Università degli Studi di Bologna
Facoltà di Ingegneria

TECNICHE BIOMETRICHE

Dott. Ing. Ambra Molesini

Dipartimento di Elettronica, Informatica e Sistemistica

amolesini@deis.unibo.it, **ambra.molesini@unibo.it**

Telefono 051.20.93541

Outline

- Introduzione
- Componenti di un sistema biometrico
- Valutazione, Rischi & Pericoli
- Progettazione, start-up e gestione di un sistema biometrico
- Passaporto Biometrico
- Addendum: Presentazione di tecniche biometriche

INTRODUZIONE

Le tecniche Biometriche

La necessità di identificare le persone correttamente ed irrevocabilmente esiste da molto tempo

L'autorizzazione ad entrare in un edificio, ad aprire un armadietto, a varcare un confine, a prelevare denaro da una banca etc. è sempre collegata all'**identità** di una persona. E' perciò necessario **dimostrare** tale identità in un modo o nell'altro

Un po' di storia

Il primo metodo scientifico d'identificazione biometrico fu sviluppato nei laboratori del carcere di Parigi da Alphonse Bertillon nel diciannovesimo secolo.

Il sistema Bertillon era composto di due fasi:
• rilevazione descrizioni fisiche del corpo umano
• rilevazione misure fisiche di determinate parti del corpo umano.

Questo sistema ha avuto vita breve perché si è scoperto che possono esistere due individui differenti con caratteristiche fisiche identiche, tali da risultare uguali per il sistema

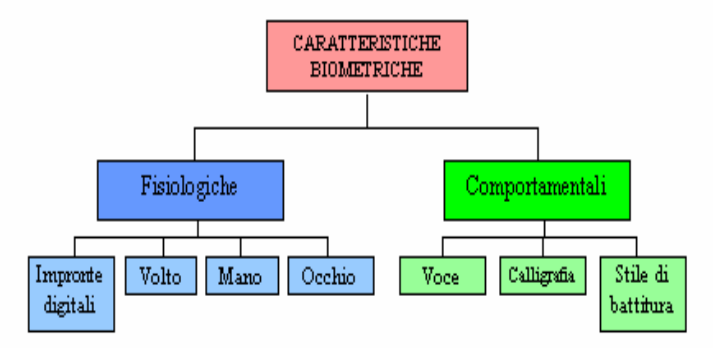
Le tecniche Biometriche

Il riconoscimento biometrico si basa su un fatto universalmente riconosciuto: certe caratteristiche biologiche o comportamentali distinguono una persona da un'altra. Alcuni esempi sono:

- **DNA**
- **Pattern della voce**
- **Pattern della retina**
- **Topografia della faccia**
- **Impronte digitali**
- ....

Una caratteristica biometrica è strettamente legata all'individuo, non può essere persa, dimenticata, duplicata come può succedere con PIN, smartcard e password

Classificazione Tecniche



i sistemi basati su caratteristiche fisiologiche sono generalmente più affidabili di quelli basati su caratteristiche comportamentali

Tuttavia questi ultimi possono risultare a volte più semplici da integrare in alcune specifiche applicazioni

Classificazione Sistemi Biometrici

- Cooperativo/non cooperativo
- Evidente/velato (sistema nascosto al pubblico o meno)
- Abituato/non abituato (usato spesso dallo stesso utente o meno)
- Frequentato/non frequentato (usato più volte nell'arco della giornata anche da utenti diversi)
- Ambiente standard
- Pubblico/privato (accessibile ad un numero elevato di utenti diversi)
- Aperto/chiuso (se vi è o meno scambio di dati con l'esterno)

Esempio Classificazione

Sistema biometrico utilizzato per prevenire l'emissione di patenti auto multiple

- *non-cooperativo*: non identifica le persone che hanno già una patente
- *evidente*: misura biometrica per ottenere la patente
- *frequentato e ambiente standard*: raccolta delle caratteristiche biometriche alla cassa della motorizzazione
- *non abituato*: le patenti sono rilasciate ogni 4-5 anni
- *pubblico*: usato dai clienti della motorizzazione
- *chiuso*: non scambiano informazioni

Qualificazione delle caratteristiche biometriche

- *universalità*: ogni individuo possiede o meno una determinata caratteristica
- *unicità*: il grado con cui si può trovare la stessa caratteristica tra due soggetti diversi
- *permanenza*: caratteristica varia o meno nel tempo
- *misurabilità*: le caratteristiche possono essere misurate quantitativamente
- *esecuzione*: raggiungimento preciso dell'identificazione
- *accettabilità*: il grado con cui una persona è disposta ad utilizzare un determinato sistema biometrico
- *insidia*: il grado di poter ingannare il sistema utilizzando una determinata caratteristica biologica.

Valore dei Parametri

	universalità	*unicità*	*permanenza*	*misurabilità*	*esecuzione*	*accettabilità*	*insidia*
Impronta	Medio	Alto	Alto	Medio	Alto	Medio	Alto
Retina	Alto	Alto	Medio	Basso	Alto	Basso	Alto
Volto	Alto	Basso	Medio	Alto	Basso	Alto	Basso
Mano	Basso	Basso	Basso	Alto	Basso	Alto	Basso
Firma	Basso	Basso	Basso	Alto	Basso	Alto	Basso
Voce	Medio	Basso	Basso	Medio	Basso	Alto	Basso

COMPONENTI DI UN SISTEMA BIOMETRICO

Componenti di una infrastruttura biometrica

Una applicazione basata sulla biometria si compone generalmente di tre parti:

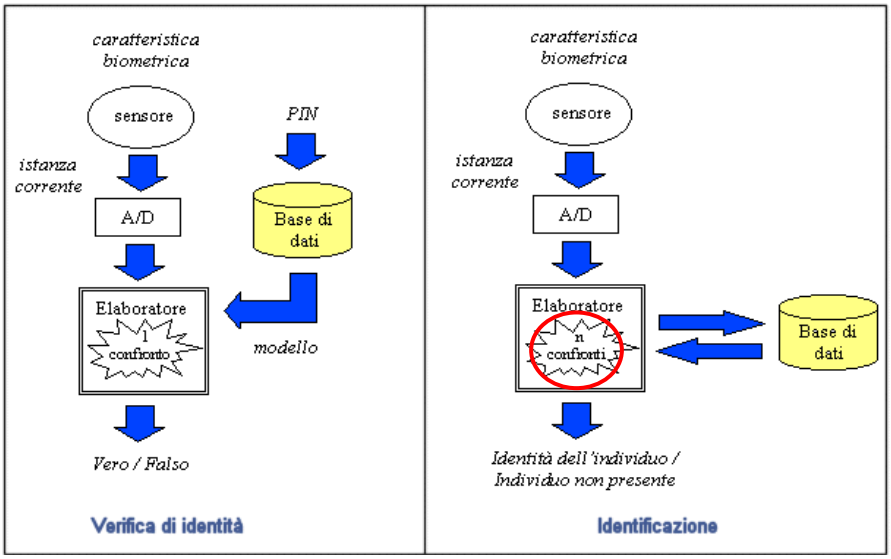
- repository dei dati biometrici: database ove sono contenute le informazioni fisiologiche o comportamentali dei soggetti da autenticare
- insieme delle procedure e dei dispositivi di input: sistemi (lettori biometrici, procedure di caricamento delle informazioni e così via) che connettono l'utente con il sistema di validazione
- procedure di output e interfacce grafiche: front end di tutta la struttura, cioè interfaccia utente

Sistema biometrico

Un sistema biometrico può essere generalmente impiegato per l'**autenticazione** o per l'**identificazione**:

- L' *autenticazione* consiste nello stabilire se un individuo è veramente colui che dichiara di essere 
- L'*identificazione* consiste invece nel determinare se una persona può essere associata (corrispondere) a una di quelle presenti in archivio 

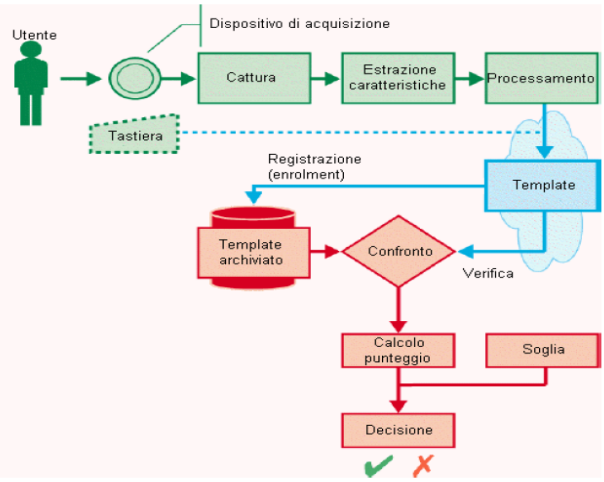
Autenticazione vs. identificazione



Enrollment

- Indipendentemente dalla caratteristica biologica che si adotta, i sistemi biometrici, per poter funzionare, hanno bisogno di una fase di *registrazione iniziale*, detta **enrollment**
- Durante tale fase, vengono *acquisite una o più istanze* della caratteristica biometrica.
- In questo modo il cliente si *presenta* al sistema biometrico e potrà quindi essere *riconosciuto* dal sistema stesso nei successivi accessi.

Il processo biometrico: enrollment e utilizzo



VALUTAZIONE, RISCHI & PERICOLI

Valutazione dei sistemi (1/2)

Nella valutazione dei sistemi biometrici è utile prendere in considerazione alcuni INDICATORI:

- *False Accept Rate* (FAR): è la percentuale di riconoscimento concesso a persone non autorizzate
- *False Reject Rate* (FRR): è costituito dalla percentuale di riconoscimento negato a utenti in realtà autorizzati

L'affidabilità del risultato di un confronto di istanze diverse della stessa caratteristica biometrica non è sicura al 100%: è possibile che una stessa caratteristica subisca variazioni o sia rilevata in modo errato

Valutazione dei sistemi(2/2)

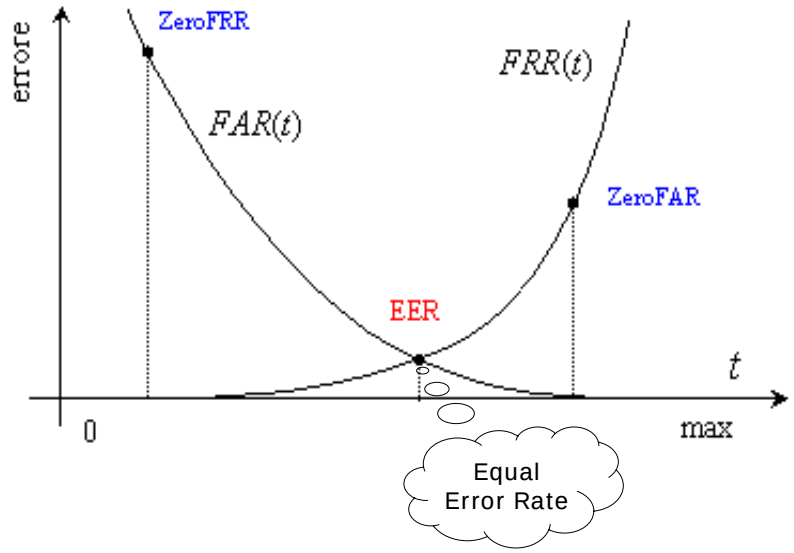
Dunque due caratteristiche biometriche *coincidono* se sono *sufficientemente simili*

↓

soglia di sicurezza *t*: stabilisce quanto stringenti debbano essere i requisiti di somiglianza delle caratteristiche biometriche

incrementando *t* diventa più arduo il compito degli impostori (diminuisce FAR), ma alcuni utenti leciti possono essere talvolta rifiutati (cresce FRR), e viceversa → compromesso

FAR e FRR



Indicatori di sintesi

Talvolta le prestazioni di un sistema biometrico vengono specificate tramite alcuni indicatori di sintesi:

• EER (Equal Error Rate): indica l'errore del sistema nel punto in cui FRR = FAR.

• ZeroFAR: indica FRR nel punto in cui FAR= 0.

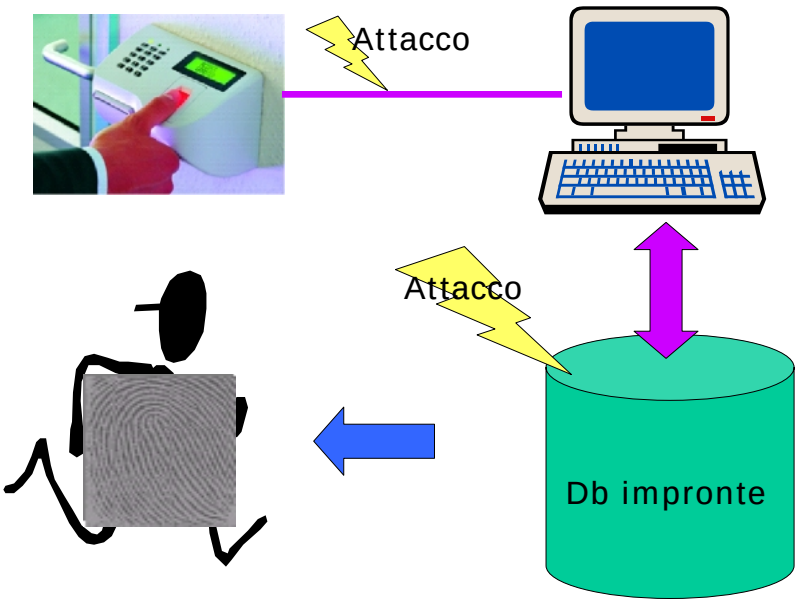
• ZeroFRR: indica FAR nel punto in cui FRR= 0.

Rischi & Pericoli

Test di violabilità di sistemi biometrici in commercio hanno dimostrato che molti sono vulnerabili a:

- Attacchi replay: un hacker ruba l'immagine digitalizzata e se ne serve in un'altra occasione
- Attacchi di manipolazione del valore di soglia tipico di ciascun sistema (obiettivo: aumentare il FAR)
- Inserimento nel sistema di un "cavallo di Troia" per fornire dati erronei al programma di estrazione dei parametri biometrici dall'immagine scansionata.
- Alterazione del risultato finale del processo biometrico: l'inserimento e l'analisi dei dati sono corretti, ma il risultato generato dal sistema è alterato

Esempio



Furto di dati biometrici

Cosa succede se vengono rubati i dati biometrici di un individuo?

La possibilità di utilizzare questa caratteristica biometrica risulta compromessa per sempre:

"***I pollici sono solo due. Se qualcuno ruba i tuoi dati biometrici, saranno persi per sempre. Niente potrà ricostituirli***"

Se qualcuno rubasse le caratteristiche biometriche del nostro volto, della nostra retina o iride sarebbe ancora peggio: non ne abbiamo altre!

Possibile soluzione

Vulnerabilità dei sistemi biometrici:

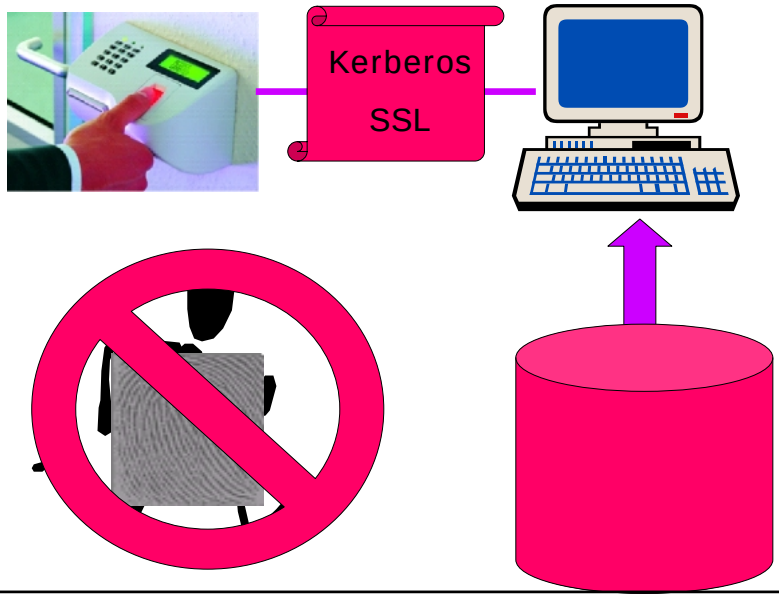
- le implementazioni delle tecniche biometriche sono scarse
- non esistono criteri unificati a livello mondiale per la valutazione della sicurezza dei sistemi biometrici.

Per garantire la sicurezza dei dati biometrici occorre

- Strong cryptography and crypto-card based solutions: adozione di crittosistemi e relativi segreti a tutela del dato biometrico.

La memorizzazione del dato biometrico è molto sensibile occorre adottare tecniche per la sua difesa, in quanto una volta rubato il dato non è rigenerabile.

Esempio



Curiosità (1/2)

- E' stato dimostrato che ben 11 sistemi biometrici disponibili sul mercato per il riconoscimento delle impronte digitali possono essere ingannati utilizzando impronte digitali "finte"
- Tali impronte sono state ottenute con un metodo relativamente semplice: utilizzando uno stampo riempito fondendo la gelatina che si trova in molti dolci è stato creato un finto dito con cui si è riusciti a ingannare i sensori di impronte 4 volte su 5

Curiosità (2/2)

- Varie carceri europee sono dotate di sistemi biometrici al fine di
  - identificare i visitatori al momento dell'uscita
  - verificare i prigionieri quando lasciano il carcere per qualsiasi ragione

  particolarmente nel caso di persone appartenenti a certi gruppi etnici per le quali l'identificazione del volto da parte degli europei risulta difficoltosa.

- Il Parlamento europeo con più di 500 delegati ha installato un sistema di votazione che richiede la verifica dell'impronta digitale per ogni voto. Questo significa un alto livello di sicurezza contro le frodi al momento del risultato delle votazioni.

PROGETTAZIONE, START-UP E GESTIONE DI UN SISTEMA BIOMETRICO

Prima dell'installazione..

Occorre una analisi preliminare delle problematiche sia tecniche che non tecniche. In particolare occorre considerare:

- Aspetti legati alla tutela dei dati personali
- Individuazione dei soggetti interessati e delle risorse per le quali abilitare l'accesso
- Analisi dell'impatto psicologico sui soggetti interessati
- Aspetti inerenti agli standard

E' anche opportuno valutare i costi dell'adozione della biometria e valutare anche l'impiego di tutte le soluzioni alternative

Privacy

La coerenza con gli indirizzi del Garante riguardo alla protezione dei dati personali rappresenta l'imprescindibile fase iniziale di ogni progetto biometrico.

Si ricorda che alla luce della normativa vigente in Italia, una applicazione biometrica deve rispettare a pieno i principi di

- Liceità
- Necessità
- Proporzionalità
- Finalità

Esempio (1/3)

Di recente alcuni istituti di credito hanno inoltrato al Garante una richiesta relativa a trattamenti di dati personali consistenti con l'associazione di dati biometrici (impronte digitali e immagini) dei clienti con altri dati personali noti agli istituti.

Il Garante, nel caso i 4 principi precedenti siano rispettati, ha stabilito regole chiare:

- gli utenti devono essere informati adeguatamente della presenza dei sistemi di acquisizione
- presenza di modalità alternative di accesso
- modalità di raccolta dei dati

Fonte: http://www.garanteprivacy.it/garante/doc.jsp?ID=1246675

Esempio (2/3)

- misure di sicurezza
  - i sistemi devono prevedere l'immediata cifratura dei dati
  - i sistemi devono garantire un elevato livello di sicurezza
  - i dati devono essere trattati con sistemi di cifratura "robusti" con l'utilizzo congiunto di crittografia simmetrica e asimmetrica
  - presenza di un "vigilatore dei dati" depositario delle chiavi crittografiche
- conservazione dei dati
  - i dati cifrati devono essere conservati per un periodo non superiore ad una settimana poi DEVONO essere eliminati definitivamente

Esempio (3/3)

- possono decifrare e accedere alle informazioni raccolte soltanto le autorità giudiziarie e le forze dell'ordine con riferimento a specifiche attività di indagine
- ciascun istituto di credito è tenuto ad inviare entro il 31 Maggio 2006 l'elenco degli sportelli nei quali i dispositivi sono già attivati prima del decreto
- ogni istituto che intende installare o aggiornare le apparecchiature deve inoltrare una specifica richiesta di verifica preliminare al Garante prima dell'attivazione
- indicazione della documentazione che ogni sportello **deve** fornire, conservare e aggiornare in previsione di verifiche future svolte a campione dal Garante

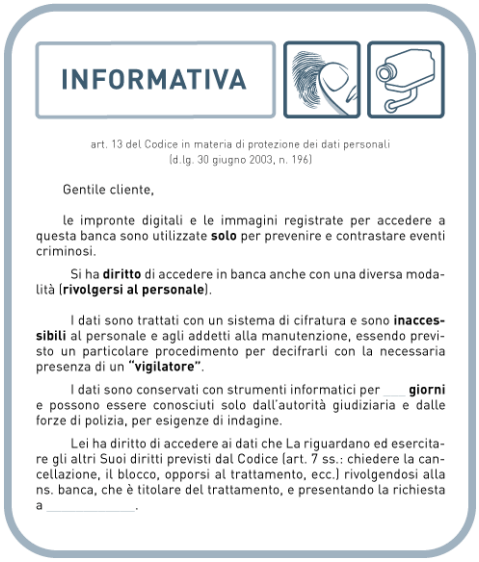
Note Informative

RILEVAZIONE DELL'IMPRONTA DIGITALE E VISIVA

Impronta digitale e immagine sono conservate dalla banca per pochi giorni e sono accessibili solo all'autorità giudiziaria e alle forze di polizia.

Si ha diritto di accedere in banca anche con una diversa modalità (rivolgersi al personale).

Il testo completo dell'informativa è esposto in banca.



INFORMATIVA

art. 13 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196)

Gentile cliente,

le impronte digitali e le immagini registrate per accedere a questa banca sono utilizzate **solo** per prevenire e contrastare eventi criminosi.

Si ha **diritto** di accedere in banca anche con una diversa modalità (**rivolgersi al personale**).

I dati sono trattati con un sistema di cifratura e sono **inaccessibili** al personale e agli addetti alla manutenzione, essendo previsto un particolare procedimento per decifrarli con la necessaria presenza di un **"vigilatore"**.

I dati sono conservati con strumenti informatici per ____ **giorni** e possono essere conosciuti solo dall'autorità giudiziaria e dalle forze di polizia, per esigenze di indagine.

Lei ha diritto di accedere ai dati che La riguardano ed esercitare gli altri Suoi diritti previsti dal Codice (art. 7 ss.: chiedere la cancellazione, il blocco, opporsi al trattamento, ecc.) rivolgendosi alla ns. banca, che è titolare del trattamento, e presentando la richiesta a _____.

Aspetti Sociali(1/2)

Occorre valutare l'impatto sia fisico che emozionale che il sistema biometrico produrrà non solo sugli utenti, ma anche sugli amministratori diretti o indiretti

Stimare il grado di collaborazione da parte degli utenti rappresenta un dato di fondamentale importanza.

Un utente poco cooperativo può

- rappresentare un grosso ostacolo per l'installazione biometrica
- *produrre livelli intollerabili di falsi rifiuti*
- la percezione fisica (grado di invasività) può avere un impatto notevole sull'accettazione

Aspetti Sociali(2/2)

E' opportuno considerare il numero degli utenti che possono risultare impossibilitati ad utilizzare un particolare tipo di biometria

- bambini e anziani, per esempio, presentano una certa difficoltà nell'autenticazione biometrica
- si arriva a parlare di una "***golden window***" cioè una finestra di età ottimale nella quale la biometria raggiunge i risultati più apprezzati (questo crea problemi nel caso del passaporto biometrico)
- inoltre ci sono da considerare anche i fattori quali la disabilità, considerazioni culturali e condizioni fisiche

Altre scelte progettuali

- Scelta della caratteristica biometrica
- Memorizzazione dei template
- Manutenzione del sistema
- Test e valutazione
- Caratteristiche ambientali
- Standard (interoperabilità tra sistemi biometrici)

PASSAPORTO BIOMETRICO

Gazzetta Ufficiale Unione Europea (13/12/04)

Articolo 1:

1. I passaporti e i documenti di viaggio rilasciati dagli Stati membri sono conformi alle norme minime di sicurezza specificate nell'allegato.

2. I passaporti e i documenti di viaggio hanno un supporto di memorizzazione che contiene un'immagine del volto. Gli Stati membri aggiungono inoltre le impronte digitali in formato interoperativo. I dati debbono essere protetti e il supporto di memorizzazione è dotato di capacità sufficiente e della capacità di garantire l'integrità, l'autenticità e la riservatezza dei dati.

3. Il presente regolamento si applica ai passaporti e ai documenti di viaggio rilasciati dagli Stati membri.

Gazzetta Ufficiale Unione Europea (13/12/04)

Articolo 6:

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Gli Stati membri applicano il presente regolamento:

a) per quanto riguarda l'immagine del volto: al più entro 18 mesi

b) per quanto riguarda le impronte digitali: al più entro 36 mesi.

Tuttavia, la validità dei passaporti e dei documenti di viaggio rilasciati in precedenza rimane impregiudicata.

Gazzetta Ufficiale Italiana(29/11/05)

Articolo 2

Nella revisione dei processi di emissione del passaporto ordinario e degli sviluppi tecnologici é previsto l'inserimento del micro-processore RF/ID di prossimità (chip) nella copertina del passaporto, conforme alla direttiva ISO 1443, alle specifiche ICAO OS/LDS con capacità minima di 64Kb e durabilità di almeno 10 anni. Nel chip verranno memorizzate, in formato interoperativo, l'immagine del volto e le impronte digitali del dito indice di ogni mano. Ove, in una mano, l'impronta del dito indice non fosse disponibile si utilizzerà per la stessa, procedendo in successione, la prima impronta disponibile nelle dita medio, anulare e pollice.

Gazzetta Ufficiale Italiana(29/11/05)

(continua)

Nel chip verranno altresì memorizzate le informazioni già presenti sul supporto cartaceo relative al passaporto ed al titolare, nonché i codici informatici per la protezione ed inalterabilità dei dati e quelle necessarie per renderne possibile la lettura agli organi di controllo.

Gli elementi biometrici contenuti nel chip potranno essere utilizzati solo al fine di verificare l'autenticità del documento e l'identità del titolare attraverso elementi comparativi direttamente disponibili quando la legge preveda che siano necessari il passaporto o altro documento di viaggio. I dati biometrici raccolti ai fini del rilascio del passaporto non saranno conservati in banche di dati.
La presente disposizione si applica anche alla normativa sui passaporti diplomatici e di servizio.

ADDENDUM

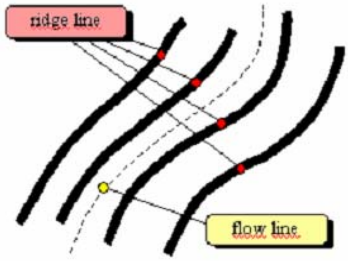
Impronte digitali

La stabilità e l'unicità delle impronte digitali costituiscono ormai concetti accettati universalmente da molto tempo

Un'impronta digitale è costituita da un insieme di linee, dette ridge line o creste, che scorrono per lo più in fasci paralleli, che a volte si interrompono e a volte si intersecano, formando un disegno denominato ridge pattern

Esaminando accuratamente l'andamento delle creste si possono notare delle regioni in cui esse assumono andamenti particolari: curvature accentuate, terminazioni o biforcazioni frequenti chiamate singolarità

Impronte digitali




Impronta

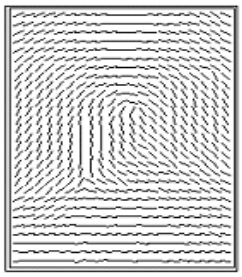
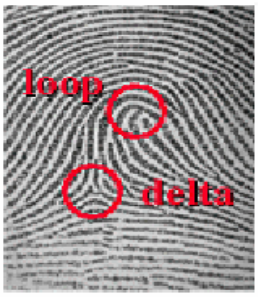


Immagine direzionale

flow-line (linea di flusso): ipotetica linea che corre parallela ad un insieme di creste contigue
immagine direzionale: matrice i cui elementi denotano l'orientazione della tangente alle ridge line in corrispondenza dei nodi di una griglia a maglia quadrata sovrapposta all'immagine dell'impronta.

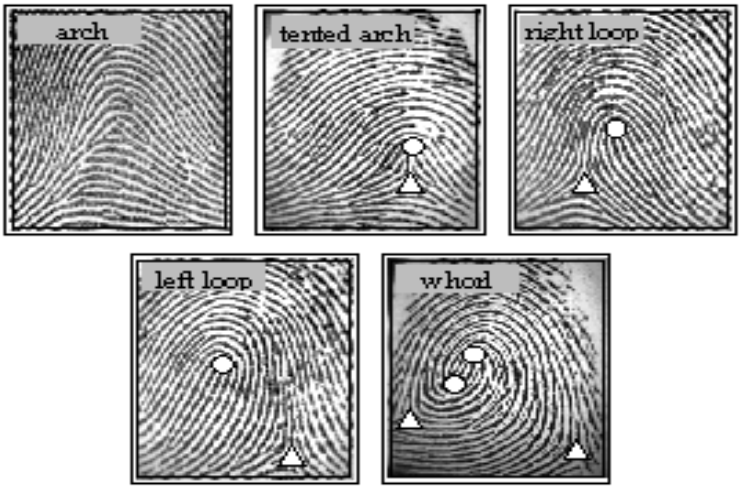
Impronte digitali

Le singolarità sono riconducibili a tre tipologie distinte:
• loop: singolarità caratterizzata da un insieme di creste che hanno un andamento ad U;
• whorl: singolarità caratterizzata da una struttura ad O (di tipo circolare);
• delta :singolarità caratterizzata da un insieme di creste che hanno un andamento semicircolare



Impronte digitali

Le impronte sono generalmente divise in cinque classi principali (arch, tented arch, left loop, right loop, whorl), in base al numero e alla posizione delle singolarità



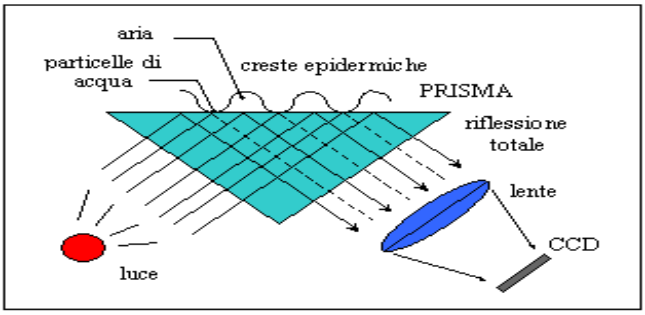
Impronte digitali

Studiando approfonditamente le singolarità, si nota che possono avere conformazioni differenti chiamate minuzie o caratteristiche di Galton, sono principalmente determinate da biforcazioni e terminazioni delle ridge line e sono molto importanti per la discriminazione delle impronte, pertanto vengono usate nella maggior parte dei sistemi di confronto automatico.

Il più noto metodo per l'acquisizione di impronte digitali è la cosiddetta tecnica "dell'inchiostro" che consiste nello sporcare il polpastrello del soggetto con inchiostro nero e operare una leggera pressione su un foglio di carta

Impronte digitali

Nell'ultimo decennio sono state proposte diverse tecnologie alternative per la "cattura" on-line delle impronte digitali. La principale e più matura tecnologia per l'acquisizione (on-line) di impronte digitali, è quella dei sistemi opto-elettronici



Alcuni esempi di sistemi per la cattura di impronte



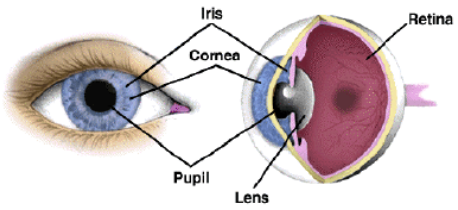



Scansione della retina

È basato sull'acquisizione e la verifica della mappa vascolare della retina dell'occhio umano: ci sono circa 180 variabili misurabili

Simon e Goldstein nel 1935 mostrarono che la forma delle vene nella retina sono uniche per ogni individuo

la rete vascolare della retina è una delle caratteristiche che presenta un indice di **variabilità** nel tempo estremamente basso



Scansione della retina

L'acquisizione delle proprietà della retina utilizza un raggio di luce che effettua la scansione della retina.

I raggi riflessi producono un'immagine in intensità della struttura rilevata.

La luce infrarossa è riflessa indietro ad una videocamera

Abbiamo due metodi differenti di acquisizione della retina:

- **metodo attivo**: l'utente deve effettuare dei movimenti con la testa (20-40cm) affinché il dispositivo di scansione possa individuare l'iride e centrare la pupilla in maniera corretta;
- **metodo passivo**: l'utente resta fermo e una serie di dispositivi di scansione in cooperazione individuano la localizzazione dell'iride.

Scansione della retina

Il dispositivo di cattura effettua una scansione della retina dell'utente tramite un raggio di luce e calcola un template di 256 byte che viene poi utilizzato per la verifica

Per la verifica, è necessario che fra il dispositivo e l'occhio vi sia una distanza di circa 10 cm, quindi il posizionamento dell'occhio gioca un ruolo importante

Tuttavia tale meccanismo non riscuote molto successo poiché non è molto accettabile da parte degli utenti è richiesta loro una cooperazione molto ampia e i costi sono decisamente alti

Scansione dell'iride

La parte colorata dell'occhio umano, con le sue 266 variabili misurabili, è forse l'unica caratteristica fisica maggiormente peculiare di un individuo: non è passibile di cambiamenti nel corso del tempo e non può essere modificata artificialmente

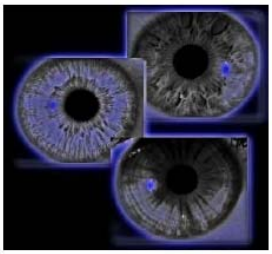
La probabilità di trovare sulla Terra due iridi uguali è praticamente nulla(una su dieci seguito da 78 zeri)

Ogni iride umano ha infatti una struttura unica al punto che persino l'iride destra e sinistra della stessa persona sono differenti.

Scansione dell'iride

La superiorità numerica dei punti caratteristici dell'iride rispetto alla retina sicuramente costituisce un punto a favore dell'iride

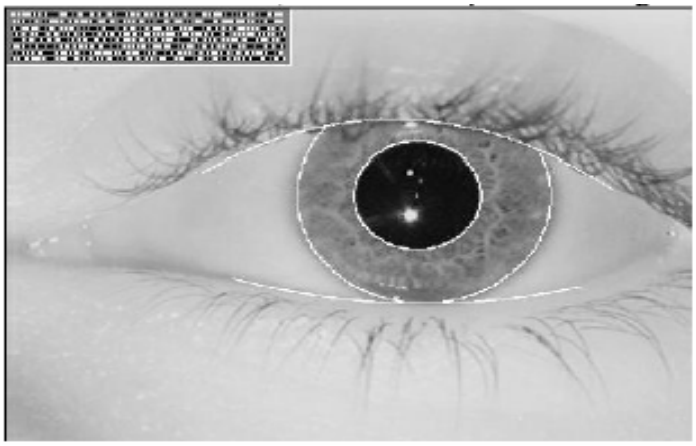
Inoltre, visto che questa membrana è situata in una posizione più esterna rispetto a quella della retina, i metodi per la scansione dell'iride risultano essere più semplici e meno invasivi.



Metodi di rilevazione dell'iride

Un sensore, collocato a circa 40 centimetri di distanza dalla persona esaminata, inizia a fotografare i margini dell'occhio; quindi, attraverso un certo numero di scansioni successive, si individuano i contorni dell'iride come una corona circolare.

Poi si seleziona un quadratino alla volta di quest'area che rappresenta l'area da decodificare. Il disegno di questa regione é convertito in un codice di 512 byte, il cosiddetto ***Iris Code*** che, confrontato con quelli archiviati nel database, identifica la persona nel giro di un paio di secondi.



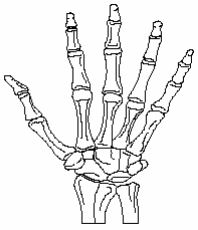
Durante la decodifica dell'immagine, si esaminano circa 250 punti caratteristici e indipendenti, chiamati **"gradi di libertà**", dalla cui combinazione complessiva risulta l'immagine particolare e unica di quell'occhio.

Geometria della mano

Consiste nel riconoscimento delle persone mediante la verifica delle misure e della conformazione della mano e consente un discreto coefficiente di univocità

Misura le caratteristiche fisiche della mano:

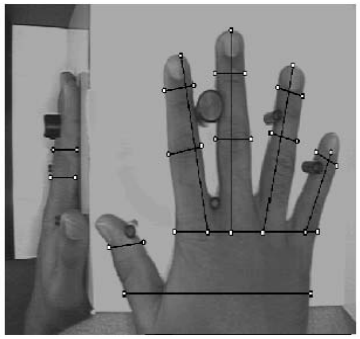
- lunghezza delle dita
- larghezza della mano
- spessore delle dita

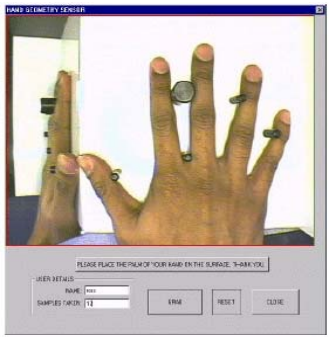


Geometria della mano

Le misure fisiche della mano sono catturate da un apparecchiatura CCD (dispositivo ad accoppiamento di carica) e la sagoma della mano viene memorizzata tridimensionalmente

La mano viene posta su un piano dove vi sono 5 pioli per posizionarla nel modo giusto





Geometria della mano

Le apparecchiature della geometria della mano non prendono in considerazione dettagli della superficie della mano come linee, cicatrici, unghie…

Vantaggi:

- Velocità di rilevamento
- E' il metodo meno invasivo
- Template piccolo sotto 10 byte

Tuttavia, va tenuto presente che la geometria può mutare a causa dell'età avanzata o a seguito di patologie fisiche, quali, per esempio, l'artrite, per questo motivo la tecnica a volte è considerata debole

Riconoscimento della voce

Distinguere le persone effettuando un'accurata analisi dei segnali vocali emessi dal soggetto interessato.

Le caratteristiche della voce di un parlante sono dovute sia a differenze fisiologiche, sia al particolare stato d'animo in cui si trova.

Il principale aspetto fisiologico è il tratto ove la voce prende forma. Il tratto vocale è generalmente considerato l'organo da dove si produce la voce

Riconoscimento della voce

Il contenuto spettrale di un'onda acustica viene modificato dal tratto vocale, producendo in ognuno di noi una voce diversa l'una dall'altra; grazie a queste variazioni siamo in grado di riconoscere una persona dalla voce

Esistono due tecniche di rilevamento della voce:

- MFCC : applicando una serie di trasformazioni matematiche, si estraggono quelli che vengono detti **coefficienti cepstrali**, ossia una serie di coefficienti che rappresentano in maniera univoca un segnale vocale
- Rasta PLP: usa tecniche di predizione lineare per estrarre i parametri con cui rappresentare il segnale vocale.

Dinamica della firma

Caratteristiche:
velocità, pressione della penna, direzione, lunghezza del tratto e il tempo in cui la penna viene sollevata dalla carta

Analizza due differenti aree:
- caratteristiche specifiche della firma
- caratteristiche specifiche del processo della firma

Ha il difetto di essere facilmente replicato e quindi di costringere, l'utente a scrivere frasi diverse ogni volta. Inoltre è soggetto allo stato d'animo dello scrittore

Riconoscimento del volto

Quando noi vogliamo riconoscere una persona, la prima cosa che osserviamo è sicuramente il suo volto

Rilevazione:
- mediante una macchina fotografica a raggi infrarossi vengono catturate le forme dei vasi sanguinei del volto.
- riconoscimento delle relative posizioni delle caratteristiche del volto(occhi, naso, bocca….) .

Altre tecniche di riconoscimento

Citiamo queste altre tecniche senza darne spiegazioni solo per dovere di completezza, ma sono praticamente inusate

- Segno delle labbra
- Riconoscimento dello stile di battitura dattilografica
- Segno della pianta del piede
- Forma delle vene nella mano e nel polso
- Salinità del corpo
- Odore
- Risposta dello scheletro ad uno stimolo fisico

Quota di “mercato” delle tecniche