3W-06

スマートフォンにおける複数個の振動パターンを用いた覗き見攻撃対策認証手法の検討

廣瀬　郁也†　　平川　豊‡　　大関　和夫‡

†芝浦工業大学大学院理工学研究科　　‡芝浦工業大学工学部

1. はじめに

近年，スマートフォンが急速に普及している．それに伴い，スマートフォンからも利用できるオンラインバンクや EC サイト，SNS が増加している．その利用にはそれぞれ ID とパスワードによる認証が必要となる．

スマートフォンにおける認証では，テキストパスワードを入力する方式のほか，数字を用いた PIN や，指で画面上に軌跡を描くパターンロックが多く用いられている．しかし，テキストパスワードや PIN，パターンロックは第 3 者がユーザの認証行為を覗き見・録画することで認証情報を不正に取得することができてしまう．オンラインバンクや EC サイト，SNS は ID とパスワードが露呈してしまうと他の端末上からでもアクセスが可能となってしまうため，個人情報が漏洩してしまう危険性が高い．

そこで本研究では，スマートフォンに標準で備わっている振動機能を用いて，覗き見攻撃・録画攻撃に耐性を持つ認証手法を検討する．

2. 関連研究

2 回の録画攻撃に耐性を持つ認証手法として，これまでに英数字を用いた方式[1]，[2]，画像を用いた方式[3]，数字を用いた方式[4]が提案されている．更に近年は 2 回だけではなく，多数回の録画攻撃に耐性を持つ数字を用いた認証方式が提案されている．多数回の録画攻撃に耐性を持つ[5]，[6]，[7]について，以下で概要を述べる．

まず，手法[5]，[6]は図 1 のようなダイヤル状のインターフェースを用いる．認証の際は外側の枠に P0～P9 で表された指定位置に，内側の枠に 0～9 で表されたパスワードを当てはめる．認証ごとにランダムに変化する指定位置を，音声でユーザに伝えられるのが[5]，認証開始時に P0～P9 までをインジケータが一定速度で 1 周し，指定位置に到達した際に振動で伝えられるのが[6]である．[7]の，インターフェースは電卓のように数字を四角く配置したもので，認証の際はまず事前に設定したパスワードがどこに配置されているかを記憶しておく．次にユーザが端末を任意の方向に傾けることで数字の配置がランダムに代わるので，最初に記憶した数字の位置にどの数字が配置されたかを記憶する．再度別の方向に傾けると元の配置に戻るので，そこで記憶した数字を入力することで認証が完了する．

問題点として，[5]は音を用いるためイヤホンの装着が必要となり，[6]は機器の装着は必要無いが，インジケータが 1 周するのを待つため認証時間が長くなっていた．[7]は画面を傾けた際に傾けた方向両側から録画された際に録画耐性を持たない．

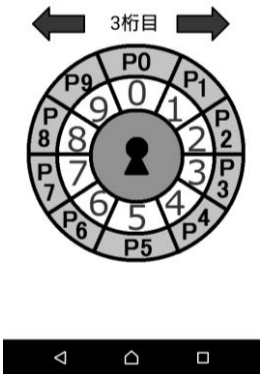

図 1 [5]，[6]の画面

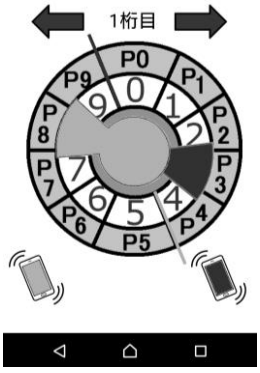

図 2 提案手法の画面

3. 提案手法

本研究では，振動を 2 パターン用意し，振動に対応したインジケータが指す場所にパスワードを当てはめることでインジケータが周り終わるまでの時間を短くすることで，[6]の問題点であった認証時間を短縮する手法を検討する．

図 2 に提案手法の画面を示す．画面は上部にパスワードを指定位置に移動させるための矢印，中央に認証用のダイヤル，下部に振動とインジケータの対応を確認するためのアイコンで構成されている．

以下に認証手順を示す．

手順 1：認証を開始すると，右側の赤のインジケータが P0～P4，左側の青のインジケータが P5～P9 を時計回りに回り始める

An Attempt of Shoulder Surfing Resistant Authentication System by Using Multiple Vibration Patterns in Smart Phones
† Fumiya Hirose, ‡Yutaka Hirakawa, ‡Kazuo Ohzeki
†Graduate School of Engineering, Shibaura Institute of Technology
‡Shibaura Institute of Technology

ので，ユーザは手に持ったスマートフォンが振動するのを待つ．

手順 2：スマートフォンが振動したら，振動の種類と対応するインジケータの位置によって指定位置を特定する．振動とインジケータの対応は表 1 の通りである．

手順 3：矢印をタップして特定した指定位置にパスワードを当てはめ，中央の鍵ボタンをタップする．

手順 4：最後の桁が終わるまで手順 1～3 を繰り返す．

表 1　振動とインジケータの対応

振動の種類	対応するインジケータ
長い振動 1 回	青いインジケータ(左側)
短い振動 2 回	赤いインジケータ(右側)

4. 評価実験

提案方式の認証成功率，認証時間を評価するための実験を行った．実験概要を以下に示す．

インジケータの回転速度は 500ms に設定し，[6]のようにインジケータが 1 周する際にパスワードを当てはめる場所で長い振動が 1 回起きるもの(振動 1)，短い振動が 2 回起きるもの(振動 2)，提案手法の 3 パターンを，本学学生 10 人に操作してもらった．なお実験手順は，手法の説明をした後に操作の練習をしてもらい，その後に暗証番号 4 桁の認証を 2 回行う試行をそれぞれのパターンで行ってもらった．4 桁の暗証番号は，記憶しやすいよう全パターン「1111」で固定した．表 2，表 3 に実験の結果を示す．

表 2 の認証成功率を見ると，振動 1 と振動 2 の間での違いは見られなかったが，提案手法では振動 1，振動 2 よりも 5%下がっていた．表 3 の誤認証の内訳を見ると，提案手法の誤認証は振動 1，振動 2 と同じパターンの誤認証とは別に，パスワードを振動が伝えた指定位置 P3 に当てはめるはずが，対角線上の P8 と誤認し当てはめてしまっているものがあった．この誤認証の原因は，振動パターンの違いが認識できなかったことであると考えられる．

認証時間については，振動 1，2 間ではあまり大きな差が無かったが，提案手法では振動 1，2 から 10 秒程短縮できた．

表 2　実験結果

	認証成功率	平均認証時間
振動 1	95%	31.8 秒
振動 2	95%	29.4 秒
提案手法	90%	22.2 秒

表 3　誤認証の内訳

	指定位置	誤認位置
振動 1	P1	P0
振動 2	P1	P0
提案手法	P1	P0
	P3	P8

5. 考察

提案手法は既存の方式よりも認証時間を縮めることはできたが，認証成功率も下がってしまった．この原因としては，振動とインジケータの対応をユーザが直感的に認識しづらかったのではないかと考えられる．そのため，今後はより対応が認識しやすいパターンを調べていく．

また，今回覗き見耐性や録画耐性についての実験はできていないので，今後覗き見耐性や録画耐性を本当に備えているのかをユーザテストや録画機器を用いて検証する必要がある．

参考文献

[1] Sakurai, Yoshida, Bunaka, “Mobile authentication method”, Computer Security Symposium 2004, pp.625-630 (Oct 2004).

[2] Yutaka Hirakawa, “Random Board: Password Authentication Method with Toletance to Video-Recording Attacks”, IJIMT Journal, vol.4, no.5, pp.455-460 (2013).

[3] Hirakawa, Take, Ohzeki, “Pass-Image Authentication Method Tolerant to Random and VideopRecording Attacks”, IJCSA Journal, vol.9, no.3, pp.20-36 (2012).

[4] Yutaka Hirakawa, Takumi Itoh, and Kazuo Ohzeki, “A new Numerical Password Authentication Method”, IJITCS Journal, vol.12, no.4, pp.7-15 (2013).

[5] Yutaka Hirakawa, Yutaro Kogure, Kazuo Ohzeki, “A Password Authentication Method Tolerant to Video-recording Attacks Analyzing Multiple Authentication Operations”, IJCSEE Journal, vol.3, Issue5, pp.356-360, ISSN 2320-4028 (online)(2015).

[6] 石塚 正也, 高田 哲司, “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”, IPSJ Interaction 2014, pp.501-503 (2014).

[7] 遠藤 将, 村松 弘明, 藤田 真浩, 西垣 正勝, “メンタルタスクと視線遮断動作を併用したユーザ認証の覗き見対策の提案”, IPSJ SIG Technical Report, vol.2016-CSEC-72, No.22, pp.1-7, ISSN 2188-8655 (2016).