Student Authentication Method by Sequential Update of Face Information Registered in e-Learning System

Taisuke Kawamata[1(✉)], Susumu Fujimori[2], and Takako Akakura[2]

[1] Graduate School of Engineering, Tokyo University of Science,
1-3 Kagurazaka, Shinjuku-Ku, Tokyo 162-8601, Japan
kawamata_taisuke@ms.kagu.tus.ac.jp
[2] Faculty of Engineering, Tokyo University of Science,
1-3 Kagurazaka, Shinjuku-Ku, Tokyo 162-8601, Japan
{fujimori,akakura}@ms.kagu.tus.ac.jp

Abstract. e-Learning is easing restrictions on time and space for a learner. However, its weak point is that a user authentication employs only on log-in with credentials, which makes it easy to cause a cheating. We have studied the changes in face image in e-Learning with the aim of detecting the cheating. We proposed an authentication method with sequential updates of student's face information using new images taken by a web-camera during the e-Learning. We examined the update timing and procedure in this study, and found that the authentication accuracy the highest by summing each face feature vector in the face image which is taken when a student operates the e-Learning system.

Keywords: e-Learning · Video lecture · Student authentication · Face image

1 Introduction

e-Learning has been widely spreading in recent years because it can alleviate time and space restrictions [1]. A lot of schools have introduced the e-Learning into their lectures and students have many opportunities to take the lectures using e-Learning system now. However, there is a problem in the e-Learning that teachers cannot observe students behavior during a lecture, because they do not face directly each other. Most e-Learning systems perform a user authentication using only a user name and password which are entered at login, making it easy to cheat, students other than ones enrolled in the course may take the learning or students may leave away from the in seats before finishing.

Agulla et al. [2] developed the method using biometric authentication based on face recognition in order to check how much time the student is in front of the computer during the e-Learning session. Theirs method uses the student frontal images taken by web-camera during e-Learning. The method guarantees that the student is the enrolled one, and also gives the exact information on how much time the student spends in front of the computer for the e-Learning content. In the case that the face authentication system is unable to identify of a user for a period of time, other verifications based on fingerprint and voice are performed.

S. Yamamoto (Ed.): HIMI 2016, Part II, LNCS 9735, pp. 138–145, 2016.
DOI: 10.1007/978-3-319-40397-7_14

However, this kind of combined authentication may become a disturbance for students to learn. It is needed to develop the highly accurate authentication method using face images only, without the other verifications. In this paper, we propose a new method based on face information and examine the effect of the new method.

2 Proposed Authentication Method

2.1 Proposed Method

We proposed the authentication method with sequential updates of student's face information for collating using newly input images taken by a web-camera during the e-Learning (Fig. 1), and named this method "update method". It is expected that the update method enables to make sure whether a student is the same person from beginning to end during e-Learning by inputting a newly taken face information in certain timing and matching it with the previously input face information.

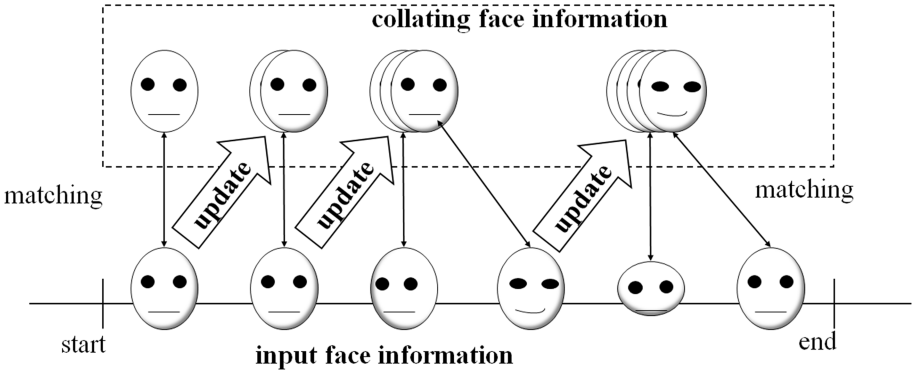

Fig. 1. The model of updating the face information for collating

The important thing in the update method is how face information for collating is updated. We assume that face detection method applied to the collation of student's face image student during e-Learning successively. The face of student often cannot be detected at such timing as student looks down to read or write notes. Therefore, the details of updating procedure have to be considered.

2.2 Face Authentication

This subsection explains conventional face authentication flow in this study. Face authentication used in this paper is based on the method proposed by Ahonen et al. [3].

First of all, we explain about the student's face information in the authentication database. An original student's frontal image is a photograph of the student himself/herself. This image, which is called a registered image, is submitted by the

student at the time of registration. A face area is detected from the registered image. Face detection method is performed using the Viola and Jones algorithm [4] included in the OpenCV library. Face feature vector is extracted from the area of face in input image. Face feature is expressed the uniform local binary patterns histogram (LBPH), proposed by Ojala et al. [5].

Next, we explain the face authentication during e-Learning. Input frontal image of the student is taken by web-camera, and this input image is used to detect the face region and to extract the face feature vector. Last, correlation coefficient between the previously taken face feature and newly input face feature is calculated. Correlation coefficient between two LBPH is referred to as "similarity", and the similarity determines whether a person in front of PC is a true student or an impostor.

3 Results

3.1 Experiment Overview

We made an analysis to find an appropriate updating procedure. Subjects of the experiment were nine students in a Japanese university. The students took the e-Learning by watching about 1 h.

The experiment flow is following. A student is explained about the experiment overview before the experiment starts. After the explanation, the student takes the video lecture using e-Learning system (Fig. 2). This system has an operation log acquisition function. Web-camera on the PC display takes the frontal image of a student every second during e-Learning. A student is permitted to take note and look at lecture materials during the experiment. When a certain time passes in the lecture, the video stops and the message, "Do you understand?" appears in the lecture video, as shown in Fig. 3. This function is implemented to make a student operate the e-Learning system. The student can restart the video by clicking the "OK" button on the dialog box. With regard to making a spoofing situation, we also make a student leave away from the seat 5 s later than the start of the lecture and return to the seat 15 s after. After the lecture finishes, a frontal image of the student is taken as a verification photograph.

Fig. 2. The conditions of an experiment

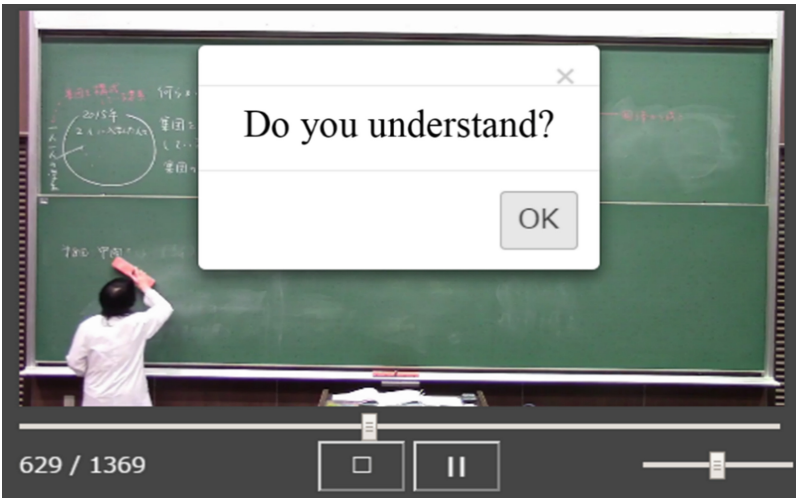

Fig. 3. Dialog box

3.2 Consideration of Update Detail

Update Timing.

The update timing is considered. We chose the time when a student operates the system, as the update timing (hereinafter referred to as "Event timing"). A student usually faces the display of PC at the timing of operating system, so probably the face detection is easy to be made successfully and the similarity is higher than other timings. To check whether a face of student can be detected and the similarity is high or low, we apply the Ahonen method to the data.

Table 1 is the result of analysis. Face detection rate indicates the percentage of successful face images detection. This result suggests that the face detection rate was higher at the Event timing than at the other timing. In addition, the average of similarity value was higher at the Event timing than the other timing. The difference in the similarities between the Event timing and the other timing was 0.05 and statistically significant. This result suggests that students face the display at the Event timing. Based on this result, we use the Event timing as the time of face image update in this study. We also use an ordinary constant timing, Normal timing, as another update timing, for comparison.

Table 1. Face detection rate and statistical value of similarity

	Event timing	Normal timing
Number	109	18388
Face detection rate (%)	92.37	60.04
Mean	0.533	0.489
Standard deviation	0.081	0.095

Update Procedure.

We proposed two update procedure. One procedure overwrites new input image on the previous student image. It is expected that the new input images are more similar to previous images, and this procedure may contribute to the increase in accepting the true student.

The other procedure updates the feature vector for collating by summing image feature vector in each previous time. The summation of feature vectors possibly contain many features of true student's face images. And, this feature vector more corresponds to the face image than any other materials. Therefore, it is expected that this procedure reduces misconceive another student as the true student, if the true students sit down in front of PC long time.

3.3 Analysis Method

We analyzed the effect of the update method for the spoofing situation. The spoofing situation was made to connect images taken before a student leaves away from the seat and images taken after another student sits down in the seat. Figure 4 shows the example of the analysis. In this figure, the horizontal axis is the learning time, and the vertical axis is the similarity. The similarity are plotted as a line diagram. Blue line on the figure means the similarity in the true student, and red line mean the similarity for the impostor. A vertical bar indicates the Event timing. It is expected that the spoofing is detected early. So, we analyzed images of the student to 250 s from 20 s in the experiment.

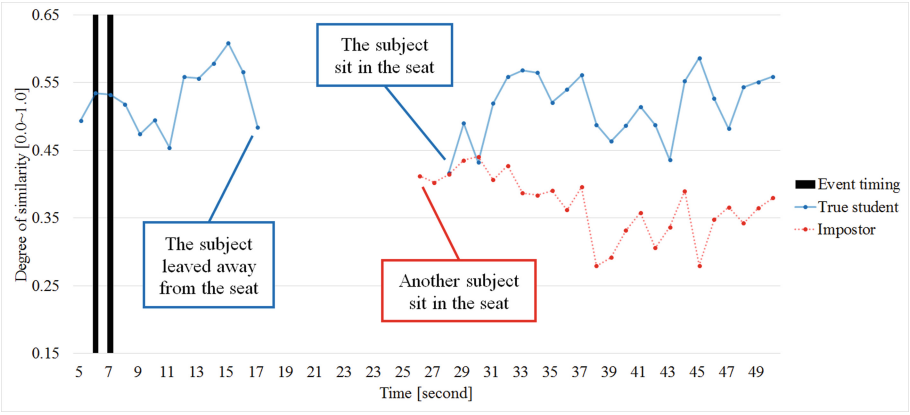

Fig. 4. Analysis method

3.4 Evaluation Method

We used d-prime (d′) to evaluate the separation between student and impostors of similarity distribution. The d-prime is the degree of separation between two distributions. High d-prime means that the identification of the person with the true student and the impostor by similarity is easy. The d-prime is calculated as follows:

$$d' = \frac{|\mu_r - \mu_n|}{\sqrt{(\sigma_r^2 + \sigma_n^2)/2}}$$

μ_r: mean of similarity for the true student,
μ_n: mean of similarity for the impostor,
σ_r: standard deviation of similarity for the true student,
σ_n: standard deviation of similarity for the impostor.

To evaluate from the different point of view, we employed False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (EER) and for evaluating accuracy. EER is the value at which the false acceptance rate (FAR) is equal to the false rejection rate (FRR): FAR is the probability that an unauthorized person is authenticated, and FRR is the probability that an authorized person is rejected. In the second phase, a given threshold is required for authentication. When threshold value is low, FAR is close to zero, but FRR becomes high; when the threshold value is high, FAR becomes high and FRR becomes low. Thus EER is frequently used to evaluate authentication methods.

3.5 Evaluation of the Appropriate Update Timing and Procedure

Compared update methods are following:

- OE: Overwriting at Event timing
- SE: Summing at Event timing:
- OC: Overwriting at Constant timing:
- SC: Summing at Constant timing:

Table 2 summarizes the results for our method. These results indicate that the method of summing at Event timing will be the best in the authentication accuracy. The d-primes of update at Event timing were higher than the conventional method. Comparing conventional method, the d-prime of update at Event timing was improved by more than 0.3. The best result from this evaluation is obtained from the summing at the Event timing. On the other hand, the d-prime of update at constant timing is low. This result suggests that updating of the face information frequently decreases the separation of similarity between the true student and impostors.

Table 2. Results of our method

	Conventional method	Proposal methods			
		OE	SE	OC	SC
d-prime	1.006	1.292	1.317	0.023	0.131
EER	0.235	0.236	0.224	0.500	0.455

The table shows EER and d-prime for each update methods. The EERs of updating at Event timing were about 0.4. We thought the frequent update of the face information makes the FAR high because constant updating uses the face of impostor many times. In the case that the update timing is restricted to the time when a student operates

e-Learning system, the authentication accuracy becomes highest. Comparing update procedures, "summing a face feature vector to each other" makes the EERs higher than overwriting the input face image onto a face image for collating. Comparing conventional method and our methods, summing at Event timing update was lower the EER than conventional method. The EER was improved by more than 0.01.

Figure 5 compares the error rate of the conventional method and that of the Event timing update. The horizontal axis is the threshold, and the vertical axis is the error rate. The FAR is plotted as a blue line and the FRR is plotted as a red line. Dot line means the error rate for conventional method and normal line means that for the update method, which is the overwriting at the Event timing. The FRR for the update method was lower than that of the conventional method and FAR of the update method was higher than that of the conventional method for each threshold. In e-Learning, the spoofing seldom occurs. Therefore, rejecting the true student is more troublesome than accepting impostors. Thus, this result indicates that update method is better than the conventional method.

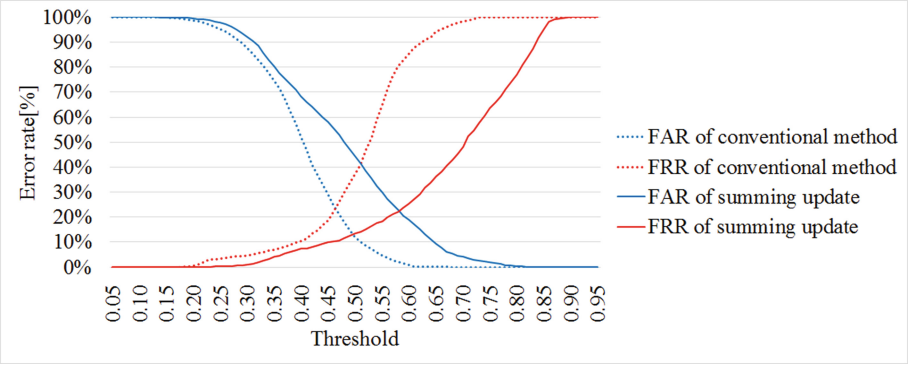

Fig. 5. Error rate curve of conventional method and event timing update method (Color figure online)

The method update the face information unconditionally, even if the input face is the impostor's one. This case causes the high FAR. Therefore, the conditions for updating will be considered in the future work.

4 Conclusions and Future Work

We proposed the authentication method with sequential updates of student's face information for collating using newly input images taken by a web-camera during the e-Learning. In this paper, we examined the update timing and procedure. In the result of analysis, we found that the method of summing at Event timing will be the best in the authentication accuracy.

However, the authentication accuracy of update method is still not enough for the authentication of a student during e-Learning in practice. We will develop a new update method using an updating threshold to improve the false accept rate.

Acknowledgments. This work was supported in part by a Grant-in-Aid for Challenging Exploratory Research (No.15K12427) from JSPS.

References

1. Suzuki, K.: e-Learning in Japan: past, present, and future. In: KAEM and the 4th BK21 GGRTE International Conference: Technology and Future Learning Space Proceedings, pp. 9–17 (2009)
2. Agulla, E., Rúa, E., Castro, J., Jiménez, D., Rifón, L.: Multimodal biometrics-based student attendance measurement in learning management systems. In: 11th IEEE International Symposium on Multimedia, pp. 699–704 (2009)
3. Ahonen, T., Hadid, A., Pietikäinen, M.: Face recognition with local binary patterns. Application to face recognition. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 2037–2041 (2006)
4. Viola, P., Jones., M.: Rapid object detection using a boosted cascade of simple features. Proc. Comput. Vis. Pattern Recognit. **1**, 511–518 (2001)
5. Ojala, T., Pietikäinen, M., Harwood, D.: A comparative study of texture measures with classification based on feature distribution. Pattern Recogn. **29**(1), 51–59 (1996)