EasyChair Preprint

№ 6372

A Review Paper for Security by Using Biometric Fusion

Kumud Sachdeva

August 26, 2021

A Review Paper for Security by using Biometric Fusion

Kumud Sachdeva

kumud.cse@cumail.in

Chandigarh University (Gharuan)

Abstract- Biometric Fusion refers to combining two different biometric approaches to enhance the security for many fields. A lot of biometric patterns are already being used in the daily life. For example, it is often seen that a smart phone comes with the finger print scanner which uses a finger as security pattern to unlock the phone. Nowadays biometric fusion is used to find out the security in research industry. In this paper reviews the existing techniques of Biometric Fusion. This paper also lights up classification techniques which includes Artificial Intelligence. In this paper, discussed with a comparative study of different methods of biometrics on the basis of biometric sample, accusation device, feature to be fetched and matching algorithm.

Index Terms-Biometric, Fusion, Feature Extraction, Classification

I. INTRODUCTION

Traditionally, the identification systems were relied on methods of cryptography needing users to keep in mind a secret text (password) or keep something with them (token, card) or a combination of both to prove their identity. Textual passwords and tokens were required in order to be able to usethe desired resources, for example; entrance control, computer logins, making bank transactions, welfare pay-outs etc. However, remembering secret passwords was a very difficult task for the user, and also the token/card for identity recognition could be stolen or misplaced. As a solution to above problem, the research community suggested the idea of human identification system based on physiological or behavioral attributes of people and termed it as "Biometrics".

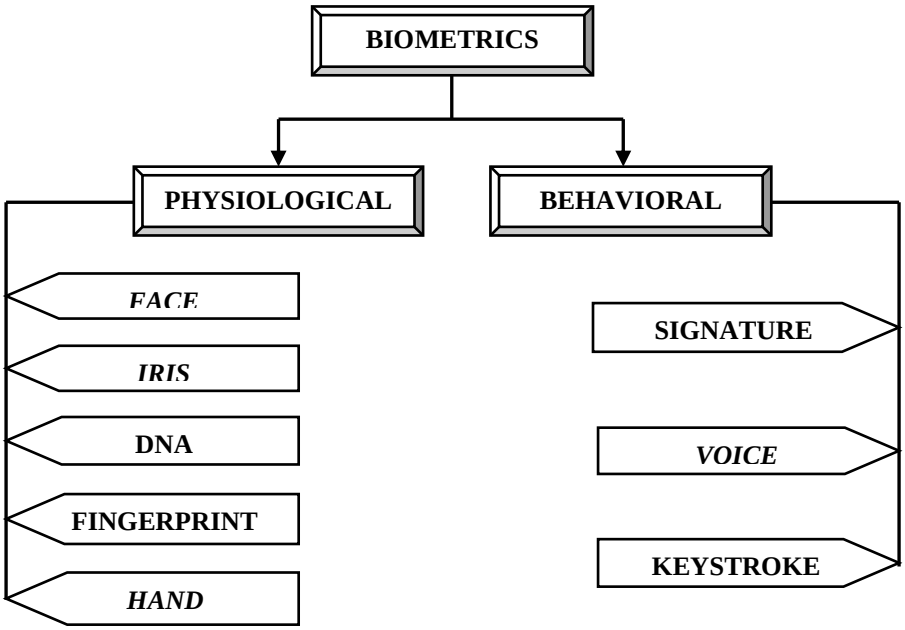

Figure 1: Classification of the biometric features

Computer Science explains biometrics as automated system of recognition of people withtheir specific identity such that Fingerprint, face, iris or Behavioral (signature or voice). It gives many features over knowledge based tricks in a method that it is not necessary to keep things in mind. Also, biometric features can be stolen or transferred and gives better security asit is very difficult to duplicate. Adding to it, they need the physical presence of the actual user and giving access to the actual inventory.

TABLE I

COMPARISON OF DIFFERENT METHODS BASED ON BIOMETRIC TECHNIQUES, ACQUISITION DEVICE WITH THE PARAMETERS AND MATCHING ALGORITHMS

Methods	**BIOMETRIC Techniques**	**Acquisition Device**	**Parameters**	**MATCHING ALGORITHMS**
Face Recognition	Face Image	Pre-processing, Acquisition	Facial feature (Eye, mouth, Nose)	Euclidian distance
Iris Recognition	Iris Image	IR enabled Video Camera	Eye feature (Pupil, retina)	Hamming distance
Finger Recognition	Finger Image	Pre-processing, Acquisition	Pore structure, indents and marks	String matching
Voice Recognition	Voice Recording	Microphone, Telephone	Words, tone	Hidden Markova Model

For becoming an applicable biometric characteristic, physical and behavioural features must meet the below criteria:

- Universal: all humans own it.
- Distinctiveness: identical and unique among the people.
- Invariance: feature must not vary with time.
- Aggregation: Should be collectable in terms of procuring, digitalisation and toretrieve features from the community.

i) *Performance:* sticks to the presence of materials and inclusion of actual limitations with regard to collection of data and assurance to deliver correct results.

ii) *Circumvention:* vulnerable to copying or imitation orillicit use of *identification system.*

II. BIOMETRIC SYSTEM

It refers to the system of automated verification of a person by using some physiological characteristicsof the person. A huge number of applications need trusted identification to confirm the verified identity of a person asking for the service. Such applications include protected allowance to towers, computer systems, and digital devices such as cellular phones, laptopsand ATMs. This system uses fingerprints, iris, retina, facial expressions in order to verify a person's uniqueness. They have their side over conventional methods of security also theycannot be easily used in an illicit manner or copied. A normal system is having a sensor, a feature fetchingand a matching compartment.

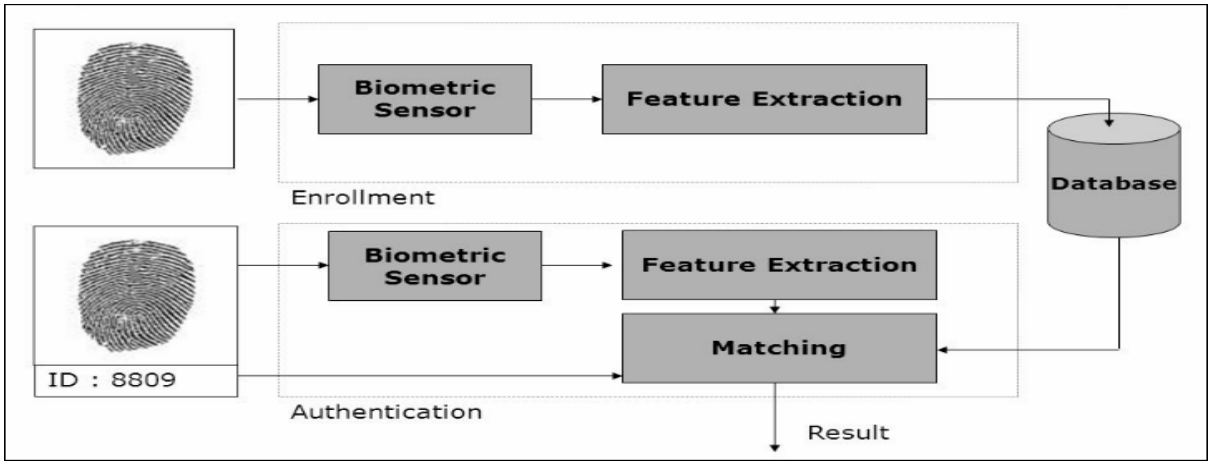

Figure 2: Normal Biometric System

These systems are based on the source of information and are known as unimodal systems. The working of this unimodal method is affected by the consistency of the sensor being used and the degrees of freedom rendered by the characteristics extracted from the signal being sensed. Adding to it, if the unimodal biometric characteristic being measured is noisy and the resultant matching number calculated by the matching technique won't be reliable. These problems can be stimulated by adding multiple sensors that can capture biometric traits and provide the reliability because of the availability of many records of evidence. For instance, the feature extraction compartment of the fingerprint system is unable to fetch the features from fingerprints of an individual, due to the poor quality of the modal. In such cases, it is useful to have more than one biometric trait for verification of the uniqueness. Multimodal systems provide measures that make it difficult for an outsider to spoof. Studies have shown that these systems can perform better compared with unimodal systems.

.

Biometric technique can be examined by calculating its false accept rate (FAR) and false reject rate (FRR) at several parameters. The FRR andFAR are calculated by generating all possible matching numbers and then setting a parameter for determining whether to accept or reject a number. A matching number is obtained when the comparison is done with the two feature vectors and matching number is obtained when comparison is done with different person of feature vectors.

2.1) CHARACTERSTIC OF BIOMETRIC SYSTEM

The functions of the biometric Technique are defined with regard to verification and identification.

Verification: Verification is defined with the process of authentication. In this method, the user provides an identity and then according to this it processed.

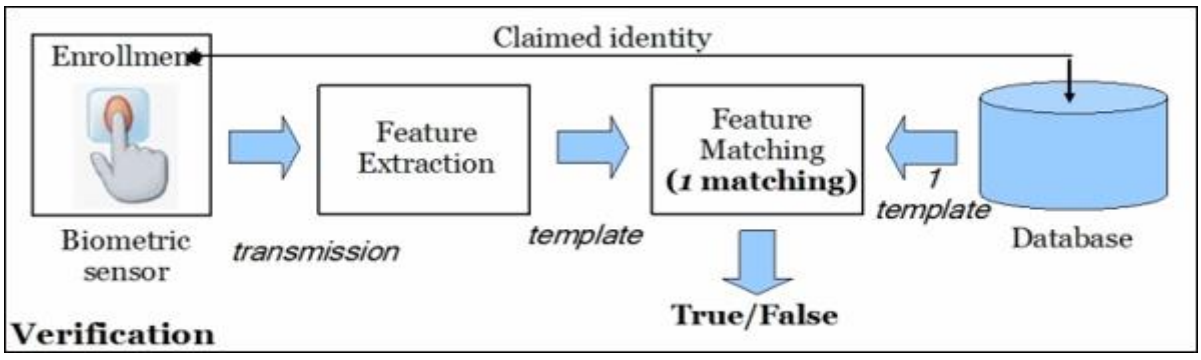

*Figure **3: Verification process for Biometric Recognition***

IDENTIFICATION: In this process, firstly create a database to identify the user because of user doesn't know his identity so it is presents its bio-metrics after matching the whole database. User's template database is compared to all the templates stored in database to identify with which template it matches.

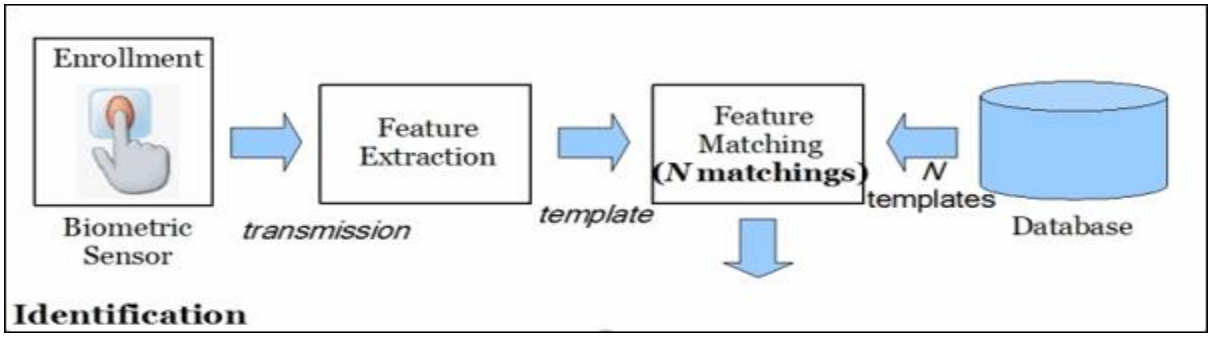

*Figure3**: verification process for Biometric Recognition***

III. FUNCTIONING OF A BIOMETRIC SYSTEM

The functioning of this system is quite easy and works in two forms which are training and classification. Manyday to day activities are usually seen, for example, the functioning of afingerprint sensor on any cellular mobile. It saves the pattern of the fingerprint and then verifies the finger every time the finger is kept onto the sensor. Below is the graphical representation of the functioning of this system

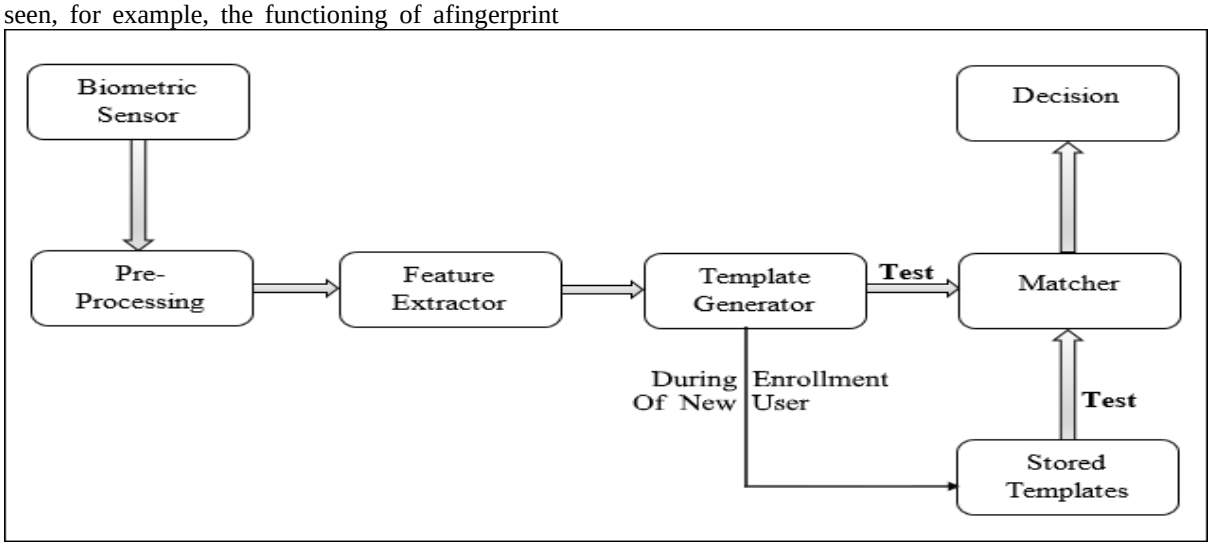

Figure **4: Functioning of a Biometric System**

The early stage here is said to be enrolment. Here, the information is stored within the system. Afterwards, while implementing, the data within the system is verified with the previously collected data in the enrolment. We have to see that the input and the storage of the dataare executed in a secure way. The first block that is the sensorworks as an user interface and the real world acquires the necessary data. Mostly, it is a representation but can change as per the desired features of the system. The second block performs the required pre-processing and debars the processed information from the sensor, and modifies the input. In the next Block which isFeature Extractor, the important and required characteristics are retrieved. This is an important phase as one needs to fetch the correct features in a best possible way. In the following block i.e. Template generator, the image of the numbers with particular characteristicsis used for creating templates. This template is a combination of all the related features fetched from the source. Artefacts of biometric measurements are isolated in templates to reduce the size and preserving the uniqueness of a user. Now, the template is stored on to the database and matching is implemented and then the procured template is carried on to the human that is matching it with the one in use, judging the gap between these two using the algorithm. This matching program accesses the template and then becomes the output for resultant data.

IV. FUSION IN BIOMETRICS

Till the extent to which the feature provides, information regarding the raw data and the output decision, the minimal level is to be provided for result. Also, fusion at this level is hard to identify

the parameter sets of various techniques be applicable and many techniques have to be failed to access the feature sets which are employed under them. The possible levels of fusion are explained below:

4.1) Fusion at the feature Extraction level

Here, signals are processed and feature vectors are fetched from the images of biometric properties. Now, these properties are combined to propose a feature vector. Since some features bear ample data of biometrics than decision of matching device, afterwards the fusion at property level is supposed to produce effective results for identification.

4.2) Fusion at the Matching number level

In matching number property vectors are worked upon and every matching number is known and the matching numbers are combined to createclassification. Many learning methods can be managed to combine match numbers.

4.3) Fusion at the decision level

In this level fusion, technique is defined by pre-processing specifically i.e. everyproperty is extracted by particular method. The final result can be classified by particular technique which is suitable to this fusion extraction. For the classification data, every biometric images is extracted to reach the final output.

V. PROS AND CONS OF BIOMETRIC TECHNIQUES

There are various biometric techniques that are being used by many security systems. All these techniques have some positive and negative points connected to them.

TABLE 2**:**Advantages and disadvantages of Biometric Modalities

BIOMETRIC MODALITIES	PROS	CONS
FACIAL	1. Don't require test for any work. 2. It can easily identify when we have found massive crowd. 3. It can be easily identified by using facial feature.	1. This method is not useful when low resolution image has found. 2. It is not effective with varying position of face. 3. This method is not working properly when bad lightening has found. .
IRIS	1. This method is going to be used to be carried out through 10 cm to a few meters. 2. By this method, we have found high accuracy and high recognition speed. 3. Data extracting can be done by contact lenses and glasses.	1. In this method scanning device is very hard to adjust. 2. Accuracy of scanning devices may impact on lightning effect and illumination. 3. In this method, iris scanner is more costly as compared to other biometric nethod.

FINGERPRINT	1. This method is very easy with high verification speed. 2. In this pattern we have to follow some pattern to provide a security also. 3. By using this method we don't remember password to capturing everything. Just we need to take swipe by fingerprint.	1. This is not suitable when someone is cheated by employing artificial finger. 2. By using this, it may take some time to register fingerprint. 3. Negative effect on when we have found mark, cuts on finger.
VOICE/SPEECH	1. By this method we not demand any training method to achieve output. 2. This method is used for that people who are handicapped. 3. This technique is more efficient and advisable for typist and same kind of profession where misspelled text must be recognized.	1. When there was a disturbance in noise due to noisy signal, we couldn't be able to identify properly.. 2. By this method hacked information by artificial voice. 3. Some text sound in very similar way such as: two, to, too. This type of text confused the system during processing.

VI. RELATED WORK

Kamal Hajari et al, proposed a method or algorithm for iris recognition. In this method, performance was measured by suitable method in noisy condition. It has been observed that technique that was used for this requirement that was not fulfilled all the criteria. Experimental result was tested on image database collected by some industries to check the performance. For the future work, it will be enhanced to create a method that will work on loud enviournment.

Navjot Kaur et al, proposed a method to describe iris recognition system and to explain how to classify the data by using particular technique. On demand iris recognition is used in research area for authenticity. In this paper has to be defined working of iris recognition system but techniques still have to work on many area such as images taken in an low contrast environment, noisy images and blurred images.

Gursimarpreet Kaur et al, described many biometric functions that was described by using particular parameter. Firstly, Extract the feature for biometric function to execute the method. Biometric system is a process for identifying an individual based on its parameters.Biometric is the application of pattern recognition. On demand biometric system is widely used in various areas such as military, forensic, controls, access etc. Iris Recognition is widely used for valid biometric but actual usage depends on the type of application.

Rupinder Saini et al, defined a comparison between various techniques of biometric systems. In this paper has to be defined the brief introduction of various technology which has to be used in earlier paper and define the comparison by testing the performance on various type of database and then classified by various parameters. It has also defined the recognition techniques. Despite the fact the biometrics security systems have several issues like data privacy, physical privacy, and spiritual arguments etc., they still have benefits that may advance our lives in a spectacular way by increasing security.

VII. CONCLUSION

Biometric system is a technique to identify individuals by using their unique property such as Physical or Behavioural. In the present scenario, biometric fusion is becoming popular in various applications. Biometric attributes would not be stolen or transferred and gives good security as they are very complex to forge. For accurate results each properties has to be extracted from a particular method to achieve a final results. The working of the biometric technique to show the result as verification and recognition. In this paper, by using the fusion technique covers all the limitation which described in earlier papers.

REFERENCES

[1] Mehdi Ghayoumi, "A review of multimodal biometric systems: Fusion methods and their applications", pp. 131-136, 2015.

[2] Hajari, K. and Bhoyar, K., "A review of issues and challenges in designing Iris recognition Systems for noisy imaging environment", (pp. 1-6). IEEE.

[3] Kaur, Navjot, and MamtaJuneja, "A review on iris recognition," In Engineering and Computational Sciences (RAECS), 2014 ,pp. 1-5. IEEE, 2014.

[4] Mali, Kalyani, and Samayita Bhattacharya, "Comparative study of different biometric features," Vol. 2, no. 7, pp: 2776-2784, 2013.

[5] 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.

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

[7] 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.

[8] 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

[9] Sudipta Roy, Abhijit Biswas, "A Personal Biometric IdentificationTechnique based on Iris Recognition,"

[10] International Journalof Computer Science and Information Technologies, Vol. 2 (4) , 1474-1477

[11] 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.

[12] 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.

[13] B. Duhan and N. Dhankhar, "Hybrid Approach of SVM and Feature Selection Based Optimization Algorithm for Big Data Security," Lect. Notes Electr. Eng., vol. 605, pp. 694–706, 2020.

[14] Hooda, N., Bawa, S., & Rana, P. S. (2018). B2FSE framework for high dimensional imbalanced data: A case study for drug toxicity prediction. *Neurocomputing*, *276*, 31-41.

[15] Hooda, N., Bawa, S., & Rana, P. S. (2018). Fraudulent firm classification: a case study of an external audit. *Applied Artificial Intelligence*, *32*(1), 48-64.

[16] Hooda, N., Bawa, S., & Rana, P. S. (2020). Optimizing Fraudulent Firm Prediction Using Ensemble Machine Learning: A Case Study of an External Audit. *Applied Artificial Intelligence*, *34*(1), 20-30.

[17] Bhardwaj, R., &Hooda, N. (2019). Prediction of Pathological Complete Response after Neoadjuvant Chemotherapy for breast cancer using ensemble machine learning. *Informatics in Medicine Unlocked*, *16*, 100219.

[18] Gupta, R., Rao, U.P.: Achieving location privacy through CAST in location based services. Journal of Communication Network 19(3), 227–238 (2017)

[19] Gupta, R., Rao, U.P.: VIC-PRO: Vicinity protection by concealing location coordinates using geometrical transformations in location based services. Wireless Personal Communication 107(2), 1041–1059 (2019)

[20] Gupta, R., Rao, U.P.: A hybrid location privacy solution for mobile lbs. Mobile Information System, 2017 (2017)

[21] Gupta, R., Rao, U.P.: An exploration to location based service and its privacy preserving techniques: A survey. Wireless Personal Communication 96(2), 1973–2007 (2017)

[22] Gupta, R. and Rao, U.P.: Preserving location privacy using three layer RDV masking in geocoded published discrete point data. *World Wide Web*, *23*(1), pp.175-206 (2020)

[23] S. Singh, M. Singh, C. Prakash, M. K. Gupta, M. Mia, and R. Singh, "Optimization and reliability analysis to improve surface quality and mechanical characteristics of heat-treated fused filament fabricated parts," Int. J. Adv. Manuf. Technol., vol. 102, no. 5–8, pp. 1521–1536, 2019.