A Study on Unimodal and Multimodal Biometrics for a Person Identification

J. Rama
Department of Electronics and Communication Engg.,
Sri Krishna College of Technology
Coimbatore, India.

P. Malathi
Principal
Bharathiyar Institute of Engineering for Women
Salem, India.

Abstract—Biometrics is a science of recognizing a person based on his/her physiological or behavioral characteristics. So it plays an important role in identification and authenticating a person for immigration, physical, Forensic and Computer society. We can identify a person by using his/her any one or more than one of the characteristic traits and extract the feature set from the acquired data, and comparing with the template stored in the database. If we consider a single trait, Unimodal and more than one it is called Multimodal. Unimodal have some disadvantages so we can go for multimodal biometric system. In order to increase the complexity to the imposter and to the accuracy, we can go for Multimodal biometrics. This paper describes the overview of multimodal biometric system.

Keywords—Unimodal, multimodal, fusion

1. INTRODUCTION

Biometrics generally used alternatively to describe characteristics of a person. Characteristics defines a measurable physiological (face, fingerprints, palm prints, hand geometry, ear) and behavioral (Speech, gait, key stroke, signature) characteristics. These are essential to identify a person. A biometric system is a Pattern Recognition system, which acquires required data, extract the feature set from it, and compare it with the template set stored in the database. Unimodal biometric system uses a single biometric traits of a person and it cannot gives us perfect identification. To overcome this disadvantage, multimodal biometric system was used. In this method, two or more biometric traits are used to identify the person and also for authenticating. The rest of the paper is organized as follows: section 2 presents overview of Biometrics, section 3 presents performance measure of a biometric system, section 4 presents multimodal system, section 5 presents different levels of fusion in multimodal system, section 6 provides application of biometrics and section 7 gives the conclusion.

2. Overview of Biometrics

Biometrics is a science of establishing the identity of an individual based on physical, chemical or behavioral attributes of the person. Problems behind the automatic person recognition attracting more and more scientists to do this project. Since it is a Pattern recognition system, we can operate in either verification mode or identification mode. (M. Golfarelli, D. Maio, and D. Maltoni, July et al., 1997).

In the verification mode, the system validates a person’s identity by comparing the acquired data with his own biometric templates stored in the database. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity (A. Ross and A. K. Jain et al, 2003).

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual’s identity (S. Prabhakar and A. K. Jain et al, 2002). Identification is a critical component in negative recognition applications where the system establishes whether the person is who he denies to be.

A simple biometric system comprises of the following four components as shown in the figure:
(1) **Sensor Module**: This module acquires the data of a person. For example, if camera is a sensor unit, it captures the face of an individual.

(2) **Feature Extraction Module**: The acquired data is preprocessed to extract the feature sets. For example, the position and location of eyes, nose and lengths of mouth and nose would be extracted in the feature extraction module of a face system.

(3) **Matching Module**: In this module feature values are compared with the template by generating a matching score.

(4) **Decision-making Module**: In this, users identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the previous module.

3. **Biometric Testing and Evaluation metrics**

Performance testing comprises a critical aspect of biometric modality assessments. Investigators are able to draw from a wide range of performance evaluation metrics that assess functional system accuracy and usability.

Jain et al suggest that a useful biometric system will possess seven specific qualities:
- **Universality**: each potential user possesses the modality
- **Uniqueness**: the modality adequately differentiates between any two users
- **Permanence**: the modality profile remains relatively constant over time
- **Collectability**: the modality samples are easy to detect and acquire
- **Performance**: the modality is robust and functional within a range of operational and environmental factors
- **Acceptability**: the extent to which users are willing to accept and use the modality
- **Circumvention**: how susceptible the modality is to spoof attacks and identity fraud

Of these seven fundamental characteristics, uniqueness and permanence are most integral to biometric performance evaluations.

### A. Common Performance Metrics

Performance metrics commonly take the form of rates: for each metric, it is important to note that the measured / observed rate noted in any evaluation is distinct from the predicted / expected rate that occurs in biometric system.

#### (i) **Failure to Enroll Rate (FTE)**

The Failure to Enroll rate (FTE) describes the proportion of enrollment transactions in which zero persons are successfully enrolled into a biometric system. FTE can apply to overall enrollment or to the enrollment of specific biometric instances.

#### (ii) **False Accept Rate (FAR)**

The False Accept Rate (FAR) describes the proportion of identification or verification transactions in which an imposter person was incorrectly matched to a genuine user template stored in a biometric system. FAR reflects the ability of a non-authorized user to access a system, whether zero-effort access attempts or deliberate spoofing or other methods of circumvention.

\[
FAR = \frac{Number\ of\ False\ Acceptance}{Total\ number\ of\ Attempts}
\]

#### (iii) **False Reject Rate (FRR)**

The False Reject Rate (FRR) describes the proportion of identification or verification transactions in which a genuine person is incorrectly rejected from a biometric system. FRR may occur as a result of user presentation error.

\[
FRR = \frac{Number\ of\ False\ Rejection}{Total\ number\ of\ Attempts}
\]

#### (iv) **Equal Error Rate (EER)**

The Equal Error Rate (EER) describes the point at which genuine and imposter error rates are closest to zero. EER can be represented as a percentage with time/unit factors. EER is not useful in assessing actual system performance, but can be helpful as a first-order performance indicator for 1:1 verification systems.

\[
EER \leftrightarrow FAR = FRR
\]

4. **Multimodal Biometric System**

The Multimodal biometric systems are providing identification and human security over last few decades. Due to this reason MBS are adapted to many fields of applications. Some of these multimodal systems are human computer dialog interaction based systems where the user interacts with the PC through voice or vision or any other pointing device in order to complete a specific task. Multimodal biometric systems are those which utilize, or are capable of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification. A biometric system is essentially a pattern recognition system. This system measure and analyzes human body Physiological characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial...
patterns and hand measurements for authentication purposes or behavioural characteristics. The biometric identifiers cannot be misplaced. In spite of inherent advantages, unimodal biometric solutions also have limitations in terms of accuracy, enrolment rates, and susceptibility to spoofing. This limitation occurs in several application domains, example is face recognition. The accuracy of face recognition is affected by illumination and facial expressions. The biometric system cannot eliminate spoof attacks.

The figure shows the block diagram of multimodal biometric system.

![Block diagram of Multimodal Biometric System](image)

This system contains four modules. They are
1. Sensor modules
2. Feature Extraction Modules
3. Matching Module
4. Decision-making module

### 5. Fusion in multimodal biometric system

A mechanism that combines the feature sets from each biometric channel is called biometric fusion.

Fusion can be used to address a number of issues faced by the designers, implementers and operators of biometric systems:

- **Accuracy**: to improve overall accuracy
- **Efficiency**
- **Robustness**
- **Applicability**
- **Universality**

#### 5.1 Levels of Fusion

According to Jain and Rose, there are various levels of fusing the biometric traits in different levels to increase the strength. They are: Sensor level fusion, feature level fusion, score level fusion and decision level fusion.

---

**Fig. 2. Block diagram of Multimodal Biometric System**

**Fig. 3. Fusion levels in multimodal biometric system**

5.1.1 **Sensor level fusion**

We combine the biometric traits taken from different sensors to make a composite biometric trait and process.

5.1.2 **Feature level fusion**

In the feature level fusion, signals from different biometric traits are first processed and feature vectors are extracted separately from each biometric trait. After that these feature vectors are combined to form a composite feature vector which is further used for classification. In case of feature level fusion some reduction techniques must be used in order to select only useful features. Some of the researchers have applied fusion at feature level. Since features contain richer information of biometric trait than matching score or decision of matcher, fusion at feature level is expected to provide better recognition results but it has also observed that when features of different modalities are compatible with each other then fusion at feature level achieves more accuracy.

**Fig 4. Fusion at Feature level**

5.1.3 **Matching level Fusion**

In this level, rather than combining feature vectors, they are processed separately and individual matching score is found and finally these matching scores are combined to make classification. Various techniques such as logistic regression, highest rank, Borda count and weighted sum, weighted product, Bayes rule, mean fusion, Linear Discriminant Analysis [LDA] fusion, k-nearest neighbour [KNN] fusion, and hidden Markov model [HMM] etc may be used to combine match scores. One important aspect has to be addressed in the matching score level is the normalization of scores obtained from multiple modalities [6]. Min-max, z-score, median-MAD, double-sigmoid, tan-h, and piecewise linear these various normalization techniques can be used for normalization of the match scores. Matching score level is the most widely used fusion level due its less complexity.
5.1.4 Decision level Fusion

In decision level fusion each modality is first pre-classified independently i.e. each biometric trait is captured then features are extracted from that captured trait, based on that extracted features these traits are classified like accept or reject. The final classification is based on fusion of the outputs of different modalities.

6. Application

Computer society with network infrastructure has become essential to functions of web based business and government. So securing access to these systems and ensuring one’s identity is essential. Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly.

The defense and intelligence communities require automated methods capable of rapidly determining an individual’s true identity as well as any previously used identities and past activities, over a geospatial continuum from set of acquired data. A homeland security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment. Key applications include border management, interface for criminal and civil applications, and first responder verification.

7. Conclusion

Nowadays Automatic person identification is an important task in our life. The traditional method of establishing a person’s identity include knowledge based like password or token based like ID cards, but representation of these identity can easily be lost, stolen or shared. Therefore they are not sufficient for identity verification. Hence biometric systems are to overcome the limitations of traditional methods. Therefore in this paper Unimodal and multimodal biometric systems are discussed. By combining multiple sources of information, the improvement in the performance of biometric system is attained. Various fusion levels of multimodal systems are discussed. Fusion at the match score level is the most popular due to the ease in accessing and consolidating matching scores.

References


J. Rama received her Bachelor’s degree in Electronics and Communication Engineering from Manonmanium Sundaranar University, Tirunelveli, India and Master’s degree from Madras Institute of Technology, Anna University, Chennai, India. She is working as Assistant Professor in Sri Krishna college of Technology, Coimbatore, India. Her research are Biometrics, Image Processing and Pattern Recognition.