Security – Biometric identification

Markus Kuhn

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Michaelmas 2003 – Part II

Identification and authentication

→ Recognition: Selection from a set of known identities

→ Verification: confirming or denying a claimed identity

Commonly used means:

→ Something you know:
PIN, password, earlier transaction, ...

→ Something you have:
metal key, ID card, cryptographic key, smartcard, RF transponder, one-time password list, car registration plate, ...

→ Something you do:
handwriting/signature, accent, habits, ...

→ Something you are:
gender, height, eye/hair colour, face, fingerprint, voice, ...

Biometric identification

Use of a human anatomic or behavioural characteristic for automatic recognition and/or verification of a person's identity.

Desired properties of this characteristic:

→ universality – everyone should have it

→ uniqueness – no two persons should share it

→ permanence – it should be invariant with time

→ collectability – it should be practical to measure quantitatively

Desired properties of the measurement technique:

→ performance (accuracy, resources)

→ acceptability

→ difficulty of circumvention

A. K. Jain et al.: Biometrics – Personal Identification in Networked Society. Kluwer, 1999.

Application requirements for biometric techniques

→ recognition or verification

→ automatic/unsupervised or semi-automatic/supervised

→ user cooperation and experience

→ covert or overt

→ storage requirements

→ performance requirements

→ acceptability to user
(cultural, ethical, social, religious, or hygienic taboos)

→ size and environmental requirements of sensor

→ cost

Recognition accuracy

Four possible outcomes

- → Correct person accepted
- → Impostor rejected
- → Correct person rejected
- → Impostor accepted

Probability of the last two incorrect outcomes is known as *False Reject Rate (FRR)* and *False Accept Rate (FAR)*.

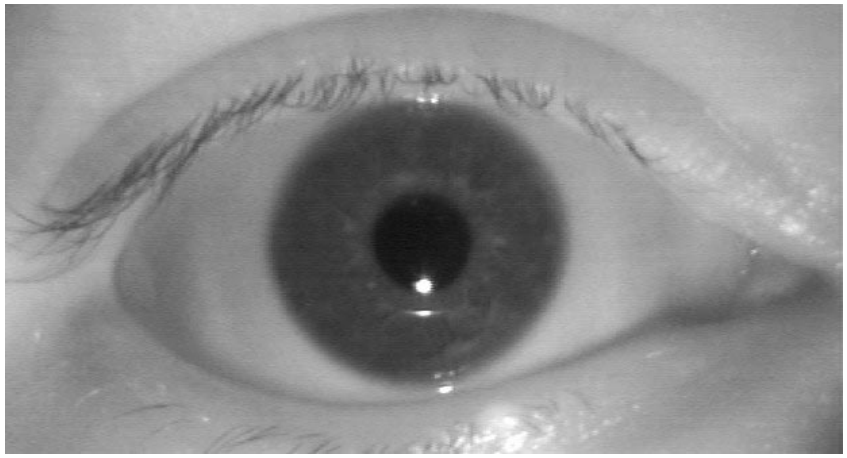
Biometric algorithms usually take a sensor signal, extract a feature vector and provide a distance metric. Adjust the maximum distance threshold for acceptance to trade-off FRR versus FAR.

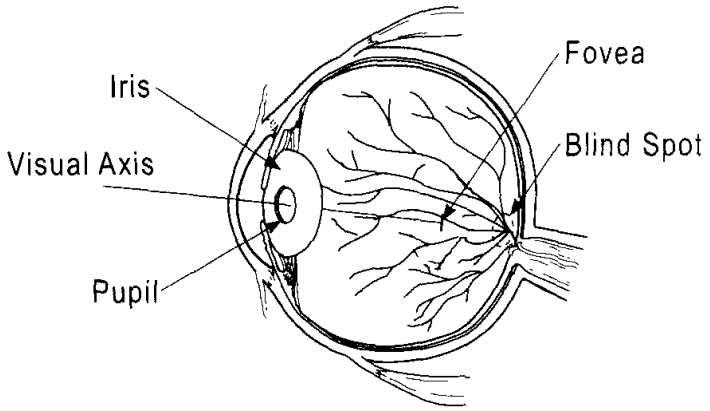
- → *Receiver Operating Characteristic (ROC)* – the curve of possible FAR/FRR tradeoffs.
- → *Equal Error Rate (EER)* – the result obtained by adjusting the acceptance threshold such that FAR and FRR are equal.

Security properties of biometrics

- → Biometric measurements should not be considered secret. Unlike passwords, measured body characteristics cannot be replaced after a compromise and they might be shared by multiple applications. Some are easy to sample covertly (face, voice, fingerprint, DNA).
- → Beware of the Birthday Paradox. To use a biometric for locating duplicates in n database entries, a false accept rate $\ll n^{-2}$ is needed.
- → Unsupervised sensors need means for distinguishing genuine live human tissue from fake templates.
- → Unsupervised biometric measurements should be attested by trusted and tamper-resistant sensor.

Iris patterns





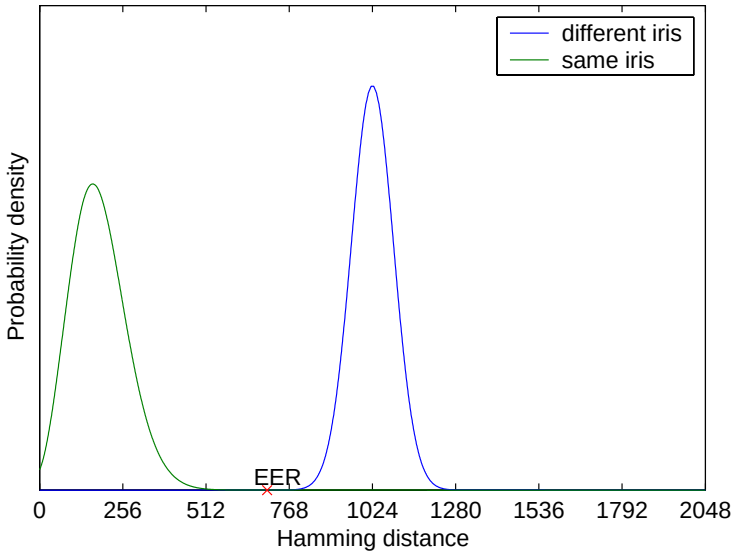
The iris pattern of the eye is uniquely suited as a biometric characteristic. It is an internal organ that is well-protected against damage by a sensitive and highly transparent window (cornea). The entropy of an iris image is at least 3 bit/mm^2.

Iris recognition

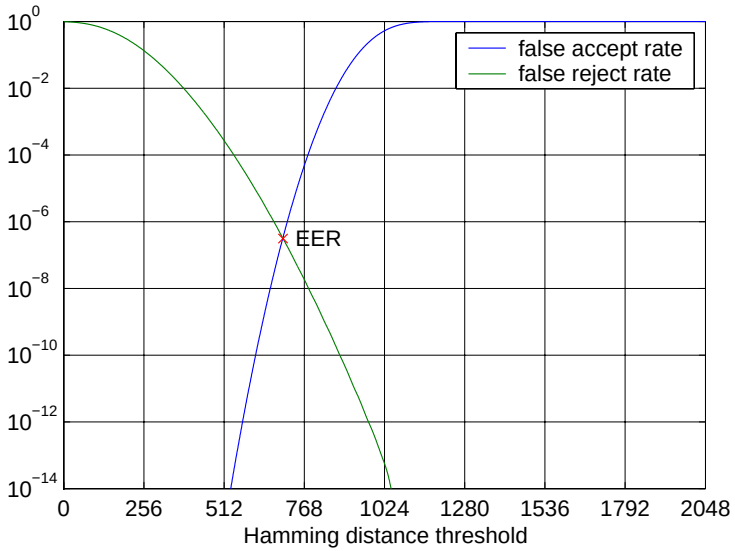
- → Acquisition from up to 1 m with wide-angle and tele camera.
- → Infrared band avoids uncomfortable visible illumination and improves the contrast of dark eyes.
- → Processing steps (Daugman's IrisCode algorithm): locate eye, zoom and focus, locate iris and pupil boundary, normalize both radii, locate obstructed areas (eyelids, eyelashes), polar coordinate transform, 2D Gabor wavelet transform, use 2048 sign bits as feature vector.
- → Compare feature vector by Hamming distance, try rotations.
- → $\approx 10\%$ mismatch for same, $\approx 50\%$ mismatch for different iris.
- → Theoretical equal error rate: $\approx 10^{-6}$
- → Live tissue verification via pupil reflex and oscillation?

J.G. Daugman: High confidence visual recognition of persons by a test of statistical independence. IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 15, No. 11, 1148-1161.

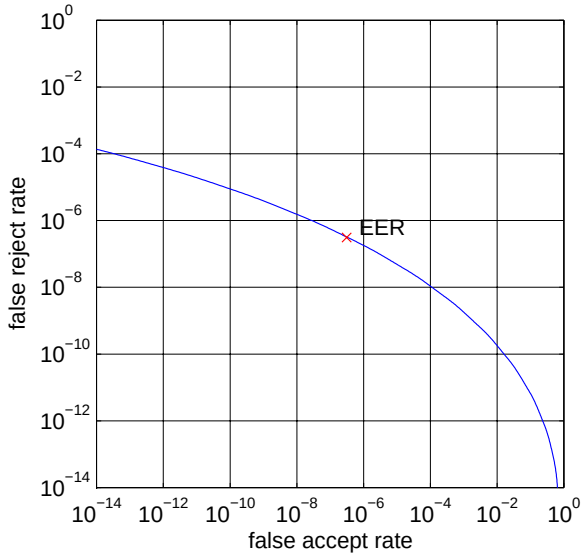
IrisCode Hamming distance threshold



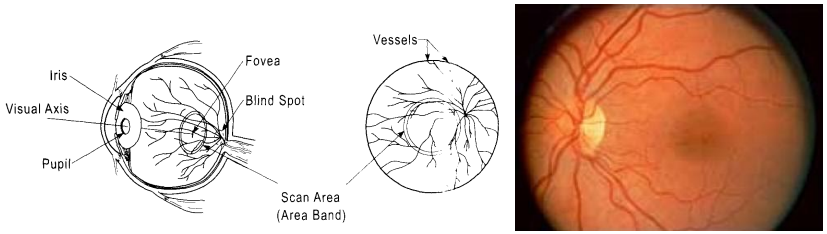
IrisCode performance



IrisCode receiver operating characteristics



Retina scan



Uses pattern of blood vessels behind the retina as a biometric characteristic. Similar to iris recognition, but several disadvantages:

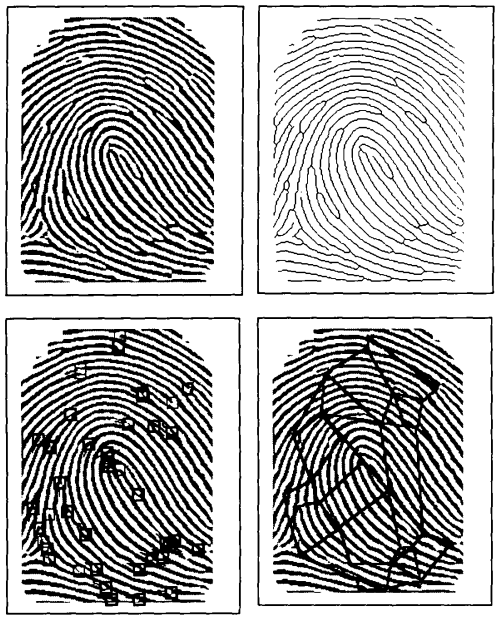
- ⟶ Compact sensor can see a significant part of the retina only from very short distance ⟶ user needs to bring head close to sensor and look directly into lens ⟶ slow and unergonomic.
- ⟶ Bright outdoor illumination causes pupil to contract too much.
- ⟶ Some users seem to be fearful because of the ophthalmologic feel of the procedure and possibly perceived health risks.

Fingerprints

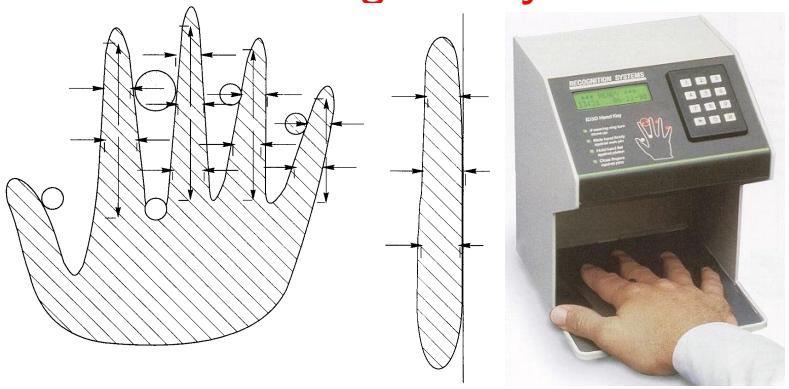
- ⟶ Biometric characteristic is the pattern of *ridges* and *valleys*.
- ⟶ Well-established forensic technique.
- ⟶ Patterns typically scanned with 0.05 mm (500 dpi) resolution.
- ⟶ Features can be the entire greyscale image, classes of ridge patterns ("arch", "loop", "whorl", with landmarks such as cores and deltas), the ridge pattern, and fingerprint minutae (locations and directions of ridge endings and bifurcations).
- ⟶ Classic recording technique is the ink fingerprint.
- ⟶ Modern fingerprint sensors:

  optical, capacitive, thermal, ultrasonic

- ⟶ Typical processing steps: normalising, thresholding, thinning, minutae extraction. Typical FAR 10^{-3}–10^{-4} with FRR 10^{-2}–10^{-1} for single image.



Hand geometry



Biometric characteristic used are several dozen length and thicknesses measurements of the fingers. Digital camera captures two hand silhouettes.

Hand needs to be aligned to posts, which may require some practice and good hand mobility.

With a typical EER of 10^{-3} more suited for verification rather than standalone recognition. Therefore usually combined with PIN or card.

Face recognition

→ Primary means of identification for humans

→ Potential of long-distance recognition and covert identification from surveillance cameras

→ Applicable to existing image databases

→ Has been combined with voice and lip movement recognition

→ Typical processing steps: locate eyes, normalize image, mask out nose/eye region, transform into "eigenface" space by using principal component analysis to obtain feature vector.

Problems:

→ Image varies significantly with illumination, facial expression, glasses, and age.

→ Field studies so far suggest that technology is far from mature.

Other biometric schemes

→ Handwitten signature dynamics or sound

→ Keystroke dynamics (for terminal applications)

→ Speaker recognition (for telephone applications)

→ Hand vein pattern (infrared image)

→ Infrared thermogram of face

→ Ear shape

→ Gait recognition
From surveillance cameras, floor pressure sensors or seismophones.

→ Body odor analysis

→ DNA
Slow analysis with Restriction Fragment Length Polymorphism (RFLP) or Polymerase Chain Reaction (PCR) markers, so far mosty used for forensic purposes, FAR limited by probability of monozygotic twins ($\approx 0.8\%$).

Attacks on biometric sensors

Fingerprint sensors:

→ Show photograph of fingerprint, recover latent fingerprint from sensor window with graphite powder.

→ Recover latent fingerprint: breathe against sensor window (residual oil pattern shapes condensation), place water-filled plastic bag onto it, or apply a bright light under the right angle.

→ Use gelatine or carbon-doped silicone rubber to mold a finger template from wax imprint or photo-etched pattern (PCB kit).

Face and iris recognition:

→ Show photograph or video on laptop to camera.

→ Cut out iris photo and stick it onto eye lid.

Live tissue verification is still a problem. Also various protocol attacks.

L. Thalheim, J. Krissler, P.-M. Ziegler: Body Check – Biometric access protection devices and their programs put to the test, c't 11/2002, p. 114, `http://www.heise.de/ct/english/02/11/114/`

T. Matsumoto: Gummy and conductive silicone rubber fingers, ASIACRYPT 2002, pp. 574-576. http://link.springer.de/link/service/series/0558/bibs/2501/25010574.htm

Biometric applications and standards

→ So far, mostly installed as independent island solution for building access control in companies and government agencies.

→ Most systems still use proprietary data formats, independent user enrolement is necessary for each.

→ Increasingly used for immigration control and issuing national identity documents.

→ US Patriot Act requires countries who want to maintain visa waiver status to introduce biometric passports by 2004-10-26.
International standardization of the underlying technology is still underway (ISO, ICAO). Passports will likely be fitted with a contact-less smartcard chip with >50 kB memory, to store JPEG photos of face, iris and two fingers. `http://www.icao.int/mrtd/`

→ Various biometric interoperability standards under development:

- BioAPI standard
  `http://www.bioapi.org/`
- Common Biometric Exchange File Format (CBEFF)
  `http://www.nist.gov/cbeff/`