International Journal For Technological Research In Engineering
Volume 5, Issue 10, June-2018 *ISSN (Online): 2347 - 4718*

BIOMETRIC TEMPLATE SECURITY

Shikha

Abstract: With the rapid increase in number of biometric recognition systems, an attacker's benefit in staging a system compromise is also increasing and thus is the need to ensure system security and reliability. This dissertation grants a thorough analysis of the vulnerabilities of a biometric recognition system with emphasis on the vulnerabilities related to the information stored in biometric systems in the form of biometric templates. To encourage the improvement of techniques to protect biometric templates, we show the use of biometric cryptography in the existing systems. The techniques to safeguard the biometric templates are categorized into two main groups: biometric cryptosystems and template transformation methods. While biometric cryptosystems permit binding a secure key to the biometric data to obtain a so called secure sketch from which no information regarding the biometric data or the key can be retrieved again, cancelable biometric template transformation techniques non-invertibly transform the biometric template with the user's password. To analyze and improve the biometric cryptosystems, we have studied its two main examples: fuzzy vault and the fuzzy commitment. Fuzzy vault is the technique used to secure templates characterized in the form of a finite set of points whereas fuzzy commitment is used for the security of templates represented as binary vectors. A superior security analysis is provided that makes biometric template more secure. A framework to effectively combine multiple biometric representations and efficiently verify an individual is also proposed. Various template transformation techniques proposed in literature are studied and the amount of security they impart is evaluated using a comprehensive set of metrics. First, we analyze the weak points of biometrics and mentioned existing system and make it strong by applying cryptography. The proposed approaches are shown to be very successful in improving the security of biometric devices. We believe that the security analysis presented in this dissertation will streamline the development of new techniques and help in finding a robust solution for protecting biometric data.

I. BODY

To identify a person with a high confidence is a serious issue in various applications, such as access control, passenger clearance, e-banking, etc. The objective of personal authentication is to determine or confirm the identity of individuals such that the right person is found out from the number of suspects, and requested services or facilities are accessed by a legitimate user, etc. A biometric system is basically a pattern recognition system that acquires biometric data from an individual, extracts a salient feature set and compares this feature set against the feature set(s) stored in the database, and takes an action based on the result of the comparison. A number of physical and behavioral body traits can be used for biometric recognition (see Figure 1.2). Examples of physical traits include face, fingerprint, iris, palm print, hand geometry and ear shape. Gait, signature and keystroke dynamics are some of the behavioral characteristics that can be used for person authentication. The basic operations for fingerprint are described as:

Sensor Module

A fingerprint is the representation of the epidermis of a finger. It consists of a pattern of interleaved ridges and valleys. To acquire a fingerprint we require a scanner where the finger is to be pressed against the flat surface.

Optical sensors: It works on frustrated total internal reflection technique. When the finger is placed on the top of the glass prism, the ridges remains in the contact of the prism and the valleys remain at certain distance. When the left side of prism is enlighten through diffused light, the light entering the prism is reflected at the valleys, and are absorbed at the ridges.

Solid State Sensor: All silicon based sensors includes an array of pixels, each pixel being a tiny sensor itself. The user directly touches the surface of the silicon: neither optical components nor external image sensors are needed.

Cancellable biometrics

Cancellable biometrics can be a good approach for privacy enforcement in Semantic Web and its applications because it provides higher privacy to the multiple templates associated with the same biometric data. The cancellable biometrics was introduced [142] to denote biometric templates that are non invertible. Cancellable biometrics requires storage of the transformed version of the biometric template and that's why provides higher privacy levels by allowing multiple templates to be associated with the same biometric data. There are three principal criteria to be fulfilled before a cancellable biometric template can be considered useful :

(i) Diversity: same cancellable template cannot be used in two different applications.

(ii) Reusability: straightforward reissuance and revocation in the event of compromise.

(iii) One-way transformation: non-invertibility of template so that secret biometric data cannot be recovered.

The two methods of cancellable biometrics are:

Biometric Salting

Biometric salting is similar to password salting in cryptography that contains the random bits R which are used as an input factor and are attached with the secret key k. The output is generally stored as hash H(R+k) in the system database. Biometric salting is similar to this but it is used to derive a distorted version of biometric template.

Non invertible Transforms

In Non-invertible type of transformation, a many-to-one

function, f is build to modify an unprocessed biometric image deliberately into a fresh form within the perspective of feature or signal space. The function f act as an mediator in the perspective of template security permitting for template non-invertibility, diversity and reusability. Since f does not have straight interaction with unprocessed biometrics, the main benefit of this approach is that f does not necessitate to be kept top secret from the users.

II. CONCLUSION

Current biometric systems have a number of vulnerabilities and a motivated adversary can undoubtedly cause severe harm to a biometric system as well as the users enrolled in the system. Furthermore, due to the permanent nature of biometrics data its theft and misuse may be irreparable. If someone‘s fingerprints or iris patterns are stolen and are falsely linked to high susceptibility of a dreaded disease, the person may be unable to obtain a medical insurance. Stolen biometric data may devoid a person of any conveniences offered by the biometric systems due to the concern of being easily impersonated using spoof biometrics. The developed technique shows a significant improvement in terms of security as it combines the advantage of cryptography and cancelable biometrics. The system can be used for any biometric trait and can also be successful in multibiometric systems and hence will make a multibiometric system simpler as well as secure. The other proposed system is also developed which is overcomes the problem of time and cost in multimodal biometrics. The system can be used to efficiently verify a person in a simple way. Hence, in future we can use the former approach to be used in multimodal biometrics and and we can also extend the system for various other attack points.

