視線の特徴量を用いたあみだくじ型視線認証

宮崎　翔吾 [a)]・國房　弘夢 [b)]・油田　健太郎 [c)]・山場　久昭 [d)]・岡崎　直宣 [e)]

Amidakuji-type Gaze Authentication Using Gaze Features

Shogo MIYAZAKI, Hiromu KUNIFUSA, Kentaro ABURADA, Hisaaki YAMABA, Naonobu OKAZAKI

Abstract

Electronic terminals such as smartphones and personal computers are exploding, and require personal authentication to determine whether the user who is using the terminal is himself or herself to prevent spoofing and unauthorized access Opportunities are increasing. For personal authentication, authentication based on storage of a password or a password or authentication using a tool such as an IC card or a face photograph is often used. However, in the case of a method in which the password is directly input with a button or a finger, the password may be known to a third party by peeping. In addition, biometrics authentication using biometric information such as behavioral characteristics of an individual has been actively studied in personal authentication, and features (individual habits) appearing in handwriting, gait, trajectories of eyes, etc. are used for authentication. These behavioral features have the advantage that they are less likely to be duplicated, and may be used in conjunction with other authentication methods. In this paper, we focus on authentication using behavioral characteristics of individuals, create two-factor authentication based on personal identification using features extracted from gaze data, based on preliminary research using Amidakuji, and verify authentication time and authentication precision. An experiment to verify the success rate was described. It was suggested that both the authentication time and the authentication success rate improved, and that the identity could be identified with an accuracy of 80% or more.

Keywords: gaze authentication, eye tracking, gaze features, SVM, shoulder surfing

1. はじめに

今日、スマートフォンやパソコンなどの電子端末は爆発的な普及を見せている。その中で、なりすましや不正アクセスを防止するために、端末を利用しているユーザが本人であるかどうかを判別するための個人認証を必要とする機会が増加している。

個人認証にはパスワードや暗証番号などの記憶に基づく認証や、IC カードや顔写真など道具を用いた認証が多く用いられている。しかし、パスワード認証はブルートフォース攻撃などで破られてしまう可能性がある。こういった攻撃の対策としてパスワードを長くする、記号を織り交ぜたパスワードにするなどが挙げられるが、複雑なパスワードになると記憶しておくのが難しいという問題が発生する。また、パスワードをボタンや指で直接入力する方式の場合、覗き見によって第三者にパスワードを知られてしまう場合がある。道具を用いた認証は紛失・盗難の恐れがある。悪意のあるユーザに盗難された場合はなりすましが容易に行われてしまう。

身体的、行動的特徴といった個人の生体情報を用いたバイオメトリクス認証 [1] も盛んに研究されている。

身体的な特徴には指紋や網膜パターンなどがある。身体的特徴を用いた認証は、パスワードを覚えておく必要もなく、怪我や病気による欠損を除けば紛失の恐れもない。しかし、そういった身体的特徴は万が一複製・盗難されると変更が困難であるという欠点がある。

一方で行動的特徴は、筆跡や歩容、視線の軌跡などに現れる特徴（個人の癖）を認証に用いる。こういった行動的特徴は複製されにくいという利点があり、また、他の認証方法と併用できる可能性がある。

本稿では、個人の行動的特徴を用いた認証に着目し、あみだくじを用いた事前研究 [2] を元に、視線データから抽出した特徴量を適用した本人判別による 2 要素認証を作成し、認証時間や認証成功率を検証する実験について述べる。以下、本概要の構成を述べる。第 2 章では既存の関連研究について述べ、第 3 章では提案手法について述べる。第 4 章では認証精度に関する評価実験および攻撃耐性について述べ、第 5 章ではまとめと今後の課題について述べる。

2. 関連研究

2.1 視線の軌跡情報からの特徴抽出

視線の特徴量に関する研究として関連研究 [3] があげられる。空中に視線で文字を描き、その軌跡に含まれる特徴量を用いてユーザの分類を行っている。認証に際し、刺激に対する視覚の反応を用いていないので機器特性に依存しない。論文の中で、著者は特徴量を用いた認証が他の認証と併用でき

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

図 1. あみだくじ型視線認証の認証画面

図 2. パスアイコン

る可能性に言及している。本稿ではこの研究を参考に特徴量を選択した。

2.2 あみだくじ型視線認証

視線の軌跡を用いた認証として、あみだくじを用いた視線認証 [2] がある。図 1 は、認証画面である。この認証は 4 個のパスアイコン 2 と 48 個の囮アイコンの計 52 個のアイコンから構成されている。視線であみだくじを上から辿っていきパスアイコンが配置されているところで右か左に視線を移す。これを認証終了位置に来るまで繰り返し、全てのパスアイコンを通過していれば認証成功となる。

また、この認証はチャレンジレスポンス方式をとっており、認証の度にアイコンの配置がランダムに変わり、毎回違う画面が表示されるワンタイム性をもっている。それによってパケットを盗聴してレスポンスをコピーする攻撃や、覗き見攻撃に耐性を持たせている。

3. 提案手法

3.1 特徴量を用いたあみだくじ型視線認証

あみだくじ型視線認証 [2] を元に、アイコンの総数を減らし、アイコン探索時間の向上と、横線の間隔が広がることによる成功率の増加を図る。あみだくじ型視線認証における経路数は表 1 の通りである。アイコンを減らすことで経路数が減少し、偶然突破率が上がってしまうため、視線の軌跡情報の特徴量を用いた本人判別を導入し、パスアイコンと特徴量の 2 要素認証とすることで、攻撃耐性が維持されることを期待する。認証時にパスアイコンを通ったかどうかに用いる視線データから有用と思われる特徴量を抽出し、学習器を作成して分類を行う。また、あみだくじを通るときだけでなくアイコンを探索する際の視線の動きにも特徴があるのではないかと考え、認証中だけでなく探索中の視線も取得した。認証時や探索時の視線データをそのまま用いることで、特徴量の取得のため

表 1. あみだくじの経路数

パスアイコン [個]	横線 [本]	アイコン総数	経路数
4	14	56	14,196
4	13	52	10,296
4	12	48	7,260
4	10	40	3,240

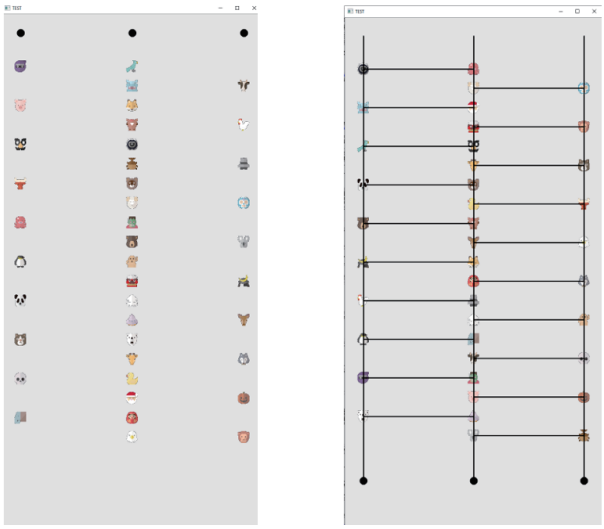

図 3. 認証画面

新たな手順を追加する必要がないという利点がある。

認証の流れを詳しく説明する。認証を開始すると、36 個の囮アイコンと 4 個のパスアイコンの計 40 個のアイコンが表示された図 3 の左の探索画面が表示される。この 40 個のアイコンの中からパスアイコンを探し、最も上に配置されているパスアイコンの列の上部にある認証開始点（黒丸）を見ることであみだくじが生成され、図 3 の右画面に切り替わる。最も上にあるパスアイコンの列から、あみだくじに沿って視線を下に移していき、パスアイコンを見つけた位置であみだくじの要領で横に視線を移す。これを下部にある認証終了点の黒丸に到達するまで行い、認証終了となる。認証終了時に正解のパスアイコンをすべて通っていれば認証成功となる。パスアイコンを探し、認証開始点を見るまでを探索とし、あみだくじが生成され、認証終了点を見るまでを実行と定義する。また探索開始から終了までの時間を計測して探索時間とし、同様に実行開始から終了までの時間を実行時間とする。探索時間と実行時間を合計したものを認証時間とする。

3.2 特徴量の抽出

取得した視線データから特徴量を抽出する。選択する特徴量は関連研究 [3] を参考に、認証時の視線の軌跡情報の x 座標、y 座標、平均速度、速度の標準偏差、認証時間、瞳孔径、瞬目速度とした。

以下に具体的な抽出方法を示す。

軌跡形状: 描いた軌跡に特徴が表れる考え、被験者から取得した実行時の視線データを 30 分割し、各区間の x 座標、y 座標の平均座標を用いてそれぞれ 30 次元の特徴量とした。

速度: 人によって視線を動かす速度が異なると考え、座標間の距離を速度と定義して、分割データの各区間における平均速度を求め。30 次元の特徴量とした。また、区間ごとの速度だけでなく全体の視線速度にも特徴があると考え、分割して

いない視線データ全体の速度と標準偏差を 4 次元の特徴量とした。

瞳孔径: 人は集中している状態で瞳孔径が変化する [4] ため、そこに個人差があるのではないかと考え、探索時と実行時の瞳孔径の平均を取得し 2 次元の特徴量とした。

瞬目速度: 人によって瞬目速度が違うのではないかと考え、目を閉じて視線データが取得できなくなった時点から再び取得が開始された時点までの差を瞬目速度と定義して、その平均値を 1 次元の特徴量とした。

認証時間 人によって認証時間に差があるのではないかと考え、探索開始から終了までの時間、および実行開始から終了までの時間を取得し、2 次元の特徴量とした。

以上、計 99 次元の特徴量を用いて特徴量を使用して SVM[5] により学習器を作成した。

3.3 特徴量の選別

学習器を作成する際に、本人判別の妨げとなるような特徴量が含まれていると判別精度に悪影響が出てしまうため、特徴量の選別を行った。本人判別に適した特徴量を選ぶ方法の一つに、変数減少法（Backward stepwise selection[6]）がある。

本稿では、認証の本人判別に有効な特徴量を選ぶために、この手法を用いることとする。まず抽出した特徴量を全て用いた学習器を作成し、そこから 1 つの特徴量を取り除き精度を比較する。もし精度が向上すればその特徴量は削除する。この Backward stepwise selection をすべての特徴量に適用して、特徴量を選別する。

4. 実験

提案手法の認証精度を評価するために実験を行った。

4.1 実装

実装は python を用いて行った。視線データの取得は外部装置である Tobii Eye Tracker 4C を使用した。

4.2 認証精度に関する評価実験

4.2.1 実験の目的と内容

あみだくじ型視線認証の既存手法と提案手法の認証精度の変化と、特徴量の導入の効果を調査した。被験者として、宮崎大学工学部に所属する学生 4 名に実験を行ってもらった。眼鏡やコンタクトレンズの有無は任意とし、目に疲労を感じた場合は休憩を自由に取ることできる。

実験の手順を以下に示す。

(1) 実験方法の説明

あみだくじ型視線認証の認証方法について説明し、40 種類のアイコンから好きなアイコンを選んでもらいパスアイコンとした。

(2) 練習

各被験者が十分と判断するまで練習を行ってもらった。練習中に視線位置がズレていると感じたとき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こととした。

(3) 認証

既存手法を 10 回行った後に、提案手法の認証を 20 回行ってもらった。

表 2. 既存手法の認証時間と認証成功率

探索時間 [s]	4.2
実行時間 [s]	11.1
認証時間 [s]	15.2
認証成功率 [%]	40.0

(4) 学習器の作成

提案手法の認証を行った際の視線データから 3.2 節で示した特徴量の抽出を行った。抽出した特徴量を用いてデータセットを作成し、各次元において平均が 0、分散が 1 となるように標準化を行った。作成したデータセットの前半の 10 回分を学習データとして学習器の生成を行い、後半の 10 回分をテストデータとして本人判別を行った。

(5) 特徴量の選別

3.3 節の方法で使用する特徴量を選定した。その結果、99 次元の特徴量のうち、認証時間、探索速度平均、実行速度の平均と標準偏差、瞬目速度、探索時瞳孔径、認証時瞳孔径、計 7 次元の特徴量が有意であった。

4.2.2 結果と考察

認証精度について、探索時間と実行時間、認証時間、および認証成功率の値を、既存手法の結果を表 2、提案手法の結果を表 3 にまとめた。既存手法と比較して、探索時間は 4.2s から 3.5s へと低下し、アイコン数を減らしたことの効果が期待通りに現れている。同時に認証成功率も上昇している。横線の数が減ったことに伴って既存手法よりもアイコンの間隔に余裕があり、パスアイコンの誤認証が減少したためと考えられる。既存手法と比較して認証成功率は向上を見せたものの、成功率自体が低くなっている。この理由のひとつとして、ユーザの意図と違った位置にポイントが入力されてしまう Midas Touch 問題 [7] が考えられる。

次に、SVM による識別結果について議論する。識別結果を表 4、表 5 に示す。ACC. は被験者毎の判別精度である。どの被験者も 80%以上の精度で本人判別ができており、全被験者の判別精度は 92.5%となった。表 3 の実質成功率とは、本人判別の成功率を考慮し、認証成功率に判別精度をかけた確率であるが、こちらも 53.2.%と既存手法を上回っている。

特徴量の厳選の結果を表 6 に示す。3.2 節で示した 99 次元の特徴量のうち、認証時間、探索速度平均、実行速度の平均と標準偏差、瞬目速度、探索時瞳孔径、認証時瞳孔径、計 7 次元の特徴量が有意であった。本人判別において、軌跡形状（x 座標、y 座標）や区間ごとの速度といった特徴量が有効に働かなかったのは、生成されるあみだくじがランダム性を持っているため、毎回の認証で描く軌跡が異なり、座標による分類が出来なかったのではないかと考えられる。

また、実験の際にヒアリングを行ったところ、続けて認証を行うことによる疲労を感じたという声があった。そのため、実験前半と後半では視線の動かし方に違いが出ている可能性がある。

表 3. 提案手法の認証時間と認証成功率

探索時間 [s]	3.5
実行時間 [s]	9.8
認証時間 [s]	13.3
認証成功率 [%]	57.5
実質成功率 [%]	53.2

表 4. 識別結果

	正解				
被験者	A	B	C	D	ACC.
A	10	0	0	0	1.00
B	1	8	0	1	0.80
C	0	0	10	0	1.00
D	0	1	0	9	0.90

表 5. 識別精度

	precision	recall	f1-score	FAR
A	0.91	1.00	0.95	0.03
B	0.89	0.80	0.84	0.03
C	1.00	1.00	1.00	0
D	0.90	0.90	0.90	0.13

表 6. 特徴量選定結果

特徴量選択前		特徴量選択後	
特徴量数 [次元]	F 値	特徴量数 [次元]	F 値
99	0.43	7	0.92

4.3 攻撃耐性に関する実験

4.3.1 実験の目的と内容

あるユーザのパスアイコンを知っている攻撃者が、そのユーザになりすまして認証を行った場合に、特徴量の判別によって本人ではないと判別できるかの実験を行う。

攻撃者のデータが学習器を構成している学習データに含まれていることを避けるため、実験 4.2 に参加していない 1 名の被験者に実験を行ってもらった。利用者のパスアイコンを使って認証を行ってもらい、実験 4.2 で作成した学習器を用いて本人判別率を調査する。実験 4.2 と同じように、キャリブレーションと練習を行ってもらった後に、提案手法の認証を 10 回を行い、取得した視線データをテストデータとして、本人判別を行う。

4.3.2 結果と考察

それぞれのユーザに成りすました場合の判別結果を表 7 に示す。攻撃者の判別精度の平均値は 0.25 となっている。また、表 5 の FAR は他人受入率 (False Acceptance Rate) であるが、その平均値は 0.048 となっている。攻撃成功率を判別率と他人受入率の合計と定義すると、攻撃成功率の値は 0.298 となる。表 1 に示した通り、提案手法の経路数は 3,240 であり、すなわち偶然突破率は 1/3,240 である。これに攻撃成功率を掛け合わせると 1/10,872 となり、既存手法の経路数 1/10,296 よりも低く、攻撃耐性は維持されていると考えられる。

表 7. 攻撃者の判別結果

攻撃対象	ACC.
A	0
B	0
C	0.70
D	0.3

5. まとめ

本論文では、既存のあみだくじ型視線認証に視線軌跡の特徴量による本人判別を導入し、認証精度と本人判別精度について検証を行った。認証精度は認証時間、認証成功率ともに向上し、本人判別も 80%以上の精度で判別できることが示唆された。

提案手法のように、認証毎に描く軌跡が異なる場合においては、描く軌跡の形状に左右される特徴量ではなく、速度平均や認証時間といった特徴量が判別精度に寄与していることが分かった。ただし、今回はサンプル数が少ないため、人数を増やすと判別の成功率が変化する可能性がある。また、視線の動かし方は目の疲れや慣れに左右されることを考えると、期間を空けて再度認証を行った場合、違った結果になる可能性がある。

今後の課題として、抽出する特徴量の見直しが挙げられる。例えば、マイクロサッカードと呼ばれる眼球の不随意運動が存在する [8] が、このマイクロサッカードは注意の影響を受けることが指摘されている [9] ため、個人を判別する特徴量として有用な可能性がある。

あみだくじ型視線認証の改良としては、アイコンのグループ化による探索時間の向上などがあげられる。

参考文献

1) 篠原　克幸： バイオメトリック認証, 画像電子学会誌, 第 37 巻, 2008.

2) 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.

3) 向井　寛人, 小川　剛史： 個人認証を目的とした視線の軌跡情報からの特徴抽出, 情報処理学会論文誌, Vol.4, pp.27-35, 2016.

4) 丹下　雄太, 中澤　篤志, 西田　豊明： 人の内部状態と瞳孔径の定量的関係, 第 77 回全国大会講演論文集, pp.413-414, 2015.

5) Chih-Chung Chang, and Chih-Jen Lin: LIBSVM: A library for support vector machines, ACM Transactions on Intelligent Systems and Technology (TIST), Vol. 2, 2011.

6) Guyon, I. and Elisseeff, A: An introduction to variable and feature selection, The Journal of Machine Learning Research, Vol. 3, pp.1157–1182, 2003.

7) Jacob, R. J. K.: What you look at is what you get:Eyemovement-based interaction technique, Proceedings of ACM CHI ’90, pp11-18, 1990.

8) Dodge, R.: An experimental study of visual fixation, Psychological Monograph Supplement, Vol.8, 1907.

9) R. Engbert and R. Kliegl: Microsaccades uncover the orientation of covert attention, Vision Research, Vol.43, pp.1035–1045, 2003.