DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5322

Volume 9, No. 1, January-February 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

RETINA BASED BIOMETRIC AUTHENTICATION SYSTEM: A REVIEW

Jarina B. Mazumdar
Department of ECE Gauhati University
Guwahati, India

S. R. Nirmala
Department of ECE Gauhati University
Guwahati, India

Abstract: A biometric system provides an automatic person authentication based on some characteristic features possessed by the individual. Among all other biometrics, the retinal biometric system is unique as well as stable. The retina is a secure and reliable source of person recognition as it lies behind the eye and is unforgeable. The process of recognition mainly includes pre-processing, feature extraction and then features matching. The features generally used in this process are either blood vessel features or non-blood vessel features. In this paper, different methods available in the literature for retina based person authentication system are described, discussed and compared.

Keywords: Biometric; retinal recognition; blood vessel segmentation; vascular feature; non-vascular feature.

I. INTRODUCTION

With the advancement in technology, the world is exposed to more threats and insecurities. In many fields, such as police or military environments and banking affairs, security is a critical issue. This requires a highly dependable and precise person authentication system. Traditional authentication systems are either information-based such as a password, a pin or token based like a card, a key. In many conditions, these systems are not sufficiently reliable due to their common impotence to individuate between a true authorized user and a user who illicitly procured the privilege of the authorized user. These problems can be solved by employing a biometric based authentication approach.

A biometric system is nothing but a pattern recognition method, which recognizes a person depending on some specific features, derived from the physiological or behavioral characteristic that a person possesses [1]. Physiological characteristics include face; fingerprints, iris, and hand and finger geometry [2] are defined below:

Face: Face authentication system analyzes facial characteristics. A digital camera is used to capture a facial image and some features are extracted from it which is then used for authentication.

Fingerprint: A fingerprint is an impression of the friction ridges of all or any part of the finger.

Iris: Iris is a colored ring of tissue that surrounds the pupil. The feature extracted from these regions are used in Iris based biometric.

Hand and finger geometry: Hand Geometry involves scanning and measuring the shape of the hand. These techniques include the estimation of length, width, thickness and surface area of the hand.

The behavioral characteristics are ear shape, voice, gait, signature, and key stroking [2].

Ear shape: The ear shape and the structure of the tissue of the pinna are unique to every individual. The approaches for ear recognition are based on matching the distance of prominent points on the pinna from a landmark location on the ear.

Voice: Voice is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

Gait: Gait biometric is the particular way that a person walks and is an intricate spatiotemporal biometric. Although, gait is not supposed to be very distinctive but is favourable in some low security applications to allow verification.

Signature: Signature verification checks the way a user signs his/her name. Like signature's static shape, some other signing features such as speed, velocity, and pressure are also countable for this verification.

Keystroke Dynamics: Keystroke dynamics is a biometric characteristic to verify the identity of a person by their typing rhythm, which can handle with the trained typists and the amateur two-finger typist as well.

Although there are some authentic systems based on different biometrics but all of these can easily be forged. However, several spoof attacks can also be carried against many types of biometrics, like fingerprint, face, and iris. Under spoof attacks replica of the genuine user's fingers are created using some artificial material like silicon or wood glue, etc. to circumvent a system [3]. Sometimes the attackers use an artificial finger, a mask over a face or a contact lens on an eye [4]. As one's signature may alter over a period and it is not as unique as Iris, Face, Fingerprint [5]. In voice recognition, the main obstacle is speech features are sensitive to background noise. Gait biometric also may vary due to change in body weights. It may not remain fixed for long period of time, owing to major injuries involving leg or brain or due to inebriety. Hence, it is required to consider such a biometric characteristic, which cannot be forged easily but is unique, stable and measurable. This leads to retina based biometric authentication system.

As the retina of human eye lies at the rare end and is not directly attainable, it is very difficult to forge. The retinal vasculature is unique to every individual and it remains same throughout a person's life unless the person undergoes some severe eye surgery or injury [2].

The first stage of a biometric system is enrollment phase, where each user has to register his or her biometric trait into the system database. Then feature is extracted from the enrolled data and a template model is been made for each

© 2015-19, IJARCS All Rights Reserved

user and stored in the database. A biometric authentication system is generally employed in verification and identification mode depending on the application environment. The vital difference between these two modes of operation is in the testing phase. In the verification mode, a user's requested identity is been authorized by comparing the extracted biometric features with the stored biometric template of the person in the database. In the identification mode, the system validates an individual by checking the templates of all the users in the database for a match [7].

For a biometric authentication system the general block diagram is shown in Fig.1. The sensor module takes an image of the biometric characteristic then features are extracted from the image. The extracted feature information is called template. This template is then sent to a matcher, where the matcher compares the newly presented biometric information with the previously stored template to make a decision.

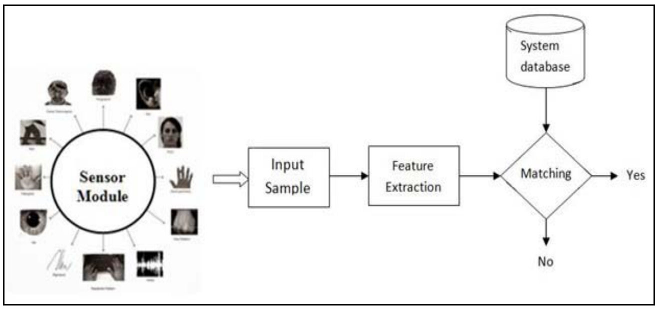

Figure 1. General block diagram of biometric authentication system

II. REVIEW OF DIFFERENT RETINA BASED BIOMETRIC AUTHENTICATION METHODS

The retinal authentication system is mainly based on the unique blood vessel pattern in the retina. The uniqueness of retinal vascular pattern was introduced by two ophthalmologists, Dr. Carleton Simon and Dr. Isodore Goldstein in 1935 [8]. And later in 1950, Dr. Paul Tower discovered that even among identical twins the vascular patterns are unique [8]. EyeDentification 7.5, the first retina identification system using commercial retinal scanner was proposed by EyeDentify Company in 1976. Another retinal scanning device named ICAM 2001 is also manufactured by this company, which can store up to 3000 templates with a storage capacity of up to 3300 history transactions [9]. Some companies like Retica System Inc. working on a multi-modal system using Retina and Iris for identification. A retinal authentication system has basically three main steps: image acquisition, feature extraction, and feature matching. These are explained below:

The first stage of a retinal authentication system is image acquisition. To capture the image of retina a fundus camera is used, where the user must position his eye very close to the lens and the user must also remain perfectly still at this point. Moreover, if the person is wearing glasses then these has to be removed to avoid signal interference.

The second stage is feature extraction. Different features are extracted from the blood vessel structure of the retina image, and/or the retinal image itself. These features are unique for each individual and stored as a reference pattern.

At the last stage, the features of test image are matched with the pre-stored template in the database depending on some criteria. If the criteria are satisfied then the person is authenticated.

The retina based authentication procedures can be broadly classified into two different categories. Few algorithms depend on the vascular features of retinal images. These processes require blood vessel segmentation, which is a very time consuming. Hence, the computational time of these methods is high. The different blood vessel features are listed below:

- **Branch point:** The vascular structure of retinal image is of tree shape. So, the main features of the blood vessel pattern are branch point where a vessel bifurcated into two vessel branches [10].
- **End point:** The end points of the blood vessel patterns, where each vessel ends, is considered as another feature for retina based authentication system [10].
- **Crossover point:** The points of intersection between two blood vessels are termed as crossover points and are taken as another feature set [11].
- **Blood vessels in and around Optic Disc (OD):** The blood vessel patterns around the OD region are also considered as a feature set because of their stability and unique variation inside that region for a particular person [12].

However, some other algorithms are based on non-vascular features extracted from retinal images. They are structural features of the retinal image like luminance, contrast, and structure. Some algorithm computed the retinal edge dissimilarity score for authentication. Whereas others used Fourier transform of retinal image to extract Fourier spectrum phase feature (FSPF). Corners of retinal image are also considered as one of the features. The implementation time of these methods is low, as this algorithm does not require blood vessel segmentation for feature extraction.

A. RETINAL AUTHENTICATION BASED ON VASCULAR FEATURES

Most of the retinal authentications systems are based on blood vessel features, as these a unique to each and every individual. The block diagram of this kind of authentication system is shown in Fig.2. Different techniques exist in literature for enhancement and segmentation of retinal blood vessels that are used to extract the feature. Few of them are discussed below:

Ortega et al. [10] have extracted the blood vessel using MLSEC (multi-local level set extrinsic curvature) which has useful invariance properties. Then they have segmented the OD using fuzzy circular Hough transform and extracted the ridge endings and ridge bifurcation from vessels inside the optical disc as their feature points. For feature matching, the affine transformation parameters are obtained to associate the query image and its best corresponding enrolled image. The computational time of this method is low as they have extracted the feature points inside the OD but, the main limitation of their algorithm is the use a very small database with 14 subjects only. In their consecutive work [11], they have considered one more feature point which is the

© 2015-19, IJARCS All Rights Reserved

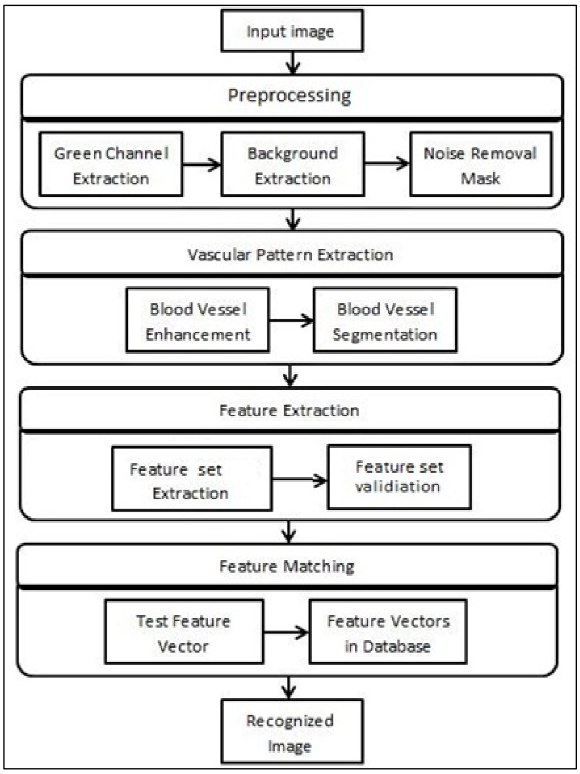

Figure 2. Block diagram of retinal authentication system based on vascular features

They have done a deep analysis of similarity metric to identify the most suitable matching pair. But this method works only for the verification of a person's identity. Farzin et al. [13] have proposed a novel recognition method based on the features of retinal images. The main steps of the method are: blood vessel segmentation, feature extraction, and feature matching. The OD of the image is detected and a circular region around the OD is selected from the segmented blood vessel image. Then, a rotation invariant template is created, using a polar transformation as shown in Fig.3.

Figure 3. Polar transformation: (a) Region of interest in Cartesian coordinates, (b) polar representation of the image [13].

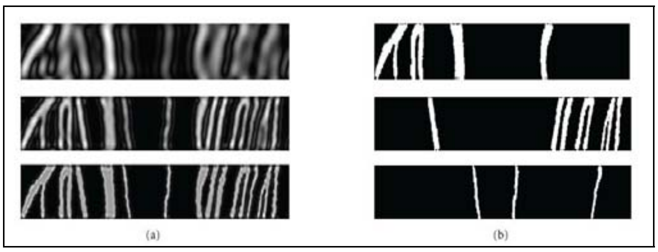

Figure 4. (a) Multiscale analysis of polar image: wavelet approximation coefficients in scale 3 (left up), 2 (left middle), and 1 (left bottom); (b) vessel separation result: large (right up), medium (right middle), and small (right bottom) vessels [13].

Next, these templates were tested in three different scales using wavelet transform to separate the vessels according to their diameter sizes shown in Fig. 4. In the last stage, vessel location and direction in each scale are used to form a feature vector for each subject in the database. For feature matching, they have introduced a modified correlation measure to obtain a similarity index for each scale of the feature vector. These steps made the computational time of the system high, and this method is used only in identification mode.

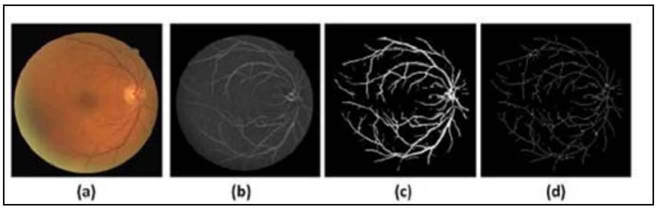

Figure 5. a) Original retinal image, b) Enhanced image, c) Segmented blood vessels, d) Thinned blood vessels [14].

In papers [14], [15] and [16], the authors have used Gabor wavelet to enhance the blood vessels of retinal images as it has the capability of selecting oriented features [17]. However, Akram et al. [14] have used an adaptive thresholding technique to segment the blood vessels. But it is hard to find one optimal threshold value for accurate vascular extraction, especially in case of PDR (Proliferative Diabetic Retinopathy) as new abnormal blood vessels are normally very thin. So, Qamber et al. [15] and Fatima et al. [16] have presented a supervised multilayered thresholding based method for accurate vascular segmentation where by varying the threshold value they can segment the thin blood vessels also. They have shown that their blood vessel segmentation technique outperforms existing methods [15]. The blood vessel segmentation result is shown in Fig.5. Then for feature extraction, all the authors have used vessel end points and branch points. Then they validated their extracted blood vessel features to remove false endings and bifurcations due to small breaks and spikes. For feature matching, Akram et al. [14] have used Euclidian distance; Qamber et al. [15] and Fatima et al. [16] have used Mahalanobis distance. For recognition [14], [15] they have taken 354 images from DRIVE, STARE and VARIA databases and got a quite good recognition rate for DRIVE (100%) and VARIA (99.5%). In STARE database, the recognition rate is 96.29% because of the presence of different retinal lesions but, in [16], 333 images were used from VARIA and RIDB database. Other than the recognition rate they have also used False Acceptance Rate (FAR), False Rejection Rate (FRR) and calculated Equal Error Rate (ERR) (0.0557%) to further check the validity of their proposed system.

The main difficulty in the retinal recognition system is due to the head or eye movement. To overcome those difficulties, it is required to design an authentication system, which will be invariant to scale, rotation and translation. In [18], Kose et al. introduced a scale, rotation and translation invariant person recognition system using retinal vascular pattern. To tolerate these factors the proposed method used a technique utilizing the distances between vessels. The method counted the number of corresponding vessels encountered along the processing line on the current and reference images stored in the database. For similarity measurement, they have employed two measures. The first one counted the matching vessel and calculated a similarity value for the reference and sample images; here, the

© 2015-19, IJARCS All Rights Reserved

maximum number of matching are found for each sample lines and then, the total number of matching for all sample lines are calculated for the identification. The second one used a rational similarity measurement of reference and sample images. Here the maximum numbers of corresponding vessels are counted. Finally, by considering these two similarity measurement techniques, they calculated the final similarity value for the images. The maximum value of comparisons between sample and reference images shows the best matching between them. Their method can identify a person with degenerated retina, most of the degeneration occurs due to Diabetic Retinopathy (DR) or Age-related Macular Degeneration (AMD). The proposed method was found to be very fast (milliseconds) in person identification and without any user intervention.

Ekka et al. [12] proposed a retinal verification system based on point set matching. In their method, they have observed that the blood vessels inside OD region are more stable and exhibit unique variation for each individual and for reason they segmented the vascular pattern inside that region only. The edge map of the OD blood vessels is used as a feature set for similarity measurement and for this; the authors have used a Hausdorff distance measure, which is an edge dissimilarity measure. The main difficulty of using Hausdorff distance technique is when a portion of an object is missed due to occlusion the mismatch is large. To overcome this, a partial Hausdorff distance method is introduced to calculate the similarity between two feature maps of the vascular structure of retina inside the OD region. The performance of their system was measured in terms of FRR, FAR and calculated EER as 9.79% for an optimum threshold. They have got the highest accuracy of 90.21%, which is not quite satisfactory, and also their method works only for retinal verification.

Khakzar et al. [19] have proposed person identification system using retinal images. Their method is rotation-invariant based on a tessellation of frequency spectrum. They have used Discrete Fourier Transform (DFT) technique to make the features invariant to translation and rotation. By analyzing the Fourier spectrum of the retina image it has been observed that the density of useful information in retina image is reduced from low to high frequency. Hence, they have implemented a multi-resolution tessellation algorithm, where a sequence of radii has tessellated the Fourier domain into concentric circles. Then the Fourier transform of retina image is divided into different sub band and the energy of each sub band was taken as a feature vector. For decision-making, they have used Euclidean distance. Though they have obtained a quite good accuracy rate of 99.29% but the performance of the algorithm has been evaluated using a small data set.

Lajevardi et al. [20] have introduced a Biometric Graph Matching (BGM) algorithm to make a retina verification system. They have generated a retinal template based on the spatial graphs derived from the blood vessel structure of the retina. For these, the vascular structures of the retinal image are segmented first by using a family of 2D matched filters. The features like vessel branch and crossover point are extracted. Then a retina graph is formed by connecting these feature points and it consists of vertex set, edge set, vertex labeling function and edge labeling function and is shown in Fig.6. In the graph matching technique the graph is first registered and then error-tolerant graph matching technique differentiates between genuine and imposter. To measure the performance of the algorithm, a Kernel Density Estimation (KDE) technique is used to obtain the authentic and imposter score distributions of the training set as the accessible data set is small. Finally, to increase the matching performance of the verification system, a combination of SVM classification and KDE model is used. This method have used multiple characteristics of the scores of retina graphs in the course of decision making whereas previous state-of-the-art retinal verification architectures have used a single measure alone to distinguish the retinal models [11], [13]. The validation of their algorithm is evaluated in terms of Equal Error Rate (ERR) for both automatic and manual retina graphs and these were 0.005 and 0.001 respectively.

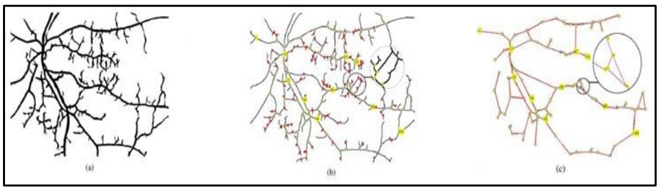

Figure 6. (a) Binarised image of the Retinal image (b) The skeleton of the retinal image with spurious feature points which have short paths ending in termination points (red marks) and true feature points (yellow marks). (c) Retina graph of (b) after removal of spurious points [20].

Hussain et. al. [21] have proposed a person identification based on the retinal vascular network features. These are branch point and crossover point. To extract these features they have segmented the blood vessels using multi-scale line detector algorithm. They have applied a vessel width measurement technique to extract the major vessels then identified the vessel branch and crossover points for the major vessels. To make the extracted retinal features invariant to scale, rotation and translation they have used a geometric hashing technique. This approach uses indices based on local Geometric features, which remained invariant to object transformation. Their method is invariant to scale, rotation and translation and also achieved a detection accuracy of 100%. Condruache et. al. [22] have proposed a novel feature extraction process that includes the segmentation of feature point using scale invariant feature transform (SIFT). To make the feature set they have also considered vessel branch point and crossover point. At first, they have segmented the vascular structure of the retinal image using a hysteresis classifier. Then they have evaluated their corresponding SIFT descriptors. Their feature vector is associated to the statistical properties of the SIFT descriptor sample in the feature-point cloud which exhibit all the invariance properties needed for the retina based person authentication. They have also shown that in their approaches it is not required to align the two images to check whether they have come from the same eye, which clearly reduces the computational burden of the system. After feature extraction, the authentication is conducted with the help of sparse classifier.

Zahedi et al. [23], authors have used the Radon transform on retinal image for designing a person identification system. The blood vessel features around the OD region of the retinal image are considered as a template. For these, they have localized the OD first, using a template matching technique then to make the template rotation invariant polar transformation has been used. Then they

© 2015-19, IJARCS All Rights Reserved

have segmented a circular ring around the optic disc and extracted features using radon transform. For matching they have used 1D-DFT (Discrete Fourier Transform) and Euclidean distance. They tested their method on 200 images by generating 5 images for every 40 subjects from DRIVE database and achieved an identification rate of 100%. After going through all these literature it has been seen that all these methods have considered different sets of images from different databases and evaluated their results using different performance metrics. These methods are compared depending on the number of images, number of subjects, authentication mode (Identification or verification), processing time, the rate of EER and Accuracy. These comparison result using blood vessel feature of the retina are shown in Table 1.

Table I. Comparison Table of different Recognition methods using Vascular feature

Method.	***No. of images***	***No. of subjects***	***Database used***	***Identification or Verification***	***Processing time (sec)***	***EER***	***Accuracy (%)***
Ortega et al. [10]	90	83	Collected from hospital	Verification	0.155	----	100
Farzin et al. [13]	300	60	DRIVE and STARE	Identification	----	0.006	99
Akram et al. [14]	354	260	DRIVE, STARE and VARIA	Identification	----	----	98.30
Qamber et al. [15]	354	260	DRIVE, STARE and VARIA	Identification	----	----	98.87
Fatima et al. [16]	333	159	VARIA and RIDB	Identification	----	0.0557	99.57,97
Kose et al. [18]	392	----	STARE	Identification	6464	----	99.5
Ekka et al. [12]	84	59	VARIA	Verification	----	9.79	90.21
Khakzar et al. [19]	280	40	DRIVE	Identification	----	----	99.29
Lajevaedi et al. [20]	135	57	DRIVE	Verification	----	0.005 for automatic and 0.001 for manual	----
Hussain et al. [21]	184	----	164(Own database), 20 Staal	Identification	----	----	100
Condurache et al. [22]	513	159	VARIA and DRIVERA	Both Identification and Verification	6	----	99.29
Zahedi et al. [23]	200	40	DRIVE	Identification	----	----	100

B. RETINAL AUTHENTICATION BASED ON NONVASCULAR FEATURES

Few researchers have carried out retinal authentication based on non-vascular features of the retina. The block diagram of this type of retinal authentication system is shown in Fig.7. After preprocessing the features of the retinal image are extracted from retina without undergoing blood vessel segmentation, hence we name them non-vascular features as these do not depend on blood vessels of retina only. Therefore, it decreases the execution time of the system while preserving its good performance.

Waheed et al. [24] proposed a non-vascular based retina recognition system. It computes similarity measure using

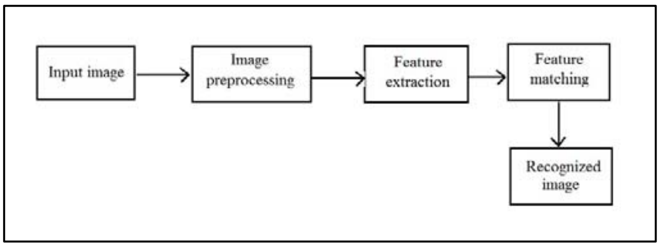

Figure 7. Block diagram of retinal authentication system based on non-vascular features.

features based upon structural information such as luminance, contrast and structural features of an image. To extract the features they have taken two images, which are to be compared at the same time. Luminance $l(x,y)$ is a measure of mean intensity, for two candidate images x and x and is given as,

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2} \quad (1)$$

Contrast *c(x,y)* function is a measure of standard deviation of images x and y and is given by,

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (2)$$

Then they have combined luminance and contrast functions to obtain structure measurement. For matching an empirically optimized function is used to generate a similarity score between two candidate images. They have used only 34 subjects for their experiment and obtained an identification rate of 92.5%. Ong et al. [25] presented a retina biometric system consisting of two stages: feature points matching and the measurement of edge dissimilarity. To obtain the feature points they have developed a graph-based method where they have used scale-invariant feature transform (SIFT). The graphs comprise of vertex set and edge set. For matching, the feature points they have employed a sub-graph matching algorithm and pruned the putative match feature points so that wrong feature points get removed. To achieve this, a robust transformation estimator is used which is based on the Least-Median-Squares (LMedS) estimator followed by a Weighted Least Squares (WLS) estimator. If a sufficient number of matched feature points have been detected, then they have performed an image registration using the estimated affine transformation parameters to register the template image with the test image. They have extracted the edges from the test retinal image and registered template retina image using Canny's edge detector and performed the edge dissimilarity measurement with the help of Robustified Hausdorff Distance (RHD) measure for decision making. To evaluate their experiment they have created DRIVERA (DRIVE for Retinal Authentication) dataset consisted of 280 images from 20 images of DRIVE database. The performance of their identification system is evaluated in terms of FAR (False Acceptance Ratio) and FRR (False Rejection Ratio), which are 0% and 3.169% respectively. They have presented that their retina verification technique surpasses two of the state-of-the-art approaches [22] and [26] when tested on the same dataset.

Sabaghi et al. [27] have introduced a human identification system based on Fourier transform (FT) and angular partitioning of the spectrum of retinal images. For a robust system, the rotation of retinal image should be compensated. To achieve this first they have localized the OD using template matching technique, and then determined the center of the OD and the center of mass to obtain the rotation angle of the retinal image as shown in Fig.8. For extracting features, they have used FT of the retinal image. The angular partitioning of the Fourier spectrum is performed to calculate the energy of Fourier spectrum. Then the sum of the phase angle per partition is computed. They have named this feature vector as Fourier Spectrum Phase Feature (FSPF) and are shown in Fig.9. They have also shown that their system is robust to noise.

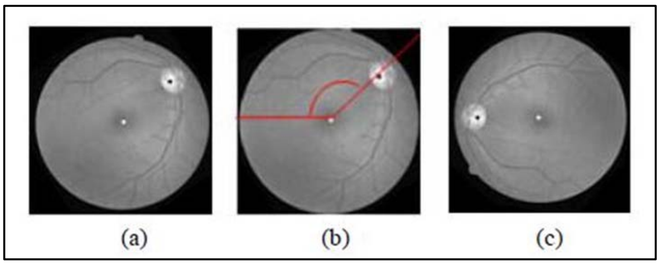

Figure 8. The result of regulate retinal image to reference position: (a) Retinal image after localized center of mass and optical disk; (b) Obtain the angle of rotate; (c) Compensated image by rotation [27].

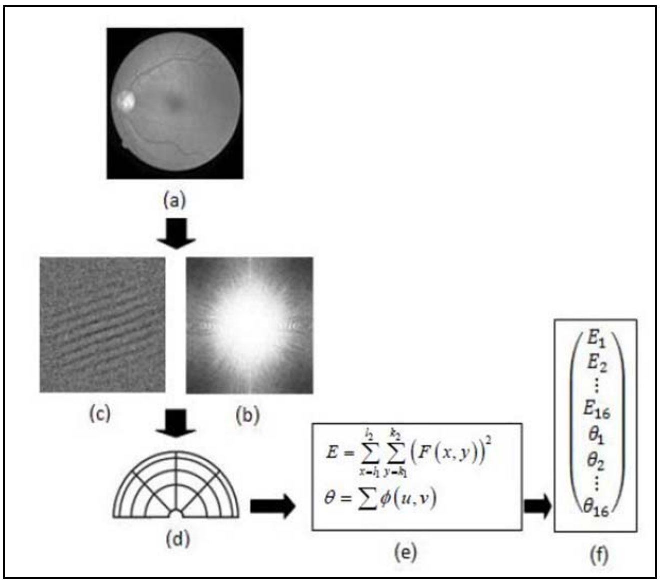

Figure 9. Complete flow diagram for feature extraction process in the proposed system. (a) Retinal image after rotation compensation (b) Fourier spectrum (c) phase angle (d) partitioning the Fourier spectrum and phase angle (e) calculate energy of Fourier spectrum and sum of the phase angle per partition (e) future vector construction [27]

Later in [28], they have introduced another method, which is a combination of wavelet transform along with Fourier transform for FSPF extraction. With Fourier transform they extracted Fourier energy feature and with wavelet transform, they have extracted wavelet energy feature. For matching they have used Euclidian distance in both the papers. They have shown that the accuracy of the identification system is 95.4% with Fourier transform features and 97.2% with wavelet transform features but it increases to 99.1% by combining both the methods. Dehghani et. al. [29] have proposed a person authentication system using retinal features. Their method consists of feature extraction, phase correlation, and feature matching. They have observed that the corners of retinal images are rotation invariant and for this, they have used Harris corner detector. After feature extraction, they have applied the phase correlation method to determine the rotation of the head and eye movement in front of a retinal scanner. Finally, for feature matching they have used a similarity function to calculate the similarity between different retinal images. Their method perform in both identification and verification mode and the system is more efficient as the rate of accuracy in both the mode is 100% and the

© 2015-19, IJARCS All Rights Reserved

processing time is also very less. The retinal recognition using different non-vascular features is discussed above. All the authors have carried out their experiments using a different database and have obtained percentage of EER and accuracy as shown in Table 2.

Table II. Comparison Table of different Recognition methods using non-vascular feature

Method.	*No. of images*	*No. of subjects*	*Database used*	*Identification or Verification*	*Processing time (sec)*	*EER*	*Accuracy (%)*
Waheed et al. [24]	100	20	RIDB	Identification	----	0.26	92.50
	42	14	AFIO	Identification	----	0.2857	85.75
Ong et al. [25]	280	20	DRIVERA	Verification	----	0.170	----
Sabaghi et al. [28]	400	40	DRIVE	Identification	----	----	99.10
Dehghani et al. [29]	480	80	DRIVE and STARE	Both Identification and Verification	5.3s for Identification 0.07 for Verification	----	100

III. STRENGTH AND WEAKNESS OF RETINAL AUTHENTICATION

After going through the literature we observed that retina based biometric authentication system possesses its own set of strength and weakness, just like all other biometric technologies. They are mentioned below:

The strengths can be described as follows:

1) The blood vessel pattern of the retina hardly ever changes during a person's life.
2) As the retina is located at back end of the eye, it is not exposed to the threats posed by the external environment, as other organs such as fingerprint, hand geometry, face etc.
3) The stable and distinctive features of retina can be extracted from the vascular structure.
4) In comparison to other biometric characteristics, the average feature vector size of retina biometric is very small, which could result in faster verification and identification processing times. Whereas, the larger sized feature vectors could decelerate the processing times.

The weaknesses can be discussed as follows:

1) If a person is affected with some eye diseases such as hard glaucoma, cataracts, and so on then the identification process will be very complicated.
2) The image acquisition involves the cooperation of the subject, entails contact with the eyepiece, and also the retinal scanning technology cannot accommodate people wearing contact lenses.
3) The blood vessel structure of retina can divulge some medical conditions of that person which are another factor obstructing the public acceptance of retina based biometric authentication system.
4) The devices used to capture the retinal images are very expensive to procure and implement.

IV. CONCLUSION AND DISCUSSION

In this paper, the different methods used for retinal authentication are reviewed. They are mainly categorized based on vascular and non-vascular feature extraction. Among all other biometric traits, retina is the most stable characteristic for person authentication because of the uniqueness in blood vessel pattern and it consistent during one's life. In this paper, a comparative study is done on the recognition rates, equal error rates, processing time and the numbers of images taken in different methods. From the study it is found that the blood vessel patterns are the foundation for retinal recognition, therefore it is important to segment it accurately. In the survey, it is observed that most of the authors used bifurcation point and end point as a feature vector. In future, technologies must be developed to extract number of features, which will increase the efficiency of the system. It is also seen that very few authors have taken retinal images suffered from diseases like AMD, DR etc. for their experiment, so in future system must be designed so that it can identify not only a normal image but also a degraded diseased image. The main difficulty in retina based authentication system is the movement of head or eye in front of the retinal scanner. Hence, to make the system more robust it should tolerate scale, rotation, and translation for accurate identification. It has been observed that most of the methods can operate in either identification or verification mode, but it is very important to develop a method which will operate in both modes for security application. It is also required to optimize the processing time to speed up the process and to make this a real-time biometric identification system for high security.

© 2015-19, IJARCS All Rights Reserved

V. REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: Security and privacy concerns,” IEEE security & privacy, vol. 99, no. 2, pp. 33–42, 2003.

[2] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1, pp. 4–20, 2004.

[3] S. K. Sahoo, T. Choubisa, and S. M. Prasanna, “Multimodal biometric person authentication: A review,” IETE Technical Review, vol. 29, no. 1, pp. 54–75, 2012.

[4] K. A. Nixon, V. Aimale, and R. K. Rowe, “Spoof detection schemes,” in Handbook of biometrics, pp. 403–423, Springer, 2008.

[5] L. R. Kumar and A. S. Babu, “Genuine and forged offline signature verification using back propagation neural networks,” IJCSIT) International Journal of Computer Science and Information Technologies, 2011.

[6] S. Shankar, V. Udupi, and R. D. Gavas, “Biometric verification, security concerns and related issues-a comprehensive study,” 2016.

[7] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, “A novel behavioural biometric technique for robust user authentication,” IETE Technical Review, pp. 1–13, 2016.

[8] R. B. Hill, “Retina identification,” Biometrics, pp. 123–141, 2002.

[9] R. Das, “Retinal recognition: Biometric technology in practice,” Keesing Journal of Documents & Identity, vol. 22, pp. 11–14, 2007.

[10] M. Ortega, M. G. Penedo, J. Rouco, N. Barreira, and M. J. Carreira, “Personal verification based on extraction and characterisation of retinal feadture points,” Journal of Visual Languages & Computing, vol. 20, no. 2, pp. 80–90, 2009.

[11] M. Ortega, C. Marino, M. Penedo, M. Blanco, and F. Gonzalez, “Biometric authentication using digital retinal images,” in Proceedings of the 5th WSEAS international conference on Applied computer science, pp. 422–427, 2006.

[12] B. K. Ekka, N. Puhan, and R. Panda, “Retinal verification using point set matching,” in Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on, pp. 159–163, IEEE, 2015.

[13] H. Farzin, H. Abrishami-Moghaddam, and M.-S. Moin, “A novel retinal identification system,” EURASIP Journal on Advances in Signal Processing, vol. 2008, no. 1, pp. 1–10, 2008.

[14] M. U. Akram, A. Tariq, and S. A. Khan, “Retinal recognition: Personal identification using blood vessels,” in Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pp. 180–184, IEEE, 2011.

[15] S. Qamber, Z. Waheed, and M. U. Akram, “Personal identification system based on vascular pattern of human retina,” in Biomedical Engineering Conference (CIBEC), 2012 Cairo International, pp. 64–67, IEEE, 2012.

[16] J. Fatima, A. M. Syed, and M. U. Akram, “A secure personal identification system based on human retina,” in Industrial Electronics and Applications (ISIEA), 2013 IEEE Symposium on, pp. 90–95, IEEE, 2013.

[17] A. Arneodo, N. Decoster, and S. Roux, “A wavelet-based method for multifractal image analysis. i. methodology and test applications on isotropic and anisotropic random rough surfaces,” The European Physical Journal B-Condensed Matter and Complex Systems, vol. 15, No. 3, pp. 567–600, 2000.

[18] C. K¨ose, C. ˙Iki, et al., “A personal identification system using retinal vasculature in retinal fundus images,” Expert Systems with Applications, vol. 38, no. 11, pp. 13670–13681, 2011.

[19] M. Khakzar and H. Pourghassem, “A rotation invariant retina identification algorithm using tessellation-based spectral feature,” in Biomedical Engineering (ICBME), 2014 21th Iranian Conference on, pp. 309–314, IEEE, 2014.

[20] S. M. Lajevardi, A. Arakala, S. A. Davis, and K. J. Horadam, “Retina verification system based on biometric graph matching,” IEEE transactions on image processing, vol. 22, no. 9, pp. 3625–3635, 2013.

[21] A. Hussain, A. Bhuiyan, A. Mian, and K. Ramamohanarao, “Biometric security application for person authentication using retinal vessel feature,” in Digital Image Computing: Techniques and Applications (DICTA), 2013 International Conference on, pp. 1–8, IEEE, 2013.

[22] A. P. Condurache, J. Kotzerke, and A. Mertins, “Robust retina-based person authentication using the sparse classifier,” in Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European, pp. 1514–1518, IEEE, 2012.

[23] A. Zahedi, H. Sadjedi, and A. Behrad, “A new retinal image processing method for human identification using radon transform,” in 2010 6th Iranian Conference on Machine Vision and Image Processing, pp. 1–4, IEEE, 2010.

[24] Z. Waheed, A. Waheed, and M. U. Akram, “A robust non-vascular retina recognition system using structural features of retinal image,” in 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 101–105, IEEE, 2016.

[25] E. P. Ong, Y. Xu, D. W. K. Wong, and J. Liu, “Retina verification using a combined points and edges approach,” in Image Processing (ICIP), 2015 IEEE International Conference on, pp. 2720–2724, IEEE, 2015.

[26] H. Oinonen, H. Forsvik, P. Ruusuvuori, O. Yli-Harja, V. Voipio, and H. Huttunen, “Identity verification based on vessel matching from fundus images,” in 2010 IEEE International Conference on Image Processing, pp. 4089–4092, IEEE, 2010.

[27] M. Sabaghi, S. R. Hadianamrei, A. Zahedi, and M. N. Lahiji, “A new partitioning method in frequency analysis of the retinal images for human identification,” Journal of Signal and Information Processing, vol. 2, no. 04, p. 274, 2011.

[28] M. Sabaghi, S. R. Hadianamrei, M. Fattahi, M. R. Kouchaki, and A. Zahedi, “Retinal identification system based on the combination of Fourier and wavelet transform,” 2012.

[29] A. Dehghani, Z. Ghassabi, H. A. Moghddam, and M. S. Moin, “Human recognition based on retinal images and using new similarity function,” EURASIP Journal on Image and Video Processing, vol. 2013, no. 1, pp. 1–10, 2013.

© 2015-19, IJARCS All Rights Reserved