Authors	Kikelomo Maria Apampa, Gary Wills, David Argles. School of Electronics and Computer Science, University of Southampton
Address for correspondence	Learning Societies Lab, School of Electronics and Computer Science, University of Southampton, Highfield, Southampton, UK, SO17 1BJ. (kma07r,gbw,da)@ecs.soton.ac.uk

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

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 an object tracking approach using a blob analysis solution. The blob analysis solution is a video processing technique that attempts to detect, verify and classify a student's presence throughout the test session. Thus, indicating the likelihood of acceptable or unacceptable activities. By employing the blob analysis operation, we propose a novel blob-based presence verification system which uses the geometric statistics of binary images to make inferences about an object's presence in the video sequence. The proposed system is designed to verify the student's presence in a non-interruptive and non-distracting fashion. Furthermore, by simulating possible student activities in test conditions, we carried out experiments to investigate the feasibility of using blob analysis for presence verification. In addition, the decisions made about a student's presence in the test environment were driven by a set of well-defined Fuzzy Logic rules. The results show that, the verification of a student's presence presents valuable improvements to preserving e-assessment user security.

Keywords

E-assessment security, Authentication, Presence verification, Blob analysis

Introduction

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 summative e-assessments

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 1 *Advantages and disadvantages of existing methods*

Approach	Method	Advantages	Disadvantages
Face-to-face Monitoring	Invigilation	i. Provide extra security in online test environments	i. Possibility of connived impersonation threats
Continuous User Authentication	Passwords	i. Simple and easy to use	i. High chances of impersonation threats ii. Interruptive and distracting
	Fingerprint biometric	i. Accepted in e-assessments ii. Minimise impersonation threats iii. Enhances security	i. Interruptive and distracting ii. Potential for false rejects during e-assessment

	Face biometric	i. Accepted in e-assessments ii. Minimise impersonation threats iii. Enhances security iv. Non-intrusive	i. Computationally expensive ii. Potential to be interruptive and distracting
	Multimodal biometric	i. Potential to provide high-level security	i. Computationally expensive
Continuous User Monitoring	Video/Webcam	i. Provides continuous monitoring, that is void of interruption	i. Non- automatic ii. Dependent on human resources iii. Potential for administrative overhead

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 statistics 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 statistics information to determine acceptable or unacceptable 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.

$$extent = \frac{blob\ area}{bounding\ box\ area}$$

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

$$\frac{ellipse\ major\ axis}{ellipse\ \min or\ axis} = \frac{a}{b}$$

Orientation

This represents the angles (in radian ranging from -π/2 and π/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 90^0. Similarly, an object lying parallel to the cameras field of view will obtain an orientation of 0^o. 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.

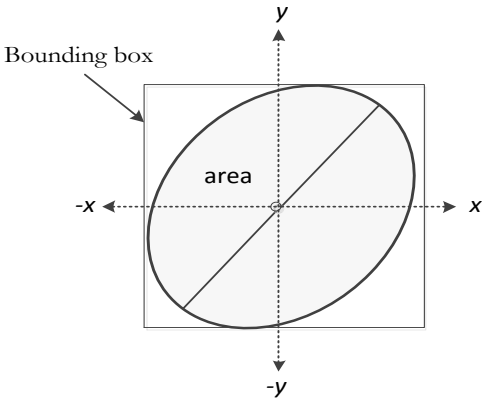


Figure 1. *Area and Extent*

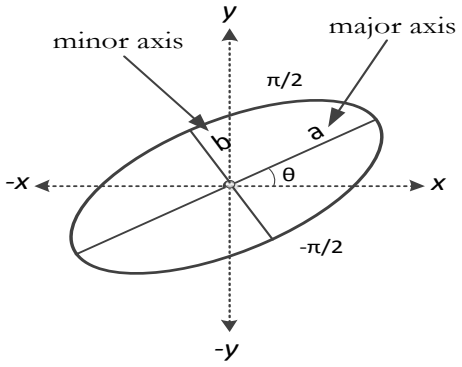


Figure 2. *Orientation, Major and Minor axes*

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 90^0. 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. Hence, to develop the blob-based presence verification system, an Activity Risk Classification strategy is proposed. This method uses a combination of blob statistics to determine the likelihood of acceptable and unacceptable object activities in an environment.

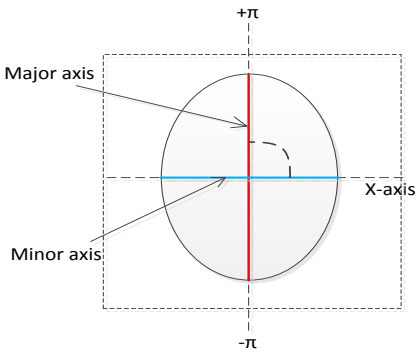


Figure 3a. Frontal Pose

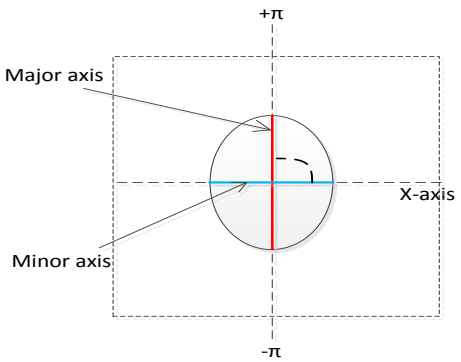


Figure 3b. Area and Extent

Activity Risk Classification strategy

In The Activity Risk Classification (ARC) approach, individual blob statistics are collated and analysed to achieve a relationship between the object's frontal pose statistics and the changes in the object's current activity statistics. This relationship depicts that, the changes in the blob statistics of the current activity is a function of the frontal pose of the same object. In practical terms, this can be used to determine the *sameness* property of the object irrespective of varying activities. The sameness attribute is the ability of a verification system to determine that the object detected in the first frame (frontal pose statistics) is the same object detected in the current

frame (current activity statistics). Thus, the relationship between the frontal pose statistics and the current activity statistics is defined as:

$$\Delta P_{X[A]} \approx f\left(P_{F[A]}\right)$$

where, Δ is the change in blob statistics for Object A's current activity, $P_{X[A]}$ is the blob statistics for object A's current activity and $P_{F[A]}$ is the blob statistics for object A's frontal pose. The frontal pose statistics is composed of the initial blob statistics which are extracted and stored; whilst the current activity statistics are the blob statistics which are extracted as long as the object is detected in the video sequence. The changes in the blob statistics between successive video frames are then fed into a fuzzy blob classifier engine which produces a decision that depicts the object's presence at the time. The five input variables required for the fuzzy blob classifier engine are *size (area), shape (major axis/minor axis), position (orientation), extent and count.* The output variable forms the conclusion about the potential threat risk of the object's presence to the environment. This implies that, for a given video frame the output variable will represent one of the threat classification schemes. The threat classification scheme is a list of three decision tasks namely, low-risk, elevated-risk and high-risk. Finally, the numeric range of the input and output variables are derived via heuristics. Additionally the numeric range also influences the input and output spaces in the design of the Fuzzy Logic membership functions.

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 thesholded 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 blob statistic values which is used by the activity risk classification method to execute the presence verification process. Figure 5 shows an experiment of the initial stages of the Activity Risk Classification method

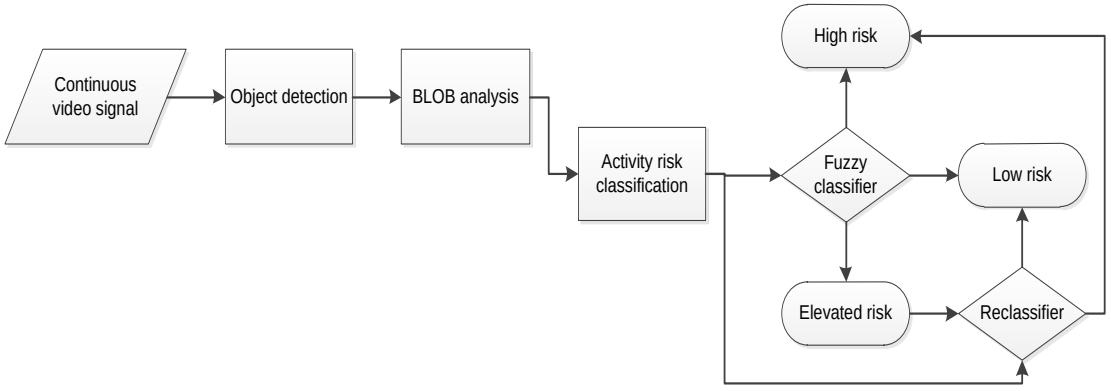


Figure 4. *A conceptual diagram for Activity Risk Classification method*

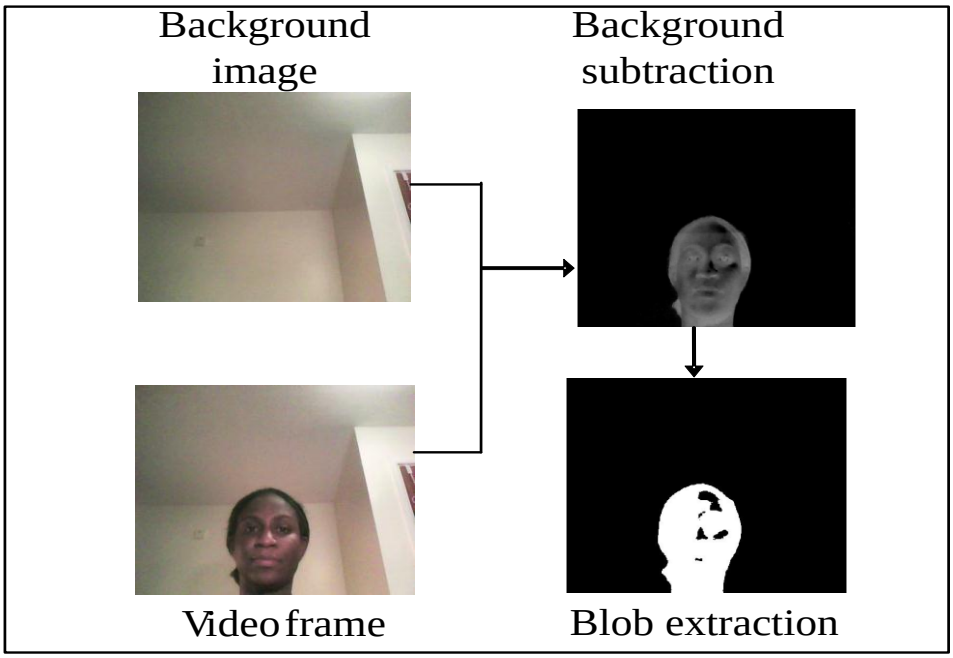


Figure 5. *Initial stages for Activity Risk Classification method*

Experimental data

The blob-based presence verification system was developed using the MATLAB/Simulink Video and Image processing Blockset. The experiments were setup with five video sequences involving volunteers. The datasets were filmed in an indoor environment with the volunteers simulating the activities in a natural test environment; thus, the individuals were not constrained to a fixed position. The videos were recorded at a real time frame rate (25 frames / second) for a video frame size of 640 X 480 pixels using a laptop integrated webcam. However, using an inexpensive webcam mounted on a PC would produce similar results. The videos were recorded in an AVI format and converted to a JPEG format in order to extract video frames that precisely illustrated the student's activities. Table 2 shows examples of possible acceptable and unacceptable student activities in an online test environment which were simulated in the experiments. It should be noted that, the activities listed below would vary from individual to individual; thus, it is impossible to cover all the possible cases that may occur. However, the list of activities in Table 2 was compiled using excerpts from the informal interviews conducted with students from the School of Electronics and Computer Science at the University of Southampton. The experiments were designed to investigate the effectiveness of a blob-based method in detecting and deducing correctly a student's presence status.

Table 2 *Examples of student activities in a test environment*

Activities	**Activity examples**	**Blob description**	**Relevant statistics**
Possible activities to substitute the original student or provide assistance towards the test	External person behind student	A new blob appears	Area Count (> 1)
	External person beside student	Blob has merged with another blob	Area Count (> 1)
	External person	Old blob	Area

	substitute student	disappears	Major/minor axes
Possible activities to obstruct the presence monitoring process during the test	Hand blocking camera	Blob moving towards camera	Extent Area
	Head blocking camera	Blob moving towards camera	Extent Area
Possible activities that depicts varying body movements	Head/face distant from camera	Blob moving away from camera	Area Major/minor axes Extent
	Head on table	Blob change in form	Area Extent
	Look left/right	Blob change in form and move in different direction	Area Orientation

Table 3 shows the changes in Object's A blob statistics and Figure 6 shows an illustration of the scenarios. From table 3, it is observed that Object A's frontal position elicited from the blob orientation is within the acceptable range and the relevant blob statistics are extracted for the verification process. During the test an external person appears in the background and moves behind Object A. Thus, due to a merge between the two objects, there is an increase in Object A's blob size and a considerable change in the blob shape. The significant increase in size and the change in the objects shape produce a suspicious effect which implies that a dishonest activity. Thus, these changes in size and shape trigger the fuzzy engine and Object A is assigned a high-risk threat class.

At the point where the external person moves close to Object A, the two blobs unmerge and are separated. This is interesting, because Object A reverts to its original blob size and the presence of the external person is undetected. However, at this stage the count statistics detects the second presence in the environment and triggers the fuzzy engine to produce a high-risk threat class. The last frame shows that the external person has eventually substituted the original student; thus, providing a clear impersonation attack. Based on the swap, the change in blob statistics would yield a high-risk threat class from the fuzzy engine. From the experiment above, we have demonstrated the feasibility of verifying presence by spotting the changes in an object's size, shape, position, extent and count statistics values with respect to the objects frontal pose statistics.

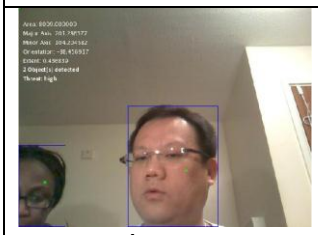
Table 3. *Object A blob statistics*

Activity	Object	Size	Shape	Position	Extent	Count	Fuzzy Result	Threat Class
Frontal pose	A	0.000	0.000	1.500	0.488	1	0.163	Low
External person behind student	A	1.444	0.152	0.119	0.407	1	0.643	High
External	A	0.617	0.315	1.568	0.484	2	0.669	High

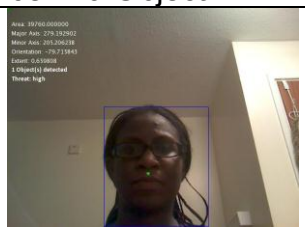
person beside to student								
External person substitute student	A	0.719	0.068	1.391	0.660	1	0.640	High

Frontal pose Object A

External person behind Object A



External person beside Object A



External person substitutes Object A

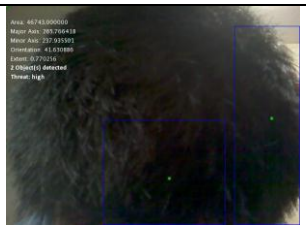
Figure 6. *Object A activity scenarios*

Table 4 shows object B's blob statistics and Figure 7 shows Object B performing activities to occlude the camera lens. A combination of the size, shape, position, extent and count statistics drives the fuzzy class engine to produce a high-risk threat class. A motivation for occluding the camera could be to disrupt the presence verification process or an attempt to engage in cheating habits during the test.

Table 4. *Object B blob statistics*

Activity	Object	Size	Shape	Position	Extent	Count	Fuzzy Result	Threat Class
Frontal pose	B	0.000	0.000	1.387	0.505	1	0.163	Low
Hand Blocking camera	B	0.204	2.723	0.331	0.292	2	0.787	High
Head Blocking camera	B	1.199	0.282	0.727	0.770	2	0.643	High

Hand blocking camera Object B

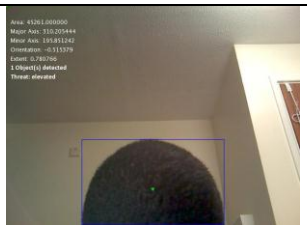


Head blocking camera Object B

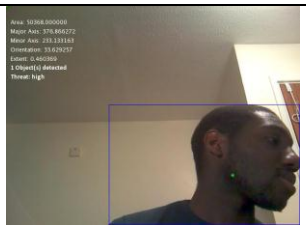
Figure 7. *Object B activity scenarios*

From Figure 8 and Table 5 it is observed that Object C's "head distant from camera" activity produces a high-risk threat class. This is because, there exists a considerable distance between Object C and the camera; thus, the object is no longer in the cameras field of view and no object is detected during the verification process. In a real world environment, the object may have disappeared from the test environment or performing a dishonest activity. The "head on table" activity is affected by an increase in size, change in shape and position. In addition, the "look left/right" activity produces a high-risk threat class due an increase in blob size and a change in shape. In reality, an increase in size for a "look left" activity could suggest the likelihood of suspicious activities in a test environment. However, the threat class assigned to a look left/right activity is determined by the amount of distance between the Object and the camera lens whilst looking left or right.

Head distant from camera Object C



Head on table Object C



Look left/right Object C

Figure 8. *Object C activity scenarios*

Table 5. *Object C blob statistics*

Activity	Object	Size	Shape	Position	Extent	Count	Fuzzy Result	Threat Class
Frontal pose	C	0.000	0.000	1.387	0.505	1	0.163	Low
Head distant from camera	C	0.871	0.054	0.009	0.767	0	0.643	High
Head on table	C	0.629	0.150	0.009	0.781	1	0.450	Elevated
Look left/right	C	0.812	0.174	0.587	0.460	1	0.643	High

Classification Accuracy

Table 6 shows a classification accuracy table obtained from the fuzzy threat class results. In this paper, a classification accuracy table indicates the extent to which the fuzzy engine is able to correctly classify the risk of an activity which reflects an object's presence in the environment. In Table 6, the ARC fuzzy engine has classified correctly 9 activities from the total number of 11 analysed activities; thus, giving a classification accuracy of 82%. The classification accuracy is evaluated by the formula:

$$C_A = \frac{\text{numberof correctlyclassified activities}}{\text{total numberof analysedactivities}} x100$$

Table 6. *Classification accuracy table*

Frame Activity	Object	Expected threat class	ARC Fuzzy threat class
Frontal Pose	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
	C	Low-risk	Low-risk
External person behind Object	A	High-risk	High-risk
External person beside Object	A	High-risk	High-risk
External person substitutes Object	A	High-risk	High-risk
Hand blocking camera	B	High-risk	High-risk
Head distant from camera	C	High-risk	High-risk
Head on table	C	High-risk	Elevated-risk
Look left/right	C	Elevated-risk	High-risk

Benefits of blob-based presence verification system

The benefits of employing the blob-based presence verification system include:

Low processing power

One advantage of employing the blob-based solution for presence verification is its low computational costs during processing. The low processing power is attributed to the connected pixels which are represented in a single dimensional binary image. In e-assessment environments, rendering of test questions with minimum delay is essential. Thus, overloading the processor with high computational tasks, such as continuous authentication as a mechanism for presence verification may be unrealistic. The blob method operates independent of the e-assessment tasks and it is carried out via a presence monitoring software. In addition, blob-based techniques are known to be successful and time efficient, especially in environments with low numbers of moving objects (Zang & Klette, 2003).

Non-interruptive re-authentication requests

Recall that, one of the limitations peculiar to password and biometric solutions is the frequent re-authentication requests which can become interruptive and distracting to a student. However, the novelty of the blob-based verification system lies in the ability of the fuzzy risk class engine to initiate change-driven re-authentication requests; thereby, reducing the amount of requests during a test session. The

flexibility of the system is also reflected within the elevated-risk threat class, such that the verification system offers a 'second chance' to confirm the student's presence without interruption. Hence, a student is interrupted only when a high-risk threat class is assigned. In this paper, the high-risk threat class is assigned when a student's current activity statistics vary significantly with respect to the frontal statistics. Thus, the blob-based technique will only attempt to interrupt a student when a significant change in statistics is observed (and that is a good reason!).

Promotes fair assessment

Fairness is a fundamental principle in the design and administration of assessments. As defined by the Scottish Qualifications Authority, in UK fairness in an assessment refers to the true measurement of the candidate's ability or achievement (SQA, 2007). Thus, an unfair assessment may result in an unfair outcome. An unfair disadvantage may occur when the student's test is interrupted leading to a low performance. Thus, the high-stake nature of summative e-assessments requires total student concentration and minimal external interruption for the duration of the test. Additionally, traditional assessment regulations from higher institutions are typically framed in such a way as to prescribe practices to maintain minimal interruption to the students test, e.g. the invigilators should avoid wearing noisy shoes in the examination room. Thus, it is expected that by adopting information technology (IT) in assessments, the risk of an unfair outcome induced through interruption would be minimised. Hence, section 7 of the Qualifications and Curriculum in UK, emphasises that "the use of technology should not inhibit a candidate's performance" (QCA, 2007). This implies that, for summative e-assessments, it is essential that the technologies employed do not become interruptive or distracting to the students test. As discussed in the paragraph above, the blob-based verification system is designed to interrupt a student's test only when it is considered necessary. Hence, adopting a blob-based presence verification system will promote fair assessments in a test environment.

Non-dependent on human invigilators

In video surveillance environments, Collins *et al,* (2000) asserts that finding extra available human resources to sit and watch the video images may incur a high-cost for organisations. Similarly in summative e-assessments, it is suggested that a higher institution will require extra invigilators to watch the video sequences in order to detect anomalous activities. This is perceived to increase the fees paid for the invigilation. In addition, watching a video for a long period may cause fatigue which may lead to human errors. However, the blob-based presence verification system is dynamic in nature and does not require a human input to infer a student's presence status. Thus, the Fuzzy Logic System (FLS) is used to allow easy representation of human decision-making particularly in a dynamic environment such as the online test environment.

Practical applications of presence verification

There exists a wide range of applications that can benefit from incorporating the presence verification process into their existing Identity-Authentication (I-A) user security model. Thus, verifying the presence of a user beyond the initial authentication procedure would determine the sameness of the user throughout the application session.

In e-assessment applications, one of the challenges is the inability to know who is there taking an online test, 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 examination conditions, a student is expected to be successfully authenticated in order to gain access to the test. However, there is likelihood that the authenticated student may swap his/her place with another person. In some scenarios, the swap may occur between two legitimate students of an institution; however, one of the students may not be authorised to take the particular test. In another example, the user substitution can take place between two authenticated students, physically present in the same room and writing the same exam. In this scenario, the two authenticated students may swap their seats for the purpose of assisting each other during the exam.

To address the issues discussed above, a presence verification process would be utilised to verify the continuous presence of the authenticated student/s taking the exam. The presence verification process is initialised after successful authentication and the first step is to extract the features required to uniquely verify the user's continuous presence throughout the session. It is important that the user is oblivious to the presence verification process; thus, it is expected that the features are extracted and monitored passively. A break in the monitoring process can signify a break in the user's continuous presence. For example, there would be an automatic break in continuous presence when two correctly authenticated students swap their seats. It should be noted that, a measure of strength for the automatic break will be dependent on the mechanism adopted for the presence verification process. For example, we assume the human heartbeat can be employed as a presence verification mechanism. To adopt this mechanism, an analogue sound recorder can be used to establish and monitor a steady continuous signal from the heartbeat. Thus, a break in the electrocardiogram (ECG) signal would mean a significant change is detected from the human being.

Another example is the online educational games applications which provide entertainment and is a contributing factor to the player's skills development. The learning-based games operate a multiplayer environment, where a player encounters other online players or a player can cooperate with other players in order to win a game. In addition, a player is required to choose a name or nickname in order to play a game; whilst other games may require a password to gain access to account information and the player's character. From a user security perspective, the Identity-Authentication model is unable to verify the presence of the players beyond the authentication level, which can lead to an identity misrepresentation challenge.

To explain the identity misrepresentation issue, we assume an online educational games website. The website includes lots of free songs, stories and activities for children between the ages of eight and ten. For security purposes, parents are required to register their personal information and the children can access the games by providing their names or nicknames. A ten-year old school girl logs on to the games website and requests a connection to another online player that is within the acceptable age group (8 -10 year olds). However, unknown to the online games system, a forty-three year old man receives the requests and is connected with the ten-year old school girl. Thus, this presents a challenge where a ten-year old girl is playing a school game with a forty-three year old man, rather than another ten-year old. To address this issue, we propose that a presence verification process can be

used to verify and monitor the presence of the correctly identified players throughout the game session.

Conclusion

In this paper, we have investigated the susceptibility of summative e-assessment environments to impersonation threats. We conclude that, the inability of the test environment to resist impersonation is due to the incompleteness of the Identity-Authentication user security model. Hence, we proposed an extension of the user security model to include the presence verification process. The presence verification process is useful as it ensures that authenticated student starting the e-assessment is the same student throughout the test session. Thus, we have proposed a novel blob analysis solution as a mechanism to achieve presence verification in test environments. In addition, we conducted experiments to investigate the feasibility of blob-based presence verification system to detect, verify and classify the risks observed from the student's presence. From our results, we conclude that the blob-based presence verification system will improve the user security process of summative e-assessments.

References

Aojula, H., J. Barber, R. Cullen., J. Andrews. (2006). 'Computer-based Online Summative Assessment in Pharmacy Teaching' *Pharmacy Education* **6**(4): 229-236.

Apampa, K. M., Wills, G. B. and Argles, D. (2009) *Towards Security Goals in Summative E-Assessment Security*. ICITST-2009*,* London, UK

Blanz, V., Grother, P., Phillips, P.J., Vetter, T. (2005) *Face recognition based on frontal views generated from non-frontal images*, IEEE Conference on Computer Vision and Pattern Recognition.

Collins, R., Lipton, A., Kanade, T. Fujiyoshi, H., Duggins, D., Tsin, Y., Tolliver, D., Enomoto, N., Hasegawa, O., Burt, P., Wixson, L. (2000) *A system for video surveillance and monitoring.* Technical Report CMU-RI-TR-00-12, May 2000, Carnegie Mellon University

Furnell, S., Dowland, P., H. Illingworth, P. Reynolds (2000), 'Authentication and Supervision: A survey of user attitudes' *Computer & Security*, **19**(6): 529-539

Furnell, S., P. Onions, U. Bleimann, M. Knahl, H. Rder, P. Sanders. (1998). 'A security framework for online distance learning and training', *Internet Research* **8**(3): 236-242

Hernandez, J.A., Ortiz, A.O., Andaverde, J., Burlak, G. (2008). *Biometrics in Online Assessments: A Study Case in High School Students*. CONIELECOMP, Puebla

Kerka, S. & Wonacott., M. (2000) *Assessing Learners Online*, Practitioner File. ERIC, ED 448285.

Klosterman A., Ganger, G (2000) *Secure Continuous Biometric- Enhanced Authentication*, Technical Report CMU-CS-00-134, Carnegie Mellon University

Ko, C. C., Cheng, C. D. (2004) 'Secure Internet Examination System Based on Video Monitoring'. *Internet research* **14**(1): pp. 48–61

Levy, Y. & Ramim, M. (2009) Initial Development of a Learners Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)', *Interdisciplinary Journal of E-learning and Learning Objects* (IJELLO).

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

Quality Assurance Agency (2000), 'Section 6: Assessment of Students' in *Code of Practice for Assurance of Academic Quality in Higher Education, 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)

Stallkamp, J., Ekenel, H.K., Stiefelhagen, R (2007) *Video-based Face Recognition on Real-World Data*, ICCV 2007.

Stoner, G. (1996) 'Implementing Learning Technology' *Learning Technology Dissemination Initiative,* Heriot-Watt University, Edinburgh

Yilmaz, A. & Javed, O., Shah, M. (2006), Object Tracking: A Survey. *ACM Computing Surveys*, 38 (4)

Zang., Q. & Klette, R. (2003) *Object Classification and Tracking in Video Surveillance*, Proceedings Computer Analysis of Images and Patterns, LNCS 2756, pp198-205

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