音と振動によるフィードバックと スマートフォンの傾きを用いた認証手法

小戸田 怜永[1,a)]　丸山 一貴[1,b)]

概要：スマートフォンが普及した今日では，スマートフォンの認証動作を盗み見る覗き見攻撃は大きな脅威となる．覗き見耐性を持った入力方法について多くの研究がなされている．指紋認証等の生体認証は覗き見攻撃に対して強い耐性を持っている．しかし，生体認証は手袋を着用している際やマスクや眼鏡を使用している際に使えないことがある．そのため，生体認証以外にも覗き見耐性のある認証手法が必要である．そこで，本研究では強度な覗き見耐性を持ち，画面の視覚情報を全く用いない認証手法の実現を目的とする．提案手法では，加速度センサ等を用いてスマートフォンの傾き具合でカーソルを動かす．カーソルがどの数字を指しているかを音と振動の組み合わせによってユーザに通知を行う．これにより，ユーザは画面視覚情報を用いることなく PIN を入力することが可能となる．10 名を対象に実験を行った結果，他人受入率は 0 %となり，覗き見耐性を持つ認証手法であることがわかる．過去に予備実験のシステムを使用したことのある被験者の本人拒否率は 0%，認証時間の中央値は 45 秒となり，最短時間は 42 秒となった．また，10 名全員の本人拒否率は 48 %，認証時間の中央値は，73 秒となり，初心者はトレーニングが必要となることがわかる．

1. はじめに

電車やエレベーター等の公共の場で，認証画面を見られてしまう危険性がある．実際に，2015 年に SoftBank SELECTION [1] が行ったスマホ利用実態調査によると，電車やバスの車内で他人のスマートフォンの画面をふと見てしまう「ふと見」をしたことがある割合が 77% であり，電車やバスの車内で他人のスマートフォンをしっかりと積極的に見る「がっつり見」をしてしまった割合は 13.6% であった．このように，公共の場において認証行為を行うことで，他人に認証画面を見られることや認証動作を録画され PIN コードが盗まれてしまうことを覗き見攻撃と言う．また，背後から画面を見られることで認証情報が盗まれたことに気づくことができないという問題がある．

覗き見攻撃を防ぐために，振動やジェスチャを用いた認証がこれまで提案されてきているが，覗き見されてしまい，パスワードが盗まれてしまう可能性が残っている．また，画面の視覚情報を全く用いない認証方式については，研究が少ない現状がある．画面の視覚情報を全く用いない生体認証は覗き見攻撃に対して強い耐性を持っている．しかし，指紋認証は手袋や指を怪我した際，顔認証はマスクや眼鏡をしている際に使えない場合があり，通常時であっても認証に失敗する場合があるため生体認証以外にも覗き見耐性のある認証手法が必要である．

本研究では，画面の視覚情報を用いずにスマートフォンに内蔵されている加速度センサ等を用いた新たな認証手法について検討する．通知方法として，イヤホンからの音と振動を組み合わせることにより覗き見攻撃に対して耐性を保ち，加速度センサ等を用いることで画面の視覚情報を用いない認証方法を実現することを目的とする．MMD 研究所 [2] が 18 歳から 69 歳の男女 7,000 人を対象に行った調査によるとイヤホン・ヘッドホンの所持率は，67.6% のため，本提案システムは多くの方が使用できると考える．また，画面の視覚情報を用いない認証が可能となることで，視覚に障害のある方も使用できると考える．

2. 関連研究

覗き見攻撃に耐性を持つ認証手法の研究として数多くの研究がなされている．本章では，加速度センサやジャイロセンサを用いた認証，振動を用いた認証と音を用いた認証の 3 つに分ける

加速度センサやジャイロセンサを用いた研究では，加速度センサやジャイロセンサを利用したジェスチャ認証が提案されている．濵野ら [3] は，加速度センサとジャイロセン

[1] 明星大学 情報学部 情報学科
[a)] 21j5056@stu.meisei-u.ac.jp
[b)] kazutaka.maruyama@meisei-u.ac.jp

© 2025 Information Processing Society of Japan.

サの両方を用い，一筆書きもしくは，単一動作をパスワードとして組み合わせるジェスチャ認証を提案している．古賀ら [4] は，加速度センサを用い端末を持った際に大きな動きを伴わない静粛な手首の動作を対象とした認証手法を提案開発した．成ケ澤ら [5] は，加速度センサとジャイロセンサを用いてスマートフォンの Y 軸を中心に回転する動作の特徴量を用いた認証手法を提案している．また，嘉藤ら [6] はスマートウォッチを利用して手首の動きを用いてスマートフォンのロックを解除する手法を提案している．これらの研究は，加速度センサとジャイロセンサを用いてジェスチャ認証を行っているため，本研究とは加速度センサとジャイロセンサの利用の仕方が異なる．

振動を使用し，ユーザに通知する認証手法の提案も数多く存在している．江原ら [7] は，既存の携帯端末の振動機能を利用した手法に対して，ユーザインターフェースを改善することで，覗き見攻撃に対する安全性を維持しつつ，認証時間を短縮した個人認証手法を提案している．立花ら [8] は，振動機能を用いたフェイク入力を入力動作時に混在させることで認証情報を特定困難にする認証手法を提案している．Manisha ら [9] は，ボタンを押すことで振動が開始され自分の入力したい数字の回数分振動が鳴った際にボタンを離すことで認証を行うことができるシステムを開発した．また，M. Monjirul ら [10] は，通常の入力に振動の回数を追加した認証手法を提案している．しかし，これらの研究では画面の視覚情報を使って認証を行っている．本研究では，画面の視覚情報は全く用いない点が異なる．

音の特徴を用いた認証手法の研究もなされている．臼井ら [11] は，カクテルパーティ効果を利用し，混成音の中から自分の聞き分けるべき音が含まれているかを判別することで認証を行うシステムを開発した．また，政重ら [12] はニーモニック認証と音記憶を併用したシステムを開発した．これらの研究は，音の特徴を記憶し，音自体が認証情報となる．本研究では，音と振動の組み合わせによる通知に用いている点で異なる．

3. 提案手法

本研究では，スマートフォンに内蔵されている加速度センサと地磁気センサを用いてスマートフォンの傾きを検出し，カーソルを動かすイメージによって認証を行う．**図 1** に作成するシステムのイメージを示す．図 1 の青い矢印がカーソルとなっており，スマートフォンを傾けることでカーソルが移動する．そのため，認証を行う際は，何も表示されていない状況となる．

3.1 認証の手順

認証の手順について述べる．本提案手法では，音と振動の組み合わせ通知のため，ユーザは音と振動の違いをそれぞれ判別する必要がある．具体的な認証の手順を以下に示す．

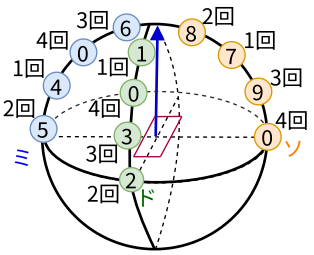

図 1 数値配置図

(1) スマートフォンを右，左，手前のいずれかにわずかに傾けて 3 種類の音を聞き分ける
(2) 音を聞き分け，入力したい数値があるグループ音の場合，さらに傾け振動の回数を判別する
(3) 振動の回数が入力する数値であった場合，画面をタップする
(4) グループ内の数値の位置が変更される
(5) 再び手順（1）に戻り，4 桁全ての入力が完了するまで繰り返す

3.2 値の配置とグループ化

画面を用いない点から数値の配置はスマートフォンの大きさや形状に限定されることなく配置することが可能である．図 1 の 中央にある赤い短形がスマートフォンを表しており，値の配置は空間上に配置されているようなイメージとなる．また，数字は右，左，手前の 4 つずつでグループ化されている．0 に関しては，3 軸全てに配置している．これは，0 から 9 までとするとひとつのグループだけ 4 つの数字が並んでしまい，配置にばらつきが出てしまうため，すべての軸に配置した．0 を使用する理由は，0 から 9 の 10 個の数字を用いた際のパスワードの場合の数は，1 から 9 までの 9 個の数字を用いた際の場合の数の約 1.5 倍となり，ブルートフォース攻撃に対して耐性を保つため 0 を使用する．

各グループの位置は 1 回の認証動作中は変更されず，4 桁の認証が完了し失敗した場合に変更され，グループ内の位置は入力をするたびに変更される．

3.3 ユーザへの通知方法

本提案手法では，音と振動を組み合わせて通知を行う．音と振動を組み合わせることで，攻撃者は音と振動両方の情報を取得しなければ推測が難しくなる利点がある．

通知方法として，音のみで通知する方法も考えられる．それぞれ指している値を音声で通知することでユーザはカーソルがどの値を指しているか判別することが容易である．しかし，音漏れしてしまっている場合，攻撃者にどの値をタップしているかすぐに判別されてしまう．

© 2025 Information Processing Society of Japan.

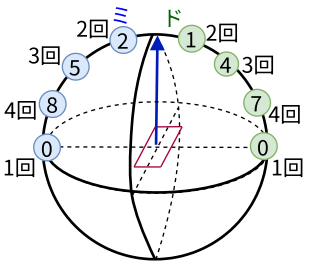

図 2 予備実験数値配置図

一方で，振動のみを通知に使う方法は，多くの関連研究があり，研究が十分になされている．また，本提案手法で振動のみで値を通知する場合，1 から 10 回まで振動させる方法が考えられる．しかし，筆者がどこまで振動の判別が可能か実験したところ，判別が可能なのは 4 回が限度であった．4 回の振動でモールス信号のように長短の振動に符号化する事で 10 種類を 4 回の振動で伝えることは可能だが，それを瞬時に判別することは困難であると考える．

そのため本提案手法では，カーソルがどのグループを指そうとしているのかを 3 種類の音を用いて通知する．ユーザは，3 種類の音を聞き分けることでスマートフォンをさらに傾けた先にどの数字が存在しているかを素早く判断することができる．

カーソルが配置されている数字の所に来た際に，振動で利用者に知らせる．振動時間は 130 ミリ秒，振動間隔は 100 ミリ秒とした．振動の回数は，1 回から 4 回まであり 0 を除き，グループの中で一番小さい数字から値が大きくなるにつれて振動の回数が 1 回ずつ増加する．また，すべての軸に配置されている 0 の振動回数は 4 回とする．このことにより，認証にかかる時間を短縮することができ，利便性の向上に繋がると考える．

4. 予備実験

音と振動についてそれぞれ判別することが可能かを調べるための予備実験を行った．

4.1 実験内容

図 2 で示すように右と左の二軸に値を順に配置し，音や振動の違いを判別し，入力することができるか調査を行った．実験後にアンケートを行い，音と振動を判別可能であったか調査した．アンケート項目は**表 1** に示す．

実験の被験者は，本学の大学祭の来場者である一般の方 7 名を対象とし，入力する PIN コードは「1 4 8 0」とした．

4.2 実験結果と考察

実験参加者のうち 7 人中 4 人が正しく入力することができていた．実験後に行ったアンケートでは，7 名全員がイヤホンを使用していると回答があった．このことから，改めてイヤホンを日常的に使用している人が多いことがわかる．また，音の違いについてわかりやすかったかという問に対して，5 名の方が「そう思う」，1 名の方が「ややそう思う」と回答し，7 名中 6 名の方が分かりやすいと感じていたことが分かる．振動の回数の違いについては，「そう思う」が 2 名，「ややそう思う」が 2 名，どちらとも言えないが 1 名，「あまりそう思わない」が 2 名という結果となった．これらの結果から，音と振動については，「そう思わない」という回答がなかった点からも，十分に判別することが可能であると考える．音に関しては、現時点では 2 音しか用いていないため，さらに判別が容易となるように一オクターブずつ音階をさらに分けることとする．このことにより，音が 3 つになった場合であっても十分に判別ができると考える．振動に関しては，0 を振動 1 回としていたが，4 回に変更しグループ内で一番小さい順番から値が大きくなるにつれて振動回数が増加するように変更する．

表 1 予備実験アンケート項目

1.	イヤホンを日常的に使っていますか？
2.	音の違いは分かりやすかったか？
3.	振動の回数を判別することは容易であったか？
4.	値を探すのは容易であったか？

5. 実装

本システムは，Android Studio を用いて，Android 用のアプリケーションを Java を用いて開発し，実験を行う．実験に使用する端末は，Motorola の moto g24 とする．

5.1 プログラム概要

3 軸方向に値を配置し，それぞれシャッフルを行っている．1 回の認証動作の間では，それぞれのグループの位置は変更せず，グループ内の位置のみを変更することができるように実装を行っている．また，3 種類の音は C3，E4，G5 の 1 オクターブずつ離れた音階を sin 波を用いて生成したものを録音し，再生している．それぞれの sin 波の値は，低い音から順に 130.813Hz，329.628Hz，783.991Hz となっている．値の入力はタッチイベントを検出し，画面タップで入力，ロングタップで入力削除とした．

5.1.1 スマートフォンの傾き検出

スマートフォンの傾きを調べるため，加速度センサと地磁気センサから回転行列を計算し，スマートフォンの傾きを検出している．また，認証を開始する際の姿勢を基準とするため，アプリケーション起動時に水平状態からの差分を取ることで手に持った状態が基準となるように実装した．

6. 実験

本研究では，本人拒否率，他人受入率と認証にかかる時間を計測する実験と，慣れにより本人拒否率と認証時間の変化を評価するため 2 種類の実験を行った．

© 2025 Information Processing Society of Japan.

表 2　認証側アンケート項目

A1.	このシステムを使うのは初めてですか？
A2.	何回程度使用したことがありますか？
A3.	システム全体の仕様は理解しやすかったか
A4.	安心感を持って入力を行うことができた
A5.	重要なデータのロック解除に使用したいと思うか
A6.	慣れれば使いやすいと思うか
A7.	その他、システムで気づいたことがあればご記載ください

表 3　攻撃側アンケート項目

B1.	システムを理解していましたか
B2.	音は聞こえましたか？
B3.	振動は聞こえたか？
B4.	推測した 5 個の数字は自信がありましたか？
B5.	今回の実験で推測することができたか？
B6.	音もしくは振動どちらか一方が聞こえた場合は、推測しやすくなると思うか？
B7.	どんなことでも構いませんので覗き見中に推測できたことがあればご記載ください
B8.	その他、覗き見中に気づいたことがあればご記載ください

6.1　実験 1

本提案手法を用いて，本人拒否率，他人受入率と認証時間を調査した．

6.1.1　実験内容

実験は二人一組で行い，実験を行ってもらう 2 名には実験前にランダムに生成した 4 桁の PIN コードで最低 20 分間練習し，20 分以内に一度も正しく入力できていない場合は成功するまで練習を行った．本人拒否率は，練習に用いた同じ 4 桁の PIN コードを 10 回入力し，成功回数で評価を行った．10 回の認証では，入力するたびにグループ内の位置が変更され，4 桁の入力が終了すると失敗成功にかかわらず，新たな認証としてグループ化の位置とグループ内の数値の位置が変更される．他人受入率は，相手が 10 回認証動作をスマートフォンから 60cm 程度の位置から覗き見し，PIN コードを 5 回推測してもらった．また，覗き見中はメモをとってもよいこととした．実験参加者のスマートフォンの持ち方は，指定せず持ちやすい状態で認証を行った．実験場所は，筆者が所属する研究室で静穏な状況であり，OneOdio Pro 10 ヘッドホンを使用し音漏れはしない程度の音量に設定している．実験終了後に認証側と攻撃側それぞれアンケートを行った．アンケート項目を**表 2** と**表 3** に示す．

6.1.2　実験結果

実験 1 の被験者は 10 名であり，被験者 D を除き全員右利きであった．それぞれの本人拒否率，他人受入率と認証時間の中央値を**表 4** に示す．実験前の練習では，被験者 B，G，H の 3 名がそれぞれ追加で 11 分，35 分，46 分練習を行い，それ以外の方は，20 分以内に最低 1 度は認証に成功した．追加実験を行った被験者は，表 4 で被験者の欄に*1，本システムを過去に使用したことがある人は*2 と印をつけた．全体の本人拒否率は，48%，他人受入率は，0% となった．また，認証時間の中央値は 73 秒となった．

表 4　ユーザごとの結果

被験者	本人拒否率 [%]	他人受入率 [%]	認証時間の中央値 [秒]
A	50	0	53.5
B*1	80	0	103
C	60	0	88
D	40	0	69
E	20	0	47
F	70	0	56
G*1	10	0	104.5
H*1	80	0	92.5
I*2	0	0	45
J	70	0	85

6.1.3　アンケート結果

アンケートは，10 件の回答を得た．

認証側のアンケートで一番評価したいことは「安心感を持って入力を行うことができた」である．この問に対して，「そう思う」と回答した方が 3 名，「ややそう思う」と回答した方が 3 名，「あまりそう思わない」と回答した方が 4 名となった．攻撃側のアンケートでは，音は聞こえましたかという問に対して全員が「そう思わない」と回答があった．また，振動に関しては 1 名の方が，「あまりそう思わない」と回答し，それ以外の方は「そう思わない」と回答した．「あまりそう思わない」と回答した方に関しては，「イヤホンのワイヤー部分が僅かに動いていたため動かし方によっては，ワイヤーから振動を判別することが可能だと思った」と回答した．

攻撃側のアンケートでは，「推測した 5 個の数字に自信がありました？」という問に対して，6 名の方が「そう思わない」と回答し，3 名の方が「あまりそう思わない」と回答した．「今回の実験で推測することはできたか？」という問に対して，2 名の方が「ややそう思う」と回答し，「どちらとも言えない」，「あまりそう思わない」と回答した方が，それぞれ 1 名となった．また，5 名の方が「そう思わない」と回答した．

6.2　実験 2

実験 1 を行った被験者のうち被験者 E，I，J を除いた 7 名を対象に，慣れによる認証時間と本人拒否率の変化を調査する．

6.2.1　実験内容

実験 1 のを行った被験者のうち 7 名を対象に，同じ PIN コードを用いて週に 3 回，本提案システムを用いて 5 回認証の練習を 2 週間練習を行った．その後，実験 1 と同様に 10 回認証を行い計測した．実験後にアンケートを行

© 2025 Information Processing Society of Japan.

表 5　継続実験後アンケート項目

C1.	練習によって音の違いを判別することが容易になりましたか？
C2.	練習によって振動の違いを判別することが容易になりましたか？
C3.	練習によって使いやすくなったと思いますか？
C4.	背後から見られていたとしてもばれないだろうという安心感はありましたか？
C5.	重要なデータのロック解除に使用したいと思うか
C8.	その他、継続実験を行った感想やご意見があればご記載ください

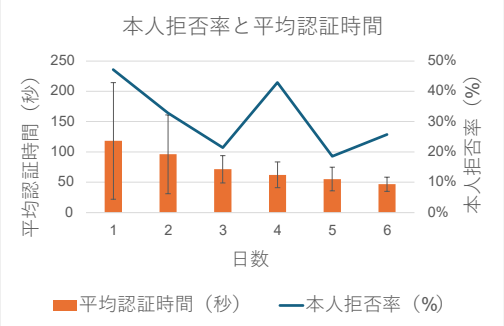

図 3　被験者全体の本人拒否率と平均認証時間の推移

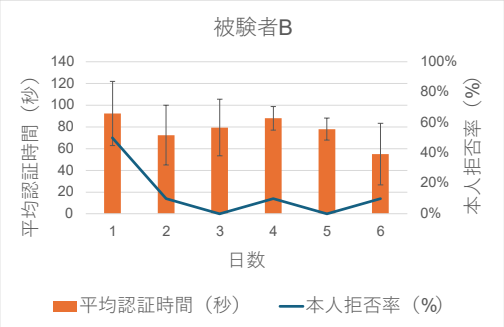

図 4　被験者 B の継続実験の結果

い，入力のしやすさに変化があったか調査した．アンケート項目を**表 5** に示す．

6.2.2　実験結果

2 週間で合計 6 回計測を行った継続実験全体の，本人拒否率と平均認証時間の推移を**図 3** に示す．2 週間練習した個人の結果として，実験 2 の参加者のうち実験 1 で本人拒否率が一番高い被験者 B と H，本人拒否率が低い被験者 G の本人拒否率と平均認証時間の推移を**図 4**，**図 5** と**図 6** に示す．それぞれのエラーバーは標準偏差を示す．全体で認証に成功した最小認証時間は被験者 D で，認証時間 17 秒であった．そのほかの，被験者は被験者 A が被験者 H と概ね同じような傾向であり，被験者 C と F は被験者 B と概ね同じ傾向であった．

6.2.3　アンケート結果

実験参加者の内 5 名から回答を得た．表 5 の C5.「練習によって使いやすくなったと思いますか」という問に対して 3 名の方が「そう思う」，2 名の方が「ややそう思う」と回答した．また，表 5 の C4.「背後から見られていたとしてもばれないだろうという安心感はありましたか」という問に対して 5 名全員が「そう思う」と回答した．

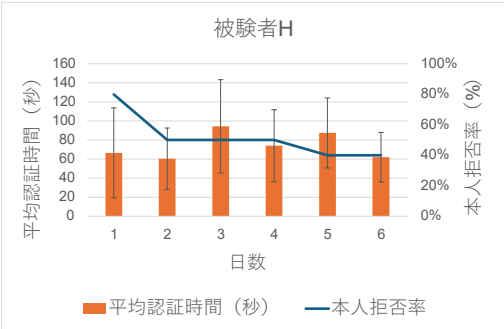

図 5　被験者 H の継続実験の結果

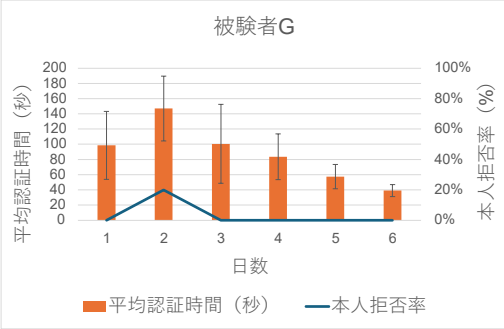

図 6　被験者 G の継続実験の結果

7.　考察

実験 1 の他人受入率の結果が 0%であったことから覗き見耐性を持つ認証手法であることがわかる．本人拒否率と平均認証時間との関係性について述べる．実験 1 の結果，本人拒否率が高い人であっても，認証時間が短いことや本人拒否率が低い人であっても平均認証時間が長い人もいることから本人拒否率と認証時間に関係はないと考えられる．また，実験 1 のアンケートの結果から，安心感をもって入力をできている人とできていない人に分かれたことがわかる．この問に関しては，安心感という問が正しく入力できている安心感と覗き見されていても PIN コードが特定されないと言う安心感が混在してしまった可能性がある．そのため，継続実験で「背後から見られていたとしてもばれないだろうという安心感はありましたか」というアンケートを行った結果，5 名全員が「そう思う」と回答したことから，覗き見攻撃に対しての安心感はあると考える．

実験 2 の全体の結果から本人拒否率と平均認証時間が 1 日目よりも低下しているため，本提案手法はトレーニングをすることで本人拒否率と認証時間を短縮することができると言える．また，実験 1 で本人拒否率が高かった被験者 B と被験者 H の結果を比較すると，2 日目に本人拒否率がどちらとも下がっているが，被験者 H は本人拒否率が 40%

© 2025 Information Processing Society of Japan.

と高い値で推移している．平均認証時間に着目すると両被験者ともに認証時間は短縮されていないことがわかる．一方，実験 1 で本人拒否率が低かった被験者 G の本人拒否率は，2 日目以外は，本人拒否率 0% であることがわかる．認証時間の推移に関しては，日数を重ねるごとに短縮されていることがわかる．

被験者 B，G，H 3 名と継続実験で最短認証時間の記録を出した被験者 D の条件の違いとして，指定した PIN コードがある．被験者 B の PIN コードは，「1 6 7 4」であり，振動回数は，1 回，3 回，1 回，1 回となっている．被験者 H の PIN コードは，「1 0 9 7」であり，振動回数は，1 回，4 回，3 回，1 回となっている．被験者 G の PIN コードは，「8 0 6 9」であり，振動回数は，2 回，4 回，3 回，3 回となっており，振動回数の多い PIN が多くあることがわかる．被験者 D の PIN コードは，「6 4 7 3」であり，振動回数は，3 回，1 回，1 回，3 回となっている．実験 1 を行った際に本人拒否率が高かった被験者 B と H を比較した際に，被験者 H の本人拒否率が高止まりしてしまった要因として PIN コードに振動の多い数字を複数含んでしまった可能性がある．しかし，被験者 G や最短認証時間を記録した被験者 D と被験者 H を同程度の振動回数の多い PIN コードであることがわかるため，本提案手法に慣れて行くことで振動の回数が本人拒否率や認証時間に影響を及ぼす可能性は低くなっていくと考える．

提案手法と関連研究の方式で本人拒否率，他人受入率と認証時間の比較を行う．江原ら [7] の振動を通知に用いた研究の認証成功率は 96.36%，他人受入率は 0%であった．また，認証平均時間は 16.07 秒であった．臼井ら [11] の音の特徴を用いた研究では，本人認証率は 93%，他人受入率は 17%であった．認証時間は評価を行っていなかった．本人拒否率は，音もしくは振動を用いている研究では，それぞれの認証成功率が 90%を超えているが，本提案手法では実験 1 の経験者 I の本人拒否率が 0%であるため，本人拒否率はトレーニングによって低下すると考える．一方で，他人受入率は本提案手法は，0%であることから関連研究よりも同程度以上の耐性があると考えられる．

8. まとめと課題

本研究では，スマートフォンの加速度センサ等を用い，画面の視覚情報を用いない認証手法を提案し，本人拒否率や他人受入率を調査した．実験 1 の結果から，他人受入率は 0%となり，覗き見耐性を持つ認証手法であることがわかる．実験 2 全体の結果からトレーニングによってばらつきはあるが本人拒否率が低くなっている点や平均認証認証も短縮されていることから，2 週間で概ね慣れることができるため，使用し続けることで本人拒否率と認証時間は短縮されるシステムであると言える．

今後の課題として，さらに認証時間を短縮していくことがある．今回はグループの違いを判別するために音を用い，それぞれの値の判別に振動を用いた．この音と振動を逆にすることで本人拒否率や認証時間が変化するのか検証していく．

参考文献

[1] SoftBank SELECTION，通勤・通学に電車やバスを利用するスマートフォンユーザー 500 人へのスマートフォン利用実態調査, 入手先 ⟨https://www.softbankselection.jp/privacy_enquete/⟩ (2024.06.03).
[2] MMD 研究所，イヤホン・ヘッドホンに関する調査，入手先 ⟨https://mmdlabo.jp/investigation/detail_2193.html ⟩ (2024.11.01).
[3] 濵野雅史, 新井イスマイル, “加速度センサ・ジャイロ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（UBI）, Vol.2014-UBI-41, No.17, pp.1–8, 2014.
[4] 古賀尭志, 小高知宏, 黒岩丈介, 白井治彦, “Android 端末上の加速度センサを用いた新しい生体認証システム”, 福井大学 大学院工学研究科 研究報告, Vol.64, pp.44–50, 2016.
[5] 成ケ澤遼太郎, 小倉加奈代, 児玉英一郎, 王家宏, 高田豊雄, “加速度センサとジャイロセンサを併用したスマホ回しによる認証手法の提案”, 平成 28 年度電気関連学会東北支部連合大会, 2016.
[6] 嘉藤鴻介, 渡辺一樹, 油田健太郎, 岡崎直宣, 朴美娘, “ウェアラブル端末を用いた覗き見耐性を持つジェスチャー認証手法の提案と評価”, 情報処理学会研究報告セキュルティ心理学とトラスト（SPT）, Vol.2021-SPT-41, No.17, pp.1–8, 2021.
[7] 江原知志, 高田哲司, “録画による覗き見攻撃に安全な個人認証のユーザインタフェース改良による実用性向上”, 情報処理学会論文誌, Vol.63, No.4, pp.1082–1093, 2022.
[8] 立花聖也, 高橋哲伸, 佐々木慎吾, 菊地友斗, 鎌田恵介, 小倉加奈代, ベッド B. ビスタ, 高田豊雄, “スマートデバイスにおける振動機能を利用したマルチタッチ解除方式の提案”, 情報処理学会第 78 回全国大会, 2016.
[9] Manisha Varma Kamarushi, Stacey L. Watson, Garreth W. Tigwell, Roshan L. Peiris, ”OneButtonPIN: A Single Button Authentication Method for Blind or Low Vision Users to Improve Accessibility and Prevent Eavesdropping”, Proceedings of the ACM on Human-Computer Interaction, No.:212, pp.1–22, 2022.
[10] M. Monjirul Kabir, Nasimul Hasan, MD Khalid Hassan Tahmid, Tanjil Ahmed Ovi, Victor Stany Rozario, “Enhancing Smartphone Lock Security using Vibration Enabled Randomly Positioned Numbers”, ICCA 2020: Proceedings of the International Conference on Computing Advancements, No.44, pp.1–7, 2020.
[11] 臼井健祐, 稲葉宏幸, “カクテルパーティ効果を利用した個人認証システムの改良”, コンピュータセキュリティシンポジウム 2013 論文集, Vol.2013, No.4, pp.459–465, 2013.
[12] 政重直希, 佐々木良一, “視覚と聴覚を併用した個人認証方式の提案”, コンピュータセキュリティシンポジウム 2011 論文集, Vol.2011, No.3, pp.78–83, 2011.

© 2025 Information Processing Society of Japan.