4ZA-01

マスク装着型デバイスによる呼気入力を用いた認証方式の提案とその実装

三品 雅揮† 川瀬 智久† 阿部 隼多† 諸戸 貴志‡ 濱川 礼‡
†中京大学 工学部 情報工学科 ‡中京大学 大学院 情報科学研究科

1 概要

本論文ではマスク装着型デバイスによる呼気入力を用いた認証手法の提案とその実装方法について述べる．これにより呼気入力を用いた第三者から認識されにくい認証が可能となった．

2 背景

近年，スマートフォンやタブレットといった携帯端末の普及により，個人情報など機密度の高い情報を持ち歩く機会が増えた．その中で，背後からパスワードや入力を盗み見る手口であるショルダーハッキングによる情報漏洩やなりすましの被害に遭う危険性が高いことが指摘されている．携帯端末は公共の場所で使用することも多く，隣の人のスマートフォン画面に目に入ってしまうこともある．実際，SoftBank SELECTION が行った調査によると，77.0 %の人が他人のスマートフォンを無意識的に見ている結果がある [1].

そこで我々は入力の際に画面に触れず，口元を覆えば外部から入力が認識されない呼気を用いて認証を行うことでこの問題を解決しようと考えた．口元に違和感なく装着でき，広く利用されているマスクを使用することで第三者から動作が認識されにくく，痕の残らない入力が可能になり，この手法を実現するためのシステムを開発した．

3 呼気による知覚されない認証

呼気は，人によって量や強弱，呼気範囲などの個人差が生じるという特徴がある．この特徴は，第三者から見てもその状態を測ることは難しく，すぐに模倣できるものではない．また，生活する上での自然な動作であり，特定の動作を必要としないことから本研究では呼気を入力として用いた．

また，呼気データは，大気圧センサを使用して測定を行う．しかし，1 つのセンサだけでは入力は容易になるが入力パターン数は少なくなり，強度の問題が生じる．そこで，センサを複数個設定し，呼気範囲と呼気の強弱を測定，入力として使用する．センサを設置・固定し，かつ口元を覆い秘匿性を補完するものとしてマスクを使用することとした．

Proposal and implementation of authentication method using the muscle potential sensor

takashi Moroto, Yuto Nakanishi, yohei Fukuda, Takuya Matusita and Rei Hamakawa
Chukyo University / 101 Tokodati, Kaizu-cho, Toyota-shi, AICHI

4 関連研究

本研究同様，第三者から認識されないという観点の研究は行われている．背景色と偽入力を用いた覗き見耐性を持つパスワード認証を行う研究 [2] がある．また，呼気を用いて入力を行うという点では呼気の風圧を用いた入力インタフェースの研究 [3] がある．前者は端末に触れ入力痕が残るという欠点があり，後者はセキュリティ分野への応用はなされていない．

5 システム概要

本研究は呼気入力を用いることで第三者から認識されない認証を行うシステムである．ユーザは呼気情報を取得する呼気センサモジュール (以降センサ)[4] を取り付けたマスクを装着し，呼気の取得を行い，スマートフォンと通信する (図 1)．システムの流れを図 2 に示す．センサで取得した値の解析は Raspberry Pi で行う．ユーザはスマートフォンの画面を操作し入力を行う．入力が始まるとスマートフォン，Raspberry Pi 間で通信しセンサから呼気情報を取得，数値解析によってキーフレーズを算出し，登録 / 認証を行う．一致すればロックを解除し一致しなければ再度入力を行う．

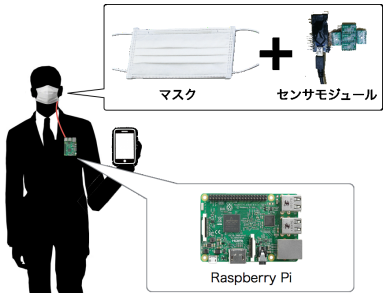

図 1: システム装着イメージ

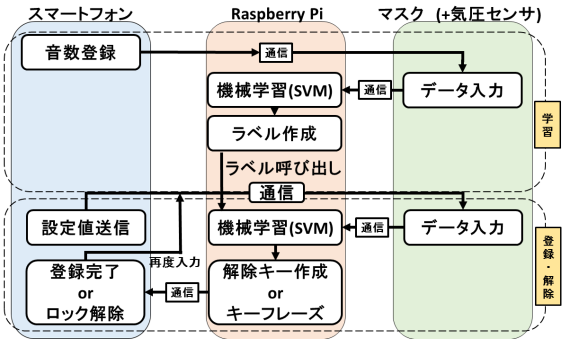

図 2: システムの流れ

5.1 呼気センサモジュール

センサ (図 3) は呼気情報を取得する 5 つのセンサと制御を行う Arduino Nano で構成する．配線図を図 4 に示す．衛生上の問題から同じマスクを複数人で使用することを防ぐため，マスクにデバイスを装着する形式をとった．また，母音毎の開口に対応するために複数のセンサを用いて呼気情報の取得範囲を拡大させた．SPI 通信方式を採用することで同じセンサを複数並列に接続することで作成した．

図 3: 呼気センサモジュール

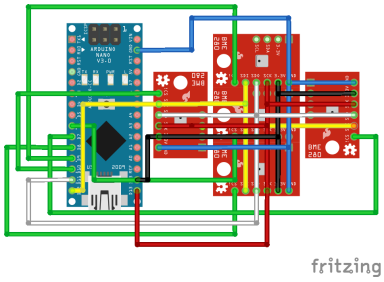

図 4: 呼気センサモジュールの配線図

また，Twe-Lite-Dip[5] を使用することで Raspberry Pi との無線通信を可能にした．

5.2 数値解析

数値解析ではセンサから取得した呼気データから機械学習により 5 つの母音に分類することでキーフレーズを算出する．機械学習にはパターン認識分野で広く使われている教師あり学習手法の SVM を用いた．

まず前実験として，学生 13 名に対し，母音を一人あたり，25 単語 合計 325 単語分の呼気データを取得し，8 : 2 の割合で学習データ，テストデータとして認識率を出力させた結果，認識率は 72.4 %となった．SVM では 5 つの母音をそれぞれ 10 回入力した呼気情報を元に分類する．

認証時，1 つの母音入力で 55 個のデータを取得し， 1 個 1 個 SVM を用いて分類し， 55 個の集まったデータの最頻値を 1 つの出力として行う．

6 第三者目線からの見破り実験

第三者からの盗み見によるハッキングを防ぐことが可能であるかの検証を行った．

検証方法は，入力動作を行っている 2 種類の映像を 4 名の学生に見てもらい，何と入力されているのかを回答してもらった．1 つは，マスクを着用した顔のみを撮影したもの，もう 1 つはマスクを着用した顔とスマートフォンを操作する様子を撮影したものである．その結果，双方において母音が一致した回答者はいなかった．このことから，マスクを着用した状態で呼気入力を行うことは，外部から知覚されることはなく秘匿性が高い入力であることがいえた．

7 認証の評価

マスクを装着しロック解除を行う評価を学生 3 名に対し行った．キーフレーズの登録から解除まで一連の動きを行い，解除成功回数から認証率を算出した．結果は 66.7 %であった．

8 考察

評価の結果，マスクを着けた状態での入力は第三者に知覚される可能性は低く，ショルダーハッキングへの耐性は高いことが分かった．

しかし．その一方でセキュリティシステムとしての有効性を確認したところ，キーフレーズの認証率は 66.7 %にとどまった．

本評価では，母音の「あ」 と「う」が 90.0 %以上の確率で認識された.「お」と入力した場合は，75.0 %の確率で認識された．これは,「お」のデータの要素が「あ」と「う」の入力データと似ているため，誤認識してしまうと考えられる.「い」と「え」は認識することができなかった．これは，他の 3 単語と比べて取得できる気圧が低いため，認識されにくくその他の母音に誤認識されてしまうと考えられる．

また，ユーザの顔の形状によりセンサの位置が変動するため，口の正面で値を取得できていない可能性も考えられる．

これらの結果から，本研究は入力に対して秘匿性が高いが，認証に使用するにはデータ取得方法の改善，センサのマスクへの固定を強くする必要があるという知見を得た．

9 展望

システム利用時にユーザが息切れしていたり泥酔していたりして，普段の呼吸ではない時に正しく認識されない恐れがある．今後はユーザの呼吸の乱れによる影響も調査し，考慮していく必要がある．

参考文献

[1] SoftBank SELECTION による スマートフォン利用実態調査 *http : //www.softbankselection.jp/privacy$_e$nquete/*

[2] 背景色と偽入力を用いた覗き見体制を持つパスワード認証方式の提案 杉本洋介 他 京都工芸繊維大 コンピュータセキュリティシンポジウム 2014

[3] 呼気の風圧を用いた入力インタフェースの基礎的検討 久米祐一郎 他 東京工芸大 映像メディア学会 2016

[4] BME280 搭載 温湿度･気圧センサモジュール *https : //www.switch − science.com/catalog/2236/*

[5] TWELITE DIP *http : //mono − wireless.com/jp/products/TWE − Lite − DIP/index.html*