

スマートロックにおける二端末の加速度を用いた 歩行状態による本人認証の検討

A Study on Authentication Using Two-Terminal Acceleration in Smart Lock

渡辺 一樹[†] 長友 誠[†]

Kazuki Watanabe Makoto Nagatomo

油田 健太郎[‡] 岡崎 直宣[‡] 朴 美娘[†]

Kentaro Aburada Naonobu Okazaki Mirang Park

1. はじめに

近年、スマートウォッチやスマートグラスなどのウェアラブル端末が年々増加傾向にある。2020年にはウェアラブル端末が3億台にも増加すると言われ、多くの製品が開発されている[1]。さらに、モノとインターネットが繋がるIoT(Internet of Things)機器も多く開発されており、2021年には約350億台にも増加すると予測されている[2]。IoT機器には、スマート家電と呼ばれるインターネットと繋がる家電や、スマートスピーカーと呼ばれる音声でコンテンツと繋がるスピーカーなどがある。その中で、スマートロックと呼ばれる電子的にドアの鍵の開閉を行うIoT製品がある。2015年はスマートロック元年と呼ばれ、現在までに、Qrio[3]やAkerun[4]、August[5]など、様々なスマートロック製品が販売されている。スマートロックにおける認証方式として、従来のパスワード方式ではパスワードが推測されやすく、ユーザに記憶負荷がかかるという問題点がある。これらの問題点を解消する方式として人間の身体的特徴や行動的特徴を用いる生体認証方式がある。しかし、生体認証方式の1つである指紋認証方式では、家の前で数秒間立ち止まらなくてはならないという煩わしさがあり、手袋を付けていればそれを外す必要がある。また、顔認証方式もドアの前で数秒間立ち止まる必要があり、マスクをつけ帽子を被っていれば、それらを外す必要がある。このように、スマートロックにおける認証の煩わしさを完全に無くすることができていないのが現状である。そこで、本論文ではユーザが所持している端末のセンサから得られる、歩行状態の行動的特徴を用いて認証を行う歩行認証に着目する。通常生活で行う歩行を用いることで、ユーザが意識することなく認証が行われるため、認証に必要な煩わしさを解消できると考えられる。

先行研究では、1つの端末を用いたスマートフォンにおける歩行認証の研究が行われてきた[6]~[8]。ここでは、端末の向きや歩行認証の精度の課題がある。そこで、本研究では認証精度向上のためスマートフォンとウェアラブル端末などの2つの端末を用い、スマートロックを想定した歩行認証のシステムモデルを提案しその有効性を確認する。

以降、2章では関連研究について示し、3章ではスマートロックを想定した、2つの端末を用いた歩行認証の提案方式を示す。また、4章では実験を行い提案方式の識別率や認証に貢献する特徴量について示す。5章では、まとめと今後の課題を述べる。

[†] 神奈川工科大学, Kanagawa Institute of Technology

[‡] 宮崎大学, University of Miyazaki

2. 関連研究

2.1 スマートフォンのセンサを用いた歩行認証

彭ら[6]は、スマートフォンの加速度センサから取得される x, y, z の3軸加速度を用いた歩行認証について提案している。ユーザの歩行時の加速度データから、平均値や標準偏差、絶対標準偏差、平均合成加速度、ピーク間の時間、ビン分布を用いた43個の特徴量を抽出し、分類アルゴリズムを用いて識別率を調べている。そこで、決定木48を用いた際のFAR(False Acceptance Rate)が0.6%、FRR(False Rejection Rate)が8.7%であり、ニューラルネットワークを用いた際のFARが0.3%、FRRが3.8%であった。また、認証に貢献した特徴量として3軸それぞれの平均値が挙げられ、認証に貢献しない特徴量として平均合成加速度やピーク間の時間を挙げている。さらに、データマイニングソフトであるWEKAの56個の分類アルゴリズムを用いて識別率を計算し、分類アルゴリズムによって精度が大きく変わることを示している。しかし、各 x, y, z 軸の加速度データから独立した特徴量を抽出したため、端末の向きを考慮しなくてはならないという課題がある。

今野ら[7]は、スマートフォンに搭載された加速度センサと角速度センサの2つのセンサを用いた歩行認証を提案している。ここでは、システムへ入力されたセンサのデータと、事前に登録されたデータとの距離を計算し、その距離を基に機械学習でユーザの識別を行っている。

2.2 端末の所持位置を考慮した歩行認証

岩本ら[8]は、ユーザの歩行状態の推定(静止状態、歩行状態、走行状態)と、端末の所持位置の推定(前ポケット、後ろポケット、胸ポケット、端末の画面を見る、腕を振る)を行ったうえで、ユーザの推定を行う歩行認証のモデルを提案している。結果として、所持位置推定については93%と高い識別率となっている。このことから、端末の所持位置によって異なったデータを取得できると考えられる。よって、複数の端末を体の異なった部位に身に着けることで歩行認証の精度向上が期待できる。

本研究では、2つの端末を異なった体の部位に装着し加速度データを取得することで、端末の向きを考慮せずに歩行認証を行う場合でも、高い識別率を得ることを目的とする。

3. 提案方式

3.1 システムモデル

本研究では、ユーザの体に装着した 2 つの端末の加速度データを用いてスマートロックの認証を行う。図 1 にそのシステムモデルを示す。提案システムモデルは、加速度センサが搭載されている端末 1, 端末 2 と、加速度データを受信しユーザの認証を行うスマートロックで構成されている。スマートロックは Bluetooth の iBeacon を用いて端末との近接検知を行う。iBeacon では、immediate(とても近い), near(近い), far(遠い)の 3 つの近接検知を行うことができ、本論文ではこの近接検知を用いて加速度データの計測を行う。提案システムモデルでの認証手順を以下に示す。

- ① 端末 1, 2 が iBeacon の far を検知する(約 1m~約 50m)
- ② 端末 1, 2 が加速度計測を開始する
- ③ 端末 1, 2 が iBeacon の near を検知する(約 1m 未満)
- ④ 端末 1, 2 が加速度計測を終了する
- ⑤ 端末 1, 2 が加速度データをスマートロックへ送信する
- ⑥ スマートロック内で、⑤ で取得した加速度データを用いてユーザの認証を行う

スマートロックでは、あらかじめ複数人の歩行データを登録しておき、登録フェーズで認証したい人のデータを登録する。手順⑥において、2 つの端末の加速度データを受信したスマートロックはデータ処理を行い、そのデータから特徴量を抽出する。その後、識別器でユーザを判定し認証を行う。識別器には、機械学習の教師あり学習を用いてユーザの分類を行う。

3.2 加速度データの処理

スマートロックでユーザの特徴量を抽出するため、2 つの端末から受信した加速度データの処理を行う。本論文では、端末の向きを考慮しない歩行認証を行うため合成加速度を用いる。ここで、端末 1, 2 の合成加速度 r_1^1, r_1^2 は次のように示す。なお、取得した x, y, z 軸の加速度データを端末 1 では x_1^1, y_1^1, z_1^1 と表し、端末 2 では x_1^2, y_1^2, z_1^2 と表す。

$$r_1^1 = \sqrt{(x_1^1)^2 + (y_1^1)^2 + (z_1^1)^2} \quad (1)$$

$$r_1^2 = \sqrt{(x_1^2)^2 + (y_1^2)^2 + (z_1^2)^2} \quad (2)$$

端末 1, 2 の加速度データの計測開始から i 番目にデータを取得した時刻を t_i^1, t_i^2 とし、計測開始から終了までに取得したデータ数を n_1, n_2 で表すと、端末 1, 2 から取得した合成加速度データの集合 d_1, d_2 は次のようになる。

$$d_1 = \{(t_i^1, r_i^1) \mid i \in \{1, \dots, n_1\}\} \quad (3)$$

$$d_2 = \{(t_i^2, r_i^2) \mid i \in \{1, \dots, n_2\}\} \quad (4)$$

例えばここで、2 つの端末の合成加速度データを図 2 に示す。青い波形は端末 1 の合成加速度データを示し、オレンジ色の波形は端末 2 の合成加速度データを示す。2 つの

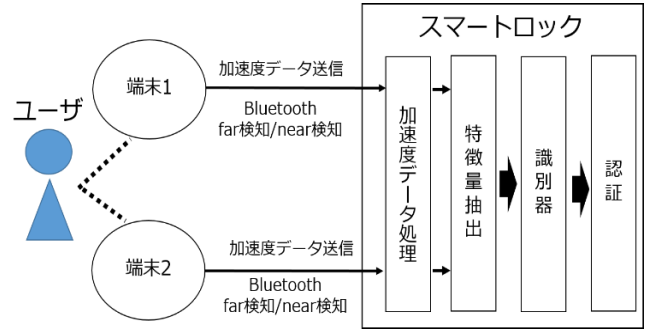


図 1 提案システムモデル

合成加速度データのサンプル数を確認してみると、端末性能や計測時間の違いから、各端末のデータのサンプル数が異なっている。そこで、2 つのデータを比較するため 2 つの端末のサンプル数を合わせる必要がある。その方法として、2 つの端末の加速度データを取得した時刻差からサンプル数を合わせる。例えば、2 つのサンプル数の大小関係が $n_1 > n_2$ であった場合の、サンプル数を合わせた後のデータの集合を d_1', d_2' で表すと次のようになる。

$$d_1' = \{(t_i^1, r_i^1) \mid i \in \{1, \dots, n_2\}\} \quad (5)$$

$$d_2' = d_2 = \{(t_i^2, r_i^2) \mid i \in \{1, \dots, n_2\}\} \quad (6)$$

ここで、 t_i^1, r_i^1 は式(7), (8)で計算される。

$$t_i^1 = t_{\underset{j \in \{1, \dots, n_1\}}{\operatorname{argmin}}(|t_j^1 - t_i^2|)}^1 \quad (7)$$

$$r_i^1 = r_{\underset{j \in \{1, \dots, n_1\}}{\operatorname{argmin}}(|t_j^1 - t_i^2|)}^1 \quad (8)$$

また、静止状態では加速度データのばらつきが少なく、歩行状態ではばらつきが多いため、一定区間の加速度データの標準偏差が高い位置を探し、その区間を歩行状態とする。その後、ローパスフィルタで加速度データのノイズの削除を行う。図 3 に上記の加速度データの処理を行なった後の波形を示す。

3.3 特徴量抽出

ユーザ識別のための特徴量として、合成加速度データの平均値、中央値、標準偏差、分散、最大値、最小値、極大値間隔の中央値、極小値間隔の中央値、周期の中央値を計算した値を端末 1, 端末 2 の合成加速度データから抽出する。加えて 2 つの合成加速度データの違いとして、上記で計算した各特徴量の値の端末 1 と端末 2 の差も特徴量とする。さらに、時間軸方向に加速度データをずらし、最も高い類似度の特徴量とする。その類似度を算出する方法として、テンプレートマッチングを用いる。使用したテンプレートマッチングは、絶対値の差から計算する SAD(Sum of Absolute Difference)、二乗和から計算する SSD(Sum of Squared Difference)、相関係数から計算する NCC(Normalized Cross Correlation)の 3 つを用いる。3 つの類似度を算出する式を式(9)~(11)に示す。ただし、式(5), (6)でそろえたサンプル数を n

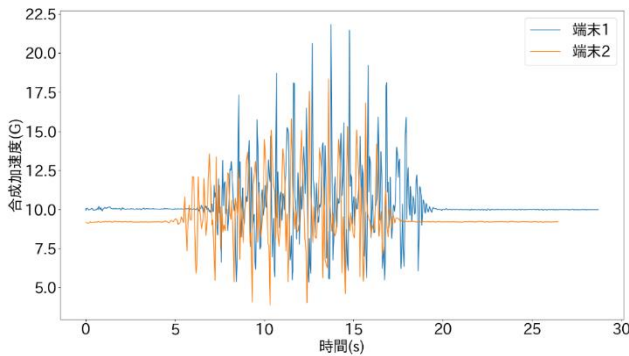


図 2 合成加速度データ

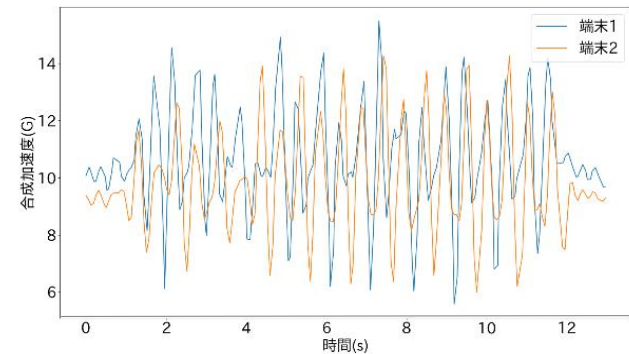


図 3 加速度処理後の合成加速度

とした場合、2つの加速度データを n までずらすと類似度を比較するサンプル数が少なくなってしまうため、ずらす個数を $k \in \{1, \dots, \frac{2}{3}n\}$ とする。

$$SAD = \min_{k \in \{1, \dots, \frac{2}{3}n\}} \frac{1}{n-k} \sum_{i=1}^{n-k} |r_i^1 - r_{i+k}^2| \quad (9)$$

$$SSD = \min_{k \in \{1, \dots, \frac{2}{3}n\}} \frac{1}{n-k} \sum_{i=1}^{n-k} (r_i^1 - r_{i+k}^2)^2 \quad (10)$$

$$NCC = \max_{k \in \{1, \dots, \frac{2}{3}n\}} \frac{\sqrt{\sum_{i=1}^{n-k} r_i^1 r_{i+k}^2}}{\sqrt{\sum_{i=1}^{n-k} r_i^1} \sqrt{\sum_{i=1}^{n-k} r_{i+k}^2}} \quad (11)$$

また、DP(Dynamic Programming)マッチングの1つである最小コスト弾性マッチングを用いる類似度も特徴量とする。その類似度を算出する式を次に示す。

$$\text{コスト} : C = |r_i^1 - r_j^2|$$

$$DP(i, j) = \min \begin{cases} DP(i-1, j-1) + 2C \\ DP(i-1, j) + C \\ DP(i, j-1) + C \end{cases} \quad (12)$$

なお、 $i, j \in \{1, \dots, n\}$ とした場合、 $DP(n, n)$ を特徴量とする。以上の特徴量を用いて、識別器で分類することによってユーザの分類を行う。



図 4 端末の所持位置

4. 実験と評価

提案した2つの端末を用いた歩行認証の有効性を確認するための実験を行った。実験条件として、図4のように端末1を右前ポケット、端末2を左前ポケットに入れ、10m歩行しながら加速度を計測した。実験には、端末1にスマートフォンXperiaXZsを用い、端末2にスマートフォンXperiaZ2を用いた。被験者は神奈川工科大学の学生11名である。実験の手順を以下に示す。

- ① 端末1, 端末2それぞれの加速度計測を開始する
- ② 被験者は5秒間その場で静止する
- ③ 被験者は廊下を10m歩行する
- ④ 被験者は5秒間その場で静止する
- ⑤ 端末1, 端末2の加速度計測を終了する

なお、手順②, ④では、手順③の歩行状態を正確に抽出するため5秒間の静止を行う。以上の手順を被験者11名に20回行ってもらった。また、機械学習を行ううえで半分のデータを学習用データ、残りの半分をテストデータとし、識別率を調べるプログラムをPythonで作成した。今回実験で使用した機械学習はPythonモジュールscikit-learn[9]のSVM, GaussianNB, MultinomialNB, RandomForest, NNの5つである。なお、識別率は正しく分類できたデータ数から全てのテストデータ数を割った値を100分率で示す。

まず、1つの端末を用いる場合の識別率を確認する。1つの端末を用いる場合、本論文で示した特徴量であるSAD, SSD, NCC, DPは2つの合成加速度の類似度を計算するための特徴量として使用することができない。そのため、1つの端末を用いた場合の特徴量として、平均値, 中央値, 標準偏差, 分散, 極大値間隔の中央値, 極小値間隔の中央値, 周期の中央値を端末1の合成加速度データで計算した値を使用する。その特徴量から、全ての組み合わせを各機械学習で計算し識別率を調べた。1つの端末を用いた場合の最も高い識別率とそのとき使用した特徴量の組み合わせを表1で示す。1つの端末を用いた場合の最も高い識別率は機械学習にGaussianNBを用いたときの76.4%であった。

次に、2つの端末を用いた場合の識別率を確認する。全ての特徴量の組み合わせに対して識別率を算出すると、試行回数が多くなりすぎてしまう。そのため、特徴量を13グループ(平均値, 中央値, 標準偏差, 分散, 最大値, 最小値, 極大値間隔, 極小値間隔, 周期, SAD, SSD, NCC, DP)に分割する。例えば、平均値のグループでは、端末1の

表 1 1つの端末を用いた場合の識別率

機械学習				
SVM	GaussianNB	MultinomialNB	RandomForest	NN
特徴量				
中央値	平均値	平均値	平均値	中央値
最大値	中央値	標準偏差	中央値	標準偏差
最小値	最大値	分散	標準偏差	分散
極大値間隔	最小値	最大値	分散	最大値
極小値間隔	極大値間隔	最小値	最大値	最小値
周期	極小値間隔	極大値間隔	最小値	極大値間隔
		極小値間隔	極大値間隔	極小値間隔
			極小値間隔	
識別率				
61.8%	76.4%	54.5%	75.5%	64.6%

表 2 2つの端末を用いた場合の識別率

機械学習				
SVM	GaussianNB	MultinomialNB	RandomForest	NN
特徴量				
平均値	平均値	平均値	平均値	平均値
標準偏差	中央値	中央値	中央値	中央値
NCC	標準偏差	標準偏差	分散	標準偏差
	分散	分散	最大値	分散
	最大値	最小値	最小値	最大値
	最小値	SSD	極大値間隔	最小値
	NCC	SAD		SSD
	DP	NCC		SAD
		DP		DP
				極大値間隔
				極小値間隔
識別率				
78.2%	99.1%	71.0%	99.1%	73.6%

平均値, 端末 2 の平均値, 端末 1, 2 の平均値の差をそのグループとする。また, 分割した 13 グループ全ての組み合わせを各機械学習で計算することで識別率を調べた。2 つの端末を用いた場合の最も高い識別率と, そのとき使用した特徴量の組み合わせを表 2 で示す。2 つの端末を用いた場合の最も高い識別率は機械学習に GaussianNB, RandomForest を用いたときの 99.1% であった。また, 表 1, 2 から, 1 つの端末を用いる場合より 2 つの端末を用いた場合のほうが, 識別率が高くなることがわかった。2 つの端末を用いた場合の特徴量の組み合わせとして, GaussianNB では平均値, 中央値, 標準偏差, 分散, 最大値, 最小値, NCC, DP を用いることで最も高い識別率を得ることができ, RandomForest では平均値, 中央値, 分散, 最大値, 最小値, 極大値間隔を用いることで最も高い識別率を得ることができた。また, 2 つの端末を用いた場合の識別率が, 90% を超

表 3 特徴量再頻出順

機械学習	
GaussianNB	RandomForest
特徴量再頻出順	
平均値(2544回)	中央値(437回)
最小値(2262回)	最小値(402回)
中央値(2200回)	平均値(342回)
最大値(1908回)	極小値間隔(333回)
標準偏差(1882回)	分散(287回)

えた分類アルゴリズムで使用された特徴量を再頻出順で 5 つまで示すと表 3 のようになる。この結果から, 今回の提案では平均値や中央値, 最小値が認証に貢献することがわかった。

5. おわりに

本研究では, スマートロックを想定した 2 つの端末の加速度データを用いた歩行認証のシステムモデルを提案し, その識別率を調べた。その結果 1 つの端末を用いた場合より 2 つの端末を用いた場合のほうが, 識別率が高くなることを示した。また, 2 つの端末を用い, RandomForest, GaussianNB で最も良い特徴量の組み合わせを選択した場合, 99.1% という高い識別率を得ることができた。さらに, 特徴量の組み合わせにより識別率が変化し, 特徴量として平均値や最小値, 中央値が認証に貢献することも確認できた。

今後は, より実際の環境やユーザビリティを考慮した実験を行うため, ユーザが身に着けているウェアラブル端末と所持しているスマートフォンの 2 つの端末から, 加速度データを取得した際の認証精度を調べる予定である。

参考文献

- [1] 総務省, “ウェアラブル端末が注目されている背景”, 情報通信白書, <<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc131410.html>>, (2016).
- [2] 総務省, “爆発的に増加する IoT デバイス”, 情報通信白書, <<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc13310.html>>, (2017).
- [3] Qrio, “Qrio Smart Lock”, <<https://qrio.me/smartlock>>, (2018/06/08 参照).
- [4] 株式会社フォトシンス, “入退室管理システムなら Akerun[オフィス向けスマートロック]”, <<https://akerun.com/feature/>>, (2018/06/08 参照).
- [5] august, “August Smart Lock | Your Smart Home Starts at the Front Door”, <<https://august.com>>, (2018/06/08 参照).
- [6] 彭 龍, 渡邊 裕司, “スマートフォンの加速度センサを用いた歩行時の認証に関する一考察”, Computer Security Symposium 2013, 2 1-23, (2013).
- [7] 今野 慎介, 中村 嘉隆, 白石 陽, 高橋 修, “複数のウェアラブルセンサを用いた歩行動作による本人認証法の精度向上”, 情報処理学会論文誌, Vol.57 No.1 109-122, (2016).
- [8] 岩本 健嗣, 杉森 大輔, 松本 三千人, “3 軸加速度センサを用いた歩行者推定手法”, 情報処理学会論文誌, Vol.55 No.2 739-749, (2014).
- [9] scikit-learn, “scikit-learn: machine learning in Python scikit-learn 0.19.1 documentation”, <<http://scikit-learn.org/stable/index.html>>, (2018/06/20 参照).