Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 235–240 DOI: 10.15439/2017R57
ACSIS, Vol. 10 ISSN 2300-5963

# To study of various security attacks against Biometric template in a generic Biometric Recognition System

Manish Kumar
THDC Institute of Hydro. Eng. & Tech.
Tehri India
manishkumar4net@gmail.com

Kunwar Singh Vaisla
B T Kumoun Institute of Technology
Dwarahat, India
vaislaks@rediffmail.com

***Abstract*—Biometric recognitions system is a system which provides the reliable solution for user authentication in identity management systems. The motivation is that how we can use the effective biometric system in e-Governance service delivery with secure channel. So first we discuss the various security attacks that can be encounter during the enrollment and verification of biometric traits. We analyze various vulnerabilities of biometric system and study the various counter measures that can be present in biometric system in any way. There are many successful developments in the field of e-Authentication but the security is remain challenge in real world. This paper focus on the risks of biometric data at the time of enrollment and verification process. There are many types of attacks like finger print in biometric system by using fake fingers at the sensor could be a serious threat for unattended applications. In biometric system fingerprint matching is very big challenge to match the saved image with real time template with reduce the false match rate and false reject rate. We focus here to analyze the behavior of fingerprint verification because fingerprint verification is the very reliable personal e-Authentication mechanism.**

***Index Terms*—Biometric Recognition System, Biometric Sensor, Biometric system vulnerability.**

## I. Introduction

Biometric recognition system is wide-spread development in the field of e-Authentication that ensures the identity of person is unique. Biometric recognition system is reliable system unlike the traditional authentication system as password, Pin number which is stolen and forgotten easily. We are review and discussing all the various types of biometric attacks and conclude the analysis of different types vulnerability encounter in biometric security opponent. There are various advantage o Biometric Recognition System which is better than traditional mechanism that is based on password, PIN number or One Time Password, digital signature etc. Recently, the research on the presenting fake biometrics to the acquisition sensor which attack has been particularly active in the fingerprint domain [1]. There are numerous difficult problems present in biometric recognition system which creates the problems for biometric stored template during the enrollment. Third party attacker may steal the stored template and may gain unauthorized access to the biometric recognition system by creating the duplicate biometric template. In the basic theme of biometric recognition system is that the biometric image is stored in the biometric system at the time of enrollment and this stored biometric image is called template. At the time of verification to stored template is matched with the real biometric image should be successfully. The challenging task is to secure the stored biometric template. In this paper we study the biometric system, enrollment phase and verification phase and then different types of attacks that may be present in the biometric system.

## II. Biometric Recognition System

A biometric recognition system is a pattern recognition system which recognizes a person with his biometric traits.There are four modules of a generic biometric system[2]:

a) Biometric sensor module- Biometric Sensor is the part of biometric recognition system. Behavior of biometric sensor is to capture the biometric image. The work of sensor is to scan the visible biometric image and capture this biometric image in the biometric system. The user can interact with biometric recognition system with the help of biometric sensor.

b) Feature extraction module- Feature extraction module is the part of biometric recognition system. The work of feature extraction module is to extracts important and qualitative area of biometric image which is useful for identifying the particular user. Because biometric image have many problem like over inked area and under inked area. Biometric extraction module remove this type of problem. And stored then stored the template in database.

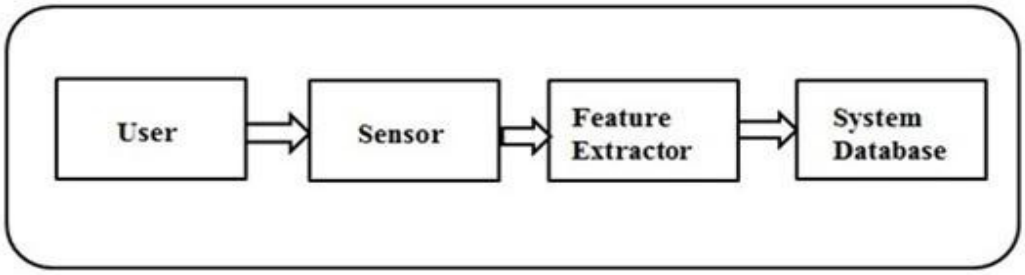


**Figure 1: Enrollment in Biometric recognition system**

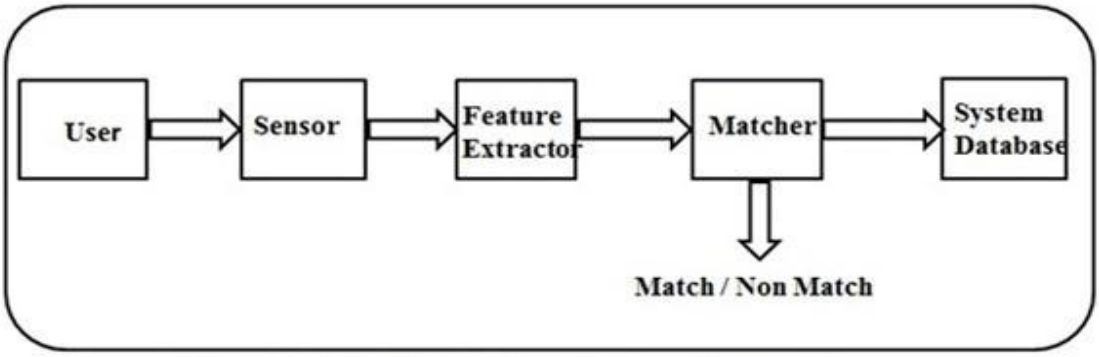


**Figure 2: Verification in Biometric recognition system**

c) Biometric matcher module- Biometric matcher module is the part of biometric recognition system. The work of biometric matcher is to match the biometric feature and compare each other and gives the output result as some match score. The score represent the two biometric image is how much similar.

d) Decision- making module- The template feature set is typically generated during enrollment when a user first interacts with the system and is refreshed or updated over a period of time in order to account for intra-class variations [3]. Decision module is Matcher module that gives the result as two biometric images is related or not. A typical biometric recognition system can be defines in two modes: (see Figure 1 and Figure 2) first is Enrolment and second is verification or authentication. In enrollment mode the biometric

recognition system capture the biometric samples from the user and biometric system store that samples in the system database which is called biometric template. In verification mode the user give his identity along with biometric sample to the biometric recognition system. The feature extractor matches the stored template with claimed identity. If match score is greater than the system threshold then the biometric system declare match otherwise non match. Identification system uses the governmental applications in the field of e-Governance where the identity of any individual matches his biometric traits against the stored template. The best part of verification system is first user verifies the user with some credential then biometric trait has to be verifying by the biometric system. Examples of identification system include the UID system by the Government of India [4]. Unique identification project was initiated by the Planning Commission of India which provides identification for each resident across the country and provide the efficient delivery of welfare service.

## III. BIOMETRIC SYSTEM VULNERABILITY

In the developing area of biometric computing technology have affordable and very easily inbuilt the various consumer devices. To avert any potential security crisis, vulnerabilities of the biometric system must be identified and addressed systematically [5]. There are different methods of vulnerability attack that could be analysis. Biometric recognition systems are prone to deliberate attacks as well as inadvertent security lapses that can lead to illegitimate intrusion, sabotage [6] or theft of sensitive information such as the biometric templates of the users enrolled in the system. There may be many factors which lead to such security lapses. A biometric system is vulnerable to different types of attack that can compromise the security afforded by the system, thereby resulting in system failure [7]. We can categorize these security lapses belong to following categories: Intrinsic failures, Administrative privileges, Non secure infrastructure, Biometric overtness. Thus it is essential to protect the template from possible attacks [10].

### A. INTRINSIC FAILURES

Intrinsic failure due to an existing limitation in the sensor of biometric system, feature extraction or matching technology. Intrinsic failure is the cause of incorrect choice by the biometric matcher module. There are two types of error committed by biometric verification system while decision matcher module which is false match. A legal user may be wrongly rejected by biometric recognition system because of various differences of two identical templates. The ridges and valleys in a finger print alternate of fingerprint reveals that the ridges or valleys exhibit anomalies of various kinds, such as ridge bifurcations, ridge endings, short ridges and ridge crossovers [8]. Two different fingerprint sample of the same finger obtain on different days which gives the large difference because of different movement that biometric finger is pressed in the sensor module. This difference is called minutia. When two unrelated biometric samples incorrectly matches using some rate of these two samples this is called false match rate. False match rate may be because of dissimilarities of two biometric traits like when two identical twins are very similar to each other which gives wrong decision while verifying the identity of the twins. When we get two very different samples obtain from the same finger, the error is called false reject rate (FRR). A biometric sensor may incorrect match due to limit of sensing technology. In biometric recognition system, a biometric sensor may not be identify a good quality fingerprint so that we can measure genuine accept rate (GAR) by the performance biometric system is GAR=1-FRR.

Intrinsic failures may occur when no explicit effort by third party that attack is called zero-effort attack. It can create a problem when the probability is high of false accept and false reject. So the objective is to create the sensors that could be reduce the intrinsic failure and the sensor should be reliable, convenient and secure.

### B. ADMINISTRATIVE PRIVILEGES

The administrative attack we may say insider attack where all vulnerabilities could be encounter all because of improper administration of biometric recognition system, because the system administrator have the privileges to register the biometric template and make the exceptions for the individual whose biometric sample cannot be obtain by the system due to some injury or disease. This attack may be introduce using the

integrity at the time of enrollment process by the administrator or a authorize user or may be improper processing procedure.

Non secure infrastructure may be encounter the hardware infrastructure, software infrastructure or communication channel of different module of a

### C. NON SECURE INFRASTRUCTURE

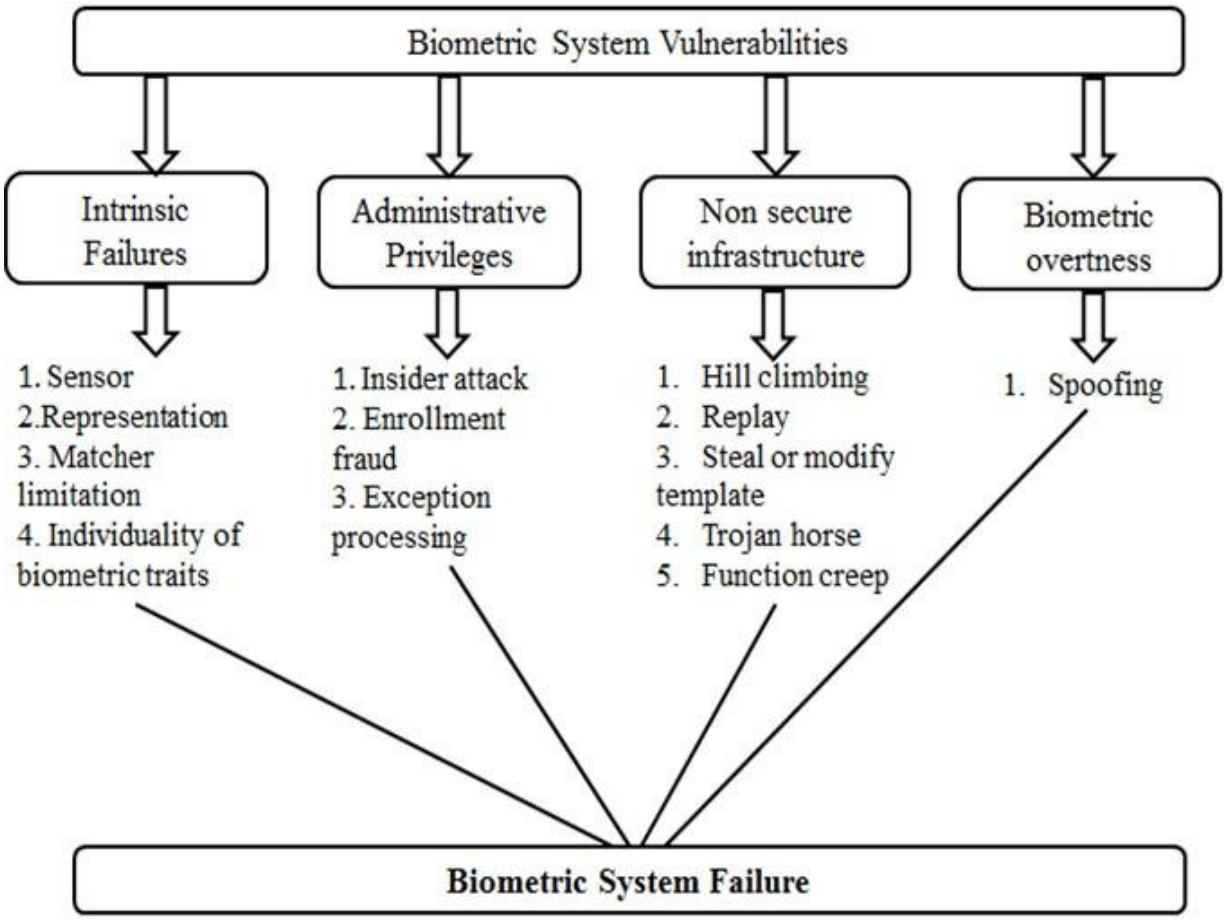


**Figure 3: Biometric System Failure**

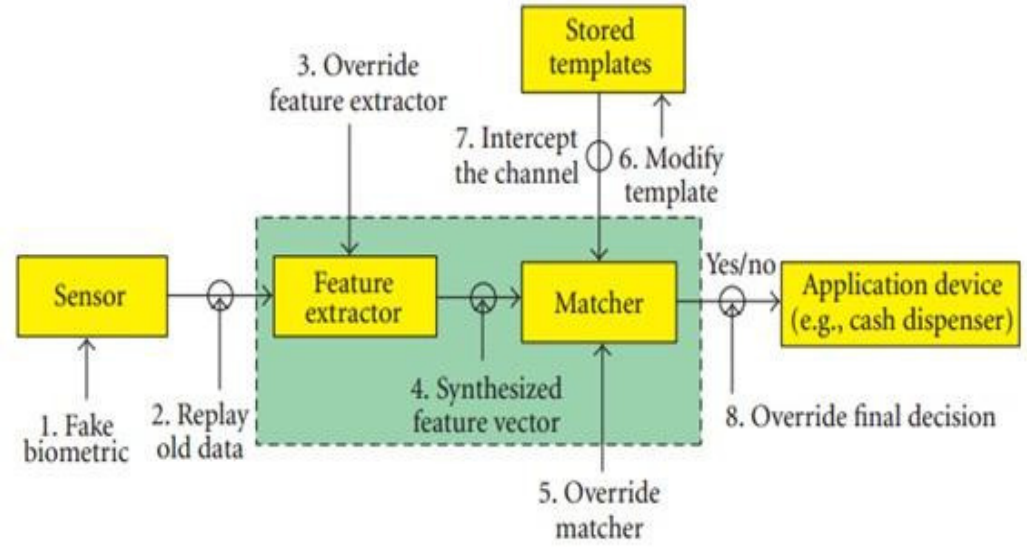


**Figure 4: various security attacks in a generic biometric system (adapted from [9])**

biometric system. An opponent can attack for the biometric infrastructure by various way so that the security may be break through the biometric infrastructure. Ratha et al.[9] identified eight point of attack in a generic biometric system(see in Figure 4). Anil K. Jain et al. [6] categorize the different types of biometric infrastructure attack into following four categories:

### a) Attacks at the user interface

In this type of attack can be introduces due to the sensor because sometimes the sensor could not distinguish between the fake and genuine biometric sample. So that the opponent can easily introduce in the biometric system through fake identity. It is best to use the liveness detection through the software and hardware solution.

### b) Attacks at interface between modules

In this types of attack the opponent introduce on the communication interface between various modules. If the communication channel is not secure or not properly encrypted, the opponent can intercept, modify the data during the transmission. This attack is called man-in-middle attack. When intruder intercept or replace information during transmission. When we use insecure communication channel the chances of replay or hill-climbing attack is high.

### c) Attacks on software modules

In this type of attack using the executable program which can modify the module such a way that output is desired by the opponent. This type of attack is like Trojan-horse attacks. An opponent may modify or replace software module using the virus.

### d) Attacks on the template database

In this types of attack the attacker damage the biometric template from the database in biometric system. An attacker can replace the templates stored in the system database with desired template. A template can be replaced by an impostor's template to gain unauthorized access, a physical spoof can be created from the template to gain unauthorized access to the system and the stolen template can be replayed to the matcher to gain unauthorized access [6].

## D. BIOMETRIC OVERTNESS

In this types of attack the opponent can acquire the biometric traits of legitimate user and use them to create copy of that biometric trait. So that the biometric system cannot identify or distinguish live biometric trait and physically artificial spoof.

## IV. Conclusion

In this paper we discussed various type of attack which compromises the security. The research is analysis of different types of attack against the stored biometric template in the biometric system. To secure the biometric template we should use the multifactor authentication. In multifactor authentication we may use one factor is necessarily being used which something is like biometric trait of individual and another factor is his/her password, OTP (One Time Password), and PIN number. In Aadhaar based authentication the UID number is first factor for authentication and his/her biometric trait is the third factor authentication.

## References

[1] Raffaele Capplellin, Alessandra Lumini. Darion Maio, “Fingerprint Image Reconstruction from Standard Templates”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No.9, pp. 1489-1503, 2007.

[2] Arun Ross, Anil Jain, “Biometric Sensor Interoperability: A Case Study in Fingerprints”, Proc. of international ECCV Workshop on Biometric Authentication (BioAW), LNCS Vol. 3087, pp 134-145, Springer Publisers, May 2004.

[3] Jain, A.K., Uludag, U., Ross, A.: Biometric template selection: a case study in fingerprints.In: Proc. of 4th Int’l Conf. on Audio- and Video-based Biometric Authentication (A VBP A).Volume LNCS 2688., Guildford, UK, Springer (2003) 335–342.

[4] Unique Identification Authority of India. Multipurpose National Identity Card. Available at http://uidai.gov.in/

[5] FaceIT SDK, L-1 Identity Solutions. Available at www.annualreports.com/HostedData/AnnualReports/PDF/id2007.pdf (Access date 14-04-2016)

[6] Anil K. Jain, karthik Nandakumar, and Abhishek Nagar, “Review article Biometric Template Security”, Hindawi Publihing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 579416, 17 pages, doi: 10.1155/2008/579416.

[7] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security”, IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, 2006.

[8] Nalini K. Ratha, Shaoyun Chen, and Ani1 K. Jain. “Adaptive flow orientation based texture extraction in finger print images”. Pattern Recognition, Vol. 28, 28(11): 1657–1672, November 1995.

[9] N. K. Ratha, J. H. Connell, and R. M. Bolle, “An analysis of minutiae matching strength,” in Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA ’01), pp. 223–228, Halmstad, Sweden,June 2001.

[10] Shenglin Yang, Ingrid Verbauwhede, “Automatic Secure fingerprint verification system based on fuzzy vault scheme”, Proceedings in (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, pp- v/609 - v/612 Vol. 5, DOI-10.1109/ICASSP.2005.1416377, 2005