World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 2, No. 4, 120-124, 2012

A Biometric Model for Examination Screening and Attendance Monitoring in Yaba College of Technology

Rufai M.M, Adigun J. O, N. A. Yekini
Department of Computer Technology, Yaba College of Technology

Abstract —Examination malpractices have consistently remained a bane of Nigerian educational system. A common form of examination malpractices is the deliberate impersonation of the applicant. Part of the requirement of a credible examination is that the real applicants wrote the exams. Several steps have been taken to check this crime unabated. Some of the methods adopted are: the use of Identity card; the presence of invigilators to identify fake students; the allocation of sitting arrangement number that determines the hall where the student will write exam and the need to sign in and out on the attendance sheets. This research work proffers solution to the problem of student impersonation during exams. A biometric model is designed to identify every applicant at the point of entry into the examination hall. A biometric verification exercise is also conducted while the examination is going and at the point of submission of examination papers. The students' attendance is captured automatically as their identity is verified on the biometric systems. The Biometric Access Control Techniques is explained. A model describing its application to examination screening and attendance monitoring is designed using denotational mathematics.

Keywords- Biometrics; Examination Malpractices; Attendance Monitoring.

I. INTRODUCTION

Examination can be defined as an instrument for testing assessment, evaluation and accreditation (Ike, 1996). It is a potent instrument for judging knowledge and competence. An exam is credible if it possess the following key elements: free and fair; devoid of partiality, cheating and all forms of examination malpractices. Candidate impersonation is one of the prominent forms of examination malpractices. The idea is that a more knowledgeable personality is hired as machinery to write exam for the original candidate. A invigilator identifies a genuine candidate by his Identity card that bears his name, picture and other relevant information. Out of all the information present on the candidate's Identity card, only the picture is verifiable on the spot. That is the invigilator looks at the face of the candidate and tries to match it with the picture on the identity card. Unknown to him, the picture of the impostor can be on the identity card while other information belongs to the genuine owner.

Genuine verification of the candidate's identity as a major requirement for participation in an exam is the primary objective of this research work. This explain why biometric fits into the overall objective of this work. At the entrance to the examination hall, the identity of student is confirmed and the attendance is automatically captured during student identity and exam eligibility biometric verification.

II. EXAMINATION PROCESS IN YABATECH

Yaba College of Technology is one of the foremost polytechnic in Nigeria established in 1963. Examination are conducted twice in a year is that first and second semester examinations. A student must satisfy some conditions before he can qualify for writing exams. Some of these conditions are:

- He must have duly registered: which includes payment of school fees and course registration
- He must have not less than 70% lecture attendance

After satisfying the above conditions a student is issued an examination docket which he presents to the invigilator at the point of entry into the examination hall. The student is additionally given a sitting arrangement number that determines the hall of examination.

For verification purpose, a student is expected to present the student identity card, the school fees receipt, the examination docket and the course registration. Each of these confirms the payment and registration status of the student.

Additionally, a student is expected to fill the attendance at the beginning of the examination and he also signs out at the end of the examination. The essence of attendance is to have on record which student actually wrote an exam.

However, the following are obvious weaknesses of the existing examination process described above:

- Identification and verification using identity card is susceptible to forgery. Forging of identity card is one of the easiest things to do. An ill-minded student can hire another student as machinery. The name and other information of the genuine student will be on the identity card but the passport photograph will be that of the impostor.
- It brings about inefficiency. Where there is a long queue of student seeking verification, it takes a long time before the last student is ushered in.

III.THE BIOMETRIC ACCESS CONTROL SYSTEM

Biometric can be defined as study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits (Commission of the European Communities, 1993). Biometric characteristics can be divided in two main classes:

Physiological are related to the shape of the body. The oldest traits that have been used for more than 100 years are fingerprints. Other examples are face recognition, hand geometry and iris recognition.

Behavioral are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. More modern approaches are the study of keystroke dynamics and of voice.

A biometric system can provide the following two functions

Verification: Authenticates its users in conjunction with a smart card, username or ID number. The biometric template captured is compared with that stored against the registered user either on a smart card or database for verification.

Identification: Authenticates its users from the biometric characteristic alone without the use of smart cards, usernames or ID numbers. The biometric template is compared to all records within the database and a closest match score is returned. The closest match within the allowed threshold is deemed the individual and authenticated.

IV.THE BIOMETRIC ACCESS SYSTEM

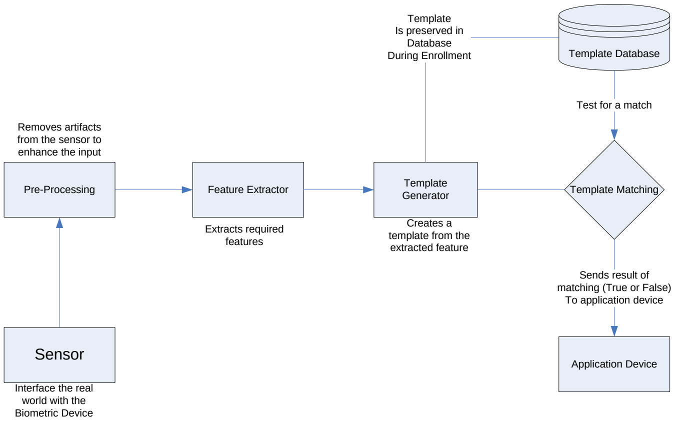

Figure 1. The Biometric Access System

The diagram above shows a simple block diagram of a biometric system.

The main operations the system can perform are enrollment and test. During the enrollment, biometric information from an individual is stored. During the test, biometric information is detected and compared with the stored information. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust.

The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. For the sake of our discussion the sensor may be a fingerprint capture device which provides an interface where the user thumbs print. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise or image), to use some kind of normalization, etc. The above feature is built into the capture device.

In the third block features needed are extracted. This step is an important step as the correct features need to be extracted and the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of all the characteristics extracted from the source, in the optimal size to allow for adequate identification. If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area).

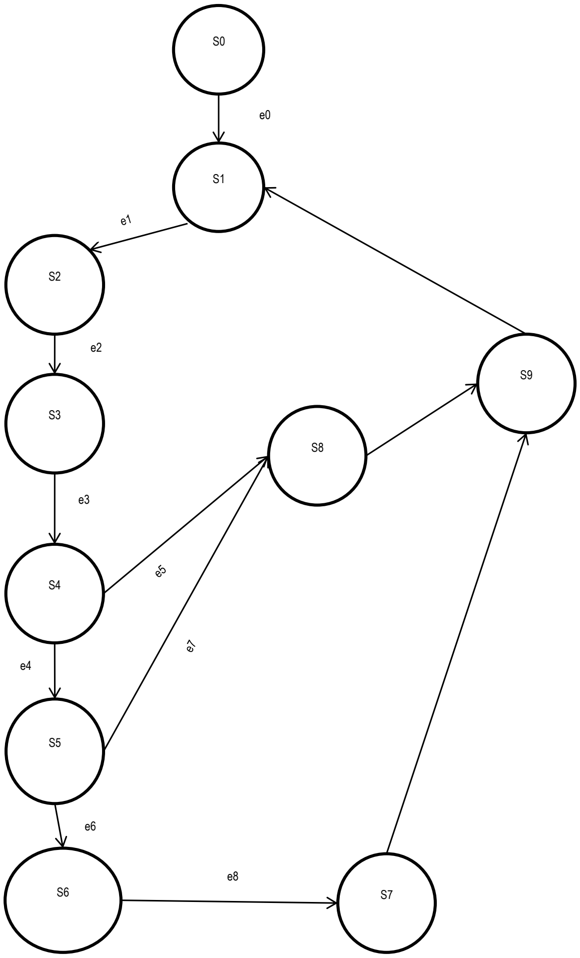

Figure 2. The Abstract Transition Model of the BESAMS Behaviours

V.BIOMETRIC MODEL FOR EXAMINATION SCREENING AND ATTENDANCE

The examination process and the biometric access control system have been described in previous sections. This section focus on modelling a biometric system that will screen student for exam based on the criteria stated in section 2(Examination Process) and at the point of screening the attendance record of the candidate is preserved.

The process in line with the general features of a biometric system. Has two parts which are:

Enrollment:

- A student registers at the beginning of a session by filling an online student and course registration form.
- The biometric identity of the student(e.g. fingerprint) is also captured
- The data is preserved in a database
- The data is updated on regular interval (e.g. at the beginning of every semester)

Verification

Verification takes place before the commencement of the examination. It is repeated two or three times during and at the end of the examination

- The student append his fingerprint on the biometric device for data capture
- The captured data is compared with the template in the database for a match. The existence of match confirms the studentship of the candidate
- The system checks for the registration and payment status of the student. If this is confirmed the student access to examination room is granted.
- At the end of the exam process 2 is repeated. This serve the purpose of sign out
- The matric no, name, time of operation and class of the student is extracted as attendance

The formal model of the Biometric Examination Screening and Attendance Monitoring System as a Finite State Machine BESAMS is defined as a Five tupple relationship

$$BESAMS \mid\mid (S, \Sigma, s, F, \delta) \qquad (1)$$

Where

- S is a set of valid states that forms the domain of the BESAMS, S = {s0, s1, …, s8} where the states are:

s0 –System,
s1 – Welcome,
s2 – BiometricID Capture,
s3 - Register,
s4 – IdentityVerification,
s5 – Registration and Payment Status checked
s6 - Attendance is taken
s7 - Entry is granted,
s8 – Entry denied
s9 – Exit

Σ is a set of events that the ATM may accept and process, Σ = {e0, e1, …, e12} where:

e0 - Start,
e1- Append Fingerprint,
e2 – Supply Registration and Payment Data,
e3 – Check for FingerPrint Match,
e4 – Match Found,
e5 – Match not found,
e6 –Status confirmed,
e7 – status not confirmed,
e8 – Sit allocated,

- *s* is the start state of the ATM, s = s1 (Welcome);
- *F* is a set of ending states, F = {s1};
- *δ* is the transition function of the ATM that determines the next state of the FSM, si+1, on the basis of the current state si and a specific incoming event ei, i.e., si+1 = δ (si, ei), where δ = f: S × Σ → S (2).

The transition table showing the transition from one state to the next state upon an event is shown below

s_i	e_i	si+1= δ (s_i,e_i)
s_0	e0	s1
s_1	e1	s2
s_2	e2	s3
s3	e3	s4
s4	e4	s5
s5	e6	s6
s6	e8	s7
s4	e5	s8
s5	e7	s8
s7		s9
s8		s9

The transition diagram derived from Table 1 is shown in Fig. 2 and Fig. 3.

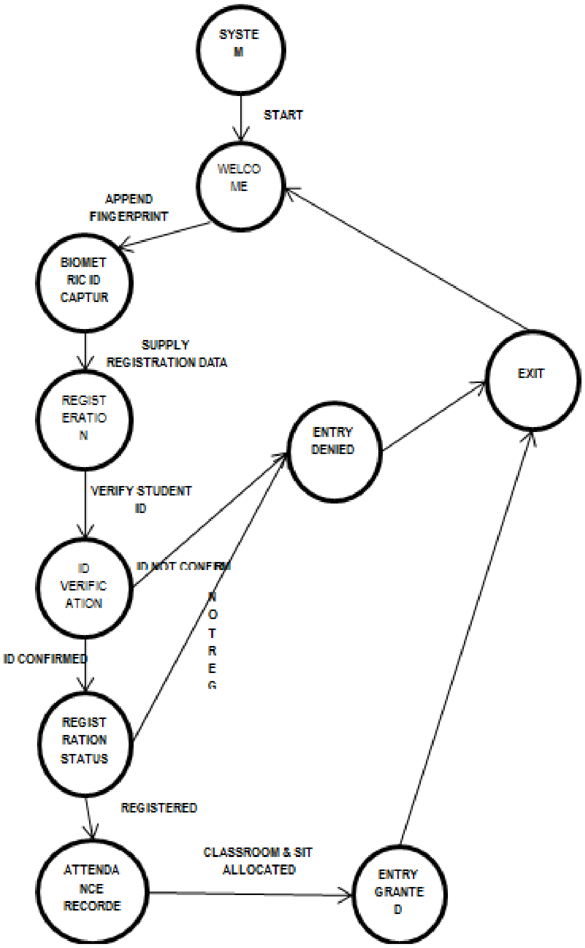

Figure 3. The Transition Model of the BESAMS Behaviours

VI. BENEFITS OF THE MODEL

The Biometric model offers the following benefits:

A. *Efficiency in Student Screening*

Unlike the manual method of screening a student does not have to go through the rigorous process of identification before he is allowed into the examination Hall. His identity information is already stored in the database. He confirms the ownership of the information by appending his finger print, after which entry is granted. The students may come to the examination hall with fewer documents.

B. *Increase in service rate and Reduction of Queue*

The steps involved in manual verification exercise prior to biometrics are numerous, consequently leading to long queue. The introduction of biometric approach reduces the steps, thereby increasing the service rate and reducing the queue.

C. *Increase Security Level*

Also the use biometric devices help increase security levels of the school and protect the students' privacy. This is because of the simple fact the as against the traditional I.D cards and Pins one student cannot misuse, forge , steal another student's biometric identity in order to access a fellow students account.

D. *Reliability and Cost Effectiveness*

Biometric means are much reliable, they save the cost of producing Identity cards, easy to use, as well as secure for the students. The biometric identification is not as high-tech ultramodern concept and is quite affordable. These methods have proved to be very handy in curbing the problems relating to forgotten Pins, lost cards, and the potential for misuse due to bullying and so on.

VII. RESEARCH RECOMMENDATION

The Biometric ATM as good as it is, in improving security, has some challenges which require further work. The first of these challenges is spoofing i.e. the use of forged biometric object (e.g. Plastic finger) in accessing a secured system. An example of such is described in an article published by a group from Yokohama National University in Japan. In this article Matsumoto and colleagues developed a method to spoof fingerprint devices (T Matsumoto et al, 2002) by making a mold from plastic, originating from both a live finger and a latent fingerprint. Artificial fingers were then created from the casts using gelatin, commonly used for confectionary, where the resultant casts were termed "gummy fingers". The resultant artificial finger works perfectly like the original natural finger in identifying the user. This development poses a serious challenge to the future of biometrics. However, a ready-made solution to this problem is liveness detection. The goal of liveness testing is to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture.

Another challenge is the security of the biometric template. Once this is compromised the user loses his identity for life. A compromised PIN can be changed to remove security threat but this is not the same for biometric template because of its permanence.

The recommendation is that more works need to be done in evolving a more robust liveness detection algorithm that eliminate the danger of spoofing and guarantee a true identification of the user.

VIII. CONCLUSION

In this paper we designed a Biometric Model for Examination Screening and Attendance Monitoring using Finite State Automata Theory. Biometric Access is a better substitute for the use of Identity card in verifying users identity. Experience has shown the porosity of Identity cards in uniquely identifying individual in the face of sophisticated forgery technology. The naturalness in the use of fingerprint makes it a reliable access control technique. The fact that a user no longer needs to carry identity cards and other documents for identification explain the ease of use. Future work may see to the implementation of the proposed model in Examination Halls.

Apart from the fact that it takes us to another level in human machine interface, it is economical and easy to use, it should be adopted by Educational institutions in Nigeria.

REFERENCES

1. Aminu, J. (2006). “Examination malpractice in Nigeria: roots, sustenance, endemicity, dangers and assailance”. Keynote Address Delivered in a Two-Day Summit on Examination Malpractice in Nigeria Organized by the House of Representatives Committee on Education Held at the Shehu Musa Yar’ Adua Centre, Abuja, August 15-16, 2006.
2. Awanbor, D. (2005). “Credentialing process in the Nigerian educational system”. Keynote Address Presented at the First Annual Conference of the Faculty of Education, Ambrose Alli University, Ekpoma, November 10-12, 2005.
3. Commission of the European Communities (1993) "Glossary of Information Systems Security "Contract 52001, Definitions within information systems security,.
4. L Thalheim, J Krissler, (November 2002).“Body Check: Biometric Access Protection Devices and their Programs Put to the Test”, c’t magazine.
5. Rufai M. M., Adetoba B. T., Adigun J. O. (2007). Biometric Access and Users Identity in Automatic Teller Machine, International Journal of Physical Science, Vol 2, No. 2.
6. Rufai M. M., Adigun J. O., Yekini N. A. (2007). Modelling Discretional Access Control in Automatic Teller Machine Using Denotational Mathematics International Journal of Computer Science and Network Security, Vol. 11, No. 11, ISSN 1738-7906
7. T Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, (January, 2002). “Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems”, Proceedings of SPIE, vol. 4677.
8. Wang, Y. (2007a). Formal description of the cognitive process of memorization. In Proceedings of the Sixth International Conference on Cognitive Informatics (ICCI’07) (pp. 284-293). Lake Tahoe, CA: IEEE CS Press.
9. Wang, Y. (2008a). Deductive semantics of RTPA. The International Journal of Cognitive Informatics and Natural Intelligence, 2(2), 95-121.

AUTHOR’S PROFILE

Rufai Mohammed Mutiu obtained his B.Sc degree from Ogun State University (Presently Olabisi Onabanjo University), Ago Iwoye, Ogun State, Nigeria. He got his Masters in Computer Science from University of Lagos, Akoka, Lagos, Nigeria. He is a member of Nigeria Computer Society and presently lectures at Yaba College of Technology, Lagos, Nigeria. His research area is Information Systems Design and Modelling.

Adigun Johnson Oyeranmi is a specialists in computer software, security and knowledge management. He obtained his first degree (B.Sc Computer Science) from University of Ibadan, Oyo State, Nigeria and his Masters(M.Sc. Computer Science) from University of Lagos. He is a member of Nigeria Computer Society of Nigeria and Computer Professionals Council of Nigeria. He is the current Dean of The School of Technology, Yaba College of Technology, Yaba, Lagos.

Yekini Nurein Asafe majors in Data Communication and Networking. He obtained his B.Sc. degree in computer Engineering from Lagos State University and Master Degree in Computer Science from University of Lagos, Nigeria. He is a member of Nigeria Society of Engineers. He currently lectures Data Communication and Networking in Yaba College of Technology, Lagos, Nigeria.