GLOBAL JOURNAL OF PURE AND APPLIED SCIENCES VOL. 18, NO. 1&2, 2012: 59-66

 ISSN 1118-0579
www.globaljournalseries.com, Email: info@globaljournalseries.com

APPLICATION OF HYBRID HASH MESSAGE AUTHENTICATION CODE APPROACH IN BIOMETRICS INFORMATION SYSTEM DESIGN

ENANGHA EYAM ABENG AND W. ADEBISI ADESOLA

(Received 15 September 2011; Revision Accepted 12 March 2012)

ABSTRACT

The Design and Implementation of a Biometric System for Nigerian Prisons Service (NPS) using Calabar Prisons as case study has been carried out. The system allows users (prison inmates) to be enrolled so that their biometric fingerprint trait is captured and encrypted using Hash Massage Authentication Code (HMAC) technique modeled via cryptographic hash algorithms. The unique corresponding HMAC of the user generated can then be stored in either the application database or in a smart memory card (smart card) for future usage and referencing.

KEYWORDS: Biometrics, fingerprint minutiae, Hash message Authentication code, encryption, Decryption.

1.0 INTRODUCTION

Biometrics refers to the automatic identification of a person based on his/her anatomical (e.g., fingerprint, iris) or behavioral (e.g., signature) characteristics or traits. This method of identification offers several advantages over traditional methods involving identity (ID) cards (tokens) or personal identification numbers (passwords) for various reasons: (i) the person to be identified is not required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. By replacing PINs (or using biometrics in addition to PINs), biometric techniques can potentially help to prevent unauthorized access to Automated Teller Machines (ATMs), cellular phones, laptops, and computer networks. Unlike biometric traits, PINs or passwords may be forgotten, and credentials like passports and driver's licenses may be forged, stolen, or lost. As a result of all these problems, biometric systems are being deployed to enhance security and reduce financial fraud via the embedded biometric traits which are being used for real-time recognition, the most popular being face, iris and fingerprint.

There are essentially two kinds of biometric systems -Manual system based on the old ink and paper method of biometric acquisition and authentication. This system can easily be manipulated and is very vulnerable to attacks. The old ink and paper method of biometric acquisition and authentication can easily wear and tear within a short period of time making room for data and records constantly been manipulated and distorted which greatly affects effective decision making .Thus, the vulnerability /complete absent of automated fingerprint identification system gives room for mistaken identity /identity swap (but no two persons can have the same biometric data) as evidenced in (Agbi vs. Ogbeh ,2003),(James Ibori vs. Great Ogboro,2003) , (James Ibori vs. the state,2003) and (Aluko Mobolaji,2003).

Automated Biometric System is an electronic version of the manual biometric system. This is based on the old ink and paper method of biometric acquisition and authentication. The Automated biometric system is operated by professionals for the purpose of identifying an individual or a criminal of a crime according to trails left on the crime scene; this is because biometric information relies on “something that you are” to make a personal identification and therefore can inherently differentiate between authorized person and a fraudulent impostor (Shoniregun, 2007).The administrators of the automated identification systems do not have any reason to manipulate the system used by the end users for any negative purpose such as access right or illegally gain of unauthorized privilege since each individual possesses unique biometric traits. Hence, biometric technology is used as a form of identity access management and access control. According to (Jain, 2007), it can be used to identify or verify individuals in groups which are placed under surveillance purpose and this will assist in the detail tracking and monitoring of all their activities. Biometric traits are sensitive data which are universal, unique, permance and is digitally collectable, reducible and acceptable in terms of speed and performance and need to be adequately protected to eliminate data distortation and manipulation by impostors. In this study, we enhanced security of the biometric traits collected from individuals (prison inmates) via the use of a cryptographic hash functions algorithms to encrypt the captured fingerprint minutiae through the fingerprint reader. Fingerprint recognition algorithms are used to analyze fingerprint minutiae point, ridge structure and image density in order to identify an individual (Simon-Zorita et al, 2001) as each individual fingerprint minutiae differs according to the bifurcrum and ridge ending patterns. Furthermore, fingerprint biometric authentication is the most sophisticated method of all biometric technologies which have been thoroughly verified through various applications and has proved its reliability and efficiency in criminal investigations for more than a century (Abeng, 2010).This makes fingerprint authentication the most acceptable form of biometric technology.

In this study, we employed the hybrid Hash Message Authentication Code (HMAC) technique to verify data integrity, authenticity and repudiation of the

Enangha Eyam Abeng, Department of computer Science, Cross River University of Technology, Calabar, Nigeria.
W. Adebisi Adesola, Department of Computer Science, Cross River University of Technology, Calabar, Nigeria.

encrypted biometric traits image.

2.0. Problem Definition

Unfortunately, in spite of the security strength and uniqueness of fingerprint biometrics technology in protecting sensitive information; it is at its lowest level of application in some key institutions in Nigeria especially the Nigerian Prisons Service (NPS) where this technology is very important.

Secondly, this vulnerability or complete absent of automated fingerprint identification system mechanism in our prisons has led to the case of mistaken identity / identity swap as seen in the case between James Ibori Vs. the State, February 2003 and in some many other cases.

Furthermore, the existing system used in our case is too localized and this enables a jail breaker from any part of Nigeria to migrate freely to another part of the country with the claim of a free citizen since he cannot be easily tracked and monitored. We therefore, proposed a system that can tackle these challenges

3.0 Significance of the Study

The major significance of this study is the need to check intrusion and jumping of prison by inmates either via identity swap or mistaken identity.

4.0. Methodology

4.1 Component of the Model

The model for this study follows the following process.

i. The Enrollment /Capturing of fingerprint
ii. The Recognition/Authentication of the fingerprint
iii. Determine the process

- Enrollment - An individual places his finger on the sensor/scanner to captures the fingerprint. The fingerprint is then analyzed with an algorithm that extracts quantifiable features fingerprint minutiae. The Biometric enrollment is depicted below.

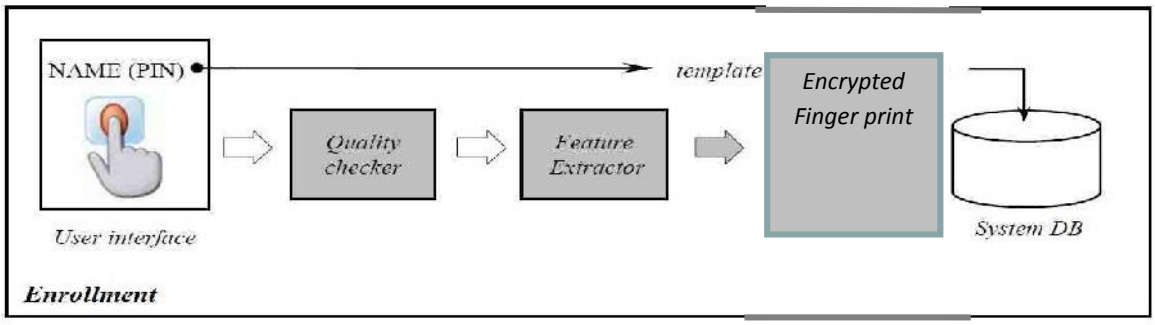


Figure 1: Shows the biometric Enrollment

- Authentication - where a one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. It can be done in conjunction with a smart card, username or ID number. The Automated Fingerprint Identification System compares the input fingerprint image and previously registered data to determine the genuinesses of the captured fingerprint minutia.

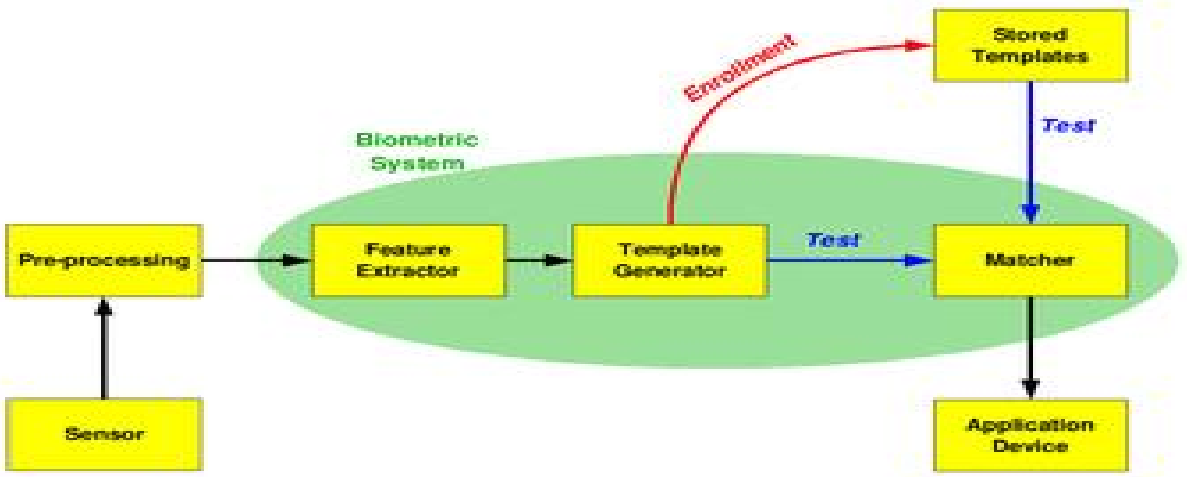
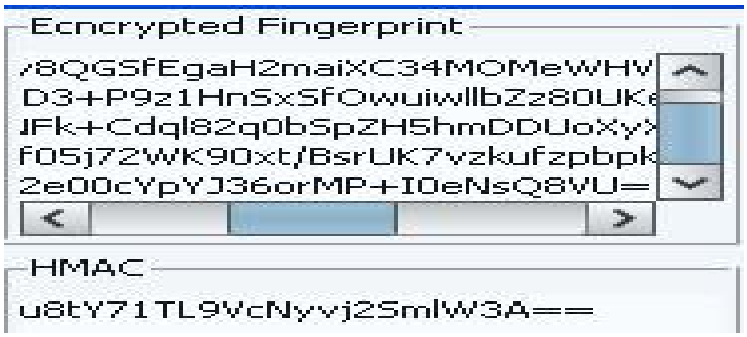


Figure 2: Shows the Authentication processes.

- **Determine the process**

The Algorithm used in the design is as below.
Step 1 - An Individual places his finger on the fingerprint scanner to capture the fingerprint minutiae.
Step 2 - The fingerprint minutiae is now extracted and the quality enhanced via the removal of dirt.
Step 3 - The extracted fingerprint minutiae is hashed.
Step 4 - The hashed fingerprint is encrypted and the HMAC code generated.
Step 5 - The encrypted fingerprint and HMAC code is stored in the system database.



Step 6 – Authenticate User fingerprint.
If user found
Open enrollee Registration form
And Register enrollee,Grant Access,
Else
Go to Step 5
Stop 7 – Stop.

5.0. Types of attacks on Biometric Information

There are diverse trends on the various ways of biometric attacks in the present global society (Chander, Ranjender & Shectal, 2008). They include:

i. **Circumventive:** An Impostor may gain access to the system protected by biometrics and peruse sensitive data such as medical records pertaining to a legitimately enrolled user. Besides violating the privacy of the enrolled user, the imposter can also modify sensitive data.

ii. **Repudiation:** A legitimate user application and the facilities offered by an application and then claim that an intruder had circumvented the system. For instance, a bank clerk may modify the financial records of a customer and then deny responsibility by claiming that an intruder stolen her biometric data.

iii. **Covert Acquisition:** An impostor may secretly obtain the raw biometric data of a user to access the system. For example, the latent fingerprints of a user may be lifted from an object by an intruder and later used to construct a digital or physical artifact of that user's fingerprint.

iv. **Collusion:** An Individual with wide super-user privileges (such as administrator) may deliberately modify system parameters to permit incursions by an intruder. (4)

v. **Coercion:** An imposter may force a legitimate user (e.g. at gunpoint) to grant him access to the system.

6.0. The Proposed Biometric System for Nigerian Prison Service.

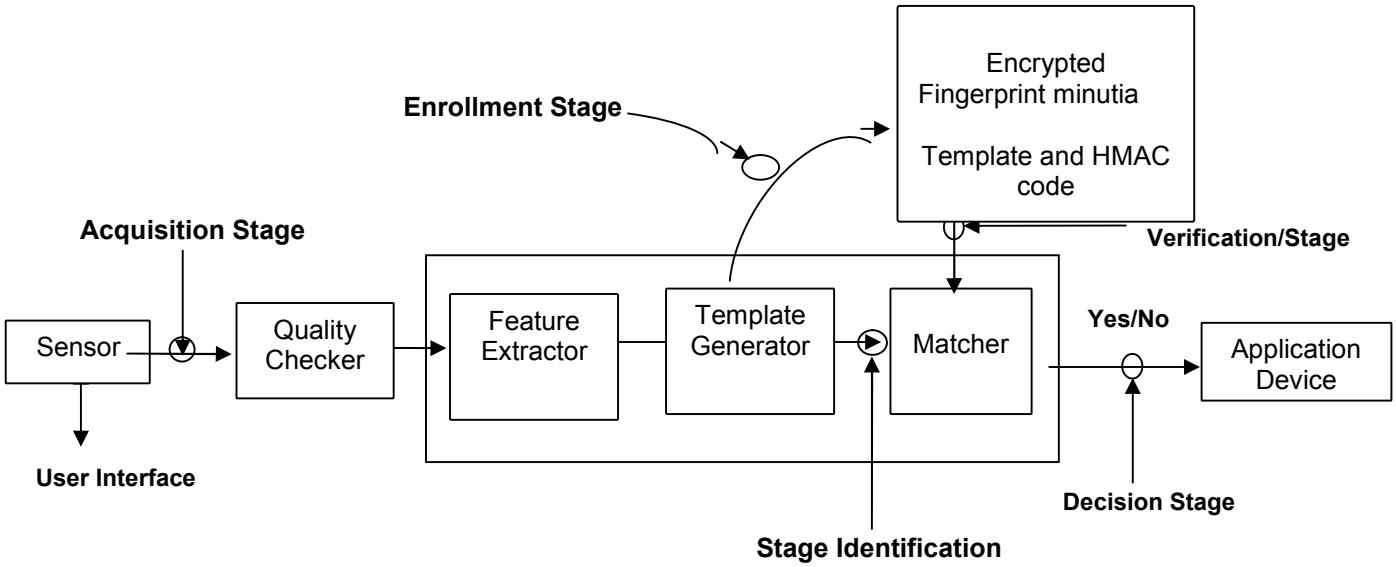


Figure 3: shows the structural framework modules of the proposed system

The proposed biometric system for Nigerian Prisons Services comprises of several modules. The sensor module acquires the raw biometric data of the person in the form of an image. The quality checker module pre-processed the captured biometric trait.

The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal. During user enrollment, the extracted feature set, labeled with the user's identity is encrypted and store in the biometric system called the template with its corresponding HMAC code that is generated. The HMAC code is to further enhance security of the biometric feature extracted (Ross et al, 2003).

The matcher module compares the feature set extracted during authentication with the enrolled template(s) and generates match scores.

The decision modules processes these match scores in order to either determine or verify the identity of an individual.

Hence, this biometric system has several layers of protection which ensures that the system is reliable, efficient, user friendly and very robust.

7.0. How to apply Cryptographic Hash Function in Biometric

The cryptographic hash functions used are SHA-1, MD5 and DES which withstand cryptanalytic attacks. This Cryptographic algorithms uses sequence to encipher and decipher messages and data in a cryptographic system. Hash functions are not reversible. The hash function process encrypted biometric trait into fixed length output.

8.0. Developing the application

This application is developed using development tools and software such as Java Language Enterprise Edition and Java Database. The experiments were conducted using Microsoft Fingerprint Reader in capturing the fingerprint minutia and a combination of cryptographic Algorithms, Hash message Authentication code (HMAC), message Digest version 5 (MD5), secure hash algorithm version 1 (SHA-1) and Data Encryption Standard (DES) were used in the encryption of the fingerprint and the generation of the HMAC Code for each individual that is being enrolled. The digitalized encrypted fingerprint minutia template is stored in the system database for future references and usage. However, the fingerprint reader does not run on windows 7.

9.0. Program Implementation

To use the application from your PC system, Lunch the Secure Prison management system. The first screen which comes up is the Administrator access page. The Primary Information required is the Authentication of the administrator via username and password. If the information supplied is correct, the page opens and it leads us to the user interface page.

Figure 4: Picture of Admin login

On the Admin Login page, you will see the login and exit highlighted on the screen. (The code for this Admin login page is inside the container). When the user clicks on the login button, it loads the whole package but if the user clicked on the exit button, it unloads the whole package.

The Admin login Dialog module prevents unauthorized users from using the package: Security. The system administrator has the ability to change and administer access code to any user.

Figure 5: Picture of system Admin Module

User Interface Page

Haven gained access to the user interface page; the user can navigate the inmate profile, case file, and Route activities and visitors record.

Figure 6: Picture of the user interface

The user interface consists of three menus: the file, view and category.

The file menu consists of the close and exit submenus. When a user click on the close submenu, the package closes while if a user click on the exit submenu, the package will be exited. The view menu have four submenus namely inmates, cases, visits and activity. Below are the screen shots.

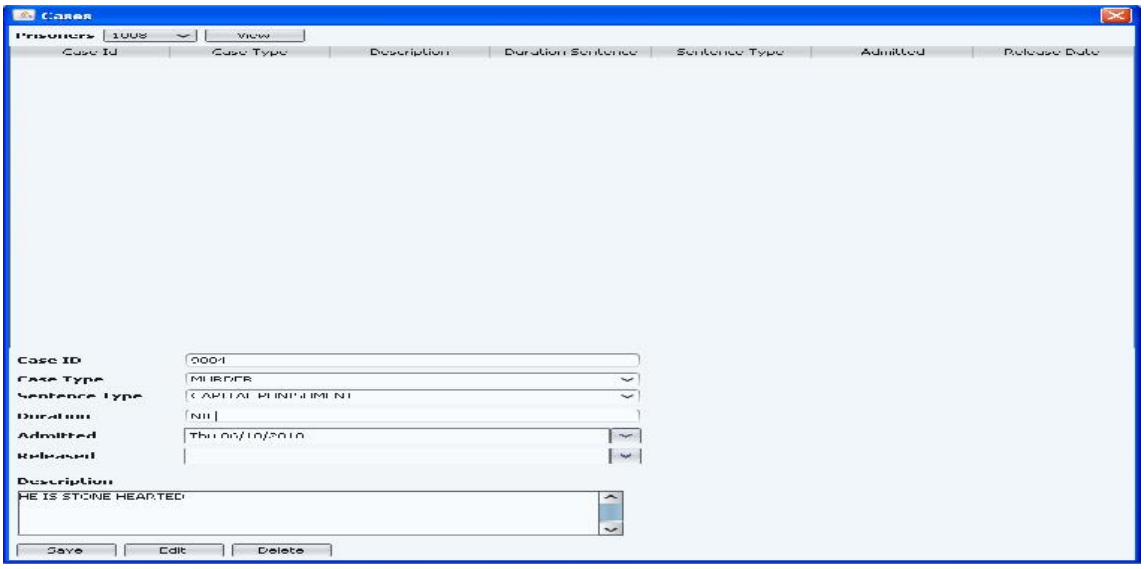


Figure 7: Picture of inmate's cases

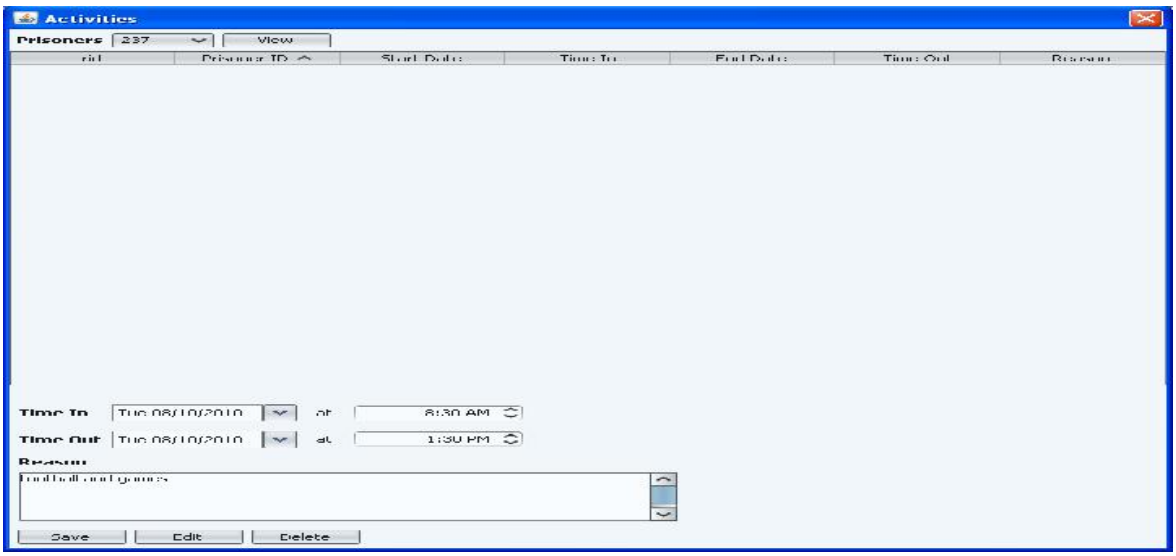


Figure 8: Picture of inmates Activities

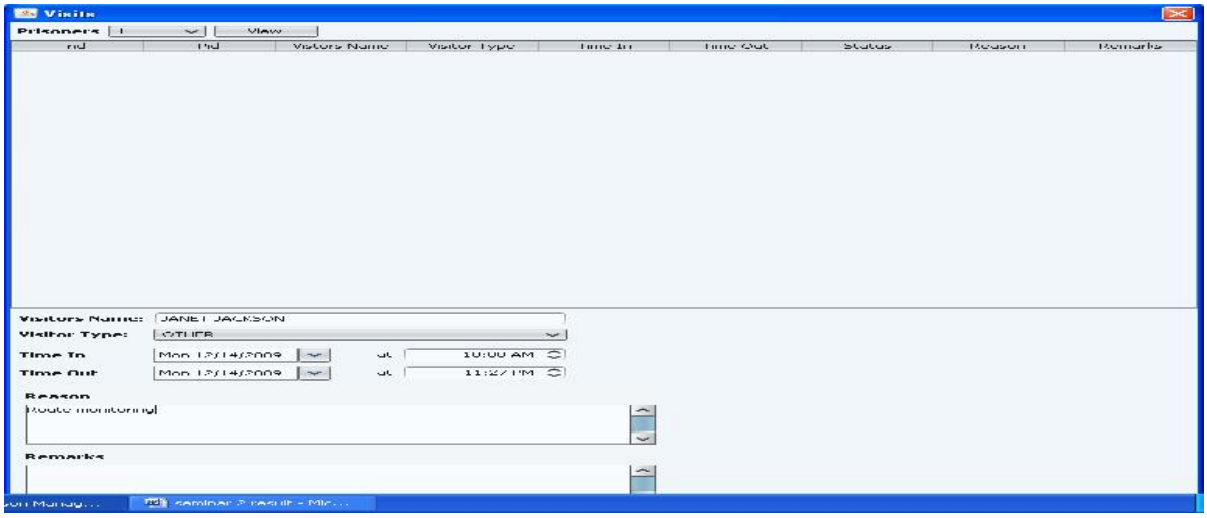


Figure 9: Picture of inmates Visits

The options menu has only users' submenu and accounts sub-sub menu. The Accounts submenu enables the Administrator via the options menu to create a new user and also delete and existing user and most especially determined a user level of access of the system.

Inmate Fingerprint Capturing

At the inmate's submenu profile, some basic information are obtained and the inmate fingerprint minutiae is captured through Microsoft fingerprint reader.

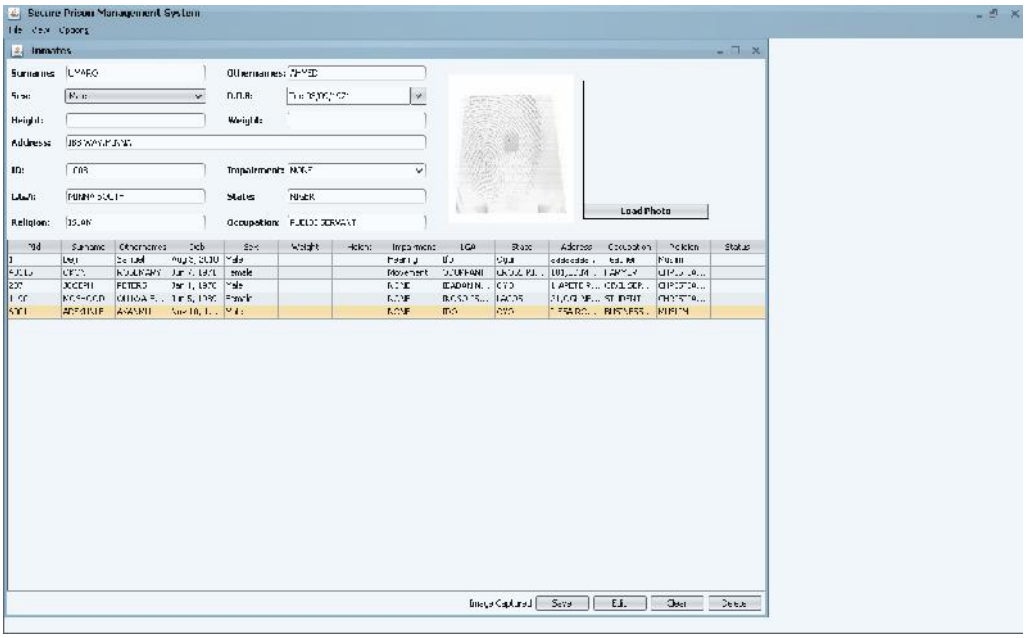


Figure 10: Picture of inmates profile and minutiae captured.

Below is the fingerprint minutiae been encrypted and its corresponding HMAC code in Figure 14.

Figure 11: Picture of Encrypted fingerprint and HMAC generated.

10.0. CONCLUSION

The primary focus of this work is the automation of the old ink and paper method of biometrics identification processes used by the Nigerian Prisons Services. The fingerprint minutiae is encrypted and hashed before storing in the system database for future references and usage in making sensitive decisions by Law enforcement agencies making it difficult for an impostor to circumvent the embedded security. This automated system is more enhanced durable, secured, reliable, fast and highly user friendly. It is our belief that if properly

implemented as proposed here, it will go a long way in removing the bottlenecks inherent in manual processing and provide a better and broader information security, availability, accessibility, and advanced tools to manage all type of biometric information (Adesola, 2006).We have discussed various types of attacks that can be launched against a biometric system. We discuss the importance of encryption and hashing principles to enhance the integrity and security of biometric template. Biometric cryptosystems can contribute to template security by supporting biometric matching in securing cryptographic domains. Also, smart cards are gaining popularity as the medium for storing biometric templates (portability).As the amount of available memory increases there is a tendency to store more information in the template. This increases the risks associated with template misuse. As a result, we recommend further research on this work via its implementation on the internet (online) to assert its vulnerability to cyber attacks. The result will broader our horizon in understanding the uniqueness of encrypting and hashing fingerprint biometric trait in managing sensitive information.

REFERENCES

Abeng, E. E., 2010. “A hybrid Hash message Authentication code (HMAC)” for authenticating and validating Biometrics Information. (A case study of the Nigerian Prison Service Calabar Prison). An unpublished M.Sc Dissertation, University of Ibadan.

Adesola, W. A., 2006. “Design and Implementation of a web based Information System for National health Insurance Scheme Using the Object Relational Database Approach”, An Unpublished M.Sc thesis University of Portharcourt.

Biometrics Fingerprint Technology- http://omin.com/fp.fphistory.html.

Chander, K., Ranjender, N and Shectal, C., 2008. “Biometrics Security using steganography”.ISSN 1985-2320, Malashiya, 2, (1): 1-5. Jan. 2008. Fingerprint-www.wkipdia.com

International Biometric Group, Biometric market Report 2000 – 2005; 2001.

Jain, A. K., Flynn, P and Ross, A., 2007. “Handbook of Biometrics”, Springer. 2007.

Jain, A. K., 2007. “Biometric recognition: Q x A”, Nature, 449, 38-40. sept. 6, 2007.

Jain, A. K., Hong, L and Pankanti, S., 2000. “Biometric Identification”, Comm. ACM, 43, (2): 90-98, February 2000.

Ross, A., Jain, A and Reisman, J., 2003. “A hybrid fingerprint matcher”. Pattern Recognition 36, 7 (July 2003), PP.1661 – 1673.

Shoniregun, C. A., 2007. “The future of internet security”, 2007.

Simon-Zorita, D., Ortega-Garcia, J., Cruz-Liamas, S and Gonzale-Rodraguez, J., 2001. “Minutiae Extraction scheme for fingerprint Recognition system”. In proceeding of the International conference on Image processing (October 2001), 3, 204-257.

http:llen.wikipedia.org/wiki/ fingerprint

http:www.asaba.com The 1995. Ibori ex-convict case Revisited, 2003.

Aluko, M., 2003. ”The strange case of Governor James Onanefe Ibori” This Day, Sunday, March 16,2003.