DBSJ Japanese Journal
Vol. 16-J, Article No. 18, March 2018

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

石山 雄大♥ 山名 早人♦
Takehiro ISHIYAMA Hayato YAMANA

近年，スマートフォンの盗難・紛失によるデータ漏洩・不正アクセスの被害が増加している．この問題を防ぐために，アクティブ認証の研究が盛んに行われている．アクティブ認証とは，ユーザの行動から動きの癖などの特徴を抽出し継続的に認証する技術である．従来のアクティブ認証の多くはバッチ学習で構築した分類器を利用している．しかし，バッチ学習の場合，姿勢や持ち方の違いによる行動特徴の変化に対応することが難しい．そこで，本研究では行動特徴を逐次的に更新可能な分類器を構築することで，1）覗き見攻撃に強固，2）不正使用の早期検知が可能，3）行動特徴の変化にロバストなアクティブ認証システムを実現する．20 人の評価実験の結果，19 ストロークごとの認証間隔で 1.8%の EER(等価エラー率)を達成した．

In recent years, the damage of data leakage and illegal access by theft and loss of smartphones is increasing. To prevent this problem, active authentication system has been developed. Active authentication is the teqnique of continuously verifying the identity of a person based on behavioral features. Related works use classifier by batch learning. However, in the case of batch learning, it is difficult to respond to changes of behavioral features because of difference between postures and styles of holding. In this study, we consider three goals: 1) robustness to sholder attacks, 2) early detecting of illegal access, 3) robustness to changes of behavioral features. As a result of the evaluation experiment of 20 people, we achieved EER of 1.8% at the authentication interval every 19 strokes.

1. はじめに

近年，スマートフォンの普及が著しく，メインデバイスがPCからスマートフォンに移行している．総務省の「通信利用動向調査」[1]によると，平成26年におけるスマートフォンの世帯普及率は64.2%であり5年前から急速な普及が進んでいる．スマートフォンには，端末保有者の個人情報やインターネットサービスのアカウント情報など多くの重要なデータが保存されている．また，ネットショッピングや金融取引など，これまでPCからアクセスしていたサービスにスマートフォンからアクセスする機会が増えている．そのため，盗難や紛失によるデータ漏洩や不正アクセスの被害は甚大である．利便性に優れている反面，PCより盗難や紛失の危険性が高いため認証を強固にすることで被害を最小限に留める必要がある．

従来のスマートフォンの認証では，パスワードやPIN（Personal Identification Number）などのユーザの記憶情報が主に利用される．ユーザは利便性と覚えやすさから単純なパスワードやPINを設定する場合が多く，攻撃者は覗き見ることでこれらの情報を簡単に盗めてしまう[1]．覗き見攻撃を防ぐためにユーザしか持ち得ない身体的情報を利用する指紋認証を搭載したスマートフォンが近年増えているが，複製した指紋で不正に認証できることが報告されている[2]．これらの従来方式には，最初に認証されたユーザが依然としてそのスマートフォンを制御し続けているかどうかを検証するための仕組みが存在しない．こうした問題を解決するために，アクティブ認証という新たな認証方式が研究されている[2]．アクティブ認証は，ユーザの行動から動きの癖などの特徴を抽出し継続的に認証する技術である．行動特徴は覗き見られても再現することが難しく，また，継続的に認証するため不正使用の素早い検知に繋がる．スマートフォンにおけるアクティブ認証の研究では，スマートフォンに搭載された各種センサから行動特徴を抽出し認証モデルを構築する．認証モデルの構築には，本人データを正例，本人以外の偽者データを負例としたバッチ学習を用いる研究が盛んに行われている[3][4][5]．しかし，バッチ学習により分類器を構築する従来手法では，姿勢や持ち方の違いによる行動特徴の変化に対応することが難しい問題がある．

そこで本研究では，オンライン分類器による認証結果が偽者だった場合，顔認証などの高度な認証を行う．高度な認証の結果，オンライン分類器の認証が間違っていると判明したとき，オンライン分類器を更新する手法を提案する．なお２段階目の認証は本研究の対象外とし，正しく認証されるものとして扱う．バッチ学習ではモデルを再構築しない限り更新できないが，オンライン学習では試行毎にモデルを逐次的に更新することができる．また，オンライン分類器を利用した1ストローク毎の認証の際に発生するノイズによる誤分類を防ぐため，オンライン分類器による認証に多数決による投票を一定の間隔で連続的に導入する．行動特徴を逐次的に更新可能なアクティブ認証を構築することで，1）覗き見攻撃に強固，2）不正使用の早期検知が可能，3）行動特徴の変化にロバストな認証スキーマを実現する．

本稿では以下の構成をとる．まず2節にて関連研究を示し，3節にて本研究の提案手法を述べる．続く4節にて評価実験の結果を示し，最後に5節にて本稿をまとめる．

2. 関連研究

本節ではスマートフォンにおける行動学的特徴を利用したアクティブ認証の中でも，タッチ情報を利用した関連研究について述べる．まず 2.1 項でタッチ情報を利用した研究の概要を述べ，続く 2.2 項にてモデル更新の従来手法について説明する．アクティブ認証のモデル更新を動的に行う研究はこれまでになく，分類器の再訓練に最適な間隔を実験的に導出している Paraskar らの研究[5]に関して詳しく述べる．

2.1 タッチ情報を利用したアクティブ認証

♥ 非会員 早稲田大学大学院基幹理工学研究科
ishiyama@yama.info.waseda.ac.jp
♦ 正会員 早稲田大学理工学術院 国立情報学研究所
yamana@yama.info.waseda.ac.jp

[1] http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc372110.html

[2] http://gigazine.net/news/20160506-fake-fingerprint-break-phone/

行動特徴に基づいたアクティブ認証とは，ユーザの行動から動きの癖などの特徴を抽出し継続的に認証を行う技術である．スマートフォンにおけるアクティブ認証の研究では，タッチ情報から特徴を抽出し認証モデルを構築する研究が盛んに行われている[3][4][5]．これらの研究では，本人から取得したデータを正例，本人以外の偽者から取得したデータを負例とした教師あり分類器をバッチ学習で構築している．一般的なタッチ情報を利用したアクティブ認証システムの全体像を図 1に示す[2]．

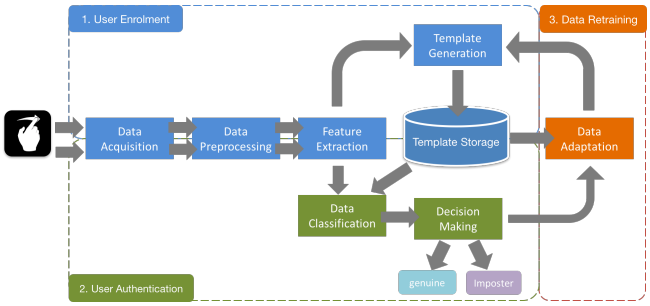

図 1 アクティブ認証システムの全体像（[2]の Fig.3 をもとに作成）

アクティブ認証システムは，1）本人登録，2）本人認証，3）モデル更新の 3 つの処理フェーズで構成される．本人登録は，ユーザのスマートフォン操作から特徴量を抽出し認証モデルを構築するフェーズである．本人認証フェーズでは，構築した認証モデルを利用し新たなタッチ情報が本人によるものかどうかを判定する．モデル更新フェーズでは，認証モデルが最新のデータから構築されるように再更新する．

2.2 アクティブ認証のモデル更新

2.1項にて説明したタッチ情報を利用するアクティブ認証は，バッチ学習を用いた分類器を構築する研究が多い[3][4][5]．これらの研究では，分類器を定期的に再訓練することで認証モデルを更新する．Palaskarら[5]は，タッチ情報の長期的な変化に対応するために最適な学習間隔を実験的に導出し，アクティブ認証のエラー率を軽減する手法を提案している．ユーザが長期的にデバイスを利用すると，デバイスやアプリケーションの使い方を習熟するため，タッチ情報に変化が起きる．この変化に対応するために最適な学習間隔を実験的に導出し，300ストローク毎の再訓練が最適だと報告している．タッチ情報から18の特徴量を抽出し，ランダムフォレストの分類器を構築している．Paraskarらが抽出した18の特徴量を以下の表 1にまとめる．31人の被験者から4週間にわたりタッチ情報を収集し，各被験者から912ストロークを取得した．収集したストロークから本人ユーザを正例，残りのユーザを負例とした分類器を構築する．分類器の判定結果を多数決する仕組みを導入し，認証間隔を1，5，9ストロークにずらし実験的に最適な間隔を決定する．31人の被験者データを利用した実験を行い，9ストロークの認証間隔で3.68%の等価エラー率（EER: Equal Error Rate）を達成している．しかし，バッチ学習における定期的な再訓練では，姿勢や持ち方の違いによる短期的な行動特徴の変化に対応できない問題がある．

表 1 Paraskar らが抽出した特徴量一覧（[5]の Table I をもとに作成）

トランザクションの種類	説明
StartX, StartY, StartPressure, StopX, StopY, StopPressure	ストローク開始・終了時の XY 座標
StrokeDuration	ストロークにかかった時間
Length_EE, Angle_EE	ストロークの開始地点と集雨量地点の距離及び角度
Length_Trj	ストロークの軌跡の長さ
Ratio_Trj2EE	開始地点と終了地点の距離と軌跡の長さの比
AverageVelocity	ストロークの速度
InterStrokeTime	ストロークの間隔時間
MidPress	ストロークの中間地点における圧力
Vel20, Vel50, Vel80	20/50/80%地点におけるストロークの平均速度
Direction	ストロークの方向（垂直/水平）

3. 提案手法

2.2 項で説明したバッチ学習による分類器では，姿勢や持ち方の違いによる短期的な行動特徴の変化に対応できない問題がある．この問題を解決するために，本研究では，Paraskar ら[5]の手法を拡張し行動特徴を逐次的に更新可能な分類器を構築することで，1）覗き見攻撃に強固，2）不正使用の早期検知が可能，3）行動特徴の変化にロバストなアクティブ認証システム実現を目指す．まず，3.1 項にてシステムの概要を説明する．続く 3.2 項にてデータ収集方法を述べ，3.3 項にて前処理を説明する．3.4 項にて本人かどうかを判定する分類器の構築に関して説明し，3.5 項にて構築した分類器を利用した本人認証の方法を述べる．3.6 項にて多数決による投票方法に関して述べ，3.7 項にて認証モデルの更新方法を説明する．

3.1 概要

2.2 項で説明した従来手法ではバッチ学習によって分類器を構築しているため，姿勢や持ち方の違いによる行動特徴の変化に対応することが難しい．そこで本研究では，Paraskar らの手法を拡張し，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，2 段階目の認証が成功したら 1 段階目の分類器を更新するシステムを提案する．なお 2 段階目の認証は本研究の対象外とし，正しく認証されるものとして扱う．

2 段階目の認証結果から 1 段階目の分類器を動的に更新するため，オンライン分類器 AROW (Adaptive Regularization of Weight Vector)[7]を利用する．バッチ学習ではモデルを再構築しない限り分類器を更新できないが，オンライン学習では試行毎にモデルを逐次的に更新できる．また，オンライン分類器を利用した 1 ストローク毎の認証の際に発生するノイズによる誤分類を防ぐため，オンライン分類器による認証に多数決の原理を一定の間隔で連続的に導入する．Paraskrar らの手法における認証モデルの全体像を以下の図 2 に，本研究で提案する認証モデルの全体像を以下の図 3 に示す．

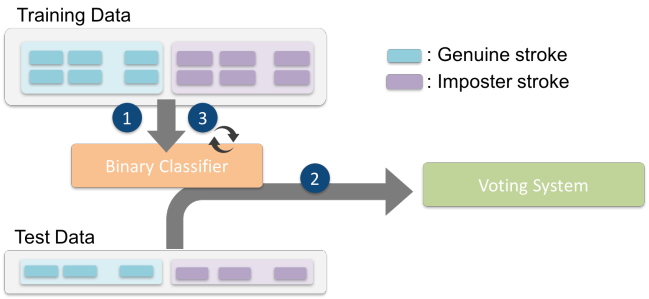

図2 Paraskar ら[5]の手法の認証モデルの全体像

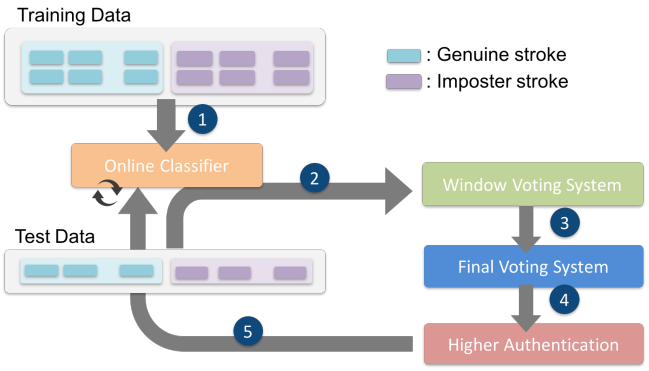

図3 提案手法における認証モデルの全体像

Paraskar らの研究[5]では，まず訓練データからバッチ学習で二値分類器を構築する（図 2-①）．分類器の結果を一定の間隔で投票し，最終的な判定結果とする（図 2-②）．分類器の更新は元々使用していたモデルを破棄し，1 から再構築する必要がある（図 2-③）．

提案システムでは，まず訓練データからオンライン分類器を構築する（図 3-①）．そして，分類器の結果を一定の間隔で投票し（図 3-②），それらの結果を決選投票して（図 3-③）最終結果とする．最終結果の判定で偽者と判断した場合，2 段階目の認証として顔認証などの高度な認証を実施する（図 3-④）．なお 2 段階目の高度な認証は本研究の対象外とし，正しく認証されるものとする．2 段階目の認証の結果，1 段階目の判定が間違っていた場合，オンライン分類器を更新する（図 3-⑤）．

3.2 データ収集

スマートフォンに搭載されるセンサを利用し，タッチ情報を取得する．取得するタッチ情報は，座標，圧力，タッチ領域の長さ（楕円の長軸・短軸），状態（指が触れた瞬間・指が触れている途中・指が離れた瞬間）とする．指がスクリーンに触れている間，数ミリ秒間隔でタッチ情報を収集する．指が触れてから離れるまでの状態を可視化したものを以下の図 4 に示す．

3.3 データ前処理

提案システムでは，ストローク単位で特徴ベクトルを生成する．ストロークとは，指がスクリーンに触れてから離れるまでの軌跡を表す．Paraskar らの研究[5]で使用している特徴抽出をベースに軌跡の情報を付け加える．具体的には，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，ストロークの 20/50/80%地点（図 4 に示す）における座標および指が触れている楕円の長軸・短軸の長さを追加する．本研究で追加した特徴量の内容を表 2 にまとめる．生成した特徴ベクトルが有する各特徴量はスケールにばらつきがあるため，データの最小値が 0，最大値が 1 になるように被験者ごとに正規化を行う．

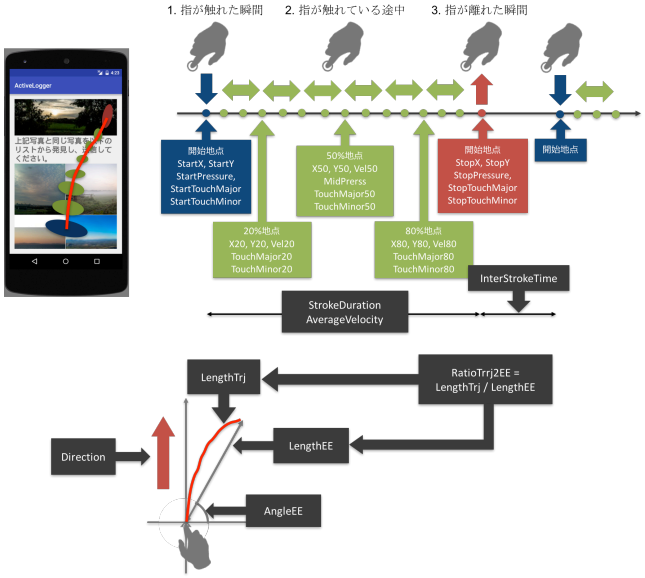

図4 提案手法における認証モデルの全体像

表2 本研究で追加した特徴量一覧

特徴量	説明
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	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

3.4 オンライン分類器の構築

3.3 項にて生成した特徴ベクトルを利用し，認証モデルを構築する．提案システムでは逐次的なモデル更新を必要とするため，認証モデルにオンライン分類器 AROW (Adaptive Regularization of Weight Vector)[7]を利用する．AROW は CW(Confidence Weighted Learning)[8]がノイズに弱いという問題を改善した手法である．t回目の学習において，学習用の入力ベクトル$\boldsymbol{x}_t$および正解ラベル$\boldsymbol{y}_t$が与えられたとすると，AROW は以下の式(1)に示す最適化問題を解くことで重みベクトル$\boldsymbol{w}$を更新する．

$$(\boldsymbol{\mu}_t, \Sigma_t) = \min_{\boldsymbol{\mu},\Sigma} D_{KL}\left(\mathcal{N}(\boldsymbol{\mu},\Sigma) \parallel \mathcal{N}(\boldsymbol{\mu}_{t-1}, \Sigma_{t-1})\right) + \frac{1}{2r} l_{h^2}(y_t, \boldsymbol{\mu}\cdot\boldsymbol{x}_t) + \frac{1}{2r} x_t^T \Sigma x_t \quad (1)$$

式(1)における$\mathcal{N}(\boldsymbol{\mu}_{t-1}, \Sigma_{t-1})$は$t$回目の学習による更新を行

う前の分布であり，$D_{KL}(\mathcal{N}(\boldsymbol{\mu},\Sigma) \| \mathcal{N}(\boldsymbol{\mu}_{t-1},\Sigma_{t-1}))$ は $\mathcal{N}(\boldsymbol{\mu},\Sigma)$と$\mathcal{N}(\boldsymbol{\mu}_{t-1},\Sigma_{t-1})$間のカルバック・ライブラー・ダイバージェンスである．式(1)の，$l_{h^2}(y_t,\boldsymbol{\mu}\cdot\boldsymbol{x}_t)$は二乗ヒンジ損失であり，この項を最小化することで，現在の学習データに対する予測の間違いをなるべく小さくするような更新を可能にする．式(1)の$x_t^T\sum x_t$を正則化項として加えることで，各重みの確信度を少しずつあげていくことを可能にする．ただし，$r>0$はモデルの更新を調節するハイパーパラメータである．上記で示した更新式をまとめると，AROW は，1) 今までの分布になるべく近い分布を探し，2) 現在の学習データを正しく分類し，3) 各特徴の確信度を少しずつ上げることで，ノイズが含まれる学習データにもロバストなオンライン学習を実現している．

3.5 オンライン分類器による判定

3.2 項および 3.3 項にて説明した，データ収集および前処理と同じ方法で特徴ベクトルを生成する．3.4 項にて構築したオンライン分類器 AROW に特徴ベクトルを入力し，入力した情報が本人かどうかを判定する．AROW による判定をシステム全体の判定とせずに，3.6 項にて説明する多数決を行うためのキューQ_{voting}に結果を保存する．また，入力する特徴ベクトルはオンライン分類器を更新する際に必要になるため，更新用バッファB_{update}に保存する．

3.6 多数決による投票

3.5 項にて述べたオンライン分類器の判定だけではノイズや外れ値に弱く，認証のエラー率が高くなってしまう．そこで，Paraskar ら[5]は，オンライン分類器の判定結果を一定の間隔ごとに多数決し最終的な認証結果としている．しかし，Paraskar ら[5]の手法では多数決の間隔が逐次的でないため，区切るタイミングによってエラー率が変動してしまう問題がある．この問題を解決するために，本研究では，オンライン分類器の判定結果を逐次的に多数決し，さらに結果を決戦投票するモデルを提案する．決選投票モデルの全体像を以下の図 5 に示す．

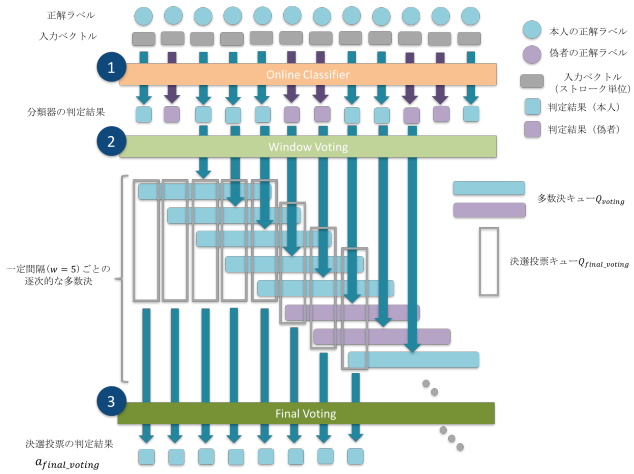

図 5 決選投票モデルの全体像

決戦投票モデルは，オンライン分類器の判定（図 5-①），結果を一定間隔ごとに逐次的に多数決（図 5-②），多数決の結果を決戦投票（図 5-③）する手順で行う．まず，オンライン分類器の判定結果を多数決キューQ_{voting}に格納する．多数決キューQ_{voting}の長さが一定の間隔長wに達した段階で，多数決キューQ_{voting}の中身で多数決を取る．w個のリストLで構成される決選投票キュー$Q_{final_voting}=\{L_1,L_2,\dots L_w\}$を用意し，多数決の結果を全てのリストに追加する．なお，多数決の結果を格納後，多数決キューQ_{voting}の先頭を削除し一定の間隔長lを保つようにする．また，多数決の結果を多数決キューQ_{voting}に格納したタイミングで，決選投票キューQ_{final_voting}の先頭（L_1）を取り出し決戦投票を行い最終的な判定結果a_{final_voting}とする．これらの操作を繰り返すことで，逐次的な認証を実現する．

3.7 分類器のオンライン更新

提案システムの認証モデルは，1) 分類器による認証，2) 顔認証などの高度な認証の 2 段階で構成する．3.6 項にて説明した多数決による決戦投票結果a_{final_voting}が偽者であった場合，顔認証などの高度な認証を要求する．なお 2 段階目の高度な認証は本研究の対象外とし正しい認証として扱う．1 段階目の分類器による認証結果が本人である場合，分類器のモデル更新は行わない．3.5 項にて説明したように，オンライン分類器による判定の際，入力する特徴ベクトルは更新用バッファB_{update}に保存する．多数決による決戦投票結果a_{final_voting}が間違っていた場合，更新用バッファB_{update}に保存されている特徴ベクトル群をオンライン分類器に入力しモデルを更新する．なお，モデルの更新は 3.4 項にて示した式(1)を用いて行う．

4. 評価実験

本節では，提案手法の有用性を評価実験にて示す．まず 4.1 項にて被験者実験によるデータ収集方法を説明し，4.2 項にて本研究の評価方法を述べる．続く 4.3 項にて実験結果に関して述べる．

4.1 データセット

Paraskar らの研究[5]では，被験者に写真マッチングゲームを行ってもらうことでタッチ情報を収集している．Paraskar らの研究を参考に，本研究では Flickr の API[3]を利用し，ランダムに選出した正解画像をリストから発見する Android アプリを作成した．正解画像をリストから探す時のスマートフォンの操作からタッチ情報を取得する．なおタッチ情報の収集は 3.2 項にて説明した方法で行う．被験者実験は日常的にスマートフォンを使用している大学生 20 名を対象とし，全ての被験者に同じデバイスを使用してもらった．普段と同じようなスマートフォンの操作を意識してもらい，座った状態および立った状態にて実験を行った．被検者実験の仕様および環境を以下にまとめる．

- 被検者数: 20 人
- 使用機種: Android Nexus 6P
  - ➢ディスプレイ: 2560 × 1440
  - ➢解像度: 515dpi
  - ➢サイズ: 159.3 × 77.8 × 7.3 mm

[3] https://www.flickr.com/services/api/

➢プロセッサ: Qualcomm® Snapdragon™ 810 v2.1, 2.0 GHz オクタコア

- 姿勢: 座った状態および立った状態

収集した 20 人のユーザ$u^i(i = 1, 2, \ldots, 20)$のタッチ情報から，評価実験で使用するデータセットを生成する．まず 3.3 項で説明した前処理を行い，ユーザごとにタッチ情報を特徴ベクトル群に変換する．本人データを正例，本人以外の偽者データを負例とした二値分類の学習器を構築するため，20 人のユーザから 1 人を本人データG^{u_i}とし，それ以外のユーザを本人以外の偽者データI^{u_i}とするデータセットを生成する．本研究では，Paraskar ら[5]の研究をベースライン手法として提案手法と比較する．具体的には，Paraskar らが提案するバッチ学習で構築された分類器の定期的な再訓練と，本研究が提案するオンライン学習を用いた逐次的な更新モデルを比較する．短期的な行動特徴の変化を再現するため，300 ストローク毎に立った状態と座った状態を変化させる．なお偽者データは本人以外のユーザから各ユーザ均等になるようランダムに選出し，本人データと偽者データは同じ数になるよう調整する．Paraskar らの手法との比較を実現するために，以下の表 3 にまとめる 4 種類のデータセット$D^{u_i}_{normal_a}$, $D^{u_i}_{normal\_b}$, $D^{u_i}_{interval_a}$および$D^{u_i}_{interval_b}$を作成する．また，データセットの構成を可視化したものを以下の図 6 に示す．

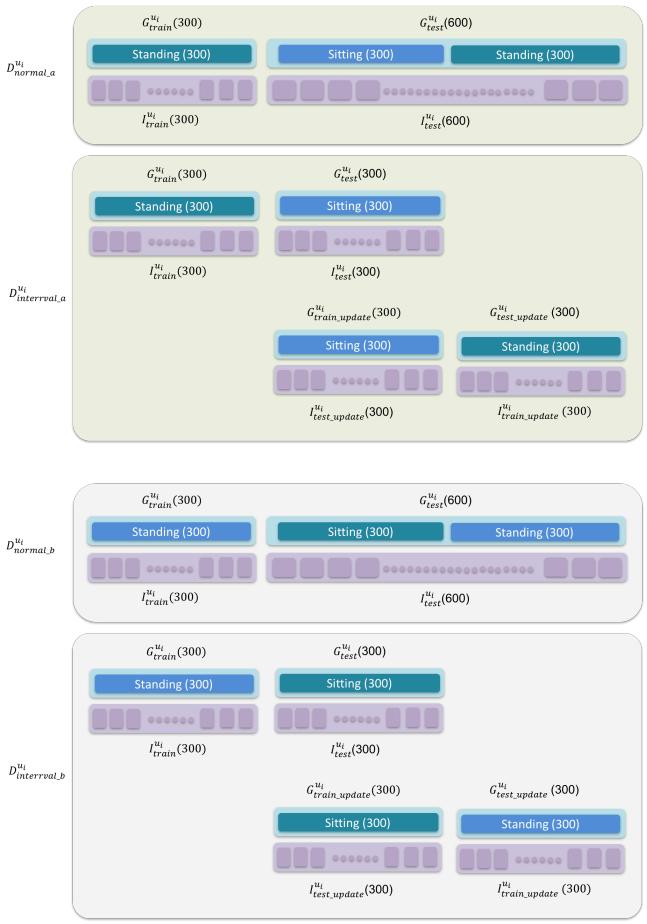

図 6 データセットの構成

4.2 評価方法

本研究では，認証技術の評価手法として一般的に使用される等価エラー率（EER: Equal Error Rate）により評価を行う．EER とは他人受入率（FAR: False Acceptance Rate）と本人拒否率（FRR: False Rejection Rate）が等しくなる点におけるエラー率である．FAR とは，システムが間違って偽物を受け入れてしまう割合である．FRR とは，システムが間違って本人を拒否してしまう割合である FAR と FRR はそれぞれ式(2)及び式(3)にて計算する．

$$FAR = \frac{TA}{TA + FA} \tag{2}$$

$$FRR = \frac{FR}{FR + TR} \tag{3}$$

TA は True Acceptance つまり本人を正しく受け入れることができた数を示す．FA は False Acceptance つまり偽物を間違って受け入れてしまった数を示す．FR は False Rejection つまり間違って本人を拒否してしまった数を示す．TR は True Rejection つまり正しく偽物を拒否できた数を示す．FAR が高いとシステムの信頼性が揺らぎ，FRR が高いとシステムの利便性が下がってしまう．したがって，FAR と FRR は互いにトレードオフの関係にあるため，FAR と FRR が一致する点 EER が認証技術を評価するのに最適な指標とされている．

4.2 実験結果

最適な本実験では，1) 軌跡特徴追加の有用性，2) 決選投票モデルの有用性，3) オンライン分類器による更新モデルの有用性，4) 提案手法の総合評価の観点から評価を行う．Paraskar らの研究[5]をベースライン手法とし，提案手法と比較する．ベースライン手法は Paraskar らの論文を参考に独自に実装した．これらの評価を行うために構築するモデルを以下の表 3 にまとめる．また，以下の表 4 にそれぞれのモデルの実験結果を示す．

1) 軌跡特徴追加の有用性

表 4 の実験結果から，特徴量に軌跡情報を追加すると，ランダムフォレストおよび AROW どちらの分類器を使用する場合においても EER が低下した．軌跡特徴は短期的に変化する特徴だが異なるユーザで比べたときに差異のある特徴であるとわかった．したがって，軌跡特徴は短期的な変化にロバストなオンライン分類機と親和性が高い．

2) 決戦投票モデルの有用性

表 4 の実験結果から，決選投票を導入すると，従来手法および提案手法どちらの場合においても EER が低下することがわかった．ベースライン手法では，一定の間隔ごとの多数決を採用しており，区切るタイミングによってエラー率が変動してしまう問題があった．本実験の結果より，提案する決選投票モデルは，ベースライン手法の問題を解決し，エラー率を低減するのに有用であると判明した．

3) オンライン分類器による更新モデルの有用性

オンライン分類器の逐次的な更新モデルと比較するために，バッチ学習における定期的な再訓練モデルを作成した．定期的な再訓練モデルの実験結果は，更新しないモデルより EER が上がってしまっている．このことから，バッチ学習

によって構築された分類器は短期的な行動特徴の変化に弱いことがわかる．更新しないオンライン分類器は，バッチ学習による分類器より EER が高い．しかし，更新する場合は大幅な EER 低下に繋がることが確認でき，短期的な行動特徴の変化にロバストであるとわかった．

4) 提案手法の総合評価

上記の 1)から 3)で各提案手法の有用性が確認できた．従来手法で提案されているバッチ学習による定期的な再訓練では，短期的な行動特徴の変化に対応できず，訓練データに含まれない行動特徴がテストデータに含まれるとエラー率が上がってしまう．一方，逐次的に更新可能なオンライン分類器は，短期的な行動特徴の変化に対応でき，強固な認証と組み合わせることでエラー率の低下に繋がることがわかった．

認証間隔であるストローク数を増やすほど EER は低下する．しかし，ストローク数を増やすほど認証間隔は長くなり，不正使用の検知に時間がかかってしまう．認証間隔と EER はトレードオフの関係にある．本研究で使用したデータセットにおける，各ストロークにかかる時間を以下の図 7 に示す．ストロークにかかる時間は線形に増えていくのに対し，EER は 13 ストロークを超えたところから変化が乏しい．したがって，本研究では平均 EER1.8%である 13 ストローク毎の認証を採用する．

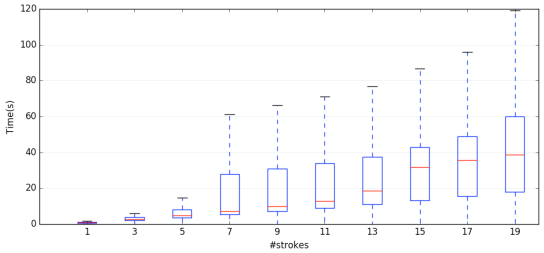

図 7 各ストロークにかかる時間

5. まとめ

本研究では行動特徴を逐次的に更新可能な分類器を構築することで，1) 覗き見攻撃に強固，2) 不正使用の早期検知が可能，3) 行動特徴の変化にロバストなアクティブ認証システムを提案した．従来手法ではバッチ学習の分類器を利用しているため，姿勢や持ち方の違いによる行動特徴の変化に対応することが難しかった．そこで本研究では，オンライン分類器による認証結果が偽者だった場合，顔認証などの高度な認証を行う．高度な認証の結果，オンライン分類器の認証が間違っていると判明したとき，オンライン分類器を更新する手法を提案した．なお 2 段階目の認証は本研究の対象外とし，正しく認証されるものとして扱う．また，オンライン分類器を利用した 1 ストローク毎の認証の際に発生するノイズによる誤分類を防ぐため，オンライン分類器による認証に多数決による投票を一定の間隔で連続的に導入した．20 名の大学生を対象に被検者実験では，1) 軌跡特徴追加の有用性評価，2) 決選投票モデルの有用性評価，3) オンライン分類器を利用した更新モデルの有用性評価，4) 提案手法の総合評価を行った．最終的な総合評価として，19 ストロークごとの認証間隔を採用し EER1.8%を達成した．

今後の課題として，認証間隔を短くしていくことが挙げられる．本研究では，分類器のエラー率低下に繋がるノイズのフィルタリングを行っていない．スマートフォンのタッチ操作には，本人の操作の中でも定常的な操作と異常な操作がある．異常な操作を本人以外の偽者と認識してしまう可能性があるため，ノイズとしてフィルタリングすることで分類器の学習精度が上がることが予想される．分類器の学習精度が上がることで，投票システムの間隔を短くすることに繋がる．

[文献]

[1] Wiedenbeck, Susan, et al. "Design and evaluation of a shoulder-surfing resistant graphical password scheme." Proc. of the working Conf. on Advanced visual interfaces. ACM, pp. 177-184, 2006.
[2] Teh, Pin Shen, et al. "A survey on touch dynamics authentication in mobile devices." Computers & Security, Vol. 59, pp. 210-235.
[3] Meng, Yuxin, and Duncan S. Wong. "Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones." Proc. of the 29th Annual ACM Symp. on Applied Computing. ACM, pp. 1680-1687, 2014.
[4] Shen, Chao, et al. "Touch-interaction behavior for continuous user authentication on smartphones." 2015 Int'l Conf. on Biometrics (ICB). IEEE, pp. 157-162, 2015.
[5] Palaskar, Nikhil, et al. "Empirical Techniques to Detect and Mitigate the Effects of Irrevocably Evolving User Profiles in Touch-Based Authentication Systems." 2016 IEEE 17th Int'l Symp. on High Assurance Systems Engineering (HASE). IEEE, pp. 9-16, 2016.
[6] Breiman, Leo. "Random forests.", Machine learning, Vol. 45, No. 1, pp. 5-32, 2001.
[7] Koby Crammer, Alex Kulesza, and Mark Dredze: "Adaptive regularization of weight vectors", in Proc. of Advances in Neural Information Processing Systems, NIPS'09, pp.414–422, 2009.
[8] Dredze, Mark, Koby Crammer, and Fernando Pereira. "Confidence-weighted linear classification." Proc. of the 25th Int'l Conf. on Machine learning. ACM, pp. 264-271, 2008.

石山 雄大 Takehiro ISHIYAMA
2017 早稲田大学大学院基幹理工学研究科修士課程修了．

山名 早人 Hayato YAMANA
1993 早稲田大学大学院理工学研究科博士後期課程修了．博士（工学).1993-2000 電子技術総合研究所.2000 早稲田 大学理工学部助教授.2005 同大学理工学術院教授，国立情 報学研究所客員教授.IEEE,ACM,AAAI,IEICE.IPSJ 各会員．

表 3　作成した 4 種類のデータセットの内容

データセット	概要	$G_{train}^{u_i}$ / $I_{train}^{u_j}$	$G_{test}^{u_i}$ / $I_{test}^{u_i}$	$G_{train\_update}^{u_i}$ / $I_{train\_update}^{u_i}$	$G_{test\_update}^{u_i}$ / $I_{test\_update}^{u_i}$	合計
$D_{normal\_a}^{u_i}$	更新を伴わない，または逐次的な更新用 立った状態・座った状態・立った状態の順にて構成	300	300・300	−	−	900
		立	立・座	−	−	
		300	300・300	−	−	900
		ランダム	ランダム	−	−	
$D_{normal\_b}^{u_i}$	バッチ学習における定期的な再訓練用 立った状態・座った状態・立った状態の順にて構成	300	300・300	−	−	900
		座	座・立	−	−	
		300	300・300	−	−	900
		ランダム	ランダム	−	−	
$D_{interval\_a}^{u_i}$	更新を伴わない，または逐次的な更新用 座った状態・立った状態・座った状態の順にて構成	300	300	(300)※	300	900
		立	座	座	立	
		300	300	(300)※	300	900
		ランダム	ランダム	ランダム	ランダム	
$D_{interval\_b}^{u_i}$	バッチ学習における定期的な再訓練用 座った状態・立った状態・座った状態の順にて構成	300	300	(300)※	300	900
		立	座	座	立	
		300	300	(300)※	300	900
		ランダム	ランダム	ランダム	ランダム	

※$G_{train_update}^{u_i}$および$I_{train_update}^{u_i}$は$G_{test}^{u_i}$および$I_{test}^{u_i}$と同じものを利用する

表 4 評価実験の結果一覧

手法名		分類器	軌跡特徴	決戦投票	更新モデル	データセット	結果（ストローク毎）				
							1	5	9	13	17
(a)	RF-ST (baseline)	RF	×	×	×	$D^{u_i}_{normal\_a}$	0.202	0.107	0.071	0.059	0.065
						$D^{u_i}_{normal\_b}$	0.203	0.111	0.083	0.063	0.053
(b)	RF-ST_TRJ	RF	○	×	×	$D^{u_i}_{normal\_a}$	0.179	0.082	0.072	0.071	0.063
						$D^{u_i}_{normal\_b}$	0.183	0.092	0.083	0.070	0.065
(c)	RF_WIN-ST	RF	×	○	×	$D^{u_i}_{normal\_a}$	0.200	0.088	0.069	0.055	0.060
						$D^{u_i}_{normal\_b}$	0.205	0.103	0.082	0.069	0.052
(d)	RF_WIN-ST_TRJ	RF	○	○	×	$D^{u_i}_{normal\_a}$	0.181	0.074	0.063	0.054	0.060
						$D^{u_i}_{normal\_b}$	0.188	0.091	0.085	0.073	0.080
(e)	RF_UP-ST	RF	×	×	△	$D^{u_i}_{interval\_a}$	0.221	0.128	0.107	0.099	0.081
						$D^{u_i}_{interval\_b}$	0.207	0.122	0.087	0.101	0.094
(f)	RF_UP-ST_TRJ	RF	○	×	△	$D^{u_i}_{interval\_a}$	0.192	0.111	0.068	0.089	0.061
						$D^{u_i}_{interval\_b}$	0.186	0.103	0.096	0.097	0.107
(g)	RF_UP-ST_WIN	RF	×	○	△	$D^{u_i}_{interval\_a}$	0.215	0.117	0.110	0.105	0.100
						$D^{u_i}_{interval\_b}$	0.196	0.092	0.089	0.083	0.084
(h)	RF_UP-ST_TRJ_WIN	RF	○	○	△	$D^{u_i}_{interval\_a}$	0.189	0.087	0.080	0.067	0.076
						$D^{u_i}_{interval\_b}$	0.183	0.097	0.100	0.108	0.093
(i)	AR-ST	AROW	×	×	×	$D^{u_i}_{normal\_a}$	0.294	0.193	0.163	0.146	0.141
						$D^{u_i}_{normal\_b}$	0.279	0.178	0.135	0.120	0.105
(j)	AR-ST_TRJ	AROW	○	×	×	$D^{u_i}_{normal\_a}$	0.245	0.135	0.098	0.092	0.083
						$D^{u_i}_{normal\_b}$	0.242	0.141	0.109	0.099	0.098
(k)	AR_WIN-ST	AROW	×	○	×	$D^{u_i}_{normal\_a}$	0.294	0.180	0.152	0.143	0.136
						$D^{u_i}_{normal\_b}$	0.279	0.159	0.120	0.103	0.091
(l)	AR_WIN-ST_TRJ	AROW	○	○	×	$D^{u_i}_{normal\_a}$	0.245	0.118	0.090	0.079	0.071
						$D^{u_i}_{normal\_b}$	0.242	0.126	0.101	0.093	0.090
(m)	AR_UP-ST	AROW	×	×	○	$D^{u_i}_{normal\_a}$	0.209	0.126	0.108	0.105	0.094
						$D^{u_i}_{normal\_b}$	0.200	0.118	0.090	0.079	0.065
(n)	AR_UP-ST_TRJ	AROW	○	×	○	$D^{u_i}_{normal\_a}$	0.155	0.076	0.050	0.050	0.045
						$D^{u_i}_{normal\_b}$	0.160	0.091	0.069	0.060	0.058
(o)	AR_UP_WIN-ST	AROW	×	○	○	$D^{u_i}_{normal\_a}$	0.209	0.104	0.056	0.035	0.026
						$D^{u_i}_{normal\_b}$	0.200	0.099	0.053	0.037	0.027
(p)	AR_UP_WIN-ST_TRJ	AROW	○	○	○	$D^{u_i}_{normal\_a}$	0.155	0.065	0.030	**0.019**	0.012
						$D^{u_i}_{normal\_b}$	0.160	0.074	0.035	**0.018**	0.023

RF: Random Forest, AROW: Adaptive Regularization of Weight Vector0
更新モデルにおける△: バッチ学習における定期的な再訓練