ISSN: 2321-7782 (Online)
Volume 2, Issue 5, May 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

# A Review on Biometric Fusion

**Anu**[1]
ECE Dept
Hindu College of Engineering
Sonipat, Haryana – India

**Madhwendra Nath**[2]
ECE Dept
Hindu College of Engineering
Sonipat, Haryana – India

**Dr. Harvir**[3]
Director-Principal
Hindu College of Engineering
Sonipat, Haryana – India

***Abstract:*** ***A biometric system is basically a pattern recognition system that acquires biometrics data from the 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 recent years, there are still challenges in authentication based on a single biometric trait, such as noisy data, restricted degree of freedom, intra-class variability, non-universality, spoof attack and undesirable error rates. Some of the restrictions can be lifted by designing a multimodal biometric system. Multimodal biometrics provides ultra-secure authentication using multiple biometric traits. We discuss here different types of multimodal biometric systems, different decision fusion techniques used in these systems.***

***Keywords: Biometrics; Multimodal Biometrics; Fusion; Feature Level Fusion; Matching Score Level Fusion; Decision Level Fusion.***

## I. INTRODUCTION

Biometrics is becoming a promising authentication and identification method because it binds an individual with his identity and overcomes the main shortcomings inherent in the use of passwords and smartcards. A number of biometric traits have been used for personal authentication in literature. Some of the examples are face [1, 2], fingerprint [3], hand vessel, finger-knuckle-print [4], iris and gait etc.

Despite these inherent advantages, the wide scale deployment of biometrics-based personal identification has been hindered due to several reasons: Firstly, the less than desirable accuracy in several application domains, for example, face-recognition. The accuracy of face recognition is affected by illumination, pose and facial expression. Secondly, the biometric system cannot eliminate spoof attacks. Thirdly, some persons cannot provide the required standalone biometric, owing to illness or disabilities. The multimodal biometric systems provide advantage over the conventional biometric systems. Some of the limitations of single modal or unimodal biometric systems are [5]:

- Susceptibility of biometric sensors to noise. This can lead to inaccurate matching, as noisy data may lead to a false rejection.
- Unimodal systems are also prone to interclass similarities within large population groups e.g. In case of identical twins, facial feature leads to inaccurate matching, as bad data may lead to a false rejection.
- Incompatibility with certain population. Elderly people and young children may have difficulty enrolling in a fingerprinting system, due to their faded prints or underdeveloped fingerprint ridges.

- Finally, Unimodal biometrics is vulnerable to spoofing, where the data can be imitated or forged. E.g. rubber fingerprints can be used for spoofing, hence liveness tests are required.

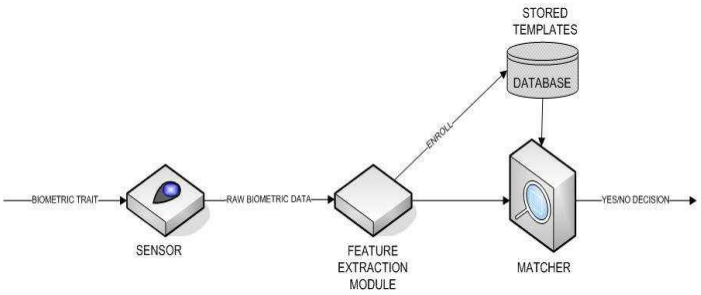
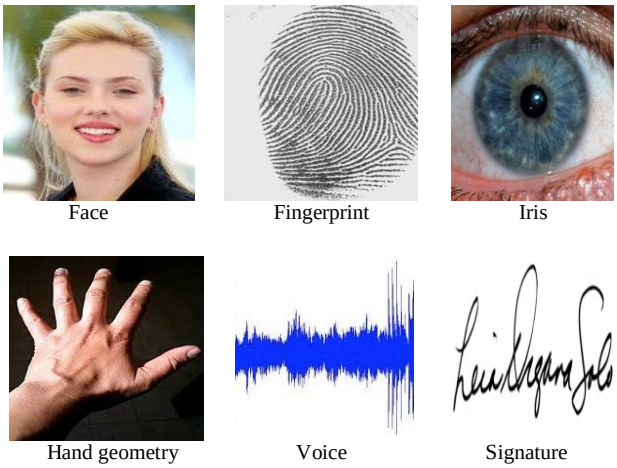



Fig. 1 Basic Block Diagram of Biometric Systems [7]

Single modal biometric system perform person recognition based on single source of biometric data and are likely affected more by the problems like noisy sensor data, intra-class variations, distinctiveness and non-universality. Therefore, the concept of multimodal biometric system comes into existence which eliminates the limitations of single modal or unimodal biometric systems. In later sections we discuss on the multimodal biometric systems [5].

The paper is organized as follows. Section II illustrates about the multimodal biometric systems. Section III describes the fusion techniques. Section IV provides advantages of biometric systems. Section V presents some biometric applications. Finally, some conclusion and future work are reported in Section VI.



Face Fingerprint Iris

Hand geometry Voice Signature

Fig. 2 Examples of body traits that can be used for Biometric Recognition

## II. MULTIMODAL BIOMETRIC SYSTEMS

Multimodal biometric systems are those that utilize more than physiological or behavioral characteristics 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. In such instances, 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 [5].

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

• False accept rate (FAR)

• False reject rate (FRR)

• Failure to enroll rate (FTE)

• Susceptibility to artifacts or mimics

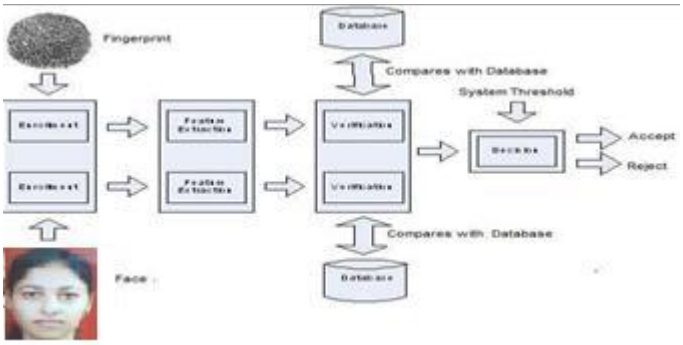



Fig. 3 Example of Multimodal Biometric Systems

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 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].

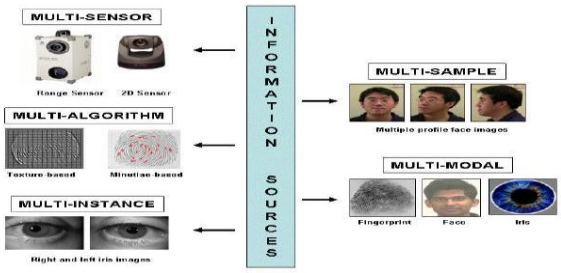



Fig. 4 Fusion Scenarios in Multimodal Biometrics [8]

Multimodal Biometrics with various levels of fusion: sensor level, feature level, matching score level and decision level are

### *A. Sensor Level Fusion*

Data coming from different sensors can be combined, so that the resulting information are in some sense better than they would be possible when these sources were individually used. The term better in that case can mean more accurate, more complete, or more dependable.

### *B. Feature Level Fusion*

The information extracted from sensors of different modalities is stored in vectors on the basis of their modality. These feature vectors are then combined to create a joint feature vector, which is the basis for the matching and recognition process. In addition, it is hard to generate homogeneous feature vectors from different biometrics in order to use a unified matching algorithm.

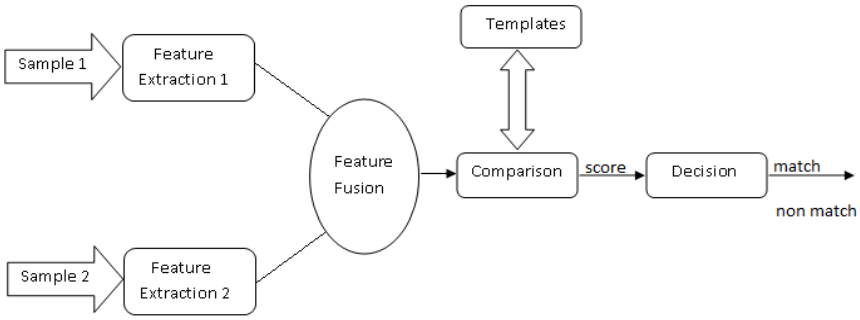



Fig. 5 Feature level fusion

### *C. Matching Score Level Fusion*

This fusion mode consists in combining the scores, which describe the similarities between the biometrics acquired and their templates, obtained by each biometric system. This mode requires a score's normalization, as the scores have to belong to a common domain before the combination.

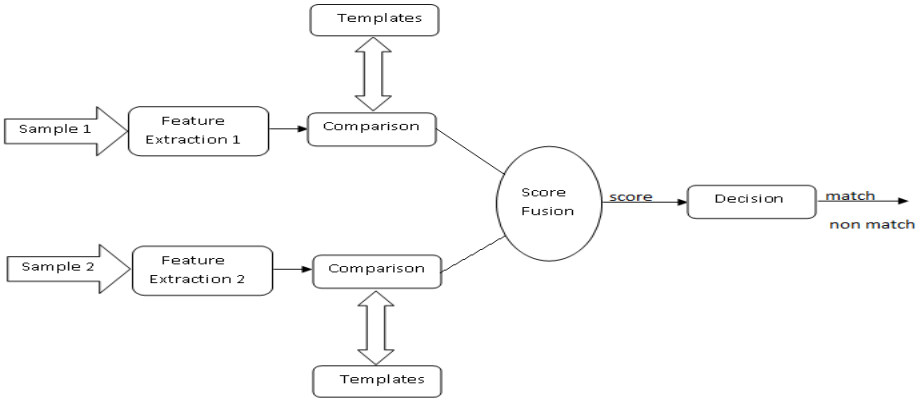



Fig. 6 Matching Score Level Fusion

*D. Decision Level Fusion*

Each sensor can capture multiple biometric data and the resulting feature vectors individually classified into the two classes- accept or reject. A majority vote scheme can be used to make the final decision.

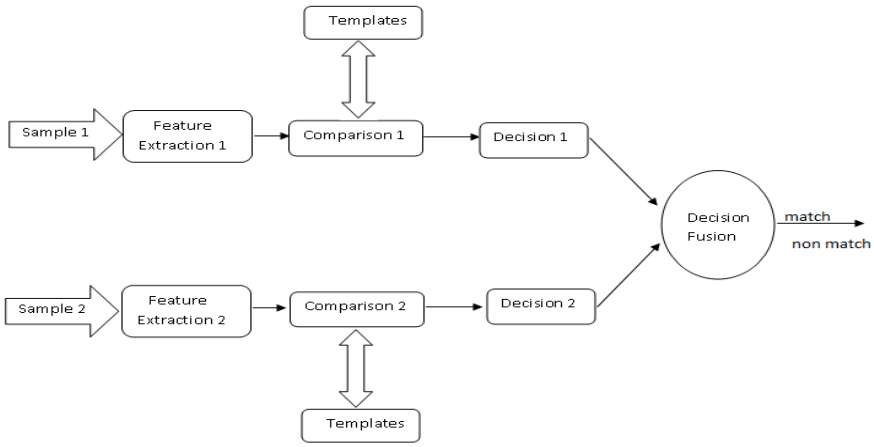



Fig. 7 Decision Level Fusion

## IV. Advantage of Multimodal Biometric Systems

Besides enhancing matching accuracy, the other advantages of multimodal biometric systems over unimodal biometric systems are enumerated below [8]:

*A. Non-universality*

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

*B. Indexing Large-scale Biometric Database*

Multimodal biometric systems can facilitate the filtering or indexing of large-scale biometric databases. For example, in 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.

*C. Spoof Attacks*

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

*D. 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.

*E. Fault Tolerance*

A multimodal biometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation. The notion of fault tolerance is especially useful in large-scale authentication systems involving a large number of subjects (such as a border control application).

## V. Application of Multimodal Biometric System

Most of the biometric applications are related to security and are extensively for military purposes and other government purposes. The applications in the public domain that are available to common people include:

- *Prison Visitor System*, where visitors to inmates are subject to verification procedures in order that identities may not be swapped during the visit- a familiar occurrence among prisons worldwide.
- *Canteen Administration*, particularly on campus where subsidized meal are available to bona-fide students, a system that was being heavily abused in some areas.
- *Border Control*, a notable example for this is the INSPASS trial in America. There are other pilot systems operating elsewhere in this respect.
- *Voting Systems*, where eligible politicians are required to verify their identity during a voting process. This is intended to stop 'proxy' voting where the vote may not go as expected.

In addition there are numerous applications in attendance systems, electronic banking, public identity cards etc.

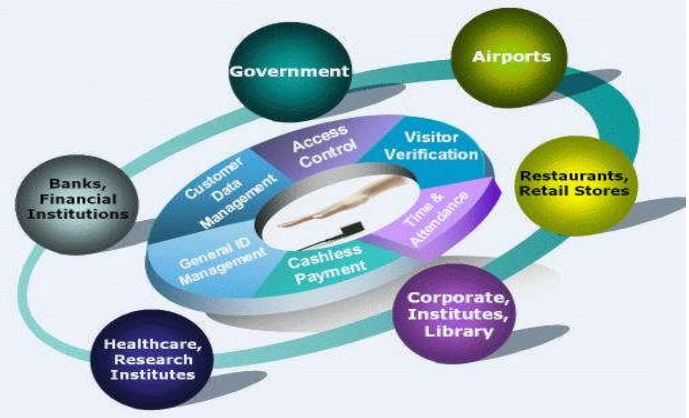



Fig. 8 Different Applications of Biometric Systems [8]

## VI. Conclusion

The increased need of privacy and security in our 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. This paper presents a comprehensive review of existing biometrics technologies.

There is still a lots of work and research need to be done in this field to achieve a prudent balance between security and privacy. Biometric technology will continue to expand as the human quest for knowledge continues.

**ACKNOWLEDGEMENT**

The authors would like to thank Department of Electronics and Communication Engineering, 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 personalidentification", 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. A. Ross; K. Nandakumar; and A. K. Jain, "Handbook of Multibiometrics". 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.