

Biometric technologies of the future

Lots of potential, but - as yet - little practical use

by Ravi Das

While many different biometric technologies have been developed over the past decades, not all are by definition practical. This article covers three biometric technologies that offer considerable potential but are either considered too invasive or inappropriate for large scale deployment. Nothing that time cannot change.

Broadly speaking, there two types of biometrics: physical biometrics and behavioural biometrics. Physical biometrics comprise unique biological and physiological characteristics, including the voice, face, fingerprint, iris and retina. In contrast, behavioural biometrics focus on unique behavioural and psychological characteristics, including the way we use a keyboard or record our signature.

On the whole, systems that recognise the voice, face, iris, retina or fingerprint are well known and widely used. This is not necessarily the case for the three biometric technologies discussed in the article, even though they claim a growing share of the limelight. While recognition systems based on the human gait, earlobe or DNA have been researched, their broad-based application is still a long way off. Here's why.

Gait recognition

Gait recognition techniques look to identify someone by his gait (or the way that he or she walks). Unlike other biometric technologies, gate recognition is based on dynamic movement. In other words, the subject is - and needs to be - in motion. Several variables affect gait recognition technologies, including:

- the subject's clothing;
- the surface on which the subject walks;
- fatigue or injury, causing the subject to walk different;
- the type of shoes the subject is wearing;
- the presence of items such as handbags, briefcases, umbrellas and the like;
- background or extraneous noise, including lighting and changes in the external environment.

Numerous methods have been created to capture the human body in motion, including stick figure models,

volumetric models and so-called 'blob' models. Modern gait recognition technology is based on a model of a moving person, which is used to obtain a series of mathematical vectors. So-called eigenvalues have also been used (these are applied to facial recognition, in much the same way). In addition to motion-based developments, primitive templates have been created by capturing and tracking the orientation of the thigh or other physical features.

In 2002, the Defence Advanced Research Projects Agency (DARPA) funded two major gait recognition projects at the Georgia Institute of Technology (under its Human ID at a Distance Program). One project examined gait on the basis of machine vision techniques, while the other relied on radar.

The machine vision project involved an examination of static body parts and stride variables, as well as the collection of distance-related data (between the feet and the pelvis, between the left and the right foot, and between the feet and the head). This type of recognition, which is based on an 'activity-specific state biometric', allows a subject's stride or leg dimensions to be determined on the basis of a single image. To obtain this data, there is no need for the subject to be in motion.

The second project involved a radar device, which was used to generate a computerised image of the subject. Radar offers several advantages over computer vision, in that it can be used under different external conditions (think of fog or poor lighting, for example). There are several areas where gait recognition enjoys advantages over more common physical and behavioural biometrics:

- There is no physical contact with the subject.
- Partly as a result of point 1, gait recognition is not particularly invasive. It may, therefore, be less affected by privacy-related issues (this is not the case for biometric technologies such as facial or iris/retina recognition).
- Because gate recognition is not evasive, it is not particularly overt either (subjects can be verified without their knowledge);
- Biometric data can be acquired at a much greater distance compared to other biometric technologies. Many popular biometric solutions require contact with the subject during enrolment and, depending on the technology, verification.



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.

Earlobe recognition

Earlobe recognition involves examining the unique geometry of the earlobe using techniques that are similar to those used for hand geometry recognition. The ability to examine the ear in its entirety is also being studied. While numerous studies have underpinned the uniqueness of the human earlobe, even amongst groups of people, earlobe recognition is still in its infancy. The scientific studies conducted to date have culminated in preliminary results only. Numerous projects have nevertheless been initiated to examine the potential and feasibility of earlobe recognition. By the Forensic Ear Identification Research Group (FEARID) for example. At this stage, it is widely felt that earlobe recognition could prove as effective as facial recognition. To become an established technology, earlobe recognition will have to leverage its strengths, however. These are as follows:

- The shape of the ear remains fairly constant; its structure does not change, either with time or with facial expression. The position of the earlobe also remains fixed.
- Unlike, for example, gait recognition, the external environment does not significantly affect the quality of the earlobe data acquired.
- Compared to other physiological biometrics, the outer ear is not greatly affected by ageing (unlike the face).

DNA recognition

The use of DNA as a means of verification is attracting growing attention. DNA - or deoxyribonucleic acid - is the unique double helix structure found in all living cells. To date, DNA has primarily been used in forensics (the identification and/or exclusion of people suspected of crimes). Even though DNA is - in the truest sense of the word - a biometric, its commercial application is still a long way off. Unlike other physiological and behavioural biometrics, DNA cannot be used for fast, automated verification and identification - it can take up to two weeks for the results of a DNA analysis to become available. DNA recognition differs from other biometric technologies in three key areas:

- As actual DNA samples are used, no biometric templates are created.
- Whereas biometric templates can be analysed and compared in real time, DNA samples cannot.
- No DNA images are taken (instead, actual biological samples are used).

As a biometrics technology, DNA enjoys several advantages over physiological and behavioural biometrics. First, DNA contains a wealth of unique information, possible exceeding the uniqueness of the retina by quite a margin (the retina is currently considered the most unique and stable biometric). Second, a person's DNA structure is not affected by time. Assuming use is made of all four nucleotides

(structural DNA units) as well as longer DNA chains, the likelihood of duplication is extremely remote. Unfortunately DNA verification also has several disadvantages:

- Current technologies focus on biometrics that cannot be separated from the carrier. However, DNA can be separated (think of nails, hair, skin, etc.).
- DNA samples are prone to degradation and contaminants.
- From a privacy perspective, the use of DNA is highly controversial (think of the handling and storage of DNA data, for example).
- There is widespread fear that the sensitive data contained in DNA could be misused (think of hereditary conditions, medical details, etc.).
- Implementing security protocols for a DNA-based biometric system could prove exceptionally complex. This applies to database protection and overall system confidentiality in equal measure.

Conclusions

Of the three biometric technologies covered in this article, gait recognition appears to offer most potential in terms of practical deployment. While a decent amount of research and development has been conducted into gait recognition, it comes nowhere near fingerprint recognition or hand geometry in terms of user acceptance. Considering that very little interaction is required between the user and the gait recognition system, some even consider it invasive. In potential, it is nevertheless a highly effective tool for multi-modal security applications. Think, for example, of a dual-level verification system whereby a subject's identity is initially established on the basis of, for example, a fingerprint before being verified using gait recognition. It is also useful for one-to-many verification requirements at, for example, airports. Under these conditions, gait recognition can offer significant time savings by allowing large groups of people to be identified in a single environment.

Compared to gait recognition, earlobe recognition has much further to go, also in terms of research and development. This also applies to DNA recognition, even though it has the potential to be the best biometric of all (on account of its uniqueness). Unfortunately a DNA system would be desperate slow and completely unsuitable to the practical applications discussed here.

Last but not least, there are several other biometric technologies that are also being explored, including brain mapping, odour recognition, and vein pattern recognition. These will be discussed at a future stage.