DEVELOPMENT OF A REAL TIME FINGERPRINT AUTHENTICATION/ IDENTIFICATION SYSTEM FOR STUDENTS' RECORD

O. Y. Ogundepo[1,*], I. O. A. Omeiza[2] and M. A. Akpojaro[3]

[1, 3,] DEPT. OF ELECTRICAL & ELECTRONICS ENGR., UNIVERSITY OF PETROLEUM RESOURCES, EFFURUN, DELTA STATE, NIGERIA
[2,] DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING, UNIVERSITY OF ILORIN, KWARA STATE, NIGERIA
E-mail addresses: [1] *yinkdare@gmail.com,* [2] *isaacavazi@unilorin.edu.ng,* [3] *mccurtisakpojaro@gmail.com*

ABSTRACT
Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. This paper presents the development of a real time fingerprint authentication system built as an application of an optical fingerprint scanner ("SecuGen") and its free software developers' kit (SDK). To achieve good minutiae extraction in fingerprints with varying quality, Gabor filter was designed and incorporated for image enhancement. The matching algorithm used in the SecuGen's SDK is capable of finding the correspondences between input minutia pattern and the stored template minutia pattern without resorting to exhaustive search. Gabor filter is used to enhance the unique features of the fingerprint before these features are compared for authentication and recognition of a person. The result shows the improvement in accuracy level of the fingerprint authentication system when the enhanced (filtered) image is used as compared to when a noisy image is used.

***Keywords**: Biometrics; Fingerprint Recognition; Gabor filters; Fingerprint Authentication/Verification; Fingerprint Identification*

1. INTRODUCTION
Biometrics is the most widely used area which helps in the identification and verification of a person based on his physiological and behavioral characteristics. The most common and accepted biometric system is the fingerprint recognition system [1]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip [2]. Fingerprints are unique across individuals and even identical twins having similar DNA, are believed to have different fingerprint [3]. The uniqueness of a fingerprint can be determined by the overall pattern of ridges and valleys as well as the local ridge anomalies [4]. Fingerprint identification is commonly employed in forensic science to support criminal investigations and in biometric systems, such as civilian and commercial identification devices. Hence, there is a widespread use of fingerprints [5]. Fingerprint recognition is being widely applied for personal identification with the purpose of high degree of security [6] by matching processes between two human fingerprints. However, some fingerprint images captured in variant

applications are poor in quality, which corrupted the accuracy of fingerprint recognition [7]. A fingerprint recognition system is essentially a pattern recognition system that can be deployed in two different modes: (1) verification and (2) identification. Verification refers to authenticating the claimed identity of a user, while identification refers to establishing the identity of a user. Identification (one-to-N matching) is inherently a more difficult pattern recognition problem as it involves an N-class classification problem, where N is the number of users enrolled in the system. Verification (one-to-one matching) is a relatively easier problem that can be formulated as a simple two class hypothesis testing problem (accept or reject). The pattern matching consists of two stages: Authentication and Verification. For enrollment, the fingerprint of the user is captured and the extracted features are stored in the database. Then during authentication, the fingerprint of the user is taken again by the scanner and the extracted features are compared with the ones already stored in the database to determine a match.

* **Corresponding author, tel: +234 – 706 – 709 – 2282**

The user is accepted or rejected depending on if his or her record could be fetched from the database. In the case of identification, fingerprints of unknown individuals (search prints) are compared with fingerprints of individuals with known identities (reference prints) in order to positively determine the identity of the unknown individual. In the case of verification, one or more fingerprints of an individual (query prints) are compared with fingerprints of the person on file whose identity is claimed by the individual submitting the query prints, in order to verify the claim of identity.

In an ideal fingerprint image, ridges and valleys alternate and flow in a locally constant direction and minutiae are anomalies of ridges, that is, ridge endings and ridge bifurcations. In such situations, the ridges can be easily detected and minutiae can be precisely located from a binary ridge map. For automatic fingerprint identification, only the two most prominent local ridge characteristics, ridge ending and ridge bifurcation (called minutiae), are widely used. A ridge ending indicates the location where a ridge ends abruptly. A ridge bifurcation indicates a location where a ridge forks or diverges into branch ridges.

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. A Gabor filter oriented in a particular direction gives a strong response for locations of the target images that have structures in this given direction. Gabor filter is structured in such a way that it can take care of different shapes, sizes and smoothness levels in the image. This paper addresses Fingerprint authentication using Gabor filter for the enhancement process of fingerprint image quality with acceptable performance.

2. RELATED WORK

This section presents the work done by other researchers related to Fingerprint Recognition Techniques. In this section, description about all reference papers are summarized.

Wang, *et al.* [8] proposed a real time fingerprint recognition system based on novel fingerprint matching strategy. In this paper they present a real time fingerprint recognition system based on a novel fingerprint minutiae matching algorithm. The system

is comprised of fingerprint enhancement and quality control, fingerprint feature extraction, fingerprint matching using a novel matching algorithm, and connection with other identification system. Here they describe a way to design a more reliable and fast fingerprint recognition system which is based on today's embedded systems in which small area fingerprint sensors are used.

Shunshan *et al.* [9] presented an Image Enhancement Method for Fingerprint Recognition System. In their proposed technique a refined Gabor filter, is presented. This enhancement method can connect the ridge breaks, ensures the maximal gray values located at the ridge center and has the ability to compensate for nonlinear deformations. It includes ridge orientation estimation, a Gabor filter processing and a refined Gabor filter processing. The first Gabor filter reduces the noise, provides more accurate distance between two ridges for the next filter and gets a rough ridge orientation map while the refined Gabor filter with the adjustment parameters significantly enhances the ridge, connects the ridge breaks and ensures the maximal gray values of the image being located at the ridge center. In addition, the algorithm has the ability to compensate for nonlinear deformations. Furthermore, this method does not result in any spurious ridge structure, which avoids undesired side effects for the subsequent processing and provides a reliable fingerprint image processing for Fingerprint Recognition System. A refined Gabor filter was applied in fingerprint image processing, then a good quality fingerprint image was achieved, and the performance of the Fingerprint Recognition System has been improved.

Mil'shtein *et al.* [10] proposed a fingerprint recognition algorithm for partial and full fingerprints. In this study, they propose two new algorithms. The first algorithm, called the Spaced Frequency Transformation Algorithm (SFTA), is based on taking the Fast Fourier Transform of the images. The second algorithm, called the Live Scan Algorithm (LSA), was developed to compare partial fingerprints and reduce the time taken to compare full fingerprints. A combination of SFTA and LSA provides a very efficient recognition technique. The most notable advantages of these algorithms are the high accuracy in the case of partial fingerprints. At this time, the major drawback of developed algorithms is lack of pre-classification of examined fingers. Thus, they use minutiae classification scheme to reduce the

reference base for given tested finger. When the reference base had shrunk, they apply the LSA and SFTA.

Manvjeet, *et al.* [11] proposed a fingerprint verification system using minutiae extraction technique. Most fingerprint recognition techniques are based on minutiae matching and have been well studied. However, this technology still suffers from problems associated with the handling of poor quality impressions. One problem besetting fingerprint matching is distortion. Distortion changes both geometric position and orientation, and leads to difficulties in establishing a match among multiple impressions acquired from the same fingertip.

Anil *et al.* [12] proposed Pores and Ridges: Fingerprint Matching Using Level 3 Features. Fingerprint friction ridge details are generally described in a hierarchical order at three levels, namely, Level 1 (pattern), Level 2 (minutiae points) and Level 3 (pores and ridge shape). Although high resolution sensors (~1000dpi) have become commercially available and have made it possible to reliably extract Level 3 features, most Automated Fingerprint Identification Systems (AFIS) employ only Level 1 and Level 2 features. As a result, increasing the scan resolution does not provide any matching performance improvement [13]. They develop a matcher that utilizes Level 3 features, including pores and ridge contours, for 1000dpi fingerprint matching.

3. DESIGN METHODOLOGY

This chapter presents an overview of the system design. In this phase, the design adapted was broken down into core functional blocks to simplify its development thereby allowing a more in-depth study of the system as a whole. This is often called the Input to output approach. The functional blocks are:

- Image acquisition
- Preprocessing
- Feature extraction
- Pattern matching

Based on established specifications, a block diagram was drawn through analytical modelling of the system to generate and evaluate concepts for the execution and interfacing of the functional blocks. Figure 1, shows the block diagram of a real time fingerprint authentication system.

3.1 Fingerprint Image Acquisiton

Image acquisition is the first step in this approach. Based on the mode of acquisition, a fingerprint image may be classified as off-line or live-scan. An off-line image is typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on paper. A live-scan image, on the other hand, is acquired by sensing the tip of the finger directly, using a sensor (scanner) that is capable of digitizing the fingerprint on contact. Live-scan is done using sensors like optical sensor (fingerprint scanner). Fingerprint scanner captures a digital image of the fingerprint.

Secugen hamster plus is the life scanner used in this work. It is a USB 2.0 optical fingerprint scanner that comes with free software developer kits (SDK) that can be tailored by the user for building leading-edge biometric applications. It is designed to capture fingerprint with a size of 260x300pixels at a resolution of 500 dot per inch (DPI).

3.2 Precesses Involed in Fingerprint Recognition

Fingerprint images contain unnecessary information such as scars, moist or areas devoid of valuable ridges and furrows, and in order to eliminate the redundant information from the useful information, a pre-processing stage is usually required.
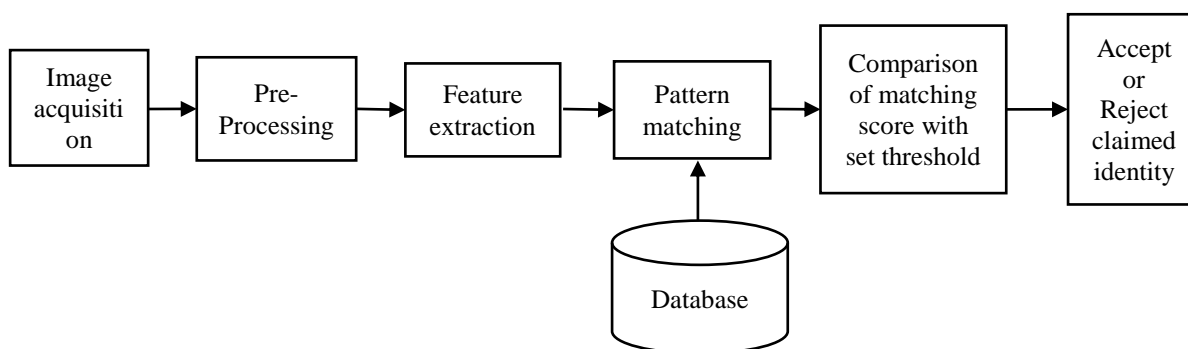

Figure 1: Real time fingerprint authentication block diagram

In fingerprint recognition, the quality of the directional image used is very essential. Therefore, enhancement algorithms are used to adaptively improve the clarity of ridge and valley structures based on the local ridge orientation and ridge frequency. They also identify the unrecoverable corrupted regions in an input fingerprint image and mask them out, which is a very important property because such unrecoverable regions do appear in some of the corrupted fingerprint images and they are extremely harmful to minutiae extraction. The accuracy of ridge direction ensures successful fingerprint image enhancement. A two-dimensional Gabor filter (a frequency and orientation selective filter) can be used to enhance the quality of the fingerprint image. Fingerprint matching refers to finding the similarity between two given fingerprint images. The choice of the matching algorithm depends on which fingerprint representation is being used. Feature extraction refers to the extraction of the fingerprint discriminating features (minutiae). The features extracted are then used for matching. Currently the most widely used and the most accurate automatic fingerprint identification techniques use minutiae-based automatic fingerprint matching algorithms. Reliably extracting minutiae from the input fingerprint images is critical to fingerprint matching. On the final analysis the level of similarity between two fingerprints is expressed in terms of a matching score which is given by [24]

$$MS(q,r) = \frac{m^r \times m^r}{n_r^b \times n_q^b} \qquad (1)$$

Where m^r is the number of matched minutiae points, n_r^b is the total number of points in the query print and n_q^b is the total number of minutiae in the reference print.

3.1.2 Gabor Filter
A Gabor filter has been known as a very useful tool in image processing, pattern recognition, computer vision, and machine learning especially for texture analysis, due to its optimal localization properties in both spatial and frequency domain; it was named after Dennis Gabor. A two-dimensional Gabor filter is a linear filter whose impulse response is represented as a complex sinusoidal   signal modulated by a Gaussian function and can be described as follows [14 − 18]:

$$G(x,y,\varphi) = \frac{1}{2\pi\sigma_x\sigma_y}exp\left(-\frac{1}{2}\left(\frac{X^2}{\sigma_x{}^2}+\frac{Y^2}{\sigma_y{}^2}\right)+j(2\pi fX+\varphi)\right)$$
$$= g^r(x,y)+jg^i(x,y) \qquad (2)$$
$$X = x.\cos\theta + y.\sin\theta \;\; and \;\; Y = -x.\sin\theta + y.\cos\theta. \quad (3)$$

Where $g^r(x,y)$ is the real component and $g^i(x,y)$ is the imaginary component of complex Gabor filter; j is the imaginary line number, σ_x and σ_y are the scaling parameters of the Gaussians envelopes along x-axis and y-axis respectively and describe the neighborhood of the pixel where weighted summation takes place, f denotes the central frequency of the complex sinusoid and $\theta \in [0,\pi]$ is the orientation of the normal to the parallel stripes of the Gabor function and its Fourier transform is given as

$$G(u,v) = Aexp\left\{-\frac{1}{2}\left[\frac{(u-F)^2}{\sigma^2{}_u}+\frac{v^2}{\sigma^2{}_v}\right]\right\} \qquad (4)$$

Comparing the real Gabor filter with other filters, including Gaussian steerable filters and the complex Gabor filters, the real Gabor filters produce the best performance in terms of ability to detect the presence of oriented features as well as in terms of accuracy in the estimation of the angles of orientation [19]. The real Gabor kernel, $g^r(x,y)$, oriented at 0^c radians, corresponding to the real component of the function in equation 1, is:

$$g^r(x,y) = \frac{1}{2\pi\sigma_x\sigma_y}exp\left(-\frac{1}{2}\left(\frac{X^2}{\sigma_x{}^2}+\frac{Y^2}{\sigma_y{}^2}\right)\right)\cos(2\pi fx) \quad (5)$$

The Fourier transform of the Gabor filter defines its frequency domain representation and specifies the modulation of each frequency component of the input image. As $g^r(x,y)$ is real and even, the corresponding Fourier transform is also real [20] given as:

$$g_r(u,v) = exp\left\{-\frac{1}{2}\left[\frac{(u-u_0)^2}{\sigma^2{}_u}+\frac{v^2}{\sigma^2{}_v}\right]\right\}$$
$$\times exp\left\{-\frac{1}{2}\left[\frac{(u+u_0)^2}{\sigma^2{}_u}+\frac{v^2}{\sigma^2{}_v}\right]\right\} \quad (6)$$

Where $\sigma_u = \frac{1}{(2\pi\sigma_x)}$ and $\sigma_v = \frac{1}{(2\pi\sigma_y)}$. The values of σ_x and σ_y determines the extent of the filters in x and y direction respectively, which can be linked by the elongation parameter L. The thickness parameter τ, controls the scale of the filter.

The parameters in equation (1), can be derived from the following design rules:

$$\sigma_y = L\sigma_x \qquad (7)$$
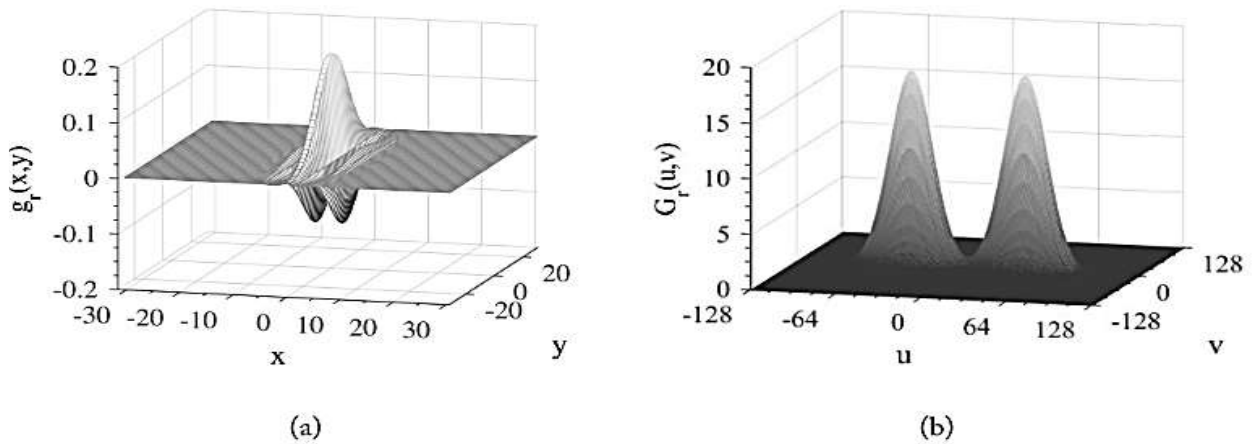$$\sigma_x = \tau/(2\sqrt{2ln2}) \; = \tau/2.35 \qquad (8)$$
$$f = 1/\tau \qquad (9)$$

Figure 2: (a) Real Gabor kernel oriented at 0^0 radians, with τ = 6 pixels and L = 4 and (b) the corresponding frequency representation [19].

Figure 2a and b. shows a spatial representation of the real Gabor filter with image resolution of 128 x 128, oriented at 0^c radians, with thickness parameter τ = 6 pixels and elongation parameter L = 4 Fig. 2b, is the Fourier transform of the above filter. Gabor filter act as a local bandpass filter. A specific bank of Gabor filters contain multiple individual Gabor filters adjusted with different parameters (scale, orientation and central frequency).

Using the Gabor filter an enhanced image E can be obtained through spatial convolution using following equation [23]:

$$E(i,j) = \sum_{u=-w/2}^{w/2} \sum_{v=-w/2}^{w/2} h\big(u,v: O(i,j), F(i,j)\big) \times G(i-u, j-v) \qquad (10)$$

Where h is the Gabor filter kernel, u and v kernel coordinates, O(i, j) and F(i, j) is the orientation and frequency at image points (i, j) respectively while G is the normalized image and w is the Gabor filter size.

3.3   Proposed System
The proposed system specification is as follows
- Enable the administrator and other authorized user to register
- Enable the administrator to store data on the database
- Enhancement of fingerprint using Gabor filter and feature extraction after enhancement
- Generating of result for verification and authentication

Figure 3 shows the proposed systems overall architecture in form of a block diagram. The system provide for (four) possible usage scenarios, namely:

(1) Registration of a candidate;
(2) Viewing the details of a candidate's records in the database;
(3) Verification of a candidate's claimed identity;
(4) Identification of a candidate based on is fingerprint.

3.6.1 System Flowchart
Registration module: It opens a form requiring details from the user/student. After imputing the required details, an image capturing sensor is used to acquire the raw biometric data of the person by clicking "capture" while the finger is placed on the sensor. Figure 4 shows the registration flow chart

Authentication/Verification module: It opens a page that performs pattern matching through either verification or authentication. The verification employs a one to one comparison. This means that it retrieves the student previously stored fingerprint from the database and the user/student places his/her finger on the sensor to capture his/her biometric data which is compared with the retrieved data to produce a matching result. This is preferable and faster. Figure 5 shows the flow chart for authentication module.

Identification module: Identification module accepts as input a candidate's fingerprint without a claimed identity and proceeds to find a fingerprint in the database that matches the query fingerprint and shows the particulars of the matching fingerprint. Figure 6 shows the flowchart for the identification module.
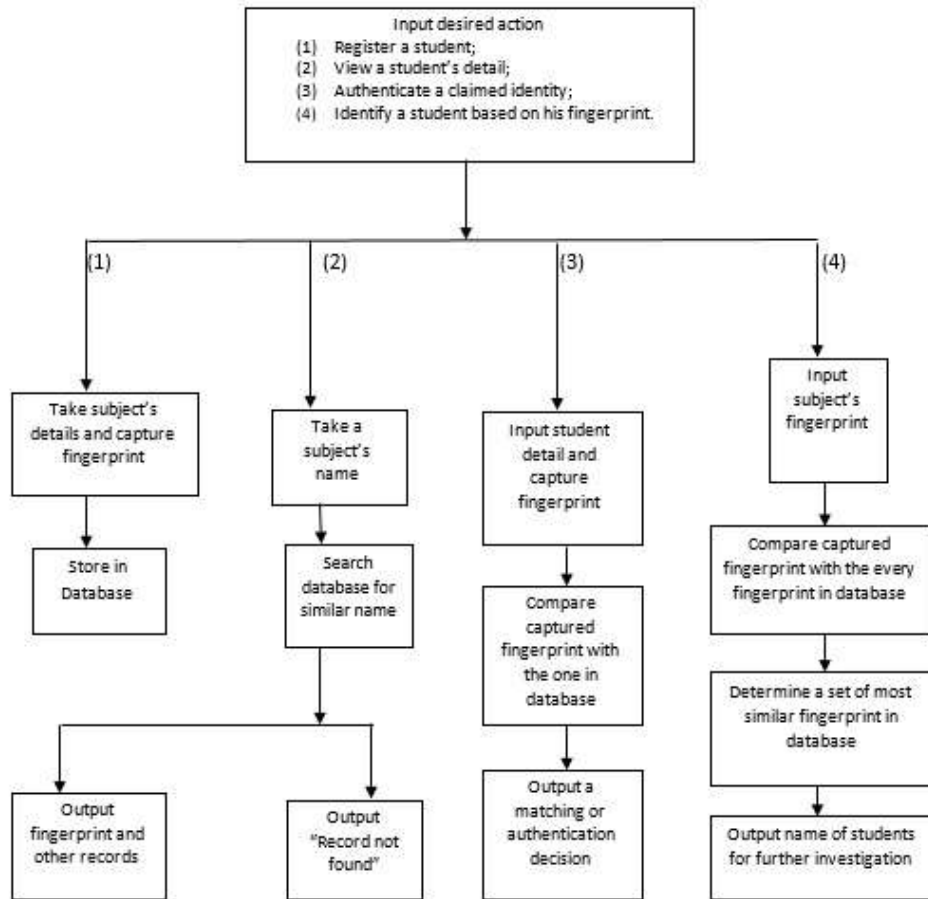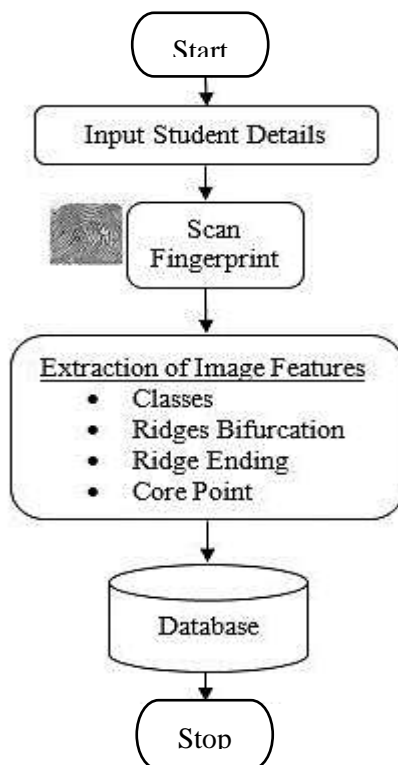
Figure 3: Proposed System Architecture

Figure 4: Registration flow chart

4. RESULTS AND DISCUSSION

Our real time fingerprint authentication system is a system designed with facilities for registration, authentication, identification and viewing student details.

The system provides a guide for the proper use of the system. The registration feature collects the students' data and also stores this data in an online database. The data required include; matric number, name, college, department, level and the captured fingerprint image.

Figure 7 shows the main page. It is designed with three functions. Each menu serves as a reference point that links all modules required for the fingerprint authentication/identification system to function as expected. The application was developed using visual studio software.

For image enhancement, a bank of 8 even-symmetric Gabor filters was designed and implemented in C# and used to filter the image. The filter bank was made up of a two-dimensional (2D) Gabor filter

design in spatial domain with σ_x and σ_y set to 4.0 based on empirical data for fingerprints [21]. The Gabor filter used has a kernel size of 11x11.

The average inter-ridge distance for 500dpi fingerprint images was assumed to be 8 pixels as used in [22], therefore, for our implementation a constant value of 0.125 (f $= \frac{1}{8}$) was used for all the filters but tuned to 8 different orientations; 0, $\pi/8$, $\pi/4$, $3\pi/8$, $\pi/2$, $5\pi/8$, $3\pi/4$, $7\pi/8$ radians with respect to x-axis.

The image was first normalized using the algorithm in [21], in order to reduce the variations of gray level values along fingerprint ridges and valleys. Thereafter the normalized image was divided into blocks of 16x16 pixels and an average orientation value computed for each block. For enhancement of the fingerprint image; at each point in the image a Gabor filter tuned to the orientation of the corresponding blocks is convolved with the image. If the value obtained is greater than zero the pixel at that point was given the value 255 or left as zero if otherwise, leading to an enhanced binary image.
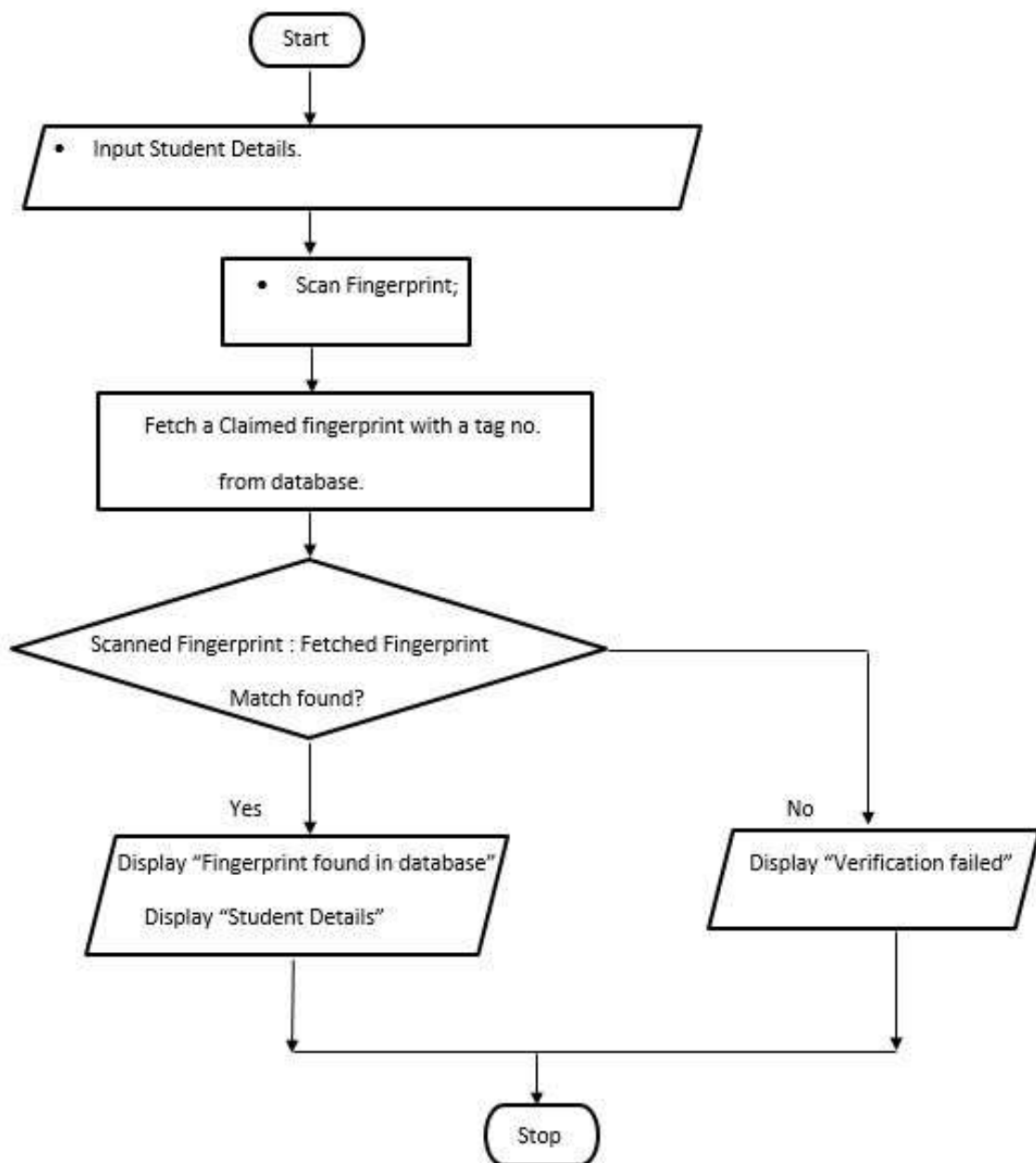
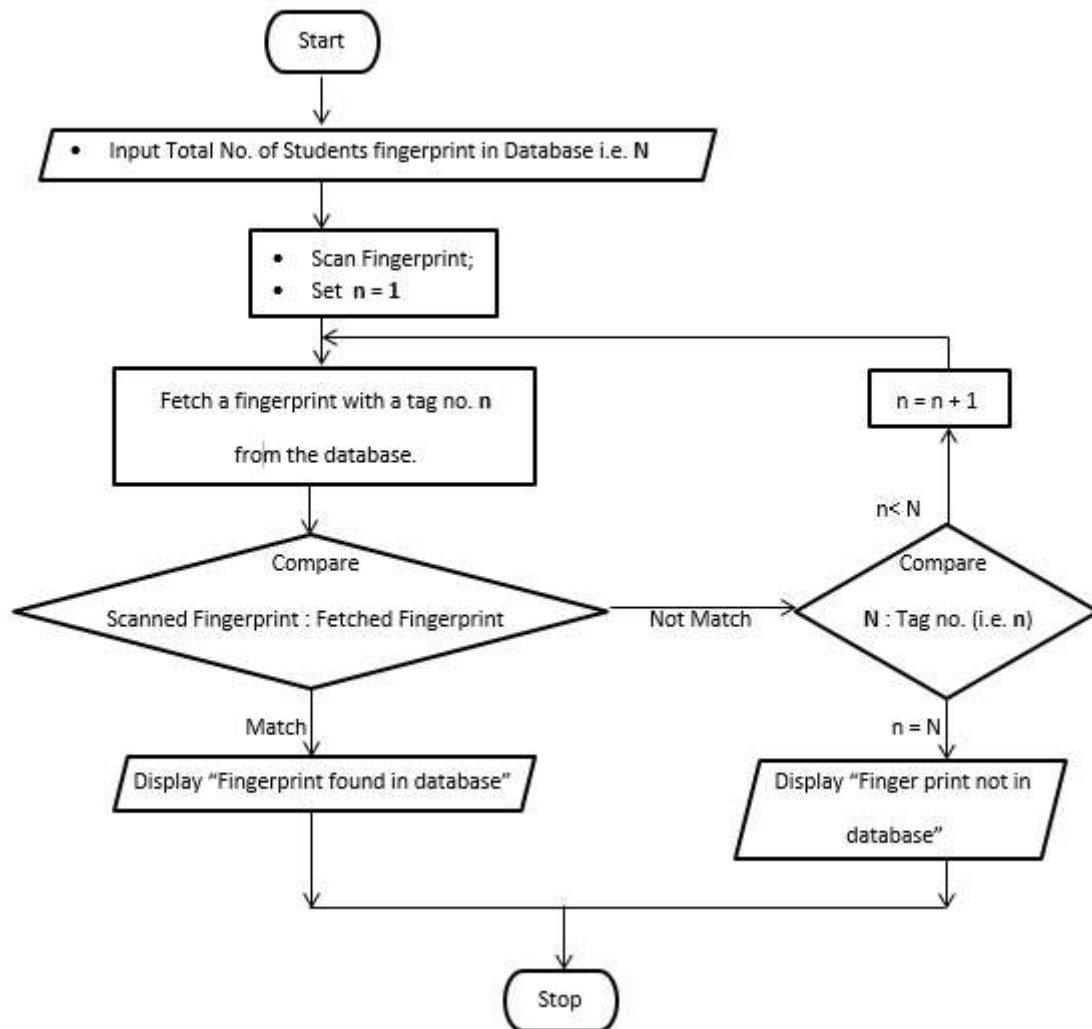

Figure 5: Verification /Authentication flowchart

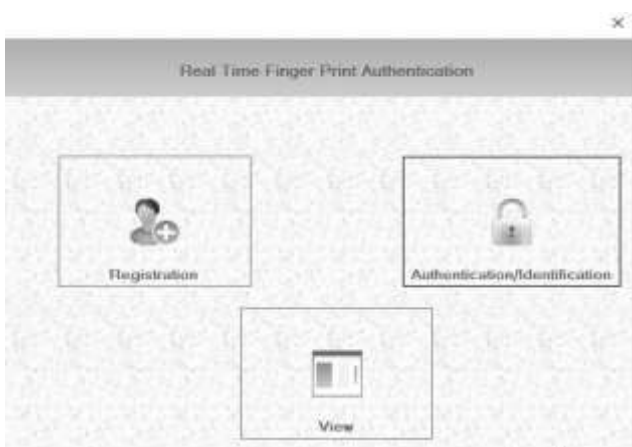Figure 6: Identification flowchart

Figure 7: Main page

Figures 8 (a) and (b) show a noisy fingerprint image and the enhanced (filtered) fingerprint image respectively.

Figure 8: (a) Noisy fingerprint image (b) Enhanced (Gabor-filtered) fingerprint image

Figure 9 shows the registration page. The registration page is the first recommended stage for all first time users. It is designed to collect all data required for the student to be properly registered. Required data include: name, college, matric number, department, level and the captured fingerprint image. Each section must be filled for the user to be properly registered.

Verification feature validates the student to know if the student has been registered by comparing his/her data with a particular data already stored in the online database using their fingerprint. Minutiae extraction and matching of the fingerprints were done using the accompanying SecuGen's SDK library routines. On successful verification, a matching score with the student data is displayed. In our experiment, for a false accept rate (FAR) of zero the optimal matching score threshold was found to be 35 on a scale of 0 to 200 as such the threshold value for a successful match was set at 35. Figure 10, shows the authentication of a user using noisy image and Figure 11, shows the authentication of the same user using filtered image. As shown, it also displays a matching score that is higher in numeric value for a filtered image. As shown in Figure 10 and 11 the inclusion of Gabor filtering for image enhancement before the matching stage increased the matching score by 47 implying a 23.5% improvement in the matching score. As such for a very poor quality fingerprint this increase in the matching score can greatly improve the false reject rate (FRR) of our system.

The identification stage is a one to many comparison stage that requires the input of the fingerprint of the user to be compared with all the fingerprints in the database. Identification was done with noisy image of a fingerprint as shown in Figure 12 and with the filtered image of the fingerprint as shown in Figure 13, where the matching score increased by 10.5% (from 161 to 182).

The 'view student' feature is an administrative feature that displays the data of every student whose details are already stored in the online database. As stated earlier, matching scores are displayed upon successful authentication/verification of a student. The matching scores for authentication/verification of the student was higher for filtered fingerprint image than for a noisy fingerprint image. On the whole, the developed system, when ran with registered users gave improved results for filtered or enhanced fingerprint as compared with the case of a noisy fingerprint.

5. CONCLUSION

A real time fingerprint verification/identification system using Gabor filter for enhancement of fingerprint image quality is presented in this paper. Fingerprint enhancement, contributed significantly to improving fingerprint image quality. Performance of

the developed system was evaluated on a database with fingerprints from different users. A bank of Gabor filter was designed and implemented in C# programming language for enhancement of the input fingerprints. The result showed improvement in accuracy level when the enhanced (filtered) image was used, as compared to when a noisy image was used.
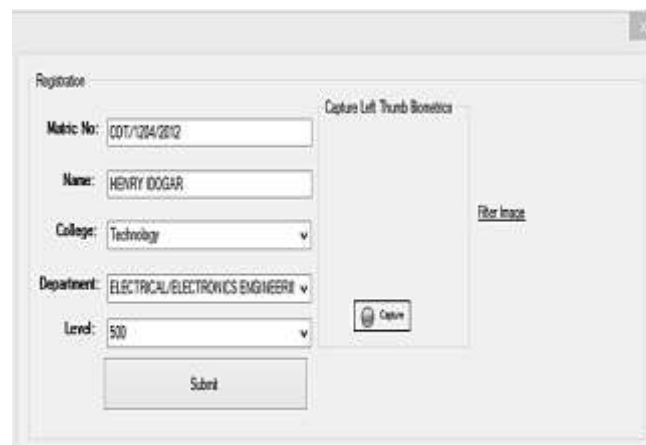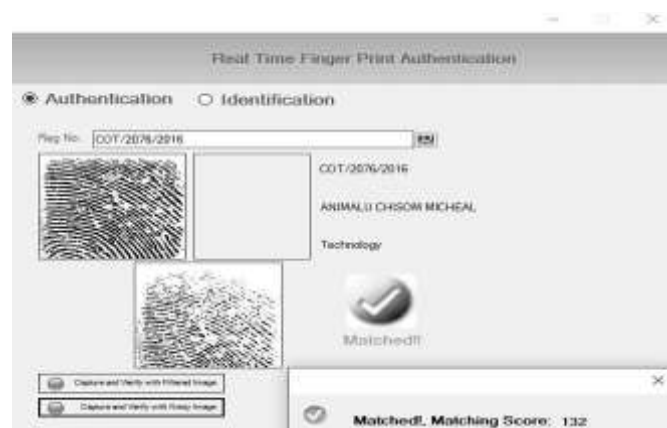

Figure 9: Registration page

Figure 10: Authentication/Verification with noisy image

Figure 11: Authentication/Verification with filtered image
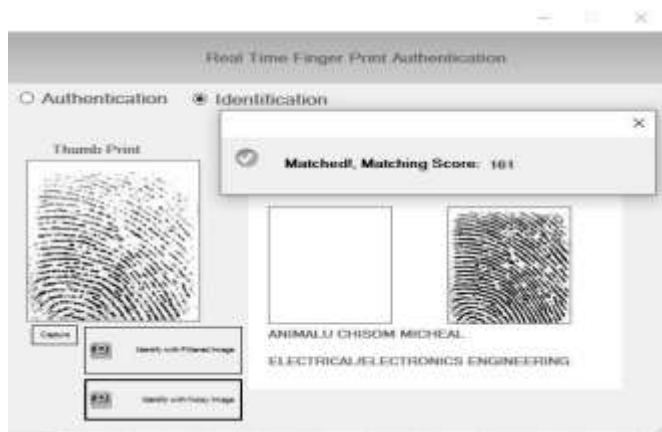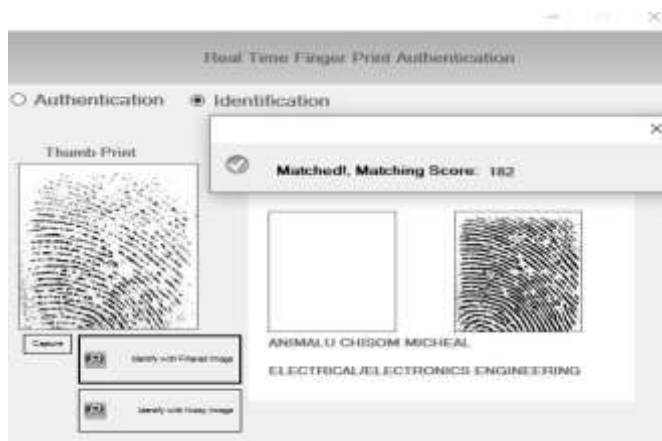
Figure 12: Identification with noisy image

Figure 13: Identification with filtered image

6. REFERENCES

[1] Chaurasia, Preeti Om. "An Approach to Fingerprint Image Pre-Processing", International Journal of Image, Graphics and Signal Processing, 6, pp 29-35, 2012.

[2] Jie, Z. and Jinwei, G. "A Model-Based Method for the Computation of Fingerprints' Orientation Field", *IEEE Transactions on Image Processing*, 13(6), 2004.

[3] Elmir, Y., Elberrichi, Z., Adjouj, R. and Benyettou, M. "Personal Identification by Fingerprints based on Gabor Filters", 2006.

[4] Jain, A. K, Prabhakar, S., Hong, L. and Pankanti, S. "Filterbank-Based Fingerprint Matching"*, IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846-859, 2000.

[5] Thai, R. "Fingerprint Image Enhancement and Minutiae Extraction", The School of Computer Science and Software Engineering, the University of Western Australia, 2003.

[6] Khalefa, M. K., Abduljabar, Z. A. and Zeki, H. A. "Fingerprint Image Enhancement by Develop Mehtre Technique", Advanced *Computing: An International Journal (ACIJ)*, 2 (6), pp. 355-363, 2011.

[7] Kanagalakshmi, K. and Chandra, E. "Frequency Domain Enhancement Algorithm Based on Log – Gabor Filter in FFT Domain", *Global Journal of Computer Science and Technology*, 12(7), 2012.

[8] Wang, Y., Yao, L. X. and Zhou, F. Q. "A real time fingerprint recognition system based on novel fingerprint matching strategy", in *Proc. the Eighth International Conference on Electronic Measurement and Instruments*, 2007.

[9] Shunshan, L., Wei, M., Tang, H., Zhuang, T. and Buonocore, H. B. "Image Enhancement Method for Fingerprint Recognition System", *Proceedings of the 2005 IEEE, Engineering in Medicine and Biology 27th Annual Conference*, Shanghai, China, pp. 3386-3389, 2005.

[10] Mil'shtein, S., Pillai, A., Shendye, A., Liessner. C. and Baier, M. "Fingerprint Recognition Algorithms for Partial and Full Fingerprints", in *Proc. Technologies for Homeland Security, IEEE*, pp. 449-452, 2008.

[11] Kaur, M., Singh, M., G. Girdhar, A. and Sandhu, P. S. "Fingerprint Verification System using Minutiae Extraction Technique", *World academy of Science, Engineering and Technology*, pp. 46, 2008.

[12] Jain, A., Chen, Y., and Demirkus, M. "Pores and Ridges: Fingerprint Matching Using Level 3 Features*", Pattern recognition letters*, pp. 2221-2224, 2004.

[13] Kryszczuk, K., Drygajlo, A. and Morier, P. "Extraction of Level 2 and Level 3 features for fragmentary fingerprints", *Proc. of the 2nd COST275 Workshop Vigo*, Spain, pp. 83-88, 2004.

[14] Elslunawy, M. Y., Zeng, J., Lo. S. B., and Chouikha, M. F. "Breast cancer detection in mammogram with AM-FM modeling and Gabor filtering", *IEEE Conference Publications*, vol. 3, pp. 2564–2567, 2004.

[15] Hussain, M. and Khan, S. "A Comparison of Different Gabor features for Mass Classification in Mammography", *IEEE Conference Publications*, pp. 142–148, 2012.

[16] Hussain, M., Khan, S., Muhammad, G., Berbar M. and Bebis, G. "Mass Detection in Digital Mammograms using Gabor Filter Bank", *IET Conference on Imaging (IPR 2012)*, London, UK, pp. 1–6, 2012.

[17] Lu, C., Jing, B., Chan, P. P. K, Xiang, D., Xie, W., Wang, J. and Yeung, D. S. "Vessel Enhancement of Low Quality Fundus Image using Mathematical Morphology and Combination of Gabor and Matched Filter", *International Conference on Wavelet Analysis and Pattern Recongition (ICWAPR)*, Jeju South Korea, pp. 168–173, 2016.

[18] Sun, Z., Bebis, G. and Miller, R. "Monocular Precrash Vehicle Detection : Features and Classifiers", *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 2019–2034, 2006.

[19] Ayres, F. J. and Rangayyan, R. M. "Design and performance analysis of oriented feature detectors", *Journal of Electronic Imaging,* vol. 16, no. 2, pp. 23007–23012, 2007.

[20] Casti, P., Mencattini, A., Salmeri, M. and Rangaraj, M. R. "Computerized Analysis of Mammographic Images for Detection and Characterization of Breast Cancer", Synthesis Lectures on Biomedical Engineering. Morgan & Claypool. Vol. 10, 2017.

[21] L. Hong, Y. Wan, and A. Jain, "Fingerprint Image Enhancement, Algorithm and Performance Evaluation," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 20, no. 8, pp. 777–789, 1998.

[22] S. K. Devireddy, "Integrated approach for automated authentication based on biometrics and tools of image processing," Institute of science & technology Jawaharlal Nehru Technological University Hyderabad – 500 072, A.P., INDIA, 2010.

[23] S. Prabhakar, "Fingerprint classification and matching using a filterbank," Michigan State University, 2001.

[24] K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A Real-Time Matching System for Large Fingerprint Databases," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 18, no. 8, 1996.