Enhancing Computer-based Assessment Security using Biometric Facial Data

Moshood Alabi Alarape
Department of Computer Science
Federal Polytechnic, Bida, Nigeria

Mudasiri Saheed
Department of Computer Science
Federal Polytechnic, Bida, Nigeria

ABSTRACT
The advancement in Information and Communication Technology has brought about a great revolution in the way most of our activities are being done in this era. Standard examinations and tests are now being conducted globally using the information technology tools. These examinations/tests are being referred to by several names, some of which are the Computer Based Tests (CBT), Computer Based Assessment (CBA), e-examinations, e-assessment and so on. The assessments carried out with these technologies have had its own several challenges in form of examination malpractices most especially impersonation. This paper presents a Computer Based Assessment system which uses biometric facial data capturing of students/candidates for assessment as a measure of preventing impersonation. The system was implemented on Visual Basic.Net platform, tested with a set of students in HND II Computer Science department of the Federal Polytechnic, Bida and the system was able to record zero percent impersonation among the selected students.

Keywords
Computer Based Assessment, Biometric, Facial data, Impersonation

1. INTRODUCTION
Formal examination can rightly be defined as the assessment of a person’s performance, when confronted with a series of questions, problems, or tasks set him, in order to ascertain the amount of knowledge that he has acquired, the extent to which he is able to utilize it, or the quality and effectiveness of the skills he has developed [1]. The formal method of assessment requires the examiners to submit a copy of their test/examination questions to their departments’ examination officer. This is where the questions are printed and given to the invigilators on the examination day to administer on students in the examination hall. Answers booklets may also be distributed to students on the examination day as the case may apply. Each student on conclusion of a test session is supposed to submit their answer booklets to the invigilators on duty. From the examination hall, the submitted answer booklets are returned to the examination officer. This is where the answers sheets are collected by the lecturers for marking. After marking the questions and each student score computed, the lecturer submits the computed scores to the department’s examination officer for further processing by the MIS (Management Information System) before the students are been allowed to check their results after academic board approval.

The paper and pencil method of writing examination, which has been in existence for years and one of which was described here may not be appealing for use because of the problems usually experienced, these includes, delay in the release of result, examination malpractices, high cost implication of printing examination materials and human errors. With the introduction of the first computers in the 1970s the potential of this new technology was not only for learning environment but also for the design and administration of assessment were quickly recognized [2].

Computer Based Testing (CBT) has become widespread in recent years. Some countries now use an online platform as the primary delivery mode for one or more computer-based tests for accountability purposes. CBT seems to have advantages over paper and pencil testing, both for organizations that run the assessment programs and for the students who use them. The CBT advocate have identified many positive merits of this approach of assessment which include efficiency administration, student preference, self-selection options for students, increased in authenticity and immediate score reporting and so on [3], [4].

This paper presents a Computer Based Assessment (CBA) client/server application which uses unique features of identification by means of facial biometric system instead of manual method of verification using identity card.

2. LITERATURE REVIEW
In today's electronically wired information society, there are an increasing number of situations e.g. accessing a multiuser computer accounts which require an individual, as a user, to be verified by an electronic device. User authentication is therefore very important. Traditionally, a user can be verified based on whether he/she is in possession of a certain token such as an ID card and/or whether he/she is in possession of specific knowledge which only an authorized person is expected to know such as a password. These approaches of user authentication have a number of significant drawbacks. Tokens may be lost, stolen, forgotten, forged, or misplaced. Passwords may be forgotten or compromised. All these approaches are unable to differentiate between an authorized user and an imposter who fraudulently acquires the "token" or "knowledge" of the authorized user. Therefore, token or knowledge-based authentication does not provide sufficient security in many critical applications involving access control and financial transactions.

Biometrics, which is the automatic identification of a person based on their physiological or behavioral characteristics, relies on "something which he/she is or he does "e.g., fingerprint of the user is collected through scanner to make a personal identification [5]. It is inherently more reliable and has a higher discrimination capability than the token-based and/or knowledge-based approaches, because the
physiological or behavioral characteristics are unique to each user. Currently, nine different biometric indicators are either widely used or are under intensive evaluation, including face, facial thermogram, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, and voice- print. All these biometric indicators have their own advantages and disadvantages in terms of the accuracy, user acceptance, and applicability. It is the requirements of an application domain which determine the choice of a specific biometric indicator [5]. In order to enable a biometric system to operate effectively in different applications and environments, a multimodal biometric system which makes a personal identification based on multiple physiological or behavioral characteristics is preferred [6]. Consider, for example, a network login application where a biometric system is used for user authentication. If a user cannot provide good fingerprint images (e.g., due to dry finger, cuts, etc.) then face and voice may be better biometric indicators. If the operating environment is “noisy” then voice is not a suitable biometric indicator. If the “background” is cluttered, then the face location algorithm, which is necessary for face recognition, may not work very well [6]. Some works on multimodal biometric systems have already been reported in the literature.

3. RESEARCH METHODOLOGY

The research methodology explored in this work is the Structured System Analysis and Design Method (SSADM) where the proposed system structure is fully analysed and new system designed and developed based on the results of the analysis.

The system is designed on a server-client based architecture with the questions for examinations being set on the server via the Computer Based Assessment (CBA) application. Also registrations of students are done one on one on the server. The server houses the main database of the application as well as the templates for the biometric information. The client application connects to the database and template of the server, to verify the last five digits of the matriculation number and password provided by each student before being allowed into the question/test interface.

The reasons given by [2] for the unsuitability of some biometric indicators as explained in the last section of this paper, is what makes the researchers of this paper limit the indicator used in the study to facial data and also to reduce the stress involved in multi modal biometrics usage. The following is the algorithmic steps of the proposed system.

- The ‘Admin’ gets the personal data of the candidate for the exams, including face capturing.
- The program prepares and prints the ‘registration slip’ and the ‘Assessment Card’ for the candidate with a password.
- Admin set the Exams question and store in database.
- Before an Examination is taken, the ‘Assessment Card’ is presented to the ‘Admin’ who will verify by comparing the candidate’s picture on the ‘Assessment’ Card with the one in the Facial database.
- Once they are the same, the student proceeds to take the exams using the CBA program.
- Result of the student is displayed after exams.
- However, if the facial data is inconsistent, the student is de-registered for the exams.
- Results sheet generated by the ‘Admin’

The architecture of the proposed system is as shown in Fig. 1 below.
Fig 1: Architecture of the Proposed System
4. RESULTS OBTAINED

The various displays from running of the CBA program are presented below.

**Fig. 2 Registration Slip**

**Fig. 3: Assessment Card**

The assessment card has the facial data captured part which is compare with the content of the database at the point of entering the examination hall. Candidate proceeds to the CBA exams if no inconsistency is discovered, otherwise candidate is disallowed to write the examination.

**Fig. 4: Test Instruction Panel**

**Fig. 5: Sample Question Panel**

**Fig. 6: Result Panel**

**Fig. 7: Student Assessment Score Interface (for the ‘Admin’)**
5. DISCUSSION
The proposed system from which some interfaces were presented in the last section, is a system of computer-based assessment which uses facial biometric data as a measure of identification into the test hall.

There are two levels of users, namely: the ‘Admin’ and the candidates (or students) for the examination.

The ‘Admin’ register new student, set questions, verifies his/her biometric facial data and if okay admits the student into the examination hall to interact with the question panel and thereafter generate reports. The student, on the hand, interacts with the system by inputting their records for the Assessment Card that is issued by the ‘Admin’ on successful registration to the students. On examination day, the student proceeded to the system login interface and enters his/her matriculation number and a password that is given by the ‘Admin’ after successful identification process. If the login is successful, the student reads the instruction on the instruction panel and then proceeds to take his test. Each student test score is displayed to him/her immediately after completing the test. All these are evident in the different displays in the previous section.

6. CONCLUSION
The proposed system when tested with a set of HND II students of the department of Computer Science, the Federal Polytechnic, Bida recorded a zero percent impersonation. This is an excellent point over what is obtainable with CBA only and the traditional mode of examining students. Although a uni-modal approach to biometrics is employed in this study with strong reasons as mentioned earlier, we strongly believe that the use of multi-modal approach whereby more than one biometric indicators are combined will go further to strengthen the security of computer based assessment. This is already being proofed right by the Joint Admission and Matriculation Board (JAMB) in Nigeria employing this in the 2017/2018 JAMB examinations. Comparing the level of security in the use of CBA with any of two biometric indicators (e.g. fingerprint and face) is a study in the future.

7. RECOMMENDATION
This system is recommended for all computer based examinations most especially where the envisaged stress in the use of more than one biometric indicators is expected to be much owing to the candidates population.

8. REFERENCES