Technology Reports

Face Authentication Online Testing Fraud Prevention

Online-testing Fraud Prevention System for Detecting Spoofing

Service Innovation Department Kazunori Yamamoto Kazuhiko Ishii Kimihiko Sekino

It is becoming increasingly important to prevent fraudulent activity such as spoofing (impersonation) in online testing that allows individuals to take tests at home and other remote locations. One method of preventing such activity is to have the test proctor monitor the student remotely by camera, but this presents issues from the viewpoint of work efficiency. We have developed an online-testing fraud prevention system that supports test proctors by applying face authentication technology to automatically detect spoofing during an online test. This system can make the proctoring of online tests more efficient.

1. Introduction

The increasing popularity of distance learning [1]–[3] in recent years has led to a desire for online testing that allows students to take tests over the Internet regardless of time or location. In online testing, however, no test proctor is present, so opportunities for inappropriate behavior exist. In addition, fraudulent activity that would be difficult to imagine at a traditional testing center can occur, such as having someone else take the test or receiving answers from someone nearby. The prevention of fraudulent activity by test takers is just as important in online testing as it is in tests taken at traditional sites, and services responding to this need have begun to be provided [4]–[7].

Fraudulent activity at the time of a test includes someone other than the student taking the test (spoofing) and obtaining information during the test by some means (cheating). Examples of

countermeasures to such activity in existing online-testing fraud prevention services are listed in **Table 1**. Although existing services have automated some procedures such as biometric authentication for identity verification at the beginning of an online test, they tend to rely on manual methods for preventing fraud during a test by having a proctor remotely monitor the test taker by camera. It therefore stands to reason that automatic detection of fraudulent activity during a test could make test proctoring much more efficient.

In this article, we focus on the automatic detection of spoofing during a test through the application of face authentication technology. We take up the automatic detection of cheating in future research. Preventing spoofing in online testing requires the detection of both spoofing from the start of the test and switching with another person during the test. It is known that existing face authentication technology can perform its task with high accuracy provided that the entire face is captured looking forward with no parts of the face hidden. In actual tests, however, the posture of the test taker tends to change in a variety of ways, so the simple application of face authentication cannot obtain a sufficient level of detection performance.

In response to this problem, NTT DOCOMO developed fraud detection technology combining face authentication technology and tracking technology[*1] and an online-testing fraud prevention system applying those technologies. This article reports on this online-testing fraud prevention system and its technologies and on the results of a verification experiment using this system.

2. Online-testing Fraud Prevention System

2.1 Overview

The overall configuration of a system providing online testing is shown in **Figure 1**. Online testing is achieved through an online-testing system, which consists of functions for providing tests such as test-application processing, delivery of test problems, and pass/fail notification, and an online-testing fraud prevention system for preventing fraudulent activity. In this article, we focus on the online-testing fraud prevention system and assume the online-testing system to be an existing system.

The purpose of the online-testing fraud prevention system developed by NTT DOCOMO is to

Table 1 Examples of countermeasures to fraudulent activity in existing online-testing fraud prevention services

	Examples of preventing fraudulent activities
Spoofing	· Identity verification before the test by face authentication [4] [7] · Identity verification by keystroke dynamics [4] · Camera monitoring of test taker by remote proctor [4]–[7]
Cheating	· Camera monitoring of test taker by remote proctor [4]–[6] · Monitoring of test taker's computer screen by remote proctor [5] · Monitoring of test taker's microphone-captured speech by remote proctor [4] [6] · Restricted launching of applications other than those for test taking [4] [6] · Recording of test taker's camera video (to obtain evidence of any fraudulent activity) [4]–[6]

*1 Tracking technology: A technology that tracks a target object in a consecutive sequence of images such as video.

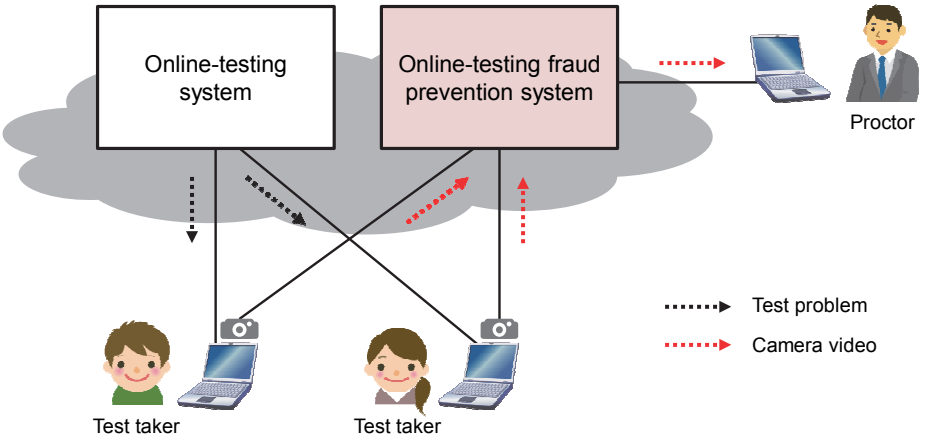


Figure 1 Overall configuration of online-testing system

support test proctors by automatically detecting spoofing through the application of face authentication technology. The following issues arose in the development of this system with regards to enrolling a facial image for cross-checking in face authentication and providing support for test proctors.

(1) Face-image enrollment
- Insuring the identity of the enrolled facial image
- Obtaining a facial image suitable for use in face authentication

(2) Proctor support
- Reliable acquisition of camera video of each test taker during testing
- Automatic detection of spoofing
- Presentation of easy-to-understand detection results to the test proctor
- Saving of evidence of fraudulent activity

The online-testing fraud prevention system consists of a facial-image enrollment function, camera-video acquisition function, video recording function, fraud detection function, and fraud-detection notification function (**Figure 2**). The following describes how each of these functions resolves the above issues.

2.2 System Functions

1) Facial-image Enrollment Function

This function enrolls the test-taker's facial image for cross-checking during face authentication and an image of an identity verification document such as a public identification card for verifying the identity of that facial image. The test taker enrolls a facial image beforehand using a camera connected to the computer being used. At that time, the system guides the test taker in how to capture a clear image of his or her entire face under good

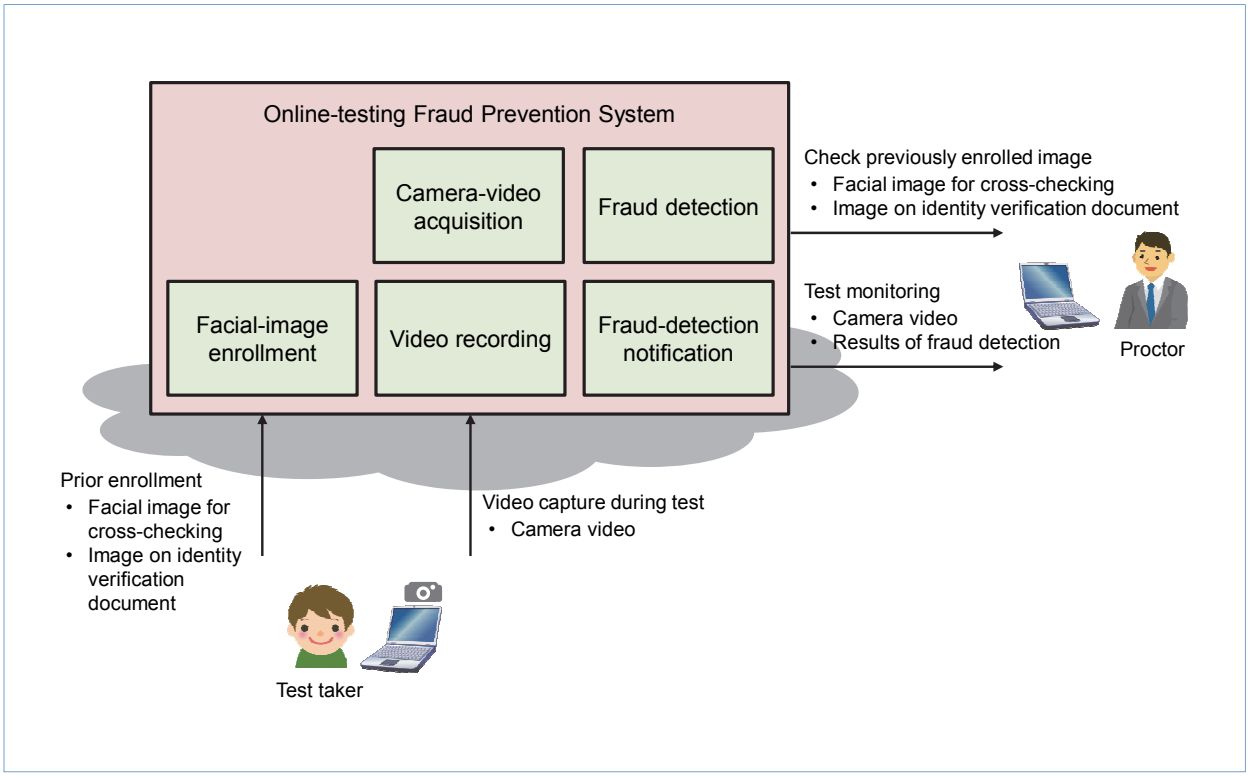


Figure 2 Configuration of online-testing fraud prevention system

lighting conditions. The proctor visually checks whether the enrolled image is suitable enough to identify the test taker in conjunction with the identity verification document and act as a biometric template in face authentication.

2) Camera-video Acquisition Function

This function obtains video of the test taker during the test using a camera connected to the computer. The video is used to automatically detect spoofing during the test and to enable monitoring by the test proctor. If the communications environment should degrade, this video can be obtained through automatic reconnection to the extent possible.

3) Video Recording Function

This function records the video obtained by the camera-video acquisition function. The video is reviewed by the proctor after the test and used as evidence if fraudulent activity has occurred.

4) Fraud Detection Function

This function automatically detects spoofing by applying the fraud detection technology described later to the camera video of the test taker during the test.

5) Fraud-detection Notification Function

This function notifies the proctor of any occurrence of spoofing. Two types of monitoring methods are provided here: monitoring of real-time video simultaneously with the test and viewing of the

video after the test. Typical screenshots of the proctor's screen for both methods are shown in **Figure 3** and described below.

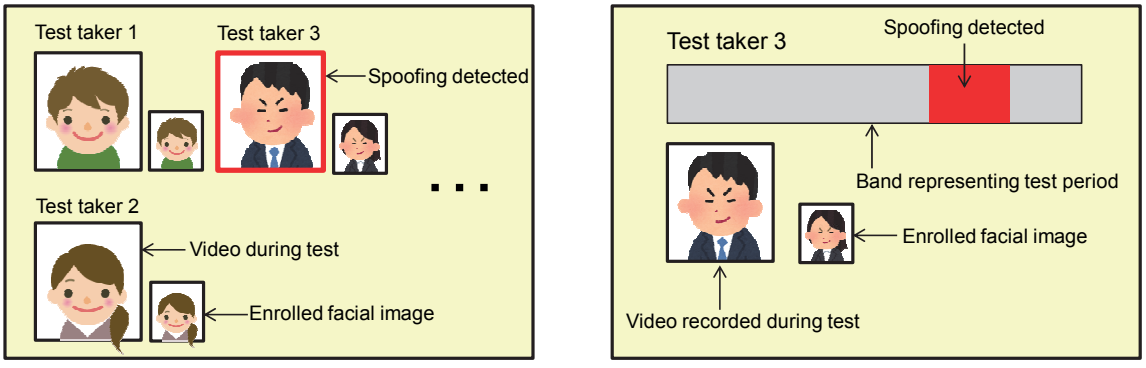
- In monitoring by real-time video, a red frame is displayed around the video of that test taker if spoofing is detected and an alert is generated for the proctor (Fig. 3 (a)). This scheme enables a higher number of students that can be simultaneously monitored compared with that by simple visual monitoring.
- In monitoring by recorded video, the occurrence of any spoofing along the band representing the test period is displayed in red at the time corresponding to its detection (Fig. 3 (b)). Clicking on the red portion plays back that video skipping the portion up to that time. This scheme enables the proctor to closely examine the location at which spoofing is suspected thereby shortening checking time significantly compared with viewing the video from the beginning.

3. Overview of Fraud Detection Technology

3.1 Problem of False Positives in Online Testing

The test taker's facial expression and posture can vary in the following ways during testing:

- Change in facial expression (due to frowning, yawning, etc.)
- Change in facial orientation (by looking away, lowering one's eyes, etc.)
- Partial hiding of face (by covering mouth with hand, etc.)
- Partial distortion of face (by resting chin on hand, etc.)



(a) Monitoring by real-time video

(b) Monitoring by recorded video

Figure 3 Typical screenshots of proctor's screen

These types of changes can cause the accuracy of face authentication to vary greatly. A problem therefore arises in the simple application of face authentication technology, namely, the frequent occurrence of false positives in which spoofing is judged to have taken place despite the fact that no spoofing actually occurred. Changes in posture and facial expression may be temporary in nature or comparatively long. Given the reality of such changes, finding a way to reduce the occurrence of false positives in fraud detection during online testing has become a key issue. The following describes a method for solving this issue.

3.2 Fraud Detection Technology

The system uses fraud detection technology to perform face authentication against still images extracted at fixed intervals from the video of the test taker as a basis for judging the occurrence of spoofing. However, using the results of face authentication as-is to make a judgment can result in false positives as described above, so the system performs face authentication based on a history of face authentication results and tracking results.

1) Use of Face Authentication History

This fraud detection technology uses a history of face authentication results instead of a single face authentication result at that time to detect spoofing. This has the effect of absorbing temporary fluctuations in face authentication accuracy and decreasing false positives. However, when attempting to absorb long-term changes in posture and facial expression using such a history, a delay in detection can occur or detection of short-term switching with another person becomes impossible. For this reason, a history of face authentication results is used for dealing with short-term changes such as looking away from the computer briefly.

2) Application of Tracking Technology

Fraud detection technology prevents false positives due to long-term changes in posture or facial expression by combining tracking technology with face authentication technology to track the test taker. This tracking technology is used to track the test taker using the last successfully authenticated facial image as the start point. That person is therefore judged to be the target test taker as long as tracking continues to be successful. On the other hand, tracking technology is not authentication technology, so the possibility exists that an impersonator who has taken the place of the test taker will be erroneously tracked and that switching with another person will be missed. Our fraud detection technology prevents the missing of such switching by taking into account the distance moved by the test taker. Additionally, to deal with the problem of a partially concealed face, the similarity of image areas can be calculated by reducing the effect of that concealed portion thereby raising the success rate of tracking.

4. Verification Experiment

Before performing a verification experiment, we evaluated scenarios in which the test taker would intentionally switch with another person. We then prepared an actual qualifying exam in cooperation with a certifying organization and a

test delivery operator and performed a total of two verification experiments using our online-testing fraud prevention system in March 2016 and March 2017.

Based on the results of these experiments, we confirmed that the developed fraud detection technology could detect spoofing and curb the occurrence of false positives due to changes in the test taker's posture and facial expressions. We also confirmed that both the real-time-video and recorded-video monitoring methods could provide the results of spoofing detection in an easy-to-understand manner thereby providing effective support for test proctors.

5. Conclusion

Focusing on the automatic detection of spoofing in online testing, this paper presented the technical issues involved, described an online-testing fraud prevention system and associated fraud detection technologies for solving those issues, and demonstrated the effectiveness of the system through a verification experiment. In future research, we plan to study the automatic detection of cheating in online tests.

REFERENCES

[1] Coursera Website.
https://www.coursera.org/
[2] edX Website.
https://www.edx.org/
[3] JMOOC Website.
https://www.jmooc.jp/
[4] KRYTERION Website.
https://www.kryteriononline.com/
[5] ProctorU Website.
https://www.proctoru.com/
[6] RPNow Website.
https://www.psionline.com/platforms/rpnow/
[7] H. Kawahara: "Student Authentication for Course Credit in Distance Learning," Journal of Multimedia Education Research, Vol.7, No.1, 2010.
http://www.code.ouj.ac.jp/media/pdf/vol7no1_shotai7_071.pdf