

楕円による MP 関節位置推定を活用した タッチベース認証特徴量の提案

高橋 なずな[†] 古川 大樹[‡] 新井 大稀[‡] 山名 早人[§]

[†] 早稲田大学 基幹理工学部 〒169-8555 東京都新宿区大久保 3-4-1

[‡] 早稲田大学大学院 基幹理工学研究科 〒169-8555 東京都新宿区大久保 3-4-1

[§] 早稲田大学 理工学術院 〒169-8555 東京都新宿区大久保 3-4-1

E-mail: [†] [‡] [§] {nzn3014, taikifurukawa, haruki-arai, yamana}@yama.info.waseda.ac.jp

あらまし 近年、スマートフォンにおける新たな認証方式として、タッチ操作から得られる特徴を基に継続的にユーザの識別を行うタッチベース認証が注目されている。同手法は追加センサを必要とせず連続的に認証を行える一方で、既存の生体認証と比較して認証精度が低いという課題がある。把持方法の変化に起因するタッチ位置のばらつきへの対策として、MP 関節位置推定に基づく特徴量が提案されているが、MP 関節位置の推定精度の限界により、本来の認証特性を引き出せていない。本研究では、ストロークを楕円軌道と仮定した MP 関節位置の新たな推定手法に基づく特徴量を提案し、認証精度改善に有効であることを確認した。さらに従来手法とのアンサンブルにより、Random Forest を使用した検証で最大 1.00% の EER 改善を確認した。

キーワード タッチベース認証, 生体認証, スマートフォン, 特徴量生成

1. はじめに

近年、スマートフォンの普及に伴い、人々は個人情報や機密情報をスマートフォン上で扱う機会が増加している。そのためスマートフォンが悪意ある第三者からアクセスされることを防ぐために、現在多くの認証技術が利用されている[1]。スマートフォンの保護に使われる認証技術には、主にピンやパスワードを用いる知識ベース認証と、指紋や虹彩といった生体情報を用いる生体認証[2]が存在する[3]。しかし、現在実用されている認証技術には課題が残されている。第一に、既存技術では操作開始時にのみ認証を行うため、認証後の操作ではロックを掛けない限り他人に操作される可能性がある。第二に、生体認証において、認証専用のセンサの搭載が必要であり特に安価な端末には認証精度にばらつきが生じることがある[4]。

これらの課題を解決する新たな認証技術として、タッチベース認証が注目されている。タッチベース認証とは、ユーザによる画面へのタッチ操作から得られるタッチ座標やタッチ圧力、タッチ速度などの特徴量を使用して、継続的にユーザの認証を行う技術である。同技術はユーザの操作中に継続的に認証を行う「継続認証」であり、認証のために追加のセンサを必要とせずスマートフォンへの導入が容易であるという点で現状の認証技術の補完に有効である[4]。一方で、実用にあたっては既存の生体認証技術と比較して精度が低いという点が課題となっている。

タッチベース認証の精度低下の原因として、把持方法及び姿勢変化によるタッチ特性のばらつきが挙げられる[5][6][7]。特に把持方法の変化への対策として、親指の第二関節である MP 関節位置の推定に基づいた

特徴量が提案されている[8]。この手法では親指によるストロークを円軌道とみなし推定を行い、円の中心座標を MP 関節位置と仮定する。MP 関節位置を極としたストロークの相対座標を特徴量として使用することで、認証精度の向上に成功した。

しかし、同手法では円軌道を仮定した MP 関節位置の推定精度には限界があり、本来の認証特性を引き出せていない。一部のストロークでは、推定された円の中心座標が時系列的に大きく変動している。これは、MP 関節位置を「把持方法の変化がない限り位置が大きく変動しない」と仮定していることに反する。つまり、MP 関節位置の推定精度を改善することにより、認証精度の更なる向上を望めると考えられる。

そこで本研究では、MP 関節位置の新たな推定手法に基づいた特徴量を提案する。ストローク軌道の形状を楕円として捉えるモデルを用いて MP 関節位置を推定することで、認証精度の向上を目指す。

本論文は以下の構成をとる。2 節では、本研究の関連研究を紹介する。3 節では楕円を用いた MP 関節位置推定手法の安定性を評価し、4 節では楕円に基づく新たな特徴量の導入と既存の手法とのアンサンブルを提案し、5 節で評価実験の手法を説明する。6 節で評価結果と考察を述べ、7 節で分類器によるモデル選択を検討する。8 節で本論文をまとめる。

2. 背景知識及び関連研究

本節では、関連研究からタッチベース認証における本研究の位置づけを示す。本研究でのアプローチを踏まえ、タッチベース認証においてこれまで提案されてきた特徴量を中心に紹介する。

2.1. タッチベース認証の特徴量

タッチベース認証は、ユーザによる画面へのタッチから得られる情報を学習することで、現在タッチ操作をしているユーザが本人であるかを判定する技術である。

タッチベース認証の特徴量は 1) 時間的特徴 (Temporal features), 2) 空間的特徴 (Spatial features), 3) 動的特徴 (Dynamic features), 4) 幾何学的特徴 (Geometric features) の 4 つに大別される[4][9]。タッチベース認証では、センサから得られたこれらの特徴量を組み合わせることで、ユーザのタッチ特性の学習を行う。

表 2.1 に示す Frank らの研究にて採用されている 27 種の特徴量[10] (以下 Frank 特徴量) は、これまでタッチベース認証の研究において広く採用されており[7][8][11][12][13]、本分野における標準的な特徴量である。

また、タッチスクリーンのタッチセンサから得られるストローク情報の他に、スマートフォンの他のセンサから得られる特徴量が提案されている。Sitova らは、スマートフォンに内蔵された加速度センサ、ジャイロセンサ、磁力センサから得られる特徴量として、HMOG 特徴量を提案している[14]。また、工藤らは従来タッチスクリーンの接触面積から計算されていたタッチ圧力を、スマートフォン内蔵の圧力センサから得られる正確なデータに置き換える手法を提案している[15]。

2.2. タッチ特性を変化させる外的要因

タッチベース認証は、既存の生体認証と比較して認証精度が低い。タッチベース認証の精度低下を招く要因として、同一ユーザにおけるタッチ特性の変化が挙げられる[5][6][7]。タッチ特性を変化させる外的要因には、主にスマートフォンの把持方法、操作姿勢の変化、デバイスの違いが挙げられる。操作への慣れに代表される中長期的な変化の他、把持方法や操作姿勢は短期的にも変化する。認証精度改善のためには、このような変化に頑健な認証手法が求められる。工藤らは姿勢毎に別々の学習器を認証使うことで精度が向上することを示した[15]。

2.3. MP 関節位置に基づくタッチベース認証特徴量

本研究の先行研究である工藤らは、特に短期的に変化する把持方法の変化への対策として円軌道による MP 関節位置の推定に基づくタッチベース認証特徴量を提案した[8]。

同研究では、ストロークを円軌道と仮定することによって MP 関節位置を推定する。1 ストロークのデータポイントの座標から最小二乗円を計算し、円の中心座標位置を MP 関節位置とする。推定した MP 関節位置を基に「MP 関節位置を中心とした軌跡円半径」、「MP 関節位置を極としたストローク開始地点の偏角」、「MP 関節位置を極としたストローク終了地点の偏角」

表 2.1 Frank 特徴量[10]の一覧

No.	定義	カテゴリ
1	直前のストロークとの間隔時間 [ms]	時間的特徴
2	ストローク継続時間 [ms]	時間的特徴
3, 4	ストローク開始地点の XY 座標 [px]	空間的特徴
5, 6	ストローク終了地点の XY 座標 [px]	空間的特徴
7, 8, 9	ストローク 20%・50%・80%地点の速度 [px/ms]	動的特徴
10	ストロークが終了する直前 3 地点の速度の中央値 [px/ms]	動的特徴
11, 12, 13	ストローク 20%・50%・80%地点の加速度 [px/ms ²]	動的特徴
14	ストローク開始直後 5 地点の加速度の中央値 [px/ms ²]	動的特徴
15, 16, 17	ストローク 20%・50%・80%地点の偏差 [px]	幾何学的特徴
18	ストローク中の偏差の最大値 [px]	幾何学的特徴
19	ストローク 50%地点の圧力	空間的特徴
20	ストローク 50%地点の接触面積 [px ²]	空間的特徴
21	ストローク端点を結ぶ線分の長さ [px]	幾何学的特徴
22	ストローク軌跡の長さとストローク端点を結ぶ線分の長さの比	幾何学的特徴
23	ストロークの平均合成ベクトル長 [15]	幾何学的特徴
24	原点とストローク内の各データ点が形成する角度の平均 [rad]	幾何学的特徴
25	ストローク方向のフラグ (up/down/left/right)	その他
26	ストローク 50%地点のスクリーンに対する指の向き	その他
27	デバイスの向き (landscape/portrait)	その他

の3つの特徴量を提案し、これらを標準的な特徴量群に加えて認証を行うことで、最大で1.09%のEER改善を達成した。

また同論文では、タッチ特徴量の絶対位置の変化が、認証精度に与える影響について検証を行っている。標準的なFrank特徴量では絶対位置を変動させると認証精度が有意に低下することを示した上で、MP関節位置に基づいた新規特徴量の追加によって、ストロークの絶対位置変動に対しても認証精度が落ちにくく、把持方法の変化に対して頑健であることを確認している。

2.4. 本研究の位置づけ

本来、スマートフォンを把持したときの親指の第二関節位置は、スマートフォンの大きさに対して大きく変動しないと考えられる。しかし3.2節に示す実験により、工藤らの推定手法では一部のストロークにおいて、推定された円の中心座標が時系列的に大きく変動していることを確認した。

そこで本研究では、より柔軟なMP関節位置の推定手法によって、更なるタッチベース認証精度の改善を目指す。具体的には、タッチストロークを円軌道ではなく楕円軌道と仮定することによって、より現実に対応したMP関節位置の推定を行う。

3. 推定した中心位置と安定性の評価

本節では、ストロークの軌跡を楕円軌道と仮定することによるMP関節位置推定手法を提案する。また、提案手法によって推定した楕円と、従来手法によって推定した円の中心位置の変動を比較し安定性の評価を行う。

3.1. 楕円軌道を仮定したMP関節位置推定手法

タッチ操作を行う指の可動域は関節によって制限される。したがって、ストロークは関節位置を中心とした弧を描いていると考えることができる。親指の第二関節であるMP関節位置を極とした座標系を導入することにより、把持方法の変化による影響を受けずにストロークからユーザーの特性を読み取ることができる。ストロークを円軌道として仮定していた従来のMP関節位置推定手法[8]（以下、円軌道による推定手法）を基に、本研究ではストロークを楕円軌道と仮定することでMP関節位置を推定する。円軌道を仮定した場合、ストローク形状の非対称性や指の伸縮に起因する偏りを表現できない。一方、楕円軌道を仮定することで、主軸方向および軸長の違いを通じて、より柔軟にストローク形状を捉えることが可能となる。

楕円軌道の推定には、OpenCVのfitEllipse関数を用いる。この関数による楕円フィッティングは、Fitzgibbonら[17]の提案する最小二乗法に基づく円錐

曲線フィッティング手法に基づいている。楕円は円錐曲線の一般式（式3.1）で表される。与えられたストローク点群に対して、この式を満たすパラメータを最小二乗法により推定する。ただし、楕円以外の円錐曲線が解として得られることを防ぐため、Fitzgibbonらによって提案された楕円条件（式3.2）を制約として用いる。

推定された楕円の中心座標をMP関節位置と仮定し、特徴量の算出に利用する。

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \quad (3.1)$$

$$4AC - B^2 > 0 \quad (3.2)$$

3.2. 推定した中心位置と安定性の評価

本節における検証の目的は、提案した推定手法によって、より多くのストロークに対して安定的にMP関節位置を推定できていることを確認することである。

MP関節位置は指でストローク描く際の基準であり、大きな変動はしないと考えられる。この観点に基づいて、「MP関節位置推定の安定性」を、式3.3に示す中心位置の時系列的な変動量（以下、中心位置変動量）で評価する。ここで Δx と Δy は連続する2ストロークにおける推定中心座標の差分であり、式は時系列的に連続するストロークから推定された中心座標位置の移動距離を表す。中心位置変動量が小さいほど中心座標、つまりMP関節位置と推定される地点が変動しないことを示す。

$$\sqrt{(\Delta x)^2 + (\Delta y)^2} \quad (3.3)$$

データセットには、工藤らの公開したeCommTouch[18]を用いる。eCommTouchデータセット（以下、ECTデータセット）は、ECサイトを再現したwebアプリケーションを、右手親指で操作している際のタッチデータで構成される。各ユーザが垂直方向へのスワイプと水平方向へのスワイプをする操作のそれぞれ3セッション分のデータが含まれている。同一セッション内のストロークは連続しており、把持方法の変化は小さいと考えられる。なお、使用するデータはiPhone XS（画面サイズ：2,436 x 1,125px）を利用した際のストロークに限定している。

円軌道による推定手法、楕円軌道による推定手法について中心位置変動量を全ストロークについて算出した。それをセッション毎、ユーザ毎に平均値を計算し「中心位置変動量ユーザ平均」とした。図3.1、3.2には垂直方向、水平方向の中心位置変動量の分布を示している。両方向共に円中心に比べて楕円中心の方が中心位置変動量が小さいことを確認した。

以上の検証から、楕円中心は円中心より安定した値を取っていることを確認した。よって楕円中心は円中心より、安定してMP関節位置を推定できている。

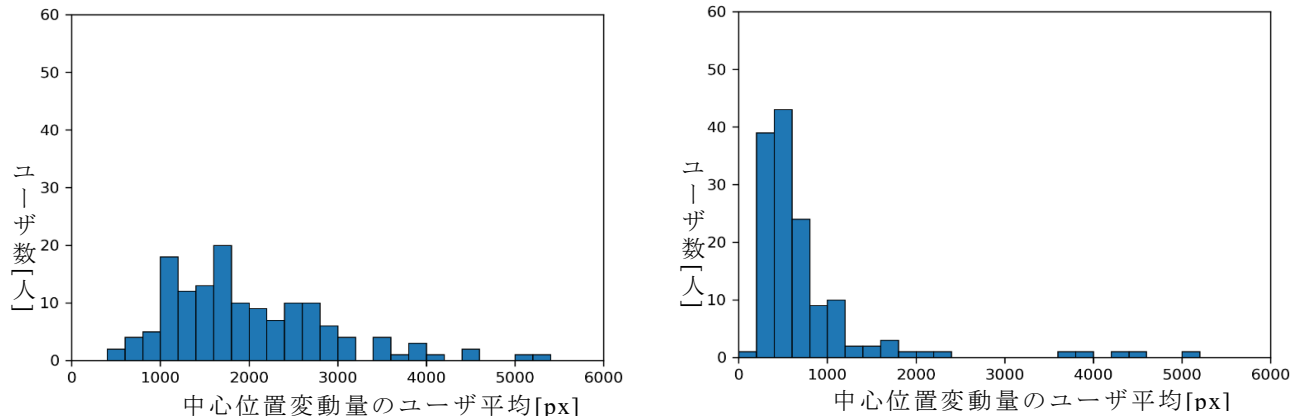


図 3.1 垂直方向ストロークの中心位置変動量の分布（左：円中心 右：楕円中心）

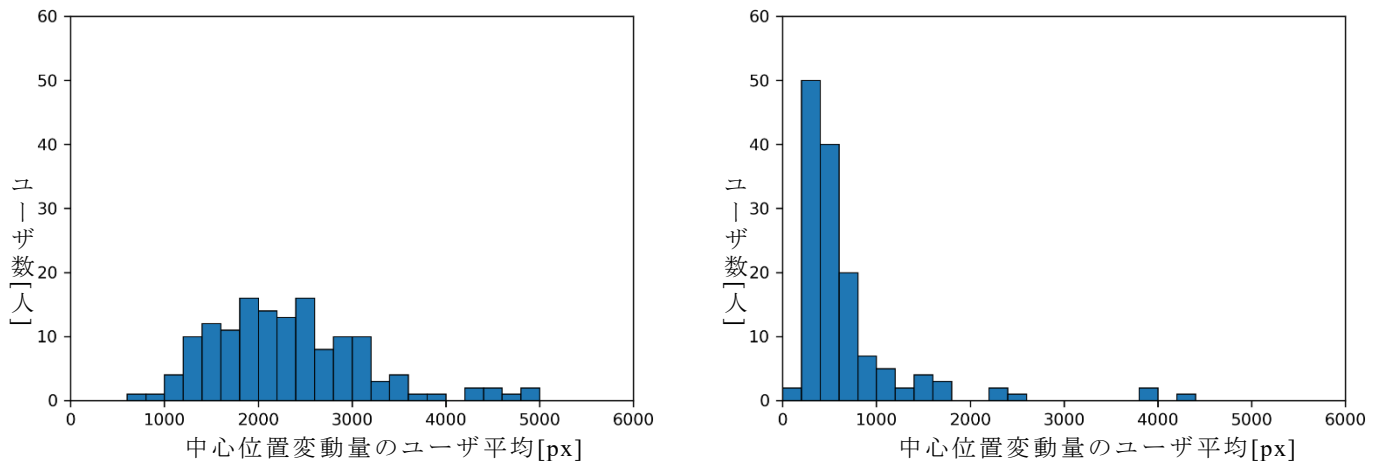


図 3.2 水平方向ストロークの中心位置変動量の分布（左：円中心 右：楕円中心）

4. 提案手法

本論文では、3.1 節にて示した楕円軌道による推定手法に基づく認証と、従来の円軌道による推定手法による認証とのアンサンブル手法を提案する。4.1 節にて推定した楕円に基づく新規特徴量を提案し、4.2 節ではアンサンブル手法について述べる。

4.1. 推定した楕円軌道に基づく新規特徴量

推定した楕円軌道に基づいて、表 4.1 に示す新たな特徴量を提案する。推定した楕円の位置、形状を表すパラメータの他、円による MP 関節位置推定に基づいた特徴量[8]を参考に、楕円の中心座標を極としたストロークの始点、終点の距離及び偏角を算出した。

なお、座標や距離の計算にあたってはスマートフォンの画面角左上を原点として、右方向を X 軸正方向、下方向を Y 軸正方向とした直交座標系を採用している。

4.2. 円による MP 関節位置推定に基づく認証とのアンサンブル

円による MP 関節位置推定に基づく認証と、楕円に

よる MP 関節位置推定に基づく認証では、それぞれ異なるストロークにおいて認証性能が高くなる傾向を観測した。このことから、両手法が捉えているタッチ特性には差異が存在する可能性が示唆される。そこで本研究では、2 つの手法による認証を組み合わせることで、精度向上を目指す。

以下の 2 つのモデル両方において認証を実施し、それぞれのモデルによるスコアアンサンブルを行う。

1. Frank 特徴量 25 種と、工藤ら[8]の提案した円推定に基づく 3 つの特徴量「MP 関節位置を中心とした軌跡円半径」、「MP 関節位置を極としたストローク開始地点の偏角」「MP 関節位置を極としたストローク終了地点の偏角」による認証（円モデル）。

表 4.1 楕円の推定による新規特徴量

No.	特徴量名	定義
1, 2	Center_x, Center_y	推定した楕円の中心 XY 座標*[px]
3, 4	Ver_axis, Hor_axis	推定楕円の傾き (Angle) を考慮した, 垂直方向／水平方向成分の軸長 [px]
5	Axis_ratio	軸の長さの比 (短軸の長さ／長軸の長さ)
6	Angle	推定した楕円の X 軸に対する傾き[rad]
7	Start_center_angle	楕円中心を極としたストローク開始地点の偏角[rad]
8	Stop_center_angle	楕円中心を極としたストローク終了地点の偏角[rad]
9	Center_angle_diff	ストローク開始地点と終了地点の偏角の差
10	Start_center_distance	楕円中心座標とストローク開始地点のユークリッド距離[px]
11	Stop_center_distance	楕円中心座標とストローク終了地点のユークリッド距離[px]
12	Stop_to_start_distance_ratio	中心座標との距離の比 (Start_center_distance／Stop_center_distance)

*:スマートフォンの画面角左上を原点として、右方向を X 軸正方向、下方向を Y 軸正方向とする直交座標系において算出

表 4.2 認証に使用する新規特徴量

ストローク方向	特徴量名
垂直	Angle, Start_center_angle, Stop_center_angle
水平	Hor_axis, Ver_axis, Angle, Start_center_angle, Stop_center_angle, Axis_ratio, Start_center_distance, Stop_center_distance, Stop_to_start_distance_ratio

2. Frank 特徴量 25 種と、本論文にて提案した楕円推定に基づく新規特徴量による認証 (楕円モデル)。ただし、認証には楕円モデル単体での検証¹において垂直方向のストローク、水平方向のストロークで最も精度が高かった表 4.2 に示す特徴量を用いる。

タッチベース認証では、ストローク特徴量から分類モデルにより本人確率 (スコア) が算出される。本手法では、円モデルおよび楕円モデルそれぞれが出力する本人確率をアンサンブルしたスコアを用いて認証を行い、セッション内の全ストロークを通して EER を算出する。

アンサンブルには平均および重み付き平均を用いる。重み付き平均の重みは、訓練データにおいて各ストロークで優位となったモデルの出現比率に基づいて決定する。

具体的には、訓練データを用いて円モデルおよび楕円モデルの学習器を構築し、各ストロークにおける両モデルのスコアを比較することで、モデルの選択比率を算出する。テスト時には、各ストロークについて両モデルのスコアを算出し、選択比率を用いて重み付き平均を計算する。最終的に、全ストロークのスコアから EER を算出する。

¹ 表 4.1 に示す各行ごとに、使用不使用を決定した特徴量の組み合わせについて網羅的に検証を実施。

5. 評価実験

本節では、提案手法のタッチベース認証における有効性を評価する実験手法について説明する。

5.1. データセット

タッチベース認証の分野では、複数の無償公開されているデータセットが存在する。今回はそのうち Frank らが公開したデータセット [11] (以下、TA データセット) と Geogiev らが公開したデータセット [7] (以下、CEP データセット)、3.2 節の検証にて使用した ECT データセットを使用する。これらのデータセットはデータ上に明確なセッション²の区切りが存在し、タッチセンサから取得した生のセンサデータが使用可能である。それぞれのデータセットにおいて、生のセンサデータに含まれるストロークのデータポイント座標から、3.1 節に示した手法によってストローク毎に円及び楕円を推定する。

5.1.1. タッチ特徴量の抽出

評価で使用するタッチ特徴量は、ベースラインとして表 2.1 に示す Frank 特徴量 [11]を採用する。なお、CEP データセットと ECT データセットからは「No.26 ストローク 50%地点のスクリーンに対する指の向き」、

² ユーザが与えられたタスクを完了するために行った時系列的に連続するストロークのまとまりを 1 セッションとする。

「No.27 デバイスの向き」を得ることができないため、それらを除外した 25 種類の特徴量でベースライン評価を行った。

また比較のため、4.2 節に示した円モデル、楕円モデル単体での評価も実施した。

5.1.2. 評価データセット構築

評価データセットの構築は、Georgiev らが採用した評価実験[12]に基づいて行う。Georgiev らはタッチベース認証の公開データセットのベンチマーク評価を行っており、本研究の先行研究である工藤ら[8]も同様の手法を採用している。

評価データは以下の手順で構築する。

まず、データセットに含まれる全ユーザから 1 ユーザを正例ユーザ（スマートフォン所有者本人）として選択し、残りのユーザを負例ユーザ（第三者）として扱う。

正例ユーザのストロークデータは取得時刻順に並び、全セッションの先頭 80%を正例訓練データ（PDtrain）、残り 20%を正例テストデータ（PDtest）とすることで、時系列を考慮した評価を行う。

負例データについては、負例ユーザをランダムに訓練用およびテスト用の 2 群に二等分し、それぞれの群から各ユーザ同数のストロークを抽出する。訓練用負例ユーザ群からは PDtrain と同数のストロークを含む負例訓練データ（NDtrain）を、テスト用負例ユーザ群からは PDtest と同数のストロークを含む負例テストデータ（NDtest）を構築する。なお、負例ユーザは個別には区別せず、単一の負例クラスとして扱う。また、テスト時には、負例ユーザが自身の操作データを用いて正例ユーザになりすますゼロエフォート攻撃を行うものと仮定する。

使用する 3 種類のデータセットは全て垂直方向のみを含むセッションと水平方向のみを含むセッションに分かれているため、データセット構築も垂直方向、水平方向で別々に実施する。なお、負例ユーザは個別には区別せず、単一の負例クラスとして扱う。また、テスト時には、負例ユーザが自身の操作データを用いて正例ユーザになりすますゼロエフォート攻撃を行うものと仮定する。

本研究では、評価に用いるデータセットの整合性および再現性を確保するため、以下の条件を満たすユーザのみを評価対象とした。

正例データセットはセッション単位で PDtrain および PDtest を構築するため、少なくとも 2 セッション以上のデータを有するユーザのみを採用した。また、オンラインで収集された CEP データセットについては、利き手の違いによる影響を排除するため、右手を利き手とするユーザのみを評価対象とした。

さらに、異なるデバイス間の混在が認証性能の評価に影響を与える[7]ため、各データセットにおいて使用ユーザ数が最も多いデバイスに限定して評価を行った。具体的には、CEP データセットでは iPhone 7, ECT データセットでは iPhone XS を対象とした。

なお、楕円の推定にあたってデータポイントを 5 点以上もつストロークのみ認証に使用する。

以上の条件を適用した結果、各データセットにおける評価対象の総数を表 5.1 に示す。

表 5.1 条件適用前後のユーザ数とストローク数

データ セット	方向	ユーザ数		ストローク数	
		処理前	処理後	処理前	処理後
TA	垂直	41	39	12,419	7,448
	水平	41	39	8,739	6,249
CEP	垂直	470	51	421,973	45,495
	水平	470	51	744,119	83,273
ECT	垂直	105	78	90,476	49,794
	水平	105	78	89,111	48,757

EER は認証における正例ユーザ、負例ユーザの組み合わせによって値にブレが生じる。そのため Georgiev ら[12]及び工藤ら[8]の評価と同様に、データセットに含まれるユーザのうち 1 ユーザが正例ユーザ、残りのユーザが負例ユーザとなる組み合わせのデータセットを全ユーザについて網羅的に構築、検証し、その平均 EER を評価結果として示す。また正例ユーザ毎の EER は、訓練用とテスト用の負例ユーザをランダムに選んで行った 10 回の検証の平均 EER を採用する。

5.2. 評価指標

誤認証率の評価指標には、認証システムの評価で一般的に使用されている EER (Equal Error Rate) を採用する。EER は、正例ユーザを誤って負例ユーザとして拒否する割合である FRR (False Rejection Rate) と負例ユーザを誤って正例ユーザとして受け入れる割合である FAR (False Acceptance Rate) が一致する時点での誤認証率を表す。タッチベース認証は、1 ストローク単位で実施する。セッションに含まれる全てのストロークについて認証を実施することで、セッション毎に EER を算出する。

5.3. 分類モデル

分類モデルには Random Forest (以下、RF) を採用する。これらは Georgiev らが実施した複数の分類モデルの性能評価において、複数の認証シナリオで安定的に高い性能を示した分類器の 1 つであり、工藤ら[8]も採用している。本実験は Python3.8.10 を使用して実施し、分類器の構築は scikit-learn0.24.0 と PyTorch1.7.0 を使用した。

RF のパラメータを表 5.2 に示す。これは工藤ら[8]の検

証と同様であり，記載していないパラメータはデフォルトの値を採用している．

表 5.2 分類モデルのパラメータ

モデル	パラメータ	値
RF	N estimators	100
	Max depth	20

6. 評価結果と考察

表 6.1 の各方向のモデル P2, P3 に提案手法の評価結果を示す．なお，各方向モデル B1 がベースライン，B2 が円モデル，P1 が楕円モデル単体による認証の評価である．

楕円モデル単体（P1）と円モデル（B2）の間には，統計的に有意差が認められなかった．一方で円モデルと楕円モデルのアンサンブル（P2, P3）により，全てのデータセットとストローク方向においてベースラインおよび各単体モデルと比較して統計的に有意な EER 改善を確認した．TA データセットでは両方向において平均によるアンサンブル（P2）が最良の性能を示した．CEP および ECT データセットでは，方向により平均（P2）または重み付き平均（P3）が最良となり，いずれのデータセットにおいても両方向で有意な改善を確認した．特に ECT データセットの水平方向においては，ベースラインと比較して 1.00% という最大の EER 改善を確認した．

また，平均（P2）と重み付き平均（P3）の間では TA データセットの垂直方向ストロークのみ統計的な有意差が認められ，他のデータセットにおいて有意差がなかった．

以上より，提案手法の平均（P2）と重み付き平均（P3）の間には差が見られないものの，アンサンブルによって単体で最も性能が良かったモデルとの有意な EER 改善を確認した．これは，円モデルと楕円モデルが異なる特性を持つ特徴量に基づいて認証を行っており，両者の誤りを相互に補完できたためと考えられる．

7. 分類器によるモデル選択の検討

6 節にて評価した平均化によるモデルアンサンブルでは，精度向上に限界がある．そこで両方のモデルではなく，より優れた認証を行うと推定されるモデルの片方の結果のみを採用することで，更なる精度の向上が期待される．本節では分類器を用いてモデルの選択を行う手法の検討及び評価を行う．

7.1. 分類器によるモデル選択

分類器によるモデル選択では，認証に用いた特徴量及び円モデル，楕円モデルによる認証にてそれぞれ算出される本人確率を分類器によって学習し，より精度

が高いと推定されるモデルを決定する．各ストロークに対して選択されたモデルの本人確率を用い，セッション内の全ストロークのスコアから EER を算出する．認証の流れを以下に示す．

まず，訓練データを用いて円モデルおよび楕円モデルの学習器を構築し，各学習器による本人確率（スコア）を算出する．次に，スコアおよび特徴量を入力として，適切なモデル（円または楕円）を選択するアンサンブル学習器を学習する．

テスト時には，各ストロークについて両モデルのスコアを算出し，アンサンブル学習器により選択されたモデルのスコアのみを採用する．最終的に，テストデータに含まれる全ストロークのスコアを用いて EER を算出する．

モデル選択では，選択のために分類器を使用する．本実験では Random Forest（RF）を用いた．RF のハイパーパラメータはユーザ毎に個別にチューニングを行った．チューニングには訓練用データのみを使用し，表 7.1 に示す 9 通りのパラメータ組み合わせを評価した．目的関数には Log Loss を用い，各ストロークから算出される Log Loss の平均値が最小となるパラメータを最適な設定として採用した．

表 7.1 分類モデルのパラメータ

モデル	パラメータ	値
RF	N estimators	10, 100, 200
	Max depth	5, 20, None

7.2. 評価結果と考察

モデル選択手法の評価結果を表 6.1 の各方向におけるモデル P4 に示す．なお，各方向の O はモデル選択において，ストローク毎に適切なモデルを選択できたと仮定した時の理想値である．

表 6.1 より，分類器によるモデル選択（P4）によりベースラインと比較して有意な EER 改善が確認できたものの，どのデータセットにおいても平均 EER では平均（P2），重み付き平均（P3）による認証に及ばなかった．

表 7.2 に，ECT データセットにおけるモデル選択の正答率を示す．モデル選択の正答率自体が十分に高いことから，現状では比率重み付き平均によるアンサンブルの方が安定して認証精度を向上させられる結果となった．しかし，単純な平均化による精度向上には限界があり，さらなる認証精度の改善を目指すためには，モデル選択の精度を向上させることが不可欠である．

8. おわりに

本研究では，タッチベース認証における誤認証率の改

善を目的として、楕円軌道を仮定した MP 関節位置推定手法を提案した．評価の結果、提案手法は従来の円軌道に基づく MP 関節位置推定と比較して、推定した中心座標の変動が小さく、より安定した推定が可能であることを確認した．

さらに、楕円軌道による MP 関節位置推定に基づく新たな特徴量を導入し、新規特徴量による認証の評価結果の分析から、従来手法と提案手法では有効となるタッチ特性が異なることが示唆された．

表 6.1 モデル単体とモデル選択の評価結果

方向	モデル	TA データセット EER (%)	CEP データセット EER (%)	ECT データセット EER (%)
垂直	B1:ベースライン(Frank[10])	14.54	14.91	13.93
	B2:ベースライン (円モデル[8])	14.28*	14.79*	13.81*
	P1:提案手法 (楕円モデル)	14.03*	14.86	13.70*
	P2: 提案手法 (円と楕円のアンサンブル：平均)	13.61* † ‡	14.65* † ‡	13.53* † ‡
	P3:提案手法 (円と楕円のアンサンブル：重み付き平均)	13.75* † ‡	14.65* † ‡	13.57* † ‡
	P4:提案手法 (円と楕円のアンサンブル学習 (RF))	14.10*	14.80	13.69*†
	O:参考 (理想的なモデル選択)	11.46	12.68	11.38
水平	B1:ベースライン(Frank[10])	11.97	15.91	14.86
	B2:ベースライン (円モデル[8])	11.29*	15.22*	13.99*
	P1:提案手法 (楕円モデル)	11.54*	15.68* †	14.41*
	P2: 提案手法 (円と楕円のアンサンブル：平均)	10.92* † ‡	15.19* ‡	13.89* † ‡
	P3:提案手法 (円と楕円のアンサンブル：重み付き平均)	11.01* † ‡	15.15* † ‡	13.86* † ‡
	P4:提案手法 (円と楕円のアンサンブル学習 (RF))	11.36*	15.28* ‡	13.97* ‡
	O:参考 (理想的なモデル選択)	8.10	12.70	11.19

* : $p < 0.05$, (各方向 B1 と B2,P1 から P4 間で対応のある両側 t 検定を実施)
† : $p < 0.05$ (各方向 B2 と P1 から P4 間で対応のある両側 t 検定を実施)
‡ : $p < 0.05$ (各方向 P1 と P2 から P4 間で対応のある両側 t 検定を実施)

表 7.2 モデル選択の正答率

方向	モデル	ECT データセット			
		EER (%)	円 比 率 (%)	楕 円 比 率 (%)	正 答 率 (%)
垂直	O:参考 (理想的なモデル選択)	11.37	53.33	46.67	70.41
	P4:提案手法 (円と楕円のアンサンブル学習 (RF))	13.69	61.98	38.02	
水平	O:参考 (理想的なモデル選択)	11.19	60.58	39.42	72.64
	P4:提案手法 (円と楕円のアンサンブル学習 (RF))	13.97	66.74	33.26	

これらの知見に基づき、従来手法と提案手法を組み合わせたアンサンブル認証を行った結果、 Random Forest による検証にて最大 1.00%の EER 改善を確認した．以上より、MP 関節位置推定の柔軟化および複数手法の統合が、タッチベース認証の性能向上に有効であることを示した．

参 考 文 献

[1] S. S. U. Hasan, A. Ghani, A. Daud, H. Akbar, and M. F. Khan, “A review on secure authentication mechanisms for mobile security,” Sensors, vol. 25, no. 3, Art. no. 700, 2025.

[2] Q. Abu Al-Haija and S. Al-Salameen, “Biometric authentication system on mobile environment: A review,” Computer Systems Science and Engineering, vol. 48, pp. 1–18, 2024.

[3] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1268-1293, 2015.

[4] A. Zaidi, C. Chong, Z. Jin, R. Parthiban, and A. Sadiq, "Touch-based continuous mobile device authentication: State-of-the-art," Journal of Network and Computer Applications, vol. 191, pp. 1-29, 2021.

[5] C. Shen, Y. Li, Y. Chen, X. Guan, and R. Maxion,

- "Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication," *IEEE Trans. Information Forensics and Security*, vol. 13, no. 1, pp. 48-62, 2017.
- [6] Z. Syed, J. Helmick, S. Banerjee, and B. Cukic, "Touch gesture-based authentication on mobile devices: The effects of user posture," *Journal of Systems and Software*, vol. 149, pp. 158-173, 2019.
- [7] M. Georgiev, S. Eberz, H. Turner, G. Lovisotto, and I. Martinovic, "Common Evaluation Pitfalls in Touch-Based Authentication Systems," *Proc. 2022 ACM onAsia Conference on Computer and Communications Security*, pp. 1049-1063, 2022.
- [8] 工藤,雅士, 高橋,翼, 越前,功, 山名,早人, "スマートフォンの把持方法に頑健な MP 関節位置に基づくタッチベース認証特微量の提案", *情報処理学会論文誌データベース (TOD)*, vol. 18, no. 2, pp. 32-46, 2025.
- [9] A. Mahfouz, T. Mahmoud, and A. Eldin, "A survey on behavioral biometric authentication on smartphones," *Journal of Information Security and Applications*, vol. 37, pp. 28-37, 2017.
- [10] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 1, pp. 136-148, 2013.
- [11] M. Georgiev, S. Eberz, and I. Martinovic, "Techniques for Continuous Touch-Based Authentication," *Information Security Practice and Experience*, vol. 13620, pp. 409-431, 2022.
- [12] M. Kudo, T. Takahashi, S. Ushiyama, and H. Yamana, "Fair and Robust Metric for Evaluating Touch-based Continuous Mobile Device Authentication," *Proc. 28th International Conference on Intelligent User Interfaces*, pp. 141-144, 2023.
- [13] P. Aaby, M. Giuffrida, W. Buchanan, and Z. Tan, "An omnidirectional approach to touch-based continuous authentication," *Computers and Security*, vol. 128, pp. 1-12, 2023.
- [14] Z. Sitov'a, J. Sed'enka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. Balagani, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 5, pp. 877-892, 2016.
- [15] M. Kudo, and H. Yamana, "Active Authentication on Smartphone using Touch Pressure," *Proc. 31st Annual ACM Symposium on User Interface Software and Technology*, pp. 96-98, 2018.
- [16] A. Fitzgibbon, M. Pilu, and R. B. Fisher, "Direct least square fitting of ellipses," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 21, no. 5, pp. 476-480, 1999.
- [17] M. Kudo, T. Takahashi, I. Echizen and H. Yamana, "eCommTouch: A Benchmark Dataset for Touch-based Continuous Mobile Device Authentication for e-Commerce," *2025 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 140-147, 2025.