

COMPARATIVE ANALYSIS OF MINUTIAE BASED FINGERPRINT MATCHING ALGORITHMS

Silas KivutiNjeru and Dr. Robert Oboko

School of Computing and Informatics, University of Nairobi, Kenya

ABSTRACT

Biometric matching involves finding similarity between fingerprint images. The accuracy and speed of the matching algorithm determines its effectiveness. This research aims at comparing two types of matching algorithms namely (a) matching using global orientation features and (b) matching using minutia triangulation. The comparison is done using accuracy, time and number of similar features. The experiment is conducted on a datasets of 100 candidates using four (4) fingerprints from each candidate. The data is sampled from a mass registration conducted by a reputable organization in Kenya. The research reveals that fingerprint matching based on algorithm (b) performs better in speed with an average of 38.32 milliseconds as compared to matching based on algorithm (a) with an average of 563.76 milliseconds. On accuracy, algorithm (a) performs better with an average accuracy of 0.142433 as compared to algorithm (b) with an average accuracy score of 0.004202.

KEYWORDS

AFIS, ANN, Fingerprint Recognition, FMR, FAR

1. INTRODUCTION

Biometric recognition refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics [2]. Some of the physiological characteristics that have been used in biometrics recognition include face, iris, fingerprints, and voice amongst others. Biometric systems are used in authentication and security access in banking systems, cross border identification, forensics, criminal investigations, paternity determinations, citizen registration and electronic voting systems [3]. Use of biometrics in the registration of citizens is becoming one of the most interesting and emerging technology applications in the authentication and identification of persons as compared to traditional password authentication. These technologies help in the detection and elimination of imposters as well as elimination of multiple registrations thus improving the accuracy, reliability and effectiveness of the electronic authentication.

It is important to note that biometric recognition system involves probability matching of records within a tolerance of approximation of observed biometric traits against previously collected data for a subject [3]. Uncertainties in biometric systems arise from variations within persons e.g. changes in age, environment, disease, emotions, occupation, training and other intentional alterations. Other variations may result from the sensitivity and calibration of the sensor devices as well as the biometric feature extraction and matching algorithm used. Therefore, biometric traits have fundamental statistical properties, distinctiveness and differing degrees of stability under natural physiological conditions and environmental challenges. A biometric match therefore represents not a certain and definitive recognition but a probability of correct recognition. The authors also hypothesize that a fraction of results from even the best designed biometric system might be incorrect or indeterminate. The purpose of this research was to

DOI:10.5121/ijcsit.2016.8606

compare various techniques for biometric matching and determine an optimal technique based on speed and accuracy of matching.

Generally, fingerprint-matching algorithms have two steps namely; (a) align the fingerprints and (b) find the correspondences between two fingerprints. The approach proposed by [4] is capable of compensating for some of the nonlinear deformations and finding the correspondences. However, since the ridges associated with the minutiae are used to estimate the alignment parameters, the size of the templates has to be large, which takes much memory and computation, otherwise, the alignment will be inaccurate. [5] use the local and global structures of minutiae in their approach. The local structure of a minutia describes a rotation and translation invariant feature of the minutia in its neighborhood, and the global structure tries to determine the uniqueness of a fingerprint. The problem with this technique is that it cannot compensate for real world distortions of a 3-Dimensional elastic finger.

Besides minutiae, researchers have also used other features for fingerprint matching. [13] proposed an approach which transforms fingerprint images into a sequence of points in the angle-curvature domain. The matching between a query fingerprint and a template fingerprint is based on the least-squares error of the Euclidean distance between corresponding points in the angle-curve domain. [4] presented a filter-based algorithm, which uses a bank of Gabor filters to capture both local and global details in a fingerprint as a compact fixed length Finger Code. The authors reported that the Finger Code-based system performs better than a state-of-the-art minutiae-based system when the performance requirement of the application system does not demand a very low false acceptance rate.

[1] Image Pre-Processing

The quality of a fingerprint image is determined by many factors which may be difficult to control; therefore fingerprint systems must be able to handle images in medium and low quality. According to [7] Feature enhancement routines are applied on an image to improve on the quality of the fingerprint features for effective recognition. [7] observes that image enhancement techniques are based on computation of the forward two-dimensional fast Fourier transform (FFT) to convert the data from its original (spatial) representation to a frequency representation. Thereafter, a nonlinear function is applied that increases the power of useful information (the overall pattern, and in particular the orientation, of the ridges and valleys) relative to noise. Finally, the backward 2-d FFT is done to return the enhanced data to a spatial representation before snipping out the middle 16×16 pixels and installing them into the output image.

[2] Types of Matching Algorithms

Fingerprint matching can be categorized as Neural Network based, Minutiae based or Correlation based. Neural Network matching is a pattern based matching algorithm which uses graphical comparison of the entire fingerprint image as opposed to the individual minutiae points. Some matching techniques use global level features and while others combine both global and local features. The characteristics that are used include the ridge thickness, curvature, or density. A pattern-based algorithm is independent of the number of minutiae points in a fingerprint as well as independent of the size of the finger print sensor. Compared to other algorithms, pattern-based algorithms are not affected by the quality of the fingerprint image. However, [5] observed that minutiae-based methods perform better than correlation-based due to their uniqueness, stability, speed of processing and memory requirements despite the fact that they may be affected by rotation, translation, deformation of the fingerprints as well as location and direction of the detected minutiae or presence of spurious minutiae. Therefore minutia features are considered to be more reliable and robust.

Minutia based matching consists of finding the best alignment between the extracted and stored template minutia and the minutiae from the subject finger print. On the other hand, Pattern based algorithms are based on scanning the overall fingerprint global features i.e. the loop, whorl or the arch patterns. The main problem in minutiae extraction methods is that minutiae in the skeleton image do not always correspond with true minutiae in the fingerprint image because of false minutiae extracted as a result of undesired spikes, breaks, and holes. For this reason, time-consuming pre-processing algorithms are required prior to the matching stage.

1.2.1 ARTIFICIAL NEURAL NETWORK BASED

An Artificial neural network (ANN) based fingerprint pattern classification algorithms are designed to automatically categorize a fingerprint image based on the arch, left loop, right loop, scar, or whorl. By first classifying a fingerprint according to its class reduces the number of candidate searches required to determine if a fingerprint matches to the file prints. This improves the computation efficiency of the matching process by partitioning the file fingerprints based on classification thus greatly reducing the number of comparisons that must be performed by the minutiae-matcher [7]. The ANN system performs all the processes of image segmentation, enhancement, feature extraction, registration, dimensionality reduction and classification. At the classification stage, the Artificial Neural network traces and analyses ridges and creates the template (hypothesized class).

The ANN algorithm classifies an input feature vector by computing the Gaussian kernel functions values which are organized into a multi-layered feed forward network with four layers namely Input layer, Hidden layer, Pattern layer/Summation layer and the Output layer as shown below. The output classification of the fingerprint is computed by applying a transfer function $f(x, y)$ to the weighted sums of the input vector values from the input image. To work with the fingerprint recognition system using artificial neural network requires training of the neurons from a training set of data and calculating the output of the network by applying some random weights until the error between the network output and the desired output is minimal.

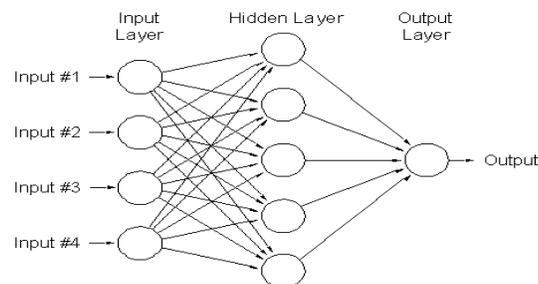


Figure 1 - Artificial Neural Network

The algorithm picks a maximum value of the category unit from this function which becomes the corresponding output value for the classification. This algorithm requires extensive training.

1.2.2 CORRELATION BASED ALGORITHMS

Texture correlation and convolution techniques are also used in image processing and can also be applied to finger print matching. The phase only correlation function (POC) uses the phase spectra of the finger print images and computes the Discrete Fourier Transforms (DFT) of two finger print images. The phase spectrum transforms an image into its frequency domain

representation. When two images are similar, their POC function gives a distinct sharp peak, but when two images are not similar, the peak drop significantly. Research conducted by [4] noted that phase correlation techniques are not influenced by image shift and brightness change and it is highly robust against noise. Texture features have been have also been applied to fingerprint matching where the finger print is tiled into cells and a bank of Gabor filters are combine with each cell and the variance of the energies of the Gabor filer responses in each cell is used as a feature vector. These techniques are computationally expensive, although it has been suggested that local correlation and correlation in Fourier domain can improve efficiency [12]

Correlation based matching uses the grey level information of the fingerprint image since it contains much richer, discriminatory information than only the minutiae locations. This takes into account the level 3 features as well as other fingerprint features. In correlation based techniques, two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments.

Matching Based Local and Global Structures [5]proposed an algorithm based on local and global features e.g. minutia type, coordinates, and the orientation angle to compare the query and the template fingerprint. The algorithm computes the Euclidian distances between the feature vectors in order to obtain the correct minutiae correspondence. The final matching score in these algorithms involves measuring both the number of matching minutiae pairs and the similarity degree of two orientation fields thus reducing the false rejection rate as well as false acceptance rate as illustrated by [5]. This method takes advantage of more information than traditional minutiae based method. By combining the Local structures and the fingerprint orientation field, this algorithm improves the minutiae correspondence.

A minutia point M detected from a fingerprint is described by the feature vector $f(x,y,\omega)$, Where (x, y) are the coordinates of the minutiae points, ω is the local ridge orientation direction of the fingerprint ridge in the range $[\pi/2, \pi/2]$ or $[0, \pi]$. To measure the difference between two ridge directions, ω_1 and ω_2 the function $d(\omega_1, \omega_2)$ is given as below;

$$d(\omega_1, \omega_2) = \left\{ \begin{array}{l} \omega_1 - \omega_2 \\ \text{if } -\frac{\pi}{2} < (\omega_1 - \omega_2) < \frac{\pi}{2} \\ \omega_1 - \omega_2 + \pi \\ \text{if } -\frac{\pi}{2} < (\omega_1 - \omega_2) < -\pi/2 \\ \omega_1 - \omega_2 - \pi \\ \text{if } \frac{\pi}{2} < (\omega_1 - \omega_2) < \pi \end{array} \right\} \dots (3)$$

Given a minutiae point M with orientation ω , a minutiae structure is defined as follows;

$$\text{Let } \theta_1 = \omega, \theta_2 = \theta_1 + \frac{2\pi}{3}, \theta_3 = \theta_2 + 2\pi/3 \dots (4)$$

Using the above minutia feature vectors, [5] developed an algorithm that receives as the input two minutia lists and two orientation fields captured from two fingerprint impressions and delivers a matching score that expresses the degree of similarity between the two fingerprints. The value of the similarity level between minutiae (b_1, b_2) is obtained by maximizing the similarity level $s(b_1, b_2) = \max_{i,j} (s(i, j))$, where i and j are the minutiae points of the input and template fingerprint. The algorithm applies two thresholds namely GlobalAngleThr and the GlobalDistThr. The GlobalAngleThr is used to compare angles in the global minutia matching step while the GlobalDistThr is used to compare minutia distances in the global minutia matching step.

1.2.3 M-TRIPLET DESCRIPTOR BASED MATCHING

M-triplet feature as proposed by [9] uses three triangular minutiae points where the ridge continuity breaks and they are typically represented as $(x; y; \Theta)$; where $(x; y)$ represent the two dimensional point coordinates, and Θ the ridge direction at that point. Minutiae detection algorithm takes a fingerprint image and locates features in the ridges and furrows of the skin. Points are detected where ridges end or split, and their location, type, orientation, and quality are stored and used for search. There are 100 minutiae on a typical ten-print, and matching takes place on these points rather than the 250,000 pixels in the fingerprint image.

According to [9], Minutiae triplets are local structures represented by three minutiae in the neighbourhood. Minutiae matching techniques aims at finding the minutiae correspondence (number of common minutiae points) between the input and the query fingerprints. In this algorithm, the number of matching minutiae points can be maximized if a proper alignment between the query and template fingerprints can be found [6].

The relative transformation between the Query image and the Template image poses a challenge known as correspondence problem. This causes ambiguity since each minutiae of one finger print can be matched onto any minutiae of the other fingerprint. To reduce the ambiguity, additional information is added called the minutiae descriptor information. This information helps to quickly establish the minutiae correspondence. A simple and accurate descriptor is based on Minutiae triplet (m-triplet). Some of the quality parameters of the minutiae triplet based matching include:

- i. The minutiae order in the triplet does not affect the correspondence and thus the algorithm finds the correct correspondence when matching.
- ii. The algorithm does not match a triplet with its reflected versions.
- iii. In order to find similar triplets, the algorithm takes into account the directions of the minutiae relative to the sides of the triangles formed by the triplets.

An m-triplet is defined as a tuple with the following components [9]

- Minutiae $p_i \in P$ which are clockwise starting at P_i
 - $d_{i \in 1 \dots 3}$ where d_i is the Euclidean distance between the minutiae different that p_i
 - $d_{max}, d_{mid}, \text{ and } d_{min}$ Which are the maximum, middle, and minimum distance values.
 - $\alpha_{i \in 1 \dots 6}$ which are the angles $ad_{2\pi}(ang(p, q), \theta)$ required to rotate the direction θ of a minutia to superimpose it to the vectors associated with the other two minutia in the triplet.
 - $\beta_i = ad_{2\pi}(\theta_i, \theta_k)$ is the angle required to rotate the direction of the minutia p_k in order to superimpose it to the direction of the minutia p_j
- Figure 2 below represents the mtriplet feature

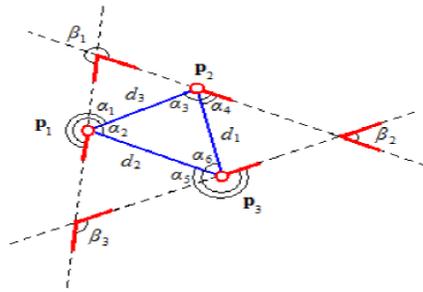


Figure 2 - M-triplet Feature representation

The M3gl developed by [9] is based on the M-triplet feature such that given a fingerprint described by the features set P we can compute the M-triplet as follows. For each $p \in P$, we find its nearest minutiae in P and build all m-triplets that include p and two of its nearest minutiae, discarding duplicates.

2. COMPUTATION OF ACCURACY SCORES

To compute the similarity accuracy scores, an algorithm computes the Euclidean distances between the two points of a fingerprint features. Given two fingerprint images with ‘T’ and ‘Q’ identified minutiae points respectively (where T need not be equal to Q), this algorithm outputs the ‘M’ common minutiae points in both the images. Effectively, if T represents the set of minutiae points in image 1 and Q represents the set of minutiae points in image 2, M would be the intersection of T and Q ($M = T \cap Q$). A fingerprint matcher takes two fingerprints vectors, T_i and Q_j and produces similarity measurement $S(T_i, Q_j)$ which is normalized in the interval [0, 1]. If the value of the matching score is close to 1, then the matcher has a higher confidence of similarity. For instance, Let the number of minutiae in T and Q be m and n respectively

$$\begin{aligned} T &= m_1, m_2, \dots, m_m, \quad m_i = x_i, y_i, \theta_i, i=1, \dots, m \dots (5) \\ Q &= m'_1, m'_2, \dots, m'_n, \quad m'_j = x'_j, y'_j, \theta'_j, j=1, \dots, n \end{aligned}$$

This category of algorithms computes the Euclidean distances between the pairs of minutiae (Feature vectors). The outputs of each comparison is either a “match” or a “non- match”. In Minutiae based algorithms, a minutiae m_i in T and m'_j in Q are considered matching if the following conditions are satisfied. This can also be written according to the equation below using the spatial distance (sd) and direction distance (dd)

$$\begin{aligned} sd(m'_j, m_i) &= \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0 \dots \dots (6) \\ dd(m'_j, m_i) &= \min(|\theta_j - \theta_i|, 360 - |\theta_j - \theta_i|) \leq \theta_0 \end{aligned}$$

where r_0 and θ_0 are the parameters of tolerance required to compensate for errors.

Minutia based fingerprint matching system usually returns the number of matched minutia on both the query and reference fingerprint and uses it to generate similarity scores in the range between [0....1]. More matched minutiae will always yield a higher similarity score and thus when the number of minutiae on both the fingerprints is large, then we can confidently distinguish the genuine and impostor fingerprints using the number of matched minutiae.

3. MATCHING TECHNIQUE

Fingerprint matching is achieved by minutia matching of the point pattern where features associated with each point pattern and inter-point distances are used to reduce the search paths.. Minutia matching processes are normally decomposed into two stages mainly (a) pre-processing stage where enhancements and transformations such as translation, rotation and scaling parameters between input minutia pattern and a template minutia are first estimated; the input minutia is then aligned with the template minutia pattern according to the estimated parameters; and (b) matching stage, where both the input and the template are converted to polygons in polar coordinate system and a matching algorithm is used to match the polygons.

In pattern based approach, the graphical center of the fingerprint image is located, then the image is cropped a fixed distance around this center point. The cropped region is then stored for subsequent matching.

Minutiae based algorithms compare several minutia points from an original image stored in a template with those extracted from a candidate finger print. Minutiae based algorithms require extensive pre-processing and image enhancement techniques in order to improve on the degree of extraction and perception of the minutia as well as to remove spurious or false minutiae.

4. PERFORMANCE EVALUATION

4.1 RECEIVER OPERATOR CURVE ANALYSIS

One of the techniques for evaluation of the performance of the algorithms is based on the receiver operating characteristics (ROC) graph. The ROC graph is used for visualizing, organizing and selecting classifiers based on their performance. A classification model based on mapping of instances to some target class is used. If the instance is positive and it is classified as positive, it is counted as a true positive; if it is classified as negative, it is counted as a false negative. If the instance is negative and it is classified as negative, it is counted as a true negative; if it is classified as positive, it is counted as a false positive. Given a classifier and a set of instances (the test set), a two-by-two confusion matrix is constructed as shown in figure 10 below;

		True Class	
		P	N
Hypothesis Class	Y	True Positive	False Positive
	N	False Negative	True Negative

Figure 1- Confusion matrix

From the above matrix, common metrics are calculated using Equation (7) and (8) below

$$TPR = \frac{\text{Positives correctly classified}}{\text{Total Positives}} \dots (7)$$

Similarly

$$FPR = \frac{\text{Negatives incorrectly classified}}{\text{Total Negatives}} \dots (8)$$

Thus the ROC graph is a two-dimensional graph in which tp rate is plotted on the Y axis and fp rate is plotted on the X axis. From the graph therefore, we can depict relative trade-offs between benefits (true positives) and costs (false positives). It is important to note that this technique measures performance in terms of accuracy but does not evaluate speed.

4.2 FALSE MATCH RATE VS FALSE NON-MATCH RATE

A second technique for evaluation of the performance of the algorithms is based on the false match rate (FMR) versus the false non-match rates (FNMR). Where FMR is the number of impostor comparisons with scores higher than the threshold divided by the total number of impostor comparisons.

Similarly, The FNMR is the number of genuine comparisons with scores lower than the threshold divided by the total number of genuine comparisons. This technique is based on accuracy as a measure of performance.

4.3 PROPOSED COMPARATIVE ANALYSIS

The key aspect of the efficiency of an algorithm is measured in terms of speed of execution and accuracy of comparison. Trade-offs are made across all of these measures to achieve the best-performing system consistent with operational and budgetary needs. For example, recognition error rates might be improved by using a better but more time-consuming enrolment process; however, the time added to the enrolment process could result in queues (with loss of user acceptance) and unacceptable costs. Previous comparative analysis of fingerprint carried out by [6] compared Minutiae based matching and distance based ratio matching and observed that minutia matching performed best in terms of time and memory requirements. Another research done by [5] evaluated the performance of minutiae matching using an ROC curve.

The proposed analysis is based on combination of the speed of matching, accuracy of the algorithm and the number of features identified. The speed of matching as a performance measure has a direct impact on the speed of identification of individuals. The accuracy is evaluated using the similarity scores and the number of common fingerprint features in two fingerprints that are matched by an algorithm. From the values obtained in the experiment, descriptive statistical analysis of the similarity scores, time taken, and the number of features is performed.

5. METHODOLOGY

5.1 INTRODUCTION

This section describes an exploratory study for comparison of the performance of two fingerprint matching algorithms; one that is based on minutiae triangulation features and another based on a combination of minutia points and global orientation features. The study is conducted on a Microsoft Visual Studio environment using C# using fingerprint images obtained from a citizen registration exercise conducted in Kenya by a reputable institution.

In this study, we aimed at carrying out an exploratory analysis of those algorithms that are based of minutia and global orientation features namely MJY [14] and MQYW [9] against those that are based on minutia triangulation (M-triplet features) namely M3gl [9].

5.2 DATA COLLECTION

The data used for this research was based on a collection of image impressions of the four (4) fingers from each candidate individuals. The data is captured using a 500 dpi resolution finger print scanner (4-4-2) that produced images of 512x480 pixels. Prior to the features extraction and matching process, each image is passed through a pre-processing stage to improve on the image quality. For ease of identification and matching, each image is assigned a unique name as follows;

- i. Left Thumb: xxxxxxxxxxxx_31.wsq
- ii. Left Index: xxxxxxxxxxxx_32.wsq
- iii. Right Thumb: xxxxxxxxxxxx_36.wsq
- iv. Right Index: xxxxxxxxxxxx_37.wsq

The .wsq fingerprint images of 100 candidates are sampled and save in a windows folder in C:\FingerprintImages\WSQImages, A program is developed in c# to convert the .wsq images to bitmap images for the algorithms to read and extract features. The converted bitmap images are stored under C:\FingerprintImages\BMPImages.

We randomly selected a sample of four (4) fingerprints (Left index, Left Thumb, Right Index, Right Thumb) from amongst 100 randomly selected candidates in the database of registered individuals. The assumptions and considerations in this research were that all the fingerprint capture equipment have the same configurations for the registration software, secondly, it is assumed that the environmental conditions did not affect the quality of the captured fingerprints and therefore the conclusions drawn from the samples were generalized into the entire population.

5.3 PROTOTYPE TESTING

Each candidate fingerprint was compared with every member in the population set. The process was automated by ensuring that each query fingerprint is selected from the population and matched against each and every finger print in the entire population. This process was able to uniquely discriminate fingerprints belonging to the same individual and thus identifying duplicate registrations either as fraudulent or erroneous enrolments. In this research, the experiment was conducted by executing each algorithm against a database of sampled fingerprints and obtaining values of similarity scores, time taken and the number of similar features obtained from the query and template fingerprints. The outputs were then analyzed using SPSS statistical tool to obtain statistical values for comparison. Fingerprint features were extracted from each of the four sampled fingerprints (Left Thumb, Left Index, Right Thumb, Right Index) and average similarity scores were computed.

6. RESULTS AND DISCUSSIONS

6.1 INTRODUCTION

This chapter describes the findings and results of the research within the scope of the research objective. The results in this chapter show the performance indicators in terms of algorithm speed and accuracy. This helps to clarify the implications on performance of the fingerprint matching implemented in solution.

6.2 OVERALL RESULTS

After the tests were successful, the image conversion program was executed to convert the four (4) fingerprint images for 100 candidates. This process took approximately two (2) minutes. The main experimental program for the matching and de-duplication was performed where the de-duplication using MWQY algorithm took about 45 minutes and the M3gl algorithm took an approximate 3 minutes to complete. The Output value indicated whether there was a positive (P) Match or Negative (N) Non-match result /Impostor

An extract of the sample results are given in the Table 3 below.

Table 1- Sample Matching Results using Minutia Triangulation

Query Image	Template Image	Accuracy (Score)	Time (ms)	No of Features
11142100	57479000	0.0036	80	3
11142100	89586000	0.0027	22	0
11142100	111925100	0.0016	25	0
11142100	123574800	0.0028	14	3
11142100	207140300	0.0014	13	0
11142100	222941600	0.0059	23	3

An extract of the sampled results of the experiment using minutia and global orientation based algorithms is shown in the Table 4 below

Table 2 - Matching Result using Minutia and Global Orientation Feature

Query Image	Template Image	Accuracy (Score)	Time Taken	No of Features
11142100	57479000	0.1329	703	3
11142100	89586000	0.1313	710	6
11142100	111925100	0.1232	856	6
11142100	123574800	0.0975	543	1
11142100	207140300	0.1146	481	1
11142100	222941600	0.155	704	4

6.3 DISCUSSIONS

Using the descriptive values of minimum, maximum, average and the standard deviation of the three variables we were able to compare and analyze the performance of the two algorithms as shown in table 5 below. The table 5 and table 6 below shows that a total of 4950 comparisons were performed and values for accuracy, time taken and number of similar features identifies were computed for each algorithm

Table 3 - Minutia Triangulation (M-Triplet) Based

M3gl Algorithm - Descriptive Statistics

	N	Min	Max	Mean	Std. Dev	Variance
Accuracy	4950	.0009	.0142	.004202	.0017840	.000
Time (ms)	4950	8	504	38.32	31.834	1013.416
No. of Features	4950	0	11	3.66	1.229	1.511
Valid N	4950					

Table 4 -Minutia and Global Orientation Based

	N	Min	Max	Mean	Std. Dev	Variance
Accuracy	4950	.0459	.3009	.142433	.0363188	.001
Time	4950	0	999	563.76	237.459	56386.784
NoofFeatures	4950	1	32	7.56	3.532	12.475
Valid N	4950					

Where N= Number of Fingerprints comparisons performed in a dataset of 100 candidates with four fingerprints each.

This research has revealed that fingerprint matching algorithms require high computational resources in terms of speed, time and memory. For instance, it took approx. 30mins to perform de-duplication of one hundred (100) candidates with four (4) fingerprint images each on a personal laptop. This research was successfully implemented on a personal laptop computer based on simulation of algorithms implemented on C# using Microsoft Visual Studio 2010 professional development environment. It is observed that fingerprint matching based on minutia triangulation algorithms performs better in terms of speed with an average of 38.32 milliseconds as compared to matching based on a combination of minutia and global orientation features with an average of 563.76 milliseconds.

In terms of accuracy of matching, the algorithms based on a combination of minutia and global orientation field features performs better with an average similarity score of 0.142433 as compared to m-triplet based matching with an average similarity score of 0.004202

7. CONCLUSIONS

This section summarizes the achievements, recommendations and future work in this area.

In this research, we were able to analyze and effectively compare the performance of two fingerprint matching algorithms a) one that is based on minutia features and b) another based on minutia triangulation features. Both of these algorithms have been compared in terms of speed of comparison and degree of accuracy.

In this research, we also developed and implemented a prototype for fingerprint matching to identify duplicate records using four (4) fingerprint images from 100 candidates. The experiment was executed in a controlled environment using some free libraries available on the internet. The prototype developed was able to extract and convert fingerprint images captured using standard enrolment devices with 500 DPI.

The research has helped re-affirm the fact that the choice of the fingerprint matching algorithm certainly improves the matching performance of the fingerprint based recognition system. Other factors affecting the performance of fingerprint recognition systems have widely been documented namely the quality of fingerprint images, enhancement techniques applied. A lot of

research efforts has previous been focused towards enhancing the quality of the fingerprint images, improving the enrolment process and enhancing the usability of the recognition software.

From this research, it has been revealed that the choice of an appropriate algorithm is largely dependent on the intended application of the biometric recognition system, the resources available as well as the desired level of accuracy. The computational resources available for carrying out large scale biometric matching affects in a large way the choice of the matching algorithm.

Biometric recognition is a new field that is gaining popularity in the Kenyan market since every industry in Kenya is adopting biometric techniques in identifying both their staff and clients. It is in this perspective that prudent practices and techniques should be adopted in the selection of solutions for biometric recognition. From the findings of this research, we can recommend institutions and organizations that intend to acquire biometric recognition systems to consider evaluating the solution proposals from vendors based on the degree of accuracy, speed of matching as well as the memory space requirements. These factors to a large extent depend on the estimated population size in terms of the number of fingerprint records to be processed at any one time as well as the processing resources available.

This project provides introductory concepts to fingerprint recognition and matching based on minutiae point matching. The tests conducted in this research can be improved to ensure their applicability in an enterprise scale. For instance, the interface can be enhanced to enable matching directly from the WSQ images. The other improvements that can be done include; a) Implementation of parallel processing using multi-threading in the matching algorithm; b) Improvement of the minutiae templates by applying image enhancement routines and c) Using fingerprint classification to speed up the algorithm.

REFERENCES

- [1] 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.
- [2] Delac K & Grgic, M (2004) "A survey of Biometric recognition methods", Electronics in marine. 46th International Symposium, vol. no. pp.184,193.
- [3] Pato J N & Millette L.I (2010), Whither Biometrics Committee; National Research Council, Biometric recognition – challenges and opportunities.
- [4] Jain K., Hong L., Pankanti S., Bolle R., (1997), An identity – authentication system using fingerprints, Proc. IEEE 85 (9) ,pp 1364-1388,
- [5] Qi J., Yang S & Wang Y (2005), Fingerprint matching combining the global orientation field with minutia," Pattern Recognition Letters, vol. 26, pp. 2424-2430,
- [6] Kumar, D. A. & Begum, T. U. S. (2013). A Comparative Study on Fingerprint Matching Algorithms for EVM. Journal of Computer Sciences and Applications, 1(4), 55-60.
- [7] Kenneth K, Stanley J, Michael M, Charles L., Elham T, Michael D., Craig I., (2007), User's Guide to NIST Biometric Image Software, NIST Interagency/Internal Report (NISTIR) – 7392.
- [8] Lukas W. (2009), A minutiae-based matching algorithm in fingerprint recognition systems, journal of medical informatics & technologies vol. 13/2009, issn 1642-6037
- [9] Medina P, Garcia, M., et.al, (2011), Robust fingerprint verification using m-triplets, International Conference on Hand-Based Biometrics, Hong Kong, 2011, pp. 1-5.
- [10] Nadaraja M, Celalettin T, et. al, (2011), Fingerprint Biometric for Identity management International Journal of Industrial Engineering and Management (IJIEM), Vol. 2 No 2, 2011, pp. 39-44 <<http://www.ftn.uns.ac.rs/ijiem/>>
- [11] Germain R. S., Califano A., & Colville S. (1997) Fingerprint matching using transformation parameter clustering. Computational Science and Engineering, IEEE Computing in Science & Engineering, 4(4):42-49,

- [12] Roli B, Priti S, & Punam B. (2011), Minutiae Extraction from Finger print Images – A review, International Journal of Computer science , vol. 8 Issue 5, No 3. Available from: www.ijcsi.org/papers/IJCSI-8-5-3-74-85.pdf:last accessed 12 March 2015
- [13] Saleh A.A., Adhami R.R., (2001), Curvature-based matching approach for automatic fingerprint identification, Proceedings of the Southeastern Symposium on System Theory, pp. 171-175,.
- [14] X. Jiang, W.-Y. Yau, and W. Ser. (2001), Detecting the fingerprint minutiae by adaptive tracing the gray-level ridge. Pattern Recognition, 34(5):999–1013,
- [15] X. Jiang & W. Y. Yau, (2000), Fingerprint Minutiae Matching Based on the Local and Global Structures, in 15th International Conference on Pattern Recognition, Barcelona, Spain, pp. 1038-1041.

AUTHORS

BIBLIOGRAPHY

Name: Mr. Silas Kivuti Njeru

Mr Silas Njeru is a holder of a Bachelor's degree in Computer Science (Egerton University, Kenya) and Master of Science degree in Computer Science (University of Nairobi, Kenya). Currently working as a Manager ICT- Service Delivery at Independent Electoral and boundaries Commission of Kenya. Previously worked at Kenya Revenue Authority Principal Systems Analyst in the ICT strategy and planning section under the Projects Management Office. He has over twelve (12) years of experience in ICT systems analysis, design, software development, software testing, ICT project management and support.



Supervisor Name: Dr. Oboko Robert Obwocha

Dr. Robert Oboko is a holder of a PhD in Computer Science (UoN) and MSc. Computer Science (Free University of Brussels). Currently a lecturer at the School of Computing and informatics at the University of Nairobi. He has wide experience and interests in Technology supported learning: e- and m-learning, instructional design, monitoring and evaluation of technology supported learning projects, adaptive user interfaces for learning, technologies for informal learning and knowledge management such as for small scale farmers

