

Sistemi Biometrici

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@dia.unisa.it

<http://www.dia.unisa.it/professori/ads>



Maggio 2018

Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Biometria

- Biometrico
 - "Bio-": vita
 - "metrico": misura
- Biometria: uso di strumenti per riconoscere tratti fisici e comportamentali di un essere umano
- Tratti acquisiti ed usati per
 - Autenticazione uno-a-uno
 - Identificazione uno-a-molti
 - Entrambe basate su caratteristiche uniche



Sistemi Biometrici - 1/2

Dispositivi automatici per identificazione/autenticazione basati su caratteristiche dell'individuo

➤ Fisiologiche

- Impronte digitali
- Volto
- Struttura vascolare della retina
- Struttura vascolare della mano
- Forma dell'iride
- Topografia della mano
- Ritmo cardiaco



➤ Comportamentali

- Timbro della voce
- Dinamica della firma



Sistemi Biometrici - 2/2

Dispositivi automatici per identificazione/autenticazione basati su caratteristiche dell'individuo:

➤ Fisiologiche

- Impronte digitali
- Volto
- Struttura vascolare della retina
- Struttura vascolare delle arterie retiniche
- Forma dell'iride
- Topografia della mano
- Ritmo cardiaco



Usati nei sistemi di controllo per

- Accesso fisico
aeroporti, sedi governative, porti, ...
- Accesso logico
sistema informativo

➤ Comportamentali

- Timbro della voce
- Dinamica della firma

Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Storia Sistemi Biometrici

- Biometria utilizzata a partire dalla preistoria
- In Cina si utilizzavano tecniche di identificazione biometrica a partire dal 14° secolo
- Nel 17° secolo le impronte digitali erano usate per apporre sigilli su documenti ufficiali

Il Sistema Bertillon - 1/2

Alphonse Bertillon (1853 - 1914)

Ufficiale della polizia francese



- Fondò il primo metodo d'identificazione scientifico biometrico, che fu sviluppato nei laboratori del carcere di Parigi
 - Prima ciò avveniva solo mediante nome e foto

Idea: L'ossatura umana non si modifica più dopo i 20 anni. Inoltre, ogni scheletro è diverso

Il Sistema Bertillon - 2/2

Basato su 16 caratteristiche

- Altezza e larghezza testa
- Lunghezza dito medio
- Lunghezza piede sinistro
- Lunghezza braccio
- Etc



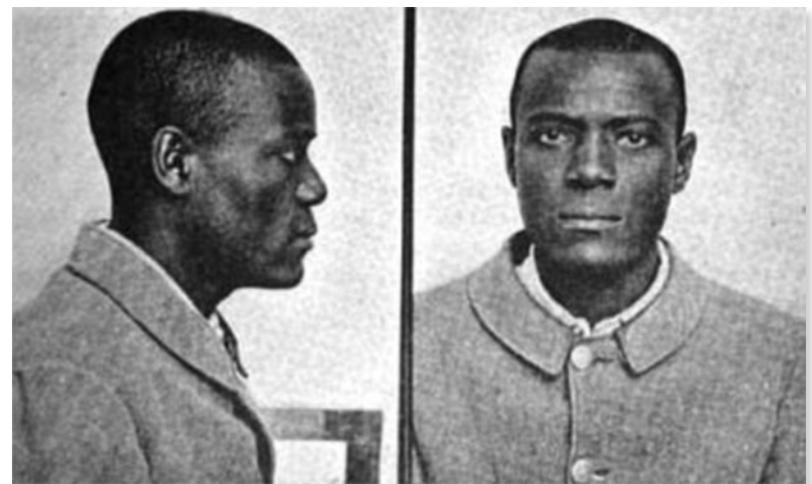
1. Taille. — 2. Envergure. — 3. Buste. —
4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. —
7. Pied gauche. — 8. Médius gauche. — 9. Coude gauche.

Sistema Bertillon: Fallimento - 1/2

Carcere di Leavenworth, Kansas, USA
Due detenuti con misure "identiche"!



Will West arriva nel 1903



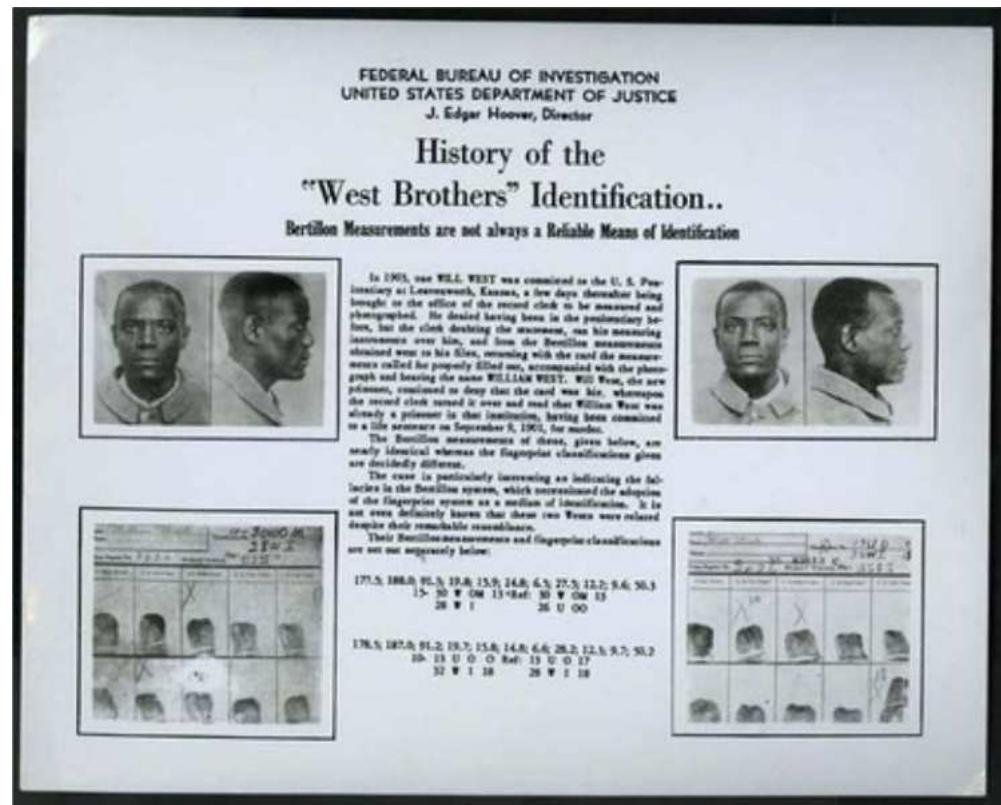
William West nel 1901

Sistema Bertillon: Fallimento - 2/2

Misure quasi identiche
Impronte digitali diverse

Anthropometric measurements of "the two Will Wests" as reportedly recorded at Leavenworth, 1903.

Measurement	Head length	Head breadth	Middle finger	Foot length	Forearm length	Height	Little finger	Trunk	Arm span	Ear length	Cheek width
Will West	19.7	15.8	12.3	28.2	50.2	178.5	9.7	91.3	187.0	6.6	14.8
William West	19.8	15.9	12.2	27.5	50.3	177.5	9.6	91.3	188.0	6.6	14.8



Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Caratteristiche Sistemi Biometrici

1/5

- **Universalità** ogni individuo deve possedere quella determinata caratteristica biometrica
- **Unicità** non è possibile che due persone condividano la stessa identica caratteristica biometrica
- **Permanenza** la caratteristica biometrica deve rimanere immutata nel tempo
- **Catturabilità** la caratteristica biometrica deve poter essere acquisita e quantitativamente misurata

Caratteristiche Sistemi Biometrici

2/5

Universalità

- Ogni persona dovrebbe possedere questa caratteristica
- Tuttavia, in pratica questo potrebbe non accadere
- La popolazione di non universalità dovrebbe essere piccola
 - < 1%

Caratteristiche Sistemi Biometrici

3/5

Unicità

- Non esistono due individui che possiedono la stessa caratteristica
- Stabilire l'unicità è difficile da dimostrare analiticamente
- Una biometria può essere unica, ma l'unicità deve essere *distinguibile*

Caratteristiche Sistemi Biometrici

4/5

Permanenza

- La caratteristica non cambia nel tempo
 - Nella migliore delle ipotesi questa è un'approssimazione
 - Grado di permanenza ha forte impatto sulla progettazione del sistema e la gestione a lungo termine dei dati biometrici
 - Enrollment, adaptive matching design, etc
 - Stabilità a lungo termine vs. stabilità a breve termine

Caratteristiche Sistemi Biometrici

5/5

Catturabilità

- La caratteristica può essere misurata quantitativamente
- La raccolta dei dati biometrici dovrebbe essere
 - Non intrusiva
 - Affidabile e robusta
 - Economicamente vantaggiosa

Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Architettura Sistemi Biometrici

1/7

L'architettura dipende dal contesto applicativo

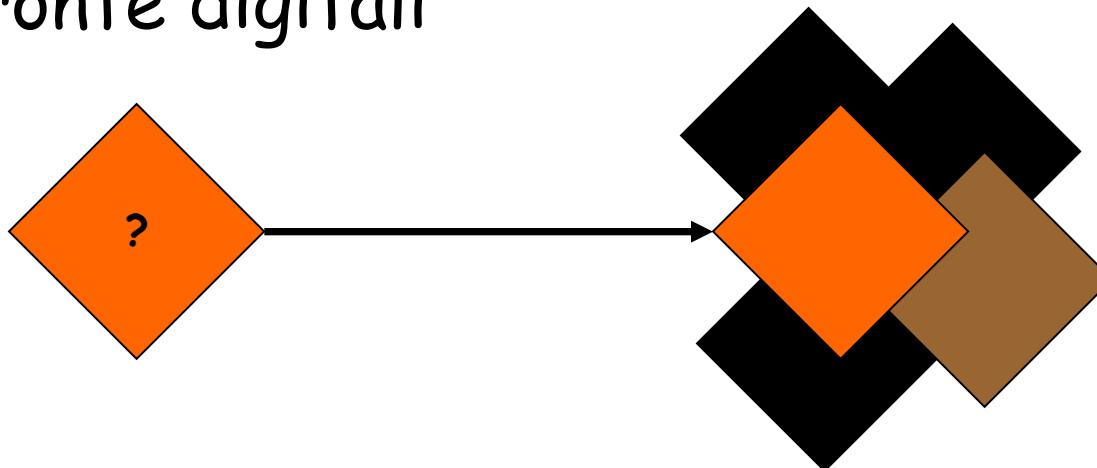
- **Identificazione:** Chi sei?
 - Match uno a molti
 - Match uno a pochi
 - Soggetti cooperativi e non cooperativi
- **Autenticazione:** Sei chi dichiari di essere?
 - Match uno ad uno
 - Soggetti cooperativi

Architettura Sistemi Biometrici

2/7

➤ Identificazione

- Cerca una corrispondenza all'interno di un database di modelli
- Applicazione tipica: identificazione di impronte digitali

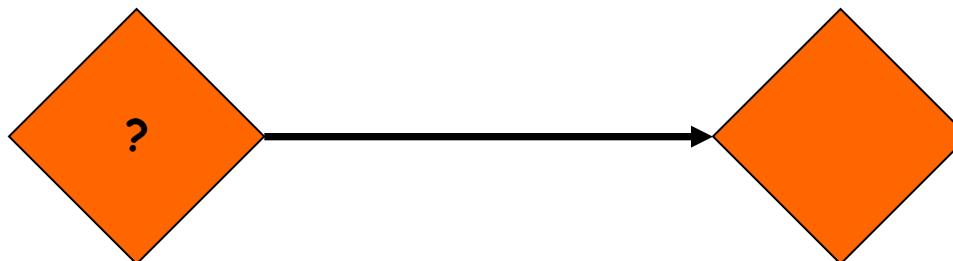


Architettura Sistemi Biometrici

3/7

➤ Autenticazione

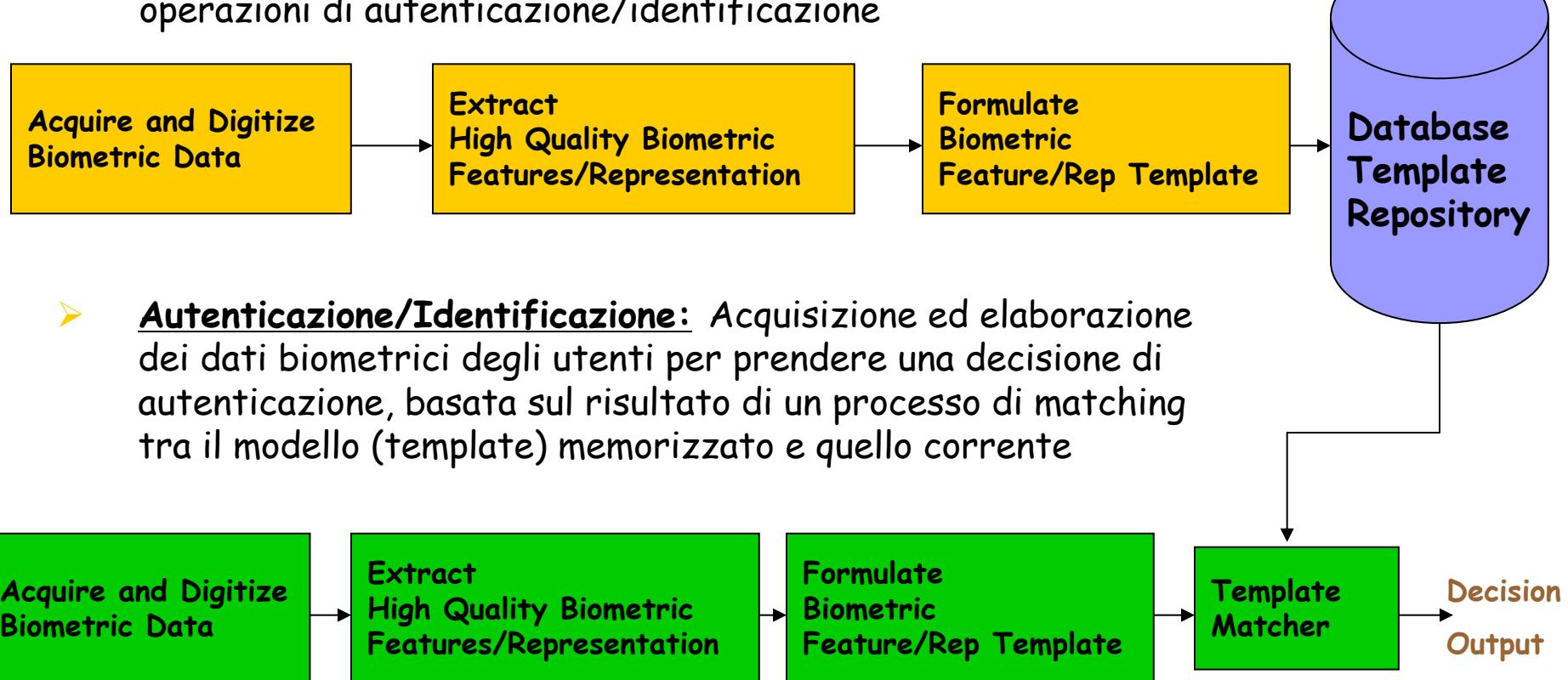
- Confronta un campione (sample) con un singolo modello archiviato



Architettura Sistemi Biometrici

4/7

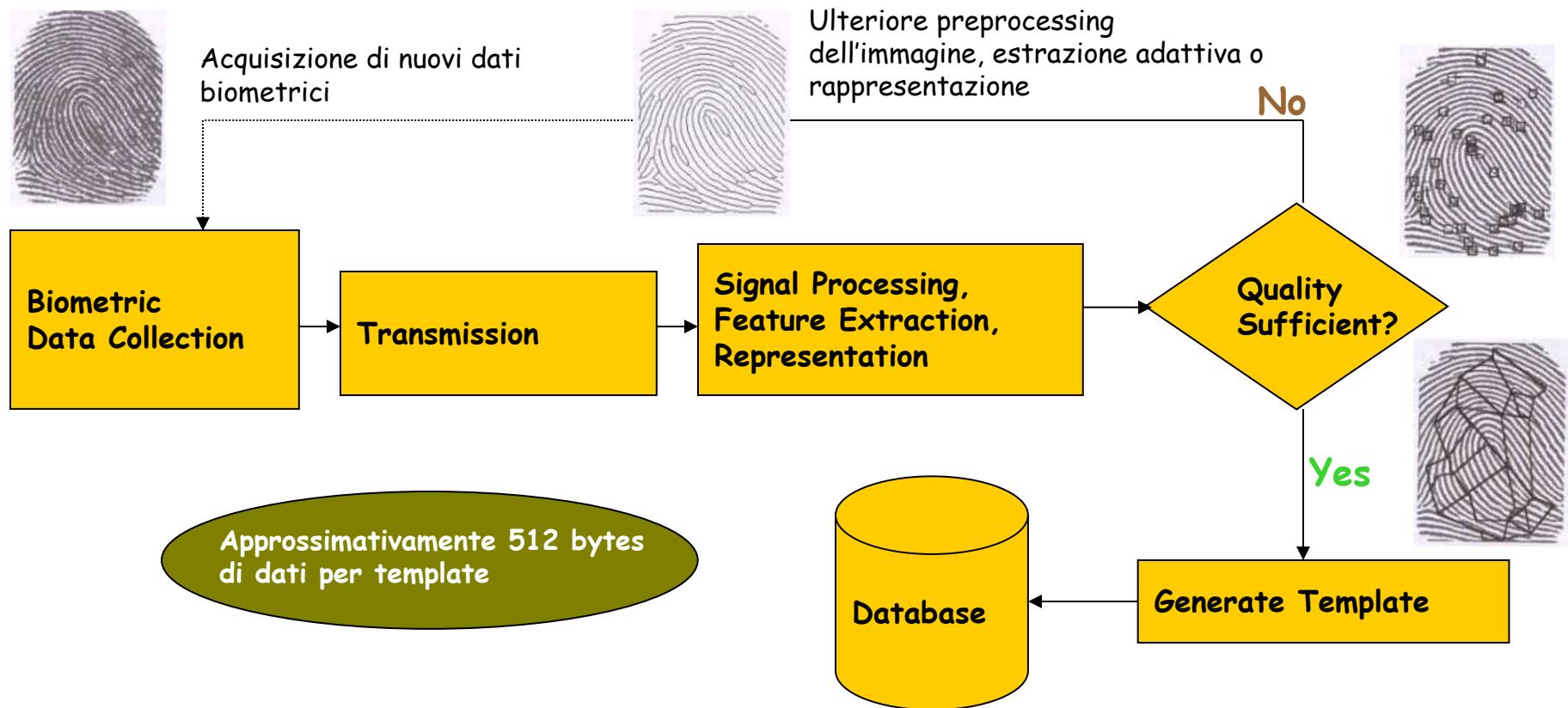
- **Enrollment:** Acquisizione ed elaborazione dei dati biometrici dell'utente per l'utilizzo da parte del sistema nelle successive operazioni di autenticazione/identificazione



Architettura Sistemi Biometrici

5/7

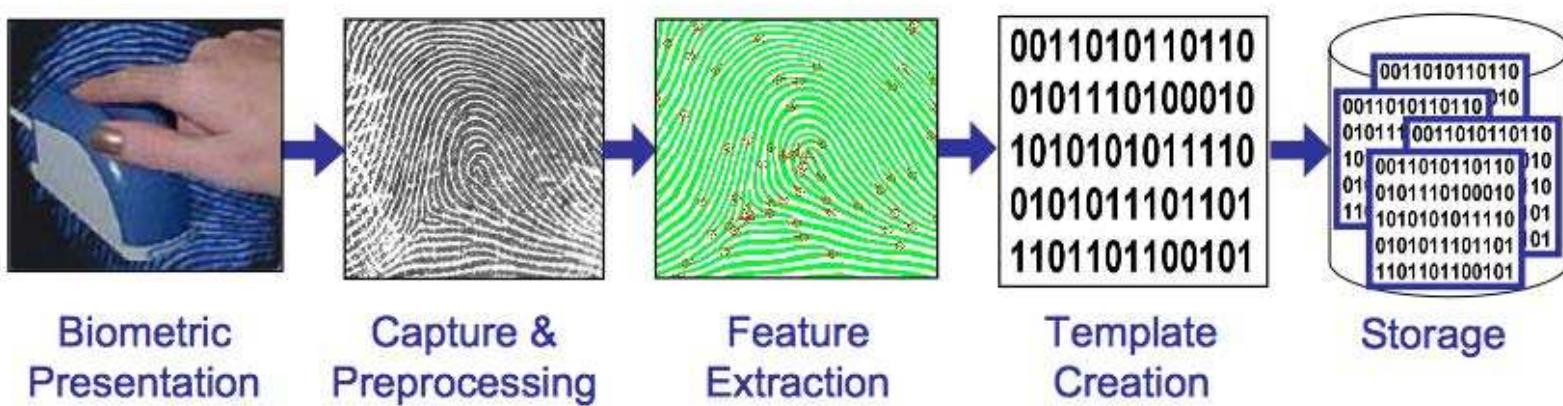
➤ Architettura della Modalità/Fase di Enrollment



Architettura Sistemi Biometrici

6/7

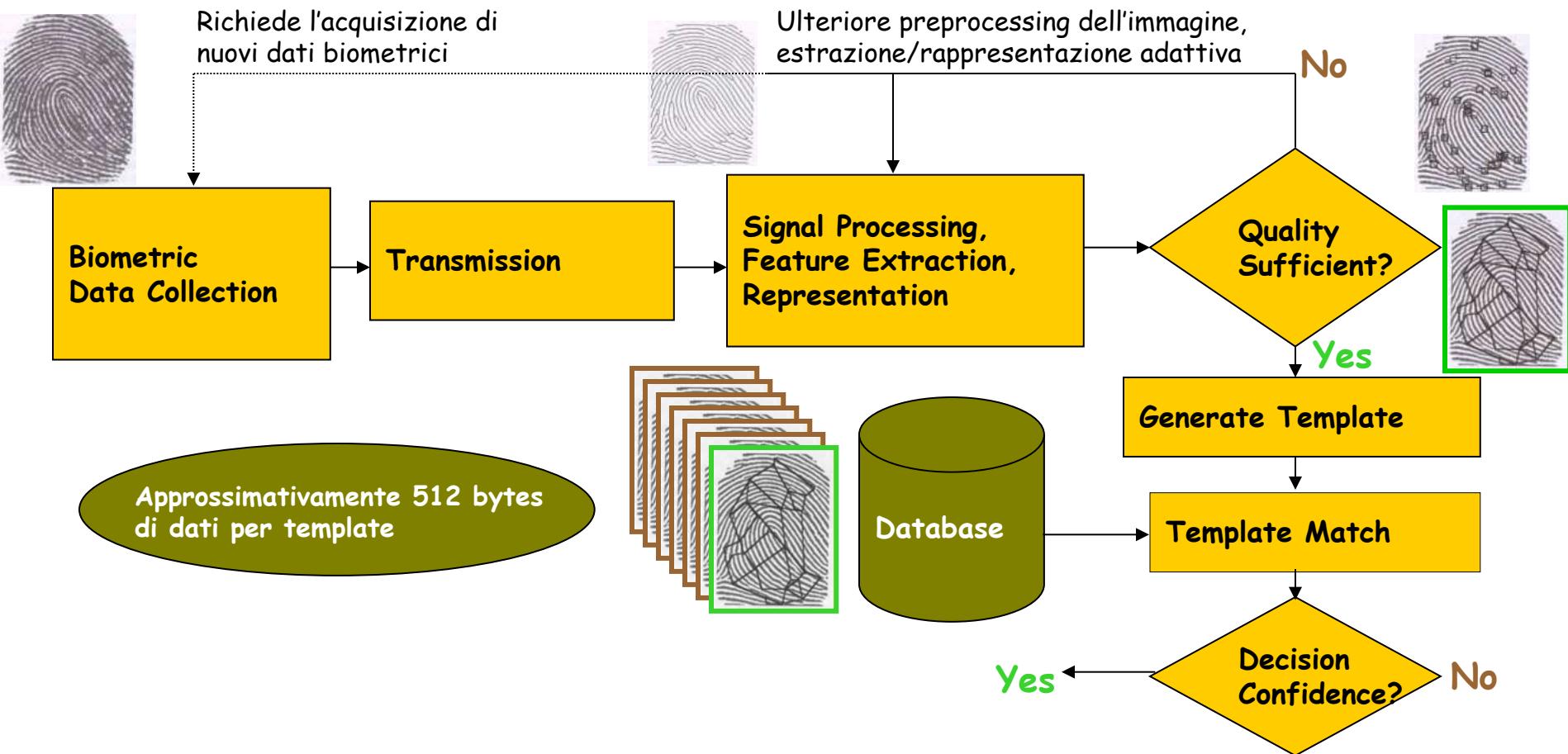
➤ Fase di Enrollment



Architettura Sistemi Biometrici

7/7

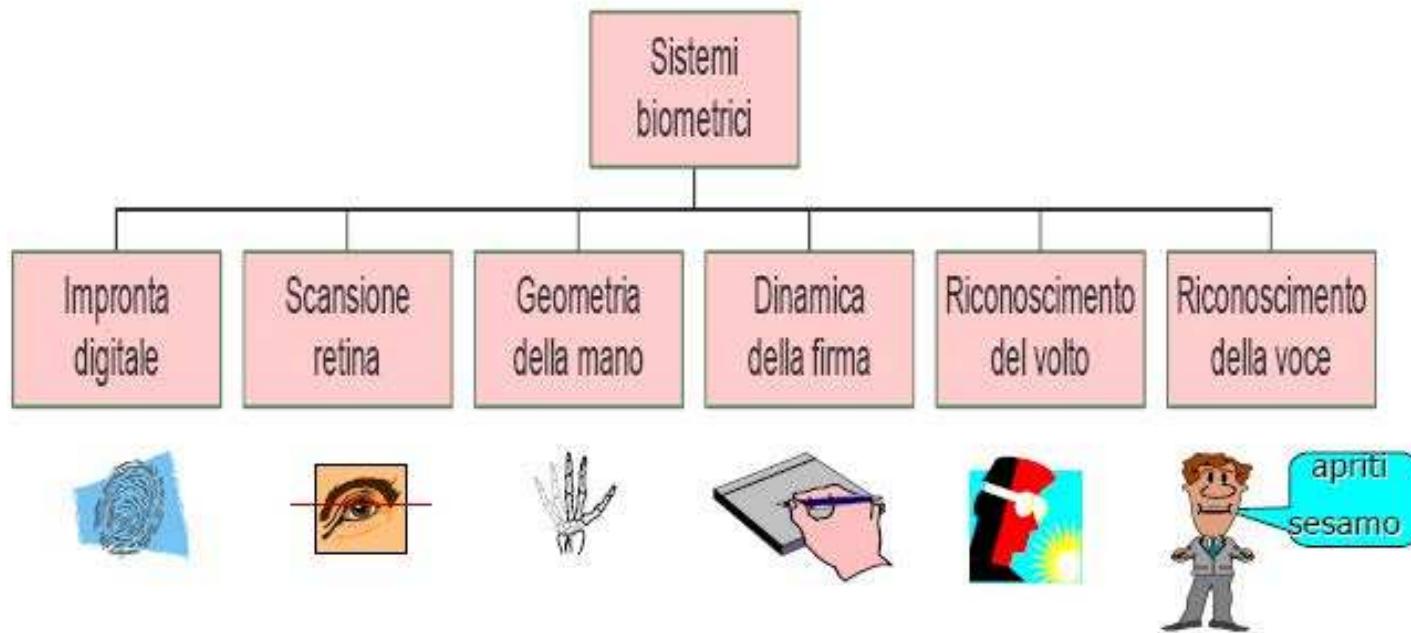
➤ Architettura della Modalità/Fase di Identificazione/Autenticazione



Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
 - Accuratezza delle Tecniche Biometriche
 - Sistemi biometrici su dispositivi portabili
 - Sistemi Biometrici Multimodali

Principali Sistemi Biometrici



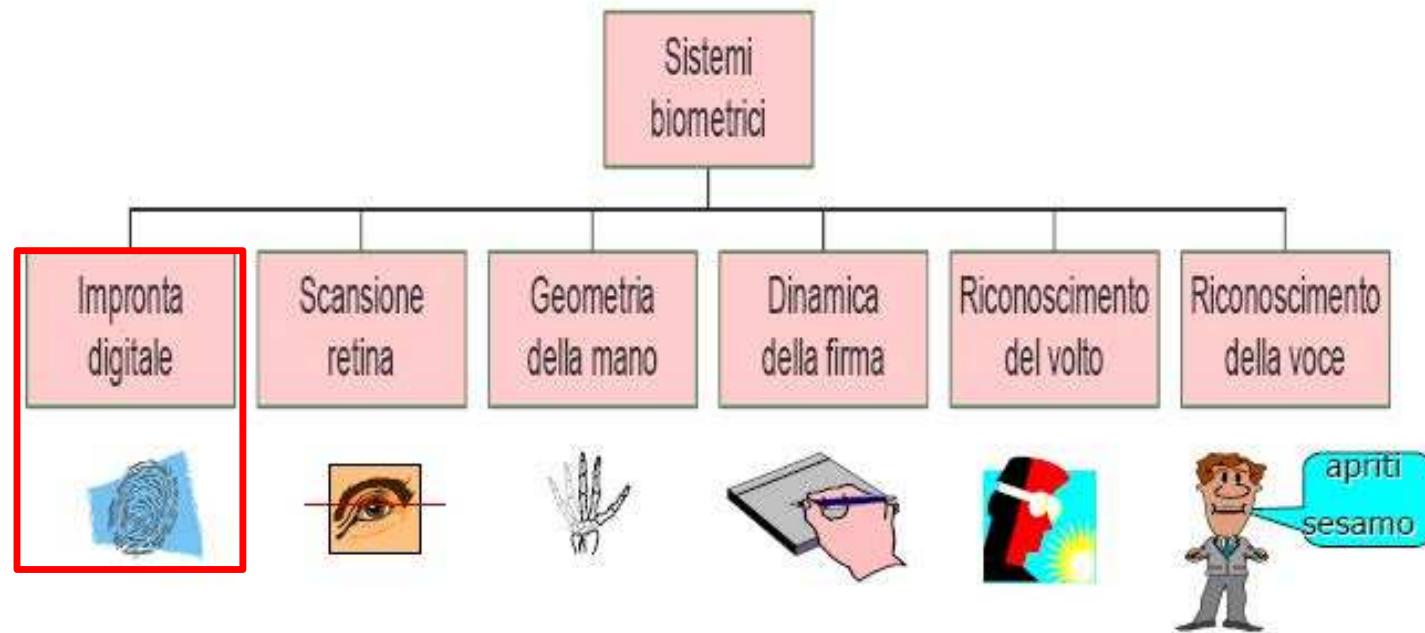
Confronto Caratteristiche alcuni Sistemi Biometrici

	Impronta	Iride	Voce	Volto	Mano
Universalità: limiti	Menomazioni, disabilità	Menomazioni, disabilità	Menomazioni, disabilità	Nessuno	Menomazioni, disabilità
Unicità	Alta	Alta	Bassa	Bassa	Media
Permanenza	Alta	Alta	Bassa	Media	Media
Catturabilità	Media	Media	Media	Alta	Alta

Confronto Caratteristiche alcuni Sistemi Biometrici

	Impronta	Iride	Voce	Volto	Mano
Universalità: limiti	Menomazioni, disabilità	Menomazioni, disabilità	Menomazioni, disabilità	Nessuno	Menomazioni, disabilità
Unicità	Alta	Alta	Bassa	Bassa	Media
Permanenza	Alta	Alta	Bassa	Media	Media
Catturabilità	Media	Media	Media	Alta	Alta

Principali Sistemi Biometrici



Impronte Digitali: Caratteristiche

- **Immutabilità**
 - configurazione e dettagli sono permanenti
- **Unicità**
 - la probabilità di trovare due impronte coincidenti, anche tra gemelli omozigoti, è minore di 10^{-20}
- **Variazioni**
 - configurazioni e dettagli cambiano solo a causa di scottature, incidenti, etc...



Impronte Digitali: Anatomia

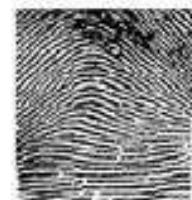
- **Creste** (ridge lines)
 - Insiemi di linee
- **Minuzie**
 - Punti in cui le creste terminano o si biforcano
 - Introdotte da Francis Galton (1882-1916)
 - Classificazione ANSI (1986) basata su
 - Terminazioni
 - Biforcazioni
 - Crossover
 - Indeterminate



Creste: Classificazione

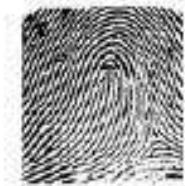
➤ *Arch*

- creste convesse con un picco nel medio



➤ *Loop*

- le creste formano una curva a forma di U e dopo svoltano indietro senza torsione

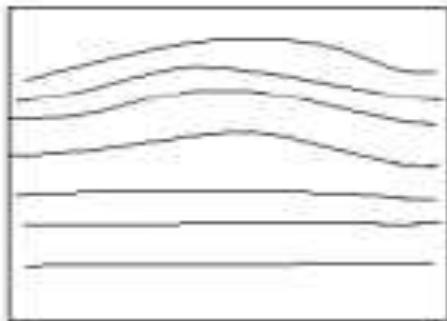


➤ *Whorl*

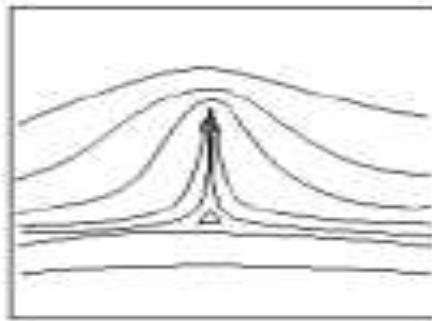
- due delta e creste convesse, almeno una cresta fa un cerchio completo



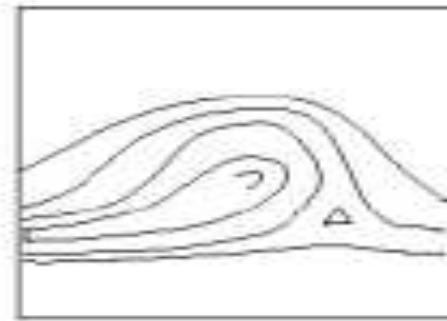
Creste: Classificazione



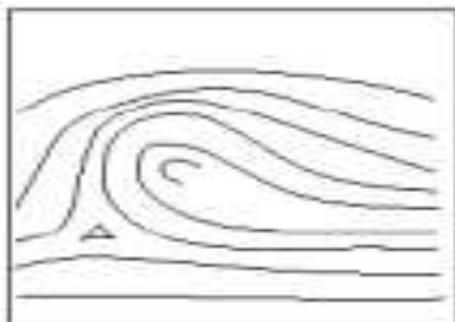
Arch



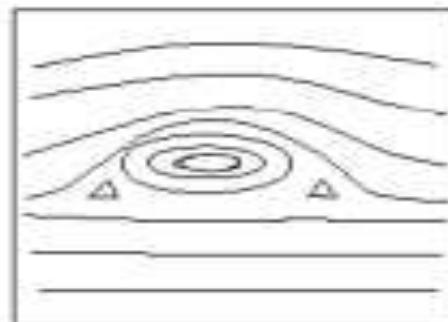
Tented Arch



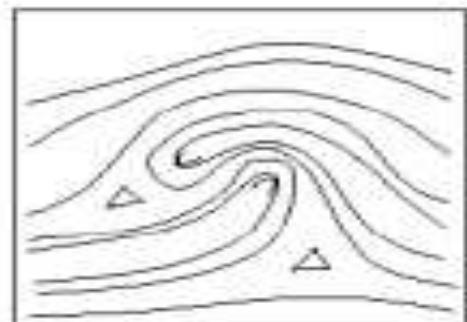
Left Loop



Right Loop



Whorl

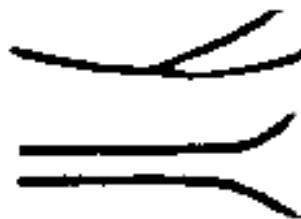


Twin Loop

Minuzie: Classificazione



[a] Ridge endings



[b] A bifurcation & a divergence



[c] A lake



[d] An independent ridge



[e] A spur

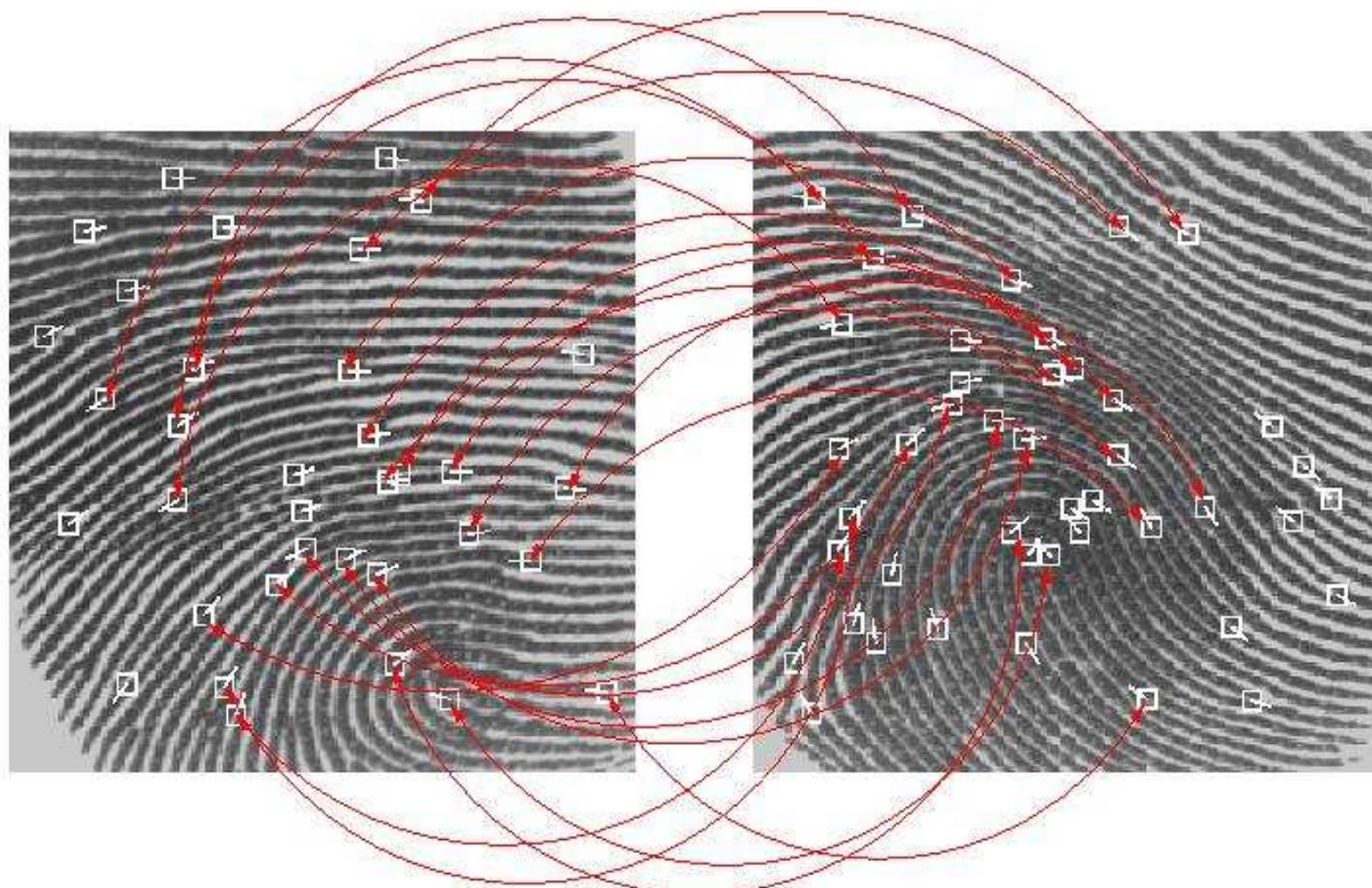


[f] A crossover

Impronte Digitali: Dettagli



Minuzie: Matching



Impronte Digitali: Acquisizione

1/7

➤ Inchiostratura e rollatura delle dita

- Viene utilizzato dell'inchiostro posto a contatto con le dita (*inchiostratura*)
- È necessario effettuare un movimento di *rollatura* con il dito sulla quale è stato applicato l'inchiostro
- In tal modo è possibile effettuare l'acquisizione dell'impronta sulla carta

Impronte Digitali: Acquisizione

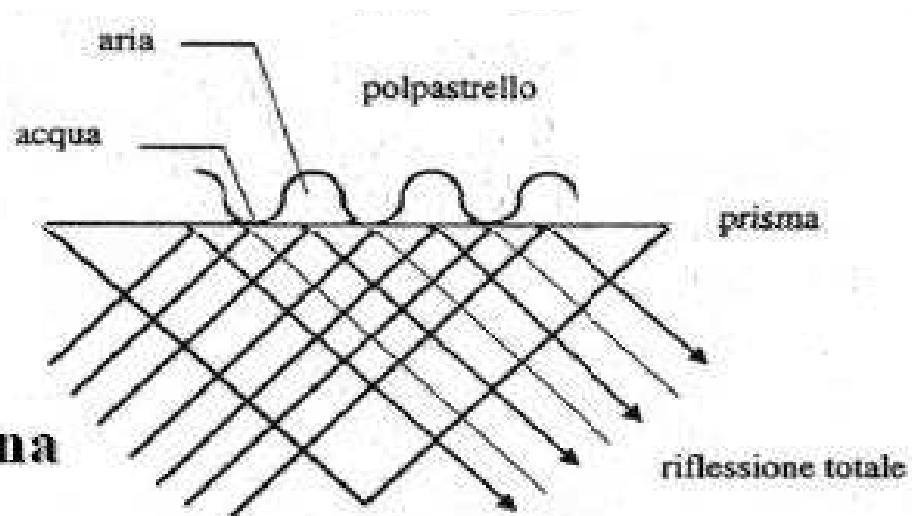
2/7

➤ Acquisizione mediante Sensori Ottici

- Si utilizza un prisma di vetro o materiale plastico sul quale è necessario poggiare il polpastrello
- Consiste nell'acquisizione di una immagine (una fotografia)
- Viene analizzata l'immagine al fine di identificare le features (minuzie, creste, etc) dell'impronta
- Miniaturizzazione difficile dei dispositivi basati su sensori ottici

Impronte Digitali: Acquisizione

3/7



**luce immessa da una
faccia del prisma**

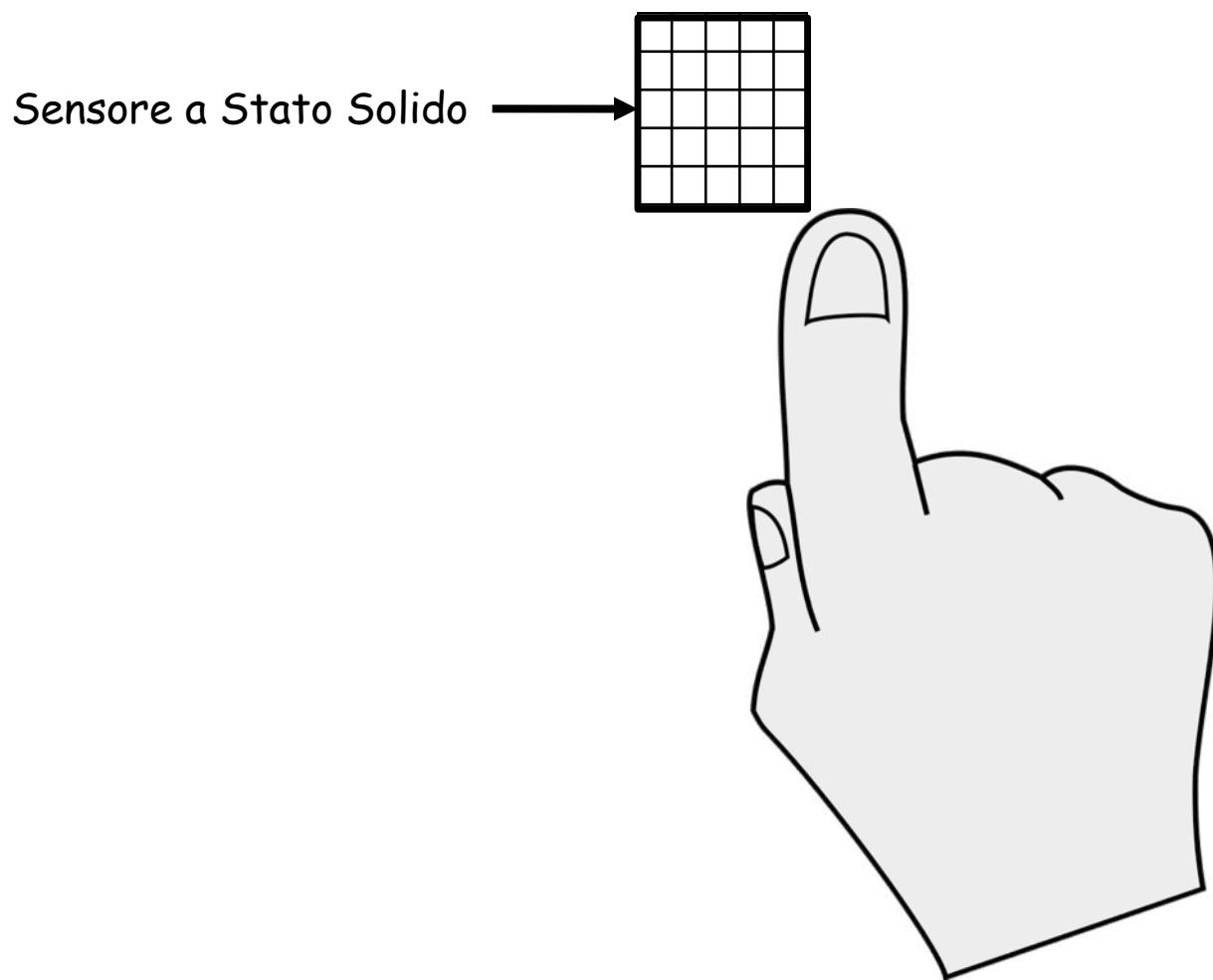
Impronte Digitali: Acquisizione

4/7

- Acquisizione mediante Sensori a Stato Solido
 - Tipicamente utilizzati nei dispositivi portabili (smartphone, tablet, ultrabook, etc)
 - Sensore costituito da una matrice di *celle*
 - Ciascuna cella è sostanzialmente composta da un circuito capacitivo di piccolissime dimensioni
 - Posizionando il dito sul sensore vengono generate ed acquisite piccole cariche elettriche
 - L'intensità di tali cariche dipende dalla distanza della pelle
 - Questo permette di identificare le *features* (minuzie, creste, etc) dell'impronta
 - Maggiornemente miniaturizzabili rispetto ai sensori ottici
 - Qualità generalmente inferiore rispetto ai sensori ottici

Impronte Digitali: Acquisizione

5/7



Impronte Digitali: Acquisizione

6/7

- Acquisizione mediante Sensori ad Ultrasuoni
 - Il sensore invia degli ultrasuoni in direzione della superficie del polpastrello e cattura l'eco prodotto
 - Necessità di un dispositivo abbastanza grande
 - Lentezza nell'acquisizione dell'impronta

Impronte Digitali: Acquisizione

7/7

- Il *template* viene memorizzato in un database
- Viene utilizzato per confrontare l'impronta digitale in tempi successivi
- Varia da 100 bytes a 1000 bytes



Impronte digitali: Problemi

- Pulizia del trasduttore
- L'accuratezza dipende dal dito da identificare
- Sono associate all'identificazione dei criminali



Impronte Digitali: Dove?

- Mastercard e Visa
- Charles Schwab e Company
- Walt Disney World ad Orlando
- Purdue Employees Federal Credit Union
(PEFCU)



Impronte Digitali

Attacchi ...

The screenshot shows the BBC News website interface. At the top, there's a red banner with the BBC logo and a link to "One-Minute World News". Below the banner, the main navigation menu includes "News Front Page", "Africa", "Americas", "Asia-Pacific" (which is highlighted in red), "Europe", "Middle East", "South Asia", "UK", "Business", "Health", "Science & Environment", "Technology", "Entertainment", and "Also in the news". On the right side of the page, a large headline reads "Malaysia car thieves steal finger". Below the headline, it says "By Jonathan Kent BBC News, Kuala Lumpur". A sub-headline states: "Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system." The text continues: "The car, a Mercedes S-class, was protected by a fingerprint recognition system. Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb. The gang, armed with long machetes, demanded the keys to his car. It is worth around \$75,000 second-hand on the local market, where prices are high because of import duties. Stripped naked The attackers forced Mr Kumaran to put his finger on the security panel to start the vehicle, bundled him into the back seat and drove off. But having stripped the car, the thieves became frustrated when they wanted to restart it. They found they again could not bypass the immobiliser, which needs the owner's fingerprint to disarm it. They stripped Mr Kumaran naked and left him by the side of the road - but not before cutting off the end of his index finger with a machete. Police believe the gang is responsible for a series of thefts in the area." At the bottom left, there's a section titled "RELATED BBC SITES" with links to "SPORT", "WEATHER", "ON THIS DAY", "EDITORS' BLOG", "Languages" (with icons for Chinese, Vietnamese, Indonesian, and Thai), and "TIẾNG VIỆT", "INDONESIA", and "Bahasa".

Impronte Digitali



Attacchi ...5 Aprile 2016



Politica Mondo Cronaca Economia Sport Motori Spettacoli Tecnologia Natura Fun Salute Cucina Istituto Luce D Edizioni locali▼

SPECIALI CASO GUIDI BRUXELLES SOTTO ATTACCO TERRORISMO IS AMMINISTRATIVE 2016 GOVERNO RENZI IMMIGRATI GIUBILEO STRAORDINARIO ELEZIONI USA 2016

00:11 / 04:44

▶ Polizia di Stato

f 30 Twitter g+ Link Embed

Visto 3.018 volte

di Matteo Sacchi

Commenta

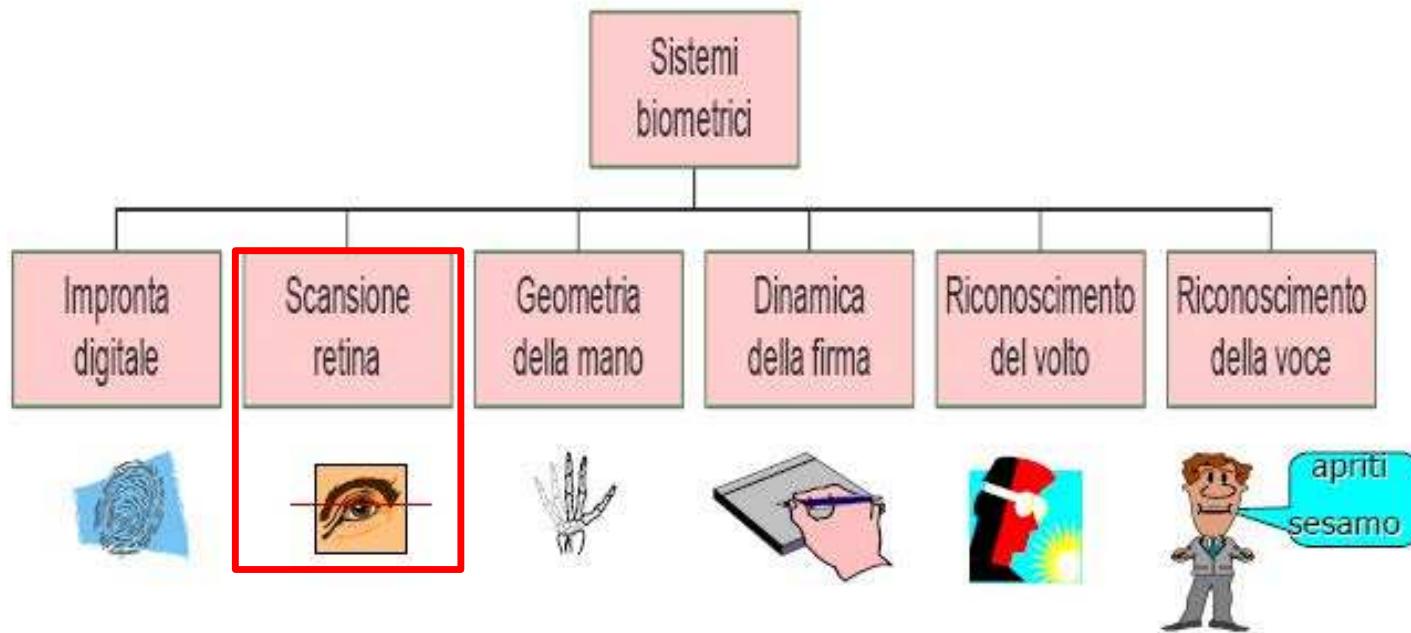
5 APRILE 2016

Milano, il dito di gomma per entrare in banca: il tutorial del rapinatore

La squadra mobile di Milano ha arrestato tre persone per una rapina compiuta al Monte dei Paschi di Siena di Rozzano (Milano) pochi giorni fa. Tutti i componenti della banda - spiegano dalla questura, sono pregiudicati, compreso 'il presidente', 77 anni. E' lui il 'protagonista' del video acquisito dagli investigatori. Lo si vede mentre parla con uno dei complici fuori dalla banca. Dalle immagini delle telecamere si vede bene anche la tecnica "del dito di gomma", una sorta di ditale in silicone usato per falsare la scansione dell'impronta digitale nella bussola d'ingresso. E quindi per non essere individuabili neanche dopo i rilievi della scientifica sui luoghi delle rapine. Il bottino incassato dalla banda è di 110mila euro. La mobile è intervenuta nel momento in cui i ladri stavano abbandonando la banca lasciandosi dietro i dipendenti e un cliente immobilizzati con fascette da elettricista

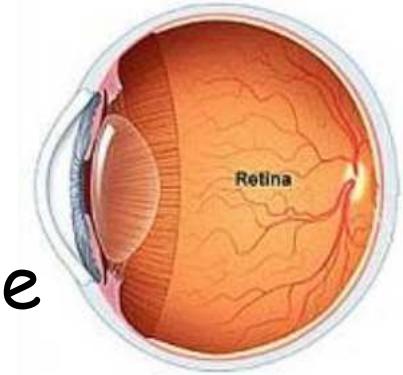
Edizione Milano • Milano, il dito di gomma per entrare in banca: il tutorial del rapinatore

Principali Sistemi Biometrici



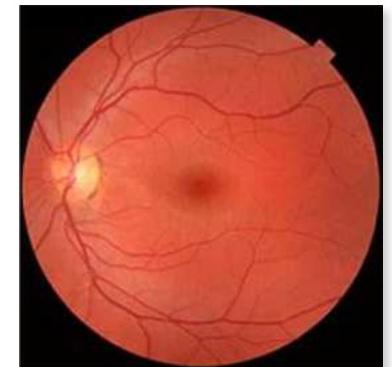
Retina

Membrana più interna del bulbo oculare

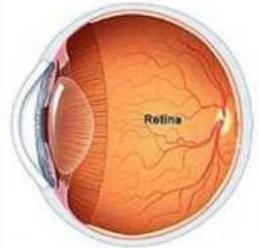


Struttura dei vasi sanguigni presenti sul fondo dell'occhio

- Unica in ogni essere umano (anche tra gemelli identici)
- Non subisce alterazioni ambientali
- Stabile per tutta la vita



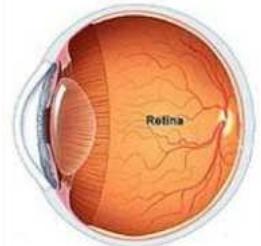
Retina: Acquisizione - 1/2



L'acquisizione è eseguita dirigendo un fascio di luce a bassa intensità nella pupilla dell'utente, che deve accostare l'occhio al dispositivo per pochi secondi

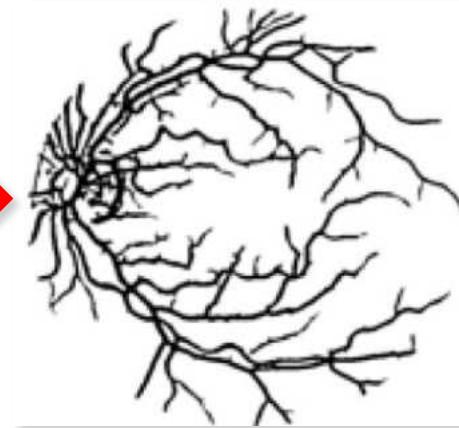
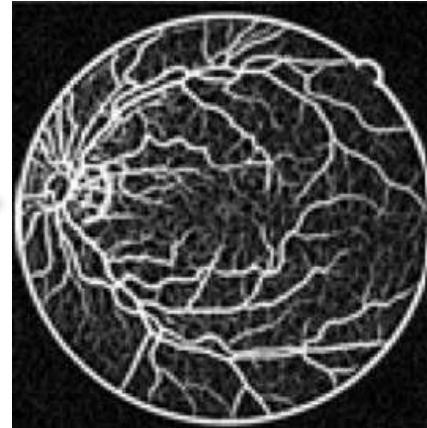
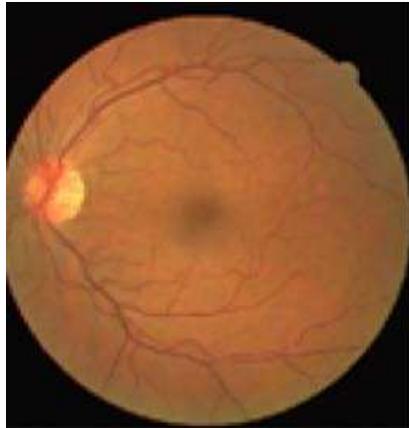


Retina: Acquisizione - 2/2



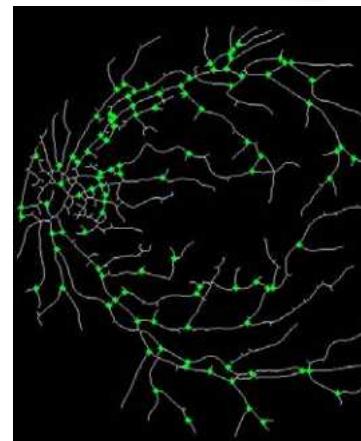
- L'acquisizione è eseguita con un fascio di luce ad infrarosso a bassa intensità, tracciando una traiettoria circolare rispetto al fondo dell'occhio
- I capillari pieni di sangue assorbono l'infrarosso più della zona circostante
 - Causando una variazione nell'intensità della riflessione
- Questi valori danno luogo ad un template di 80 byte

Retina: Minuzie

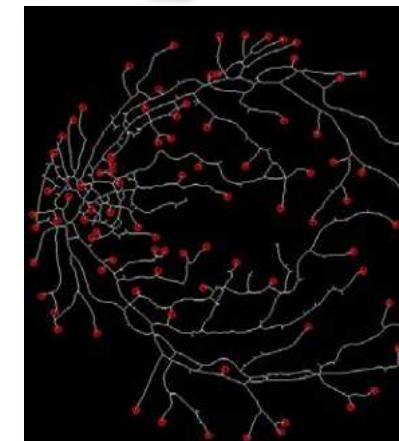


Ending	Bifurcation	Crossover

Island	Lake	Spur



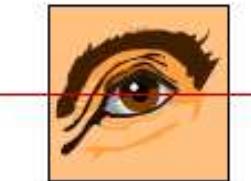
Bifurcation point



Ending point

Scansione della Retina

- Le forme delle vene nella retina sono uniche per ogni individuo (Simon e Goldstein, 1935)
- Il primo sistema, **EyeDentify 7.5**, è apparso nel 1985
- Le caratteristiche della retina sono misurate da formule matematiche (Daugman, 1994)



Retina: Vantaggi

- Alta protezione: Interna all'occhio
- Stabile per tutta la vita
- Unicità
- Basso errore di riconoscimento

Retina: Svantaggi - 1/2

- Difficile da acquisire
- Oscurata da ciglia, lenti, riflessione
- Non visibile se non ben illuminata
- Localizzata dietro superficie curva e riflettente
- Occhio fermo

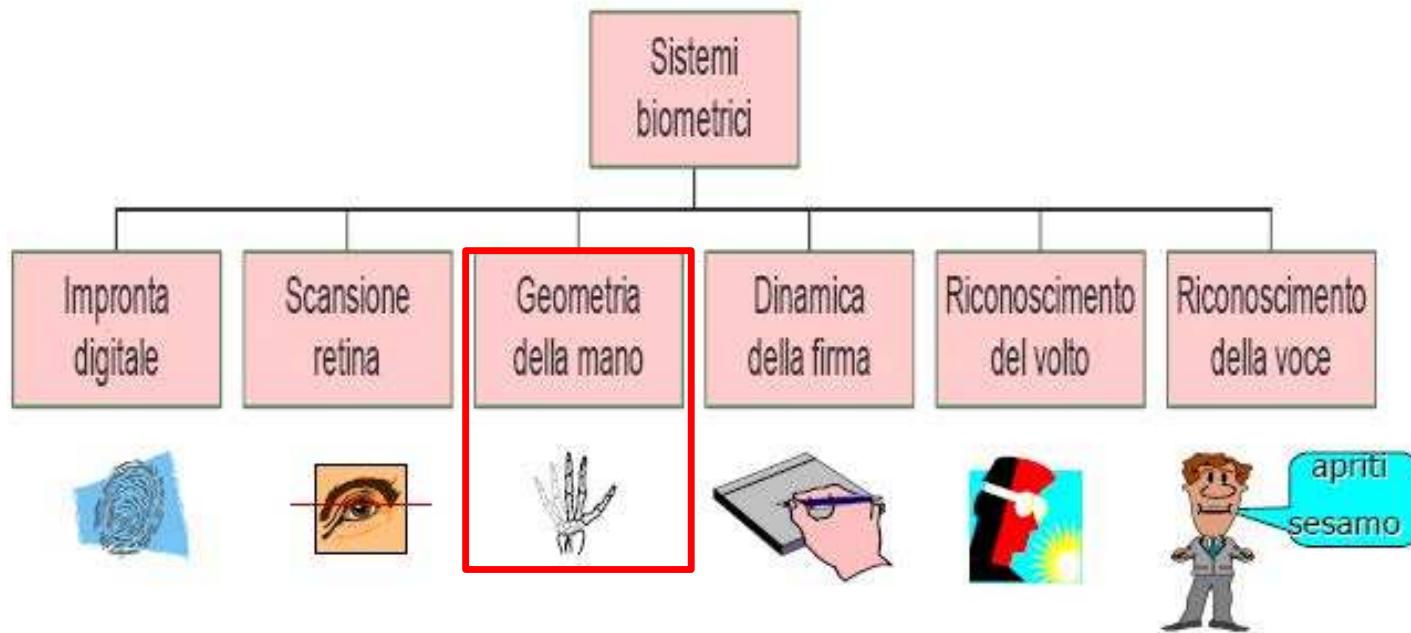
Retina: Svantaggi - 2/2

- Possibili alterazioni per malattie
 - Glaucoma, diabete, pressione alta, etc
- Potrebbe essere percepita come invasiva
- Cooperazione utente
 - Sguardo nella telecamera ed occhio fermo

Retina: Uso

- Pentagono
- Agenzie governative e militari
- Central Intelligence Agency (CIA)
- Federal Bureau Investigation (FBI)
- National Aeronautics and Space Administration (NASA)

Principali Sistemi Biometrici



Geometria della Mano

- È considerato il nonno di tutti i sistemi biometrici
- Misura le caratteristiche fisiche della mano
 - lunghezza dita
 - larghezza mano
 - spessore dita
- Il primo sistema fu adottato 20 anni fa dalla banca Shearson Hamil in Wall Street



Geometria della Mano: Caratteristiche

➤ Unicità

- virtualmente la mano di un individuo è plasmata in modo differente da un'altra mano

➤ Immutabilità

- la forma della mano di una persona non cambia significativamente nel corso del tempo



Geometria della Mano: Misure Fisiche

- Acquisizione meccanica
- Misure catturate da un apparecchiatura *charge-coupled (CCD)*
- Dettagli della superficie (linee, cicatrici, unghie e immondizia) trascurati
- La sagoma della mano viene memorizzata tridimensionalmente
- *Template* costruito in base alle misure della mano



Geometria della Mano: Vantaggi

- Velocità di operazione: 1 secondo
- Affidabilità
- Accuratezza
- Template piccolo: sotto i 10 byte

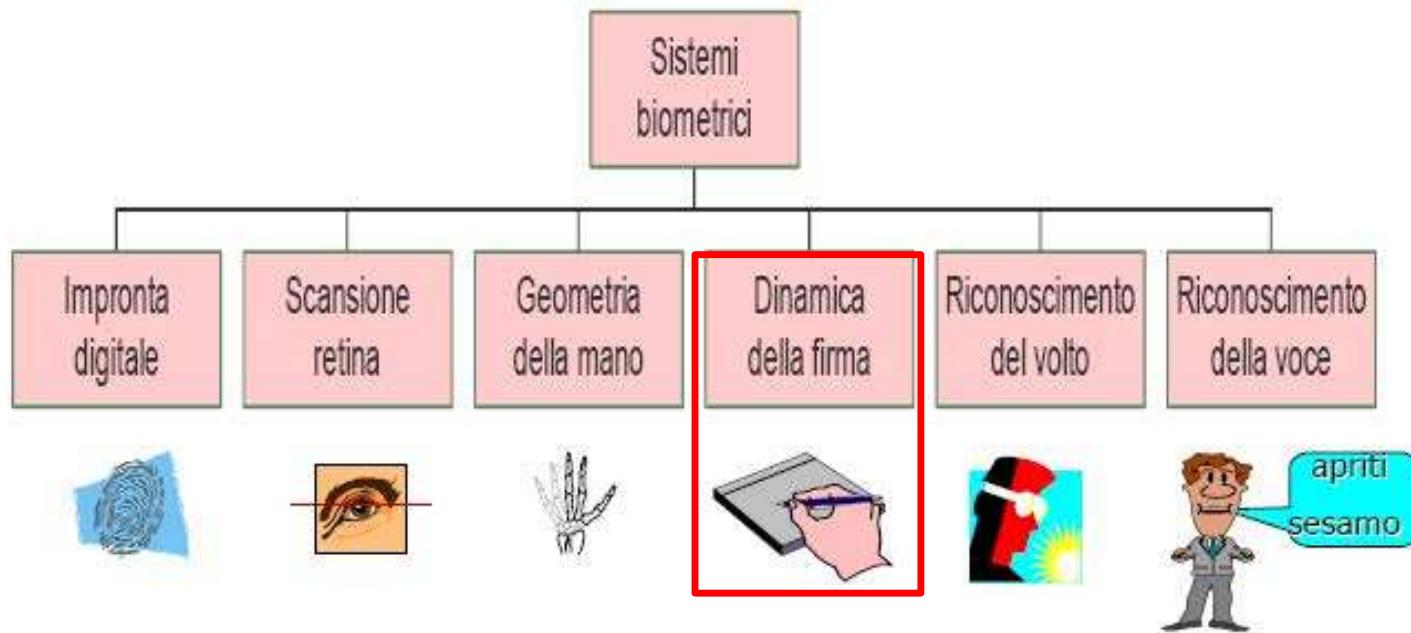


Geometria della Mano: Dove?

- I giochi olimpici nel 1996
- Aeroporto internazionale di San Francisco
- L'università di Georgia

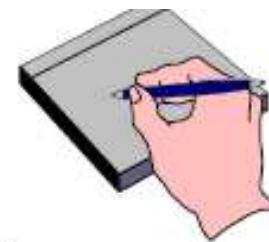


Principali Sistemi Biometrici



Dinamica della Firma

- Semplice confronto della firma
 - facile da falsificare
 - molti hanno diverse variazioni nella firma
- In aggiunta al controllo delle coordinate:
 - controllo pressione, tempo, velocità, accelerazione
- Per maggiore sicurezza:
 - cambiare ogni volta la frase da scrivere!



Dinamica della Firma: Problema

Ridurre la differenza tra le parti della firma

- abituali e costanti
- alterate in base allo stato d'animo

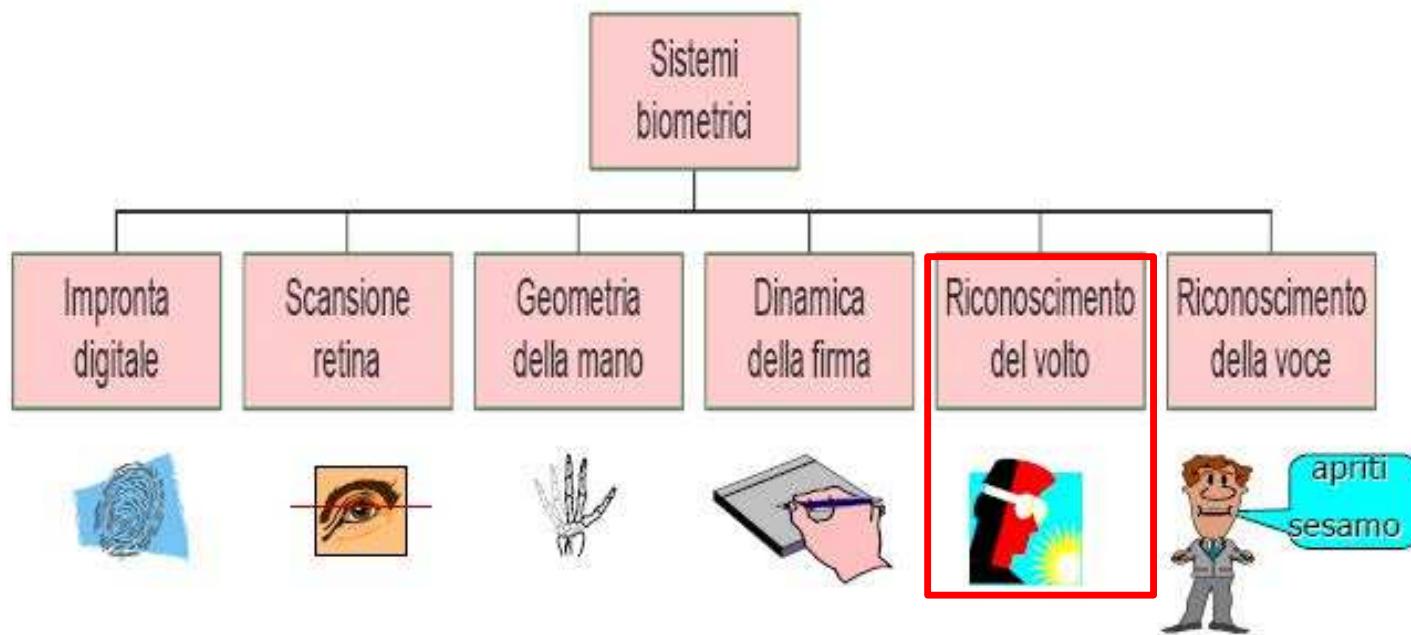


Dinamica della Firma: Dove?

- Prigione di Pentonville in Inghilterra
- International Revenue Service (IRS)
- Banca di Manhattan



Principali Sistemi Biometrici



Riconoscimento del Volto

Metodi Basati su Immagini

- I metodi basati su immagini utilizzano informazioni ottenute dall'acquisizione del volto, mediante immagini o sensori ottici (fotocamere, etc)

- **Vantaggi**
 - Velocità e Semplicità di implementazione
- **Svantaggi**
 - Problematiche di acquisizione (ad esempio, variazione della posa, variazione della luminosità, etc)

Riconoscimento del Volto

Metodi Basati su Caratteristiche

- I metodi basati su caratteristiche utilizzano caratteristiche morfologiche del volto e la loro disposizione geometrica
 - Assegnano un significato semantico alle regioni di interesse individuate
-
- **Vantaggi**
 - Maggiore robustezza per quanto riguarda le condizioni di posa e luminosità
 - **Svantaggi**
 - Complessità computazionale più elevata rispetto ai metodi basati su immagini

Riconoscimento del Volto

Metodi Basati su Caratteristiche

Tecnica Elastic Bunch Graph Matching

- Utilizzo di grafi per la rappresentazione del volto
- Tecnica basata sulla ricerca di una corrispondenza tra grafi che rappresentano un volto
- Mappatura mediante alcuni punti specifici, detti *fiducial points*
 - I fiducial points rappresentano pupille, angoli della bocca, punta del naso, etc, di un volto

Riconoscimento del Volto

Metodi Basati su Caratteristiche

Tecnica Elastic Bunch Graph Matching

1. Posizionamento dei *fiducial points* sul volto



2. Calcolo delle caratteristiche individuali

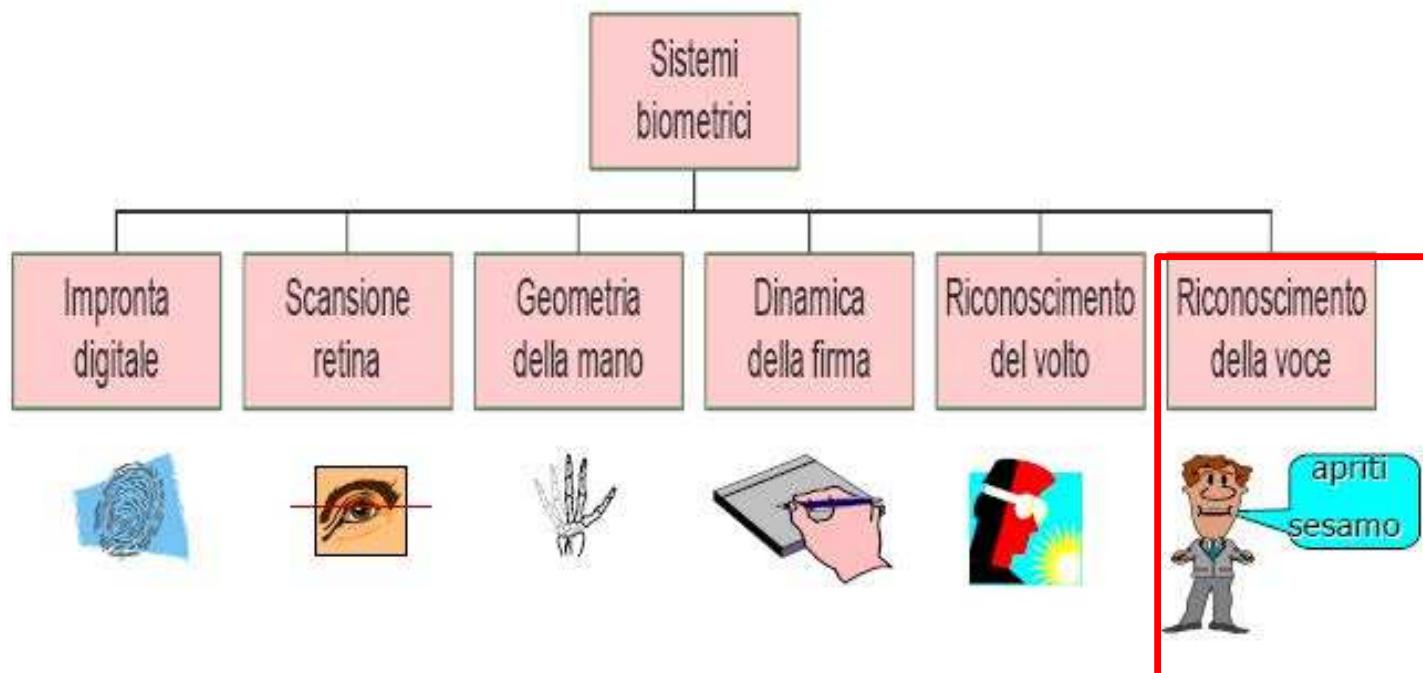


3. Conoscendo la posa del volto è possibile confrontare il grafo con tutti i grafî precedentemente memorizzati



4. Ricavati i valori di similarità, si decide se attribuire al volto l'identità del soggetto

Principali Sistemi Biometrici



Riconoscimento della Voce

1/2

➤ **Template**

- costruito pronunciando ripetutamente una frase fissa

➤ **Parametri**

- tono
- dinamica
- waveform



Riconoscimento della Voce

2/2

➤ *Speaker dependent*

- Sistema addestrato a riconoscere un dato utente
- Contiene un vocabolario tra 30.000 e 120.000 parole

➤ *Speaker independent*

- Sistema non addestrato
- Può essere utilizzato da chiunque
- Contiene un vocabolario più piccolo



Riconoscimento della Voce: Vantaggi

- Affidabilità
- Flessibilità
- Tecnologia biometrica naturale
- Occhi e mani sono liberi



Riconoscimento della Voce: Svantaggi

- Training lungo
- L'efficacia dipende dal livello di rumore
- La voce cambia col tempo e ... con le malattie
- A molti non piace parlare ad un computer
- Computazione complicata (trasformata di Fourier,...)
- Attacchi di replay
 - Difesa: cambiare ogni volta la frase da leggere!

Ricocoscimento della Voce: Dove?

- Texas Instruments, primo prodotto (1990)
- General Motors
- Ospedale di Chicago
- Charles Schwab e Company



Altre Tecniche Biometriche

1/4

- Segno delle labbra 
- Segno della pianta dei piedi 
- Odore 
- Forma delle vene nella mano o nel polso 
- Risposta dello scheletro ad uno stimolo fisico 

Scarsa accettabilità

Altre Tecniche Biometriche

2/4

Ayman Abaza and Arun Ross,

Towards Understanding the Symmetry of Human Ears: A Biometric Perspective,

Proc. of 4th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS),
(Washington DC, USA), September 2010

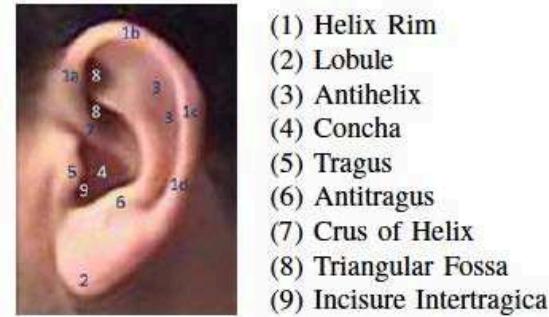


Fig. 1. External anatomy of the ear

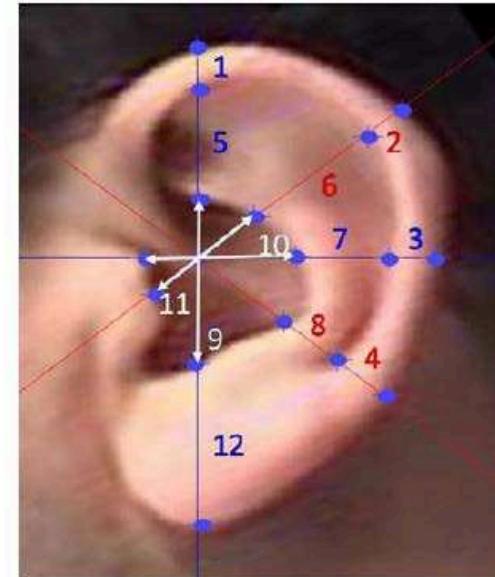


Fig. 2. Iannarelli measurement

Altre Tecniche Biometriche

3/4

... researchers at Japan's Advanced Institute of Industrial Technology developed a system that can recognize a person by the backside when the person takes a seat. The system performs a precise measurement of the person's posterior, its contours and the way the person applies pressure on the seat. The developers say that in lab tests, the system was able to recognize people with 98 percent accuracy. (Dec 25, 2011)



<http://www.physorg.com/news/2011-12-unleash-car-seat-rear.html>

Altre Tecniche Biometriche

4/4

... researchers at Japan's Advanced Institute of Industrial Technology developed a system that can recognize a person by the backside when the person takes a seat. The system performs a precise measurement of the person's posterior, its contours and the way the person applies pressure on the seat. The developers say that in lab tests, the system was able to recognize people with 98 percent accuracy. (Dec 25, 2011)

Commenti sul web:

- tasche posteriori,
- soprabiti lunghi,
- dieta,
- ...



<http://www.physorg.com/news/2011-12-unleash-car-seat-rear.html>

Vascular Pattern Matching - 1/3

- Luce LED a infrarossi
- Dita e dorso della mano
- Non sempre applicabile



Vascular Pattern Matching - 2/3

➤ Vantaggi

- Semplicità nell'acquisizione
- Elevata unicità
- Invarianza temporale
- Bassa intrusione

Vascular Pattern Matching - 3/3

Possibili Applicazioni Future

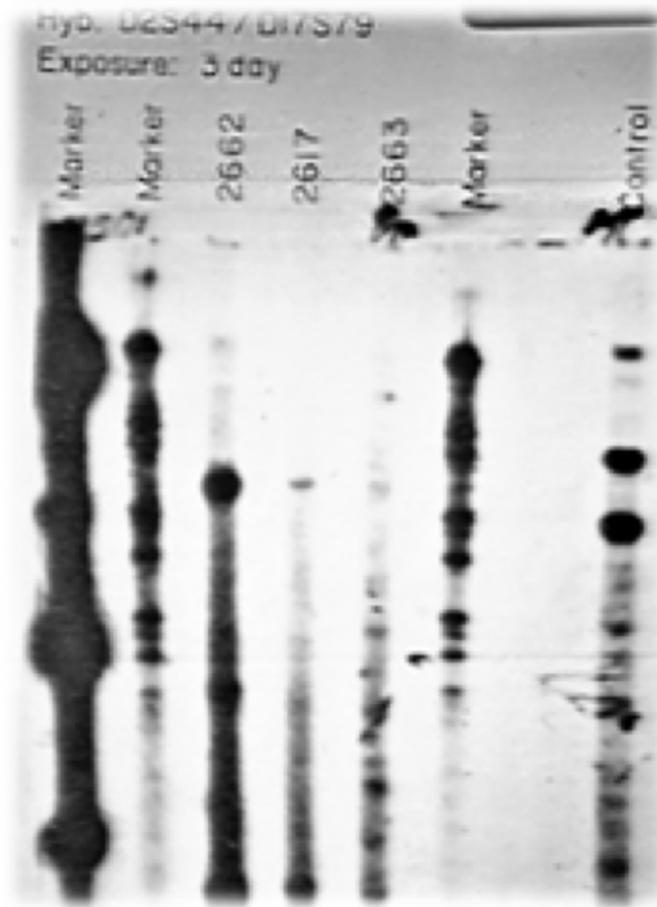
- Fujitsu in collaborazione con Microsoft sta lavorando ad un sistema di riconoscimento dei vasi sanguigni nel palmo della mano (Febbraio 2018)
 - L'obiettivo è quello di rendere tale sistema fruibile su notebook dedicati al mondo business
- Anche Samsung ha brevettato un sistema di riconoscimento dei vasi sanguigni nel palmo, che potrebbe essere implementato in futuro su smartphone

Fonti

- <https://blogs.windows.com/business/2018/02/08/fujitsu-microsoft-focused-advancing-security-modern-workplace/#AZA5qVzgGLzgXDoc.97>
- <https://www.galaxyclub.nl/2017/11/samsung-patent-handpalmherkenning>

DNA Identification

- Ampiamente accettato per le scene del crimine
- Possibili problemi con persone gemelle



Altri Tipi di Sistemi Biometrici

- Keystroke
- Battitura
- Gait
- Andatura



Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Tecniche Biometriche: Accuratezza

1/6

False Non-Match Rate (FNMR)

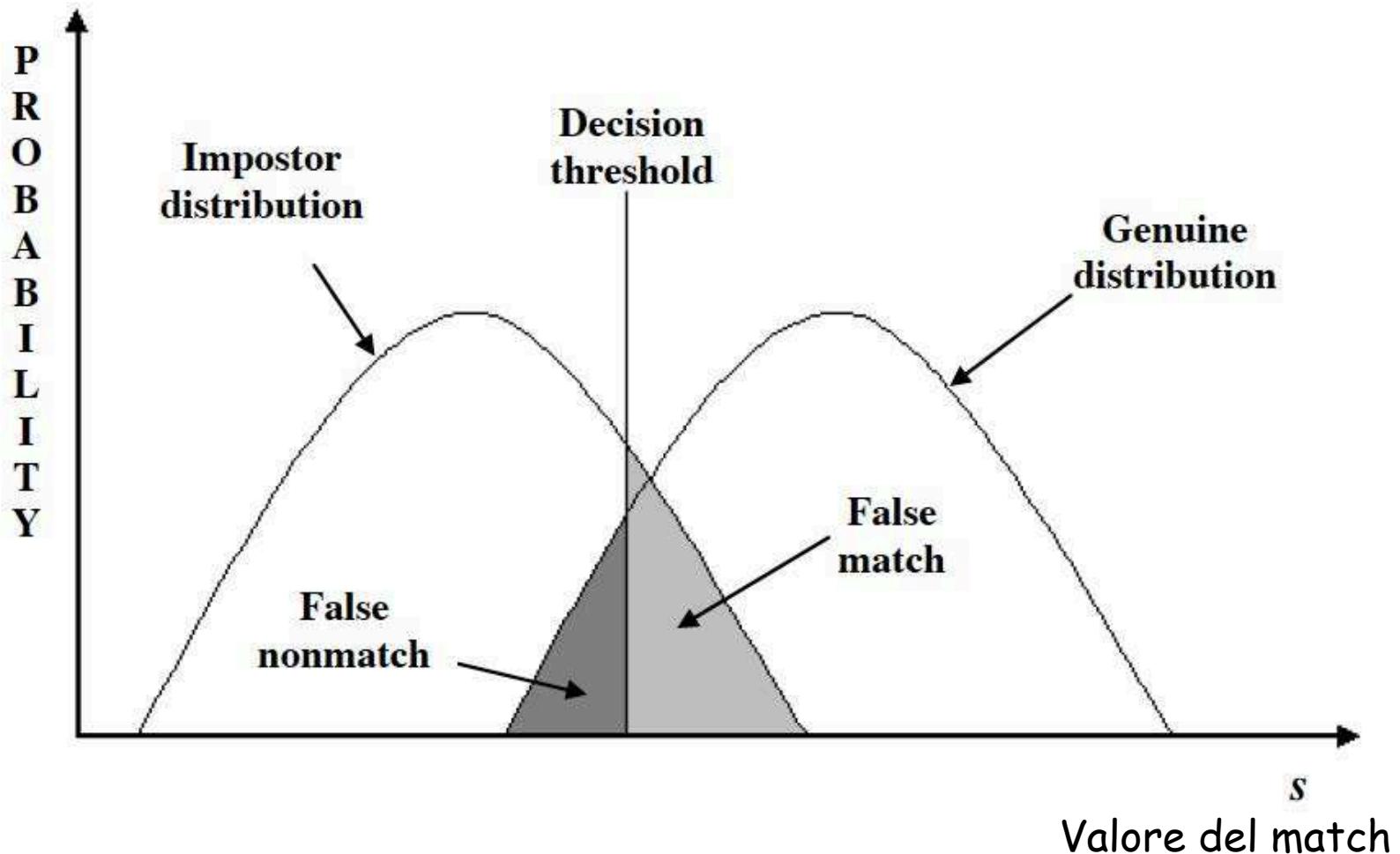
- (Falso rigetto) misure dello stesso utente sono dichiarate appartenere a diversi utenti

False Match Rate (FMR)

- (Falsa accettazione) misure di due diversi utenti sono dichiarate appartenere allo stesso utente

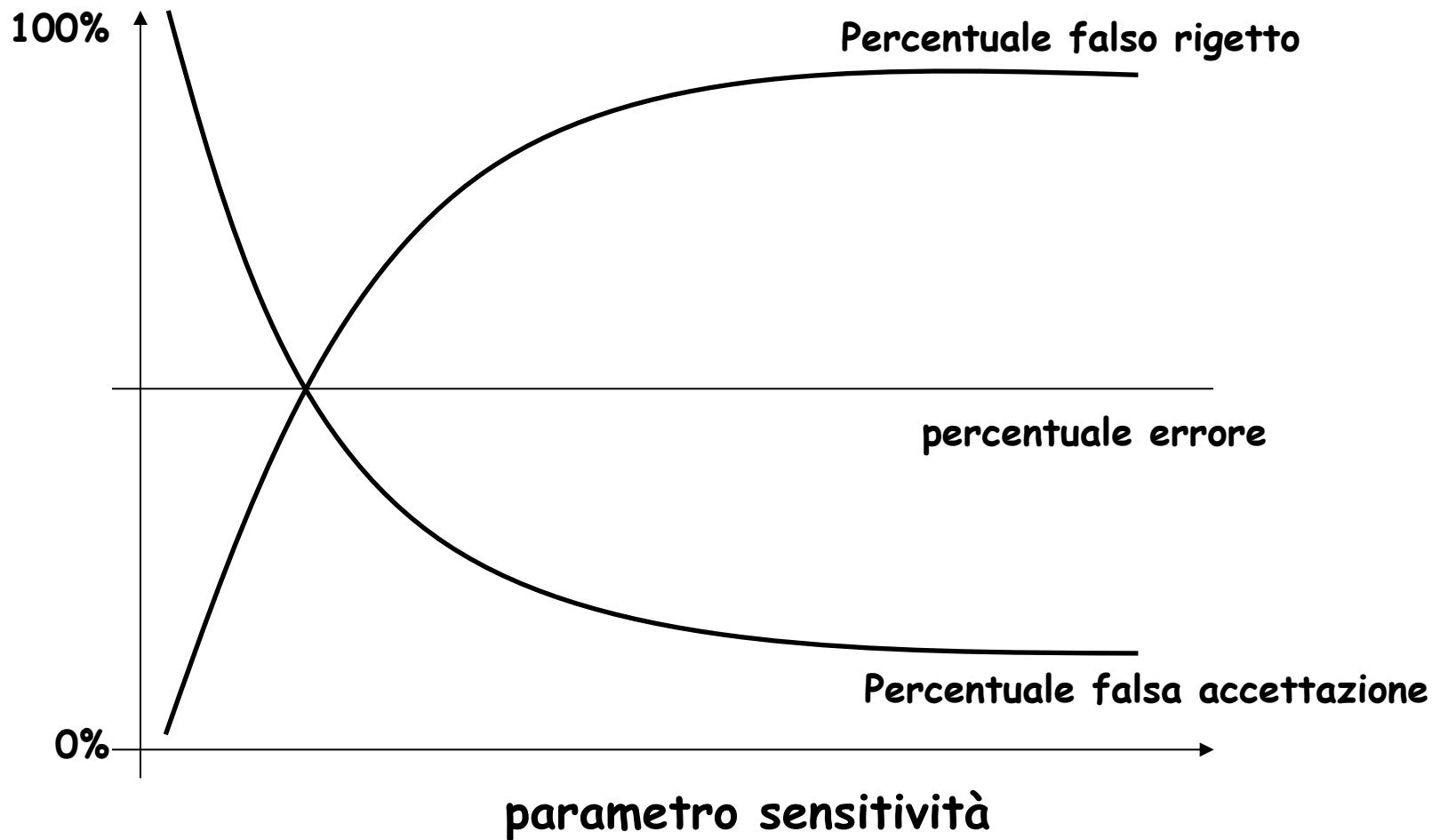
Tecniche Biometriche: Accuratezza

2/6



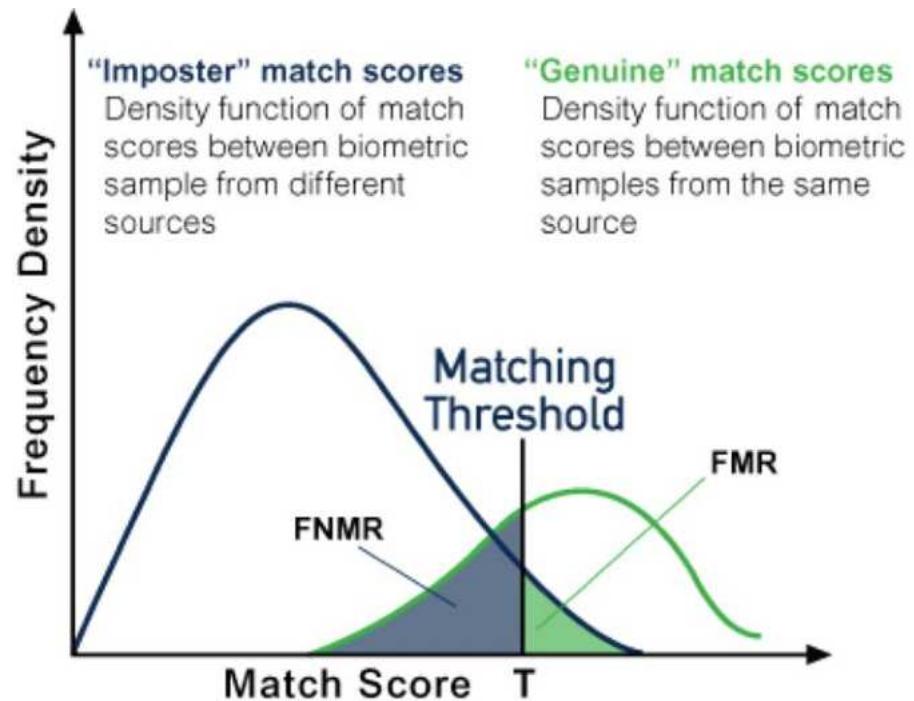
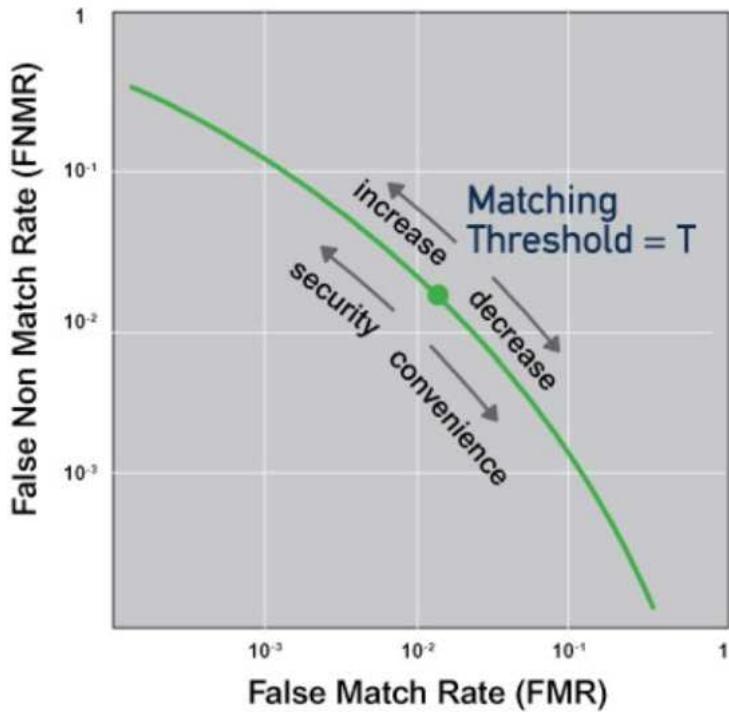
Tecniche Biometriche: Accuratezza

3/6



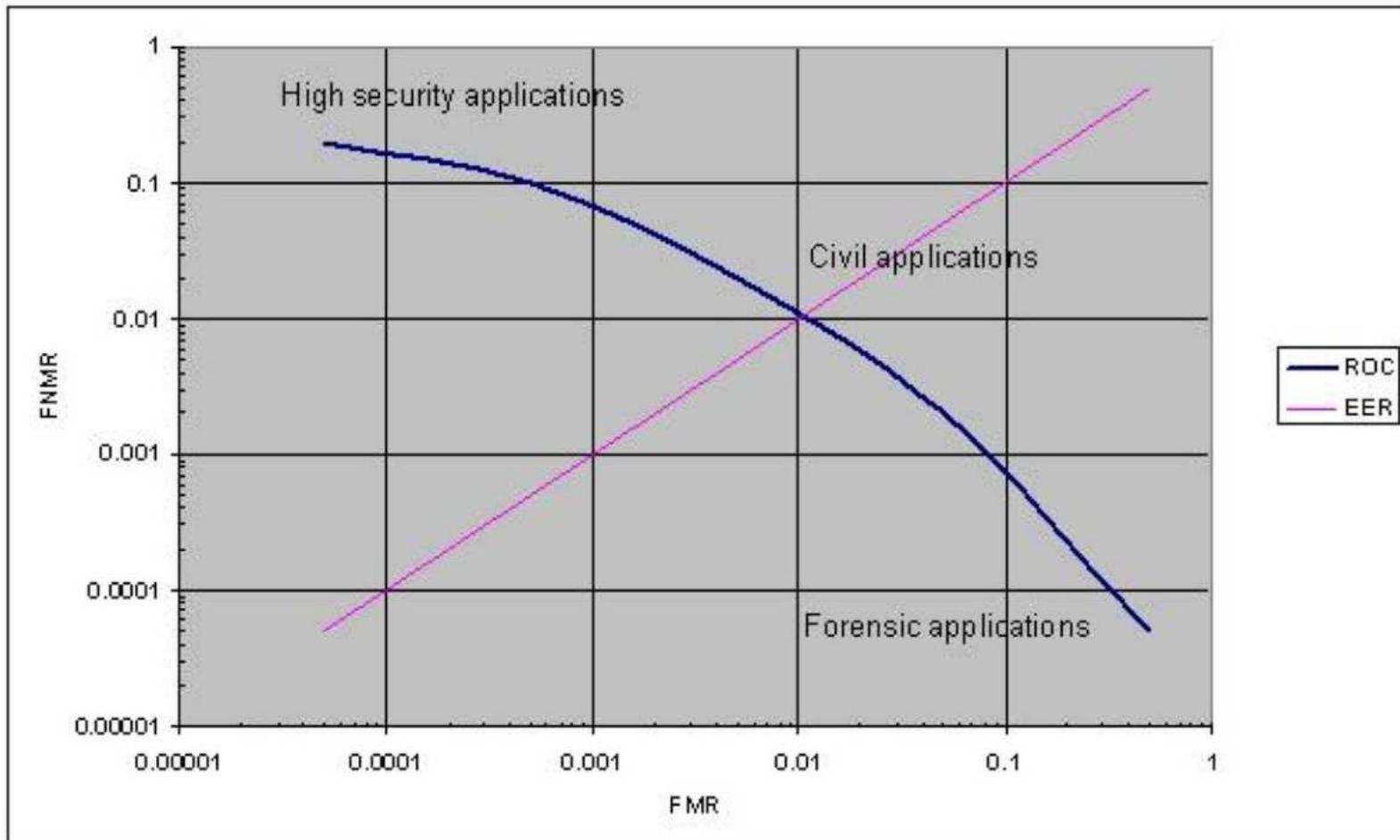
Tecniche Biometriche: Accuratezza

4/6



Tecniche Biometriche: Accuratezza

5/6



Tecniche Biometriche: Accuratezza

6/6

Failure To Capture (FTC)

- Percentuale delle volte che il dispositivo non riesce ad acquisire un campione

Failure To Enroll (FTE)

- Percentuale delle volte che gli utenti non riescono ad essere accettati dal sistema di riconoscimento

Confronto

Biometric characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial thermogram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palmprint	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

Tecniche Biometriche: Valutazioni

- Studio Sandia National Labs, su sistemi commerciali

tecnica	errore
voce	2%
firma	2%
retina	0,40%
mano	0,10%
impronta	9% falso rigetto nessuna falsa accettazione

caratteristica	migliore	peggiore
accettabilità	mano	voce
falso rigetto	mano	impronta
falsa accettazione	mano, retina, impronte	voce
throughput	mano, retina, impronte	voce, firma
difficoltà di imitazione	retina	voce, firma
grandezza template	retina	voce
costo	voce	retina

- Alta percentuale di errore
- Bene usarle insieme alle password!

il sistema controlla ciò che l'utente è + quello che sa

Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Sistemi Biometrici su Dispositivi Portabili

- Negli ultimi anni numerosi dispositivi portabili (smartphone, tablet, ultrabook, etc) hanno integrato sensori per l'autenticazione/identificazione tramite caratteristiche biometriche
- I metodi di autenticazione biometrica rappresentano un'alternativa o un'integrazione ai meccanismi già comunemente utilizzati dai dispositivi portabili
 - Password, PIN, etc

Sistemi Biometrici su Dispositivi Apple - 1/4

- A partire dall'**iPhone 5S** (presentato nel 2013) **Apple** ha integrato nei suoi dispositivi il **Touch ID**
- Un rilevatore di impronte digitali presente nel tasto Home
- È possibile memorizzare fino a 5 impronte digitali



Fonte Immagine: Apple

Sistemi Biometrici su Dispositivi Apple - 2/4

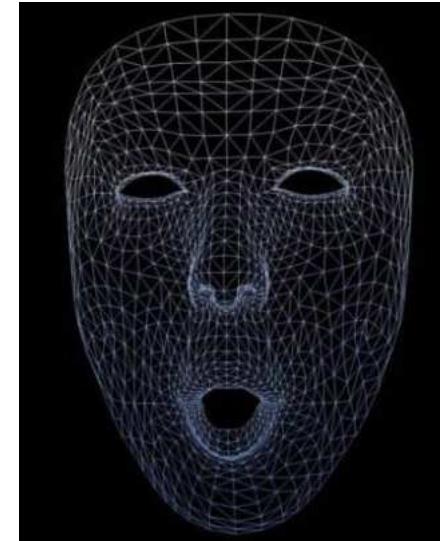
- A partire dall'iPhone X, Apple ha introdotto un sistema biometrico per il riconoscimento del volto, denominato Face ID
- Il sistema Face ID è costituito da diversi sensori, presenti nella parte frontale del dispositivo
 - Fotocamera frontale da 7 MP
 - Emissore ad infrarossi
 - Camera ad infrarossi
 - Sensore per luce ambientale
 - Flood illuminator
 - Sensore di prossimità



Fonte Immagini: Apple

Sistemi Biometrici su Dispositivi Apple - 3/4

- Con il Face ID vengono eseguite le seguenti operazioni
 - **Proiezione** di 30000 punti sul volto dell'utente
 - Sensore utilizzato: *Emissore ad infrarossi*
 - **Acquisizione, mappatura 3D ed analisi** di tali punti
 - Sensore utilizzato: Flood illuminator (in situazioni di scarsa luminosità del soggetto)
 - **Salvataggio** dei dati sul dispositivo



Fonte Immagini: Apple

Sistemi Biometrici su Dispositivi Apple - 4/4

- Tramite il Touch ID/Face ID è possibile
 - Sbloccare il dispositivo
 - Acquistare su
 - App Store
 - iTunes
 - Apple Pay



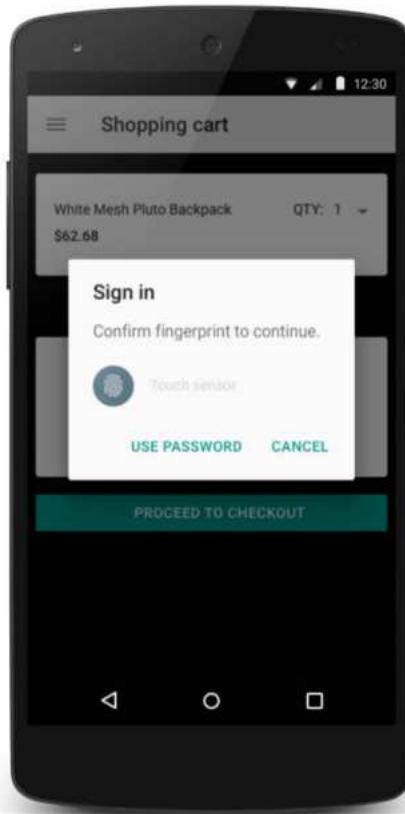
Fonte Immagini: Apple

Sistemi Biometrici su Dispositivi Android - 1/2

- Con le API di Livello 23 presenti su **Android 6.0 (Marshmallow)**, presentato a ottobre 2015, viene introdotto il supporto nativo alle impronte digitali
- Questo permette di
 - Sbloccare il dispositivo
 - Autorizzare acquisti
 - Sbloccare App specifiche dal Google Play Store

Sistemi Biometrici su Dispositivi Android - 2/2

```
<uses-permission  
    android:name="android.permission.USE_FINGERPRINT" />
```



Fonte Immagini: Google

Sistemi Biometrici su Dispositivi Windows 10 - 1/2

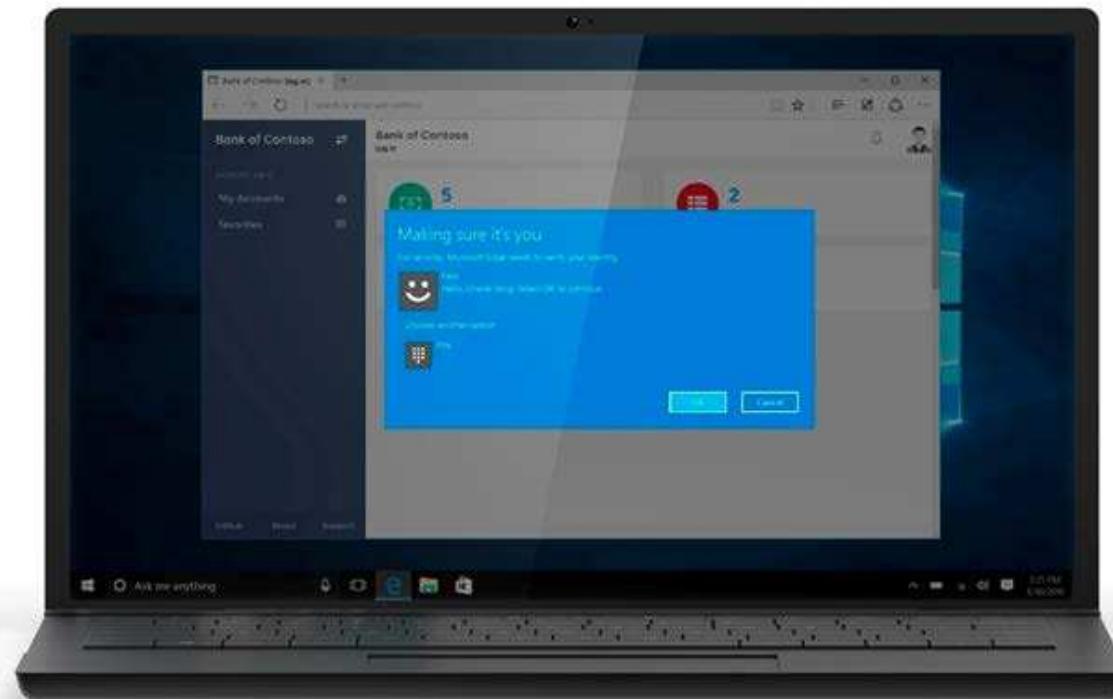
- Introdotto con Windows 10 (luglio 2015), il sistema Windows Hello integra il supporto a caratteristiche biometriche
 - Volto
 - Impronta digitale
 - Iride



Windows Hello:
you are the password
Fonte Immagini: Microsoft

Sistemi Biometrici su Dispositivi Windows 10 - 2/2

- In futuro sarà possibile utilizzare Windows Hello anche per l'autenticazione su siti web mediante il browser Microsoft Edge



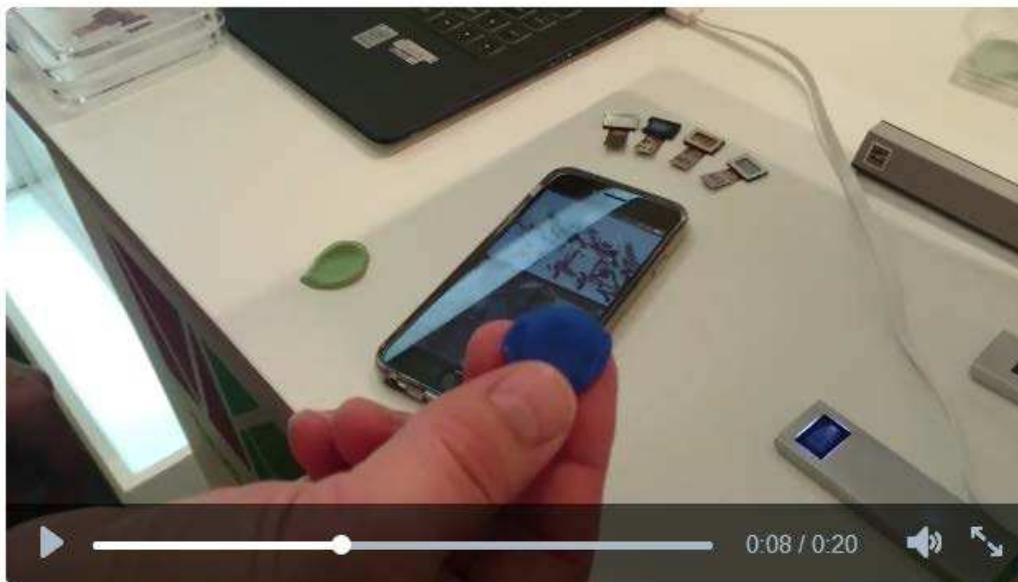
Possibili Criticità dei Sistemi Biometrici su Dispositivi Portabili - 1/5

- Durante il *Mobile World Congress 2016 (MWC 2016)*, il CEO dell'azienda cinese Vkansee (specializzata in lettori di impronte digitali) ha mostrato come **bypassare il Touch ID** di un iPhone
 - Replicando la propria impronta digitale su un po' di pongo
- Per portare a termine l' «attacco» è necessario un contatto fisico con la vittima, in modo da poter replicare l'impronta



MOBILE.
WORLD CONGRESS

Possibili Criticità dei Sistemi Biometrici su Dispositivi Portabili - 2/5



Arjun Kharpal @ArjunKharpal



Segui

Vkansee showed how to hack an iPhone fingerprint sensor using Play-Doh #MWC16

17:47 - 24 Feb 2016

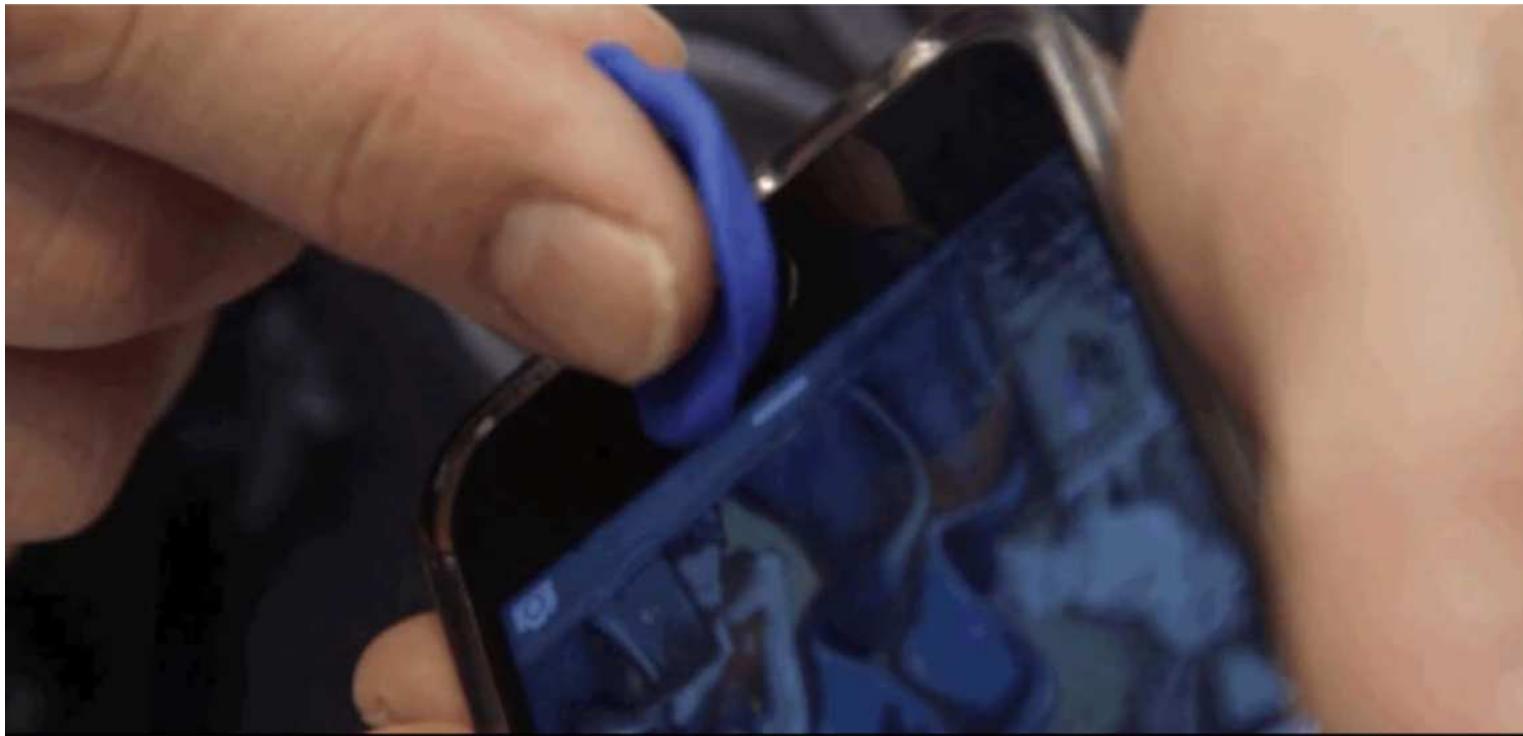


169



86

Possibili Criticità dei Sistemi Biometrici su Dispositivi Portabili - 3/5



Possibili Criticità dei Sistemi Biometrici su Dispositivi Portabili - 4/5

- I ricercatori della Michigan State University hanno trovato un modo per "ingannare" alcune tipologie di sensori di impronte digitali di cui sono dotati diversi smartphone
- L'attacco avviene usando della carta speciale (di tipo AgIC) e dell'inchiostro particolare (inchiostro conduttivo)
 - Il costo complessivo dell'attacco è di circa 500\$
- Link all'articolo:
 - http://www.cse.msu.edu/rgroups/biometrics/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf

Possibili Criticità dei Sistemi Biometrici su Dispositivi Portabili - 5/5



Fonte (Video su YouTube sul canale ufficiale della Michigan State University)
https://www.youtube.com/watch?v=fZJI_BrMZXU

Possibili Criticità dei Sistemi Biometrici su Dispositivi Portabili - 5/5



Fonte (Video su YouTube sul canale ufficiale della Michigan State University)
https://www.youtube.com/watch?v=fZJI_BrMZXU

Sommario

- Biometria e Sistemi Biometrici
 - Definizioni Preliminari
 - Cenni Storici
 - Caratteristiche di un Sistema Biometrico
 - Architettura di un Sistema Biometrico
- Principali Sistemi Biometrici
- Accuratezza delle Tecniche Biometriche
- Sistemi biometrici su dispositivi portabili
- Sistemi Biometrici Multimodali

Limitazioni dei Sistemi Biometrici a Singola Biometria (*Unimodali*) - 1/6

- I sistemi biometrici che utilizzano una singola biometria sono detti *sistemi biometrici unimodali*
- Tali sistemi possono avere delle limitazioni legate al fatto che viene utilizzata una singola biometria
- Una singola biometria, ad un certo punto, potrebbe non soddisfare una o più delle seguenti caratteristiche
 - Universalità
 - Unicità
 - Permanenza
 - Catturabilità

Limitazioni dei Sistemi Biometrici a Singola Biometria (*Unimodali*) - 2/6

➤ Esempio 1/3

Limiti sulla caratteristica di <u>Universalità</u>	
<i>Biometria</i>	Impronta digitale
<i>Possibile Limite</i>	Impronta non rilevabile a causa di mutilazioni o incidenti
<i>Biometria</i>	Voce
<i>Possibile Limite</i>	Impossibilità di rilevare la voce (mutismo)

Limitazioni dei Sistemi Biometrici a Singola Biometria (*Unimodali*) - 3/6

➤ Esempio 2/3

Limiti sulla caratteristica di <u>Permanenza</u>	
<i>Biometria</i>	Volto
<i>Possibile Limite</i>	Tratti del viso modellati dall'invecchiamento
<i>Biometria</i>	Voce
<i>Possibile Limite</i>	Cambio del timbro di voce o stato influenzale che altera il timbro vocale

Limitazioni dei Sistemi Biometrici a Singola Biometria (*Unimodali*) - 4/6

➤ Esempio 3/3

Limiti sulla caratteristica di <u>Unicità</u>	
<i>Biometria</i>	Volto
<i>Possibile Limite</i>	Tratti del viso estremamente simili (gemelli omozigoti)
<i>Biometria</i>	Voce
<i>Possibile Limite</i>	Possibile soggetti in grado di imitare la voce del soggetto in esame

Limitazioni dei Sistemi Biometrici a Singola Biometria (*Unimodali*) - 5/6

- Altre limitazioni dei sistemi biometrici unimodali possono derivare dagli strumenti di acquisizione della biometria
- Possono esservi errori durante il processo di acquisizione della biometria
 - Errata acquisizione dovuta a fattori esterni del sensore di acquisizione
 - Esempi
 - Polvere e/o sporcizia su sensore di acquisizione di impronte digitali
 - Forte sorgente di luce su sensore di acquisizione del volto
 - Etc

Limitazioni dei Sistemi Biometrici a Singola Biometria (*Unimodali*) - 6/6

Possibili Soluzioni

- Integrazione del sistema biometrico unimodale con tecniche di autenticazione tradizionali (non basate su biometrie)
 - Autenticazione mediante PIN, password, SmartCard, etc
- Progettazione di un sistema biometrico in grado di utilizzare più biometrie
 - Sistemi Biometrici Multimodali

Limitazioni dei Sistemi Biometrici a Singola Biometria (*Unimodali*) - 6/6

Possibili Soluzioni

- Integrazione del sistema biometrico unimodale con tecniche di autenticazione tradizionali (non basate su biometrie)
 - Autenticazione mediante PIN, password, SmartCard, etc
- Progettazione di un sistema biometrico in grado di utilizzare più biometrie
 - Sistemi Biometrici Multimodali

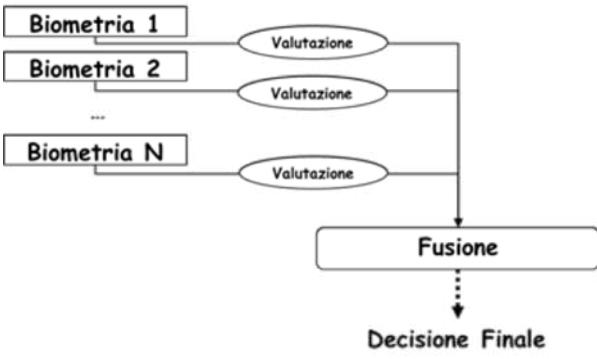
Architettura di un Sistema Biometrico Multimodale

- La fase di progettazione di un sistema biometrico multimodale deve tener conto di diversi aspetti
 - Requisiti funzionali
 - Quali biometrie utilizzare
 - Il livello architetturale dove effettuare la combinazione (*fusione*) delle biometrie
 - Deve essere definita la metodologia con la quale si effettua tale fusione

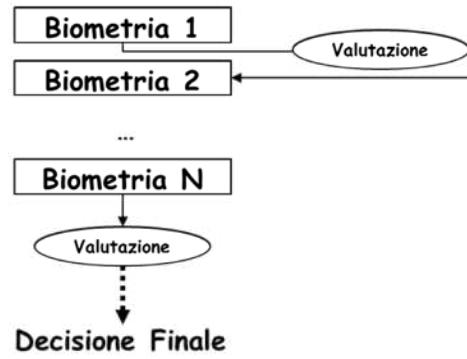
Architettura di un Sistema Biometrico Multimodale

Tre possibili scelte progettuali possono essere delineate per la definizione dell'architettura di un sistema biometrico multimodale

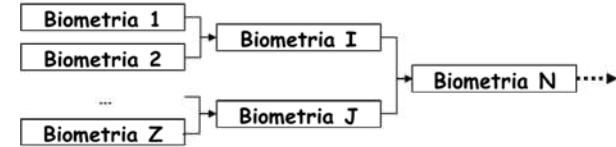
Progettazione in Parallello



Progettazione in Serie



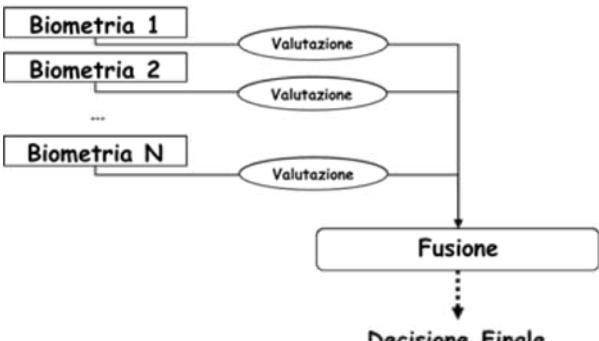
Progettazione a Livello Gerarchico



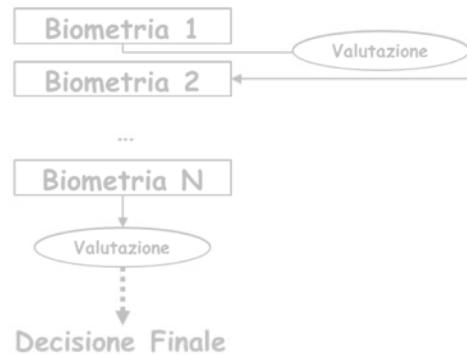
Architettura di un Sistema Biometrico Multimodale

Tre possibili scelte progettuali possono essere delineate per la definizione dell'architettura di un sistema biometrico multimodale

Progettazione in Parallello



Progettazione in Serie

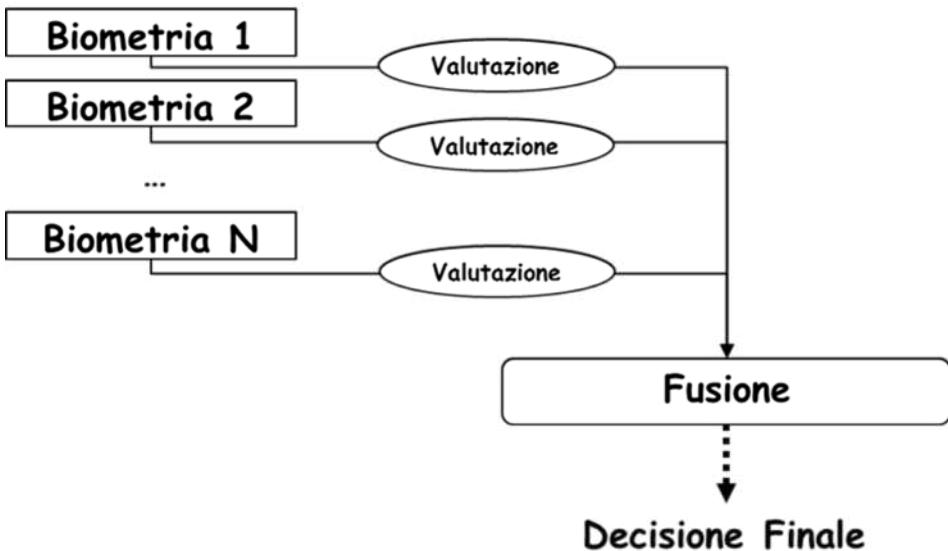


Progettazione a Livello Gerarchico



Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello



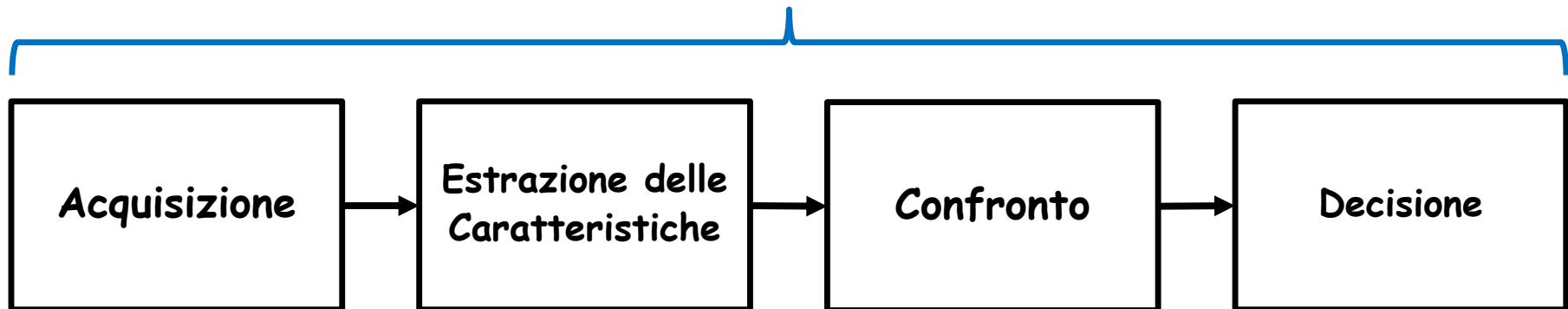
Caratteristiche

- L'acquisizione e la valutazione delle biometrie vengono svolte in maniera indipendente per ciascuna biometria
- Le valutazioni sono poi combinate mediante la *fusion*
- La fusione può avvenire a diversi livelli nell'architettura e secondo diverse strategie operative

Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Livelli e Strategia di Fusione

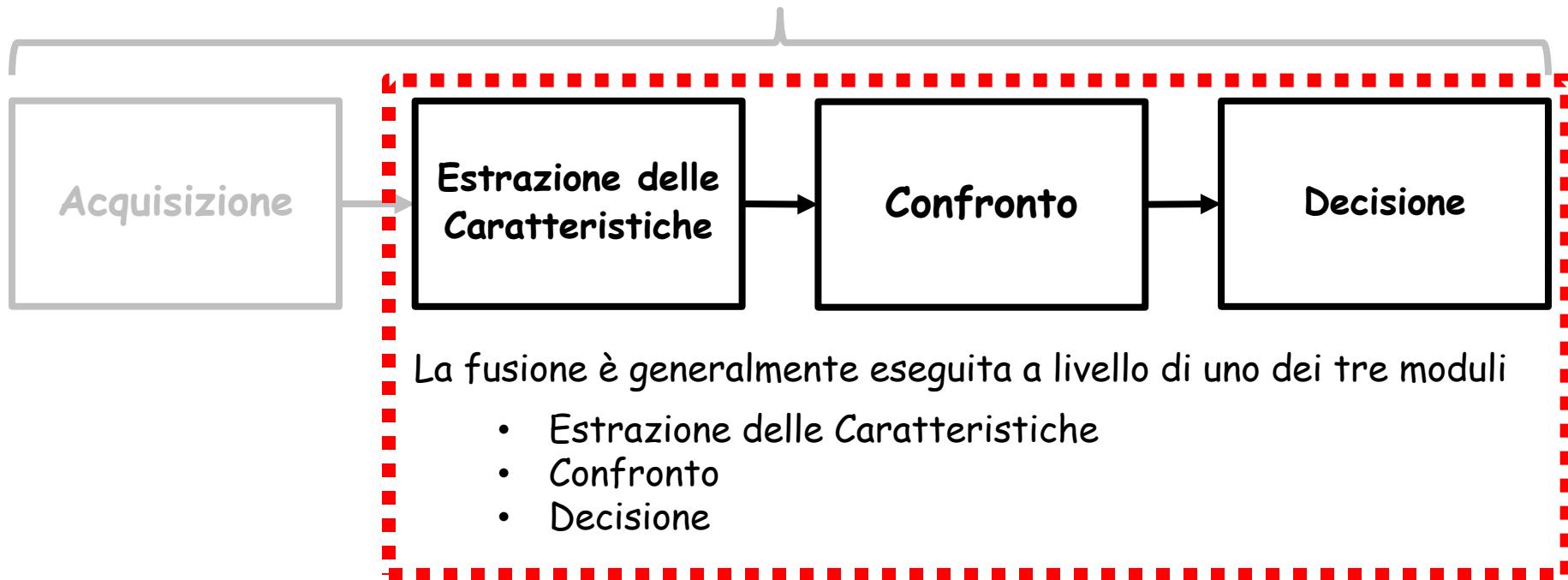
Moduli relativi alle fasi di *Verifica* e *Identificazione* in un sistema biometrico



Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Livelli e Strategia di Fusione

Moduli relativi alle fasi di *Verifica* e *Identificazione* in un sistema biometrico



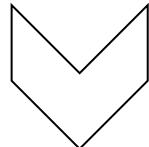
Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello

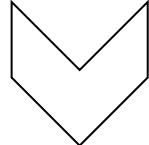
Fusione a Livello del Modulo di Estrazione delle Caratteristiche



Raccolta dei template ottenuti dalle caratteristiche estratte da ciascuna biometria



Fusione di tutte le informazioni dei template in un'unica entità logica



I moduli successivi (*Confronto e Decisione*) considereranno l'output prodotto da tale entità

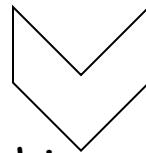
Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello

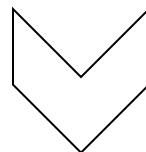
Fusione a Livello del Modulo di Controllo (o Matching)



Per ciascun template viene calcolato un *matching score*, comparando il template ottenuto dal modulo precedente (*Estrazione delle Caratteristiche*) con i template già memorizzati



Fusione dei valori relativi ai matching score, che restituisce in output un unico risultato



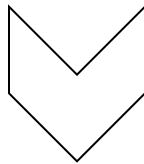
Il modulo successivo (Decisione) utilizzerà l'output prodotto dalla fusione

Architettura di un Sistema Biometrico Multimodale

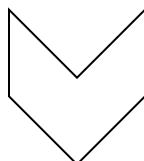
Progettazione in Parallello
Fusione a Livello del Modulo di Decisione



Esecuzione dei processi decisionali: un processo distinto per ciascuna biometria



Fusione dell'output dei processi decisionali



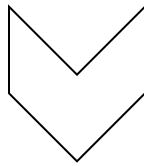
Calcolo della decisione finale

Architettura di un Sistema Biometrico Multimodale

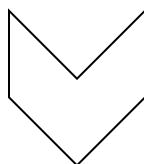
Progettazione in Parallello
Fusione a Livello del Modulo di Decisione



Esecuzione dei processi decisionali: un processo distinto per ciascuna biometria



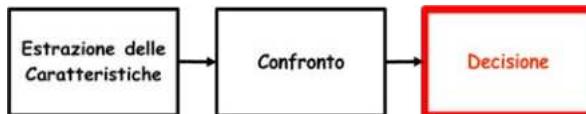
Fusione dell'output dei processi decisionali



Calcolo della decisione finale

Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Fusione a Livello del Modulo di Decisione

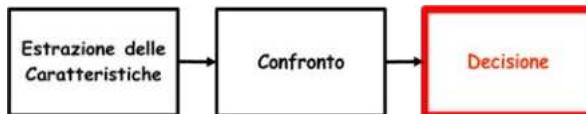


Possibili strategie per il calcolo della **decisione finale** - 1/2

- Strategia AND oppure Strategia OR
- Strategia di combinazione pesata

Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Fusione a Livello del Modulo di Decisione

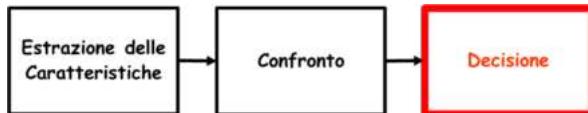


Possibili strategie per il calcolo della **decisione finale** - 1/2

- Strategia AND oppure Strategia OR
- Strategia di combinazione pesata

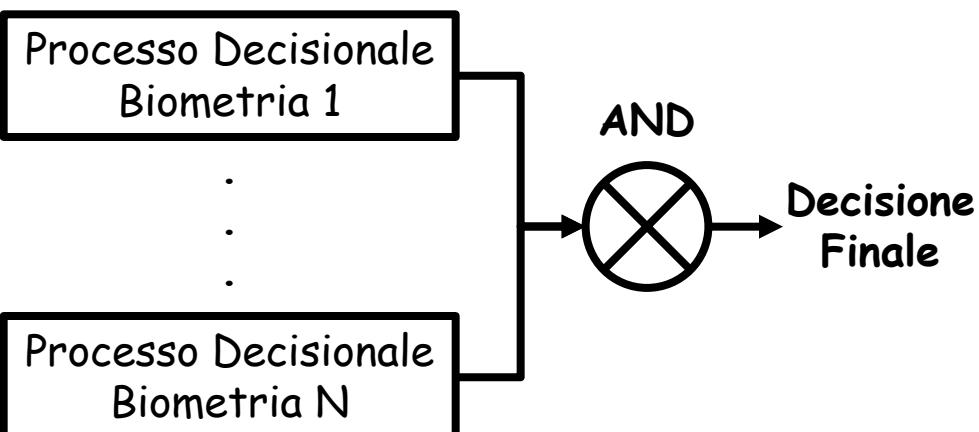
Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Fusione a Livello del Modulo di Decisione



Possibili strategie per il calcolo della **decisione finale** - 1/2

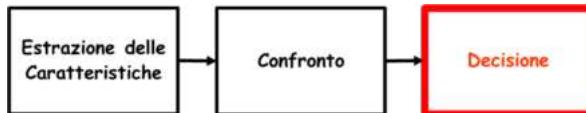
- Strategia AND oppure Strategia OR
- Strategia di combinazione pesata



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

Architettura di un Sistema Biometrico Multimodale

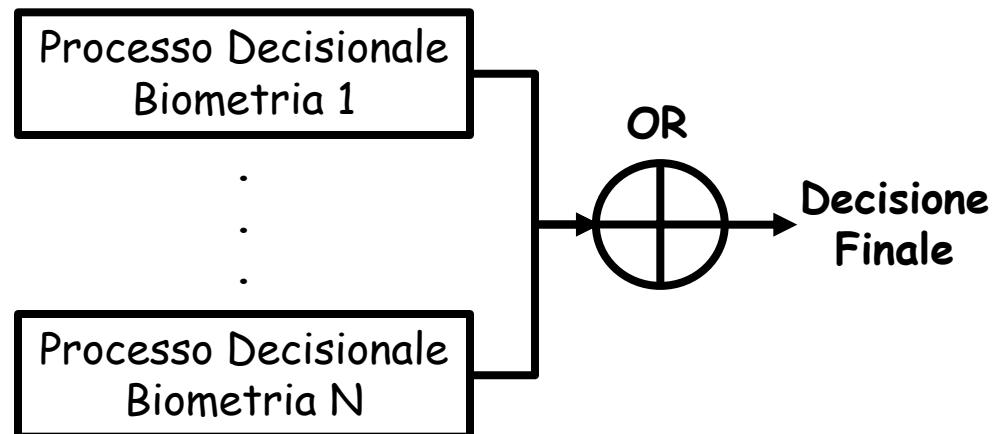
Progettazione in Parallello
Fusione a Livello del Modulo di Decisione



Possibili strategie per il calcolo della **decisione finale** - 1/2

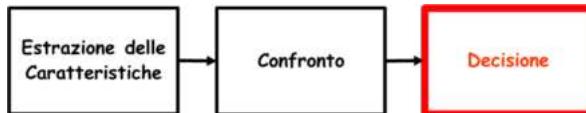
- Strategia AND oppure Strategia OR
- Strategia di combinazione pesata

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



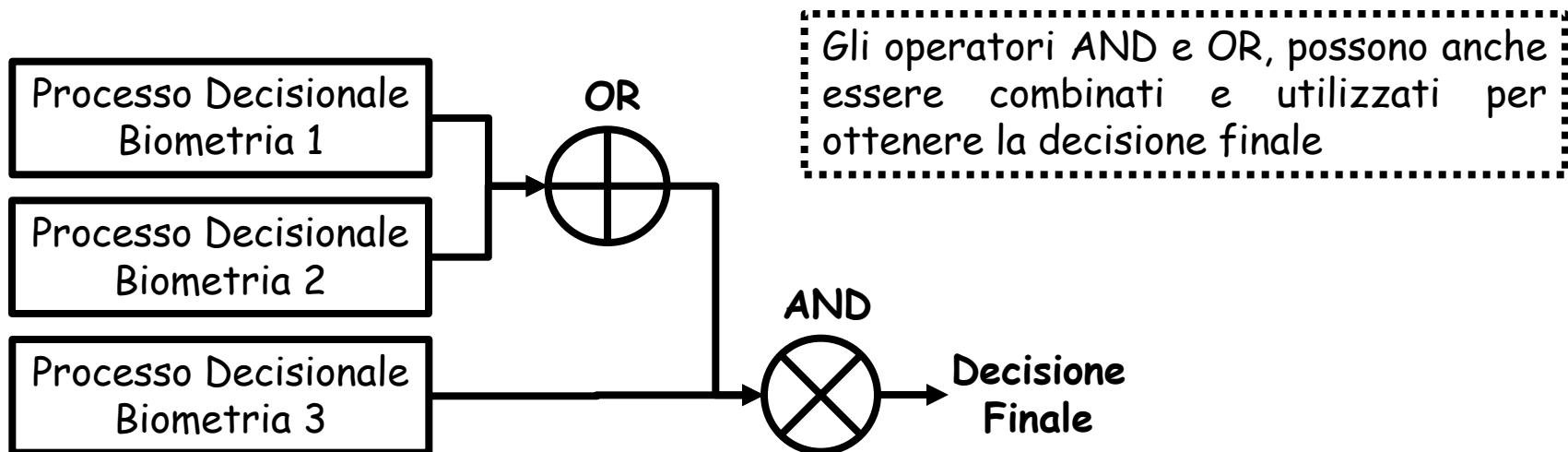
Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Fusione a Livello del Modulo di Decisione



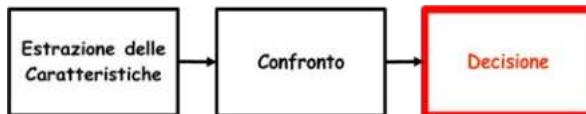
Possibili strategie per il calcolo della **decisione finale** - 1/2

- Strategia AND oppure Strategia OR → Strategia AND/OR
- Strategia di combinazione pesata



Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Fusione a Livello del Modulo di Decisione

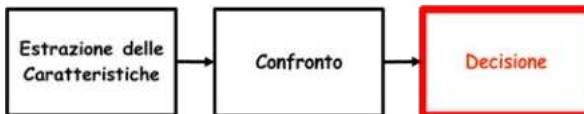


Possibili strategie per il calcolo della **decisione finale** - 1/2

- Strategia AND oppure Strategia OR
- Strategia di combinazione pesata

Architettura di un Sistema Biometrico Multimodale

Progettazione in Parallello
Fusione a Livello del Modulo di Decisione



Possibili strategie per il calcolo della **decisione finale** - 1/2

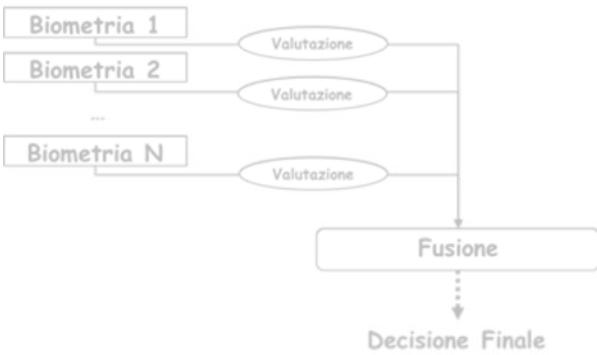
- Strategia AND oppure Strategia OR
- **Strategia di combinazione pesata**

- A ciascuna biometria viene associato un peso
- Ciascun processo decisionale restituisce un output, in accordo al peso assegnato alla biometria
- Viene effettuato il calcolo della *decisione finale*, sulla base degli output dei processi decisionali pesati

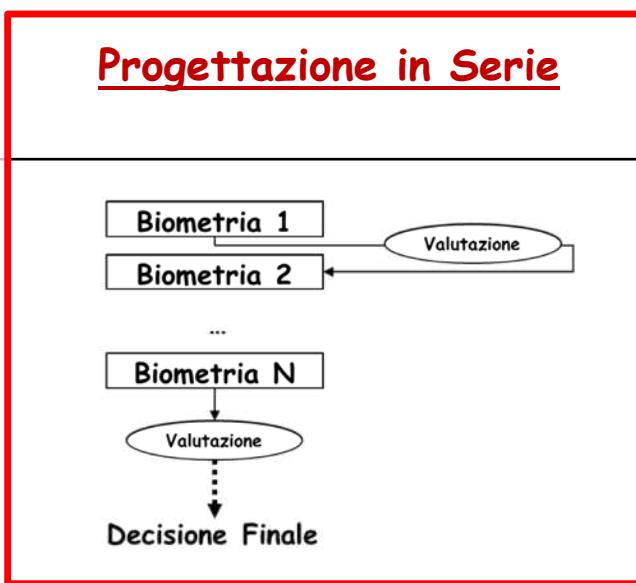
Architettura di un Sistema Biometrico Multimodale

Tre possibili scelte progettuali possono essere delineate per la definizione dell'architettura di un sistema biometrico multimodale

Progettazione in Parallello



Progettazione in Serie



Progettazione a Livello Gerarchico

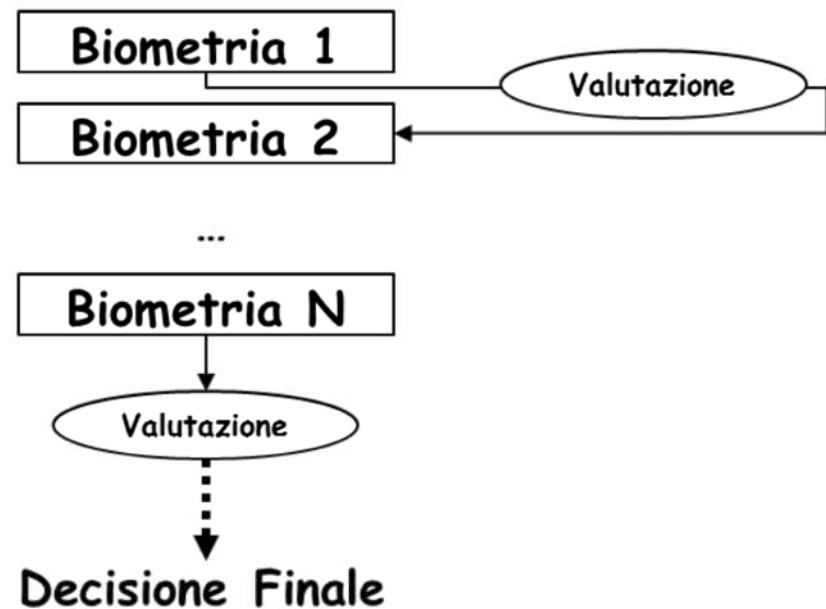


Architettura di un Sistema Biometrico Multimodale

Progettazione in Serie

Caratteristiche

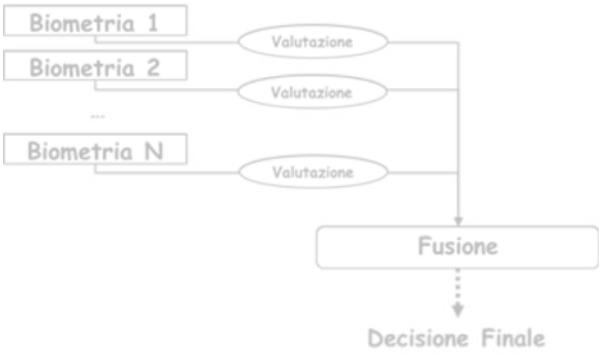
- L'acquisizione e la valutazione delle biometrie vengono svolte in maniera indipendentemente per ciascuna biometria
- Le valutazioni sono poi combinate mediante una delle possibili *tecniche di fusione*



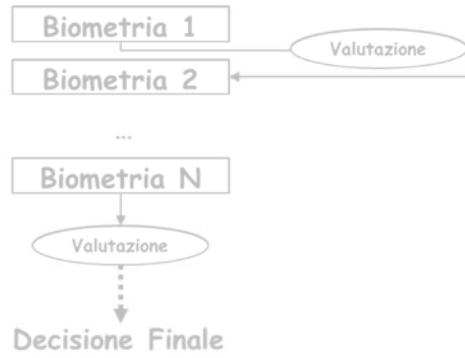
Architettura di un Sistema Biometrico Multimodale

Tre possibili scelte progettuali possono essere delineate per la definizione dell'architettura di un sistema biometrico multimodale

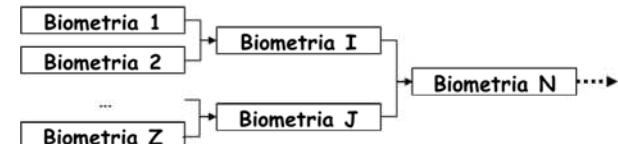
Progettazione in Parallello



Progettazione in Serie

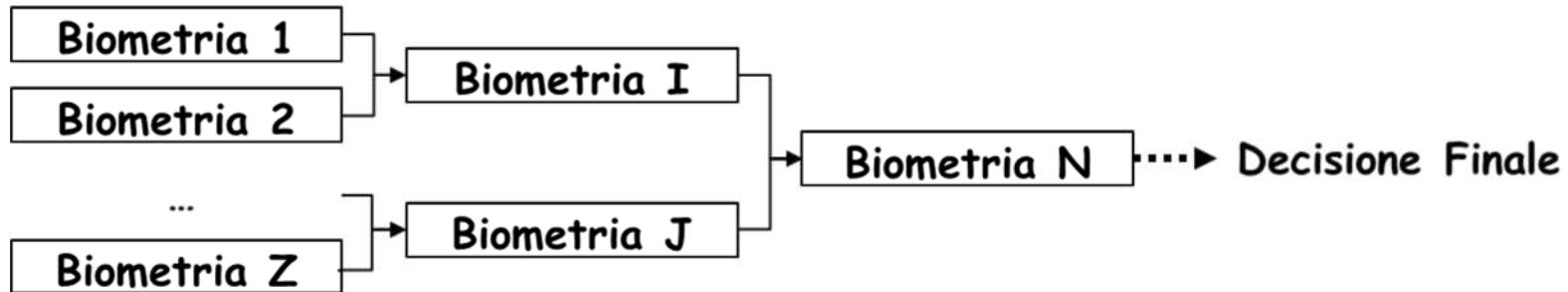


Progettazione a Livello Gerarchico



Le prossime slide sono nascoste per il riuso dei grafici

Progettazione in Serie

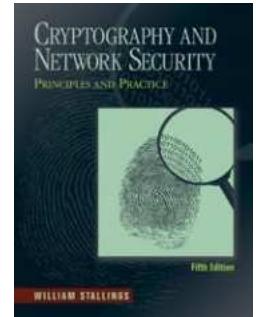


Caratteristiche

- Definizione di una gerarchia, mediante tecniche di classificazione individuali delle biometrie
- Memorizzazione delle valutazioni di ciascuna biometria in una struttura ad albero
- *Fusione* delle valutazioni, considerando le valutazioni nella struttura ad albero, per il calcolo della decisione finale

Bibliografia

- **Cryptography and Network Security**
by W. Stallings, 2010
 - cap. 18
- Tesina di Sicurezza su reti
 - Autenticazione utente + password
- *Biometrics.gov*. Aprile, 2016
<http://www.biometrics.gov/ReferenceRoom/Introduction.aspx>



Bibliografia

- Anil K. Jain, Arun Ross and Salil Prabhakar: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Techn. 14(1): 4-20, 2004
- Anil Jain, Patrick Flynn and Arun A. Ross: Handbook of biometrics. Springer Science & Business Media, 2007
- P. Jonathon Phillips, Alvin F. Martin, Charles L. Wilson, Mark A. Przybocki: An Introduction to Evaluating Biometric Systems. IEEE Computer 33(2): 56-63, 2000

Bibliografia

Sistemi Biometrici su dispositivi portabili

- Apple Touch ID e Face ID
 - <https://support.apple.com/it-it/HT208108>
 - <https://support.apple.com/it-it/HT204587>
- Android 6.0 (Marshmallow) API
 - <http://developer.android.com/about/versions/marshmallow/android-6.0.html>
- Windows Hello biometrics
 - [https://msdn.microsoft.com/it-it/library/windows/hardware/mt282187\(v=vs.85\).aspx](https://msdn.microsoft.com/it-it/library/windows/hardware/mt282187(v=vs.85).aspx)