

BIOMETRICS: A SELF-SERVICE VIEWPOINT

Introduction

Biometrics can be defined as the use of physiological or behavioural characteristics to recognise or verify the claimed identity of an individual. Biometric techniques are of interest in areas where it is an advantage to positively associate a presented identifier or token with a specific individual rather than just identify the token itself and assume the association. Not surprisingly, biometrics developed in high security application areas, particularly military and other government applications, but had its (non-automated) roots in trading and later in criminology where, for fingerprint, it is most renowned. Paradoxically, on-line trading is one of the latest application areas to employ biometrics. Other growth application areas are immigration control, workstation/network access, and physical access security.

Biometrics and the ATM

As cards and PINs (Personal Identification Numbers) were one of the first automated identity tokens (card) and identifiers (PIN), it is easy to see why the biometrics system vendors have suggested ATMs (Automated Teller Machines) as a potential application area for their products and, conversely, why ATM vendors and their customers saw biometrics as a possible replacement for PIN. Indeed, many ATM customers use biometrics as an alternative to card/PIN for internal physical access security. On the surface there are valid reasons to replace PIN at the ATM:

- PIN does not prove the identity of the card holder – just that the user knows the PIN
- PINs can be forgotten leading to user frustration and cost of card/PIN replacement.
- PINs can be mistakenly used with incorrect cards due to proliferation of cards/PINs.
- 4 digit PINs only provide a variability of 1 in 10000.
- People write down PINs as memory aid but risk fraud
- PINs are easily transferred or distributed
- PINs can be “stolen” by observation or fraud measure.

Biometrics could provide a more secure, easier to use alternative. *Ideally* biometrics:

- Proves the claimed identity of the card holder
- Cannot be forgotten
- Has very high variability
- Cannot be transferred or stolen (surgery, 2D and 3D copies and severed body parts should not work *ideally*)

With the correct choice and application of a biometrics system, all of this can be valid. As mentioned, biometrics systems have replaced card/PIN in many physical access security systems, but do not have widespread use in self-service terminals, particularly ATMs. Much has to do with the environment in which a biometrics system would have to work, the biometrics systems available, the biometrics industry, and customer requirements. These issues will be covered later in this paper.

BIOMETRIC TECHNIQUES

What are the available biometric techniques? How do they work? How do you use them? Are they effective? Biometric techniques are split into the popular biometrics, which are detailed below and address the above questions, and some potentially interesting but unproven or impractical systems which are listed but cannot be described in detail at present.

The popular biometrics are listed below in order of market size according to the International Biometric Group report of 2000 [ref: www.biometricgroup.com].

Fingerprint

Fingerprint systems tend to use characteristics of the fingerprint (usually one specific finger) rather than the actual image of the fingerprint. This is done to minimise storage space and reduce data handling. A small number of companies still use (part of) the image and straight pattern matching, but feature extraction is considered the norm. The data extracted from the fingerprint image is based on the position and nature of the minutiae – the irregularities that break up the otherwise smooth pattern of ridges and valleys that make up the fingerprint. There are many of these, some of which are shown in Figure 3.1 below.

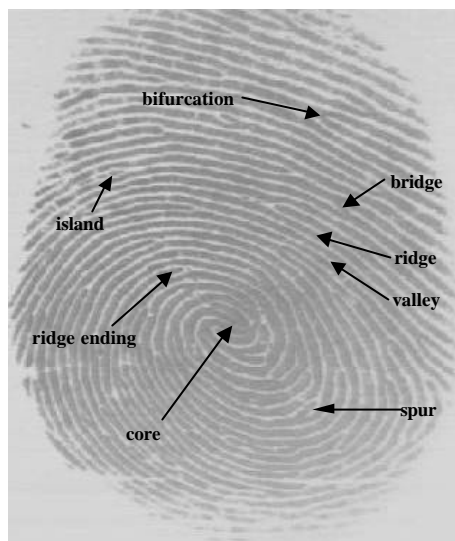


Figure 3.1: Fingerprint showing examples of some features used in authentication..

In simple systems the location of ridge endings and bifurcation points, with respect to the core, are used to describe the fingerprint, but it can be much more complicated than this by using finishing angle, type and quality, for example.

Concerns about fingerprint sensors include health, association with crime (although this is diminishing) and fear of fraud from severed or artificial fingers, or from images of the print. Some vendors offer life-testing sensors as an option.

The devices are easy to use and enrolment is straightforward. Small area devices do require a more accurate placement of the finger than the larger area ones. The performances of the system can be affected by pressing too hard, or too lightly, by misalignment, by cold and/or dry fingers and by dirt but these are dependent on the image capture methodology.

There are several diverse methods of capturing the initial fingerprint image, the most common methods being:

Optical. The oldest and most popular technique but losing favour to direct contact silicon systems.

It uses a CCD to capture an image from a finger placed on a transparent platen (usually the coated face of a prism). These are of reasonable cost but quite large (depth) due to the focusing requirements. This makes integration into small devices, such as cell-phones, impossible. They degrade with time and suffer from latent prints from previous users, although one company does offer a platen-free solution. Cold and/or dry fingers produce poor images. There are many vendors of this type of sensor, the main one being Identicator. One interesting variant comes from DELSY who make a very neat optical sensor with no lens. An optical fibre platen takes the light from the print (illuminated by the ambient light or by integrated IR LEDs) to a 2D CMOS sensor. This produces less distortion in the image than with lens based systems. It also has integral life sensing based on pulse and blood oxygen level. Its construction makes it quite robust.

Capacitive. The fastest growing fingerprint image capturing technique is to use a silicon sensor, made up of discrete rows and columns, as one plate of a capacitor with the user's finger acting as the other. This generates better images (generally) than the optical technique, although size reduction means a smaller area of print captured which requires placement to be more exact. The cost of the sensors is coming down significantly as

take up increases, primarily because integration is easy due to the chip size (typically 1 cm x 1.5 cm x 1 mm deep). The size is so small that integration onto smartcards is feasible. One company do this for health care in The Netherlands, but the sensor end of the card is thicker than the conventional smartcard end. Other companies are also looking at this. Although the size is small for biometric sensing, it is huge compared to most silicon chips, which is why they cost as much as they do. Coating of the chips has improved durability to about the same as that of optical systems. The sensors are very sensitive to electrical fields and electrostatic discharge. Cold and dry fingers produce poor images, as does over or under pressure from the user on the platen. Veridicom were the main company in this field but Infineon (Siemens) have grown large in this area over the last two years (due to producing a chip smaller than Veridicom). One company, Authentec, who use ac capacitance (dc is more common) claim to read the live sub-surface layer of skin thus ignoring dirt and other surface flaws. Finger Card make a near one-dimensional capacitive sensor (usual width but with a greatly reduced height) that requires the user to swipe their finger across it to create a 2-D image. This reduces the size and provides a self-cleaning process.

Ultrasonic. This technique is used by a single company (Ultra-Scan) and is theoretically the most accurate of the fingerprint image capture techniques. Being ultrasonic it overcomes the problems associated with dirty fingers and platens. It has a large area (similar to optical) so you get a bigger image that has advantages. It has the disadvantage of being relatively big (OEM > 10 cm x 14 cm x 18 cm), heavy (6 lb) and expensive so integration is limited. It takes about 3 seconds to validate a user, which is relatively long. The next generation promises to be considerably smaller and cheaper for "mobile" use. The vibration experienced whilst using the device may have a negative effect on the user although this is not confirmed. It is more robust than the silicon or optical devices.

Thermal. Another technique not used extensively. A silicon matrix (similar to capacitance sensors) detects thermal differences. The ridges are in contact with the sensor whilst the valleys are at ambient temperature. The temperature differences are converted to voltages and an image is formed. Unfortunately it does not last very long as the sensor and finger quickly reach a thermal equilibrium. Such a problem does not exist in the chip by Atmel-Grenoble. They use a sweeping motion across a near one-dimensional sensor ("The world's smallest fingerprint sensor" [ref]) to maintain a shifting thermal differentiation. The small array (finger wide but of much less rows) grabs an image of a slice of the fingerprint. Each slice comprises several overlapping rows and so the full image can be reconstructed from the slices. This makes the sensor production 5 times cheaper than the large area image arrays. Unfortunately that cost reduction has not yet been reflected in the marketplace. Insufficient data exists to compare the performance of this sensor to the others. It appears less intuitive to use given the movement involved.

Amongst other techniques tried or developing are:

- Using piezo-electric effect to detect pressure differences between ridges and valleys. This was one of the first methods tried but insensitivity amongst other problems meant no production.
- Using micro mechanical switches to detect pressure differences. This has never left the laboratory. It would result in a purely binary image that may be deficient in information content.
- Using RF field to stimulate the finger and have a sensor that acts as the antenna and detects the localised conductivity. At present there is not much information on the viability of this technique.

It is estimated that 5 to 10% of the adult population have "poor" fingerprints (dry, ill-defined prints). For a fingerprint sensor to be considered successful, it must be able to respond to these outlying cases. The ultrasonic system has been shown to be better than either the optical or the capacitance sensors in independent testing [ref] as it is higher resolution and can deal with dry fingers. No evidence is available for the thermal sensor.

Many companies produce software algorithms for fingerprint recognition that work on any image. In a recent study [ref] Sagem provided the top two algorithms. The test did not include all vendors, although most of the top ones were invited to participate.

The main uses of the technology at present are in PC/LAN access, physical access, health authority, driver licensing, and it is still prominent in criminology.

Fraud

The severing of fingers to get the user's print (whether it will work or not), or using latent prints to commit fraud is a real threat. Fingerprint sensors on cards could be an ideal solution.

Hand Biometrics

These systems can be split into three distinctive groups. Palm print, hand/finger geometry and vein pattern.

Palm print is a larger scale version of fingerprint. It uses optical techniques to image the palm and extracts features. There are several vendors of this type of system. Its obvious disadvantage is size and cost.

Hand geometry is performed by Recognition Systems (Ingersoll-Rand) only, and **finger geometry** by Biomet Partners only. Dermalog are developing a system for full hand geometry but it is not on the market yet. Hand exploits features such as surface area, finger length and width, etc whilst finger geometry uses the (3D) features of just two fingers (index and middle of leading hand). Both systems require accurate hand placement and use pins to dictate the location. Both systems have found applications in mass physical access systems (by verification) at theme parks (Disney World) and the sports events (Atlanta Olympics 1996), for example, as well as prisons and other more secure physical access applications. Both generally find user favour but size and cost have prevented mass-market installation. Sceptics still question the degree of variance available from hand geometry as well as long and short-term stability of the features used. All hand verification may have some cultural problems and be inoperable by older people with arthritis and other manual deficiencies. As the techniques are based on geometry, one assumes that growing children will have problems with such systems.

Vein pattern is used by two vendors vendor. A NeuScience produced device uses a low cost CCD camera with infrared pass filter to capture the vein pattern in the back of the hand. Not much is known about the pattern-matching algorithm but vein pattern (other than scale) is claimed to remain constant throughout life. Again it is quite large and costly but it is easy to use. The template is 300 byte, compared to 9 byte for hand geometry and 20 byte for the finger geometry, although 300 bytes is still small enough for magnetic strip or barcode storage. Palm print template sizes vary by vendor but are also small. "Livegrip" is produced by Advanced Biometrics. It uses vein pattern, but also artery and tissue, obtained from infrared scanning of the inside of the hand when it grips the sensor. Targets for the company are time/attendance systems, followed by trackballs (PC access), door handles (for physical access), firearm control via their hand grip.

Fraud

Fraud through the use of severed hands may not be possible but people actually trying it is possible. Forcing someone to present their hand is also more likely than forcing them to divulge their PIN.

Face

Biometrics systems based on face use the areas of the face least susceptible to short term change (eye sockets, cheekbones, mouth, etc. rather than hairline area for example). Generally they use off-the-shelf video cameras as the detection source, giving them many advantages. Cameras can be small and low cost (<\$50), are often integrated into systems anyway (multimedia PCs for example) and do not bind an integrator to a specific supplier or specialist. They are also non-contact and the user is familiar with the technology. In some cases they can be used without the person's knowledge, although this has privacy law implications as seen at Superbowl XXXV in 2000. Drawbacks are when faced with uncooperative subjects, poor illumination, finding wrong face in image field, and angled face. Like all biometrics systems they rely on getting a good image and having good enrolment data. The use of face may not be conducive with some cultures and religions.

The method of matching a face is based on one of four techniques:

Automatic face processing. Uses distances and ratios between common facial features. This is the most simple technique and the least robust, and does not tend to be used as much as the others. It's advantages are simplicity and it is less effected by poor lighting conditions.

Neural Network processing. Used by several companies, it uses the neural network to determine whether the presented face features are similar enough to the enrolled face features. Has the theoretical ability to be very intelligent and adaptive to changes.

Eigenfaces is an MIT technique that uses greyscale images that represent characteristics of a face. Any one facial image can be represented by combining many (100+) eigenfaces, and it is the coefficients representing that combination which make up the template which is used to determine if the presented face is the claimed face.

Local Feature Analysis. This technique is used by Visionics who are probably the top player in face recognition. The technique uses many small features and their relative location to build a template. It uses features from the centre of the face so it can deal with more angular displacement than the other techniques.

Many claims have been made about ability of facial recognition and whilst the technique is undoubtedly improving, it has never been shown to be as effective in practice as is claimed by the vendors.

Fraud

Persons trying fraud via decapitation of the legitimate user is gruesome but imaginable. The use of masks is another avenue for potential fraud. Again forcing someone to look at a camera is relatively easy – even more so that the contact systems. In theory, this biometric technique could be used without the user's co-operation or even their knowledge as a backup or addition to any other biometric deployed.

Speaker

Biometrics systems based on speech appear very attractive due to the non-contact nature and the familiarity of the biometric used. However, the lengthy enrolment process, local acoustics and transducer variation plagued early systems. On the plus side the transducers are low cost and already available in telephones, cell phones, PCs, etc and are easy to use. The technique is still being widely researched and is evolving to overcome the early problems. Phone services use speech verification systems, such as SpeechSecure from Veritel, in place of PINs and passwords. The technique is often quoted for use in multiple biometrics systems along with face and fingerprint. One interesting development is Voicevault by Buytel. This is a third party service that is available via telephone, the web or Internet, and authenticates a user by their voice. It is fast (1/2 second for Internet users anywhere in the world). Worries over false rejection at times of illness, stress and natural speech variation are some of the user worries.

Fraud

Fraud by mutilation is not a factor here, but recording of the human voice may create a simple fraud potential, although some companies claim recorder detection. It is also less easy to force someone to speak than to physically move that person, and the stress of forced speech could alter the voice enough so that failure of the system could occur anyway.

Iris

Iridian, who used to be Iris Scan but wanted to disassociate themselves from “scan” as it put users off, are the only vendor of this technique. Used in many high security areas in the USA and also to a limited degree in ATMs, it is an image-based method that identifies a person from an inherent radial pattern and visible characteristics (freckles, rings, furrows and corona for example) of their iris. Examination of an iris reveals just how complex the pattern is (figure 3.2). The pattern of the iris is formed prior to birth and does not change through life (except in cases of severe eye disease or head trauma).

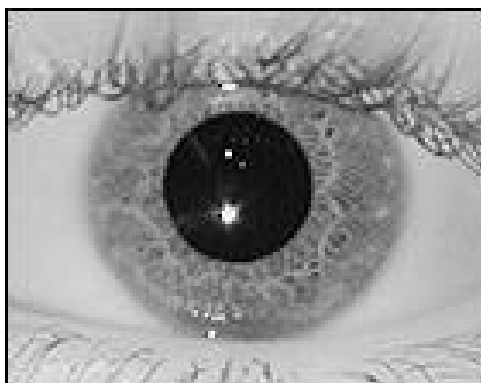


Figure 3.2: The human iris.

The IrisCode™ template produced at enrolment and in use is 512 byte. The uniqueness is quoted at $1:10^{52}$ and given there have only ever been 10^{11} people ever, the chances of false accept are negligible, even at 75% match (10^{16}). If a good image is captured, the chance of false rejection is nominal. One problem with the technique is getting the image. User co-operation is required to obtain a good image but unlike face and retina methods, normal spectacles do not cause a problem. Like all optical systems illumination is important (can be visible and/or infrared). The (monochrome) camera tends to be of higher quality than normal low cost video but a low cost camera version is, allegedly, being developed. The speciality camera, illumination and other factors result in a high cost system. Size is also an issue and the size prevents use in many applications. A relatively small unit (5" tall, 2" wide, 3" deep) for PC login and e-commerce exists, but it is not integrated into the PC or monitor. The "scan" implication gave a false impression of how the technique worked and created technology acceptance problems. Actual trials and installations of the device have been very successful. In independent testing the performance has proved better than any other common biometric device [ref]. Due to the necessary co-operation of the user, failure to capture is iris's poorest performance metric.

Fraud

The risk of fraud by the use of force is possible. The thought of attempting fraud by mutilation of a user is distasteful but could exist. This latter form of fraud is considered to be pointless, as a responsive eye is required. Using the system is not intuitive and it is comparatively slow. The fact that there is only one vendor is not an advantage.

Retina Scan

This technique also has only one vendor in EyeDentifier but with one product (Icam 2001). Next to iris, this is the most accurate and reliable methodology if a good image is collected. However, it is easily the most difficult (of the popular) method to use and the most invasive. To capture the image of the blood vessel pattern on the retina at the back of the eye (figure 3.3) via the pupil requires a very co-operative user to have a sensor close (<1") to their eye while the pattern at many (100s) points is captured. The resulting template is small at only 96 bytes.

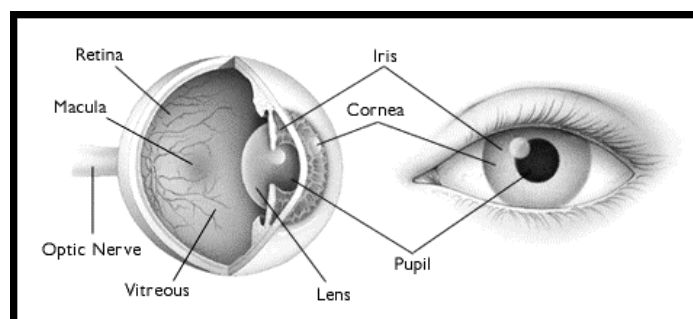


Figure 3.3: Construction of the human eye [ref. American Academy of Ophthalmology].

This method is used exclusively in high security areas where training can be provided. It is relatively slow and too expensive (>\$2000). The size (about that of a numerical keypad) allows desktop use but nothing smaller. EyeDentify claim a false accept rate of $1:10^6$. The false accept rate, failure to capture rate and failure to enrol rates may be high due to the operation of the device which is not conducive to spectacle wearers as it requires focusing at short distances for relatively long periods. Given that it is the vein pattern in the retina that is examined, the authors assume that a live eye is required. The requirement for a live eye and sci-fi film propaganda are the only positive aspects outside theoretical performance that this technique has.

Negative aspects

The technique has to be invasive and requires training and patience to use. It is non-contact (physically), but you have to place your eye very close to the sensor. The fact that the user must look into the output from a laser is perceived to be an unfavourable aspect for user acceptance. There are questions as to the stability of the measured feature (body temperature and tiredness for example have been quoted as possible causes of variance

within the pattern). The technique may evolve and theoretically the performance is attractive, but at present it has too many negative aspects.

Signature Dynamics

This is a behavioural biometric rather than a physiological one. Signature systems enjoy an acceptance and familiarity that no other biometric system has at present. Curiously then that it has never enjoyed good market share as a biometric. This could be because many systems, such as Cybersign, use CAD-style writing tablets with stylus rather than a real pen. These stylus-based writers are quite common for credit card voucher signature capture and PDA use but do take a bit of practice. Such systems look at time, stroke speed, spacing, letter formation, stylus pressure, etc. Used mostly in the electronic signature field, financial systems and PDA security. Systems like LCI-SMARTpen use a system that is more familiar to the user – a slightly oversized pen (actually writes) that is loaded with accelerometers to monitor the motion of the pen. It can be used on any surface, which is a huge advantage. Cost and size are quite attractive, but past performance could be off-putting. Like many biometrics systems of the past, many went to market before they or the public were ready and as such subsequent systems have suffered through association.

Typing Dynamics

Another behavioural biometric that only really works in a keyboard based environment, although one could in theory install or integrate a keyboard anywhere to use the technique. For network or PC access it can be continually used to ensure that the same person that logged in initially is still the person using the system. It has been shown to work well on subjects that are experienced typists that have characteristic typing habits. Not a widely used biometric.

Other techniques

Many other biometrics systems have been proposed but never brought to market - yet. These include the use of the earlobe, a person's smell, and a person's gait to identify an individual.



Preliminary paper written by: Gary Ross
Senior Research Engineer
Advanced Technology Group
NCR Financial Systems Division
Kingsway West
Dundee DD2 3XX
Scotland UK

Danish contact: Tue Bertelsen
NCR Danmark A/S
Svanevej 14
2400 København NV
Email: tue.bertelsen@ncr.com
Phone: +45 70 23 91 00