LETTER

# Sequential Authentication Using Handwriting Biometrics for Free Response e-Testing

**Taisuke KAWAMATA**[†a)], *Student Member and* **Takako AKAKURA**[††b)], *Fellow*

**SUMMARY** To prevent proxy-test taking among examinees in unsynchronized e-Testing, a previous work proposed an online handwriting authentication. That method was limited to applied for end of each answer. For free response tests that needed to authenticate throughout the answer, we used the Bayesian prior information to examine a sequential handwriting authentication procedure. The evaluation results indicate that the accuracy of this procedure is higher than the previous method in examinees authentication during mathematics exam with referring the Chinese character.

***key words:*** *e-Testing, proxy-test taking, handwriting biometrics*

## 1. Introduction

Unsynchronized e-Testing, in which a test is administered on the Web, saves time and mitigates geographical and spatial restrictions for examinees. The introduction of e-Testing is, however, not gaining acceptance for university classes due to have a risk of proxy test taking between finished and not taken registrants [1]. Many educational institutions authenticate an examinee only at beginning the test, which are vulnerable to exchange the examinees during the test. We thus need to authenticate examinees throughout the test, not only at the beginning.

To solve this problem, a method for individual authentication using a pen and tablet has been proposed [2]. In this method, handwriting information from the tablet is used for online authentication, thus allowing for authentication while not disturbing examinees during the test. However, the previous research [2] depend on the shape of registered characters and cannot apply in the situation such as essay tests that we have little prior knowledge of input texts.

Such problem area is called online writer identification/authentication, has received interest by many researchers. For the essay tests, Furuta et al. [3] proposed a method that is independents on the shape of an answer character based on the sub-stroke. But, this method [3] could not apply to numeric characters that contain curved strokes due to optimize for Japanese kanji (Chinese character). Wu et al. [4] proposed writer identification incorporating the time information by hidden Markov model to improve the performance of the previous identification system which neglects the dynamic information between observations. Kutzner et al. [5] proposed writer authentication using various geometrical, statistical and dynamic features in handwritten cursive texts and single character words. These method [4], [5] has high accuracy with the dynamic information of pen coordinate, but we assumed the pen angle can be taken for prevent to forged writing such as a text made by tracing or copy. In addition, these researches [3]–[5] assume to identify users at the end of the character or text input and calculate the likelihood of being a principle from all of a subdivided character such as stroke unit. So, it is difficult to apply to the free response tests that have to authenticate the examinee in the middle of writing an answer. On the other hand, Kawamata et al. [6] thus proposed updating a reference feature and using window functions for the reduction of the false rejection rate in e-Learning. This method authenticates utilizing not only one information but the multiple information inputted sequentially and showed the importance of time series information in student authentication. However, this method focused on the face authentication in e-Learning. To the best of our knowledge, sequential authentication by strokes inputted during free response tests has been not applied in handwritten answer authentication.

In this paper, we examined a procedure for sequential authentication by using online handwriting answer gathered during a free response test. The procedure was compared with previous examinee authentication [3] in a math exam.

## 2. Methodology

In e-Testing, it is possible for the righteousness likelihood to be lower than the threshold for authentication, which causes false rejection. However, this likelihood is never low throughout the test if the examinee is valid. If the examinee $j$ equals the examinee ID at a certain point $t-1$ during a test, it is likely that the examinee at $t$ is also valid like Fig. 1. We therefore developed a sequential handwriting authenti-

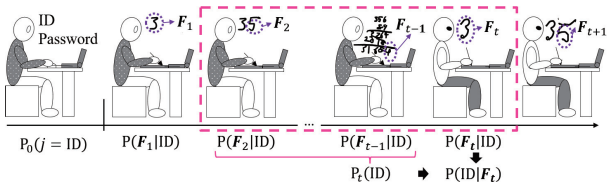


**Fig. 1** Proposed authentication procedure.

Manuscript received August 1, 2019.
Manuscript publicized January 20, 2020.
[†]The author is with Graduate School of Engineering, Tokyo University of Science, Tokyo, 125–8585 Japan.
[††]The author is with Faculty of Engineering, Tokyo University of Science, Tokyo, 125–8585 Japan.
a) E-mail: 4417701@ed.tus.ac.jp
b) E-mail: akakura@rs.tus.ac.jp
DOI: 10.1587/transinf.2019EDL8144

cation used the prior knowledge of registrants. That can be expressed as follows:

$$\mathrm{P}(j|\boldsymbol{F}_t) = \frac{\mathrm{P}(\boldsymbol{F}_t|j)\mathrm{P}_t(j)}{\sum_j \mathrm{P}(\boldsymbol{F}_t|j)\mathrm{P}_t(j)}, \tag{1}$$

where $\mathrm{P}(j|\boldsymbol{F}_t)$ is a conditional probability that the examinee is $j$ in $\boldsymbol{F}$, $\boldsymbol{F}_t = (f_1, f_2, \ldots, f_d, \ldots, f_D)$ is a feature vector extracted from an online stroke taken at $t$ and $j$ is classes of registered examinee. $\mathrm{P}(\boldsymbol{F}_t|j)$ is the likelihood of $\boldsymbol{F}$ occurring given that $j$ is true. $\mathrm{P}_t(j)$ is a prior probability of $j$ at $t$. In this paper, we let each stroke $\boldsymbol{F}_t$ is an independent event. The prior probability for registrant $j$ is calculated as follows:

$$\mathrm{P}_t(j) = \frac{\mathrm{P}(j|\boldsymbol{F}_{t-1})}{\mathrm{P}(j|\boldsymbol{F}_{t-win})}, \tag{2}$$

$$\mathrm{P}_0(j) = \begin{cases} 1-\epsilon & j = \mathrm{ID}, \\ \epsilon & \text{else}, \end{cases} \tag{3}$$

where, *win* is the range of referring to the preceding probability. It is expected small *win* detected the impersonation quickly and small *win* help prevent false rejection. $\epsilon$ means machine epsilon. The calculation $\mathrm{P}_0(j)$ is based on the belief that the examinee is a same user who inputted the ID/Password.

We newly selected the method of feature extraction and likelihood calculation to evaluate the proposed procedure. In follow section, we describes the actual calculation methods of $\boldsymbol{F}$ and $\mathrm{P}(\boldsymbol{F}|j)$.

### 2.1 Implement

The specific authentication schematic is shown in Fig. 2. The left half of the figure shows the process of storing (i.e., registering) feature vectors in the authentication database. A student resists personal information such as signature, department and more by pen tablet for a situation in which identity can be confirmed beforehand. The right half of the figure shows the examination flow, which iterates throughout e-Testing session.

On both flow, the first step is to take an online stroke information. An online stroke $s(t)$, collected using a pen tablet, can be represented as a sequence of points sampled at time $t$ along the stroke's trajectory. The pen tablet in this study, samples 100 points per second. Each point includes five pieces of information: the coordinates of the point $(\mathrm{cx}(t), \mathrm{cy}(t))$, the pen pressure $(\mathrm{p}(t))$, the right/left tilt $(\mathrm{tx}(t))$, and the front/back tilt $(\mathrm{ty}(t))$.

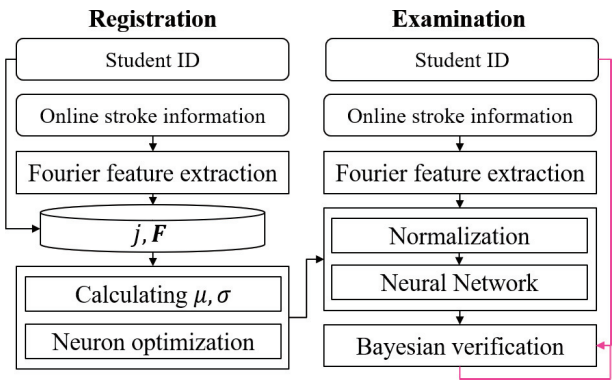


**Fig. 2** Authentication flow.

The second step is to extract a feature from the online stroke information. We adopted the Fourier descriptors used in online signature verification [7]. We can obtain handwriting features from each stroke signal as Fourier described as follows:

$$a_n = \frac{1}{T}\sum_{t=1}^{T} s_t \cos(2\pi n t), \tag{4}$$

$$b_n = \frac{1}{T}\sum_{t=1}^{T} s_t \sin(2\pi n t), \tag{5}$$

where $s_t$ is the input stroke, $T$ is the number of points in the stroke, and $n$ indicates the frequency of the particular harmonic in range $0 < n < N$. We can extract $2N-1$ features containing the mean value $a_0$, sine series $a_{1\sim N}$, and cosine series $b_{1\sim N}$. The Fourier descriptors extracted from the 5 pieces of information are concatenated to describe the stroke feature $\boldsymbol{F}$. We removed the dependence on canvas size and specific character shapes in the stroke authentication by discarding the lowest-frequency components $a_0$ of the coordinates of the points on the stroke trajectory. Therefore, the feature dimension $D$ is calculated as $5(2N-1)-2$.

The third step is to calculate a probability of a login user from $\boldsymbol{F}$. Conventional authentication methods verify a user is valid or not, but we determined that the softmax neural network, that is a multiclass classification method, is effective for the detection of the examinee exchange by registrants. We can obtain a conditional probability $\mathrm{P}(\boldsymbol{F}|j)$ over classes of registered examinee $j$ by using feature $\boldsymbol{F}$ normalized by the averages and the standard deviations of registered $\boldsymbol{F}$:

$$\mathrm{P}(\boldsymbol{F}|j) = \frac{\exp\left(\sum_{h=1}^{D} w_{jh}\mathrm{H}_h(\boldsymbol{F})\right)}{\sum_{j'}\exp\left(\sum_{h=1}^{D} w_{j'h}\mathrm{H}_h(\boldsymbol{F})\right)}, \tag{6}$$

$$\mathrm{H}_h(\boldsymbol{F}) = \frac{1}{1+\exp\left(\sum_{d=1}^{D} w_{hd} f_d\right)}. \tag{7}$$

Here, $w_{jh}$ is optimized by minimizing the categorical cross entropy between estimated probability distributions and true distribution, and $\boldsymbol{w}_h$ is optimized by backpropagation algorithms.

At examination, the online information is inputted to an authentication system every writing stroke. And, the system verifies an examinee with $\mathrm{P}_t(\mathrm{ID})$ in addition $\mathrm{P}(\boldsymbol{F}_t|\mathrm{ID})$.

### 2.2 Evaluation

We used two error rates to evaluate classification error. The first is FRR0, which is the false acceptance rate (FAR) at a threshold such that the false rejection rate (FRR) equals 0%.

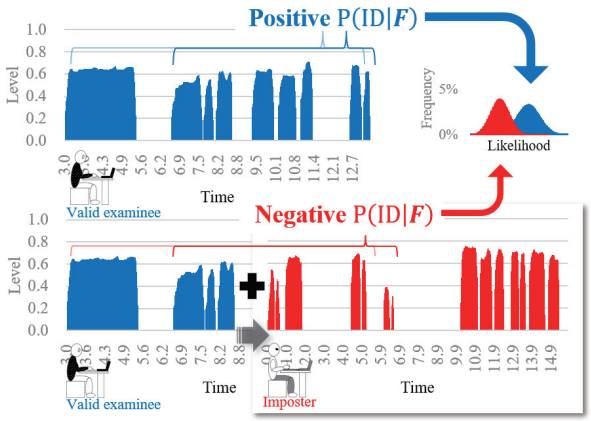


**Fig. 3** Proposed authentication procedure.

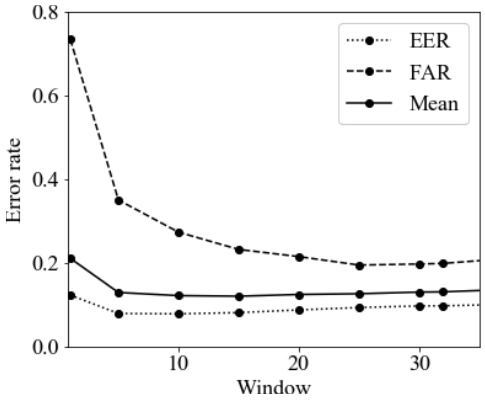


**Fig. 4** Error rate for a range of *win*.

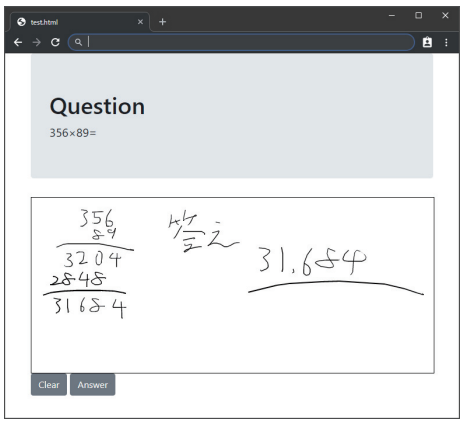


**Fig. 5** Experimental system.

In a regular examination of the university, which adopts absolute evaluation, acceptance of legitimate examinee is more important than a rejection of unauthorized examinees. The reason is the attackers passing exams is not influenced others' evaluation. We thus focused on the FRR0. The second is the equal error rate (EER), which is the error rate at which the FAR equals the FRR. To calculate the error rates, we defined P($\boldsymbol{F}|j$) when participant $j$ took an exam as a positive sample, and P($\boldsymbol{F}|j$) when participant $k \neq j$ took the exam as a negative sample.

Figure 3 shows an example of the positive and negative sample from the analysis. The positive sample means the P($j$ = ID|$\boldsymbol{F}$) when the examinee is a valid one. The negative sample means the P($j$ = ID|$\boldsymbol{F}$) when the examinee is an imposter. We simulated assuming that a valid examinee exchanges own seat to imposter after input $t$ strokes. So, we analyzed strokes from t to end of the test as the negative sample.

### 2.3 Parameter Optimization

To determine the parameter *win*, we used the dataset of Furuta et al. [3]. The participants in the experiment were 12 students at Tokyo University of Science (東京理科大学), who registered 30 kanji characters, including characters from the school name. A week after registration, the participants took an examination consisting of 30 questions which tested their knowledge of kanji.

First, we selected four characters "東", "京", "理", and "科" as registered data of them university name and optimized the $w_{jh}$ and $w_{hd}$ for identifying registrants by these data. Next, we incremented *win* from 5 to 30 s in steps of 5 and calculated the EER, FRR0 and harmonic mean of these error rates for each value of *win*. We adopted the minimum argument *win* of harmonic mean.

We extracted 409 strokes from the registration data and 2,463 strokes from the test data. The number of negative sample is 27,093. The minimum length of a stroke in the registered information was 4 points, so based on the sample rate of 100 points per second, we defined a stroke with duration of less than 40 ms as noise and determined $N = 4$. The feature dimension $D$ is therefore 33. Figure 4 shows the error rate at each *win*. The average error rate of the proposed method was lowest when *win* equals 20. From this result, we decide the *win* = 20.

### 2.4 Experimental Overview

To evaluate the authentication error of the proposed procedure in a free response test, we performed an experiment to obtain writing data. The examinees in the experiment were 12 students who were provided with an overview of the experiment and then wrote the school and department names. They answered questions using the e-testing system showed in Fig. 5. They wrote their calculation processes and answers in e-testing sessions for 2 mathematical questions that each lasted for about 2 minutes.

## 3. Result

We extracted 957 strokes from the registration data and 1,225 strokes from the test data. The number of negative sample is 672,253. We compared the FRR0 of the proposed and previous methods [3]. Figure 6 shows the FAR and FRR of the previous method "SubStroke" [3], the likelihood function and the posterior function at *win* = 20. The error rate

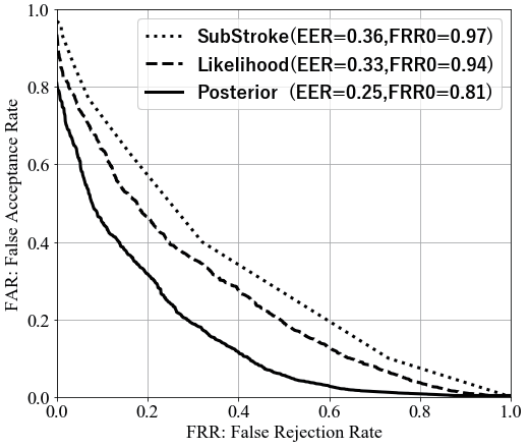


**Fig. 6** Detect error tradeoff curves.

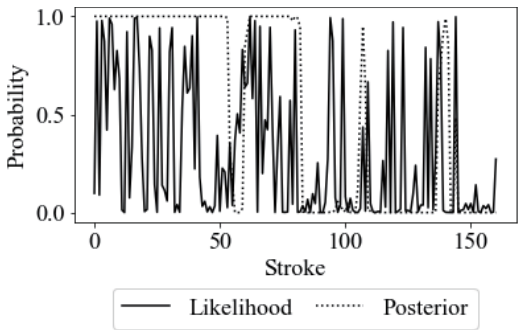


**Fig. 7** Example of probability trends in the spoofing situation.

of the likelihood function was the same that of the previous method. The FRR0 of the posterior function is 78%, which is less than the 97% of the previous method. From these results, it is showed that our proposed method is lower FAR at FRR = 0 than the original method.

Although, the accuracy of our method is lower than general situation. Figure 7 shows a time series of the likelihood $P(\boldsymbol{F}|j)$ as the previous method and the $P(j|\boldsymbol{F})$ as the proposed method in the situation a valid examinee exchanged own seat to an imposter just after the input of 80 stroke. In spite of the valid examinee, the likelihood took a low value during $45 \sim 55$ so proposed method also took a low value at 55 stroke. Figure 8 showed the calculation process at around 50 stroke and the likelihood function cannot identify by a right parenthesis or long horizontal bar like Fig. 8. This result means proposed method depends on the likelihood, and we should examine the classifier selection or output regularization. Therefore, it would be much easier to identify the examinee using those measures. However, the posterior probabilities described as a dotted line in

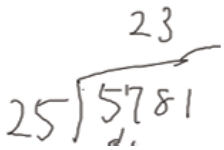


**Fig. 8** Answer text inputted at around 50.

Fig. 7 is high in a lot of time. Therefore, it would be much easier to identify the examinee using those measures. Thus, the proposed procedure was more effective than the previous method of examinee authentication.

## 4. Conclusion

We examined a real time authentication procedure using online handwritten information and bayes theorem to prevent proxy test taking in free response e-testing. The results of our analysis showed that the proposed procedure performed better than the previous method in spite of authenticating the mathematical expression by offering Japanese kanji. However, this procedure has a lower accuracy than the general authentication methods, thus we will examine a method to adapt the parameter *win* of prior information during the test in future studies.

### References

[1] J.A. Wollack and J.J. Fremer, Handbook of Test Security, Routledge, 2013.

[2] D. Hayashi and T. Akakura, "Proposal for writing authentication method using tablet PC and online information in e-testing," Human Computer Interaction International, pp.253–265, June 2018. DOI: 10.1007/978-3-319-92046-7_23

[3] T. Furuta and T. Akakura, "A method for authentication of examinees during e-testing using their styles of handwriting," International Conference of Education, Research and Innovation, pp.1659–1663, March 2014.

[4] Y. Wu, H. Lu, and Z. Zhang, "Text-independent online writer identification using hidden Markov models," IEICE Trans. Inf. & Syst., vol.E100-D, no.2, pp.332–339, Feb. 2017. DOI: 10.1587/transinf.2016EDP7238

[5] T. Kutzner, C.F. Pazmiño-Zapatier, M. Gebhard, I. Bönninger, W. Plath, and C.M. Travieso, "Writer identification using handwritten cursive texts and single character words," Electronics, vol.8, no.4, pp.1–25, April 2019. DOI: 10.3390/electronics8040391

[6] T. Kawamata, T. Ishii, and T. Akakura, "Face authentication for e-learning using time series information," IEEE International Conference on Teaching, Assessment, and Learning for Engineering, pp.116–121, Dec. 2016. DOI: 10.1109/TALE.2016.7851780

[7] B. Yanikoglu and A. Kholmatov, "Online signature verification using Fourier descriptors," EURASIP Journal on Advances in Signal Processing, vol.1, 260516, Jan. 2009. DOI: 10.1155/2009/260516