Biometric Identification

When it comes to working biometric identification technologies, it's not only our fingerprints that do the talking. Now, our eyes, hands, signature, speech, and even facial temperature can ID us.

Questions related to the identity of individuals such as "Is this the person who he or she claims to be?," "Has this applicant been here before?," "Should this individual be given access to our system?" are asked millions of times every day by organizations in financial services, health care, e-commerce, telecommunication, and government. In fact, identity fraud in welfare disbursements, credit card transactions, cellular phone calls, and ATM withdrawals totals over $6 billion each year [5].

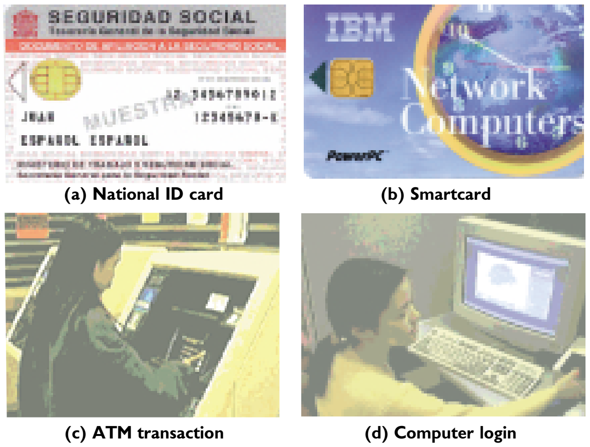
For this reason, more and more organizations are looking to automated identity authentication systems to improve customer satisfaction and operating efficiency as well as to save critical resources (see Figure 1). Furthermore, as people become more connected electronically, the ability to achieve a highly accurate automatic personal identification system is substantially more critical [5].

Personal identification is the process of associating a particular individual with an identity. Identification can be in the form of verification (also known as authentication), which entails authenticating a claimed identity ("Am I who I claim I am?"), or recognition (also known as identification), which entails determining the identity of a given person from a database of persons known to the system ("Who am I?"). Knowledge-based and token-based automatic personal identification approaches have been the two traditional techniques widely used [8]. Token-based approaches use something you have to make a personal identification, such as a passport, driver's license, ID card, credit card, or keys. Knowledge-based approaches use something you know to make a personal identification, such as a password or a personal identification number (PIN). Since these traditional approaches are not based on any inherent attributes of an individual to make a personal identification, they suffer from the

WALTER SIPSER

Anil Jain, Lin Hong, and Sharath Pankanti

Figure 1. Biometric applications.


(a) National ID card

(b) Smartcard

(c) ATM transaction

(d) Computer login

THE AUTHORS ARE GRATEFUL TO EYEDENTIFY CORP., IRISCAN INC., AND MIKOS LTD. FOR PROVIDING THE PICTURES OF RETINA, SMART-CARD, IRIS, AND THERMOGRAM, RESPECTIVELY

obvious disadvantages: tokens may be lost, stolen, forgotten, or misplaced, and a PIN may be forgotten by a valid user or guessed by an impostor. (Surprisingly, approximately 25% of the people appear to write their PIN on their ATM card, thus defeating the protection offered by PIN when ATM cards are stolen [5]!) Because knowledge-based and token-based approaches are unable to differentiate between an authorized person and an impostor who fraudulently acquires the token or knowledge of the authorized person [8], they are unsatisfactory means of achieving the security requirements of our electronically interconnected information society.

Biometric identification refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics (biometric identifiers) [5]. It associates/disassociates an individual with a previously determined identity/identities based on how one is or what one does. Because many physiological or behavioral characteristics are distinctive to each person, biometric identifiers are inherently more reliable and more capable than knowledge-based and token-based techniques in differentiating between an authorized person and a fraudulent impostor.

A biometric system is essentially a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user. Logically, a biometric system can be divided into the enrollment module and the identification module (see Figure 2). During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric sensor to acquire a digital representation of the characteristic. In order to facilitate matching and to reduce the storage requirements, the digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a "template." Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a magnetic card or smartcard issued to the individual.

During the recognition phase, the biometric reader captures the characteristic of the individual to be identified and converts it to a digital format, which is further processed by the feature extractor to produce the same representation as the template. The resulting representation is fed to the feature matcher that compares it against the template(s) to establish the identity of the individual.

An ideal biometric should be *universal*, where each person possesses the characteristic; *unique*, where no two persons should share the characteristic; *permanent*, where the characteristic should neither change nor be alterable; and *collectable*, where the characteristic is readily presentable to a sensor and is easily quantifiable.

In practice, however, a characteristic that satisfies all these requirements may not always be feasible for a useful biometric system. The designer of a practical biometric system must also consider a number of other issues, including:

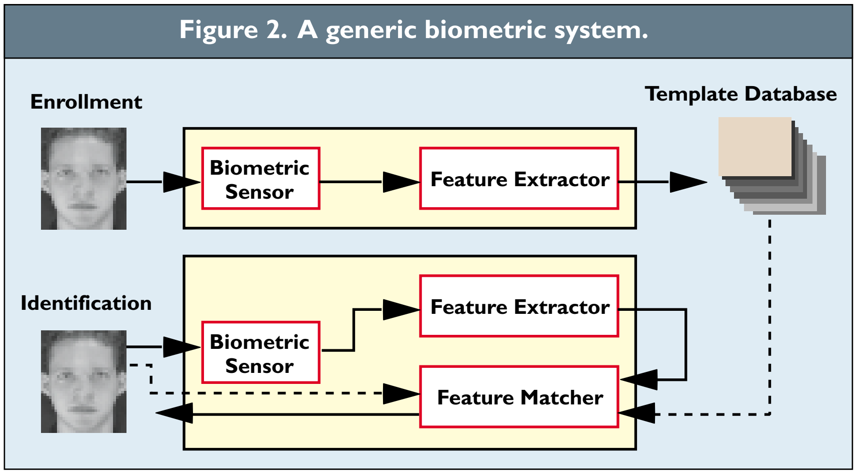
Table 1. Biometric applications

Forensic	Civilian	Commercial
Criminal investigation	National ID	ATM
Corpse identification	Driver's license	Credit card
Parenthood determination	Welfare disbursement	Cellular phone
	Border crossing	Access control

- *Performance*, that is, a system's accuracy, speed, robustness, as well as its resource requirements, and operational or environmental factors that affect its accuracy and speed;
- *Acceptability*, or the extent people are willing to accept for a particular biometric identifier in their daily lives;
- *Circumvention*, as in how easy it is to fool the system through fraudulent methods.

Depending on the application context, a biometric system may either operate in a verification (authentication) mode or in a recognition (identification) mode [5]. A verification system authenticates a person's identity by comparing the captured biometric characteristic with the person's own biometric template(s) prestored in the database. In this system, an individual who desires to be identified submits a claim to an identity usually via a magnetic-stripe card, login name, or smartcard, and the system either rejects or accepts the submitted claim of identity. In a recognition system, the system establishes a subject's identity (or fails to if the subject is not enrolled in the system database) by searching the entire template database for a match—-without the subject having to claim an identity.

Figure 2. A generic biometric system.



Measuring Performance

Evaluating the performance of a biometric identification system is a challenging research topic [12]. The overall performance of a biometric system is assessed in terms of its accuracy, speed, and storage. Several other factors, like cost and ease-of-use, also affect efficacy.

Biometric systems are not perfect, and will sometimes mistakenly accept an impostor as a valid individual (a false match) or conversely, reject a valid individual (a false nonmatch). The probability of committing these two types of errors are termed false nonmatch rate (FNR) and false match rate (FMR); the magnitudes of these errors depend upon how liberally or conservatively the biometric system operates. Figure 3 shows the trade-off between a system's FMR and FNR at different operating points; it's called the "Receiver Operating Characteristics (ROC)" and is a comprehensive measure of the system accuracy in a given test environment.

High-security access applications, where concern about break-in is great, operate at a small FMR. Forensic applications, where the desire to catch a criminal outweighs the inconvenience of examining a large number of falsely accused individuals, operate their matcher at a high FMR. Civilian applications attempt to operate their matchers at the operating points with both a low FNR and a low FMR. The error rate of the system at an operating point where FMR equals FNR is called the equal error rate (EER) which may often be used as a terse descriptor of system accuracy. Accuracy performance of a biometrics system is considered acceptable if the risks (benefits) associated with the errors in the decision-making at a given operating point on ROC for the given test environment are acceptable. Similarly, accuracy of a biometrics-based identification is unacceptable/poor if the risks (benefits) associated with errors related to any operating point on the ROC for a given test environment are unacceptable (insufficient).

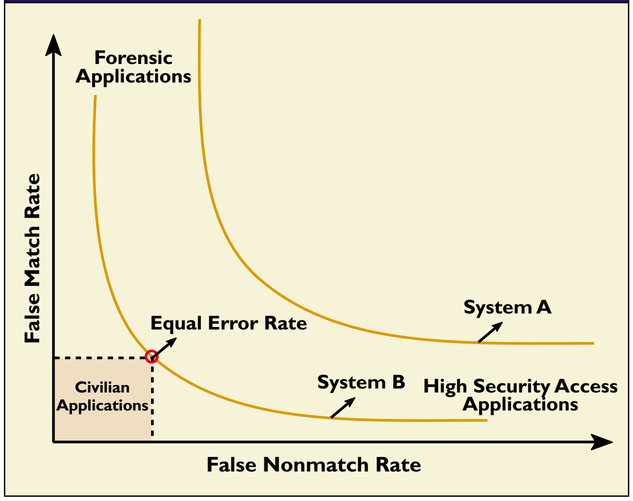
The size of a template, the number of templates stored per individual, and the availability of compression mechanisms determine the storage required per user. When template sizes are large and the templates are stored in a central database, network bandwidth may become a system bottleneck for identification. A typical smartcard may only hold a few kilobytes of information (for instance, 8K) and in systems using smartcards to distribute the template storage, template size becomes an important design issue.

The time required by a biometric system to make an identification decision is critical to many applications. For a typical access-control application, the system needs to make an authentication decision in real-time. In an ATM application, for instance, it is desirable to accomplish the authentication within about one second. For forensic applications, however, the time requirements may not be very stringent.

All other factors remaining identical, the widespread use of biometrics will be stimulated by its adoption in the consumer market. The single most important factor affecting this realization is the cost of the biometrics systems including the sensors and related infrastructure. Some sensors, such as microphones, are already very inexpensive, while others, such as CCD cameras, are now becoming standard peripherals in a personal computing environment. With the recent advances in solid-state technology, fingerprint sensors will become sufficiently inexpensive in the next few years. Storage requirements of the biometric templates and processing requirements for matching are among the two major considerations towards the infrastructure cost.

The human factors issue is also important to the

Figure 3. Receiver Operating Characteristics (ROC) of a system illustrates false nonmatch rate (FNR) and false match rate (FMR) of a matcher at all operating points. Each point on a ROC defines FNR and FMR for a given matcher, operating at a particular matching score threshold. A smaller FNR (that is, a more tolerant system) usually leads to a larger FMR while a smaller FMR (a less tolerant system) usually implies a larger FNR. Note that System A is consistently inferior to System B in accuracy performance.



success of a biometric-based identification. How easy and comfortable is it to acquire a given biometric? For example, biometric measurements that do not involve touching an individual, such as face, voice, or iris, may be perceived as more user-friendly. Additionally, biometric technologies requiring very little cooperation/participation from the users (such as face and thermograms) may be perceived as more convenient to users. A related issue is public acceptance. There may be a prevalent perception that biometrics are a threat to the privacy of an individual. In this regard, the public needs to learn that biometrics could be one of the most effective, and in the long run, more profitable means for protecting individual privacy. For instance, a biometrics-based patient information system can reliably ensure that medical records can only be accessed by medical personnel and the individual concerned. As in any industry, government regulations and directives may either provide a boost or lead to the demise of certain types of biometric technologies. Upcoming U.S. legislation such as the Health Information Portability Act (HIPA), may have a favorable impact on the biometrics industry. A good approach to piloting and gaining gradual acceptance of a biometrics solution could be to introduce it on a voluntary basis with either explicit or implicit incentives for opting biometrics-based solution.

Applications Flourish

Biometrics is a rapidly evolving technology that has been widely used in forensics, such as criminal identification and prison security. Biometric identification is also under serious consideration for adoption in a broad range of civilian applications. E-commerce and e-banking are two of the most important application areas due to the rapid progress in electronic transactions. These applications include electronic fund transfers, ATM security, check cashing, credit card security, smartcards security, and online transactions. There are currently several large biometric security projects in these areas under development, including credit card security (MasterCard) and smartcard security (IBM and American Express). A variety of biometric technologies are now competing to demonstrate their efficacy in these areas.

The market of physical access control is currently dominated by token-based technology. However, it is predicted that, with the progress in biometric technology, market share will increasingly shift to biometric techniques.

Information system and computer-network security, such as user authentication and access to databases via remote login is another potential application area. It is expected that more and more information systems and computer-networks will be secured with biometrics with the rapid expansion of Internet and intranet. With the introduction of biometrics, government benefits distribution programs such as welfare disbursements will experience substantial savings in deterring multiple claimants. In addition, customs and immigration initiatives such as INS Passenger Accelerated Service System (INSPASS), which permits faster processing of passengers at immigration checkpoints based on hand geometry, will greatly increase the operational efficiency. A biometric-based national identification system provides a unique ID to the citizens and integrates different government services. Biometrics-based voter registration prevents voter fraud; and biometrics-based driver registration enforces issuing only a single driver license to a person; and biometrics-based time/attendance monitoring systems prevent abuses of the current token-based manual systems.

Biometric Technologies

There are a multitude of biometric techniques either widely used or under investigation. These include,

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.