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

彭 龍† 渡邊 裕司†

†名古屋市立大学 システム自然研究科
467-8601 愛知県名古屋市瑞穂区瑞穂町川澄 1
houryu@nsc.nagoya-cu.ac.jp

あらまし スマートフォンに入っている大切な個人情報は，不正使用によってとかく漏れやすい．そこで筆者らは，スマートフォンにおけるユーザ認証の一手段として，スマートフォンに搭載された加速度センサを用いて歩行時のユーザを認証するシステムを検討している．既存研究では，加速度データから抽出した 43 個の特徴に対して，分類アルゴリズム（決定木とニューラルネットワーク）を用いて特定ユーザかそうでないかを判別し，90%以上の認証精度を達成した．本稿では，既存研究で検討が不十分な特徴と分類アルゴリズムについて詳細に比較した．その結果，判別にあまり貢献しない特徴や分類アルゴリズムによって精度が大きく変わることなどを確認した．

A Study on authentication at the time of the walk of using the acceleration sensor of smartphone

Ryu Hou† Yuji Watanabe†

†Nagoya City University Graduate School of Natural Sciences
Kawasumi, Mizuho-cho, Mizuho-ku, Nagoya-city,
467-8601, JAPAN
houryu@nsc.nagoya-cu.ac.jp

Abstract Important personal information contained in smartphone is easy to leak by the unauthorized use. As a method of user authentication, we examine the system for authenticating the user by the acceleration sensor installed in smartphones during walk. In the existing research, for 43 features extracted from the acceleration data, using 2 classification algorithm, it was determined whether or not the specific user, and then authentication accuracy of 90% has achieved. In this paper, we compare these features and classification algorithms in detail which the previous paper did not deal with.

1　はじめに

爆発的に普及したスマートフォンなどの携帯情報端末には多くの重要な個人情報が含まれるが，これらの情報は不正使用あるいは不注意からとかく漏れやすい．そのために，パスワード認証や指紋・顔画像など生体的特徴を用いたバイオメトリクス認証が一般的に行われている．しかし，これらの認証はログイン時に一度だけ行われることが多く，ログイン後には正規ユーザだけでなく不正使用者も自由にアクセスできてしまう．ログイン後にも認証のために何度もパスワードを再入力させることは，ユーザを煩わせるだけである．

そこで，ユーザを煩わせることなくログイン後も認証可能な方法として，個人の行動・操作の特徴や癖を用いた「行動的特徴に基づく生体認証」がある．この認証では，通常時の正規ユーザの行動や操作から特徴を表すプロファイルを作成し，そのプロファイルと現在の行動との間に著しい相違があれば，不正使用として警告する．そのためログイン後も継続的に監視することができる．ただし問題点として，ユーザの作業や心理状態などの影響を受けやすく誤報が多いこと，認証すべき人数が増加するにつれて認証精度が悪くなることなどが挙げられる.パソコンに対しては，キーストロークやコマンド列やマウス操作などに基づく認証研究が 1990 年代から広範に行われている．一方，携帯電話やスマートフォンにおける行動的特徴による認証研究はまだ最近であるため,多くの研究[1-5]はログイン時の認証に着目し，ログイン後の認証を扱った研究は相対的に少ない．それは，ログインタスクは全ユーザに対して共通にできるが,ログイン後のタスクはユーザ毎に異なり，ログイン後の認証は難しくなるためである．その一方で挑戦し甲斐のある研究でもある．

そこで筆者らの研究室では，スマートフォンにおいてタッチパネル,加速度センサ,GPS センサなどの複数センサそしてスマートフォンやアプリケーション（以下アプリと略す）の使用履歴などから各ユーザの操作や行動の特徴を抽出し，ログイン後も継続的に個人認証するプロジェクトを進めている．先行研究[6]では,スマートフォンにおいてユーザのタッチ操作の特徴に着目した．その認証結果を文献[7]で発表予定であるが,タッチ操作だけでは良い精度を達成することは難しい．認証精度を改善する一つのアプローチとして，複数センサを用いてそれぞれ認証し，それらの認証結果を統合することが挙げられる．

本報告では，スマートフォンに搭載された加速度センサを用いて歩行時のユーザを認証することを検討する．スマートフォンに限らず加速度センサを用いた歩行や走行や階段昇降時のユーザ識別・認証の研究はすでにいくつか報告され，例えば Mantyjarvi ら[8]や Kwapisz ら[9]の研究がある．文献[9]では，Android アプリを使って取得した 3 軸加速度データから 43 個の特徴を抽出し,分類アルゴリズム（決定木とニューラルネットワーク）を用いて識別（36 人の被験者のうち誰かを判別）と認証（特定ユーザかそうでないかを判別）を行い，歩行と走行時には 90%以上の識別精度を達している．しかし，43 個の特徴と分類アルゴリズムについて検討が十分に行われていなかった．そこで筆者らは，加速度取得アプリを作成し，実験を行い，特徴と分類アルゴリズムについて詳細に比較した．その結果，判別にあまり貢献しない特徴や分類アルゴリズムによって精度が大きく変わることなどを確認した．

2　加速度センサを用いた歩行時の認証

2.1　歩行時の加速度取得アプリ

まずユーザの歩行時の 3 軸加速度センサ値を取得するために，加速度取得アプリを iOS 上で作成した．スマートフォンの 3 軸方向を

図 1 に示す．Kwapisz らの研究[9]に倣って，50ms のサンプリング周期つまり 1 秒間に約 20 個の各軸の加速度データを計測する．そして，その時系列データに対してオーバーラップを許さないサイズ 200（約 10 秒に相当）のウィンドウに分割し，各ウィンドウに含まれるデータから特徴を抽出する．

図 1:スマートフォンの 3 軸方向

2.2 特徴の抽出と分類

各ウィンドウの各軸 200 個のデータから抽出する特徴は，まずは既存研究[9]と同様に以下の 43 個とする．ここで x_i，y_i，z_i はウィンドウ内の i 番目の各軸の加速度を表す．

- 平均値（3 軸）：$\bar{x} = \sum_{i=1}^{200} x_i/200$
- 標準偏差（3 軸）：$\sqrt{\sum_{i=1}^{200}(x_i - \bar{x})^2/200}$
- 平均絶対偏差（3 軸）：$\sum_{i=1}^{200}|x_i - \bar{x}|/200$
- 平均合成加速度：$\sum_{i=1}^{200}\sqrt{x_i^2 + y_i^2 + z_i^2}/200$
- ピーク間の時間（3 軸）：歩行時には加速度は正弦曲線のような波形の繰り返しがみられるため，ピーク間の時間を求める．実際には，200 個のデータ中の最大値を 1 個目のピークとして，この最大値のあるパーセント（例えば 95%）を超える値があるかどうかを調べ，あればそれを 2 個目のピークとし，なければパーセントを下げる．最低 3 個のピークが見つかるまで続ける．そして連続したピーク間の時間を求めて平均する．
- ビン分布（3 軸×10 個）：200 個のデータ中の最大値から最小値を引くことで範囲を求め，その範囲を 10 個の等しい大きさのビンに分割する．200 個のデータそれぞれがどのビンに入るかを数え，各ビンのデータの割合を求める．

認証つまり本人かそうでないかを分類するために，これら特徴に分類アルゴリズムを適用する．分類アルゴリズムとして，WEKA のデータマイニングソフト[10]を用いる(文献[9]では決定木（J48）とニューラルネットワーク（NN）だけを使用）．WEKA の設定はデフォルトのままとし，10 分割交差検証を用いる．

評価指標として，認証研究で一般的に使われる「他人受入率（False Acceptance Rate: FAR）」と「本人拒否率（False Rejection Rate: FRR）」を使用する．FAR とは，誤って他人を受け入れる割合であり，本人以外のデータ数に対して間違って本人とみなしたデータ数として求める．FRR とは，本人を誤って他人として拒否した割合であり，本人のデータ数に対して間違って他人とみなしたデータ数として求める．

3 実験結果

8 人の被験者に対して，作成したアプリを搭載した iPod touch をポケットに入れて歩いてもらうことで歩行時の 3 軸加速度値を記録する実験を行った．約 50m の長さの廊下を 5 往復してもらった（実験時間は 7，8 分）．歩き終わったら iPod touch を回収して加速度データを iTunes 経由で取得した．

まずは既存研究[9]と同様に，各被験者に対して決定木 J48 とニューラルネットワーク NN を適用した時の他人受入率 FAR(%)と本人拒否率 FRR(%)を表 1 に示す．分類アルゴリズム

においては，例えば被験者 A を本人とした場合,残りの被験者 B～D を他人とみなして適用した．FAR と FRR ともに小さいほど認証精度が良く,既存研究では最低でも一桁であり(さらに実用化のためには 0%に限りなく近いことが求められ)，文献[1]の加速度センサを用いたログイン時の 3D 動作認証では 1%未満の FAR と 1.5%未満の FRR を達成している．表 1 から FAR に関しては良い結果であるが，FRR についてはやや悪いことが分かる．また，決定木よりもニューラルネットワークを用いた方が特に FRR の改善が読み取れる．

表 1：各被験者に対して二つの分類アルゴリズムを用いた他人受入率 FAR と本人拒否率 FRR

被験者	決定木 J48		ニューラルネットワーク NN	
	FAR(%)	FRR(%)	FAR(%)	FRR(%)
A	0.4	0	0	0
B	0.4	13.9	0.8	8.3
C	1.2	11.1	0.4	0
D	0.8	5.6	0.8	8.3
E	0.8	5.6	0.4	8.3
F	0	2.8	0	0
G	0.4	16.7	0	2.8
H	0.8	13.9	0	2.8
平均	0.6	8.7	0.3	3.8

次に，文献[9]では 43 個の特徴が本当に必要かどうかについて触れられていないため，特徴を減らして認証精度が変わるかを調べた．8 人の被験者に対して平均した FAR と FRR を表 2 に示す．用いた分類アルゴリズムは，決定木 J48 とニューラルネットワーク NN である．結果から，平均値のみでも非常に良い精度であり，平均合成加速度やピーク間の時間はあまり判別に貢献していない（逆に悪影響を与えているかもしれない）といえる．ただし，平均値を除いた特徴を用いた場合は，表 1 より若干悪くなる程度である．

表 2：特徴を減らした場合の二つの分類アルゴリズムを用いた平均 FAR と平均 FRR

特徴	決定木 J48		ニューラルネットワーク NN	
	FAR(%)	FRR(%)	FAR(%)	FRR(%)
平均値のみ	0.3	4.9	1.0	2.1
標準偏差のみ	2.1	18.4	3.1	18.4
平均絶対偏差のみ	2.6	15.6	1.0	24.3
平均合成加速度のみ	1.3	84.0	0.4	85.8
ピーク間の時間のみ	1.5	91.7	1.3	93.8
ビン分布のみ	2.3	19.5	1.1	8.0
平均値なし	2.1	14.9	0.7	4.9

最後に，決定木とニューラルネットワーク以外の分類アルゴリズムについて検討する．WEKA のデータマイニングソフトには,56 個の分類アルゴリズムがあるため，それらすべてに対して 43 個の特徴を用いて FAR と FRR の 8 被験者の平均を求めた．紙面の都合上，表 3 に結果が良かった上位 3 アルゴリズムと悪かった下位 3 アルゴリズムの FAR と FRR を示す．この表から分類アルゴリズムによって精度が大きく変わることが確認できる．今回取得したデータに対しては，ニューラルネットワーク以外により良い精度を示す分類アルゴリズムがあることが分かった．

表 3：43 個の特徴に対して様々な分類アルゴリズムを用いた時の平均 FAR と平均 FRR

分類アルゴリズム	FAR(%)	FRR(%)
RBF Network	0.1	3.5
IB1	0.3	1.4
Decorate	0.2	4.5
・・・		
Grading	0	100
Stacking	0	100
Zero R	0	100

4 おわりに

本報告では，スマートフォンに搭載された加速度センサを用いて歩行時のユーザを認証することを検討した．既存研究で検討が不十分な特徴と分類アルゴリズムについて詳細に比較した結果，判別にあまり貢献しない特徴や分類アルゴリズムによって精度が大きく変わることなどを確認した．今後は，ポケットに入れるスマートフォンの向きを解決する必要がある．

参考文献

[1] 石原進，太田雅敏，行方エリキ，水野忠則，“端末自体の動きを用いた携帯端末向け個人認証”，情報処理学会論文誌，46(12)，pp.2997-3007，2005.

[2] J. Angulo and E. Wastlund, “Exploring Touch-screen Biometrics for User Identification on Smart Phones,” *IFIP Summer School*, 2011.

[3] S. B. Napa, A. Kowsar, I. Katherine, and M. Nasir, “Biometric-Rich Gestures: A Novel Aprroch to Authentication on Multi-touch Devices,” *CHI*, Austin, Texas, USA, 2012.

[4] 見上一憲，林原尚浩，“タッチパネルと加速度センサを用いた携帯端末向けジェスチャ認証とその入力方式の提案”，情報処理学会研究報告，CSEC-56(8), 2012.

[5] 居城秀明，金岡晃，岡本栄司，金山直樹，“タッチパネルによる手指の行動的特徴を用いた生体認証に関する一考察”，情報処理学会研究報告，CSEC-60(15), 2013.

[6] 渡邊裕司，市川俊太，“スマートフォンにおけるタッチ操作の特徴を用いた継続的な個人識別システムの検討”，コンピュータセキュリティシンポジウム，pp.797-804, 2012.

[7] Y. Watanabe, Houryu, T. Fujita, “Toward Introduction of Immunity-based Model to Continuous Behavior-based User Authentication on Smart Phone,” *17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems (KES2013)*, in press, 2013.

[8] J. Mantyjarvi, M. Lindholdm, E. Vildjounaite, S. M. Makela, and H. Ailisto, “Identifying users of portable devices from gait pattern with accelerometers,” *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp.973-976, 2005.

[9] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, “Cell Phone-Based Biometric Identification,” *Proc. of the 4th IEEE International Conference on Biometrics: Theory Applications and Systems*, pp.1-7, 2010.

[10] I. Witten and E. Frank, “Data Mining: Practical Machine Learning Tools and Techniques,” Morgan Kaufmann Publishers, 2005.