スマートフォンのフリック入力方式の特徴に着目した継続認証手法の提案

伊藤駿吾 [1,a)]　　白石陽 [2,b)]

近年，Facebook や Twitter などの SNS が普及しており，スマートフォンのアプリケーションからこれらのサービスを利用することで簡単に情報を発信したり多くの人とコミュニケーションを取ることが可能となった．これらのアプリケーションの多くは一度ログインすると意図的にログアウトしない限りログイン状態を保持するため，スマートフォンのロックを解除されると誰でもアクセス可能な状態になってしまう．特にテキスト入力動作時はコミュニケーションだけでなく個人情報などの重要な情報を入力することがあるため，テキスト入力中の本人性の保証が重要であると考える．そこで，本研究ではスマートフォンのテキスト入力時のユーザの入力動作に着目し，スマートフォンを操作しているユーザが特別な操作を行うことなく継続的に本人性を保証することを目的とする．提案手法では，多くの日本人がスマートフォンで日本語を入力する際に利用しているフリック入力方式の特徴に着目し，母音の種類ごとに設定されているタップ動作と 4 方向のフリック動作の合計 5 種類の識別器を作成する．提案手法では本人の入力動作のデータを正常なデータ，他人の入力動作のデータを異常なデータとみなし，異常検知手法の一つである OCSVM (One Class Support Vector Machine) によって本人または他人の判定を行う．また，本稿では提案手法に有効な特徴を検討するための実験として複数の特徴パターンを作成し，認証精度の比較を行った．本実験では，まず 6 名の被験者を対象に 3 種類の文章を入力した際のデータを収集した．そして，ある被験者を本人とした際に 3 種類中 2 種類の文章を学習データ，残りの 1 種類の文章を認証データとして認証精度を求めた．この処理を全ての文章が認証データとなり，かつ，全ての被験者が本人となるよう繰り返し行い，その平均値を求めた．その結果，最も認証精度が高かった特徴パターンについてタップ動作，各方向へのフリック動作の全てにおいて 9 割以上の精度が得られた．

1. はじめに

近年，Facebook や Twitter などの SNS が普及しており，スマートフォンのアプリケーションからこれらのサービスを利用することで簡単に情報を発信したり多くの人とコミュニケーションを取ることが可能となった．一方で，これらのアプリケーションの多くは一度ログインすると意図的にログアウトしない限りログイン状態を保持するため，スマートフォンのロックを解除されると誰でもアクセス可能な状態になってしまう．

スマートフォンのロック解除に用いられている認証技術として，PIN やパスワードを用いた知識認証，指紋や虹彩などの身体的特徴を用いた生体認証が利用されている．知識認証ではユーザがパスワードを覚える必要があり，誕生日のような単純なパスワードを使用するとパスワードを破られる危険性が上がり，複雑なパスワードを使用するとパスワードを破られる危険性は下がるが，パスワードを覚えにくく，ユーザの負担が大きくなるトレードオフがある．また，近年普及している指紋を利用した生体認証では認証時にパスワードを入力するよりも認証のために必要な操作が少なく，負担が小さいため簡単に利用できる．しかし，本人の指紋を模した人工指による指紋で認証を行えることを示唆した研究が報告されている[1]．指紋のような身体的特徴は変更することが困難であるため，一度模倣されると作成された人工指を用いて認証が行われる恐れがある．さらにこれらの認証方式共通の問題点として，認証はロック解除時に一度しか行われず，ロック解除後は継続的に本人性が保証されない．そのため，スマートフォンの持ち主がアプリケーションにログインした後，悪意のあるユーザがスマートフォンを盗み，ロックを解除することでログイン済みのアプリケーションにアクセスする恐れがある．

この問題を解決する方法として，スマートフォン操作時の行動特徴を利用した継続認証に関する研究が盛んに行われている[2-5]．これらの研究ではスマートフォン操作時の指の移動の軌跡，端末に搭載されている加速度，角速度，地磁気センサなどを利用し，Web 上のドキュメント閲覧，テキスト入力など様々な端末操作時の動作から特徴を抽出し，機械学習による本人または他人の判定を行っている．

また，スマートフォンは様々な用途で使用されているが，テキスト入力は SNS やメールなどのコミュニケーション以外にもパスワードや PIN の入力，文書作成など多くの場面で利用され，重要な情報を入力することがある．そのため，特にテキスト入力中の本人性の保証が重要であると考えられ，テキスト入力動作に着目した研究も盛んに行われている[6-12]．これまでに行われているテキスト入力動作に着目した認証に関する研究は，大きく分けて定型文による認証と非定型文による認証の二つに分けられる．定型文による認証では，学習に使用する文字列と同じ文字列による認証を行うことで，高精度な認証を実現し，主にパスワードや PIN による知識認証と行動特徴による認証を組み合わせて 2 要素認証を行うことでより安全な認証を行う研究[6-8]が行われている．一方，非定型文による認証では学習に使用する文字列とは異なる任意の文字列の入力動作に基づいて認証を行うことが可能となり，テキストを入力する際に継続的な認証を行う研究が行われている[9-12]．そこで，本研究ではスマートフォンでのテキスト入力動作に着

1 公立はこだて未来大学大学院システム情報科学研究科
Graduate School of Systems Information Science, Future University Hakodate
2 公立はこだて未来大学システム情報科学部
School of Systems Information Science, Future University Hakodate
a) g2116002@fun.ac.jp
b) siraisi@fun.ac.jp

©2017 Information Processing Society of Japan

目し，テキスト入力中にユーザが特別な操作を行うことなく継続的に認証を行う手法を提案する．提案手法では多くの日本人が日常的に利用しているフリック入力の動作に着目し，任意の文章を入力した際に，本人による入力か他人による入力かの判定を行う．

本研究により以下の貢献が期待される．

- スマートフォンのロック解除後も継続的に本人性を保証する．
- スマートフォンでのテキスト入力中に，ユーザが特別な操作を行うことなく本人性を保証する．
- パスワードなどの知識と入力動作の特徴を組み合わせて 2 要素認証を可能にする．

以下，2 章では本研究の関連研究としてテキスト入力動作に着目した行動特徴による認証手法に関する研究について述べる．3 章では提案手法として特徴抽出の方法，本人の学習データから認証を行う方法について述べる．4 章では提案手法の有効性を評価するための実験と考察について述べる．最後に 5 章では本稿のまとめを述べる．

2. 関連研究

本研究ではスマートフォンのテキスト入力時の動作に着目した継続的に個人認証を行う手法を提案する．そこで，非定型文を入力した際の動作を利用した行動特徴による継続認証手法に関する研究について述べる．

2.1 ジェスチャキーボードによる入力を対象とした継続認証

Burgbacher ら[9]はジェスチャタイピングによるテキスト入力時の動作から特徴を抽出し，SVM(Support Vector Machine)による本人または他人の分類を行うことで個人認証を行っている．ジェスチャタイピングとは，連続的な動きで単語内に含まれる全ての文字のキーを指でスライドさせて入力する方式である．この方式ではある文字列を入力する際に，一文字目のキーをタップした後，指を画面から離さずにそのまま次の文字のキーに向かって指をスライドさせる．以降同様の操作を繰り返し，最後のキーまでスライドした後に画面から指を離すと，連続して入力されたキーの系列を一つの文字列として認識する．この手法では，ある文字列を入力した際の画面上の指の動きの軌跡を一つのシーケンスとしたとき，ある文字のキーから次の文字のキーまでの軌跡をサブシーケンスとして分解し，それぞれのサブシーケンスから特徴を抽出しており，学習に使用する文字列と同じ文字列を入力した場合において高精度な認証を行っている．

しかし，サブシーケンスから特徴を抽出する場合，入力された文字列から得られる連続した二文字の組み合わせの数だけ識別器を作成する必要がある．そのため，学習を行うために必要なデータ量を日常的に入力している文章から得ることが難しく，学習用の文字列と認証用の文字列が異なる場合は認証を行うことができない．したがって，この手法はログイン時の認証には有効だが，テキスト入力中に継続的な認証を行うことは困難であると考えられる．

2.2 ソフトウェアキーボードによる入力を対象とした継続認証

テキスト入力中に継続的な認証を行う手法として，Feng ら[10]は英語テキストの統計分布に基づいて選ばれた，最も頻繁に使用される 40 種類のキーの組み合わせのみから特徴を抽出し，学習することで，スマートフォンのロック解除後でもテキスト入力時の継続認証を可能とした．しかし, 認証に利用する分類アルゴリズムとして Random Forest や C4.5 決定木を使用し, 学習データに本人または他人のラベルを与えて学習しているため，他人の入力動作のデータがなければ全て本人として分類されてしまう．

一方，Hao ら[11]は本人のテキスト入力データのみを学習データとして識別器を作成し，継続的な認証を行う手法を提案している．この手法では識別器を作成する際に入力された文字列においてどのキーをタップしたか判定し，一文字ずつ分解して，キーごとに識別器を作成する．そのため，学習時と認証時に異なる文字列を入力しても認証が可能となり，継続認証に応用可能であると考えられる．さらに識別器を作成する際に，異常検知手法の一つである One Class Support Vector Machine（以下，OCSVM）によって，本人の入力動作のデータを正常なデータ，他人の入力動作のデータを異常なデータとして扱うことで，本人のみの入力動作を学習し, テキスト入力時の継続認証を可能とした．

しかし，これらの手法ではタップ動作からしか特徴を抽出できず，本研究で想定しているフリック入力のように画面上で指が移動する場合の特徴を考慮できない．

2.3 フリック動作による入力を対象とした継続認証

泉ら[12]は日本語入力において多くの日本人が利用しているフリック入力から，入力されたひらがなごとに識別器を作成することで，任意の文字列を入力した際の動作から個人認証を行う手法を提案している．しかし，この手法では予備実験として 300 字程度の文章を入力したところ，各文字の出現回数が最も多い文字でも 15 サンプル程度しか特徴ベクトルが得られなかった．さらに出現回数が少ない文字も存在することから，全てのひらがなに対して識別器を作成するために必要なサンプルを得るためには大量の文章を入力する必要があるため，学習コストが大きいという問題がある．

3. 提案手法

3.1 研究目的とアプローチ

本研究ではテキスト入力動作として，多くの日本人が利用しているフリック入力方式に着目する．フリック入力方式とは「あ」から「わ」まで，あ段が書かれたキーに対して，母音が「あ」のときはタップ動作，その他の母音のと

©2017 Information Processing Society of Japan

きは上下左右の各方向へフリック動作を行うことで文字を入力する方式である．また，フリック入力方式ではひらがな一文字に対して一つのキーとタップ動作またはフリック動作の組み合わせが割り当てられている．そのため，文献[11,12]のように文字ごとに特徴を抽出し，識別器を作成するとひらがなだけで 46 種類の識別器が必要となり，全ての文字で認証を行うために必要な学習データのサンプルを収集するコストが大きい．そこで，本研究ではフリック入力方式によってテキストを入力することを想定し，学習コストを抑えた上でフリック入力の動作からユーザが特別な操作を行うことなく継続的に本人性を保証することを目的とする．

この目的を達成するために，本研究ではフリック入力方式の特徴であるタップ動作と上下左右方向へのフリック動作に着目する．これらの動作は母音ごとに設定されているため，合計 5 種類の動作しか存在しない．そこで，入力された日本語の文字を母音の種類別に分類し，母音の種類ごとに入力動作の特徴を学習させることで，必要な識別器の種類を 5 種類まで削減し，学習コストを抑えられると考える．一方で，異なる文字を同一の識別器によって認証を行うため認証精度が低下するトレードオフが考えられる．したがって，異なる子音のデータでも同じ母音のデータとして学習し，識別器を作成するために適切な特徴を選択する必要があると考える．

また，テキストの入力動作に着目した先行研究の多くは識別器を作成する際に本人のラベルを与えたサンプルと他人のラベルを与えたサンプルを利用し，SVM や Random Forest などの様々な機械学習の手法により識別器を作成していた[6,9,10,11]．つまり，これらの手法では識別器を作成するために予め本人以外のユーザからテキスト入力時の動作を収集し，作成した特徴ベクトルに他人のラベルを与える必要がある．実際にスマートフォンを使用する環境を想定すると，スマートフォンを持ち主以外のユーザが入力する機会は少ないため，他人のラベルを与えるためのサンプルを収集することが困難である．そこで，Hao らは異常検知手法のひとつである OCSVM によって本人の入力動作のみを学習して識別器を作成している．本研究も Hao らの手法と同様に，OCSVM により識別器を作成する．

3.2 システム概要

図 1 に本研究の提案システムの全体像を示す．まず，ユーザは SNS やメール等のアプリケーションでテキストを入力する．入力したテキストデータと入力時にスマートフォンの複数のセンサから取得したデータを利用し，特徴を抽出する．このとき，学習データのサンプル数が閾値未満の場合は学習フェーズとして特徴ベクトルをそのまま学習データに追加する．もし，サンプル数が閾値以上の場合は，認証フェーズとして学習データから識別器を作成し，入力されたデータから作成された特徴ベクトルを利用し，認証を行う．認証に成功した場合は本人の入力動作のデータとして学習データに追加する．認証に失敗した場合は他人による入力と判断し，例えば入力したテキストの送信を中断し，再度テキスト入力の画面に遷移するなどの措置を行う．

以降の節では提案システムの主要な構成要素である特徴抽出の方法，認証フェーズにおける外れ値除去の方法，識別器の作成方法，認証の方法について述べる．

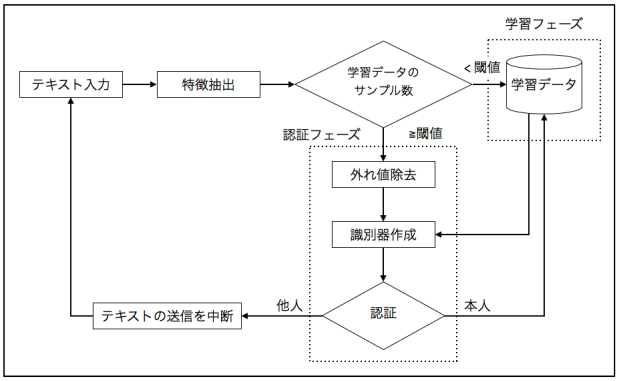


図 1 提案システムの全体像

3.3 特徴抽出

現在普及しているスマートフォンには様々なセンサが搭載されており，加速度や角速度だけでなく，画面にかかる圧力などのデータを取得することができる．本研究ではこれらのセンサデータを利用し，テキスト入力の動作から特徴を抽出する．

まず複数のユーザのフリック入力時にどのような個人差があるかを調査することを目的とした予備実験を行った．予備実験では，2 名の被験者（被験者 1，被験者 2）に 40 字程度の短い文章を入力させ，iPhone6s で取得可能なセンサデータとして指が画面に触れている間の画面の X/Y 座標，圧力，3 軸加速度，3 軸角速度，タイムスタンプを収集した．そして収集したデータを用いて指が画面に触れている間の X/Y 座標，圧力を可視化した．図 2 に被験者 1，図 3 に被験者 2 のテキスト入力時のフリック動作の軌跡を示す．

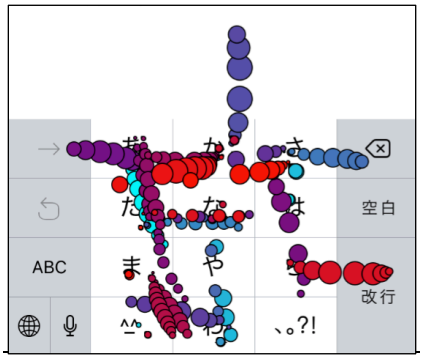


図 2 被験者 1 のテキスト入力時の
フリック動作の軌跡

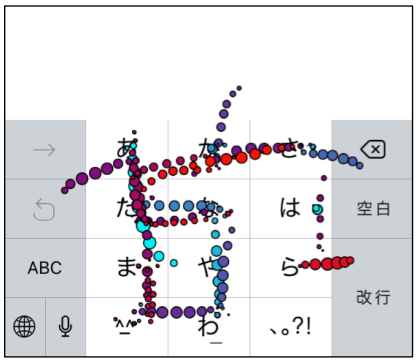


図 3 被験者 2 のテキスト入力時の
フリック動作の軌跡

図 2，図 3 の円の大きさは圧力の大きさを表し，円の色は青から赤へのグラデーションが時間の経過を表しており，入力した文字列の一文字目が青，最後の文字が赤となる．これらの図から，テキスト入力時の圧力の大きさに個人差が現れていることが分かる．また，フリック動作の始点から終点までの軌跡を見ると，カーブの曲がり方と距離にも差が現れている．カーブの曲がり方と距離については，入力したキーと次に入力するキーとの相対的な位置関係によって曲がり方や長さが異なり，被験者によって同じ方向へのフリック動作でも曲がり方が大きく異なることから，入力したキーとその前後のキーによって特徴が異なる可能性が考えられる．さらに，プロットされた円の間隔から，フリック動作の速度にも個人差があることが分かる．

以上の結果を踏まえて，本手法では認証に利用する特徴として，キーを入力するために指が画面に触れている間の圧力についての統計量（平均値，分散，中央値，最大値），フリック動作の角度と距離，i 番目に入力したキーに対して，そのキーの子音と母音，前後のキーの子音と母音，キー入力にかかった時間，入力したキーとその前後のキー入力との時間間隔（図 4），さらに，テキスト入力時のスマートフォン端末自体の揺れにも特徴が現れると考えられるため，3 軸合成加速度/角速度の統計量（平均値，分散，中央値）の合計 21 種類を特徴の候補とする．ただし，タップ動作はフリック動作と異なり，画面上で指を移動させないため，フリック動作の距離と角度を除いた 19 種類の特徴を候補とする．4 章ではこれらの特徴から本研究の目的である継続認証に必要な特徴を検討した結果と考察を述べる．

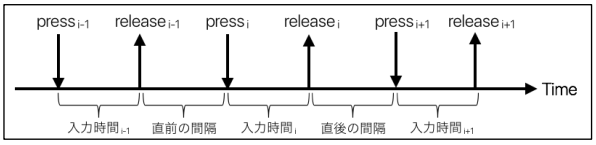


図 4 キー入力のタイミングと時間の特徴

3.4 認証

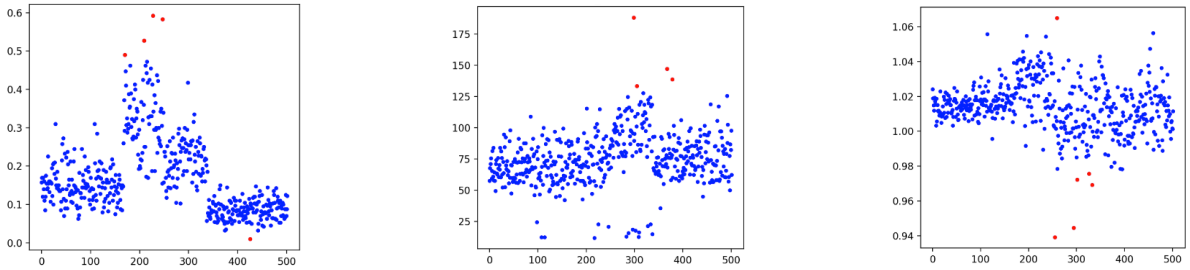
3.4.1 外れ値除去

ユーザから収集したデータを基に作成した特徴ベクトルの中には外れ値が含まれていることがあり，特徴ベクトルの中に外れ値が存在したまま識別器を作成すると識別精度に大きな影響を与えることがある．そこで，識別器を作成する前に学習データに使用するサンプルから外れ値除去を行う必要がある．外れ値除去の手法には様々な手法が存在するが，本研究では LOF(Local Outlier Factor)[13]を応用した手法により外れ値除去を行う．LOF とは，データ空間の密度に基づいた局所的な外れ値検出手法の一つである．あるデータの点 P に対して k 個の近傍点周辺の密度の平均値と点 P 周辺の密度との比を点 P の局所的な密度比として求める．局所的な密度が高い点は密度比が 1 に近い値になり，局所的な密度が低い点は密度比が大きくなることから，閾値以上の密度比が得られた場合，その点 P を外れ値と判定する．また，LOF では複数次元のデータ空間から局所的な密度を求める．

しかし，本研究で対象とする特徴ベクトルは次元数が多く，サンプルが疎になりやすい．そのため，本研究では特徴ごとに 1 次元のデータとして LOF による外れ値除去を行う．この処理を全ての次元で実行し，1 つの次元でも外れ値と判定された場合，その特徴ベクトルを外れ値のサンプルとして除去する．また，各特徴で LOF による外れ値除去を実行する際に最も大きい値をもつサンプルから順に実行し，LOF で外れ値と判定されないサンプルまで繰り返し，これを最小の値からも同様に実行することで計算量の削減を図る．図 5 に LOF による外れ値除去後のサンプルの例を示す．図 5 では 6 名の被験者から収集したフリック入力の動作データから，圧力の最大値，フリック動作の距離，3 軸合成加速度の平均値に対して外れ値除去を行った．縦軸は各特徴のサンプルの値を表し，横軸はサンプル番号を表す．また，赤の点は外れ値と判定されたサンプル，青の点は外れ値と判定されなかったサンプルを表す．提案手法では識別器の作成時に学習用の入力データから，認証時に認証用の入力データからそれぞれ外れ値除去を行う．

3.4.2 識別器の作成

本研究ではスマートフォンの持ち主の入力動作のみから学習して識別器を作成するために OCSVM により識別器を作成する．OCSVM は ν-SVM を 1 クラスのみの学習に用いて，未知の入力データがそのクラスに入るか入らないかを判定する．SVM は既に行動特徴を利用した個人認証の分野で広く利用されている[3,4,5,6,11]ことから，本研究にも適した分類アルゴリズムであると考える．また，識別器を作成する際にパラメータを設定することにより高精度な識別器を作成することができる．設定するパラメータは ν-SVM のパラメータである ν と SVM のカーネルとして使用する RBF カーネルのパラメータである γ の 2 種類とする．



(a) 圧力の最大値　(b) フリック動作の距離　(c) 3 軸合成加速度の平均値

図 5　LOF による外れ値除去後のサンプル

本研究では識別関数を求める際に，この 2 つのパラメータの最適な組み合わせをグリッドサーチにより求める．

3.5 認証方法

前節の手法で作成した識別器は未知の入力データに対して正常なデータと出力された場合に本人であると判定し，異常なデータと出力された場合に他人のデータであると判定する．提案手法では，複数の文字からなるテキストを 1 文字ずつ特徴ベクトルに変換し，本人または他人の判定を行う．そして，全ての文字で判定を終え，本人と判定された割合がある閾値以上の場合は本人の入力データとして扱う．閾値未満の場合は他人の入力動作として，例えば入力したテキストの送信を中断し，再度テキスト入力の画面に遷移するなどの措置を行う．ただし，本稿では前述の認証のための閾値の検討は今後の課題として，入力された未知の入力データが本人または他人と判定された際の精度の評価実験を行い，認証に有効な特徴の検討を行う．

4. 評価実験

本章では，前章で述べた提案手法について複数の特徴パターンの認証精度を比較し，本研究に有効な特徴の検討及び提案手法の有効性を検証する．

4.1 フリック入力時の動作データの収集

6 名の被験者を対象にフリック入力時の動作データの収集を行った．各被験者は椅子に座った状態でフリック入力方式によって 3 種類の文章を入力した．ただし，入力中に漢字変換などは行わず全てひらがなで入力し，濁点，半濁点，読点はタップ，句点は左方向のフリックとしてデータを取得した．また，入力した文章は全て 200 字程度の文章で，表 1 に全文章の各入力動作の平均出現頻度を示す．

表 1 各入力動作の平均出現頻度

動作の種類	母音の種類	出現頻度
タップ	あ	約 34%
左フリック	い	約 22%
上フリック	う	約 14%
右フリック	え	約 13%
下フリック	お	約 18%

4.2 認証精度の算出

本実験では被験者から 3 種類の文章の入力データを収集した．ある被験者を本人としたとき，本人から収集した 2 種類の文章を学習データとして使用し，入力動作の種類ごとに識別器を作成する．そして，本人から収集した残りの文章を本人のテストデータ，本人のテストデータと同じ種類の文章を入力した他人の入力データを他人のテストデータとして認証を行い，精度を評価する．本実験で認証精度は式(1)によって算出する．

$$\text{精度} = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \qquad (1)$$

ただし, TP は本人の入力動作を正しく本人と判定した回数，TN は他人の入力動作を正しく他人と判定した回数，FP は他人の入力動作を誤って本人と判定した回数，FN は本人の入力動作を誤って他人と判定した回数を意味する．この精度算出を 3 種類全ての文章がテストデータとなるように繰り返し行い, その平均値を本実験の認証精度とする．

また，全ての文章がテストデータとなるように精度を求めた際のサンプル数の平均を表 2 に示す．

表 2 実験のサンプル数

母音	本人の学習データ数	本人のテストデータ数	他人のテストデータ数
あ	125.6	59.1	327.6
い	83.4	36.6	219.9
う	50.1	21.7	139.0
え	43.8	17.2	125.1
お	64.1	26.7	177.6

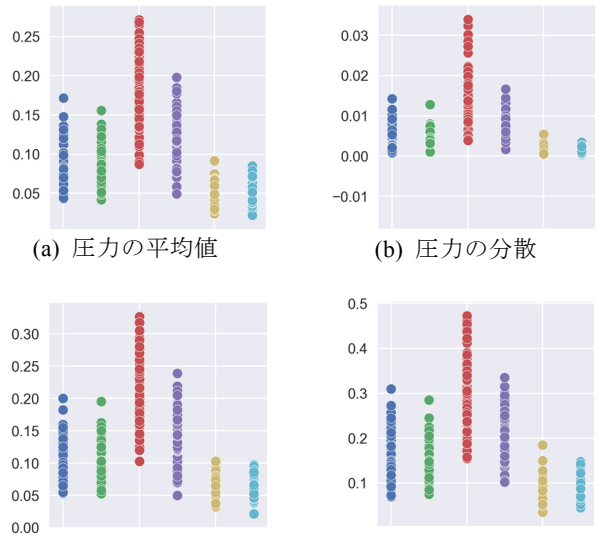
4.3 特徴選択

3.3 節ではフリック動作の場合は 21 種類，タップ動作の場合は 19 種類の特徴を候補として挙げた. これらの特徴から本研究で有効と考えられる特徴を選択し，複数パターンの特徴ベクトルを作成する．本実験で作成した 4 パターンの特徴ベクトルについて表 3 に示す．各パターンの特徴ベ

©2017 Information Processing Society of Japan

クトルは，表 3 において○が表示されている項目の特徴を採用した特徴ベクトルとする．また，次元数の項目は各方向へのフリック動作に対する特徴ベクトルの次元数を表し，括弧の中の数字はタップ動作に対する特徴ベクトルの次元数を表す．以下，各特徴パターンについて詳細を述べる．

まず，圧力，3 軸合成加速度/角速度の統計量に関する特徴について検討する．図 6 に被験者と圧力の各統計量の関係を示す．縦軸は各統計量のサンプルの値を表し，横軸は被験者を表す．これらの図から，平均値，中央値，最大値は同様の傾向を示していることが分かる．分散は他の統計量よりも被験者間で値の範囲が重なっていることから被験者間の特徴の差が現れにくいと考えられる．また，この傾向は 3 軸合成加速/角速度にも見られたことから，本実験では，収集した統計量の中から平均値のみを利用する．以上を踏まえ，パターン 1 では本実験で作成する特徴パターンの基準として，平均値以外の統計量を除いた全ての特徴を選択する．



(a) 圧力の平均値　(b) 圧力の分散

(c) 圧力の中央値　(d) 圧力の最大値

図 6 各被験者と圧力の各統計量との関係

次に，3.3 節では入力したキーとその前後のキーも特徴の候補として挙げていたが，特に入力したキーと次に入力するキーとの相対的な位置によってフリックの角度や距離が変化することが考えられる．したがってこれら 2 つのキーの位置が精度に影響を与えるかどうかを調査するために，パターン 2 では，母音と子音に関する特徴のうち入力したキーと次に入力したキーの子音のみを利用する．そして，パターン 2 との比較としてパターン 3 では全ての母音と子音の特徴を除いた特徴ベクトルとする．

また，本研究で着目するフリック入力の動作にはタップ動作とフリック動作の 2 種類の動作が存在する．そのため，フリック動作の特徴であるフリック動作の距離と角度はタップ動作では利用できない．そこで，これら 2 つのフリック動作の特徴を除いた場合でも認証に利用できるかどうかを調査するため，パターン 2 からフリック動作の距離と角度を除いた 8 種類の特徴から構成される特徴ベクトルをパターン 4 として精度評価を行う．

表 3 比較を行う特徴パターン

	パターン 1	パターン 2	パターン 3	パターン 4
i 番目の母音	○	×	×	×
i 番目の子音	○	○	×	○
i+1 番目の母音	○	×	×	×
i+1 番目の子音	○	○	×	○
i-1 番目の母音	○	×	×	×
i-1 番目の子音	○	×	×	×
入力時間	○	○	○	○
直前の間隔	○	○	○	○
直後の間隔	○	○	○	○
フリック動作の距離	○	○	○	×
フリック動作の角度	○	○	○	×
圧力（平均値）	○	○	○	○
3 軸合成加速度（平均値）	○	○	○	○
3 軸合成角速度（平均値）	○	○	○	○
次元数	14 (12)	10 (8)	8 (6)	8 (8)

4.4 特徴パターンによる認証精度の比較

前節で述べた 4 種類の特徴パターンについて認証精度の評価を行った．まず，被験者ごとに，4.2 節で述べた方法により自分を本人としたときの認証精度を算出した．そして，全ての被験者の認証精度の平均値を算出した．このように計算された各特徴パターンの認証精度を表 4 に示す．

また，表 5 に本実験で求めた各特徴パターンの精度の中で全ての母音の精度の平均値が最も高かったパターン 2 について，被験者別の精度を示す．

表 4 各特徴パターンの精度（単位：%）

	あ	い	う	え	お	平均
パターン 1	97.95	95.04	92.22	92.09	94.72	94.40
パターン 2	98.69	95.04	92.25	92.09	94.72	94.56
パターン 3	89.83	95.04	92.32	92.09	94.72	92.80
パターン 4	98.69	95.73	95.03	89.99	93.28	94.54

©2017 Information Processing Society of Japan

表 5 パターン 2 について各被験者を
本人とした際の認証精度（単位：%）

	あ	い	う	え	お
被験者 A	98.69	94.91	95.65	89.86	95.71
被験者 B	98.96	96.08	94.34	89.07	95.78
被験者 C	98.54	95.47	85.51	94.38	90.26
被験者 D	98.05	91.23	90.00	93.93	96.91
被験者 E	99.31	95.03	92.37	93.14	94.94
被験者 F	98.35	97.54	95.66	87.06	96.41
平均	98.69	95.04	92.25	92.09	94.72

4.5 考察

4.5.1 特徴パターンの比較

4.4 節では 4 種類の特徴パターンについて，評価を行った．まず，パターン 1 ではどの母音でも 9 割以上の精度で認証を行うことができていることが分かる．母音の種類によって精度にばらつきがあるが，実験に用いた全文章の各母音の出現頻度（表 1）と認証精度を比較すると，出現頻度が高い母音のときは認証精度が高く，出現頻度が低い母音のときは認証精度が低くなる傾向が見られた．これは出現頻度が低い母音のサンプル数が少ないため，一度の誤判定の影響が大きいため精度が悪化したと考えられる．

パターン 2 では母音と子音に関する特徴の中から入力したキーと次のキーの子音のみを利用することであ段の精度が向上している．一方，パターン 3 では全ての子音と母音の特徴を取り除くことであ段の精度が低下している．このことから，タップ動作において入力したキーと次のキーの位置の関係により何らかの個人差が現れていると考えられる．

パターン 4 ではフリックの角度と距離を除くことによって，母音が「い」,「う」の場合は精度が向上したが，母音が「え」,「お」の場合には精度が低下した．しかし，どの場合も精度の変化が小さいため，認証用のサンプルが少なかったことによる誤差の可能性が考えられる．

また, 本実験で最も精度が良かったパターン 2 について，タップ動作ではどの被験者も誤差が 1%程度しか無かったが，フリック動作では方向によらず，5~10%程度の誤差が確認された．このことから，フリック動作には被験者による動作のパターンに似たような特徴があり，入力動作の特徴が似ている被験者同士の精度が悪化したことが原因であると考えられる．

以上より，本実験から文字ごとに識別器を作らずに，タップ動作と各方向のフリック動作の 5 種類の動作から特徴抽出しても 9 割程度の精度を得られることが示唆された．

4.5.2 今後の課題

本実験により，被験者間による精度のばらつきが見られたことから，より正確に認証を行うことができる特徴を検討する必要があると考える．さらに，本研究では学習コストを抑えるためにフリック入力方式に着目した認証手法を提案したが，本手法で有効な精度を維持するために必要な学習サンプル数については調査できていない．また，実際に認証を行う場面として椅子に座っている状態以外にも歩行時や乗り物に乗るなどのスマートフォン端末が揺れている環境のように様々な環境でも利用可能な特徴について検討する必要がある．

5. おわりに

本研究はスマートフォンで日本語のテキスト入力中にユーザが特別な操作を行うことなく継続的に本人性を保証することを目的として，フリック動作の特徴に着目した認証手法を提案した．提案手法ではフリック動作を母音ごとにタップ動作，4 方向へのフリック動作に分け，合計 5 種類の識別器を作成した．また，本稿ではスマートフォンに搭載されているセンサから得られるデータを利用し，特徴の候補を挙げ，複数の特徴パターンで精度評価を行った．実験の結果として，最も認証精度が高かった特徴パターンについてタップ動作，各方向へのフリック動作の全てにおいて 9 割以上の精度が得られた．しかし，フリック動作の場合において被験者間で精度にばらつきが見られたことから，より正確にユーザを認証するための特徴や認証に必要な学習データのサンプル数の検討が必要であると考える．

参考文献

[1] 山田浩二，松本弘之，松本勉，“指紋照合装置は人工指を受け入れるか”，情報処理学会研究報告コンピュータ・セキュリティ (CSEC)，Vol.2000，No.68，pp.159-166 (2000).

[2] Q. Yang, G. Peng, T. Nguyen, X. Qi, G. Zhou, Z. Sitova, P. Gasti and K. S. Balagani, “A Multimodal Data Set for Evaluating Continuous Authentication Performance in Smartphones, ” 12th ACM Conference on Embedded Network Sensor Systems (SenSys’14), pp.358-359 (2014).

[3] W. Lee and R. B. Lee, “Multi-sensor Authentication to Improve Smartphone Security,” 1st International Conference on Information System Security and Privacy (ICISSP), pp.270-280 (2015).

[4] M. Temper, S. Tjoa and M. Kaiser, “Touch to Authenticate – Continuous Biometric Authentication on Mobile Devices,” 1st International Conference on Software Security and Assurance (ICSSA), pp.30-35 (2015).

[5] Z. Ali, J. Payton and V. Sritapan, “At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices,” 2016 IEEE Security and Privacy Workshops (SPW), pp.272-275 (2016).

[6] 味岡孝昇，梅澤猛，大澤範高，“暗証番号入力時の腕の加速度を用いた携帯端末向け個人認証”, 情報処理学会研究報告モバイルコンピューティングとパーベイシブシステム (MBL)，Vol.2016-MBL-81，No.22，pp.1-6 (2016).

[7] N. Takeuchi and R. Uda, “Password Security Enhancement Method by Flick Input with Considering the Floor Shake,” 9th International Conference on Ubiquitous Information Management and Communication (IMCOM'15), pp.1-8 (2015).

[8] 沼沢誠，千石靖，“フリック入力を利用したスマートフォンの個人認証システム”，情報処理学会コンピュータ・セキュリティシンポジウム 2013 論文集，Vol.2013，No.4，pp.472-477 (2013).

[9] U. Burgbacher and K. Hinrichs, “An Implicit Author Verification

©2017 Information Processing Society of Japan

System for Text Message Based on Gesture Typing Biometrics," SIGCHI Conference on Human Factors in Computing Systems (CHI'14), pp.2951-2954 (2014).
[10] T. Feng, X. Zhao, B. Carbunar and W. Shi, "Continuous Mobile Authentication Using Virtual Key Typing Biometrics," 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp.1547-1552 (2013).
[11] Z. Hao and Q. Li, "Towards User Re-Authentication on Mobile Devices via On-Screen Keyboard," 4th IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), pp.78-83 (2016).
[12] 泉将之，佐村俊治，西村治彦，"フリック入力による日本語非定型文のキーストローク認証"，情報処理学会関西支部支部大会講演論文集，E-15, Vol.2013 (2013).
[13] M. M. Breunig, H. -P. Kriegel, R. T. Ng and J.Sander, "LOF: Identifying Density-Based Local Outliers," the 2000 ACM SIGMOD Conference of Management of Data, pp.93-104 (2000).

©2017 Information Processing Society of Japan