IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-6, Issue-1 E-ISSN: 2347-2693

Biometrics System: An Overview

Shubhangi Neware

Assistant Professor, Dept. of CS, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

Corresponding Author: newareshubhangi@gmail.com,newares@rknec.edu, Tel.: 9425519266

Available online at: www.ijcseonline.org

Received: 30/Dec/2017, Revised: 06/Jan/2018, Accepted: 22/Jan/2018, Published: 31/Jan/2018

***Abstract*—** Use of biometrics system growing rapidly due to increase in demands for rigorous security in applications like national identity cards, border security, government benefits, network or computer login, time and attendance management, criminal investigation, passport control and access control. This paper is a review paper presenting introduction to biometrics technology comprising of its working, classification and operating modes. Different biometric modalities and related research work by researchers is also presented in this paper. Performance metrics for biometric system is also presented. This paper helps researchers to know the overall working of biometric system and research areas associated with different modalities in the field of biometrics.

***Keywords*—** Biometrics, Finger Knuckle Print (FKP), Ocular Biometrics, verification, identification, False Acceptance,False Rejection, Equal Error Rate.

I. INTRODUCTION

The global biometrics market is growing very rapidly due to increase need of security, person identity and authenticity applications in different areas. Commercial applications are needed for authentication technologies that not only provide reliable security but are also extremely difficult to spoof. Biometrics is one such solution that fulfils all these conditions as well as provides a great deal of convenience to the users. Biometrics is the science and technology used to analyze and measure biological data of human being. In computer security, biometrics refers to authentication techniques that are based on measurable physical or behavioural characteristics that can be automatically checked. Biometrics is the most accurate form of identifiers and it can greatly simplify life if used properly. Biometric traits such as fingerprint, palm print, face, and iris cannot be stolen, lost or forged. As a result adoption of biometrics technology is increasing rapidly in different areas. Recently identified areas for use of biometric technology are mobile payment, online banking, immigration services, eGovernment processes, workforce management, health care and welfare, multifactor authentication, point of sale (POS), Internet of things and wearable devices etc. Following sub-sections are introducing the basic concepts of biometric system such as overall working of biometric system, classification and operating modes of biometric system. This review paper is contributing towards biometric related research work by presenting overall working of biometric system and research areas associated with different modalities in the field of biometrics.

1.1 Block Diagram of Biometrics System

A typical biometric system with its basic components is as shown in Figure-1. First step is related to the data acquisition that uses various input devices to capture data using different biometric identifiers .Input devices provides an interface between the real world and the system. After acquisition of the data it is to be pre-processed. Pre-processing includes operation such as removal of background and finding region of interest. Third step is feature extraction where the acquired data is processed using algorithms to extract feature vectors. This is an important step as the correct features need to be extracted in the optimal way. Feature vectors are then used to create templates. Template is a synthesis of the relevant

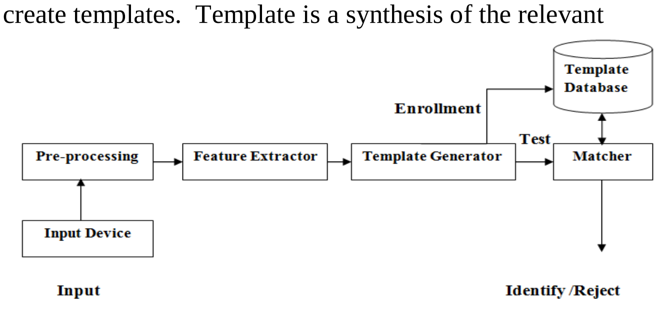

Figure-1 Block Diagram of Biometrics System

Characteristics extracted from the source. Feature extracted from collected samples is then stored in database.
First time when an individual's biometric information captured and stored in the database is known as enrolment process. Enrolment process is needed to be done for every genuine person. In matching phase, the obtained template

which is to be tested is passed to matcher that compares it with other existing templates those are in the template database. Matcher estimates the distance between template to be tested and the existing templates using algorithms. Matcher module finds best match with optimal distance. Matcher module decides whether claimed identity is accepted or rejected.

1.2 Classification

Biometric systems recognize user based on their physiological and behavioural characteristics. Therefore biometric systems can be classified as follows [14].

Physiological: These are related to the shape of the body. The oldest trait under this category that is being used today in various applications is fingerprint. Face recognition, hand geometry, palm print and iris recognition technology also use physical characteristics of a person.

Behavioural: These are related to the pattern of behaviour of a person. Signature of a person is most common characteristic that is used today in banking and ecommerce applications. More modern approach is the study of keystroke dynamics . Further voice recognition and gait analysis are other examples of behavioural trait. The design and suitability of biometric technology for person identification depends on the requirements of applications. These requirements are typically specified in terms of identification accuracy, throughput, user acceptance, system security, robustness, and return on investment.

1.3 Operating Modes

Two basic operating modes of biometric systems are verification and identification. The identification process involves comparison of the biometric information of a person to be identified against templates corresponding to all users in the database. On the other hand verification process involves comparison with only those templates corresponding to the claimed identity. In verification mode the user claims an identity. Based on claim identity biometric system performs “one to one” matching and determine whether claim is true or not. But in identification mode system conducts “one to many” comparisons to identify a person [1] [4].

Section I contains introduction to biometric system which further include block diagram, working, classification and operating modes of typical biometric system. Section II consists of information about different biometric modalities and its related research work. Section III consists of use of emerging biometric modalities to identify a person. Section IV includes performance metrics that is needed to evaluate performance of any biometric system. Section V is introducing the concepts of multimodal biometrics. Lastly section VI is concluding section that concludes overall paper.

II. BIOMETRIC MODALITIES AND RELATED RESEARCH WORK

Biometric modality is a class or category of biometric system depending on the type of human trait it takes as input. It is also called as biometric identifiers. Commonly implemented or studied modalities include face, iris, voice, fingerprint, hand geometry, palm print and signature. The selection of a particular biometric modality depends on the nature and requirements of the intended identification application [1] [7]. Figure 2 shows the different biometric modalities that are being used for different applications.

(a) Fingerprint: Fingerprint based recognition system is more popular and successful system for person identification. It has been used for many centuries. Fingerprint consists of a texture pattern of ridges located on tip of each finger. Landmark point on ridges is called as minutiae. It is in the form of ridge endings and ridge bifurcations. These minutiae point is claimed to be unique for each fingerprint. In fingerprint matching process comparison of two-dimensional minutiae patterns extracted from an individual’s finger with minutiae patterns saved in the template database will take place. T. Yang [30] presents an approach that uses localized secondary features derived from relative minutiae information. A flow network-based matching technique is introduced to obtain one-to-one correspondence of secondary features. This method balances the tradeoffs between maximizing the number of matches and minimizing total feature distance between query and reference fingerprints. At two-hidden-layer fully connected neural network is trained to generate the final similarity score based on minutiae matched in the overlapping areas. A. Abhayankar [31] utilizes a wavelet based approach to detect liveness, integrated with the fingerprint matcher. The integrated system of fingerprint matcher and liveness module gives EER as 0.03%.

(b) Voice: Speech or voice-based recognition systems identify a person based on their spoken words. Voice generation depends on the shape and size of vocal tracts, lips, nasal cavities, and mouth of a person. The movement of lips, jaws, tongue, velum, and larynx constitute the behavioural component of voice. These components can vary over time due to aging and medical condition of a person. Speaker recognition is highly suitable for applications like tele-banking. Voice biometric is primarily used in verification mode.

(c) Iris: Coloured annular ring that surrounds the pupil is called as iris. Iris images acquired under infrared illumination consist of complex texture pattern. Its complex pattern contains many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and freckles. Irises of identical twins are different. Throughout adulthood the iris is supposed to be consistent but it varies up to adolescence. John Daugman [25] presents the four advances in iris recognition: 1) more disciplined methods for detecting and faithfully modelling the iris inner and outer boundaries with active contours, leading to more flexible embedded coordinate systems; 2) Fourier-based methods for solving problems in iris trigonometry and projective geometry, allowing off-axis gaze to be handled by detecting it and “rotating” the eye into orthographic perspective; 3) statistical inference methods for detecting and excluding eyelashes; and 4) exploration of score normalizations, depending on the amount of iris data that is available in images and the required scale of database search.

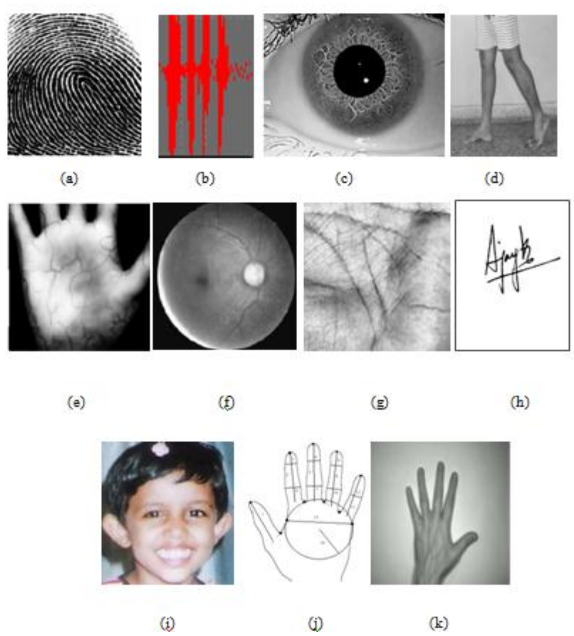

Figure-2 Biometric modalities (a) Fingerprint (b) Voice (c) Iris (d) Gait (e) Palm vein (f) Retina (g) Palm print (h) Signature (i) Face (j) Hand Geometry (k) Hand Vein

(d) Gait: Gait is the peculiar way one walks. It is a behavioural biometric identifier. This biometric modality aimed to recognize person by their walking patterns. Gait analysis is the systematic study of human walking. Gait analysis using wearable sensors is an inexpensive, convenient, and efficient manner of providing useful information for multiple health-related applications. As a clinical tool applied in the rehabilitation and diagnosis of medical conditions and sport activities, gait analysis using wearable sensors shows great prospects [21]. The Smartphone and portable media devices, such as the iPhone and iPod, constitute wireless accelerometer platforms capable of acquiring gait features based on the acceleration waveform. The accelerometer data can be transmitted by wireless connectivity to the Internet as an email attachment [22].

(e) Palm Print and Palm vein: Latent palm print identification is of growing importance in forensic applications. Palms of the human hands contain unique pattern of ridges, valleys, principal lines, and Palm print is expected to be even more reliable than fingerprint as it covers larger area as compared to fingerprint. Many of the researchers considered palm print for personal identification. Guagming Lu, David Zhang [11] has been worked on palmprint recognition using mathematical based approach. By using Karhunen–Loeve transform, they transformed the original palm print images into a small set of feature space, called ‘‘eigenpalms’’. Eigenpalms are the eigenvectors of the training set and can represent the principal components of the palm prints. Then, the eigenpalm features are extracted by projecting a new palm print image into the subspace spanned by the ‘‘eigenpalms’’. Euclidean distance classifier used for palm print recognition. Zhang D., Wai-Kin Kong, Wong M. [12] implemented online palm print identification. A robust image coordinate system was defined by them to facilitate image alignment for feature extraction. In addition to this they proposed a 2D Gabor phase encoding scheme for palm print feature extraction and representation. Connie et al [5] developed palm print recognition using PCA (Principal Component Analysis) and ICA (Independent Component Analysis). Latent palm print matching using minutiae features was presented by Anil K. Jain and Feng [8]. Michael Goh, Kah Ong, Connie Tee, Andrew Teoh, Beng Jin[6] proposed touch less palm print biometrics using local binary pattern (LBP) texture descriptor on the palm print directional gradient responses.

Palm vein is also identified as biometric modality that uses the vascular patterns produced on human palm as a biometric data for personal identification. Compared with back of hand palm has broad and more complicated vascular pattern which is helpful to differentiate among individuals.

(f) Retina: This biometric modality uses vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Retina is protected in an eye itself, and it is not easy to change or replicate the retinal vasculature. Therefore this is one of the most secure biometric. H Tabatabaee, A Milani-Fard, H Jafariani [23] presents a novel human identifier system using retina image and fuzzy clustering approach.

(g) Signature: Signature is a behavioural biometric modality and can be used in daily business transactions. Due to large intra class variations in person’s signature over time it may not be highly accurate. Accuracy can be gain using dynamic or online capturing of signature which requires pressure sensitive pen pad. Dynamic signatures help to acquire the shape, pen pressure, order and speed of strokes during the actual act of signing. M.Faundes [24] proposed On-line signature recognition based on vector quantization (VQ), nearest neighbor (NN), dynamic time warping (DTW) and Hidden Markov Models (HMM).

(h) Face: Human being have a natural ability to identify a person by his/her face. Face recognition systems typically utilize the relationship among the locations of facial features such as nose, eyes, chin, lips, eyebrows and the global appearance of a face. Face recognition is non-intrusive and has high user acceptance. It provides acceptable levels of recognition performance under controlled environments. Robust face recognition in non-ideal situations still has pose challenges. Z Chen, W Huang, Z Lv [27] proposed Sparse Preserving Projection (SPP) for feature extraction. The discriminant information was introduced into SPP to arrive at a novel supervised feather extraction method that named Uncorrelated Discriminant SPP (UDSPP) algorithm. J Yang, L Luo, J Qian, Y Tai, F Zhang [28] proposed nuclear norm based matrix regression with applications to face recognition with occlusion and illumination changes

(i) Hand Geometry: Hand geometry involves the comparisons between dimensions of fingers, location of joints, shape and size of palm. Person identification using hand geometry utilizes hand images to extract a number of geometrical features such as length, width and thickness of fingers. Ajay Kumar and David Zhang [26] investigate the possibilities to improve the performance of the existing hand-geometry systems using the discretization of extracted features. This paper proposes employing discretization of hand-geometry features, using entropy-based heuristics, to achieve the performance improvement. Doublet, J. Lepetit, Revenu [10] employed contact less hand recognition using shape and texture features by combining information from colour and texture.

(j) Hand vein: The pattern of blood vessels hidden underside of the skin is quite dissimilar in individuals and also stable over long period of time. A vein carries blood from one part of the body to another part and therefore vascular pattern is spread throughout the body. The veins that are present in hands are easy to acquire (using near infrared illumination) and can be used for the biometric identification. For biometric purposes, CCD or CMOS camera with high sensitivity to the sub-spectrum of infrared radiation has to take a snapshot of the vein pattern or, depending on the application requirements, offer real-time image processing with the help of progressive scan algorithms [20]. Radon like features method has been applied by R. B.Trabelsi for preprocessing of hand vein image [4].

However each biometric modality has its own advantages and disadvantages. Factors that can determine the suitability of above discussed biometric modalities for any application are listed as follows.

1) Universality. This factor determines the availability of biometric trait in every individual accessing the application. Universality means how commonly a biometric identifier can be found in an individual and how readily it can be used.
2) Uniqueness. Degree by which biometric trait differentiates one person from another.
3) Permanence. Biometric trait must be sufficiently invariant with respect to time. It should not vary over long period of time.
4) Measurability. This factor indicates the ease of acquiring biometric characteristics using corresponding devices. Measurability considers practical aspect of using various devices for acquiring biometric characteristics.
5) Performance. It indicates the biometric systems accuracy, robustness and speed.
6) Acceptability. It indicates the degree of acceptability of biometric identifier by people.
7) Circumvention. This refers to the difficulty to spoof a biometric system [7].

III . EMERGING BIOMETRIC MODALITIES

3.1 Finger Knuckle Print

Texture pattern produced by the finger knuckle bending (knuckle joint) is called as Finger Knuckle Print (FKP). FKP can be extracted from inner side (Figure-3) or back side of finger surface (Figure-4). FKP is highly unique and makes the knuckle surface as a distinctive biometric identifier. The finger back surface at knuckle joint can be highly useful for user identification purpose and has attracted attention of very few researchers. A. Kumar [2] employed subspace methods such as ICA and LDA. Finger geometry features were also extracted from the same image at the same time and integrated to further improve the user identification accuracy of such a system. Ajay Kumar, Yingbo Zhou [3] investigated a new approach for efficient and effective personal identification using KnuckleCodes.

Figure -3 Inner Knuckle Surface

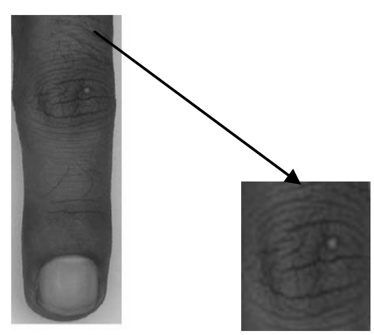

Figure-4 Outer Knuckle Surface

S. Neware et al proposed Finger Knuckle Identification using RLF and Dynamic Time Warping. They also proposed Finger Knuckle Identification using Principal Component Analysis and Nearest Mean Classifier. K.Mehta and S. Neware investigated new approach for Finger Knuckle Feature Extraction using Radon like Features. They have also proposed Finger Knuckle Print Identification using Gabor Features [15] [16] [17] [18] [19].

3.2 Ocular and Periocular Biometrics

Ocular biometrics exploits characteristic features extracted from the eyes for personal recognition. Ocular biometric modalities in visible light have mainly focused on iris, blood vessel structures over the white of the eye (mostly due to conjunctival and episcleral layers), and periocular region around eye. Most of the existing studies on iris recognition use the near infrared spectrum. However, conjunctival vasculature and periocular regions are imaged in the visible spectrum. U.Park [32] extracted Global and local information from the periocular region using texture and point operators resulting in a feature set that can be used for matching. G. Santos [33] proposed the application of well-known iris and periocular recognition strategies based on classical encoding and matching techniques, as well as demonstrating how they can be combined to overcome the issues associated with mobile environments.

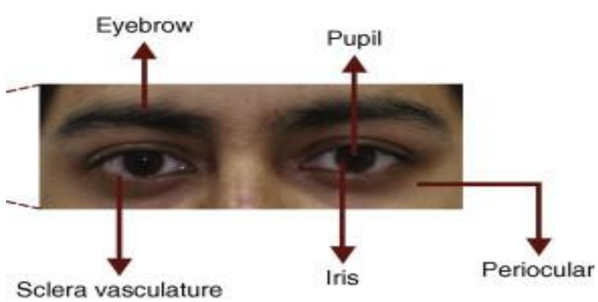

Figure-5 Ocular Biometrics

.

IV. PERFORMANCE MEASURES

Performance metrics obtained from a biometric system is the most important factor for the deployment of any biometric system. The biometric system's performance is measured by its error rates. Three types of errors or failure that may occur in biometric systems are Failure to Enrol (FTE), False Accept Rate (FAR) and False Reject Rate (FRR). Transaction time or throughput may also be used to evaluate system performance. The accuracy of a biometric system is not static. It is dependent on the data which is influenced by several factors such as (a) biometric quality, which is related to the quality of input signal/image, (b) composition of target user population (e.g. gender and age), (c) size of database is related to the number of persons enrolled in the system, (d) time interval between enrolment and verification / identification process, (e) variations in the operating environment such as temperature, humidity, and illumination, (f) distinctiveness of biometric modality, and (g) robustness of employed algorithms (feature extraction and matching algorithms).

4.1 Decidability Index

The Decidability Index (*Di*) can be used to assess the overall quality of similarity measurement used by a biometric system. *Di* is the ratio of the difference between genuine and impostor distribution means over the combined measure of their standard deviations. *Di* measures the amount of overlap between the matching score distributions. A smaller *Di* value indicates a larger overlap.

$$Di = \frac{|\,\mu_G - \mu_I|}{\sqrt{(\sigma_G^2 + \sigma_I^2)/2}}$$

Where

μ_G is the mean of genuine matching scores

μ_I is the mean of imposter matching scores

σ_G is the standard deviation of genuine matching scores

σ_I is the standard deviation of imposter matching scores

4.2 FAR and FRR

False acceptance and false rejection are two main errors that can be encountered in any biometric system. False acceptance means accepting persons those are not enrolled in database. Persons those are not enrolled in database are termed as 'imposter'. Now false rejection means rejecting persons those are enrolled in database. Persons those are enrolled in database are termed as 'genuine'. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application. At a given threshold, the probability of accepting the imposter is known as False Acceptance Rate (FAR) and probability of rejecting the genuine user is known as False Rejection Rate (FRR). For a given biometrics system, it is not possible to reduce both these errors simultaneously.

FAR can be computed as:

FAR = NFA/NIIA where

FAR is the false acceptance rate.

NFA is the number of false acceptances.

NIIA is the number of impostor identification attempts.

FRR can be computed as:

FRR = NFR/NEIA where

FRR is the false rejection rate.

NFR is the number of false rejections.

NEIA is the number of enrolee identification attempts.

4.3 ROC Curve & Equal Error Rate

The receiver operating characteristics (ROC) curve is another measure used for measuring performance of a biometric system. ROC is generated by plotting FAR against FRR for different thresholds. ROC curve represents how the false rejection rate and false acceptance rate vary according to the threshold. Equal error rate (EER) is the error rate where FAR = FRR. EER is the error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances (Figure-6). A smaller EER value indicates better performance of biometric system.

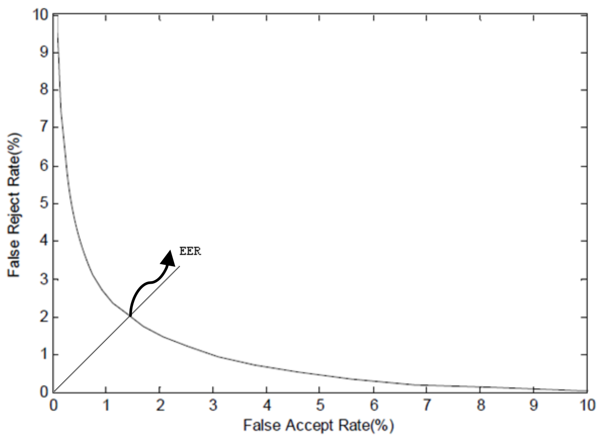

Figure-6 ROC Curve and EER

V. MULTIMODAL BIOMETRICS

A biometric system that performs verification/ identification using more than one physiological or behavioral characteristic/modality is termed as Multimodal Biometrics. Use of multiple modalities reduces false non-match and false match rates, providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample.

Ross and Jain [13] have presented an overview of Multimodal Biometrics and have proposed various levels of fusion, the different modes of operation, integration strategies and design issues. A multimodal system can operate in three different modes: serial mode, parallel mode, or hierarchical mode. In the serial mode of operation, the output of one modality is typically used to narrow down the number of possible identities before the next modality is used. Therefore, multiple sources of information (e.g., multiple traits) do not have to be acquired simultaneously. Further, a decision could be made before acquiring all the traits. This can reduce the overall recognition time. In the parallel mode of operation, the information from multiple modalities is used simultaneously in order to perform recognition. The levels fusion proposed for multimodal systems are broadly categorized into three system architectures by performing fusion at the Feature extraction Level, at the Matching Score Level and at the decision Level.

In Fusion at the Feature Extraction Level, information extracted from the different sensors is encoded into a joint feature vector, which is then compared to an enrollment template and assigned a matching score as in a single biometric system.

In Fusion at the Matching Score Level**,** feature vectors are created independently for each sensor and are then compared to the enrollment templates which are stored separately for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score which is passed to the decision module.

In Fusion at the Decision Level, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote. This architecture is rather loosely coupled system architecture, with each subsystem performing like a single biometric system.

VI. CONCLUSION

Biometrics systems are widely used to overcome the problems associated with the traditional methods of authentication in different applications. This paper introduces overall working of biometric system including different modalities and their related research work. Performance metrics such as FAR, FRR, EER and DI needed to evaluate any biometric system is also presented in this paper. EER can be determined using ROC curve. EER value should be less for better performance of the biometric system. A unimodal biometric system may fail due to insufficient biometric data. To overcome these problems associated with unimodal biometrics, multiple modalities may be involved to identify/verify a person called multimodal biometrics. This paper presented different fusion criteria that may be used in multimodal biometrics. Individual scores of multiple modalities may be fused at different levels in order to develop a multimodal biometric system. Multimodal biometrics using different fusion methods is an emerging research area in the field of biometrics. This review paper is an attempt to help new researchers to understand overall working of biometric system and also to identify research scope using different biometric modalities.

REFERENCES

[1]A.K. Jain, R. Bolle, S. Pankanti, “Biometrics: A personal identification in networked society”, Kluwer academic publishers, 2006.

[2]A. Kumar, C. Ravikanth, “Personal Authentication Using Finger Knuckle Surface”, IEEE Transactions on Information Forensics and Security, Vol 4, no 1, 98 –110, 2009.

[3]A. Kumar and Y. Zhou, “ Human Identification using Knuckle Codes”, BTAs Proceedings of third IEEE International Conference on Biometrics: Theory, Applications and Systems, 147-152,2009.

[4]B. Randa, Trabelsi, D. Alima, M. Sellami, “Hand Vein Image Enhancement with Radon Like Features Descriptor”, World Academy of Science, Engineering and Technology, Vol 7, 06-20, 2013.

[5]C. Tee, T. Andrew, G. Michael, N. David, “Palmprint Recognition with PCA and ICA”, Proceedings of Image and vision computing, 227-232, 2003.

[6]G. Michael, O. Kah, T. Connie, Andrew. Beng J., "Bimodal Palmprint and Knuckleprint Recognition system", Journal of IT in Asia, Vol3, 2010.
[7] A. K. Jain, A Kumar, "Biometrics of Next Generation: An Overview, Second Generation Biometrics", Springer, 2010.
[8] A. K. Jain and J. Feng, " Latent Palmprint Matching", IEEE Transactions on Pattern Analysis Machine Intelligence, Vol 31, no. 6, 1032-1047,2009.
[9]G. Michael, O. Kah, T. Connie , Andrew T, Beng J, "Touchless Palmprint Biometrics", Image And Vision Computing, Elsevier, Vol. 26, no. 12,1551-1560,2008.
[10]J. Doublet, O. Lepetit, Revenu, "Contactless Hand Recognition using Shape and Texture Features", IEEE Signal processing, 8th international conference, ISBN 0-7803-9736-3, Vol-3, 2006.
[11] L. Guangming, David , W Kuanquan, "Palmprint Recognition Using Eigenpalms Features", Elsevier Pattern Recognition Letters 24, 1463–1467,2003.
[12] A.S. Naik , S.M. Metagar , P.D. Hasalkar, "A Survey on Secure Crypto-Biometric System using Blind Authentication Technique", International Journal of Volume Computer Sciences and Engineering,vol-2 , Issue-5 , Page no. 93-97, May-2014.
[13] A. Ross & A. K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.
[14] A. K. Jain, P.J. Flynn, A. Ross, "Handbook of Biometrics", Springer-Verlag, USA, 2007.
[15] S. Neware, K. Mehta, A.S. Zadgaonkar, "Finger Knuckle Identification using RLF and Dynamic Time Warping", International Journal of Computer Applications (0975 – 8887), Volume 119 , No.3,2015.
[16] S. Neware, K. Mehta, A.S. Zadgaonkar, "Finger Knuckle Print Identification using Gabor Features", International Journal of Computer Applications (0975 – 8887) ,Volume 98, No. 16,2014.
[17] K. Mehta, S. Neware, A.S. Zadgaonkar, "Finger Knuckle Feature Extraction using Radon like Features", International Journal of Computer Science & Communication, ISSN 0973-7391,Volume 5, 134-137,2014.
[18] S. Neware, K. Mehta, A.S. Zadgaonkar, "Finger Knuckle Identification using Principal Component Analysis and Nearest Mean Classifier", International Journal of Computer Applications, (0975 – 8887) Volume 70, No. 9,2013
[19] S. Neware, K. Mehta, A.S. Zadgaonkar, "Finger Knuckle Surface Biometrics", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, No. 12,2012.
[20]R. Jiang et al. (eds.), "Biometric Security and Privacy", Signal Processing for Security Technologies, Springer International Publishing Switzerland 2017.
[21] Weijun Tao, "Gait Analysis Using Wearable Sensors", Sensors 12(2), 2012,
[22] R.Lemoney, "Wearable and wireless gait analysis platforms: Smartphones and portable media devices", Wireless MEMS Networks and application, Pages 129–152, 2017
[23] H Tabatabaee, A Milani-Fard, H Jafariani , "A novel human identifier system using retina image and fuzzy clustering approach", Proceedings of the 2nd IEEE International conference, 2006.
[24] M.Faundes, "On-line signature recognition based on vq-dtw", pattern recognition, volume 40, issue 3, pages 981-992, 2007.
[25]J. Daugman, "New Methods in Iris Recognition", IEEE transactions on systems, man, and cybernetics—part b: cybernetics, vol. 37, no. 5, 2007.
[26] A. Kumar, D. Zhang, "Hand-Geometry Recognition Using Entropy-Based Discretization", IEEE transactions on information forensics and security, vol. 2, no. 2, 2007.
[27] Z Chen, W Huang, Z Lv , "Towards a face recognition method based on uncorrelated discriminant sparse preserving projection", Multimedia Tools and Applications, Springer, 2017.
[28] J.Yang L Luo, J Qian, Y Tai, F Zhang, " Nuclear norm based matrix regression with applications to face recognition with occlusion and illumination changes", IEEE transactions , 2017.
[30] T.Yang, V. Govindaraju, "A minutia-based partial fingerprint recognition system", Pattern Recognition 38, 1672 – 1684, 2005.
[31] A. Abhyankar, S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition", Pattern Recognition, Elsevier, 2008.
[32] U. Park, A. Ross, A. K. Jain, "Periocular Biometrics in the Visible Spectrum: A Feasibility Study, Theory, Applications and Systems", BTAS 09, Washington DC, September 2009.
[33] G. Santos, H. Proenca, "Periocular biometrics: An emerging technology for unconstrained scenarios", Computational Intelligence in Biometrics and Identity Management (CIBIM), 2013

Authors Profile

Dr. Shubhangi Neware Completed her Masters Degree in Computer Science and Engineering from Chhattisgarh Swami Vivekanand Technical University in year 2009. She has completed her PhD on topic "Finger Knuckle Surface based Biometrics for Personal Identification" in year 2017 from CVRU, Bilaspur. She has 15 years of teaching experience and 2 years of Industry Experience.She is currently working as Assistant Professor in the Department of Computer Science & Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur. She has published more than 20 research papers in reputed international journals and conferences. Her area of interest includes Image Processing , Biometrics, Pattern Recognition and Optimization Techniques in Artificial Intelligence.

