Pitfalls in “part of yours” System: Biometrics

Garima Yadav
Bharati College
Delhi University

Nikita Yadav
Bhagini Nivedita College
Delhi University

ABSTRACT

Security? Yes, security in itself is the biggest concern today. From ancient time to present we have come a long way from “something you know” (e.g., password, Personal identification number- Knowledge based approach), to “something you carry” (e.g., physical key, ID card- token based approach) and to “something you are” (e.g., face, voice) [1]. All these methods of establishing the identity of the persons have their own advantages and limitation. But out of these three “something you are” is the latest, gaining popularity and used all over the world. This method is known as “Biometrics”, but this system is also having some pitfalls. In this paper we are trying to present the pitfalls in the biometric system.

Keywords

Biometrics, Security

1. INTRODUCTION

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual. Biometric data could be physical or behavioral body trait of a person. Examples of physical traits include face, fingerprint, iris, palm print, hand geometry and ear shape. Gait, signature and keystroke dynamics are some of the behavioral traits of a person.Fig1 showing some of physical and behavioral traits. A biometric system can work in two modes:

a. Verification is generally 1:1 process, the user claims an identity and the system verifies whether the claim is genuine or not. In this process user’s data is compared with the data of the person he/she claims to be. When biometric are implemented for verification purposes, they will answer the question: “AM I WHO I SAY I AM?”[2]

b. Identification can be viewed as 1: many process. Identification can be classified as positive and negative identification. In identification process, system verifies the user’s identity with the other present identity in the system database. They will answer the question “WHO I AM”. Negative identification is also known as screening. Screening is often used at airports to verify whether a passenger’s identity matches with any person on a “watch-list”.[3]

Figure1: representing some of the physical (iris, hand geometry, finger print, face) and behavioral traits (keystroke, walk, and signature)

2. BIOMETRICS MODULES

Biometric system works in four stages [4]. Figure2 shows the Basic Structure of a Biometric Authentication System

2.1 Enrollment Unit

This unit is also called sensor module. It acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal.

2.2 Feature Extraction Unit

The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user’s identity, is stored in the biometric system and is known as a template.

2.3 Matching Unit

This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user’s master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one too many matching).

2.4 Decision Maker

This module accepts or rejects the user based on a security threshold and matching score.

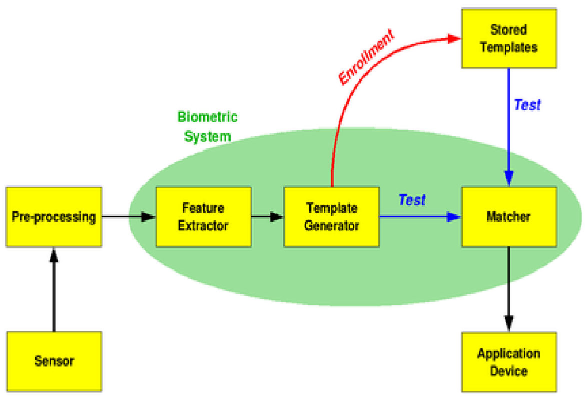

Figure 2: Basic Structure of a Biometric Authentication System

3. BIOMETRICS- DEFORMITY (FACTORS, CAUSING BIOMETRIC SYSTEMS TO FAIL)

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted; it is possible to locate and minimize factors [5] that can reduce/affect system performance. These factors are known as Biometrics- Deformity.

3.1 Fingerprint

Biometric system which uses the fingerprint as its biometric trait uses the tip of finger to takes the measurement of ridges and minutia point in the finger, which is a small area and it's very difficult to take measurement from there. This task became more complicated when following conditions are reverse at the time of enrollment:

- Cold finger
- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Cuts to fingerprint

3.2 Voice recognition

Voice biometrics uses the pitch, tone, and rhythm of speech and all these factors can get affected by one of the following reasons

- Cold or illness that affects voice
- Different enrollment and verification capture devices
- Different enrollment and verification environments (inside vs. outside)
- Speaking softly
- Variation in background noise
- Poor placement of microphone/ capture device
- Quality of capture device

3.3 Facial recognition

Face recognition uses the spatial geometry of distinguishing features of the face. Any change in these features can lead to the improper working of biometric system such as:

- Change in facial hair
- Change in hairstyle
- Lighting conditions
- Adding/removing hat
- Adding/removing glasses
- Change in weight

3.4 Iris-scan

Iris recognition solutions measure the unique patterns in the colored circle around the pupil to identify and authenticate. Following things can become the barrier in the working of iris based biometric system.

- Too much movement of head or eye
- Glasses
- Colored contacts
- Retina-scan
- Too much movement of head or eye

3.5 Hand geometry

Biometric system uses hand geometry as biometric trait mainly include characteristics like thickness of the palm area and width, thickness and length of the fingers. These characteristics may be affected by:

- Jewellery
- Change in weight
- Bandages
- Swelling of joints

3.6 Signature-scan

Signature scan system works by analyzing the shape, speed, stroke, pen pressure and timing information during the act of signing. This can be affected by:

- Marking too quickly
- Different marking positions (e.g., sitting vs. standing)

In addition, for many systems, an additional strike occurs when a long period of time has elapsed since enrollment or since one's last verification. If significant time has elapsed since enrollment, physiological changes can complicate verification. If time has elapsed since a user's last verification, the user may have "forgotten" how he or she enrolled, and may place a finger differently or recite a pass phrase with different intonation. The performance of many biometric systems varies for specific populations.

4. CHEATING A BIOMETRIC SYSTEM

Security of the biometric system is very important. All security systems are not fool proofed; all systems have some limitations because of which security came at risk. Same is with the biometric system despite of having many advantages biometric system is also having few weak points. A biometric system can be fooled or cheated at the various levels. Figure3 is showing some such points in the biometric system.

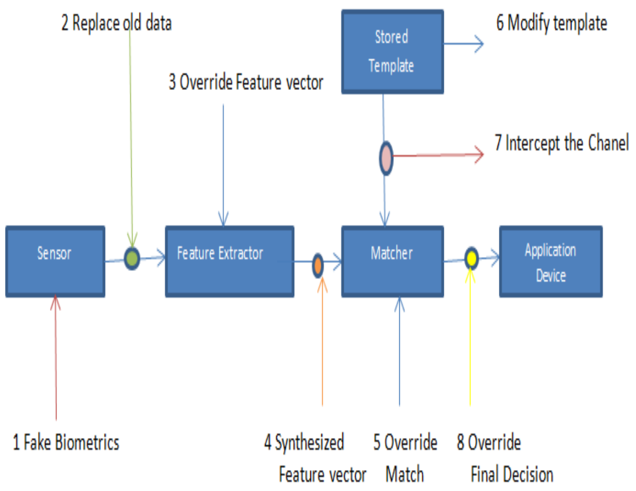

Figure3: How to Cheat the Biometric System

a. **Fake Biometric :** A biometric system may be faked by presenting the artificial finger at the sensor **[6]**

b. **Replay old data:** illegally intercepted data may be resubmitted to the system,

c. **Override Feature Extractor:** The feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets.

d. **Synthesized Feature Vector:** Legitimate feature sets may be replaced with synthetic feature sets.

e. **Override Matcher:** The matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security.

f. **Store Template:** The templates stored in the database may be modified or removed, or new templates may be introduced in the database.

g. **Interpret Channel:** The data in the communication channel between various modules of the system may be altered, and

h. **Override Final Decision:** The final decision **[7].**

5. CONCLUSION AND FUTURE WORK

In this paper we tried to put forward some of the pitfalls in the present biometric system. Despite, of all these limitations biometric system is gaining popularity and acceptance all over. Even today it is the safest and more reliable system for the authentication of the person and security and we cannot ignore its advantages. In this world of technology everyone is educated today. This may be because technology is becoming easier to use. Business organizations and individuals think and spend more on security. Therefore, understanding biometrics from both the individual's perspective and from the organization that is implementing it is very important.

Steps has been taken to overcome the pitfalls in the biometric system, introduction of the multibiometric system is step forward in this direction. Multibiometric system consolidates evidence from multiple sources of biometric information in order to reliably determine the identity of an individual is known as multibiometric systems [8]. Multibiometric systems can alleviate many of the limitations of unibiometric systems because the different biometric sources usually compensate for the inherent limitations of the other sources [9]

6. REFERENCES

[1] IBM Corporation. The Consideration of Data Security in a Computer Environment. Technical Report G520-2169, IBM, White Plains, USA, 1970.

[2] www.globalseci.com/?pageid=37

[3] karthikNandKumar_Multibiometric System_phd08.pdf

[4] Kant Chander, Nath Rajender, Chaudhary Sheetal "Biometrics Security usingSteganography," cssjournals.com/Journals/IJS/Volume2/Issue1/IJS-5.pdf

[5] Heckathorn, D.D., Broadhead, R.S., Sergeyev, B.: A Methodology for ReducingRespondent Duplication and Impersonation in Samples of Hidden Populations. In: Annual Meeting of the American Sociological Association, Toronto, Canada (1997)

[6] U.K. Biometric Working Group, "Biometric security concerns," Technical Report, CESG, September 2003, http://www.cesg.gov.uk/site/ast/biometrics/media/ BiometricSecurityConcerns.pdf.

[7] A. Adler, "Can images be regenerated from biometric templates?," in Biometrics Consortium Conference, (Arlington, VA), September 2003.

[8] A. Ross, K. Nandakumar, and A. K. Jain. Handbook of Multibiometrics. Springer, 2006.

[9] L. Hong, A. K. Jain, and S. Pankanti. Can Multibiometrics Improve Performance? In Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), pages 59–64, New Jersey, USA, October 1999.