Biometric Recognition: Overview and Recent Advances

Anil K. Jain

Department of Computer Science and Engineering
Michigan State University, East Lansing, MI 48824, USA
jain@cse.msu.edu
http://biometrics.cse.msu.edu

Abstract. The emerging requirements of reliable and highly accurate personal identification in a number of government and commercial applications (e.g., international border crossings, access to buildings, laptops and mobile phones) have served as an impetus for a tremendous growth in biometric recognition technology. Biometrics refers to the automatic recognition of an individual by using anatomical or behavioral traits associated with that person. By using biometrics, it is possible to recognize a person based on who you are, rather than by what you possess (e.g., an ID card) or what you remember (e.g., a password). Besides bolstering security, biometric systems also enhance user convenience by alleviating the need to design and remember multiple complex passwords. In spite of the fact that the first automatic biometric recognition system based on fingerprints, called AFIS, was installed by law enforcement agencies over 40 years back, biometric recognition continues to remain a very difficult pattern recognition problem. A biometric system has to contend with problems related to non-universality of biometric (failure to enroll rate), limited degrees of freedom (finite error rate), large intra-class variability, and spoof attacks (system security). This paper presents an overview of biometrics, its advantages and limitations, state-of-the-art error rates and current research in representation, fusion and security issues.

1 Introduction

A reliable identity management system is a critical component in several applications that render services to only legitimately enrolled users. Examples of such applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions or boarding a commercial flight. The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centers (e.g., credit cards) have further enhanced the need for reliable identity management systems. The overarching task in an identity management system is the determination (or verification) of an individual's identity (or claimed identity). Traditional methods of establishing a person's identity include knowledge-based (e.g., passwords) and token-based (e.g., ID cards) mechanisms, but these surrogate representations of the identity can easily be lost, shared, manipulated or stolen thereby

L. Rueda, D. Mery, and J. Kittler (Eds.): CIARP 2007, LNCS 4756, pp. 13–19, 2007.
© Springer-Verlag Berlin Heidelberg 2007

undermining the intended security. Biometrics offers a natural and reliable solution to certain aspects of identity management by utilizing automated schemes to recognize individuals based on their inherent anatomical and/or behavioral characteristics [1]. By using biometrics it is possible to establish an identity based on *who you are*, rather than by *what you possess*, such as an ID card, or *what you remember*, such as a password.

Although biometrics emerged from its extensive use in law enforcement to identify criminals, i.e., forensics, it is being increasingly used today to carry out person recognition in a large number of civilian applications (e.g., national ID card, e-passport and smart cards) [1], [2] (see Figure 1). Most of the emerging applications can be attributed to increased security threats as well as fraud associated with various financial transactions (e.g., credit cards).

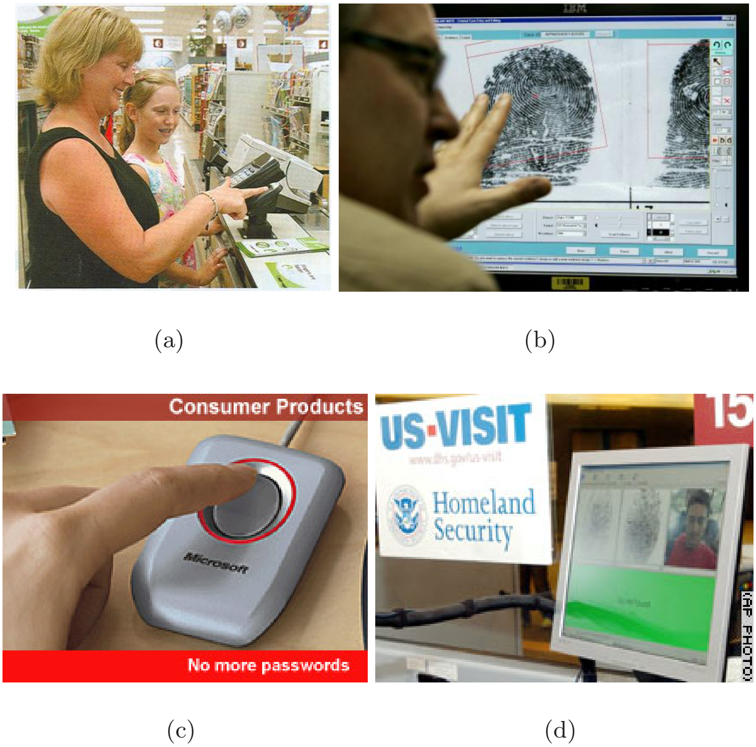
What physical measurements qualify to be useful in a biometric system? Any human anatomical or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic;
- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- Collectability: the characteristic can be measured quantitatively.

However, in a practical biometric system (i.e., a system that employs biometrics for person recognition), there are a number of other issues that should be considered, including:

- Performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired performance, as well as the operational and environmental factors that affect the performance;
- Acceptability, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
- Circumvention, which reflects how easily the system can be fooled using fraudulent methods.

A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, be easy to use and be sufficiently robust to various fraudulent methods and attacks on the system. Among the various biometric measurements in use, systems based on fingerprints [3], face [4] and iris [5] have received the most attention in recent years. 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 enrolled template set in the system database. Depending on the application context, a biometric system may operate either in a verification mode or an identification mode [6] (see Figure 2). A biometric system is designed using the following four main modules: (i) sensor module, (ii) feature extraction module, (iii) matcher module, and (iv) system database module.



(a) (b)

(c) (d)

Fig. 1. Biometric systems are being deployed in various applications. (a) A Pay-by-Touch system (`www.paybytouch.com`) at a grocery store where customers pay by fingerprints; (b) An Interpol fingerprint expert identifies a tsunami victim using the victim's fingerprint at a laboratory in Phuket, Thailand; (c) A fingerprint verification system used for computer and network log-on and (d) The US-VISIT program currently employs two-print information to validate the travel documents of visitors to the United States (`www.dhs.gov`).

2 Issues and Research Directions in Biometrics

Two samples of the same biometric characteristic from the same person (e.g., two impressions of a user's right index finger) are not exactly the same due to imperfect imaging conditions (e.g., sensor noise), changes in the user's physical or behavioral characteristics (e.g., cuts and bruises on the finger), ambient conditions (e.g., temperature and humidity) and user's interaction with the sensor (e.g., finger placement). In other words, biometric signals have a large *intra-class variability*. Therefore, the response of a biometric matching system is a match score that quantifies the similarity between the input and the database template representation. A higher score indicates that the system is more certain that the two biometric measurements come from the same person. The system decision is regulated by the threshold: pairs of biometric samples generating scores

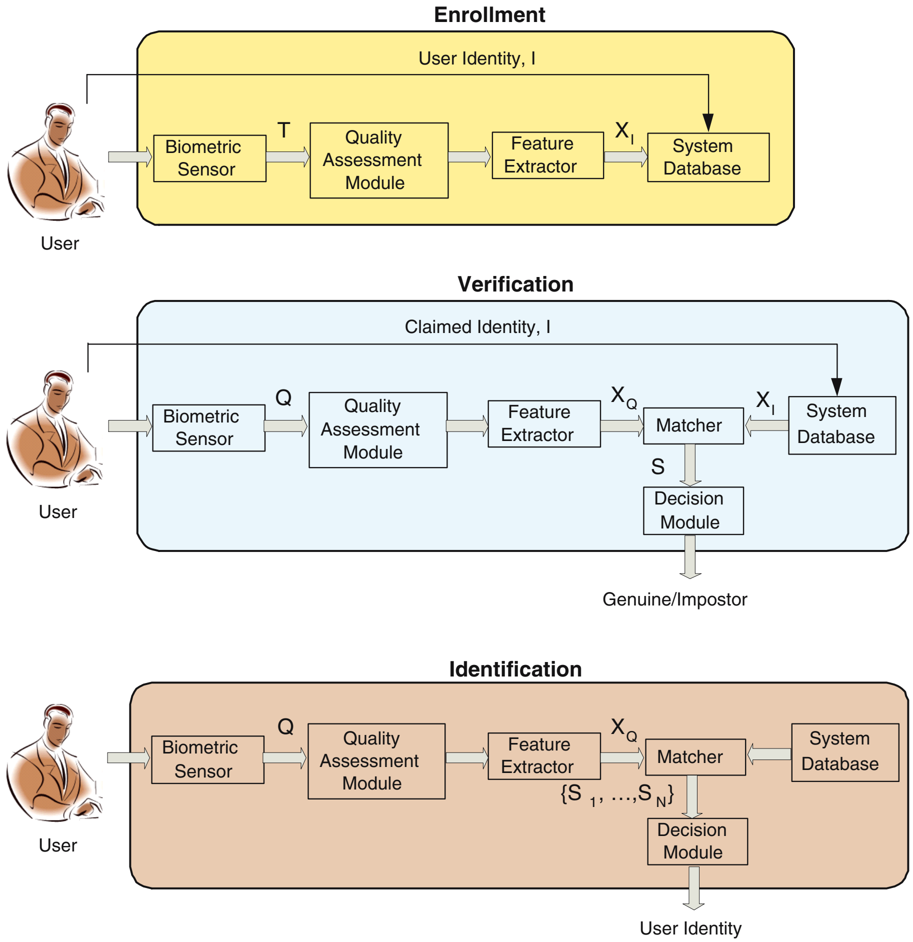


Fig. 2. Block diagrams of enrollment, verification, and identification tasks. Enrollment creates an association between an identity and its biometric characteristics. In a verification task, an enrolled user claims an identity and the system verifies the authenticity of the claim based on her biometric feature. An identification system identifies an enrolled user based on her biometric characteristics without the user having to claim an identity. Here, T represents the biometric sample obtained during enrollment, Q is the query biometric sample obtained during recognition, X_I and X_Q are the template and query feature sets, respectively, S represents the match score and N is the number of users enrolled in the database.

higher than or equal to the threshold are inferred as mate pairs (i.e., belonging to the same person); pairs of biometric samples generating scores lower than the threshold are inferred as non-mate pairs (i.e., belonging to different persons). A biometric verification system makes two types of errors: (i) mistaking biometric measurements from two different persons to be from the same person (called *false match*), and (ii) mistaking two biometric measurements from the same person to be from two different persons (called *false non-match*). These two types of errors are often termed as *false accept* and *false reject*, respectively.

Deployment of biometric systems in various civilian applications does not imply that biometric recognition is a fully solved problem. Table 1 presents the state-of-the-art error rates of four popular biometric traits. It is clear that there is a plenty of scope for improvement in the performance of biometric systems. We not only need to address issues related to reducing the error rates, but we also need to look at ways to enhance the usability of biometric systems and address the *return on investment* issue.

Table 1. False reject and false accept rates associated with state-of-the-art fingerprint, face, voice and iris verification systems. Note that the accuracy estimates of biometric systems are dependent on a number of test conditions (e.g., population characteristics and specific sensors used).

Biometric Trait	**Test**	**Test Conditions**	**False Reject Rate**	**False Accept Rate**
Fingerprint	FVC 2006 [7]	Heterogeneous population including manual workers and elderly people	2.2%	2.2%
	FpVTE 2003 [8]	U.S. government operational data	0.1%	1%
Face	FRVT 2006 [9]	Controlled illumination, high resolution	0.8%-1.6%	0.1%
Voice	NIST 2004 [10]	Text independent, multi-lingual	5-10%	2-5%
Iris	ICE 2006 [9]	Controlled illumination, broad quality range	1.1%-1.4%	0.1%

Biometric systems that operate using any single biometric characteristic have the following limitations: (i) noise in sensed data, (ii) intra-class variations, (iii) lack of distinctiveness [11], (iv) non-universality, and (v) spoof attacks. Some of the limitations imposed by unibiometric systems can be overcome by using multiple biometric modalities (such as face and fingerprint of a person or multiple fingers of a person). Such systems, known as multibiometric systems, are expected to be more reliable due to the presence of multiple, independent pieces of evidence [12]. These systems are also able to meet the stringent performance requirements imposed by various applications [13]. Multibiometric systems address the problem of non-universality, since multiple traits ensure sufficient population coverage. Further, multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. By asking the user to present a random subset of biometric traits (e.g., right index finger followed by right middle finger), the system ensures that a “live” user is indeed present at the point of data acquisition. Thus, a challenge-response type of authentication can be facilitated by using multibiometric systems. Of course, multibiometric systems involve additional cost and increase the enrollment and verification times.

With the widespread deployment of biometric systems in various applications, there are increasing concerns about the security and privacy of biometric technology [14]. Public confidence and acceptance of the biometrics technology will depend on the ability of system designers to demonstrate that these systems are robust, have low error rates and are tamper proof. To avert any potential security crisis, vulnerabilities of a biometric system must be identified and addressed systematically. A number of studies have analyzed potential security breaches in a biometric system and proposed methods to counter those breaches e.g. [15], [16]. In particular, biometric template security is an important issue because unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Due to intra-user variability in the acquired biometric traits, ensuring the security of the template without deteriorating the recognition performance is a challenging task. Although a number of biometric template protection schemes have been proposed [17,18,19,20,21], a comprehensive template protection mechanism with provable security guarantees and high recognition performance has thus far remained elusive and the development of such a mechanism is crucial when biometric systems proliferate into the core physical and information infrastructure in the near future.

3 Summary

Reliable personal recognition is critical to many government and business processes. The conventional knowledge-based and token-based methods do not really provide positive person recognition because they rely on surrogate representations of the person's identity (e.g., exclusive knowledge or possession). It is, thus, imperative that any system assuring reliable person recognition would involve a biometric component. This is not, however, to state that biometrics alone can deliver error-free person recognition. In fact, a sound system design will often entail incorporation of many biometric and non-biometric components (building blocks) to provide reliable person recognition. 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.

References

1. Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics 14, 4–20 (2004)
2. Wayman, J.L., Jain, A.K., Maltoni, D., Maio, D. (eds.): Biometric Systems, Technology, Design and Performance Evaluation. Springer, Heidelberg (2005)

3. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, Heidelberg (2003)
4. Li, S., Jain, A.K. (eds.): Handbook of Face Recognition. Springer, Heidelberg (2005)
5. Daugman, J.: Recognizing Persons by their Iris Patterns. In: Jain, A.K., Bolle, R., Pankanti, S. (eds.) Biometrics: Personal Identification in Networked Society, pp. 103–122. Kluwer Academic Publishers, London, UK (1999)
6. Jain, A.K., Bolle, R., Pankanti, S. (eds.): Biometrics: Personal Identification in Networked Security. Kluwer Academic Publishers, Dordrecht (1999)
7. Biometric System Laboratory - University of Bologna: FVC 2006: The Fourth International Fingerprint Verification Competition Available at `http://bias.csr.unibo.it/fvc2006/default.asp`
8. Wilson, C., Hicklin, A.R., Bone, M., Korves, H., Grother, P., Ulery, B., Micheals, R., Zoepfl, M., Otto, S., Watson, C.: Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report. Technical Report NISTIR 7123, NIST (2004)
9. Phillips, P.J., Scruggs, W.T., OToole, A.J., Flynn, P.J., Bowyer, K.W., Schott, C.L., Sharpe, M.: FRVT 2006 and ICE 2006 Large-Scale Results. Technical Report NISTIR 7408, NIST (2007)
10. Przybocki, M., Martin, A.: NIST Speaker Recognition Evaluation Chronicles. In: Odyssey: The Speaker and Language Recognition Workshop, Toledo, Spain, pp. 12–22 (2004)
11. Pankanti, S., Prabhakar, S., Jain, A.K.: On the Individuality of Fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence 24, 1010–1025 (2002)
12. Ross, A., Nandakumar, D., Jain, A.K.: Handbook of Multibiometrics. Springer, Heidelberg (2006)
13. Hong, L., Jain, A.K.: Integrating Faces and Fingerprints for Personal Identification. IEEE Transactions on Pattern Analysis and Machine Intelligence 20, 1295–1307 (1998)
14. Prabhakar, S., Pankanti, S., Jain, A.K.: Biometric Recognition: Security and Privacy Concerns. IEEE Security and Privacy Magazine 1(2), 33–42 (2003)
15. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security 1(2), 125–143 (2006)
16. Buhan, I., Hartel, P.: The State of the Art in Abuse of Biometrics. Technical Report TR-CTIT-05-41, Centre for Telematics and Information Technology, University of Twente (2005)
17. Teoh, A.B.J., Goh, A., Ngo, D.C.L.: Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence 28(12), 1892–1901 (2006)
18. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating Cancelable Fingerprint Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4), 561–572 (2007)
19. Juels, A., Sudan, M.: A Fuzzy Vault Scheme. In: Proceedings of IEEE International Symposium on Information Theory, Lausanne, Switzerland, p. 408 (2002)
20. Nandakumar, K., Nagar, A., Jain, A.K.: Hardening Fingerprint Fuzzy Vault Using Password. In: Proceedings of Second International Conference on Biometrics, Seoul, South Korea, pp. 927–937 (2007)
21. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Technical Report 235, Cryptology ePrint Archive (2006)