2Z-4

スマートフォンにおける PIN 入力タッチスクリーンバイオメトリクスの実装

泉将之 † 佐村敏治 † 西村治彦 ‡

† 明石工業高等専門学校 ‡ 兵庫県立大学

1 はじめに

現在，スマートフォンは急激に普及しており，それに伴い，不正利用や情報漏洩の危険性も増加しつつある．従来の PIN（Personal Identification Number）やパスワードのみの認証システムでは総当たり攻撃や覗き見攻撃に対して脆弱であり，比較的容易になりすましを行うことができる．その対策の一つとして，PIN やパスワード入力と同時に行うタッチスクリーンバイオメトリクスが注目されている．我々は，評価実験を行ってデータ収集・解析を行い，スマートフォンでの PIN 入力時に得られるタッチスクリーンバイオメトリクスの認証可能性について検討を行ってきた [1].

一方で実用化まで視野に入れた場合，認証率のみの検討では不十分である．個人による閾値の設定，インタフェースの選定，他の認証方法の組み込みなど自明でない実装上の問題を検討する必要がある．本研究では PIN 入力タッチスクリーンバイオメトリクスを実用的見地から議論し，実際に Android 端末のアプリケーションとして開発することを目的とする．

2 PIN 入力タッチスクリーンバイオメトリクス手法

本研究で実装した PIN 入力タッチスクリーンバイオメトリクスの手法について説明する [1]．ただし，アプリケーションという立場からは本アルゴリズムの適用は必要条件ではなく，アルゴリズムの変更が可能なように実装することを要求した．

2.1 特徴量抽出

PIN の桁数を n としたとき特徴量数は $7n-1$ 個である．特徴量ベクトルを $\boldsymbol{a} = (a_1, a_2, \cdots, a_i, \cdots, a_{7n-1})$ とする．本研究では以下の特徴量を用いる．

- 隣接時間間隔（$a_i, i \in \{1, \cdots, 2n-1\}$）
- 押/離時の x，y 座標（$a_i, i \in \{2n, \cdots, 6n-1\}$）
- 押下圧（$a_i, i \in \{6n, \cdots, 7n-1\}$）

2.2 認証方法

本節で扱う照合認証はプロファイル登録フェーズと認証フェーズに分かれる．また，識別手法として ED（Euclidean Distance）法と MD（Manhattan Distance）法を用いる．

2.2.1 プロファイル登録

登録プロファイル数を m とするとき，j 番目のプロファイルの特徴量ベクトルは $\boldsymbol{a}_j = a_{ij}, i \in \{1, 2, \cdots, 7n-1\}, j \in \{1, 2, \cdots, m\}$ となる．登録プロファイルにおける各特徴量の平均値 $\overline{a_i}$ と標準偏差 σ_i は次式になる．

$$\overline{a_i} = \frac{1}{m}\sum_{k=1}^{m} a_{ik}, \quad \sigma_i = \sqrt{\frac{1}{m}\sum_{k=1}^{m}(a_{ik} - \overline{a_i})^2} \tag{1}$$

次に正規化をおこない（a'_{ij}），登録プロファイルの平均値をとることでプロファイル特徴量（$\overline{a'_i}$）とする．

$$a'_{ij} = \frac{a_{ij} - \bar{a}_i}{\sigma_i}, \quad \overline{a'_i} = \frac{1}{m}\sum_{k=1}^{m} a'_{ik} \tag{2}$$

2.2.2 照合

入力者の特徴量を u_i とするとき，次式のように正規化をおこなう．

$$u'_i = \frac{u_i - \bar{a}_i}{\sigma_i} \tag{3}$$

続いて次式により ED 法および MD 法による距離 d^{ED} および d^{MD} を求める．

$$d^{ED} = \frac{1}{7n-1}\sqrt{\sum_{i=1}^{7n-1}(u_i - \overline{a'_i})^2} \quad \text{(ED)} \tag{4}$$

$$d^{MD} = \frac{1}{7n-1}\sum_{i=1}^{7n-1}|u_i - \overline{a'_i}| \quad \text{(MD)} \tag{5}$$

照合には ED 法および MD 法でそれぞれ閾値 d^{ED}_{TH} および d^{MD}_{TH} を設定し，以下の式を満たした場合に入力者を本人と判定する．

$$d^{ED} \le d^{ED}_{TH}\ \text{(ED)}, \quad d^{MD} \le d^{MD}_{TH}\ \text{(MD)} \tag{6}$$

3 提案手法

3.1 認証の流れ

我々の提案する PIN 入力タッチスクリーンバイオメトリクスのシステムアーキテクチャを Fig.1 に示す．本アプリケーションにはプロファイル登録（Registration）フェーズ，認証（Authentication）フェーズの 2 種類の状態が存在する．

プロファイル登録フェーズはスマートフォンアプリを起動して登録を行う．本フェーズを Fig.1 の実線に示す．まず認証に設定する PIN（4 桁以上）を入力し，次に登録

Implementation of Touch-screen Biometrics for PIN input on Smartphone
†Masayuk Izumi †Toshiharu Samura ‡Haruhiko Nishimura
†Akashi National College of Technology
‡University of Hyogo

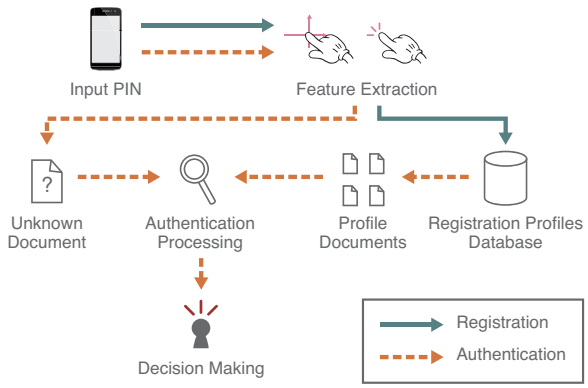

Fig.1 System architecture of Touch-screen biometrics for PIN input

Fig.2 Screenshot from interface of our system. (left): setting screen, (right): login screen

回数分の入力を促す．登録回数はデフォルトを 10 回としているが設定画面（Fig.2 左）により変更することができる．節 2.2.1 に従って特徴量抽出を行い，プロファイル特徴量を生成し，端末に保存する．ただし，閾値の決定については次節で述べる手法を用いる．

認証フェーズはスマートフォンの電源を入れた際に画面にテンキーが表示されて PIN 入力を行う．本フェーズを Fig.1 の破線に示す．節 2.2.2 に従って照合を行う（Fig.2 右）．本人と認証された場合はロックが解除され通常通り端末を利用することができる．一方，本人ではないと判断された場合は再度入力を促される．

3.2 特徴

本アプリケーションでは様々な機能を実装している．本章では，主な特徴として，個人別閾値決定手法と認証アルゴリズムのモジュール機能について説明する．

3.2.1 個人別閾値決定手法

多くの先行研究では同じ閾値を用いて最適な認証率（例えば EER: Equal Error Rate）を求めることが多かった．その場合，被験者により認証率が大きく異なってしまうという問題が発生する．

そこで，我々は個人別に閾値を設定する手法を提案する．例としてプロファイルの登録回数を 10 回とする．まず任意に 1 つプロファイルを取り出す．残りの 9 つについてプロファイル特徴量 $(\overline{a_i'})$ を計算する．取り出したプロファイルを入力者データとして，式 (4) または式 (5) の距離を計算する．次に他のプロファイルを取り出し，同様に距離を計算する．これを 10 回繰り返すと，それぞれ $d_0, d_1, \cdots, d_9$ の距離が求まるが，一番大きい距離を閾値とする．

3.3 認証アルゴリズムのモジュール機能

我々は認証アルゴリズムとして 2 章を採用した．しかし，アルゴリズム自体には様々なものが存在し，異なったアルゴリズムを使用したいという要請も出てくることが考えられる．

そこで，本アプリケーションではシステムアーキテクチャに MVC（Model View Controller）を採用し，認証アルゴリズム部分のモジュール化を行う．MVC の採用により認証に関わる処理がすべて Model にモジュール化されるため，例えば新しい認証アルゴリズム検証などを最小限の労力で容易に行うことが可能である．具体的には，Controller 部から Model 部へ特徴量ベクトル $\boldsymbol{a} = (a_1, a_2, \cdots, a_i, \cdots, a_{7n-1})$ が渡され，Model 部では認証アルゴリズムを実装するプログラムを記述する．認証フェーズでは，Model 部から View 部へ本人か他人を渡すインタフェースを備えることで，認証アルゴリズムのモジュール化を実現させた．

4 認証実験

本アプリケーションの動作確認及び性能評価のために 18-20 歳の高専生男子 8 名を対象に以下の実験を行った．PIN の桁数は最小の 4 桁で行った．本人によるプロファイル登録を 10 回行った後，本人による認証を 10 回，他人 7 名によるアタックをそれぞれ 10 回ずつ行った．その結果，FRR~ 38%，FAR~ 7.9% という認証率が得られた．FRR の精度は悪いが，1 回の試行時間は 1 秒未満のため，他の生体認証と比較すると 1 回の失敗に対するストレスは少ないと考える．しかし，FRR を向上させるための閾値決定法については今後検討を行なっていく．

5 まとめ

本研究では PIN 入力タッチスクリーンバイオメトリクスを実用的見地から検討し，アプリケーションを実装した．今後，本アプリケーションを利用してもらうことで，キーストローク認証研究の普及に貢献していきたいと考える[*1]．

参考文献

[1] 西村，柏木，佐村，西村: スマートフォンを用いた PIN 入力に対するタッチスクリーンバイオメトリクス，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）

[*1] 本アプリケーションを試用したい方は下記までメールを下さい．“masayuki@izumin.info”