Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends

Sunil Swamilingappa Harakannanavar[1]
[1]S. G. Balekundri Institute of Technology, Belagavi-590010, Karnataka, India
sunilsh143@gmail.com
Prashanth Chikkanayakanahalli Renukamurthy[2]
[2]Dr. Ambedkar Institute of Technology, Bangalore-560056, Karnataka, India
prashanthcr.ujjani@gmail.com
Kori Basava Raja[3]
[3]University Visvesvaraya College of Engineering, Bangalore, Karnataka, India

ABSTRACT

Authentication is the key parameter to speak the truth of an attribute claimed by the real entity. There are several ways to make authentication more robust and biometrics is one among them. From past decade, Biometric technology is widely adopted and accepted everywhere to authenticate an individual's identity. Also the adopted technology overcomes the limitations faced by the traditional authentication process such as knowledge based issues including password and token for the authentication of an individual. This paper makes a comprehensive study of the existing biometric methodologies, their usage and limitations that are employed in real time cases. It also presents the motivation for adapting biometrics in current situations. In addition to this, it also makes an attempt to talk on the technical and security related issues towards biometric systems.

Keywords— **Biometrics, authentication, security, password, real time.**

Date of Submission: Nov 30, 2018 Date of Acceptance: Dec 21, 2018

I. INTRODUCTION

Biometric refers to unique characteristics of an individual person such as physiological or behavioral which doesn't change with time. The physiological characteristics include fingerprint, iris, palmprint, face, etc., and the behavioral characteristics such as hand-written signature, voice, gait and walking style of individual, typing style on keyboard [2][4][5][7]. Biometric plays a very important role to identify and verify (to confirm the identity of a claimant) an individual's identity [21]. The human characteristics such as physiological or behavioral traits can be used for biometrics in terms of related parameters described in table 1.

Table 1: Desirable properties of Biometric traits

Parameters	Descriptions
Universality	Each candidate should have characteristic.
Uniqueness	Each has separate characteristics and do not matches with other person.
Permanence	Measures how better a biometric resists aging and over time.
Collectability	Ease of acquisition for measurement.
Performance	Accuracy and robustness of techniques used.
Acceptability	Degree of approval of a technology.
Circumvention	Ease of use of a substitute.

The biometric procedure consists of enrolment and verification stage. In enrolment process the one or more biometric features of the individual person are validated against known biometric profile. Therefore, the verification section requires a one-to-one match to decide the results such as genuine or imposter. In case of identifying a person, biometric identity of unknown person is matched with others in known database. Hence, identification of individual is performed using one-to-many comparison. The effectiveness of authenticator including biometric or non-biometric based on their relevance to a particular application along with their robustness to various types of attacks. Choudary et al., [53] lists a several attacks that are launched against authentication systems on passwords and tokens.

- Client attack (passwords guessed, tokens are stealed).
- Host attack (accessing plain text file containing passwords).
- Eaves dropping (shoulder surfing for passwords).
- Repudiation (claiming that tokens are misplaced).
- Trojan horse attack (bogus log-in screen are installed to steal passwords).
- Denial of service (deliberately supplying an incorrect password several times leads to failure the system).

Hence, the biometrics offers several advantages viz., negative recognition and nonrepudiation which are not provided by traditional techniques such as tokens and passwords.

A. Objective of the Scope

Biometrics provide better security and more suitable than other conventional methods of human recognition. In few

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

applications, biometrics can supplement the current technology. This paper makes a comprehensive study of the existing biometric methodologies, their usage and limitations that are employed in real time cases. The rest of the article is organized as follows: the various categories of biometric and their challenges are discussed in Section II. The general block diagram of the biometric system is described in Section III. Section IV discusses about performance parameters to measure their accuracy. Section V discusses the advantages and applications of biometric systems. Section VI concludes the detailed work on biometric system.

II. BIOMETRIC TECHNOLOGIES AND CHALLENGES

In this section, the major biometric traits based on human's characteristics to authenticate an individual identity along with major advantages and challenges of each technology are discussed. Figure 1 shows the various biometric traits.

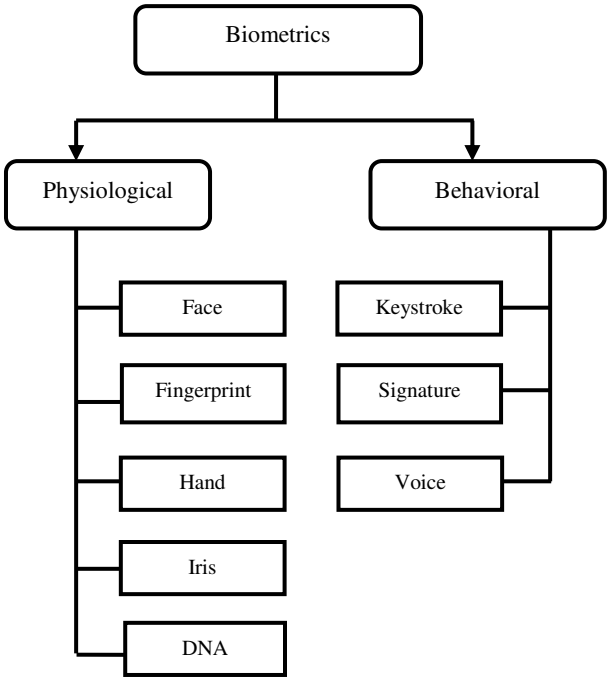


Figure 1: General block diagram of Biometrics system

Biometric refers to unique characteristics of an individual person such as physiological or behavioral which doesn't change with time. The physiological characteristics include face, fingerprint, iris, hand, DNA etc., and the behavioral characteristics such as hand-written signature, voice and typing style on keyboard etc.

A. Face Recognition

It is an universal truth that every individual has a unique face, it can be adopted as a biometric profile for secure authentications [28][29]. This idea of usage of face for authentications has emerged into face recognition systems. The face is captured using high capacity cameras and is used as a template for matching. Now the template is matched using various pattern matching techniques to identify or verify an individual identity. Figure 2 shows the scanner and samples of face database.

Figure 2: Face scanner and Samples of face database

The various face databases such as ORL, JAFFE, Indian databas, Yale, Multi Pie, AR database, FERET database, Combined Face database etc., are used to obtain the rates.

Challenges: Face recognition is an eminient biometric trait offers several challenging tasks. Some of them are listed as follows

- face rotation (pose variation)
- variation in lighting conditions (illumination problem)
- persons wearing collusions such as hat, scrap, eye glasses, etc.,
- various facial expressions degrades the performance of the system.

Research needs to be more focused to address above issues in order to implement reliable recognition system.

B. Fingerprint Recognition

A fingerprint consists of loop, arch and whorl patterns. It appears as a series of dark lines and white spaces, when captured from device [15][18]. Figure 3 shows the fingerprint scanner and sample.

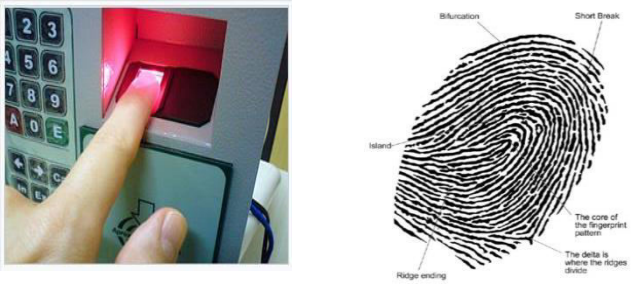


Figure 3: Fingerprint Scanner and sample

The matching is performed using Minutiae based (relies on locations and directions of minutiae points) and the pattern matching (fingerprints can be compared to judge the similarity.

Challenges: The recognition rate of biometric profile degrades when the finger is wet and wrinkled. Research needs to be focused to address when the finger is wet and wrinkled towards development of system.

C. Hand Recognition

The human's hand or fingers can be used as biometric profile for authentication because its arrangement contains the spatial geometry with different dimensions (unique) for every person and cannot be altered [31][32]. It is required to measure two or three fingers of a subject to authenticate an individual as it requires a very low space

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

for storage. Figure 4 shows the hand geometry scanner and sample.

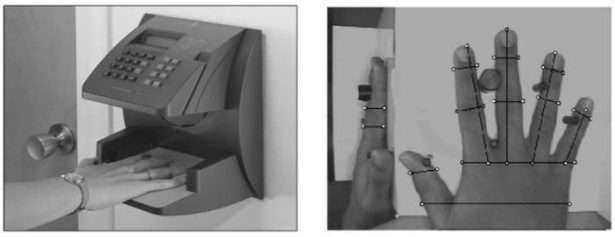


Figure 4: Hand Geometry Scanner and sample

Challenges: The research should be advanced to reduce the hardware requirements.

D. Iris Recognition

The iris of every individual possesses certain unique characteristics that can be used to distinguish individuals [36][38]. It is a colored muscular ring around the pupil of the eye which contains inner zone as pupillary zone and the outer zone as ciliary zone whereas the iris lies between cornea and lens of the human eye as shown in Figure 5.

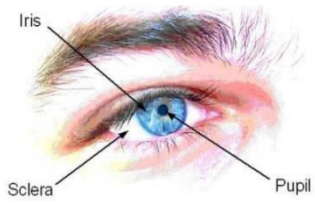


Figure 5: Eye diagram

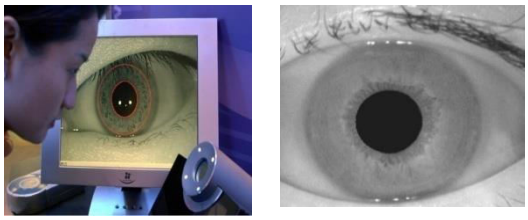


Figure 6: Iris Scanner and CASIA sample

For authentication process, the iris images are captured by the scanner and the iris patterns are analysed using various iris databases such as CASIA, MMU, UPOL, IITD etc., to obtain the performance rate. Figure 6 shows the iris scanner and sample of CASIA database.

Challenges: The recognition rate degrades, when the human eyes are covered by some occlusions and if the face images with various facial expressions are captured from the device.

Research in this area needs to be more improved to assure its reliability against important factors namely contact lenses, eye glasses, watery eyes etc.

E. Retina Recognition

This biometric profile is based on the pattren of blood vessel within the retina of human eye. The characteristics generated from the blood vessel pattern is unique and can be used for authentication process. In addition to this, the retinal characteristics of identical twins are also unique and served as the foundation for retinal recognition system [40][43]. The image blood vessel pattern (retina) is captured and stored as a biometric template for further process to identify the individuals.

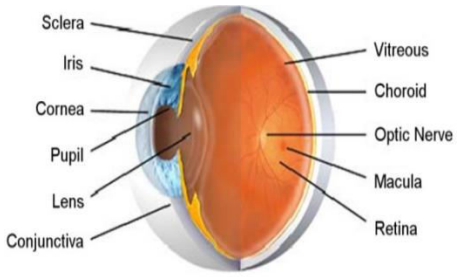


Figure 7: Anatomy of human eye showing retina

Challenges: It has to be developed to distinguish and identify individual wearing glasses or lens.

F. DNA Recognition

At present, DNA recognition is an intrusive aproach and it needs a form of saliva, blood, semen, hair, tissue sample etc., for authentication process [44][46]. Figure 8 shows the structure of DNA.

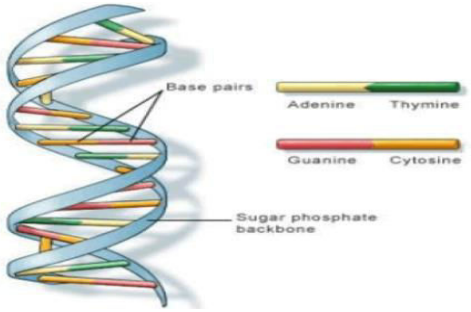


Figure 8: DNA structure

Challenges: This approach is not automatic and the method of aquisition of samples needs to be developed.

G. Keystroke Recognition

The style of hitting keys in the keyboard comes under the category of behavioral characteristic of human. The technology examines key stroke dynamics including time taken by a person to type the password, speed and pressure.

Figure 9: Keystroke

Challenges: Technology has to be developed more to increase the accuracy.

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

H. Signature Recognition

Signature biometric trait comes under the category of behavioral characteristic of human. This approach captures informative details namely direction, speed, pressure of writing and shape of signature [42] [45].

Figure 10: Signature samples

Challenges: Long term reliability and lack of accuracy are the main issues to be focused in this approach.

I. Voice Recognition

Every individual has own vocal characteristics, so it can be adopted as a biometric profile to authenticate an individual's identity, this is known as speech recognition [47][49]. Here, the sensor records the voice signal and further it will be converted into a unique digital code (template) and processed to recognize the person.

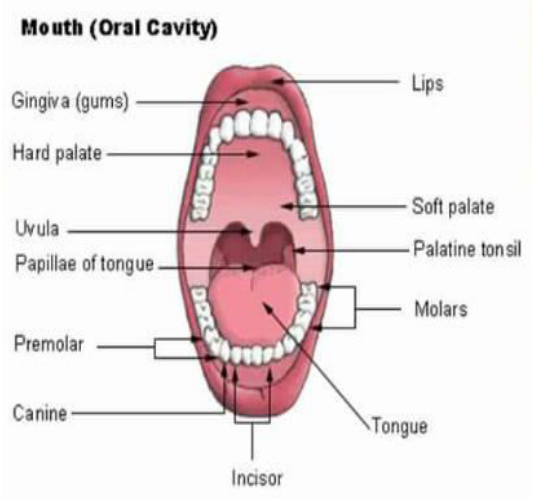


Figure 11: Voice recognition

J. Comparison of Various Biometrics Techniques

A brief comparison of various biometric technique based on their accuracy, cost and convenience is provided in table 2 and comparison of various biometrics traits based on the desirable properties is given in Table 3.

Table 2: Desirable properties of Biometric traits [47]

Rank	Accuracy	Cost	Convenience
1	DNA	Voice	Voice
2	Iris	Signature	Face
3	Retina	Finger	Signature
4	Finger	Face	Finger
5	Face	Iris	Iris
6	Signature	Retina	Retina

Table 3: Comparison of various Biometrics traits based on the desirable properties [47]

Biometric Traits	Circumvention	Permanence	Acceptability	Uniqueness	Universality	Collectability	Measurability
Face	Low	Medium	High	High	High	High	High
Fingerprint	High	Medium	Medium	High	Medium	Medium	High
Ear	Low	High	High	High	Medium	High	High
Iris	Low	Medium	Low	High	Medium	Low	High
Palm Print	Medium	Medium	Medium	Medium	Medium	Medium	High
Signature	High	Medium	Medium	High	Low	Medium	High
Voice	High	Medium	High	Medium	High	High	High
Gait	Low	Medium	High	Medium	High	High	Medium
Keystroke	Medium	Medium	High	Medium	Medium	Medium	Medium

Figure 12: Voice authentication to digital banking

Challenges: The technology need to be advanced to store the unique digital code by decreasing the space. And also, the accuracy degrades, when the person's voice changes (emotional or sick).

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

III. BIOMETRIC SYSTEMS

A biometric system works in two modes namely identification mode (one to one comparison for subject verification) and Verification mode (one to many comparisons to establish an individual identity). The general biometric system used to authenticate/identify an individual person is shown in Figure 13. The biometric system contains four important blocks.

- Data acquisition
- Preprocessing
- Feature extraction
- Comparison and decision.

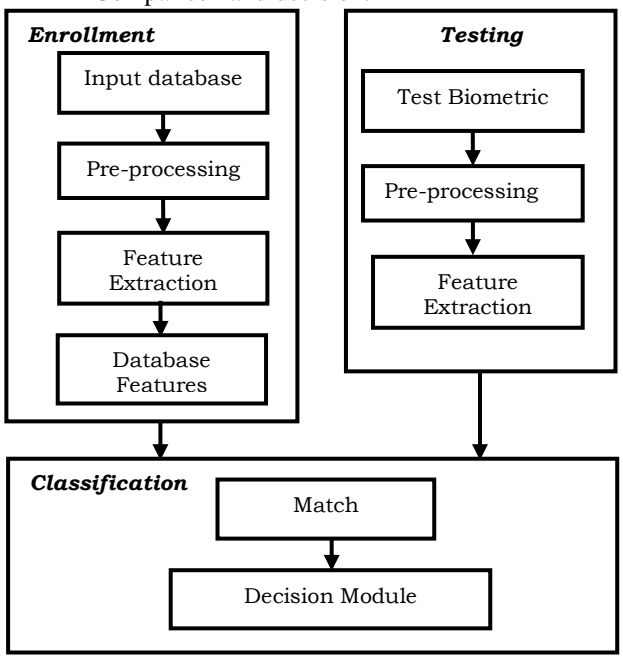
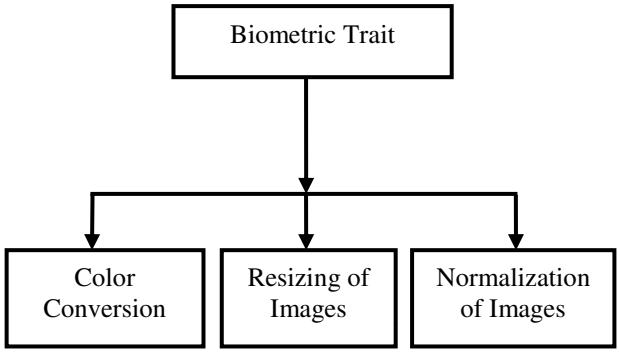


Figure 13: General block diagram of Biometric system

A. Preprocessing

In image processing, the pre-processing is adopted as a primary stage to improve the quality of the images that are captured from the devices [31] [34]. The process of pre-processing includes (i) Color Conversion (ii) Resizing (iii) Normalization. The fundamental steps of preprocessing are shown in Figure 14.

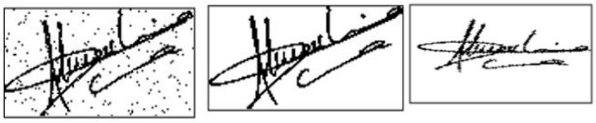


Fundamental steps of Pre-processing

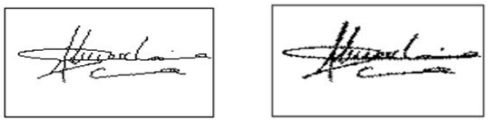
(i) Color Conversion: It performs the conversion operation from colour to gray scale image producing an intensity values between 0 and 255.

(ii) Resize: The size of the original images are increased or decreased without losing any information content of the original image. Most of the time the images are resized by applying cropping operation.

(iii)Normalization: It includes noise removal, rotation, thinning, smoothing etc. The database images and test images are normalized before applying the images to extract the features. The normalized images of signature trait are shown in Figure 15.



(a) Original Image (b) Noise removal (c) Smoothed image



(d) Thinned image (e) Rotated image

Figure 15: Normalized images of Signature biometric trait

B. Feature Extraction

Once the images are pre-processed, it is required to apply the feature extraction algorithms to extract the informative details of the images. The features of the images are extracted from three important domains (i) Spatial domain (ii) Transform domain (iii) Hybrid domain.

(i) Spatial Domain

Spatial domain features: The statistical parameters such as mean, variance and standard deviation are computed from the intensity values of spatial domain images. The Principal Component Analysis (PCA), Local Discriminant Analysis (LDA) [21] [25], Local Binary Pattern (LBP), Local Ternary Pattern (LTP), Speeded Up Robust Features (SURF), Independent Component Analysis (ICA), Singular Value Decomposition (SVD) [32] [34], Scale Invariant Feature Transform (SIFT) etc., are used to obtain spatial domain features. The fusions of two or more spatial domain features are necessary to improve the performance rate of the system. The fusions of two or more spatial domain feature types are shown in Figure 16.

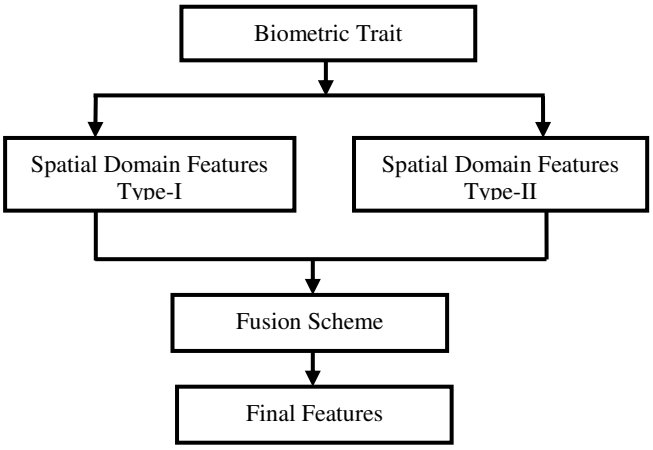


Figure 16: Fusion of Spatial domain features

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

(ii) Transform Domain

The spatial domain images are converted into frequency domain (transform domain) to extract the effective details of the images. The techniques such as Fast Fourier Transform FFT) [21], Discrete Cosine Transform (DCT) [25], Discrete Wavelet Transform (DWT) [26], Complex Wavelet Transform (CWT) [29], Dual Tree Complex Wavelet Transform (DTCWT) [31] etc., are transform domain approaches that are applied on pre-processed images to extract the sufficient details of images (features). The fusion of two or more transform domain feature types are shown in Figure 17.

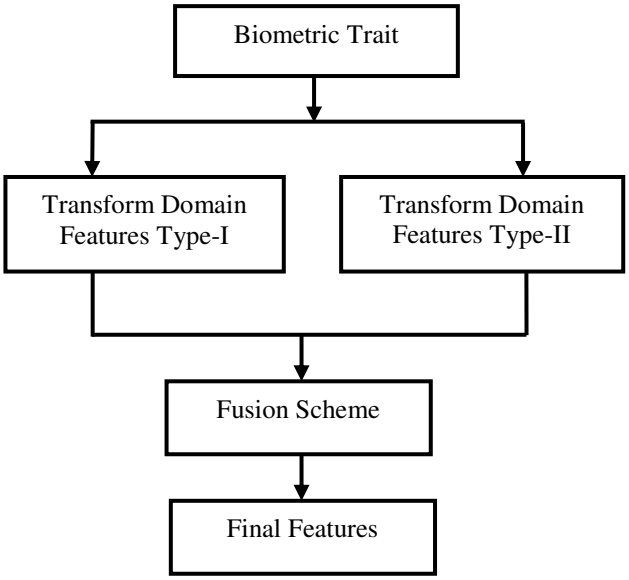


Figure 17: Fusion of Transform domain features

(iii) Hybrid Domain:

The combination of spatial and transform domain techniques are applied on biometric trait images to extract the final features is known as hybrid domain technique [35][37]and is shown in Figure 18.

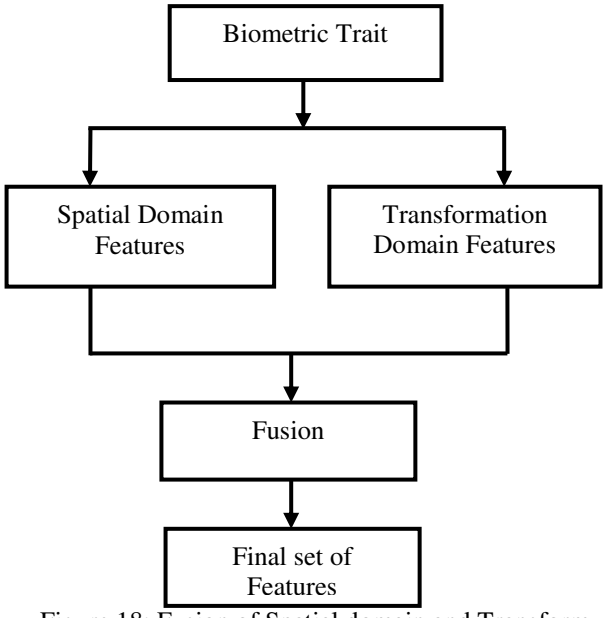


Figure 18: Fusion of Spatial domain and Transform domain features

Consider the image that decomposed into cell1 and cell2. Now apply the spatial domain to cell-I and transform domain to cell-II individually to obtain the features. Finally the features obtained by the combination of both the domains are fused to get the final features are shown in Figure 19.

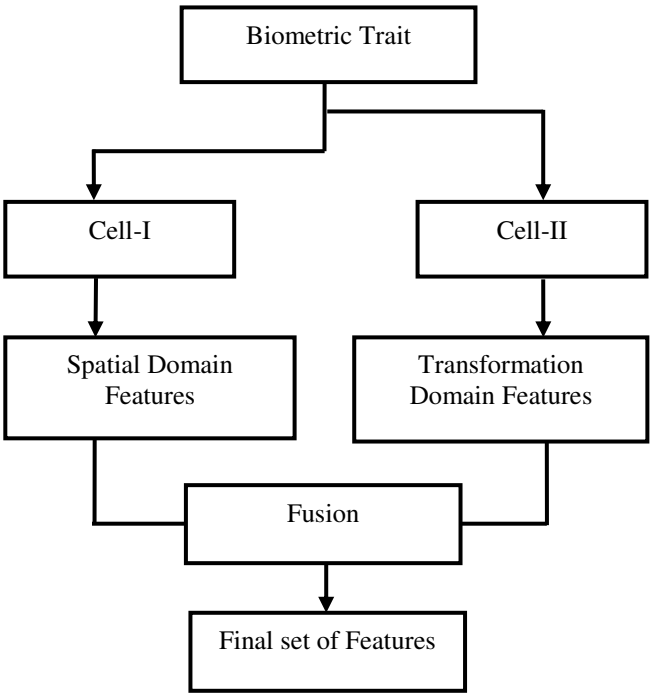


Figure 19: Decomposition of image into cells

C. Classification

For the authentication of an individual, the features of test image and database image are compared using certain classifiers viz., Euclidean Distance (ED), Hamming distance (HD), Chi-Square distance (CSD) [51], Support Vector Machine (SVM) [52], Random Forest (RF), K-Nearest Neighborhood (K-NN), Neural Network (NN) etc. The block diagram of matching procedure is shown in Figure 20. Based on the classification result obtained, the biometric system takes a decision of acceptance or rejection of the sample.

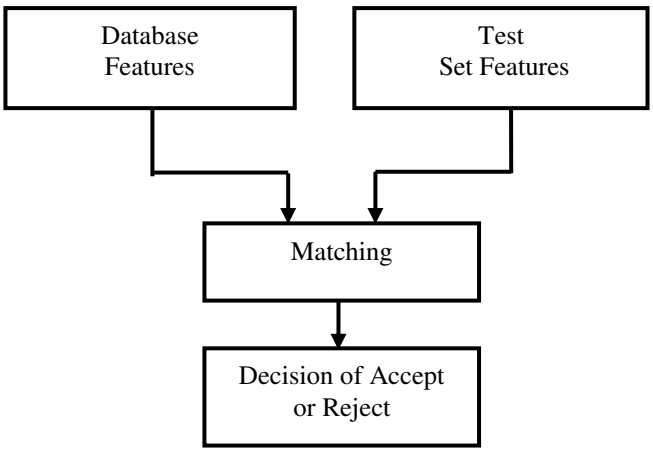


Figure 20: Matching of features

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

IV. PERFORMANCE EVALUATION OF BIOMETRIC SYSTEMS

The main aspect of biometrics techniques is to evaluate their performance. The performance of any biometric techniques can be measured by various parameters namely False Accept Rate (FAR), False Reject Rate (FRR), Crossover Rate (CER) or Equal Error Rate (EER) and True Successive Rate (TSR) [47][48][51]. The performance of the verification process depends on the feature vectors (X_I) and the similarity $S(X_q, X_I)$. Based on the matching scores and a predetermined value, it is possible to estimate the accuracy of a biometric system. From the database of feature sets, two distributions of matching scores can be generated namely genuine (match) and imposter (non-match). For genuine, scores produced between pairs of samples from the same person and for imposter, scores produced between pairs of samples from the different persons. Figure 21 shows the graphical representation of FAR, FRR and EER parameters to evaluate the accuracy of biometric system [37] [38].

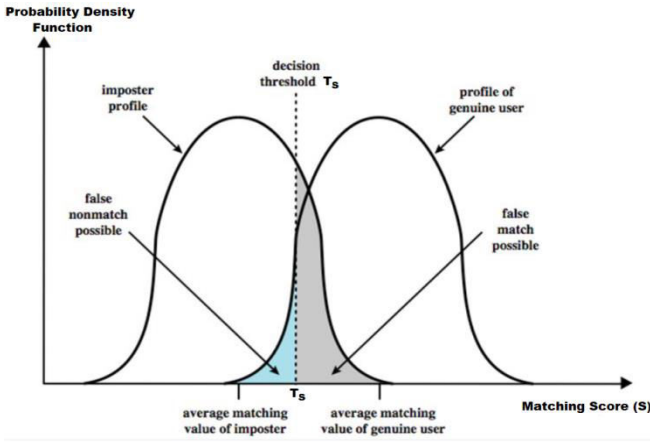


Figure 21: Probability density function v/s matching score [37]

The decision of accept and reject is based on the similarity index. It accepts, if $S(X_q, X_I) \geq T_s$ and rejects, if $S(X_q, X_I) < T_s$. The FAR and FRR are defined by considering areas A and B, shown in Figure 22, when a threshold value 'T_s' is chosen.

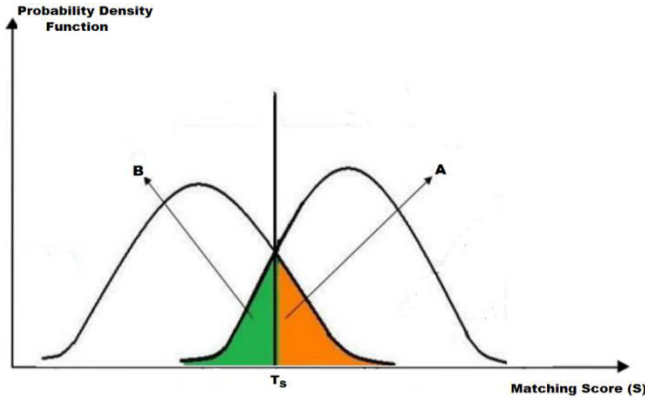


Figure 22: Probability density function v/s matching score for known threshold value 'T_s' [38]

- Area A (i.e., $S > T_s$): It is noticed that some imposters are falsely accepted in this region. So it is said to be False Accept Rate (FAR) or False Match Rate (FMR) or Type-I error. To estimate $P_n(s)$ for Type-I error is given in equation 1.

$$\boldsymbol{FAR = \int_{Ts}^{\infty} P_n(S)\, ds} \text{----------(1)}$$

- Area 'B (i.e., $S \leq T_s$): It is noticed that some genuine users are falsely rejected in this region. So it is said to be False Rejected Rate (FRR) or False Non Match Rate (FNMR) or Type-II error. To estimate $P_n(s)$ for Type-II error is given in equation 2.

$$\boldsymbol{FRR = \int_{-\infty}^{Ts} P_m(S)\, ds} \text{----------(2)}$$

I. Estimation of the score distributions from a set of feature vectors

Assume two sets, $X=\{X_1, X_2, \ldots\ldots X_M\}$ is a set of M match scores (genuine) and $Y=\{Y_1, Y_2, \ldots\ldots Y_N\}$ is a set of N match scores (imposter). Then match and non-match score distributions for sets X and Y are given in equation 3 and equation 4 respectively.

$$\boldsymbol{P_m(S) = \frac{1}{M}\sum_{i=1}^{M} 1(X_i = S), \quad \forall S} \text{----------(3)}$$

$$\boldsymbol{P_n(S) = \frac{1}{N}\sum_{j=1}^{M} 1(Y_j = S), \quad \forall S} \text{----------(4)}$$

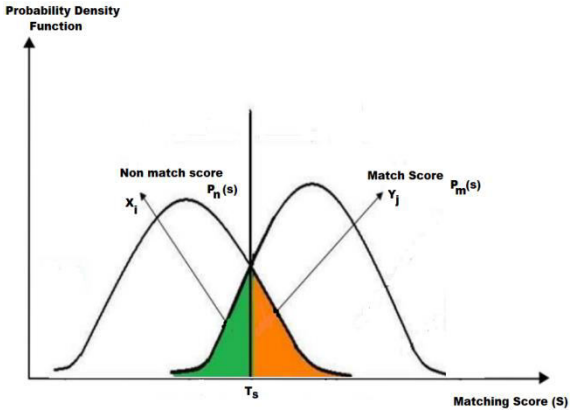


Figure 23: Probability density function v/s matching score [38]

In this case as shown in Figure 23, the decision of accept and reject is based on the similarity index. It accepts, if $S(X_q, X_I) \geq T_s$ and rejects, if $S(X_q, X_I) < T_s$. Depending upon the choice of the threshold value (T_s), the FAR and FRR rates will be different.

- Lowering 'T_s' will make the system more tolerant (false acceptance is more). Therefore FAR will increase.

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

- Increasing 'T_s' will make the system more secure (false rejection is more). Therefore FRR will increase.

Using two sets X={X_1, X_2, …….X_M} and Y={Y_1, Y_2, …….Y_N} which represents genuine and imposter scores respectively. It is possible to estimate FAR and FRR which is given in equation 5 and equation 6.

$$FAR(T_s) = \frac{1}{N}\sum_{j=1}^{N} 1(Y_j > T_s) \text{----------(5)}$$

$$FRR(T_s) = \frac{1}{M}\sum_{i=1}^{M} 1(X_i \leq T_s) \text{----------(6)}$$

J. Threshold Value (T_s):

As application require certain acceptable values of FAR and FRR, threshold value 'T_s' can be determined. The following graph shown in Figure 24 gives the error rates at different threshold values.

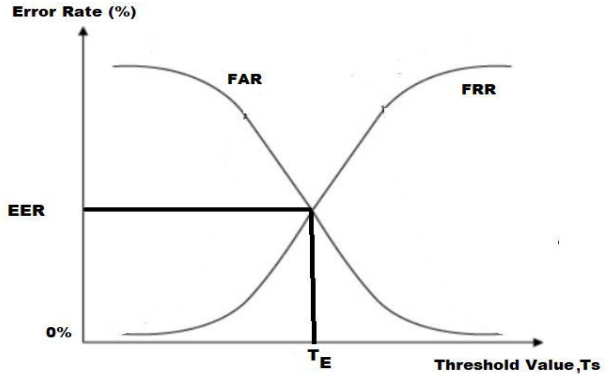


Figure 24: Graph of EER for different Threshold values [38][54]

By knowing the value of FAR and FRR, 'T_E' can be determined. The lower value of EER produces the higher efficiency of the biometric system.

K. Receiver Operating Characteristic (ROC) Curve

It is noticed that there is another way to measure the performance parameters of the biometric system by plotting FAR against FRR and the obtained curve is called as ROC curve shown in Figure 25.

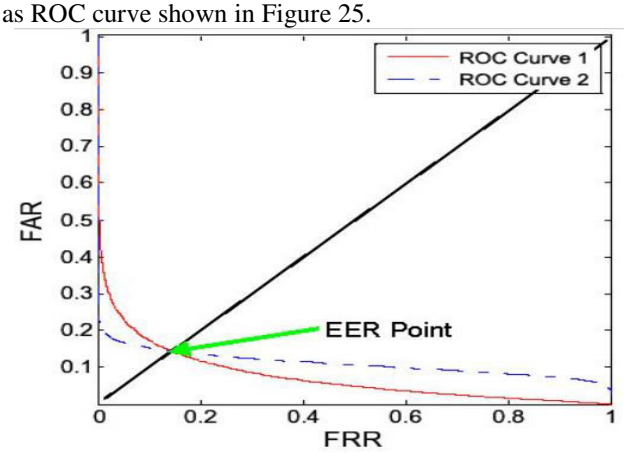


Figure 24: Graph of FAR v/s FRR [38][54]

The possible error rate for the different biometric traits is shown in Figure 26.

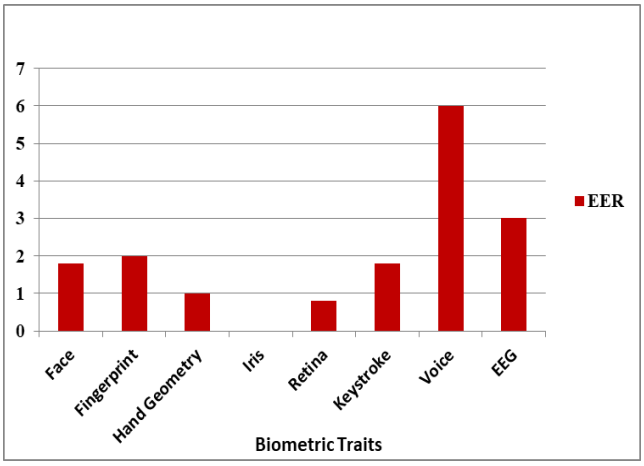


Figure 26: The Equal Error Rate (EER) for different biometric systems [53]

L. Other Possible Errors

The performance of the biometric system degrades for FAR, FRR and EER increases. In addition to these errors, the failure to capture (FTC) which results when the system fails to capture the image characteristics and other is failure to enroll (FTE) that results, when the system rejects poorly captured images during enrollment stage [38][54].

V. ADVANTAGES AND APPLICATIONS

The advantages of adopting biometrics for authentication of an individual are listed below.

- Security: The biometric systems offer a higher degree of security than conventional methods.
- Accountability: The biometric-based authentication systems are able to keep track of the user's activities.
- Scalability: The biometric-based authentication systems are easily scalable.

Biometric systems are extensively used in various fields for identification and authentication issues of an individual. Some of the applications of biometric systems are as follows

- Attendance and time monitoring in classes.
- Banking systems.
- Boarding pass for personal authentication
- Home security systems
- Electronic voting and ATM machine to secure an individual
- Military force to authenticate refugee.
- Companies, government offices, institutions and other private sectors to authenticate employees.
- Entry to high security places such as parliamentary house and defense zone.

VI. CONCLUSION AND FUTURE SCOPE

Biometric technology is widely adopted and accepted everywhere to authenticate an individual's identity. Also the adopted technology overcomes the limitations faced by the traditional authentication process such as knowledge

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

based issues including password and token for the authentication of an individual. This paper makes a comprehensive study of the existing biometric methodologies, their usage and limitations that are employed in real time cases. It also presents the motivation for adapting biometrics in current situations. In addition to this, it also makes an attempt to talk on the technical and security related issues towards biometric systems. In future, the individual traits can be replaced by multi-factor authentication and the behavioral biometrics can analyze candidates and helps users to re-identify them.

REFERENCES

[1] Anil K Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no.1, pp. 1-29, 2004.

[2] Kresimir Delac and Mislav Grgic, "A Survey of Biometric Recognition Methods," *IEEE International Symposium on Electronics in Marine*, pp. 184-193, 2004.

[3] Arun Ross and Anil Jain, "Information Fusion in Biometrics," *Pattern Recognition Letters*, vol. 24, pp. 2115-2125, 2003.

[4] Manuel R Freire, Julian Fierrez and Javier Ortega-Garcia, "Dynamic Signature Verification with Template Protection using Helper Data," *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1713-1716, 2008.

[5] Alonso Fernandez, MC Fairhurst, J Fierrez and J Ortega-Garcia, "Impact of Signature Legibility and Signature Type in Off-line Signature Verification," *IEEE International Biometrics Symposium*, pp. 1-6, 2007.

[6] Lucas Ballard, Daniel Lopresti and Fabian Monrose, "Forgery Quality and Its Implications for Behavioral Biometric Security," *IEEE Transactions on System, Man and Cybernetics*, vol. 37, no. 5, pp. 1107-1118, 2007.

[7] Shih Yin, Andrew Beng, Jin Teoh and Thian-Song Ong, "Compatibility of Biometric Strengthening with Probabilistic Neural Network," *IEEE International Symposium on Biometrics and Security Technologies*, pp. 88-93, 2008.

[8] Yu Qiao, Jianzhuang Liu and Xiaoou Tang, "Off-line Signature Verification using On-line Handwriting Registration," *IEEE International Conference on Computer Vision and Pattern Recognition*, pp. 1-8, 2007.

[9] Vu Nguyen, Michael Blumenstein and Graham Leedham, "Global Features for the Off-line Signature Verification Problem," *IEEE International Conference on Document Analysis and Recognition*, pp. 1300-1304, 2009.

[10] Tirtharaj Dash, Tanishta Nayak and Subaghata Chattopadhyay, "Off-line Handwritten Signature Verification using Associative Memory Net," *International Journal of Advanced Research in Computer Engineering and Technology*, vol. 1, no. 4, pp. 370-374, 2012.

[11] M P Dale and M A Joshi, "Fingerprint Matching using Transform Features," *IEEE International Conference on Technology, Education and Networking,* pp. 1-5, 2008.

[12] M Dadgostar, P R Tabrizi, E Fatemizadeh and H Soltanian-Zadeh, "Feature Extraction using Gabor Filter and Recursive Fisher Linear Discriminant with Application in Fingerprint Identification," *IEEE International Conference on Advances in Pattern Recognition,* pp. 217-220, 2009.

[13] Zhang Yuanyuan and Jing Xiaojun, "Spectral Analysis Based Fingerprint Image Enhancement Algorithm," *IEEE International Conference on Image Analysis and Signal Processing,* pp. 200-203, 2010.

[14] Chomtip Pornpanomchai and Apiradee Phaisitkulwiwat, "Fingerprint Recognition by Euclidean Distance," *IEEE International Conference on Computer and Network Technology*, pp. 437-441, 2010.

[15] Sarat Dass, "Assessing Fingerprint Individuality in presence of Noisy Minutiae," *IEEE Transactions on Information Forensics and Security,* vol. 5, no. 1, pp. 62 - 70, 2010.

[16] Narayan Vetrekar, Kiran B Raja, R Raghavendra, R S Gad and Christoph Busch, "Band Level Fusion using Quaternion representation for extended Multi-Spectral face Recognition", *IEEE International Conference on Information Fusion*, pp. 1-16, 2017.

[17] Navaneeth Bodla, Jingxiao Zheng, Hongyu Xu, Jun Cheng Chen, Carlos Castillo and Rama Chellappa, "Deep Heterogeneous Feature Fusion for Template Face Recognition", *IEEE International Conference on Applications of Computer Vision*, pp. 586-595, 2017.

[18] Ze Lu, Xudong Jiang and Alex Kot, "Enhance Deep learning Performance in face Recognition", *IEEE International Conference on Imaging, Vision and Computing*, pp. 244-248, 2017.

[19] Menglu Wu and Tongwei Lu, "Face Recognition based on LBP and LNMF Algorithm", *IEEE International Symposium on parallel and Distributed computing*", pp. 368-371, 2016.

[20] Jesus Olivares Mercado, Karina Toscano Medina and Gabriel Sanchez Perez, "Face Recognition System for Smartphone based on LBP", *IEEE International Workshop on Biometrics and Forensics,* pp. 1-6, 2017.

[21] Ashraf S Huwedi and Huda M Selem, "Face Recognition using Regularized Linear Discriminant Analysis under Occlusions and Illumination Variations", *IEEE International Conference on Control Engineering and Information Technology*, pp. 1-5, 2016.

[22] Zhihan Xie, Peng Jiang and Shuai Zhang, "Fusion of LBP and HOG using Multiple Kernel Learning for Infrared Face Recognition", *IEEE International Conference on Computer and Information Science*, pp. 81-84, 2017.

[23] Yichuan Wang, Zhen Xu, Weifeng Li and Qingmin Liao, "Illumination Robust Face Recognition with

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

Block-Based Local Contrast Patterns", *IEEE International Conference on Acoustics, Speech and Signal Processing,* pp. 1418-1422, 2017.

[24] Haoxi Li, Haoshan Zou and Haifeng Hu, "Modified Hidden Factor Analysis for Cross Age Face Recognition", *IEEE Journals and Magazines on Signal Processing Letters*, vol. 24, no. 4, pp. 465-469, 2017.

[25] Jou Lin and Ching Te Chiu, "LBP Edge-Mapped Descriptor using MGM Interest points for face recognition", *IEEE International Conference on Acoustics, Speech and Signal Processing,* pp. 1183-1187, 2017.

[26] Kang Geon Kim, Feng Ju Chang, Jangmoo Choi, Louis Philippe and Morency, "Local-Global-landmark Confidences for Face recognition", *IEEE International Conference on Automatic Face and Gesture Recognition*, pp. 666-672, 2017.

[27] Jagadeesh N and Chandrasekhar M Patil, "Conceptual view of the Iris recognition systems in the biometric world using image processing techniques", *IEEE International Conference on Computing Methodologies and Communication*, pp. 1018-1022, 2017.

[28] Charan S G, "Iris Recognition using Feature Optimization", *IEEE International Conference on Applied and Theoretical Computing and Communication Technology*, pp. 726-731, 2016.

[29] Dolly Choudhary, Ajay Kumar Singh and Shamik Tiwari, "A Statistical Approach for Iris Recognition Using K-NN Classifier", *International Journal of Image, Graphics and Signal Processing*, vol. 5, no. 4, pp. 46-52, 2013.

[30] Anithakumar A and Maya V Karki, "Iris Recognition System with Error Detection and Reconstruction Algorithms for Template Security", *IEEE International Conference On Recent Trends in Electronics Information & Communication Technology*, pp. 824-829, 2017.

[31] Akshay Agarwal, Rohit Keshari, Manya Wadhwa, Mansi Vijh, Chandani Parmar, Richa Singh and Mayank Vatsa, "Iris sensor identification in multi-camera environment", *Elsevier Information Fusion*, vol. 45, pp. 333-345, 2019.

[32] K Ivanko, N Budik and N Ivanushkina, "Feature Selection for Biometric Iris Recognition", *IEEE Workshop on Advances in Information, Electronic and Electrical Engineering,* pp. 1-5, 2017.

[33] Christian Rathgeb and Christoph Busch, "Improvement of Iris Recognition based on Iris-Code Bit Error Pattern Analysis", *International Conference of the Biometrics Special Interest Group,* pp. 1-6, 2017.

[34] M Rabiul Islam, "Feature and Score Fusion Based Multiple Classifier Selection for Iris Recognition", *Hindawi International Computational Intelligence and Neuroscience,* pp. 1-12, 2014.

[35] Gayathri Rajagopal and Ramamoorthy Palaniswamy, "Performance Evaluation of Multimodal Multi-feature Authentication System Using KNN Classification", *Hindawi International Scientific World Journal,* pp. 1-9, 2015.

[36] Vineet Kumar, Abhijit Asati and Anu Gupta, "A Novel Edge-Map Creation Approach for Highly Accurate Pupil Localization in Unconstrained Infrared Iris Images", *Hindawi International Journal of Electrical and Computer Engineering,* pp. 1-10, 2016.

[37] Anil K Jain, Karthik Nandakumar and Arun Ross, "50 years of biometric research, Accomplishments, Challenges and Opportunities", *Pattern Recognition Letters*, vol. 79, pp. 80-105, 2016.

[38] Jain K Anil, Ross Arun and Prabhakar Salil, "An introduction to biometric recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004.

[39] A K Jain, A Ross and S Pankanti, "Biometrics, A Tool for Information Security", *IEEE Transactions on Information Forensics And Security*, vol. 1, no. 2, pp. 125-144, 2006.

[40] C Miyamoto, S Baba and I Nakanishi, "Biometric person authentication using new spectral features of electroencephalogram", *IEEE International Symposium of Intelligent Signal Processing and Communications Systems*, pp. 1-4, 2009.

[41] Koji Tsuru and Gert Pfurtscheller, "Brainwave Biometrics, A New Feature Extraction Approach with the Cepstral Analysis Method", *Transactions of Japanese Society for Medical and Biological Engineering*, vol. 50, no. 1, pp. 62-167, 2012.

[42] R Palaniappan and D P Mandic, "Biometrics from brain electrical activity, A machine learning approach", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, pp.738-742, 2017.

[43] A Riera, A Soria-Frisch, M Caparrini, C Grau and G Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis", *Eurasip Journal of Advanced Signal Processing*, pp. 1-8, 2008.

[44] J Hu, "New biometric approach based on motor imagery EEG signals", *International Conference on Future BioMedical Information Engineering*, pp. 94-97, 2009.

[45] P Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface", *International Journal of Computer Applications*, vol. 14, no. 5, pp. 10-15, 2011.

[46] Himanshu Srivastva, "A Comparison Based Study on Biometrics for Human Recognition", *International Journal of Computer Engineering*, vol.15, pp. 22-29, 2013.

[47] Gursimarpreet Kaur and Chander Kant Varma, "Comparative Analysis of Biometric Modalities", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 4, pp. 603-613, 2014.

[48] R Kavitha Jaba Malar and V Joseph Raj, "Geometric Finger Nail Matching using Fuzzy Measures", *International Journal of Innovative Technology and Exploring Engineering*, vol. 4, no. 4, pp. 1-8, 2014.

[49] Himanshu Srivastava, "Personal Identification Using Iris Recognition System, A Review", *International*

Volume: 10 Issue: 04 Pages: 3958-3968 (2019) ISSN: 0975-0290

Journal of Engineering and Applications, vol. 3, pp. 449- 453, 2013.

[50] T R Saraswathi, G Mishra and K Ranganathan, "Study of lip prints", *International Journal of Forensic Dental Science*, vol. 1, no. 1, pp. 28-31, 2009.

[51] Shradha Tiwari, J N Chourasia and Vijay S Chourasia, "A Review of Advancement in Biometric Systems", *International Journal of Innovative Research in Advanced Engineering*, vol. 2, no. 1, pp. 187-204, 2015.

[52] Shrutika Deokar and Sudeep Talele, "Literature Survey of Biometric Recognition Systems", *International Journal of Technology and Science*, vol. 1, no. 2, pp. 1-5, 2014.

[53] Choudhury B, Then P, Issac B, Raman V and Haldar M K, "A Survey on Biometrics and Cancelable Biometrics Systems", *International Journal of Image and Graphics*, pp. 1-28, 2018.

[54] R M Bolle, J H Connel, S Pankanti, N K Ratha, A W senior, "Guide to Biometrics", *Springer*, 2004.

Author's Profile

Mr. Sunil S Harakannanavar completed his Bachelor of Engineering in the stream of Electronics & Communication Engineering from Sri Taralabalu Jagadguru Institute of Technology, Ranebennur and his Masters in the field of Microelectronics and Control Systems from Nitte Mahalinga Adyanthaya Memorial Institute of Technology, Nitte. Presently he is working as Assistant Professor with S. G. Balekundri Institute of Technology Belagavi. He is pursuing his Ph.D at Visvesvaraya Technological University, Belagavi and his area of interests includes Computer Vision, Pattern Recognition and Biometrics. He is a life member of Indian Society for Technical Education, New Delhi and Institute for Exploring Advances in Engineering (IEAE).

Dr. Prashanth C R received the BE degree in Electronics, ME degree in Digital Communication and Ph.D degree from Bangalore University, Bangalore. He is currently working as a Professor, Department of Telecommunication Engineering, Dr. Ambedkar Institute of Technology, Bangalore. His research interests include Computer Vision, Pattern Recognition and Biometrics. He is a life member of Indian Society for Technical Education, New Delhi, Member of IEEE, IACSIT, ACM and Fellow of Institution of Engineers.

Dr. K. B. Raja is a Professor and Chairman, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics & Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 200 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing and Computer Networks.