161C62
2016/3/2

スマートデバイスにおける振動機能とマルチタッチ機能を利用した覗き見攻撃対策認証方式の提案

立花 聖也[†1]　高橋 啓伸[†1]　佐々木 槙吾[†1]　菊地 友斗[†1]　鎌田 恵介[†1]　小倉 加奈代[†2]
ベッド B. ビスタ[†2]　高田 豊雄[†2]

概要：近年，スマートフォンをはじめとするスマートデバイス所有者が増加している．スマートデバイスには，個人情報が多く含まれているにも関わらず，その利便性や携帯性の高さから公共の場で扱われることが多いため，情報の流出・漏えいの問題が発生するリスクがある．そのため，所有者以外が端末の操作をできないように，端末をロックする方法がとられている．しかし，既存のロック方式である 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では覗き見された場合のセキュリティ強度は低くなる．本研究では，覗き見へのセキュリティ強度を高めるために，利用者のみがわかる端末振動機能と複数の点を同時にタッチする入力を利用した個人認証方式を提案する．

A Proposal of Shoulder Surfing Attack Measures Authentication Using the Vibration Function and Multi-touch Function in Smart Devices

SEIYA TACHIBANA[†1]　HIRONOBU TAKAHASHI[†1]　SHINGO SASAKI[†1]　YUTO KIKUCHI[†1]
KEISUKE KAMADA[†1]　KANAYO OGURA[†2]　BHED BAHADUR BISTA[†2]　TOYOO TAKATA[†2]

Abstract: In recent years, smart device owners, including smart phones are increasing. The smart devices contain a large amount of personal information. However, they are often used in public places for convenience and portability. Thereby, there is a spill or leakage problem of information. Therefore, as other than the owner does not operate the terminal, there is a method of locking the terminal. However, existing locking scheme such as PIN code authentication scheme, pattern authentication scheme, or password authentication scheme, the security strength is low when it is exposed to shoulder surfing. In this paper, in order to enhance the security strength against shoulder surfing, we propose a personal authentication scheme that employs multiple simultaneous touch mixed with fake by the terminal vibration function that only the user can be aware.

1. はじめに

近年，携帯電話の利用者が急増し，それに伴いスマートフォンをはじめとするスマートデバイス所有者も多く存在する．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 %と半数以上を占めている [1]．理由として，スマートデバイスは携帯性の良さや利用できるアプリケーションの豊富さの点で利便性が高く，多機能なために様々な用途に使用できるためである．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．そのため，端末の所有者以外が端末の操作を行えないようにしなければならない．現在使用されている端末のロック方式として，暗証番号を入力する PIN コード認証方式や，画面上に表示された 9 つの点から所有者が決めたルートを再現するパターン認証方式，パスワード認証方式の 3 つの既存認証方式がある．しかし，スマートデバイスのような携帯端末は使用される環境が多岐にわたり，状

[†1] 現在，岩手県立大学大学院
Presently with Iwate Prefectural University Graduate School
[†2] 現在，岩手県立大学
Presently with Iwate Prefectural University

況に応じては第三者が認証情報を入手するために，認証行動の覗き見や録画を行う場合も想定される．そのような場合，既存の認証方式では再現性が高いため，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，振動と複数の点を同時にタッチする入力を利用したフェイク認証方式の提案を行う．

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，音，振動，2 点以上の同時タッチを利用した認証方式を概観する．

2.1 音を利用した手法

竹田ら [2] は，人間の聴覚効果である，複数の音源から自分の意識した音を聞き分けるカクテルパーティ効果を利用した個人認証システムを提案した．これは，複数の音源から成る混合音というものを使用して，複数回異なるパターンの混合音が再生された中から，認証音を含む混合音のパターンを識別して回答する手法である．この研究では，被験者を用いて覗き見や盗み聞きされた場合の攻撃実験を行っている．実験内容として，4 つの混合音を順に再生し，それぞれに認証音が入っているか否かを被験者に伝え，認証音の推測を行わせている．その後，認証音は同一のまま認証実験を 3 回行い，他人拒否率を算出している．結果として，他人拒否率は平均で 60.8%であり，一概に覗き見・盗み聞きに対して安全性が高いとは言えない．しかし，一度に再生する音源の数を増やした混合音を用いた実験の結果，本人受入率への影響は僅かになっており，覗き見・盗み聞きに対応可能な根拠を示している．この手法の問題点は，音を利用した手法であるため，音が聞き取れないほどの大きな環境音がある場所では使用できず，使用環境が限定される点である．また，聴覚効果には個人差があるため，人によっては聞き取れない可能性がある．

2.2 振動を利用した手法

石塚ら [3] は，携帯端末の振動機能を利用した CCC(Circle Chameleon Cursor) という暗証番号による個人認証システムを開発した．この認証システムでは，数字が割り振られたダイヤルの上を回転するインジケータがあり，インジケータが回転している途中で端末に振動が発生する．インジケータの回転停止後，ダイヤルを操作して，その時点で入力すべき番号と振動が発生した位置を合わせることで入力を行う．この振動を用いることで，覗き見攻撃による認証情報の特定を困難としている．この研究では，被験者を用いて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った．その結果，認証情報を特定できた被験者も，振動が入った瞬間を特定できた被験者もおらず，結果として覗き見，録画攻撃のいずれにも効果があることが示された．先行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ている．しかし，この手法では振動で入力位置を指定することに用いているのに対し，本提案方式では，フェイクを入れる合図として振動を用いているという違いがある．この手法の問題点は，入力のたびにインジケータの回転による入力位置の決定を待たなければいけないため，認証に要する時間が長くなる点である．

2.3 2 点以上の同時タッチを利用した手法

益子 [4] は，タッチスクリーンの 2 点以上の同時タッチ (以下，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．これは，画面上に複数のチェックポイントが用意されており，通過すべきチェックポイントの数と，通過する際の指の本数を認証情報に用いた手法となっている．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った．その結果，認証情報の一部を特定できた被験者が数名いたが，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 1 人もいなかった．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示された．本提案方式でも，指を複数本用いた入力を利用しているが，益子の手法のように指の本数を認証情報に用いてはいないという点で異なっている．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．

他にも，2 点以上の同時タッチを利用した手法として澤村ら [5] の提案があるが，この手法は既に覗き見への耐性の問題が益子の研究で指摘されている．

3. 振動機能とマルチタッチを用いた端末認証方式の提案

本研究では，第三者に認証行為を見られても，視覚情報から認証情報の特定を困難とする個人認証方式を提案する．

本認証方式で用いる主な機能は次の 2 つである．

(1) 振動によるフェイク
(2) マルチタッチによる入力

これらの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

本認証方式では，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．これは，ランダムなタイミングで端末を振動させ，そのタイミングを利用してフェイクの操作を織り交ぜることで，覗き見攻撃者からパスワードの特定を防ぐ．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，第三者によるフェイクが入ったタイミ

ングの特定を困難とするためである．しかし，PIN 認証方式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ってしまう．

そこで本認証方式では，覗き見攻撃者へ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，覗き見攻撃者からの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

本認証方式では，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として，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．

本認証方式では，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．それぞれの入力について図を用いて説明を行う．

3.2.1 通常時入力

図 1 左側は，本認証方式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点ともう一点別の点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 の例では，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，入力にはマルチタッチが必要なため，1 とそれ以外の適当な数字 (図 1 の例では 8) をタッチして，1 つ認証情報が入力される．

図 1 通常時マルチタッチ入力例

3.2.2 フェイク時入力

本認証方式では，任意のタイミングで，図 2 の左側のように端末が振動する．この振動が持つ意味は，次の入力はフェイクを入れる合図であり，本来タッチすべき数字以外のいずれかをマルチタッチすることでフェイク入力をする必要がある．図 2 の例では，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 の例では 3 と 9) をマルチタッチして，フェイク入力が完了する．

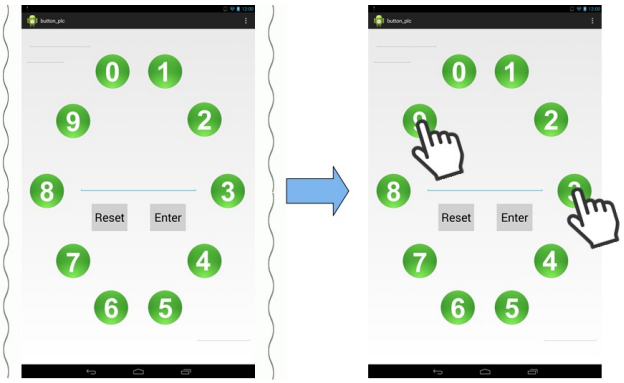

図 2 振動によるフェイク時入力例

3.3 フェイク発生の回数とタイミング

本認証方式の振動の回数は，最大で，認証情報の長さ/4 まで振動する．また，認証のたびに振動によるフェイクのタイミング，回数いずれも変動する．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．

3.4 想定される使用状況

本認証方式はスマートデバイスを必ず手に持っているか身に着けていることを想定する．理由として，本認証方式はフェイク発生時にスマートデバイスが振動するため，机などの物体にスマートデバイスが接触していると音が響いてしまう．それにより，フェイクが入ったことが第三者に知られる可能性があり，認証情報を特定されることが懸念されるためである．

4. 予備実験

本認証方式について，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予備実験を行い確認をした．実験内容は，本学ソフトウェア情報学部の学生 3 名を被験者として，認証作業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った．今回の予備実験は，「電車など，一度きりしか会わない人に覗き見を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．そのため，被験者は本認証方式のシステムを知らない状態で実験を行う．各被験者には，暗証番号の長さが 4 ケタの場合と 8 ケタの場合の 2 通りを 5 回ずつ認証を試行してもらい，認証が成功した場合は，何回目の回答で認証成功したか記録する．また，実験中は被験者の認証行為を撮影する．これは，撮影した映像からどのような入力を行っていたか確認するためである．

4.1 実験結果

予備実験により得られた各被験者の結果を表 1 に示す．

表 1 予備実験時の各被験者の覗き見攻撃結果

	4 ケタ	8 ケタ
被験者 1	失敗	失敗
被験者 2	成功 (1 回目)	失敗
被験者 3	失敗	失敗

表 1 より，4 ケタのパターンで認証成功してしまう被験者がいたが，8 ケタのパターンでは認証に成功した被験者はいなかった．また，認証に成功した被験者を撮影した映像を確認したところ，認証に成功した瞬間に驚く素振りをしていたことから認証情報の特定までには至っていなかったと考えられる．

次に，被験者 1 と被験者 3 を撮影した映像を確認したところ，一度入力しては回答せずに入力内容を消すという行動が見受けられた．これは，攻撃試行中に，本認証方式では振動が発生することを知り，端末が発する振動が何かしらの意味を持っていると推測し，規則性を見出そうと試行錯誤していたと考えられる．しかし，最終的に認証に失敗していたため，本提案方式の仕組みを想起することは困難であったものと思われる．

4.2 考察

今回の予備実験では覗き見耐性の確認を目的とし，録画攻撃を考慮したものとはなっていない．しかし，現状の本認証方式では，4 ケタの場合 1/125 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，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以下を検討する．

4.2.1 認証情報の長さの固定

予備実験の結果，4 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，最大 20 回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を初期化する処理が強制的に行われる．そこで，予備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とすることが考えられる．

5. おわりに

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の 2 通りの入力で認証を行うマルチタッチロック解除方式の提案を行った．また，覗き見攻撃へ耐性があるか予備実験を実施し，その結果と考察を述べた．

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，改めて本認証方式の有用性について検討する．また，今回は本認証方式を知らない攻撃者を想定し予備実験を行ったが，本認証方式を知っている攻撃者を想定し，覗き見および録画攻撃耐性の評価を行う．

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学生主体のプロジェクト学習 (PBL) の一環として実施したものである．本研究の一部は，プロジェクト学習 (PBL2015-16) 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：2015/12/20).
[2] 竹田昂生，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提案，信学技報，Vol.112，No.127，SITE2012-36，pp.217–221，(2012).
[3] 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).
[4] 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 2011 年度，pp.1–52(2012).
[5] 澤村隆志，成田匡輝，野地脩宏：マルチタッチスクリーンを利用した認証方式の提案，コンピュータセキュリティシンポジウム 2010 論文集，第二冊，pp.645–650 (2010).