Biometric Recognition: How Do I Know Who You Are?

Anil K. Jain

Department of Computer Science and Engineering,
Michigan State University, MI 48824, U.S.A.
jain@cse.msu.edu

Abstract. Reliable person recognition is an integral component of identity management systems. Biometrics offers a natural and reliable solution to the problem of identity determination by recognizing individuals based on their physiological and/or behavioral characteristics that are inherent to the person. Although biometric systems have been successfully deployed in a number of civilian applications, current biometric systems are not perfect. In this paper, we describe the various obstacles that prevent biometric systems from achieving foolproof automatic person recognition. We also show that using multiple biometric modalities can alleviate some of the problems faced by unimodal biometric systems. Finally, we present the vulnerabilities of biometric systems and discuss solutions to protect biometric systems from some common attacks.

1 Biometric Recognition

A wide variety of systems require reliable person 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). Another emerging application of biometrics is in the domain of digital rights management. The utilization of digital techniques in the creation, editing and distribution of multimedia data offers a

F. Roli and S. Vitulano (Eds.): ICIAP 2005, LNCS 3617, pp. 19–26, 2005.

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 [3]. 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 [4].

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:

- 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 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 [5] and face recognition systems [6] 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. 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.

The response of a biometric 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 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.

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 [7]	Exaggerated skin distortion, rotation	2%	2%
	FpVTE 2003 [8]	U.S. government operational data	0.1%	1%
Face	FRVT 2002 [9]	Varied lighting, outdoor/indoor	10%	1%
Voice	NIST 2004 [10]	Text independent, multi-lingual	5-10%	2-5%

2 Multimodal Biometrics

Biometric systems that perform person recognition based on a single source of biometric information are often affected by the following problems [11]:

– Noisy sensor data : Noise can be present in the acquired biometric data mainly due to defective or improperly maintained sensors. For example, accumulation of dirt or the residual remains on a fingerprint sensor can result in a noisy fingerprint image. The recognition accuracy of a biometric system is highly sensitive to the quality of the biometric input and noisy data can result in a significant reduction in the accuracy of the biometric system [12].

- Non-universality: Not all biometric traits are truly universal. The National Institute of Standards and Technology (NIST) has reported that it is not possible to obtain a good quality fingerprint from approximately two percent of the population (people with hand-related disabilities, manual workers with many cuts and bruises on their fingertips, and people with oily or dry fingers) [13]. Hence, such people cannot be enrolled in a fingerprint verification system. Similarly, persons having long eye-lashes and those suffering from eye abnormalities or diseases cannot provide good quality iris images for automatic recognition [14]. Non-universality leads to Failure to Enroll (FTE) and/or Failure to Capture (FTC) errors in a biometric system.
- Lack of individuality: Features extracted from biometric characteristics of different individuals can be quite similar. For example, appearance-based facial features that are commonly used in most of the current face recognition systems are found to have limited discrimination capability [15]. A small proportion of the population can have nearly identical facial appearance due to genetic factors (e.g., father and son, identical twins, etc.). This lack of uniqueness increases the False Match Rate (FMR) of a biometric system.
- Lack of invariant representation: The biometric data acquired from a user during verification will not be identical to the data used for generating the user's template during enrollment. This is known as "intra-class variation". The variations may be due to improper interaction of the user with the sensor (e.g., changes due to rotation, translation and applied pressure when the user places his finger on a fingerprint sensor, changes in pose and expression when the user stands in front of a camera, etc.), use of different sensors during enrollment and verification, changes in the ambient environmental conditions (e.g., illumination changes in a face recognition system) and inherent changes in the biometric trait (e.g., appearance of wrinkles due to aging or presence of facial hair in face images, presence of scars in a fingerprint, etc.). Ideally, the features extracted from the biometric data must be relatively invariant to these changes. However, in most practical biometric systems the features are not invariant and therefore complex matching algorithms are required to take these variations into account. Large intra-class variations usually increase the False Non-Match Rate (FNMR) of a biometric system.
- Susceptibility to circumvention: Although it is difficult to steal someone's biometric traits, it is possible for an impostor to circumvent a biometric system using spoofed traits. Studies [16] have shown that it is possible to construct gummy fingers using lifted fingerprint impressions and utilize them to circumvent a biometric system. Behavioral traits like signature and voice are more susceptible to such attacks than physiological traits. Other kinds of attacks can also be launched to circumvent a biometric system [17].

Some of the problems that affect unimodal biometric systems can be alleviated by using multimodal biometric systems [18]. Systems that consolidate cues obtained from two or more biometric sources for the purpose of person recognition are called multimodal biometric systems. Multimodal biometric systems have several advantages over unimodal systems. Combining the evidence

obtained from different modalities using an effective fusion scheme can significantly improve the overall accuracy of the biometric system. A multimodal biometric system can reduce the FTE/FTC rates and provide more resistance against spoofing because it is difficult to simultaneously spoof multiple biometric sources. 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. However, multimodal biometric systems also have some disadvantages. They are more expensive and require more resources for computation and storage than unimodal biometric systems. Multimodal systems generally require more time for enrollment and verification causing some inconvenience to the user. Finally, the system accuracy can actually degrade compared to the unimodal system if a proper technique is not followed for combining the evidence provided by the different modalities. However, the advantages of multimodal systems far outweigh the limitations and hence, such systems are being increasingly deployed in security-critical applications.

The design of a multimodal biometric system is strongly dependent on the application scenario. A number of multimodal biometric systems have been proposed in literature that differ from one another in terms of their architecture, the number and choice of biometric modalities, the level at which the evidence is accumulated, and the methods used for the information fusion. Fusion at the matching score level is generally preferred due to the presence of sufficient information content and the ease in accessing and combining matching scores. A principled approach to score level fusion is the computation of likelihood ratios based on the estimates of genuine and impostor score distributions [19]. Information obtained from soft biometric identifiers like gender, ethnicity and height can also be integrated with the primary biometric information like face and fingerprint, to improve the recognition accuracy of the biometric system [20].

3 Biometric System Vulnerabilities

Biometric systems are vulnerable to several kinds of attacks that can compromise the security afforded by the biometric component and causing the failure of the system that it is intended to protect. Figure 1 summarizes the ways in which a biometric system can be attacked. The failure of a biometric system can be classified into two types. Large inter-class and small inter-class variability may result in the matcher erroneously accepting an impostor. Studies on the individuality of the biometric trait attempt to calculate the theoretical probability of this type of biometric system failure. For example, individuality of the minutiae information in a fingerprint was studied in [21].

The second kind of biometric system failure occurs when an impostor is deliberately attempting to masquerade the system. Ratha et al. [17] identified different levels of attacks that can be launched against a biometric system. These attacks are intended to either circumvent the security afforded by the system or

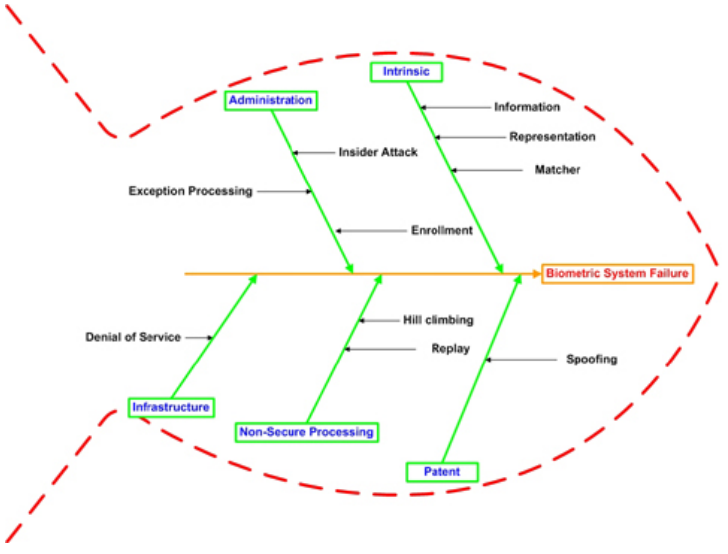

Fig. 1. Fishbone (cause & effect) illustration of biometric failures. The security afforded by a biometric system can be undermined by: (a) Administration: The system administrator can abuse and compromise the system. (b) Intrinsic: The inherent limitations of the representation/matching schemes may result in erroneously accepting an intruder. (c) Infrastructure: Denial of service attacks can disable system functionality. (d) Non-secure processing: An impostor can hack system processes to gain access into the system. (e) Patent: Since biometric identifiers are not secrets, an impostor could create physical or digital artifacts to fool the system.

to deter the normal functioning of the system: (i) A fake biometric trait such as an artificial finger may be presented at the sensor. (ii) Illegally intercepted data may be resubmitted to the system. (iii) The feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets. (iv) Legitimate feature sets may be replaced with synthetic feature sets. (v) The matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying the system security. (vi) The templates stored in the database may be modified or removed. Alternately, new templates may be introduced in the database. (vii) The data in the communication channel between various modules of the system may be altered. (viii) The final decision output by the biometric system may be overridden.

Among these attacks, the presentation of fake biometric traits at the sensor and the protection of biometric templates have been widely studied in the literature and a number of solutions have been proposed to guard against such attacks. A challenge-response type of authentication can prevent the problem of fake biometric submission to a great extent. Other methods such as detection of liveness during the presentation of the biometric trait have also been suggested.

For the protection of biometric templates, Jain and Uludag [22] suggested the use of steganography principles that hide biometric data (e.g., eigen-coefficients of a face image) in host images (e.g., fingerprints). Ratha et al. [23] proposed the use of distortion functions to generate biometric data that can be canceled if necessary. Thus, careful design and planning is necessary to ensure the integrity of the biometric system and thwart the impostor attempts to circumvent the security of the system.

4 Summary

Reliable person 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., eds.: Biometric Systems, Technology, Design and Performance Evaluation. Springer (2005)
3. 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
4. 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
5. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer (2003)
6. Li, S., Jain, A.K., eds.: Handbook of Face Recognition. Springer (2005)
7. 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, Hong Kong, China (2004) 1–7

8. Wilson, C., Hicklin, A.R., Korves, H., Ulery, B., Zoepfl, M., Bone, M., Grother, P., Micheals, R.J., Otto, S., Watson, C.: Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report. NIST Internal Report 7123; available at `http://fpvte.nist.gov/report/ir_7123_summary.pdf` (2004)
9. 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` (2002)
10. 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. Volume 1., Philadelphia, PA (2005) 177–180
11. Jain, A.K., Ross, A.: Multibiometric Systems. Communications of the ACM, Special Issue on Multimodal Interfaces **47** (2004) 34–40
12. Chen, Y., Dass, S.C., Jain, A.K.: Fingerprint Quality Indices for Predicting Authentication Performance. In: Proceedings of Fifth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA) (To appear), New York, U.S.A. (2005)
13. NIST report to the United States Congress: Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability. Available at `ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf` (2002)
14. News, B.: Long lashes thwart ID scan trial. Available at `http://news.bbc.co.uk/2/hi/uk_news/politics/3693375.stm` (2004)
15. Golfarelli, M., Maio, D., Maltoni, D.: On the Error-Reject Tradeoff in Biometric Verification Systems. IEEE Transactions on Pattern Analysis and Machine Intelligence **19** (1997) 786–796
16. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems. In: Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE. Volume 4677. (2002) 275–289
17. Ratha, N.K., Connell, J.H., Bolle, R.M.: An Analysis of Minutiae Matching Strength. In: Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), Sweden (2001) 223–228
18. Hong, L., Jain, A.K., Pankanti, S.: Can Multibiometrics Improve Performance? In: Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, New Jersey, U.S.A. (1999) 59–64
19. Dass, S.C., Nandakumar, K., Jain, A.K.: A Principled Approach to Score Level Fusion in Multimodal Biometric Systems. In: Proceedings of Fifth International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA) (To appear), New York, U.S.A. (2005)
20. Jain, A.K., Nandakumar, K., Lu, X., Park, U.: Integrating Faces, Fingerprints and Soft Biometric Traits for User Recognition. In: Proceedings of Biometric Authentication Workshop, LNCS 3087, Prague, Czech Republic (2004) 259–269
21. Pankanti, S., Prabhakar, S., Jain, A.K.: On the Individuality of Fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence **24** (2002) 1010–1025
22. Jain, A.K., Uludag, U.: Hiding Biometric Data. IEEE Transactions on Pattern Analysis and Machine Intelligence **25** (2003) 1493–1498
23. Ratha, N., Connell, J., Bolle, R.: Enhancing Security and Privacy in Biometrics-based Authentication Systems. IBM Systems Journal **40** (2001) 614–634