CCC:振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案

石塚 正也[1,a)]　高田 哲司[1,b)]

概要：本論文では個人認証における脅威の一つである覗き見攻撃に対して，安全性を向上しうる新たな携帯端末向けの認証方法を提案する．この脅威に対する既存の対策方法は，入力方法が複雑，秘密情報の増大に伴う記憶負担の増大，専用デバイスが必要という問題が指摘されている．これに対して我々は，市販のスマートフォンで暗証番号認証を行うことを想定し，スマートフォンの振動機能を秘密共有に応用することで覗き見攻撃への安全性を向上しうる，記憶負担も既存の暗証番号による認証と同一であり，専用デバイスを必要としない認証手法，CCC(Circle Chameleon Cursor) を考案した．提案手法を Android 搭載スマートフォンに実装を行い，そのシステムを利用して 10 人の被験者による覗き見攻撃実験を行った結果，入力値を特定できた被験者は 0 人という結果になった．

CCC:Shoulder Surfing Resistant Authentication System by Using Vibration

Masaya Ishizuka[1,a)]　Tetsuji Takada[1,b)]

Abstract: In this paper, we proposed a simple and secure Personal Idenfication Number(PIN) authentication scheme against shoulder surfing attack using a vibration of mobile device. A shoulder surfing attack(also known as an observation attack,social hacking) is an actual threat for cell phone users. Some research works propose a secure authentication scheme againsta this attack. These schemes have issues such as a complex input method, increased memory load for a secret and required an additional device. Our scheme CCC(Circle Chameleon Cursor) focuses on improving a PIN authentication on a smart phone and resolves above issues. The features of our scheme as follows: 1) We use two secret and the second secret is shared with a vibration signal between a mobile-phone and a user. It makes hard to retrieve an input value even if an attack has some movies about both a screen and an input operation. 2) The scheme does not increase a memory load of a secret. And 3) The scheme does not need an additional dedicated device. We implemented a prototype system on an Android smart-phone and conducted a shoulder surfing attack experiment with 10 subjects using the system. The result was that no one succeeded to identify an input value.

1. はじめに

携帯端末の普及とそれに伴い，携帯端末で利用できる電子通貨や割引といったサービスも増えつつある．この結果，携帯端末を通じて個人認証を行う機会は増えつつある．

多くの携帯端末は Personal Identification Number(PIN) やパスワード，パターンロックといった方法の認証方式を提供しており，利用者は自分で選択した認証方式を用いることができる．

しかし，これらの認証手法は、第三者に認証行為を見られると暗証番号やパスワードを知られてしまうという問題がある．これを「覗き見攻撃」と呼ぶ．加えて，攻撃者はカメラの性能向上から手軽に，そして攻撃対象者に認識されずに撮影ができるようになった．特に携帯端末は，公共の場で認証する機会があるため，攻撃者によって撮影されていることに，認証中の利用者が認識していない可能性がある．

[1] 電気通信大学 大学院情報理工学研究科
182-8585 東京都調布市調布ケ丘 1-5-1
[a)] ishizuka@uec.ac.jp
[b)] zetaka@computer.org

認証においてカメラ録画による覗き見攻撃は大きな脅威になる．人間による覗き見攻撃と異なり，記録できる視覚情報の多さ，データ化することで複数回，複数人の解析が可能であるためである．

本論文では携帯端末上での個人認証において，ビデオカメラに認証操作を複数回記録されたとしても，その記録から暗証番号を特定困難にする個人認証手法を提案する．

2. 関連研究

Undercover [1] は，パスワードと手で覆ったトラックボールの上下左右の回転の方向と振動を利用して秘密情報を共有する認証方式である．問題点は，認証のためのトラックボールが必要となる点である．fakePointer [2] は，既定の暗証番号とランダムに生成された値を組み合わせて入力値を確定させる認証手法である．問題点は，秘密情報を共有するために安全な通信路が必要である点である．Phone Lock [3] は，各入力マスの選択肢に割り当てられている数値を，視覚情報でなく振動パターンで伝達する方式である．問題点として振動パターンと数値の対応表を記憶する必要が有り，記憶負荷が増大する点である．

3. CCC(Circle Chameleon Cursor)

安全性向上策について，金庫の暗証番号入力つまみを例にして説明する．金庫の入力つまみは，つまみの上方に入力値を指し示すための箇所 (以後カーソルと述べる) が 1 つだけある．したがって第三者の入力操作を眺め，カーソルで指し示す数字を見ていれば暗証番号が特定可能である．

そこで CCC ではカーソルの位置を 1 箇所に固定しないこと，視覚的にカーソル位置を特定が困難になるように設計した．カーソルの位置を視覚的に判別が困難にすれば第三者が入力操作を眺めていても暗証番号の特定が困難になるからである．

一方でこの手法では正規利用者も複数あるカーソル候補の中でどれで暗証番号を指し示すかが不明であるため，正しいカーソルの位置を認証システムと共有する必要がある．そこで CCC では，振動機能を利用して利用者と認証システム間で入力カーソルを共有する．

図 1 は提案システムのインターフェース画面である．インターフェース画面は大きく 3 つの部分から構成される．上から，入力状況のインジケーター，暗証番号入力用つまみ，操作用のボタンで構成されている．また，暗証番号入力用つまみには，暗証番号入力用カーソルを利用者に伝達するために使用されるインジケーターが用意されている．なお，システムは Web アプリケーションとして実装されている．

認証方法について説明する．以降では数字 1 つの入力操作について説明する．実際の認証では暗証番号の桁数回この入力操作を繰り返す．入力操作は以下の 2 つの操作からなる．

手順 1:入力位置 (マス) の認識

認証を始めると図 2 のようにインジケーターが回転する．インジケーターが特定の数字マスに到達すると端末が振動する．つまりインジケーターがつまみの外周を一周するとどこかの数字マスで一回必ず振動する．その数字マスが暗証番号入力用カーソルとなる．なお，振動が発生する数字マス (入力用カーソル) はシステムがランダムに決定する．

手順 2:数字の入力

手順 1 で入力用カーソルが分かったので，そのカーソル位置に入力したい数字が表示されるように，暗証番号入力用つまみを回転させる．回転には画面下部の”時計回り”ボタンと”反時計回り”ボタンを利用する．つまみを直接触って回転させる操作を許容すると，被験者は暗証番号を指し示してしまう懸念があるため，ボタンによる操作としている．回転操作により入力カーソルの位置に入力したい数字を表示させたら，画面下部にある”決定”ボタンを押下する．これにより入力値が確定する．

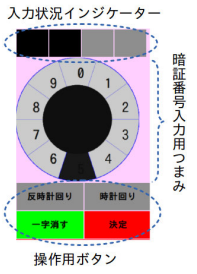

図 1 認証画面の全体像

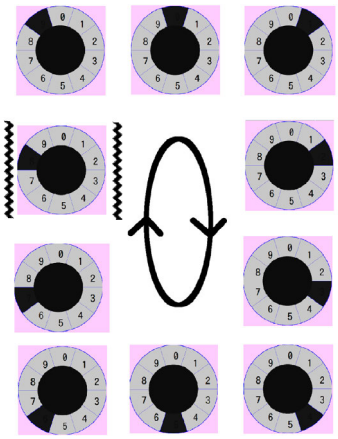

図 2 認証中の画面の推移

入力値と既定の暗証番号値が同一であれば認証成功となる．

4. 評価実験

4.1 比較対象

図 1 のインターフェイスである円盤配列以外にも，テンキー配列を併せて実装した．これは形状の差による優劣を図る目的で作成した．

4.2 利用可能性に関する実験

利用者が提案方式で正しく認証を行うことができるか，またどれほどの時間を必要とするか実験を行った．実験方法について説明する．被験者に実験方式の説明を行い，実際に入力システムで認証をインターフェイス毎に 2 回練習させた．その後に評価実験をさせた．カーソルの移動速度を 300 ミリ秒とし，円盤配列とテンキー配列の 2 条件で，

5 回ずつ合計 10 回認証操作をさせ，操作による入力値と認証時間を実験結果として記録した．暗証番号は被験者の記憶しやすい値で固定し，実験させた．被験者は 10 人 (うち女性 3 人)，年齢は 20 代〜50 代，8 人は普段スマートフォンを利用している被験者，全員が高等教育を受けているか修了している被験者であった．

4.2.1 実験結果

実験結果を表 1 に示す．形状の差が認証時間に影響を与えるかマン・ホイットニーの U 検定をした結果，有意な差がないことが分かった．続いてエラー率に有意差があるか調査したが，有意な差がないことが分かった．

表 1 実験の認証時間 · エラー率

配列	平均値 (秒)	中央値 (秒)	標準偏差 (秒)	認証エラー率 (%)
テンキー	40.53	35.33	16.70	8
円盤	40.99	32.34	18.00	10

4.3 安全性確認実験

認証操作を撮影した動画を作成し，暗証番号の推測実験を実施した．2 つの表示方法 (テンキー配列, 円盤配列) で行った認証操作を録画し，推測をさせた．

実験方法を説明する．3 種類の覗き見をされやすい状況 (部屋の中，電車内，ファーストフード店内) を想定し，それぞれの場所で実際に認証操作をした動画を作成した．次にその動画を 10 人の被験者に視聴させ，その動画情報から暗証番号の抽出を試みさせた．現実で覗き見攻撃に遭う距離を 60cm として考えた文献 [3] と同距離で撮影し，本当に解析が不可能かを実験した．被験者には動画から推測した暗証番号値と，その値の推測に至った根拠を提示させた．

4.3.1 実験結果

正しく推測ができた被験者は 0 人であった．被験者が試みた攻撃方法としては，手の動き始め，手に伝わっている振動，音声処理をする手法が報告されている．しかし，今回の実験に用いた動画においてはどれも有効な攻撃方法にはなりえなかったと推測される．今回の実験では全てのカメラによる攻撃に対して安全であるということは言えないが，少なくとも一定の環境音がある状況では，有用な対策手法になりうる可能性が示唆された．

4.4 考察

2 章で述べた既存の提案手法との比較を表 2 に示す．認証時間，エラー率の括弧内には提案手法を 100%としたときの値を表す．別装置の欄には認証をするのに，端末以外で必要な装置を記した．

fakePointer は提案手法と比較して，認証時間やエラー率のどちらも良い結果になっている．しかし，認証時間の内訳に”秘密情報を共有し，覚える時間”が含まれていないため，同じ実験条件であるとは言えない．Undercover は，提案手法より認証時間，エラー率共に提案方式の結果のほうが優れている．Phone Lock は提案手法と比較して認証時間が 18%短い一方で，エラー率が 15%高い．

表 2 実験結果の比較

	認証時間 (秒)	エラー率 (%)	別装置
fakePointer	17.35(50.5%)	5.6(62.2%)	安全な通信経路
Undercover	45(131.0%)	26.3(292.2%)	トラックボール
Phone Lock	28.2(82.1%)	10.4(115.6%)	不要
提案手法	34.34(100%)	9(100%)	不要

今回の評価実験において、認証エラーの 9 回の原因の内訳は”正しく認識ができなかった”が 6 回，”操作ミス”が 3 回であった．この操作ミスの原因は，本システムの操作性にあると考えられる．数字のシフト操作を完了せずに決定ボタンを押下し，その結果認証に失敗しており，また被験者もその失敗を認識し，そのように申告していた．よって，操作性を改善することによって認証エラー率の改善は実現できると考える．これは今後の課題である．

5. まとめ

本論文では，携帯端末上での個人認証における覗き見攻撃への対策手法として，携帯端末の振動機能を利用した CCC を提案し，被験者における評価実験を実施した．今後は実験で得た知見を元に，操作性の改善による認証時間の改善と，エラー率の低下を考えていきたい．

参考文献

[1] Sasamoto, H., Christin, N. and Hayashi, E.: Undercover: authentication usable in front of prying eyes, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pp. 183–192 (2008).

[2] 高田哲司：fakePointer: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, (2008).

[3] Bianchi, A., Oakley, I., Kostakos, V. and Kwon, D. S.: The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices, *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*, TEI '11, pp. 197–200, (2011).