

Dr Ted Dunstone



Emerging Biometric Techniques

What do you get when you cross biology statistical analysis, computer science and engineering? You get biometrics, the use of a distinctive and relatively stable physical or behavioural characteristic of a person for purpose of recognition.

In the last few years, biometrics has become the new growth market in security. However, most of the biometric security systems available today focus only on a limited range of what are considered to be "mainstream" biometrics, such as fingerprint, iris, face, hand, voice and signature recognition systems. In fact, such mainstream systems represent only the tip of the iceberg with regards to possible biometric identification techniques.

There is a plethora of alternative biometrics technologies currently being developed, some of which are complementary (assisting an existing biometric system, such as skin type recognition for facial recognition), while others are essentially orthogonal - providing additional biometric checks leading to improved resistance to attack (such as pulse recognition). There are even a few that propose using exotic new sensor types for recognition such as brain wave detection.

The esoteric biometric system referred to in this article is related to the biometric type, although not by means of capture. Fingerprint capture can, for instance, be achieved in several different ways, many of them quite niche, including ultrasonic

reading and special light emitting polymers. These capture systems, however, still use the same or similar fingerprint information as the more common optical or capacitance readers and as such are not 'esoteric'.

True esoteric biometrics provides several useful benefits when combined with the mainstream biometric identification techniques. The additional information gathered by the newer esoteric biometrics can help ensure inclusiveness for those people who are unable, or find it difficult, to use one or more of the traditional biometric identifiers. These newer esoteric systems also improve the security and accuracy of the traditional identifiers.

As biometric systems become more prevalent in the protection of critical infrastructure, or are used in more places (such as in passports), bio-hackers will continue to evolve new ways to break a biometric system. The use of esoteric biometrics techniques will help keep ahead of these hackers. It is likely that in the future, these types of multi-sensory systems will become the norm, where a variety of sensors, some similar to those used now and some that are similar to those discussed in this article, will be used to come to a decision on identity.

Assessing the security provided by the well known biometric is often controversial, even though the testing samples may number many thousand and the system has been in use for many years. Given this fact, one of the biggest

problems with implementing the more esoteric biometrics is the lack of data both for development and testing. In many cases these biometrics may only have been examined on a small sample of people (sometimes even just the people from the lab) and this is seldom indicative of real world performance. Neither stability nor uniqueness of a biometric can be established until a properly controlled (and ideally independent) trial has taken place under real world conditions. Many other issues including susceptibility to environmental effects and the durability of sensor also need to be considered. The low cost and improving performance of traditional biometric systems creates an increasingly high barrier for the entry of new techniques; however there is always an opportunity for a new technology where significantly enhanced levels of performance are achieved.

Esoteric biometric systems are a diverse collection of techniques. The following brief descriptions, in no particular order, provide a selection of some of the more obscure techniques.

- **Skin pore recognition.** Even the smoothest skin is covered with minute pores. The pattern produced by these pores is distinctive for every patch of skin, leading to a technique called pore recognition. This technique has been used with some success for improving fingerprint recognition. However, reading one's pores consistently requires much higher resolution

than is common to existing scanners.

- **Ear recognition.** Used primarily to recognise people from the side, ear recognition enables identification of an individual in cases where his/her face may be obscured. This technology would ideally be used as an adjunct to face recognition. However, the reliability of such a system remains to be seen, as the ear is not always visible depending upon people's hairstyle or earrings.
- **Infrared detection and recognition.** This technology depends upon the body heat emitted, generally from the face. The heat signature of an individual can vary significantly depending on what they are wearing or doing. However, the structure of the branching of blood vessels in the face supplies a unique pattern of heat flow to the face that will remain consistent irrespective of make-up or minor cosmetic surgery. The recent SARS epidemic has prompted the use of infrared cameras in airport environments to catch infected travellers, which may prompt a renewed interest in this technology.
- **Skin pattern identification.** Visionics, specialists in facial recognition systems, have recently bought a company that developed technology for analysing the skin patterns of individuals. The algorithm uses the skin regions around the cheeks and exploits the high frequency information found there to enable recognition. Previously, this information was considered as little more than noise and discarded. However, the claimed performance of this newly developed system is impressive (even distinguishing between identical twins) and on a small demo observed in Dublin recently, appears to work well. Its strength also lies in the fact that it can be easily combined with existing face recognition systems.
- **Skin composition.** Another new system under development by Johnson and Johnson explores the optical properties of skin. Using spectroscopic techniques, the structure and composition of the skin can be determined from its optical pattern. This has been used to enhance fingerprint recognition systems by providing additional recognition information.
- **DNA matching.** In its current wide spread use for forensics, where the sample can be examined in a lab over a number of hours, there is nothing particularly esoteric about DNA matching. What is new is the capability to analyse the DNA in real-time on the surface of a chip. The technology for undertaking this has yet to be perfected for recognition purposes. However, applications

for this technology, such as the rapid screening of genetic illnesses or biological pathogens, mean that continued development will see this technology become practical in the near future. DNA has the draw back that identical twins share exactly the same information, although this could be compensated for by also using another biometric technique. Another potential problem with this technology centres around the fact that we leave samples of our DNA everywhere, so again, this technology would most likely have to be used in conjunction with another identifier.

- **Gait recognition.** The way we move (our gait) is also relatively unique as it depends upon the length of our limbs and the conditioning of our muscles. At one time or another we have all identified someone when their back is turned, mainly by the way they are walking. This technology has been developed primarily for military surveillance purposes as it can be used from a long distance away when other visible cues are masked.
- **Heart beat recognition.** Despite our pulse varying in speed, there are a number of features that make heart beats distinct. These features can be used to validate an identity and are particularly useful for fingerprint systems where it is possible to both read the fingerprint and take the pulse simultaneously. One possible drawback of this type of system is that the finger needs to be pressed onto the sensor for some duration for sensor to obtain an accurate identity reading.
- **Grip recognition.** The protection of firearms using biometrics has, as a concept, been around for many years. This task is challenging for a number of reasons. First of all, a situation where the user wishes to fire the gun but cannot due to a false rejection by the identification system is unacceptable. Secondly, any identification system used to control the weapon must be robust. The weapon must still be usable in extremes of temperature and should not fail if it gets wet, dirty or dusty. The operator may also be wearing gloves or dark glasses making the recognition task more difficult. Under stressful situations, even the use of the voice to activate the firearm will be unreliable. A proposed solution uses the way a user grips the firearm handle as a biometric. Grip recognition could potentially work though gloves and could be relatively predictable under stressful situations. However, the alleged 'uniqueness' of grip as a biometric technique would need to be stringently tested

as it seems reasonable to assume that many people have similar grips.

- **Brain imaging.** Advances in scanning technology will eventually improve to the point where brain imaging is possible without the use of cumbersome and expensive NMI equipment (although it will still probably require the user to wear some kind of head set). As a biometric, the system would examine and record the way the brain responds to set stimulus, which will be highly specific to a particular individual. The resulting data could then be used for recognition and identification purposes.
- **Vein recognition** is being examined for deployment in Korea for use in border control. This technology uses the vein pattern on the back of the hand to undertake recognition. Considered to be less intrusive than some other existing biometric technologies, a number of companies are currently offering working models of this type of system. Of those techniques proposed above that have made it off the drawing board, most have suffered significant commercialisation problems – often due to accuracy or user inconvenience factors. Some, however, will become more relevant in the future as the technology improves and as the importance of multi-sensory systems become better understood. There are also a number of other technologies now making in-roads into enhancing more mainstream recognition technology. Over the next ten years, get ready for many surprises in the kinds of biometric technologies that will appear. At the extreme end of esoteric biometric systems, a recent example was raised about the use of lip recognition for forensics applications. So perhaps some time in the future we will need to pucker-up and kiss our computers in order to login. That will certainly be an advance in the human machine interface. ■

For more information on biometric systems please email ted@biometrics.com or call 02 9209 4599.

Dr. Ted Dunstone is the CEO of Biometix (www.biometix.com), a company specialising in security and biometric consulting and services. He has been involved with biometrics and authentication for over ten years and has particular specialty in use the use of biometrics for large-scale systems. He is currently also the chair of the technical panel of the Biometrics Institute.

Dr. Dunstone has a computer engineering degree from the University of South Australia and doctorate in machine learning and biometric identification from University of Wollongong. His PhD was completed in 1995 under a scholarship to investigate the detection of terrorists in airports. In 2003 he was the recipient of the state NSW Percy Award, which is given for innovative and pioneering achievement and contribution to research and development within the IT&T industry.