Securing Stored Biometric Template Using Cryptographic Algorithm

Manmohan Lakhera, Uttarakhand Technical University, Rishikesh, India
Manmohan Singh Rauthan, HNB Garhwal University, Srinagar, India

ABSTRACT

The biometric template protection technique provides the security in many authentication applications. Authentication based on biometrics has more advantages over traditional methods such as password and token-based authentication methods. The advantage of any biometric-based authentication system over a traditional one is that the person must physically be present at that place while recognizing him. So, it is essential to secure these biometrics by combining these with cryptography. In the proposed algorithm, the AES algorithm is used for securing the stored and transmitted biometric templates using helping data. The helping data is a variable type of data which is changed at every attempt for registration. The final symmetric key AES algorithm is a combination of helping data and actual symmetric keys of the AES algorithm. The experimental analysis shows that a brute force attack takes a long time to recover the original biometric template from cipher biometric template. So, the proposed technique provides sufficient security to stored biometric templates.

KEYWORDS

AES, Biometric, Brute-Force, Decryption, Encryption, Template

1. INTRODUCTION

Security of stored biometric template is the main challenge in today’s digital scenario. This chapter explores how to resolve the current security issues with the stored biometric template. The main objective of the proposed technique is to secure the biometric template before storing it into the database. For the security of biometric template, the AES encryption algorithm is used with helping data which will use as a symmetric key for AES encryption algorithm. This research is mainly based on the oldest security system of stored data where the password was stored as it is in normal text format in the personal computer database and the regular text format is easily compromised. If the normal password is compromised, one can easily change and replace it with the new one. However, if the stored biometric feature is compromised, it will be lost permanently, and the user can never use this biometric feature in future for any verification process. The biometric template security is based on three types of technique- transformation, biometric cryptosystem and watermarking. The proposed scheme is based on template transformation technique.

DOI: 10.4018/IJRSDA.2018100103

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
1.1. Template Transformation

Template transformation is a process where the input biometric template is modified by the user given key which is difficult to retrieve the original biometric template from the encoded template. During authentication, the same process is applied to the biometric query. The input biometric feature is also encrypted by the same user specific key. For verification the stored and received biometric template are decrypted and then are matched with each other; if the received and stored biometric feature is matched then the requested user is authorized or if does not match, the request for verification is rejected.

2. PREVIOUS WORK

Biometric template is the particular attributes of a biometric sample. It is a reference to particular attributes that have been extracted from a biometric sample. This paper is dealt with the background study of biometric template security techniques. Many research scholars have work on this technique. Jain et al., (2002, 2008) pointed that the fake biometric data replaces the stored biometric data in order to illegal access such as physical spoof, a set of fake biometric data. For gaining illegal access the stolen biometric is replayed to the matcher. The stored biometric data consist of the data of an individual in a database which is used for comparison for biometric verification system. If the biometric data is quite close to the one presented, the person is verified. Hence this system has great problem for security of the biometric data. The privacy of stored biometric data is affected by internal and external attacks.

Rudolf et al., (1998), Maltoni et al., (2009), Putte and Keuning (2000) have analyzed the problem in verification system. During verification system in large scale the stored database can be accessed by several verifiers who cannot be trusted. The database is not secured from the serious threat in a network situation. According to Matsumoto et al., (2002) the biometric data can be mistreated to construct artificial biometric in order to impersonate individual.

Hill et al., (2001) point out that the artificial biometric used for illegal verification may be constructed if some data of biometric (minutia) are available. Schneier, (1999) hold the view that the identity of an individual is stolen if his biometric data is stolen. The identity of a person is lost permanently when his biometric data is stolen. Therefore, it is very essential to maintain the security of biometric data. vide (Babler, 1991; Miller, 1973; Penrose, 1965) show the genetic information in the fingerprint which creates a serious problem. Ratha et al. (2001) finds the different types of attack on biometric system:

1. Use of false biometric attribute such as artificial finger;
2. The modification of the biometric by an attacker;
3. The swapping of biometric feature extractor by Trojan horse program;
4. Replacing the biometric attribute by the fake ones;
5. The problem of Trojan horse program which replaces the matcher;
6. vi. The stored data may be modified, removed or a new data may be inserted in the database;
7. During communication one may modified the data and makes an artificial biometric such as an artificial finger. Resubmission of such data is dangerous. The attacker has a hold on sensor and the fake biometric set is created. It can change the final matcher result itself. Thus, it reduces the security of biometric system (Jain & Uludag, 2003).

Sun et al., (2007) have constructed a template known as KMT, or Key-Mixed Template. It is used in the combination with a secret key to create a new biometric template. Template and the secret key is mixed at the end of as well as that of verifier. It can check the attacks snooping tempering.

According to Teoh and Yuan, (2007) the biometric template can be canceled and restored with another authentication factor. This technique is known as BioHash. The Johnson-Linden Strauss
What Does the Future Hold for Innovation Management Education?
www.igi-global.com/chapter/what-does-the-future-hold-for-innovation-management-education/215147?camid=4v1a