1W-06

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

立花聖也† 高橋啓伸† 佐々木槙吾† 菊地友斗† 鎌田恵介†
小倉加奈代‡ ベッド B. ビスタ‡ 高田豊雄‡
†岩手県立大学大学院 ‡岩手県立大学

1 はじめに

近年，スマートフォンをはじめとするスマートデバイスの利用者が急増しており，総務省の 2014 年の携帯端末利用率の調査によると，10 代から 60 代のスマートフォン利用率は 62.3 %と調査対象者の半数以上を占めている [1]．しかし，スマートデバイスには数多くの個人情報が含まれており，その情報の流出・漏えいは大きな問題である．その対策として，PIN コード認証方式やパターン認証方式，パスワード認証方式の主に 3 つの方式が用いられている．しかし，スマートデバイスのような携帯端末は公共の場で扱われることも多く，認証行動の覗き見や録画をされる可能性がある．その場合，既存の認証方式では再現が容易であるため，簡単に突破される．

そこで本研究では，覗き見攻撃に対しセキュリティ強度を高めるため，振動と 2 つの数字を同時にタッチするマルチタッチ入力を用いたマルチタッチロック解除方式を提案する．

2 関連研究

本研究同様に，覗き見や録画攻撃を想定した認証方式として，振動，マルチタッチを利用した認証方式に関する研究を概観する．

2.1 振動を利用した手法

石塚ら [2] は，携帯端末の振動機能を利用した Circle Chameleon Cursor という暗証番号による個人認証システムを提案した．この研究では，被験者に複数の認証行為を録画した映像を見せた録画攻撃実験を行い，提案手法の有効性を評価した．その結果，認証情報や振動が入った瞬間を特定できた被験者はおらず，覗き見，録画攻撃のいずれにも効果があることが示された．この研究のように振動を用いることは，利用者だけに伝える手段としては最適であり，本提案方式でも参考にした．一方，この手法の問題点は，認証情報の入力位置の決定を振動で利用者に知らせるため，利用者はその振動を待たなければならず，認証に要する時間が長くなる点である．

2.2 マルチタッチを利用した手法

益子 [3] は，タッチスクリーンのマルチタッチ機能とドラッグを利用した個人認証手法を提案した．この研究では，認証者の隣で認証の様子を見てもらい，なりすましを行う覗き見攻撃実験を行い，提案手法の有効性を評価した．その結果，完全に認証情報を特定できた被験者はおらず，なりすましによる認証成功者はいなかった．この研究から，認証に複数の指を用いた入力が認証情報の特定を困難とすることに役立っていることがわかる．一方，この手法の問題点は，ユーザへ求める認証操作の負荷が高い点である．

3 提案手法

本研究では，PIN コード認証において第三者に認証行為を見られても，認証情報の特定を困難とする個人認証方式を提案する．本提案で用いる主な機能について次節以降説明する．

3.1 振動によるフェイク

本提案では，スマートデバイスの振動機能を用いたフェイクを入れることで，入力の再現による突破を困難とする．振動を用いる目的は，端末に触れている利用者にのみフェイクを入れることを伝え，第三者にフェイクが入ったことの特定を困難とするためである．しかし，PIN コード認証のように一点だけに触れて認証情報を入力する方法では，振動によるフェイクを用いても覗き見攻撃者に対し，フェイクの入力であるかそうでないかを推測させるだけのものとなる．

そこで本提案では，覗き見攻撃者に対し推測すべき情報を増やすため，マルチタッチによる入力方法を組み合わせ，認証情報の特定を困難とする．

3.2 マルチタッチによる入力

本提案では，マルチタッチを用いて認証情報を入力する．振動によるフェイクだけでなく，マルチタッチを用いる理由は，どちらのタッチが正しい入力であるかを覗き見攻撃者から隠すためである．

本提案では，通常時入力とフェイク時入力の 2 種類の入力が存在する．

3.2.1 通常時入力

図 1 左側は，本提案で用いる認証画面である．画面上の各点には数字が割り振られており，利用者は，設定された認証情報に対応した数字ともう 1 つ別の数字をマルチタッチすることで，認証情報を入力することが求められる．図 1 では，1 が認証情報に対応した数字であり，利用者は 1 をタッチしなければならない．しかし，マルチタッチ入力が必要であるため，1 とそれ以外の任意の数字 (図 1 では 8) をタッチして，1 つ認証情報が入力完了となる．

3.2.2 フェイク時入力

フェイク時入力では，任意のタイミングで，図 2 左側のように端末が振動する．この振動が持つ意味は，「次はフェイクを入力する」という合図であり，本来タッチすべき数字以外のいずれかをマルチタッチ入力をす

A Proposal of Multi-touch Release System Using the Vibration Function in Smart Device
†Seiya Tachibana, Hironobu Takahashi, Shingo Sasaki, Yuto Kikuchi, Keisuke Kamada ‡Kanayo Ogura, Bhed Bista, Toyoo Takata
†Iwate Prefectural University Graduate School
‡Iwate Prefectural University

る必要がある．図2では，2が本来認証情報に対応した数字であるが，入力前に振動が発生したため，2を除くいずれかの2つの数字 (図2では3と9) をマルチタッチして，フェイク入力が完了する．

図 1: 通常時マルチタッチ入力例

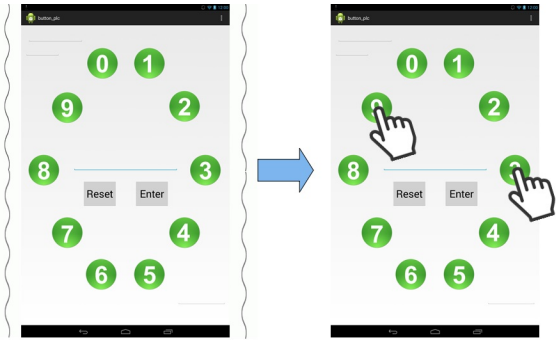

図 2: 振動によるフェイク時入力例

3.3 フェイク発生回数とタイミング

本提案の振動回数は，最大で，認証情報長/4(小数点以下繰り上げ) まで振動し，認証のたびに，振動によるフェイクのタイミングおよび回数が変動する．これにより，覗き見攻撃者は，マルチタッチによってどちらのタッチが正しい入力であるかを推測する必要があり，さらに，推測する入力がフェイクだった場合はそのどちらでもないため，認証情報の特定が困難になると考えられる．

4 覗き見耐性の評価実験

本提案について，実際に覗き見攻撃に耐性があるかプロトタイプシステムを用いて評価実験を行い確認する．実験内容は，大学生3名を被験者として，本認証方式の仕組みを説明した後，認証行為が録画された動画を見せ，実際にプロトタイプシステムを操作して覗き見攻撃を試行してもらう．この録画動画は，覗き見攻撃を想定し単一の認証行為が録画されたものであり，複数の認証行為を撮影して認証情報を特定する録画攻撃とは異なる．今回の実験は，「研究室などで，本認証方式を知っている第三者に認証行為を覗き見された場合に突破できるかどうか」という状況を想定する．各被験者は，暗証番号の長さが6ケタの場合と8ケタの場合のそれぞれで5回ずつ認証を試みる．

4.1 実験結果

実験より，6ケタの場合に認証に成功する被験者が1名いたが，8ケタではいなかった．

4.2 考察

実験結果より，認証に成功した被験者がいたが，振動のタイミングや認証情報の特定ができた被験者はいなかった．しかし，今回の実験では録画攻撃を考慮していない．また，現状の本提案の6ケタの場合では，1回の認証行為中に最大で2回ランダムなタイミングでフェイク入力が入る．その場合，1/625の確率で認証に成功することとなり，数通りの違う場面を撮影した録画映像によりさらに認証情報の特定が容易になるものと考えられるため，録画攻撃への耐性に問題があるといえる．録画攻撃対策として今後，以下の点について改良する予定である．

4.2.1 認証情報の長さの固定

実験の結果，6ケタのパターンで認証に成功した被験者がいたことから，認証情報の長さを8ケタ以上にする必要がある．これにより，攻撃者による認証成功確率は1/15625となり，攻撃成功率は低くなることが予想できる．

4.2.2 認証入力可能回数の制限

現在，スマートフォンなどで使用されているロック方式では機種によって違いはあるが，一定回数まで認証入力を行うことが可能であり，それを超えた場合は端末初期化処理が強制的に行われる．そこで，実験の制限と同様に認証入力可能回数を上限5回までとすることで，偶然に認証成功してしまう可能性を低くすることが考えられる．

4.2.3 フェイクのパターンの追加

現状よりもフェイクパターンを増やすことで複数の認証映像から認証情報の特定を困難にすることが考えられる．

5 まとめ

本稿では，振動と2つの数字を同時にタッチするマルチタッチ入力を用い，通常時とフェイク時それぞれの入力で認証を行うマルチタッチロック解除方式を提案した．また，覗き見攻撃に対する耐性があるか実験を行い，有効性が見込まれる結果となった．

今後は，4.2節で述べた録画攻撃への耐性を高めるための改良を進め，改めて本提案の有用性について検討する．

謝辞

本研究は，岩手県立大学大学院ソフトウェア情報学研究科およびソフトウェア情報学部によるプロジェクト学習（PBL2015-16）及びJSPS科研費26330159の助成を受けたものである．

参考文献

[1] 総務省 平成26年度情報通信メディアの利用時間と情報行動に関する調査報告書の公表，入手先 <http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000028.html>(参照日付：2016/1/7).

[2] 石塚正也，高田哲司：CCC：携帯端末での暗証番号認証における振動機能を応用した覗き見攻撃対策手法，情報処理学会論文誌，Vol.56，No.9，pp.1877–1888 (2015).

[3] 益子純平：タブレットPCのマルチタッチ機能を用いた個人認証手法の提案，岩手県立大学ソフトウェア情報学部卒業論文（2012）．