Regular Paper

A Personal Authentication Method Based on Eye Movement Trajectory

Takumi Fujimoto[*] and Yoh Shiraishi[**]

[*]Graduate School of Systems Information Science, Future University Hakodate, Japan
[**]School of Systems Information Science, Future University Hakodate, Japan
{g2119039, siraisi}@fun.ac.jp

Abstract – Password authentication and biometric authentication have become popular as personal authentication technology for mobile terminals. However, these technologies have weaknesses regarding security. In password authentication, authentication information can be leaked when one person surreptitiously looks at another's password. In biometric authentication, it is difficult to deal with impersonation when authentication information has been forged. In order to overcome these weaknesses, this study focuses on the user's eye movement. As an example of existing research, Kinnunen et al. proposed an authentication method using features of unconscious eye movement when users are viewing a video [1]. In this method, it is difficult to update the registered authentication information. De Luca et al. proposed a password authentication method in which the user inputs a PIN by looking at number keys shown on a display [2]. This method has the risk that its authentication information can be guessed. Our study proposes a personal authentication method based on eye movement trajectory when users draw, with their eyes, on the display of a mobile terminal. The proposed system performs authentication based on the shape of the user's eye movement trajectory and authentication based on its drawing features. We conducted an experiment to evaluate features relating to fixation and saccade that are effective for classifying users. Fixation is the eye movement which people hold the line of sights, and saccade is the rapid eye movement to change the position of the sight. In this experiment, we used these features to classify users. The experimental result showed the proposed method improved classification accuracy when compared to our previous method. It was suggested that the fixation and saccade features were effective for user classification. Next, we conducted an experiment to examine a learning algorithm suitable for the proposed method. In this experiment, we used One Class SVM and Isolation Forest for personal identification. The experimental result showed that Isolation Forest was effective for personal identification. In future work, we will consider a method to solve the lack of learning data for improvement of authentication accuracy. In addition, we need to investigate learning algorithms to improve identification accuracy.

Keywords: Personal authentication, Eye movement trajectory, Drawing feature, Classification of users, Error detection

1 INTRODUCTION

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 level of authentication on mobile terminals.

Password authentication and biometric authentication are popular means of personal authentication, and are also used for authentication on mobile terminals. Password authentication is authentication that uses the user's knowledge such as passwords and PINs. Password authentication information cannot get lost because it does not require a physical object such as an IC card or key. However, authentication information can be leaked when someone looks over another person's shoulder in a public space. This is an act of information theft that is possible even if the attacker does not have specialized knowledge. Therefore, authentication information can be leaked to anyone. In addition, if the authentication information of the number of digits is small, there is a risk that authentication information can be guessed.

Biometric authentication is authentication that uses a part of the body (physical features) and human behavior (behavioral features) as authentication information. Physical features are information of body parts that are unique such as fingerprints and faces. Behavioral features are information of human behavior that can be reproduced by a person. Biometric authentication is robust against over-the-shoulder information theft and incurs less burden, in that users do not need to remember authentication information. However, in authentication based on physical features, there is a risk that the physical features registered as authentication information may be forged. It is difficult to deal with impersonation if authentication information is forged, because information such as fingerprints and irises cannot be consciously altered. In authentication based on behavioral features, it is difficult to forge the authentication information because it does not use part of the body. Nevertheless, it is difficult to update authentication information consciously when unconscious habits are used as authentication information. If the authentication information is forged, it is difficult to deal with impersonation because users cannot update the authentication information. Therefore, biometric authentication has also difficulty dealing with impersonation if the biometric authentication information is forged once.

The weakness of password authentication is the ease of leakage of authentication information. In addition, the password authentication information be guessed easily. The weakness of biometric authentication is the difficulty of dealing with impersonation because it is difficult to update authentication information. These weaknesses must be overcome in order to perform secure authentication on mobile terminals. There are many works of research using physical

ISSN1883-4566

features or behavior features for authentication [3-8]. In addition, as examples of methods that are robust against over-the-shoulder information theft, there are studies using user eye movement for authentication [1], [2], [9-11]. We think user's eye movement prevents leakage of authentication information because it is difficult for others to observe eye movement. In addition, we think that it is difficult to guess the eye movement information. Also, user eye movement can be consciously reproduced. Authentication information can be updated by updating the user eye movement.

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 on a mobile terminal (eye movement trajectory). The goal of this study is to realize personal authentication that solves the problems with password and biometric authentication, by using user eye movement. In our previous research, we investigated the features for trajectory classification based on the shape of the eye movement trajectory, and feature values of drawing features [16]. As feature values for the shape of trajectory, we investigated features that can be extracted from images and coordinates data of trajectory. The results show that coordinates data are effective for the proposed method. We extracted global drawing features from eye movement trajectory for classifying users, but sufficient accuracy was not obtained. In this paper, we reexamined drawing features to improve the accuracy of personal authentication. In addition, we examined the learning algorithm for building an authentication model.

In section 2, we explain related works using behavioral features or eye movement for authentication. In section 3, we explain the details of the proposed method for personal authentication. In section 4, we explain the experiment to investigate the local eye movement features used in the proposed method and the effectiveness of the error detection algorithm for the proposed method. In section 5, we conclude this paper.

2 RELATED WORK

2.1 Authentication Based on Behavioral Features

There are studies using keystroke for authentication [3], [4]. Nakakuni et al propose a method that uses features of keystroke dynamics when users enter their surname for authentication [3]. In this method, it is thought that the input of a surname is highly reproducible and has a stable rhythm. Based on this hypothesis, the timing of the user's keystrokes is used for authentication. Zhou et al. used keystroke acoustic features in addition to keystroke dynamics features for authentication [4]. In this method, keystroke acoustics are collected with a microphone. In addition, they calculate MFCC (Mel-Frequency Cepstral Coefficients) by the acoustics and used for authentication.

There are studies using walking features for authentication [5], [6]. Li et al. use walking features while holding a mobile phone for authentication [5]. This method extracts features of walking by an accelerometer which is mounted on the mobile phone and calculates statistical features for authentication. Musale et al. extract leg and arm movement features during walking and use these features for authentication [6]. This method uses a smartwatch or smartphone to extract features related to human behavior. These features make it possible to classify users by a small number of features.

There are studies using the features of smartphone operation for authentication [7], [8]. Salem et al. use keystrokes as a second authentication factor when performing authentication with a touchscreen terminal [7]. In this method, they have developed a virtual keyboard and use features such as the timing and position of presses on the keyboard for authentication. Ito et al. have proposed an authentication method based on the features of the flick input method on smartphones [8]. Features such as flicking and shaking of the terminal during text input are used for continuous authentication.

These methods use unconscious habits and patterns that appear in each user's behavior as authentication information. Therefore, we think that it is difficult to update such authentication information and deal with impersonation.

2.2 Authentication Based on Eye Movement Features

There are studies using unconscious or conscious eye movement for authentication [1], [2], [9-11].

Kinnunen et al. propose an authentication method using features of unconscious eye movement when users are viewing a video [1]. Ma et al. have proposed an authentication method using eye movement and head movement [9]. In this method, authentication is performed by displaying random visual stimuli and measuring the unconscious eye movements and head movements with a camera.

These studies do not make users aware of authentication during authentication. However, in these methods, it will be difficult to update the registered authentication information. Therefore, we think that it is difficult to deal with impersonation.

As studies using conscious eye movement for authentication, there are studies performing authentication using password by eye movement [2], [10]. In addition, there is a study that performs authentication by having the user draw with their eye movement trajectory [11]. De Luca et al. proposed a password authentication method by gazing at PIN keys shown on a display [2]. In this method, the user enters a PIN code by gazing at numbers on the keypad shown on the display and authentication is performed. Khamis et al. have proposed a personal authentication method that combines passwords and eye movement information [10]. This method uses multimodal passwords with touch input and gaze direction (e.g., left-3-right-4) for authentication. In contrast, Mukai et al. have users draw a specified character with their eyes, and use the features of the eye movement trajectory for classifying users [11]. In this method, users select one of the characters from a set of characters to be used as the authentication information. This study uses characters and symbols that can be registered for authentication information. The features such as drawing time and drawing speed extracted from these characters are used for authentication. It is possible to update the authentication information by updating the characters registered as authentication information.

In these methods, it is possible to update authentication information and deal with impersonation. However, we think that in the methods used in [2] and [10], authentication information is simple if the number of authentication password digits is small. In the method used in [11], the characters that can be used as authentication information are limited. The methods in [10] and [11] use alphabets and numbers that are well known for everyone as authentication information. These authentication information can be guessed by attackers because alphabets and numbers are usually used by many users on a daily basis and are familiar for them. On the other hand, the proposed method uses the user's own defined eye movement trajectory as authentication information. It is difficult for an attacker to guess the authentication information of the proposed method because each user defines the trajectory information independently and the authentication information is not formed from well-known information such as alphabets and numbers. Accordingly, we think the proposed method are more robust for attackers compared to the methods in [10] and [11].

3 METHOD

3.1 Goal of Our Study

The goal of this study is to propose a personal authentication method based on the user's eye movement trajectory to overcome the weaknesses of password and biometric authentication. Our method prevents information theft or forgery because eye movement information is not visible. In addition, authentication information can be updated by updating eye movement, because the user's eye movement is consciously reproduced. Therefore, we think it is possible to deal with impersonation.

The proposed method consists of authentication based on the shape of the user's eye movement trajectory and authentication based on personal features when the user draws the eye movement trajectory (drawing features). The shape of the eye movement trajectory is defined by users and can be consciously updated by the users. We think that defining the shape of trajectory by users themselves makes difficult to guess the authentication information because authentication information does not depend on alphabets and numbers. If only the shape of the eye movement trajectory is used for authentication, there is a risk of impersonation because the shape of trajectory does not contain personal features. We introduce the authentication based on drawing features to makes the proposed method more robust against impersonation.

The goal of this paper is to investigate the combination of features related on local eye movement that are effective for the proposed method, and investigate learning algorithms suitable for 1:1 authentication.

3.2 Proposed System

In this section, we explain the structure of the proposed system. Fig. 1 shows an overview of the proposed system.

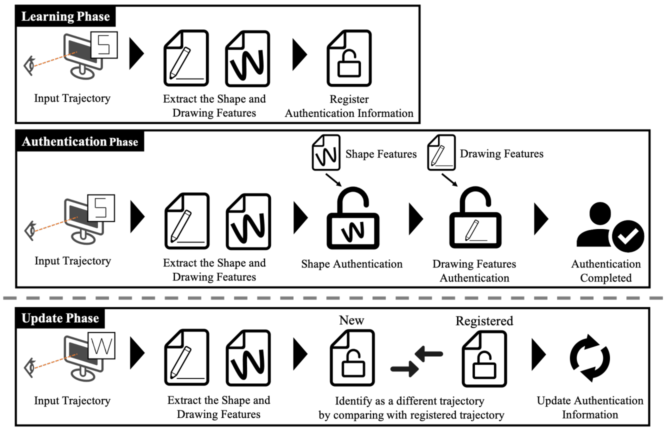

Learning Phase
Input Trajectory
Extract the Shape and Drawing Features
Register Authentication Information
Authentication Phase
Shape Features
Drawing Features
Input Trajectory
Extract the Shape and Drawing Features
Shape Authentication
Drawing Features Authentication
Authentication Completed
Update Phase
New
Registered
Input Trajectory
Extract the Shape and Drawing Features
Identify as a different trajectory by comparing with registered trajectory
Update Authentication Information

Figure 1: An overview of the proposed system

The proposed system consists of a learning phase, and an authentication phase and an update phase. Features are extracted from the eye movement trajectory and these features are used in each phase. The learning phase is the phase of creating the authentication information with multiple entries. Nothing is displayed on the screen during drawing the eye movement trajectory. During drawing the eye movement trajectory, neither authentication information nor guides for drawing the trajectory are displayed. Users input and register multiple eye movement trajectories. The shape and drawing features of the eye movement trajectory are extracted and registered as authentication information.

The authentication phase is the phase which authentication is performed. In this phase, users enter the eye movement trajectory registered on the learning phase on a blank screen for authentication. First, users perform the authentication based on the shape of the user's eye movement trajectory. If the authentication is successful, the authentication based on drawing features is performed as the next step. The authentication of the proposed method is completed by success of these two steps authentication.

The update phase is the phase which authentication information is updated. In the phase, users input eye movement trajectory which users want to newly register. After extracting features, the newly entered authentication information is compared with the registered authentication information. If the new trajectory is identified as a different trajectory, authentication information is updated.

3.3 Research Tasks and Approaches

The main research tasks of this paper are as follows:

- **Research task 1:** Selecting a measurement device to use in the proposed method.
- **Research task 2:** Investigating features which are effective for authentication based on shape.
- **Research task 3:** Investigating features which are effective for authentication based on drawing features.
- **Research task 4:** Investigating learning methods for 1:1 authentication.

The approaches to these research tasks are as follows:

Approach to research task 1

We use a contactless type device. As eyeline measurement devices, there are contact type devices such a glasses-shaped device, and contactless devices such as a desktop device [17]. We think contact type devices impose a burden, such as a sense of unfamiliarity and blocking of sight for users who do not normally wear glasses. In this study, we assume that the proposed method will use a camera on a mobile terminal to perform eye tracking in the future. If users use contactless type devices, the burden on the user during authentication is low because users are not required to wear the devices. Therefore, the proposed method uses a contactless type device.

Approach to research task 2

We use features that can be extracted from the coordinates data of the eye movement trajectory. Since the proposed system uses the eye movement trajectory defined by the user, it is necessary to estimate the shape of trajectory. In our previous study [16], we classified trajectories using each feature that can be extracted from coordinates data and images in order to investigate features that are effective for estimating the shape of trajectory. The F-measure of using coordinates data was 0.96 and the F-measure of using images was 0.72. The experimental results showed that coordinates data was effective for estimating the shape of trajectory.

Approach to research task 3

We use fixation and saccade features during eye movement for classifying users. We classify users in order to identify the registered users and protect against impersonation. In our previous study, we classified users by using the amount of change in the coordinates of all frames of the eye movement trajectory during drawing. However, some of the features were not effective for classifying users. In this paper, we extract fixation and saccade features from the user's eye movement trajectory. Fixation is the eye movement that make the line of sight move to fixing in position. Saccade is the rapid eye movement that change the points of sight. We think we can extract features which are more effective for classifying users, by detecting features of local eye movement.

Approach to research task 4

We use an error detection algorithm. Error detection is the method that learns only normal data and identifies whether unknown data is normal data or error data. There are 1:1 authentication and 1:N authentication, as authentication methods. 1:1 authentication uses only the user's data for learning and identifies whether the person attempting to access the device is the original user or attackers. 1:N authentication identifies the as one user from among all the registered users. The proposed method performs 1:1 authentication because we assume that the proposed method is applied to mobile terminals retained by people. Therefore, we think that the error detection algorithm is effective for the user identification in the proposed method.

In this paper, we focus on research tasks 3 and 4. We evaluate effectiveness of fixation and saccade feature for classifying users. In addition, we use One Class SVM (Support Vector Machine) and Isolation Forest for personal identification to evaluate the effectiveness of error detection algorithms for personal identification.

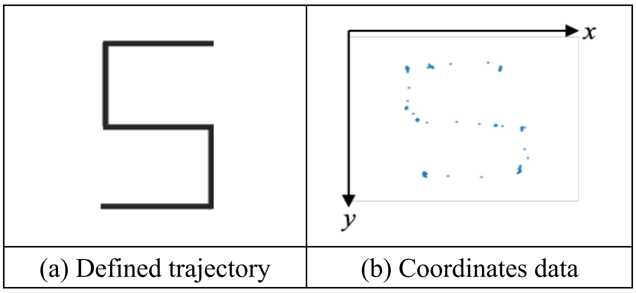
3.4 Measurement Device and Data

In this study, we use a contactless type device as a measurement device. We use the Tobii Pro Tx-300 (Fig. 2) for eye tracking. The positions of the line of sight on the screen are recorded at about 60 Hz. Subjects sit 60 cm away from the screen. We instructed subjects to draw eye movement trajectory within the range of the screen and not to move their heads during drawing eye movement trajectory. draw an eye movement trajectory not to move their heads. Only the shape of the trajectory to be drawn was indicated, and the size was not specified. During the measurement, the trajectory drawn by the subject's line of sight is not displayed on the screen, nor is there a guide for drawing it. The measurement environment is shown in Fig. 3. An example of the collected data is shown in Fog. 4.

The coordinates data consists of coordinates and their corresponding time stamps chronologically recorded. In the proposed method, this data is preprocessed. We extract features used for authentication based on the shape or drawing features from the preprocessed data.

Figure 2: Measurement equipment (Tobii Pro Tx-300)

Figure 3: Measurement environment



(a) Defined trajectory

(b) Coordinates data

Figure 4: An example of collected data

3.5 Preprocessing Data

We think shakes of eye movement and fixations that occur in the raw coordinates data pose a hindrance to the authentication based on shape. On the other hand, we think shakes of eye movement and fixations are effective for the authentication based on drawing features. However, large shakes may become outliers. Therefore, we perform preprocessing before the authentication based on shape and drawing features.

First, we divide all the frames of the drawn trajectory in chronological order. Next, we calculate the average of all coordinates in each partitioned area and generate the average coordinate data. Shakes of eye movement and fixations are removed by this process. A smaller number of divisions can remove shakes of eye movement and maintain the approximate shape information of trajectory. A larger number of divisions can remove large outliers while maintaining the original shape information of trajectory. Therefore, the smaller number of divisions will be suitable for the authentication based on shape. The larger number of divisions will be suitable for the authentication based on drawing features. We extract features from the average coordinates data calculated with each division.

3.6 Investigation of the Features for the Proposed Method

In this section, we explain drawing features using for personal identification.

3.6.1 Investigation of Drawing Features for Personal Identification

In this paper, we use fixation and saccade features for personal identification. Fixation is an eye movement that is performed to fix the direction of sight. Saccade is a rapid eye movement that abruptly changes the point of fixation [12], [13]. A representative example of saccade is the eye movement during line transitions while reading. If we can capture individual differences in these eye movements, we will be able to use these differences as personal features for authentication. The researches [14], [15] have discussed the individual differences in eye movements by saccade. The proposed method extracts these eye movement features to use for personal identification. We think personal features appear in these eye movements. The proposed method extracts these eye movement features.

3.6.2 Extracting Fixation and Saccade Features

In the proposed method, we extract fixation and saccade features from average coordinates data.

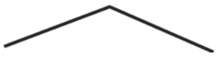
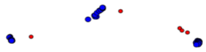
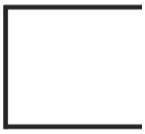
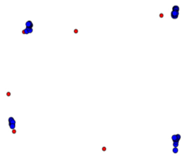
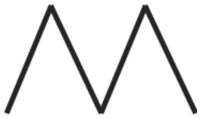
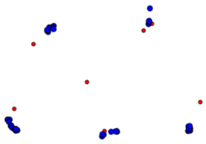
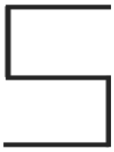
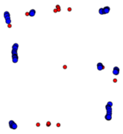
First, we explain about extracting fixation features. We detect fixation points from average coordinates by window sliding. The points where the coordinates are crowded in each window sliding is fixation points. In this paper, points where five or more coordinates are crowded were detected as fixation points. We extract fixation features for each fixation point. The fixation occurs multiple times during drawing trajectory by the eye movement. Therefore, we calculate the features from all fixations detected.

Second, we extract saccade features. The trajectory has a beginning and an end point, with a turning point in the middle. Since the shape is drawn by connecting these points, fixation is expected to occur at the turning points. In addition, saccades are generated when moving the line of sight between the turning points. It is thought that the user's drawing trajectory consists of the repetition of fixation and saccade. In order to extract the saccade, we focus on the fixation. We calculate average coordinates for each fixation point and calculate coordinates data consisting of only fixation points. Next, we extract saccade features by calculating the amount of change between two consecutive frames of the average coordinates data for each fixation point. The saccades are occurred multiple times during the drawing the eye movement trajectory, as well as the fixation. Therefore, we calculate the features used in the proposed method from all saccades detected during drawing an eye movement trajectory.

We analyzed whether the fixation points could be detected by using the proposed method. We extracted fixation points from the average coordinates data of four trajectories. Table 1 shows the results of the analysis.

Blue points are where fixations were observed. Blue points are crowded at the starting and, finishing point of the trajectory and turning points. The result shows that the proposed method can detect fixation points.

Table 1: Fixations extracted from trajectory

Trajectory	Fixations
	
	
	
	

3.6.3 Features Used for Classifying Users

Table 2 shows features used for the proposed method and our previous study [16]. Previous study used the global features such as the amount of change in the average coordinates data. The proposed method does not use the global features, but fixation and saccade features are used as local features. We think that the amount of change in the average coordinates data has redundant information for classifying users because its data contains the data of all frames when users draw an eye movement trajectory. Therefore, we think that we can extract eye movement features which do not contain redundant information by using fixation and saccade features. Drawing time is the time from the start to the end of the drawing. Fixation time includes the maximum and average times that occurred fixation at each point. Variance of fixation includes the maximum, minimum and average variance that occurred fixation at each point. Standard deviation of fixation is calculated in the same way as variance of fixation. The features for fixation and saccade shown in Table 2 are regarded as local features.

3.7 Investigation of Learning Algorithm

The proposed method uses an error detection algorithm for building a learning model. There are studies using error detection algorithms for personal authentication [8], [18]. These studies use One Class SVM or Isolation Forest. One Class SVM is an error detection algorithm that learns only normal data in SVM and identifies whether unknown input data is normal or error data. Isolation Forest is an error detection algorithm that detects error data by repeatedly selecting features and dividing points of data classes. In this paper, we use these algorithms for personal identification. We treat users as normal data and attackers as error data.

Table 2: Features used for experiments

Features	Previous study [16]	Proposed method
Amount of change in average coordinates data	○	×
Variance of x and y coordinates	○	○
Standard deviation of x and y coordinates	○	○
Drawing time	○	○
Fixation time (Maximum, Average)	×	○
Variance of fixation (Maximum, Minimum, Average)	×	○
Standard deviation of fixation (Maximum, Minimum, Average)	×	○
Number of occurrences of fixation	×	○
Speed of saccade in the x and y directions (Maximum, Minimum, Average)	×	○
Number of occurrences of saccade	×	○

4 EVALUATION

We explain the experiment using local features of eye movement for classifying users in Section 4.1. In addition, we explain the experiment using error detection algorithms for personal identification in Section 4.2.

4.1 Classifying Users Using Local Features

In the proposed method, authentication information is created for each individual. The features that can capture the characteristic differences of the individual are desirable for personal authentication. The individual differences are effective not only personal authentication but also personal classification. In other words, if we cannot find the individual differences that are effective features for the classification, it will be difficult to realize personal identification. Therefore, we conducted the experiment about classification of five subjects by using Random Forest to examine the features effective for the classification. In this classification, we used fixation and saccade features. We instructed the subjects to draw the trajectory shown in Fig. 5 30 times. Table 2 shows the features used for classifying users in the proposed method and our previous study [16]. We classify users and calculate the F-measure to evaluate classification accuracy by 10-fold cross-validation. The training and test data in cross-validation include data for all subjects. In addition, we calculate variable importance to investigate the effective features for classifying users. Table 3 shows the environment of the experiments.

Figure 6 shows the result of classification. The experimental result shows that the F-measure of the proposed method was 0.91 and the F-measure of our previous study was 0.83. The proposed method improved the classification accuracy. This method does not use the amount of change in average coordinates data, and adds the fixation and saccade features for classifying users. Therefore, we think that these features improve the classification accuracy.

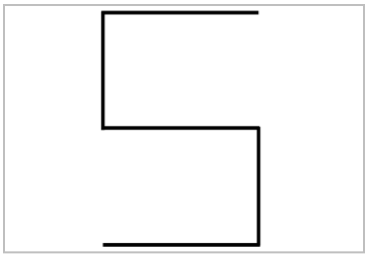


Figure 5: Trajectory used for the experiments

Table 3: Environment of the experiments

Items	Specification
CPU	Intel Core i5 2.4GHz
OS	macOS Catalina10.15.2
Language	Python3.4.5
Library	scikit-learn0.18.1

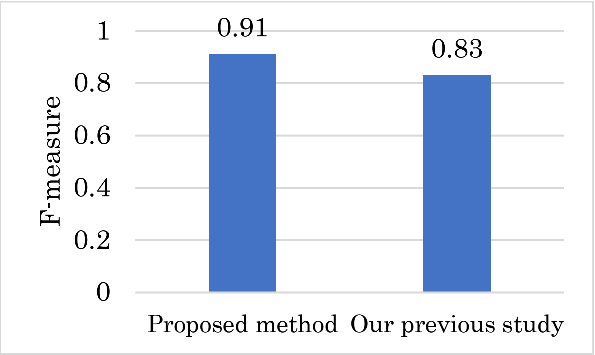


Figure 6: Result of classifying users

Table 4 shows the top 10 features of the proposed method with variable importance. The variable importance with related on saccade is high. This shows that saccade features contribute to the classifying users. However, the variable importance of fixation is low and it is not included in the top 10 features shown in Table 4. In this paper, fixation points are defined as the points where five or more coordinates are crowded. Fixations are not detected if the time of fixation is short. Therefore, we think that the variable importance of fixation was low because we could not extract the personal features of fixation. The variable importance of variance and standard deviation of x-coordinates are high in the proposed method. The proposed method does not use the amount of change in the coordinates for the classifying users. Therefore, we think that other features contribute to classification.

These results showed that the features of local eye movement (Minimum speed of saccade in x direction, Average speed of saccade in x direction, Maximum speed of saccade in x direction, Average speed of saccade in y direction, Minimum speed of saccade in y direction, Maximum speed of saccade in y direction) are effective for classifying users. We think it is necessary to extract and add other local eye movement features to improve classification accuracy.

Table 4: Variable importance of features used to classify users

Features	Variable importance	
	Proposed method	Our previous study
Standard deviation of x coordinates	1.99	0.56
Variance of x coordinates	1.69	0.30
Minimum speed of saccade in x direction	1.48	-
Average speed of saccade in x direction	0.62	-
Drawing time	0.61	0.15
Maximum speed of saccade in x direction	0.55	-
Average speed of saccade in y direction	0.45	-
Minimum speed of saccade in y direction	0.44	-
Variance of y coordinates	0.36	0.17
Maximum speed of saccade in y direction	0.35	-

4.2 Personal Identification Using Error Detection Algorithms

We use One Class SVM and Isolation Forest for personal identification to evaluate the effectiveness of the error detection algorithms for the proposed method. We instructed five test subjects to draw the trajectory shown in Fig. 5 30 times. We use the features shown in Table 2 for this experiment. We evaluate the identification accuracy by F-measure, Precision, Recall, Specificity, FAR (False Acceptance Rate), and FRR (False Rejection Rate). Precision is the percentage of data that predict the user's identity among the data that predict the user. Recall is the percentage of data that are predicted to be the user among the data that are actually the user. Specificity is the percentage of data that are predicted to be others among the data that are actually others. FAR is the probability of mistakenly identifying others (non-users) as authentication users. FRR is the probability of mistakenly identifying users as others. The process for calculating the identification accuracy is as follows:

(1) We perform a test to identify the attacker, using one subject's data as the training data and the other subject's data as the evaluation data to calculate the accuracy. The same process is applied to each subject, and the average accuracy of the five subjects is calculated. This test calculates the number of correctly rejected attackers (true negative) and the number of incorrectly accepted attackers (false positive). The Specificity and FAR are calculated based on these calculated results.

(2) We perform a test to identify the user, and the accuracy is calculated by performing a 10-fold cross-validation using the data of a single subject. The same process is applied to each subject, and the average accuracy of the five subjects is calculated. This test calculates the number of correct acceptances (true positive) and false rejections (false negative). The Recall and FRR are calculated based on these results.

We calculate the F-measure and Precision the accuracy of the personal identification. The accuracy calculated in this way is summarized in Table 5.

This result showed that the personal user was accepted with relatively high accuracy in the case of Isolation Forest. But, the identification accuracy does not reach the level enough to perform authentication. We think that we were unable to build a learning model which is effective for personal identification, because there was not sufficient learning data. Therefore, solving the lack of learning data is one of our future tasks. The results of the evaluation suggested that Isolation Forest is effective as an algorithm for personal identification in our study.

Table 5: Result of personal identification

	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

We performed feature selection using the stepwise method to evaluate which features were effective for personal identification using Isolation Forest. We adopted the stepwise method that is one of representative feature selection methods. The feature selection method searches for the best combination of features by adding or deleting features one by one. We used the selecting and forward feature selection method. The method is one of the stepwise methods. This method increases features one by one from the initial state with no features. We can see which features contribute it by checking the order of addition of the features based on this method.

The process for feature selection in this method is as follows:

(1) Add one feature from among the unselected features, perform personal identification and calculate the F-measure.

(2) After calculating the F-measure, undo the added features and add another feature.

(3) Perform the steps (1) and (2) using all the features, and actually add the features that have the highest F-measure.

(4) Return to the step (1) and repeat the steps (1) ~ (3) until all the features have been added.

The process can be used to evaluate which features are effective for personal identification. The result is shown in Fig. 7.

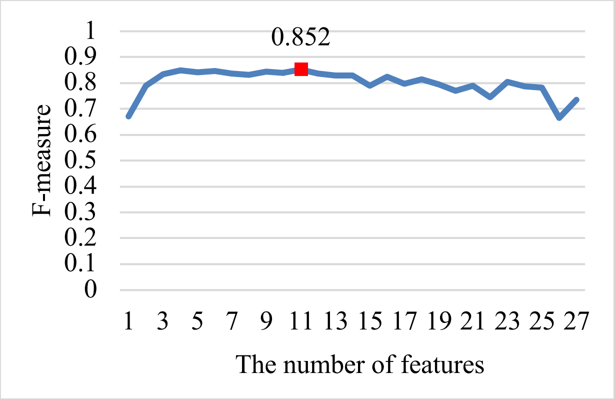


Figure 7: The change of F-measure over the number of features

Table 6: List of features when F-measure is the highest

Order of addition	Features
1	Standard deviation of x coordinates
2	Drawing time
3	Standard deviation of y coordinates
4	Average speed of saccade in y direction
5	Number of occurrences of fixation
6	Minimum speed of saccade in x direction
7	Minimum variance of fixation in x direction
8	Maximum speed of saccade in x direction
9	Minimum standard deviation of fixation in x direction
10	Variance of y coordinates
11	Variance of x coordinates

When the number of the added features was 11, the F-measure was the highest and the value was 0.852. At this time, the FAR was 0.008 and the FRR was 0.23. The features at this time and the order of addition are shown in Table 6. This table shows that these features are effective for personal identification. The fixation and saccade features are included in these effective features. Comparing Table 4 with Table 6, the features that occur in both tables are Average speed of saccade in y direction, Minimum speed of saccade in x direction, Maximum speed of saccade in x direction. These features showed significant individual differences. This experimental result suggested that these features were effective in authentication based on drawing features. The number of occurrences of fixation was included only in Table 6 as a fixation feature. In this experiment, there were few individual differences in the fixation features. In the trajectory used for the experiment, individual differences appeared in saccades. However, individual differences did not appear in fixation because the subjects did not perform fixation much and drew smoothly. In addition, the number of fixation and saccade features that were effective in this study was 6 out of 22 dimensions. In order to increase the accuracy of the personal identification, it is necessary to re-examine and add the features that are effective for personal identification.

4.3 Discussions and Future Works

The goal of this research is to realize an authentication for mobile terminals such as laptop PCs and smartphones. Applications that we assume include unlocking of mobile terminals themselves and login to services from mobile terminals. In public spaces such as stations and cafes, it is important to prevent unauthorized login by others while the user is away from the terminal, or login by others when the terminal is lost. In the experiment in Section 4.2, we performed personal identification and feature selection. As a result, in personal identification using the features with the highest accuracy, the F-measure was 0.852, FAR was 0.008 and FRR was 0.23. Related researches [3], [7], [9], for similar applications (to mobile terminals) have achieved FAR of less than 0.1. We think that regarding FAR, we have achieved a satisfactory level in comparison with these researches. On the other hand, the FRR in the related researches [3], [7], [9], is less than 0.1, but the FRR in the proposed method is 0.23. It is difficult to say that the accuracy is sufficient at this point. The reason for the low accuracy may be that each subject cannot reproduce the same eye movement trajectory. As a countermeasure, we are considering improvement of reproducibility of the eye movement trajectory by displaying a reference point during the drawing process.

5 CONCLUSION

This study proposes a personal authentication method using the user's eye movement trajectory to solve the weaknesses of password and biometric authentication. This method performs authentication based on the shape of the user's eye movement trajectory, and authentication based on drawing features. In this paper, we extract fixation and saccade features and classify users to investigate features that are effective for classifying users. In addition, we conducted an experiment that identified users by using representative error detection algorithms in order to investigate the learning algorithm for the proposed method.

First, we performed classifying users by using fixation and saccade features. We compared the classification accuracy of the proposed method with the classification accuracy of our previous study. The experimental result showed that the F-measure of the proposed method was 0.91 and the F-measure of the previous study was 0.83. Therefore, it was suggested that fixation and saccade were effective for classifying users. The saccade variable importance was high. The results showed that local eye movement features were effective for classifying users.

Next, we identified users by One Class SVM and Isolation Forest to investigate a learning algorithm. We evaluated the identification accuracy by F-measure, Precision, Recall, Specificity, FAR, and FRR. In the case of using One Class SVM, the F-measure was 0.61, Precision was 0.86, Specificity was0.97, Recall was 0.49, FAR was 0.03 and FRR was 0.51. In the case of using Isolation Forest, the F-measure was 0.73, Precision was 0.75, Recall was 0.75, Specificity was 0.91, FAR was 0.08 and FRR was 0.27. The experimental result showed that the accuracy was high when using Isolation Forest for personal identification. Therefore, it was suggested that Isolation Forest was effective as the algorithm for the proposed method.

There are three future tasks for this study. First, we need to consider other features about local eye movement and add these to improve classification accuracy. Next, we will consider a method to solve the problem of lack of learning data for improvement of personal identification accuracy. Finally, we will further investigate learning algorithms to improve the accuracy of each authentication.

ACKNOWLEDGEMENTS

Part of this work was carried out under the Cooperative Research Project Program of the Research Institute of Electrical Communication, Tohoku University.

REFERENCES

[1] 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).

[2] 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).

[3] 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).

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

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

[6] 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).

[7] 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).

[8] S. Itou and Y. Shiraishi, “A Proposal of a Method for Continuous Authentication Focusing on Characteristics of Flick Input System on Smartphones”, Proceedings of 25th Multimedia Communication and Distributed Processing Workshop, Vol.2017, pp.1-8 (2017) (*in Japanese*).

[9] 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, Vol.18, No.9 (2018).

[10] 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 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp.2156-2164 (2016).

[11] H. Mukai and T. Ogawa, “Feature Extraction of Eyegaze Path for Personal Authentication,” IPSJ Transaction on Digital Contents (DCON), Vol.4, No.2, pp.27-32 (2018) (*in Japanese*).

[12] K. Ukai, “Eye Movement: Characteristics and Method of Measurement,” Japanese Journal of Optics, Vol.23, No.1, pp.2-8 (1994) (*in Japanese*).

[13] 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).

[14] G. Bargary, 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).

[15] 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).

[16] T. Fujimoto and Y. Shiraishi, “An Examination of Personal Authentication Method Using Shape of Gaze Trajectory and Drawing Features,” Proceedings of Multi-

media, Distributed, Collaborated and Mobile Symposium of IPSJ, pp.1423-1432 (2019) (*in Japanese*).

[17] Tobii Pro Mechanism of Eye Tracker, tobii pro, https://www.tobiipro.com/ja/service-support/learning-center/eye-tracking-essentials/how-do-tobii-eye-trackers-work/ (accessed 2019-05-06).

[18] K. Watanabe, M. Nagatomo, K. Aburada, N. Okazaki and M. Park, “Gait-Based Authentication using Anomaly Detection with Acceleration of Two Devices in Smart Lock,” Advances on Broad-Band Wireless Computing, Communication and Applications, Lecture Notes in Networks and Systems (LNNS), Vol. 97, Springer, pp.352-362 (2019).

(Received October 30, 2020)
(Accepted February 8, 2021)

Takumi Fujimoto received his B.E. and M.E. degrees in information science from Future University Hakodate, Japan in 2019 and 2021. His research interests include mobile sensing, security and machine learning. He

Yoh Shiraishi received doctor’s degree from Keio University in 2004. He is currently a professor at the Department of Media Architecture, School of Systems Information Science, Future University Hakodate Japan. His re-