IJCSC 0973-7391 Vol 6 • Number 2 April - Sep 2015 pp. 223-226 **Impact Factor: 2.5** **Available at** www.csjournals.com

Biometric System: Secure User Authentication

Nippun Kamboj, Arun Kumar Yadav
Department of Computer Science and Appl, K.U., Kurukshetra, Haryana

Abstract: Authentic person identification is an important problem in many applications. The purpose of such schemes is to ensure that the particular services are accessed only by a legal user and no one else. In the absence of proper recognition schemes, these systems are vulnerable to impostor. Biometrics, identification based on distinct personal traits, has the potential to become key part of any identification system. Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. With the availability of inexpensive biometric sensors and computing power, it is becoming increasingly clear that widespread usage of biometric person identification is being blocked by our lack of understanding of three fundamental problems: (i) How to accurately and efficiently represent and recognize biometric patterns? (ii) How to guarantee that the sensed measurements are not false? And (iii) How to make sure that the application is indeed exclusively using pattern recognition for the expressed purpose. For these reasons, we view biometrics as a grand challenge - "a fundamental problem in science and engineering with broad economic and scientific impact".
Key Words: Biometrics, multimodal biometrics, recognition, identification, verification.

Introduction

Person identification is an integral part of the infrastructure needed for diverse business sectors, transportation, entertainment, law enforcement, security, access control, border control, government, communication etc. As our society becomes electronically connected to form one big global community, it has become necessary to carry out reliable person identification often remotely and through automatic means. Substitute representations of identity such as passwords and cards no longer suffice. Further, passwords and cards can be shared and thus cannot provide reliability.

Biometrics, which refers to automatic identification of people based on their distinctive physiological (e.g., face, fingerprint, iris, retina, hand geometry) and behavioral (e.g., voice, gait) characteristics, should be an essential component of any effective person identification solution because biometric identifiers cannot be shared, misplaced, and they intrinsically represent the individual's identity [1]. Consequently, biometrics is not only an important pattern recognition research problem but is also an enabling technology that will make our society safer, reduce fraud and lead to user convenience generally providing the following functionalities: (a) Positive Identification ("Is this person who he claims to be?"). A positive identification verifies the authenticity of a claimed enrolled identity based on the input biometric sample. For example, a person claims that he is Dr. Subhash to the authentication system and offers his fingerprint; the system then either accepts or rejects the claim based on a single match performed between the input pattern and the enrolled pattern associated with the claimed identity. (b) Large Scale Identification- also referred to as negative identification ("Is this person in the database?"). Given an input biometric sample, a large-scale identification determines if the pattern is associated with any of a large number (e.g., millions) of enrolled identities. These large-scale identification applications require a large sustainable throughput with as little human supervision as possible.

Biometric Systems

A *biometric system* is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in *verification* mode or *identification* mode (Figure 1) [2]. In the verification mode, the system validates a person's identity by comparing the captured biometric data with his own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not. Identity verification is typically used for *positive recognition*, where the aim is to prevent multiple people from using the same identity [3].

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity [4]. Identification is a critical component in *negative recognition* applications where the system establishes whether the person is who he denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities.

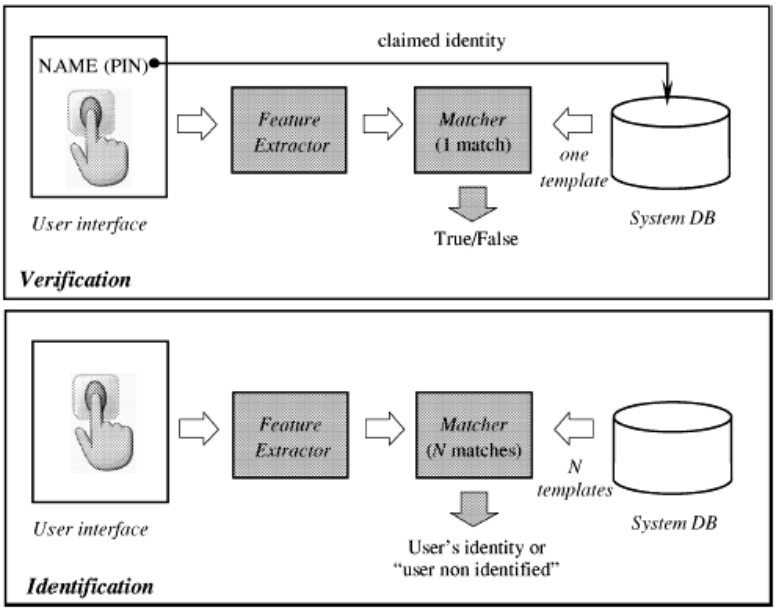

Figure1. Verification and identification tasks of a biometric system

Biometrics technologies

The primary biometric disciplines include the following [5]:

- Fingerprint (optical, silicon, ultrasound, touch less)
- Facial recognition (optical and thermal)
- Voice recognition (not to be confused with speech recognition)
- Iris-scan
- Retina-scan
- Hand geometry
- Signature-scan

Factors Cause Biometric Systems to Fail?

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted. While it is not possible to definitely state if a biometric submission will be successful, it is possible to locate factors that can reduce affect system performance [6].

Biometric Deformations

Fingerprint

- Cold finger
- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Location of finger on platen (poorly placed core)

- Cuts to fingerprint
- Manual activity that would mar or affect fingerprints (construction, gardening)

Voice recognition

- Cold or illness that affects voice
- Different enrollment and verification capture devices
- Different enrollment and verification environments (inside vs. outside)
- Speaking softly
- Variation in background noise
- Poor placement of microphone / capture device
- Quality of capture device

Facial recognition

- Change in facial hair
- Change in hairstyle
- Lighting conditions
- Adding/removing glasses
- Change in weight
- Change in facial aspect (angle at which facial image is captured)

Iris-scan

- Too much movement of head or eye
- Glasses
- Colored contacts

Retina-scan

- Too much movement of head or eye
- Glasses

Hand geometry

- Jewelry
- Change in weight
- Bandages
- Swelling of joints

Signature-scan

- Signing too quickly
- Different signing positions (e.g., sitting vs. standing)

In addition, for many systems, an additional strike occurs when a long period of time has elapsed since enrollment or since one's last verification. If significant time has elapsed since enrollment, physiological changes can complicate verification. If time has elapsed since a user's last verification, the user may have "forgotten" how he or she enrolled, and may place a finger differently [7]. For the most part, a single strike will probably not materially affect the performance of a given system. However, as you have more and more strikes for a given submission, your chances of a successful verification diminish.

These strikes do not include inherent characteristics such as age, ethnicity, or gender, which can also affect system accuracy. The performance of many biometric systems varies for specific populations.

Multimodal biometrics

A multimodal biometric system uses multiple applications to capture different types of biometrics [8]. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements.

A multimodal system could be, for instance, a combination of fingerprint verification, face recognition, voice verification and smart card or any other combination of biometrics [9]. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric.

A multimodal system can combine any number of independent biometrics and overcome some of the limitations presented by using just one biometric as your verification tool. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject. A multimodal system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions [10].

5. Conclusions

Biometrics is one of the important and more interesting pattern recognition applications with its associated unique challenges. There are a large number of biometric solutions that have been successfully deployed to provide useful value in practical applications. The scope of this paper is intended to expand the popularity of biometric technology. A successful biometric solution does not have to be 100% accurate or secure. As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. It is too early to predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business.

4. References

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

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer- Verlag, 2003.

[3] A. K. Jain, Arun Ross and U. Uludag "Biometrics Template security: Challenges and solutions" in *Proc. of* European Signal Processing Conference September 2005.

[4] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Audio and Video-based Biometric Person Authentication (AVBPA)*,pp. 223–228, (Halmstad, Sweden), June 2001.

[5] www.biometricsinfo.org

[6] R. Cappelli, R. Erol, D. Maio, and D. Maltoni, "Synthetic fingerprint-image generation," in *Proc. Int'l. Conf. Pattern Recognition (ICPR)*, vol. 3, pp. 475–478,
(Barcelona, Spain), September 2000.

[7] JJ Eggers, R Bauml, Bernd Grid, "A Communication Approach to Image Steganography", Proceedings of SPIE vol 4675, Jan 2002, Security and Watermarking of Multimedia Contents IV, San Jose, Callifornia.

[8] A. Adler, "Can images be regenerated from biometric templates?," in *Biometrics Consortium Conference*, (Arlington, VA), September 2003.

[9] Neil F. Johnson, Sushil Jajodia, "Steganalysis of Images Created Using Current Steganography Software", Lecture Notes in Computer Science, vol 1525, 1998, Springer-Verlag.

[10] A. Ross, J. Shah, and A. K. Jain, "Towards reconstructing fingerprints from minutiae points," in *Proc. SPIE, Biometric Technology for Human Identification II*, vol. 5779, pp. 68–80, (Orlando, FL), March 2005.