Cascaded Biometric System Based on Fingerprint and Retina for User Identity Recognition

T.S. Sasikala, K. Siva Sankar

Abstract—This work proposes a cascaded biometric system based on both the fingerprint and retinal features of the user. This work compares the identity of the user with the feature database based on a single biometric and when mismatch is observed, the second biometric is utilized for user identity recognition. This idea conserves time and supports when a single biometric is not conscribed properly. This phase does not rely on a single biometric and the performance of this phase is better in terms of security. The performance of the work is tested in terms of accuracy, sensitivity, specificity and time consumption rates. The proposed approach outperforms the existing approaches.

Keywords – Biometric system, fingerprint, retina.

1. INTRODUCTION

The standard security systems of identity verifications rely on passwords or physical identity cards. The main drawbacks associated with these approaches are that the passwords can be misused or stolen from the legitimate users. At this scenario, biometrics based security systems come into picture and these systems are more reliable than the traditional identity verification systems. Basically, the biometric systems can be classified into two categories, which are unimodal and multimodal biometric systems.

The biometric system presented in the previous chapter performs better, however when there is a fault in the conscription phase, then the entire task of recognition goes in vain. As the process of recognition is closely related to security, granting access to illegitimate users or denying access to legitimate users creates a serious impact.

However, when the user identity recognition system relies on a single biometric, the possibility of getting false acceptance and false rejection rates is greater. This issue is addressed by presenting a user identity recognition system based on cascaded biometric system in this chapter. The cascaded biometric system relies on both retina and fingerprint.

As the name suggests, cascaded biometric system processes the biometric one after the other. When the user cannot be recognized with a single biometric, then the second biometric is collected and processed. This idea conserves time and the computational complexity is reduced. The proposed approach is not based on a single biometric and hence, the false acceptance and false rejection rates are minimized.

The proposed approach is classified into two stages and they are conscription and recognition phases. The conscription phase collects the biometrics such as fingerprint and retina of the user and the features are extracted from the biometric. The feature vector is formed and stored in the database.

The recognition phase is meant for verifying the identity of the user. The recognition phase collects the biometric data from the user and the features of the biometric are collected. The so collected features are compared with the feature database and the access is given, when the features are matched. In case of mismatch, the second biometric, which is the fingerprint is extracted and compared with the feature database.

This cascaded approach results in better results than the previous approach, which presents the unimodal biometric system. The entire system is based three basic phases, as in the previous chapter and they are pre-processing, feature extraction and recognition. The same phases are involved for both the biometrics and the contributions of this research are presented as follows.

- The cascaded biometric system for user identification relies on two different biometrics of the user and hence, when the recognition of a biometric fails the second biometric complements the other.
- The second biometric is processed only when the first biometric cannot be recognized. This idea conserves time and reduces the computational complexity.
- As this work performs double check for recognizing the individual, the accuracy of the system is better.
- The performance of the work is better than the previously proposed unimodal approach, which is presented in our previous work [1].

The remainder of this paper is organized as follows. Section 2 presents the related review of literature and the proposed approach is described in section 3. The performance of the proposed approach is analysed in section 4 and section 5 concludes the paper.

2. REVIEW OF LITERATURE

Minutiae features likes Ridge ending, Bifurcation and crossing point are the important land marks of retinal vessels for authentication.Most effective detection of these features

Revised Manuscript Received on April12, 2019.
   T.S. Sasikala, Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kanyakumari, Tamilnadu, India. (E-mail: tssasikala.niu@gmail.com)
   Dr. K. Siva Sankar, Department of Information and Computer Engineering, Noorul Islam Centre for Higher Education, Kanyakumari, Tamil Nadu, India.

Retrieval Number: F12750486S419/19©BEIESP
DOI: 10.35940/ijitee.F1275.0486S419

1357

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

is the important task in minutiae extraction. Adaptive histogram equalization for enhancing the contrast of complimentary image is proposed in [2].To estimate background of image, analyze shape of image and to thicken blood vessels morphological operations are used.

After removing illumination variation in the image using median filtering, they have obtained a skeleteon of blood vessels.Finally minutiae is detected from skeleton of retinal vessels using crossing number (CN) concept with window of size 3x3 pixel. By this method this 3x3 pixel size window is applied to all pixels of the image except edges of the image.Based on the central pixel value and its four neighbouring values all points are classified into either bifurcation, ridge ending or crossing point.This method is efficient and robust for detecting blood vessels of retina and bifurcation point from the octal fundus image.

Three types of matching in retina based authentication are minutiae based matching, non- minutiae feature based matching and correlation -based matching. Minutiae based matching aims to find the alignment between the stored template features and input minutiae feature sets. Extracting minutiae from n retinal image with low-quality blood vessel is difficult they use non-minutiae based matching.

Non-minutiae based matching extracts ridge shape, texture information, local orientation and frequency for matching.Distinctiveness and persistence of low quality image is low.

In Correlation based matching the correlation between the corresponding pixels of both query image and stored image is computed for different alignments and are used for matching.

In [3], a method is proposed by which the skeleton of blood vessel are extracted from retina using Morphological image analysis method, minutiae features like ridge ending and bifurcation points are extracted using crossing number method and are used for classification. A 3x3 window is used to extract minutiae by scanning the local neighborhood of each ridge pixel in the image. Classify the image as ridge ending if it is has only one neighboring ridge pixel in the window and bifurcation if it has three neighboring ridge pixel. Remove the false minutiae from the extracted minutiae points by selecting core point.Personal authentication based on morphological operator and crossing number method is fast and secure.

In [4], identification of retina based on pattern of blood vessels is presented by segmenting blood vessels from the retina they are thinned by morphological operations and two feature vectors namely RP feature vector and AP Feature vector are extracted by counting number of Pattern points in each angular partitions and radial partitions respectively.During decision making stage two manhattan distances are estimated between query feature and stored feature. Result shows decision based on RP feature over performs decision based on AP feature.Accuracy of retina based authentication system is improved by applying fuzzy rules during decision making stage.

Vascular pattern extracted using wavelet and multilayered thresholding technique is of variable thickness. Morphological thinning operation is applied to make the width of vascular pattern as single pixel, then vessel ending and bifurcation point is extracted as feature vector using

crossing number method. False vessel ending and bifurcation point are removed by applying windowing technique.Here, the size of window chosen is of size 9x9.Feature vector set with true feature vectors are stored as a template.During authentication Feature distance between the query image and stored template is estimated using Mahalanobis distance.

A method is proposed in [5], which extracts blood vessels using Multi Local level Set Extrinsic Curvature (MLSEC) and fuzzy circular Hough transform is used to detect Optic disc and to extract ridge endings and ridge bifurcation as feature vectors from the vessels inside the Optic Disc. Affine transform parameters obtained from the minutiae feature associates the query image with the best corresponding enrolled image for authentication. Since the feature points are extracted from inside the optic disc computation time of this method is low but this is works good only for very small database with 14 subjects.

In [6], a method is proposed which is based on rotation invariant template from the segmented circular region around the optic disc using polar transformation.Blood vessels are separated according to their diameter size using wavelet transform by testing the rotation invariant template in three different scales.Location and direction in each scale of vessels are used to form a feature vector. Finally, during matching similarity index for each scale of feature vector between the query feature and stored feature is obtained using modified correlation measure.

In [7], a translation, scaling and rotation invariant authentication system based on retinal vascular pattern is proposed.To abide this transformation factors this methods utilizes distance metrics calculated between vessels. During matching number of corresponding vessels encountered along the processing line on the query image and stored reference images are counted.

A retinal authentication system based on point set matching is proposed in [8].Blood vessels inside the optic Disc are more stable and unique for each individual so vascular pattern inside the optic disc is segmented for feature extraction. Edge dissimilarity measure namely Hausdorff distance measure is used to measure the similarity between edge map of optic disc of current image and reference image. Demerits of using Haursdorff distance technique are as follows, if portion of an object is missed due occlusion the mismatch is large.This problem can be solved by introducing partial Harusdorff distance method.This new technique estimates the similarity between two feature maps of the vascular structure of retina insider the Optic Disc.

Motivated by these existing works, this research work attempts to present a cascaded biometric system based on iris and fingerprint.

3. PROPOSED CASCADED BIOMETRIC SYSTEM

The proposed cascaded biometric system relies on fingerprint and the retina. Initially, the retina is collected from the user and the comparison of features is done

between the current user and the feature database. When the person cannot be recognized, then the fingerprint of the user is extracted and processed. The so framed feature vector is compared with the feature database. The overall flow of proposed approach is illustrated in figure 1.
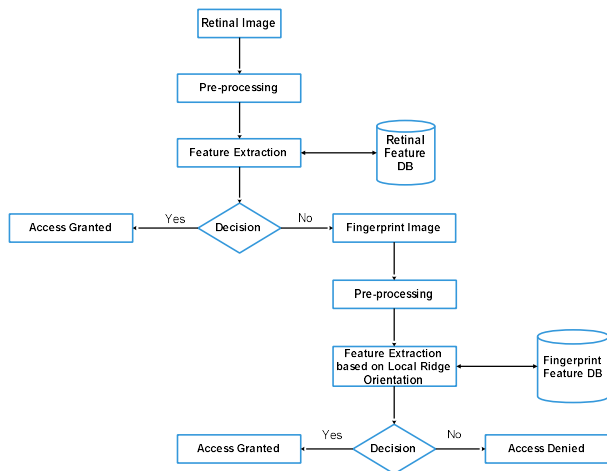

Fig.1. Overall flow of the cascaded biometric system

When the features match with each other, then the access is given to the user, even when the retinal features do not match. This case may occur due to the imperfect conscription phase. In the case of unimodal biometric system, the imperfect conscription results in the denial of access, even when the user is legitimate. In order to deal with this issue, this work includes a secondary line of user recognition. This idea helps in boosting the access provision to the legitimate user and the access denial for the illegitimate users. The main idea here is that the legitimate users must not be denied access. The two recognition phases of retina and fingerprint are presented as follows.

3.1 Retina Recognition Phase

It is proven by Simon C. and Goldstein I. et al. (1935) that the vascular pattern of retina is quite unique and in very low cases, retinal similarity is observed between twins. Hence, the retinal recognition has gained popularity, however the accuracy rates of recognition is solely depend on the effective extraction of vascular patterns. The retinal recognition phase involves three major sub-phases such as pre-processing, feature extraction and recognition. All the phases involved in the retinal recognition system are described in the following section.

3.1.1 Retinal image pre-processing

The retinal image is pre-processed in the way similar to the previous chapter. Initially, the retinal images are treated with color model conversion and contrast enhancement. The blood vessels are detected by means of 2D gabor filter, as discussed in the previous chapter. As soon as the blood vessels are detected, the features are extracted from the blood vessels. The process of feature extraction is presented in the forthcoming section.

3.1.2 Retinal recognition

The most significant points of retina are the finishing parts of the vessels and the bifurcation points. The proposed approach detects the finishing and bifurcation points by

employing crossing number based technique, as mentioned by Jain A.K. et al. (1999). Each and every detected vessel of the pre-processed image is processed with respect to pixels, as shown in equation 1.

$$F(px) = \frac{1}{2}\sum_{i=1}^{8} |im(px_{im}) - im(px_{i-1})| \qquad (1)$$

In the above equation, the processed pixels are denoted as px_i and the value of i ranges from 1 to 8. All the eight pixels are the neighbourhood pixels of the current pixel. The current pixel is denoted by $im(px)$ and its value is 1, when the current pixel is vessel bifurcation and 0 elsewhere.

When $F(px)$ is 3, then the pixel is vessel bifurcation and when $F(px)$ is 1, the pixel is the finishing point of the vessel. In this kind of feature extraction, there is no need for validating the blood vessels, as the wavelengths are varied while detecting the blood vessel. This idea removes the false points in the blood vessel, which results in better accuracy rates.

The features are compared and the access is given, only when the features match with each other. The feature comparison is carried out by computing the angles and distance between the features and the neighbourhood feature points. Let x be the feature point with y orientation and p, q, r, s are the neighbourhood points.

Similarly, the orientation points are represented by ang_1, ang_2, ang_3 and ang_4. The angles $ang_1, ang_2, ang_3, ang_4$ are the angle between the orientation of x and orientation of p, q, r, s respectively. By this way, the angles are computed with respect to the orientation of the vessel and the distance is computed with respect to the pixel coordinates.

Hence for each and every feature point, the feature set is formed as $< ang_1, ang_2, ang_3, ang_4, dis_1, dis_2, dis_3, dis_4 >$. When the features are exactly the same between the template and the current user, then the user is given access to the data. The Euclidean distance is employed to find the similarity between the feature vectors, as in the previous chapter. In case of mismatch, the second biometric fingerprint is extracted and processed, as presented in the following section.

3.2 Fingerprint recognition

Fingerprint is the secondary biometric, which is used for recognizing the individuals, when the user cannot be recognized with the help of retina. Sample visual results of fingerprint processing are shown in the following figure 2.
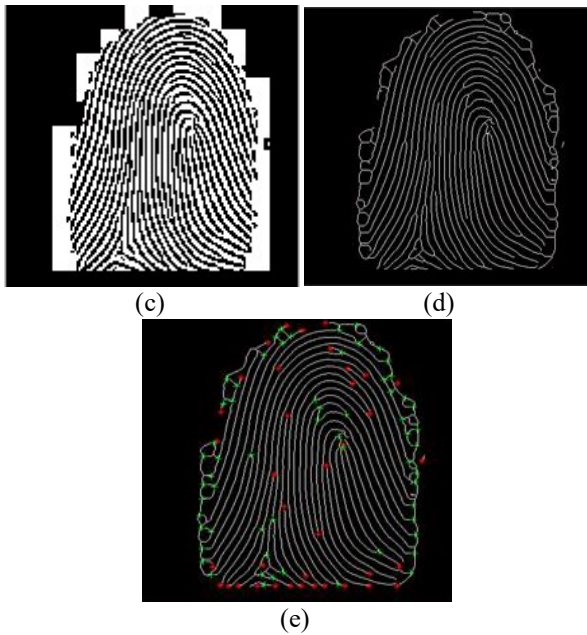

(a)   (b)

(c)   (d)

(e)
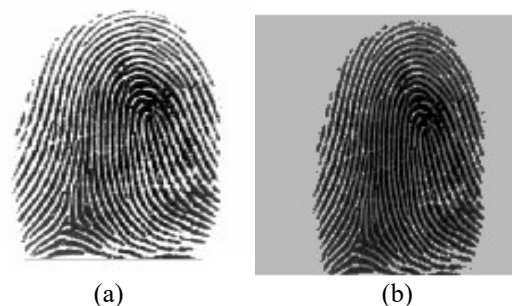
Fig. 2. Sample results (a) Input image (b) Pre-processed image (c) Binarized image (d) Ridge thinned image (e) feature extracted image

The reason for the utilization of fingerprint as a secondary measure is that several works such as Kong A. et al. (2006), Jain A.K. et al. (2002), Sun Z. et al. (2010) state that identical twins share similar fingerprint structure.

Considering this fact, this work employs retina as the primary measure for granting access to the application and suppose, when the user cannot be recognized, then the secondary measure is utilized for user identification. The fingerprint recognition is also based on three fundamental steps, which are pre-processing, feature extraction and recognition, as presented in the following subsections.

3.2.1 Fingerprint Pre-processing

This step intends to enhance the contrast of the fingerprint images such that the forthcoming process of the fingerprint recognition can have clear-cut information. The better the pre-processing, the greater is the quality of the recognition process.

The contrast of the fingerprint is enhanced by means of histogram equalization technique. The goal of histogram equalization is to enhance the contrast of the complete fingerprint image. This is attained by detecting the frequently occurring intensity values of the pixels, which range between 0 and 255. This way of fingerprint pre-processing results in better representation of images.

The histogram equalized image is then normalized by means of the following formula.

$$N_{im}(i,j) = \left\{ Mn + \sqrt{\frac{V0(In(i,j)-Mn)^2}{V}} \right\} \qquad (2)$$

In the above equation, Mn is the mean and V is the variance. This step is followed by the computation of local ridge orientation. The local ridge orientation is meant for computing the coordinates of ridges and furrows available in the fingerprint.

3.2.2 Feature extraction by local ridge orientation computation

This step intends to compute the local ridge orientation by decomposing the normalized image N_{im} into $Q \times Q$ sub-blocks. The gradient is computed for every pixel and the local orientation is computed as follows.

$$B_x(i,j) = \sum_{a=i-\frac{q}{2}}^{i+\frac{q}{2}} \sum_{b=j-\frac{q}{2}}^{j+\frac{q}{2}} 2\partial_x(a,b)\,\partial_y(a,b) \qquad (3)$$

$$B_y(i,j) = \sum_{a=i-\frac{q}{2}}^{i+\frac{q}{2}} \sum_{b=j-\frac{q}{2}}^{j+\frac{q}{2}} (\partial_x^2(a,b)\,\partial_y^2(a,b)) \qquad (4)$$

The local orientation of ridge is calculated as follows.

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\frac{B_x(i,j)}{B_y(i,j)} \qquad (5)$$

The $\theta(i,j)$ may be erroneous due to the presence of noise or any other factors. Hence, the $\theta(i,j)$ is treated by low pass filtering. Before performing the filtering process, the image is transformed to continuous vector field as presented by the following equations.

$$\delta_x(i,j) = \cos(2\theta(i,j)) \qquad (6)$$

$$\delta_y(i,j) = \sin(2\theta(i,j)) \qquad (7)$$

The process of low-pass filtering is shown in the below presented equations.

$$\delta_x'(i,j) = \sum_{a=-\frac{q\delta}{2}}^{\frac{q\delta}{2}} \sum_{b=-\frac{q\delta}{2}}^{\frac{q\delta}{2}} Q(a,b)\delta_x(i-aq,j-bq) \qquad (8)$$

$$\delta_y'(i,j) = \sum_{a=-\frac{q\delta}{2}}^{\frac{q\delta}{2}} \sum_{b=-\frac{q\delta}{2}}^{\frac{q\delta}{2}} Q(a,b)\delta_y(i-aq,j-bq) \qquad (9)$$

In the above equations, Q is the 2D low pass filter based on integral and $q\delta$ denotes the filter size. Finally, the orientation of local ridge is computed by

$$Orn(i,j) = \frac{1}{2}\tan\frac{\delta_y'(i,j)}{\delta_x'(i,j)} \qquad (10)$$

When the orientation of the local ridge of the fingerprint is computed, the image is then binarized by employing local adaptive thresholding based technique. The binarized image shows the image details in a better way.

This step is followed by performing the thinning operation, which is done by utilizing the inbuilt function available in MATLAB. This function conserves the endpoints and the connectivity of the ridges, while reducing the occurrence of false bifurcations.

The minutiae feature extraction is done on the so processed image by utilizing a 3×3 window. Each and every minutiae point is represented by the (x,y) locational coordinates and the orientation of the ridge on which the minutiae is found. For instance, when a current pixel with value 1 is surrounded by three ones, then the current pixel is found to as bifurcation. On the other hand, when the current pixel with value 1 is surrounded by only one neighbour with value one, then the current pixel is identified as the termination point of ridge.

3.2.3 Recognition phase

The process of feature extraction is done for all the fingerprint images and the extracted ridge pattern is stored in the database. During the process of recognition, the same processes such as fingerprint pre-processing and feature extraction are carried out to obtain the minutiae points. The proposed algorithm is presented as follows.

Proposed Cascaded Biometric System based on Retina and Fingerprint for User Recognition

---

// Training
Input: Retina (DRIVE, VARIA), Fingerprint (FVC2002)
Begin
For all retinal images
  Do
    Pre-process the retinal and fingerprint images;
    Detect the blood vessels of retina;
    Extract orientation and angular features;
    Build feature vector and store;
  End do;
For all fingerprint images
  Do
    Pre-process the images;
    Extract local ridge orientation features;
    Build feature vector and store;
  End do;
End;
//Testing
Input: User's retinal image
Output: Access grant or denial
Begin
Pre-process the image;
Extract orientation and angular features;
Build feature vector fv;
Apply Euclidean distance and compare fv with the feature vector database;
If match exists
  Grant access;
Else
  Obtain fingerprint image from user;
  Pre-process the image;
  Extract local ridge orientation from the image;
  Build feature vector and compare it with the database;
  If match exists
    Grant access;
  Else
  Deny access;
End if;
End if;
End;

When the minutiae points are obtained from the user, the obtained outcome is compared with the feature database. The comparison is done with the help of Euclidean distance, as discussed in the previous chapter. Finally, the access to the application is granted when the match is observed and denied in the case of mismatch.

By this way, the cascaded biometric system works by considering both the retina and fingerprint images of the user. The performance of the proposed approach is analysed in the following section.

4. RESULTS AND DISCUSSION

The performance of the proposed cascaded biometric system is analysed in two scenarios. The first scenario justifies the performance of cascaded biometric system over unimodal biometric systems. The second scenario compares the performance of the proposed approach with the existing approaches such as iris+fingerprint proposed by Gawande U. et al. (2013) and fingerprint+fingervein presented by Wencheng Y. et al. (2018). The performance of the proposed approach is analysed in terms of standard performance metrics such as accuracy, sensitivity, specificity, F-measure and time consumption rates.

This work utilizes three different publicly available datasets for validating the performance of the proposed approach. The retinal images used for analysis are the same as in our previous work [1]. Two different databases are used for retinal recognition and the average results are presented in this section. The fingerprint database used for analysis is FVC2002, in which the images are of size 388×374. The database contains a total of 110 images, out of which 60 images are used for training and the rest of images are utilized for testing.

Accuracy is the most significant performance metric that is meant for checking the reliability of recognition system. The accuracy rate of the recognition system must be greater and is computed by the following equation.

$$accu = \frac{T_p + T_n}{T_p + T_n + F_p + F_n} \qquad (11)$$

where the true positive, true negative, false positive and false negative rates are represented by T_p, T_n, F_p and F_n respectively. Sensitivity and specificity rates of the approach are based on the false negative and false positive rates respectively.

Greater sensitivity and specificity rates are attained, when the false negative and false positive rates are minimal. The sensitivity and specificity are inversely proportional to the false negative and false positive rates.

Most of recognition approaches in the existing literature focus on attaining better accuracy rates but fail to prove reasonable sensitivity and specificity rates. The sensitivity and specificity rates are computed as follows.

$$sen = \frac{T_p}{T_p + F_n} \qquad (12)$$

$$spe = \frac{T_n}{T_n + F_p} \qquad (13)$$

The F-measure of a proposed approach relies on the sensitivity and specificity rates of the approach. The F-measure of the system is computed by

$$F_{msr} = \frac{2 \times sen \times spe}{sen + spe} \qquad (14)$$

The F-measure is directly proportional to sensitivity and specificity rates. The greater the F-measure, the better is the performance of the recognition approach with minimal false positive and false negative rates.

4.1 Performance analysis of Proposed Approach w.r.t. Individual Biometric

This section compares the performance of the proposed approach with the unimodal biometric systems that employ retina and fingerprint. The performance of cascaded biometric system proves better performance and the results are presented in the following section. This work utilized two datasets for retina and the average results are tabulated in table 1.

Table 1. Experimental results of unimodal and cascaded biometric systems

Performance Metrics/Feature extraction techniques	Unimodal (Fingerprint)	Unimodal (Retina)	Proposed Cascaded (Fingerprint + Retina)
Accuracy (%)	79.6	83.8	**92.4**
Sensitivity (%)	76.2	79.3	**90.6**
Specificity (%)	72.4	77.4	**89.3**
F-Measure (%)	74.25	78.33	**89.94**
Time Consumption (s)	**15.7**	16.4	17.6

From the experimental results, it is observed that the performance of the proposed cascaded biometric system is better than when the retina and fingerprint biometrics are utilized individually. The main reason is that relying on a single biometric may lead to incorrect results, in spite of the better performance of the algorithm. The main reason for the minimal accuracy, sensitivity and specificity rates is that the system denies access to the legitimate users owing to the presence of noise or issues in data acquisition.

The proposed cascaded biometric system relies on different biometrics, such that when the first retinal recognition is unsuccessful, the second biometric fingerprint is processed. This idea reduces the false negative and false positive rates, which is very important in the case of recognition systems.

Besides this, the second line of recognition system is executed, only when the retinal recognition system identifies the user as illegitimate. This conserves time and saves the system from computational complexity as well. Hence, the cascaded biometric system performs better in all means. The following section compares the performance of the proposed approach with the existing approaches.

4.2 Performance analysis of Proposed Approach w.r.t. Existing Approaches

In the existing literature even in the case of multimodal biometric systems, the combination of retina and fingerprint together as a system is quite rare. Most of the existing works combine fingerprints and iris together. Taking this as a challenge, the proposed cascaded approach clubs the retina and fingerprints together for analysing the performance.

The existing approaches considered for comparison are the combination of fingerprint and finger vein proposed by Wencheng Y. et al. (2018), fingerprint and iris proposed by Gawande U. et al. (2013). The accuracy rate analysis is presented in figure 2.
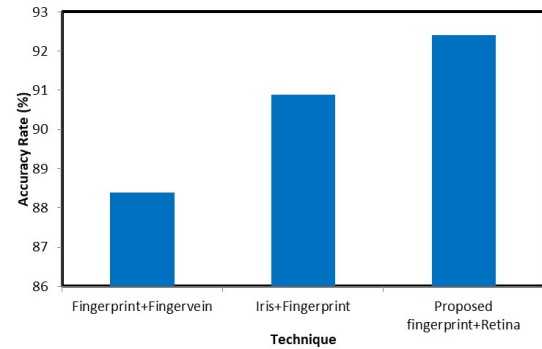

Fig.2 Accuracy rate analysis

The accuracy rate of the proposed approach is analysed and compared with the existing biometric systems. From the experimental analysis, it is proven that the performance of the combination of fingerprint and retina is better than the other systems.

The other two existing techniques work in bimodal fashion but the proposed approach works in cascaded mode. Hence, the proposed work performs double check before granting access to the application. The accuracy of the system is satisfactory with the accuracy rate of 92.4%. The following section shows the sensitivity rate analysis of the proposed approach.
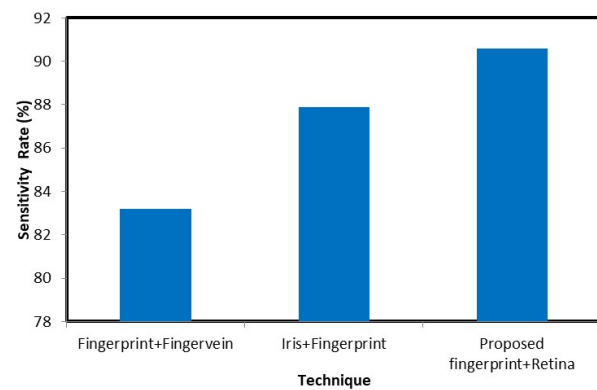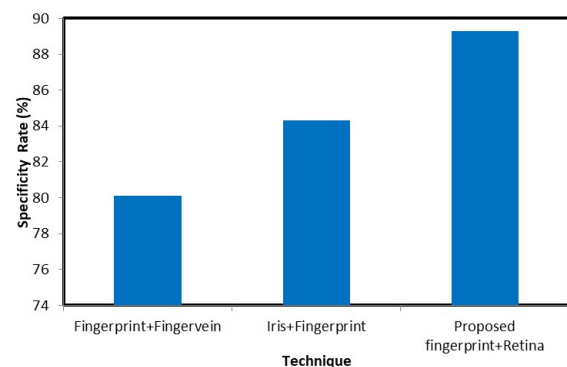

Fig.3 Sensitivity rate analysis

Fig. 4. Specificity rate analysis

The sensitivity and specificity rates of the proposed approach are then analysed and compared with the existing approaches. The sensitivity and specificity rates of the proposed approach are greater, as the proposed approach

double checks the final decision of the recognition system. On the other hand, both the existing techniques utilize the biometrics based on the concept of fusion.
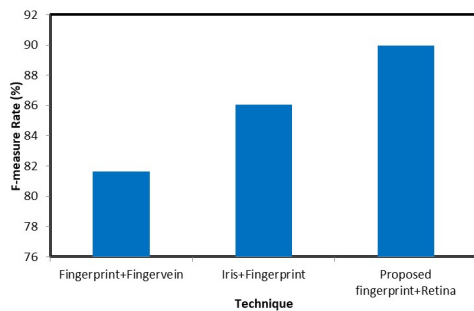

Fig. 5. F-measure rate analysis

The F-measure rate depends on the sensitivity and specificity rates, such that the proposed approach shows better F-measure rate than the existing approaches. The time consumption rate of the proposed approach is shown in figure 6.
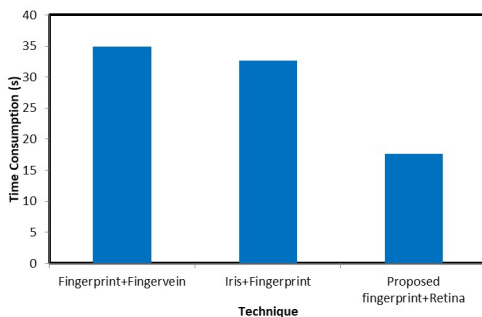

Fig.6. Time consumption rate analysis

The time consumption of the proposed approach is minimal, when compared to the existing approaches. The reason behind minimal time consumption is that the second line of recognition, which is fingerprint recognition is executed only when the user cannot be recognized with the help of retinal features. This idea reduces the time consumption of the proposed approach, which shows an average of 17.6 seconds.

On the other hand, the existing approaches make the final decision by clubbing both the biometrics. On the whole, the performance of the proposed approach is better than the existing approaches.

5. CONCLUSION

This paper presents the cascaded biometric system that is based on retina and fingerprint. Initially, the retinal images of the users are processed and the decision is made based on the similarity between the computed feature vector and the feature database. Suppose, when the exact match cannot be located, then the second line of recognition is executed with the help of fingerprint. The features of the fingerprint are extracted and the comparison is done for making the final decision. This cascaded biometric system has proven better sensitivity and specificity rates, while consuming minimal period of time. In future, this work is planned to be extended with multi-biometrics for boosting up the security.

REFERENCES

1. T.S. Sasikala , Dr. K. Siva Sankar, "Unimodal Biometric Based Security Application by Exploiting Retina", International Journal of Engineering and Advanced Technology, Vol.8, No.2S, pp. 344-353, 2018.
2. Gubbi, T. Extraction of Blood Vessels and Recognition of Bifurcation Points in Retinal Fundus Image.
3. Lincy, D. G., &Joans, S. M. Segmentation of Image Using Enhanced Morphological Gradient Hit Method. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231-2307.
4. Barkhoda, W., Akhlaqian, F., Amiri, M. D., &Nouroozzadeh, M. S. (2011). Retina identification based on the pattern of blood vessels using fuzzy logic. EURASIP Journal on Advances in Signal Processing, 2011(1), 113.
5. Ortega, M., Marino, C., Penedo, M. G., Blanco, M., & Gonzalez, F. (2006, April). Biometric authentication using digital retinal images. In Proceedings of the 5th WSEAS international conference on Applied computer science (pp. 422-427).
6. Farzin, H., Abrishami-Moghaddam, H., &Moin, M. S. (2008). A novel retinal identification system. EURASIP Journal on Advances in Signal Processing, 2008(1), 280635.
7. Köse, C., &İki, C. (2011). A personal identification system using retinal vasculature in retinal fundus images. Expert Systems with Applications, 38(11), 13670-13681.
8. Ekka, B. K., Puhan, N. B., & Panda, R. (2015, February). Retinal verification using point set matching. In 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 159-163). IEEE.
9. Simon, C., & Goldstein, I. (1936). The retina method of identification. Series, 4, 1900-25.
10. A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in a Networked Society", Springer- Verlag New York Inc (C), 1999.
11. Kong, A. W. K., Zhang, D., & Lu, G. (2006). A study of identical twins' palmprints for personal verification. Pattern Recognition, 39(11), 2149-2156.
12. Jain, A. K., Prabhakar, S., &Pankanti, S. (2002). On the similarity of identical twin fingerprints. Pattern Recognition, 35(11), 2653-2663.
13. Sun, Z., Paulino, A. A., Feng, J., Chai, Z., Tan, T., & Jain, A. K. (2010, April). A study of multibiometric traits of identical twins. In Biometric Technology for Human Identification Vii (Vol. 7667, p. 76670T). International Society for Optics and Photonics.
14. Gawande U., MukeshZaveri, AvichalKapur, "Bimodal biometric system: feature level fusion of iris and fingerprint", Biometric Technology Today, Vol. 2013, No.2, pp.7-8, 2013.
15. Yang Wencheng, Wang Song, Hu Jiankun, ZhengGuanglou, Craig Valli, "A fingerprint and finger-vein based cancelable multi-biometric system", Pattern Recognition, Vol.78, pp.242-251, 2018.