L-009

携帯端末の加速度センサを用いたシェイキング認証システムに関する研究

Study on shaking authentication system using the acceleration sensor of mobile terminal

松井 博敬† 福元 伸也† 鹿嶋 雅之† 佐藤 公則† 渡邊 睦†
Hirotaka Matsui , Shinya Fukumoto , Masayuki Kashima , Kiminori Sato , Mutsumi Watanabe

1. はじめに

近年，我々の身の回りにスマートフォンが広く普及している[1]．既存のスマートフォンの認証手法では指紋認証やパターン認証などが主流である．しかし，いずれも認証時に画面との接触を伴うため痕跡が残りやすくハッキングが懸念される[2]．そこで本研究では，スマートフォンに搭載された加速度センサを用い，非接触で痕跡が残らない認証システムの構築を目的とする．

2. 関連研究

加速度センサを用いたスマートフォンのセキュリティシステムとして，タッチパネルと加速度センサを用いたジェスチャ認証[3]や加速度センサ・ジャイロセンサを併用したスマートフォンの利用認証手法[4]が提案されているが，これらはいずれも認証における動作が複数存在するため利便性に欠けている．本研究では振り動作とハードキー押下の組み合わせによる認証を行い，利便性の高い認証システムを目指す．

3. シェイキング認証システム

3.1 システムの概要

本手法では，スマートフォンに搭載された加速度センサを用いて 3 次元方向へと振ることにより認証を行う．この時，振る動作と同時にスマートフォンの側面に標準的に装備されているハードキー（±Volume ボタン）を押下し，それらの動作の組み合わせによって入力を行う．図 1 に示すのが 3 次元方向に対する振り動作入力例と押下するハードキーの模式図である．

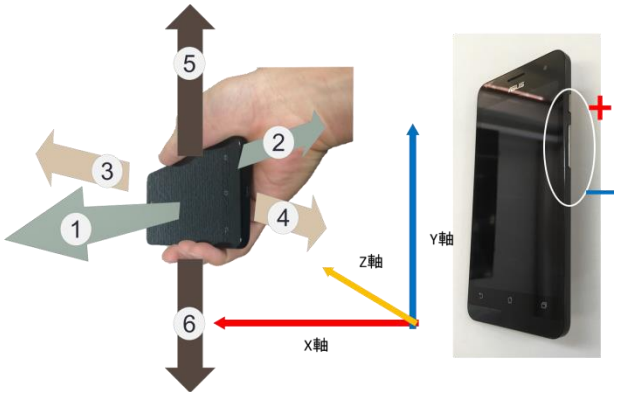

図 1　振り動作と押下するハードキー

†鹿児島大学大学院理工学研究科，Graduate School of Science and Technology, Kagoshima University.

3.2 動作の組み合わせ

ハードキーの押下には表 1 に示すような合計 5 つのパターンを用いる．ここから振り動作とハードキー押下を組み合わせてユーザ登録し，個人認証を行う．本手法では認証時間を可能な限り短縮することを目的とするため，入力に関しては 2 回の動作で認証可能なシステムを構築した．また，振り方向は 6 通りであるが，このとき持ち方を+X 軸方向，+Y 軸方向，+Z 軸方向の 3 通りに区別することによって，割り振ることのできる振り方向を 18 通りとなるようにした[5]．従って，一回の振り動作において 6×3×5＝90 通りの入力パターンが存在することとなる．

表 1　押下するハードキーの組み合わせ

	ハードキー動作
①	何も押下しない
②	Volume＋ボタンを 1 回のみ押下
③	Volume－ボタンを 1 回のみ押下
④	Volume＋ボタンを押下し続ける
⑤	Volume－ボタンを押下し続ける

3.3 システムの処理手順

提案するシステムの処理手順を図 2 に示す．手順は大きく分けて取得フェーズと認証フェーズの 2 つのフェーズに分けられる．

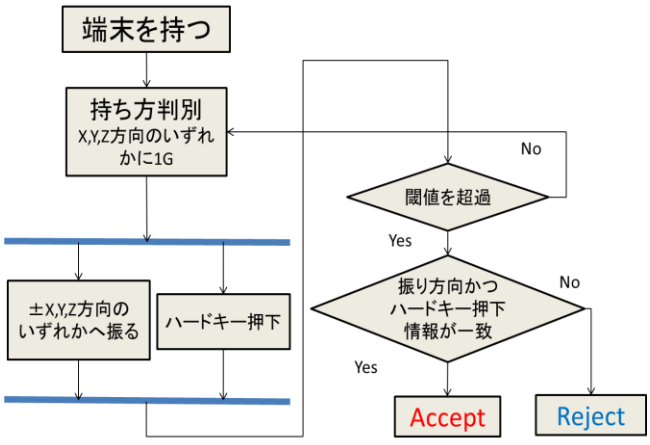

図 2　本システムの処理手順

3.3.1 取得フェーズ

本研究では，Android 端末(ASUS 社製 Zen-Fone5) を用いる．この端末に本研究で開発した認証用アプリケーションをインストールし，各ユーザの動きを取得する．加速度を

取得する際にハイパスフィルタを用いることによって，低周波成分である重力加速度の影響を除去する．ハイパスフィルタの適用により，加速度の変位量のみを抽出することが可能となった．

3.3.2 認証フェーズ

端末を各軸方向へと振ることにより PIN を入力するが，そのときの対応した PIN を配列へと格納する．あらかじめ登録された PIN の配列と入力した PIN の配列が全て一致していれば認証成功となる．端末の画面をキャプチャしたものが図 3 である．図 3 左上 のように「Change your form」の指示文が表示されたら持ち方を変え，赤字で「Please Shake ！」の指示文が表示されたら各軸方向へと振る．この一連の流れを 2 桁分繰り返すことで，PIN の入力が完了となる．認証に成功した場合は，図 3 左下のように「Accept!!」が表示され，認証失敗の場合は，図 3 右下 のように「Reject!!」が表示される．

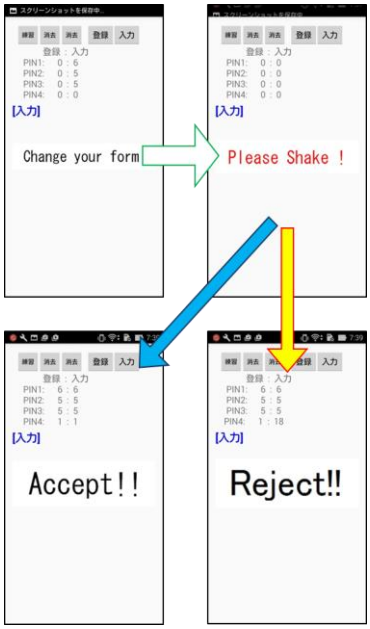

図 3　認証時の端末画面

4. 評価実験と結果

4.1 評価実験

4.1.1 他人受入実験

シェイキング認証システムを構築し，評価実験を行った．20 代大学生の実験協力者 10 名に対して，本システムの概要を説明後，端末を振って実際に認証している同様の動画 3 種類を見せた．実験協力者の動画の再生回数は無制限とし，その後ハッキングを行ってもらった．

4.2 結果

4.2.1 他人受入実験

評価実験の結果を表 2 に示す．3 種類の動画を 10 名に見せたところ，ハッキングできたのは動画①で 1 名，動画②，③ではそれぞれ 0 名という結果となった．

表 2　他人受入実験結果

	2 桁入力	振り方向	ハードキー
動画①	1/10[名]	9/10[名]	1/10[名]
動画②	0/10[名]	8/10[名]	0/10[名]
動画③	0/10[名]	9/10[名]	0/10[名]

4.3 実験結果まとめ

端末の振り方向を識別できた実験協力者は多かったが，その内ハードキー押下までを識別できたものは 1 名であった．10 名の実験協力者に対して，3 種類の動画を見せる実験は，即ち合計 30 回のハッキング試行である．このうち，突破できたのは 1/30 回であり，ハッキング成功率は 3.3%であるという結果を得た．

5. 考察

実験から，他人受入実験におけるセキュリティに関しては，振り方向は大方見破られるようであったが，ハードキー押下に関しては 1 回しか見破られなかった．このハッキングに成功した 1 名の実験協力者は，ハードキーの押下の確証はなく答えた場合に正解したため，このような当てずっぽうでの推測手法によっては，本システムは突破される可能性がある．

6. おわりに

近年，スマートフォンの普及に伴い多くの人々が様々な情報を持ち運べるようになり，重要な個人情報の管理の徹底は必要不可欠な課題である．現在スマートフォンに実装されている認証手法では，未だシステムの脆弱性を残したままである．そこで本研究では，加速度センサを用いた振り動作によるシェイキング認証システムを提案した．実験協力者 10 名での評価実験の結果，本システムの FAR（他人受入率）は 3.3%という結果を得た．

今後は，幅広い実験協力者層を確保・増員し，ハッキングに対する評価実験を進め，本システムのセキュリティの有用性を検証していく．また，本人認証においても複数名の実験協力者を確保し実際に端末を振ることによる登録と認証を行っていく．その際に認証時間の計測とユーザビリティ評価も行っていき，ユーザの声に耳を傾けながらシステムの修正と再構築を進めていく．

参考文献

[1] 総務省，“平成 27 年通信利用動向調査の結果”http://www.soumu.go.jp/johotsusintokei/statistics/data/1607221.pdf
[2] 江口雅人，岡田泰輔，佐々木良一，” Android スマートデバイスにおける情報漏洩防止策の安全性評価”，マルチメディア，分散協調とモバイルシンポジウム 2014 論文集，pp.1735-1740，(2014)
[3] 見上一憲，林原尚浩，“タッチパネルと加速度センサを用いた携帯端末向けジェスチャ認証とその入力方式の提案”，情報処理学会，研究報告コンピュータセキュリティ，2012-CSEC-56(8)，pp.1-7，(2012)
[4] 濱野雅史，新井イスマイル“加速度センサ・ジャイロセンサを併用したスマートフォンの利用認証手法の提案”，情報処理学会，研究報告ユビキタスコンピューティングシステム(UBI)，2014-UBI-41(17)，pp.1-8，(2014)
[5] 松井博敬，福元伸也，鹿嶋雅之，佐藤公則，渡邊睦，“加速度センサの持ち方と振り動作を用いた PIN コード入力システムに関する研究”，信学技報，バイオメトリクス研究会，Vol.117，No.42，BioX2017-6，pp. 49-53（2017.5）