

2 タッチストロークを用いた 1 クラス分類器によるスマートフォンの継続認証

大竹 知美[‡] 真部 雄介[†]

[†] 千葉工業大学情報科学部

[‡] 千葉工業大学大学院情報科学研究科

1 はじめに

スマートフォンの保有率は年々増加傾向にあり、総務省の調べ [1] によると 2019 年時点で世帯保有率 83.4% に達していることから、私たちの日常生活に必要不可欠なものとなっている。それに伴い様々なサービスが提供され、それらを利用するにあたり多くの個人情報保持されるようになった。そのため盗難にあった際に個人情報の漏洩や不正利用のリスクが極めて大きく、セキュリティ対策が重要となっている。しかし、現在の認証方法では 1 度ログインが成功してしまうと後は自由に操作可能となり、不正利用による被害を防ぐためにも重要なサービスにアクセスし続けるユーザを継続的に認証することが必要と考えられる。

そこで近年、追加のハードウェアや煩わしいインターフェースを使用しないことからタッチストロークを用いた継続認証に関する研究が行われている。

関連研究として、Xu らによりユーザが作成した複数種類のタッチデータをどのようにモデル化するかという問題をターゲットにした一連の方法を提案した研究が行われている [2]。この研究で挙げられた問題点のうち以下の 2 つに焦点を当てた。

1. SVM 等の識別において他人のユーザの選択がパフォーマンスに影響を及ぼす。
2. 1 タッチ操作だけではエラー率は依然としてゼロに近づかない。

そこで本研究では、問題点 1 に対するアプローチとして本人データのみで学習可能な 1 クラス分類器を使用する。また、問題点 2 に対するアプローチとして連続した 2 つのタッチストロークを 1 つの操作とみなし、ストローク間の時間による特徴も考慮することで精度等の改善がみられるか調査を行う。タッチ操作は、垂直方向 (上下) と水平方向 (左右) のタッチストロークの計 4 つを用いる。また、組み合わせの種類は 16 パターンを検討する。

2 提案手法

提案手法の概要と特徴抽出について述べる。

2.1 提案手法の概要

図 1 に提案手法における概要を示す。これは一般的な生体認証システムの構成に基づいており、主に登録フェーズと認証フェーズの 2 つの主要なフェーズから構成される。本研究では入力される一連のタッチ操作から順に

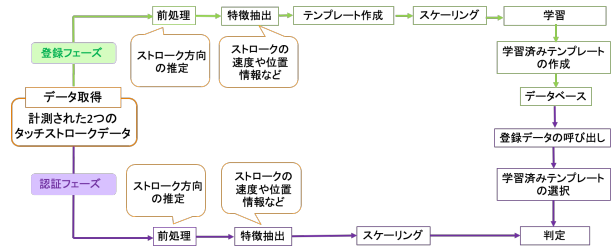


図1 提案手法の概要

2 つずつタッチストロークを取得し 1 つのタッチ操作としてまとめて特徴抽出等を行う。また、この一連のタッチ操作は上下左右方向の 4 つのストロークが無作為に入力されたものとするため、16 パターンのうちの組み合わせに該当するかを判断するため各フェーズの前処理にてストローク方向の推定を行う。

まず、登録フェーズについて説明する。取得されたデータよりストローク方向の推定を行う。次に、タッチストロークの速度や加速度等の特徴量を抽出し、テンプレートを作成する。このテンプレートは、2 つのタッチストロークそれぞれの特徴量とストローク間の時間を考慮した特徴量などを結合させた学習用データである。その後、テンプレートごとにスケールリングと学習を行い分類器において識別境界を決定し、学習済みテンプレートを作成、登録する。

次に、認証フェーズについて説明する。まず、データ取得後は登録フェーズと同様に前処理や特徴抽出を行い、認証用データの作成を行う。次に、登録データと同じスケールでスケールリングを行う。そして、登録されたデータの呼び出しを行い、学習済みテンプレートの選択をする。その後、学習済みモデルとのマッチングを行い、本人または他人の判定を行う。

2.2 特徴抽出

新たに追加した特徴量について述べる。本研究では Frank ら [3] のデータセット (被験者 41 人) を使用している。このデータセットは初日と 7~14 日後の 2 回のセッションに分けてデータが取得されており、 x 座標や y 座標、圧力、時間 [ms] 等から抽出された 28 次元の特徴量が含まれている。

今回追加した特徴量は 2 つの連続したタッチストローク間の時間と x 座標や y 座標から算出された始点や終点の位置情報から得られた距離より求めた速度や加速度、加えて 2 ストロークの合計時間等を算出した計 10 次元である。これらを追加したのはストローク間の時間にも個人を識別可能な特徴が含まれている可能性があると考えたためである。

2 つのタッチストロークを組み合わせた評価実験を行う際には、1 つ目のタッチストロークの 28 次元、2 つ目のタッチストロークの 28 次元、そして、ストローク間の時間を考慮した 10 次元をあわせた計 66 次元の特徴

Continuous Authentication of Smartphone with One-Class Classifiers Using Two Touch-Strokes

[‡]Tomomi OTAKE [†]Yusuke MANABE

[†]Faculty of Information and Computer Science, Chiba Institute of Technology [‡]Graduate School of Information and Computer Science, Chiba Institute of Technology

量を使用する。

3 評価実験

実験概要と結果を述べる。

3.1 実験概要

本実験では Frank データセットを使用する。スケーリングは標準化 (平均 0, 分散 1) を行った。また, 実験は Fierrez ら [5] によって示されている 3 つのシナリオに基づいている。各シナリオは以下の通りである。

1. intra-session: 同日に取得されたデータでモデルの作成と評価を行う。
2. inter-session: 1 回目のセッションデータでモデルの作成を行い, 2 回目のセッションデータで評価を行う。
3. combined-sessions: 2 つのセッションデータを使用しモデルの作成と評価を行う。

これらの各シナリオにおいて本実験では, 学習用に本人データ 40 個, 評価用に本人データ 10 個と他人データ 10 個の計 20 個を使用して評価を行う。そして, 本研究では以下の 2 つの評価実験を行った。

1. 1 タッチストロークにおける各 1 クラス分類器の性能比較
2. 1 タッチストロークと 2 タッチストロークの精度等の比較

実験 1 では, 上下左右 4 パターンのタッチストロークをそれぞれ使用し, 各 1 クラス分類器の性能比較を行う。実験 2 では, 上下左右 4 パターンの各タッチストロークを組み合わせた 2 タッチストロークの比較を行う。

今回使用する 1 クラス分類器 (OCC) は, Local Outlier Factor (LOF), Isolation forest (IF), One Class Support Vector Machine (OCSVM), Elliptic Envelope (EE) の 4 つである。これらの分類器を選択した理由としては文献 [4] にて異なる動作方法と明確な意思決定能力を持つと述べられ性能評価をする際に有用だと考えたためである。また, 評価は主に FAR (誤受率), FRR (誤棄却率), BER (平均エラー率) にて行う。BER は FAR と FRR の平均である。

3.2 実験結果

表 1 と表 2 の各方向における () 内の数値は条件にあるデータ数をもつ被験者数である。

表 1 に実験 1 の結果を示す。LOF と IF では FRR よりも FAR が高い結果となり, これは他のシナリオや方向でも同じような傾向がみられた。また, 各シナリオの比較を行うと LOF と OCSVM では intra-session に比べ inter-session のほとんどで 3%~12%BER が悪化し, inter-session に比べ combined-sessions では intra-session と同程度まで改善した。これは文献 [5] にて多クラス分類器を用いた場合の結果と似た傾向が 1 クラス分類器でもみられたことになる。

次に, 実験 2 の結果を表 2 に示す。LOF や IF では全体的に FAR の改善がみられ, right&right では FRR の改善もみられた。OCSVM では FAR と比べ FRR がかなり高い結果となった, EE に関しては悪化した。

表1 intra-session における実験 1 の FAR, FRR, BER の結果%(標準偏差)

dir	OCC	FAR	FRR	BER
up (8)	LOF	32.50(24.93)	20.00(15.12)	26.25(15.75)
	IF	67.50(26.05)	18.75(12.46)	43.13(16.24)
	OCSVM	2.50(4.63)	52.50(13.89)	27.50(7.56)
	EE	23.75(28.75)	47.50(25.50)	35.63(8.63)
down (41)	LOF	41.22(26.48)	12.93(11.46)	27.07(13.32)
	IF	67.78(23.79)	8.78(10.29)	38.78(12.79)
	OCSVM	4.63(9.51)	45.61(17.33)	25.12(9.91)
	EE	20.00(26.08)	38.29(25.49)	29.15(11.45)
left (38)	LOF	32.11(30.59)	17.37(12.89)	24.74(16.96)
	IF	53.42(31.39)	10.26(11.02)	31.84(16.04)
	OCSVM	1.32(3.43)	45.26(17.97)	23.29(9.03)
	EE	13.68(27.06)	47.11(23.24)	30.39(12.75)
right (38)	LOF	28.68(16.63)	18.95(16.57)	23.82(9.19)
	IF	50.26(27.36)	12.89(11.83)	31.58(13.51)
	OCSVM	2.11(4.13)	53.95(19.66)	28.03(9.69)
	EE	6.58(11.22)	51.58(24.33)	29.08(10.39)

表2 intra-session における実験 2 の FAR, FRR, BER の結果%(標準偏差)

dir	OCC	FAR	FRR	BER
up & up (1)	LOF	10.00(-)	0.0(-)	5.00(-)
	IF	30.00(-)	0.00(-)	15.00(-)
	OCSVM	0.00(-)	30.00(-)	15.00(-)
	EE	0.00(-)	100.00(-)	50.00(-)
down & down (41)	LOF	29.76(26.97)	19.27(13.85)	24.51(15.60)
	IF	53.17(29.53)	10.73(10.34)	31.95(15.20)
	OCSVM	3.17(7.56)	55.61(19.11)	29.39(10.20)
	EE	0.00(0.00)	99.51(2.18)	49.76(1.09)
left & left (11)	LOF	5.45(8.20)	28.18(18.89)	16.82(9.02)
	IF	26.36(29.76)	18.18(16.62)	22.27(14.55)
	OCSVM	1.82(4.05)	61.82(20.89)	31.82(10.79)
	EE	0.00(0.00)	100.00(0.00)	50.00(0.00)
right & right (13)	LOF	16.92(14.37)	13.08(9.47)	15.00(7.91)
	IF	40.77(27.22)	3.85(5.06)	22.31(12.85)
	OCSVM	2.31(5.99)	53.85(19.38)	28.08(8.79)
	EE	0.00(0.00)	99.23(2.77)	49.62(1.39)

4 おわりに

本研究では, 本人データのみを使用し学習を行い各 1 クラス分類器の性能を比較した。また, 新たな特徴量を加え連続した 2 つのタッチストロークを 1 つの操作とした場合の結果との比較を行った。その結果, 各分類器における傾向や FAR の改善がみられたものがあることを確認した。しかし, パフォーマンス向上のためには特徴量の見直しが求められる。また 16 パターンの組み合わせのうちデータが足りず評価実験を行えていないものがあるため他のデータセットでの調査も行う必要がある。

参考文献

- [1] 総務省: 令和 2 年版情報通信白書: 情報通信機器の保有状況, <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd252110.html>. (最終閲覧日: 2021.01.03)
- [2] H. Xu, Y. Zhou and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones", Proc. 10th Symp. Usable Privacy Secur., pp. 187-198, 2014.
- [3] M. Frank, R. Biedert, E. Ma, I. Martinovic and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication", IEEE Trans. Inf. Forensics Secur., vol. 8, no. 1, pp. 136-148, Jan. 2013.
- [4] R. Kumar, P. P. Kundu and V. V. Phoha, "Continuous authentication using one-class classifiers and their fusion", Proc. IEEE Int. Conf. Identity Secur. Behav. Anal., pp. 1-8, Jan. 2018.
- [5] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally and A. Morales, "Benchmarking touchscreen biometrics for mobile authentication", IEEE Trans. Inf. Forensics Secur., vol. 13, no. 11, pp. 2720-2733, Nov. 2018.