Leap Motion とテンキーロックを組み合わせた 2 要素認証

真鍋 智紀[†1]　森山 優姫菜[‡2]　山名 早人[‡34]

†1 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
†2 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
†3 早稲田大学理工学術院 〒169-8555 東京都新宿区大久保 3-4-1
†4 国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2
E-mail: †{tomoki_manabe, ymoriyama, yamana}@yama.info.waseda.ac.jp

あらまし 近年，スマートフォンに指紋認証や顔認証の機能が実装されるなど，生体認証が身近になりつつある．生体認証は従来のパスワード入力に比べて手間が少なく，かつ，鍵となる生体情報の窃取が難しく安全であると考えられてきた．しかし，昨今では画像認識技術の進歩により生体情報が盗まれる危険性が高まっている．また，生体認証はパスワード入力に比べて認証精度が低いという問題もある．こうした生体認証の特徴を踏まえ，本研究ではパスワード方式に生体認証を組み合わせた 2 要素認証を提案する．提案手法では，パスワード入力の際の指の動く速さや手と指の骨の長さ，入力にかかる時間を特徴量として生体認証を行う．パスワード認証と生体認証を組み合わせ，安全性を高めることが本研究の目的である．被験者 21 名による実験の結果より，提案手法では 4 桁のパスワード入力を行う際の限られた時間で，99.13%の正解率で生体認証が可能であることを示した．

キーワード 生体認証，2 要素認証，機械学習

1. はじめに

近年，パスワード認証の脆弱性が指摘されている．パスワード漏洩による SNS のアカウント乗っ取りのような事例が増加する一方で,新たな認証方法として,生体情報を用いた認証システムが一般的になりつつある．昨今ではスマートフォンに指紋認証や虹彩認証，顔認証の機能が実装されるなど，生体認証の実用化が進んでいる．

生体認証は従来のパスワード認証に比べて手間が少なく，かつ個人の身体的特徴を認証に用いるため，鍵となる情報の盗用が難しく，利便性と安全性を同時に確保できると考えられていた．しかし，最近ではカメラや画像認識技術の進歩によって生体情報が盗まれてしまう危険性が高まっている．例えば，スマートフォンの指紋認証システムでは，タッチスクリーンに残った指紋から作成した偽造指紋によってロックを解除される危険がある[1]．生体情報はパスワードのように変更することができないため，一度盗まれてしまうと認証キーとしての再使用が困難である．さらに，生体認証はカメラや赤外線センサといった装置を使用するため，パスワード認証に比べて認証精度が低く，また精度が安定しないという問題もある．具体的には，同じ認証装置であっても，カメラや赤外線センサが日光や装置の汚れの影響を受け，精度が左右される場合がある．したがって，生体認証の分野ではこのような外乱の影響を減らすことに重点を置いた研究もなされている[2]．

上記の生体認証とパスワード入力の利点や欠点を踏まえ，従来のパスワード方式に生体認証を組み合わせた 2 要素認証によって安全性を高める取り組みがなされている.パスワード認証によって精度を確保しつつ，生体認証を組み合わせることで安全性の向上を図ることが狙いである．

本稿では Leap Motion[3]を用いた生体認証とパスワード認証を組み合わせた 2 要素認証を提案する．Leap Motion は手の位置や指の動きをトラッキングする赤外線 3D センサである．手や指の形状や動作には個人差があり，かつ手の動きには無数のパターンが存在する．このため，手の動きや形状を用いた認証は，生体認証の手法の一つとして注目されている．手の骨格や指の動きの特徴を用いた生体認証の既存研究では，誤り率 0.00333%の精度を達成した例がある[4]. しかし，[4]の手法では認証する際にセンサに 25 秒以上手をかざす必要があり，認証に長時間を要するのが問題であった．そこで，[4]の問題点である認証時間の長さを短縮することを本研究では目指す．具体的には，パスワード認証とパスワード認証中に得られる生体認証を組み合わせることで，パスワード認証が突破されても生体認証で侵入を防ぐ仕組みを構築する．本研究の貢献は，パスワード入力の際の短時間のみで得られる限られたデータ量で生体認証が可能であることを示した点である．

提案手法では，パスワード入力の際の手の動く速さや指骨と中手骨の長さ，入力にかかった時間を特徴量

として生体認証を行う．入力にかかった時間や指の動く速さといった情報は，短時間で得られるデータでありながら個人差があり，個人の識別に有用であると判断したため特徴量として採用した．また，本研究では生体認証に用いる特徴量として，骨の長さという不変の情報だけではなく，指の動く速さや入力にかかった時間という変動しうる情報を用いる．これは，変動しうる情報を特徴量として利用することにより，不変の情報のみを用いる生体認証より特徴量の盗難や再現を困難にすることができると考えたためである．具体的には，

・指骨と中手骨の長さ (19 本分)
・各指の幅 (5 本分)
・指の速さの最大値，最小値，平均値 (各 5 本分)
・入力にかかった時間

を特徴量として用い，判定器を構築する．

本論文の構成は以下の通りである．2 節で Leap Motion の概要を説明する．3 節で Leap Motion を用いた生体認証の研究について述べる．4 節で提案手法の概要の説明を行う．5 節で被験者実験とシステムの精度評価の結果，および結果の考察について説明する．最後に，6 節で本論文をまとめる．

2. Leap Motion の概要

Leap Motion は手の位置や指の動きをトラッキングする光学式 3D センサである．Leap Motion を用いたハンドトラッキングでは，まず赤外線 LED からトラッキング対象となる物体に赤外線を照射する．そして照射した赤外線の反射時間に基づいて手や指の深度情報を取得する．Leap Motion は，通常，水平な場所にセンサを垂直上向きにして設置する．検知可能範囲は接地面から垂直上方に向かう軸に対して中心角 150°，センサからの距離が約 2.5~60cm の空間で，0.01mm 単位で動作を認識できる[1]．両手と 10 本の指を独立に認識でき，ジェスチャ認識も可能だが，センサを机などに固定して使用する必要がある．

本研究では，Leap Motion を用いて手の骨の長さと指の幅，指の先端を基準とした指の速度ベクトルを計測した．本研究の環境では，Leap Motion は 1 秒間に 60 回の処理を行う．つまり，Leap Motion はユーザの手の情報を 1 秒間に 60 回計測し，計測結果を保存できる．本論文では，Leap Motion が手の情報を 1 回計測するのに要する時間をフレームという単位で表す．すなわち，本研究において，1 フレームは 1/60 秒である．

3. 関連研究

関連研究として，Leap Motion を用いた生体認証に関する研究について述べる．

図 2.1　Leap Motion

3.1. ジェスチャを用いた生体認証

Chan らは，パソコンのログイン時の認証と利用時のオンライン認証に関する研究として，ジェスチャを用いた生体認証システムを提案した[4]．Chan らの研究は 2 つのパートから構成される．第 1 のパートでは，ユーザがログイン認証のために Leap Motion を使う場面を想定した一時的な認証 (静的認証) を扱う．第 2 のパートでは，連続的な認証（オンライン認証）を扱う．オンライン認証を行う状況としては，例えばユーザがオンラインでウェブページを閲覧する間，同時に認証も行いつづけるといった場面を想定している．

静的認証では，ユーザはまず Leap Motion センサの上で両手を 25 秒間静止させる．そして手の幾何学的構造から，センサの認識した手が誰のものであるかを判別する．センサの認識した手がユーザ本人のものであると判断されると，ユーザは 1 本の指で円を描くよう要求される．両手を静止させ，次に円を描くという 2 つのセッションがデータの再現性を保証する．Chan らの静的認証システムでは，107 の特徴量が 1 秒につき 55 回ストアされる．ストアされる特徴量のうち 3 つは円を描くジェスチャに関する特徴量であり，残りは手や腕の幅と長さに加え，全ての指の中手骨と 3 つの指骨の幅と長さから成る身体的な特徴量である．ただし，親指については，中手骨の長さは 0 としている．ジェスチャの特性には円の半径とジェスチャにかかった時間，そして指の加速度が含まれる．被験者 16 名による実験の結果，ランダムフォレストアルゴリズムを用いた静的認証の分類精度 (1-EER) は 99.9667%を記録した．ここで，等価エラー率(Equal Error Rate, EER)とは，本人拒否率 (False Rejection Rate, FRR) と他人受け入れ率 (False Acceptance Rate, FAR)が等しくなる時の誤り率である．

---

1 https://developer.leapmotion.com/documentation/cpp/devguide/Leap_Overview.html

オンライン認証では，ユーザはジェスチャによってパソコンを操作できるアプリケーションを用いてカーソルやシークバーを操る．マウスカーソルを動かすために，ユーザは右手の人差し指を動かす．クリックをするには左手でキータップまたは右手でスクリーンタップのようなジェスチャをし，スクロールには左手で円を描くジェスチャあるいは右手でスワイプのジェスチャを行う．Chan らのオンライン認証システムでは 135 の特徴量を検出する．静的認証システムで取得していたものと同様の身体的な特徴量に加え，オンライン認証システムで用いるジェスチャの特徴量も記録される．記録される特徴量はそれぞれの手の方向，手と指の速さ，それぞれの手で掴んだりつまんだりする強さの他， オンライン認証システムで用いる 4 つのジェスチャに関連する様々な特徴量を含んでいる．被験者 10 名による実験の結果，オンライン認証システムでは，分類精度 (1-EER) の値は 98.3862%を記録した．

3.2. 手書きサインを用いた生体認証

Kamaishi らは，手書きサインによる生体認証システムを提案した[5][6]. Kamaishi らの目指すシステムは，手書きサインによるパスワードと，サインをする際の手から読み取ることのできる特徴量を組み合わせた生体認証である.パスワードと生体情報を用いることで，鍵の変更が可能な生体認証を実現できる．提案手法では，Leap Motion によって計測した指の形質と軌道，速さを個人の特定に利用している．[6]では，手書きサインを用いた生体認証の初期段階として，直線を描く指の単純な動きをトラッキングし，個人の特定に用いるシステムの実験を行っている．実験の結果，EER は 13.43%を得ている．

他の手書きサインによる生体認証システムの研究例としては，Xiao らの研究がある[7]．Xiao らは Leap Motion によってキャプチャされた生体データおよび行動データを用いたユーザ認証の効果を調べる実験を行った． Xiao らは，まずユーザの手の生体データとユーザがセンサの前でサインをしたときの行動データをもとに認証を行うシステムを試作した.そして 10 人の被験者から実験データを集め，実験結果を本人拒否率 (False Rejection Rate, FRR) ，他人受け入れ率(False Acceptance Rate, FAR) ，EER によって評価した．実験の結果, 手の生体データの面では平均 34.80%の EER を達成している．サインモーションの行動データでは平均 3.75%の EER を達成しており, [6]に比較して精度向上を達成している．

さらに，Nigam らは手書きサインと顔認証と組み合わせたシステムを提案している[8]．手書きサインと顔認証を組み合わせることで，手書きサインのみ，あるいは顔認証のみの場合と比較して認証の精度を上げることを目指している．実験では被験者 60 人のデータを用い，FAR が 1.43%の時に本人受け入れ率(Genuine Acceptance Rate, GAR)は 91.43%を記録している．

3.3. まとめ

[4]-[8]の論文について, それぞれの分類精度 (1-EER) の値をグラフ化したものを図 3.1 に示す．ただし，[8]の論文については EER の結果が記載されていなかったため, 参考として GAR の値をグラフ化した．また，[5][6]は，同じ著者による論文であるため，最新の論文のデータのみを載せる．

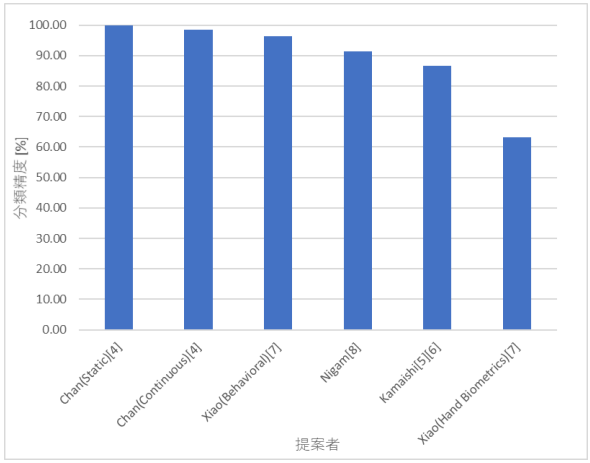

図 3.1 各論文の分類精度の比較

図 3.1 より, 全体では Chan らの静的認証および連続的な認証[4]の分類精度は，他の手法に比べて高いことがわかる． Chan らは，自分たちの手法が高い正確性を実現した理由として, Leap Motion とランダムフォレスト分類器による手の構造認識が非常に高精度であることを挙げている．また，Chan らの静的認証は，一時的な認証に比べて手の動きをより多く検知する連続的な認証よりもわずかに高い精度を達成している．すなわち，手の幾何学的な生体情報に比べ，ジェスチャやサインなどのもたらす情報は個人の識別に役立てるのが困難であると考えられる．

4. 提案手法

本節では提案手法である HPCA (Hand and Password Combination Authentication) について述べる．

本研究の第一の目的は，パスワード認証と生体認証を組み合わせることにより安全性を向上させることである.パスワード認証と生体認証を同時に行うことで，第三者が正しいパスワードを入力しても生体認証により侵入を阻止することができる．

本研究の第二の目的は，生体認証の速さを向上させることである.既存手法[4]は誤り率 0.00333%の精度を達成したが，認証に 25 秒以上を要するのが問題であった．本研究では実用性を考慮し，パスワード入力を終えるまでの短時間で得たデータのみで生体認証を行うことを目指した．

4.1. 概要

Leap Motion とテンキーロックによる 2 要素認証手法である HPCA (Hand and Password Combination Authentication)を提案する．HPCA で想定している認証手順を図 4.1 に示す．HPCA ではパスワード入力の際にキー入力をする人物の全ての中手骨と指骨の長さ，各指の幅と動く速さを Leap Motion によって取得する．パスワードの入力が完了すると，まずパスワードの正誤判定を行う．そして入力されたパスワードが正しい場合，パスワード入力の際に Leap Motion から得られたデータにより生体認証を行う．すなわち，パスワードの他に Leap Motion で取得した手の骨の長さ，各指の幅と動く速さを入力とし，パスワードが正しく，かつ入力した人物があらかじめ登録されたユーザである場合のみロックを解除する．

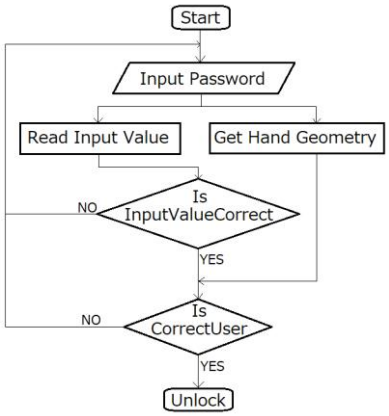

図 4.1　提案手法のフローチャート

4.2. 本研究の目的

HPCA を実用化する場面としては，マンションのロビー等における開錠を想定している．[4]の研究では 99.9667%という高い認識精度を実現しているが，認証に最低 25 秒かかるという問題がある．そこで，本研究では，認証にかかる時間を短縮させ，実用性を向上させることを目指す．具体的には，パスワードの入力開始から終了までの限られた時間で Leap Motion によってデータを取得し，生体認証を行うことのできるシステムを目指す．

短時間での認証を可能にするため，認証に利用する特徴量としては，パスワード入力の間に得られ，かつ個人差があると考えられるものを採用した．具体的には，手指の骨の長さや指の太さの他に，入力にかかった時間や指の動く速さの最大値，最小値，平均値を特徴量として用いた．また，認証の誤りには，登録されたユーザを第三者だと誤認する本人拒否 (False Rejection, FR) と，第三者を登録されたユーザだと誤認する他人受け入れ (False Acceptance, FA) が考えられる．マンションのロビー等では，開錠する権利のない人物の侵入を阻むことが肝要である．したがって本研究では，認証の誤りのうち，特に FA を減らすことに重点を置く．具体的には，できるだけ多くの他人のデータを分類器に学習させ，他人拒否率を高める．

4.3. 生体認証の方法

Leap Motion から得た情報を用いてどのように生体認証を行うかを述べる．生体認証には，表 4.1 に示す計 40 個の特徴量を用いる．

表 4.1　生体認証に用いる特徴量

特徴量の種類	概要
指骨と中手骨の長さ (19 本分)	各指の末節骨，中節骨，基節骨の長さ(mm) 親指以外の中手骨の長さ(mm)
各指の幅 (5 本分)	単位: mm
指の速さの最大値，最小値，平均値 (各 5 本分)	各指の先端の速さの最大値，最小値，平均値(mm/s)
入力にかかった時間	単位: 秒(s)

次に，Leap Motion を用いて得た特徴量をもとに，ランダムフォレスト分類器によってユーザが鍵を開ける権利のある人物か否かを判別する．分類には以下の方法をとる．まず，システムに利用者として登録されたユーザに対して，それぞれ分類器を用意する．開錠する際，それぞれの分類器にパスワード入力者の特徴量を入力として与える．各分類器は，与えられた特徴量が対応する本人のものなら「1」を，本人以外のものなら「0」を出力する．

ここで，パスワード入力時に入力者の 40 個の特徴量が n セット得られたとする．分類器は，n 個のデータセットについてそれぞれ本人かどうかの判定を行う．そして本人と判断されたデータセットの数が閾値 th 以上の場合のみ本人であると結論付け，最後に「1」を出力する．ここで，閾値 th は，パラメータ調整用のデータセットをもとに決定する．入力者が他人であると結論付けた場合の最後の出力は「0」である．すなわちパスワードが一致し，かつ利用者に対応する分類器の最後の出力が「1」で，他の分類器の最後の出力が「0」の場合のみ開錠する．

4.4. まとめ

本節では，提案手法である HPCA の概要と目的，生体認証の方法について述べた．本論文において提案するシステムは，Leap Motion とテンキーロックによる 2 要素認証である．本研究は，マンションのロビー等における開錠を実用化の場面として想定している．

本研究の目的は，パスワード入力に生体認証を組み合わせることでパスワード認証単体の場合より安全性を向上させることである．本研究の目的を達成するために，「短時間での認証」および「低い FAR」を実現するための方法を考えた．既存手法のうち，最も分類精

度の高い[4]の研究では，認証に用いるデータの取得に最低 25 秒もかかるという問題がある．

そこで本研究では，パスワード入力にかかる短い時間で十分得られ，かつ個人差があると考えられるデータを特徴量として採用し，認証時間の短縮を図った．具体的には，手指の骨の長さや指の太さの他に，入力にかかった時間や指の動く速さの最大値，最小値，平均値を特徴量として用いた．また，低い FAR を達成するためには多様な他人のデータを学習させることが必要であると考えた．そこで，第 5 章で述べる被験者実験により集めたデータのうち，本人以外の 20 人全員のデータを他人のデータとして分類器の学習に用いた．

5. 実験

5.1. データ収集

図 5.1 の装置を使い，生体認証に使う特徴量のデータを収集した．実験には 21 名の被験者 (男性 11 名，女性 10 名の大学生) が参加した．実験では，被験者は画面に表示された 4 桁のランダムな数字をテンキーで 21 回繰り返し入力する作業を 3 セット行った．

被験者がテンキーによる入力操作を行う間，被験者の全ての中手骨と指骨の長さ，各指の幅と動く速さを，テンキーの上部に設置した Leap Motion により計測した．被験者が入力に慣れるにつれて入力時間が短くなり，手の動きが安定することを考慮し，実験ではまず練習として入力作業を 2 セット行い，3 セット目のデータを実験に用いることとした．また，本研究では，入力のたびにテンキーの各数字キーの配置が変化するシステムを想定している．しかし，実験で使用したテンキーは数字キーの配置が固定されている．そこで，実験においては画面に表示される数字を無作為に決定することで，同じ数字を入力する場合でも押すキーの位置が変わる状況を再現した．

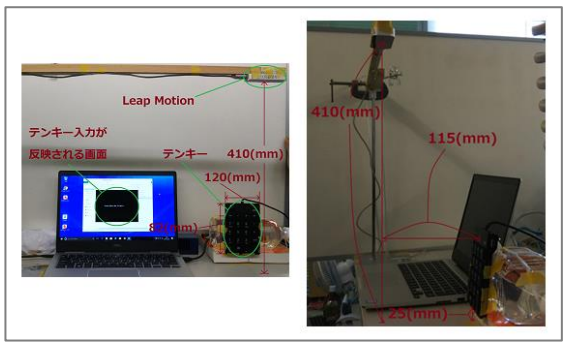

図 5.1　データ収集に用いた装置

5.2. Leap Motion の精度の計測

予備実験として，被験者実験により収集したデータを用いて Leap Motion の計測精度を確認した．検証には，被験者 21 名，1 人当たり 20 回のパスワード入力で得られた入力 420 回分のデータを用いた．

検証ではまず，各パスワード入力時に Leap Motion によって得られたデータのうち，指骨と中手骨の長さについて，最大値と最小値の差をそれぞれ計算した．ここで，i($1 \leq i \leq 21$)番目 の被験者のj($1 \leq j \leq 20$)回目のパスワード入力にかかった時間を$n_{i,j}$フレームとする．すなわち，i番目 の被験者のj回目のパスワード入力において，Leap Motion は指骨と中手骨の長さをそれぞれ$n_{i,j}$回計測したことになる．2 節で述べた通り，Leap Motion は 0.01mm 単位で手の動作を認識できるとされている．そこで，本実験ではパスワード入力中に計測した$n_{i,j}$回分の指骨または中手骨の長さのうち，最大値と最小値の差をi番目の被験者のj回目のパスワード入力における計測誤差と定義した．そして，指骨と中手骨の長さそれぞれについて計測誤差が 0.01mm より大きくなった回数を各被験者，各パスワード入力のデータから算出した．指骨と中手骨の総数は片手につき 19 本であるため，Leap Motion はパスワード入力 420 回で指骨と中手骨の長さをそれぞれ 420 回ずつ，合計 7,980 回計測したことになる．

検証の結果，7,980 回の計測のうち，指骨または中手骨の長さの計測誤差が 0.01mm より大きくなった回数は 1,125 回で，0.01mm より大きな計測誤差の発生した割合は 14.10%であった．0.01mm より大きな計測誤差について，計測誤差の大きさと計測誤差の発生した割合の関係を図 5.2 に示す．

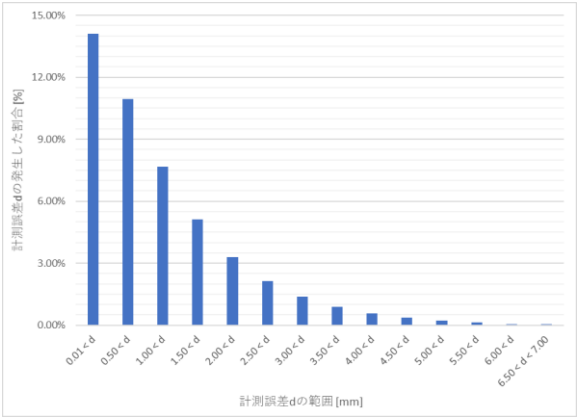

図 5.2　計測誤差の大きさと計測誤差の発生した割合の関係

ここで，Leap Motion がパスワード入力中に計測した指骨と中手骨の長さが生体認証の特徴量として有用かどうかを改めて考える．まず，成人の指骨と中手骨の長さはいずれも数十ミリ程度である．そして，Leap Motion の精度検証の結果より，パスワード入力における計測誤差が 0.01mm 以下となる割合は 85.90%である．また，計測誤差は最大で 7mm 未満である．さらに，図 5.2 より，例えば計測誤差が 1mm 以下の割合は 92.33%となる．したがって，パスワード入力中のユーザの手

に対する Leap Motion の計測結果は，生体認証の特徴量として利用可能であると考えられる．

5.3. システムの評価

以下では，分類器の分類精度を検証する．

5.3.1. 評価指標

システムの評価指標として，FRR，FAR，誤り率 (Error Rate: ER) を算出した．ここで，

nTrue: テストに用いた本人のテストデータの数
nFalse: テストに用いた他人のテストデータの数
nFR: テストにおいて生じた FR の数
nFA: テストにおいて生じた FA の数
とすると，FRR, FAR, ER は次のように表される．

$$\mathrm{FRR} = \frac{\mathrm{nFR}}{\mathrm{nTrue}} \quad (式\ 5.1)$$

$$\mathrm{FAR} = \frac{\mathrm{nFA}}{\mathrm{nFalse}} \quad (式\ 5.2)$$

$$\mathrm{ER} = \frac{\mathrm{nFR}+\mathrm{nFA}}{\mathrm{nTrue}+\mathrm{nFalse}} \quad (式\ 5.3)$$

また，本研究の精度評価においては，分類精度を 1-ER の百分率 (%) で表すものとする．

5.3.2. データセット

学習およびテストに用いるデータセットは，5.1 項で説明した通り，被験者実験の 3 回目で得られたデータセットを用いる．各データセットの特徴量は，以下に示す 40 の特徴量から構成される．

・指骨と中手骨の長さ (19 本分)
・各指の幅 (5 本分)
・指の速さの最大値，最小値，平均値 (各 5 本分)
・入力にかかった時間

ここで，被験者実験において，4 桁のパスワードを入力しエンターキーを押した瞬間をパスワードの入力終了および次のパスワードの入力開始と定義する．ある 1 回のパスワード入力において，入力開始から終了まで n フレーム（1 フレームは 1/60 秒）かかったとすると，1 回のパスワード入力に対してデータセットは n 個生成される．$i(1 \le i \le n)$番目のデータセットに含まれる特徴量のうち，手指の骨の長さと各指の幅は，i フレーム目において得られたデータである．一方，i番目のデータセットに含まれる特徴量のうち，指の速さの最大値, 最小値, 平均値および入力にかかった時間は，パスワード入力が終了してから計算されたものである．

5.3.3. 学習

決定木を n (n=1, 2, …, 200) 個もつランダムフォレスト分類器を構築した. 学習に用いるデータセットは，本人のデータセット 100 セットおよび 19 人の他者のデータセット合計 1900 セット（一人 100 セット×19 人）から成る．なお，他者のデータのうち残り 1 人分はテストデータとして用いるため，学習データには含めていない．学習用のデータセットは，各人のパスワード入力 20 回分のデータそれぞれについて，得られたデータのうち最初から 5 フレーム分ずつを抽出し，1 人分のデータセットとした．

5.3.4. テスト

決定木を n (n=1, 2, …, 200) 個もつランダムフォレスト分類器 21 人分について，出力のエラー数を確かめた．テストに用いるデータセットは学習データに含めなかった本人のデータセットおよび学習データに含めなかった他者 1 人のデータセットから成る．テストデータセットの総数は，本人のデータセットを 70 セット， 他者のデータセット 70*20 セットずつ計 1470 セットとした．

実験において，被験者が 4 桁のパスワード入力にかかった時間の最小値は 1.22 秒(>73 フレーム)であった．つまり，データセット 70 セット分のデータ量は，1 回のパスワード入力中に十分取得できるデータ量である．本人のデータセットは，パスワード入力 1 回分のデータから最初の 70 フレーム分を抽出したものである．一方，他者のデータセットはパスワード入力 20 回分のデータからそれぞれ最初の 70 フレーム分を抽出した．

また, 検証の妥当性を確認するため, 学習およびテストでは以下の方法を取り入れた．まず，本人のデータセットについては，パスワード入力 21 回分のデータのうち 1 つをテスト用，残りを学習用とし，21 分割交差検証を行った．テストにおいて本人データをパスワード入力 1 回分から抽出したのは, 21 分割交差検証により最終的にパスワード入力 21 回分のデータについてテストを行うことができるためである．また，他者のデータセットについても, 20 人分のうち 1 人分をテスト用, 残りを学習用とし, 21 分割交差検証を行った．

5.4. 各特徴量の重要度の評価

学習およびテストで用いた各特徴量が分類に与える影響の大きさを調べた．まず，評価実験に用いた特徴量のうち, $i(1 \le i \le 40)$番目の特徴量を除いた 39 個の特徴量を用いて，特徴量 40 個の場合の評価実験と同じ手順で学習およびテストを行う．特徴量 40 個による評価実験で求めた分類精度の最大値を A, i番目の特徴量を除いた場合の分類精度を A_i[%]とするとき，i番目の特徴量の重要度を以下のように定義する．

$$A - A_i[\%] \quad (式\ 5.4)$$

式 5.4 より，重要度の値が大きいほど分類精度の向上に寄与していると考えられる．

5.5. 結果

本節では, 各特徴量の重要度の評価結果から実際に利用する特徴量を厳選し，システムを評価する．

5.5.1. 各特徴量の重要度の評価結果

全 40 種の特徴量の重要度を図 5.3 に示す．また，特徴量の種類ごとに，重要度の値が正になった数と負になった数を表 5.1 にまとめる．なお，本研究では，親指の骨を先端から順に末節骨 (Distal)，中節骨 (Intermediate)，基節骨 (Proximal) とし，中手骨 (Metacarpal) の長さは 0 としている．

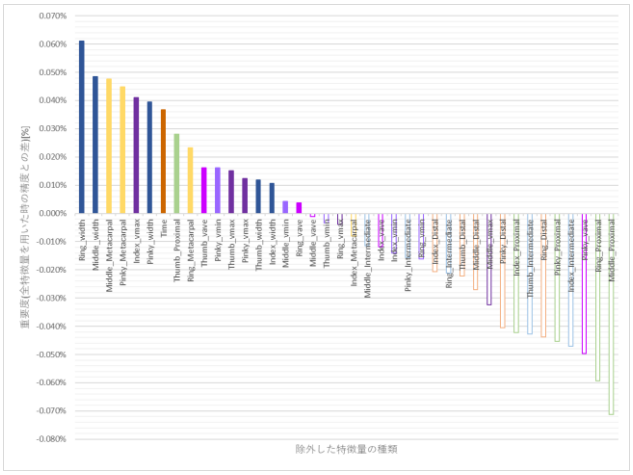

図 5.3　各特徴量の重要度

表 5.1　特徴量の種類と重要度の関係

特徴量の種類		重要度が正/負となった特徴量の数	
		正	負
中手骨の長さ (Metacarpal)		3	1
基節骨の長さ (Proximal)		1	4
中節骨の長さ (Intermediate)		0	5
末節骨の長さ (Distal)		0	5
指の幅 (Width)		5	0
指の速さ	最大値 (Vmax)	3	2
	最小値 (Vmin)	2	3
	平均値 (Vave)	2	3
入力にかかった時間 (Time)		1	0
合計		17	23

図 5.3，表 5.1 より，指の幅の重要度が 5 つ全て正となった．また，中手骨の長さの重要度は 4 つのうち 3 つが正である．しかし，基節骨の長さの重要度は 5 つのうち 4 つが負であり，中節骨と末節骨の重要度はすべて負である．ここで，図 5.4 に示すように，中手骨と指骨の長さは一般に，末節骨<中節骨<基節骨<中節骨となる．すなわち，指骨と中手骨のうち，長い骨ほど重要度が高いと言える．5.2 項の Leap Motion の計測精度の検証結果を踏まえると，長い骨ほど重要度が高い理由としては，長い骨ほど計測誤差の影響を受けにくいことが考えられる．また，指の速さに関する特徴量の重要度は全体の半分が正となった．そして，時間の重要度は全特徴量 40 個中 7 番目に高い．以上より，指の速さや入力にかかった時間といった動的な特徴量は，分類に一定以上寄与していると言える．

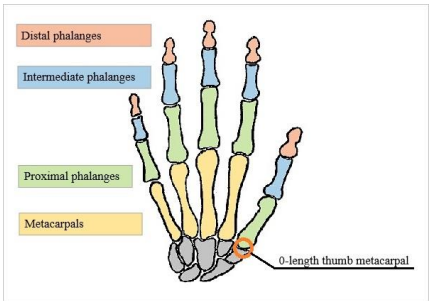

図 5.4　指骨と中手骨 ([2]を元にトレース)

5.5.2. 各特徴量の重要度を踏まえた評価実験

各特徴量の重要度の評価結果を踏まえ，5.3 項の実験で用いたデータセットから末節骨と中節骨の特徴量を除外し，5.3 項と同様の手順で再度評価実験を行った．新しいデータセットに含まれる 30 個の特徴量の内訳を表 5.2 に示す．

表 5.2　追加実験で用いた特徴量

特徴量の種類	概要
指骨と中手骨の長さ(9 本分)	各指の基節骨の長さ(mm) 親指以外の中手骨の長さ(mm)
各指の幅 (5 本分)	単位: mm
指の速さの最大値，最小値，平均値 (各 5 本分)	各指の先端の速さの最大値，最小値，平均値 (mm/s)
入力にかかった時間	単位: 秒(s)

評価実験に用いたデータセットに含まれる特徴量について，全ての指骨の長さを含む場合(P)と末節骨と中節骨の長さを含まない場合(Q)の分類精度の最大値，および分類精度が最大となったときの FRR, FAR を表 5.3 にまとめる．表 5.3 より，特徴量から末節骨と中節骨を除くと FRR は 1.33%増加することがわかる．しかし，特徴量から末節骨と中節骨を除くと FAR は 0.18%減少し，分類精度は 0.10%向上している．

表 5.3　特徴量の変更による精度と誤り率の変化

特徴量	分類精度 (1-ER) [%]	FRR [%]	FAR [%]
変更前 (P)	99.03%	8.99%	0.57%
変更後 (Q)	99.13%	10.32%	0.39%
Q-P	0.10%	1.33%	-0.18%

5.6. 考察

4.2 項で述べたように，本研究では第三者の侵入を防ぐことに重点を置いている．そこで，実用性と安全性の観点から，FRR および FAR について考察する．

---

2 https://developer.leapmotion.com/documentation/cpp/devguide/Leap_Overview.html

表 5.3 より，特徴量から末節骨と中節骨を除くと FRR は 8.99%から 10.32%に増加している．しかし，ここで 1 回の入力において本人拒否の発生する確率が 10.32%とすると，n 回連続で本人拒否が発生する確率は，

$$(0.1032)^n \quad (式\ 5.5)$$

と表される．よって 2 回連続で拒否される確率は 1.07%であり，3 回連続では 0.11%となる．すなわち，FRR が 10.32%であれば，本人拒否が起きても何度か入力し直すことで開錠することが十分可能であると考えられる．一方， FAR については，1 回の入力で他人受け入れの発生する確率を p%とすると，第三者が正しいパスワードを n 回入力した時，n 回連続で拒否される確率は，

$$(1-p)^n \quad (式\ 5.6)$$

となる．表 5.3，式 5.6 より，入力回数と他人拒否率の関係は図 5.9 のようになる．

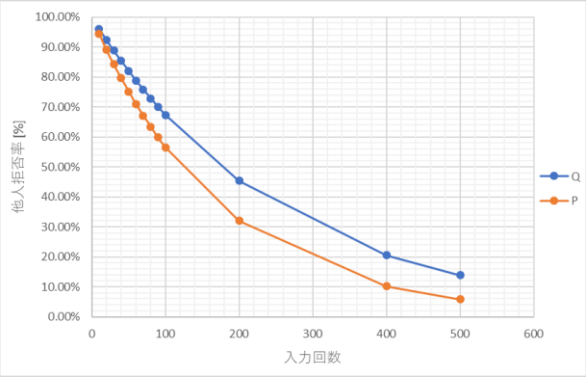

図 5.9　入力回数と他人拒否率の関係

図 5.9 より，第三者が正しいパスワードを 100 回入力したとき，鍵を突破されてしまう確率は P の場合 43.43%，Q の場合 32.66%となる．したがって，P, Q いずれの場合も，侵入される危険性は十分にあると言える．しかし，第三者が正しいパスワードを 100 回入力したとき， Q の場合は P の場合に比べて鍵を突破される確率の値が 10.77%小さく，より安全であると言える．以上より，本人が開錠できるという実用性を確保しつつより安全性を高めるには FR を多少犠牲にしてでも FA を減らすことが求められる．

6. おわりに

本稿では，まず Leap Motion を用いた生体認証の先行研究について述べた．Leap Motion を用いた生体認証では，[4]のように静的認証において 99%以上の認識精度を実現している例もあり，認証システムとして使用できる可能性は十分にある．しかし，Leap Motion の上に手を 25 秒以上かざす必要があり，認証に長い時間を要することが課題であった．

本研究では，パスワードを入力する間に Leap Motion から得られたデータをもとに生体認証を行うことを目指した．実験では，短時間で得られるデータで認証が行えるかどうかを確かめた．結果として，パスワード入力における限られた時間で得られるデータ量でも 99.13%の精度で認証可能であることを示した．

今後は引き続き Leap Motion を用いた生体認証について調査を進めつつ，FAR の低下に重点を置いて認証手法を改良していく．

参　考　文　献

[1] Chaos Computer Club breaks Apple TouchID – Chaos Computer Club, http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid, last access: 2018/1/2.

[2] 河原英喜，広野淳之，中元栄次，遠藤淳平，森康洋: “外乱光に対応した高速・高精度顔認証センサ”, パナソニック電工技報 Vol.57 No.2 特集「情報機器関連技術」, 2009.

[3] Leap Motion – LEAP MOTION, Inc. https://www.leapmotion.com/, last access: 2018/1/2.

[4] Alexander Chan, Tzipora Halevi and Nasir Memon: “Leap motion controller for authentication via hand geometry and gestures”, LNCS (including subseries LNAI and LNB) vol.9190, pp.13-22, 2015.

[5] Satoshi Kamaishi and Ryuya Uda: “Biometric authentication by handwriting Using Leap Motion”, Proc. of the 10th Int'l Conf. on Ubiquitous Information Management and Communication, Article No. a36, 2016.

[6] Satoshi Kamaishi and Ryuya Uda: “Biometric authentication by handwriting with single direction using self-organizing maps”, Proc. of the 11th Int'l Conf. on Ubiquitous Information Management and Communication, Article No.106, 2017.

[7] Grady Xiao, Mariofanna Milanova and Mengjun Xie: “Secure behavioral biometric authentication with Leap Motion”, Proc. of IEEE 4th ISDFS 2016, Article No.7473528, 2016.

[8] Ishan Nigam, Mayank Vatsa and Richa Singh: “Leap signature recognition using HOOF and HOT features”, Proc. of 2014 IEEE Int'l Conf. on Image Processing, pp.5012-5016, 2014.

[9] Kohonen T. “Self-organizing formation of topologically correct feature maps.” *Biol Cybern 43*, pp.59-69, 1982.

[10] 杉山将: “イラストで学ぶ機械学習 -最小二乗法による識別モデル学習を中心に”, 講談社, 2014.