IOSR Journal of Engineering (IOSRJEN)
ISSN: 2250-3021 ISBN: 2878-8719 PP 04-08
National Symposium on engineering and Research

Biometric Template Security Attack: A Review

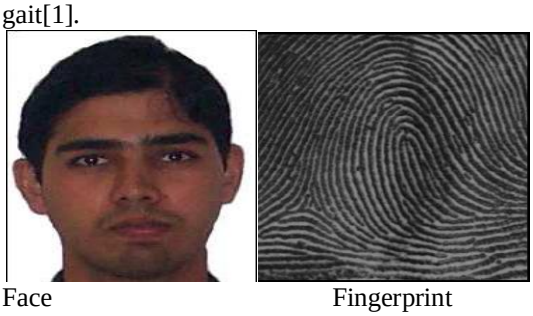
Mrs.Swati A.Jadhav
M.E.[computer]student, MCOE & RC,eklahere,Nasik,

Abstract: - *Now a days, for any computer security biometric is became more popular due to its uniqueness. Mainly biometric is used for identification and verification of a particular person but this is suffered from some kind of security threats. In many application authentication for a particular system is provided with biometric template protection. Because biometric based authentication has more advantage over traditional method such as password and token based authentication method. The main advantage of any biometric over traditional method is that while recognizes any person at that time the person must be physically present at that place. But in case of password mechanism system does not identify difference between the attacker and an authorized person/user. Hence, we can say that biometric is a strong weapon in any traditional authentication method. Sometime biometric is also lacks in some of its privacy, security and revocability .So, there is need to secure these biometric by/with combining these it with cryptography. Also we are aware that biometric plain template cannot be replaced if they are get compromised or attacker can access it purposely. For any secure system authentication can be identified with three main components that are what the person know? What he have? What he is? In this paper we summarized various aspects of biometric system security. Our goal is to broadly categorize various attacks that affect the biometric system failure and identify the effects of such failure.*

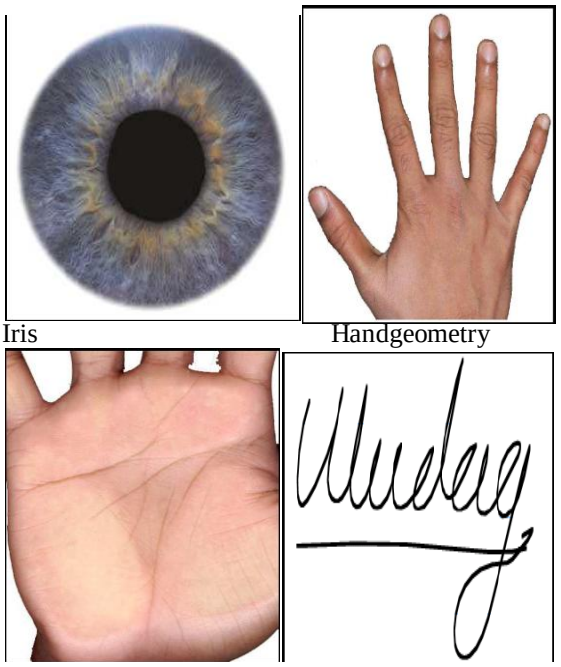
Keywords: - *authentication, cryptography, Identity management, revocability, biometric systems security, template protection, salting, non-invertible transform, key binding, key generation.*

I.INTRODUCTION

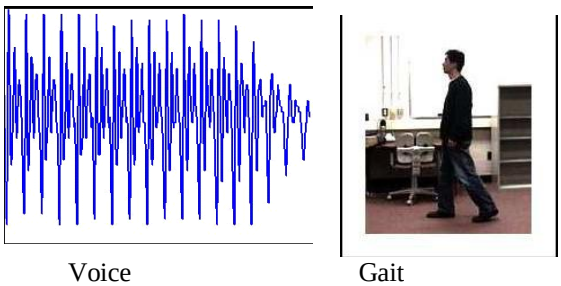
In increasing use of biometric in various applications there is need to security of user and privacy of his biometric technology. Because it offers a reliable and natural solution to an authentication system .Our focus is on biometric template protection because once it is compromised it cannot be revoke and reissued. We present an overview of various biometric template protection scheme and compare their advantages and limitation in terms of security, revocability and matching of captured image. For any identity management system to provide identity of a particular person is a very trivial task.Because identity such as a password and ID card of a particular person is not so much reliable because they can be easily hacked or an intelligent user can guess it. Instead of this biometric is a solution which verify persons identity with behavioral characteristics.Commonly used biometric are fingerprint,iris,face,hand geometry,palmprint,handwritten signature and gait[1].



Face Fingerprint



Iris Handgeometry Palmprint Signature



Voice Gait

Fig.1 VARIOUS BIOMERIC APPLICATION

Biometric individuality have number of property with their use as an uniqueness,reliability,security,authentication token ,convience.These characteristics shows that biometric having pervasive use in various authentication system.But still there were some problem regarding biometric and we have to deal with them to secure integrity in order to public acceptance system.There are five main component in any basic biometric authentication system namely these are sensor, feature extractor, template database, matcher and decision box.

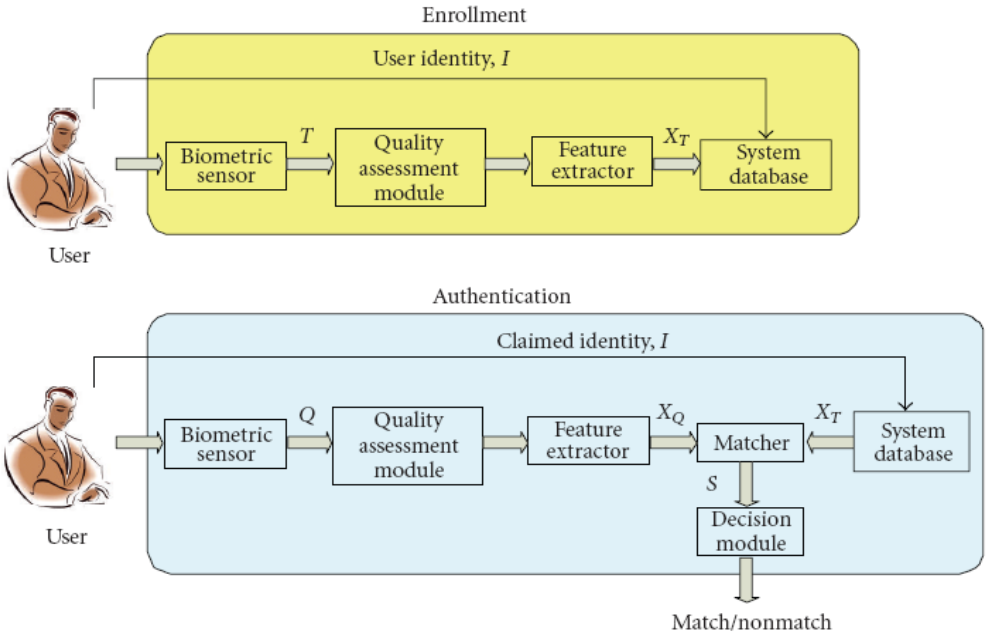


Figure 2: Enrollment and recognition stages in a biometric system

. Here, T represents the biometric sample obtained during enrollment, Q is the query biometric sample obtained during recognition, XT and XQ are the template and query feature sets, respectively, and S represents the match score[1]. In figure sensor is

interface between user and authentication system and is able to scan the biometric trait of user .

Feature extractor extracts the silent feature of a particular biometric trait in order to differentiate between different users with their identities. Sometimes this feature extractor is includes quality measure module to determine whether scanned biometric trait is enough quality for further processing. At the enrollment process extracted feature of particular biometric is stored in a database as a template and shows users identical information.

Matcher module is an executable program accepts two biometric feature such as template database and template query as input and produces match result to indicate that similarity in between two sets. Finally decision module takes a decision and give response to query.

The main objective of biometric template protection is to protect the privacy of user and their biometric data. First level for this template protection there are many algorithm has been proposed.

1. Quatization scheme for a continuous biometric 2.Fuzzy extractor and scheme for discrete biometric
3. cancellable biometric[5].

Hardware is second level for template protection.One can replace existing hardware or provide better security on it.

At third level security on biometric template can be achieved by using protocol that based on cryptographic technique such as multiparty computation homomorphic encryption or private information retrieval prptocols. We list all existing attacks on a biometric and we show only their consequences.some of the attacks can easily handled. However, existing protocol have some drawbacks.

II.RELATED WORK

This section reviews the all existing schemes for biometric template protection.

1. In year 2000 C.Souter et al. design a mechanism for biometric to retrieve a digital key.It may be a 2D images such as fingerprint,iris,face,palmprint.

Corelation

Researcher Randal K.Nichols in 1999 design correlation algorithm for linking and retrieving a digital key for secure biometric.Algorithm design by this researcher uses entire image instead of only image failure.

The correlation between input image f1(x) and captured image during verification process f0(x) is defined as C=(x) FT-i{f1(u)f0*(u)}[4].

2. In year2002, researcher F.monrose et.al design key strokes dynamic method for biometric cryptography security.Its purpose is to generate difficult password which no one can easily found or difficult to guess.This difficult password is generated using text's characteristics and pattern of user typing.Then this password can be used as cryptographic key for biometric security as well as computer security[8].

Limitation:

It limits the system that attacker may be able to identify user frequently typing repeatation.

3. In year 2001,researcher F.monrose et.al generate a cryptographic key from voice for biometric security. Key is generated when user speaks password to it. This is so because key is not easily guess by an attacker or it cannot be reproduced by an opponent at the time of cryptographic operation.

Limitation:Problem with this system is that intelligent recognizer can only recognize upto 104 words.

Solution:

User speak password in its own device and after that device is generates a key associated with his password.Repetition while talking of the same password by the same user can improve the security of the key.

4.From a decades there is very important issue of protecting storage of biometric template in an authentication phase.

In year2007,researcher Yagiz sutu and nasir memon proposed a secure sketch for cryptography to provide protection to template.

Although biometric template protection is a relatively young discipline, already over a decade of research has brought many proposals. The main objective of template protection methods and the main difficulty is to prevent an attacker to compromise privacy of users or biometric data.

Method	Examples	Properties
What you know	User ID Password PIN	Shared Many passwords easy to guess Forgotten
What you have	Cards Badges Keys	Shared Can be duplicated Lost or stolen
What you know and what you have	ATM card + PIN	Shared PIN a weak link (Writing the PIN on the card)
Something unique about the user	Fingerprint Face Iris Voice print	Not possible to share Repudiation unlikely Forging difficult Cannot be lost or stolen

Table 1 Existing user authentication techniques

Due to quick expansion of sensors and other computing technique biometric having more advantages and are easily rooted in a variety of end user device(Eg. portable devices including mobile phones). We judge that template security is one of the most vital issues in designing a secure biometric system and it stress appropriate and exact attention[8].

Towards this end, we present a detailed overview of different template protection approaches that have been proposed.

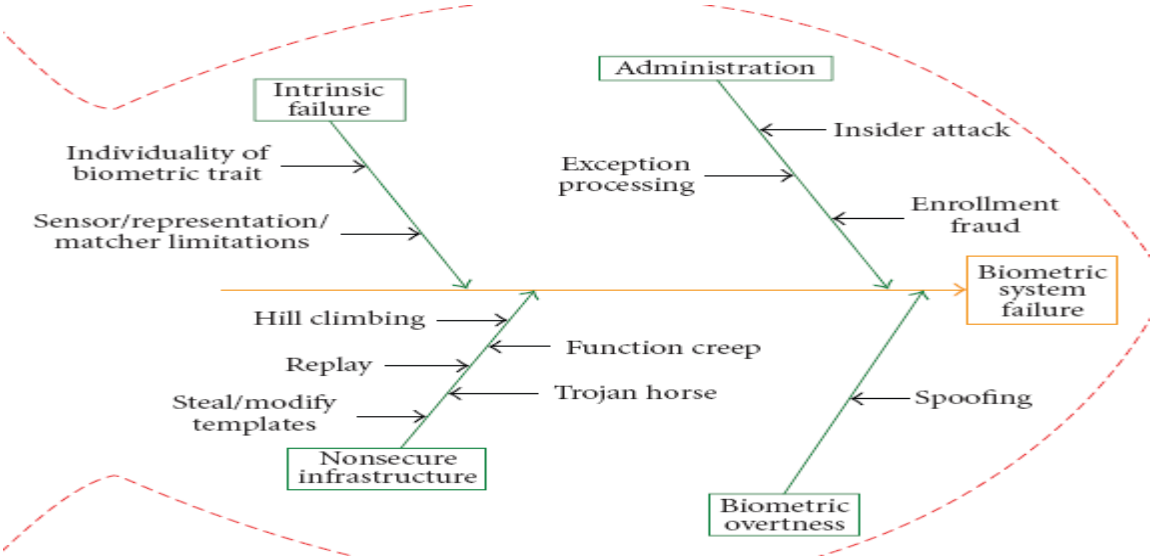


Fig.2 biometric system vulnerabilities

III.Biometric System Vulnerability

In figure.2 fish shaped model shows that at the top level biometric system categorized into two classes

1.Intrinsic or native failure

Native failures occur due to inbuilt restrictions in the sensing a biometric , extracting image feature to specific biometric individual.

2.failure due to adversary attack

In adversary attacks, a ingenious Opponent attempts to avoid the biometric system for its personal purpose. We also divide these attack into three types based on those attack which can compromised the systems security. These are as follows: system administration, nonsecure infrastructure ,biometric overtness.

A) Native failure

This failure is occur due to the incorrect decisionmade by biometric system . While At the verification process decision making done on false accept and false reject. A authentic user may be incorrectly rejected by the biometric system due to the large differences in the user's stored pattern and query biometric feature sets. This variations is due to lack of interaction between user and the biometric system or due to the occurance of noise in sensor.

False accepts are happen due to lack of uniqueness

in the biometric which can show similarity between feature sets of different users (e.g., similarity in twins faces).

A sensor may sometime fail to acquire the biometric trait of a user due to limits in the sensing technology or undesirable environmental conditions. For example, a fingerprint sensor unable to scan good quality fingerprint of dry fingers. This leads to failure-to-enroll (FTE) or failure-to-acquire (FTA) errors. Even there were no explicit effort by an adversary attack around the system the native failures can occur .. So this type of failure is also known as zero-effort attack. It should be serious threat if the false accept and false reject probabilities are too high.

B) Adversary attacks

The adversary attacks categorize into three classes:

Administration attack, Nonsecure infrastructure, and Biometric overtness.

(i) Administration attack

Many times this type of attack is known as insider attack because it happens due to improper administration
of the biometric system.

(ii) Nonsecure infrastructure

The infrastructure consists of hardware, software, and the message between the various modules. For securing biometric native attack can manipulated in various ways.

(iii) Biometric overtness

It is possible for native attack to secretly acquire the biometric characteristics(e.g., fingerprint impressions
lifted from a surface) .

C)Effects of biometric system failure

Biometric system can lead to two main effects:

(i) denial-of-service

It refers that authorized user is prevented from services that are assigned to him. An opponent can causes harm to the infrastructure (e.g.physically damage a fingerprint sensor) so preventing these users from accessing the system. Native failures like false reject, failure-to-capture, and failure-to-acquire lead to such adenial-of-service .

(ii)Intrusion

It refers to a fake person gaining illegal access to the system which results in defeat to privacy (e.g., unauthorized access to personal information) and security threats (e.g., terrorist cross the border). biometric system vulnerability, namely, intrinsic failure, administrative abuse, nonsecure infrastructure, and biometric overtness, can results in intrusion.

IV.SUMMARY

Here in this paper we presented various security mechanism on face recognition which allows us to generate a key and random for unique biometric.

We focus on various biometric template protection schemes and possible type of attack on template. Also we studied Enrollment and recognition stages in a biometric system using various components. Biometrics offer many advantages over traditional authentication methods so they need to secure from attacker .because they are well situated for users and cannot be forgotten or Shared between users. They are particularly attractive for use with single sign on systems, as both the benefits and the costs of the biometric system can be shared across multiple domains.

REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process. 2008.

[2] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in IEEE Symp. Privacy and Security, 1998, pp. 148–157.

[3] F. Monrose, M. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in Proc. IEEE Symp. Security and Privacy, 2001, pp. 202–213.

[4] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometric-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.

[5] F. Monrose, M. K. Reiter, Q. Li, S. Wetzel, "Using voice to generate cryptographic keys: A position paper", Proc. Of Odyssey 2001, The Speaer Verification Workshop, June 2001.

[6] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–752, Apr. 2007.

[7] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in Proc. Int. Conf. Pattern Recognition, 2008, pp. 1–4.

[8] Y. Sutcu, H. Sencar, and N. Nemon, "A secure biometric authentication scheme based on roubst hashing," in Proc. Seventh Workshop Multimedia and Security, 2005, pp. 111–116.

[9] Yi C. Feng, Pong C. Yuen, Member, IEEE, and Anil K. Jain, Fellow, IEEE," A Hybrid Approach for Generating Secure and Discriminating Face Template " IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, March 2010

[10] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for face template protection," in Proc. Int. Society for Optical Engineering (SPIE), 2008, vol. 6944, pp.1–11.

11] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in CVPR Biometrics Worshop, Jun. 2007, pp. 1–7.

[12] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004.

[13] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in CVPR Biometrics Worshop, Jun. 2007, pp. 1–7.