IJCSC 0973-7391
International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 10 • Issue 1 pp. 232-238 Sept 2018 - March 2019 www.csjournals.com

Advancement in Biometric Security System: A Case Study

Ramesh Kumar
Asstt. Professor, Deptt of Computer Science
Shaheed Udham Singh Govt College, Matak Majri, Indri, Karnal

Abstract: Security is an important issue in modern systems. The level of traditional security system can be increased by biometrics system. Biometrics basically uses physiological and behavioral traits of human being for identification and verification. Although biometric system has various advantages but they are vulnerable to attacks that can decrease the level of security. The biometrics system security level can also be enhanced by using different new technologies such as cryptography, watermarking, liveness detection, multimodal and stagnography etc. This paper discussed an introduction about advanced technologies which are used for resist different type of biometric system attacks and provide better security concerns.

Keyword: Attacks in Biometric system, cryptography, liveness detection, multimodal, Stagnography, watermarking.

I. INTRODUCTION

Biometric authentication system provide high security level as compared to traditional authentication system because they uses pin, password, key, tokens for identifying whether the person is authorized or not as shown in Fig 1. Biometric system uses unique characteristics of person for identification and verification. These unique characteristics includes various physiological (face, fingerprint, iris etc.) and behavioral (voice, signature, gait etc.) traits for differentiating actual and fake user. Biometric system increases security and comfort for today's world because traditional way of authentication can be lost, stolen and forgotten.

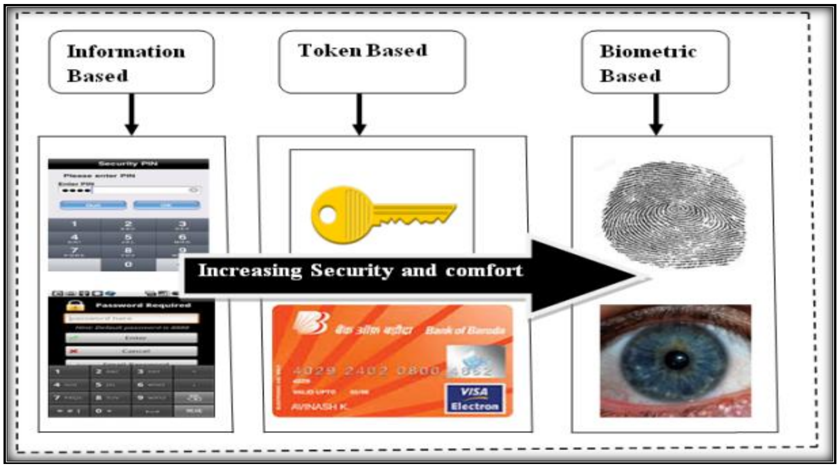

Fig 1 Different authentication methods

A. Biometric Authentication System

Biometric system uses person unique characteristics for differentiating real user and imposter in different application of modern world. These application includes banking system, attendance system, airport security and also used by defense organization for protecting their confidential data. Biometric system recognizes imposter after comparison of new extracting feature set with template stored in database (1). In biometric system firstly user is registered with biometric system called enrollment phase and then authentication is performed. Biometric system serves for two purposes either verification or identification(2). Identification is used for differentiating individual from a collection of record stored in database as shown in Fig 2.

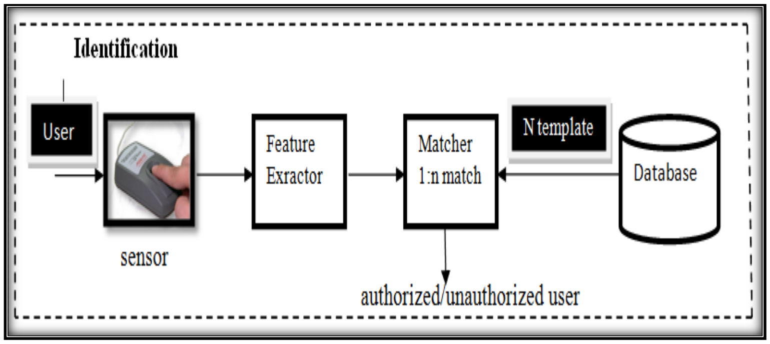

Fig 2 identification

Where as in verification individual sample is compared with already captured one individual stored template as shown in Fig 3. Verification also called 1:1 matching process because in this individual person sample is compared with their already existing profile (3). This process provides faster and more accurate result as compared to identification.

Use of biometric system for different contexts is increasing day by day in our society because today’s world has become digital and criminals have great expertise for breaking traditional authentication systems. It makes our life simple and secure by providing easy, cheap and more convenient methods of identification and verification. But after a huge impact of biometric system on today’s world, there is some vulnerability such that attacks on biometric system which are discussed in next section of paper.

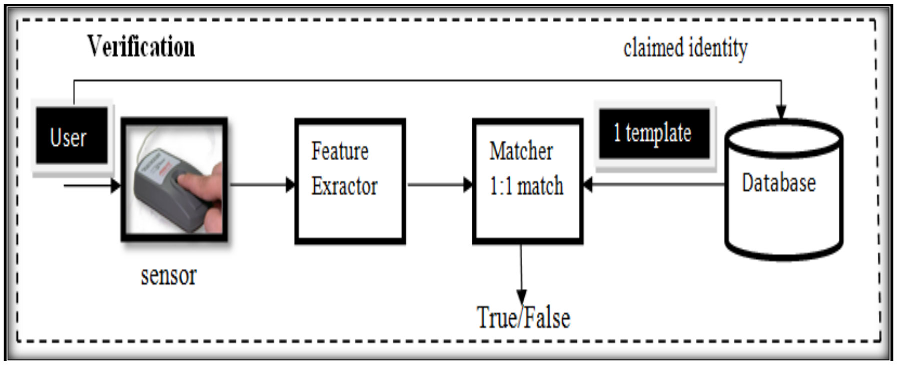

Fig 3 verification

II. BIOMETRIC SYSTEM ATTACK POINTS

Biometric based authentication overcome the limitation of traditional system such as (can not be lost,shared,forgotten and no need to remember password). After providing better security concern these system are vulnerable to attacks (4). Biometric system have mainly eight different type of attack as shown in Fig. 4 (5). These point of attack are discussed in detail below (6):

i.Attack on the biometric sensor

This point of attack also known as “Type 1” attack. At this point of attack, the attacker can physically destroy the recognition scanner and cause a denial of service. In this type of attack imposter present a fake biometric trait (artificial finger) to the sensor (5). It is very easy to attack at the sensor because no specific knowledge about the system operation is needed.

ii. Attack on the channel between the sensor and feature extractor

The other names for this point of attack are “Type 2” or “Replay attack”. When an sensor acquire an biometric trait it send its output to feature extractor module for further processing through channel. At this point attacker intercept channel for stealing biometric trait and stored somewhere or replace with other.

iii. Attack on the feature extractor module

This point of attack is known as “Type 3”. In this attack, the attacker can replace the feature extractor module with a Trojan horse. At this point imposter forces the feature extractor module for producing fake feature value instead of original data feature value.

iv. Attack on the channel between the feature extractor and matcher

This point of attack is known as “Type 4”. The difference between type 2 and type 4 is that the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher at a later time.

v. Attack on the matcher

This point of attack is known as “Type 5”. At this point the attacker replaces the matcher with a Trojan horse and produce high matching scores by the imposter instead of output produce by actual data.

vi. Attack on the system database

This point of attack is known as “Type 6”. In this attack, the attacker compromises the security of the database where all the templates are stored. Compromising the database can be done by exploiting vulnerability in the database by adding new templates, modify existing templates or delete templates.

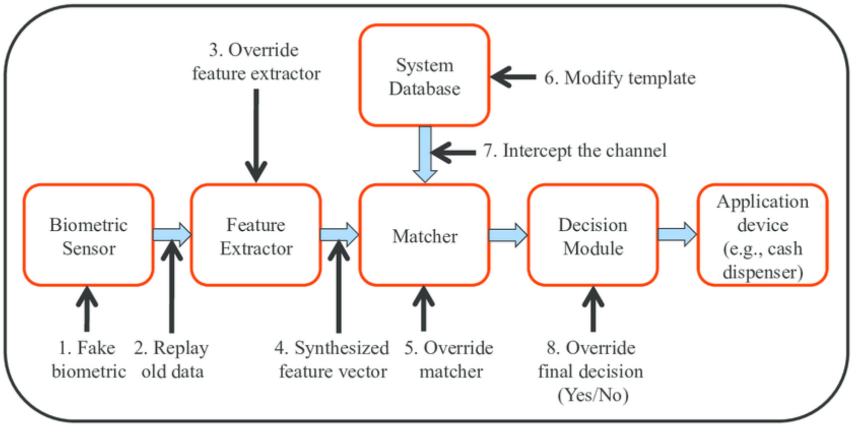

Fig 4 attack point on biometric system

vii. Attack on the channel between the system database and matcher

This point of attack is known as “Type 7”. In this attack, the attacker intercepts the communication channel when template is transmitting from database to matcher module. At this point attacker intercept the channel to steal or alter the biometric template.

viii. Attack on the channel between the matcher and the application

This point of attack is known as “Type 8”. In this attack, the attacker intercepts the communication channel between the matcher and the application to replay previously submitted data or alter the data. At this point attacker change the original decision of matcher module when transmitted through channel to the application.

III. TECHNIQUES TO RESIST THE ATTACKS

Biometric system authentication mechanism are more convenient for users and providing better security level than traditional authentication mechanism.Biometric system uses different biometric traits instead of using keys,pin and password. In spite of several advantages over traditional methods biometric system suffer from some problem which decrease the level of security. There are many new technologies which are used for handling various vulnerable threats and attack on the system are discussed below in this section. These techniques improve the security level of biometric system.

A. Liveness Detection

Liveness detection method was proposed for handling spoofing attack on biometric system.This technique is used for identifying and detecting whether biometric sample presented is alive or not. This method increase the security and reliability of biometric system and also used for preventing data from unauthorized access. Liveness detection techniques easily detect artificially created or fake sample and check the presented sample belong to live human being or not. There are three ways for introducing liveness detection in biometric system (7):

1. Using extra hardware: This approach is an very expensive and fast approach.
2. Using software: It is done at processing stage. It is less costly but takes much time in comparison to first.
3. Using combination of hardware and software: This is expensive as well as time consuming. It provides a good solution for livenesss detection.

Thus Liveness detection technique can be a hardware based or software based or a combination of both. Detection methods in this technique are as follow (8):

- head, face, eye and pupil movement
- lip movement with voice
- skin spectroscopy
- measurement of finger perspiration patterns
- Physical characteristics such as temperature, pulse etc.

B. Cancelable Biometric

Cancelable biometric is also most advance technology for enhancing security and privacy of biometric authentication. This technology mainly used in biometric system for template protection. In addition of enrolling original biometric sample,various distorted biometric samples are also stored in database. These distorted samples are used when our true biometric is stolen.

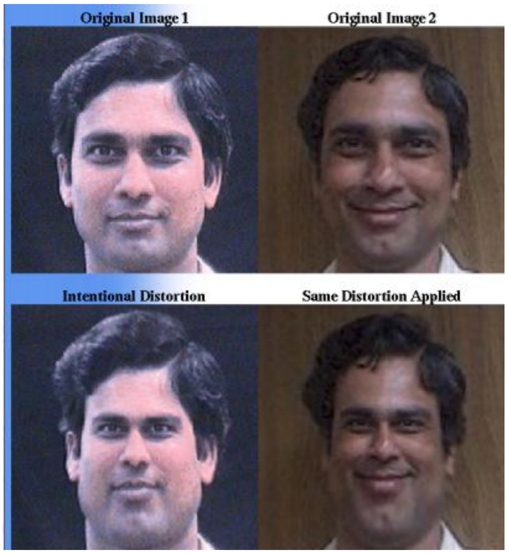

Fig 5 Distortion applied during cancellable process

Cancelable biometric provides a high level of security and privacy concern of biometric template because it used multiple distorted template are associated with same biometric data.

C. Biometric Cryptography

Biometric system was combined with cryptography for increasing security level called biometric cryptosystem. This system includes feature of both fields biometric (traits) and cryptography (add key into plaintext) and better solution for protecting attacks on biometric database. Cryptography technique converts original data into encoded data by using key which is not a understandable form for attacker. Cryptography prevent data from attacker by adding encryption key to the original data and convert into cipher text which is stored in database as shown in Fig 5. When attacker wants to steel data then he needs a decrypting key for converting cipher text into plain text. So this is very useful technique for protecting data from imposter (9).

There are many ways to combine biometrics with a Cryptosystem.
1) Biometrics key release,
2) Biometrics key generation and
3) Biometrics key generation

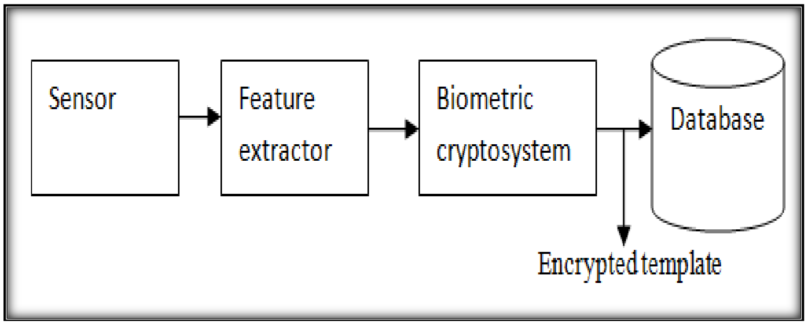

Fig 6 Biometric cryptography

D. Biometric Watermarking

Watermarking is a technique which is mainly used for increasing security level of biometric data and also used for improving security against biometric system attack points discussed above in this paper. This technique convert original data into digital content (for e.g. text, audio data , video, images etc.) without reducing original data quality. It provides security even after the decryption which is biggest problem of biometric cryptosystem. Watermarking hides the information which is to be transferred over the channel and provide copyright protection (10).Watermarking is a better approach for biometric system. It contain following benefits:
1) Provide integrity of biometric system
2) Provide privacy and security of biometric data
3) Provide biometric template protection during transmission
4) Provide help in multimodal biometric recognition

E. Multibiometric Approaches

Multibiometric approach basically uses more than one traits, sensors, algorithm and instances of single traits. This approach is mainly defined to overcome the

limitation of unimodal approach. As the name shows unimodal uses single source of information for recognition, identification and verification of user. There are some problems with unimodal approach which are reduced by multimodal technology by using more than one biometric traits instead of only one.

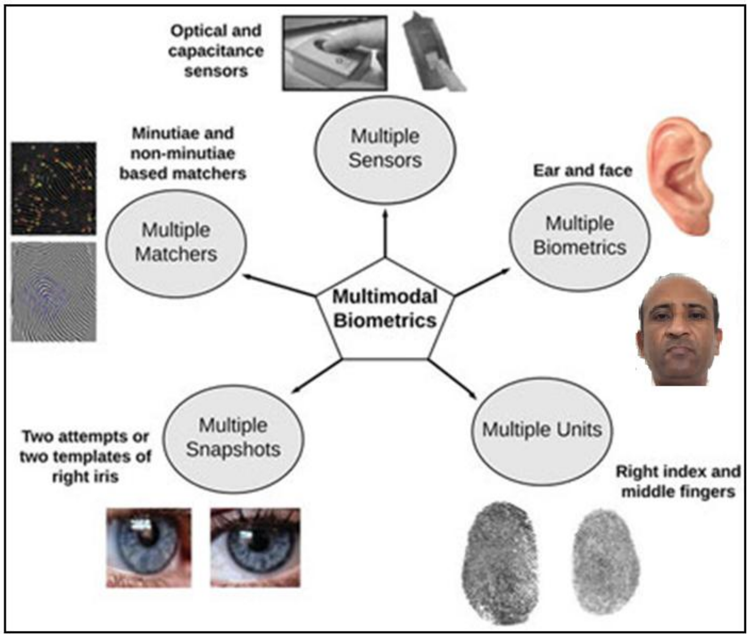
Optical and capacitance sensors
Multiple Sensors
Minutiae and non-minutiae based matchers
Multiple Matchers
Ear and face
Multiple Biometrics
Multimodal Biometrics
Two attempts or two templates of right iris
Multiple Snapshots
Multiple Units
Right index and middle fingers

Fig 7 Different types of a multibiometric system

The problems associated with unimodal biometric are:
1) Noise in sensed data
2) Non universality
3) Intra class variation
4) Spoof attack

If two biometric traits or more than two technique (face and finger, finger and iris etc.) are used in one application then this method is known as multimodal biometric system. Multimodal biometric systems are more reliable and provide better performance as compared to unimodal biometric system. Multimodal system uses information from multiple sources. So, different categories of multimodal biometric system are shown in Fig 7(11).

IV. CONCLUSION

Biometric systems provide better and secure authentication mechanism. Biometric system uses different biometric traits for identification and verification instead of ATM card, keys, pin and password. In this paper author discussed biometric system, their authentication methods which provide several advantage over traditional authentication methods. This paper also discuss different vulnerabilities exist on biometric system and different technology for improving security of biometric system. Liveness detection is used for identifying whether the person is alive or not. Cryptography increase security by adding encrypting key to the original data. Multimodal biometric overcomes the limitation of unimodal biometric technique. Watermarking and stagnography are the new advance technology for protecting data during transmission over the channel through information hiding. At last author conclude that above discussed technologies are very useful for increasing security of biometric data and resist different threats of biometric system.

References

1. A Review On Biometric Recognition. Gagandeep Kaur, Gurpreet Singh And Vineet Kumar. S.L. : International Journal Of Bio-Science And Bio - Technology, 2014, Vol. 6.
2. Vulnerabilities Of Biometric Authentication “Threats And Countermeasures”. Abdulmonam Omar Alaswad, Ahlal H. Montaser,Fawzia Elhashmi Mohamad. 2014, International Journal Of Information & Computation Technology, Vol. 4.
3. Stephen, Mayhew. Explainer: Verification Vs. Identification Systems. [Online] June 1 2012. Http://Www.Biometricupdate.Com/201206/Explainer-Verification-Vs-Identification-Systems.
4. Attacks On Biometric System: An Overview. Rubal Jain, Chander Kant. 07, S.L. : International Journal Of Advances In Scientific Research, 2015, Vol. 01.
5. A Study On Attacks And Security Against Fingerprint Template Database. Mrs.U.Latha, Dr.K.Rameshkumar. 5, September 2013, International Journal Of Emerging Trends & Technology In Computer Science (Ijettcs), Vol. 2.
6. A Simple Review Of Biometric Template Protection Schemes Used In Preventing Adversary Attacks On Biometric Fingerprint Templates. Joseph Mwema, Michael Kimwele, Stephen Kimani. 1, Feb 2015, International Journal Of Computer Trends And Technology (Ijctt), Vol. 20.
7. A Study Of Liveness Detection In Face Biometric Systems . S.Hemalatha, Amitabh Wahi. S.L. : International Journal Of Computer Applications (0975 – 8887), 2014, Vol. 91.
8. Biometric Attack Vectors And Defences. Roberts, Chris. 2007, Journal Homepage: Www.Elsevier.Com/Locate/Cose.
9. Security Enhancement Of Biometrics, Cryptography And Data Hiding By Their Combinations. Tan, Jing Dong And Tieniu.
10. Authentication Watermarking For Transmission Of Hidden Data Using Biometric Technique. Dr.Shubhangi D.C, Manikamma Malipatil. 5, S.L. : International Journal Of Emerging Technology And Advanced Engineering, 2012, Vol. 2.
11. Overview Of Multimodal Biometrics. V.Sireesha, K.Sandhyarani. 01, S.L. : Publications Of Problems & Application In Engineering Research - Paper, 2012, Vol. 04.