Multimodal Interaction

Lesson 12
Multibiometric systems

Maria De Marsico
demarsico@di.uniroma1.it

Presentation Outline

• Biometric Systems
  o Short introduction
  o Multibiometric Systems

• Data Normalization
  o Existing functions
  o Quasi Linear Sigmoid Function (QLS)

• System Response Reliability
  o Existing margin-based approaches
  o Proposed reliability indexes SRR I e SRR II

• Supervised Fusion
  o The Supervisor
  o Performances by Supervisor

• Cross Testing Protocol
  o Architecture
  o Performances

• Introduction to Ambient Intelligence
  o Definitions and trends
  o 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

Hallo Grandma, do you mind if I scan your iris?
Architecture of a Biometric System

**Enrollment:**
Capture 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 system 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 matching 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

Maria De Marsico - demarsico@di.uniroma1.it
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
- **Signature biometry** – signature recognition (still and dynamic)
- **Keys typing**
- **Voice biometry** – vocal recognition
- **DNA**

Voice: Gaussian Mixture Model (GMM)

From: Dr. Andrzej Drygajlo, Biometrics for Identity Verification, 2007
Signature

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

First level
global

Second level
local

Fingerprint

First level
global

Second level
local

From: M. Nappi, Sistemi Biometrici, 2009
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)

- 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 regions, called domains, are also identified (side length = 2 side length of ranges)
PIFS: self-similarities coding

Each range is coded through the best approximating domain after a suitable affine transformation.
PIFS: self-similarities coding (range location)

- They represent a coverage of the image.

\[ I = \bigcup_i r_i \]
\[ r_i \cap r_j = \emptyset, \quad \forall i \neq j \]

This means \(2^{12}\) 8x8 ranges, on a 512x512 pixel image.

PIFS: self-similarities coding (domain location)

This means \(2^{18}\) 16x16 domain, for a 512x512 pixel image.
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 effect of partial occlusions on the face image is mitigated.

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.

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

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

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

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 ...
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.
Problems: possible wide intra-class variations

Problems: possible very small intra-class variations

Twins  Father and son

Maria De Marsico - demarsico@di.uniroma1.it
Problems: noisy and/or distorted acquisitions

- Poor quality fingerprints (e.g., heavy worker)
- Non-uniform lighting

Problems: non-universality

4% of population presents poor quality fingerprints
In some groups it is a particularly widespread characteristic (e.g., 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 individuals 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
Multimodal, multibiometric and multiexpert (or multiclassifier)

- **Multimodal:**

- **Multibiometric:**

- **Multiexpert:**

Kinds of fusion

[Aguller, J., Adapted Fusion Schemes for Multimodal Biometric Authentication, 2000]
Kinds of fusion

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

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.
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.

\[
\begin{align*}
p_{i1} &= 0.10, & r_i &= 1 \\
p_{i2} &= 0.75, & r_i &= 3 \\
p_{i3} &= 0.15, & r_i &= 2
\end{align*}
\]

• 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.

<table>
<thead>
<tr>
<th>Rank Value</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>a</td>
<td>b</td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td></td>
</tr>
<tr>
<td>a</td>
<td>c</td>
<td>d</td>
<td></td>
</tr>
</tbody>
</table>

\[
\begin{align*}
r_a &= r_{a1}^{(n)} + r_{a2}^{(n)} + r_{a3}^{(n)} = 1 + 4 + 3 = 8 \\
r_b &= r_{b1}^{(n)} + r_{b2}^{(n)} + r_{b3}^{(n)} = 3 + 4 = 10 \\
r_c &= r_{c1}^{(n)} + r_{c2}^{(n)} + r_{c3}^{(n)} = 4 + 1 + 2 = 7 \\
r_d &= r_{d1}^{(n)} + r_{d2}^{(n)} + r_{d3}^{(n)} = 2 + 2 + 1 = 5
\end{align*}
\]

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, etc.

• 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*:
  o Similarity/distance
  o Different ranges (e.g. [0,1] o [0,100])
  o 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:
  o *Robustness*: the transformation should not be influenced by outliers.
  o *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):

\[
M(\Delta) = |FAR(\Delta) - FRR(\Delta)|
\]

based on FAR e FRR estimates.

Maria De Marsico - demarsico@di.uniroma1.it

• 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.

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

• Serial combination **AND**
  global authentication requires all positive authentication 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**.
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
  o Short introduction
  o Multibiometric Systems

• Data Normalization
  o Existing Functions
  o Quasi Linear Sigmoid Function (QLS)

• System Response Reliability
  o Existing margin-based approaches
  o Proposed reliability indexes SRR I e SRR II

• Supervised Fusion
  o The Supervisor
  o Performances by Supervisor

• Cross Testing Protocol
  o Architecture
  o Performances

• Introduction to Ambient Intelligence
  o Definitions and trends
  o 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

<table>
<thead>
<tr>
<th>Method</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min/Max</td>
<td>$s'_k = \frac{s_k - \text{min}}{\text{max} - \text{min}}$</td>
</tr>
<tr>
<td>Z-score</td>
<td>$s'_k = \frac{s_k - \mu}{\sigma}$</td>
</tr>
<tr>
<td>Median/Mad</td>
<td>$s'_k = \frac{s_k - \text{median}}{\text{MAD}}$</td>
</tr>
<tr>
<td>Sigmoid</td>
<td>$s'_k = \frac{1}{1 + e^{-\alpha_k}}$</td>
</tr>
<tr>
<td>Tanh</td>
<td>$s'_k = \frac{1}{2} \left[ \tanh \left( 0.01 \left( \frac{s_k - \text{median}}{\text{MAD}} \right) \right) + 1 \right]$</td>
</tr>
</tbody>
</table>

• 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 $[0, 2\pi]$ interval.
The Min/Max Function

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

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

\[ \mu \] represents the arithmetic average of scores and \( \sigma \) 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.

\[
\text{Median/MAD} \quad s' = s_k - \text{median}_{MAD}
\]

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.
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

<table>
<thead>
<tr>
<th>Function</th>
<th>Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min/Max</td>
<td>$s'_k = \frac{s_k - \text{min}}{\text{max} - \text{min}}$</td>
</tr>
<tr>
<td>Z-score</td>
<td>$s'_k = \frac{s_k - \mu}{\sigma}$</td>
</tr>
<tr>
<td>Median/MAD</td>
<td>$s'_k = \frac{s_k - \text{median}}{\text{MAD}}$</td>
</tr>
<tr>
<td>Sigmoid</td>
<td>$s'_k = \frac{1}{1 + e^{-ks}}$</td>
</tr>
<tr>
<td>Tanh</td>
<td>$s'_k = \frac{1}{2} \tanh \left( 0.01 \frac{(s_k - \tilde{E}[s_k])}{\sigma(s_k)} \right) + 1$</td>
</tr>
</tbody>
</table>

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
  \[ f(x) = \frac{1}{1 + e^{-x}} \]
  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 \( F(x) \in [0,1) \).

\[
F(x) = \frac{k}{1 + 500 \exp(-2x)}
\]

We find the null points of the third derivative:

\[
f^3(x) = 6e^{3k^2}e^{-2x} - 6e^{2k^2}e^{-3x} + cke^{-2x}
\]

• Which are

\[
x_{max} = -\frac{1}{k} \log \left( \frac{2 - \sqrt{3}}{c} \right)
\]

• And

\[
x_{min} = -\frac{1}{k} \log \left( \frac{2 + \sqrt{3}}{c} \right)
\]

[\( x_{min}, x_{max} \)] is the range in which the sigmoidal function assumes a pseudo-linear trend.
Quasi-Linear Sigmoid (QLS)

- Knowing that \( x_{min} = 0 \) and combining the two equations we can write:
  \[ c = 2 + \sqrt{3} \]

- And
  \[ k = -\frac{1}{x_{max}} \log \left( \frac{2 - \sqrt{3}}{2 + \sqrt{3}} \right) \]

\( x_{max} \) is the only parameter we have to know.

Mapping \( f(x_{min}) \) to 0

- To map \( f(x_{min}) \) to 0 we define a new function:
  \[ g(x) = f(x) - f(x_{min}) = f(x) - f(0) \]

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

\[
F(x) = \frac{1}{L} g(x) = \frac{1 - b \frac{x}{b_{\text{max}}}}{x - a \frac{x}{a_{\text{max}}} + 1}
\]

with

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

Summary of results with monodimensional

- Normalization techniques:
  - Min-Max
  - Z-score
  - Median/MAD
  - Tanh Estimator
  - Sigmoidal
  - QL-Sigmoidal

- 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 Sigmoid
- QL-Sigmoidal assures a common 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 $x_{\text{max}}$ estimation

<table>
<thead>
<tr>
<th>System</th>
<th>Performances</th>
<th>min</th>
<th>max</th>
<th>$z$ scores</th>
<th>Median mad</th>
<th>sigmoid</th>
<th>QLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>RR</td>
<td>93%</td>
<td>93%</td>
<td>93%</td>
<td>93%</td>
<td>93%</td>
<td>93%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.03</td>
<td>0.23</td>
<td>0.12</td>
<td>0.04</td>
<td></td>
<td>0.03</td>
</tr>
<tr>
<td>Ear</td>
<td>RR</td>
<td>72%</td>
<td>72%</td>
<td>72%</td>
<td>72%</td>
<td></td>
<td>72%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.14</td>
<td>0.25</td>
<td>0.17</td>
<td>0.16</td>
<td></td>
<td>0.14</td>
</tr>
<tr>
<td>Face</td>
<td>RR</td>
<td>95%</td>
<td>93%</td>
<td>93%</td>
<td>94%</td>
<td></td>
<td>98%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.018</td>
<td>0.23</td>
<td>0.11</td>
<td>0.02</td>
<td></td>
<td>0.015</td>
</tr>
</tbody>
</table>
## Min-Max vs QLS

### with a wrong estimation of the maximum face score

<table>
<thead>
<tr>
<th>System</th>
<th>Overestimated Maximum Score</th>
<th>Underestimated Maximum Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min/max</td>
<td>QLS</td>
</tr>
<tr>
<td>Face</td>
<td>RR</td>
<td>93%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.04</td>
</tr>
<tr>
<td>Ear</td>
<td>RR</td>
<td>72%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.14</td>
</tr>
<tr>
<td>Face &amp; Ear</td>
<td>RR</td>
<td>78%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.08</td>
</tr>
</tbody>
</table>

### Min-Max vs QLS

### with a wrong estimation of the maximum face score

<table>
<thead>
<tr>
<th>Sistema</th>
<th>Score Massimo sovrastimato</th>
<th>Score Massimo sottostimato</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min/max</td>
<td>QLS</td>
</tr>
<tr>
<td>Volto</td>
<td>RR</td>
<td>93%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.04</td>
</tr>
<tr>
<td>Orecchio</td>
<td>RR</td>
<td>72%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.14</td>
</tr>
<tr>
<td>Volto &amp; Orecchio</td>
<td>RR</td>
<td>78%</td>
</tr>
<tr>
<td></td>
<td>EER</td>
<td>0.08</td>
</tr>
</tbody>
</table>
Min-Max vs QLS

with a wrong estimation of the maximum face score

<table>
<thead>
<tr>
<th>Sistema</th>
<th>Score Massimo sovrastimato</th>
<th>Score Massimo sottostimato</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min/ max</td>
<td>QLS</td>
</tr>
<tr>
<td>Volto</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RR</td>
<td>93%</td>
<td>93%</td>
</tr>
<tr>
<td>EER</td>
<td>0.04</td>
<td>0.04</td>
</tr>
<tr>
<td>Orecchio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RR</td>
<td>72%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.14</td>
<td>0.14</td>
</tr>
<tr>
<td>Volto + Orecchio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RR</td>
<td>78%</td>
<td>78%</td>
</tr>
<tr>
<td>EER</td>
<td>0.08</td>
<td>0.08</td>
</tr>
</tbody>
</table>

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
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.

![Reliable and Not Reliable responses]

Some techniques (1)

• Quality based margins

  (Kryszczuk, Richiardi, Prodanov and Drygajlo):

- 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.

Some techniques (2)

• Error estimation based margins (Poh and Bengio):

Performance of the system are measured in terms of:

\[
\text{FAR}(\Delta) = \frac{\text{number of FAR}(\Delta)}{\text{number of impostor accesses}},
\]

\[
\text{FRR}(\Delta) = \frac{\text{number of FRR}(\Delta)}{\text{number of client accesses}}.
\]

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

\[
M(\Delta) = |\text{FAR}(\Delta) - \text{FRR}(\Delta)|.
\]


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.

Gallery | Probe
---|---

We compare the probe image with all the gallery images

Gallery images are sorted according to the distance

<table>
<thead>
<tr>
<th>7.5</th>
<th>10.5</th>
<th>11.5</th>
<th>15.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5</td>
<td>15.5</td>
<td>7.5</td>
<td>11.5</td>
</tr>
</tbody>
</table>
System Response Reliability

- We analysed two different measures:
  - Relative distance \( \varphi(p) = \frac{F(d(p,g_i)) - F(d(p,g_{i0}))}{F(d(p,g_{i0}))} \)
  - Density Ratio \( \varphi(p) = 1 - \frac{|N_p|}{|G|} \)

where \( N_p = \{ g_h \in G | F(d(p,g_h)) < 2 \cdot F(d(p,g_i)) \} \)

Relative distance:

\[
\begin{align*}
7.5 & \quad 10.5 & \quad 11.5 & \quad 13.5 \\
10.5 - 7.5 & = 3.0
\end{align*}
\]

Density Ratio:

\[
2 \times 7.5 = 15.0
\]

Density Ratio = \( 1 - \frac{2}{3} = 0.333… \)

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 $\phi_k$ for the reliability index separating genuine subjects from impostor ones.

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

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

The SRR is defined as:

$$ SRR = \frac{|\phi(p) - \phi_k|}{S(\phi(p), \phi_k)} $$

with

$$ S(\phi(p), \phi_k) = \begin{cases} 1 - \phi_k & \text{if } \phi(p) > \phi_k \\ \phi_k & \text{otherwise} \end{cases} $$

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:

$$ w_j = \frac{srr_j}{\sum_i srr_i} $$

$$ \sum_j w_j = 1 $$

to assure

• A consistent threshold $th$ is estimated for each subsystem $T_i$ above which we can consider its
Threshold setup

- Thresholds \( t_i \) 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 a 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:

\[
th_i = \frac{E[\bar{S}_i]^2 - \sigma[\bar{S}_i]}{E[\bar{S}_i]}
\]


How to integrate SRR index into the fusion protocol

- The main integration policies are:

**OR**

- ok
- fail
- ok

**AND**

- ok
- fail
- ok

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.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Or</td>
<td>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</td>
</tr>
<tr>
<td>And</td>
<td>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</td>
</tr>
</tbody>
</table>
### Performances of different fusion rules

<table>
<thead>
<tr>
<th>Database</th>
<th>Feret Faflb</th>
<th>Statistichce</th>
<th>None</th>
<th>SRR I</th>
<th>SRR II</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>SIMPLE</td>
<td>OR</td>
<td>AND</td>
</tr>
<tr>
<td>RR</td>
<td>98%</td>
<td>99%</td>
<td>100%</td>
<td>96%</td>
<td>100%</td>
</tr>
<tr>
<td>EER</td>
<td>0.028</td>
<td>0.016</td>
<td>0.003</td>
<td>0.015</td>
<td>0.000</td>
</tr>
<tr>
<td>NRR</td>
<td>100</td>
<td>75</td>
<td>63</td>
<td>94</td>
<td>38</td>
</tr>
<tr>
<td>RR</td>
<td>55%</td>
<td>76%</td>
<td>100%</td>
<td>84%</td>
<td>-</td>
</tr>
<tr>
<td>EER</td>
<td>0.167</td>
<td>0.153</td>
<td>0.002</td>
<td>0.117</td>
<td>-</td>
</tr>
<tr>
<td>NRR</td>
<td>100</td>
<td>85</td>
<td>2</td>
<td>74</td>
<td>0</td>
</tr>
<tr>
<td>RR</td>
<td>75%</td>
<td>81%</td>
<td>100%</td>
<td>87%</td>
<td>100%</td>
</tr>
<tr>
<td>EER</td>
<td>0.238</td>
<td>0.228</td>
<td>0.001</td>
<td>0.177</td>
<td>0.000</td>
</tr>
<tr>
<td>NRR</td>
<td>100</td>
<td>91</td>
<td>18</td>
<td>84</td>
<td>22</td>
</tr>
</tbody>
</table>

Maria De Marsico - demarsico@di.uniroma1.it

### Performances of different fusion rules

<table>
<thead>
<tr>
<th>Database</th>
<th>Feret Faflb</th>
<th>Statistichce</th>
<th>None</th>
<th>SRR I</th>
<th>SRR II</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>SIMPLE</td>
<td>OR</td>
<td>AND</td>
</tr>
<tr>
<td>RR</td>
<td>98%</td>
<td>99%</td>
<td>100%</td>
<td>96%</td>
<td>100%</td>
</tr>
<tr>
<td>EER</td>
<td>0.028</td>
<td>0.016</td>
<td>0.003</td>
<td>0.015</td>
<td>0.000</td>
</tr>
<tr>
<td>NRR</td>
<td>100</td>
<td>75</td>
<td>63</td>
<td>94</td>
<td>38</td>
</tr>
<tr>
<td>RR</td>
<td>55%</td>
<td>76%</td>
<td>100%</td>
<td>84%</td>
<td>-</td>
</tr>
<tr>
<td>EER</td>
<td>0.167</td>
<td>0.153</td>
<td>0.002</td>
<td>0.117</td>
<td>-</td>
</tr>
<tr>
<td>NRR</td>
<td>100</td>
<td>85</td>
<td>2</td>
<td>74</td>
<td>0</td>
</tr>
<tr>
<td>RR</td>
<td>75%</td>
<td>81%</td>
<td>100%</td>
<td>87%</td>
<td>100%</td>
</tr>
<tr>
<td>EER</td>
<td>0.238</td>
<td>0.228</td>
<td>0.001</td>
<td>0.177</td>
<td>0.000</td>
</tr>
<tr>
<td>NRR</td>
<td>100</td>
<td>91</td>
<td>18</td>
<td>84</td>
<td>22</td>
</tr>
</tbody>
</table>

Maria De Marsico - demarsico@di.uniroma1.it
## Performances of SRR I and SRR II

<table>
<thead>
<tr>
<th>Face distortion</th>
<th>Performance</th>
<th>Face @ Ear</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Face</td>
<td>Ear</td>
</tr>
<tr>
<td></td>
<td>RR</td>
<td>RR</td>
</tr>
<tr>
<td><strong>Left light</strong></td>
<td>93%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.09</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>37</td>
<td>70</td>
</tr>
<tr>
<td><strong>Sad</strong></td>
<td>100%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.07</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>86</td>
<td>43</td>
</tr>
<tr>
<td><strong>Scarf</strong></td>
<td>80%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.17</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td><strong>Scream</strong></td>
<td>47%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.18</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>23</td>
<td>46</td>
</tr>
<tr>
<td><strong>Glasses</strong></td>
<td>90%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.14</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>87</td>
<td>70</td>
</tr>
</tbody>
</table>

## Performances of SRR I and SRR II

<table>
<thead>
<tr>
<th>Face distortion</th>
<th>Performance</th>
<th>Face @ Ear</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Face</td>
<td>Ear</td>
</tr>
<tr>
<td></td>
<td>RR</td>
<td>RR</td>
</tr>
<tr>
<td><strong>Left light</strong></td>
<td>93%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.09</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>37</td>
<td>70</td>
</tr>
<tr>
<td><strong>Sad</strong></td>
<td>100%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.07</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>86</td>
<td>43</td>
</tr>
<tr>
<td><strong>Scarf</strong></td>
<td>80%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.17</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td><strong>Scream</strong></td>
<td>47%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.18</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>23</td>
<td>46</td>
</tr>
<tr>
<td><strong>Glasses</strong></td>
<td>90%</td>
<td>72%</td>
</tr>
<tr>
<td>EER</td>
<td>0.14</td>
<td>0.12</td>
</tr>
<tr>
<td>NRR</td>
<td>87</td>
<td>70</td>
</tr>
</tbody>
</table>
and SRR II

<table>
<thead>
<tr>
<th>Face distortion</th>
<th>Performance</th>
<th>Face</th>
<th>Ear</th>
<th>Face @ Ear</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Face A</td>
<td>Face B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Left light</td>
<td>RR 93%</td>
<td>RR 72%</td>
<td>RR 100%</td>
<td>RR 100%</td>
</tr>
<tr>
<td></td>
<td>EER 0.09</td>
<td>EER 0.12</td>
<td>EER 0.001</td>
<td>EER 0.008</td>
</tr>
<tr>
<td></td>
<td>NRR 37</td>
<td>NRR 70</td>
<td>NRR 37</td>
<td>NRR 70</td>
</tr>
<tr>
<td>Sad</td>
<td>RR 100%</td>
<td>RR 72%</td>
<td>RR 100%</td>
<td>RR 100%</td>
</tr>
<tr>
<td></td>
<td>EER 0.07</td>
<td>EER 0.12</td>
<td>EER 0.005</td>
<td>EER 0.008</td>
</tr>
<tr>
<td></td>
<td>NRR 86</td>
<td>NRR 43</td>
<td>NRR 86</td>
<td>NRR 43</td>
</tr>
<tr>
<td>Scarf</td>
<td>RR 80%</td>
<td>RR 72%</td>
<td>RR 100%</td>
<td>RR 100%</td>
</tr>
<tr>
<td></td>
<td>EER 0.17</td>
<td>EER 0.12</td>
<td>EER 0.015</td>
<td>EER 0.020</td>
</tr>
<tr>
<td></td>
<td>NRR 70</td>
<td>NRR 70</td>
<td>NRR 70</td>
<td>NRR 70</td>
</tr>
<tr>
<td>Scream</td>
<td>RR 47%</td>
<td>RR 72%</td>
<td>RR 100%</td>
<td>RR 100%</td>
</tr>
<tr>
<td></td>
<td>EER 0.18</td>
<td>EER 0.12</td>
<td>EER 0.001</td>
<td>EER 0.020</td>
</tr>
<tr>
<td></td>
<td>NRR 23</td>
<td>NRR 46</td>
<td>NRR 23</td>
<td>NRR 46</td>
</tr>
<tr>
<td>Glasses</td>
<td>RR 90%</td>
<td>RR 72%</td>
<td>RR 100%</td>
<td>RR 100%</td>
</tr>
<tr>
<td></td>
<td>EER 0.14</td>
<td>EER 0.12</td>
<td>EER 0.016</td>
<td>EER 0.010</td>
</tr>
<tr>
<td></td>
<td>NRR 87</td>
<td>NRR 70</td>
<td>NRR 87</td>
<td>NRR 70</td>
</tr>
</tbody>
</table>

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

Parallel Protocol

Component Face Detector

| T1 | DB Left Eye | PIFS | Matcher | Srr1 |
| T2 | DB Right Eye | PIFS | Matcher | Srr2 |
| T3 | DB Nose | PIFS | Matcher | Srr3 |
| T4 | DB Mouth | PIFS | Matcher | Srr4 |

Fusion

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

Maria De Marsico - demarsico@di.uniroma1.it
The Supervisor

Case I: an identity got more votes

If \( \text{srr}_k < \text{th}_k \) \( \Rightarrow \) decrease \( \text{th}_k \), \( k = \{1, 2, 3\} \)
If \( \text{srr}_k > \text{th}_k \) \( \Rightarrow \) increase \( \text{th}_k \), \( k = \{4\} \)

Case II: more identities share the maximum number of votes

\( \exists k \) \( \exists \text{srr}_k > \text{th}_k \) with \( k = \{1, 2, \ldots\} \)
\( k_{\text{max}} = \text{argmax} \{ \text{srr}_k | \text{srr}_k > \text{th}_k \} \)

Suppose \( k_{\text{max}} = 2 \)
For \( k = \{2, 4\} \) If \( \text{srr}_k < \text{th}_k \) \( \Rightarrow \) decrease \( \text{th}_k \)
For \( k = \{1, 3\} \) If \( \text{srr}_k > \text{th}_k \) \( \Rightarrow \) increase \( \text{th}_k \),
else the response is unreliable


1 while (true)
2 .
3 .
4 Acquire a new face;
5 .
6 foreach \( k \)
7 \( u_k = 0.0 \)
8 .
9 .
10 if (more I \(_j\) share the same maximum number of voting \( T_k \))
11 .
12 if (SRR\(_k\) > \text{th}_k \text{ for at least one such } T_k \)
13 .
14 Select among those \( I \(_j\) \) the one with the highest SRR\(_k\) > \text{th}_k ;
15 .
16 .
17 Set response as reliable;
18 .
19 else Set response as unreliable;
20 .
21 else if (one \( I \(_j\) \) got more votes)
22 .
23 .
24 Set response as reliable;
25 .
26 if response is RELIABLE
27 foreach \( T_k \)
28 .
29 if (\( T_k \) rated the returned \( I \(_j\) \))
30 .
31 if (SRR\(_k\) < \text{th}_k )
32 .
33 Set the weight \( u_k = -u \);
34 .
35 else if (SRR\(_k\) > \text{th}_k )
36 .
37 Set \( u_k = +u \);
38 .
39 Update \( \text{th}_k = \text{th}_k + u \);
Experiments with AR-Faces database

- The initial threshold configuration is \( \{\theta_1 = 0.0, \theta_2 = 0.0, \theta_3 = 0.0, \theta_4 = 0.0\} \), 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

  ![Image sets from AR-Faces database](image)

  Set 1  Normal  Set 2  Smile  Set 3  Sad  Set 4  Scream
  Set 5  Right light  Set 6  Left light  Set 8  Glasses  Set 11  Scarf

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.
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 a higher variability than eyes, making the corresponding systems $T_3$ and $T_4$ 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.

**Answer - 1**

**Question - 2**

• Does the initial setting of thresholds influence the system behaviour?

  o Even in this case, we considered 100 probe sequences of 1000 images randomly extracted among the 126 of set 2.

  o For each system run, the initial values for thresholds are randomly chosen (all values are equally probable) in the interval $[0, 1]$. 

Maria De Marsico - demarsico@di.uniroma1.it
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.
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.

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.
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 $\mu$.

Convergence speed $\lambda_k$ 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. $\Xi = \min_k(\lambda_k), \ k \in \{1, 2, 3, 4\}$. 

### Table: OCCLUSIONI

<table>
<thead>
<tr>
<th></th>
<th>PCBP</th>
<th>PP</th>
<th>PERF.</th>
<th>SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SET 8 SUN GLASSES</td>
<td>RR 0.71</td>
<td>0.25</td>
<td>0.98</td>
<td>th_1</td>
</tr>
<tr>
<td></td>
<td>EER 0.09</td>
<td>0.23</td>
<td>0.04</td>
<td>th_2</td>
</tr>
<tr>
<td></td>
<td>NRR 126</td>
<td>20</td>
<td>50</td>
<td>th_3</td>
</tr>
<tr>
<td>SET 11 SCARF</td>
<td>RR 0.85</td>
<td>0.61</td>
<td>0.92</td>
<td>th_4</td>
</tr>
<tr>
<td></td>
<td>EER 0.09</td>
<td>0.19</td>
<td>0.02</td>
<td>th_2</td>
</tr>
<tr>
<td></td>
<td>NRR 126</td>
<td>23</td>
<td>115</td>
<td>th_3</td>
</tr>
</tbody>
</table>
Presentation Outline

• Biometric Systems
  o Short introduction
  o Multibiometric Systems

• Data Normalization
  o Existing Functions
    o Quasi Linear Sigmoid Function (QLS)
  o System Response Reliability
    o Existing margin-based approaches
    o Proposed reliability indexes SRR I e SRR II

• Supervised Fusion
  o The Supervisor
  o Performances by Supervisor

• Cross Testing Protocol
  o Architecture
  o Performances

• Introduction to Ambient Intelligence
  o Definitions and trends
  o 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

N-Cross Testing Protocol - Results

<table>
<thead>
<tr>
<th>DATA SETS</th>
<th>SIMPLE N-CROSS-TESTING</th>
<th>RELIABLE N-CROSS-TESTING</th>
<th>SUPERVISED N-CROSS-TESTING</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RR</td>
<td>EER</td>
<td>NRR</td>
</tr>
<tr>
<td>SET 2</td>
<td>0.962</td>
<td>0.018</td>
<td>126</td>
</tr>
<tr>
<td>SET 3</td>
<td>0.971</td>
<td>0.014</td>
<td>126</td>
</tr>
<tr>
<td>SET 4</td>
<td>0.652</td>
<td>0.17</td>
<td>126</td>
</tr>
<tr>
<td>SET 5</td>
<td>0.744</td>
<td>0.127</td>
<td>126</td>
</tr>
<tr>
<td>SET 6</td>
<td>0.584</td>
<td>0.207</td>
<td>126</td>
</tr>
<tr>
<td>SET 8</td>
<td>0.522</td>
<td>0.238</td>
<td>126</td>
</tr>
<tr>
<td>SET 11</td>
<td>0.359</td>
<td>0.320</td>
<td>126</td>
</tr>
</tbody>
</table>

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**

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 advanced integration among electronics, telecommunications and computation, developed in the late '90 thinking of the period 2010-2020
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 Mark Weiser

- 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
What is AmI?

• As devices become smaller, more connected and more integrated in the ambient, technology disappears until (possibly) only the interface remains perceptible.

• Body Area Network (BAN)!
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.

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 remember 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:

- **Choice of biometries**: more biometries allow an higher accuracy but require higher costs and correlation among biometries must also be considered.
- **Choice of architecture**: serial, parallel, hyerachic, N-cross testing.
- **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).
- **Choice of the fusion step**: doing it before (feature) is better but more difficult; score level is a good compromise.
- **Choice of the fusion method**: depends on architecture and 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