Biometric Enhancement of Home and Office Security to Reduce Assassinations in Nigeria

Ugwu Gabriel E.

Department of Computer Science, Ebonyi State University, Abakiliki
Email: ugwugabrielevo@yahoo.co.uk

Abstract

Insecurity is posing national threat in Nigeria today. You do not know who your next door neighbor is, because of security challenges in the country. Indiscriminate killing of innocent people, kidnapping, fraud by unknown person is becoming a worrisome national problem. The question is how do we minimize this menace? Biometrics security technology uses the physiological and behavourial characteristics of a person to properly identify him and helps to tell the class of person he belongs based on the available data. Your fingerprint, face and iris can grant or deny you access if they are tampered with. Since nobody can be trusted, our motivation is to find a way to minimize killer syndrome, impersonation, terrorism attack and fraud by unknown persons. We used verification and authentication methodology to verify how facial screening explores the different aspects of the face structure and pattern of arrangement to implement a unique personal identification system. It measures the different components of the face structure, such as the nose position, the mouth, the distance of the left eye to right eye and the actual location of the eyes to the mouth, nose etc and stores the bio-information extracted from the face of every person that enrolls in a database. These form the basic identification data. Reduction of financial fraud, assassination and kidnapping is the outcome of the work system. It has minimized unauthorized access to confidential documents and impersonation.

Keywords: Security, Authentication, Physiological, Facial, Enrollment,

1.0 Introduction

Security is of primary concern to the nation. In international setup, the issue of security cannot be swept aside. Government in one way or the other creates a measure to safeguard life and property against bandits, terrorist and men of the underworld. Most of these measures centre on identification of these individuals, and disclosure of vital information concerning them, and subsequently, bringing any culprit to book. A person can be recognized by his various characteristics. You recognize others by their faces when you meet with them. One can also be identified by his voice.Identity verification has originally been by keys, pins, passwords etc. These help to realize the proper person, who owns and or is a member, as the case may be. But these are not absolute ways of identification because, keys sometimes are stolen or lost and passwords are often forgotten or disclosed.

However, to achieve a more reliable identification, we should use something that gives us real points of measurement. The biometrics of a person actually provides vital points that can be used to properly identify him. This method of identification is based on the principles of measurable physiological or behavioural characteristics of the person. Such characteristics as fingerprint, voice sample, pattern of the face, DNA etc, are peculiar to an individual. These characteristics are measurable and are readily available for any given person. Biometrics technology is considered by its usefulness, ease to use, and its security ability. This can be viewed in two modes, the authentication and verification modes.

2.0 Literature Review

2.1 Biometrics Security

Biometrics security application is best implemented in environments with critical physical security requirements or prone to identity theft, Cory Janssen [8]. The issue of security of life and property cannot be over-emphasized. In the world today, the rates of terrorist attack, kidnapping, hijacking, fraudster activities, murdering, stealing and arm rubbery are growing rapidly. The time these activities are carried out is uncertain, and it becomes difficult to predict their mode of operation. Against this backdrop, there is need for a security mechanism to be put in place, to

.

counter the activities of these undesirable elements in our society. Biometric security system pre-stored individual body characteristics. Stanley et al [15] described biometrics as the most secured and convenient authentication tool that cannot be stolen, forgotten, borrowed or forged. If biometric authentication is used in government offices and individual homes for access, it will reduces kidnapping, fraud, assassination, etc: Thamer Alhussain and Steve Drew [13] in their titled Developing a Theoretical Framework for the Adoption of Biometrics in M-Government Applications Using Grounded Theory described biometrics technology as a tools that can ensure that correct working times are recorded and that only authorized personnel have access to government property and resources. Selina Oko and Jane Oruh [14] described biometrics technology application to ATM security as a means to reduce fraud in ATM industry.

.

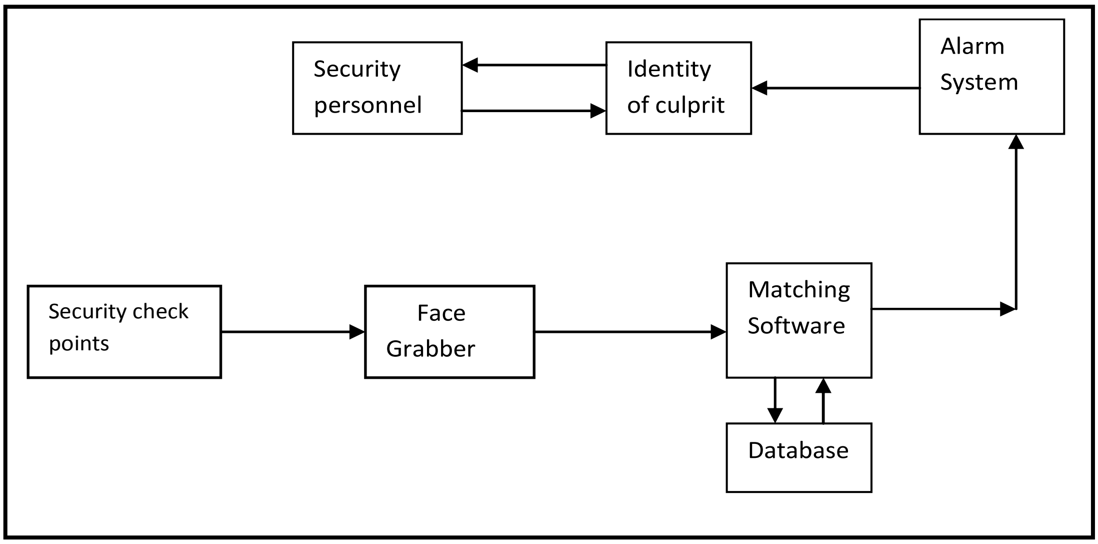


Figure 2.1 Block diagram of biometric enrollment platform

2.2 Biometric Authentication Technology

F.O. Aranuwaand and G. B Ogunniye [1] identified biometric technology as a foundation of an extensive array of highly secure identification and verification solutions, in communication and in our environments. Biometrics is one of the most reliable and secure means of authentication because it uses human distinctive physiological properties like face, eye (retina, iris), fingerprint, etc and behavioural like voice, signature dynamics etc characteristics for authentication Stanley et al (2009) described biometrics as the most secured and convenient authentication tool that cannot be stolen, forgotten, borrowed or forged. Their study identified a number of features that make biometrics a reliable authentication tools. These include: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention Authentication involves the ability of the system in verifying the identity of a user to indicate that he/she is whom he/she claims to be. Authentication could be carried out in the following three ways: i) password and pin, ii) token and smart card . Ratha et al, had pointed out that passwords, cards and pins are no more enough to authenticate holders' identity.

2.3 Types of Biometrics Measurement

Biometrics measurement can be classified into two major types Physiological and Behavioral biometric. According to Julia Zangl Colby and Bernadette Koczwara 2004), Physiological biometrics measures the distinct traits that people have, usually (but not always or entirely) dictated by their genetics. They are based on measurements and data derived from direct measurement of a part of the human body. The face is an important part of the human body. It is this part that can tell who you are, and how people can identify you. Imagine how difficult it would have been to recognize even your own brother if all human faces were to look the same. Facial recognition is a natural way of identifying people. This part of the body helps us to distinguish one person from another.

Therefore, facial recognition is a natural means of biometric identification. Originally facial recognition was not regarded as a science because any good camera can be used to get the image of the face. This biometric measurement is collectable and does not have invasive and intrusive effect. According to Kevin Bonsor (2006), human face when observed critically, has some distinguishing landmarks. These he called valleys and peaks, they make up the different features of the human face. These landmarks are called node. The human face contains about 80 nodal points, which include the following and more:

- Depth of the eye socket
- Cheekbones
- Distance between eyes
- Jaw line
- Width of the nose
- Chin, etc

Computer reads in these measurable points, and covert them into numerical codes, (that is numbers that represents the face), and stores it in the database. These codes are known as faceprint. Facial recognition is primarily used by the Law Enforcement Agencies. They use this technology to capture people faces in the crowd. The faces are compared to a database of criminal mug shots to ascertain the presence of any unknown criminal. This system is also used for security surveillance. Facial recognition is also very useful in the following areas:

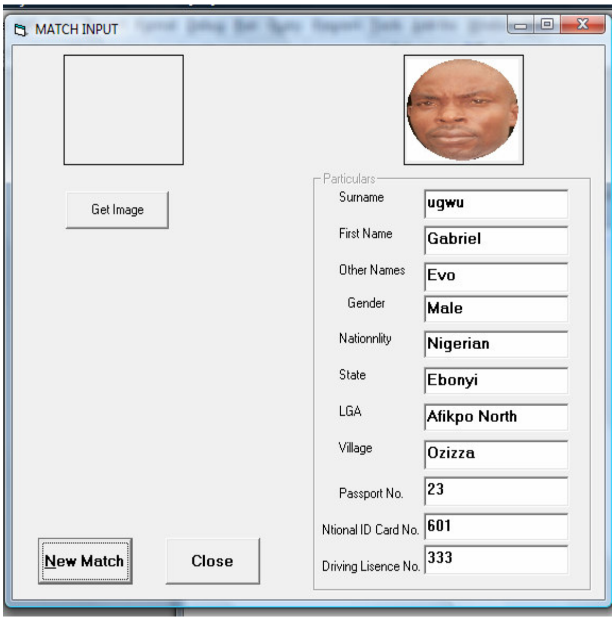
- Elimination of Voting Fraud
- Computer Security
- Checking-cashing identity Verification
- Home and office security.

3.0 Methodology

In the cause of this research a lot of people were interviewed including my supervisor and other professionals in the field of security and. Educational publication by eminent personalities on biometric and security systems also formed source of our information gathering. Analysis of the old manual methods of security check points was very vital to this work. development of a platform for the biometric traits feature extraction (see figure 3.1). The warehouse of information, the Internet was a backbone of our research, a lot of data were gathered from it.

4.0 Discussion

The server and client components of the proposed biometric application can be installed in our office and home entrances or in confidential areas that requires authentication. It is design secured for this purpose, bearing in mind user convenience and security. In view of this, the requirements of the system are defined as follows: (i) prospective users (office members or customers) for face enrollment which includes user's bio-data or photograph captured by the system after registration (ii) verification and authentication on access which involves physical presentation of the face or passport. Biometrics application in security system remains one of the most effective means in checking financial fraud, unauthorized access to confidential documents, impersonation, murder, kidnapping etc. The system authenticates a user properly since it is difficult for two persons to have the same biometric traits. It uses Physiological properties like depth of the eye socket, Cheekbones, Distance between eyes, Jaw lines, Width of the nose and Chin in facial biometrics for identification and verification and this gives it an age over other security measures because these traits cannot be cloned. As a good biometrics security system it was able to spot out key areas of the image input, and extracted it from the whole lot of the image and stores this extracted Bio-Capsule in the database. It also matches this Bio-Capsule in the database against a current input presented across for verification and present a result of the match in a yes/no format. (See figure 4.1and figure 4.2) The system is designed to use the web or digital camera to capture the face of people on enrolment and the bio capsules are stored in the database for future matching. A web or digital camera installed on the entrance (Office or Home) captures the face of the user on access, matches it with the one stored in the database. If it matches access is granted other wise denied. A secured communication channel is suggested to be able handle the possible threats of hacking and tampering with biometric feature in the database. More over, the biometric database should be stored in a reliable environment so as to prevent any attacks that may arise from an intruder.



Surname: ugwu
First Name: Gabriel
Other Names: Evo
Gender: Male
Nationnlity: Nigerian
State: Ebonyi
LGA: Afikpo North
Village: Ozizza
Passport No.: 23
Ntional ID Card No.: 601
Driving Lisence No.: 333

Fig 3.1: samples of pre face extraction mode

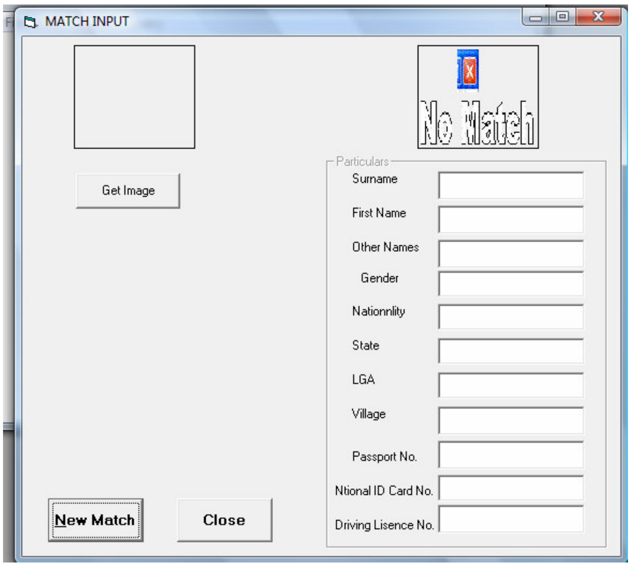
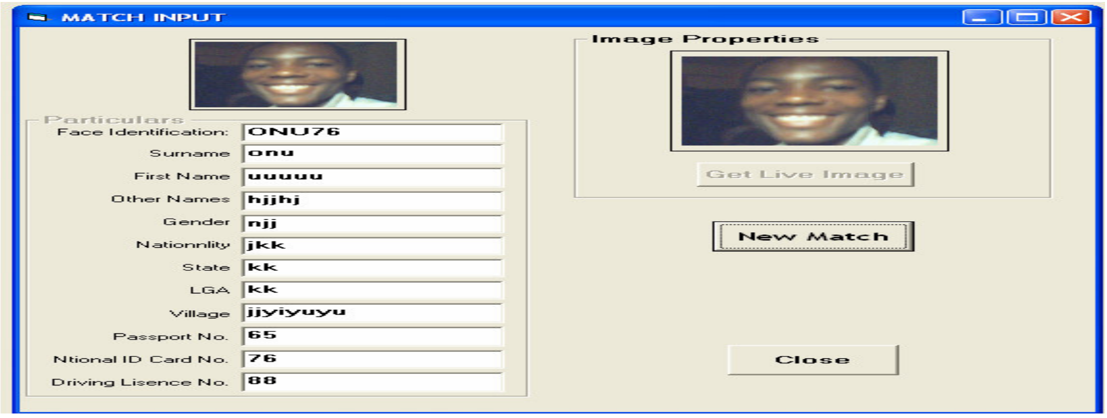


Figure 4.1: output sample for a non match access denied.



Face Identification: ONU76
Surname: onu
First Name: uuuuu
Other Names: hjjhj
Gender: njj
Nationnlity: jkk
State: kk
LGA: kk
Village: jjyiyuyu
Passport No.: 65
Ntional ID Card No.: 76
Driving Lisence No.: 88

Figure 4.2 out sample of a match, access granted

5.0 Conclusion

An enhancing home and office security to reduce the rate of assassination in Nigeria using biometrics has been developed and implemented for use in our environment. The work embraces facial screening that measure the face pattern to extract the features. The stored bio-information of users is used for authentication. it is targeted for offices and home use to reduces kidnapping, assassination . and fraud in our society to the barest minimum . We can store images of the customers, office staff and friends, also families and relations to be granted access depending on the intention of the user. We encourage the Government at both federal and state, level and even individuals, to employ the use of this security system as may be applicable.

References

[1] Aranuwaand F.O. and Ogunniye G. B (2012) Enhanced Biometric Authentication System for Efficient and Reliable e-Payment System in Nigeria

[2] Ayhan E. (2006) Biometric Security Technologies [On-line] http://www.biometrics.tibs.org

[3] Barber, C. B., Dobkin, D. P. and Huhdanpaa H. (1996) The Quickhull Algorithm for Convex Hulls, ACM Trans. *Mathematical Software, Vol. 22, No. 4, pp 469-483*

[4] Belhumeur, P.N., Hespanha, J. P. and Kriegman, D. J. (1997). Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection, *IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 19: 711–720,*

[5] Bobick, A. F. and Davis, J. W. (2001). The Recognition of Human Movement Using Temporal Templates, *IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 23: 257-267*

[6] Bonsor, K and Johnson, R, How Facial Recognition Systems Work, How Stuff Works, viewed on 2nd March 2008 at available at http://computer.howstuffworks.com/facialrecognition.htm

[7] Biometrics History (2006) [On-line] http://www.cs.indiana.edu/- zmcmahon/biometrics-history.htm

[8] CoryJanssen (2015) [On-line] http://www.techopedia.com

[9] Dorai, C. and Jain, A. K. (1997) A Representation scheme for 3D Free form Object, *IEEE Trans, pattern recognition and Machine Intelligent, vol. 19 no. 10 pp 1115-1130*

[10] Geomagic Studio (2005).[On-line]. http:// www.geomagic .com/product/studio

[11] Gordon, G. (1992) Face Recognition Based on Depth and Curvature Features. *Proc, IEEE CS Conf Computer Vision and pattern recognition. pp 129- 136*

[12] Lee, K., Ho, J., Yang M. and Kriegman, D (2003). Video-based face recognition using probabilistic appearance manifolds, *In Proc. CVPR, Vol. I 313-320*

[13] Stanley, P., Jeberson, W., and Klinsega V.V. 2009. Biometric Authentication: A Trustworthy Technology for Improved Authentication. 2009 International Conference on Future Networks

[14] Selina Oko and Janr Oruh (2012) Enhanced ATM Security System using Biometrics International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012

[15] Thamer Alhussain1 and Steve Drew(2012) Developing a Theoretical Framework for the Adoption of Biometrics in M-Government Applications Using Grounded Theory www.intechopen.com