場合、入力データ x は登録されているいずれかの所有者から得られたデータであると判定し認証する。式 4 を満たさない場合、入力データ x は登録されているいずれの所有者でもない人物のデータであると判定し拒否する。

3.5 ソフトウェア

Arduino MEGA のプログラムは Arduino IDE で実装した。Arduino MEGA からのデータを受信して csv 形式で保存するコンピュータのプログラムは Python で実装した。保存したデータの解析プログラムは Python で実装した。

個人識別では、事前に収集したセンサデータの csv ファイルを読み出し、sklearn.svm.SVC を用いて学習と識別を行う。sklearn.svm.SVC とは標準的なソフトマージン SVM を実装した scikit-learn[16] のライブラリである。

また、評価のために交差検証を行うライブラリである、sklearn.model.selection.cross_val_score を使用した。

本人認証では、事前に収集したセンサデータの csv ファイルを読み出し、sklearn.covariance.MinCovDet を用いて分散共分散行列を計算する。分散共分散行列の逆行列から、scipy.spatial.distance を用いてすべての学習データ x_i に対する入力データ x のマハラノビス距離を計算する。sklearn.covariance.MinCovDet とは、異常値に対して頑健な分散共分散行列の推定アルゴリズムである Minimum Covariance Determinant (MCD) を高速化した Fast-MCD[17] を実装した scikit-learn のライブラリである。また、scipy.spatial.distance とは、さまざまな距離計算の関数を実装した SciPy[18] のライブラリである。

4. 評価

本節では、提案手法の有効性を評価するために行った実験について説明する。

4.1 データ収集

被験者 9 名 (A~I, 全員男性, 平均年齢 23 歳) に 3 節で実装したヘルメットを装着させ、サンプリングレート約 30Hz でセンサデータを収集した。2 秒間装着してデータを採取し、取り外して再び 2 秒間装着してデータを採取する試行を 1 セット (2 サンプル) として、日を変えて 10 セット、合計で 2 秒 $\times$ 20 サンプル $\times$ 9 人のデータを収集した。ヘルメットの装着具合の変化にともなうセンサと頭部のさまざまな位置関係のデータを収集するために、セット間に 30 分以上の休憩時間を設けた。また、データの収集は 1 人あたり 1 日最大 4 セットとした。

4.2 個人識別

4.2.1 評価環境

収集したデータに対して、各被験者のデータの 80% (16 サンプル) を学習させ、20% (4 サンプル) をテストデータとする 5 分割交差検証によって評価した。使用するセンサの個数による影響も調査するため、1 個使用する場合から 32 個使用する場合までのすべてのセンサの組合せにおいて前述の試行を行った。

また、工事現場などで使用されるハーフ型ヘルメットを想定し、32 個のセンサのうち頭頂部の 4 個と頭頂部周囲の 16 個の合計 20 個のセンサに限定して、同様に 1 個使用する場合から 20 個使用する場合までの全てのセンサの組合せにおいて評価した。本評価では、32 個のセンサを使用する場合をフルフェイス型ヘルメット、20 個のセンサを使用する場合をハーフ型ヘルメットと呼ぶ。

4.2.2 結果と考察

フルフェイス型ヘルメットでの個人識別の精度を表 1 に示す。センサ数が 32 個の場合は、32 個すべてを使用する

表 1 フルフェイス型ヘルメットにおいてセンサ数を 1 個から 32 個まで変化した場合の個人識別精度

センサ数	精度
32	1.000
31	1.000
⋮	⋮
5	1.000
4	0.994
3	0.972
2	0.922
1	0.600

表 2 ハーフ型ヘルメットにおいてセンサ数を 1 個から 20 個まで変化した場合の個人識別精度

センサ数	精度
20	1.000
19	1.000
⋮	⋮
5	1.000
4	0.994
3	0.967
2	0.900
1	0.600

1 通りでの精度であり、センサ数が 31 個の場合は、32 個のうち 31 個を使用する ${}_{32}C_{31}=32$ 通りの中で最も高かった精度である。ここで、センサ数が 32 個および 31 個の場合の精度を評価したところ 1.00 であったため、センサ数を 1 個から増やしていき、精度が 1.00 に到達するところまでを評価した。

結果より、センサ数が 5 個のとき、9 人の識別に 100% の精度で成功した。センサ数が 4 個で 99.4%，3 個で 97.2%，2 個で 92.2% と高い精度が得られたが、センサ数が 1 個では 60% と大幅に下がった。

ハーフ型ヘルメットでの個人識別の精度を表 2 に示す。この結果もフルフェイス型ヘルメットと同様にセンサ数が 20 個および 19 個の場合の精度を評価したところ 1.00 であったため、センサ数を 1 個から増やしていき、精度が 1.00 に到達するところまで評価した。

結果より、センサ数が 5 個のとき、9 人の識別に 100% の精度で成功した。センサ数が 4 個、3 個、2 個の場合では 99.4%，96.7%，90.0% と高い精度が得られたが、センサ数が 1 個では 60% と大幅に下がった。

これらの結果より、本実験で利用したデータセットに対して、フルフェイス型ヘルメットおよびハーフ型ヘルメットのどちらにおいても、センサ数 5 個で 100% の精度で識別できることを確認した。しかしながら、登録者数が増加した場合、高い精度を得るためには必要となるセンサ数が増加すると考えられる。

4.3 本人認証

4.3.1 評価環境

収集したデータのうち、1 名の被験者を本人、残り 8 名の被験者を他人として、本人としたデータの 80% (16 サンプル) を学習データとして登録し、残り 20% (4 サンプル) をテストデータとして 5 分割交差検証を行い本人の認証精度を計測した。さらに、交差検証で使った 5 パターンの学習データに対して、他人とした 8 名すべてのデータ (160 サンプル) を用いて他人の認証精度を計測した。また、本人を 9 名全員ローテーションして評価した。

認証精度の評価指標として、FRR, FAR, EER を用いる。FRR (False Reject Rate: 本人拒否率) は本人を他人であると誤って判断し拒否する割合である。FAR (False Accept Rate: 他人受入率) は他人を本人であると誤って判断し認証する割合である。認証するか否かを決定する閾値を小さく設定するほど認証判定が厳密になるため FRR が増加し、対して閾値を大きく設定するほど認証判定が緩くなるため FAR が増加する。FRR と FAR はトレードオフの関係にあり、FRR と FAR が同値になるときの値を EER (Equal Error Rate: 等誤り率) と呼ぶ。通常、本人認証手法の性能評価においては EER の値が指標として用いられ、EER が小さいほど性能が良いとされる。

4.3.2 結果と考察

各被験者の EER を表 3 に示す。また、閾値を変化させたときの各被験者の FRR と FAR を図 8 に示す。Total は被験者全員の平均を示している。表 3 より被験者 A, E, G, I の EER はおよそ 0.01 以下と良い結果が得られた。これは、検証に用いたデータセットにおいて、本人は 100 回に 1 回以下の割合で認証に失敗し、他人は 100 回に 1 回以下の割合で認証を突破することを意味している。文献 [19] において、顔認証の EER が 0.012 であると報告されていることを考慮すると、これらの被験者については同等の性能が得られたといえる。図 8 より、被験者 E については、閾値が他の被験者よりも大きい 60 程度で FRR と FAR が交差している。これは収集した圧力データのサンプルに外れ値が存在したため、外れ値を正しく認証するために閾値を大きくする必要があったためである。

次に精度が良い被験者は C, D, H であり、EER はおよそ 0.05 である。ここで精度の低下の要因を究明するために、収集したすべてのデータに対して主成分分析を行い、第一主成分および第二主成分の 2 次元に圧縮したデータを 2 次元平面上にプロットし、目視で確認した。結果を図 9 に示す。図 9 より、被験者 C について見ると、被験者 C のデータ群のうち 1 サンプルが被験者 I のデータ群と近い位置にあるが、他の被験者のデータ群との重なりは見られない。しかしながら、第一主成分方向の分散が大きい。一方、被験者 D, H のデータ群は互いに大きく重なっており、両者が影響し合って精度が低下したと考えられる。

表 3 本人認証における各被験者および全被験者平均の EER

被験者	EER
A	0.002
B	0.095
C	0.050
D	0.055
E	0.006
F	0.094
G	0.012
H	0.050
I	0.000
Total	0.076

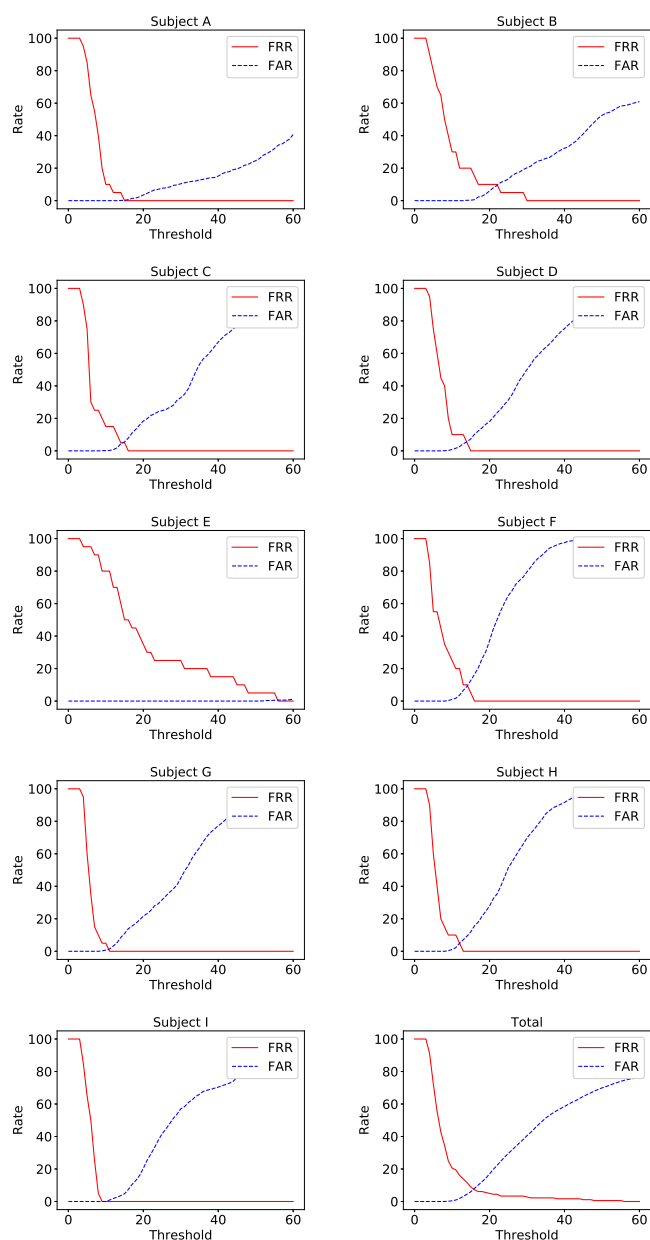


図 8 本人認証における各被験者および全被験者平均の FRR と FAR

最も精度が悪かった被験者は B, F であり, これらの被験者の EER はおよそ 0.095 であった. 被験者 B のデータ群は分散が小さいが, 被験者 I のデータ群との重なりが

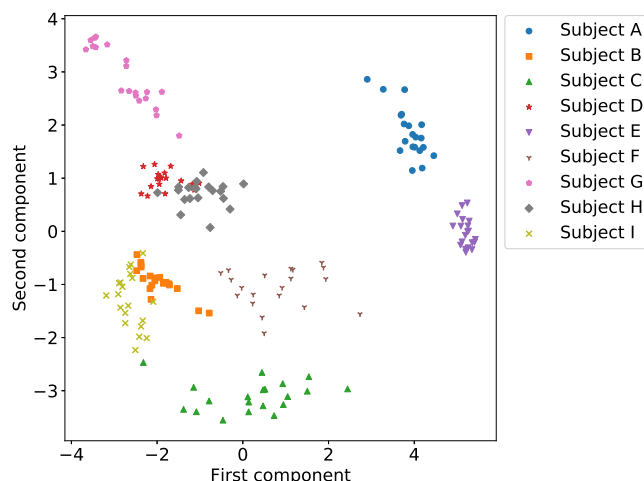


図 9 32 次元の特徴量を PCA によって 2 次元に圧縮した主成分の分布

見られる. しかしながら, 検証に用いたデータセットにおける被験者 I の EER は 0 であり, 誤りなく判別ができていた. したがって, これらのデータ群の重なりは主成分分析で 2 次元に圧縮した際のデータの損失による影響だと考えられる. 一方, 被験者 F のデータ群は他の被験者のデータ群との重なりが見られないが, 第一主成分と第二主成分の両方向の分散が大きい. 主成分分析によるデータ圧縮の影響を考慮すると, 32 次元のデータでは他の被験者のデータ群との重複が推察される. 被験者 F のデータの散らばりに影響されて, 被験者 F のデータ群の近くに位置する被験者 B, C の精度も低下したと考えられる. 特に, 被験者 B は 2 サンプルが被験者 F のデータ群と近い位置に存在するため, 被験者 C に比べて精度が低下したと考えられる.

被験者全員の平均 EER は約 0.076 であった. 被験者ごとの EER に差が見られたことから, より多くの被験者のデータを用いて検証する必要がある. また, 提案手法は学習データと入力データの距離を用いて認証を行うため, 学習データ数をさらに増やすことで精度の改善が見込まれる. このほか, ヘルメットを装着する一連の流れにおける時系列圧力データを用いて認証する手法についても今後検証する.

5. おわりに

本研究では, 圧力センサを内部に取り付けたヘルメットを装着することで頭部の形状を計測して, 頭部形状の個人差から個人を識別する手法を提案し, プロトタイプデバイスの実装と評価を行った. プロトタイプデバイスは市販のフルフェイス型ヘルメットを加工し, 圧力センサを取り付けた. 評価では, プロトタイプデバイスからデータを取得するためにデータ収集プログラムを作成し, 頭部形状データとして被験者 9 人からそれぞれ 2 秒間のセンサ値を 20 回分取得した. 複数の登録者のうち誰が装着したのかを判別することを目的とした個人識別と, 二輪車の鍵のように

用いることを想定して1名の登録者であるか他人であるかを判別することを目的とする本人認証を行った。

評価実験では、個人識別では非常に精度が高かったため、識別に使用するセンサ数を減少させて識別精度がどのように変化するかを検証した。その結果、本実験で使ったデータセットに対して一番効率の良いセンサ数は、フルフェイス型ヘルメットおよび、ハーフ型ヘルメットのどちらの場合も5個であった。本人認証では認証の精度の評価指標であるEERが9名中4名が0.012以下、平均0.076という結果が得られた。これらの結果より、本手法は個人識別手法として有効であると考えられる。今後はさらなるデータの収集を行い、実環境での提案手法の評価を行う。

参考文献

- [1] R.G. Attewell, K. Glase, and M. McFadden. Bicycle helmet efficacy: a meta-analysis. *Accident Analysis & Prevention*, Vol. 33, No. 3, pp. 345–352, 2001.
- [2] T. Nakao, N. T. Hung, M. Nagatoshi, and H. Morishita. Fundamental study on curved folded dipole antenna. In *Proceedings of the 2012 IEEE International Symposium on Antennas and Propagation*, pp. 1–2, 2012.
- [3] Y. Chen, J. Sun, X. Jin, T. Li, R. Zhang, and Y. Zhang. Your face your heart: Secure mobile face authentication with photoplethysmograms. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, 2017.
- [4] R. F. Nogueira, R. de Alencar Lotufo, and R. Campos Machado. Fingerprint liveness detection using convolutional neural networks. *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 6, pp. 1206–1213, 2016.
- [5] R. Izuta, K. Murao, T. Terada, T. Iso, H. Inamura, and M. Tsukamoto. Screen unlocking method using behavioral characteristics when taking mobile phone from pocket. In *The 14th International Conference on Advances in Mobile Computing and Multimedia (MoMM 2016)*, pp. 110–114, 2016.
- [6] Roman Bednarik, Tomi Kinnunen, Andrei Mihaila, and Pasi Fränti. Eye-movements as a biometric. In Heikki Kalviainen, Jussi Parkkinen, and Arto Kaarna, editors, *Image Analysis*, pp. 780–789, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.
- [7] J. Ajay Siddharth, A. P. Hari Prabha, T. J. Srinivasan, and N. Lalithamani. Palm print and palm vein biometric authentication system. In Subhransu Sekhar Dash, K. Vijayakumar, Bijaya Ketan Panigrahi, and Swagatam Das, editors, *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, pp. 539–545, Singapore, 2017. Springer Singapore.
- [8] A. Sayo, Y. Kajikawa, and M. Muneyasu. Biometrics authentication method using lip motion in utterance. In *2011 8th International Conference on Information, Communications Signal Processing*, pp. 1–5, 2011.
- [9] D. Kim and K. Hong. Multimodal biometric authentication using teeth image and voice in mobile environment. *IEEE Transactions on Consumer Electronics*, Vol. 54, No. 4, pp. 1790–1797, 2008.
- [10] J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra. Authentication in mobile devices through hand gesture recognition. *International Journal of Information Security*, Vol. 11, No. 2, pp. 65–83, 2012.
- [11] Jooyeun Ham, Jonggi Hong, Youngkyoon Jang, Seung Hwan Ko, and Woontack Woo. Smart wristband: Touch-and-motion-tracking wearable 3d input device for smart glasses. In Norbert Streitz and Panos Markopoulos, editors, *Distributed, Ambient, and Pervasive Interactions*, pp. 109–118, Cham, 2014. Springer International Publishing.
- [12] J. Hernandez, Y. Li, J. M. Rehg, and R. W. Picard. Bioglass: Physiological parameter estimation using a head-mounted wearable device. In *2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MO-BIHEALTH)*, pp. 55–58, 2014.
- [13] A. Nishajith, J. Nivedha, S. S. Nair, and J. Mohammed Shaffi. Smart cap - wearable visual guidance system for blind. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 275–278, 2018.
- [14] J. Toth and M. Arvaneh. Facial expression classification using eeg and gyroscope signals. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 1018–1021, 2017.
- [15] J. Kwon, D. Kim, W. Park, and L. Kim. A wearable device for emotional recognition using facial expression and physiological response. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 5765–5768, 2016.
- [16] scikit-learn. <https://scikit-learn.org/>.
- [17] Peter J. Rousseeuw and Katrien Van Driessen. A fast algorithm for the minimum covariance determinant estimator. *Technometrics*, Vol. 41, No. 3, pp. 212–223, 1999.
- [18] SciPy.org. <https://www.scipy.org/>.
- [19] Qian Tao and Raymond N.J. Veldhuis. Biometric authentication for a mobile personal device. In *Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services Workshops*, pp. 1–3, 2006.