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† 高田 哲司†

†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
ishizuka@uec.ac.jp,zetaka@computer.org

あらまし 本研究では携帯端末の振動機能を活用した，覗き見攻撃に対して安全な認証方式を提案する．振動で秘密情報を共有することで覗き見に対して安全性を担保し，記憶負荷の低い，4 桁の暗証番号だけで利用でき，新たに装置を必要としない認証方式である．また理論上ではビデオカメラによる覗き見攻撃にも安全性を確保しうる携帯端末向け個人認証手法であり，Android スマートフォンでの実装，実験をした．実験の結果，最短の被験者は 21 秒で認証に成功し，認証時間が最も優れていた速度で 9%程度の認証エラー率であること，そして認証操作の動画から正しい暗証番号の推測ができた被験者がいないことが分かった．

Shoulder Surfing Resistant Authentication System by Using Vibration

Masaya Ishizuka† Tetsuji Takada†

†Graduate School of Informatics and Engineering, The University of Electro-Communications
1-5-1 Chofugaoka, Chofu-si, Tokyo, 182-8585, JAPAN
ishizuka@uec.ac.jp,zetaka@computer.org

Abstract Our study is shoulder surfing resistant authentication system with smart-phone's vibration. Our authentication system shares secret information between user with vibration, which has some features, possible to defend against shoulder surfing attack with camera, low memory load, possible to authenticate the user only with 4-digit PINs, without any extra devices. This paper describes that the design of the authentication system with smart-phone's vibration, which theoretically enable to resistant multiple times shoulder surfing with camera. We did a feasibility experiment and safety experiment with Android smart-phone. We find that the fastest user was able to authenticate within 21 seconds, authentication failure rate was 9% in fastest authentication speed. Furthermore, all subjects were unable to guess true password from video movies.

1 はじめに

携帯端末の普及とそれに伴った携帯端末で利用できるメールや SNS，社内ネットワークへのアクセスといったサービスも増え，多くの人が個人情報の入った端末を持ち歩くようになった．

しかし携帯端末が普及したことで誰でも気軽に動画を撮影できるようになったこと，監視カ

メラがいたるところに配置されていること，ウェアラブル機器の登場でカメラを撮っているとは気づかれないようになったこと，カメラ自体が非常に小さくなったことで，撮影されていることに気づかない可能性がある．パスワードの入力中に撮影をされている可能性もある．多くのモバイルデバイスは 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，これらのデバイスで提供されている既存の認証方式の多くは，覗き見攻撃に対して考慮されていないため，一度覗き見攻撃をされてしまうとパスワードが容易に特定されてしまう．

個人認証における覗き見の問題に対して，様々な研究が行われている [1–7]．しかしながら，以下に挙げるような課題が残されている．

- 記憶負担の増大
- 入力方法の複雑化
- カメラによる録画記録からの抽出

これまでの議論から，本研究ではスマートフォンにおける個人認証への覗き見対策に焦点をおく．さらにその脅威と利用環境に配慮し，既存の携帯端末での利用可能性と複数回の覗き見攻撃にも配慮することとする．

2 関連研究

2.1 人間による覗き見攻撃への対策手法

目の動きで数字を描く EyePIN [4] は目の動きを数字に変換する装置が必要になることや，目の動きを録画してしまえば攻撃ができてしまう．ATM などの認証端末を携帯端末と連動させ，携帯端末が振動したら嘘の情報を入力する Vibrapass [2] は，別途利用者が携帯端末を認証端末とペアリングさせる必要があること，認証端末と安全な通信ができる環境が必要である．タッチ操作を前面のディスプレイだけではなく両面でできる端末を利用し，端末の背面に図形を描くことで背後から覗き見をしづらい方式である Back-of-Device Shapes(BoDS) [3] は，利用者の前面からのカメラを用いた攻撃に対しては安全性ではない．喜多らの 6x6 のマスの中からパスワードとなる英数字を探し，振動機能で入力する文字を変化させる方式 [7] は，カメラによる複数回の攻撃には安全ではない．

2.2 カメラ録画による攻撃への対策手法

手で覆ったトラックボールの上下左右の回転と振動を利用して秘密情報を共有する Undercover [5] は認証のためのトラックボールが必要となる．認証画面に数字とは別の 10 個の記号を表示させ，あらかじめ安全な経路で送られた秘密情報を利用し，記号と数字を重ねて入力することでカメラによる攻撃に対して安全性を担保した fakePointer [6] は秘密情報を共有するために認証端末とは別に安全な通信経路が必要になる．触ったマスの数字を振動や音で利用者に知らせることで覗き見攻撃に対して安全性を保証した Phone Lock [1] の振動モードは覗き見対策には優れ，認証のために端末以外の装置を必要としないが，振動に対応した数値を記憶する必要があるため，記憶負荷が増える．

2.3 既存方式の比較

既存研究の比較をしたものを表 1 にまとめた．表の認証情報の欄には認証に必要な記憶すべき秘密情報で，4 桁 PIN 程度の安全性を保証するのに必要な秘密情報量と種類である．別装置の欄には現在スマートフォンを所持している利用者が，認証のためにスマートフォン以外の装置が必要か不要かを記している．カメラ欄にはカメラを用いた覗き見攻撃に対して，秘密情報が完全に守ることができるなら○を，一度の撮影で秘密情報の部分情報が特定されてしまい，複数回の撮影で秘密情報を特定されてしまうなら△を，一度の撮影で完全に特定されてしまうなら×をそれぞれ記載した．

表 1: 認証システムの比較表

方式	認証情報	別装置	カメラ
EyePIN	4PIN	必要	×
VibraPass	6PIN	不要	△
Undercover	6 画像	必要	○
fakePointer	4PIN	必要	○
BoDS	2 記号	必要	×
喜多ら	3 文字	不要	△
Phone Lock	4PIN+α[1]	不要	○

3 提案システム

本研究で提案する手法は 2 つの特徴からなる．1 つは暗証番号の入力を間接的に行うことである．これは入力値を視覚的に特定することを困難にし，覗き見攻撃に対する安全性を確保する．もう 1 つは，暗証番号入力のために必要なもう一つの秘密を振動を用いて端末と利用者間で共有する．そのため，ビデオで認証行為を撮影しても，その録画記録から入力値を抽出することが困難な仕組みとなっている．

3.1 認証方法

提案システムの画面表示例を図 1 に示す．図からわかる通り，認証画面は，入力中の桁表示欄，表示インターフェイス，”反時計回り”，”時計回り”，”決定”，”一字消す”の 4 つのボタンで構成されている．本手法で暗証番号を入力するためには，2 つの手順をふむ必要がある．それを以下に説明する．

手順 1:入力位置 (マス) の認識
認証を始めると図 2 のようにカーソルが回転する．回転をする中で，カーソルが特定のマスに重なっている時だけ端末が振動する．この振動するマスが入力位置となる． 図 2 の例では 8 が表示されているマスが入力位置となる．このマスは数字の入力や削除のたびにランダムで変化するため，入力毎に入力するマスを探す必要がある．

手順 2:暗証番号の入力
手順 1 で探した入力位置に表示されている数字を，入力したい数字になるように”反時計回り”や”時計回り”ボタンで表示されている数字を動かす．数字の動き方は図 3 のように動く．振動するマスと入力したい数字を重ねたら決定ボタンを押す．図 4 に”1”の入力手順を載せた．

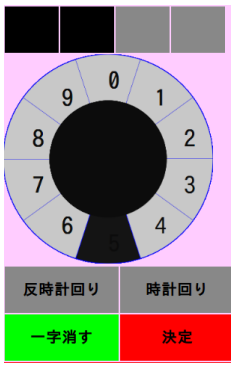

図 1: 認証画面の全体像

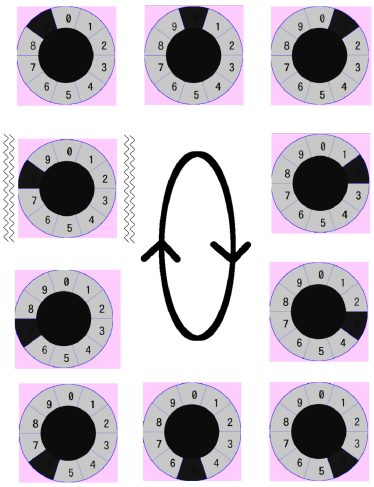

図 2: 認証中の画面の推移

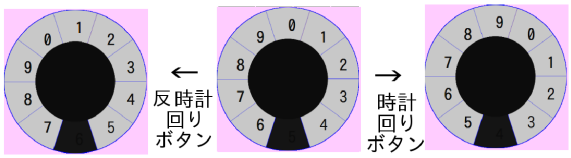

図 3: 表示されている数字の移動方法

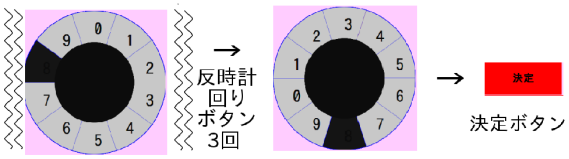

図 4: ”1”の入力方法

この手順を入力桁回繰り返す．入力された値と既定の暗証番号値が同一であれば認証成功となる．また結果画面では，認証結果と認証時間が表示される．

カメラ録画に対して安全な理由は，端末と利用者で入力位置を振動によって共有しているからである．複数回の覗き見に対して安全な理由

[1]振動に対応した数字

は，入力位置が毎回ランダムに変動するからである．

3.2　比較対象の表示方式

3.1 節で紹介した円形表示のユーザインタフェースを CircPad と呼ぶ．これに対し，比較対象として図 5 に示すようなテンキー配列のユーザインタフェースも実装した．これは NumPad と呼ぶ．形状以外の差は，ボタンの位置や表示されるラベル，塗りつぶしの色と動作である．

図 5: NumPad

4　実験

本システムを利用者が利用できるか確認する評価実験と，実際の認証手順を踏んだ動画から暗証番号の特定が可能かを検証する攻撃実験を行った．

4.1　利用可能性に関する実験

利用者がこの認証方式を使うことができるかを確認すること，表示形状と速度はどの組み合わせが最適かを確認するために評価実験を行った．提案方式の要は”利用者が端末の振動したマスの位置を正しく認識し，暗証番号を入力可能か”であるため以下の実験方式を執った．

4.1.1　実験方法

まず被験者に対して認証方式の説明を行い，その後に正しく理解できたかの確認と使い方を覚えてもらうために CircPad と NumPad で 2 回ずつの計 4 回認証システムを実際に操作させてから評価実験を実施した．評価実験終了後には NASA-TLX テストと事後アンケートを行った．

- 暗証番号を被験者の覚えやすい値で固定
- CircPad，NumPad の 2 種類
- カーソルの移動速度を低速 (450ms), 普通 (300ms), 高速 (150ms) の 3 種類

評価実験は上記にあるように，2 種類の表示方法，3 種類のカーソル移動速度の計 6 条件で，5 回ずつ合計 30 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．6 種類の順番は被験者毎にランダムな順番でさせることで，操作の慣れによる差が現れにくいようにした．

実験に利用したハードウェアは京セラ製のスマートフォン，KYY04(端末サイズ: 125 × 64 × 10.8 mm， 重量: 140g，画面サイズ: 4.0 インチ) を利用し，端末の持ち方に制約を付けることはしなかった．実験に使用したソフトウェアは，Cordova を用いて Android 用アプリケーションとして実装したものを用いた．

被験者は 10 人（うち女性 3 人），年齢は 20 代〜50 代 (20 代 7 人，30 代 1 人，50 代 2 人), 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 (大学教育や短大や専門大学など) を受けているか修了している被験者であった．

4.1.2　結果

NASA-TLX の結果を図 6 に，認証時間とエラー率を図 7，8 と表 2 に記載した．(Num,Circ) は Numpad と CircPad を，ハイフンの後の (S,N,F) をそれぞれカーソル移動速度の低速，普通，高速を表している．

速度が普通，低速におけるほとんどの認証失敗は，一桁だけ間違えてしまうという理由であった．速度が高速では振動しているマスとその次のマスのどちらが正しいマスなのかの判断ができず，全桁ずれて入力してしまうエラーが目立った．実際に”次のマスとどちらかが判断が難しい”という回答がいくつかあった．

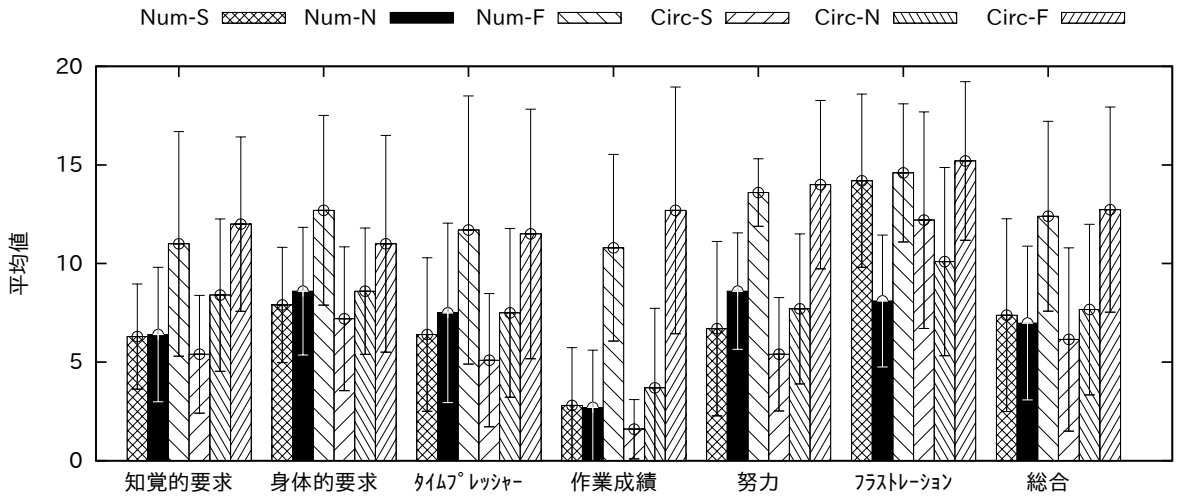

図 6: NASA-TLX の結果

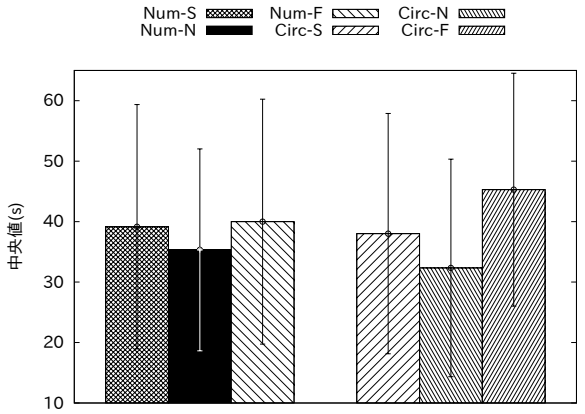

図 7: 実験の認証時間

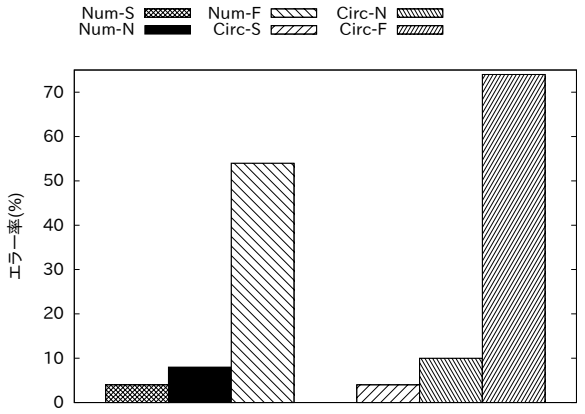

図 8: 認証エラー率

表 2: 実験の認証時間 (秒)

	Num-S	Num-N	Num-F	Circ-S	Circ-N	Circ-F
平均値	47.50	40.53	44.67	44.83	40.99	49.39
中央値	39.15	35.33	40.00	38.01	32.34	45.28
標準偏差	20.20	16.70	20.25	19.87	18.00	19.26

また普段スマートフォンを利用していない被験者の中にはタッチ操作がうまくできず認証に時間のかかる被験者もいた．最速の入力時間は 21 秒で入力することができ，25 秒以内に入力が完了できた被験者は 6 人 (Num-S:1 回，Num-N:4 回，Circ-N:4 回，Circ-F:2 回，被験者の重複あり) であった．

速度や形状が与える認証への影響を調べるためいくつかの検定をした．

まずカーソル移動速度について述べる．速度が普通と低速では高速に比べ低いエラー率で認証ができるので，どちらの速度がより良い認証方式であるかを比較した．認証時間において普通と低速をマン・ホイットニーの U 検定をした結果，有意な差があることが分かった (U=3695.00, z=3.19, p<.01)．続いてエラー率に関して有意差があるか調査した．エラー率において普通と低速で U 検定をした結果，有意な差がないことが分かった (U=126.50, z=0.94, p=0.35)．

被験者へのアンケートの結果”速度が低速と高速はフラストレーションが高い”という回答を得られたため，NASA-TLX の結果のフラスト

レーションの項において普通と低速でU検定をした結果，有意な差があることが分かった (U=98.50, z=2.76, p<.01)．このため統計的にも速度の低速は普通と比べてフラストレーションが高いという事が分かった．

上記から速度の普通は，認証速度は低速に比べ統計的に有意な差があり，エラー率が最も低い低速に比べ統計的に有意な差がない速度である．更にフラストレーションのより低い速度であることが分かった．

続いて形状は CircPad と NumPad でどちらが優れているか比較をした．前項より速度普通が最も良いことが分かったため，普通において認証速度，エラー率，NASA-TLX の結果で有意な差があるかを U 検定で比較した．形状と認証速度 (U=1172.00, z=0.54, p=0.59) や形状とエラー率 (U=45.50, z=0.40, p=0.69) で有意な差は見つからなかった．

さらに形状の違いを NASA-TLX のそれぞれの項目の結果と全項目の平均で比較したが，有意な差がないことが分かった．

4.1.3　アンケート結果

”電卓型の動きのほうが，速度が高速でも区別しやすい”という意見がある一方”円型のほうがこの辺りで動いていたからそのマス近辺まで先に動かすという操作ができるため素早く打てる”という回答が見られた．

またアンケートでは”覗き見攻撃の脅威”(強く感じる〜全く気にならない)，”実験の良さ”(良い〜悪い)，”正しいマスを認識できたか”(できた〜できなかった)，”今後使いたいか”(使いたい〜使いたくない) を 5 段階で答えてもらった．実験の結果とアンケートの結果に相関があるかスピアマンの順位相関係数で調べた結果，”今後も使いたい”と”実験においての入力時間”には相関がある (r=0.46) ことが分かった．

4.2　安全性確認実験

カメラを利用した覗き見攻撃に対して安全であることを検証するために，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．

4.2.1　実験手順

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．胸元で撮影を行った場合 (スマートフォンとの距離を 10cm 程度) 振動音を動画から聞くことができ，攻撃が容易であることは事前に分かっていた．よって実際に覗き見攻撃にあう距離を 60cm として考えた文献 [1] と同距離で撮影し，本当に解析が不可能かを実験した．その後に暗証番号の推測と，推測に至った根拠を提示させる．利用可能性に関する実験の結果から速度普通とし，2 つの表示方法 (NumPad,CircPad) で録画し，推測をさせた．動画撮影には OLYMPUS の TG-320 と内臓のマイクを利用した．

被験者は 10 人，20 代，30 代で 8 人は普段スマートフォンを利用している被験者で，全員が高等教育を受けているか修了している被験者で実験させた．予備実験を受けていない被験者には別途認証方式の使い方を説明した．推測手法は各個人に任せ，動画を任意に解析，推測させた．回答には推測した暗証番号と，推測した理由，自信の有無を記入させた．

4.2.2　結果

10 人中正しく推測ができた被験者はいなかった．自信があると回答した中に，2 桁以上正解している回答はなかった．攻撃手法については手の動き始めや，手に伝わっている振動を用いて推測をするという回答が多かった．さらに，音声処理をする被験者もいたが，今回実験に用いた映像記録からは振動音を抽出することはできなかった．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かったが，少なくとも一定の環境音がある環境では，有用な認証手法になりうる可能性が示唆された．

5 考察

5.1 評価実験結果

Android スマートフォンでの実装，実験をした結果，最短の被験者は 21 秒で認証に成功し，最適な速度である”普通”の速度では 9%程度の認証エラー率であること，表示形状による有意な差はないということが明らかになった．両表示形状の認証時間の中央値は 34.34 秒であった．

目で見ている情報と振動の認識の差は，振動を始めるタイミングや振動パターンによって，利用者が振動の認識が変わることが予想できる．つまりカーソルが振動するマスと重なっている間は振動をし続けるか，途中で振動を止めるかで認識の差がでることが予想できる．目で見た情報と振動の認識の差を縮小することで，認証エラーを低減することが可能と考えている．

認証失敗の原因の一つに操作性があげられる．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た事例が 3 件あった．それを差し引くと認証エラー率は 6%になる．このことから，多くの被験者が指摘するレスポンスの悪さの改善を行えば，操作ミスによる認証エラーが減少するとともに，認証時間の短縮にもなると考えている．

5.2 安全性確認実験結果

カメラによる解析は 10 人の解析で暗証番号が特定されることは無かった．しかし，利用者が急いでいるためカーソルが一周回る前に操作をしようとすると，操作を始める前に振動するマスがあったと推測ができてしまうため，情報の一部を攻撃者が手に入れることができる．本システムではカーソルが一周回転し終わる前に操作ができないようにしているが，利用者の手の動きで予想ができてしまう．今後の課題の一つである．

今回の端末とカメラの組み合わせでは推測できた被験者はいなかったが，覗き見攻撃が不可能なわけではない．端末の振動音の強さは個体差があり，あるタブレット端末では，振動音が大きく，離れた場所からでも振動音が聞こえる．このような端末での認証は，覗き見攻撃に成功する可能性が高くなる．カメラのマイクの性能にも個体毎に違いがあることが予想でき，例えば指向性マイクのような特定の方向からの音を録音することに特化したマイクを利用すれば，離れた場所からでも攻撃に成功する可能性がある．このような環境でも攻撃に対して安全な方法を検討していく必要がある．

5.3 既存のシステムとの比較

カメラによる攻撃に対して安全な既存の認証方式と比較をすると，fakePointer との差は安全な通信経路として振動を利用することで別途秘密情報を共有する装置を必要としないこと，Undercover との差はトラックボールの有無とその動きに該当する値の計算が不要である．振動で秘密情報を供する Phone Lock との差は振動をしたマスを見つけるだけなので振動に対応した数字を覚えなくて済むため記憶負荷が低い．上記 3 方式の実験結果と提案手法の実験結果との比較表が表 3 である．

表 3: 実験結果の比較

	認証時間 (秒)	エラー率 (%)	別装置
fakePointer	17.35(平均値)	5.6	必要
Undercover	45	26.3	必要
Phone Lock	28.2	10.4	不要
提案手法	34.34	9	不要

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．提案手法は，Undercover と比較してエラー率が 66%低く，認証時間も 24%短い．また提案手法は Phone Lock と比較してエラー率が 13%低い一方で，認証時間が 18%長い．

5.4 今後の課題

評価実験の事後アンケートの結果覗き見攻撃を脅威に感じる，強く脅威に感じると回答した被験者は 7 人，操作感が悪く素早い操作を認識

しないという点を指摘する被験者 9 人であった．これは実験に利用したソフトウェアの実装に問題があることがわかっており，今後改善する予定である．また”右シフト左シフトボタンの代わりに，一回の操作で複数回シフトできないか”という回答もあったため，今後取り入れていきたい機能である．ただし，取り入れたことで安全性が低下しないよう考慮し取り入れる必要がある．認証時間は”今後も使いたい”と相関があるので重要視して改善していきたい点である．また操作性の悪さで認証に失敗してしまった例もあるので操作性の改善でエラー率を下げることが可能だと考えられる．

振動音と操作画面を録画される攻撃に対してこのシステムは明らかに脆弱であるため，静かな場所での振動音を隠す方法を検討する必要があると考えている．認証中にスピーカーから認証とは無関係な音を鳴らすことで，静かな環境下でも振動音を捉えることができないようにするといった方法が考えられる．また Phone Lock のように，振動のかわりに音を用いるならば，ヘッドホンを持ち歩く利用者にとっては非常に使いやすくなることが予想できる．音を利用すればカーソルの移動が不要になるため非常に高速な入力が可能であると考えている．

本システムでは 0〜9 までの数字を用いたが，これをそのまま記憶負荷のより低い画像に置き換えることが容易にできる．画像に置き換えれば更に記憶負荷の低い認証方式の実現も可能であると考えている．

6　おわりに

本研究では，携帯端末での個人認証における覗き見攻撃を対象とし，その対策となりうる新たな携帯端末向け個人認証手法の提案した．提案手法は，4 桁暗証番号を基本とし，間接的に数値を入力する方法を採用することで，視覚情報による覗き見攻撃を困難にした．また間接的に入力するのに必要な入力位置の伝達を携帯端末の振動機能で行うことで，ビデオ録画による覗き見攻撃にも一定の安全性を確保した．さらにその入力位置が毎回ランダムに変更されることにより，複数回の覗き見攻撃に対しても安全性を確保可能とした．そして提案手法を Android アプリケーションとして実装し，利用可能性と覗き見攻撃に対する安全性に関する評価実験を行った．その結果，カーソル速度が普通の条件では，認証時間の中央値は，34.3 秒，認証エラー率は 9%という結果を得た．また安全性に関する実験においては，一定の条件下で撮影された動画からの暗証番号の抽出が困難であることが確認された．

参考文献

[1] 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, TEI ’11, pp. 197–200.

[2] De Luca, A., von Zezschwitz, E. and Hussmann, H.: Vibrapass: secure authentication based on shared lies, , CHI ’09, pp. 913–916.

[3] De Luca, A., von Zezschwitz, E., Nguyen, N. D. H., Maurer, M.-E., Rubegni, E., Scipioni, M. P. and Langheinrich, M.: Back-of-device authentication on smartphones, , CHI ’13, pp. 2389–2398.

[4] De Luca, A., Weiss, R. and Drewes, H.: Evaluation of eye-gaze interaction methods for security enhanced PIN-entry, OZCHI ’07, pp. 199–202.

[5] Sasamoto, H., Christin, N. and Hayashi, E.: Undercover: authentication usable in front of prying eyes, CHI ’08, pp. 183–192.

[6] Takada, T.: FakePointer: An Authentication Scheme for Improving Security against Peeping Attacks Using Video Cameras, UBICOMM ’08, Washington, pp. 395–400.

[7] ”喜多義弘，朝貝洸紀，菅井文郎，朴　美娘，岡崎直宣”: ”覗き見耐性を持つパスワード認証方式の提案と実装”, SCIS ’13.