DESIGN OF PATTERN RECOGNITION SYSTEM FOR FINGERPRINT IDENTIFICATION AND VERIFICATION: AN AUTOMATED FINGERPRINT DIGITAL TIME BOOK APPLICATION

ISSN: 2141 – 3290

UMOH, U. A. AND NYOHO, E. E.
Department of Computer Science,
University of Uyo, Nigeria.

ABSTRACT: Fingerprint recognition refers to the automated method for verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics use to identify individual and verify their identity. Fingerprint verification is one of the most reliable personal identification methods and it plays an important role in forensic applications like fraud and criminal investigations, terrorist identification and National security issues. The popular biometric used to authenticate a person is fingerprint which is unique and permanent throughout a person's life. Some fingerprint identification algorithm include; Fast Fourier Transform (FFT), Minutiae Extraction etc. A minutia matching is widely used for fingerprint recognition and can be classified as a ridge ending and ridge bifurcation. This paper presents the implementation of automated fingerprint signer using the JRFinger API, JMF, Java programming language java SDK and Netbeans IDE. The system is capable of acquiring, extracting, storing and matching of fingerprint, to identify a staff. The fingerprint digital time book "automatically" answers the question – when and what time did I report to work? Hence staff need not manually sign the time book. Just a fingerprint will do it all, thereby eliminating the act of signing with an incorrect time, signing for friends or backdating, etc.

INTRODUCTION

Fingerprints are imprints formed by friction ridges of the skin and thumbs. Fingerprint-based personal identification is an important biometric technique with many current and emerging applications.It has long been used for identification because of their high acceptability, immutability and individuality. Fingerprint identification is one of the well known biometrics. Because of their uniqueness and consistency over a century, they have more recently becoming automated due to advancement in computing technologies. They are popular because of inherent ease in acquisition and sources available for collection. The probability that two fingerprints are alike is about 1 in 1.9 x 10^{15}. These features make the use of fingerprints extremely effective in areas where the provision of a high degree of security is an issue. The major steps involved in automated fingerprint recognition include; fingerprint acquisition, fingerprint segmentation, fingerprint image enhancement, feature extraction, minutiae matching and fingerprint classification, (Afsar, *et. al.* 2004; Fronthaler, *et. al*;. 2008, Girgisa, *et. al*; 2007, and Gu, *et. al;* 2006).

The fingerprint patterns recognition system using Huffman Coding has been proposed by Aburas, *et. al.* (2008). It uses vector which generated from Huffman coding compression process. Therefore, the matching process is done between code (vector) and codes (vectors) and the database is sharply decreased. The obtained results are considerably promising since very low FAR i.e. 0.733%, FRR i.e. 2.6% and high accuracy i.e. approximately 97%. However, the weakness of the system comes from the point of different captured environments for the images.

Fingerprint identification in biometric security systems (Hong, and Jain, 1998) deals with the issue of selection of an optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy. Fingerprint recognition using Minutia Score Matching Method (FRMSM) has also been proposed. (Lourde and Khosla, 2010). For Fingerprint thinning, the Block Filter is used, which scans the image at the boundary to preserves the quality of the image and extract the minutiae from the thinned image. The false matching ratio is better compared to the existing algorithm.

Similarity of identical twin fingerprints has been investigated, Tao, et. al. (2012). The study tested identical twin fingerprint database that contains 83 twin pairs, 4 fingers per individual and six impressions per finger: 3984 (83*2*4*6) images. Thai and Tam (2010) has also shown Fingerprint recognition technique based on wavelet based texture pattern recognition method. In view of the fingerprint recognition method; based on Fast Fourier Transform (FFT) and Minutiae Extraction, the proposed wavelet based technique results in high recognition rates.
.

Fingerprint recognition using standardized fingerprint model has been proposed by Sonavane, and Sawant (2007). The work discussed the Standardized Fingerprint Model used to synthesize the template of fingerprints, In their model, after pre-processing step, transformation between templates, adjust parameters, synthesize fingerprint, and reduce noises are found. Then final fingerprint are used to match with others in FVC2004 fingerprint database (DB4) to show the capability of the model. Study on noisy fingerprint image enhancement technique for image analysis using a structure similarity measure approach has also been documented, (Negi, and Sharma, 2009).

This paper presents the implementation of automated fingerprint signer using the JRFinger API, JMF, and java programming language. The system is capable of acquiring, extracting, storing and matching of fingerprint, to identify a staff. The fingerprint digital time book system proposed in the work can "automatically" answer the question – when and what time did I report to work? Hence staff need not manually sign the time book. Just a fingerprint will do it all, thereby eliminating the act of signing with an incorrect time, signing for friends or backdating.

Fingerprint Identification and Verification

According to Afsar, *et. al.* (2004), the major steps involved in automated fingerprint recognition include i) Fingerprint Acquisition, ii) Fingerprint Segmentation, iii) Fingerprint Image Enhancement, iv) Feature Extraction v) Minutiae Matching, vi) Fingerprint Classification (Fig. 1).

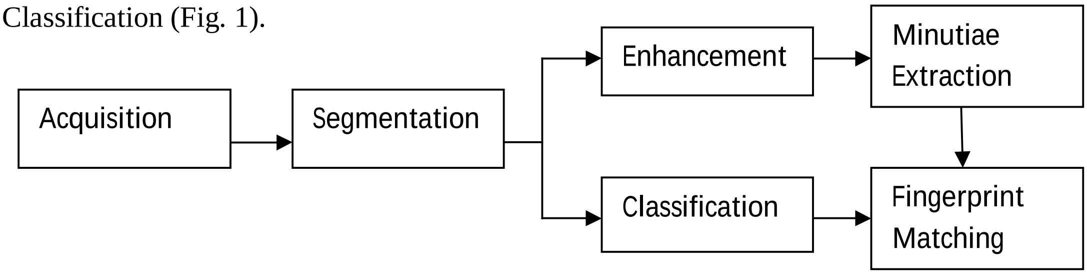


Figure 1: Steps involved in Automated Fingerprint recognition

i. Acquisition: We can have either offline (inked) or online (live scan) fingerprint acquisition. In the offline method an imprint of an inked finger is first obtained on a paper, which is then scanned. This method usually produces images of very poor quality because of the non-uniform spread of ink and is therefore not exercised in online AFIS. Optical fingerprint scanner such as URU 4000 is employed for online fingerprint image acquisition. This device makes use of Frustrated Total Internal Reflection (FTIR), ultrasound total internal reflection, sensing of differential capacitance, and non contact 3D scanning methods for image development. Live scan scanners give superior reliability during matching as compared to inked fingerprints, (Afsar, *et.al.*, 2004).

ii. **Fingerprint Segmentation:** Fingerprint segmentation plays an important role in a fingerprint identification and verification system. An algorithm that works well in the extraction of the required region but computational cost is very high, (Verma, and Goel, 2011). An efficient algorithm that works with acceptable performance and has a lower computational cost is has been developed by Afsar, *et.al.*, (2004). This algorithm is based only on the block coherence of an image, giving a measure of how well the gradients of the fingerprint image are pointing in the same direction. In a window of size *WxW* around a pixel, the coherence is defined as:

$$Coh = \frac{\left|\sum_{W}(G_{s,x}, G_{s,y})\right|}{\sum_{W}\left|(G_{s,x}, G_{s,y})\right|} = \frac{\sqrt{(G_{xx} - G_{yy})^2 + 4G_{xy}^2}}{G_{xx} + G_{yy}} \qquad (1)$$

$$G_{xy} = \sum_{h=-8}^{h=+8}\sum_{k=-8}^{k=+8} G_x(x_i + h, y_j + k) \cdot G_y(x_i + h, y_j + k),$$

$$G_{xx} = \sum_{h=-8}^{h=+8}\sum_{k=-8}^{k=+8} G_x(x_i + h, y_j + k)^2,$$

$$G_{yy} = \sum_{h=-8}^{h=+8}\sum_{k=-8}^{k=+8} G_y(x_i + h, y_j + k)^2$$

Where *Gx* and *Gy* are the local gradients along X and Y directions respectively.

Gaussian smoothing filter is explored to smooth the resulting gradient coherence image, giving a coherence image *C(x, y)*. The smoothed image is then binarized resulting in a segmentation mask *CB*. The binarization is performed by global threshold as;

$$C_B(i, j) = \begin{cases} 1 & C(i, j) > M_c - 0.5S_c \\ 0 & Otherwise \end{cases} \qquad (2)$$

Where, *Mc* is the global mean of the coherence image and *Sc* is its global standard deviation.

iii. **Fingerprint Enhancement:** The fingerprint enhancement algorithm is mentioned in Hong and Jain (1998). Better results were obtained using Yang and Fan, (2003) but it is slightly more time consuming. This algorithm calls for the development of a ridge frequency image IRF and ridge orientation IRO image for a fingerprint. Gabor filters are used to enhance the fingerprint utilizing the ridge frequency and ridge orientation information obtained from the frequency and orientation images. The enhanced image IE is then binarized using adaptive threshold to give a binarized image IEB. The binarized image is thinned to give IT and the thinned version is used for minutiae extraction.

iv. **Minutiae Extraction:** Cross number approach of minutiae extraction, where crossing number of pixel '*p*' is defined as half the sum of the differences between pairs of adjacent pixels defining the 8-neighborhood of '*p*'. This is given as,

$$cn(p) = \frac{1}{2}\sum_{i=1..8}\left|val(p_{i\bmod 8}) - val(p_{i-1})\right| \qquad (3)$$

Where *p0* to *p7* are the pixels belonging to an ordered sequence of pixels defining the 8-neighborhood of *p* and *val (p)* is the pixel value. One of the main difficulties in the minutiae-based approach is that it is very difficult to reliably extract minutiae in a poor quality fingerprint image. The simplest correlation-based technique is to align the two fingerprint images and subtract the input image from the template image to see if the ridges correspond (Lourde and Khosla, 2010).

v. **Minutiae Matching:** In this step, matching is based on a simple computation of the Euclidean distance between the two corresponding feature vectors, and hence is extremely fast (Lourde and Khosla, 2010). According to Afsar, *et.al.*, (2004), let T and I be the representation of the template and input fingerprint, respectively. The minutiae sets of the two fingerprints are assumed to be:

$$T = \{m_1, m_2, \ldots, m_m\} \qquad m_i = \{x_i, y_i, \theta_i\}, i = 1..m$$
$$I = \{m'_1, m'_2, \ldots, m'_n\} \qquad m'_j = \{x'_j, y'_j, \theta'_j\}, j = 1..n$$

When the spatial and orientation differences are within specified thresholds, *ro* and θ *o*, a minutia *mj'* in I and a minutia *mi* in *T* match. Minutia matching is carried out by first registering using a derivative of the Hough transform followed by fingerprint matching using spatial and orientation-based distance computation. The matching algorithm returns a percentage match score, which is then used to take the match-no match decision based on the security criterion.

vi. **Fingerprint Classification:** Fingerprint classification is done by the extracting singular points from the fingerprint image and rule-based classification is performed, Afsar, et.al., (2004).

System Design

We employ UML design tools and notations in the development of our model. UML graphically depicts object-oriented analysis and design models. It is a language for specifying, visualizing and constructing the artifacts of software systems, as well as for business modeling. It shows the interactions and relationships between its different classes and components.

Figure 2 shows the architecture of the system. Figure 3 shows the overall flow of the proposed system. Figure 4 presents the main entities for the database and their attributes. The designed database structure has four logical subdivisions. These are user personal information, enrolment information and authentication information and system. Each subdivision has its unique tables and relations. We adapt and modify the model of Tao, *et. al.*, (2012) (Fig. 5). Figure 5 shows the digital fingerprint-based verification and identification time book model. It depicts; user enrollment, user verification and user identification.

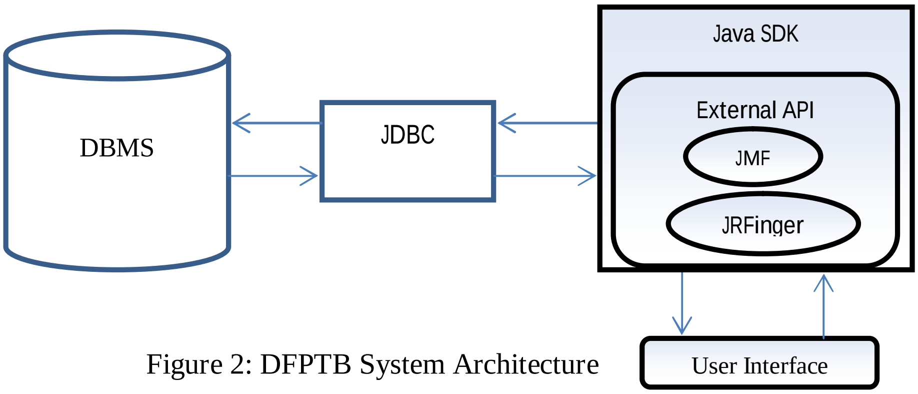


Figure 2: DFPTB System Architecture

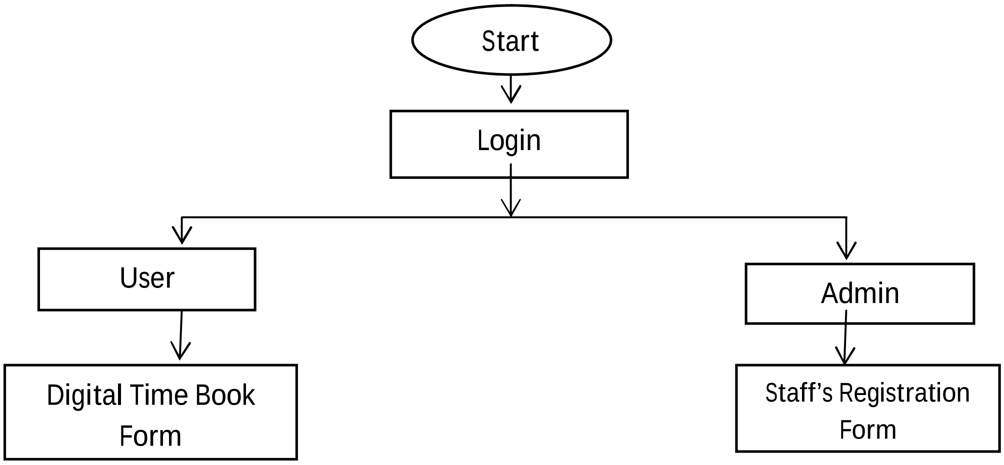


Figure 3: DFPTB System Diagram

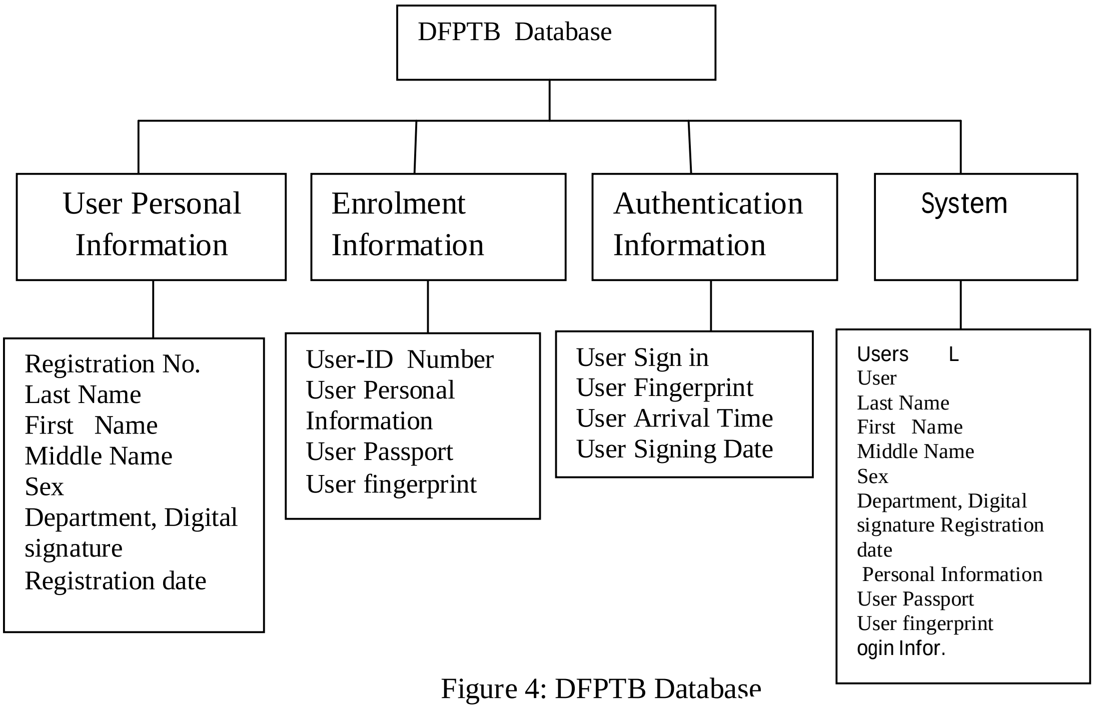


Figure 4: DFPTB Database

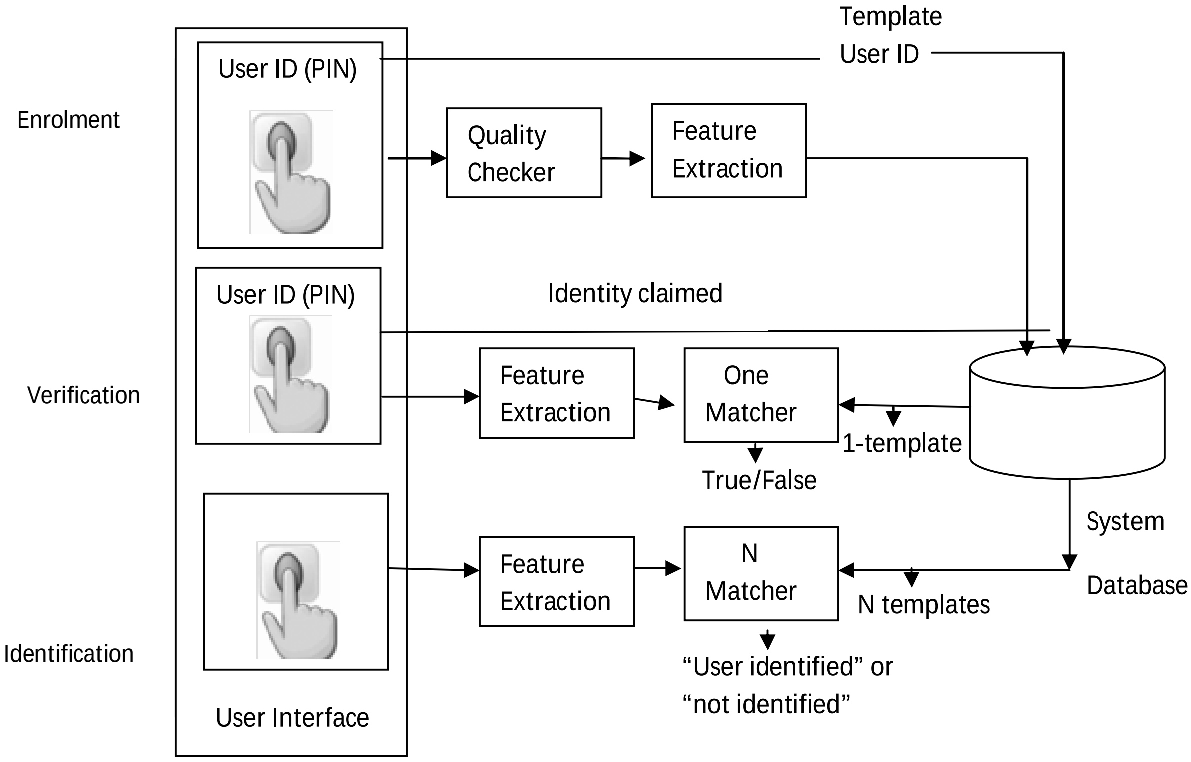


Figure 5: Digital Fingerprint-based Time book Model

System Implementation

The model is developed using the java SDK, Netbeans IDE, an external API – JRFinger and the JMF (Java Media Framework). We also used Microsoft Access 2010 as database management system for the creation and management of our database. The components of the fingerprint digital time book include; Fingerprint database, Enrolment module, Authentication module, It also consists of the following forms; Splash screen, Login form, User registration form, User time book form and Log reader.

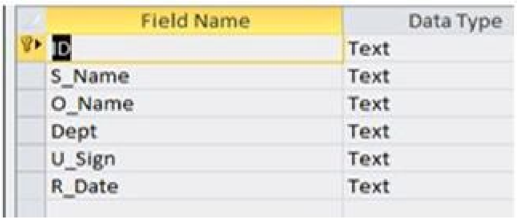
The fingerprint database stores the fingerprint templates along with the staff's ID. This refers to the structure of the database file used in the implementation of the system. It consists of the structure of the table, the number of the records, the name of the attributes and the value of the attributes. The tables used by the system comprises; UserInfo Table, Enrol Table

The UserInfo table (Table 1) stores the staff information during registration. This information includes the Surname, Other Names, Department, Digital signature (a pseudo randomly generated alphanumeric set), and registration date. This information will be referenced during authentication. Enrolment table (Table 2) is used to store the fingerprint template together with an ID number. The relationship between the UserInfo and the enrol table is the "ID".

The enrollment module is responsible for registering individuals in the biometric system database (system DB). During the enrollment phase, the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the raw digital representation is usually further processed by a feature ex-tractor to generate a compact but expressive representation, called a *template*. Enrolment module, this is where user registration takes place. The enrolment module takes as input the staff's personal information, the staff's passport, and the staff's fingerprint. These data are kept in the database which are later be used to identify a staff each time He comes to work.

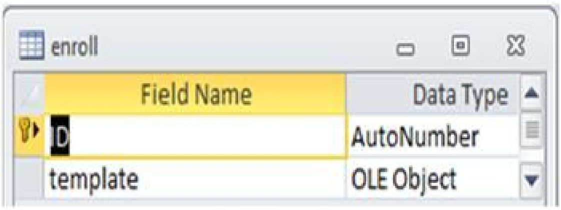
The verification task is responsible for verifying individuals at the point of access. During the operation phase, the user's name or PIN (Personal Identification Number) is entered through a keyboard; the biometric reader captures the fingerprint of the individual to be recognized and converts it to a digital format, which is further processed by the feature extractor to produce a compact digital representation. The resulting representation is fed to the feature matcher, which compares it against the template of a single user (retrieved from the system DB based on the user's PIN).

In the identification task, no PIN is provided and the system compares the representation of the input biometric against the templates of all the users in the system database; the output is either the identity of an enrolled user or an alert message such as "user not identified." Authentication module allows a staffs to "sign in" when they report to work. Upon fingerprinting, the system automatically inserts other necessary details including the staff's arrival time.



Field Name	Data Type
ID	Text
S_Name	Text
O_Name	Text
Dept	Text
U_Sign	Text
R_Date	Text

Table 1: The UserInfo Table



Field Name	Data Type
ID	AutoNumber
template	OLE Object

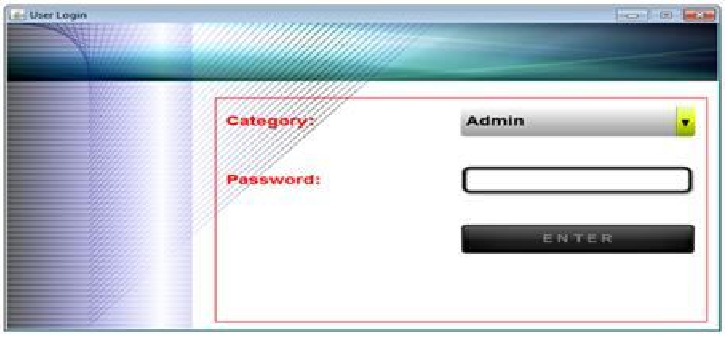
Table 2: The Enrol Table

Screen Short of the System

Figure 6 presents the splash form whicht introduces the fingerprint digital time book syetm and also loads the neccesary files used by the software such as the backgrounds. Figure 7 shows the user login form which allows a staff to login either as an Admin or a User. If an admin category is selected the form requests a compulsory password. The user category is used for staff "sign in" while the admin is used for registration. Figure 8 presents the User digital signature registration form. Before a staff is recognized by the fingerprint digital time book during "sign in", the staff needs to register first. Hence the fingerprint digital time book user registration form collects the necessary staff data including the staff picture and fingerprint image. The fingerprint template is then extracted from the image and stored in a database for future identification as presented in Figure 9. The two forms that take care of the staff registration. The user time book form presents the most effective and easiest way of signing a time book as shown in Figure 10. The fingerprint digital time book uses this form to automate the process of time book signing by staff. Instead of filing ones name, date and other information on paper, the fingerprint digital time book is signed simply by fingerprinting, which as a result automate the process of signing. Figure 11 presents the Log reader form. When a staff signs the time book using the form in Figure 10, the fingerprint digital time book verifies the fingerprint of the staff, if a match is found the system extracts some personal information associated with this fingerprint and also inserts automatically other neccesary information such as the time and date of signing. This helps to eliminate signing incorrect time by the staff (faking of time). These personal information together with the automatically inserted information are saved to a file log file. The essence of keeping the log of staff "sign in" is such that it will be used to track who comes to work and when. The log reader is displayed in an uneditable text area.

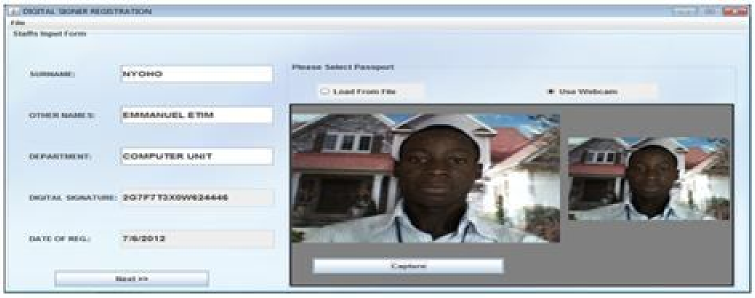
Fingerprint Digital Time Book
By
Dr.(Mrs.) U.A Umoh
& Nyoho, Emmanuel Etim

Figure 6: Splash Screen of the System



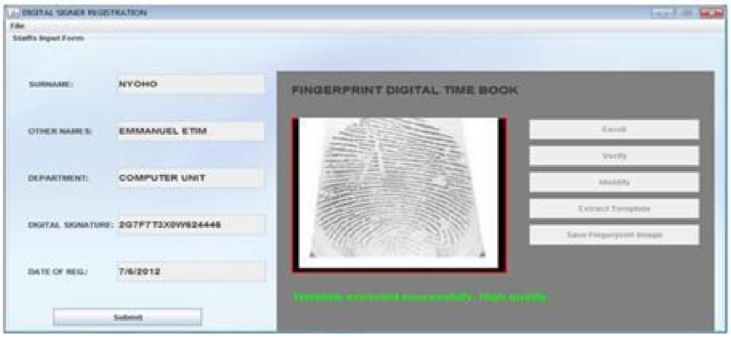
Category: Admin
Password:

Figure 7: The user login form



SURNAME: NYOHO
OTHER NAMES: EMMANUEL ETIM
DEPARTMENT: COMPUTER UNIT
DIGITAL SIGNATURE: 2G7F7T3X0W624446
DATE OF REG.: 7/6/2012
Please Select Passport
○ Load From File ● Use Webcam

Figure 8: Digital Signer Registration Form



SURNAME: NYOHO

OTHER NAMES: EMMANUEL ETIM

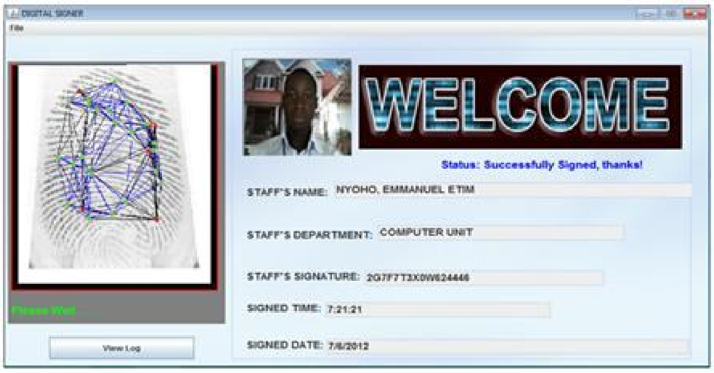
DEPARTMENT: COMPUTER UNIT

DIGITAL SIGNATURE: 2G7F7T3X0W624446

DATE OF REG.: 7/6/2012

Template extracted successfully, High quality

Figure 9: User Digital Fingerprint Template Extract Form



Status: Successfully Signed, thanks!

STAFF'S NAME: NYOHO, EMMANUEL ETIM

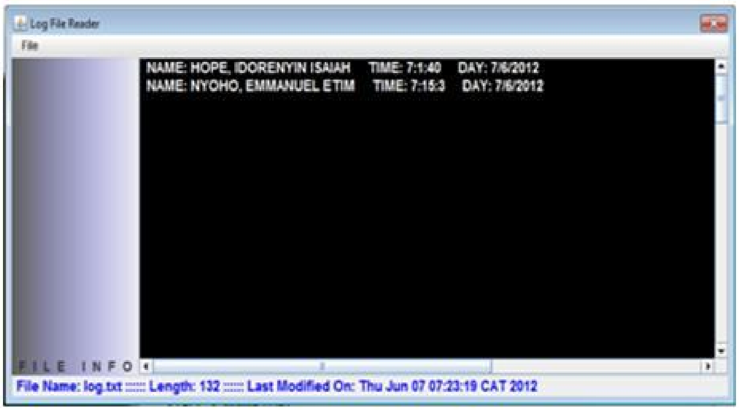
STAFF'S DEPARTMENT: COMPUTER UNIT

STAFF'S SIGNATURE: 2G7F7T3X0W624446

SIGNED TIME: 7:21:21

SIGNED DATE: 7/6/2012

Figure 10: The Digital Signer Time Book form



```
NAME: HOPE, IDORENYIN ISAIAH    TIME: 7:1:40    DAY: 7/6/2012
NAME: NYOHO, EMMANUEL ETIM    TIME: 7:15:3    DAY: 7/6/2012
```

File Name: log.txt :::::: Length: 132 :::::: Last Modified On: Thu Jun 07 07:23:19 CAT 2012

Figure 11: The Log reader

CONCLUSION

The fingerprint is one of the popular biometric methods used to authenticate human being. In this paper, we propose a fingerprint digital time book system to provide a reliable and better tool for an organization to keep track of when the staff reports to work. The fingerprint digital time book model uses the fingerprint template extracted from the image and the user time book form to automate the process of time book signing by staff. Instead of filing ones name, date and other information on paper, the fingerprint digital time book is signed simply by fingerprinting, which as a result automate the process of signing. The system is implemented with the java codes, two java APIs (JRFinger & JMF) and Microsoft Access as our database tool. The model is capable of acquiring, extracting, storing and matching of fingerprint, to identify a staff and the time a he reports to work. The fingerprint digital time book "automatically" answers the question – when and what time did I report for work? This system helps to eliminate manually signing of time book by staff in an organization which is prone to errors, like, signing incorrect time, signing time for one another. Because identification in large databases is computationally expensive, classification and indexing techniques are recommended to limit the number of templates that have to be matched against the input.

REFERENCES

Aburas, A. A. and Rehiel, S. A., (2008). Fingerprint patterns recognition system using Huffman Coding. *Proceedings of the World Congress on Engineering,* 3: 1794-1796.

Afsar, F. A., Arif, M. and Hussain, M., (2004). *Fingerprint Identification and Verification System Using Minutiae Matching. National Conference on Emerging Technologies,* pp. 140-146.

Fronthaler, H., Kollreider, K. and Bigun, J. (2008) "Local Features for Enhancement and Minutiae Extraction in Fingerprints", *IEEE Transactions on Image Processing*, 17 (3): 354- 363.

Girgisa, M. A., Sewisyb A. A. and Mansourc, R. F. (2007) "Employing Generic Algorithms for Precise Fingerprint Matching Based on Line Extraction*", Graphics, Vision and Image Procession Journal*, 7, 51-59.

Gu, J., Zhou, J. and Yang, C., (2006), "Fingerprint Recognition by Combining Global Structure and Local Cues*", IEEE Transactions on Image Processing,* 15(7), 1952 – 1964 .

Hong, Wan and Jain, (1998): *Fingerprint Image Enhancement: Algorithm and Performance Evaluation*, IEEE Transaction on Pattern Analysis and Machine Intelligence.

Lourde R, M. and Khosla, D. (2010): Fingerprint Identification in biometric security systems. *International Journal of Computer and Electrical Engineering,* 2 (5): 1793-8163

Tao, X., Chen, X., Yang,X., Tian, J., (2012): *Fingerprint Recognition with Identical Twin Fingerprints*. PLoS ONE 7(4): e35704. doi:10.1371/journal.pone.0035704

Thai, L. H. and Tam, H. N (2010), Fingerprint recognition using standardized fingerprint model. *International Journal of Computer Science Issues* (IJSCSI) 7(3).

Sonavane, R. and Sawant, B. S. (2007) "Noisy Fingerprint Image Enhancement Technique for Image Analysis: A Structure Similarity Measure Approach", *Journal of Computer Science and Network Security*, 7 (9): 225-230.

Negi, B. and Sharma, V. (2009), Fingerprint Recognition System. International Journal of Electronics and Computer Science Engineering.3, 872-878

Verma, R. and Goel, A. (2011), Wavelet application in fingerprint recognition. *International Journal of Soft Computing and Engineering* (IJSCE). 1 (4): 129-134.

Yang, Liu, Jiang and Fan, (2003): *A Modified Gabor Filter Design Method For Fingerprint Image Enhancement*, Elsevier Pattern Recognition Letters.