The Survey Multi-Model Biometric Authentication System With Fusion Technique

Rakhi Choudhary[1], Er. Krishan Kumar[2]
[1]M.Tech (Scholar), [2]Assistant Professor
Department of Computer Science Engineering, Jan Nayak Chaudhary Devi Lal Memorial College of Engineering

Abstract - A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. Multimodal biometric system uses multiple biometric characters of person in establishing his identity. The sources of information from different characters are captured, pre-processed, features are extracted and matched with the stored templates in the database. The information fusion of biometric characters can take place in any of the levels such as sensor level fusion, feature level fusion, match score level fusion or finally in decision level fusion. Evaluation schemes are presented to test the performance of quality metrics for various applications. A survey of the features, strengths, and limitations of existing quality assessment techniques in fingerprint, iris, and face biometric are also presented. This paper summarizes the multimodal biometrics techniques which identify an individual from others and also describes a lot of multimodal biometrics systems. Many literatures show that multimodal biometrics techniques have performed more reliability and security than monomodal biometrics ones as they take more than one physiological or behavioral characteristics of the person into account to identify and verify that person. Multimodal biometrics have become one of inevitable trends in the future.

Keywords *– Biometric Authentication, multi-modal system, ATMs, quality metrics.*

I. INTRODUCTION

Biometrics is the science and technology used for measuring, analysing the biological data. In information technology, biometrics usually refers to measuring and analysing human body characteristics such as fingerprints, eye retinas and irises, voice patterns[1], facial designs, and hand measurements, expressly for authentication purposes. The biometric is used for extracting a feature set from the acquired information, and comparing this set alongside to the template set in the database. Biometric fusion can be defined as the use of multiple types of biometric data for improving the performance of biometric systems. Therefore combination of several complementary biometrics can provide higher recognition accuracy than any individual biometric alone[2]. Multimodal biometric systems perform better than uni-modal biometric systems as it removes the limitations of single biometric system. The most used identification used in criminology is personal identification. The personal identification makes it possible to arrest the criminal in accurate way. Defining the identification of human being that is criminal is very difficult. Biometric system has now been used in the various commercial and forensic applications. These biometrics highly based on the fingerprints, speech, ear, gestures, hand geometry, iris, retina, face, hand vein etc [3].

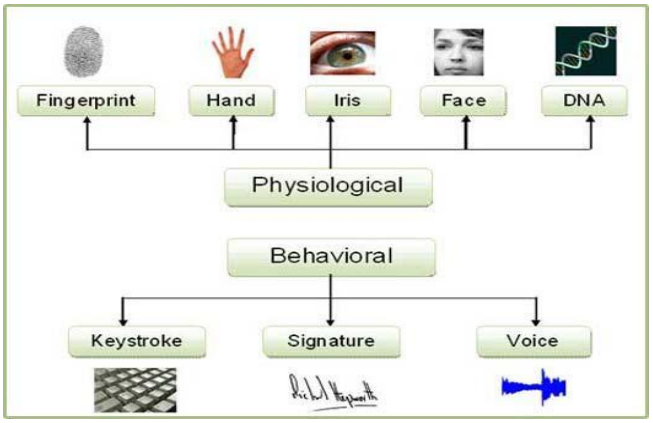


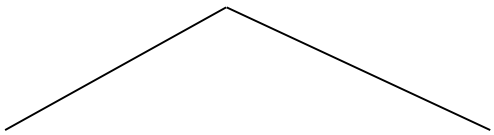
Fig 1. Biometric Traits

Generally, any typical authentication biometric system comprises of the following units:

- *Data acquisition unit:* consist of acquiring the biometric signal with a special sensor and then converting the signal to a digital form.
- *Feature extraction unit:* extraction of features is done using various classifiers like SVM, Neural network, HMM and feature extraction methods like GA, PCA, and ICA etc[4].
- *Matching unit:* matching of testing and training samples is done using various distances like hamming, Euclidean distances.
- *Decision making unit:* this final step issues a binary decision whether to accept or reject the claimed identity [5].

Multiple biometric indicators for identifying individuals is known as multimodal biometrics. In the multimodal biometric systems firstly, individual biometrics systems are run then fusion is made using various algorithms to enhance the performance of the system. There are two parameters named FAR and FRR. Their rate can be reduced if the negative results are less than the positive results. There are many levels at which fusion takes place like sensor level, extraction level, matching the score level and decision level[6].

Biometric Modalities



Physiological **Behavioural**

Fingerprint	**Signature**
Veins	Voice
Hand	Gait
Eye	Keystroke

Speech recognition process is basically done by the Speech Recognition System. In the speech recognition process, speech input signal is processed into recognition of speech as a text form. Speech Recognition System helps the technology to bring computers and humans more closely. There is basic terminology that one must know in order to implement or develop a Speech Recognition System[7].

Fig.2: Speech Sample

The human face plays a significant role in our social [8] interface, conveying people's identity. With the human face as a key to safety, biometric face recognition expertise has received significant attention in the past few years due to its possible for a wide variability of applications in both law enforcement & non-law enforcement.

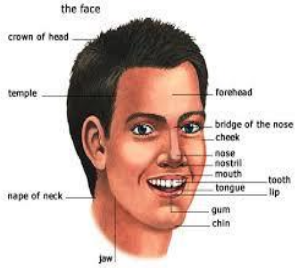


Fig.3: Face Sample

The categorized into 2 types:

i) Fusion prior to similar
ii) Fusion before matching

A. Fusion prior to matching

In Fusion prior to similar integration of data can take place either at sensor level or at feature level.

a. Sensor level

In sensor level fusion, for single biometric trait, multiple pictures can be taken from multiple sensors to get the information.

b. Feature level [9]

When features are related then usual feature can be measured. When features are non- similar than we can assimilate them to form single feature. Concatenation is problematic due to following details:

(i) The unidentified relation amongst feature vectors.
(ii) Integration leads to large vector space.

B. Fusion after matching

c. Matching score level

The dissimilar modules are generated, the extracted features generates the scores from dissimilar modules produce a single score by combining. Concluding result is taken by in view of the combined score. The final decision are based on Normalization and Similarity/ Dissimilarity Score

d. Decision level [10]

It is the highest level fusion of biometric evidences. Decision is based on the number of matches performed having threshold and it independently makes its conclusion.

e. Rank level

The output is the ranks of enrolled identities for identification. This fusion scheme is used to fuse the ranks of entity biometric systems to obtain a fused status for each individuality. It reveals less in sequence than match scores. The ranking output by multiple biometric systems is comparable. Therefore, the exactness of biometric systems can be enlarged by means of any of the above fusion methods.

II. RELATED WORK

Hachim El Khiyari et al., 2016 [11] described that the novel use and efficiency of deep learning, in general, and convolutional neural networks , in individual, for automatic rather than hand-crafted feature abstraction for robust face recognition crossways time lapse. A CNN construction using the VGG-Face deep learning is found to harvest highly discriminative and interoperable features that are healthy to aging differences even across a mix of biometric datasets. The structures removed show high inter-class and low intra-class unevenness leading to low generalization errors on aging datasets using ensembles of subspace discriminant classifiers. **Ismahène DEHACHE et al., 2015 [12]** defined that numerous identification and verification systems are now advanced, however their presentations remain unacceptable facing to the increasing security needs. Generally, the use of only one biometric decreases the reliability of these schemes; thus, we have to association several modalities. It proposes a multi biometric fusion approach for identity verification using two modalities: the

fingerprints and the signature. Mixtures of neural multi-layer perceptron's (MLP) are used for the unimodal classification. The multimodal integration method is based on the use of Support Vector Machines (SVM). The last individuality verification decision is made giving to the scores generated by the SVM classifier. **LamisGhoualmi(et al.),2015[13]**The projected method has been applied on a synthetic multi-modal biometrics database. The latter is shaped from Casia and USTB 2 databases which represent iris and ear image sets respectively. **Satrajit Mukherjee(et.al),2014[14]** Novel adaptive weight and supporter based function mapping the matching scores from dissimilar biometric causes into a single merged matching score to be used by a classifier for further decision making. Differential Growth has been working to regulate these unable parameters with the independent being the minimization of the covering area of the occurrence distributions of open and imposter scores in the fused score space, which are projected by Gaussian kernel density technique to achieve higher level of accuracy. **Samarth Bharadwaj(et.al), 2014 [15]**Review of the features, strengths, and boundaries of existing quality evaluation technique in fingerprint, iris, and face biometric are also obtainable. lastly, courier set of quality metrics from these three modalities are evaluate on a multimodal database consisting of2D images, to appreciate their performance with deference to match score obtained from the state of the art recognition systems. The study of the characteristic function of excellence and match scores show that a cautious selection of admiring set of superiority metrics can provide more advantage to various applications of biometric excellence. **Vincenzo Cont(et.al),2013 [16]**In this section fingerprint and iris based unimodal and multimodal confirmation systems will be describe, analyse and evaluate. To conclude, a prototype embedded multimodal biometric sensor will be sketch. Software and hardware prototypes have been checked against common and broadly used databases.

III. ARCHITECTURE OF MULTI-MODAL BIOMETRIC SYSTEM

Architecture of a multimodal biometric structure refers to the order in which the multiple cues are acquired and processed. The multi-model biometric system are two kinds i.e **Serial and Parallel.**

A. ***Serial Architecture****:* In this architecture, processing takes place in the sequential manner. E.g. ATM processing.[17]

B. *Parallel Architecture:* In parallel architecture, processing takes place in the non-sequential manner. e.g. military.

Most of the biometric systems will serve one of the two basic purposes: authentication/verification or identification. Authentication (or verification) is the process of positively identifying the user. Identification, on the other hand, is the procedure of distinguishing a separate from a larger set of individual records by comparing the presented biometric data with all entries in the system database. This is also referred to as one-to-many match and therefore, it is a much more time consuming operation than authentication, as it requires a large number of comparisons. These are: knowledge-based systems, (based on what you know, such as, keyword, personal identification number (PIN)); [18] object-based systems, (based on what you have, such as, token, smartcard); and physiological/behavioural characteristic-based systems, (based on who you are, such as, biometrics) . In fact, the social network of the user, that is, somebody you know, recently proposed as the fourth factor that can be used for authentication.

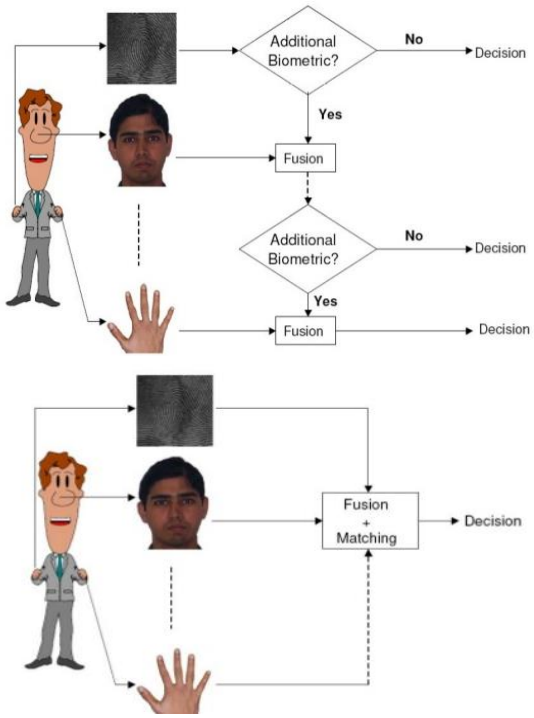


Fig.4: Serial Architecture and Parallel Architecture

IV. FUSION OF MULTIMODAL BIOMETRICS

The fusion of multimodal biometrics includes many aspects such as fusion ways, fusion levels, normalization techniques, fusion methods and operational modes etc. We will introduce these problems one by one.

A. Fusion Ways

Generally biometric system consists of sensors, feature extraction, matching score and decision-making modules. The combination of single biometric and the fusion of multimodal biometrics may occur at any stage of this process. Some of them may not involve multiple modalities but imply a fusion at some points. They are described as follows.

a) Single biometric and multiple sensors: The same biometric can be obtained using different sensors, and combined to improve the recognition rate[19].

b) Multiple biometrics: Multiple biometrics of the same person can be obtained and fused to improve the recognition rate. This is a real sense of 'fusion'.

c) Single biometric and multiple units: This way uses the same biometric but different unit. For example, we can collect fingerprint of the same person but different finger.

d) Single biometric and multiple representations: The same biometric unit can be obtained several times by a same sensor and represented by multiple ways. Every representation has its classifier, and matching scores generated by classifier are computed and combined to improve the recognition rate.

e) Single biometric and multiple matchers: The same biometric is obtained by a single sensor. Different approaches of feature extraction and matching methods are combined to improve the recognition rate.

B. Fusion Levels

Biometric systems have four important components, and information fusion or combination can occur at every stage.

- ***a) Features extraction:*** If the extracted biometrical features or traits are independent each other, they can be fused or combined to form a unique feature vector.
- ***b) Matching score level :*** Matching score which describes the similarities between the acquired biometrics and their templates is put out by every biometric system and combined. This kind of fusion requires normalization of the matching scores in order to assure that matching scores belong to the common domain [3, 4]before they are fused or combined. Generally two steps are performed: statistical estimation of the scores distribution and translation into a common domain[20].

V. CONCLUSION AND FUTURE SCOPE

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.

VI. REFERENCES

[1]. Snelick, Robert, Umut Uludag, Alan Mink, Mike Indovina, and Anil Jain. "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems." IEEE Transactions on Pattern Analysis and Machine Intelligence 27, no. 3 (2005): 450-455.

[2]. Wayman, James, Anil Jain, Davide Maltoni, and Dario Maio. An introduction to biometric authentication systems. Springer London, 2005.

[3]. Tuyls, Pim, Anton HM Akkermans, Tom AM Kevenaar, Geert-Jan Schrijen, Asker M. Bazen, and Raimond NJ Veldhuis. "Practical biometric authentication with template protection." In International Conference on Audio-and Video-Based Biometric Person Authentication, pp. 436-446. Springer Berlin Heidelberg, 2005.

[4]. Fierrez-Aguilar, Julian, Javier Ortega-Garcia, Joaquin Gonzalez-Rodriguez, and Josef Bigun. "Discriminative multimodal biometric authentication based on quality measures." Pattern Recognition 38, no. 5 (2005): 777-779.

[5]. Burger, Paul M. "Biometric authentication system." U.S. Patent 6,219,439, issued April 17, 2001.

[6]. Snellick, R., U. Uludag, and A. Mink. "Large scale evaluation of multi-model biometric authentication using state-of-the-art system." IEEE Trans on Pattern Analysis and Machine Intelligence 27, no. 3 (2005): 450-455.

[7]. Lee, Y., Lee, K., Jee, H. and Pan, S., Lee Yong J, Lee Kyung H, Jee Hyung K and Pan Sung B, 2005. Method for multi-model biometric identification and system thereof. U.S. Patent Application 11/245,586.

[8]. Wang, Jingyan, Yongping Li, Ping Liang, Guohui Zhang, and Xinyu Ao. "An effective multi-biometrics solution for embedded device." In Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, pp. 917-922. IEEE, 2009.

[9]. Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." IEEE Transactions on circuits and systems for video technology 14, no. 1 (2004): 4-20.

[10]. Ross, Arun, and Anil Jain. "Information fusion in biometrics." Pattern recognition letters 24, no. 13 (2003): 2115-2125.

[11]. El Khiyari, Hachim, and Harry Wechsler. "Face Recognition across Time Lapse Using Convolutional Neural Networks." *Journal of Information Security* 7, no. 03 (2016): 141.

[12]. El Khiyari, Hachim, and Harry Wechsler. "Face Recognition across Time Lapse Using Convolutional Neural Networks." *Journal of Information Security* 7, no. 03 (2016): 141.

[13]. El Khiyari, Hachim, and Harry Wechsler. "Face Recognition across Time Lapse Using Convolutional Neural Networks." *Journal of Information Security* 7, no. 03 (2016): 141.

[14]. Ghoualmi, Lamis, SalimChikhi, and AmerDraa. "A SIFT-Based Feature Level Fusion of Iris and Ear Biometrics." Multimodal Pattern Recognition of Social Signals in Human-Computer-Interaction.Springer International Publishing, 2015.102-112.

[15]. Ghoualmi, Lamis, SalimChikhi, and AmerDraa. "A SIFT-Based Feature Level Fusion of Iris and Ear Biometrics." Multimodal Pattern Recognition of Social Signals in Human-Computer-Interaction.Springer International Publishing, 2015.102-112.

[16]. Ghoualmi, Lamis, SalimChikhi, and AmerDraa. "A SIFT-Based Feature Level Fusion of Iris and Ear Biometrics." Multimodal Pattern Recognition of Social Signals in Human-Computer-Interaction.Springer International Publishing, 2015.102-112.
[17]. Ghoualmi, Lamis, SalimChikhi, and AmerDraa. "A SIFT-Based Feature Level Fusion of Iris and Ear Biometrics." Multimodal Pattern Recognition of Social Signals in Human-Computer-Interaction.Springer International Publishing, 2015.102-112.
[18]. Fu, Bo, Jie Lin, and GuiduoDuan. "Analysis of multi-biometric encryption at feature-level fusion." Intelligent Control and Automation (WCICA), 2012 10th World Congress on.IEEE, 2012.
[19]. Dagher, Issam, and RabihNachar. "Face recognition using IPCA-ICA algorithm." IEEE transactions on pattern analysis and machine intelligence28, no. 6 (2006): 996-1000.
[20]. Fox, Niall A., Ralph Gross, Jeffrey F. Cohn, and Richard B. Reilly. "Robust biometric person identification using automatic classifier fusion of speech, mouth, and face experts." IEEE Transactions on multimedia 9, no. 4 (2007): 701-714.