Authentication of Students and Students' Work in E-Learning

By Hannan Xiao (h.xiao@herts.ac.uk) and Wei Ji (w.1.ji@herts.ac.uk)

July 2011

This report consists of three parts:

Part I. Overview and authentication of students and students' exams in E-learning

Part II. Authentication of students and students' coursework in E-learning

Part III. Proposal for further research in authentication of students and students' coursework in E-Learning

Table of Content

Part I. Overview and Authentication of Students and Students' Exams in E-learning

Hannan Xiao (h.xiao@herts.ac.uk)

Wei Ji (w.1.ji@herts.ac.uk)

Abrar Ullah* (a.ullah3@herts.ac.uk)

* Abrar Ullah is a research student who contributes subsections 3.1-3.4.

Table of Content

1. Introduction

Global e-learning market is projected to reach $107.3 billion by 2015 according to a new report by The Global Industry Analyst (Analyst 2010). The popularity and growth of the online programmes within the School of Computer Science obviously is in line with this projection. However, also on the rise are students' dishonesty and cheating in the open and virtual environment of e-learning courses (Shepherd 2008). Institutions offering e-learning programmes are facing the challenges of deterring and detecting these misbehaviours by introducing security mechanisms to the current e-learning platforms. In particular, authenticating that a registered student indeed takes an online assessment, e.g., an exam or a coursework, is essential for the institutions to give the credit to the correct candidate.

Authenticating a student is to ensure that a student is indeed who he says he is. Authenticating a student's work goes one step further to ensure that an authenticated student indeed does the submitted work himself. This report is to investigate and compare current possible techniques and solutions for authenticating distance learning student and/or their work remotely for the e-learning programmes. The report also aims to recommend some solutions that fit with UH StudyNet platform.

2. A Survey

At the beginning of the project, a survey was carried out among the members of academic staff who have been teaching on the online programmes within the School of Computer Science. The purpose of the survey is to study the types of assessments used in online programmes, and to collect colleagues' awareness of possible student cheatings in these assessments and opinions on providing solutions in authenticating students and their work. Appendix 1 shows the survey questionnaire.

The colleagues participated in the survey have good experiences of online teaching with 33% teaching on more than 3 online modules and 67% teaching on more than 2 modules across different levels of BSc and MSc. The results show that individual coursework is favoured as the main assessment method (92%) compared to in-class-test (42%) and examination (17%) (see Figure 1). Group coursework is not adopted due to the lack of face-to-face communication among students. The coursework ranges from question-and-answers, programming codes, short reports, to long project report (see Figure 2). QuestionMark has been used in online exams containing both multiple choice questions and open-answer questions.

Colleagues are concerned about online students' cheating in submitted work. Although only being asked to tick the most concerned type of cheating, many of them wrote "all of the above". As shown in Figure 3, plagiarism is still the most common cheating and concern (83%) while impersonation seems to be the least worried by tutors. However, hiring or finding someone else to do the coursework for the students becomes the biggest concern if combined them together. Turnitin has been commonly practised to detect plagiarism by academic staff. Colleagues would welcome a solution for authenticating student and/or their work if not too much administrative overhead is required.
'

Figure 1: Percentage of Assessment in Online Programme

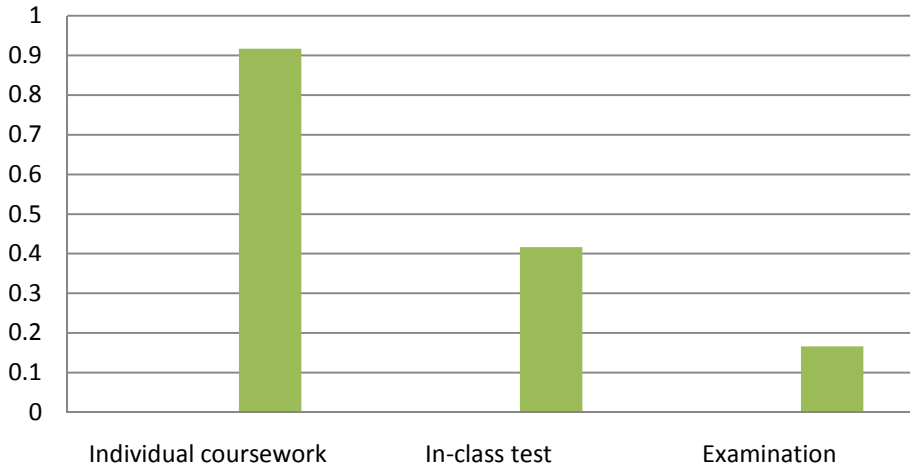


Figure 2: Percentage of different types of individual coursework

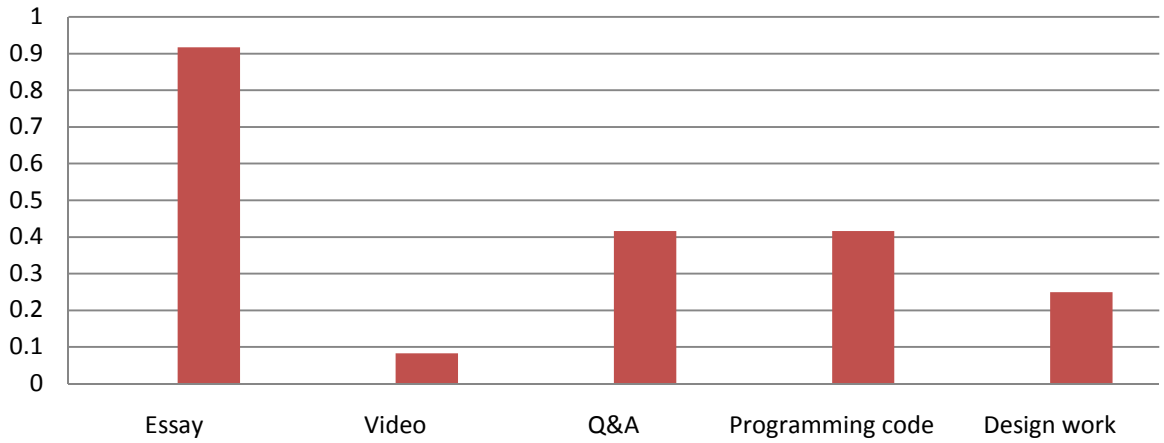
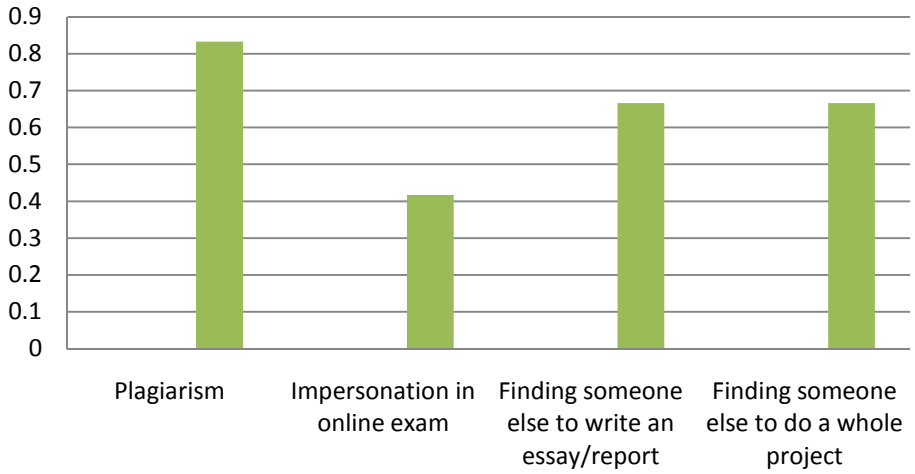


Figure 3: Cheating Concerns



3. Approaches

Researchers in the e-learning sector have been investigating various ideas from leading research outcomes to address the vulnerabilities in e-learning authentication in order to gain trust of educational institutions and other end users. The following subsections outline some of the well established authentication techniques adopted for verification of student identity on the e-learning systems.

3.1 Proctored Examination

Proctored examination refers to human or automated supervision of examinations. (Marais, Argles et al. 2006) suggests that, online examination should be taken in a supervised location. In Proctored exam, only registered candidates are invited for the exam session as initial authentication step and further verification may be administered later on the recorded or face to face session. Application of proctored examination in distance learning enhances credibility of e-learning by minimising threats. The proctored examination requires students to be available for the supervised examination on a scheduled time. Proctored examination methods are explained below:

- Face-to-Face Proctoring: This is a traditional and legacy supervision and authentication procedure for examinations, where candidate's identity is verified face to face. The course work is delivered via distance learning and finally the assessment is monitored in a face to face session. The candidate requires attending an examination centre at a scheduled time (University 2007). This requires extensive resources for invigilation and may not be an ideal way for distance learning education. Some may conduct regional face-to-face proctored examination in an attempt to reduce the travelling cost for distance learners (Dentistry 2011).
- Video Conference Proctoring: This is an attempt to make e-learning similar to face to face supervision of examination process by video conference or online camera recording (Bari, Sullivan et al. 2004). The examination is proctored remotely via web link and learner may access assessment module from home PC (Mahmood 2010). This method requires the candidate to appear online for assessment at a specified schedule and invigilators require proctoring the examination session.

The face-to-face Proctored examination incurs additional administration, travelling cost and may be an expensive option for an online programme with global reach. The video conference Proctored Examination requires audio and video hardware and all learners require web camera and microphone for their exam session (Strobl 2010). It may be a challenge to accommodate learners in one examination session from different universal time zones. Face-to-face Proctored examination may be helpful to authenticate, however, it may be resource intensive and not in line with the goals of distance learning. Video conference proctoring may be less expensive option as compare to face-to-face examination in designated centres.

3.2 User Id and Password

It is one of the widely used authentication methods across the Internet. Traditionally, user id and password are the simplest and widely used authentication scheme of verifying digital identities (Das, Saxena et al. 2004; World 2004). The learners are provided with a user name and password and the information is used during authentication process to verify supplied pattern against stored credentials on the system. It has proven to be a safe method of authentication as password are made strong by implementation of password salt, multiple attempts locking and encryption techniques. However, passwords with low entropy are prone to off-line dictionary attacks (Bellovin and Merritt 1993; Huiping 2010), risking user impersonation. In e-learning environment, learners can voluntarily pass on their password to a third party in order to gain maximum credit on the online course. Other threats to the use of user id and password are hacking software', which can break security of applications with low entropy password (Ives, Walsh et al. 2004).

In spite the strength and weaknesses, it is still a preferred way of first line authentication on e-learning and other web applications at large, which cannot be written off. However, to maximise the effectiveness of password based authentication, this can be coupled with additional techniques.

3.3 Biometrics

In biometric authentication, user identification process is performed by verification of individual's physical or behavioural characteristics (Asha and Chellappan 2008). Biometric frees individual from passwords and carrying cards as the person is the key for identification (Gil, Castro et al. 2010). A number of biometric authentication features have been evolved from recent research and some of them are integrated in e-learning systems including finger print, video authentication, face recognition, audio recognition or combination of these features in a form of multi modal biometrics. Biometrics have recently emerged as the most reliable form of authentication and employed at high security zones, restricted access installations, service access, advance and domestic computer systems. With rapid developments in e-learning systems, biometric features are used as authentication component in e-learning security model. An analytical view of known authentication techniques in context of e-learning is given below.

3.3.1 Finger Print

It is one of the widely used of all biometrics authentication features (Ali, Ali et al. 2006; Aggarwal, Ratha et al. 2008; Asha and Chellappan 2008). The fingerprint biometric technique is phased out in multiple steps, initially acquisition of sample, processing and storage; secondly taking user input and finally the matching step. Fingerprint is individual's physical characteristic which works as a unique global identifier and is a reliable authentication candidate. The user logins remotely using fingerprint scanner to gain access to learning system. This feature is consistent and fitting the needs to solve the purpose easily with less complexity compare to other biometric traits. Fingerprint readers are highly portable and available at low cost (Auernheimer and Tsai 2005).

Fingerprint authentication improves the overall authentication; however, it has other drawbacks which compromises its value (Derakhshani, Schuckers et al. 2003). The wider implementation of fingerprint over the internet in disbursed geographical locations with additional hardware peripherals incurs additional cost. It requires software integration within e-Learning system and has additional administration requirements like sample recording for each user etc. (Aggarwal, Ratha et al. 2008). Individual's fingerprint can be lifted from surfaces of objects without one's knowledge (Derakhshani, Schuckers et al. 2003; Moini and Madni 2009) and used for replay attacks. Security of stored fingerprint pattern may be an issue, when the course is finished.

3.3.2 Face Recognition

In face recognition biometric, individual face snap shot is used for authentication. Face recognition biometric trait implements image recognition and pattern matching algorithms to verify user identity (Zhao and Ye 2010). Face sample is acquired, processed and stored during registration and enrolment phase. Authentication is implemented by using image recognition algorithms for identification of complex human face structure. The extracted face images are analysed and compared with the stored image to find a match in order to validate. The user' face image is extracted using a digital camera, and image processing techniques are applied for matching compatibility.

Face recognition has a number of problems due to complexity of computer image recognition over the years (Shashua 1997). Variable face expression, capture point direction, variable light, environment, web camera, weather and other pertinent accessories (beards, glasses) can make matching difficult and prone to errors (Srisuk, Petrou et al. 2003). Although, 3D image capture attempts to solve the issue of positioning, nevertheless, the special camera and software' pack could be a costly solution. Face recognition biometric may not ensure robust and secure authentication for e-learning system (Agulla, Rifón et al. 2008). Like other biometric features, face recognition is also an expensive adaptation in the e-learning arena. Digital camera of certain specification, high speed Internet, and administration of the process adds to the problems of face recognition authentication technique.

3.3.3 Audio, Voice or Speech Authentication

The audio or voice biometric is used both for speech recognition and speaker identification (Chandra and Sunitha 2009). It is a biometric trait, where human voice is recognized using automated system based on the data from speech wave. Acoustic, voice pitch and speaking style or accent in the human voice provide a unique identifier for using it as a biometric trait (Jayamaha, Senadheera et al. 2008). The user authentication in voice recognition is performed in two phases. In first phase, user' voice print is stored through automated software application during the enrolment. In the authentication phase, user's test sample is taken and matching is performed by comparing a variety of voice features with the saved audio pattern. The sample may be recorded both text-dependent, when user needs to speak the same word in authentication as recorded and text-independent, when user is not bound to read the same text as recorded (Chandra and Sunitha 2009).

However, varying speaking speed e.g. fast, slow, louder, environmental noises, quality of recording equipment are the factors that makes it less reliable for authentication in distance learning as compared to other biometrics. (Hayes and Ringwood 2009) states, that intra-individual variation can be a major practical issue in speaker recognition. User training is another overhead when recording voice samples during the enrolment and authentication. Some researchers suggest that microphone or recording system variation affects the error rate in voice authentication (Shaver and Acken 2009). The user' voice may be recorded for use in replay attacks as the 'liveness' of user can not be verified (Eveno and Besacier 2005).

It is inferred from the literature review that speaker recognition may not provide a requisite solution for use with distance learning system due to known challenges and higher degree of complexity (Eveno and Besacier 2005; Shaver and Acken 2009).

3.3.4 Signature Recognition

Evolution in technology has enabled capture and verification of signature using computer software giving recognition to signature biometric feature (Meshoul and Batouche 2010). Signature verification has been widely used and highly acceptable in day to day life transactions (Jain, Ross et al. 2006; Adamski and Saeed 2008). Technology enabled signature recognition is one of the behavioural biometric traits and a potential candidate for user authentication. Purpose built accessories like digital signature pads, tablets and digital pens are used to capture signature information (Adamski and Saeed 2008). In the first step signatures are recorded using digital pad and pen, and processed before storing to the database. The processing and matching of signature depends upon the type of algorithm used for authentication like Hidden Markov Model (HMM)(Kashi, Hu et al. 1998; Muramatsu and Matsumoto 2003; Coetzer, Herbst et al. 2004; Afsar, Arif et al. 2005; Gruber, Hook et al. 2006), Dynamic Time Wrapping (DTW)(Parizeau and Plamondon 1990; Wirtz 1995; Fang, Leung et al. 2003; Fang, Wu et al. 2005; Adamski and Saeed 2008), Neural Networks (Bajaj and Chaudhury 1997) and Support Vector Machine (SVM)(Justino, Bortolozzi et al. 2005). In the authentication phase, signature of individual user is captured, processed and compared with the recorded reference to verify the signature as genuine or forged.

However, signature recognition may not deliver authentication accuracy (Jazahanim, Ibrahim et al.). It incurs extra cost on additional hardware and software.

3.4 Challenge Questions

Challenge questions are important authentication and credential recovery technique. The challenge questions authentication has been used by leading email providers such as Yahoo, Google, Microsoft and AOL for credential recovery process, when user needs to reset or retrieve lost credentials (Schechter, Brush et al. 2009). A set of questions are initially stored during the registration process and individuals are queried to answer the questions during authentication or recovery process. Challenge questions may be reliable and unique as it pertains to information known to individual users.

Low entropy questions are prone to brute force attack and thus not very secure (Just and Aspinall 2009). Challenge Questions memorability, information in public knowledge, lack of clarity may cause security and usability issues (Griffith and Jakobsson 2005).

To our knowledge, based on review of research literature, this form of authentication has not been used in the e-learning platform for user verification. However, (Jortberg 2009) argues to implement Challenge Questions from a US consumer database for e-learning platforms. Since e-learning has global reach, hence, consumer database would not have enough information about every individual undertaking an online course. Implementation of Challenge Questions has other challenges including, Integration, data protection, accessibility, bandwidth usage and data tariff for using third party database (Jortberg 2009). Answer to certain questions may be easily guessed, and hence, low entropy questions are prone to dictionary and brute force attack. Challenge questions authentication is not a first level authentication like user id and password (Just and Aspinall 2009).

3.5 Comparison of Approaches

Table 1 is taken from (Jortberg 2009) paper which lists the four primary available approaches for student authentication.

Methodology	**Challenge Questions**	**Biometrics and Web Video Recording**	**Web Video Conference**	**Proctor Face-to-Face Proctored Exam**
	Challenge questions based on third-party data.	Unique typing style or fingerprint plus targeted recording of student in exam via webcam.	Audio and video Conference proctoring via webcam. Screen monitoring service with live, certified proctors.	Face to face with government or institution issued identification.
Mainstream Use	Widely used in financial services.	New, rarely used.	New, but used in family communications.	Commonly used.
Sophisticated	Yes. Based on large-scale databases of U.S. public records.	Yes. Uses newest web conference technology and biometrics or unique typing sequencing.	Yes. Uses newest Web conference technology.	No
Privacy	Student releases directory data to a third party. Institution never sees/ receives data. Leverages publicly available data from prior address, phone and other available data. No FERPA violations. Covered by Gramm-Leach- Bliley Act and Driver's Privacy Protection Act.	Institution has access to videos of students taking assessments. Need policies for video review, use and release. Maintain database of student ID, directory information and student fingerprint or unique typing sequence	Students participate in audio and video broadcast during exams. Proctor conducts exams from start to finish, with no intervention required from institution.	Student shows government-issued ID at approved facility.
Technical Pre-requisites	Integration to learning Management software. Dial-up Internet connection. Secure access to third-party system.	Proprietary software, integration to learning or assessment software and broadband.	Commercially available webcam and broadband.	Varies by location. May require special software and PC. Each location requires review by academic staff.
Student Enrolment or Registration Process	None required. Supports walk-up students.	Capture fingerprint, typing samples or digital pictures. Device registration for student and student's PC. May require student signature on consent form.	Acquire webcam upon enrolment. Student schedules exam with proctor via scheduling system.	Usually none for on-campus facilities. May require preregistration of exam time, location and proctor.
Administration or Academic Staff Efforts	Determine when to pose identity questions. Determine	Set up course assessment in software, or integrate	Instruct students to schedule exams with proctor. Onetime	Proctor must ensure student complies with

	ramifications of failure to authenticate. Onetime distance learning staff involvement to set up process and program monitoring.	to learning software. Troubleshoot devices and user training, and monitor post assessment video or audio. Manage device availability, inventory, assignment to students and break / fix process. Program monitoring to oversee usage.	distance learning staff involvement to set up process and program monitoring.	proctored exam policies and procedures. (No calculator, no notes, etc.) Staff to verify proctor quality, proctor facilities, time, exam shipping, etc.
Additional Institution or Student Costs	None	Server software and Database applications. Shipping costs for special device. May require specialized webcam or PC software.	Purchase of a standard, sound equipped webcam.	Varies. Some institutions have no cost testing facility sharing agreements, others charge for access. Some remote facilities charge $15 to $75 per assessment.
Investment*	$2–4 per exam $8–18 per student per year	$25–45 per exam $150–270 per student per year	$15–20 per exam	$90–120 per student per year Varies from free to $75 per exam

**Assuming six courses per year and two assessments per course*

Table 1. Comparison of authentication approaches (Jortberg 2009)

4. Commercial Solutions

There are various commercial products available. This section surveyed four commercial products in the aspects of software and hardware, usages and cost. Contacts have been made with the company for demos, quotations and discussions. Finally, cost analysis is carried out across the products.

4.1 Proctor U

ProctorU (ProctorU 2011) is a live proctoring service for students taking exams online via web cam. It is a half-automatic proctoring approach since human proctors are needed remotely invigilating the whole duration of an online exam. Students are authenticated by the certified proctor through remotely ID checking and challenging questions from a US consumer database – a twofold multi-factor authentication process.

Software and Hardware:

No software needs to be downloaded except that an executable file on ProctorU website should be clicked to start the examination process.

There are no extra requirements on hardware. The standard requirements are listed on (ProctorU 2011):

(1) PC Users: A well-working computer running Windows XP or higher with 1024 MB of RAM or higher
(2) A web cam with 640x480 video pixel resolution (web cams built into laptops or monitors are acceptable)
(3) Headphones or working speakers connected to the computer
(4) A microphone connected to the computer (your web cam or laptop may already have one built into it.)
(5) A reliable high speed internet connection (minimum 768 Kbps/384 Kbps Download/Upload)
(6) A web browser with Adobe Flash Player installed
(7) Student's authority to allow remote access to student's computer and screen by a proctor

Usage:

A demo had been run between the ProctorU and the School on 28th June 2011. Through the demo the following steps for a student to take an online exam with ProctorU are understood.

(1) Student logins to the Proctor U website by username and password pre-setup by the company. Once login, the student page shows a pre-booked online exam session.
(2) The student chooses to take the exam and clicks an executable file on the web page. The executed application connects the student to a video chat with a live proctor from proctoring centers. The proctor can see the student's screen and can have full control over the student's computer if permitted by the student. This allows the proctor to help the student through the exam process during the exam if he has technical difficulties.

(3) The proctor authenticates the student by asking to see an official photo ID. Comparing the photo on the ID and the one in the student with the student himself remotely helps the proctor decide whether the student is the genuine registered student.
(4) The proctor also asks the student to answer a few questions about him that are generated from a US costumer database. Four questions were asked during the demo with a pass rate set at 50%.
(5) The student can start the exam after the twofold authentication process is done. During the exam, the certified proctor invigilates the whole exam remotely. Any suspicious conducts will be recorded in the log.
(6) Once the exam is finished, the executable file clears up any temporary files from the student's computer regarding the exam.
(7) The exam log file saved at thProctorU server can be accessed and reviewed by tutors or administrators anytime afterwards.

Cost:

The cost is straightforward. Quotation is given as $25.00 per two-hour (or less) exam in June 2011. Exam times are based on the maximum time limit of the exam. The rate would include all administrative and technical support as well. Proctor U provides the proctors, the technical support, the scheduling, the customer service, and the setup. Students are able to schedule appointments online in the time frame they specify. There is no setup fee, no contract fee, and no minimum number of exams.

Payment can be made by the institution monthly or by the student via credit card when they make an appointment. Note that in the "student pays" scenario, it doesn't cost the institution anything.

It seems proctorU has established many partnership institutions as seen on their website. Discussion with technical people after the demo reveals that there is no public information about UK or other students outside US. ProctorU would be happy to provide just online proctoring plus remote photo identity check without asking challenging questions, at a reduced price.

4.2 Secureexam Remote Proctor

Securexam Remote Proctor (SecureExam 2011) is intended to remove the need for test centres by allowing computer-based assessments to be administered remotely with a similar level of exam room integrity. As the vender has been contacted by colleagues within the School (Pyper et al. 2010), no new contact has been made with the company this time.

Software and Hardware:

The software includes a secure browser to lock down the testing application and restrict key functions during examinations (e.g. copy and paste, accessing files and folders, opening applications, access to browsers). The hardware is a USB powered device with a 360 degree

webcam, a microphone and a biometric fingerprint scanner. This device sits on the desktop during examinations and monitors the environment.

Usage:

(1) Enrollment: This involves capturing an image of their fingerprint and taking a digital photo of their face (possibly next to some form of ID). No fingerprint images are stored; instead key points on the image are mapped to create a digital key.

(2) Student Authentication. This includes: placing their finger on the scanner, to compare with the biometrics stored during the initial enrolment, followed by the taking of a picture of their face and some form of photographic ID or just their face.

(3) Take the assessment (e.g. as mediated by QuestionMark Perception). During the assessment, audio and video monitoring is used to capture the session. Securexam Remote Proctor captures 30 seconds of video that are uploaded to the server at 30 second intervals. As monitoring data are stored locally and synchronized remotely, the reliability of student internet connections should not be an issue. These captures are available for review by the institution or, alternatively, a review service can be purchased from Software Secure.

Costs:

Hardware device (one-off). Price does not include P&P.	£100
Software (per annum)	£20
Technical support 24/7 (per annum)	£10

The cost of the capture review service provided by Software Secure is 5p per minute.
In terms of costs, if we assume that a 'direct' Level 6 student takes 3 taught modules over a period of 1 year and that each module would have one 90-minute assessment, the overall cost per student would be £143.50 (i.e. £100 + £20 + £10 + £13.50, where £13.50 is the cost of reviewing the assessment captures). In practical terms, we would be paying around £31 per hour of assessment invigilation (Pyper et al. 2010).

4.3 Bio-Pen

Bio-Pen (BioPen 2011) solution is based on user's signature recognition to authenticate a student whose handwriting contains unique biometric information.

Software and Hardware:

A driver is required to be installed to use with Bio-Pen. The driver is PC compatible (Windows 98/NT/ME/2000/XP/Vista). Note Linux system is not compatible with the driver. There is a charge for updating the software/driver after initial investment in the Pen.

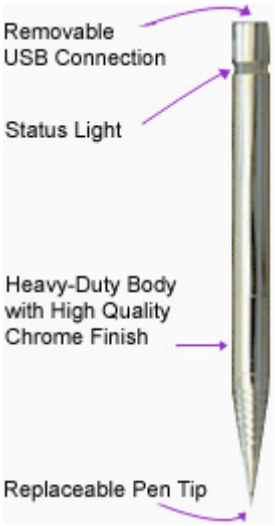


Figure 4: Bio-Pen (picture from BioPen 2010)

Hatdware is the Bio-Pen itself as shown in Figure 4. The Pen has a USB connection and works by capturing the biometric feature such as the inertial and pressure forces on the Pen and time intervals between strokes in each dimension. As a result the multi-dimensional signature cannot be spoofed because a student cannot instruct or coerce another to apply forces on a Bio-Pen to recreate his signature. Unlike username and password to be passed around by students, Bio-Pen cannot be used by anyone else except its owner. The Pen captures the unique act of signing rather than the signature. Sensors inside the Bio-Pen capture information which is encoded and encrypted. Copying and replay are prevented due to the processing on the signal. In addition, because the stored data is not reversible the original signature or any other personal information cannot be obtained so as piracy is eliminated.

Usage:

Contacts have been made to the European representative of Bio-Pen in London. No demo has been done due to the lack of hardware but explanations of how to use Bio-Pen were given via telephone and email communications.

(1) Bio-Pen purchase and assignment. One Bio-Pen needs to be purchased by a student during enrolment when the Bio-Pen signature of the student is taken and stored at the Bio-Pen server. The institution maintains the mapping between the Pen IDs and the student's registration number, passing only the Pen IDs and their associated signatures to the Bio-Pen server. The Bio-Pen server does not collect any personal information apart from the Pen ID.

(2) Verification. During the verification process, the real time signature will be compared with the stored one. Access is granted only when a match is found, otherwise access is denied. Bio-Pen authenticates the same student logged in to each session and test, and confirms the same student accessed all sessions and tests, and is the same student who signed and returned an assignment or test. Note the authentication is done at the login point only.

(3) Online Proctoring. Bio-Pen does not provide video proctoring. It may serve as a limited proctor if the school allows prompting students to verify their presence three times randomly during an fixed time e.g. two-hour test. With a Web-camera, the Bio-Pen can also take a picture of the user at the time of signing. But there is no continuous authentication.

Costs:

Quotations are given based on the quantities of Bio-Pen ordered by European representative Wayne Chodosh as follows.

Quantity	500	750	1000
Price	£133.67+VAT	£119.43+VAT	£109.77+VAT
Maintenance	£12 per annum	£12 per annum	£12 per annum

Each pen comes with 12 month warranty. Maintenance includes upgrades, help desk etc. University own server fee is available on application, UK server available is on request, and US server is available free of charge.

4.4 Kryterion Webassessor

Kryterion (Kryterion 2011) is a company based in Phoenix, Arizona. It seems to provide the most complete solution for online testing compared with other solutions. Face recognition and keystroke rhythms are used as multimode biometric authentication with a notable feature of continuous authentication provided by keystroke rhythms. Kryterion also provides human proctors invigilating online tests through live video monitoring by webcams. In addition, students' computers are "locked down" with security software, to prevent unauthorised windows from being opened.

Despite many attempts to contact with the company, the response is not very productive. No demo or quotation has been given, therefore the requirements on software and hardware, the ways of usages below are understood from the company's website only.

Software and Hardware

A piece of software needs to be installed on a student's machine which capture facial features, keystroke rhythms and locks-down the student' computer. Additionally, the software is claimed to be easily integrated with a variety of Course Management/Learning Management.

Hardware specification is not clearly identified on the web. But through the context it should include web cam, speaker and microphone with standard technical requirements.

Usage:

(1) Registration. During registration procedure digital photos of students are taken and stored in the student file. Keystroke features of the student should also be taken at the registration but this is clearly stated.

(2) Student authentication. This is done through multiple biometric authentications - face recognition software to match the face features of a student taking online test with the sample stored in the student file, and real time keystroke rhythms analysis to match the online inputs with the stored sample.

(3) Proctoring: Live video monitoring through webcam and screen locked down and human proctor at the test centre are combined together to invigilate the whole test duration. Additionally, the proctor helps the student to sort out issues regarding video, audio transmission etc.

(4) Session Reviews. Tutors or administrators are able to review the test session at any time post-test should they feel necessarily. Suspicious head movement are recorded and the software also reports if difficult questions are being answered suspiciously quickly, or if the answers of different students are too close.

Cost:

Pending

4.5 Cost Analysis

Commercial Solutions	**ProctorU**	**Secureexam**	**Bio-Pen**	**Kryterion Webassessor**
	Challenge questions, ID check by remote human proctor	Face recognition, and finger print recognition	Signature recognition	Face recognition, keystroke rhythms analysis
Hardware (one-off)	None. Standard webcam required.	360 degree webcam £100	Bio-Pen £109 to £133 plus VAT when order 1000 or 500 in a batch	None. Standard webcam required.
Software	Executable file no need for downloading	Secure browser Per annum £20	Included in the hardware package	Not mentioned
Technical support (24/7)	$25 per 2 hours(or less) exam	£10 (per annum)	£12 (per annum)	pending
Capture review service	None	5p per minute	Fees depending on where the server is held. University own server fee is available on application. UK server available is on request. US server is available free of charge.	pending
cost per student per year *	$25*3 = $75 = £46.78 (approximately)	£100+£20+£10+ £6*60*0.05 =£148	£109*1.2 + 12=£142.8 (min) £133*1.2 + 12=£171.6 (max)	Pending
Contacts	Rebecca Tweedy rtweedy@provtorU.com 1-205-870-8122 ext. 602	No contact made while writing this report	Wayne Chodosh wayne.chodosh@securesignaturesystems.com London office 02079350308(W) 07971881661(M)	John Dight jdight@kryteriononline.com (sales manager but no response)

Table 2. Cost comparison of four products

***(assuming 3 modules per year, 3 up to 2 hours exams per module)**

5. Discussions

Institutions in US have been taking actions in authenticating students in their distance learning programmes. This is mainly attributes to the fact that U.S. accreditors are now required to ensure that institutions with distance education programs to have policies to verify the identity of distance learning students. In the bill that renewed the Higher Education Act of 1965 (HEA) in 2008, it is stated that the Department of Education *"shall not require an accreditor to have separate standards, procedures or policies for evaluation of distance education. Accreditors must, however, require institutions that offer distance education to establish that a student registered for a distance education course is the same student who completes and receives credit for it." (*Jortberg 2009). Currently in UK education sector there is no such requirement yet but it may soon arrive.

The specific points for checking students' identity could be when the students registers in an online programme, participates various learning activities, complete academic work or receives academic credit.

- During registration, ID verification can be done by taking photos, signatures, and/or keystroke features depending on the technical approaches to be used in the following procedures.
- For participation, at the moment only signature-based solution authenticates when students log in to a study activity. But because the verification is only done at the logging point, it cannot stop other people from using the material after the right student signs.
- There are mainly two types of assessment in online programmes: online exams and coursework. The solutions in previous section all focus on the online proctoring throughout the whole exam period. No commercial product addresses authentication of students' coursework so as to make sure that the submitted work in indeed completed by the named student.
- The institutions normally send academic credit to a student by mailing to the home address or preferred address nominated by the student. No verification is done. The certificate could contain a photo of the student if necessary.

Although current solutions focus mainly on the point when students complete academic work, an all-in-one solution which systematically links all these specific points together may be more powerful in defeating cheating.

Secondly there is a lack of solutions for coursework authentication. When the companies were asked why they don't provide solutions for authenticating students' coursework, the answers were that they assumed that only a small percentage of assessment is set as coursework and the big portion would still be online exams. This assumption does not apply to the School of Computer Science though as we use coursework extensively. Plagiarism checking is to make sure the work is not copying somebody else's published work. It does not detect if somebody is hired to do this piece of coursework for the student.

Thirdly, because a coursework cannot be invigilated due to the longer time required completing it, the only way to authenticate the students' work is through academic judgement.

6. Recommendations

6.1 Online Test

We would recommend using ProctorU, the cheapest commercial solution. It is easy to use and works with any types of online test environment. For example students can take QuestionMark online test while invigilated by ProctorU certified proctors. ProctorU solution does satisfy the minimum requirement for ID checking and test invigilation. With human being the best hardware and software being used, no face recognition, signature recognition or keystroke rhythms analysis is involved therefore the cost is kept low. However, how much you trust the proctors is another issue.

Extra cost of using ProctorU includes obtaining a digital photo of a registered student during registration and kept the photo in the student file, setting up student file and account in the ProctorU server. We could ask students to pay for the online test at the rate of up to $25 per 2 hour test. This makes sense because students would pay for their referral tests.

This solution is not technically brilliant, but it is considerably cheaper than other solutions. Given the fact the UK government has not put any legal requirements on identifying online student, providing the cheapest solution is good enough from the practical point of view.

6.2 Large Piece of Coursework / Project Report

This is discussed in the "Part II. Authentication of Students and Students' Coursework in E-learning".

6.3 Media to Small Pieces of Coursework

This is discussed in the "Part III. Proposal for further research in authentication of students and students' coursework in E-Learning".

7. Summary

This report has looked the issue of authentication of students and students' work in e-learning, particularly in the setting of the School of Computer Science. The types of assessment used in online programmes are surveyed and staff's views on the authentication issue collected. Available approaches and commercial products are reviewed and compared. Cost analysis is done after contacting companies, seeing demos and obtaining quotations. Based on the technical and market surveys, recommendations and proposals are given in the report. We would like to carry out the work further if the School decides to continue supporting us.

Part II Authentication of Students and Students' Coursework in E-Learning

Wei Ji (w.1.ji@herts.ac.uk)

Hannan Xiao (h.xiao@herts.ac.uk)

Table of Content

1. Introduction

In part I of the report "Authentication of students and students' work in e-learning" , we have reviewed the authentication problem in e-learning and the current market solutions of authentication in online exams.

Four approaches have been discussed: proctored examination, user ID and password, biometric authentication, and challenge questions. Four associated commercial products have been looked at and compared: Proctor U, Secreexam Remote Proctor, Bio Pen, and Kryterion Webassessor. These solutions mainly focus on the online exams which are assessed in a short time period (2-3 hours) under close supervision or invigilation, and are completed online in real time.

Another format of assessment in e-learning is coursework, which is assessed in a relatively long period of time (2-4 weeks) and is completed offline without supervision or invigilation. Authentication of this type of assessment is rarely discussed in literature. This is mainly due to a) that it is viewed by some commercial developers that the percentage of coursework in a module assessment is small compared to exams (Part I of the report); and b) that the problems in coursework authentication in online environment and in on-campus environment are identical, in the way that the completion of a coursework can be done by a hired third party whilst the submission can be made by the legitimate person.

Contradicted to the view a), a survey carried out at the beginning of this project in the School of Computer Science shows (Part I of the report), that the majority of CS online modules (92%) uses individual coursework as main assessment method, and the majority of these individual coursework (84%) uses essay style or Q&A style. These results place the coursework authentication in a very crucial position for the School online programme.

The view point b) imposes a real concern in coursework authentication: do we really know how much a student learnt from a piece of coursework?

Despite of the information shortage in this area, a pilot study of coursework authentication is carried out, based on the many years' teaching experience in e-learning.

This short report is to present a pilot study in coursework authentication in an online module and to look at the possibility of applying the method to other similar situations.

2. Approaches

There is no straightforward solution for coursework authentication in e-learning. The approaches discussed here come from the ideas used in video conferencing and challenge questions.

2.1 Essential differences of exam authentication and coursework authentication

Coursework is a piece of work completed by student offline without supervision and invigilation. Because of this nature, coursework authentication involves not only the authentication of the submission procedure by a legitimate student but also the academic judgement of whether or not a student gains the knowledge claimed in the coursework.

Coursework authentication is different from exam authentication:

1) Exam authentication needs to verify a student at the point of him/her entering an exam and completing an exam. Coursework authentication needs to verify a student at the point of composing a coursework.

2) Exam authentication needs to verify a student at the same time as verifying the work the student carries out. Coursework authentication needs to verify that the student carries out the work him/herself before the point of submission so part of the issue becomes the academic judgement of student's knowledge.

From this point of view, exam authentication could be viewed as a one-stop shop: as long as a student is verified in a correct session, the submitted work is verified as legitimate. Coursework authentication is essentially a two step procedure: first is to verify that the person who submitted the coursework is the person who should be; second is to verify that the submitted work is indeed the student's own.

The majority of the approaches discussed in part I of the report are not suitable to coursework authentication here. One exception is the challenge question method which is to verify a student's work by asking questions of stored information. This method is discussed in section 6.3 of part I of the report.

2.2 Strategy of coursework authentication

The two-step coursework authentication requires a strategy of coursework design. Prevention approach and compliance approach are both taken into account to promote academic integrity (Epper, 2008) Prevention approach is to eliminate or reduce the opportunities to cheat and reduce the pressure to cheat. Compliance approach is to catch and punish those who cheat.

To prevent coursework cheating, the following points are used in coursework design:

- To establish student's identity from very beginning: when a student applies for the online course, his/her identity data (photo and signature) is stored in the student's profile electronically.
- To confirm student identity at the time when a student enrols on a module: to create a formative coursework to gather student's identity data, i.e., photo, signature, or a self-introduction video.

- To verify a student at the point of composing a coursework: to set up video coursework to have student report on their progressive achievement with their identity visible.
- To verify student's work for consistency: to set up coursework so that the written work and the work shown in the video are connected and have common factors, to allow cross-verification.
- To verify student's knowledge of their work: student should demonstrate their work with their identity visible, and should have interactive communication with assessors.

The compliance approach is reflected on the following points:

- To challenge student's knowledge about their submitted work: to set up live viva session online.
- To further verify student's knowledge of their submitted work: to set up oral session to access student's desktop for questioning.

3. Environment of the pilot study

The pilot study is carried out within the BSc online project module in semester A 2010-2011. BSc online project module (module code 6com1002, 6com1008, 6com1009, 6com1021) is a 100% coursework assessment module. The module is on offer twice a year to around 130 students of each group. Credit is awarded to student's work on both theoretical side and practical side.

Students who enrolled on the project module are widely located across the world with different levels of internet access capability, from dial up connection to broadband connection. When asked to set up web camera and headset for coursework purposes, none of the students raised any questions. Therefore, the setup is viewed as the standard configuration for an online study.

Since the module is delivered via Studynet, all coursework submission is supposed to go to the Assignments section. The pilot study requires video submission so the capacity of uploading size is crucial. With the old assignment system, there is a 16MB limitation a file could be uploaded at one submission. By consulting the LRC staff, the module was told that the limitation is upgraded to 100MB with the V3 new assignment system, but this cannot be set up by the time the module was on offer. So other channel of large size file transfer has to seek.

4. Pilot Study

The proposed coursework authentication is not working on one piece of coursework, but on the overall module assessment regime.

4.1 Software and hardware:

On student's side:

(1) A well working computer or laptop with Windows XP or above.
(2) A web cam with 640x480 video pixel resolution (web cams built into laptops are acceptable)
(3) A headset with speaker and microphone. Built in speakers and microphones are not recommended as they may affect the recording quality.
(4) A reliable internet connection. It is recommended that a high speed internet connection is used but this is not essential for the majority of students. Some students may be asked to attend online session which requires high speed internet access, but this can be arranged beforehand.
(5) Download Blueberry BB FlashBack Express from: http://www.bbsoftware.co.uk/bbflashback.aspx
(6) Register on Yousendit file transfer service: https://www.yousendit.com/.
(7) Skype account.
(8) Have access to Elluminate! Live session. This is only required for a small number of students who are called for project oral.

On assessor's side:

(1) A well working computer or laptop with Windows XP or above.
(2) A headset with microphone. Built in microphones are not recommended as they may affect the playing quality of a video.
(3) A reliable internet connection. It is recommended that a high speed internet connection is in place.
(4) Download flv player FLVplayer from http://www.applian.com/flvplayer/.
(5) Register on Yousendit file transfer service: https://www.yousendit.com/. This is not a must, but may be needed since some file transfer is protected by some students.
(6) Skype account.
(7) Have access to Elluminate! session when required.

4.2 Coursework organisation

The coursework organisation in the online project module is in line with the strategy of coursework authentication as well as the module learning outcomes specified in the module DMD.

(1) About You: Formative assessment. Students need to fill up a form which requires student's photo and signature. Studynet submission.
(2) DPP (Detailed Project Proposal): Summative assessment. 1%. Studynet submission.

(3) EA (Ethics Approval) Application: Summative assessment. 1%. Students need to work with their supervisor to complete the application. Signature is required on the form. Studynet submission and postal submission to the Faculty Ethics Committee.
(4) VPL01 (Visual Production Log 01): Summative assessment. 4%. Students need to record a video to report on their progressive achievement. Studynet submission and Yousendit service.
(5) IPR (Interim Progress Report): Summative assessment. 10%. Students need o submit a written report to report on their interim achievement. Studynet submission.
(6) VPL02: Summative assessment. 4%. The second video recording to report on student's progress. Studynet submission and Yousendit service.
(7) FPR (Final Project Report): Summative. 70%. Written report and evidence of practical work. Studynet submission.
(8) VPD (Visual Production Demonstration): Summative. 7%. Students need to record a video to demonstrate their software artefact developed for the project or to present their project work. There are detailed requirements of what are expected in this VPD. Yousendit service.
(9) Project Viva: Summative. 3%. Students are required to attend a live Q&A session via Skype. Students are questioned by assessors about anything involved in their project work, as seen in their FPR and VPD after the final submission.
(10) Project Oral: Formative. A small number of students is called for the project oral for verification purposes.

4.3. Coursework authentication

Elluminate live session used to be used in all students' project demonstration as a single gate of coursework authentication in the project module. The session allows assessors to access students' desktop and to provide communication channel for both parties. In the pilot study, this usage is reduced to minimum in that only a small number of students need to attend the session at the project oral stage. This is due to the excessive bandwidth requirement that makes the assessment very much resource demanding, e.g., longer session, reschedule, and poor screen and audio quality.

The current implementation of coursework authentication in the project module contains multiple steps:

(1) When students enrolled on the module, they are to submit the "About You" form containing their photo and signature. This can be compared to the data stored in student profile. The photo is a base for verification of other coursework submission which has the element of a student image identity.
(2) In VPL01, students need to record the screen activities of them presenting their project work. They also need to record the web camera image of themselves operating on the

log, as well as their speech explaining their work. Since this is locally recorded, there is no need for bandwidth or connection speed. The written work presented in VPL01 is to be submitted in the next assessment for verification.

(3) In IPR, the written documents produced in VPL01 are checked and further progress is reported.

(4) VPL02 continues the visual log presented by student. Again, progressive work is reported and student's knowledge of their work is recorded.

(5) All evidence shown in the VPLs are included in the FPR submission. The VPD provides further verification of students and students' practical work in a student-led project demonstration and presentation in a video.

(6) By the time of the final submission, we are able to establish a consistent picture of student's progressive work presented by him/herself. The next thing is to verify whether or not the student gains the knowledge claimed in his/her coursework submissions.

(7) The project viva is a live session between assessors and students using Skype. The "video call function" in Skype usually takes up great bandwidth so should be only used at the beginning of the viva session for those whose bandwidth is a concern. With a high speed broadband connection, video function should be always enabled. Questions from assessors can be raised from any work student submitted so that student's knowledge can be verified.

(8) If a project is in dispute, or no VPLs and VPD are submitted during the course of project development, a project oral is called. The oral is to use Elluminate! Live session to allow assessors to access student's desktop, including software artefact, as well as to allow Q&A. The Elluminate session is the last gate of coursework authentication.

4.4 Cost

Hardware: The standard configuration on student side is assumed to include PC/laptop, web camera, headset for online study. There is no extra hardware cost on assessor's side.

Software: Bluberry BB FlashBack Express – free

Yousendit file transfer service – at the time the pilot study was implemented, 100MB file transfer is free. It is now reduced to 50MB free uploading. There are other free file hosts, e.g., Mediafire, so no fees occur. Studynet is also available to allow up to 100MB submission in the future.

Flvplayer – free media player

The total cost is 0. However, downloading video file from Yousendit service is time consuming since the download window is 7 days. The resource demanding may be eased by using Studynet service once it is available in the future.

5. Discussion

Plagiarism and collusion detection is adopted by the module in conjunction with the coursework authentication described here. All students' reports are fed into Turnitin after the final submission but before the project viva. So any suspected cases can be checked in the project viva and a project oral is usually followed for these cases.

The observation of the pilot study is as follow:

(1) The coursework authentication relies on the coursework design and organisation. It is a systematic procedure to verify students and students' work.
(2) The authentication of students is based on the matching of stored data (photos) and the appearance of the student in several videos coursework.
(3) The authentication of students' work is based on two verifications: a) verification of the progressive work student presented; and b) challenge questions in live viva sessions.
(4) There is less bandwidth demanding at student's side compared to a live demonstration session, since all videos are recorded offline.
(5) The total cost is 0.

At the end of the pilot study, two students who didn't submit any video files are called for oral. One passed and one failed. Normal Turnitin detection found out 6 cases of plagiarism in final report writing.

There are feedbacks from supervisors orally to appreciate the overall coursework setup in the project module, especially the video coursework. Also in the feedbacks are the comment on the delayed file transfer and poor video quality by some submission. This will be improved by using Studynet service in the future.

6. Recommendation

The pilot study is the only implementation of a systematic coursework authentication within the project module. There is no comparative study carried out that can be discussed in this report.

We believe, though, some good practice can be recommended to other modules with the similar situation.

(1) Design of coursework structure is part of coursework authentication.
(2) Video coursework is a good way to know student and their work.
(3) Project viva and oral provide opportunities to verify student's knowledge of their submitted work.
(4) There is no extra hardware installation and no cost.

(5) The implementation of the coursework authentication in the project module is mostly fit with Studynet platform. If the uploading size is increased, it would be fully fit with Studynet platform.

Part III. Proposal for Further Research in Authentication of Students and Students' Coursework in E-Learning

Hannan Xiao (h.xiao@herts.ac.uk)

Wei Ji (w.1.ji@herts.ac.uk)

Table of Content

1. Introduction

The majority of our online modules are using media to small pieces of coursework as main assessment methods which may include programming codes, short report, question and answers, designs and experiments, etc. To address the issue of authenticating coursework, a project bid for the UH Charitable Trust Grant has been submitted in June 2011 as an outcome from this teaching development project (Xiao, 2011). StudyNet development team has been consulted before submitting the bid. For details of the application please see Appendix 2.

2. Summary

This project will design, implement and test an application that helps academics to authenticate whether a coursework submitted by a named distance learning student is indeed completed by the student. The application will ask the student few randomly chosen questions during submission procedure, and then capture a short video of few minutes of the student answering the questions. The questions can be general in order to save staff time, but answers must be specific regarding the contents of the submitted coursework. The application will be independent firstly and later integrated into Moodle, an open source Learning Management System.

3. Aims and objectives

Coursework is one of the major types of assessments of most distance learning programmes. However, limited work has been done to authenticate that an online submission of a piece of coursework is indeed completed by a registered distance learning student. Commercial products currently focus on authenticating and proctoring students in online exams only. The common practise for institutions is to require a viva or demonstration for a big piece of coursework like a project report, but not for other smaller pieces of coursework due to the demand on staff time.

To detect and prevent student cheatings in online coursework, this project is aimed to design, implement, and test an application that helps academics to authenticate a coursework submitted by a named distance learning student. The idea is to ask students few automatically generated questions which can be very general in order to save staff time, and through the answers that should be specific to the contents of the submitted coursework, a tutor is able to authenticate by academic judgement whether the work is done by the student later on if suspicion arises. The project is also aimed to integrate the application into Moodle.

4. Who will benefit from the project?

The member of staff on the University distance learning programme would be the first group of people benefiting from the project. Within the School of Computer Science, over the years the external examiner has expressed increasing concerns on the authentication issues in the online programmes. Once the application is in use after sufficient testing and further integration into StudyNet, it will help tutors to have a means to check whether a student has done a coursework himself without too much extra staff time.

The students on the distance learning project would benefit from the project because they would learn something by having to do the coursework themselves rather than hiring someone to do the coursework for them.

The University's distance learning programme would benefit from the project which makes the programme more secure by authenticating students and their coursework. This feature would make our online programme in the leading position in this area. In the long run, the application could be adopted for on-campus modules that use online submissions for coursework, such as short reports.

Integrating the application into Moodle would make distance learning programmes at other institutions benefit from it thanks to the open source of Moodle.

5. Evaluation

The project will be evaluated by the successful delivery of the application within the planned time period and the results from pilot study with an online module. The application will be evaluated against following criteria.

(1) Scalability. Scalability of the application is a key issue due to the storage requirements on video files. We will look at the available CODECs in the development in order to reduce the size of video files.

(2) Accuracy. The application does not provide face recognition at the moment. The captured video image will be compared to the students' photo required during registration by the tutor if cheating is suspected. This might lead to inaccuracy in authenticating the student. We will test this as well.

(3) Usability. The application should be easy to use. Student feedbacks will be gathered after the pilot tests.

6. Sustainability

If the project is granted and the application developed and tested, the application could be further improved based on the results from pilot study and student feedbacks. Being integrated with Moodle would make the application usable to other institutions running distance learning programmes too. If the application is integrated with StudyNet then UH on-campus programmes may also benefit from it.

Unfortunately the application to the UH Charitable Trust Grant is unsuccessful. We believe it is a good idea and would like School to fund it is possible. Details of the application please see appendix 2.

References

Adamski, M. and K. Saeed (2008). "Online Signature Classification and its Verification System." 7th Computer Information Systems and Industrial Management Applications: 189-194.

Afsar, F., M. Arif, et al. (2005). Wavelet Transform Based Global Features for Online Signature Recognition. 9th International Multitopic Conference, IEEE.

Aggarwal, G., N. Ratha, et al. (2008). Gradient based Textural Characterization of Fingerprints. Biometrics: Theory, Applications and Systems, IEEE.

Agulla, E. G., L. A. Rifón, et al. (2008). Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments. Eighth IEEE International Conference on Advanced Learning Technologies, IEEE.

Ali, I., U. Ali, et al. (2006). Face and fingerprint biometrics integration model for person identification using Gabor filter. Computer Systems and Applications, 2006, IEEE.

Alwi, N. H. M. and I. S. Fan (2010). "Threats analysis for e-learning." International Journal of Technology Enhanced Learning **2**(4): 358-371.

Analyst, G. I. (2010). eLearning – A Global Strategic Business Report. [1] Global Industry Analyst.

Asha, S. and C. Chellappan (2008). Authentication of e-learners using multimodal biometric technology. International Symposium on Biometrics and Security Technologies IEEE.

Auernheimer, B. and M. J. Tsai (2005). Biometric Authentication for Web-Based Couse Examinations. Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS '05), IEEE.

Bajaj, R. and S. Chaudhury (1997). "Signature verification using multiple neural classifiers." Pattern Recognition **30**(1): 1-7.

Bari, J., R. Sullivan, et al. (2004). Security method in distance-learning. 34th Annual Frontiers in Education IEEE.

Bellovin, S. M. and M. Merritt (1993). Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise. Proceedings of the 1st ACM conference on Computer and communications security CCS '93, ACM.

Bio-Pen Website. (2011) http://www.securesignaturesystems.com/products.html

Chan, Y. Y., C. H. Leung, et al. (2003). Evaluation on Security and Privacy of Web-Based Learning Systems. The 3rd IEEE International Conference on Advanced Learning Technologies.

Chandra, E. and C. Sunitha (2009). A review on Speech and Speaker Authentication System using Voice Signal feature selection and extraction. IEEE International Advance Computing Conference, IEEE.

Coetzer, J., B. Herbst, et al. (2004). "Offline signature verification using the discrete radon transform and a hidden Markov model." EURASIP Journal on Applied Signal Processing **2004**: 559-571.

Colwell, J. L. and C. F. Jenks (2005). Student Ethics in Online Courses. 35th Annual Conference Frontiers in Education (FIE '05) IEEE.

Das, M. L., A. Saxena, et al. (2004). "A dynamic ID-based remote user authentication scheme." Consumer Electronics, IEEE Transactions on **50**(2): 629-631.

Dentistry, B. a. T. L. S. o. M. a. (2011). "Postgraduate Diploma in Clinical Dermatology." Retrieved 13/07/2011, 2011, from http://www.londondermatology.org/courseint/index.html.

Derakhshani, R., S. A. C. Schuckers, et al. (2003). "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners." Pattern Recognition **36**(2): 383-396.

Dick, M., J. Sheard, et al. (2002). Addressing student cheating: definitions and solutions. ITiCSE-WGR '02 Working group reports from ITiCSE on Innovation and technology in computer science education, ACM.

Epper, R., Anderson, M., etc (2008) “Are Your Online Students Really the Ones Registered for the Course? “, A WCET Briefing Paper, February 2008.

Eveno, N. and L. Besacier (2005). Co-inertia analysis for liveness test in audio-visual biometrics. Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, IEEE.

Fang, B., C. Leung, et al. (2003). "Off-line signature verification by the tracking of feature and stroke positions." Pattern Recognition **36**(1): 91-101.

Fang, P., Z. C. Wu, et al. (2005). "Improved DTW algorithm for online signature verification based on writing forces." Advances in Intelligent Computing: 631-640.

Gil, C., M. Castro, et al. (2010). Identification in web evaluation in learning management system by fingerprint identification system. Frontiers in Education Conference (FIE), IEEE.

Griffith, V. and M. Jakobsson (2005). Messin’with Texas Deriving Mother’s Maiden Names Using Public Records. Third International Conference, ACNS, Springer.

Gruber, C., C. Hook, et al. (2006). A flexible architecture for online signature verification based on a novel biometric pen. Mountain Workshop on Adaptive and Learning Systems IEEE.

Harmon, O. R., J. Lambrinos, et al. (2010). "Assessment design and cheating risk in online instruction." Online Journal of Distance Learning Administration **13**(3).

Hayes, B. and J. Ringwood (2009). Authenticating student work in an e-learning programme via speaker recognition. 3rd International Conference on Signals, Circuits and Systems (SCS) IEEE.

Huiping, J. (2010). Strong password authentication protocols. 4th International Conference on Distance Learning and Education (ICDLE), IEEE.

Ives, B., K. R. Walsh, et al. (2004). "The domino effect of password reuse." Communications of the ACM **47**(4): 75-78.

Jain, A. K., A. Ross, et al. (2006). "Biometrics: a tool for information security." Information Forensics and Security, IEEE Transactions on **1**(2): 125-143.

Jayamaha, R., M. Senadheera, et al. (2008). VoizLock-Human Voice Authentication System using Hidden Markov Model. 4th International Conference on Information and Automation for Sustainability IEEE.

Jazahanim, K. S., Z. Ibrahim, et al. Online zones' identification using signature baseline. Second International Conference on the Applications of Digital Information and Web Technologies, IEEE.

Jortberg, M. A. (2009). "Methods to verify the identity of distance learning students." Retrieved 01/04/2011, 2011, from www.acxiom.com/education.

Jung, I. Y. and H. Y. Yeom (2009). "Enhanced security for online exams using group cryptography." IEEE Transactions on Education **52**(3): 340-349.

Just, M. and D. Aspinall (2009). Challenging challenge questions. Socio-Economic Strand, Oxford University UK.

Justino, E. J. R., F. Bortolozzi, et al. (2005). "A comparison of SVM and HMM classifiers in the off-line signature verification." Pattern Recognition Letters **26**(9): 1377-1385.

Karvonen, K. (1999). Creating trust. In Proceedings of the Fourth Nordic Workshop on Secure IT Systems, Citeseer.

Kashi, R., J. Hu, et al. (1998). "A Hidden Markov Model approach to online handwritten signature verification." International Journal on Document Analysis and Recognition **1**(2): 102-109.

Kryterion website. (2011) http://www.kryteriononline.com/

Levy, Y. and M. M. Ramim (2007). A Theoretical Approach For Biometrics Authentication of E-Exams. International Journal of Digital Society (IJDS).

Mahmood, N. (2010). "Remote Proctoring Software Means Students Can Now Take Exams From Home." Retrieved 13/07/2011, 2011, from http://thetechjournal.com/science/remote-proctoring-software-means-students-can-now-take-exams-from-home.xhtml.

Maiorana, E., P. Campisi, et al. (2010). "Cancelable templates for sequence-based biometrics with application to on-line signature recognition." IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans **40**(3): 525-538.

Marais, E., D. Argles, et al. (2006). "Security issues specific to e-assessments." The International Journal for Infonomics.

McCabe, D. L., L. K. Treviño, et al. (2001). "Cheating in academic institutions: A decade of research." Ethics & Behavior **11**(3): 219-232.

Meshoul, S. and M. Batouche (2010). Combining Fisher Discriminant Analysis and probabilistic neural network for effective on-line signature recognition. 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA), IEEE.

Micheal G. Moore, G. K. (2005). A System View. Belmount, CA.

Moini, A. and A. M. Madni (2009). "Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective." IEEE Systems Journal **3**(4): 469-476.

Muramatsu, D. and T. Matsumoto (2003). An HMM online signature verifier incorporating signature trajectories. Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), IEEE.

Mwakalinga, J., S. Kowalski, et al. (2009). Secure e-learning using a holistic and immune security framework. International Conference for Internet Technology and Secured Transactions (ICITST), IEEE.

Olt, M. R. (2002). "Ethics and distance education: Strategies for minimizing academic dishonesty in online assessment." Online Journal of Distance Learning Administration **5**(3).

Parizeau, M. and R. Plamondon (1990). "A comparative analysis of regional correlation, dynamic time warping, and skeletal tree matching for signature verification." IEEE Transactions on Pattern Analysis and Machine Intelligence **12**(7): 710-717.

Pillsbury, C. (2004). "Reflections of academic misconduct: An investigating officer's experiences and ethics supplements." Journal of American Academy of Business **5**(1/2): 446-454.

ProctorU website. (2011) http://www.proctoru.com/

Pyper, A. Meere, J , Lilley, M. (2010) Secureexam Remote Proctor Report, August 2010

Ruiz, J. G., M. J. Mintzer, et al. (2006). "The impact of e-learning in medical education." Academic medicine **81**(3): 207.

Schechter, S., A. J. B. Brush, et al. (2009). It's No Secret. Measuring the Security and Reliability of Authentication via. 30th IEEE Symposium on Security and Privacy, IEEE.

Secureexam Website. (2011). http://www.softwaresecure.com/US/solution/securexam-remote-proctor.aspx

Shashua, A. (1997). "On photometric issues in 3D visual recognition from a single 2D image." International Journal of Computer Vision **21**(1): 99-122.

Shaver, C. D. and J. Acken (2009). Effects of equipment variation on speaker recognition error rates. International Conference on Acoustics Speech and Signal Processing (ICASSP), IEEE.

Shepherd, J. (2008). History essay in the making. The Guardian, Guardian News and Media Limited.

Srisuk, S., M. Petrou, et al. (2003). Face authentication using the trace transform. IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '03).

Strobl, S. (2010, 29/11/2010). "Student identification verification." Retrieved 21/06/2011, 2011, from http://jjay.cuny.edu/academicaffairs/OLTF_Appendix_5B.pdf.

Strother, J. B. (2002). "An assessment of the effectiveness of e-learning in corporate training programs." The International Review of Research in Open and Distance Learning **3**(1): Article 3.1. 2.

University, C. (2007). "Diploma in Practical Dermatology Examination." Retrieved 03/07/2011, 2011, from http://www.dermatology.org.uk/courses/dpd/dpd-overview.html.

Vician, C., D. D. Charlesworth, et al. (2006). "Students' Perspectives of the Influence of Web-Enhanced Coursework on Incidences of Cheating." Journal of Chemical Education **83**(9): 1368.

Wielicki, T. (2006). Integrity of online testing in e-learning: Empirical study. Fourth IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), IEEE.

Wirtz, B. (1995). Stroke-based time warping for signature verification. Proceedings of the Third International Conference on Document Analysis and Recognition, IEEE.

World, D. I. (2004). "Digital ID." 2011, from www.digitalidworld.com.

Xiao, H (2011) Authentication of Students' Coursework in Distance Learning, July 2011, Application for University of Hertf ordshire Charitable Trust.

Zhao, Q. and M. Ye (2010). The application and implementation of face recognition in authentication system for distance education. 2nd International Conference on Networking and Digital Society (ICNDS), IEEE.

Appendix 1. Online Assessment Authentication Questionnaire

Dear Colleagues,

This questionnaire is used for the teaching development project in online programme. We would very much appreciate if you could spend around 5 minutes to complete this. Thank you for your time.

Hannan and Wei

**********Please circle one or more options.**********

1. How many online modules do you teach?

a) 0

b) 1

c) 2

d) 3

e) More than 3, please specify _____

2. Which level(s) of online modules do you teach?

a) BSc final year

b) MSc

c) PhD

d) None

e) Other level, please specify: _____

3. What assessment method(s) do you use in your teaching?

a) Individual coursework

b) Group coursework

c) In-class test

d) Examination

e) Others, please specify: _____

4. Which format(s) do you use in *individual coursework* assessment?

a) Essay style coursework (including report style coursework)

b) Video style coursework

c) Question-and-answer style coursework

d) Programming code style coursework (including practical work coursework)

e) Other style, please specify: _____

5. Which format(s) do you use in *group coursework* assessment?

a) Essay style coursework (including report style coursework)

b) Video style coursework

c) Question-and-answer style coursework

d) Programming code style coursework (including practical work coursework)

e) Other style, please specify: _____

6. Which format(s) do you use in *in-class test* assessment?

a) Multiple choice questions

b) Question-and-answer

c) Generating programming code

d) Producing practical work

e) Other style, please specify: _____

7. Which format(s) do you use in *examination* assessment?

a) Multiple choice questions

b) Question-and-answer

c) Generating programming code

d) Producing practical work

e) Other style, please specify: _____

8. Which one of the following cheatings concerns you most when assessing an online student's work?

a) Plagiarism

b) Find someone to sit in an online exam for them

c) Find someone to write a report for them

d) Find someone to do the whole project for them

e) Others, please specify: _____

9. Which one of the following best describes the situation you use Turnitin for detecting paganism in students' work?

a) I use Turnitin in all or most of student's work submissions.

b) I use Turnitin in one or two submissions, e.g., report, essay.

c) I use Turnitin in programming code submission.

d) I am interested in using Turnitin.

e) I do not use Turnit in at all.

10. What measurement(s) do you use to authenticate students' work?

a) None or minimum (e.g., signed assignment briefing)

b) Elluminate live session

c) Skype video conference or similar

d) Securexam remote proctor

e) Others, please specify: _____

11. Which one of the following best describes your attitude if the School is going to enforce some form of authenticating online students in assessment?

a) Welcome & supportive

b) It is not a big issue, but I am happy to try it on my module

c) It is not cost-effective

d) Against it

e) Others, please specify: _____

Appendix 2. Application for University of Hertfordshire Charitable Trust