スマートフォンのモーションセンサを利用した
個人認証アプリケーションの開発に関する研究

15M7112　髙坂 賢佑
指導教員　小林 孝史

1　はじめに

近年，スマートフォンの普及により日々の生活がより豊かになった一方で，端末がより多くの個人情報を内包するようになった．現在スマートフォンにおいて個人の認証方式として広く使われている方法としてパスコード認証と指紋認証がある．だが，パスコード認証には認証作業が煩雑で認証に用いる鍵情報の自由度が低いということが，指紋認証には鍵情報が変更できないため何らかの原因で鍵情報が第三者に漏洩した場合に今後その情報を用いた個人認証ができなくなるということが問題点として挙げられる．本研究では，スマートフォンに一般的に搭載されている加速度センサと角速度センサを利用し，人間の動き（以下，モーション）を用いて個人認証を行うシステムを開発することで，既存の認証方式が抱える問題点の解決を目指す．

2　システム概要

本システムは，Android 端末に搭載されている加速度センサと角速度センサを用いてモーションデータ（以下，データ）を収集し，Denoising Autoencoder（以下，dA）とその後ろに識別用ニューロンを繋げた識別器を用いて個人認証を行う．本システムではモーション入力を任意の時間で行えるが，データ数の差異を解決するため，登録モードでは入力時間の最も長かったものを，認証モードでは登録時に用いたものを基準にゼロによるパディングか末尾の切り落としを行う．また，フーリエ変換を用いたローパスフィルタによりデータ入力時に生じる手の震えによる影響を減少させる．さらに，加速度から変位，角速度から角度に変換したのち変位データを角度データで回転させ，データの変化が小さいことによる識別器の精度低下を防ぐために全データを 1000 倍したものを用いて以降の処理を行う．

登録モードでは，モーション入力を任意回数で行える．モーションが入力され前述のデータ加工をしたのち，CUDA サーバで動作するプログラム（以下，サーバ）にデータを送信する．サーバでは，受信したデータについて平均が 0，分散が 1 になるように正規化する．そして，正規化したデータの 30%に平均が 0 で分散が 1 のガウシアンノイズによる加工を行う．加工を行った後，dA の学習を行う．学習データに加工を行ったデータを，教師信号に加工を行う前のデータを与え，損失関数に最小二乗誤差を用いて誤差が 0.1 未満になるまで最大 200 回の学習を行う．学習時の dA の構成は，中間層のニューロン数を入力層や出力層から 30%削減し，中間層の活性化関数にシグモイド関数，出力層の活性化関数に恒等関数を用い，中間層ニューロンのうち 50%をランダムに Dropout させる．

dA の学習が終われればパラメータを固定して，その後ろに活性化関数にシグモイド関数を用いたニューロンを繋げる．そして，データの 20%を 0 で上書きしたダミーデータを生成し，正規化する．学習データに正規化したデータとダミーデータを，教師信号にそれぞれ 0.0 と 1.0 を与え，損失関数に交差エントロピー誤差を用いて誤差が 0.1 未満になるまで最大 500 回の学習を行う．学習が終われば，識別器を構成するニューロンが持つパラメータを文字列として連結したデータを，クライアントに送信する．クライアントは受信したパラメータを暗号化し，他アプリからの読み書きができない形で保存する．

表 1: 識別精度の評価結果

	本人	なりすまし
A	0.346374	0.999796
B	0.412742	0.665270
C	0.497443	0.615715
D	0.430046	0.618092
E	0.730683	0.566426
F	0.472196	0.512435

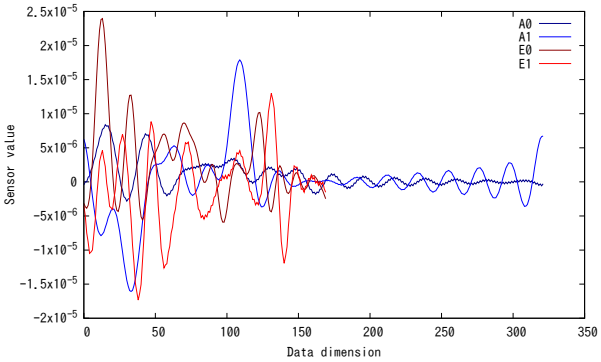

図 1: 被験者 A と被験者 E のデータ比較

認証モードでは，モーション入力は 1 回のみ行える．モーションが入力され前述のデータ加工をしたのち，サーバにデータと保存したパラメータを送信する．サーバは，受信したデータを平均が 0，分散が 1 になるように正規化する．次に，受け取った学習済みニューラルネットワークのパラメータを元に識別器を構築する．そしてこれに正規化したデータを与え，出力をクライアントに送信する．クライアントはこれを受け取り，値が 0.5 未満であれば認証成功とし，0.5 以上であれば認証失敗とする．また，認証モードに限り，クライアントが何らかの理由でサーバに接続できない場合は，クライアント側でサーバと同様の処理を行うことができる．

3　評価及び考察

本システムの識別精度を確認するため，端末を持ち上げるモーションを対象とした実験を行った．本システムを用いて 6 名の被験者にモーションを 4 回入力してもらい，データの収集を行った．各被験者ごとに，最初の 3 回分を登録モードにおける学習データとして用い，最後の 1 回分を認証モードにおける入力データとして 10 回認証を試行した．また，各試行時になりすまし認証データとして筆者自身が同様のモーションを行ったデータも入力した．識別器より得られたデータを各被験者ごとに平均したものを表 1 に示す．表中の数値が低いほど端末所有者のモーション入力であると意味しており，“本人” の列では数値が低いほど良く，“なりすまし” の列では数値が高いほど良い．

結果から，被験者 E を除いて識別できているとわかる．本システムでは，本人によるデータとなりすましによるデータを識別するためにダミーデータを用いた．ダミーを含める割合は，増やしすぎるとなりすまし認証によるデータから得られる識別器の出力が低くなり，減らしすぎると端末所有者のデータから得られる識別器の出力が高くなるため，バランスを取る必要がある．また，結果の良くなかった被験者 E は終始データの変動が激しく，入力回数ごとで一致している部分があまり見られなかった．これにより識別器の学習が進まず，本人が入力したデータでもなりすまし認証であると識別されたのではないかと考えられる．識別率の良かった被験者 A と良くなかった被験者 E のデータを比較したものを図 1 に示す．

4　おわりに

本研究では，Android 端末に搭載されている加速度センサと角速度センサを用い，人間の動きで個人認証を行うシステムを開発した．識別精度の評価実験より，本人によるモーション入力となりすましによるモーション入力を上手く識別できた被験者が多かったものの，一部の被験者については識別できなかった．本システムではダミーデータを作成して識別を試みたが，畳み込みニューラルネットワークのようなより高度な人工ニューラルネットワークを用いて，端末所有者の端末の振り癖を学習させることでより精度の高い個人識別が実現できる可能性があるため，引

き続き研究を進めたい.