An introduction to biometrics

A concise overview of the most important biometric technologies

by Ravi Das

In many ways, biometrics has all the hallmarks of a double-edged sword. At one end of the spectrum, it is viewed with wonder and intrigue, while at the other it is considered invasive, conjuring up images of Big Brother. In the final analysis, there is really nothing special about biometric technology. Instead, it is a security solution like any other. This article describes the essence of biometrics and provides an overview of existing technologies.

The article is divided into the following sections:

1. A definition of biometrics;
2. A brief review of the major biometric technologies;
3. The differences between behavioural and physical biometrics;
4. A review of the major biometric concepts;
5. A last thought.

1. A definition of biometrics

We all have unique physiological and behavioural characteristics that distinguish us from other people. Biometrics uses these unique characteristics (or identifiers) to ascertain and verify people's identity. Unique identifiers include distinct features such as fingerprints, various iris patterns, blood vessel patterns in the retina, voice inflections in speech, and hand shape/geometry. It also includes the way we sign our name or use a computer keyboard.

2. A brief review of the major biometric technologies

There are a total of seven major biometric technologies available today. They are:

- Fingerprint recognition;
- Hand geometry recognition;
- Facial recognition;
- Iris and retina recognition;
- Voice recognition;
- Keystroke recognition;
- Signature recognition.

Of these technologies, fingerprint recognition, hand geometry recognition and iris recognition are most prevalent. Having said that, considerable time and effort is being invested in biometric technologies of the future, which include gait recognition (the way and manner in which somebody walks), earlobe recognition (examining the geometry of the earlobe) and DNA recognition (examining the unique strands found in DNA samples). A brief description of each biometric technology is provided below.

Fingerprint recognition

Fingerprint recognition involves the location and determination of the unique characteristics of the fingerprint. The fingerprint is composed of various 'ridges' and 'valleys', which form the basis for the loops, arches and swirls on your fingertip. The ridges and valleys contain different kinds of breaks and discontinuities. These are known as 'minutiae'. It is from these minutiae that the unique features are located and determined. There are two types of minutiae: ridge endings (the location where the ridge actually ends) and bifurcations (the location where a single ridge splits into two ridges).

Hand geometry recognition

Hand geometry recognition involves looking for unique features in the structure of the hand. These features include the thickness, length and width of the finger, the distances between finger joints, and the hand's overall bone structure. A 3-dimensional image is taken of these unique characteristics. It should be noted that the hand does not contain as many unique characteristics as other identifiers.

Facial recognition

Facial recognition involves taking many images (or pictures) of the face, and extracting the unique facial features and distances from - or between - the ears, nose, eyes, mouth and cheeks.

Iris and retinal recognition

Iris recognition entails examining the unique features of the iris. The iris is the coloured section between the pupil and the white region of the eye (also known as the sclera). Its primary purpose is to control the size of the pupil (the part of the eye that allows light to pass through). The unique features of the iris include the trabecular meshwork (the tissue that gives the iris its 'radial' impression) as well as other physiological properties such as freckles, furrows, rings, and the corona.

***Ravi Das** is a Consultant for HTG Solutions. He has been involved in the IT industry for 10 years and launched HTG's security solutions division in January 2003. This division offers a complete security solutions package and uses biometric technology as its main product offering. Ravi holds a Master of Science Degree in Agribusiness Economics from Southern Illinois University and a Master of Business Administration (specialising in Management Information Systems) from Bowling Green State University.*

Retinal recognition involves examining the pattern of blood vessels in the retina, which is located at the back of the eye. The examination focuses on the juncture of the optic nerve (the area where the nerve leaves the brain and enters the eye).

Voice recognition

With voice recognition, it is the unique patterns of an individual's voice - as produced by the vocal tract - which is examined. In order to capture the voice inflections, a text phrase is usually recited. The vocal tract consists of the laryngeal pharynx, oral pharynx, oral cavity, nasal pharynx and the nasal cavity.

Keystroke recognition

Keystroke recognition works by examining the unique way in which an individual types on a computer keyboard. Variables include typing speed, the length of time that keys are held down, and the time taken between consecutive keystrokes.

Signature recognition

Signature recognition examines the way and manner in which we sign our name. Unique characteristics include changes in timing, pressure and speed during the signing process. It is important to note that it is not the signature itself that is examined.

3. The differences between behavioural and physical biometrics

The above biometric technologies fall in two categories: behavioural biometrics and physical biometrics. In general, behavioural biometrics can be defined as the non-biological or non- physiological features (or unique identifiers) as captured by a biometric system. As behavioural biometrics also covers any mannerisms or behaviour displayed by an individual, this category includes signature as well as keystroke recognition.

Physical biometrics may be defined as the biological and physiological features (or unique identifiers) as captured by a biometric system. This category includes fingerprint recognition, hand geometry recognition, facial recognition, iris and retinal recognition, and voice recognition.

4. A review of the major biometric concepts

When examining the various biometric technologies and systems, it is important that one has a basic understanding of the key concepts that are associated with biometrics. Each of these concepts is explained below:

- Verification and identification
- Biometric templates
- The processes of enrolment, verification and authorisation;
- Biometric performance standards.

Verification and identification

The verification process aims to establish someone's claimed identity. When you first enrol into a biometric system, it assigns you a number, which is linked to your biometric template. The database containing your template is searched on the basis of this number. If a positive match is established, you will be extended a given service or privilege. As the number is linked to the template, a one-to-one (or 1:1) relationship is said to exist.

As its name suggests, the identification process looks to establish someone's identity. In the absence of a unique number, the entire database needs to be searched in order for the system to 'recognise' you. As the template can belong to anyone in the database, a one-to-many (1:n) relationship is said to exist. A good example of a 1:n database is AFIS (Automated Fingerprint Identification Services), which is used by many law enforcement agencies to identify and track known criminals.

Biometric templates

When you first enrol in a biometric system, it takes numerous images/recordings of your biological and non-biological data (including, for example, a voice recording or keystroke pattern). These raw images and recordings are subsequently consolidated into one main image, known as the 'biometric sample'. It is from this sample that the unique features (discussed above) are captured and extracted. Next, they are converted to a 'biometric template', which, in turn, is used for the purposes of verification and identification. It should be noted that the biometric system does not contain actual images of the biological or non-biological data - it only stores the mathematical files. The type of mathematical file that is created depends on the biometric system in use. Whereas fingerprint recognition and hand geometry recognition systems create binary mathematical files, iris recognition systems generate hexadecimal files. In other words, the image of your fingerprint or hand becomes a series of 0s and 1s (0001010100001111111, for example).

The processes of enrolment, verification and authorisation

Imagine trying to enter a high-security area. To do so, your template must be included in a database, alongside those of other authorised individuals. In turn, this requires you to register your fingerprint. This process is known as enrolment. Several fingerprint images are taken, which are combined in a single biometric sample. Next, a mathematical formula or extraction algorithm is used to extracts the unique features from the biometric sample. These features are subsequently stored in a mathematical file known as an enrolment template, which is used for the purposes of verification.

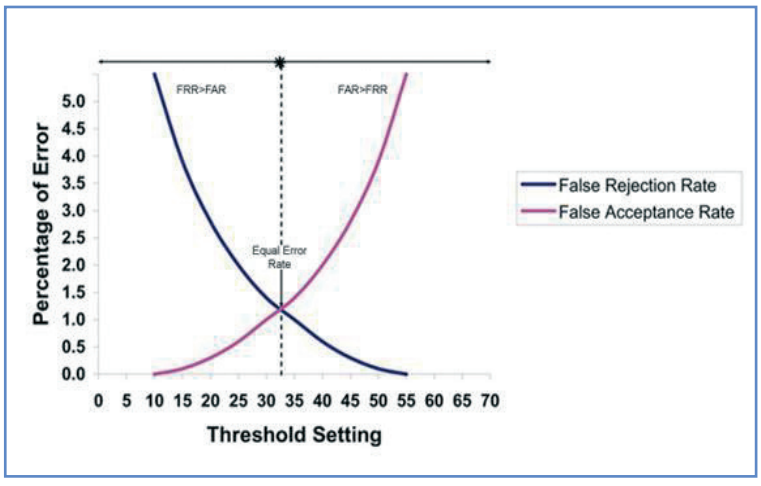

Figure 1
Biometric systems are rated on the basis of several performance standards. The most important are the False Rejection Rate (FRR), the False Acceptance Rate (FAR) and the Equal Error Rate (EER)

The next step involves verification. In order to enter a high-security area, you are required to identify yourself by placing your finger on a fingerprint scanner. The scanner's sensor will capture 'an image' of your print. The extraction algorithm subsequently extracts the unique features from the image, and stores these in a file known as the verification template.

The next stage involves comparing the verification template to the enrolment template in order to determine the extent to which they match. This is achieved with the assistance of a matching algorithm. The latter assigns a score, based on the amount of overlap between both templates. If this score is higher than an agreed value (or threshold) you are authorised to enter the area. If the score is lower than the threshold value, you are denied access (and the verification process may be repeated).

Although much happens during the enrolment, verification and authorisation processes, they only take a few seconds to complete. At this point, it is important to remember that an enrolment template is never completely (100%) the same as a verification template.

Biometric performance standards

Biometric systems are rated on the basis of several performance standards. The most important are the False Rejection Rate (FRR), the False Acceptance Rate (FAR) and the Equal Error Rate (EER) (figure 1).

The FRR (also known as type 1 errors) can be defined as the probability of a registered user being wrongly rejected by the biometric system. (In case of the above example: what is the likelihood of a legitimate, registered user being denied access to the high-security area on the basis of a fingerprint scan?)
The FAR (also known as type 2 errors) can be defined as the probability of an impostor being wrongly authorised by the biometric system. (In case of the above example: what is the likelihood of a legitimate, registered user being wrongly authorised to access to the high-security area on the basis of a fingerprint scan?)

The EER (or crossover rate) reflects the probability of the FAR and the FRR being (nearly) the same.

There are also other biometric standards. For example, the Failure To Enrol rate (FTE), which defines the statistical probability that a person is simply unable to enrol in a biometric system. This may be attributable to the fact that the person in question does not have enough unique features for the system to capture.

The Ability To Verify rate (ATV) indicates the overall percentage of users that can be verified by a biometric system. The ATV can also be thought of as the combination of the FTE and the FRR. Mathematically, this relationship can be represented as follows:

ATV = [(1-FTE) * (1-FRR)]

5. A last thought

When evaluating a biometric system, it is important to review its actual performance based on the standards described above. Of these, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are most important.