Progettazione, Valutazione e Comparazione di sistemi biometrici

Parte XI

Indice

Capitolo 1

Valutazione di un sistema biometrico

1.1 Technology, Scenario, Operational

Un sistema biometrico può essere valutato secondo tre aspetti:

- **Technology**
  - vengono fatti test algoritmici su DB di sample
- **Scenario**
  - viene controllato il sistema biometrico in un ambiente che simula l'applicazione; si testano diverse combinazioni di sensori e algoritmi, con l'obiettivo di trovare quella migliore per il sistema finale
- **Operational**
  - simile a quella precedente, ma con uno specifico algoritmo o applicazione, sul luogo esatto e con gli utenti finali; si ottengono i risultati più vicini a quelli che compariranno nella applicazione finale

Ogni valutazione ha le sue regole e i suoi parametri da seguire; quando si compara un sistema biometrico è bene avere informazioni da tutte e 3 i tipi di valutazioni.

1.2 Quale valutazione usare?

- Durante le fasi di sviluppo di algoritmi/sistemi, di solito si impiegano i test **tecnologici**
- in fase di valutazione su **scenario** la popolazione è chiusa e limitata, quindi la veridicità statistica dei dati può essere compromessa

1.3 Intervallo di confidenza dei parametri

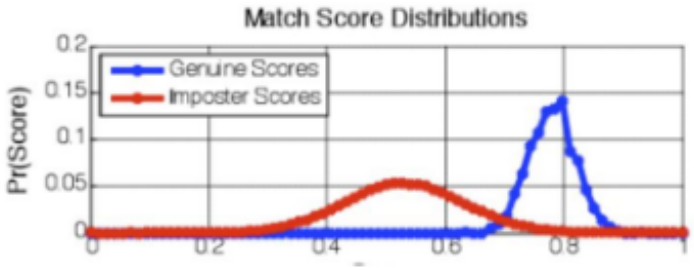
- I tassi di errore non significano quasi nulla se non è possibile **associare ad ogni misura il suo intervallo di confidenza**
- Gli intervalli di confidenza solitamente vengono costruiti da **un modello statistico che descrive al meglio possibile l'esperimento**

Capitolo 2

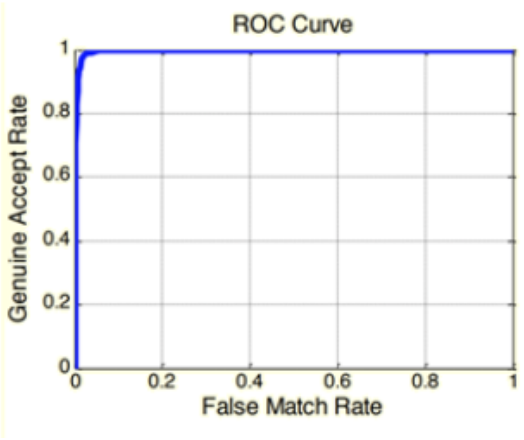
Comparazione di sistemi biometrici

L'ideale è avere, oltre ai numeri puri come EER, FTE, FTM, ..., i tre grafici di:

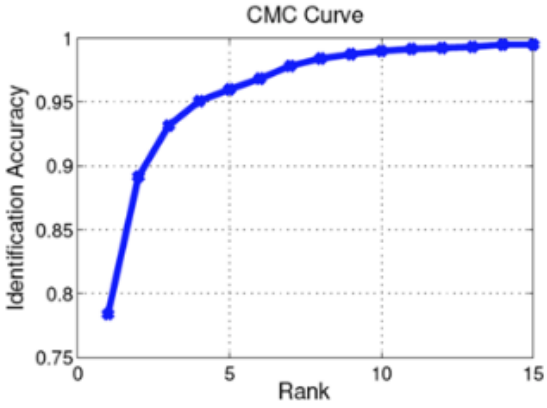
- Distribuzioni



- DET/ROC



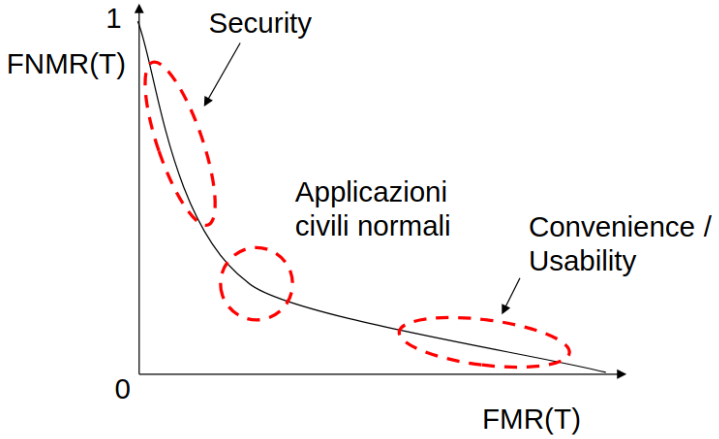
- CMC



2.1 Indici aggiuntivi: security, convenience

Le zone della curva DET:

- basso FMR → zona di security
- basso FNMR → zona di convenience



- Nelle zone di **sicurezza** c'è una bassa probabilità che un utente non abilitato possa entrare in un area riservata; potremo avere un più alto tasso di utenti abilitati che non entrano al primo tentativo, ma che dovranno mostrare il loro tratto biometrico al sensore più volte per entrare
  - *accesso a struttura critica*
- Nelle zone di **convenienza** il sistema tende a non far perdere tempo agli utenti abilitati, in quanto con bassa probabilità un utente abilitato non passerà al primo tentativo; avremo un tasso leggermente più alto di utenti non abilitati che entreranno nell'area controllata
  - *tornello della metropolitana*

Capitolo 3

Standard per la biometria

3.1 Standard ISO

Si occupa dell'interscambio dei dati biometrici fra istituzioni e aziende.

3.2 Standard BioAPI

È uno standard *informale* che già dal 2000 contiene le **specifiche di interazione dei moduli componenti il sistema biometrico**.
Fornisce un modello di autenticazione ad alto livello per ogni tecnologia biometrica disponibile sul mercato.
Inlcude le specifiche di funzionalità di:

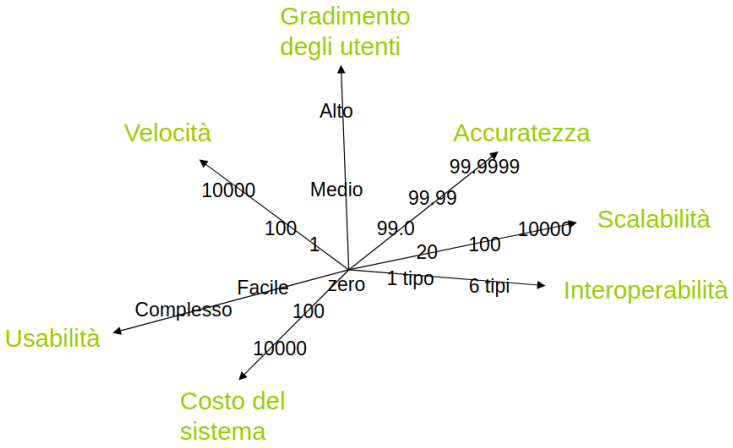
- Enrollment
- Verification
- Identification

e delle interfacce con i DB in modo tale da permettere al *Biometric Service Provider (BSP)* di gestire template nel DB in modo ottimale.
Fornisce anche primitive per permettere alla applicazione di gestire l'acquisizione dei campioni anche su **sistemi distribuiti**, con l'acquisizione su un modulo *client* ed invece enrollment, verification e identification su un modulo *server*.

Capitolo 4

Progettazione di un sistema monomodale

È un problema molto complesso, ci sono molti parametri di giudizio difficilmente stimabili.

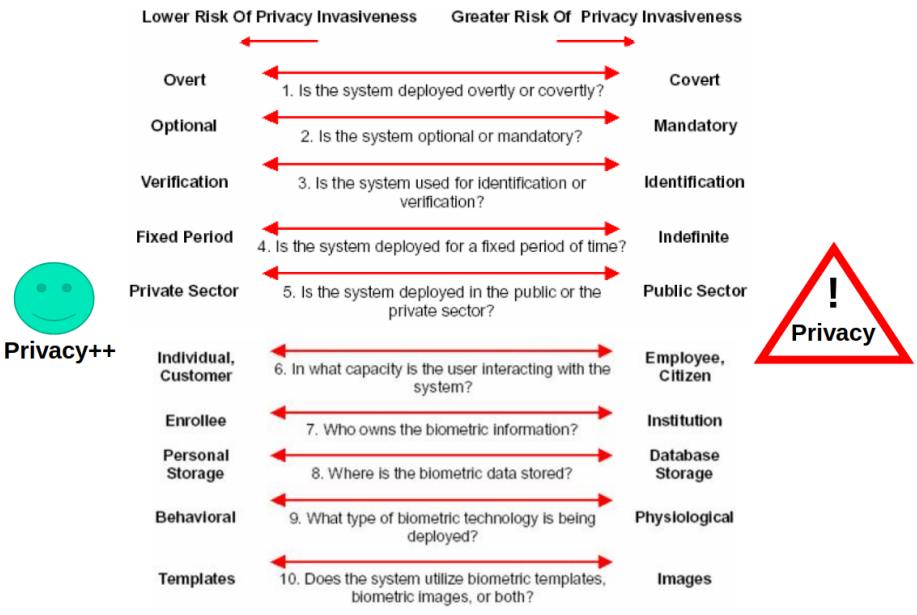


4.1 8 domande per scegliere il tratto

1. È una applicazione di **autenticazione** o **identificazione**?
   - se identificazione, occorre controllare le proprietà di:
     - scalabilità
     - unicità del tratto
2. È un sistema **semiautomatico** o **automatico**?
   - se semiautomatico:
     - occorre prevedere una persona sempre al fianco del sensore
3. Gli **utenti sono abituati**? Possono essere convinti ad abituarsi?
   - le evidenze mostrano che le performance migliorano notevolmente se gli utenti imparano a *farsi acquisire* e sono collaborativi
4. È un sistema **aperto o coperto/nascosto**?
   - alcuni tratti biometrici non possono essere acquisiti senza mettere a conoscenza il soggetto, per privacy o per le caratteristiche del tratto biometrico stesso
5. I soggetti sono **collaborativi o non collaborativi**?
   - se i soggetti sono non collaborativi (criminali), è necessario usare tratti che non possono essere cambiati
   - evitare tratti biometrici comportamentali
6. Quali sono i requisiti sulla **capacità di memorizzazione del sistema**?
   - i template hanno dimensione che può variare moltissimo (pochi byte per le impronte a molto kbyte per la voce)
7. Quanto sono stringenti le **richieste sulle performance** (accuratezza, velocità, distanze di acquisizione, ...) ?
   - è possibile unire 2 tratti veloci in un sistema multimodale per ottenere l'accuratezza richiesta, che singolarmente i tratti non riuscirebbero a garantire
8. Quali tipi di tratti biometrici sono **accettati dalla popolazione** degli utenti?
   - l'accettazione varia molto in base al livello culturale, etico, sociale religioso ed igienico

4.2 Classificazione dei sistemi biometrici rispetto alla privacy

- Applicazioni a protezione della privacy
  - La biometria protegge informazioni personali che potrebbero altrimenti essere compromesse
- Applicazioni compatibili con la privacy
  - Progettate tenendo conto di tecniche di protezione della privacy (la maggior parte delle applicazioni attuali)
- Applicazioni neutrali rispetto alla privacy
  - Sistemi di autenticazione per dispositivi elettronici
- Applicazioni invasive rispetto alla privacy
  - Applicazioni di sorveglianza e alcuni servizi di identificazione nazionale



4.3 Livelli di accuratezza da impostare

Alcuni ordini di grandezza considerati come necessari:

- **Autenticazione**
  - $FNMR = 0,1\%$
  - $FMR = 0,1\%$
- **Identificazione su larga scala** (1 milione di ID)
  - $FNMR = 10\%$
  - $FMR < 0,0001\%$ (meno di 1 errore su 1M match)
- **Screening** (500 ID)
  - $FNMR = 1\%$
  - $FMR = 0,001\%$

4.4 Utenti

Nella stesura del progetto occorre:

- definire la struttura/servizio da proteggere con il sistema biometrico
- definire le procedure di
  - system training (messa a punto dei parametri)
  - enrollment
- definire la classe degli utenti operatori sul sistema, e che operazioni possono eseguire
- prevedere la figura di impostore che potrebbe avere interesse a forzare il sistema

4.5 Sistema di backup

Nella stesura del progetto occorre definire:

- quale strategie sono da attuare se il sistema non dovesse funzionare (backup system)
- quali sono i costi del fermo del sistema biometrico

4.6 Costi del sistema

Nella stesura del progetto occorre definire e quantificare i seguenti costi:

- violazione del sistema
- strutture di sicurezza prima e dopo l'introduzione del sistema
- fermo del sistema biometrico
- costo medio dei *failure to enroll*
- costo medio per la *user education*
- costo medio *supervisory labor*
- costo medio *maintenance labor*

4.7 Passi successivi

- *Come acquisire i dati biometrici?*
- *Quale rappresentazione interna (sample) è migliore per gli algoritmi di estrazione delle feature?*
- *Quale tipo di feature estrarre dai sample?*
- *Con quali algoritmi le estraiamo?*
- *Dati due template, quale funzione e quale algoritmo di matching usiamo?*
- *Come organizziamo il DB dei template?*
  - *Numero di template per individuo?* Occorre trovare un equilibrio tra accuratezza del matching e tempo di ricerca
  - *Come organizziamo la divisione dei template del DB per aumentare efficienza delle ricerche (binning)?*

Capitolo 5

Biometria nel cloud - BaaS

Come estensione dei BSP si hanno anche le ***Biometric Services Platform***:

- Nuove soluzioni per fare riconoscimento biometrico basate sul cloud
- Vanno a semplificare installazione, uso, gestione e manutenzione del sistema biometrico
- Abbassano i costi e i tempi per iniziare ad usare un sistema biometrico, specialmente per grandi organizzazioni
- Necessitano di connessioni affidabili
- **Vantaggi**
  - scalabilità
  - costi
  - affidabilità
  - indipendenza dall'hardware
  - accesso costante a dati privati e servizi
- **Svantaggi**
  - dipendenza dal fornitore per prezzi e contratti
  - privacy, usi non concordati, liste di proscrizione, ...