機器特性を考慮したあみだくじ視線認証の提案

藤　竜成 [a)]・黒野 聖 [b)]・山場　久昭 [c)]・油田　健太郎 [d)]・岡崎　直宣 [e)]

Ladder Lottery Type Gaze Authentication Considering Device Characteristics

Ryusei FUJI, Seira KURONO, Hisaaki YAMABA, Kentaro ABURADA, Naonobu OKAZAKI

Abstract

With the spread of mobile devices, the risk of being logged in the devices illegally by third parties has been increasing. There are various attacks, shoulder-surfing, thermal-attack, smudge-attack, for example. For that reason, we studied the gaze authentication as the authentication has the resistant to the above attacks. However, the previous study proposed the ladder lottery type gaze authentication that solves the problems of gaze authentication. In the authentication, there are a screen for displaying four path icons determined beforehand and for actually performing the authentication. The previous study has problems of eye tracking, so in this study, we tackle the problems. As a result of the comparative experiments, the time to find the path of the proposed method was longer by 4.8 s, but the time performing the authentication was shorter by 2.8 s. Eventually, the authentication time was longer by 1.9 s, but the authentication success rate was improved by 26.7%. From the result, it is considered that the proposed method can be improved the authentication time by devising the screen searching for the path icons.

Keywords: gaze authentication, ladder lottery, shoulder-surfing, eye tracking

1. はじめに

各個人がパソコン、モバイル端末を保有していることが一般的となり、街中では端末を凝視している人を見かけない日が無くなった現代では、各々が個人の情報を厳重に管理する必要がある。その個人を識別する物の大部分を占めるのが認証であり、認証は本人かそうでないかを識別し、個人情報や機密情報を保護する大きな役割を担っている。そのため、認証では世に普及しているパスワード認証、PIN 認証だけではなく、現在進行形で様々な認証の研究が日々行われている。

本論文では主に視線を用いた認証について記述をする。視線認証はショルダーサーフィン、スマッジアタック、サーマルアタックなどに耐性がある事で注目されている。また、欠点としては認証成功率の低さや認証速度の遅さが挙げられる。それらの欠点を改善するために日本古来からある、あみだくじというシンプルな手法を用いて認証を単純化する事で、視線認証における欠点の軽減を図った事前研究 [1)] を元に本研究は行。うその事前研究 [1)] の向上のために横画面に対応したあみだくじ認証を作成し、それぞれの認証成功率や認証速度を確かめる実験を行った。その実験からユーザビリティアンケートを記述してもらい、考察を述べ最後にまとめを述べる。

[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)] 情報システム工学科助教
[d)] 情報システム工学科准教授
[e)] 情報システム工学科教授

2. 研究背景

2.1 認証について

認証は大きく分けて 3 種類のものがある。最も普及している物を例に挙げると、本人のみが知っている事を前提とした (1) パスワード認証、PIN 認証がある。また、現在も更なる研究がされている指紋認証、虹彩認証、静脈認証などの個人の体の特徴を用いた (2) 生体認証がある。その他に (3) 個人の所有物で本人を認識する ID カードなどを用いる認証がある。上に記述した (1)〜(3) のいずれかを利用し、本人であるかどうかを識別する。

2.2 認証に対する攻撃

2.1 に記述した認証方式は今も広く利用されている。一番身近なものでスマートフォン、タブレットやパソコンのロック画面を解除する際に頻繁にパスワードが用いられ、街中や人込みでも何の気もなく指を動かし認証を行う。その行為にはいくつか危険を孕んでいて、他者から攻撃を受けるきっかけに十分成り得る。

考えられる攻撃としては 3 つある。

1. 認証している画面を後ろから覗き見されて覚えた暗証番号やパスワードで不正ログインを行うショルダーサーフィン。
2. 認証した後の指の熱を頼りに不正ログインを行うサーマルアタック。
3. 認証する際に付着した指紋などの汚れをたどり不正ログインを行うスマッジアタック。

これらの攻撃に耐性があるとして、視線認証が注目されている。

2.3 視線追跡技術

最近では、モバイル端末やパソコンの内カメラの性能の向上や視線を追跡する外部装置の発展により視線を用いた技術の研究も多方面に行われるようになった。例えば、本人が凝視している部分以外にフィルタを掛け、後ろから覗き見して情報を盗むショルダーサーフィンを防ぐ技術[2]、視線の速度を特徴量として個人を識別する視線を用いた生体認証[3]、VR ヘッドセットの疑似仮想空間内で視線を用いて PIN 入力を行う認証[4]などがある。今後も視線追跡技術の更なる発達に伴い、高度に視線の利用が出来る可能性を秘め、期待される技術である。

2.4 視線認証

2.3 に記述した視線追跡技術の発展により視線を使った認証もまた視野が広がりつつある。2.2 に記述した攻撃に対し、認証動作を観測されない、認証時に画面に触れる事が無いなどの視線のみを扱う強みを生かした認証を可能としている。

しかし、認証成功率が低い、認証時間が長いという欠点もある. そのため、視線認証の課題としてはいかに素早く認証が完了でき、またいかに正確に認証ができるかが研究の肝となっている。その他に視線追跡の欠点として、頭の動きや視線のズレの許容が難しい事も挙げられる。この頭のブレなどの視線のズレは 2.3 に記述した追跡技術の進歩によって今後改善されると考えられる。

最後に、視線認証特有の問題としてミダスタッチ問題がある。視線で操作を行う限り、認証判定は連続的なデータを判定に用いる。そのため、本来見るべき対象とは別の対象を誤認識してしまうミダスタッチ問題が起こってしまう。この問題を解消するために対象と対象の距離を離したり、認証の判定時間を調整したり、認証完了時にマウスやキーボードからの入力をしたりなどの工夫が必要となる。また、この問題を解決するためにフィッツの法則を用いて見るべき対象に到達する時間の予測を計算し、実際の視線の到達時間と比べ判定するという研究[5]もあり、ミダスタッチ問題に対しての研究も進んでいる。

2.5 視線認証に対する攻撃

視線認証に対する攻撃としては 2 つ考えられる。

1. 録画機器で認証行為を録画し、パスワードを推測する録画攻撃。

2. 認証している画面と認証している人の顔を見て、その認証行為からパスワードを推測し攻撃する反復攻撃。

が挙げられる。

しかし、横、斜め後ろから覗いても横顔と認証画面だけでのパスワードの推測は難しく、視線の大きな動きや認証画面に規則性などが無い限りは容易ではない事が分かる。また、真後ろから覗かれた際や真正面から見られた際などの一方向のみの観測では、観測対象の変化が見られないためパスワードの推測は不可能に近いものだと考えられる。

3. 関連研究

3.1 あみだくじ視線認証

事前研究としてランダム性を持ったあみだくじ型視線認証の提案[1]がある。48 個の囮アイコンと 4 個のパスアイコンとが 3 列で左から 13、26、13 の数で縦に羅列してある。それをあみだくじの要領で上から注視していき、パスアイコンを見つけた位置で左か右に視線を移すというシンプルな認証である。また、チャレンジレスポンス方式を用いており認証の度にアイコン配置がランダムに変わる。そのため、攻撃者にとっては毎回異なる視線の動きと認証画面になり、攻撃がしにくいものとなっている。さらにはパケットを監視して認証をしようとしても毎回レスポンスが変わるため、コピーして認証をしようとしても認証に失敗する。この様な盗聴攻撃に対しても耐性を持ち合わせている。

4. 提案手法

事前研究のあみだくじ認証を横画面として対応させた。この提案手法の利点としては視線追跡装置の上下幅の範囲が、縦にすると認識しづらい問題の解決と人間の目の動きが上下をあまり得意としていないため、横に広く視線幅を取ることで認証速度の向上が期待出来ると考えたからである。また、この認証を実際に扱う際に現在のモバイル端末の内カメラの精度を考慮すると適用することは難しい。そのため、パソコン、ノートパソコンに向けた実装が主となる場合、画面を横長で使っている人が大多数であるという利点もある。

この認証では大きく分けて図 1, 図 2 の 2 つの画面がある。それぞれの画面で時間計測が行われており、それぞれの時間の合計が認証時間となっている。

4.1 アイコン探索画面

認証を開始したと同時に図 1 のアイコン探索画面が表示され、時間の計測が始まる。ここで計測した時間のことを探索時間とする。この画面でパスアイコンを探す。探しだした 4 つのパスアイコンのうち最も左側に配置されているパスアイコンの行の左端にある認証開始点を見ることで次の図 2 の画面に移る。

4.2 認証開始画面

アイコン探索画面の左端にある認証開始点を見ると、図 2 の認証開始画面が表示され、ここでも時間の計測を行う。ここで計測した時間のことを実行時間とする。認証が開始すると、視線でなぞる指標となるようにあみだの黒線が表示される。左端からパスアイコンの所まで視線でなぞっていき、パスアイコンが配置されている所で上か下に黒線に沿って視線を移すことで認証を可能としている. 最後に 4 つ目のパスアイコンから視線を移動させた行の右端にある認証終了点を見ることで認証完了となる。この一連の動作があみだくじ認証となっている。

5. 実験

第 5 章では、始めに実装のために使用した機器と環境開発を述べ、次に実験方法。最後にあみだくじを横画面にしてど

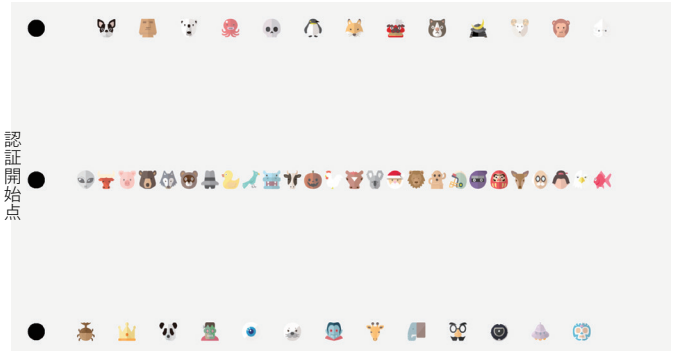

図 1. アイコン探索画面

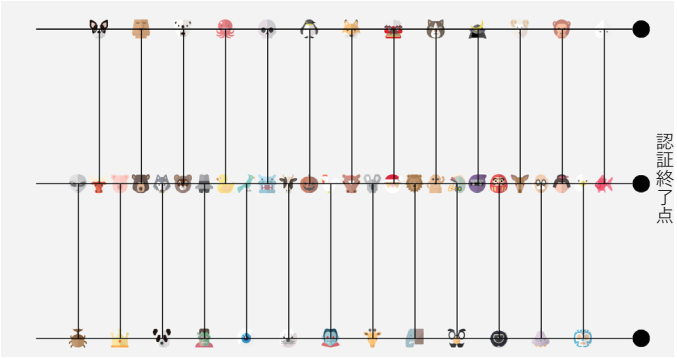

図 2. 認証開始画面

図 3. Tobii Eye Tracker 4C

の様な成果が得られたのかを実際に縦画面と横画面のあみだくじ認証の実験を行い、それぞれの認証成功率、認証速度とユーザビリティアンケートで得られた結果を述べる。

5.1 実装

実装には C # 言語を用い, 開発ソフトは Visual Stdio 2017 を使用した。視線追跡は外部装置である Tobii Eye Tracker 4C(図 3) を用いてユーザの視線位置を検出した。

5.2 実験方法

提案手法と既存手法の認証時間、認証成功率をそれぞれ調査した。被験者として宮崎大学工学部生 3 名に実験を行ってもらった。被験者は眼鏡やコンタクトの着用が可能であり、目の疲労も考慮して自由に休憩を取ることができる。

実験手順としては、始めに被験者に実験の流れを説明し、パスワードとなる 4 つのアイコンを任意で選んでもらった。次に, 入念にキャリブレーションを行い, 認証に慣れるまで練習をしてもらった。なお、練習中は何度でもキャリブレーションをやり直すことができる。本実験では、提案手法の認証を 10 回行った後、既存手法の認証を 10 回行った。

最後に、実験後にアンケートを記入してもらった。アンケートでは既存手法と提案手法それぞれについて以下の 3 項目について 1（そう思わない）～5（そう思う）の 5 段階評価で回答してもらった。また、意見なども記入してもらった。

1. この認証を利用するには慣れが必要であると感じた。

表 1. 既存手法の認証時間と認証成功率

探索時間 (s)	実行時間 (s)	認証時間 (s)	成功率 (%)
6.6	9.0	15.6	50.0

表 2. 提案手法の認証時間と認証成功率

探索時間 (s)	実行時間 (s)	認証時間 (s)	成功率 (%)
11.3	6.2	17.5	76.7

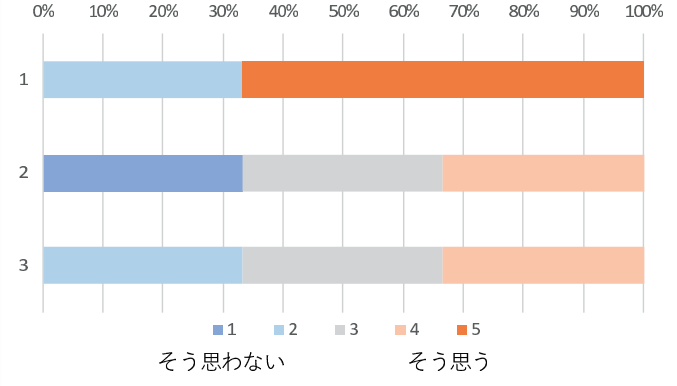

図 4. 既存手法アンケート

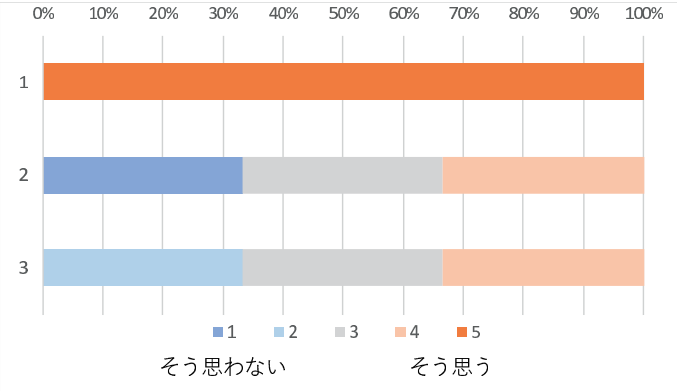

図 5. 提案手法アンケート

2. この認証は使いやすかった。
3. パスアイコンは探しやすかった。

5.3 結果

5.3.1 認証精度

既存手法の認証時間と認証成功率の平均を表 1、提案手法の認証時間と認証成功率の平均を表 2 にまとめた。

表 1 と表 2 から、提案手法の探索時間は既存手法よりも 4.7s 長く、実行時間は 2.8s 短くなった。最終的に認証にかかった時間は提案手法の認証時間は既存手法よりも 1.9s 長くなった。また、認証成功率は提案手法の方が 26.7 %向上するという結果になった。

5.3.2 ユーザビリティ評価

図 4、図 5 から、どちらの手法も慣れがかなり重要な要素になっている事が分かる。また、それぞれの提案手法と既存手法の使いやすさやパスアイコンの探しやすさについてはグラフとして見ると、評価は同等となっている。

6. 考察

今回の実験では提案手法から始めに実験を行ってもらい、既存手法を後に実験をしてもらう流れとなっている。そのため、既存手法はある程度の慣れを含んでいる可能性があり、結果だけを見て優劣を下す事は困難を有するのではないかと考えられる。また、母数の少なさから、結果の偏りが生じている可能性もある。

6.1 認証精度

今実験の結果からは第 4 章で述べた認証速度の向上と外部装置で認識出来る上下の範囲超過による認証成功率低下の改善が本研究の期待通り現れている。 1 つは実行時間である。提案手法では視線に横の動きを増やすことによって、人の目が苦手とする縦の動きを削減できた結果、実行時間の短縮に繋がったのでないかと考えられる。もう一つは認証成功率である。認証成功率に関しては、提案手法の方がキャリブレーションもたやすく視線の位置も少しの誤差で済んだ。そのため、あみだくじの経路を辿る際にも的確な視線の位置情報のやり取りがされることで認証成功率の向上が出来たのではないかと考えられる。

しかし、結果からこの実験の提案手法の大元に盲点がある事も気づいた。その盲点とは、あみだくじは上から下に見ていくという風習が定着しているため、提案手法には戸惑いを抱く被験者もいた。そのため、パスアイコンを探す時間がかかり、探索時間が延びてしまったと考えられる。このことから、背景に色を付け、左を明るい色、右を暗い色へとグラデーションしていく工夫等により、人間が明るい方から見る習性などを利用する事でパスアイコンの把握が円滑化出来るのではないかと考える。また、認証成功率に関しては、認証終了点がパスアイコンと近いとパスアイコンを通り過ぎてしまい、認証終了判定がされる事があったため、アイコン配置を中央寄せして、認証終了点と認証開始点とアイコンが近くなり過ぎない配置設定が必要なのではないかと考えられる。また、少し見分けづらいアイコンがあるため、紛らわしさを排除することで認証速度、認証成功率は更に向上できると考えられる。

6.2 ユーザビリティ評価

ユーザビリティ評価はそもそも日常的に何かを視線のみで扱う事は無いに等しいため、慣れの部分は大きく関わってくるだろうと考えられる。そのためか、使いやすいかどうかも慣れの部分が大いに関係していると考えられる。また、あみだくじは通常、上から下へ向けて視線を動かす仕様であるため、説明の方も少し曖昧で把握するのに、既存手法を説明するよりか時間がかかった。そのため、仕様の分かりやすさについては既存手法に劣ると考えられる。別の横画面あみだくじ認証として、既存のあみだくじ認証を縦のままで縦線をたくさん増やすことで横に広いあみだくじ認証も考えられる。しかし、あみだくじの横線がアイコンの見にくさにより、少なくなる事によって偶然突破確率が高くなってしまう欠点がある。そのため、横に広く、上から下へ向かうあみだくじ認証を実現するには、アイコンの狭い配置による圧迫感と偶然突破確率などのセキュリティ面での側面をも考慮する必要がある。

パスアイコンの探しやすさについては、4 つのパスアイコンのうち最も認証開始点に近いパスアイコンが分かれば、認証が開始できる仕様であるため、パスアイコンをランダムで 1 つだけ左半分に表示する事でパスアイコンを探す手間と探索時間が軽減できると考えられる。その他の方法としては、パスアイコンをいくつかグループ化してアイコンの配置をグループ毎に行う事により、グループ内でのパスアイコンの探索を可能とすることで、パスアイコンの探しやすさと探索時間が改善されるのではないかと考えられる。しかし、認証に偏りを持たせることで、利用者のパスアイコン選択の単純化に伴い、他者からの攻撃の単純化が容易になり、偶然的に認証が突破される危険性が増加してしまう。

7. まとめ

提案した横画面のあみだくじ認証は、ランダムでアイコンの配置が変わるため、認証結果にもばらつきがあるが、実行時間の短縮と認証成功率の向上に期待が出来ると考えられる。今回は母数が少なく、偶然の偏りが生じている可能性もあるが、今後は、被験者を増やし、実験を行うと、更に正確な数値が出ると考えられる。また、4 つのパスアイコンのうち認証開始点に最も近いパスアイコンの行の認証開始点を見なかった時点で失敗する仕様、または、4 回以上視線の移動を行うとその時点で認証失敗となる仕様はパスアイコンの推測が他者にとって容易になるため、付け加える必要は無いと感じた。結果がまた、あみだくじという日本古来から知れ渡っている文化的背景もあり、多くの人が仕様については理解を容易に行えるが、今後は留学生の被験者も実験して結果を検討する。

参考文献

1) 宮崎　翔吾: ランダム性を持ったあみだくじ型視線認証の提案., 宮崎大学卒業論文, 2018.
2) Mohamed Khami, Malin Eiband, Martin Zurn and Heinrich Hussman: EyeSpot : Leveraging Gaze to Protect Private Text Content on Mobile Devices from Shoulder Surfing., Multimodal Technologies and Interact., 2018, 2, 45.
3) Hong-Jun Yoon, Folami Alamudun, Kathy Hudson, Garnetta Morin-Ducote and Georgia Tourassi: Deep Gaze Velocity Analysis During Mammographic Reading for Biometric, Identification of Radiologists., Published online : 1-24-2018.
4) Mohamed Khamis, Carl Oechsner, Florian Alt and Andreas Bulling: VR Pursuits : Interaction in Virtual Reality using Smooth Pursuit Eye Movements., AVI ’18, May 29-June 1, 2018, Castiglione della Pescaia, Italy, 2018.
5) Toshiya Isomoto, toshiyuki Ando, Buntarou Shizuki and Shin Takahashi: Dwell Time Reduction Technique using Fitts’ Law for Gaze-Based Target Acquisition., ETRA ’18, June 14-17, 2018, Warsaw, Poland, 2018.