A Review Of Various Attacks On Biometrics System And Their Known Solutions

Kamaldeep
Assistant Professor
Savera Group of Institutions (Gurgaon)
kamalmintwal@gmail.com

Abstract— In the current digital world we have various authentication systems which identify an individual. For example biometrics authentication system, knowledge based authentication system, token based authentication system. These systems have their own advantages and disadvantages. One system removes the disadvantages of other. A biometrics system is known as one of the robust system. But it also falls into several of attacks, which have been discussed in this paper. Also the known solution has been discussed. So that we can make a more robust authentication system.

Keywords- Biometrics, Authentication, Attacks on biometrics, Security, Watermarking, Steganography etc.

I. INTRODUCTION

Now a days people are moving towards the digital world, the increasing number of application makes use of networks for example E-commerce, banking, and other authentication system. Which lead to the various theft problems and other typed of attacks on this system. So, the design of the appropriator authentication system is more and more important. In the recent time the traditional authentication system were used for authentication purpose. This system was not the appropriate system for authentication and had several disadvantages like stolen of password, forgotten of the password, time consuming, password guess for easy password etc. To remove these types of disadvantages biometrics system came into existence. Biometric systems offer several advantages over traditional authentication methods. Biometric information cannot be acquired by direct covert observation. It is impossible to share and difficult to reproduce. It enhances user convenience.
by alleviating the need to memorize long and random passwords. It protects against repudiation by the user. Biometrics provides the same level of security to all users unlike passwords and is highly resistant to brute force attacks. Beside of these advantages the biometrics authentication system has

several type of attack which is being discussed in the paper. Some of These attacks can be removed by watermarking and steganography. The role of watermarking and steganography in the biometrics authentication system can be shown in the fig 1.

II. KNOWN ATTACKS ON A BIOMETRIC SYSTEM

In spite of numerous advantages of biometrics-based personal authentication systems over traditional security systems there are many vulnerable affect the biometrics system. These vulnerable decreases the security of the biometrics system decrease their security considerably. This chapter discusses about various attacks on the biometrics authentication system and different schemes and methods to secure the biometric system from these attacks given by the previous researcher. At the last of this chapter the comparison of various security schemes has been discussed.

Biometrics work well only if the verifier can verify two things:

- The biometric came from the genuine person at the time of verification.
- The biometric matches the master biometric on file [1].
But a variety of problems hinder the ability to verify the above [2].

- Noise in acquired data – Noisy biometric data caused by defective sensors, defective physical characteristics and unfavorable ambient conditions. This causes the data to be incorrectly matched or incorrectly rejected.
- Intra-class variations – The data acquired during authentication may be different from the data used to generate the template during enrollment, affecting the matching process.
- Distinctiveness – Every biometric trait has an upper bound in terms of its discrimination capabilities.
- Non-Universality – A subset of the users not possessing a particular biometric.

The above-mentioned problems form the basis for many types of attacks against biometric systems.

Various researchers defined many attack on the biometrics system which can be classified into two categories:

**BIOMETRIC SECURITY THREATS**

Ratha et al. analyzed these attacks and grouped them into eight classes [3]. Fig. 2 shows the locations of these attacks in a biometric system. Jain et. al. proposed a 9th attack on the biometrics system. These points of attack are discussed in below.

- **Type 1:** The type 1 attack is point out the “attack on the sensor”. In this attack, the attacker presents fake biometrics traits on
the sensor and gets the access to the authentication system.

- **Type 2:** This point of attack is known as “Attack on the channel between the scanner and the feature extractor” or “Replay attack”. In this attack, the attacker intercepts the communication channel between the scanner and the feature extractor to steal biometric traits and store it somewhere. The attacker can then replay the stolen biometric traits to the feature extractor to bypass the scanner.

- **Type 3:** This point of attack is known as “Attack on the feature extractor module”. In this attack, the attacker can replace the feature extractor module with a Trojan horse. Trojan horses in general can be controlled remotely.

- **Type 4:** This point of attack is known as “Attack on the channel between the feature extractor and matcher”. In this attack, the attacker attacks 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.

- **Type 5:** This point of attack is known as “Attack on the matcher”. In this attack, the attacker replaces the matcher with a Trojan horse. The attacker can send commands to the Trojan horse to produce high matching scores and send a “yes” to the application to bypass the biometric authentication mechanism.

- **Type 6:** This point of attack is known as “Attack on the system database”. In this attack, the attacker breaks the security of the database where all the templates are stored. Compromising the database can be done by exploiting vulnerability in the database software or cracking an account on the database. In either way, the attacker can add new templates, modify existing templates or delete templates.

- **Type 7:** This point of attack is known as “Attack on the channel between the system database and matcher”. In this attack, the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data.

- **Type 8:** This point of attack is known as “Attack on the channel between the matcher and the application”. In this attack, the attackers intercept the communication channel between the matcher and the application to replay previously submitted data or alter the data.

- **Type 9:** This attack is called “Attack on the application” [4]. Bugs are a
consequence of the nature of the programming task that no one can deny. It is a fact that any software has at least one bug in it. Since biometric authentication systems are not 100% accurate, most of these systems use traditional authentication schemes as a backup.

**GENERIC SECURITY THREATS**

Maltoni et al. described typical threats for a generic authentication application. Any system (including biometric systems) is susceptible to various types of threats [6]. These threats are discussed below:

- **Denial of Service:** An adversary overwhelms computer and network resources to the point that legitimate users can no longer access the resources.
- **Circumvention:** An adversary gains access to data or computer resources that he may not be authorized to access.
- **Repudiation:** A legitimate user accesses the resources offered by an application and then claim that an intruder had circumvented the system.
- **Covert acquisition:** An adversary compromises and abuses the means of identification without the knowledge of a legitimate user.
- **Collusion:** In any system, there are different user privileges. Users with super-user privileges have access to all of the system’s resources. Collusion occurs when a user with super-user privileges

---

*Fig.3 Types of Attacks on Biometrics System [5]*
abuses his privileges and modifies the system’s parameters to permit incursions by an intruder

- **Coercion:** A legitimate user is forced to give an intruder access to the system. For example, an ATM user could be forced to give away her ATM card and PIN at gunpoint

## III. KNOWN TECHNOLOGIES TO RESIST THE ATTACKS

**LIVENESS DETECTON MECHANISMS**

Liveness detection can be used to thwart the attacks at attack point: 1 (attacking the sensor). Liveness detection refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artifact. Liveness detection can be implemented using software or hardware means.

- Using extra hardware to acquire life signs like temperature, pulse detection, blood pressure etc for fingerprints and movements of the face for face recognition. Iris recognition devices can measure the involuntary papillary hippos (Constant small constrictions and dilations of the pupil caused by spontaneous movements of the Iris). The drawback is that extra hardware makes the system expensive and bulky. Using the information already captured to detect life signs. The only researched method is using information about sweat pores. For this a sensor that can acquire a high-resolution image is required. It is difficult to reproduce the exact size and position of the pores on an artificial mold.

- Using liveness information inherent to the biometric being obtained. For fingerprints, using a side impression near the nail, which has been enrolled earlier, can do this. The advantage is that people do not leave side impressions as latent prints and no major changes in the scanner is needed to acquire this additional information. A system that uses multiple instances of the same biometric can be used for liveness detection by asking the user to provide a random subset of biometric measurements, for e.g. left index finger followed by right middle finger [7].

Liveness detection can also be done through challenge-response like passing a small impulse current to the finger and capturing the fingers, response. Also, a new research is being done by the biomedical signal analysis laboratory at West Virginia University on an algorithm based on the detection of perspiration in a time progression of fingerprint images. Liveness detection through perspiration patterns is based on the fact that the
perspiration changes the fingerprint image darkness over time. In addition to the technical procedures, procedural techniques like supervision are highly efficient for liveness detection.

STEGANOGRAPHIC AND WATERMARKING TECHNIQUES

Steganographic and Watermarking techniques are used to resist attacks at the attack points 2 and 7 (Channel between the sensor and feature extractor and also the channel between the stored template and the matcher). Steganography meaning secret communication, it involves hiding critical information in unsuspected carrier data. Steganography based techniques can be suitable for transferring critical biometric information from a client to a server. There are two application scenarios where hiding method is the same, but differs in the characteristics of the embedded data, host image and medium of data transfer [8].

![Steganographic Techniques Diagram]

---

Fig. 4 Steganographic techniques
Fig. 5 Watermarking Techniques
In the first scenario the biometric data that need to be transmitted is hidden in a host or carrier image whose only function is to carry the data. The carrier image can be a synthetic fingerprint image, a face image or any arbitrary image. Using such a synthetic image to carry actual fingerprint data provides good security since the person who intercepts the carrier image might treat that image as the real fingerprint image. The security of transmission can be further increased by encrypting the stego image before transmission.

In the second scenario an additional biometric (e.g. Face) is embedded into another biometric (e.g. Fingerprint) in order to increase the security of the latter and stored on a smart card. At the access control site, the fingerprint of the person is compared to the fingerprint on the smart card. Then the face information hidden in the fingerprint is recovered and used as a second source of authenticity either automatically or by a human in a supervised biometric application.

Ratha proposes a water marking technique applicable to fingerprinting images compressed with WSQ wavelet-based scheme [9]. The discrete wavelet transform coefficients are changed during WSQ encoding by taking into consideration possible image degradation. This method is used to secure biometric authentication systems for commercial transactions against replay attacks. To achieve this, the service provider issues a different verification string for each transaction. The string is mixed with the fingerprint image before transmission. When the image is received by the service provider it is decompressed and the image is checked for a one-time verification string. Here, the message is not hidden in a fixed location, but is deposited in different places on the structure of the image so that it cannot be easily recovered. Spatial domain water marking methods for fingerprint images and utilizing verification keys are also available. Water-marking the information in the biometric template database allows for the integrity of the contents to be verified when retrieved for matching.

**CHALLENGE RESPONSE SYSTEMS**

Challenge-Response systems can be used to prevent replay attacks at attack points 2 and 7. One approach is the image based challenge-response method where the challenge is presented to the sensor and the response string computed depends on the challenge string and the content of the input image acquired [10]. In another approach the verification data to be transferred to the smart card for on-card matching is protected with a cryptographic checksum that is calculated within a security module controlled by a tamper resistant card terminal with integrated biometric sensor [11].

**MULTI-MODEL BIOMETRIC SYSTEMS**

Multi-model biometric systems can be used to resist spoofing attacks (attacks at point 1). Multi-model Biometric systems use multiple
representations of a single biometric, a single biometric with multiple matchers or multiple biometric identifiers [12]. These systems can address the problem of non-universality since multiple traits can ensure sufficient population coverage. They can be used to counteract spoofing attacks, since it is difficult for a hacker to simultaneously spoof multiple biometric traits of a legitimate user. The choice and the number of biometric traits is decided by the nature of the application, the computational demands and costs introduced, and the correlation between the traits considered. The fusion of the multiple traits can be done at the feature extraction level, the matching score level or the decision level. At the feature extraction level, the feature sets of multiple bimodalities are combined to generate a new one, which is then used in matching and decision-making. At the matching level, the scores produced by each biometric subsystem are integrated using different techniques like weighted averaging to generate a new score which is then compared with the threshold to make the accept or reject decision. At the decision level each biometric system makes its own decision and a majority-voting scheme is used to make the final decision. Usually fusion at the matching score level is preferred because different biometric traits can be given varying degrees of importance based on their strength and weaknesses for different users. The problem of noise in the acquired data can be reduced by using multi-model biometrics and assigning different degrees of importance for the different traits. This, in turn, results in improved matching performance and accuracy that makes spoofing attacks more difficult. Since the multi-model biometric system introduces computational and cost overheads, the cost versus performance trade-off should be studied before deploying these systems.

SOFT BIOMETRICS

Soft biometrics can be used to thwart attacks at the attack points 1 and 8 (attacks on the sensor and decision maker). Soft Biometric traits are those characteristics that provide some information about the individual, but lack the distinctiveness or permanence to sufficiently differentiate any two individuals (gender, ethnicity, age, height, weight etc) [13]. Most of the biometric systems collect ancillary information about the users during enrollment, which is stored either in the database or in the smart card possessed by the user. The ancillary information collected together with the matching scores will lead to the correct identification of the user, which in turn prevents spoofing. The factors like age, gender, color, etc can affect the performance of a biometric system. The use of soft biometric traits helps to filter a large biometric database to get a reduced number of templates to do the comparison with, which in turn, will improve the speed and efficiency of the biometric system. Soft biometric traits can also be used for tuning the parameters of a biometric...
system like the threshold on the matching score in a uni model system, and the thresholds and weighing of different modalities in a multi-modal biometric system to obtain the optimum performance for a particular user or class of users. Incorporating soft biometrics will reduce FAR and FRR errors which in turn prevents spoofing.

CANCELABLE BIOMETRICS

Cancelable biometrics can be used to resist attacks at point 6 (template database). Cancelable biometrics involves an intentional repeatable distortion of a biometric signal based on a chosen noninvertible transform [14]. This reduces the stored template compromise by using the legitimate substitution of a transformed version of a template for matching against a similarly transformed vector. Cancelable biometrics also addresses the issue of non replaceability of biometric systems. Here, cancellation simply requires the specification of a new distortion transform. The distortion transforms selected are non-invertible so that the original biometric cannot be recovered even if the transform function and the transformed biometric data are known. The transform can be applied to the acquired signal or the features extracted from it. Signal level transforms include grid morphing and block permutation. Feature level transform is usually a set of random, repeatable permutations of feature points. Cancelable biometrics is especially useful when an individual user is subscribed to multiple services. Here, privacy and security are enhanced because different distortions can be used for different services and true biometrics are never stored or revealed to the authentication server.

IV. COMPARISON OF VARIOUS METHODS

The table given below gives a comparison of the advantages and drawbacks of the different protection techniques.
Table 1 Advantages and Drawbacks of the Different Protection Techniques.[15]

<table>
<thead>
<tr>
<th>Technique</th>
<th>Advantages</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liveness Detection</td>
<td>Resists spoofing attacks.</td>
<td>Increased cost for the extra hardware and software, user inconvenience and increased acquisition time.</td>
</tr>
<tr>
<td>Watermarking</td>
<td>Prevents replay attacks and provide integrity of the stored templates.</td>
<td>Problem of image degradation and lack of algorithms to deal with it.</td>
</tr>
<tr>
<td>Soft Biometrics</td>
<td>Provides improved performance through filtering and tuning of parameters.</td>
<td>Lack of techniques for automatic extraction of soft biometric techniques.</td>
</tr>
<tr>
<td>Multi-model Biometrics</td>
<td>Improves performance, resists spoofing and replay attacks and provides high population coverage.</td>
<td>Increased system complexity, computational demands and costs.</td>
</tr>
</tbody>
</table>

V. CONCLUSION AND FUTURE SCOPE

As computer growing rapidly, all the people rely on the computer directly or indirectly. So the need of secure authentication system is a mandatory issues. Today the biometrics authentication system is considering most secure system. But as we have discussed above, the biometrics system is also has some limitation. In this paper, we have studied various attacks on biometrics system. Also some known solution for these attacks. Steganography, in its multitude of forms, has been in use literally for thousands of years. It appears to have been utilized primarily and most effectively in time of war or civil strife. With the advancement in technology improvements are done on Steganography techniques as well as watermarking techniques. So it will focus to develop more secure and robust biometric system with help of steganography and watermarking technique.
REFERENCES


