Multimodal Biometric Identification System - An Overview

N.Gopal [#1], Dr.R.K. Selvakumar [*2]

[#1]*Research Scholar,*
Research & Development Center, Bharathiar University, Coimbatore, Tamilnadu, India.
[*2]*Professor and Head,*
Department of Computer Science and Engineering,
Agni College of Technology, OMR, Thalambur, Chennai. Tamilnadu, India.

Abstract - *In the development of recent technologies, a biometrics system has been the important affordable and more reliable system. A Biometrics identification system is refers to the automatic recognition of individual person based on their characteristics. Basically biometrics system has two broad areas namely unimodal biometric system and multimodal biometric system. In unimodal system it has some disadvantage due to its lack of non-universality and unacceptable error rate. To overcome those unimodal challenging issues, multimodal is the better system for its two or three level of identification and verification. In this paper multimodal biometrics system characteristics are studied with various biometrics traits. The comparison of different modalities is also processed in this paper to choose the best authentication mechanism. This paper performs a well studied system based on multi biometrics system with its processing*

Keywords — *Biometrics, Unimodal system, Multimodal biometrics, Biometrics traits.*

I. INTRODUCTION

With the growth of technology improvements biometric identification system is one of the important authentication techniques to provide a validation operation. This validation method gives a well protection from any misleading activities to the user (1). In past decade's knowledge based security like password and token based security like ID cards have been accessed to restrict the misbehaviours on the secured system. This kind of security considerations can be easily breached when the passwords are revealing to an authorized user or the ID card is stolen by an impostor. So a fine planned authentication is needed to overcome those issues. Biometrics authentication mechanism is a powerful tool for access control, security and real world applications (2). It was developed for several years and the recent advancements in technology have been made of affordable and more reliable. In biometric modalities it can be divided into three main categories such as, Psychological, Behavioral and Chemical (11). It basically refers to the automatic recognition of individuals based on their characteristics.

The category of psychological biometric modality (8) is based on the nature of the body it includes finger print, retina, palm print, hand geometry, DNA, facial thermo grams. A finger print is the psychological nature that has been used more than 100 years. In behavioral biometrics are associated to the behavior of a person includes hand written signature, keystroke dynamics, voice, lips dynamics, voice and handgrip dynamics. This can be used the form of identification and verification. Chemical biometrics is still an emerging field and involves evaluating chemical cases such as body odor and the chemical composition of human sweat which was posses the determination of automated recognition of individuals (9).

The rest of the paper is organized as follows; section 1 follows the introduction about biometrics authentication and its categories. Section 2 describes the existing methods on biometrics. Section 3 gives the basic biometrics traits characteristics on authentication. Section 4 presents the overall information on multimodal biometrics system and the comparison analysis of the multimodal system modalities and section 5 provide the contribution of the entire paper.

II. RELATED WORKS

In 2015, Sheetal Chaudhary and Rajender Nath (10) describes a new multimodal biometric system that integrates multiple traits such as iris, face and voice. The authors developed a multimodal biometric system which is able to improve the problems faced by unimodal biometric system. They compared their proposed method with three individual biometric by plotting ROC curves. In the experimental evaluations on a public data set the authors also demonstrate its accuracy. The ROC curves shows in this paper improve the recognition performance compared with single biometric systems. The authors also check the effectiveness of this system regarding FAR (False Accept Rate) and GAR (Genuine Accept Rate) is demonstrated with the help of MUBI (Multimodal Biometrics Integration) software.

In 2014, Komal sondhi and Yogesh bansal (5) proposed a new method based on some studied biometrics schemes. Their research aimed to explore the use of minutia points and ridge to detect the spoofing attacks. In this paper finger print mechanism and iris system is used to authenticate. The authors provide some special measures to counter the spoofing type of attacks on the entire authentication processing. For those combination of these mechanisms it is useful because as one needs a close up system and other needs to contact. The each image minute points in this paper are extracted locations can be used as predicting variable. The authors also test various image samples with this multi biometric scheme to detect spoofing attacks.

In 2010, Mohamed soltane et al. (7) has come out with the idea of GMM (Gaussian Mixture Model) based Expectation Maximization (EM) estimated algorithm. They discussed a multimodal biometric system include psychological and behavioral features. The authors presented a human authentication method combined face and speech information. The experimental result in this paper shows the better processing of this multimodal mechanism. The authors say that this explained results on simulation model which is provide a significant performance.

In 2009, Karthick Nandakumar et al. (3) have proposed a Bayesian approach for consolidating ranks and a hybrid scheme. This was utilizes both ranks and scores to perform fusion in identification systems. The authors observes that the recognition performance of the simplest rank level fusion scheme which is also perform complex fusion strategies. They also show the fusion algorithm that was originally designed for the verification code, can be extended for synthesis in the identification scenario. This fusion rules can also easily deal with missing data that is commonly encountered multi biometric identification systems without any need of ad-hoc-modifications. They also compared some existing methods with their proposed method to enhance the fusion multi biometric identification systems.

A. Challenges in Biometric systems

The following three main factors that contribute to the complexity (3) of biometric system such as,

Accuracy (FAR, GAR and rank identification rate)

An ideal biometric system should always provide the correct identity decision when a biometric sample is presented. However, a biometric system seldom encounters a sample of a user's biometric trait that is exactly the same as the template.

Scalability (Database size)

In the case of a biometric verification system, the size of the database (number of enrolled users in the system) is not an issue because each authentication attempt basically involves matching the query with a single template.

Usability (Ease of use, security and privacy)

Although it is difficult to steal someone's biometric traits, it is still possible for an impostor to circumvent a biometric system in a number of ways. For example, it is possible to construct fake or spoof fingers using lifted fingerprint impressions (e.g., from the sensor surface) and utilize them to circumvent a fingerprint recognition system. Behavioral traits like signature and voice are more susceptible to such attacks than anatomical traits.

III. BIOMETRIC AUTHENTICATION TRAITS

In this paper, we have discussed a multimodal biometric authentication system which is enhancing the security considerations as much as possible. Here some basic biometric authentication traits are conferred as follows,

A. *Fingerprint Recognition*

Fingerprint is a graphical pattern of ridges and valleys on the surface of human finger (8). It has used on personal identification because of it is one of the human characteristics. The fingerprint recognition is mainly used on various forensic departments like criminal identification. Most automatic system for fingerprint comparison is based on minutiae matching. The minutiae matching characteristics represent the termination and bifurcations of the fingerprints. A good quality fingerprint image contains about 40 to 100 minutiae. A fingerprint is the feature pattern of one finger and it is believed that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and recognition. A fingerprint is composed of ridges and furrows which are parallel and have same width.

Fig1. Fingerprint Recognition

B. ***Iris Recognition***

Iris is one of the biometrics authentication systems which are located between cornea and lens of the human eye (6). Basically the iris function is to control the amount of light entering through the pupil. It consists of a number of layers, in the lowest layer it contains dense color cells and also it determines the color of iris. In image processing techniques it can be employed to convert iris pattern to unique code which can be stored in a database and allows comparison between templates. The overall process for acquiring and storing iris features with iris images as listed as follows,

- Image acquisition: take photo of iris with good resolution and quality.
- Segmentation: process the acquiring image for separation of iris from eye image.
- Normalization.
- Feature extraction and feature encoding.
- Storing extracted codes in database and comparing acquiring iris images with codes in database.

Fig.2. Iris Recognition

C. ***Face***

The facial attributes are probably the most common biometric features used by humans to recognize one person to another (6). There are two most popular approaches are available, the first one is depends on the location and shape of facial attributes such as eyes, nose, lips and chin. Another analysis of the face image represents a face as a weighted combination of a number of canonical faces.

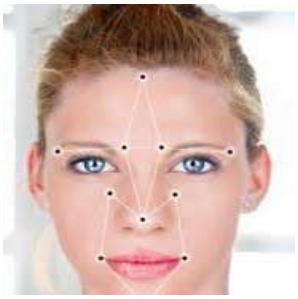

Fig.3. Face Biometrics

D. ***Signature***

A person signs his name is a unique way is known to be characteristic of that individual (11). The general shape of the signed name is to be verified in addition a signature recognition system can also measure pressure and velocity of the points of the stylus across the sensor pad.

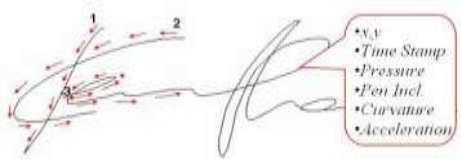

Fig.4. Signature Biometrics

E. ***Voice***

In voice biometrics it is a combination of physical and behavioral biometric characteristics (11). The physical features of an individual's voice are based on the shape and size of the vocal tracts, mouth, 4 nasal cavities, and lips that are used in the synthesis of the sound. The feature extraction of the voice measures sounds is unique to each and every person, because of its vocal tract.

Fig.5. Voice Biometrics

IV. MULTIMODAL BIOMETRIC IDENTIFICATION SYSTEM

In unimodal biometric system it is easily interrupted or any malicious attacks accruing are possible (4). So when we want to provide high authentication, multimodal identification is the better choice. Multimodal authentication mechanism is nothing but it is the combination of unimodal system with two or three and so on. Furthermore, multi

biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. By asking the user to present a random subset of biometric traits, the system ensures a live user is indeed present at the point of data acquisition.

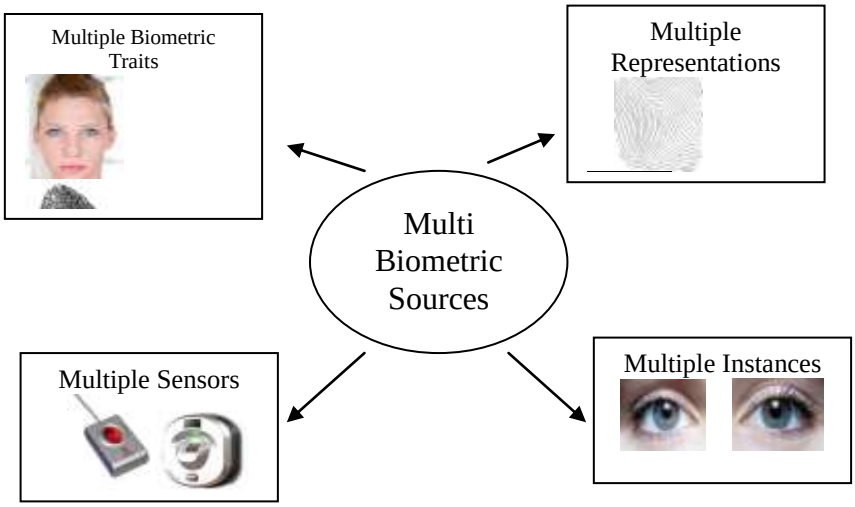

Fig.6. Data base diagram on Multi Biometric sources

When designing a multimodal biometric system a variety of factors should be considered. These include the choice and number of biometric traits, the level in the biometric system and the methodology. The choice and number of biometric traits is largely driven by the nature of the application, the overhead introduced by multiple traits and the correlation between the traits considered. In a multi biometric system it offers several advantages like better recognition accuracy, increased population coverage, greater security and flexibility.

The better performance of the multi model biometric system is to establish the following two types of error rates (3),

FAR (False Acceptance Rate)
It is defined as the probability of an imposter being accepted as a genuine individual. FAR is measured as the fraction of impostor score exceeding the predefined threshold.

FRR (False Rejection Rate)
It is defined as the probability of a genuine individual being rejected as an imposter. FRR measured as the fraction of genuine score below the predefined threshold.

A. **Comparisons on various multimodal systems**

The following types of papers are referred and compared with the multimodal fusion methodology and its level of fusion.

TABLE.1. ***Comparison of Various Biometrics***

Multi Modalities type and its fusion

The above table shows the fusion methodology and levels of fusion in multi model systems. This can be used on identification and verification process to access the secured data.

S.NO.	MODALITIES TYPE	LEVEL OF FUSION	FUSION METHODOLOGY	REFERENCE
1	Face & Voice	Matching Level	Voting k-NN	9
2	Face & Fingerprint	Score & Decision	Sum Rule	4
3	Lips (Audio & Visual)	Decision Level	Optimal Weight (SVM)	11
4	Fingerprint & Hand geometry	Combination Approach	Sum, Max, Min scores	6
5	Speech & Signature	Matching Level	Likelihoods Ratio	1
6	Left & Right iris	Matching Level	Simple sum	10

V. CONCLUSION

Multi biometric systems provide an efficient authentication method compared with unimodal biometric system. Because multi biometric systems

afford to improve matching performance, increase population coverage, spoofing attacks and facilitate indexing. Various fusion levels and scenarios are possible in multi biometric systems, the important method is being the fusion at the matching score level. Basically multimodal biometrics system is a combination of biometrics traits. In this paper, a study of various biometrics traits is discussed and multimodal identification method characteristics are provided. The comparison of different levels of fusion and fusion methodologies gives an optimal identification of multimodal traits selection criteria. In future, a better result can be obtained by using the combination of two or three traits by improving the genuine acceptance rate and decreasing the false acceptance rate with the help of some specific algorithms.

REFERENCES

[1] V. Aggithaya et al., "A Multimodal biometric authentication system based on 2D and 3D palmprint features", Proc. of SPIE Vol. 6944 69440C-1- 2012.

[2] Jain.A et al., "An identity authentication system using Fingerprints", In Proceedings of the IEEE (September 1997), vol. 85, pp. 1365–1388.

[3] Karthik Nandakumar et al. "Fusion in Multibiometric Identification Systems: What about the Missing Data", to appear in Proc. of ICB, Alghero, June 2009, pp. 1-10.

[4] M. Kazi and Y. Rode, "multimodal biometric system using face and signature: a score level fusion approach", Advances in Computational Research, Vol. 4, No. 1, 2012.

[5] Komal Sondhi and Yogesh Bansal, "Concept of Unimodal and Multimodal Biometric System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014, pp. 394-400.

[6] Meraoumia et al., "Fusion of Finger-Knuckle-Print and Palm print for an Efficient Multi-biometric System of Person Recognition", IEEE ICC 2011.

[7] Mohamed Soltane et al. "Face and Speech Based Multi-Modal Biometric Authentication", International Journal of Advanced Science and Technology, Vol. 21, August, 2010, pp. 41-56.

[8] Ratha.N et al. "Adaptive flow orientation based feature extraction in fingerprint images Pattern Recognition", Vol.11, Issue 28 (1995), pp. 1657–1672.

[9] A.Ross and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", In Proceeding of SPIE Conference on Biometrics Technology for Human Identification, volume 5779, Florida, U.S.A., March 2005, pp.196-204.

[10] Sheetal Chaudhary and Rajender Nath, "A New Multimodal Biometric Recognition System Integrating Iris, Face and Voice", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015, pp. 145-150.

[11] Dr. Shubhamgi and D.C.Manohar Bali, "Multi-Biometric Approaches to Face and Fingerprint Biometrics", International Journal of Engineering Research & Technology, ISSN- 2278-0181, 2012.