International Journal of Advances in Scientific Research
ISSN: 2395-3616 (Online)
Journal DOI: 10.7439/ijasr
Review Article

Attacks on Biometric Systems: An Overview

Rubal Jain[*1] and Chander Kant[2]

[1]*Research Scholar, Department of Computer Science and Applications, K.U., Kurukshetra, India*
[2]*Assistant Professor, Department of computer Science and Application, K.U., Kurukshetra, India*

***Correspondence Info:**
Rubal Jain
Research Scholar,
Department of Computer Science and Applications,
K.U., Kurukshetra, India
E-mail: rubaljain.92@gmail.com

Abstract

Biometrics is a pattern recognition system that refers to the use of different physiological (face, fingerprints, etc.) and behavioral (voice, gait etc.) traits for identification and verification purposes. A biometrics-based personal authentication system has numerous advantages over traditional systems such as token-based (e.g., ID cards) or knowledge-based (e.g., password) but they are at the risk of attacks. This paper presents a literature review of attack system architecture and makes progress towards various attack points in biometric system. These attacks may compromise the template resulting in reducing the security of the system and motivates to study existing biometric template protection techniques to resist these attacks.

Keywords: Biometrics, Biometric Attacks, Biometric Traits, Biometrics System Template, Generic Threats, Architecture, Template Protection Techniques.

1. Introduction

Biometric is a science through which system can uniquely identify an individual on the basis of his physiological (face, iris, fingerprint, hand geometry, retina etc.) and behavioral (gait, voice, signature, keystroke etc.) traits [1]. The use of biometric traits as an authentication technology has become widespread from door access to e-commerce due to the need of better security in many fields. Biometric systems are more convenient to use as compared with traditional authentication systems such as token based (e.g., ID cards) or knowledge based (e.g., passwords) because it alleviates the need to remember long passwords and to carry tokens with itself. It also guards the user against repudiation. Biometric-based personal authentications system may operate in two different modes: identification and verification modes [1].

In identification mode (shown in fig.1), system carries out a one-to-many comparison to set up an individual's identity. In other words, the user's input is compared with all the templates stored in system database. The purpose of identification is to answer the question: "Who am I?". Identification systems are costly to deploy and needs processing time to find a match within database.

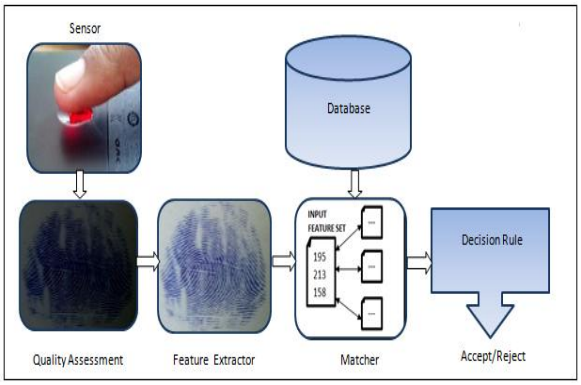

Fig.1. Identification Process

In verification mode (shown in fig.2), system carries out a one-to-one comparison to set up an individual's identity. In other words, the user claims an identity and the system verifies whether the claim is genuine or not on the basis of validating a sample collected against a previously collected biometric sample for the individual. The purpose of verification is to answer the question "Am I who I say I am"?

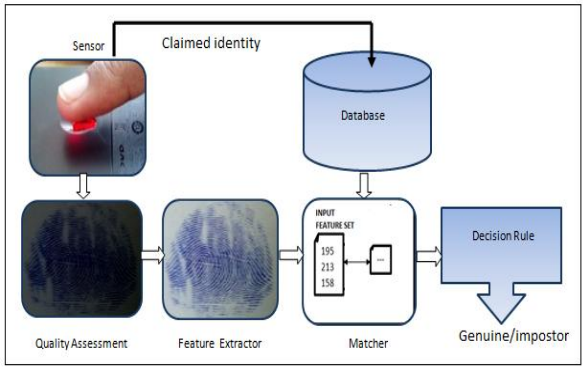

Fig.2. Verification Process

Each biometric system has four basic modules whether it is identification system or verification system. In the following section 2 biometrics system along with its four basic modules (sensor module, feature extractor module, matcher module and decision module) is explained.

2. Biometric System

All the biometric systems have four basic modules which are sensor module, feature extractor module, matcher module and decision module [2]. These four modules are necessary in any biometric system to acquire and process raw biometric data and convert it into some useful information. The block diagram of biometric system is shown in fig. 3.

2.1. Sensor Module

In this type of module raw biometric data is captured by the sensor and it scans the biometric trait to convert it into digital form. After converting it to digital form, this module transmits the data to feature extraction module.

2.2. Feature Extraction Module

It processes the raw data captured by sensor and generate a biometric template. It extracts the necessary features from the raw data which needs much attention because essential features must be extracted in an optimal way. It basically removes noise from the input sample and transmits the sample to input sample to the succeeding module known as matcher module.

2.3. Matcher Module

This module compares the input sample with the templates being stored in the database using matching algorithm and produces match score. The resulting match score is transmitted to the decision module, which decides whether to accept the individual or not.

2.4. Decision Module

After accepting the match score from matcher module, it compares the matching score against the predefined security threshold. This module accepts or rejects the individual on the basis of predefined security threshold. If match score is greater than predefined security threshold it will accept the individual otherwise reject it.

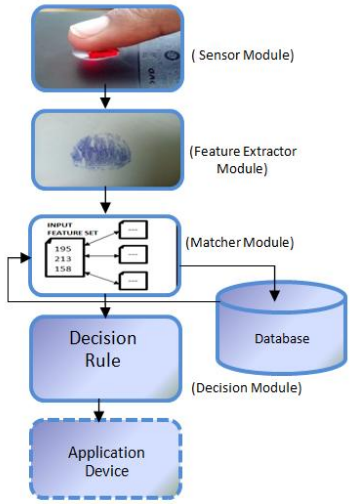

Fig.3. Biometric System

There is no doubt biometrics-based authentication systems may overcome the limitations of traditional systems (alleviates the need to remember passwords, to carry tokens, etc.) but they also possesses some limitations such as they are vulnerable to attacks. There are eight different attack points in biometric system which can be attacked and the following section 3 deals with these attack points.

3. Attacks on biometric system

Biometric based authentication systems that uses physiological (face, iris etc.) and behavioral traits (voice, signature etc.) are becoming increasingly popular and utilized in many applications to increase the security of the system. Traditional systems are unable to distinguish between an authorized person and intruder who can fraudulently access the system. Biometric systems are more convenient to use because there is no need to remember any password and with a single biometric trait different account can be secured without the burden of remembering passwords. Biometric systems offer great advantages over traditional systems but they are vulnerable to attacks [3]. There are eight attack points in biometric system which can be attacked as shown in fig.4. These attack points are divided into two categories: Direct attacks and indirect attacks.

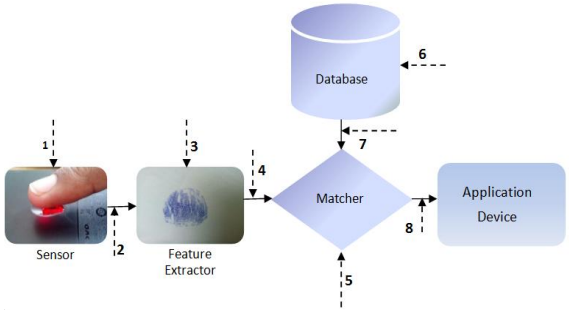

Fig.4. Attack points on biometric system

3.1. Direct attacks

It refers to the attacks that do not require any specific knowledge about the system operation such as matching algorithm used, feature vector format, etc. It includes only type 1 attack which is referred as "Sensor Attack".

3.1.1. Type 1 attack

The sensor module is vulnerable to type 1 attack which is known as "Attack at the sensor". In this attack, a fake biometric trait such as an artificial finger or facial image is presented to the sensor by an imposter to bypass recognition systems [4]. An imposter can also physically damage the recognition system and flood the system with bogus access requests. It is very easy to attack at the sensor because no specific knowledge about the system operation is needed and there is no digital protection mechanisms such as watermarking, cryptography are used at the sensor level. Sensors are unable to distinguish between fake and real characteristics of an individual and can be fooled easily by using synthetic fingerprints and facial image of a person.

3.2. Indirect attacks

Unlike direct attacks, these are the attacks where information about the inner working of the authentication system is required to make an attack successful. It includes all the remaining seven points of attack (2, 3, 4, 5, 6, 7, 8.) that can be attacked by an impostor in a biometric-based authentication system.

3.2.1. Type 2 attack

When the sensor acquires a raw biometric data, it sends the raw data to feature extractor module for pre-processing through a communication channel. This channel is in between sensor and the feature extractor module. It is intercepted to steal the biometric trait and stored somewhere. The previously stored biometric trait is replayed to the feature extractor to bypass the sensor. This is known as "replay attack" [4].

3.2.2. Type 3 attack

The feature extractor module is vulnerable to type 3 attack which is known as "Attack on feature extractor module". When the sensor acquires a raw biometric data, it sends the raw data to feature extractor module. An imposter pressurize the feature extractor module to produce the feature values chosen by the intruder instead of producing the feature values generated from the original data obtained from the sensor.

3.2.3. Type 4 attack

This attack is similar to attack of type 2 but difference is in that, an imposter intercepts the communication channel between the feature extractor and matcher modules and steal the feature values of genuine user [4]. These values can be replayed to the matcher later on. It is known as "Attack on the channel between the feature extractor and matcher".

3.2.4. Type 5 attack

A matcher module is vulnerable to type 5^{th} attack which is known as "Attack on matcher module" [5]. It is attacked to generate the high matching score as selected by the imposter to bypass the biometric authentication system regardless of the values obtained from the input feature set.

3.2.5. Type 6 attack

It occurs when the imposter compromises with the security of the database by adding new templates, modifying existing templates and removing existing templates [5]. It is not an easy task to attack system database because templates are protected by digital mechanisms such as steganography, watermarking, etc. To make successful attack on system database some knowledge of inner working of the system must be needed.

3.2.6. Type 7 attack

Attack can be made possible only when template is transmitting through communication channel between system database and matcher module. It occurs when imposter modifies or tampers the contents of the transmitted template. An imposter intercepts the channel to steal, replace or alter biometric template. It is known as "Attack on the communication channel between system database and the matcher".

3.2.7. Type 8 attack

An imposter may override the result declared by the matcher module. In this attack, imposter may tamper the match score which is transmitted through communication channel between matcher module and application device. It tampers the match score to change the original decision (accept or reject) of the matcher module.

After studying these eight attack points author observed that most of the time adversary attacks on the templates which are to be stored in database. These templates which are stored in database can be tampered by adding new templates to database, modifying existing templates in database and removing existing templates from the database. In the following section 4, the author had discussed about architecture of attack system, which explains how to made successful attack by tampering with synthetic fingerprint templates.

4. Architecture of attack system

A template is a digital reference of distinct traits that represents a set of important features extracted from the biometric data of an individual. Its nature is compact in database, due to which it infers

that template cannot reveal complete information about original biometric data. In addition, the templates are stored in an encrypted form, it is difficult to decipher and find out the contents of the stored template without knowing the suitable decrypting keys. However, an attack system presented in the literature review conflict these beliefs.

The architecture of an attack system that attacks a minutiae-based fingerprint authentication system is shown in fig. 5 [6]. The attack system consists of two subsystems: attacking system and target system. Both the subsystems consists of different modules such as attacking system consists of synthetic template generator (STG) and attack module whereas; target system consists of fingerprint matcher and template database.

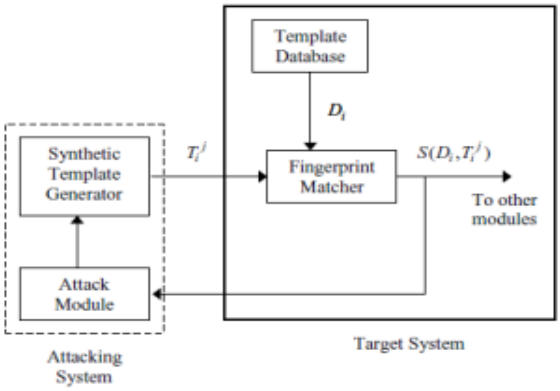

Fig.5. An Attack System Architecture

A minutiae–based fingerprint authentication system makes the use of synthetic template generator to produce synthetic fingerprint templates, which in turn makes the use of "Hill Climbing Attack" to find out the contents of a targeted fingerprint template (D_i) for the i^{th} user. The minutiae points which consist of ridge bifurcations and endings are used to create fingerprint minutiae. In general, all the minutiae based systems use the sequence of location (c, r) of the minutiae and orientation θ of the minutiae as its attributes but some systems also use ridges flow around the minutiae as supplementary information. The working of attack system begins with STG by generating a fixed number of synthetic templates (T_i^j where j= 1, 2, 3…….m) each of which composed of randomly generated minutiae points [7]. These templates are compared against the target template via the matcher and the synthetic template resulting in the best match score (S^{best} (D_i, $T_i^{\ j}$)) is retained. The template ($T_i^{\ best}$) with best score is then modified via the following four operations:

(i) the r, c and θ values of an existing minutia are perturbed.

(ii) an existing minutia is replaced with a new minutia.

(iii) a new minutia is added to the template.

(iv) an existing minutia is deleted.

If modified template results in increasing the match score then declare the modified template as $T_i^{\ best}$ and update the high match score accordingly. The current best score is then compared against decision threshold ($S^{\ threshold}$) set by the matcher and if (($S^{\ best}$ (D_i, $T_i^{\ best}$) > ($S^{threshold}$)) then stop the attack; else, the process of modifying the current synthetic template and comparing it against the target template, is repeated until the match score exceeds a decision threshold.

As discussed above biometric systems are vulnerable to attacks which can make use of various generic security threats to harm the integrity of any biometric system. These threats may result in different effects on different systems. In section 5, the author has discussed about various generic security threats which can be possible to any biometric systems.

5. Generic security threats

All traditional systems and biometric systems are susceptible to various threats [7]. These threats are as follows:

i. Denial of service: It refers to act where an imposter overwhelms the authentication system with bogus requests so that genuine users cannot use it. An authentication server that processes access requests can be loaded with many bogus access requests, to a point that all computational resources are wasted in bogus requests and cannot handle valid requests any more.

ii. Circumvention: It occurs when an imposter gains access to the system that was secured by the authentication process and manipulates the system by changing records in an unauthorized manner.

iii. Repudiation: A genuine user may access the resources of the system and claims that system had been circumvented by the imposter. For example a corrupt bank officer tampered some financial records illegally and claims that his/her biometric data has stolen.

iv. Contamination: It refers to an act where an imposter can secretly obtain biometric data of genuine users and use it to access the system in an unauthorized manner. For e.g., a biometric data associated with a specific application can be used in another application (using a fingerprint for accessing medical records instead of the intended use of office door access control).

v. Coercion: An imposter threatens the legitimate user to take the control of the system in his own hands. For e.g., an ATM user can be threaten at gunpoint.

vi. Collusion: It occurs when root or super user with high privileges makes wrong use of his privileges and modify the parameters of system illegally. A root user with wide access privileges has right to access all the system's resources.

All the threats discussed above are used to make dangerous attacks on biometric-based authentication systems. These attacks are most probably made for financial purposes such as hacking a bank account secured with biometric authentication to withdraw an amount from it, so it is necessary to resist these attacks. In following section 6, the author has discussed about various template protection techniques to resist attacks.

6. Techniques to resist attacks

All the techniques used for biometric template protection are known for resisting attacks. Some of the known biometric template protection schemes are as follows:

6.1. Liveness detection

Liveness detection is a mechanism that is used to detect that input sample feature is provided by live human being or not. It is used to prevent from attacks at sensor. It is an ability to distinguish between real input sample feature provided by living human being and a fake input feature provided by an artifact [8]. Liveness detection can be applied using software or hardware means.

- Use of extra hardware to implement liveness detection means to measure various life signs like pulse detection, blood pressure, temperature for fingerprints and movements of face, eyes for face recognition. The limitation of using extra hardware makes the system too much expensive.
- Using software means to use the information already captured to detect life signs. The only used method is to use information about sweat pores. For this a scanner that can acquire a high-resolution image is required. It is practically impossible to reproduce the exact size and position of the pores on an artificial mold.

6.2. Biometric cryptosystems

Biometric cryptosystems combines biometrics and cryptography to take advantages from the strengths of both the fields [9]. Cryptography provides higher degree of security and biometrics eliminates the need to remember any passwords or to carry any tokens. In traditional Cryptographic systems, one or more keys are used to convert a plain text into cipher text and key is known as encrypting key(s). Cipher text can be mapped back to plain text only with the help of decrypting key. If imposter obtains the cipher text he/she cannot extract useful information from it without the help of decrypting key. We use cryptographic systems to avoid dictionary attacks that can easily breaks the security of simple password based authentication systems. Biometric cryptosystems are subdivided into key generation and key binding.

- **Key generation:** In this helper data is only obtained from the biometric traits and the cryptographic key is directly generated from the helper data.
- **Key release:** In this helper data is obtained by binding a key with biometric template.

6.3. Steganography and Watermarking

Steganography means covered writing. It refers to the process in which cover image is used to hide the original data [10]. Watermarking technology is the embodiment of steganography. Steganography and watermarking are used to prevent attacks on attack points 2 (attack on the channel between sensor and feature extractor) and 7 (attack on channel between matcher and application device). These two techniques are same in their hiding method, but differ in the characteristics of the embedded data, host image and medium of data transfer. Watermarking is used in the authentication of ownership claims. Steganography can be used for transferring critical biometric information from a client to a server.

6.4. Cancellable biometrics

Cancellable biometrics is a technique that involves intentional and systematic distortion of biometric template based on a selected non-invertible transform [11]. If transformed template is misplaced then it can be cancelled and re-issued by changing parameters of template. Cancellable biometrics is used to prevent form attacks at the attack point 6 (attack on system database). It also addresses the issue of non-replaceability.

7. Conclusion

In this paper author discussed about a biometric system along with its modules and then make progress towards various attacks on biometric system. An author found that most of the attacks makes target to the biometric templates which are stored in system database. This paper also highlights various techniques to resist attacks that can be used to protect biometric templates and also discussed about generic security threats to any system. It also gives idea about steganography, watermarking, cancellable biometrics and biometric cryptosystems techniques to enhance the integrity of the biometric templates and found that there is no security technique which can

satisfy all the aspects of an ideal biometric template protection scheme. There is still need to do research work in this field so that an efficient and foolproof security technique is established.

References

[1] Tiwalade O. Majekodunmi, Francis E. Idachaba, "A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies", proc. *World Congress On Engineering* 2011; 2.

[2] Jain Anil K., Ross Arun and Salil Prabhakar, "An Introduction to Biometric Recognition", proc. *IEEE Transactions on circuits and systems for video technology*, 2004; 14 (1).

[3] Abdulmonam Omar Alaswad, Ahlal H. Montaser, and Fawzia Elhashmi Mohamad, "Vulnerabilities of Biometric Authentication "Threats and Countermeasures", proc. *International Journal of Information & Computation Technology*, 2014; 4 (10): 947-958.

[4] U. Latha and K. Rameshkumar, "A Study on Attacks and Security Against Fingerprint Template Database", proc. *International Journal of Emerging Trends & Technology in Computer Science*, 2013; 2 (5).

[5] Joseph Mwema, Michael Kimwele, Stephen Kimani, "A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates", proc. *IJCTT*, 2015; 20 (1).

[6] Uludag U. and Jain A. K., "Attacks on biometric systems: a case study in fingerprints", proc. SPIE, Security, 2004; Vol. 5306, pp. 622–633.

[7] Jain Anil K., Ross Arun, Uludag Umut, "Biometric template security: challenges and solutions", proc. Europeon Signal processing conference (EUSIPCO), September 2004.

[8] Nalinakshi B.G, Sanjeevakumar M. Hatture, Manjunath S.Gabasavalgi and Rashmi P. Karchi, "Liveness Detection Technique for Prevention of Spoof Attack in Face Recognition System", proc. *IJETAE*, 2013; 3 (12).

[9] Christian Rathgeb and Andreas Uhl, "A survey on biometric cryptosystems and cancellable biometrics", proc. *EURASIP Journal on Information Security*, March 2011.

[10] Jasleen Kour and Deepankar Verma, "Steganography Techniques –A Review Paper", proc. *International Journal of Emerging Research in Management &Technology*, 2014; 3 (5).

[11] Supriya V G, S Dr Ramachandra Manjunatha, "Chaos based Cancellable Biometric Template Protection Scheme-A Proposal", proc. *International Journal of Engineering Science Invention*, 2014; 3 (11):14-24.