1V-03

ウェアラブルセンサを用いた打鍵特徴による個人認証手法の提案

伊藤　駿吾†　　白石　陽†

公立はこだて未来大学システム情報科学部†

1. はじめに

現在，多くの PC やスマートフォンなどの認証システムではユーザ名とパスワードを用いた知識による認証方式が利用されている．この方式は ID とパスワードの両方を知っているユーザのみがログイン可能となるが，パスワードの漏洩による不正アクセスや，忘却による認証拒否などの恐れがある．また，近年注目されている認証方式として，生体情報による認証方式がある．生体情報とは指紋や虹彩のような身体的特徴や署名や音声のような行動特徴のことである．身体的特徴を用いた方式として指紋認証を利用したデバイスが登場した．しかし既に人工指による指紋照合に関する研究[1]で，グミで作成された人工指による指紋認証が可能であることを確認され，指紋認証の安全性に問題があると指摘されている．行動特徴を用いた方式は一般的に筆跡や音声を利用しており，ペンタブレットやマイクを使用する必要があるため，利用可能な場面が限られてしまう．

一方，近年加速度センサや角速度センサが小型化されたことによって，スマートウォッチやリストバンド型の活動量計など手首に装着可能なウェアラブルデバイスが普及している．そのため，これらのデバイスを利用した行動推定や動作分析の研究[2]が行われており，行動特徴を用いた個人認証への応用も期待できると考える．

本研究では PC ログイン時の個人認証に着目し，キーボードを用いた知識による認証方式の安全性を高めるために，知識による認証方式と行動特徴による認証方式の両方を利用した個人認証手法を提案する．行動特徴として，キーボード打鍵時の手と指の動作（以下，手指動作）を利用する．ただし，個人認証手法のうち，知識による認証は既に成功している状況を想定している．本稿ではパスワードを入力したユーザが本当に本人かどうかを確かめるために，ウェアラブルセンサを利用することで，キーボード打鍵時の手指動作の特徴による個人認証手法について述べる．

2. 関連研究

2.1 キーボードの打鍵特徴を用いた個人認証

キーボードの打鍵特徴を用いた個人認証手法として，キーボードの打鍵時間を用いた個人認証に関する研究[3]がある．この研究では，ある文字列を入力した時の各キーが押されてから離されるまでの時間を測定し，品質工学のパターン分析手法の一つである誤圧によってパターン距離を求めることで個人認証を行っている．しかし，特徴量抽出に使用しているデータがキーボードの打鍵時間のみである．そのため，タイピングスキルの低いユーザは複数回入力する際の打鍵時間の標準偏差が大きくなり，入力パターンのばらつきが大きくなることから認証精度が悪化するという問題がある．

Personal authentication method by using wearable sensors based on the characteristics of keystroke actions

†Shungo Ito　†Yoh Shiraishi

†School of Systems Information Science, Future University Hakodate

2.2 打鍵動作の分析

打鍵動作の分析手法として，スマートウォッチに搭載された加速度センサと角速度センサを利用して打鍵のタイミングと入力したキーを推定する研究[4]がある．この研究では，加速度データのピークを検出することで打鍵のタイミングを推定し，同時に加速度データと角速度データの二重積分によってキーボード上の手指の軌跡を求めることで，入力したキーを推定している．しかし，個人認証を行うことを想定していないため，打鍵のタイミングと入力したキーだけでは個人認証を行うことは困難であると考える．

2.3 まとめ

以上のように，打鍵動作の特徴を用いた個人認証の研究があるが，キーボードの打鍵時間による特徴だけでは個人認証を行うためには不十分であると考えられる．また，打鍵時の手指動作はスマートウォッチのように手首にセンサを装着することで各センサデータの収集および特徴量の抽出が可能であると考えられる．しかし，文献[4]の研究では打鍵のタイミングと入力したキーを推定するための特徴量としてセンサデータのピークと二重積分による変位を利用しているが，個人認証を行うためには新たな特徴量を抽出する必要があると考える．

3 提案手法

本研究では，キーボードの打鍵時間と打鍵時の手指動作から特徴量を抽出することで個人認証を行う．

文献[3]ではキーボードの打鍵時間から特徴量を抽出しているが，高精度な個人認証を行うには打鍵時間から抽出した特徴量だけでは不十分であると考えられる．しかしキーボード打鍵時の手指動作には個人の癖が現れると予想される．そこで文献[4]のように加速度センサと角速度センサを手首に装着することで，キーボード打鍵時の手指動作を取得し，個人認証を行うために必要な特徴量を抽出する．

個人を認証する方法として，教師あり学習によって本人または他人の分類を行う．本人と分類された場合に認証成功とする．

3.1 センサデータの取得

キーボード打鍵時の手指動作から特徴量を抽出するために，被験者の両手首に加速度センサと角速度センサを装着することで，文字列を入力した時のキー入力データ，3 軸加速度データ，3 軸角速度データを取得する．ここで，キー入力データとは入力したキーの種類とキーを押した時刻，離した時刻を記録したデータを指す．また，3 軸加速度データ，3 軸角速度データとは文字列の一文字目のキーが押された時刻から最後のキーを押して離した時刻までに記録したデータを指す．図 1 に両手首にセンサを装着した様子と打鍵時のセンサの各軸の方向を示す．

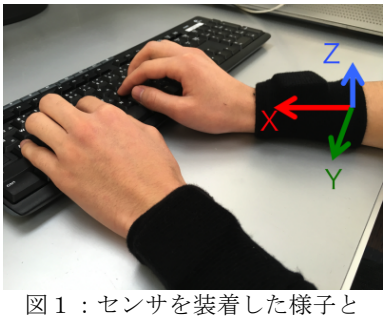

図 1 ：センサを装着した様子と
打鍵時のセンサの各軸の方向

3.2 特徴量抽出

キーボード打鍵時の手指動作から個人認証を行うための特徴として，各キーの打鍵時に現れる手指動作の癖に着目した．例えば，ある文字列を入力した際に，頻繁に入力するキーを打鍵するときは手指動作に無駄がなく手指動作のぶれが小さくなる．しかし，普段入力しないキーを打鍵するときは打鍵する前に一旦手指動作を止め，キーを探すため入力時間が長くなり，手指動作のぶれが大きくなることがある．そのため，ある文字列の打鍵時間全体ではなく，キーごとに打鍵時の手指動作を特徴量とすることでより詳細な打鍵時の手指動作の癖を抽出することができると考える．入力したキーごとにキーを押した方の手首に装着したセンサから取得したデータを使用し，キー入力時間と 3 軸加速度データの分散値，3 軸角速度データの分散値の合計 7 種類を特徴量として求める．*n* 番目のキーの入力時間は，*n-1* 番目のキーを押した時刻から *n* 番目のキーを押した時刻までの差分とする．ただし，文字列の最後のキーのみ押した時刻からそのキーを離した時刻までの差分とする．センサデータの分散値は各キーの入力時間内のセンサデータから計算する．文字数を *N* とすると，*N*×7 次元のデータ（以下，サンプル）を作成する．

3.3 個人認証のための分類

個人認証を行う際に，登録済みのデータと認証用のデータが同一人物のデータであるかを比較するために，サポートベクターマシン（SVM）による分類を行う．SVM は 2 クラス分類に利用される教師あり学習の一つである．本研究では作成したサンプルのデータセットを学習データとテストデータに分け，本人または他人の分類を行う．このとき，データセットの分散値は入力したユーザによって値の範囲が大きく異なり，分類に影響を与えるため，事前に最大値が 1，最小値が 0 になるように正規化する．

4 実験および考察

3 章で述べたキー入力時間とセンサデータの分散値が個人認証のための特徴量として有効かどうかを調べるために実験を行った．

4.1 実験

まず，3 軸加速度センサと 3 軸角速度センサ搭載した無線センサである TSND121（ATR-Promotions 社製）を 3 名の被験者の両手首にリストバンドで固定した．次に，サンプリングレート 100Hz で “defence”，“ground”，“japanese”，“geological” の 4 種類の文字列を 20 回ずつ入力した時のキー入力データと 3 軸加速度データ，3 軸角速度データを記録し，得られたキー入力データ，センサデータからデータセットを作成した．そして leave-one-out 交差検定によって全てのサンプルが一度ずつテストデータとなるように SVM を実行し，本人または他人の分類を行った．なお，SVM は Python の機械学習ライブラリである scikit-lean 利用して実装を行った．

4.2 実験結果

4 種類の単語別に SVM による認証精度を表 1 に示す．A，B，C はそれぞれ 3 名の被験者を表し，認証精度は被験者が本人であると分類された割合を示す．

表 1：SVM による認証精度（単位：%）

		単語			
		defence	ground	japanese	geological
被験者	A	95.0	90.0	93.3	93.3
	B	100.0	95.0	98.3	96.7
	C	91.7	95.0	98.3	96.7

4.3 考察

実験結果から，全ての文字列で 9 割以上の認証精度が得られた．この結果からキーボード打鍵時の手指動作には個人の癖があり，個人認証を行う上で有用な特徴になり得ることが示唆された．しかし，今回の実験は被験者数が 3 名と少ないため 9 割以上の精度で分類ができたと考えられる．そのため，今後の実験で被験者数が増加した時に今回の実験と同等の精度が得られるかどうか検証する必要がある．また，今回の実験ではテストデータのサンプルのユーザは全て事前に学習データも用意されていたが，SVM は事前に学習データを登録していないユーザが認証を行おうとすると，特徴が最も似ているユーザに分類されてしまうため，対策を考える必要がある．

5. おわりに

本稿では，PC ログイン時の個人認証に着目し，ウェアラブルセンサを利用することで，キーボード打鍵時の手指動作の特徴による個人認証手法を述べた．キーボード打鍵時の手指動作の特徴量として，キー入力時間，3 軸加速度データの分散値，3 軸角速度データの分散値を利用して 3 名の被験者を対象に個人認証の予備実験を行った．その結果，打鍵時の手指動作には個人の癖があり，個人認証を行う上で有用な特徴になり得ることが示唆された．今後は実験の被験者数を増やし，認証アルゴリズムの改良を行っていく．

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] 卓璐，王琛，浅井洋樹，山名早人，“3 軸加速度計を用いたデスクワーク中の割り込み可能性の推定”，第 7 回データ工学と情報マネジメントに関するフォーラム（DEIM2015），E1-5，pp.1-8，2015.

[3] 大坂一司，矢野耕也，“品質工学の手法を用いたキーストロークによる本人認証”，情報処理学会研究報告コンピュータセキュリティ（CSEC），Vol.2012-CSEC-58，No.19，pp.1-6，2012.

[4] He Wang, Ted Tsung-Te Lai, and Romit Roy Choudhury. MoLe: Motion Leaks through Smartwatch Sensors. ACM MobiCom '15, pp.155-166, 2015.