Biometric Template Security and Biometric Encryption Using Fuzzy Frameworks

Debanjan Sadhya
IIT-BHU, India

Sanjay Kumar Singh
Indian Institute of Technology (BHU), India

INTRODUCTION

Biometrics refers to the traits or characteristics associated with living beings. These are recently extensively used for verification and authentication purposes and so can be classified as an access control mechanism. The biometric traits can be categorized into two groups namely physiological (fingerprint, face, iris, DNA etc.) and behavioral (gait, voice etc.). The selection of these biometric traits is based upon certain properties associated with individuals, the major being universality, distinctiveness, permanence and collectability as mentioned by Jain et al., (2004). Apart from these, properties like acceptability by the users, the level of security offered and the performance of the system are also critical parameters.

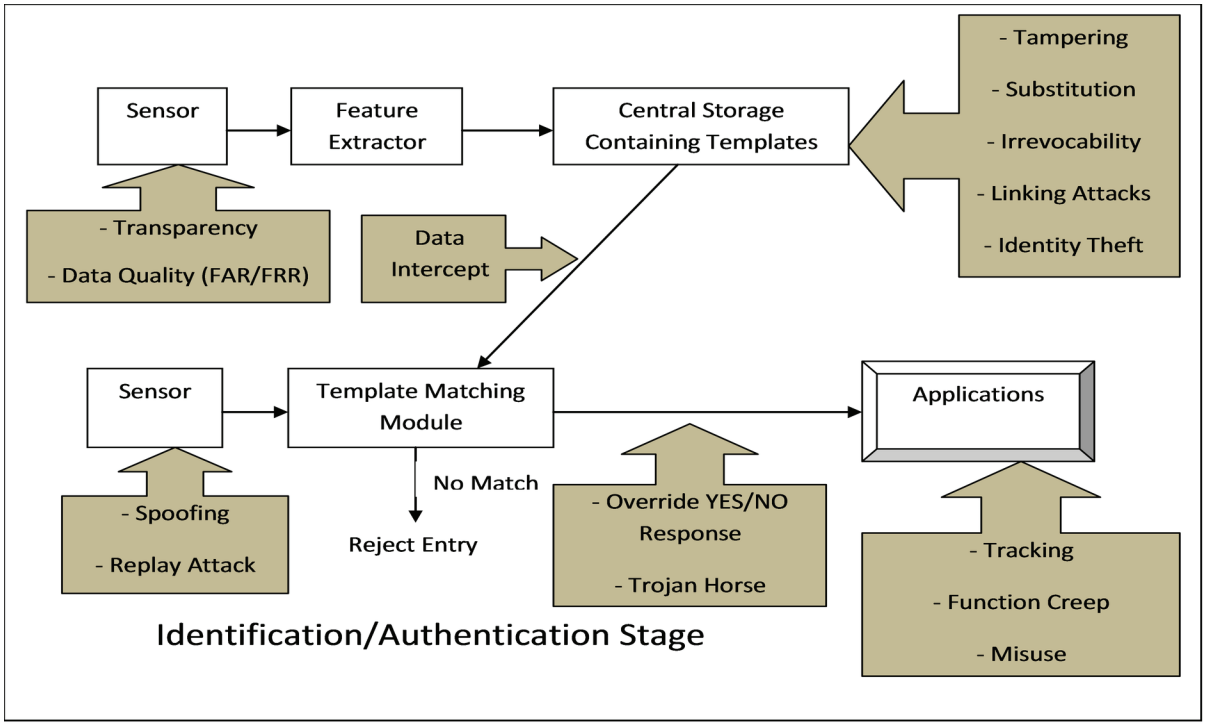
The biometric recognition system gained its popularity as early as the mid 19th century but was not extensively used till now mainly because of the difficulty in collecting the traits itself. But with the advancement of technology this problem was eliminated and in recent years biometric authentication systems is preferred over traditional authentication systems almost everywhere. The previous systems consisted of token, tied to and thereby representing an individual (like username-password, pin number etc.). The main reason for this technological shift was forced due to the lack of security measures associated with the techniques. For example, passwords could be easily forgotten by the users and PIN numbers could be easily lost or stolen from valid users. Both these situations pose significant threat to the users and could easily prove fatal for them. Biometric system overcomes these limitations because the observed characteristic of the human body cannot be lost (except by accident) or be exchanged with another individual. More than that, counterfeiting the biometric characteristics is often a difficult task.

Biometric systems works in two phases namely enrollment phase and identification/authentication phase. In the enrollment phase biometric traits are collected from enrolling individuals and are stored in a database. In the second phase, individuals present their biometric data for either identification or authentication purpose. In identification, the presented biometric data is compared with all other entries in the database for a match, and upon a successful match the associated individual gets accepted as a genuine user and subsequently is granted permission for any application. This process is often referred to as a "one-to-many" match and is used by police to identify criminals on lists, as well as by governments for registration systems such as voting id, driver's license etc as described by Jain et al., (2008). On the other hand, biometric verification or authentication involves a "one-to-one" search. Here a biometric sample presented by a person is compared to a stored sample contained in the database. A successful matching or authentication renders the used as a genuine entity and is granted permissions for any other application.

In spite of all the exciting prospects of using biometrics as an authentication system, there are many security vulnerabilities associated with it. Primarily the attacks on a biometric system include spoofing, replay attacks, substitution attacks, tampering, masquerade attacks and trojan horse attacks. The area in which these attacks work can be summarized in Figure 1.

DOI: 10.4018/978-1-4666-5888-2.ch049

Figure 1. Different types of attacks on biometric systems



An in-depth study of these attacks and other privacy requirements are given by Cavoukian et al., (2007), Snijder (2006) and Jain et al., (2004).

In a nutshell it can be stated that although biometric system was originally designed as an alternative security application in contrast to the conventional ones, the system itself is exposed to various security threats. So, to provide security to biometric systems (more specifically the templates), a number of techniques were proposed. The premium technique that is most widely used and researched upon is called Biometric Encryption. In this article we will understand and analyze this in detail along with the state of the art enhancement s made to it to further enhance its security aspects.

BACKGROUND

The importance of providing security measures to biometric templates is very critical. To cater for these needs different techniques have evolved with time. The most common technique which provides security is the usage of passwords but due to some reasons it cannot be used in this case. Firstly the user has to remember the password each and every time during the authentication/identification phase which undermines the convenience provided to users. Moreover the strength of a password depends on its length, and for a biometric system this security level provided by average length passwords is just not enough. The actual software based techniques which has been developed for providing biometric template security is broadly categorized into three divisions - encryption, biometric cryptosystems and template transformation.

Encryption

In encryption based systems, the biometric template is encrypted using an encryption key during enrolment. During authentication phase the stored data is decrypted using the corresponding decryption key and is matched with the captured query. One of the main limitations of encryption based techniques is insecure key management since the decryption key is exposed to the system during each attempt to authenticate and thus can be easily stolen by the adversary. The advantage,