Introduzione ai sistemi biometrici

Annalisa Franco
annalisa.franco@unibo.it

Dario Maio
dario.maio@unibo.it

Provare la propria identità

Interazioni dirette

Interazioni remote

Interazioni uomo-macchina

Riconoscimento di persone

- **Esempi di richieste che emergono abitualmente in organizzazioni pubbliche e private:**
  - Questa persona è autorizzata a entrare in questa struttura?
  - Questo individuo ha il permesso di accedere a queste informazioni?
  - Questa persona ha già presentato in precedenza una domanda d'assunzione?

Qualcosa che l'utente POSSIEDE

Qualcosa che l'utente CONOSCE

Qualcosa che CONTRADDISTINGUE l'utente

Qualcosa che l'utente **POSSIEDE**

- Magnetic card, chip card, ...
  - una chiave d'accesso che autorizza il possessore a effettuare un'operazione (es. carta bancomat)
- Problemi
  - Possono essere rubate
  - Possono essere prestate
  - Possono essere copiate
  - In realtà il sistema autentica l'oggetto, non il possessore!

Qualcosa che l'utente **CONOSCE**

- **Password, PIN**
  - un'informazione **facile da ricordare** → **facile da indovinare**
- **Problemi**
  - Può essere rubata, spiata e suscettibile ad attacchi da parte di hacker

Gli hacker riescono tipicamente a indovinare più del 30% delle password di una rete

  - Facile da condividere
  - Le password vengono spesso dimenticate

Su www.NYTimes.com site, 1000 utenti ogni giorno dimenticano la loro password

Furti d'identità (1)

- Gli utenti più assidui del web hanno in media 21 password; l'81% degli utenti seleziona password comuni e il 30% le scrive o le memorizza su file (2002 NTA Monitor Password Survey).

Furti d'identità (2)

- I ladri d'identità rubano numeri della sicurezza sociale, numeri della patente e cognomi da celibi/nubili – spesso utilizzati come password per proteggere un conto – per aprire conti dai quali prelevare fondi.
- I furti d'identità sono una realtà e rappresentano il crimine con il tasso di crescita maggiore negli U.S.A.
- Le imputazioni per furti d'identità segnalate alla SSA fraud hotline sono aumentate da 11000 nel 1998 a 65000 nel 2001; le indagini del Postal Inspection Service ID Theft sono aumentate nel 2000 del 65% rispetto all'anno precedente;
- Le chiamate al FTC ID Theft Clearinghouse sono aumentate da 2000 alla settimana nel marzo 2001 a 3000 alla settimana nel dicembre 2001;
- Le frodi a carte di credito sono cresciute negli USA da circa $700M nel 1996 a circa $1B nel 2000.

Source: General Accounting Office (March, 2002)

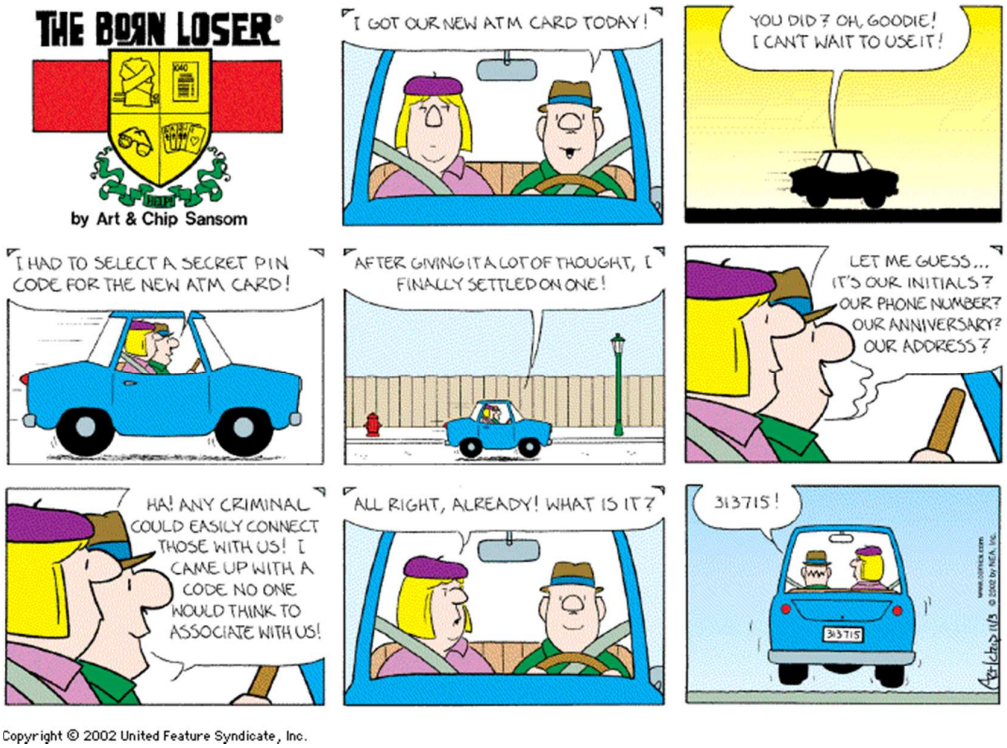
Alcuni ben noti problemi ...

	Percent of Adult Population[1]	Number of Persons (millions)[2]
New Accounts & Other Fraud	0.8 % (0.5 % - 1.2%)	1.8 (1.2 – 2.8)
Misuse of Existing Non-Credit Card Account or Account Number	1.5 % (1.1% - 2.1%)	3.3 (2.4 – 4.6)
Misuse of Existing Credit Card or Credit Card Number	1.4 % (1.0 % - 2.1%)	3.2 (2.1 – 4.6)
Total Victims in 2005	3.7 % (3.0% - 4.6%)	8.3 (6.6 – 10.3)

8.3 milioni di furti d'identità negli USA nel 2005

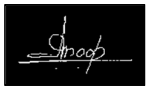
Nel 2004 circa 57 milioni di americani sono stati bersaglio di phishing in un anno; le frodi mediante phishing hanno già raggiunto il miliardo di dollari annuo.

Codici segreti…



Qualcosa che **CONTRADDISTINGUE** l'utente: caratteristiche biometriche

- L'uso di caratteristiche biometriche rappresenta di fatto la forma più antica di riconoscimento:
  - **Volto**
  - **Voce**
  - **Impronta**
  - **Firma**



- **"You are your authenticator"**

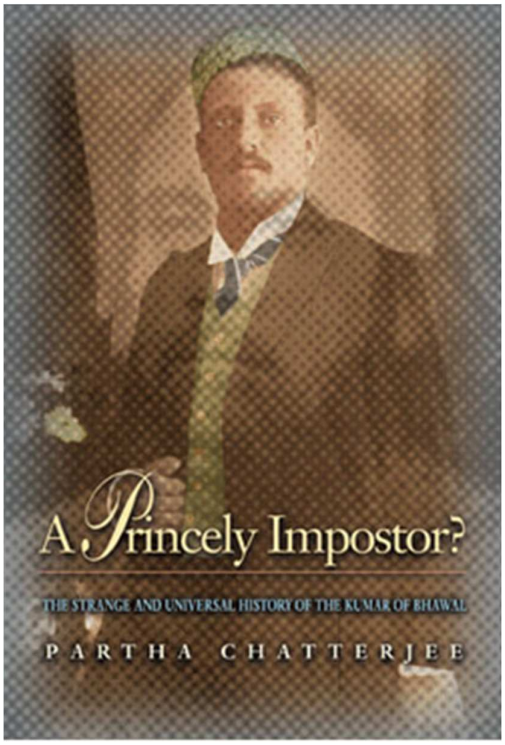
  (Schneier, *Secrets and Lies: Digital Security in a Networked World*)

  Una grandezza biometrica è descritta come una caratteristica fisiologica o comportamentale che possa essere misurata e successivamente identificata al fine di attestare l'identità di una persona (o più in generale di un essere vivente).

"Chi sei" invece di
"Che cosa possiedi" o "Che cosa conosci"

- **Il riconoscimento di una persona attraverso il suo corpo , collegandolo a un'identità definita esternamente**

Tichborne Case of Bengal: Bhawal Sanyasi (Monk), The Princely Imposter



Identification Data	The Prince (Kumar Ramendra Narayan Roy, The second Kumar of Bhawal)	The Monk (Bhawal Sanyasi)
Hair	Brownish	Brownish
Moustache	Wavy	Wavy
Eyes	Brownish	Brownish
Lips	Twist on the right lower lip	Twist on the right lower lip
Ears	A sharp angle at the rim	A sharp angle at the rim
Earlobes	Not adherent to the cheeks and pierced	Not adherent to the cheeks and pierced
Index and middle fingers of the left hand	Less unequal than those of the right hand	Less unequal than those of the right hand
Feet	Scaly, size 6 for shoes	Scaly, size 6 for shoes
Gait	similar	similar
Voice	similar	similar
Expression	similar	similar

Riconoscimento e grandezze biometriche

Nel 1882 Alphonse Bertillon (1853-1914), capo del servizio di identificazione della polizia di Parigi, introdusse un nuovo sistema di misurazione corporea studiato appositamente per l'identificazione dei criminali. Queste misure erano studiate in modo tale che, in teoria, potessero identificare univocamente ogni persona e non cambiassero durante il corso della vita adulta.

Scheda per la memorizzazione delle informazioni

Caliper compass

Sliding compass

Altri strumenti

Il caso di Will e di William West

Due uomini imprigionati nel penitenziario di LeavenWorth (Kansas) avevano misure molto simili secondo il sistema di Bertillon.

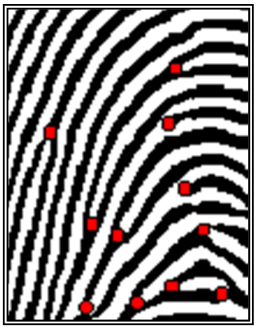
William rilasciato nel 1901, Will imprigionato nel 1903.

Will West's Bertillon Measurements
178.5; 187.0; 91.2; 19.7; 15.8; 14.8; 6.6; 28.2; 12.3; 9.7

William West's Bertillon Measurements
177.5; 188.0; 91.3; 19.8; 15.9; 14.8; 6.5; 27.5; 12.2; 9.6

Il potere discriminante delle impronte

Alla fine del XIX secolo, nel suo lavoro sull'ereditarietà, Galton criticò il sistema di Bertillon dal punto di vista statistico. Nel 1892 introdusse la nozione di minuzia e suggerì un primo sistema di classificazione di impronte molto elementare.



Nel 1893, l'Home Ministry Office, UK, riconobbe che non esistono due individui con la stessa impronta.

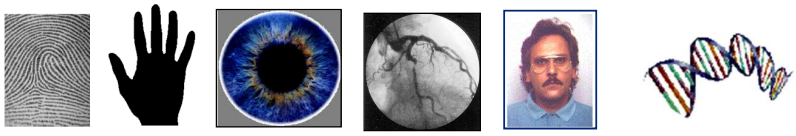
Presto molti dei maggiori dipartimenti di polizia cominciarono a "schedare" le impronte dei criminali. Molti studi rigorosi furono finanziati e furono sviluppati metodi scientifici per il confronto visivo di impronte.

Il sistema di classificazione di Galton-Henry (1900) è alla base dei sistemi di riconoscimento di impronte di molti dipartimenti di polizia in diversi Paesi.

Riconoscimento biometrico

Con il termine "riconoscimento biometrico" si fa di solito riferimento all'uso di caratteristiche fisiologiche o comportamentali distintive per il riconoscimento automatico di individui.

- **fisiologiche**



  - **impronta, mano, iride, retina, volto, dna,...**

- **comportamentali**

  - **firma, voce, stile di battitura, ...**

Nota: probabilmente tutte le caratteristiche biometriche sono in realtà una combinazione di caratteristiche fisiologiche e comportamentali e non dovrebbero essere classificate in maniera esclusiva come appartenenti a una delle due categorie.

Genotypic vs phenotipic traits

Biometric traits develop:

1. through genetics:
Genotypic

2. through random variations in the early phases of an embryo's development:
Phenotypic

3.through training:
Behavioral

Biometric Trait	*genotypic*	*phenotypic*	*behavioral*
Fingerprint (only minutia)	o	ooo	o
Signature (dynamic)	oo	o	ooo
Facial geometry	ooo	o	o
Iris pattern	o	ooo	o
Retina (Vein structure)	o	ooo	o
Hand geometry	ooo	o	o
Finger geometry	ooo	o	o
Vein structure of the back of hand	o	ooo	o
Ear form	ooo	o	o
Voice (Tone)	ooo	o	oo
DNA	ooo	o	o
Odor	ooo	o	o
Keyboard Strokes	o	o	ooo
Comparison: Password			(ooo)

Source:
http://www.bromba.com/faq/biofaqe.htm#entstehen

Vantaggi nell'uso di caratteristiche biometriche

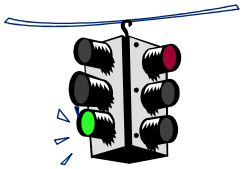
- **Le password o i token utilizzati per l'identificazione sono metodi di autenticazione "innaturali"!**
  - Non possono attestare con sicurezza l'identità della persona, ma semplicemente garantire che l'utente sia a conoscenza di qualcosa o la possegga.
- **Le caratteristiche biometriche sono un metodo di autenticazione "naturale"**
  - **Vantaggi**
    - Le caratteristiche biometriche non possono essere perse, prestate, rubate o dimenticate
    - L'utente deve "semplicemente" presentarsi di persona
    - Le caratteristiche biometriche garantiscono la presenza della persona, in quanto risulta molto difficile per un individuo falsificare le caratteristiche fisiche di qualcun altro.
  - **Svantaggi**
    - Non garantiscono un'accuratezza del 100%
    - Esistono utenti che non possono utilizzare alcune tecnologie
    - Le caratteristiche possono mutare nel tempo
    - I dispositivi biometrici, in alcune circostanze, possono non essere affidabili

Motivazioni

- Aumento delle violazioni della sicurezza
- Incertezza nella situazione internazionale
- Complessità della società dell'informazione
- Attività fraudolente nelle transazioni economiche
- Notevoli progressi nella tecnologia biometrica con una riduzione dei costi
- Consapevolezza diffusa dei problemi di sicurezza, applicazione di disposizioni di governo
- .....

Obiettivo

Riconoscimento di persone attraverso tecniche non intrusive, con costi e sicurezza appropriati per la particolare applicazione.



Qual è il sistema biometrico ideale per il controllo degli accessi?

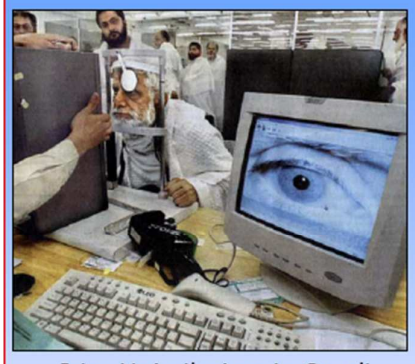
Campi d'applicazione

- Controllo accessi, controllo risorse, controllo presenze, sorveglianza ambientale
- Identificazione agli aeroporti o alle frontiere
- Login al computer, transazioni sicure, commercio elettronico
- Carta d'identità, servizi sociali, servizi sanitari, votazioni, identificazione di criminali
- …






Alcuni esempi d'applicazione (1)


Iris: Haj pilgrims in Saudi Arabia


Fingerprint: Point of sale

Fingerprint, Face, Iris: Australia airport security


Iris: Identifying insurgents


Fingerprint: Mobile phone


Palm Vein: Japan ATM

Alcuni esempi d'applicazione (2)

Face: Surveillance Applications

Keyless ignition: Audi A8

Iris: Frankfurt Airport

Hand Geometry: Ben Gurion Airport

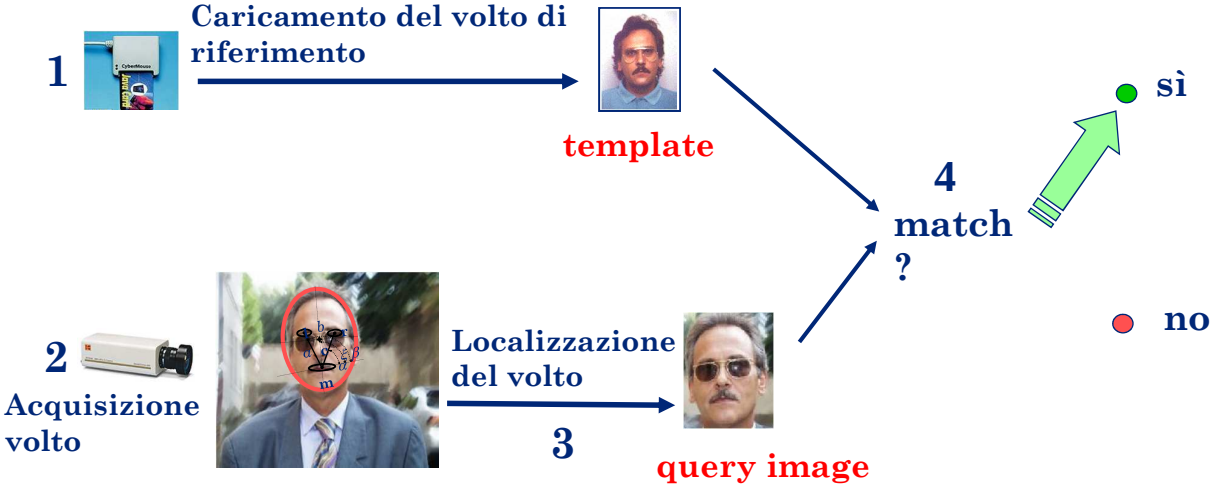
Fingerprint: US-VISIT program

Finger Vein: Accessing ATMs in Japan

Modalità di riconoscimento: Verifica vs. Identificazione (1)

Verifica (Autenticazione): Sono chi dichiaro di essere?

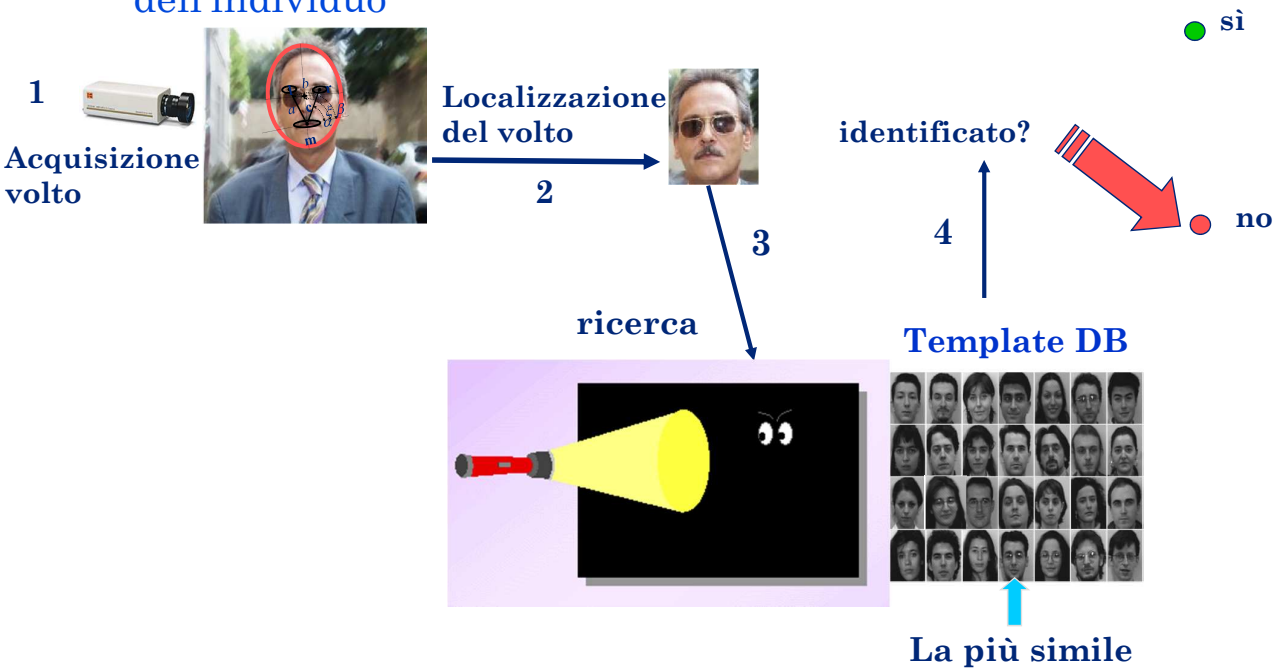
- Confronto uno a uno al fine di determinare se l'identità dichiarata dall'utente sia vera o no



Verifica vs Identificazione (2)

Identificazione: Chi sono?

- Confronto uno a molti al fine di stabilire l'identità dell'individuo



Modalità di riconoscimento: positivo vs. negativo

- **Riconoscimento positivo:**
  - Il sistema stabilisce se la persona è chi dichiara di essere
  - Lo scopo è quello di impedire che **più persone utilizzino** la **stessa identità**
  - Modalità verifica o identificazione

Controllo accessi, login su computer, commercio elettronico, ...

- **Riconoscimento negativo:**
  - Il sistema stabilisce se la persona è chi nega di essere
  - Lo scopo è quello di evitare che **una singola persona utilizzi più identità**
  - Sola modalità identificazione

Servizi sociali, applicazioni forensi

Il riconoscimento negativo può essere effettuato solo attraverso un sistema biometrico

Classificazione delle applicazioni biometriche (1)

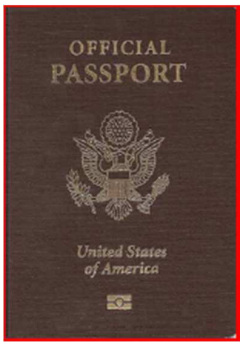
- **Cooperative vs. non cooperative**
  - Qual è il comportamento degli impostori nell'interazione con il sistema?
- **Evidenti vs. nascoste**
  - L'utente è a conoscenza di essere sottoposto a riconoscimento biometrico?
- **Abituali vs. non abituali**
  - Quanto spesso l'utente registrato è soggetto a riconoscimento biometrico?
- **Supervisionate vs. non supervisionate**
  - Il processo di acquisizione di dati biometrici è controllato, guidato o supervisionato da un operatore?

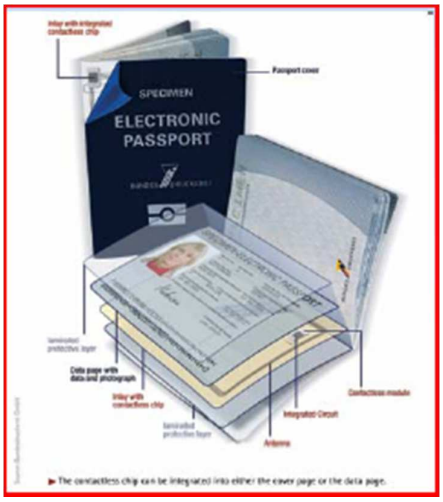
Classificazione delle applicazioni biometriche (2)

- **Ambienti operativi standard vs. non standard**
  - Il sistema opera in un ambiente controllato (temperatura, pressione, umidità, condizioni d'illuminazione, ...)?
- **Pubbliche vs. private**
  - Gli utenti del sistema sono clienti o impiegati dell'organizzazione che utilizza il sistema biometrico?
- **Aperte vs. chiuse**
  - Il modello biometrico della persona è utilizzato per una singola applicazione o per più applicazioni?

Passaporti biometrici

- ICAO (International Civil Aviation Organization) ha raccomandato l'uso di caratteristiche biometriche (volto, impronta e iride) per i passaporti



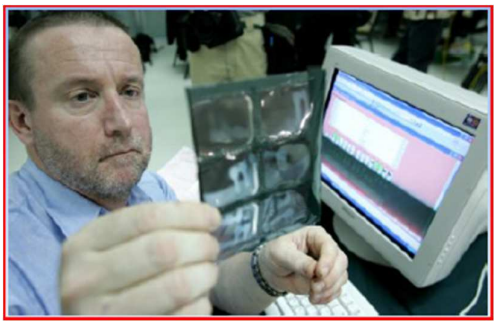


http://www.epassportphoto.com/Blog/?tag=/biometric+passport
http://www.i4donline.net/articles/current-article.asp?articleid=921&typ=News

Identificazione su larga scala

- Per accedere negli Emirati Arabi è necessario confrontare l'iride del passeggero – via internet – con un DB contenente 1 milione di IrisCode relativi a persone espulse.
- Il tempo di ricerca è circa 1 sec.
- In media ogni giorno arrivano 12000 passeggeri.

Identificazione vittime di un disastro



- Quando un corpo è decomposto le usuali tecniche di identificazione biometrica (volto, impronta) spesso falliscono.
- Il 90% delle vittime dello tsunami in Phuket (Thailand) del 2005 è stato identificato attraverso il confronto delle arcate dentali.
- A ground zero, fra le vittime identificate, il 20% è stato riconosciuto sempre attraverso le arcate dentali.

Applicazioni: il ruolo dell'utente (1)

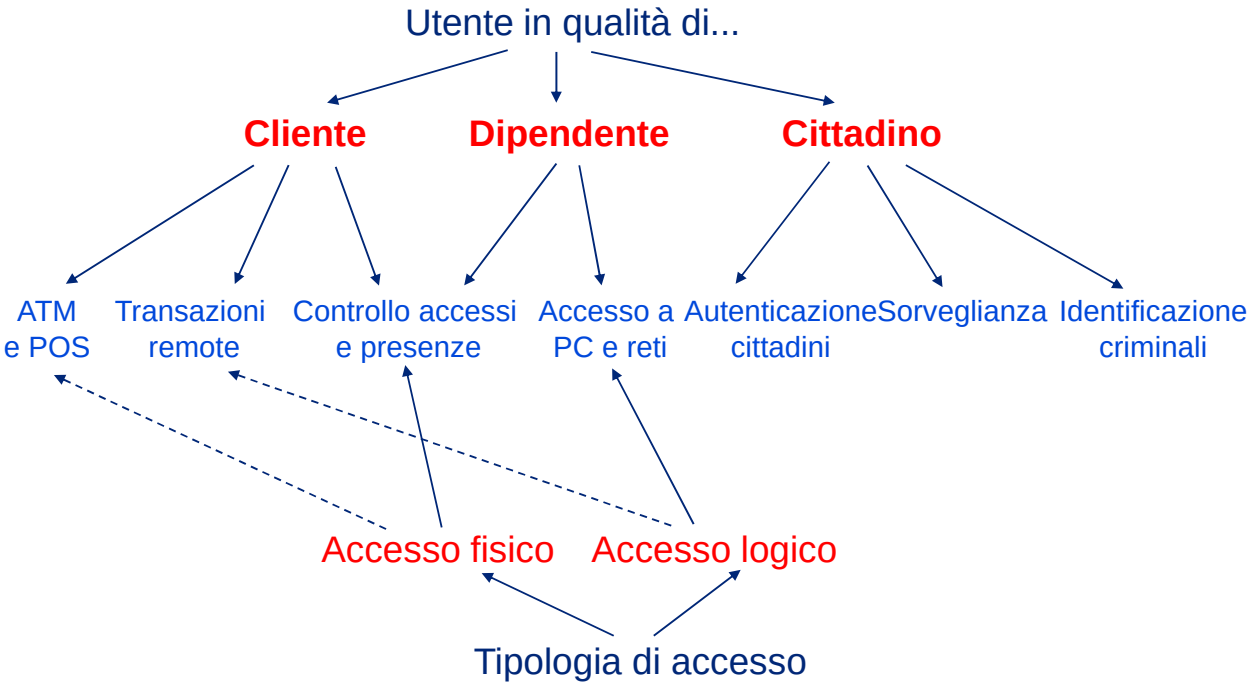
Con quale ruolo l'utente utilizza il sistema biometrico nelle diverse applicazioni?

- in qualità di **cittadino**
- in qualità di **dipendente**
- in qualità di **cliente**

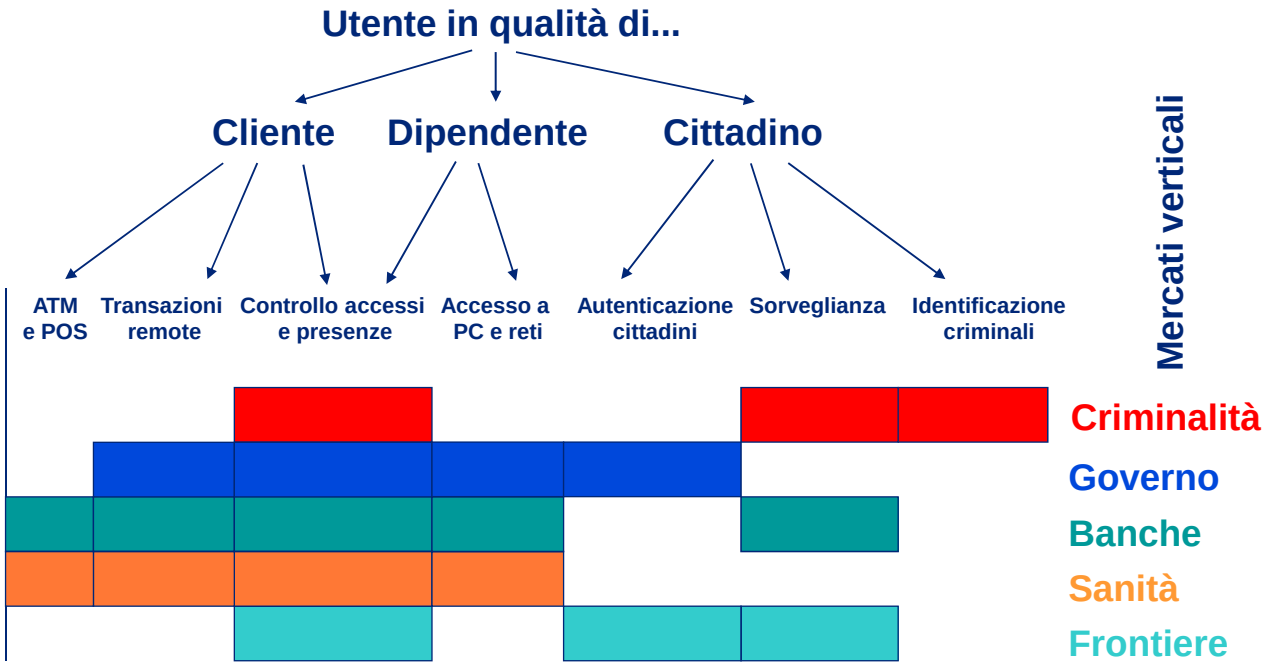
È un punto di vista spesso sottovalutato ma fondamentale relativamente a:

- Privacy
- Accuratezza e prestazioni
- Modalità di enrolment
- ...

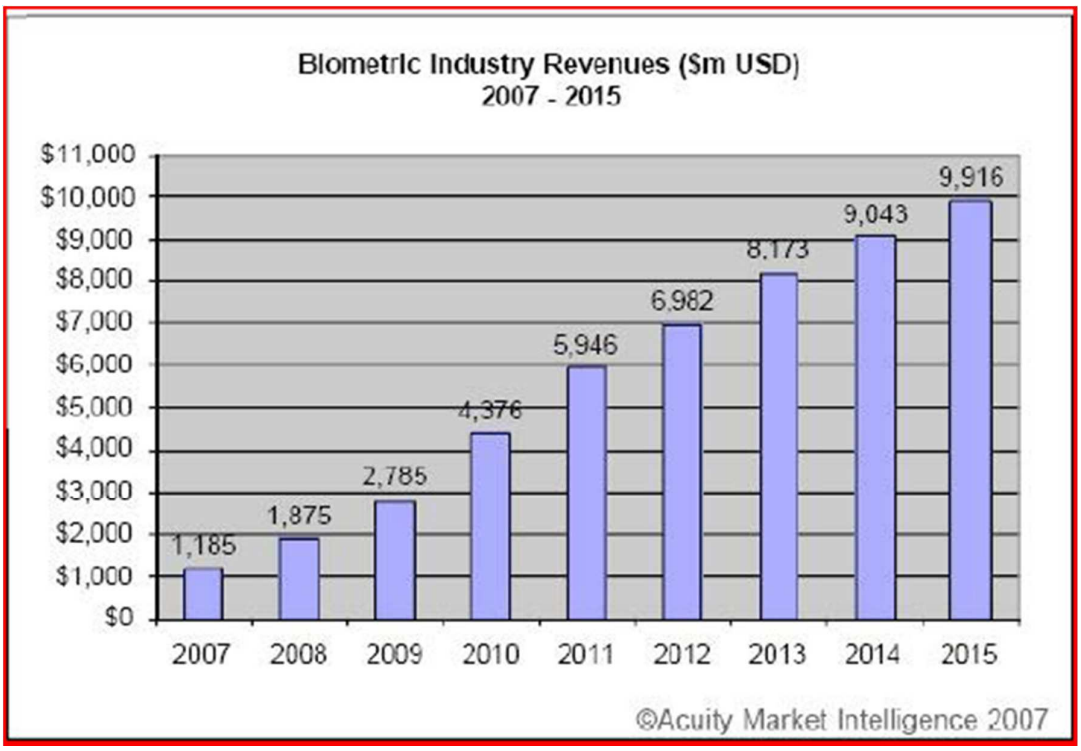
Applicazioni: il ruolo dell'utente (2)



Applicazioni e mercati verticali



Previsioni di mercato 2007-2015



Principali iniziative in Italia

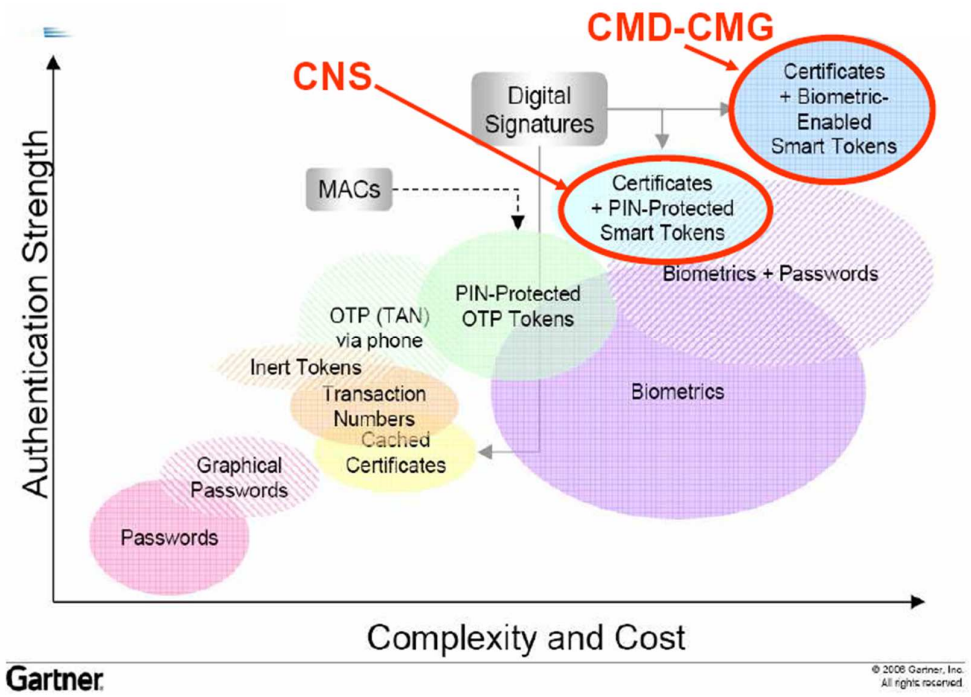
Progetti europei
- Passaporto elettronico
- Visti

Progetti nazionali
- Permesso di soggiorno elettronico (PSE)
- La Carta d'Identità Elettronica (CIE)

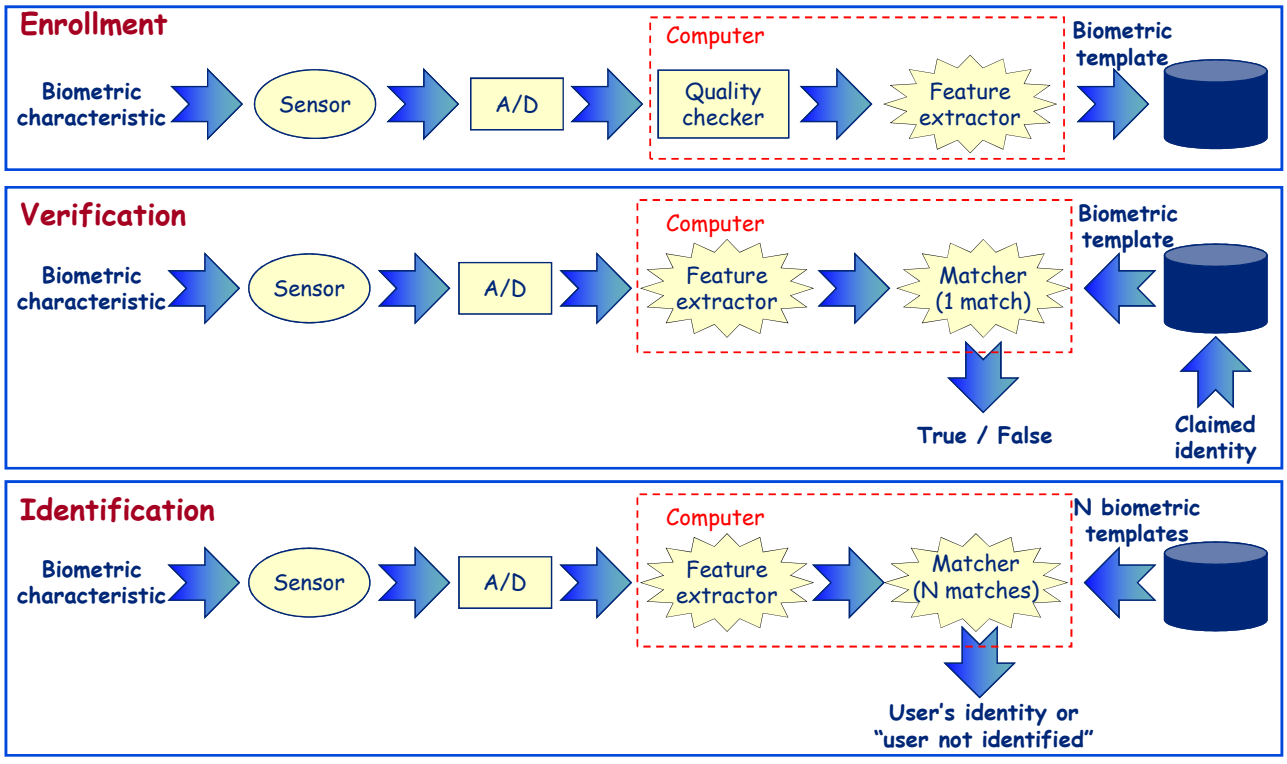
Progetti per i dipendenti del settore pubblico
- La Carta Multiservizi della Difesa (CMD)
- La Carta Multiservizi della Giustizia (CMG)
- Accesso logico a dati sensibili in alcune PAL

Settore privato
- Accesso logico a dati sensibili
- Accesso fisico ad aree alta criticità

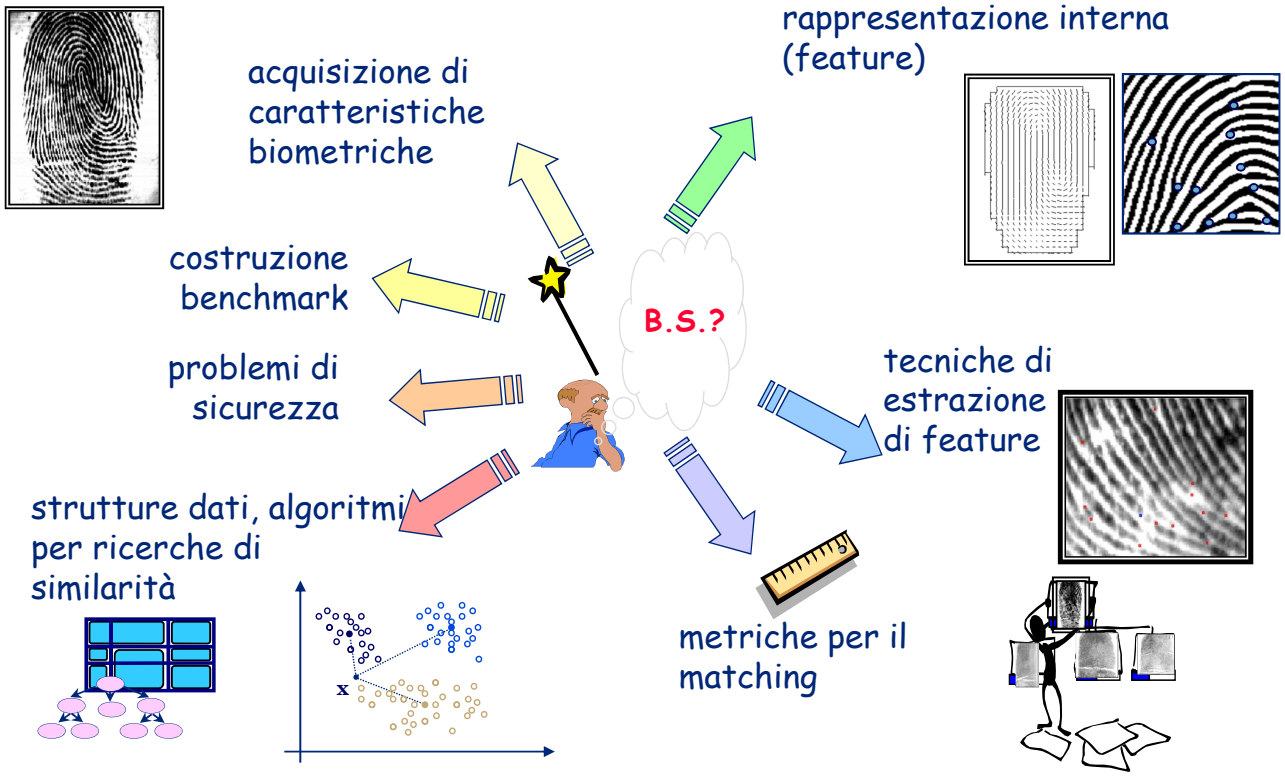
Carte multiservizio con biometria



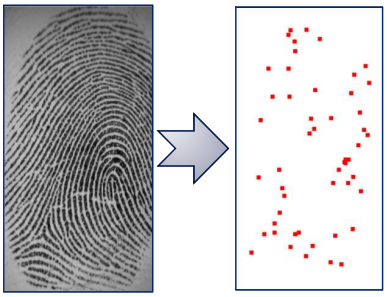
Architettura di un sistema biometrico



Prestazioni di un sistema biometrico



Template (1)



- Definizione
  Dati caratteristici e codificati ottenuti dalle feature uniche di un esempio biometrico

- Un elemento fondamentale di un sistema biometrico
  - Per il matching si utilizzano i template, *non gli esempi*
  - Quantità di dati inferiore rispetto agli esempi (es. 1/100, 1/1000)
  - Un template "non dovrebbe permettere di ricostruire" un esempio valido
  - La dimensione favorisce la cifratura e la memorizzazione su più supporti
  - Template diversi vengono generati ogni volta che un individuo fornisce un esempio biometrico

Template (2)

- Valori tipici di indicatori biometrici di un individuo
- Per ciascun individuo sono solitamente memorizzati più template per tenere conto di possibili variazioni della caratteristica biometrica
- I template sono aggiornati periodicamente

Tre diverse acquisizioni dell'impronta di un individuo (6 mesi) e del suo volto (2 anni)

Template e tutela del dato biometrico

- La conservazione dei template può avvenire:

a) nella memoria di un dispositivo biometrico;
b) in una base dati centrale;
c) in tessere plastificate, schede ottiche o smart card. Questo metodo consente agli utilizzatori di portare con sé i propri modelli come dispositivi di identificazione.

- Secondo i Garanti europei, ai fini dell'autenticazione/verifica, non è necessario memorizzare i dati di riferimento in una base di dati; è preferibile, invece, utilizzare dispositivi decentralizzati dove archiviare i dati personali.

- L'identificazione, invece, è possibile solo memorizzando i dati di riferimento in una base di dati centralizzata dato che, per accertare l'identità della persona interessata, il sistema deve confrontare i suoi template o i suoi dati grezzi (immagine) con i modelli o i dati grezzi di tutte le persone i cui dati sono già registrati a livello centrale.

Matching

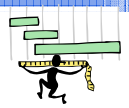
I sistemi biometrici **non forniscono** un match al 100%

Il risultato del match ("punteggio") è confrontato con una **soglia prefissata**, per prendere la decisione finale ("match" o "no match")

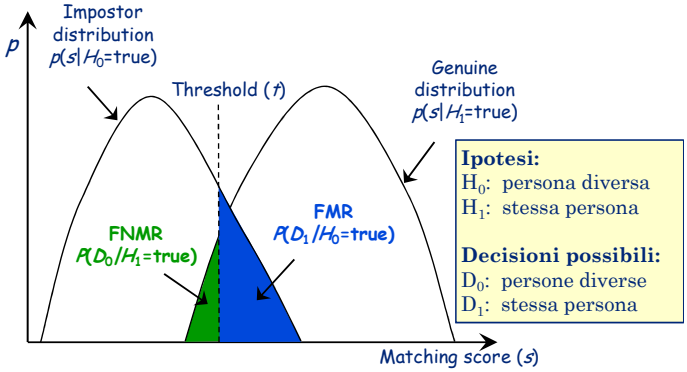
Errori nei sistemi biometrici (1)

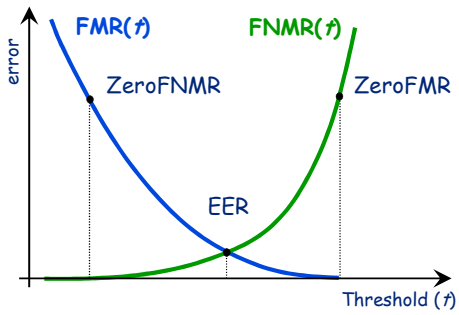
- Uno score è detto *genuine* (autentico) se è il risultato del matching di due esempi della stessa caratteristica biometrica di un individuo; è detto *impostor* se nasce dal confronto tra due esempi di individui diversi.
- Uno score *impostor* che supera la soglia prefissata causa una falsa accettazione (*false match*).
  - False Match (chiamato spesso False Acceptance)
    - misurazioni biometriche di persone diverse sono erroneamente considerate come appartenenti alla stessa persona
- Uno score *genuine* inferiore alla soglia prefissata determina una falsa reiezione (*false non-match*).
  - False Non-Match (chiamato spesso False Rejection)
    - misurazioni biometriche della stessa persona sono erroneamente attribuite a persone diverse

Errori nei sistemi biometrici (2)



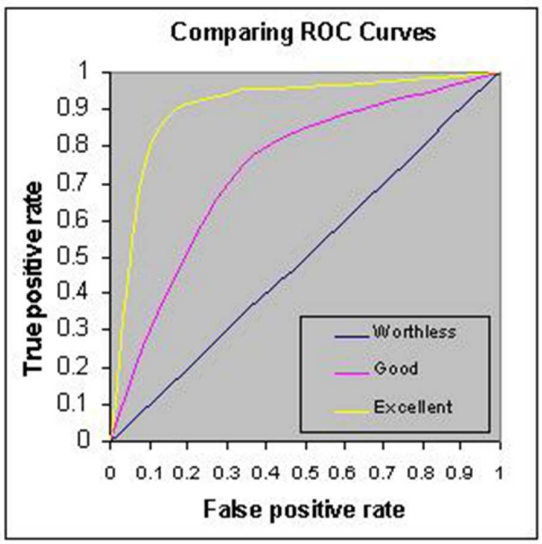
- **False Match Rate (FMR)**
  - Percentuale degli score impostor che superano la soglia.
- **False Non-Match Rate (FNMR)**
  - Percentuale degli score genuine che non superano la soglia.
- **Genuine Match Rate (GMR)**
  - 1-FNMR
- **Equal Error Rate (EER)**
  - Percentuale di errore che si ha quando FMR = FNMR.
- **ZeroFNMR**
  - FMR quando FNMR = 0
- **Zero FMR**
  - FNMR quando FMR = 0





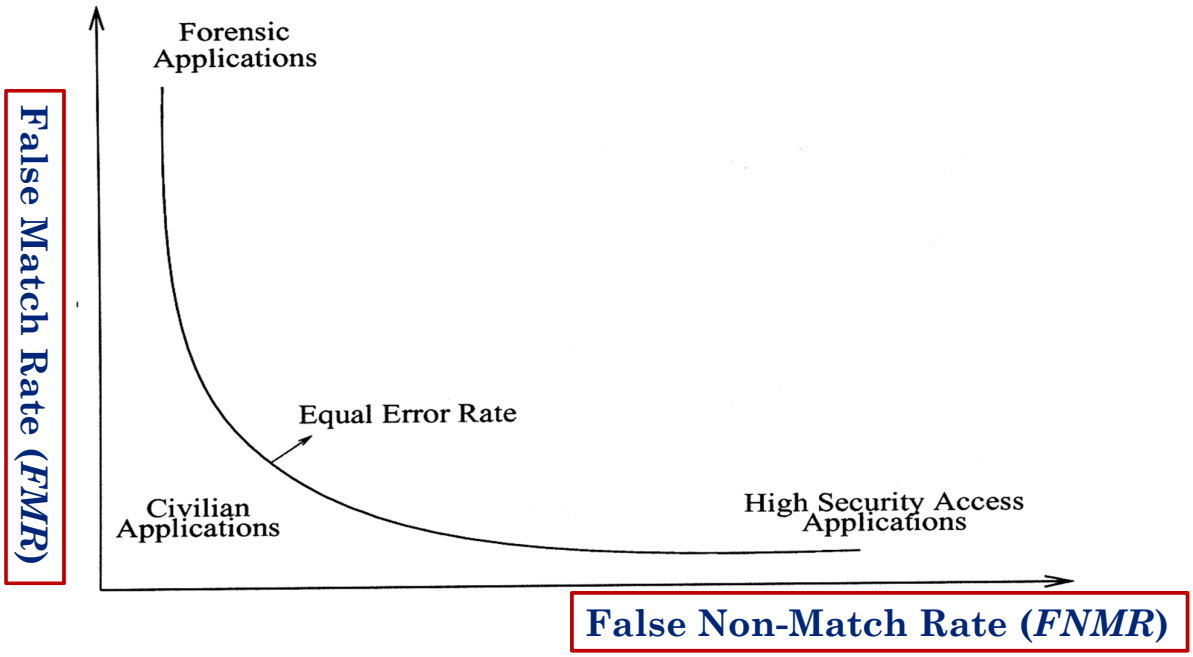
Errori nei sistemi biometrici (3)

- Curva DET
  (Detection Error Tradeoff)
  - Grafico che riporta FMR in funzione di FNMR. Talvolta si adotta una scala logaritmica.
- Curva ROC
  (Receiver Operating Characteristic)
  - Grafico che riporta il Genuine Match Rate (GMR) in funzione in funzione del False Match Rate (FMR).



Applicazioni, FMR e FNMR

Receiver Operating Characteristic: i requisiti in termini di prestazioni sono strettamente legati al tipo di applicazione



Scelta di una tecnologia biometrica (1)

- Qual è la migliore caratteristica biometrica?

Scelta di una tecnologia biometrica (2)

- Per poter sviluppare in modo efficace una soluzione biometrica, è necessario analizzare la specifica applicazione sotto molteplici aspetti
  - Alcuni esempi:
    - È possibile operare in verifica o è necessario operare in identificazione?
    - È un caso di riconoscimento positivo o negativo?
    - Qual è il rischio nel caso di errore di false-match? e di false-non-match?
    - L'utente è interessato/motivato a cooperare?
    - In quale ambiente deve operare il sistema (luci, rumori, ...)?
    - Il processo di riconoscimento è supervisionato?
    - Con quale frequenza gli utenti utilizzano il sistema?
    - Quali sono i rischi per la privacy?
    - ...

Linee guida CNIPA

Tecnologie/applicazioni	impronte digitali	geometria della mano	iride	viso	voce	firma
accesso fisico di massa	buono	ottimo	buono	buono / medio	-	-
accesso fisico a zone sensibili	buono	buono/ medio	ottimo	buono / medio	-	-
accesso logico	ottimo	-	medio	buono/ medio	medio	-
documenti	ottimo	-	buono	ottimo	-	-
transazioni economiche/e-government	buono	-	medio/ buono	medio/ buono	buono	buono
sorveglianza	-	-	-	buono	-	-

Parametri di valutazione

C. **Sicurezza**
- Accuratezza
  - FMR (False Match Rate)
  - FNMR (False Non Match Rate)
  - ROC (Receiver Operating Curve)
  - EER (Equal Error Rate) o CER (Crossover Error Rate)
  - Zero FMR
  - Zero FNMR
- Resistenza a contraffazioni
  - Vivezza
  - Falsificazione

D. **Robustezza**
- Rispetto alla stabilità della caratteristica biometrica
- Rispetto ad alcuni individui, popolazioni, lavoratori
- Rispetto all'ambiente

C. **Usabilità**
- Interazione con l'utente
  - Facilità d'uso
  - Praticità
  - Training
  - Enrolment
- Interazione con l'amministratore
  - Praticità
  - Strumenti di amministrazione
  - Necessità di supervisione
- Efficienza
  - Nella fase di enrolment
  - Nella fase di identificazione/verifica

D. **Accettabilità**
- Della caratteristica biometrica
- Delle operazioni di enrolment e riconoscimento

E. **Vari**
- Costo
- Occupazione di spazio
- Dimensione del template
- Possibilità di integrazione
- Adattabilità

Sicurezza del dato biometrico

- Si definisce come l'insieme di misure adottate nelle fasi di registrazione e memorizzazione dei template, nelle modalità di trasporto e nell'integrazione del dato all'interno del sistema. Per dispositivi di trasporto si intendono il database, i collegamenti di rete e i dispositivi d'acquisizione dati. Si distinguono principalmente:
  - attacchi ai dispositivi biometrici, (biometric device attack) nella registrazione e memorizzazione dei template
  - attacchi contro i link (biometric device-to-computer link attack) nelle modalità di trasporto del dato: database, collegamenti di rete e i device di acquisizione dati;
  - attacchi contro i collegamenti tra client e host (client/server-network link attack);
  - attacchi sui processori delle smart card (power analysis attack).

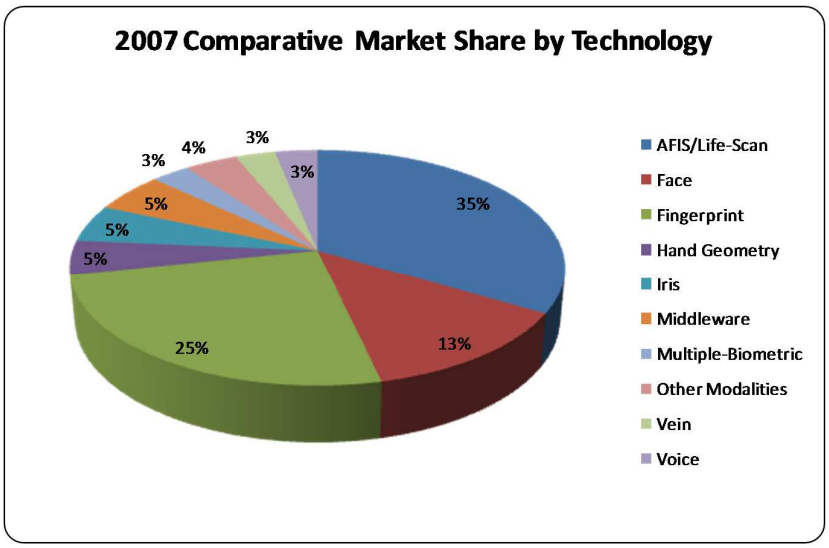
La sicurezza è una catena che spesso si rompe nell'anello più debole

Attacchi ai sistemi biometrici

- Attacchi ai dispositivi biometrici nella registrazione e memorizzazione dei template:
  - smontando o sostituendo alcuni componenti del sistema per catturare le informazioni
- Attacchi ai collegamenti:
  - tra dispositivi, server e workstation
- Risposta agli attacchi → crittografia
- Orientati al software utente → protezione del software
- Client/server – attacchi ai collegamenti di rete → protocolli per transazioni sicure (SSL e TLS)
- Attacchi a smart-card:
  gli attacchi ai processori possono essere evitati utilizzando processori non vulnerabili di prezzo elevato oppure adottando appropriati algoritmi di crittografia

Confronto tra diverse caratteristiche biometriche (1)

- **Universalità**
- **Unicità**
- **Persistenza**
- **Facilità di acquisizione**
- **Prestazioni**
- **Accettabilità**
- **Contraffazione**

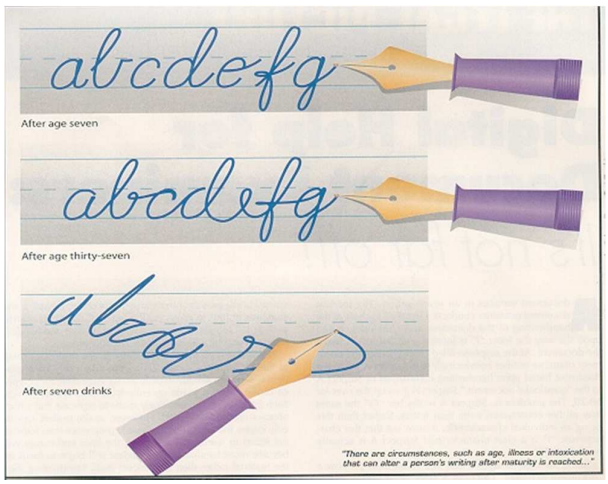


Confronto tra diverse caratteristiche biometriche (2)

Caratteristiche biometriche	Universalità	Unicità	Persistenza	Collezionabilità	Prestazioni	Accettabilità	Contraffazione
DNA	H	H	H	L	H	L	L
Orecchio	M	M	H	M	M	H	M
Volto	H	L	M	H	L	H	H
Termogramma facciale	H	H	L	H	M	H	L
Impronta	M	H	H	M	H	M	L
Andatura	M	L	L	H	L	H	M
Geometria della mano	M	M	M	H	M	M	M
Vene della mano	M	M	M	M	M	M	L
Iride	H	H	H	M	H	L	L
Stile di battitura	L	L	L	M	L	M	M
Odore	H	H	H	L	L	M	L
Retina	H	H	M	L	H	L	L
Firma	L	L	L	H	L	H	H
Voce	M	L	L	M	L	H	H

Variabilità intra-classe

Due impronte dello stesso dito



Similarità inter-classe

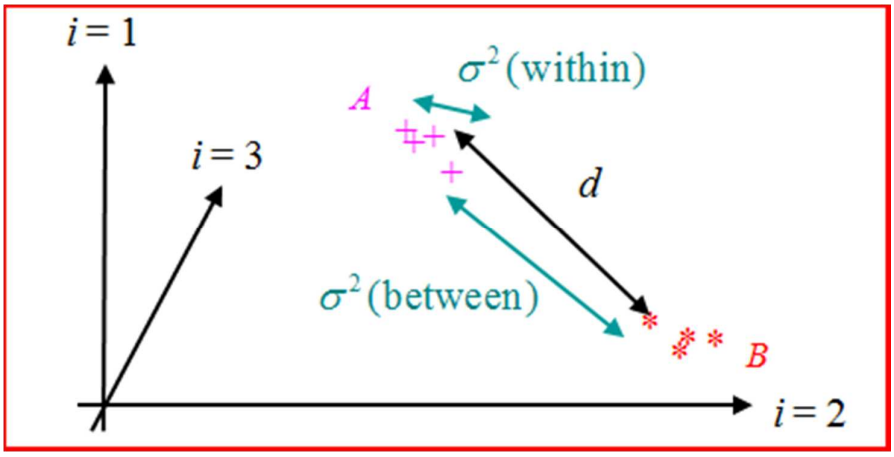
Due persone diverse possono avere caratteristiche biometriche molto simili

Gemelli

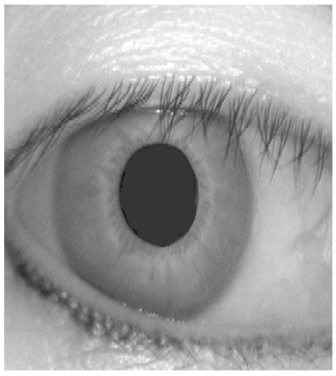
Padre e figlio

Comportamento ideale

- Esempio: nel caso in cui i template siano rappresentati come punti in un spazio a più dimensioni in cui sia definito il concetto di distanza **d** tra due punti
- è desiderabile che la varianza inter-classe sia molto maggiore della variabilità intra-classe



Rumore nei dati acquisiti

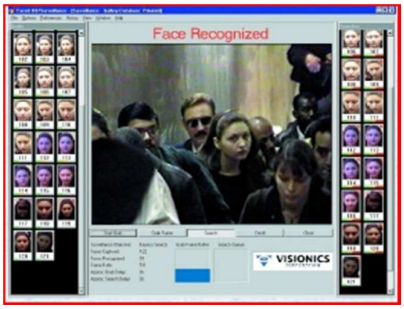


Percentuale di errori allo stato dell'arte

	Test	Parametri	False Reject Rate	False Accept Rate
Impronta	FVC [2006]	Sensore ottico 569dpi	0.02%	0.1%
Volto	FRVT [2006]	Illuminazione variabile Interno / esterno	20%	0.1%
Voce	NIST [2004]	Indipendente dal testo	5-10%	2-5%
Iride	ITIR [2005]	Ambiente indoor	0.99%	0.94%

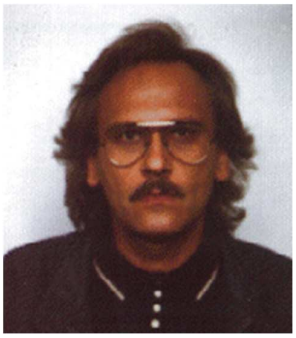
Volto

- **Una delle caratteristiche biometriche più accettate**
  - È uno dei metodi di riconoscimento utilizzati più comunemente dagli esseri umani
  - L'acquisizione del volto è un'operazione non intrusiva
- **Un problema di riconoscimento molto difficile**
  - Invecchiamento, diverse espressioni facciali
  - Variazioni nell'ambiente (es. sfondo complesso, illuminazione)
  - Variazioni nella posizione del volto rispetto alla telecamera
- **Non rappresenta la scelta migliore per applicazioni che richiedono un elevato grado di sicurezza**
  - Bassa resistenza agli attacchi



Al Gore e Bill Clinton? Maio e Maio?

Bush padre e figlio? Chi delle due?

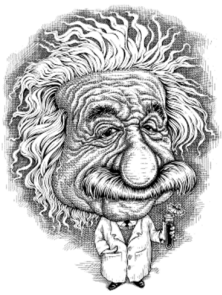


La stessa persona può presentarsi con aspetti del volto “molto diversi”

Quante facce?

Caricature


Vincent Van Gogh


Albert Einstein


Bill Gates


Bill Cosby


G.W. Bush


Jim Carrey

- Gli esseri umani possono riconoscere volti da caricature e fumetti
- Il volto di ciascun individuo è caratterizzato da alcuni particolari

www.magixl.com
www.pritchettcartoons.com
www.interchile.com/benjamin

Localizzazione del volto (1)


sfondo semplice / sfondo complesso


condizioni d'illuminazione differenti


rotazioni


scale diverse (distanza dalla telecamera)

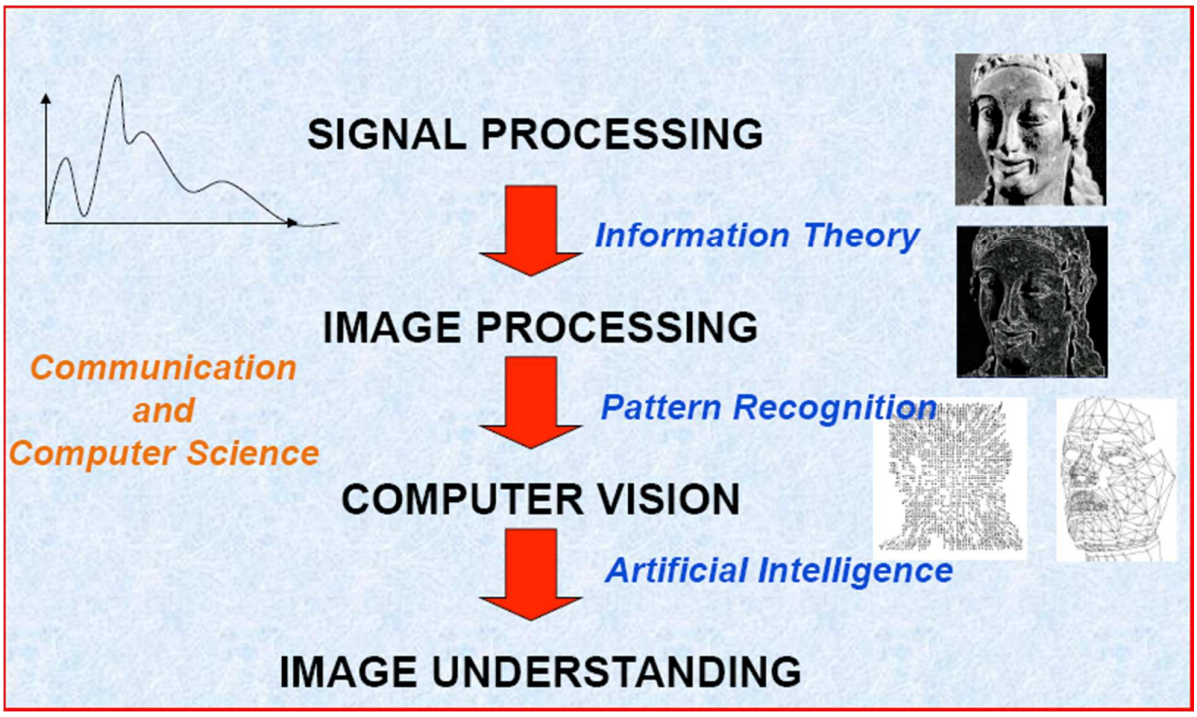
Localizzazione del volto (2)

Riconoscimento del volto: applicazioni

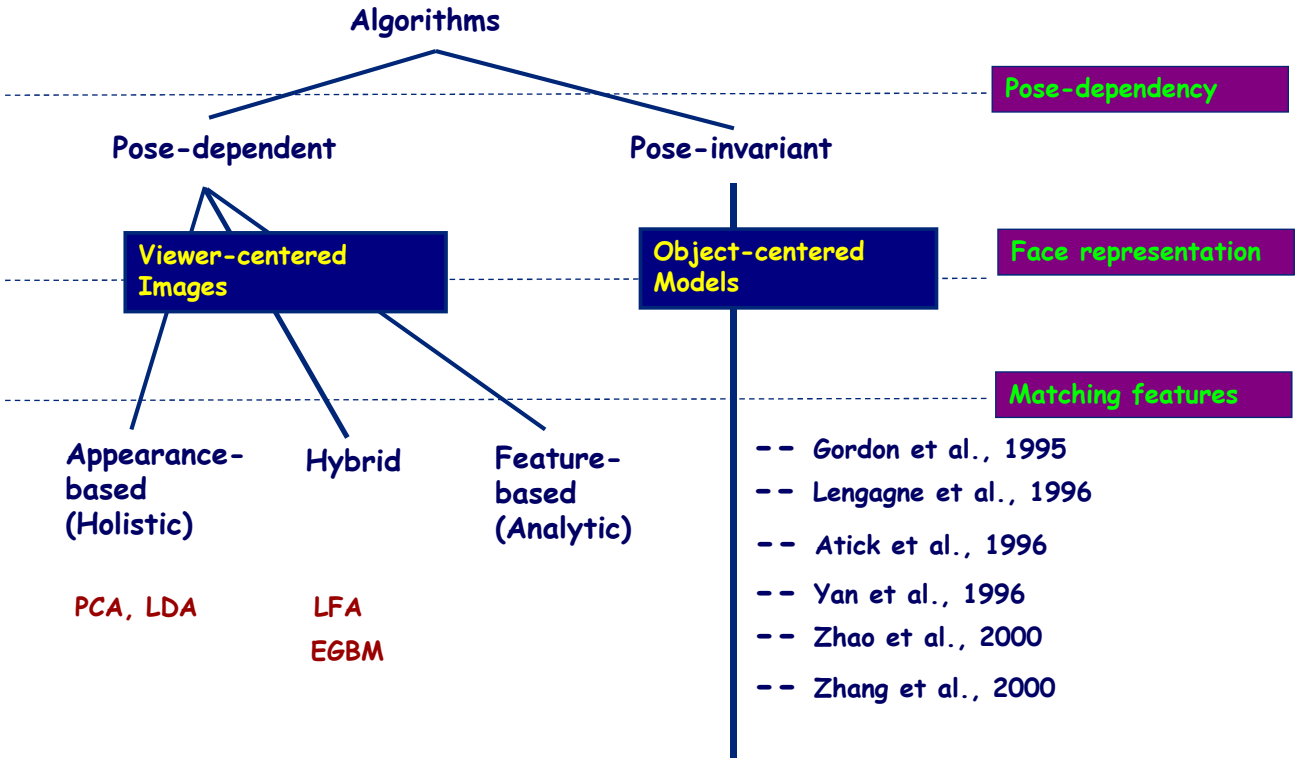
- Video sorveglianza automatica (aeroporti, super bowl)
- Controllo accessi
- Identificazione da foto segnaletiche
- Comunicazioni multimediali (es. facce sintetiche)
- Human computer interface (HCI), es. controllo attività automobilisti

Video sorveglianza: Super Bowl Face Scan

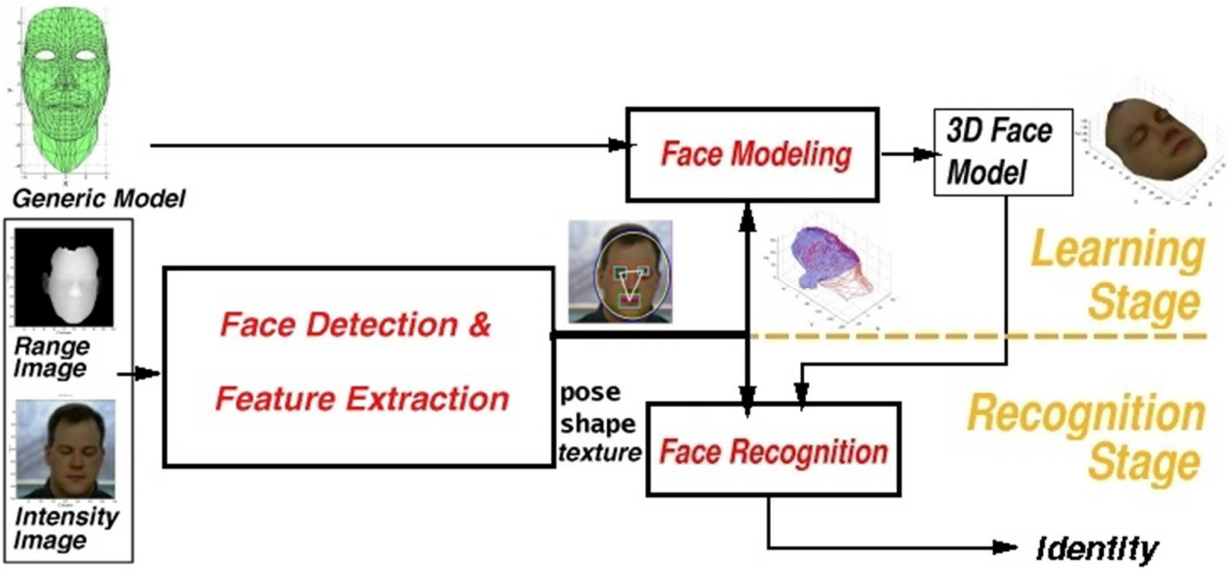
Le basi per il riconoscimento del volto



Tassonomia dei metodi per il riconoscimento del volto

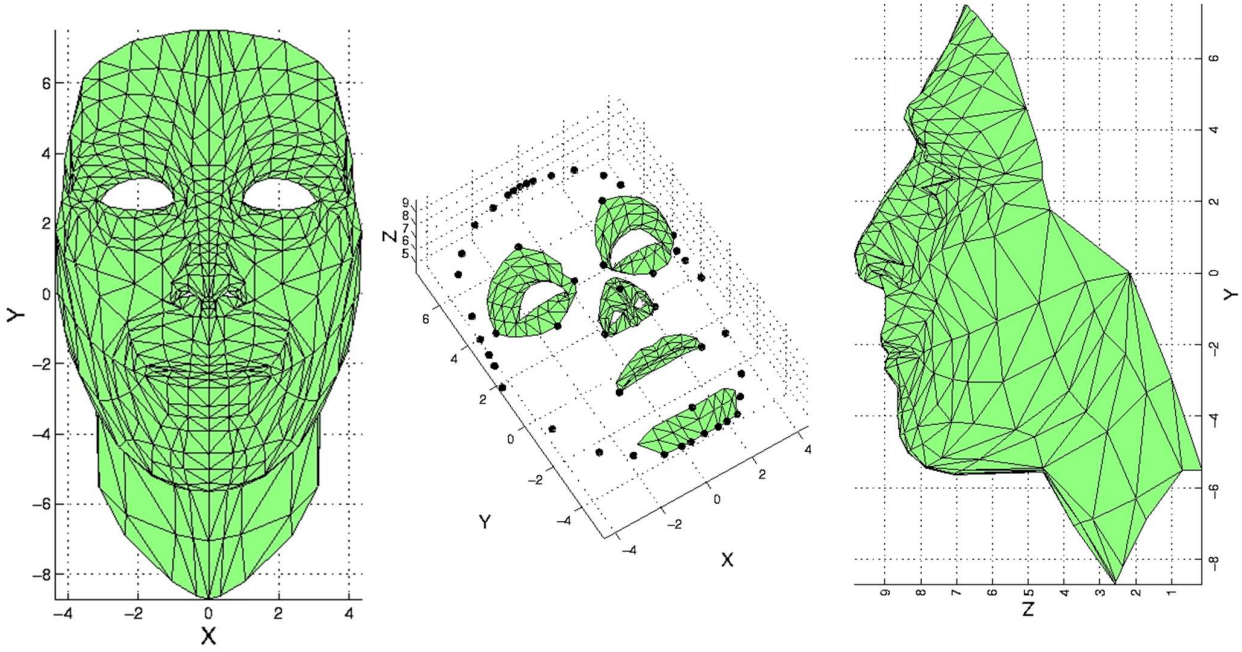


Riconoscimento del volto basato su modelli



Water's Animation Model

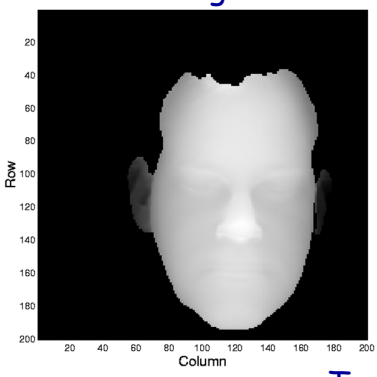
- Una griglia triangolare 3D, e le feature che ne fanno parte



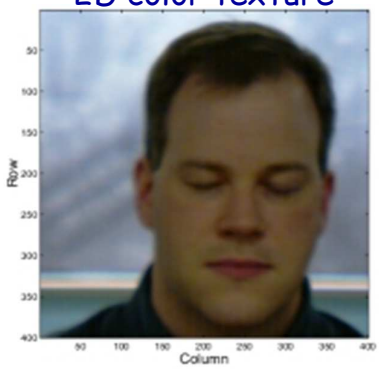
Frontal View **Features** **Profile View**

Range & Color Images

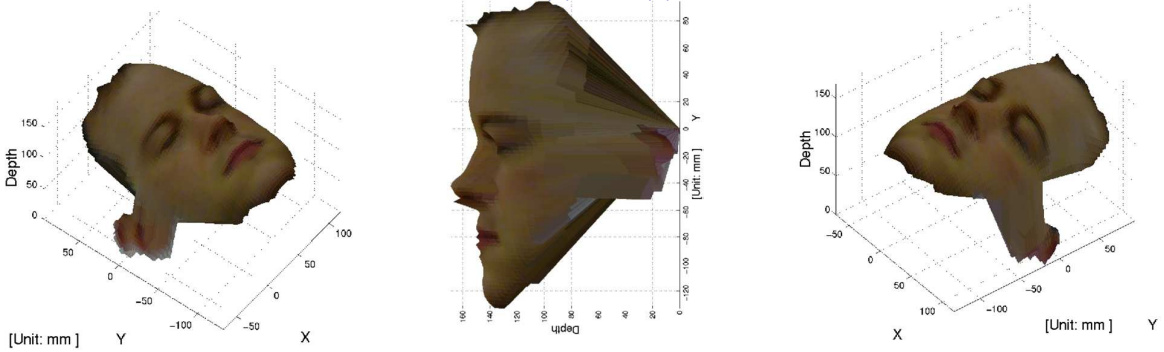
2.5D range data



2D color texture



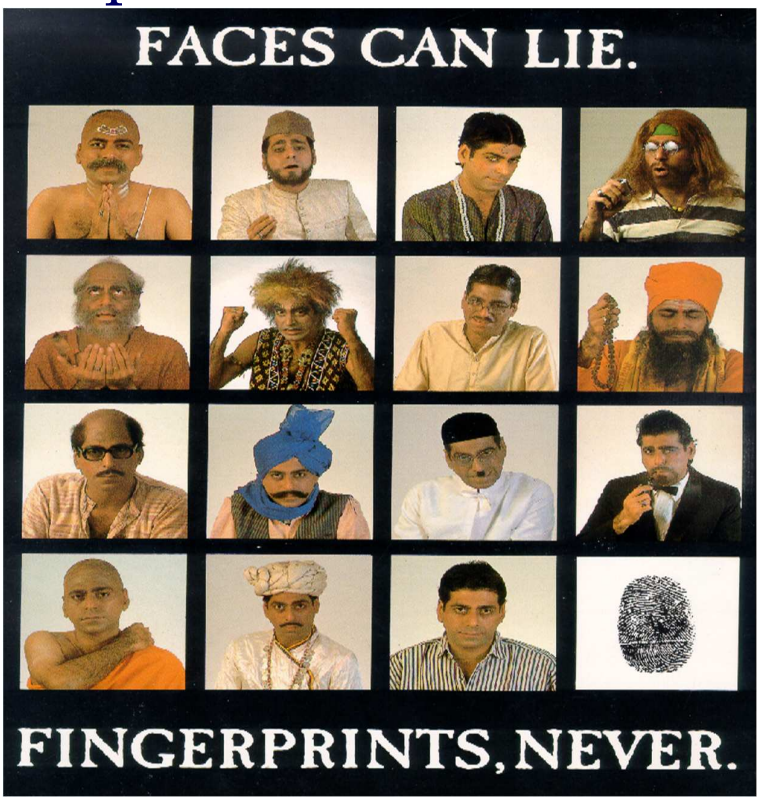
Texture-mapped appearance



Resistenza alla contraffazione

Fonte: c't Magazine 2002

Volto o impronta?



Impronte digitali

- Vantaggi
  - Elevato potere discriminante e unicità
  - Non mutano nel corso della vita di una persona (anche se possono variare temporaneamente a causa di tagli e abrasioni o delle condizioni meteorologiche)
  - Pubblicamente riconosciute come affidabili
  - Gemelli identici hanno impronte diverse
- Svantaggi
  - Sporcizia sul sensore o sul dito può compromettere il riconoscimento
  - Alcune persone presentano impronte di bassa qualità intrinseca
  - Associazione con "criminalità"

Acquisizione impronte

- Acquisizione off-line
  - Tecnica a inchiostro
  - Impronte latenti

Acquisizione on-line
  - Optical sensors
  - Silicon-based sensors
  - ...

Alcuni tipi di sensori

- Optical, capacitive, ultrasound, pressure, thermal, electric field

Localizzazione minuzie

- **Problemi legati agli individui**
  - Le persone più anziane e i lavoratori manuali possono avere ridge line poco prominenti e il pattern dell'impronta può risultare illeggibile
  - Sospetti e criminali non hanno interesse a collaborare durante l'acquisizione delle impronte

- **Problemi di efficienza**
  - Nei sistemi automatici il processo di estrazione delle minuzie deve essere molto efficiente.

Matching: problema difficile

- Spostamenti e rotazioni, parziali sovrapposizioni, distorsioni non lineari, pressione e condizioni della pelle, rumore, errori nell'estrazione di feature

scarsa sovrapposizione

condizioni della pelle molto diverse

elevata distorsione non lineare

Coppie di immagini della stessa impronta, che erroneamente non sono state riconosciute come tali dalla maggior parte degli algoritmi sottomessi a FVC2002

IN THE WORKS

No Need for a Wallet

Invidos is one company in California with a new pay-with-your-fingerprint technology. Pilot programs have begun in fast-food restaurants and will soon expand to local supermarkets.

❶ At the checkout line, an optical scanner registers the customer's fingerprint and the customer types in his or her phone number.

❷ The fingerprint is encrypted and sent to a remote database, where it is matched to a print the customer has on file.

❸ The customer chooses a payment type from the checking account or credit card information on file, and payment is routed through the register just like credit cards or paper checks.

Source: Invidos

Thumb Is the New Currency At Store, at Bank, on the Job

February 20, 2002

The New York Times ON THE WEB

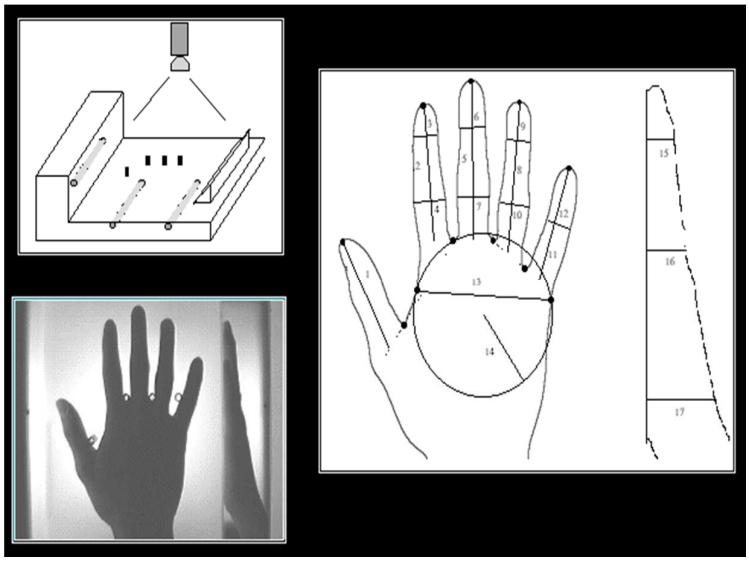
Resistenza alla contraffazione

- Con gli opportuni strumenti e la giusta esperienza, è possibile creare un dito finto (silicone, gelatina, ...) a partire da quello vero o da un'impronta latente (più arduo)
- A oggi non sembrano esistere soluzioni complete al problema del riconoscimento di impronte contraffatte (anche se alcuni sensori risultano più difficilmente attaccabili di altri)
- Finger aliveness detection: uno dei settori in cui la ricerca scientifica è più attiva negli ultimi anni

Geometria della mano e del dito

- **Caratteristiche della mano (es., lunghezza delle dita)**
  - Relativamente invarianti (*anche se non molto discriminanti*)
  - Richiedono poco spazio per la memorizzazione (~ 20 bytes), caratteristica importante per sistemi con larghezza di banda e memoria limitate
- **Tecnologie tipicamente impiegate per la verifica** (non adatte per applicazioni di identificazione)
- **Il dispositivo di acquisizione è solitamente abbastanza voluminoso**
- **Dispositivi per l'acquisizione della forma di dita**
  - Misurano solo la forma di un dito o due dita
  - Preferibili per le dimensioni ridotte

Esempi geometria mano e dito



3D- hand geometry

Geometria della mano

Time & Attendance Terminal

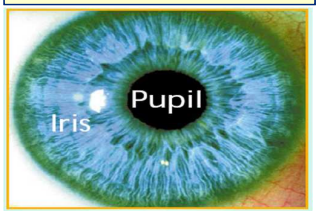
HandPunch Recognition Systems

Geometria del dito

FingerPhoto BioMet Partners

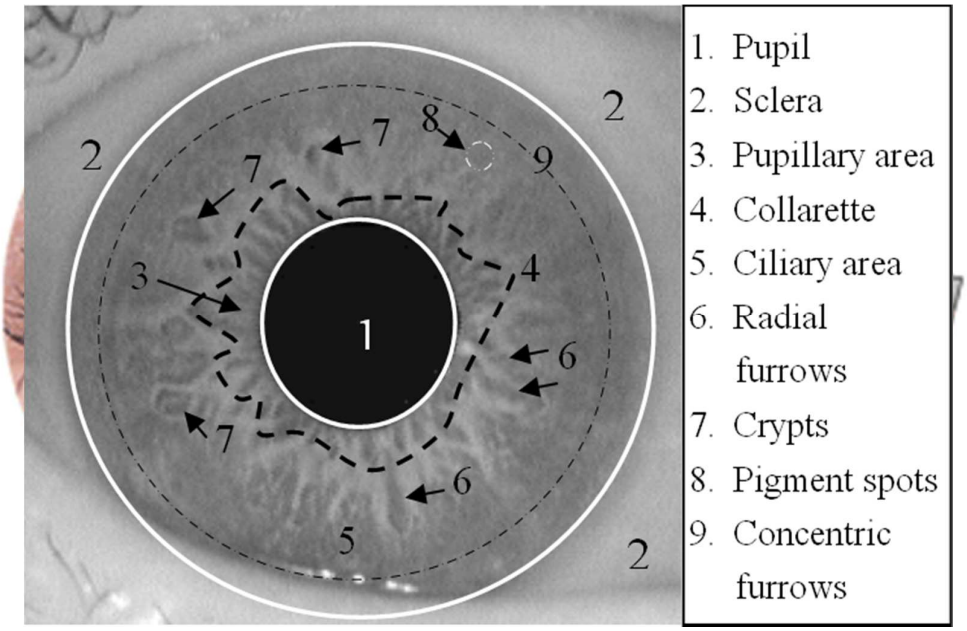
Iride

Iride: la corona di tessuto colorato che circonda la pupilla dell'occhio.



- Vantaggi
  - Estremamente discriminante
  - Stabile e invariante durante tutto il corso della vita
- Svantaggi
  - Richiede un appropriato controllo ambientale
  - Tecnica che a volte può essere considerata invasiva (a seconda del dispositivo adottato)
  - Costi medio/alti (telecamere a elevata precisione)
  - L'acquisizione dell'iride può richiedere un certo grado di collaborazione da parte del soggetto
- Adatta per applicazioni che richiedono un elevato grado di sicurezza

Anatomia dell'iride



Storia del riconoscimento dell'iride

- **1936, Frank Burch, un oftalmologo, affermò l'unicità dell'iride e il suo possibile impiego per l'identificazione di persone.**
- **1987, Aran Safir e Leonard Flom, due oftalmologi, proposero il riconoscimento automatico dell'iride e registrarono un brevetto (anche se non sapevano come realizzare un metodo idoneo).**
- **1991, Johnson (Los Alamos National Laboratory) descrisse come realizzare in pratica un sistema di riconoscimento.**
- **1993, John Daugman propose un efficiente metodo che è attualmente impiegato in sistemi commerciali.**
- **1996, Richard Wildes sviluppò un diverso sistema che comprendeva sia l'acquisizione dell'immagine dell'iride sia un algoritimo di riconoscimento.**
- **2000, CASIA sviluppò il primo sistema di riconoscimento dell'iride in Cina**
- **2005, Sarnoff presentò un sistema per riconoscere persone in movimento a distanza di 3 metri.**

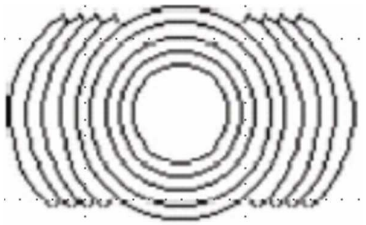
Iride: un tipico approccio (1)

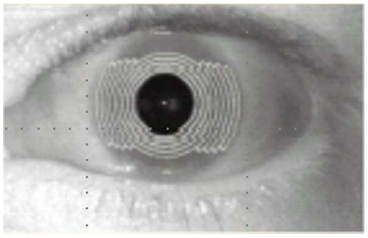
1. L'utente si posiziona a 1-3 piedi di distanza dal sistema costituito da **tre telecamere standard**

2. Due telecamere grandangolari acquisiscono l'immagine del busto dell'utente. Utilizzando tecnologie sviluppate appositamente per questo problema, il sistema determina la posizione degli occhi.

3. Una terza telecamera focalizza l'occhio e acquisisce una singola immagine in bianco e nero. L'utente può essere riconosciuto anche in presenza di occhiali, lenti a contatto o di notte. Se necessario l'immagine può essere ruotata per correggere l'eventuale inclinazione della testa

Iride: un tipico approccio (2)



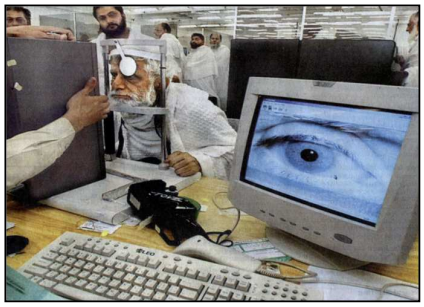


4. Il sistema usa una griglia circolare come guida per codificare il pattern nell'iride
5. La griglia è sovrapposta all'immagine dell'occhio. Il sistema analizza la presenza di luci e ombre nell' area dell'iride e la loro distribuzione all'interno della griglia, generando un "codice" (ad es. 512 byte) per ciascun individuo. Il sistema funziona correttamente anche nel caso in cui le ciglia o la palpebra occludano parte della griglia.
6. Il sistema confronta il codice con quello memorizzato nel database. L'intero processo, dall'acquisizione della prima immagine all'identificazione, richiede circa due secondi.

Alcune applicazioni

Access control

Airport



Homeland security

Welfare distribution

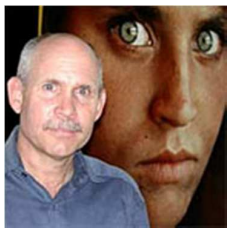
Missing child identification

ATM

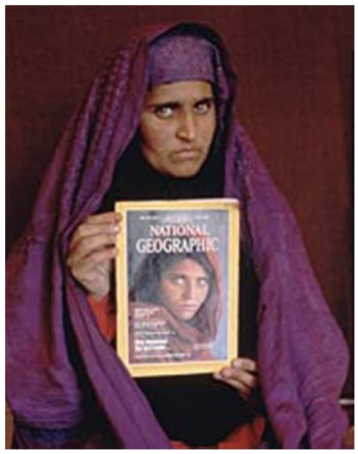
Difficoltà nell'acquisizione

- Small size (11mm)
- High resolution image (200 pixels)
- Narrow depth of field
- Must be optically on-axis
- Stop and stare
- Near infrared illumination
- Specular reflections
- Eyeglasses

Sharbat Gula (1)

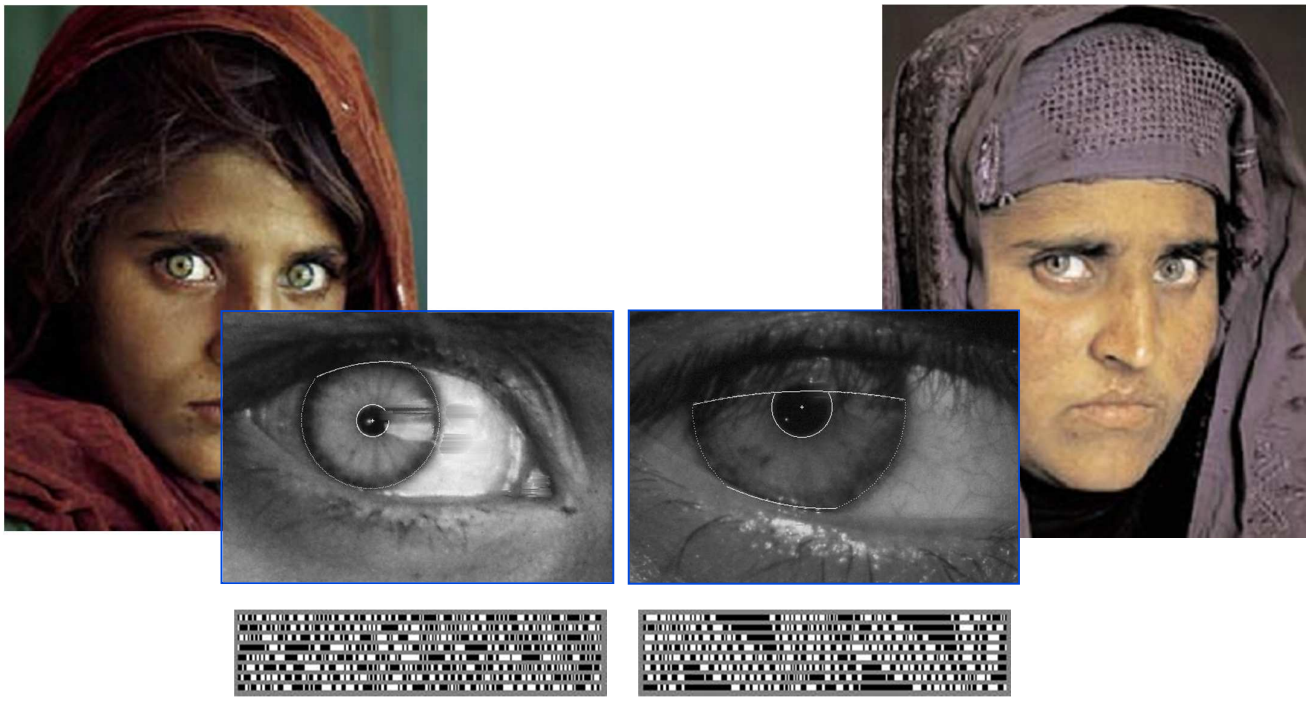


Fotografie di Steve McCurry



(Left photo © Steve McCurry. Right photo Steve McCurry, © National Geographic Society.)

Sharbat Gula (2)



HD=0.31

Resistenza alla contraffazione

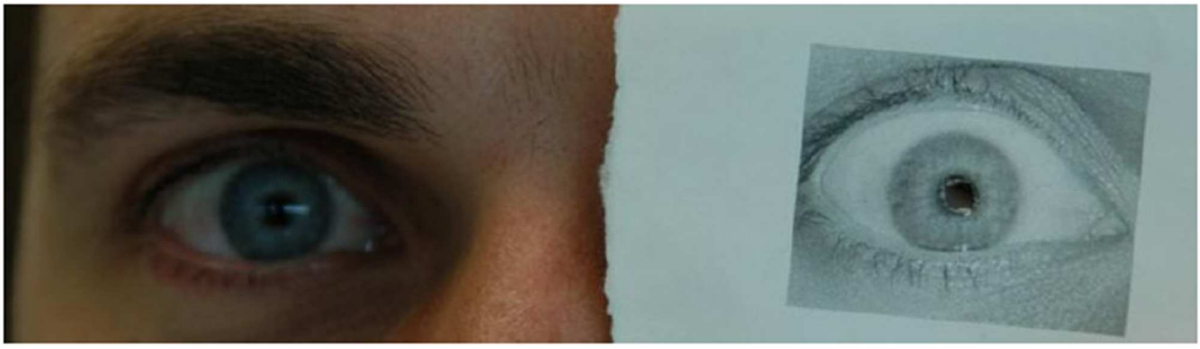


Figure 5-21: Original live iris and the paper spoof

Source: FIDIS Deliverable D6.1 "Forensic Implications of Identity Management Systems"

Scansione della retina

Source: www.cnn.com

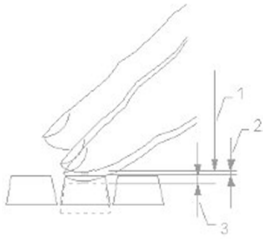
- Vantaggi
  - Estremamente discriminante
  - Una delle caratteristiche biometriche più sicure (è molto difficile modificare o riprodurre la vascolarizzazione della retina)
- Svantaggi
  - Richiede collaborazione e uno sforzo consapevole da parte dell'utente
  - È una tecnica invasiva – bassa accettabilità
  - Costi molto elevati
- Adatta per applicazioni che richiedono un grado di sicurezza molto elevato

Firma

Sono possibili approcci statici (geometria della firma) e dinamici (accelerazione, velocità, traiettoria, pressione, …).
Si ricorre a particolari sensori, ad es. tavolette grafiche per gli approcci dinamici o scanner b/n per l'analisi statica della firma

- Vantaggi
  - User friendly
  - Già accettata e utilizzata in molte transazioni amministrative, legali e commerciali
- Svantaggi
  - Cambia con il passare del tempo
  - È influenzata dalle condizioni fisiche ed emotive del soggetto
  - La firma di alcune persone è molto variabile (anche in due esempi consecutivi)
  - **I falsari di professione possono riprodurre la firma e ingannare il sistema**

Stile di battitura

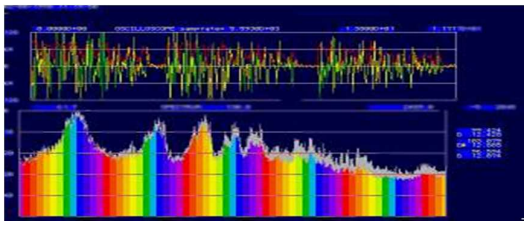


Si ipotizza che ciascuna persona scriva sulla tastiera in modo caratteristico (misure: **"dwell time" e "fight time")**

Questa caratteristica biometrica comportamentale ***non è unica*** per ciascun individuo ma può esibire, in alcune applicazioni, un potere discriminante sufficiente ai fini della verifica di identità

- **Vantaggi**
  - Non richiede la presenza di ulteriori strumenti hardware collegati al PC
  - Non intrusiva
  - Appropriata per l'immissione di grandi quantità di dati
- **Svantaggi**
  - Bassa affidabilità e sicurezza
  - Forte variabilità nei pattern di battitura osservati in alcuni individui
  - Problemi di standardizzazione delle tastiere
- **Approcci tipici**
  - Reti neurali
- **Sistemi commerciali: BIOPASSWORD- Net Nanny**

Voce



- Vantaggi
  - Accettabilità elevata da parte dell'utente
- Svantaggi
  - Caratteristica comportamentale che può mutare nel tempo ed essere influenzata da fattori fisici ed emotivi, e dal rumore dell'ambiente
  - Bassa sicurezza, facilmente falsificabile
- Approcci
  - Reti Neurali, Hidden Markov Models, Vector Quantization, Dynamic Time Warping
- Applicazioni
  - Sistemi locali/remoti, dipendenti/indipendenti dal testo
  - Di fatto l'unica tecnologia possibile nel caso di accesso via telefono

Termogramma facciale

- Vantaggi
  - Accettabilità elevata da parte dell'utente
  - Elevata unicità della caratteristica
  - Elevata sicurezza
- Svantaggi
  - Caratteristica che può essere influenzata da diversi fattori esterni (fonti di calore)
  - Costi elevati

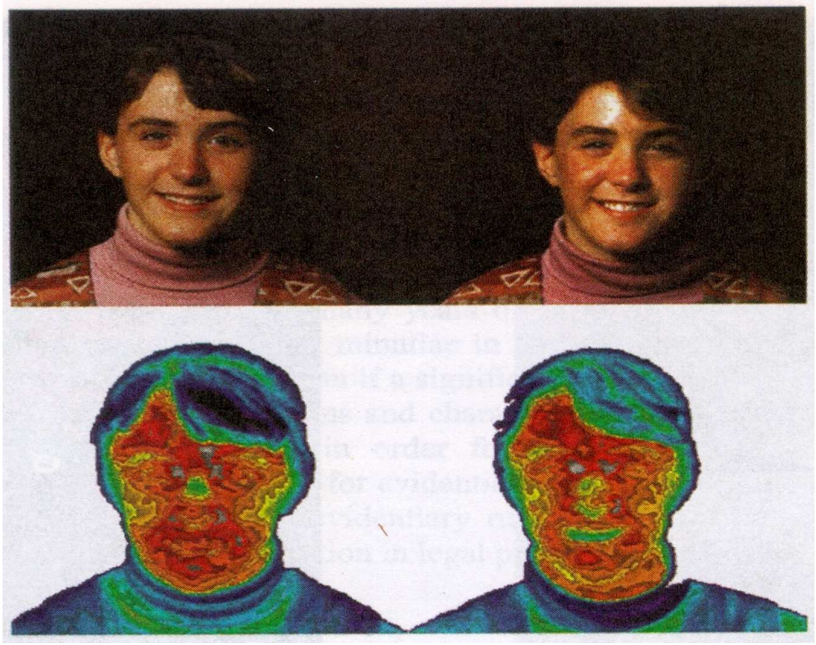
Modalità di acquisizione

- Sensore sensibile all'emissione di raggi infrarossi da parte della faccia di una persona

Applicazioni

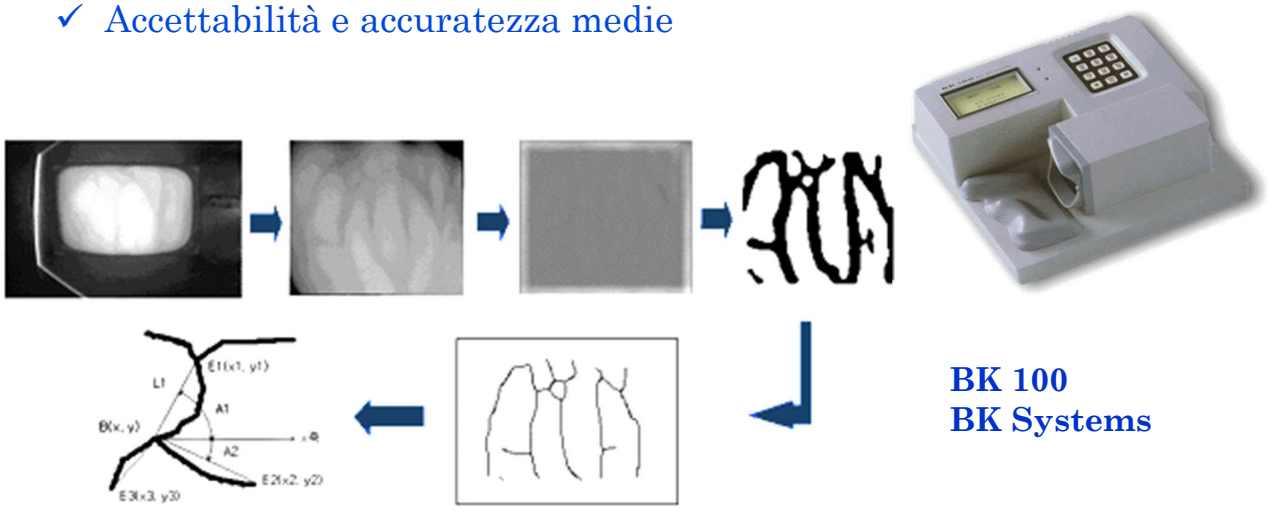
- Identificazione di soggetti che hanno assunto droga

Termogramma di due gemelli



Vene delle mani

- ✓ Si fa ricorso a sensori a infrarossi per analizzare il dorso del pugno chiuso per determinare la struttura delle vene
- ✓ Accettabilità e accuratezza medie



BK 100
BK Systems

Resistenza alla contraffazione

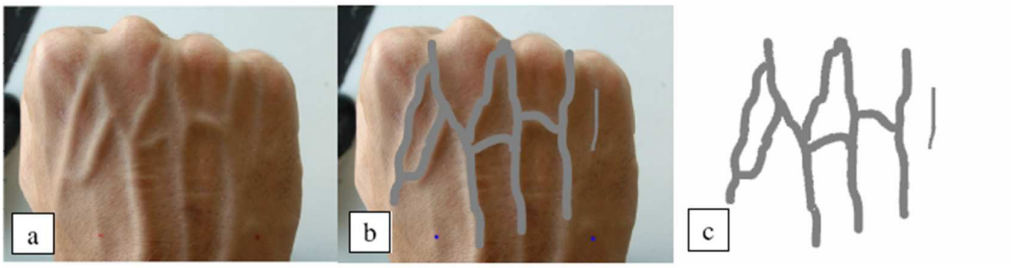


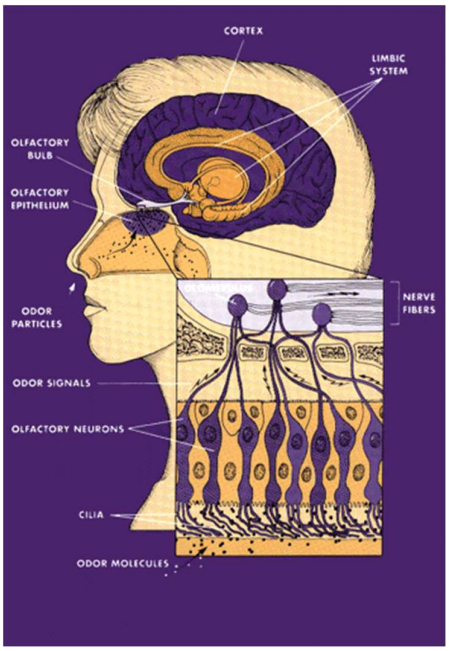
Figure 5-24: Obtaining a vascular pattern using a digital camera. a) Image of the back of a hand shot in daylight using a common digital photo camera. b) Visible veins manually traced using image processing software. c) The drawn layer ready for printing

Figure 5-27: Vascular pattern spoofs effective with liveness detection turned off. a) The copy of a vascular pattern stuck on a bottle. b) The bottle spoof verified as an authorised user. c) The copy of a vascular pattern stuck on a hand (left), next to the original hand (right) of an authorised user. d) The hand spoof verified as the authorised user

Source: FIDIS Deliverable D6.1 "Forensic Implications of Identity Management Systems"

Odore

- Vantaggi
  - Elevata unicità e permanenza della caratteristica
- Svantaggi
  - Non è chiaro come si possa riconoscere l'odore di un corpo umano in presenza di deodoranti o altri composti chimici nell'ambiente circostante



Modalità di acquisizione

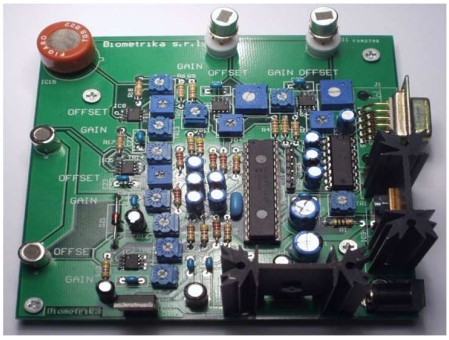
- Array di sensori chimici sensibili a vari composti

Applicazioni

- Non esistono sistemi commerciali di verifica di identità basati sull'odore

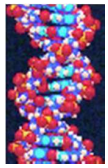
Nasi elettronici

Presso i laboratori Caltech è stato studiato un naso elettronico con circa 10000 sensori su un chip di 1 cm^2.
Innumerevoli sono le applicazioni per test di qualità di cibi e bevande, per rilevare la presenza di sostanze nocive nell'ambiente, per diagnosticare malattie, ……

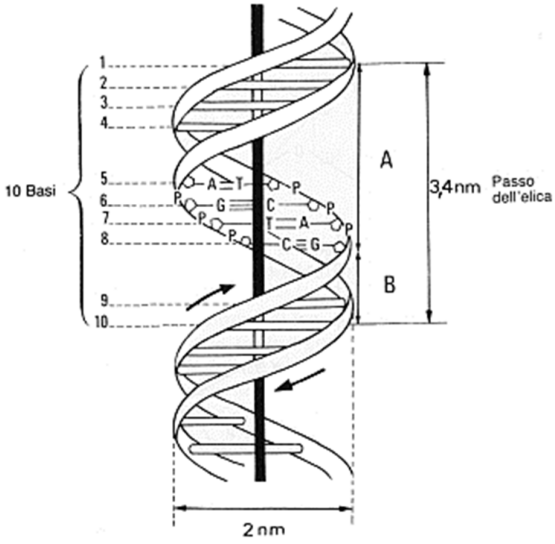


Presso il Biometric Systems Laboratory è stata studiata l'applicazione dei sensori di odore al problema della verifica della vivezza di impronte digitali.
Il sistema è in grado di "riconoscere" l'odore di sostanze usate tipicamente per fabbricare impronte artificiali (gelatina, silicone, lattice).

DNA (Acido DesossiriboNucleico)



Il DNA è il componente fondamentale dei cromosomi delle cellule e porta il messaggio genetico; la molecola di DNA è formata da nucleotidi ciascuno caratterizzato da una base azotata
Adenina A, Citosina C, Timina T, Guanina G. A può accoppiarsi solo con T tramite due legami a idrogeno, G solo con C con tre legami a idrogeno.

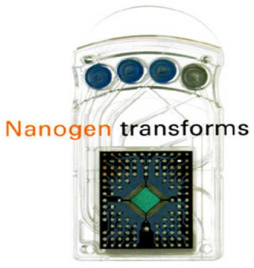


La struttura a doppia elica mostra due filamenti che scorrono in senso opposto. I nucleotidi lungo una catena della doppia elica possono essere disposti in un ordine qualunque, ma la loro sequenza determina quella dell'altra catena, infatti le basi sono complementari (A con T e G con C).

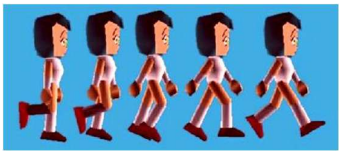
Il DNA porta l'informazione genetica, codificata nella sequenza delle basi. Il numero di basi appaiate varia da circa 5000 per i virus a circa 5 miliardi nei 46 cromosomi umani.

Identificazione del DNA

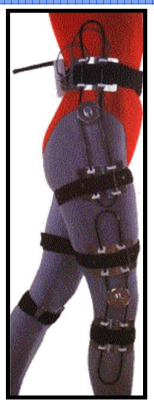
- Gli uomini condividono dal 99.5% al 99.9% del proprio DNA; le differenti piccole porzioni del genoma umano contengono milioni di coppie base, e ciò rende unico il DNA di un individuo, a parte il caso di due gemelli identici (monozigoti).
- I metodi chimici per l'analisi di particolari frammenti di DNA sono lenti e laboriosi, non completamente automatici.
- A causa della scarsa accettabilità (per ovvi motivi di pericolo di violazione della privacy) non c'è oggi interesse a investigare su metodi non intrusivi completamente automatici, per applicazioni diverse da quelle in ambito forense.
- Nanogen ha recentemente sviluppato un chip per velocizzare il processo di identificazione.



Andatura



Nixon et al, in Jain et al Eds.: *Biometrics*, 1999



Clinical Gait Analysis

MIE Medical Research

- Vantaggi
  - Elevata accettabilità, non necessario contatto,
  - acquisibile a distanza
- Svantaggi
  - Caratteristica comportamentale, bassa unicità e permanenza, bassa sicurezza

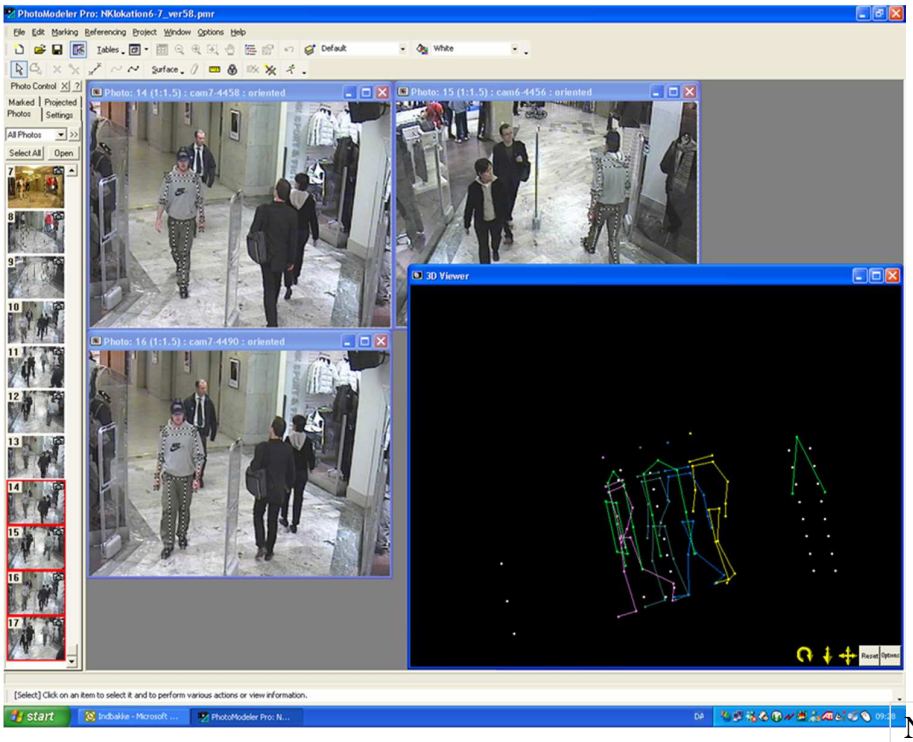
Modalità di riconoscimento

- Analisi di sequenze di immagini, con elevati tempi di calcolo; uso di modelli complessi.

Applicazioni potenziali

- In vari settori tra cui sorveglianza, applicazioni forensi, immigrazione, medicina.

Andatura: esempio d'applicazione



N. Lynnerup and J. Vedel "Forensic Sci, 2005

Orecchio

- Vantaggi
  - Elevata permanenza, elevata accettabilità
- Svantaggi
  - Unicità media

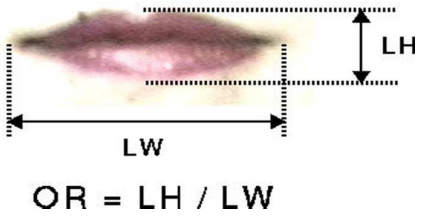
Modalità di riconoscimento

- Essenzialmente sono considerati i contorni e la forma della cartilagine dell'orecchio.

Applicazioni

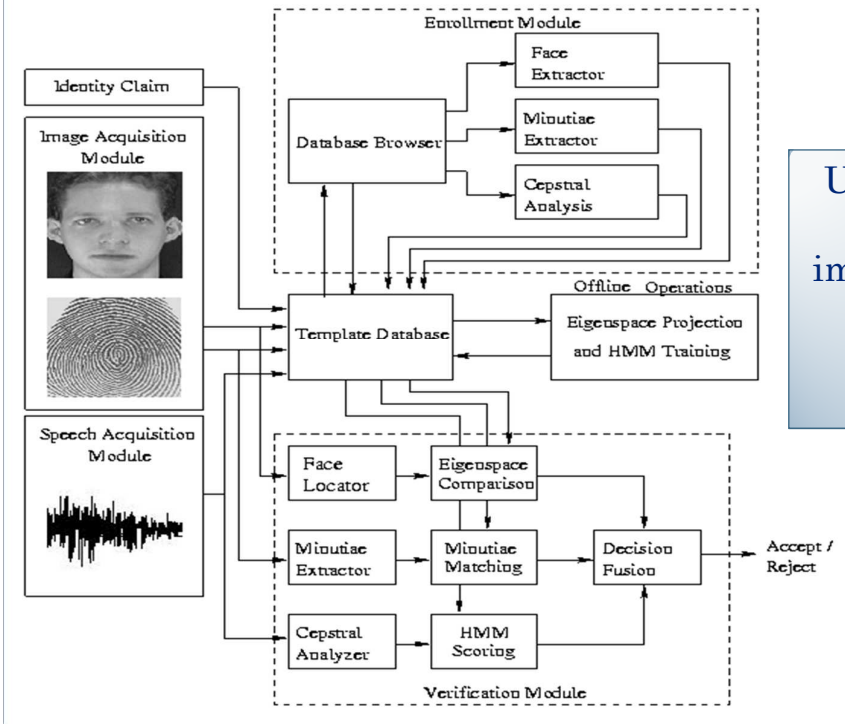
- Il National Training Centre for Scientific Support to Crime Investigation ha collezionato un database di impronte di orecchie umane, al fine di investigare la possibilità di discriminare persone sulla base di questa caratteristica. A volte infatti queste impronte si trovano sulla scena del crimine.

Labbra



- Il movimento delle labbra può fornire indicazioni per riconoscere la presenza di una persona.
- Un recente studio è stato condotto presso il Chihara Lab. in Giappone.
- Difficoltà di discriminazione fra persone con la stessa espressione.

Sistemi Biometrici Multimodali (1)



Un esempio di sistema che impiega volto, impronta digitale e voce

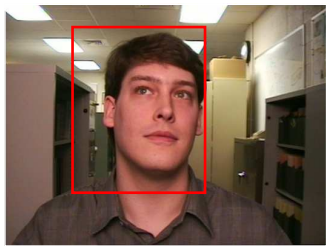
Michigan State University

Sistemi biometrici multimodali (2)

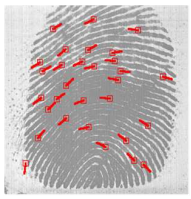
- Limitazioni all'uso di una singola caratteristica biometrica:
  - Percentuale di impossibilità di acquisizione (~4% per l'impronta)
  - Rumore nelle immagini acquisite (uso continuativo del sensore)
  - Mancanza di persistenza (voce alterata a causa del freddo)
  - Potere discriminante limitato (rapporto FAR/FRR elevato)
  - Più facile da raggirare (falsificazione del volto)

- I sistemi biometrici multimodali:
  - Aumentano le prestazioni
  - Riducono la percentuale di impossibilità di acquisizione
  - Più robusti ai tentativi di frode

Progettazione di sistemi multibiometrici



- EigenFaces
- Distanza euclidea

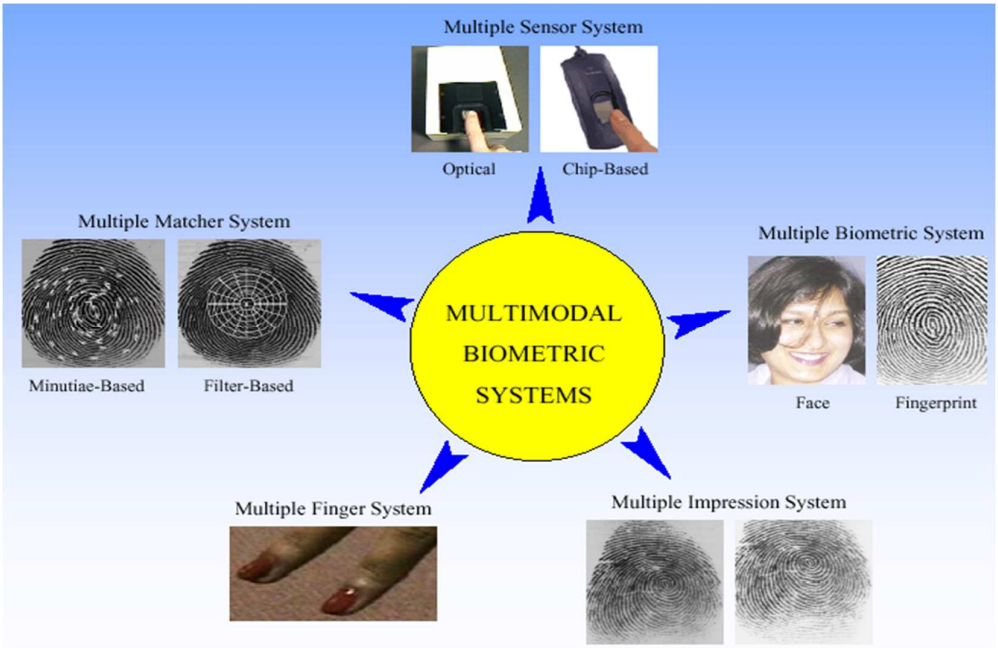


- Minuzie
- String Matching

- Lunghezza/larghezza
- Distanza euclidea

- Scelta del numero di indicatori biometrici
- Livello di fusione: rappresentazione, matching score, decisione
- Apprendimento di pesi delle caratteristiche biometriche individuali per ciascun utente
- Trade-off costi / prestazioni

Approcci multibiometrici



L'uso di sistemi multipli (es. impronte di più dita o più acquisizioni) reintroduce il problema dell'impossibilità di acquisizione; l'uso di più caratteristiche biometriche rappresenta un'alternativa migliore

Combinazione di diverse caratteristiche