An Enhanced Minitiae-based Fingerprint Matching Algorithm

Omojokun G. Aju
Adekunle Ajasin University
Department of Computer Science
Akungba-Akoko, Nigeria

Segun M. Orimoloye
Adekunle Ajasin University
Department of Computer Science
Akungba-Akoko, Nigeria

Taiwo G. Omomule
Adekunle Ajasin University,
Department of Computer Science
Akungba-Akoko, Nigeria

ABSTRACT
Fingerprint authentication has been considered as the most complex and the matchlessly the most unchangeable form of all the biometric techniques, a procedure that has been established through various applications. A person's face or signature can change with time and may be fabricated or imitated, but a fingerprint occurs uniquely to an individual and remains unchanged for lifetime. Human fingerprints are known to be rich in details, otherwise known as minutiae which can be used as identification marks for fingerprint verification. There are two main applications involving fingerprints: fingerprint verification and fingerprint identification. The purpose of fingerprint verification is to authenticate a person's claimed identity, while the goal of fingerprint identification is to establish the identity of a person. Minutiae matching essentially consist of finding the best alignment between the template (set of minutiae in the database) and a subset of minutiae in the input fingerprint, through a geometric transformation. This paper is to establish an enhanced fingerprint recognition system based on minutiae matching by improved image segmentation and matching algorithms.

General Terms
Fingerprint Biometric

Keywords
Biometric, Fingerprints, Minutiae Matching, False Acceptance Rate, False Rejection Rate

1. INTRODUCTION
In the present age, identification is used for nearly everything. With technology being on a rapid pace of improvement, the need for accuracy and efficiency in identification is very necessary, especially with the high usage of automated transactions. Human beings have some certain properties to them and the study of these properties is called biometrics. Biometrics can be defined as automated methods of identifying a person or verifying the identity of a person based on physiological or behavioural characteristics such as fingerprints, face, retina or iris from the eye, voice, and hand geometry [3]. Each of these methods of recognition has its advantages and disadvantages. There are attributes that can help to determine how suitable it is for different applications. These attributes includes cost, size, reliability, operating environment, speed and accuracy. Examining each of these biometric recognition methods in detail, it can be assumed that fingerprint recognition is the most applicable for most systems and is the best place to begin a search for an appropriate biometric. Each person has a different pattern of fingerprint, and these patterns are made of ridges that make loops and whirls that are unique to each person [8].

A fingerprint is defined by a set of ridge lines and they run parallel and sometimes terminate and sometimes intersect. Each ridge is characterized by numerous minute peculiarities called Minutiae, which may divide and almost immediately reunite, enclosing a small circular or elliptical space or sometimes the independent beginning or ending of ridges [7]. In a fingerprint image, ridges are dark whereas valleys are bright. Ridges and valleys often run in parallel; sometimes they bifurcate and sometimes they terminate.

The skin of human fingertips consists of ridges and valleys and when they mix together, they form the distinctive patterns. At the time of pregnancy these distinctive patterns are fully developed and are permanent throughout the whole lifespan. Those patterns are called fingerprints. From different researches it has been observed that no two persons have the same fingerprints, so they are unique for each individual [5] [12]. Because of the aforementioned characteristics, fingerprints are very popular for biometrics applications. However, matching two fingerprints or finding duplicates of fingerprint in a database of fingerprints can be very difficult depending on the adopted method for the matching [2]. It is not only that fingerprints are more accessible, but also fingerprint recognition systems generally have lower costs, faster speed, and more reliable compare to other biometric recognition methods.

From observations, it can be concluded that the fingerprints offer more secure and reliable personal identification than passwords, signatures or key can provide. For this reason, several electronics products such as computers, mobile phones, smart doors equipped with fingerprint sensing devices for fingerprint based security protection are being implemented to replace the traditional password protection methods.

Minutiae based fingerprint identification system approaches toward the extraction of the ridge patterns correctly. However, the fingerprint image captured through poor scanners are found to have fewer number of minutiae points stressing the need for the fingerprint images enhancement to increase the clarity of the minutiae during the matching procedure [13].

Fingerprints are commonly classified into five different types: whorl, left loop, Right loop, arch, and tented arch [17]. In fingerprints, many recognition systems use neural networks to find minutiae, the ridge ends or splits to match a fingerprint. Since the number of minutiae varies among fingerprints, many people have tried to exploit this fact to enhance fingerprint matching [9]. Many of the problems for fingerprint recognition systems are related to obtaining the fingerprint images. Plastic distortions, scanning artifacts, scanning resolution, and uneven pressure are examples of such issues. However, these problems have to be addressed in order to

maintain reasonable and consistent results. This paper aims to design a better algorithm to increase the images enhancement of the input through segmentation to provide better matching results in term of accuracy and speed performance.

2. FINGERPRINT SENSORS

A fingerprint sensor is an electronic device used to capture a digital image of a fingerprint pattern. The captured image is called a live scan which is digitally processed to create a biometric template (a collection of extracted features) that is stored and used for matching [14].

The commonly used fingerprint sensor technologies include optical sensors, capacitive sensor and ultra-sound sensors.

A. *Optical Sensor*

Optical Sensors are the traditional and low cost solutions fingerprint sensor technology. It involves such technologies as: Optical reflection, Optical transmission, Optical Sweep, Optical Touchless, Optical TFT and Electro-Optical. Its low cost and strong prevention of Electro Static Discharge (ESD) are its major advantages, though its relative big size and high power consumption are the technology's minus, but, unlike other sensors, this sensor technology is not susceptible to electrostatic discharge damage. It is scratch-proof with unbreakable glass platen made of material as hard as quartz, highly resistant to shock and extreme weather [12].
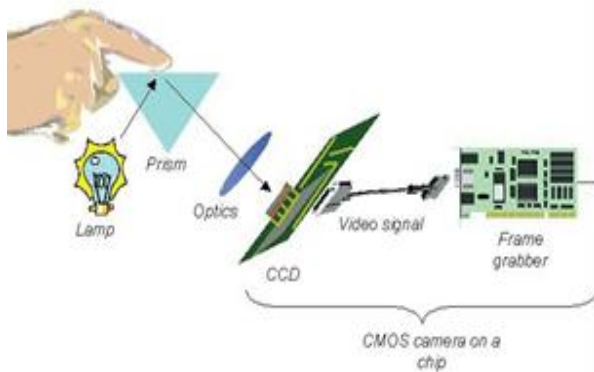

Figure 1: Optical Fingerprint Sensor Technology [14]

The technology involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface. Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge-coupled device) that captures a visual image of the fingerprint [12].

B. *Ultrasonic Sensor*

Ultrasonic sensors make use of the principles of medical ultrasonography in order to create visual images of the fingerprint. Unlike optical imaging, ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of skin. The sound waves are generated using piezoelectric transducers and reflected energy is also measured using piezoelectric materials. Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements is used to form an image of the fingerprint.
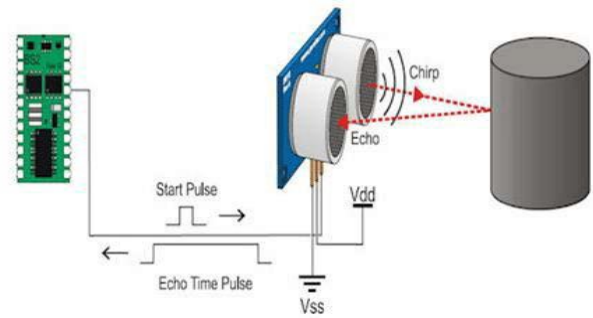

Figure 2: Ultrasound Fingerprint Sensor Technology [14]

Ultrasound fingerprint reading is not common as it requires quite a big device with mechanical parts which is very expensive. More so, it takes longer time to capture an image. Its greatest advantages are the reading of the derma, the sub-surface of the skin, rather than the surface, its high reliability compare to capacitive and optical fingerprint sensors since it measures the differences between the acoustic impedance of the ridges and valleys on user's finger.

C. *Capacitance*

Capacitive sensor uses the electrical property of capacitance to form fingerprint images. Capacitance is a property that exists between any two conductive surfaces within some reasonable proximity. The sensor array pixels each act as one plate of a parallel-plate capacitor, the dermal layer (which is electrically conductive) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric. The measurement of the capacitance between the skin and the pixel is the essential factor used to acquire fingerprints. Where there is a ridge or a valley, the distance varies, as does the capacitance. As the sensor uses very small sensing surfaces, it is therefore positioned very close to the targets. The measured capacitance values are then used to distinguish between fingerprint ridges and valleys [14].
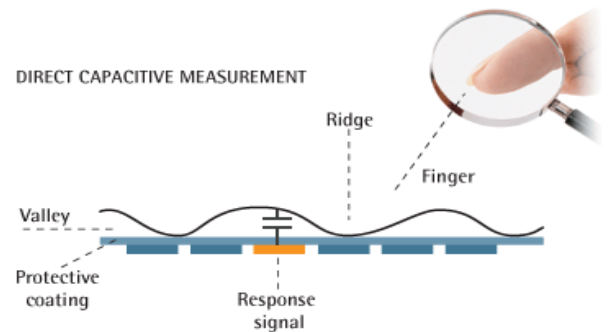

Figure 3: Capacitive Fingerprint Sensor Technology [14]

The advantages of the capacitive silicon fingerprint sensor technologies are its small in size, low power consumption and work for almost everyone. However, unlike the optical sensors, capacitive sensors usually need surface treatments, including electro static discharge (ESD) and other protective coatings.

A change in the distance between the surfaces changes the capacitance as defined here.

$$C = {}^{Q}/_{V} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad (1)$$

$$C = \varepsilon_0 \varepsilon_r {}^{A}/_{d} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad (2)$$

Where C is the capacitance; Q is the charge in coulombs; V

is the potential in volts; $İ_0$ is the permittivity of free space measured in meters; $İ_r$ is the dielectric constant of the insulator used; d is the separation between the electrodes measured in meters and A is the area of each plane electrode measured in square meters (50m x 50m for 500 dpi).

3. STUDY IMPLEMENTATION

This study is centred on improving the matching accuracy of the enrolled fingerprint image with the stored extracted fingerprint templates focusing on the image segmentation and matching processes through improved image segmentation and matching algorithms to increase the security in the fingerprints authentication. The minutiae based methods of fingerprint matching has been adjudged to perform better than other fingerprint matching methods such as Neural Network and Correlation based methods due to its high features reliability and robustness resulting from the method's uniqueness, stability, speed of processing and memory requirements [4].

3.1 Experiment Design

The minutiae based fingerprint matching technique is divided into two major parts; the pre-processing part involving the segmentation, enhancement and feature extraction of the fingerprint images and the processing part involving the minutiae matching of the fingerprints. However, this study is centred on the design of improved segmentation through image enhancement and minutiae matching algorithms with reference threshold of 0.48 to produce better matching accuracy.
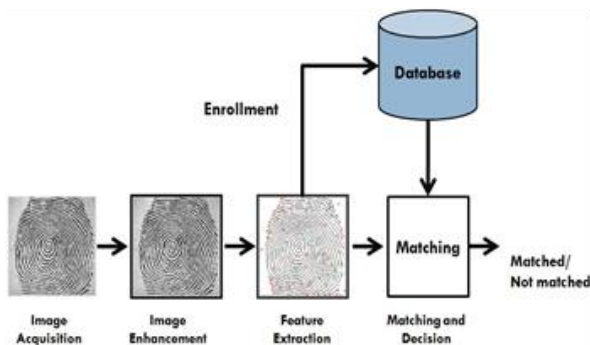

Figure 3: Flow Chart of the Proposed Method

A database template containing extracted fingerprint minutia points for one hundred and thirty (130) prints from one hundred and twenty (120) persons is used in the training of the improved minutiae based matching algorithm. The database contains ten (10) datasets of DS1, DS2, DS3, …..DS10, with each dataset containing 13 different fingerprint images. Each user (enrolled) fingerprint was compared with every fingerprint sample in the database template. The process was automated by ensuring that each query fingerprint is selected from the enrolled fingerprint image and matched against each and every fingerprint in the stored template. The choice of one hundred and thirty (130) prints from one hundred and twenty (120) persons test the algorithm's accuracy in uniquely discriminating fingerprints belonging to the same person and thus identifying duplicate registrations either as fraudulent or erroneous enrolments. This study is implemented using the MATLAB R2015a version environment and optical sensor to capture the fingerprint images with the images resolution set to 500dpi.

3.2 Performance Metrics

The proposed matching algorithm is measured in terms of accuracy of comparison derived from the "False Acceptance Rate" and "False Rejection Rate" of the matching samples and the speed of execution as performance metrics. Although, the previous comparative analysis of fingerprint authentication processes of minutiae based matching and distance based ratio matching had proved that minutiae based matching performs better in term of time of execution [11]. However, such better time of execution performance can be improved upon while increasing the matching accuracy at the same time.

The proposed analysis is based on the combination of the accuracy of the matching algorithm and the time taken for the matching to complete. The time taken for the matching to complete as a performance metric has direct effect on the speed of identifying and authenticating of persons.

The accuracy of the algorithm is evaluated using the following expression:

False Acceptance Rate (FAR): this is expressed as the probability of the system incorrectly matching two non-matching samples.

$$FAR = \frac{Number\ of\ Incorrectly\ Accepted\ Individuals}{Total\ Number\ of\ Wrong\ Matching} \qquad \ldots\ldots\ldots (3)$$

False Rejection Rate (FRR): this is expressed as the probability of the system incorrectly rejecting two matching samples.

$$FRR = \frac{Number\ of\ Incorrectly\ Rejected\ Individuals}{Total\ Number\ of\ Correct\ Matching} \qquad \ldots\ldots\ldots (4)$$

$$ACCURACY = 1 - \frac{FAR + FRR}{2} \qquad \ldots\ldots\ldots\ldots$$

(5)

3.3 Image Enhancement Process

The fingerprint enhancement process helps to improve the quality of low images before the segmentation by removing the noise from the fingerprint images as segmentation cannot be performed on images of low quality; therefore, enhancement of such images is necessary. The frequency and orientation of parallel ridges and valleys were used to remove unwanted noise in the fingerprint images to enhance the clarity of the ridge structure. Gabor filter is used to enhance the fingerprint utilizing the ridge frequency and ridge orientation information. Segmentation is therefore performed on the enhanced images and the segmented version is used for minutiae extraction.

The advantage of using a Gabor filter is its properties of optimal joint resolution in spatial and frequency domain and of its frequency-selective as well as orientation-selective [16]. The modulation transfer function (MTF) of the Gabor filter was adopted and is represented by:

$$H(u, v: \phi, f) =$$

$$2\pi\delta_x\delta_y \exp\left\{-\frac{1}{2}\left[\frac{(u_\phi - u_0)^2}{\delta_u^2} + \frac{(v_\phi - v_0)^2}{\delta_v^2}\right]\right\} +$$

$$2\pi\delta_x\delta_y \exp\left\{-\frac{1}{2}\left[\frac{(u_\phi + u_0)^2}{\delta_u^2} + \frac{(v_\phi + v_0)^2}{\delta_v^2}\right]\right\},$$

$$u_\phi = u\cos\phi + v\sin\phi,$$

$$v_\phi = -u\sin\phi + v\cos\phi.$$

$$u_0 = \frac{2\pi\cos\phi}{f},$$

$$v_0 = \frac{2\pi\sin\phi}{f},$$

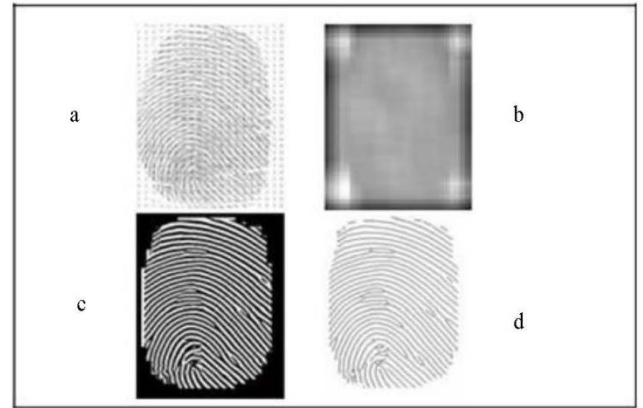**Figure 6: Steps in the Enhancement process**

(a). Orientation Field (b) Ridge Frequency Image

(c) Enhanced Image (d) Thinned Image

Where
du= 1/2dx and dv = 1/2πdy.
In applying G a b o r filter for the image enhancement

purpose, three essential parameters were specified:

1) The sinusoidal plane frequency, f,

2) The orientation of the filter,

3) The standard deviations of the Gaussian envelope, that is, dx and dy.

The local ridge frequency and the local ridge orientation were used in determining the frequency characteristic of the filter, f.

3.4 Image Segmentation

The segmentation stage is very crucial in the fingerprint matching system. It is the process of partitioning the fingerprint image into regions according to specific and common features. While the areas with effective ridges and furrows are highlighted based on the ridge orientation and region of interest (ROI) techniques, the areas with no significant details are discarded. The algorithm used in performing the segmentation is based on the block coherence of image which gives a measure of how well the gradients of the fingerprint image are pointing in the same direction. In a given window of size *W x W* around a pixel, the coherence is defined as shown in figure

$$Coherence = \frac{\left|\sum_W (G_{x,x}, G_{x,y})\right|}{\sum_W |G_{x,x}, G_{x,y}|} = \frac{\sqrt{(G_{x,x}, G_{x,y})^2 + 4G_W^2}}{G_{x,x} + G_{x,y}} \quad \text{......................} (6)$$

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

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

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

Figure 4: Image Block Coherence Mathematical Model

where G_x and G_y represent the local gradients along X and Y axes. The resulting gradient coherence image is smoothed by the use of a Gaussian smoothing filter to give a coherence image $C(x, y)$. The smoothed image is then binarized to produce a segmentation mask C_B. The binarization is carried out by global thresholding as:

$$C_B(i,j) = \begin{cases} 1 \to if \_ C(i,j) > M_c - 0.5S_c \\ 0 \to Otherwise \end{cases} \quad \text{...............} (7)$$

M_c is the global mean of the coherence image and S_c is its global standard deviation. This mask on pixelwise multiplication with the fingerprint image gives the segmented

image. The different steps in the segmentation are shown in figure 5.

Figure 5: Different stages of Segmentation

(a). Original image (b) Coherence image

(c) Segmentation Mask (d) segmented image

3.5 Minutiae Features Extraction

Minutiae points are unique characteristic features of a fingerprint. Therefore, extraction and analysis of these unique points are paramount in fingerprint matching algorithm. Minutiae extraction was carried out using the crossing number approach. Crossing number of pixel 'p' is defined as half the sum of the differences between pairs of adjacent pixels defining the 13-neighbourhood of 'p'. Explicitly expressed as

$$CrossNumber(p) = \frac{1}{2} \sum_{i=1,13} \left| val(p_{i \bmod 13}) - val(p_{i-1}) \right|$$

Where p_0 to p_{12} are the pixels belonging to an ordered sequence of pixels defining the 13-neighbourhood of p and $val(p)$ is the pixel value. Figure 7 shows a non-minutiae region, a bifurcation and a ridge ending where cross number (p) = 2, cross number (p) = 3 and cross number (p) = 1 respectively.
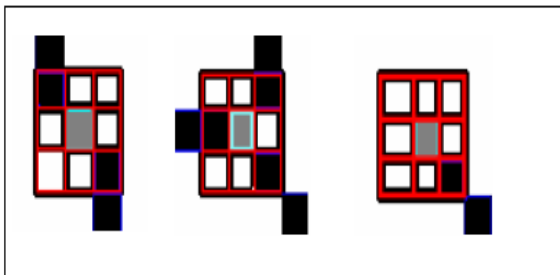

Figure 7: Minutiae extraction for a non-minutiae region,

a bifurcation and a ridge ending

Crossing numbers 1 and 3 correspond to ridge endings and ridge bifurcations respectively. An intermediate ridge point has a crossing number of 2. The minutiae obtained from this algorithm are filtered to preserve only the true minutiae. The different types of false minutiae introduced during minutiae extraction include spike, bridge, hole, break, spur, ladder, and misclassified border areas.

The number of minutiae in a given area is also limited; therefore the minutiae density must also be kept in check. In order to filter out these false minutiae a 3 level-filtering process is applied:

Level 1: Removes the false ridge endings created as a result of the application of minutiae extraction algorithm at the end of the thinned image.

Level 2: Removes the first three types of minutiae mentioned above using the rule based morphological minutiae filtering approach.

Level 3: This stage limits the maximum number of minutiae present in the thinned image to a pre-specified threshold.

A minutiae m is described by the triplet $m=\{x, y, \theta\}$, where x, y indicate the minutiae location coordinates and θ denotes the minutiae orientation, which is the orientation evaluated for the minutiae location from the orientation image obtained during the enhancement process.
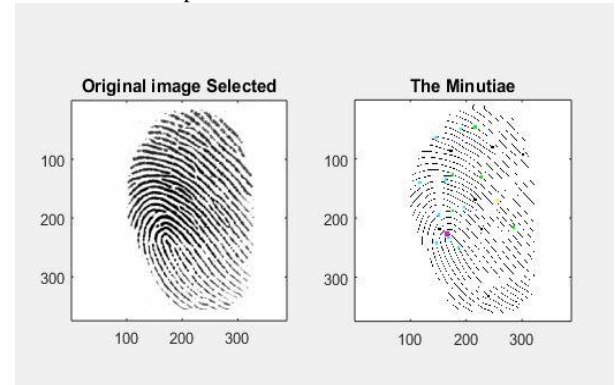

Figure 6: Original Image Selected and the Minutiae

3.6 The Minutiae Matching

Minutiae-based technique is the backbone of many fingerprint recognition processes as it uses the rich local features of a fingerprint, such as termination points and bifurcation [10]. It is widely used as it is computationally inexpensive. This technique locates the maximum number of minutiae pairings between the template and an enrolled set of minutiae extracted from the enrolled image for matching purpose.

Fingerprint minutiae based matching is accomplished by minutia matching of the point pattern where features associated with each point pattern and inter-point distances are used where both the enrolled fingerprints and the templates are converted to polygons in polar coordinate system and a matching algorithm is used to match the polygons [15].

The minutiae based algorithms compare various minutia points from an original image stored in a template with those extracted from a candidate enrolled fingerprint following the enhancement, segmentation and features minutiae extraction process in order to improve on the degree of extraction and perception of the minutia as well as to remove spurious or false minutiae.

Given two fingerprint images with 'T' and 'I' identified minutiae points respectively (T need not be equal to I), where T represents the set of minutiae points in the template and I represents the set of minutiae points of the enrolled fingerprint, M would therefore be the intersection of T and I (M = T ∩ I). This algorithm outputs the 'M' common minutiae points in both the image.

Input: P, Q_T, candidate minutiae pair index set Φ_π, $n\partial_A = \{n\partial(m_{A_i}) | i \in \Phi_\pi(1)\}$ and

$n\partial_B = \{n\partial(m_{B_j}) | j \in \Phi_\pi(2)\}$ as the neighbourhood sets

Initialize: $sim\delta \leftarrow$ Nil

Program:

For all minutiae pair indexes $(i, j) \in \Phi_\pi$ **do**

$\quad sim_\delta(m_{A_i}, m_{B_j}) \leftarrow 0$

$\quad O_{score} \leftarrow S(m_{A_i}, m_{B_j})$

$\quad$ **If** $O_{score} < O_{min}$ **Then**

$\quad\quad$ remove $(i, j) \in \Phi_\pi$

$\quad\quad$ continue

$\quad$ **end if**

$\quad$ **For all** $s \in n\partial_{A_i}$ **do**

$\quad\quad$ **For all** $t \in n\partial_{B_j}$ **do**

$\quad\quad\quad rdiff_{(m_{A_i}, m_{B_j})}(s, t) \leftarrow |d_{A_i(s)} - d_{B_j(t)}|$

$\quad\quad\quad \angle diff_{(m_{A_i}, m_{B_j})}(s, t) \leftarrow \min(|\angle_{A_i(s)} - \angle_{B_j(t)}|, 2\pi - |\angle_{A_i(s)} - \angle_{B_j(t)}|)$

$\quad\quad\quad \theta diff_{(m_{A_i}, m_{B_j})}(s, t) \leftarrow \min(|\theta_{A_i(s)} - \theta_{B_j(t)}|, \pi - |\theta_{A_i(s)} - \theta_{B_j(t)}|)$

$\quad\quad\quad$ **If** $r_{diff(m_{A_i}, m_{B_j})}(s, t) > r_{max}$ **or** $\angle diff_{(m_{A_i}, m_{B_j})}(s, t) > \angle max$ **or**

$\quad\quad\quad\quad \theta diff_{(m_{A_i}, m_{B_j})}(s, t) > \theta_{max}$ **Then**

$\quad\quad\quad\quad$ Continue

$\quad\quad\quad$ **End If**

Remove $s \in n\partial_{A_i}$

$\quad\quad\quad$ Remove $t \in n\partial_{B_j}$

$\quad\quad\quad \alpha(s, t) \leftarrow \exp(-rdiff_{(m_{A_i}, m_{B_j})}(s, t) - \theta diff_{(m_{A_i}, m_{B_j})}(s, t) - \angle diff_{(m_{A_i}, m_{B_j})}(s, t)$

$\quad\quad\quad \beta(s, t) \leftarrow \exp(-\Gamma diff_{(m_{A_i}, m_{B_j})}(s, t))$

$\quad\quad\quad sim_\delta(m_{A_i}, m_{B_j}) \leftarrow sim_\delta(m_{A_i}, m_{B_j}) + \alpha(s, t) + \chi\beta(s, t)$

$\quad\quad$ **End for**

$\quad$ **End for**

End for

{calculate shape context from the minutiae sets P (which has been non-affinely transformed) and Q_T (which has been affinely transformed)}

$C^{**} \leftarrow TPS_{cost}(P, Q_T)$

$D_{SC}^{**}(P, Q) \leftarrow \frac{1}{n}\sum_{p | e \in P | D_0(p_i, q_{\pi(i)}) < b} C(p_i, q_{\pi(i)}) + \Delta D_0(p_i, q_{\pi(i)}) + \beta D_{be}$

$S_{max} \leftarrow \arg\max_{(i, j)} S^*(m_{A_i}, m_{B_j}, I(A_i, B_j))$

$sim_{score} \leftarrow \frac{n_M(\sum_{(i,j)} sim_\delta(m_{A_i}, m_{B_j})) * (\sqrt{S_{max}})}{n_A * n_B} - \nu D_{SC}^{**}$

Return sim_{score}

Output: sim_{score}

Let the number of minutiae in T and I be m and n respectively, the minutiae sets of the two fingerprints be given by:

$$T = \{m_1, m_2, ..., m_m\}\ m_i = \{x_i, y_i, \theta_i\}, i = 1....m$$

$$I = \{m_1', m_2', ..., m_n'\}\ m_j' = \{x_j', y_j', \theta_j'\}, j = 1....n$$

A minutia m_j' in I and a minutia m_i in T are considered to be matched if their spatial and orientation differences are within specified thresholds r_o and θ_o. The threshold level is 0.5. The matching algorithm returns a percentage match score, which is then used to take the Match - No Match decision. The improved minutiae based fingerprint matching algorithm is designed here:

The returned similarity score (sim_{score}) is the output of the

algorithm and the decision module takes action based on this threshold value. Similarity computation is based on setting a threshold. For this system, a reference threshold value of 0.48 was used. This means that if a similarity score of this value or above is gotten for any template comparison out of the 0.5 standard threshold, then a match corresponding to enrolled template (in database) is recorded, otherwise no match is recorded.

4. RESULTS AND DISCUSSION

The results from the experiment implementation allow for the performance metrics in terms of matching algorithm accuracy and execution time to be established.

The result from table 1 shows that the algorithm provided high matching accuracy as it produced above ninety percent (90%) in all the matching processes of the samples during the experiment. It is also observed from the result that there is a relationship between the matching accuracy of the algorithm and the time of execution (speed). The process with the highest matching accuracy took the shortest time to be processed while the process with the lowest matching accuracy took the longest time to be processed. It is therefore interesting to know that, the shorter the processing time, the higher the matching accuracy.

Table 1: Performance Results of the Algorithm

Dataset	FAR	FRR	Matching Accuracy (%)	Average Execution Time (ms)
DS1	0.034	0.000	98.30	34
DS2	0.018	0.021	98.05	43
DS3	0.025	0.000	98.75	28
DS4	0.028	0.035	96.85	63
DS5	0.036	0.019	97.25	52
DS6	0.022	0.012	98.30	32
DS7	0.015	0.000	99.25	21
DS8	0.064	0.004	96.60	67
DS9	0.106	0.063	91.55	86
DS10	0.012	0.015	98.65	31

5. CONCLUSION

This paper has developed and implemented a prototype for fingerprint matching using an improved minutiae based matching algorithm through the use of routine image segmentation approach with one hundred and thirty (130) prints from one hundred and twenty (120) persons grouped into ten (10) datasets each containing thirteen prints with reference threshold of 0.48 for obtaining the similarity accuracy using optical sensor as image capturing device with 500dpi. The algorithm comparison accuracy through the FAR and FRR values and the time of execution were used as the algorithm's performance metrics.

The result of the study shows that the algorithm produces high rate of comparison accuracy of ninety-one percent and above. It produces very low rate of both FAR and FRR, resulting to higher comparison accuracy rate. The result from the study also shows a relationship between the level of comparison accuracy of the datasets and the matching processing time (Time of execution), it is observed that a higher comparison accuracy rate is produced at a shorter matching processing time and the less accurate matching takes longer time to be processed.

The study was conducted using optical sensor as an image capturing device with 500dpi resolution and MATLAB R2015a version as an implementation environment with 130 fingerprint image samples from 120 persons. However, the matching accuracy and the time of execution (speed of comparison) of this minutiae-based matching algorithm may give different results when implemented on differentenvironment and sensor device with different resolution as the choice of sensor technology, implementation environment and number of matching samples can affect the results of matching algorithms.

6. REFERENCES

[1] Lokesh, S., Manish, M. (2016). A Review Paper on Fingerprint Biometric and Security. Journal of Information, Knowledge and Research in Computer Engineering, Vol. 4, No. 2. pp. 901-906.

[2] Gurpreet, S., Vinod, K. (2014). Review On Fingerprint Recognition: Minutiae Extraction and Matching Technique.. International Journal of Innovation and Scientific Research, Vol. 10. No. 1. pp. 64-70.

[3] Jain, A. K., Bolle, R. M., Pankanti. S. (2006). Biometrics: Personal Identification in Networked Society. ISBN: 978-0-387-32659-7 (Ebook). Springer, Verlag USA.

[4] Qi J., Yang S & Wang Y (2005). Fingerprint matching combining the global orientation field with minutia," Pattern Recognition Letters, vol. 26, pp. 2424-2430

[5] Madhuri, M., Richa, Mishr. (2012). Fingerprint Recognition using Robust Local Features. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 6. pp. 1-5.

[6] Kumar, D. A. & Begum, T. U. S. (2013). A Comparative Study on Fingerprint Matching Algorithms for EVM. Journal of Computer Sciences and Applications, Vol. 1, No. 4. pp. 55-60.

[7] Nadaraja, M., Celalettin, T., et. al, (2011). Fingerprint Biometric for Identity management. International Journal of Industrial Engineering and Management (IJIEM), Vol. 2, No 2. pp. 39-44 < http://www.ftn.uns.ac.rs/ijiem/>

[8] Umut, U., Arun, R. and Anil, J. (2004). Biometric Template Selection and Update: A Case Study in Fingerprint. Pattern Recognition (Elsevier) 37, pp. 1533 – 1542.

[9] Chaohong, W. (2007). " Advanced feature extraction algorithms for automatic fingerprint recognition systems". A dissertation submitted to the faculty of the graduate school of state university of New York at buffalo in partial fulfilment of the requirements for the degree of doctor of philosophy.

[10] Li, J., Tulyakov, S., Farooq, F., et al. (2008). "Integrating minutiae based fingerprint matching with local mutual information," In the Proceeding of 19th International Conference on Pattern Recognition (ICPR 2008), Dec 2008, pp. 1-4, doi: 10.1109/ICPR.2008.4761888.

[11] Kumar, D. A. and Begum, T. U. S. (2013). "A Comparative Study on Fingerprint Matching Algorithms for EVM". Journal of Computer Sciences and Applications, Vol. 1, No. 4. pp. 55-60.

[12] Ray, M., Meenen, P and Adhami, R. (2005) "A novel approach to fingerprint pore extraction." In Proceedings of Southeastern Symposium on System Theory, pp. 282–286.

[13] Silas, K. and Robert, O. (2016). "Comparative Analysis of Minutiae Based Fingerprints Matching Algorithms". International Journal of Computer Science and Information Technologgy, Vol.8, No. 6. Pp. 59-71

[14] Lunji, Q. (2014). "Fingerprint Sensor Technology". In proceedings of 9th IEEE Conference on Industrial Electronics and Application, IEEE, Hangzhou, China. pp. 1433-1436

[15] Maltoni, D., Maio, D., Jain, A and Prabhakar, S. (2003) "Minutiae-based Methods". Extract from Handbook of Fingerprint Recognition, Springer, New York, pp. 141-144.

[16] Helfroush, M and Mohammadpour, M. (2008). "Fingerprint segmentation," In Proceedings of the 3rd International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, Syria.

[17] Vishal, K. S, Mathai, K. J and Shailendra, S. (2014). Fingerprint Segmentation: Optimization of a filtering technique with Gabor Filter. In Proceedings of Fourth International Conference on Communication Systems and Network Technologies.