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．このことから，第三者によって不正に個人情報にアクセスされたり，インストールされたアプリを通じて様々なサービスをなりすまし利用されたりといった場合の危険性はより高くなった．そのため，端末利用時には本来の端末所有者であるか認証するよう設定することが推奨されている．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．これら認証方式には，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用いてモーションデータ（以下，データ）を収集し，人工ニューラルネットワークの一つである Denoising Autoencoder 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，これによる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たものを用いて以降の処理を行う．

登録モードでは，Android 端末で動作するアプリケーション（以下，クライアント）から，モーションの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ノイズ加工を行う．ノイズ加工を行った後，中間層のニューロン数を入力層や出力層のニューロン数から 50%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た Denoising Autoencoder を構築する．訓練データにノイズ加工を行ったデータを，教師信号にノイズ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 300 回の学習を行う．また，訓練時に中間層ニューロンのうち 50%をランダムに Dropout させる．Denoising Autoencoder の学習が終わ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，正規化する前のデータの値域で生成した乱数でデータの 20%を上書きしたダミーデータを生成し，正規化する．訓練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

表 1: 識別精度の評価結果

A	0.091889	なりすまし	0.996035
B	0.247552	なりすまし	0.492324
C	0.098498	なりすまし	0.096458
D	0.154409	なりすまし	0.123204
E	0.637218	なりすまし	0.495835
F	0.246713	なりすまし	0.32779536

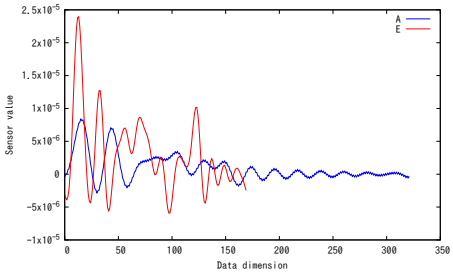

図 1: 被験者 A と被験者 E のデータ比較

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 1000 回の学習を行う．この際 Dropout を無効にし，Denoising Autoencoder の出力に対して 1 から先ほどの学習時に適用した Dropout 率を引いた 0.5 を掛ける．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．クライアント側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．

認証モードでは，クライアントからのモーション入力は 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．サーバでは，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．構築できたらこれに正規化したデータを与え，得られた出力値をクライアントに送信する．クライアント側はこの値を受け取り，値が 0.3 未満であれば認証成功とし，0.3 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が行える．

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あらかじめ 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訓練データとして用い，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，それぞれの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入力して得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てまとめたものを表 1 に示す．

結果から，被験者 A と被験者 B，被験者 F については識別できているとわかる．だが他の 3 名についてはなりすまし認証のデータで得られた識別器の出力がより低く出ており，識別できていない．本システムでは，端末所有者のデータとなりすまし認証によるデータを識別するためにダミーデータを用いた．ダミーデータは元データの値域及び次元数に依存するため，これらが小さい場合は元データとの差があまり出ない可能性がある．これにより，端末所有者が入力したデータであってもなりすまし認証であると識別されてしまっ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