

ユーザの視線経路を用いた PIN 入力手法の提案

平田 木乃美^{a)}・山口 翔太^{b)}・山場 久昭^{c)}・油田 健太郎^{d)}・岡崎 直宣^{e)}

Proposal of a PIN Authentication Method Using User's Sight Line Path

Konomi HIRATA, Syota YAMAGUCHI, Hisaaki YAMABA, Kentaro ABURADA, Naonobu OKAZAKI

Abstract

Traditional knowledge-based authentication techniques such as inputting a password with a keyboard are vulnerable to malicious observers. They can grab password information by shoulder surfing attack. To prevent such attacks, the gazing-based authentication method without touching a keyboard was proposed. The method has a shoulder surfing resistance, however most gazing-based method needs a high-precision calibration. It is troublesome for users and causes decline of usability. In this paper, we focus on the calibration. Our proposal is the method by user's sight-line path, not sight-line position. We implemented the method and evaluate the performance.

Keywords: user authentication, shoulder surfing, sight-line path

1. はじめに

PIN (個人識別番号) は、個人認証のためのパスワードとして広く利用されている。偶然に認証を突破する確率 (偶然認証突破確率) を低くするため、PIN は通常、0~9 の数字の 4 桁の組み合わせから成っている。4 桁の数字というのは人間にとって記憶しやすく、また入力にかかる時間も非常に短いため様々な場面で利用されている。身近なところでは銀行の ATM の個人認証や、スマートフォンなどのモバイル機器におけるロック解除などがある。しかし、PIN 入力による認証は正当なユーザが PIN を入力しているところを肩越しから盗み見る覗き見攻撃に対して非常に脆弱である。この問題を解決するために様々な手法が提案されている¹⁾²⁾³⁾⁴⁾。覗き見攻撃に耐性を持つ手法の中に、ユーザの手ではなく視線で PIN 入力を行う手法がある¹⁾²⁾。視線によって PIN 入力を行う手法は、第三者が PIN 入力画面を見たとしてもどの数字が入力されたか推測出来ないため、覗き見攻撃や入力画面の録画画像を用いた攻撃である録画攻撃に耐性を持っている。しかし、視線による PIN 入力手法はユーザごとにキャリブレーションを行わなければならない、キャリブレーションの精度次第では認証成功率が低下する可能性がある。また、一度入力が終了し、入力画面の前を離れ、再び入力を行うといった場合、以前の入力時と比べ、ユーザの頭の位置や姿勢にずれが生じ、キャリブレーションの効果が弱まる傾向にある。PIN 入力のたびにキャリブレーションを行えば常に高い効果を維持できるが、

それはユーザにとって煩雑であり、ユーザビリティの低下につながる。本研究では、このキャリブレーションに着目し、ユーザが行うキャリブレーションの回数を減らすことを大きな目的とする。そこで、ユーザの視線位置情報を用いた入力手法ではなく、ユーザの視線経路情報を用いた入力手法を提案する。提案手法では、各数字タイルが移動し、ユーザは移動するタイルを視線で追跡することによりその数字を入力することができる。また、ユーザの視線によって入力を行うため覗き見攻撃、録画攻撃に耐性を持ち、パスワードを数字 4 桁にすることで、偶然認証突破確率を低下させることが出来た。

2. 関連研究

2.1 注視による PIN 入力手法

この手法¹⁾は、スクリーン上に表示された数字のキーパッドの中から自分が入力したい数字を見ることで PIN を入力する手法である。この手法の PIN 入力画面を図 1 に示す。注視による PIN 入力手法は、見たものがすべて入力とされてしまうミダスタッチ問題が大きな問題点として挙げられるが、この手法では、1 秒以上注視していたと判定された数字を PIN として入力することでミダスタッチ問題の発生を抑えている。しかし、この手法はキャリブレーションの精度により認証成功率が低下する可能性があることが指摘されている。

2.2 注視と視線のジェスチャによる PIN 入力手法

この手法²⁾は、中央の点と入力したい数字を交互に見て数字の入力を行う手法である。この手法は、入力したい数字を見た後に中央の点を見なければ入力数字の判定が行われれないというアルゴリズムと、数字をロータリー型の配置にすることで、ミダスタッチ問題の発生を抑えている。この手法も¹⁾と同様に、注視による入力判定部分が存在するため、キャリブ

^{a)}工学専攻機械・情報系コース大学院生

^{b)}情報システム工学科学部生

^{c)}情報システム工学助教

^{d)}情報システム工学助教授

^{e)}情報システム工学助教授



図 1. 注視による PIN 入力手法

レーションの精度により認証成功率が低下する可能性がある。

2.3 人間の眼球の動きについて

人間が物を見るときにの眼球の動きにはいくつか種類があるが⁵⁾、視線による PIN 入力と特に関係が深いのは、固視、衝動性眼球運動、滑動性追従眼球運動の 3 つである。固視は、ある一箇所を見続けるときの眼球の動きである。普段私たちは視線が止まった状態である固視と、視線を瞬間的に移動させる衝動性眼球運動(後述)を繰り返すことで視覚情報を取り入れている。衝動性眼球運動は、ある視線位置から離れた別の位置へ視線を移動させるときの瞬間的な眼球の動きである。サッカード、サックードとも呼ばれる。滑動性追従眼球運動は、ゆっくり動く物体を目で追従するときの滑らかな眼球の運動である。パーストとも呼ばれる。本稿の提案手法では、この運動が主に用いられる。

3. 提案手法

3.1 研究方針と目標

既存の研究では、スクリーン上に表示された数字を注視して PIN を入力する手法が提案されているが、数字を注視するという性質上、ユーザが見ている位置と検出したユーザの視線位置にずれが生じると認証成功率が低下する可能性がある。そのため、ユーザが PIN 入力を行うたびにキャリブレーションを行わなければならない、その精度も高いものが要求される。そこで本研究では、ユーザの視線位置ではなく、ユーザの視線経路を用いた PIN 入力手法を提案する。提案手法の設計目標を以下にまとめる。

- キャリブレーション回数低減と認証成功率の維持
ユーザが手法を初めて使うときはキャリブレーションを行うが、以降はキャリブレーションを行わなくても PIN 入力成功率が低下しない設計を目指す。
- ユーザビリティ
ユーザが直感的に理解しやすい操作で PIN 入力を行うことができる設計を目指す。

3.2 前提条件

3.2.1 視線追跡デバイスの使用

本研究では、視線追跡デバイスの使用を前提として提案手法の設計を行った。使用したデバイスは Tobii EyeX Controller



図 2. Tobii EyeX Controller

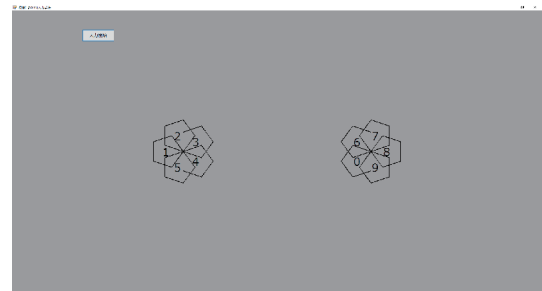


図 3. 提案手法の PIN 入力画面と数字の配置

(以下 Tobii EyeX) である。デバイスの外観を図 2 に示す。このデバイスを用いてユーザの視線位置を検出する。

3.2.2 PIN の入力桁数

提案手法では、数字 4 桁のパスワードを PIN として入力することで認証を行う。PIN は、1 桁につき 0~9 のいずれかの数字で構成されている。4 桁入力時の偶然認証突破確率は、

$$\frac{1}{10^4} = \frac{1}{10000}$$

となり、従来の PIN 認証と同じ偶然認証突破確率を達成している。また、4 桁の PIN は、スマートフォンなどのモバイル機器におけるネットワーク認証や銀行の ATM における個人認証などに用いられているため、ユーザにとって馴染みやすい桁数である。

3.3 提案手法

既存手法では、ユーザが見ているものがすべて選択されてしまうこと(ミダスタッチ問題)と、キャリブレーションの精度が低い場合、認証成功率が低下する可能性があることが主な問題点として挙げられていた。これらの問題点を改善するために、注視によって PIN 入力を行うのではなく、ユーザの視線経路によって PIN 入力を行う手法を提案する。

提案手法の入力画面には、0~9 の数字が設定されたタイルが表示され、入力を開始すると各タイルは移動を開始する。ユーザは、移動するタイルを視線で追跡することで PIN 入力を行う。

提案手法の PIN 入力画面と各数字の配置を図 3 に示す。提案手法は画面上部の入力開始ボタンと画面中央付近の数字タイルで構成されており、ユーザが入力開始ボタンをクリックすることで認証が開始される。

次に各タイルの動きについて説明する。各タイルは動的なオブジェクトである。ユーザが画面上部の入力開始ボタンをクリックすると、各タイルが移動を開始する。各タイルはそれぞれが離れていくように広がり、一定の場所まで広がったら(図 4)、元の位置(図 3)へ戻っていく。ユーザは、広がっていくタイルを視線で追跡することで、そのタイルの数字を入力することができる。この、広がって戻る、という動作 1 回が PIN 入力 1 桁に相当しており、提案手法では、この動作を 4 回繰り返すことで 4 桁の PIN 入力を行う。

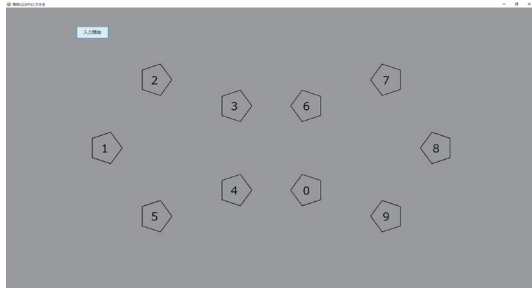


図 4. 移動後のタイル

4. 評価実験

4.1 実験概要

評価実験では、提案手法の認証成功率、ユーザの離席による認証成功率への影響、また、他人のキャリブレーション設定を用いて入力した場合の認証成功率を検証した。被験者は宮崎大学工学部の学生 10 人、視線追跡デバイスは Tobii EyeX を使用した。実験の前に提案手法における PIN 入力方法を説明して、その後、PIN 入力習熟のための練習を行う。そして実験 1、実験 2、実験 3 の順に実験を行った。また、本実験における認証成否の定義は、提示された PIN と被験者が入力した PIN が完全に一致した場合を認証成功とし、提示された PIN と被験者が入力した PIN が 1 桁でも異なっていた場合を認証失敗とする。3 種類の実験の詳細を以下に示す。

実験の際のキャリブレーションは、使用デバイスのキャリブレーション機能を用いる。

被験者が実験 1、実験 2、実験 3 で入力する 4 桁の PIN は、0000～9999 の範囲でランダムに作成した 4 桁の数字である。

4.2 実験 1 (キャリブレーション後の入力成功率)

実験 1 は、被験者のキャリブレーションを行った状態での認証成功率を検証する実験である。被験者のキャリブレーション設定は練習前に行ったキャリブレーション設定をそのまま使用し、提案手法を用いて 4 桁の PIN を被験者 1 人当たり 10 回入力してもらった。

4.3 実験 2 (離席後の入力成功率)

実験 2 は、離席によりユーザの姿勢や頭の位置にずれが生じた場合でも、キャリブレーション後の認証成功率を維持できるかを検証する実験である。実験 2 ではキャリブレーション設定は変更せず、被験者には一度離席し再び着席した後、実験 1 と同様に 4 桁の PIN を 10 回入力してもらった。

4.4 実験 3 (他人の設定を用いた場合の入力成功率)

本研究では、視線追跡デバイスの使用を前提として提案手法の設計を行ったが、本研究で使用したデバイスでは、初回使用時でも必ずゲスト、もしくはユーザとしてキャリブレーションを行わなければ視線検出が開始されないため、完全にキャリブレーションが行われていない状態で PIN 入力を行うことは出来ない。そのため、代案としてユーザが他人のキャリブレーション設定を用いて PIN 入力を行い、キャリブレーションを行わずに高い認証成功率を得られるかを検証する。被験者には著者のキャリブレーション設定を他人のキャリブレーション設定として用いたうえで 4 桁の PIN を 10 回入力してもらった。

表 1. 実験 1 と実験 2 の結果

	認証成功率
実験 1 (キャリブレーション後)	74%
実験 2 (離席後)	85%

5. 実験結果と考察

5.1 実験 1 と実験 2 の結果と考察

実験 1 と実験 2 は、ランダムに作成された 4 桁の PIN を被験者 1 人当たり 10 回入力してもらい、それぞれ 100 回の 4 桁 PIN 入力結果が得られた。実験 1 及び実験 2 により得られた、提案手法におけるキャリブレーション後の認証成功率、離席後の認証成功率を表 1 に示す。

表 1 より、実験 1 の認証成功率は 74%、実験 2 の認証成功率は 85% である。実験 2 は一度被験者に離席してもらった後に PIN 入力を行うため、実験 2 の認証成功率は低下すると予想していたが、実験 1 よりも実験 2 の方が 11% 高い結果となった。実験 1 と比べて実験 2 の認証成功率が低下した被験者は 2 人、同じ認証成功率だった被験者は 3 人、認証成功率が向上した被験者は 5 人であった。しかし、実験 1 と比べて実験 2 の認証成功率が低下した 2 人の被験者も大幅に低下したわけではなく、それぞれ 10% 低下した (入力が成功した PIN の個数が 1 個減少した) 程度であった。これらの実験結果は、提案手法は離席によるキャリブレーション効果の減少の影響をほぼ受けないことを示している。

また、実験 1 よりも実験 2 の認証成功率が高くなった要因は、実験 1、実験 2 という順で実験を行ったことにあると考えられる。4.1 で述べたように、被験者は、実験を行う前に提案手法における PIN 入力の習熟を図るための練習を行っている。そのうえで実験へ移ったが、実験 1 で 4 桁の PIN を 10 回入力することで、さらに習熟が図られたのではないかと考えられる。

5.2 実験 3 の結果と考察

実験 3 は、被験者のキャリブレーション設定を著者のキャリブレーション設定に変更し、そのうえで実験 1、実験 2 と同様に 4 桁の PIN を被験者 1 人当たり 10 回入力してもらい、計 100 回の 4 桁 PIN 入力結果が得られた。実験 3 より得られた認証成功率を表 2 に示す。

表 2 より、提案手法で他人のキャリブレーション設定を用いて PIN 入力を行った場合の認証成功率は 63% である。実験 3 の結果から、提案手法は、他人のキャリブレーション設定を用いて PIN 入力を行った場合でも 50% を超える認証成功率を達成できることが分かった。しかし、被験者毎の認証成功率にはばらつきがあり、入力成功率が 0% の被験者は 1 人、約 50～60% の被験者は 5 人、90～100% の被験者は 4 人であった。他人のキャリブレーション設定には著者の設定を用いたことを考慮すると、著者との体格の差によってばらつきが発生したと考えられる。

表 2. 実験 3 の結果

実験 3 (他人のキャリブレーション設定)	認証成功率
	63%

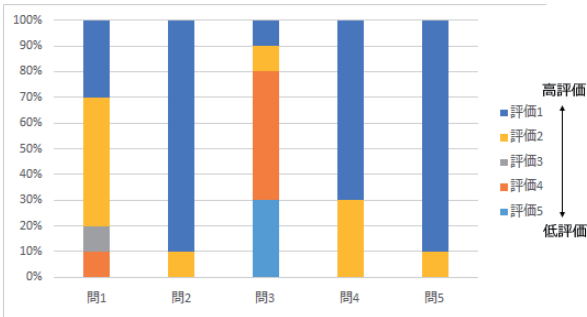


図 5. アンケート結果

5.3 提案手法の PIN 入力時間

ここでは、提案手法の PIN 入力時間に関する考察を行う。PIN 入力手法において、PIN 入力時間は重要な評価項目の一つである。提案手法では、移動するオブジェクトを視線で追跡して PIN 入力を行う。そのため、PIN 入力時にはオブジェクトの移動時間も含まれることになる。しかし、提案手法のオブジェクト移動時間、入力間のインターバル時間は一定であり、また、入力する PIN の桁数も 4 桁と固定されているため、ユーザによって PIN 入力時間が変動することはない。

提案手法の PIN 入力時間は、入力画面上部の入力開始ボタンを押してから入力した 4 桁の PIN が表示されるまでの時間とする。著者が PIN 入力時間を 10 回計測し、その平均を求めたところ、12.04 秒という入力時間が求められた。このことから、提案手法を用いて 4 桁の PIN を 1 つ入力する場合、約 12 秒かかることが分かった。

6. ユーザビリティに関するアンケート調査

提案手法のユーザビリティを評価するため、実験に参加した被験者 10 名にアンケートを実施した。アンケート調査では、各質問に対し 1 (高評価) ~ 5 (低評価) の 5 段階評価で回答してもらい、最後に自由記入欄を設けた。質問内容を以下に示す。

- 問 1 当 PIN 入力手法は使いやすかったか
- 問 2 視線で移動するタイルを追いかけるといった操作は直感的に理解しやすいか
- 問 3 視線で移動するタイルを追いかけて入力するという操作に慣れは必要か
- 問 4 1 桁の PIN 入力ごとのインターバル時間はユーザにとって適切なものであったか
- 問 5 タイルの移動速度はユーザにとって適切なものであったか

5 段階評価のアンケート結果を図 5 に示す。図 5 より、問 1 で 80% の被験者が 1、2 の高評価をつけたため、提案手法はユーザにとって使いやすい手法であるといえる。問 2 では、90% の被験者が、視線で移動するタイルを追跡するという操作を理解しやすいと回答したが、問 3 では、80% の被験者が視線

で移動するタイルを追跡するという操作に慣れが「必要」、「やや必要」と回答していることから、この操作はユーザが理解しやすい操作だが、慣れも必要な操作であることが分かった。問 4、問 5 では、1 桁の入力間のインターバル時間とタイルの移動速度に関して、全ての被験者が 1、2 の高評価をつけたため、提案手法における入力間のインターバル時間とタイルの移動速度は、多くのユーザにとって好ましい時間、速度であることが分かった。そのほか、入力の慣れ次第でタイルの移動速度を変更したいという意見もあり、このことから、ユーザが自分で入力間のインターバル時間やタイルの移動速度を調整できる機能を追加することで、更なるユーザビリティの向上につながると考えられる。

7. まとめ

本研究では、ユーザのキャリブレーション回数を減らすことを大きな目的として、ユーザの視線経路を用いた PIN 入力手法の提案を行った。そして、提案手法の実装と評価を行った。提案手法のキャリブレーション後の認証成功率は 74%、離席後の認証成功率は 85% となり、これらの結果から、提案手法は離席などによるユーザのキャリブレーション効果の減少の影響をほぼ受けないということが分かった。さらに、他人のキャリブレーション設定を用いた場合の認証成功率は 63% であり、本研究は、キャリブレーションフリーの PIN 入力手法の実現に寄与できたと考えられる。

今後の課題として、設計の改善による PIN 入力時間の短縮を含むユーザビリティの向上、認証成功率の向上が挙げられる。

参考文献

- 1) Mythreya Seetharama, Volker Paelke, and Carsten Rocker : SafetyPIN: Secure PIN Entry Through Eye Tracking, HAS(Human Aspects of Information Security, Privacy, and Trust) 2015, pp.426-435, 2015.
- 2) Darrell S. Best, Andrew T. Duchowski : A Rotary Dial for Gaze-based PIN Entry, ETRA(Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications) 2016, pp.69-76, 2016.
- 3) 東山侑真, 岡村真吾, 矢内直人, et al. : 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, 情報処理学会 Computer Security Symposium 2014, pp.1023-1028, 2014.
- 4) 石塚正也, 高田哲司 : 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, 情報処理学会 Computer Security Symposium 2013, pp.708-715, 2013.
- 5) Wikipedia:眼球運動障害, available from (<https://ja.wikipedia.org/wiki/>), (2018/02/05).