PRESTAZIONI DI UN SISTEMA BIOMETRICO

La natura inesatta dei processi di acquisizione e confronto causa errori inevitabili.
Diversamente da un'operazione di controllo di una password, l'affidabilità del risultato di un confronto di istanze diverse della stessa caratteristica biometrica non è del 100%. Le principali cause delle differenze tra acquisizioni successive della stessa caratteristica sono:

- variazioni sopravvenute nella caratteristica biometrica (ad esempio tagli o escoriazioni nelle impronte digitali);
- errato posizionamento rispetto al sensore di acquisizione;
- salienti variazioni dell'ambiente di acquisizione (variazioni di illuminazione, temperatura, umidità, ...) .

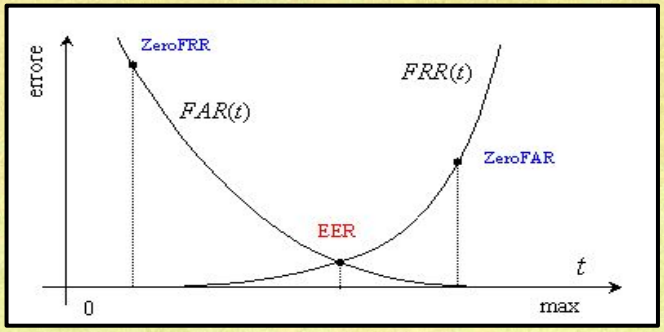
Risulta quindi necessario attribuire alla frase "*due caratteristiche biometriche coincidono*" il significato "*sono sufficientemente simili*" ed essere coscienti che, anche se molto raramente, il sistema può commettere errori.

Due sono i tipi di errori che un sistema biometrico può commettere; la probabilità di tali errori è espressa da due parametri (legati tra loro) che prendono il nome di **FRR** e **FAR**:

- **FRR** (**False Rejection Rate**: frequenza di falsi rifiuti) specifica la frequenza con la quale il sistema rifiuta ingiustamente individui che sono autorizzati all'accesso.
- **FAR** (**False Acceptance Rate**: frequenza di false accettazioni) specifica la frequenza con cui il sistema è ingannato da estranei che riescono a essere autorizzati, pur non avendo diritto di accesso.

SICUREZZA E TARATURA DI UN SISTEMA BIOMETRICO

Il grado di sicurezza di un sistema biometrico può essere impostato dall'amministratore agendo sulla soglia di sicurezza ***t***, che stabilisce quanto stringenti debbano essere i requisiti di somiglianza delle caratteristiche biometriche.
FRR e **FAR** (vedi colonna a sx) sono infatti funzioni della soglia ***t***.



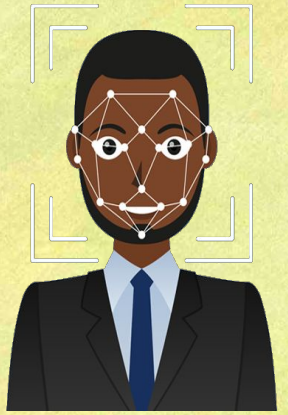
Incrementando il valore di ***t*** si rende più arduo il compito agli impostori (cioè diminuisce **FAR**), ma al tempo stesso, alcuni utenti, che tentano lecitamente di accedere al sistema, possono essere talvolta rifiutati (cioè cresce **FRR**).
Al contrario, diminuendo il valore di ***t*** per facilitare estremamente gli accessi a chi ne ha diritto (diminuisce **FRR**) potrebbe aumentare il pericolo di false accettazioni (cresce **FAR**).

RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/autenticazione_biometria/

AUTENTICAZIONE BASATA SU BIOMETRIA

Scopri come funziona l'autenticazione basata su biometrica e quali sono i possibili rischi che si corrono ad usarla .



POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

AUTENTICAZIONE BIOMETRICA

L'**autenticazione biometrica** è una tecnica di riconoscimento comoda ed immediata che utilizza delle caratteristiche biologiche delle persona per la sua **autenticazione**.

Il tratto biometrico che viene misurato deve essere:

- universale (tutti lo devono avere);
- unico;
- permanente;
- difficile da falsificare;
- facile da misurare;
- economico da misurare;
- non troppo invasivo (es. il **DNA** è unico, ma è troppo invasivo da estrarre per una semplice autenticazione)

Nel caso di **accesso remoto** i fornitori di servizi internet non utilizzano le credenziali biometriche a causa della difficoltà di raccolta dei dati biometrici e per la criticità di memorizzazione di questi dati.

Per contro l'autenticazione biometrica è un sistema ottimo e ampiamente sperimentato per le **credenziali memorizzate a livello locale** come nel caso degli smartphone. In questo caso, oltre ad essere estremamente pratico da usare è anche molto sicuro per le soluzioni tecniche adottate, che rendono estremamente difficile il furto dei dati biometrici locali anche nel caso in cui un attaccante entri in possesso dell'apparecchio.

Un limite del sistema è che nel caso di **furto delle credenziali** biometriche, questo questo tipo di autenticazione diventa inutilizzabile proprio per l'impossibilità di cambiare i dati biometrici.

Un ulteriore problema dell'autenticazione biometrica è quello che l'utente potrebbe essere costretto da qualcuno a fornire le proprie credenziali biometriche. Una situazione possibile in caso di aggressioni da parte di criminali, ma che potrebbe presentarsi, anche se in modo meno drammatico, in caso di richiesta di accesso a un'apparecchiatura per motivi di controllo da parte di polizie e autorità governative. Uno scenario che aprirebbe di fatto una serie di problemi etici sulla **privacy** e la sicurezza.

TRATTI COMUNI E MENO COMUNI

I tratti più comunemente usati per implementare sistemi di autenticazione biometrica sono:

- l'impronta digitale (dito);
- la retina;
- l'iride;
- il volto;
- la mano;
- la voce.




Tra i meno comuni troviamo invece:

- le orecchie;
- il piede;
- le vene;
- l'ECG;
- l'andatura.

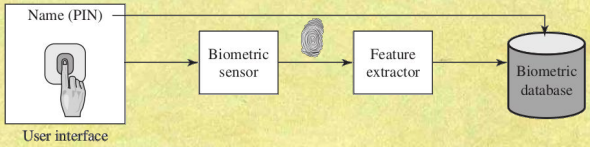
Nel seguente grafico è illustrata la relazione tra accuratezza e costi di implementazione di sistemi biometrici basati su alcune delle diverse tipologie sopracitate.

Si nota, a conferma del fatto che è molto usata nei sistemi attuali, che l'**impronta digitale** è il giusto compromesso per realizzare un sistema biometrico di modesta efficacia.

ARRUOLAMENTO, VERIFICA E IDENTIFICAZIONE

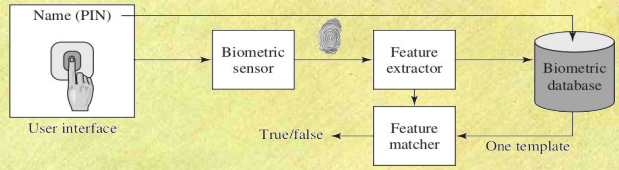
Nel contesto di un sistema di autenticazione biometrico, si distinguono due fasi: la fase di **arruolamento** al sistema, seguita dalla fase di **identificazione** o **verifica**.

Arruolamento



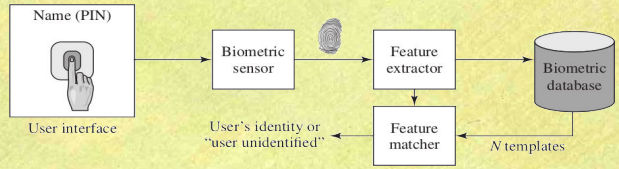
Fase preliminare in cui l'utente associa la sua identità al tratto biometrico memorizzando l'informazione in un database.
C'è un'interfaccia utente (che può richiedere o meno la presenza fisica di un agente di arruolamento) nella quale il tratto del corpo è rilevato dal **sensore biometrico**; successivamente il tratto viene trasformato (grazie all'estrattore di features - **features extractor**) in un'informazione digitale memorizzabile da un sistema informatico.

Verifica



È La seconda fase (più comune) in cui l'utente si mostra al sistema ed esso decide se ammetterlo.

Identificazione



Seconda fase (meno comune) in cui è il sistema che cerca direttamente una corrispondenza nel database con il tratto dell'utente ed eventualmente lo identifica.