Towards a Blob-based Presence Verification System in Summative E-assessments

Kikelomo Maria Apampa, Gary Wills, David Argles
School of Electronics and Computer Science, University of Southampton, UK

Abstract

Traditionally, authentication systems are required to verify a claimed identity only one time at the initial login. However, in high-stake environments such as a summative e-assessment environment, a one-time authentication session is insufficient to guarantee security. Hence, the security of online summative assessments goes beyond ensuring that the 'right' student is authenticated at the initial login. More is required to verify the presence of an authenticated student for the duration of the test. In this paper, we explore potential approaches to achieving presence verification. However, these approaches have limitations that make them unsuitable for verifying presence in e-assessments. Hence, we propose a novel blob-based system to detect the presence and activities of a student. By exploiting the significant statistical information inherent in blob statistics, we investigate the feasibility of blob-based presence verification in e-assessments.

Influenced by advances in technology, the assessment process has begun to make its way out of the traditional classroom into online environments. The online summative assessment is categorised as a high-stake assessment which count towards a final course mark. There exists enormous advantages in adopting summative e-assessments over traditional methods, this include automated marking, immediate feedback and on-demand tests. In higher education, summative e-assessments can occur in supervised and non-supervised environments. Supervised environments include campus based exams and authorised test centres (Rowe, 2004), whilst non-supervised environments include distance learning examinations and on-demand tests. The distinction between the former and latter environment is
based on the inclusion or exclusion of an authorised invigilator/proctor. In the context of this paper, we assume summative e-assessments conducted in a supervised/controlled environment. Thus, amidst the benefits of online summative assessments, the e-assessment user security process is susceptible to impersonation challenges which affect its reliability and efficiency (Kerka and Wonacott, 2000).

In this paper, we associate the impersonation threats perpetrated in e-assessment environments to the exclusion of presence verification throughout the test session. Furthermore, we explore the potential approaches which can be used to achieve presence verification and finally we present a blob-analysis approach towards verifying presence in summative e-assessment environments.

**Impersonation threats in Summative E-assessments**

The code of practice for the Assurance of Academic Quality and Standards in Higher Education (QAA) for the UK suggests that, an academic misconduct with respect to e-assessment would include plagiarism, collusion, impersonation and the use of inadmissible material (Quality Assurance Agency, 2000). In higher education, security considerations do not feature prominently; however, this changes when an online environment is considered (Furnell et al., 1998). Thus, due to the increased influence of technology in assessments, it is often easier to cheat online (Rowe, 2004). In e-assessments, the issue of impersonation is considered as a major concern and it is perceived as an even greater risk by the academic community (Quinn et al., 2003).

During an online assessment, a student cannot ‘accidentally’ impersonate another (Stoner, 1995); thus, the fraudulent act is an intentional collusion between two or more people.

In this paper, we do not generalise impersonation threats; rather, we classify the threats into Type A, Type B and Type C. The Type A or ‘connived impersonation’ threat occurs when an invigilator willingly colludes with fraudulent students to perpetrate an impersonation. A connived impersonation may originate from a feeling of sympathy towards the student; thus, an external person may be allowed to take a test on behalf of a legitimate student. This paper does not eliminate the use of a human invigilator; however, the correctness of a student during an online test should be carried out independent of an invigilator. The Type B impersonation threat can occur as a result of the strength or weakness of the authentication method adopted. User authentication is the process of confirming that the identity claimed actually belongs to the user requesting access. Furnell et al., (2000) describes categories of authentication methods, they are possession (e.g. smart cards, keys), knowledge (e.g. passwords, PINs) and biometrics (e.g. fingerprint, face recognition). For example, employing a password method for an online test makes a Type B threat more appealing to impersonators, whilst a biometric method may deter impersonation. A Type C impersonation threat occurs, when an external person substitutes a correctly authenticated student during the test session. As pointed out in recent studies (Aojula et al., 2006; Hernandez et al., 2008), a major challenge when conducting summative e-assessments is the inability to determine the correct identity of the person taking an exam over a specified time i.e. to know if the correct student is there taking the exam or someone else has taken over the test on their behalf.

In summative e-assessment security, a student’s identity and authentication details are useful to provide user security; however, using these details only is insufficient to minimise impersonation. Hence, in our previous work (Apampa et al., 2009), we
proposed that the verification of a student’s presence throughout the test session will minimise impersonation threats and improve the e-assessment security.

**Presence Verification in E-assessment Security**

A major goal of the presence verification process is to ensure the presence of a correctly authenticated student for the duration of the online summative test. This implies that the authenticated student starting the e-assessment should remain the same student throughout the test session. However, due to the high-stake nature of summative e-assessments, it is perceived that these tests can easily attract impersonation threats. Hence, there is a need to verify the presence of an authenticated student beyond the initial login procedure. This section describes briefly, the potential approaches which can be employed to achieve presence verification during summative e-assessments. Table 1 shows a summary of the advantages and disadvantages of the methods.

*Invigilation*

In summative e-assessment environments, an invigilator/proctor is required to provide extra security alongside the identity and authentication goals. The advocates of human invigilators in online environments, (Rowe, 2004) describe the method as a low technology means of promoting both identity and academic honesty. This paper does not eliminate the use of an invigilator for summative e-assessments; however, an invigilation only approach may have limitations for verifying student’s presence.

*Passwords*

Adopting passwords provide a simple and easy-to-use method to realising presence verification in summative e-assessments. However, this method promotes the chances of impersonation threats, due to its shareable attributes. Employing a password to verify presence throughout test requires that the student continuously re-types his/her password following a fixed or random pattern. This method is perceived to be inconveniencing and distracting to the student’s concentration.

*Unimodal Biometric (active)*

In summative e-assessments, biometric solutions such as fingerprint and face recognition methods are suggested to enhance security and minimise impersonation threats. Thus, it is expected that only correct students can perform a successful login, due to the unique attributes of a biometric. To achieve presence verification, a continuous re-scan of the student’s fingerprint throughout the test session is required. This method is perceived *interruptive* and distracting to the student’s concentration. In this paper, the term interruptive refers to the ability of an event to interfere with and alter a sequence of normal activities.

*Unimodal Biometric (passive)*

In biometric systems, the face recognition is an example of a passive biometric method that can be used for continuous authentication. However one of the challenges in a continuous authentication is the large processing power consumed to compare the biometrics during the authentication process (Stallkamp *et al*, 2007). In a summative test, continuously authenticating a student’s face will be impractical and expensive. Additionally, one of the prominent problems encountered in face recognition technology, is the intolerance to pose variations (Zhang and Gao, 2009). Most face recognition systems are optimised for frontal views only; thus, the selection of frames which contain frontal face images is important for successful face authentication *(Blanz *et al*, 2005).*
In summative e-assessments, it is possible that a student would not maintain an acceptable frontal pose required for the re-authentication process at all times. This could be as a result of varying poses caused by student activities. For example, a student’s face may be partially occluded from the camera’s view due to tilting of the head. Thus, if this occurs during a re-authentication process the biometric system will be unable to authenticate the student’s face. Hence, the consequence will be an interruptive re-authentication request or an automatic log out.

**Multimodal Biometrics**

Multimodal biometrics is new to e-assessment; and there exists few proposals in adopting the concept. Levy and Ramim, (2009) propose a model for the integration a fingerprint and web-camera head geometry scanner. The focus in their paper was a survey on the intentions of using multi-biometrics, but there was no implementation of the actual system. However, a multi-biometric solution is as effective as the individual biometrics integrated. In addition, continuous authentication of the multi-biometric traits will incur a high computational cost (Klosterman and Granger, 2000).

**Video and webcam solutions**

Ko and Cheng (2004), propose a secure internet examination system based on random video monitoring. In another work, Hernandez et al, (2008) used the biometric fingerprint for authentication and a webcam for monitoring the students in real-time throughout the test. The similarity between the video and webcam solutions is the human invigilator monitoring the environment via a screen. Thus, there exist the possibilities of connived impersonation, error-prone decisions and administrative overhead.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Method</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous User Monitoring</td>
<td>Invigilation</td>
<td>i. Provide extra security in online test environments</td>
<td>i. Possibility of connived impersonation threats</td>
</tr>
<tr>
<td>Face-to-face Monitoring</td>
<td>Passwords</td>
<td>i. Simple and easy to use</td>
<td>i. High chances of impersonation threats</td>
</tr>
<tr>
<td></td>
<td>Fingerprint biometric</td>
<td>i. Accepted in e-assessments</td>
<td>i. Interruptive and distracting</td>
</tr>
<tr>
<td></td>
<td>Face biometric</td>
<td>i. Accepted in e-assessments</td>
<td>i. Potential for false rejects during e-assessment</td>
</tr>
<tr>
<td></td>
<td>Multimodal biometric</td>
<td>i. Potential to provide high-level security</td>
<td>i. Computationally expensive</td>
</tr>
<tr>
<td></td>
<td>Video/Webcam</td>
<td>i. Provides continuous monitoring, that is void of interruption</td>
<td>i. Non-automatic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ii. Dependent on human resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>iii. Potential for administrative overhead</td>
</tr>
</tbody>
</table>
Object Tracking Approach: A Blob Analysis Solution

From the table 1, it is observed that a connived impersonation is possible when presence verification is completely reliant on a human invigilator. A user password is simple to use; however, the method can be easily compromised and it possess interruptive traits. The susceptibility of the invigilation and password methods to impersonation threats would defeat the purpose of presence verification; since, there exists a possibility that the presence of an illegal student may be verified instead! Thus, adopting the biometric solutions would minimise impersonation threats; however, these methods have a potential to become interruptive and distracting when the re-authentication process is initiated constantly. Additionally, it is computationally expensive to perform biometric authentication constantly in a summative e-assessment environment. Lastly, the video/webcam solutions are non-automated methods for verifying presence as they largely depend on human resources.

Hence, to address the short comings of these approaches outlined above, this paper proposes a blob analysis solution which follows an object tracking approach. In the approach, the detected object in the video sequences is tracked to estimate the object motion information. Thus, the proposed solution uses the geometrical statistics of the blobs to make inferences about an object’s presence in the video frame. A blob (binary large object) is defined as a region of connected pixels within an image, in which all the pixels have the same logical state. Blobs can correspond to actual object or parts seen in the image. This paper suggests that, it is feasible to analyse the variability and stability of the blobs found in an object within a video frame. Furthermore, the analysis of the blobs would present statistical information which can be useful in determining an object’s activity in each video frame. In this context, an activity is described as incidents which occur in a video frame. An object executes an activity within an environment and this could be normal or abnormal. For example, in a test environment, the presence of an object is normal whilst the absence of the same object is abnormal. However, there exist sub-activities of a ‘present’ object that indicates abnormal behaviours e.g. a blob has merged with another blob. Thus, one of the goals of this paper is to investigate the feasibility of using blob statistical information to determine normal or abnormal activities in a summative e-assessment environment. We describe examples of existing blob statistics with implications for the proposed solution below:

Area

This represents the actual number of pixels in the foreground object (blob) i.e. the non-black pixels in an image. Figure 1 depicts the filled region of an ellipse corresponding to the area of the blob. The blob area is useful in determining the variations of the blob size. For example, in a merged blob, the blob sizes can indicate the presence of more than one object. In our proposed system, the blob area will be exploited to estimate an object’s pose and to detect multiple presence.

Extent

This represents the proportion of the pixels in the bounding box that are also in the blob, i.e. the area of the blob divided by the area of the bounding box surrounding it (both in pixels). An increase or decrease in the blob area will determine an increase or decrease in the extent value. For example, an increase in blob area will imply that a large percentage of bounding box is occupied (see figure 1). In our system, the
extent statistics is exploited to detect possible camera occlusion and to provide information of the objects distance from a camera.

\[
\text{extent} = \frac{\text{blob area}}{\text{bounding box area}}
\]

**Major and Minor axes**

The major axis and minor axis represents the longest and shortest axes of an ellipse (see figure 2). In this study, a variation in blob shape is attributed to the ratio of the major axis of the ellipse to its minor axis given by

\[
\frac{\text{ellipse major axis}}{\text{ellipse min or axis}} = \frac{a}{b}
\]

**Orientation**

This represents the angles (in radian ranging from $-\pi/2$ and $\pi/2$) between the $x$-axis and the major axis of the ellipse (see figure 2). The blob orientation provides precise information regarding an object’s pose and position within the cameras field of view. For instance, an object looking straight at the camera (i.e. perpendicular to the cameras field of view), will obtain an orientation of $90^\circ$. Similarly, an object lying parallel to the cameras field of view will obtain an orientation of $0^\circ$. In our proposed system, the orientation statistics is useful to accurately estimate an object’s pose or direction.

**Count**

In this paper, the blob count statistics is introduced to determine the number of objects present in a video frame. In our system, the count statistics is useful for detecting single or multi-presence in an environment.

Towards a Blob-based Presence Verification System

From the sections above, the proposed blob analysis solution exploits the geometric statistics of a blob to determine the current activity of a monitored object in a video frame. For example, by using orientation statistics, an object gazing directly at a camera can be accurately estimated (figure 3a). Similarly, the extent statistics can provide information about an object’s distance from the camera (figure 3b), whilst the count statistics can detect multi-presence in the video frame. Figures 3a depicts an object’s frontal pose with the orientation approximately $90^\circ$. It is assumed that the same object shown in figure 3a is depicted in figure 3b; however, the blob in figure 3b shows a reduction in area which would effectively produce an increase in
the extent statistics ratio. Thus, based on these simple instances it is suggested that a variety of activities can be precisely deduced from the blob statistics. Table 2 shows suggested activities in a summative e-assessment environment that can be detected using blob analysis.

Hence, to develop the blob-based presence verification system, an activity risk classification strategy is proposed. In this method, the changes in the blob statistics values between successive video frames are aggregated to form a single value. This value is then fed into a fuzzy blob classifier engine which produces a decision that depicts the status of the object’s presence at the time. The decision process (a.k.a. threat classification scheme) is a list of three decision tasks namely, low-risk, elevated-risk and high-risk. Thus, in the activity risk classification method, an object’s presence status is inferred by classifying the statistical changes identified from the blobs detected in the video frame. Figure 4 shows a conceptual diagram of the proposed activity risk classification method. From figure 4, it is observed that an object is monitored via continuous video signal and the first step is to segment each video frame to detect the object; this is known as foreground segmentation. In this step, a static background image is separated from the current image to detect the object. The result is an intensity image which is then thresholded to obtain a binary image required for the blob analysis operation. In the blob analysis process, the foreground pixels are segmented in order to select the blobs (i.e. the connected pixels) from the binary image. Lastly, the blobs are analysed to extract the relevant statistical values which can be used by the activity risk classification method to verify presence.

### Table 2 Object activities and Relevant blob statistics

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Activity examples</th>
<th>Blob description</th>
<th>Relevant statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible activities to substitute the original student or provide assistance towards the test</td>
<td>External person behind student</td>
<td>A new blob appears</td>
<td>Area Count (&gt; 1)</td>
</tr>
<tr>
<td></td>
<td>External person beside student</td>
<td>Blob has merged with another blob</td>
<td>Area Count (&gt; 1)</td>
</tr>
<tr>
<td></td>
<td>External person substitute student</td>
<td>Old blob disappears</td>
<td>Area Major/minor axes</td>
</tr>
<tr>
<td></td>
<td>Face close to camera</td>
<td>Blob moving towards camera</td>
<td>Extent Area</td>
</tr>
<tr>
<td></td>
<td>Hand blocking camera</td>
<td>Blob moving towards camera</td>
<td>Extent Area</td>
</tr>
</tbody>
</table>

### Discussions and Conclusion

One of the benefits of the blob analysis solution is its low-resource consumption i.e. the process is computationally inexpensive. The low resource benefit can be attributed to the connected pixels which are represented in a single dimensional
binary image. The blob analysis method produces valuable gains as opposed to employing biometric methods which are computationally expensive. Additionally, blob-based techniques are known to be successful and time efficient, especially in environments with low numbers of moving objects (Zang & Klette, 2003). During a typical summative e-assessment, the test environment is limited to the authenticated students concentrating on the test task. Thus, the blob operation will be administered to the students individually.

Another key advantage of the blob analysis solution is realised through a novel blob classifier engine embedded within the activity risk classification method. The blob classifier initiates change-driven re-authentication requests only. Recall that, employing biometric technologies for presence verification can lead to frequent re-authentication requests which may become distracting to a student. Thus, in a change-driven approach, a student is only interrupted when there are significant changes to the blob statistical values. For example, when a student’s current activity statistics vary significantly relative to the frontal statistics. Hence, the blob analysis technique is able to achieve presence verification with minimal distraction to the student.

The second advantage is quite useful as it promotes a fair assessment. Fairness is a fundamental principle in the design and administration of assessments. An unfair disadvantage may occur when a student’s test is interrupted which may lead to a low performance. In high-stake tests, it is required that students have total concentration and minimal external interruption for the duration of the test. Additionally, as stated in section 7 of the Regulatory Principles for E-assessment, “the use of technology should not inhibit a candidate’s performance” (QCA, 2007). Thus, in summative e-assessment environments, it is essential that the technologies employed do not become interruptive or distracting to the students task.

In this paper, we have proposed a novel blob-based approach to presence verification in summative e-assessments. We have investigated the feasibility in using blob statistics to detect a student’s current activity in an e-assessment environment. We conclude that introducing video and image processing techniques to improve the security in e-assessment is a feasible research area. Thus, our current work focuses on implementing the presence verification system and the blob classifier engine in test environments.

![Figure 4. A Conceptual Diagram for Activity Risk Classification Method](image-url)
References


Qualifications and Curriculum Authority (2007), 'Section 7: Avoidance of barriers to New Technology for Learners’ in Regulatory Principles for E-assessment, UK.


Quinn, P., Muldoon, N., M. Mozer (2003), 'An institutional re-positioning of examinations', 16th ODLAA Biennial Forum Conference Proceedings

Rowe, N. C. (2004). Cheating in Online Student Assessment: Beyond Plagiarism, Online Journal of Distance Learning Administration VII (II)


Zhang, X. & Gao, Y (2009), Face Recognition across pose: A review. Pattern Recognition, 42 (11) pp 2876 - 2896