International Journal of Scientific Research in Computer Science and Engineering

ISROSET

Review Paper

Volume-1, Issue-2, Marh-April-2013

Available online at www.isroset.org

ISSN No. 2320-7639

Security and Privacy in Biometrics: A Review

Amandeep Kaur Bhatia[1] and Harjinder Kaur[2]

[1]Department of Computer Science & Engineering,Punjabi University, India, amansviet@gmail.com

[2] Department of Computer Science & Engineering, Punjabi University, India, hksaini2006@yahoo.co.in

Abstract— **The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).It refers to the Automated Recognition of Individuals based on their physiological or behavioural traits like fingerprints, hand geometry, face, iris recognition, signature, voice and many more. By using biometrics it is possible to confirm or establish an individual's identity based on "who she is" ,rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password).In this Paper, we give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.**

Keywords- Biometrics; Recognition; Verification; identification.

I. INTRODUCTION

As a person requirements increase, a person has to remember lots of pin numbers, account numbers, passwords and other security codes. The weak passwords can be easily guessed and the strong ones can be hacked or broken. Once an intruder gets the user ID and password, the intruder has total access to the user's resources. It is suggested that people should not use same password for different applications.

In the modern world, that would mean memorizing a large number of passwords. Biometric is most suitable solution to all these requirements. In the future the biometric system will be more convenient and reliable. Biometric refers to the automated recognition of individual based on their physiological or behavioral trait [1]. Physiological traits include iris, face, hand, finger images and behavioral traits include keystroke dynamics, signature verification, speaker verification etc.

Biometric authentication system requires comparing an enrolled biometric sample against a newly capture biometric [3], for example a hand geometry captured during login. During enrollment a sample of the biometric data is captured, processed by the computer and stored for later comparisons. Biometric recognition can also be used in identification mode where the system identifies a person from entire stored population by searching a database for a match based on biometric. It is called one to many matching and verification mode is called one to one matching [3]. Biometrics can be used to identify you as you.

II. *WORKING OF BIOMETRIC TECHNOLOGY:*

At their most basic level, biometric technologies are pattern recognition systems that use either image acquisition devices, such as scanners or cameras in the case of fingerprint or iris recognition technologies, or sound or movement acquisition devices, such as microphones or platens in the case of voice recognition or signature recognition technologies, to collect the biometric patterns or characteristics.

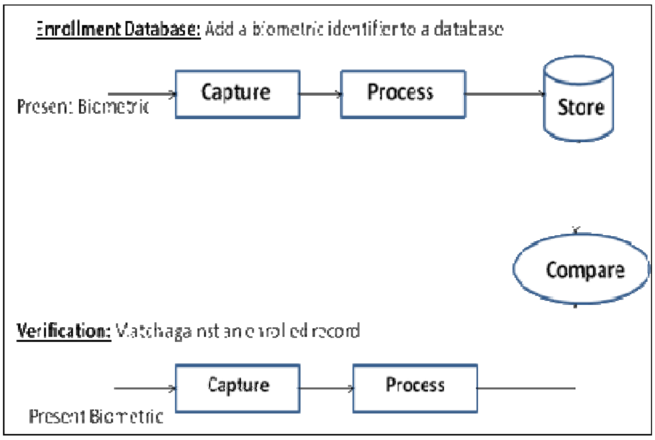
Enrollment Database: Add a biometric identifier to a database
Present Biometric
Capture
Process
Store
Compare
Verification: Match against an enrolled record
Capture
Process
Present Biometric

Figure 1: Generic Biometric Process **Error! Reference source not found.**

The characteristics of the acquired samples considered the most distinctive between users and the most stable for each user are extracted and encoded into a biometric reference or template that is a mathematical representation of a person's biometric feature. These templates are stored in a database or on a smart card or other token and used for comparison when recognition is warranted. Biometric systems are automated by hardware and software, allowing for fast, real-time decision making in identification situations [4].

Different biometric technologies offer varying features and benefits, which should be analyzed based on how and why they will be used. They all vary in performance,

Corresponding Author: Amandeep Kaur Bhatia[1] capabilities, infrastructure requirements, and cost, and all have their unique limitations and operating methodologies. While individual biometric devices and systems each have their own operating methodology, there are some generalizations that can be made as to what typically happens within a biometric system implementation.

Before an individual's identity can be verified via a biometric, a biometric template or model must first be created. This template serves as the template data against which subsequent samples/templates provided at time of verification are compared.

III. *PERSONAL BIOMETRIC CRITERIA:*

Any human biological or behavioral characteristics can become a biometric identifier, provided the following properties are met:

A. Universality: Every person should have the characteristic. There are always exceptions to this rule: mute people, people without fingers, or those with injured eyes. These exceptions must be taken into account through "work-around" such as conventional non-biometric authentication processes. Most biometric devices have a secure override if a physical property is not available, such as a finger, hand, or eye. In these cases, the person is assigned a special access device, such as a password, PIN, or secure token. This special access code or token is entered into the biometric device to allow access [5].

B. Distinctiveness: No two people should have identical biometric characteristics. Monozygotic twins, for example, cannot be easily distinguished by face recognition and DNA-analysis systems, although they can be distinguished by fingerprints or iris patterns.

C. Permanence: The characteristics should not vary or change with time. A person's face changes significantly with aging and a person's signature and its dynamics may change as well, sometimes requiring periodic re-enrollment.

D. Collectability: Obtaining and measuring the biometric feature(s) should be easy, non-intrusive, reliable, and robust, as well as cost effective for the application.
Typically, biometric systems or devices have three primary components:

1. Automated mechanism that scans or photographs (video or still) and captures a digital or analog image of a living biometric characteristic.
2. Another mechanism that handles compression, storage, processing, and comparison of the captured data with the stored data (enrollment template).
3. Interface with the application system.

IV. COMMONLY USED BIOMETRIC TECHNOLOGIES:

When personal identification is used, biometric technologies measure and analyze human biological and behavioral characteristics. Identifying a person's biological characteristics, based on direct measurement of a part of the body, such as fingerprints, hand structure, facial features, iris patterns, and others. The corresponding biometric technologies are fingerprint recognition, hand geometry, facial, and iris recognition, among others.

Biometric systems using predominantly behavioral characteristics are based on data derived from actions, such as speech and signature, for which the corresponding biometrics are speaker verification and dynamic signature analysis. Almost all biometrics, however, incorporate both biological and behavioral components. Biometrics is an effective personal identifier because the characteristics measured are distinct to each person.

Unlike other identification methods that use something a person has, such as an identification card to gain access to a building, or something a person knows, like a password or PIN to log on to a computer system, the biometric characteristics are integral to something a person is. Because biometrics is tightly bound to an individual, they are more reliable, cannot be forgotten, and are less likely to be lost, stolen, or otherwise compromised.

A. Dynamic Signature Analysis: It authenticates identity by measuring and analyzing handwritten signatures. It does not rely on the physical appearance of the signature, but instead on the manner in which a signature is written, using a stylus on a pressure-sensitive tablet to track hand movements. This technology measures how the signature is signed, changes in pressure, position and velocity of the pen during the course of signing using a pressure-sensitive tablet or personal digital assistant (PDA). Dynamic signature analysis devices have proved to be reasonably and lend themselves to applications where the signature is an accepted identifier. One of the suggested advantages for signature verification is that it has a high level of resistance to impostors [7].

For example, although it is easy to forge a signature, but it is difficult to mimic the behavioral patterns associated with signing one's signature.

B. Fingerprint: Some argue that fingerprint identification was not a true biometric until the emergence of the more recent fully automated systems. More accurately, fingerprints represent the transition from a manual biometric to the automated form of the technology. Fingerprints have long been used to identify people. In 14th century China, they were used as a form of signature. Today fingerprint verification technology is the most prominent biometric technology, used by millions of people worldwide [6].

It is estimated that the number of possible fingerprint patterns is 10 to the 48th power.25 Fingerprint technology can be used effectively in both verification (1:1) and identification (1:N) applications. Fingerprint verification systems work by identifying the locations of small lines or ridges found in the fingerprint. They extract features from impressions that are made by these distinct ridges. Typically, fingerprints are either flat (capture by placing a finger directly on the scanner) or rolled (rolling the finger from one edge of the fingernail to the other).

C. Hand Geometry: Historically, hand geometry systems have dominated the access control and “time and attendance” market in terms of biometrics being used for these purposes. Hand geometry-based verification systems measure the layout of a person’s hand, including the fingers, joints, and knuckles. Some systems measure the geometry of two fingers.

Hand geometry measures the two-dimensional physical characteristics of the user’s hand and fingers using an optical camera, mirrors, and light-emitting diodes (LEDs). In measuring size and shape, a hand geometry system collects the measurements. In the measurement of the different features, a person places his/her hand flat on the reader’s surface, where pegs guide the fingers into position.[5] Hand geometry systems require the user to squeeze his/her fingers against the pegs to confirm the hand is “living” rather than a prosthetic. Cameras capture the images of the back and sides of the hand.

D. Iris Recognition: Iris recognition technology is based on the patterns resident in the iris of the eye—the colored ring surrounding the pupil. Iris recognition technology identifies people by the unique patterns in the iris using a fairly conventional charge coupled device (CCD) camera.

Made from elastic connective tissue, the iris represents a richly patterned surface under the reflective cornea of the eye. The image of the iris under infra-red illumination can be quantified and used to identify an individual [2].

E. Keystroke Dynamics: Keystroke dynamics, or analysis, is also referred to as typing rhythms. It is an automated method of analyzing the way a user types at a terminal or keyboard, examining dynamics such as speed, pressure, total time taken to type particular words, and the time elapsed between hitting certain keys. Specifically, keystroke analysis measures two distinct variables: “dwell time,” which is the amount of time a person holds down a particular key, and “flight time,” which is the amount of time it takes between keys [8].

The technique works by monitoring the keyboard inputs to identify the user by his/her habitual typing rhythm patterns.

V. *CONCLUSION*

In this review paper, we step ahead into the new millennium, identity thefts and Internet scams are becoming increasingly common. More and more governments and institutions are now using this technology to safeguard their airports, hospitals, prisons and other sensitive areas. In this era, it is imperative that we continuously upgrade our security systems and the use of biometrics is a step towards the security upgrade that we continuously require.

REFERENCES

[1] Rashmi Singhal and Payal Jain, "BIOMETRICS:ENHANCING SECURITY," *Asian Journal of computer science and information technology*, pp. 89-92, 2011.

[2] N.K Ratha, J.H Connell, and R.M Bolle, "Enhancing Security and privacy in biometrics based authentication systems," *IBM systems journal*, pp. 614-634, 2011.

[3] Sampda A Dhole and V.H. Patil, "Person identification using pegfree hand geometry measurement," *International journal of engineering science and technology*, vol. 4, no. 6, 2012

[4] Biometric Technology Application Manual," in *Biometric Basics*.: National Biometric Security Project, 2008.

[5] Yaroslav Bulatov, Sachin Jambawalikar, Piyush Kumar, and Saurabh Sethia, "Hand Recognition Using geometric classifiers," *ICBA,Hong Kong*, pp. 753-759, July 2004.

[6] Pierre Baldi and Yves Chauvin,Neural N etworks for Fingerprint Recognition,Neural Computation 5,pp.402-418,1993

[7] Ayer, J., Lama, K., & Iskandar, B. S. (2009). A Novel Approach to Dynamic Signature Verifi cation Using Sensor-Based Data glove Faculty of Information Science and Technology, Multimedia University, Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS, Faculty of Engin. American Journal of Applied Sciences, 6(2), 233-240.

[8] Salil P. Banerjee,"Biometric Authentication and Identification using Keystroke Dynamics: A Survey", journal of Pattern Recognition Reserch 7(2012) 116-139

AUTHORS PROFILE

Harjinder: Ms. Harjinder is now pursuing her M.E from Punjabi University regional campus of Information Technology and Management Mohali, India. She has done her B.tech from Sant baba bhag Singh College of Engineering, Punjab. She has interest in the field of Network Security, Image Processing and database.

Amandeep: Ms. Amandeep is now pursuing her M.E from Punjabi University regional campus of Information Technology and Management Mohali, India. She has done her B.tech from Sviet, Punjab. She has interest in the field of Biometrics, Image Processing and database.