Chapter 6
Verification of Multimodal Biometric: IRIS, Finger, and Palm Using Different Algorithms

Shashidhara H. R.
JSS Academy of Technical Education, India

Siddesh G. K.
JSS Academy of Technical Education, India

ABSTRACT

Authenticating the identity of an individual has become an important aspect of many organizations. The reasons being to secure authentication process, to perform automated attendance, or to provide bill payments. This need of providing automated authentication has led to concerns in the security and robustness of such biometric systems. Currently, many biometric systems that are organizations are unimodal, which means that use single physical trait to perform authentication. But, these unimodal systems suffer from many drawbacks. These drawbacks can be overcome by designing multimodal systems which use multiple physical traits to perform authentication. They increase reliability and robustness of the systems. In this chapter, analysis and comparison of multimodal biometric systems is proposed for three physical traits like iris, finger, and palm. All these traits are treated independently, and feature of these traits are extracted using two algorithms separately.

INTRODUCTION

Biometric authentication systems are those which used for identifying certain individuals and provide access control to the designated users to perform authentication the biometric systems rely on certain unique characteristics in an individual. These characteristics are provided by certain body parts such as finger, iris and palm etc.
Traditionally user authentication was performed through certain popular documents such as driving license or employee identity card, but these methods are prone to be duplicated. By using unique body characteristics of an individual robust, effective and efficient user authentication can be achieved.

The biometric systems are expected to provide the seven functionalities listed below:

1. The body parts that are chosen for performing authentication should be present in every individual.
2. The body characteristics which will be employed for designing the biometric systems should provide uniqueness property which means that no two individuals should have the same characteristics for the body part.
3. The designated characteristics of the body part remain free from deformities over a long period of time.
4. The characteristics must be easy to acquire and processed in order to come for authentication decision.
5. The authentication procedure always be robust and exhibit good efficiency.
6. The developed biometric systems should be acceptable to the community in-order to be effectively deployed in organizations.
7. The biometric systems should exhibit strict non-circumvention such that the body characteristics that will be used for authentication should not be duplicated by using another substitute.

There are number of performance metrics used to evaluate the efficiency and effectiveness of the biometric systems such as,

1. **False Match Rate (FMR):** It is the ratio of number of false authentication performed to the number of authentication attempted.
2. **False Non-Match Rate (FNMR):** It is the ratio of number of correct authentications which could not be established to the number of authentication attempted.
3. **Receiver Operating Characteristic:** It is the trade-off plot between False Match Rate and the False non-match rate.
4. **Equal Error Rate:** It is the rate in which the False Match Rate and False Non Match rate are equal.
5. **Failure to Enroll Rate:** It is the ratio of number of instances in which template creation was unsuccessful to the total number of template creation attempts.
6. **Failure to Capture Rate:** It is the ratio of number of instances in which the biometric system failed to capture the test image to the total number of biometric login attempted.
7. **Genuine Acceptance Rate (GAR):** It is the ratio of number of test image instances that needed to be authenticated and were authenticated to the total number of authentication instances.

The main issue in today’s biometric system is of effectiveness and efficiency. Effectiveness means the authentication quality provided by the biometric system. The biometric systems need to provide high accuracy in above mentioned performance metrics. Currently many biometric systems have been unable to achieve the desired level of authentication accuracy. Efficiency refers to the response time of the biometric system to provide its decision on the user authentication status. Today large volume of user information is stored in the database. So has to provide good efficiency and still maintaining good effectiveness is an unresolved challenge in designing biometric systems.