Computer Security Symposium 2020
26 - 29 October 2020

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

江原 知志[1,a)]　高田 哲司[1,b)]

概要：覗き見攻撃は携帯端末での個人認証において現実的に起こりうる脅威の一つである．この脅威に対する対策手法として，携帯端末の振動機能を利用した個人認証手法が提案されている．しかしそれらの手法には認証に時間がかかるという実用面の課題がある．そこで本研究では，振動機能を利用した既存手法の 1 つに対しユーザインタフェースの改良を試みることによって，覗き見攻撃に対する安全性を維持しながら既存の手法より操作時間を短縮することを試みた．1 つは入力操作に必要な情報の取得時間を短縮させるものであり，もう 1 つはボタン操作よりも直感的な入力操作を可能にする方法の導入である．この提案に基づく認証システムを Android アプリケーションとして実装し，実験参加者による 2 つの評価実験を行った．操作性評価実験の結果，改良前の手法と比較して操作時間が短縮されることが確認できた．また安全性評価実験では，改良前とした認証手法に安全性の問題があることを発見し，提案手法ではこの問題に対しても安全であることを示した．

キーワード：覗き見攻撃，録画攻撃，個人認証，認証時間，ユーザインタフェース，振動，入力方法

Better Usability of Camera-recording based Shoulder Surfing Resilient User Authentication by Redesigning User Interface

Satoshi Ehara[1,a)]　Tetsuji Takada[1,b)]

Abstract: Shoulder surfing attack is one of practical threats in a user authentication. As a countermeasure against this threat, some authentication schemes using vibration are proposed. However, these schemes have a usability issue about a longer operation time. Therefore, we attempted to improve the user interface (UI) to reduce the operation time while maintaining security against the target threat. We updated the UI for (1) reducing the transfer time of the input position, and (2) enabling an intuitive input operation (than using a button). We implemented a prototype system as Android application and conducted experiments with subjects. As a result, we succeeded to reduce the operation time compared to the original scheme. Moreover, we found a security issue against the target threat in the original scheme, and our improvement is effective in addressing the issue.

Keywords: Shoulder surfing, Recording attack, User authentication, Authentication time, User interface, Vibration, Input operation

1. はじめに

個人認証における脅威の 1 つに「覗き見攻撃」がある．覗き見攻撃とは，攻撃者が正規ユーザの認証行為を覗き見ることで入力された秘密情報を不正に取得する攻撃である．この攻撃は，実行に際して技術的なスキルを必要としないため誰でも攻撃者になりうる．また様々なシーンで計算機や携帯端末を利用するようになり，個人認証を行う機会も増えている．このような状況から，本脅威は身近に存在する脅威であり，そのリスクは無視できないものだと考

[1] 電気通信大学
The University of Electro-Communications
[a)] e.azlab@gmail.com
[b)] zetaka@computer.org

える．

このような現状を背景に，覗き見攻撃の対策手法について様々な研究が報告されている．これらの提案は，大きく分けて 2 つの脅威モデルのどちらかに基づいた提案となっている．

- 認証行為をビデオカメラで録画することを想定
- 人間が認証行為を覗き見することを想定

以降本論文では前者を「録画攻撃」，後者を「人による覗き見攻撃」と呼ぶ．これらの脅威モデルの違いは，認証行為の捕捉・記録能力にある．「人による覗き見攻撃」は，人間が認証行為を見てその状況を記憶するため，認証行為から捕捉できる情報が一部に限られる可能性がある．また時間経過とともに忘却によって捕捉した情報が欠損する可能性もある．これに対して「録画攻撃」は，視覚的に捕捉可能な情報はすべて記録でき，忘却による情報欠損も発生しないと仮定する．さらに記録した情報を繰り返し再生することが可能であり，録画データに情報処理を適用して秘密情報を特定することも可能である．Shukla ら [20] や Guixin ら [5] は，指先と携帯端末の位置を追跡することで，携帯端末の画面内容が映っていない録画映像からの入力値の推測が可能であることを示した．したがって，「人による覗き見攻撃」よりも「録画攻撃」の方が攻撃者に有利な状況を示した脅威モデルとなっている．

そこで本研究では，録画攻撃に対して安全性を提供しうる個人認証手法に着目し現状調査を行なった．録画攻撃に着目した理由は，録画攻撃に対する安全性が提供されれば，人による覗き見攻撃への対策にもなると言えるからである．調査の結果，我々は既存の提案手法は認証操作にかかる時間（認証時間）が長くなる傾向にあることに着目した．対象脅威に対する安全性を改善するため，認証時間が長くなることはやむを得ないのかもしれない．しかし，認証時間の長さが個人認証そのものを利用しない理由になりうるという事実がある．Harbach ら [6] の調査で，携帯電話で画面ロックを使用しないユーザ 32 名を対象にその理由を調査したところ，約 6 割のユーザが「認証に時間がかかるためである」と回答した．したがって，認証時間の長さは個人認証におけるユーザビリティの評価軸として無視できないと言える．

そこで本研究では，録画攻撃を脅威モデルとした個人認証には認証時間が長くユーザビリティ上の問題が残されていることを明らかにし，その改善策として当研究グループが過去に提案した個人認証手法 “Circle Chameleon Cursor”(CCC)[9] のユーザインタフェースを改良することで録画攻撃への安全性を確保しつつ，認証時間の短縮を試みた．その結果，有望な結果を得ることができたのでここに報告する．

以降，本論文では 2 章で録画攻撃に耐性のある既存の個人認証手法の調査結果を提示する．3 章で CCC の説明と CCC を改良した本研究での提案手法の説明を行う．4 章で CCC と提案手法を比較するために行った評価実験の結果を示し，5 章で実験結果に対する考察，今後の課題を述べる．6 章で結論を述べる．

表 1 録画攻撃対策の関連研究の比較

認証手法	秘密情報種別	カテゴリ	AD	AT(s)
SSSL[18]	PIN(5 桁)	音声	必要	8*2
SpinLock(音声)[2]	PIN(4 桁)	音声	必要	10.81*2
近藤ら [10]	PIN(4 桁)	音声	必要	11.73*2
PhoneLock(音声)[1]	PIN(4 桁)	音声	必要	12.2*1
SpinLock(振動)[2]	PIN(4 桁)	振動	-	13.86*2
TicTocPIN[12]	PIN(4 桁)	振動	-	15.31*2
M-VDLS[3]	PIN(4 桁)	振動	-	18.88*2
PVRotate[8]	PIN(4 桁)	振動	-	21.2*2
VibraInput[11]	PIN(4 桁)	振動	-	23.8*2
PhoneLock(振動)[1]	PIN(4 桁)	振動	-	28.2*1
CCC[9]	PIN(4 桁)	振動	-	36.41*2
GlassUnlock[21]	PIN(4 桁)	その他	必要	4.8*2
3DPIN[13]	PIN(4 桁)	その他	必要	12.9*2
Undercover[17]	画像 (5 枚)	その他	必要	32*1

2. 関連研究

本章では録画攻撃に対して安全性を提供しうる個人認証の先行研究について調査し，それらの手法における認証時間が長い傾向にあることを明らかにする．またその改善が実用性の向上になることについて議論する．

調査した録画攻撃対策の個人認証手法を**表 1** に示す．表内の “AD(Additional Device)” 列は認証を行う装置以外に追加の装置が必要であるかを示しており，“AT(Authentication Time)” 列は各認証手法における認証時間を示している．認証時間値の注釈*1, *2 は，*1 が中央値，*2 が平均値であることを示している．

表内のいずれの手法も，録画攻撃に対する安全性を確保するため，秘密情報を直接指し示す形で入力させず，攻撃者が視覚的に捕捉可能な情報から入力値を特定することが困難な入力方法にしている．このため録画攻撃対策の認証手法では，視覚的に捕捉困難な方法で入力に必要な情報をシステムからユーザに伝達し，それを用いて間接的に秘密情報を入力させる．我々は，この情報伝達方法について「振動，音声，その他」の 3 カテゴリに分類した．「振動，音声」は文字通り振動や音声を用いてシステムからユーザに情報を伝達する手法であり，「その他」はそれら以外の方法で情報伝達する手法である．

3 つのカテゴリを比較すると，同じ秘密情報種別でも認証時間に差があることがわかる．「音声」と「その他」のカテゴリの認証手法は，PIN(4 桁) の秘密情報において 4.8 秒から 12.9 秒の認証時間となっている．一方，「振動」カテゴリに該当する認証手法の認証時間は，最も短い SpinLock においても 13 秒以上の時間を要し，それ以外の手法ではさ

らに多くの時間を要する．このため「振動」カテゴリの認証手法は認証時間が長いという問題点があると言える．一方で「振動」カテゴリの認証手法は，他カテゴリの手法との比較で利用シーンに関する制約が少ないと言える．「音声」や「その他」のカテゴリの認証手法では認証時にイヤホンやトラックボール等の追加の装置が必要となるが，「振動」カテゴリの認証手法では，携帯端末に実装されている振動機能を利用できるため，追加装置を必要としないからである．

従って，「音声」や「その他」のカテゴリの認証手法では，利用シーンが制限されるという問題点を，「振動」カテゴリの認証手法では認証時間が長いという問題点を改善することで，実用性を向上させることができると考える．しかし，利用シーンの制限は追加装置を必要とする限り発生し，これを改善することは別の情報伝達方法を使用することに等しいと考えられる．一方，認証時間の短縮は，同じ「振動」カテゴリの認証手法でも伝達の仕方や入力方法を工夫することで実現できる可能性があると考えた．よって本研究ではこのアプローチに基づく改善を試みた．

3. CCC の改善提案

前章までの議論から，本研究では「振動」を利用した認証手法の操作時間短縮を試みる．振動を利用した録画攻撃対策の認証手法では，以下の 2 つの手順で 1 つの値を入力する．

(1) ユーザは振動を利用してシステムから情報を受け取る
(2) ユーザは受け取った情報を用いて秘密情報を入力する

そこで上記のそれぞれの操作にかかる時間短縮を検討する．以降，本章では本研究の提案手法の改良元となる CCC[9] についての説明をし，CCC の問題点と本研究での改善策を述べる．

3.1 CCC について

CCC[9] はいわゆる「ダイヤル式金庫」のダイヤル入力を模して考案された手法である．録画攻撃対策として，2 点が既存のダイヤル入力とは異なる．1 つ目は，既存のダイヤル入力では数値の「入力位置」は固定位置で視認可能だが，CCC ではこれを数値入力のたびに変更し，振動を利用してユーザに伝達することで視認困難にした点である．2 つ目は，ダイヤルを回して入力したい数字を入力位置へ移動させる際，ダイヤルを直接触らずにボタンで移動する点である．これによりユーザが操作時に入力値を指し示してしまう懸念を排除した．これら 2 点によって，CCC では振動タイミングが分からない限り認証行為をカメラで録画しても入力値は特定困難であり，録画攻撃に対する安全性が確保されている．

具体的には以下の 2 つの手順で認証を行う．

(1) 入力位置の認識．認証を開始すると**図 1** において，カーソルが 0 の位置から 1，2，...，9 へと順に移動する．カーソルが特定の数字の位置を示した際に携帯端末が振動する．この数字の位置を入力位置と呼ぶ．入力位置は数字を 1 桁入力するごとにランダムに変化する．

(2) 数字の入力．入力したい数字を入力位置へと移動させる．数字の移動には図 1 の「反時計回り・時計回り」ボタンを用いる．数字を入力位置へ移動させた後，「決定」ボタンを押下し入力を確定させる．

この 2 手順によって数字 1 桁を入力できるため，4 回繰り返して 4 桁の数字を入力する．

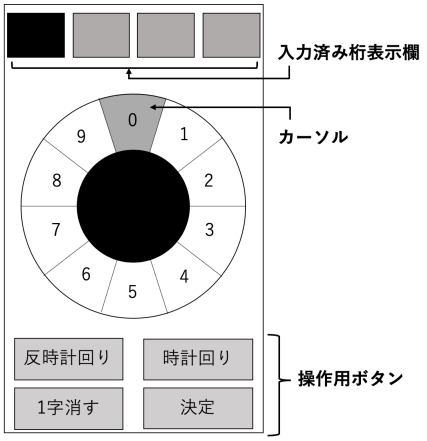

図 1 CCC のインタフェース

3.2 CCC の問題点と改善提案

CCC[9] において認証時間を長くする要因として以下の 2 点に注目し，改善を試みる．

- 入力位置の通知．CCC では，カーソルがとある位置から次の位置へ移動するまでの時間間隔が 300ms であった．カーソルが 0 から 9 へ計 10 回移動する間，ユーザは操作せずに待つ必要があるため，CCC の認証時間は最短でも 12 秒 (0.3 秒 × 10 回移動 × 4 桁) 以上かかる．そこで入力位置の示し方を変更することでカーソルの移動回数を減らし，入力位置の通知にかかる時間を短縮する．
- 数字の入力．CCC の認証手順の 2 つ目において，数字を入力位置へ移動させる方法は「時計回り・反時計回り」ボタンであった．しかし，よりスムーズに数字を入力する方法を新たに用いることで認証時間を短縮できる可能性がある．

提案手法のインタフェースを**図 2** に示す．入力位置の認識，数字の入力に用いられる画面中央のインタフェースを変更し，数字の移動に使用するボタンは「タッチバー」というものに変更した．

提案手法の認証手順は以下の 2 つの手順からなる．

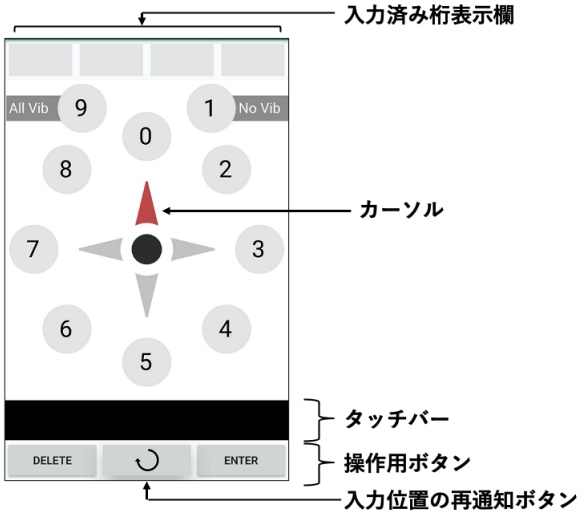

図 2　提案手法のインタフェース

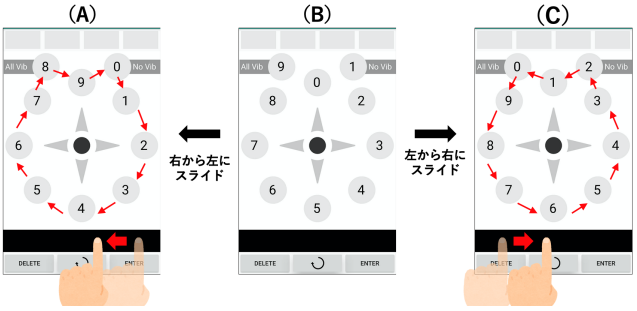

図 3　タッチバーの操作と数字の移動の仕方の対応
B → A（B → C）：タッチバー上で右から左へ (左から右へ) 指をスライドした場合の数字の移動の仕方

(1) 入力位置の認識．認証を開始すると図 2 において，カーソルが，「上→右→下→左」を順に方向を指し示す．カーソルが特定の方向を示した際に携帯端末が振動する．振動した時にカーソルが示していた方向を「振動方向」と呼ぶ．振動方向に対応する位置が入力位置となる．振動方向とそれに対応する入力位置についての説明は後述する．

(2) 数字の入力．入力したい数字を入力位置へと移動させる．数字の移動には「タッチバー」を用いる．タッチバーは図 2 内の画面下部にある黒塗りの領域である．この領域上で指をスライドさせると，その移動量に応じて数字が移動する．タッチバー上での指の動かし方と数字の移動の仕方の関係を**図 3** に示す．数字を入力位置へ移動させた後，「ENTER」ボタンを押下し入力を確定させる．

CCC では，10 箇所の入力位置の候補が存在した．本研究の提案手法では，4 つの方向を用いて 10 箇所の入力位置を示す．これを実現するために，提案手法では振動方向の組み合わせで入力位置を示すこととした．**図 4** に振動方向の組み合わせと入力位置の対応を示す．図 4（A）は振動方向が一方向の場合である．この場合の入力位置は振動方向が指す位置 (0，3，5，7) となる．図 4（B）は振動方向が二方向の場合である．例として振動方向が「上」と「右」であった場合，入力位置は 2 の位置となる．同様にして 4，6，8 は振動方向が二方向の場合に示される入力位置である．図 4（C）は振動方向が四方向全てであった場合である．この場合には入力位置は 9 の位置となる．また．図 4（D）は振動がない場合である．この場合には入力位置は 1 の位置となる．

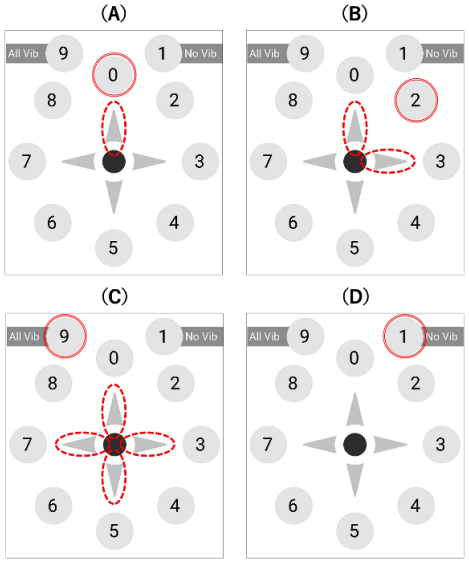

図 4　振動方向と入力位置の対応

4. 評価実験

提案手法による効果を検証するために評価実験を行なった．実験は提案手法を参加者に使用させ，実用性を検証する操作性評価実験と，提案手法の録画攻撃に対する安全性を検証する安全性評価実験の 2 つを実施した．提案手法と CCC を同一の条件で比較するために，CCC と提案手法をそれぞれ Android のネイティブアプリケーションとして実装し，実験に使用した．

4.1 操作性評価実験

本実験は，3 章で述べた改善提案が認証時間や認証成功率にどのような影響を与えたかを検証することを目的として行なった．これらを検証するため，「入力位置の通知」と「数字の入力」が CCC と提案手法で異なることから，以下の 4 条件を設けて実験を実施した．

- C1：CCC・ボタン方式
- C2：CCC・タッチバー方式
- C3：提案手法・ボタン方式
- C4：提案手法・タッチバー方式

11 人の参加者が実験に参加した．全員が 20 代男性で大学生，大学院生または大学を修了した社会人であり，スマー

表 2　各条件の認証時間・認証成功率の結果

条件	AT（s）（平均値）	AT（s）（中央値）	AT（s）（最小値）	SR
C1	22.70	19.70	17.39	85.45%
C2	22.05	21.56	18.11	89.09%
C3	15.94	15.14	12.33	94.55%
C4	16.07	15.51	11.47	96.36%

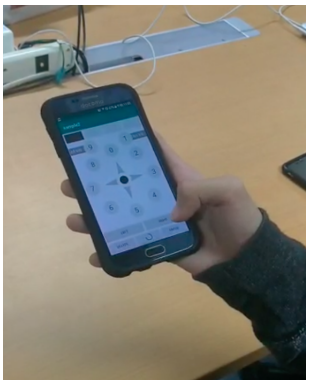

図 5　安全性評価実験に使用した録画映像

トフォンを所持していた．実験に使用した Android 端末は Samsung Galaxy S6，ASUS ZenFone 5，Google Nexus 5X であった．

実験は以下の手順で実施した．

(1) 実験の手順説明
(2) 暗証番号の登録：システムでランダムに生成した 4 桁数字を暗証番号として割り当てた．
(3) 操作説明・操作練習：認証画面の 4 条件それぞれについて操作方法を説明し，認証成功するまで練習させた．
(4) 認証操作：各実験条件ごとに各参加者に認証操作を 5 回ずつ行わせた．4 条件の実施順序は参加者ごとにランダム順とし，学習効果による影響に配慮した．
(5) アンケート：実験の各条件に対するアンケートを実施した．

各条件ごとの認証時間と認証成功率の結果を**表 2** に示す．表内の AT は認証時間，SR は認証成功率を表す．各条件の平均認証時間について，全てのペアの組み合わせでウィルコクソンの符号付き順位和検定を行った．その結果，CCC・ボタン方式と CCC・タッチバー方式，提案手法・ボタン方式と提案手法・タッチバー方式以外の全てのペアで有意差が得られた（$p < 0.01$）．一方，認証成功率についてもウィルコクソンの符号付き順位和検定を行ったところ，全てのペア間で有意差は得られなかった（$p > 0.05$）．

4.2　安全性評価実験

本研究で実装した CCC と提案手法に対し，同一の条件下で録画攻撃を行い，録画攻撃に対する安全性を評価した．操作性評価実験で用いた 4 条件に対してそれぞれ攻撃を行なった．

表 3　各条件の特定成功桁数ごとの推測数

条件	0 桁	1 桁	2 桁	3 桁	4 桁	合計推測数
C1	4	8	6	2	0	20
C2	14	2	0	0	1	17
C3	7	8	5	0	0	20
C4	17	3	0	0	0	20

4 人の参加者が攻撃者役として，1 人の参加者が被害者役として実験に参加した．攻撃者役の参加者全員が著者と同じ研究室に所属する 20 代の学生であり，操作性評価実験にも参加していた．このため，CCC と提案手法のどちらの認証手法についても十分理解していた．被害者役の参加者は操作性評価実験の参加者の中で，上記の 4 人以外でなおかつセキュリティを専門として学んでいない人を選んだ．これは平均的なユーザによる認証行為を想定したためである．

まず実験の事前準備として，被害者役の参加者に前述の 4 条件で 1 回ずつ認証操作を行わせ，その様子を録画した．入力する暗証番号は各条件ごとに乱数を用いて無作為に決定した．録画は ASUS ZenFone5（動画の解像度:1920 × 1080）を使用し，被害者役の参加者の携帯端末から約 60cm の距離で行った．ZenFone5 は一般的なスマートフォンであり，携帯端末から約 60cm の距離ではカメラが被害者の視界に入らないため，現実世界で実行可能な条件であると考えられる．また，この距離は石塚ら [9] の録画攻撃実験において採用された距離である．撮影した映像のスクリーンショットを**図 5** に示す．

次に，攻撃者役の参加者による入力値の推測を行わせた．事前準備で録画した動画を攻撃者役の参加者のみが閲覧できるよう Web 上にアップロードし，参加者には各動画を最低 3 回視聴した上で推測を行うよう指示した．推測した入力値とどのような方法を用いて推測を行ったかを Google フォームを利用して回答させた．推測は 5 回までとし，参加者には 1 回の推測ごとに推測値が正しいか間違っているかのみのフィードバックが与えられた．参加者は何回でも動画を閲覧することができ，一時停止やスロー再生なども自由に行えた．

各条件の動画に対する特定成功桁数をまとめた結果を**表 3** に示す．1 人の参加者による CCC・タッチバー方式（条件 C2）への攻撃において 4 桁全てが特定された．表 3 の条件 C2 において合計推測数が 17 となっているのは，この参加者が 2 回目の推測で 4 桁全てを特定したからである．また CCC・ボタン方式（条件 C1）に対しては 3 桁特定成功した推測が 2 件あった．一方，提案手法 (条件 C3・C4) に対しては 3 桁以上特定成功した推測はなかった．条件 C2 で攻撃が成功した理由は，被害者役の参加者が行ってしまったある動作にある．これについての詳しい議論は第 5 章で述べる．

5. 考察

本章では評価実験の結果から提案手法の操作性と安全性についての考察を行い，「振動」カテゴリに属する他の認証手法との比較を行う．また，今後の課題について述べる．

5.1 提案手法の改善効果について

本研究の目的は，ユーザインタフェースの改善により録画攻撃への安全性を維持しつつ認証時間を短縮し，覗き見対策となりうる CCC の実用性改善を実現することである．まず提案手法による改善の効果について考察する．はじめに録画攻撃への安全性であるが，CCC と提案手法との比較で録画攻撃に対する安全性は同等程度であったと言える．表 3 の結果から，CCC と提案手法の各条件に対して 4 名の実験参加者が録画データから入力値の推測を 5 回ずつ試みたが，特定に至ったのは CCC で 1 件，提案手法では 0 件という結果であった．また 2 桁，3 桁の特定に至った件数も CCC が（6 件, 2 件）であるのに対して，提案手法は（5 件, 0 件）となった．これらの結果から提案手法の録画攻撃に対する安全性は低下してはおらず，CCC と同等程度の安全性を維持できていると言える．次に認証時間であるが，CCC との比較で提案手法の認証時間は短縮されたと言える．CCC（条件 C1）の認証時間平均値が 22.70 秒であるのに対し，提案手法（条件 C4）の認証時間平均値は 16.07 秒となり，CCC と提案手法の間で有意差があるという結果となった．これら 2 つの結果から，第 3 章で述べた 2 つの改善提案による本研究の目的であった「CCC における録画攻撃への安全性を損なわずに認証時間を短縮する」は実現できたと考える．

5.2 操作性・安全性への影響

前節で述べた以外の影響について，操作性と録画攻撃への安全性の 2 点について議論する．まず操作性について 2 点考察する．1 つ目は認証時間以外に対する影響である．提案手法により認証時間は短縮されたが，その一方で操作負担や入力位置の認識負担を増す結果になっている懸念がある．この点について，認証成功率，入力位置の再通知回数，アンケートの結果から議論する．はじめに認証成功率だが，表 2 の結果から有意差はないものの提案手法は CCC よりも良好な認証成功率となっている．次に入力位置の再通知回数である．入力位置の再通知とは，入力位置の認識に失敗した際にその処理のやり直しを要求する処理であり，認証画面内のボタンを押すことで実行される (図 2 参照)．このボタンの押下回数が多い場合，入力位置の認識が何度もやり直さないと認識できないほど難しいものであるということになる．しかし，各参加者の実験全体を通しての平均押下回数は CCC で 2.36 回，提案手法で 0.91 回であり，入力位置の認識も CCC と同等程度であり困難化してはいないと言える．最後にアンケート結果である．アンケートで「CCC と提案手法でどちらの方が入力位置の認識が容易か？（CCC・提案手法・どちらも同じ，のいずれかで回答)」を尋ねたところ，参加者 11 名中 10 名が提案手法，1 名がどちらも同じと回答した．これらの結果から提案手法は CCC と比べて操作性を悪化させた点は見あたらず，操作性を維持したまま認証時間を短縮したといえる．

2 つ目は数字の入力方法である．今回の改善提案で従来のボタン操作のほかにタッチバーによる操作方法を提案した．しかし CCC と提案手法の双方において 2 種類の入力方法の間で認証時間に差は見られなかった．このことから，認証時間の短縮という観点ではタッチバーによる効果は少ないと言える．しかしアンケート結果から「タッチバー方式は数字を早く移動できるように感じるが，指のスライド量の加減が難しい」という意見が得られている．現状ではタッチバーは黒塗り領域となっており指のスライド量と数字の移動量の対応が分かりにくい．指のスライドと数字の移動の対応が分かるようユーザインタフェースの改良を試みることによってこの問題が改善可能か今後検討する．

次に安全性について 2 点考察する．1 つ目はタッチバーによる安全性への影響である．表 3 において，条件 C1,C3 がボタン操作，条件 C2,C4 がタッチバー操作による結果となるが，ボタン操作とタッチバー操作で特定された桁数に差があると解釈できる．条件 C2 で 4 桁特定された事例を除くと，ボタン操作による条件 C1,C3 では 2 桁，3 桁まで特定できている事例があるが，タッチバー操作による条件 2,4 では 1 桁の特定のみにとどまり，2,3 桁の特定に至っている事例がない．今後の検証が必要と言えるが，タッチバー操作は認証時間短縮には影響ないものの，安全性には影響する可能性がある．

2 つ目は，入力位置の通知の改善によるユーザの望ましくない動作の抑制である．CCC も提案手法も「入力位置の認識」ではカーソルが移動を完了するまで次の「数字の入力」を行わずに待つ必要がある．移動完了を待たずに入力動作を始めると，その動作を開始するまでのカーソル移動範囲で入力位置が認識できたということを視覚的に示してしまうことになり，入力位置の特定または絞り込みを可能にしてしまうからである．特に CCC の場合は移動回数が 10 回であり，その移動中に 1 回だけ振動するため，少数の移動で入力位置が認識できた場合，カーソルが最後まで移動するのを待たずに数字入力操作の準備をユーザが始めてしまう懸念があった．第 4.2 節の安全性評価実験で，攻撃者役の参加者 1 名が条件 C2 において入力値特定に至った理由は，被害者役の参加者がこのような動作を行ったからであった．これに対して提案手法はカーソルの移動回数が 4 回であり，また複数回の振動が発生する可能性もあるので，カーソルの移動が完了するまで振動を認識しなけれ

ばならなくなる．したがって，前述のような望ましくない動作をユーザが行いにくい入力位置の認識手法に改良したと言える．ゆえに，今回の入力位置の通知の改善に関する提案は認証時間の短縮だけでなく，録画攻撃への安全性向上という点でも CCC の改良に貢献する提案になっていると言える．

5.3 他の振動カテゴリの手法との比較

第 2 章の表 1 に挙げた CCC 以外の振動カテゴリの手法について，提案手法より認証時間が長い手法と短い手法に分けて比較考察する．

まず，提案手法より認証時間が長い認証手法との比較をする．このような手法として，M-VLDS[3]，PVRotate[8]，VibraInput[11]，PhoneLock[1] がある．これらの認証手法は振動のパターンを利用して，入力に必要な情報をシステムからユーザに伝達している．提案手法においても複数回の振動を利用するため，振動パターンの一種と言える．これらの認証手法と提案手法の異なる部分は，視覚情報を同時に利用するかという点にある．M-VLDS，PVRotate，VibraInput，PhoneLock では振動のみを用いてユーザに情報を伝達するが，提案手法では振動に加えて方向をカーソルで示すという視覚的な情報を同時に使用する．この情報伝達方法の違いが認証時間に影響した可能性がある．この検証については今後の課題とする．

次に，提案手法より認証時間が短い認証手法との比較をする．SpinLock（13.86 秒）[2] と TicTocPIN（15.31 秒）[12] がこれに該当するが，これらの手法には録画攻撃に対する安全性の面で問題点がある．まず SpinLock だが，これは複数回の録画攻撃に対して安全でない．複数回の録画攻撃とは，同一のユーザの認証行為を何度も録画し，それを攻撃に利用する場合である．入力操作にランダム性が含まれていたとしても，入力操作と入力値の間に何らかの相関関係がある認証手法では，1 回の録画攻撃では入力値を特定できないが，複数回の録画攻撃により入力値の絞り込み，特定が可能になる．SpinLock はこれに該当する認証手法であるため，複数の録画攻撃に対して十分に安全でない．一方，提案手法は入力操作と入力値の間に相関関係はなく，このような手法には該当しないため複数回の録画攻撃にも安全であると考えられる．次に TicTocPIN だが，これは 1 回の録画攻撃によって入力値を絞り込むことが可能という問題点がある．TicTocPIN は 4 桁の PIN を秘密情報とするが，入力操作を録画することによって各桁の値を 5 通りに絞り込むことができる．4 桁では $5^4 = 625$ 通りとなる．これは本来の 4 桁 PIN の候補数 10000 通りより大幅に少ない値となっており，攻撃者による秘密情報特定の可能性を高める．一方，提案手法では入力操作によって入力値を絞り込むことは困難であると考えられる．

以上から，我々が知る限り提案手法は録画攻撃に対する理論的に十分な安全性を確保した認証手法の中で最も認証時間が短い認証手法となった．

5.4 今後の課題

提案手法の改善に向けて，以下に 3 点今後の課題を示す．

まず 1 つ目に，より大規模な評価実験の再実施である．操作性評価実験の結果，提案手法では「入力位置の通知」において，認証時間が短縮された．今回の実験では，それに伴って認証成功率が低下した，CCC よりも使いづらくなったという意見が得られたなどといった結果はなかった．しかし，今回の実験の参加者は少人数であり，年齢や性別にも偏りがあった．そのため，より一般的なユーザが提案手法を使用した場合の結果は，今回の実験結果とは異なる可能性がある．従って，より大人数の参加者による評価実験を実施することで，年齢や性別による結果の違いの有無を確認する必要性があると考える．また，安全性評価実験においても，今回は 1 人の被害者役の参加者に対して各条件 1 回の録画攻撃を行うのみにとどまった．しかし，同一のユーザの認証行為を複数回録画した場合や，複数のユーザに対して攻撃を行った場合に新たな脆弱性が発生しないか検証する必要がある．

2 つ目に，タッチバーの改良である．操作性評価実験の結果，タッチバーは認証時間短縮には繋がらなかった．しかし，実験の参加者らの意見から得られたタッチバーの問題点を改善することで，認証時間短縮につなげられる可能性があると考えている．現在のタッチバーのデザインでは指のスライド量に対する数字の移動量がわからないため，指のスライド量の調節が難しくなっている．そこで，指のスライド量と数字の移動量の対応がひと目でわかるようタッチバーに目盛りのような表示を加えることによって，操作時間短縮に繋げることができる可能性があると考えている．

最後に，振動音の漏洩に関する調査とその対策である．安全性評価実験の結果，今回の撮影条件では CCC と提案手法どちらも録画によって振動音は感知されなかった．しかし，振動音は周囲の環境音の大きさや撮影距離，撮影機器，被害者側が使用している携帯端末の種類やケースの有無などによって感知できる可能性がある．また，CCC では振動は数値入力毎に 1 回のみだったが，提案手法では 0,1,2,4 回のいずれかである．この振動の回数によっても振動音を感知可能性が変動する恐れもある．従って，どのような状況であれば振動音が感知可能，不可能かを調査し，感知可能な場合への対策を講じる必要があると考えている．

6. おわりに

本論文では，録画攻撃対策の既存の認証手法を調査し，3 つのカテゴリに分類した．その上で，それらの中で「振動」を利用した認証手法は，それ以外の手法と比較して利

用シーンの制限が少ない一方で認証時間が長いという問題点があることに注目し，「振動」を利用した認証手法の 1 つである CCC のユーザインタフェースについて，「入力位置の認識」「数字の入力」の 2 点を改善することで認証時間の短縮を試みた．

提案手法を Android のネイティブアプリケーションとして実装し，操作性と録画攻撃に対する安全性を CCC と直接比較する評価実験を行った．その結果，平均認証時間は 16.07 秒となり，同様に実装した CCC の平均認証時間 22.70 秒より 6 秒程度短縮された．また録画攻撃に対する安全性については，CCC に対してユーザの動作による入力値の特定が可能であることが確認されたが，提案手法に対してはこの方法が困難であることを示した．また，他の振動を利用した認証手法と比較して録画攻撃に対して安全かつ高速な認証手法となっていることを示した．

参考文献

[1] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2010. The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction (TEI ’ 11). Association for Computing Machinery, New York, NY, USA, 197–200.

[2] Andrea Bianchi, Ian Oakley, Dong-Soo Kwon. (2011). Spinlock: A Single-Cue Haptic and Audio PIN Input Technique for Authentication. 81-90.

[3] N. Chakraborty, S. V. Anand, G. S. Randhawa and S. Mondal, ”On Designing Leakage-Resilient Vibration Based Authentication Techniques,” 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 1875-1881.

[4] Jan Gugenheimer, Alexander De Luca, Hayato Hess, Stefan Karg, Dennis Wolf, and Enrico Rukzio. 2015. ColorSnakes: Using Colored Decoys to Secure Authentication in Sensitive Contexts. In Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI ’15). ACM, New York, NY, USA, 274–283.

[5] Ye Guixin, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor and Zheng Wang. “Cracking Android Pattern Lock in Five Attempts.” NDSS (2017).

[6] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI ’16). ACM, New York, NY, USA, 4806-4817.

[7] 東山侑真, 岡村真吾, 矢内直人, 藤原融. 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, Computer Security Symposium 2014, October 2014, pp.1023-1028

[8] Yutaka Hirakawa, Fumiya Hirose, and Isao Sasano, ”PVRotate: An Improved Vibration-Based User Authentication Method,” International Journal of Future Computer and Communication vol. 8, no. 2, pp. 50-54, 2019.

[9] 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).

[10] 近藤 潤，平野 学，神谷直希，”音声入力と相対値入力による覗き見に強い認証方式の提案”, FIT2011（第 10 回情報科学技術フォーラム）論文誌, vol.4, pp.33-38, 2011.

[11] Kuribara, Takuro & Shizuki, Buntarou & Tanaka, Jiro. (2014). Vibrainput: two-step PIN entry system based on vibration and visual information.

[12] T. Kwon and J. Hong, ”Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks,” in IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 278-292, Feb. 2015, doi: 10.1109/TIFS.2014.2374352.

[13] Lee, Mun-Kyu, Jin Bok Kim, and Matthew K. Franklin. ”Enhancing the Security of Personal Identification Numbers with ThreeDimensional Displays.” Mobile Information Systems 2016 (2016).

[14] Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces (OZCHI ’ 07). Association for Computing Machinery, New York, NY, USA, 199–202.

[15] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now you see me, now you don’t: protecting smartphone authentication from shoulder surfers. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’ 14). Association for Computing Machinery, New York, NY, USA, 2937–2946.

[16] M. Lee, ”Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry,” in IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695-708, April 2014, doi: 10.1109/TIFS.2014.2307671.

[17] 増田裕仁, 喜多義弘, 朴美娘, 岡崎直宣. タッチスクリーンを利用した覗き見耐性を持つパズル型認証方式の提案, マルチメディア, 分散協調とモバイルシンポジウム 2014 論文集,2014,1005-1010 (2014-07-02)

[18] T. Perkovic, M. Cagalj and N. Rakic, ”SSSL: Shoulder Surfing Safe Login,” SoftCOM 2009 - 17th International Conference on Software, Telecommunications & Computer Networks, Hvar, 2009, pp. 270-275.

[19] Kai. R. Volker. R. and Rene. A pin-entry method resilient against shoulder surfing. In Proceedings of the 11th ACM conference on Computer and communications security, CCS 2004, pages 236-245. ACM, (2004).

[20] Diksha Shukla, Rajesh Kumar, Abdul Serwadda, and Vir V. Phoha. 2014. Beware, Your Hands Reveal Your Secrets!. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS ’14). ACM, New York, NY, USA, 904-917.

[21] Christian Winkler, Jan Gugenheimer, Alexander De Luca, Gabriel Haas, Philipp Speidel, David Dobbelstein, Enrico Rukzio. 2015. Glass Unlock: Enhancing Security of Smartphone Unlocking through Leveraging a Private Near-eye Display.

[22] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI ’15). ACM, New York, NY, USA, 1403-1406.