Biometric Recognition: How Do I Know Who You Are?

Anil K. Jain

Department of Computer Science and Engineering,
3115 Engineering Building, Michigan State University,
East Lansing, MI 48824, USA
jain@cse.msu.edu
http://biometrics.cse.msu.edu

Extended Abstract

A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust person recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics it is possible to confirm or establish an individual's identity based on who she is, rather than by what she possesses (e.g., an ID card) or what she remembers (e.g., 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]. 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 biological measurements qualify to be a biometric? Any human physiological and/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:

H. Kalviainen et al. (Eds.): SCIA 2005, LNCS 3540, pp. 1–5, 2005.

- 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, fingerprint-based systems [3] and face recognition systems [4] are the most popular.

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 a verification mode or an identification mode [5]. 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.

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 physiological 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 matching score that quantifies the similarity between the input and the database template representation. 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 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 three popular biometric traits. It is clear that there

Table 1. State-of-the-art error rates associated with fingerprint, face and voice biometric systems. Note that the accuracy estimates of biometric systems are dependent on a number of test conditions

	Test	**Test Parameter**	**False Reject Rate**	**False Accept Rate**
Fingerprint	FVC 2004 [6]	Exaggerated skin distortion, rotation, skin conditions	2%	2%
Face	FRVT 2002 [7]	Enrollment and test images were collected in indoor environment and could be on different days	10%	1%
Voice	NIST 2004 [8]	Text independent, multi-lingual	5-10%	2-5%

is a plenty of scope for improvement in the performance of biometric systems. We not only need to address issues related to reducing error rates, but we also need to look at ways to enhance the usability of biometric systems and address the *return on investment* issue.

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 [9], (iv) non-universality, and (v) spoof attacks. Some of the limitations imposed by unimodal biometric 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 multimodal biometric systems, are expected to be more reliable due to the presence of multiple, independent pieces of evidence [10]. These systems are also able to meet the stringent performance requirements imposed by various applications [11]. Multimodal biometric systems address the problem of non-universality, since multiple traits ensure sufficient population coverage. Further, multimodal biometric 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 multimodal biometric systems. Of course, multimodal biometric systems involve additional cost and increase the enrollment and verification times.

The utilization of digital techniques in the creation, editing and distribution of multimedia data offers a number of opportunities to a pirate user, such as high fidelity copying. Furthermore, Internet is providing additional channels for a pirate to quickly and easily distribute the copyrighted digital content without the fear of being tracked. As a result, the protection of multimedia content (image, video, audio, etc.) is now receiving a substantial amount of attention. Multimedia content protection that is based on biometric data of the users is

being investigated [12]. Password-only encryption schemes are vulnerable to illegal key exchange problems. By using biometric data along with hardware identifiers such as keys, it is possible to alleviate fraudulent usage of protected content [13].

In 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, obvious that any system assuring reliable person recognition must necessarily 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** (2004) 4–20
2. Wayman, J.L., Jain, A.K., Maltoni, D., Maio, D.: Biometric Systems, Technology, Design and Performance Evaluation. Springer (2005)
3. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer (2003)
4. Li, S., Jain, A.K.: Handbook of Face Recognition. Springer (2005)
5. Jain, A.K., Bolle, R., Pankanti, S.: Biometrics: Personal Identification in Networked Security. Kluwer Academic Publishers (1999)
6. Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain, A.K.: FVC2004: Third Fingerprint Verification Competition. In: Proceedings of International Conference on Biometric Authentication, LNCS 3072, Hong Kong (2004) 1–7
7. Philips, P.J., Grother, P., Micheals, R.J., Blackburn, D.M., Tabassi, E., Bone, J.M.: FRVT2002: Overview and Summary. (Available at `http://www.frvt.org/FRVT2002/documents.htm`)
8. Reynolds, D.A., Campbell, W., Gleason, T., Quillen, C., Sturim, D., Torres-Carrasquillo, P., Adami, A.: The 2004 MIT Lincoln Laboratory Speaker Recognition System. In: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, Philadelphia, PA (2005)
9. Pankanti, S., Prabhakar, S., Jain, A.K.: On the Individuality of Fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence **24** (2002) 1010–1025
10. Ross, A., Jain, A.K.: Information Fusion in Biometrics. Pattern Recognition Letters, Special Issue on Multimodal Biometrics **24** (2003) 2115–2125

11. Hong, L., Jain, A.K.: Integrating Faces and Fingerprints for Personal Identification. IEEE Transactions on Pattern Analysis and Machine Intelligence **20** (1998) 1295–1307
12. Uludag, U., Jain, A.K.: Multimedia Content Protection via Biometrics-based Encryption. In: Proceedings of IEEE International Conference on Multimedia and Expo, vol. III, Baltimore, USA (July 2003) 237–240
13. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric Cryptosystems: Issues and Challenges. Proceedings of IEEE, Special Issue on Multimedia Security for Digital Rights Management **92** (2004) 948–960