Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering -- RTCCE 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6184-4

Biometrics : Echelon of Secured Authentication

Varun Sharma

***Abstract*—Biometrics is the utilization of biological characteristics or behavioral traits for an identification and verification of an individual. Biometric technology is fast gaining popularity as means of security measures to reduce cases of fraud and theft due to its use of physical characteristics and traits for the identification of individuals. Biometric system has now been deployed in various commercial, civilian and forensic applications as a means of establishing identity. We have outlined the usage of various Biometrics systems, working, comparison between different techniques and their advantages and disadvantages. Various probable attacks on biometric systems and their solutions are also discussed.**

Keywords — authentication, biometrics, cryptography, recognition, validation, verification

I. Introduction

Biometrics is the automated identification, or verification of human identity through the measurement of repeatable physiological, or behavioral characteristics. The term “biometrics” is derived from the greek words bio (life) and metric (to measure). Biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics, such as fingerprints, irises, voice patterns, facial patterns, and hand measurements, for identification and verification purposes. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems and thus led to a widespread deployment of biometric authentication system. But there are still some issues concerning the security of biometrics recognition system that need to be addressed in order to ensure the integrity and public acceptance of these systems

A. *Biometric System*

A biometric system is essentially a pattern recognition system that recognizes a person based on a feature vector derived from specific physiological and behavioral characteristics that a person possesses. Depending on application context, a biometric system typically operates in one of two modes, verification or identification (Fig. 1). In verification mode, system validates a person’s identity by comparing the captured biometric characteristics with individual biometric template, which is pre stored in system database. In such system, an Individual who desires to be recognized claims an identity. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. In Identification mode, system recognizing an individual by searching the entire template database for a match. The system conducts a one to many comparisons to establish an individual’s identity. Identification is critical component of negative recognition application, in which the system prevents a single person from using multiple identities.

Varun Sharma
M Tech Student, Dep’t. Of Electronics and Communication Engineering
Maharishi Markandeshwar University, Solan
HP, INDIA

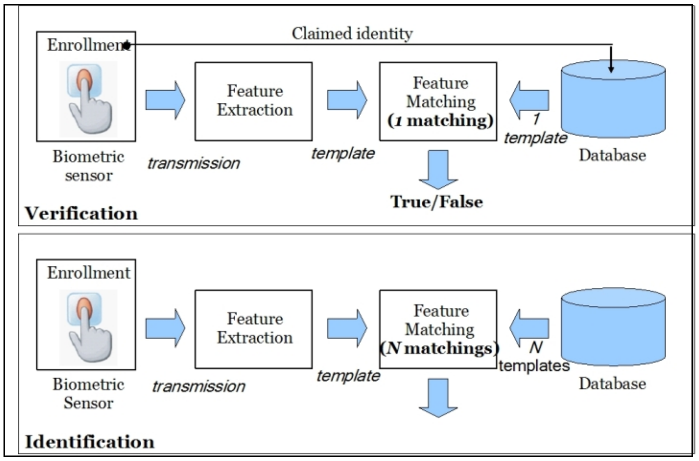

Figure 1. Verification and Identification task of Biometric System

B. *Biometric Technologies*

A brief description of various biometric technologies is given below (Fig. 2).

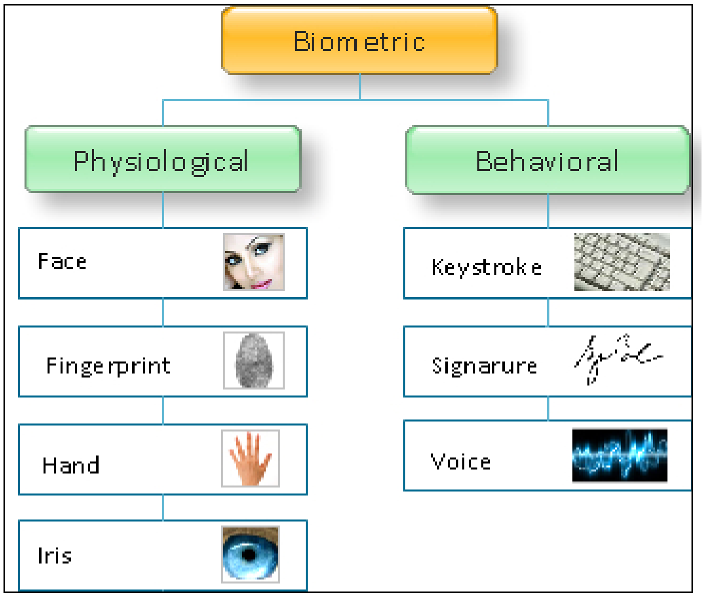

Figure 2. Biometric Technologies

1) **Fingerprint:** A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high. The fingerprint biometric is an automated digital version of the old ink and paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device involves users placing their fingers on a platform for the print to be electronically read. The accuracy of current available fingerprint recognition system is adequate for authentication systems for hundred users. Multiple fingerprints of a person provide additional information to allow for a large scale identification involving millions of identities. Finally, fingerprints of small fraction of the population may be unsuitable for the automatic identification because of genetic factors, aging, environmental, or occupational reasons.

2) **Hand Geometry:** Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and length and widths of the fingers. Commercial hand geometry based authentication systems have been installed in hundreds of locations around the world. The technique is very simple and, relatively easy to use, and inexpensive. The geometry of hand is not known to be very distinctive and hand geometry based recognition cannot be scaled up for the systems requiring identification of an individual from the large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices such as laptops. There are authentication systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those used for hand geometry, but are still much larger than those used in some other biometrics (e.g., fingerprint, face, and voice).

3) **Face:** Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make personal recognition. The applications of facial recognition range from a static, controlled "mug shot" authentication to a dynamic, uncontrolled face identification in a cluttered background. The most popular approaches to face recognition are based on either the location or shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships or the overall analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the authentication performance of the face recognition systems that are commercially available is reasonable, they impose a number of restrictions on how the facial images are obtained, often requiring a fixed and simple background or special illumination. These systems also have difficulty in matching face images captured from two drastically different views and under different illumination conditions. In order that a facial recognition system works well in practice, it should automatically detect whether a face is present in the acquired image, locate the face if there is one and recognize the face from a general viewpoint (i.e., from any pose).

4) **Iris:** The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris based recognition systems is promising and points to the feasibility of large-scale identification systems based on iris information. Each iris is believed to be distinctive and, like fingerprints, even the irises of identical twins are expected to be different. It is extremely difficult to surgically tamper the texture of the iris. Although the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user friendly and cost effective.

5) **Keystroke:** It is hypothetical assumption that each person types on a keyboard in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it is expected to offer sufficient discriminatory information that permits identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information. However, this biometric permits "continuous verification" of an individual over a period of time.

6) **Signature:** The way a person signs his or her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of authentication. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system.

7) **Voice:** Voice is a combination of physical and behavioral biometrics. The features of an individual's voice are used in the synthesis of the sound. These physical characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as common cold), emotional state, etc. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what he or she speaks. A text-independent system is more difficult to design than a text dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the communication channel.

II. Working of Biometrics

Biometrics is typically collected data using a device called sensor from behavioral or physiological characteristics for recognition and to convert the data to a templates in digital form. The quality of sensor used has a significant impact on the recognition results. Example “sensors” could be digital cameras (for face recognition) or a telephone (for voice recognition). So biometric system may be viewed as a signal detection system with a pattern recognition architecture that senses a raw biometric signal, processes the signal to extract a salient set of features, compares these features against the feature sets residing in the database, and either validates a claimed identity or determines the identity associated with the signal. This is a multi-stage process whose stages are described below(Fig. 3).

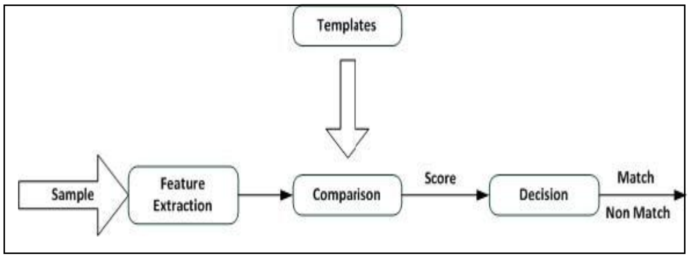

Figure 3. Biometric process

Enrollment - Here the sample of biometric trait is captured, accessed, processed and stored for ongoing use in biometric system. Enrollment takes place in both 1:1 and 1: N systems

Acquisition device - The hardware used to acquire biometric samples.

TABLE 1. ACQUISITION DEVICES USED IN BIOMETRIC SYSTEM

Technology	**Acquisition Device**
Fingerprint	Desktop peripheral, Reader embedded in keyboard
Voice Recognition	Microphone, telephone
Facial recognition	Video Camera, PC Camera, single-image camera
Iris Scan	Infrared-enabled video camera, PC Camera
Retina Scan	Proprietrt desktop or wall-mounted unit
Hand Geometry	Proprietry wall mounted unit
Signature-Scan	Signature tablet, motio-sensitive stylus
Keystroke-Scan	Keyboard or keypad

Submission - The process where a user provides behavioral or physiological data in the form of biometric samples to a biometric system.

Biometric sample - The Identifiable, unprocessed image or recording of a physiological or behavioral characteristics acquired during submission, used to generate biometric templates. Also referred to as biometric data.

TABLE 2. BIOMETRIC SAMPLES IN DIFFERENT TECHNOLOGIES

Technology	**Biometric Sample**
Fingerprint	Fingerprint image
Voice Recognition	Voice recording
Facial recognition	Facial Image
Iris Scan	Iris Image
Retina Scan	Retina Image
Hand Geometry	3 – D image of top and sides of hand and fingers
Signature-Scan	Image of signature and record of related dynamics measurements
Keystroke-Scan	Recording of charaters typed and record of related dynamics measurements

Feature Extraction - Here the acquired biometric data is processed to extract a set of salient or discriminatory features. For example, Voice recognition technologies can filter out certain frequencies and patterns. Furthermore, if the sample provided is inadequate to perform the feature extraction, biometric system will generally instruct the user to provide another sample, often with some type of advice or feedback.

TABLE 3 : EXTRACTED FEATURE OF VARIOUS BIOMETRIC TECHNOLOGIES

Technology	**Feature Extracted**
Fingerprint	Location and direction of ridge endings and bifurcations on fingerprints
Voice Recognition	Frequency, Cadence and duration of vocal pattern
Facial recognition	Relative position and shape of nose, position of cheekbones
Iris Scan	Furrows and striations in iris
Retina Scan	Blood vessel patterns on retina
Hand Geometry	Height and width of bones and joints in hands and fingers
Signature-Scan	Speed, stroke order, pressure, and appearance of signature
Keystroke-Scan	Keyed sequence, duration between characters

Template - A biometric template is a digital representation of an individual’s distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. A template is created after a biometric algorithm locates features in a biometric sample. Biometric system utilizes the original sample to perform a comparison.

Biometric decision - making is frequently misunderstood. For the vast majority of technologies and systems, there is no such thing as a 100% match, though systems can provide a very high degree of certainty. The biometric decision-making process is comprised of various components, as indicated below.

Matching - The comparison of biometric templates to determine their degree of similarity or correlation. A match attempt results in a score that, in most systems, is compared against a threshold. If the score exceeds the threshold, the result is a match; if the score falls below the threshold, the result is a non-match.

Score – A number indicating the degree of similarity or correlation of a biometric match. Traditional verification methods – passwords, PINs, keys, and tokens - are binary, offering only a strict yes/no response. This is not the case with most biometric systems. Nearly all biometric systems are based on matching algorithms that generate a score subsequent to a match attempt.

Threshold - A predefined number, often controlled by a biometric system administrator, which establishes the degree of correlation necessary for a comparison to be deemed a match. If the score resulting from template comparison exceeds the threshold, the templates are a "match" (though the templates themselves are not identical)

Decision – The result of the comparison between the score and the threshold. Depending on the type of biometric system deployed, a match might grant access to resources, a non-match might limit access to resources, while inconclusive may prompt the user to provide another sample.

III. Biometrics Evaluation:

When it is time to use biometric authentication, the degree of security is concerned. In this paper we discuss the number of biometric authentication techniques.

1) **False Accept Rate or False Match Rate (FAR or FMR):** The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

2) **False reject Rate or False Non-Match Rate (FRR or FNMR):** The probability that the system fails to detect match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

3) **Receiver Operating Characteristic or Relative Operating Characteristic (ROC):** The ROC plot is a Visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR.

4) **Equal Error Rate or Crossover Error Rate (EER or CER):** the rates at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of the devices with different ROC curves. In general, the device with lowest EER is most accurate.

5) **Failure to Enroll Rate (FTE or FER):** The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

6) **Failure to Capture Rate (FTC):** Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

7) **Template Capacity:** The maximum number if sets of data which can be stored in the system.

IV. Comparison of Biometric Technologies

Several biometrics characteristics are in use in various applications. Each biometrics has its strengths and weaknesses, and choice typically depends on the application. No single biometric can effectively meet the requirement of all applications and none is optimal. There are following evaluation categories using which we compared the performance of various biometrics technologies.

- **Universality** describes how commonly a biometric trait occurs in each individual
- **Uniqueness** is how well the biometric distinguishes one individual from another
- **Permanence** measures how well a biometric resists aging
- **Collectability** explains how easy it is to acquire the biometric for measurement
- **Performance** indicates the accuracy, speed, and robustness of the system capturing the biometric.
- **Acceptability** indicates the degree of approval of a technology by the public in everyday life
- **Circumvention** is how easy it is to fool the authentication system.

TABLE 4 : COMPARISON OF VARIOUS BIOMETRICS TECHNOLOGIES

Biometrics:	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Face	**H**	**L**	**M**	**H**	**L**	**H**	**L**
Fingerprint	**M**	**H**	**H**	**M**	**H**	**M**	**H**
Hand geometry	**M**	**M**	**M**	**H**	**M**	**M**	**M**
Keystrokes	**L**	**L**	**L**	**M**	**L**	**M**	**M**
Hand veins	**M**	**M**	**M**	**M**	**M**	**M**	**H**
Iris	**H**	**H**	**H**	**M**	**H**	**L**	**H**
Retinal scan	**H**	**H**	**M**	**L**	**H**	**L**	**H**
Signature	**L**	**L**	**L**	**H**	**L**	**H**	**L**
Voice	**M**	**L**	**L**	**M**	**L**	**H**	**L**

H=High **M=Medium** **Low=Low**

Each system is ranked as low, medium, or high in each category. A low ranking indicates poor performance in the evaluation criterion, whereas a high ranking indicates very good performance.

V. Attack Points On Biometric System

Biometrics definitely is protected data and therefore should be properly protected, but cannot be considered secret. The general analysis of a biometric system for vulnerability assessment determines the extent to which an imposter can compromise the security offered by biometric system. We briefly discuss the characteristics of such attacks, which needs to be effectively thwarted in biometric systems. Adversary attack on biometric system is shown in fig 4.

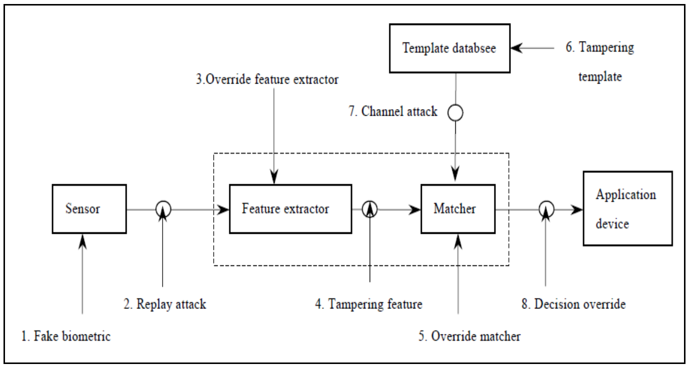

Figure4. Attack points in biometric system

1) **Fake biometric at the sensor:** In this mode of attack, a possible reproduction of the biometric being used will be presented to the system. Examples include a fake finger, a copy of a signature, a face mask.

2) **Resubmission of old digitally stored biometrics signal:** In this mode of attack, an old recorded signal is replayed into the system bypassing the sensor.

3) **Override feature extract**: The feature extractor could be attacked with a Trojan horse so that it would produce feature sets chosen by the hacker.

4) **Tampering with the feature representation:** After the features have been extracted from the input signal they are replaced with a different synthesized feature set (assuming the representation is known).

5) **Override matcher:** The matcher is attacked to always directly produce an artificial high or low match score.

6) **Tampering with stored templates:** The stored template attacker tries to modify one or more templates in the database which could result in authorization for a fraudulent individual, or at least denial of service for the person associated with the corrupted template.

7) **Channel attack between stored templates and the matcher:** The templates from the stored database are sent to the matcher through a channel which could be attacked to change the contents of the templates before they reach the matcher.

8) **Overriding Yes/No response:** If the final result can be overridden with the choice of result from the hacker, the final outcome is very dangerous. Even if the actual pattern recognition system had excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the result.

VI. Conclusion and Future Work

Biometrics can be defined as the science and technology of measuring and statistically analyzing biological data. There is vast number of biometrics technologies available with us but still there be major concerns about the technology. First, biometric system itself be attacked or compromised. Second, security and privacy of individual's template is a difficult task. Third, there are cultural and religious objections. With the advancement of time, there has been an expansion in the flow of people and goods. In order to prevent counterfeiting and piracy along with terrorism activities, more reliable identification and authentication methods are required. The scope of this paper is to introduce with the biometrics. The ongoing research in the field will replace other traditional authentication system and the future of this smart technology will help in law enforcement and biometrics are perceived as future of security industry and getting popular as accurate verification technology in the market.

References

[1] Anil K Jain, Arun Ross, and Sharath Pankanti, "Biometrics : A Tool for information Security," IEEE Transaction on Forensic and security., vol 1, no 2, pp. 125 – 143,June 2006

[2] A. K. Jain, A. Ross, and S. Prabhakar, " An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, 14(1):4–20, January 2004..

[3] Neha Dahiya, Dr. Chander Kant, " Biometrics Security Concern", Second Interational Confernce on Advanced Computing & Communication technologies, pp. 297- 302, 2012.

[4] Anil K. jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security", EURASIP journal on Advances in Signal Processing, vol 2008, Article ID 579416,pp. 33-42, Dec 2007.

[5] Salil Prabhakar, Sharath Pankanti, Anil K Jain, "Biometric recognition: Security and Privacy Concern", IEEE Security & Privacy, pp. 33-42, April 2003.

[6] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A, and Minkyu Choi, " Biometric : A Review", Internationa Journal of u-and-e-Service,Science and Technology, vol. 2, no. 3, pp. 13-28, September 2009.

[7] Chander Kant, Rajender Nath, and Sheetal Chaudhary, " Biometrics Security using Steganography", International Journal Of Security, vol. 2, Issue(1), pp. 1-5.

[8] Anil K Jain, " Biometric Recognition", nature, vol 449|6, pp. 38-40, September 2007.

Rozeha A. Rashid, Nur Hija Mahalin, Mohd Adib Sarijari, Ahmed Aizuddin Abdul Aziz, "Securiy System using Biometric Technology ; Design and Implementation of Voice Recognition System(VRS)", proc of the international Conference on Computer and Communication Engineering, pp. 898-902, May 2008

About Author (s):

Varun Sharma received B. Tech degree in Electronics and Communication Engineering from Institute of Engineering & Emerging Technologies, H P University, Shimla, HP, India in year 2008. He is pursuing M tech degree in ECE from Maharishi Markandeshwar University, Solan, HP, India. His research interest includes Biometrics and Speech Processing.