International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 30-35
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

A COMPARATIVE STUDY OF VARIOUS BIOMETRIC APPROACHES

Ramandeep Chahal
Department of CSE
GVIET, Banur, Punjab, India

ABSTRACT – Biometric is the science for recognizing an individual on the basis of his or her physical or behavioural traits, it is beginning to increase acceptance as a genuine method for finding an individual identity. Fusion of biometric is the combination of two varied biometrics for enhancing the measures of security. This paper lights up biometric system with the traits. The existing techniques for the biometric recognition are described for the fusion. From the last few years, the remarkable growth in biometric recognition technology is taken place due to the increasing need of highly reliable personal identification with the authentication in a number of government and commercial applications as described .The advantages and disadvantages associated with various modalities of biometric systems are represented in this paper along with a comparison between the different modalities of biometrics on the basis of biometric sample, accusation device, feature to be extracted and matching algorithm.

Keywords: Biometric, Fusion, Feature Extraction, Classification, Biometric Framework

I. INTRODUCTION

An extensive variety of systems require dependable individual recognition schemes to either confirm or decide the identity of an entity requesting their services [1]. The reason of such schemes is to make sure that the render services are access only by a rightful user, and not by anyone else. Example of such applications includes secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the nonexistence of strong personal recognition schemes, these systems are susceptible to the tricks of the frauds. Biometric recognition, or just biometrics, refers to the mechanical recognition of persons based on their physiological and behavioural individuality. By using biometrics, it is probable to confirm or establish an individual's identity based on "who she is", rather than by "what she possesses" (e.g., an Identity Card) or "what she remembers" (e.g., a password) [2]. In this document, we give a concise impression of the field of biometrics and summarize some of its compensation, disadvantage, strengths, limitations, and linked isolation concerns. Computer science describes biometrics as automatic recognition of individuals through their unique attributes i.e. Physiological (fingerprint, face, iris etc.) or Behavioral (voice, signature etc.). Besides, biometric attributes cannot be lost, transferred or stolen, and ensures better security because they are very difficult to forge. Moreover, they require the presence of the genuine user while granting access to the particular resources

Figure 1: Biometric Traits

In order to become a qualified biometric trait, every physiological or behavioural trait must satisfy the following criteria [3]:

- Universality – every person must own this characteristic.
- Distinctiveness – two persons possessing the same characteristic do not exist.
- Permanence – the characteristic must be invariant for a time period as long as possible.
- Collectability – indicates the fact that biometric may be quantitatively measured;
- Performance – which refers to the accuracy of the tangible recognition,

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 30-35
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

- speed, robustness, as well as the prerequisites for touching a certain level of performance;
- Acceptability – indicates the degree in which the given biometric characteristic is accepted by the users;

II. BIOMETRIC FRAMEWORK

A normal biometric framework comprises of four principle segments, specifically, sensor, extractor,

matcher and choice modules [3]. A sensor is utilized to secure the biometric information from a person. A quality estimation calculation is once in a while used to learn whether the obtained biometric information is adequate to be prepared by the resulting parts. At the point when the information is not of adequately top notch, it is generally re-procured from the client.

The element extractor gathers just the remarkable data from the procured biometric example to frame another representation of the biometric characteristic, called the list of capabilities. In a perfect world, the list of capabilities ought to be one of a kind for every individual (amazingly little between client similitude) furthermore invariant regarding changes in the distinctive examples of the same biometric quality gathered from the same individual (greatly little intra-client variability). In the middle of confirmation, the list of capabilities removed from the biometric specimen (known as inquiry or info or test) is contrasted with the layout by the matcher, which decides the level of likeness (divergence) between the two capabilities. The choice module settles on the character of the client in light of the level of similitude between the format and the inquiry [4].

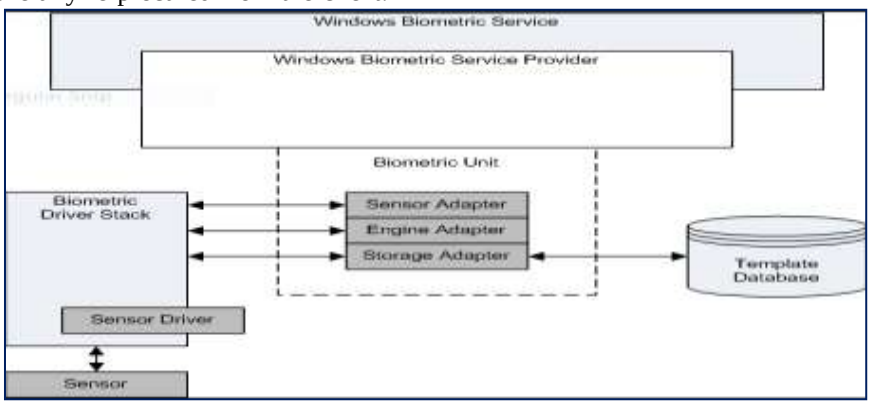

Figure 2: Biometric Framework

2.1 FUNCTIONALITY OF BIOMETRIC SYSTEM

Depending on the application context, a biometric system may operate either in verification mode or identification mode [5].

VERIFICATION: It refers to 1:1 matching. Verification is also known as authentication, the user claims an identity and system verifies whether the claim is genuine or not [6].

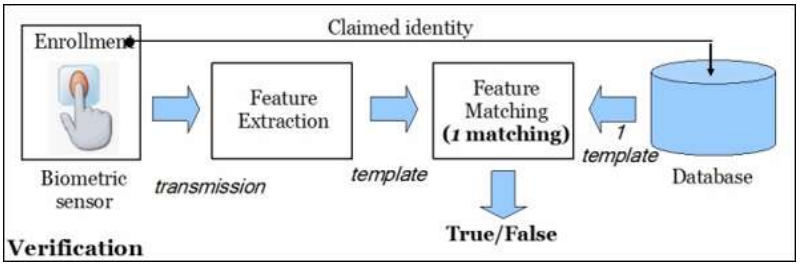

Figure 3: Verification process for Biometric Recognition

IDENTIFICATION: It refers to 1: m matching. In this situation user does not know its identity, it is simply presenting its bio-metrics for matching with whole database. User's template is matched with all the templates stored in database to identify with which template it has highest similarity [7].

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 30-35
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

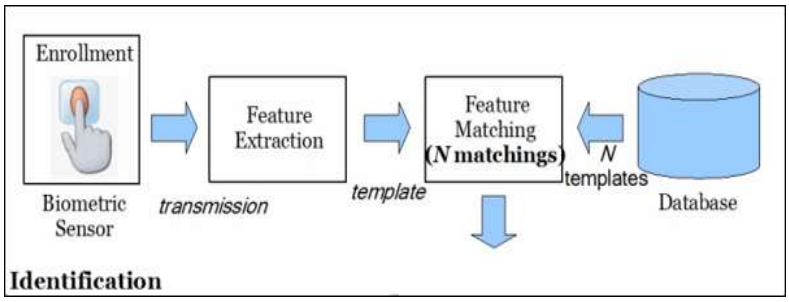

Figure 4: Identification process for Biometric Recognition

III. VARIOUS BIOMETRICS TYPES

This section describes the comparison of the various modalities on biometric basis. The modalities taken are Face, Fingerprint, Iris and Voice recognition. The comparison has been made with the features like biometric sample, accusation device, features extracted and matching algorithms [8].

Table 1: Comparison of different modalities

BIOMETRIC MODALITIES	PROS	CONS
FACIAL	It does not require any co-operation of the test subject to do any work. Systems set up in open public areas can easily identify an individual among the massive crowd. It performs massive identification which usually other biometric system can't perform.	Facial recognition is not much effective for low resolution images. Face recognition isn't perfect and faces challenges for instance associated with the varying position of face. It doesn't work effectively in bad lighting, sunglasses, lengthy hair, or other objects that partly covers the subject's face.
IRIS	An iris scan can be carried out through 10 cm to a few meters apart. High accuracy and High recognition process speed. Data capturing can be carried out even though a user is putting contact lenses or glasses.	The scanning devices are often hard to adjust and may annoy multiple people of various heights. The accuracy of scanning devices may impacted by unusual lighting effects and illumination from reflective types of surfaces. Iris scanners tend to be more expensive in comparison with additional biometrics.
FINGERPRINT	It is easy to use along with the high verification process speed and accuracy. A fingerprint pattern has individually distinctive composition and characteristic remains the same with time. One should not have to remember long passwords, you simply swipe your finger on scanner and done it.	Fingerprint scanning system could be cheated by employing artificial fingers or perhaps showing another person's finger. Sometimes it may take many swipe of fingerprint to register. Cuts, marks transform fingerprints which often has negatively effect on performance.

VOICE/SPEECH	Speech can be recommended as a natural input as it does not demand any training and it is considerably quicker as compared to some other input. This technique helps those people who have difficulty of using their hands. One of the major advantages of voice recognition technique is to cut back misspelled texts of which many typists may perhaps suffers a problem during typing.	Voice recognition systems very often may make mistakes, when there is disturbance or some noise in the surrounding. Voice Recognition systems may be hacked with some pre-recorded voice messages. Several words sound very similarly. Case: two, to, too. This may sometimes confuse the system.

Table 2: Pros and Cons of Biometric Modalities

MODALITIES	BIOMETRIC SAMPLE	ACCUSATION DEVICE	FEATURE EXTRACTED	POPULAR MATCHING ALGORITHM
Facial Scan	Face Image	Video Camera, PC Camera	Distance of specific facial features (eyes, nose, mouth)	Euclidian distance
Iris Scan	Iris Image	IR enabled Video Camera	Texture of the iris (freckles, coronas, strips, furrow, and crypts)	Hamming distance
Fingerprint	Fingerprint Image	Sensor	A friction Ridge curves-a raised portion, pore structure, indents and marks	String matching
Voice Recognition	Voice Recording	Microphone, Telephone	Words, tone	Hidden Markova Model

IV. FUSION IN BIOMETRICS

As the feature set holds extended knowledge regarding the input biometric data than the matching score or the output decision of a matcher, therefore, fusion at the feature level is supposed to provide sufficient recognition results [9]. However, fusion at this level is complex to achieve in practice because the feature sets of the several modalities may not be suitable, and most of the popular biometric systems do not grant access to the feature sets which they employ. There are three possible levels of fusion that are briefly described below [10]:

Fusion at the feature extraction level

In feature extraction level of fusion, the signals are initially processed and feature vectors are extracted individually from the each biometric attribute. Subsequently, these feature vectors are merged to create a composite feature vector which is further utilized for classification. Since features bear abundant information of biometric attribute than matching score or decision of matcher, therefore the fusion at the feature level is presumed to give excellent results for recognition [11].

Fusion at the matching score level

Match score-level fusion is also called confidence-level fusion. In matching score level, the feature vectors are processed exclusively and the individual matching score is determined and ultimately these matching scores are fused to create classification. Several statistical learning techniques may be employed to merge match scores [12].

Fusion at the decision level

In decision level fusion, each modality is initially pre-classified individually i.e. each biometric attribute is apprehended, and later the features are

extracted from that particular attribute. The final classification is based upon the fusion of the outputs of different modalities. This is the highest level of fusion with respect to human interface. In other words, the decision from each biometric system is gathered to deliver the final decision.

V. RELATED WORK

Kamal Hajari et al, provided a brief review of challenges, databases, and algorithms for iris recognition. The noisy imaging conditions, as well as constrained conditions, influences the performance of iris recognition system. Most of the researchers concentrated on the steps of iris recognition system by taking up some concerns and their noise identification and extraction algorithms. From this study, it has been observed that most of the researchers are not able to find flawless and reliable resolution to all the challenges considered in this paper. Most of the methods and algorithms were examined on the databases gathered by various organizations and certain attempts were also made to estimate the accuracy of the systems designed. From the performance evaluation, it has been observed that there is still a scope for enhancements in the existing approaches dealing with the noisy environment.

Navjot Kaur et al, reviewed the steps associated in iris recognition system and several techniques used by different researchers for every recognition step. The need for iris recognition is expanding day by day because of the authenticity, efficiency, and uniqueness. It is the most effectual identification feature among all other biometric features as human iris remains constant throughout the whole of the life. The author eventually concluded that for the effective functioning of iris recognition system, researchers still have to work on numerous challenges like images taken in an unconstrained environment, noisy images, blurred images and several more.

Gursimarpreet Kaur et al, illustrated several biometric modalities and also these are analyzed on the basis of various aspects. Feature sets of these modalities are also represented Biometric is automated process of identifying an individual based on its biometric characteristics. It is quite reliable as compared to traditional methods of authentications. Biometric is primarily developed based on methods of pattern recognition. Nowadays, biometric is representing a vital component in various application areas such as military, forensic, controls, access etc. Iris seems to be most valid biometric but actual usage depends on the type of application. Although there are some difficulties with biometric systems but it is also becoming an emerging technology in the field of security.

Rupinder Saini et al,performed a comparison among the various biometric systems on the basis of their benefits and drawbacks. The author has provided an introduction to numerous biometric techniques undertaking the comparison examination concerning extensively used biometric identifiers and also the identification strategies. There are numerous apps along with alternative solutions employed in security techniques. Despite the fact the biometrics security systems have several issues like data privacy, physical privacy, and spiritual arguments etc., they still give benefits that may enhance our lives in such a way by raising security and efficiency.

VI. CONCLUSION

Biometric is defined as automatic recognition of individuals through their unique attributes i.e. Physiological or Behavioral. It offers several advantages over traditional approaches in such a way that there is no need to remember anything. Besides, biometric attributes cannot be lost, transferred or stolen, and ensures better security because they are very difficult to forge. In order to become a qualified biometric trait, every physiological or behavioral trait must satisfy certain specific criteria's. The functionality of the biometric system is defined in the terms of verification and identification. This paper will cover the various advantages and disadvantages associated with the biometric modalities. Nowadays fusion of biometric has gained a lot of attention in research industry, and in this paper the basic review of fusion in biometrics is presented along with the various levels of the fusion.

VII. REFERENCES

1. Samarth Bharadwaj, MayankVatsa and Richa Singh, "Biometric quality: a review of fingerprint, iris, and face", EURASIP Journal on Image and Video Processing, pp. 34-62, 2014.
2. Mehdi Ghayoumi, "A review of multimodal biometric systems: Fusion methods and their applications", In IEEE/ACIS 14th International Conference on Computer and

Information Science (ICIS), pp. 131-136, 2015.

3. Muhtahir o. Oloyede and Gerhard p. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review", In IEEE Access, Vol. 4, pp. 7532-7555, 2016.

4. Hajari, K. and Bhoyar, K., "A review of issues and challenges in designing Iris recognition Systems for noisy imaging environment", In International Conference on Pervasive Computing (ICPC), 2015 (pp. 1-6). IEEE.

5. Kaur, Navjot, and MamtaJuneja. "A review on iris recognition." In *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in*, pp. 1-5. IEEE, 2014.

6. Mali, Kalyani, and Samayita Bhattacharya. "Comparative study of different biometric features." *International Journal of Advanced Research in Computer and Communication Engineering, Vol*. 2, no. 7, pp: 2776-2784, 2013.

7. Kaur, Gursimarpreet, and C. K. Verma. "Comparative analysis of biometric modalities." *International Journal of Advanced Research in Computer Science and Software Engineering* 4, no. 4 (2014): 603-613.

8. Saini, Rupinder, and NarinderRana. "Comparison of various biometric methods." *International Journal of Advances in Science and Technology (IJAST)* 2, no. 1 (2014): 2.

9. Dolly Choudhary, Shamik Tiwari and Ajay Kumar Singh, "A Survey: Feature Extraction Methods for Iris Recognition", International Journal of Electronics Communication and Computer Technology (IJECCT), Vol. 2, No. 6, 2012, pp. 275-279.

10. Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," IEEE Trans. Pattern Anal. Mach. Intell., vol. 36, no. 6, pp. 1120–1133, 2014

11. J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, 2014

12. Sudipta Roy, Abhijit Biswas, "A Personal Biometric IdentificationTechnique based on Iris Recognition,"

13. (IJCSIT) International Journalof Computer Science and Information Technologies, Vol. 2 (4) ,2011, 1474-1477

14. Elgamal, Mahmoud, and Nasser Al-Biqami. "An efficient feature extraction method for iris recognition based on wavelet transformation." Int. J. Comput. Inf. Technol 2, no. 03 (2013): 521-527.

15. X Li, Z Sun, T Tan, "Predict and improve iris recognition performance based on pairwise image quality assessment", in Proceedings of the International Conference of Biometrics, June 2013, pp. 1–8.