

ランダム性を持ったあみだくじ型視線認証の検討

宮崎翔吾¹ 油田健太郎¹ 山場久昭¹ 朴美娘² 岡崎直宣¹

概要：現在、パスワード認証やPIN認証などは様々な場面で使用されているが、覗き見攻撃への耐性が十分ではない。視線追跡技術の向上により、覗き見攻撃に耐性を持った視線認証という認証が注目されてきている。しかしその視線認証にも認証成功率の向上や認証時間の短縮、他の攻撃への耐性などの課題が存在する。そこで本研究では、視線入力補助としてあみだくじを導入し、認証ごとに正解の入力を変化させることで視線認証の問題点を改善することを目的とした。あみだくじを用いた視線認証を実装し、認証の時間と成功率、ユーザビリティの評価を行った結果、認証総時間の平均は27.5sであり、認証成功率は74.0%であった。

A study of Amidakuji-type gaze authentication with randomness

SHOGO MIYAZAKI¹ KENTARO ABURADA¹ HISAAKI YAMABA¹ MIRANG PARK²
NAONOBU OKAZAKI¹

1. はじめに

スマートフォンやタブレットのロック画面やウェブサイトへのログイン時などに個人情報了他者に見られないために、個人を識別する様々な認証方式がある。現在、パスワード認証やPIN認証などは様々な場面で使用されているが、覗き見攻撃への耐性が十分ではない。また、指紋や虹彩などのバイオメトリクス認証は、一度盗まれると変更することができないなどの問題点がある。

近年、視線追跡技術の向上により、スマートフォンやタブレットなどのモバイル端末やコンピュータの画面のどこをユーザが見ているか判別することが容易になった[1]。そのため、ユーザの視線を追跡することでキーボード入力やタッチ入力の必要ないユーザ認証を行うことができるようになってきている。この視線追跡技術を用いた認証は、後ろから入力を覗き見る覗き見攻撃や操作した後の熱をたどるサーマルアタック、指紋などの汚れをたどるスマッジアタックなどに耐性を持っている。こういった利点がある一方、視線を用いた認証には認証成功率が低いことや認証に時間がかかること、反復攻撃や録画攻撃で破られる可能性があることなどの欠点が存在する。

そこで本研究では、視線入力補助としてあみだくじを導入することで、視線認証の問題点を改善することを目的とする。あみだくじは線を視線で辿るため、視線の動きの単純化やブレの減少が期待できる。また、一筆書きで入力が可能のため認証時間の短縮も期待でき、視線認証の入力補助としてあみだくじを用いることとした。今回提案する手法では、あみだくじの分岐点にパスアイコンを配置し、パスアイコンに沿った視線入力を行うことで個人を識別する。また、反復攻撃への耐性を持たせるために、認証ごとにパスアイコンをランダム配置するチャレンジレスポンス方式をとる。この手法を実装し、時間と成功率の評価を行う。また、アンケートによるユーザビリティの評価も行う。

2. 研究背景

2.1 認証要素

認証を行うためには、知識要素、所有要素、生体要素の3つの内いずれか1つの要素が必要である。また、これらの要素を複数組み合わせることでマルチファクタ認証と呼ばれるより強固な認証を行うことができる。知識要素とはPIN認証やパスワード認証などの本人しか知らない情報による要素を認証に用いることであり、所有要素とは身分証やセキュリティトークンなどの持っている物を要素として認証する。生体要素とは、指紋や虹彩などの人間の生体の

¹ 宮崎大学工学部

² 神奈川工科大学 情報学部

特徴を要素として用いる認証である。

2.2 認証方式

日常生活でモバイル端末やパーソナルコンピュータなどのロック解除や、個人のアカウントや銀行口座などを利用するときに認証を行うことは多い。ここでいくつかの種類の認証方式を紹介する。

2.2.1 PIN 認証

PIN 入力とは 0~9 の数字から数字の並びをあらかじめ作成しておき、認証時に入力した数字が一致すれば成功と判定される認証方式である。一般的には 4 桁の数字の並びを用いることが多く、入力の組み合わせは 10^4 通りあり、偶然突破確率は、 $1/10,000$ である。モバイル端末のロック解除や、銀行口座を利用するとなど日常生活で頻繁に使用されているが、認証動作を他人に覗き見られた場合に容易に突破されるという問題がある。

2.2.2 指紋認証

個人の生体的特徴を計測して認証に用いる手法の一つに指紋認証がある。幅広い場面に用いられており、生体認証技術の中で最も普及している認証技術である。指紋を構成している凹凸の深さや高さ、形状は千差万別であるたり、高い認証精度を誇る。認証に用いる機器のコストが比較的安価で済むが、指の状態によっては認証がうまくいかない場合がある。一度盗まれると変更することができず、指紋を偽造して突破されることがあるなど課題は残っている。

2.2.3 虹彩認証

人の虹彩には個人差があり複雑な模様であるため、偽造が困難であることから高い精度を誇った認証として使用されている。虹彩とは目の中の角膜と水晶体の間にある環状の領域のことであり、ほとんど形状が変化することがないため認証の不具合が生じにくい。虹彩認証はスマートフォンにも搭載されるようになってきたが、一定の位置や距離を保つ必要があることや日光など環境的な要因で認証が失敗すること、虹彩を盗まれて突破されることなどの問題もある。

2.2.4 ウェアラブル機器を用いた認証

スマートグラスなど特別なデバイスを経験した認証に用いることも考えられている [2]。例えば、スマートグラス上に表示される数字を見ながら PIN 認証を行うことができ、これによって覗き見攻撃に耐性を持つことができる [3]。また、スマートグラスを計測器のように扱い、人のうなずく動作でも認証を行うことができる [4]。

2.2.5 視線認証

近年、視線追跡技術が発達してきており、デスクトップのモニター等に取り付けて視線位置を測定する視線追跡装置が普及してきているため、視線の動きを用いて認証を行う視線認証と呼ばれる手法が存在する [5]。また、意識的な視線の動きだけでなく、無意識な眼球運動であるサッカー

ド運動から特徴量を測定して個人を識別し認証を行うこともできる [6]。

視線認証は認証動作を観測されにくいため覗き見攻撃やサーマルアタック、スマッジアタックなどの攻撃に強いが、認証成功率が低いことや、認証に時間がかかってしまうことなどの欠点も存在する。さらに、認証を行っている画面とユーザ自身の視線の動きを同時に覗き見や録画される攻撃で突破されることもある。

特別なデバイスを用いなくともスマートフォンの内カメラで視線位置を測定することもでき [7]、スマートフォン単体での視線認証も行われている。スマートフォン上で単純な目の動きと PIN 入力を組み合わせた認証なども行われており [8][9]、個人認証の手法の一つとして視線認証は注目されている。

2.3 想定される攻撃

2.3.1 覗き見攻撃

人々が集まる場所では、意図的でなくともモバイル端末などの画面を覗き見られ情報を盗み見られることがある [10]。モバイル端末の個人認証として現在広く用いられている PIN 認証やパターン認証などや、キーボードによるパスワードの入力は第三者に覗き見られた場合、その認証情報を盗まれやすい。その結果、容易にロックを解除されたり、不正なアクセスをうけてしまうことがある。このような正規ユーザの認証行為を覗き見することにより暗証番号やパスワードなどの認証に必要な情報を不正に取得する行為を覗き見攻撃と呼ぶ。覗き見を困難にさせること、された場合にも安全性の確保ができるようにする対策が必要であるが容易ではない [11]。

2.3.2 サーマルアタックとスマッジアタック

ユーザによる入力操作後には体温によって熱が残ってしまう。その熱の動きを追うことで入力した内容を知る攻撃をサーマルアタックと呼ぶ。他にも、入力した際に指紋などの油脂の汚れがついてしまい、その汚れの後を跡をたどられて入力を特定される攻撃方法をスマッジアタックと呼ぶ。どちらの攻撃方法も画面やキーボードの操作による入力を行わない認証では攻撃することができないため、視線認証などはこれらの攻撃に耐性を持っている。

2.3.3 録画攻撃

近年ではビデオカメラなどの録画機器を用いて認証情報を録画により取得するという録画攻撃も脅威になりつつある。録画攻撃への基本的な対策として、第三者に覗き撮られることのない環境で認証動作を行う必要があるが、我々の生活環境にはいたる所に監視カメラが設けられてきており、意図的でなくとも認証動作を録画されてしまい個人情報漏洩される可能性は否めない。

2.3.4 反復攻撃

友人や職場の同僚のような関わる頻度の高い相手から認

証画面や認証行為のどちらかを何度かずつ観測された場合、両方の観測した場面を組み合わせることで認証情報を盗む攻撃を反復攻撃と呼ぶ。例えば視線認証において、単純な動きであれば何度か認証画面と視線の動きを観測し組み合わせることで、認証情報を奪われてしまう危険性がある。

2.4 チャレンジレスポンス方式

チャレンジレスポンス方式とは、ワンタイムパスワードと呼ばれる1回限りの使い捨ての認証方式の内の一つである。この認証は、認証をしたいユーザが認証サーバ側から送られてくるチャレンジに対して、ユーザ自身の持っているパスワードを組み合わせるレスポンスとして認証サーバ側に送り返す手法であり、パスワードを直接やり取りすることなく認証できる手法である。認証サーバは自身に登録されているパスワードとチャレンジを内部で演算し、ユーザから送られてきたレスポンスと照合した結果が一致すれば、ユーザのパスワードが正しいと判断し認証を成功とする。チャレンジとレスポンスからパスワードを逆算することはできず、チャレンジは毎回変わるため、レスポンスも毎回変化する。そのため、パケットを盗聴してもパスワードは解読できず、レスポンスをコピーしてサーバへ認証しようとしても、毎回レスポンスが変わるため、認証に失敗する。

3. 関連研究

3.1 視線によるPIN認証

[5]の手法は、スクリーン上に表示された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入力を行う手法である。注視によるPIN入力は、見たものがすべて入力とされてしまうミダタッチ問題が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断された数字を入力することでミダタッチ問題の発生を抑えている。

3.2 覗き見耐性を持つあみだくじと画像の認証

人間の画像認識能力を用いた画像認証方式があるが、多くの画像認証方式は覗き見攻撃に脆弱であるため、攻撃者に認証情報が特定されないよう認証情報の入力を曖昧にする方式が提案されている。しかし、既存の方式は広い空間の中からパス画像を探し出すことが困難という問題があった。そこで[12]の手法では、常に同じ位置にパス画像とおとり画像を配置することで、ユーザの探索負荷を軽減している。そして、認証の都度変化するあみだくじを画像群上に配置することによって、パス画像を起点に毎回異なる経路を辿ってレスポンスを生成させるワンタイム性を追加し、覗き見攻撃耐性の維持を図っている。

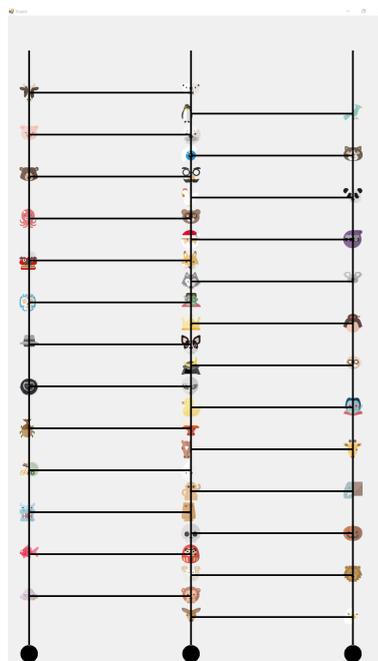


図1 認証実行画面

4. 提案手法

4.1 あみだくじの性質

日本では特定の人数から当たり・はずれを決めたり、順番を決めたりする際にあみだくじと呼ばれる方法を用いることがある。現在、形としては縦と横の直線からなるはしご上にあみだくじが一般的であり、一つの縦線の上端から線を下へと辿って行き、横線にさしかかった場合は必ず曲がる。下限までたどり着いた時点で終了となり、どの縦線を選んだ場合でも上端から下端までの経路は重複することはないという法則がある。

あみだくじは日本ではなじみのあるくじであり、知らない人でも上下左右の動きで済むため動きが単純で理解しやすい。そこでこのあみだくじを視線認証と組み合わせることで、ユーザに求められる視線の動きも単純で理解のしやすい認証の作成を目指す。それだけでなく、線を視線で辿るため視線のブレの減少や、一筆書きでの入力を行えるため一つずつ視線で数字を入力するよりも認証時間の短縮が期待できる。

4.2 アイコンの配置

単純なあみだくじの動きだけで一定の強度を持った認証を行うには、膨大な経路数を持ったあみだくじが必要であるため、実用的な大きさのあみだくじにはならない。そこで、一定の大きさのあみだくじで認証を行うため図1のようにあみだくじの分岐点にアイコンを配置する。このアイコンの中からユーザはあらかじめパスアイコンと呼ばれる分岐の目印となるアイコンを決めておき、分岐をするかど



図 2 認証準備画面

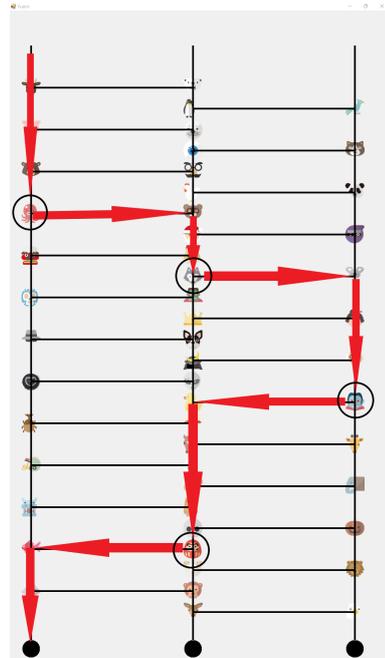


図 4 認証例



図 3 パスアイコンの例

うかで一定の大きさのあみだくじから膨大な経路数を確保する。

4.3 認証方法

事前準備として認証を行うユーザは、あらかじめ認証に用いる 52 個のアイコンの中からパスアイコンを 4 つ決めておく。通常のアミだくじとは異なり、このあみだ式視線認証ではパスアイコンにさしかかった場合のみ横線を辿る。

認証時、図 2 のようにユーザは初めにあみだが表示されていない状態で、ランダムに配置された 52 個のアイコンを確認する。このとき、ユーザは自信が指定したパスアイコンの中から一番上に存在するパスアイコンを確認する。確認後、いずれかの開始位置と呼ばれる上端の黒丸を見ることで図 1 のようにあみだが表示されるため、ユーザは指定していたパスアイコンが一番上にある縦線から線を視線で追って下へ進んで行く。このとき、パスアイコンがある分岐のみあみだのルールに従って曲がり、いずれかの縦線の下限の終了位置と呼ばれる黒丸にたどり着いた場合認証は終了する。正解経路と認証時に通った経路が一致したと判定された場合に認証を成功とする。パスアイコンが図 3 の場合の認証の動きを図 4 に示す。認証開始から開始位置を見てあみだくじが表示されるまでの時間を認証準備時間、あみだくじが表示されてから認証終了位置を見るまでを認証実行時間とする。

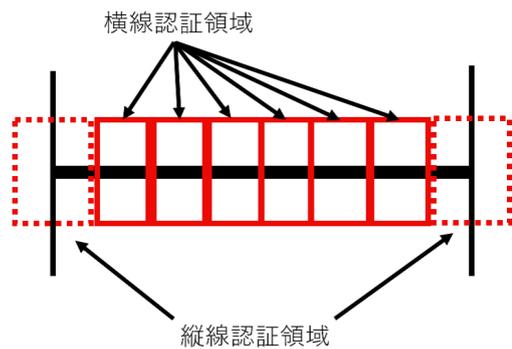


図 5 認証領域

4.4 判定方法

すべての横線に図 5 のような 2 種類の認証領域を設け、ユーザがパスアイコンが存在する横線を正しい方向に辿ったかを判定する。今回は、視線位置を 11ms ごとに一回計測し、視線位置が認証領域に含まれているかを測定する。実線で囲まれた箇所が横線認証領域であり、視線が横線認証領域を多く通過するほどその横線を見ていると判定する。また、点線で囲まれた箇所が縦線認証領域であり、横線を通るまでにどの縦線を見ているかを測定する。この縦線から縦線への移動で視線の動いた方向の判定をする。これら 2 種類の認証領域の判定を用いて、すべてのパスアイコンが含まれている横線が、正しい方向へと移動した場合に経路が一致したと判定する。

4.5 偶然突破率

PIN 認証は 0~9 の数字を 4 桁入力するため 10^4 通り選択肢があり、偶然突破確率は $1/10,000$ である。

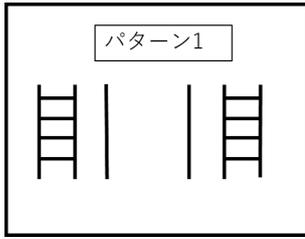


図 6 あみだくじの成立パターン 1

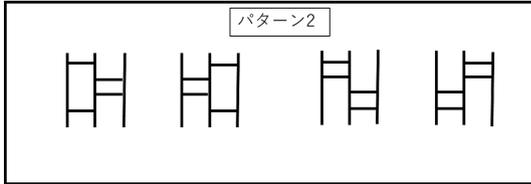


図 7 あみだくじの成立パターン 2

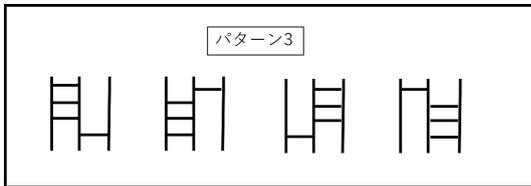


図 8 あみだくじの成立パターン 3

縦線が 2 本、横線が m 本、パスアイコンが n 個のあみだ式認証の場合の経路数は、 m 本の横線うちの n 本にパスアイコンが 1 つずつ入り、開始位置が左右どちらかの 2 パターンなので、縦線が 2 本の場合のあみだくじの経路数は $mC_2 \times 2$ となる。縦線が 2 本のときの 1 万通り前後の経路数となるあみだの横線の本数とパスアイコンの数を表 1 に示す。このように縦線 2 本では PIN 認証と同程度の 1 万通り前後の経路を確保するためには、横線の数が多くなり認証に用いるあみだが縦長になるか、パスアイコンの数が多くなるためユーザビリティに影響が出てしまう。

そこで次に、縦線 3 本、横線の総数を $2m$ (1 つの縦線間にある横線の本数は m)、パスアイコンが 4 つのときのあみだくじの経路数を計算した。このときのあみだくじが成立するパターンはおおよそ 3 パターンに分けることができ、細かく分けると図 6、図 7、図 8 のように分けられる。経路の総数はこの 3 パターンの合計であり、次のように計算することができる。

- (1) 横線が片側に 4 本ある場合

$$mC_4 \times 4$$

- (2) 横線が片側に 2 本ずつある場合 (左右交互では成立しない)

$$4 \sum_{i=2}^{m-1} iC_2(m-i)$$

- (3) 横線が片側に集中して 3 本、もう片方に 1 本存在する場合

$$4 \sum_{i=3}^{m-1} iC_3 + mC_3 \times 2$$

表 1 縦線 2 本あみだの経路数

パスアイコン数	横線の数	経路数
4	20	9,690
4	21	11,970
5	17	12,376
6	15	10,010

表 2 縦線 3 本あみだの経路数

パスアイコン数	横線の数	経路数
4	10	3,240
4	12	7,260
4	13	10,296
4	14	14,196

縦線が 3 本のときの 1 万通り前後の経路数となるあみだの横線の本数を示している表 2 より、縦線 3 本、1 つの縦線間にある横線の本数が 13 本するとき、偶然突破率が PIN 認証よりも低い $1/10,296$ という値になる。以降はこの値を用いて実装を行う。

5. 実験

この章では、提案したあみだ式認証がどれほどの有効性を示すかの評価実験を行う。評価項目は成功率とパスアイコンを探す認証探索時間、あみだを視線で辿る認証実行時間、そしてその総合的な時間を評価する。その後アンケートを行いユーザビリティについての評価を行う。

5.1 実装

提案方式を実現させるために、実装には C# 言語を用い、開発ソフトは Visual Studio 2017 を使用した。また、視線追跡のデバイスとして Tobii Eye Tracker 4C を用いてユーザの視線位置を検出した。フローチャートを図 9 に示す。

5.2 実験手順

提案手法の認証探索時間と認証実行時間、その二つの時間の合計、認証成功率を調査した。被験者として宮崎大学工学部生 10 人に実験を行ってもらった。被験者は視力矯正のための眼鏡やコト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。

実験手順としてまず被験者に実験の流れを説明し、提案手法の説明後、被験者本人のキャリブレーションを行う。その後、任意に選んだアイコンを 4 つパスアイコンとして設定し、実際に実装したシステムで本人が満足するまで練習をする。練習時には何度でもキャリブレーションをやり直すことができ、パスアイコンの記憶と探索方法の把握を意識させる。練習を終えた後に本実験を行う。本実験では提案手法の認証方式を 10 回行い、認証の成否と認証探索時間、認証実行時間を記録した。

また、本実験終了後には、提案手法の認証方式の使いや

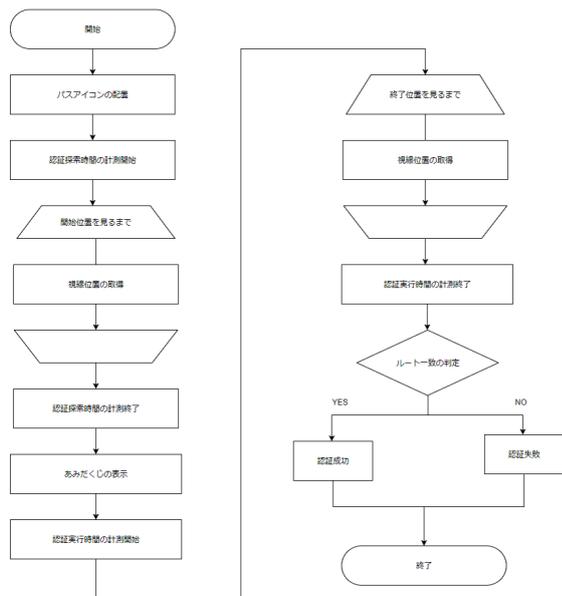


図 9 フローチャート

表 3 認証時間と認証成功率

認証準備時間 (s)	認証実行時間 (s)	認証総時間 (s)	認証成功率 (%)
12.8	14.7	27.5	74.0

すさを確認するために宮崎大学工学部生 10 人に実験の後アンケートを実施した。アンケートでは、提案手法について、以下の 7 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、意見や感想があれば記入する。

- (1) この認証を利用したいと思う。
- (2) この認証を利用するには慣れが必要であると感じた。
- (3) この認証は使いやすかった。
- (4) この認証はわかりやすかった。
- (5) この認証のアイコンの配置は見やすかった。
- (6) パスアイコンは探しやすかった。
- (7) あみだくじを視線で追うことは認証の補助になった。

5.3 結果

認証時間と認証成功率の平均の値を表 3 に示す。認証開始からあみだくじ表示までの認証準備時間の平均 12.8s であり、あみだくじの表示から認証終了までの認証実行時間は平均 14.7s であった。また、それらを合わせた認証総時間の平均は 27.5s であり、平均認証成功率は 74.0 % であった。

そして、ユーザビリティ評価のアンケート結果は図 10 となっている。(1), (2), (4), (7) の項目では否定的な回答は少なかったが、アイコンに関する (5), (6) の項目では、肯定的な回答が少なかった。(3) の項目については、肯定的な回答と否定的な回答は同程度であった。意見として、認証ごとに精度にばらつきがあるように感じられたこと、パスアイコンの配置に工夫が必要であること等が挙げられた。

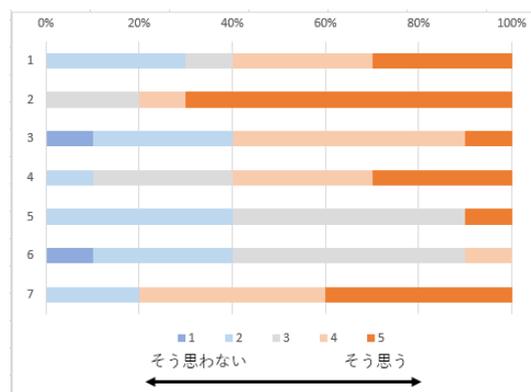


図 10 アンケート結果

6. 考察

今回の提案手法での認証成功率は 74.0 % であった。元々視線追跡装置を使用したことのある被験者や、練習時間が長かった被験者の成功率が高く、アンケート (2) の結果が示すように、この認証には慣れが必要であることが分かった。また、精度のばらつきについては、画面上部分のキャリブレーション時にずれが発生すること、被験者の数名が頭部の動きによるずれを感じたことからあみだくじが縦長であったことが原因ではないかと考えられる。よって、あみだくじを横長にするために縦線を増やし練習時間やキャリブレーション時間を多くとることで、認証成功率を上昇させることができる。そして、アンケート (7) の評価も高く、認証実行時間は長くないため、視線認証にあみだくじを用いることは入力補助になると考えられる。

一方、パスアイコンについては肯定的な意見が少なく、ランダム配置により認証探索時間が発生することもあり、より工夫が必要であることが分かった。したがって、今後の課題として、パスアイコンの単純化による認識負担を低下させることや、チャレンジレスポンス方式としたことによる録画攻撃や、反復攻撃に対する耐性を調査することが挙げられる。

7. まとめ

本研究では、覗き見攻撃に耐性を持っている視線認証に着目し、視線認証の欠点とそれに対する解決案を考えた。その結果、入力の動きを補助するためにあみだくじを用いる手法を提案した。この手法では、ユーザが毎回ランダムに表示されるパスアイコンに沿って視線を動かすことで、正しいあみだくじの経路をたどることができるか判断し認証する。提案手法を実装し認証時間、認証成功率、ユーザビリティについて評価を行った結果、あみだくじは視線認証の補助になるがパスアイコンの工夫が必要であることが分かった。

今後の課題として、パスアイコンやあみだくじを改良しユーザビリティと成功率を向上させること、録画攻撃と反復

攻撃に対する耐性の調査が挙げられる。

謝辞 本研究は JSPS 科研費 JP17H01736, JP17K00139, JP18K11268 の助成を受けたものです。

性を有する画像認証方式に関する一検討” 研究報告マルチメディア通信と分散処理 (DPS) 2009, pp.91-96, 2009.

参考文献

- [1] E. Miluzzo, T. Wang, A. T. Campbell, and a. C. M. S. I. G. o. D. Communication. “EyePhone: Activating Mobile Phones with Your Eyes.” Workshop on Networking, Systems, and Applications on Mobile Handhelds (MobiHeld), pp.15-20, 2010.
- [2] Buti Al Delail, Chan Yeob Yeun, “Recent Advances of Smart Glass Application Security and Privacy ” , Internet Technology and Secured Transactions (ICITST), pp.65-69, 2015.
- [3] Christian Winkler, Jan Gugenheimer, Alexander DeLuca, Gabriel Haas, Philipp Speidel, David Dobbstein, Enrico Rukzio, “Glass Unlock: Enhancing Security of Smartphone Unlocking through Leveraging a Private Near-eye Display ” , CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp.1407-1410, 2015.
- [4] Sugang Li, Ashwin Ashok, Yanyong Zhang, Chenren Xu, Janne Lindqvist, Macro Gruteser, “Whose Move is it Anyway? Authenticating Smart Wearable Devices Using Unique Head Movement Patterns ” , 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp.1-9, 2016
- [5] Mythreya Seetharama, Volker Paelke, and Carsten Rucker, “SafetyPIN: Secure PIN Entry Through Eye Tracking” , HAS(Human Aspects of Information Security, Privacy, and Trust) 2015, pp.426-435 , 2015.
- [6] Ivo Služanović, Marc Roeschlin, Kasper B. Rasmussen, Ivan Martinović, “Using Reflexive Eye Movements for Fast Challenge-Response Authentication ” , CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp.1056-1067, 2016.
- [7] Kyle Krafka, Aditya Khosla, Petr Kellnhofer, Harini Kannan, Suchendra Bhandarkar, Wojciech Matusik, Antonio Torralba, “Eye Tracking for Everyone” , Computer Vision and Pattern Recognition (CVPR), 2016 IEEE Conference on , 2016.
- [8] Mohamed Khamis, Mariam Hassib, Emanuelvon Zeischwitz, Andreas Bulling, Florian Alt “Gaze-TouchPIN: Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication” , ICMI 2017 Proceedings of the 19th ACM International Conference on Multimodal Interaction, pp.446-450 , 2017.
- [9] Mohamed Khamis, Regina Hasholzner, Andreas Bulling, Florian Alt “GTmoPass: Two-factor Authentication on Public Displays Using Gaze-Touch passwords and Personal Mobile Devices” PerDis '17 Proceedings of the 6th ACM International Symposium on Pervasive Displays Article No. 8 , 2017.
- [10] Malin Eiband, Mohamed Khamis, Emanuelvon Zeischwitz, Heinrich Hussmann, Florian Alt “Understanding Shoulder Surfing in the Wild: Stories from Users and Observers”, CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems Pages pp.4254-4265 , 2017.
- [11] 和斉薫, “モバイル端末向け個人方式における柔軟な安全性強度の実現手法に関する研究”, 宮崎大学大学院修士論文 (2015)
- [12] 小島 悠子, 山本 匠, 西垣 正勝, “覗き見攻撃耐性と利便