**IJITKM** Volume 7 • Number 1 • December 2013 pp. 112-116 (ISSN 0973-4414)

# Biometric Recognition Challenges

Dr. Chander Kant, Archana Toky
Assistant Professor, Deptt. of computer Science & Appl. K.U. Kurukshetra
Faculty, Deptt. Of Computer Science, Govt. College for women, Hisar
ckverma@rediffmail.com, archanatoky@gmail.com

**Abstract**
Authentic person identification is an important problem in many applications. The purpose of such schemes is to ensure that the particular services are accessed only by a legal user and no one else. n the absence of proper recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometrics, identification based on distinct personal traits, has the potential to become key part of any identification system. Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. With the availability of inexpensive biometric sensors and computing power, it is becoming increasingly clear that widespread usage of biometric person identification is being blocked by our lack of understanding of three fundamental problems: (i) How to accurately and efficiently represent and recognize biometric patterns? (ii) How to guarantee that the sensed measurements are not fraudulent? And (iii) How to make sure that the application is indeed exclusively using pattern recognition for the expressed purpose. For these reasons, we view biometrics as a grand challenge - "a fundamental problem in science and engineering with broad economic and scientific impact".
*Key Words*—Biometrics, multimodal biometrics, recognition, identification, verification.

## 1. Introduction

Person identification is an integral part of the infrastructure needed for diverse business sectors, transportation, entertainment, law enforcement, security, access control, border control, government, communication etc. As our society becomes electronically connected to form one big global community, it has become necessary to carry out reliable person identification often remotely and through automatic means. Substitute representations of identity such as passwords and cards no longer suffice. Further, passwords and cards can be shared and thus cannot provide non-repudiation.

Biometrics, which refers to automatic identification of people based on their distinctive physiological (e.g., face, fingerprint, iris, retina, hand geometry) and behavioral (e.g., voice, gait) characteristics, should be an essential component of any effective person identification solution because biometric identifiers cannot be shared, misplaced, and they intrinsically represent the individual's identity [1]. Consequently, biometrics is not only an important pattern recognition research problem but is also an enabling technology that will make our society safer, reduce fraud and lead to user convenience generally providing the following three functionalities: (a) Positive Identification ("Is this person who he claims to be?"). A positive identification verifies the authenticity of a claimed enrolled identity based on the input biometric sample. For example, a person claims that he is Dr. Subhash to the authentication system and offers his fingerprint; the system then either accepts or rejects the claim based on a single match performed between the input pattern and the enrolled pattern associated with the claimed identity. (b) Large Scale Identification- also referred to as negative identification ("Is this person in the database?"). Given an input biometric sample, a large-scale identification determines if the pattern is associated with any of a large number (e.g., millions) of enrolled identities. These large-scale identification applications require a large sustainable throughput with as little human supervision as possible.

## 2. Biometric Systems

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 *verification* mode or *identification* mode (Figure 1) [2]. In the verification mode, the system validates a person's identity by comparing the captured biometric data with his own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not. Identity verification is typically used for *positive recognition*, where the aim is to prevent multiple people from using the same identity.

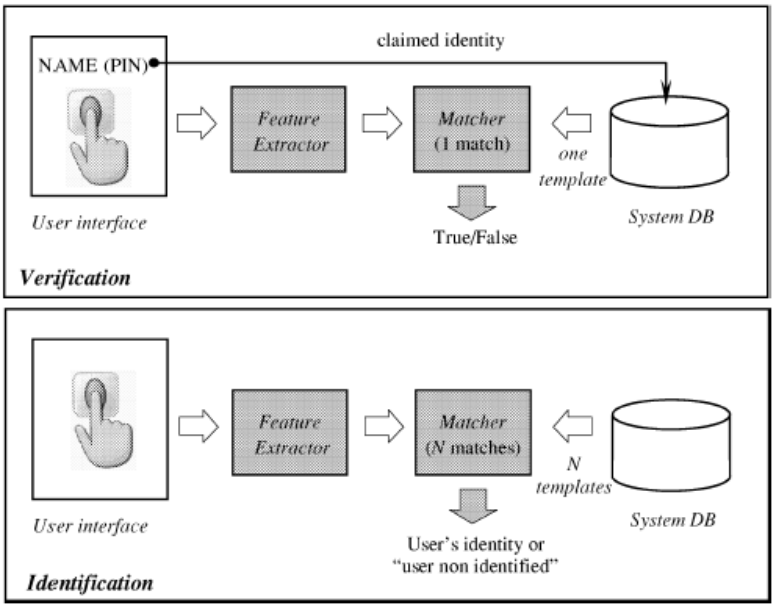


Figure1. Verification and identification tasks of a biometric system

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity. Identification is a critical component in *negative recognition* applications where the system establishes whether the person is who he denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities.

**3. Biometrics Challenges**

Here we categorize the fundamental barriers of biometrics into four main categories [3]:
(a) Accuracy (b) Scale (c) Security (d) Privacy.

***3.1 Accuracy***

The critical promise of the ideal biometrics is that when a biometric identifier sample is presented to the biometric system, it will offer the correct decision. Unlike password or token-based system, a practical biometric system does not make perfect match decisions and can make two basic types of errors: (i) False Match: the biometric system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database or the pattern associated with an incorrectly claimed identity (ii) False Non-match: the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database (identification/screening) or the pattern associated with the correctly claimed identity (verification).

***3.2 Scale***

How does the number of identities in the enrolled database affect the speed performance of the system? In the case of verification systems, the size of the database does not really matter since it essentially involves a 1:1 match. In the case of large scale identification and screening systems containing a total of N identities, sequentially performing N 1:1 matches is not effective (see Table 3); there is a need for efficiently scaling the speed of the system with an increase in the size of the database.

| | Authenti-cation | Large Scale ID throughput | Screening throughput |
|---|---|---|---|
| Finger | 10 msec | 1/min | >1/sec |
| Face | 90 µsec | 0.66/min | 22/sec |
| Iris | < 1 µsec | > 1/sec | >2000/sec |

Table3. Performance for commonly used biometric technologies.

Typical approaches to scaling include using multiple hardware units and coarse pattern classification (e.g., first classifying a fingerprint into major classes such as Arch, Tented Arch, Whorl, Left loop and Right loop). Both these approaches do not perform well in practice. Using hardware linearly proportional to the database size is not feasible. Therefore, in large scale applications, the throughput issues are also critical in screening applications.

### *3.3 Security*

The integrity of biometric systems, i.e., assuring that the input biometric sample was indeed presented by its legitimate owner, and the system really matched the input pattern with genuinely enrolled pattern samples, is crucial. While there are a number of ways a executor may attack a biometric system [4], there are usually two very serious criticisms against biometric technology that have not been addressed satisfactorily: (i) biometrics are not secrets and (ii) enrolled biometric templates are not revocable. The first fact implies that the attacker has a ready knowledge of the information in the legitimate biometric identifier and, therefore, could fraudulently inject it into the biometric system to gain access. The second fact implies that when biometric identifiers have been "compromised", the legitimate user has no recourse to revoking the identifiers to switch to another set of uncompromised identifiers. We believe that the knowledge of biometric identifier(s) does not necessarily imply the ability of the attacker to inject the identifier measurements into the system. The challenge then is to design a secure biometric system that will accept only the legitimate presentation of the biometric identifiers without being fooled by the doctored or spoofed measurements injected into the system.

### *3.4 Privacy*

A reliable biometric system provides an undeniable proof of identity of the person. Consequently, the users have two concerns: Will the undeniable proof of biometrics-based access be used to track the individuals that may breach upon an individual's right to privacy? Will the biometric data be harmed for an unintentional purpose, e.g., will the fingerprints provided for access control is matched against the fingerprints in a criminal database? How would one ensure and assure the users that the biometric system is being used only for the intended purpose and none other? The problem of designing information systems whose functionality is verifiable at their deployed instantiation is very difficult. Perhaps, one needs to devise a system that meticulously records authentication decisions and the people who accessed the logged decisions using a biometric-based access control system [5]. Such a system can automatically generate alarms to the users upon observing a suspicious pattern in the system administrator's access of users' logs. One promising research direction may be biometric cryptosystems - generation of cryptographic keys based on biometric samples.

## 4. Advantages and Disadvantages of Biometrics

Let us now examine the advantages and disadvantages of biometrics in two groups of applications: the commercial positive recognition applications that may work either in the verification or the identification modes and the government and forensic negative recognition applications that require identification. The traditional technologies available to achieve a positive recognition include knowledge-based methods (e.g., PINs and passwords) and token-based methods (e.g., keys and cards) [6]. Most people set their passwords based on words or digits that they can easily remember, such as names and birthdays of family members, favorite movie or music stars, and dictionary words. Such passwords are easy to crack by guessing or by a simple brute force dictionary attack. Although it is possible, and even advisable, to keep different passwords for different applications and change them frequently, most people use the same password across different applications and never change them. If a single password is compromised, it may result in a breach in security in many applications. For example, a hacker may create a bogus web site that attracts users with free air miles if they were to register on the website with a login name and password. The hacker may then try to use the same login name and password to attack the users' corporate accounts, and most likely succeed. Longer passwords are more secured but harder to remember which prompts some users to write them down in accessible locations and hide it under the keyboard. Strong passwords are difficult to remember and result in more help desk calls for forgotten or expired passwords.

Cryptographic techniques such as encryption can provide very long passwords that are not required to be remembered but that are in turn protected by simple passwords, thus defeating their purpose. Further, a hacker needs to break only one password among all the employees to gain access to a company's Intranet and thus, a single weak password compromises the overall security of every system that the user has access to. Thus, the security of the entire system is only as good as the weakest password. Finally, when a password is shared with a colleague, there is no way for the system to know who the actual user is. Similarly, there are many problems with possession-based personal recognition. For example, keys and tokens can be shared, duplicated, lost or stolen and an attacker may make a "master" key that may open many locks. It is significantly more difficult to copy, share, and distribute biometrics with as much ease as passwords and tokens.

Biometrics cannot be lost or forgotten and online biometrics-based recognition systems require the person to be recognized to be present at the point of recognition. It is difficult to create biometrics and extremely unlikely for a user to reject, for example, having accessed a computer network. Further, all the users of the system have relatively equal security level and one account is no easier to break than any other. Biometrics introduces incredible convenience for the users while maintaining a sufficiently high degree of security.

Let us now consider a brute force attack on a biometric system operating in a verification mode in a commercial application [7]. The chance of success of a brute force attack depends on the matching accuracy of the biometric verification. Let us assume that a certain commercial biometric verification system wishes to operate at 0.001% FMR. At this setting, several biometric systems (e.g., the state-of-the-art fingerprint and iris recognition systems) can easily deliver less than 1% FNMR [3]. A FMR of 0.001% indicates that, if a hacker launches a brute force attack with a large number of different fingerprints, 1 out of 100 000 attempts will succeed on an average. This may be considered equivalent to the security offered by a randomly chosen five-digit PIN (although a brute force attack against a five-digit PIN is *guaranteed* to succeed in 100 000 attempts and requires only 50 000 attempts, on an average). To attack a biometric-based system, one needs to generate (or acquire) a large number of samples of that biometric (e.g., fingerprints), which is much more difficult than generating a large number of PINs/passwords. Finally, the FMR of a biometric system can be arbitrarily reduced for higher security at the cost of increased inconvenience to the users that results from a higher FNMR [8]. Note that a longer PIN or password also increases the security while causing more inconvenience in remembering and correctly typing them. Certain commercial applications would like to operate the biometric system in an identification mode instead of the verification mode for the added convenience of not requiring the users to claim an identity. Usually, speed is perceived as the biggest problem in scaling up an identification application. However, the fact is that the identification accuracy scales even worse than the speed. Consider an identification application with 10000 users. We can certainly find a combination of a fast fingerprint matching algorithm and special purpose hardware capable of making an identification in a few seconds. On the other hand, a matching algorithm with a verification FMR of 0.001% will have an identification $FMR_N$ of 10,000X0.001% = 10%. This implies that an impostor has a good chance of gaining access to the system by simply using all of the ten fingers on her two hands. Therefore, while small- to medium-scale commercial applications (e.g., a few hundred users) may still use single biometric identification, the only obvious solution for building a highly accurate identification system for large scale applications appears to be *multimodal biometric* systems [9]. For example, a system may combine face and fingerprint of a person or fingerprints from multiple fingers of a person for recognition. Finally, in commercial applications, addition or replacement of existing personal recognition methods with biometrics-based solutions should be based on a cost-benefit analysis.

## 5. Conclusions

Biometrics is one of the important and more interesting pattern recognition applications with its associated unique challenges. While this work emphasizes the open fundamental problems in biometrics, this should not be construed to imply that the existing biometric technology is not useful. In fact, there are a large number of biometric solutions that have been successfully deployed to provide useful value in practical applications. The scope of this paper is intended to expand the frontiers of the state of the art biometric technology performance for their effective widespread deployment. A successful biometric solution does not have to be 100% accurate or secure. In this work, we have explored the fundamental roadblocks for widespread adoption of biometrics as a means of automatic person identification: effective and efficient pattern recognition; ensuring system integrity and system application integrity. From system perspective, both security and privacy are open problems with no clear satisfactory solutions on the horizon. The recognition problems have historically been very elusive and have been underestimated in terms of the effort needed to arrive at a satisfactory solution. Additionally, since humans seem to identify people with high accuracy, biometrics has incorrectly been perceived to be an easy problem.

## 4. References

1. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", *Proceedings of* the *IEEE*, Vol. 91, No. 12, Dec. 2003, pp. 2019- 40.
2. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security & Privacy Concerns", *IEEE Security and Privacy Magazine*, Vol. 1, No. 2, pp. 33-42, March-April 2003.

3. R. Derakhshani R, S.A.C. Schuckers, L. Hornak, L. O'Gorman, "Determination of Vitality From A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners", *Pattern Recognition*, No.2, pp. 383-396, 2003.
4. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", *Proceedings of the IEEE*, *Special Issue on Enabling Security Technologies for Digital Rights Management*, Vol. 92, No. 6, June 2004.
5. P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J.M. Bone, "FRVT 2002: Evaluation Report", http://www.frvt.org/ DLs/FRVT_2002_Evaluation_Report.pdf, March 2003.
6. A. K. Jain, S. C. Dass and K. Nandakumar, "Soft Biometric Traits for Personal Recognition Systems", To appear in *Proceedings of International Conference on Biometric Authentication*, Hong Kong, July 2004.
7. A. K. Jain and A. Ross, "Multibiometric Systems", *Communications of the ACM*, *Special Issue on Multimodal Interfaces*, Vol. 47, No. 1, pp. 34-40, January 2004.
8. A. Ross, S. Dass and A. K. Jain, "A Deformable Model for Fingerprint Matching", To appear in *Pattern Recognition*, 2004. 24. U.V. Chaudhari, J. Navratil, G.N. Ramaswamy, R.D. Zilca, "Future speaker recognition systems: Challenges and solutions" *Proceedings of AUTOID-2002*, Tarrytown, NY, March 2002.
9. A. K. Jain and S. Pankanti, "Biometrics Systems: Anatomy of Performance", *IEICE Transactions Fundamentals*, Vol. E84-D, No. 7, pp. 788-799, 2001.