International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 5
ISSN: 2088-5334

A New Approach for Fingerprint Authentication in Biometric Systems Using BRISK Algorithm

Elaf J. Al Taee[#], Zainalabideen Abdulsamad[#]

[#] *Computer Science Dept., College of Education, Kufa University, Najaf, Iraq*
E-mail: elafj.altaee@uokufa.edu.iq, zainalabideena.alsaraf@uokufa.edu.iq

***Abstract*— Nowadays, authentication process in biometric system become most critical task with the expansive of individual information in the world. Where in many current applications, devices and commercial treatments required fingerprint identification process in order to verify the requested services. Most technologies also motivate to this direction. With the increasing of fingerprints uses, there is a need to provide a technique that able to handle the issues that exist in fingerprint acquisition and verification processes. Typically, fingerprint authenticated based on pick small amount of information from some points called Minutiae points. This approach suffers from many issues and provide poor results when the samples of fingerprints are degraded (scale, illumination, direction) changes. However, BRISK algorithm used to handle the previous issues and to extract the significant information from corner points in fingerprint. BRISK is invariant to scale, illumination, and direction changes and its able to pick large number of information when compared with minutiae points. In this paper, BRISK algorithm used based on image based approach, where current recognition matrices are developed and proposed new metrics without need for human interaction. UPEK dataset used to test the performance of proposed system, where the results show high accuracy rate in this dataset. Proposed system evaluated using FAR, FRR, EER and Accuracy and based on selected metrics the proposed system and methodology achieve high accuracy rate than others, and gives a novel modification in authentication task in biometric systems**

***Keywords*— fingerprint matching; fingerprint retrieving; UPEK; BRISK algorithm; FAST detector; biometric system.**

I. INTRODUCTION

The expansive growth of the information and frequent data randomly added to the internet and other storage media, and many other challenges made the security accomplishing very critical task. Traditional security systems either working based on knowledge methods (e.g. Pin code, Password, etc.) or based on token methods [e.g. personal ID card, passport, etc.]. Both methods may suffer from reliability and authentication issues, and these methods typically required foolproof personal identification. The drawbacks of traditional security systems are the methods could be prone at any time, in such a way that the password could be lost, forget, or hacked at any time [1]. In token method, the authorized samples could be stealing, duplicated, or lost from the secondary storage media in databases. However, current security system used biometric based methods such as iris, handwriting, fingerprint, sound, DNA, etc. These methods typically proposed to handle the drawbacks of traditional security systems, and to provide a robust identification method with high uniqueness accuracy than traditional methods [2]. Biometric based method also characterized by the following advantages as follow: first, person identification process performed in very fast manner than traditional methods. Second, ease of use than others. Third, provide high accuracy, precision, trust worthy and economics than traditional knowledge or tokens methods. Biometric based authentication system commonly divided into four mainly steps which are, sample capture, feature extraction, feature matching and then authentication decision, the following figure (fig.1) shows the block diagram of general biometric based authentication systems [3, 4].

In the figure (fig.1) at first step, the general biometric system typically required authenticated samples where every acquired sample, typically submitted as an image sample. Image sample commonly acquired through certain biometric device, and at feature extraction, the feature of acquired sample is stored in database. Finally, these features compared with the query one to either authenticate the individual sample or rejected it [5]. Among all other biometrics identifier, fingerprint is oldest and commonly used technique to provide a robust human identifier method. Feature extraction step is a significant process in every pattern recognition system, where the extracted features play an important role in every identification step.

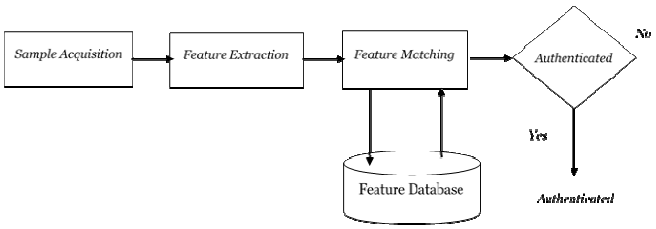

Fig.1: Block Diagram of General Biometric Based System

There are two types of features as discussed later, can extracted from fingerprint samples, which are global features and local features. Global features typically focused on extracting structure surface patterns, then use the core point property, fingerprint authenticated. Local features typically focused on extracting the property of minutiae points. Local feature considers more robust than global features, for authentication tasks [6]. Therefore, this paper introduce a robust algorithm called Binary Robust Invariant Scalable Key points (BRISK) algorithm. This algorithm working after converted the fingerprint into grayscale space, then using binary nature, feature descriptor constructed. Hence, by use BRISK, the proposed system developed to perform the matching in efficient manner.

II. Material and Method

A. Fingerprint Authentication Challenges

The quality of fingerprint plays an important role in authentication step, where the quality of fingerprint either affected by the way of image capturing, or such other internal or external factors. Commonly fingerprint surface degraded by such reasons (e.g. skin cracks, miss fingers, acquisition accuracy, etc.). Typically, fingerprint degradation is divided into two classes are sensor factors and fingerprint factors. Sensor factors typically concern with the resolution and the degradation at this step could not avoided (e.g. dirtiness, noise) [7]. Fingerprint factors, these factors are concern with the human skins and all the factors that affected on fingerprint acquisition (e.g. skin dryness, transformation issue, dirtiness, etc.). Biometric based authentication system required several steps includes the following: fingerprint acquisition, feature extraction, feature descriptor, matching calculation, and finally authentication (recognition and identification). Actually, the fingerprint from first step until last step are degraded by semantic metrics, where many fingers may look like similar to each other, while in fact these fingers are different. Fingerprints feature extraction required a strongest algorithm for finding features that have discriminative power [8]. Fingerprint surface typically constructed from three structural components: Loop, Delta and Whorl. Moreover, most of global features shows that two adjacent features from candidate images are similar in such way. However, global features techniques are not convenient for fingerprint recognition or authentication because the valleys and ridges in fingerprints not recognized in global description of fingerprint images [9].

B. Fingerprint Matching Techniques

Fingerprint matching techniques plays an important role in order to authenticate the individual person. Typically, fingerprint authentication process need an accurate algorithm that able to extract strongest features from candidate samples and infer the result if the matching has accrued. Hence, matching of fingerprint based on the type of feature that extracted from fingerprint sample itself can divided into two classes, which are: image based and minutiae based methods [10, 11]. In minutiae based method, the minutiae points should have detected in the given candidate samples, after that features extracted from these points, and finally an approximate measure used to find the accumulative distance among the features that extracted priori from both candidate minutiae points for the given samples [12]. The following figure (fig.2) shows the minutiae points' detection process in fingerprint sample.

Fig.2: Detection of Minutiae Points in Fingerprint Sample

Minutiae based approach suffer from critical issues, where the complexity of this approach is very high due to its required high computation. In addition to the previous issue, this approach required good quality fingerprint samples, so when the samples have degraded by such sources, the accuracy will become very low. However, many issues could have occurred if the quality of fingerprint is not acceptable, where the minutiae points not detected properly. Therefore, to overcome the previous issues, image based method used, where the local features detection algorithms used to extract feature vectors from the candidate fingerprint images, then distance measure calculated to infer if the candidate are similar or not [13]. In such biometric systems, which used fingerprints as a base for authentication task, in these systems the authentication has performed based on matching between the candidate samples. In many authenticating systems that working based on image based approach, the given fingerprint samples enhanced when entered to the system, this step is very important to perform high matching accuracy. Then the feature vectors are stored in database in appropriate manner, and when such sample given to verified, the extracted feature vectors compared to those in database to infer a decision regarding it. Most popular local descriptor algorithms used with biometric systems are: SIFT [14], SURF [15], BRISK [16], ORB [17], MSER [18], etc., and the working of these algorithms can be summarized in five steps are: feature detection, feature extraction, feature representation, feature indexing, and finally feature matching. Typically, features could be a pixel (interest points), corners, blob, etc., based on the type of algorithm used. The following figure (fig.3) shows the feature detection in such given fingerprint sample.

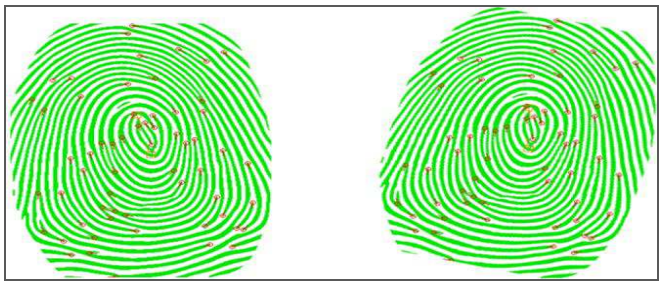

Fig.3: Detection of Local Features in Fingerprint Using SURF Algorithm

C. Overview Of Brisk Algorithm

BRISK algorithm (Binary Robust Invariant Scalable Key-points), one of the robust algorithm used in computer vision application such as object detection, object recognition and image classification. BRISK comes from the idea of detecting the interest regions in the given image, so this research work supposes the best matching in fingerprints can calculated using this algorithm [19]. The heart of BRISK algorithm is FAST detector (is a feature detector method, and called Features from accelerated segment test). FAST is a corner detection method where its computation faster than other well-known detection methods like SUSAN, DOG, SIFT, Harris. FAST corner detector uses 16 circles to classify the candidate pixel if is it a corner, then every surrounding pixel labeled from 1to 16 in clockwise mode as shown in the following figure (fig.4) [20].

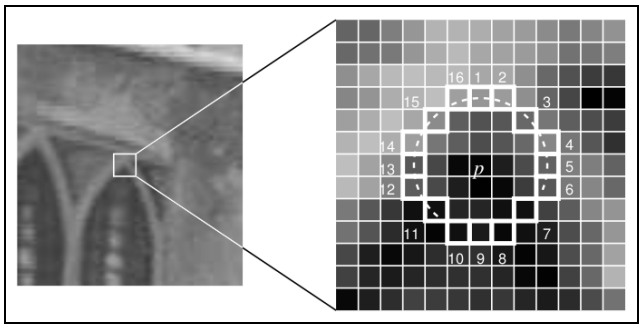

Fig.4: Corner Detection with FAST Detector

For every candidate pixel in the circle, if the set of N contiguous pixels are brighter than the candidate pixel intensity plus the threshold value (T), or all pixels darker than the candidate pixel intensity minus threshold value (T), then the candidate pixel (P) is a corner. BRISK typically detect corner pixels in different scale space in pyramid mode in such level calls (Octaves), and this make the BRISK algorithm strongest against image scale changes. It is important to note that the BRISK algorithm actually uses 9-16 masks to scaling the image in pyramid mode, which is equivalent to scale space in consecutive manner [21]. FAST detector in BRISK algorithm has applied on each octave and intra-octave (generally 4 octave levels), and the threshold has calculated from contiguous pixels, and in every octave level, the potentially interest regions of interest is detected. Every point belonging to interest regions is subjected to nun-maximum suppression, and points is selected if satisfy the maximum condition (with respective to the pixel neighbors). After the key points detection step, BRISK applies sampling patterns that rotated by (α) around the interest point (key point) [18]. These information uses in interest point descriptors to pick the information of rotation and scale normalization. BRISK bit vector descriptor for every interest point (P) constructed by performing all short distance intensity calculation among the pixel pairs $\left(P_i^{\alpha}, P_j^{\alpha}\right)$ that belong to (S) where S is a subset of short-distance pairings. BRISK algorithm estimate the intensity values at each interest point also to represented in the bit vector, the intensity of sampling points $I\left(P_i, \sigma_i\right)$ and $I\left(P_j, \sigma_j\right)$ is smoothed by using Gaussian function, and used to estimate the local gradient of pairs point as in the following equation Eq.1 [19].

$$G(P_i, P_j) = (P_j - P_i).\frac{I(P_j, \sigma_j) - I(P_i - \sigma_i)}{\left\|P_j - P_i\right\|^2} \qquad (1)$$

\Then each bit in the bit-vector descriptor of pairs point $\left(P_i^{\alpha}, P_j^{\alpha}\right)$ is corresponding to,

$$B = \begin{cases} 1, & I\left(P_j^{\alpha}, \sigma_j\right) > I\left(P_i^{\alpha}, \sigma_i\right) \\ 0, & otherwise \end{cases} \quad \forall\, I\left(P_i^{\alpha}, P_j^{\alpha}\right) \in S \qquad (2)$$

quality of matching between the candidate's samples, in such a way the decision of matching typically picks based on matching score value as discussed in later sections.

D. Related Works

Local descriptors algorithms used commonly in many computer vision applications such as object recognition, object tracking, and many others. In biometric systems, local features algorithms applied successfully in many objectives, where image based mode used frequently in these applications. In this section, the most related works illustrated based on fingerprint recognition and matching. In 2009, Kant and Nath [22], they used singular delta point to identifying the individual persons based on his fingerprint central point, which is also used to distinguish it from other samples. In 2010, Sanjekar and Dhabe [23], they used Haar wavelet for sampling fingerprint images into 3 levels to extract the statistical features from it, then distance measure used for comparison purpose. In 2014, Kumar et all [10],

ROI has been used for extracting and constructing the feature vectors, then Euclidian distance, Histogram intersection, Chi-square distance and Support vector machine) to infer the matching score. In 2015, Zhong and Peng [24], SIFT algorithm and LSH function used in fingerprint authentication system, where LSH used to hashing the feature vectors in database, then distance measure used to find the index of similar candidates based on using multi-template image feature fusion technology. In 2015, Saini et all [25], SURF algorithm has been used for fingerprint authentication based on calculating the distance percentage among query fingerprint sample and the whole samples in database. In 2016, Dubey et all [26], they combine SURF and PHOG methods to enhanced the accuracy of matching performance and improve the quality of recognition process. In this paper, BRISK is one of the robust algorithm used for pattern recognition tasks, the modification has performed in recognition score. The traditional recognition algorithm typically recognizes the objects with our prior decision, however, in this paper two important metrics have proposed to improve the performance of recognition process. These metrics are able to give a decision regarding the matching score without refer to user perception.

E. Proposed System

In the proposed system, the recognition process has enhanced to handle some issues that exist in fingerprint samples. The first step in proposed system includes contrast enhancement to adjust the brightness in such samples. This process could be able to avoid such degradation when fingerprints samples converted into grayscale color space. After the feature descriptors construction step, the feature vectors are stored their matrices where the dissimilarity has calculated among these feature vectors. Typically, the feature vectors are not identical in both matrices, hence the accumulative distance value is considering by take the dissimilarity of all feature vectors. The general block diagram of proposed system shown in the following figure (fig.5) where the proposed methodology represented in it.

As shown in the figure (fig.4), after the pairwise distance has calculated the result of this process involve a number of valid feature vectors that meet one or more samples in vectors database. The result of this calculation differently involve noise-matching features, this actually occurred when such feature vectors are similar to more than one vectors in candidate image. However, of course in fingerprint samples where the intensity patterns could be reflecting similar to other feature vectors when such structural content identical. So in the proposed system, the fingerprint analyzed for choosing a robust local descriptor algorithm to represent the features in efficient way, and because the fingerprints do not involve variant colors in its texture. BRISK algorithm has selected to capture as possible as large number of corner points. In image analysis field, the most robust features can be used to compare the identical patterns between two samples is by take the corner points due to these corners are not repeated arbitrary. Thus, the distance is not considering for the first matching vector, but also navigate to consider the second nearest vector. Generally, this process occurred by KNN algorithm where in our case the (K) value in KNN algorithms is equal to (2).

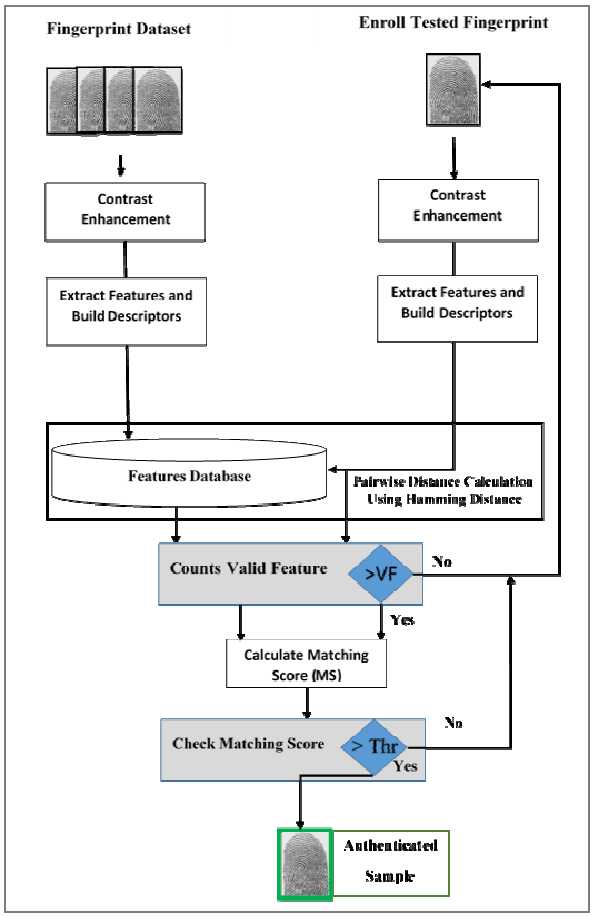

Fig.5: The Proposed System Block Diagram

Therefore, the distance percentage calculated to reflect the ration of distance between the two selected vectors based on Eq.3.

$$D(P_i, P_j)_{Percentage} = \frac{V1_{pj}}{V2_{pj}} \quad (3)$$

Now, to calculate the average of minimum distance among the feature vectors, minimum distance is accumulating for the whole feature vectors. This process helps to find the valid feature score, which used in forthcoming process by using Eq.4.

$$Avg_{D(P_i,P_j)} = \frac{1}{N}\sum_{i=1}^{N} min\ D(P_i,P_j) \quad (4)$$

After the percentage of whole vectors calculated using the above equation, next step calculates the average percentage for all vectors (N) by using the following equation Eq.5.

$$Avg\ (D(P_i,P_j)_{Percentage})_e = \frac{1}{N}\sum_{i=1}^{N} D(P_i,P_j)_{Percentage} \quad (5)$$

Now to find the valid features between the candidate samples, the average of distance values is calculated, this value used to check if there is a sufficient number of

matching features are existing or not, and can be calculated as in the following equation Eq.6.

$$Match_{VF} = \frac{\left[Avg_{D(F_i,F_j)} + Avg\left(D(F_i,F_j)_{Percentage}\right)_c \right]}{2} \quad (6)$$

Final step in proposed system involve matching score calculation, in other words, what is the score value that reflected from the candidate samples matching. Actually, the metric used for compute the matching score return a fuzzy value, where the values ranged from (0 to 1). The feature vectors that fall from previous step are not actually the real matched features. A new model has applied to test the similarity validation of these features, and this applied by using RANSAC algorithm. RANSAC proposed fit model in every iteration and consider the matched vectors are points belongs to model space, then if the feature vectors are really similar, then its shown in all iteration contiguous than others and these features called inlier features (real features) [27]. If the applied model shows, some features are far away from the corresponding features, then these features called (outlier or noise features) as shown in the following figure (fig.6) where the inlier features are fit the proposed model.

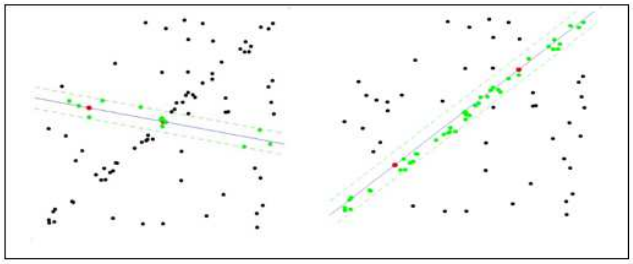

Fig.6 Fit Data Points (Feature Vectors) In Space to Suggested Model Using RANSAC

Next step after perform RANSAC algorithm, the Proposed system uses a matching score metric which return a fuzzy set value that represent how much the matching has occurred between the corresponding samples. The matching score simply uses a neat formula to calculate the matching score value based on the following equation Eq. 7.

$$Ms = \left(\frac{IF}{T_{VF}}\right) > Thr \quad (Threshod) \quad (7)$$

Where (IF) is the inlier feature vectors that produced from the previous step (after applying RANSAC algorithm), and (T_VF) is the number of total valid features before applying the RANSAC algorithm. However, if the (Ms) is greater than proposed threshold, the tested fingerprint is verified with the corresponding fingerprint sample that satisfy the threshold [28].

III. Results and Discussion

A. Experimental Results

In order to check the performance of proposed system, (UPEK [29]) dataset used for this purpose. UPEK involves 128 fingerprint samples belongs to 16 individual persons, for every person there 8 samples, some samples may exist in degradation status. The main GUI involve two kinds of fingerprint authentication are pairwise fingerprint authentication and multi-fingerprint authentication. In first type, only two fingerprints compared at each time (one selected from dataset either arbitrary or based on prior information) and one enrolled through sensor, then the proposed system checks the matching between these samples. Second kind concern with find the most similar fingerprint samples, this part look like retrieving similar images in traditional CBIR systems. The following figure (fig.7) views the interest points (corner points) for the candidate fingerprints using proposed system.

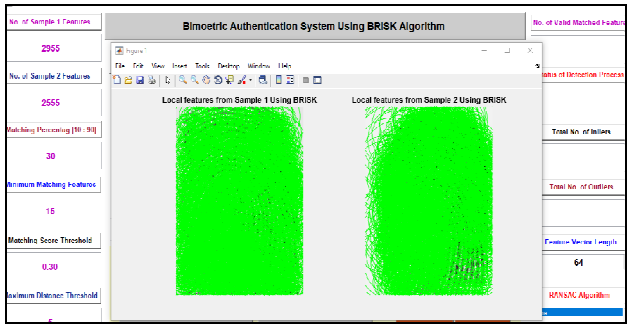

Fig.7: Interest Points Detection in Candidate Samples using FAST Detector

After the interest point detection step as shown in the above figure (fig.6), pairwise distance calculation among feature vectors calculated based on Hamming distance metric, and by following the previous measures the decision is made based on threshold value. In the following figure, (fig.8) two samples selected from different persons and it has shown that the enrolled fingerprint not authenticated.

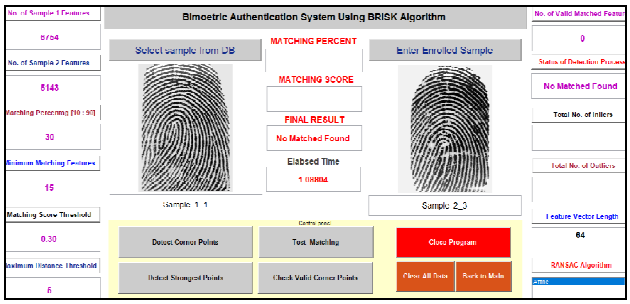

Fig.8: Rejection of Fingerprint in Proposed System

In the figure (fig.8) we can notice that the number of corner points (interest points) is very large, these points typically sufficient to pick the patterns of every sample, and because the fingerprint structural involve many details, the number of points became very large. However, it is able to distinguish the individual samples from others in high accuracy rate as shown above. In the following figure (fig.9) the enrolled fingerprint sample is authenticated and the decision made by consider the matching score threshold as shown below.

The proposed system also provides a facility to find all the relevant samples in database as shown in the following figure (fig.10), where the outer loop is parse all relevant feature vectors in database and also its shown the relevant result matching score.

In the figure (fig.10), the relevant result matching score compared with the matching threshold, and if the matching score less than threshold, the result will be shown in the main GUI as verified sample.

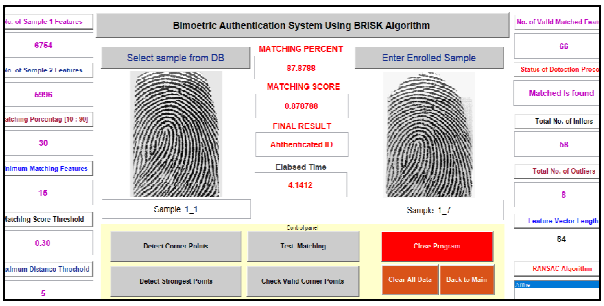

Fig. 9: Fingerprint Authentication in Proposed System

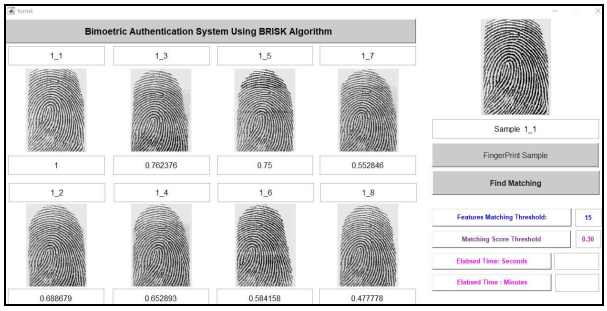

Fig.10: The Relevant Results of Fingerprint Sample in Proposed System

B. Results Evaluation

Performance evaluation is a significant step in any proposed system; however, in this paper there are four metrics used to evaluate the performance of proposed system, which are FAR, FRR, EER and Accuracy [30].

1) FAR (False Acceptance Ratio):

FAR can defined as a ratio of false acceptance authenticated samples, and can calculated by take the ratio of false accepted samples to the total related samples in database.

$$FAR = \frac{False\ Acceptance\ Fingerprints}{Total\ number\ of\ Related\ Fingerprints\ in\ DB} \times 100\ \% \quad (8)$$

2) FRR (False Rejection Ratio):

FRR represent the rejection rate of system to those fingerprints that should not rejected. FRR can calculated by take the ratio of the number of false rejected samples to the total related samples in database.

$$FRR = \frac{False\ Rejection\ Fingerprints}{Total\ number\ of\ Related\ Fingerprints\ in\ DB} \times 100\ \% \quad (9)$$

3) EER (Equal Error Ratio):

EER can defined as the ratio of FAR and FRR, and its consider an optimal score in the case of FAR is equal to FRR.

$$EER = \frac{FAR + FRR}{2} \times 100\ \% \quad (10)$$

4) Accuracy (ACC)

AC is the ratio of the corrected classified fingerprint samples, in other words is the system able to classify fingerprints to their correct classes from the whole classes in database. Therefore, in biometric system based on fingerprints, AC is a metric of classified the fingerprint that belongs to the same person from whole other samples.

For evaluating the proposed system, (10) individual fingerprint samples are consider from UPEK dataset, where every individual person there are (8) samples divided into (3) samples in training phase and (5) samples in testing phase. The following table (Table 1) shows the execution time in millisecond for the whole steps in proposed system.

TABLE I
EXECUTION OF PROPOSED SYSTEM STEPS IN MILLISECOND

Proposed System Level	Elapsed Time in Millisecond
Contrast Enhancement	1.11
Interest Points (Corners) Detection	0.92
Feature Vectors Building	0.78
Pairwise Distance Calculation	1.10
Eliminate Outliers	2.15
Feature Vectors Matching	1.21
Total	7.27

TABLE II
PERFORMANCE EVALUATION OF PROPOSED SYSTEM USING UPEK DATASET

Sample Name	Performance Evaluation in Training Phase				Performance Evaluation in Testing Phase			
	FAR	FRR	EER	AC	FAR	FRR	EER	AC
Fingerprint 1	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0
Fingerprint 2	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0
Fingerprint 3	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0
Fingerprint 4	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0
Fingerprint 5	0.03	0.04	0.04	99.80	0.0	0.0	0.0	100.0
Fingerprint 6	0.01	0.01	0.01	99.90	0.0	0.0	0.0	100.0
Fingerprint 7	0.08	0.08	0.08	99.40	0.04	0.04	0.04	99.80
Fingerprint 8	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0
Fingerprint 9	0.06	0.06	0.06	99.35	0.0	0.0	0.0	100.0
Fingerprint 10	0.02	0.02	0.02	99.90	0.0	0.0	0.0	100.0
Average	0.02	0.02	0.03	99.83	0.004	0.004	0.004	99.98

The following ROC graph in figure (fig.11) shows the evaluation curves of FAR, FRR and EER of proposed system in Training and Testing Phases.

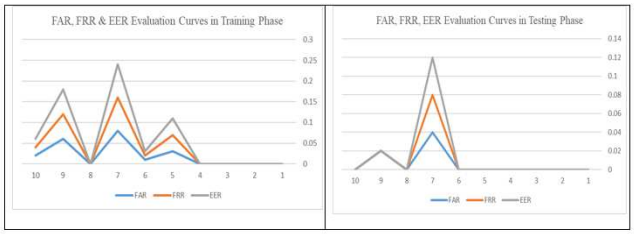

Fig.11: Proposed System Evaluation Graphs in Training and Testing Phases

The following figure (fig.12) show the proposed system authentication rate for the given samples with respect to time in millisecond.

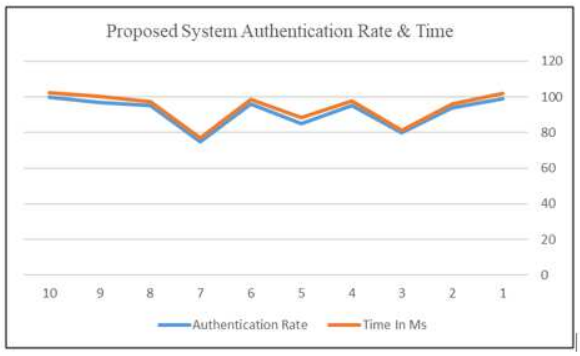

Fig.12: Authentication Rate and Time of Proposed System

IV. CONCLUSIONS

Authentication task in biometric systems is a very critical process due to the challenges that exist in biometric samples. Fingerprint identity used commonly in many legal operation as unique identifier for individual property. However, fingerprint still currently one of the most robust identifier for peoples around the world. With the expansive development in information technology field, there is a need to develop technique that able to recognize, identify and authenticate such individual human from large number of identities that stored in database. Thus, in this paper one of the most robust algorithm used to build the proposed system, which provide a solution for such issues that exist in traditional biometric systems that works based on fingerprint identifier. Where in these systems, the authentication process is fail when samples degraded in such manner (scale change, illumination change, rotation). The proposed system by adopts such metrics is able to handle these issues and provide a novel modification in biometric system where the authentication decision made based on dynamic metrics without need to human interaction. The proposed system performance tested by using UPEK dataset and evaluated using FAR, FRR, EER and Accuracy metrics, which used frequently to evaluate pattern recognition systems especially the biometric systems.

REFERENCES

[1] Yoichi Seto, “Development of Personal Authentication Systems using Fingerprint with Smart Cards and Digital Signature Technologies", Seventh International Conference on Control Automation Robotics and Vision (ICARCV’OZ), Singapore, pp: 996-1001, 2002.

[2] A. C. Leniski, R. C. Skinner, S. F. McGann, and S. J. Elliott, "Securing the Biometric Model," presented at Security Technology, in proceedings of the 37th IEEE Annual 2003 International Carnahan Conference, 2003.

[3] Karthik Nandakumar, " Multi-biometric Systems: Fusion Strategies and Template Security", PhD Thesis, Department of Computer Science and Engineering, Michigan State University, USA, pp: 1-202, 2008.

[4] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain, "Biometric Cryptosystems: Issues and Challenges", in proceeding of IEEE, Vol.92, No.6, pp: 948-960, 2004.

[5] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B.V.K.V Kumar, "Biometric Encryption", in R.K. Nichols, editor ICSA Guide to cryptography, McGraw Hill New York, pp: 42-46, 1999.

[6] Umma Hany, Lutfa Akter, "Speeded Up Robust Feature Extraction and Matching for Fingerprint Recognition", 2nd International Conference on Electrical Engineering, Information and Communication Technology, IEEE, 2015.

[7] Ami M Patel, Rikin Thakkar,” Object Based Image Retrieval from Database using Local and Global Features”, IJIRT, Vol.1, No.12, 2015.

[8] Guesmi, H., Trichili, H., Alimi, A.M., Solaiman, B, “Curvelet Transform-Based Features Extraction for Fingerprint Identification”, in Biometrics Special Interest Group (BIOSIG), BIOSIG-Proceedings of the International Conference of the IEEE, pp. 1-5, 2012.

[9] R. Shakthi Pooja, S. Swetha,S., K. Alice, “Robust Fingerprint Matching Using Ring Based ZERNIKE Moments: A Survey.” International Journal of Engineering Science and Research Technology, Vol. 6, No. 3, pp. 329-340, 2017.

[10] R. Kumar, P. Chandra, M. Hanmandlu: "Rotation Invariant Fingerprint Matching Using Local Directional Descriptors", International Journal of Computational Intelligent Studies, Vol. 3, No. 4, PP. 292-319, 2014.

[11] P.H. Saini, Rakesh S., “Perspective of Fingerprint Recognition Using Robust Local Feature.” International of Science and Research, Vol. 4, No. 6, pp. 2428-2433, 2015.

[12] Sheng Li, A. C. Kot, “Fingerprint Combination for Privacy Protection", IEEE Transactions on Information Forensics and Security, Vol.8, No.2, PP. 350-360, 2012.

[13] Karthik Nandakumar, " Multi-biometric Systems: Fusion Strategies and Template Security", PhD Thesis, Department of Computer Science and Engineering, Michigan State University, USA, pp: 1-202, 2012.

[14] David G. Lowe, "Distinctive Image Features from Scale-Invariant Key points", International Journal of Computer Vision, Vol.60, No.2, pp 91-110, 2004.

[15] H. Bay, A. Ess, T. Tuytelaars, and L. V. Gool, 2008. "Speeded-Up Robust Features (SURF)" Journal of Computer Vision and Image Understanding, Vol.110, No.3, PP.346-359.

[16] Leutenegger S. Chli M., Siegwart R. Y, "Binary Robust Invariant Scalable Key-Points", Journal of Computer Vision, (ICCV), IEEE, pp 2548-2555, 2011.

[17] Rublee, Ethan; Rabaud, Vincent; Konolige, Kurt; Bradski, Gary, "ORB: an efficient alternative to SIFT or SURF", Journal of Computer Vision, (ICCV), IEEE International Conference on Computer Vision (ICCV), 2011.

[18] J. Matas, O. Chum, M. Urban, T. Pajdla, "Robust Wide Baseline Stereo from Maximally Stable Extremal Regions.” Proc. of British Machine Vision Conference, pp 384-396, 2002.

[19] Meenu, Surender Singh, " Enhanced the Fingerprint Matching using BRISK, SURF & MSER” International Journal of Advance Research in Computer Science and Management Studies, Vol.4, No.7, pp 78-83, 2016.

[20] Leutenegger, Stefan, Margarita Chli, and Roland Y. Siegwart. “BRISK: Binary robust invariant scalable keypoints.” Computer Vision (ICCV), 2011 IEEE International Conference on. IEEE, 2011.

[21] L. Najman and M. Couprie: "Building the component tree in quasi-linear time" Archived 2011-04-09 at the Wayback Machine.; IEEE Transaction on Image Processing, Volume 15, Numbers 11, pp 3531-3539, 2006.

[22] Kant C., Nath R., “Reducing Process-Time for Fingerprint Identification System”, International Journals of Biometric and Bioinformatics, Vol.3, No. 1, pp. 1-9, 2009.

[23] P. S. Sanjekar, P. S., Dhabe, “Fingerprint Verification Using Haar Wavelet”, 2nd International Conference on Computer Engineering and Technology, IEEE, Vol.3, pp. 361-365, 2010.

[24] Yunfei Zhong, Xiaoqi Peng, “SIFT Based Low Quality Fingerprint LSH Retrieving and Recognition Method.” International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8, No. 8, pp. 263-272, 2015.

[25] P.H. Saini, Rakesh S., “Perspective of Fingerprint Recognition Using Robust Local Feature.” International of Science and Research, Vol. 4, No. 6, pp. 2428-2433, 2015.

[26] Rohit K. Dubey, Jonathan, V. L.L. Thing, “Fingerprint Liveliness Detection”, Information Forensics and Security, Vol.11, No.7, 2016.

[27] Martin A. Fischler, Robert C. Bolles, “"Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography", Comm. ACM., Vol.24, No.6, pp: 381-395, 1981.

[28] Tawfiq A. AL-asadi, Ahmed J.Obaid, “Object detection and Recognition by Using Enhanced Speeded Up Robust Feature” International Journal of Computer Science and Network Security, Vol.16 , No. 4, pp. 66-71, 2016.

[29] UPEK fingerprint Database, BERKELEY, Calif.--(Business Wire) --May 3, 2006, UPEK, Inc. Steve Hahm, downloaded from http://www.advancedsourcecode.com/fingerprintdatabase.asp, last updated 2012.

[30] Ertugrul Bayraktar, Pinar Boyraz, “Analysis of Feature Detector and Descriptor Combinations with a Localization Experiment for Various Performance Metrics” Turkish Journal of Electrical Engineering & Computer Sciences, pp. 2444 - 2454, 2017.