## 3. SISTEMI BIOMETRICI

Il termine Biometria deriva da due termini distinti: "Bio" (vita) – "Metrico" (misura). La biometria usa gli strumenti per riconoscere tratti fisici e comportamentali di un essere umano. Questi tratti acquisiti vengono usati per: ***Autenticazione*** (verificare che una persona e chi effettivamente dice di essere) e ***Identificazione*** (riconoscere un individuo tra un insieme di possibili individui). Autenticazione e Identificazione sono basate su caratteristiche **uniche,** ossia caratteristiche che permettono di riconoscere unicamente una persona.

Un sistema biometrico è un dispositivo automatico per identificazione/autenticazione basati su caratteristiche dell'individuo:

- **Fisiologico**: impronte digitali, volto, forma dell'iride, etc..
- **Comportamentali**: timbro della voce, dinamica della firma, etc…

La differenza tra queste 2 caratteristiche appena descritte sono che per Fisiologico s'intende un insieme di caratteristiche che l'utente possiede mentre per quanto riguarda le Comportamentali come il nome fa intendere, sono legate al comportamento dell'individuo.

I sistemi biometrici sono usati in tanti contesti, aeroporti, sedi governative, porti, … (strutture critiche e quindi c'è bisogno di autenticazione), ma anche per accedere a sistemi informatici.

Vediamo ora quali sono le caratteristiche di un Sistema Biometrico:

- **Universalità:** ogni individuo deve possedere quella determinata caratteristica biometrica.
- **Unicità**: non è possibile che due persone condividano la stessa identica caratteristica biometrica.
- **Permanenza**: la caratteristica biometrica deve rimanere immutata nel tempo.
- **Catturabilità**: la caratteristica biometrica deve poter essere acquisita e quantitativamente misurata (acquisizione facile di un dato biometrico).

Dopo aver analizzato le caratteristiche di un Sistema Biometrico, vediamo l'Architettura di un sistema biometrico:

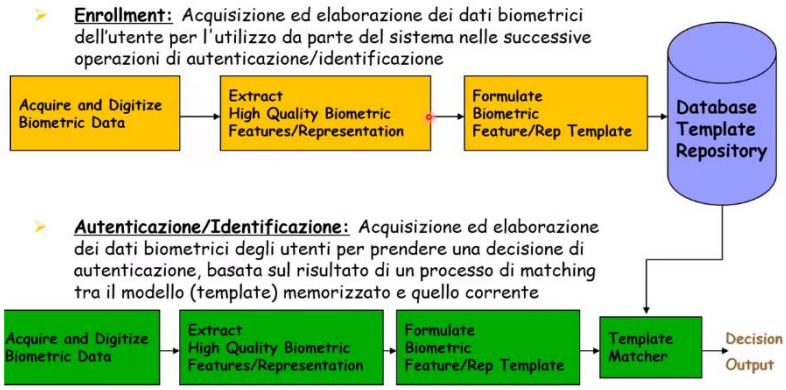
partiamo da una premessa, l'Architettura di un Sistema Biometrico dipende dal contesto di utilizzo (Identificazione: Chi sei? – Autenticazione: Sei chi dichiari di essere?)

- L'identificazione consiste di: **Match uno a molti** (acquisizione di un impronta digitale e la confronto con tutte le impronte digitali che ho in un database) **, Match uno a pochi** (restringo la ricerca sul database ad un sottoinsieme delle persone)**, Soggetti cooperativi e non cooperativi.**
- L'autenticazione consiste di: **Match uno ad uno** (confronto un'impronta digitale con un singolo modello archiviato, ad esempio questo accade su uno smartphone)

Vediamo ora l'architettura:

I passi che un passo biometrico esegue sono:

la prima fase (in cui si addestra il sistema) è detta di **Enrollment:** si effettua l'acquisizione e l'elaborazione di dati biometrici (ad esempio si assuma di comprare uno smartphone e di fare registrare per la prima volta l'impronta digitale. I nuovi smartphone prevedono una ripetuta immissione del dito con cui si effettua il controllo in maniera tale che il sensore venga istruito a riconoscere l'impronta. Si faccia attenzione che l'immissione deve superare un piccolo test che lo smartphone esegue: quello di sufficienza, ossia se è di buona qualità. Se non supera questo test il dispositivo chiede nuovamente l'immissione del dito).




La biometria viene acquisita e digitalizzata, vengono estratte le **Features** (informazioni che caratterizzano la biometria) che devono essere di buona qualità altrimenti il sistema non permette l'autenticazione.

Successivamente viene generato un **Template** che è un modello che caratterizza in maniera precisa la biometria di un singolo utente (su uno smartphone potrebbe essere: "L'impronta digitale di Ciro Immobile").

Acquisita l'impronta, adesso la posso usare per prendere **decisioni** di Autenticazione/Identificazione che è basata sul risultato di un processo di matching tra il modello (template) memorizzato e quello corrente. Anche in questa fase viene generato un **Template** come descritto sopra, dopo questa avviene la decisione.

Tutto ciò si può riassumere in: **ACQUISIZIONE → ESTRAZIONE DELLE CARATTERISTICHE → CONFRONTO → DECISIONE**

Vediamo ora **Sistemi Biometrici Multimodali**, che nascono dal fatto che, usando una singola biometria, una o più delle seguenti caratteristiche (universalità, unicità, permanenza, catturabilità) non sono più soddisfatte.

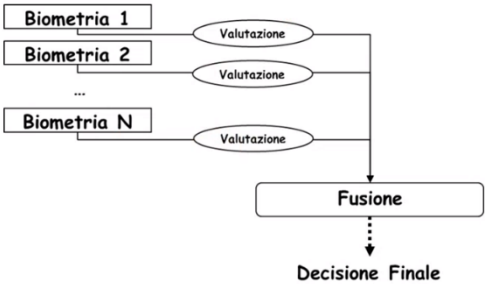
Una limitazione di un sistema biometrico unimodale può essere: polvere e/o sporcizia su sensore di acquisizione di impronte digitali, forte sorgente di luce puntata verso il sensore di acquisizione del volto.

Due possibili soluzioni a questo possono essere: integrazione del sistema biometrico unimodale con tecniche di autenticazione tradizionali (non basate su biometrie), ad esempio mediante immissione di PIN, password,…, oppure progettare un sistema biometrico in grado di utilizzare più biometrie (o modalità): **Sistemi Biometrici Multimodali.** Concentriamoci su quest'ultima tecnica.

Ci sono 3 scelte possibili per progettare un Sistema Biometrico Multimodale:

- **Progettazione in Parallelo** (la più importante)
- **Progettazione in Serie**
- **Progettazione a Livello Gerarchico**

La Progettazione in **Parallelo** si basa sul fatto che le biometrie di un utente sono acquisite e valutate in maniera indipendente. Gli esiti che derivano da queste valutazioni vengono passati ad un livello detto di Fusione il quale si occupa di mettere insieme i vari responsi e generare la decisione finale relativo al Sistema Biometrico. La Fusione può avvenire in diversi moduli dell'architettura di un sistema biometrico e secondo diverse strategie operative (ossia può essere implementato in fase di ACQUISIZIONE, ESTRAZIONE DELLE CARATTERISTICHE , CONFRONTO, DECISIONE). Ci concentreremo sulla Fusione che avviene nella fase di Decisione: questa è una fase delicata che deve essere stabilita in modo rigoroso. Per il calcolo della decisione finale possono essere usate 3 strategie:




- **Strategia AND**
- **Strategia OR**
- **Strategia di combinazione pesata**

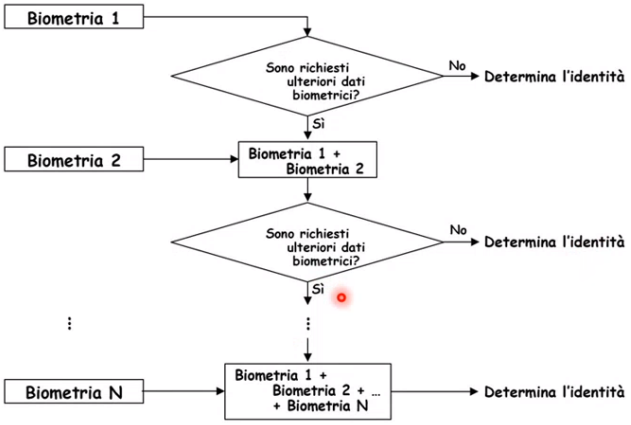
Con la strategia AND, affinché la decisione finale risulti essere positiva (true), è richiesto che **tutti i processi decisionali** relativi a ciascuna biometria restituiscono output positivo (true).

Con la strategia OR, affinché la decisione finale risulti essere positiva (true), è sufficiente che **almeno uno dei processi decisionali** relativi a ciascuna biometria restituisca output positivo (true).

Si possono usare strategie combinate di AND e OR (ad esempio per i primi due processi decisionali biometrici c'è un OR e il risultato di quest'OR va in AND con il terzo processo decisionale biometrico).

Con la strategia di combinazione pesata, si associa ad ogni biometria un peso diverso ("La scansione del volto è la più importante, quindi assegna il 60% del peso"). Di conseguenza, il calcolo della decisione finale è dato sulla base degli output dei processi decisionali pesati.

La progettazione in **Serie** avviene in questo modo: viene acquisita la prima biometria e il Sistema Biometrico verifica se sono necessari altri dati per verificare l'utente: se non servono altri dati allora l'utente è autenticato/identificato. Se sono richiesti ulteriori dati perché il sistema non riesce ad identificare l'utente, è richiesta un'ulteriore biometria e il sistema valuta queste 2 biometrie insieme. La fase di verifica è quella descritta sopra. Questa modalità è molto meno sicura rispetto alla strategia descritta nella progettazione in Parallelo.




La progettazione a **Livello Gerarchico** prevede che un sottoinsieme delle biometrie sia acquisito in modo parallelo, un altro sia acquisito in maniera seriale e poi vengono valutati a seconda di vari criteri di fusione. La peculiarità di questa progettazione e la fusione di acquisizioni seriali e in parallelo. Questo Sistema Biometrico non è mai usato.