BIOMETRIC SECURITY

Kaladiya Faiz, Shaikh Abdur Rehman, Ansari Arfat Aslam, Ansari Fahad
Computer Department,
Anjuman.Islam.Abdul.Razzak.Kalsekar.Polytechnic, Panvel, India

Abstract: Over the last few years a new area of engineering science has been established whose products are likely to create a large market in the near future. It has been called ''biometrics". The pioneers of this new domain intend to construct devices which would allow identification of a person on the basis of his/her ''biological'' characteristics: voice, dynamics of movements, features of face and other parts of the body, retina or iris pattern. Nature has made human beings with different characteristics which may vary from one person to another. This property is made use of by Biometric technology to distinctly identify each person

Biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system. First, a user must be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to the user. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in a verification (authentication) or an identification mode.

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification offers several advantages over traditional methods involving ID cards (tokens) or PIN numbers (passwords) for various reasons: (i) the person to be identified is required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased integration of computers and Internet into our everyday lives, it is necessary to protect sensitive and personal data. By replacing PINs (or using biometrics in addition to PINs), biometric techniques can potentially prevent unauthorized access to ATMs, cellular phones, laptops, and computer networks. Unlike biometric traits, PINs or passwords may be forgotten, and tokens like passports and driver's licenses may be forged, stolen, or lost.

This paper gives an overview of key biometric technologies and basic technique involved. The various opportunities for biometrics are mentioned, followed by the uses, benefits, drawbacks, and applications.

Introduction:

The first modern biometric device was introduced on a commercial basis over 25 years ago when a machine that measured finger length was installed for a time keeping application at Shearson Hamil on Wall Street. In the ensuing years, hundreds of these hand geometry devices were installed at high security facilities operated by Western Electric, Naval Intelligence, the Department of Energy, and the like. There are now over 20,000 computer rooms, vaults, research labs, day care centers, blood banks, ATMs and military installations to which access is controlled using devices that scan an individual's unique physiological or behavioral characteristics. Reduced prices have lead to increased awareness of biometric technologies; this coupled with lower overall prices will certainly bode well for this industry as we move through the new millennium.

Biometrics:

The term biometrics refers to the emerging field of technology devoted to the identification of individuals using biological traits or behaviors. In practice, this means capturing an image of a unique feature of an individual such as a fingerprint, hand, eye or face, and comparing it with a template captured previously. For ease of explanation this has been over-simplified, but in essence this is how biometric technology works.

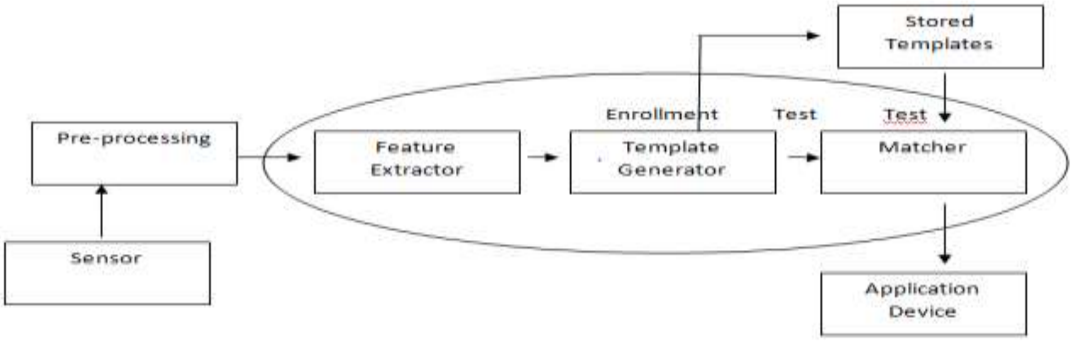
Definition - What does Biometric Security mean?

Biometric security is a security mechanism used to authenticate and provide access to a facility or system based on the automatic and instant verification of an individual's physical characteristics. Because biometric security evaluates an individual’s bodily elements or biological data, it is the strongest and most foolproof physical security technique used for identity verification.

Techopedia explains Biometric Security

Biometric security is mainly implemented in environments with critical physical security requirements or that are highly prone to identity theft. Biometric security-based systems or engines store human body characteristics that do not change over an individual's lifetime. These include fingerprints, eye texture, voice, hand patterns and facial recognition.

An individual's body characteristics are pre-stored in a biometric security system or scanner, which may be accessed by authorized personnel. When an individual walks into a facility or tries to gain access to a system, the biometric scanner evaluates his/her physical characteristics, which are matched with stored records. If a match is located, the individual is granted access.



Block Diagram of a Biometric System

Types of Biometric Sensor

Biometric sensors or access control system are classified into two types such as Physiological Biometrics and Behavioral Biometrics. The physiological biometrics mainly include face recognition, fingerprint, hand geometry, Iris recognition and DNA. Whereas behavioral biometrics include keystroke, signature and voice recognition. For better understanding of this concept, some of them are discussed below.

Fingerprint Recognition

Fingerprint Recognition includes taking a fingerprint image of a person and records its features like arches, whorls, and loops along with the outlines of edges, minutiae and furrows. Matching of the Fingerprint can be attained in three ways, such as minutiae, correlation and ridge

Minutiae based fingerprint matching stores a plane includes a set of points and the set of points are corresponding in the template and the i/p minutiae.

Correlation based fingerprint matching overlays two fingerprint images and association between equivalent pixels is calculated.

Ridge feature based fingerprint matching is an innovative method that captures ridges, as minutiae based fingerprint capturing of the fingerprint images is difficult in low quality

To capture the fingerprints, present methods employ optical sensors that use a CMOS image sensor or CCD; solid state sensors work on the principle of transducer technology using thermal, capacitive, piezoelectric sensors or electric field ; or ultrasound sensors work on echography in which the sensor sends acoustic signals through the transmitter near the finger and captures the signals in the receiver

Face Recognition

Face recognition system is a one type of biometric computer application which can identify or verify a person from a digital image by comparing and analyzing patterns. These biometric systems are used in security systems. Present facial recognition systems work with face prints and these systems can recognize 80 nodal points on a human face. Nodal points are nothing but end points used to measure variables on a person’s face, which includes the length and width of the nose, cheekbone shape and the eye socket depth.

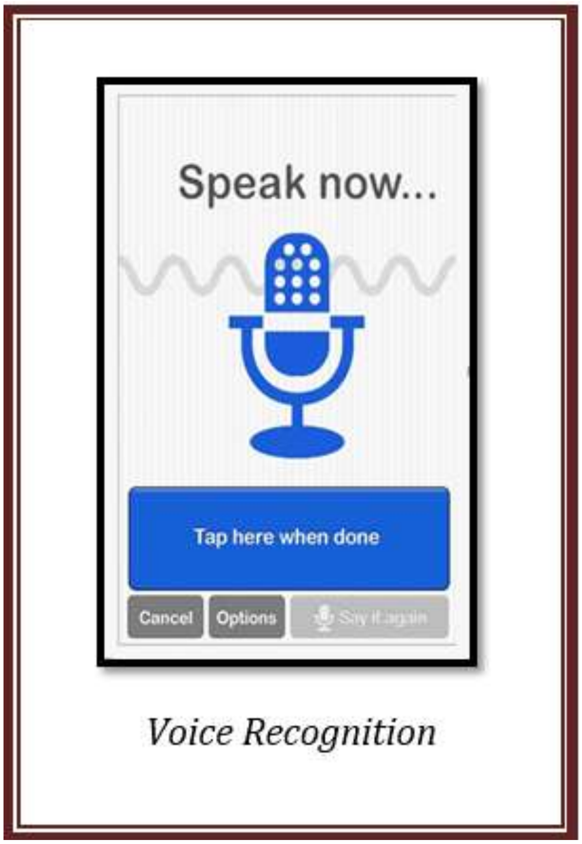
Face recognition systems work by capturing data for the nodal points on a digital image of a person’s face and resulting data can be stored as a face print. When the conditions are favorable, these systems use a face prints to identify accurately. Currently, these systems focus on smartphone applications which include personal marketing, social networking and image tagging purposes. Social sites like FB uses software for face recognition to tag the users in photographs. This software also increases marketing personalization. For instance, billboards have been designed with integrated software that recognizes the ethnicity, gender and estimated age of onlookers to deliver targeted marketing.

Iris Recognition

Iris recognition is a one type of bio-metric method used to identify the people based on single patterns in the region of ring shaped surrounded the pupil of the eye. Generally, the iris has a blue, brown, gray or green color with difficult patterns which are noticeable upon close inspection. Please follow the below link to know more about iris recognition technolo

Voice Recognition

Voice recognition technology is used to produce speech patterns by combining behavioral and physiological factors that can be captured by processing the speech technology. The most important properties used for speech authentication are nasal tone, fundamental frequency, inflection, cadence. Voice recognition can be separated into differen categories based on the kind of authentication domain, such as a fixed text method, in the text dependent method, the text independent method and conversational technique.



Voice Recognition

Signature Recognition

Signature recognition is a one type of biometric method used to analyze and measure the physical activity of signing like the pressure applied, stroke order and the speed. Some biometrics are used to compare visual images of signatures. Signature recognition can be operated in two different ways, such as static and dynamic.

In static mode, consumers write their signature on paper, digitize it through a camera or an optical scanner. This system identifies the signature examining its shape.

In dynamic mode, consumers write their signature in a tablet which is digitized, that obtains the signature in real time. Another option is the gaining by means of stylus-operated PDAs. Some biometrics also operate with smart-phones with a capacitive screen, where consumers can sign using a pen or a finger. This type of recognition is also known as "on-line"

The emergence of biometric technologies

Biometrics is a very strong authentication mechanism as it based on something that you are as opposed to something you know or something you have. Passwords and tokens are highly vulnerable to being lost or stolen. A weak or compromised password is the primary reason for the rising cases of security and data breaches. Passwords are the weakest link in an organization's security system and even strong passwords cannot resist sophisticated hacker attacks. Further, the costs of maintaining password and token based systems are very high and inefficient. Resetting lost or forgotten passwords takes up IT support time and reduces employee productivity. Fingerprint recognition looks for the unique patterns of ridges and valleys that are present in an individual's fingerprint. These patterns are unique to every individual and thus help to identify individuals from an entire population. Fingerprints are inherent to individuals and can neither be lost nor stolen which makes it highly accurate and reliable. Moreover, the availability of low-cost fingerprint readers coupled with easy integration capabilities has led to the wide spread deployment of fingerprint biometrics in a variety of organizations. Verification and identification are the two ways in which an individual's identity can be determined using biometric technology. Verification confirms that a person is indeed who they claim to be and performs a one-to-one comparison of the individual's fingerprint sample with a stored reference template. Identification, on the other hand, performs a one-to-many comparison to confirm an individual's identity. The identification process compares the individual's fingerprint sample against all the reference templates stored on file. An individual is positively identified if the individual's fingerprint image matches any of the stored templates.

Why should organizations choose biometric fingerprinting technology?

An organization can enjoy limitless benefits by correctly deploying biometric technology. Today's economy is an evolving one and technological advancements have changed the way in which organizations function and conduct businesses. Modern organizations need to be adaptive, flexible and agile to survive in the competitive business environment. Fingerprint technology can benefit organizations in a variety of sectors such as health care, government, retail enterprises, technology organizations, manufacturing industry, libraries, universities etc.

Workforce
Time and Attendance
Payroll Management
Human Resource Management
Enterprise

Employee identification and workforce management becomes faster, accurate and more efficient with fingerprint technology. Unlike magnetic strip cards or passwords, individuals always carry their fingerprints with them and they cannot be lost or forgotten. Tracking attendance of employees in manufacturing organizations prevents employee time theft and reduces fraudulent behavior. A biometric system enables automated calculation of employee hours thus reducing paper wastage and time spent in manual reconciliation of attendance data.

Finance
Customer Identification
Non-account Holder Identification
Employee Identification
Finance & Banking

Fingerprint biometrics can provide both physical access to company buildings and logical access to internal resources such as enterprise computers and systems.

Governments and organizations all around the world are choosing biometric technology to combat identity fraud and security breaches, secure confidential data, reduce costs and to improve overall user experience. Biometrics is one of the rapidly growing fields in the information technology sector with fingerprint recognition expected to remain the most dominant form of biometric technology. The global biometrics market is growing at an exponential rate and is forecasted to reach $23.54 billion by 2020.

Government
Border Control
Voter Registration
National ID
ePassport
Government Sector

References:

- Wikipedia
- Techopedia
- www.elprocus.com

Conclusion:

In this article, we have discussed how the implementation of fingerprint technology in various sectors has increased security, accuracy and reliability in identification systems. The adoption of biometric systems has gained momentum and it continues to grow further as hardware costs reduce and easy integration solutions become available.