Introduzione ai Sistemi Biometrici

Raffaele Cappelli
DEIS - Università di Bologna
(http://bias.csr.unibo.it/cappelli)

BIOLAB - Biometric Systems Lab

Università di Bologna

(Web site: http://bias.csr.unibo.it/research/biolab/)

CLUSIT EDUCATION

Outline

- Riconoscimento di persone e biometria
- Sistemi biometrici: definizione
- Prestazioni di un sistema biometrico
- Panoramica sulle caratteristiche biometriche
- Tecnologie biometriche

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?

Come riconoscere una persona?

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**

Le carte di credito possono essere rubate dalla buchetta delle lettere!

- 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**

➢ **Problemi:** → **facile da indovinare**

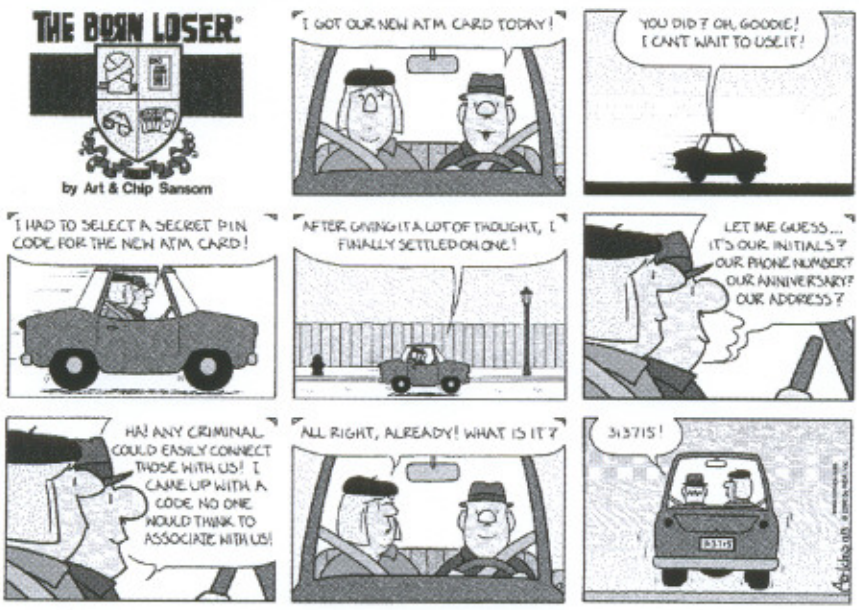
- Può essere rubata, spiata e suscettibile ad attacchi da parte di hackers

Gli hackers 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

Codici segreti...



Qualcosa che CONTRADDISTINGUE l'utente

L'uso di caratteristiche biometriche rappresenta 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 viene descritta come una caratteristica fisiologica o comportamentale che possa essere misurata e successivamente identificata al fine di attestare l'identità di una persona.

Riconoscimento biometrico

Con il termine "riconoscimento biometrico" si fa 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.

Vantaggi dell'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 lo 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

Eliminazione di frodi d'identità (1)

- I ladri d'identità rubano numeri della sicurezza sociale, numeri della patente e cognomi da 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)

Vantaggi dell'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 lo 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

Eliminazione di frodi d'identità (1)

- I ladri d'identità rubano numeri della sicurezza sociale, numeri della patente e cognomi da 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)

Eliminazione di frodi d'identità (2)

"Sorry about the odor. I have all my passwords tattooed between my toes."

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).

Obiettivo

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

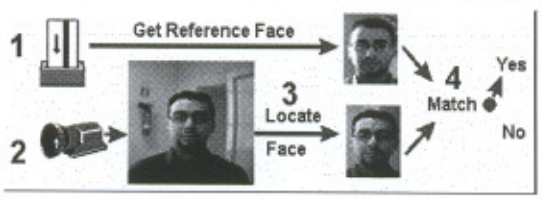
Qual è il sistema biometrico ideale per il controllo degli accessi?

Campi d'applicazione

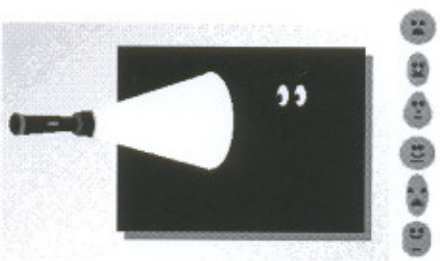
- Controllo accessi, controllo risorse, controllo presenze, sorveglianza ambientale
- Identificazione agli aeroporti o alle frontiere
- Login al computer, transazioni sicure, commercio elettronico
- Carta d'identità, servizi sociali, votazioni, identificazione di criminali
- ...

Modalità di riconoscimento

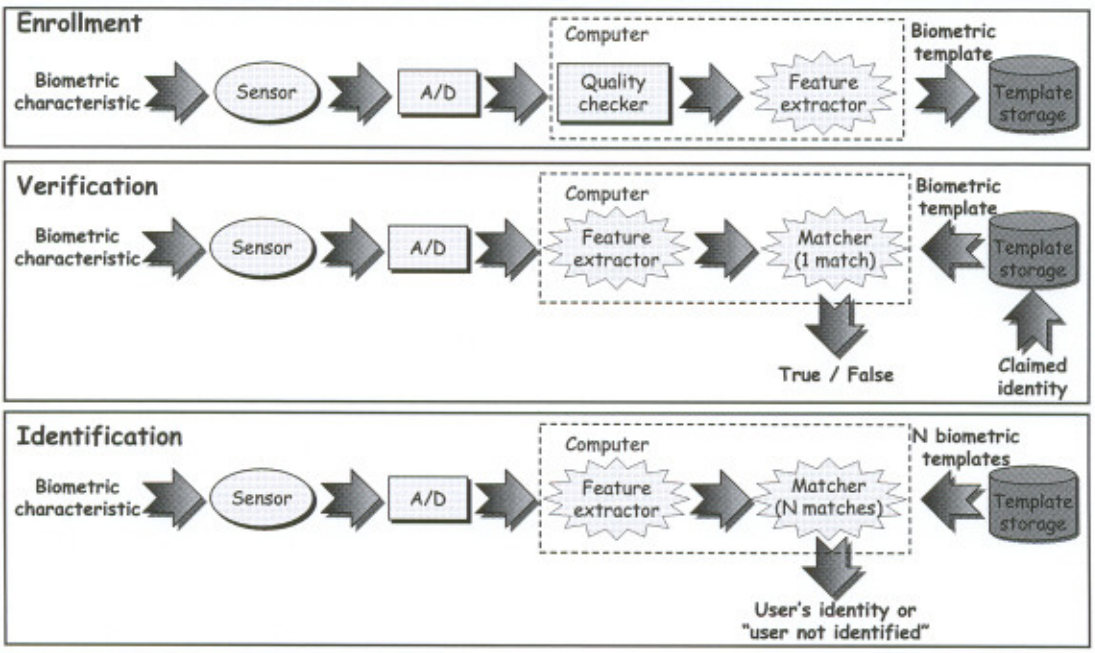
- **Verifica (Autenticazione): Sono chi dichiaro di essere?**
  - Confronto uno a uno al fine di determinare se l'identità dichiarata dall'utente è vera o no



- **Identificazione: Chi sono?**
  - Confronto uno a molti al fine di stabilire l'identità dell'individuo



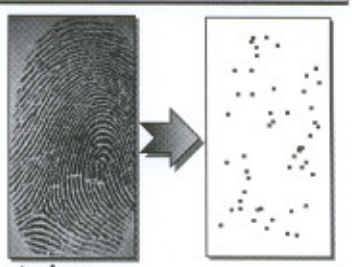
Architettura di un sistema biometrico



Template

Definizione

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



Un elemento fondamentale di un sistema biometrico

- Per il matching vengono utilizzati 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 criptatura e la memorizzazione su più supporti
- Template diversi vengono generati ogni volta che un individuo fornisce un esempio biometrico

Matching

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

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

Soglia=0.5, Punteggio=0.9

Soglia=0.5, Punteggio=0.6

Soglia=0.5, Punteggio=0.3

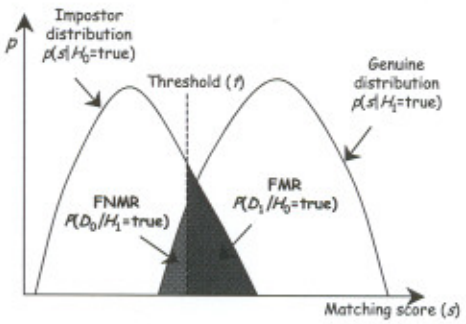
Errori nei sistemi biometrici (1)

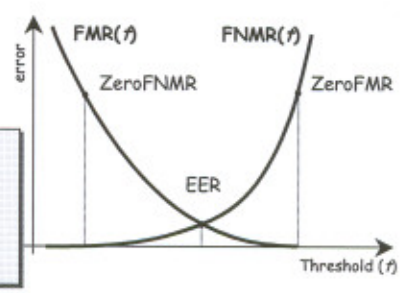
False Match (nel riconoscimento positivo chiamato spesso False Acceptance)

- misurazioni biometriche di persone diverse vengono erroneamente considerate come appartenenti alla stessa persona

False Non-Match (nel riconoscimento positivo chiamato spesso False Rejection)

- misurazioni biometriche della stessa persona vengono erroneamente attribuite a persone diverse



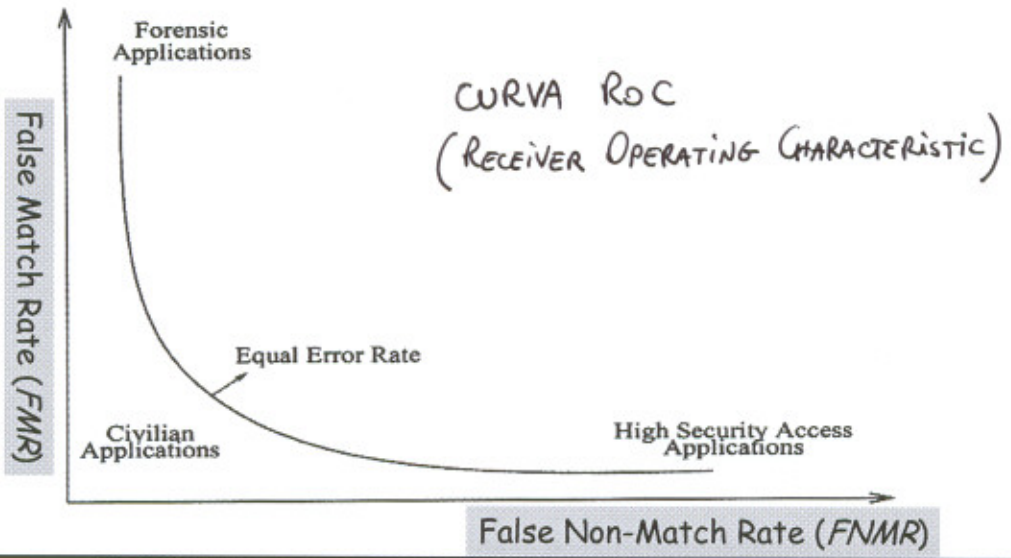


Ipotesi:
H_0: persona diversa
H_1: stessa persona

Decisioni possibili:
D_0: persone diverse
D_1: stessa persona

Applicazioni, FMR e FNMR

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



CURVA ROC
(RECEIVER OPERATING CHARACTERISTIC)

Parametri di valutazione

A. 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

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

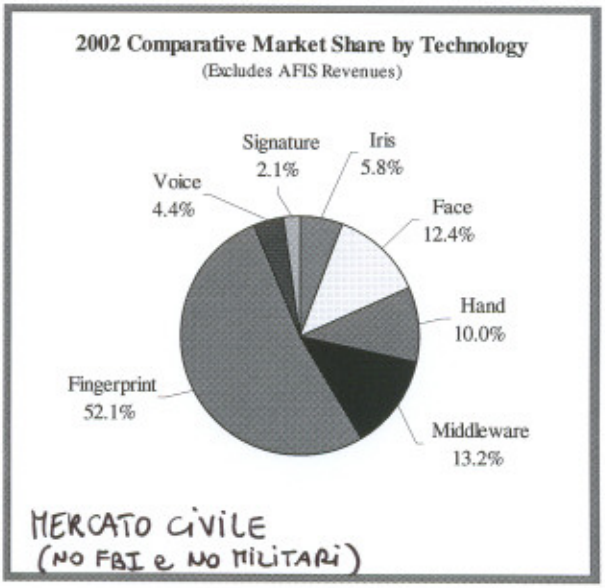
C. Usabilità
- Interazione con l'utente
  - Facilità d'uso
  - Praticità
  - Training
  - Enrolment
- Interazione con l'amministratore
  - Praticità
  - Strumenti di amministrazione
  - Necessità di supervisione
- Efficienza
  - Nella fase di enrolment
  - Nella fase di identificazione/verifica

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

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

Confronto tra diverse caratteristiche biometriche (1)

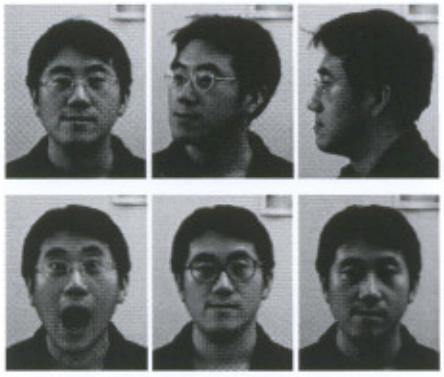
- Universalità
- Unicità
- Persistenza
- Facilità di acquisizione
- Prestazioni
- Accettabilità
- Contraffazione

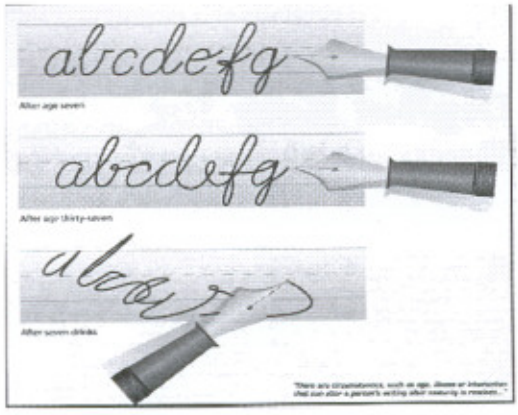


Confronto tra diverse caratteristiche biometriche (2)

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

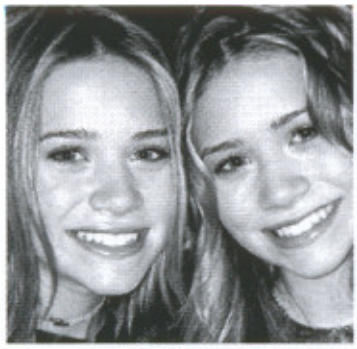
Variabilità intra-classe





Similarità inter-classe

Due persone diverse possono avere lo stesso aspetto



www.marykateandashley.com

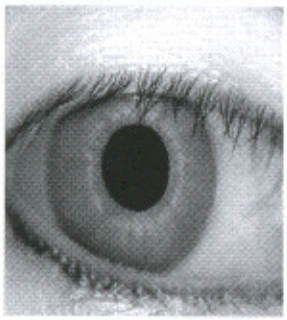
Gemelli

news.bbc.co.uk/hi/english/in_depth/americas/2000/us_elections

Padre e figlio

Rumore nei dati acquisiti

rumore di POSIZIONE



rumore di FORMA

rumore di USURA

rumore di LUCE

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

Localizzazione del volto (1)

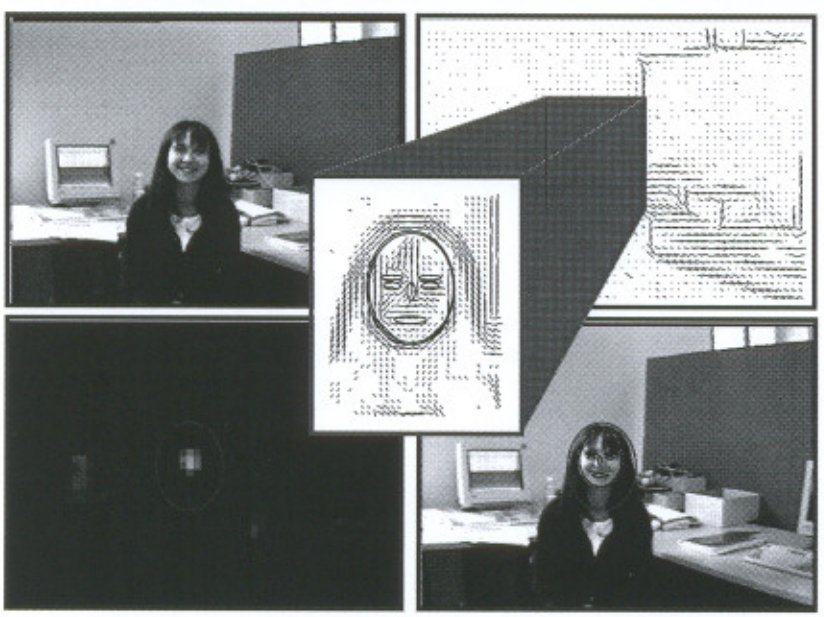

sfondo semplice / sfondo complesso


condizioni d'illuminazione differenti


rotazioni


scale diverse (distanza dalla telecamera)

Localizzazione basata su immagine direzionale



Calcolo immagine direzionale

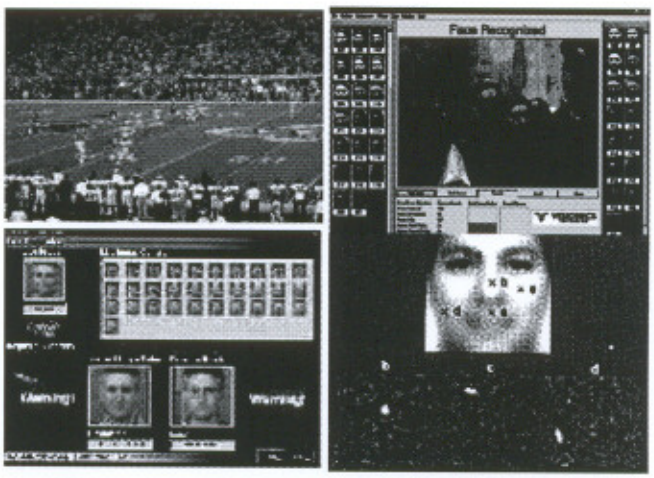
Localizzazione approssimata

Raffinamento immagine direzionale

Localizzazione accurata e verifica

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

Resistenza alla contraffazione

Fonte: c't Magazine 2002

Approcci al riconoscimento del volto (1)

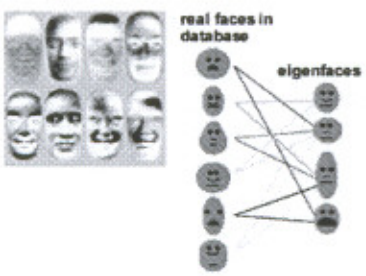
Come gestire le variazioni del volto?

- Invariance at feature-extraction level (**IFL**)
  - Si cerca di estrarre feature invarianti rispetto ad alcune variazioni intra-classe (trasformazioni geometriche, illuminazione, ...)
  - Eigenfaces, Fisherfaces, ...

- Invariance at classification level (**ICL**)
  - Si cerca di controllare le variazioni intra-classe attraverso tecniche di classificazione robuste
  - Il template del volto viene confrontato con la faccia corrente in maniera "tollerante" alle variazioni
  - Elastic-matching, Active-shape, ...

Approcci al riconoscimento del volto (2)

Eigenfaces



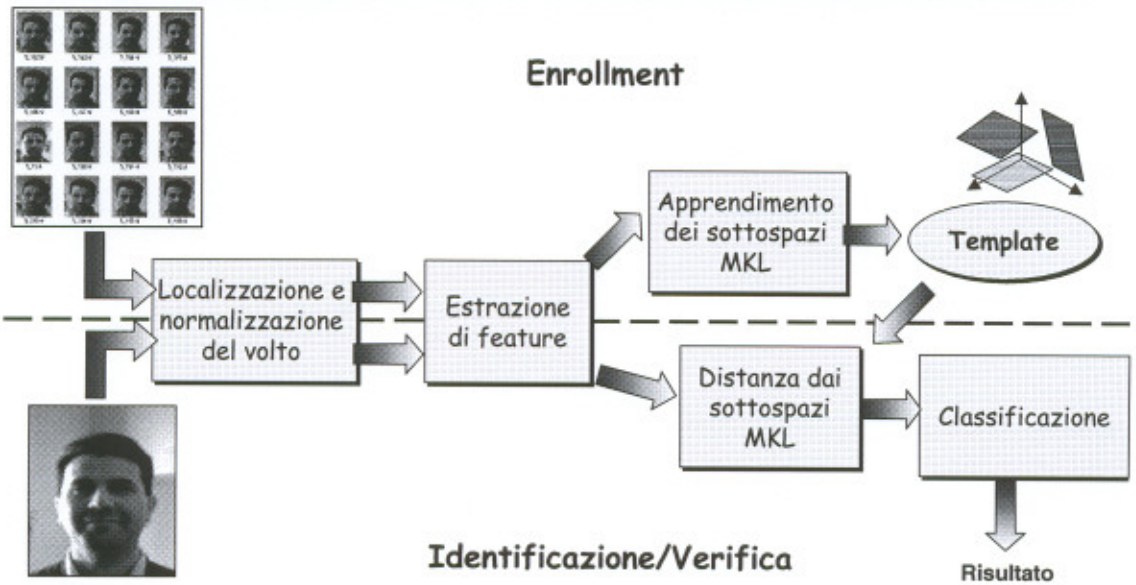
Un volto viene rappresentato come un punto in uno spazio multidimensionale, generato da un insieme di vettori ortonormali (eigenfaces)

Due volti vengono considerati "simili" se i punti corrispondenti sono vicini nello spazio

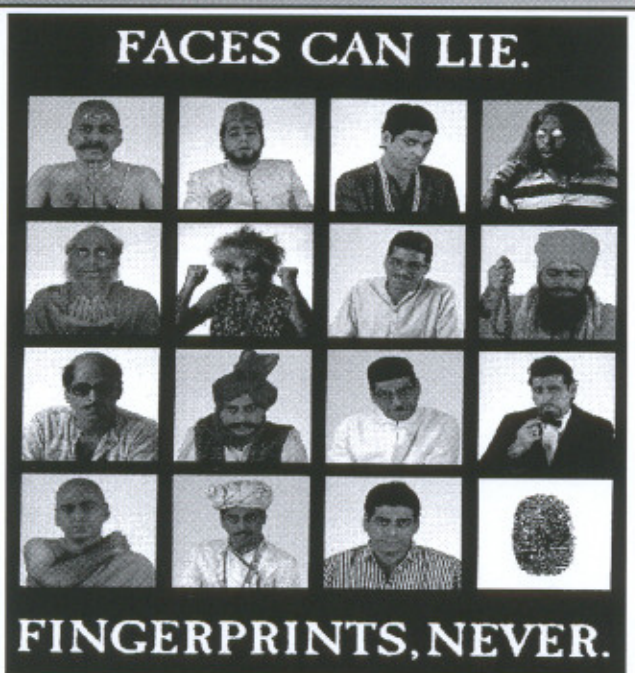
Elastic graph matching

Un volto viene rappresentato come un grafo, i cui nodi sono etichettati con la risposta a banchi di filtri di Gabor nei punti corrispondenti

Riconoscimento del volto basato su MKL



Volto o impronta?



VOLTO:
POCO POTERE
DISCRIMINANTE

STESSA
PERSONA

FINGERPRINT
UNICO

Impronte

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"

Storia delle impronte

Neolithic Carvings

(Gavrinis Islands)

(a)

(b)

2000 B.C.

Standing Stone (Goat Island)

300 B.C.

A Chinese clay seal

(c)

(d)

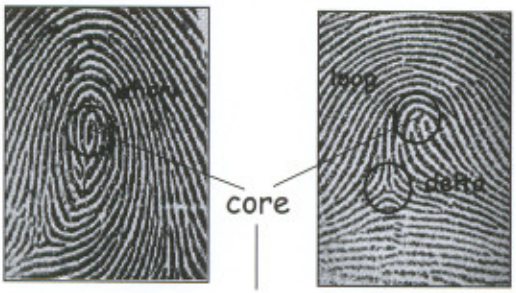
400 A.D.

An impression on a Palestian lamp

Macro- e micro-caratteristiche delle impronte

Un'impronta è composta da un insieme di linee (ridge line), che scorrono principalmente parallele, creando un pattern (ridge pattern)

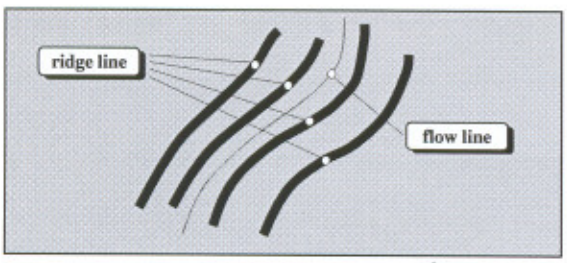
Talvolta le ridge line producono macro-singolarità locali, chiamate whorl (O), loop (U) e delta (D)

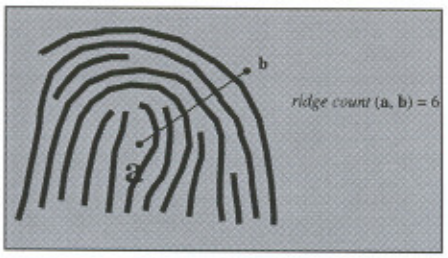


Il punto più a nord della ridge line più interna

Le minuzie, o caratteristiche di Galton, vengono determinate a partire dalle terminazioni o biforcazioni delle ridge line

Macro-caratteristiche delle impronte





impronta

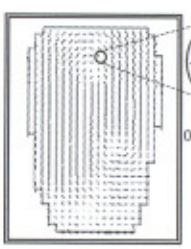


immagine direzionale

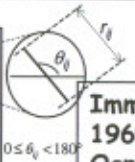


Immagine direzionale (Grasselli 1969):
Ogni elemento θ_{ij}, corrispondente al nodo $[i,j]$ di una griglia a maglie quadrate sovrapposta al pixel $[x_i, y_j]$, indica l'orientazione media delle ridge delle impronte in un intorno di $[x_i, y_i]$

mappa di densità

Micro-caratteristiche: minuzie

Le minuzie, o feature di Galton (1892), consistono in discontinuità delle ridge line.

Il modello di coordinate basato su minuzie dell'FBI considera solo terminazioni e biforcazioni.

I tipi di minuzie più comuni

	Terminazione
	Biforcazione
	Lake
	Independent ridge
	Point or island
	Spur
	Crossover

Acquisizione di impronte: parametri del dispositivo

- Risoluzione

  il numero di dot per inch (dpi). 500 dpi è la risoluzione minima per scanner FBI-compliant; la risoluzione minima per l'estrazione di minuzie è di circa 200-300 dpi.

- Area

  un'area maggiore o uguale a un quadrato 1x1 inch (secondo le specifiche FBI) permette l'acquisizione chiara di un'intera impronta

- Range dinamico (o profondità)

  numero di bit utilizzati per codificare il valore di intensità di ciascun pixel

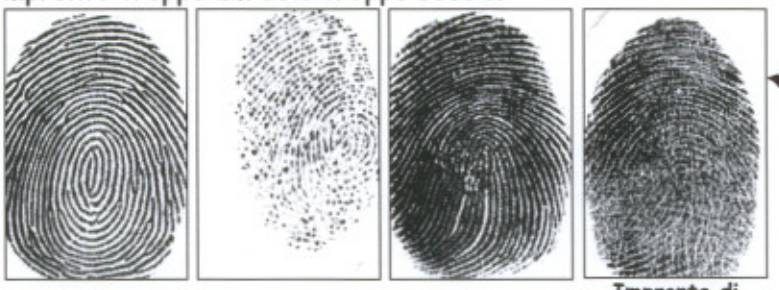
- Accuratezza geometrica

  la massima distorsione geometrica introdotta dal dispositivo di acquisizione

Acquisizione delle impronte: qualità delle immagini

Qualità delle immagini di impronte

- È difficile scindere la qualità dell'immagine dell'impronta [Modulation Transfer Function, Signal-to-Noise Ratio, Output Gray-Level, Contrast, Ridge-direction consistency, ...] dalla qualità intrinseca e dalle condizioni dell'impronta.
- Impronte di bassa qualità:
  - ridge line poco prominenti (lavoratori manuali e persone anziane)
  - impronte troppo umide o troppo secche

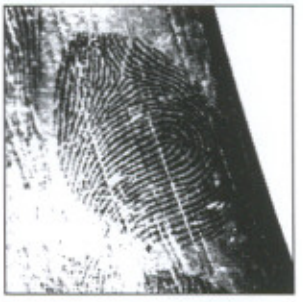


Buona qualità | Impronta secca | Impronta umida | Impronta di cattiva qualità intrinseca

Acquisizione di impronte: off-line vs. on-line

Acquisizione off-line

- Tecnica a inchiostro
- Impronte latenti



Acquisizione on-line

- Optical sensors
- Silicon-based sensors
- ...

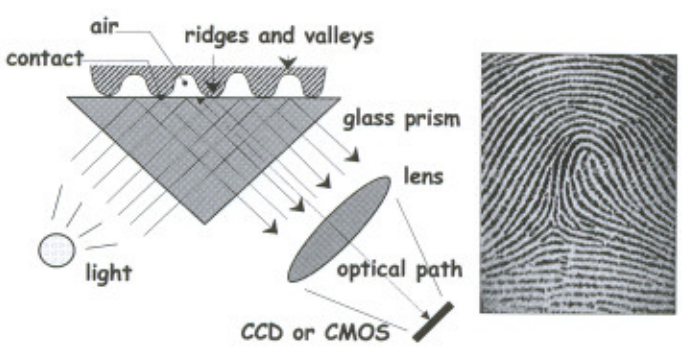
Tecnica a inchiostro

- La pelle dell'impronta viene prima ricoperta con inchiostro nero e poi pressata su carta
- L'immagine viene convertita in formato digitale (utilizzando uno scanner o una telecamera CCD ad alta qualità)
- La risoluzione di default è 500 dpi
- In alcune regioni parte delle informazioni possono andare perse a causa di un'eccessiva o insufficiente inchiostrazione

Sensori ottici (1)

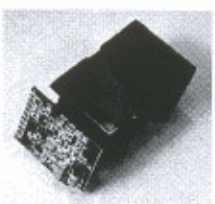
Frustrated Total Internal Reflection (FTIR)

- L'impronta tocca la parte superiore di un **prisma di vetro**
- La luce che attraversa il prisma viene riflessa nelle valli, e sparsa casualmente (assorbita) dalle ridge
- I dispositivi basati su FTIR non possono essere rimpiccioliti notevolmente




Biometrika


Identix Touchview II

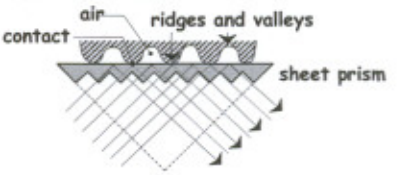

Identicator DFR200

CON IL PRISMA OTTICO NON FUNZIONANO LE FALSIFICAZIONI BASATE SU FOTO O IMMAGINI (RAGGIO RIFLESSO NEGLI AVVALLAMENTI - RAGGIO ASSORBITO SULLE RIDGES LINES

Sensori ottici (2)

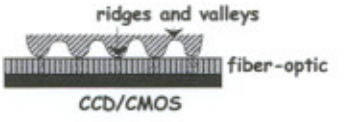
FTIR con prismi multipli

La dimensione può essere in parte ridotta; la qualità delle immagini risulta inferiore rispetto al FTIR tradizionale.



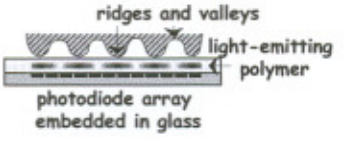
Fibre ottiche

La dimensione può essere ridotta ulteriormente; richiede un grande CCD/CMOS (costo elevato).



Elettro-ottico

Un polimero che emette luce a seconda del potenzionale applicato su un lato: vengono utilizzati potenziali diversi per ridge e valli. Elevata miniaturizzazione ma scarsa qualità delle immagini.



Who?Vision TactileSense

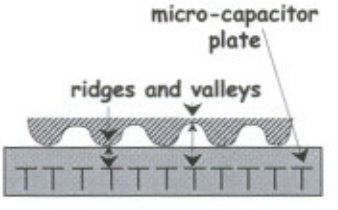
Sensori a stato solido (1)

Silicon-based sensors

- Costituiti da un array di pixel; ogni pixel è un piccolo sensore
- L'utente tocca direttamente la superficie del silicio
- Non sono necessari componenti ottici
- *Maggior grado di miniaturizzazione, ma qualità inferiore rispetto a FTIR*
- Effetto capacitivo:
  - Un array bidimensionali di micro-condensatori
  - L'altro lato di ciascun micro-condensatore è il dito stesso
  - Quando il dito viene posizionato sul sensore si creano delle piccole cariche elettriche
  - Il valore di queste cariche dipende dalla distanza dalla pelle, permettendo così la determinazione di ridge e valli
- Altri effetti sfruttati in sensori a stato solido:
  - Termico, Campo elettrico e piezoelettrico

STM - TCS1A TouchChip

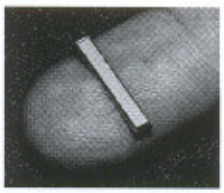
Veridicom FPS100



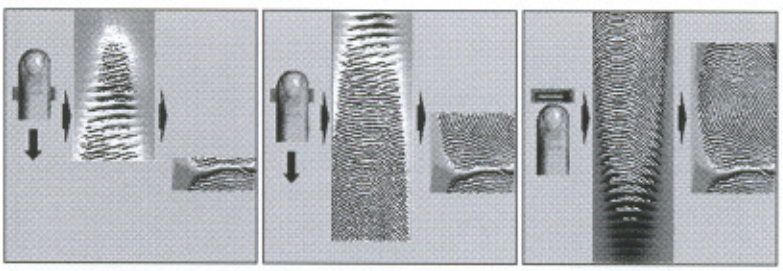
Sensori a stato solido (2)

Sensori a scorrimento

- Un metodo di acquisizione diverso: far scorrere l'impronta sul sensore
- L'altezza del sensore può essere ridotta drasticamente (in teoria 1 pixel) → costo inferiore
- Difficile da usare (gli utenti devono essere addestrati)
- La ricostruzione dell'immagine non è semplice



Atmel FingerChip

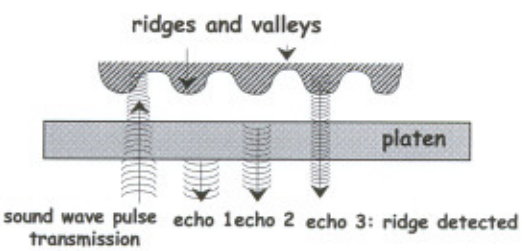


Sensori a ultrasuoni

SENSORE POCO DIFFUSO

Simile all'*ecografia*

- Segnali acustici vengono inviati verso la punta del dito e viene catturata l'eco
- Questo metodo descrive lo strato sottostante la pelle del dito (anche attraverso guanti sottili)
- Non risente di sporcizia o presenza di unto
- È necessario un dispositivo abbastanza grande
- Molto lento: richiede qualche secondo per l'acquisizione di un'impronta
- Costo elevato



Trade-off tra area del sensore e accuratezza

L'area del sensore varia da circa 1.0x1.0 inches quadrati nei dispositivi professionali a 0.42"x0.42" per dispositivi più economici.

Si noti che nel secondo caso l'immagine acquisita è circa 5.6 volte più piccola

Le dimensioni di un'impronta media sono circa 0.5"x0.7" (più piccole nelle donne e nei bambini, più grandi negli uomini adulti).

La porzione d'immagine registrata in acquisizioni diverse dello stesso dito è diversa a causa del differente posizionamento del dito sul sensore

Quattro immagini diverse dello stesso dito acquisite con un sensore ottico di dimensioni 0.51"x0.51".

Localizzazione delle minuzie (1)

- **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 dovrebbe essere molto efficiente.

Un problema di fondamentale importanza: molti ricercatori si dedicano allo studio di queste problematiche.

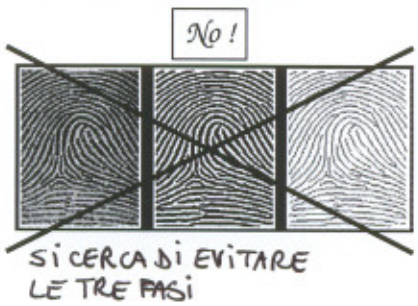
Localizzazione delle minuzie (2)

- **Approcci tradizionali:** l'immagine a livelli di grigio dell'impronta viene convertita in un'immagine binaria, che viene poi sottoposta a una face di assottigliamento (lo spessore delle ridge line viene ridotto a un pixel) e infine una semplice scansione dell'immagine permette di determinare i pixel che corrispondono alle minuzie

- Per localizzare le minuzie: pixels p che corrispondono a un **crossing number cn(p) ≠ 2**

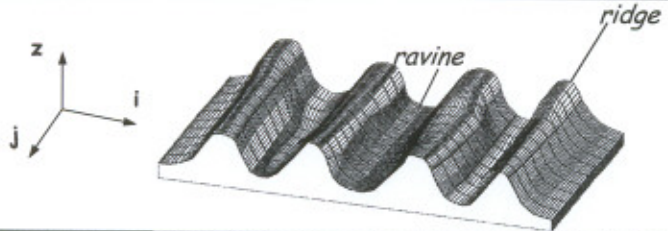
$$cn(\mathbf{p}) = \frac{1}{2} \sum_{i=1..8} \left| val(\mathbf{p}_{i \bmod 8}) - val(\mathbf{p}_{i-1}) \right|$$

Localizzazione diretta su immagini a livelli di grigio (1)



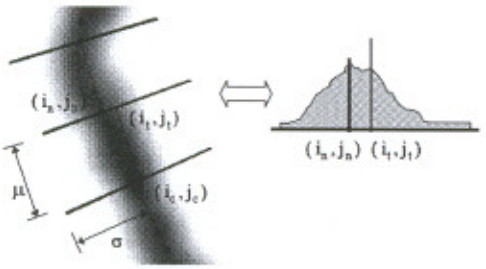
- ✓ durante il processo di binarizzazione si potrebbero **perdere informazioni significative**
- ✓ la binarizzazione e l'assottigliamento sono **costose** dal punto di vista dei **tempi** di elaborazione
- ✓ l'assottigliamento potrebbe introdurre un numero elevato di **false minuzie**
- ✓ molte tecniche di binarizzazione non forniscono buoni risultati quando applicate a immagini di scarsa qualità

Seguire le ridge line sull'immagine a livelli di grigio seguendo l'orientazione locale del ridge pattern

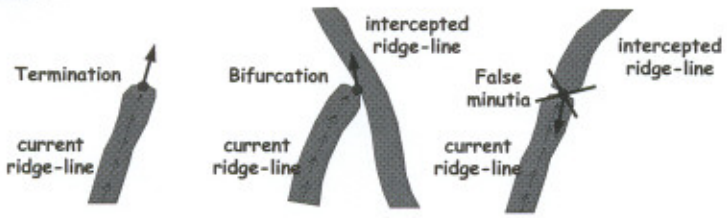


Localizzazione diretta su immagini a livelli di grigio (2)

Una ridge line è costituita da un insieme di punti che rappresentano massimi locali rispetto all'immagine direzionale della ridge line stessa



Viene determinato un insieme di punti di partenza (sulla base di una griglia a maglie quadrate sovrapposta all'immagine); per ogni punto, l'algoritmo cerca la ridge line più vicina e la segue finché raggiunge una biforcazione o una terminazione.



Matching di minuzie

Template dell'impronta:

Vettore di minuzie

Immagine direzionale

Singolarità

.....

Problema di inexact point pattern matching

Perché il matching di impronte è così 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

Impronte: variabilità inter-classe

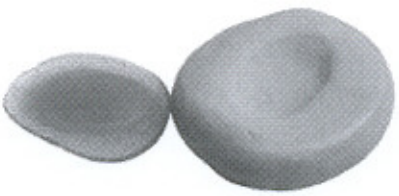
Impronte diverse possono sembrare abbastanza simili, soprattutto a livello di struttura globale (es. posizione delle singolarità, orientazione locale delle ridge line, ...).

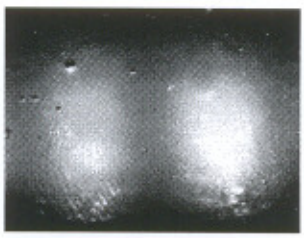
Per risultare robusti a spostamenti, rotazioni e distorsioni, gli algoritmi di riconoscimento di impronte tendono a dichiarare il matching anche se le minuzie non coincidono perfettamente, riducendo in questo modo la variabilità inter-classe.

Ciascuna riga mostra una coppia di immagini di dita diverse, estratte dai database di FVC2002 che sono state accoppiate erroneamente da alcuni degli algoritmi sottomessi a FVC2002.

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 (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 (1)

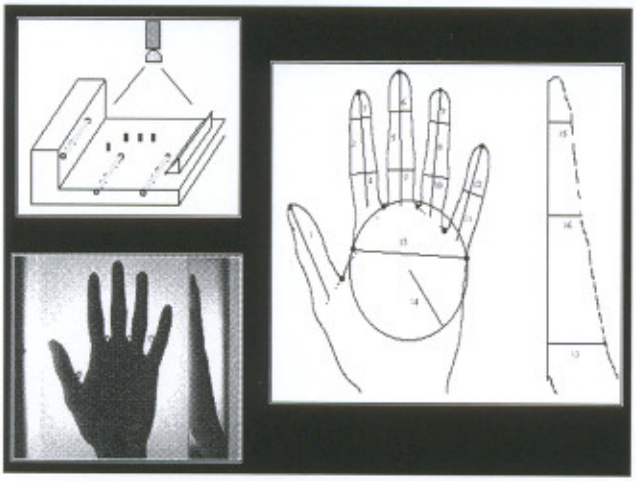
Caratteristiche della mano (es., lunghezza delle dita)
- Relativamente invarianti (*anche se non molto discriminanti*)
- Richiedono poco spazio per la memorizzazione (~ 20 bytes), caratteristica importante per sistemi con larghezza di banda e memoria limitata

Usate tipicamente per la verifica (non sono 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

Geometria della mano e del dito (2)



3D- hand geometry

DISPOSITIVI PIÙ INGOMBRANTI

Geometria della mano

Time & Attendance Terminal

HandPunch
Recognition Systems

Geometria del dito

FingerPhoto
BioMet Partners

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 avere 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

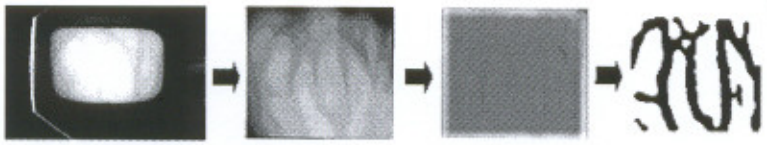
Approcci tipici

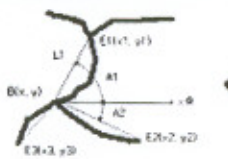
- Reti neurali

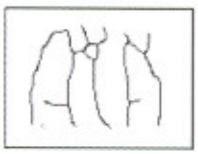
Sistemi commerciali:
BIOPASSWORD- Net Nanny

Vene delle mani

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





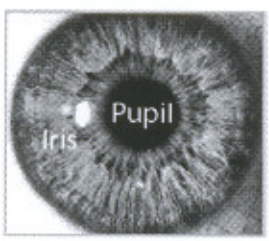


BK 100
BK Systems

NON HANNO RISCOSSO SUCCESSO PER ORA

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 rigido controllo ambientale
- Tecnica abbastanza invasiva
- Costi medio/alti (telecamere a elevata precisione)
- L'acquisizione dell'iride richiede una forte collaborazione da parte del soggetto

Adatta per applicazioni che richiedono un elevato grado di sicurezza

Sharbat Gula

IN QUESTO CASO SOLO L'IRIDE HA DATO ESITO POSITIVO

1985 2002

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

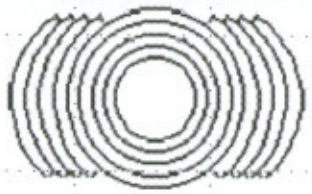
Sistemi di identificazione dell'iride

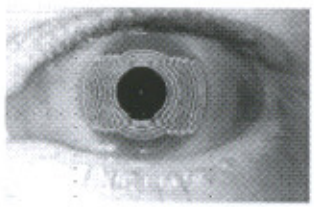
1. L'utente si posiziona a 1-3 piedi di distanza dal sistema costituito da tre telecamere standard

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

Identificazione dell'iride





4. Il sistema usa una griglia circolare come guida per codificare il pattern nell'iride
5. La griglia viene 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 a barre" di 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.

Prestazioni e limitazioni dei sistemi basati sull'iride

- Prove svolte sul campo hanno mostrato che la percentuale di false accettazioni per i sistemi di riconoscimento dell'iride è molto bassa
- La lunghezza costante e l'invarianza rispetto alla posizione permettono un confronto molto veloce
- L'acquisizione dell'immagine dell'iride richiede la collaborazione dell'utente che deve posizionarsi davanti alla telecamera, a una distanza e in una posa prefissata; possono sorgere problemi di acquisizione
- Difficile da applicare in presenza di palpebre abbassate, persone affette da forte miopia, presenza di lenti a contatto
- Il costo dei sistemi di riconoscimento basati su iride è relativamente alto

Resistenza alla contraffazione

- I sistemi iride attualmente in commercio sembrano essere facilmente attaccabili
- Non è tuttavia così semplice ottenere immagini di iride di sufficiente qualità, senza la collaborazione della persona

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, ...). Vengono utilizzati particolari sensori, ad es. tavolette grafiche per gli approcci dinamici o scanner b/n per l'analisi statica della firma

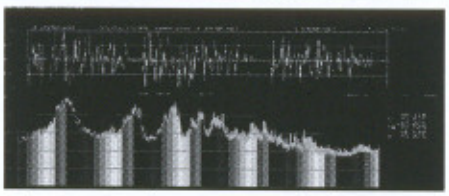
Vantaggi

- User friendly
- Già accettata e utilizzata in molte transazioni amministrative, legali e commerciali

Svantaggi

- Cambia con il passare del tempo (ELEVATA VARIANZA INTRA-CLASSE)
- È influenzata dalle condizioni fisiche ed emotive del soggetto
- La firma di alcune persone è molto variabile (anche due esempi consecutivi)
- I falsari di professione possono riprodurre la firma e ingannare il sistema

Voce



- ✓ **Accettabilità elevata da parte dell'utente**
- ✓ **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**
- ✓ **Sistemi locali/remoti, dipendenti/indipendenti dal testo**
- ✓ **Di fatto l'unica tecnologia possibile nel caso di accesso via telefono**

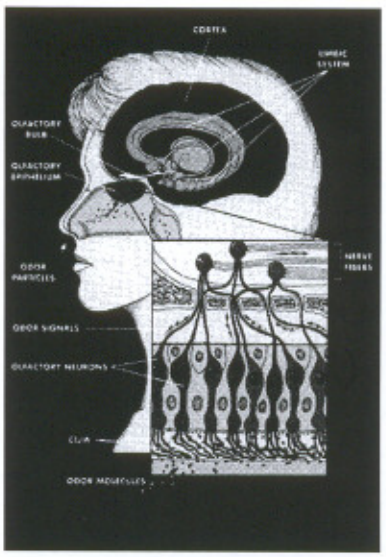
Termogramma facciale

- ✓ Accettabilità elevata da parte dell'utente
- ✓ Caratteristica che può essere influenzata da diversi fattori esterni (fonti di calore)
- ✓ Elevata unicità della caratteristica
- ✓ Elevata sicurezza
- ✓ Sensore sensibile all'emissione di raggi infrarossi da parte della faccia di una persona
- ✓ Tecnologia proposta per identificare soggetti che hanno assunto droga
- ✓ Costi elevati

Termogramma di due gemelli

Odore

- ✓ Elevata unicità e permanenza della caratteristica
- ✓ Array di sensori chimici sensibili a vari composti
- ✓ Non è chiaro come si possa riconoscere l'odore di un corpo umano in presenza di deodoranti o altri composti chimici nell'ambiente circostante
- ✓ Non esistono sistemi commerciali di verifica di identità basati sull'odore



Un prototipo di naso elettronico

Presso i laboratori Caltech è allo studio 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, ...

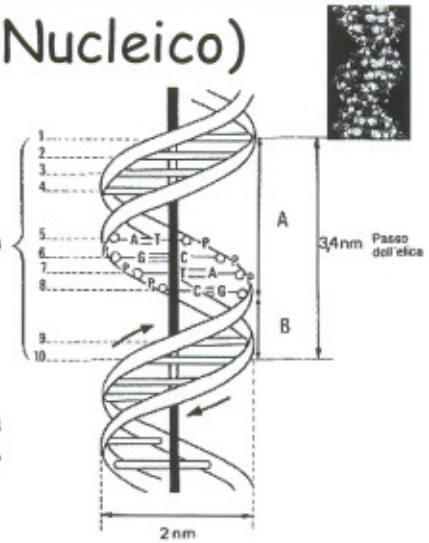
DNA

(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.



Modello di Watson e Crick

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

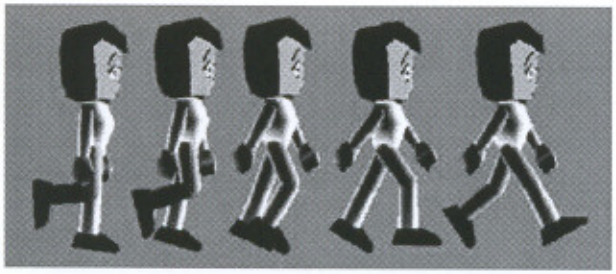
- ✓ Gli uomini condividono dal 99.5% al 99.9% del proprio DNA; le differenti piccole porzioni del genoma umano contengono milioni di coppie base, e ciò rende unico il DNA di un individuo, a parte il caso di due gemelli identici (monozigoti).
- ✓ I metodi chimici per l'analisi di particolari frammenti 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 ambi forense.
- ✓ Nanogen ha recentemente sviluppato un chip per velocizzare il processo di identificazione.

Andatura

✓Caratteristica comportamentale, bassa unicità e permanenza, elevata accettabilità, bassa sicurezza

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

✓Non esistono sistemi commerciali di verifica di identità (SOLO RICERCA PER ORA)



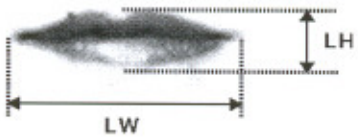
Orecchio

✓Elevata permanenza, unicità media, elevata accettabilità.

✓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.

✓Essenzialmente vengono considerati i contorni e la forma della cartilagine dell'orecchio.

Labbra



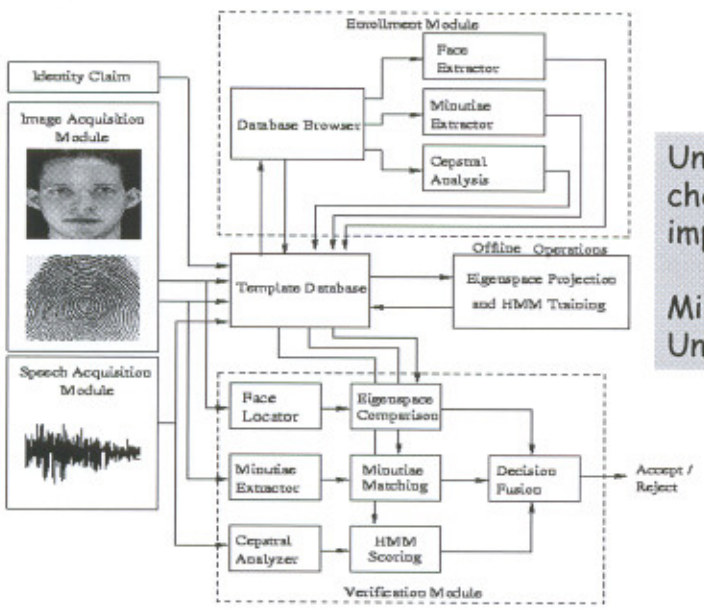
OR = LH / LW

✓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

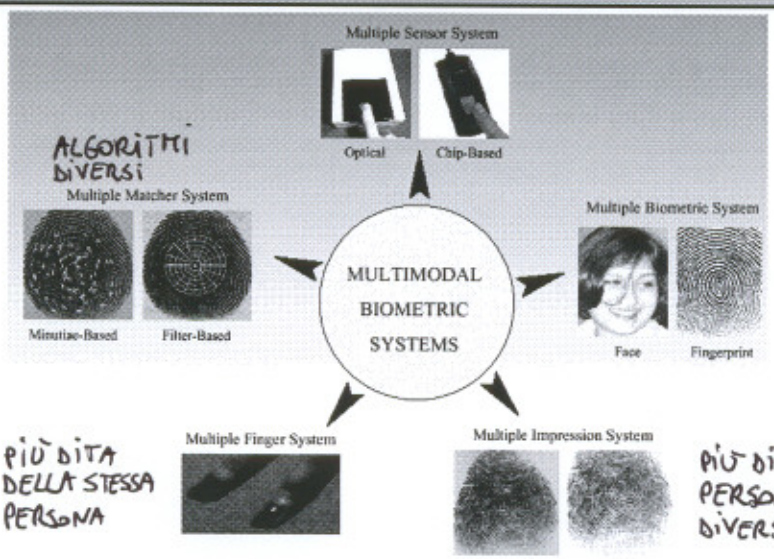


Un esempio di sistema che impiega volto, impronta digitale e voce

Michigan State University

AUMENTA LA SICUREZZA
L'UNIVERSALITÀ
LA CONTRAFFAZIONE RISULTA MOLTO PIÙ COMPLESSA

Approcci multimodali



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