Biometric Technologies

Mayank Vatsa
Indian Institute of Technology Kanpur, India

Richa Singh
Indian Institute of Technology Kanpur, India

P. Gupta
Indian Institute of Technology Kanpur, India

A.K. Kaushik
Electronic Niketan, India

INTRODUCTION

Identity verification in computer systems is done based on measures like keys, cards, passwords, PIN and so forth. Unfortunately, these may often be forgotten, disclosed or changed. A reliable and accurate identification/verification technique may be designed using biometric technologies, which are further based on the special characteristics of the person such as face, iris, fingerprint, signature and so forth. This technique of identification is preferred over traditional passwords and PIN-based techniques for various reasons:

- The person to be identified is required to be physically present at the time of identification.
- Identification based on biometric techniques obviates the need to remember a password or carry a token.

A biometric system essentially is a pattern recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic." A biometric system can be either an identification system or a verification (authentication) system; both are defined below.

- **Identification:** *One to Many*—A comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates.
- **Verification:** *One to One*—A comparison of two sets of biometrics to determine if they are from the same individual.

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (*Capture, Process, Enroll*) followed by a *Verification* or *Identification*.

During *Capture*, raw biometric is captured by a sensing device, such as a fingerprint scanner or video camera; then, distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (biometric template). Next is enrollment, in which the processed sample (a mathematical representation of the template) is stored/registered in a storage medium for comparison during authentication. In many commercial applications, only the processed biometric sample is stored. The original biometric sample cannot be reconstructed from this identifier.

BACKGROUND

Many biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires the following properties of biometric characteristics:

- **Universal:** Everyone must have the attribute. The attribute must be one that is seldom lost to accident or disease.
- **Invariance of properties:** They should be constant over a long period of time. The attribute should not be subject to significant differences based on age or either episodic or chronic disease.
- **Measurability:** The properties should be suitable for capture without waiting time and it must be easy to gather the attribute data passively.
- **Singularity:** Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are unique attributes, assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.
- **Acceptance:** The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies; that is, technologies requiring a part of the human body to be taken or (apparently) impairing the human body.
- **Reducibility:** The captured data should be capable of being reduced to an easy-to-handle file.
- **Reliability and tamper-resistance:** The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
- **Privacy:** The process should not violate the privacy of the person.
- **Comparable:** The attribute should be able to be reduced to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
- **Inimitable:** The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

Among the various biometric technologies being considered are fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature and so forth.

Fingerprint

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 (Maltoni, 2003). The biometric device requires each user to place a finger on a plate for the print to be read. Fingerprint biometrics currently has three main application areas: large-scale Automated Finger Imaging Systems (AFIS), generally used for law enforcement purposes; fraud prevention in entitlement programs; and physical and computer access. A major advantage of finger imaging is the long-time use of fingerprints and its wide acceptance by the public and law enforcement communities as a reliable means of human recognition. Others include the need for physical contact with the optical scanner, possibility of poor-quality images due to residue on the finger such as dirt and body oils (which can build up on the glass plate), as well as eroded fingerprints from scrapes, years of heavy labor or mutilation.

Facial Recognition

Face recognition is a noninvasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code (Zhao, 2000). Facial recognition records the spatial geometry of distinguishing features of the face. Facial recognition technologies can encounter performance problems stemming from such factors as non-cooperative behavior of the user, lighting and other environmental variables. The main disadvantages of face recognition are similar to problems of photographs. People who look alike can fool the scanners. There are many ways in which people can significantly alter their appearance, like slight change in facial hair and style.

Iris Scan

Iris scanning measures the iris pattern in the colored part of the eye, although iris color has nothing to do with the biometric[6]. Iris patterns are formed randomly. As a result, the iris patterns in the left and right eyes are different, and so are the iris patterns of identical twins. Iris templates are typically around

Related Content

PIR: A Domain Specific Language for Multimedia Information Retrieval

Xiaobing Huang, Tian Zhaoand Yu Cao (2014). *International Journal of Multimedia Data Engineering and Management (pp. 1-27).*

www.irma-international.org/article/pir/117891

Multiple Points Localization With Defocused Images

Dongzhen Wangand Daqing Huang (2020). *International Journal of Multimedia Data Engineering and Management (pp. 1-15).*

www.irma-international.org/article/multiple-points-localization-with-defocused-images/260961

Lost in the Funhouse, is Anyone in Control?

Steve McRobb, Pat Jefferiesand Bernd Carsten Stahl (2008). *Handbook of Research on Digital Information Technologies: Innovations, Methods, and Ethical Issues (pp. 438-454).*

www.irma-international.org/chapter/lost-funhouse-anyone-control/19858

Mobility within Rich Multimedia Services

Frédéric Lassabe, Philippe Canalda, Damien Charlet, Pascal Chatonnayand François Spies (2009). *Handbook of Research on Mobile Multimedia, Second Edition (pp. 804-819).*

www.irma-international.org/chapter/mobility-within-rich-multimedia-services/21046

AI and NLP-Empowered Framework for Strengthening Social Cyber Security

Mudasir Ahmad Wani (2023). *Recent Advancements in Multimedia Data Processing and Security: Issues, Challenges, and Techniques (pp. 32-45).*

www.irma-international.org/chapter/ai-and-nlp-empowered-framework-for-strengthening-social-cyber-security/331433