Centre for Research and Development (CERAD) ***JoST 2018***
The Federal University of Technology, Akure, Nigeria (www.journal.futa.edu.ng)

HS4FI: A Hybrid System for Fingerprint Identification

AWOTUNDE, J.B.[1]; TAOFEEK-IBRAHIM, F.A.[2]; ADEKUNLE, K.O.[3]; JIMOH, R.O.[4] and AFOLAYAN, A.A.[4]

[1]Department of Computer Science, University of Ilorin, Ilorin, Kwara State, Nigeria
[2]Department of Computer Science, Federal Polytechnic, Offa, Kwara State, Nigeria
[3]Information and Communication Technology Center, Federal Polytechnic, Ile-Oluji, Ondo State, Nigeria
[4]Department of Computer Science, Kwara State College of Education, Oro, Kwara State, Nigeria

ABSTRACT: Biometric identification still remains one of the most reliable and consistent methodologies for identification as established over the years from various studies among other authentication systems. Fingerprint biometrics is the most commonly and universally accepted biometric due to its uniqueness among all other biometrics. Minutiae algorithm remains the widely and popularly used method but still needs improvement for better performance due to its poor performance in real-time validation. The problems of minutiae method can be eliminated and its performance enhanced by combining correlation approach. This paper used a hybrid fingerprint matching system with the fusion of minutiae and correlation features. The final matching score is calculated by fusing matching scores of the two algorithms. The False Acceptance Rate (FAR), False Recognition Rate (FRR), and the Mean Evaluation Metrics (MEM) were used for performance evaluation of the proposed system. The hybridized system achieves better results when compared with other related works on commonly used databases Fingerprint Verification Competition (FVC) 2002. The authors obtained FAR = 0.0038, FRR = 0.0156 and an accuracy = 99.25%. The evaluation results show an effective performance over the use of only minutiae algorithm for identification and authentication. Moreso, the results show the improvement in performance of the proposed method and the added advantages of combining both algorithms for identifications systems and performed better in real time identification and verification of large databases.

Keywords: Hybrid system, correlation technique, fingerprint identification, Minutiae algorithm, biometric.

JoST. 2018. 9(2): 123-133.
Accepted for Publication, November 28, 2018

INTRODUCTION

Biometric is the art of identifying, establishing and verifying the individual using hand-geometry, face, fingerprint, palm and DNA (physiological features) or handwriting, gait, speech, and signature (behavioral traits). The methods have been extensively used in entity identification of objects and forensics (prison security and criminal identification) (Chandana, Surendra and Manish, 2015; Satya, Muzhir and Salwa, 2015; Young-Hoo, Seong-Yun, Jong-Hyuk and Mun-Kyu, 2016; Zhigang, Jean-Marie, Christophe and Christophe, 2016). The biometric method has the potential of evolving around new technology and is widely used in different application areas like information system security, banking security, physical access control, custom and immigration, voters' and drivers' registration, and national identification card. The use of fingerprint identification is considered to be the most trustworthy method

*Correspondence to: Awotunde, J.B.; awotunde.jb@unilorin.edu.ng

for authentication (Anil, Yi and Melten, 2007). (Arun, Anil and James 2003; Kumar and Begum 2013) said that using just one matching algorithm or one form of representation will make it difficult to increase the accuracy of that system.

Research suggests that fingerprint provide information about future diseases an individual suffered or developed; thus, fingerprints are commonly used to uniquely identify an individual (Venakatesan and Kumar, 2018). Fingerprint recognition has been researched for a long period of time and it has shown the most promising future in real-world application: however, due to distortions characteristics among different impression of the same finger in real life, fingerprint recognition is still a challenging problem (Devarasan and Manickam, 2017; Helala, Muhammad, Hatim and Mansour, 2018; Mouad, Vivek, Pravin and Gaikwad, 2016; Satya, Muzhir, and Salwa, 2015).

The biometric identifiers cannot be easily misplaced, forged, or shared; therefore, it is considered to be more reliable for person recognition than a traditional token or knowledge-based methods (Kumar and Begum, 2013). This method is one of the old biometric authentications, this account for the various proposed algorithms and models for fingerprint identification and authentication (Mouad, Vivek, Pravin and Gaikwad, 2016; Pakutharivu and Srinath, 2015; Smita, Pradnya and Milind, 2012). The fingerprinting technique being a variant of matching algorithms is quite a robust biometric trait when compared with a face, iris, voice and so on (Helala, Muhammad, Hatim and Mansour, 2018; Pravin and Gaikwad, 2016; Satya, Muzhir, and Salwa, 2015).

Minutiae, correlation matching, and non-minutiae feature-based matching are among the prominent matching algorithms for fingerprint (Mehtre and Chatterjee, 1989). A minutia matching involves finding the best match between databases of known minutiae through a systematic alteration for a subset of minutiae in the input fingerprint. On the other hand, correlation-based matching is a direct alignment between the given two fingerprint images. To ensure that correlations pixel is superimposed, it must be computed between scan fingerprint and template in the database. The maximum level of the correlation factor is inferred as the matching units for the images. In other words, the correlation value is the similarity score between the two images. In other algorithms apart from minutiae matching, ridge outlines, surface information, location fields, and others are used for matching the images template and the input image. Minutiae algorithm with good images quality will always bring more appropriate results, but if the quality of the image is poor, then the algorithm may repeatedly offer inappropriate results that are not good for real-time verification request coupled with extraction difficulty of the technique.

In order to overcome the identified problems, the minutiae based algorithm can be enhanced by combining correlation-based algorithms. This study focuses on hybrid minutia and correlation matching scores for a fingerprint identification system. Therefore, the final matching results were computed through the combination of their matching scores. For the purpose of evaluation, the performance of the proposed system can be calculated by using the Software Application Standard (SPS) and the Mean Evaluation Metrics (MEM).

MATERIALS AND METHOD

The Framework for the Developed Hybrid Fingerprint Identification Model

The hybridized method was used to strengthen the weakness of each algorithm minutiae and the correlation techniques. The hybridized fingerprint matching framework is shown in Figure 1.

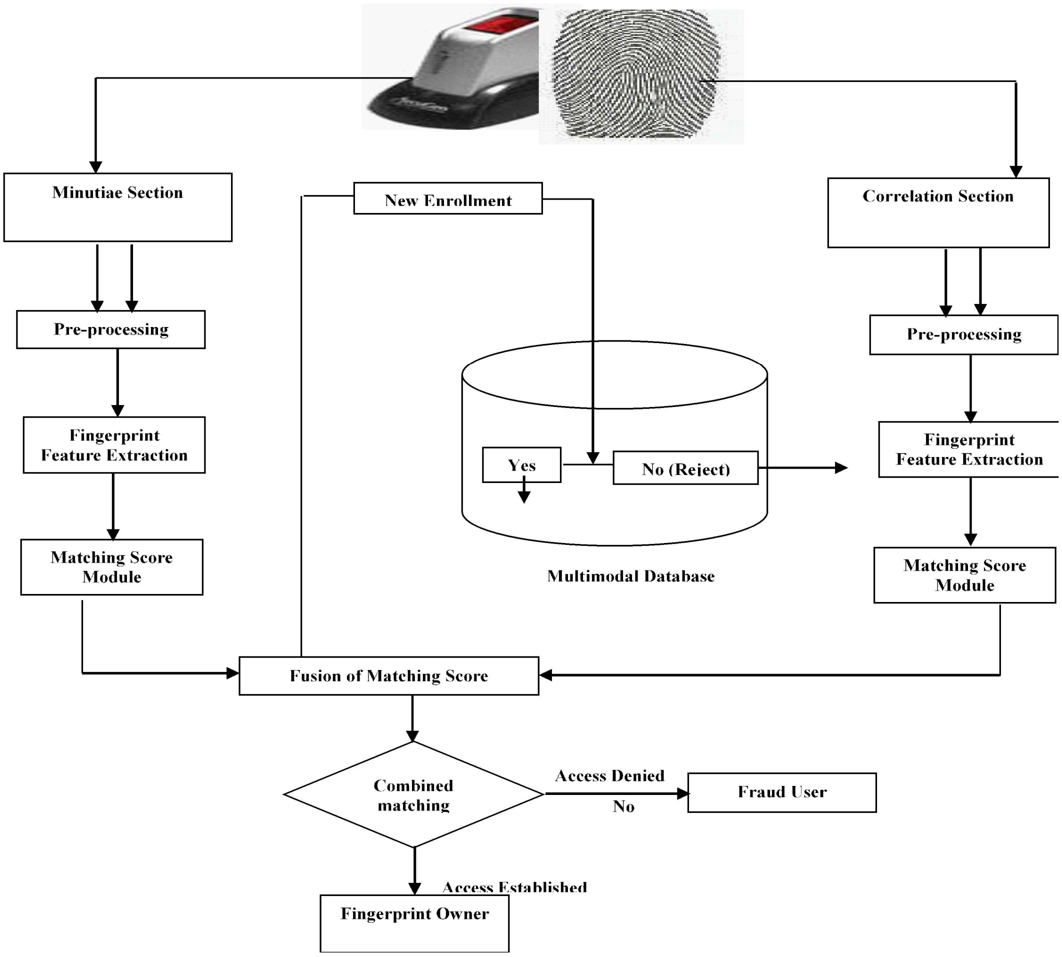

Figure 1: The Framework for the Enrollment and Verification of the System

Fingerprint Matching Methods

The two fingerprint matching algorithms used to form the hybrid system are minutiae and correlation matching methods.

Minutiae Algorithm Method

This is practically the most frequently used fingerprint matching method in all obtainable techniques for identification and verification of fingerprint (Muzhir, 2013). A minutia symbolizes the native configurations of the human fingerprint, the closures, and bifurcations known as minutia. It represents the trivial points of importance in the fingerprint image. The algorithm performs its recognition in two phases: firstly, minutiae feature selection and secondly, minutiae alignment. To reliably select the minutiae important patterns, the algorithm requires overall preprocessing operations. These operations include image improvement, separation and thinning, and false minutiae detection. Minutiae method requires time to remove patterns used for matching this increasing its computational time (Muzhir, 2013; Venkatesan. and Kumar 2018; Kumar and Begum, 2013; Ravi, Kumar, Prasad, Roa and Prakash, 2012; Sangita, 2012).

The fingerprint images are matched using the alignment scheme after removing the real minutiae features. To choose the overall number of matched minutiae from two sets of trivia points, the alignment based technique is used. Minutiae-based features application is suitable for the database that is dedicated for one-to-many matching. Although the method is not suitable for people with no minutiae points or with few points, these are people with an exceptional skin condition, because these people cannot use the system efficiently. A small number of minutiae points can reduce the reason for the security of the system and can also result to regions of confusion that appears due to bad enrollment, fingerprint ridge detail or imaging (false minutia points). Also, the important unit rich partial information of the fingerprints was not properly exploited by the minutiae feature concept.

Fingerprint Minutiae Extraction

Naturally, minutiae m_i is denoted by four variables as presented in equation 1:

$$m_i = (x_i, y_i, \theta_i, t_i) \qquad (1)$$

where:

x_i, y_i – denote the synchronization of the minutiae point,

i – denotes the minutiae direction attained from the resident edge positioning,

t_i – represents the ridge or ridge bifurcation of the minutiae point.

The direction of the minutiae is computed to the X axis and not to the Y-axis, and the position of its point is at the tip of the edge of the valley.

Feature Extraction

The edge thinning stage and binarization are the two approaches of the minutia extraction procedure. The two approaches are mostly used methods and are found to be the simplest. The thinning direct gray-scale extraction has been used by several authors due to the problem of the false minutiae with previous methods.

Ridge Thinning Method

The crossing number (CN) has predominantly dominated techniques used for minutiae extraction since minutiae features extraction precedes the binary ridge image treatment. To have a single pixel wide, the first phase is to binarize before ridges thinning. In order to define the minutiae points, the scanner reads the residential neighborhood of each pixel in the ridge thinned image, using a 3×3 window. From the minutiae point the CN value is calculated by half-sum of the changes between pairs of neighboring pixels pi and $pi + 1$ as in equation 2.

$$CN_{(x,y)} = \frac{1}{2}\sum_{i=1}^{8} |p_i - p_{i+1}|, \qquad p_i = p_9 \qquad (2)$$

The properties used for the crossing number is: 0 = Isolated point, 1 = Ridge ending, 2 = Continuing ridge, 3 = Bifurcation, and 4 = Crossing, the ridge pixel can at that time be classified as a ridge ending, bifurcation or non-minutiae point.

The Segmentation

This is the procedure used to eliminate needless units of the image where the actual fingerprint image is encircled. The relevant units of the image have been designed with the segmentation of the fingerprint, there is no time consumed on preprocessing steps. The variance of the gray-scale intensities and local directional histogram values, gradient coherence values are the operation based that can be used (Maltoni, Maio, Jain & Prabhakar, 2003). The variance based segmentation operation proposed by (Vedpal & Irraivan, 2015) was used and it is calculated by equations 3 and 4 respectively:

$$M(x, y) = \frac{1}{w * w} \sum_{u=\frac{x-w}{2}}^{\frac{x+w}{2}} \sum_{v=\frac{y-w}{2}}^{\frac{y+w}{2}} I(u, v) \qquad (3)$$

$$\sigma(x, y) = \frac{1}{w * w} \sum_{u=\frac{x-w}{2}}^{\frac{x+w}{2}} \sum_{v=\frac{y-w}{2}}^{\frac{y+w}{2}} (I(u, v) - M(x, y))^2 \qquad (4)$$

Orientation Estimation

The calculation of slopes in scanned fingerprint image for orientation field approximation is the simplest and natural way of finding it. Nevertheless, the most frequently used method by many researchers is least mean square method (Devarasan & Manickam, 2017; Zhigang, Jean-Marie, Christophe, & Christophe, 2016; Satya R.P., Muzhir S.A., And Salwa M.N. 2015) for orientation estimation. The images of a fingerprint can be estimated as an oriented texture outline, this advocates that native orientation of the ridges is the orientation field of a fingerprint image. The orientation fields designate the route of the minutiae. The local orientation at pixel (i, j) can be projected by equations 5, 6 and 7 respectively:

$$V_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v), \quad (5)$$

$$V_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v), \quad (6)$$

$$\theta(i,j) = \frac{1}{2}tan^{-1}\frac{V_y(i,j)}{V_x(i,j)}, \quad (7)$$

where

q (i, j) - denote the least square approximation for native orientation at the block center at pixel (i,j),

∂_x , ∂_y – denote the Sobel operator (the slope magnitudes) in the x and y directions.

Normalization

Normalization is used to ease the influence of the fingerprint pressure difference and sensor noise. This method is pixel based procedures that not affect the valley tracks and the clarity of the ridge on the fingerprint and executed on the subdivided image blocks. The mean and standard deviation are used to obtain the blocks conforming to new pixel colors. To reward the strength variation triggered by the fingerprint pressure difference, the procedure is executed on the partitioned blocks rather than the whole image. To normalize pixel value within the block, the sigmoid function is used as in equation 8.

$$N(u,v) = 255 \text{ x } \frac{1}{1 + exp\left[-\frac{I(u,v) - M(x,y)}{\sqrt{\sigma(x,y)}}\right]} \quad (8)$$

Template Matching

Template Matching Score for Minutiae

The number of aligned minutiae of both input and reference fingerprints is used to produce match score in a minutiae-based fingerprint matching system. If two fingerprints have a minimum of 12 matched minutiae, then it is as originated from the same finger especially when considered the forensic guiding principle stated in the study conducted by Muzhir (2013).

Minutiae Matching algorithm aligns two minutiae sets: template T = {m1,m2 ,...,mi} from reference fingerprint and input I = {m1,m2 ,...,mj} from the query and returns match score S (T, I). The minutiae pair mi and mj are taken to be matched only if changes in their position and directions are predefined tolerance distances as in equations 9, 10, 11 and 12 respectively:

$$sd(m_i, m_j) = 1 \leftrightarrow \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \leq r_0 \quad (9)$$

$$dd(m_i, m_j) = 1 \leftrightarrow \min(|\theta_i - \theta_j|, 360 - |\theta_i - \theta_j|) < \theta_0 \quad (10)$$

$$S(T,I) = max\left(\forall \sum_{i=1}^{n} md(m_i, map_m(m_i^{'}))\right) \quad (11)$$

$$md(m_i, m_j) = sd(m_i, m_j).\, dd(m_i, m_j) \quad (12)$$

where:

n – denotes the amount of minutiae points in I input set,

m – denotes the amount of transformation identical to the number of minutiae in T template set.

Template Matching Score for Correlation using Correlation Theorem by Fast Fourier Transform

$$f\ (x,y)\ o\ h(x,y)\ \ F\ (u,v)\ H*(u,v) \qquad (13)$$

f(x, y) examine image with N x M sizes and h(x, y) is the template image with K x L sizes. The correlation theorem is as follows:

1. Reproduce the search and the template image by $(-1)^{x+y}$ centre transformed.
2. Calculate $F\ (u,v)$, the zero padded search image of Fast Fourier Transform (FFT) from (13).
3. Calculate the FFT of the zero padded templates with $H\ (u,v)$ from (13).
4. From $H*\ (u,v)$ (Conjugate of $H\ (u,v)$) reproduce $F\ (u,v)$.
5. The inverse of FFT can be calculated from the result obtained in (4).
6. from step 5 obtain the real part of the result.
7. Use $(-1)^{x+y}$ to multiply the result obtained in step 6.

Figure 2 represents the proposed system flowchart and sequence of execution steps comprising of the matching and enrolment phases.

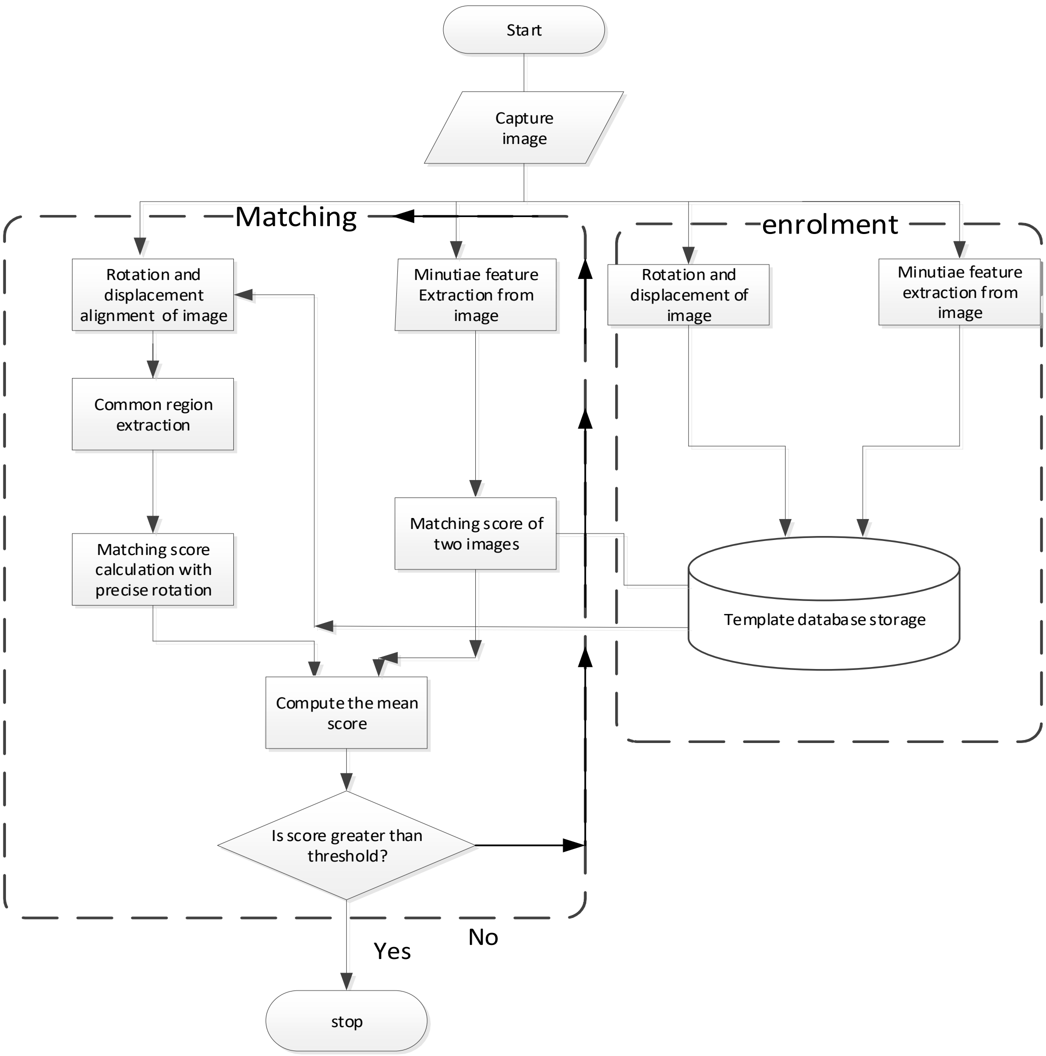

Figure 2: Systems Flowchart

Fusion of Minutiae and Correlation Fingerprint Identification Algorithms

All algorithms for fingerprint matches consist of four basic and important modules; the sensor, feature extraction, the matching, and the decision modules.

In the sensor module, the fingerprint trait is captured as an image in form of raw data. The feature extraction module analyses the image captured to remove a feature set, which is a compressed form of the attributes; the matching module matches the extracted feature set by using a classifier with the pattern in the database to produce a matching score for the image compared from the scanner; and the decision module uses the matching score gotten to either authenticate a claimed identity or define an identity. Resolution can take place in any of the aforementioned modules in fingerprint biometric system.

When the image is analyzed from the fingerprint scanner, the input pattern and template pattern are harmonized to have a matching score (minutiae features). Also, the input pattern and template are matched to obtain its matching score (correlation features). After the computation of both minutiae and the correlation matching scores, next is the hybridization of the matching scores to yield a unique matching score. Rank decision and score level fusion methods were used to fuse together the matching score of minutiae and the correlation algorithms for fingerprint identification.

The matching scores achieved from both minutiae sets and correlation features are computed and pooled to produce a single match score. The sum rule used by (Gnem, Yang and Tian, 2012; Marius, Erro, Pauli, Pauli and Jukka, 2001; Tico, Kuosmanen & Saarinene, 2001; Yuliang, Jie, Xiping and Tanghui, 2003) was adapted for the hybridized system. The Minutiae Matching Score (MMS) and Correlation Matching Score (CMS) represent the matching scores reached from minutiae matching and correlation matching respectively. Hence, Final Matching Score (FMS) represents the final matching score as computed using equation 14.

$$FMS = \alpha \times MMS + (1-\alpha) \times CMS \quad (14)$$

where, $\alpha \in [0, 1]$, and α is set as 0.5

Decision Fusion

Decision fusion was used to fuse the outputs of minutiae and correlation matching scores into a feature vector $[\Delta^1(X), \ldots, \Delta^n(X)]$ and a classifier used to decide if the fingerprint image is valid or invalid. A simple classifier was used to decide the system in equation 15:

$$\mathrm{P(X,Y|C)} = w.\Delta_C^p(X) + (1-w).\Delta_C^f(Y) \quad (15)$$

Finally, the amalgamation of the matching score produces the result $\Delta^*(\mathrm{X.Y})$ that is used for the final decision.

The logical AND was used for the decision fusion of the two matching results. Hence, the two modes must have an output of recognition for authentic classification otherwise the final result is not recognized (that is it is a forgery).

EXPEREIMENTAL RESULTS

Evaluation of the Hybrid Fingerprint Identification System

Table 1 shows the performance of the hybridized system using the previously described frequency-based approach on the same full FVC2002 and compared the result obtained with other research and database has also been for evaluation. This proposed system has resulted in FAR = 0.0038, FRR = 0.0156 and accuracy = 99.25%.

In the developed fingerprint identification system, two hundred and fifty people from five departments (d1, d2, d3, d4, and d5) and five metrics (parameters) were used (p1, p2, p3, p4, and p5) as in Table 1. Statistical Package for Social Sciences (SPSS) 21 Version was employed to obtain the mean scores. This was used with a view to arriving at a reasonable method for evaluating the standardization of system developed for use in a fingerprint identification system.

Table 2 shows the evaluation metrics and their corresponding relative importance. The numerical value is the membership grade assigned to each metric and the cut off mark is 2.5. Any metric that has a weighted mean score below 2.5 not meet the specification of the proposed system.

The standards set for the metrics were symbolized with two letters in Table 3.

Table 1: The percentage of FAR, FRR and Accuracy on FVC2002

Experiments on Database	Recognition Accuracy		
	FAR	FRR	Accuracy
Vincenzo et al. 2010	0.0015	0.0231	98.23%
Yang et al. 2012	0.0150	0.0134	99.01%
Morteza & Ozra, 2013	0.0432	0.0326	89.74%
Mouad et al. 2016	0.0154	0.0137	98.55%
Proposed system	0.0038	0.0156	99.25%

Table 2: Evaluation metric

Evaluation metrics	Representation
Security compliance	P1
User friendliness	P2
Dependability	P3
Platform compatibility	P4
Robustness	P5

Table 3: standards set for the metrics

Symbols	Standards set for the metrics	Relative Importance
US	Unacceptable standard	2.0
MS	Minimum standard	2.5
NS	Normal standard	2.7
BS	Best standard	3.0

Table 4: Fingerprint identification system software standard rating across the selected Departments

	C1	C2	C3	C4	C5
P1	BS	NS	NS	NS	NS
P2	MS	MS	MS	NS	BS
P3	MS	NS	NS	NS	BS
P4	NS	NS	BS	BS	MS
P5	NS	BS	BS	BS	BS

Table 5: Fingerprint identification system software standard rating across the selected Departments

	C1	C2	C2	C4	C5
P1	3.0	2.7	2.7	2.7	2.7
P2	2.5	2.5	2.5	2.7	3.0
P3	2.5	2.7	2.7	2.7	3.0
P4	2.7	2.7	3.0	3.0	2.6
P5	2.7	3.0	3.0	3.0	3.0

Table 6: Overall rating score across the selected Departments

Department	Overall Score
Computer Science D**1**	2.68
Library Science **D2**	2.75
Mass Communications **D3**	2.78
Telecommunication **D4**	2.82
Information Science **D5**	2.86

The opinions of people regarding the system were randomly sampled, an opinion that has the highest frequency in respect of each metric (which reflect the general opinion of people) is recorded as shown in Table 4. The summaries of data from the respondents were extracted to Table 5.

In Table 5, the numerical value replaces the standards set symbols in Table 4. The table gives the relative importance of metrics 1 to 5 across the five departments where the opinions were sampled.

Part of testing the security requirements of the fingerprint identification system, identification was conducted for some selected departments in the Faculty of Information and Communication Science, University of Ilorin, Ilorin. The system was used to identify and validate the participants to check whether they are an impostor or not. Questionnaire method was adopted to gather relevant information about the developed fingerprint identification system from the respondents. The result was weighed using Statistical Package for Social Sciences (SPSS) 21 Version to obtain the mean scores.

Table 7 shows mean evaluation metrics on the validation of the developed fingerprint identification system. The findings from the evaluation of the authentication security requirement of the developed system indicated that the evaluated means were greater than the expected minimum mean of 2.00. This implies that the developed fingerprint identification system satisfied the security requirement of identification. The respondents' rating of the developed system on System Degree of Fingerprint Identification System Index (SDFSI) indicated 2.45 out of the maximum obtainable value of 3.00.

Table 7: Mean evaluation metrics on authentication of the developed fingerprint identification system

S/n	Items	Observed	SDFIS
1	The developed system provides an interface that can be used easily for enrolment and verification.	2.42	
2	The system verifies every individual correctly.	2.37	
3	The developed system prevents a false identity.	2.48	
4	The fingerprint identification system features prevent all unauthorized attempts to the developed system.	2.39	2.45
5	The developed system provides extremely accurate and secured access to voting procedures.	2.53	
6	The developed system makes the votes cast remain secret	2.44	
7	The developed system has the potential of restoring confidence for proper identification of the respondents	2.54	

N=250 $\bar{X} = 3.00$

CONCLUSION

In the developed fingerprint identification system the authors have implemented and hybridize minutiae and correlation algorithms. Minutiae algorithm has been proven to be very robust and provide excellent information for fingerprint matching and the correlation technique showed a favorable approach to fingerprint identification. However, minutiae methods are characterized with poor contrast due to skin dryness, distortion, low contact pressure, artifacts due to noise and wet fingers, and small commonality of the imaged area between different images of the same finger. Moreso, the technique is problematic and computationally intensive task during extraction, as well as showing poor performance if incomplete images were used as input or a poor quality image. In overcoming the aforementioned problems and to enhance minutiae effectiveness, it is very vital and essential to apply an additional sensitive information expedient for matching a fingerprint. Since the correlation technique is suitable for dealing with low-quality images from which no reliable minutiae can be extracted. Also, the correlation technique performs well in the presence of non-uniform shape distortions fingerprints, and it can be used for the image smoothing and for the edge detection. Therefore, minutiae features and correlation features were combined to strengthen each other in terms of their weaknesses. The hybridized system has been tested on matching datasets obtained by the official FVC2002 and obtained the following results of FAR = 0.0038, FRR = 0.0156 and an accuracy = 99.25%. The developed system was evaluated using the Software Application Standard (SPS) and the mean evaluation metrics (MEM). The system is suitable for real-time identification with big image template database. The developed system showed the ability to distinguish between the valid person and an intruder in the presence of damaged or partial fingerprint image.

REFERENCES

Akhil V., and Anoop N. (2014). Learning Minutiae Neighborhoods: A New Binary Representation for Matching Fingerprints, 2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops,

Anil, K.J., Yi .C. and Melten .D. (2007). Pores and ridges: High-resolution fingerprint matching using Level 3 features, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(1), 1-13.

Arun, R. Anil J, and James .R, (2003). A hybrid fingerprint matcher, **Pattern Recognition**, 36, 1661-1673.

Chandana, Surendra, Y., and Manish .M. (2015). Fingerprint Recognition based on Minutiae Information, International Journal of Computer Applications, 120(10), 39-41.

Conti V., Carmelo M., Filippo S. (2010). A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems, IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews,.40(4). 384-395.

Devarasan E. and Manickam A. (2017). A review study on latent fingerprint recognition techniques, Journal of Information and Optimization Sciences, 38:3-4, 501-516.

Jucheng Y., Shanjuan X., Sook Y., Dongsun P., Zhijun F., Shouyuan Y. (2012). Fingerprint matching based on extreme learning machine, Neural Computing and Application 22, 435-445**.**

Helala A., Muhammad H., Hatim A. and Mansour A. (2018). A Large-Scale Study of Fingerprint Matching Systems for Sensor Interoperability Problem, Sensors, 18(4), 1-18

Kumar, D.A. and Begum, T.U.S. (2013). A Comparative Study on Fingerprint Matching Algorithms for EVM, *Journal of Computer Sciences and Applications,* 1(4), 55-60.

Kumar, R. Chandra, P., and Hanmandlu, M (2013). Local directional pattern (LDP) based fingerprint matching using SLFNN", IEEE Second International Conference on Image Information Processing (ICIIP), 493 - 498**.**

Maltoni, D., Maio, D. Jain A.K..and Prabhakar, .S. (2003). Handbook of Fingerprint Recognition. Springer Verlag.

Marius, T., Erro, I. Pauli, R., Pauli K. and Jukka S. (2001). Fingerprint recognition using wavelet features, *IEEE Proceedings,* pp. 21.

Mehtre, B.M., and Chatterjee. B. (1989). Segmentation of fingerprint images. A composite method. Pattern Recognition, 22: 381-385.

Morteza Z., Ozra R. (2013). Combining Gabor filter and FFT for fingerprint enhancement based on a regional adaption method and automatic segmentation, Signal, Image and Video Processing, 1-9

Mouad, M.H.A., Vivek H.M., Pravin, Y. and Gaikwad, A.T. (2016). Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching, 2016 IEEE 6th International Conference on Advanced Computing, 332-339.

Mouad.M.H.A., Vivek H.M., Pravin .Y. and Gaikwad A.T. (2016). Overview of Fingerprint Recognition System, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT 2016), 1-6.

Muzhir S.A. (2013). A Novel Thinning Algorithm for Fingerprint Recognition, *International Journal of Engineering Sciences*, 2(2), 43-48.

Pakutharivu .P. and Srinath M. V. (2015). A Comprehensive Survey on Fingerprint Recognition Systems, Indian Journal of Science and Technology, Vol 8(35),1-7.

Ravi L.K., Kumar, S.S., Prasad, J.R., Rao, B.V.S, Prakash, P.R. (2012). Fingerprint Minutia Match Using Bifurcation Technique, *International Journal of Computer Science and Communication Networks*, 2(4), 478-486.

Sangita K.C. (2012). An algorithm for fingerprint enhancement and matching, *National Conference on Emerging Trends in Engineering and Technology (VNCET-30 Mar'12)*, pp. 308.

Satya R.P., Muzhir S.A., and Salwa M.N. (2015). An Efficient Approach for Fingerprint Recognition, International Journal of Engineering Innovation and Research, 4(2), 307-313.

Senior, A. (2001). A combination fingerprint classifier," IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(10), 1165-1174.

Smita S.M., Pradnya M.S., and Milind V.S.. (2012). Biometrics Authentication Technique for Intrusion Detection Systems using Fingerprint Recognition, International Journal of Computer Science, Engineering and Information Technology, 2(1). 57-65.

Tao X, Chen X, Yang X, Tian J. (2012). Fingerprint Recognition with Identical Twin Fingerprints. PLoS ONE 7(4): e35704.

Tico, M. Kuosmanen, P., and Saarinen, J. (2001). Wavelet domain features for fingerprint recognition," *Electronics Letters*, 37(1), 21-22.

Vedpal, S. and Irraivan, E. (2015). Fingerprint matching algorithm for poor quality images, *The Journal of Engineering*, 20(1), 1-5.

Venakatesan N. and Kumar M.R. (2018). A Survey on Fingerprint Matching Algorithms, International Journal of Pure and Applied Mathematics, 119(7), 851-856.

Young-Hoo J., Seong-Yun J., Jong-Hyuk I., and Mun-Kyu L., (2016). Security Analysis and Improvement of Fingerprint Authentication for Smartphones, Mobile Information Systems, 20(16), 1-12.

Yuliang .H., Jie T., Xiping L., and Tanghui Z, (2003). Image enhancement and minutiae matching in fingerprint verification, *Pattern Recognition Letters*, 24, 1349-1360.

Zhigang Y, Jean-Marie L.B., Christophe C., Christophe R. (2016). A Literature Review of Fingerprint Quality Assessment and Its Evaluation. IET journal on Biometrics, 1-13.