修士論文

視線軌跡を用いた個人認証

公立はこだて未来大学大学院　システム情報科学研究科
情報アーキテクチャ領域

藤本　巧海

指導教員　　白石　陽

提出日　2021 年 2 月 15 日

Master's Thesis

Personal Authentication Based on Eye Movement Trajectory

by

Takumi FUJIMOTO

Graduate School of Systems Information Science, Future University Hakodate
Media Architecture Field
Supervisor Prof: Yoh SHIRAISHI

Submitted on February 15, 2021

Abstract

In recent years, mobile terminals such as laptops, smartphones, and tablets have become popular. Many users perform personal authentication on web services, applications, and online shopping. A variety of information is shared by mobile terminals. If the authentication information is leaked, there is a risk of it being used fraudulently. Therefore, it is important to improve the security of authentication in mobile terminals.

Password authentication and biometric authentication are popular means of personal authentication, and are also used for authentication on mobile terminals. One of the weaknesses of knowledge authentication is the leakage of authentication information can be leaked when someone looks over another person's shoulder in a public space such as train stations and cafes. One of the weaknesses of biometric authentication is that it is difficult to prevent identity theft by forging authentication information such as fingerprints, face, and iris. The information cannot be intentionally changed, it is difficult to deal with impersonation. In order to solve these weaknesses of authentication, this study focused on eye movement. Eye movements are considered to be highly robust against to look over another person's shoulder because it is difficult for others to observe. In addition, eye movements can be reproduced intentionally by the user, the authentication information can be changed. We think that it is difficult to guess the authentication information if the user himself defines the eye movement used as the authentication information.

In this thesis, this study proposes a personal authentication method using a personal authentication based on eye movement trajectory, that is the trajectory drawn by trajectory drawn by the user's eye movement. The proposed method uses the trajectory defined by the user. The proposed method consists of two parts: (1) authentication based on the shape of the gaze trajectory and (2) authentication based on the drawing characteristics of the gaze trajectory. As the features used for authentication based on the shape of the eye movement trajectory, this study focused on the amount of change in the coordinate group data which is recorded in chronological order of the x and y coordinates when the eye movement trajectory is drawn. As the features used for authentication by drawing features, this study focused on the features that can be extracted from the eye movement (fixation and saccade). In addition, we use an error detection algorithm as the learning algorithm for the proposed method. Error detection is a method that learns only normal data and identifies unknown data as normal or error. The proposed method does not use other people's input data for learning because it is intended to be applied to mobile terminals owned by an individual. Therefore, we think that the error detection algorithm is an effective learning algorithm for the proposed method.

The proposed method performed trajectory identification using features extracted from the coordinates data and an error detection algorithm to evaluate the accuracy of authentication based on the shape of the eye movement trajectory. The F-measure, FAR, and FRR of the One Class SVM are 0.87, 0.001, and 0.22. The F-measure, FAR, and FRR of the Isolation Forest are 0.68, 0.031, and 0.33. The F-measure, FAR, and FRR of Isolation Forest were 0.68, 0.031, and 0.33. The proposed method performed personal identification using fixation and saccade features and an error detection algorithm to evaluate the accuracy of authentication based on drawing features. The experimental results suggested that fixation and saccade features and Isolation Forest are effective. In order to improve the accuracy, the proposed method performed personal identification using the training data which was augmented with SMOTE, and Isolation Forest. In addition, a drawing guide was displayed during inputting data. As a result, the F-measure, FAR, and FRR were 0.92, 0.03, and 0.04.

Keywords: Personal Authentication, Eye Movement Trajectory, Shape Identification, Personal Identification, Error Detection

概要

近年，ノートパソコンやスマートフォン，タブレットなどのモバイル端末が普及している．端末のロック解除，Web サービスやアプリケーションへのログイン，ネットショッピングでの購入手続きなど多くのユーザがモバイル端末による個人認証を行っている．様々な情報がモバイル端末経由で共有されているため，認証情報が漏洩するとなりすましによる様々な被害に遭うことが考えられる．したがって，モバイル端末における認証の安全性を向上させることが重要である．

モバイル端末に用いられている認証方式として，知識認証とバイオメトリクス認証が用いられている．知識認証の脆弱性として，駅やカフェなどの公共空間において他者の覗き見による認証情報の漏洩が挙げられる．また，バイオメトリクス認証の脆弱性として，認証情報である指紋や顔，虹彩などの情報の偽造による，なりすましへの対処が困難であることが挙げられる．これらの情報は意図的に変更することができないため，偽造された場合の対処が困難である．これらの認証の脆弱性を解決するために，本研究では，視線移動に着目する．視線移動は他者が観測することが困難であり，覗き見に対する頑健性が高いと考える．また，視線移動はユーザが意図的に再現できるため，認証情報として利用することで，認証情報の変更も可能である．認証情報として用いる視線移動をユーザ自身が定義することで認証情報の推測が困難になると考える．

本研究では，ユーザがモバイル端末の画面上に視線で描画した軌跡である，視線軌跡を用いた個人認証手法を提案する．提案手法で用いる視線軌跡はユーザ自身が定義した軌跡を用いる．提案手法は，入力された視線軌跡の形状による認証と視線で描画した際の個人の特徴である描画特徴による認証から構成される．視線軌跡の形状による認証に用いる特徴量として，描画した視線軌跡の画面の座標が時系列順で記録されたデータである座標群データの変化量を用いる．描画特徴による認証に用いる特徴量として，視線運動である注視とサッケードから抽出できる特徴量を用いる．また，提案手法の認証に用いる学習アルゴリズムとして異常検知アルゴリズムを用いる．異常検知とは，正常なデータのみを学習し未知のデータを正常か異常か識別する手法である．提案手法は個人が保有するモバイル端末に適用することを想定しているため，他人の入力したデータを学習に用いない．よって異常検知アルゴリズムが提案手法の学習アルゴリズムとして有効であると考える．

視線軌跡の形状による認証の精度評価のために，異常検知アルゴリズムを用いて座標群データから抽出した特徴量による軌跡識別を行った．結果として，One Class SVM を用いた場合の F-measure が 0.87，FAR が 0.001，FRR が 0.22 となった．Isolation Forest を用いた場合の F-measure が 0.68，FAR が 0.031，FRR が 0.33 となった．実験結果から，視線軌跡の形状による認証に用いる特徴量として座標群データ，学習アルゴリズムとして One Class SVM が有効であることが示唆された．描画特徴による認証の精度評価のために，異常検知アルゴリズムを用いて注視とサッケードによる個人識別を行った．実験結果から，描画特徴による認証に用いる特徴量として注視とサッケードから抽出した特徴量，学習アルゴリズムとして Isolation Forest が有効であることが示唆された．精度向上のために学習データを SMOTE により水増しして，Isolation Forest を用いた個人識別を行った．また，データ収集の際に描画ガイドを表示した．結果として，F-measure が 0.92，FAR が 0.03，FRR が 0.04 となった．提案手法において，学習データの水増しと，視線軌跡描画時にガイドを表示することにより精度向上が見られた．

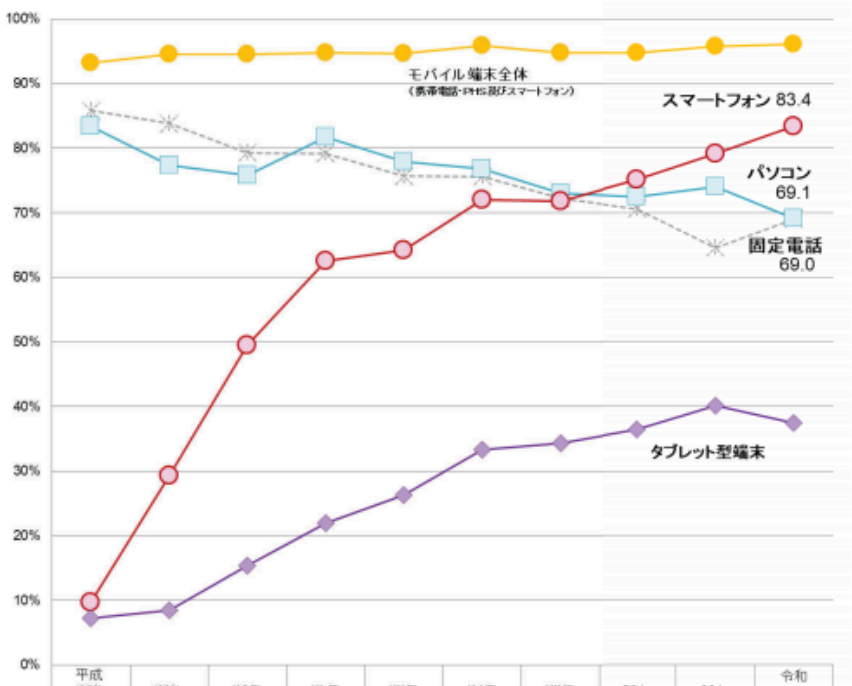
キーワード: 個人認証，視線軌跡，形状識別，個人識別，異常検知

目次

第1章　序論

1.1　背景

近年，スマートフォンやタブレットなどのモバイル端末が普及し，保有率が増加している[1]．モバイル端末による SNS などのサービスの利用者もまた年々増加している．SNS や Web サービスへログインするためにはパスワードの入力が必須となる．また，パスワードやパターン，顔認証を用いた端末のロック機能の利用率も増加している．このようにモバイル端末を用いて多くの人がサービスへのログインや端末のロック解除の際に個人認証を行う機会が増加している．



	平成22年 (n＝22,271)	23年 (n＝16,530)	24年 (n=20,418)	25年 (n=15,599)	26年 (n=16,529)	27年 (n=14,765)	28年 (n=17,040)	29年 (n=16,117)	30年 (n=16,255)	令和元年 (n=15,410)
固定電話	85.8	83.8	79.3	79.1	75.7	75.6	72.2	70.6	64.5	69.0
パソコン	83.4	77.4	75.8	81.7	78.0	76.8	73.0	72.5	74.0	69.1
スマートフォン	9.7	29.3	49.5	62.6	64.2	72.0	71.8	75.1	79.2	83.4
モバイル端末全体	93.2	94.5	94.5	94.8	94.6	95.8	94.7	94.8	95.7	96.1
タブレット型端末	7.2	8.5	15.3	21.9	26.3	33.3	34.4	36.4	40.1	37.4

図 1 情報通信機器の保有状況の推移（文献[1]より引用）

Fig. 1 Transition of ownership rate of information and communication equipment

モバイル端末に用いられている個人認証方式として，知識認証やバイオメトリクス認証が普及している．知識認証とは，パスワードや暗証番号などの本人のみが保有する知識を認証情報とした認証方式である．知識認証は，IC カードや鍵などの所有物を認証情報として用いていないため，認証情報を紛失することはない．しかし，駅やカフェなどの公共空間において，パスワードなどの認証情報を入力する際に覗き見される可能性がある．覗き見は攻撃者が専門的な知識を習得していなくても可能なハッキング行為である．そのため，知識認証の認証情報は誰に対しても漏洩する可能性がある．また，知識認証の認証情報は入力桁数が少ないと認証情報を推測される恐れがある．バイオメトリクス認証とは，身体の一部（身体的特徴）や人間の行動（行動的特徴）を認証情報として用いた認証方式である．身体的特徴とは，指紋や顔などの固有性が高い

身体の部位を示す．また行動的特徴とは，人間が持つ様々な行動の癖やパターンであり，本人であれば再現可能な特徴を示す. バイオメトリクス認証は, 他者からの覗き見に対して頑健であり，認証情報を記憶する負担が少ない．しかし，身体的特徴を用いた認証では，認証情報として登録している身体的特徴が偽造されるリスクがある．また，認証に使用する指紋や虹彩などの身体的特徴は意識的に変更することができないため，認証情報を偽造された場合の対処が困難である．一方で，手の動きや歩行などの行動的特徴を認証に用いた場合，身体の一部を認証情報として用いていないため，認証情報の偽造が困難である．しかし，人の無意識な癖などを認証情報として扱う場合には，人が認証情報を意識的に変更することは困難である．よって，バイオメトリクス認証は，なりすましの被害に遭った際に対処が困難になることが考えられる．

モバイル端末で安心して認証を行うためには，知識認証の脆弱性である覗き見により認証情報が漏洩すること，バイオメトリクス認証の脆弱性である認証情報が偽造された場合，認証情報の変更が困難であるため，なりすましへの対処が困難であることを解決することが必要である．個人認証の脆弱性を解決することを目的とした，知識認証に関する研究[2], [3], [4], [5], [6], [7]やバイオメトリクス認証に関する研究[12], [13], [14], [15], [16], [17]が盛んに行われている．また，覗き見に対して頑健な行動的特徴を認証に用いた研究として視線移動を認証に用いた研究がある[18], [20], [19], [21], [22]．視線移動は腕の動きや脚の動きなどの行動的特徴とは異なり，他者が観測することが困難であり，覗き見に対する頑健性が高いと考える．また，視線移動は人が意識的に再現できるため，認証情報に用いる視線移動を変化させることで，認証情報の変更が可能になり，なりすましへの対処が可能である．よって，個人認証の脆弱性を解決するために，視線移動を用いることが有効であると考える．

1.2 本研究の目的と目標

モバイル端末で安心して認証を行うために知識認証やバイオメトリクス認証の脆弱性である（1）覗き見により認証情報が漏洩すること，（2）認証情報が他者に推測されること，（3）認証情報の変更が困難であることを解決することが必要であると考える．

そこで本研究では，ユーザがモバイル端末の画面上に視線で描画した軌跡（視線軌跡）に着目し，知識認証やバイオメトリクス認証の脆弱性を解決する個人認証システムを実現することを目的とする．視線軌跡は視線移動の情報を用いるため，他者からの認証情報の入力の覗き見に対して頑健である．視線軌跡は意識的に再現することができるため，認証情報として登録している視線軌跡を変更することで認証情報の変更が可能になると考える．また，他者からの認証情報の推測に頑健にするために，認証に用いる視線軌跡はユーザ自身が定義した軌跡を用いる．パターンロックやPINコードなどは入力を行う際にマス目や数字など，システムが提示されたものに合わせて入力するため，ユーザが登録できる情報が限られている．ユーザが形状を自身で定義することで，登録できる認証情報の種類を限りなくすることができると考える．よって視線軌跡をユーザ自身が定義することで他者が認証情報の推測をすることが困難になると考える．

以上のことから，ユーザ自身が定義した視線軌跡を個人認証に用いることで，知識認証やバイオメトリクス認証の脆弱性を解決することができると考える．

1.3 システム情報科学における本研究の位置付け

本研究はシステム情報科学において，モバイル端末に適用する個人認証手法の一つとして位

置付けられる．システム情報科学の分野では，様々な認証システムにおける脆弱性を解決する認証手法の提案を目的とした研究が数多く行われている[2], [3], [4], [5], [6], [7], [8], [9], [12], [13], [14], [15], [16], [17], [23], [36], [38], [39]．これらの研究によって，認証システムにおける脆弱性を解決し，認証システムの安全性向上とシステムごとに適した認証手法の実現が期待されている．

本研究は，認証情報の入力の覗き見，他者からの認証情報の偽造と推測に頑健である，認証情報の変更が可能である認証手法の提案を目的とした研究である．提案する認証手法は，ユーザがモバイル端末の画面上に視線で描画した軌跡の形状による認証と描画時の個人の癖を用いた認証を行う．提案手法の新規性としてユーザ自身が定義した視線軌跡から形状と描画時の癖のそれぞれを認証情報として用いることである．認証情報の入力の覗き見に対して頑健な個人認証手法として，視線移動を認証に用いた研究が行われている[18], [19], [20], [21], [22]．よって，視線軌跡を認証に用いることで，認証情報の入力の覗き見が困難になると考える．また，視線は偽造が困難であり，ユーザが意図的に描画した視線軌跡を用いることで認証情報の変更が可能になると考えられる．ユーザ自身が視線軌跡を定義することで，他者が認証情報を推測することが困難になると考えられる．よって，知識認証の脆弱性である入力の覗き見と認証情報の推測，バイオメトリクス認証の脆弱性である認証情報の偽造と認証情報の変更が困難であることを解決できる．これは，周囲に人がいる空間（公共空間）における安全な認証手法として有用であると考える．

1.4 論文の構成

本論文は全 5 章から構成される．第 1 章では本研究を行うに至った背景と本研究の目的と目標について述べる．第 2 章では，本研究の関連研究として知識認証に関する研究，バイオメトリクス認証に関する研究，視線移動を用いた認証に関する研究について述べる．第 3 章では，研究目的と提案システム，関連研究を踏まえ本研究の研究課題とアプローチについて述べ，その後に本研究の提案手法について述べる．第 4 章では，提案手法の評価実験と結果および考察について述べる．第 5 章では今後の展望について述べる．

第2章　関連研究

本章では，まず知識認証に関する研究について述べる．次に，バイオメトリクス認証に関する研究について述べる．最後に視線移動を認証に用いた研究について述べた後，関連研究のまとめと本研究の位置付けについて述べる．

2.1　知識認証に関する研究

知識認証に関する研究として，認証端末とは別のデバイス操作による入力を用いた研究[5], [6]と，認証端末のみで入力を行う研究[7]がある．

長友らは，マウス操作を用いた認証手法を提案している[5]．マウス操作とは，左右のクリック，ホイールクリック，ホイールの上下回転，上下左右の移動である．これらの操作を任意の回数繰り返し，パスワードを登録する．認証時に同様の操作を行うことで個人を認証する．山本らは，イヤホン内に搭載されている磁気センサを用いてスマートフォンのパスワードの入力を行う手法を提案している[6]．イヤホンの向きと，スマートフォンとイヤホンの位置による磁気の変化を判別し，それらをパスワードとしている．また，イヤホンごとによる磁気の違いを観測しているため，イヤホンの種類も認証情報として扱うことが可能であることを示唆している．

森らはスマートフォンにおけるスクロールとスライド操作を用いた認証手法を提案している[7]．この手法では，複数枚の画像を画面に表示させ，認証情報として登録した画像を選択することで認証を行うニーモニック認証に基づいている．画面上に 4×4 のグリッドを表示させ，あらかじめ設定した入力用の画像をスクロールとスライド操作を用いて選択することでパスワード入力を行う．また，廣瀬らは，スマートフォンに標準で搭載されている振動機能を用いた認証手法を提案している．この手法で用いる振動として，10 種類の振動が設定されており，それぞれ 0~9 の数字に対応している．スマートフォンが振動し，ユーザがパスワードとして登録した数字に対応した振動が行われたら画面上の数字ボタンを押すことでパスワード入力が行われる．

文献[5], [6]の手法では，認証端末の他にデバイスを用いるため，デバイスがないと認証を行うことができない．また，文献[7]の手法では，認証端末のみで認証を行うことができるが，特殊な操作を求められる場合があり，慣れていないユーザにとって認証負担が大きいと考えられる．

2.2　バイオメトリクス認証に関する研究

本節では，バイオメトリクス認証に関する研究として，身体的特徴を認証に用いた研究と，行動的特徴を認証に用いた研究について述べる．

2.2.1　身体的特徴を用いた認証に関する研究

身体的特徴とは，指紋や顔などの固有性が高い身体の部位を示す．身体的特徴を認証に用いた研究として，白川らは，虹彩と目の周辺の分割画像を用いた個人認証を行っている[8]．目の周辺画像全体から特徴量を抽出するのではなく，目の周辺を領域分割し各領域から特徴量を抽出する．この研究では，EER (Equal Error Rate) と識別率によって精度評価を行っている．EER は，

本人であるにも関わらず本人でないと誤認してしまう本人拒否率と他人であるにも関わらず本人であると誤認してしまう他人拒否率が等しくなるポイントである．識別率とは，EER と本人同士のスコアが最も高い割合である．EER と識別率は異なる粒度の分割領域から得られる特徴量を組み合わせることで向上することが確認されている．この手法では，虹彩と目の周辺の画像を認証情報として用いている．よって赤外線写真などで認証情報が容易に偽造されるリスクが考えられる．

藤田らは，肌理をマイクロスコープで撮影し，その画像を認証情報として用いた認証手法を提案している[9]．マイクロスコープの先端の形状とサイズに合わせた円形のマークを肌に記し，マークを目印として肌理の撮影を行っている．また，肌理の特徴として，皮溝と呼ばれる皮膚表面の溝，皮丘と呼ばれる浅い皮溝で囲まれた細かい隆起，皮野と呼ばれる深い皮溝に囲まれる多角形の隆起などを用いている．この手法では，認証情報として登録する肌の一部分にマークを記すため，被認証者に対する負担が大きいと考える．また，肌の認証情報として用いる部位が他者から明確に分かるため，偽造されるリスクがある．

上松らは，指間の線を用いることでスマートフォンにおける掌紋認証における掌紋の検出精度を向上した認証手法を提案している[10]．この手法では，人差し指，中指，薬指の間の三本線を抽出し，手のひらの角度と指の太さを算出することで手のひらの回転や拡大・縮小に対応している．そのため，ユーザは認証時にカメラに対して手のひらの向きや距離を意識することなく認証を行うことが可能である．この手法では，認証時に掌を撮影するため，他者から情報を盗み取られ偽造される恐れがある．

Chetana らは，指の関節の画像を認証情報に用いた認証手法を提案している[11]．前処理された指の関節の画像に対してラドン変換を行い，固有値を算出し，データベースに登録されている値と相関関係を計算することで認証を行っている．この手法では，掌紋認証と同様に認証情報を偽造される恐れがある．

これらの手法では認証情報として，体の一部を用いているため認証情報の変更が困難である．そのため，認証情報を偽造された際のなりすましに対して対処が困難になると考えられる．

2.2.2 行動的特徴を用いた認証に関する研究

キーボードの打鍵動作を認証に用いた研究がある[12], [13].

Nakakuni らは姓名の入力時のキーストロークダイナミクスの特徴を認証に用いている[12]．この研究では姓名を対象とすることで再現性が高く安定したリズムで入力が可能だと考える．この仮説に基づきユーザのキーストロークのタイミングを用いてユーザの分類を行っている．Zhou らはキーストロークダイナミクスの特徴に加え，キーストローク音響特徴を用いた認証を行っている[13]．マイクにより収集されたキーストローク音をフィルタリングし，MFCC（メル周波数ケプストラム係数）を算出し認証に用いている．

歩行時の特徴を認証に用いた研究がある[14], [15]．Li らは携帯電話を所持した状態における歩行を用いた認証を行っている[14]．この研究では，携帯電話搭載の加速度センサを用いて歩行時の特徴を抽出し，統計的特徴量を算出し認証に用いている． Musale らは歩行時の足や腕の動きの特徴を抽出し認証に用いている[15]．この研究ではスマートウォッチとスマートフォンを用いて人間の行動に関連づいた特徴量を抽出している．これにより，少ない特徴量でも高い精度でユーザの分類を行っている．

スマートフォンの操作時の特徴を認証に用いた研究がある[16], [17]．Salem らはタッチスクリーン端末で行う認証時のキーストロークを第 2 の認証要素として用いている[16]. この研究では，仮想キーボードを開発し，キーボード上で行う押下タイミングや位置などを特徴として用いて

認証を行っている．伊藤らは，スマートフォンにおけるフリック入力方式の特徴を用いた認証手法を提案している[17]．テキスト入力時のフリック動作や端末の揺れの特徴を用いて継続的に認証を行っている．

これらの手法では，ユーザそれぞれの行動に現れる無意識な癖やパターンを認証情報として用いているため，認証情報の変更が困難であり，なりすましへの対処が困難になると考える．

2.3 視線移動を用いた認証に関する研究

本節では，視線移動を用いた認証に関する研究として，無意識な視線移動を用いた認証に関する研究と意識的な視線移動を用いた認証に関する研究について述べる．

2.3.1 無意識な視線移動を用いた認証に関する研究

無意識な視線移動を認証に用いた研究として，Kinnunen らは，ビデオをディスプレイに表示し，それを見た被験者が行う無意識な視線移動の特徴を用いた認証手法を提案している[18]．Ma らは視線移動と頭部の動きを用いた認証手法を提案している[19]．ランダムな視覚刺激を表示し，その際に行う無意識な視線移動と頭部の動きをカメラにより計測し認証に用いている．

これらの手法では，ユーザに意識させず認証を行うことができる．しかし，意識的に認証情報を入力することは難しく，一度登録した認証情報の変更が困難であると考えられる．そのため，なりすましへの対処が困難であると考える．

2.3.2 意識的な視線移動を用いた認証に関する研究

ユーザの意識的な視線移動を認証に用いた研究として，視線でパスワードを入力する認証を行う研究[20]，[21]と，視線軌跡を描画し，描画時間や描画速度などの特徴量を抽出することで認証を行う研究がある[22]．De Luca らは，視線で PIN コードを入力する認証手法を提案している[20]．この手法では，ディスプレイ上に表示されたキーパッドの数字を一定時間注視することで PIN コードを順番に入力し，認証を行う．Khamis らは視線情報とパスワードを組み合わせた個人認証手法を提案している[21]．この研究では，タッチ入力と視線の方向を用いたマルチモーダルなパスワード（例 : left-3-right-4）を用いて認証を行う．一方，向井らは，あらかじめ与えられた文字を視線で描画し，その視線軌跡から得られる特徴を用いて，個人識別を行っている[22]．この手法では，認証情報として登録できる文字としてアルファベットと○記号を用いている．登録されている文字を一つ選択し，その文字をユーザが視線で描画する．描画された文字から抽出した特徴を用いて認証を行っている．この手法では，認証情報として登録された文字を変更することで認証情報の変更が可能になる．

これらの手法は，認証情報の変更が可能でありなりすましへの対処が可能である．しかし，文献[20]，[21]の手法では桁数が少ないパスワードを認証情報とした場合，攻撃者に推測されやすいと考えられる．文献[22]の手法では，認証情報として利用できる視線軌跡が限られており，他者から認証情報が推測されやすいことが考えられる．

2.4 まとめと本研究の位置付け

本節では，2.1 節，2.2 節，2.3 節で述べた関連研究をまとめ，本研究の位置付けについて述べる．

本研究では，モバイル端末の認証の安全性を考慮した個人認証手法の提案を目的とする．認証の安全性として，認証情報の覗き見，認証情報の偽造，他者からの認証情報の推測に対して頑健，認証情報の変更が可能であることが挙げられる．まず知識認証に関する研究についてまとめる．認証端末とは別のデバイスの特殊な操作を用いた手法と，認証端末の特殊な操作を用いた手法がある．どちらの手法もユーザが普段行わない操作が要求されるため，攻撃者が認証方法を知らない場合，認証情報の推測が困難になると考えられる．しかし，認証方法が知った攻撃者に対しては入力の覗き見や認証情報が推測される恐れがある．次にバイオメトリクス認証に関する研究についてまとめる．身体的特徴や行動的特徴を認証に用いると，認証時に特殊な操作を求められないため，認証が容易になり，認証情報の記憶負担が少なくなることが考えられる．しかし，身体的特徴は偽造されるリスクがある．この特徴は簡単に変化する情報ではないため，認証情報が一度偽造されるとなりすまされてしまう．また，顔や虹彩などの情報は不変的な情報であるため認証情報が困難である．よって，攻撃者に対して対処することができなくなると考える．行動的特徴は無意識に現れる特定の行動の癖やパターンであるため，一部の身体的特徴と同様に認証情報が困難である．最後に視線移動を認証に用いた研究についてまとめる．視線を認証に用いることで覗き見に対して頑健になる．しかし無意識な視線移動を認証に用いた場合，行動的特徴と同様に認証情報の変更が困難になると考えられる．また，意識的な視線移動を認証に用いた場合，認証情報を強固なものにするためには，複雑な操作が求められるため，認証負担が大きくなると考えられる．

関連研究を踏まえ，本研究では，無意識な視線移動と意識的な視線移動を組み合わせた情報を認証に用いる．意識的な視線移動として，ユーザ自身が定義した視線軌跡を用いる．視線軌跡を用いることで入力の覗き見，偽造に対して頑健になると考える．また，視線軌跡は意識的に再現することが可能であるため，認証情報の変更が可能になる．認証情報に用いる視線軌跡をユーザ自身が定義することで，他者からの推測に対して頑健になると考える．視線軌跡の形状のみを認証情報とすると同様の軌跡を描画した複数のユーザを同一のユーザとして誤識別することが考えられる．そこで，無意識な視線移動として，視線軌跡を描画した際の個人の癖を認証情報に用いる．

第3章　提案手法

本章では，本研究の提案手法について述べる．3.1 節では，関連研究を踏まえた本研究における研究目的について述べる．3.2 節では，提案システムの概要について述べる．3.3 節では研究目的を達成するための研究課題とそのアプローチについて述べる．3.4 節以降では，提案手法の詳細について述べる．

3.1　研究目的

本研究の目的は，知識認証とバイオメトリクス認証の脆弱性を解決する視線軌跡を用いた個人認証手法の提案である．視線は目に見える情報ではないため，覗き見や偽造により漏洩するリスクが低いと考える．また，ユーザにより意識的に視線を再現することができるため，認証情報の変更が可能になる．よって，認証情報の偽造によるなりすましへの対処が可能になると考える．

提案手法は，入力された視線軌跡の形状による認証と視線で描画した際の個人の特徴（以下，描画特徴と呼ぶ）による認証から構成される．視線軌跡の形状は入力するユーザにより意識的に変更が可能であるため，認証情報の要素として視線軌跡の形状を用いることで，認証情報の変更が可能になる．視線軌跡の形状のみを認証情報とする場合，同一の軌跡を描画した異なるユーザが同一のユーザとして識別され，なりすましの被害に遭う恐れがある．よって，描画特徴を用いることで，軌跡の形状の偽造によるなりすましに対して頑健になると考える．

3.2　提案システムの概要

本節では，提案システムのシステム構成について述べる．本研究の提案システムの全体像を図に示す．提案システムは学習フェーズと認証フェーズから構成される．

学習フェーズは認証情報となる視線軌跡の形状，個人の描画特徴を登録するフェーズである．認証情報を登録する際は，ユーザが認証情報として登録したい視線軌跡を複数回入力する．描画した視線軌跡から特徴量を抽出し認証情報として登録する．また，認証情報を新たに登録するだけでなく，既に登録されている認証情報の更新も学習フェーズで行われる．認証情報を更新する際は，認証情報の登録時と同様に新しく登録したい視線軌跡を複数回入力する．入力された視線軌跡の形状と既に登録している視線軌跡の形状を比較し，異なる形状であると識別し認証情報を更新する．

認証フェーズは認証を行うユーザが登録されたユーザと一致するかを識別するフェーズである．まず視線軌跡を入力し，入力された視線軌跡から形状を推定するための特徴量を抽出し，認証情報として登録された視線軌跡と同様の形状であれば，1 段階目の認証成功とする．次に描画特徴を抽出し，既に登録している描画特徴と比較を行い，同様の個人描画特徴であれば 2 段階目の認証成功とする．2 段階目の認証が成功することで登録したユーザと認証を行うユーザの識別が完了し提案システムでの認証成功とする．

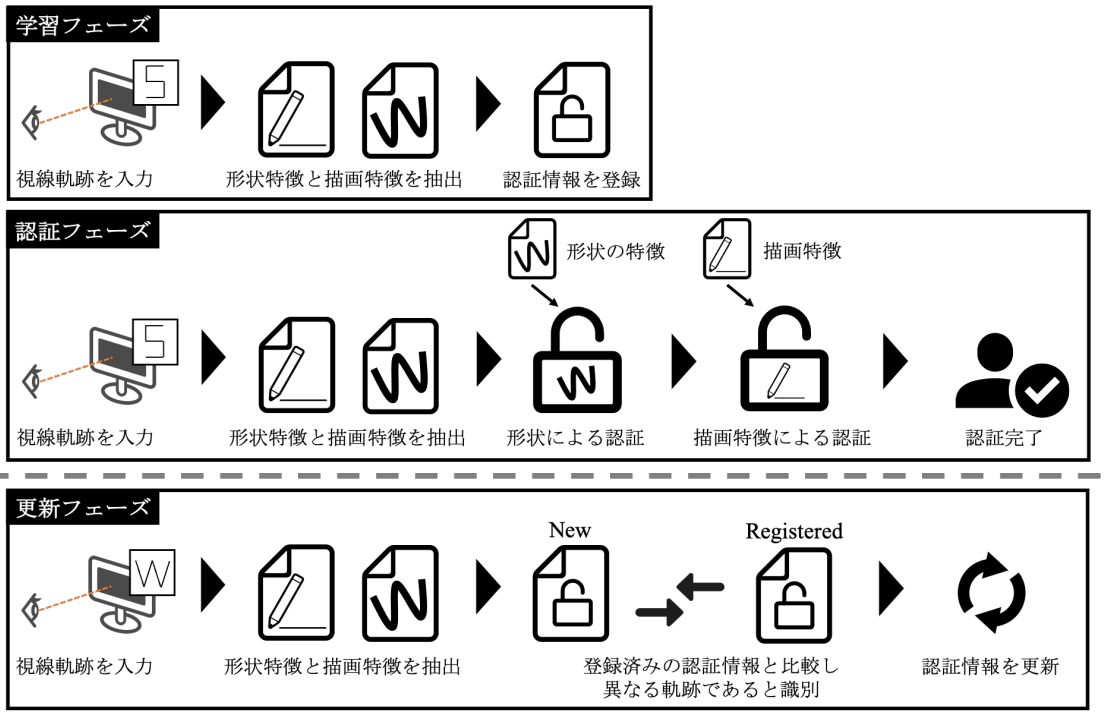


図 2 提案システム

Fig. 2 Proposed system

3.2.1 学習フェーズ

学習フェーズにおいて，認証情報を登録する際，軌跡の形状の特徴と個人の描画特徴の抽出を行い，それぞれの学習モデルの作成を行う．学習フェーズでは始めに視線軌跡の入力後，どのような形状の軌跡であるかの推定（形状推定）を行う．形状推定を行うために入力されたデータに対して前処理を行う．前処理終了後に視線軌跡のデータから形状推定に用いる特徴量の抽出を行う．その後に視線軌跡の形状による認証のための識別モデルの作成を行う．個人識別モデル作成でも同様に，入力された視線軌跡に対して前処理を行い特徴量の抽出を行う．形状推定とは別に描画特徴の抽出を行い，描画特徴による認証のための識別モデルの作成を行う．認証情報を更新する際は，まず視線軌跡の入力を行う．

3.2.2 認証フェーズ

認証フェーズにおいて，視線軌跡の入力後に 1 段階目の認証として，入力された視線軌跡に対し前処理を行い，視線軌跡の形状による認証を行うための特徴量を抽出する．抽出した特徴量と学習フェーズで作成した形状識別モデルを用いて入力された視線軌跡と既に登録している認証情報を比較し，形状が一致するかを照合する．1 段階目の認証で同様の形状であると識別される場合に 2 段階目の認証に進む．2 段階目の認証では，形状推定とは別に個人描画特徴を抽出する．登録している個人識別モデルと比較し，同様の特徴であると識別されることで 2 段階目の認証が完了する．2 段階目の認証が完了することで，入力を行ったユーザと登録しているユーザが同一人物であると識別され提案システムでの認証が完了する．

3.2.3 更新フェーズ

認証情報を更新する際は，まず視線軌跡の入力を行う．入力された視線軌跡から登録時と同様に形状識別モデルと個人識別モデルの作成を行う．新たに入力した視線軌跡と，既に登録している視線軌跡のそれぞれの形状を比較し，異なる形状であると識別された場合に認証情報を上書きし更新を行う．

3.3 研究課題とアプローチ

本研究では，最終目的を達成する上での研究課題を以下の 4 つとする．

a) 計測デバイスの選定
b) 視線軌跡の形状による認証に有効な特徴量の検討
c) 描画特徴による認証に有効な特徴量の検討
d) 1 対 1 認証を想定した学習

これらの課題に対するアプローチを以下に述べる．

課題 a に対するアプローチとして，非接触型デバイスを計測デバイスとして用いる．視線計測装置としてメガネ型の接触型のデバイスと，据え置き型やディスプレイ一体型の非接触型のデバイスがある．メガネ型の接触型デバイスを用いた場合，計測デバイスのみを用いてデータ収集するため，認証端末との位置や傾きなどを考慮する必要がない．しかし，普段メガネをかけないユーザにとって，メガネをかけた際の視線の遮りや装着感などが負担になると考えられる．そのため，メガネ型の接触型デバイスを認証に用いた場合，認証負担が大きくなると考える．一方，非接触型デバイスは装着などの負担を与えないため，ユーザが制限されることがない．しかし，正確に計測を行う際にユーザと視線計測デバイスの配置について考慮する必要がある．ユーザと視線計測デバイスの位置が離れている，ユーザや視線計測デバイスが傾くなどによりデータが正しく計測されないことが考えられる．以上の理由により，本研究では，計測デバイスとして非接触型デバイスを用いる．

課題 b に対するアプローチとして，視線軌跡の形状推定に対して有効な特徴量の選定を行う．提案システムでは，認証情報の登録時に視線軌跡の形状と描画特徴を用いる．また，ユーザ自身が定義した視線軌跡を認証に用いるため，視線軌跡の形状が認証者本人のみが知り得る情報となる．そのため，認証時にユーザがどのような形状の軌跡を描画したかの推定を行う必要がある．視線軌跡のデータは座標群や軌跡画像として扱うことができる．座標群と軌跡画像それぞれから特徴を抽出し，視線軌跡の分類を行い，分類精度を比較することで形状推定に対して有効な特徴量の調査を行う．

課題 c に対するアプローチとして，視線軌跡から局所的に抽出した注視とサッケードの特徴を個人分類に用いる．なりすましに対して頑健にするために登録されたユーザが本人か否かを識別するための要素技術として個人分類を行う．実験として，座標群データから視線軌跡の描画の全フレームの座標の変化量を特徴量として用いて個人分類を行った．しかし，特徴量の中に個人分類に有効でない特徴が含まれていた．そこで視線移動から注視やサッケードを検出し，特徴量を抽出する．局所的に視線移動を検出することで，個人の特徴がより現れる特徴量が抽出できると考える．

課題 d に対するアプローチとして，異常検知アルゴリズムを用いる．異常検知とは，正常なデータのみを学習し未知のデータを正常か異常か識別する手法である．認証方式として，本人のデ

ータのみを学習し本人か否か識別する 1 対 1 認証と，登録されているユーザのうちの誰なのかを識別する 1 対 N 認証がある．提案手法は個人が保有するモバイル端末に適用することを想定している．よって，提案手法では学習に本人のデータのみを用いる 1 対 1 認証を行う．そこで，異常検知アルゴリズムが提案手法の学習アルゴリズムとして有効であると考える．

3.4 計測デバイスの選定

視線計測デバイスとして挙げられる接触型デバイス，非接触型デバイスの比較表を以下に示す．

表 1 視線計測デバイスの比較表

Table 1 The comparison between different kinds of gaze tracking devices

	装着負担	認証時の環境の統一性	計測デバイスのバッテリー
接触型デバイス	×	○	×
非接触型デバイス	○	×	○

接触型デバイスを用いると，装着したデバイスで視線を計測するため，認証端末との位置や傾きなどを考慮する必要がないため，認証時に統一性を持って認証を行うことができる．しかし，身につける必要があるため，認証時に装着負担が発生する．普段メガネをかけないユーザにとっては装着時の装着感や視界の妨げが負担となることが考えられる．モバイル端末への適用を想定すると，認証端末とは別に認証用の端末を用意する必要があると考える．よって，認証端末だけでなく，計測デバイスのバッテリーも考慮する必要性が発生する．

非接触型デバイスは計測デバイスと認証端末が一体になっているため，ユーザに装着負担が発生しない．また，ノートパソコンやスマートフォンなどのカメラを計測デバイスとすると，認証端末のバッテリーを十分に充電しておくことで認証を行うことができる．しかし，認証時に認証端末との位置や傾きを考慮せずに計測を行うと正しくデータが収集できない．そのため端末が変わることで認証時の環境が変化することが考えられる．

提案システムは，スマートフォンやノートパソコンなどのモバイル端末に搭載され，ユーザが非接触で視線計測することを想定している．非接触型のデバイスでは角膜反射法という測定法に基づいて視線計測を行う．まず，角膜に対して弱い近赤外線を照射する．反射点と瞳孔の動きのパターンをアイトラッキングカメラにより映像解析を行い，ユーザの注視点を計測する．さらに，低価格な視線計測の装置が登場してきており，視線計測装置の低コスト化が進み様々な分野への応用が期待されている．この流れを受けて低コストかつ高精度なカメラ開発を目的とした研究が行われている[25]．また，TrueDepth カメラや赤外線カメラなどの高精度なカメラを搭載したモバイル端末が登場し，普及しつつある[26], [27]．これにより将来，あらゆるモバイル端末に視線計測が可能なカメラが搭載されることが考えられる．

以上の理由により，本研究ではデータ収集に用いる視線計測デバイスとして，非接触型デバイスを用いる．

3.5 視線軌跡の形状による認証

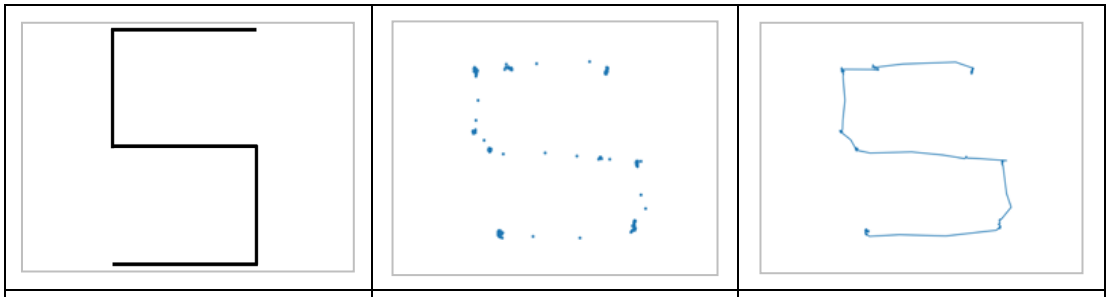
本節では提案システムにおける視線軌跡の形状による認証について述べる．

3.5.1 視線軌跡の形状推定

提案システムでは，ユーザ自身が定義した視線軌跡を用いる．認証時にはユーザがどのような視線軌跡を描画したかを識別する必要がある．そこで，提案手法では，視線軌跡から抽出できる特徴量を用いてどのような軌跡か形状推定を行う．

3.5.2 視線軌跡の形状推定に用いるデータ検討

視線軌跡の形状推定を行う上で，有効な特徴量を選定する必要がある．図 3 に収集される視線軌跡のデータの一例を示す．視線軌跡の形状推定において，座標群あるいは軌跡画像を用いるアプローチが考えられる．軌跡画像は座標群を時系列順に線で結び，画像化したデータを指す．



(a) 定義した図形　(b) 座標群　(c) 軌跡画像

図 3 収集したデータの一例

Fig. 3 An example of collected data

本研究で想定する認証に用いる視線軌跡は，直線と転折のみで構成される図形である．

3.5.3 軌跡画像の前処理

図 3 の軌跡画像の一例より，軌跡画像には描画時の注視点や視線の動きのブレが見られる．これらが視線軌跡の形状推定においてノイズになると考え，ノイズを除去するために，軌跡画像に対して前処理を行う．

軌跡画像に対する前処理の手順を以下に示す．

(1) 2 値化
(2) 膨張処理
(3) 細線化処理

まず軌跡画像に対して 2 値化を行う．2 値化された軌跡画像では，軌跡は白色で表現される．次に 2 値化した軌跡画像に対して膨張処理，細線化処理の順で処理を行う．膨張処理は，2 値画像において注目画素の周辺に白い画素が 1 画素でも存在する場合に注目画素の色を白に置き換える処理である．膨張処理を行うことにより視線の細かいブレを除去することができると考える．細線化処理とは 2 値画像を幅 1 ピクセルの線画像に変換する処理である．膨張処理を行うことで，注視点の部分の幅が大きくなる．また，膨張処理を行った際，注視点や視線のブレにより凹凸が生じる．それらの凹凸により形状が正しく推定されない可能性がある．そこで，膨張処理後の軌跡の幅を統一するために細線化処理を行う．細線化処理とは 2 値画像を幅 1 ピクセルの線画像に変換する処理である．膨張処理を行うことで，注視箇所の部分の幅が大きくなる．膨張

処理を行った際，注視箇所や視線のブレにより凹凸が生じる．それらの凹凸により形状が正しく推定されないことが考えられる．これらの処理を用いることで，視線軌跡の形状推定においてノイズとなる注視点や視線の動きのブレを除去することができると考える．

表 2 に，視線軌跡データに対して前処理を行った環境を示す．

表 2 処理環境

Table 2 Processing Environment

PC，ソフトウェア	仕様
CPU	Intel Core i5 2GHz
OS	High Sierra10.13.6
言語環境	Python2.7.15
使用ライブラリ	OpenCV3.4.3

軌跡画像に対して 2 値化，膨張処置，細線化処理を行った画像を図 4 に示す．視線軌跡の注視箇所のブレは軌跡ごとに異なるため，どのようなブレにおいても均等に滑らかにするために膨張処理を 30 回行った．また，(c)においては見やすさを考慮して白黒を反転させて表示している．

(a) 軌跡画像	(b) (a)に対して 2 値化・膨張処理した画像	(c) (b)に対して 細線化処理をした画像

図 4 前処理を行った画像

Fig. 4 Preprocessed images

前処理を行った画像から軌跡の形状推定に用いる特徴量の抽出を行う．

3.5.4 軌跡画像の特徴量の検討

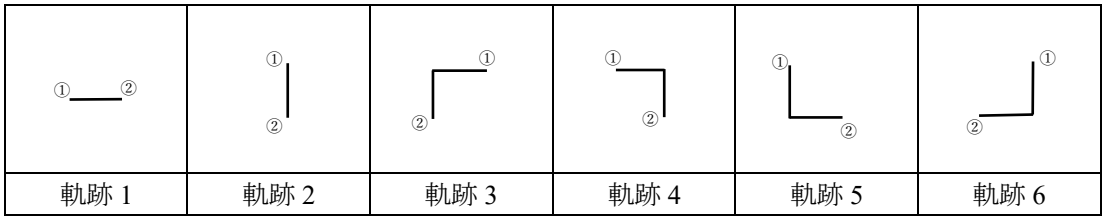
画像から抽出できる特徴量として，局所特徴と大域特徴が挙げられる．局所特徴とは，エッジや大きな濃淡の変化などの画像内に見られる一定のパターンや際立った特徴が表れている部分を指す．局所特徴は回転とスケール変化に対して頑健な特徴である．大域特徴とは画像全体の情報を持った特徴であり，位置ズレとスケール変化に対して頑健である．

提案システムでは，モバイル端末に対しユーザが正面を向き，モバイル端末上の画面上に視線軌跡を描画することで認証を行う．ユーザが毎回画面上の同じ位置，同じ大きさで視線軌跡を描画することは困難である．そのため，提案手法では，位置ズレとスケール変化に対して頑健な大域特徴が望ましいと考える．また，局所特徴は回転に対して頑健であるため，異なる形状の軌跡間において回転すると同様の軌跡であると同一の形状の軌跡であると誤認識される恐れがある．以上の理由により，提案手法では画像から抽出する特徴として大域特徴を用いる．

代表的な大域特徴として HoG (Histograms of Oriented Gradients) 特徴[28]，Haar-like 特徴[29], LBP (Local Binary Pattern) 特徴[30]が挙げられる．HoG 特徴とは，画像の画素の勾配方向をヒストグラム化した大域特徴である．HoG 特徴は画像のスケール変化と照明変化に対して頑健である. Haar-like 特徴とは, 画像の明暗差に着目し, 明暗のパターンから特徴を抽出した特徴である．Haar-like 特徴は画像の明暗に対して頑健である．しかし，パターンを用いて特徴を抽出するため，輪郭の情報が損なわれる．LBP 特徴は局所的な部分の輝度値の大小関係のパターンを 2 値化した特徴量である．LBP 特徴は画像全体の濃淡の変化に対して頑健である．しかし，不規則な照明の変化に対して弱い．本研究では，モバイル端末を用いて様々な環境において認証を行うことを想定しているため，照明の変化を考慮する必要がある．以上のことから提案手法では，大域特徴の中で HoG 特徴に着目し，視線軌跡の形状推定に対する有効性の調査を行う．

3.5.5 HoG 特徴量の形状推定に対する有効性調査

HoG 特徴が視線軌跡の形状推定に対して有効であるかを調査するための予備分析を行った．実験で設定した軌跡を図 5 に示す．①は描画の開始点，②は終了点を表す．基礎検討として，視線軌跡の構成要素となり得る基本的な軌跡の形状推定を行う．収集したデータ数は各軌跡 20 個ずつで計 120 個である．また，被験者は 1 名である．収集した視線軌跡に対し 3.5.3 項で述べた前処理を行い軌跡画像に変換した．軌跡画像から HoG 特徴を抽出し，軌跡ごとに平均値を算出した．HoG 特徴は対象画像から算出される 32 方向の輝度勾配をヒストグラム化した 32 次元の特徴である．各軌跡に対する HoG 特徴の抽出結果を図 6 に示す．横軸は輝度勾配の各方向であり，縦軸は各方向の輝度勾配の合計値である．横軸の番号は画像を 32 分割し，左上から順に番号を振った.



軌跡 1	軌跡 2	軌跡 3	軌跡 4	軌跡 5	軌跡 6

図 5 軌跡一覧

Fig. 5 Trajectories list

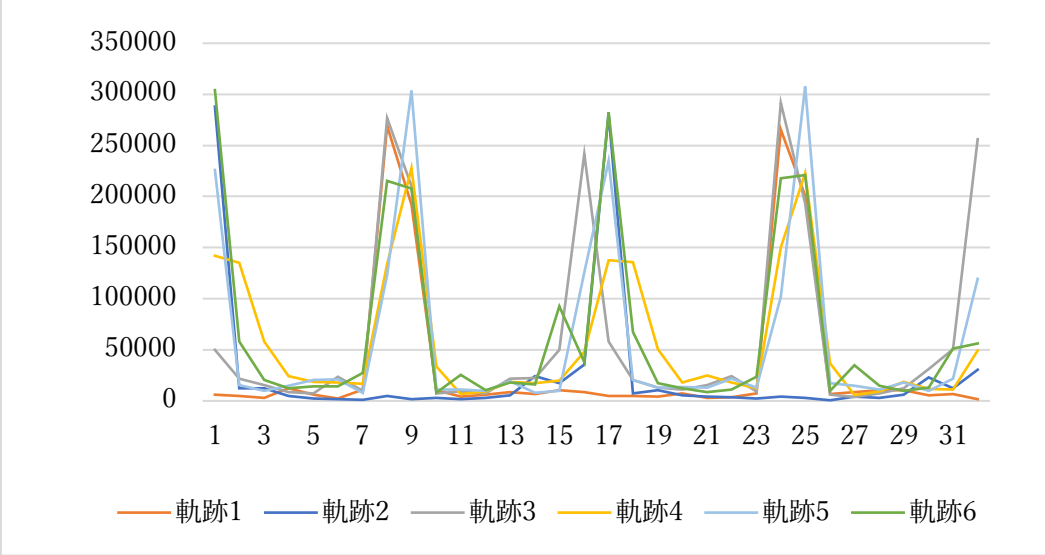


図 6 軌跡ごとの HoG 特徴

Fig. 6 HoG features by trajectories

図 6 より，水平方向を示す 9，25 付近の輝度勾配が高くなることで水平方向の直線が含まれると考えられる．鉛直方向を示す 1，17 付近の輝度勾配が高くなることで鉛直方向の直線が含まれると考えられる．軌跡 1 は水平方向の直線であり，軌跡 2 は鉛直方向の直線である．よって各軌跡の方向に対応した輝度勾配が大きくなる．軌跡 3 から軌跡 6 は直線と転折を含む軌跡である．よって水平方向と鉛直方向の輝度勾配が大きくなっている．また，軌跡 3 から軌跡 6 はそれぞれ異なる方向へ転折を行っている．そのため，水平方向と鉛直方向付近の輝度勾配に軌跡ごとに違いが見られる．このように軌跡の形状ごとに HoG 特徴において違いが見られるため，HoG 特徴が視線軌跡の形状推定において有効であると考える．

3.5.6 形状推定に用いる座標群データの前処理

収集される座標群データをそのまま用いると，視線のブレや注視点などがあり，形状による認証においてノイズになると考えられる．生データを用いる場合，描画時の視線の大きな乱れが含まれていることもあり，それが外れ値となりノイズになると考えられる．よって，形状推定を行う前に座標群データの前処理を行う．

まず，描画された軌跡の全フレームを時系列順に分割する．次に分割された区域ごとに座標の平均化を行い，平均座標群データを算出する．これにより，視線のブレが除去されると考えられる．また，注視による複数の集中した座標が含まれる区域において，平均座標群データを算出することで注視点を除外することが可能であると考える．平均座標群データを算出する際の分割数は，多いほど元の軌跡データの形状情報を維持しつつ大きな外れ値を除外することができる．また，分割数が少ないほど元の軌跡データの概形を維持し視線のブレの削除が可能である．よって，視線軌跡の形状による認証においては分割数を少なく，描画特徴による認証においては分割数を多くした状態で平均座標群データの算出を行う．それぞれで算出した平均座標群データから形状による認証と描画特徴による認証に関する特徴量の抽出を行う．

3.5.7 座標群データの特徴量の検討

座標群から抽出できる特徴量として，視線軌跡の描画の開始から終了までの全フレームから特徴の抽出を行う．連続する 2 フレーム間の変化量を用いることで描画の方向を抽出することができる．全フレームの変化量からどのような視線移動をしたかを把握することができるため，視線軌跡の座標の変化量が形状推定に有効な特徴量であると考える．しかし，全フレームの座標群を用いると，視線のブレや注視点などが形状推定においてノイズになると考えられる．描画の全フレームを複数に分割すると，分割フレームごとに一定の領域に分布する座標群が得られる．各分割領域の平均座標を算出し，平均座標を結ぶことで，視線のブレが滑らかになると考えられる．また，注視による複数の集中した座標が含まれる領域において，平均座標を算出することで注視点を削除することが可能だと考える．

形状推定において考えられるノイズを平均座標群の x 座標と y 座標それぞれにおいて連続する 2 フレーム間の変化量を特徴として用いる．x 座標と y 座標の変化量の次元数は，それぞれフレームの分割数より 1 少ない数である．フレームの適切な分割数については，分割数ごとの分類精度により評価し検討を行う．

3.6 描画特徴による認証

本節では，提案システムにおける描画特徴を用いた認証について述べる．

3.6.1 描画特徴を用いた個人分類

本研究では，視線軌跡を描く際の描画特徴に個人差が現れると考え，その個人差に基づいた認証手法の実現を目指す．個人認証において，他者と類似する特徴を用いた場合，他人受け入れ率が高くなる可能性があると考える．したがって，個人の特徴が顕著に現れる特徴量を見つけることで，その特徴量が個人識別において有効な特徴量の候補になると考える．そこで，描画特徴に用いる特徴量の検討の基本評価として，描画特徴を用いた個人分類を行う．

3.6.2 大域的な描画特徴の検討

描画特徴を検討する上で，複数のユーザが描画した視線軌跡間でどのような個人差が見られるか分析を行った．描画する視線軌跡が簡素な場合，個人差があまり見られず，描画特徴の抽出が困難であると考えた．しかし，複雑な図形である場合，描画が困難となり，設定した図形を被験者が再現することができないと考えた．そこで，試験的に直線と転折から構成される図 7 の図形を用いた．被験者 3 人に対して図 7 の図形を視線で 30 回描画するように指示し，データの収集を行った．中村らは，複数のユーザ間の手書き文字の平均をとった平均文字は個人の描画の癖が弱まり綺麗になる傾向があると主張している[31]．この知見を踏まえて同一ユーザの平均文字には個人の描画の癖が強くなり，個人差が現れやすくなると考えた．そこで，視線により描画した図形についても，手書き文字と同様の傾向が現れると考え，被験者ごとに収集したデータを平均化した視線軌跡を算出し，その平均化された軌跡を対象として描画特徴の分析を行った．図 8 に各被験者の平均化された視線軌跡を示す．

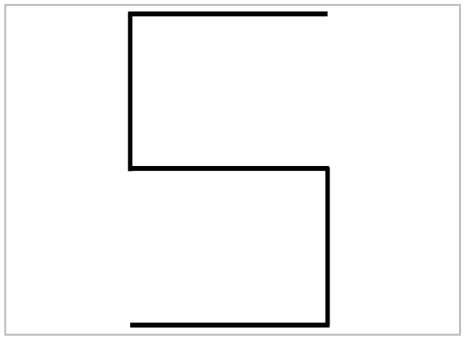


図 7 被験者に描画を指示した図形

Fig. 7 A trajectory that the subject was instructed to draw

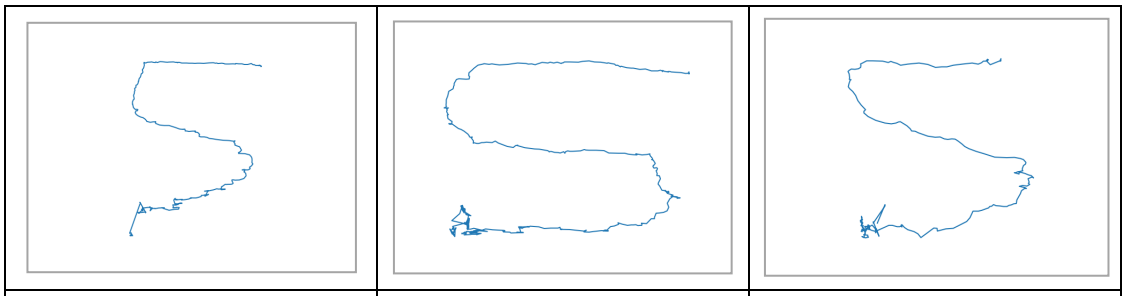


図 8 各被験者の平均化した視線軌跡

Fig. 8 Averaged eye movement trajectory for each subject

図 8 の平均化された視線軌跡もまた，座標群により構成されており，各座標を線で結んだものである．図 8 において，線が交差している部分は注視点である．図 8 の視線軌跡では，描画中にどの部分で注視を行っているか，転折する際の角度，視線の散らばり具合（描画範囲）に個人差が見られる．また，各被験者の 30 回分の描画時間を平均した値を表 3 に示す．

表 3 各被験者の平均描画時間

Table 3 Average drawing time for each subject

被験者	描画時間(s)
被験者 A	4.91
被験者 B	5.12
被験者 C	3.59

表 3 より，描画時間にも同様に個人差が見られると考えられる．

描画特徴として転折の角度，注視点，視線の描画範囲，描画時間を描画特徴として用いることを検討する．

個人毎に転折や注視するタイミングが異なる．そこで，描画時間の全フレームの特徴を用いることにより，転折と注視を漏れなく抽出できると考えた．転折の角度と注視点を表現するものとして，x 座標と y 座標の変化量を用いることを検討する．描画の開始から終了までのフレームを分割し，連続した分割フレームに対する平均座標の変化量を用いる．転折は描画の方向が急激に変わるため，x 座標や y 座標の変化量にも大きな変化が見られ，変化量の値から転折の角度を抽出できると考える．また，注視点は視線が集中するため，座標の変化量が少なくなる．よって，分割フレームの平均座標の間の変化量により転折の角度と注視点を抽出できると考える．平均

座標の x 座標と y 座標に関する特徴量の次元数は，ともに分割数より 1 少ない数となる．例として，分割数が 20 の場合，x 座標と y 座標の変化量がそれぞれ 19 次元であるため，合計で 38 次元となる．分割数が少ないと注視点や転折がスムージングされ，注視点や転折が抽出できないと考える．よって，分割数を多くすることで注視点や転折の抽出が行いやすくなると考えられる．

視線軌跡の描画範囲を示すものとして，軌跡全体の x 座標と y 座標のそれぞれの標準偏差と分散を用いる．また，描画時間としては視線軌跡の描画開始から終了までのフレーム数を用いる．よって，描画範囲と描画時間に関する特徴量の次元数の合計は 5 次元である．

3.6.3 局所的な描画特徴の検討

局所的な描画特徴として，注視とサッケードに関する特徴量を用いる．注視とは視線を固定するために行う視線移動である．また，サッケードとは，ある点からある点へと視線を向ける際の断続的に行われる高速な眼球運動である[32], [33]．サッケードの例として，読書中に次の行へ移る際の視線移動が挙げられる．注視とサッケードの個人差を調査する研究があり，それらの研究では実験結果からこれらの視線移動に個人差があることを示唆している[34], [35]．提案手法では，これらの視線移動に個人の特徴が現れると考え，特徴量の抽出を行う．

前処理を行い，算出された平均座標群データから注視とサッケードの特徴量の抽出を行う．

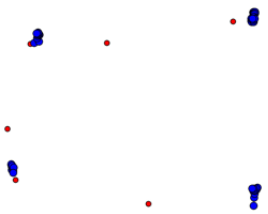
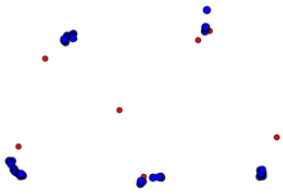
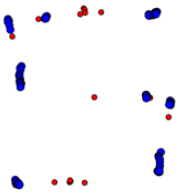
まず，注視の特徴量抽出のために注視の検出を行う．平均座標群からスライディングウィンドウを用いて注視箇所の検出を行う．スライディングウィンドウにより任意の大きさの検出窓を一定のフレーム数ずらしながら注視箇所の検出を行う．検出窓内において，計測された視線の座標が密集している箇所を注視箇所とする．本研究では，5 個以上の点が密集している箇所を注視箇所として検出を行った．検出された注視箇所ごとに注視の特徴量の抽出を行う．

次に，サッケードの検出は，注視箇所ごとに平均座標を算出し，注視箇所のみで形成される注視座標群データを算出する．軌跡描画に伴い，注視とサッケードは繰り返し行われていると考えられるため，注視座標群データの連続する 2 フレーム間の座標の変化量を算出することでサッケードの抽出を行う．

提案手法を用いて注視箇所が検出できているか予備分析を行った．提案手法を用いて 4 種の軌跡の平均座標群データから注視を抽出した結果を表 4 に示す．

表 4 軌跡から抽出された注視

Table 4 Fixations extracted from trajectory

描画した軌跡	抽出した注視
	
	
	
	

青の点が注視と判定された視線の計測点を示す．軌跡の開始点，終了点，転折箇所に青の点が密集している．よって，注視箇所が検出できていることが示される．提案手法では，このように抽出された注視箇所を用いてサッケードの検出と，特徴量の抽出を行う．

抽出する注視とサッケードの特徴量として，注視時間，注視の分散，注視の標準偏差，注視の回数，x，y 方向のサッケードの速度，サッケードの回数を検討する．注視時間とは，注視を行った最大と最小の時間，それぞれを 1 次元で表した特徴量である．注視の分散とは，注視箇所の座標の分散の最大値，最小値，平均値をそれぞれ 1 次元で表した特徴量である．注視の標準偏差とは，注視の分散と同様に注視箇所ごとに算出した標準偏差の最大値，最小値，平均値である．

表 5 局所的な特徴量の一覧
Table 5 List of local features

特徴量
注視時間（最大値，平均）
注視の x，y 方向の分散（最大値，最小値，平均）
注視の x，y 方向の標準偏差（最大値，最小値，平均）
注視の回数
x，y 方向のサッケードの速度（最大値，最小値，平均）
サッケードの回数

3.7 1 対 1 認証を想定した学習

本節では提案手法における認証情報の学習方法について述べる．

3.7.1 本研究で想定する認証方式

本研究では，1 対 1 認証を想定する．認証方式として，1 対 1 認証と 1 対 N 認証がある．1 対 1 認証とは，本人のみのデータを学習し，認証の際に入力されたデータが本人か他人かの識別を行う認証方式である．1 対 N 認証とは，複数人のデータを学習し，認証の際に入力されたデータが登録されているユーザの誰かを識別する認証方式である．提案手法は個人が保有するモバイル端末に適用することを想定している．そのため，端末所持者のデータは入力されるが，他人のデータが入力されることはないと考える．よって，提案システムの視線軌跡の形状による認証と描画特徴による認証において 1 対 1 認証を行う．

3.7.2 1 対 1 認証を想定した学習アルゴリズムの検討

1 対 1 認証を想定した学習アルゴリズムとして，異常検知が挙げられる．異常検知とは，正常なデータのみを学習し，未知のデータが入力された際にそのデータが正常か異常かの識別を行う手法である．提案手法において認証に用いるデータは本人のデータを正常なデータ，他人のデータを異常なデータとして扱う．異常検知アルゴリズムを個人認証に用いている研究として，One Class SVM と Isolation Forest を用いた研究がある[17]，[36]．One Class SVM（以下，OCSVM）とは，SVM において，正常なデータを 1 クラスとして学習に用いて，未知の入力データが正常か異常かを識別する異常検知アルゴリズムである[37]．Isolation Forest（以下，IForest）とは，ランダムに特徴量と分割点の選択を繰り返し，孤立したデータを異常データとする異常検知アルゴリズムである．これらのアルゴリズムを用いて識別モデルを作成し，精度を算出することで提案手法に有効なアルゴリズムの検討を行う．

第4章　実験および考察

本章では，提案手法の認証精度を評価するために行った実験について述べる．4.1 節では，実験に用いる評価指標について述べる．4.2 節では，視線軌跡の形状による認証に関する実験について述べる．4.3 節では，描画特徴による認証に関する実験について述べる．4.4 節では学習データの水増しの有効性を検討するために行った実験について述べる．最後に 4.5 節では視線軌跡描画時におけるガイドの有効性を検討するために行った実験について述べる．

4.1　評価指標

本節では, 評価実験に用いる評価指標について述べる. 本研究の評価実験で用いる評価指標は, Precision，Recall，Specificity，F-measure，FAR (False Acceptance Rate)，FRR (False Rjection Rate) である．Precision とは，本人であると予測されたデータの中で実際に本人であるデータの割合であり，式 (1) で定義される．Recall とは，実際に本人であるデータの中で本人であると予測されたデータの割合であり，式 (2) で定義される．Specificity とは，実際に他人であるデータの中で他人であると予測されたデータの割合であり，式 (3) で定義される．F-measure とは，Recall と Precision の調和平均であり，式 (4) で定義される．FAR とは他人を誤って本人と識別する確率であり，式 (5) で定義される．FRR は本人を誤って他人と識別する確率であり，式 (6) で定義される．FAR と FRR はエラーの確率であるため，低ければ低いほど精度が高いと言える．

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$Specificity = \frac{TN}{FP + TN} \tag{3}$$

$$F\text{-}measure = \frac{2Recall \times Precision}{Recall + Precision} \tag{4}$$

$$FAR = \frac{FP}{TN + FP} \tag{5}$$

$$FRR = \frac{FN}{FN + TP} \tag{6}$$

4.2 視線軌跡の形状による認証に関する実験

4.2.1 HoG 特徴を用いた視線軌跡の形状推定

HoG 特徴の視線軌跡の形状推定に対する有効性を調査するために軌跡画像から HoG 特徴を抽出し，軌跡の分類を行った．実験に用いた軌跡は，3.5.5 項での予備分析に用いた軌跡と同様の図 5 の軌跡である．データ数は各軌跡 20，合計 120 である．SVM を用いた 10-分割交差検証を行い，Precision，Recall，F-measure による評価を行った．分類結果を表 6 に示す．また，表の右下の太枠内は F-measure を示す．

表 6 HoG 特徴を用いた分類結果

Table 6 The classification result using HoG features

		予測結果						Recall
		軌跡 1	軌跡 2	軌跡 3	軌跡 4	軌跡 5	軌跡 6	
								
正解ラベル		20	0	0	0	0	0	1.00
		0	20	0	0	0	0	1.00
		0	0	9	4	5	2	0.45
		0	0	2	13	5	0	0.65
		0	0	4	5	11	0	0.55
		0	0	4	1	2	13	0.65
Precision		1.00	1.00	0.47	0.57	0.48	0.87	0.72

軌跡 1 と軌跡 2 の分類精度が 100%となった．また，軌跡 3 から軌跡 6 では，誤分類が見られた．図 6 より，これらの軌跡では転折を行う前後の線の方向が違うために HoG 特徴の違いが生じている．そのため，転折を行う際に転折の方向にブレが生じてしまうと勾配方向が描画を指示された軌跡とは異なるため，分類精度に影響を与えたと考えられる．また，軌跡 3 から軌跡 6 が軌跡 1，2 へ誤分類されていない．転折が含まれることで描画方向が変わるため，輝度勾配も大きく変化する．よって，転折が含まれない軌跡 1，2 の HoG 特徴の値と，転折が含まれる軌跡 3 から 6 の HoG 特徴の値が大きく異なったため，誤分類が発生しなかったと考えられる．また，各軌跡で転折の角度が同一になった場合，軌跡ごとに勾配方向に差が生じない．そのため，転折角度が同一の場合においても分類精度に影響を与えたと考えられる．よって転折の角度も分類精度に影響を及ぼすことが考えられる．

4.2.2 座標群の特徴を用いた視線軌跡の形状推定

座標群から抽出した特徴が視線軌跡の形状推定に対して有効であるかを調査するために 3.5.7 項で述べた特徴を用いて視線軌跡の分類を行う．分析対象のデータとしては，4.2.1 項と同様に，120 個の視線軌跡を用いる．座標群を用いた形状推定では，特徴量の次元数が分割数に応じて多くなる．そのため，分類器としては，特徴量の次元数が多い場合でも対応することができる Random Forest による 10-分割交差検証により評価を行う．実験環境は 4.2.1 項と同様の環境である．

実験手順として，まず分割数ごとに F-measure を算出する．次に精度が最も高い分割数において 4.2.1 項の実験と同様に，Recall，Precision，F-measure を算出し評価を行う．分割数ごとの F-measure の値を図 9 に示す．

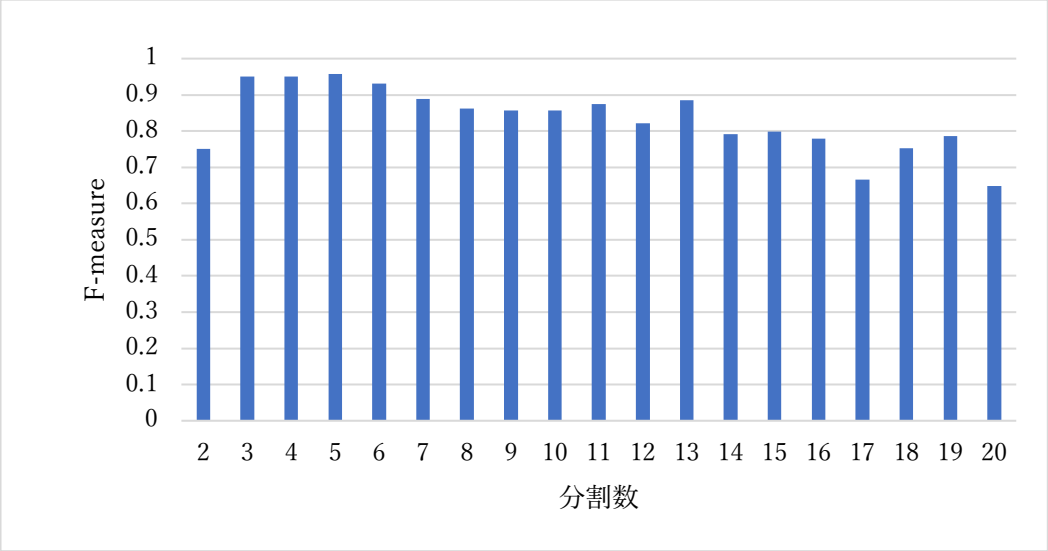


図 9 座標群を用いた分割数ごとの F-measure

Fig. 9 F-measure for each number of divisions using coordinates data

図 9 より，分割数が少ないほど F-measure の値が高くなる傾向が見られる．分割数が少なくなることで，描画した軌跡の大まかな形状のみが保持されつつ，注視や視線のブレが削除されたため，F-measure の値が高くなったと考えられる．しかし，分割数が極めて少なくなった場合，F-measure が減少している．分割数が少なくなることで，平均座標により軌跡の形状が保持しきれなくなったため F-measure に影響を及ぼしたと考えられる．また，分割数が増えるにつれて F-measure の値が低くなる傾向が見られる．分割数が増えることで，平均座標の数が多くなり，注視点やブレを削除しきれない可能性がある．それらが F-measure の値に影響を及ぼしたと考えられる．

次に F-measure の値が最も高くなった分割数が 5 の時の分類結果を表 7 に示す．太枠内は F-measure を示す．

表 7 座標群を用いた分類結果（分割数 : 5）

Table 7 The classification result using coordinates data (Number of divisions : 5)

		予測結果						Recall
		軌跡 1	軌跡 2	軌跡 3	軌跡 4	軌跡 5	軌跡 6	
								
正解ラベル		19	0	0	1	0	0	0.95
		0	20	0	0	0	0	1.00
		0	0	20	0	0	0	1.00
		1	0	2	19	0	0	0.95
		2	1	0	0	17	0	0.85
		0	0	1	0	0	19	0.95
Precision		0.86	0.95	0.95	0.95	1.00	1.00	0.96

表 7 より, 軌跡画像を用いた分類実験と比べ, F-measure, Recall, Precision の値が高くなった．一方，軌跡 1 の Precision と軌跡 5 の Recall が低くなった．実験で用いた特徴は視線軌跡を描画した全フレームをほぼ等しく分割し, 各分割フレームの平均座標の変化量を用いている. よって，分割数が少ないほど，平均座標により形成される形状が大まかな視線軌跡となる．また，注視により平均座標に偏りが見られることで形状が変わり分類精度に影響を与えたと考えられる．今回実験で用いた視線軌跡の形状は簡素なものであるため，分割数が少ない場合においても軌跡の形状が保持され，分類精度が高くなったと考えられる．今後はより複雑な図形を用いた場合において分割数が分類精度に与える影響を調査する必要がある．

表 6 より，HoG 特徴を形状推定に用いた場合，軌跡 1，2 の分類精度が非常に高くなった．しかし，軌跡 3 から軌跡 6 の分類精度が低くなり F-measure に影響を及ぼした．表 7 より，座標群を形状推定に用いた場合，軌跡 1 から軌跡 6 の分類精度が高くなり，表 6 の F-measure を大きく上回った．これらの結果より，HoG 特徴を用いた場合は形状により分類精度が異なったが，座標群を用いた場合は形状によらず高い精度で分類ができている．4.1.1 項と 4.1.2 項で行った実験結果から，提案手法の視線軌跡の形状推定においては，座標群を用いることが有効であることが示唆された．

4.2.3 異常検知アルゴリズムを用いた視線軌跡の形状識別

登録された視線軌跡の形状か否かを識別するための学習アルゴリズムとして異常検知アルゴリズムが有効かを調査するために，異常検知アルゴリズムである OCSVM (One Class SVM) と IForest (Isolation Forest) を用いて視線軌跡の形状識別を行った．本実験では，4.2.1 項と 4.2.2 項の実験に用いたデータと同様のデータを用いる．10-分割交差検証を行い，Precision，Recall，

Specificity，FAR，FRR，F-measure を用いて評価する．F-measure が最も高くなった分割数における識別結果を図 10 に示す．

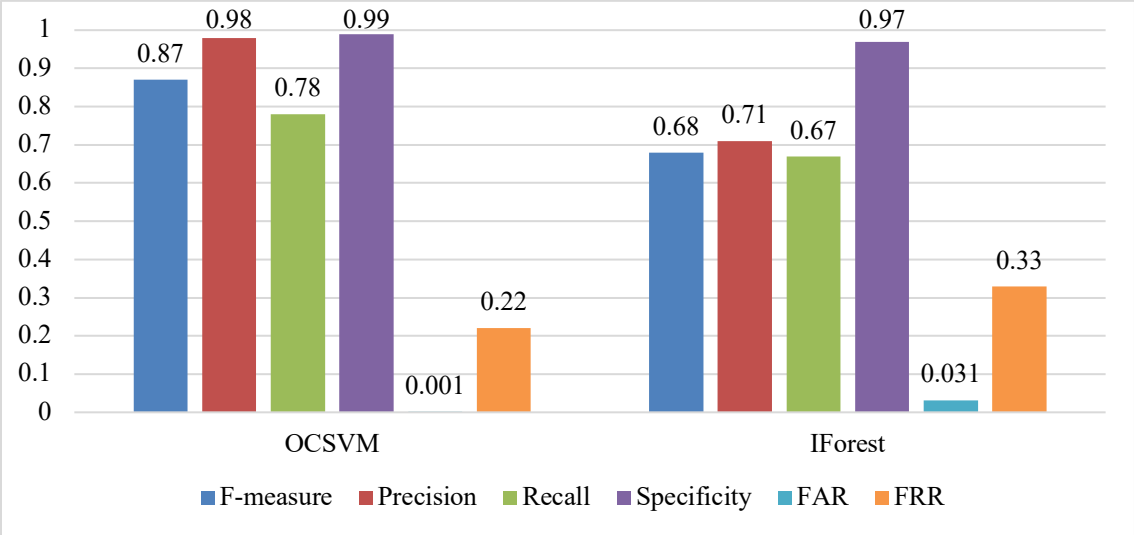


図 10 異常検知アルゴリズムごとの識別精度

Fig. 10 Identification accuracies for each error detection algorithm

図 10 より，今回用いた異常検知アルゴリズムにおいて，OCSVM を用いた場合，IForest と比較して F-measure，Precision，Recallm，Specificity が高くなった．また，FAR と FRR は低くなり OCSVM の方の識別精度が高くなった．どちらのアルゴリズムにおいても，FAR より FRR が高くなった．Precision，Recall の値から登録した軌跡と識別した正解率は高い一方で，実際に登録した形状と同じ形状の軌跡が拒否されている．Specificity，FAR，FRR の値から異なる形状であると識別した際の正解率が高く，誤って受けいれる確率が低い．しかし，登録した形状と同じ形状の軌跡を入力した際に拒否される確率が高いことがわかる．このような値になった理由として F-measure が最高になった際の分割数は 3 であり，特徴量の次元数が分割数に伴い少なくなったため，特徴量の値が類似し登録した形状の軌跡を誤って拒否したと考えられる．実験結果から，形状による認証における学習アルゴリズムとして OCSVM が有効であることが示唆された．

4.3 描画特徴による認証に関する評価実験

本節では，提案手法における描画特徴による認証に関する評価実験について述べる．

4.3.1 大域的な描画特徴を用いた個人分類による特徴量の検討

描画特徴の個人分類に対する有効性を調査するために，3.6 節で挙げた特徴を用いて，Random Forest による 3-分割交差検証によって図 8 で示した被験者 A，B，C の分類を行った．被験者には図 7 の図形を 30 回描画するように指示した．図 7 は本研究で想定する直線と転折を全て含んだ図形であるため，描画特徴の有効性を検討する上で適切な図形であると考えた．視線軌跡を描画した全フレームを特定のフレームごとに分割し，分割数ごとの F-measure の算出を行った．視線軌跡の分割数と個人分類の精度の関係について評価を行った．また，特徴量の重要度を算出し，有効な特徴量の検討を行った．実験環境は表 10 と同様である．特徴量ごとに重要度を算出し，高い順に並べた結果を表 8 に示す．

表 8 重要度が高い順に並べた特徴量

Table 8 Features in order of variable importance

特徴量の名称	変数重要度
x 座標の標準偏差	0.56
x 座標の分散	0.30
y 座標の標準偏差	0.23
y 座標の分散	0.17
描画時間	0.15
x，*y* 座標の変化量	0 ~ 0.09

今回の実験では，視線軌跡の *x* 座標の標準偏差と分散が *y* 座標の標準偏差と分散より重要度が高くなった．図 8 より，被験者 B は他の被験者と比べ視線軌跡の横幅が大きい．よって，水平方向に対応する *x* 座標の標準偏差と分散が被験者間で個人差に影響を与えたため，重要度が高くなったと考えられる．また，*x*，*y* 座標の変化量については，各次元に対して重要度が算出されるため，重要度が低くなったと考えられる．今回用いた特徴量の一つである，*x*，*y* 座標の変化量は描画した視線軌跡の全フレームを分割，平均化し変化量を求めている．そのため，転折や注視の視線移動の情報が含まれている．これらの情報が個人分類においてノイズになると考えられる．図 11 に分割数ごとに算出した F-measure の値を示す．

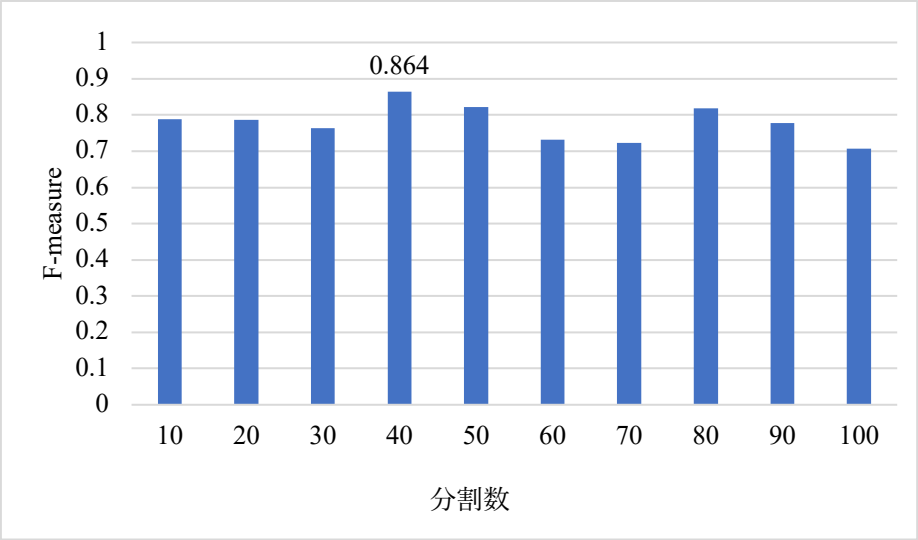


図 11 分割数ごとの F-measure

Fig. 11 F-measure for each number of divisions

図 11 より，分割数が 40 の時に F-measure の値が最大となった．分割数が少ない場合，注視点がスムージングされ，転折の形状も元データとは異なる形状となる．また，分割数が多い場合，注視点を正確に検出することができる．しかし，元データの形状に近づくため，細かい視線のブレが生じ，これらがノイズとなったため分類精度に影響したと考えられる．

4.3.2 大域的な描画特徴を用いた個人識別

描画特徴による認証に用いる特徴量の有効性を評価するために，One Class SVM と Isolation Forest を用いて個人識別を行う. 各被験者 5 名には図 7 の図形を 30 回描画するように指示した. 本実験に用いる特徴量は 4.3.1 項で行った実験と同様の特徴量を用いる．また，分割数は 4.3.1 項で行った実験において F-measure が最大になったときの 40 に設定する．前述の異常検知アルゴリズムを用いて本人か否かを識別し，識別精度を F-measure, Precision, Recall, Specificity, FAR, FRR により評価を行う. 識別精度の算出として，まず被験者一人のデータを学習データとして，その他の被験者のデータを評価データとし，他人を他人であると識別するテストを行う．次に，同様の被験者のデータを用いて 10-分割交差検証を行い，本人を本人であると識別するテストを行う．これにより，被験者一人のデータを用いた際の F-measure，Precision，Recall，Specificity，FAR, FRR を算出し, 同様の手順を各被験者分行う. 最後に F-measure, Precision, Recall, Specificity, FAR，FRR それぞれの平均を算出することで識別精度を算出する．異常検知アルゴリズムごとの識別結果を表に示す.

表 9 異常検知アルゴリズムごとの識別精度
Table 9 Identification accuracies for each error detection algorithm

	One Class SVM	Isolation Forest
F-measure	0.35	0.42
Precision	0.36	0.30
Recall	0.50	0.81
Specificity	0.49	0.43
FAR	0.50	0.58
FRR	0.50	0.19

One Class SVM を用いた際の識別結果として，F-measure は 0.35，Precision は 0.36，Recall は 0.50，FAR が 0.50，FRR が 0.50 となり，Isolation Forest を用いた識別結果として，F-measure は 0.73，Precision は 0.75，Recall は 0.75，FAR が 0.58，FRR が 0.27 となった．認証に用いる制度としては不十分であるという結果となった．このような結果になった理由として，今回用いた特徴量の一つである，x，y 座標の変化量は描画した視線軌跡の全フレームの情報を用いているため，余分な情報が含まれており，個人を識別するための特徴が十分に出なかったためであると考える．そのため，精度向上するためには余分な情報を削除し，個人の特徴がより現れる特徴量を抽出する必要がある.

4.3.3 局所的な描画特徴を用いた個人分類による特徴量の検討

注視とサッケードに関する特徴の個人分類に対する有効性を評価するために，Random Forest による 10-分割交差検証を行い，被験者 5 名の分類を行った．各被験者に図 7 に示す図形を 30 回描画するように指示した．表 5 に個人分類に用いる局所的な特徴量を挙げる．これらの特徴量を用いて分類を行い F-measure を算出し比較することで，分類精度の評価を行う．加えて，変数重要度を算出することで，有効な特徴量を検討する．実験環境を表 10 に示す.

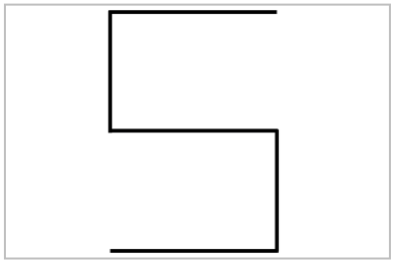


図 12 被験者に描画を指示した図形

Fig. 12 A trajectory that the subject was instructed to draw

表 10 実験環境

Table 10 Experimental environment

項目名	仕様
CPU	Intel Core i5 2.4GHz
OS	macOS Catalina10.15.2
言語環境	Python3.4.5
使用ライブラリ	scikit-learn0.18.1

局所的な特徴量を用いた場合と，4.3.1 項で行った大域的な特徴量を用いた場合のそれぞれの分類結果を図 13 に示す．

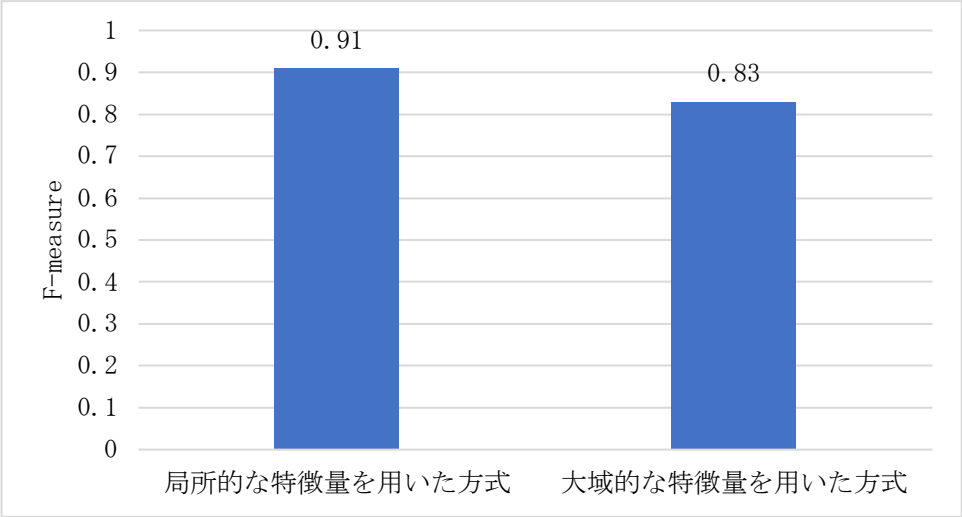


図 13 個人分類の結果

Fig. 13 A result of personal classification

局所的な特徴量を用いた方式の分類精度は，F-measure が 0.91，大域的な特徴量を用いた方式の分類精度は 0.83 となり，分類精度が向上した．提案手法で抽出した注視とサッケードに関する特徴量は，冗長な情報が含まれていない．そのため分類精度が高くなったと考えられる．

提案手法の変数重要度が高い上位 10 個の特徴量を表 11 に示す．

表 11 個人分類に用いた特徴量の変数重要度

Table 11 Variable importance of features used for personal classification

特徴量	変数重要度	
	局所的な特徴量を用いた方式	大域的な特徴量を用いた方式
x 座標の標準偏差	1.99	0.56
x 座標の分散	1.69	0.30
x 方向のサッケードの最小速度	1.48	-
x 方向のサッケードの平均速度	0.62	-
描画時間	0.61	0.15
x 方向のサッケードの最大速度	0.55	-
y 方向のサッケードの平均速度	0.45	-
y 方向のサッケードの最小速度	0.44	-
y 座標の分散	0.36	0.17
y 方向のサッケードの最大速度	0.35	-

表 11 より，サッケードに関する特徴量の変数重要度が高く，サッケードが分類に寄与していることが示された．しかし，注視に関する特徴量の変数重要度が低く表 11 に示す上位 10 個に含まれていないため，注視が分類精度に寄与していない結果となった．そこで，3.6.2 項で述べたように，注視の特徴量を抽出する際に 5 フレーム以上視線が密集していた箇所を注視箇所とした. よって, 短時間の注視の場合, 5 フレーム未満の注視は注視箇所として検出されないため, 注視の個人特徴が十分に抽出できず，変数重要度の値が低くなったと考える．また，*x* 座標の分散や標準偏差などの提案手法で用いている帯域的な特徴量において，提案手法の変数重要度が高くなっている．4.3.1 項で用いていた平均座標群データの変化量は用いていないため，その他の特徴量が分類に寄与したためであると考えられる．

F-measure と変数重要度による評価の結果から，局所的な視線移動の特徴が個人分類に対して有効であることが示唆された．よって分類精度を向上させるために，視線軌跡の局所的な転折部分などの描画特徴を抽出し，追加する必要があると考える．

4.3.4 注視とサッケードの特徴を用いた個人識別

異常検知アルゴリズムの提案手法への有効性を評価するために，One Class SVM と Isolation Forest を用いて個人識別を行う. 各被験者 5 名には図 7 の図形を 30 回描画するように指示した. 本実験に用いる特徴量は表 5 に示した提案手法の特徴量を用いる．前述の異常検知アルゴリズムを用いて本人か否かを識別し，識別精度を F-measure，Precision，Recall，Specificity，FAR，FRR により評価を行う．識別精度の算出として，まず被験者一人のデータを学習データとして，その他の被験者のデータを評価データとし，他人を他人であると識別するテストを行う．次に，同様の被験者のデータを用いて 10-分割交差検証を行い, 本人を本人であると識別するテストを行う．これにより，被験者一人のデータを用いた際の F-measure，Precision，Recall，Specificity，FAR，FRR を算出し，同様の手順を各被験者分行う．最後に F-measure，Precision，Recall，Specificity，FAR，FRR それぞれの平均を算出することで識別精度を算出する．識別結果を表 12 に示す.

表 12 異常検知アルゴリズムごとの識別精度

Table 12 Identification accuracies for each error detection algorithm

	One Class SVM	Isolation Forest
F-measure	0.61	0.73
Precision	0.86	0.75
Recall	0.49	0.75
Specificity	0.97	0.91
FAR	0.03	0.08
FRR	0.51	0.27

One Class SVM を用いた際の識別結果として，F-measure は 0.61，Precision は 0.86，Recall は 0.49，FRR が 0.51 となり，本人を他人であると高確率で誤識別している．また，Specificity が 0.97，FAR が 0.03 となり，他人を高確率で拒否できている．Isolation Forest を用いた識別結果として，F-measure は 0.73，Precision は 0.75，Recall は 0.75，FRR が 0.27 となり，One Class SVM と比較して本人を本人であると高確率で識別している．また，Specificity が 0.91，FAR が 0.08 となり，One Class SVM を用いた場合と比較し低くなっているため，比較的高精度で本人を受け入れている．このような識別精度になった理由として，学習させる本人のデータが少なく，識別に有効な学習モデルが作成できなかったと考えられる．よって，学習データのサンプル数を増やすことが課題となる．これらの結果から比較的識別精度が高くなった Isolation Forest が提案手法の学習アルゴリズムとして有効であることが示唆された．

異常検知を用いた個人識別において，どの特徴量が有効であったかを検証するためにステップワイズ法を用いた特徴量選択を行った．ステップワイズ法とは，特徴量を一つずつ追加や削除を行い，最適な特徴量の組み合わせを探す特徴量選択の手法の一つである．今回はステップワイズ法における，特徴量なしの状態から 1 つずつ特徴量を選択し増やしていく変化増加法を用いた．特徴量選択の手順として，(1) まず始めに選ばれていない特徴量の中から一つ追加し個人識別を行い F-measure を算出する．(2) F-measure を算出した後に追加した特徴量を元に戻し別の特徴量を追加する．(3) (1)，(2) の手順を全ての特徴量を用いて行い，F-measure が最も高くなった特徴量を実際に追加する．手順 (1) に戻り手順 (1) ~ (3) を全ての特徴量を追加し終わるまで繰り返す. これらの手順により個人識別において, どの特徴量が有効であるかの評価を行う. 結果を図 14 に示す.

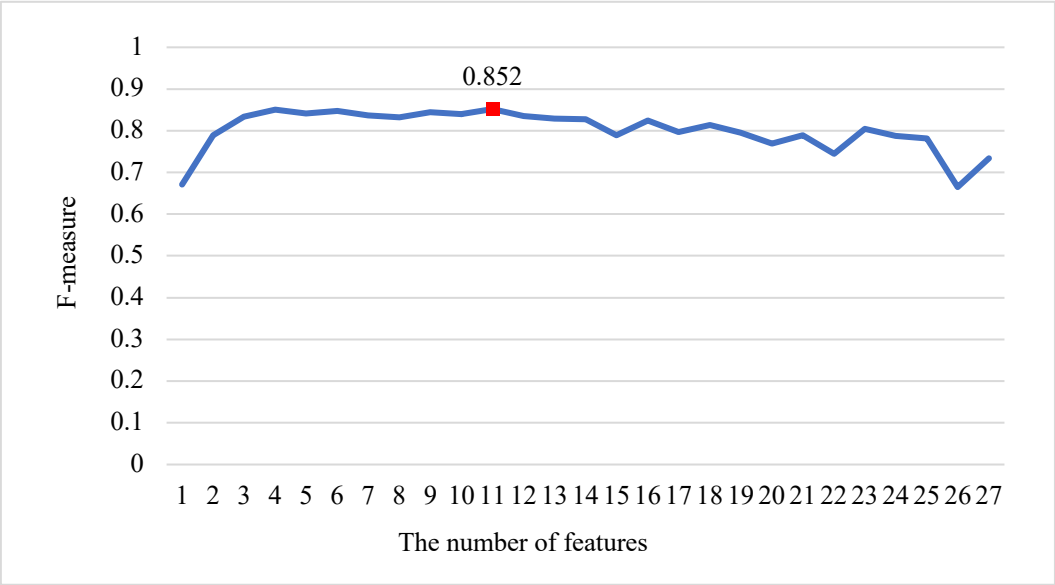


図 14 ステップワイズ法による F-measure と特徴量の遷移

Fig. 14 F-measure and features transitions by stepwise method

特徴量数が 11 の時に F-measure が 0.852 となり最大となった．この時の特徴量を表 13 に示す．また，特徴量は追加した順を昇順としている．

表 13 F-measure が最大の時の特徴量一覧

Table 13 List of features when F-measure is maximum

追加順	特徴量
1	x 座標の標準偏差
2	描画時間
3	y 座標の標準偏差
4	y 方向のサッケードの平均速度
5	注視回数
6	x 方向のサッケードの最小速度
7	x 座標の注視の分散の最小値
8	x 方向のサッケードの最大速度
9	x 座標の注視の標準偏差の最小値
10	y 座標の分散
11	x 座標の分散

表 13 からこれらの特徴量が個人識別において有効であることが示された．結果として，注視とサッケードの特徴が有効である特徴量に含まれている．しかし，今回有効であった注視とサッケードの特徴量の数は 22 次元のうちの 6 次元である．提案手法において，注視とサッケードの特徴がより有効であると示すには特徴量を再検討し，個人識別に有効である特徴量を追加する必要がある．

4.4 学習データの水増し手法の検討

4.3.4 項で行った実験から，学習データの不足が課題として挙げられた．また，視線で軌跡を描画するという行為は人間が普段行わない行為である．そのため，認証情報を登録する際に複数回軌跡を入力することはユーザに対して負担が大きいと考える．そこで，少ない学習データで個人を高精度で識別するために，学習する認証者本人のデータの水増しを検討する．データの水増しを行う手法として，オーバーサンプリングが挙げられる．オーバーサンプリングとは，クラス間においてデータ数に偏りのある不均衡なデータにおいて，データ数が少ないクラスのデータ数を増幅する手法である．個人認証の研究に用いられているオーバーサンプリングの手法として，SMOTE (Synthetic Minority Over-sampling Technique) がある[38], [39]．SMOTE とは，k-近傍法を用いて得た近傍の同クラスの訓練データとの間に新たな訓練データを生成する手法である[40].

4.4.1 SMOTE を用いた個人識別

SMOTE を用いて学習データ数を増やし，被験者 5 名の個人識別を行う．提案手法に用いるデータ数は各被験者 30 である．また，SMOTE により学習データの数を 30 から 120 へ増加し，実験では，本のデータが 120，他人のデータが 120 とする．Isolation Forest を用いた 10-分割交差検証を行い，F-measure，Precision，Recall，Specificity，FAR，FRR による評価を行う．実験の手順として，まず被験者一人を本人と設定して本人のデータに対し SMOTE を適用しデータ数を 30 から 120 に増加する．増加したデータを学習させ，4.2 節で行った実験と同様の手順で個人識別を行い，これらの手順を各被験者分繰り返す．最後に各識別において算出された識別精度の平均を算出することでこの実験の識別精度を算出する．SMOTE の適用の有無で識別精度を比較し，評価を行う．識別結果を表 14 に示す.

表 14 SMOTE の適用の有無による識別結果
Table 14 Identification results with and without SMOTE

	SMOTE 無し	SMOTE あり
F-measure	0.73	0.88
Precision	0.75	0.96
Recall	0.75	0.82
Specificity	0.91	0.99
FAR	0.08	0.01
FRR	0.27	0.17

SMOTE の適用が無しの識別結果は，4.2 節で行った実験の Isolation Forest を用いた際の識別精度と同様である．SMOTE を適用した際の識別精度は F-measure が 0.88，Precision が 0.96，Recall が 0.82, FRR が 0.17 となり適用しなかった場合と比較して本人を高精度で識別している．また，Specificity が 0.99，FAR が 0.01 となり，他人を高精度で拒否できている．学習データ数の増加識別精度に寄与していると考えられる．実験結果から，SMOTE による学習データの増加が提案手法に有効であることが示唆された．一方で，FRR が FAR と比較して高いため，認証者本人が高確率で拒否されている．同じ被験者の中でも，安定して同じ視線軌跡を再現できていないと考えられる．よって，識別精度を向上するためには，視線軌跡の入力方法を再検討し，被験者が視線軌跡を安定して再現する必要がある．

4.5 視線軌跡描画時におけるガイドの検討

視線軌跡を描画する際に画面上にどのような軌跡を描画したかを表示しないことで，覗き見に対して頑健になる．しかし，画面に何も表示しない場合，ユーザが入力を行う際にどの位置にどのように描画しているか把握できない．さらに，視線で軌跡を描画する行為は日常的に行わない行為であるため，視線軌跡の入力負担が大きくなると考える．入力負担が大きくなると，認証情報として登録した視線軌跡を再現することが困難になり，認証において本人が他人として識別されることが考えられる．よって，提案手法において視線軌跡の描画の入力負担を軽減する必要があると考える．提案手法では視線軌跡の入力を行う際に画面上にガイドを表示することで視線奇跡の入力負担を軽減できると考える．そこで，入力時に画面上に表示するガイドの検討を行う．描画ガイドとして，覗き見による認証情報の漏洩に対して頑健にするために，認証情報のヒントとなる情報を表示しないことが望ましい．そのため，登録した視線軌跡を表示することは提案手法には適さない．また，なぞるだけで登録した視線軌跡を描画できるガイドも提案手法には適さないと考える．

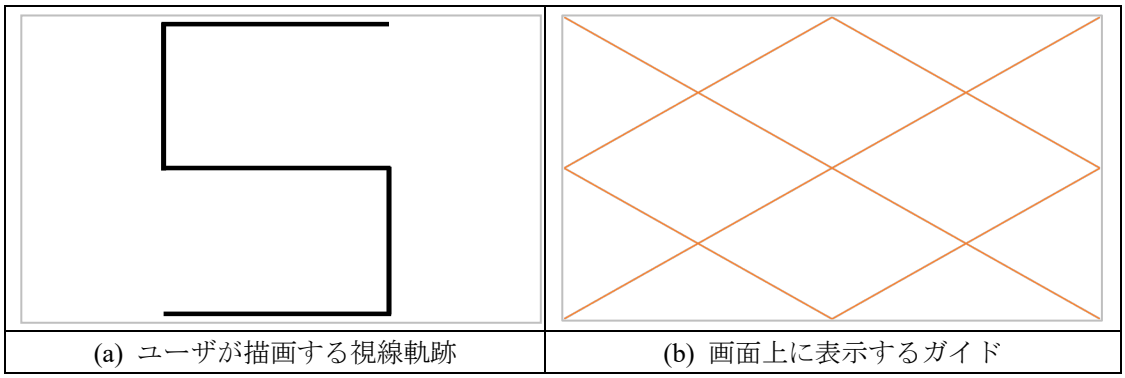
4.5.1 DTW (Dynamic Time Warping)

本研究では，ガイドが視線軌跡の描画に有効であるか調査をする分析を行う．有効性を調査するにあたり，ユーザが視線軌跡を再現できているかを分析する必要がある．そこで，分析に DTW (Dynamic Time Warping) を用いる．DTW とは，2 つの時系列データの各店の距離を総当たりで算出し最短となる距離を求める手法である[41]．DTW により，長さや周期の異なる時系列データの類似度の算出が可能である．DTW を用いて求められる距離を DTW 距離と呼ぶ．データ長が m の時系列データ $X = (x_1, x_2, \ldots x_m)$ とデータ長が n の時系列データ $Y = (y_1, y_2, \ldots y_n)$ の DTW 距離 $D(x, y)$ は式 (7) で定義される．本研究では，DTW 距離を用いてユーザが視線軌跡を再現できているか分析を行う．

$$
\begin{gathered}
D(x,y) = d(m,n), \\
d(0,0) = 0, \\
d(i,0) = d(0,j) = \infty \\
d(i,j) = \sqrt{\left(x_i - y_j\right)^2} + min\begin{cases} d(i,j-1) \\ d(i-1,j) \\ d(i-1,j-1), \end{cases} \\
(i = 1, \ldots, m;\ j = 1, \ldots, n).
\end{gathered}
\tag{7}
$$

4.5.2 DTW 距離を用いたガイドの視線軌跡描画に対する有効性調査

視線軌跡描画に対するガイドの有効性調査を目的として，視線軌跡の DTW 距離を算出し，比較することで有効性の評価を行った．被験者は 20 代の大学生 5 名である．実験に用いるデータとして，ガイドの表示しない状態と表示した状態のそれぞれで 10 個のデータを収集した．本実験において設定したユーザが描画する軌跡と画面上に表示するガイドを図に示す．被験者にはガイドの使い方については自由に使うように指示をした．



(a) ユーザが描画する視線軌跡　　(b) 画面上に表示するガイド

図 15 ユーザが描画する視線軌跡と表示するガイド

Fig. 15 Eye movement trajectory to be drawn by users and guide to be displayed

実験手順として，まず始めに 1 つの視線軌跡を選択しその他の視線軌跡との DTW 距離の平均を算出する．次にこの手順を描く軌跡においてこの手順でそれぞれの DTW 距離の平均を算出する．最後に算出された全ての DTW 距離の平均から全体の平均を求めることで評価に用いる DTW 距離の算出を行う．実験結果を表 15 示す．

表 15 被験者ごとの DTW 距離

Table 15 Dynamic time warping distances for each subject

	ガイド無し	ガイド有り
被験者 A	9910	8187
被験者 B	26803	10542
被験者 C	8592	7389
被験者 D	11864	5571
被験者 E	9036	8082

実験結果として，ガイド無しに比べガイド有りの状態で描画された視線軌跡の DTW 距離が低くなった．ガイドを表示させることで被験者が視線軌跡を描画する際に，ガイドのどのポイントを用いるかを被験者自身が描画しやすくなるように決めることができた．また，全被験者において個人差があるが DTW 距離の減少が見られた．DTW 距離が減少したということは入力した軌跡が類似していると言える．実験の結果から，視線軌跡の描画時にガイドを表示させることが描画負担の軽減に有効性が示唆された．

4.5.3 描画ガイドを用いた個人識別

描画ガイドを用いて入力した視線軌跡による個人識別の精度評価のために，図 15 で示した軌跡とガイドを用いてデータ収集を行った．収集したデータを用いて被験者 5 名の識別を行った．実験手順は 4.4.1 項で行った実験と同様である．Isolation Forest を用いた 10-分割交差検証を行い，F-measure，Precision，Recall，Specificity，FAR，FRR を用いて評価を行った．SMOTE による本人データの水増しを行う数による F-measure の遷移を図 11 に示す．

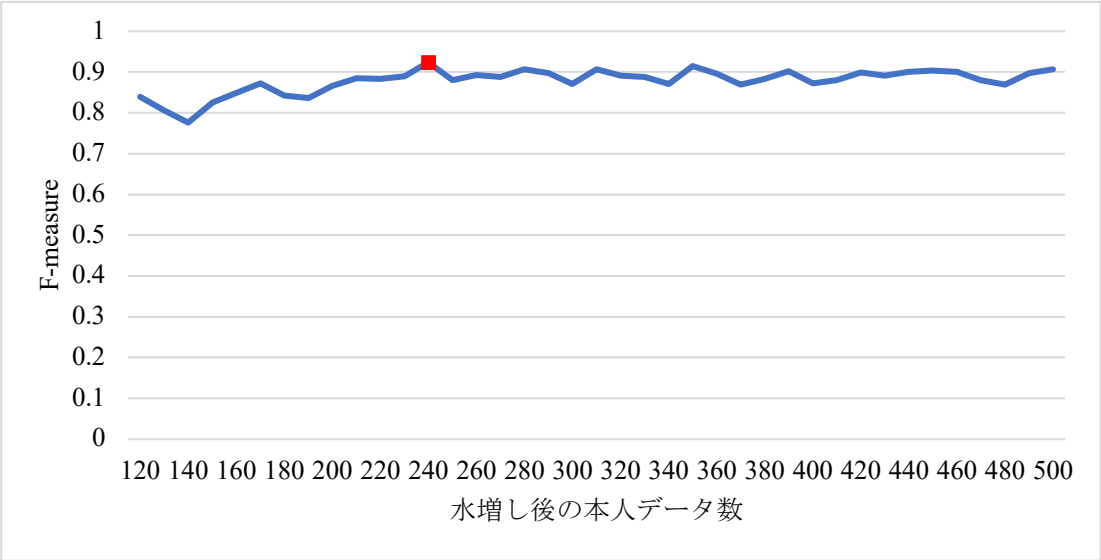


図 16 水増し数による識別精度

Fig. 16 Identification accuracies by number of augments

図 16 から，水増し後の本人データ数が 240 のときに F-measure が最大となった．このときの F-measure，Precision，Recall，Specificity，FAR，FRR を表 16 に示す．図 16 において F-measure が最大となった時に IForest のハイパーパラメータである contamination を変化させ，FAR と FRR を算出した．contamination とはデータ中の異常なデータの割合を設定する値である．contamination の変化による FAR と FRR を図 17 に示す．

表 16 識別結果

Table 16 A result of identification

F-measure	Precision	Recall	Specificity	FAR	FRR
0.92	0.89	0.96	0.97	0.03	0.04

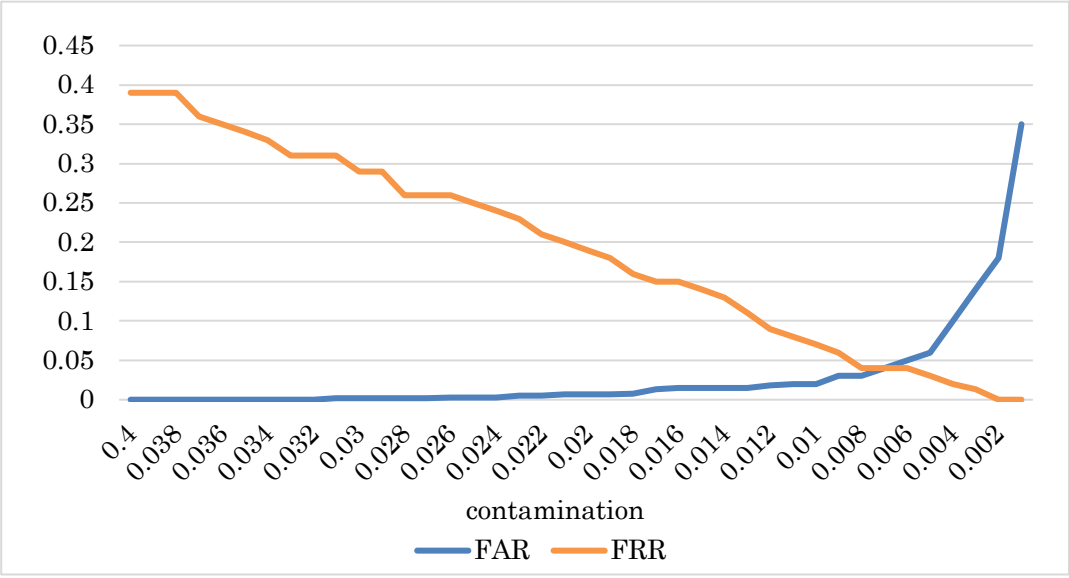


図 17 FAR と FRR

Fig. 17 FARs and FRRs

4.4.1 項で行った実験と比較し，FRR が低下したため本人が拒否される確率が低下した．また，FAR が増加したためわずかであるが他人が本人であると誤識別される確率が増加した．また，F-measure，Precision，Recall，Specificity が約 9 割となり，本人を本人である，他人を他人であると高精度で識別していることが分かる．図 17 から，EER が 0.04 となった．結果から，描画特徴による認証において，4%の確率で誤識別が発生することがわかる．ガイドを表示することにより被験者が視線軌跡を再現することができたと考えられる．一方で，今回用いたガイドには複雑性がないため複数の被験者において描画の際のガイドの使い方が類似したため他人を本人であると識別されたと考えられる．複雑なガイドを表示する場合，入力時のユーザに対する情報量が増え視線軌跡の入力の妨げになるとことが考えられる．そのため，ガイドは可能な限りシンプルなものが望ましい．その上で，高精度で識別するために描画特徴を再検討する必要がある．

第5章　結言

5.1　まとめ

本研究では，知識認証の脆弱性である認証時の入力の覗き見と推測，バイオメトリクス認証の脆弱性である認証情報の偽造と認証情報の変更が不可であることを解決する認証手法の提案が最終目的である．本論文では，最終目的の達成に向けてユーザ自身が定義した視線軌跡を用いた個人認証手法の提案を研究目的として設定した．提案手法では，視線軌跡の形状による認証と描画特徴による認証を行う．それぞれの認証において，視線軌跡のデータとして収集できる座標群のデータを用いる．形状による認証において，座標群の変化量を特徴量として認証に用いる．描画特徴による認証において，局所的な視線移動である注視とサッケードの特徴を認証に用いる．また，提案手法は個人のモバイル端末に適用する 1 対 1 認証を想定しているため，学習アルゴリズムとして異常検知アルゴリズムを用いる．

視線軌跡の形状による認証に用いるデータとして，軌跡画像と座標群データが挙げられる．それぞれのデータから抽出できる特徴量を用いて 6 種の軌跡の分類を行い，精度を比較することで特徴量の検討を行った．軌跡画像の特徴量を用いた場合の F-measure が 0.72，座標群データを用いた場合の F-measure が 0.96 となった．結果から座標群データの変化量が形状による認証に有効な特徴量であることが示唆された．学習アルゴリズムの検討として，異常検知アルゴリズムである One Class SVM と Isolatin Forest を用いて入力された視線軌跡から登録されたユーザか否かの識別を行った．結果として，One Class SVM を用いた方の識別精度が高くなったため，One Class SVM が形状による認証における学習アルゴリズムとして有効であることが示唆された．

描画特徴による認証に用いる特徴量の検討として，大域的な特徴量と局所的な特徴量を用いて被験者 5 名の個人分類を行った．大域的な特徴量である座標群の変化量を用いた場合の F-measure が 0.83, 局所的な特徴量である注視とサッケードの特徴を用いた場合の F-measure が 0.91 となり，描画特徴による認証において局所的な特徴量が有効であることが示唆された．描画特徴による認証に用いる学習アルゴリズムの検討として，異常検知アルゴリズムである One Class SVM と Isolatin Forest を用いて 5 名の被験者の識別を行った．One Class SVM を用いた際の識別結果として，F-measure は 0.61，Precision は 0.86，Recall は 0.49，FAR が 0.03，FRR が 0.51 となり，Isolation Forest を用いた識別結果として，F-measure は 0.73，Precision は 0.75，Recall は 0.75，FAR が 0.08，FRR が 0.27 となった．Isolation Forest を用いた方が高精度で識別できているため描画特徴による認証に用いる学習アルゴリズムとして Isolation Forest が有効であることが示唆された．しかし，識別精度が低いことが課題として挙げられた．そこで精度向上のために SMOTE を用いて学習データの数を 30 から 120 へ水増しを行い，個人識別を行った．結果として，識別精度は F-measure が 0.88，FRR が 0.17 となり精度が向上した．よって SMOTE が提案手法に有効であることが示唆された．しかし，FRR が高く本人が高確率で拒否されている．この理由として被験者が同じ軌跡を再現できていないことが原因であると考えた．そこで，入力時に描画ガイドを表示させた状態で描画した視線軌跡のデータを用いて個人識別を行った．結果として，F-measure が 0.92，FAR が 0.03，FRR が 0.04 となり FRR の低下をさせることができた．描画ガイドを用いることが提案手法において有効であることが示唆された．

5.2 今後の課題と展望

今後の展望として，形状による認証においては，複雑な形状の考慮が挙げられる．また，描画特徴による認証においては，注視とサッケードの特徴量の再検討が挙げられる．さらに提案手法全体としては，最適な描画ガイドの検討が挙げられる．

まず始めに複雑な形状の考慮として，本研究では，形状による認証の精度評価の実験として，転折と直線を含む基本的な図形のみを用いて形状識別を行った．9 割近くの精度が得られ，提案手法の有効性を示したが，実際に認証を用いる場合は複雑な図形を描画し認証情報として登録することが想定される．したがって，今後は複雑な図形を用いた際の形状識別の精度評価と特徴量の再検討をする必要がある．本研究で用いた視線軌跡は基本的な形状の軌跡であるため，基本的な形状を組み合わせ構成される複雑な形状を用いる場合，本研究の知見を生かすことができると考える．

次に注視とサッケードの特徴量の再検討について，4.3.4 項で行った実験において個人識別に有効であった注視とサッケードの特徴量が少なかった．一方で有効な特徴量もいくつかあったため，個人識別の精度向上のために注視とサッケードの特徴量やその他の特徴量を再検討し追加する必要があると考える．

最後に最適な描画ガイドの検討として，今回行った描画ガイドの有効性調査において，登録した軌跡をそのまま表示しない，なぞるだけで軌跡を描画できるガイドを表示しない，という条件のもとで描画ガイドを設定した．提案手法で実際に認証を行う場合にもこの条件を満たしたガイドを用いることが望ましいと考える．提案手法で用いる視線軌跡はユーザ自身が定義した形状を用いるため，どのような軌跡に対しても条件を満たし，かつユーザの入力負担を軽減できるような描画ガイドを検討する必要がある．また，提案手法はノートパソコンやスマートフォンなどのモバイル端末への適用を想定しているため，端末ごとに適用する描画ガイドの検討も必要であると考える．

謝辞

本研究を進めるにあたり，3 年間論文や発表資料の添削，ゼミにおいて熱心にご指導していただいた本学白石陽教授に深く感謝申し上げます．研究の進め方や論文のまとめ方，研究に対する議論のやり方，プレゼンテーション方法を日頃のゼミや発表を通して実感しております．また，本論文の審査を担当していただいた本学稲村浩教授，中村嘉隆准教授に厚くお礼を申し上げます．そして，本学角康之教授，本学竹川佳成准教授には実験場所と実験機材を快く提供していただき心より感謝申し上げます．本学卒業生の東爵亜久さんには学部 4 年時に実験協力に加え実験場所の管理をして頂きました．重ねてお礼を申し上げます．白石研究室で共に研究をした，横山達也さん，武安裕輔さん，渡辺泰伎さん，橋本智広さん，岩佐和真さん，多賀広奈さん，若林勇汰さん，岩崎賢太さん，青地美桜さん，細川諒さん，若園裕太さん，山田楓也さん，安本詞音さん, 山本浩貴さんには, 研究内容について数多くの知見やアドバイスをいただきました. また，お忙しい中にも関わらず，実験に協力して頂き大変感謝しております．本研究を進めるにあたりとても多くの人と関わりお世話になりました．みなさまのおかげで本論文を書き上げることができました．最後にお世話になりました全ての方へ重ねて感謝申し上げます．

発表・採録実績

発表

[I] 藤本巧海，白石陽：視線軌跡の形状と描画特徴を用いた個人認証手法の検討，情報処理学会，マルチメディア，分散，協調とモバイルシンポジウム 2019 論文集，Vol.2019，pp.1423-1432 (2019). 「査読付き」

[II] 藤本巧海，渡辺泰伎，白石陽：視線軌跡描画における注視とサッケードの特徴を用いた個人認証手法の検討，情報処理学会研究報告コンピュータセキュリティ(CSEC)，Vol.2020-CSEC-88，No.44，pp.1-8 (2020).

[III] T. Fujimoto and Y. Shiraishi：A Proposal of Personal Authentication Method Based onEye Movement Trajectory withFixation and Saccade Features", In Proceedings of the International Workshop on Informatics 2020, pp.141-148 (2020). 「査読付き」

採録

[I] T. Fujimoto and Y. Shiraishi : A Personal Authentication Method Based on Eye Movement Trajectory, International Journal of Informatics Society (IJIS), Vol.13 (2021). (to appear)

参考文献

[1] 総務省，情報通信動向調査令和元年，情報通信機器の普及状況 https://www.soumu.go.jp/johotsusintokei/statistics/data/200529_1.pdf，(参照 2020-11-08).

[2] 小島悠子, 山本匠, 西垣正勝：間違い探しを利用したワンタイム・パスワード型画像認証の提案, 情報処理学会研究報告マルチメディア通信と分散処理(DPS), Vol2007, No16, pp375-380 (2007).

[3] 徐強, 西垣政勝：ニーモニックに基づくワンタイム・パスワード型画像認証の実現可能性に関する検討, 情報処理学会研究報告マルチメディア通信と分散処理(DPS), Vol2006, No26, pp317-322 (2006).

[4] 稲村勝樹, 新林直樹：改良型パターンロック覗き見体制向上手法の提案と評価, 情報処理学会論文誌, Vol59, No.1, pp179-188 (2018).

[5] 長友誠, 朴美娘, 岡崎直宣：覗き見耐性を持つマウス操作を用いた個人認証方式の提案, 情報処理学会研究報告コンピュータセキュリティ(CSEC), Vol.2017-CSEC-78, No29, pp1-8 (2017).

[6] 山本涼太, 宮下芳明：イヤホンを用いたスマートフォンの操作と個人認証, 情報処理学会インタラクション 2013, Vol.2013-Intetraction (3EXB-17), pp.626-631 (2013).

[7] 森康洋, 高田哲司：スクロールとスライド操作による携帯端末向け個人認証, 情報処理学会インタラクション 2015, Vol.B27, pp.542-545 (2015).

[8] 白川功浩, 吉浦裕, 市野将嗣：虹彩および目の周辺の分割画像を用いた個人認証, 情報処理学会論文誌, Vol.59, No.9, pp.1726-1738 (2018).

[9] 藤田真浩, 眞野勇人, 佐野絢音, 高橋健太, 大木哲史, 西垣正勝：肌理を利用したマイクロ生体認証：ユーザビリティ向上のためのプロトタイプシステム改良, 情報処理学会コンピュータセキュリティシンポジウム 2017 論文集, Vol.2017, No.2, pp.704-711 (2017).

[10] 上松晴信，神田龍一，松井利樹，三宅優，伊藤康一，青木孝文：指間の線を利用した掌紋認証の提案，コンピュータセキュリティシンポジウム 2016 論文集，Vlo.2016，No.2, pp.185-191 (2016).

[11] C. Hegde, J.Phanindra, D. P. Shenoy, R. K. Venugopal and M. L. Patnaik : Human Authentication Using Finger Knuckle Print, Proceedings of the Fourth Annual ACM Bangalore Conference, pp.1-8 (2011).

[12] M. Nakakuni and H. Dozono : User Authentication Method for Computer-based Online Testing by Analysis of Keystroke Timing at the Input of a Family Name, 2018 International Conference on Computational Science and Computational Intelligence (CSCI), pp.71-76 (2018).

[13] Q. Zhou, Y. Yang, F. Hong, Y. Feng and Z. Guo : User Identification and Authentication Using Keystroke Dynamics with Acoustic Signal, 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), pp.445-449 (2016).

[14] H. Li, J. Yu and Q. Cao : Intelligent Walk Authentication: Implicit Authentication When You Walk with Smartphone, 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), pp.1113-1116 (2018).

[15] P. Musale, D. Baek, N. Werellagama, S.Woo and B. Choi : You Walk, We Authenticate: Lightweight Seamless Authentication Based on Gait in Wearable IoT Systems, IEEE Access, Vol.7, pp.37883-37895 (2019).

[16] A. Salem, D. Zaidan, A. Swidan and R. Saifan : Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices, 2016 Cybersecurity and Cyberforensics Conference (CCC), pp.15-21 (2016).

[17] 伊藤駿吾，白石陽：スマートフォンのフリック入力方式の特徴に注目した継続認証手法の提案，情報処理学会第 25 回マルチメディア通信と分散処理ワークショップ論文集，Vol.2017，pp.1-8 (2017).

[18] T. Kinnunenn, F. Sedlak and R. Bednarik : Towards Task-Independent Person Authentication Using Eye Movement Signals, Proceedings of the 2010 ACM Symposium on Eye-Tracking Research & Applications, ETRA'10, pp.187-190 (2010).

[19] Z. Ma, X. Wang, R. Ma, Z. Wang and J. Ma : Integrating Gaze Tracking and Head-Motion Prediction for Mobile Device Authentication: A Proof of Concept, Sensors (Basel, Switzerland), Vol.18, No.9 (2018).

[20] A. De Luca, R. Weiss and H. Drewes : Evaluation of Eye-Gaze Interaction Methods for Security Enhanced PIN-Entry, Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces, OZCHI'7, pp.199-202 (2007).

[21] M. Khamis, F. Alt, M. Hassib, E. Zezschwitz, R. Hasholzner and A. Bulling : GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices, Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp.2156-2164 (2016).

[22] 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デジタルコンテンツ(DCON)，Vol.4，No.2，pp.27-35 (2016).

[23] 藤本巧海，白石陽：視線軌跡の形状と描画特徴を用いた個人認証手法の検討，情報処理学会マルチメディア，分散．協調とモバイルシンポジウム論文集，Vol.2019，pp.1423-1432 (2019).

[24] Tobii Pro アイトラッカーの仕組み，tobii pro，https://www.tobiipro.com/ja/service-support/learning-center/eye-tracking-essentials/how-do-tobii-eye-trackers-work/ (参照 2019-05-06).

[25] 川上隼人, 笹田裕太, 五十嵐覚, 秋田純一：サッケード追尾可能な視線計測カメラの開発とそれを用いるインタラクションの可能性, 情報処理学会論文誌, Vol.56, No.4, pp.1174-1183 (2015).

[26] iPhone XR FaceID, Apple(日本), https://www.apple.com/jp/iphone-xr/face-id/ (参照 2019-02-15).

[27] Galaxy S9/S9+ 仕様, Galaxy Mobile Japan 公式サイト, https://www.galaxymobile.jp/galaxy-s9/specs/ (参照 2019-02-15).

[28] N. Dalal, B. Tringgs, C. Schmid, S. Soatto and C. Tomaso: Histograms of Oriented Gradients for Human Detection, International Conference on Computer Vision & Pattern Recognition (CVPR '05), Vol.1, pp.886-893 (2005).

[29] M. Oulla, A. Sadiq and S. Mbarki: Comparative Study of the Methods Using Haar-like Features, International Journal of Engineering Sciences & Research Tecnology, Vol.435, pp.35-43 (2015).

[30] D. Huang, C. Shan, M. Ardabilian and L. Chen: Local Binary Patterns and Its Application to Facial Image Analysis: A Survey, IEEE Transactions on Systems, Man, and Cybernetics, Part C, Vol.41, pp.765-781 (2011).

[31] 中村聡史，鈴木正明，小松孝徳：平仮名の平均手書き文字は綺麗，情報処理学会論文誌，Vol.57，No.12，pp.2599-2609 (2016).

[32] 鵜飼一彦：眼球運動とその種類，光学，Vol.23，No.1，pp.2-8 (1994).

[33] Q. Yang, P. M. Bucci and Z. Kapoula: The Latency of Saccades, Vergence, and Combined Eye Movements in Children and in Adults, Investigative Ophthalmology & Visual Science, Vol.43, No.9, pp.2939-2949 (2002).

[34] B. de Haas, A. L. lakovidis, D. S. Schwarzkopf and K. R. Gegenfurtner : Individual Differences in Visual Salience Vary Along Semantic Dimensions, Proceedings of the National Academy of Sciences," Vol.116, No.24, pp.11687-11692 (2019).

[35] G. Cargary, J. M. Bosten, P. T. Goodbourn, A. J. Lawrance-Owen, R. E. Hogg and J. D. Mollon : Individual Differences in Human Eye Movements: An Oculomotor Signature?, Vision Research, Vol.141, pp.157-169 (2017).

[36] 渡辺一彦，長友誠，油田健太郎，岡崎直宣，朴美娘：スマートロックにおける異常検知を用いた二つの端末の加速度における歩行認証の提案，情報処理学会マルチメディア，分散，協調とモバイルシンポジウム論文集，Vol.2019，pp.1155-1160 (2019).

[37] Bernhard Scholkopf, John C. Platt, John Shawa-Taylor, Alex J. Smola and Robert C. Williamson : Estimating the Support of a High-Dimensional Distribution, Neural Computation, Vol.13, No.7, pp.1443-1471 (2001).

[38] 味岡孝昇, 梅澤猛, 大澤範高 : 暗証番号入力時の腕の加速度を用いた携帯端末向け個人認証, 情報処理学会研究報告モバイルコンピューティングとパーベイシブシステム（MBL），Vol.2016-MBL-81，No.22，pp.1-6 (2016).

[39] 今野慎介，中村嘉隆，白石陽，高橋修 : 複数のウェアラブルセンサを用いた歩行動作による本人認証法の精度向上，情報処理学会論文誌，Vol.57，No.1，pp.109-122 (2016).

[40] N.V. Chawla and K.W. Bowyer : SMOTE: Synthetic Minority Over-sampling Technique, Journal of Article Intelligence Research, Vol.16, pp.321-357 (2002).

[41] Eamon J.Keogh and Michael J. Pazzani : Derivative Dynamic Time Warping, Proceedings of the 2001 SIAM International Conference on Data Mining, pp.1-11 (2001).

図目次

表目次