J Sci.Univ.Kelaniya **4** (2008): 95-104

DETECTING AND PREVENTING PLAGIARISM IN ONLINE ASSESSMENT

C.T. WANNIGE[1], D.U.J. SONNADARA[1], H.A. USOOF[2] AND K.P. HEWAGAMAGE[2]

[1]Department of Physics, University of Colombo, Sri Lanka
[2]University of Colombo, School of Computing, Sri Lanka

ABSTRACT

Assessment is an important area in both teaching and learning. E-assessment is the foremost methodology for assessment in distance learning. This paper presents a method based on client-server architecture that can be used in capturing/preventing plagiarism in online assessments for distance learning centres. Among many possible scenarios of plagiarism, developed system focused on preventing or capturing unauthorised help obtained from online chat forms, websites or other types of communication mediums as well as use of stored text/restricted software. Bench tests show high degree of accuracy in capturing plagiarism scenarios by monitoring the change of grey values observed in edge detected screen shots. During pilot tests, participants attempted activities of plagiarism although the software was designed to prevent the act of plagiarism. The results show 97% accuracy in capturing plagiarism scenarios by the developed software in a restricted Ubuntu Linux environment.

Key words: e-assessment, plagiarism, distance learning

INTRODUCTION

Among the vast advantages offered with the emerging of internet in the last decade, distance learning or e-learning plays a major share in training and education. Many institutions offer varying degree of online courses for large number of disciplines that is tailor made to meet the demands of regional as well as global labour markets. However, technologies for robust e-assessment which is also an important area in both teaching and learning is still at its infancy.

Most of the assessment systems that are widely used today are traditional manual systems which require heavy involvement of human resources. When candidates are

facing an assessment, invigilators and supervisors are required to look after the plagiarism issues and to subjugate them. The traditional testing techniques based on papers and pencils have become a time consuming and wastage of resources. Thus, the traditional assessment systems are slowly moving towards assessment systems based on internet technologies. When distance learning is considered, e-assessments offer many benefits and often offer no other alternative due to candidates being located in various regions of the world. However, when a student scores well in an online assessment, it may not be because he or she knows the material (Ford, 1996). Plagiarism is the major issue in an e-assessment as internet tend to offer vast information which can be frequently misused with the availability of today's latest technologies. Humans tend to cheat at one time or another (Ford, 1996) and cheating is common in education (Cizek, 1999; Lathrop, 2000; Dick, 2003; Rowe, 2004). A study carried out in United States (Bushweller, 1999) indicates that 70% of American high school seniors admit to cheating on at least one test and 95% of the students claim that they have never being caught. A report that discusses 12 studies of cheating with college students (Dick, 2003) indicates that 75% students cheat sometime during their college career. Thus, candidates facing assessments at their own desirable locations and time of convenience is restricted, as the monitoring the environment and usage of resources are quite difficult.

Since e-assessment is relatively new, although it is essential, not much research has been done in preventing and detecting plagiarism. Most of the systems created are to detect plagiarism using the submitted materials (http://www.plagiarism.com/index.htm). In most of foreign universities, submitted materials are checked to detect plagiarism using techniques such as visual cues or content cues of the material and tracking down originals with search engines. For visual cues, unusual formatting, mixed citation styles, strange or poor layout, jargon or advanced vocabulary and strange grammar or syntax are often used. For content cues, techniques such as finding similar chunks in the submitted paper with internet using search engines and differences in the writing style are used.

There are also user logger systems constructed to store information about who used the computer, when they used it and what they did (http://chemware.co.nz/usrlog.htm). This is a good monitoring mechanism. Nevertheless, these systems can be easily hacked as they store captured data in a folder in the system itself. There are also key loggers which can be connected to the keyboard port. These loggers store all typed words in it. However, these types of

solutions fail to provide sufficient evidence in the case of an e-plagiarism. Hardware based solutions to provide evident information in e-plagiarism is yet to be developed.

Four major possible scenarios of plagiarism can be identified in an unsupervised e-assessment. In the first scenario candidate can get online help from chat forums, websites or other type of electronic communication methods. In the second scenario candidate can access restricted software or stored text. In the third scenario candidate could be impersonated by another person to answer the assessment. In the fourth and final scenario candidate could get assistance from an external source. The scope of this pilot project was to develop software solution to prevent first two scenarios of plagiarism in a distance e-assessment environment. It is assumed that there is a supervisor at the remote centre who will be in charge of the external issues of plagiarism of the students such as the third and fourth scenarios.

IMPLEMENTATION

Overview

The software solution presented in this work, a restricted Linux operating system and the client software to be used is provided to the remote centre, so that each candidate could access the examination paper from a central server.

The restricted Linux system provides the front-end software to be used during the assessment in a restricted environment. The software allows examination questions to be downloaded from a remote server and candidate's answers to be sent back to the central server. Linux system provides a restricted environment for the computers used by the candidates where internet access is restricted via a firewall and restricted assess is provided to the local hard disk. In order to monitor the candidates accessing any unauthorized material from external sources using new technologies such as Bluetooth, screen activities are frequently monitored. Screenshots are captured frequently by the software without candidate's knowledge and selected screenshots and the essential data of candidates are saved in a restricted folder. The suspicious screenshots are automatically processed by image processing techniques and these data are sent to the assessment centre to be used in the final evaluation.

Development of the software

The software modules were developed based on the client-server architecture for the candidate to download questions from a remote location and submit answers to the central server. Since bandwidth could be an issue, the exchange of information should

be limited as much as possible. The client software can be provided in a bootable Linux live compact disk so that it can be used in any machine with reasonable RAM. Java (Horton, 2000) was used as the programming language and the remote server was a SQL server 2005.

At the client end, the first screen interface is a welcome screen which provides instruction for the candidate on the selected examination as well as rules and regulations. The second screen gathers initial information such as candidate's index number, date and time of the examination and the designated server URL. In principle, multiple servers could be accessed by the remote centres depending on services provided by them. Server allows randomly selected questions to be downloaded from the remote database specific to the examination. Answers are automatically submitted to the server by the clients. In addition, screen activities are monitored randomly by hidden processes.

In order to capture the liable screen shots among other normal screen shots, image processing techniques were adopted. Convolution filtering was used as the main technique in image processing due to the high computation speed (Brown, 2002).

Initially, the captured screen shots were processed using a high pass filter kernel. In high pass filtering, high-frequency components are accentuated and a little effect is offered on low frequency components. Thus, the image passed through a high-pass filter becomes a sharper image with increased detail in the areas of brightness transition such as edges.

In order to detect the edges, Laplacian operator was used as it has a better speed in computation (Brown, 2002). The Laplacian $G(x, y)$ of an image with pixel intensity values $f(x, y)$ is given by:

$$G(x,y) = \frac{d^2 f(x,y)}{dx^2} + \frac{d^2 f(x,y)}{dy^2}$$

Since the input image is represented as a set of discrete pixels, a discrete convolution filter was used (Sun Microsystems, 1999).

In order to classify suspicious screen shots from normal screen shots, the sum of grey values of edge detected images was used. The limiting grey level was calculated by analyzing five separate scenarios. Once a suspicious screen shot was detected, it was saved in a restricted folder. At the end of the examination, the percentage of screenshots that was different to typical screen shots were calculated by the software and sent to the remote server together with the suspicious screen shots.

The Server

The SQL server 2005 was used as the main database of the server which contained the question table with multiple choice questions. For each candidate, questions were randomly selected. In addition, for each candidate, the server maintained candidate information as well as the answers and percentage of screenshots that were suspicious.

To identify the average grey value expected for each screen, facilities were provided at the server end to calculate the limiting grey level for each and every screen. When new questions or examinations are loaded to the server, it is expected to repeat this process so that optimum values are always known before the comparison.

The Client

The Linux system [Ubuntu 7.04] where the client software is installed can also be provided in a live compact disk. In the re-mastering process, all the unwanted software components such as web browsers, document viewing software etc. was removed. The commercial JDBC - ODBC driver “Easy Soft JDBC - ODBC Bridge” (EasySoft, 2007) was used to access data objects in different platforms.

Hard disk, CD Rom, Floppy drive, and the USB port access were restricted by constructing a special user account with minimum access privileges for each of the candidates. The internet access was restricted via a firewall [Fire Starter] with only allowing the candidate to retrieve and send data packets to the server URL.

BENCH TESTS

In order to detect the plagiarism during an online assessment, possible scenarios were divided into five categories, namely, (1) use of stored text, (2) use of restricted software, (3) web browsing, (4) chat or communication and (5) use of online web forums. To study each of the above scenarios, bench tests were carried out with 100 random samples of edge detected screen shots captured by the monitoring software.

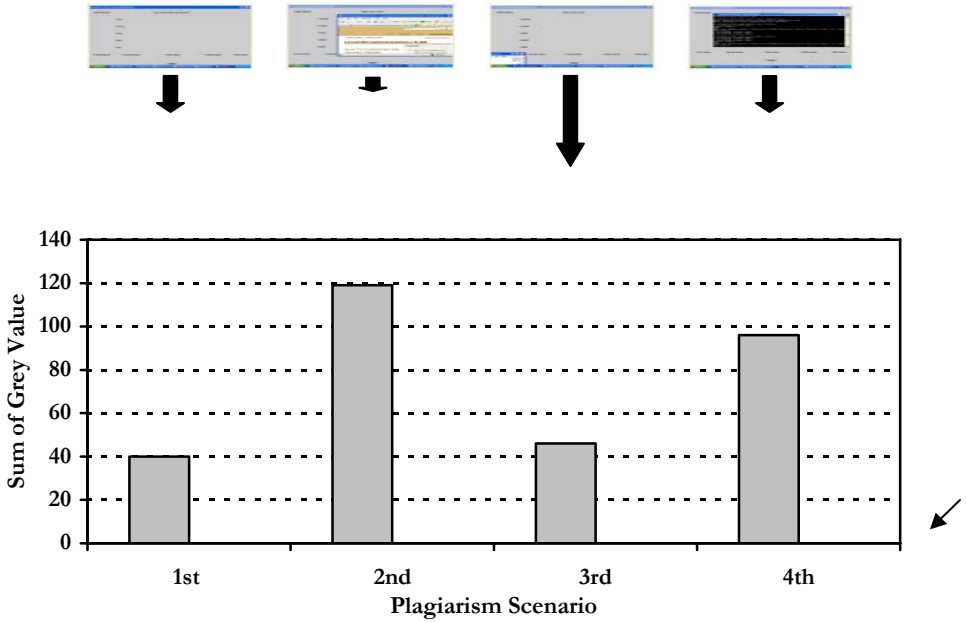

Figure 1: Typical and non-typical screen shots. 1st screen shot shows the typical examination screen and other three screen shots show possible plagiarism scenarios.

The sum of grey values detected for several typical and non-typical screenshots are shown in Figure 1. It was seen that the sum of grey values can be used effectively to distinguish between typical edge detected screens with examination questions and non-typical edge detected screens with other windows overlaid on top of the examination screens. However, as expected if the overlaid screen is covering only a small portion of the examination screen (see 3rd screen shot), a sum of grey value close to the limiting grey value was observed. This scenario is a case where the developed software may run into difficulties of distinguishing between the typical and non-typical screen shots.

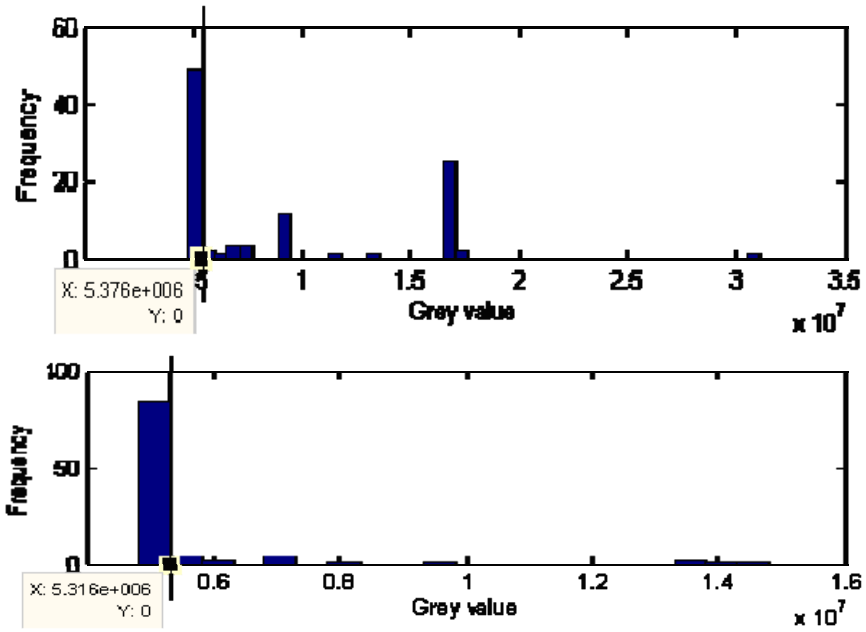

Figure 2: Grey values observed for the use of stored text [top] and use of restricted software [bottom]

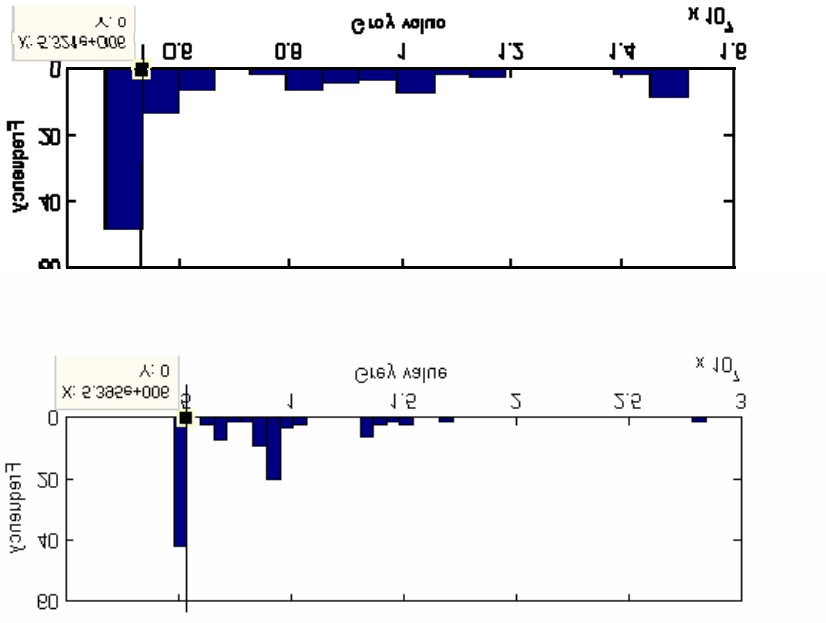

Figure 3: Grey values for web browsing [top] and chat/messaging [bottom].

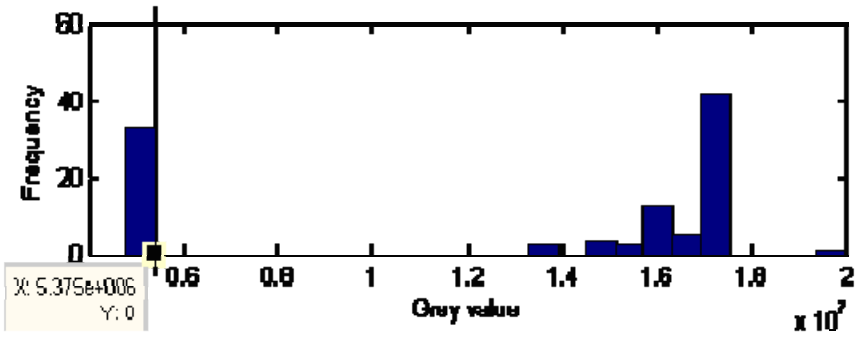

Figure 4: Grey values for use of online Web forums

In Figures 2-4, histograms for sum of grey values observed for the random sample of edge detected screen shots taken under various plagiarism cases are shown. In all three graphs, a higher grey value corresponds to cases with non-typical screen shots. In most of these cases, several minutes can be elapsed before the restricted software is ready to be used. So, the screen shots captured in the meantime have lower grey values corresponding to typical screen shots.

The limiting grey value can be identified by analyzing the graphs. For the pilot test discussed in the next section of this work, the limiting grey value used is indicated by a vertical line in the graphs. However, the limiting grey value depends on the resolution of the screen image. The Linux systems is giving the user two choices of screen resolutions and for those two screen resolutions limiting grey values were calculated and the software was programmed accordingly.

RESULTS

The final system for pilot tests was constructed with one client machine and the server. The client machine works under Ubuntu Linux [Version 7.04] operating system. It contains the java software to be executed during an assessment. The candidate can access the system only via a special user account with limited privileges. The internet access is also restricted via a firewall.

The pilot tests were carried out with the involvement of randomly selected individuals. Some of them were aware of Linux operating system and some were not. They were allowed to answer the assessment questions using the software installed in the special user account. They were asked to attempt plagiarism while answering the

examination. The information related to the plagiarism activity and the interpretations of the results of the tests are presented in Table 1. From the results given in the table, it can be concluded that most of the plagiarism attempts have been detected or prevented by the developed software.

Table 1: Plagiarism activities and the interpretations of results

Plagiarism scenario	Plagiarism activity	Successfulness of the activity	Reason for the successfulness or unsuccessfulness	Detection Accuracy
Use of stored text	1. Trying to access internal data (folders)	1.Uncsuccessful	1. Access restrictions imposed by the administrator allowing only limited privileges for the user.	96.6%
	2. Trying to use calculator	2. Successful	2. Ubuntu provides calculator for all user accounts by default.	
	3. Try to use the pen driver	3. Unsuccessful	3. Special user account doesn't allow accessing the pen driver.	
	4. Trying to use the floppy driver.	4. Unsuccessful	4. Special user account doesn't allow accessing the floppy driver.	
Use of restricted software	5. Internal software accessing (Open Office Databases)	5. Successful	5. Special user account allows access to software, but do not allow access to the hard disk.	98%
Web Browsing	6. Trying to access Internet using UDP, Telnet, http, ftp	6. Unsuccessful	6. The firewall restricts accessing the Internet.	96%
Chat or communication	7. Trying to access Internet using UDP, Telnet, http and chat	7.Unsuccessful	7. The firewall restricts accessing internet.	98%
	8. Trying to access the mail client.	8. Unsuccessful	8. The firewall restricts the access and user has no privileges to install s/w.	
Use of online web forums	9. Trying to access internet using UDP, Telnet, http	9. Unsuccessful	9. The firewall restricts accessing Internet	96%

CONCLUSIONS

The developed system provided a restricted environment suitable for conducting examinations at remote centres since it is capable of detecting unauthorized activities. Using the method presented in this paper, e-assessments for distance learning centres can be carried out with much less supervision. Bench tests show high degree of accuracy of capturing plagiarism scenarios by the software. During pilot tests, plagiarism were not allowed, but the participants attempted activities of plagiarism under five identified categories. Tests show 97% accuracy in capturing plagiarism scenarios by the developed software in the restricted Ubuntu Linux environment.

The constructed system can be presented to the candidate in a re-mastered Linux live compact disk. The constructed system can be used for assessments such as International Computer Driving Licence [ICDL] or Bachelor of Information Technology examinations [BIT] where the assessments could be taken at any location in the country.

REFERENCES

Brown, E.D. 2002. Optical Characterization of Domain Growth in Polymer Systems, MSc Thesis, Department of Computer Science, University of Sheffield, U.K. pp 17-20.

Bushweller, K. 1999. Generation of cheaters. The American School Board Journal 186(4) : 24-32.

Cizek, G.J. 1999. Cheating on tests: How to do it, detect it, and prevent it. Lawrence Erlbaum Associates. ISBN: 0805831452.

Dick, M., J. Sheard, C. Bareiss, J. Carter, D. Joyce, T. Harding & C. Laxer. 2003. Addressing student cheating: definitions and solutions. ACM SIGCSE Bulletin 35(2) : 172-184.

EasySoft Limited. 2008. Easysoft data access user's guide, 1993-2007, pp 18-86.

Ford, C.V. 1999. Lies! Lies!! Lies!!! The psychology of deceit. The American Psychiatric Publishing Inc. ISBN: 0880489979.

Horton, I. 2000. Mastering Java 2, V5, Oxford University Press, pp 794-797.

Lathrop, A. & K. Foss. 2000. Student cheating and plagiarism in the Internet era: a wake-up call. Libraries Unlimited. ISBN: 156308841X.

Rowe, N.C. 2004. Cheating in Online Student Assessment: Beyond Plagiarism, Online Journal of Distance Learning Administration, 7(2).

Sun Microsystems. 1999. Programming in Java Advanced Imaging. Sun Microsystems Inc.