The Role of Biometrics in Virtual Communities and Digital Governments

Chang-Tsun Li

Department of Computer Science
University of Warwick
Coventry CV4 7AL
UK
Tel: +44 24 7657 3794
Fax: +44 24 7657 3024
E-mail: ctli@dcs.warwick.ac.uk

The Role of Biometrics in Virtual Communities and Digital Governments

Abstract

This chapter is intended to introduce the role of biometrics in virtual communities and digital governments. Key steps for a biometric system to complete an identification or verification / authentication process are introduced. Main biometric techniques, such as fingerprint recognition, face recognition, iris recognition, and voice recognition, for the security purposes of identification and authentication are included. The key features need to be extracted and technical challenges posed to each individual technique will also be covered. We will also discuss the applications, requirements, technical limitations, and issues of privacy intrusion, and point out the trends in the development of biometric systems in the future.

INTRODUCTION

Pervasive services of virtual communities and digital governments are achievable only if trust, privacy and security can be secured and strengthened. To meet these requirements, mechanisms, which provide secure management of information and facilities without compromising privacy and civil rights, have to be devised. The success of such mechanisms relies on effective identity authentication. While traditional security measure such as PINs and passwords may be forgotten, stolen, or cracked, biometrics provides authentication mechanisms based on unique human physiological and behavioral characteristics that can be used to identify an individual or authenticate the claimed identity of an individual, but cannot be easily duplicated

or forged. Typical characteristics include but not limit to fingerprint, face, iris, hand geometry, palm, voice pattern, signature, keystroke dynamics, etc. Moreover, in the light of homeland security, biometrics has become a powerful measure in the government's fight against identity fraud, illegal immigration, illegal workers, and terrorism. It is also useful in preventing abuses of the public health services and other government entitlement.

BIOMETRIC TECHNIQUES

Biometrics is concerned with the techniques harnessing various human physiological and behavioral characteristics. Usually, for a biometric system to complete an identification or verification / authentication process, five major steps have to be taken:

1. *Sample capturing*: An input device such as fingerprint reader, microphone, or camera is required for capturing and digitizing a biometric sample.
2. *Sample processing*: Operations such denoising, enhancing, contrasting, or filtering may be necessary for compensating sensor and environment imperfection so as to smooth the way for feature extraction.
3. *Feature extraction*: This step extracts salient features from the pre-processed sample. Features exploited by various biometric systems will be discussed later in this section.
4. *Template construction*: A compact and invariant descriptor, called template, is constructed based on the extracted features to represent each sample.
5. *Template matching*: To identify or authenticate a person, the person’s template constructed is matched against the existing templates stored in the database. An authentication decision is usually made on the basis of a similarity measure.

Reliable features extraction is the key to the success of a biometric recognition system. Although there is a wide spectrum of modalities, we will only focus on four mainstream techniques currently in widespread use and the features they exploit.

Fingerprint Recognition

Fingerprint recognition systems attempt to extract the location and orientation of bifurcations and endings of ridge, peak, and valley on fingerprints, which distinguish one finger from another. Main technical challenges pose to fingerprinting systems are wounds, dry/oily fingers, pressure and location of finger placement on the fingerprint reader. Full coverage of this technique can be found in (Maltoni et al., 2003).

Face Recognition

Main features to be extracted for comparison are positions of cheekbones, and positions and shapes of eyes, mouth, and nose. Though 2D face recognition technologies have been making steady progress with some success, obstacles have been encountered in some practical applications. For example, poor illumination, rotated facial images, glasses, and facial expressions may degrade the performance of face recognition systems. Another problem with face recognition systems in screening or surveillance applications is that in environments such as shopping malls and railway stations with moving crowds, the tasks of detecting faces, matching faces against the stored templates in the database, and manually resolving false matches are time consuming. Good reviews can be found in (Kong et al., 2004).

Iris Recognition

Iris is the colored portion that surrounds the pupil of the eye. Among various parts of the human body, the one gives most information is the eye. The iris is unique and remains invariant over time. Compared to another form of eye recognition - retina recognition, iris recognition is less invasive, more accurate, and less expensive. One of the prominent algorithms was developed by Daugman (2004). With the algorithm, an image of the iris is converted into a digitized code. For security sake, the code is usually hashed and encrypted. High-end systems can accommodate users wearing glasses and contact lenses.

Voice Recognition

Voice recognition, sometimes confused with speech recognition that aims at recognizing what the speaker is saying rather than at who is speaking, is a biometric method intended for recognizing who is speaking rather than what the speaker is saying. Therefore voice recognition is also called speaker recognition. Frequency, cadence, and duration of voice pattern are the main feature voice authentication systems are looking for. Cold, illness, background noises, and poor microphone positioning may pose problems for the system. Another limitation of this technique is that system training for each person is needed. The reader is referred to (Ramachandran et al. 2002) for more details.

APPLICATIONS OF BIOMETRICS

There are two different purposes of resolving personal identity: *verification / authentication* and *identification*. Verification / authentication is concerned with

confirming or rejecting a claimed identity, i.e., the system is expected to answer the question of “Is the user whom she/he claims she/he is?”. Basically, this is a *one-to-one* comparison process in which the user claims her/his identity by submitting a biometric sample and the system has to verify it against only the registered template of the claimant’s. Identification is about establishing a user's identity. This is a *one-to-many* comparison in which, without a claimed identity, the system is expected to report the identity of the user if the submitted sample matches one of the registered templates.

The following list is not intended to be exhaustive, but to highlight the areas where biometrics is applicable.

- Criminal identification and prison security
- Prevention of unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, computer networks, shopping malls, and other facilities and government installations.
- Replacing vehicle keys with key-less entry and key-less ignition
- Border control and airport security
- Travel document (driver license, visa, passport)
- Battling benefit and entitlement frauds
- Voter registration
- National identification

ISSUES OF BIOMETRICS

The deployment of biometric systems in some verification-oriented applications, such as ATM application and national identity card, requires the users to enroll with their personal traits, which may sometimes raise concern about privacy intrusion. Even in

some identification-oriented applications, such as border/port control and shopping mall security, where pre-enrollment is not necessary; users' fear of having their biometric samples abused still cannot be eliminated.

By submitting a prerecorded biometric sample of an enrolled person, a non-enrolled person can fool the authentication systems. On the other hand, by using a mask and makeup, an enrolled/registered person may circumvent an identification system based on face recognition techniques. These types of impersonation attack all need to be tackled when developing and deploying biometric systems.

While new PINs and passwords can be issued when an old one is stolen, the invariance of biometric characteristics and the limited number of body parts make reissuance virtually impossible – each person has only one face and at most two irises. This limitation makes the problem of identity theft (Scheier, 1999) an acute issue. The reader is referred to Bolle et al. (2002) and Ratha et al. (2003) for more details on security threats to biometrics systems.

CONCLUSIONS AND TRENDS

Technically, new methods such as instant DNA testing, 3D face recognition, thermal imaging, palm recognition, non-invasive retina recognition, gait, and brain wave scanning will draw reasonable attention from the researchers in the future. As expectations for better performance and higher anti-spoofing strength grow, more systems that fuse multiple biometric modalities are anticipated to be developed and deployed (Ross & Jain, 2003; Rukhin & Malioutov, 2005). To resolve the non-reissuable problem and thwart identity theft, researches on cancelable biometrics (Bolle, et al. 2002 & Connie, Teoh, Goh & Ngo, 2005), a technique that allows the user to choose non-invertible transformation functions to be operated on her/his

original biometric sample in order to generate multiple variants to represent the same person, is expected to gain more momentum. Standardization facilitates interoperability and data exchange among systems. Uniform file and template formats, anti-spoofing techniques, security practices, device testing, application interfaces, biometric terminology, etc., are the areas where the industry will have to look into to realize standardization.

REFERENCES

Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002). Biometric perils and patches. *Pattern Recognition 35*(12), 2727-2738.

Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005). PalmHashing: a novel approach for cancelable biometrics. *Information Processing Letters*, *93*(1), 1-5.

Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and systems for video technology 14*(1), 21-29.

Kong, S. G., Heo, J., Abidi, B. R., Paik, J., & Abidi, M. A. (In press) Recent advances in visual and infrared face recognition – a review. *Computer Vision and Image Understanding*.

Maltoni, D., Maio, D., Jain, A. K., & Salil Prabhakar, S. (2003). Handbook of Fingerprint Recognition. Springer Verlag.

Ramachandran, R. P., Farrell, K. R., Ramachandran, R., & Mammone, R. J. (2002). Speaker recognition—general classifier approaches and data fusion methods. *Pattern Recognition 35*(12), 2801-282*1*.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2003). Biometrics break-ins and band-aids. *Pattern Recognition Letters 24*(13), 2105-2113.

Ross, A. & Jain, A. (2003). Information fusion in biometrics. *Pattern Recognition*

Letter 24(13), 2115-2125.

Rukhin, A. L. & Malioutov, I. (2005). Fusion of biometric algorithms in the recognition problem. *Pattern Recognition Letters*, *26*(5), 679-684.

Scheier, B. (1999). Inside risks: the uses and abuses of biometrics, *ACM* Communications *42*. 136.

TERMS AND DEFINITIONS

Biometrics: The science of automatically identifying people or verifying people's identity based on unique human physiological or behavioral characteristics such as face, fingerprint, iris retina, voice, etc.

Identity theft: The act of using someone else's personal information such as name, PIN, or even biometric data, without her/his knowledge for malicious purposes.

Verification/Authentication: A one-to-one matching process for determining whether the user is indeed the one she/he claims she/he is.

Identification: A one-to-many matching process for establishing the identity of the user if the submitted biometric sample matches one of the registered templates.

Fingerprinting: A technique for identity verification or identification based on the users' fingerprint features such as location and orientation of bifurcations and endings of ridge, peak, and valley.

Face recognition: A technique for identity verification or identification based on the users' facial features such as positions of cheekbones, and positions and shapes of eyes, mouth and nose.

Iris recognition: A technique for identity verification or identification based on the users' encoded iris pattern.

Voice recognition: A technique for identity verification or identification based on the

users' vocal features such as frequency, cadence, and duration of voice pattern.

Cancelable biometrics: A technique that allows the user to choose non-invertible transformation functions to be operated on her/his original biometric sample in order to generate multiple variants to represent the same person.