

Implementing Biometrics to Curb Examination Malpractices in Nigeria

O.A.Odejebi and N.L.Clarke

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

The problem of examinations malpractices that has been plaguing Nigeria for decades in spite of visible efforts by the stakeholders is examined in this paper. The main fundamental problems are identified as the absence of a credible identity verification system. This has an over bearing effect on knowing who should be where and at what time. Biometrics is considered as an adequate solution, with its proven achievement level in identification and verification of identities effectively answering the question- who you are. But given the peculiarity of Nigeria, there are general and solution specific requirement to be met for a successful implementation of biometrics in Nigeria. The proposed biometric solution; a smartcard based fingerprint verification technology incorporating the security strength of smartcards and the accuracy and speed of fingerprint biometrics is presented. A case for it is made, discussing the choice of technologies, cost and the views of the stakeholders. The paper concludes by looking at limitations of the presented solution and necessary future work if examination malpractices will be absolutely defeated.

Keywords

Examination malpractice, biometrics, identity verification, smartcard, fingerprint

1 Introduction

The recent ruthless and constant upward increase in examination malpractice cases in public examinations in Nigeria, the forms of its perpetration and the increase in its sophistication at an alarming rate called for at least equal measure of sophistication in the effort to curb this menace. The fact that examinations has to do with testing individual abilities means that in the minimum, the examiner needs to be able to identify the examinee in some way to be sure that the appropriate person is examined.

In Nigeria today, the examination institutions are using several manual methods of identity verification. These methods entirely relied on the ability of human beings to perform verification or authentication tasks and have failed so far in this concept to impact on the growing problem, hence the need for a reliable and accurate way of carrying out these checks.

Biometrics, described by (Blackburn, 2004) as “automated methods of recognising an individual based on their physical and behavioural characteristics” has been in

existence for centuries although in a non-sophisticated form (Zang, 2000). Biometric technologies have been used in various capacities to enhance security of processes, procedures and systems usually serving a complementary purpose. Different types of biometrics exist with peculiar merits and demerits in varying level of complexity and sophistication.

Its implementation to provide a viable solution towards curbing the rampant examination fraud in Nigeria is discussed. This paper presents Identity Smartcard with fingerprint match on Card as a viable solution which is proposed after a careful understudy and analysis of the problems as capable of keeping the vice under control.

2 Problem of Examination Malpractice

The fundamental success of any examination administration is the ability to keep the examinations materials confidential, making sure that the candidates sitting for the examinations are authentic and abide by the rules and ensuring that the process of scoring candidates is transparent and fair. A departure from any of these is regarded as examination malpractice.

There has been a persistence increase in the number of reported examination malpractice cases since year 2000. There are 40,805 malpractice cases in the senior school certificate examinations conducted by the National Examinations council-NECO in year 2000 and this figure has grown to 469,582 cases in 2007 (NECO, 2007). These figures show an annual increase of about 167%. The number of candidates caught in the act is up by about 5% within the same time frame (NECO, 2007). Taking into account the fact that an average of 1million candidates register for this examination yearly, this implied about 50,000 candidates are caught every year.

2.1 Impersonation

West African Examinations Council, a sister examination body to NECO reported increase in impersonation figure from 0.2% of the total malpractice cases in 2000 to 1.2% in 2005 (Uzoigwe, 2007). This figures does not justify in anyway the effort that goes into planning and administering these examinations as discovered while understudying operations of these examination bodies. The impersonations are now planned from the registration stage, making it difficult more than ever to spot ordinarily.

2.2 Leakages

Examinations materials leakage is the most serious problem capable of disrupting the whole examinations especially when it leaks well ahead of the examination day. It was made manifest during the studies that these leakages might be through the distribution drivers, subject officers, centre supervisors and custodian points. The fact that this problem in particular is hardly admitted by the examination institutions makes availability of statistical data very hard to come by. However, it is well known that the leakages are becoming more serious threat as the year goes by.

3 Solution Requirements

The biometric verification of the identity of the candidates as well as that of the officials administering these examinations could go a long way in reducing the problem of malpractice. Identity verification is capable of at least eradicating impersonation and by extension contributes towards behaviour improvement within the examination hall. Its variant could be implemented for access control to enforce who can access what resources.

To successfully implement biometric identity verification in examination in Nigeria, the following requirements need to be met.

3.1 General requirements

The uniqueness of Nigeria where the system or the solution will be deployed necessitates meeting some basic requirements that may otherwise not be necessary if the same solution is to be deployed in another part of the world. These are bulleted below:

- The system must be independently powered.
- Use of matured technology is mandatory
- Biometric template storage method must be carefully selected
- The system must be quick and secure

These are made necessary by peculiar conditions in the country such as incessant power failures, poor communication infrastructures, Nigerians impatience and curiosity.

3.2 Solution Specific Requirements

These requirements stems from the problems that needs to be solved and the need for the solution to be able to effective in solving those problems while been able to seamlessly work with the existing systems and processes. They include:

- The solution must be one that could be Integrated with the existing registration procedure
- The system must be able to conclusively carry out identity verification
- Integration of candidate attendance record keeping not negotiable
- The solution must incorporate blacklisting function

Working closely with these requirements is essential. Only then will it be possible to achieve a solution that will be effectively able to curb the problem of impersonation first hand and other forms of examination malpractice by extension.

4 The Biometric Solution

Biometric solutions are generally implemented using one or more of the human physiological or behavioural attributes. Biometric technologies that could be used to implement the solution includes but not limited to; iris scanning, hand geometry,

voice recognition, fingerprint scanning and keystroke analysis. All biometric systems are basically made up of the same fundamental blocks and they all work the same way (Xiao, 2007).

4.1 Identity Smartcard with fingerprint match on card

The solution combines the smartcard technology with the speed and performance of the fingerprint biometrics to solve the perennial problem of examination malpractice. A multiple card operating system- MACOS capable microprocessor smartcard is used as an identity card with the photograph of the holder printed on the card secured with ultraviolet and hologram printing. The card equally will hold the biometric fingerprint template that will be used for verification. The verification unit will be custom built to house the fingerprint scanner, the smartcard reader and a visual display unit capable to operate in enrolment or verification mode. Figure 1 shows the block diagram of the enrolment process.

4.1.1 Enrolment

The enrolment process is divided into two stages the online registration and the biometric enrolment. During the online registration stage individual candidates will be required to register using a web form to submit their personal information as well as the subjects for which they wish to sit for during examinations. This data is centrally stored.

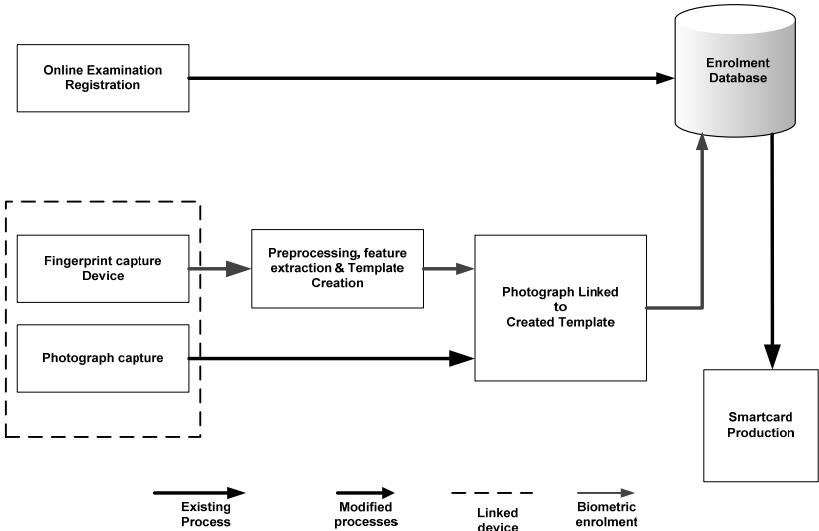


Figure 1: Enrolment block diagram

However during the biometric enrolment, the candidates will first be required to provide the registration number issued to them during the online registration phase and another source of information that could be used to verify their identity, such as driving licence, national identity card or international passport. The candidates'

photographs will be taken at this stage as well as the fingerprint sample using the fingerprint scanner. The minutiae based system is used. Figure 1 shows the general block diagram of the enrolment process.

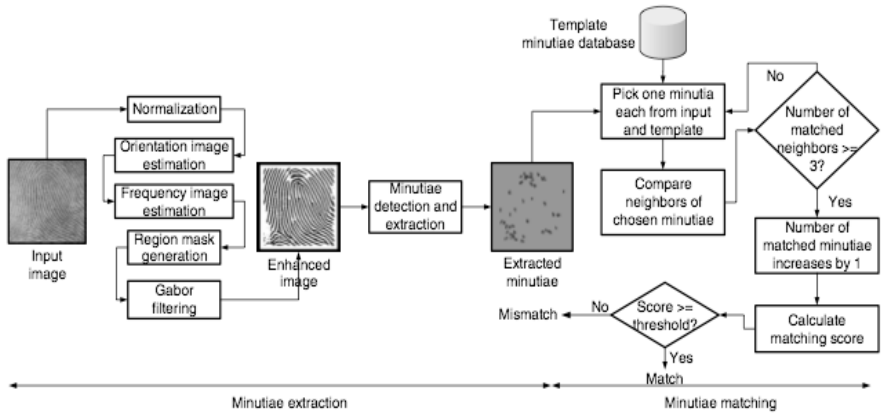


Figure 2: Typical minutiae extraction and matching source (Pallav, et al. 2005)

The fingerprint image obtained is normalised, its orientation and frequency estimated and region mask applied then Gabon filtered to obtain an enhanced image (Pallav, et al. 2005). The minutiae will be detected, extracted and stored as template. Figure 2 shows typical minutiae extraction and matching process. But in this case, the template obtained for individual candidate is then stored on the smartcard.

4.1.2 Verification

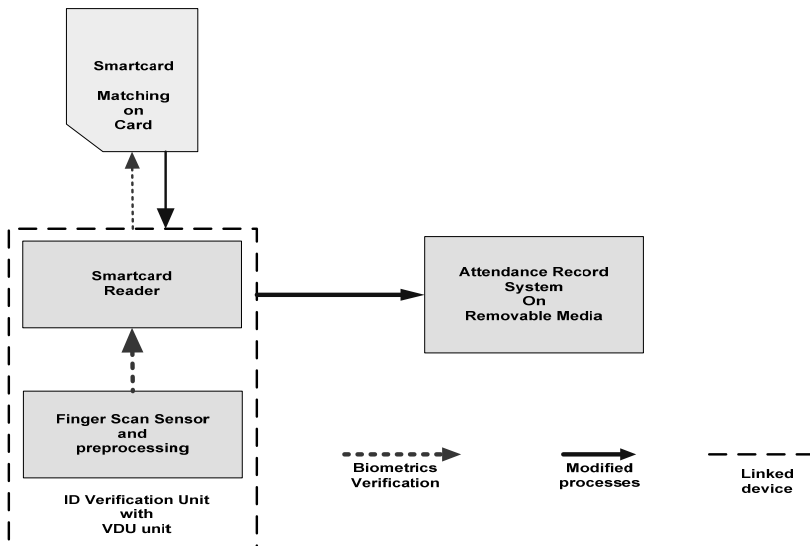


Figure 3: Verification and attendance record system

During verification stage, the candidate is required to produce ‘what he/she has’ - the smartcard issued during enrolment. Then, the verification unit will prompt for finger scanning. The process of template creation is then repeated and the minutiae extracted but this time the created minutiae template is communicated to the card holding the enrolment minutiae template. The matching algorithm resident in the card is used to match the minutiae and a matching score is calculated. The candidate is considered a match if the calculated score exceeds threshold. The smartcard then allows the attendance record application access to the candidate information stored on the card. Figure 3 shows the general verification block diagram of the identity smartcard with match on card fingerprint biometrics.

This 1:1 matching is typically enough to conclusively verify candidate or staff claimed identity. This verification is carried out offline and removes the envisaged communication problem that may hunt match on server approach.

5 Discussion

There is more than one possible solution that can be used to solve this problem of examinations malpractice. The choice of the identity smartcard with match on card fingerprint biometrics is a synergy of effective problem analysis; clear understanding of the available options and insightful cost management. The solution’s successful implementation to curb examinations malpractice in a country like Nigeria requires a little bit more to be considered especially in making the choice of the technology that will effectively do the job.

5.1 Choice of Technology

The choice of fingerprint biometrics is selected after a careful study of every option available. Such technology includes iris technology, hand geometry, voice and face recognition. Availability of the biometric attribute is considered; about 99.98% of the candidates have fingers with they would write the examinations (NECO, 2007). There are sizable numbers of deaf and dumb candidates enrolling for examinations annually. Therefore, the implementation of fingerprint will translate to use of less pragmatic alternative verification approach for the remaining less than 0.02%. Usually alternative biometric attribute is implemented for those users who either do not have fingerprints or a fingerprint good enough for enrolment.

Considering the performance measure statistics, fingerprint technology has a false acceptance rate FAR of 0.0008% and false reject rate FRR of 2.5% (Deutsche Bank Research, 2002). Although iris scans technology that has a better FAR figure, however, taking into consideration the acceptability factor, fingerprint technology has a better standing. The same is applicable when considering speed and accuracy. Although, at present the technology is implemented in verification mode, if necessary it is identification mode capable, this is good for scalability.

The solution combines biometrics with smartcard technology. Smartcards are made to securely resist any attack or in the minimum to show evidence of attack. The decision to use smartcard is not only informed by the security needs but also by the need to carry out the verification offline. The selection of the solution fits the

ambition of all the educational and examination institutions in Nigeria to make the solution work across board.

5.2 Cost

This is a very important factor to be given consideration since there is always a limit on the amount of resources available for every project. The government through the examination bodies will finance part of the project while the candidates themselves will bear the cost of the identity smartcard issued them. Since the cost of implementing a solution does not always indicate it is the best solution for a specific problem, it is necessary to include cost as a factor to be considered when making decision on the kind of technology to be implemented.

The equipments and software cost is about \$4.2 million when roughly estimated. The overall cost of implementation is expected to be a little different since the retail costs of most of the equipments are used. It must although be stated that this is the initial cost subsequent cost for each examination will be limited to the cost of producing the card for the enrolled candidates.

5.3 Stakeholders Opinion

This solution when presented to some officials of examinations institutions in Nigeria, in spite of their little understanding of the technology, saw its possibility of helping to put a stop to the identity based examination malpractice problems especially impersonations. Some believed that its being new will make it enjoy success for a while. Others said it would in the minimum serve as deterrent while some are rather uncomfortable with spending \$4.2 million only to get a solution that will only serve as a deterrent.

When they were asked about their fear with regards to the implementation of the solution, the response was clear and suggestive of the general and solution specific requirements initially enumerated. Other than this, there are concerns about what will happen should a candidate's card get lost. Some student can loose the card intentionally so as to escape the biometric verification. In as much as this type of problem is not unexpected, therefore well-defined procedures such as using other official identity documents for verification and treating such candidates as special and possibly keeping special eyes on them if they are at all allowed write the examination.

The majority of the stakeholders have cost as their top priority, also many of them place more emphasis on the effective identity verification at the expense of security and maintenance. This is not unexpected, but when they were asked which of the two solution presented, majority clearly agree that identity smartcard match on card fingerprint biometrics is better.

5.4 Future Work

Copying from other candidates or textbooks and substitution of answer booklets etc. all still constitute examination malpractice (Adamu,1998 and Fagbemi, 2001). This,

sloppy or unpatriotic attitude of the verification supervisors for example can not be curbed by the proposed solution.

Having stated that this solution cannot summon all the problems independently, then there are other areas that must be looked into for solution in the future. Handwriting recognition for the purpose of verifying who actually write the examination will be a huge step forward if it could be effectively implemented. It might just be the required solution to eradicate vices like swapping of examination answer booklets. Not this alone, work needs to be done towards implementation of fingerprint screening of answer booklets or sheets as the case may be, especially the optical mark reader sheet currently used for collecting multiple choice type questions responses.

6 Conclusion

The result of the research carried out on the examination institutions in Nigeria show that there are concerted efforts towards perfect delivery of the examinations with little to show for the work done. This is largely due to the fact that there is a large number of identity related loopholes. With problems such as impersonation forming foundation for other kinds of malpractices, the effective way of verifying individual identity has to be implemented. Biometrics of course is the right direction to follow but the availability of just few independent evaluation of the existing biometric technology does not make the selection of which technology to implement an easy one.

Biometrics on its own cannot be regarded as a perfect authentication solution, but it is at its best when combined with other forms such as token and PIN or passwords. The choice of technology requires tradeoffs to be made, if not properly set, arriving at a solution that is neither cheap nor fit for purpose is not impossible. While the stakeholder agrees that this solution meets their requirements, it still suffers the same weakness peculiar to every human supervised security. The supervising being is always the weakest link.

7 References

- Adamu, H. (1998). *Indiscipline in Nigerian institutions: Causes, effects and solution*. cited in Ehiozuwa, A. O. (Ed). *Etiology Effect and control of Malignancies in Nigerian Education (EEC OFMINE)*. CPSE Publishers.
- Blackburn, D. M. (2004). *Biometrics 101 version 3.1*. Retrieved January 16, 2008 from www.biometricscatalog.org/biometrics/biometrics_101.pdf
- Deutsche Bank Research. (2002). Biometrics – hype and reality. *Economics* (22).
- Fagbemi, J. (2001). Assesment and Examination Malpractice. *Proceedings of the 16th Annual Congress of the Nigerian Academy Of Education*, (pp. 82-100). Jos.
- NECO. (2007). *The statistical facts of the conducted examinations so far*. Minna, Nigeria: National Examinations Council.

Pallav, G., Srivaths, R., Raghunathan, A., & Jha, N. K. (2005). Efficient Fingerprint-based User Authentication for Embedded Systems. Anaheim, California, USA: ACM.

Uzoigwe, M. G. (2007). WAEC Press Release. Lagos.

Xiao, Q. (2007). Biometrics—Technology, Application, Challenge,. *IEEE Computational Intelligence Magazine* , pp. 5-9 and 25.

Zang, D. (2000). *Automated Biometrics: Technoloies and Systems*. Massachusetts: Kluwer Academic Publishers.