A Facial Authentication Method Robust to Postural Changes in e-Testing

Masashi Komatsu[1(✉)] and Takako Akakura[2]

[1] Graduate School of Engineering, Tokyo University of Science, 6-3-1 Niijuku, Katsushika-ku, Tokyo 125-8585, Japan
4415040@ed.tus.ac.jp
[2] Faculty of Engineering, Tokyo University of Science, 6-3-1 Niijuku, Katsushika-ku, Tokyo 125-8585, Japan
akakura@rs.tus.ac.jp

Abstract. Examinee posture changes during e-Testing, making it difficult to perform facial authentication throughout the duration of the exam. We propose two methods for addressing this. The first method is to combine facial detection and tracking of facial information during the test. The second method is to pre-register facial information at various postures for authentication by computing the most similar image at the time of authentication. We conducted certification experiments using 21 examinees. The results showed authentication accuracy of 82.8%, an improvement of 16.8% over previous research, thus demonstrating the effectiveness of the proposed method.

Keywords: e-Testing · Biometrics · Facial authentication

1 Introduction

e-Learning is becoming increasingly more popular at universities [1]. Web-based e-Learning overcomes temporal and geographical restrictions, allowing broader segments of students to take classes. e-Learning also has advantages not found in traditional classroom instruction. For example, by sequentially storing learning-history data, students can be provided with adaptive feedback and lectures can be viewed at their own pace.

However, few universities give credits for e-Learning courses, or require test-taking at examination sites, thereby negating e-Learning's inherent advantages. There is thus a need for mitigating testing constraints and e-Testing is one such effective method because it has various advantages over conventional paper tests:

- Evaluation of remote examinees
- Adaptive testing that can estimate examinee abilities at any time and tailor questions to examinee abilities
- Automatic scoring and instant feedback
- Data acquisition that cannot be measured in paper testing, such as time required for answering and revision

S. Yamamoto and H. Mori (Eds.): HCII 2019, LNCS 11570, pp. 372–384, 2019.
https://doi.org/10.1007/978-3-030-22649-7_30

The above-mentioned advantages are found in e-Testing. However, most current e-Testing performs identity authentication using an ID and password at the start of the examination, making fraudulent acts during the examination easy to perform. There is thus a need for continual authentication during testing. It is inappropriate to ask examinees to perform frequent authentication operations during testing, because doing so would interfere with the examination. Methods for continual authentication must therefore operate without active examinee input.

2 Related Research

Methods for authentication based on facial recognition during testing have been proposed in studies on fraud prevention in e-Testing.

Tanaka et al. [2] authenticated individuals using examinee handwriting information from pen tablet input and facial information from a camera attached to the top of a PC display. One limitation in their method was that consistent facial detection was unreliable due to changes in examinee posture, such as when the examinee looked away from the screen or leaned on their hand while thinking. Thus it was impossible to maintaining facial authentication throughout the entire examination.

Kawamata et al. [3] searched for the nose when the examinee's face could not be detected, and derived facial information based on the detected nose position. As a result, they succeeded in acquiring 61% of facial information over the whole examination time, but authentication accuracy was only 65%.

As Fig. 1 shows, these studies are limited in that authentication cannot be performed during the entire examination time.

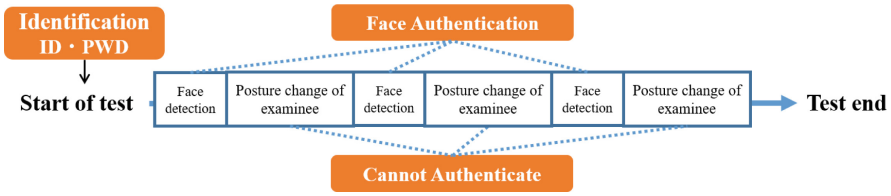

Fig. 1. Face authentication in existing e-Testing.

3 Purpose of This Study

In this study, based on the task in our previous research, we aimed to make individual authentication possible at all times when e-Testing was conducted with a camera attached on top of the display. The focus of this study was to simultaneously apply facial recognition and tracking method. Specifically, when the examinee's face cannot be detected due to a posture change, the area surrounding the nose is tracked from the next successful face detection point. Individual authentication is performed from the resulting face images throughout the examination time.

4 Proposed Method

4.1 Overview of Face Authentication

Facial authentication calculates the distance between a preregistered facial image and facial images captured during testing. Figure 2 shows the examinee authentication flow assumed in this study. Kawamata et al. [3] authenticated examinees from a single registered image. However, because examinees' facial expressions and posture change, it is difficult to perform authentication from a single registered image. We therefore propose "PreTest" for the registration process, a method that acquires information of various postures by applying facial detection with tracking. During e-Testing, the distance to the image having the nearest facial orientation as acquired by PreTest is calculated for examinee authentication.

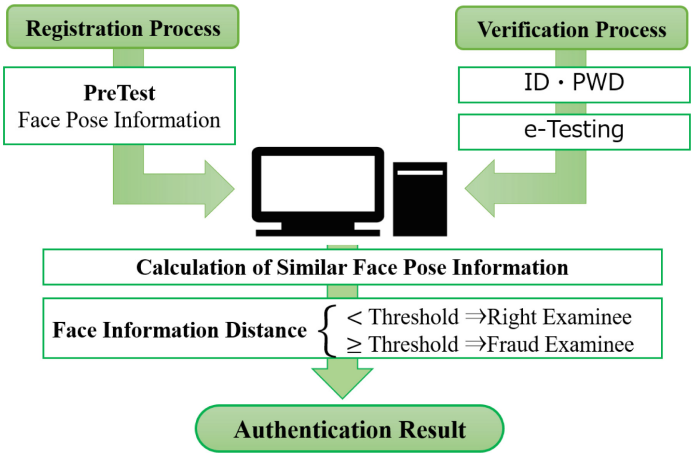

Fig. 2. Authentication process

4.2 Face Detection Method

Face detection is a process for automatically determining regions in an input image containing a face. Face detection uses a method proposed by Viola et al. [5]. This method is capable of high-speed face detection by using a combination of specific rectangular features in the input image (Fig. 3). Rectangular features are described using properties such as differences in luminance under the eyes and between the nose and nose ridge. The figure shows an example of its use.

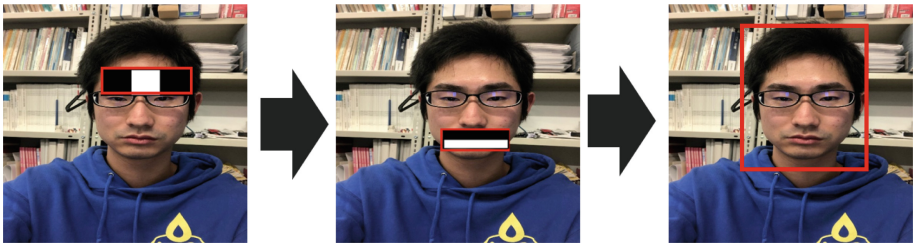

Fig. 3. Face detection

4.3 Face Tracking Method

For face tracking, we use the MeanShift method proposed by Comaniciu et al. [6]. MeanShift is a method for tracking the region with the highest distance between color histograms. Tracking is performed when face detection cannot be performed due to attitude variation of the examinee, and the face area is tracked from the very next successful face detection point. Personal authentication is performed throughout the examination from the resulting face information. Based on the results of Kawamata et al., we use a facial area that is difficult to hide during tracking as shown in Fig. 4. Specifically, the region within 20 pixels of the position where the coordinate value is lowest within the face detection part is set as the tracking part. The authentication method combining face detection and tracking proposed in this study is called the "hybrid method."

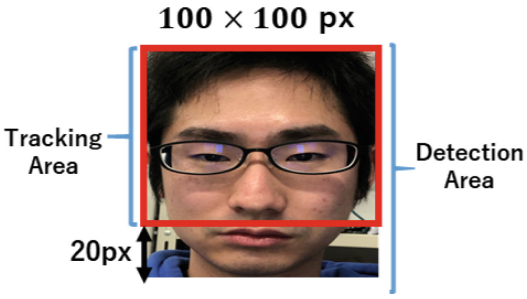

Fig. 4. Tracking area

4.4 Numerization of Facial Images

To perform face authentication, it is necessary to quantify similarity between facial images acquired by face detection and tracking. In this study, we use a method proposed by Ojala et al. [7]. In this method, an image is first divided into arbitrary rectangular regions, neighboring pixels are binarized with the central pixel as a threshold in each region, and that region is represented as a binary number. After that, a local binary pattern histogram (LBPH) is created using a local binary pattern (LBP) value obtained by converting the binary number obtained for each area to a decimal number. An image distance between the registered image and the verification image is calculated using the histogram It is a method to compare similar images. LBPH in this study is calculated by the following procedure (Fig. 5):

(1) LBP is calculated by comparing the pixel value of the target pixel and the pixel value of 8 neighborhood.
(2) A LBP histogram is created for each area when the image is divided into 64 sections.
(3) Concatenate the LBP histograms of the whole area.

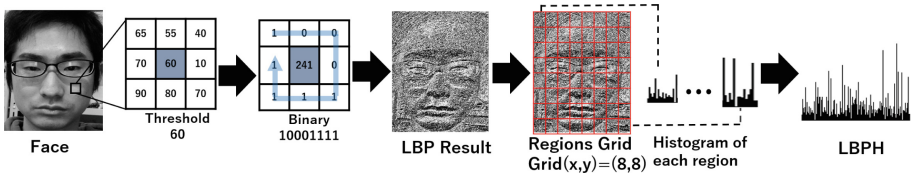

Fig. 5. Calculation of LBPH

4.5 Evaluation Index of Authentication Accuracy

The equal error rate (EER) is widely used as an evaluation index for authentication [4]. The EER is the value at which the false rejection rate (FRR) and the false acceptance rate (FAR) agree. There is a trade-off relationship between FRR and FAR, with a decrease in one corresponding to an increase in the other. The closer the EER value is to 0%, the higher the authentication accuracy (Fig. 6).

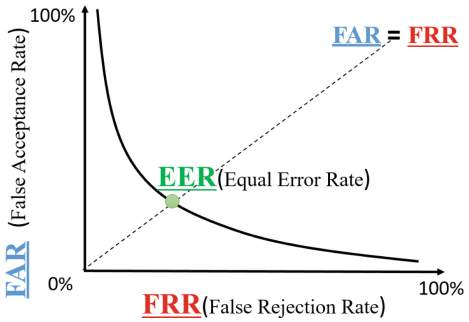

Fig. 6. Error rate curve

5 Evaluation Experiment

5.1 e-Testing System

We developed an e-Testing system to achieve the objectives of this study. Figure 7 shows the system. One feature of this system is that taking exams requires only mouse operations. The screen display includes a calculator and memo space and displays the remaining time.

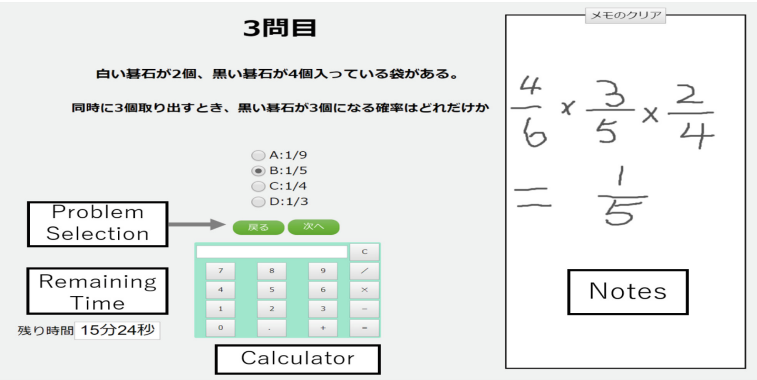

Fig. 7. e-Testing system

5.2 Experiment Contents

To achieve the objectives of this study, we conducted an experiment involving 21 college students. Table 1 shows the questions and the test duration. The evaluation method is compared with the authentication accuracy in Kawamata et al. [3], which was EER = 35.0%. We used the results from Kawamata et al. It was set as the target value because the authentication time was 61% and the authentication time was long. The camera used in this experiment captured images at 30 fps. PreTest acquires all frames and performs authentication every 30 frames. In other words, authentication is performed every second. Face detection, tracking, and LBPH calculations were performed using the open source software package OpenCV.

Table 1. Question Contents

	PreTest	e-Testing
Test Time	Within 10 min	Within 25 min
Contents	Inference Probability Special calculation	Long text Inference Probability Special calculation

6 Experimental Result and Discussion

Through these experiments, we obtained 155,656 registered images with PreTest and 23,765 verification images with e-Testing. Figures 8, 9, and 10 show the error rate curves for the authentication results using face detection, tracking, and the hybrid method.

Figure 11 summarizes the results in Figs. 8, 9 and 10. Table 2 shows authentication times and authentication accuracy. In Fig. 9, the vertical axis shows FAR

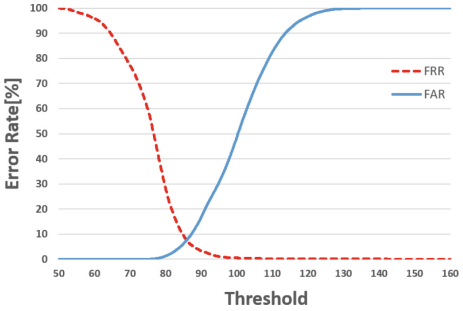

Fig. 8. Face detection

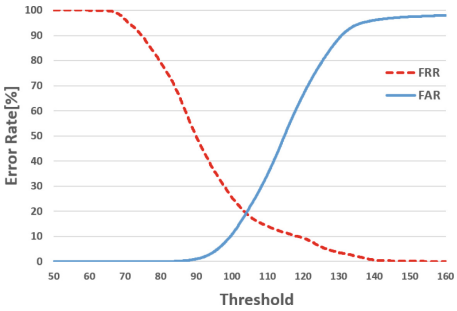

Fig. 9. Tracking

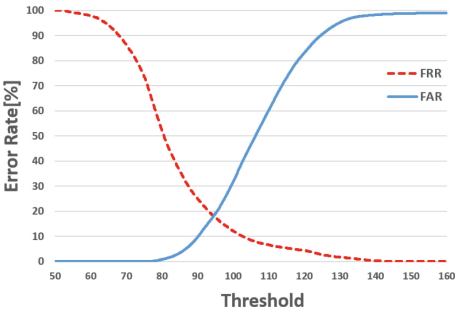

Fig. 10. Hybrid

and the horizontal axis shows FRR. EER is the value where FAR = FRR. The authentication accuracy is considered based on the results shown in Fig. 11.

The following describes the results from face detection, tracking, and the hybrid method shown in Fig. 11 and Table 2.

Face detection had an EER of 7.4%. The authentication accuracy is highest because face detection is performed when the examinee is facing forward.

Tracking had an EER value of 19.3%. Authentication is performed correctly when PreTest and e-Testing detect the same changes in posture, but authentication could not be performed when posture differed from PreTest.

Table 2. Authentication results

	Acquisition time	EER
Previous research [3]	61%	35.0%
Face detection	53%	7.4%
Tracking	47%	19.3%
Hybrid	100%	18.2%

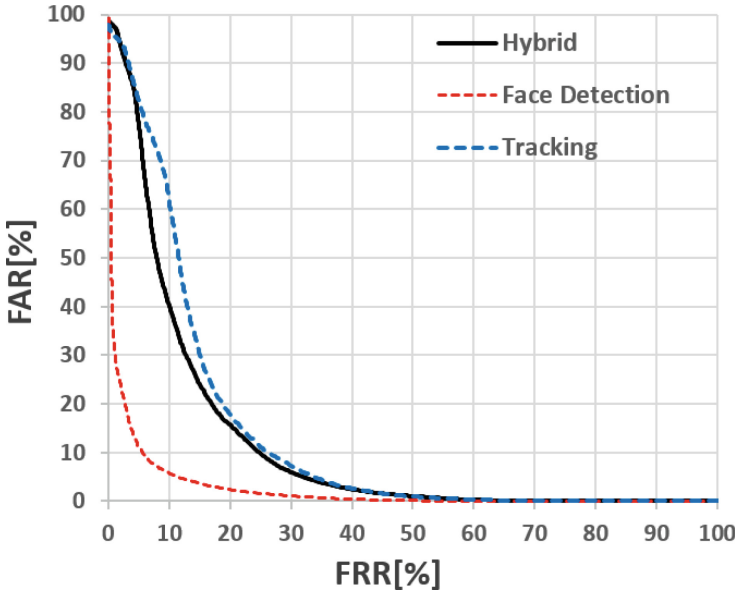

Fig. 11. ROC curve of error rate

The hybrid method resulted in an EER of 18.2%. This is a 16.8% improvement in authentication accuracy over Kawamata's EER of 35.0%. Therefore we believe that the result of the hybrid method is effective. Tables 3 and 4 summarize the authentication accuracy for examinees in order of highest tracking rate. We consider results from the hybrid method shown in Tables 3 and 4.

Table 3. Tracking rate of 21 examinees in descending order (1/2)

Examinee	A	B	C	D	E	F	G	H	I	J
Face detection rate [%]	0.9	1.4	2.4	5.0	11.4	12.3	19.4	24.9	27.6	41.3
Tracking rate [%]	99.1	98.6	97.6	95.0	88.6	87.7	80.6	75.1	72.4	58.7
Authentication accuracy [%] (EER = 18.2%)	74.0	3.6	14.8	94.7	96.1	92.0	78.2	86.6	51.5	61.6

Table 4. Tracking rate of 21 examinees in descending order (2/2)

Examinee	K	L	M	N	O	P	Q	R	S	T	U
Face detection rate [%]	51.8	55.6	60.8	91.2	92.8	96.4	97.3	98.5	99.5	99.7	99.8
Tracking rate [%]	48.2	44.4	39.2	8.8	7.2	3.6	2.7	1.5	0.5	0.3	0.2
Authentication accuracy [%] (EER = 18.2%)	88.6	86.6	59.1	98.0	96.9	96.4	98.7	97.6	99.6	97.3	99.8

We considered the relationship between the tracking rates in Tables 3 and 4 and the authentication accuracy by dividing data into four patterns.

(Pattern 1)
Tracking rate 50% or more and authentication accuracy 70% or more
⇒ A · D · E · F · G · H
(Pattern 2)
Tracking rate 50% or more and authentication accuracy less than 70%
⇒ B · C · I · J
(Pattern 3)
Tracking rate less than 50% and authentication accuracy 70% or more
⇒ K · L · N · O · P · Q · R · S · T · U
(Pattern 4)
Tracking rate less than 50% and authentication accuracy less than 70%
⇒ M

6.1 Discussion of Pattern 1

Pattern 1 featured a tracking rate 50% or more and authentication accuracy 70% or more and included Examinees A, D, E, F, G, and H. We considered Examinee E, who had high authentication accuracy, and Examinee A, who had low authentication accuracy. Time series data for examinees A and E are shown in Figs. 12 and 13.

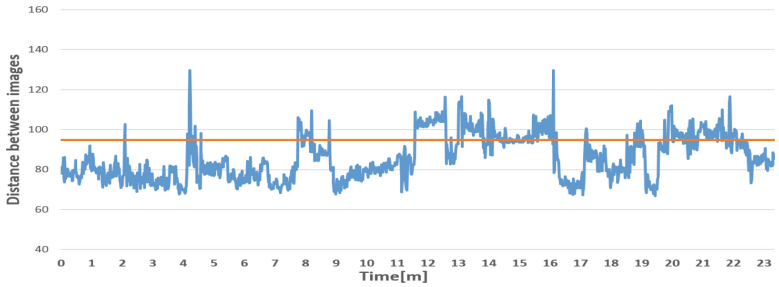

Fig. 12. Results of examinee A

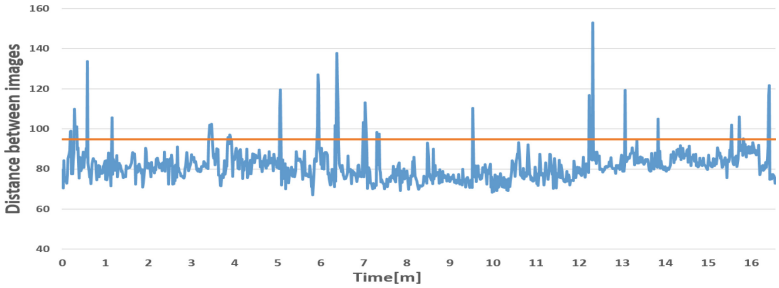

Fig. 13. Results of examinee E

For Examinee A, there was a tendency for erroneous detection of the right eye as a face area. Authentication accuracy possibly decreased due to tracking of an erroneously detected face area.

Authentication accuracy for Examinee E is thought to be lowered due to blurring of the image resulting from a low camera frame rate. To reduce blurring, a camera with a higher frame rate should be used.

6.2 Discussion of Pattern 2

Pattern 2 featured a tracking rate of 50% and authentication accuracy less than 70%, and included Examinees B, C, I, and J. We consider the results for Examinee B, who had extremely poor authentication accuracy, and Examinee I, whose certification accuracy was 50%.

From Fig. 14, Examinee B did not succeed in authentication except when face detection succeeded. During e-Testing, authentication likely failed because the face area was not accurately tracked due to the examinee looking at the bottom of the screen throughout the duration of the exam.

From Fig. 15, authentication accuracy was lower for Examinee I because there was no posture change that took the hands during PreTest and because a misdetected face region was tracked in the latter half of the test.

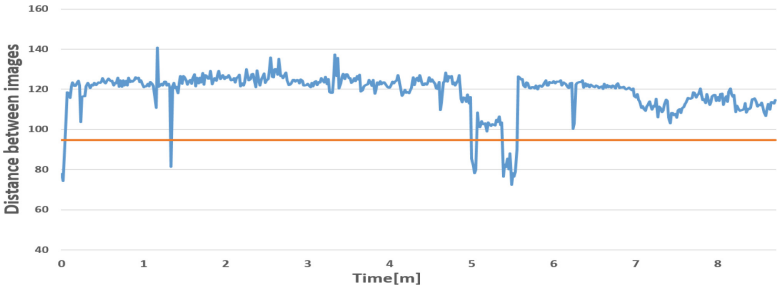

Fig. 14. Results for examinee B

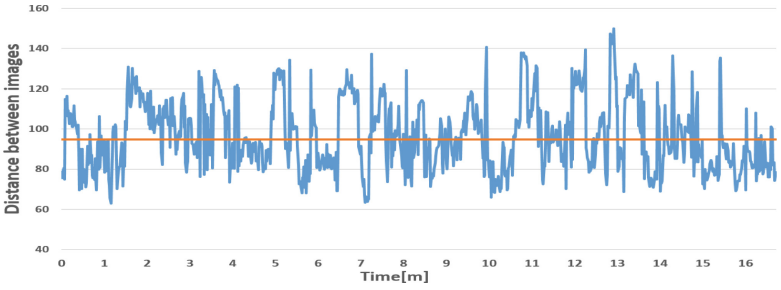

Fig. 15. Results for examinee I

6.3 Discussion of Pattern 3

Pattern 3 featured a tracking rate less than 50% and authentication accuracy of 70% or more, and included Examinees K, L, N, O, P, Q, R, S, T, and U.

Pattern 3 had overall high authentication accuracy. We consider Examinee L, who had the lowest authentication accuracy in this pattern, and Examinee U, who had the highest.

Figure 16 shows that Examinee L failed authentication when repositioning eyeglasses and when yawning. The action of correcting for changes in eyeglass positioning may be possible if authentication is during during registration at PreTest.

Figure 17 shows that authentication for Examinee U was successful except when he turned his neck. Authentication accuracy was likely high because the examinee did not have obscuring objects such as eyeglasses or long hair covering the facial area.

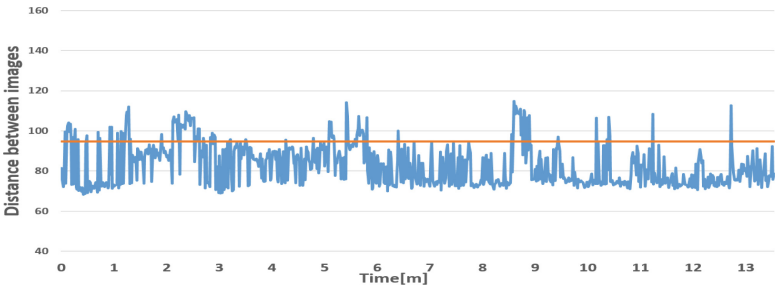

Fig. 16. Results for examinee L

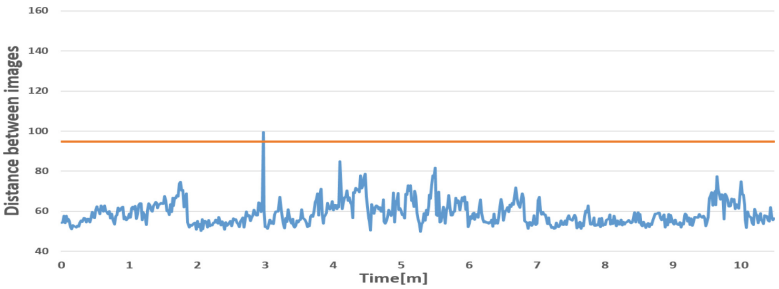

Fig. 17. Results for examinee U

6.4 Discussion of Pattern 4

Pattern 4 featured a tracking rate less than 50% and authentication accuracy less than 70%, and included only Examinee M.

From Table 4, the accuracy of authentication for Examinee M was almost the same as the face detection rate. From Fig. 18, Examinee M had a high face detection rate but low authentication accuracy. The low authentication accuracy was likely due to tracking.

Figure 19 shows the face tracking area for Examinee M. Figure 2 shows that Examinee M wore a hooded sweatshirt that was included in the tracking area. Tracking likely followed this clothing instead of the examinee's face, lowering authentication accuracy.

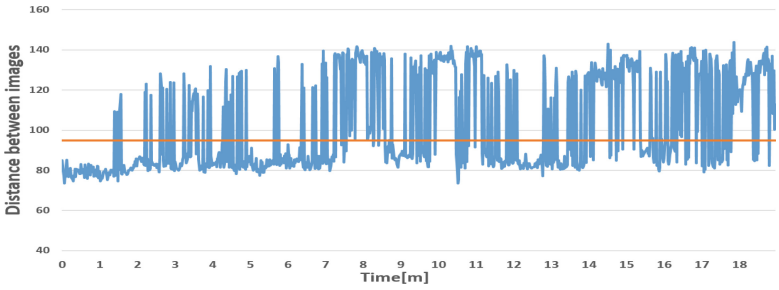

Fig. 18. Results for examinee M

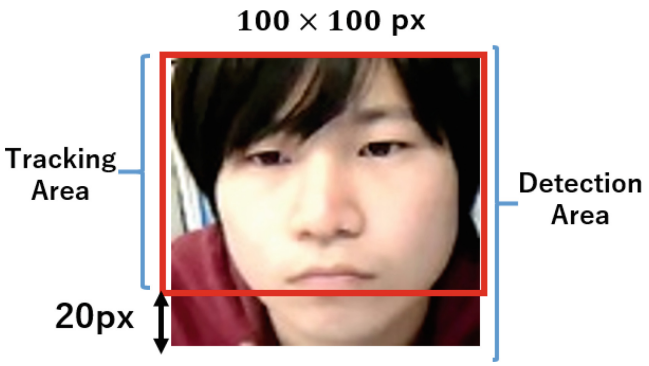

Fig. 19. Face tracking area of examinee M

7 Conclusion

We proposed two methods for authentication throughout the duration of an examination.

The first method was to register various facial orientations of examinees using PreTest, calculating the closest distance between images registered during e-Testing, and performing facial authentication even when the examinee posture changed.

We also proposed an authentication method that performs face authentication for throughout the exam by tracking the face area when face detection was not possible.

The results suggested that the authentication accuracy was 16.8% higher than in previous study, and that the proposed method is robust against posture changes.

The following issues remain as future tasks. In this experiment, we assumed that regular exam examinees are authenticated when taking the exam. Future research will investigate fraud detection by testing resistance against attacks such as spoofing.

Acknowledgments. This study was partially supported by a Grant-in-Aid for Scientific study (A) (#15H01772; Principal Investigator: Maomi Ueno) from the Japan Society for the Promotion of Science (JSPS).

References

1. University ICT Promotion Council: Survey study survey report on ICT utilization in higher education institutions (2016). http://www.mext.go.jp/a_menu/koutou/itaku/__icsFiles/afieldfile/2016/06/02/1371459_01.pdf. (in Japanese)
2. Tanaka, Y., Yoshimura, Y., Tomoto, T., Akakura, T.: Examinee authentication method using face image in e-Testing toward preventing impersonation. D Abstracts IEICE Trans. Inf. Syst. (Japan. Ed.) **J98–D**(1), 174–177 (2016)
3. Kawamata, T., Ishii, T., Akakura, T.: A study on robust face authentication method for examinees' attitude variation in e-Testing. In: Proceedings of the 2010 IEICE General Conference Papers, Information and Systems Society Special Project Student Poster Session Proceedings, p. 214 (2017). http://www.ieice.org/~iss/jpn/Publications/issposter_2017/data/pdf/ISS-SP-214.pdf
4. Hangai, S.: Biometric textbook From principle to programming, The Institute of Image Information and Telecommunications, Corona Company, Tokyo (2012)
5. Viola, P., Jones, M.: Rapid object detection using a boosted cascade of simple features. Proc. Comput. Vision Pattern Recogn. **1**, 511–518 (2001)
6. Comaniciu, D., Ramesh, V., Meer, P.: Real-time tracking of non-rigid objects using mean shift, vol. 2, pp. 142–149 (2000)
7. Ojala, T., Pietikänen, M., Harwood, D.: A comparative study of texture measures with classification based on featured distributions. Pattern Recogn. **29**, 51–59 (1996)