Several Feature Extraction Algorithms in Multi-Model Biometric Recognition System – A Review

Monica Rani[1], Dr.Rakesh Kumar[2],Harinder Kaur[3]
[1]*Research Scholar,* [2]*Principal,* [3]*Assistant Professor*
[123]*Department of Computer Science & Engineering, Sachdeva Engineering College For Girls, Gharuan Mohali (Punjab)*

Abstract- Multi-model biometric system is used for the recognition of the biometric traits in order to overcome the challenges of single biometric system. The two or more biometric labels used for the recognition of the images in biometric system are called as multi biometric system. The main feature of the biometric is the security of the system. The characteristics based on biometric traits used to establish the identity. In this review paper, compare and summarize the multi biometric recognition for the identification of the image. The biological and physiological characteristics such as face, iris, DNA, pattern and signature are identified using biometric system. The applications and types of the multi biometric system are described in this paper. The system improves the privacy, accuracy and the enrollment of the data.

Keywords- Multi biometric system, Biometric traits, Signature.

I. INTRODUCTION

The biological and behavioural characteristics of the individuals recognised automatically are called as biometrics. The biometrics characteristics may be face, iris, DNA, palm print, ear, signature and the patterns [14]. Biometrics basically means life measurement and the term associated by the physiological and biological characteristics for the identification of an individual. The main feature of the biometric is the security of the system. The characteristics based on biometric traits used to establish the identity. The biometric system based on the two phases: -

(i) Enrolment
(ii) Recognition

In enrolment the biometric data is captured using specific sensors and the fresh samples of biometric are recognised in recognition of the scene. A biometric system is the identification system based on the biometric features of the people such as fingerprints, eye retinas and irises, voice designs for the purpose of the authentication and attributes.

Physiological

Behaviour Characteristics

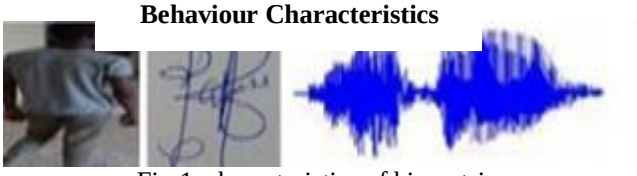


Fig.1: characteristics of biometrics

A. Multi model Biometric System

The process of the identification in combination of two biometric modalities is called as multimodal biometrics. An example of the multimodal biometric can be combination of the face and iris recognition. The multimodal biometrics provides a lot of information to overcome the problems of single biometrics system. The examples of multimodal biometric is secure banking, data secure, transactions to access the data base[12].

The multimodal biometric systems collect a lot of biometric information to make the identification system more accurate. There has been lot of advancements in the biometric system which helps to maintain the reliability and the cost of the identification of the system [13].

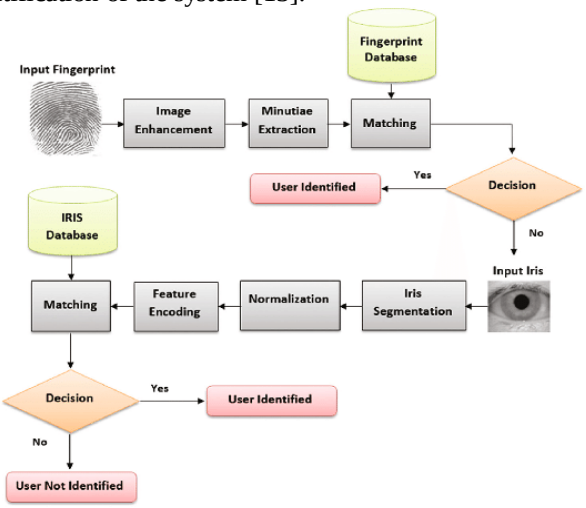


Fig.2: Architecture of multimodal biometric systems

B. Types of Multi Model Biometric System

The multimodal biometric system based on the consideration for designing the architecture of the biometric system[14]. The multimodal biometric system includes the range of the modalities, choice of the biometrics and the level of accumulation the data. The assigned weight of the biometrics based on the reliability and secures system of the biometric

system [2]. The types of the multimodal biometric system are described below:-

i) Fusion Phase: - The multiple source of data are fused which in involves multiple traits obtained by the multiple classifiers. When the resulted data is obtained, the several decision levels obtained from the decision classifiers.

ii) Scenarios of the fusion system: - The scenarios of the multimodal biometric system depends on the number of the sensors and categorised as:-

a)Multiple sensor:- The same biometric trait from different data recorded on the multiple sensors.

b) Multiple classifiers: - The extracted feature sets involve the multiple classifiers and the single sensor.

c) Several units: - The data is discriminated in different categories for improving the performance of the system.

d)Biometric traits:- To determine the identity of the individual, it involve the biometric traits and ensuring the significant improvement in the performance of the traits.

Straightforward biometric framework incorporates four vital segments:-

(i) Sensor module procures the biometric information of an individual. A precedent is a face sensor that catches face pictures of a client.

(ii) Highlight extraction module obtains information in order to separate element esteems. For instance, the position and introduction of the surface in an iris picture would be separated in the component extraction module of an iris framework. Coordinating module thinks about the component esteems against the format vector by producing a coordinating score. For instance, in this module, the separation of two coordinating component vectors will be figured and treated as a coordinating score.

(iii) Basic leadership module guarantees the client's personality: acknowledged or dismissed dependent on the coordinating score produced in the coordinating module.

C. Advantages of multimodal biometric system

The multimodal biometric system improves the performance of the combinational of single biometric system. The system improves the privacy, accuracy and the enrolment of the data.

The applications of multi biometrics are given as [3]:-

i) Accurate recognition: - The two individuals have similar signatures and the signature verification produce large FAR system so to make more accurate and reliable data the multimodal biometric system is used.

ii) Information Private:- The obstruction offered to type of vulnerabilities prevents the type of biometric systems in the database.

iii) Data Enrolment:-The poor quality of biometric data can be captured using multimodal biometric systems.

II. TYPES OF BIOMETRIC TRAITS

Several types of biometric traits are described in below:

(i) Fingerprint:- The Fingerprint verification is used for the operating the system within the controlled structure. The applications areas based on the small size and the ease of the integration [11]. Fingerprint biometrics used in the form of the data encryption for the identification of an individual. The scanning of the fingerprints is done electronically to recognise the information. After the recognition of fingerprint the accuracy can be maintained manually [4].

Fig.3: Fingerprint Recognition

(ii) Face:- The face recognition is done either from the long or the short distance. The recognition is less reliable than iris and fingerprint recognition. In this type of recognition the facial structure matches the face on the computer screen [16]. The image examined on the overall face recognition for the shorter distance gives correct recognition but less accuracy in larger distance. This type of the recognition is done in criminal activities and person is not concerned about the recognition or being monitored.

(iii) Iris Recognition:- The iris scanning is simply done by digital cameras near-infrared light for high contrast picture of iris. When the pupil of the person is black, the computer screen will isolate the pupil and iris. The camera automatically focuses when a person looks in to the scanner. The eye must be 3 to 10 inches from the camera. Iris scanners give better security because the every person have unique eye. The iris is visible but protected structure, and it does not usually change over time, making it ideal for biometric identification.

Fig.4: Iris Scanner

III. RELATED WORK

Thanki, R., and Borisagar et al ., 2015[6] proposed a research on the quality measure to determine the peak signal to noise ratio and index measure to reconstruct the image. The problems in the multi biometric associated with the designing of the multi biometric system. In this paper, compressive sensing theory and Discrete Wavelet Transform used for the generation of the multi biometric patterns using fusion technique. The fused face images are recognized using sparse measurements. The images are reconstructed using CS recovery processes. The face print images are verified using multi biometric system. ***Makul, O., and Ekinci, M et al***

2015[7] presented a multi biometric approach for the recognition of the long vector image using palm finger joint and palm print. The image normalization and Discrete Wavelet Transform was used to recognise the palm fingerprint images. The biometrics joined by a long vector machine approach. In this paper the 1614 palm fingers was tested belongs to 132 persons. The performance of palm finger based on multi biometric structure based on long vector. ***Maiorana, E., Hine, G. E. et al.,2015[8]*** studied on hill climbing attacks using multi biometric system. The attacker generates synthetic biometric data which could allow a false acceptance, this increase the possibility of the attackers.

In this paper several fusion schemes and system architectures studied on the basis of multi biometric system against the Hill climbing attacks. The possible countermeasure evaluated for the success rate and the performance of the recognition of the Hill climbing. ***Pedro Tome, Julian Fierrez et al., 2010[9]*** discussed the benefits of the biometric systems based on the physical features to improve the recognition scenarios. The distance between the objects and cameras was recognised by the soft biometric system. The sparse representation with real and the ideal scenarios was analysed by the soft biometric traits to improve the recognition of the face. This study helps to determine the soft labels for face recognition at large distance using biometric traits. ***Jain, A. K., Ross, A., et al.,2004[10]*** proposed a research on the biometric methodologies selecting a particular biometric technology. In this biometric system, which identifies the person by measuring the characteristics and the characteristics are measured which belongs to many people. The biometric and fingerprints consists of the scanning device, which converts the scanned information in to digital form and the data base store the information of the biometric data.

IV. MULTIMODAL BIOMETRIC USING SEVERAL FEATURE EXTRACTION APPROACHES

In this section, described the various feature extraction methods in multi-model biometric system. The multimodal biometric system is similar to uni-modal biometric system. So the multimodal biometric system can be classified in to state of fusion technique. The multimodal biometric system determined by the biometric data. Detailed explanation is given below:-

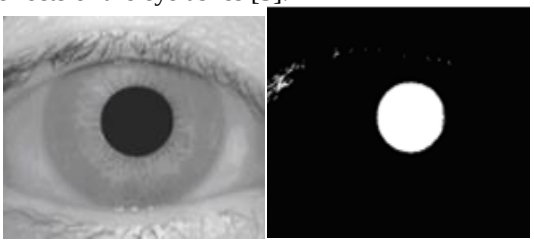
(i) Decision Making:- In feature extraction technique the data are extracted by the featurevalues. In the form of the example the location of the texture of the iris image would be extracted in the feature extraction module of the system.

(ii) Feature Matching:- The feature values of the modules generate the matching score against the vector. The modules of decision making recognise the identity which is matched to score of modules which may accepted or rejected.

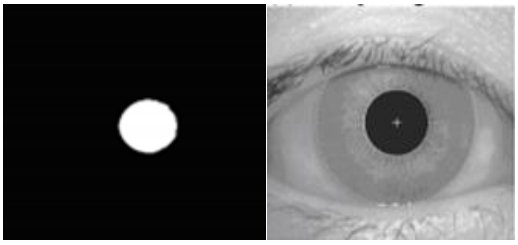
In this feature extraction technique, the feature of the face and iris are extracted and normalised before the fusion process. The feature process are normalised in the form of the series and classified on the basis of the Euclidean distance.

A. Iris Recognition Feature Extraction Method (GABOR)

The Gabor filter is used or the Iris extraction and the feature obtained by the face feature represented by the binary vector. The iris feature obtained by the real vector and the image contains only the iris values. The iris image attains the information from the eye region. The portion of the iris inside the sclera without the eyelids will not be included. The example, highlight extraction, the iris area is a key advance. The iris is an annular part between the student and the sclera. Hence, before iris highlight extraction, it is imperative to find the iris. As such, two outskirts ought to be affirmed, which are the internal limit (the fringe between the understudy and the iris) and the external limit (the fringe between the iris and the sclera). From an iris picture the dimension is expanding from the internal to the external among three segments: the student, the iris and the sclera. The inner and the outer boundary is recognised by the circular contour. The binary image shows the eyelashes are left besides pupil. The open operator adopted using effects of the eyelashes [5].



(a) Real Image (b) Binary Image



(c) Open Operator (d) Result Location

Fig.5: Iris Feature Extarction Image

B. CoifletWavelet

Coiflets are discrete wavelets planned by Daubechies [17], having scaling capacities with disappearing minutes. It has N/3 disappearing minutes and N/3-1 scaling functions and close symmetric. The capacity Ψ has 2N minutes equivalent to 0 and the capacity φ has 2N-1 minutes equivalent to 0. The two capacities have a help of length 6N-1 [18].

C. Local Feature

Rather than the all-encompassing highlights where a whole picture is utilized to process the component portrayal, neighbourhood include extraction techniques remove the data from various dimensions of region and evaluate them absolutely. The general thought of neighbourhood highlight extraction system is to separate the picture into a few sections and afterward the data is extricated each part independently. Another strategy is to find a few segments of highlights, for example, the eye, nose and mouth in a facial picture, and after that arrange them utilizing a few coordinating strategies.

D. Multi-Resolutions Gabor Filter

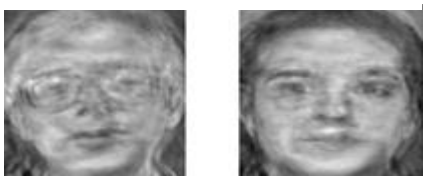
Gabor Filter utilized as a component extraction and picture portrayal technique in the biometric acknowledgment framework. Nearby element extraction utilizing multi resolution investigation includes the convolution of the picture with a lot of Gabor channels registered for a particular district of the picture. The Gabor change or Gabor wavelets, whose parts are like the 2D responsive field profiles of mammalian cortical basic cells, are generally utilized in picture examination because of their organic significance and computational properties[15]. The multi resolution structure in the recurrence space is like that of the wavelets, however without the symmetrical properties. Gabor highlights are considered to traverse an edge that has numerous gainful properties, for example, spatial area and introduction selectivity, and are ideally restricted in the space and recurrence areas. Gabor wavelets can be isolated into a curved Gaussian and a perplexing plane wave.2D DCT Feature Extraction [19].

The previous areas, showed the component extraction technique utilizing multi resolution Gabor highlights, which focus basically on highlight examination utilizing diverse introductions and scales. The primary reason for this segment is to change pictures from the Gabor highlight space to the recurrence area utilizing DCT, where a picture is decayed into a mix of different and related recurrence parts. The benefit of DCT is that it can extricate the highlights in the recurrence area to encode distinctive surface subtleties that are not specifically available in the spatial space [20].

E.Component Analysis (PCA)

The biometric advancements that have the benefits of both high accommodation and low rudeness, face acknowledgment has the wide application fields, for example, data security, law implementation and reconnaissance, savvy cards, get to control. Accordingly, various face acknowledgment calculations and reviews have been exhibited [9-14]. One of the prevalent methodologies for face acknowledgment is eigenface technique.

(a) Original face images



(b) Eigen faces

Fig.6: Component Feature Extraction Data

V. CONCLUSION AND FUTURE SCOPE

Multi-model biometric system concluded that multi biometric system plays a main role in the recognition of the image. In this review an overview of multi biometric system is summarised. The multi biometric system depends on the two phases enrolment and recognition of the image. The applications of multi biometric system described in this paper are the information security, accuracy and enrolment of the data. The different types of the multi-biometric system are explained like as fusion level, feature level and sensor level. Analysed the various feature extraction algorithms to fetch the unique properties in the multi-model biometric images.

Though multi biometric system overcomes the features of the single biometric system, still an improvement is required in the privacy security and performance metrics.

VI. REFERENCES

[1]. Jamdar, C., and Boke, A. (2017). Review paper on person identification system using multi-model biometric based on face. *International Journal of Science, Engineering and Technology Research*, *6*(4), 2278-7798.

[2]. Iwasokun, G. B., Udoh, S. S., and Akinyokun, O. K. (2015). Multi-Modal Biometrics: Applications, Strategies and Operations. *Global Journal of Computer Science and Technology*.

[3]. El-Sayed, A. Y. M. A. N. (2015). Multi-biometric systems: a state of the art survey and research directions. *IJACSA) International Journal of Advanced Computer Science and Applications*, *6*.

[4]. Jain, A. K., Ross, A., and Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, *14*(1), 4-20.

[5]. Wang, Z., Wang, E., Wang, S., and Ding, Q. (2011). Multimodal Biometric System Using Face-Iris Fusion Feature. *JCP*, *6*(5), 931-938.

[6]. Thanki, R., and Borisagar, K. (2015, November). Multibiometric template generation using CS theory and discrete wavelet transform based fusion technique. In *Engineering (NUiCONE), 2015 5th Nirma University International Conference on* (pp. 1-6). IEEE.

[7]. Makul, O., and Ekinci, M. (2015, May). Development and implementation of multibiometric on palm finger joint and palm pattern. In *Signal Processing and Communications Applications Conference (SIU), 2015 23th* (pp. 1619-1622). IEEE.

[8]. Maiorana, E., Hine, G. E., and Campisi, P. (2015). Hill-climbing attacks on multibiometrics recognition systems. *IEEE Transactions on Information Forensics and Security*, *10*(5), 900-915.

[9]. Tome, P., Fierrez, J., Vera-Rodriguez, R., and Nixon, M. S. (2014). Soft biometrics and their application in person recognition at a distance. *IEEE Transactions on Information Forensics and Security*, *9*(3), 464-475.

[10]. Jain, A. K., Ross, A., and Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, *14*(1).

[11]. Jain, A. K., Feng, J., and Nandakumar, K. (2010). Fingerprint matching. *Computer*, *43*(2).

[12]. Panchal, T., and Singh, A. (2013). Multimodal biometric system. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5).

[13]. Thanki, R., and Borisagar, K. (2013). A novel robust digital watermarking technique using compressive sensing for biometric data protection. *Int J Electron Commun Comput Eng*, *4*(4), 1133-1139.

[14]. Ross, A., and Jain, A. K. (2004, September). Multimodal Biometrics: an overview. In *2004 12th European Signal Processing Conference* (pp. 1221-1224). IEEE..

[15]. Unar, J. A., Seng, W. C., and Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern recognition*, *47*(8), 2673-2688.
[16]. Turk, M. A. (1991). *Interactive-time vision--face recognition as a visual behavior* (Doctoral dissertation, Massachusetts Institute of Technology).
[17]. Geetha, K., and Radhakrishnan, V. (2013). Multimodal biometric system: A feature level fusion approach. *International Journal of Computer Applications*, *71*(4).
[18]. Raghavendra, R., Dorizzi, B., Rao, A., and Kumar, G. H. (2011). Designing efficient fusion schemes for multimodal biometric systems using face and palmprint. *Pattern Recognition*, *44*(5), 1076-1088.
[19]. Prabhakar, S., and Jain, A. K. (2002). Decision-level fusion in fingerprint verification. *Pattern Recognition*, *35*(4), 861-874.
[20]. Jain, A., Nandakumar, K., and Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern recognition*, *38*(12), 2270-2285.