ISSN:2249-5789
Gunjan Jiwnani et al , International Journal of Computer Science & Communication Networks,Vol 5(2),115-119

Multi-modal Biometric Authentication using Fingerprint and Iris: a Review

Gunjan Jiwnani
MTech Student
Mody university of science & technology
(FET) Email:gunjanjiwnani@gmail.com

Mr. Nisheeth Saxena
Assistant Professor
Mody university of science & technology (FET)
Email:

Abstract —

In the present era of information technology, there is a need to implement authentication and authorization techniques for security of resources. There are number of ways to prove authentication and authorization. But the biometric authentication beat all other techniques. Biometric techniques prove the authenticity or authorization of a human being based on his/her physiological or behavioral traits. It also protects resources access from unauthorized users. We will develop a biometric identification system that represents a valid alternative to conventional approaches. In biometric system physical or behavioral traits are used. A multimodal biometric identification system aims to fuse two or more physical or behavioral traits. Multimodal biometric system is used in order to improve the accuracy. Multimodal biometric identification system based on Iris & fingerprint trait based on fuzzy logic is proposed . Typically in a multimodal biometric system each biometric trait processes its information independently. The processed information is combined using an appropriate fusion scheme.

Keywords – Biometric, Multi-modal Biometric, Fuzzy Logic;

1. INTRODUCTION

In the last few years, authentication has become an increasingly important issue in modern society. Authentication has been required in all today's consumer applications in which financial transaction takes place like ATM's, e-commerce etc [3]. It is extremely important to prove that a person is who he/she claims to be. There are a number of procedures and techniques available to identify a person to a computer system, which can be classified into 3 ways

1. Based on what you know.
2. Based on what you have.
3. Based on who you are.

"What you know" undertake approaches like passwords and PINs that have less safety because they can be lost, stolen, or guessed.
"What you have" undertake technologies like e-tokens that can also be stolen.
"Who you are" comprises the class of Biometrics
Among all the available methods biometric has gained more and more attention these days. Biometrics is based on the fact that a person possesses certain characteristics such as retinal patterns, fingerprint patterns, gait, etc that are biologically or behaviorally unique to an individual [3]. It refers to the automatic identification of an individual based on his/her physiological and behavioral traits [5].
It refers to metrics related to human characteristics which can be subdivided into behavioral and physiological approaches.
Behavioral biometric include signature recognition, voice recognition, keystroke pattern, and gait analysis. Physiological biometric include fingerprints, iris, retina scans, hand, finger, face, ear geometry, hand vein, nail bed recognition, DNA and palm prints. As biometrics can't be borrowed, stolen, forgotten, and forging is practically impossible, it has been presented as a natural identity tool that offers greater security and convenience than traditional methods of personal recognition [7].

Biometric systems ensure much greater security as compared to physical features like PIN etc. For Example, face or fingerprint can be stored on a chip in a credit card, and if someone steals the card and tries to use it, the thief's biometric feature will not match the card, and the system will prevent the transaction. An important challenge among biometric is the measurement of quality of a biometric sample. Biometric systems can be affected by the quality of input. Therefore, it is important to evaluate the quality of a

sample to function as a biometric. We can say that quality of a biometric is beyond measuring the quality of the image itself [10] like a sample's quality is susceptible to irregularities during capture or it may also have low quality by its very nature.
As in figure 1.1 we can see that there are different nature of images, some can act as biometric input while some cannot. Therefore, it is necessary to first analyze the quality of biometric input else the system fails.

(a)Good Quality (b) Low Quality

(c) Very Low Quality

Fig 1.1 Qualities of Images

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:
1. Universality: each person should have the characteristic.
2. **Distinctiveness:** any two persons should be sufficiently different in terms of the characteristic.
3. **Permanence:** the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
4. **Collectability:** the characteristic can be measured quantitatively.

5. **Performance:** which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed?

6. **Acceptability:** which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives?
7. **Circumvention:** which reflects how easily the system can be fooled using fraudulent methods?

Biometric-based authentication systems represent a valid alternative to conventional approaches [12] but Biometric systems based on a single source of information (unimodal systems) suffer from much limitation like:
1) ***Trouble with data sensors:*** Captured sensor data are often affected by noise due to the environmental conditions (insufficient light, powder, etc.) or due to user physiological and physical conditions (cold, cut fingers, etc).
2). ***Intra-class variations.*** The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor or when sensor characteristics are modified like changing sensors, the varying psychological makeup of an individual might result in vastly different behavioral traits at various time instances.
3) ***Distinctiveness ability***: Not all biometric features have the same distinctiveness degree (for example, hand geometry based biometric systems are less selective than the fingerprint-based ones).
4) ***Lack of universality:*** All biometric features are universal, but due to the wide variety and complexity of the human body, not everyone is endowed with the same physical features and might not contain all the biometric features, which a system might allow. The biometric system may not be able to acquire meaningful biometric data from a subset of individuals resulting in a failure-to-enroll (FTE) error
5). ***Spoof attacks.*** An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system.

3. NEED FOR MULTIBIOMETRIC

In highly sensitive environments, a single, initial authentication may not be sufficient to guarantee security [3]. Combining the evidence obtained from different sources using an effective fusion scheme can significantly improve the overall accuracy of the biometric system [5].
These systems demonstrate significant improvements over

unimodal biometric systems, in terms of higher accuracy and high resistance to spoofing (A type of scam where an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user.). Multibiometric systems are being increasingly deployed in many large-scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to unibiometric systems. However, multibiometric systems require storage of multiple biometric templates (e.g., fingerprint, iris, and face) for each user, which results in increased risk to user privacy and system security.

4. INTEGRATION OF MULTIBIOMETRIC

There exist many possibilities of integration of different biometrics depending upon the system requirement [3]:

1. *Multiple sensors:-* The single biometric trait imaged using multiple sensors. Different sensors can be used to acquire the same biometric trait. For example, optical and capacitive fingerprint sensors used for the same finger, or the both 2D and 3D images of the face. Therefore, the system reliability is increased since the identification/verification can be performed even if one sensor fails the acquisition.
2. *Multiple biometrics:* The use of the evidences collected from multiple traits. Biometric characteristics such as fingerprint and face are combined. These systems contain more than one sensor with each sensor sensing a different biometric characteristic.
3. *Multi-instance systems* –The use of multiple instances of same biometric trait like for the enrollment and/or recognition. For example, multiple impressions of the same finger, multiple samples of the voice, or multiple images of the face may be combined.
4. *Multi-sample systems* – A single sensor used to get multiple samples of same biometric trait like fingerprints from two or more fingers of a person may be combined, or one image each of the two irises of a person may be combined.
5. *Multi-algorithm systems* – The same biometric data processed with different algorithms. This involves combining different approaches to feature extraction and matching of the biometric characteristic.

5. LEVEL OF FUSION IN MULTIBIOMETRIC

Multi-biometrics data can be combined at different levels:
1. Fusion at data-sensor level
2. Fusion at the feature extraction level.
3. Fusion at the matching level, and
4. Fusion at the decision level.

Multi-modal systems are based on different biometric features or introduce different fusion algorithm of these features. There are many different fusion techniques available like neural networks, fuzzy logic etc.

Categories of fusion:

1. Fusion prior to matching (pre-classification fusion) i.e. combining information prior to the matching decision.
2. Fusion after matching (post-classification fusion) i.e. combining information after the matching decision.

Fusion prior to matching takes place either at the sensor level or at the feature extraction level.

Sensor level: For example face image from multiple cameras form a single face image at the sensor level but the images obtained from camera must be of same resolution, because images of different resolution cannot be fused.

***Feature extraction level*:** biometric traits can be homogeneous (multiple images of user's fingerprint) or heterogeneous (face, fingerprint images of user). In case of homogeneous a single average feature vector can be calculated while in case of heterogeneous diff feature vectors are combined to form single one.

Fusion after matching can be categorized ito 4 ways:

1. ***Dynamic classifier selection*:** it chooses the result of that matcher (classifier) which gives the correct decision corresponding to particular output.
2. ***Fusion at the abstract level:*** it occurs when each matcher individually chooses the correct output based on its input.
3. ***Fusion at the rank level:*** it occurs when output of each matcher act as an input to other.
4. ***Fusion at the matching scores level*:** it occurs when the matcher produces a set of matches.

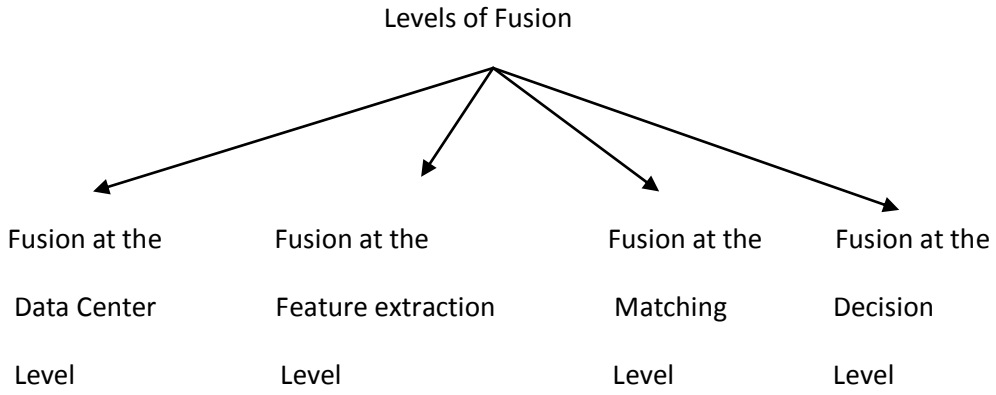

Fig 5.2 Levels of Fusion

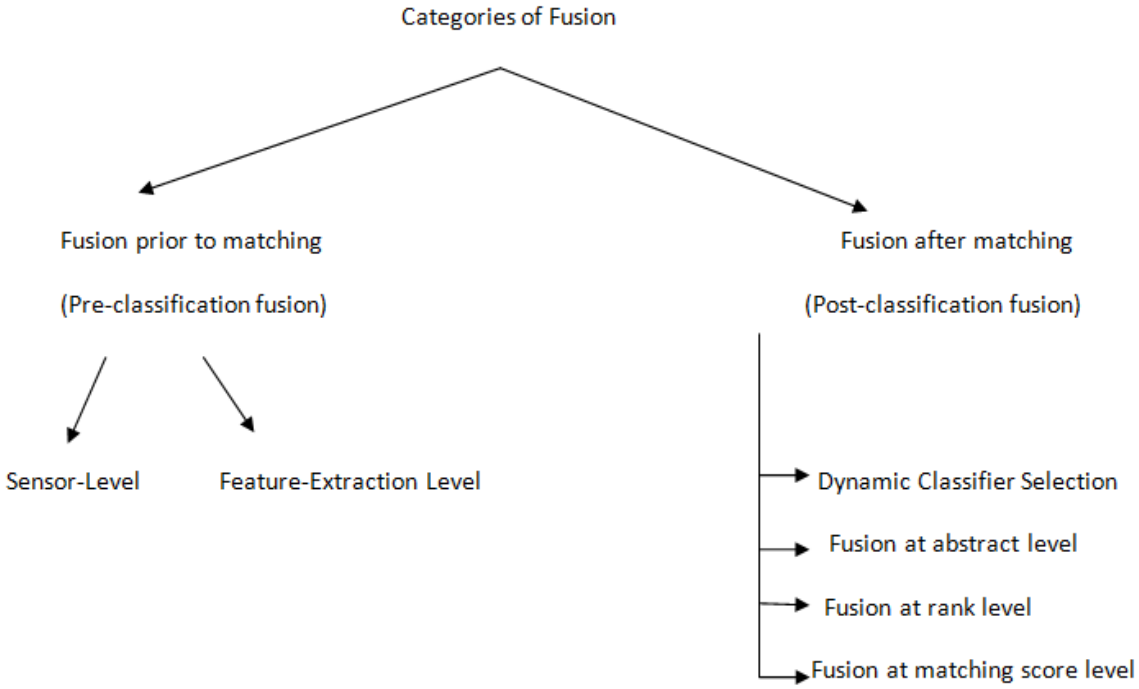

Fig 5.2 Categories of Fusion.

6. PROPOSED MODEL

In the proposed model we are taking two biometric traits fingerprint and iris and after performing the processing individually on two biometrics. We will apply the fuzzy fusion technique and finally take decision that the authentication is very high or low. Its steps are

1. Firstly, some steps are performed on fingerprint image which are segmentation, normalization, remove noise, binarization, thinning and minutiae extraction. Then fingerprint image will go for fusion.
2. Now based on the minutae extraction features of fingerprint, its matching process will be performed whether the input fingerprint image is genuine or not. If it is matched then user is authenticated.
3. After this, we will check for iris. The radius of each iris image is calculated and matched with the input iris image. If it is matched then the user is authenticated.
4. After matching both the biometric traits individually we will perform fusion based on fuzzy logic.
5. In this step through appropriate application of fuzzy rules we will develop the relationship between the biometric traits and the final decision (level of security (S)).
6. If (fig is low) and (iris is low) then
(S is Very Low)
If (fig is low) and (iris is middle) then
(S is middle)

If (fig is low) and (iris is high) then
(S is Very Good)
If (fig is middle) and (iris is low) then
(S is Low)
If (fig is middle) and (iris is middle) then
(S is Good)
If (fig is middle) and (iris is high) then
(S is Very Good)
If (fig is high) and (iris is low) then
(S is Middle)
If (fig is high) and (iris is middle) then
(S is Very Good)
If (fig is high) and (iris is high) then
(S is Excellent).

7. After performing these steps, we will calculate the FAR(False acceptance rate) and FRR (False Rejection rate).

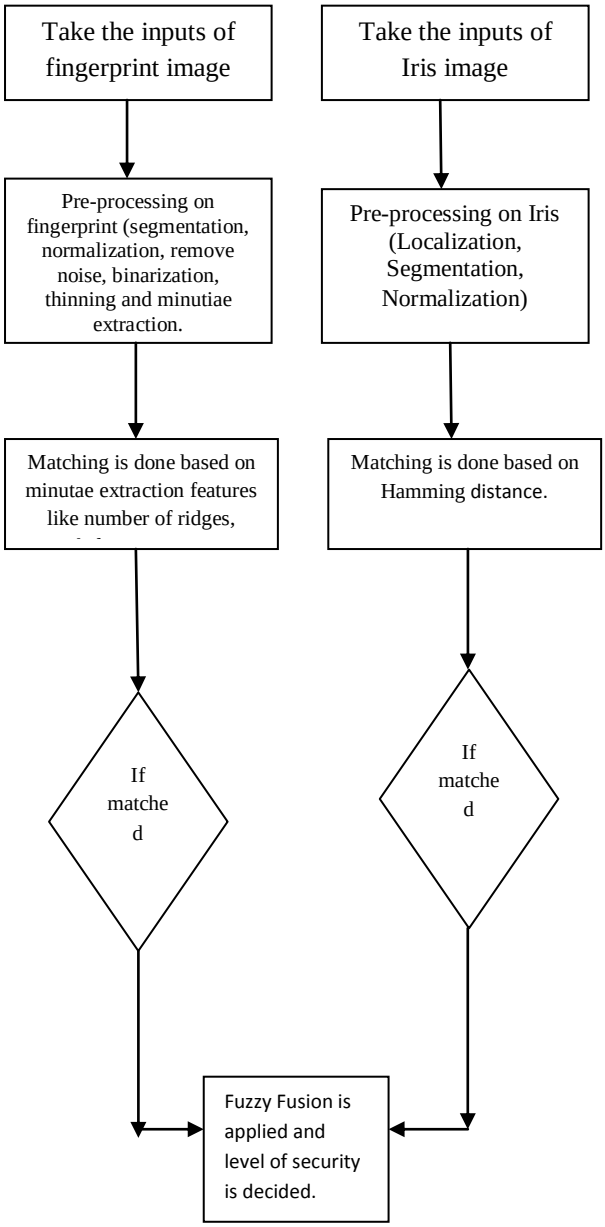

Fig 6.1 Proposed Model

7. CONCLUSION

Nowadays, Biometric systems are used for authentication due to limitations of traditional systems like using PIN, PASSWORD etc. We can use either single biometric trait or multiple biometric traits. Single biometric trait also has some limitations so to overcome these limitations we use multi biometric authentication which gives result with more accuracy but also requires more storage as compared to single biometric.

3. REFERENCES

[1] Mohamad Abdolhi, majid Mohamadi, Mehdi jafari "Multimodal Biometric System Fusion using fingerprint ad Iris with Fuzzy Logic", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

[2] Dipti S. Randive, Manasi M. Patil, "Iris and Fingerprint Fusion for Biometric Identification", International Journal of Computer Applications (0975 – 8887) Volume 77 – No.11, September 2013.

[3] Antonia Azzin, Stefania Marrara,Roberto Sassi, Fabio Scotti, "A Fuzzy Approach to multimodal biometric continuous authentication", Springer Science June 2008.

[4] Mitul D Dhameliya, Jitendra P Chaudhari," A Multimodal Biometric Recognition System based on Fusion of Palmprint and Fingerprint", International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue5- May 2013.

[5] Shekhar Karanwal, " Secure and Reliable Multimodal Biometric Systems Using two and three Biometric Traits", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 7, July 2013.

[6] Dapinder Kaur, Gaganpreet Kaur, "Level of Fusion in Multimodal Biometrics: a Review", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 2, February 2013.

[7] B. Shanthini, S. Swamynathan, " A Novel Multimodal Biometric Fusion Technique for Security", 2012 International Conference on Information and Knowledge Management (ICIKM 2012) Singapore.

[8] Arun Ross, "AN INTRODUCTION TO MULTIBIOMETRICS", 15th European Signal Processing Conference (EUSIPCO), (Poznan, Poland), September 2007.