Volume 3, Issue 3, July 2016 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Biometric Recognition: Security and Privacy Concerns

Dr. Sudeep Kishore Sharma
Professor
St. Aloysius Institute of Technology
Jabalpur (M.P.), [INDIA]
Email: sharma.sudeepcs@rediffmail.com

Amaresh Singh
Assistant Professor
St. Aloysius Institute of Technology
Jabalpur (M.P.), [INDIA]
Email: prempsgtech12@gmail.com

ABSTRACT

A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. In some applications, biometrics can replace or supplement the existing technology. In the absence of robust personal 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.

Keywords:—*Biometrics, identification, multimodal biometrics, recognition, verification. Privacy, Databases, Protection, Humans, Robustness, Pattern recognition*

I. INTRODUCTION

Biometric technology is used for automatic personal recognition based on biological traits—fingerprint, iris, face, palm print, hand geometry, vascular pattern. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process (either automated or human-assisted) uses the results from the matching component to make a system-level decision." [15]. A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. One emerging technology that is becoming more widespread in such organizations is biometrics—automatic personal recognition based on physiological or behavioral characteristics.[1] Biometric identifiers also carry risks. Engineering professor, Tsutomu Matsumoto, demonstrated this point by using a digital camera, a PC, and gelatin to fashion a fake finger which fooled biometric scanners 80% of the time. [16] However, new applications can detect fakes by identifying sweat pores, measuring conduction properties, and determining the differences in how a live finger and a dummy finger deform the surface of a sensor. [17]

2. VARIOUS BIOMETRICS SYSTEMS

A number of biometric characteristics exist and are in use in various applications each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications.

A brief introduction to the commonly used biometrics is given below.

DNA: Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality

Three issues limit the utility of this biometrics for other applications:

1. ***Contamination and sensitivity:*** it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose;

2. ***Automatic real-time recognition issues:*** the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line noninvasive recognition; and

3. ***Privacy issues:*** information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.

Ear: It has been suggested that the shape of the ear and the structure of the cartilegenous tissue of the pinna are distinctive.

Face: Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition.

The verification performance of the face recognition systems that are commercially available is reasonable [11]. a large number of identities with an extremely high level of confidence [12]. A facial recognition system to work well in practice.

Facial, hand, and hand vein infrared thermogram: The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph.

Fingerprint: Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [13].

Gait: Gait is the peculiar way one walks and is a complex spatiotemporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications.

Hand and finger geometry: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers.

Iris: The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost- effective.

Keystroke: It is hypothesized that each person types on a keyboard in a characteristic way.

Odor: It is known that each object exudes an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds.

Palmprint: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper [14].

Retinal scan: The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not

easy to change or replicate the retinal vasculature.

Signature: The way a person signs his or her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification.

Voice: Voice is a combination of physiological and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound.

3. BIOMETRIC SYSTEMS

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses. Depending on the application context, a biometric system typically operates in one of two modes: verification or identification Figure 1.

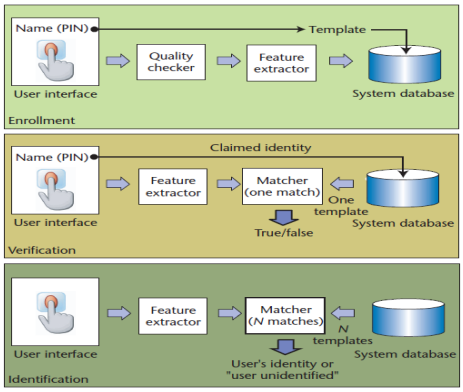

Figure 1. Block diagrams of enrollment, verification, and identification tasks. Enrollment creates an association between an identity and its biometric characteristics. In a verification task, an enrolled user claims an identity and the system verifies the authenticity of the claim based on her biometric feature. An identification system identifies an enrolled user based on her biometric characteristics without the user having to claim an identity.

Claims an Identity

Usually via a personal identification number (PIN), login name, smart card, or the like—and the system conducts a one-to-one comparison to deter-mine whether the claim is true. The question being answered is, "Is this person Bob?" Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. Figure 1 contains block diagrams of a verification system and an identification system, both performing the task of user enrollment.

Measurement requirements

What biological measurements qualify as biometrics? Any human physiological or behavioral trait can serve 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 different in terms of the characteristic.
- ***Permanence***. The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- ***Collectibility***. The characteristic should be quantitatively measurable.

Biometric System Errors

The distribution of scores generated from pairs of samples from different persons is called an impostor distribution; the score distribution generated from pairs of samples from the same person is called a genuine distribution (see Figure 2).

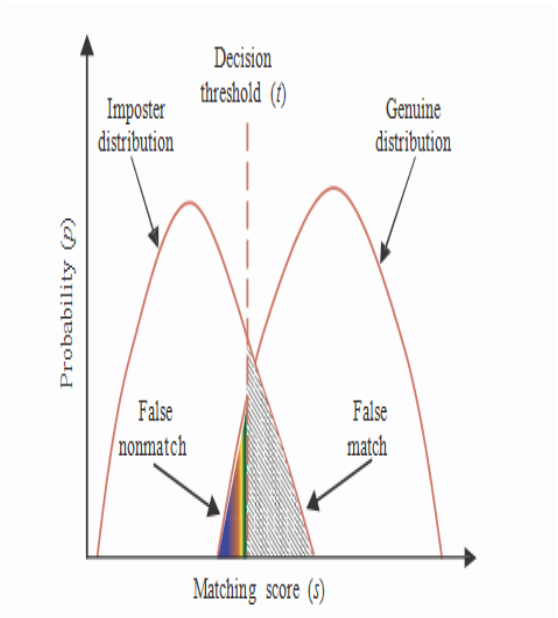

Figure 2. Biometric system error rates: The curves show false match rate (FMR) and false nonmatch (FNMR) rate for a given threshold t over the genuine and impostor score distributions. FMR is the percentage of nonmate pairs whose matching scores are greater than or equal to t, and FNMR is the percentage of mate pairs whose matching scores are less than t

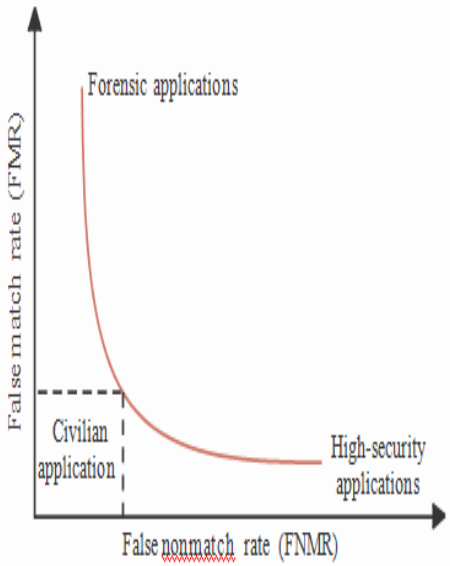

Figure 3. Receiver operating characteristic curve: Different biometric application types make different trade-offs between the false match rate and false nonmatch rate (FMR and FNMR). Lack of understanding of the error rates is a primary source of confusion in assessing system accuracy in vendor and user communities alike.

In fact, both FMR and FNMR are functions of the system threshold t: If the system's designers de-crease t to make the system more tolerant to input variations and noise, FMR increases. FTE errors typically occur when the system rejects poor-quality templates during enrollment. Consequently, the database contains only high-quality templates, and the perceived system accuracy improves. Because of the interdependence among the failure rates and error rates, all these rates—FTE, FTC, FNMR, and FMR—constitute important performance metrics of a biometric system.

We can depict system performance at all operating points (thresholds t) in the form of a receiver operating characteristic (ROC) curve. An ROC curve plots FMR against (1 – FNMR) or FNMR for various values of threshold t (see Figure 3).

Comparison of Biometrics

Several biometric characteristics are in use in various applications. Each biometric has its strengths and weaknesses, and the choice typically depends on the application. No single biometric can effectively meet the requirements of all applications—none is "optimal." We match a specific biometric to an application depending on the application's operational mode and the biometric characteristic's properties.

Applications of Biometric Systems

Biometric applications fall into three main groups: commercial applications, such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit cards, physical access control, cellular phones, PDAs, medical records management, and distance learning; government applications such as national ID cards, correctional facilities, driver's licenses, social security,

border control, passport control, and welfare-disbursement; and forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

Figure 4 shows some examples of biometric applications in use. Traditionally, commercial applications have used knowledge-based systems employing PINs and passwords, government applications have utilized systems based on tokens such as ID cards and badges, and forensic applications have relied on human experts to match biometric features.

Figure 4. Biometrics application examples. (a) Digital Persona's fingerprint verification system provides personal recognition for computer and network login. (b) Indivos manufactures a fingerprint- based point-of-sale (POS) terminal that verifies customers before charging their credit cards. (c) BioThentica's fingerprint-based door lock restricts access to premises. (d) The Inspass immigration system, developed by Recognition Systems and installed at major airports in the US, uses hand geometry verification technology.

Positive recognition: Commercial applications

Passwords are easy to crack by guessing or by simple brute-force dictionary attacks. Although it is possible, and even advisable, to keep different passwords for different applications and to change them frequently, most people use the same password across different applications and never change it. Trojan horse attacks against a biometric system's modules and replay attacks against its communication channels are similar to those against password-based personal recognition systems. We can secure biometric systems against these attacks using the building blocks of standard cryptographic techniques.

With standing brute-force attacks

Now let us consider a brute-force attack on a commercial biometric system operating in verification mode. A brute-force attack's chances of success depend on the bio-metric verification's matching accuracy for example fake figure prints Figure 5.

The only obvious solution for building accurate identification systems for large-scale applications appears to be multi-modal-biometric systems (for example, requiring multiple fingerprints, a face and fingerprint, or some other combination, from each user).[3]

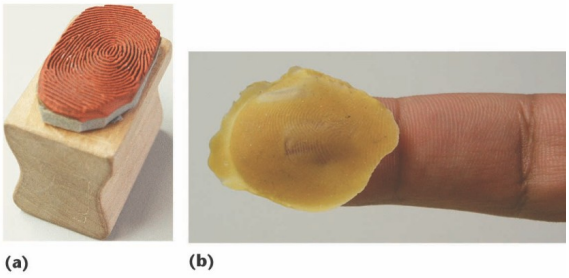

Figure 5. Fake fingers made from consenting users. (a) Rubber stamp made from a live-scan fingerprint image. (b) Wafer-thin plastic sheet housing a three-dimensional replication of a fingerprint.

Vitality detection and multimodal-biometrics for increased security

Many commercial applications could improve their personal recognition systems' security by adding required credentials or building blocks—for example, using a token or password together with biometric recognition. However, in high-security applications (such as access control to nuclear energy facilities), it is important that each component of the recognition system is secure in it-self and that the many components provide additional layers of security. Therefore, in our opinion, the best method for vitality detection is to use a characteristic distinctive to each individual,

and not easily available to an adversary for copying—that is, another biometric.

Replacing compromised biometrics

One disadvantage of biometrics is that they cannot be easily revoked.[7] If a biometric is ever compromised, it is compromised forever. With a credit card, the bank can issue the user a new card with a new number. But a user has only a limited number of biometrics—one face, 10 fingers, and so on—and they are not easy to replace. Also, because different applications might use the same biometric, a thief who acquires a person's biometric in one application could also use it in others. Ultimately, in commercial applications, the decision to add or replace existing personal recognition methods with biometrics-based solutions should be based on a cost-benefit analysis.

Negative recognition: Government and forensic applications

To illustrate the difference, let us suppose airport authorities are looking for the FBI's 100 most-wanted criminals (yielding a database size of 100), and that the state-of-the-art fingerprint verification system operates at 1 percent FNMR and 0.001 percent FMR. If we deployed this system in verification mode, it would fail to match the correct users 1 percent of the time and erroneously verify wrong users 0.001 percent of the time. In our opinion, using biometrics in negative recognition applications does not infringe on civil liberties be-cause unless you are already in the "criminal database," the recognition system has no record of you. However, we do need appropriate legislation to protect the abuse of such systems.

Privacy and biometrics

Privacy is the ability to lead your life free of intrusions, to remain autonomous, and to control access to your personal information. As the incidence and magnitude of identity fraud increase, strong biometrics such as fingerprints will increasingly come into play for positively recognizing people; the conventional technologies—knowledge- or token- based, for example—cannot deliver this functionality.

Finally, the use of biometrics indeed raises several privacy concerns. A sound trade-off between security and privacy might be necessary; but we can only enforce collective accountability and acceptability standards through common legislation. On the positive side of the privacy issue, biometrics provides tools to enforce accountable logs of system transactions and to protect individuals' right to privacy. As biometric technology matures, interaction will in-crease among applications, the market, and the technology. The technology's value, user acceptance, and the service provider's credibility will influence this interaction. It is too early to predict where and how biometric technology will evolve and which applications will ultimately embed it. But it is certain that biometric-based recognition will profoundly influence the way we conduct our daily business

REFERENCES:

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

[2] Best Practices in Testing and Reporting Biometric Device Performance, version 2.0, tech. report, United Kingdom Biometric Working Group, 2002; www.cesg.gov.uk/ technology/ biometrics.

[3] D. Maltoni et al., Handbook of Fingerprint Recognition, Springer, 2003.

[4] Password Clues, The Central Nic Password Survey Report, Central Nic, 13 July 2001; www.centralnic.com/ page. php?pid=73.

[5] D. Maio et al., "FVC2002: Second Fingerprint Verification Competition," Proc. Int'l Conf. Pattern Recognition, vol. 3, IEEE CS Press, 2002, pp. 811–814.

[6] T. Matsumoto et al., "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, Int'l Soc. for Optical Engineering, 2002, pp. 275–289.

[7] B. Schneier, "Inside Risks: The Uses and Abuses of Biometrics," Comm. ACM, vol. 42, no. 8, Aug. 1999, 136.

[8] Jules and M. Sudan, "A Fuzzy Vault Scheme," Proc. IEEE Int'l Symp. Information Theory, IEEE Press, 2002, 408.

[9] J.D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?" Proc. IEEE, vol. 85, no. 9, Sept. 1997, pp. 1480–1492.

[10] European Data Directive 95/46/EC, Feb. 1995; www. privacy.org/pi/ intl_orgs/ec/final_EU_Data_ Protection. html.

[11] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. FRVT 2002: Overview and Summary. [Online]. Available: http://www.frvt.org/ FRVT2002/documents.htm

[12] M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," IEEE Trans. Pattern Anal. Machine Intell., vol. 19, pp. 786–796, July 1997.

[13] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint verification competition," in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, Aug. 2002, pp.744 –747.

[14] D. Zhang and W. Shu, "Two novel characteristic in palmprint verification: Datum point invariance and line feature matching," Pattern Recognit., vol. 32, no. 4, pp. 691–702, 1999.

[15] "Biometrics Overview." National Science and Technology Council. http://www.biometricscatalog.org/ NSTCSubcommittee/Documents/ Biometrics Overview.pdf.

[16] "Doubt cast on fingerprint security." BBC News, May 17, 2002.

[17] Jain, Anil K. and Sharathchandra Pankanti. "A Touch of Money." IEEE Spectrum, July 2006. p. 22-27

* * * * *