

スマートフォンの保持位置による 本人確認可能な SNS アプリケーション

吉田 亮雅^{1,a)} 宇田 隆哉^{1,b)}

概要：本研究では、スマートフォンの保持位置による本人確認可能な SNS アプリケーションについて考察する。スマートフォン向けアプリケーションを使用している間に取得したデータを機械学習により分類することで、個人を識別し、犯罪を未然に防ぐことを目的とする。最近、SNS のアカウントが乗っ取られたり、スマートフォンが本人ではない人に操作されたりすることを起因とした犯罪が多数起きている。そこで、実際に SNS を利用している最中のデバイスの傾きを Android に標準搭載されている加速度センサで取得し、機械学習によって分類を行うことで、実際にアプリケーションを利用している人が本人である確率を他のユーザが分かるようにする。それによって、様々な犯罪を未然に防ぐことができるのではないかと考える。

キーワード：個人識別, 機械学習, スマートフォン, SNS

SNS Application with Personal Identification by Holding Position of Smart Phone

RYOGA YOSHIDA^{1,a)} RYUYA UDA^{1,b)}

Abstract: We have developed a SNS application which can identify users by holding positions of smart phones. In our system, data by acceleration sensors of a smart phone are collected for preventing impersonation when users are using applications. We implemented an actual SNS application which can acquire the inclination of a smart phone by the sensors. We also evaluate the inclination data by machine learning. Users can see the validation rate of a person who is communicated with the users when they are communicating. We think that crimes by impersonation on SNS can be prevented by our system.

Keywords: Personal Identification, Machine Learning, Smart phone, SNS

1. はじめに

今日、我々はスマートフォンを用いて SNS を始めとした様々なアプリケーションを利用している。しかし、利用している SNS のアカウントのなりすましなどによる犯罪が多数起きている。一般的な SNS サービスではメールアドレスとパスワードによる本人確認を行っているものが多い。SNS はコミュニケーションツールであるため、アカ

ウントが乗っ取られて攻撃者に操作された場合、被害は本人に留まらない。例えば、友人から動画などの情報が紹介され、URL が送られてきた場合、その URL の先にあるものが安全なものとは限らない。また、ゲームなどのアプリケーションであれば、不正な課金につながる恐れがある。さらに、PayPay のように個人間で送金可能な仕組みも充実してきており、信頼のおける友人に金を貸したつもりでも、攻撃者に搾取されている可能性もある。かつては表現が不自然であった詐欺メールも、近年では進化しており、啓蒙活動やリテラシー教育だけで攻撃を防ぐことは限界を迎えている。

¹ 東京工科大学
Tokyo University of Technology
^{a)} c0118286ba@edu.teu.ac.jp
^{b)} uda@stf.teu.ac.jp

そこで、実際に SNS を利用している最中のデバイスの傾きを Android に標準搭載されている加速度センサで取得し、機械学習によって分類を行うことで、実際にアプリケーションを利用している人が本人であるかを確認できるようにしたい。画面をタップした時の押下や押上、保持している際のデバイスの傾きは個々人によって異なるため、分類できると考えられる。

本研究では、本人確認を 100% の精度で行うことを目指しているものではない。使用方法としては、SNS でコミュニケーションをとる際に、メッセージ送信者の本人識別率を受信者に通知することを想定している。本人かどうか疑わしい結果であっても、それがたわいのない内容であれば気にする必要はないし、URL が示されていた場合や、金銭に関わる内容であった場合には、その際の本人識別率を気にすればよい。本研究の目的は、SNS による詐欺被害の抑止にある。

2 章では関連研究について説明する。3 章では実際に加速度の値を取得するために利用したアプリケーションやサービス、端末の機能について説明する。4 章にて実際のデータ取得方法について述べる。5 章は実験結果、6 章は本論文の結論とする。

2. 関連研究

向井らの研究 [1] では特徴抽出用の Web ページに対して、スマートフォンのピンチイン、ピンチアウトを行わせることで個人を識別する手段を提案している。実験結果としてピンチインとピンチアウトのそれぞれの正解率は 0.98 以上、適合率と再現率は 0.80 を下回ることはなかった。従って、個人を識別する手段としては有用であるといえる。しかし、この研究の問題点は使用するスマートフォンの機種によって取得できるデータに差が出てしまうことや、ピンチインやピンチアウトの操作をあまり行わない環境では正規ユーザかどうかを判別するのに十分なデータをできない可能性があることである。

松島らの研究 [2] では Web ページの画面をスクロールする際のスマートフォンの加速度の値から個人を識別する手段を提案している。この研究ではデータを取得用の Web ページを決まった方向にスクロールした時の値を用いており、実際に 100% に近い値で個人を識別できている。従って、加速度の値は個人を識別するうえで有効な手段であると考えられる。

3. 加速度の値の取得に用いたツール

加速度の値を取得するにあたって利用したサービスやツールについて説明する。

3.1 Android に標準搭載されている加速度センサ

Android 端末には様々な種類のセンサが標準で搭載され

ている。その中でも今回は加速度センサを用いている。加速度センサは端末の x , y , z 軸方向の加速度を計測できる。それをアプリ内のメソッドにより呼び出し、加速度の値を取得する。

3.2 Firebase について

Google が提供しているモバイルおよび Web アプリケーションのバックエンドサービスである。アプリケーションから送信されたデータは JSON 形式のファイルとして保存している。今回の研究では加速度センサで取得したデータをアプリ内から Firebase に送信し、データを取得し終わった段階で JSON ファイルをエクスポートしている。

3.3 被験者に操作してもらうスマートフォン向けアプリケーションについて

Java を用いてプログラムした自作のアプリケーションを用いる。内容としてはスマートフォン向け SNS アプリケーションを模したものとなっており、アプリケーションを起動すると加速度の計測を開始し、指定した間隔で Firebase にデータを送信できるようになっている。また、また画面をタップした際に最初にポイントが検知されたときに “DOWN”，指を持ち上げた時に “UP” のラベルがつくようになっており、後に指定したラベルのデータを抽出できるようになっている。

4. 提案手法

2 章で述べたように、スマートフォンの操作や特定の環境に左右されずに個人を識別する手段が必要である。加速度の値は松島らの研究から手段として妥当であることに加え、ユーザのスマートフォンの操作方法によらないデータが取得できるため、本研究では実際に SNS アプリケーションの利用中の加速度の値によって個人を識別することを提案する。

本研究ではスマートフォンの加速度の値を取得し保存した後、データセットを作成する。それを用いて CNN により個人を識別する。

4.1 スマートフォンの加速度の取得と保存

本研究で取得する特徴はアプリケーションを利用している際のデバイスの傾きである。アプリケーションを起動すると同時に SensorManager クラスのメソッドを利用し加速度センサを起動する。

タッチアップした際に “UP”，タッチダウンした際に “DOWN” のラベルをつける。取得したデータは key を「ラベル, sensorX, sensorY, sensorZ, データ送信時刻」として HashMap に格納してから、Firebase に送信する。

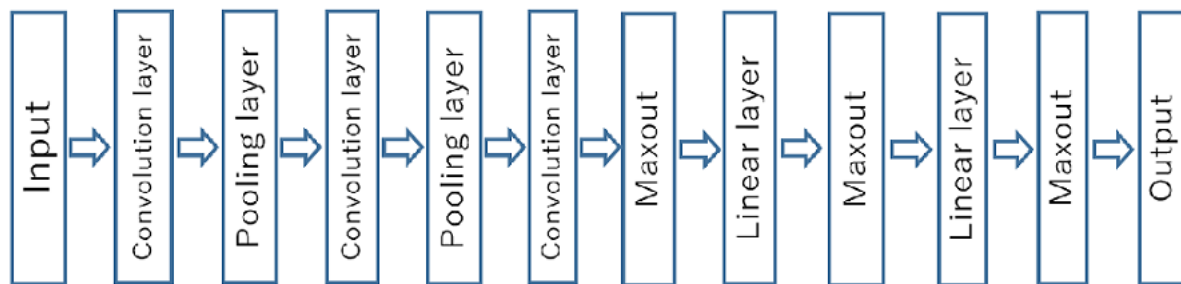


図 1 CNN の構成

4.2 データセットの作成

Firestore から取得した JSON ファイルを CSV ファイルに変換し、10 行ずつに CSV ファイルを分割する。なお、1 行の CSV ファイルの中には x, y, z 軸方向の加速度が 1×3 のサイズで格納されている。本実験では、片手のみでスマートフォンを操作してもらうため、被験者によっては画面の押す位置によって大きくデバイスが傾いてしまう。このようなゆらぎを排除するために、データの送信間隔が 0.2 秒であることから、2 秒毎のデータにするために 10 行ずつデータを分割する。

4.3 CNN による個人識別

作成したデータセットに対して機械学習による分類を行う。用いた CNN の構成を図 1 に示す。エポック 50, バッチサイズ 5 である。尚、以下の表 1 に示されているデータの内、3 分の 1 をテスト、3 分の 2 を訓練（トレーニング）に使用している。また、切り出し方の「全てのデータ」、「UP」の前後 10 行を削除、「DOWN」の前後 10 行を削除、「UP」の前後 10 行を抽出、「DOWN」の前後 10 行を抽出の順に“All”, “ReUP”, “ReDO”, “ExUP”, “ExDO”としている。

表 1 切り出し方によるデータの個数

	All	ReUP	ReDO	ExUP	ExDO
A	298	146	167	152	131
B	303	113	167	191	137
C	296	181	226	116	71
D	298	119	155	179	143
E	294	108	167	187	128
F	296	106	127	190	170
G	300	130	194	171	107
H	300	131	188	170	113
I	298	175	215	123	82
J	296	47	80	249	215
K	303	118	161	185	142

5. 実験結果

本節では具体的な実験内容と得られた結果について述べる。

5.1 実験の構成

本実験では、東京工科大学コンピュータサイエンス学部

コンピュータサイエンス学科の学生 11 人を被験者として行う。実験の流れは以下の通りである。

被験者には椅子（TOYOSTEEL : C-020448）に背もたれに軽く寄りかかってもらった状態で着席してもらう。そして利き手でアプリをインストールしたスマートフォン（モデル番号 : SC-04G）を 10 分間操作してもらう。この時も片方の手は膝の上に置いてもらい、スマートフォンは利き手のみで操作してもらう。また最初に持ってもらった位置からスマートフォンの位置は動かさず、画面をタップやキーボードの操作のみの動きを許すものとする。別の方法として、片手でスマートフォンをもち、もう片方の手で操作するときのデータを取得することも考えられたが、実際のアプリケーションの利用においては片手のみでスマートフォンを操作する状況も十分に考えられるため、このようにした。また、データの送信間隔についてだが、本研究の実験環境においては 0.2 秒よりも短い間隔でデータを送信しようとする、同じデータが複数送信されてしまうという問題点があったため、このような値とした。

5.2 結果

取得データ全体による F 値, FAR, FRR の平均値と標準偏差についての表を示す。尚、平均値を AVE, 標準偏差を SD としている。

表 2 データを切り出さない場合

	F1-score		FAR		FRR	
	Ave	SD	Ave	SD	Ave	SD
A	0.1378	0.0998	0.0521	0.0642	0.8505	0.1614
B	0.5982	0.1086	0.0585	0.0095	0.3248	0.1338
C	0.3936	0.1238	0.0654	0.0141	0.5838	0.1442
D	0.3161	0.0506	0.0326	0.0045	0.7495	0.0488
E	0.2738	0.0828	0.0561	0.0429	0.7245	0.1842
F	0.3819	0.1782	0.0632	0.0327	0.5657	0.2207
G	0.397	0.0644	0.0685	0.0274	0.568	0.1575
H	0.2128	0.0869	0.0655	0.0067	0.8	0.0869
I	0.4227	0.1209	0.0706	0.0415	0.5111	0.2022
J	0.2915	0.1857	0.0649	0.0495	0.6327	0.303
L	0.3806	0.1408	0.0837	0.0581	0.5069	0.2877
ave	0.346	0.112954545	0.061918182	0.031918182	0.619772727	0.175490909

次に、様々なデータの切り出し方による F 値, FAR, FRR の平均値と標準偏差についての表を示す。

表 3 “UP” のラベルの前後 10 行を削除した場合

	F1-score		FAR		FRR	
	Ave	SD	Ave	SD	Ave	SD
A	0.1677	0.1018	0.0425	0.0274	0.8583	0.1041
B	0.4399	0.0836	0.0736	0.0458	0.4595	0.2242
C	0.2828	0.0941	0.144	0.0663	0.6667	0.152
D	0.425	0.1814	0.0357	0.0301	0.5692	0.2759
E	0.081	0.043	0.012	0.0112	0.95	0.0272
F	0.1331	0.1438	0.0526	0.0752	0.8171	0.2218
G	0.5208	0.0826	0.0654	0.0192	0.4326	0.0827
H	0.1648	0.0819	0.0502	0.0512	0.8512	0.1015
I	0.554	0.0355	0.1519	0.0422	0.2207	0.1146
J	0.083	0.1257	0.0114	0.0135	0.9067	0.1555
K	0.6157	0.0659	0.0459	0.0107	0.3282	0.1472
ave	0.315254545	0.094481818	0.062290909	0.035709091	0.641836364	0.146063636

表 4 “DOWN” のラベルの前後 10 行を削除した場合

	F1-score		FAR		FRR	
	Ave	SD	Ave	SD	Ave	SD
A	0.1993	0.1265	0.0693	0.0583	0.76	0.2023
B	0.3765	0.1005	0.0408	0.0095	0.6655	0.1187
C	0.2897	0.1295	0.1536	0.0893	0.6053	0.2265
D	0.4991	0.0874	0.0502	0.0095	0.4745	0.1355
E	0.0935	0.0525	0.035	0.0316	0.9273	0.0563
F	0	0	0.0018	0.0011	1	0
G	0.4824	0.0785	0.0745	0.0255	0.4656	0.1557
H	0.2116	0.1756	0.0523	0.0249	0.7871	0.1984
I	0.5451	0.0354	0.1249	0.0293	0.262	0.1441
J	0	0	0.0082	0.0069	1	0
K	0.553	0.0272	0.0835	0.0191	0.2792	0.1122
ave	0.295472727	0.073918182	0.0631	0.027727273	0.656954545	0.1227

表 5 “UP” のラベルの前後 10 行を抽出した場合

	F1-score		FAR		FRR	
	Ave	SD	Ave	SD	Ave	SD
A	0.1271	0.1198	0.0192	0.0176	0.9	0.111
B	0.4682	0.101	0.06	0.0309	0.5206	0.154
C	0.1354	0.1813	0.0151	0.0178	0.8684	0.2038
D	0.2849	0.0964	0.0791	0.0397	0.6814	0.1627
E	0.3546	0.0475	0.0991	0.05	0.5839	0.1213
F	0.4347	0.1255	0.1105	0.0475	0.4095	0.257
G	0.1656	0.0748	0.0299	0.0205	0.8737	0.0651
H	0.1771	0.0327	0.1348	0.0595	0.7679	0.0714
I	0.1276	0.0722	0.0078	0.0087	0.9171	0.0609
J	0.546	0.0476	0.1625	0.0142	0.2169	0.0982
K	0.0875	0.0538	0.0182	0.0166	0.941	0.0471
ave	0.264427273	0.0866	0.066927273	0.029363636	0.698218182	0.122954545

表 6 “DOWN” のラベルの前後 10 行を抽出した場合

	F1-score		FAR		FRR	
	Ave	SD	Ave	SD	Ave	SD
A	0.2331	0.1648	0.0819	0.0624	0.6791	0.2612
B	0.5255	0.0679	0.0813	0.0321	0.3778	0.0629
C	0.1547	0.1681	0.0182	0.0072	0.8696	0.1455
D	0.2342	0.1197	0.0488	0.0344	0.7872	0.115
E	0.482	0.1056	0.0719	0.0226	0.4476	0.1463
F	0.4063	0.1853	0.1113	0.0668	0.4714	0.2798
G	0.2397	0.1567	0.0543	0.0456	0.6971	0.2906
H	0.1263	0.1372	0.0243	0.0148	0.8919	0.1378
I	0.0863	0.1127	0.009	0.0095	0.9333	0.0977
J	0.5172	0.0828	0.1522	0.0471	0.3296	0.1887
K	0.2398	0.0864	0.0376	0.0328	0.8	0.1223
ave	0.295009091	0.126109091	0.0628	0.034118182	0.662236364	0.167981818

また、各ラベルのデータの個数についての表を示す。尚、
“UP” または “DOWN” のラベルがついていない時のデータ
については “NONE” のラベルをつけている。

表 7 各ラベルのデータの個数

	UP	DOWN	NONE
A	161	120	2715
B	186	111	2751
C	99	52	2828
D	224	151	2611
E	205	135	2617
F	156	123	2695
G	138	76	2804
H	173	108	2739
I	146	71	2769
J	274	212	2481
L	228	153	2656

次に、各被験者毎の加速度の値の平均値と標準偏差につ
いての表を示す。上記の表の通り平均値を AVE、標準偏差
を SD と表記する。

表 8 加速度の値の平均値と標準偏差

	AVE			SD		
	x 軸	y 軸	z 軸	x 軸	y 軸	z 軸
A	-0.243635196	5.699730383	8.025723306	1.085558558	1.536134968	1.076320586
B	-1.788253443	2.447451086	9.31852758	1.128574087	1.693529101	1.164488516
C	0.138704166	5.434100064	8.118576424	1.071680291	1.369629254	1.081685993
D	-0.995730126	2.314950894	9.402469471	1.132141569	1.684733764	1.096476284
E	-1.2417466	5.955901809	7.598718887	1.110471083	1.175534903	1.069181982
F	-0.36071418	5.830911594	7.917032516	1.055494734	1.41165851	1.108845348
G	-0.414319064	4.913818159	8.525613415	1.10687652	1.599952453	1.120640398
H	-1.539507762	5.302771079	7.904540158	1.086232766	1.478867951	1.243246357
I	-0.967238646	6.430732755	7.291999509	1.043729683	1.369139097	1.109300882
J	-0.060307335	3.772205988	9.147167027	1.135301085	1.529350447	1.234622416
K	0.109506544	3.668712048	9.15008667	1.084684748	1.539468636	1.077724
ave	-0.669385604	4.706480533	8.40004136	1.094613193	1.489818098	1.125684796

6. 考察

この章では得られた結果に対する考察を述べる。

向井、松島らの研究では、被験者がデバイスに対して単
一的な動作を繰り返す中で得られた傾きのデータによって個
人を識別している。それに対し、本研究では被験者が 10 分
間の中で自由にデバイスを操作する中で得られた特徴に関
して分類を試みている。従って加速度の値のゆらぎが大き
くなり、分類の精度が低くなったと考えられる。向井、松
島らの研究で良いデータが得られたのはデバイスの操作が
単一的であることに起因すると考えられる。本研究のよう
に一定時間、自由に操作してもらおうという環境下ではデ
ータの切り出し方による大幅な精度の向上は見られなかつ
た。スマートフォンを片手で固定し、もう片方の手で操作
してもらおうと精度が向上するのではないかと考えられる。
また、仮に向井らの実験のように、一度も左手を下ろすこ
となく、右手でピンチインとピンチアウトを繰り返した場
合、スマートフォンの傾きは基本的に変わらない。しかし、
毎回腕を下ろしてスマートフォンを持ち直した場合、同一
人物でもスマートフォンの傾きが変わる可能性が大きくな
ると考えられる。つまり、本人である可能性は低くなる
と思われる。そのような点においてこれから改善の余地が
あると思われる。

6.1 ラベル毎の考察

データの切り出し方によって若干の値の変動はあるものの標準偏差を考えると誤差の範囲だと言わざるを得ない。

6.2 被験者毎の考察

表 3, 4 から “DOWN” のラベルの前後を削除した場合は被験者 F と被験者 J が本人だと分類されたデータは 0 であった。このことから、タッチダウンに個人の特徴が表れていると言える。また、表 7 から “NONE” のラベルがついている個数が一番少ない被験者 J がデータの切り出し方によっては比較的分類できていることが読み取れる。さらに、表 8 から被験者 J の加速度の値の標準偏差を見てみると、y, z 軸方向の値が比較的大きい。従って、タッチダウンの時に大きくデバイスが傾いている時に個人の特徴をよく抽出できていると言える。

x, y, z 軸方向の加速度の値のそれぞれの標準偏差のデータの範囲は 0.091, 0.518, 0.174 である。このことから、実験中に x, z 軸方向に比べて y 軸方向にデバイスが大きく傾いていることが分かる。また、標準偏差については、x, y, z 軸方向のいずれにしても、平均値に標準偏差を加味すると、過半数の値が他人の平均値を含む範囲となってしまう。従って同一被験者でも実験中にスマートフォンの持ち方が大きく変わっていると言える。

7. おわりに

本研究では、被験者の特徴を Android 端末の加速度センサによって取得し、得られたデータを様々な方法で抽出することで個人を識別することを試みた。全体的な分類精度は約 4 割弱程度であり、分類はあまりうまくいかなかった。

これからの展望として、計測方法を片手から両手に変更してみることやタップした位置の座標や Android に搭載されている他のセンサを用いることによる個人の特徴の抽出を試みることを検討している。

参考文献

- [1] Mukai, D. and Uda, R.: Personal Identification by Behavioral Features of Pinch-in and Pinch-out, IMCOM '18: Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication January 2018, Article No: 67, pp 1–5 <https://doi.org/10.1145/3164541.3164618>
- [2] Matsushima, H. and Uda, R.: Personal Identification by Tilt of Smartphone on Browsing IMCOM '18: Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication January 2018, Article No: 70, pp 1–5 <https://doi.org/10.1145/3164541.3164587>