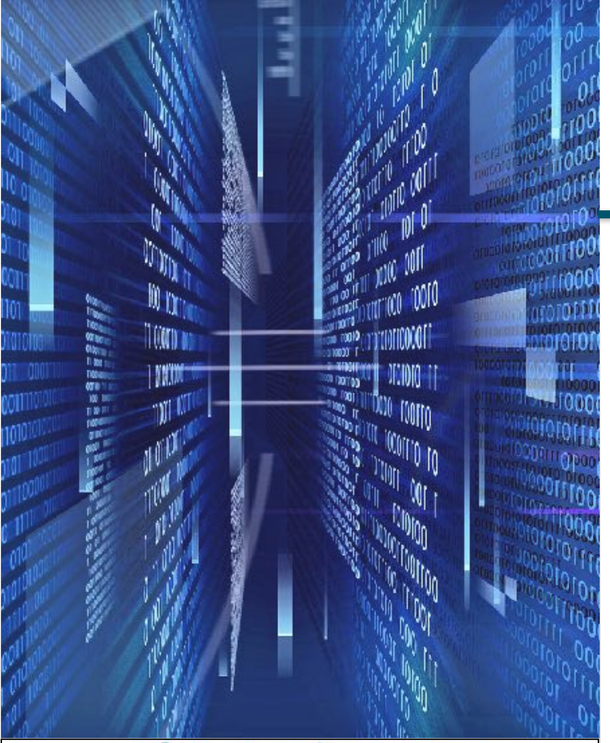

cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

UNIVERSITY OF Southampton

comp6224 (2016)
week 8: Biometrics

Vladimiro Sassone

Cyber Security Centre

University of Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

Biometrics

signatures

Handwritten signatures are a very weak authentication mechanism by themselves but have worked well for centuries because of the context of their use: in the UK and many other places a forged handwritten signature is completely null and void.

The essence of a signature is the intent of the signer, so an illiterate's '*X*' on a document is just as valid. In fact, a plaintext name at the bottom of an email message also has just as much legal force as an handwritten signature.

Signatures are better for the customer, while PINs and electronic tokens can be better for the bank. This is not universal: some Swiss banks make customers liable for forged cheques; in the USA, banks are liable for their electronic systems.

An experiment showed that 105 professional document examiners, who each did 144 pairwise comparisons, misattributed 6.5% of documents. Meanwhile, a control group of 34 untrained people of the same educational level got it wrong 38.3% of the time.

signature verification

The signature verification is done by an operator who is simultaneously presented on screen with the check image and the customer's reference signature. Verifying checks for small amounts is not economic unless it could be automated. A number of researchers have worked on systems to compare handwritten signatures automatically. This turns out to be a very difficult image processing task because of the variability between one genuine signature and another.

Most biometric systems have a trade-off between *false accept* and false *reject rates*, often referred to in the banking industry as the fraud and insult rates and in the biometric literature as *type 1* and *type 2* errors. The *equal error rate* is when the system is tuned so that the probabilities of false accept and false reject are equal.

For purely optical comparison this is several percent. This is not fatal for a check processing centre, as the automated comparison is used as a filter to preselect dubious checks for scrutiny by a human operator. However, it is a show-stopper in a customer-facing application: UK banks set a target for biometrics of a *fraud rate* of 1% and an *insult rate* of 0.01%, which is beyond the current state of the art in signature verification and indeed fingerprint scanning.

signature verification

So instead tuning for a

low insult rate and correspondingly high fraud rate

it is convenient to tune for fraud and insult rates approximately equal. When a signature is rejected, this merely tells the staff to look more closely, and ask for a driver's license or other photo-ID.

In an experiment with 8500 samples taken from 343 customers, 98.2% were verified correctly at the first attempt, rising to 99.15% after three attempts.

But this rate was achieved by excluding goats. With them included, the false reject rate was 6.9%. Because of this disappointing performance, sales of signature recognition technology are only 1.7% of the total biometric market; automation has cost it its leadership of the biometric market.

face recognition

The human ability to recognise faces is important to security because of the widespread reliance placed on photo ID. These are also used to bootstrap most other systems, which often require a photo ID to start the setup process.

But: *how good* are we at identifying strangers by photo ID? The simple answer is that *we are not*.

An experiment recruited 44 students and issued each of them with four credit cards each with a different photograph on it:

- one of the photos was '*good, good*': genuine and recent;
- one was '*bad, good*': genuine but old; the typical photo that most people have on their photo ID;
- the third was '*good, bad*': from a pile of random photographs, investigators chose the one which most looked like the subject; the typical photo that criminals would get;
- the fourth was '*bad, bad*': chosen at random except that it had the same sex and race as the subject; the typical photo that really lazy, careless criminals would get.

None of the checkout staff could tell the difference between '*good, bad*' photos and '*bad, good*' photos. In fact, some of them could not even tell the difference between '*good, good*' and '*bad, bad*'.

The experiment was done under optimum conditions, and real life performance can be expected to be worse. The overall conclusion was that the benefit to be had from photo ID is essentially its deterrent effect

So maybe people won't use their facial recognition skills effectively in identification contexts, or maybe the information we use to identify people in social contexts is stored differently in our brains from information we get by looking at a single photo.

automated face recognition

Attempts go back to the nineteenth century, when Francis Galton devised a series of spring-loaded ‘mechanical selectors’ for facial measurements.

Automated face recognition is actually a number of separate problems:

- typical identity verification: the subject looks straight at the camera under controlled lighting conditions, and his face is compared with the one on file;
- harder problem in forensics: establish whether a suspect’s face fits a low-quality recording on security video.
- hardest in surveillance: scan a moving crowd to pick out anyone who is on a list of thousands of known suspects.

Even picking out faces from an image of a crowd is non-trivial.

- an academic study of robustness of different facial feature extraction methods found that given reasonable variations in lighting, viewpoint, expression, no method was sufficient by itself and error rates were up to 20%;
- the U.S. Department of Defense in 2002 found that a leading face-recognition product correctly recognised one individual out of 270 only 51% of the time, and one person correctly out of 10 participants 81% of the time;
- A UK Passport Office trial in 2005 used a better approximation to field conditions, found it recognised only 69% of users.

Yet facial recognition is already the second largest-selling biometric with a nominal 19% of the market. However, much of this relates to the automated storage of facial images that are compared by humans — for example, the photos stored in the chips on the new biometric passports.

anthropometry

‘*Anthropometry*’, also known as ‘*Bertillonage*’:

system based on bodily measurements, such as height standing and sitting, the length and width of the face, and the size and angle of the ear.

Used since the 1970s for nuclear premises entry control, hand geometry is used at airports by the U.S. Immigration and Naturalization Service to provide a ‘fast track’ for frequent flyers.

NPL trials found a single-attempt equal error rate of about 1%.

Hand geometry is now reported to have 8.8% of the biometric market.

fingerprints

Automatic fingerprint identification systems (AFIS) are by far the biggest single technology.

In 1998, AFIS products accounted for a whopping 78% of the $50 m sales of biometric technology;

the huge growth of the industry since then has cut this in percentage terms to 43.5% of $1,539m by 2005.

The use of fingerprints to identify people was discovered independently a number of times.

- Mark Twain mentions thumbprints in 1883 in *Life on the Mississippi*
- fingerprints accepted in a seventh century Chinese legal code as an alternative to a seal or a signature;
- required by an eighth century Japanese code when an illiterate man wished to divorce his wife;
- mentioned by the English botanist Nathaniel Grew in 1684, by Marcello Malpighi in Italy in 1686;
- in 1691, 225 citizens of Londonderry used their fingerprints to sign a petition asking for reparations following the siege by King William.
- first modern systematic use: in India from 1858, William Herschel introduced handprints and then fingerprints to sign contracts, stop impersonation of pensioners who had died, and prevent rich criminals paying poor people to serve their jail sentences for them.
- Henry Faulds, a medical missionary in Japan, in the 1870s came up with the idea of using latent prints from crime scenes to identify criminals.

fingerprints

Galton wrote an article in *Nature*; this got him in touch with the retired Herschel, whose data convinced Galton that fingerprints persisted throughout a person's life.

Galton went on to collect many more prints and devise a scheme for classifying their patterns

The practical introduction of the technique owes a lot to *Sir Edward Henry,* who had been a policeman in Bengal. He wrote a book in 1900 describing a simpler and more robust classification, of *loops*, *whorls*, *arches* and *tents*, that he had developed.

In the same year he became Commissioner of the Metropolitan Police in London from where the technique spread round the world.

Henry's real scientific contribution was to develop Galton's classification into an indexing system.

By assigning one bit to whether or not each of a suspect's ten fingers had a whorl he divided the fingerprint files into 1024 bins. In this way, it was possible to reduce the number of records that have to be searched by orders of magnitude.

automatic fingerprint identification

how good are automatic fingerprint identification systems? A good rule of thumb is

to verify a claim to identity, it may be enough to scan a single finger;

to check someone against a blacklist of millions of felons, you had better scan all ten.

US-VISIT program set out to scan just the two index fingers of each arriving visitor, and has been overwhelmed by false matches. With 6,000,000 bad guys on the database, the false match rate in 2004 was 0.31% and the missed match rate 4%. The program is moved to '10-prints'.

In 2001, the NPL study found a 1% false match and 8% false accept rate for common products; by now, the better ones have an equal error rate of slightly below 1% per finger. False accepts happen because of features incorporated to reduce the false reject rate.

Errors are not uniformly distributed: manual workers and pipe smokers damage their fingerprints frequently, and both the young and the old have faint prints; fingerprint damage can also impair recognition.

Fingerprint identification systems can be attacked in a number of ways.

old trick was for a crook to distract (or bribe) the officer fingerprinting him, so that instead of the hand being indexed wrong under the Henry system and his record isn't found;

The most recent batch of headlines was in 2002, when T. Matsumoto and his colleagues showed that fingerprints could be moulded and cloned quickly and cheaply using cooking gelatine;

low-cost capacitative sensors are often fooled by such simple tricks as breathing on a finger scanner to reactivate a latent print left there by a previous, authorised, user;

fingerprints can also be reactivated — or transferred — using adhesive tape;

the more expensive thermal scanners could still be defeated by rubber moulded fingers.

iris scans

Recognising people by the patterns in the irises of their eyes is far and away the technique with the best error rates of automated systems when measured under lab conditions.

So far as is known, every human iris is *measurably unique*.

- it is fairly easy to detect in a video picture, it does not wear out, and it is isolated from the external environment by the cornea.
- the iris pattern contains a large amount of randomness, and appears to have many times the number of degrees of freedom of a fingerprint.
- it is formed between the third and eighth month of gestation, and (like the fingerprint pattern) is *phenotypic*, i.e., has limited genetic influence;
- the mechanisms that form it appear to be chaotic. So the patterns are different even for identical twins (and for the two eyes of a single individual), and they appear to be stable throughout life.

iris scans: technique

John Daugman found signal processing techniques that extract the information from an image of the iris into a 256 byte *iris code,* using a circular wavelet transform taken at a number of concentric rings between the pupil and the outside of the iris.

The resulting iris codes have the neat property that two codes computed from the same iris will typically match in 90% of their bits.

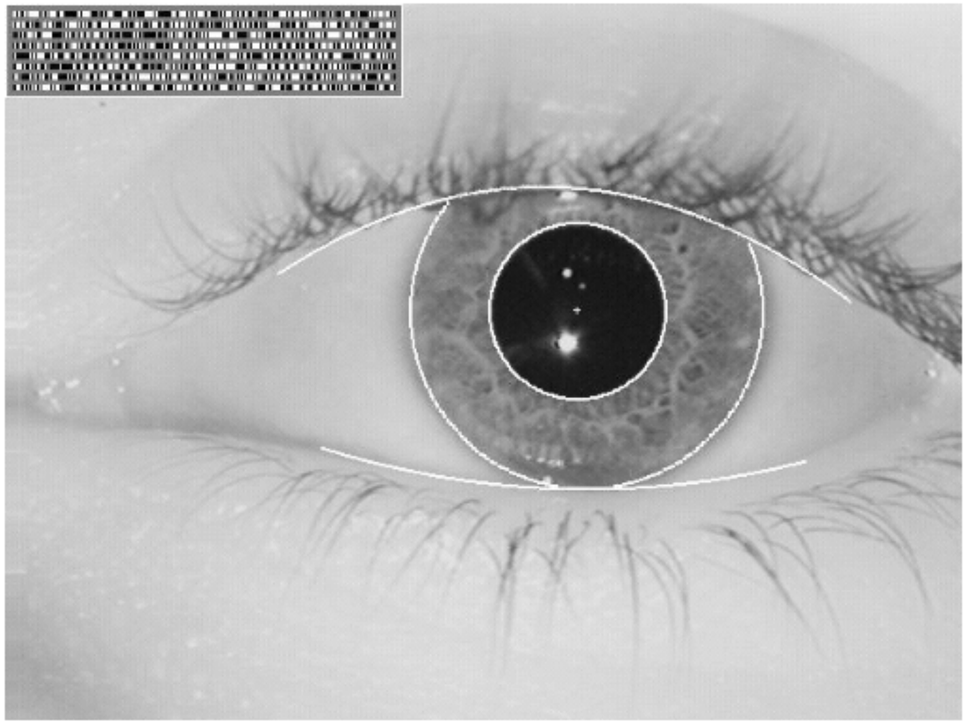

Figure 15.3: An iris with iris code (courtesy John Daugman)

iris scans: performance

The equal error rate has been shown to be better than one in a million, and if one is prepared to tolerate a false reject rate of one in ten thousand then the theoretical false accept rate would be less than one in a trillion.

One practical problem with iris scanning used to be getting the picture cheaply without being too intrusive:

- cooperation can be assumed with entry control to computer rooms;
- less acceptable in general retail applications as some people find being so close to a camera uncomfortable;
- current iris scanning systems use infrared light, and some people feel uncomfortable when this is shone in their eyes;

Given more sophisticated cameras, with automatic facial feature recognition, pan and zoom, it is now possible to capture iris codes from airline passengers covertly as they walk along a corridor.

iris scans: attacks

A typical attack was to take atropine eyedrops on the plane, dilating her pupils. Nowadays such travellers are held in custody until their eyes return to normal.

Evidentiary problems as:

- iris recognition depends on computer processing;
- there are no ‘experts’ at recognising eyes;
- it’s doubtful whether humans could do so, as the human eye is mostly insensitive to the information that John Daugman’s algorithms depend on.

Despite the difficulties, iris codes remain a very strong contender as they can, in the correct circumstances, provide much greater certainty than any other method that the individual in front of you is the same human as the one who was initially registered on the system.

They alone can meet the goal of automatic recognition with zero false acceptances.

voice recognition

Voice recognition — also known as *speaker recognition* — is the problem of identifying a speaker from a short utterance.

While speech recognition ignore speech idiosyncrasies to identify sentences, voice recognition systems need to amplify and classify them to identify people.

In *forensic phonology*, the task is usually to match a recorded telephone conversation, such as a bomb threat. A more straightforward biometric authentication objective is to verify a claim to identity in some telephone systems.

A recent application is the use of voice recognition to track asylum seekers in the UK

> they will be required to ring in several times every week; such systems tend to use caller-ID to establish where people are, and are also used for people like football hooligans who're under court orders not to go to certain places at certain times.

Attacks on these systems, quite apart from the possibility that a villain might somehow manage to train himself to imitate your voice in a manner that the equipment finds acceptable.

System fielded in U.S. EP-3 aircraft:

> breaks up intercepted messages from enemy aircraft and ground controllers into quarter second segments that are then cut and pasted to provide new, deceptive messages.

This is primitive compared with what can now be done with digital signal processing. Some expect that there will soon be products available that support real-time voice and image forgery.

other biometry systems

Typing patterns, also known as keystroke dynamics, were used in products in the 1980s but don't appear to have been successful.

Writing styles: there has been growing interest recently in identifying anonymous authors from their writing styles. Applications range from trying to identify people who post to extremist web fora to such mundane matters as plagiarism detection. It's possible that such software will move from forensic applications to real-time monitoring, in which case it would become a biometric identification technology.

Facial thermograms (maps of the surface temperature of the face, derived from infrared images), the **shape of the ear**, **gait**, **lip prints** and the **patterns of veins in the hand**, …

DNA typing. Its accuracy is limited by the incidence of monozygotic twins: about one white person in 120 has an identical twin. There's also a privacy problem in that it should soon be possible to reconstruct a large amount of information about an individual from his DNA sample.

summary

As with other aspects of security, we find the usual crop of failures due to bugs, blunders and complacency. Any protection measure that's believed to be infallible will make its operators careless enough to break it.

Biometrics are also like many other physical protection mechanisms (alarms, seals, tamper sensing enclosures, ...) in that environmental conditions can cause havoc. Noise, dirt, vibration and unreliable lighting conditions all take their toll.

There are a number of interesting attacks that are more specific to biometric systems and that apply to more than one type of biometric.

- Forensic biometrics often don't tell as much as one might assume.
- Most biometric systems can, at least in theory, be attacked using suitable recordings.
- Most biometrics are not as accurate for all people, and some of the population can't be identified as reliably as the rest.
- Most systems may be vulnerable to collusion.

summary

The statistics are often not understood by system designers:

> with 10,000 biometrics in a database, there are about 50,000,000 pairs; so even with a false accept rate of only one in a million, the likelihood of there being at least one false match will rise above one-half as soon as there are somewhat over a thousand people (in fact, 1609).

Designers assume that by combining biometrics they can get a lower error rate. The curious and perhaps counter-intuitive result is that a combination will typically result in improving either the false accept or the false reject rate, while making the other worse.

Consider the *hill-climbing attack* on face recognition systems: given a recogniser that outputs how close an input image is to a target template, the input face can be successively altered to increase the match.

Automating biometrics can subtly change the way in which security protocols work, so that stuff that used to work now doesn't.

What happens when humans and computers disagree? Iris data can't be matched by unaided humans at all: that technology is automatic-only.

But what happens when a guard and a program disagree on whether a subject's face matches a file photo, or handwriting-recognition software and a human controller disagree over whether a bank manager's writing looks genuine?