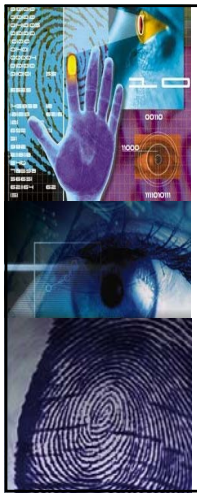


BIOMETRIC SYSTEMS

"Artificial Intelligence" Course
University of Naples Federico II
May 13, 2010

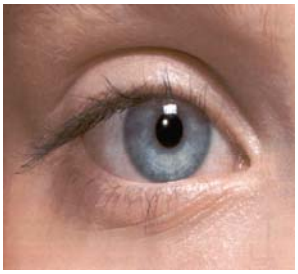
outline

1. Introduction to Biometrics
2. Fingerprint Recognition
3. Face Recognition
4. Iris Recognition
5. Multimodal Biometric Systems
6. Liveness Detection in Fingerprint Scanners

"State-of-the-art" Error rates

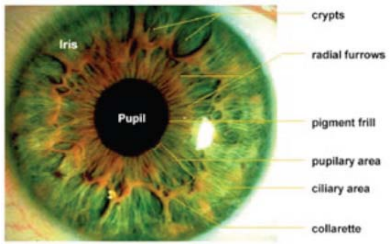
Modality	Test Label	Test Parameter	FNMR	FMR
Fingerprint	FpVTE 2003	US Government operational data	0.1%	1%
Fingerprint	FVC 2006	Heterogeneous population (young, elderly)	2.2%	2.2%
Face	FRGC 2006	Controlled Illumination, high-resolution images	0.8-1.6%	0.1%
Voice	NIST 2004	Text independent, multi-lingual	5-10%	2-5%
Iris	ITIRT 2005	Indoor environment	0.99%	0.94%
Iris	ICE 2006	Controlled Illumination, broad quality range	1.1-1.4%	0.1%

Iris Pattern



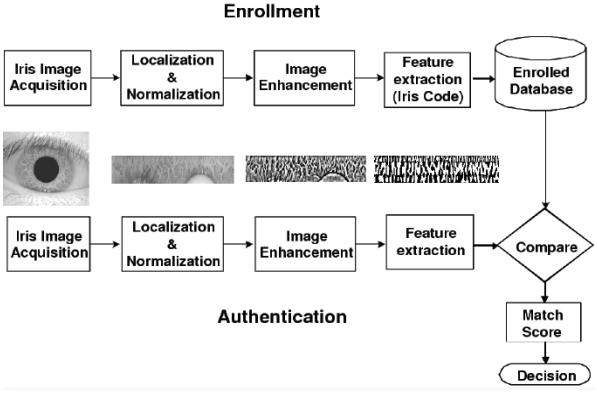

The iris is stable after the first year of life.
John Daugman

Texture of the iris

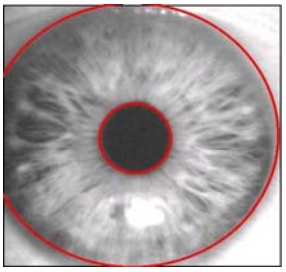


The iris exhibits a very rich texture. It consists in pectinate ligaments adhering into a tangled mesh revealing striations, ciliary processes, crypts, rings, furrows, vasculature and other features.
John Daugman

Iris processing steps



Localizing Iris



- Localize precisely the inner and outer boundaries of the iris.
- Detect and exclude eyelids if they intrude.

- These detection operations are accomplished by an integro-differential operator, which behaves as a circular edge detector:

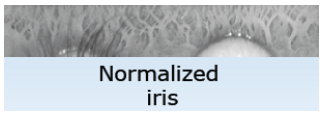
$$\max_{(r,x_0,y_0)} |G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds|$$

- The operator searches for a circular boundary with radius r and center (x_0, y_0) such that the change in radial pixel intensity across the boundary is maximum.

Iris Encoding

The output of the segmentation process is a binary mask that indicates the Iris and non-iris pixels in the image.

Normalization scheme: each point in the (x,y) domain is mapped to a pair of Polar coordinates (r, Θ). This results in a fixed size rectangular iris image.



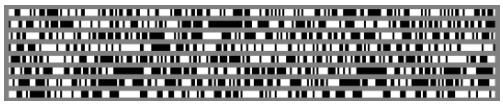
Normalized iris

IrisCode

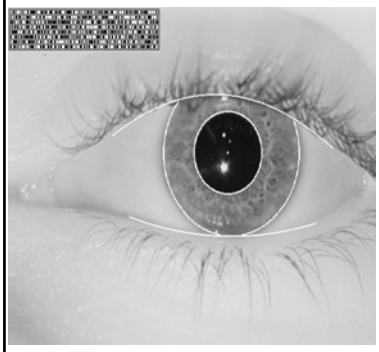
Gabor filters are then used to extract the textural information from the iris encoding.

$$G(x,y) = e^{-\pi[(x-x_0)^2/\alpha^2+(y-y_0)^2/\beta^2]} e^{-2\pi i[u_0(x-x_0)+v_0(y-y_0)]}$$

Since the prominence of iris texture changes as one moves away from the pupil, three different Gabor filters are applied to different regions of the normilized iris.



Comparison



- **Two IrisCodes** of eyes are compared by using Hamming Distance (HD) in order to detect the fraction of their bits that disagree.

$$\mathrm{HD} = \frac{\|(I_1 \otimes I_2) \cap M_1 \cap M_2\|}{\|M_1 \cap M_2\|}$$

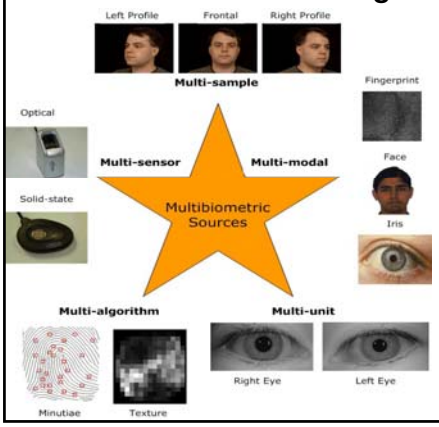
Fusion in Biometrics

A combination of multiple *pieces* of the *evidence*

Why Multi-Biometrics?

- **Performance Improvement,** error rates are not zero
- **Noisy Data**, e.g., low quality images
- **Intra-class Variations,** e.g., different samples of the same person
- **Distinctiveness**: Inter-class Similarity
- **Non-Universality**
- **Spoof Attacks**, e.g., artificial fingers

What to integrate?

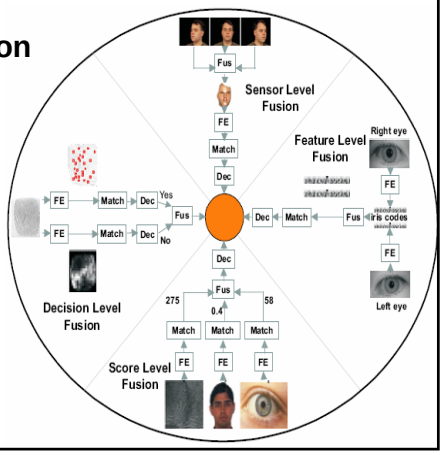


Multiple sources of evidence to obtain **multiple sources**:

- multi-Sensor
- multi-Sample
- multi-Algorithm
- multi-Instance
- multi-Modal

Levels of fusion

- Fusion *before* matching:
  - Sensor-level fusion.
  - Feature-level fusion.
- Fusion *after* matching:
  - **Score-level fusion.**
  - Decision-level fusion.

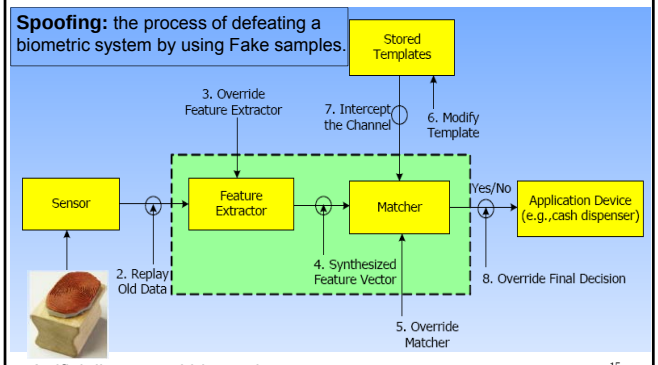


Biometrics and Liveness

- Is Biometrics a reliable, secure solution?
- What are the **threats** to biometric systems?
- How can we make biometric systems more secure?
- Since intruders will introduce a large number of spoofed biometrics, Liveness will enhance performance of a biometric system.
- Liveness detection reads claimant's physiological signs of life.

Attacks to Biometric Systems

Spoofing: the process of defeating a biometric system by using Fake samples.



Artificially created biometrics

Examples

Live

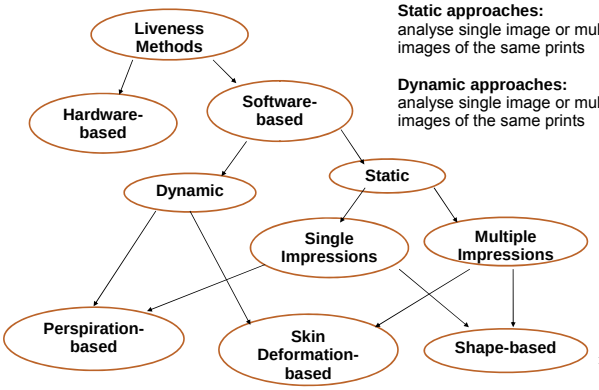
Gummy

Using an optical sensor

Analysis of the attack

1) Latent fingerprint dusted visible on the side of mug.
2) Finished **trasparency** showing negative image.
3) Finished board (mold).
4) Gelatine spread on the board as a thin layer.
5) Press the gelatine gently on the pad with the finger.

Taxonomy of approaches



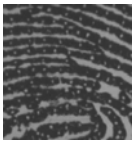
Static approaches: analyse single image or multiple images of the same prints

Dynamic approaches: analyse single image or multiple images of the same prints

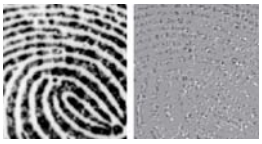
Static Algorithm

- The fingerprint image is tranformed into a *ridge signal*.
- The algorithm is based on statical features derived from a single fingerprint image.
  - Pore spacing.
  - Residual noise of the fingerprint image.
  - Intensity-based features.
  - Texture analysis.

Over 1000 dpi

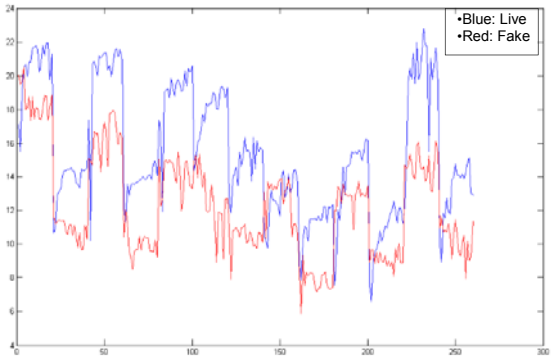


1000 dpi sensor



Original and noise residual images

Searching for discriminant features



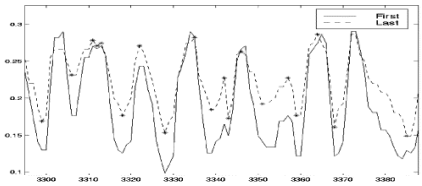
Standard Deviation of the Residual Noise

Dynamic Algorithm

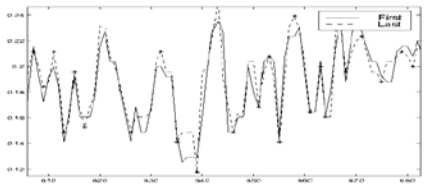
West Virginia Perspiration Method:

- The algorithm analyse the perspiration over time as sign of life.
- Fingerprint images are processed and ridge signals are obtained.
- Signal amplitude is proportional to the moisture along the traversed ridges.
- Peaks relate to the moistest and valleyss to driest regions.
- In live fingers, perspiration starts around the pores and spread along the ridges creating a distinct signature of the process.

Derived features



Live fingerprint signal



spoof

Constant periodic Peaks and rising valleys for the live signal.

References

- K. Choi H. Choi, R. Kang and J. Kim, "**Aliveness detection of fingerprint using multiple static features**", *World Academy of Science, Engineering and Technology, 28: 157-162, 2007.*
- S. Schuckers, "**Spoofing and Anti-spoofing measures**", *Information Security Technical Report,* 7(4): 56-62, 2002.