タッチパネル端末の特性を利用した覗き見攻撃耐性をもつ個人認証手法

東山 侑真 † 岡村 真吾 ‡ 矢内 直人 † 藤原 融 †

† 大阪大学
565-0871 大阪府吹田市山田丘 1-5

‡ 奈良工業高等専門学校
639-1058 奈良県大和郡山市矢田町 22

あらまし 近年，スマートフォンが爆発的に普及し，よく街中でも見掛けることが多い．しかし，街中のような人の目に多く晒された環境において画面ロック解除といった認証処理を行った場合，背後にいる第三者に暗証番号 (秘密情報) を盗まれる危険性が高い．そこで本研究では，タッチパネル端末の特性を利用した覗き見攻撃耐性をもつ個人認証手法を提案する．本手法ではチャレンジ＆レスポンス認証を採用しており，チャレンジにスワイプ機能，レスポンスにタップ圧力をそれぞれ利用する．また，安全性とユーザビリティの二つの観点から提案手法の有用性を検証する．

User Authentication with Shoulder-Sufing Resistance using Properties of Touch Panel

Yuma Higashiyama† Shingo Okamura‡ Naoto Yanai† Toru Fujiwara†

†Osaka University
1-5 Yamadaoka, Suita-shi, Osaka 565-0871, JAPAN
‡Nara National College of Technology
22 Yatacho, Yamatokoriyama-shi, Nara 639-1058, JAPAN

Abstract Recently, we often use smartphones on the street. If a PIN authentication is used in a public place exposed to many people's eyes, there is a high risk of stealing a PIN by shoulder surfing attacks. In this study, we propose a new challenge-response authentication method with shoulder surfing resistance using properties of touch panel. The proposed method uses a swiping for receiving a challenge and a touch pressure for providing a response. We also evaluate the secrecy and the usability of the proposed method.

1 はじめに

近年，スマートフォンが新しい情報端末として広く普及してきている．スマートフォンは，音声通話や電子メールだけでなく，パソコンと同様にインターネット上でのサービスが利用可能など高い利便性を備えている．その一方，仕事上の大切なデータやプライバシー情報といった機密性の高い情報が端末に保存されるため，悪意をもつ第三者の不正利用に伴う情報漏えいのリスクが大きい．

端末の不正利用に対するセキュリティとして，画面ロック機能がある．スマートフォンにはPIN (Personal Identification Number) やパターン記憶による画面ロック機能が搭載されている．しかし，これらの個人認証手法では，人の目に多く晒された環境において認証動作を行った場合，PIN やパターンなどの秘密情報を簡単に盗まれてしまう危険性がある．このような背景から，背後から覗き見られても安全な個人認証手法の確立が望まれている．

覗き見攻撃耐性をもつ認証方式として，人の

生体情報を利用したバイオメトリック認証がある．バイオメトリック認証とは，指紋や顔といった身体的特徴や筆跡やキーストローク [1] といった行動的特徴によって本人確認を行う認証方式のことで，生体情報の唯一性により覗き見攻撃に対して原理的に安全であると言える．しかし，本人の生体情報が漏えいした場合，他人に生体情報を偽造されることで簡単に認証突破される危険性がある．

別の方式として，チャレンジ＆レスポンス認証方式を用いたものがある．チャレンジ＆レスポンス認証方式とは，チャレンジと呼ばれるワンタイム情報がユーザに送られ，それとユーザが設定した秘密情報の演算結果をレスポンスとして返すことで個人認証を行う方式である．このとき，レスポンスはチャレンジに依存するため認証の度に異なる．しかし，この認証手法を人の脳で演算可能な範囲で利用しようとした場合，本来の複雑な演算が不可能になる．このため，チャレンジとレスポンスから秘密情報が演算できるおそれがある．この問題の対策として，チャレンジを攻撃者に知られないよう秘匿化する方法 [2]-[3] が提案されている．チャレンジを秘匿化することで，攻撃者は秘密情報の推測が困難となる．結果として，複数回の覗き見攻撃による秘密情報の漏えいの可能性を低下させることができるが，それに伴ってユーザビリティが低下するという問題がある．

そこで本研究では，安全性の向上に伴うユーザビリティの損失が小さく，複数回の覗き見攻撃耐性をもつチャレンジ＆レスポンス認証手法を提案する．以前発表した手法 [4] では，圧力センサを利用することにより，適当に入力するランダム攻撃に対する安全性を向上させたが，認証時間が長いといった問題があった．なお，認証時間とは，認証に必要な操作を開始してから終了するまでの時間を意味する．よって提案手法では，スマートフォンなどが備えるタッチパネルの特性を利用することで，高いランダム攻撃耐性を維持しつつ，認証時間の短縮を図る．既存手法と提案手法を安全性・ユーザビリティの二つの観点で比較し有用性を検証する．

2 既存手法

2.1 フリック入力を対象としたキーストローク認証

キーストローク認証とは，キーストロークデータに含まれる個人特有のパターンを行動的特徴として利用するバイオメトリック認証である．フリック入力を対象としたキーストローク認証 (以下，フリック認証) [5] では，スマートフォンによるフリック入力を行う際の個人認証可能性について検討している．

図 1: フリック認証 [5]

フリック認証では，従来のキーストロークデータに加えてスマートフォンにおけるセンサ情報を利用する．センサ情報はフリック時の押下圧，フリック角度，フリック距離，フリック時間の四つの特徴量である．これらの情報を，重み付きユークリッド距離法と Array Disorder 法を組み合わせた手法により識別する．認証画面は図 1 のようになっており，文章を 1 文字ずつフリック入力することで認証を行う．実験により 100 文字程度の入力で識別が可能なレベルに達することが判明しているが，入力動作が多く，認証時間が長いといった問題がある．

2.2 Fake Pointer

Fake Pointer[2] では，攻撃者が複数回の認証行為を背後から覗き見するという脅威という脅威を想定している．この脅威への対策として，攻撃者が認証行為から入力数値を判定不可能にすることで覗き見攻撃耐性をもたせる．

前提として，ユーザは事前に 4 桁の PIN (秘密情報) を認証者へ登録している．まず始めに，

図 2: 数字キーの操作例

選択シンボル情報と呼ばれるチャレンジを取得する．選択シンボル情報は四つの記号で構成される．選択シンボル情報は，人の目に晒されない場所で確認する必要がある．

次に，レスポンスとして秘密情報と選択シンボル情報の入力を行う．Fake Pointer の認証画面には記号を背景としたパネル上に数字が表示されている．このうちパネル上の数字は左右ボタンによりその配置を一つずつ移動させることができる．この動作により，秘密情報と選択シンボル情報を重ね合わせ入力する (図 2)．入力の際には，目的のパネルを直接タップするのではなく決定ボタンをタップする．また，入力は 1 桁ずつ行う．

以上の認証動作により，攻撃者は複数回認証動作を見た場合でもチャレンジと秘密情報を推定することができないので，複数回の覗き見攻撃耐性をもつと言える．しかし，認証の度に人の目に晒されない場所に移動し選択シンボル情報を確認しなければならない点や，1 桁あたりのタップ数が多い点，1 桁あたりの入力パターンが 10 個しかないという点で問題がある．

2.3 加算型 PIN 認証

加算型 PIN 認証 [3] では，攻撃者が複数回の認証行為を背後から覗き見するという脅威を想定している．この脅威への対策として，被認証者に対する攻撃者の距離からでは判別困難な情報をチャレンジとして与えることで覗き見攻撃耐性をもたせる．

前提として，ユーザは事前に 4 桁の PIN (秘密情報) を認証者へ登録している．まず始めに，0〜9 の数字のうちの一つをチャレンジとして取得する．チャレンジの伝達方法として，ヘッドホンを介して音声で提示する方法と，重畳画像で提示する方法がある．前者では，他人に聞こえない程度の音量でチャレンジをヘッドホンを介して音声で提示する．後者では，認証画面 (図 3) の右下の領域に重畳画像としてチャレンジを表示する (図 4)．次に，秘密情報の現在の桁とチャレンジを加算し，その一の位をレスポンスとして入力する．入力の際には，演算結果の数字を直接タップする．

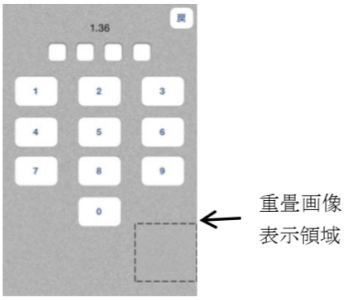


図 3: 加算型 PIN 認証 [3]

図 4: 重畳画像の例 [3]

以上の動作を 4 桁分行うことにより，攻撃者は複数回認証動作を見た場合でもチャレンジと秘密情報を推定することができないので，複数回の覗き見攻撃耐性をもつと言える．しかし，ヘッドホンが無く，攻撃者が重畳画像を視認できる範囲にいる場合では，PIN と同等の安全性になるという問題がある．また，計算能力によってはユーザビリティが低下する可能性が考えられる．

3　提案手法

3.1　認証手順

既存手法は複数回の覗き見攻撃に対して頑健ではあるが，安全性向上に伴ってユーザビリティが低下するという問題があった．そこで本研究では，安全性の向上に伴う認証時間の増加や認証状況の制限といったユーザビリティの損失が小さく，複数回の覗き見攻撃耐性をもつチャレンジ＆レスポンス認証手法を提案する．

提案手法では，Fake Pointer や加算 PIN 認証と同じ脅威を想定している．この脅威への対策として，視覚と聴覚では判別困難な情報をチャレンジとして与えることで覗き見攻撃耐性をもたせる．前提として，ユーザは事前に 0〜9 の数字及び 8 種類の記号から構成される 4 桁の秘密情報 (図 5) を認証者へ登録している．

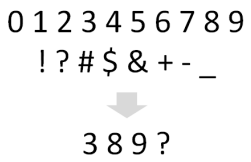
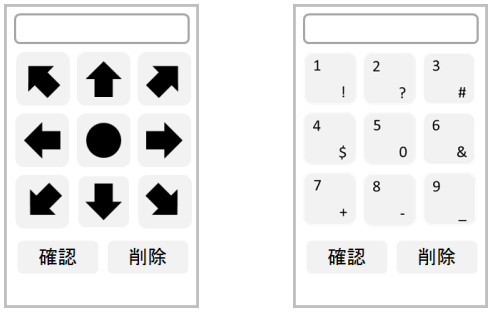


図 5: 4 桁の秘密情報の例

提案手法ではチャレンジを取得するときとレスポンスを入力するときで画面表示が異なる．まず始めに 8 方向の矢印または矢印無しのうちの一つをチャレンジとして取得する．認証画面 (図 6a) 上に表示されている 8 方向の矢印または矢印無しの九つのパネル上を図 7 のように乙の字を描くようにスワイプすると，ランダムで選ばれたパネル上を指が通過する際にバイブレーション機能により端末が振動する．

このとき，振動したパネル上の矢印がチャレンジとなる．スワイプ動作中に振動するパネル上で減速したり，何度もパネル上を行き来することにより攻撃者にチャレンジを特定される問題も考えられるが，スワイプ動作を減速したり途中で止めたりした場合にスワイプをやり直させる (チャレンジを再発行する) ことで，この問題を解決している．1 回のスワイプで正しいチャレンジを受け取ることができなかった場合は，認証画面上の確認ボタンをタップすること



(a) チャレンジ取得画面　(b) レスポンス入力画面

図 6: 提案手法

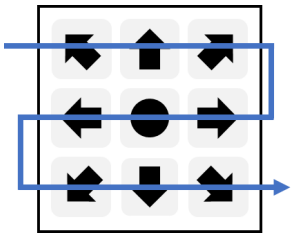


図 7: チャレンジの取得方法

で再度チャレンジを受け取ることができる．

すべてのパネル上をスワイプで通過すると，認証画面は図 6b のように切り替わる．次に，秘密情報の現在の桁が表示されてるパネルから見て，チャレンジの矢印方向にあるパネルをレスポンスとして入力する．入力の際には，矢印方向のパネルを直接タップする．またタップの際には，秘密情報が元パネル上の左上にあれば弱く，右下にあれば強くタップする．なお，強弱判定方法については，第 3.2 節で説明する．

以上の動作を 4 桁分行うことで，本人確認を行うことができる．提案手法では，レスポンスの直接入力を実現することにより，以前発表した手法 [4] に比べて 1 桁あたりのタップ数を大幅に削減した．また，スワイプ動作により短時間でチャレンジを受け取ることができるので，音声に比べてチャレンジ伝達時間が短くなると考えられる．これにより，全体的な認証時間の削減を図っている．

3.2 タップ圧力の強弱判定

タップ圧力はタッチパネル端末に搭載されている圧力センサから取得する．しかし，個人内及び個人間でタップ圧力の強弱にばらつきがあるといった問題が存在する．そこで，20 代の大学生 10 名のタップ時圧力の推移データを元に閾値の設定を行った．図 8 は測定した 200 個分の推移データから得たタップ時の最大圧力の分布であり，上方の放物線が強くタップした時の最大値の分布，下方の放物線が弱くタップした時の最大値の分布を示している．

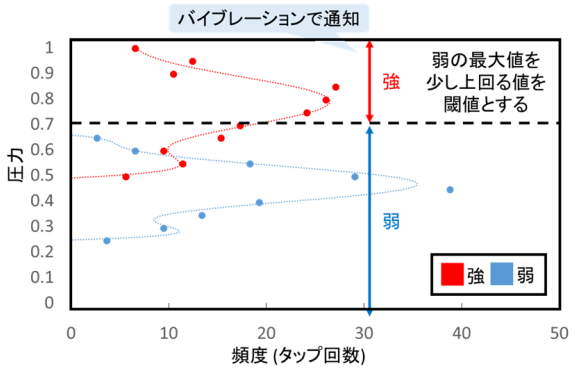


図 8: タップ時の最大圧力の分布

強弱判別にあたって，提案手法では弱を少し超える値を閾値と設定することで，弱タップ時の成功確率を向上させた．これは弱くタップすることに対し，強くタップすることの方が容易であることが理由となっている．一方，強タップ時だが，閾値を超えた場合にバイブレーションで通知することにより，ユーザの制御を可能にした．これにより，ユーザは強弱を区別してタップすることができる．

4 評価

4.1 安全性

PIN 方式，Fake Pointer，加算型 PIN 方式，提案方式の四つの認証方式において，事前に登録する秘密情報を i 桁とした場合の攻撃成功確率を表 1 に示す．攻撃方法として，適当に入力するランダム攻撃と複数回の覗き見攻撃を想定している．なお，複数回の覗き見攻撃とは，被認証者の複数回に及ぶ認証行為を覗き見た際に得られる情報を用いて行う攻撃を意味する．

表 1: 認証方式に対する攻撃成功確率

認証方式	ランダム攻撃	覗き見攻撃
PIN	$(1/10)^i$	1
Fake Pointer[2]	$(1/10)^i$	$(1/10)^i$
加算型 PIN[3]	$(1/10)^i$	$\geq (1/10)^i$
提案手法	$(1/18)^i$	$(1/18)^i$

同表では，ランダム攻撃と覗き見攻撃で攻撃成功確率が変わらなければ覗き見攻撃耐性をもち，そうでなければ覗き見攻撃耐性をもたないことを示している．加算型 PIN の覗き見攻撃成功確率は，攻撃者が重畳画像を視認できる範囲にいる場合，増加する可能性がある．Fake Pointer と提案手法はどちらも覗き見攻撃耐性をもつが，Fake Pointer に比べて提案手法の攻撃成功確率が低いことから，提案手法の安全性が高いことが分かる．提案手法では，レスポンス入力時にタップ圧力の強弱を判別することで 1 入力あたりのパターン数を増加した．これにより，PIN 方式や加算型 PIN 方式と同等のタップ数を維持しつつ，安全性を向上させることができた．

4.2 ユーザビリティ

Fake Pointer，加算型 PIN 方式，提案方式の三つの認証方式について，チャレンジ受取時，レスポンス演算時，レスポンス入力時に分け比較し，ユーザビリティを評価する．

三つの認証方式はそれぞれチャレンジの受け取り方法が異なる．加算型 PIN 認証や提案手法が認証時に受け取るのに対し，Fake Pointer は認証前に安全な場所で受け取る必要がある．これにより，記憶負荷や高頻度の認証が困難といった問題が生じる．加算型 PIN 認証では，音声でチャレンジが伝達される場合，伝達に時間が掛かり，結果として認証時間が長くなるという問題がある．提案手法では，スワイプ動作とバイブレーション機能により端末を保持してい

るユーザにのみチャレンジを伝達できるので，認証状況の制限が緩い．しかし，スワイプ動作により認証時間が長くなるという問題がある．

次に，レスポンスの演算について考える．ここで演算とは，チャレンジとして与えられた値から入力する値を求める処理を意味する．Fake Pointer ではチャレンジとして与えられる選択シンボル情報をそのまま入力に用いるので演算する必要がない．一方，加算型 PIN 認証では秘密情報にチャレンジを加算して入力する値を求める演算が，提案手法では秘密情報が記されたパネルの位置からチャレンジで与えられる矢印の方向にあるパネルの位置を求める演算がそれぞれ必要である．

最後に，レスポンスの入力について考える．加算型 PIN 認証や提案手法では，どちらも演算結果を直接タップするだけなので，タップ回数は 1 回である．一方，Fake Pointer では秘密情報と選択シンボル情報を重ねる必要があるため，タップ回数は左右移動と決定を含めた 1〜6 回となる．

以上より，認証状況という観点でユーザビリティについて考えた場合，提案手法では他手法とは異なり，安全確保のために認証状況を制限する必要がない．しかし，認証時間という観点で考えた場合，提案手法ではチャレンジの受取とレスポンスの演算に時間が掛かるため，他手法に比べて認証時間が長くなる可能性がある．一方，Fake Pointer では認証に伴うタップ数が多いことが，加算型 PIN 認証では音声にチャレンジを伝達していることが認証時間の増加を招いており，ユーザビリティを低下させている．今後は，認証実験により，実験値でのユーザビリティの評価を行う必要がある．

5　おわりに

本稿では，タッチパネル端末の特性を利用した覗き見攻撃耐性をもつ個人認証手法について述べた．最初に，既存手法として，フリック入力によるキーストローク生体認証，チャレンジ＆レスポンス認証におけるチャレンジを秘匿化した認証方式について説明した．次に，提案手法として，タッチパネル端末の特性であるスワイプ機能やバイブレーション機能，圧力センサを利用したチャレンジ＆レスポンス認証手法について説明した．最後に，既存手法と提案手法を安全性とユーザビリティの二つの観点で比較し有用性を検証した．結果として，提案手法は既存手法に比べて安全性の向上に伴うユーザビリティの損失が小さく，複数回の覗き見攻撃耐性をもつことを分かった．

今後の課題として，(1) 認証実験，(2) タップ時の強弱判別成功確率の向上，(3) ユーザビリティの評価基準の策定及び評価，の三つが挙げられる．

参考文献

[1] S.Banerjee, D.Woodard, “Biometric authentication and identification using keystroke dynamics: A survey, ” Journal of Pattern Recognition Research, Vol.7, No.1, pp.116-139, Jul. 2012.

[2] 高田 哲司, “Fake Pointer: 映像記録による覗き見攻撃にも安全な認証手法, ” 情報処理学会論文誌, Vol.49, No.9, pp.3051-3061, Sep. 2008.

[3] 磯貝 尚明, 長谷川 まどか, 篠田 一馬, 加藤 茂夫,“ 覗き見攻撃耐性を考慮した加算型 PIN 認証方式に関する一検討, ” 情報処理学会研究報告, Vol.2013-SPT-6, No.1, pp.1-6, Jul. 2013.

[4] 東山 侑真, 岡村 真吾, 藤原 融, “覗き見耐性をもつ認証手法の圧力センサによる改善, ” 電子情報通信学会 2014 年総合大会, A-7-4, Mar. 2014.

[5] 佐村 敏治, 泉 将之, 西村 治彦, “スマートフォンにおけるセンサー情報を用いたキーストローク生体認証, ” 電子情報通信学会技術報告, BioX2013-4, Vol.4, pp.1-6, Aug. 2013.