International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12 – No. 12, April 2018 – www.ijais.org

An Improved Framework for Intrusion Prevention in a Host-based Biometric Identification System

Idris Mohammed Kolo
Computer Science Department
Federal University of Technology,
Minna, Niger State, Nigeria

Salihu Alhassan
Computer Science Department
Kebbi State Polytechnic,
Dakin Gari, Kebbi State, Nigeria

Hussain Abubakar Zubairu
Information and Media Technology Department
Federal University of Technology,
Minna, Niger State, Nigeria

ABSTRACT
This research work is aimed at proposing a framework for intrusion prevention on host-based biometric identification systems (BIS). Intrusive activities in biometric identification systems are mostly perpetuated before the existing prevention systems prevent its future occurrence if the same pattern is exhibited by the perpetuator. The research produced a framework that shows an inclusion of a sensor database that registered all acceptable and certified sensors by the system to capture biometric image. This framework has shown using a developed application to some great extent how it is used to minimize the issue of fake template in the database which will make compromise easy. Once a sensor is attached to the BIS its status will be immediately shown and accessed for qualification to capture image.

General Terms
Biometric Intrusion Prevention

Keywords
Biometric Systems, Intrusion prevention Architecture, Host-based Biometric System Framework

1. INTRODUCTION
Traditionally, the use of password and keys has been the medium for controlling access to a system that requires identification or authorization. However, technological advancement has made it possible for malicious users to device series of ways to guess actual password combinations perfectly to access authentication based system. To curb these challenges inherent in the traditional method, [1] showed that biometric trait can be used to uniquely identify every individual based upon the measurement of one or more of physiological attribute (Iris, fingerprint, facial recognition and hand geometry) and/or biological attribute (voice, signature pattern, body odour, gaits) of the individual. A system that can use the biometric trait to identify an individual is referred to as a Biometric identification system.
A typical Biometric Identification System (BIS) comprises sensing, feature extraction and matching components. A BIS can be installed on a standalone system known as a host-based or on a network platform known as network-based. In a network-based BIS, the frontend comprising of a console window and the backend comprising of database will be at different locations. While in a host-based BIS both the frontend and the backend are on the same system [2].

The BIS has two phases, which include: authentication and verification. At the authentication phase, the biometric trait (fingerprint, iris, facial, hand geometry) image of an individual is collected and saved in a database called a template database. At the verification phase, the biometric trait of the person is again collected and compared (matched) with the content of the template database to ensure that what the person claimed is what he/she truly is. Access will then be granted or denied based on the response received from the matched result.

A BIS has advantages that make them suitable for use in places like boarder control and access control. The advantages of a BIS includes: Ease of use, convenience, easier fraud detection and provides high level of security since no two persons have the same biometric pattern [3].

However, a BIS; either a host-based or a network-based are faced with series of security challenges ranging from: Denial of Service (DoS), eaves dropping which makes the intended benefits of a biometric system almost unattainable.

There are series of existing intrusion detection and prevention techniques in the literature. [2] identify two basic categories of intrusion detections. The host-based and network based, depict the point at which each of the intrusion detection systems are applied and what they monitored. Network-based monitors the network traffic and report suspicious activity to the security administrator while a host-based system monitors activity within the host system. Intuitively, an intrusion detection system only detects an anomaly after it has been perpetuated.

2. PROBLEM DESCRIPTION
Biometric system has become a reliable security apparatus for systems where control of access is of highest significance. In the existing biometric identification system domain certain efforts have been made to propose detection techniques using Artificial intelligent based approaches like the neural network and support vector machine. But most of the approaches are for preventing intrusions after it has taken place. In such existing systems, the mostly available preventive approach is to terminate the session automatically or notify the administrator for a necessary action. These methods are highly inappropriate and time consuming (Particularly for a BIS) because once a biometric characteristic is compromised it remains compromised forever. The best way to prevent such attacks or threats is not to allow it to occur in the first instance. Hence, the need for a more reliable preventive approach.

3. SOLUTION STRATEGY
The identified problem is aimed to be solved in this research work by developing an improved framework for intrusion prevention for a host-based Biometric identification system.

4. EXISTING LITERATURE AND RELATED HIGHLIGHTS

[1] Discussed biometric template security and said Biometric recognition offers a reliable solution to the problem of user authentication in identity management systems. But with the widespread deployment of biometric systems in various applications, there are increasing concerns about the security and privacy of biometric technology. He further reiterated that Public acceptance of biometrics technology will depend on the ability of system designers to demonstrate that these systems are robust, have low error rates, and are tamper proof.

[2] Pointed out some of the basic point of attack by intruders in a biometric identification system. In his research, he showed that a Biometric system has some points with high vulnerability rate which is as a result of the use of network system. Thus, because of these facts, the system becomes exposed to some forms of attack ranging from: Eavesdropping, replay attack, spoofing and denial of service. The paper further introduced a neural network based approach based on anomaly detection of intrusion technique. This approach has a machine learning component incorporated, which facilitate learning of the normal way of behaviour of the biometric system, a violation of which constitutes an intrusion. The model was able, to certain degree of accuracy; detect abnormal behaviour and lower false positive rate on the intrusion detection system.

[4] Series of intrusion detection and prevention software were review and their vulnerability assessment. In that the researcher examined symantec host based intrusion detection and prevention system, Jupiter network intrusion and prevention system, internet security network proventia IPS. But in all the software examined the preventive approaches used are either: kill the process action, disconnect the session or disconnect user action. These actions are all taken after an intrusive activity has taken place.

[5] Worked on the enhancement of the fingerprint image where the total pixels that formed the element of the blocks of the M^xN segmented image. The research was able to determine the total completion time of the algorithm.

[6] Another dimension was taken and the proposed enhancement technique deals with only the centre pixel of each of the M*N segmented block of image, instead of the complete pixel in the block, the centre pixel of each of the block was consider. When the research was subjected to similar conditions of hardware and coding it was noted to outperform (in terms of completion time) what [5] proposed.

[8] Confirmed existing algorithms designed for Fingerprint Image Enhancement either lack the ability to enhance poor quality image or are computationally expensive which in most cases makesit easy to be compromised. Evolutionary algorithms are often used to enhance images. Particle Swarm Optimization (PSO) is one of the most progressive algorithms but has parameters, which are not properly tuned to reduce the number of iterations. In this paper, PSO parameters; inertia weight (w) and acceleration constants (c 1 and c 2) were fine-tuned. PSO-based parameterized transformation function, which incorporates both the global and local information of an image, was developed to maximize the information content of the fingerprint image. In the transformation function, a threshold of 0.99 was set to control the contrast effect of the enhanced image. The intensity values of pixels that are less than the threshold were transformed. The image quality was subsequently improved.

5. METHODOLOGY

Based on research conducted by [2] and [7] lot of detection techniques were proposed and developed including the actual points of vulnerability in the biometric identification systems. The issue of prevention of intrusion is still a thing of concern, as, in those works, the prevention techniques were proposed ranging from termination of the session but still inherent in it is still the fact that prevention of intrusion before occurrence is the best prevention approach.

5.1 Description of the Proposed Architecture

The proposed biometric intrusion prevention approach has similar module with a biometric identification system, only that it is emphasis is on prevention approach not on the identification of the intrusive activity alone. The system has the following modules: the user account creation (enrolment module), the sensor module, the administrator's account with their individual levels of permissions. The first module, which is the sensor, captures the biometric trait of the user at the enrolment stage. This trait is used to identify an individual at the verification stage. After the capturing of the biometric trait, the captured template is store in the database which served as a home for the biometric of all the users of the biometric identification system. In this new system, since our concern is on the intrusion prevention approach at both the sensor and feature extraction level, we employed a technique at each level to curb the incidence of intrusion. To do this, at the sensor level, for a sensor to be accepted by the biometric system, it must be enlisted in the sensor database so as to minimize the incidence of poor biometric capturing that give room for vulnerable template.

The architecture of the proposed system is shown on figure A. The sensor, which is the component in charge of biometric data capturing that is used to generate unique data for each of the registered users of the biometric system. The feature extractor is used to extracts the required features of the biometrics that helps to distinguish a biological property of a person from another. The sensor dataset, this is an attached approach that is meant to extract genuine biometric sensor from a fake type. The issue of fake biometric in most instances, are attributed to poor/fake sensor used in capturing trait for template formation. sensors without a clearly registered manufacturer identification number are prone to having feature extraction errors. This database will help to distinguish a standard or internationally approved manufactured biometric device from one that is not approved. Matcher, help in matching the content of the template database with a newly enrolled or verifying template to grant access. While at the template level, with an increasing case of biometric theft, the need for adequate scrutiny of the security of the system becomes paramount. Therefore, in this research the template database will be encrypted so that even with an attempt to delete, modify or update the content of the database, the act becomes impossible.

The next chapter shows the implementation Graphical User Interface (GUI) of the proposed framework that will aid to minimize intrusive attacks on the Biometric Identification System based on the registered sensor concept as proposed in the framework.

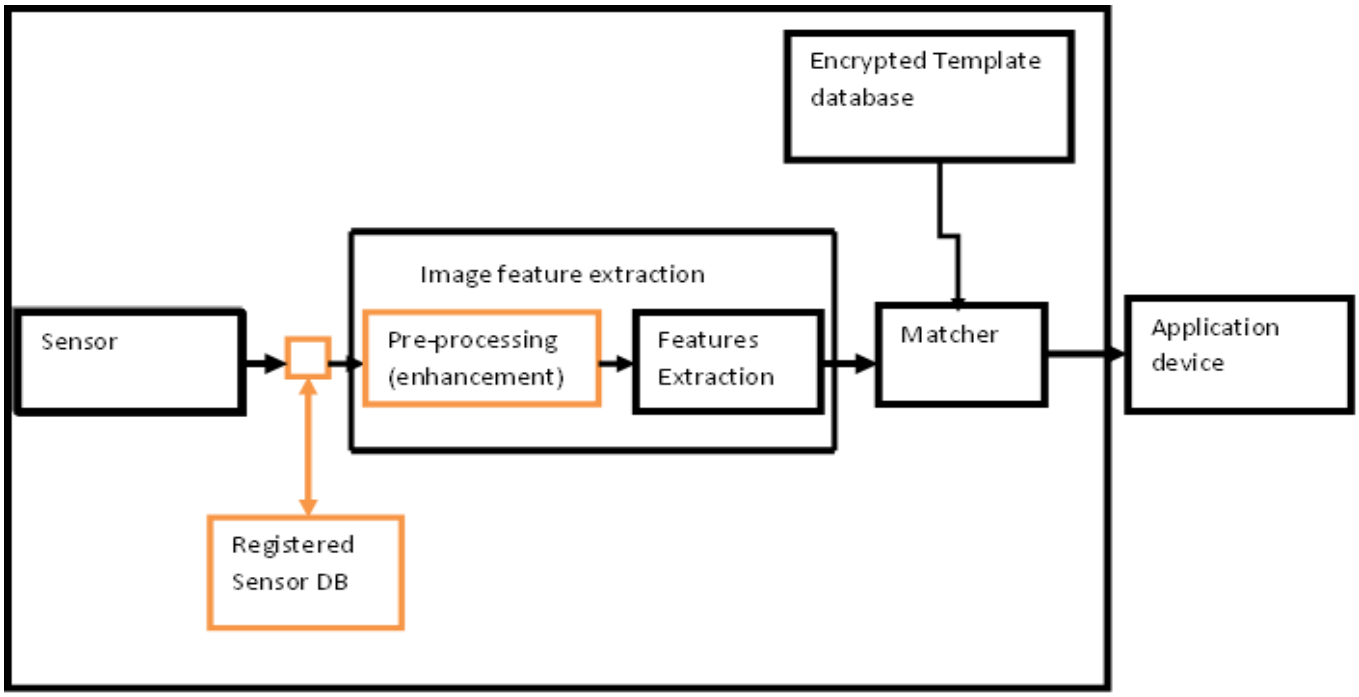

Figure 1: The Improved Framework

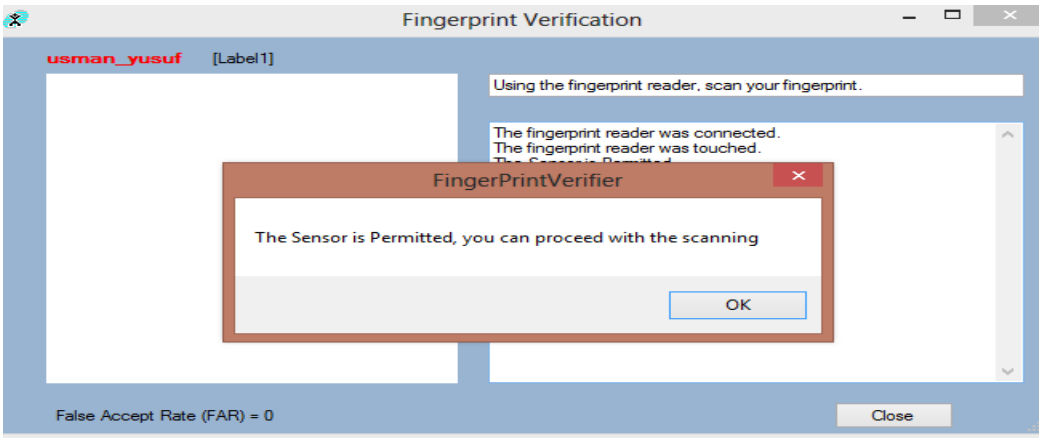

Figure 2: Behaviour of the application when a registered sensor is connected

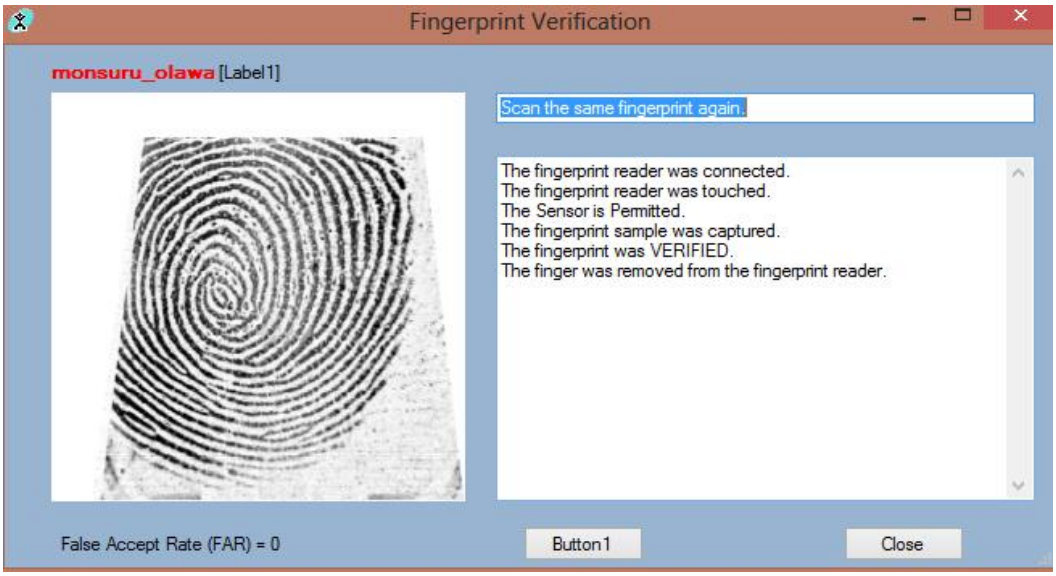

Figure 3: showing system behavior when a registered sensor is used to capture fingerprint image

6. GRAPHICAL USER INTERFACE OF THE IMPLEMENTED IMPROVED FRAMEWORK

The implementation submenu depicts some of the functionalities associated, particularly with users of the biometric system. The system was developed to ensure that anomalies associated with fake sensors that mostly lead to poor image capturing are eliminated by restricting the use of sensor to only certified sensors registered (which was what the framework described) in the BIS database. Figure 2 shows the behavior of the system when a sensor is connected. It shows the status of the connected sensor that will be used for fingerprint image capturing. If the sensor is not registered in the sensor database it will not be permitted for capturing

Figure 3: depicts the behavior of the system if a registered sensor is used to capture an image. It doesn't only capture the image but also shows that the sensor is permitted to capture image which serve as a first line of defense at image capturing level for intrusion prevention

7. ALGORITHM FOR ENROLMENT AND VERICATION PROCESS

7.1 Enrolment Process

Start

Step 1 Attach sensor

Step 2 Verify sensor from the date base if in the database move to step 3 else contact administrator.

Step 3 Captures image of the user

Step 4 Pre-process the image using proposed the algorithm.

Step 5 Extract the features of the fingerprint image

Step 6 Store the extracted features into the template database.

Stop

7.2 Verification

Start

Step 1 Attach sensor to the system

Step 2 Verify if sensor is already registered into the sensor database. If yes proceed to step 3, else contact administrator

Step 3 Pre-process the image & extract its features.

Step 4 Compare the extracted features with the contact of the template database. If the matched comparison is above the threshold then step 5, else step 6

Step 5 Grant access to facility

Step 6 Deny access to facility

Stop

8. CONCLUSION

This research work has shown to reasonable level of conviction that an improvement in the architecture of the existing biometric system can actually improve on the preventive approach to biometric system intrusion. In section 5.1, an architectural view is presented to depict the position of the additional structure to the existing system which will help to minimize the case of use of uncertified sensors that might lead to poor fingerprint image capturing. It will be appropriate to further the research by investigating on the liveness of the fingerprint tha is to be captured so that even if the of a legal user who is no longer alive or has left the system cannot be used to bye-pass the provided security feature a BIS is intended to provide.

Further work can also be done on the feature extraction unit to incorporate other machine approaches to image enhancement and better encrypting algorithm for the template database.

9. ACKNOWLEDGEMENT

Our profound gratitude goes to all those that went through this work and constructively criticize it to attain this level of perfection.

10. REFERENCES

[1] Jain, A. K., Ross, A, and Prabhakar, S. 2004. An Introduction to Biometric Recognition. IEEE Transaction on Circuits and Systems for Video Technology, 14(1), 4–20.

[2] Mgabile, T., Msiza, I. S, and Dube, E. 2012. Anomaly based intrusion detection for Biometric Identification System Using neural Network. International Conference on Artificial Intelligent and Image Processing. Dubai, (December, 2012).

[3] Ioannis M , Yves P., Sabine D., Elsa L., Carlos R., Martin U, and Marcelino C. 2013. European Union: Biometric at the frontier.

[4] Jain, B. 2005. Intrusion Prevention and Vulnerability Assessment in Sachet intrusion detection. Masters Thesis. Department of Computer Science and Engineering. Indian Institue of Technology, Kanpur.

[5] Raymond, T. 2003. Fingerprint Image Enhancement and Minutiae Extraction. Unpublished Phd thesis submitted to School of Computer Science and Software Engineering. University of Western Australia.

[6] Babatunde, I. G., Charles, A.O., and Olatubosun, O. 2012. A mathematical modeling method for fingerprint ridge segmentation and normalization. International Journal of Computer Science and Information Technology & Security, 2(2), 263-267.

[7] Arjunwadkar, M., and Kulkarni, R.V. 2010. The rule based intrusion detection and prevention model for biometric systems. Journal of Emerging Trends in Computing and Information Science, 1(2), 117-120.

[8] Abdullahi M. B., Fati I. and Mohammed A. A. 2016. Performance analysis of particle swarm optimization algorithm-based parameter tuning for fingerprint image enhancement. Futures Technologies Conference. IEEE transaction. Pg: 528-536.