

スマートフォンにおける タッチ圧力を利用したアクティブ認証の実現

工藤 雅士^{†1} 森山 優姫菜^{‡2} 山名 早人^{‡3,4}

^{†1} 早稲田大学基幹理工学部 〒169-8555 東京都新宿区大久保 3-4-1

^{‡2} 早稲田大学大学院基幹理工学研究科 〒169-8555 東京都新宿区大久保 3-4-1

^{‡3} 早稲田大学理工学術院 〒169-8555 東京都新宿区大久保 3-4-1

^{‡4} 国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2

E-mail: [†] kudoma34@yama.info.waseda.ac.jp, [‡] {ymoriyama, yamana}@yama.info.waseda.ac.jp

あらまし スマートフォンの普及に伴い、重要なデータをスマートフォンで扱う場面が増えてきている。一方、スマートフォンではパスコード認証や指紋認証などの簡易な認証が用いられており、突破された例が多く存在する。これに対し、ログイン時の認証だけでなく利用時に継続的な認証を行う方法として「アクティブ認証」の研究が盛んになってきている。こうした背景のもと、我々はスマートフォンを対象としたアクティブ認証の精度向上に関する研究を進めてきている。本稿では、最近のスマートフォンで利用可能となった圧力センサーを新たな特徴量として用いることにより、アクティブ認証の精度向上を目指した。具体的には、タッチの強弱を感知できるタッチ圧力センサーを内蔵したデバイスを用いて、タッチ圧力値をアクティブ認証に利用する。評価実験では、複数の姿勢でスマートフォンを操作した際のタッチストローク情報を収集し、オンライン学習器 AROW により認証モデルの構築と評価を行った。精度評価の結果、13 ストローク毎の認証において 0.83% の EER (Equal Error Rate) を達成し、タッチ圧力値利用による EER の低減を確認した。

キーワード アクティブ認証, オンライン学習, タッチ圧力

1. はじめに

近年、スマートフォンは世界的に広く普及している。総務省の「通信利用動向調査」¹によると、2016 年における日本のスマートフォンの世帯保有率は 71.8% であり、スマートフォンは日本国内において高い保有率を誇っている。また、端末別のインターネットの利用状況はパソコンが 58.6%、スマートフォンが 57.9% であり、パソコンとスマートフォンの差は僅か 0.7% となっている。

スマートフォンはコミュニケーションツールや健康管理など、日常生活に役立つ機能を豊富に併せ持っている。そのため、現代の生活において無くてはならない存在となりつつある。スマートフォンはその多機能さや利便性から利用が増加する一方で、個人情報や生体情報といった重要なデータをスマートフォン上で扱う場面が増えてきている。近年では電子マネーを使った金融取引も増加し、個人情報を扱うだけでなく、個人資産の運用もスマートフォン上で行えるようになった。しかし、スマートフォンの操作開始時やインターネット上で個人情報を扱う場面において、さまざまな本人認証機能が利用されるが、指紋認証やパスコードに代表されるスマートフォンの認証機能はセキュリ

ティが甘く、第三者によって突破された例が多く存在する²³。認証突破による個人情報の漏洩を防ぐためには、第三者による再現性が低く模倣されにくい認証機能をスマートフォンに搭載する必要がある。

こうした背景のもとアクティブ認証に関する研究が盛んになっている。アクティブ認証とは、個人の行動的特徴を利用した認証機能であり、第三者によって再現されるリスクが低い。さらに、アクティブ認証は、ユーザの行動を継続的に監視して認証を行うため、不正な使用を素早く検知することができるという利点がある。例としては、スクリーンキーボード操作時のキーストローク情報を用いる認証[1]-[4]、フリックやピンチといったタッチジェスチャーを用いる認証[5][6]、画面操作時のタッチストローク情報を用いる認証[7]-[9]が挙げられる。また、著者らもアクティブ認証の研究を進めており、オンライン学習を取り入れたアクティブ認証を提案した[9]。

スマートフォンにおけるアクティブ認証では、内蔵するセンサーを利用してタッチ面積、タッチ座標、タッチ圧力といったタッチ情報を取得し、これらの特徴量として認証を行う。しかし、使用するデバイスによっては直接取得できないタッチ情報が存在する。特に、

¹ http://www.soumu.go.jp/johotsusintokei/statistics/data/170608_1.pdf

² 『日経 MJ (流通新聞)』2016.1.15, 「LINE、漏洩に用心—スマホの画面ロック機能、安全性は設定次第。」

³ 『毎日新聞』2017.8.10 大阪朝刊, 「詐欺：アップルペイで商品搾取 本人確認抜け穴 大阪など、6 容疑者逮捕」

タッチ圧力は直接取得できるデバイスが限られている。そのため、従来の研究では、他のタッチ情報から疑似的に算出した値をタッチ圧力値として使用する手法が用いられている。しかし、他のタッチ情報から疑似的に算出した値を認証に用いると、スマートフォンを操作する指やシチュエーションによって得られる値にばらつきが生じてしまい、認証精度が低下してしまう可能性がある。

そこで本研究では、タッチの強弱を感知できるタッチ圧力センサーを内蔵したスマートフォンを用いたアクティブ認証を提案する。タッチ圧力センサーでストローク中のタッチ圧力値を取得し、正確なタッチ圧力値アクティブ認証に利用することで、スマートフォンを操作する指やシチュエーションが変化した場合でも、常に正確な圧力値を認証に利用することができる。

本稿では次の構成をとる。まず、第2節でタッチストローク情報を用いたアクティブ認証の流れを説明し、第3節でアクティブ認証に関する関連研究をまとめ、第4節で提案手法について述べ、第5節で評価実験の結果を示し、第6節で本稿をまとめる。

2. アクティブ認証の流れ

タッチストローク情報を利用したアクティブ認証では、一般的に1) 本人登録、2) 本人認証、3) 分類器更新の3段階の処理フェーズが存在するとされている[10]。本節では、[10]に基づき、3段階の処理フェーズについてそれぞれ説明する。

2.1. 本人登録

本人登録フェーズでは、以下に示される4つの処理が行われる。

1. データ取得
2. データ前処理
3. 特徴量抽出
4. 分類器生成

デバイスに内蔵されたセンサーからタッチデータを取得し、タッチデータの品質や認証精度の向上を図るために異常値除去や正規化等の前処理を実行する。前処理が施されたタッチデータからユーザに共通の特徴を抽出し、ユーザのタッチ特性が判別可能な分類器を生成する。分類器の生成には通常、機械学習のアルゴリズムが用いられる。

2.2. 本人認証

本人認証フェーズでは、以下に示される2つの処理が行われる。

1. データ分類
2. 意思決定

第一フェーズの本人登録が完了した後、新たに取得されたタッチデータが本人のものであるかどうかの評価を行う。取得されたタッチデータを分類器に与え、評価結果を類似度スコアとして算出し、その値から本人であるかの識別を行う。

2.3. 分類器更新

ユーザのタッチ特性は、操作環境や時間とともに徐々に変化していく。タッチ特性の変化が大きくなると、分類器の誤認証を招く可能性がある。そのため、ユーザのタッチ特性の変化に対応できるように、一定の間隔で分類器の更新を行う操作が必要になる。分類器の更新方法としては、更新に用いるデータを一括で与え、バッチ学習によって分類器の再構築を行う方法と、更新に用いるデータを短い間隔で与え、オンライン学習によって逐次的に分類器の更新を行う方法が挙げられる。バッチ学習は全体の誤差を直接最小化するため、ノイズや外れ値に強いが、短期的な行動的特徴の変化に対応しにくいという欠点がある。一方で、オンライン学習は逐次的に分類器の更新を行うため、短期的な行動的特徴の変化に対応可能であるが、ノイズや外れ値が連続した場合、性能が著しく低下する可能性がある。

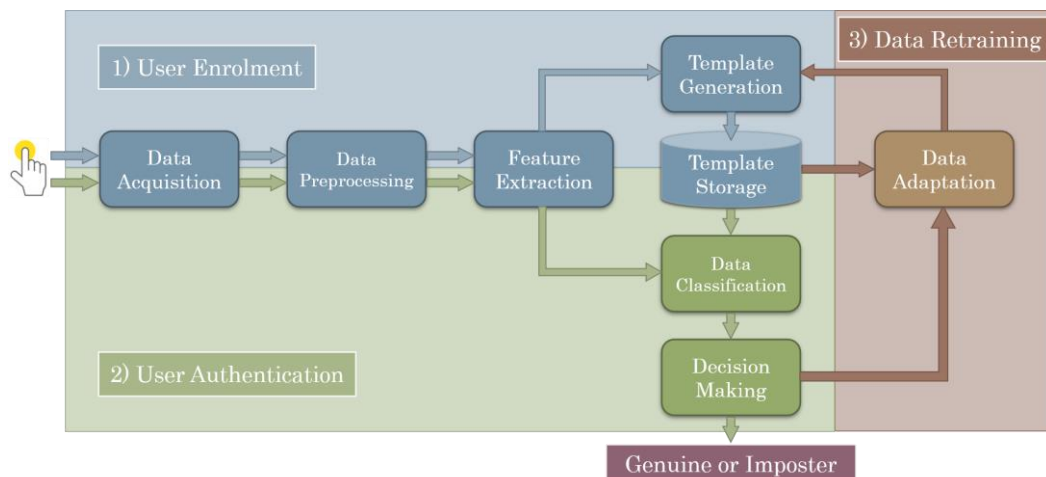


図 1 アクティブ認証の全体像 ([10]の Fig. 3 をもとに作成)

3. 関連研究

本節では、タッチ情報を利用したアクティブ認証に関する研究について述べる。

3.1. キーストロークを利用した認証

Carnegie Mellon University の Killourhy ら[2]は、2009 年に 51 人の被験者から 400 回パスワード入力を行った際のキーストローク情報を収集し、収集したキーストローク情報から分類器の構築を行った。評価実験の結果、9.6%から 10.2%の EER(Equal Error Rate)を達成した。University of Lincoln の Teh ら[3]は、2012 年にパスワード認証とキーストローク認証を統合した認証機能を提案している。特徴量として使用する「パスワード入力時におけるキーを押した時間」と「離れた時間」の 2 つの指標の最適な組み合わせを導出し、最大 1.4%の EER を達成した。

以上のようなキーストロークを利用した認証は、タッチキーボード使用時のみに適用可能であり、常時継続的に認証を行うことはできないという問題がある。

3.2. タッチジェスチャーを利用した認証

University of Houston の Zhao ら[5]は、2014 年にスマートフォンで一般的に使用されるタッチジェスチャーを接触軌道と接触圧力を基に画像化し、画像の類似度によって認証を行う手法を提案した。認証システムにオンライン学習を利用することで、認証時間の削減と短期的なタッチジェスチャーの変化への対応を実現し、有用性を実証した。Tanta University の Ramadan ら[6]は、2017 年にタッチ入力を監視し、ストロークレベルでの認証と、タッチジェスチャーをひとまとまりとして捉えるセッションレベルでの認証の比較を行った。その結果、セッションレベルでの認証がより利便性があると結論付けた。

以上のようなタッチジェスチャーを利用した認証は、認証に使用するジェスチャー毎にトレーニングデータが必要になるため、本人登録において用意すべきデータの数が多という問題がある。

3.3. タッチストロークを利用した認証

本項では、本研究と同様にタッチストローク情報を利用した研究を、バッチ学習を利用した研究[8]とオンライン学習を利用した研究[9]に分けて述べる。

3.3.1. バッチ学習を利用した認証

University of Michigan-Flint の Palaskar ら[8]は、2016 年に長期的にデバイスを使用すると操作方法に変化が生じて分類器の認証精度が低下するとし、定期的に再訓練を行う再訓練型分類器モデルを提案した。本モデルでは、表 1 に示されるタッチストローク情報を特徴量に使用し、300 ストロークごとにバッチ学習で分類器の更新を行う。独自の写真マッチングゲームで被験者 31 人からタッチストローク情報を取得して

認証実験を行った結果、9 ストローク毎の認証で 3.68% の EER を達成した。Palaskar らのバッチ学習による再訓練モデルでは、短期的な行動的特徴の変化に迅速に対応できないという欠点がある。

表 1 Palaskar らが抽出した特徴量
([8]の Table I をもとに作成)

Features	Description
StartX, StartY, StopX, StopY	ストローク開始・終了時のXY座標
StartPressure, StopPressure	ストローク開始・終了時の圧力
MidPress	ストロークの中間地点における圧力
AverageVelocity	ストローク中の平均速度
Vel20, Vel50, Vel80	ストロークの20/50/80%地点におけるストローク速度
StrokeDuration	ストロークにかかった時間
InterStrokeTime	ストローク間隔の時間
Length_EE, Angle_EE	ストロークの開始地点と終了地点の距離及び角度
Length_Trj	ストローク軌跡の長さ
Ratio_Trj2EE	ストローク開始・終了時の距離と軌跡の長さの比
Direction	ストロークの方向

3.3.2. オンライン学習を利用した認証

著者らの先行研究である Waseda University の石山らの研究[9]では、2018 年に姿勢や持ち方の違いによる行動的特徴の変化に対応するために、アクティブ認証を 1)分類器による認証、2)顔認証などの高度な認証の 2 段階で行い、オンライン学習によって逐次的に分類器を更新するシステムを提案した。石山らは、表 1 に示される Palaskar らが使用した特徴量に、表 3 に示されるストローク中のタッチ情報を追加し、オンライン学習器 AROW[11]のアルゴリズムを用いて分類器の構築を行った。また、分類器の判定だけではノイズや外れ値に弱いとして、分類器の判定結果を逐次的に多数決する決戦投票モデル(図 2)を提案した。独自の写真マッチングゲームで被験者 20 人からタッチストローク情報を取得して認証実験を行った結果、13 ストローク毎の認証で 1.8%の EER を達成した(表 2)。石山らの研究では、デバイス自体にタッチ圧力を取得できるセンサーが存在しない。そのため、タッチ圧力情報はタッチ面積などの情報から疑似的に算出した値が用いられており、正確なタッチ圧力情報であるとは言えない。

表 2 石山らによる認証実験の評価結果
([9]の表 4 をもとに作成)

Dataset	Training	Test		EER (%)
	Posture	Posture	Posture	
(a)	stand	sit	stand	1.9
(b)	sit	stand	sit	1.8

表 3 石山らが追加した特徴量
（[9]の表 2 をもとに作成）

Features	Description
StartTouchMajor, StartTouchMinor, StopTouchMajor, StopTouchMinor	ストローク開始・終了時において指が触れている楕円領域の長軸・短軸の長さ
X20, X50, X80, Y20, Y50, Y80	ストロークの20/50/80%地点におけるXY座標
TouchMajor20, TouchMajor50, TouchMajor80, TouchMinor20, TouchMinor50, TouchMinor80	ストロークの20/50/80%地点において指が触れている楕円の長軸・短軸の長さ

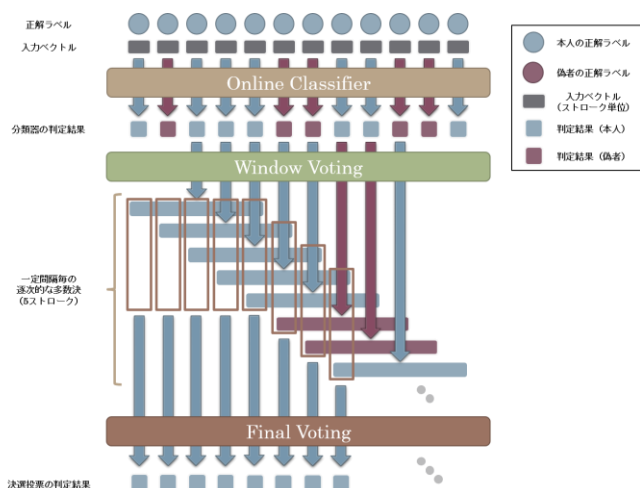


図 2 決選投票モデルの全体像
（5 ストローク毎の認証の場合）
（[9]の図 5 をもとに作成）

4. 提案手法

本節では、本研究で提案するタッチの強弱を感知できるタッチ圧力センサーを内蔵したスマートフォンを用いたアクティブ認証について詳しく述べる。

4.1. 提案概要

石山らの研究をはじめとするタッチストローク情報を利用した従来のアクティブ認証の研究[8][9]では、デバイスにタッチ圧力を取得できるセンサーが存在しない。そのため、タッチ圧力ではなく、タッチ面積を代わりに用いている。タッチ圧力とタッチ面積の関係に関して、Ochanomizu University の池松ら[12]は 2017 年に、スマートフォン上で親指を用いた 1 点のタッチ入力を行う場合の指の接触面積と内蔵センサーによって取得するタッチ圧力の差を検証する実験を行った。実験の結果、タッチ面積よりも内蔵センサーによって取得したタッチ圧力の方がより細かい刻み幅で値の取得が可能であることを示した。

そこで本研究では石山らの研究[9]をベースラインとして、タッチ圧力センサーを内蔵したデバイスを用いて、姿勢や持ち方といった操作シチュエーションによるタッチ情報の誤差が少なく、短期的な行動的特徴の変化に対応可能なオンライン学習型のアクティブ認

証を提案する。認証に用いる圧力を、タッチ面積からではなく、内蔵センサーから取得することで、操作シチュエーションに依存しない認証を実現する。また、認証を 1) 分類器による認証、2) 顔認証などの高度な認証の 2 段階で行うことにより、短期的な行動的特徴の変化に対応できる認証を実現する。なお、1 段階目の分類器による認証では、ベースラインと同様に決選投票モデルを使用する。本研究とベースライン研究では、使用デバイスの違いにより取得できるタッチ情報が異なるため、可能な範囲で条件を揃えて比較を行う。

4.2. 抽出する特徴量

本研究では、従来研究[8][9]と同様にスマートフォン内蔵センサーによってタッチ情報の取得を行う。本研究で取得するタッチ情報を表 5、表 4 に示す。各ユーザで、3 つの操作姿勢において特徴量毎に最大値と最小値を抽出し、その値に対してスミルノフ・グラブス検定を行い、外れ値除去を行った。また、取得した各タッチ情報にはスケールにばらつきがある。そのため、前処理として以下の式 (1) にてデータの最大値が 1、最小値が 0 となるようにユーザごとに正規化を行い、特徴ベクトルの生成を行う。各特徴量の正規化範囲を表 6 に示す。

$$x_{new} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (1)$$

表 4 本研究で使用するタッチ圧力情報

Features	Description
startPressure	ストローク開始時の圧力
stopPressure	ストローク終了時の圧力
midPressure	ストロークの中間地点における圧力
maxPressure	ストローク中の最大圧力
averagePressure	ストローク中の平均圧力

表 5 本研究で抽出する特徴量

Features	Description
startX, startY, stopX, stopY	ストローク開始・終了時の XY 座標
startPressure, stopPressure	ストローク開始・終了時の圧力
midPressure	ストロークの中間地点における圧力
averageVelocity	ストローク中の平均速度
vel20, vel50, vel80	ストロークの 20/50/80% 地点におけるストローク速度
strokeDuration	ストロークにかかった時間
interStrokeTime	ストローク間隔の時間
lengthEE, angleEE	ストロークの開始地点と終了地点の距離及び角度
lengthTrj	ストローク軌跡の長さ
ratioTrj2EE	ストローク開始・終了時の距離と軌跡の長さの比
direction	ストロークの方向
x20, x50, x80, y20, y50, y80	ストロークの 20/50/80% 地点における XY 座標
maxPressure	ストローク中の最大圧力
averagePressure	ストローク中の平均圧力

表 6 各特徴量の正規化範囲
(ユーザ毎に正規化)

Features	Normalization range	
	X _{min}	X _{max}
startX, startY, stopX, stopY	ストロークデータの最小値	ストロークデータの最大値
startPressure, stopPressure	0	6.66666*
midPressure	0	6.66666*
averageVelocity	ストロークデータの最小値	ストロークデータの最大値
vel20, vel50, vel80	ストロークデータの最小値	ストロークデータの最大値
strokeDuration	ストロークデータの最小値	ストロークデータの最大値
interStrokeTime	ストロークデータの最小値	ストロークデータの最大値
lengthEE	ストロークデータの最小値	ストロークデータの最大値
angleEE	ストロークデータの最小値	ストロークデータの最大値
lengthTrj	ストロークデータの最小値	ストロークデータの最大値
ratioTrj2EE	ストロークデータの最小値	ストロークデータの最大値
direction	1	2
x20, x50, x80, y20, y50, y80	ストロークデータの最小値	ストロークデータの最大値
maxPressure	0	6.66666*
averagePressure	0	6.66666*

*デバイスで取得できる最大値

4.3. オンライン認証システム

本研究ではベースライン手法[9]と同様に、アクティブ認証を1)分類器による認証、2)顔認証などの高度な認証の2段階で行い、オンライン学習によって逐次的に分類器を更新するシステムを採用している。そこで本節では、本研究で用いるオンライン学習を用いた認証手法について[9]を基に詳しく説明する。

4.3.1. オンライン認証システム

本研究では、まず事前に用意した訓練データからオンライン学習器 AROW[11]のアルゴリズムを用いて分類器の生成を行う。その後、逐次型のオンライン認証システムへと移行する。オンライン認証システムは以下の流れをとる。

1. オンライン学習器 AROW[11]による判定
2. 多数決投票 (13 ストローク間隔)
3. 決選投票

まず、1 ストローク毎にオンライン学習器による判定を行い、判定結果を多数決キュー (長さ 13) の末尾に格納する。オンライン学習器による判定結果が 13 ストローク分集まった段階で、多数決投票による判定を行う。多数決投票による判定結果は、決選投票キュー (長さ 13) の末尾に格納する。このとき、多数決キューが保持する判定結果が一定数に保たれるように、決選投票キューへの格納と同時に多数決キューの先頭要素の削除を行う。続いて、決選投票キューに判定結果が格納されたタイミングで決選投票を行い、決選投票の結果を最終的な認証結果とする。なお、決選投票キ

ューが保持する多数決投票による判定結果が 13 に達した段階で、決選投票キューの先頭要素の削除を行う。これらの操作を繰り返すことで、逐次的なオンライン認証を実現する。

4.3.2. 分類器更新

本研究では、アクティブ認証を1)分類器による認証、2)顔認証などの高度な認証の2段階で行う。4.3.1 項で説明した、1 段階目の分類器による認証の結果が「本人」であった場合は分類器の更新を行わずに認証を継続し、「偽者」であった場合は2 段階目の顔認証などの高度な認証へと移行する (図 3 ①)。2 段階目の高度な認証の結果が、1 段階目の分類器による認証の結果と異なる場合、分類器の更新を行う (図 3 ②, ③)。なお、本研究では2 段階目の高度な認証は研究の対象外とし、必ず正しい認証結果を出力するものとする。また、分類器の更新は最新 13 ストローク分のデータで行う。

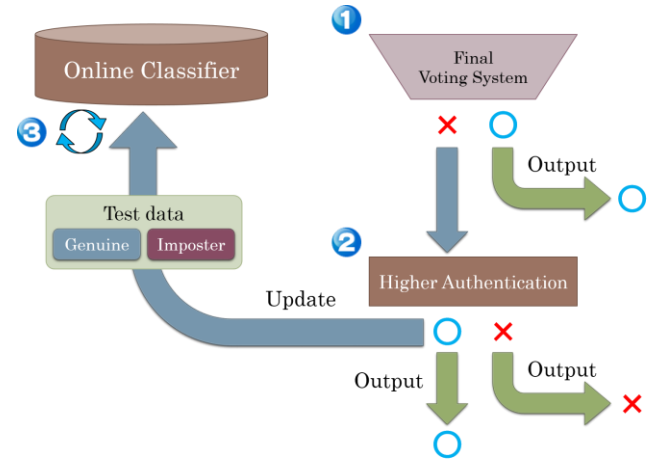


図 3 分類器更新の流れ

5. 評価実験

本節では、本研究で行った疑似的な評価実験について詳しく説明する。

5.1. データ収集

従来の研究[8][9]を参考に、本研究ではタッチストローク情報が取得可能な写真マッチングゲーム (図 4) を作成し、Apple 社製の iPhone 7 plus⁴ に本アプリケーションをインストールした。本アプリケーションのゲームの流れは以下の通りである。

1. ゲーム側：ランダムで正解画像を 1 枚設定する。
2. ユーザ：100 枚の写真リストをスクロールする。
3. ユーザ：正解画像と一致する画像を選択する。
4. ゲーム側：画像の確認画面を表示する。
5. ゲーム側：画面上に正誤を表示する。

⁴ <https://www.apple.com/jp/iphone-7/specs/>

1～5の一連の流れを1ゲームとし、7ゲーム終了した時点で1セッションとして区切り、操作姿勢の変更を行った。操作姿勢は1セッション毎に、座る姿勢(図5①)、立つ姿勢(図5②)、うつ伏せ姿勢(図5③)の順に変更を行い、各姿勢で4セッションずつ、計12セッション分のタッチストローク情報の収集を行った。タッチストローク情報は大学生21人(男性11人、女性10人)を対象とした被験者実験により収集した。本研究では、各姿勢で600ストローク以上のデータが得られた14人のユーザを十分なストロークデータが得られたユーザとし、以降で実施する認証実験において本人データセットを作成する対象とする。なお、偽者データセットを作成する際は本人を除いた20人のユーザを、データの抽出対象とする。



図4 写真マッチングゲームの流れ

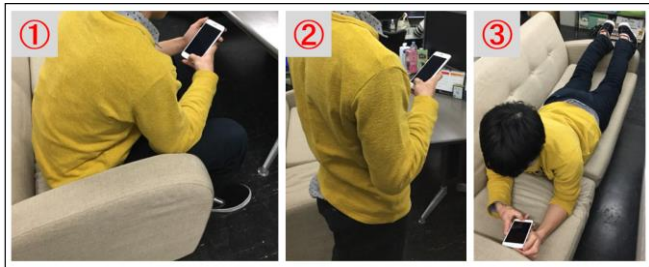


図5 3つの操作姿勢
(①座る姿勢, ②立つ姿勢, ③うつ伏せ姿勢)

5.2. 評価方法

本研究では、認証技術評価において一般的に用いられている等価エラー率(EER: Equal Error Rate)により認証の評価を行う。等価エラー率は本人拒否率(FRR: False Rejection Rate)と他人受入率(FAR: False Acceptance Rate)が等しくなる点におけるエラー率である。本人拒否率(FRR)と他人受入率(FAR)はそれぞれ以下の式(2)(3)で表される。

$$FRR = \frac{FR}{TA+FR} \quad (2)$$

$$FAR = \frac{FA}{TR+FA} \quad (3)$$

式(2)において、TA(True Acceptance)は本人を正しく受け入れた回数を示し、FR(False Rejection)は本人を間違えて拒否した回数を示す。式(3)において、TR(True Rejection)は偽者を正しく拒否できた回数を示し、FA(False Acceptance)は偽者を間違えて受け入れた回数を示す。

5.3. 実験データセット

本節では、疑似的な認証実験を行うために作成したデータセットについて述べる。

5.3.1. 1姿勢で訓練する実験データセット

1姿勢で訓練をして認証を行う場合、タッチ圧力情報の有無によって認証精度がどの程度変化するかを検証する実験データセットを作成した。座る姿勢、立つ姿勢、うつ伏せ姿勢の3つの姿勢それぞれにおいて、タッチストローク情報が600以上得られたユーザ14人に対して本人データセットを作成した。各本人データセットは、図6①に示される抽出方法で、タッチストローク情報に被りが生じないように連続したストロークを抽出して構築を行った。

続いて、本人データセットと対になる偽者データセットを、十分なタッチストローク情報が得られた14人に対してそれぞれ作成した。本人を除く20人のユーザから、図6②に示される抽出方法を用いて各姿勢15ストロークずつ均等に連続したストロークを抽出し、各偽者データセットの構築を行った。

作成した本人データセットと偽者データセットを基に、表7に示される実験データセットを作成した。認証間隔を13ストローク([9]と同一のストローク数)とし、表4に示されるタッチ圧力情報を特徴量を含む場合と含まない場合で被験者14人ごとにEERを算出し、EERの平均値で認証の疑似的な評価を行った。

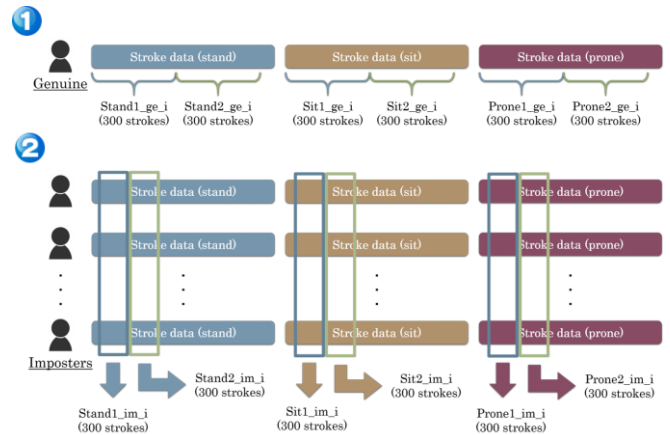


図6 ストロークデータの抽出方法(1)

表 7 実験データセット① (user_i)

Dataset	Training [Genuine]	Test [Genuine]		Total (stroke)
	Training [Imposter]	Test [Imposter]		
Dataset1_1_i	Stand1_ge_i	Sit1_ge_i	Stand2_ge_i	900
	Stand1_im_i	Sit1_im_i	Stand2_im_i	900
Dataset1_2_i	Stand1_ge_i	Prone1_ge_i	Stand2_ge_i	900
	Stand1_im_i	Prone1_im_i	Stand2_im_i	900
Dataset1_3_i	Sit1_ge_i	Stand1_ge_i	Sit2_ge_i	900
	Sit1_im_i	Stand1_im_i	Sit2_im_i	900
Dataset1_4_i	Sit1_ge_i	Prone1_ge_i	Sit2_ge_i	900
	Sit1_im_i	Prone1_im_i	Sit2_im_i	900
Dataset1_5_i	Prone1_ge_i	Stand1_ge_i	Prone2_ge_i	900
	Prone1_im_i	Stand1_im_i	Prone2_im_i	900
Dataset1_6_i	Prone1_ge_i	Sit1_ge_i	Prone2_ge_i	900
	Prone1_im_i	Sit1_im_i	Prone2_im_i	900

5.3.2. 複数姿勢で訓練する実験データセット

複数姿勢で訓練をして認証を行う場合、タッチ圧力情報の有無によって認証精度がどの程度変化するのかを検証する実験データセットを作成した。今回作成するデータセットは、5.3.1 項で作成したデータセットのトレーニングデータとテストデータの比率 (Training : Test = 1 : 2) と揃えるために、トレーニングデータを 180 ストローク、テストデータを 360 ストロークとして実験データセットの構築を行った。

5.3.1 項と同様に、十分なタッチストローク情報が得られた 14 人に対して、各々図 7 ①、図 7 ②に示される抽出方法で本人データセットと偽者データセットを作成した。

作成した本人データセットと偽者データセットを基に、表 8 に示される実験データセットを作成した。認証間隔を 13 ストローク ([9] と同一のストローク数) とし、表 4 に示されるタッチ圧力情報を特徴量に含む場合と含まない場合で被験者 14 人ごとに EER を算出し、EER の平均値で認証の疑似的な評価を行った。

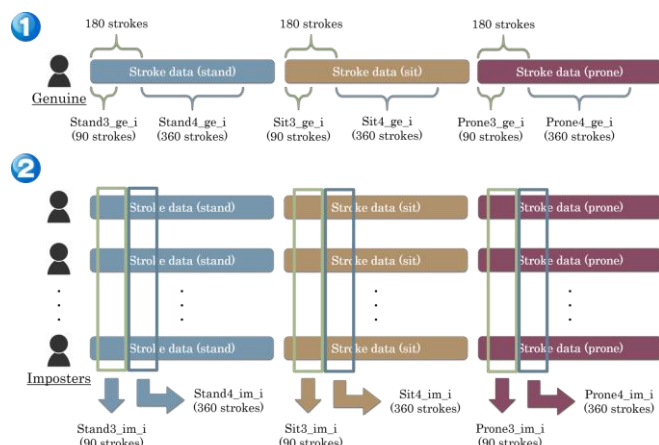


図 7 ストロークデータの抽出方法 (2)

表 8 実験データセット② (user_i)

Dataset	Training [Genuine]		Test [Genuine]	Total (stroke)
	Training [Imposter]		Test [Imposter]	
Dataset2_1_i	Stand3_ge_i	Sit3_ge_i	Stand4_ge_i	540
	Stand3_im_i	Sit3_im_i	Stand4_im_i	540
Dataset2_2_i	Stand3_ge_i	Sit3_ge_i	Sit4_ge_i	540
	Stand3_im_i	Sit3_im_i	Sit4_im_i	540
Dataset2_3_i	Stand3_ge_i	Sit3_ge_i	Prone4_ge_i	540
	Stand3_im_i	Sit3_im_i	Prone4_im_i	540
Dataset2_4_i	Sit3_ge_i	Prone3_ge_i	Stand4_ge_i	540
	Sit3_im_i	Prone3_im_i	Stand4_im_i	540
Dataset2_5_i	Sit3_ge_i	Prone3_ge_i	Sit4_ge_i	540
	Sit3_im_i	Prone3_im_i	Sit4_im_i	540
Dataset2_6_i	Sit3_ge_i	Prone3_ge_i	Prone4_ge_i	540
	Sit3_im_i	Prone3_im_i	Prone4_im_i	540
Dataset2_7_i	Stand3_ge_i	Prone3_ge_i	Stand4_ge_i	540
	Stand3_im_i	Prone3_im_i	Stand4_im_i	540
Dataset2_8_i	Stand3_ge_i	Prone3_ge_i	Sit4_ge_i	540
	Stand3_im_i	Prone3_im_i	Sit4_im_i	540
Dataset2_9_i	Stand3_ge_i	Prone3_ge_i	Prone4_ge_i	540
	Stand3_im_i	Prone3_im_i	Prone4_im_i	540

5.4. 実験結果

5.3.1 項で作成したデータセットを EER の平均値によって評価した結果を表 9 に示す。表 2(a), (b) と Dataset1_1, Dataset1_3 をそれぞれ比較すると、同一の組み合わせにおいて従来の研究よりも認証精度が向上することが示された。さらに、特徴量に正確な圧力情報を含む場合と含まない場合を比較すると、特徴量に正確な圧力情報を含む場合の方が認証の精度が高いことが示された。

続いて、5.3.2 項で作成したデータセットの評価結果を表 10 に示す。評価の結果、多くの場合で、特徴量に正確な圧力情報を含む場合の方が認証の精度が高いことが確認された。また、座る姿勢とうつ伏せ姿勢で訓練する場合が最も汎用性が高いことが示された。

表 9 認証の評価結果 (1 姿勢での訓練)

Dataset	Posture			EER (%)	
	Training	Test		w/ pressure	w/o pressure
Dataset1_1 *a	stand	sit	stand	0.83	1.15
Dataset1_2	stand	prone	stand	0.95**	1.61
Dataset1_3 *b	sit	stand	sit	0.61*	1.13
Dataset1_4	sit	prone	sit	0.68*	1.09
Dataset1_5	prone	stand	prone	1.15	1.27
Dataset1_6	prone	sit	prone	0.58*	1.18

*a 表 2 (a) と同じ姿勢の組み合わせ、*b 表 2 (b) と同じ姿勢の組み合わせ

* P<0.10 で有意、** P<0.05 で有意

表 10 認証の評価結果（複数姿勢での訓練）

Dataset	Posture			EER (%)	
	Training		Test	w/ pressure	w/o pressure
Dataset2_1	stand	sit	stand	0.90	<u>0.79</u>
Dataset2_2	sit	prone	stand	<u>0.14</u> **	0.67
Dataset2_3	stand	prone	stand	<u>0.62</u> *	0.95
Dataset2_4	stand	sit	sit	<u>0.75</u>	1.04
Dataset2_5	sit	prone	sit	<u>0.39</u>	0.83
Dataset2_6	stand	prone	sit	<u>0.43</u> **	1.08
Dataset2_7	stand	sit	prone	<u>1.02</u>	1.25
Dataset2_8	sit	prone	prone	<u>0.72</u> *	1.29
Dataset2_9	stand	prone	prone	<u>0.72</u>	0.91

* P<0.10で有意, ** P<0.05で有意

6. おわりに

タッチストローク情報を用いた従来のアクティブ認証の研究では、タッチ圧力を他のタッチ情報から疑似的に算出していたため、操作シチュエーションが変化した場合に正確な圧力を認証に利用することができず、認証精度が低下してしまう可能性があった。そこで本研究では、タッチの強弱を感知できるタッチ圧力センサーを内蔵したスマートフォンを用いたアクティブ認証を提案した。21人の大学生から取得したタッチストローク情報を用いて行った認証実験では、3つの姿勢の組み合わせを変えて認証の精度評価を行った。ベースライン手法と同じ姿勢の組み合わせで行った認証実験では、立った姿勢・座った姿勢・立った姿勢の組み合わせで0.83%、座った姿勢・立った姿勢・座った姿勢の組み合わせで0.61%のEERを達成し、タッチ圧力値利用によるEERの低減を確認した。複数姿勢で訓練をする認証実験では、座った姿勢とうつ伏せ姿勢で訓練をする場合が最も汎用性が高いことが示された。また、座った姿勢とうつ伏せ姿勢で訓練をして立つ姿勢をテストする組み合わせで最大0.14%のEERを達成した。

今後の課題としては、姿勢毎に適した圧力の扱い方を検討すること、疑似的に行った認証実験を実機上で行うことが挙げられる。

参 考 文 献

- [1] F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 367-397, 2002.
- [2] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," *Proc. Int' l Conf. Dependable Syst. Networks*, pp. 125-134, 2009.
- [3] P. S. Teh, S. Yue, and A. B. J. Teoh, "Improving keystroke dynamics authentication system via multiple feature fusion scheme," *Proc. Int' l Conf. Cyber Secur. Cyber Warf. Digit. Forensic, CyberSec 2012*, pp. 277-282, 2012.
- [4] K. R. Corpus, R. J. D. Gonzales, A. S. Morada, and L. A. Veal, "Mobile user identification through authentication using keystroke dynamics and accelerometer biometrics," *Proc. Int' l Work. Mob. Softw. Eng. Syst. - MOBILESoft '16*, pp. 11-12, 2016.
- [5] X. Zhao, T. Feng, W. Shi, and I. A. Kakadiaris, "Mobile user authentication using statistical touch dynamics images," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 11, pp. 1780-1789, 2014.
- [6] A. Ramadan, "Touch-Input Based Continuous Authentication Using Gesture-Level and Session-Level Features," *8th IEEE Annu. Inf. Technol. Electron. Mob. Commun. Conf.*, pp. 222-229, 2017.
- [7] C. Shen, Z. Cai, T. Yu, and M. O. E. Kli, "Touch - Interaction Behavior for Continuous User Authentication on Smartphones," *Int' l Conf. Biometrics (ICB)*, pp. 157-162, 2015.
- [8] N. Palaskar, Z. Syed, S. Banerjee, and C. Tang, "Empirical Techniques to Detect and Mitigate the Effects of Irrevocably Evolving User Profiles in Touch-based Authentication Systems," *IEEE 17th Int. Symp. High Assur. Syst. Eng.*, 2016.
- [9] T. Ishiyama and H. Yamana, "オンライン学習を用いたアクティブ認証の実現 - スマートフォンを対象として - Realization of Active Authentication for Smart Phone by Using Online Learning," *DBSJ Japanese J.*, vol. 16, no. 18, pp. 1-8, 2018.
- [10] P. Shen, N. Zhang, A. Jin, and K. Chen, "A survey on touch dynamics authentication in mobile devices," *Comput. Secur.*, vol. 59, pp. 210-235, 2016.
- [11] K. Crammer, A. Kulesza, and M. Dredze, "Adaptive regularization of weighted vectors," *Nips*, pp. 1-9, 2009.
- [12] K. Ikematsu, "タッチサーフェスにおける押下圧と接触面積を組み合わせた直接操作技法 Direct Manipulation Technique Using 3D Touch and Contact Size for Mobile Touch Surfaces," pp. 503-508, 2017.