Open access Journal International Journal of Emerging Trends in Science and Technology

Biometric Another Way of User Authentication

Author
Mamta Gupta
Shyam Lal College, Computer Science Department, University of Delhi,
Email: *Mamta07_gupta07@yahoo.com*

Abstract
Biometric system is a pattern recognition system that recognizes the user's identity through their physical or behavioral traits. In this work, an attempt has been made to show you that how the biometric authentication system works and at what level it will be secure and accurate to authenticate the user's identity.
Keywords: *Authentication, Verification, Identification, Enrollment, Biometric, Security.*

1. Introduction

Biometric technology is a method of recognizing the identity of a person based on physiological or behavioral traits. The biometric system scans the individual's physical attributes after verifying it (physical attributes) system allow the user to login, or allow to access the resources/sensitive data. Currently the options available for user are - what he has (means the user has token, cards like smart card or debit card), what he knows (means pin or password), what he is (means his physical/behavioral attributes). Biometric authentication falls into what he is category. Today's time our first priority is to secure the information and the biometric authentication can provide the highest level of security.

2. Biometric recognition works generally in four steps

- Sample acquisition- biometric data are collected using an appropriate sensor.
- Feature extraction- after collection of biometric data it converted into templates (digital data).
- Storage- after generation of templates it will be stored in memory devices, choice of memory devices, depends on the application.
- Matching- this step is used to authenticate the user by comparing his biometric templates with existing templates that is stored in the database.
- Decision- this step uses the result of matching step. Based on the result user will be authorized to access the resources or not.

3. How it works for user authentication

Biometric system is a pattern recognition system that recognizes the user's identity through their physical or behavioral traits. For using biometric system authentication, the user has to firstly enroll in biometric systems. Based on application context, biometric system operates in one of two modes (verification/identification) for user authentication.

3.1 Enrollment

During enrollment, features of the individual are extracted from the sensor or user interface, then features are converted into templates, after that templates are stored in the system database.

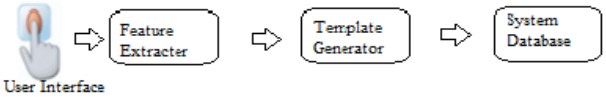

Figure 1: Enrollment

3.2 Verification (one to one match)

Verification validates a person's identity by comparing his captured biometric traits with the specific biometric template (digital form of biometric data) that is stored in system database. Verification method can be used either centralized storage or distributed storage.

Verification with centralized storage- database exists in a centralized mode in which all biometric templates are stored. From the system database, a specific template is retrieved for comparison with live person's physical/behavioral traits. And both data can be either match or not. Two types of error possible in verification- false match/false positive, false negative/false rejection.

False matches/false positive-A person is not who he claims, but the system accepts it, Acceptance of pretender.

False rejection/false negative- A person is who he claims to be but the system fails to accept, rejection of legitimate person.

False rejection will cause unnecessary inconvenience to an innocent individual, whereas the false match is more dangerous as they allow an imposter to pass.

Verification with distributed storage- biometric data stored in a memory device that is carried by individual, for example, smart card, In which biometric data of individuals are stored. Verification is done by comparing biometric data which are provided by an individual's memory device like smart card with a specific template stored in the system database. Like, verification with centralized storage, false acceptance and false rejection errors are possible Verification with distributed storage technique. Unlike, verification with centralized storage, memory device like token or smart card can be damaged or can be tampered.

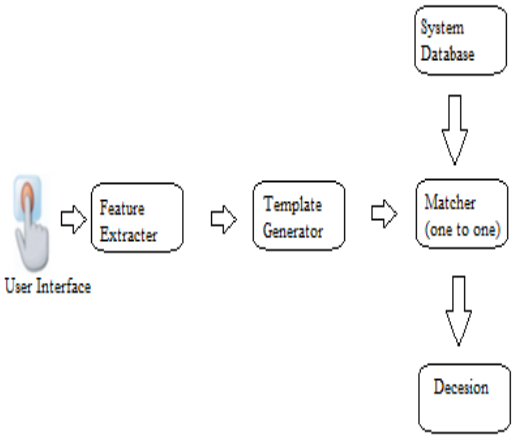

Figure 2: Verification

3.3 Identification (one to many match)

This technique is used to discover the identity of a person when the identity is unknown; in this mode biometric data of the individual is captured and compared with all templates which stored in the system database. To determine the identity of the unknown person, database of templates is required that contains biometric templates of all people known to the system. Identification not possible without database of templates. Like verification, identification can also produce two types of error, false match or false reject.

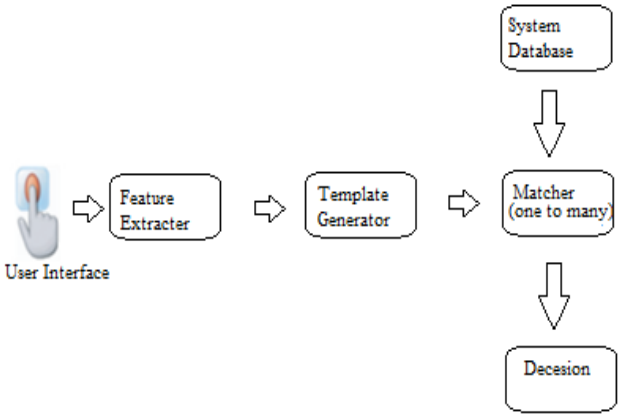

Figure 3: Identification

4. TYPES OF BIOMETRICS

- Physical traits
- Behavioral traits

4.1 Physical traits

Generally, physical biometrics includes five factors of physical attributes that are used or can be used in user authentication

4.1.1 Fingerprint scan

Among all the biometric techniques, this is the oldest method which has been successfully used in numerous applications. For example, fingerprint scan use in forensic for criminal identification, use in attendance system. Because the patterns of ridges on the fleshy part of fingertips are unique. No two individuals even twins have same fingerprints. The patterns of ridges leave impression on whatever they touch. Injuries such as minor burns or cuts do not mop out or change the pattern , the new skin grows showing the same pattern.

4.1.2 Retina or iris scan

These have been used to confirm a person's identity by reading the arrangement of blood vessels in the retina or patterns of color in the iris. It is very reliable technique and difficult to map by forgers.

4.1.3 Facial recognition

This technique use unique facial attributes to identify an individual. Biometric facial recognition systems generally read the overall structure, shape and proportions of the face taking into account the distance between the eyes, nose, mouth, and jaw edges, upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, etc.

4.1.4 Finger vein recognition

The technology of finger vein recognition is quite younger then fingerprint or facial recognition system. Finger vein recognition system uses pattern-recognition techniques based on images of human finger vein patterns under the skin's surface. Key advantage of vein patterns for biometric identification is that the forgers cannot easily create a copy of finger vein due to lack of known method, as it is possible with fingerprints.

4.1.5 Palm vein recognition

As the blood vessels zigzag beneath our skin these give a unique pattern that can be used to identify a person. Infrared beam is used to enter in the hand and the veins in the person's palm show up as black lines .Like the finger vein , Palm vein also cannot be easily forged. Due to that they can provide highest level of security.

4.2 Behavioral traits

Behavioral biometrics includes voice, signature and keystroke traits.

4.2.1 Voice scan

It uses a voice print that analyses how a person says a particular word or sequence of words unique to that individual.

4.2.2 Signature scan

Signature scan is a method of, examining an individual's signature. This technology examines speed, direction, and pressure of writing, total time of the signature. Unfortunately, signature is one of the least reliable methods of Identification. Forgers have number of ways to reproduce a signature that looks similar to the owner.

4.2.3 Keystroke scan

It is a method of, examining an individual's keystroke on a keyboard. This technology examines speed and pressure, the total time of typing a particular password, and the time a user takes between hitting certain keys.

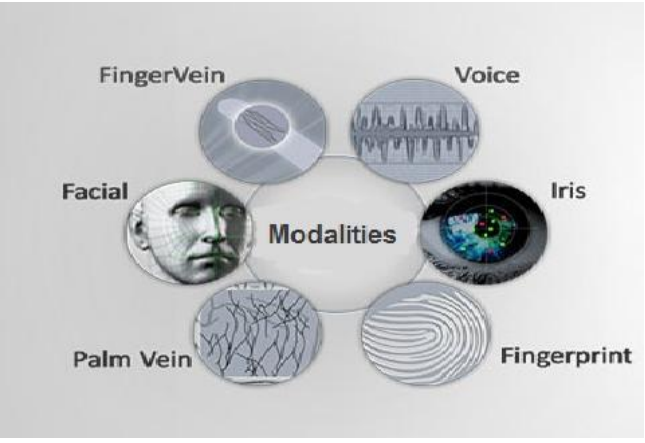

Figure 3: Physical and Behavioral traits

5. Biometric privacy and security issues

Whenever we talk about biometric authentication people always want to know about the security level of personal data. They want to know who will access the system. Will the imposter, or some other group, be able to get personal information about the users? Because, if a biometric data is ever compromised, it is compromised forever.

Disadvantages of biometric that they will change, as your age, as your occupation. Also they can change or damaged due to suffering from physical injuries or diseases. Like, password or card biometric data cannot be changed after any misshaping. With a credit card, the bank can issue the user a new card with a new number. Also password can be changed if password stolen. But a user has only a limited number of biometrics—one face, 10 fingers, and so on. And they are not easy to replace. Also, because different applications might use the same biometric, an intruder who acquires a person's biometric in one application could also use it on the others.

Compromising of individual attributes cannot always be prevented by protecting database and transmission channels because biometric attributes, although privately owned, are sometimes publicly observable (e.g. a photo of a person's face can be taken with a camera or downloaded from social site, voice can be recorded).

In general, biometric attribute are not secret, still it might be quite complicated to reproduce it (e.g. a retinal map) without the cooperation of the owner. When used for security, biometric characteristics are more like public keys than private keys. Unlike public keys, however, biometric attributes cannot be easily revoked.

Advantage of biometric data is that, they cannot get stolen, lost, replicated or forgotten like password or token, cards. They also can not be forgotten, compromised, shared, observed or guessed like password, secret codes or PIN. You don't need to change biometric data from time to time as you do with passwords. No need to write them as most people write password. Due to high security level and accuracy of biometric authentication, government agencies are also attracted towards the biometric authentication method, for example Indian government used this technology to recognize country's people and name of this program is adhaar .

Conclusion

Although biometrics technology provides a strong user authentication solution, there are other Factors to be considered in the authentication protocol. When a high level of security is needed, you can combine other authentication factors with biometrics. When you combine what you know, what you have, and what you are, you will attain the highest level of security across multiple applications and systems.

References

[1] A.K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, 1999.

[2] Salil Prabhakar, Sharath Pankanti, Anil K. Jain., Biometric Recognition: Security and Privacy Concerns, published by the IEEE COMPUTER SOCIETY, 2003.

[3] Biometric Authentication method Pro's and Con's, http://www.idcontrol.com/keystroke-biometrics/biometric-authentication-methodpros-and-cons.

[4] Biometrics and User Authentication, SANS Institute 2002.

[5] James Wayman, Anil Jain, Davide Maltoni and Dario Maio (Eds), Biometric Systems Technology- Design and Performance Evaluation, Springer Science & Business Media, 2005.

[6] Biometrics: Today's Choice for the Future of Authentication, 2015, http://resources.infosecinstitute.com/biometricstodayschoicefutureauthentication.