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

本研究で開発したシステム（以下，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．モーションデータの入力は任意の時間で行うことができる．モーションデータの取得間隔は Android API で用意された “SENSOR_DELAY_FASTEST” を指定しており，本システムの開発時に使用した Nexus5 ではおよそ 5 ミリ秒間隔でデータが取得できていることを確認した．

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たら，後述するモーションデータの加工をしたのち GPGPU の一つである CUDA を用いた高速演算が可能な計算機上で動作するサーバプログラム（以下，サーバ）に TCP ソケットを用いてモーションデータを送信する．サーバでは，受信したモーションデータのそれぞれに対して平均が 0，分散が 1 になるように正規化する．そして，正規化したモーションデータのそれぞれ 40%にそのデータの最大値あるいは最小値で上書きす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 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た Denoising Autoencoder を構築する．訓練データにノイズ加工を行ったモーションデータを，教師信号にノイズ加工を行う前のモーションデータを与え，損失関数に最小二乗誤差を用いて 500 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，Denoising Autoencoder の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

のモーションデータにおける最大値と最小値の範囲内で生成したランダム値からなる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モーション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 10000 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それぞれ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たら，後述するモーションデータの加工をしたのちサーバにモーションデータと保存したパラメータを TCP ソケットを用いて送信する．サーバでは，受信したモーションデータを平均が 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もとに識別器を構築する．構築できたらこれに正規化したモーションデータを与え，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 0.2 未満であれば認証成功とし，0.2 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のみでサーバと同様の処理が行えるようにしている．

2.1　モーションデータの加工

3　評価及び考察

4　おわりに