L-020

スマートフォンにおけるログイン後の個人認証の一考察：免疫型診断モデルの適用に向けて

A Study of User Authentication after Login on Smart Phone: Toward Application of Immunity-Based Diagnosis

渡邊 裕司† 彭 龍† 藤田 奨†
Yuji Watanabe Houryu Tsutomu Fujita

1. はじめに

スマートフォンなど多機能な携帯電話に含まれる多くの重要な個人情報は，不正使用者から守られなければならない．パスワード認証や指紋など生体的特徴を用いた認証は，一般的に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現実的ではない．ユーザを煩わせることなくログイン後も個人認証する方法として，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認証」がある．この認証では，通常時の正規ユーザの行動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，不正使用者として警告する．そのためログイン後も継続的に監視が行える．スマートフォンにおける行動的特徴による認証研究は最近始められつつある（例えば[1,2]）．しかし，多くの研究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まだ少ない．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るため，ログイン後の認証は難しくなる．その一方で挑戦し甲斐のある研究でもある．

そこで筆者らは，スマートフォンにおいてタッチパネル，加速度センサなどの複数センサから各ユーザの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システムを構築している．先行研究[3]では，ユーザのタッチ操作の特徴に着目し，簡易な文章閲覧アプリケーションで操作履歴を取得し，個人認証として使える操作特徴を検討した．

本報告では，タッチ操作に基づく認証および加速度センサを用いた歩行時の認証について予備実験の最新結果を示す．さらに，センサ統合手法として免疫型診断モデルの適用について考察する．

2. タッチ操作に基づく認証

2.1 操作履歴を取得する文章閲覧アプリ

先行研究[3]で作成したタッチ操作の履歴を記録するアプリケーション（アプリ）をまず説明する．ブラウジングは多くのスマートフォンアプリに備わった基本的機能の一つであることから，iOS 上で動く簡易な文章閲覧アプリ（テキストブラウザ）を作成し，ユーザが表示されたテキストを読むことでその操作履歴を継続的に記録する．画面の大きさは縦 480 ピクセル×横 320 ピクセルである．また，本ブラウザは縦方向のみのスクロール操作が可能であるため，「フリック」と「ドラッグ」の二つの操作によって縦スクロールする．なお，タップやピンチなど他の操作も取得可能なアプリの開発を Android 上（開発の制約が少なく，OS シェアが大きいため）で進めている．

既存のクラスを用いて画面上の座標位置を取得することが困難であるため，UITextView クラスを用いてテキスト上の座標位置を取得する．原点はテキストの左上に存在し，X 軸と Y 軸の範囲はともに用意するテキストの量に依存する．このアプリによって継続的に取得する「操作履歴」は，{*event*, (*x*, *y*), *t*}の形式である．ここで，*event* はタッチパネルに指が触れているときに呼び出される以下の三つのタッチイベントである．

1. 指をタッチした瞬間
2. 指を触れたまま動かしたとき
3. 指を離したとき

そして，(*x*, *y*)はタッチイベントを検出したときの座標位置，*t* はその検出時刻である．

2.2 特徴抽出と分類アルゴリズム

得られた「操作履歴」から個人認証のために抽出した「操作特徴」として，タッチした指に対して以下の基本的特徴を求める．

1. X 座標：縦スクロールであるため X 座標を集計
2. 移動距離：指をタッチした瞬間（始点）と指を離したとき（終点）の 2 地点間の距離を計算
3. 移動速度：移動距離を時間で割って速度を計算
4. 移動角度：2 地点間の移動角度を計算

継続的な個人認証のために，求めた 4 特徴の全データを，オーバーラップを許したサイズ *n* のウィンドウに分割し，ウィンドウ毎に各特徴の平均値と標準偏差を計算する．そして，認証つまり本人かそうでないかを分類するために，その平均値と標準偏差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，加速度センサを用いた認証研究[2]を参考にして，WEKA のデータマイニングソフト[4]から決定木（J48）とニューラルネットワーク（NN）を使用する．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）を求める．

2.3 予備実験結果

4 人の被験者に文章閲覧アプリを iPod touch で使用してもらい，操作履歴を取得する予備実験を行った．実験手順としては，まず被験者に iPod touch とアプリの操作方法を説明し，そのアプリを使って自由に文章を読んでもらった．読み終わったら iPod touch を回収して操作履歴を iTunes 経由で取得した．

†名古屋市立大学システム自然科学研究科，Graduate School of Natural Sciences, Nagoya City University

表 1 は，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 である．ウィンドウサイズ n は 10 である．FAR と FRR ともに小さいほど認証精度が良く，例えば文献[1]のキー操作に基づく認証では，約 2%の FAR と 0%の FRR を達成している．表 2 から被験者 A の FAR が悪く，被験者 B と C では逆に FRR が悪く，一方で被験者 D の精度は非常に良いというように被験者によって精度がかなり異なることが読み取れる．また，J48 よりも NN の方が良い精度であることも分かる．しかし，他の研究と比較すると十分に良い精度とは言えないため，認証に用いる操作特徴，分類アルゴリズムなどの要因を変えながら，精度向上を今後目指していく必要がある．

表 1　タッチ操作に基づく認証の結果

被験者	決定木 J48		ニューラルネットワーク NN	
	FAR(%)	FRR(%)	FAR(%)	FRR(%)
A	15.7	4.8	12.4	3.3
B	1.5	14	1.2	11.6
C	2.6	20.6	2.1	20.6
D	0	0	0.2	0
荷重平均	12	7.8	9.5	6.4

3. 加速度センサを用いた歩行時の認証

3.1 歩行時の加速度取得アプリと特徴抽出

単一センサによる悪い認証精度を改善する別のアプローチとして，複数センサを用いて，それらの認証結果を組み合わせることが挙げられる．そこで手始めとして，歩行時の 3 軸加速度を取得するアプリを iOS 上で作成した．加速度センサを用いた既存研究[2]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 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．

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[2]と同様に，平均値（3 軸），標準偏差（3 軸），平均偏差（3 軸），平均合成加速度，ピーク間の時間（3 軸），ビン分布（3 軸×10 個）の 43 個とする．これら特徴に分類アルゴリズムを適用し，認証性能を評価する．分類アルゴリズムには 2 節と同じく J48 と NN を使用し，評価指標には FAR と FRR を用いる．

3.2 予備実験結果

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 軸加速度を記録する予備実験を行った．実験では約 50m の長さの廊下を 5 往復してもらった（実験時間は 7~9 分）．歩き終わったら iPod を回収して加速度データを取得した．

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 を用いた場合の他人受入率 FAR と本人拒否率 FRR を表 2 に示す．表 1 のタッチ操作の結果と比べると，FAR と FRR ともに低い値であり（特に FAR は 0%に近い），より良い認証精度であるといえる．しかし，ここまでの手法は既存研究[2]に倣っただけであるが，その手法について十分に説明されていないところがあり，忠実に再現できているか不明である．特に既存研究にはポケットに入れたスマートフォンの向きをどう扱っているかの記述がなく，実際には座標変換が必要であるといえる．

表 2　加速度を用いた歩行時の認証の結果

被験者	決定木 J48		ニューラルネットワーク NN	
	FAR(%)	FRR(%)	FAR(%)	FRR(%)
A	0.8	0	0	0
B	1.2	8.3	1.6	5.6
C	0	2.8	0.4	2.8
D	0.4	11.1	0.8	8.3
E	0.8	5.6	0.8	8.3
F	0.4	2.8	0.4	0
G	2	8.3	0.4	5.6
H	0.8	5.6	0.4	2.8
荷重平均	0.8	5.6	0.6	4.2

4. 考察：免疫型診断モデルの適用に向けて

現時点では，タッチセンサと加速度センサからのそれぞれのデータに基づいて認証を試みているが，他のセンサとして GPS センサやマイクなどから認証用データを取得することも可能である．また，スマートフォンやアプリの使用履歴をもとに個人認証を試みることもできる．もし各センサに基づく認証システムが完成したら，各認証結果を統合する手法を検討しなければならない．

そこで，石田[5]によって提案された免疫型診断モデルの適用を試みる．この診断モデルでは，各センサノードは他のノードと相互にテストし，そのテスト結果をもとに各ノードが自分の「信用度」を更新して正常・異常を判定する．複数センサによる認証システムに免疫型診断モデルを適用すると，各センサに基づく認証システムそして最終的なメタ認証をノードとみなして，それぞれに信用度を割り当てる．各認証システムからメタ認証へのテスト結果には，認証結果を使う．そして各ノードの認証結果に信用度を重みづけたメタ認証の信用度を求め，あるしきい値以上であれば最終判定として不正使用であると警告を出す．また各認証システムの信用度は，相互テストと他の認証システムの信用度を用いて更新する．具体的な方法については今後の検討課題である．

参考文献

[1] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, “Keystroke-Based User Identification on Smart Phones,” Proc. of the 12th International Symposium on Recent Advances in Intrusion Detection, pp.223-243 (2009).

[2] 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).

[3] 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).

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

[5] Y. Ishida, “Fully Distributed Diagnosis by PDP Learning Algorithm: Towards Immune Network PDP Model,” Proceedings of International Joint Conference on Neural Networks, pp.777-782 (1990).