Q&A

D. HALLINAN/ALAMY; J. MONE/AP

M. LONGHURST/ALAMY; MEDICAL-ON-LINE/ALAMY

TECHNOLOGY

Biometric recognition

Anil K. Jain

Whether in passports, credit cards, laptops or mobile phones, automated methods of identifying people through their anatomical features or behavioural traits are an increasing feature of modern life.

Are biometric techniques the future of personal identification?

Yes, because unlike conventional recognition techniques such as passwords or ID cards, which are based on 'what you know' or 'what you have', biometric recognition is based on 'who you are': anatomical features such as face, fingerprint or iris, or behavioural traits such as signature or gait. This makes biometric technologies much more difficult to abuse than traditional methods of identification. Unlike passwords or ID cards, it is extremely difficult to guess, share, misplace, copy or forge biometric identifiers.

Why is the future arriving just now?

It's a combination of increased demand and increased supply. On the demand side, there are growing concerns about security threats and fraud. Governments want to keep track of who is entering and leaving their borders and receiving welfare payments; companies want to control who can enter their facilities, websites and proprietary databases. Crucially, public acceptance of the technology is also growing: citizens worried about identity theft are willing to use biometric systems for accessing laptops and mobile phones, and for making payments using credit cards at point-of-sale terminals. On the supply side, the explosion in the use of biometric techniques has been fuelled by the recent advent of compact and cheap sensors, and systems capable of fully automatic and 'real-time' identification (typically within a second).

How do these new technologies differ from familiar methods of biometric recognition such as fingerprinting?

Fingerprints have been used in forensics for about 100 years to identify repeat offenders and to establish the identity of a criminal from prints left at the scene of a crime. But in traditional fingerprint identification, a human expert is generally in the loop (so to speak), to make the final determination of identity from a candidate list generated by an automatic system. Other methods of identification used in forensics — analysis of DNA, hair and fibre samples, for example — are not fully automated either and take a long time (hours to days) to make the identification. That's OK for criminal investigations, but no good for many commercial applications.

How are fingerprinting technologies being updated?

The traditional method of capturing fingerprints, still practised by police and government agencies, is based on 'inked impression on paper', called rolled fingerprints. But electronic sensors based on optical, solid-state, thermal, ultrasound and multispectral technologies are now available. These sensors generate digital images from differences in the physical properties (such as reflectance and capacitance) of ridges and valleys as the finger surface touches a plate (Fig. 1, page 40). 'Touchless' variants record an image of the finger surface directly using one or more digital cameras. Many of these sensors are extremely compact and cheap, enabling them to be embedded in consumer electronic products such as mobile phones, personal digital assistants and laptops.

Iris recognition is a buzz phrase at the moment. What does this involve?

Iris recognition is based on the analysis of unique and stable texture patterns that are visible within the iris (the coloured portion) of the human eye. Video-camera technology is used to record an image of the eye, and the iris region is localized after digitally removing the pupil, eyelids and eyelashes. The phase information of the digitally filtered iris image (which represents the unique wavy pattern of each iris), is computed and stored as a string of bits. Recognition is performed by comparing two such bit sequences.

What are the elements of a biometric recognition system?

They all have four features in common (Box 1). First, there is the sensor, to capture or read the biometric trait — a fingerprint, iris, signature, voice trait or similar. Then there's the feature extractor, to extract some salient characteristics of the trait for recognition; the enrolment database, where the biometric features (also called templates) of all the enrolled users of the system are stored; and the matcher, which compares an input biometric sample with the templates in the database.

How is the identification performed?

We can distinguish between two cases: positive and negative recognition. Positive recognition is easy. Say you want to log in to your laptop with a built-in fingerprint reader. Instead of entering your password, you place your finger on the sensor. If the features extracted from your fingerprint match the fingerprint template associated with your ID in the laptop's enrolment database, access is granted.

And how does negative recognition work?

Negative recognition is more challenging. Suppose you want a new driver's licence. Typically, you have to produce one or more forms of paper identification such as a birth certificate or a passport. But these can be relatively easily forged. How does the licensing authority know that you do not already have a licence under a different name? A biometric database allows the licence issuer to find this out by matching a biometric trait (your face, for example) with that of all the individuals in the database who have already been issued with a licence. There are many such examples in which 'multiple enrolments' by the same person need to be detected — issuing passports and disbursing welfare payments, for example.

Have biometric systems been successfully deployed on a large scale?

Certainly. An example of a high-throughput positive-recognition system is the multispectral fingerprint sensor used by the Walt Disney World Resort in Orlando, Florida, to prevent ticket fraud. Every visitor to the resort must provide his or her index finger at the turnstile along with the ticket. That fingerprint gets linked to that particular ticket, so if you visit the resort again (either later the same day or on a different day if you have a multiple-entry ticket) you must present the same finger that was used to validate the ticket. The Disney system can handle a large number of visitors (around 100,000 every day) efficiently and — an important point, this — it works equally well in all weathers. Another example is the UK government's Iris Recognition Immigration System (IRIS), a positive-recognition system based on iris scanning, which allows enrolled travellers to bypass normal immigration channels at major airports.

Are there working negative-recognition systems?

The most high-profile example of a negative-recognition system is perhaps the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system used by the Department of Homeland Security. Every visitor to the United States must now provide fingerprint images of left and right index fingers and a facial image at their port of entry. The two fingerprints are matched against a watch-list of 2.5 million records in less than 10 seconds. More than 75 million visitors have been processed through this system since its inception in January 2004, and about 1,000 have been denied entry.

Where has biometric technology been tried and found wanting?

Surveillance at public places such as airports and busy streets is a perennial problem for biometric recognition. Although surveillance cameras can be used to detect suspicious behaviour or events, capturing facial images and thereby identifying known criminals and hooligans is more difficult. Face-matching algorithms generally use statistical techniques to analyse the distribution of pixel intensities in a face image and measure the relative positions of different features (eyes, nose and so on). But state-of-the-art face-recognition algorithms are not very accurate when the light is not good, when only a partial face image is available, or when a person's appearance has changed since the entry in the database, through, for example, ageing, a different expression or the addition of glasses or a beard.

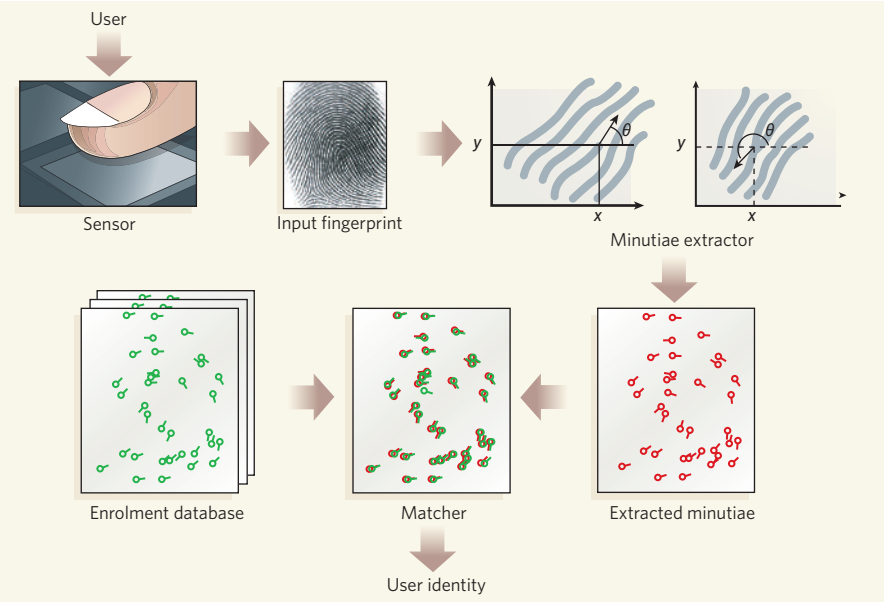
How is the accuracy of a biometric recognition system measured?

Through two figures: the false reject rate (FRR), the frequency with which a genuine user is not correctly recognized and hence denied access; and the false accept rate (FAR), the frequency with which an impostor is accepted as a genuine user. Of course, these two metrics are not independent for a given system. A system that accepts all the right people, and so has a desirably low FRR, might not reject all the wrong people, and so could have a higher FAR.

How accurate are current systems?

Current fingerprint-recognition systems can provide an FRR of up to 0.01% (1 in 10,000) at an FAR of 0.1% (1 in 1,000). Of course, the actual performance of a biometric system depends on several factors, including the specific biometric trait, characteristics of the sensor used to capture it, the number and characteristics of the people enrolled in the database, as well as various environmental factors (indoors or outdoors, temperature, humidity, and so on). And where the emphasis on accuracy lies depends on the specific application: Disney World, for example, will want as low an FRR as possible, so as not to upset customers unnecessarily, at the expense of a higher FAR. For the US-VISIT system, the opposite is true: a low FAR is needed (to keep potential

Box 1 | Automated biometric identification



A typical biometric recognition system, here an automated fingerprint identification system, has two stages of operation: the enrolment stage and the identification stage. In the enrolment stage, a sensor captures a digital image of a legitimate user's fingerprint. Its salient features, or minutiae, are extracted and stored as a template in an enrolment database.

These minutiae take the form of locations (x and y coordinates) and orientations (θ) of abrupt ends and junctions of fingerprint ridges. In a high-quality image, there are typically 20–70 such minutiae, depending on the size of the sensor surface and how users place their finger on the sensor.

During identification, fingerprint minutiae are extracted from a query print in the same way and compared with the minutiae of the templates stored in the enrolment database. Variations in placement and pressure mean that template and query fingerprints must be aligned before matching. The number of minutiae that have similar x, y and θ coordinates forms a basis for determining the identity of the user.

In iris recognition, phase information from the pattern of the iris takes the place of minutiae and is stored in a database in the form of a barcode. For face recognition, the distribution of pixel intensities and positions of features in a facial image are extracted for comparison with stored templates. **A.K.J.**

criminals and terrorists out) at the expense of a higher FRR.

What can be done to decrease errors?

Efforts are afoot to design better biometric sensors/readers, to improve algorithms to extract features from raw biometric data and to match two biometric samples quickly and accurately. Another research track being pursued specifically to decrease recognition error is to fuse information from several independent biometric sources. The US-VISIT scheme, with its two-fingerprint strategy, is an operational example of such a 'multibiometric' system. In the future, the fingerprint images could be supplemented with data from face-recognition software. Several different types of multibiometric systems can be envisaged (Fig. 2).

Are some biometric traits better than others?

Yes. Fingerprint and iris have the smallest error rates. But error rate is only one consideration. Other factors include system cost, size of the scanner, integration into existing security infrastructure, and user comfort and perception. So there's no perfect biometric trait.

Are people's fears about biometric technology justified?

Concerns can be classified into three broad categories. First, there is security: that a biometric system can itself be attacked or compromised (for example, by providing a fake input fingerprint). Second, there is the issue of privacy: that governments and states might use the technologies to track and snoop on people, or that a person's biometric template might be stolen and abused. Third, there are cultural and religious objections. Concerns relating to security and privacy issues are justified, and are the subject of research. As far as privacy and cultural objections are concerned, government regulation and public education will be required if full acceptance is to be achieved.

Can biometric security realistically be breached?

One way to attack a biometric system particularly beloved of film-makers and authors is to employ a spoof biometric trait (an artificial or dead finger, or a face mask, for example). This is a serious concern, but new fingerprint sensors can detect whether the finger placed at the sensor is living or not by using, for example, a multispectral imaging technique to measure how much light the finger absorbs, or by measuring the finger's electrical conduction properties using electric-field sensors.

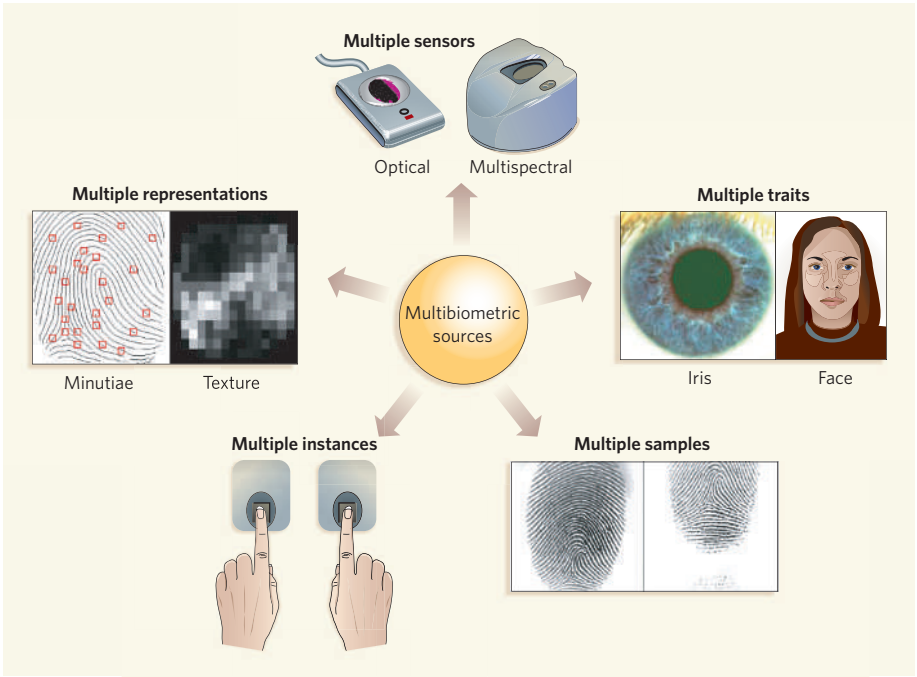


Figure 2 | Multibiometric identification. Sources of information in a multibiometric system include (clockwise from the top) using different sensors to capture the same biometric trait; using more than one independent trait; taking more than one sample of the same trait (for example, the same fingerprint or iris scan); taking multiple instances of a trait (prints of both the left and right index finger, or the irises of right and left eyes); and more than one type of representation of the same trait. The US-VISIT immigration scheme is a multibiometric system based on multiple instances (two fingerprints) with the future potential also to take a multiple-trait approach, fusing fingerprint data with face-recognition technology.

What about hacking into the underlying computer systems?

The most sensitive parts of a biometric system are the enrolment database, an attack on which constitutes both a security and a privacy threat, and the channels used to transmit information between the different elements of the system. Both can be protected through clever combinations of biometrics with cryptographic techniques to prevent hackers intercepting, relaying or modifying information. Alternatively, to eliminate the danger of interception in transmission, the entire biometric system (sensor, feature extractor, database and matcher) can be built on a single chip or a 'smart card', so that no biometric data ever leave the card or the chip.

Will concerns about its security stop the onward march of biometric recognition?

No, because whatever its problems, biometric recognition offers greater security and convenience than traditional methods of person recognition based on official documents, PINs and passwords. In some applications, such as access to computer systems, biometrics can replace or supplement existing methods to improve recognition accuracy. In others, such as issuing passports and driving licences, biometrics is the only viable approach for determining whether an individual has already been issued these documents under a different name. Like it or loathe it, the technology is here to stay. ■

Anil K. Jain is in the Department of Computer Science and Engineering, Michigan State University, East Lansing, Michigan 48824-1226, USA.
e-mail: jain@cse.msu.edu

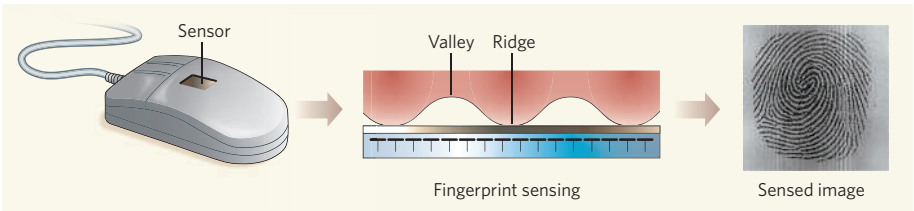


Figure 1 | A capacitive fingerprint sensor. When a user places a finger against a silicon chip containing an array of microcapacitor plates, a small electric charge arises in the insulating air gap, the magnitude of which depends on the distance between the finger and the plates. The capacitance values of different plates, converted into pixel intensities, form a digital image of the ridges and valleys of the fingerprint. Such fingerprint-sensing chips cost only about US$5, and are compact enough to be embedded in mobile phones, key fobs and hand-held computers.

FURTHER READING
Jain, A. K., Bolle, R. & Pankanti, S. (eds) *Biometrics: Personal Identification in Networked Society* (Springer, Heidelberg, 2006).
Maltoni, D. *et al. Handbook of Fingerprint Recognition* (Springer, Heidelberg, 2003).
Daugman, J. *IEEE Trans. Pattern Anal. Mach. Intell.* **15,** 1148–1161 (1993).
Ross, A., Nandakumar, K. & Jain, A. K. *Handbook of Multibiometrics* (Springer, Heidelberg, 2006).
Rowe, R. K. *et al. Proc. SPIE* **5694,** 90–99 (2005).