RESEARCHERID
THOMSON REUTERS

[Selvi * *et al.*, 6(9): September, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

FUSION TECHNIQUES FOR BIMODAL AND MULTIMODAL BIOMETRIC SYSTEM AUTHENTICATION

Mrs. M. Tamil Selvi[*1] & Mrs. A. Sumathi [2]

[*1]M.Phil.,Research Scholar, Department of Computer Science, Navarasam Arts & Science College for Women, Erode, Tamil Nadu, India.

[2]Assistant Professor, Department of Computer Science, Navarasam Arts & Science College for Women, Erode, Tamil Nadu, India

DOI: 10.5281/zenodo.884845

ABSTRACT

Biometrics is the one of the security mechanism for computer network security. It is science and technology of measuring and analyzing biological data of human body, extracting details from the acquired data, and comparing the data to the stored in database. Existing system is unimodal biometric system. The proposed system is supported fusion techniques multimodal biometric system. However Multimodal biometrics requires storage of multiple biometric templates for each user, which results in increased risk to user privacy and system security. This paper will discuss the concept off biometrics, biometric working process, unipolar biometrics, bipolar biometrics and multipolar biometrics with their fusion techniques.

KEYWORDS: Fusion, Biometrics, Multipolar, Bipolar, Unipolar, Accuracy

I. INTRODUCTION

Biometrics means ''Life measurement''. Biometrics refers to the study of measurable organic characteristics. It also refers to some of the techniques that access repeatedly and checked. It also characterized in physical or behavioral things. Biometric identification has eventually a much broader significance as computer interface becomes more natural.

Biometrics is used for security systems and substitution systems for ID cards, tokens or PINs. A key difference between biometrics and other systems is that biometric confirmation of physical information requires a person to be present, which adds a layer of security because other ID types can be stolen, lost or forged.

Biometric component and feature

A biometric system includes the following components and features:

- A sensor that grabs data and changes it into a usable, digital format via software. This data may be from human behavioral or corporeal characteristics, such as a fingerprint or retinal scan. An attainment device, such as a microphone or scanner, captures the data.
- A biometric template developed via the biometric system's signal processing algorithms. These templates are compared to the biometric system's data storage, and data is usually encrypted for added security. A matching algorithm compares new templates with others held in the biometric system's data storage facility.
- A decision process uses matching event results.

There are several types of biometrics identification schemes:

- Face: The facial characteristics are analyses by Biometrics.
- Hand geometry: The analysis of the shape of the hand and the length of the fingers.
- Retina: The analysis of the capillary vessels located as the back of the eye.
- Finger print: An individual's unique finger prints are analyses.
- Vein: The analysis of pattern of veins in the back if the hand and the wrist.
- Iris: The analysis of the colored ring that surrounds the eye's pupil.

- Verification: In a biometric security system, the process of comparing a biometric sample beside a single reference templates of the specific user in order to confirm the identity of the person trying to gain access to an organization.
- Signature: The analysis of the way a person signs his name.
- Voice: The analysis of the quality, pitch, tempo and frequency of a person's voice.

Biometric Working Process

In biometric security system the administrators access the biometric data during the enrollment, capture, extraction, comparisons and matching stages of the process. The biometric engine is a software program that works in conjunction with the hardware devices that a biometric system uses.

Biometric Accuracy

The accuracy used to describe how accurate a biometric system performs. Biometric accuracy is based on several verifying criteria including the identification rate,error rate, false acceptance rate, False alarm rate and additional biometric system standards.

Performance Metrics for Biometric Systems

The different performance metrics for evaluating the biometric system are as follows

FAR (False Acceptance Rate): The FAR is defined as the likelihood that a user creation a false claim about his/her identity will be verified as that false identity. FAR is the strength of the corresponding algorithm. The stronger algorithm is less likely that a false authentication will happen.

Crossover Error Rate (CER): A lower value for the CER is desired for a biometric system in order to be considered more convenient as well as accurate for its users. The rate at which both accept and reject errors will be same.

FRR (False Rejection Rate): The FRR is defined as the probability that a user making a true claim about his/her identity will be rejected as him/her self. The strength of the FRR is the robustness of the algorithm. The more accurate the matching algorithm, the less likely a false rejection will happen.

Failure to Capture Rate (FCR): A ppropriate for automated systems, the likelihood that the system fails to detect a biometric input when presented correctly.

Template Capacity: The number of single users that can be represented by its contents.

Failure to Enroll Rate (FER): The rate at which attempts to create a template from an input is not successful. This is most commonly caused by low quality inputs that are inadequately characteristic biometric samples or from a system design that makes it difficult to provide consistent biometric data.

Tradeoff: Larger the FER, inferior the FAR and FRR; and vice-versa.

Unipolar biometric System

Unimodal biometric which uses only one biometric data such as finger print or face or palm print or iris. Unimodal authentication suffers from the following problems:

1. Noisy sensor data
2. Non Universality
3. Lack of individuality
4. Lack ofinvariant representation
5. Susceptibility to the circumvention

Unimodal biometric limit

- Iris recognition affects from some problems like camera, distance, eyelids and eyelashes occlusion, lenses and reflections.
- Fake faces from mobiles may assault system.
- Face identification changes over ages and unbalanced, twins may have similar face features.

- Finger print may have some cuts, burns and small injuries transitory or permanent.
- DNA-More expensive several hours to be obtained.
- Fake fingers made from gelatins and/or silicon have skill to attack the finger print based on identification system.

Bipolar biometric system

Bimodal biometric which uses any two biometric data such as finger print, face or face, palm print or iris, face and so on.

Multipolar biometric system

While every user is predictable to possess the biometric identifier being acquired, in reality, it is possible for a subset of the users to be not able to give a particular biometric. An impostor may attempt to burlesque the biometric identifier of a legitimate enrolled user in order to get around the system. So multimodal biometric system having more advantage when compared to unimodal system. A Multi-biometric system could address the problem of non-universality, since multiple biometric identifiers would ensure sufficient inhabitants coverage. Provide anti-spoofing actions by making it difficult for an intruder to at the same time burlesque the multiple biometric identifiers of a legitimate user. Ensure a "live" user is present at the point of data acquisition by asking the user to present a random subset of the multiple biometric identifiers. Overall, multi- biometric systems could smooth the progress of a challenge-response kind of confirmation. It is the usage of multiple biometric indicators by personal identification systems for identifying this individual.Multibiometric authentication can be achieved in different ways like:

1. Multi algorithm system-More than one algorithm is used for comparing the biometric traits.
2. Multi sensor system
3. Multi instance system-Multiple instances used for the traits.
4. Multimodal system-Multiple biometric data is used.

Fusion Techniques

Biometric fusion is the use of multiple biometric inputs or methods of processing to improve performance. The key purposes for biometric fusion are to improve system accuracy, efficiency, applicability, and robustness.

i) Prematching Fusion Techniques

- ***Sensor level Fusion:***
  - Integration of information can be either at the sensor level or at the feature level. The raw data from the sensor are combined in sensor level fusion.
  - For example the face images obtained from the different sensors must be compatible and this may not always be possible (eg.) it may not be possible to fuse face images obtained from camera with different resolution.
- ***Feature level Fusion:***
  - Refers to combining different feature vectors that are obtained by either using multiple sensors that are obtained by either using multiple sensor or employing multiple feature algorithm on the same sensor data. Feature vector may be homogenous (Finger print impression of a axis finger) or heterogeneous (different like face and hand geometry).

The feature sets extracted from each biometric identifier sources can be fused to generate another feature set to represent the individual

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

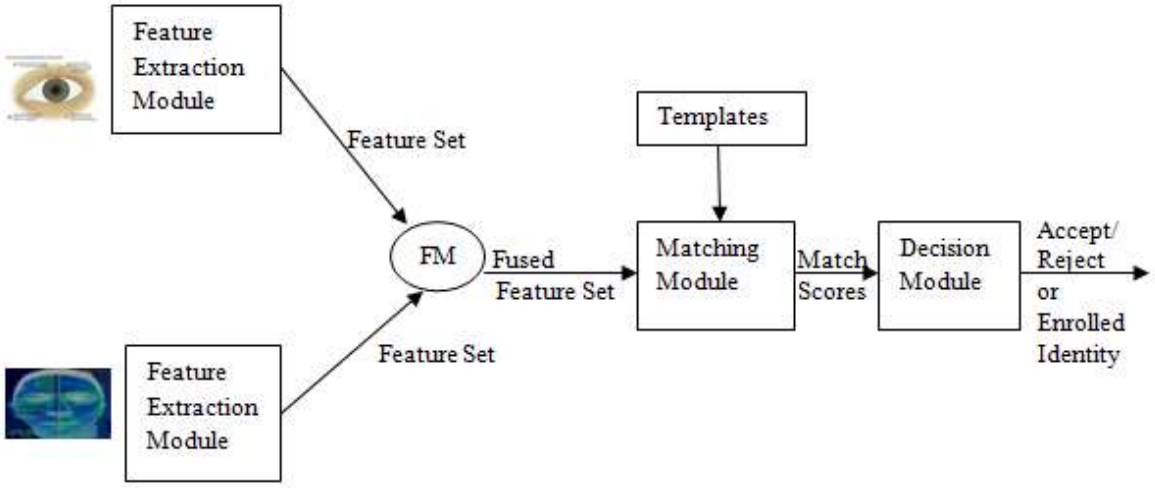

Figure 1. Bimodal representations for Feature level fusion

ii) Post matching fusion Techniques

- ***Decision Level Fusion:(Abstract level Fusion)***
  - It provide the result of matching in the form of whether the user is genuine or imposter with decision level fusion, there are different rules that can be used to authenticate the user.
- ***Rank level Fusion :***
  - We have to compare the template only with one template in the database, here we have to generate rank of identities in stored order with all modalities. Then after with the help of one method of fusion, we have to fuse the ranking for each person available for different modalities.
  - The identify with lowest score is identified as the correct person. This method provide more accuracy with compare to just an identifying best match with one modality. This contains different training set, different architectures. It uses different number of larger or transfer K-nearest neighbor, neural network, support vector machine, decision tree etc.
- **Score Level Fusion Techniques:**
  - Match score is a measurement of the relation between the template biometric and input biometric feature vectors. Based on the resemblance of feature vector and the template, each and every subsystem calculates its own match score value. These individual scores are finally combined to obtain a total score, which is then passed to the decision module and score normalization, after which acceptance is performed.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

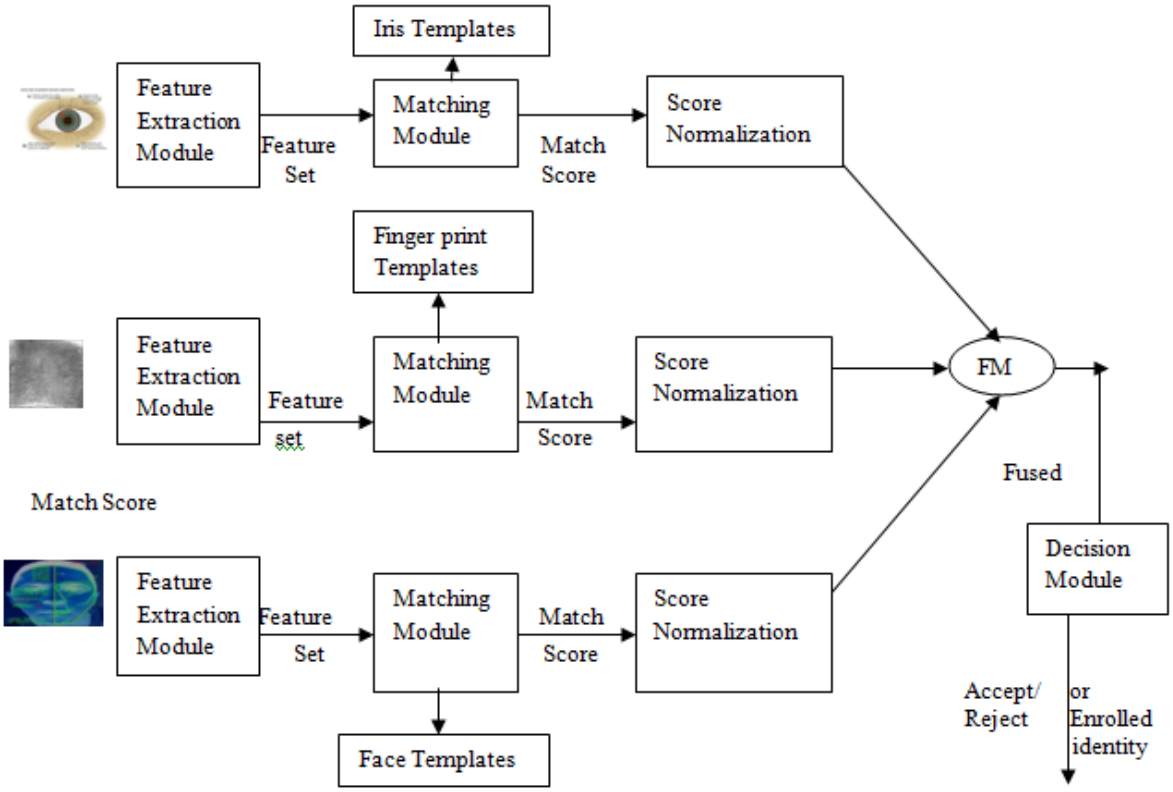

Figure 2. Multimodal representations for score level fusion

II. CONCLUSION

In this paper we discussed about multimodal biometric, various fusion techniques that are involved in bipolar and multipolar biometric fusion process. It increases the overall system accuracy and hence increases security, as well as reduces the enrollment problems. An effective and appropriate fusion strategy is needed to integrate different biometric information in such multimodal systems. It also provides an in-depth overview of traditional multimodal biometric systems.

III. FUTURE WORK

In the multimodal biometric system will be created by using different multi biometric data like two irises and ear. Because ear can not affected by the age. Iris is easy to capture as compared to traits like retina..

IV. REFERENCES

[1] Mamta Devi, Gurrmeetkaur, Dr.Chander Kant "A Novel approach to improve the biometric security using Liveness Detection" International Journal of Advanced Research in computer science, Vol 8,No.5,May 2017.
[2] Omprakash Kaiwartya "An Investigation on Biometric Internet Security" International Journal of Network security, Vol 19,No.2,March 2017.
[3] B.Shanthini,S.Swamynathan,"Nternational conference on Information and knowledge Management", IPCSIT ,Vol 45.
[4] Rupesh Wagh,Saurabh Darokar, Shubham Khobragade,Multimodal Biometrics Features with Fusion level Encryption, International Journal of Engineering science and computing, IESC,Vol 7,No 3,Mar 2017.
[5] Yakhita Jain and Mamta Junija,"A Review on Iris and Palm print based unimodal Biometric system", IJCTA,2016.
[6] E.Sujatha,A.Chilambuchdvan,"Neural Network based Normalized Fusion Approaches for optimized multimodal biometric authentication algorithm", circuits &systems scientific Research publishing,2016.

[7] Neelam Thapa, Dr.Vinayak Bharadi ,"Multimodal Fusion of Iris And signature using WLD based Feature Extraction" ,ISOR Journal of Computer Engineering, 2017.
[8] Subha Barman ,Debasis semanta and Samiran Chattopadhaya,"Finger print based crypto biometric system for network security", Journal of information security-2015.
[9] George chellin chandran, Dr.Rajesh.R.S, "Performance Analysis of multimodal Biometric system Authentication", International journal of computer science and network security, Vol 9,March 2009.
[10] Lavinia Mihacla, Gerhard Hancke, "User centric key Entropy: Study of biometric key Derivation Subject to spoofing attacks",MDPI,2017.
[11]]Waheeda Almayyan, "Performance Analysis of multimodal Biometric fusion",2012
[12] Yakshita Jain and Mamta Juneja,"A Review on Iris and palm print based unimodal and multimodal biometric syayem",IJCTA,2016

CITE AN ARTICLE

Selvi, M. T., Mrs, & Sumathi, A., Mr. (2017). FUSION TECHNIQUES FOR BIMODAL AND MULTIMODAL BIOMETRIC SYSTEM AUTHENTICATION. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(9), 40-45. Retrieved September 5, 2017.