Sistemi multi-biometrici

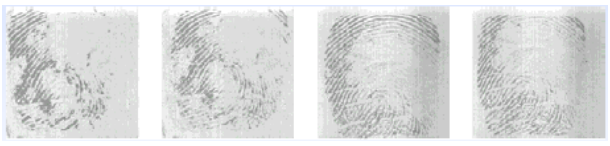
Dario Maio
dario.maio@unibo.it

Annalisa Franco
annalisa.franco@unibo.it

Limitazioni dei sistemi mono-modali

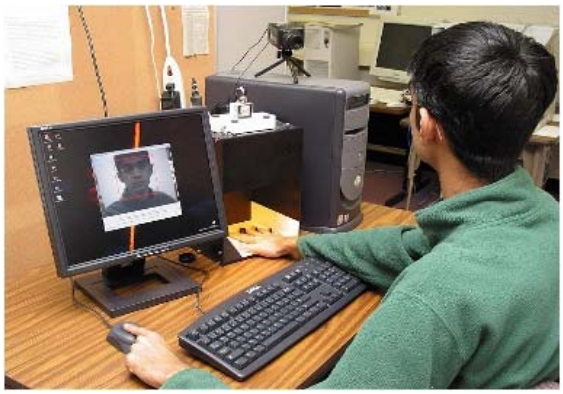
- Rumore nei dati acquisiti dovuto al sensore o a condizioni ambientali o fisiologiche sfavorevoli.
- Variazioni intra-classe.
- Grado di individualità: il contenuto della rappresentazione biometrica è limitato e alcune caratteristiche presentano un grado di individualità più basso rispetto ad altre.
- Non universalità: talvolta risulta difficoltoso acquisire il dato biometrico (Failure To Enroll). Ad es. il 4% delle impronte ha una qualità intrinseca troppo bassa.
- Attacchi e contraffazioni: tentativi di ingannare il sistema presentando caratteristiche biometriche false.



I sistemi multi-biometrici

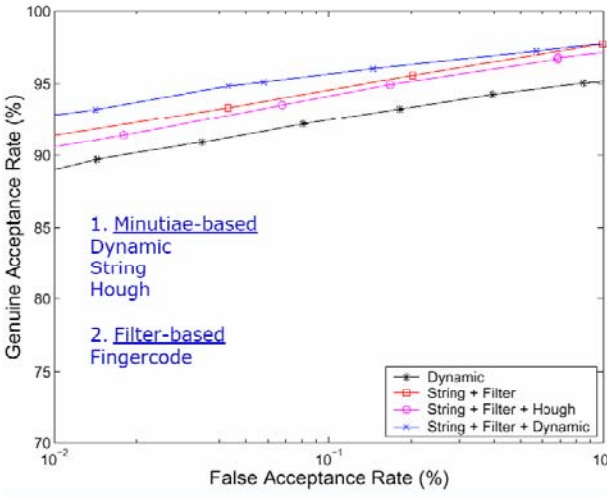
- Sistemi che integrano più sorgenti di dati biometrici al fine di migliorare le prestazioni di riconoscimento.
  - Aumentano la copertura della popolazione, riducendo i casi di failure to enroll.
  - Risultano più robusti rispetto a tentativi di frode poiché è più difficile contraffare più caratteristiche biometriche contemporaneamente.

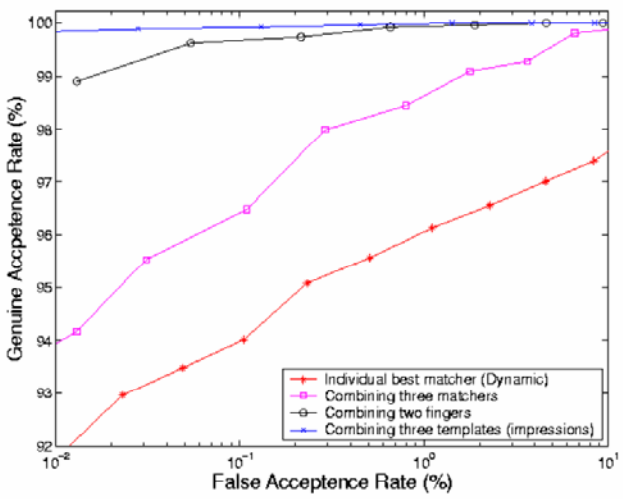


Possibili architetture: multi…

Esempio

Combinazione di più algoritmi di matching di impronte





Tecniche di fusione

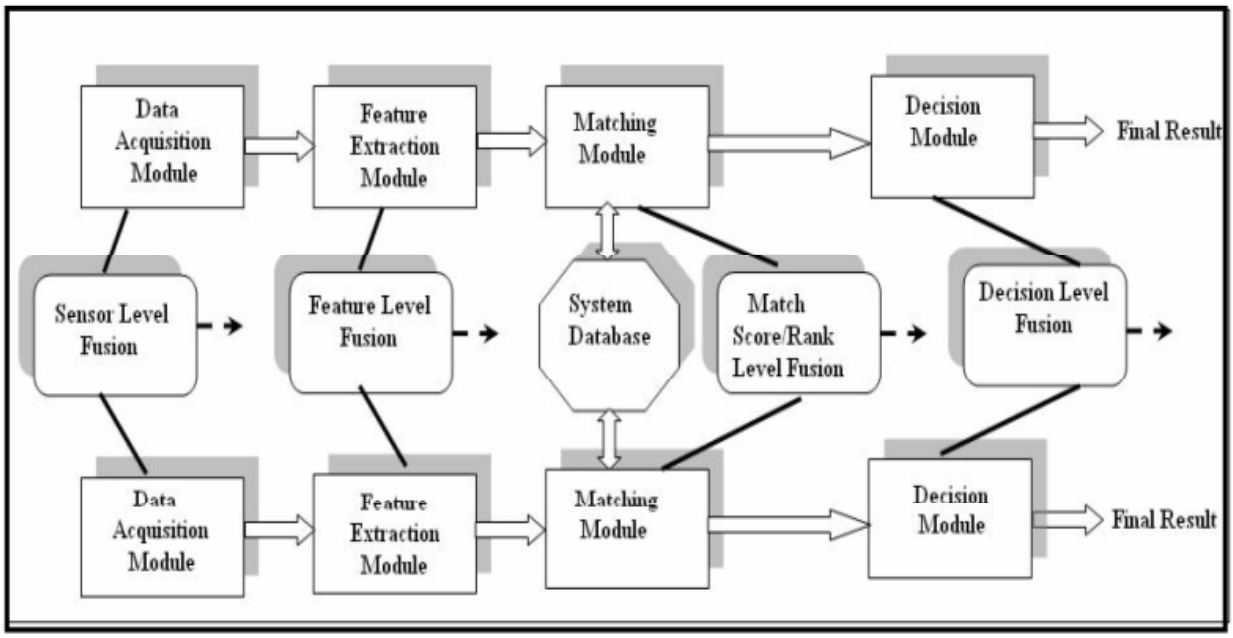
Fusione prima del matching

- Fusione a livello di sensore
  - I dati acquisiti da sensori diversi possono essere elaborati e integrati per generare nuovi dati dai quali si estraggono poi le feature.
    - Per esempio, nel caso di riconoscimento del volto, si possono fondere le informazioni 2D (tessitura) e quelle 3D (range image), ottenute usando sensori diversi, per generare un modello 3D completo.
- Fusione a livello di feature
  - Le feature estratte con tecniche diverse possono essere fuse per creare un nuovo vettore di feature rappresentativo dell'individuo.
    - Le caratteristiche geometriche della mano, per esempio, possono essere abbinate alle feature estratte dal volto usando il metodo Eigenface, ottenendo così un vettore unico. Si possono poi eventualmente applicare tecniche di selezione delle feature per ridurre la dimensionalità del vettore, mantenendo solo le informazioni più significative.

Fusione dopo il matching

- ***Fusione a livello di score***
  - Algoritmi di matching diversi restituiscono un insieme di score che vengono poi fusi per generare un unico score finale.
    - Ad esempio gli score ottenuti dal matching dell'impronta e del volto possono essere combinati usando la regola della somma per ottenere un singolo score complessivo.
- ***Fusione a livello di rank***
  - Questo tipo di fusione è utile in sistemi di identificazione; in questo caso diversi classificatori forniscono un ranking (ordinamento) delle classi (rank elevato indica un buon match).
  - I rank dei diversi classificatori sono unificati per ottenere una "classifica finale" utile per la decisione sull'identità della persona (es. Borda count).
- ***Fusione a livello di decisione***
  - Ogni classificatore restituisce in output la propria decisione (accept/reject in caso di verifica o l'identità in caso di identificazione). La decisione finale è presa combinando le singole decisioni a seconda di una regola (es. maggioranza dei voti).

Livelli di fusione



Fusione a livello di decisione e di rank

Ogni classificatore fornisce in output la propria decisione che consiste della *classe* cui ha assegnato il pattern e opzionalmente del *livello di confidenza* della classificazione eseguita (*ovvero di quanto il classificatore si sente sicuro della decisione presa).* Le decisioni possono essere tra loro combinate in diversi modi:

- ***Majority vote rule:***
  - *ogni classificatore vota per una classe*, il pattern viene assegnato alla classe maggiormente votata. Inoltre l'affidabilità del multi-classificatore può essere calcolata mediando le singole confidenze.
- ***Borda count:***
  - *ogni classificatore produce una classifica* o ranking delle classi (dalla prima all'ultima) a seconda della probabilità che il pattern appartenga a ciascuna di esse. I ranking sono poi convertiti in punteggi che sono tra loro sommati; la classe con il più elevato punteggio finale è quella scelta dal multi-classificatore.

Fusione a livello di score: tecniche (1)

Transformation-based score fusion

- Gli score sono dapprima *normalizzati* (trasformati) in un dominio comune e poi *fusi* usando una delle possibili regole (somma, max, min, avg, ecc.).

Classifier-based score fusion

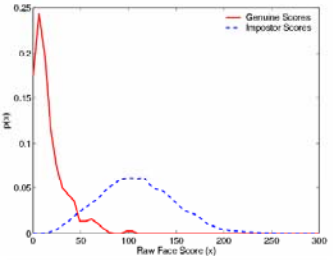
- Gli score ottenuti dai vari classificatori sono considerati *feature* e inseriti in un feature vector. Si addestra un *classificatore* in grado di discriminare gli score genuine e impostor. È necessario fare attenzione ad alcuni fattori che possono influire sull'efficacia della fusione:
  - Training set non bilanciato: se il numero di score genuine è molto inferiore rispetto al numero di score impostor, il classificatore non può essere addestrato in modo ottimale.
  - Costo di errata classificazione: la gravità di una falsa accettazione dipende strettamente dal tipo di applicazione e deve avere generalmente un peso diverso rispetto alle false reiezioni.
  - Scelta del classificatore.

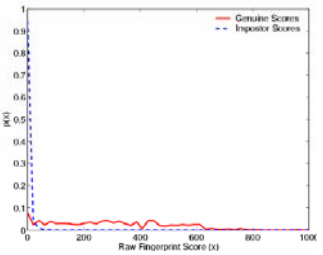
Density-based score fusion

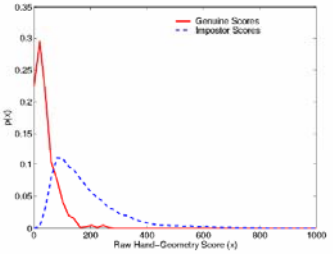
- Questo approccio si basa sul *likelihood ratio test* e richiede la stima esplicita della densità degli score genuine e impostor. Se la stima della densità è sufficientemente accurata, questo approccio permette di raggiungere prestazioni ottimali in corrispondenza di qualsiasi condizione operativa (FAR).

Transformation-based score fusion (1)

- Gli score restituiti dai diversi matcher tipicamente *non* sono *omogenei*:
  - Similarità/distanze
  - Range diversi (es. [0,1] o [0,100])
  - Distribuzioni diverse
- Per facilitare la fusione a livello di score si può:
  - Modificare i parametri che controllano la posizione e la scala della *distribuzione degli score* per i singoli matcher.
  - Applicare delle trasformazioni (*normalizzazione*) agli score, ponendo particolare attenzione a quelli che si trovano nella regione di sovrapposizione tra genuine e impostor.
- Fattori da considerare:
  - *Robustezza*: la trasformazione non dovrebbe essere influenzata dalla presenza di outlier.
  - *Efficacia*: i parametri stimati per la distribuzione degli score devono approssimare al meglio i valori reali.







Transformation-based score fusion: tecniche di normalizzazione

- **MIN-MAX:** dati gli score $\{s_k\}$, k=1,2,..,n gli score normalizzati sono:

$$s' = \frac{s - \min\{s_k\}}{\max\{s_k\} - \min\{s_k\}}$$

- **DECIMAL SCALING:** usata quando gli score dei diversi matcher differiscono di un fattore logaritmico (es. range [0,1] e [0,1000]):

$$s' = \frac{s}{10^n}, \quad n = \log_{10} \max\{s_k\}$$

- **Z-SCORE:**

$$s' = \frac{s - \mu}{\sigma}$$

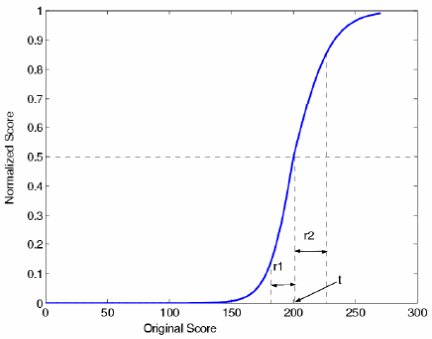
- **MEDIAN E MEDIAN ABSOLUTE DEVIATION (MAD):**

$$s' = \frac{s - median}{MAD} \qquad MAD = median(|\{s_k\} - median|)$$

Transformation-based score fusion: tecniche di normalizzazione

- **DOUBLE SIGMOID FUNCTION:**

$$s' = \frac{1}{1 + \exp\left(-2\left(\frac{s-t}{r}\right)\right)} \quad \text{dove} \quad \begin{matrix} r = r_1 \text{ se } s < t \\ r = r_2 \text{ altrimenti} \end{matrix}$$



- **TANH ESTIMATOR:**

$$s' = 0.5\left[\tanh\left(0.01\frac{(s - \mu_{GH})}{\sigma_{GH}}\right) + 1\right]$$

dove μ_{GH} e σ_{GH} rappresentano rispettivamente la media e la deviazione standard della distribuzione degli score stimata con lo stimatore di Hampel (*Hampel et al., Robust Statistics: The Approach Based on Influence Functions, 1986*).

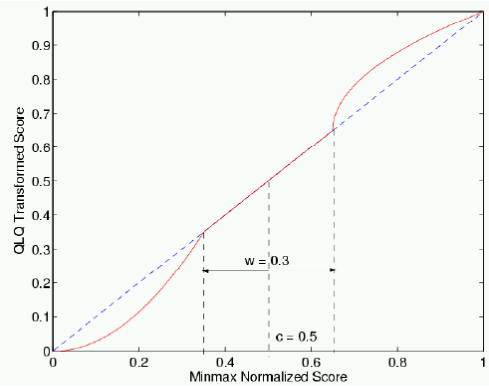
Transformation-based score fusion: regione di sovrapposizione

- **TRASFORMAZIONE QLQ:**

$$n_{QLQ} = \begin{cases} \dfrac{1}{\left(c-\frac{w}{2}\right)} n_{MM}^2 & \text{se } n_{MM} \le \left(c-\frac{w}{2}\right) \\ n_{MM} & \text{se } \left(c-\frac{w}{2}\right) \le n_{MM} \le \left(c+\frac{w}{2}\right) \\ \left(c+\frac{w}{2}\right) + \sqrt{\left(1-c-\frac{w}{2}\right)\left(n_{MM}-c-\frac{w}{2}\right)} & \text{altrimenti} \end{cases}$$

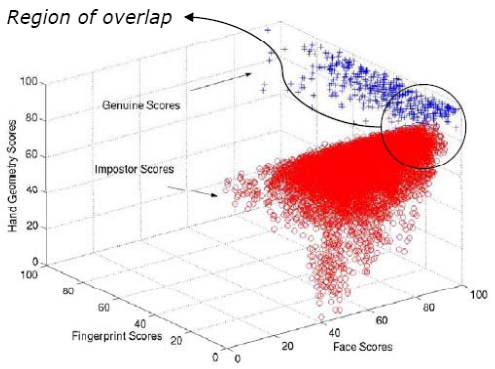
dove:

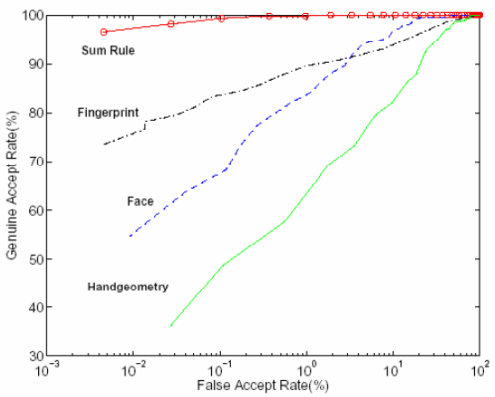
- n_{MM} è lo score normalizzato con la tecnica MIN-MAX
- c è il centro della regione di sovrapposizione
- w è la larghezza della regione di sovrapposizione



Transformation-based score fusion: metodi di fusione

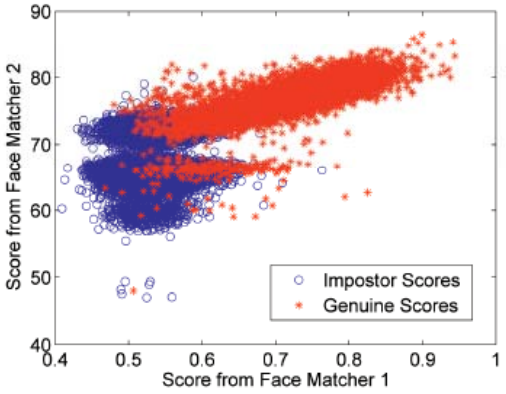
- Ogni singolo classificatore fornisce in output la *confidenza di classificazione* del pattern rispetto a ciascuna delle classi, ovvero un vettore in cui l'i-esimo elemento indica la probabilità di appartenenza del pattern alla classe i-esima. Diversi metodi di fusione sono possibili tra cui (somma, media, prodotto, max, min).
- Il ***metodo della somma*** è uno dei più noti e utilizzati per la sua robustezza. Il metodo prevede di eseguire la somma dei diversi vettori confidenza, e di classificare il pattern sulla base dell'elemento maggiore.





Density-based score fusion (1)

- Sia $\boldsymbol{X}=[X_1, X_2,\ldots, X_K]$ il vettore di matching score di K matcher diversi.
- Indichiamo con $\boldsymbol{f_{gen}(x)}$ e $\boldsymbol{f_{imp}(x)}$ le funzioni di densità congiunta dei K score per le classi genuine e impostor rispettivamante.



Supponiamo di dover assegnare un vettore di score $\boldsymbol{X}$ alla classe genuine o impostor.
Sia Ψ un test statistico per testare l'ipotesi H_0: *lo score s corrisponde a un impostor*, contro l'ipotesi H_1 *lo score s corrisponde a un genuine*. La probabilità di rigettare H_0 quando H_0 è vera corrisponde al *False Acceptance Rate*, mentre la probabilità di rigettare correttamente H_0 quando H_1 è vera corrisponde al *Genuine Acceptance Rate*.

Density-based score fusion (2)

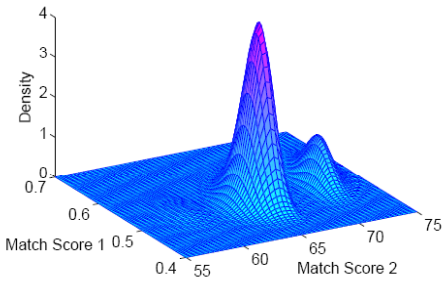
- Il teorema di Neyman-Pearson afferma che
  1. Per testare H_0 contro H_1 esiste un test Ψ e una costante η tale che:

$$(1)\ P(\Psi(X)=1|H_0)=\alpha \quad \text{e} \quad (2)\ \Psi(x)=\begin{cases} 1, \text{ quando } \dfrac{f_{gen}(x)}{f_{imp}(x)} \geq \eta \\ 0, \text{ quando } \dfrac{f_{gen}(x)}{f_{imp}(x)} < \eta \end{cases}$$

  2. Se un test soddisfa entrambe le condizioni per qualche η, allora è il test più potente per testare H_0 contro H_1 a livello α.
- In base a questo teorema, dato il False Acceptance Rate (FAR) α, il test ottimale per decidere se uno score s è genuine o impostor è dato dal *likelihood ratio* (2). *Per un fissato FAR, è possibile selezionare una soglia η tale che il test massimizza il genuine acceptance rate*.
- L'ottimalità del test è garantita solo quando le densità degli score genuine e impostor sono note. In pratica esse devono essere stimate a partire dagli score ottenuti su un training set, e l'accuratezza del test dipende dalla correttezza di tale stima…

Density-based score fusion (3)

- Alcuni studi hanno mostrato che il Gaussian Mixture Model (GMM) fornisce una buona approssimazione della densità di probabilità degli score genuine e impostor se il training set contiene un numero sufficiente di esempi.



- Sia $\phi^K(x;\mu,\Sigma)$ una densità gaussiana k-variata con vettore medio μ e matrice di covarianza Σ:

$$\phi^K(x;\mu,\Sigma)=(2\pi)^{-K/2}|\Sigma|^{-1/2}\exp\left(-\frac{1}{2}(x-\mu)^T\Sigma^{-1}(x-\mu)\right)$$

- Le stime di $f_{gen}(s)$ e $f_{imp}(s)$ si ottengono come:

$$\hat{f}_{gen}(x)=\sum_{j=1}^{M_{gen}} p_{gen,j}\phi^K\left(x;\mu_{gen,j},\Sigma_{gen,j}\right) \qquad \hat{f}_{imp}(x)=\sum_{j=1}^{M_{imp}} p_{imp,j}\phi^K\left(x;\mu_{imp,j},\Sigma_{imp,j}\right)$$

- Uno dei problemi principali consiste nel fissare il giusto numero di componenti M.

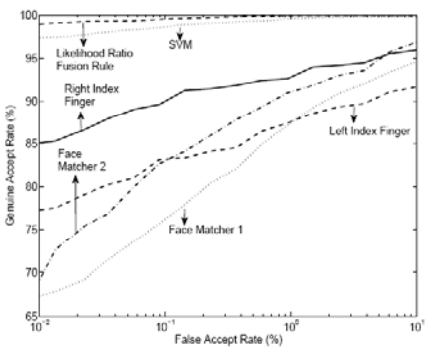
Density-based score fusion (4)

- La regola di fusione basata su ***likelihood ratio*** si definisce come segue: dato un vettore di K matching score $\boldsymbol{x}=[x_1,\ldots,x_K]$ e le densità stimate $\hat{f}_{gen}(x)$ e $\hat{f}_{imp}(x)$, calcolare il *likelihood ratio*:

$$LR(x)=\frac{\hat{f}_{gen}(x)}{\hat{f}_{imp}(x)}$$

Assegnare $\boldsymbol{x}$ alla classe genuine se $LR(x)\geq\eta$ dove η è la soglia decisionale determinata sulla base di un prefissato FAR.

SVM con kernel lineare



SVM con kernel RBF