Android 端末上のタッチ操作に基づく個人認証に対する操作特徴の比較

渡邊 裕司†

†名古屋市立大学大学院システム自然科学研究科
467-8501 愛知県名古屋市瑞穂区瑞穂町山の畑 1
yuji@nsc.nagoya-cu.ac.jp

あらまし ユーザを煩わせず継続的に認証可能な方法として，ユーザの行動的特徴に基づく生体認証がある．我々の先行研究では，基本操作・文章閲覧・Webブラウジング時にタッチ操作の履歴を記録するAndroidアプリを開発し，被験者2名による予備実験の結果，ピンチ操作での個人の違いを観測した．本研究では，そのアプリを用いて被験者20名に対して行った最新結果を報告する．操作履歴から4方向のスワイプとピンチイン・アウトの6種類の操作を抽出し，各操作に対して距離と速度と角度の基本的な特徴を求める．それらの操作特徴に分類アルゴリズムを適用して認証した結果，本人拒否が多発するものの，ピンチアウトでは他人受入率0.58%と本人拒否率4.65%を達成した．

Comparison of operational features for authentication based on touch operation on Android device

Yuji Watanabe†

†Graduate School of Natural Sciences, Nagoya City University
1 Yamanohata, Mizuho-cho, Mizuho-ku, Nagoya 467-8501, JAPAN
yuji@nsc.nagoya-cu.ac.jp

Abstract Toward behavior-based authentication using features of touch operation on smartphone, our previous study developed an application to get the history of touch operation on Android devices. From the pre-experimental results, some features of pinch operation were interestingly different. In this study, we perform experiments for 20 subjects using the application to record fingers history. The history is divided into 6 gestures of swipe and pinch, and the basic features are extracted for each gesture. For all the operational features, we carry out authentication using some classification algorithms. The results show that there are high false rejection rates except pinch-out operation.

1 はじめに

爆発的に普及したスマートフォンに含まれる多くの重要な個人情報を不正使用から守るために，4 桁の PIN やロックパターンを用いる認証，または指紋や顔などの生体的特徴を用いた生体認証が一般的に行われている．しかし，これらの認証は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．しかもログイン時以外にも認証のため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ある．

そこで，ユーザに煩わしさを感じさせずログイン時以外も認証可能な方法として，個人の行動・操作の特徴や癖を用いた「行動的特

徴に基づく生体認証」がある．この認証は通常時の正規ユーザの行動から特徴を抽出し，その特徴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．そのためログイン時以外にも継続的に監視が可能である．パソコンにおいてはキー操作やコマンド列やマウス操作などを利用した認証が1990年代から広範に研究されていたが，携帯端末やスマートフォンにおける行動的特徴を利用した認証の研究も最近活発になりつつある[1-19]．しかし，多くの研究はログイン時または特定の状況下の認証に着目し，ログイン時以外も含む継続的な認証を扱った研究は相対的に少ない．それは，ログインタスクは全ユーザに対して共通にできるが，ログイン時以外のタスクはユーザ毎に異なり，ログイン時以外の認証は難しくなるためである．その一方で挑戦し甲斐のある研究でもある．

そこで我々は，スマートフォンに搭載された複数センサ（タッチセンサ, 加速度センサ, ジャイロセンサなど）から，ログイン時以外の様々な状況下（タッチ操作時や歩行時など）での各ユーザの操作・行動の特徴を抽出し，継続的に個人認証する研究プロジェクトを進めている[20]．タッチセンサを用いた先行研究[21]では, iOS 上で動作する簡易な文章閲覧アプリケーション（以下アプリと略す）を作成し，ユーザが画面内のテキストを読む時の「スワイプ」と「ドラッグ」の操作履歴を取得した．しかし，このアプリには，テキストブラウザ上の履歴しか取得できない，シングルタッチにしか対応していないなどの問題点があった．そこで，この問題点を改善した Android OS 上で動作するアプリを開発した[22]．具体的には画面上の操作履歴を取得でき，様々な画面サイズの端末に対応し，「ピンチ」などマルチタッチ操作も扱えるようにした．さらに文章閲覧だけでなく，基本操作と Web ブラウジングを追加し, 複数の状況を比較可能にした．そして，被験者 2 名による予備実験の結果，ピンチ操作における個人の違いを観測した．しかし，被験者を増やした本実験やピンチ操作以外の分析などが行えていなかった．

そこで本研究では，文献[22]で開発したアプリを用いて, 被験者 20 名に対して行った最新の結果を報告する．アプリによって取得した操作履歴から 4 方向のスワイプとピンチインとピンチアウトの 6 種類の操作を抽出する．そして，各操作に対して距離と速度と角度の特徴を求める．Feng らの研究[15-17]ではより多くの特徴を使用しているが，各特徴の必要性については触れられていないため，本研究ではまずはこれら基本的な特徴のみでどれだけ認証に使えるかを調査する．これらの基本的な操作特徴に対していくつかの分類アルゴリズムを適用して認証を試みる．

2 関連研究

携帯端末やスマートフォンにおける行動的特徴に基づく認証の研究は 2005 年頃から活発になりつつある．例えば，キー操作に基づく認証[1][2], 加速度センサを用いた認証[3-5], タッチパネルによる認証[6-17], 複数センサを用いた認証[18][19]などがある．文献[1]では，パソコンよりも性能が劣る携帯電話を考慮して，キーストロークの頻度を用いた簡便な認証方法を提案した．文献[2]では，スマートフォンにおいて 25 ユーザのキーストロークに対して様々な分類アルゴリズムの性能を評価した．石原らの加速度センサを用いた 3D 動作認証[3]では，手に持った携帯端末の動きから個人的な動作特徴を抽出するが，継続的な認証のためには端末を何度も動かす必要がある．文献[4][5]の加速度センサを用いた歩容認証は，端末をベルトやポケットに入れた状態で歩行，走行，階段の昇降の動作から個人的な特徴を得て認証を行う．しかし静止時には識別できない．

本研究の対象であるタッチパネルによる認証として，文献[6][7]では Android のロックパターンを使い，文献[8][9]では 5 本の指の動き

を特徴とし，文献[10]の GEAT では 10 個のタッチ操作を選んで使い，文献[11]では PIN 入力時の認証を検討している．しかし，これらは基本的にログイン時の認証である．見上らのタッチパネルと加速度センサを用いた認証[19]もログイン時である．

本研究と同様にログイン後のタッチ操作に着目した研究は，ここ 1，2 年に報告されて，関心の高まりつつある生体認証の分野である．泉ら[12]は，日本語非定型文の入力という特定の状況下であるが，フリック入力データから認証を行う手法を提案し，被験者 43 名に対してひらがな 200 文字程度で十分な認証が可能であることを示した．Touchalytics[13]では，タッチ履歴から 30 個の特徴を抽出し，k 近傍法とサポートベクターマシンを用いて分類した．41 人の被験者に対して 3 個の Wikipedia の記事を読ませて質問に答えさせる実験と二つの画像間の間違い探しの実験を行い，2-3%の等誤り率(Equal Error Rate: ERR)を達成した．SilentSense[14]では，ユーザが歩いているような動的な状況にも対応するため，タッチ操作だけなく加速度やジャイロによる端末の動きからも特徴を抽出し，サポートベクターマシンを用いて分類した．被験者 100 名に対する実験の結果，99%以上の識別精度であることを示した．Feng らの FAST[15]では，タッチ画面に加えて，より正確な指の動きを検出するため加速度とジャイロを備えたセンサグローブも使って，6 個の操作に対して 53 個の特徴を抽出し，分類アルゴリズムとして決定木とランダムフォレストとベイジアンネットワークを適用した．40 人の被験者に対する実験を行い，4.66%の他人受入率(False Acceptance Rate: FAR)と 0.13％の本人拒否率(False Rejection Rate: FRR)を達成した．FAST と同じグループによる GTGF[16]では，タッチ履歴をイメージに変換し，二つのイメージ間で L1 や L2 ノルムを直接求められるようにした．被験者 30 名に対する実験の結果，2.62%の ERR を実現した．同じく Feng らの最新研究である TIPS[17]では，コントロールされていない環境でのタッチ操作に基づく識別のために，ブラウザや地図などのアプリごとに異なるタッチ操作テンプレートを用意している．

これら既存研究と本研究との相違について説明する．本研究に近い FAST[15]に対して，6 個の操作と分類アルゴリズムは同じであるが，53 個の特徴についてそれらの特徴がどれだけ必要であるかの定量的な説明がない（文献[16][17]も同じ）．本研究ではまず基本的な特徴に絞ってそれらの比較を行う．一方，特徴の定量的な比較を行っているのは Touchalytics[13]であり，ユーザと特徴との相互情報量や全特徴の相関行列を示している．しかし，横と縦方向のスワイプ操作だけであり，マルチタッチを扱っていない．SilentSense[14]でもタップ，スワイプ，フリックであり，使用頻度の観点からピンチは無視している．本研究ではマルチタッチのピンチ操作についても調査する．

3 タッチ操作による認証

3.1 タッチ操作記録アプリと操作履歴

本研究では，文献[22]のタッチ操作履歴記録アプリに若干機能を追加したものを使用する．以下ではそのアプリと取得できる「操作履歴」について説明する．

本アプリは以下の 5 つから構成される：

(1) アンケート
(2) 実験1：基本操作
(3) 実験2：文章閲覧
(4) 実験3：Webブラウジング
(5) アンケート回答（今回新たに追加）

本アプリを実際にイメージしてもらうために図 1 にアプリ起動後のメニュー選択画面（左）と実験 3 の Web ブラウザの画面（右）を示す. アプリ起動後の画面にはアンケート，実験 1，実験 2，実験 3，アンケート回答のボタンが設置され，各画面に移動する．まず「アンケート」では，性別，年齢，スマートフォン使用年数，スマートフォンのセキュリティ

について回答してもらう．性別，年齢，使用年数については該当する回答を選択してもらい，セキュリティについては自由に入力してもらう．メニューの「アンケート回答」によってアンケートの内容を確認できる．次に「実験 1：基本操作」では，画面上の基本タッチ操作によって画像が移動・拡大縮小する．そして「実験 2：文章閲覧」については，先行研究[21]と同様に文章を表示させタッチ操作によりスクロールする．最後に「実験 3：Web ブラウジング」は Web ページを自由に閲覧するものである．ここでユーザが使いやすくなるように，標準のブラウザを参考にして「戻る」「進む」「更新」「ホーム」「メニュー」の 5 つのボタン（図 1（右）の画面下のボタン）を設置する．

図 1：アプリ起動後のメニュー画面（左）と実験 3 の Web ブラウザの画面（右）

このアプリによって，「操作履歴」として，タッチイベント *event*，イベント検出時の座標 (x, y) と時刻 *time*，タッチ点の数 *count*，各タッチ点の ID，タッチ時の圧力 *press*，タッチされている範囲 *size*，端末の回転を継続的に取得できる（実際に取得できるかは端末に依存する）．ここで，*event* とは「タッチしたとき」「タッチしたままの状態で動かしたとき」「画面から離れたとき」「複数タッチしたとき」「複数タッチした状態でタッチ位置に変化があったとき」「複数タッチした状態から一つでも画面から離れたとき」などに呼び出されるタッチイベントである．なお，文献[22]から追加した履歴として端末の回転がある．Android では，端末右向きを x 軸，上側を y 軸，スクリーンから外に向かう方向を z 軸とし，x 軸回りの回転をピッチ(pitch)，y 軸回りをロール(roll)，z 軸回りをアジマス(azimuth)としている．

3.2 操作特徴の抽出

上述の様々な「操作履歴」から個人認証に有効な「操作特徴」を抽出しなければならない．まずスマートフォンにはタップ，スワイプ，ドラッグ，ピンチなどいくつかの操作があるため，Feng らの研究[15-17]に倣って以下の 6 個の「操作」に絞って抽出する．

(1) 上から下へスワイプ
(2) 下から上へスワイプ
(3) 左から右へスワイプ
(4) 右から左へスワイプ
(5) ピンチイン（縮小操作）
(6) ピンチアウト（拡大操作）

(1)から(4)までがシングルタッチ，(5)と(6)がマルチタッチである．そして，先行研究[21]と同様に以下の基本的な「特徴」を求める．

(a) 指の移動距離：画面をタッチした瞬間（始点）と離れた瞬間（終点）の 2 点間の距離
(b) 指の移動速度：指の移動距離を時間で割った速度
(c) 指の移動角度：始点と終点の 2 点間の移動角度

「移動角度」については，(1)から(4)のスワイプ操作では角度によってすでに上下左右に分類しているため，ピンチ操作に限定した特徴である．つまりスワイプ操作では距離と速度の 2 特徴である．一方，ピンチ操作では左と右のタッチに対して距離と速度と角度の 3 特徴があるため，合計 6 個の特徴となる．

3.3 認証

前節の「操作特徴」にはばらつきがあるた

め，特徴の全データに対して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を計算する．そして，認証つまり本人と他人を判別するために，その平均値に「分類アルゴリズム」を適用する．分類アルゴリズムは，Weka(Waikato Environment for Knowledge Analysis)のデータマイニングソフト[23]から選ぶ．先行研究[20]では決定木(J48)とニューラルネットワーク(NN)を用いたが，本研究では Zhao らの研究[16]で用いられたベイジアンネットワーク(BN)とランダムフォレスト(RF)も比較のため追加する．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．10 分割交差検証では，データを 10 個のセグメントにランダムに分割し，9 個のセグメントで学習して，検証用の 1 個のセグメントで評価する．そして検証用セグメントを変えながら 10 回繰り返して誤差を得る．限られたデータを用いて学習モデルの汎化性能の推定する方法である．

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 FAR と本人拒否率 FRR を求める．FAR は他人のデータに対して間違って本人とみなしたデータ数として，FRR は本人のデータに対して間違って他人とみなしたデータ数として求められる．FAR と FRR にはトレードオフの関係があるが，できるだけ FAR と FRR ともに小さいほど好ましい．

4 実験結果

4.1 実験方法

被験者 20 名に対して，SONY の NW シリーズの Android 端末とネット接続をできるように WiMAX モバイルルーターを用いて，操作履歴を取得する実験を行った．実験方法として，実験について記載された実験手順書と開発したアプリがインストールされた端末を被験者に渡し，実験手順書に沿って被験者に実験を行ってもらった．すべての実験が終了したら端末を回収し，操作履歴データを端末本体から取得した．

実験 1 の基本操作では，スワイプとピンチの 6 個の操作をしてもらうため，「上から縦線を 10 回以上描画してください」などの指示をアプリ側から被験者に提示し，それに沿って操作してもらった．実験 2 の文章閲覧においては，実験時間と取得できるデータ量を考慮して読んでもらう文章として芥川龍之介の「羅生門」を選択した．実験 3 では，Web ブラウザを利用して，人の記憶に残っていないが調べるとすぐに解答を導ける設問（例えば「第 10 代の日本の内閣総理大臣は誰か？」）を五つ用意し，それらについて解答してもらった．実験時間は約 30 分であった．アンケートに基づく被験者の性別内訳は男性 18 名と女性 2 名，年代内訳は 20 代 7 名，30 代 4 名，40 代 5 名，50 代 1 名，60 代 3 名であった．使用年数の内訳としては，使用したことがないが 3 名，2 年以内が 3 名，2 年以上が 14 名であった．

4.2 結果と考察

実験 1 では 6 個の操作を必ずしてもらうように指示するのに対して，実験 2 と 3 ではタスクは指定するものの操作は自由である．そこで，まず各実験において各被験者が 6 個の操作を行った回数を調べた．表 1 は 20 人の被験者の平均操作回数である．この結果から分かるように実験 2 では下から上へのスワイプ操作が突出しているが，文章を読むだけであるため十分予測されることである．また，実験 3 では他のスワイプ操作も観測されるものの，ピンチ操作は少ない．文献[14]で述べられた「ロングタップやダブルタップやピンチなどの複雑な操作は，日ごろの使用において 5%以下である」にも一致する結果である．

各実験で得られた操作履歴を用いて被験者の認証を試みた．表 1 で示したように回数不足の操作があるため，実験 2 では下から上のスワイプ操作のみ，実験 3 ではスワイプ操作

に対して，4 つの分類アルゴリズム（決定木 J48，ニューラルネットワーク NN，ベイジアンネットワーク BN, ランダムフォレスト RF）を適用した．各実験における各操作に対する各アルゴリズムを用いたときの他人受入率 FAR と本人拒否率 FRR を表 2 に示す. なお, 実験 1 での各操作 10 回以上の指示により, 10 回前後しか各操作をしていない被験者が多いため，ウィンドウサイズ n を 5 とした.

表 1：各実験における平均操作回数

操作	実験 1	実験 2	実験 3
上から下	18.2	0.8	38.6
下から上	14.3	58.3	86.4
左から右	18.4	0.4	22.0
右から左	16.2	0.3	11.1
ピンチイン	16.1	0.0	1.0
ピンチアウト	12.6	0.1	3.1

まず，表 2 の全体的な傾向として，他人受入率 FAR が低いものの，本人拒否率 FRR が極端に悪く，本人の特徴判別がきちんとできていない．特に操作を指示する実験 1 よりも操作の自由度が高くなる実験 2 そして 3 になるにつれて，本人の操作のばらつきが大きくなり本人判別が困難になっているといえる．本人拒否が多い原因として，まずウィンドウサイズ n が小さいこと，スワイプ操作の特徴数が 2 であることが考えられる．それらに加えて，被験者数が増えることによって，本人と似たような特徴を持つ他人がいる可能性が増え，他人データの方が本人データより圧倒的に多くなり，他人データを広く覆うように学習していることも考えられる．特にニューラルネットワーク NN ではスワイプ操作に対して 0%の他人受入と 100%の本人拒否という極端な結果が散見された．ウィンドウサイズを増やすことは認証に時間をかけることにつながり好ましいとはいえず，今後は特徴を増やすことで性能の改善を図る必要がある．

次に，結果の詳細について見ていく．第一に分類アルゴリズムを比較すると，前述の極端な結果のニューラルネットワーク NN に対して，ランダムフォレスト RF では FAR が僅かに増加する一方で FRR が低くなり, 本人判別をうまくできる傾向があるといえる．決定木 J48 やベイジアンネットワーク BN ではそれが不十分で中途半端である．本結果は，RF が J48 よりも良いと報告した Feng らの結果 [15]とも一致する．第二に実験 1 における各操作に対する結果を比較すると，スワイプ操作に比べてピンチ操作の本人拒否の改善が確認される．特にピンチアウトの NN において 0.58%の FAR と 4.65%の FRR を達成している．2 特徴のスワイプに対してピンチは 6 特徴あるためと考えられるが，NN が良い理由など詳細については今後の調査が必要である．

最後に各被験者の結果を調べたところ，すべての被験者で本人拒否が発生しているわけではなく，0%またはわずかな FAR で 0%の FRR の被験者も存在した．具体的に 3 つ以上の分類アルゴリズムで FRR が 0%であった被験者を抜き出すと，実験 1 において，「下から上」で被験者 C, J, P, S の 4 名,「左から右」で B, J, S の 3 被験者，「右から左」で 2 被験者の J, P, 「ピンチアウト」で E, H の 2 被験者であった．実験 2 の「下から上」においては H, R の 2 被験者であった. 被験者 J, P, S はスワイプ操作に共通して多数の他人とは大きく異なる特徴を有していると考えられる．またはある被験者が特定の操作（例えば被験者 B が「左から右」）において他人とかなり相違していると予想される．各被験者についてより詳細な解析を今後行う．

5　おわりに

本研究では，タッチ操作履歴記録アプリによって取得した操作履歴から 6 個の操作に絞って移動距離・速度・角度の基本的な特徴を抽出した．そして，分類アルゴリズムを用いて被験者 20 名の認証を試みた結果, スワイプ操作では本人拒否が極めて多かったものの, ピンチ操作では本人拒否の改善が確認され,

表 2 : 各操作に対する四つの分類アルゴリズムを用いた他人受入率 FAR(%) と本人拒否率 FRR(%)

実験	操作	J48		NN		BN		RF	
		FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
1	上から下	1.45	42.80	0.76	57.20	1.27	52.14	1.23	39.30
	下から上	1.20	44.12	0.71	72.55	1.82	42.65	**1.23**	**31.37**
	左から右	0.94	48.17	0.48	63.30	0.54	62.39	1.55	42.20
	右から左	1.39	35.22	0.62	67.21	2.13	41.30	**1.17**	**31.98**
	ピンチイン	0.95	24.45	**0.57**	**24.45**	1.10	40.17	**0.28**	**27.51**
	ピンチアウト	0.84	18.60	**0.58**	**4.65**	1.45	29.65	**0.29**	**20.93**
2	下から上	1.23	54.31	0.43	84.92	1.29	60.46	**1.97**	**45.69**
3	上から下	0.40	86.85	0.35	88.11	0.42	93.15	2.60	74.77
	下から上	0.37	91.51	0.34	89.61	0.21	93.71	2.29	77.10
	左から右	4.02	58.04	1.67	69.64	3.57	68.75	**3.35**	**44.64**
	右から左	0.43	95.44	0.16	95.44	2.35	89.12	2.56	63.16

特にピンチアウトにおいて 0.58%の FAR と 4.65%の FRR を達成したことを確認した.

今回は操作特徴の詳細な比較であるが，多数の被験者や長期間に渡って実際にオンラインでの認証まで行っている海外の既存研究に比べると，著者らを含む国内の研究は一歩遅れていて，それらとの差別化が明確ではないといえる．例えば，文献[17]では 23 人のスマートフォン所持者と 100 人のゲストユーザに対して数週間に渡って操作履歴を取得している．筆者らもより多くの被験者に対して，十分な操作回数が得られるように長期間の実験を今後行う必要がある．また，距離・速度・角度という基本的な特徴のみではなく，既存研究も参考にして操作特徴を増やしながら性能を向上させなければならない.

謝辞 本研究の一部は，名古屋市立大学特別研究奨励費の支援を受けて行われた．ここに謝意を表します.

参考文献

[1] T. Isohara, K. Takemori, and I. Sasase, “Anomaly Detection on Mobile Phone Based Operational Behavior,” IPSJ Journal, 49(1), pp.436-444, 2008.

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

[3] 石原進，太田雅敏，行方エリキ，水野忠則，“端末自体の動きを用いた携帯端末向け個人認証”，情処学論，46(12), pp.2997-3007, 2005.

[4] J. Mantyjarvi, M. Lindholdm, E. Vildjunaite, S. M. Makela, and H. Ailisto, “Identifying users of portable devices form gait pattern with accelerometers,” IEEE International Conference on Acoustics, Speech, and Signal Processing, pp.973-976, 2005.

[5] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, “Cell Phone-Based Biometric Identification,” IEEE BTAS, pp.1-7, 2010.

[6] J. Angulo and E. Wastlund, “Exploring Touch-screen Biometrics for User Identification on Smart Phones,” IFIP Summer School, 2011.

[7] A. D. Luca, A. Hang, F. Brudy, C. Lindner,

and H. Hussmann, “Touch me once and I know it’s you!: implicit authentication based on touch screen patterns,” CHI, pp.987-996, 2012.

[8] S. B. Napa, A. Kowsar, I. Katherine, and M. Nasir, “Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices”, CHI, pp.977-986, 2012.

[9] 居城秀明, 金岡晃, 岡本栄司, 金山直樹, “タッチパネルによる手指の行動的特徴を用いた生体認証に関する一考察”，情報処理学会研究報告，CSEC-60(15), 2013.

[10] M. Shahzad, A. Liu, and A. Samuel, “Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it,” MobiCom, pp.39-50, 2013.

[11] 西村友佑，柏木まもる，佐村敏治，西村治彦，“スマートフォンを用いた PIN 入力に対するタッチパネルバイオメトリクス”，第 3 回バイオメトリクスと認識・認証シンポジウム，pp.79-84, 2013.

[12] 泉将之，佐村敏治，西村治彦，“スマートフォンにおける日本語非定型文でのフリック入力認証”，第 3 回バイオメトリクスと認識・認証シンポジウム, pp.85-90, 2013.

[13] 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. on Information Forensics and Security, 8(1), pp.136-148, 2013.

[14] C. Bo, L. Zhang, and X. Li, “Silentsense: Silent user identification via dynamics of touch and movement behavioral biometrics,” MobiCom, pp.187-190, 2013.

[15] T. Feng, Z. Liu, K. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, “Continuous mobile authentication using touchscreen gestures,” IEEE HST, pp.451-456, 2012.

[16] X. Zhao, T. Feng, and W. Shi, “Continuous mobile authentication using a novel graphic touch gesture feature,” IEEE BTAS, 2013.

[17] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, “TIPS: Context-Aware Implicit User Identification using Touch Screen in Uncontrolled Environments,” ACM HotMobile, 2014.

[18] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, “SenGuard: Passive User Identification on Smartphones Using Multiple Sensors,” IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications, pp.141-148, 2011.

[19] 見上一憲，林原尚浩，“タッチパネルと加速度センサを用いた携帯端末向けジェスチャ認証とその入力方式の提案”，情報処理学会研究報告，CSEC-56(8), 2012.

[20] Y. Watanabe, Houryu, T. Fujita, “Toward Introduction of Immunity-based Model to Continuous Behavior-based User Authentication on Smart Phone,” Procedia Computer Science, vol.22, pp.1319-1327, 2013.

[21] 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.

[22] 藤田奨，渡邊裕司，“Android 端末におけるタッチ操作の特徴を用いた個人認証に向けたアプリケーションの開発”，コンピュータセキュリティシンポジウム，pp.688-694, 2013.

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