2nd International Conference on Recent Innovations in Science, Engineering and Management
JNU Convention Center, Jawaharlal Nehru University, New Delhi (ICRISEM-15)
22 November 2015 www.conferenceworld.in ISBN: 978-81-931039-9-9

INSIGHT OF MULTIMODAL BIOMETRICS AND FUSION

Priti[1], Tejal[2], Madhwendra Nath[3], Sudhir Mahajan[4], R. B. Dubey[5]

[1,2,3,4,5]*Department of Electronics and Communication Engineering*

Hindu College of Engineering, Sonepat, Haryana, (India)

ABSTRACT

A biometric system is basically a pattern recognition system that acquires biometrics data from a person, extracts the most significant feature set from the acquired data, and compares this feature set against the template set stored in the database, and take the final decision based on the result of comparison. Despite considerable advances in last a few years, there are still challenges in authentication based on a single biometric trait e.g. noisy data, restricted degree of freedom, intra-class variability, non-universality, spoof attack and undesirable error rates. Some of the limitations could be lifted by designing a multimodal biometric system. Multimodal biometrics provides ultra-secure authentication using multiple biometric traits. Here, the various types of multimodal biometric systems and fusion techniques have been discussed.

Keywords: Biometrics, Unimodal, Multimodal, Spoofing, Fusion.

I. INTRODUCTION

Biometrics is going to be very effective authentication and identification method because it binds an individual with his identity and overcomes the main shortcomings inherent in the use of passwords and swap cards. Various biometric characteristics have been used for personal authentication and detection. Some of the biometric techniques are face [1], [2], fingerprint [3], hand vessel, finger-knuckle-print [4], iris recognition and gait etc.

In spite of these inherent advantages, the wide scale deployment of biometrics-based personal identification has been restrained due to several reasons: the first reason less than desirable accuracy in several application domains e.g. in face-recognition. Here, the accuracy of face recognition is affected by illumination, pose and facial expression. The Second is biometric system cannot eliminate spoof attacks. And the third reason is some persons cannot provide the required standalone biometric due to illness or disabilities. The multimodal biometric technologies provide advantage over the conventional unimodal biometric systems.

Some limitations of conventional unimodal or single modal biometric systems are [5]:

Sensitivity of biometric sensors towards noise could lead to inaccurate matching, as noisy data may lead to a bogus rejection.

Unimodal systems are also intended to interclass similarities within huge population groups e.g. in case of identical twins, the facial feature leads to inaccurate matching.

Incompatibility in authentication with certain class of population e.g. the elderly people and young children may have difficulty in enrolling in a fingerprinting system, either due to faded fingerprints or underdeveloped fingerprint ridges.

Finally, Unimodal biometrics is prone to spoofing, where the data can be imitated or forged e.g. rubber fingerprints can be used for spoofing. To prevent this, liven tests are required.

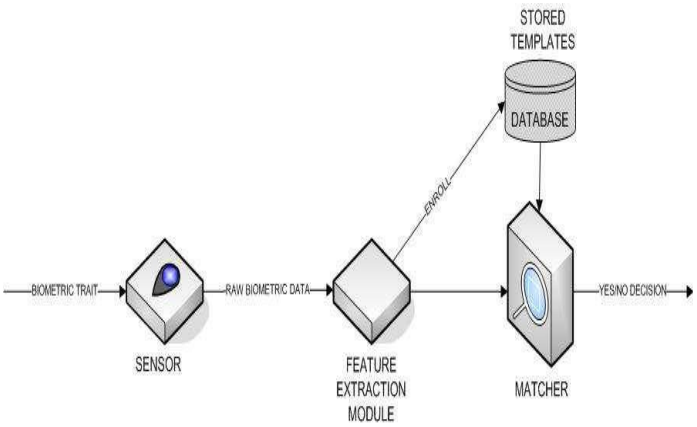

Fig.1. Basic Block Diagram of Biometric Systems [7]

In unimodal biometric system the recognition of a person is performed on the basis of only single type of biometric data and is likely to affect by various problems like noisy data, intra-class variations, distinctiveness and non-universality.

Hence, the idea of multimodal biometric system comes into existence which eliminates the limitations and disadvantages of unimodal biometric systems [5].

Face

Fingerprint

Iris

Hand geometry

Voice

Signature

Fig.2. Some Kind of Body Traits Used for Biometric Recognition

II. MULTIMODAL BIOMETRIC SYSTEMS

Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrollment, identification or verification. A multimodal biometric system uses multiple sensors for data acquisition. This allows capturing multiple samples of a single biometric trait (called multi-sample biometrics) and/or samples of multiple biometric traits (called multi source or multimodal biometrics). This approach also enables a user who does not possess a particular biometric identifier to still enroll and authenticate using other traits, thus eliminating the enrollment problems and making it universal.

The multimodal biometric system significantly improves the recognition performance of a biometric system besides improving population coverage, deterring spoof attacks, and reducing the failure-to-enroll rate. Hence, it is useful to acquire multiple biometric traits for verifying the identity. Multimodal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. By asking the user to present a random subset of biometric traits, the system ensures that a live user is indeed present at the point of acquisition. However, an integration scheme is required to fuse the information presented by the individual modalities. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different applications. Another reason is simply customer preference and satisfaction [5].

The goal of multimodal biometrics is to reduce one or more of the following:

• False accept rate (FAR)

• False reject rate (FRR)

• Failure to enroll rate (FTE)

• Sensitivity to artifacts or mimics

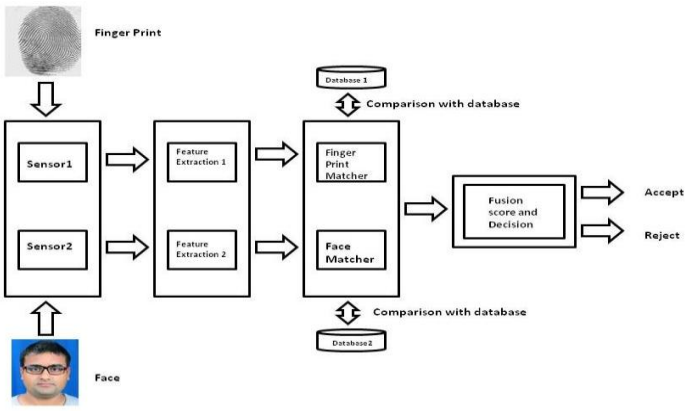

Fig.3. An Example of Multimodal Biometric Systems

The multimodal biometric categories are briefly summarized in the following:

Multiple modalities combine the different types of biometric modalities. This is also known as multimodal biometrics. These systems combine the evidence presented by different body traits for establishing identity. For example, some of the earliest multimodal biometric systems utilized face and voice scores to improve the identity verification of an individual [8].

Multi-algorithmic biometric systems take a single biometric input and process it with different feature extraction algorithms in order to create templates with different information content. One example is processing fingerprint images according to minutiae-and texture-based representation [8].

Multi-instance biometric systems use one sensor (or possibly multiple sensors) to capture samples of two or more different instances of the same biometric characteristics. For example, systems capturing images from multiple fingers are considered to be multi-instance rather than multimodal. However, systems capturing, for example, sequential frames of facial or iris images are considered to be multi-presentation rather than multi-instance. This is whether or not the repeated captured images are combined at the image (feature) level, some other level of combination or a single image is selected as the one best used for pattern matching [5].

Multi-sensorial biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors. Processing of the multiple samples can be done with one algorithm or some combination of multiple algorithms. For example, a face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency (or several frequencies) of infrared illuminations [5].

Multi-biometrics can inherently increase system robustness by removing the dependency on one particular biometric approach. Further, a system that utilizes more than one biometric feature or matcher may be more difficult to deliberately spoof. Systems that make use of multiple biometric features can also provide redundancy that may lower failure-to-acquire rates.

III. FUSION IN MULTIMODAL BIOMETRIC SYSTEMS

Fusion strategies can be divided into two main categories: pre-mapping fusion (before the matching phase) and post-mapping fusion (after the matching phase). The first strategy deals with the feature-vector fusion level. Usually, these techniques are not used because they result in many implementation problems. The second strategy is realized through fusion at the decision level, based on some algorithms, which combine single decisions for each component of the system. Furthermore, the second strategy is also based on the matching-score level, which combines the matching scores of each component system [7].

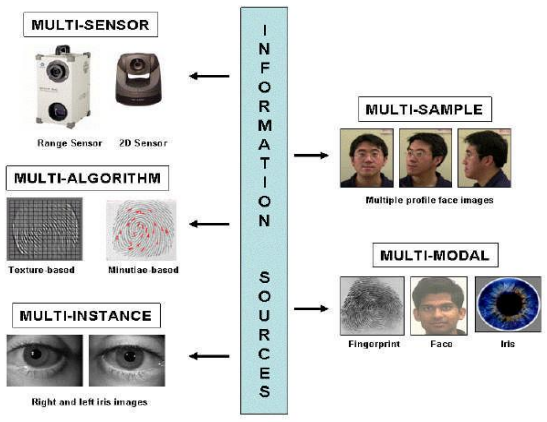

Fig.4. Fusion Scenarios in Multimodal Biometrics [8]

Fusion in multi-modal biometrics systems can be implemented in five ways:

1) Multiple sensors may be used to capture the same biometric;
2) Multiple biometrics may be captured;
3) Multiple readings of the same biometric may be combined to achieve an optimal reading;
4) Readings of two or more units of the same biometric may be taken (*e.g.* two different fingerprints or both irises).
5) Different matching and/or feature extraction algorithms may be used on the same biometric reading to give separate results [7].

IV. ADVANTAGES OF MULTIMODAL BIOMETRIC SYSTEMS

Besides enhancing matching accuracy, some other advantages of multimodal biometric systems over unimodal biometric systems are as following [8]:

Accessibility ease:

Multimodal biometric systems address the problem of non-universality encountered by unimodal biometric systems e.g. if a subject's dry or cut finger prevents his/her from successfully enrolling into a fingerprint system, then the availability of another biometric trait, say iris or face can be used in the inclusion of the individual in the biometric system.

Indexing large-scale biometric databases:

Multimodal biometric systems can facilitate the filtering or indexing of large-scale biometric databases e.g. a bimodal system consisting of face and fingerprint, the face feature set may be used to compute an index value for extracting a candidate list of potential identities from a large database of subjects. The fingerprint modality can then determine the final identity from this limited candidate list.

Spoof attacks:

It becomes very difficult for an impostor to spoof multiple biometric traits of a legitimately enrolled individual.

Noise in sensed data:

Multimodal biometric systems also effectively address the problem of noisy data. When the biometric signal acquired from a single trait is corrupted with noise, the availability of other (less noisy) traits may aid in the reliable determination of identity. Some systems take into account the quality of the individual biometric signals during the fusion process. This is especially important when recognition has to take place in adverse conditions where certain biometric traits cannot be reliably extracted. For example, in the presence of ambient acoustic noise, when an individual's voice characteristics cannot be accurately measured, the facial characteristics may be used by the multimodal biometric system to perform authentication.

V. CONCLUSION

The increased need of privacy and security in one's daily life has given birth to the biometrics technology and this is a very interesting & exciting field that has been growing exponentially in recent years. There are various applications in attendance systems, electronic banking, public identity cards etc where the performance and accuracy of existing biometrics systems may enhanced and improved by implementing the multimodal biometric concept. This paper presents a comprehensive review of existing biometrics technologies and emerging multimodal biometric system.

VI. ACKNOWLEDGMENT

The authors would like to thank Department of Electronics and Comm. Engg. , Hindu College of Engineering Sonepat, Haryana for providing invaluable resources and expertise.

REFERENCES

[1]. W. Zhao, R. Chellapa, P. J. Phillips, and A. Rosenfield, "Face recognition: A literature survey", ACM Computing Surveys, vol. 35, pp.399-458, 2003.

[2]. L. Shen and L. Bai, "A review on Gabor wavelets for face recognition",Pattern Analysis and Applications, vol. 9, pp. 273-292, 2006.

[3]. L. Hong and A. Jain, "Integrating faces and fingerprints for personali dentification", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 20, pp. 1295-1307, 1998.

[4]. L. Zhang, D. Zhang, and H. Zhu, "Online finger-knuckle-print verification for personal authentication", Pattern Recognition, vol. 43, pp. 2560-2571, 2010.

[5]. A. Mishra, "Multimodal biometrics: it is need of future systems" in Int. Journal of Computer Applications, vol. 3, pp. 0975-8887, 2010.

[6]. A. Ross; K. Nandakumar; and A. K. Jain, "Handbook of Multi-biometrics". Springer Science and Business Media, 2006.

[7]. N. Samoska "Evaluation and Performance prediction of multimodal biometric systems" 2006.

[8]. M. Demri "Multimodal biometric fusion using evolutionary techniques" 2012.

[9]. A. Ross and A. Jain, "Information fusion in biometrics," Pattern Recognition Lett., vol. 24, pp. 2115-2125, 2003.