

## Le tecniche biometriche di identificazione



▪ Svolto da Rosa Franzese

## Il sistema Bertillon

○ Bertillon (1853-1914) creò un nuovo sistema per identificare i criminali

- antropometria: lunghezza braccio e dita, altezza e larghezza testa, lunghezza piedi,...
- l'ossatura umana non si modifica più a partire dal ventesimo anno
- ogni scheletro è diverso



## Sistema Bertillon: strumenti

- ⇒ Caliper Compass
- ⇒ Sliding Compass
- ⇒ Small Sliding Compass
- ⇒ Vertical measure
- ⇒ Horizontal Measure



## Caliper Compass

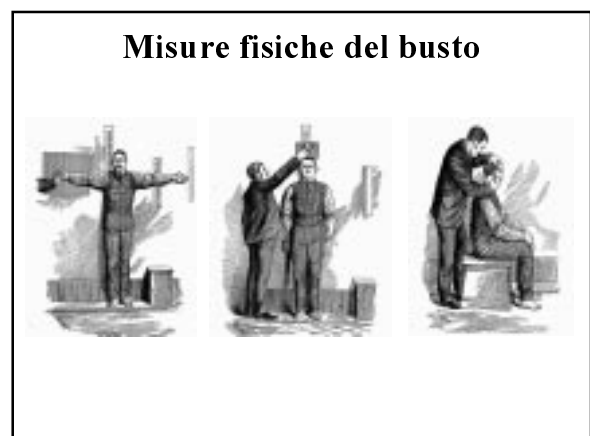
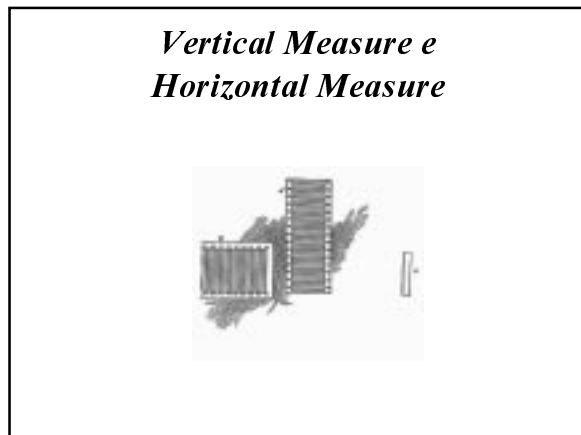


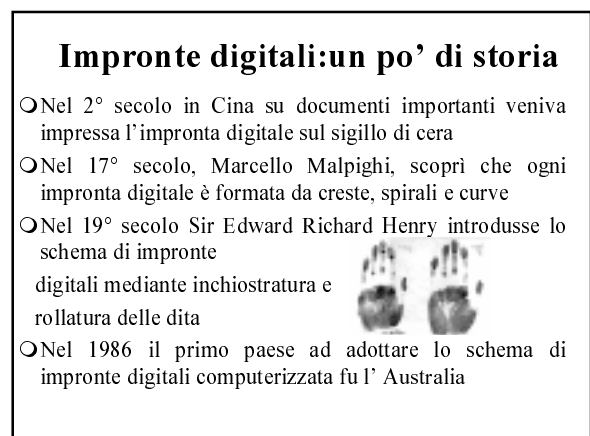
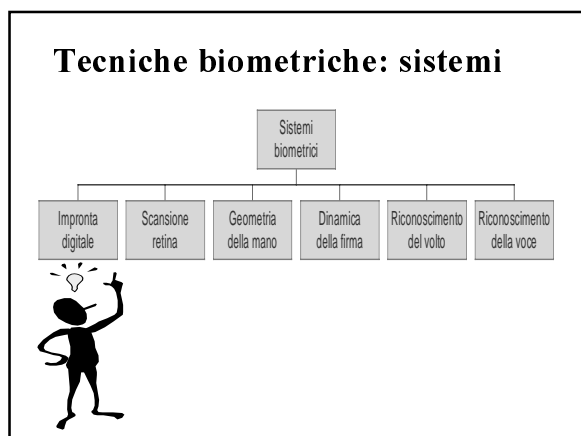
## Sliding Compass



## Small Sliding Compass







### Impronte digitali: caratteristiche

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



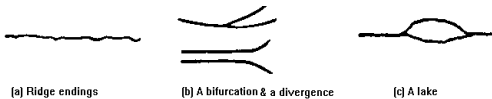
### Impronte digitali: anatomia

- Formate da insieme di linee dette creste (*ridge lines*)
- **Minuzie:** punti in cui le creste terminano o si biforcano
  - Furono introdotte da Francis Galton (1882-1916)
  - Classificazione



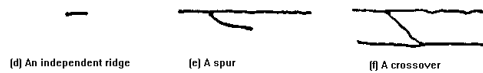
### Minuzie: classificazione

- **Ridge Ending:** è dove una cresta comincia e finisce improvvisamente
- **Bifurcation:** è dove una cresta è divisa o è inforcata in due o più creste parallele
- **Divergence:** è la crescita di due creste separate che corrono parallele
- **Lake:** è la congiunzione di due biforcazioni dove una forma il lato sinistro e l'altra forma il lato destro



### Minuzie: classificazione

- **Independent Ridge:** è una cresta piccola che è separata dalla cresta da ambo i lati
- **Spur:** è una combinazione di due creste indipendenti e una biforcazione
- **Crossover:** è una cresta indipendente che attraversa due creste parallele



### Impronta digitale: dettagli di Galton



### Impronta digitale

- In un impronta digitale vi sono 30, 40 minuzie
- Due individui possono avere in comune solo 8 minuzie



### Ridge lines: classificazione

○ **Arch:** è un modello di creste convesse con un picco nel medio



○ **Loop:** le creste verso il centro formano una curva a forma di U e dopo svoltano indietro senza torsione



○ **Whorl:** ha almeno due delta (il punto più vicino al centro di divergenza) e creste convesse, almeno una cresta fa un cerchio completo



### Impronte digitali: metodi di acquisizione

○ Metodo Ottico:

- tecniche
- problemi

○ Metodo *Capacitive*:

- tecniche
- vantaggi



### Metodo Ottico: tecniche

○ Il polpastrello viene appoggiato su un prisma di vetro, poi una fonte leggera di luce interna all'apparecchiatura viene proiettata sopra il polpastrello

○ Immagine è catturata da una apparecchiatura *charge-coupled (CCD)*



### Metodo Ottico: problemi

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



### Metodo *Capacitive*: tecniche

○ Rivela il campo elettrico dell'impronta digitale utilizzando un *sensor chip* e un *array di circuiti*



### Metodo *Capacitive*: vantaggi

- Più affidabile
- Più compatto
- Più costoso



## Impronta digitale

○ Il *template* viene memorizzato in un database e verrà utilizzato per confrontare l'impronta digitale del soggetto in tempi successivi e varia dai 100 bytes ai 1000 bytes



## Impronte digitali: dove?

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



## Impronta digitale: prodotti

### ○ EyeD Mouse II

- Verifica 1 minuto
- Metodo ottico
- Ciclo di utilizzo: 3.000.000 cicli
- Velocità di cattura 300mm/sec



## Impronte digitali: prodotti

### ○ EyeDKeyboard

- Verifica 1 minuto
- Metodo ottico
- Ciclo di utilizzo: 20 milioni di cicli



## Scansione della retina: un po' di storia

- Simon e Goldstein nel 1935 mostrarono che la forma delle vene nella retina sono uniche per ogni individuo
- Il primo sistema, **EyeDentify 7.5** è apparso nel 1985
- Dott. Jhon Daugman nel 1994 ha creato le formule matematiche che misurano le differenti caratteristiche della retina



## Scansione della retina: caratteristiche

- **Immutabilità:** configurazione e dettagli sono permanenti
- **Classificazione:** scia, contrazione, striatura, cavità, fibre collaginosi, filamenti, cripte (aree scure dell'iride), vascolature serpentine, anelli e lentiggini
- Ci sono 400 caratteristiche che possono essere quantificate e usate per identificare un individuo
- **Unicità:** non ci sono due iride simili, anche fra gemelli omozigoti



### Scansione della retina: metodi

○ **Attivo:** il sistema richiede che l'utente si muova avanti e indietro in modo che la macchina fotografica può acquistare e concentrarsi sull'iride dell'utente, il quale si può spostare dai 13 ai 39 cm dalla camera

○ **Passivo:** il sistema contiene una serie di macchine fotografiche che localizzano e si concentrano sull'iride dell'utente, il quale si può spostare dalle camere dai 30 cm ai 91 cm



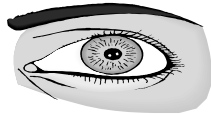
### Scansione della retina: procedimento

- L'utente sta in piedi di fronte al sistema di identificazione dell'iride e la macchina fotografica calcola la posizione dell'occhio
- La macchina fotografica effettua un secondo zoom e ne cattura un'immagine
- Il sistema ha l'iride in fuoco e pone l'immagine in una griglia circolare dove identifica le aree di luce e quelle oscure
- L'immagine catturata viene confrontata con il template memorizzato nel database
- Il tempo richiesto per identificare l'iride è approssimativamente 2 secondi



### Scansione retina

- Scansione dell'occhio con raggi infrarossi
- La luce infrarossa è riflessa indietro ad una video camera
- **template** in sistemi commerciali di 35 byte



### Retina: vantaggi

- Possiede un alto grado di casualità
- Interna all'occhio quindi estremamente protetta
- Visibile esternamente
- Stabile per tutta la vita



### Retina: svantaggi

- Oscurata da ciglia, lenti, riflessioni
- Obiettivo piccolo
- Non visibile se non illuminata
- Localizzata dietro una superficie curva e riflettente



### Scansione retina: dove?

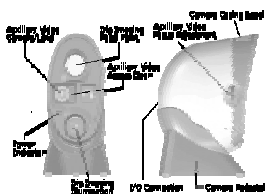
- Citibank
- Banche inglesi
- Central Intelligence Agency (CIA)
- Federal Bureau Investigation (FBI)



### Scansione retina: prodotti

○Secure Cam C2

- Tempo di cattura <2 sec
- Tempo di verifica <10sec
- Tempo di elaborazione <20 sec
- Distanza di acquisizione 15-20cm



### Geometria della mano: un po' di storia

- È considerato il nonno di tutti i sistemi biometrici
- 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

- Misura le caratteristiche fisiche della mano
  - lunghezza dita
  - larghezza mano
  - spessore dita



### Geometria della mano: procedimento

- Misure fisiche: acquisizione
  - meccanico
  - scoperta *image-edge*
- Template viene costruito in base alle misure della mano
- Le misure fisiche della mano sono catturate da un apparecchiatura *charge-coupled (CCD)* e la sagoma della mano viene memorizzata tridimensionalmente



### Geometria della mano

- Le apparecchiature della geometria della mano non prendono in considerazione i dettagli della superficie della mano come linnee, cicatrici, unghie e immondizia





### Gemetria 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



### Geometria della mano: prodotti

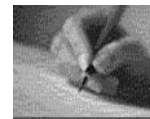
#### ○ Hand Key II

- Tempo di verifica: 1 secondo
- Memoria: 5 anni
- Template 9 bytes
- Capacità utente: 512 utenti standard



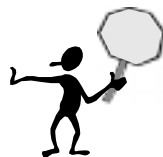
### Dinamica della firma

- **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
- **Semplice confronto della firma**
  - facile da falsificare
- Per maggiore sicurezza cambiare ogni volta la frase da scrivere



### Dinamica della firma: problema

- Cercare di ridurre la differenza tra le parti delle firme che sono abituali e costanti e quelle che vengono alterate in base allo stato d'animo



### Dinamica della firma: dove?

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



### Riconoscimento del volto: metodi

- Scoperta: il volto umano è catturato dall'obiettivo della macchina fotografica e viene isolato dagli oggetti catturati con esso, poi il software pone l'immagine in un frame rettangolare chiamato *binary mask*
- Riconoscimento: il volto viene confrontato con gli altri volti memorizzati in un database
- *Thermal imaging*: mediante una macchina fotografica a raggi infrarossi vengono catturate i vasi sanguigni del volto
  - può essere anche usato in oscurità completa

### Riconoscimento del volto: dove?

- Agenzie dei veicoli statali (DMU)
- Reparto immigrazione e naturalizzazione (SENTRI) in Mexico



### Riconoscimento della voce

- Texas Instruments nel 1960 creò il primo prodotto

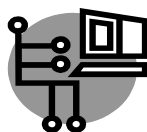


### Riconoscimento della voce: tecnologia

- *Speaker dependent*: il sistema viene addestrato a riconoscere un dato utente e contiene un vocabolario tra 30.000 e 120.000 parole
- *Speaker independent*: il sistema non viene addestrato e può essere utilizzato da chiunque. Contiene un vocabolario più piccolo
- *Discrete speech input*: l'utente che parla deve effettuare piccole pause
- *Continuous speech input*: l'utente può parlare continuamente ma il sistema riconosce solo un numero limitato di parole e frasi
- *Natural speech input*: l'utente parla liberamente e il sistema esegue al volo i comandi

### Riconoscimento della voce

- **Template** viene costruito pronunciando ripetutamente una frase fissa
- **Parametri**: tono, dinamica, *waveform*



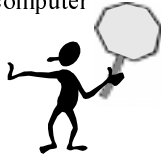
### Riconoscimento della voce: vantaggi

- Affidabilità
- Flessibilità
- Tecnologia biometrica naturale
- Occhi e mani sono liberi per l'operazione



### Riconoscimento della voce: svantaggi

- Training lungo
- L'efficienza dipende dal rumore
- La voce cambia con il tempo e le malattie
- Computazione complicata (trasformata di Fourier)
- A molti non piace parlare a un computer
- Attacchi di replay
  - Cambiare ogni volta la frase da leggere



### Riconoscimento della voce: dove?

- General motors
- L'ospedale di Chicago
- Charles Schwab e Company



### Altre tecniche biometriche

- Segno delle labbra
- Segno della pianta del piede
- Forma delle vene nella mano e nel polso
- Salinità del corpo
- Cattivo odore
- Risposta dello scheletro ad uno stimolo fisico



### Tecniche biometriche: definizione

○ Sistemi che utilizzano le caratteristiche fisiologiche o comportamentali di un individuo

*Fisiologica:* caratteristica fisica e stabile

- impronta digitale, scansione della retina, geometria della mano, riconoscimento del volto

*Comportamentale:* caratteristica influenzata dalla personalità dell'individuo

- riconoscimento della voce, della firma e battitura della tastiera e del mouse



### Le caratteristiche fisiologiche e comportamentali

- **Universalità:** ogni persona possiede le caratteristiche
- **Unicità:** due persone non hanno le stesse caratteristiche
- **Permanenza:** le caratteristiche non variano nel tempo
- **Collectability:** le caratteristiche possono essere misurate quantitativamente
- **Esecuzione:** il raggiungimento preciso dell'identificazione
- **Accettabilità:** il grado con cui le persone sono disposte ad accettare un sistema biometrico
- **Insidia:** il grado di facilità di ingannare il sistema

### Esempio sulle caratteristiche

	universalità	unicità	permanenza	collectability	esecuzione	accettabilità	insidia
Impronta	media	alto	alto	medio	alto	medio	alto
Retina	alto	alto	medio	basso	alto	basso	alto
Volto	alto	basso	medio	alto	basso	alto	basso
Mano	medio	medio	medio	alto	medio	medio	medio
Firma	basso	basso	basso	alto	basso	alto	basso
Voce	medio	basso	basso	medio	basso	alto	basso

### Sistemi biometrici: identificazione

- **Identificazione positiva:** verificare che l'individuo che si presenta al sistema sia l'autorizzato mediante un confronto tra quest'ultimo e un template memorizzato nel sistema
- **Identificazione negativa:** verificare che l'individuo che si presenta al sistema non sia l'autorizzato



### Sistemi biometrici: classificazione

- Cooperativo/non cooperativo
- Evidente/velato
- Abituato/non abituato
- Frequentato/non frequentato
- Ambiente standard
- Pubblico/privato
- Aperto/chiuso

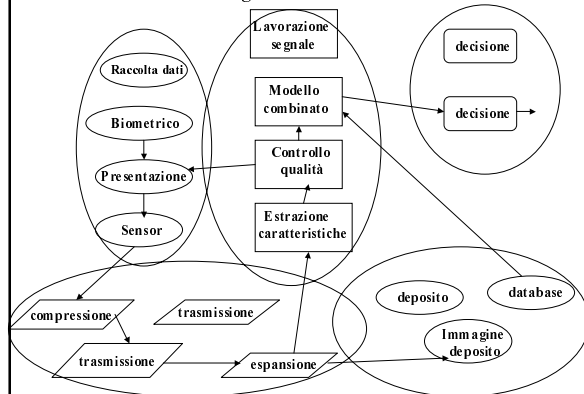


### Esempio della classificazione

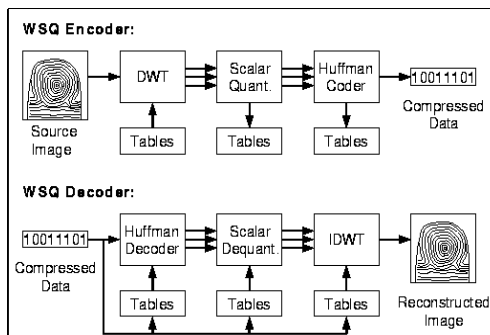
- Sistema biometrico utilizzato per prevenire l'emissione di licenze multiple per le auto
  - **non-cooperativo:** non identifica quelle persone che hanno già una licenza
  - **evidente:** dare una misura biometrica come condizione di ottenere la licenza
  - **frequentato e ambiente standard:** la raccolta delle caratteristiche biometriche avviene alla cassa della motorizzazione
  - **non abituato:** le licenze vengono rilasciate ogni 4 o 5 anni
  - **pubblico:** usato dai clienti della motorizzazione
  - **chiuso:** non scambiano informazioni



### Sistema biometrico: generico

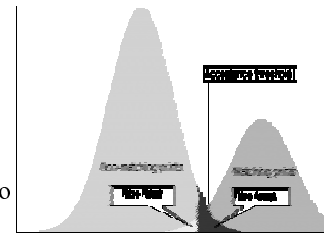


### Esempio di compressione dell'impronta digitale



### Accuratezza dei sistemi biometrici

- **Rifiuto falso:** un sistema biometrico non identifica individuo onesto
  - FRR indica la probabilità di tale evento
- **Accettazione falsa:** un sistema biometrico identifica un individuo disonesto
  - FAR indica la probabilità di tale caso



## Tecniche biometriche: conclusioni

- Studio Sandia National Labs, su sistemi commerciali

tecnica	errore	caratteristica	migliore	peggiore
voce	2%	accettabilità	mano	voce
firma	2%	falso rigetto	mano	impronta
retina	0.40%	falsa accettazione	mano, retina, impronta	voce
mano	0.110%	throughput	mano, retina, impronta	voce, firma
impronta	9% falso rigetto	difficoltà di imitazione	retina	voce, firma
	nessuna falsa accettazione	orrendezza 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