UNIVERSITY OF Southampton

University of Southampton Research Repository
ePrints Soton

Copyright © and Moral Rights for this thesis are retained by the author and/or other copyright owners. A copy can be downloaded for personal non-commercial research or study, without prior permission or charge. This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the copyright holder/s. The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the copyright holders.

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given e.g.

AUTHOR (year of submission) "Full thesis title", University of Southampton, name of the University School or Department, PhD Thesis, pagination

http://eprints.soton.ac.uk

UNIVERSITY OF SOUTHAMPTON

FACULTY OF ENGINEERING, SCIENCE AND MATHEMATICS

School of Electronics and Computer Science

Presence verification for summative e-assessments

by

Kikelomo Maria Apampa

Supervisor: Dr Gary Wills

Co-supervisor: Dr David Argles

Thesis for the degree of Doctor of Philosophy

August 2010

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF ENGINEERING

SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE

Doctor of Philosophy

PRESENCE VERIFICATION FOR SUMMATIVE E-ASSESSMENTS

by Kikelomo Maria Apampa

Influenced by information technology advances, the assessment process has begun to make its way out of the traditional classroom into online environments. The online summative assessment is a high-stake examination which counts towards a final course mark. Thus, as a result of the important consequences of such summative tests, security measures are put in place to ensure that only the 'right' students are assessed. However, the identity-authentication model adopted for user security is susceptible to impersonation challenges.

This thesis introduces the concept of presence verification as an essential extension to the existing identity-authentication user security model. The presence security goal is aimed at ensuring that the correctly authenticated student at the start of a test is the same student throughout the test session. Thus, verifying a student's presence beyond the initial login procedure minimises the impersonation threats. In order, to embrace the gains of ensuring presence during summative e-assessments, a blob-analysis solution which follows an object tracking approach is proposed. The design of the blob-based presence verification (BlobPV) system involves video processing techniques which can be used to detect, verify and classify a student's presence status in the test environment. Thereby, indicating the likelihood of acceptable or unacceptable activities.

Experiments were carried to demonstrate the feasibility of a blob-based presence verification system in summative test environments. Additionally, the BlobPV system was evaluated to determine the accuracy of correctly classifying a student's presence status. For each experiment and evaluation, the methods and results are described. The results clearly state that, such an approach would significantly improve the detection rate of impersonation attempts during online summative assessments.

Contents

List of Figures

List of Tables

Declaration of Authorship

I, Kikelomo Maria Apampa, declare that the thesis entitled "Presence verification for summative e-assessments" and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a research degree at this University;
- where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
- where I have consulted the published work of others, this is always clearly attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
- parts of this work have been published as:

1. Apampa, K. M., Wills, G. B., Argles, D. and Marais, E. (2008) Electronic Integrity Issues in E-Assessment Security. In*: The 8th IEEE International Conference on Advanced Learning (ICALT 2008)*, July 1-5, Santander, Spain.
2. Apampa, K. M., Zhang, T., Wills, G. B. and Argles, D. (2008) Ensuring Privacy of Biometric Factors in Multi-Factor Authentication Systems. In: *International Conference on Security and Cryptography (SECRYPT 2008) part of the International Joint Conference on e-Business and Telecommunications (ICETE08),* July 26-29, Porto, Portugal.
3. Apampa, K. M., Wills, G. B. and Argles, D. (2009) Towards Security Goals in Summative E-Assessment Security. In: *E-learning Security Workshop (ELS-2009) in conjunction with ICITST'09,* November 9-12, London, UK.
4. Apampa, K. M., Wills, G. B. and Argles, D. (2009) Towards Security Requirements in Online Summative Assessments. In: *World Conference on E-*

Learning in Corporate, Government, Healthcare & Higher Education (E-Learn 2009) part of the AACE, October 26-30, Vancouver BC, Canada.

5. Apampa, K. M., Wills, G. B. and Argles, D. (2010) An Approach to Presence Verification in Summative E-Assessment Security. In: *E-learning Security Workshop (ELS-2010) in conjunction with i-Society-2010,* June 28-30, London, UK.
6. Apampa, K. M., Wills, G. B. and Argles, D. (2010) Towards a Blob-based Presence Verification System in Summative E-Assessments. In: *International Computer Assisted Assessment (CAA 2010) Conference Research into E-Assessment,* July 20-21, Southampton, UK.
7. Apampa, K. M., Wills, G. B. and Argles, D. (2010) A Non-Biometric Approach to Presence Monitoring in Summative E-assessments (poster). In: *Grace Hopper Celebration of Women in Computing (GHC 2010)*, September 28 – October 2, 2010, Atlanta, Georgia.
8. Apampa, K. M., Wills, G. B. and Argles, D. (2010) User Security Issues in Summative E-Assessment Security. *(Submitted to the International Journal for Digital Society)*

Signed: Kikelomo Maria Apampa

Date: 25 August 2010

Acknowledgements

My sincere appreciation goes to the Trinity, to whom I owe everything; words are not enough to say thank you, I'm forever grateful.

To my supervisor, Dr Gary Wills, thank you for the unwavering support and positive encouragement throughout my research, especially during difficult times. With his enthusiasm, inspiration, valuable intellectual and spiritual advice, he helped me gain the confidence needed to complete my PhD. To my second supervisor, Dr David Argles, for the constant support, excellent ideas and wonderful supervision, especially his patience in reading and commenting on my thesis as it progressed. To my colleagues and the staff at Learning Societies Lab, thank you for creating a wonderful research atmosphere.

Special thanks to my parents, Prince Bola and Esther Apampa, my siblings and entire family, for their indispensable love, continuous provision, constant support and encouragement throughout my degree. To my best friend Olubunmi Okunwobi, thank you for being there in good and bad times; though the distance, you were always near. To my church family at Living Faith Connections, thank you for your love and prayers.

Finally, completing a PhD is an onerous task, which is rarely carried out without the help of others. Hence, I wish to express my gratitude to all my friends for their priceless moral support throughout my research. And to Dr Frank Ekpenyong, thank you for challenging me in new research directions.

Definitions and Abbreviations

Hash Functions	This is an algorithm that is used to condense an arbitrary length message or text into a fixed length or size.
Digital Signatures	A digital signature is an electronic signature that can be used to identify and authenticate the sender of a message or to verify the documents origin and contents.
Static IP Addresses	A static IP address is a permanent address that can be issued to a computer on the network.
Biometric Templates	These are representations of the raw biometrics (e.g. fingerprints) using series of numbers and letters.
False Positives	This is also known as the False Accept Rate (FAR) or percentage of impostors accepted. This can occur when the biometric measurements from two different individuals are perceived to be from the same individual
False Negatives	This is also known as the False Reject Rate (FRR) or percentage of authorised users rejected. This can when the two biometric measurements from the same individual are thought to be from two different individuals

Chapter 1. Introduction

Assessment is an integral part of the student's learning experience. Influenced by information technology advances, the assessment process has begun to make its way out of the traditional classroom into online environments. The e-assessment process offers enormous opportunities to enhance the student's learning experience such as delivering on-demand tests, providing electronic marking and immediate feedback on tests. In higher education, e-assessment is typically employed to deliver formative and summative tests to the students. The online formative assessments are low-stake examinations designed to improve the student's learning; whilst the online summative assessment is categorised as a high-stake examination which takes place at the end of a course and counts towards the final course mark. However, due to the high-stakes nature of the summative tests, the summative e-assessment process remains a target for user security challenges.

Thus, it is the responsibility of the e-assessment user security model to ensure that only the correct students take a summative test. To accomplish this task, user authentication methods such as passwords, smartcards and biometric technologies are employed. However, the identity-authentication user security model remains fallible to impersonation threats; threatening the reliability and validity of the e-assessment process. According to Kerka & Wonacott (2000), impersonation threats are a major concern and it poses a greater risk to the academic community. Interestingly the impact of an impersonation threat on a user security model is varied based on the strength or weakness of the authentication method adopted. Thus, the shareable attributes of a password would make impersonation more appealing whilst the uniqueness of biometric traits would deter potential impersonators. Biometrics technology is regarded as an ultimate solution for user security issues in e-assessments (Marais *et al,* 2006); however, adopting biometric solutions in test environments is plagued with cost, privacy and acceptance issues. Thus, from the above discussions it is concluded that the existing user security model is susceptible to impersonation challenges and the existing user authentication methods are incapable of solving the problem. Hence, there exists a gap in

the user security process of summative e-assessments and it is a research area seeking solutions.

1.1 Research Objectives

The objectives of this research are to:

1. Investigate why summative e-assessments are susceptible to security challenges.
2. Investigate a robust solution for monitoring continuous presence in a supervised summative e-assessment environment.
3. Evaluate (a design of the solution to show) the feasibility and stability of the BlobPV system.

1.2 Thesis Structure

The remainder of this thesis is divided into nine chapters.

Chapter 2: ***Learning***

This chapter presents a background review of learning and the foundational learning theories which can influence an assessment process. The concept of e-learning and the role of existing learning theories in e-learning are discussed.

Chapter 3: ***Assessment***

This chapter presents a detailed overview of assessment and its related components such as, principles of assessment, purposes of assessment, grading schemes, methods for the delivery of assessment and feedback in assessment.

Chapter 4: ***Electronic Assessment Security***

In this chapter, the purpose and benefits of electronic assessment as an alternative assessment delivery method is discussed. This chapter also introduces the core of this thesis which is the user security of summative e-assessments. This is followed by an in-depth discussion of user authentication methods and their uses in summative e-assessments.

Chapter 5: ***Identity-Authentication (I-A) User Security Model***

In this chapter, the existing user security model adopted in summative e-assessments is introduced and the limitations of the model are highlighted. The chapter ends with a brief review of impersonation challenges in online assessments.

Chapter 6: ***Presence-Identity-Authentication (P-I-A) User Security Model***

This chapter explains in-depth the fallibility of the I-A user security model to three types of impersonation threats. Thus, by using a goal-oriented approach the concept of presence and its benefits is introduced. Furthermore, potential approaches to achieving presence verification are evaluated and a novel blob analysis solution is proposed.

Chapter 7: ***Blob-based Presence Verification (BlobPV) System***

This chapter presents the blob statistics operation and the system design of the proposed blob-based presence verification system. This chapter also describes the video processing techniques and the fuzzy logic implementation for the BlobPV system. Finally, a justification for adopting a blob-based solution in online summative test environments is discussed

Chapter 8: ***BlobPV System Experiments and Results***

This chapter reports the experiments carried out to demonstrate the feasibility of blob analysis to achieve presence verification in test environments. An evaluation of the activity risk classification approach which is adopted for the BlobPV system is also reported. Results from the experiments and the evaluation process are also presented.

Chapter 9: ***Conclusions and Future work***

This chapter concludes the thesis with a summary of its contributions and directions for future work.

Chapter 2. Learning

Learning is not confined to the boundaries of a formal education system. Learning can occur throughout an individual's life time; presented in varying ways and settings. This chapter presents a background of existing learning theories based on the behaviourist, cognitive and constructivist schools of thought. In addition some underlying principles of learning which is influenced by the type of learning theory adopted are discussed. Electronic learning may be the learning future which has been long awaited; thus, this learning approach is gradually being employed in generic learning environments. In this chapter, the influences of electronic learning on existing learning environments will be presented. Finally, the role of learning theories in e-learning is described, providing insights on learning theoretical ideas in modern learning.

2.1 Paradigms of learning

The approach to teaching a subject and the manner in which a student learns the content is affected by the existing learning theories. In this section, the attributes of each theory will be discussed with emphasis on how assessment is being administered to students.

2.1.1 Behaviourism

Behaviourism presents a traditional classroom setting where the lecturer dominates the learning environment and the student takes the passive role. Students are subjected to the specific course content delivered by the lecturer, where the aims and objectives of the course are expected to yield a known outcome. Theories such as the law of effect (Thorndike, 1911) and operant conditioning (Skinner, 1957) give an insight of what is expected in the learning environment. Based on prior work of Thorndike, Skinner explains that changes to human behaviour are instigated by positive or negative responses that occur in the environment. His model is based on the premise that, when a particular Stimulus-Response (S-R) pattern is reinforced (rewarded), the individual is conditioned to respond (Skinner, 1983).

In the context of assessment, students must be assessed at the end of a learning event to determine if the objectives of the course were fulfilled. In addition, the behaviourists emphasise the frequent use of rewards/reinforcements during the learning process. Examples of incentives include practice questions and student feedback. Providing students' with incentives during the course does not automatically mean success during assessment. There are possibilities for the students to achieve top grades during assessment; however this is not entirely attributed to the reinforcements received. For example, a student receives learning incentives (e.g. extra personal classes) during a mathematics course; however, if the student is less interested in mathematics failure may be inevitable. In the behaviourists' school of thought, failure means a constant repetition of the learning content until mastery is achieved. A fundamental principle of behaviourism proposes that a new behavioural pattern should be repeated until it becomes automatic (Mergel, 1998). However, repetition does not imply automatic assimilation; rather a habit may be formed from constant repetition (e.g. going on a diet). Thus, if a habit is not enjoyed it may become obligatory and the intended purpose defeated. In assessment, re-sitting a test may not imply thorough understanding of the course content and failure may still be inevitable.

2.1.2 Cognitivism

The behaviourists' approach to learning was widely accepted and influential, but gradually it became increasingly obvious that there were some anomalies in the theory. Tolman (1932) a non-reinforcement behaviourist, proposed a theory that had a cognitive flair and the rivalry between the "S-S" (stimulus-stimulus) and the "S-R" (stimulus-response) learning theories was consummated. Cognitive psychologists believe that individuals have the ability to process information in their brain, to socially interact with their environment and to identify a link between present observations and past experiences. They argue that learning occurs as a change in the mental state of a student rather than a change in the students' behaviour. Organised information and knowledge is a key principle in Cognitivism; therefore, there must be a knowledge structure formed in the students' memory.

Content delivered by lecturers should encourage links to existing knowledge. Thus, when information is well organised it is easier to learn and remember (Hartley, 1998). If content is delivered in a way that will aid easy retrieval, then during assessment

students can organise and relate the assessment questions to existing knowledge in memory. Thus, the assessment questions are scanned against the students' memory to determine an appropriate action. During assessment the student is thus expected to produce a high degree of mental alertness.

Cognitivism theory also believes in reinforcement but from a different perspective. They argue that students are reinforced through the presentation of new information such as receiving feedback about their success or failure in an assessment. This is when students receive their results; there are feelings of joy for students that have passed (reward) and sadness for those that have failed (punishment).

2.1.3 Constructivism

Constructivism is based on the premise that humans construct their own perspective of the world, through individual experiences and schema. Therefore, it suggests that learning is active and students can understand only what they have constructed based on personal experiences and their environment. The works of Piaget (1955), Bruner (1966), and Vygotsky (1986) among others also provide historical precedents for constructivist learning theory. In the constructivists' theory, motivation is the key to the students' success (Von Glasersfeld, 1989). The lecturer is active but plays the role of a facilitator (Bauersfeld, 1995); thus the student controls and manipulates the things they learn and sets their pace for learning. Learning to the constructivists is about creating meaning, constructing personal conceptualisations and finding solutions to their own problems. Content is not specified beforehand; thus it is constructed by the students own knowledge to fit the situation. Students have the ability to master autonomy and to solve problems that allow them to go beyond the information provided.

Assessment in constructivists approach forms an integral part of the learning process (Holt and Willard-Holt 2000). The assessment process is viewed as a two-way process which involves interaction between the lecturer and the student. In this view, the student plays a larger role in judging their own progress. Failure means the student needs help and the lecturer needs to find out what level of their performance needs to be improved. Communication between students is encouraged, because each student has a unique way of solving problems.

2.2 Principles of Learning

Learning can have different definitions based on the different school of thoughts employed. Ertmer and Newby (1993), asserts that the behaviourists believe learning is a change in the form or frequency of observable behaviour, the cognitivists define learning as changes between states of knowledge rather than probability of response and the constructivists proposes that learning is creating meaning from experience. Based on the above definitions, it is sufficient to conclude that learning occurs in various patterns. Learning can be described as the ability to give students an opportunity to gain a skill based on their past and present information; and also using the skill to expand their knowledge. Due to the diversity in learning patterns, a balance should be created between the intended learning outcomes and assessment. For example, a trainee caterer learns to how cut tomatoes in cubes. During assessment, the student will dice the tomatoes in cubes and not in circles; this is the method learnt to cut the tomatoes

2.2.1 Scaffolding

The initial representation of scaffolding can be portrayed in situations where parents train their children, supporting them till they are old enough to attain independence (Sharma *et al,* 2007).The constructivist school of thought have embraced 'scaffolding' and this idea is attributed to Vygotsky's (1978) Zone of Proximal Development (ZPD). The ZPD is a point when a student needs the support of lecturers and peers to achieve a learning activity. Scaffolding can include working in groups, performing role-plays, access to useful learning resources, learning support helpful lecturer comments, self-assessment and quizzes (Oliver & Herrington, 2003). All of these methods form the structures on which students learning can be built on. The experiences and knowledge provided to the students during the 'scaffold' aid the students during assessments. The scaffolds provided by the lecturer are retained as long as learning is still fragile (Taber, 2003). However, the assistance and help is gradually reduced as the learning progresses to the point where the student is finally able to act independently (Oliver & Herrington, 2003).

Fading is an important concept in scaffolding which leads to independence and finally expertise. Scaffolding is intended to be temporary and there is a need to fade support as students gain experience and skills (Dodge, 2001). Fading breeds assessment. When a student shows competency in a particular subject, it is important to assess

knowledge so that progress can be documented, feedback given and where possible the process of scaffold re-started.

2.2.2 Situated Learning

Situated learning is a general theory of knowledge acquisition and it is usually unintentional rather than deliberate. In the model, learning occurs as a result of an everyday situation (situated), therefore learning is done 'just in time', purposeful and controlled. A student's environment involves collaborating with people, creating names for objects and interpreting statements. Situated learning offers knowledge presented in authentic contexts, where the situations support social interaction and collaborative construction of knowledge. In this model assessment may take place alongside learning, without being a separate activity. Mueller (2005) asserts that in authentic assessment, students are asked to perform real-world tasks that demonstrate meaningful application of knowledge and skills.

In exam conditions, authentic assessments allow students to display a blend of originality and novelty. Thus, their critical thinking, cognitive and reasoning skills are being assessed. For example, if a group of students were taken on a trip to view a site (real-world problem), and upon return they are assessed given a similar scenario. The students will be expected to demonstrate proficiency as to what they have learnt personally, making decisions on relevance and appropriateness of the test scenario. In this example the act of plagiarism is defeated, because there would not be just one correct answer to the scenario, but the ability of a student to analyse and create new meaning to the question will be rewarded.

2.2.3 Blended Learning

In blended learning, various classroom activities are combined to enhance learning. Masie (2003) asserts that, *"people are not single-method students! We are, as a species, blended students"*. In this learning approach, two or more methods of learning are blended (mixed) together to produce a well balanced and effective combination. Driscoll (2002) defines blended learning as a combination or mixing of four different methodologies:

- To combine or mix models of web-based technology (e.g., live virtual classroom, self- paced instruction, collaborative learning, streaming video, audio and text) to accomplish an educational goal.
- To combine various pedagogical approaches (e.g., constructive, behavioural, cognitive) to produce an optimal learning outcome with or without instructional technology.
- To combine any form of instructional technology (e.g., videotape, CD-ROM, web-based training, film) with face-to-face lecturer-led training.
- To mix or combine instructional technology with actual job tasks in order to create a harmonious effect of learning and working.

The most common type of blend is a two-component blend, which is made up of the face-to-face classroom learning and e-learning (using technology in learning). In addition, the institutional culture may also determine the type of components that will be blended into the learning framework. For example blended learning could include a combination of lectures, seminars, workshops and laboratory work. Assessment in blended learning will need to draw directly from the methods or components used in the combination. A student should be assessed in the similar manner which a course was delivered.

2.2.4 Problem-based Learning

In Problem Based Learning (PBL) a problem is presented and the students' are expected to construct a deep understanding of the problem. Thus, new knowledge is created which aids in problem solving. Problem-based learning embraces the social collaborative attribute of constructivism; where an emphasis is laid on the importance of working in small groups. By applying this strategy, students can interact, communicate and work cooperatively to solve a problem. This may also fuel their enthusiasm, such that they go beyond their textbooks to pursue knowledge from other sources (Kaminskienė *et al,* 2006). In the PBL model, the lecturers act as the facilitators during group meetings, rather than provide easy answers to learning groups. This may also keep a constant flow between the lecturer and the student (Rhem, 1998). This presents a different approach from the conventional didactic approach, where the lecturers impart knowledge and the students take assessments tasks which are completed individually.

In PBL, assessment of students' progress is often a major weakness and sometimes it is non-existent. Nowak & Plucker (1999) explain that assessment in PBL does not often align well with the objectives of the problem-based learning that preceded it. They argue that the use of PBL is defeated, if students' are taught using real-life authentic situations and then assessed via traditional multiple choice questions. This may result in students' performing poorly, since they are un-prepared for assessment delivered in the format different from their learning pattern. One approach suggested to maximising the potentials of PBL is that, if the instruction/learning is problem-based, then, the assessment should be similarly structured.

2.2.5 Ubiquitous Learning

In ubiquitous learning environments there are no constraints to what may be learnt, where it may be learnt and how it could be learnt. The ubiquitous learning environment provides an interoperable, pervasive, and seamless learning architecture (Yang, 2006). In today's literature, ubiquitous computing foresees a pervasive environment where tiny processors and sensors will be integrated into everyday objects (Mattern, 2004). These can be achieved, because all the devices will be interwoven and connected together by wireless networks which will be in the form of Bluetooth or Wifi (IEEE 802.11). Ubiquitous learning lends itself to the school of constructivism where learning is not controlled by physical space or schedules (Laurossi, 2004). This learning environment is persistent; allowing students to access education flexibly, calmly and seamlessly (Jones & Jo, 2004). The use of handheld computers can also empower students to take responsibility for their own learning.

Introducing ubiquitous handheld devices can enhance learning and teaching, but it can also encourage cheating during summative assessments. Bluetooth or wireless technology may cause a breach of security in summative assessment if not properly curtailed. For example, students with Bluetooth enabled laptops or mobile phones can exchange answers via the Bluetooth technology.

2.3 E-Learning

Electronic learning (E-learning), computer based training (CBT), web-based learning (WBT), Internet-based training (IBT), and a host of other names may be the learning future which has been long awaited. The Joint Information Systems Committee

in the UK defines e-learning as the "*the process of learning which is supported by the use of ICT"* (JISC 2006). The use of information and communication technology for learning includes the Internet, local network, standalone computer, interactive whiteboard or portable device. In this thesis, e-learning is described as the acquisition of information and knowledge via any form of electronic media for the purpose of expanding prior knowledge of the student. Electronic learning delivered through asynchronous training offers a self-paced learning via electronic media (Internet, intranets, extranets, satellite broadcast, tape, interactive TV and CD-ROM). This method makes learning more flexible; however, it may or may not include access to lecturers. The most advanced form of e-learning lends itself to synchronous training. In this method students' from diverse geographical locations can communicate with their lecturer and peers. Electronic media employed includes the Internet websites and audio/video conferencing.

The process of electronic learning promises a wide range of benefits such as the access of learning content and on-demand delivery, life-long learning, social and intellectual collaboration. According to Coomey & Stephenson (2001) four features of good e-learning practice include dialogue, involvement, support and control. Thus, during the dialogue process the lecturer can build virtual structures for interaction using e-mail, bulletin boards, chat rooms, group discussions and wikis. All these activities embedded into the course content may make learning more robust and interesting. The use of varying types of course content (graphics, animations, sounds and texts) may also reduce boredom whilst learning and improve retention during assessment.

2.4 E-Learning Environments

Since the advent of the Internet, learning has begun to make its way out of the traditional classroom into online environments. Thus, electronic learning can be conducted anywhere, anytime and learning content delivered through various activities (Mason, 2002). This section describes examples of electronic learning activities employed in generic learning environments. Generic learning environments in the UK, context may include (but are not limited to), further education, higher education and vocational training.

Further Education

Further Education is provided at a higher level than the secondary school. One of the popular uses of electronic learning in further education is as a presentation tool; particularly the use of the interactive whiteboard (iWB). Finlayson *et al,* (2006) asserts that using the interactive whiteboard may have an impact on a student's receptiveness to learning and cognition. Electronic learning in further education may be used to provide online practice resources, online assessment of key skills and online space for e-portfolio development.

Higher Education

The higher education level is usually referred to education taken at the universities. This consists of undergraduate degree, postgraduate degrees (Taught Masters or Masters by research) PhD degree and the HND/HNCs. Based on the positive influence that e-learning has on higher education Garrison & Anderson (2003) asserts that, combining information technology with effective pedagogy and reflective teaching, will transform higher education. Thus, electronic learning may be used as a medium and it is integrated into virtual learning environments (VLE). Additionally, electronic learning in higher education may be used to provide online peer and tutor support, online practice test resources and online assessment of basic and key skills.

Vocational Education and Training

Vocational education and training are traditionally non-academic and includes commercial, technical, professional development as well as transferable personal skills. This environment is flexible, responsive and relevant to the needs of industry as well as individuals. The training acquired are designed to give students' the skills and knowledge to do a particular job, work in a particular industry or acquire more general skills to do a variety of jobs. In this environment, e-learning may be used as a presentation tool where the online platform interacts with the students in a personalised manner. Mikalsen *et al,* (2008) describes the experience and implementation of electronic learning employed in a vocational training environment. Their work presents an integrated multimedia e-learning model which is formed by textual and multimedia resources (e.g. videos) to enhance the learning experience.

2.5 Learning Theories in E-Learning

In this section, the existing learning theories (see section 2.1) are described with respect to their roles in electronic learning.

2.5.1 Behaviourism

Behaviourism has found a place in E-learning, but there are some constraints in exhibiting its full potentials. The behaviourist school of thought presents a lecturer-centred scenario, where students are subjected to the specific course content delivered by the lecturer. Mason (2002) argues that, lecturers who emphasise the content delivery side of e-learning very often have a behaviourist or cognitive conception of learning (either consciously or not). Lecturers in the behaviourist school tend to choose and offer learning materials to students; however, the learning resources are tailored to produce an expected learning outcome. Thus, student efforts to organise learning activities for themselves play little role. Behaviourists embrace the idea of e-learning because it can deliver the same experience and content to large numbers of students. However, this approach tends to turn students away from e-learning and become a barrier rather than an enabler of learning (Wild, 2007). Overall, behaviourists recommend a structured, didactic approach in designing an online course (Mödritscher, 2006).

2.5.2 Cognitivism

The cognitivist, like the behaviourists, remain focused on content delivery and intend to deliver the same learning experience to a large number of users but with a varying experience (Wild, 2007). This approach breaks learning content into smaller parts, where each chunk can be re-structured in different ways. In dividing the tasks and creating groups, some form of interaction between the students can occur. This may provide better understanding of the course content. The cognitive approach relies on the course designer charting the learning pathway which would conform to the specific course objectives.

2.5.3 Constructivism

There is a wider acceptance of the constructivists learning approach in electronic learning. Mason (1998) explains that the students' constructivist thoughts could be encouraged through active participation in online discussions, collaborative online activities and online assessment. Laurillard's (1995) conversational framework proposes

four teaching media divisions; this consists of discussion, interaction, adaptation and reflection. Thus, the student and lecturer can discuss and share their views on the course content. During the interaction process, the student can also receive meaningful feedback.

Laurillard's and Mason's view on constructivism in e-learning acknowledges the need for a rethink; such that universities should permit open, critical and discursive learning (Gulati 2004). Taking a closer look at the universities, the reverse is seemingly the case where an objectivist model is assumed (Hanley 1994). In e-learning, the constructivists do not focus wholly on course content but rather on the student (Wild, 2007). Thus, e-learning empowers the individual student so that the lecturer is no longer the gatekeeper of knowledge (Mason, 2002). In view of this, active participation in online discussion may be a positive influence for some students while some may choose not to be involved (Williams, 2002: 267). To accommodate the constructivist's view of a student-centred approach, lecturers need to be aware of some students who prefer learning informally and silently (Gulati, 2004).

2.6 Summary

The approach to teaching, learning and assessing may be largely affected by underlying learning theories. Thus, the existing learning theories include behaviourist, cognitive and constructivists' schools of thought. In a behaviourist classroom, the lecturer dominates the learning environment while the students take a passive role. In this school of thought, students' are frequently assessed to determine if the learning objectives were met. However, failure means a constant repetition of the course content until mastery is achieved. In cognitivism, it is assumed that new information is linked to prior knowledge; thus, students' can interact with information, interpret it and create a mental construct of the information. In a cognitive classroom, course content is delivered in an easy way to aid retrieval. Therefore, during assessment students' can retrieve information from memory and apply it to the context of the test. Constructivists view knowledge as a skill that grows from the inside realm unto the outer realm. To the constructivist, the assessment process is viewed as a two-way process which involves interaction between the lecturer and the student. Failure means the student needs help and the lecturer needs to find out what areas need improvement.

Scaffolding, blended, situated, problem-based and ubiquitous learning are existing learning patterns which are implemented for pedagogy. These principles may have an influence on student learning and assessment. For example, in the situated approach, learning occurs unintentionally rather than deliberately; this in turn may breed authentic assessments. Electronic learning sets the stage for the gradual replacement of the traditional paper-based learning methods. The advantages of e-learning include, on-demand course content, lifelong learning, social and intellectual collaboration between students'. Finally, the behaviourist, cognitive and constructivist schools of thought are integrated into the modern world of electronic learning. This depicts the roles of the underlying learning theories in an electronic learning environment.

Chapter 3. Assessment

To most people assessment means sitting in a room or hall and answering a printed question paper. Assessment does not generally mean testing a students' competence in a subject; however, the use of examination, oral test, essays, quiz and projects are methods of assessing competencies (Knight, 2001). More importantly than testing for competency, an assessment should reflect learning objectives and course content (Prior & Lister, 2004). A key component that can positively or adversely influence an assessment is the application of learning theories. Thus, the existing learning theories may determine a lecturer's style of teaching and assessing (Kelly & Melograno 2004).

Recall, in the preceding chapter, assessment in a behaviourist class implies frequent student assessment until course objectives are met. Additionally, students may retake tests regularly until the course content is mastered. Assessment in a cognitive classroom takes advantage of a student's prior knowledge on a course. Prior knowledge is enhanced using graphics, visuals and key points to aid retention during assessment. A constructivist perceives assessment as a social collaboration of events amongst students. Thus, students work in small groups to construct their own meaning of a task and then present their findings to the lecturer. Assessment is an integral aspect of the learning cycle and it is crucial that the process is aligned with the intended course objectives (Beard, 1970). A simple formula to depict the connection between an assessment and the intended learning outcomes is presented: *"aims and objectives → content → teaching and learning activities → assessment" (*Morgan & O'reilly 1999: 47). Hence, this chapter describes the concepts of assessment, purposes of assessment, delivery of assessment and the general grading schemes employed in assessments.

3.1 Assessment vs. Evaluation

The process of assessment is frequently confused with the process of evaluation. These two concepts are expressed and defined differently in American and European countries. In the statements endorsed by the American Education Research Association (AERA); assessment improves student learning for future performances while evaluation

judges the worth of a performance against pre-defined standards (Parker *et al,* 2001). In this respect, assessment is a continuous process and it provides information for improving learning and teaching. This information is anonymous and not graded. Evaluation is the judgement of a student's performance and it focuses on grades. Table 3-1 summarises key differences between assessment and evaluation.

As stated in Brown *et al,* (1996), the Joint Information Systems Committee (JISC) and the Scottish Qualifications Authority (SQA) in the UK; define assessment as "*the process of collecting and interpreting evidence of a student's performance while the process of evaluation is often conducted to check out teaching"*. Irrespective of varying definitions; in a wider sense assessment and evaluation should be viewed as a feedback on performance in learning and teaching (Beard (1970). However, in the context of this research the assessment process will be expressed as providing improvement and judgment on student learning.

Dimension of difference	**Assessment**	**Evaluation**
Content: timing, purpose	*Formative*: ongoing, to improve learning	*Summative*: final, to gauge quality
Orientation: focus of measurement	*Process-oriented*: how learning is going	*Product-oriented*: what has been learned
Findings: uses thereof	*Diagnostic*: identify areas for improvement	*Judgemental*: arrive at an overall grade/score

Table 3-1 Key differences in assessment and evaluation (Angelo & Cross, 1993)

3.2 Assessment Concepts

There are several key concepts which need to be considered when designing or administering an assessment. Examples of these assessment characteristics include reliability, validity, usability, timeliness, fairness, and security. However, in this chapter the reliability and validity of assessments will be considered. These two concepts are intertwined in their description, but more importantly they will inform the concept of fairness discussed in chapter 7.7. In essence, the reliability and validity of an assessment is compromised when there is a breach in security.

3.2.1 Reliability

Reliability in assessment is defined as the extent to which assessment results represents an accurate measurement of the candidate's demonstration of the abilities specified by the assessment criteria (QCA, 2007). Reliability should prove consistency in its criteria for assessment and repeatability when presented with the same assessing factors (Knight, 2001). Hence, an assessment is deemed reliable when a student's score or grade does not vary, regardless of when the assessment occurred or who did the scoring. According to Brown *et al*, (1996), there should be a compelling evidence to show that results are consistent across examiners. For example, given a reliable test, a first examiner assigns a score to a student; thus, a second examiner should arrive at the same approximate score applying the same criteria. This is called the inter-tutor reliability (Race, 2001). Hence, marking student tests on the same standard will foster reliability in assessments.

3.2.2 Validity

The term validity refers to a degree of accuracy of an object. An assessment is considered valid when it is fit for the purpose required or when it measures what it is planned to measure (QCA, 2007). Validity in assessment reflects the degree to which the programme specification and course learning outcomes are assessed (Baird, 1997). Thus, a valid assessment would require that the students complete a task or action that should reflect knowledge of the learning process. An assessment may become invalid when factors that are irrelevant to the learning outcomes are accommodated. An extraneous factor could occur when a student is graded on the quality of their writing; however, the writing skills may not be pertinent to the assessment (Atherton, 2005). Additionally, an assessment could have low validity, such that a topic taught at a certain level, would require performance of a higher order during the assessment. This is the problem of content validity. Thus it is required that the course content of an assessment should closely match the content of the specification it is designed to assess (CIEA, 2007).

3.3 Grading Schemes

Grading can be described as 'assigning a level' or 'rating'. Grading is an important phase of the assessment process, which may assist the lecturers in monitoring

the student's progress. Two main grading approaches employed in the educational system are the norm-referenced and criterion-referenced grading schemes.

3.3.1 Norm Referenced Grades

In a norm referenced scheme, the students' performances are compared against each other and grades are assigned according to a student's relative standing with other students on the same test. In this approach, students' are placed into arbitrary boundaries of achievements; hence, they compete for limited numbers of grades within these bands (Dunn *et al,* 2002). Thus, regardless of the actual exam score attained, the students' scores are dispersed along a "grading curve" where the range is between a pass and fail (Aviles, 2001). However, Lister & Leany, (2003) warned that the danger of employing a norm referenced system is that one is likely to produce average students who lack academic substance. In addition, employing a norm referenced grading in assessments may be an unhealthy approach due to its emphasis on class rank between high and low scorers. This method does not provide information about individual student performances; rather it requires students compete with each other for grades. Lastly, competing for grades may have many unfortunate consequences for a student's academic life. For example, a student may cheat to achieve top grades in an assessment.

3.3.2 Criterion Referenced Grades

The criterion-referenced grading scheme measures students' performances against a set of criteria (e.g. score 85-100 = A, score 69-84 = B); rather than on achievement of other students. In this approach, students are taught and assessed in alignment to the intended learning outcomes (Wu & Kuo *et al*, 2006). Thus, a grade is assigned based on how well a student has learnt the course objectives. The benefit of criterion referencing is evident when the precise goals of the course and clear criteria for each grade are provided to the students. This approach is perceived to have a positive impact on the student's performance during assessment. In criterion referencing, grades are a measure of absolute levels of performance; thus, it is possible for all students to earn a passing score if the course material is well-understood. This implies that, for a given assessment all the students could attain the grade A or all students could get the D grade. Thus, in the defining the quality and validity of the standards required for an assessment, the criterion reference scheme may breed disagreement amongst educators (Speck, 2002). According to Knight (2001), criterion referencing is inherently complex

as it is harder to conceptualise learning goals and to capture them in useful criteria statements. Finally, the criterion referencing scheme may yield a fair assessment; therefore it is gradually replacing the norm referencing as the preferred grading choice in many universities (Dunn *et al*, 2002).

3.4 Purposes of Assessment

In higher education, there exist several approaches which are used to assess learning. The aim in choosing an assessment method is to choose the method which most effectively asses the purposes and learning objectives of the course (Elton, 2002). A non-comprehensive list of assessment methods include multiple choice questions, unseen examination, portfolios, oral examination, coursework, group assessment and peer assessment (Nightingale, 1996). In practice, there are several reasons for designing an assessment and these reasons may occur simultaneously. Rowntree (1990) identifies two major purposes of assessing students:

1. To provide support and feedback to students and to improve their ongoing learning
2. To report on what they have already achieved (a grade or a written assessment).

Thus, the purpose of assessment can be categorised into assessment for learning and assessment for decision making (Elton, 2002)

3.4.1 Formative Assessment

Early work in formative assessment is attributed to leading theorists in education (Black & Wiliam, 1998). Formative implies a process or product which is capable of developing or shaping. Formative assessment is influenced by the need to provide information to students, in a manner that will contribute to the use of their acquired skills. Thus, the aim of formative assessment is to help students' learn something (Rosbottom, 1997). As described in Morgan & O'reilly (1999: 15) traditional formative assessment has commonly taken the form of:

- Non-assessable activities and feedback in study materials
- Self-assessment quizzes and tests that help students monitor their own progress
- Feedback from assignments, or from peers, colleagues or mentors
- Dialogue with teachers, tutors and other students
- Non-assessable tests that prepare students for formal examinations

Formative assessment takes place while a class is ongoing and it continuously monitors student progress rather than at the endpoint. This type of assessment provides a short term feedback loop which offers insight into the student's strengths and their conceptual errors (Earl, 2003). Thus, the students are presented with opportunities to improve. In another view, Sadler (1989) describes formative assessment as the means to identify the "gap" between a student's current understanding and the desired goal. Hattie & Timperley, (2007), suggests that different students will have different "gaps" and the lecturers should design strategies to identify and close these gaps.

3.4.2 Summative Assessment

Summative assessments are administered to record or report an estimate of the students' achievements (Morgan & O'reilly, 1999: 15). Summative assessments are also called high-stakes assessments when used for promotion, placement, certification, and accountability (Rovai, 2000). Thus, reliability is central to summative assessments; since the results may have an enormous impact on students' academic future. For summative purposes, achievement is generally summarised in terms of grades, which aids in the comparison and classification between students. However, summative assessment should be viewed in terms of accountability rather than as a means of classifying students. Therefore, when summative assessments are focused on grading or classification, students are likely to do their best to obtain good marks and look competent in comparison with their peers (Cowie, 2005). In conclusion, the goal of a summative assessment is to provide overall information on the amount and quality of the student learning.

3.5 Delivery of Assessment

The methods of presenting formative and summative assessments are integral to the assessment process. These approaches are described below.

3.5.1 On-paper/Traditional Approach

Traditional assessments are popular in the educational system and this mode of assessment readily comes into mind when using the term test or exam. As defined by JISC (2006), an on-paper test is "*an assessment delivered to the candidate on paper and where the candidate responds on paper".* Thus, in the traditional approach, the test is presented on a paper and usually accompanied with time constraints i.e. the exams are

done within a limited period of time. Traditional tests are often reliable as students are tested through the same standardised procedure and at the same controlled location; hence, measurements are generally consistent with each other (Rovai, 2000). However, the disadvantages of traditional tests are evident in the inability to cater for distance students. This implies that students who reside in remote places need to be physically present at the assessment site. Additionally, lecturers are burdened with the administrative task of marking scripts which may lead to fatigue (Brown *et al*, 1996: 72).

3.5.2 On-screen Approach

The on-screen approach provides an alternative to the traditional on-paper approach and offer benefits such as instant results, interactive on-screen questions and greater accessibility. On-screen testing simply refers to as "*an assessment delivered to the candidate on a computer screen"* (JISC, 2006). On-screen assessment is widely used in academic and non-academic environments. For example, the Driving Standards Agency (DSA) in the UK, offers on-screen tests for student car drivers and motorcyclists; whilst, the Home office UK Border Agency offers the 'Life in the UK tests' on-screen to applicants for British citizenship. In an educational setting, the on-screen test involves installing the assessment software and running the test on the computers. To conduct the on-screen assessment, the test is downloaded to a Server (central) computer through a secure internet connection. Thereafter, the test can be distributed to other computer which is then accessed securely. However, the test is not run online, i.e. there is no live internet connection whilst conducting an on-screen test. Thus, the test is accessed on each individual client computer from the server via the institution's network.

3.5.3 On-demand Approach

The on-demand approach will provide the platform for assessment 'anywhere'. According to JISC (2006), the on-demand testing produces *"a high degree of flexibility in the date and time that tests can be offered to suit the student or learning programme"*. In traditional tests, students are subjected to writing examinations in the same controlled location (e.g. examination hall) and within a specific time. Early advocates of on-demand assessment suggest that, a student may do well, (or badly) if assessed on a different day, or in a different place (Miller & Parlett, 1973). On-demand assessment embraces the idea that each student is unique and their capacity to assimilate and retain learning content

vary between the individuals. Thus, one of its profound benefits is that, candidates' can be assessed at their own intellectual and psychological convenience i.e. when learning content is completely comprehended.

3.5.4 Online Approach

The term online describes the state of 'being connected' via the internet. Several transactions which can be conducted via the internet include, online banking, online shopping, online gaming and online dating. Online assessment refers to an entirely automated process which relies on the delivery of tests and uploading candidate responses on an internet connection (JISC 2006). One of the key benefits of online assessment is the ability to bridge the gap between distance students and the higher institutions. This collaboration enhances the learning experience and provides the student with a sense of involvement that is almost comparable with on-campus students. In a typical online assessment setting, tests can be offered at different locations or different times and the test items can be randomised to provide a different paper (Harvey & Mogey, 1999). Thus, after a test is completed, the test responses are uploaded for automatic marking. In addition, the immediate collation of results and personalised feedback relevant to the test performance is provided. As suggested in Johnson & Green (2004), taking exams online produces a private and personal experience for the student; as opposed to writing test responses on paper, which can potentially reveal the student's errors to the public.

3.6 The Role of Feedback in Assessment

Feedback is a crucial component in a learning and assessment cycle. The primary aim of this process is to inform students on how well they have done and how to improve (Brown, 2001). Hence, engaging in constructive and timely feedback assists students' in reflecting on their progress. In the feedback mechanism, the type of feedback given to a student is dependent on the purpose of assessment employed (Gibbs & Simpsons, 2002).

Formative feedback typically occurs in an informal setting, where the goal is to provide information about the students' improvement and to motivate the students. Thus, one benefit of the continuous, constructive formative feedback is to create a point of dialogue between lecturers' and students' (Morgan & O'Reilly, 1999). According to Laurillard's (1995) conversational framework, such points of dialogue foster an

interactive environment providing meaningful feedback for the assessment tasks. Summative feedback may not provide feedback to each question; however, feedback is given based on a student's competency of the assessment tasks. The Summative feedback is often found on the comments section of a response sheet; and may or may not be discussed with the student (Schwiebert & Bondurant, 2000).

Generally, it is recommended that feedback should be provided quickly and without delay. As described in Gibbs & Simpsons, (2002) a delayed feedback may induce the student into learning a new content and the feedback from a previous assessment would become irrelevant to their ongoing studies. Hence, the feedback information may be considered less interesting and it is unlikely to enhance learning.

3.7 Summary

Assessment is an integral part of the educational process and it should not be divorced from it. To promote the reliability and validity of an assessment, the assessment task needs to be aligned in relation to the objectives of the course. By doing this, the extent to which a student has mastered the syllabus of a course taken is assessed. However, assessment is influenced by the underlying learning theories of the educational process. This implies that a curriculum designer or an assessor's decisions on the style of teaching and assessing reflects a Behaviourist, Cognitivist or Constructivist classroom. To a behaviourist, assessment means a re-take of tests until the learning content is mastered. A cognitivist enhances the prior knowledge of a learning resource, whilst constructivists' view the assessment process as a point of interaction between the lecturer and the student. Additionally, the method employed in grading an assessment task also influences the assessment process.

A norm-referenced grading scheme emphasises class ranking, where a student's scores is compared against a group of other scores to determine a grade. A downside of this method is that the individual performances are not revealed, but rather discrimination between high and low scorers. Hence, students are required to compete with each other for grades, which in turn may produce an unhealthy approach to assessment. For example, candidates may want to achieve high grades through every means possible; thus, an increase in security threats on the assessment process is inevitable. A criterion referenced scheme assigns a grade by measuring a student's score against a set of pre-defined criteria. This implies that a score would reveal the extent to

which a learning content is mastered. Criterion referencing embraces fairness in assessment, where the weak and strong students can be accommodated. By doing this, security threats are minimised as students are inspired to improve. However, defining the quality and validity of the criteria required often breeds disagreement amongst educators. The security of assessments is discussed in the next chapters.

Lastly, it is important to determine the purpose of designing an assessment either to monitor a student's progress during the course (formative) or to classify the student's performance at the end of a course (summative). The formative and summative assessments can be presented conventionally using pen and paper (on-paper) or displayed on a computer screen without an internet connection (on-screen) or offered flexibly to suit varying date and times (on-demand) or delivered electronically via the internet (on-line). However, a major drawback of all the presentation types is the security of the assessment process which is discussed in the next chapter.

Chapter 4. Electronic Assessment Security

In chapter three, it is noted that the on-paper, on-screen, on-demand and online approaches can be used to deliver a formative or summative assessment. The on-paper/traditional approach is highly susceptible to security challenges e.g. identity fraud and plagiarism; hence, the assessment system seeks solace in alternative approaches, i.e. on-screen, on-demand and online methods. In this thesis, the online approach and its security of assessment systems is considered. It should be noted that there exist security challenges in the on-screen and on-demand approaches; however, the discussions are beyond the scope of this research.

This chapter presents a detailed overview on using the online approach for the delivery of assessment tasks. In this thesis, the terms *'online'* and *'electronic'* will be used interchangeably, to denote an assessment task which is delivered via an internet connection. Employing an online delivery of assessment tasks presents valuable gains to the educational process; however, the approach is susceptible to a variety of security challenges. According to Rowe (2004), cheating online becomes easier, since what or who the student brings to the assessment site cannot be seen. Furthermore, four types of e-assessment security which can influence summative e-assessments are discussed; this includes user security, data security, location security and software security. Lastly, this chapter presents the three types of user authentication methods (i.e. possession, knowledge and biometric methods) and their implications for e-assessment security.

4.1 Electronic Assessment

Electronic assessment is presented as an alternative to traditional assessments where the assessment task is delivered and displayed on a computer screen via the internet. A formal definition refers to e-assessment as the use of ICT for the presentation of assessment activity and the recording of responses (JISC, 2006). Thus, in order to provide an alignment between the teaching, learning and assessment processes, it is

essential to employ the use of ICT in assessment (Gipps, 2003). Additionally, Brown *et al*, (1996) suggests that due to paradigm shift in educational technology, it may become unfair to train students online and then use pens for assessments. Adopting electronic assessments in a higher education environment embodies enormous benefits such as, automatic marking, immediate feedback to students, opportunities for lifelong learning and improved access for disabilities or geographically dispersed students. The three types of e-assessment which may be employed for assessing include: online formative, online summative and diagnostic assessment.

4.1.1 Formative E-assessment

Online formative assessment readily brings to mind the theory of Vygotsky (1986), where he suggests the need to build an atmosphere of social constructivism amongst the students and lecturers. The formative e-assessment process is supported through synchronous and asynchronous communication tools such as email, bulletin boards, news groups, and wikis. These electronic methods allow the students to pursue areas of perceived weakness and to affirm areas of strength (Challis, 2005). The core of a successful online formative assessment is the provision of immediate online feedback to students (Charman, 1999; 85). Typically, this is a personalised feedback aimed at addressing the student's individual needs. In addition, the online feedback should provide explanations for wrong responses to questions or advices on approaching the questions differently. Thus, the quality of formative feedback received is crucial as it distinguishes an effective course from other courses (Gilbert & Gale, 2008).

In online formative assessment, issues relating to security may be irrelevant as the priority is to improve learning and keep the students' informed about their progress. Thus, it is pointless to cheat in an assessment that is designed to gain knowledge (Challis, 2005). Additionally, adopting a high-level of security measure for formative assessments will be a waste of resources and can be a 'turnoff' for the students. Hence, in this thesis, the security of formative e-assessments would not be considered.

4.1.2 Summative E-assessment

Online summative assessment is categorised as high-stake examinations which takes place at the end of a course of study. Online summative examinations enjoy the benefits of an internet-network environment, where student responses to questions are automatically uploaded and marked (Aojula *et al*, 2006). This online approach

eliminates the need to safe-guard printed questions and answers sheets. One of the key benefits of summative e-assessments is the ability to automatically mark tests, which can minimise human errors due to fatigue.

Amidst the advantages, the summative e-assessment is perceived to be susceptible to a variety of security issues which challenges the online system. For example, to ensure data security, the item bank should be accessed by authorised parties only. Additionally, to ensure user security, the assessment should be delivered and taken by the correct student only. Hence, due to the high-stake nature of the summative tests it is essential to maintain a high security level. The remaining sections of this chapter and the successive chapters of this thesis focus on improving the security of online summative assessments.

4.1.3 Diagnostic Assessment

Diagnostic assessment has been associated as a testing carried out by educational psychologists for students with learning difficulties. However, in modern education it is used to identify a student's strengths and weakness or prior knowledge and skills in relation to a course programme (JISC, 2006) Diagnostic assessment sits between summative and formative assessments and it can be used to diagnose a student's ability at the beginning of a course (Boston, 2002). In formative assessment, an initial diagnosis aids in making decisions about a student's skills whilst as a summative test it serves as a basis for making a decision about a student's suitability for entry to a course (Ecclestone, 1996). Traditionally, diagnostic assessment may take the form of a one-to-one session with a career counsellor; however, in an online mode computerised diagnostic tools replace the physical advisor (Kutty *et al,* 2003). The diagnosis may present the lecturer with an overview of the students' ability, which may influence their teaching strategies. For example, in a work environment, a job applicant may be required to undergo a diagnostic test in order to determine the individual's competency for a job and the extra skills that may be needed.

Hence, it is futile for a student to cheat during diagnostic assessments; since the test is aimed at identifying strengths and weakness to aid intellectual growth. Thus, the students' who cheat during a diagnostic assessment may pass the test, feigning competency in the subject area. However, due to the lack of appropriate knowledge, the fraudulent students may have to continue cheating till the end of the course. Therefore, it

is important to ensure adequate security during diagnostic assessments to avoid security breaches during high-stake assessments. The security of diagnostic assessment is a potential research area; however, it will not be discussed in this thesis.

4.2 Computer Security Fundamentals

Security is a fundamental concept which is relevant in our daily lives and a top priority in several applications. Computer security is the generic name for the collection of related components such as assets, threats, goals and preventive measures designed to protect the system (Stallings, 2000). An asset refers to resources in the system that might have value and needs to be protected (ISO/IEC, 2005). Examples of assets that are protected in a system include: personal information, money (tangibles) and reputation (intangibles). Thus, identifying the relevant assets of a system can prevent harm to the assets if the system is misused. In general, every computer system is required to protect three primary assets, i.e. the hardware, software and data assets (Pfleeger & Pfleeger, 2003).

Computer and network security addresses three specific security goals of a computer system; these are the confidentiality (C), integrity (I) and availability (A) goals (Gollman 2006). The confidentiality goal ensures that only authorised users should have access to the protected asset. The integrity goal ensures that the protected asset is unaltered by unauthorised users or in unauthorised ways. The availability goal ensures that the assets are operational and available to authorised users.

A security relationship exists between the C-I-A security goals and the valuable assets of a computer system. Thus, a compromise of the C-I-A security goals may lead to a compromise of the critical assets. For example, a data asset is expected:

- To be accessed by only authorised parties; thus, data must be restricted (confidentiality goal).
- To contain no alterations of the original data; modification should be done by authorised parties only (integrity goal).
- To be operational and accessible whenever it is needed; except during authorised downtimes (availability goal).

A threat presents a source of danger which has the potential to cause loss or harm. In designing a computer system, it is important to understand the type of threats that can compromise the critical assets. Thus, computer security threats are grouped into

four classes, i.e. interception, interruption, modification and fabrication (Pfleeger & Pfleeger, 2003). Interception represents an attack on confidentiality when an unauthorised user gains access to an asset. Modification is an attack on integrity, such that an unauthorised user gains access and alters an asset. Interruption is an attack on availability and it occurs when there is a disruption to the service being provided, rendering the asset unusable. Fabrication is an attack on authenticity and it occurs when an unauthorised user creates a counterfeit of an asset. Authenticity is an addition to the three primary security goals; it may or may not be included in the taxonomy (Stallings, 2000). Thus, the authenticity goal verifies a claimed identity of a user.

4.3 Summative E-assessment Security

Online summative assessment is a powerful tool which embodies great benefits such as automated marking, immediate feedback and on-demand tests. Online summative assessments are categorised as high-stake examinations which count towards a final course mark. In higher education, summative e-assessments can be divided into two classes: (1) e-assessments in supervised environments and (2) e-assessments in non-supervised environments. Summative e-assessments which are conducted in supervised environments include campus based exams and authorised test centres (Rowe, 2004). In these environments, authorised personnel or proctors are required to monitor and supervise the examination process from start to finish. Non-supervised environments include tests conducted for distance learning. In these environments, the examination process may be supervised remotely; however the examinee is required to maintain academic honesty. This research focuses on summative e-assessments conducted in supervised/controlled conditions and do not assume a non-supervised environment.

Furnell (1998) asserts that higher education is not a sector in which security considerations feature; however, this changes when an online assessment is considered. Thus, for the purpose of conducting high-stake summative tests, it is important to define appropriate e-assessment security measures. In their work, Marais *et al,* (2006) identify two categories of security in e-assessments i.e. the web security and e-assessment security. They suggest that web security (securing of servers and web applications) is a well investigated area but it is insufficient to fulfil the security needs of e-assessment. Hence, the concept of e-assessment security requires that certain security checks be applied to ensure that a fair assessment is taken. The security checks identified in Marais

et al, (2006) and also pointed out in several researches are divided into four main classes: user security, data security, location security and software security (Table 4-1)

E-assessment Security Type	Examples	References
User security	• To ensure the correct identity and authenticity of the person taking the test	Paulsen, 2000; Aojula *et al,* 2006; Weippl, 2006
Data security	• The non-deniability of e-assessment submissions • The e-assessment integrity should deter electronic corruption. • The privacy and confidentiality of assessment data	Summons & Simon, 1998; McKeena & Bull, 2000; Weippl, 2005; Gonzalez-Tablas *et al,* 2006
Location security	• The e-assessment should be taken in the correct/supervised location	Marais *et al,* 2006; Apampa, *et al* 2008a; Walton, 2005
Software security	• The secure set-up of client and server software.	von Solms, 2004; Harwood, 2005; Gilbert *et al,* 2009

Table 4-1 E-assessment security types

4.3.1 User Security

Due to the high-stake nature of a summative e-assessment, it is essential that only a legitimate student can gain access to the online test. A user security process consists of user security components, such as identification, authentication and access control, to determine a user's access rights. The user security process of a summative e-assessment makes up a core area of ensuring the reliability and validity of the online assessment. Hence, a compromise to the user security process may render the assessment unreliable and invalid. However, the user security process is fallible to security threats which plague existing online summative assessment systems (Warren & Hutchinson, 2003; Sangi, 2008). The user security process and its security threats are discussed in the next chapter.

4.3.2 Data Security

Data security in summative e-assessment is the practice of ensuring that assessment data is administered securely without endangering the integrity of the data. According to the Office of the Qualifications and Examinations Regulator in the UK

(QCA, 2007), it is vital that the e-assessment system have sufficient capacity to store, retrieve, generate and share assessment data, including the ability to exchange data securely. In Gilbert *et al,* (2009) recommendations to ensure data security in summative e-assessments are divided into two classes, security of test materials and results; security of assessment data transferred over networks.

Security of test materials and results:

The e-assessment database is a large pool of related components from which assessments can be built; including test items, scoring keys and assessment algorithms (Anzaldua, 2002). Therefore, it is vital that steps are taken to ensure security of the database. A concern during the design of the e-assessment database is the exposure of items and this flaw can occur through item authoring, item selection or item validation. A worst scenario occurs when a student gains prior knowledge of such items and solutions; it can be used to their advantage during the test.

In literature, there are proposals towards the deployment of cryptography as a solution for most data security issues in e-assessment. Examples of existing work in cryptography include: digital signatures can be used to ensure non-repudiation of test submissions (Gonzalez-Tablas *et al,* 2006), data encryption can be used to obtain confidentiality for test responses (Weippl, 2005) and hash functions can be used to maintain the integrity of the test responses (Shafarenko & Barsky, 2000). Additionally, the secure storage of the assessment data is an important aspect of the e-assessment data security. Therefore to maintain the reliability and validity of an online test, security measures are required to restrict access to the results data, including backup results data.

Security of assessment data transferred over networks

The design of the e-assessment system should allow for secure transfer of test materials over the network. Thus, where a test is delivered on a network or intranet, the server and connections should be adequate to ensure integrity of data, secrecy of data and availability of service. In addition, the e-assessment system should have features that ensure regular and frequent backups of all collected data that allow for data recovery if problems occur with the network.

4.3.3 Location Security

Marais *et al,* (2006), proposes the concept of location security for e-assessments. Their work suggests that the electronic integrity of an e-assessment system may be threatened as a result of un-implemented location security measures. In addition, the electronic integrity of an e-assessment system can be violated by electronic corruption. An example of electronic corruption during an online test is when a student double submits a test from the same location. This means that when Student A completes his test; he can use the knowledge of a just completed test to complete another Student B's test if security measures are not in place. Thus, to deter the fraudulent act, the server should deny two logins originating from the same IP address (Marais *et al,* 2006). However, this solution can present further loopholes when non-static IP addresses are used and an invigilator is required to override the system rules. Thus, the students can exploit the flexibilities presented by the invigilator.

A workaround to this solution is the use of static IP addresses tied to the student login ID (Apampa, *et al* 2008a). In our approach, a student's login ID is associated with an available static IP address (Bx07r + 192.168.10.3), such that a computer that is connected to the network will retain the same IP address for the duration of the assessment. Thus, a deliberate reboot of the computer will not produce a new IP address neither would the invigilator need to modify functions when a computer stalls. Figure 4-1 shows a diagrammatic illustration of the proposed solution by assuming two characters Bob and Alice. In Figure 4-1, access is granted to Bob when he logs in on a computer assigned to his user ID. Likewise, access is granted to Alice by logging on to a computer assigned to her user ID. However, Bob is denied access when logging on to his assigned computer via Alice's user ID; thus, access is granted only when Alice's user ID is used on her computer. Additionally, to track the static IP and user ID process a registration log can be printed when all available computers are occupied. The log is also useful to prevent student swaps during the test. Irrespective of the techniques suggested, location security is still an unexplored research area embedded with potential research opportunities.

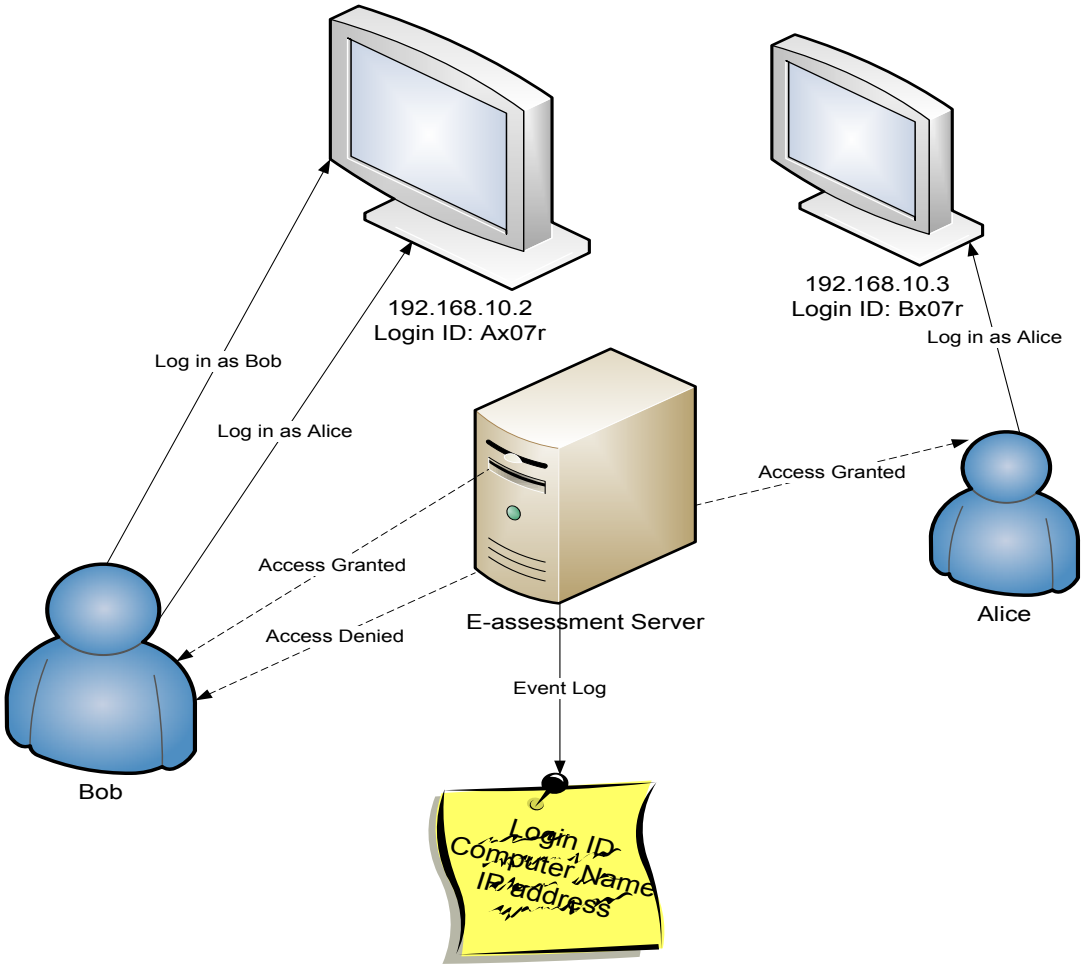


Figure 4-1 Static IP address mapped to user ID

4.3.4 Software / Application Security

The availability of an e-assessment software or application is important to the success of the e-assessment system. Therefore, it is important that the application software is developed from the beginning with security in mind, as this will enable the software to resist, tolerate and recover from attacks effectively (Allen *et al,* 2008). It is important to ensure that a malicious person or programs does not disrupt a summative e-assessment before, during or after the test. For example, a student that failed to prepare for the online test may decide to launch an attack on the e-assessment server. Thus, it is the responsibility of the systems administrator to install OS patches, virus and mail scanners and this should be kept up to date (WebCT Security, 2005).

4.4 User Authentication Techniques for E-assessment Security

User authentication is a crucial procedure in existing computer security systems; the authentication step is used to determine the users that can gain access to a secured resource or asset. In literature, there are three primary classes of a user authentication procedure, namely possession, knowledge and biometrics methods (Nanavati *et al,* 2002). This thesis adopts the three primary classes of user authentication; these classes present a foundation for the e-assessment user security discussions in the remaining chapters.

Possession: this consists of physical objects which belong to the correct user. The object is required to gain access to a resource or service. Examples in this category include smart cards, badges and keys.

Knowledge: this consists of information or data which is known only to the correct user and it is required to be kept a secret. Examples include, passwords, PINs, combination locks and challenge questions.

Biometrics: this consists of the unique physiological and behavioural characteristics of a human being. Examples include fingerprint technology, iris recognition, facial recognition, voice recognition and signature recognition.

Table 4-2 lists examples and properties of user authentication methods. For example, a user is able to access a requested service via the knowledge of password. Additionally, to achieve a higher level of security more complex systems such as two-factor or multi-factor authentication should be implemented (Bolle *et al,* 2003). These complex systems employ more than one form of authentication to verify the identity of a user. A typical example of the two-factor authentication can occur using a bank card and a PIN to carrying out bank transactions via an automated teller machine (ATM). Therefore, a bank card is useless without the knowledge of the associated PIN in carrying out transactions. However, in this thesis, the two-factor or multi-factor authentication method is not considered.

Method	Examples	Properties
What the user has *(P)*	User IDs, accounts, smartcards, badges, keys	Can be shared Can be duplicated Can be lost or stolen
What the user knows*(K)*	Password, PIN, Mother's maiden name, Lock codes	Easy to guess Can be shared Can be forgotten
Something unique about the user *(B*)	Fingerprint, face, iris, voiceprint	Cannot be shared Cannot be lost or stolen Not forgeable
What you have and what you know *(P, K)*	ATM card + PIN	Can be shared PIN is a weak link

Table 4-2 Existing user authentication methods

4.5 Possession Methods

Possession methods consist of physical objects which belong to the correct user and they are required for access. A smart card is a commonly used physical object which can be used to achieve user authentication. Smart cards are credit card-sized plastic cards with embedded memory to store and process data. The smart cards have benefits which can improve the security of the user authentication process, e.g. the smart card can store a hash function of a user login details (Yang *et al,* 2008). Additionally, the smart cards can be used as a Single Sign-on (SSO) for logging in to several computers in an environment (Fugkeaw *et al,* 2007). The smart card technology is not new to higher education and it is typically adopted for student identification. Thus, the student ID card via the smart card can contain the details which could allow access to several facilities in the institution environment, such as access to library services, catering facilities, transportation and buildings.

However, the use of smart cards for student authentication during summative e-assessments is not a common method. Owing to its hardware and infrastructure implications, smart cards may be an expensive authentication method for online tests. Lastly, Graf (2002) asserts that, the use of smartcards is not a viable alternative for user

authentication in summative e-assessments. For the purpose of this study, the possession methods would not be considered.

4.6 Knowledge Methods

A user password is a popular method of authentication in accessing computer systems (Oorschot & Thorpe, 2008). Passwords refer to mutually agreed-upon code words, which is shared between the user and the system only. Thus, a password can either be user-chosen (where a user chooses easy-to-remember passwords) or system-assigned (where the password is written in a safe place). However, Argles *et al*, (2007) assert that, insisting on short and easy passwords to memorise can lead to a breach of security. This implies that users are likely to employ passwords that can be broken through an exhaustive search of a relatively small subset from a small domain (Klein, 1990). In a small password domain, adversaries attempt to try all possible passwords until the correct password is located. The password management system is an approach which can be used to strengthen password against adversaries. For example, a password system may enforce rules which require that user passwords should include a numeric digit and/or a capital letter. In a password operation, the user enters an identification detail, e.g. a username or a user ID. To verify the identity claimed, a password request is made to the user. Thus, the system compares the input password and the stored password; a match indicates successful authentication and a mismatch would require that the user re-types the password.

In a survey of identity management in higher education, Yanosky & Salaway, (2006), found out that 91.1% of respondents continue to rely on passwords for authenticating students in online environments. In e-assessments, the password is the most popular and inexpensive method of identifying and authenticating students. The success of the password is attributed to its ease of use, such that a special device is not required for data collection. Thus, the students are able to choose short and easy-to-remember passwords for their convenience (Adams & Sasse, 1999). However, these passwords have inherent weaknesses which make them easily susceptible to compromise. For example, the passwords are often poorly selected and infrequently changed. Additionally, due to the shareable and transferable nature of knowledge methods, a student's login details can be shared with other people. Lastly in this section,

existing password authentication implementations are presented. The password schemes show the various resistance levels to intruder attacks.

Basic Password:

In this method, the password is transmitted in plaintext from the client to the server. The server compares the plaintext password with a stored version and access is granted when authentication is successful. However, due to the simplicity of the method, the user password can be intercepted and used in a variety of attacks, such as eavesdropping (Boyd & Mathuria, 2003) and man-in-the-middle attacks (Lowe, 1995).

Hash Password:

The hash password method is an improvement to transmitting a user's password in the clear. In this technique an image of the password is computed under a one-way hash function and the image is stored in the password file. To verify a user's password, the server compares the hash password from the client and the hash stored in the server. Thus, a match indicates that the input user password is correct. In a one-way hash operation, the function takes a plaintext value returns a hash value which is hard to invert (Menezes *et al,* 1996). This means that it is computationally infeasible to find the input from a given hash value. However, to prevent cryptanalysis, the hash functions are used together with nonce values (Anderson, 2001). The nonce (number used once) is a random value used as proof of freshness or timeliness.

Kerberos:

Kerberos was developed at the Massachusetts Institute of Technology (MIT) as a third party authentication service for the protection of network services (Steiner *et al,* 1988). In traditional authentication schemes, passwords are transmitted either as plaintext or hashed values. However, in Kerberos the encrypted keys are transmitted instead of the passwords. Additionally, to improve security and reduce man-in-the-middle attacks, a mutual authentication facility between the client and server is implemented. In a mutual authentication, the identity of the client and server is verified.

One time passwords:

Adopting a one-time password scheme, the computer system is required to generate a new password for each authentication process (Haller, 1994). This means that, once a password is used it cannot be re-used; thus, the computer system produces one-

time passwords by decrementing a sequence number. Additionally, one-time passwords can be derived from a chosen user password; however, the user will be provided with a long list of potential passwords which is written (Halevi & Krawczyk, 1999). A disadvantage of this method is the inconvenience incurred in carrying a long list of passwords and ensuring that the list is safe and secret. A variant of the one-time passwords is the challenge-response mechanism, where the server selects a random challenge for each new authentication instance (Liang & Wang, 2005).

4.6.1 Password Authentication Schemes in Higher Education

In this section, two prominent password authentication schemes employed in the higher education environment is discussed. This includes the Lightweight Directory Access Protocol (LDAP) and the Shibboleth technology.

4.6.1.1 The Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) is a general purpose database management system, optimised for use as a directory server and the directory structure is suitable for storing user data, which can be accessed through the LDAP protocol (RFC 1777). In higher education institutions in the UK, the LDAP is a common choice for providing user authentication (central user password system) and directory information for individuals throughout the institution. Furthermore, the LDAP can be used for verifying users membership in a university community, retrieving an employee's contact information, confirming a student's course registration and accessing the email directory (of some mail clients). The LDAP is a platform-independent protocol which is integrated with most network operating systems. For example, LDAP directories such as Microsoft Active Directory and Novel eDirectory provide a low cost method for implementing fast identity look-ups and authentication.

One of the disadvantages of the traditional LDAP is the inability to support a single sign-on authentication for users. In a single sign-on (SSO) process, gaining access into one service automatically authenticates the user for all the other services. Thus, this reduces the amount of passwords a user is required to memorise. A SSO process may also be used to implement stronger authentication methods. For example, a user's password may be employed to gain access to a computer; however, a two-factor authentication method may be required to gain access to sensitive information or applications.

4.6.1.2 Shibboleth Technology

In higher education institutions, the Shibboleth protocol is gradually replacing the LDAP as a method for user management and authentication. This protocol offers the account synchronisation capabilities of the LDAP including the single sign-on functionality. Thus, a user logged into a Shibboleth system is provided a seamless access to other Shibboleth protected services, eliminating the need to log in again. The Shibboleth protocol improves the users' experience by eliminating the need to remember multiple passwords (Shibboleth, 2001). Additionally, the Shibboleth is designed to be used across institutions to verify a user's affiliation to an institution. Hence, web applications establish a trust relationship between institutions in order to allow users log in to services outside their institution. This relationship is provided through a federation; a federation represents groups of similar organisations (e.g. universities) which use the shibboleth technology to share and access a set of resources.

In Shibboleth, the user authentication process is delegated to the user's local institution or organisation which is known as the Shibboleth Identity Provider (SIP). The Shibboleth Identity Provider ensures that the relevant authentication detail about the user is up-to-date and available to the application. Lastly, the Shibboleth Service Provider (SSP) determines whether a user is authorised to access the resource. The decision of the Service Provider is influenced by the affiliation status information supplied from the user's home institution. Thus, the information passed on to the Service Provider is about status rather than personal identity and this helps to preserves user privacy (JISC 2006).

4.6.2 LDAP and Shibboleth in Electronic Assessments

User authentication is one of the main purposes of an LDAP. Thus, during a summative e-assessment the student would simply enter a password in an entry point. The LDAP server (either remotely or locally) would receive the authentication requests and respond to the requests accordingly. Amidst its technical disadvantages, a LDAP authentication is perceived to be a more suitable solution for an online summative assessment environment. This is as a result of its strong user authentication functionalities which is core to a summative e-assessment. The Shibboleth technology offers benefits in providing a secure channel for the transfer of user affiliation information between institutions (and publishers). However, the primary purpose of the Shibboleth software is not for user authentication. Hence, incorporating the Shibboleth

software into the online assessment may be unsuitable for high-stake summative assessments. In Shibboleth, the user authentication process is not included in the Shibboleth software, but rather devolved to be performed by the home institution. This implies that, Shibboleth relies on the local institution (Shibboleth Identity Provider) to establish the students' identity before access is granted. In most cases, the LDAP authentication will be deployed at the student's institution; thus, the Shibboleth Identity Provider will be naturally connected to an existing identity management structure.

However, irrespective of the potentials apparent in the LDAP-Shibboleth integration; a downside in adopting the protocol for summative e-assessments will be the SSO services of the Shibboleth software. A SSO will improve the student's online experience, such that a student is required to log in once only for the duration of the test. It is perceived that, integrating an SSO in summative e-assessments will attract security threats and decrease the reliability standards of the test. For example, an external person may substitute a correctly authenticated student halfway through a test. However, the dishonest act may not be detected, since the original student is expected to sign in once only at the start of the test.

4.7 Biometric Methods

Biometric technology is the measurement of the unique characteristics inherent in human beings. This distinct attributes provide an assurance about the true identity of an individual. A biometric system is a pattern-recognition system that distinguishes people based on a feature vector derived from the physiological and/or behavioural characteristics (Jain *et al,* 2004). The physiological characteristics are derived from the direct measurements of a human body part (e.g. finger and face); whilst, the behavioural characteristics are indirectly measured (e.g. keystroke analysis). The behavioural biometric data is derived over a period of time and the temporal variation of the characteristics contains the required identity information. However, a biometric system which adopts physiological characteristics is often more reliable than a behavioural-based biometric system (Delac & Grgic, 2004).

A biometric architecture consists of two simple stages depicted in Figure 4-2. During the enrolment phase, a user's biometric image is acquired and a biometric template is created. The templates may be stored in a database or on a portable storage device (Davida *et al,* 1998). During the authentication phase, a user's raw biometric data

is compared with the stored template. A match between the input data and the stored template signifies that the user is successfully authenticated.

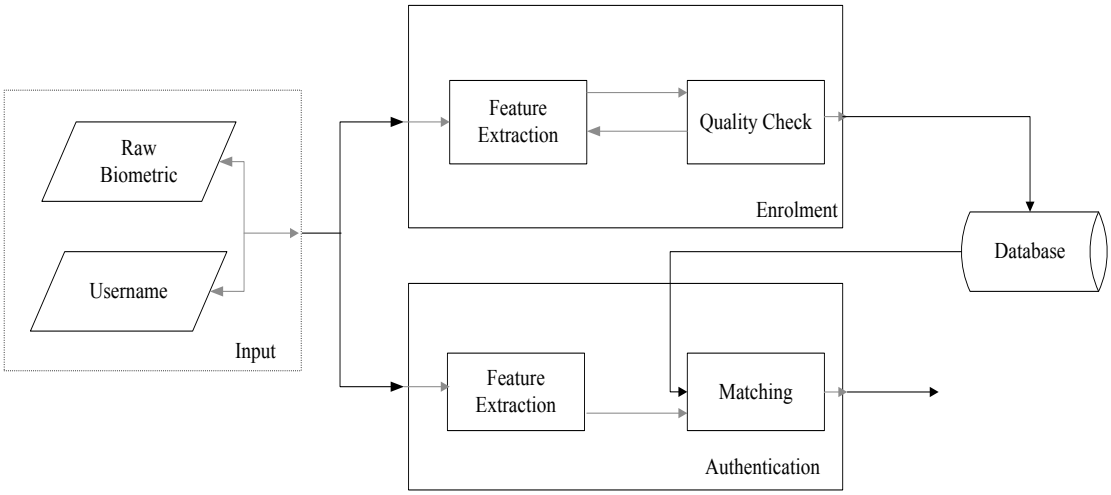


Figure 4-2 Biometric architecture (Jain & Panakanti, 2000)

To characterise a biometric human identifier it is important to employ a set of criteria. The suitability of a chosen biometric identifier can be evaluated using the following seven guidelines (Jain *et al,* 2004).

- Universality: All human beings should be endowed with the same physical characteristics, e.g. fingers, face and iris
- Uniqueness: For each person these physical characteristics should be distinct.
- Permanence: These characteristics should remain largely unchanged over time
- Collectability: A person's unique physical characteristics need to be measureable and collected in a reasonable easy manner.
- Performance: The degree of accuracy of identification must be quite high before the system can be operational.
- Acceptability: The user population and the public in general should have no (strong) objections to the measuring/collection of the biometric
- Resistance to Circumvention: In order to provide added security, the system needs to be robust to withstand fraudulent methods

4.7.1 Biometric Methodologies

In biometric literature, there exists a progressing list of biometric technologies implemented in applications. According to Prabhakar *et al,* (2003), there is no single biometric which is the 'ultimate' recognition tool and the methodology chosen depends

on the application. In this section, examples of commonly used biometric methods are presented (see Figure 4-3).

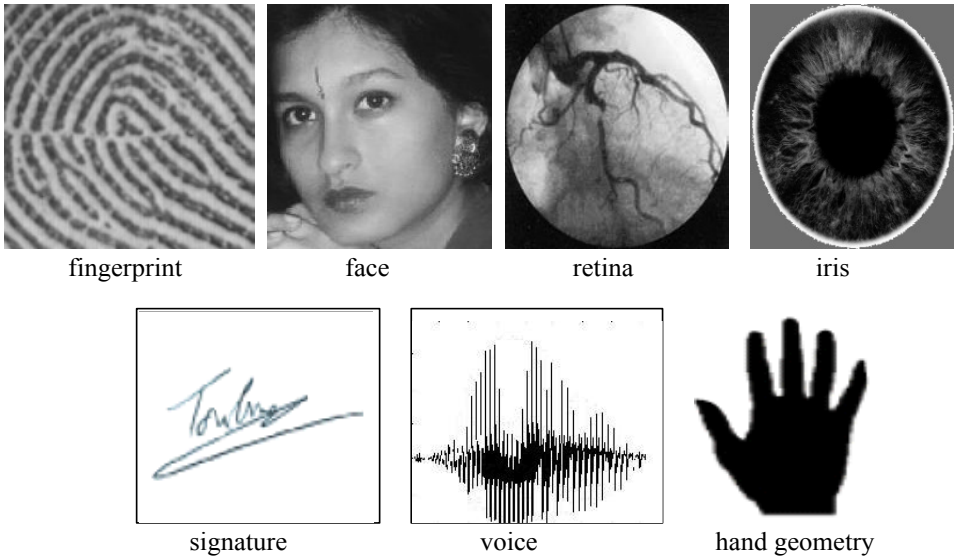


Figure 4-3 Examples of biometric characteristics

Fingerprint:

The fingerprint biometric is an automated digital version of the old ink and paper method used for identification (Maio *et al,* 2004). A fingerprint is made up of ridges and furrows located on the fingertips; hence, the uniqueness of a fingerprint can be determined by the pattern of ridges, furrows and the minutiae points. In fingerprint recognition operation, the input image is acquired through a direct contact of the finger on the fingerprint scanner. The acquired images are then sent to a feature extraction module, where the feature values corresponding to the position of the minutiae points are computed. Finally, the minutiae patterns extracted from the fingerprints are compared with the stored template.

The biometric fingerprint is a mature technology and it enjoys a wide public acceptance (Jain *et al,* 1997). Additionally, the biometric fingerprint is proposed as a suitable authentication method for summative e-assessments (Marais *et al,* 2006; Levy & Ramim, 2007). A biometric fingerprint is an active authentication/verification method; thus, a level of user involvement is required during the verification process. Hence, adopting the fingerprints for presence verification in summative e-assessments can become interruptive and distracting to the students test.

Face:

Facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The biometric face recognition is an automated method which is used to record the spatial geometry of distinguishing features of the face. The facial features can be based on the spatial relationship of facial attributes (e.g. eyes, eyebrows, nose and lips) or on the overall analysis of the face image (Jain *et al,* 2004). During the verification process, a two-dimensional image of the user's face is obtained and a feature set is extracted. The facial features extracted are then matched with the stored templates. The biometric face recognition is a non-intrusive method, which is suitable for covert recognition applications i.e. applications were the image is taken without the knowledge of the individual.

The non-intrusive ability of the face biometric is well suited for achieving presence verification in summative e-assessments. The face is a passive biometric which does not require active user participation during the authentication; hence, it is unlikely to interrupt user's activities during the process (Jain *et al,* 2004). However, a potential challenge to adopting the face biometric for presence verification is the inability of the face recognition system to authenticate/verify non-frontal poses (Zhang & Gao, 2009). In a test environment, it is unlikely for a student to consistently focus on the camera throughout the test session. However, it is likely that the student will focus on the camera at non-calculated times during the test. Thus, there will be an increase in false negatives due to the inability of the face authentication system to accurately verify the student's non-frontal poses. This implies that the face biometric may be unsuitable for presence verification in summative e-assessments.

Retina Scan:

The retina recognition creates an 'eye signature' by measuring the blood vessel patterns in the back of the eyes. The blood vessel patterns are a unique characteristic of each individual (Jain *et al,* 2002). During the image acquisition process, the individual is required to look through a lens at an alignment target; thus, the concentration and cooperation of the user is essential to capture a useful image. Replicating the retinal vasculature is a non-trivial task and this makes the retina one of the most secure biometric.

As a secure biometric, the retina scan will be suitable for presence verification in summative e-assessments environments; this is because the stored biometric templates cannot be easily compromised. In addition, the deception of the system is very unlikely (Newman, 2009). This implies that, the method will provide a proof that the student presenting the raw biometric image is the original student. However, a challenge to adopting the retina scan method is that, an individual's retina can change as a result of medical conditions such as pregnancy or high blood pressure. Thus, the variations or changes to a student's retina can increase the risk of false positives and false negatives during a presence verification process.

Iris Scan:

The iris contains many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and zigzag collarette (Daugman, 2004). Daugman, (1993) asserts that, the unique nature of the iris shows that a person's left and right eyes have different iris patterns and even irises of identical twins are different.

Adopting the iris-scan for presence verification in summative e-assessments will produce a less intrusive and more user friendly method for students. Additionally, the iris-scan method offers a highly accurate method which will reduce the risk of false positives (Ashbourn, 2005). However, the iris can be difficult to capture as it is easily obscured by eyelashes, eyelids and reflection from the cornea. The difficulties presented in capturing the iris for verification, can pose a challenge when used for presence verification in a test environment.

Signature Verification:

Signature verification (Ohishi *et al,* 2000) is an automated method, which can be used to determine the pattern that a name is signed. In this technology, a person's signature is collected using a stylus (pen) and a sensor pad; thus, dynamics such as speed, direction, pressure of writing and total time of signature is examined for uniqueness.

A signature verification method is non-intrusive; thus, it is suitable for presence verification as it is unlikely to interrupt a user during the process. However, a signature is a behavioural biometric that is unstable and may vary over a period time. Additionally, the technology is perceived susceptible to fraud and imitation (Fairhurst, 1997). In a test

environment, the signature method may increases the risk of impersonation challenges in and will become less-efficient for presence verification.

Hand Geometry:

Hand geometry recognition relies on measuring the structure of the hand, by using the distinctive aspects of an individual's hand, such as the dimension of fingers, location of joints, shape and size of the palm (Zunkel, 1998).

The hand geometry is one of the earliest and well-developed technologies. The simple, inexpensive and easy to use nature of the technique makes it a suitable candidate for presence verification in summative e-assessments. However, the hand geometry biometric has a low-level of uniqueness which is unsuitable for authentication/verification processes; hence, this method is better suited for identification purposes (Sanchez-Reillo *et al,* 2000).

Keystroke Dynamics:

In keystroke dynamics it is perceived that each person types on a keyboard in a distinct way (Monrose & Rubin, 2000). This technology examines dynamics such as typing speed, pressure, total time of typing a password and the time taken to hit certain keys. The combination of these features creates a template and forms a statistical profile of the person's behavioural characteristics.

The keystroke dynamics does not require extra additional hardware and minimal training is required for enrolment. Additionally, the technique is easy to implement in real time applications and a person's keystrokes can be monitored unobtrusively. However, the keystroke dynamics is less-suited for presence verification in e-assessment; this is due to the changes in typing patterns and the variations in keyboard layout. Lastly, the technology is still in its infancy and has not been tested on a wide scale for authentication/verification purposes (Levy & Ramim, 2007).

4.8 Biometric Authentication Systems

In current security systems, biometrics can operate in two modes: as an identification or authentication mechanism. A biometric identification system performs a one-to-many match, such that the system establishes a subject's identity without the subject having to claim an identity (Jain *et al,* 1997). For example, using fingerprints, a biometric identification system matches the fingerprint scan against a large database of

enrolled fingerprints in order to find a match. Thus, the matcher is only required to return the most similar template. However, in a biometric authentication system, a person desired to be identified submits an identity claim to the system (e.g. username, smart card) and the security system either rejects or accepts the claimed identity (Wayman, 2001). For example, in a biometric authentication system, a fingerprint scan is matched against only one possible user i.e. a one-to-one match. Hence, a biometric authentication system is required to match a fingerprint to its owner; rather than to any subject's fingerprint (most similar template).

In educational environments, the quest to implement advanced security measures, suggests biometrics as the ultimate solution for authentication in summative e-assessments (Marais *et al,* 2006). Thus, in summative e-assessment security, the fingerprint biometrics is gradually accepted and adopted as a method for student authentication (Williams, 2002; Hernandez *et al*, 2008). Fingerprint solutions are the less expensive and are more convenient compared to other biometric methods. Employing the fingerprints for identification does not require a username i.e. the matcher compares the input biometric against all the templates in the database. However, using the fingerprints as a method for student authentication requires a claimed identity i.e. a username should be associated with the fingerprint. In the real-world e-assessment environment, a biometric authentication system is more commonly used than a biometric identification system.

4.8.1 Biometric Template Security in Authentication Systems

Biometric data is unchangeable and not forgettable; thus, it is useful for ensuring user authentication (Ashbourn, 2000). However, incorporating biometrics as an authentication method presents privacy concerns derived from storage of the template data (Jain *et al*, 2007). According to Ratha *et al,* (2007) *"if a biometric identifier is compromised it is lost forever and possibly for every application where the biometric is used"*. This is particularly significant, as a biometric factor loses its uniqueness when a users' raw biometric is exposed. Thus, it is the responsibility of a system which adopts biometrics for authentication to ensure that the biometric templates are kept private.

One potential means of safe-guarding stored templates is encryption. However, Braithwaite *et al,* (2002) asserts that, since the biometric templates require decryption prior to matching; there is a risk of exposing the biometric data to potential hacker

attacks. In a review article, Jain *et al,* (2007) also suggests that biometric templates cannot be stored in an encrypted form. In literature, several methods have been suggested to protect the biometric templates during the matching process. A popular method is the cancellable transforms proposed by Ratha *et al,* (2001) to minimise the exposure of biometric data. In their work, the raw biometric data are uniquely distorted such that the original raw biometric is transformed using a one-way function. Thus, the transformed biometric and the transformation are stored instead of the raw biometric. This method aims to preserve privacy since the transformations are intended to be non-reversible; therefore it is computationally hard to recover the original biometric identifier from the transformed version. However, (in some cases) it may be necessary to revert the transformation prior to the matching process; again, this would expose the raw biometric data and make it susceptible to hacking (Braithwaite *et al,* 2002).

Recently, Argles *et al,* (2007) suggested a method to ensure privacy of the user's biometric even when the biometric database is compromised. In their work, a split and merge technique is used to ensure privacy of the biometric factors; and this is done by splitting the authentication factor into multiple components. One half of the encrypted template is stored on an electronic media and the other is retained inside the secure biometric database. An advantage of storing the encrypted data in two separate locations is such that, it becomes harder for an attacker to compromise the system. Therefore, without the decryption key the attacker will be required to break the encryption algorithm. However, once the key generator is exposed the information leakage reduces the difficulty of guessing the template; thus, it is essential that the key generator is kept private (Apampa *et al,* 2008b). The method introduced in Apampa *et al,* (2008b) to preserve the privacy of user biometrics is discussed in the next chapter. Other solutions for protecting biometric templates include the Steganography principles (Jain & Uludag, 2003) and the Secure Sketch Scheme (Sutcu *et al,* 2007).

4.9 Summary

Electronic assessment is a valuable addition to higher education. The e-assessment process embodies great benefits such as delivery of online tests, automatic marking, immediate feedback, improved access and opportunities for lifelong learning. The three types of e-assessment employed for assessing include the online formative, diagnostic assessment and online summative. Online formative assessments are

designed to improve the student's learning and give information about their progress. The diagnostic assessments are used identify a student's strengths and weaknesses to determine a suitable course programme; whilst the online summative assessment is categorised as a high-stake examination which takes place at the end of a course of study. In this thesis, security issues for formative and diagnostic e-assessments are not considered since these tests are designed to improve the student's learning experience. However, the high-stake nature of the summative e-assessments makes these tests a target for fraudulent activities. This chapter introduced the user security process of the summative e-assessment as a challenge in the academic community. Thus, user security of online summative assessments is discussed extensively in the next chapters.

User authentication is an essential procedure in securing the users of computer systems; this procedure consists of possession, knowledge and biometrics methods. Additionally, these methods present a foundation for the summative e-assessment user security discussions in the remaining chapters. The smart card is an example of the possession methods which are suitable for student identification; however, the smartcards are not viable for user authentication summative e-assessments. A password is a popularly employed knowledge method to authenticate students in e-assessments; this method is simple and easy to use. Biometric technologies are gradually gaining acceptance in e-assessment environments and commonly proposed methodologies for user authentication include fingerprint scan, face recognition and keyboard dynamics. In biometric technology, adopting biometrics for authentication (as opposed to identification) requires a match between the biometric identifier and only one possible user. This implies that an identity (e.g. a username) should be associated with the biometric identifier prior to authentication; this is particularly suitable for an e-assessment environment. However, one of the challenges in adopting a biometric authentication system is the issue of preserving the privacy of the raw biometrics during the matching process. The next chapter describes an inexpensive method which does not expose raw biometric data and which is suitable for an e-assessment environment.

Chapter 5. Identity-Authentication (I-A) User Security Model

Recall in chapter four, the data security and software security of a summative e-assessment are well-researched areas. The location security is in its early stages, but it is a promising area of research. However, the user security process is susceptible to security threats which threaten the overall security of the summative e-assessment environment. Due to the positioning of the user security process in e-assessment, it becomes expedient to determine the type of security challenges facing the security model. Thus, this chapter presents a review of the Identity-Authentication user security model which is commonly adopted for the user security of summative e-assessments. Lastly, the capability of the I-A user security model to provide a secure environment void of impersonation threats is discussed. Overall, this chapter lays a foundation for the first research objective of this thesis. A complete exploration is presented in the next chapter.

5.1 Identity-Authentication (I-A) User Security

One of the characteristics of an e-assessment system is the ability to securely deliver a test, at the right time and to the correct student. Thus, the user security model plays a vital role in e-assessments; as it ensures that only the correct students write an online test at any particular time. To fulfil this role, the user security model poses two questions in the form of a challenge to the students. Hence, the receipt of correct responses to the questions will assure the security system that the correct students are taking the test. In this section, the questions provided by the security system and the common types of responses are explored. Figure 5-1 depicts the questions posed to the student during an online assessment.

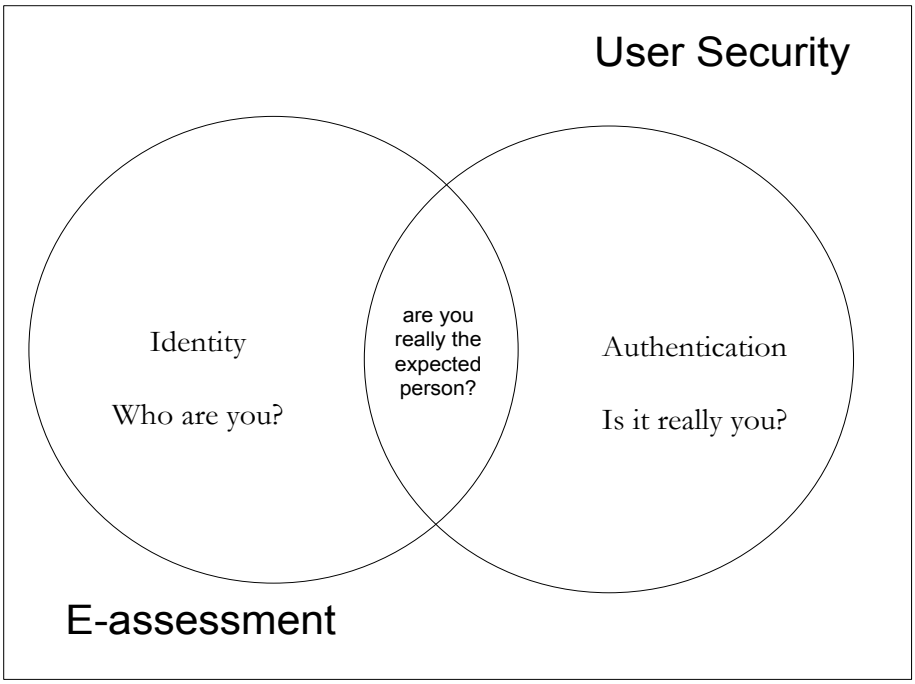


Figure 5-1 Identity-Authentication User Security Model

5.1.1 Identity

Identity is a term that cuts across several disciplines, sectors, cultures and industries; thus the term is defined differently, yet similar in perception. For example, in the field of Mathematics, identity refers to an equality that is true irrespective of the values of its variables (Biggs, 2002); whilst in Social Sciences, identity is a term used to describe a person's comprehension of him or herself as a discrete entity (Padilla & Perez, 2003) and in Computer Science (object-oriented programming) it is described as the property of objects that makes them different from other objects (Turner & Eden, 2008). Irrespective of the diversity in definition, it is observed from the above examples that identity reflects uniqueness, sameness and distinctness. Hence, when an e-assessment security system solicits an answer to the "who are you?" question, it simply requires that the student provides a unique response which distinguishes him/her from every other student. The responses provided by a student are typically in form of a username, student name, student number and email address. The method of student response is often decided by the e-assessment personnel; however, a commonly used form of identity in e-assessment is the *username*.

A username in the context of this thesis refers to a unique log-in name that can be a fictitious name, a combination of the student's name and/or student number or the

student's email address. It is important that the security system recognises the username supplied and associates it with a particular student. Hence, the username is stored on the security system and retrieved for comparison when access is needed. A username is not secret information and it can be shared or stolen for fraudulent purposes. In addition, providing a username only method makes the e-assessment security system an easy hurdle for the students to scale through. In an identity only system, the students are required to provide one answer; however, this response does not ensure correctness of the student. In order to ensure correctness, the e-assessment security system solicits an additional response to confirm the claimed identity. It should be noted that there are no known examples of an identity only system in existing summative e-assessment security systems.

5.1.2 Authentication

In e-assessment, it is insufficient to assume correctness of a student based on corresponding identities (i.e. claimed and stored identity); however, more is required to prove that the identity claimed actually belongs to the owner who stored the information. As described in section above, the e-assessment security requires an additional security layer to ensure that the identity presented is correct. Hence, when the security system solicits an answer to the "is it really you?" question; it simply requests a confirmation or evidence of the claimed identity. Authentication data is often a secret which should be known to the student and the security system alone. Thus, a student chooses an authentication data and stores it on the security system, in order to gain access to the online test during authentication.

User authentication is a widely discussed subject both in assessment and non-assessment online environments and it is well-documented (Clarke & Furnell, 2007; Furnell *et al,* 2008). Recall in chapter four a detailed overview on user authentication categories was presented. In general, user authentication is classified into three categories: something the user has (possession), something the user knows (knowledge) and something the user is (biometrics). Possession based methods, such as smart cards are widely used in e-learning environments. Example applications include, access to building and transportation facilities. However, these solutions are more suited for identification purposes and are not a viable alternative for user authentication (Graf, 2002). Additionally, it is not common to find smart cards as an authentication technique

for summative e-assessments; hence, the use of smart cards is beyond the scope of this thesis.

In knowledge based methods, the password is commonly used to authenticate students, whilst in biometric methods the biometric identifier (e.g. fingerprints) is employed for authentication. Figure 5-2 shows the cycle of a username/password pair and Figure 5-3 depicts the login procedure using biometric fingerprints. During a summative e-assessment, the login procedure is initiated when a student requests access to an online test. Thus, at the system prompt, the students are required to provide responses to the "who are you" and "is it really you" challenge questions. The evaluation process validates the identity and authentication responses by comparing the details provided with the stored details. A decision is made at this point and the authenticated students are allowed access to the online test. At this point, the non-authenticated students may be required to re-type their passwords or re-scan their fingerprints to enable access.

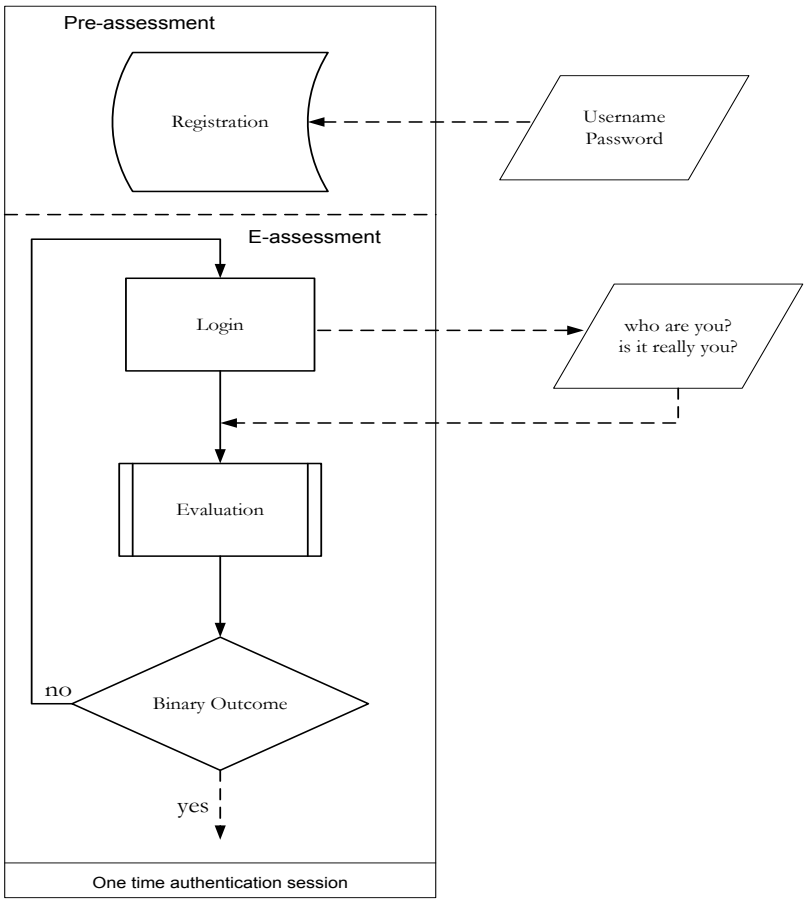


Figure 5-2 Username and password pair

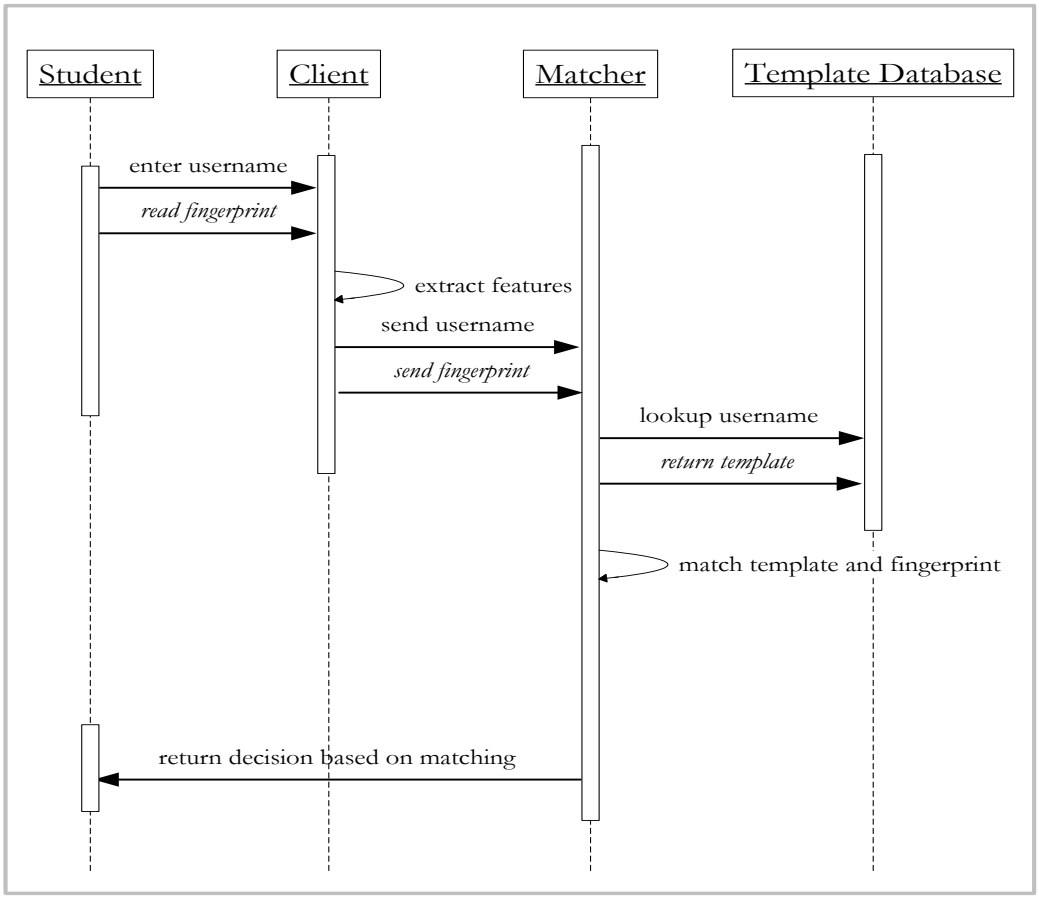


Figure 5-3 Login process via biometrics

5.1.3 A Multi-factor Authentication Method for Biometric Privacy

Biometric authentication poses some non-trivial security challenges because of the inherent features of the biometric data itself. The usable biometric features in humans are limited in number and they must be kept secret. As described in chapter four, biometric systems are gradually replacing the conventional password systems for student authentication. For example, employing biometric fingerprints is becoming a common feature. In summative e-assessments, the fingerprints are considered as an authentication factor; hence, it is essential that the biometric templates are not exposed to potential attacks. Conducting a summative online assessment is a capital intensive task; thus, it is vital to shield the system against security compromises without the additional costs of securing the student's biometrics.

The use of hash functions would be an ideal solution to protect the student's raw biometrics without incurring additional cost. However, a biometric authentication system cannot perform a one-way hash function on the user input (the hash functions are

common to some password systems). This is because the stored hashed template and the input raw biometric would have different hash values (Bhargav-Spantzel *et al,* 2006).Thus, the inability to match the input template with the stored template will lead to unacceptably high false rejection rates (Prabhakar *et al,* 2003).

Hence, in this section an inexpensive method that preserves the privacy of user biometrics in summative e-assessment is described (Apampa *et al,* 2008b). Our work shows that the resilience of a multi-factor authentication system could be improved by combining factors to preserve the privacy of a user's biometric. By using an elastic matching algorithm we construct a digest from the biometric and physical factors. The digest is used in place of the raw biometrics during the authentication phase; thus, the raw biometric is never exposed. One of the benefits of using the digest is its ability for trivial sorting and indexing, making the system scalable. Additionally, by obtaining a digest of the biometric template, it will be computationally infeasible for an attacker to recover the template. In our system, the biometric factors consists of biometric reader and a transformer (software on the client), whilst the physical factor is made up of a token and a portable storage device (smartcard or modified USB storage). Figure 5-4 shows the components of the proposed multi-factor authentication method. The operation of system is simplified into the following steps:

- The biometric reader provides input to the transformer (e.g. an image of the fingerprint). The transformer then provides an invariant digest of the input.
- The physical factor attempts to assert the given identity by means of the security token component. The system relies on the security token component for protection against forgery.
- The storage component could be made public without affecting the security of system as it is used to produce the biometric digest
- The authentication server hosts a lookup table of all biometric digest and their corresponding security tokens.

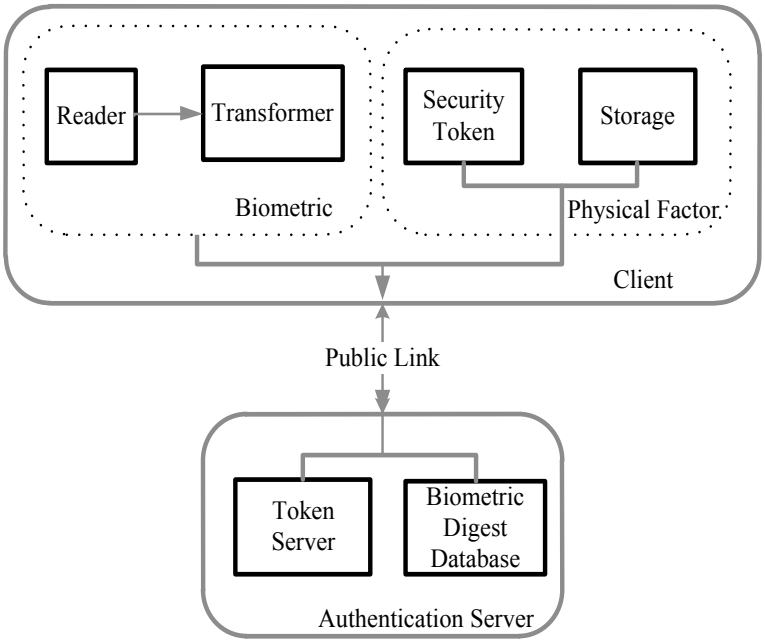


Figure 5-4 Components of a biometric privacy system

5.2 Threat on Identity-Authentication User Security Model

A summative e-assessment system is perceived as secure, when a student satisfies the identity and authentication security goals. In Figure 5-5 the Identity-Authentication (I-A) user security model, is made up of two user security questions and the respective methods that provide responses. It is assumed that each response method (e.g. password is a member of the goal set) contain an individual level of security. Hence an intersection of the goal sets (identity and authentication) is sufficient to ensure the security of the summative e-assessments; this is based on the cumulative security of the response methods. In some e-assessment user security models, a human invigilator may be required to check a photo ID card to ensure the correctness of a student. Thus, the invigilator resides in the e-assessment environment and not included in the goal sets. This is because an invigilator provides an added layer of security alongside the identity and authentication methods.

To a large extent, the overall security of a system depends on its ability to securely allow only correct users access to the system. Therefore, it is essential that the steps to attain user security are carefully designed, as it can easily become a weak point to be exploited. More so, user security is located at the entry point of the system; making it more appealing to intruders. According to Pflegeer & Pfleeger (2003), "*any system is most vulnerable at its weakest point*"; this implies that the harm to a security system can

be linked to a weakness in the procedures, design or implementation of that system. For example, given data stored in a computer system, it is required that the contents should be protected in some way. Thus, the data security system should ensure that data is not disclosed to unauthorised parties, neither should the data be modified in illegitimate ways; however, it is required that the data can be accessed by legitimate users. Based on the example described, it is assumed that the data security system may be susceptible to unauthorised data modification; which could occur due to lack of user identification before allowing data access. Hence, a weakness in the system can be identified as the lack of user identification.

In summative e-assessment, the user security model should ensure that illegal students are restricted from taking an online test. Furthermore, the process should ensure that only correct students are accessing the test for the duration of the assessment.

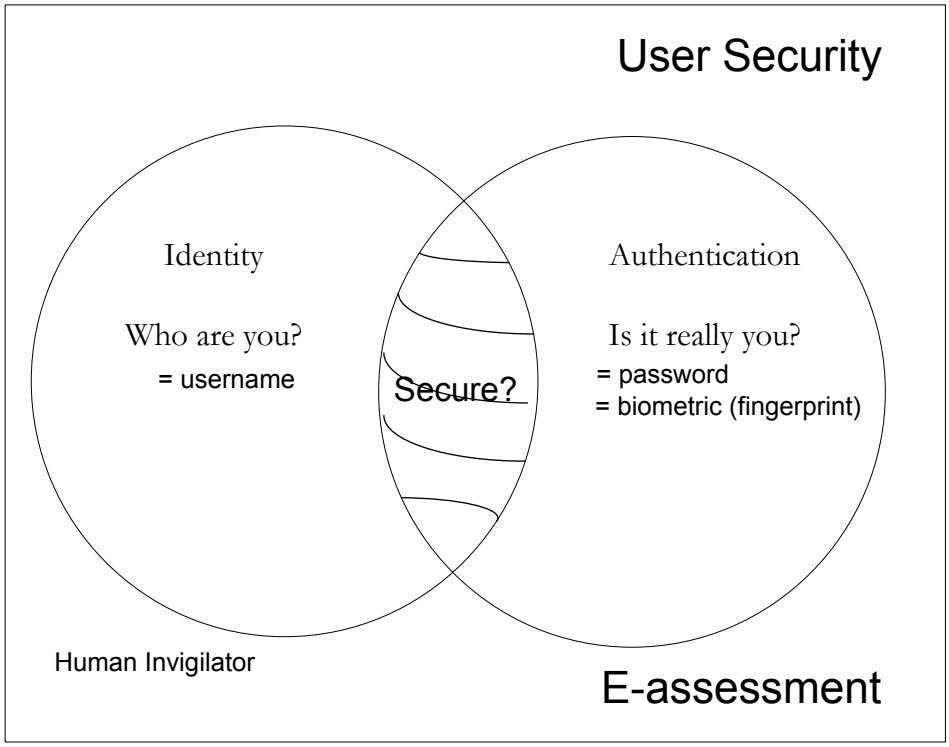


Figure 5-5 Is the I-A user security model secure?

5.3 Background Literature on Impersonation Challenges

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, 2006). In higher education, security

considerations do not feature prominently; however, this changes when an online environment is considered (Furnell *et al,* 1998). Due to the increased influence of technology in assessments, it is often easier to cheat online (Rowe, 2004). Similarly, the results of a recent study by King *et al,* (2009), suggests that 73.6% of the students (in the sample population) held the perception that it is easier to cheat in an online course compared to its traditional counterpart. Thus, there exists an increased risk of academic fraud in online assessments versus the traditional assessments. The higher educational sector has constantly focused on plagiarism as a major academic misconduct (Naude & Horne, 2006) and there exists an extensive knowledge of plagiarism detectors to curb plagiarism (McLafferty & Foust, 2004). However, other dishonest acts in online assessments have gained little attention.

In generic (non-assessments) online environments, one of the major security challenges to user security is the act of impersonation. Impersonation is a fraudulent action with the aim of imitating a legitimate user and defrauding the security system. For example, in online banking, customers refrain from divulging their assigned login details to prevent others from accessing their bank account. However, there is a possibility that the customer's login details can be stolen, eavesdropped or hijacked without the knowledge of the customer. Thus, when a service is requested, the system grants access to the impersonator believing the details presented originates from the customer. In an approach to minimise impersonation in online environments, the banking industry invest in a second layer of protection to ensure risks are minimised (Bailie & Jortberg, 2009).

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 (Kerka & Wonacott, 2000). Weippl (2005) asserts that, students who want to cheat willingly reveal their login details to another person for the purpose of impersonation. Hence, this shows a striking departure from other online environments (e.g. e-banking) where people will not knowingly cooperate with someone who tries to steal money out of their bank account (Weippl, 2005). According to Stoner (1996), a student cannot 'accidentally' impersonate another during an online assessment. In traditional (pen and paper) exams, the need to correctly identify a student is well understood and the requirement is to produce a student ID card which includes a photograph. The traditional approach of using a photo ID card and matching it with a student's login details in online environments is generally

adopted (Vollans, 2008). This approach provides an added security layer, whereby a human invigilator ensures the correctness of the student taking the test.

5.4 Summary

The user security model of a summative e-assessment ensures that only the correct student takes the summative test. Thus, a summative e-assessment user security model poses two challenge questions to a student, i.e. 'who are you?' and 'is it really you?' The 'who are you?' question is posed to solicit a response to student's identity, whilst the 'is it really you?' question solicits a response to confirm the claimed identity. A commonly used response is the combination of a username and password. Another example of a response is a username and a biometric fingerprint. It is important to note that, adopting biometrics for authentication simultaneously requires that the raw biometrics data is never exposed during the matching process. Hence, in this chapter an inexpensive multifactor authentication method was introduced to preserve the biometric data. This method constructs and stores a digest of the biometric template using an elastic matching algorithm. Thus, during the matching process the digest is used in place of the raw biometrics.

The Identity-Authentication user security model is simple, easy-to-use and provides a satisfactory level of security for the e-assessment environment. To a large extent, the overall security of a system depends on its ability to securely allow only correct users access to the system. Therefore, it is essential that the user security model is designed to resist security challenges. In summative e-assessment, the security model should ensure that only correct students are accessing the test for the duration of the assessment and without any external assistance. However, the Identity-Authentication user security model is fallible to security threats that are ignited through user fraudulent actions, e.g. impersonation. The susceptibility of the Identity-Authentication user security model to impersonation challenges questions the ability of the model to sufficiently ensure and maintain security during summative e-assessments. The I-A model represents a typical user security model adopted for summative e-assessments; however, the inability of the model to resist impersonation threats presents a gap in e-assessment security. The next chapter provides a detailed overview of the impersonation challenges in the I-A user security model and a novel solution is proposed.

Chapter 6. Presence-Identity-Authentication (P-I-A) User Security Model

In chapter five, an overview of the Identity-Authentication (I-A) user security model was discussed; however, the model is susceptible to impersonation challenges which are a major concern in summative e-assessments. In this chapter, a further exploration of the impersonation challenges and its influences on the I-A user security model is presented. Hence, to address the shortcomings of the I-A model; assets, threats and security goals specific to e-assessment user security are identified. Furthermore, the Presence-Identity-Authentication (P-I-A) user security model is presented as an improvement of the I-A user security model. Overall, this chapter fulfils the intent of the first research goal stated in chapter one.

6.1 Types of Impersonation threats

In this section the impersonation challenges introduced in section 5.3 are classified into three types, namely Type A, B and C impersonation threats. The impersonation threats described below reflect a supervised online test environment. A scenario-based method is used for illustration.

6.1.1 Type A impersonation Threat

A tutor/invigilator is assumed trustworthy for the purpose of the online test; however, there exists the possibility of a connived impersonation (a.k.a. Type A impersonation threat). A connived impersonation is the ability of an invigilator to collude with fraudulent students to allow the fraudulent act. A connived impersonation

may originate from a sympathetic feeling towards the student and it should not be overlooked especially when the assessment counts towards a student's degree or qualification. For example, if a student has continually failed a certain test, the tutor/invigilator may respond to human emotions and allow another student take the online test on behalf of the initial student. This type of impersonation can easily go undetected. A successful connived impersonation hinders a fair assessment and it extenuates the reliability of the test (Heinrich *et al,* 2009). Additionally, there is a possibility of a connived impersonation for monetary purposes. In this situation, the fraudulent students can influence the invigilator to receiving a large sum of money to help perpetrate the act. Irrespective of the motives for a connived impersonation, it is essential to find methods to minimise such threats in a summative e-assessment system. This thesis does not eliminate totally the use of a human invigilator; however, measures should be taken to ensure that the correctness of a student is independent of an invigilator.

6.1.2 Type B Impersonation Threat

The following example introduces a scenario which will be used to illustrate the Type B impersonation threat. This impersonation threat poses the question "is the student really who they say they are?"

Example 1: Consider that Alice has initially registered for the COMP101 online test. Thus, Alice has an account on the e-assessment system which includes a user profile. Alice's user profile on the database includes her name, date of birth, year of study, registered courses and login details. The online test is scheduled to commence at 10am for the duration of 60mins in the departments' computer laboratory. At 10am on the assessment day, Eva walks into the test room with the knowledge of Alice's login details and other information required. Eva satisfies the identity and authentication goals by inputting Alice's login details. The online security system believes that Alice has requested to gain access to the online test; as a result of a match between the stored login details and the login details presented. However, the security system is oblivious to the swap between Alice and Eva; hence, Eva is not really who she claims to be for the purpose of the online test.

In the scenario illustrated above, it is directly observed that Alice is absent for the online test; however, Eva has the ability to produce Alice's login details when requested

by the security system. In order to analyse the scenario, the identity and authentication paradigms in chapter five are recalled. A username and password is classified under the knowledge methods in which a user has; thus, it can be easily shared amongst users. This academic misconduct can be undetected, especially when the requirement for accessing an online test is a student's username and password alone. However, in past and recent times employing the username and password alone has proven to be the most convenient and popular method in the e-assessment (Oorschot & Thorpe, 2008). In exploiting this weakness, students can perpetrate a Type B impersonation threat by not showing up for the test; but sharing their details with another student (see example scenario). It can be argued that, using a tutor/invigilator can curb a Type B impersonation; however, a Type A threat readily comes into mind. By employing a tutor/invigilator in the scenario above, the occurrence of a connived impersonation cannot be totally eliminated. Additionally, a tutor/invigilator can be tricked when the student's password details is shared with the student's look-alike, e.g. identical twins.

In order to minimise a Type B impersonation threat it is observed that the problem is peculiar to the *strength of the authentication method*. Employing a username and password paradigm for an online test makes a Type B threat more appealing to impersonators. It is observed that due to the inherent attributes of a password scheme (shareable), it is unable to resist an impersonation threat. In addition, a student's access is authenticated once at the login for the duration of the test session; however, the repeated authentication is performed based on the password cached in the browser (Levy & Ramim, 2007). Hence, a method which would increase the difficulty of responses solicited by the security system is required.

Authentication	Registration	Login	Evaluation	Implication
Password	Alice	Eva	Eva	Impersonation

Table 6-1 Type B Impersonation: password

6.1.3 Type C Impersonation Threat

In a continuing description from the example above, example 2 illustrates a scenario to depict one approach that can be employed to minimise the Type B impersonation threat. However, the solution presents a potential security challenge which

is explained in example 3. Thus, the Type C impersonation threat poses the question "who is there?"

Example 2: Consider that a biometric fingerprint authentication method is employed for a student login; thus Alice is required to scan her fingerprint on a capture device and await a positive confirmation before continuing with the online test. This implies that Alice needs to be present to carry out the login procedure.

In summative e-assessment, a biometric fingerprint authentication method is suggested as the ultimate solution to minimise a Type B impersonation threat (Hugl, 2005). An advantage of a biometric scheme as opposed to a password scheme is its non-shareable attributes. Using the scenario above and given a biometric fingerprint method for login, it is impossible for Alice to provide Eva with a finger to gain access to the test. This implies that, during enrolment Alice has enrolled her fingerprint and a template is stored in the database alongside her user profile. Thus, access to the online test can only be granted when there is a match between the raw biometric fingerprint presented and the stored template. The use of biometric fingerprint method for authentication is gradually becoming popular in summative e-assessments (Levy & Ramim, 2007). It is suggested that adopting this method will deter the impersonators and the impersonated students from the act. Hence, using a biometric method, Alice will be obliged to take the online test herself instead of employing Eva.

Authentication	Registration	Login	Evaluation	Implication
Fingerprint	Alice	Alice	Alice	Correct representation

Table 6-2 Type B Impersonation: fingerprint

Example 3: It is assumed that Alice, successfully gains access to the online test; hence, the security system believes that Alice has initiated the request due to a match between the scanned fingerprint and the stored template. At a certain time t during the duration time T of the online test, Eva takes over Alice's test. However, at these particular times the security system is unaware of the academic misconduct; hence Eva is the one there instead of Alice.

In example 3 above, it is observed that there is an increase in the difficulty of the authentication challenge; thus, Alice's physical presence is required to carry out the login procedure. Additionally, it is observed that there exists a possibility for Eva to take over

Alice's test after the login procedure. Hence, the responsibility of the e-assessment user security does not terminate at ensuring the correctness of the student; rather, it extends to verifying that the correct student is there taking the test for the period of time. As pointed out in recent researches (Wisher *et al*, 2005; Aojula *et al,* 2006; Levy & Ramim, 2007; Hernandez *et al,* 2008), a major problem when conducting summative e-assessments is the inability to know who is there taking the exam i.e. to know if the correct student is there taking the exam or someone else has taken over the test on their behalf.

6.2 Assets, Threats and Security Goals

One aim of this research is to investigate the sufficiency of the Identity-Authentication user security model in ensuring that only correct students take an online test for the allocated duration of the test. Based on a qualitative review of existing literature on e-assessment user security, it is observed that impersonation threats are a major challenge in summative e-assessment systems (Aojula *et al,* 2006; Hernandez *et al,* 2008). The existing user security model requires that a student identity and authentication goals only are satisfied prior to accessing the online test; thus, this implies that the student accessing the test is the correct student. However, in this thesis it is suggested that the authenticated student is sometimes not the expected student or the expected student begins a test but does not complete it. Hence, it is concluded that the existing Identity-Authentication e-assessment user security model is insufficient to ensure that only the correct students take an online test for the allocated duration of the test (see Figure 6-1).

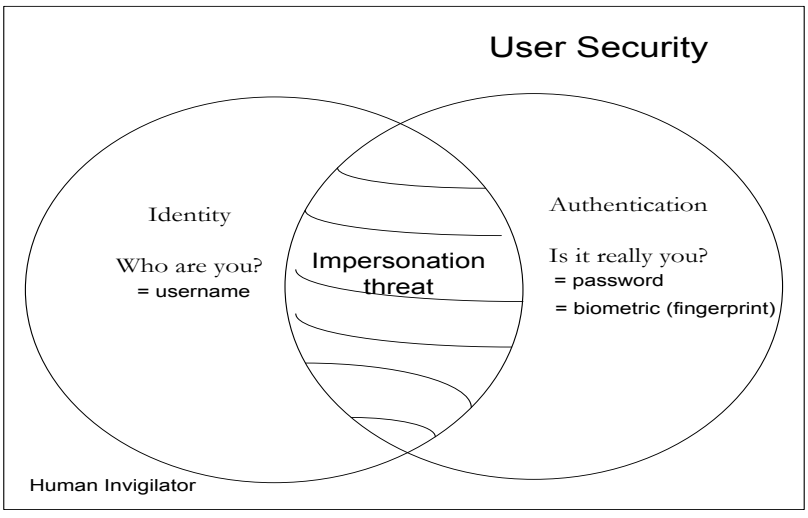


Figure 6-1 Impersonation in I-A user security model

In an attempt to address this issue, this thesis suggests that satisfying the identity and authentication security goals only is not enough to assure user security during summative e-assessments. Much more is required to ensure that the authenticated student is the expected student and that the correctly authenticated student is taking the online test un-assisted for the duration of the test time. Thus, there is a need for an improved e-assessment user security model which is sufficient to ensure that only the correct students take an online test for the allocated duration of the test. Thus, it is proposed that one of the ways to ensure correct user security during online tests is to combine the presence goals with the existing identity and authentication security goals. This implies that a student will be required to satisfy the presence (P), identity (I) and authentication (A) security goals prior to and during the online tests.

Finally, a goal-oriented approach is adopted to propose a summative e-assessment asset, security threats and security goals.

6.2.1 E-Assessment Security Assets

An asset refers to something that is valuable which needs to be protected (ISO/IEC, 2005) and this suggests that the valuable assets of a summative e-assessment system extend beyond the hardware, software and data needs. It should be noted that the importance of the above computer assets are not discarded; however, assets specific to user security are considered. In chapter two, a constructivists' perspective of e-learning was discussed. In a constructivist's mind, the student plays the centre role in the learning process; hence, they need to be correctly assessed and securely authenticated in the e-assessment environment. In addition, a summative e-assessment system is perceived busy when delivering an online test and a student taking a test signifies the occurrence of an activity on the system. Thus, it may be pointless to develop an online summative assessment system if the students' participation is excluded. A student taking a test is an indispensable component of the e-assessment system; hence, it is proposed that a *student* is a valuable asset of the e-assessment user security (Apampa *et al,* 2009a).

6.2.2 E-assessment Security Threats

A threat is the potential for misuse/abuse of an asset that will cause harm in the context of the system (Haley *et al,* 2004). The level of harm that can occur depends on the asset type; thus, it is appropriate to identify the relevant threats that may apply to each asset type. For example, the storage of assessment data in a university may be under

threats from unauthorised exposure and unauthorised alteration. A major threat to the summative e-assessment user security process is the threat of impersonation. As described in section 6.1.1, the Type A impersonation threat can be minimised by ensuring that the correctness of a student is independent of an invigilator; similarly, the Type B impersonation threat is overcome by employing a strong authentication method. However, it is noted that a Type C impersonation threat presents a greater security challenge than its counterparts.

One aim of the Type C impersonation threat is to subtly permit an incorrect student to take an online test on behalf of the correct student. Thus, a successful impersonation (threat) launched on a student (asset) will reduce the credibility of the online test (harm) in an e-assessment context. Hence, the security system is required to set security goals which can be used to protect the students from impersonation threats. Simultaneously, the e-assessment system is also secure from the fraudulent act. In the C-I-A security model (see section 4.2), the interception threat is an attack on confidentiality; the modification threat is an attack on integrity and the interruption threat attacks availability. Similarly, the threat of unauthorised exposure is converted to the goal of protection from unauthorised exposure, commonly known as confidentiality (Haley *et al,* 2006). Hence, the threat of impersonation is converted to the goal of protection from impersonation, known as presence, i.e. an impersonation threat is an attack on presence. It is concluded that the exclusion of the presence security goal in online summative tests will increase impersonation threats in e-assessment user security.

6.2.3 E-assessment Security Goals

A goal is something people interpret differently depending on the nature of job they are doing. For example, a goal would mean different things to a footballer, psychologist, engineer etc. In general, a goal expresses what is desired. It can also refer to a specific, measureable occurrence that any business or system plans or intends to achieve or avoid. According to Haley *et al*, (2008) security goals are presented in form of a desire and they aim to protect the assets from harm (threats). In computer system security, the confidentiality, integrity and availability security goals ensure that the hardware, software and data assets of a system are not compromised (see section 4.2). This implies that a compromise in the C-I-A security goals may lead to a compromise of the critical assets.

During a summative e-assessment, the C-I-A security goals can be employed to protect the e-assessment system's hardware (PC), software (assessment application) and data (item bank) from potential interception, modification, interruption and fabrication threats. However, it is proposed that the C-I-A security goals are unsuitable to protect the e-assessment security asset from its potential threat (Apampa *et al*, 2009b). In generic computer security, the people who use or maintain particular applications on a computing system are examples of the valuable assets to the organisational system (Pfleeger & Pfleeger, 2003). These key people are carefully selected because of their skills and potential value to the organisation. For example, a problem would occur if one of the key people decides to leave the organisation (taking away the knowledge) and no other person can fill the position. Based on this description, it is observed that the key people do not depend directly on the C-I-A security goals; instead they would be required to satisfy other goals, e.g. trustworthiness. Hence, it is suggested that the C-I-A security goals are not entirely suited for human assets due to their unpredictable attributes.

In another perspective, it is impractical for a student to satisfy the C-I-A security goals. For example in computer security systems, it is commonplace to apply the C-I-A goals to the data asset; thus, producing data confidentiality, data integrity and data availability. In particular, confidentiality protects the data item from interception, integrity protects from modification and availability protects from interruption. However, applying the C-I-A goals to the student (asset) produces student confidentiality, student integrity and student availability. These terms are defined respectively: student confidentiality refers to privacy of a student's personal information, health records or educational records, which an institution is not required to disclose without prior consent of the student. Student integrity describes an honourable and ethical conduct which is expected from every student during an online test. The student integrity can be written as a set of policies and sanctions relating to the student's academic conduct during an assessment. Finally, student availability requires that the student is there when needed to take an online test. This thesis does not disregard the importance of the C-I-A security goals; however, security goals specific to e-assessment user security is defined. Hence three security goals of a summative e-assessment user security are proposed (see Figure 6-2)

Presence:

This reflects a state of a student being at a specific space or place. Only correct and legal students are required to be present for an online test. Continuous authenticated presence ensures that only correctly authenticated students are continually present (from start to finish) for the duration of the test and taking the test un-assisted.

Identity:

This is a distinct attribute which differentiates a student from other students in a given population (e.g. a student's username in a database)

Authentication:

This provides a proof of the identity claimed by a student.

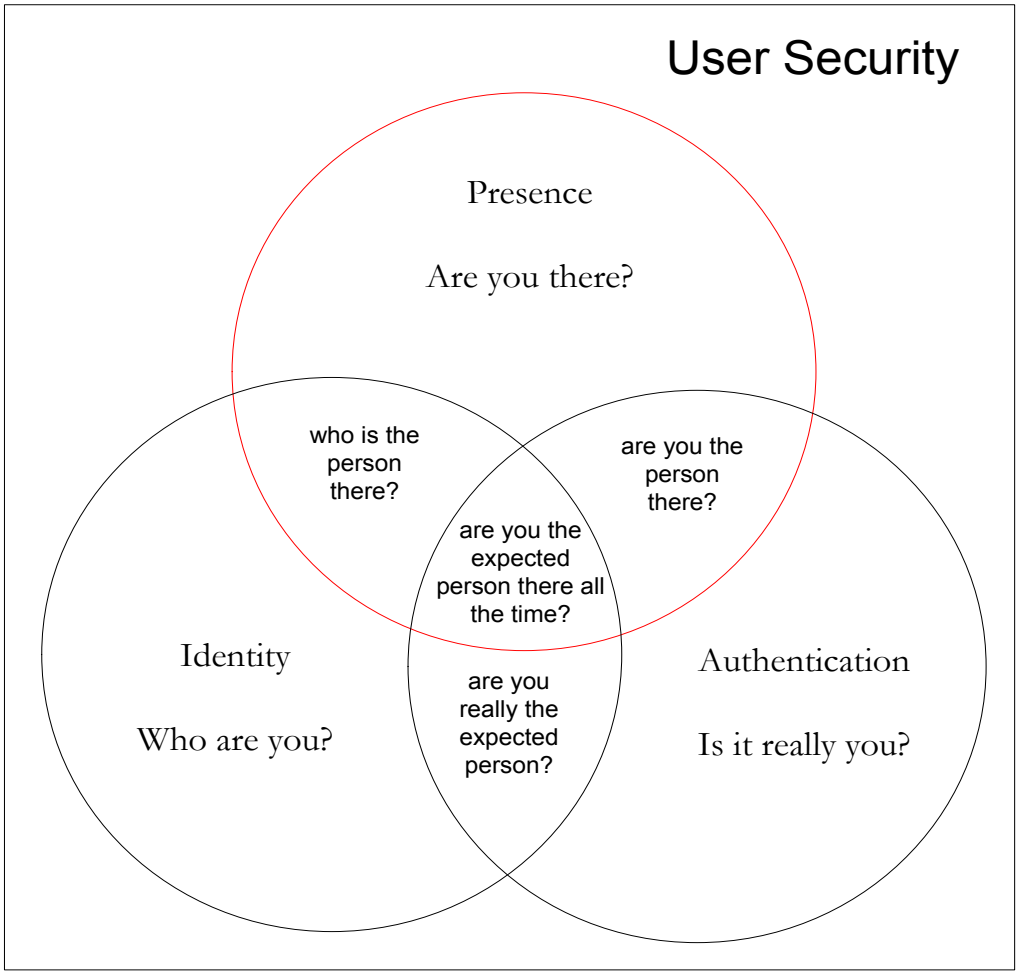


Figure 6-2 Relationship between Presence, Identity and Authentication

6.3 Presence, Identity and Authentication (P-I-A) Security Goals

As discussed in chapter five the existing user security model is made up of the identity and authentication security goals only. The easiest technique employed to fulfil the requirements of security goals is the username and password. The model is simple, easy to use and expected to provide the robust security for summative e-assessments. However, as shown in section 6.1, the e-assessment user security model is fallible to impersonation threats. Initially, this vulnerability can be traced to the strength of the authentication methods adopted. Hence, a review of the password authentication method translates to a Type B impersonation threat. Additionally, a human invigilator is an example of a secondary authentication method which can be used to ensure correct student authentication. Nevertheless, student authentication that is dependent on a human invigilator is susceptible to a connived impersonation threat a.k.a. Type A impersonation.

Thus, in a bid to eliminate the aforementioned impersonation threat types, the biometric technology is perceived as an ultimate solution. Employing biometrics as an authentication method can improve the user security model by ensuring the authentication of only the 'right' students. However, this solution introduces a third type of vulnerability i.e. the Type C impersonation threat. One of the theoretical propositions made in this thesis suggests that, *the fallibility of the Identity-Authentication user security model to impersonation threats is as a result of a flaw in the model itself; rather than the authentication methods adopted.* This implies that, irrespective of the authentication method applied, either a single biometric or multiple biometrics, there exist a probability to perpetrate a Type C impersonation threat.

In this thesis, it is proposed that one of the solutions to improve the I-A user security model is the ability to fulfil the presence security goal along with the identity and authentication security goals. The presence security goal ensures that, an authenticated student at the start of a test is the same student at the end of the test and has taken the test without external assistance. Thus, integrating the presence security goal ensures the presence of the correct student beyond the initial login; however, it is suggested that the exclusion of presence verification will increase impersonation challenges.

6.4 Potential Approaches to Presence Verification

Traditionally, authentication systems are required to verify a claimed identity only one time at the initial login or sign-on. This process is secure for one-time applications such as accessing a protected file. However, in highly sensitive environments e.g. an e-assessment environment, a one-time authentication session is insufficient to guarantee security (Sim *et al,* 2007). Hence, the security of online summative assessments goes beyond ensuring that the 'right' student is authenticated at the initial login. More is required to ensure that the same authenticated student is present throughout the test session. Thus, in section 6.2.3 the presence security goal (hereafter known as *presence verification*) aims to ensure the presence of a correctly authenticated student for the duration of the online test.

The high-stake nature of a summative e-assessment is perceived to attract impersonation threats to the environment. Hence, there is a need to verify the presence of an authenticated student beyond the initial presence verification. This section explores the potential approaches to realising presence verification in an e-assessment environment. Table 6-3 shows a summary of advantages and disadvantages of existing methods.

6.4.1 Face-to-Face Monitoring

The approach refers to a physical supervision of the e-assessment environment, whilst the participants (i.e. students and invigilators) are within each other's presence.

6.4.1.1 Human Invigilation

In summative e-assessment environments, an invigilator/proctor is required to provide extra security alongside the identity and authentication goals. One of the major goals of an invigilator is to supervise or monitor the activities occurring in a test environment. The advocates of human invigilators in online environments, (Cizek, 1999; Rowe, 2004) describe the method as a low technology means of promoting both identity and academic honesty. Thus, by employing the invigilation technique, security is enhanced and the student's presence is correctly verified throughout the test session.

However, using an invigilation only technique in a test environment exposes the possibility of a connived impersonation, a.k.a. Type A impersonation threat (see section 6.1.2). A connived impersonation refers to a fraudulent act where the invigilator

willingly colludes with students to perpetrate an impersonation. Thus, a connived impersonation can expose the e-assessment system to other types of impersonation threats. A connived impersonation may occur for monetary purposes or feeling of sympathy towards the student; hence, its likelihood should not be overlooked. This thesis 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.

6.4.2 Continuous User Authentication

In this approach, a user in the e-assessment environment is verified continuously for the duration of the test via an authentication method. Usually, the authentication method used during the initial login procedure is adopted for the continuous process.

6.4.2.1 Knowledge-based Solutions

A low-cost method for achieving presence verification is the use of knowledge-based authentication solutions. An example is the password authentication method which is simple and easy-to-use. However, adopting passwords for presence verification promotes the chances of impersonation threats, due to its shareable attributes. This means that, a student can make available their passwords to another student for dishonest purposes. Employing a password to verify presence throughout test requires that the student continuously re-types his/her password following a fixed or random pattern. For example, a student may be required to re-type the password every 10minutes within a 60-minute test session. Hence, the student's concentration will be diverted from the test task at six different times during the test. This method is perceived to be inconveniencing and distracting to the student's concentration.

6.4.2.2 Unimodal Biometric Solutions (active)

An alternative to conventional password based methods is the biometric solutions. In summative e-assessments, biometric solutions such as fingerprint and face recognition methods are suggested to enhance security (Agulla *et al,* 2008). Thus, it is expected that only correct students can perform a successful login, due to the unique attributes of a biometric. In biometric technology, the biometric traits can be categorised based on their data acquisition techniques i.e. active and passive biometrics (Jain *et al,* 2004). Active biometrics requires a level of user involvement during the authentication process; whilst passive biometrics does not require the user's active participation.

The fingerprint is one of the most accepted biometric methods in e-assessments; however, it is requires the user's active participation during the authentication process. This implies that, for presence verification a continuous re-scan of the student's fingerprint throughout the test session is required. For example, a student may be required to re-scan the fingerprint every 10minutes within a 60-minute test session. Hence, the student's concentration will be diverted from the test task at six different times during the test. Additionally, the use of biometric data is not always accurate, such that the threshold for authentication may produce a false reject (Klosterman & Ganger, 2000). This can be due to the variation in placing a finger on a scanner surface. Using the example above, a student may be required to re-authenticate for the fifth time during the test and suddenly the fingerprint scanner rejects the fingerprint due to errors. At this point, the student's test is disrupted, since the re-authentication process is unsuccessful. Thus, this method is perceived *interruptive* and distracting to the student's concentration. In the context of this thesis, the term 'interruptive' refers to the ability of an event to interfere with and alter a sequence of normal activities.

6.4.2.3 Unimodal Biometric Solutions (passive)

In biometric systems, adopting passive biometrics is desirable to achieve continuous authentication. This means that the biometric employed should not require active user participation and be unlikely to interrupt the user's activities. The face recognition is an example of a passive biometric method that can be used for continuous authentication. An example of a continuous video-based face recognition method to enhance user authentication in desktop systems is presented in Klosterman & Ganger (2000). In their work, authenticated faces are tracked and authentication is performed periodically for active consoles. The face tracking process exploits the temporal correspondence between the observed faces in the different frames i.e. detecting and tracking the faces over time. Subsequently, the tracked faces are authenticated for the entire video sequence. In summative e-assessments, employing the face biometric method will enhance security and deter potential impersonators. Additionally, in e-assessment security, face recognition is perceived non-interruptive as it possesses non-intrusive capabilities. Thus, the student's face image is continuously authenticated to verify presence throughout the test session.

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 their work, Klosterman & Ganger (2000) reports the high computational costs of performing the biometric evaluation algorithms; thus, their proposed system was implemented in two separate systems. Xiao and Yang (2009) proposed a facial presence monitoring system to monitor an authenticated user. An objective of their system is to lock the screen or log out a user when the authenticated user's face disappears from visibility. The CAMSHIFT algorithm was used to perform face tracking. However, during face authentication processing the system skipped a number of frames to save computational resources. In a one-time authentication, the computation latency would not be a concern; however, this becomes a challenge during presence verification. In e-assessment environments, rendering of test questions with minimum delay is essential; thus, overloading the processor with high computational tasks may be unrealistic. Thus, the literature suggests that continuously authenticating a student's face for the test duration will be impractical and expensive.

Additionally, one of the prominent problems encountered in face recognition technology, is the difficulties in handling varying poses i.e. intolerance to pose variations (Zhang & Gao, 2009). According to Blanz *et al,* (2005), most face recognition systems are optimised for frontal views only and their performance drops due to non-frontal pose from the input image. This implies that, when a subject does not look directly at the camera, a user authentication attempt may fail. In a continuous face authentication experiment, Altinok & Turk (2003) reports that a non-frontal pose throughout the entire video sequence led to a poor face recognition rate. Hence, the selection of frames which contain frontal face images is important for successful face authentication.

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. As suggested in Cass & Riezenman (2002), a face recognition system with a low pose tolerance level is perceived to require cooperative subjects. Thus, an increase in pose variations, leading to non-frontal poses

will result in false re-authentication alarms which may be costly in test environments. In our context, the high sensitivity of the face recognition method will make it interruptive and distracting for verifying presence. There exist promising techniques to achieve pose invariance (Xu *et al,* 2007); however, this thesis is not focused on pose detection in face recognition. Additionally, the pose invariance techniques will be an expensive overhead in summative e-assessment environments.

Other passive biometric methods proposed in e-assessments include the keystroke analysis (Asha & Chellappan, 2008) and mouse dynamics (Ahmed & Traore, 2007); however, as behavioural biometric traits they are yet to find their way into commercial use (Levy & Ramim, 2007). Thus, the use of keystroke and mouse dynamics for presence verification is a potential research area.

6.4.2.4 Multimodal Biometric Solutions

Multimodal biometrics is the integration of two or more biometric methods (Jain *et al,* 2004). A recent trend in biometric technology is the adoption of multi-biometrics to enhance security in applications. Continuous authentication using multimodal biometrics has been explored using face with fingerprint (Sim *et al,* 2007) and the combination of voice, face and fingerprint (Altinok & Turk, 2003). Sim *et al,* 2007, experimented with using a face and fingerprint biometrics to continuously verify the presence of an authenticated user. They used a Hidden Markov Model (HMM) in Bayesian framework to form a holistic fusion method for combining the biometric modalities and time synchronously. Their system was integrated into an operating system, to allow the operating system take action on the presence/absence of a legitimate user.

In e-assessments, Rabuzin *et al,* (2006) suggest that to implement absolute security, it is essential to combine different biometric traits. However, multimodal biometrics is new to e-assessment; and there exist few proposals in adopting the concept. Levy & Ramim, (2009) propose a model for the integration of 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. Another multi-biometric approach worth mentioning is the use of a mouse embedded with a fingerprint sensor (Levy & Ramim, 2007). In this method, the sensor is located on the thumb area to continuously monitor a student over time without interfering with the activities of the student. Adopting multi-biometric solutions in an e-assessment

environment will improve user security, beyond the initial login procedure. However, a multi-biometric solution is as effective as the individual biometrics integrated. Thus, a multi-biometric system employed to verify presence may be reduced to an interruptive and distracting solution. In addition, continuous authentication of the multi-biometric traits will incur a high computational cost.

6.4.3 Continuous User Monitoring

In this approach, a test environment is continuously monitored whilst the participants (i.e. students and invigilators) are not necessarily within each other's presence.

6.4.3.1 Video/Webcam Solutions

The aim of continuous user monitoring is to ensure the presence of a user both in time and space, without any form of interruption. This solution monitors user activities by recording the visual and audible signals in the environment. A typical example is the use of video cameras for surveillance applications (Au *et al,* 2006).

In e-assessment environments, Lin *et al,* (2004) suggested that the monitoring of student's interaction via video images is a promising approach to ensure security in online tests. Thus, Ko & Cheng (2004) propose a secure internet examination system based on random video monitoring. In their work, passwords were used as a method for authentication; whilst monitoring involved the random capture and transmission of a student's face during the test. An initial limitation of their system is the use of passwords which can be easily compromised. Secondly, a human invigilator is required to perform a manual monitoring process by watching a video of the environment throughout the test session. 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. A workaround to minimising cost, is to record the activities in the test environment, such that the video can be viewed at a later time. This solution will gradually become overwhelming and an administrative overhead, due to the amount of data watched. Additionally, invigilators are human beings and watching a video for a long period will be prone to errors. This may be due to fatigue and distraction; thus, there is a chance of

'missing' certain events. There is also a possibility of connived impersonation, as presence verification partly depends on the invigilator.

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. A webcam (miniature video camera) is an inexpensive device that is used to visually monitor an area and capture video images which can be viewed or stored. The miniature size of the webcam is useful in test environments as it can be mounted or in-built on a PC or laptop. However, the solution shares the limitations associated with using video monitoring. Hence, it is concluded that whilst these solutions are useful for user monitoring, they are unsuitable for presence verification.

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

Table 6-3 Advantages and disadvantages of existing methods

6.5 A Conceptual Architecture for Presence Verification

From Table 6-3 it is observed that a connived impersonation is possible when presence verification is completely reliant on a human invigilator. A user password can be easily compromised and it possesses 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! Adopting biometric solutions have a potential to become interruptive and distracting when a re-authentication process is initiated constantly. Additionally, the biometric solutions can become frustrating when presumptuous re-authentication requests are constantly initiated. This type of request may be triggered due to the high sensitivity of a biometric identifier to the environment e.g. face biometrics. For example, a face recognition process can become over-sensitive to the activities in the test environment; this may lead to constant presumptuous re-authentication requests which can ruin a student's test. In addition, it is computationally expensive to perform biometric authentication constantly in a summative e-assessment environment. Lastly, the video/webcam solutions would still depend on human resources to verify presence.

The discussion above emphasises on the disadvantages of the potential approaches; nevertheless, these solutions also possess benefits that are useful to the test environment. From Table 6-3 (see page 76), it is observed that one of the important advantages to the test environment is the deterrence of potential impersonators at the login phase. Recall in the earlier chapters, biometrics solutions have been described as a stronger authentication method which can be used to preserve the user security of summative e-assessments. Thus, the goal of the e-assessment user security is to ensure that the 'right' student is correctly authenticated at the initial login and that the student's presence is accurately verified for the duration of the test. Hence, this research does not disregard the relevance of the biometric solutions in summative e-assessments; rather a solution to achieve the presence verification process is proposed.

Figure 6-3 shows a conceptual design of the proposed presence verification system, where the biometric solutions are included for (re)authentication purposes. From the high-level diagram, it is observed that the first step in a summative e-assessment environment is to ensure correctness of the student via an authentication method. In this case, a fingerprint biometric authentication system is employed. Therefore, provided a

successful authentication outcome is achieved the student is allowed to proceed with the test and the presence verification module is initialised. The novelty of this research is embedded in the presence verification module; this module will be discussed in later chapters. However, a potential (futuristic) operation of the biometric authentication systems and the presence verification module within a test environment is briefly described.

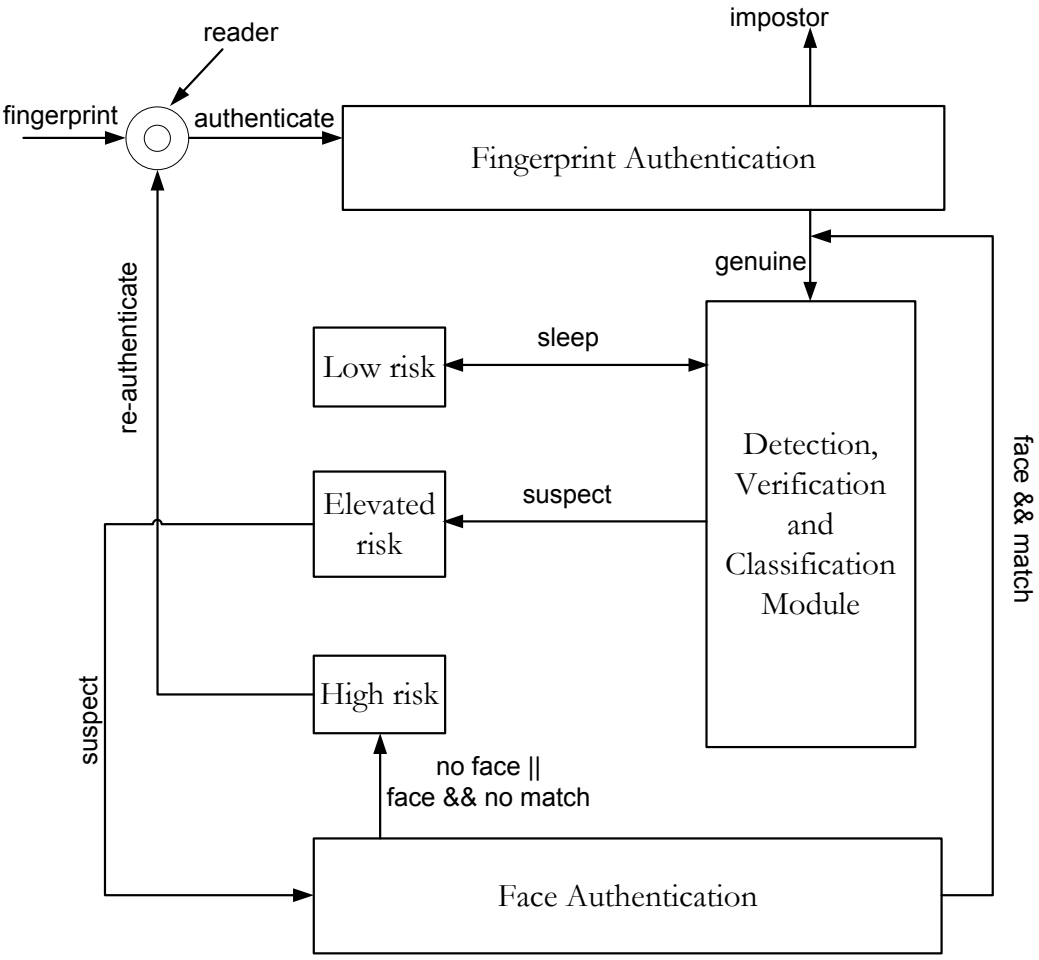


Figure 6-3 High-level design of a presence verification system

For the purpose of this description, a genuine student is assumed and the monitoring process is initiated. It is suggested that at a low-risk state, the student's presence does not pose any risk to the test environment; thus, the monitoring process is continued in a loop and no biometric processing is required. At the elevated-risk state, the student's presence becomes suspicious in the test environment; thus, a reclassification process is initiated to re-assign the student's presence to a low-risk or a high-risk state. In this process, the biometric face authenticator is required to re-confirm

a student's face within a specified time in a non-interruptive fashion. A high-risk state occurs when a student's presence poses a significant risk to the test environment. Additionally, a high-risk class can be assigned during the reclassification when a student's face is not detected within the specified time or a face cannot be re-confirmed. Hence, at this stage the student would be required to re-authenticate. It should be noted that, until the high-risk state is assigned, the student would be oblivious to the presence verification process.

As explained, the brief description provided above is a futuristic operation of the proposed presence verification system; however, the components of the presence verification module (detect, verify, classify and risk states) are investigated and demonstrated in later chapters. In the next section a novel non-biometric presence verification solution is described.

6.6 Object Tracking Approach: A Blob Analysis Solution

This section proposes a novel blob analysis solution which follows an object tracking approach. In this method, significant blob statistics from the detected object are extracted and the blob statistics information is analysed. Thus, the analysis of the blobs can be used to track an object, detect the object's presence and estimate the object's activity in the video sequence. In this context, an *activity* is described as acceptable or unacceptable incidents which occur in a video sequence. For example, in a test environment, the presence of an object is acceptable whilst the absence of the same object is unacceptable. The motivation for acceptable and unacceptable activities will be discussed in the next chapters. Hence, one of the goals of this research is to investigate the feasibility of using geometric blob statistics to detect a variety of activities in a summative e-assessment environment. To accomplish this, a blob analysis operation will be used to detect the blobs and extract the significant blob statistics such as perimeter, diameter, area and centre of mass.

Furthermore, the extracted blob statistics values will be calculated and classified into three output threat classes to infer the student's presence in the test environment. As will be discussed in the next section, existing blob analysis applications exploit blob statistics for object tracking and people or vehicle counting purposes. Additionally, the blob statistics can also be used for classification purposes, such that the goal is to classify the moving object into single person, people group or a vehicle. In literature,

classification algorithms employed for blob analysis applications include: nearest neighbour classifier (Zhou & Aggarwal, 2001), neural network (Sacchi *et al,* 2001), support vector machines (Wu *et al,* 2005), and Bayesian classifier (Cucchiara *et al,* 2005). However, these machine techniques are not suitable for the proposed blob system due to requirements for prior training sets. Moreover, it is impractical to provide training samples to suit an e-assessment application, because proving that the training set is a representation of the population is non-trivial. Hence, a fuzzy logic system (FLS) is chosen as it allows an easy representation of human decision-making particularly in a human-dominated environment such as the summative test environment.

One of the key benefits of the blob analysis method is its low-resource consumption i.e. the process is computationally inexpensive. The low-resource advantage is 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 within the cameras field of view (Zang & Klette, 2003). Thus, in a summative test environment the cameras field of view is limited to only one student at a time, as the students are expected to individually concentrate on the test task. This implies that, for x number of students, there would be x number of cameras and the blob operation is carried out individually.

Another interesting advantage of the proposed blob analysis solution is the ability to achieve presence verification with minimal distraction to the student (Apampa *et al*, 2010b). This task is accomplished through a novel blob classifier fuzzy engine which would initiate change-driven re-authentication request as opposed to the frequent re-authentication requests of password and biometric methods. This dynamic classification method would be implemented using a fuzzy logic system (FLS). The final sections in this chapter, presents a brief background of blob analysis techniques and an overview of fuzzy logic systems.

6.7 Existing Applications of Blob Analysis Techniques

Blob analysis techniques have been widely used for a variety of applications such as tracking, event detection, video surveillance, people counting and vehicle counting. Typically, these applications exploit the versatility of the blob statistics embedded in the

blob analysis process. For example in a vehicle tracking system, Bas *et al* (2007) used the bounding boxes to detect the blob and the centroid statistics to mark the vehicle's position. In another work, Javed & Shah (2002) classified objects into categories of humans and vehicles using the centroid and bounding box statistics. These statistics are useful in detecting a blob and estimating the position of the blob over a sequence of frames; however, they provide insufficient information in a case where two blobs merge. Several related works adopt blob analysis for people counting systems, where the blob area significantly reflects the size of the blob. Velipasalar *et al*, (2006) proposes a people counting system that learns automatically the size interval for a single person and uses the blob area to determine the number of people forming the blob.

Automatic video surveillance is useful in detecting and preventing unauthorised human activities in monitored environments (Collins *et al,* 2000). Thus, employing blob analysis can determine whether a person is standing in a forbidden area, running or hiding (Fuentes & Velastin, 2006). Commonly used blob statistics in video surveillance application include the area, centroid and bounding boxes; however, a combination of this statistics can improve the video monitoring process (Ali *et al,* 2006). An important parameter infused with the blob statistics is the colour feature, where the RGB colour values are collected from each blob and they are typically extracted for similarity comparison during tracking (Lipton *et al,* 1998).

Video surveillance applications which involve monitoring humans make use of the skin colour or hair colour (Zhang *et al,* 2009) whilst other applications target the object's colour (Chen & Yang, 2005). The colour feature is useful in monitoring objects as it is independent of the object size and it remains invariant to geometric information (Birchfield, 1998). However, the colour feature may become unreliable due to variation in lighting or when the object and background have similar colour distributions (Zhou & Aggarwal, 2001). Additionally, tracking a blob becomes difficult when the object is at a far distance from the camera, change in direction or occlusion. Thus, for this research the colour feature such as facial complexion, hair colour, and shirt colour would not be considered, as the challenge is to investigate the potentials in adopting the geometric attributes of binary images.

Lastly, it is worth mentioning applications which employ elliptic fitting methods to extract the geometric information of blobs. Ellipse fitting is one of the classic issues of pattern recognition area and it has received considerable attention in a variety of

applications. In a head tracking application, Zhang *et al,* (2005) applied the direct least-square technique (Fitzgibbon *et al,* 1999) to fit the ellipse on a head blob. By doing this, the position, orientation and shape parameters of the head are explicitly represented in preparation for the head tracker. Amidst the adaptation of blob techniques in a variety of applications; this thesis presents the first research in using blob analysis for e-assessment applications. Thus, this research seeks to investigate and demonstrate the feasibility of adopting blob geometric statistics for improving the user security of summative e-assessments.

6.8 An Overview of Fuzzy Logic Systems (FLS)

This section presents an overview of the fuzzy logic systems; however, in-depth discussions on FLS can be found in Klir & Yuan, (1995). Fuzzy logic is a problem-solving methodology which is widely adopted in applications due to its simplicity and flexibility in handling complex processes and drawing definite conclusions from vague or incomplete information. Examples include automatic control (Nemoto *et al,* 1999) and expert systems (Macian *et al,* 2006). In conventional (i.e. crisp) set theory, an element either belongs to a set or it does not. This implies that crisp sets contain elements that satisfy precise properties required for membership i.e. full membership or no membership. For example, in a crisp set, membership or non-membership of element x in set A is described by the function:

$$\mu_A(x), \text{ where } \mu_A(x) = 1 \text{ if } x \quad A \text{ and } \mu_A(x) = 0 \text{ if } x \quad A. \qquad (6.1)$$

Thus, μ_A maps all real numbers $x \quad A$ onto the two points (0, 1), crisp sets represent a two-valued logic: on or off, black or white, 1 or 0. Thus, the characteristic (or membership) function of a crisp set assigns a value of either 1 or 0 to each element in a universal set, thereby discriminating between members and non-members of the set under consideration. The fuzzy set theory introduced by Lotfi Zadeh (1965) is a generalisation of the classical set theory, characterised by a *membership function* and expresses the degree to which an element belongs to a set. A membership function provides a measure of the degree of an element to a given set and it is not restricted to the integers 0 and 1, but may take on any value between 0 and 1 i.e. [0, 1]. For example, given a universal set X, and it is elements be denoted as x, the fuzzy set A of X has a characteristics function associated to it:

$$\mu_A : X \quad [0,1] \tag{6.2}$$

such that, for any $x \quad A$, the fuzzy membership function $\mu_A(x)$ indicate the degree of belonging of element x belongs to the universe of discourse X. For example,

$$\mu_{young} : (alice) = 0.8 \tag{6.3}$$

is read as "Alice belongs to the set of young people to the degree 0.8". The membership function maps each element of X to a membership grade which can take on values between 0 and 1.

Traditional classical or Boolean logic is based on the assumption that every proposition is either 1 (*true)* or 0 (*false)*. In crisp logic, rules are a form of proposition usually denoted as an IF-THEN rule, where the IF part of the rule is called the a*ntecedent* or *premise* and the THEN part is the *consequent* or *conclusion*. Thus, the concepts in crisp logic can be extended to fuzzy logic by replacing 0 or 1 values with fuzzy membership values. An example of a fuzzy logic rule assume the form "IF *x* is *A*, THEN *y* is *B*", where $x \quad U$ and $y \quad V$, and has a membership function, $\mu_{A \quad B}(x,y)$ where $\mu_{A \quad B}(x,y) \quad [0,1]$. To interpret the if-then rule, firstly evaluate the antecedent which involves 'fuzzifying' the input. Secondly, apply the result of the antecedent (i.e. implication) to the consequent, which evaluates the membership function $\mu_{A \quad B}(x,y)$. Hence, in the fuzzy logic, a rule is fired as long as there is a non-zero degree of similarity between the premise and the antecedent of the rule. Additionally, an object can belong to a fuzzy set to different degrees and the set can overlap. Thus, the concept of fuzzy rule-based systems is built on fuzzy sets and fuzzy logic. Non-fuzzy rules (e.g. crisp logic) deal with precise, crisp situations and assertions; however, fuzzy rules address imprecise fuzzy sets. In the next chapter, a detailed implementation of FLS as employed in this thesis is presented.

6.9 Summary

In this chapter, the impersonation challenges threatening the Identity-Authentication user security model are classified into three types namely, Type A, Type B and Type C impersonation threats. The type A or 'connived impersonation' threat can occur when an invigilator willingly colludes with fraudulent students to perpetrate an

impersonation. The Type B impersonation threats can occur as a result the strength or weakness of the authentication method adopted; whilst, the Type C impersonation threat occurs, when an external person substitutes a correctly authenticated student during the test session. The Type A, B and C impersonation threats are known to be a major challenge when conducting summative e-assessments. In this chapter, it is suggested that the vulnerability of the Identity-Authentication user security model is linked to a weakness in the model itself; thus, making the model fallible to the Type A, B and C impersonation threats. Thus, to address this limitation the Presence-Identity-Authentication user security model is proposed. In this context, satisfying the presence security goal ensures that the correctly authenticated student at the beginning of a test is the same student that completes the test whist taking the test void of external assistance.

In order to adopt the P-I-A user security model, it is essential to employ a suitable method to achieve the presence security goal. The potential approaches reviewed in this chapter, were unsuitable to achieve presence verification in summative e-assessments. Hence, an object tracking approach using a blob analysis method was suggested. The blob analysis solution is a video processing technique that attempts to verify the student's presence in a non-distracting fashion throughout the test session. In the next chapter, the system design of the blob-based presence verification system is described.

Chapter 7. Blob-based Presence Verification (BlobPV) System

Recall in chapter six, potential approaches to achieving presence verification and their limitations were discussed. Additionally, due to these disadvantages a blob analysis solution which follows an object tracking approach was suggested. In this chapter, the concept is developed into a novel blob-based presence verification system and this satisfies the second research objective of this thesis.

The blob-based presence verification system (hereafter known as *BlobPV*) uses the geometric statistics of blobs to make inferences about an object's presence in the video frame. In the BlobPV system, an *object* refers to an entity of interest detected in a video sequence and can be characterised using blobs, whilst a *blob* (Binary Large OBject) is defined as a group of connected pixels with the same properties within a binary image. In order to exploit the potentials embedded in the connected components, various blob statistics can be calculated using a blob analysis operation. *Blob analysis* is a process that allows the identification of blobs and the calculation of the statistical information of the blobs within a binary image. The analysis is concluded by summarising the information extracted from each image in a report which can be further analysed. Examples of the blob statistics discussed in this chapter include: area, centroid, major axis, minor axis orientation, bounding box and eccentricity. This chapter presents the system design for the BlobPV system, which includes modules such as pre-processing, blob operation, methods and risk classification.

7.1 Blob Statistics in BlobPV System

This section describes the blob geometric attributes that can be extracted from a binary image. The blob statistics described include: centroid, area, bounding box, extent,

major axis, minor axis, orientation, eccentricity, diameter, perimeter and count. Amongst the statistics listed above, the orientation, eccentricity, major and minor axes are derived from ellipse geometric properties. In literature (Sheu *et al,* 1997) the ellipse is characterised with a five dimensional parameter space $\{x_0, y_0, a, b, \theta)$, where (x_0, y_0) is the centre coordinates, (a, b) represents the length of the major and minor axis and (θ) is the orientation angle of the major axis. It should be noted that, the other blob statistics are not derived from the ellipses; however, the ellipse is used for illustrative purposes. The following describes the blob statistics with implication for this research.

Centroid

The centroid represents the centre of mass of a blob in an image which is measured by the *x*- and *y*-coordinate values. Typically, the centriod can be used to report an object's position in a video frame; thus, providing the location information of the blob. This is particularly useful as the current position of the blob within the region is known. However, when two blobs merge, the centroid statistics are incapable of reporting the information. In this case, the coordinates of the centre of gravity of the merged blob is computed without suggesting the appearance of a new blob. For the purpose of this research, the event where two blobs are merged is important as it depicts an external object in the video frame. Hence, due to this limitation the centroid statistics would not be considered in this thesis. Figure 7-1 shows the (x_0, y_0) coordinates of the centroid.

Area

The area statistics represents the actual number of connected pixels that make up a blob, i.e. the total number of pixels which fills up a blob. A pixel is the smallest physical unit in the video image. The blob area provides a quick access to the overall blob size; thus, a change in the size of a blob will result in re-calculation of the area of the blob. Hence, the blob area is useful when determining the variations of the blob size. For example, the area of a merged blob will vary significantly from the area of a single blob; consequently, the sizes will reflect the changes. Thus, for the purpose of this research the area statistics can be used to estimate the changes to an initial known area value. Figure 7-1 illustrates the area of the blob, i.e. is the shaded region.

Bounding box

The bounding box represents the smallest rectangle that encloses the detected blob in an image. This information can be used to precisely identify the object in order to compute various parameters. Typically blobs in an image are determined by their centre coordinate (i.e. centroid) and the bounding box encompasses all the blobs found. Bounding boxes are also useful in determining the current location of a blob which is tracked over time. Additionally, bounding boxes offer useful statistics in determining the relative sizes of the blobs; thus, a merged blob will depict an increase in the size of the bounding box. Although robust, the bounding box does not provide sufficient statistics that can be used independently. Due to this limitation, the bounding box will not be considered for this research. In Figure 7-1 the bounding box is illustrated.

Extent

The extent statistics 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 size of its bounding box. For example, a blob with an increased area will occupy a larger percentage of its bounding box (see Figure 7-1). The result from this is a decrease in the extent ratio which simultaneously reveals a change in the area of the blob. In the BlobPV system, the extent statistics are exploited to detect occlusion and to provide information about the objects distance from the camera. The extent ratio is computed by:

$$extent = \frac{blob\ area}{bounding\ box\ area} \tag{7.1}$$

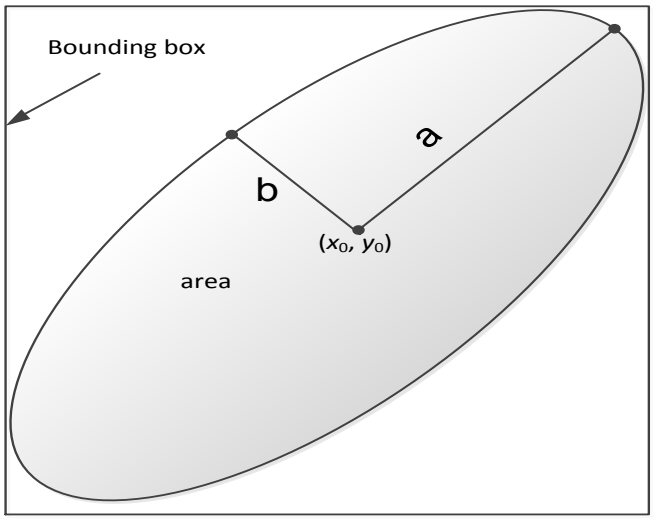


Figure 7-1 Centriod, Area, Bounding box and Extent properties

Major and Minor axes

The major axis represents the long axis of an ellipse, whilst the minor axis is the line perpendicular to the major axis and it represents the shorter axis. Traditionally, the length of the major axis is indicated by 2a and the minor axis by 2b, where the two axes are distinguished by a ≥ b (Note: where a = b, the ellipse is a circle). Figure 7-2 and Figure 7-3 shows an ellipse in two of its standard forms where the major axis is parallel to the x-axis and y-axis respectively. The position of the major and minor axis in an ellipse suggests that the shape of the blob can be derived. This implies that the value of the aspect ratio (ratio of major to minor axis) of an ellipse can be used to estimate the current shape of a blob in the image. It is assumed that the blob in Figure 7-3 has a vertical direction, whilst the same blob in Figure 7-2 depicts a varying or near-horizontal direction. Visual observation of the two blobs reveals different shapes and different positioning of the major and minor axis. Additionally, an increase in the length of the major axis will produce an elongation of the ellipse towards a particular direction; thus, showing a deviation from the initial shape. Hence, the more elongated the ellipse in a particular direction, the larger the ratio reflecting a change in shape. The BlobPVS proposes that the ratio of the major to minor axis of a blob can estimate the varying activities of a moving object in a video frame to estimate the shape of the blob. The ratio of the major axis of the ellipse to its minor axis is given by:

$$\frac{ellipse\ major\ axis}{ellipse\ \min or\ axis} = \frac{a}{b} \tag{7.2}$$

Orientation

The orientation represents the angle formed between the *x*-axis of reference and the major axis of the ellipse (see Figure 7-2). The direction is calculated in radian (-π/2 and π/2) counter-clockwise from the x-axis. The blob orientation can provide the information to determine an object's pose within a video frame. For example, an object with a vertical direction relative to the camera (i.e. major axis parallel to the y-axis) will obtain an orientation value of 90^o or 1.57radians. Similarly an object with a horizontal direction relative to the camera will obtain an orientation value of 0^o or 0.0radians. In the BlobPV system, it is proposed that the orientation statistics would accurately estimate a moving object's pose or direction in the video frame.

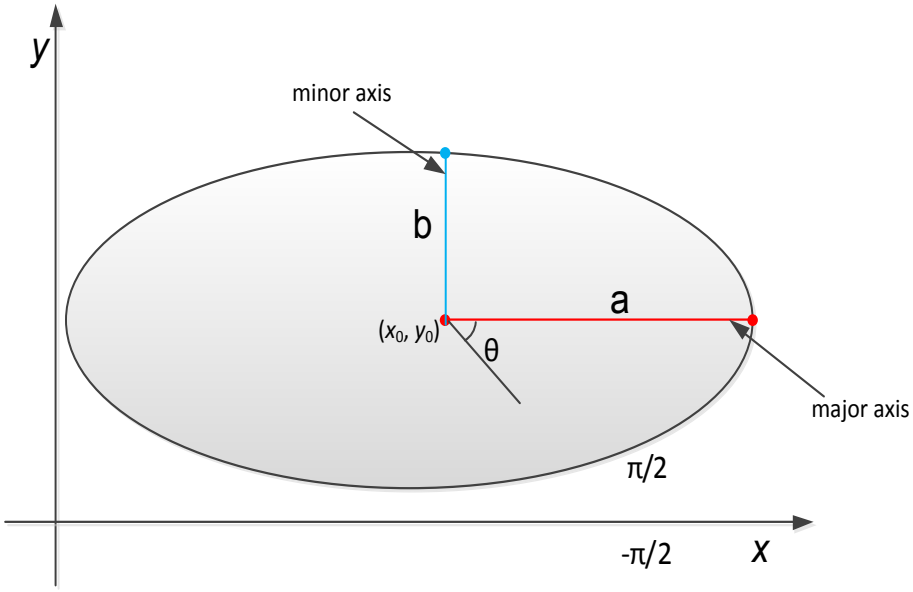


Figure 7-2 Major Axis Parallel to the *x*-axis

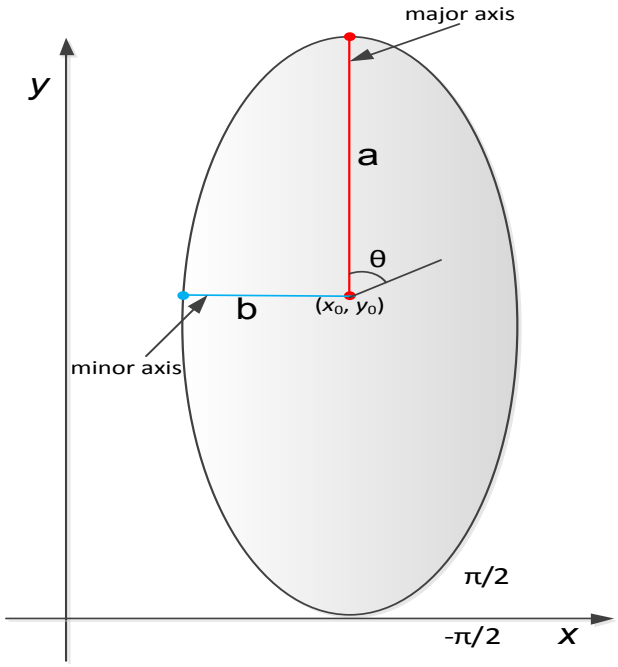


Figure 7-3 Major Axis Parallel to the *y*-axis

Eccentricity

The shape of an ellipse (i.e. the fatness or thinness) is typically expressed by the eccentricity statistics. The eccentricity value ranges between 0 and 1, where 0 means a=b (i.e. major and minor axis are equal in length), in which the ellipse is a circle. Consequently, a value of 1 depicts a straight line where the minor axis does not exist. The eccentricity of an ellipse is the ratio of the distance between the foci to the length of the major axis length of an ellipse. In this research, the eccentricity statistics is not considered, as the major and minor axes provide sufficient information about the shape of a blob.

Equivalent Diameter Squared

This diameter statistics represents the size of the largest blob and it is computed by taking the square root of the pixel area of the blob. The calculation is roughly equivalent to the diameter of the blob and this would be the length of the side of the blob, assuming the blob is a square. Irrespective of the object activities in a video frame, the diameter statistics value varies minimally from a known initial value. Thus, for the purpose the BlobPV system a significant change to a known value will be useful in detecting changes in the object.

Perimeter

The perimeter statistic is represented as the total length of the outside edges of a blob (in pixels). That is the number of pixels that surround the blob and it is calculated by the distance between each adjoining pair of pixels around the border of the blob. Hence, the perimeter value of an object performing an activity will vary to another object performing a similar activity. Irrespective of the object activities in a video frame, the perimeter statistics value would vary insignificantly from a known initial value. Thus, for the purpose the BlobPV system a significant change to a known value will be useful in detecting changes in the object.

Count

The count statistics is introduced to determine the number of blobs found in a binary image. In the BlobPV system, the count statistics is useful to determine the number of objects in a video frame.

7.2 Presence Verification using Blob Statistics

From section 7.1 it is observed that the proposed blob analysis technique would exploit an object's blob statistics to determine the object's current activity in a video frame. For example, using the blob orientation statistics, an object gazing directly at a camera can be accurately estimated. Similarly, the blob extent statistics can provide information about an object's distance from the camera, whilst the count statistics can detect multi-presence in the video frame. Thus, based on these simple instances it is suggested that a variety of activities can be precisely deduced from the blob statistics. However, it is assumed that there exist other activities which cannot be accurately determined using a single blob statistics. For example, relying on the changes in the area statistics only would produce insufficient information to determine an object's activity from frame-to-frame in a video sequence. However, combining the area statistics with the orientation or extent statistics may reveal an object moving away from the camera or the direction of movement. Figure 7-4(a – d) illustrates the examples described above

Figure 7-4a depicts an object's frontal pose with the orientation approximately 90^0. It is assumed that the same object shown in Figure 7-4a is depicted in Figure 7-4b; however, the blob in Figure 7-4b shows a reduction in area which would effectively produce an increase in the extent statistics. For example, a decrease in blob area may be

due to the object's distance from the camera. In Figure 7-4c and Figure 7-4d, it is assumed the object's area and extent statistics remain unchanged from the initial values in Figure 7-4a (provided there is insignificant change in the object's distance to the camera). However, it is observed that the Figure 7-4c and Figure 7-4d suggest a change in the object's pose which results in the change of polarity from a negative orientation to a positive orientation. This suggests that the object has turned in an opposite direction from its initial position. Additionally, the Figure 7-4c and Figure 7-4d show a change in the direction of the major and minor axis, which would affect the shape of the object. This illustration demonstrates that whilst some blob statistics can sufficiently estimate an object's activity; the correct detection of other activities will require a combination of different blob statistics.

Thus, based on the above discussions two approaches to implement the BlobPV system is proposed. The first approach is based on estimating an object's pose directly from the blob statistics, i.e. mapping an object's activity to a blob statistic. This approach would rely on discriminative blob statistics such as count, orientation and extent to accurately determine an object's activity. Hence, the pose estimation approach would attempt to make inferences about an object's presence directly from the video frames. The second approach is an activity risk classification, which is based on aggregating the changes in the blob statistics between successive video frames. This implies that the activity risk classification approach would make inferences about an object's presence by analysing and classifying the changes in the blob statistics. Figure 7-5 shows a conceptual diagram of the two approaches. From the diagram, it is observed that an object is tracked via continuous video signal and the first step is to detect and extract the object from the background. The foreground object is segmented and the connected pixels are grouped to form a blob. Additionally, the relevant geometric attributes of the blob is extracted. Thereafter, the pose estimation and activity risk classification approaches would be implemented. The suitability of these approaches is discussed in the next chapter. Table 7-1 show the proposed blob statistics and their relevance in example object activities.

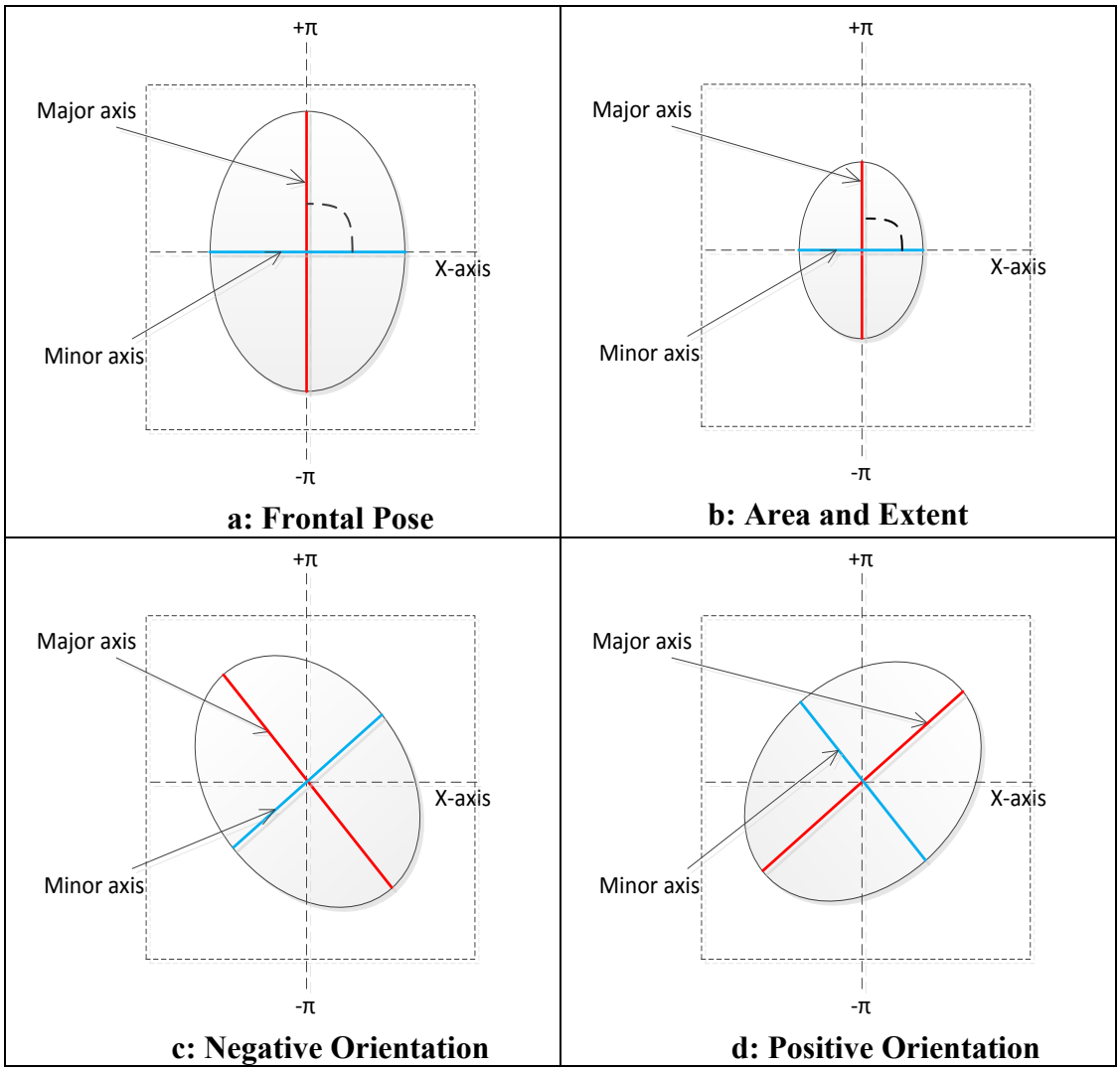


Figure 7-4 Blob statistics example illustrations

Activity examples	Blob description	Relevant statistics
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 substitute student	Old blob disappears	Area Major/minor axes
Face close to camera	Blob moving towards camera	Extent Area
Hand blocking camera	Blob moving towards camera	Extent Area
Head blocking camera	Blob moving towards camera	Extent Area
Head/face distant from camera	Blob moving away from camera	Area Major/minor axes Extent
Lean on table	Blob moving in different direction	Area Extent Orientation
Look down	Blob change in form	Area Extent
Look forward	Blob is stationary	Orientation
Look left/right	Blob change in form and move in different direction	Area Orientation
Look up	Blob change in form	Area Orientation
Hand on cheek	Blob expands	Area Major/minor axes Orientation
Cover face	Blob expands	Area Major/axes

Table 7-1 Identifying blob statistics in activity examples

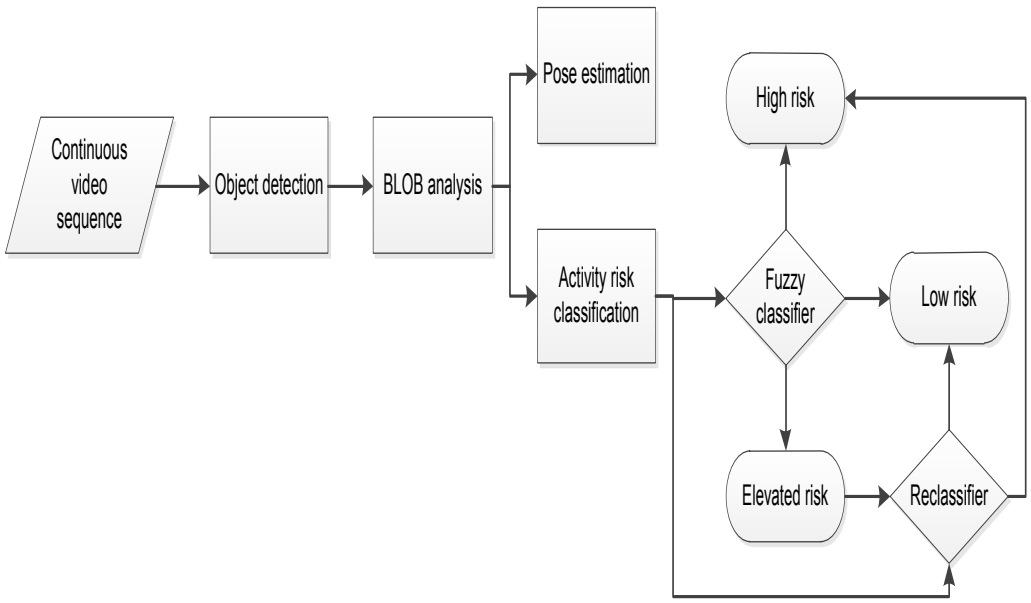


Figure 7-5 A conceptual diagram for the presence verification approaches

7.3 BlobPV System Design

This research investigates the feasibility of using blob analysis for presence verification in a summative e-assessment environment. Figure 7-6, shows the architecture of the proposed system. The system architecture is divided into four stages, namely: object pre-processing, blob operation, methods and activity classification. These stages are further discussed in this section. The system is developed using the MATLAB/Simulink Video and Image processing Blockset. The MATLAB/Simulink modelling environment is employed due to its simple and easy-to-use graphical user interface for performing simulations.

7.3.1 Frame Pre-processing

The pre-processing stage starts with converting from a multi-dimensional (RGB, HSV or any other) colour space to a matrix of intensity values between 0 and 255. In this study, an RGB colour space is converted to an intensity image and the conversion from an RGB image to an intensity image takes place on-the-fly. Intensity (greyscale) images refer to normalised images, since each pixel value is expressed within a given range between the minimum and maximum values. The resulting intensity image is used for object detection in the next stage.

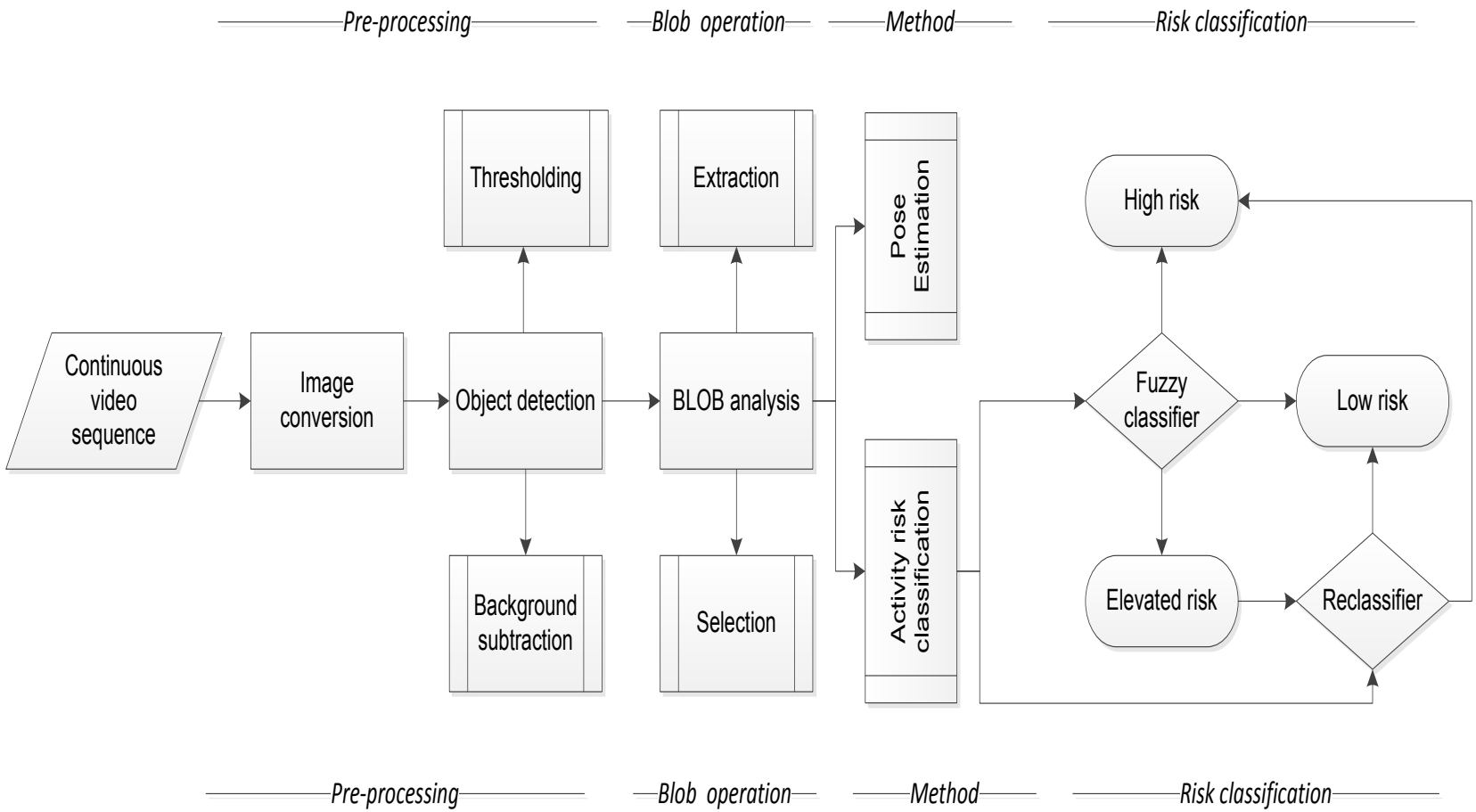


Figure 7-6 The BlobPV system architecture

7.3.1.1 Object Detection

The first stage in object tracking applications is the detection and segmentation of the moving objects in the images. Three conventional approaches include temporal differencing, background subtraction and optical flow. The background subtraction is a commonly used technique due to its simple implementation and low computational costs (McIvor, 2000). In an e-assessment environment the assumption is that the camera is fixed such that only the object of interest is captured in the cameras field of view. This implies that a stationary background is recommended. To improve the detection accuracy, the background image should be provided in advance. The background subtraction approach was adopted for the BlobPV system and a 100% object detection rate was achieved. The results of the background subtraction process are background-removed images, which are forwarded to the thresholding subsystem.

The thresholding operation aims to segment the background subtracted image, to extract the object of interest from other features in the frame. To accomplish this, a threshold value to determine the inclusion or exclusion of a pixel as a background or foreground object is required. Thus, the input to a thresholding process is intensity (greyscale) or a colour image and the output is a binary image. The challenge of manual thresholding lies in the choice of threshold value to use. A suitable threshold value can be determined by looking at the histogram plot of the background subtracted image. In this case, the pixel values of the foreground object are manually separated from the pixels within the background. However, due to variations in lighting, object features and object motion, this thresholding technique does not produce good results.

7.3.1.2 Autothresholding

The autothreshold operation, automatically converts intensity images to a binary image using the Otsu threshold selection method (Otsu, 1979). This method automatically selects an optimal threshold by minimising the intra-class variance of black and white pixels in the binary image; thus, eliminating the manual process of choosing threshold values. Hence, irrespective of the object variations in the intensity images, the autothreshold method allows on the on–the-fly-thresholding. This approach is implemented in the Simulink Autothreshold block and it is adopted for the system design.

7.3.2 Blob Operation

At this stage, the idea is to segment the foreground pixels, find blobs and extract the relevant statistics for further analysis. To select the blobs, a connected component analysis process is used to identify and label sets of connected pixels. Two commonly used methods which defines a connected neighbourhood for a 2D image is 4-connected neighbourhood and 8-connected neighbourhood (Haralick & Shapiro, 1992; Rosenfeld, 1970). These techniques can be distinguished based on their pixel connectivity (see Figure 7-7). In the 4-connected neighbourhood, the four connected pixels share an edge i.e. pixels on the same row or column, whilst in an 8-connected neighbourhood, connected pixels share edges or vertices i.e. pixels on the same row or column and the diagonal pixels. Thus, the effectiveness of a blob analysis technique relies on the type of pixel connectivity chosen. Due to undesirable configuration anomalies, a common pattern is to use a different pixel connectivity for the foreground and background i.e. either using 4-connectivity for the foreground with 8-connectivity for the background or using 8-connectivity for the foreground with 4-connectivity for the background. Thus, once all groups have been determined, each pixel is either on or off, black or white depending on the chosen method.

In the BlobPV system, the 8-connectivity method is chosen due to the sensitivity of the shape from the input image, i.e. it is assumed that each initial blob contains one object. For the purpose of this research, the pixels that are set to binary '1' are considered the blobs and appear white in the image; whilst, the background pixels are set to binary '0' and appear black in the binary image. Other forms of pixel connectivity include the 6, 18, and 26–connected neighbourhood; however, they are suited for three dimensional (3D) images and will not be considered.

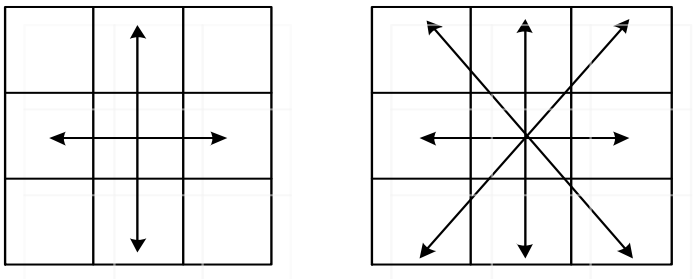


Figure 7-7 4-connected neighbour and 8-connected neighbour

7.3.3 Methods

Recall in section 7.2, the pose estimation and activity risk classification approaches were proposed as suitable techniques to implement the BlobPV system. For the pose estimation approach, it is suggested that an object's activity can be determined directly by mapping each activity to the extracted blob statistics. However, the activity risk classification approach suggests that analysing the changes of the blob statistics would infer an object's activity in the video frame. The two approaches would receive as input the proposed blob statistics in Table 7-2. The feasibility of these approaches is demonstrated in the next chapter.

Blob Statistics	Description	Study Expectations
Area	Area of blob	The area statistics would vary insignificantly through the different activities, provided the same detectable feature (e.g. face) is presented to the camera
Extent	Percentage occupancy of blob in the bounding box	The extent statistics would indicate the obstruction of a cameras field of view. In addition, the dissimilarity in extent statistics for the same object would indicate a change in the object's pose.
Major axis	Long length of an ellipse	The major and minor axes would indicate a change in the object's shape.
Minor axis	Short length of an ellipse	
Orientation	Angle between the major axis of an ellipse and x-axis of the image plane	The orientation statistics will indicate an object's direction through the different activities. For example an object looking straight would be approximately 90^{o}.
Count	Number of blobs in an image	The count statistics would indicate the number of objects present in a cameras field of view
Perimeter	Length of blob	The perimeter and diameter statistics values would not change significantly through the different activities. This statistics would indicate the sameness of an object during the re-classification process.
Diameter	Size of blob	

Table 7-2 Proposed Blob Statistics for Presence Verification

7.3.4 Risk Classification

The risk classification is the final stage of the system architecture. The components in this phase are the novel blob classifier engine implemented using a fuzzy

logic system and the threat classification scheme. The threat classification scheme is made up of three risk decisions (Apampa *et al,* 2010a). Thus, the blob classifier engine receives as input the blob statistics values and it outputs a threat class assigned to each object detected. The threat classification scheme is described in this section whilst the blob classifier engine is discussed in the next section. A schematic diagram of the threat classification scheme is shown in Figure 7-8.

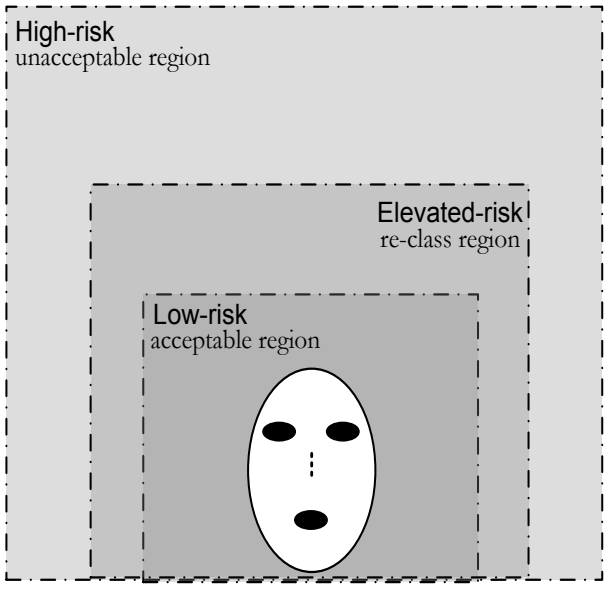


Figure 7-8 Threat classification scheme

7.3.4.1 Low-risk Threat Class

A low-risk threat class is assigned when the detected object's presence does not pose a security threat. This implies that the blob statistics values extracted from the object vary insignificantly when compared to an initial frontal statistics. In practical terms, a low-risk implies that the student's presence is within an acceptable range and does not reflect the likelihood of dishonest activities in the environment. Hence, the summative e-assessment environment is not at risk of the student's presence.

7.3.4.2 Elevated-risk Threat Class

An elevated-risk threat class is assigned when the detected object's presence reveal suspicious actions that may lead to a security threat. At this stage, the extracted blob statistics values show significant variations from an acceptable range; thus, the values reflect the likelihood of suspicious activities in the environment. However, in an elevated-risk class there exists an opportunity for a reclassification. Thus, an object's

presence would be re-classed as a low-risk or a high-risk. In practical terms, an elevated-risk class attempts to reconfirm a student's presence in a non-interruptive and non-distracting approach. However, the summative e-assessment environment is still at risk of the suspected student's presence until a new threat class is assigned.

7.3.4.3 High-risk Threat Class

A high-risk threat class is assigned when the detected object's presence pose a security threat to the environment. In the high-risk class, the extracted blob statistics values lie within an un-acceptable range; thus, the values reflect the occurrence of user security threat activities. The high-risk class can be assigned directly or from the elevated-risk class. In practice, the high-risk class suggests that the summative e-assessment environment is at risk of user security threats or suspicious activities that could lead to a security threat. Hence, it is required that the student's presence is re-confirmed to ensure that the authenticated student at the beginning of a test is the same student at that point. Thus, the student is requested to re-authenticate. Interestingly, this is the only stage where the student is aware of the presence verification process.

7.4 Blob Classifier Engine Operation

The blob classifier engine is embedded in the activity risk classification approach (see Methods in 7.3.3) and the process is executed using two fuzzy rule engines namely the *frontal class engine* and the *risk class engine*. The frontal class engine is the initial state of the process and its goal is to test for *frontalness* of the detected blob. In this thesis, 'frontalness' refers to the satisfactory frontal pose of an object. Thus, when an object's frontal pose meets the pre-defined requirements the frontal class engine initialises the risk class engine. The risk class engine is responsible for classifying the detected object's blob statistics in accordance with the threat classification scheme, i.e. low, elevated or high risk (see Section 7.3.4). Figure 7-9 shows the blob classifier engine within the activity risk classification and its operation is described below. Given an input video sequence, the activity risk classification process requests a frontal pose from the object detected. A satisfactory frontal pose is recorded when the object achieves an orientation statistics value of $+/-90^{o}$. Thus, achieving a satisfactory frontal pose would imply that the object's blob statistics is extracted and stored as *frontal pose statistics*.

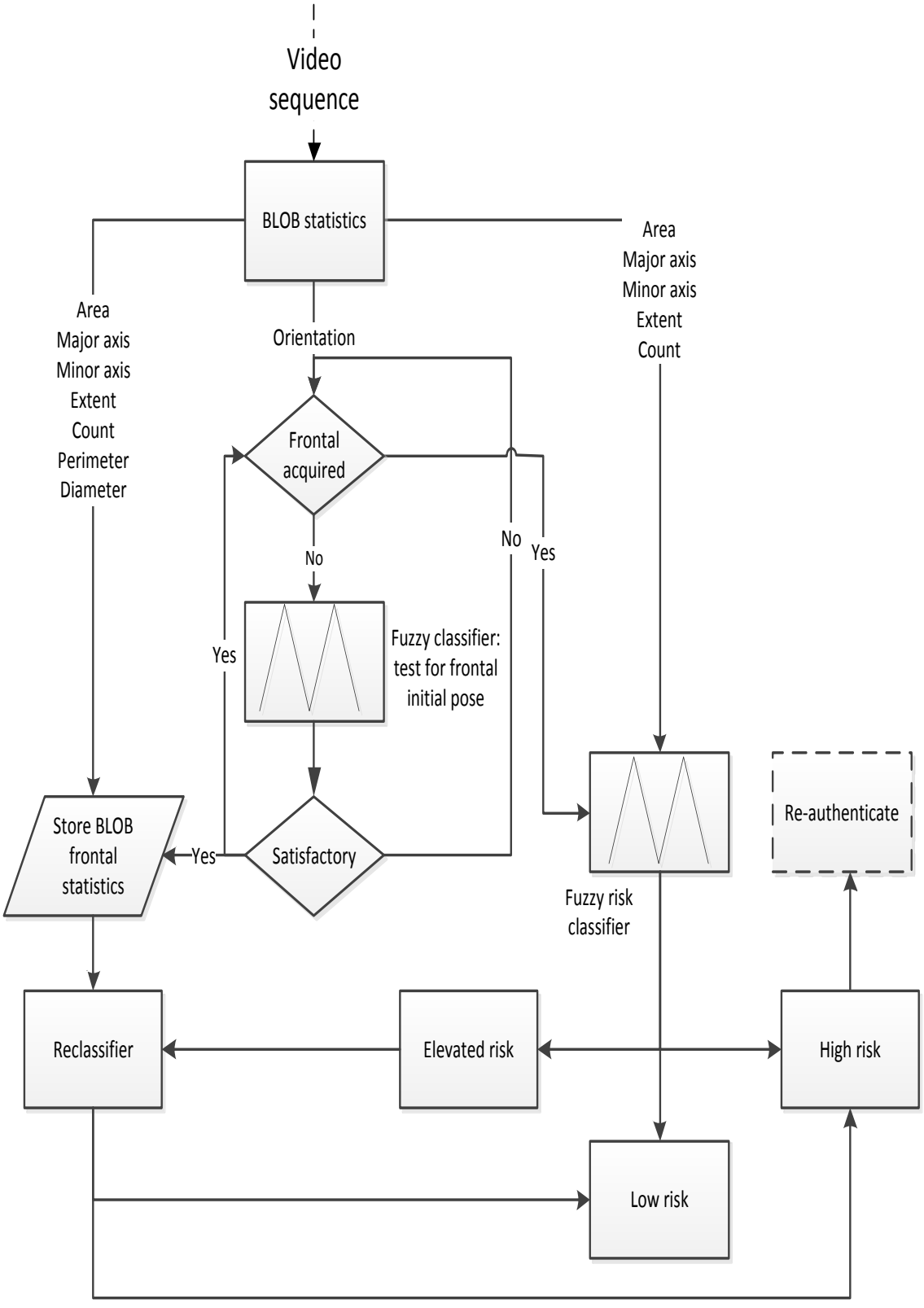


Figure 7-9 Blob classifier engine in activity risk classification approach

The frontal pose statistics is composed of initial blob statistics (such as area, extent, perimeter, count, major axis, minor axis, and diameter) extracted from a blob. The values of the area, extent, orientation, major axis and minor axis statistics (hereafter known as *current activity statistics*) are extracted as long as the object is detected in the video sequence. This statistics are then fed into the risk class engine. However, the values of the perimeter and diameter statistics are stored for use during the re-classification process. Thus, for every video frame received (after the frontal pose) the object's current activity statistics would be passed on to the risk class engine; whilst the perimeter and diameter statistics is employed for re-classification.

At this stage, the fuzzy risk class engine takes over the process and the engine is required to extract, analyse and classify all the video frames where an object is detected. The output risk is determined using the threat classification scheme (i.e. low, elevated or high) and the risk class is assigned based on the significant changes in the object's current activity statistics. A re-classification of an output class occurs when an initial output class is set to an elevated-risk. At this stage, the perimeter and diameter statistics of the current activity is compared to a pre-defined constant value. Hence, the outcome of the comparison would lead to a low-risk or high-risk reclassification. The activity risk classification approach is demonstrated in the next chapter.

7.5 BlobPV Software Design

This section describes the design of the software system that was used for the BlobPV experiments demonstrated in the next chapter. The system is developed using the MATLAB/Simulink Video and Image processing Blockset. The BlobPV software design is divided into two parts namely the *frontal activity model* and the *after frontal activity model*. The two models are made up of subsystems which are discussed in greater detail below.

7.5.1 Frontal Activity Model

The Frontal activity model in Figure 7-10 consists of the following subsystems: image pre-processing, frontal pose detection and frontal pose classification. This model also contains the frontal class fuzzy engine (see section 7.4), which is used to test for 'frontalness' of the detected blob. The value of an object's blob orientation statistics will then be displayed to indicate a satisfactory/unsatisfactory frontal pose.

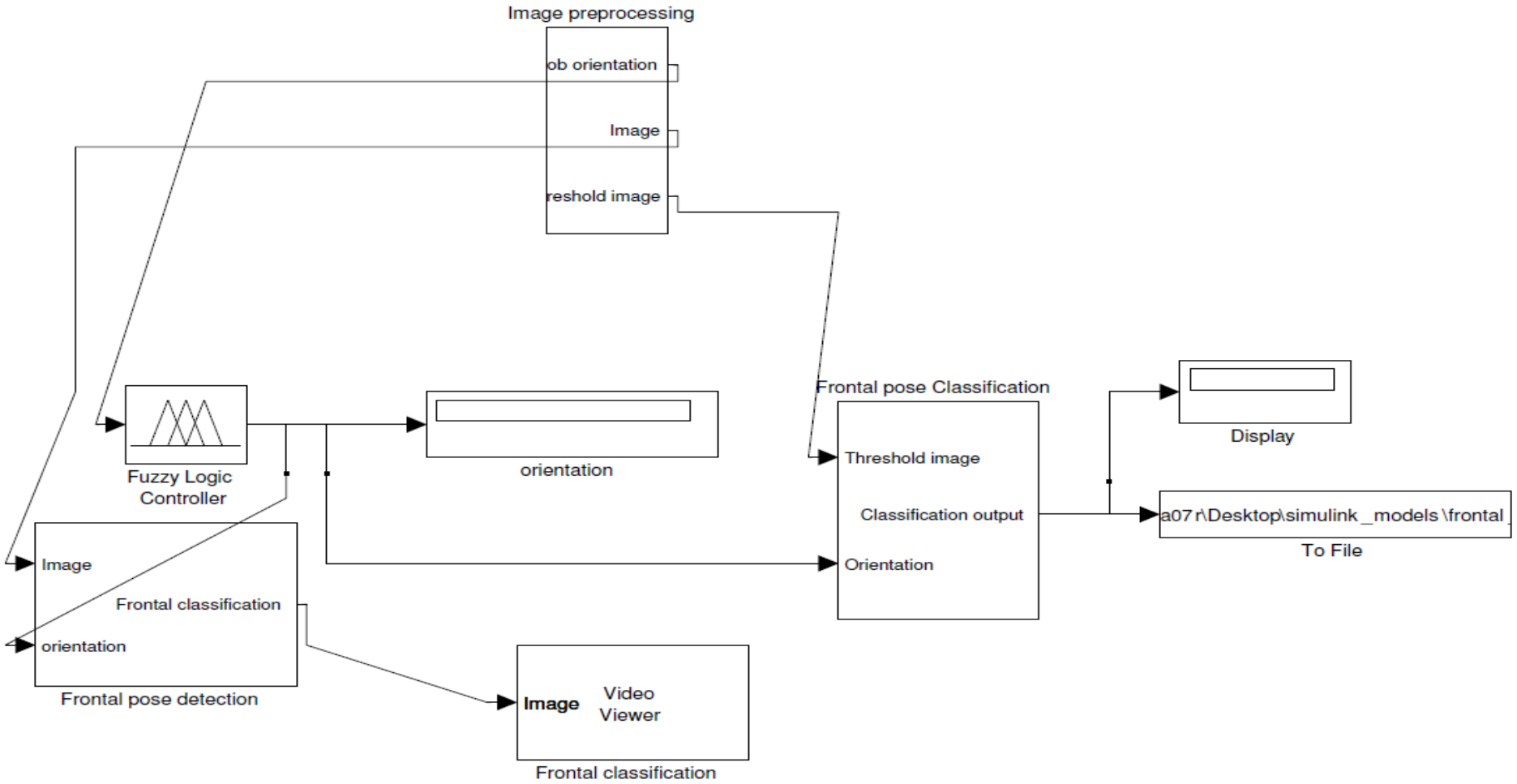


Figure 7-10 Frontal activity model

In addition, the object's blob statistic values is stored in a Matlab file (M-file) which is fed into the *After Frontal activity model* discussed in the next section. This action is required to ensure that the object's current activity statistics will be calculated as a function of the object's satisfactory frontal pose statistics.

7.5.1.1 Image pre-processing subsystem

In the image pre-processing subsystem (see Figure 7-11) two images are loaded on to the modelling environment, that is the object's background image and the object's frontal image. Thereafter, the frame pre-processing activities discussed in section 7-3 are applied on the two images; examples of these activities include colour conversion, object detection and autothresholding. Lastly, a blob operation is applied on the threshold image, where the blob orientation statistics value is used to test for 'frontalness'.

7.5.1.2 Frontal pose detection subsystem

The input to the frontal pose detection subsystem (see Figure 7-12) will be the image that is output from the image pre-processing subsystem. Thus, this subsystem is responsible for detecting a frontal pose activity from the received image. If a frontal pose activity is detected, the image is forwarded for a frontal classification; otherwise the system requests for a satisfactory frontal pose.

If Action subsystem

This subsystem contains the "if-then-rule" which is used to compare the blob orientation statistic values.

7.5.1.3 Frontal pose classification subsystem

The input to the frontal pose classification subsystem (see Figure 7-13) will be the blob orientation statistics value obtained from the frontal pose detection subsystem. This subsystem determines the satisfactory qualities of an object's frontal pose by comparing the object's blob orientation statistics against a set of criteria (Constants). Hence, an acceptable or unacceptable frontal classification is assigned. Lastly, the object's blob frontal pose statistics are stored in an M- file.

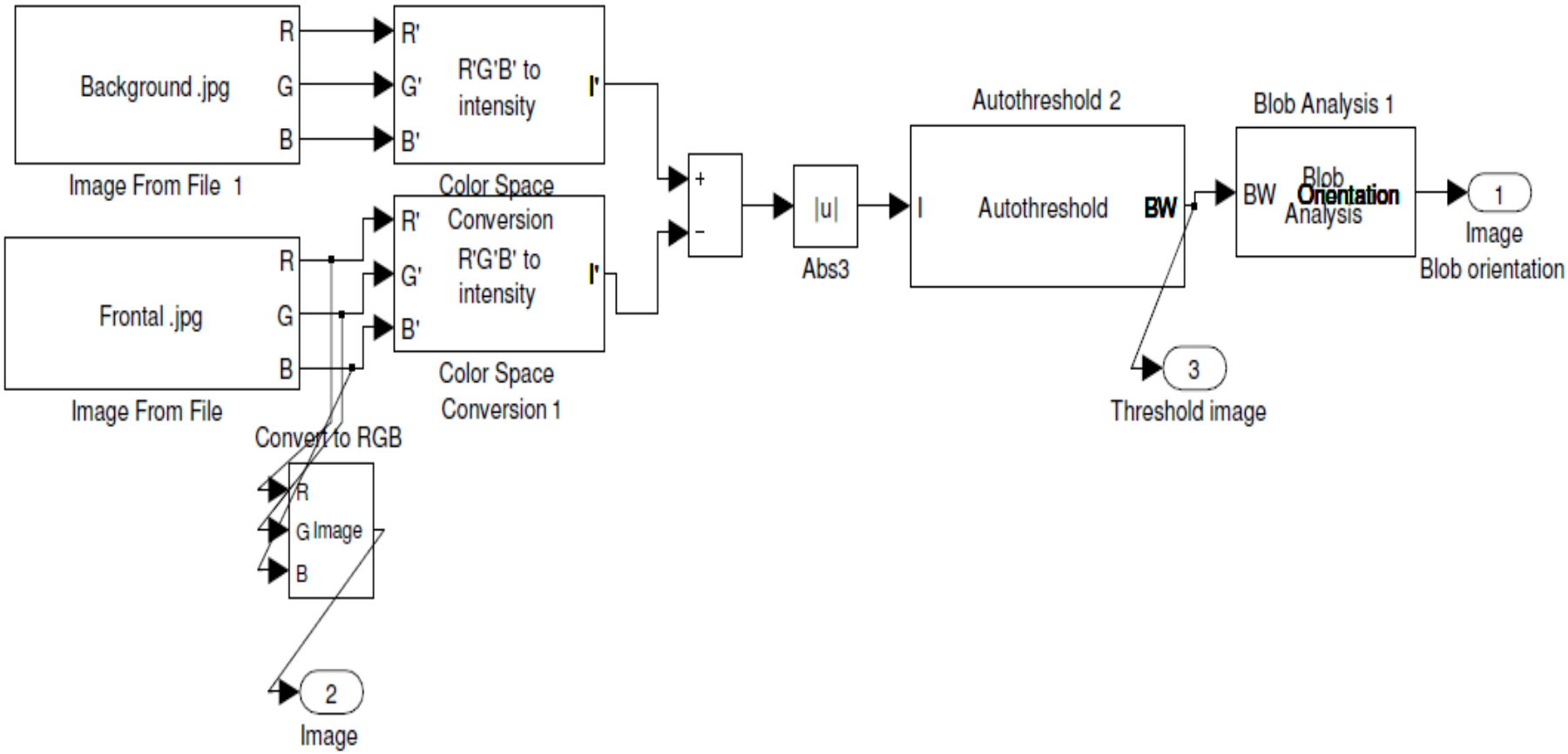


Figure 7-11 Image pre-processing subsystem

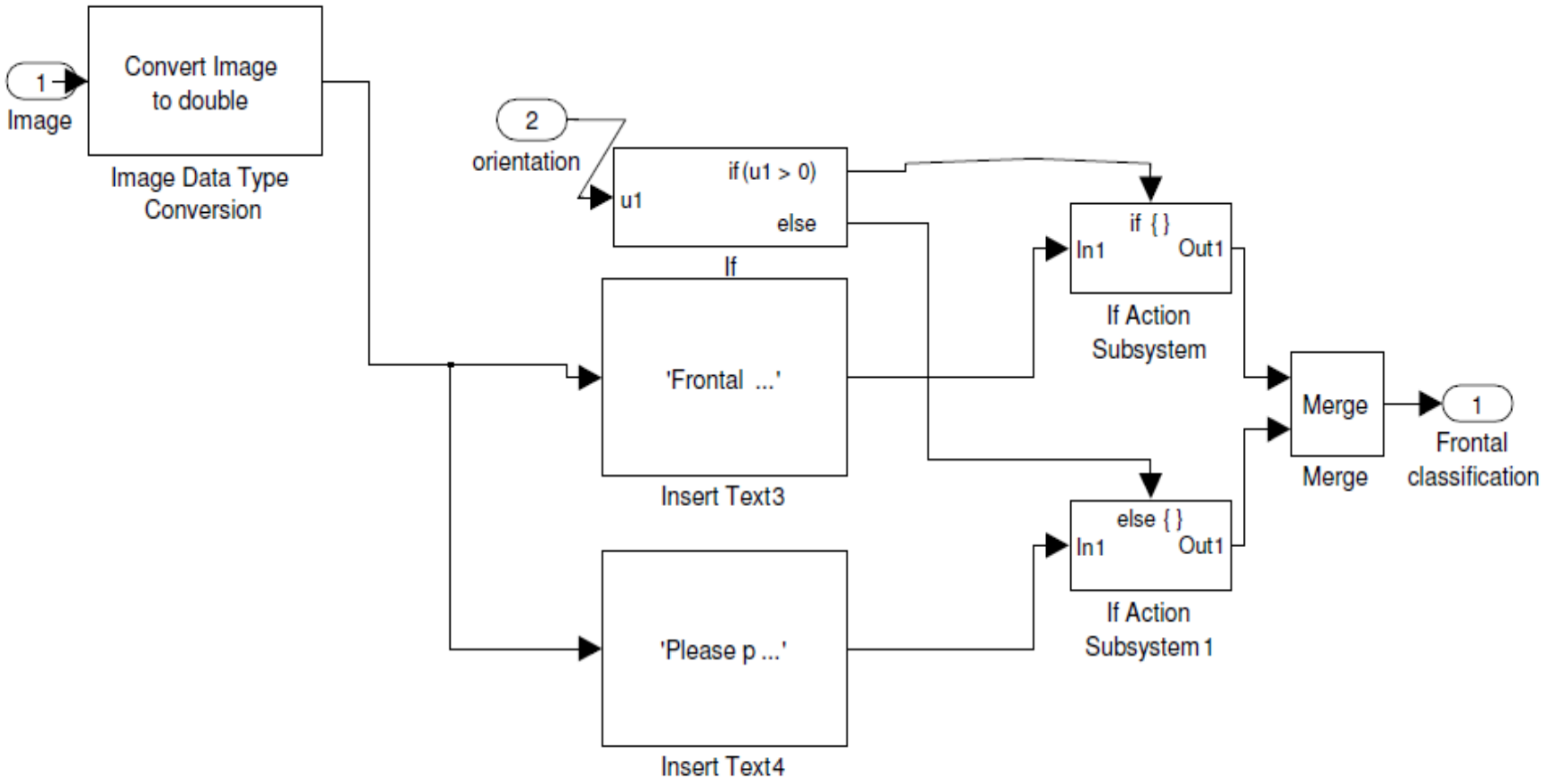


Figure 7-12 Frontal pose detection subsystem

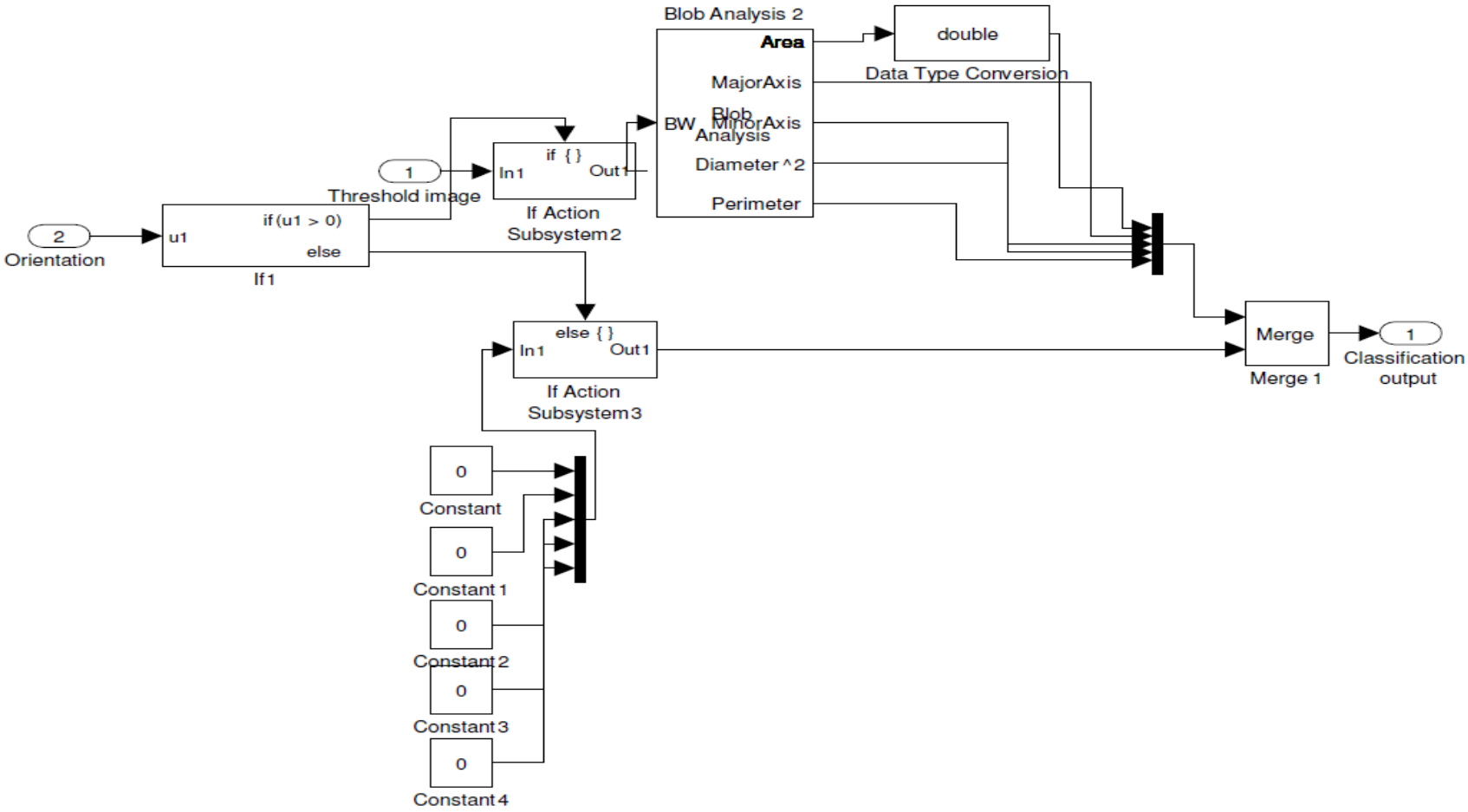


Figure 7-13 Frontal pose classification subsystem

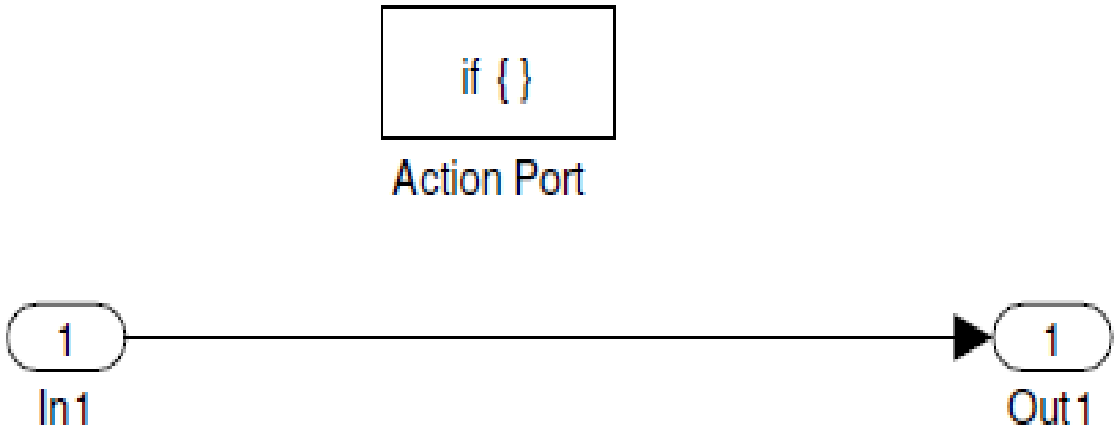


Figure 7-14 If Action subsystem

7.5.2 After Frontal Activity Model

The After Frontal activity model in Figure 7-15 consists of the following subsystems: image pre-processing, operations, conversion, activity statistics, threat classification and threat re-classification. This model also contains the risk class fuzzy engine (see section 7.4), which is responsible for classifying the detected object's blob statistics in accordance with the threat classification scheme. The M-file containing information about the object's frontal pose statistics (i.e. values for orientation, area, major axis, minor axis, extent and count) is fed into the After Frontal activity model. Recall that, the M-file was compiled in the Frontal activity model; thus, the object's current activity statistics are calculated with respect to the object's frontal pose statistics.

7.5.2.1 Image pre-processing subsystem

The image pre-processing subsystem (see Figure 7-16) consists of two images which are loaded on to the modelling environment, this are the object's background image and the object's non-frontal activity, e.g. "left hand on cheek". It should be noted that, several images of the object performing diverse activities can be loaded; however, it is important that the background image is constant. Thereafter, the frame pre-processing activities discussed in section 7-3 are applied on the two images; examples of these activities include colour conversion, object detection and autothresholding.

7.5.2.2 Operations subsystem

The M-file (contains object's frontal pose statistics) stored in the frontal pose classification subsystem (from the Frontal activity model), is fed into the operations subsystem (see Figure 7-17). This ensures that the changes to the object's current blob statistics are calculated with respect to the frontal pose activities retrieved from the file. The mathematical and relational operators shown in the subsystem perform numerical operations to reflect the changes in the object's blob statistics. The Constant values and relational operators for threat re-classification are also defined in the operations subsystem. For threat re-classification purposes the object's diameter and perimeter blob statistics are extracted and stored.

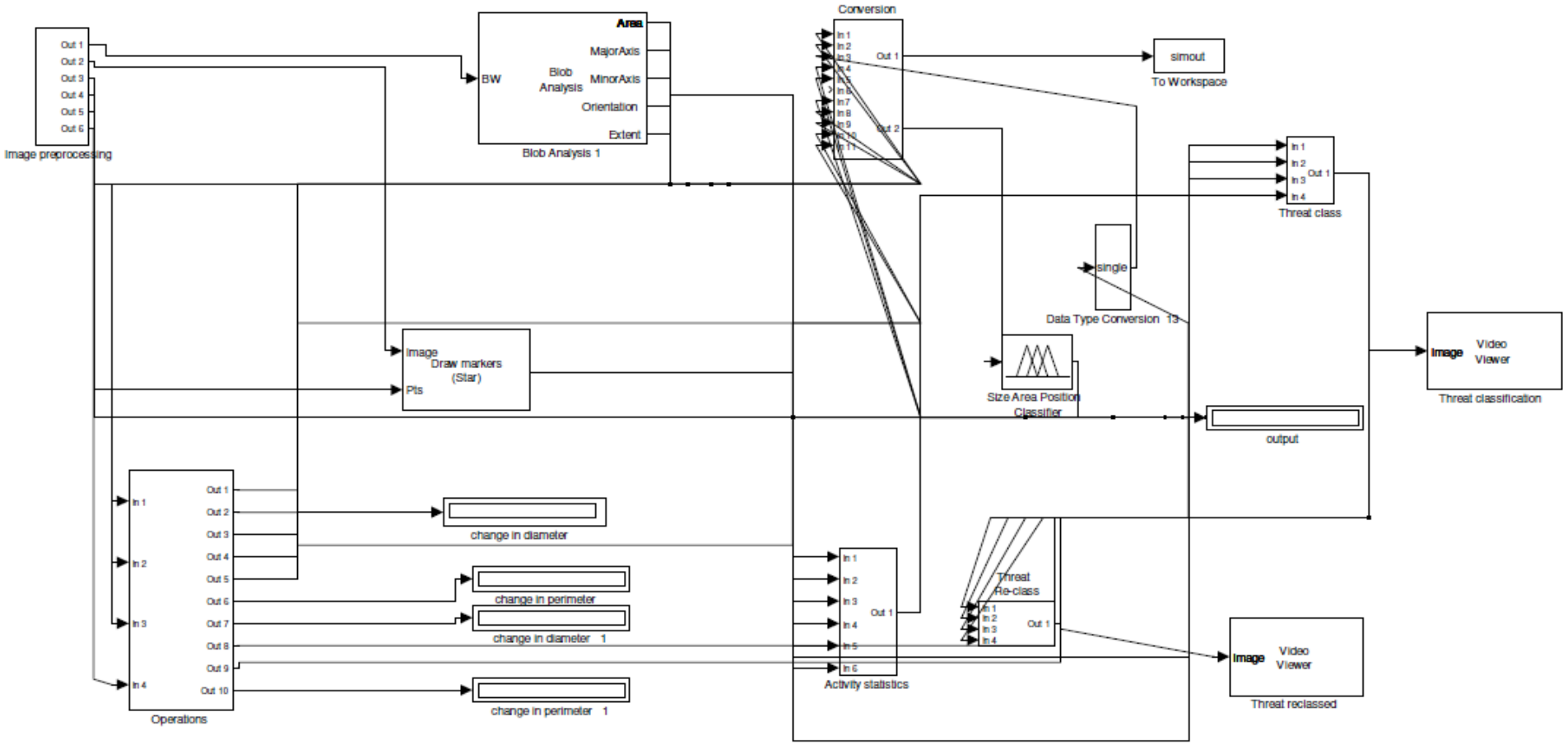


Figure 7-15 After frontal activity model

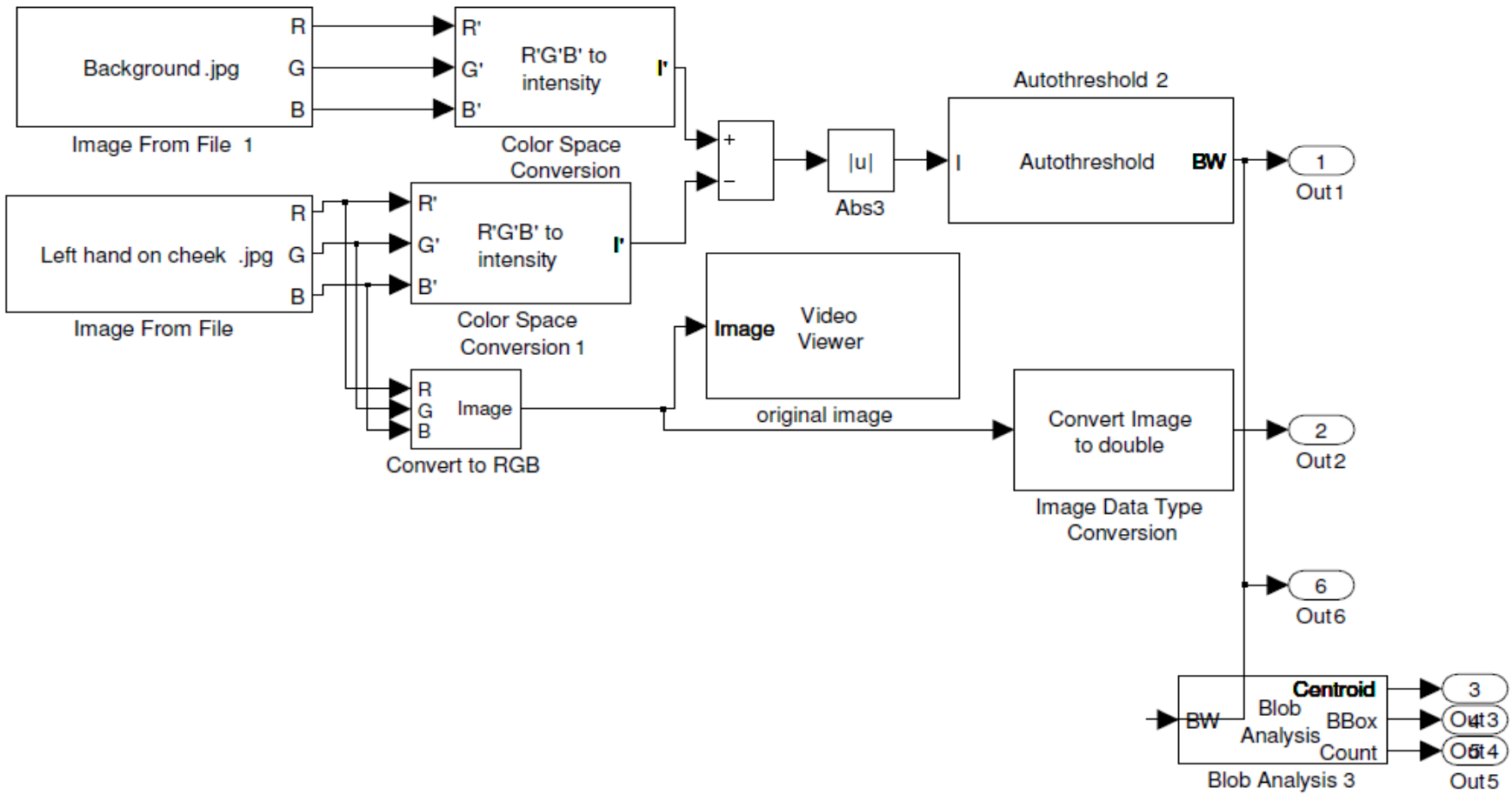


Figure 7-16 Image pre-processing subsystem

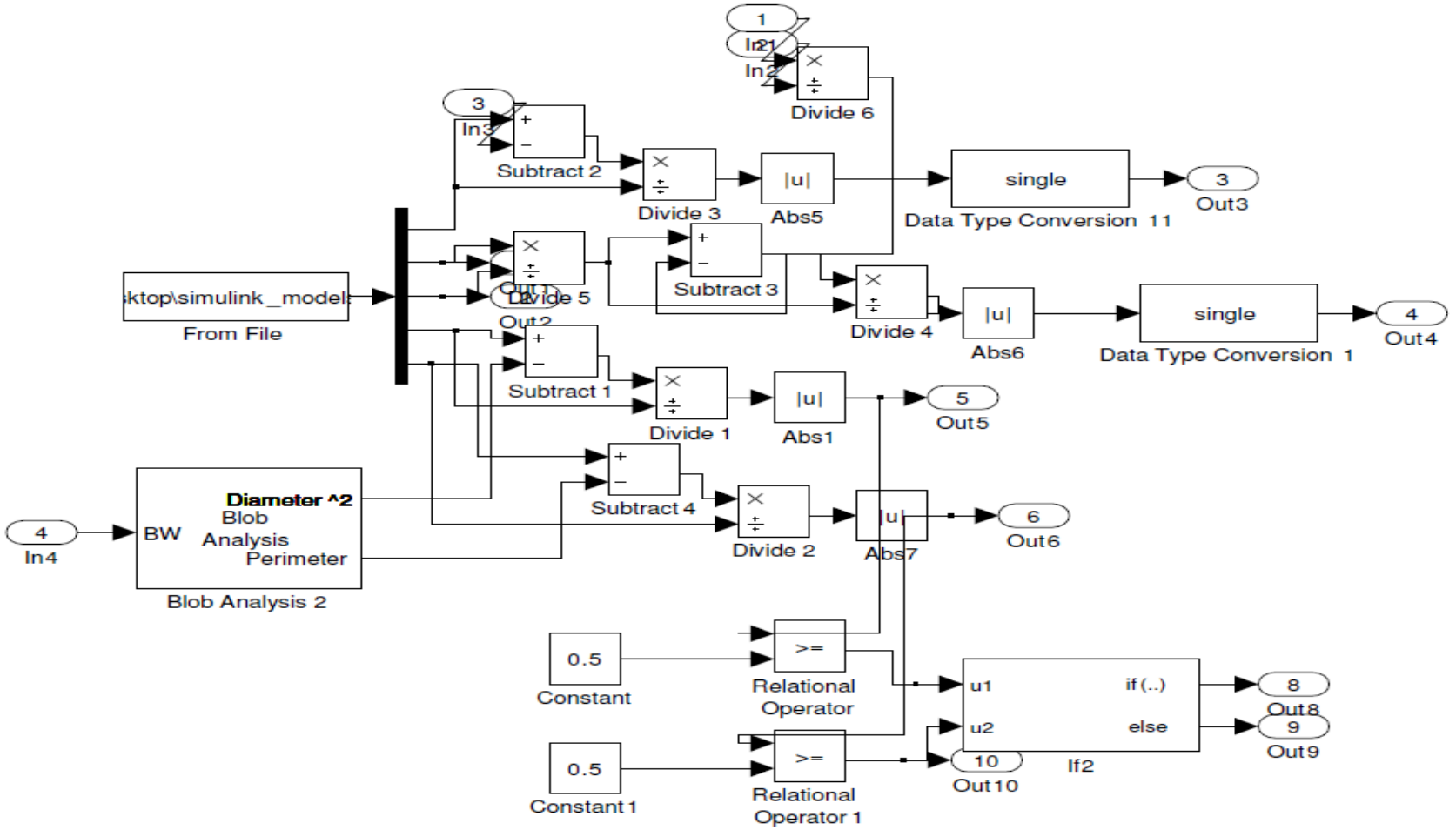


Figure 7-17 Operations subsystem

7.5.2.3 Conversion subsystem

The conversion subsystem (see Figure 7-18) work alongside the operations subsystem to ensure that the object's current blob statistics are calculated relative to the frontal pose statistics. Additionally, the subsystem ensures that the blob statistics changes are correctly fed to the risk class fuzzy engine. Lastly, the blob statistics changes are concatenated to produce a single fuzzy result.

7.5.2.4 Activity statistics subsystem

In the activity statistics subsystem (see Figure 7-19), the changes to the object's blob statistics values are recorded and displayed on the image. This action is performed on all the images received via the video sequence. The activity statistics subsystem functions alongside the operation and conversion subsystems to ensure that a single result is achieved.

7.5.2.5 Threat class subsystem

The input to the threat class subsystem (see Figure 7-20) is the single result produced by the operation, conversion and activity statistics subsystems. The result is interpreted using predefined Fuzzy logic rules and then classified using the threat classification scheme proposed section 7.3.4. These classes are the low-risk threat, elevated-risk threat and high-risk threat.

If Action subsystem

This subsystem contains the "if-then-rule" which assigns the appropriate threat classes to the single result obtained from the blob statistics.

7.5.2.6 Threat re-class subsystem

The threat re-class subsystem (see Figure 7-21) receives as input the single result which is assigned an elevated-risk threat. This subsystem is responsible for re-classing an elevated-risk threat to low-risk threat or high risk threat. The reclassification process is performed by comparing the object's perimeter and diameter statistics values with a Constant value which is defined in the Operations subsystem (see section 7.5.2.2). The outcome of comparison would determine the threat re-classification status, i.e. either a low-risk or high-risk threat.

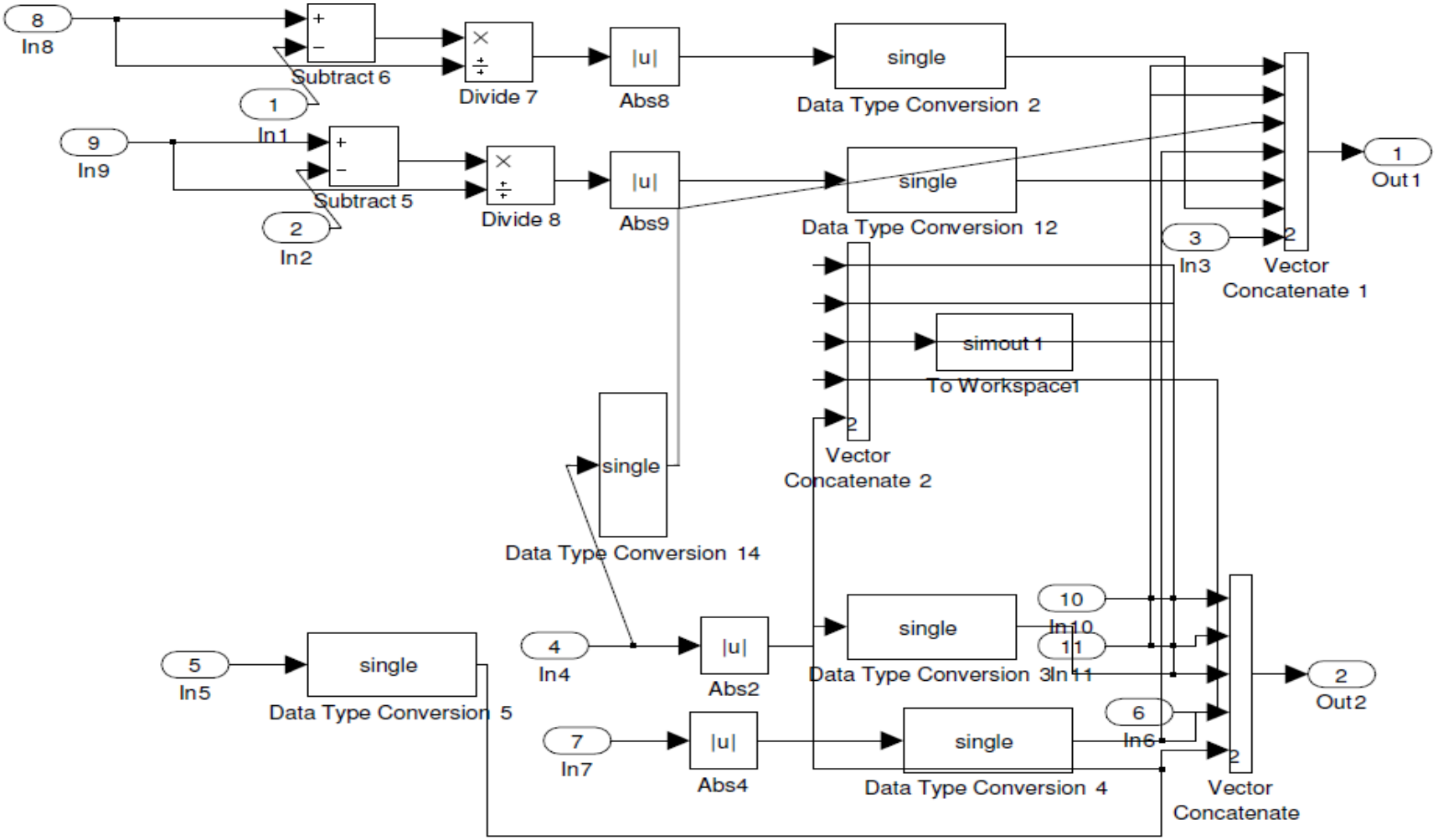


Figure 7-18 Conversion subsystem

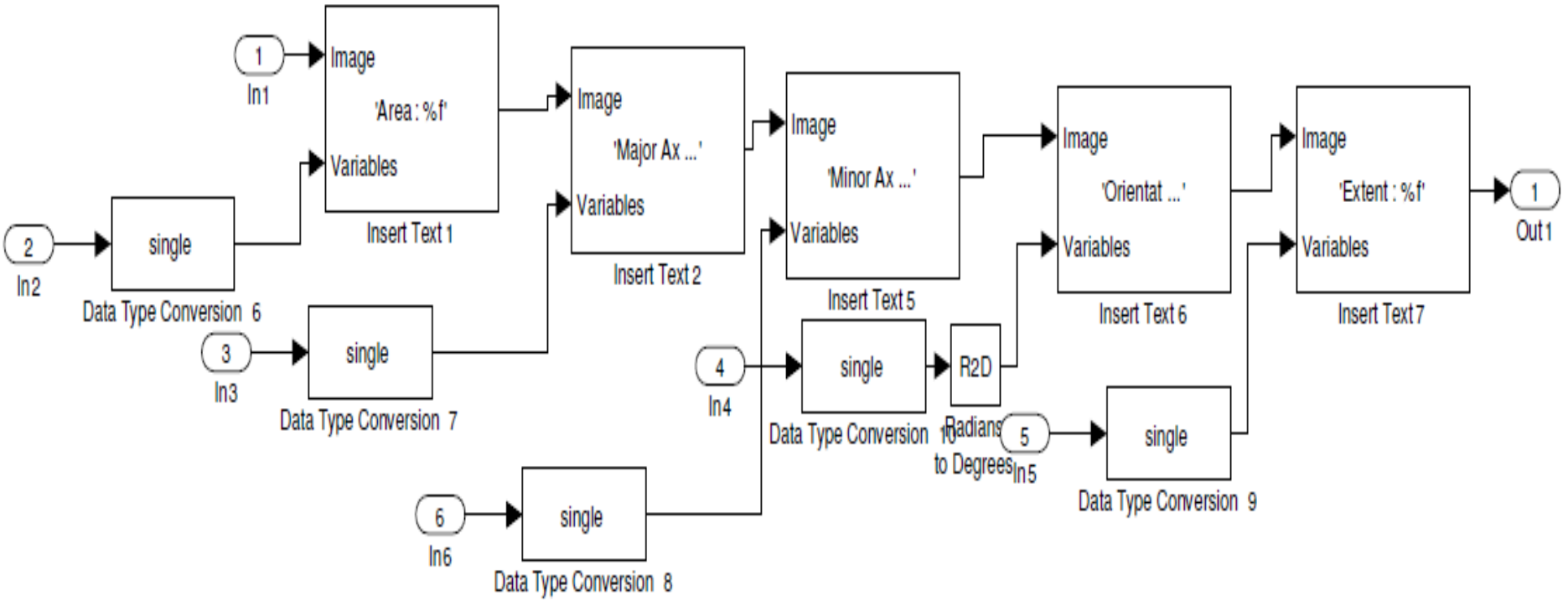


Figure 7-19 Activity statistics subsystem

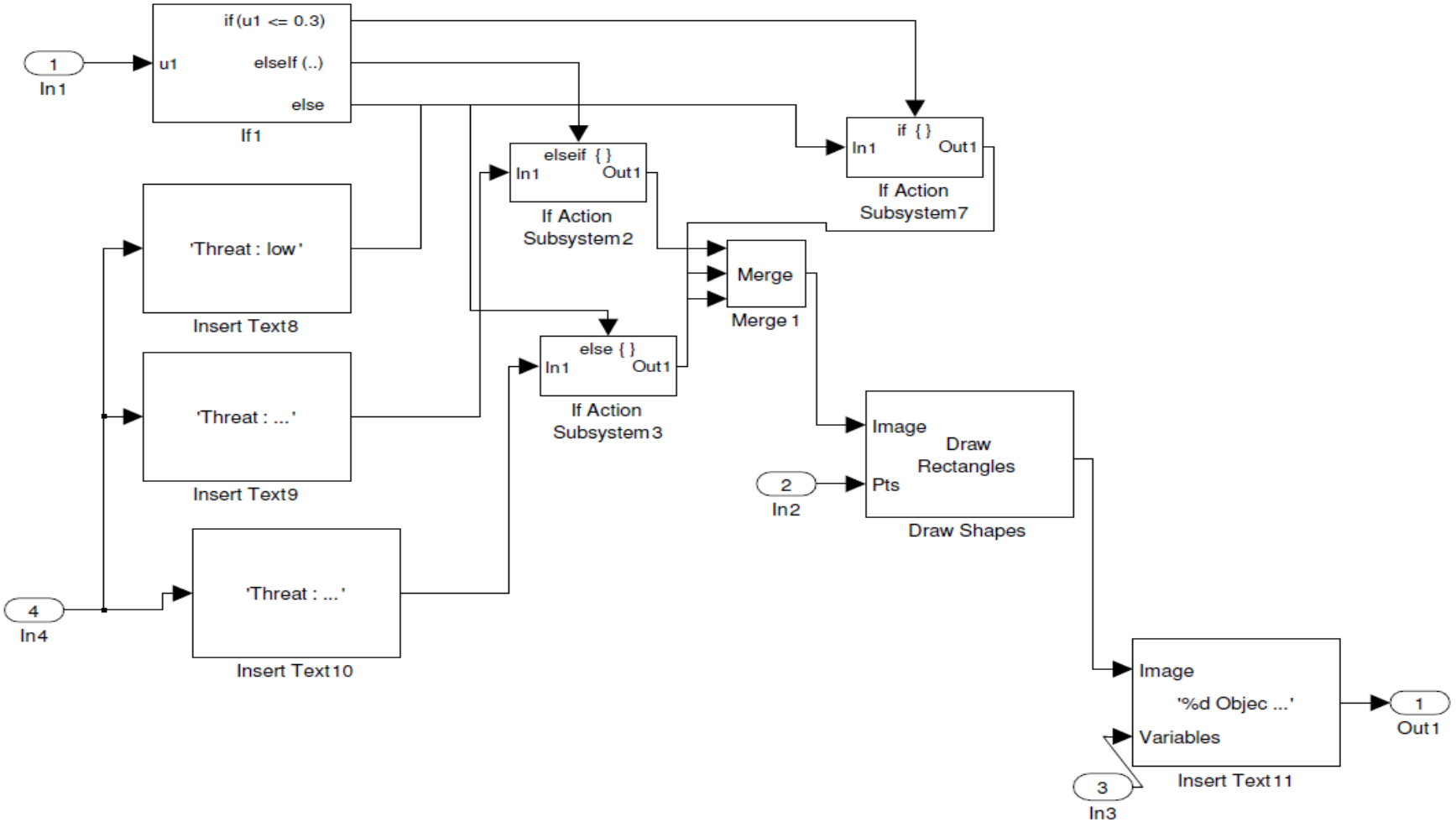


Figure 7-20 Threat class subsystem

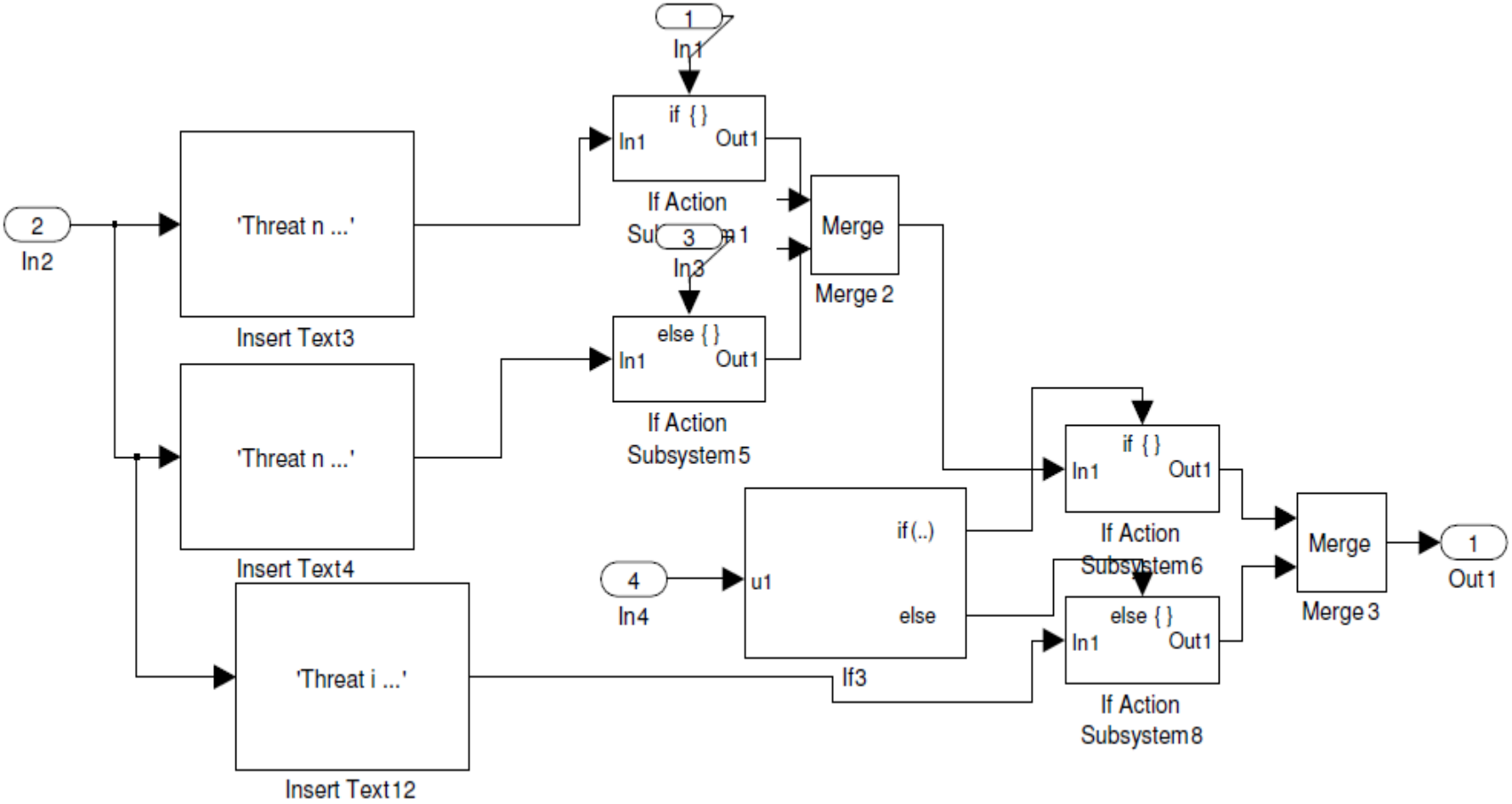


Figure 7-21 Threat re-class subsystem

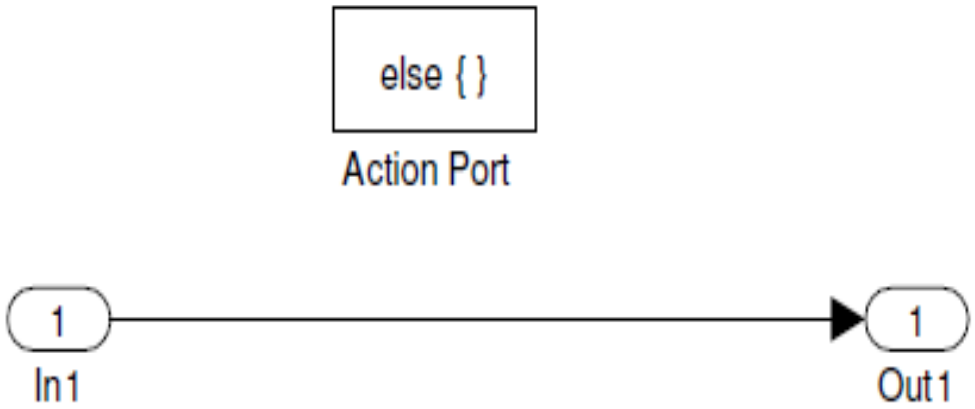


Figure 7-22 If Action subsystem

7.6 Blob Classifier Engine via Fuzzy Logic System

A fuzzy logic system (see section 6.8) refers to a nonlinear mapping from an input to the output space, i.e. maps crisp inputs to crisp outputs. The operation in a fuzzy logic system (FLS) starts with an input (crisp number) which is converted into a fuzzy set (fuzzification) Thereafter, an inference engine maps input fuzzy sets to output fuzzy sets and the FLS calculates crisp values from the fuzzy values (defuzzification). Figure 7-23 shows a block diagram of a FLS using four basic components.

7.6.1 Fuzzifier

The aim of this component is to map the degree of each input (i.e. crisp number) into appropriate fuzzy sets via membership functions. The fuzzifier is required to activate rules formulated in terms of linguistic variables and associated with fuzzy sets. According to Zadeh (1975) "linguistic variables imply variables whose values are not numbers but words or sentences in a natural or artificial language". Thus, the ability to present linguistic variables is one of the strengths of the fuzzy logic system; since numeric values can be converted to the linguistic variables which are easily understood. In the ARC approach, a fuzzy set F is defined on a universe of discourse X and is characterised by a degree of membership $\mu(x)$. Additionally, a multi-input single-output fuzzy system which performs a mapping from $U \quad R^m$ to $V \quad R$ is considered. The mapping function is defined as:

$$f : U \quad R^m \quad V \quad R \tag{7.3}$$

where $U = U_1, U_2, U_3, ..., U_n \quad R^m$ is the input space and $V \quad R$ is the output space. A single-input, single-output fuzzy system is also considered; however, the input space is reduced.

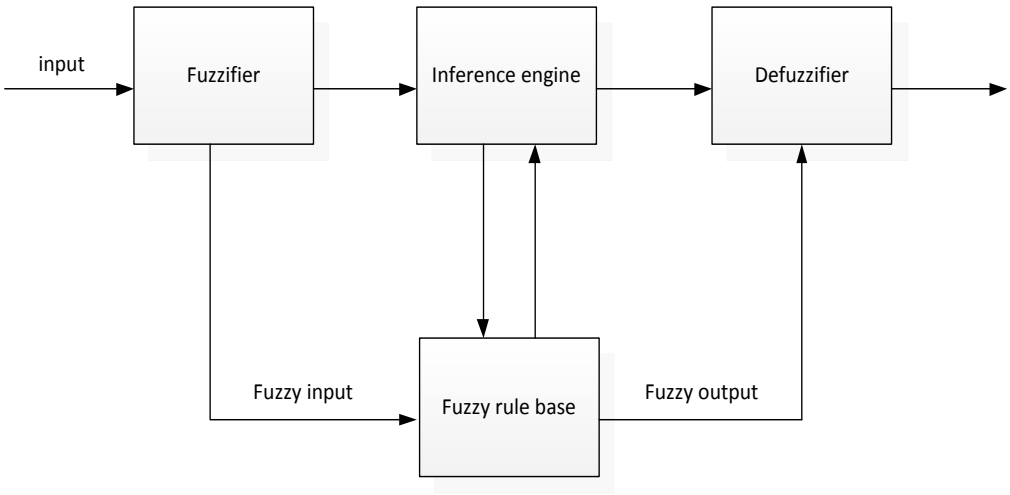


Figure 7-23 A general block diagram of a fuzzy logic system

7.6.2 Fuzzy rule base

By using the linguistic variables, fuzzy if-then-rules are formulated. Two approaches to determining rules are either through human experts or extracts from numeric data (Jantzen, 1998) and these rules are expressed as a collection of IF-THEN statements. Thus, for a given rule the following is required: select meaningful linguistic variables; quantify the linguistic variables, provide logical connections for the variables (e.g. "and", "or") and provide implications. In the ARC approach, a linguistic variable u is used to represent the numerical value x, where x is an element of X. The linguistic variable is characterised by $T(u)$ which denotes the set of names of linguistic values of x. Membership functions $\mu(x)$ come in various shapes such as triangular (trimf), trapezoidal (zmf) or Gaussian (gbellmf). Membership functions take values between 0 and 1 and define the fuzzy set. The linguistic variables and the membership functions used in the ARC approach are demonstrated in the next chapter.

7.6.3 Inference engine

This step is analogous to the way human beings use different types of inferential procedures to understand things or to make decisions. Thus, the inference engine combines the measurements of input variables with relevant fuzzy IF-THEN rules to make inferences regarding the output variable. This implies that the engine maps from input fuzzy sets into output fuzzy sets, determining the degree to which the antecedent is satisfied for each rule.

For the inference engine in the ARC approach, it is assumed that there are N rules for the fuzzy system expressed as:

$$R_i: \text{ IF } x_1 \text{ is } T_{x_1} \text{ and } x_2 \text{ is } T_{x_2} \text{ and....and } x_n \text{ is } T_{x_n} \text{ THEN } y \text{ is } C_i,\ i = 1,2,...,N,$$

where $x_i \ (i = 1,2,....,n)$ and y are the input and output variables, T_{x_i} U_i and C_i V are fuzzy sets characterised by the membership functions $\mu_{T_{xi}}(x)$ and $\mu_{C_i}(y)$ respectively. Each rule can be viewed as a fuzzy implication $T_{x_i} = T_{x_1}, T_{x_2}, T_{x_3}, ..., T_{x_n}$ C_i, which is a fuzzy set in $U \text{ X } V = U_1, U_2, ..., U_n \text{ X } V$ given by:

$$\mu_{R_i}(x,y) = \mu_{T_{x_1}}(x_1) * \mu_{T_{x_2}}(x_2) * ..... * \mu_{T_{x_n}}(x_n) * \mu_{C_i}(y) \tag{7.4}$$

where (*) is the T-norm (Zimmerman, 1996) with $x = [x_1, x_2, ...x_n]$ U and y V.

7.6.4 Defuzzifier

The defuzzification represents the final component of a fuzzy system, where the output of the fuzzy sets for each rule is combined into a single fuzzy set to make a decision. Thus, the process of combining output fuzzy sets into a single set is called aggregation (Yager, 1992). The input of the defuzzifier is the aggregate output of the fuzzy set. The goal of defuzzification is to convert the fuzzy set and output a single a real number (i.e. crisp number). The defuzzification method used in the ARC approach is the centroid defuzzifier, which converts a single fuzzy set to a crisp output value. In this method, the defuzzifier determines the centre of gravity and uses the value as the output of the fuzzy logic system (Mendel, 1995).

7.7 Justifying BlobPV in Summative E-assessment

A justification for adopting BlobPVS in summative test environments is reflected in *fairness* which is a key 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.

Interestingly, one of the benefits of adopting the BlobPVS is that presence verification would be achieved in a non-interruptive and non-distracting pattern. Recall in chapter six, one of the limitations peculiar to password and biometric solutions is the frequent re-authentication requests which gradually become interruptive and distracting to a student. However, the novelty of BlobPVS lies in the ability of the fuzzy risk class engine to initiate change-driven re-authentication requests; thus, reducing the amount of requests during a test session. The flexibility of BlobPVS 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. However, a student is interrupted when a high-risk threat class is assigned. A high-risk threat class implies that, the 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!).

7.8 Summary

This chapter presents a novel blob-based verification (BlobPV) system which can be used for presence verification in a non-interruptive and non-distracting manner. The BlobPV system employs the geometric statistics of the binary images to make inferences about an object's presence in the video frame. The system architecture of the BlobPV system is made up of four modules: the pre-processing and blob operation modules are usually the first steps in video processing applications. In the methods module, the pose estimation and activity risk classification approaches are proposed. The risk classification module forms a part of the activity risk classification and it is made up of the blob classifier engine and the threat classification scheme. In the next chapter, the pose estimation and activity risk classification approaches would be experimented using

video sequences that contain example activities. The aim of the experiments would be to (1) investigate the feasibility of using blob analysis for presence verification and (2) to decide on a suitable approach which can be adopted for the BlobPV system.

Chapter 8. BlobPV System Experiments and Results

In chapter six, it was suggested that the exclusion of presence verification from the e-assessment user security model would attract impersonation threats; thus, a novel presence verification system was proposed. The system design of the proposed blob-based system was shown in chapter seven and two approaches were introduced to evaluate the feasibility of the presence verification system. This chapter outlines the experiments that were carried out to investigate the suitability of the pose estimation and activity risk classification approaches for the BlobPV system. For each approach, the methods and experimental results are described. Hence, in this chapter the feasibility and stability of the BlobPV system is evaluated and this satisfies the third research goal of this thesis.

8.1 Experimental Design

The aim of these experiments was to determine which of the two approaches discussed in chapter seven would be suitable for carrying out presence verification in a simple and accurate way. The first two experiments focus on the pose estimation approach, whilst the third and evaluation experiments were focused on the activity risk classification approach. The three experiments and evaluation experiments were implemented in Matlab/Simulink R2008b running on a 64-bit operating system with a 2.40GHz processor speed and a 4GB memory. The following sections below describe the experimental setup.

8.1.1 Activity examples

Recall in chapter seven, a list of possible student activities was introduced alongside the relevant blob statistics proposed for the BlobPV system. Thus, to investigate the validity of the activities suggested in Table 7-1, informal interviews were conducted with students from the School of Electronics and Computer Science at the University of Southampton. The informal interviews were also aimed at eliciting possible acceptable and unacceptable student activities during an online test. Many of the interviewees agreed with the activities in Table 7-1 and a few more activities were suggested to buttress the previous examples. It should be noted that, possible student activities in a test environment would vary from individual to individual; thus, it is impossible to cover all the possible cases that may occur. However, the list of activities used in the experiments was compiled using excerpts from the interviews.

8.1.2 Datasets

To demonstrate the efficacy of the BlobPV system for e-assessment presence verification the proposed approaches for detecting and deducing correctly a student's presence status have been evaluated on newly recorded video sequences which contain a variety of activities and scenarios. The choice of collecting fresh video sequences was as a result of unavailable public data which contained the activities and scenarios required for the experiments. The experiments were applied on a set of five video sequences involving two undergraduate and three postgraduate students at the University of Southampton. The datasets were filmed in an indoor environment with the five people (one person in each) simulating the activities in a natural test environment; thus, the students 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. For example, converting a 2mins and 30secs video sequence produced approximately 14,600 video frames; thus, extracting the required video frames for analysis was useful. In reality, a video sequence is a series of video frames and each frame can be considered as an image. Thus, when

analysing a continuous video sequence, it is important to use discrete video frames to initially model the video.

Additionally, calculating a sample size for the experiments did not require analytical methods, as it was determined that a widespread testing of many volunteers is unnecessary since the experiments is aimed at testing the two presence verification approaches from a system's perspective. Thus, the human-role in the experiments is to simulate specific activities and scenarios which would serve as an input for analysing the suitability of the approaches and the feasibility of implementing the BlobPV system. Hence, the sample size *n=5*, was chosen randomly where two of the video sequences were used as trial data and the remaining three videos for testing/evaluation. This implies that a sample size of *n=4* or *n=10* would produce similar results. More importantly, it should be noted that, the datasets were collected independent of variables such as hat size, skin colour, lighting, gender, age or race. This is quite useful since the research exploits the geometric properties of binary images (i.e. 0s or 1s); thus, these variables are considered extraneous for these experiments.

8.2 Pose Estimation Approach

The pose estimation approach has been evaluated on two video sequences represented as Object A and Object B. These datasets are used for trial purposes.

8.2.1 Pose estimation from blob orientation: Experiment 1

The first stage in an object tracking application is the detection of moving objects from the background via the background subtraction method. In this technique, moving objects are detected by taking the difference between the current image and the static background image in a pixel-by-pixel manner:

$$\left| I_t\left(x,y\right) - B_t\left(x,y\right) \right| > T \tag{8.1}$$

An autothreshold operation was employed to convert the intensity image to a binary image and an 8-connected component analysis method is used to extract the blob from the binary image. Figure 8-1 shows the results of the background subtraction followed by the blob extraction. In addition, it is observed that the background subtraction and blob extraction processes was not affected by the conspicuous sharp edge reflected in the

background image. The sharp edge was left intentional in order to observe the effect of an unclear background on the experiments

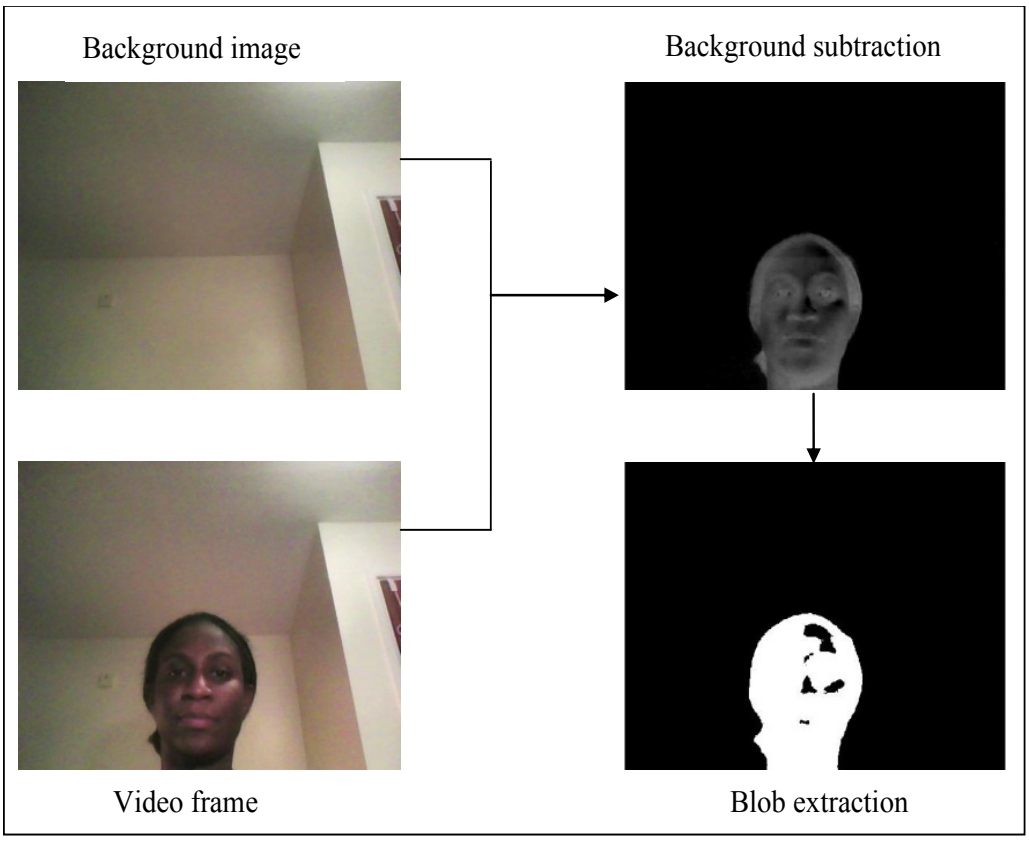


Figure 8-1 Object detection and Blob extraction

Having detected moving objects using object segmentation algorithm, the next step is to extract and verify the relevant blob statistics over a sequence of frames. Recall in chapter six, the blob orientation measures the angle between the major axes of the ellipses and the x-axis. Thus, it is assumed that when an object is looking forward, an orientation of approximately 90^0 (1.57 radians) would be obtained. Thus, it is suggested that an object's frontal pose can be estimated from the blob orientation value. A diagrammatic illustration of an object's frontal pose orientation value range is shown in Figure 8-2. Additionally, Figure 8-3 shows the same object tilting towards the left and right respectively. Hence, it was suggested that by relying on the orientation statistic values there exists a possibility to estimate the object's direction. Therefore based on this suggestion, the first experiment was aimed at comparing an object's frontal blob area statistics with its current pose area statistics to demonstrate whether an initially detected

object is the same object with a different pose/direction or to determine whether an external object is within the camera's view. That is:

$$A_0 = A_1 = A_2 \tag{8.2}$$

where A_0 is the blob area statistic value for frontal pose in Figure 8-2, A_1 and A_2 are the blob area statistic value for left and right tilt direction in Figure 8-3. The first experiment is evaluated on the video sequence which contain Object A only. Thus, Object A's current pose blob statistics which is pooled from seven different activities is compared relative to Object's A initial frontal pose blob statistics. Table 8-1 shows Object A's blob statistics from the following: the frontal, right hand on cheek, left hand on cheek, lean on right, lean on left, tilt head, look right and look left activities. Additionally, the percentage changes in the area and perimeter blob statistics relative to the frontal area and perimeter statistics are also recorded.

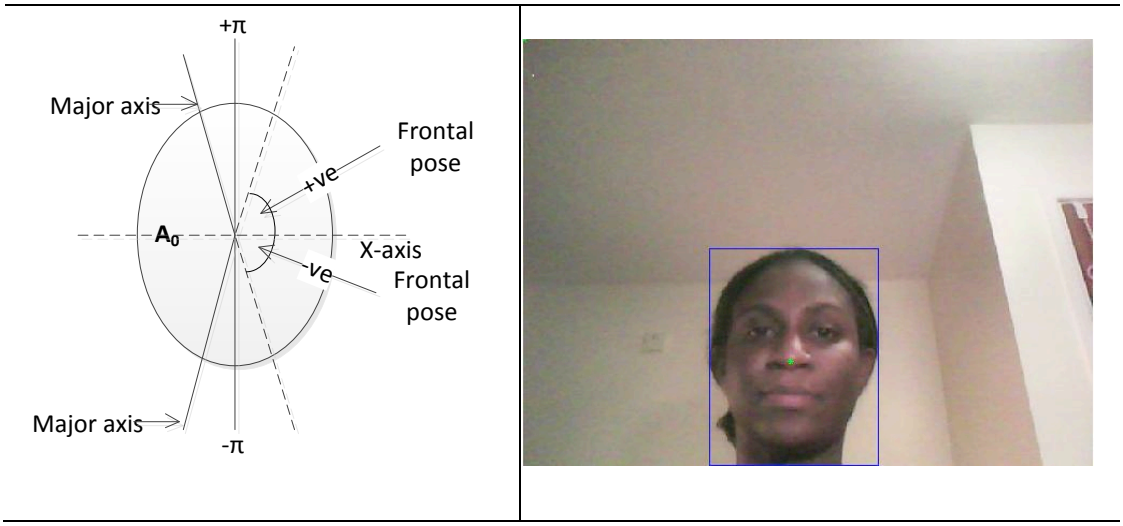


Figure 8-2 Object frontal pose estimation from ellipse (blob) orientation

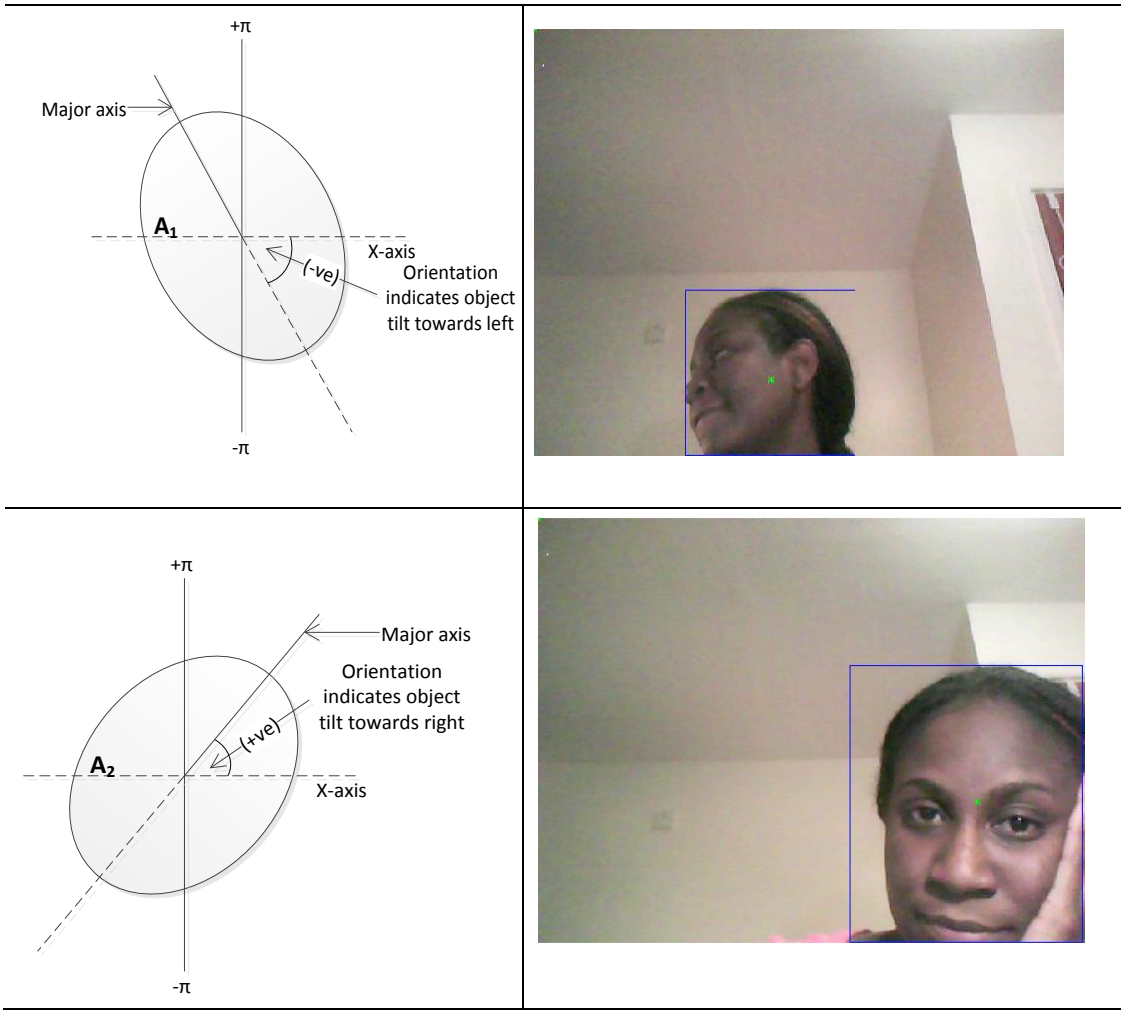


Figure 8-3 Orientation suggests object is tilting (a) left and (b) right

Frame Activity	Area	% change in area	Perimeter	% change in perimeter	Orientation (rad/deg)	
Frontal pose	34486	0	778.9848	0.00	1.52	87.16
Right hand on cheek	54992	59.46	1220.365	56.66	-1.23	-70.51
left hand on cheek	41288	19.72	1231.578	58.10	1.12	64.16
Lean on right	28228	-18.15	1694.823	117.57	-1.57	-89.7
Lean on left	59275	71.88	1132.926	45.44	1.35	77.38
Tilt head	10293	-70.15	411.7645	-47.14	-0.03	-1.52
Look right	31982	-7.26	744.1148	-4.48	-0.34	-19.49
Look left	48990	42.06	1182.749	51.83	0.24	13.83

Table 8-1 Object A blob statistics

The visual inspection of Table 8-1 and Figure 8-4 shows that the orientation statistics reflects the object's position in the frame. For instance, it is noticed that the

orientation statistics of "lean on right and look right" activities produce negative values i.e. -89.7deg & -19.49deg. Similarly, in the "tilt head" activity, it is observed that Object A is almost at a horizontal position, i.e. -1.52deg as opposed to the normal vertical position expected. Thus, the above observation shows that it is feasible to estimate an object's position from the blob orientation statistics.

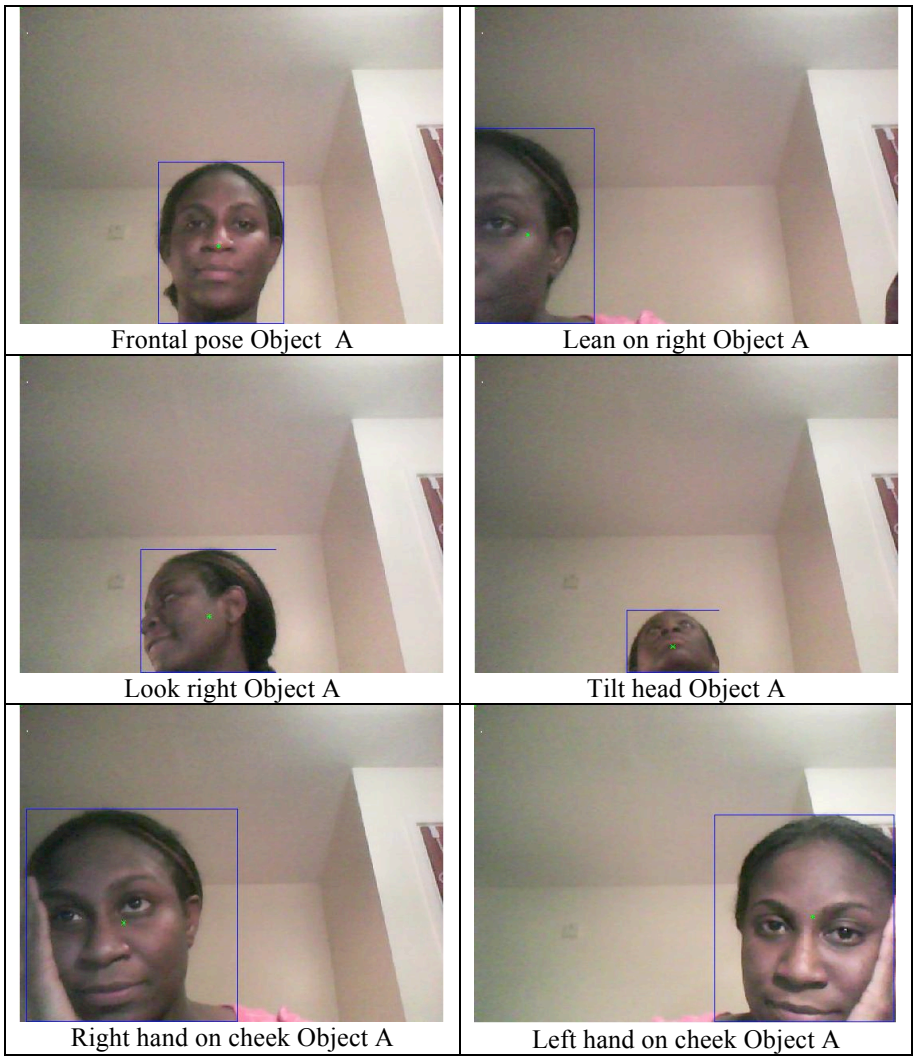


Figure 8-4 Object A frame activities

From Table 8-1 a significant variation in the percentage changes of the area and perimeter statistics with respect to the frontal area and perimeter statistics is observed. This suggests that, the dissimilar statistics is attributed to the inconsistency of the detectable features on the object. Detectable features refer to the features that are capable of being detected as a result of the object's pose. For example, it is noticed that the "right and left hand on cheek" activities (Figure 8-4), show a significant increase in the area and perimeter statistics. Thus, it is suggested that the increase in the area and perimeter

statistics is as a result of the additional "right and left hand" placed on the cheek. Additionally, the decrease in the area statistics for the lean on right and tilt head activities is be linked to a reduction of the noticeable features on the object (Figure 8-4). Furthermore, the dissimilar blob statistics can occur as a result of the distance (in metres) of the detectable features from the camera's view; however, the distance of the features depends on the distance (metres) of the object from the camera. For example, it is observed that the there is a ~72% increase in area statistics on the "lean on left" activity, whilst the "lean on right" activity show a ~18% reduction in area statistics. Hence, the dissimilarity in the percentage changes suggests an inconsistency in the object's distance to the camera; thus, affecting the distance of the detectable features.

8.2.2 Stability of blob statistics: Experiment 2

Table 8-1 above shows that an object's area, perimeter and orientation blob statistics is likely to change due to varying activities which can influence an object's pose. Thus, the second experiment was designed to investigate the relative stability of the blob statistics across two different objects performing similar activities. Additionally, the percentage changes in the blob statistics relative to the frontal statistics for the two objects are compared to determine stability. This is illustrated in the equation below:

$$\%P_{F[A]}P_{X[A]} \qquad \%P_{F[B]}P_{X[B]} \tag{8.3}$$

where $\%$ is the percentage change, $P_{F[A]}$ is the blob statistics for object A's frontal pose and $P_{X[A]}$ is the blob statistics for object A's current pose. Similarly, $P_{F[B]}$ is the blob statistics for object B's frontal pose and $P_{X[B]}$ is the blob statistics for Object B's current pose. Thus, it is assumed that suppose the relationship in Equation 8.2 exists, then it would be feasible to estimate the poses of tracked objects using blob analysis. Hence, for a summative e-assessment the existence of Equation 8.2 would allow continuous real-time tracking and pose detection of the student during the test. For this experiment, Object A and Object B video sequences are analysed and the percentage changes in blob statistics with respect to the frontal pose statistics is compared. Table 8-2 shows the blob statistics obtained for the two Objects and in Table 8-3, the percentage changes for the blob statistics are shown.

Frame Activity	Object	Area	Major axis	Minor axis	Extent	Perimeter	Diameter
Frontal pose	A	34486	253.37	189.37	0.74	778.99	43908.90
	B	48433	313.54	209.35	0.62	1863.25	61666.80
Right hand on cheek	A	54992	382.38	266.75	0.53	1220.36	70018.00
	B	35719	353.14	209.35	0.62	2361.93	45478.80
left hand on cheek	A	28228	336.26	169.98	0.53	1694.82	35941.00
	B	31156	251.83	170.29	0.78	771.563	39669.10
Lean on right	A	28228	336.26	169.98	0.53	1694.82	35941.00
	B	44837	300.66	210.30	0.77	915.26	57088.20
Lean on left	A	59275	320.82	253.86	0.79	1132.93	75471.30
	B	35113	251.94	202.63	0.74	975.49	44707.30
Cover face	A	39216	296.46	230.55	0.70	898.30	49931.40
	B	36523	294.65	246.84	0.55	2140.61	46502.5
Touch head	A	36106	241.70	220.95	0.75	1350.15	45971.60
	B	43485	265.12	249.55	0.51	1347.50	55366.80
Look right	A	31982	211.98	196.52	0.83	744.12	40720.70
	B	48467	266.45	245.30	0.76	958.68	61710.10
Look left	A	48990	299.86	229.92	0.70	1182.75	62376.00
	B	49977	274.77	248.63	0.74	1089.80	63632.70
Head on table	A	20082	226.35	133.02	0.50	769.65	25569.20
	B	97329	458.29	292.48	0.78	1812.15	123923.00

Table 8-2 Object A and Object B blob statistics

Frame Activity	Object	% change in area	% change in major axis	% change in minor axis	Extent	% change in Perimeter	% change in Diameter
Frontal pose	A	0.0	0.0	0.0	0.74	0.0	0.0
	B	0.0	0.0	0.0	0.62	0.0	0.0
Right hand on cheek	A	59.5	50.9	40.9	0.53	56.7	59.5
	B	-26.3	12.6	-17.2	0.62	26.8	-26.3
left hand on cheek	A	-18.1	44.1	39.8	0.53	58.1	19.7
	B	-35.7	-19.7	-32.6	0.78	-58.6	-35.7
Lean on right	A	-18.1	32.7	-10.2	0.53	117.6	-18.1
	B	-7.4	-4.1	-16.8	0.77	-50.9	-7.4
Lean on left	A	71.9	26.6	34.1	0.79	45.4	71.9
	B	-27.5	-19.6	-19.8	0.74	-47.6	-27.5
Cover face	A	13.7	17.0	21.7	0.70	15.3	13.7
	B	-24.6	-6.0	-2.4	0.55	14.9	-24.6
Touch head	A	4.7	-4.6	16.7	0.75	73.3	4.7
	B	-10.2	-15.4	-1.3	0.51	-27.7	-10.2
Look right	A	-7.3	-16.3	3.8	0.83	-4.5	-7.3
	B	0.1	-15.0	-3.0	0.76	-48.5	0.1
Look left	A	42.1	18.3	21.4	0.70	51.8	42.1
	B	3.2	-12.4	-1.6	0.74	-41.5	3.2
Head on table	A	-41.8	-10.7	-29.8	0.50	-1.2	-41.8
	B	101.0	46.2	15.7	0.78	-2.7	101.0

Table 8-3 Percentage changes of Object A and Object B blob statistics

The visual inspection of Table 8-3 reveals a trend in the dissimilar change statistics for Objects A and B performing similar activities. To illustrate this, Figure 8-5 show the initial frontal poses of Objects A and B; the frontal poses represents a reference which is used to estimate the change in blob statistics.

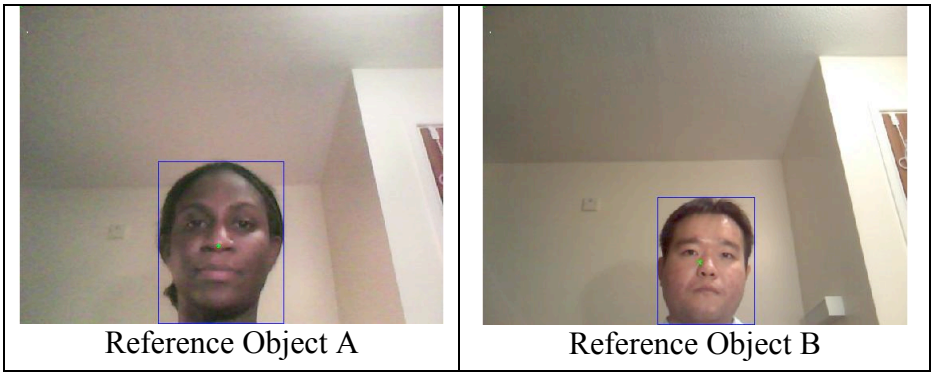


Figure 8-5 Reference poses: Object A and B

Figure 8-6 show the "right hand on cheek" activity for Objects A and B respectively. A visual inspection shows that ~59.5% increase in Object A's blob area statistics values whilst the area statistics of Object B was reduced ~26.3% for the same activity. The increase in Object A's blob area is explained by the change in the object's position from the initial pose (Figure 8-5) relative to the cameras field of view. In addition, the increase is also reflected by Object A's hand to the image detected.

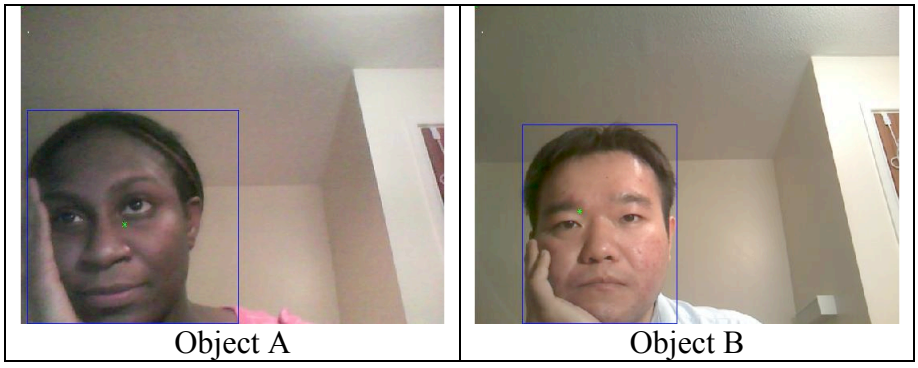


Figure 8-6 Right hand on cheek: Object A and B

In Figure 8-4b the "look left" activity shows ~42% increase in the blob area for Object A whilst a 3.2% increase is recorded for Object B. By comparing the reference images (Figure 8-5) with the activity look left images (Figure 8-7), it is suggested that the increase in blob area is as a result of the camera capturing a larger object size when an object looks left (or right) as opposed to when the object is looking straight.

Additionally, it is required that the object's position in reference to the cameras field of view is constant; otherwise, the inconsistency would produce an increase (or decrease) in blob area.

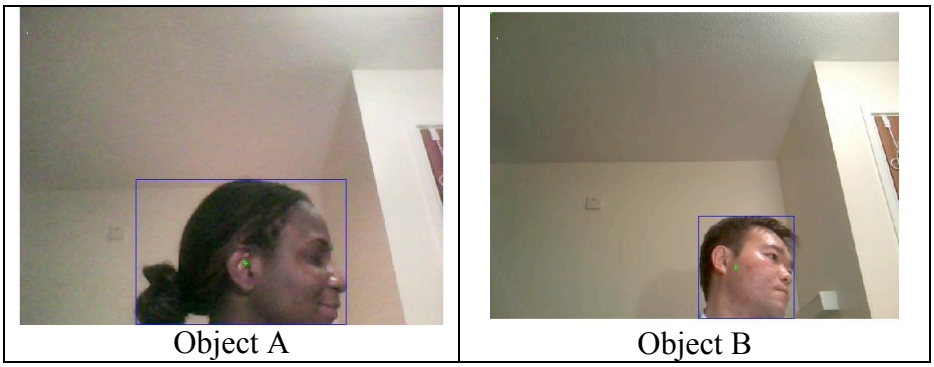


Figure 8-7 Look left: Object A and B

In a similar trend, the "head on table" activity shows a 41% reduction in blob area for Object A and a 101% increase for Object B (Figure 8-8). This is as a result of decrease (Object A) and increase (Object B) in the object's size within the camera's field of view.

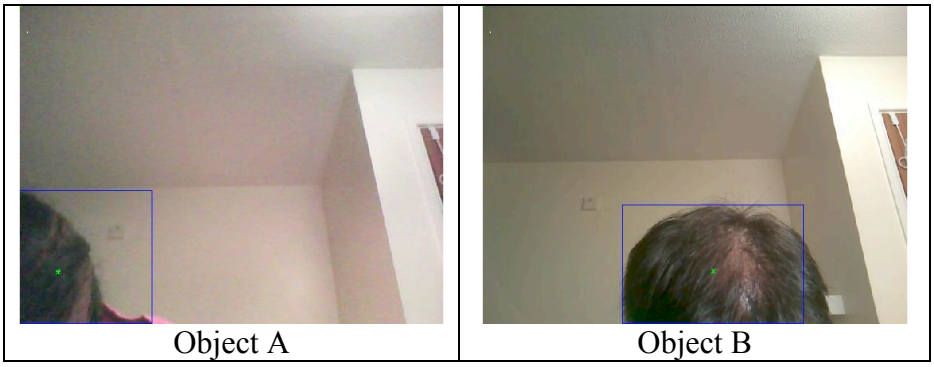


Figure 8-8 Head on table: Object A and B

From the above experiment, it is seen that the change in the blob statistics does not reveal the exact activities which is performed in the video frame. However, it is observed that by comparing an object's reference pose and current pose, the changes in the object's position and size relative to the camera's field of view can influence the similarity of the two poses. Hence, to adopt the pose estimation approach the object's activities must be controlled, such that an object's pose in a reference image and current image is similar. It should be noted that, this requirement is impractical for a test

environment as the student will be required to 'look and act' in a predetermined or constrained manner.

Therefore, to eliminate the constraints on the student's activity and allow for passive student monitoring, the deterministic pose estimation approach is relaxed to accommodate an activity risk classification. Additionally, from the initial experiments it is noticed that the blob statistics reveal significant information relating to an object's position, size, shape and extent. Thus, this information can be exploited to classify the potential risk of an object's activity; rather than, determining the object's actual pose/activity in a video frame. An experiment to determine the feasibility and suitability of the activity risk classification approach is reported later in the chapter.

8.2.3 Summary of initial results

One of the lessons learned from experiment 1 is the feasibility of detecting an objects frontal pose from the blob orientation. The orientation statistics is advantageous, as an object's frontal pose statistic values is used as a reference point to estimate the changes in statistic values from other activities. However, the two limitations of adopting pose estimation approach are the inability to determine the *sameness* property of the object irrespective of varying activities and the instability of the blob statistics values across two or more objects performing a similar activity.

In this context, the sameness attribute refers to the ability of a verification system to determine that the object detected in the first frame is the same object detected in the current frame. Establishing the sameness attribute using the pose estimation approach shows that the direct estimation of an object's pose/activity from the video frame is non-trivial. From the experiments, it is observed that this limitation occurs as a result of the inconsistencies in the blob statistic values, influenced by an object's varying positions and sizes relative to the cameras field of view. Additionally, a second experiment was carried out to investigate the stability of the blob statistics across different objects performing similar activities. The results from this experiment also revealed dissimilar blob statistic values across the two objects as a result of varying positions and sizes of the objects to the cameras field of view. Hence, findings from the initial experiments reveal inconsistencies in an object's blob statistics due to varying positions and size in the environment.

8.3 Activity Risk Classification (ARC) Approach

The ARC approach does not aim to detect an object's exact activity from the video frames, e.g. "right hand on cheek" or a "tilt head"; rather, the approach uses a combination of blob statistics to determine the likelihood of an acceptable or unacceptable activity in the environment. Thus, individual blob statistics (such as area, orientation, major axis, minor axis and extent) 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 means that the change in the blob statistics of the current activity is a function of the frontal pose of the same object and this is illustrated in equation 8.3:

$$\Delta P_{X[A]} \quad f\left(P_{F[A]}\right) \tag{8.4}$$

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 blob statistics used in the ARC approach also represents the five input variables required for the fuzzy blob classifier engine described in section 7.6. These variables are *size (area), shape (major axis/minor axis), position (orientation), extent and count.*

8.3.1 Deriving Numeric Range Values via Heuristics

The ARC fuzzy logic system was built with five input variables (size, shape, position, extent and count) and one output variable. Recall the proposed threat classification scheme in section 7.3.4, i.e. the low-risk threat class, the elevated-risk threat class and the high-risk threat class. Thus, 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. Firstly, it is important to derive the numeric values x of the input variables X, where the value x is an element of the variable X and the linguistic variables $T(u)$ are defined for each input variable X. The numeric range values of the input variables 'size' and 'shape' are derived heuristically from the blob statistics of

Object A and B performing similar acceptable and unacceptable activities in the environment.

Table 8-4 show the initial values of Object A and B's blob size & shape and the percentage changes in the blob size & shape. Additionally, Table 8-4 shows the percentage changes when Object B's blob statistics is analysed with respect to Object A's frontal statistics and vice versa. Similarly, the swap is also applied to percentage change in the shape values. In the columns which represent the % change in size and % change in shape, it is observed that the percentage changes recorded for the frontal pose activities of Object A and B is '0.0' and'0.0' respectively. This shows that Object A and Object B's blob size and shape produce no-change which can infer the sameness of the object. However, in the columns which represent the % change in size (swap) and % change in shape (swap) there is a significant change which reveals the swap in the frontal pose blob statistics.

For example, given Object A's frontal pose statistics as a reference; the percentage change in blob size for the "face to camera" activity relative to the frontal pose statistics is calculated as:

$$\frac{Size\ \text{frontal pose of object A - size face to camera object A}}{\text{size frontal pose of object A}} x100 \qquad (8.5)$$

The % change in size statistics derived as shown in Equation 8.5 is recorded. Similarly, the percentage change in size (swap) when using Object B's 'face to camera' blob statistics with reference to Object's A frontal pose statistics is shown in Equation 8.6 is recorded.

$$\frac{Size\ \text{frontal pose of object A - size face to camera object B}}{\text{size frontal pose of object A}} x100 \qquad (8.6)$$

Frame Activity	Object	Size	% change in size	% change in size (swap)	Shape	% change in shape	% change in shape (swap)
Frontal pose	A	34486	0.0	28.80	1.337963	0.00	10.66
	B	48433	0.0	-40.44	1.497683	0.00	-11.94
External person behind Object	A	31617	-8.32	34.72	1.180338	11.78	21.19
	B	37403	-22.77	-8.46	1.231152	17.80	7.98
External person beside Object	A	71456	107.2	-47.54	1.759964	-31.54	-17.51
	B	90805	87.49	-163.31	1.313292	12.31	1.84
Face to camera	A	70746	105.14	-46.07	1.693476	-26.57	-13.07
	B	66457	37.21	-92.71	1.464312	2.23	-9.44
Cover face	A	39216	13.72	19.03	1.285882	3.89	14.14
	B	36523	-24.59	-5.91	1.193688	20.30	10.78
Touch head	A	36106	4.69	25.45	1.093913	18.24	26.96
	B	43485	-10.22	-26.09	1.062392	29.06	20.60
Look right	A	31982	-7.26	33.97	1.078669	19.38	27.98
	B	48467	0.07	-40.54	1.086221	27.47	18.82
Look left	A	48990	42.06	-1.15	1.304193	2.52	12.92
	B	49977	3.18	-44.92	1.105136	26.21	17.40
Head on table	A	20082	-41.77	58.54	1.701624	-27.18	-13.62
	B	97329	100.96	-182.23	1.566911	-4.62	-17.11

Table 8-4 Percentage changes for size and shape input variables

A visual inspection of Table 8-4 shows that the percentage changes computed from the blob statistics follow a simple trend and can be categorised. In the column, which represents Object A and B's % change in size, 9 out of the 18 statistics show changes within *0 - 30%* whilst the remaining 9 values lie within the range *31 – 60%*. Similarly, in the % change in shape column, 17 out of 18 statistics reflect changes within the range of *0 - 30%*. However, the % change in size (swap) column depict that, 5 statistics fall within the range *0 - 30%*, whilst the remaining 13 statistics show changes > *30%*. The % change in shape (swap) column shows 2 statistics within the range of *0 - 10%*, whilst the remaining 16 statistics show changes >*10%*.

Thus, it can be concluded that the changes in blob size which fall within *0 - 30%* show a high possibility that the object detected is the original object, hence a low-risk threat class. However, changes within the range *31 – 65%* suggest that the original object is engaged in suspicious activities, hence an elevated-risk class. Additionally, changes in blob size which are >66% suggest a likelihood of a change in the original object, hence a high-risk threat class. Similarly, the changes in the object's shape which lie within the range *0 - 10%* suggest a low-risk, *11% – 30%* suggest an elevated-risk and the *31% - 100%* suggest a high-risk threat class. Therefore, the numeric values x of the input variables X is categorised and shown in Table 8-5. For this thesis, the linguistic variables $T(u)$ defined for the input variables take on three terms *{low, elevated, high}*. The linguistic variables represent the derived range of numeric values.

	Input variables	
Linguistic variables	**Size**	**Shape**
Low	0 – 30%	0 – 10%
Elevated	31% – 65%	11% – 30%
High	>66%	31% - 100%

Table 8-5 Size and shape numeric values

Frame Activity	Object	% change in size	% change in shape	Position	Extent
Frontal pose	A	0.0	0.00	1.5212282	0.74
	B	0.0	0.00	-1.485541	0.62
External person behind Object	A	-8.32	11.78	-1.550529	0.74
	B	-22.77	17.80	-1.473013	0.61
External person beside Object	A	107.2	-31.54	0.0520501	0.72
	B	87.49	12.31	0.4425047	0.61
Face to camera	A	105.14	-26.57	-1.180514	0.40
	B	37.21	2.23	-1.239024	0.46
Cover face	A	13.72	3.89	-1.564642	0.70
	B	-24.59	20.30	1.2458946	0.55
Touch head	A	4.69	18.24	-0.273931	0.75
	B	-10.22	29.06	-0.107549	0.51
Look right	A	-7.26	19.38	-0.340247	0.83
	B	0.07	27.47	0.2474963	0.76
Look left	A	42.06	2.52	0.2414605	0.70
	B	3.18	26.21	-0.310793	0.74
Head on table	A	-41.77	-27.18	-1.087535	0.50
	B	100.96	-4.62	-0.033249	0.78

Table 8-6 Position and extent input variables

Similarly, from Table 8-6 the range of values for the input variables position and extent is defined. It should be noted that, the position and extent variables are capable of explicitly detecting potential object poses; thus, it is impractical to consider their percentage changes as implemented for the size and shape variables. Hence, for the position variable, an orientation statistics of the range *1.22 – 1.57 radians* suggest that the object is 'looking straight' or at a perpendicular angle to the camera's field of view, e.g. an object's "frontal pose" activity. In a test environment, it is expected that the object would constantly assume a posture that is perpendicular to the camera's field of view when taking a test. Therefore, values that lie within the perpendicular angle range are acceptable. Additionally, when an object's pose is tilted (e.g. 45^0) relative to the camera's field of view, this indicates that the range is within *0.87 – 1.20 radians*. In reality, an object could have a tilted pose as a result of a 'look right or left' activity; however, the system is unable to determine the possibility of a suspicious act or not. The range of values *0 – 0.86 radians* suggests that the object is parallel to the camera's field of view. In examination conditions, activities that lead to such poses suggest that an object is engaged in a dishonest act. For example, the "head on table" activity recorded in Table 8-6. The statistic values for the position input variables are converted to absolute values when used in the ARC fuzzy system.

From Table 8-6, it is observed that activities which are closer to the camera's field of view produce small extent values. For example in the "face to camera" activity, an extent value of ~0.46 is recorded for both objects. Hence, the closer an object is to the camera, the smaller the cameras field of view measured by the extent (i.e. percentage of occupancy). Therefore, the extent input variable is defined to have two possible states, i.e. camera occlusion and acceptable states.

The count variable records the number of objects detected in a video frame. In a test environment, only one object is expected to take a test within a cameras field of view; thus, no-object or multi-object detection in the scene is unacceptable. Table 8-7 shows the numeric values for the position, extent and count variables.

	Input variables		
Linguistic variables	**Position**	**Extent**	**Count**
Low	1.57 -1.22	0.57 – 1	1
Elevated	1.20 – 0.87	-	-
High	0.86 – 0	0 – 0.56	0, >1

Table 8-7 Position, extent and count numeric values

Recall that the output variable forms the conclusion about the potential threat risk of the object's presence to the environment and it is represented by the threat classification scheme. Thus, the five input variables shown above will be mapped to one conclusion for every video frame analysed; hence, the proposed multi-input single-output fuzzy system (see section 7.6). Table 8-8 shows the range on which the output variable is defined for the three threat classification terms *{low-risk, elevated-risk, high-risk}*.

Threat Class	**Output variable**
Low-risk	0 – 0.3
Elevated-risk	0.31 – 0.6
High-risk	0.61 – 1.0

Table 8-8 Output variable numeric values

Finally, the numeric values of the input and output variables influence the design of the membership functions used in the fuzzy logic system (FLS). Recall in chapter seven, the FLS is useful for the analysing the incoming real-time video frame and classifying the risk posed by the activity detected in the frame. This task is accomplished using the object's blob statistics as discussed in the earlier sections of this chapter.

8.4 Membership Functions

In chapter seven, the membership function of a fuzzy logic system (FLS) was introduced. In the ARC approach the membership functions (MF) is defined to provide flexibility for the linguistic range of the input variables. This means that the MF take up the values between [0, 1] and they indicate the degree to which a linguistic value belongs

to an input variable set. As earlier discussed the five input variables used in the ARC approach are: the changes in the object's blob size and shape statistics with respect to the object's frontal pose statistics, the position (given as orientation), extent and count. In section 7.4 the blob classifier operation consists of the fuzzy frontal class engine to check for an object's 'frontalness' property. Thus, in order to proceed in a test, an object's frontal pose must be correctly established and the relevant blob statistics extracted. The extracted statistics is fed into the ARC fuzzy risk class engine for activity risk classification. Figure 8-9 defines the input and output spaces used to determine the correctness or non-correctness of an object's initial frontal pose test.

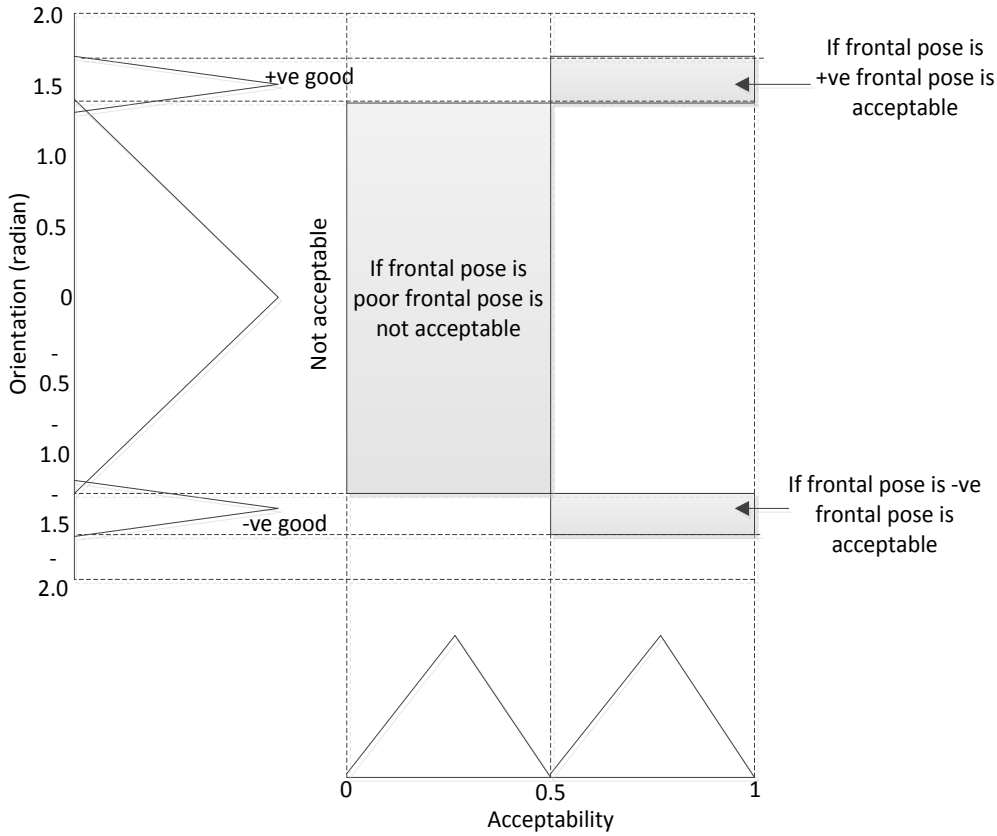


Figure 8-9 Frontal pose membership function

Figure 8-9 shows that, an object's accurate frontal pose is established when an object's orientation statistics lies between 1.2 to 2.5 radians (equivalent to 70^0 to 90^0). Consequently, the output space is defined on the range 0.5 to 1.

8.4.1 Size Membership Function

Figure 8-10 defines the input and output spaces for the changes in size. This is influenced by the percentage changes in an object's blob area statistics with respect to

the object's frontal pose statistics. As shown in Table 8-5, the size membership function was divided into three groups and defined on the range [0 – 0.3]: low change in size, [0.3 – 0.65]: elevated change in size and [>0.65] is high change in size.

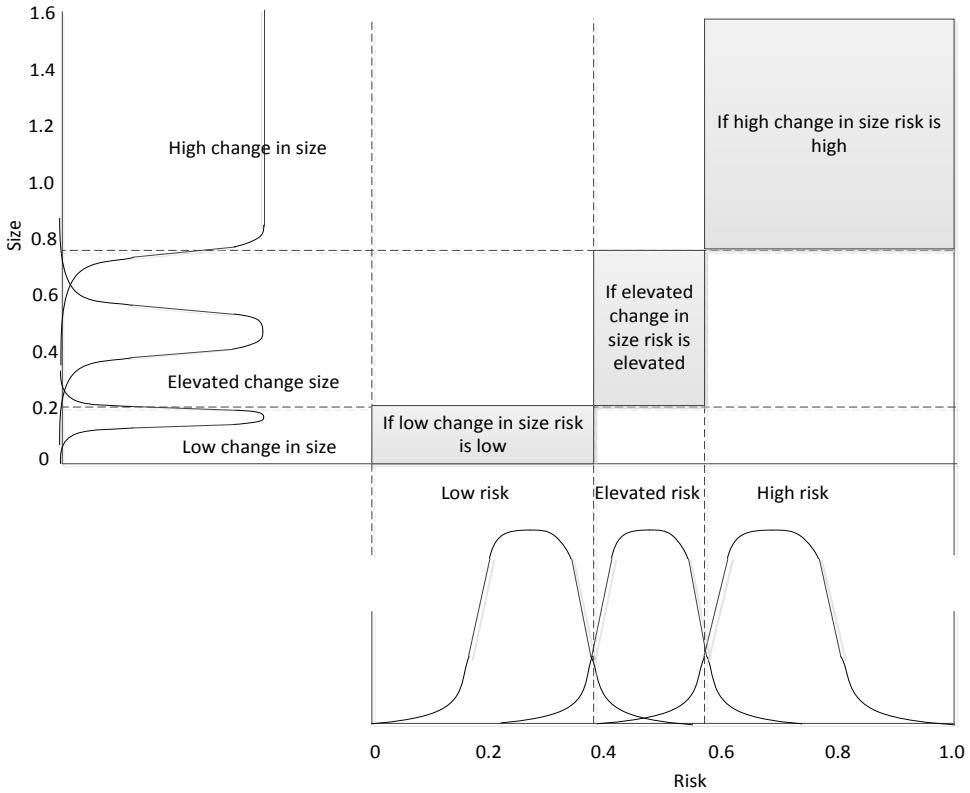


Figure 8-10 Size membership function

8.4.2 Shape Membership Function

Figure 8-11 defines the input and output spaces for the changes in shape. This is influenced by the percentage changes in the ratio of major and minor axis statistics with respect to the object's frontal pose statistics. The shape membership function is defined on the range [0 – 0.1]: low change in shape ratio, [0.11 – 0.3]: elevated change in shape ratio and [>0.3] is high change in shape ratio

8.4.3 Position Membership Function

Figure 8-12 defines the input and output spaces for the position variable. This is influenced by an object's blob orientation statistics with respect to the object's frontal pose statistics. The position membership function is defined on the range [1.57 – 1.22]: low change in position, [1.20 – 0.87]: elevated change in position and [0.86 - 0.0] is high change in position.

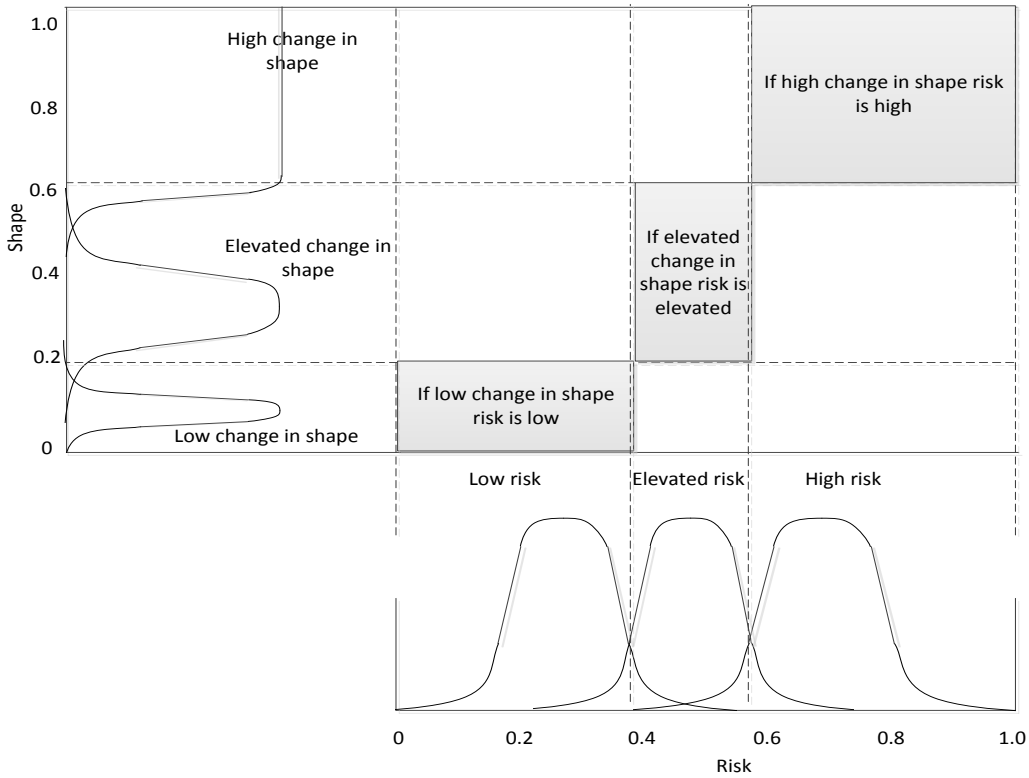


Figure 8-11 Shape membership function

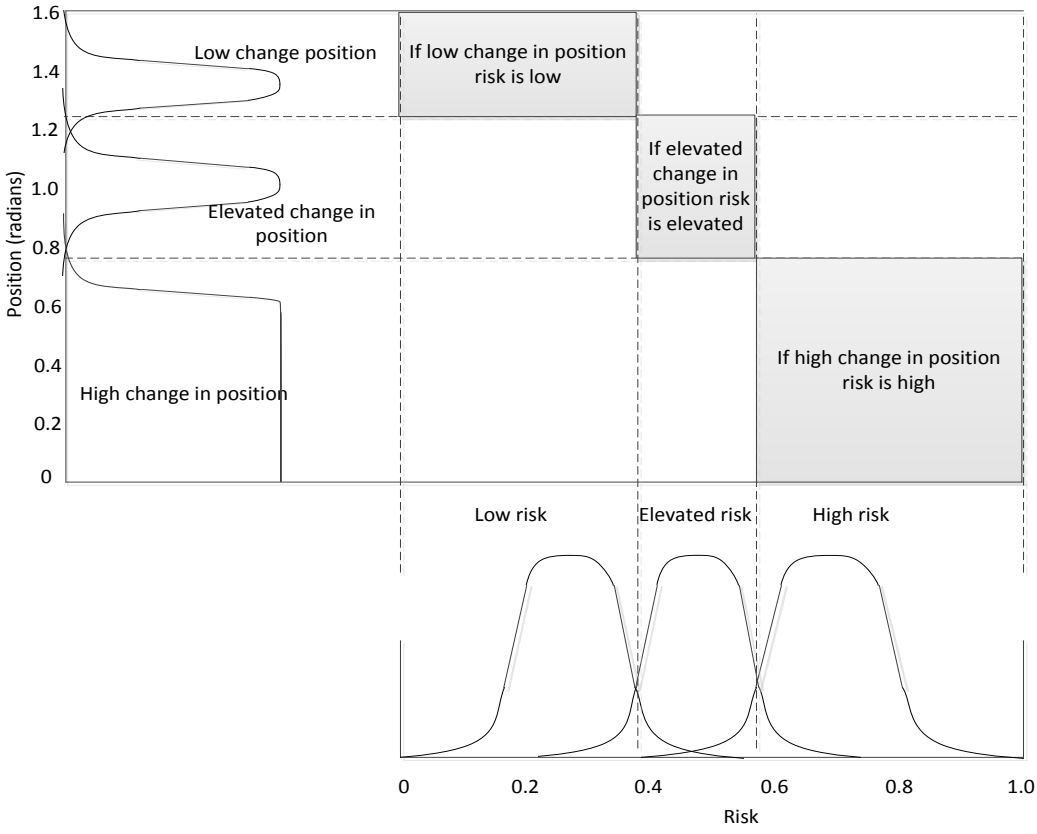


Figure 8-12 Position membership function

8.4.4 Extent Membership Function

Figure 8-13 defines the input and output spaces for an object's blob extent statistics with respect to the object's frontal pose statistics. The extent membership function is defined on the range [0.57 – 1.0]: low extent value and [0.0 – 0.56]: high extent value.

8.4.5 Count Membership Function

The count is executed as a simple if-then-rule which reflects the changes in the number of blobs detected. The count membership function is defined as low when count depicts a single presence value [1] and high when count depicts no-presence [0] and multi-presence values [>1].

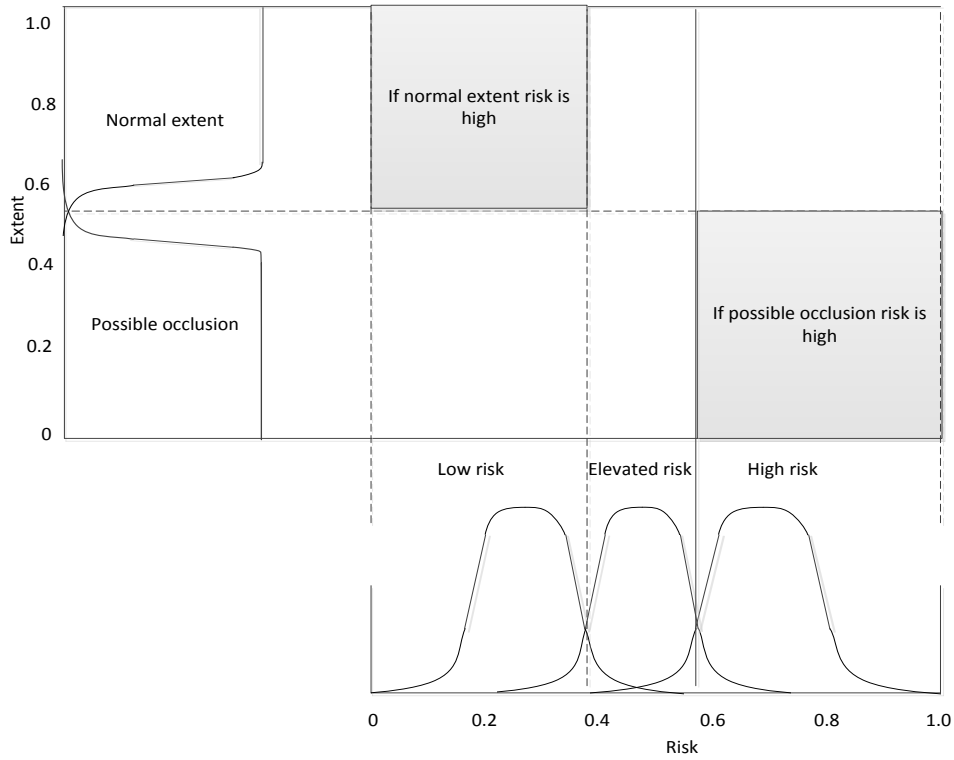


Figure 8-13 Extent membership function

8.4.6 Fuzzy Rule Base

The fuzzy if-then-rules are formed using the linguistic variables described above. In Table 8-9 the fuzzy rule-base which drives the ARC fuzzy rule engine is shown.

Fuzzy rules of Presence Verification
IF (Size is lowsize) **AND** (Shape is lowshape) **AND** (Position is lowpos) **THEN** (risk is low)
IF (Size is elevatedsize) **AND** (Shape is elevatedshape) **THEN** (risk is elevated)
IF (Size is highsize) **AND** (Shape is highshape) **THEN** (risk is high)
IF (Size is lowsize) **AND** (Shape is lowshape) **AND** (Position is highpos) **THEN** (risk is low)
IF (Size is elevatedsize) **AND** (Extent is occlusion) **THEN** (risk is elevated)
IF (Size is elevatedsize) **AND** (Shape is lowshape) **AND** (Position is highpos) **THEN** (risk is elevated)
IF (Size is elevatedsize) **THEN** (risk is elevated)
IF (Size is lowsize) **AND** (Shape is elevatedshape) **THEN** (risk is low)
IF (Size is elevatedsize) **AND** (Extent is occlusion) **THEN** (risk is elevated)
IF (Count is multi-presence) **THEN** (risk is high)
IF (Count is no-presence) **THEN** (risk is high)

Table 8-9 ARC Fuzzy rules

8.5 ARC Approach: Experiment 3

The third experiment was designed to investigate the feasibility of adopting the activity risk classification (ARC) approach in the BlobPV system. Table 8-10 shows the input variables and the corresponding output result for each activity performed by Object's A and B. As mentioned, the blob statistics values fed into the fuzzy engine are converted to absolute values for simplicity.

Frame Activity	Object	Size (change in area)	Shape (change in major/minor axes)	Position	Extent	Count	Fuzzy Results	Threat Class
Frontal pose	A	0.00	0.00	1.52	0.74	1	0.16	Low
	B	0.00	0.00	1.49	0.62	1	0.16	Low
External person behind Object	A	1.07	0.32	0.05	0.72	1	0.64	High
	B	0.87	0.06	0.44	0.61	1	0.64	High
External person beside Object	A	0.08	0.12	1.55	0.74	2	0.72	High
	B	0.23	0.01	1.47	0.61	3	0.53	High
Face to camera	A	1.05	0.27	1.18	0.40	1	0.64	High
	B	0.37	0.18	1.24	0.46	1	0.72	High
Cover face	A	0.14	0.04	1.56	0.70	1	0.16	Low
	B	0.25	0.04	1.25	0.55	1	0.17	Low
Touch head	A	0.05	0.18	0.27	0.75	1	0.16	Low
	B	0.10	0.14	0.11	0.51	1	0.17	Low
Look right	A	0.07	0.19	0.34	0.83	1	0.16	Low
	B	0.00	0.12	0.25	0.76	1	0.19	Low
Look left	A	0.42	0.03	0.24	0.70	1	0.44	Elevated
	B	0.03	0.11	0.31	0.74	1	0.20	Low
Head on table	A	0.42	0.27	1.09	0.50	1	0.44	Elevated
	B	1.01	0.26	0.03	0.78	1	0.64	High

Table 8-10 ARC approach: Object's A and B blob statistics

From Table 8-10, it is observed that the “frontal pose”, “cover face”, “touch head” and “look right” activities across Objects A and B are classified as a low-risk. Additionally, across the two objects the “external person behind object”, “external person beside object” and “face to camera” activities are classified as a high-risk. An illustration of Table 8-10 is presented below. Figure 8-14 shows that Object’s A and B frontal pose satisfies the ‘frontalness’ requirement; hence, the frontal poses are validated and the relevant statistics recorded.

Frontal pose A | Frontal pose B

Figure 8-14 Frontal pose: Object A and B

In Figure 8-15, the presence of an external person behind Object B reveals an increase in size. The change in size occurs as a result of the two blobs merging into one single blob. Additionally, the second frame in Figure 8-15 shows that an external person beside an original object can be detected via the blob count. Recall that, only one object is expected to be within a cameras field of view. Hence, the significant changes to Object B’s presence justify the high-risk output class. In a test environment, these results show that the ARC approach is able to detect changes in an object’s size through a blob merge or multi-blob count; thus, enhancing its suitability for the BlobPVS.

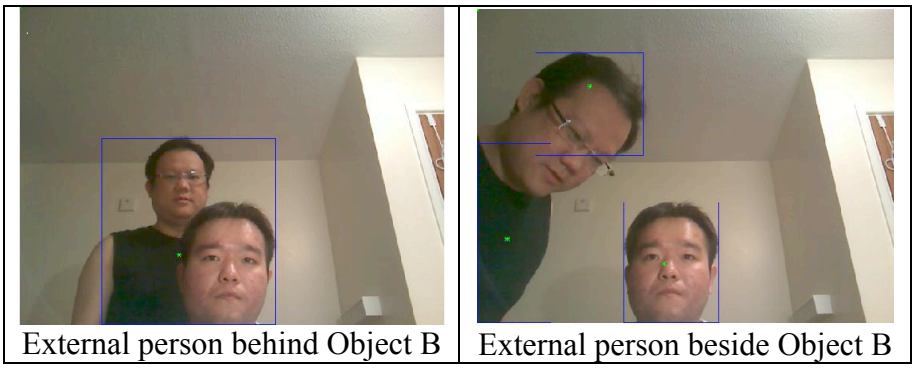

External person behind Object B | External person beside Object B

Figure 8-15 External person behind/beside Object B

Figure 8-16 shows the 'face to camera' activity for Objects A and B. From these frames, it is observed that the objects are positioned closer to the cameras field of view; thus, occupying a large percentage of the cameras lens. Thus, due to the 'close-up' pose low extent statistics values are produced. Recall that, the extent value defined on the range [0 – 0.56] suggests that the cameras field of view is obstructed.

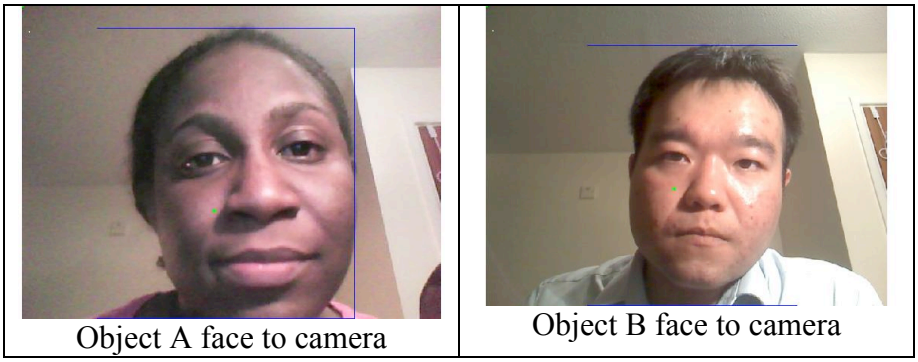

Object A face to camera | Object B face to camera

Figure 8-16 Face to camera: Object A and B

Figure 8-17shows the "cover face" activities for Objects A and B. A visual inspection of Table 8-10 reveals that the "cover face" activity was classed as a low-risk due to the low changes in the size and shape values of the Objects with respect to their frontal (or reference) poses. The low change values recorded for this activity is as a result of the addition of the object's hand on the face, which is still along the position of the initial (reference) face pose with respect to the cameras field of view. Thus, a feature added to the cameras field of view would be classed as a low-risk provided the addition occurs along the position of the object's frontal pose.

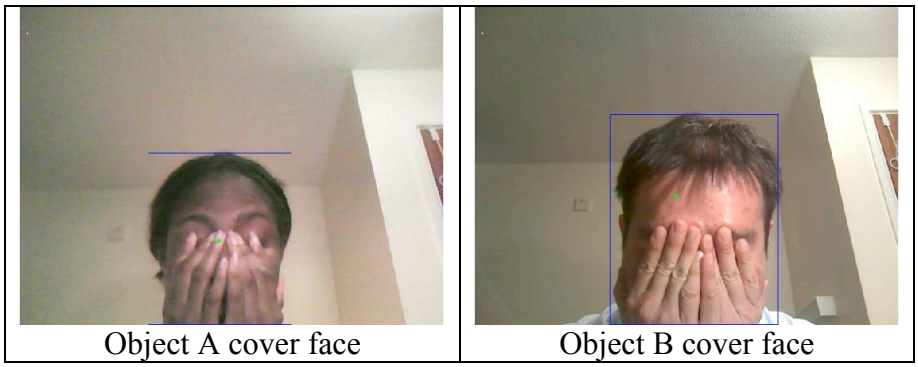


Figure 8-17 Cover face: Object A and B

Figure 8-18 shows the 'look left' activity for Objects A and B. From Table 8-10 it is observed that Object A is classed as an elevated-risk whilst for the same activity Object B is classed as a low-risk. In addition, Object A has ~42% increase in size compared to ~3% increase for Object B. Thus, as defined in the size membership function, a change in an object's size that falls within the range [31% and 65%] should be classed as an elevated-risk. In reality, an increase in size for a "look left" activity could suggest the likelihood of suspicious activities in a test environment. A similar trend is also observed from the "head on table" activity shown in Figure 8-19. In this case, Object A has an elevated-risk output, whilst Object B's presence is classed as a high-risk. A visual inspection of the table shows a 101% increase in size for Object B and a 42% increase in size for Object A; thus, justifying the output classification.

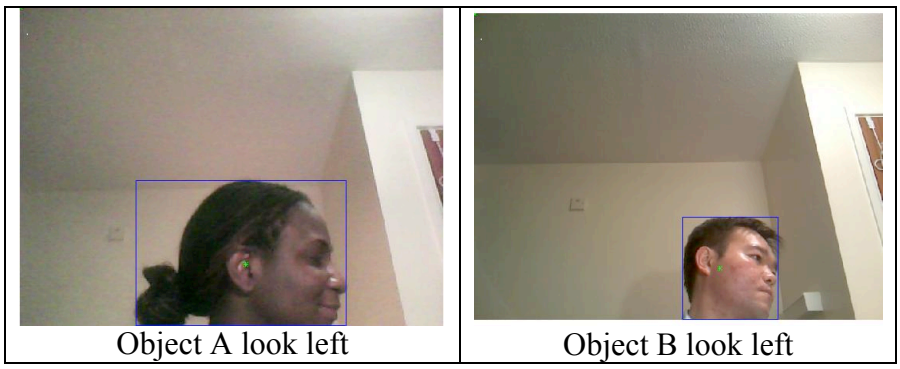


Figure 8-18 Look left: Object A and B

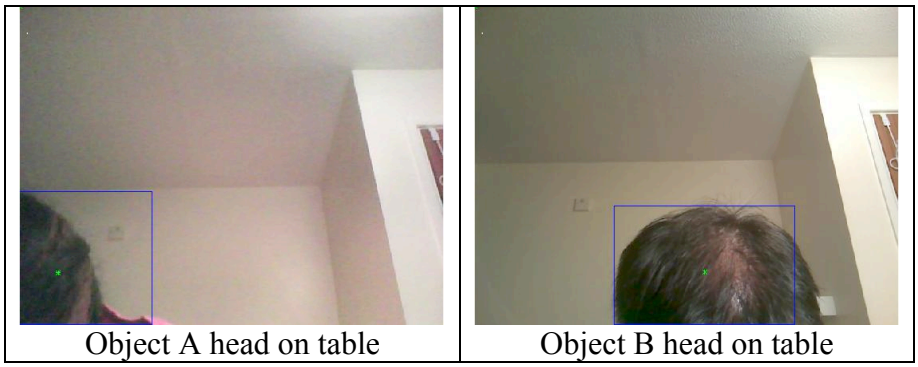


Figure 8-19 Head on table: Object A and B

8.5.1 Classification Accuracy

Table 8-11 shows a classification accuracy table obtained from the fuzzy threat class results. For this thesis, 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 8-11, the ARC fuzzy engine has classified correctly 14 activities from the total number of 18 analysed activities; thus, giving a classification accuracy of 78%. The remaining 4 activities were expected to be classed as elevated-risk; however, they are misclassified as a low-risk or high risk. Thus, the misclassification rate is 22%. The classification accuracy is evaluated by the formula:

$$C_A = \frac{\text{number of correctly classified activities}}{\text{total number of analysed activities}} x100 \qquad (8.7)$$

Frame Activity	Object	Expected threat class	ARC Fuzzy threat class
Frontal pose	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
External person behind Object	A	High-risk	High-risk
	B	High-risk	High-risk
External person beside Object	A	High-risk	High-risk
	B	High-risk	High-risk
Face to camera	A	High-risk	High-risk
	B	High-risk	High-risk
Cover face	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
Touch head	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
Look right	A	Elevated-risk	Low-risk
	B	Elevated-risk	Low-risk
Look left	A	Elevated-risk	Elevated-risk
	B	Elevated-risk	Low-risk
Head on table	A	High-risk	Elevated
	B	High-risk	High-risk

Table 8-11 Classification accuracy table

8.5.2 Threat Class Reclassification

Recall in section 7.3.4, that an elevated-risk threat class will attempt to re-classify an elevated-risk activity using the perimeter and diameter statistics. Thus, to improve the classification accuracy rate and promote the non-interruptive abilities of the ARC approach, it is important to re-classify the elevated-risk activities. The re-classification process is accomplished using simple if-then-rule statements that exploit an object's blob perimeter and diameter statistics. Thus, an activity with a change in the diameter (or perimeter) statistics [0.5] would be re-classified as a high-risk, i.e. from elevated-risk to high-risk. Conversely a change in diameter (or perimeter) statistics [0.5] would be re-classed to a low-risk, i.e. from elevated-risk to low-risk. Equation 8-7 shows the range of values required for the re-classification process:

$$\begin{aligned} diameter &= -0.5 \quad x \quad 0.5 \\ perimeter &= -0.5 \quad x \quad 0.5 \end{aligned} \tag{8.7}$$

where, x is the diameter (or perimeter) statistics value.

Additionally, the re-classification process logically assigns a re-class risk based on the logic table shown in Table 8-12. This is useful as is it ensures that a low-risk class is assigned only when the two statistics are less than or equal to [0.5]. It is important to note that, the perimeter and diameter statistics of the same object would not vary significantly from the perimeter and diameter statistics of the initial frontal pose. This implies that, these statistics can vary through an object's different activities; however, the change in values should remain within the range defined in equation 8-7. Table 8-13 shows the re-classification results for the activities that were initially assigned an elevated-risk. From the table, it is observed that the "look left" activity for Object A is now re-classed as a low-risk; this, is due to the low change (*<50%*) for both the diameter and perimeter statistics. However, the "head on table" activity for Object B is re-classed to a high-risk due to the significant change *(>50%)* in the diameter statistics.

Perimeter	**Diameter**	**Threat Re-classification**
0.5	*0.5*	Low-risk
0.5	*0.5*	High-risk
0.5	*0.5*	High-risk
0.5	*0.5*	High-risk

Table 8-12 Re-classification logic tables

Frame Activity	**Object**	**Size**	**Shape**	**Perimeter**	**Diameter**	**Fuzzy Results**	**Initial threat Class**	**Threat Re-class**
Look left	A	0.42	0.03	0.42	0.32	0.44	Elevated	Low
	B	0.03	0.11	0.12	0.42	0.20	Low	-
Head on table	A	0.42	0.27	0.27	1.01	0.44	Elevated	High
	B	1.01	0.26	0.42	0.32	0.64	High	-

Table 8-13 Threat re-classification for Object A and B

As a result of the re-classification results, it is important to obtain a revised classification accuracy matrix. Recall that in Table 8-11 the misclassification rate was 22% as a result of the 4 wrongly classed activities, where 2 of the activities were classed as an elevated-risk. Thus, a re-classification of these 2 activities resulted in a low-risk and high-risk class respectively. The "head on table" activity was re-classed to high-risk;

thus, increasing the classification accuracy rate to 83%. The "look left" was also re-classed to a low-risk threat class. It should be noted that a low-risk threat class is desirable as the object presents no risk to the test environment. Hence, based on the re-classification process, the elevated-risk classes in the expected threat class can be revised to a low-risk class. This implies that the ARC fuzzy threat class now matches the expected threat class; thus, a classification accuracy of 100% is achievable as shown in Table 8-14

Frame Activity	Object	Expected threat class	ARC Fuzzy threat class
Frontal pose	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
External person behind Object	A	High-risk	High-risk
	B	High-risk	High-risk
External person beside Object	A	High-risk	High-risk
	B	High-risk	High-risk
Face to camera	A	High-risk	High-risk
	B	High-risk	High-risk
Cover face	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
Touch head	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
Look right	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
Look left	A	Low-risk	Low-risk
	B	Low-risk	Low-risk
Head on table	A	High-risk	High-risk
	B	High-risk	High-risk

Table 8-14 Revised classification accuracy matrix

8.6 Test Case Scenarios: Evaluating the ARC Approach

In order to evaluate the accuracy and stability of the ARC approach, the remaining three datasets were evaluated and represented as Object C, Object D and Object E respectively.. Recall, that the datasets collected simulate a natural test environment; thus, the students are not constrained to a fixed position. To design the three case scenarios, the activity examples employed in the trial data were grouped under three general headings. These groupings were useful as it made clearer the classification

accuracy of the ARC approach through the different activities. For the evaluation process, the scenarios contain additional example activities shown in Table 8-15. As mentioned earlier, the list of possible student activities is quite enormous; however, the example activities shown reflect user security activities.

Test case One: Impersonation Scenarios

This scenario includes activities that can lead to impersonation threats. In this case, an external presence different from the original authenticated student is detected in the test environment.

Test case Two: Occlusion Scenarios

This scenario includes activities that can lead to obstructing the camera's field of view. 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.

Test case Three: Miscellaneous Scenarios

This scenario includes a variety of student activities (acceptable and unacceptable) which can occur during a test. These activities are characterised by varying body movements that may change a student's original pose, which can lead to a suspicious pose

8.6.1 Impersonation scenarios

In this experiment it is expected that the fuzzy results will detect activities that can lead to impersonation activities in Objects C, D and E. The rate of change in the blob statistics with respect to the objects frontal pose is shown in Table 8-16, whilst the original blob statistics can be found in Appendix A.

.

Case scenarios	Description	Activity examples
Test case one: Impersonation scenarios	Activities that attempt to provide assistance towards a student's test or an attempt to substitute an original student during the test	External person move towards student
		External person behind student
		External person beside student
		External person close to student
		External person substitutes student
Test case two: Occlusion scenarios	Activities that attempt to obstruct the camera's lens during the test.	Face close to camera
		Hand blocking camera
		Head blocking camera
Test case three: Miscellaneous scenarios	A variety of acceptable and unacceptable student activities during a test	Head distant from camera
		Lean on table
		Head on table
		Look left/right
		Look up
		Hand on forehead

Table 8-15 Test case scenarios and Activity examples

Frame Activity	Object	Size (change in area)	Shape (change in major/minor axes)	Position	Extent	Count	Fuzzy Results	Threat Class
Frontal pose	C	0.000	0.000	1.387	0.505	1	0.163	Low
	D	0.000	0.000	1.539	0.773	1	0.163	Low
	E	0.000	0.000	1.500	0.488	1	0.163	Low
External person move towards student	C	1.046	0.187	0.772	0.502	1	0.643	High
	D	0.780	0.175	1.356	0.606	1	0.643	High
	E	1.416	0.159	0.113	0.403	1	0.643	High
External person behind student	C	1.488	0.151	0.355	0.475	1	0.643	High
	D	0.795	0.155	0.455	0.538	1	0.643	High
	E	1.444	0.152	0.119	0.407	1	0.643	High
External person beside student	C	3.159	0.170	0.856	0.456	1	0.643	High
	D	0.819	0.983	0.338	0.268	2	0.643	High
	E	0.474	0.207	0.948	0.470	2	0.642	High
External person close to student	C	0.151	0.049	1.302	0.446	2	0.519	High
	D	0.217	0.064	1.163	0.632	2	0.781	High
	E	0.617	0.315	1.568	0.484	2	0.669	High
External person substitutes student	C	0.108	0.166	1.518	0.770	1	0.162	Low
	D	0.084	0.264	1.439	0.456	1	0.159	Low
	E	0.719	0.068	1.391	0.660	1	0.640	High

Table 8-16 Test case one: Impersonation scenarios for Object C, D, E

Figure 8-20 shows that Object C's frontal position elicited from the blob orientation is within the acceptable range and the relevant blob statistics are extracted for the verification process. However, during the test an external person appears in the background and moves towards Object C. It is observed that, due to a merge between the two objects, there is an increase in Object C'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 may be occurring. Thus, these changes in size and shape trigger the fuzzy engine and Object C is assigned a high-risk threat class. Hence, as the external person gradually moves behind and beside Object C, an increase in blob size and change is shape is consistently recorded.

At the point where the external person moves close to Object C, the two blobs unmerge and are separated. This is interesting, because Object C 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. Additionally from the last frame in Figure 8-11a, it is observed that the external person has eventually substituted the original student; thus, providing a clear impersonation attack. Based on the swap, it is expected that the change in blob statistics would yield a high-risk threat class from the fuzzy engine. However, from Table 8-16 the "external person substitutes Object C" activity is assigned a low-risk.

A visual inspection of this activity reveals that Object C's initial blob size was further reduced by *~11%*; thus, the external blob size falls within the low-risk range defined for the size membership function. Additionally, the external person's position statistic values are also within the acceptable range defined, i.e. *1.52radians*. Therefore, based on this blob statistics it is unlikely that the swap between Object C and the external person would be detected. However, it should be noted that the external person and Object C does not necessarily possess similar blob statistics; rather, the near-similar statistic scenario occurred as a result of the external person's distance (in metres) to the cameras field of view. Hence, the proximity or remoteness of an individual would affect the blob statistics extracted and fed to the fuzzy engine.

From another perspective, it can be argued that there exists a low chance for the external person to substitute Object C. A visual inspection of the frames below show

that, it is unlikely that a swap from Object C's frontal pose to a different frontal pose would pass undetected; this is because the merging and separation activities would have occurred or even a background with zero objects detected would have been spotted as an anomaly. Hence, a high-risk threat class is inevitable for impersonation scenarios.

Figure 8-20 Object C impersonation scenarios

Figure 8-21 show Object D's impersonation scenarios, where an external person moving towards and behind Object D results in a high-risk threat class due to the increase in blob size and change in shape. Similarly an external person beside and close to the object is flagged by the count statistics revealing the two objects in the background. Additionally, a low-risk threat class is assigned for the "external person substitute Object D" activity as opposed to the expected high-risk threat class. A visual observation from Table 8-16 reveals *~8%* reduction from Object D's original blob size;

thus, justifying the external person's distance (in metres) from the camera's field of view.

Figure 8-21 Object D impersonation scenarios

Figure 8-22 shows Object E's impersonation scenarios, where an external person detected in the environment produces a high-risk threat class. However, in this scenario the "external person substitutes Object E" activity produces a high-risk threat class instead of the low-risk threat class reported in Object C and D. From Table 8-16, it is noticed that a *~71%* increase in Object E's blob size was recorded. The statistics value falls within the high-risk range defined for the size membership function. The significant increase in Object E's blob size can occur as a result of the external person's proximity to the camera or as a result of additional detectable features (see external person's hair). In a real test environment, the impersonators proximity or remoteness to the cameras

field of view may be uncontrolled; however, additional detectable features can expose potential student swaps.

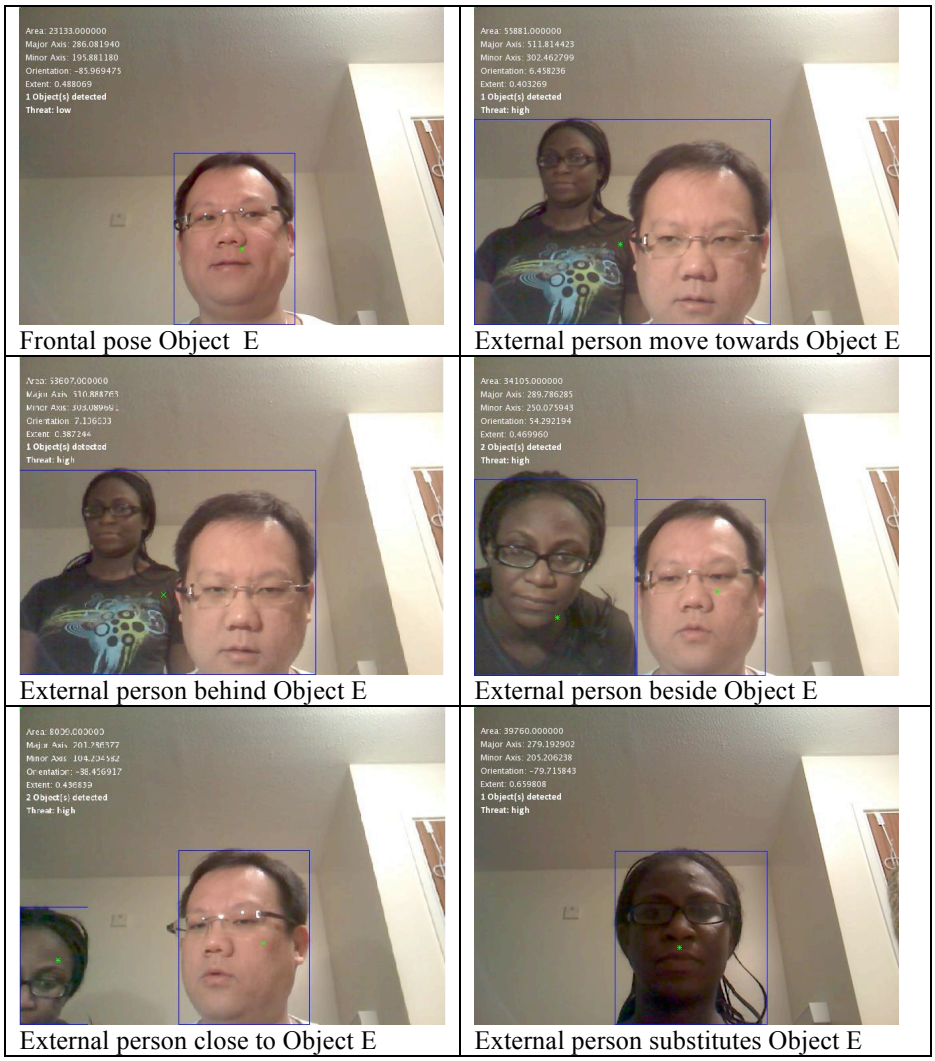


Figure 8-22 Object E impersonation scenarios

On a final note, the Object C, D and E impersonation scenarios 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. In the impersonation scenarios, a high-risk threat class is the expected output for all the frame activities. Thus, when an object is assigned a high-risk class, the next step is the re-authentication process using one of the existing strong authentication methods, e.g. biometrics. The re-authentication process is not considered for this experiment.

8.6.2 Occlusion Scenarios

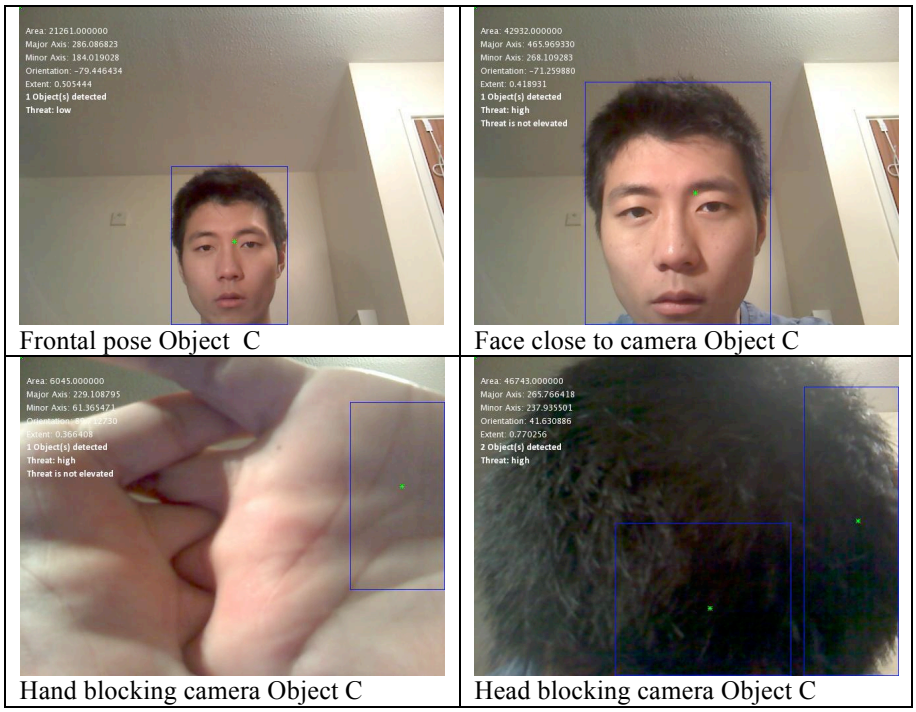
In this experiment it is expected that the fuzzy results will detect activities that can obstruct the cameras field of view in Objects C, D and E. The rate of change in blob statistics with respect to an object's frontal pose is shown in Table 8-17, whilst the original blob statistics can be found in Appendix A.

Frame Activity	Object	Size (change in area)	Shape (change in major/minor axes)	Position	Extent	Count	Fuzzy Results	Threat Class
Frontal pose	C	0.000	0.000	1.387	0.505	1	0.163	Low
	D	0.000	0.000	1.539	0.773	1	0.163	Low
	E	0.000	0.000	1.500	0.488	1	0.163	Low
Face close to camera	C	1.019	0.118	1.244	0.419	1	0.643	High
	D	1.195	0.095	0.770	0.493	1	0.643	High
	E	0.478	0.137	0.008	0.157	2	0.642	High
Hand blocking camera	C	0.204	2.723	0.331	0.292	2	0.787	High
	D	0.777	0.115	0.741	0.741	3	0.643	High
	E	0.924	0.271	0.158	0.463	1	0.643	High
Head blocking camera	C	1.199	0.282	0.727	0.770	2	0.643	High
	D	3.451	0.011	1.018	0.464	1	0.643	High
	E	0.304	0.286	0.083	0.392	2	0.643	High

Table 8-17 Test case two: Occlusion scenarios for Object C, D, E

Figure 8-23 show three activities which occlude the cameras lens and can eventually disrupt the presence verification process. In the "face close to camera" activity, Object C's face occupies a large percentage of the cameras lens; thus, increasing the blob size by *~101%.* Additionally, the extent statistics value is decreased to *0.42* falling within the occlusion range defined in the extent membership function. This activity attracts a high-risk threat class, alongside the "hand and head blocking camera" activities. However, an interesting part of the fuzzy engine is that all the statistic values are considered for the decision making. From Table 8-17, it is observed that the count statistics is also included in the decision process as it can detect multiple features on an object. In addition, the shape and position statistics for the three activities fall within the elevated-risk or high-risk range of their respective membership functions. A visual inspection of the "hand and head blocking camera" activity frames show distinct changes

in the shape and position of Object C from the initial frontal pose. Thus, the combination of this statistics infers a suspicious action that justifies a high-risk threat class.

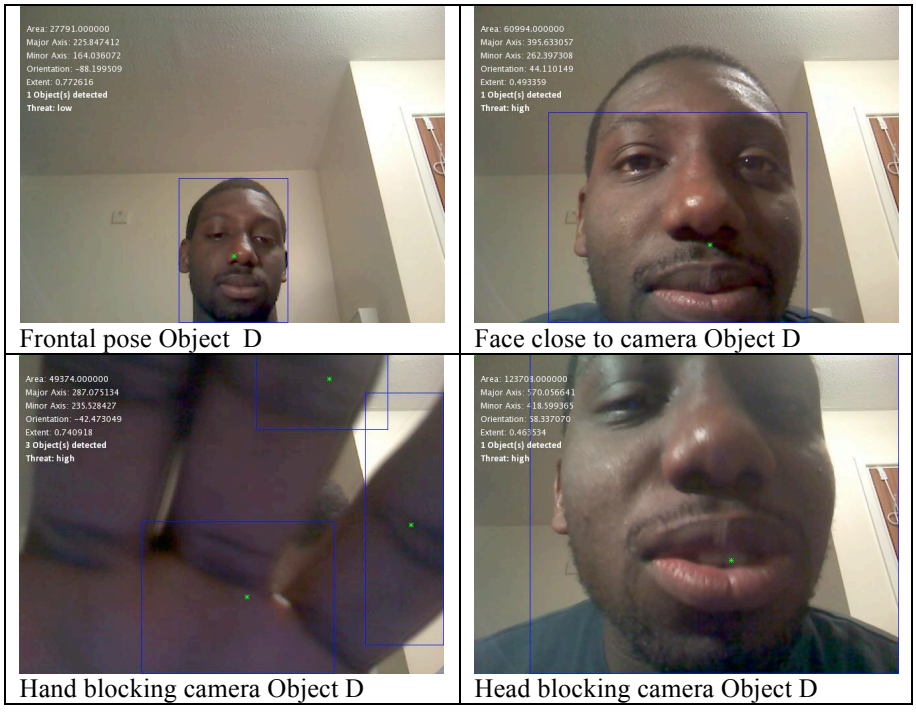


Frontal pose Object C | Face close to camera Object C

Hand blocking camera Object C | Head blocking camera Object C

Figure 8-23 Object C occlusion scenarios

Figure 8-24 show the occlusion scenarios for Object D, where the combination of the size, shape, position, extent and count statistics drives the fuzzy class engine to produce a high-risk threat class.

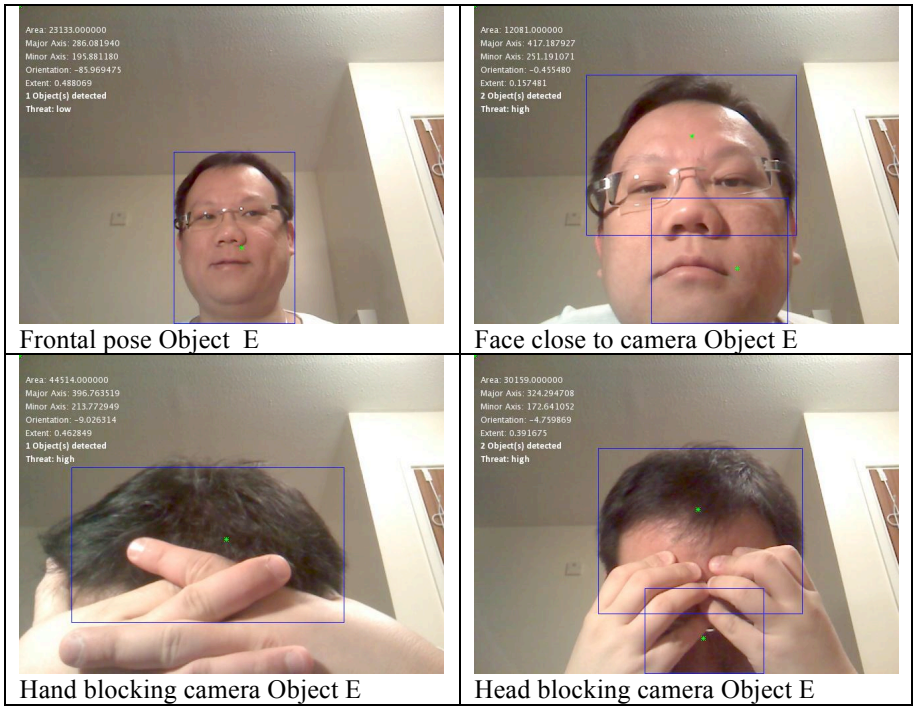


Frontal pose Object D | Face close to camera Object D

Hand blocking camera Object D | Head blocking camera Object D

Figure 8-24 Object D occlusion scenarios

Figure 8-25 show the occlusion scenarios for Object E, where the combination of the size, shape, position, extent and count statistics drives the fuzzy class engine to produce a high-risk threat class.



Frontal pose Object E | Face close to camera Object E

Hand blocking camera Object E | Head blocking camera Object E

Figure 8-25 Object E occlusion scenarios

In summary, the Object C, D and E occlusion scenarios have demonstrated the feasibility of detecting a disruption to the presence verification process when the cameras lens is obstructed. This task was accomplished by taking into consideration an object's size, shape, position, extent and count statistics values to produce a decision. In the occlusion scenarios, a high-risk threat class is the expected output for all the frame activities; thus, leading to a re-authentication process.

8.6.3 Miscellaneous Scenarios

In this experiment it is expected that the fuzzy results of the miscellaneous scenarios will correctly detect acceptable and unacceptable activities. The results are expected to be stable across the Objects C, D and E. The rate of change in blob statistics are shown in Table 8-18, whilst the original blob statistics can be found in Appendix A.

Frame Activity	Object	Size (change in area)	Shape (change in major/minor axes)	Position	Extent	Count	Fuzzy Results	Threat Class
Frontal pose	C	0.000	0.000	1.387	0.505	1	0.163	Low
	D	0.000	0.000	1.539	0.773	1	0.163	Low
	E	0.000	0.000	1.500	0.488	1	0.163	Low
Head distant from camera	C	0.491	0.069	1.553	0.595	1	0.449	Elevated
	D	0.871	0.054	0.009	0.767	0	0.643	High
	E	0.869	0.227	0.077	0.423	0	0.643	High
Head on table	C	1.111	0.560	0.010	0.679	1	0.643	High
	D	0.629	0.150	0.009	0.781	1	0.450	Elevated
	E	1.115	0.130	0.172	0.550	1	0.643	High
Look left/right	C	0.398	0.019	1.475	0.508	1	0.428	Elevated
	D	0.812	0.174	0.587	0.460	1	0.643	High
	E	0.618	0.289	0.662	0.361	1	0.450	Elevated
Look up	C	0.365	0.016	1.282	0.324	1	0.370	Elevated
	D	0.203	0.220	1.133	0.745	1	0.161	Low
	E	0.690	0.169	0.037	0.477	0	0.719	High
Hand on forehead	C	1.376	0.118	0.922	0.541	1	0.643	High
	D	0.781	0.082	0.113	0.499	1	0.643	High
	E	0.787	1.855	1.217	0.244	1	0.643	High

Table 8-18 Test case three: Miscellaneous scenarios for Object C, D, E

The first frame in Figure 8-26 shows Object C's "head distant from camera" activity which reports a *49%* change in size from the original size recorded. In this activity, the shape, position and extent values are within the acceptable range; however, the significant reduction in size triggers the high-risk threat class. In a practical test environment, this type of activity is unacceptable as the student is not concentrating on the test task and moving away from the camera may imply a suspicious action, such as receiving external assistance or attempt to exit the environment. This activity is expected to produce an elevated-risk threat class as the fuzzy engine is unsure of Object C's next action.

Much more than a significant increase in size, the "head on table" activity distorts the shape and position of the object. From Figure 8-26 and Table 8-18, it is observed that Object C's position (orientation) has changed from a perpendicular direction to a parallel or straight line. This change in position also affects the shape of the object, as the length of the major axis lies horizontal to the *x*-axis. A combination of these statistics reflects a significant change from the initial frontal pose statistics extracted; thus, a high-risk threat class is assigned. In the "look left/right" activity the blob size records *~49%* increase whilst the "look up" activity records *~37%* decrease in size. The increase in size occurs as a result of the change in the object's shape due to the object tilting to the left direction. Thus, the length of the major axis elongated in the left direction changes the shape of the object and increases the blob size. Conversely, the decrease in size is as a result of the object tilting in an upward direction. In this case, there would be a change in shape; however, there will be no increase in size due to the objects direction. Hence, an elevated-risk threat class is assigned, as the shape predominantly drives the fuzzy engine for the two activities.

The "hand on forehead" activity produces a significant increase in the object's size *(~137%)*, a significant change in object's position and a decrease in the extent value. The increase in size and decrease in the extent value occurs as a result of the additional detectable feature (i.e. hand) encapsulated on the objects forehead. Thus, a combination of this statistics produces a high-risk threat class.

Figure 8-26 Object C miscellaneous scenarios

From Table 8-18, it is observed that Object D's "head distant from camera" activity produces a high-risk threat class. From Figure 8-27, it is seen that there exist a considerable distance between Object D and the camera. This implies that the object is no longer in the cameras field of view and no object is detected during the verification process. The assigned high-risk threat class is driven by the count statistics as no presence is detected in the background. In a real world environment, the object may have disappeared from the test environment or performing a dishonest activity. Object D's "head on table" activity is affected by an increase in size, change in shape and position as discussed for Object C. there is a similarity in the blob statistics recorded; however, an elevated-risk threat class is assigned. The "look left/right" activity for Object D produces a high-risk threat class due a *~81%* increase in blob size and a change in shape.

It is observed from Figure 8-27, that the addition of Object D's shoulder as a result of tilting deep into the right direction produced an increase in size. However, the tilt in a upward direction resulted in a low-risk threat class. This implies that Object D has not incurred significant changes in the "look up" activity. A visual inspection of Figure 8-27, shows that the objects size and shape is similar to the geometry in the frontal pose frame. This trend is also reflected in the blob statistics in Table 8-18. The "hand on forehead" activity results in a high-risk threat class due to an increase in size and decrease in extent values as described for Object C.

Figure 8-27 Object D miscellaneous scenarios

From Figure 8-28, it is observed that no presence is detected in Object E's "head distant from camera" and "look up" activities; thus, a high-risk threat class is assigned. The "head on table" and "hand on forehead" activities produce a high-risk threat class

due to an increase in size, change in shape and position. In the “look left/right” activity, a *~61%* change in size falls within the elevated-risk range in the size membership function; hence, an elevated-risk threat class is assigned.

Figure 8-28 Object E miscellaneous scenarios

In summary, the Object C, D and E miscellaneous scenarios have demonstrated the feasibility of detecting acceptable and unacceptable activities in a test environment. This task was accomplished by taking into consideration an object’s size, shape, position, extent and count statistics values to produce a variety of low-risk, elevated-risk and high-risk decisions.

8.7 Success Rate

To evaluate the classification accuracy of the test case scenarios (Table 8-19), the formula introduced in Equation 8-6 is adopted:

$$C_A = \frac{\text{number of correctly classified activities}}{\text{total number of analysed activities}} x100$$

Frontal pose: Object C, D and E frontal poses was correctly classed for each test case scenario.

$$C_A = \frac{3}{3} x100 \quad = 100\%$$

Impersonation scenarios: the expected threat class for all the activities in this test case scenario is the high-risk class. However, the ARC fuzzy engine classified correctly 13 activities giving a classification accuracy of 87%. The remaining 2 activities were classed as a low-risk threat instead of the expected high-risk threat; thus, a13% misclassification rate was recorded. Interestingly, the 13% misclassification rate can be argued against, because the ARC approach is designed to spot the variations in an objects proximity or remoteness to a cameras field of view. Consequently, these variations can affect the objects size. Thus, the threat class decisions are assigned based on the statistics detected from the object. However, it should be noted that a classification accuracy of 100% is achievable when an object's distance to the camera is controlled.

$$C_A = \frac{13}{15} x100 \quad = 87\%$$

Occlusion scenarios: the expected threat class for all the activities in this test case scenario is the high-risk class. In the experiments, 9 activities were analysed and the ARC fuzzy engine classified correctly all the 9 activities; thus, achieving a classification accuracy of 100%.

$$C_A = \frac{9}{9} x100 \quad = 100\%$$

Miscellaneous scenarios: the expected threat class in this scenario varies from low-risk to high-risk depending on the different activities. The ARC fuzzy engine classified correctly 6 activities giving a classification accuracy of 40%. 5 out of the 9 misclassified activities were assigned an elevated-risk threat class. The elevated-risk threat class is useful as it presents an opportunity to improve the success rate of the overall system. Thus, assuming the 5 elevated-risk threat activities are re-classed to match the expected threat class; then the current classification accuracy rate would increase by 33%.

However, the remaining 4 high-risk threat activities, i.e. “look up” activity for Object E and “hand on forehead” for the three objects represent the 26% misclassification rate.

$$C_A = \frac{6}{15} x100 \quad = 40\%$$

Overall classification accuracy: in the ARC evaluation process a total of 42 frames depicting three test scenarios and three objects were analysed. The ARC fuzzy engine classified correctly 31 activities giving an overall classification accuracy of 74%. However, this figure is expected to change after the re-classification process. Currently the overall misclassification rate is 26%.

$$C_A = \frac{31}{42} x100 \quad = 74\%$$

Object C, D and E: in 14 activities analysed for each object, the ARC fuzzy engine classified correctly 9, 10 and 11 activities giving a classification accuracy of 64%, 71% and 79% respectively.

			ARC Fuzzy threat class			
	Frame Activity	**Expected threat class**	**Object C**	**Object D**	**Object E**	**Classification accuracy**
Test case scenarios	Frontal pose	Low-risk	Low-risk	Low-risk	Low-risk	**100%**
Impersonation scenarios	External person move towards student	High-risk	High-risk	High-risk	High-risk	**87%**
	External person behind student	High-risk	High-risk	High-risk	High-risk	
	External person beside student	High-risk	High-risk	High-risk	High-risk	
	External person close to student	High-risk	High-risk	High-risk	High-risk	
	External person substitutes student	High-risk	Low-risk	Low-risk	High-risk	
Occlusion scenarios	Face close to camera	High-risk	High-risk	High-risk	High-risk	**100%**
	Hand blocking camera	High-risk	High-risk	High-risk	High-risk	
	Head blocking camera	High-risk	High-risk	High-risk	High-risk	
Miscellaneous scenarios	Head distant from camera	High-risk	Elevated-risk	High-risk	High-risk	**40%**
	Head on table	High-risk	High-risk	Elevated-risk	High-risk	
	Look left/right	High-risk	Elevated-risk	High-risk	Elevated-risk	
	Look up	Low-risk	Elevated-risk	Low-risk	High-risk	
	Hand on forehead	Low-risk	High-risk	High-risk	High-risk	
			64%	**71%**	**79%**	

Table 8-19 Success rate for test case scenarios

8.7.1 Risk and Success Rate Reclassification

For the risk reclassification process, the perimeter and diameter logic tables introduced in Table 8-12 was adopted.

Perimeter	Diameter	Threat Re-classification
0.5	*0.5*	Low-risk
0.5	*0.5*	High-risk
0.5	*0.5*	High-risk
0.5	*0.5*	High-risk

Table 8-20 shows the re-classification results for the activities that were initially assigned an elevated-risk threat class. From the table, it is observed that the "head distant from camera" activity for Object C is re-classed as a high-risk due to the significant change in the perimeter statistics values.

Frame Activity	Object	Size	Shape	Perimeter	Diameter	Fuzzy Results	Initial threat Class	Threat Re-class
Head distant from camera	C	0.49	0.07	0.83	0.37	0.45	Elevated	High
	D	0.87	0.05	1.0	1.0	0.64	High	-
	E	0.87	0.23	1.0	1.0	0.64	High	-
Head on table	C	1.11	0.56	0.55	1.11	0.64	High	-
	D	0.63	0.15	0.29	0.63	0.45	Elevated	High
	E	1.11	0.13	1.50	1.28	0.64	High	-
Look left/right	C	0.40	0.02	0.50	0.40	0.43	Elevated	Low
	D	0.81	0.17	1.08	0.75	0.64	High	-
	E	0.62	0.29	0.39	0.58	0.45	Elevated	High
Look up	C	0.37	0.02	0.39	0.49	0.37	Elevated	Low
	D	0.20	0.22	0.12	0.20	0.16	Low	-
	E	0.69	0.17	1.0	1.0	0.72	High	-

Table 8-20 Risk reclassifications for test scenarios

In a real test environment, the re-class from elevated-risk to high-risk is practical as the presence verification system is unsure of the student's presence due to the distance (in metres) from the camera. Thus, initiating a re-authentication process at this stage is non-interruptive. Additionally, the "head on table" activity for Object D and the "look left/right" activity for Object E were re-classed to a high-risk threat class. A visual inspection of the activity frames in Figure 8-27 and Figure 8-28 reflects the re-class

decisions alongside the significant changes in the diameter statistics. In Table 8-20, it is observed that the "look left/right" and "look up" activities for Object C are re-classed as a low-risk. However, the newly assigned threat class for the "look left/right" does not match the expected high-risk threat class. It is noticed from the table that, the change in perimeter statistics is exactly 50%, which is a 'near-miss' to being re-classed as a high-risk.

Hence, whilst a low-risk threat class is good news for the student, the mismatched threat class accounts for the 1 misclassified activity out of the 5 reclassified activities. Thus, there is a 7% increase in the misclassification rate of the miscellaneous scenarios. Nevertheless, the 4 correctly reclassified activities from the miscellaneous scenarios improve the classification accuracy from 40% to 67%. Hence, based on the re-classification process the overall classification accuracy (i.e. the extent to which the fuzzy classifier engine is able to correctly classify the risk of an activity) is improved to 83%. Table 8-21 and Table 8-22 show the success rate results after the reclassification process.

	Classification accuracy rate (%)	**Misclassification accuracy rate (%)**	**Reclassification accuracy rate (%)**	**Misclassification accuracy rate (%)**
Frontal pose	100	-	-	-
Impersonation scenarios	87	13	-	-
Occlusion scenarios	100	-	-	-
Miscellaneous scenarios	40	26	67	7
Overall system accuracy	74	26	83	16

Table 8-21 Classification, misclassification and reclassification rates

			ARC Fuzzy threat class			
	Frame Activity	**Expected threat class**	**Object C**	**Object D**	**Object E**	**Classification accuracy**
Test case scenarios	Frontal pose	Low-risk	Low-risk	Low-risk	Low-risk	**100%**
Impersonation scenarios	External person move towards student	High-risk	High-risk	High-risk	High-risk	**87%**
	External person behind student	High-risk	High-risk	High-risk	High-risk	
	External person beside student	High-risk	High-risk	High-risk	High-risk	
	External person close to student	High-risk	High-risk	High-risk	High-risk	
	External person substitutes student	High-risk	Low-risk	Low-risk	High-risk	
Occlusion scenarios	Face close to camera	High-risk	High-risk	High-risk	High-risk	**100%**
	Hand blocking camera	High-risk	High-risk	High-risk	High-risk	
	Head blocking camera	High-risk	High-risk	High-risk	High-risk	
Miscellaneous scenarios	Head distant from camera	High-risk	High-risk	High-risk	High-risk	**67%**
	Head on table	High-risk	High-risk	High-risk	High-risk	
	Look left/right	High-risk	Low-risk	High-risk	High-risk	
	Look up	Low-risk	Low-risk	Low-risk	High-risk	
	Hand on forehead	Low-risk	High-risk	High-risk	High-risk	
			79%	**86%**	**86%**	

Table 8-22 Success rate after reclassification process

8.8 Discussion

Recall that the aim of the three experiments carried out in this chapter was to investigate the suitability of the pose estimation and the activity risk classification approaches for the Blob PV system. This section discusses the experimental results and the usefulness the approaches towards achieving presence verification.

8.8.1 Experiment 1

In the pose estimation approach, the idea is to map each activity to a blob statistics to determine a student's presence status. Thus, one of the lessons learnt in experiment 1, is the use of blob orientation statistics to estimate a student's frontal pose, i.e. to determine when a student is looking straight (directly) at the camera. This information was useful in establishing a student's reference pose; thus, all other poses occurring from the different activities can be calculated relative to the frontal/reference pose. However, findings from experiment 1 also showed that mapping each activity to a blob statistic proved problematic for non-frontal activities. This implies that relating an increase or decrease in blob area statistics to a "lean on left" activity or "right hand on cheek" activity is unreliable as a result of inconsistent measurements. The blob statistics values yielded dissimilar values across the different activities, making it difficult to determine the sameness of the student. For instance, an increase in blob area for a "look left" activity could yield a decrease in blob area for a "look right" activity of the same object. Thus, the findings in experiment 1 indicate uncertainty when using the pose estimation approach to determine that the same student at the start of the test is still the same student detected, due to the inconsistency in blob statistics

8.8.2 Experiment 2

One of the findings in experiment 1 was the usefulness of the blob orientation statistics in determining a student's frontal pose. This information was adopted in experiment 2 and it also informed the goal of this experiment. Still based on using the pose estimation approach (i.e. mapping an activity to a blob statistics), it was suggested that, the difficulty in determining the sameness of a student would be minimised by establishing a trend in the blob statistics values of similar activities across two students. This implies that, an increase in blob area for Student A's "hand on cheek" activity should yield an increase in blob area for Student B's "hand on cheek" activity. However,

the findings from experiment 2 indicate dissimilarity in the blob statistics for the two objects performing similar activities. In reality, this requirement would be impractical, as it would require that the students respond to activities in a similar fashion. Nevertheless, one of the useful lessons in experiment 2 was the changes to a student's pose as a result of the changes to the student's position and size relative to the cameras field of view. This also revealed significant information relation to a blob's extent statistics.

8.8.3 Experiment 3

From experiments 1 and 2, it was observed that irrespective of the problems associated with the pose estimation approach, some valuable lessons which were adopted in the activity risk classification (ARC) approach were revealed, i.e. the usefulness of the blob's orientation and extent statistics. Thus, in experiment 3 the ARC approach considered changes to the student's size (area statistics) and shape (major axis/minor axis statistics) with respect to the cameras field of view. In addition, the changes in the size and shape were combined with the position (orientation statistics), extent and count statistics. The values from the individual variables were fed into a fuzzy logic controller to make a decision on the detected student's presence. The fuzzy logic controller operates using a known logic-rule base that was informed from the statistics obtained in experiment 1 and 2. Thus, findings from the experiment indicate a significant change in size, shape, position, extent and count variables to suggest the likelihood of a student performing acceptable or unacceptable activities.

For example, when a student performs a "look up" activity, it is expected that the student's sameness attributes would be established provided that there is no significant change to the student's size, shape, count and extent statistics values. However, changes would be detected in the position statistics values as a result of the student's upward direction. Hence, by combining the statistics, the fuzzy controller makes a decision to determine the risk of the student's presence to the test environment. In the example given, a low-risk class is expected. The low-risk class is assigned provided that the other statistics values fall within the acceptable range, then the change in position only would be insufficient to determine the likelihood of an unacceptable activity. In reality, a student facing an upward direction is most likely the same student staring at the ceiling. As used in the pose estimation approach (experiments 1 and 2), the ARC approach was also tested using the trial datasets, Object's A and B. In this experiment, the findings

indicate stability and consistency in the blob statistics across the two different students performing similar activities. Additionally, an initial percentage of correctly detected and classified activities were given at an accuracy rate of 78%; however, a 100% classification accuracy rate is achievable after the reclassification process. This can be accomplished when the elevated-risk activities in the expected threat class is revised to a low-risk.

8.8.4 Evaluation

The evaluation experiments of the ARC approach was carried out on the datasets representing Object's C, D and E. the goal of these experiment was to evaluate the stability and the classification accuracy of the ARC approach across three different blob statistics extracted from three students that have not been involved in the trial experiments. Thus, three test case scenarios containing 13 activities were introduced to be simulated by the three students. The findings from the test scenarios show stability in blob statistics across the students. The classification accuracy of the frontal pose activities and the occlusion scenarios was 100%; this indicates that the presence of the detected students was correctly classified. In the impersonation scenario, the classification accuracy rate remained at 87% since there were no elevated-risk classes for reclassification. However, in this the scenario majority of the cheat/dishonest cases were correctly classified. The miscellaneous scenario was a combination of acceptable and unacceptable activities. 40% of the activities were correctly classified and majority of the classifications were an elevated-risk. Thus, a reclassification of the risks improved the accuracy rate to 67%. Finally, the overall accuracy rate for the evaluation experiments was set at 83% for correctly (re)classifying 35 out of 42 activities. It should be noted that issues relating to camera calibration, variable video frame rates, processing power and performance measurements of the ARC approach are relevant but not considered for this research; however, these issues will be discussed in the next chapter.

8.9 Summary

This chapter presented three experiments to demonstrate the feasibility of using a binary image to detect and verify presence in a test environment. From the experiments, the ARC approach emerged as a suitable method for the BlobPV system during summative e-assessments. Finally, in this chapter an evaluation of the ARC approach

was presented and the results were found stable across different objects. The evaluation experiments have confirmed the potential of blob-based presence verification solutions. The results confirm the capability of the BlobPV system to detect, verify and classify the risks observed from the student's presence in the test environment. The results demonstrate the feasibility of automatically controlling the decisions made about the student's presence from a set of well-defined logic rules. The next chapter describes the main contributions of this research and suggests the future outlook of presence verification in potential research areas such as un-supervised summative e-assessment, games assessment and non-assessment environments.

Chapter 9. Conclusion and Future work

This thesis capitalises on the importance of an extended user security model for summative e-assessments; thus, the concept of presence verification using a blob-analysis solution was proposed. This chapter presents the conclusions which reflect the research questions and objectives introduced in chapter one. Additionally, this chapter summarises the main contributions and a future outlook depicting the role of presence verification in security environments.

9.1 Conclusion

In an e-learning environment, the approach to learning and assessment is largely influenced by the existing learning theories which govern the educational process. To a behaviourist, assessment means a re-take of tests until the learning content is mastered, whilst cognitivists' view assessment as a process to enhance the prior knowledge of a learning resource. In a constructivists mind, the assessment process is a two-way process which involves interaction between the lecturer and the student. Thus, from an education perspective, the constructivist's school of thought promotes the modern methods of learning and assessing i.e. online learning and assessment. Influenced by information technology, the assessment process has gradually metamorphosed from the traditional pen and paper, classroom confined experience to an electronic environment that is not limited with walls. The e-assessment process embodies great benefits such as delivery of online tests, automatic marking, immediate feedback and opportunities for lifelong learning. Additionally, an online assessment can be designed to monitor the student's progress (formative), identify the student's strengths and weaknesses (diagnostic) or to report on the student's achievements at the end of a course (summative). The aforementioned assessments are designed to improve the student's learning; however, the high-stake nature of the summative e-assessments makes these tests a target for user security challenges. It is the responsibility of the user security process of a summative e-

assessment to ensure that only the correct student takes the summative test. Hence, the existing user security model solicit answers to the "who are you" (show your identity) and "is it really you" (confirm your identity) challenge questions. Commonly employed responses include the combination of a username and password or a username and a biometric (e.g. fingerprint). Thus, the Identity-Authentication user security model is simple, easy-to-use and it ensures that only the correct students can gain access to the assessment. However, the Identity-Authentication user security model is susceptible to security challenges which threaten the reliability and validity of the summative tests. One example of a pertinent user security challenge which poses a risk to the academic community is an impersonation threat.

Therefore, the first research goal of this thesis was focused on determining the reasons for the susceptibility of summative e-assessments to impersonation threats. To provide answers to the research question, the generic description associated with impersonation challenges was further classified into Type A, Type B and Type C impersonation threats. The type A or 'connived impersonation' threat can occur when an invigilator willingly colludes with fraudulent students to perpetrate an impersonation. The Type B impersonation threats can occur as a result the strength or weakness of the authentication method adopted; whilst, the Type C impersonation threat occurs, when an external person substitutes a correctly authenticated student during the test session. Hence, the results from the literature exploration suggested that the vulnerability of the Identity-Authentication (I-A) user security model is linked to a weakness in the model itself; thus, making the model fallible to the Type A, B and C impersonation threats. As proposed in this thesis, one way to improve the user security process is to combine the verification of the student's presence with the existing student's identity and authentication processes. Thus, it is responsibility of the Presence-Identity-Authentication (P-I-A) user security model to ensure that the correctly authenticated student at the beginning of a test is the same student that completes the test whist taking the test void of external assistance. This implies that, the model continuously solicits answers to the "are you the expected person there all the time" challenge question.

Recall from the first paragraph that, the username represents a response for the student's identity, whilst a biometric represents a suitable response for the student's authentication. Thus, the second research goal was focused on providing a method to represent a response for verifying the student's presence throughout the test session. In

chapter six, potential approaches such as face-to-face monitoring, continuous user authentication and continuous user monitoring were reviewed; however, these solutions are unsuitable for achieving presence verification during summative tests. The disadvantages of these solutions include connived impersonation threat, high-processing power, interruptive and distracting abilities. Hence, to provide answers to the second research question, an object tracking approach using a blob analysis solution was proposed. The blob analysis solution is a video processing technique that attempts to verify the student's presence throughout the test session.

By employing the blob analysis operation, a blob-based presence verification (BlobPV) system was designed to verify the student's presence in a non-interruptive and non-distracting fashion. From the BlobPV system architecture, two strategies were proposed as suitable approaches to detect and verify presence using the geometric statistics from binary images. Hence, to provide answers to the third research question, the feasibility and stability of the pose estimation and activity risk classification (ARC) approaches were evaluated. Results from the experiments, show the ARC approach as a suitable method for the BlobPV system as the approach was found stable across different objects. Additionally, the ARC evaluation results confirm the capability of the BlobPV system to detect, verify and classify the risks observed from the student's presence. Finally, the verification of a student's presence in a test environment presents valuable improvements to preserving the user security of summative e-assessments. From an education perspective, verifying a student's presence promotes the fairness, reliability and validity principles of online summative assessments.

9.2 Summary of Contributions

This thesis has presented a novel approach to improve the user security of summative e-assessments. In the process this thesis has made a number of contributions as noted below:

9.2.1 A goal-oriented user security model

The Presence-Identity-Authentication (P-I-A) user security model was developed has a result of the fallibility of the existing Identity-Authentication (I-A) user security model to user security challenges. One of the main security challenges in the I-A model is the exclusion of presence verification which can lead to the increase of impersonation

threats. Thus, the P-I-A model is an improved summative e-assessment user security model which emphasises the need to satisfy the presence security goal beyond the initial login/authentication procedure. In summative e-assessments, it is required that the correctly authenticated student at the start of a test remains the same student for the duration of the test; hence, the importance of verifying the student's presence throughout the test session. Additionally, verifying a student's presence preserves the security of the online summative test environment and promotes the reliability and validity of the e-assessment.

9.2.2 A presence verification system

The existing user security model employs suitable methods to achieve the identity and authentication processes, e.g. username/password or username/biometric fingerprint. Thus, having established the need to verify a student's presence, it is essential to employ a suitable method to achieve the verification process. The blob-based presence verification (BlobPV) system is a novel solution which adopts a video blob analysis operation to detect and classify the changes to a student's presence status in the test environment. The BlobPV system operates using a low processing power and the system does not require a high computational effort, which is synonymous with performing a constant biometric authentication. From a security perspective, the system has an advantage of deterring students from engaging in fraudulent activities, such as cheating or Type C impersonation threats. This security advantage occurs as a result of the quick detection of the significant changes in a student's pose which simultaneously reflects the student's activity in the test environment.

9.2.3 A blob classifier engine

In an assessment process it is essential that the use of technology does not inhibit a student's performance (QCA, 2007). Thus, employing technologies that can lead to frequent re-authentication requests may become interruptive and distracting to a student. The key contribution is that a blob classifier engine initiates change-driven re-authentication requests using fuzzy logic systems (FLS) for the decision making. In a change-driven system, the student is interrupted only when significant pose changes are detected from the blob statistics; hence, providing minimal distraction to the student throughout the summative e-assessment process.

9.2.4 A threat classification scheme

The threat classification scheme represents the decisions made by the fuzzy blob classifier engine; these are the low-risk, elevated-risk and high-risk threat classes. By using the threat classification scheme, the low-resource benefits of the BlobPV system is accentuated. For example a student can be at a low-risk to the test environment for the duration of the test. Thus, eliminating the need to employ high-level techniques or incur extra computational cost for verifying presence. Additionally, the classification scheme reduces the amount of re-authentication requests initiated, since the students are interrupted only when it is necessary. The minimised re-authentication requests is intended to replace the frequent re-authentication requests which can become frustrating to the student, especially when the student is still the same person. Hence, the dynamic nature of the threat classification scheme is also reflected in the elevated-risk class. An elevated-risk class can be referred to as a suspicious class, where the system estimates the likelihood of a dishonest activity based on the student's current pose. However, in this case the student's presence is not accurately verified; thus, a reclassification process which is oblivious to the student is carried out. The outcome of this process would determine the necessity of initiating a re-authentication request.

9.3 Future work

This thesis has introduced solutions to improve the user security of summative e-assessments. Suggestions to extend this work are described below:

9.3.1 Enhancing the efficiency of the reclassification process

A reclassification process is initiated when the detected presence is assigned an elevated-risk threat class. In its original implementation, the perimeter and diameter blob statistics from the student's frontal pose and current pose is compared. Thus, based on the amount of changes in the blob statistics, the blob classifier engine reclassifies the elevated-risk to a low-risk or high-risk threat class. The BlobPV system has provided a basic framework for the reclassification process that can easily be extended to include other methods. Hence, to improve the overall efficiency of the BlobPV system, a non-intrusive biometric method (e.g. face biometric) and a clock timer can be used in the reclassification process. Recall that, regardless of the student's activities within the test environment, a student's face is required to be within the cameras field of view for the

duration of the test. Therefore, a student engaged in suspicious activities would incur significant changes in blob statistics and would be at an elevated-risk to the test environment.

Hence, in the enhanced method when an elevated-risk threat class is assigned, the system would automatically initiate the face biometric process in order to detect and authenticate the student's face within a specified period to time. For example, the timer is set at 15secs to detect, capture and authenticate the student. In the event that within the 15secs (or specified time) the authentication process is successful a low-risk threat class is re-assigned; otherwise, a high-risk threat class is assigned.

9.3.2 Conducting wide-scale experiments for the BlobPV system

This research has successfully demonstrated the feasibility and stability of a blob-based presence verification system. However, it is important to take the BlobPV system to real-world test environments and conduct widespread experiments. Whilst these experiments could be a complex process, the deployment of the BlobPV system in real-life scenarios would determine the stability of the solution across a wider population. One of the benefits from this study would be determine the effects of different head sizes, head with scarves or turbans, gender and race on the blob-based presence verification system.

9.3.3 Presence verification in unsupervised e-assessment environments

This research focused on presence verification in supervised summative e-assessments, where the human invigilator is employed as a secondary form of security in the test environment. Thus, the invigilator can work alongside the automated verification system to ensure security. A future outlook would be to introduce the presence verification process in non-invigilated test environment, e.g. in distance learning courses. The focus would be to determine the impact of presence verification in improving the e-assessment user security in unsupervised environments. Additionally, the acceptability and privacy issues would be considered.

9.3.4 Presence verification in non-assessment online environments

There exists a wide range of applications that can benefit from incorporating the presence security goal into their existing Identity-Authentication 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. Future work would focus on integration of the presence verification process in variety of sectors such as online banking, online gaming and accessing computers in high-security environments.

9.4 Summary

The contributions of this research will improve the user security process of summative e-assessments from a presence-oriented user security model. Additionally, the video-based blob analysis solution depicts the feasibility of incorporating emerging technologies into higher education to provide a secure test environment; hence, promoting reliable, valid and fair summative assessments.

References

Adams, A., Sasse, M. (1999) Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. In: *Communications of the ACM*, 42(12), pp. 41-46

AERA (2000) *Position statement concerning high-stakes testing* www.aera.net/about/policy/stakes.htm, Accessed February 10, 2008

Agulla, E.G., Rifon, L.A., Alba castro, J.L., Mateo, G.C (2008) Is my student at the other side? Applying biometric web authentication to e-learning environments. In: Proceedings of the *8th IEEE International Conference on Advanced Learning (ICALT 2008),* Santander, Cantabria, Spain.

Ahmed AAE. And Traore, I. (2007) A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure computing,* 4(3), pp. 165–179.

Ali, M., Indupalli, S., Boufama, B. (2006) Tracking multiple for video surveillance. In: Proceedings of the *1st International Workshop on Video Processing for Security (VP4S-06), in CRV'06,* June 7-9,Quebec City, Canada

Allen, J., Barnum, S., Ellison, R., McGraw, G., Mead, N. (2008) *Software security engineering: A guide for project managers*, Boston, MA: Addison-Wesley Professional

Altinok, A. and Turk, M. (2003) Temporal integration of continuous multimodal biometrics. In: Proceedings of *Multimodal User Authentication'03,* December 11-12, Santa Barbara, CA , pp. 131-137

Anderson, R. (2001) *Security Engineering: A Guide to Building Dependable Disturbed Systems.* NY: John Wiley & Sons, Inc.

Angelo, T, and Cross, K.P (1993) *Classroom assessment techniques: A handbook for college teachers*: Jossey-Bass A Wiley Imprint, San Francisco, CA.

Anzaldua, R. M. (2002) *Item banks: Where, why, and how.* In: Proceedings of the 25th annual meeting for the Southwest Education Research Association, Austin, TX. http://www.eric.ed.gov/PDFS/ED462435.pdf, Accessed on December, 12 2009.

Aojula, H., Barber. J, Cullen, R., Andrews, J. (2006) Computer-based online summative assessment in undergraduate pharmacy teaching: The Manchester experience. *Pharmacy Education,* 6(4), pp. 229-236.

Apampa, K. M., Wills, G. B. and Argles, D. (2009b) Towards security requirements in online summative assessments. In: Proceedings of the *World Conference on E-Learning in Corporate, Government, Healthcare & Higher Education (E-Learn 2009)* October 26-30, Vancouver BC, Canada.

Apampa, K. M., Wills, G. B., Argles, D. (2009a) Towards security goals in summative e-assessment security. In: *E-learning Security Workshop (ELS-2009) in conjunction with ICITST'09,* November 9-12, London, UK.

Apampa, K. M., Wills, G. B., Argles, D. (2010a) An approach to presence verification in summative e-assessment security. In: *E-learning Security Workshop (ELS-2010) in conjunction with i-Society-2010,* June 28-30, London, UK.

Apampa, K. M., Wills, G. B., Argles, D. (2010b) Towards a Blob-based Presence Verification System in Summative E-Assessments. In: Proceedings of the *International Computer Assisted Assessment (CAA 2010) Conference Research into E-Assessment,* July 20-21, Southampton, UK.

Apampa, K. M., Wills, G. B., Argles, D., Marais, E. (2008a) Electronic integrity issues in e-assessment security. In*:* Proceedings of the *8th IEEE International Conference on Advanced Learning (ICALT 2008)*, July 1-5, Santander, Cantabria, Spain.

Apampa, K. M., Zhang, T., Wills, G. B., Argles, D. (2008b) Ensuring privacy of biometric factors in multi-factor authentication systems. In: Proceedings of the *International Conference on Security and Cryptography (SECRYPT 2008),* July 26-29, Porto, Portugal.

AQA. Assessment and Qualifications Alliance. (2007) *e-Assessment: Frequently Asked Questions.* http://www.aqa.org.uk/over/eassessment_faq.php, Accessed on February 10, 2008.

Argles, D., Pease, A., Walters, J. (2007) An improved approach to secure authentication and signing. In: Proceedings of the *21st International Conference on Advanced Information Networking and Applications Workshop (AINAW '07),* May 21-23, Niagara Falls, Ontario, vol. 1, pp. 119-123

Asbourn, J. (2005) *The social implication of the wide scale implementation of biometric and related technologies.* European Commission, DG JRC, Sevilla, Spain

Asha, S. and Chellappan, C**.** (2008). Authentication of E-learners using multimodal biometric technology. In: Proceedings of the *International Symposium on Biometrics and Security Technologies (ISBAST 2008),* April 23-24, Islamabad, pp. 1-6

Ashbourn, J. (2000) *Biometrics Advanced Identity Verification*. London: Springer-Verlag.

Au, C., Skaff, S., Clark, J. (2006) Anomaly detection for video surveillance applications. In: Proceedings of the *18th International Conference on Pattern Recognition (ICPR'06),* August 20-24, Hong Kong, pp. 888-891

Aviles, C. B. (2001) Grading with norm-referenced or criterion-referenced measurements: to curve or not to curve, that is the question. *Social Work Education,* 20(5), pp. 6093-608

Bailie, J. and Jortberg, M. (2009) Online learner authentication: Verifying the identity of online user's. *MERLOT Journal of Online Learning and Teaching*, 5(2), pp. 197-207.

Baird, H. (1997) *Performance Assessment for Science Teachers,* http://www.schools.utah.gov/curr/science/Perform/past1.htm, Accessed April 10, 2008

Bas, E., Tekalp, A., Salman, F. (2007) Automatic vehicles counting from video for traffic flow analysis. In: Proceedings of the *IEEE Intelligent Vehicles Symposium,* June 13-15, Istanbul, pp. 392-397

Bauersfeld, H. (1995) Language games in the mathematics classroom: Their function and their effects. In P. Cobb & H. Bauersfeld (eds.) *The emergence of mathematical meaning: Interaction in classroom cultures,* NJ: Lawrence Erlbaum, pp. 211-292.

Beard, R. M. (1970) Considerations for group discussions. *Conferences on Assessment of Learning, Courses and Teaching,* University of London Institute of Education

Bharagav-Spantzel, A., Camenisch, J., Gross, T., Sommer, D. (2006) Privacy preserving multi-factor authentication with biometrics. In: Proceedings of the *2nd ACM Workshop on Digital Identity Management,* Alexandria, Virginia, pp. 63-72

Biggs, N.L. (2002) *Discrete Mathematics*. 2nd edition. NY: Oxford University Press

Birchfield, S. (1998) Elliptical head tracking using intensity gradients and color histograms. In: Proceedings of *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'98),* June 23-25, Santa Barbara, CA, pp. 232-237, 1998.

Black, P. and D. Wiliam (1998) Inside the Black Box: Raising standards through classroom assessment. *Phi Delta Kappan.* 80(2), pp. 139-148.

Blanz, V., Grother, P., Phillips, P.J., Vetter, T. (2005) Face recognition based on frontal views generated from non-frontal images. In: Proceedings of the *IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2005),* June 20-26, San Diego, CA, pp. 454–461

Bolle, R., Connell, J., Pankanti, S., Ratha, N., Senior, A. (2003) *Guide to Biometrics Springer Professional Computing.* New York Inc: Springer-Verlag.

Boston, C. (2002) The concept of formative assessment. *Practical Assessment Research & Evaluation,* 8(9). http://pareonline.net/getvn.asp?v=8&n=9, Accessed December 10, 2007.

Boyd, C. and Mathuria, A. (2003) *Protocols for Authentication and Key Establishment,* Berlin: Springer-Verlag.

Braithwaite, M., vonSeelen, C., Cambier, J., Daugman, J., Glass, R., Moore, R., Scott, I. (2002) Application-specific biometrics templates. In: Proceedings of the

IEEE Workshop on Automatic Identification Advanced Technologies, Tarrytown NY, pp.167-171

Brown, G. (2001) Assessment: A guide for lecturers. *LTSN Generic Centre Assessment Series No 3.* York: LTSN.

Brown, S., Race, P., Smith B. (1996) *500 Tips on Assessment*, London: Kogan Page.

Bruner, J. (1966) *Studies in cognitive growth: A collaboration at the center for cognitive studies*. New York: Wiley & Sons

Cass, S. and Riezenman, M.J. (2002) Improving security, preserving privacy. *IEEE Spectrum,* 39(1), pp. 44-49

Challis, D. (2005) Committing to quality learning through adaptive online assessment. *Assessment in Education*, 30(5), pp. 519-527.

Charman, D. (1999) Issues and impacts of using computer-based assessments (CBAs) for formative assessment. In S. Brown, P. Race and J. Bull (eds.) *Computer-assisted assessment in higher education*, Abingdon, Oxon: Routledge, pp. 85-93.

Chen, D. and Yang, J. (2005) Online learning region confidences for object tracking. In: Proceedings of the *2nd Joint IEEE International Workshop on Visual Surveillance and Performance Evaluation of Tracking and Surveillance (VS-PETS'05),* Beijing, pp. 1-8

CIEA. Chartered Institute of Educational Assessors. (2007) Assessment Reliability. http://www.ciea.org.uk/knowledge_centre/articles_speeches/general_articles/assessment_reliability.aspx, Accessed April 10, 2008

Cizek, G.J. (1999) *Cheating on tests: How to do it, detect it and prevent it.* New Jersey: Lawrence Erlbaum Associates

Clarke, N.L., Furnell, S.M (2007) Advanced user authentication for mobile devices. *Computers & Security*, 26(2), pp.109-119

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

Coomey, M., and Stephenson, J. (2001) Online learning: it is all about dialogue, involvement, support and control – according to research. *Teaching and Learning Online,* London: Kogan Page.

Cowie, B. (2005) Pupil commentary on assessment for learning. *Curriculum Journal* 16(2), pp. 137-151.

Cucchiara, R., Grana, C., Prati, A., Vezzani, R. (2005) Probabilistic posture classification for human behaviour analysis. I*EEE Transactions on Systems, Man and Cybernetics – Part A,* 35(1), pp. 42-54

Daugman, J. (1993) High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 15(1), pp. 1148-1161

Daugman, J. (2004) How iris recognition works. IEEE *Transactions Circuits and Systems for Video Technology,* 14(1), pp. 21-30

Davida, G., Frankel, Y., Matt, B. (1998) On enabling secure applications through off-line biometric identification. In Proceedings of the *IEEE Symposium on Security and Privacy*. Oakland, CA, USA.

Delac, K. and Grgic, M. (2004) A survey of biometric recognition methods. In: Proceedings of the *46th International Symposium Electronics in Marine (ELMAR-2004)*, Zadar, Croatia, pp. 184-193

Dodge, B. (2001) *FOCUS:* Five rules for writing a great WebQuest. *Learning and Leading with Technology,* 28(8), 6-9, 58.

Driscoll, M. (2002*) Blended Learning: Let's get beyond the hype.* Learning and training innovations newsline. Accessed December 3, 2007 http://www.ltimagazine.com/ltimagazine/article/articleDetail.jsp?id=11755.

Dunn, L., Parry, S., Morgan, C. (2002) Seeking quality in criterion referenced assessment. *Learning Communities and Assessment Cultures Conference Organised by the EARLI Special Interest Group on Assessment and Evaluation*, August 28-30, University of Northumbria.

Earl, L. (2003) *Assessment as Learning: Using Classroom Assessment to Maximise Student Learning.* Thousand-Oaks, CA: Corwin Press.

Ecclestone, K. (1996) *How to assess the vocational curriculum*, London: Routledge

Elton, L. (2002) *Good assessment practice*. Accessed April 10, 2008, http://www.materials.ac.uk/events/assessmentgp.pdf

Ertmer, P. and Newby, T. (1993) Behaviorism, cognitivism, constructivism: comparing critical features from an Instructional design perspective. *Performance Improvement Quarterly*, 6(4), pp. 50-72.

Finlayson, H., Maxwell, B., Caillau, I. and Tomalin, J. (2006) *Impact of e-learning in student intermediate and end-point outcomes in further education.* http://www.education.gov.uk/research/data/uploadfiles/RR739.pdf, Accessed August 4, 2009.

Fitzgibbon, D., Filu, M., Fisher, R. (1999) Direct least square fitting of ellipse. IEEE *Transactions on Patten Analysis and Machine Intelligence,* 21(5), pp. 476-480

Fuentes, L. and Velastin, S. (2006) People tracking in surveillance applications. *Image and Vision Computing,* 24(11), pp. 1165-1171

Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S. (2007) A robust single sign-on model based on multi-agent system and PKI. In: Proceedings of the *Sixth International Conference on Networking (ICN'07)*, Martinique, pp. 101- 107

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

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

Garrison, D.R. and Anderson, T. (2003) *E-Learning in the 21st Century: A framework for research and practice,* London: Routledge

Gibbs G. and C. Simpson (2002), *How assessment influences student learning – A conceptual overview*. http://hlst.brookes.ac.uk/current/assessment%20_influences.pdf, Accessed July 20, 2008.

Gilbert, L. and Gale, V. (2008) *Principles of e-learning systems engineering*. Oxford, England: Chandos Publishing.

Gilbert, L., Gale, V., Wills, G. and Warburton, B. (2009) Report on E-*Assessment Quality (REAQ) in UK Higher Education*, University of Southampton, UK. Accessed December 15, 2009, http://eprints.ecs.soton.ac.uk/17697/1/REAQ_Final_Report_v1-4.pdf

Gipps, C. (2003) Should universities adopt ICT-based assessment? *Exchange,* Issue 4, Spring 2003, www.exchange.ac.uk/issue4.asp, Accessed March 15, 2008.

Gollman, D. (2006) *Computer Security.* West Sussex, England: John Wiley & Sons.

Gonzalez-Tablas, A., Diaz-Pabon, A., Alvarez, B., Garnacho, A. (2006) EVAWEB v2: Enhancing a web-based assessment system. In: Proceedings of the *4th International Conference on Multimedia and Information Communication Technologies in Education,* Sevilla, Spain, pp. 837-840

Graf, F. (2002) Providing Security for E-Learning. *Computer Graphics* 21(1), pp. 355-365

Gulati, S. (2004) Constructivism and emerging online learning pedagogy: A discussion for formal to acknowledge and promote the informal. Paper Presented at the *Universities Association for Continuing Education Conference*, April 5-7 University of Glamorgan. http://www.leeds.ac.uk/educol/documents/00003562.htm, Accessed December 12, 2007.

Halevi, S. and Krawczyk, H. (1999) Public-key cryptography and password protocols. *ACM Transactions on Information and System Security*, 2(3), pp. 230-268

Haley, C. B., Laney, R. C., Moffett, J.D., Nuseibeh, B. (2008) Security Requirements Engineering: A Framework for Representation and Analysis, *Transactions on Software Engineering (IEEE)* 34(1), pp. 133-153

Haley, C. B., Laney, R. C., Nuseibeh, B. (2004) Deriving Security Requirements from Crosscutting. In: Proceedings of the *3rd International Conference on Aspect-Oriented Software Development (AOSD'04),* Lancaster, UK, pp. 112-121.

Haley, C.B., Moffett, D., Laney, R., Nuseibeh, B. (2006) A Framework for Security Requirements Engineering. In: the proceedings of the *International Workshop on Software Engineering for Secure Systems (SESS'06),* Shanghai, China, pp. 35-42.

Haller, N. (1994) The S/Key one-time password system. In: Proceedings of the *Symposium on Network and Distributed Systems Security*, San Diego, CA, pp. 151-157, Internet Society.

Hanley, S. (1994) *On Constructivism*. Accessed December 12, 2007, http://www.inform.umd.edu/UMS+State/UMDProjects/MCTP/Essays/Constructivism.txt

Haralick, R. and Shapiro, L. (1992) *Computer and Robot Vision,* Volume. I, Boston, MA: Addison-Wesley

Hartley, J. (1998) *Learning and Studying: A research perspective*, London: Routledge.

Harvey, J. and Mogey, N. (1999) Pragmatic issues when integrating technology into the assessment of students. In S. Brown, P. Race and J. Bull (eds.) *Computer-assisted assessment in higher education*, Abingdon, Oxon: Routledge, pp. 7-19.

Harwood, I.A. (2005) When summative computer-aided assessments go wrong: disaster recovery after a major failure. *British Journal of Educational Technology*, 36(1), Special issue on Thwarted Innovation in E-Learning

Hattie, J. and H. Timperley (2007) The power of feedback. *Review of Educational Research,* 77(1): 81-112.

Heinrich, E., Milne, J., & Moore, M. (2009) An investigation into e-tool use for formative assignment assessment: Status and Recommendations. *Educational Technology & Society*, 12(4), pp. 176–192.

Hernandez, J.A., Ortiz, A.O., Andaverde, J., Burlak, G. (2008) Biometrics in online assessments: A Study Case in high school students. In: *Proceedings of the 18th international conference on electronics, communications and computers. (CONIELECOMP'08),* Cholula, Puebla, Mexico, pp. 111-116.

Holt, D. and Willard-Holt, C. (2000) Let's get real – students solving authentic corporate problems. *Phi Delta Kappan,* 82(3), pp. 243-246

Hugl, U. (2005) Tech-developments and possible influences on learning processes and functioning in the future. *Journal of American Academy of Business,* 6(2), pp. 250-256

ISO/IEC (2005) Information technology - security techniques - evaluation criteria for IT security, *Part 1: Introduction and General Model, 15408-1* http://www.iso.org/iso/catalogue_detail.htm?csnumber=40612, Accessed August 20, 2009

Jain, A. K. and Uludag, U. (2003) Hiding biometric data. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(11), pp. 1493-1498.

Jain, A., Greiss, F., Connell, S. (2002) Online Signature Verification. *Pattern Recognition,* 35(12), pp. 2963 – 2972

Jain, A., Hong, L., Pankanti, S. (2000) Biometric identification. *Communications of the ACM,* 43(2), pp. 91-98.

Jain, A., Nandakumar, K., Nagar, A. (2007) Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, Hindawi Publishing Corporation.

Jain, A., Ross, A., Prabhakar, S. (2004) An introduction to biometric recognition. In: Proceedings of the *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), pp. 4-20

Jain, A.K., Hong, L., Pankanti, S., Bolle, R. (1997) An identity-authentication system using fingerprints. *Proceedings of the IEEE,* 85(9**)**, pp. 1365-1388

Jantzen, J. (1998) *Tutorial on Fuzzy Logic.* Technical University of Denmark, 98-e-868 edition. www.iau.dtu.dk/~jj/pubs/logic.pdf, Accessed March 15, 2010.

Javed, O. and Shah, M. (2002) Tracking and object classifications for automated surveillance. In: Proceedings of the *7th European Conference on Computer Vision – Part IV, (ECCV'02),* Copenhagen, Denmark, pp. 323-357

JISC. Joint Information Systems Committee (2004) *Federated Access Management.* http://www.jisc.ac.uk/news/stories/2006/03/access_qanda.aspx, Accessed April 10, 2008.

JISC. Joint Information Systems Committee (2006) *e-Assessment Glossary (Extended),* http://www.jisc.ac.uk/uploaded_documents/eAssess-Glossary-Extended-v1-01.pdf, Accessed March, 15, 2008

JISC. Joint Information Systems Committee (2007) *Effective Practice with e-Assessment*, Accessed, February 25, 2008 http://www.jisc.ac.uk/media/documents/themes/elearning/effpraceassess.pdf

Johnson, M. and S. Green (2004) On-line Assessment: the impact of mode on student performance. Paper presented at the *British Educational Research Association* conference, September 15-18, University Manchester Institute of Scene and Technology, UK.

Jones, V. and Jo, J.H. (2004) Ubiquitous learning environment: An adaptive teaching system using ubiquitous technology**.** In: Proceedings of the *21st ASCILITE Conference*, December 5-8, Perth, Western Australia, pp. 468-474

Kaminskienė, L. and Janulienė, A. (2006) Problem-based learning in the academic setting: Language teaching issues. Accessed December 20, 2007 http://www.coactivity.vgtu.lt/upload/filosof_zurn/l_kaminskiene_%20januliene_filologija_nr2.pdf

Kelly, L. and Melograno, V (2004) *Developing the Physical Education Curriculum: An Achievement-Based Approach*, Champaign, IL, USA: Human Kinetics.

Kerka, S. and Wonacott, M. (2000) *Assessing learners online*. ERIC, clearing house on adult, career and vocational education. Accessed May 20, 2009 http://www.eric.ed.gov/PDFS/ED448285.pdf

King, C, Guyette, R., Piotrowski, C. (2009) Online exams and cheating: An empirical analysis of business students views. *The Journal of Educators Online, 6*(1)

Klein, D.V (1990) Foiling the Cracker: A survey of, and improvements to, password security. In: Proceedings of the *2nd USENIX security workshop,* Portland, pp. 5-14

Klir, G. and Yuan, B (1995) *Fuzzy Sets and Fuzzy Logic: Theory and applications,* Upper Saddle River, NJ: Prentice-Hall, PTR

Klosterman A. and Ganger, G (2000) *Secure continuous biometric-enhanced authentication.* Technical Report CMU-CS-00-134, May, 2000, Carnegie Mellon University.

Knight, P. T. (2001) A briefing on key concepts: formative and summative, criterion and norm-referenced assessment. *LTSN Generic Centre Assessment Series No 7.* York: LTSN

Ko, C. and Cheng, C. (2004) Secure internet examination system based on video monitoring. *Internet research* 14(1), pp. 48–61

Kutty, K. Schapira, R, van Ruiswyk, J. (2003) *Kochar's Concise Textbook of Medicine*, 4th edition, Baltimore, MD: Lippincott Williams & Wilkins.

Laroussi, M. (2004) New E-Learning Services Based on Mobile and Ubiquitous Computing: Ubi-Learn Project. *Computer Aided Learning in Engineering Education (CALIE'04),* Grenoble, France. Accessed February 20, 2008 http://hal.inria.fr/docs/00/19/01/86/PDF/Laroussi_2004.pdf

Laurillard, D. (1995) Multimedia and the changing experience of the learner. *The British journal of Educational Technology*, 26(3), pp. 179-189

Levy, Y. and Ramim, M. (2007) A theoretical approach for biometrics authentication of e-exams. In: Proceedings of the *Chais Conference on Instructional Technologies Research*, the Open University of Israel, Raanana, Israel.

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,* 5(1), pp. 379-397

Liang, W. and Wang, W. (2005) On performance analysis of challenge/response based authentication in wireless networks. *Journal of Computer Networks and ISDN Systems*, 48(2), pp. 267-288

Lin, N.H., Korba, L., Yee, G., Shih, T., Lin, H.W (2004) Security and privacy technologies for distance education applications. In: Proceedings of the *18th International Conference on Advanced Information Networking and Applications (AINA'04),* March 29-31, Fukuoka, Japan, pp. 580-585

Lipton, A., Fujiyoshi, H., Patil, R. (1998) Moving target classification and tracking from real-time video. In: Proceedings of the *4th IEEE Workshop on Applications of Computer Vision (WACV'98),* October 19-21, Princeton, NJ, pp. 8-14

Lister, R. and L. Leany (2003) Introductory programming, criterion-referencing, and bloom. In: Proceedings of the *34th SIGCSE Technical Symposium on Computer Science Education,* Reno Nevada, 35(1), pp. 143-147

Lowe, G. (1995) An Attack on the Needham-Schroeder public-key authentication protocol. *Information Processing Letters*, 56(3), pp. 131-133

Macian, V., Tormos, B., Sala, A., Ramirez, J. (2006) Fuzzy logic-based expert system for diesel engine oil analyses diagnosis. *Insight (BINDT),* 48(8), pp. 462-469

Maio, D., Maltoni, D., Cappelli, R., Wayman, J., Jain, A. (2004) FVC2004: Third fingerprint verification competition. In: Proceedings of the *International Conference on Biometric Authentication (ICBA),* Hong Kong, pp. 1–7.

Marais, E., D. Argles, von Solms, S.H (2006) Security Issues Specific to e-Assessments. In: Proceedings of the *8th Annual Conference on WWW Applications*, September 6-8, Bloemfontein.

Masie, E. (2003) Blended Learning: The magic is in the mix. In A. Rossett (Eds.), *The ASTD E-Learning Handbook*, McGraw-Hill, pp. 59-63.

Mason, R. (1998) Models of online courses. *Asynchronous Learning Networks Magazine,* 2(2). Accessed January 10, 2008 http://aln.org/alnweb/magazine/vol2_issue2/Masonfinal.html

Mason, R. (2002) Information and communication technologies in education and training. *Scientific and Technological Options Assessment Series*, http://www.europarl.europa.eu/stoa/publications/studies/stoa106_en.pdf, Accessed April 10, 2008.

Mattern, F. (2004) Wireless Future: Ubiquitous Computing. In: Proceedings of *Wireless Congress*, Munich, Germany.

McIvor, A. (2000) Background subtraction techniques. In: Proceedings of *Image and Vision Computing,* Auckland, New Zealand, pp. 147-153

McKenna, C. and Bull, J. (2000) Quality assurance of Computer-assisted assessment: practical and strategic issues. In: *Quality Assurance in Education,* 8 (1) pp. 24-31.

McLafferty, C. and Foust, K. (2004) Electronic plagiarism as a college instructor's nightmare prevention and detection: Cyber dimensions. *Journal of Education for Business,* 79(3) pp.186-190

Mendel, J. (1995) Fuzzy logic systems for engineering: A tutorial. *Proceedings of the IEEE,* 83(3) pp. 345-377

Menezes, A., v. Oorschot, P., Vanstone, S. (1997) *The Handbook of Applied Cryptography*, Florida: CRC Press LLC.

Mergel, B. (1998) *Instructional design and learning theory* http://www.usask.ca/education/coursework/802papers/mergel/brenda.htm, Accessed February 10, 2008

Mikalsen, A.B., Klefstad, B., Horgen, S.A., Hjeltnes, T. (2008) An integrated multimedia e-Learning for vocational training. In: Proceedings of the *6th International Conference on Networked Learning (NLC2008)*, Halkidiki, Greece.

Miller, C. and M. Parlett (1973) *Up to the Mark: A research report on assessment.* Occasional paper (13), pp. 115, University of Edinburgh, UK

Mödritscher, F. (2006) E-Learning theories in practice: A comparison of three methods. *Journal of Universal Science and Technology of Learning*, pp. 3-18

Monrose, F. and Rubin, A.D (2000) Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4), pp. 351-359

Morgan, C. and O'reilly, M. (1999) *Assessing Open and Distance Learners*. London: Routledge.

Mueller, J. (2005) The authentic assessment toolbox: Enhancing student learning through online faculty development, *Journal of Online Learning and Teaching* 1(1)

Nanavati, S., Thieme, M., Nanavati, R. (2002) *Biometrics: Identity verification in a networked world*. London: John Wiley and Sons.

Naude, E. and Hörne, T. (2006) Cheating or collaborative work: Does it pay? *Issues in Informing Science and Information Technology,* 3(1), pp. 459-466

Nemoto, T., Hatazakis, G., Thorpe, C., Olivenstein, R., Dial, S., Bates, J. (1999) Automatic control of pressure support mechanical ventilation using fuzzy logic. *American Journal of Respiratory and Critical Care Medicine,* 160(2), pp. 550-556

Nightingale, P., Tewiata, I., Toohey, S., Ryan, G., Highes, C., Magin, D. (1996) *Assessing Learning in Universities.* Sydney: University of New South Wales Press.

Nowak, J.A. and Plucker, J.A. (1999) *Do as I Say, Not as I Do: Student assessment in problem-based learning*, Indiana University. Accessed February 10, 2008, http://www.indiana.edu/~legobots/q515/pbl.html

Ohishi, T., Komiya, Y., Matusumoto, T. (2000) Online signature verification using pen-position, pen-pressure and pen-inclination trajectories. In: Proceedings of the *15th International Conference on Pattern Recognition (ICPR'00),* Barcelona, Spain, pp. 547 –550

Oliver, R. & Herrington, J. (2003) Exploring technology-mediated learning from a pedagogical perspective. *Journal of Interactive Learning Environments*, 11(2), pp. 111-126.

Oorschot, P. and Thorpe, J. (2008) On predictive models and user-drawn graphical passwords. *ACM Transactions on Information and system Security (TISSEC),* 10(4), pp. 1-33

Otsu, N. (1979) A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man and Cybernetics (SMC),* 9(1), pp. 62-66

Padilla, A.M and Perez, W. (2003) Acculturation, Identity and Social Cognition: A New Perspective. *Hispanic Journal of Behavioural Sciences,* 25(1), pp. 35-55

Parker. P, Fleming, P., Beyerlein. S, Apple. D, Krumsieg, K. (2001) Differentiating assessment from evaluation as continuous improvement tools. In: Proceedings of the *31st ASEE/IEEE Frontiers in Education* Conference, Reno, NV.

Paulsen, M.F. (2000) An International Analysis of Web-based Education and Strategic Recommendations for Future Development of Online Education, *IVETTE Workshop*, Barcelona.

Pfleeger, C. and S. Pfleeger (2003) *Security in Computing*. Upper Saddle River, New Jersey: Prentice Hall.

Piaget, J. (1955) *The child's construction of reality.* London: Routledge and Kegan Paul

Prabhakar, S., Pankanti, S., Jain, A.K. (2003) Biometric recognition: security and privacy concerns. *IEEE Security and Privacy Magazine,* 1(2), pp. 33-42

Prior, J. C. and R. Lister (2004) The backwash effect on SQL skills grading. In: Proceedings of the *9th ACM SIGCSE Conference on Innovation and Technology in Computer Science Education (ITiCSE '04)* 36(3), pp. 32-36, Leeds, UK

QCA. Qualifications and Curriculum Authority. (2007) *Regulatory Principles for E-assessment*. http://www.qcda.gov.uk/resources/5798.aspx, Accessed May 19, 2008.

Quality Assurance Agency (2006) *Section 6: Assessment of Students*. Code of Practice for Assurance of Academic Quality in Higher Education. Accessed July 5, 2009 http://www.qaa.ac.uk/academicinfrastructure/codeOfPractice/section6/COP_AOS.pdf

Rabuzin, K. Baca, M. Sjako M. (2006) E-Learning: Biometrics as a security factor. In: Proceedings of the *International Multi-Conference on Computing in the Global Information Technology (ICCGI'06),* Bucharest, pp. 64-70

Race, P. (2001) Assessment: A guide for students. *LTSN Generic Centre Assessment Series No 4.* York: LTSN.

Ratha, N. Connell, J., Bolle, R. (2001) Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal,* 40(3), pp. 614-634.

Ratha, N., Chikkerur, S., Connell, J, Bolle, R. (2007) Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 29(4), pp. 561-572.

RFC 1777 *Lightweight Directory Access Protocol (LDAP)*. Network Working Group, March 1995, http://www.rfc-archive.org/getrfc.php?rfc=1777, Accessed December 20, 2009.

Rhem, J. (1998) *Problem-based learning: An Introduction.* In: The National Teaching and Learning Forum, 8(1). Accessed February 10, 2008. http://www.ntlf.com/html/pi/9812/v8n1smpl.pdf

Rosbottom, J. (1997) Computer managed, open question, open book assessment. In: Proceedings of the *2nd Conference on Integrating Technology into Computer Science Education (ITiCSE '97)* Uppsala, Sweden, pp. 100-102

Rosenfeld, A. (1970) Connectivity in digital pictures. *Journal of ACM,* 17(1), pp. 146-160

Rovai, A. P. (2000) Online and traditional assessments: what is the difference? *The Internet and Higher Education.* 3(3), pp. 141-151.

Rowe, N. C. (2004). Cheating in online student assessment: Beyond plagiarism. *Online Journal of Distance Learning Administration,* VII (II).

Rowntree, D. (1990) *Teaching through Self Instruction*. London: Kogan Page.

Sacchi, C., Regazzoni, C., Vernazza, G. (2001) A neural network-based image processing system for detection of vandal acts in unmanned railway environments. In: Proceedings of the *11th International Conference on Image Analysis and Processing,* September 26-28, Palermo, Italy, pp. 529-534

Sadler, R. (1989). Formative assessment and the design of instructional systems. *Instructional Science*, 18 (2), pp. 119-144.

Sanchez-Reillo, R., Sanchez-Avila, C., Gonzalez-Marcos, A. (2000) Biometric Identification through Hand Geometry Measurements. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 22(10), pp. 1168-1171

Sandhu, R. S. and P. Samarati (1994) Access control: Principles and practice. *IEEE Communications Magazine,* 32(9), pp. 40-48.

Sangi, N. (2008) Electronic assessment issues and practices in Pakistan: A case study. *Learning Media and Technology*, 33(1), pp. 191-220

Schwiebert, L. P. and Bondurant, W (2000) Summative feedback, evaluation, and grading students. In P.M. Paulman, J.Susman and C.A. Abboud (eds.), *Precepting Medical Students in the Office.* Baltimore: John Hopkins University Press, pp. 81-87

Scottish Qualifications Authority (2007) *Guide to effective practice- Section 7.* http://www.sqa.org.uk/sqa/files_ccc/Section_7.pdf, Accessed March 25, 2010.

Shafarenko, A. and Barsky, D. (2000) A secure examination system with multi-mode input on the World Wide Web. In: Proceedings of the *International Workshop on Advanced Learning Technologies (IWALT 2000),* Palmerston North, NZ, pp. 97-100

Sharma, P and Hannafin, M. J. (2007) Scaffolding in technology-enhanced learning environments. *Interactive Learning Environments,* 15(1), pp. 27-46

Sheu, H., Chen, H., Hu, W. (1997) Consistent symmetric axis method for robust detection of ellipses. *IEEE Vision, Image and Signal Processing,* 144(6), pp. 332-338

Shibbleth (2001) *Shibboleth overview and requirements*. Accessed April 20, 2009. http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-requirements-01.html

Sim, T., Zhang, S., Janakiraman, R., Kumar, S. (2007) Continuous Verification Using Multimodal Biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 29(4), pp. 687-700

Skinner B.F. (1957) *Verbal Learning,* New York: Appleton-Century-Crofts

Skinner, B. F. (1983) Origins of a hehaviourist, *Psychology Today*, pp. 22–33.

Speck, B.W (2002) Learning-teaching-assessment paradigms and the on-line classroom. In R.S Anderson, John F. Bauer, B.W Speck (eds.), *Assessment Strategies for the Online Class: From Theory to Practice.* New Directions for Teaching and Learning, 2002(91), pp. 5-18.

SQA. Scottish Qualifications Authority. (2003). *Guidelines on Online Assessment for Further Education*, http://www.sqa.org.uk/sqa/2424.html. Accessed May 10, 2008

Stallings, W. (2000) *Data and Computer Communications*, Upper Saddle River, New Jersey: Prentice Hall.

Stallkamp, J., Ekenel, H.K., Stiefelhagen, R (2007) Video-based face recognition on real-world data. In: Proceedings of the *11th IEEE International Conference on Computer Vision (ICCV 2007),* Rio de Janeiro, pp. 1-8

Steiner, J., Neuman, B., Schiller, J. (1988) Kerberos: An authentication service for open network systems. In: Proceedings of the *Winter 1988 Usenix Conference*, pp. 191-201

Stoner, G. (1996) *Implementing Learning Technology*. Learning Technology Dissemination Initiative (LTDI). http://www.icbl.hw.ac.uk/ltdi/implementing-it/implt.pdf, Accessed July 5, 2009.

Summons, P. and Simons, C. (1998) Authentication Strategies for Online Assessments. In: Proceedings of the *3rd Australian Computer Science Education Conference (ACSE98),* Brisbane, Australia, pp.101 -105

Sutcu, Y., Li, Q., Memon, N. (2007) How to protect biometric templates. In: the *SPIE conference on security, steganography and watermarking of multimedia contents IX*, San Jose, CA, vol. 6505.

Taber, K.S. (2003) Examining structure and context - questioning the nature and purpose of summative assessment. *School Science Review,* 85(311), pp.35-42

Thorndike, E. L. (1911) *Animal intelligence*, New York: Macmillan

Tolman, E. C. (1932). *Purposive behavior in animals and men*. New York: Century

Turner, R. and Eden, A. (2008) The Philosophy of Computer Science. Stanford Encyclopaedia of Philosophy, http://plato.stanford.edu/entries/computer-science/, Accessed December 12, 2009.

Velipasalar, Y., Tian, L., Hampapur, A. (2006) Automatic counting of interacting people by using a single uncalibrated camera. In: *IEEE International Conference on Multimedia and Expo,* July 9-12, Toronto, Ontario, pp. 1265-1268

Vollans, T. (2008) *The Law School with two Masters?* Web Journal of Current Legal Issues. http://webjcli.ncl.ac.uk/2008/issue2/vollans2.html, Accessed July 5, 2009.

Von Glasersfeld, E. (1989) Constructivism in education. In T. Husen & N. Postlewaite (eds.) *International Encyclopaedia of Education*. Oxford, England: Pergamon Press, pp.162-163.

Von Solms B. (2004) Information Security Governance in ICT-Based Educational Systems, In: *Discourse*, 32(1)

Vygotsky, L. (1978) Interaction between Learning and Development. *Mind in society*, pp. 79-91. Cambridge, MA: Harvard University Press.

Vygotsky, L. (1986) *Thought and language*. Boston: MIT Press.

Walton, S. (2005) KS3 ICT Onscreen Test Project. In: *Qualifications & Curriculum Authority, BETT 2005*, Accessed December 5, 2010 http://www.qca.org.uk/downloads/6967_ks3_ict_bett_2005.pdf.

Warren, M and Hutchinson, W. (2003) Information Security: An E-Learning Problem. In: Proceedings of the *2nd International Conference on Advances in Web-Based Learning (ICWL'03),* Melbourne, Australia, pp. 21-26

Wayman, J. (2001) Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics*, 1(1), pp. 93-113.

WebCT Security (2005). How to protect your identity and use WebCT at the same time. http://www.cofc.ecu/~webct/faculty/WebCTSecurity.pdf, Accessed December 12, 2009

Weippl, E. R. (2005) *Security in E-Learning (Advances in Information Security)* New York: Springer-Verlag

Weippl, E. R. (2006) On the use of test centers in e-Assessment, *eLearningreports.*

Wild, M. (2007) *Third Generation eLearning*. Accessed December 10. 2007, http://www.ninelanterns.com.au/files/9L/pdf/Third-Gen-eLearning.pdf

Williams, C. (2002) Learning On-line: A review of recent literature in a rapidly expanding field. *Journal of Further and Higher Education,* 26(3), pp. 263-272

Williams, J. M. (2002) New security paradigms. In: *Proceedings of the 2002 Workshop on New Security Paradigms,* Virginia Beach, Virginia, pp. 97-107.

Wisher, R. Curnov, C., Belanich, J. (2005) Verifying the Learner in distance learning. In: Proceedings of the *18th Annual Conference on Distance Teaching and Learning*, August 13-15, Madison, WI.

Wu, P., Kuo, C., Wu, P., Wu, T. (2006) Design a competence-based networked learning system: Using sequence control as example. In: Proceedings of the *Current Developments in Technology-Assisted Education*, pp. 787-791

Wu, X., Qu, Y., Qian, H., Xu, Y. (2005) A detection system for human abnormal behaviour. In: Proceedings of the *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2005),* August 2-6, Edmonton, Canada, pp. 1204-1208

Xiao, Q. and Yang, X.D (2009) A facial presence monitoring system for information security. In: *IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms and Applications (CIB 2009),* Nashville, TN, pp.69-76

Xu, Y., Roy-Chowdhury, A., Patel, K. (2007) Pose and illumination invariant face recognition in video. In: Proceedings of the *IEEE Conference on Computer Vision and Pattern Recognition (CVPR'07),* June 17-22, Minneapolis, MN, pp. 1-7

Yager, R. (1992) A general approach to rule aggregation in fuzzy logic control. *Applied Intelligence,* 2(4), pp. 333-361

Yang, G., Wong, D., Wang, H., Deng, X (2008) Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences* 74(7), pp. 1160-1172

Yang, S. J. (2006) Context Aware Ubiquitous Learning Environments for Peer-to-Peer Collaborative. *Learning Educational Technology & Society,* 9(1), pp. 188-201.

Yanosky, R. and Salaway, G. (2006) *Identity management in higher education: A baseline Study.* EDUCAUSE Center for Applied Research. Accessed August 5, 2009. http://net.educause.edu/ir/library/pdf/ers0602/rs/ers0602w.pdf

Zadeh, L (1975) The concept of a linguistic variable and its application to approximate reasoning - Part 1. *Information Sciences,* 8(3), pp. 199-249

Zadeh, L. (1965) Fuzzy Sets. *Information and Control,* 8(3), pp. 338-353

Zang, Q. and Klette, R. (2003) Object classification and tracking in video surveillance. In: Proceedings of the *Computer Analysis of Images and Patterns, LNCS 2756,* Springer, Berlin, pp. 198-205

Zhang, J., Lu, Y., Jonathan-Wu, Q. (2005) Real time head tracking via camera saccade and shape-fitting. In: Proceedings of the *2nd International Conference on Image Analysis and Recognition (ICIAR 2005),* September 28-30, Toronto, Canada, pp. 828-835

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

Zhang, Z., Gunes, H., Massimo, P. (2009) Head detection for video surveillance based on categorical hair and skin colour models. In: Proceedings of the *16th IEEE International Conference on Image Processing (ICIP'09),* November 7-10, Cairo, pp. 1133-1136

Zhou, Q. and Aggarwal, J. (2001) Tracking and classifying moving objects from video. In Proceedings of *2nd IEEE Workshop on Performance Evaluation of Tracking and Surveillance (PETS),* Kauai, USA.

Zimmermann, H. (1996) *Fuzzy Set Theory and its Applications*, 3rd Edition, Norwell, MA: Kluwer Academic Publishing.

Appendix A – Original Blob Statistics for Object C, D, E

Frame Activity	Object	Area	Major axis	Minor axis	Orientation	Extent	Count
Frontal pose	C	21261	286.0868	184.019	1.386602	0.505444	1
	D	27791	225.8474	164.03607	1.539372	0.772616	1
	E	23133	286.0819	195.88117	1.50045	0.488069	1
External person move towards student	C	43509	372.83	295.0673	0.771746	0.501672	1
	D	49457	290.6023	255.85236	1.355859	0.605534	1
	E	55881	511.8144	302.46279	0.112718	0.403269	1
External person behind student	C	52901	457.9309	255.847	0.35458	0.474674	1
	D	49879	360.2165	226.48596	0.455082	0.537825	1
	E	56537	511.6389	304.08743	0.118576	0.407093	1
External person beside student	C	88419	487.3256	377.6271	0.856224	0.455721	1
	D	5032	190.7193	69.86876	0.337647	0.268245	2
	E	34105	289.7863	250.07594	0.947578	0.46996	2
External person close to student	C	24480	319.0891	195.7513	1.30189	0.446341	2
	D	33833	255.7823	198.40009	1.163474	0.631543	2
	E	8868	201.2501	104.75109	1.568208	0.483692	2
External person substitutes student	C	18968	181.5104	140.0482	1.517957	0.769805	1
	D	25462	341.2683	196.14244	1.439074	0.456014	1
	E	39760	279.1929	205.20624	1.391304	0.659808	1

Impersonation Scenarios: Original Blob Statistics for Object C, D, E

Frame Activity	Object	Area	Major axis	Minor axis	Orientation	Extent	Count
Frontal pose	C	21261	286.0868	184.019	1.386602	0.505444	1
	D	27791	225.8474	164.03607	1.539372	0.772616	1
	E	23133	286.0819	195.88117	1.50045	0.488069	1
Face close to camera	C	42932	465.9693	268.1093	1.243719	0.418931	1
	D	60994	395.6331	262.39731	0.769867	0.493359	1
	E	12081	417.1879	251.19107	0.00795	0.157481	2

Hand blocking camera	C	6045	229.1088	61.36547	0.330614	0.292131	2
	D	49374	287.0751	235.52843	0.741295	0.740918	3
	E	44514	396.7635	213.77295	0.157539	0.462849	1
Head blocking camera	C	46743	265.7664	237.9355	0.726596	0.770256	2
	D	123703	570.0566	418.59937	1.018174	0.463534	1
	E	30159	324.2947	172.64105	0.083075	0.391675	2

Occlusion Scenarios: Original Blob Statistics for Object C, D, E

Frame Activity	Object	Area	Major axis	Minor axis	Orientation	Extent	Count
Frontal pose	C	21261	286.0868	184.019	1.386602	0.505444	1
	D	27791	225.8474	164.03607	1.539372	0.772616	1
	E	23133	286.0819	195.88117	1.50045	0.488069	1
Head distant from camera	C	10814	178.1817	123.1689	1.553475	0.595091	1
	D	3587	84.15369	57.970001	0.008733	0.767273	0
	E	3023	132.1032	73.71718	0.077031	0.422797	0
Head on table	C	44874	387.2208	159.6796	0.009739	0.678911	1
	D	50368	376.8663	233.13316	0.586941	0.460369	1
	E	48918	348.9756	211.40189	0.171683	0.550333	1
Look left/right	C	29727	293.6331	192.6124	1.47529	0.508302	1
	D	45261	310.2054	195.85124	0.008995	0.780766	1
	E	8828	168.7048	89.62405	0.66196	0.361285	1
Look up	C	13493	287.0408	187.6383	1.281776	0.32446	1
	D	22161	179.7643	167.31694	1.13273	0.745058	1
	E	7173	167.9834	98.40503	0.037212	0.476865	0
Hand on forehead	C	50513	380.4709	277.3537	0.921683	0.5413	1
	D	49501	317.3228	250.99887	0.112587	0.49871	1
	E	4931	226.5512	54.32388	1.217404	0.244157	1

Miscellaneous Scenarios: Original Blob Statistics for Object C, D, E