Multimodal Interaction

Lesson 12
Multibiometric systems

Maria De Marsico
demarsico@di.uniroma1.it

Presentation Outline

- Biometric Systems
  - Short introduction
  - Multibiometric Systems
- Data Normalization
  - Existing functions
  - Quasi Linear Sigmoid Function (QLS)
- System Response Reliability
  - Existing margin-based approaches
  - Proposed reliability indexes SRR I e SRR II
- Supervised Fusion
  - The Supervisor
  - Performances by Supervisor
- Cross Testing Protocol
  - Architecture
  - Performances
- Introduction to Ambient Intelligence
  - Definitions and trends
  - Interacting with an intelligent ambient
- Conclusions

Why biometric systems

At present, recognition (often for authentication purposes) is performed according to two modalities:

- Something one **owns**: a card or a document … but … it can be lost or stolen

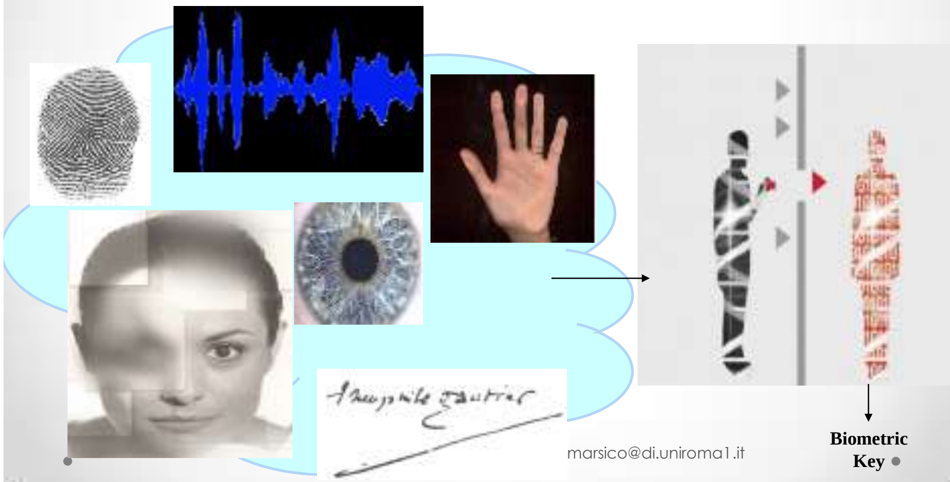
- Something one **knows**: an individual or community password … but … it can be guessed, wormed out or forgotten

Access Types

- Physical Access
  - Room
  - Building
  - Area
- Logical Access
  - Electronic resources
  - Critical data

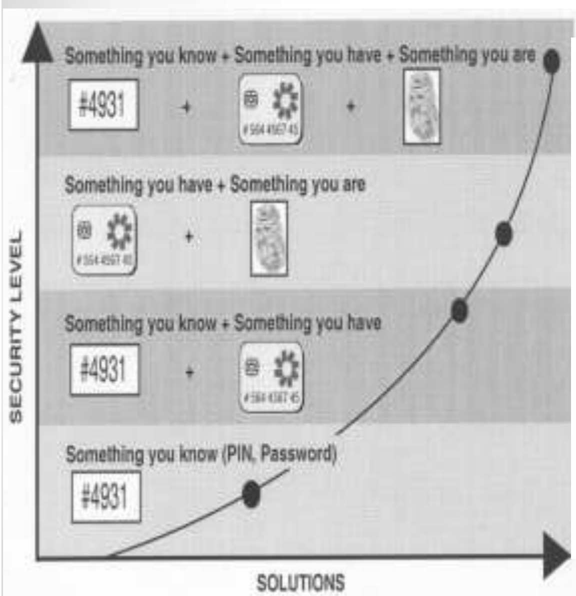
Why biometric systems

- Based upon what **one is**



marsico@di.uniroma1.it

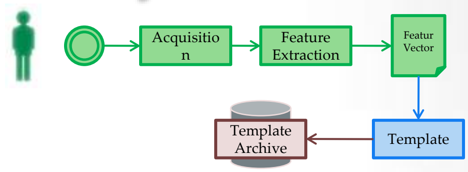
Why biometric systems

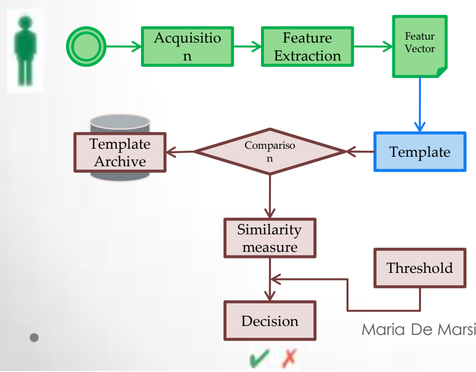


ırsico@di.uniroma1.it

Architecture of a Biometric System

Enrollment:
*C*apture and processing of user biometric data for use by system in subsequent authentication operations (gallery).





Recognition:
Capture and processing of user biometric data in order to render an authentication decision based on the outcome of a matching process of the stored to current template. (verification 1:1 identification 1:N)

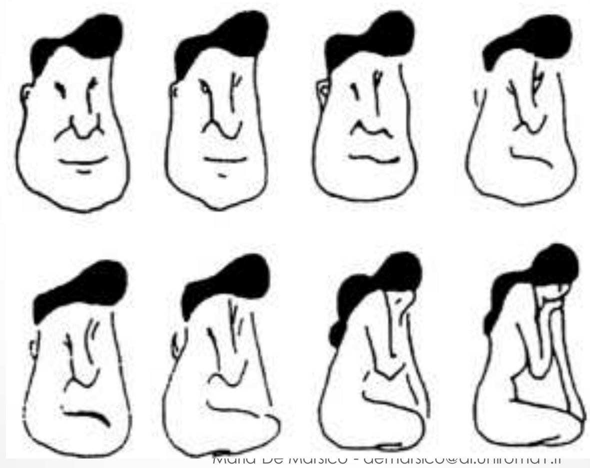
Modules of a biometric system

A biometric systema is generally designed to operate with four modules.

- Sensor Module : where biometric data are caught.
- Feature extraction module : where a set of main characteristics is extracted from acquired data. During enrollment it produces the templates to be stored in the system.
- Matching module: where extracted features are matched with stored templates to return one or more matsching scores.
- Decision module: where a decision is made according to matching results.

Biometric System – Pattern Recognition System

Two patterns are similar if the measure of the distance between their feature vectors, once suitably defined, is sufficiently small

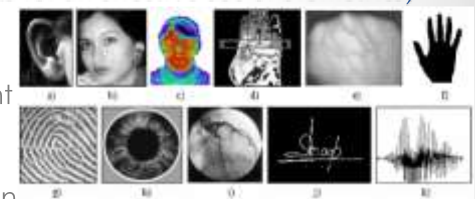


Requirements for a biometric trait

- **Universality**
  – The trait must be owned by any person (except for rare exceptions …)
- **Uniqueness**
  – Any pair of people should be different according to the biometric trait
- **Permanence**
  – The biometric trait should not change in time
- **Collectability**
  – The biometric trait should be measurable by some sensor
- **Acceptability**
  – Involved people should not have any objection to allowing collection/measurement of the trait

Acknowledged techniques in X9.84 - 2003 Standard

(minimum security requirements for an effective use of biometrics)



- **Fingerprints biometry** – fingerprint recognition
- **Eye biometry** – **iris** and **retina** recognition
- **Face biometry** – face recognition (**photo**, **infrared**)
- **Ear biometry** – ear recognition
- **Hand biometry** – finger **geometry**

Physiological Features

- **Signature biometry** – signature recognition (still and dynamic)
- **Keys typing**

Behavioural Features

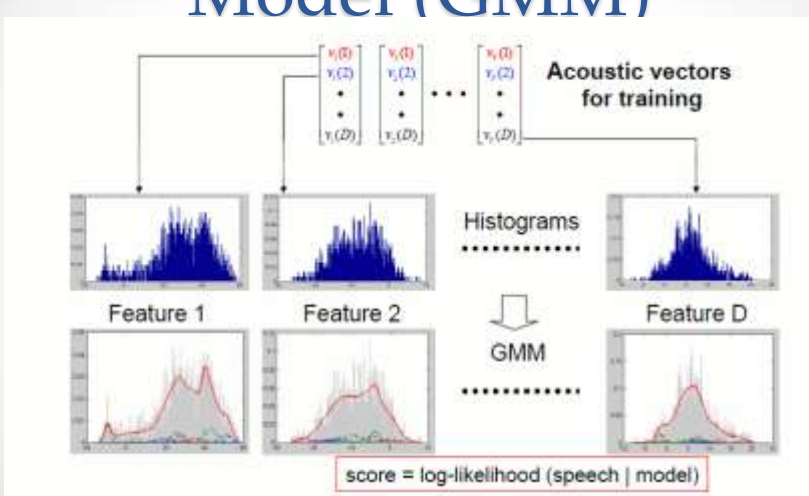
- **Voice biometry** – vocal recognition

Mixed features miste

- **DNA**

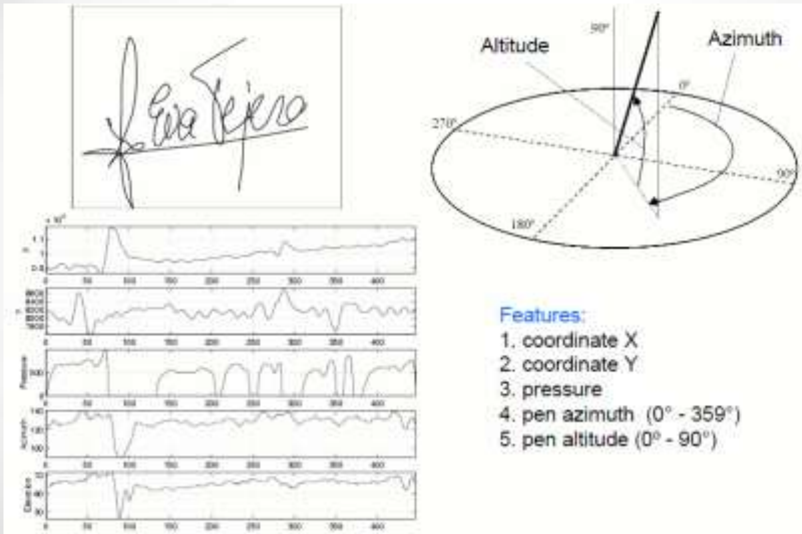
Biological Traces

Voice: Gaussian Mixture Model (GMM)



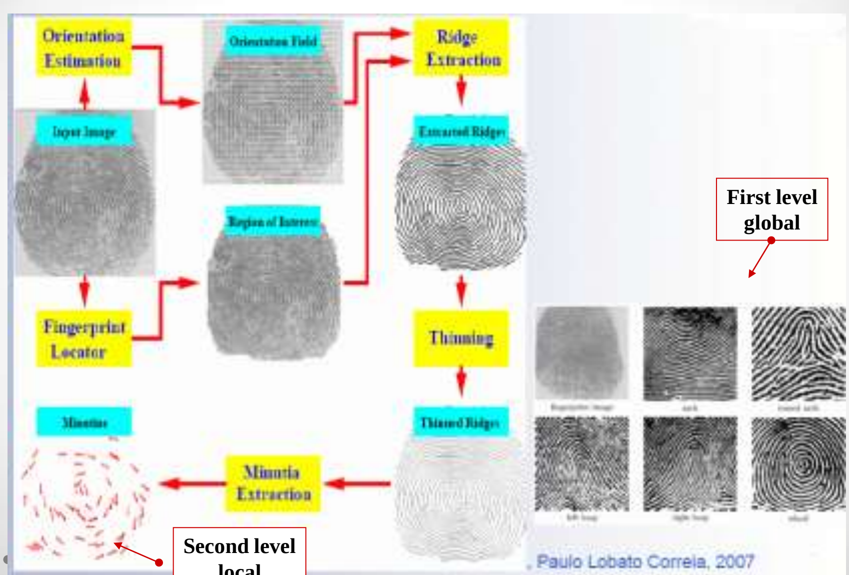
From: Dr. Andrzej Drygajlo, Biometrics for Identity verification, 2007

Signature

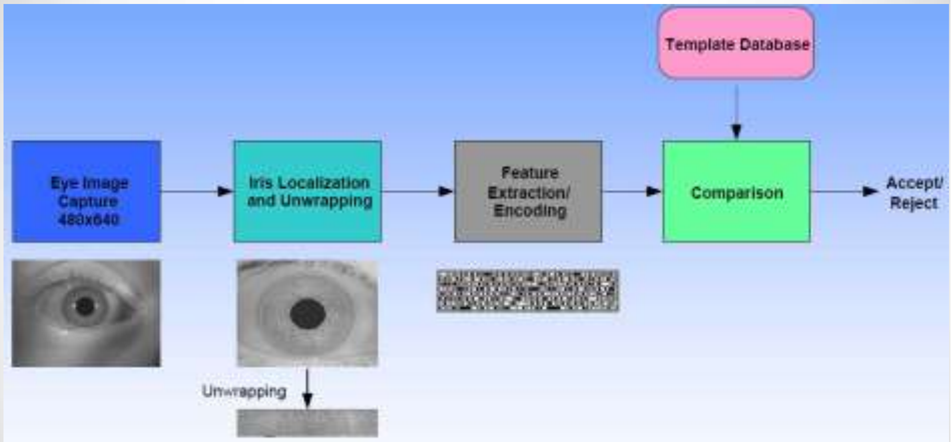


From: Dr. Andrzej Drygajlo, Biometrics for Identity verification, 2007

Fingerprint



Iris



J. Daugman,"Biometric Personal Identification System Based on Iris Analysis", US Patent5291560, 1994

Maria De Marsico - demarsico@di.uniroma1.it

Retina

- **Retina scanning**
  - Mapping of capillary vessels on the eyeground

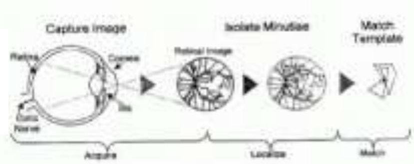
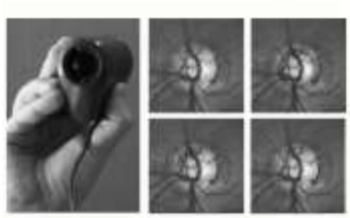
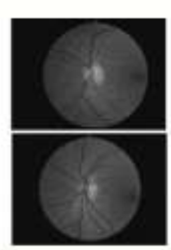


Exhibit 11-6. Retinal recognition process.

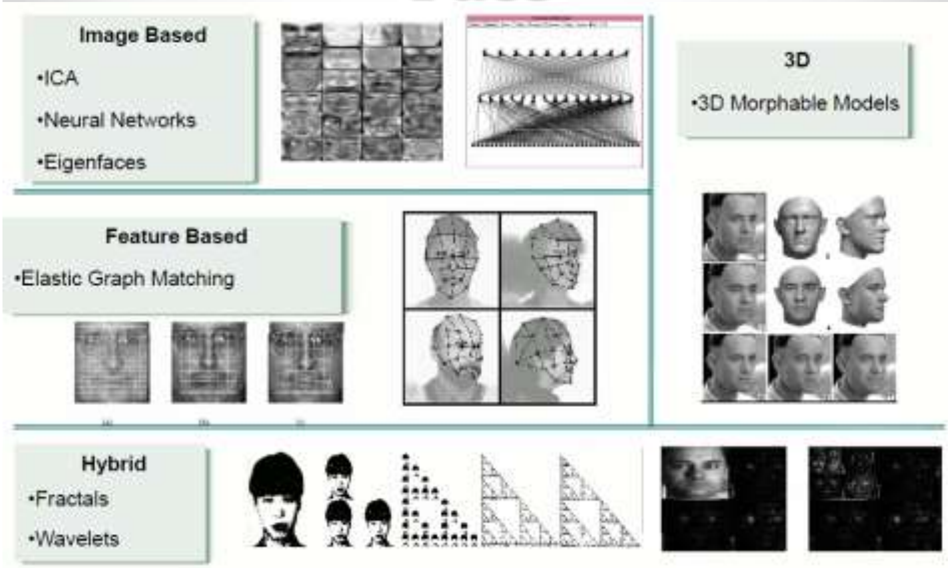




From: M. Nappi, Sistemi Biometrici, 2009

Maria De Marsico - demarsico@di.uniroma1.it

Face



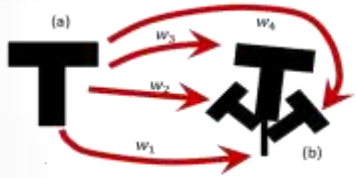
From: D. Riccio, Face Recognition, 2007

PIFS

- PIFS = Partitioned Iterated Function System
- A powerful fractal-based approach to image compression and indexing
- Exploits and codes the image self-similarities

PIFS(cont.)

- Evolution of **IFS** or **Iterated Function System**
- Arbitrary Image -> affine transformations -> finale image(self-similar).



IFS: (a) Initial image (b) image obtained at first iteration

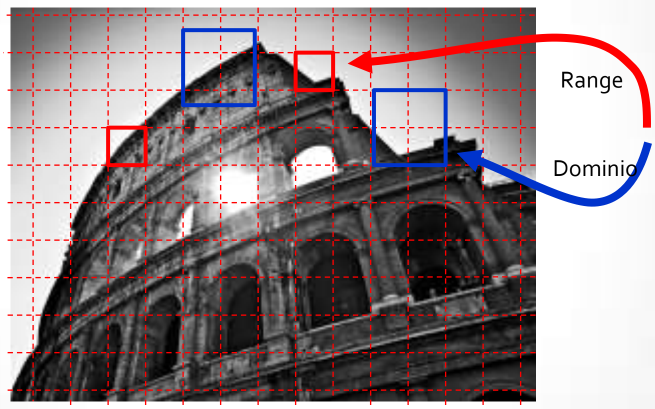
Image generated by an IFS (self-similar)

- **Only transformations can be recorded to recreate the final image**
- Real images are not perfectly self-similar

PIFS(cont.)

- An image can be composed by copies of a set of its subparts
- The image is partitioned in square non-overlapping regions called ranges
- Further square overlapping reagions, called domains, are also identified (side lenght = 2 side lenght of ranges)

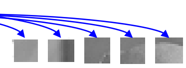
PIFS(cont.)



PIFS: self-similarities coding

Each range is coded through the best approximating domain after a suitable affine transformation

PIFS: self-similarities coding (range location)



Range blocks

- They represent a coverage of the image.

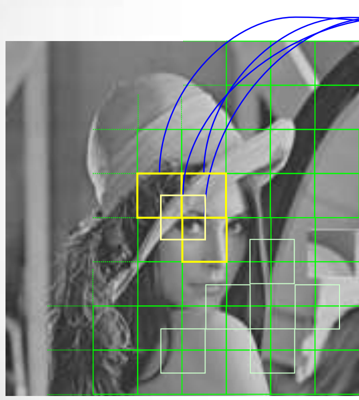
$$I = \bigcup_i r_i$$

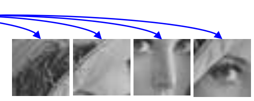
$$r_i \cap r_j = \varnothing, \qquad \forall i \neq j$$

This means 2^{12} 8×8 ranges, on a 512×512 pixel image.

Maria De Marsico - demarsico@di.uniroma1.it

PIFS: self-similarities coding (domain location)



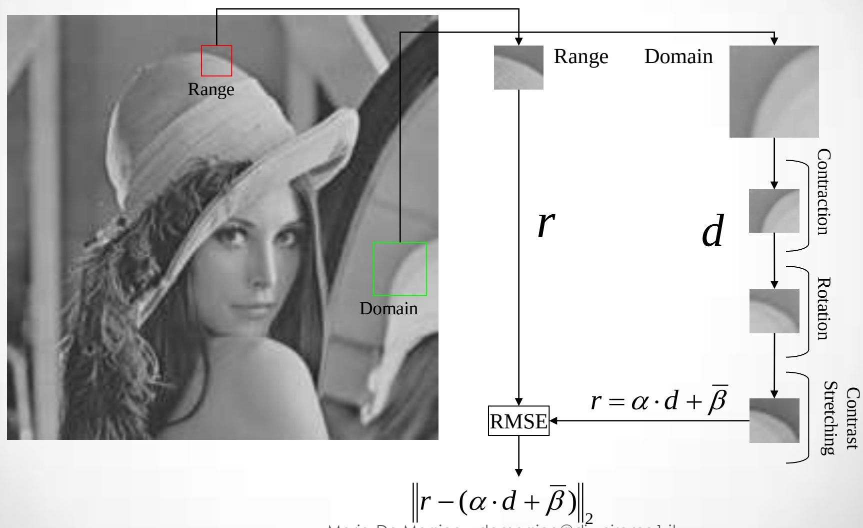


Domain blocks

This means 2^{18} 16×16 domain, for a 512×512 pixel image.

Maria De Marsico - demarsico@di.uniroma1.it

PIFS: self-similarities coding (range/domain matching)



Rearranging PIFS to face Recognition

Face Segmentation

The face image is segmented in four different regions (eyes, nose, mouth) and each one is segmented independently.

In this way, the feature extraction process is made local and the the effect of partial occlutions on the face image is mitigated.

A.F. Abate, R. Distasi, M. Nappi, D. Riccio, “Face Authentication using Speed Fractal Technique”, in *Image and Vision Computing* , vol. 24, no. 9, September 2006, pp.977-986.
A.F. Abate, M. Nappi, D. Riccio, G. Sabatino, “Face Recognition: A Survey on 2D and 3D Technques”, *Pattern Recognition Letters*, vol. 28, n° 14, pp. 1885-1906, 2007.
M. De Marsico, M. Nappi, D. Riccio. FARO: FAce Recognition Against Occlusions and Expression Variations. IEEE Transactions on Systems, Man, and Cybernetics — Part A: Systems and Humans, Vol. 40, No. 1, January 2010, pp. 121-132

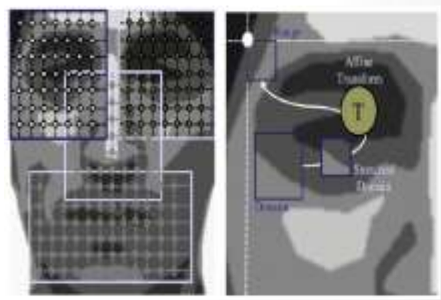
FARO

- FARO (Face Recognition against Occlusions).
- Face divided into regions, PIFS is executed on each region .
- Domains are clustered.
- A list of centroids is created for formatching.

$$C_k(x) = \frac{1}{|c_k|} \sum_{d \in c_k} d(x)$$

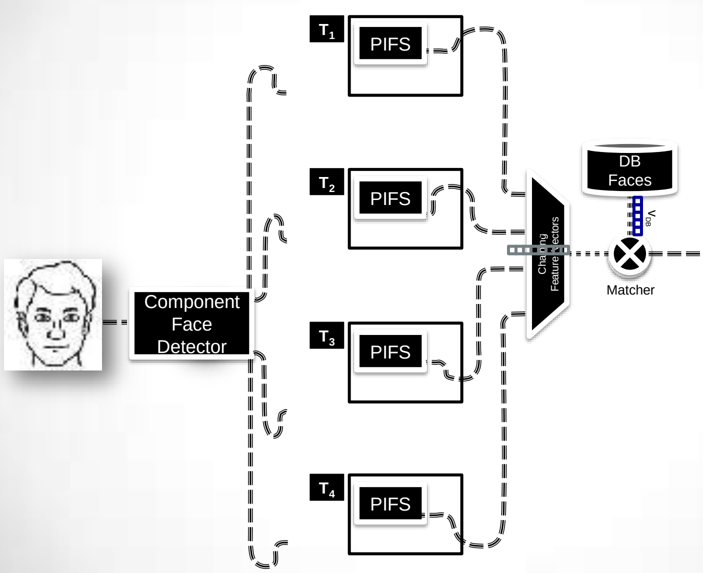
$$C_k(y) = \frac{1}{|c_k|} \sum_{d \in c_k} d(y)$$

$$C_k(\sigma) = \frac{1}{|c_k|} \sum_{d \in c_k} \sigma(d)$$



Maria De Marsico - demarsico@di.uniroma1.it

Plain Component-Based Protocol



Maria De Marsico - demarsico@di.uniroma1.it

The use of biometric traits

Biometric traits are a “natural” authentication methodology

•Benefits

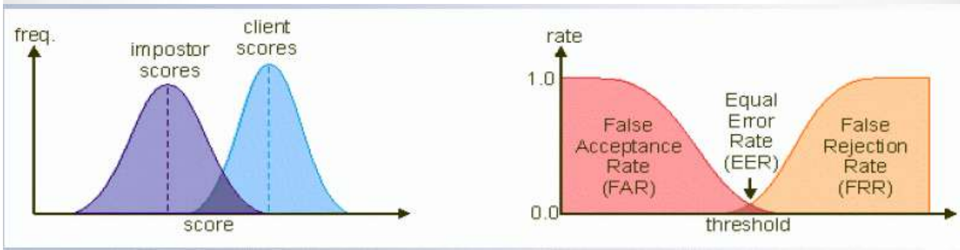
- Biometric traits cannot be lost, lent, stolen or forgotten (or changed either … see below)
- The user must only appear in person

•Drawbacks

- They do not ensure 100% accuracy
- Some users cannot be recognized by some technologies (e.g. heavy workers show damaged fingerprints)
- Some traits may change over time (e.g. face)
- If a trait is “copied”, the user cannot change it, as it happens for usernames or passwords (plastic surgery ?)
- Biometric devices may be unreliable under some circumstances.

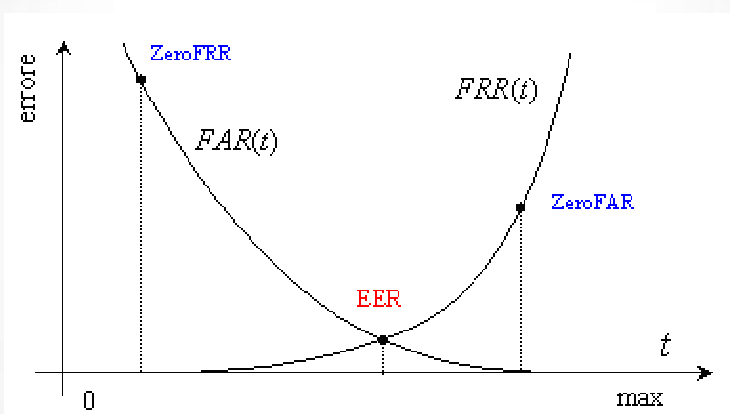
All that glitters… is not gold …

Biometric System – Possible errors



A score is said *genuine* (authentic) if it results from matching two samples of the biometric trait of a same enrolled individual; it is said *impostor* if it results from matching the sample of a non-enrolled individual.

Biometric System – Possible errors



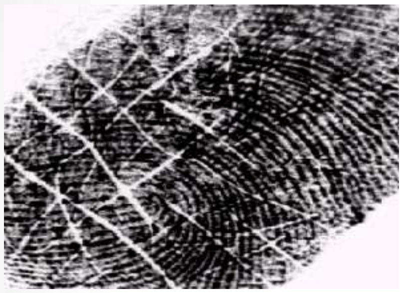
Problems: possible wide intra-class variations

Problems: possible very small intra-class variations

Twins

Father and son

Problems: noisy and/or distorted acquisitions



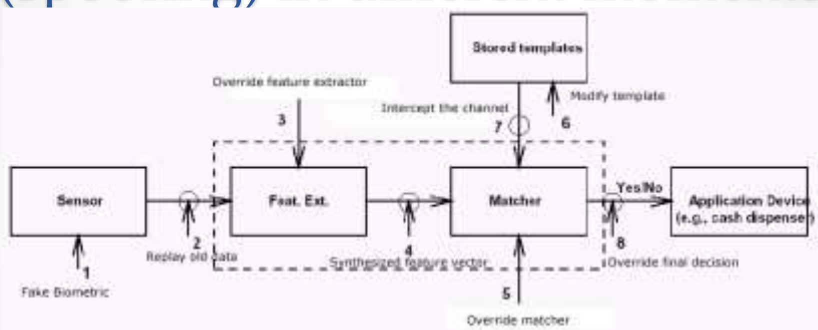
Poor quality fingerprints (eg. heavy worker)

Non uniform lighting

Problems: non universality

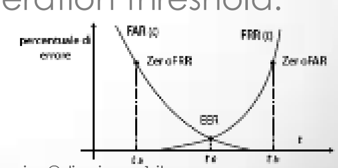
4% of population presents poor quality fingerprints
In some groups it is a particularly widespread characteristic (eg. elderly people)

Problems: possible attacks (spoofing) in different moments



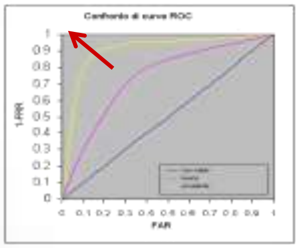
Evaluation measures (1:1)

- **FAR** - False Acceptance Rate, i.e. the probability of authenticating an unauthorized user, as a function of the operation threshold (acceptance threshold).
- **FRR** - False Reject Rate, i.e. the probability of rejecting an authorized user , as a function of the operation threshold (acceptance threshold).
- **EER** - The two curves intersect in this point, where the two errors present the same probability. Such point identifies a particular operation threshold.



Evaluation measures (1:1)

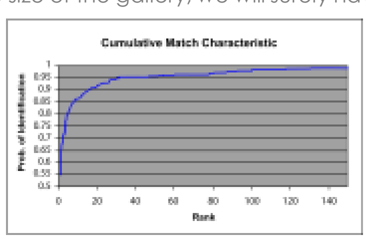
- **ROC** (Receiver Operating Characteristic) – ROC depicts the probability of Genuine Accept (GAR) of the system, expressed as 1-FRR, vs False Accept Rate (FAR) variation.



- **DET** (Detection Error TradeOff) - DET depicts the probability of False Reject (FRR) of the system, vs False Accept Rate (FAR) variation. It is plotted in logarithmic form.

Evaluation measures (1:N)

- **CMS (at rank k)** (Cumulative Match Score (at rank k) – The *probability of identification at rank k*, or even the ratio between the number of individuals which are correctly recognized among the first k and the total number of idividuals in the test set (probe).
- **CMC** (Cumulative Match Characteristic) – A *Cumulative Match Characteristic (CMC)* curve shows the *CMS* value for a certain number of ranks (clearly, each implying the following ones). It therefore reports the probability that the correct identity is returned at the first place in the ordered list (*CMS at rank 1*), or at the first or second place (*CMS at rank 2*), or in general among the first *k* places (*CMS at rank k*). If the number *n* of ranks in the curve equals the size of the gallery, we will surely have a probability value of 1 at point *n*.



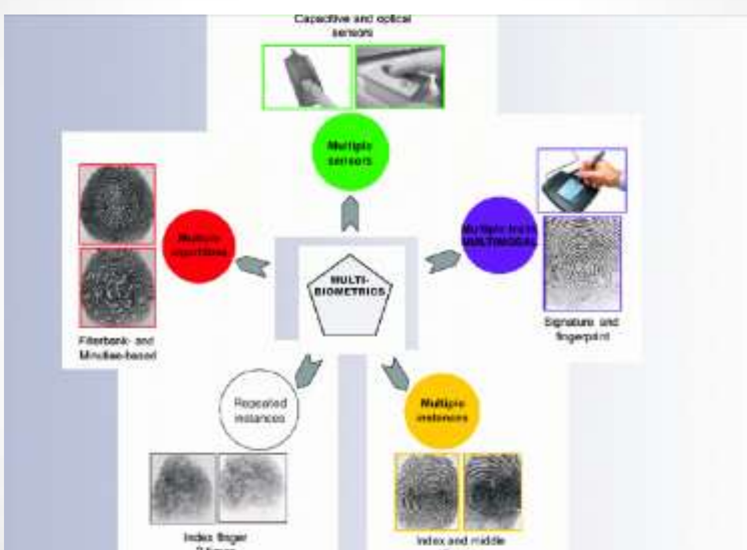
- **RR** (Recognition Rate) - CMS at rank 1 is also defined as Recognition Rate.

Systems with a single biometry vs Multibiometric Systems

Most present systems are based on a single biometry. This makes them vulnerable to possible attacks, and poorly robust to a number of problems.

A multimodal system provides an effective solution, since the drawbacks of single systems can be counterbalanced thanks to the availability of more biometrics.

Kinds of multibiometric systems



Biometrics, Paulo Lobato Correia, 2007

[Aguilar, J., *Adapted Fusion Schemes for Multimodal Biometric Authentication*, 2006]

Multimodal, multibiometric and multiexpert (or multiclassifier)

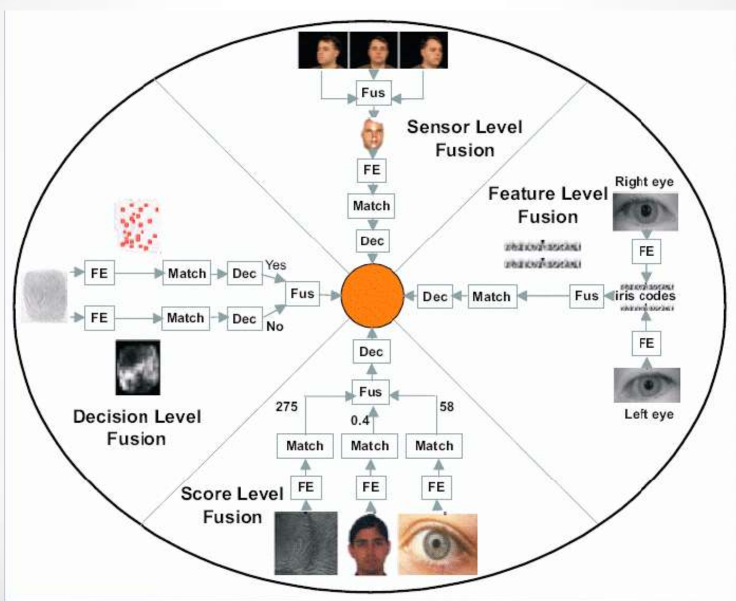
- **Multimodal**:

- **Multibiometric**:

- **Multiexpert**:

Maria De Marsico - demarsico@di.uniroma1.it

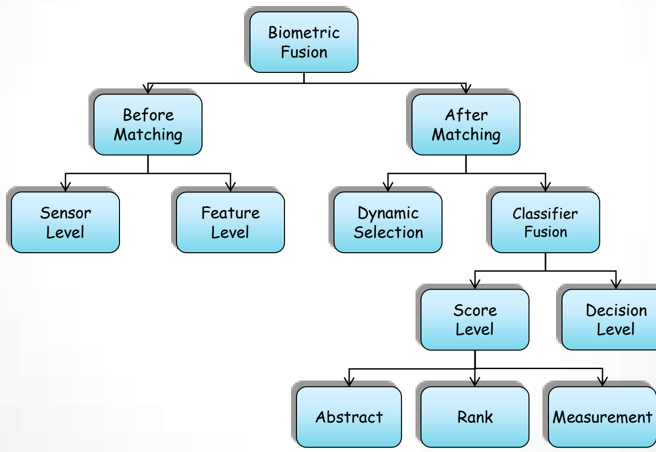
Kinds of fusion



[Aguilar, J., *Adapted Fusion Schemes for Multimodal Biometric Authentication*, 2006]

Kinds of fusion

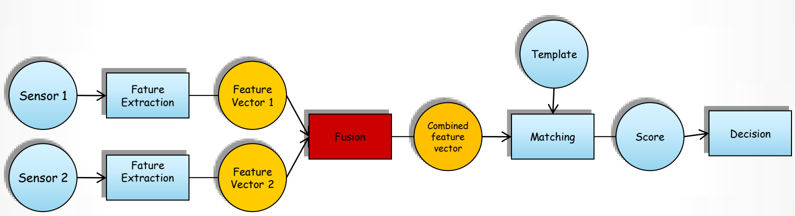
The combination of the different biometries can be peformed in each of the four system modules.



Maria De Marsico - demarsico@di.uniroma1.it

Feature level fusion

Features that were extracted with possibly different techniques can be fused to create a new feature vector to represent the individual.

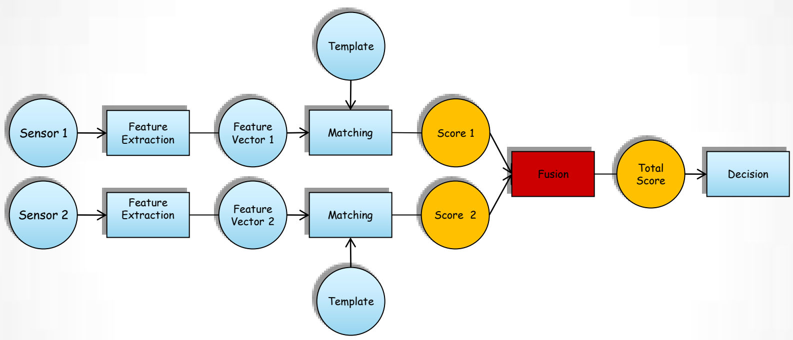


Better results are expected, since much more information is still present
Possible problems:
•Incompatible feature set.
•Feature vector combination may cause “curse of dimensionality”.
•A more complex matcher may be required.
•Combined vectors may include noisy and/or redundant data.

Maria De Marsico - demarsico@di.uniroma1.it

Score level fusion

Different matching algorithms return a set of scores that are fused to generate a single final score.



•***Transformation-based*** : the scores from different matchers are first normalized (transformed) in a common domain and then combined using fusion rules.

•***Classifier-based:*** the scores from different classifiers are considered as features and are included into a feature vector. A binary classifier is trained to discriminate between genuine and impostor score vectors (NN- Neural Networks, SVM – Support Vector Machine).

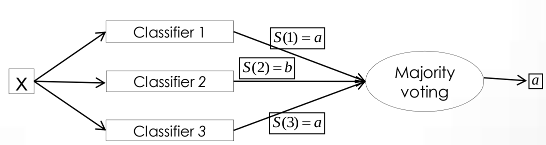
Score level fusion – Fusion Rules

Abstract:

Each classifier outputs its assignment of a *class label* to the input pattern.

•***Majority vote:***

- *each classifier votes for a class*, the pattern is assigned to the most voted class. Moreover, reliability of the multi-classifier is computed by averaging the single confidences.



Score level fusion – Fusion Rules

Rank:

Each classifier outputs its class rank.

$$\longrightarrow \begin{pmatrix} p_{c_1} = 0.10 \\ p_{c_2} = 0.75 \\ p_{c_3} = 0.15 \end{pmatrix} \longrightarrow \begin{pmatrix} r_{c_1} = 1 \\ r_{c_2} = 3 \\ r_{c_3} = 2 \end{pmatrix}$$

•***Borda count:***

- *each classifier produces a class ranking ogni classificatore* according to the probability of the pattern belonging to each of them. Ranking are then converted in scores that are summed up; the class with the highest final score is the one chosen by the multi-classifier.

Rank Value	C1	C2	C3
	c	a	b
	b	b	a
	d	d	c
	a	c	d

$$r_a = r_a^{(1)} + r_a^{(2)} + r_a^{(3)} = 1 + 4 + 3 = 8$$

$$\boxed{r_b = r_b^{(1)} + r_b^{(2)} + r_b^{(3)} = 3 + 3 + 4 = 10}$$

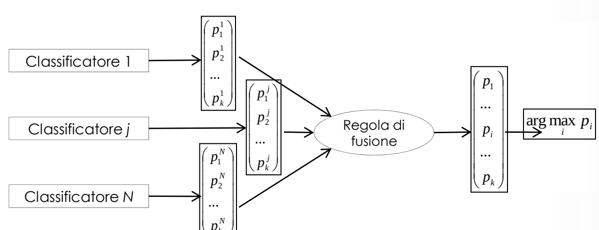
$$r_c = r_c^{(1)} + r_c^{(2)} + r_c^{(3)} = 4 + 1 + 2 = 7$$

$$r_d = r_d^{(1)} + r_d^{(2)} + r_d^{(3)} = 2 + 2 + 1 = 5$$

Score level fusion – Fusion Rules

Measurement:

Each classifier outputs its *classification score* for the pattern in comparison with each class.



Different methods are possible, including sum, weighted sum, mean, product, weighted product, max, min, ecc.

•Sum :

- the sum of the returned confidence vectors is computed, and the pattern is classified according to the highest obtained value

Maria De Marsico - demarsico@di.uniroma1.it

Score level fusion - Normalization

- Scores from different matchers are typically *unhomogeneous*:
  - Similarity/distance
  - Different ranges (eg. [0,1] o [0,100])
  - Different distributions
- To support a consistent score level fusion it is possible to exploit some score transformations (*normalization*), with particular attention to those laying in the overlap region between genuine and impostor.
- Issues to consider when choosing a normalization method:
  - *Robustness*: the transformation should not be influenced by outliers.
  - *Effectiveness*: estimated parameters for the score distribution should best approximate the real values.

Maria De Marsico - demarsico@di.uniroma1.it

Reliability

Due to the possible different quality of input data for the different subsystems, as well as to the possible different accuracy of the adopted recognition procedures, it would be desirable to define a *reliability measure* for each single response of each single subsystem before fusing them in a final response.

•A possible solution to reliability estimate is represented by *confidence margins*.

•Among the most popular ones (Poh e Bengio 2004):

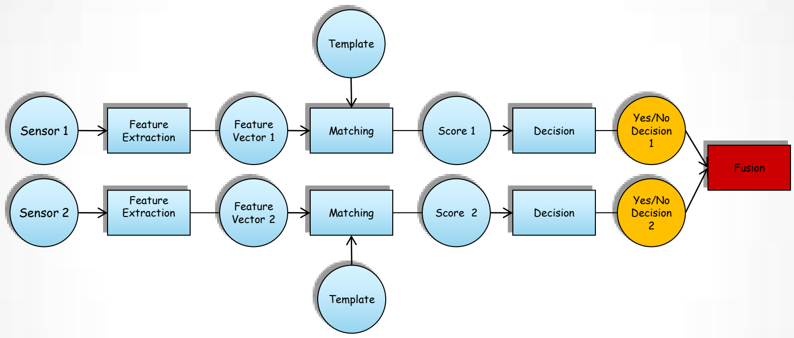
$$\mathrm{M}(\Delta) = \left| FAR(\Delta) - FRR(\Delta) \right|$$

based on FAR e FRR estimates.

Maria De Marsico - demarsico@di.uniroma1.it

N. Poh, S. Bengio, Improving Fusion with Margin-Derived Confidence In Biometric Authentication Tasks, IDIAP-RR 04-63, November 2004.

Decision level fusion



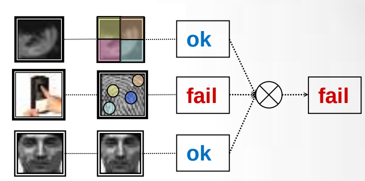
- Each classifier outputs its decision (accept/reject for verification or identity for identification). The final decision is taken by combining the single decisions according to a fusion rule.

Maria De Marsico - demarsico@di.uniroma1.it

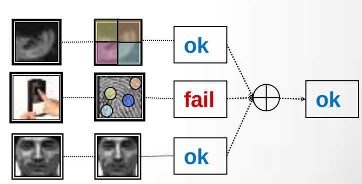
Decision level fusion

Different combination strategies are possible. The simplest ones imply a simple logical combination

•Serial combination *AND*
global authentication requires
all positive decisions.
This improves FAR.



•Parallel combination *OR*
the user may be authenticated
even by a single biometric modality.
This improves FRR.



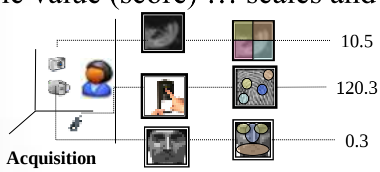
•A further important fusion rule at decision level is *Majority Voting*.

Maria De Marsico - demarsico@di.uniroma1.it

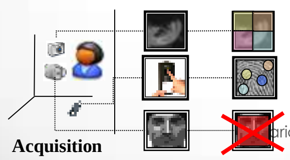
Critical Aspects of Multibiometric Systems

Let us return to some critical aspects:

• When each subsystem assigns a label to each subject with a numeric value (score) … scales and ranges can be different.



•It may happen that responses are not equally reliable.



Presentation Outline

- Biometric Systems
  - Short introduction
  - Multibiometric Systems
- Data Normalization
  - Existing Functions
  - Quasi Linear Sigmoid Function (QLS)
- System Response Reliability
  - Existing margin-based approaches
  - Proposed reliability indexes SRR I e SRR II
- Supervised Fusion
  - The Supervisor
  - Peformances by Supervisor
- Cross Testing Protocol
  - Architecture
  - Performances
- Introduction to Ambient Intelligence
  - Definitions and trends
  - Interacting with an intelligent ambient
- Conclusions

What about data normalization?

- A number of different solutions have been proposed in literature to solve this problem.

Normalization Functions	
Min/Max	$s'_k = \frac{s_k - \min}{\max - \min}$
Z-score	$s'_k = \frac{s_k - \mu}{\sigma}$
Median/Mad	$s'_k = \frac{s_k - median}{MAD}$
Sigmoid	$s'_k = \frac{1}{1 + ce^{-ks_k}}$
Tanh	$s'_k = \frac{1}{2}\left[\tanh\left(0.01\frac{(s_k - E[s_k])}{\sigma(s_k)}\right) + 1\right]$

- When minimum and maximum values are known, the normalization process is trivial.
- For this reason, we assumed to miss an exact estimate of the maximum value
- We chose the average value in its place, in order to stress normalization functions even more.

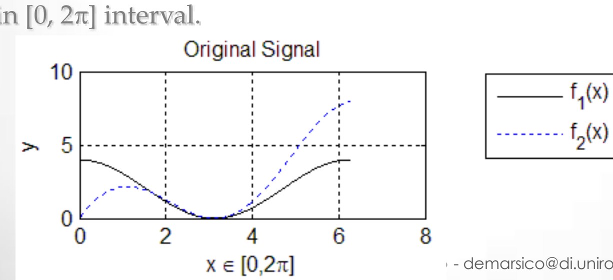
Testing the existing normalization functions

- we chose the two following test functions:

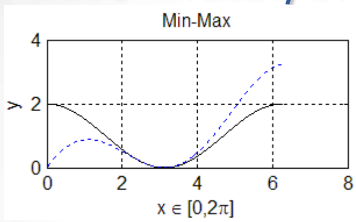
$$f_1(x) = 2 \cdot (\cos(x) + 1)$$

and $$f_2(x) = 2 \cdot \log(x+1) \cdot (\cos(x) + 1)$$

in [0, 2π] interval.



The Min/Max Function

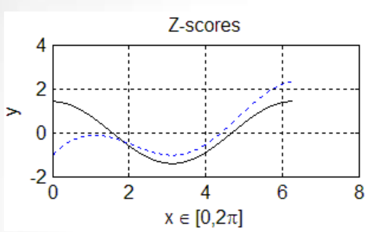


Normalization Functions	
Min/Max	$s'_k = \frac{s_k - \min}{\max - \min}$
Z-score	$s'_k = \frac{s_k - \mu}{\sigma}$
Median/Mad	$s'_k = \frac{s_k - median}{MAD}$
Sigmoid	$s'_k = \frac{1}{1 + ce^{-ks_k}}$
Tanh	$s'_k = \frac{1}{2}\left[tanh\left(0.01\frac{(s_k - E[s_k])}{\sigma(s_k)}\right) + 1\right]$

The Min-max normalization technique performs a “mapping” (shifting + compression/dilation) of the interval between the minimum and maximum values in the interval between 0 and 1

Such technique assumes that the minimum and maximum ever generated by a matching module are known.

The Z-Score function



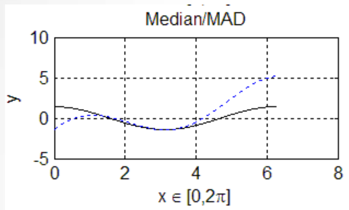
Normalization Functions	
Min/Max	$s'_k = \frac{s_k - \min}{\max - \min}$
Z-score	$s'_k = \frac{s_k - \mu}{\sigma}$
Median/Mad	$s'_k = \frac{s_k - median}{MAD}$
Sigmoid	$s'_k = \frac{1}{1 + ce^{-ks_k}}$
Tanh	$s'_k = \frac{1}{2}\left[tanh\left(0.01\frac{(s_k - E[s_k])}{\sigma(s_k)}\right) + 1\right]$

The Z-score technique is the most widespread and uses arithmetic average and standard deviation of scores returned by the single subsystem.

μ represents the arithmetic average of scores and σ is the standard deviation.

Z-score is that it does not guarantee a common interval for normalized values coming from different subsystems.

The Median/MAD function

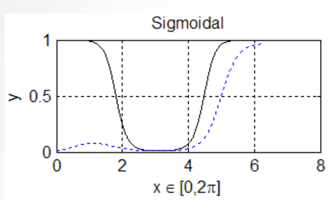


The Median/MAD technique uses the median and the MAD (median of absolute values) .

Median/MAD is less effective, most of all when values have a non-Gaussian distribution; in such cases it neither preserves the original value distribution nor transforms the values in a common numeric interval.

Normalization Functions	
Min/Max	$s'_k = \frac{s_k - \min}{\max - \min}$
Z-score	$s'_k = \frac{s_k - \mu}{\sigma}$
Median/Mad	$s'_k = \frac{s_k - median}{MAD}$
Sigmoid	$s'_k = \frac{1}{1 + ce^{-ks_k}}$
Tanh	$s'_k = \frac{1}{2}\left[tanh\left(0.01\frac{(s_k - E[s_k])}{\sigma(s_k)}\right) + 1\right]$

The Sigmoidal function



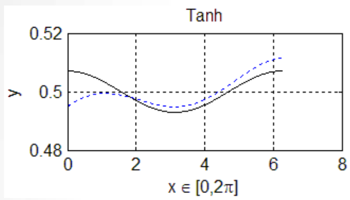
A Sigmoid function has the open interval (0,1) as codomain.

It has two drawbacks:

a) the distortion introduced by the function when x tends to the extremes of the interval is excessive;
b) the shape of the function depends on the two parameters c and k that in turn strongly depend on the domain of x parameter.

Normalization Functions	
Min/Max	$s'_k = \frac{s_k - \min}{\max - \min}$
Z-score	$s'_k = \frac{s_k - \mu}{\sigma}$
Median/Mad	$s'_k = \frac{s_k - median}{MAD}$
Sigmoid	$s'_k = \frac{1}{1 + ce^{-ks_k}}$
Tanh	$s'_k = \frac{1}{2}\left[tanh\left(0.01\frac{(s_k - E[s_k])}{\sigma(s_k)}\right) + 1\right]$

The Tanh function



The Tanh function guarantees data to be projected in the open interval (0,1).

It excessively concentrates values around the centre of the interval (0.5).

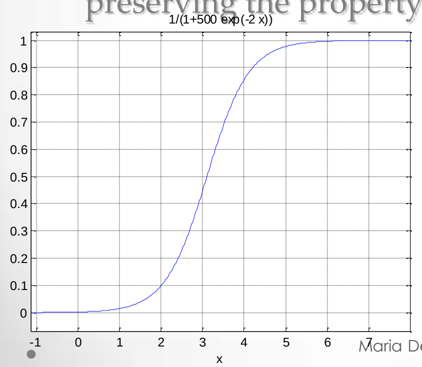
Normalization Functions	
Min/Max	$s'_k = \frac{s_k - \min}{\max - \min}$
Z-score	$s'_k = \frac{s_k - \mu}{\sigma}$
Median/Mad	$s'_k = \frac{s_k - median}{MAD}$
Sigmoid	$s'_k = \frac{1}{1 + ce^{-ks_k}}$
Tanh	$s'_k = \frac{1}{2}\left[tanh\left(0.01\frac{(s_k - E[s_k])}{\sigma(s_k)}\right)+1\right]$

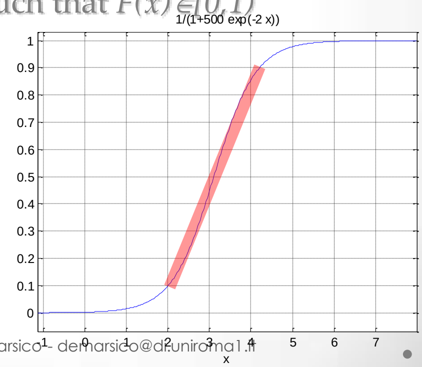
A new normalization function
Quasi-Linear Sigmoid (QLS)

- The desired properties of a new normalization function are:
  - The (0,1) codomain;
  - Minimal distortion of the input data distribution.
  - High robustness to imprecise maximum estimations.
  - A limited number of parameters.

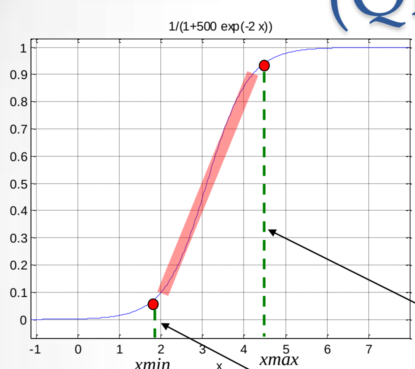
A new normalization function

- It is possible to reduce the distortion of the Sigmoid function $s'_k = \frac{1}{1+Ce^{-ks_k}}$ by deriving a new function *F(x)* from *f(x)*, with a pseudo-linear behaviour in the whole codomain though preserving the property such that $F(x) \in [0,1)$





Quasi-Linear Sigmoid (QLS)



- We find the null points of the third derivative:

$$f^3(x) = 6\frac{c^3k^3e^{(-kx)^3}}{(1+ce^{-kx})^4} - 6\frac{c^2k^3e^{(-kx)^2}}{(1+ce^{-kx})^3} + \frac{ck^3e^{(-kx)}}{(1+ce^{-kx})^2}$$

- Which are

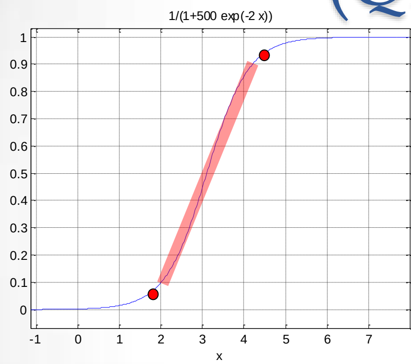
$$xmax = -\frac{1}{k}\log\left(\frac{2-\sqrt{3}}{c}\right)$$

- And

$$xmin = -\frac{1}{k}\log\left(\frac{2+\sqrt{3}}{c}\right)$$

[*xmin*, *xmax*] is the range in which the sigmoidal function assumes a pseudo-linear trend.

Quasi-Linear Sigmoid (QLS)



- Knowing that *xmin=0* and combining the two equations we can write:

$$c = 2 + \sqrt{3}$$

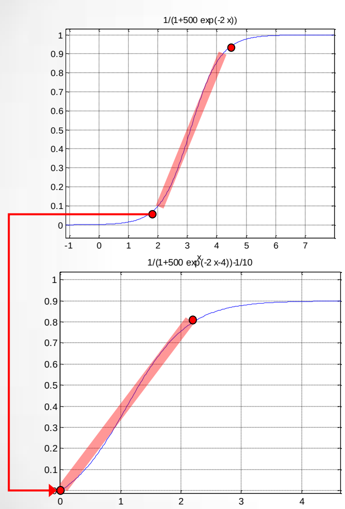
- And

$$k = -\frac{1}{xmax}\log\left(\frac{2-\sqrt{3}}{2+\sqrt{3}}\right)$$

xmax is the only parameter we have to know.

Maria De Marsico - demarsico@di.uniroma1.it

Mapping *f(xmin)* to *0*



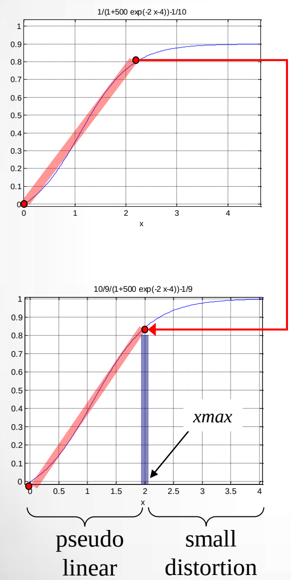
- To map *f(xmin)* to *0* we define a new function:

$$g(x) = f(x) - f(xmin)$$
$$= f(x) - f(0)$$

The upper limit of the function *g(x)* has to be mapped on *1*.

Maria De Marsico - demarsico@di.uniroma1.it

Mapping $f(\infty)$ to 1



- To map $f(\infty)$ to 1 we compute:

$$L = \lim_{x \to \infty} g(x) = \frac{2+\sqrt{3}}{3+\sqrt{3}}$$

- and, finally, we define:

$$\boxed{F(x) = \frac{1}{L} g(x) = \frac{1 - b^{\frac{x}{xmax}}}{ab^{\frac{x}{xmax}} + 1}}$$

- with

$$a = (2+\sqrt{3}) \quad \text{and} \quad b = (7-4\sqrt{3})$$

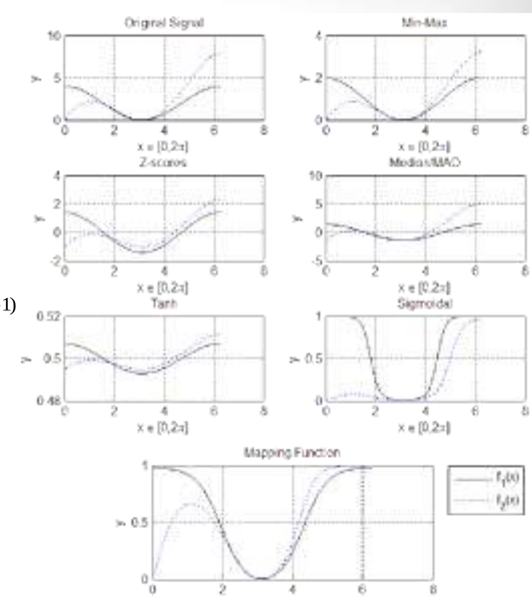
A.F.Abate, M.Nappi, D.Riccio, M.DeMarsico, Data Normalization and Fusion in Multibiometric Systems, in: International Conference on Distributed Multimedia Systems, DMS2007, 2007, pp.87–92

Summary of results with monodimensional

- Normalization techniques:
  - Min-Max
  - Z-score
  - Median/MAD
  - Tanh Estimator
  - Sigmoidale
  - QL-Sigmoidale
- Test functions

$f_1(x) = 2 \cdot \cos(x) + 1 \quad f_2(x) = 2 \cdot \log(x) \cdot (\cos(x)+1)$

- The first three do not assure a mapping of original value onto the common interval [0,1]
- Tanh and Sigmoid in (0,1) with too central values for Tanh and distortion near 0 for Sigmoi
- QL-Sigmoidal assures a commo interval [0,1] and preserves the original data distribution.



Experiments with biometric data

The used databases were:

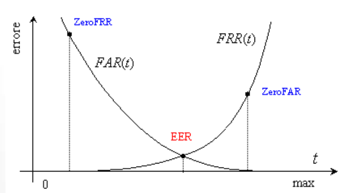
- *Face*: FERET e AR-Faces (first 100 subjects).



- *Ear*: Notre-Dame (first 100 subjects).



Performances were measured in terms of Recognition Rate and Equal Error Rate (EER).



Performance of biometric systems for different normalization functions with correct *xmax* estimation

System		Performances				
		min max	z scores	Median mad	sigmoid	**QLS**
Face	RR	93%	93%	93%	93%	**93%**
	EER	0.03	0.23	0.12	0.04	**0.03**
Ear	RR	72%	72%	72%	72%	**72%**
	EER	0.14	0.25	0.17	0.16	**0.14**
Face ⊕ *Ear*	RR	95%	93%	93%	94%	**98%**
	EER	0.018	0.23	0.11	0.02	**0.015**

Min-Max vs QLS

with a wrong estimation of the maximum face score

System		Overestimated Maximum Score		Underestimated Maximum Score	
		Min/ max	QLS	Min/ max	QLS
Face	RR	93%	93%	38%	93%
	EER	0.04	0.04	**0.81**	**0.034**
Ear	RR	72%	72%	72%	72%
	EER	0.14	0.14	0.14	0.14
Face ⊕ Ear	RR	78%	78%	81%	97%
	EER	0.08	0.08	**0.10**	**0.058**

Min-Max vs QLS

with a wrong estimation of the maximum face score

Sistema		Score Massimo sovrastimato		Score Massimo sottostimato	
		Min/ max	QLS	Min/ max	QLS
Volto	RR	93%	93%	38%	93%
	EER	0.04	0.04	**0.81**	**0.034**
Orecchio	RR	72%	72%	72%	72%
	EER	0.14	0.14	0.14	0.14
Volto ⊕ Orecchio	RR	78%	78%	81%	97%
	EER	0.08	0.08	**0.10**	**0.058**

Min-Max vs QLS

with a wrong estimation of the maximum face score

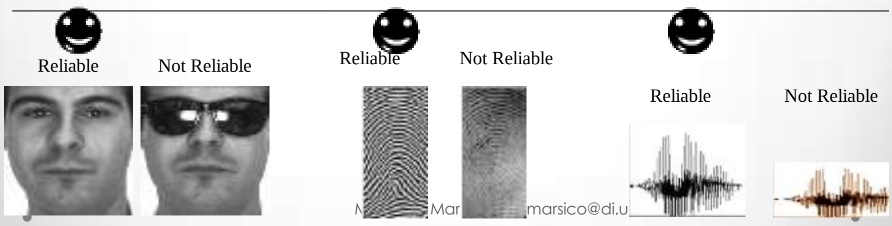
Sistema		Score Massimo sovrastimato		Score Massimo sottostimato	
		Min/max	QLS	Min/max	QLS
Volto	RR	93%	93%	38%	93%
	EER	0.04	0.04	**0.81**	**0.034**
Orecchio	RR	72%	72%	72%	72%
	EER	0.14	0.14	0.14	0.14
Volto ⊕ Orecchio	RR	78%	78%	81%	97%
	EER	0.08	0.08	**0.10**	**0.058**

Presentation Outline

- Biometric Systems
  - Short introduction
  - Multibiometric Systems
- Data Normalization
  - Existing Functions
  - Quasi Linear Sigmoid Function (QLS)
- System Response Reliability
  - Existing margin-based approaches
  - Proposed reliability indexes SRR I e SRR II
- Supervised Fusion
  - The Supervisor
  - Peformances by Supervisor
- Cross Testing Protocol
  - Architecture
  - Performances
- Introduction to Ambient Intelligence
  - Definitions and trends
  - Interacting with an intelligent ambient
- Conclusions

The reliability of identification systems

- Due to the possibly different quality of data inputted to each subsystem, and to the possibly different accuracy of exploited recognition procedures, it could happen that not all responses are equally reliable.
- The definition of a measure for the response reliability of the single subsystems would be significant for fusing the single results in an overall final response.



Some techniques (1)

- Quality based margins
- (Kryszczuk, Richiardi, Prodanov and Drygajlo):

Few samples from BANCA database

Correlation with an average face image

The quality of the training images can be modeled by creating an average face template out of all the face images whose quality is considered as reference.

Image sharpness estimation

The cross-correlation with an average image gives an estimate of the quality deterioration in the low-frequency features. At the same time that measure ignores any quality deterioration in the upper range of spatial frequencies. The absence of high-frequency image details can be described as the loss of image sharpness.

K. Kryszczuk, J. Richiardi, P. Prodanov and A. Drygajlo, "Reliability-based decision fusion in multimodal biometric verification", EURASIP Journal on Advances in Signal Processing 2006, Volume 2007 (2007), Article ID 86572, 9 pages.

Some techniques (2)

- Error estimation based margins
  (Poh and Bengio):

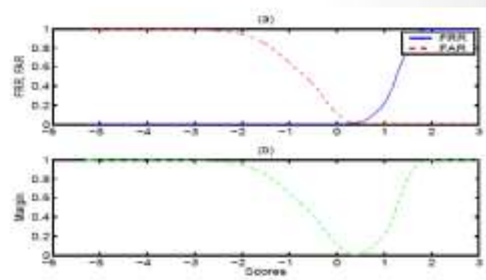
Performance of the system are measured in terms of:

$$\mathrm{FAR}(\Delta) = \frac{\text{number of FAs}(\Delta)}{\text{number of impostor accesses}},$$

$$\mathrm{FRR}(\Delta) = \frac{\text{number of FRs}(\Delta)}{\text{number of client accesses}},$$

The margin $M(\Delta)$ is defined as:

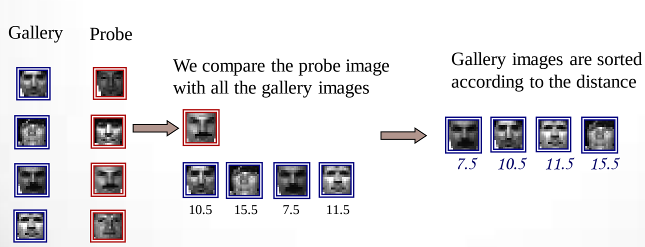
$$\mathcal{M}(\Delta) = |\mathrm{FAR}(\Delta) - \mathrm{FRR}(\Delta)|.$$



N. Poh, S. Bengio, Improving Fusion with Margin-Derived Confidence In Biometric Authentication Tasks, IDIAP-RR 04-63, November 2004.

The Identification Process

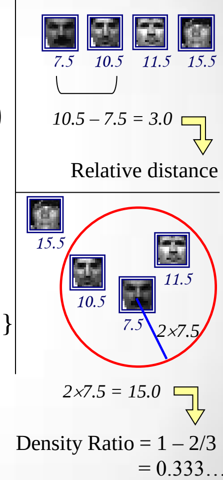
- Let A be an identification system and G its gallery of genuine subjects who were correctly enrolled.
- Assume there are at least n>0 acquisitions for each.
- Let *p* be a person to be identified.



System Response Reliability

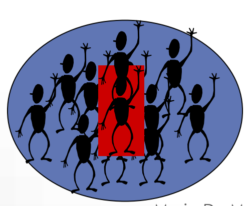
- We analysed two different measures:
  - Relative distance $\varphi(p)=\dfrac{F\left(d\left(p,g_{i_2}\right)\right)-F\left(d\left(p,g_{i_1}\right)\right)}{F\left(d\left(p,g_{i_{|G|}}\right)\right)}$
  - Density Ratio $\varphi(p)=1-|N_b|/|G|$

  where $N_b=\{g_{i_k}\in G \mid F(d(p,g_{i_k}))<2\cdot F((d(p,g_1)))\}$



System Response Reliability (SRR)

Less "crowded" cloud around the returned subject = More reliable response



More "crowded" cloud around the returned subject = Less reliable response

System Response Reliability

We need to establish a value φ_k for the reliability index separating genuine subjects from impostor ones

The optimal φ_k is given by that value able to minimize the wrong estimates of function $\varphi(p)$, i.e. impostors with $\varphi(p)$ higher than φ_k or genuine subjects with $\varphi(p)$ lower than φ_k

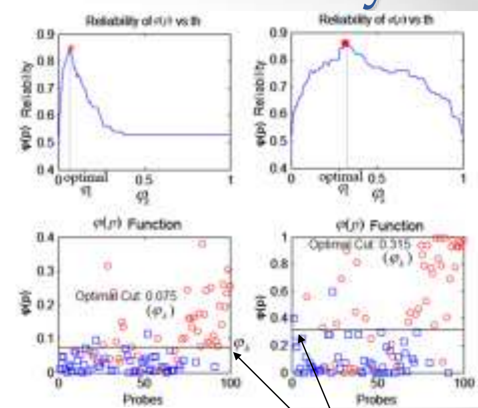
SRR gets high values both for $\varphi(p)$ much higher than φ_k (genuine subjects) and $\varphi(p)$ much lower than φ_k (impostors).

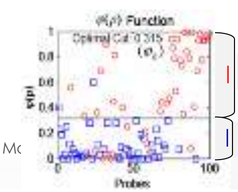
The SRR is defined as:

$$SRR = \frac{|\varphi(p) - \varphi_k|}{S(\varphi(p), \varphi_k)}$$

with

$$S(\varphi(p), \varphi_k) = \begin{cases} 1 - \varphi_k & if\ \varphi(p) > \varphi_k \\ \varphi_k & otherwise \end{cases}$$





φ_k

$S(\varphi_k)$ if $\varphi_j(p) \geq \varphi_k$

$S(\varphi_k)$ if $\varphi_j(p) < \varphi_k$

How to integrate SRR index into the fusion protocol

- Let us assume to have a system S composed by N subsystems $T_1, \ldots, T_N$, each able to produce a sorted list $T_i(1,\ldots,|G|)$ of $|G|$ subjects and a SRR value srr_i.
- In order to guarantee a consistent fusion we define
$$w_i = \frac{srr_i}{\sum_{j=1}^{N} srr_j}, \forall i$$
to assure
$$\sum_i w_i = 1$$
- A consistent threshold th is estimated for each subsystem T_i above which we can consider its

Threshold setup

- Thresholds *thi* for each subsystem are automatically estimated according to a certain number M of subsequent observations.

$$\bar{S}_i = \{srr_i^1, \ldots, srr_i^M\}$$

- The desirable characteristic for a certain *Ti* subsystem is that its vector has an high mean value (the system in generally reliable) and a low value for the variance (basically stable system).

- We can summarize this in the formula :

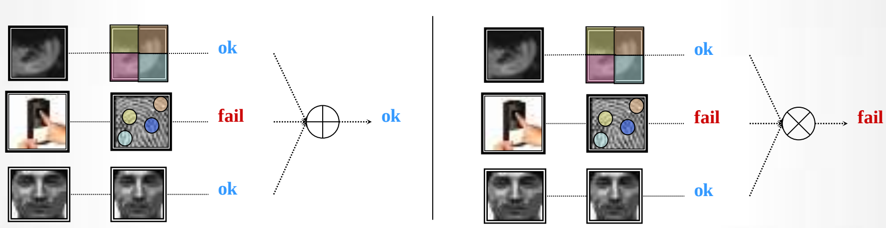
$$th_i = \left| \frac{\mathrm{E}[\bar{S}_i]^2 - \sigma[\bar{S}_i]}{\mathrm{E}[\bar{S}_i]} \right|$$

A. F.Abate, M. Nappi, D. Riccio, M. De Marsico, "Data Normalization and Fusion in Multibiometric Systems", Proceedings of The Thirteenth International Conference on Distributed Multimedia Systems DMS 2007, September 6-8 2007, San Francisco, USA, pp. 87-92

How to integrate SRR index into the fusion protocol

- The main integration policies are:

OR AND



We apply a decision fusion techniques to the set of reliability indexes associated to returned responses, before applying a further fusion technique to the actual responses.

Rule	DESCRIPTION
Or	the combined response is valid only if at least one subsystem response reliability is above the corresponding threshold; the system returns the first identity from the list of the subsystem with the higher reliability above the corresponding threshold
And	the combined response is valid only if all subsystem response reliabilities are above the corresponding thresholds; the system returns the identity with the minimum weighted sum of distances from the probe, where weights are the reliability degrees of the different subsystems

Performances of different fusion rules

Database		Statistiche				
		None	SRR I		SRR II	
		SIMPLE	OR	AND	OR	AND
Feret Fafb	RR	98%	99%	100%	96%	100%
	EER	0.028	0.016	0.003	0.015	0.000
	NRR	100	75	63	94	38
Feret Fafc	RR	55%	76%	100%	84%	-
	EER	0.167	0.153	0.002	0.117	-
	NRR	100	85	2	74	0
Feret Dup I	RR	75%	81%	100%	87%	100%
	EER	0.238	0.228	0.001	0.177	0.000
	NRR	100	91	18	84	22

Maria De Marsico - demarsico@di.uniroma1.it

Performances of different fusion rules

Database		Statistiche				
		None	SRR I		SRR II	
		SIMPLE	OR	AND	OR	AND
Feret Fafb	RR	98%	99%	100%	96%	100%
	EER	0.028	0.016	0.003	0.015	0.000
	NRR	100	75	63	94	38
Feret Fafc	RR	55%	76%	100%	84%	-
	EER	0.167	0.153	0.002	0.117	-
	NRR	100	85	2	74	0
Feret Dup I	RR	75%	81%	100%	87%	100%
	EER	0.238	0.228	0.001	0.177	0.000
	NRR	100	91	18	84	22

Maria De Marsico - demarsico@di.uniroma1.it

and SRR II

Face distortion		Performance: Face	Ear	Face ⊕ Ear	SRR I	SRR II
Left light	RR	93%	72%	RR	100%	100%
	EER	0.09	0.12	EER	0.001	0.008
				NRR	37	70
Sad	RR	100%	72%	RR	100%	100%
	EER	0.07	0.12	EER	0.005	0.002
				NRR	86	43
Scarf	RR	80%	72%	RR	100%	100%
	EER	0.17	0.12	EER	0.015	0.020
				NRR	70	70
Scream	RR	47%	72%	RR	100%	100%
	EER	0.18	0.12	EER	0.001	0.020
				NRR	23	46
Glasses	RR	90%	72%	RR	100%	100%
	EER	0.14	0.12	EER	0.016	0.010
				NRR	87	70

and SRR II

Face distortion		Performance: Face	Ear	Face ⊕ Ear	SRR I	SRR II
Left light	RR	93%	72%	RR	100%	100%
	EER	0.09	0.12	EER	0.001	0.008
				NRR	37	70
Sad	RR	100%	72%	RR	100%	100%
	EER	0.07	0.12	EER	0.005	0.002
				NRR	86	43
Scarf	RR	80%	72%	RR	100%	100%
	EER	0.17	0.12	EER	0.015	0.020
				NRR	70	70
Scream	RR	47%	72%	RR	100%	100%
	EER	0.18	0.12	EER	0.001	0.020
				NRR	23	46
Glasses	RR	90%	72%	RR	100%	100%
	EER	0.14	0.12	EER	0.016	0.010
				NRR	87	70

Maria De Marsico - de

and SRR II

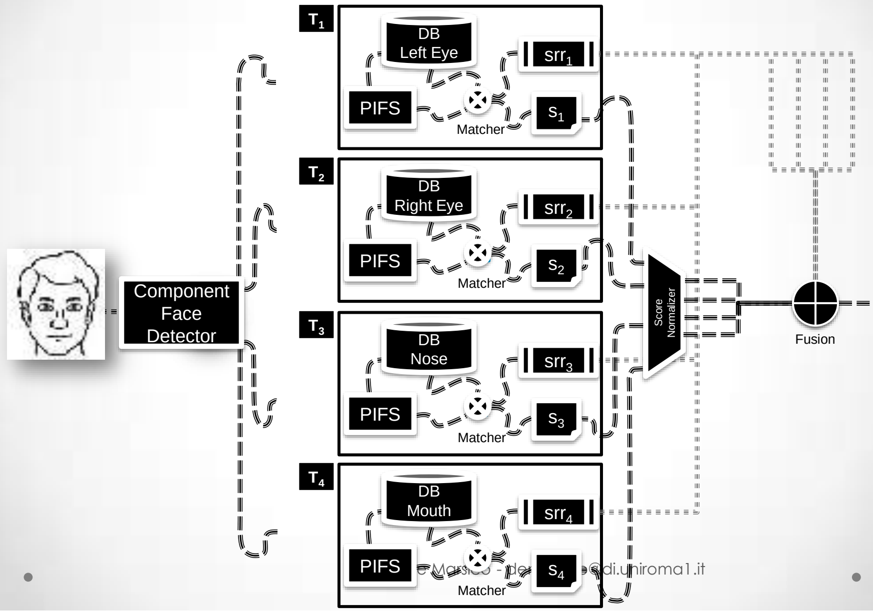
Face distortion		Performance				
		Face	Ear	Face ⊕ Ear		
					SRR I	SRR II
Left light	RR	93%	72%	RR	100%	100%
	EER	0.09	0.12	EER	0.001	0.008
				NRR	37	70
Sad	RR	100%	72%	RR	100%	100%
	EER	0.07	0.12	EER	0.005	0.002
				NRR	86	43
Scarf	RR	80%	72%	RR	100%	100%
	EER	0.17	0.12	EER	0.015	0.020
				NRR	70	70
Scream	RR	47%	72%	RR	100%	100%
	EER	0.18	0.12	EER	0.001	0.020
				NRR	23	46
Glasses	RR	90%	72%	RR	100%	100%
	EER	0.14	0.12	EER	0.016	0.010
				NRR	87	70

The novelty of our approach

- We pushed the multibiometric approach to divide the face into distinct components
- Each component is processed by a separate classifier module
- Modules are embedded in a multicomponent architecture
- Reliability measures and self-tuning policies enhance the simple result fusion

M. De Marsico, M. Nappi, D. Riccio. A Self-Tuning People Identification System from Split Face Components. Proceedings of The 3rd Pacific-Rim Symposium on Image and Video Technology, PSIVT2009, January 13th—16th, 2009, Tokyo, Japan, LNCS 5414 pp. 1-12.

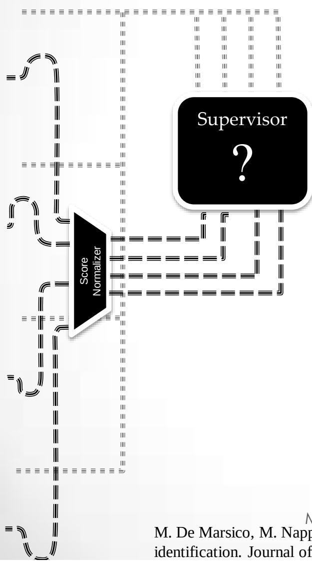
Parallel Protocol



Presentatio Outline

- Biometric Systems
  - Short introduction
  - Multibiometric Systems
- Data Normalization
  - Existing Functions
  - Quasi Linear Sigmoid Function (QLS)
- System Response Reliability
  - Existing margin-based approaches
  - Proposed reliability indexes SRR I e SRR II
- Supervised Fusion
  - The Supervisor
  - Performances by Supervisor
- Cross Testing Protocol
  - Architecture
  - Performances
- Introduction to Ambient Intelligence
  - Definitions and trends
  - Interacting with an intelligent ambient
- Conclusions

The Supervisor



Case I: an identity got more votes

T$_1$ T$_2$ T$_3$ T$_4$

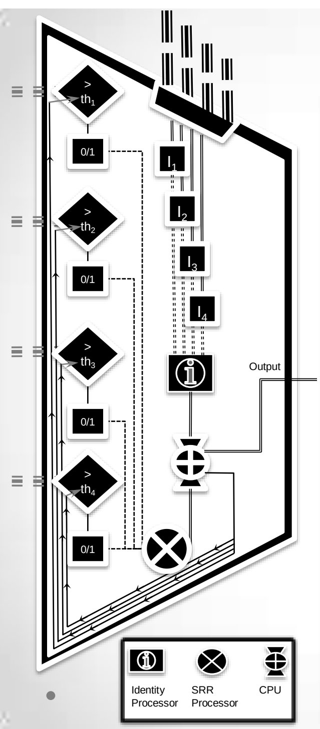
If $srr_k<th_k \Rightarrow$ decrease th_k, k={1,2,3}
If $srr_k>th_k \Rightarrow$ increase th_k, k={4}

Case II: more identities share the maximum number of votes

T$_1$ T$_2$ T$_3$ T$_4$
T$_1$ T$_2$ T$_3$ T$_4$

$\exists\, k \ni' srr_k>th_k$ with k={1,2,...}
k_{max}=argmax { srr_k | $srr_k>th_k$ }
Suppose k_{max} = 2
For k={2,4} If $srr_k<th_k \Rightarrow$ decrease th_k
For k={1,3} If $srr_k>th_k \Rightarrow$ increase th_k,
else
the response is unreliable

M. De Marsico, M. Nappi, D. Riccio, G. Tortora. A multiexpert collaborative biometric system for people identification. Journal of Visual Languages & Computing, Volume 20, Issue 2, April 2009, Pages 91-100



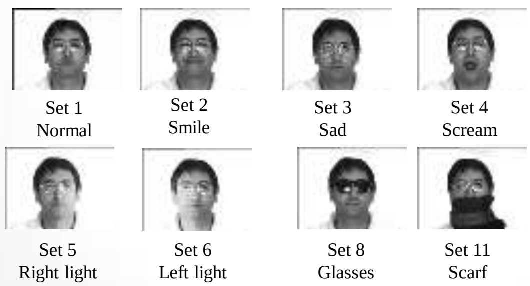
Supervisor Module in Split-Face

```
while(true)

Acquire a new face;
Split the face in 4 regions R_k;

foreach k
   u_k=0.0
   Submit R_k to the Subsystem T_k;

  if(more I_j share the same maximum number of voting T_k)
    if(SRR_k>th_k for at least one such T_k )
     Select among those I_j the one with the highest SRR_k>th_k;

     Set response as reliable;

    else Set response as unreliable;

  else if(one I_j got more votes)

     Set response as reliable;

if response is RELIABLE
     foreach T_k
       if(T_k rated the returned I_j)
          if(SRR_k<th_k)
           Set the weight u_k=-us;
       else if(SRR_k>th_k)
           Set u_k=+us;

       Update th_k = th_k + u_k;
```

Experiments with AR-Faces database

- The initial threshold configuration is $\{th_1 = 0.0, th_2 = 0.0, th_3 = 0.0, th_4 = 0.0\}$, i.e. all responses are considered as reliable at the beginning. The update step is fixed at 0.05.

- Image sets from AR-Faces database



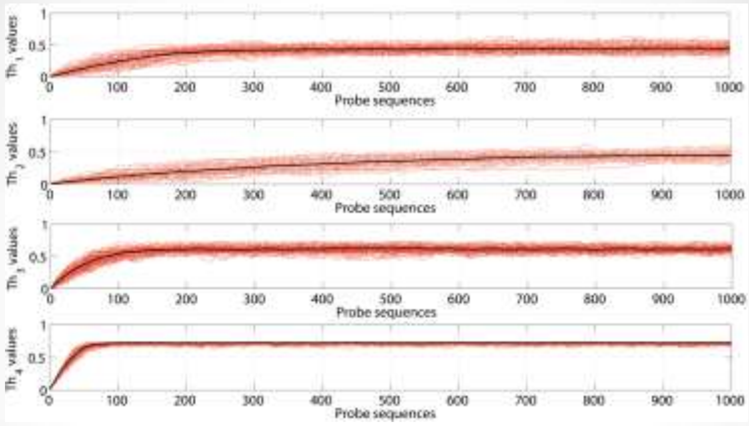
Question - 1

- Does the thresholds converge ?

  - For this experiment, set 1 is used as gallery, while *100* probe sequences are extracted from set 2, 6 and 11.

  - Each probe sequence is built by randomly extracting 1000 times one of the 126 images from the probe set.

Answer - 1

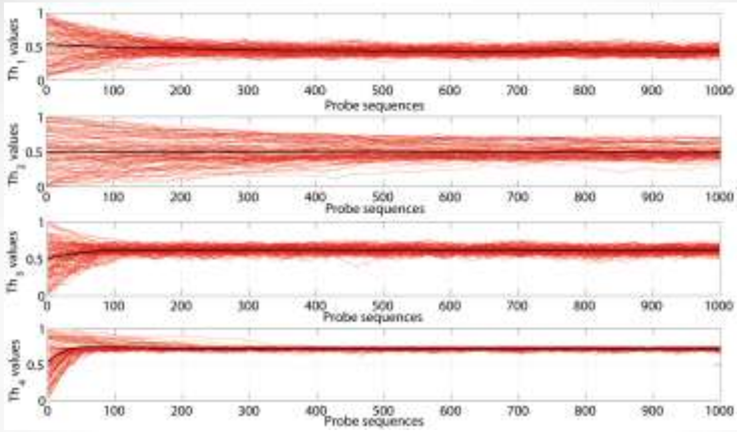


- Thresholds th_1 and th_2 (right and left eye) tend to assume lower values than th_3 and th_4 (nose and mouth). The latter values show an initial variation, and then stay constant for all the remaining part of the probe sequence. Notice the higher values for the right eye, which in *set 6* is poorly lit.
- This can be explained by observing that, since images in *set 2* belong to smiling subjects, nose and mouth show an higher variability than eyes, making the corresponding systems T_3 e T_4 less reliable, and therefore demanding higher values for the respective thresholds.
- The darker line (in black) is the mean value of the *100* computed curves and represents the mean trend for thresholds variation.

Question - 2

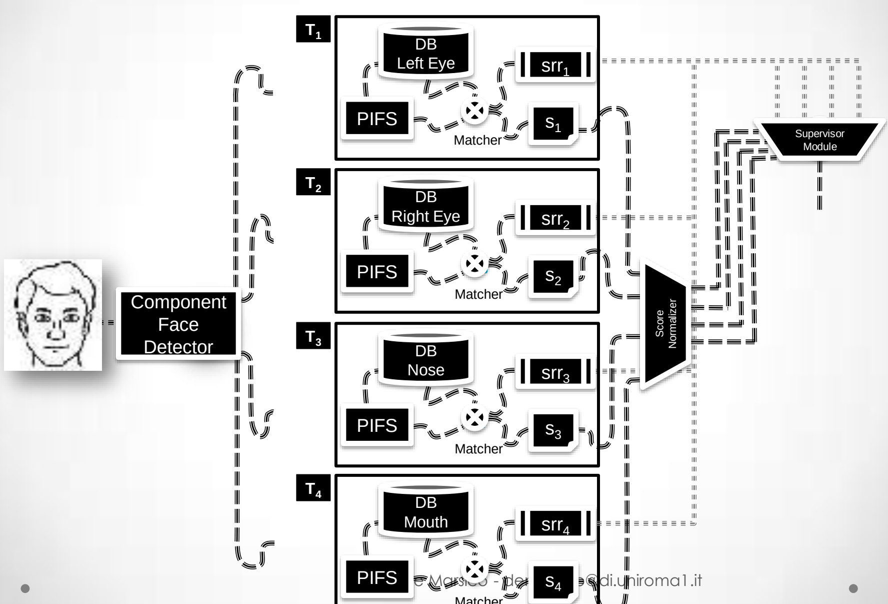
- Does the initial setting of thresholds influence the system behaviour ?
  - Even in this case, we considered 100 probe sequences of 1000 images randomly extracted among the 126 of set 2.
  - For each system run, the initial values for thresholds are randomly chosen (all values are equally probable) in the interval [0, 1]

Answer - 2



- Results on set 2 for different initial thresholds show that curves generated by the different probe sequences tend to always concentrate in a relatively small final interval. This confirms the convergence of the updating procedure.

Supervised Protocol



Experimental Results on AR-Faces (Face Database)

- In most cases, PP offers worse performances than PCBP, which is in general robust to occlusions and local distortions. Such result can be ascribed to the fact that single subsystems do not have any information about all the others.

PCBP = Plain Component Based Protocol
PP = Parallel Protocol
SP = Supervised Protocol

Sottoinsieme		Variazioni di Espressione						
		PCBP	PP	SP				
				PERF.	th_1	th_2	th_3	th_4
SET 2 SMILE	RR	0.92	0.89	0.94				
	EER	0.07	0.05	0.03	0.15	0.30	0.40	0.70
	NRR	126	38	120				
SET 3 ANGRY	RR	0.95	0.98	0.94				
	EER	0.05	0.03	0.03	0.20	0.25	0.40	0.50
	NRR	126	56	125				
SET 4 SCREAM	RR	0.48	0.36	0.76				
	EER	0.15	0.29	0.12	0.05	0.00	0.65	0.70
	NRR	126	33	50				

Experimental Results on AR-Faces (Face Database)

Sottoinsieme		VARIAZIONI DI ILLUMINAZIONE						
		PCBP	PP	SP				
				PERF.	th_1	th_2	th_3	th_4
SET 5 LEFT LIGHT	RR	0.92	1.00	0.96				
	EER	0.03	0.02	0.02	0.45	0.50	0.65	0.60
	NRR	126	30	112				
SET 6 RIGHT LIGHT	RR	0.94	0.97	0.96				
	EER	0.05	0.07	0.03	0.00	0.75	0.75	0.75
	NRR	126	37	107				

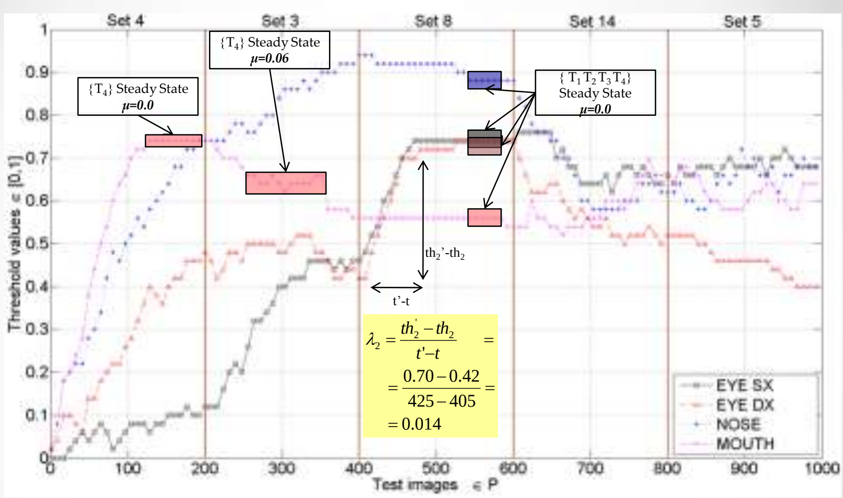
- As expected, PCBP performances are quite constantly worse than those obtained with SP.We can observe that, even when the accuracy of SP drops slightly below that of PP (sets 5 and 6), this is counterbalanced by a much higher number of reliable responses.

Experimental Results on AR-Faces (Face Database)

Sottoinsiemi		OCCLUSIONI						
		PCBP	PP	SP				
				PERF.	th_1	th_2	th_3	th_4
SET 8 SUN GLASSES	RR	0.71	0.25	0.98				
	EER	0.09	0.23	0.04	0.65	0.60	0.60	0.00
	NRR	126	20	50				
SET 11 SCARF	RR	0.85	0.61	0.92				
	EER	0.09	0.19	0.02	0.35	0.45	0.75	0.75
	NRR	126	23	115				

- The sets of equilibrium thresholds reached by the system perfectly agree with the variations introduced by the different sets of face images.
- The number of reliable responses for SP drops to 50 for sun glasses (set 8) and to 115 for scarf (set 11). This agrees with our expectations, as the distortions introduced involve a larger face area.
- However, out of a lower number of reliable responses, the system is able in both cases to guarantee a significantly higher accuracy than PCBP (RR of 0.98 versus 0.71 and of 0.92 versus 0.85) and lower EER

System Equilibrium vs. Convergence Speed



- A system equilibrium state (**steady state**) is given by the consecutive instants when threshold fluctuations are lower than a fixed μ
- Convergence speed λ_k of a subsystem T_k is defined as the ratio between the total variation of its threshold and the number of instants needed to obtain such transition.
- Total system convergence speed is defined as the minimum speed among all its subsystems, i.e. $\lambda = min_k(\lambda_k)$, $k \in \{1, 2, 3, 4\}$.

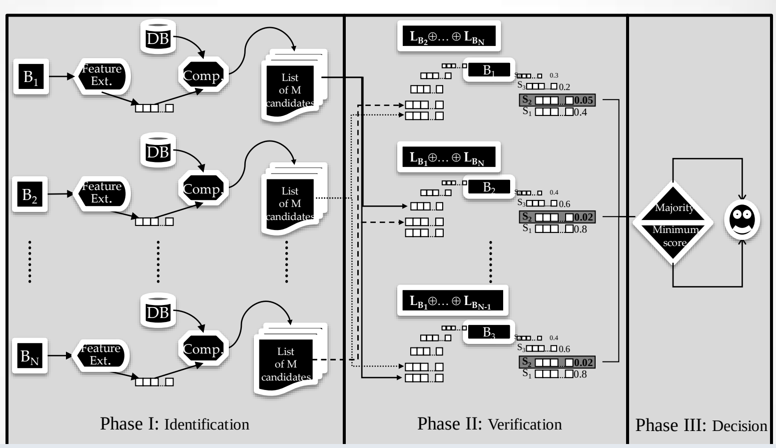
Maria De Marsico - demarsico@di.uniroma1.it

Presentation Outline

- Biometric Systems
  - Short introduction
  - Multibiometric Systems
- Data Normalization
  - Existing Functions
  - Quasi Linear Sigmoid Function (QLS)
- System Response Reliability
  - Existing margin-based approaches
  - Proposed reliability indexes SRR I e SRR II
- Supervised Fusion
  - The Supervisor
  - Performances by Supervisor
- **Cross Testing Protocol**
  - **Architecture**
  - **Performances**
- Introduction to Ambient Intelligence
  - Definitions and trends
  - Interacting with an intelligent ambient
- Conclusions

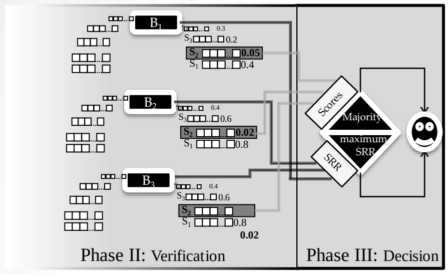
Maria De Marsico - demarsico@di.uniroma1.it

N-Cross Testing Protocol



•In this protocol, subsystems communicate by exchanging the respective score lists before returning the final response.
•Each single produced list is a merge of the received ones (does not contain the list of the returning subsystem).
•This allows each subsystem to take into account the others' results and to overcome the rigidity of traditional systems.

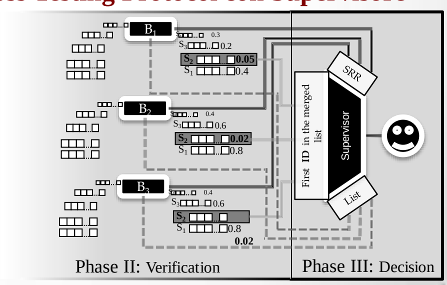
N-Cross Testing Protocol con SRR



- Only reliable subsystems send their list to the companions
- Each subsystem returns the list obtained by merging the received ones
- Single response reliability is introduced, apart from that of the returning subsystem

N-Cross Testing Protocol con Supervisore

- The Supervisor receives the lists of the different subsystems and computes both the final response and the thresholds update



Maria De Mars

N-Cross Testing Protocol - Results

DATA SETS	ARCHITECTURE								
	SIMPLE N-CROSS-TESTING			RELIABLE N-CROSS-TESTING			SUPERVISED N-CROSS-TESTING		
	RR	EER	NRR	RR	EER	NRR	RR	EER	NRR
SET 2	0.962	0.018	126	0.989	0.005	115	**0.990**	**0.004**	121
SET 3	0.971	0.014	126	0.987	0.006	96	**0.989**	**0.005**	116
SET 4	0.652	0.17	126	0.933	0.033	35	**0.962**	**0.018**	94
SET 5	0.744	0.127	126	0.925	0.037	95	**0.940**	**0.029**	118
SET 6	0.584	0.207	126	0.825	0.087	94	**0.905**	**0.047**	112
SET 8	0.522	0.238	126	0.839	0.080	65	**0.849**	**0.075**	102
SET 11	0.359	0.320	126	**0.975**	0.023	61	**0.975**	**0.012**	94

- M. De Marsico, M. Nappi, D. Riccio, G. Tortora. A multiexpert collaborative biometric system for people identification. Journal of Visual Languages & Computing, Volume 20, Issue 2, April 2009, Pages 91-100

Presentation Outline

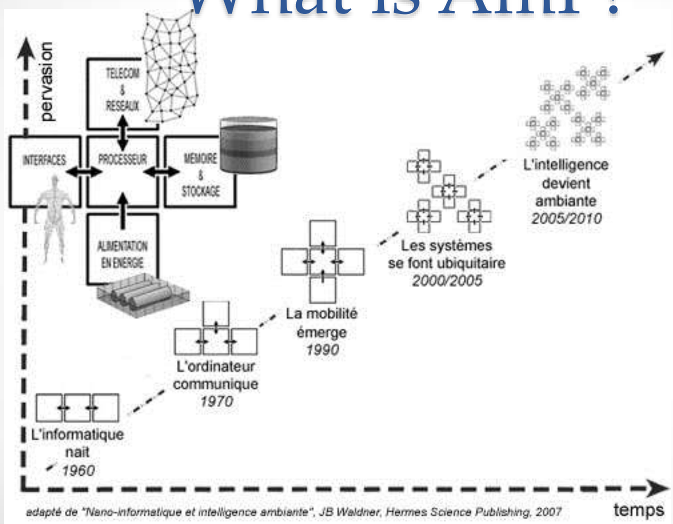
Maria De Marsico - demarsico@di.uniroma1.it

What is AmI ?

- The term Ambient Intelligence (AmI) was coined in 1998 by Eli Zelkha and Brian Epstein from Paolo Alto Ventures and refers to electronic contexts which are sensible as well as reactive to the presence of people
- It provides a futurist vision of the dvanced integration amonf electronics, telecommunications and computation, developed in the late'90 thinking of the period 2010-2020

Maria De Marsico - demarsico@di.uniroma1.it

What is AmI ?



What is AmI ?

- Within an intelligent ambient, devices work together on behalf of the users to allow performing everyday activities in a simple and natural way, by using information and intelligence which are hidden in the network connecting the devices

What is AmI ?

- It is the more human centric vision of the ubiquitous computing conceived in the early '90 by MarkWeiser
- It merges concepts and techniques from
  - natural human-computer interaction
  - autonomous and intelligent systems
- The resulting ambient is considered as a "community" of smart objects
  - which are provided with computing resources
  - which are extremely user-friendly, so that the user is surrounded by intelligent and intuitive interfaces
  - which are able to recognize and respond to the presence of different individuals in a non-intrusive and often invisible way

Maria De Marsico - demarsico@di.uniroma1.it

What is AmI ?

- As devices become smaller, more connected and more integrated in the ambient, technologgy disappears until (possibly) only the interface remains perceptible.
- Body Area Network (BAN) !

What is AmI ?

What is AmI ?

Ambient Intelligent environments combine ubiquity, awareness, intelligence and natural interaction.

- ✓ Awareness refers to the ability of the system to locate and recognize objects and people, and their intentions.
- ✓ Intelligence allows the system to analyze the context, adapt to the people that live in it, learn from their behavior, and eventually to recognize as well as show emotion.

Definition by Philips

Maria De Marsico - demarsico@di.uniroma1.it

Features of interaction in a context of AmI

Systems and technologies are:

- **embedded**: many devices are connected and integrated within the ambient
- **context aware**: such devices can **recognize** the user and the situation
- **personalized**: ambient can be **adapted** to the needs of individual users
- **adaptive**: devices can modify themselves in response to users' actions
- **anticipatory**: ambient can anticipate users' desires

Maria De Marsico - demarsico@di.uniroma1.it

What's biometries got to do with it?

- User recognition should be performed in a non-intrusive and transparent way, even (if possible) without being required by the user (if possible)
- Two strategies:
  - wireless recognition devices (e.g. RFID (Radio Frequency IDentification) tags)
  - biometric recognition
- Limits
  - devices can be lost, stolen or simply forgotten, and not be available just when they are needed
  - Biometries do not require to own or rimember anything, but each one suffers from specific limitations, due to computational complexity (fingerprints or DNA) or to sensitivity to specific ambient conditions (e.g. face recognition suffers from pose and lighting)
- Multimodal biometric systems can concurrently exploit more traits, and enhance recognition accuracy and reliability, since drawbacks of one system can be overcome by the availability of more different systems or algorithms

Presentation Outline

- Biometric Systems
  - Short introduction
  - Multibiometric Systems
- Data Normalization
  - Existing Functions
  - Quasi Linear Sigmoid Function (QLS)
- System Response Reliability
  - Existing margin-based approaches
  - Proposed reliability indexes SRR I e SRR II
- Supervised Fusion
  - The Supervisor
  - Performances by Supervisor
- Cross Testing Protocol
  - Architecture
  - Performances
- Introduction to Ambient Intelligence
  - Definitions and trends
  - Interacting with an intelligent ambient
- Conclusions

Conclusions

The design of a multibiometric system requires to consider five main aspects :

1. Choice of biometries: more biometries allow an higher accuracy but require higher costs and correlation among biometries must also be considered.
2. Choice of architecture: serial, parallel, hyerachic, N-cross testing.
3. Choice of a reliability measure : measures that are bound to input quality are complex, so that it is preferred to rely on statistics about recognition accuracy (FAR,FRR), or on gallery composition(SRR).
4. Choice of the fusion step: doing it before (feature) is better but more difficult; score level is a good compromise.
5. Choice of the fusion method: depends on architecture and e fusion step.

Conclusions

- Multimodal systems solve some problems encountered with unimodal ones; since they are more robust they lend themselves to be exploited in less controlled settings (Ambient Intelligence ?)
- However, some present limits must be considered :
  - Technological:
    - most widespread acquisition devices still present limited performances
  - Architectural:
    - subsystems do not communicate among them
    - Subsystems do not get feedback from the final response
    - (we proposed solutions for both problems!)
- We addressed some typical problems in designing multibiometric architectures, especially by implementing higher cohesion among systems and a coordinating supervisor module
- We are also using the Supervisor for Template Updating