A Multimodal Biometric System for Secure Identification

Ahmad Tasnim Siddiqui
Research Scholar OPJS University,
Churu, Rajasthan, India
Email: tasnim5@yahoo.com

Dr. Vaibhav Bansal
Associate Professor - CSE
OPJS University,
Churu, Rajasthan, India

Abstract: **A biometric system is a methodological system that uses information about a person to recognize that person. Biometric systems focusing completely on the identification of humans have become the major kind of biometric system in today's IT word. Biometrics machines have different techniques to do the verification first is the physical verification in which fingerprint recognitions, face recognition, retina recognition etc. have done second one is the behavioral recognition in which voice recognition, signature recognition have done. Unimodal biometrics systems have lots of problem for e.g. noisy sensor data, lack of invariant representation etc. These problems lead to the use of multi-modal biometrics. In this paper our objective is to provide overview of multimodal biometric and to provide security of biometrics template stored in the database.**

Keywords: **Biometric system, physical characteristics based techniques, behavioural characteristics based techniques, fingerprint recognition, sensor module.**

I. INTRODUCTION

1.1 Definition of biometric system:

Biometrics is the science of establishing the identity of an individual depend on the physical, chemical or behavioral attributes of the person. Biometric systems are more convenient than traditional authentication techniques since there is no password to be forgotten or smart card to be lost [3].Biometric-based verification systems represent a valid alternative to conventional approaches [1]. In the subscription process, user's initial biometric sample(s) are collected, assessed, processed, and stored for ongoing use in a biometric system. In verification mode (1:1 matching process) the user claims an identity and the system verifies whether the claimant is accurate or fraud. If the user's input and the template of the claimed identity have a high degree of similarity, then the claim is accepted as correct. Otherwise, the claim is rejected and the user is considered as "fraud". In Identification mode (1:N matching process) the user's input is compared with the templates of all the persons registered in the database and the identity of the person whose template has the highest degree of similarity with the user's input is the biometric system's output. If the highest similarity between the input and all the templates is less than a fixed minimum threshold, system rejects the input, which implies that the user presenting the input is not one among the enrolled users [4].

1.2 Category of Biometrics Technique

Biometric techniques can be divided into two categories i.e physical characteristics and behavioral characteristics based methods.

(i) Physical Characteristics Based Techniques

Biometric techniques based on physical characteristics of human being such as hand geometry, fingerprint, palm-print etc. are called physical features based techniques. Following are examples of biometric techniques based on physical features.

- Hand geometry recognition
- Face recognition
- Vein pattern recognition
- Retina recognition
- Iris recognition
- Fingerprint recognition

(ii) Behavioural Characteristics Based Techniques

Biometric techniques which are depend on the behavior of human being like as voice, signature, gait, keystroke etc. are called behavioral characteristics based techniques. Following are examples of biometric methods based on behavioral characteristics.

- Voice recognition
- Signature recognition
- Keystroke dynamics

- Gait recognition

1.3 Modules of Biometric System

The biometric system consists of following four modules:

- Sensor module
- Feature Extraction
- Matcher
- System database

Sensor module: It captures the biometric data of personal. Fingerprint sensor is example of sensor module,it captures the ridge and valley structure of user finger.

Feature extraction: In this module captured biometric data is processed and set of features are extracted.

Matcher module: In this module to produce matching score during recognition, features are compared against the stored templates.

System database module: This module stores the templates of users. It stores the multiple templates of user to account for deviations observed in biometric data & templates in database are updated over time [4].

1.4 Biometric Technologies

1.4.1 Fingerprint Identification

Fingerprint identification is the method of identification using the perception made by the minute ridge formations or patterns found on the fingertips. No two persons have exactly the same compromise of ridge patterns (even identical twins), and the patterns of any one individual remain unchanged throughout life.

1.4.2 Hand Geometry

When measuring hand geometry biometrics, three-dimensional image of the hand is occupy and the shape and length of fingers and knuckles are measured. Hand geometry has been in use for many years in many applications, predominantly for access control. The technology does not achieve the highest levels of accuracy but it is appropriate and fast use. On the capture process a user places a hand on the reader, aligning fingers with especially situated guides. Cameras, positioned on above and on the side of hand capture images from which measurements are taken at selected points.

1.4.3 Face Recognition

Face recognition technologies analyze the unique shape, pattern and positioning of facial attributes. The face is natural biometric because it is a key component in the way we humans recollect and recognize each other. Face recognition is very typical technology and largely software based. Artificial intelligence is used to duplicate human interpretation of faces. The problem with human face is that people do change over time; wrinkles, beard, glasses and location of the head can affect the performance considerably. To increase the accuracy and adjust to these changes some kind of machine learning has to be executed. There are essentially two methods of capture: employ video or thermal imaging. Video is more frequent as standard video cameras can be used. The precise position and angle of the head and neighboring lightning conditions may affect the system's performance.

1.4.4 Finger Geometry

Finger geometry biometric is very closely linked to hand geometry. The use of just one or two fingers means more concentrated, smaller devices and even higher throughput. Two variations of capture processes are used, first being similar to hand geometry defined above. The second technique requires the user to insert a finger into a burrow so that three-dimensional measurements of the finger can be prepared.

1.4.5 Palm Scanning

Palm biometrics is close to finger scanning and in specific AFIS technology. Ridges, valleys and other minutiae data are found on the palm as with finger images. Main charm in palm biometrics industry is law enforcement as latent images - "palm prints" – formed from the crime scenes is equally useful as latent fingerprints.

1.4.6 Signature

Signature is one of the most accepted methods of asserting ones identity. As we generally use it the signature is scrutinized as a static trace of pen on the paper. In computerize form the static geometry of signature is not adequate to ensure the uniqueness of its author. Signature biometrics often mentioned to dynamic signature verification (DSV) and look at the way we sign our names. Examples of these behavioral features are the angle of the pen is held, the time taken to sign, velocity and speeding up of the tip of the pen, number of times the pen is uplifted from the paper. Signature data can be catched using a special sensitive tablet or pen, or both. On some easier cases equipment found relatively cheap from normal computer stores can be used. This measures the sound that a pen makes versus paper. Because of the behavioral temper of signature, more than one signature register is needed so that the system can build a profile of the signing properties [5].

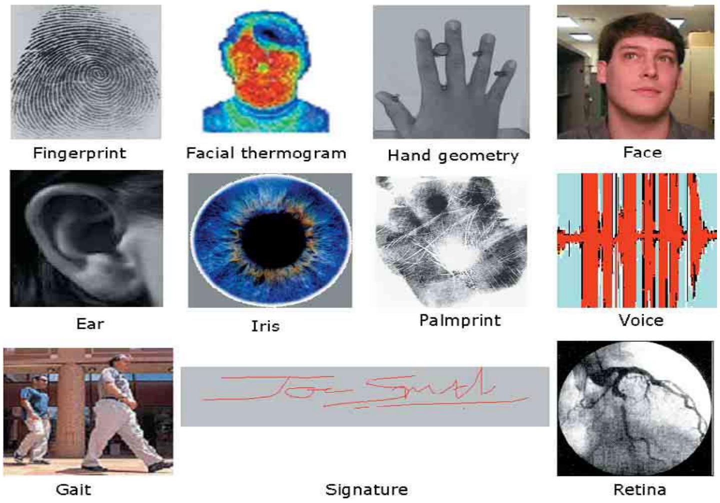

Figure 1.1: Examples of some of the biometric traits used for validating an individual

1.5 Architecture of a Biometric System

Basically speaking, there are two phases in a biometric system (see Fig 1.2.): a learning phase (enrolment) and a recognition phase (verification). The recognition module permits a decision to be taken. In identification mode, the system relates. The measured signal with the lotsof models occupied in the data base and selects the model most closely related to the signal. And In verification mode, the system will collate the measured signal with just one of the data base models and then sanction the person or refuse him. Identification may be a very difficult task if the data base occupied thousands of individuals. Access time problems then become crucial [6].

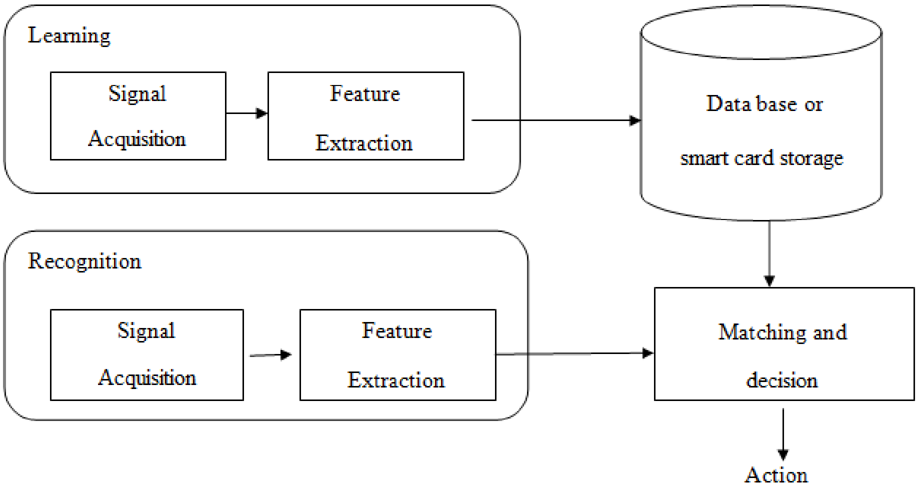

Figure 1.2: The various modules of a biometric system

1.5.1 Different Problems with Different Scopes and Challenges

We refer to identify three various ways of using a biometric system:

1. Positive Identification

Biometrics can check with high confidence the authenticity of a requested enrolment based on the input biometric sample. business applications such as computer network login, electronic data safety, ATMs, credit card shopping, physical access control, cellular phones, PDAs, medical records arrangements, and distance learning are sample validation applications.

2. Large Scale Identification

Mentioned an input biometric sample, a large-scale recognition dictates if the pattern is associated with any of a bulk numbers (e.g., millions) of enrolled identities. Classic large-scale identification applications comprises welfare- payment, national ID cards, border control, driver's license, criminal investigation, voter ID cards, body identification, parenthood confirmation, missing children recognition etc.

(iii) Screening

Screening applications secretly and unobtrusively decide whether a person belongs to a check-list of identities. Examples of screening applications could consist of airport security, safety at public events, and other surveillance applications. The screening watch list consists of an average (e.g., a few hundred) number of identities.

II. RELATED WORK

The research work performed in this field by different researchers is presented as follows:

Kankrale R.N. et al [1] author aims at combining two biometric features namely iris and fingerprint at decision level using Fuzzy logic. Multimodal biometric identification system to combine two or more physical traits to minimize False Accept Rate (FAR) and FRR (False Reject Rate) in more detail, fuzzy logic based approach at decision level is used for concatenation and every biometric result is weighted for engaged in final decision. Fuzzy logic is used for the effect of each biometric result integration. The proposed multimodal system attains interesting results with several commonly used databases. For example, the author had produced an interesting working point with FAR = 0% and FRR=3.43% using entire CASIA Fingerprint and a unplanned separated same size subset of the CASIA Iris database.

Mohamad Abdolahi et al. [2] Single biometric systems have a lots of problems like as noisy data, non-universality, spoof attacks and unacceptable error rate. These restrictions can be resolved by positioned multimodal biometric systems. Multimodal biometric systems utilize two or more individual procedures like face, iris, retina and fingerprint. Multimodal biometric systems improve the identification accuracy more than uni-modal methods. The author uses, two unimodal biometrics, iris and fingerprint are used as multi-biometrics and display applying this biometrics has good result with high accuracy. Decision level is used for fusion and every biometric result is weighted for to take part in final decision. Fuzzy logic is used for the effect of each biometric result combination.

N. Radha et al. [3] Authentication of users is an essential and difficult to achieve in all systems. Disclosed secrets like PIN i.e.Personal Identification Numbers or Passwords and key devices such as Smart cards are not presently appropriate in certain situations. The biometric refines the capability to recognize the persons. A biometric identification system is an self-directing recognition system that recognizes a person based on the physiological features (e.g., fingerprints, face, retina, iris, ear) or behavioral features (e.g., gait, signature, voice) characteristics. In many real-world programs, uni-modal biometric systems often face has remarkable limitations due to sensitivity to noise, intra class inconstancy, data quality, non-generalization and other factors. Multimodal biometric systems overcome some of these limitations. Multimodal biometric system assigns more accuracy when related to uni-modal biometric system. The main goal of multimodal biometric system is to develop the safety system for the areas that require high level of security.

Taruna Panchal and Ajit Singh [6]. They concluded that the biometric template is much more secure than before as there was just little change in biometric template using parity check method used in watermarking technique. The modified data is encrypted and hence while decryption real data is not exposed which also overcomes encryption disadvantage. It provides good security and is suitable for any large scale data. In future, these techniques can be applied to different attack areas to protect attacking on these areas.

III. PROPOSED WORK

1.1 Problem Formulation

Uni-modal biometric system performs person identification based on a single source of biometric statistics. Such systems are often affected by the following problems:

- Noisy sensor data
- Non- universality
- Lack of individuality
- Susceptibility to circumvention
- Lack of invariant representation

Such factors lead to the usage of multimodal biometric for identifying humans. Combining the evidence obtained from various modalities using an effective fusion scheme can appreciably improve the overall accuracy of the biometric system. Multimodal biometric system can reduce the FTE/FTC rates and provide more resistance versus spoofing because it is difficult to concurrently spoof multiple biometric sources [7].Multimodal biometrics system has lots of advantage as follows [8]:

- Its makes better system operations.
- Its accuracy is better as contrast to the uni-biometric system.
- It prevent from stolen the templates of biometric system as at the time it stock the two characteristics of biometric system in the database.

IV. PLANNING OF WORK

Our main focus is to enhance the technique of feature extraction of both the characteristics. This enhancement is done through feature level extraction and fusion is done through fuzzy logic. Then the fused vector is encrypted using different security technology. Our planning includes the step by step approach as given:

Step 1: Fingerprint and Iris biometric sample will be recorded using different sensors.

Step 2: Features will be extracted differently from both the biometrics.

Step 3: Fusion of both extracted attributes will take place at this level (i.e fusion at feature extraction level) using neural network or fuzzy tomb or genetic algorithm. The feature sets originating from multiple biometric algorithms will integrate into a single feature set by the application of appropriate feature normalization, transformation and reduction schemes.

Step 4: Generated template will be stored in the database.

Step 5: Above stored template will be protected through Cancellable Biometric.

Step 6: Security will forby increase by encrypting the template using cryptography.

4.1 Tool Used

4.1.1 MATLAB

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment, a high-level language and interactive environment, and fourth-generation programming language for numerical computation, visualization, and programming. MATLAB provides built-in 2-D and 3-D plotting functions, as well as volume visualization functions. You can automatically produce a report when you execute a MATLAB program. The report contains your code, comments, and program results containing plots. Reports can be published in a variety of formats, such as HTML, PDF, Word, or Latex.

4.1.2 Fuzzy logic

These are used for the fusion of two feature extracted templates. Fuzzy logic enables us to process the information in a same way like human thinking, i.e. big against small or high against low. It makes intermediate values to be explained between true and false by partial set memberships [9].

4.2 Methodology

4.3.1 Fingerprint Recognition

A fingerprint is collection of ridges and furrows which are parallel and have same width [2].

4.3.2 Iris recognition

Iris is a circular diaphragm which is placed between cornea and lens of the human eye. The function of iris is to control the amount of light entering through the pupil.

V. CONCLUSION AND FUTURE SCOPE

For generations, many highly safe environments have used biometric technology for entry access. These days, biometric systems are predominantly utilized for validation, but the unimodal biometric system has some problem like noisy sensor data, non-generalization, lack of individuality, lack of invariant representation and susceptibility to circumvention. So for removing these disadvantages, multi-modal biometric system are used. Multi biometrics is a new technique used to accurate verification of the person. This paper gives a multimodal biometrics combining fingerprint and iris with feature extraction level and fusion is finished by fuzzy logic. In future, the working system using MATLAB can be developed to provide efficient security system by using iris and fingerprint traits. Many types of filters can be used for extraction. And in encryption many techniques can be used like DES etc. More filters can be used to increase the extraction of images of fingerprint and iris and can be fused using any other techniques.

REFERENCES

[1] Kankrale R.N., Jawale M.A, “Fuzzy Logic Concatenation in Fingerprint and Iris Multimodal Biometric Identification System”, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, October 2013.

[2] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari, “Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

[3] TarunaPanchal and Ajit Singh, “Multimodal Biometric System”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[4] Shweta Malhotra and Chander Kant “A Novel approach for securing biometric template”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[5] K P Tripathi, “A Comparative Study of Biometric Technologies with Reference to Human Interface”, International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011

[6] Bernadette Dorizzi, “Biometrics at the frontiers, assessing the impact on Society Technical impact of Biometrics”, Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission, January 2005

[7] Ajay Kumar, Vivek Kanhangad, David Zhang “A New Framework for Adaptive Multimodal Biometrics Management” IEEE Transactions on Information Forensics and Security vol. 5, pp. 92-102, Mar. 2010

[8] K.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna & K. Kailasa Rao, “Multimodal Biometric Systems – Study To Improve Accuracy and Performance”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010

[9] V. Conti, G. Milici, P. Ribino, S. Vitabile, and F. Sorbello, “Fuzzy fusion in multimodal biometric systems”,‖ in Proc. 11th LNAI Int. Conf. Knowledge.-Based Intell. Inf. Eng. Syst. (KES 2007/WIRN 2007), Part I LNAI 4692. B. Apolloni et al., Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 108–115.