

# Sistemi biometrici, concetti fondamentali

## Sommario

Introduzione alla biometria	12
Autenticazione biometrica e tecniche tradizionali	12
Definizione di Biometria	12
Riconoscimento	12
Autenticazione e Identificazione	12
Metodi classici di Autentificazione	12
Biometrics and Biometry	12
Le 7 proprietà del tratto biometrico	12
Aspetto e funzionamento dei sistemi biometrici	13
Applicazioni	13
Acquisizione e Riconoscimento	13
Tratti biometrici: caratteristiche fondamentali	13
Impronta digitale	13
Volto	13
Mano	14
Iride	14
Firma	14
Voce	14
Sistemi multimodali	14
Soft biometrics	14
Evoluzione della biometria	15
Impronte digitali nell'antichità	15
Sistema Bertillon (1882)	15
Esordi delle impronte digitali	15
Mondo, 1960-2000	15
Comparazione dei sistemi biometrici Privacy e regolamento GDPR	16
Problema della comparazione	16
Autenticazione/Identificazione	16
Variazioni del tratto	16
Campioni indipendenti	16
Velocità del sistema	16
Interoperabilità	16
Impiego di un sistema biometrico: aspetti di privacy	16

Percezione degli utenti	16
L'anello debole della catena	17
Sample o template	17
Proscrizione	17
Decalogo del garante sulla biometria (2006)	17
GDPR: General Data Protection Regulation	18
Dato Biometrico	18
Conseguenze per l'Italia	18
Obblighi del gestore dei dati	18
Pseudonimizzazione (art. 4.5)	18
Resilienza	18
Sistema biometrico: elementi caratteristici	18
Struttura di un sistema biometrico	18
Fasi di un sistema biometrico	18
Sistemi biometrici multimodali	19
Sistemi biometrici distribuiti	19
Match biometrici on card	19
Match on sensor	19
Tratto biometrico: aspetti analitici	20
Variabilità temporale del tratto	20
Variabilità intraclasse	20
Similitudine interclasse	20
<b>Fasi da analizzare</b>	20
Acquisizione	20
Template, estrazione di caratteristica e matching	21
Rappresentazione	21
Matching	21
Ricerca ed organizzazione dei DB biometrici	21
Scalabilità	21
Organizzazione del DB	21
Tasso di penetrazione	21
Binning	22
<b>Calcolo del numero di bin ottimale</b>	22
Binning error	22
Introduzione alla misura dei parametri	22
Genuini ed impostori	22

<b>Problema di identificazione</b>	23
Distanza fra i template	23
Genuini ed impostori	23
False Match e False Non-Match	23
<b>FM Rate, FNM Rate</b>	23
<b>Decision Error Tradeoff (DET) e Receiver Operating Characteristic (ROC)</b>	24
Regioni di funzionamento	24
Equal Error Rate	24
Metodi statistici per la stima dei parametri di un sistema biometrico	24
Modello utilizzato: Processo di Bernoulli	24
<b>Regola dei 3</b>	25
Da verification a Identification, errori	25
<b>La regola dei 30</b>	25
Sistemi biometrici basati su impronte digitali	25
Impronte digitali: excursus storico e introduzione	25
Introduzione storica	25
Primi sistemi di classificazione	26
Cosa sono le impronte digitali	26
Sistema di classificazione attuale	26
Alcune applicazioni basate sulle impronte	26
Sistemi AFIS	26
Punti di forza e debolezze	26
I tre livelli di analisi delle impronte	27
Tre livelli di analisi	27
Livello I	27
Livello II	27
Livello III	27
Ed i gemelli?	27
Come procede un esperto (umano)	27
Il Sistema AFIS italiano	27
La legge italiana	28
Tecnologie sul mercato	28
Future trends negli AFIS	28
Impronte digitali e sensori: caratteristiche	28
Tipologie di sensori e caratteristiche	28
Problemi di acquisizione	29

Sistemi commerciali	29
Rappresentazione, compressione e non unicità	30
Rappresentazioni delle impronte	30
Immagini delle impronte	30
Formati di compressione	30
Unicità delle impronte (al secondo livello)	30
Algoritmi per le impronte digitali	30
Algoritmi di prefiltraggio ed enhancement	30
Filtraggi iniziali	30
Segmentazione	31
Manipolazione immagine (enhancement)	31
Estrazione di caratteristica (estrazione delle feature)	32
Tipi di caratteristiche da estrarre	32
Livello I	32
Livello II	34
Thinning	35
Come identificare la minuzia	35
Metodi di post processing	35
Livello III	35
"Spoofing e anti-spoofing"	35
Fake finger	35
Test di vitalità per sensori ottici	36
Test di vitalità per sensori allo stato solido	36
Generazione sintetica di impronte	36
Sistemi biometrici basati sull'iride	36
Caratteristiche dell'iride e sensori	36
Panoramica della applicazione	36
Unicità dell'iride	36
Quale luce per acquisire l'iride?	36
Quale sensore per acquisire l'iride?	36
Rappresentazione delle iridi	37
Struttura dei moduli secondo Dougman	37
Dalla immagine iride al template	37
<b>La sequenza dei passi principali</b>	37
Calcolo dei centri e raggi di iride e pupilla	37
Rimozione di palpebre e ciglia	37

Linearizzazione dell'iride	37
Calcolo dell'iris code	38
Proprietà dell'iris code	38
Algoritmi di enhancement e prefiltraggio	38
Quality checker	38
Feature Extraction Module	39
Algoritmi di matching (Matching module)	39
<b>Distribuzione dei bit in un singolo Iriscode</b>	39
Come sono legati i bit in un singolo iriscode	39
Alcuni fattori che aumentano la variabilità intraclasse	40
Algoritmi di matching per gli Iriscode	40
Velocità del matching di Iriscode	40
Rotazioni dell'Iriscode	40
Algoritmi matching e prestazioni	40
Tassi di errore del sistema	40
Svantaggi della tecnica	41
Quanti bit significativi nell'Iriscode?	41
Progettazione della soglia?	41
Perché le distribuzioni reali non sono simmetriche?	41
Come sono le distribuzioni di occhi geneticamente uguali?	41
Iride nel visibile e spoofing/antispoofing	41
Iride nel visibile	41
Watch list	41
Problemi di privacy	42
Frodi attuabili sul sistema	42
Attacchi al sensore	42
Possibili controlli	42
Generazione sintetica di iridi	42
Sistemi basati sul volto	43
Introduzione alla biometria del volto	43
Sistemi biometrici basati sul volto	43
Vantaggi	43
Svantaggi	43
Non solo identification/verification	43
Fasi principali	43
Similitudine interclasse per il volto	43

Standard per il template	44
Compressione per le immagini facciali	44
Passive biometric identification	44
Algoritmi di prefiltraggio ed estrazione di caratteristica	44
Sensori per i volti 2D	44
Face detection	44
Approcci alla face detection	45
Face detection – color based	45
Face detection – Haar feature	45
Face tracking	45
Estrazione di caratteristica e matching	46
Estrazione di features	46
Metriche per il matching	46
Analisi lineare di un sottospazio delle facce	46
Analisi lineare di un sottospazio mediante PCA	46
La PCA è molto utile!	46
Vantaggi e svantaggi della PCA	46
Significato degli autovalori nella PCA	47
Significato delle Autofacce	47
Considerazioni sulle autofacce	47
Altri metodi di estrazione delle feature e matching	47
Graph matching	47
Spoofing e anti-spoofing	48
Alcuni limiti oggettivi e tipi di attacchi	48
Un esempio di attacco: <b>Hill Climbing</b>	48
Contromisure (non efficaci) alla tecnica Hill Climbing	48
Controllo della sincronia parlato – movimenti labbra	48
Facial fingerprinting (Infrared identification)	48
Attacco con immagini	49
Near Infrared Antispoofing	49
Sistemi basati sul volto 3D	49
Sensori e caratteristiche del tratto in 3D	49
Acquisizione 3D mediante scanner laser	49
Acquisizione 3D mediante luce strutturata	49
Acquisizione 3D mediante diverse viste	49
Vantaggi e svantaggi dei sistemi 3D	50

Confronto sensori 2D e 3D	50
Algoritmi di matching 3D - Accuratezza sistemi 2D e 3D	50
Confronto fra 2 template 3D	50
Face Recognition Vendor Test	50
Esempio di sistemi commerciali (con sensore 3D)	50
Confronto con umani	50
Critiche verso il Face Recognition (FR)	50
Spoofing e anti-spoofing per il volto 3D	51
Controllo del volto 3D usando un sistema 2D	51
Tipi di attacchi di spoofing	51
Tecniche di antispoofing	51
Biometria a contatto	52
Mano e palmo	52
Introduzione	52
Applicazioni	52
Vantaggi e svantaggi	52
Sensori	52
Pegs or Pegs-free	52
Alcuni tipi delle circa 90 features estraibili	53
Passi per il matching	53
Eigenfingers	53
Standard e accuratezza dei sistemi	53
Firma, Retina, Voce	53
Biometria della firma	53
Riconoscimento della firma	53
Firma online	54
Firma offline	54
Pro e contro	54
Applicazioni	54
Biometria della retina	54
Riconoscimento della retina	54
Acquisizione ed estrazione di caratteristiche	55
Pro e contro	55
Retica	55
Biometria della VOCE	55
Voice Recognition	55

Sistemi basati sul riconoscimento vocale	55
Speaker Rec.: Acquisizione della voce	56
Caratteristiche generali della voce	56
Estrazione e confronto delle caratteristiche	56
Speaker Rec.: Pro e contro	56
Signal Requirements	57
Speaker Rec.: Feature Extraction	57
Speech Recognition Performance	57
Speaker Identification	57
Esempio di curva DET per la voce	58
Effetto dei secondi di enrollment sulla curva DET per la voce	58
<b>DNA Orecchio Autovalutazione</b>	58
DNA - Uso nella biometria	58
Introduzione alla biometria del DNA	58
Vantaggi e svantaggi del DNA	59
Cosa è il DNA?	59
Gene	59
Replicazione del DNA	59
Che feature si estraggono dal DNA	60
Satelliti e STR	60
Allele	60
Quali dati mettiamo nel template	60
Passi principali	60
Principio base	60
Lettura del gel tramite laser	60
Genotipizzazione	61
Valori estratti	61
Omozigoti e identificazione	61
<b>Orecchio (Altri sistemi monomodali)</b>	61
Vantaggi e svantaggi	61
Stato dell'arte	61
Diversità del tratto fra gli individui separazione <b>interclasse</b>	62
Ear localization and normalization	62
Feature extraction (ear template)	62
<b>Biometria della digitazione della tastiera e schermi</b>	62
Keystroke dynamics	62

Behavioural biometrics	62
Comportamento dell'utente sul terminale	62
<b>Keystroke dynamics biometrics → Two factors authentication</b>	62
Estrazione delle feature	63
Feature globali	63
Punti di forza	63
<b>Attacco su canale SSH</b>	63
Impronta e palmo unconstrained (o almeno less-constrained)	64
Unconstrained and less-constrained biometrics	64
Touchless fingerprints	64
Contactless fingerprint: Advantages	64
Contactless fingerprint: Cons & Challenges	64
PALM e PALM PRINT (Contact e Contact-less 2D e 3D)	64
Palmpoint recognition	64
Features	64
Touchless vs touch-based	65
Contactless 2D Palmpoint	65
Contactless palmpoint: VANTAGGI	65
Contactless palmpoint: SVANTAGGI	65
Methods	65
Palm in Near infrared (Palm Vein)	65
3D Palm acquisition (Using 2 cameras)	65
Palmpoint recognition: 3D (vs 2D)	65
Progettazione, valutazione e confronto di sistemi biometrici	66
Documento «Best Practices ...»	66
Struttura del documento	66
Diverse valutazioni	66
Technology Evaluations	66
Scenario Evaluations	67
Operational Evaluations	67
Online evaluation	67
Offline Evaluation	67
Intervallo di confidenza dei parametri	67
Progettazione, valutazione e confronto di sistemi biometrici	68
Comparazione sistemi biometrici	68
Comparazione dei sistemi	68

ROC = 1 – DET	68
Riassunto sulla comparazione di DET	68
Accuratezza in identificazione: Cumulative Match characteristic (CMC)	68
Legame fra distribuzioni DET e CMC	68
Distribuzioni: d'	69
Indici aggiuntivi: Security, Convenience	69
Security and Convenience	69
Regione di sicurezza	70
Regione di convenienza	70
Standard ISO per la biometria	70
ISO/IEC 19794	70
Chi sono gli «Standard body»	70
Standard BioAPI	70
Progettazione di un sistema monomodale	71
Problema della progettazione	71
8 domande per scegliere il tratto	71
Tabelle comparative	72
Maturità, dimensioni, costo,....	72
Fattori di progetto VS Tratti ordinati	72
Che livelli di accuratezza sono da impostare?	73
Piattaforme e Biometrics as a Service	73
Biometria in cloud	73
Biometric Services Platform	73
Biometrics as a Service (BaaS)	73
BaaS – Pro e Contro	73
Sistemi multimodali	73
Sistemi multibiometrici e multimodali: Metodi avanzati di fusione	73
Svantaggi dei sistemi monomodali	73
Sistemi multimodali	74
I sistemi multimodali sono più accurati	74
Vantaggi e svantaggi dei sistemi multimodali	74
Cosa si può unire? (Multibiometrico)	74
Quali tratti unire?	74
Terminologia usata in letteratura	74
Tecniche di datafusion biometrica	75
Schemi classici	75

Fusione a livelli diversi	75
Metodi di fusione del match score	75
Normalizzazione degli score	76
Funzioni di normalizzazione	76
Integrazione di sistemi commericali	76
Tecniche avanzate di datafusion per sistemi multimodali	76
Sistemi multimodali gerarchici	76
Fusione a livello di feature	77
Parametrizzazione specifica per il singolo utente	77
Modalità di integrazione della soft biometrics	77
Esempi di sistemi multimodali	78
Sistemi multimodali per il volto	78
Sistema BioID	78
Sistema Iride+Retina	78

# Introduzione alla biometria

## Autenticazione biometrica e tecniche tradizionali

### Definizione di Biometria

Insieme di tecniche automatiche per il riconoscimento degli individui basato sulle loro caratteristiche fisiche e comportamentali.

### Riconoscimento

Il riconoscimento può essere suddiviso in due categorie:

- Verifica dell'identità (*Autenticazione*) = Sono chi dico di essere?
  - Confermare o negare l'identità dichiarata dall'utente
  - Metodi one-to-one (1:1)
- Ricerca dell'identità (*Identificazione*) = Chi sono io?
  - Metodi one-to-many (1:N)
  - Da un insieme di identità note (*problema di identificazione chiuso*)
  - In altre situazioni (*problema di identificazione aperto*)

### Autenticazione e Identificazione

#### Autenticazione/Identificazione POSITIVA

Quando si cerca di stabilire con elevata accuratezza che l'utente sia chi dice di essere.

#### Autenticazione/Identificazione NEGATIVA

Quando si cerca di stabilire con elevata accuratezza se l'utente non è chi dice di essere.

### Metodi classici di Autentificazione

- **Possesso** (qualche cosa che possiedi), di solito chiamate anche **Token-based**
- **Conoscenza** di una porzione di informazione (qualche cosa che sai)

### Biometrics and Biometry

#### BIOMETRICS

Metodi di identificazione (automatica) basati sulle caratteristiche fisiche e comportamentali dell'individuo.

#### BIOMETRY

Campo di studio molto più ampio che comprende l'applicazione della statistica alla biologia e alla medicina.

### Le 7 proprietà del tratto biometrico

- **Universalità**
  - Ogni persona deve possedere questo tratto/caratteristica
- **Unicità**
  - Due persone non devono avere lo stesso tratto uguale
- **Permanenza**
  - La caratteristica deve essere invariante nel tempo
- **Misurabilità**
  - Il tratto deve poter essere esaminato quantitativamente
- **Performabilità**

- Accuratezza della identificazione che deve essere adeguata e deve poter essere garantita senza particolari condizioni operative
- **Accettabilità**
  - Percentuale di persone che potrebbero accettare l'uso del sistema biometrico
- **Circonvenzione**
  - Grado di difficoltà nell'ingannare il sistema con tecniche fraudolente

## Aspetto e funzionamento dei sistemi biometrici

### Applicazioni

- Applicazioni forensi
- Governative
- Commerciali

### Acquisizione e Riconoscimento

#### Enrollment - Fase di Acquisizione

- Il tratto biometrico viene per la prima volta acquisito dal sistema e registrato oppure viene creato il documento biometrico
- Tratto (trait) - ACQUISITION -> Campione (sample) - FEATURE EXTRACTION -> Caratteristiche (features) - CODING -> Template - DATABASE

#### Identificazione/Verifica - Fase di Riconoscimento

- Il tratto biometrico viene nuovamente acquisito. Se risulta sufficientemente aderente alle informazioni registrate nel sistema biometrico l'accesso è consentito
- Trait - ACQUISITION, FEATURE EXTRACTION, CODING -> Template - MATCHING (with the DB stored template) -> Matching score - IS OVER THE THRESHOLD PERCENTAGE -> Yes or No

## Tratti biometrici: caratteristiche fondamentali

### Impronta digitale

- Tratto biometrico più antico e diffuso al mondo, è un pattern di creste e valli che è già presente nell'embrione. Non cambia nel tempo e si ritiene siano uniche.
- **Riconoscimento** avviene attraverso **tre approcci**
  - **Correlation-based** (Pixel by pixel)
  - **Ridge feature-based** (Solo i ridge)
  - **Minutia-based** (Ridge ending, biforcation, valley, ridge memorizzati come insieme di coordinate)

### Volto

- Tratto biometrico tra i meno intrusivi, molto usato da applicazione e dalle persone per riconoscersi
- Difficoltà nel creare sistemi che affrontino le seguenti problematiche:
  - Invecchiamento del volto
  - Variazioni degli sfondi e delle luci di una scena
  - Espressioni del volto
  - Variazioni della posa
- **Riconoscimento** avviene attraverso **due approcci**:
  - **Trasformazione**
    - Si crea una "base di immagini" che permette di ricostruire un nuovo viso come una somma di immagini contenute nella base
  - **Attributi**

- Si localizza il volto nell'immagine e si misurano delle caratteristiche come la distanza fra gli occhi, la lunghezza del naso, della bocca, ecc.

## **Mano**

- Tratto biometrico molto ben accettato dagli utenti perché poco invasivo. Offre un discreto livello di sicurezza. Può funzionare in modo multimodale controllando più aspetti
- Si applicano **diversi algoritmi**
  - Rilevamento dei contorni
  - Allineamento per fare i confronti
  - **Analisi immagine termica per controllo "liveness" e misura vene**
- **Riconoscimento** avviene attraverso **diversi approcci**
  - **Misura delle lunghezze**
  - **Confronto delle immagini delle parti** (ritagliate e confrontate immagini **per dita, palmo**)
  - **Studio delle linee**

## **Iride**

- Considerato come il tratto biometrico più accurato. Poco gradito da utenti per "percepita" invasività. Presenta **caratteristiche numerose e stabili dall'ottavo mese di vita**. Complesso e costoso ma difficile da frodare.
- Il sistema possiede **algoritmi per:**
  - **Trovare l'occhio** nel viso
  - **Scattare e confrontare più frame** per verificare se l'iride è "viva"
  - **Selezionare la parte utile**
  - **Eliminare i riflessi e le ciglia**
  - **Compensare le deformazioni dell'iride** che si comporta elasticamente con le variazioni di luce
- **Riconoscimento**
  - Pupilla
  - Iride
  - Ciglia e riflessi
  - **Linearizzazione iride**
  - **Creazione dell'IRIS CODE**

## **Firma**

- Metodo molto diffuso e semplice. **Bassa accuratezza**. Moderato costo del sensore. **Firma statica e dinamica**
- **Riconoscimento basato sugli andamenti nel tempo:**
  - delle coordinate x,y
  - della pressione
  - dell'azimut
  - dell'inclinazione

## **Voce**

- Tratto biometrico accettato dagli utenti. Bassa accuratezza e moderato costo. **Template di grandi dimensioni**. Piuttosto facile da frodare.

## **Sistemi multimodali**

- **Uniscono più tecnologie biometriche** in un sistema, con l'obiettivo di aumentare l'accuratezza o la robustezza alle frodi

## Soft biometrics

Alcuni tratti biometrici **non posseggono le 7 caratteristiche** necessarie ma **possono essere usati in aggiunta** (es: genere, colore della pelle, degli occhi, peso, altezza...)

## Evoluzione della biometria

### Impronte digitali nell'antichità

- Usate da **Assiri (2500 AC)** per firmare documenti legali.
- Usate per **riconoscimento di criminali nel regno di Hamurabi (1792-50 AC)** (riconoscimento)
  - Usate anche da autori di incisioni cuneiformi su argilla per evitare contraffazioni (autenticazione)
- Usate già in **Cina nel 300 AC per firmare documenti legali** e registrare i criminali tramite sigilli in argilla
- Durante la **dinastia Jin (220-420 DC)** venne invece usata la **seta e l'inchiostro per firmare con le impronte i documenti**

### Sistema Bertillon (1882)

- Creò un sistema per identificare i criminali basato su misure antropometriche
- Le **ipotesi di Bertillon** sono:
  - **Lo scheletro umano non si modifica dal 20 anno di età**
  - **Ogni scheletro è diverso**, quindi dai dati si può risalire ad una identità
- Funzionamento
  - **Enrollment:** ogni persona veniva **registrata attraverso una scheda con fotografia**
  - **Matching: ricerche effettuate manualmente**
- Fattori che portarono al fallimento
  - **Troppe categorie usate per dividere le schede rallentavano le ricerche** (246) fino a parecchie ore per archivi di 50000 schede
  - **La non accuratezza delle misure dei criminali adolescenti** che poi crescevano
  - **L'arrivo delle impronte digitali negli USA (1880-1900)**
  - **Il caso WEST (1903)**
    - **Will West viene imprigionato e schedato ma le sue misure e foto corrispondono ad una scheda già presente in archivio, suo fratello William West** (incarcerato nel 1901)
    - **Cade l'unicità del metodo Bertillon**

### Esordi delle impronte digitali

- Nel 1880 Sir Francis Galton inizia i suoi studi sulle impronte e **scopre che tutte le impronte possono esser classificate in 4 classi** (ancora oggi fondamentale negli archivi)
  - **A delta**
  - **Monodelta**
  - **Bidelta**
  - **Composta**
- Nel 1900 Sir Edward Henry, un ispettore della Polizia Indiana, pubblica un libro per classificare le impronte. Il suo metodo diventa standard in UK fino all'avvento dell'elaboratore elettronico
- A partire dal 1900 tutto il mondo gradualmente inizia a usare le impronte digitali
  - Nel 1903 il New York State Prison Department inizia a schedare i detenuti
  - In UK nel **1901** Sir Edward Henry fonda il **Fingerprint Bureau (Scotland Yard)**
  - Nel **1946** l'**FBI ha 46 milioni di set di impronte**
  - Nel **1963** in UK iniziano ad usare i computer ma con confronti manuali
  - Nel **1971** l'**FBI arriva a 200 milioni di set ed inizia ad usare il sistema computerizzato AFIS**
  - Nel **1999** l'**FBI abbandona la carta per le impronte**, tutto il sistema è digitale (scan, store, match...)

## Mondo, 1960-2000

- Ad oggi in tutto il mondo sono registrati **dati biometrici di centinaia di milioni di individui**
- In 4 decenni si è passati da un metodo (impronte) a sistemi automatici per circa 10 diversi tratti biometrici. Esempi: Geometria della mano (1985), iride (1994), vene della mano (1998)

## Comparazione dei sistemi biometrici Privacy e regolamento GDPR

### Problema della comparazione

- È un problema molto complesso, molti parametri di giudizio e difficilmente stimabili
  - Gradimento degli utenti
  - Accuratezza
  - Scalabilità
  - Interoperabilità
  - Costo del sistema
  - Usabilità
  - Velocità

### Autenticazione/Identificazione

- Ad oggi solo **iride** e **impronta** sono usati per **Identificazione (1:N) con N grandi**.
- Requisiti per il funzionamento 1:N
  - **Accuratezze elevatissime** (tasso errore << 1E-5)
  - **Template in byte ridotti** (Dimensione < kB )
  - **Tempo** per un singolo confronto **molto basso** ( $T < ms$ )
- Per questo motivo **mano, volto, voce e firma** vengono usati solo per
  - **autenticazione (1:1)**
  - **identificazione 1:N con N solo di qualche decina** di persone (es. per i dipendenti di una banca)

### Variazioni del tratto

L'alta variabilità del tratto biometrico nel tempo produce una **peggiore accuratezza** del sistema biometrico

### Campioni indipendenti

Maggiore è il numero di sample indipendenti (dello stesso tratto) che possiamo usare nello stesso sistema biometrico, maggiore è l'accuratezza rispetto ad usare un sample

### Velocità del sistema

- **Tempo di riferimento: "il tempo (in sec) per eseguire un singolo matching"**
- Da questo tempo si arriva a stimare il numero di utenti massimo identificabile/autenticabili in un'ora
- I sistemi possono funzionare
  - **in Tempo reale**
    - la velocità è cruciale
    - Esempio: Gate Aeroportuale
  - **Off-line**
    - la velocità è importante ma non cruciale
    - Esempio: ricerca delle impronte di un criminale in un archivio

### Interoperabilità

la capacità di un sistema biometrico di funzionare anche con sample biometrici acquisiti con sensori di diverso tipo usando lo stesso tratto biometrico

## Impiego di un sistema biometrico: aspetti di privacy

### Percezione degli utenti

- Vantaggi
  - “Non devo avere chiavi o ricordare codici” VERO
  - “Sarà più difficile clonare o rubarmi i soldi con il mio bancomat” PARZIALMENTE VERO
  - “Funzionerà contro il terrorismo” PARZIALMENTE VERO
- Svantaggi
  - “Le mie impronte saranno schedate come fanno per i criminali” PARZIALMENTE VERO
  - “Sapranno dove vado e dove sono stato” GIA’ OGGI VERO
  - “Sapranno che cosa compro” GIA’ OGGI VERO

### L'anello debole della catena

L'anello debole della catena di identificazione rimane anche se usiamo le tecnologie biometriche: **il problema è la fonte!**

Un documento biometrico nasce da altri **documenti tradizionali**.

### Sample o template

- SAMPLE
  - PRO: può essere nuovamente
    - Filtrato
    - Analizzato
    - Permette cambi tecnologici
  - CONS:
    - Occupa più spazio
    - Dato utile per attacchi con fake
    - Allunga la “vita” del tratto biometrico
    - Lede la privacy
- TEMPLATE
  - PRO:
    - Minore elaborazione in verifica
    - Minore occupazione memoria e banda in trasmissione
    - Protegge “meglio” la privacy
  - CONS:
    - Legato alla tecnologia che lo ha generato
    - Difficilmente migliorabile

## Proscrizione

Quando un dato biometrico è inviato ad un dato sistema, l'informazione contenuta non dovrebbe essere usata per altri scopi se non quello dell'uso richiesto dell'utente

## Decalogo del garante sulla biometria (2006)

1. Affidabilità del sistema
2. Informativa chiara (con libertà di aderire, e tecniche alternative a biometria)
3. Liceità (perché usare proprio i dati biometrici?)
4. Deroga motivata
5. Delimitata memorizzazione (non centralizzazione)
6. Temporanea conservazione
7. Scrupolose misure di sicurezza
8. Piena ed immediata conoscibilità dei dati biometrici da parte dell'interessato
9. Rispetto rigoroso delle norme e obblighi di verifica preliminare e notifica del Garante
10. Disattivazione automatica, immediata e certa di funzioni di smart card o altre analoghe in caso di smarrimento o furto

## GDPR: General Data Protection Regulation

### Dato Biometrico

- Definisce i DATI BIOMETRICI come una **CATEGORIA SPECIALE DI DATI PERSONALI** e **proibisce** la loro **elaborazione e memorizzazione presso terze parti** senza il consenso.
- “dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloskopici”
- La loro elaborazione allo scopo di “**identificare in modo univoco una persona fisica**” è **proibita**.

### Conseguenze per l'Italia

- Il dato biometrico diventa un dato sensibile a tutti gli effetti
- Cambia completamente l'approccio alla materia della sicurezza informatica.
- Data breach comunicato in 72 ore (20M €)

### Obblighi del gestore dei dati

- Il titolare/responsabile del trattamento deve **valutare il rischio informatico**:
  - rischi impliciti nella tecnologia (di natura **endogena**)
  - rischi **esogeni** derivanti dall'automazione di processi operativi aziendali
- Predisporre **specifiche misure per limitare tali rischi**, quali la **cifratura** e tenere conto dello **stato dell'arte** e costi di attuazione rispetto ai rischi.

### Pseudonimizzazione (art. 4.5)

- Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive
  1. **l'assenza di identificabilità diretta** del soggetto interessato
  2. **l'adozione di misure di sicurezza ulteriori** da aggiungere alla pseudonimizzazione (fra le quali la **cifratura**)
  3. l'incorporazione della **pseudonimizzazione nella privacy-by-design**

### Resilienza

La capacità di un sistema di adattarsi alle condizioni d'uso in modo da garantire la disponibilità dei servizi erogati per un lasso di tempo adeguato (**continuità operativa in caso di guasti o attacchi**)

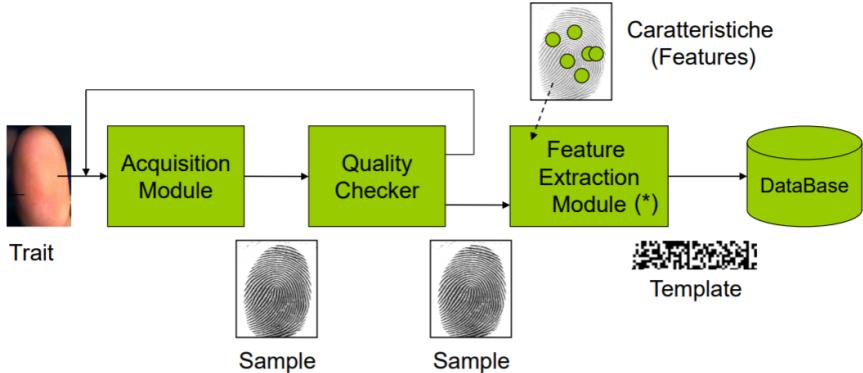
# Sistema biometrico: elementi caratteristici

## Struttura di un sistema biometrico

### Fasi di un sistema biometrico

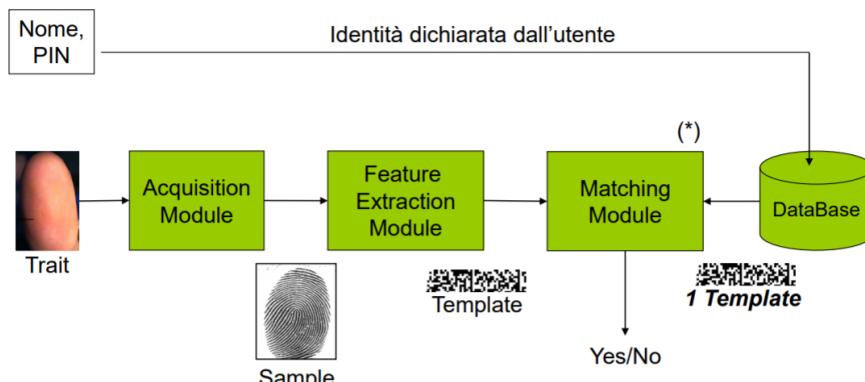
- Enrollment

#### Enrollment: (template) → DB



- Verification

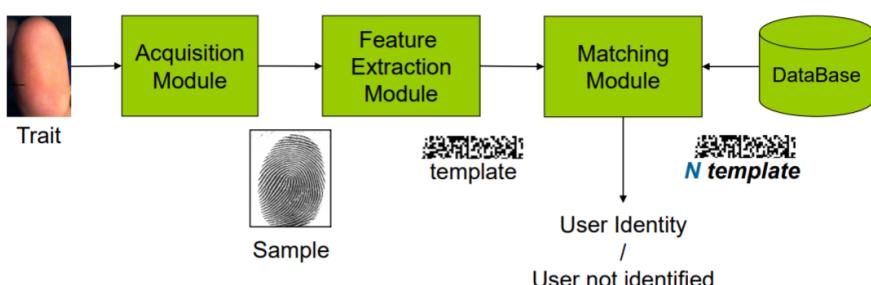
#### Verification usando un DB



(\*) In questi schemi consideriamo come facenti parte del modulo di Matching l'algoritmo di decisione (solitamente un confronto con una soglia fissa).

- Identification

#### Identification



- Enrollment e verification sono molto simili anche per i documenti biometrici, la differenza è che non vengono presi dati da un DB ma vengono letti dal documento biometrico

## Sistemi biometrici multimodali

“Multimodal biometric systems are those which utilize, or are capable of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification”

## Sistemi biometrici distribuiti

- Il termine “distribuito” si riferisce ad un sistema biometrico quando i moduli componenti sono separati e collegati in rete
  - Piuttosto raro quando si tratta di sistemi di autenticazione
  - E’ comune quando si tratta di sistemi di identificazione di grosse dimensioni
  - Solitamente è il modulo dei DB dei template che viene ad essere dislocato rispetto ai terminali

## Match biometrici on card

Il termine on card si riferisce al fatto che il template biometrico risiede su una smart card, la quale non effettua il matching e non possiede un sensore di acquisizione

## Match on sensor

Arrivano sul mercato nuovi sensori con molte funzionalità utili per lo sviluppo del sistema

## Tratto biometrico: aspetti analitici

### Variabilità temporale del tratto

Come un tratto varia all’interno dello stesso soggetto con il passare del tempo.

### Variabilità intraclassesse

- Si intende la **variazione del sample o delle feature dello stesso individuo** tra acquisizioni effettuate in istanti di tempo diversi
  - Effetti casuali (rumore del dispositivo)
  - Variazioni dello sfondo
  - Variazioni tratto (invecchiamento, posizione, espressione, usura)
  - Parziali occlusioni

### Similitudine interclasse

Particolare vicinanza dei sample o delle feature acquisiti da **individui diversi** (Es.: gemelli, sosia)

### Fasi da analizzare

- Acquisizione del tratto
  - Sensori e dati ambientali
  - Controllo della qualità dell’acquisizione
- Rappresentazione
  - del sample
  - estrazione delle caratteristiche
  - del template
- Matching
- Ricerca, organizzazione e scalabilità del DB

### Acquisizione

- Il processo di acquisizione si suddivide in 2 fasi:
  - **Valutazione della qualità:** controllo automatico sulla correttezza dei dati in ingresso coerentemente alle successive elaborazioni
  - **Segmentazione:** separazione dei dati in ingresso nell’**oggetto di interesse** (foreground) e nello **sfondo/informazione non rilevante** (background)

### *Controllo della qualità*

- Dopo l'acquisizione molti sistemi attuano un controllo automatico della qualità del tratto rilevato per evitare problemi di funzionamento molto importanti
- I sistemi di controllo della qualità producono un indice di qualità del sample acquisito.
  - Se indice è basso viene acquisito un altro sample, altrimenti se è sufficientemente alto si procede

### *Signal/image enhancement*

- In alcuni casi **non è possibile rifiutare un sample** perché il suo indice di qualità è basso. In questo caso il sistema cerca di **estrarre le informazioni (foreground) dal rumore (background)** in modo tale da far funzionare il resto della catena di moduli del sistema
  - Questa fase si chiama signal/image enhancement
  - Solitamente è ad elevata complessità computazionale
  - **Può generare i cosiddetti “artefatti” (artefacts)**

### *Metodi di segmentazione*

La regione di interesse nell'immagine acquisita viene selezionata nella fase di segmentazione ( con metodi diversi per applicazione, es. volto o impronta)

### *Template, estrazione di caratteristica e matching*

#### **Rappresentazione**

- Il problema della rappresentazione della informazione in un sistema biometrico consiste nello stabilire quale rappresentazione “machine-readable” catturi completamente l'informazione invariante e discriminatoria della misura in ingresso
- La rappresentazione deve fornire:
  - **Alta variabilità interclasse**
  - **Bassa variabilità intraclasse**
- L'affidabilità della rappresentazione dipende dal
  - tratto biometrico
  - dominio applicativo del sistema

#### *Effetto del dominio applicativo*

- la **rappresentazione** diventa **meno affidabile**
  - **all'aumentare degli individui** da confrontare fra loro nello spazio delle caratteristiche (e quindi nel DB)
  - **in caso di sensori rumorosi, soggetti non allenati o collaborativi**, ecc

#### *Rappresentazione del sample*

- Si riferisce alle caratteristiche tecniche del processo di acquisizione e memorizzazione (anche temporanea) del sample
- Varia con il tipo di tratto biometrico

#### *Estrazione di caratteristiche*

Avendo i dati raw provenienti dalle misurazioni (sample) occorre ora estrarne la rappresentazione nello spazio delle caratteristiche, fino a creare diversi tipi di template

#### **Matching**

- Il modulo di matching implementa una metrica nello spazio delle feature
- Possono essere inclusi moduli software addizionali migliorativi, ad esempio per:
  - prendere provvedimenti per evitare che l'utente deformi l'impronta durante la scansione

- inserire nell'algoritmo di matching anche un modello elastico di deformazione, che aumenta la similitudine intraclasse ma tende a diminuire la distanza interclasse

## Ricerca ed organizzazione dei DB biometrici

### Scalabilità

- I sistemi che devono gestire una grande quantità di identità dovrebbero essere in grado di operare efficacemente quando il numero di utenti registrati nel DB aumenta
- Il tasso di peggioramento delle prestazioni sia minore del tasso di nuovi utenti immesso

### Organizzazione del DB

Un DB organizzato permette di non confrontare un template in ingresso con tutti i template nel DB ma solo con quelli contenuti in una partizione

### Tasso di penetrazione

- “the expected proportion of the templates to be searched over all input samples under the rule that the search proceeds through the entire partition regardless of whether a match is found”
- Attualmente i sistemi di grandi dimensioni funzionanti su 2 impronte riescono a funzionare correttamente con dei Penetration Rate del 10%

### Binning

- Per giovare delle partizioni del DB occorre disporre di un algoritmo automatico molto robusto per la classificazione dei template
- Quando il DB viene creato, i template vengono disposti nelle partizioni (bins)

### Calcolo del numero di bin ottimale

- Se ho  $N_{\text{impronte}}$  distinguibili (indice, medio..) tutte divisibili in  $N_{\text{tipi}}$  (arch, whorl, ...) allora il numero migliore di bin è  $\mathbf{N\_bin = N\_tipo^Nimpronte}$

### Binning error

- Quando un individuo presenta i propri tratti biometrici al sistema e l'algoritmo di classificazione del tratto sbaglia il bin
  1. Se l'individuo era registrato nel DB, con alta probabilità non si avrà un match in quanto i template che “matchano” sono registrati in un bin diverso da quello scandito
- Attenzione: **avere  $N$  bin non porta ad avere un Penetration Rate del  $100/N!$**  Questo accade perché i bin **non contengono necessariamente un numero di individui uguali**
- Test in letteratura dimostrano come si possa arrivare ad un **errore del 5-10% in un DB di medie dimensioni** attuando la **classificazione di Henry** con un sistema automatico (**5 classi**)
- Test sul NIST 4 fingerprint database (4000 impronte 8-bit gray scale) **4 classi**: errore = **3-8%**
- **Attenzione: gli errori si moltiplicano se si usano  $N$  impronte!**
- **abbassando il numero di classi**
  1. **P.R. sale** → si abbassa la qualità del P.R. ottenibile (**non buono**)
  2. **si abbassa l'errore di classificazione (buono)**

## Introduzione alla misura dei parametri

### Genuini ed impostori

- **Genuino** per indicare un individuo che accede al sistema e ha titolo per farlo
- **Impostore** per chi prova ad accedere senza averne titolo

Problema della verifica

- Dato in ingresso (query) un insieme di caratteristiche  $X_Q$  e la dichiarata identità  $I$  occorre determinare se  $(I, X_Q)$  appartengono a  $\omega_1$  o  $\omega_2$ , dove
  - $\omega_1$  indica che la richiesta è vera (utente genuino)
  - $\omega_2$  indica che la richiesta è falsa (un impostore)

## Regola di decisione per la verifica

- Si tratta di una comparazione con soglia

$$(I, X_Q) \in \begin{cases} \omega_1 & \text{se } S(X_Q, X_I) \geq T \\ \omega_2 & \text{altrimenti} \end{cases}$$

- $S$  è la funzione che misura la similitudine tra  $X_Q$  e  $X_I$
- $T$  è la soglia prefissata

- $S(X_Q$  e  $X_I$ ) si chiama **similarity score** o **match score**

### Problema di identificazione

- Dato in ingresso (query) un insieme di caratteristiche  $X_Q$ , determinare l'identità  $I_k$ , con  $k$  appartenente all'insieme  $\{1, 2, 3, \dots, M, M+1\}$  dove  $I_1, I_2, \dots, I_M$  sono le  $M$  identità memorizzate nel sistema e  $I_{M+1}$  rappresenta il caso di reiezione
- Nel caso di reiezione nessuna delle  $M$  identità registrate è sufficientemente simile all'ingresso

## Regola di decisione per l'identificazione

- Si tratta di  $M$  comparazioni con soglia con la seguente regola di decisione

$$X_Q \in \begin{cases} I_k & \text{se } K = \arg \max_k \{S(X_Q, X_{Ik})\} \text{ and } S(X_Q, X_{Ik}) \geq T \\ I_{M+1} & \text{altrimenti} \end{cases}$$

- Dove  $X_{Ik}$  è il template corrispondente alla identità  $I_k$
- $T$  è la soglia prefissata

- $S(X_Q$  e  $X_I$ ) si chiama **similarity score** o **match score**

- In alcuni casi ci si riferisce ad una **misura della distanza** fra  $X_Q$  e  $X_I$ . Una grande distanza fra i vettori di feature

- porta a un **basso match score**

### Distanza fra i template

- Esiste sempre una distanza nello spazio delle feature che separa i template anche della stessa persona. Questo è dovuto a fattori come:
  - Rumore di acquisizione
  - Diversa posa del soggetto
  - Diversa illuminazione o sfondo
  - Condizioni ambientali (umidità, temperatura, ...)
- Questo porta al fatto che la soglia  $T$  non può essere arbitrariamente abbassata, altrimenti nessuno sarà identificato

- Se si riscontrasse una distanza fra  $X_Q$  e  $X_I$  nulla ( $S(X_Q \text{ e } X_I) = \text{massimo\_valore\_ammissibile}$ ) probabilmente saremmo di fronte ad un replay attack

### Genuini ed impostori

- Si dice **genuine score** quando si confrontano le **distanze fra template dello stesso individuo**
- Si dice **impostor score** quando si confrontano le **distanze fra template di individui diversi**

### False Match e False Non-Match

Occorre distinguere i due casi possibili di errore:

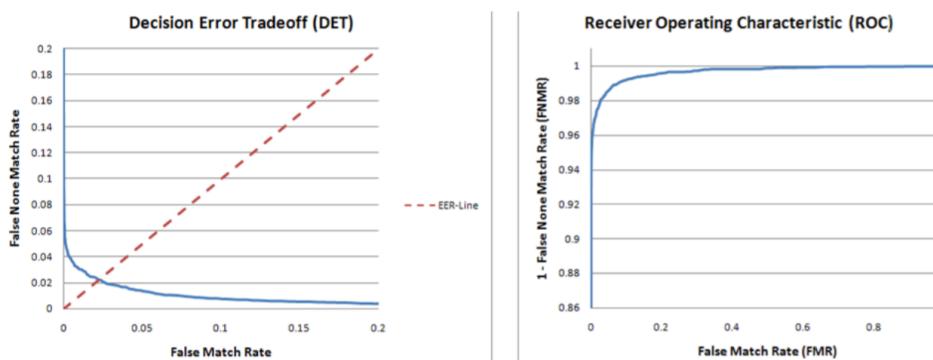
- Il ladro entra in casa perché il sistema biometrico lo ha scambiato per voi (False Match, Errore di tipo I)
  - Corrisponde al caso nel quale questo impostor score era maggiore della soglia T impostata
- Voi non entrate in casa perché il sistema biometrico ritiene che il vostro template non assomigli abbastanza a quello/i registrati (False Non-Match, Errore di tipo II)
  - Corrisponde al caso nel quale questo genuine score era minore della soglia T impostata

### FM Rate, FNM Rate

- Un certo numero di persone appartenenti al gruppo dei genuini sono sotto la soglia T e quindi non saranno autorizzati dando luogo ad errori di **False Non-Match (FNM)**.
  - $\text{FNMR}(T) = \text{FNM}(T) / \text{Totale_Genuini}$
- Al contrario una parte degli impostori hanno valori di match sopra la soglia T e quindi saranno autorizzati dando luogo ad errori di **False Match**.
  - $\text{FMR}(T) = \text{FM}(T) / \text{Totale_Impostori}$
- Nel caso si tratti di una **identificazione positiva** i tassi  $\text{FMR}(T)$  e  $\text{FNMR}(T)$  vengono rispettivamente chiamati **False Accept Rate FAR(T)** e **False Non-Accept Rate FNAR(T)**

### Decision Error Tradeoff (DET) e Receiver Operating Characteristic (ROC)

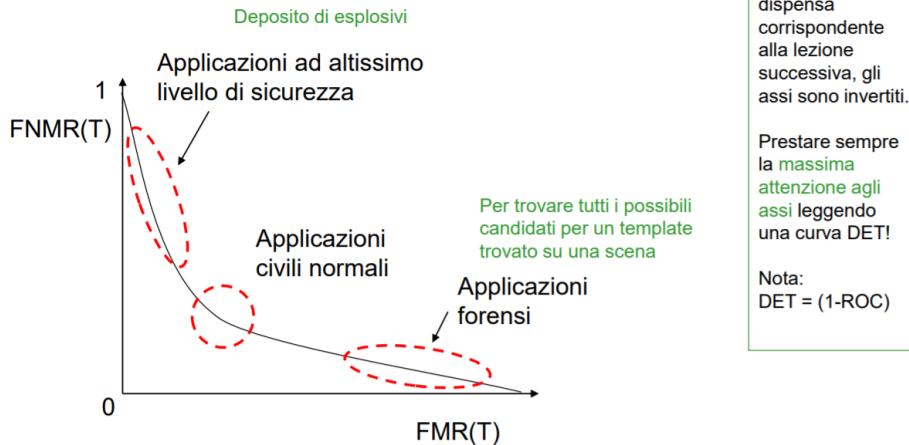
$$\text{DET} = 1 - \text{ROC}$$



**La curva DET e la curva ROC mostrano le stesse informazioni.**  
Riferendoci ad autenticazione positiva, la DET mette l'attenzione sul FNM (genuini che non entrano) mentre la ROC mette in evidenza 1-FNM (quanti genuini che riescono ad entrare)

## Regioni di funzionamento

Regolando la soglia T possiamo regolare il livello di sicurezza



## Equal Error Rate

- L'EER è il tasso di errore corrispondente all'unico punto nel quale abbiamo  $\text{FNMR}=\text{FMR}$
- L'EER è l'unico numero singolo che può riassumere il funzionamento del sistema

## Metodi statistici per la stima dei parametri di un sistema biometrico

### Modello utilizzato: Processo di Bernoulli

- Un SB (Sistema Biometrico) che venga usato in identificazione (1:N) si può modellizzare come un N prove di Bernoulli, ovvero un processo di Bernoulli
- Il numero di "successi" (errori del SB) dopo n prove è dato dalla variabile aleatoria  $S_n$ 
  - $S_n = X_1 + X_2 + \dots + X_n$
- La probabilità di avere k errori su n prove è (con  $q=1-p$ )
  - Ovvero al numero di sequenze di k successi e  $n-k$  fallimenti, moltiplicato per la probabilità che una qualunque di queste si verifichi

### Regola dei 3

“Quale è il tasso di errore più basso  $p$  che può essere stimato con un esperimento di comparazione di N campioni indipendenti?”

- Il tasso di errore  $p$  per il quale si ha la probabilità di ZERO errori in N prove è circa  $p \approx 3/N$ , per un intervallo di confidenza del 95%.
  - Altro modo di leggere la cosa: se abbiamo un sistema che commette ZERO errori su N prove non dobbiamo pensare di avere un sistema con  $p=0$ , ma con il 95% di confidenza abbiamo un sistema che ha  $p \approx 3/N$ .
  - Esempio: Se faccio 300 prove con campioni indipendenti e ho ZERO errori, allora posso dire che con confidenza del 95% il mio sistema ha un tasso di errore stimato del  $p \approx 3/N = 3/300 = 1\%$
- Estensione della regola dei 3: Se il sistema commette  $x$  errori su N prove indipendenti posso dire che l'errore sarà all'interno di un intervallo di confidenza stimato.

### Da verification a Identification, errori

“Quanto aumentano gli errori se uso un sistema di Verifica (FMR,FNMR) in modalità di Identificazione (FMRN,FNMNRN)?”

- $FNMR_N = FNMR$  (I tassi di errore per i **genuini** non cambiano)
- $FMR_N = 1 - (1 - FMR)^N$   
Ovvero =  $1 - (1 - FMR)^N$  (la probabilità che **non** ci sia un False match su tutti i campioni confrontati N)

### La regola dei 30

- La regola dei 30 è usata per determinare la larghezza del campione biometrico in questo modo:
  - “**Per essere sicuro con intervallo di conf. del 90% che il tasso di errore vero sia tra il ±30% del tasso di errore osservato ci devono essere almeno 30 errori**”.
- ES: Se abbiamo 30 falsi NON-match in 3000 comparazioni di genuini indipendenti, possiamo dire (con interv. di conf. del 90%) che l'errore vero sta tra 0.7% e 1.3%.

## Sistemi biometrici basati su impronte digitali

### Impronte digitali: excursus storico e introduzione

#### Introduzione storica

- Prime apparizioni come incisioni nel neolitico o su menhir (4000 – 2000 aC)
- Atto di vendita cinese per un terreno firmato con una impronta (1800 circa)
- **Primo documento “biometrico” India (1858)**
- Diffusione nel mondo dei primi sistemi:
  - 1858 India (dominio UK): Documenti riscossione, Controllo criminali
  - 1880 UK: inizio utilizzo per identificazione criminali
  - 1901 UK: Criminal Identification (Fingerprint bureau) New Scotland Yard
  - 1901 USA: Primo uso ufficiale delle impronte da parte del New York City Civil Service Commission
  - 1930 USA: L’FBI installa il National Fingerprint File

#### Primi sistemi di classificazione

- E. R. Henry, Classification and Uses of Fingerprints, London, 1900

#### Cosa sono le impronte digitali

- Sono creste e valli della pelle (Dermatoglyphics) sui palmi e sulle dita di molti animali
- **Sono tratti biometrici stabili dall’ottavo mese di gestazione** a meno di abrasioni, malattie o incidenti gravi

#### Sistema di classificazione attuale

- Le impronte si dividono in
  - Arch (Plain e Tented)
  - Loop (Left, Right)
    - Essentials of a loop:
      - Sufficient recurve;
      - One delta;
      - A ridge count across a looping ridge
  - Whorl (Plain, Twin loop)
    - The type of pattern in which
      - at least two deltas are present
      - with a recurve in front of each
  - Accidental
    - A volte categorizzata come Whorl, combina due tipi diversi di pattern o nessuno

- Attraverso
  - l'individuazione degli eventuali Core e Delta
  - lo studio degli orientamenti dei ridge

### Alcune applicazioni basate sulle impronte

- Applicazioni forensi
- Governative
- Commerciali

### Sistemi AFIS

- AFIS (Automated Fingerprint Identification System) è un sistema hardware e software per
  - **l'acquisizione e la classificazione dei cartellini decadattilarì**
  - **ricerche delle impronte sconosciute in una banca dati unica consultabile dal centro principale e dai terminali distribuiti.**

### Punti di forza e debolezze

- Punti di forza:
  - È una **tecnologia matura, ampiamente controllata, altamente accurata e funzionante in molti ambienti operativi**
  - **L'acquisizione** è mediamente **facile** ed ergonomica
  - Offre la **possibilità di usare più dita**, aumentando notevolmente l'accuratezza dei sistemi
- Debolezze:
  - Tutti i dispositivi **non riescono ad acquisire le impronte di una frazione della popolazione (solitamente il 4%)**
  - **L'accuratezza tende a degradare nel tempo**
  - Essendo largamente associata ad applicazioni forensi, **alcune persone provano senso di disagio nel fornire il tratto biometrico**

### I tre livelli di analisi delle impronte

#### Tre livelli di analisi

- Una impronta può essere esaminata su tre livelli:
  - globale (livello I)
  - locale (livello II)
  - ultra-fine (livello III)

#### Livello I

- A **livello globale** si osservano:
  1. **il flusso delle linee** (arch, loop, whorl o sottoclassificazioni)
  2. **i punti singolari** (core,delta), accurato.
  3. **la forma dell'impronta**
  4. **l'orientamento**
  5. **la frequenza delle righe dell'immagine.**

#### Livello II

- A **livello locale** è possibile identificare fino a circa 150 diverse caratteristiche locali delle creste (**minutiae**)
  - Le due principali caratteristiche sono le **terminazioni** e le **biforazioni**
  - L'FBI per i sistemi automatici (AFIS) usa solo terminazioni e biforazioni

### Livello III

- A **livello ultra-fine** è possibile individuare i seguenti dettagli:
  - intra-cresté (i **pori** per la sudorazione)
  - inter-cresté (**incipient ridges**)
- I dettagli del livello III sono considerati altamente distintivi, ma si rilevano solo ad altissima risoluzione, **almeno 1000 dpi ed in condizioni ideali** (i pori hanno dimensione 60-250 µm)

### Ed i gemelli?

- Anche i gemelli omozigoti (con lo stesso DNA) hanno impronte diverse!
- Le **impronte sono una manifestazione del fenotipo** (dipendente quindi anche da fattori casuali ed ambientali) pur partendo dallo stesso genotipo (DNA)

### Come procede un esperto (umano)

- Un tecnico esperto della comparazione di impronte digitali controlla
  1. la concordanza nella configurazione del **pattern globale**, che implica una tipologia comune per le due impronte confrontate
  2. la **concordanza qualitativa**, che implica che le minutiae corrispondenti siano identiche
  3. il **fattore quantitativo** che specifica il numero minimo di dettagli minutiae che devono corrispondere tra le due impronte (per esempio almeno 12)
  4. la **corrispondenza dei dettagli di livello III** che devono risultare identicamente intercorrelati

### Il Sistema AFIS italiano

- Progetto: 1994
- Inizio funzionamento: 1995
- Statistiche: 12,5 milioni di cartellini; 7,5 milioni di individui memorizzati
- Funzionamento: Impronte acquisite con un rapporto 1:1, ad una risoluzione di 500dpi, in scala di grigi (per identificazione giudiziaria necessaria la presenza di un riferimento metrico)

### La legge italiana

- La sentenza 2559 del 14.11.1959 espressa dalla Corte di Cassazione indica in **16-17 punti caratteristici** il minimo numero di segni **uguali per forma, posizione ed orientamento**

### Tecnologie sul mercato

Le quali riconoscono da 100 milioni fino ad un miliardo di impronte al secondo. Ed hanno una accuratezza che raggiunge anche il 99,98%

### Future trends negli AFIS

- Aumentare a 1000 dpi la risoluzione standard
- Acquisizioni delle impronte digitali senza contatto
- Aumentare interoperabilità
- Automatizzare e aumentare precisione estrazione minutiae
- Estensione a sistemi multimodali (AFIS->ABIS)

### Impronte digitali e sensori: caratteristiche

#### Tipologie di sensori e caratteristiche

*Quale è il compito dei sensori?*

- I sensori devono cercare di **catturare la distribuzione di creste e valli sulla pelle**
- Maggiori dettagli catturiamo, migliore sarà la capacità del sistema di identificare/verificare le identità delle persone

- Possiamo immaginare le **impronte** come **immagini bidimensionali ma anche come superfici tridimensionali**

#### *Modalità di acquisizione*

- Due modalità fondamentali:
  - **off-line**
  - **live-scan**

#### *Acquisizione offline*

- L'acquisizione off-line è in due fasi:
  - i polpastrelli vengono prima passati su un tampone inchiestrato e poi vengono rotolati su una scheda di carta.
  - La scheda viene acquisita con uno scanner ottico o telecamera ad alta risoluzione.

#### *Impronte latenti*

- Le **impronte digitali latenti** (per esempio provenienti dalla scena del crimine) sono di tipo off-line
  - sono prodotte dalle tracce lasciate del grasso secreto dalla pelle che lascia sulle superficie una traccia evidenziabile successivamente con speciali reagenti chimici.

#### *Tipi di sensori live-scan*

- Nella modalità **live-scan**, invece, l'immagine digitale dell'impronta digitale è acquisita in tempo reale direttamente tramite il contatto del polpastrello con un apposito sensore
- I sensori possono essere:
  - **Ottici**, basati:
    - sul fenomeno della frustrated total internal reflection (FTIR)
    - su scanner tradizionali
  - **Stato solido**, con pixel sensibili alle variazioni di:
    - capacità
    - pressione (Piezoelettrici)
    - temperatura
  - Altro tipo
    - Ultrasuoni

#### *Panoramica delle immagini dei sensori*

- I vari sensori producono delle immagini con delle caratteristiche molto diverse fra loro

#### *Proprietà del sensore*

- Nello scegliere un sensore dobbiamo controllare:
  - risoluzione
  - area di acquisizione
  - numero di pixel e bit per pixel (8, 16, 24 bit)
  - contrasto
  - distorsione geometrica
- In alcune applicazioni può essere utile considerare anche altre caratteristiche (supporto, documentazione e funzioni avanzate)

### *Sensori ottici*

- Tipologie:
  - Rifrazione interna
  - A foglio di prismi
  - Con fibre ottiche
  - Elettro-ottico
- Risposta alle diverse condizioni di acquisizione (dito asciutto, bagnato...)

### *Sensori a stato solido*

Il contatto fra il ridge e la superficie del sensore cambia la capacità del circuito del singolo pixel

### *Sensori 3D*

Esistono dei sensori che riescono a rilevare la tridimensionalità della impronta digitale

## **Problemi di acquisizione**

- Diversi problemi nella fase di acquisizione:
  - **Pressione**
    - I ridge da discontinui tendono a diventare continui
    - Iniziano a vedersi meglio i pori e gli incipiens ridge
    - Quando la pressione diventa troppa, iniziano ad unirsi i ridge fra loro o con gli incipiens ridge
  - **Roto-traslazioni e deformazioni**
    - Le parti in contatto con il sensore tendono a non ruotare/spostarsi con il dito creando una deformazione non lineare come sarebbe invece una semplice roto-traslazione
    - Deformazioni non lineari di diverso tipo

## **Sistemi commerciali**

- I sistemi commerciali completi hanno valori che si attestano attorno a:
  - FNMR=0.23%@FAR=0.01%
  - EER=0.258%
  - Capacity: 4,000 fingerprints, 2,000 face, 10,000 card credentials

## **Rappresentazione, compressione e non unicità**

### **Rappresentazioni delle impronte**

- La rappresentazione delle impronte digitali in un sistema biometrico dipende dal:
  - Sensore impiegato
  - Livello di analisi
  - Caratteristiche che si estraggono

### **Immagini delle impronte**

- Il sample della impronta è una immagine in toni di grigio quindi si controlla
  - risoluzione,
  - bit per pixel
- Un esempio: l'**FBI digitalizza le impronte del DB nazionale a 500 Dpi con 8 bit per pixel**. Una cartella con **10 impronte** occupa circa **10 MB!**

## Formati di compressione

- Usando un formato “**lossless**”, con le impronte si ottiene un **fattore di compressione 2:1**, troppo poco per un archivio di grandi dimensioni
- Esistono dei **formati di compressione appositi** per le immagini di **impronte digitali**
  - L’**FBI ed il NIST** americano **usano** il seguente algoritmo **Wavelet Scalar Quantization (WSQ)** “Gray-scale Fingerprint Image Compression Algorithm”

## Unicità delle impronte (al secondo livello)

- Data una impronta con n minutiae, è possibile calcolare la probabilità di condividere q minutiae con un altro template contenente m minutiae  $p(M,m,n,q)$ 
  - $M = \text{Area di Overlap} / \text{Area di tolleranza} = A/C$
- In realtà abbiamo a disposizione molti altri parametri quindi la stima diventa ancora più conservativa
  - Minuzie
  - Pori
  - Ridge count
  - Core

## Algoritmi per le impronte digitali

### Algoritmi di prefiltraggio ed enhancement

- Nel modulo per l’**Estrazione delle feature** si eseguono tipicamente questi passi:
  1. Filtraggio iniziale
  2. Manipolazione della immagine (enhancement)
  3. Estrazione delle feature
  4. Codifica (Il modulo di codifica è talvolta rappresentato esternamente al modulo di feature extraction)

### Filtraggi iniziali

- Fra i filtri iniziali usati di solito si trovano:
  - Contrast stretching
  - Histogram manipulation
  - Normalization
  - Wiener Filtering

### Contrast stretching

- Le immagini delle impronte digitali hanno di solito una dinamica dei toni di grigio molto limitata
- L’operazione di Contrast Stretching allarga la dinamica dell’immagine

### Manipolazione dell’istogramma

- L’istogramma di una immagine può essere mappato in un altro mediante diverse funzioni
- Il logaritmo permette ad esempio di evidenziare delle variazioni sottili di toni di grigio in una immagine che ha già una dinamica elevata

### Filtro di Wiener

- Quando si conoscono le caratteristiche spettrali dell’immagine e del rumore si usa il filtro di Wiener
- Nel caso delle impronte si considera la distanza inter-ridge media e si considera il rumore come additivo gaussiano
- Il filtro di Wiener in questa applicazione si comporta come un passa-banda ottimizzato

### *Normalizzazione*

- L'obiettivo della normalizzazione è quello di standardizzare le variazioni di grigio dei ridge in tutta l'immagine per agevolare gli algoritmi successivi
- NON equivale ad una equalizzazione dell'istogramma in quanto il filtraggio può essere programmato per lavorare anche localmente

### **Segmentazione**

- Gli algoritmi per la segmentazione estraono il foreground (l'impronta) dal background (lo sfondo)
- Una tecnica basilare molto usata **calcola la varianza locale dell'immagine (oppure il modulo del gradiente dell'immagine) in blocchi (16x16) e scarta i blocchi sotto ad una soglia prefissata (unrecoverable)**

### **Manipolazione immagine (enhancement)**

- Obiettivi:
  - **migliorare la chiarezza della struttura di ridge** nelle regioni dove possibile
  - **marcare le regioni dove non è possibile estrarre informazione** perché presente **troppo rumore**
- Ingresso: immagine a toni di grigio
- Uscita: immagine a toni di grigio o binarizzata a seconda dell'algoritmo usato

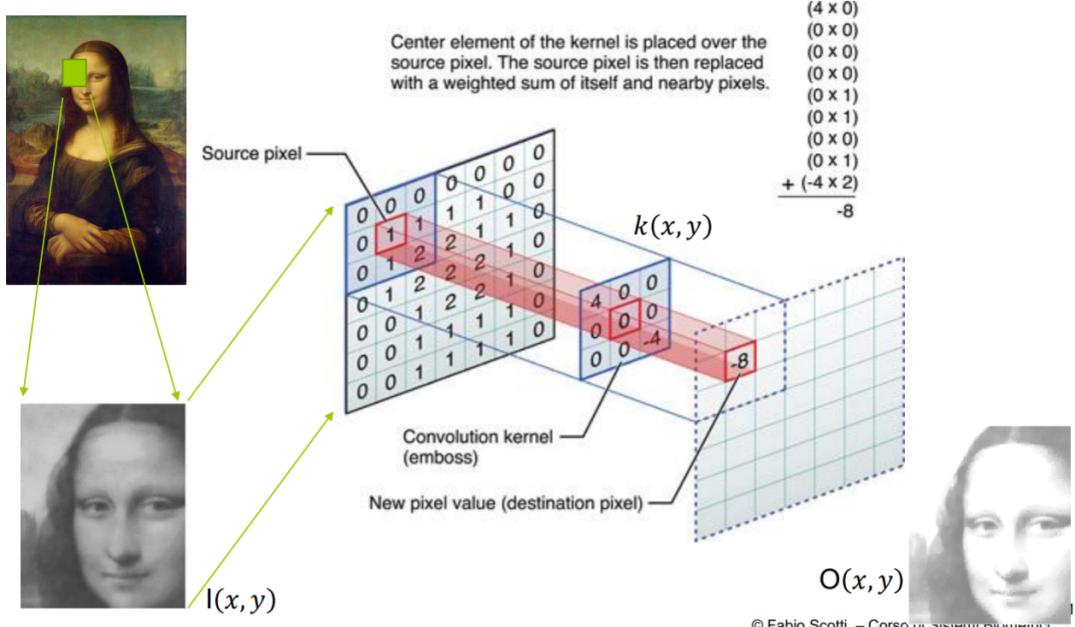
### *Manipolazione delle immagini: filtri contestuali*

- Per ottenere i massimi risultati nell'evidenziare la struttura dei ridge in una immagine occorre ricorrere ai **filtri adattativi o contestuali**
- Questa categoria dei filtri per le immagini **modifica automaticamente i propri parametri per meglio adattarsi ai mutamenti delle condizioni dell'immagine**
  - Distanza fra i ridge
  - Orientamento dei ridge
  - Livello di rumore presente
- Questi filtri lavorano sulla immagine in ingresso attraverso **un'operazione chiamata convoluzione con una maschera di filtraggio**
- A seconda del tipo di maschera usata il filtro aumenta/diminuisce alcune caratteristiche piuttosto che altre
- Una parte del filtro controlla la porzione dell'immagine in esame e adatta i parametri della maschera

Filtraggio immagini = convoluzione

$$O(x, y) = I(x, y) * k(x, y)$$

## Filtraggio immagini = convoluzione



### Manipolazione delle immagini: filtro di O'Gorman and Nickerson

- La forma particolare di questa **maschera** è fatta per fare “match” con lo spessore dei **ridge**, la loro distanza di separazione, il valore del massimo e del minimo in un intorno del punto di esame
- Mediante la **rotazione della maschera** si cerca anche di fare “match” anche **con la direzione preferenziale dei ridge**
- Inoltre questo filtro tende ad **attenuare il rumore locale**

### Manipolazione delle immagini: filtro di Gabor

- è basato sul **filtro di gabor** (prodotto fra una funzione sinusoidale in 2D ed una gaussiana)
  1. Viene creato il cosiddetto **banco di filtri**, preparato per **varie angolazioni e varie distanze inter-ridge**
  2. La **maschera** che offre **migliore “match”** viene **impiegata nella convoluzione di quella zona dell'immagine**
- Quando si analizzano regioni “unrecoverable” il filtro viene disattivato per non creare falsi ridge (artefatti)
- In alcune regioni, tuttavia degli artefatti possono essere introdotti ugualmente
- Il filtraggio di Gabor può introdurre effetti di blocchettizzazione

### Estrazione di caratteristica (estrazione delle feature)

#### Tipi di caratteristiche da estrarre

- Possiamo estrarre feature dal sample appartenenti ai 3 livelli
  - Livello I: direzioni dei ridge, core, delta, ridge count
  - Livello II: minutiae
  - Livello III: pori, cicatrici

#### Livello I

##### Ridge counting

- È una misura dei ridge che attraversano una linea immaginaria passante tra due minutiae

- La grandezza del ridge counting, pur essendo calcolata partendo dalle minutiae (livello II) è considerata come appartenente al livello I in quanto porta informazioni non localizzate attorno ad un punto ma su cosa succede nell'impronta fra alcuni punti anche lontani fra loro

#### *Analisi delle frequenze spaziali*

- È una misura di quanto sono stretti o larghi i ridge nelle varie regioni dell'impronta
- Ridge frequency: inverso della distanza media tra due picchi consecutivi

#### *Mappa delle frequenze spaziali*

- Usando l'informazione ricavata dalle frequenze di ridge per ogni blocco dell'immagine è possibile avere la mappa delle frequenze dell'immagine

#### *Orientamento di un ridge*

## Orientamento di un ridge

- Non è un calcolo banale!
- Di solito si divide l'impronta in blocchi WxW non sovrapposti
- Si calcolano le immagini gradiente G<sub>x</sub> e G<sub>y</sub> tipicamente usando gli operatori di Sobel o Marr-Hildreth
- La seguente formula calcola la stima ottimizzata dell'orientamento medio nel blocco

$$\theta(i, j) = \left( \frac{1}{2} \right) \tan^{-1} \left( \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} \frac{2G_x(u, v)G_y(u, v)}{G_x^2(u, v) - G_y^2(u, v)} \right)$$

$\theta = \tan^{-1} \left[ \frac{g_y}{g_x} \right],$   
Formula classica  
del gradiente dell'immagine puntuale

- Occorre ora controllare che non vi siano salti di fase dovuti al fatto che il ridge non ha un verso ma solo la direzione (ad esempio, da 5 gradi a 175)
- In alcuni casi è necessario effettuare un filtraggio passa-basso (una media spaziale) per evitare comunque salti bruschi vicino ai punti singolari come core e delta
- Il calcolo esatto e robusto dell'orientamento dei ridge è fondamentale nell'enhacement, nell'identificazione delle minutiae e nelle funzioni di matching delle impronte digitali

#### *Mappa degli orientamenti*

- Usando il valore di θ<sub>ij</sub> calcolato in ogni blocco si ottiene una mappa (heatmap)
- Usando il vettore gradiente dell'immagine in un blocco B<sub>ij</sub> si possono anche produrre mappe nelle quali si visualizza il vettore ottenuto dal modulo e dall'orientamento del gradiente
  - mappa che mi mostra moduli e angolo dei singoli punti analizzati (gradiente)

#### *Orientation Field Flow Curves*

- Le OFFC sono curve (sintetiche) all'interno delle impronte digitali la cui tangente è parallela al campo di orientamento dell'impronta
- Sono molto usate per studiare la topologia e per classificare le impronte

#### *OFFC e classificazione delle impronte*

- Le OFFC permettono di localizzare in modo molto robusto la presenza di punti singolari come core e delta attraverso il loro andamento
- Le OFFC si proiettano in uno spazio attraverso le mappe isometriche. L'andamento della proiezione (scostamento angolare della curva intanto che evolve) individua il tipo di punto singolare

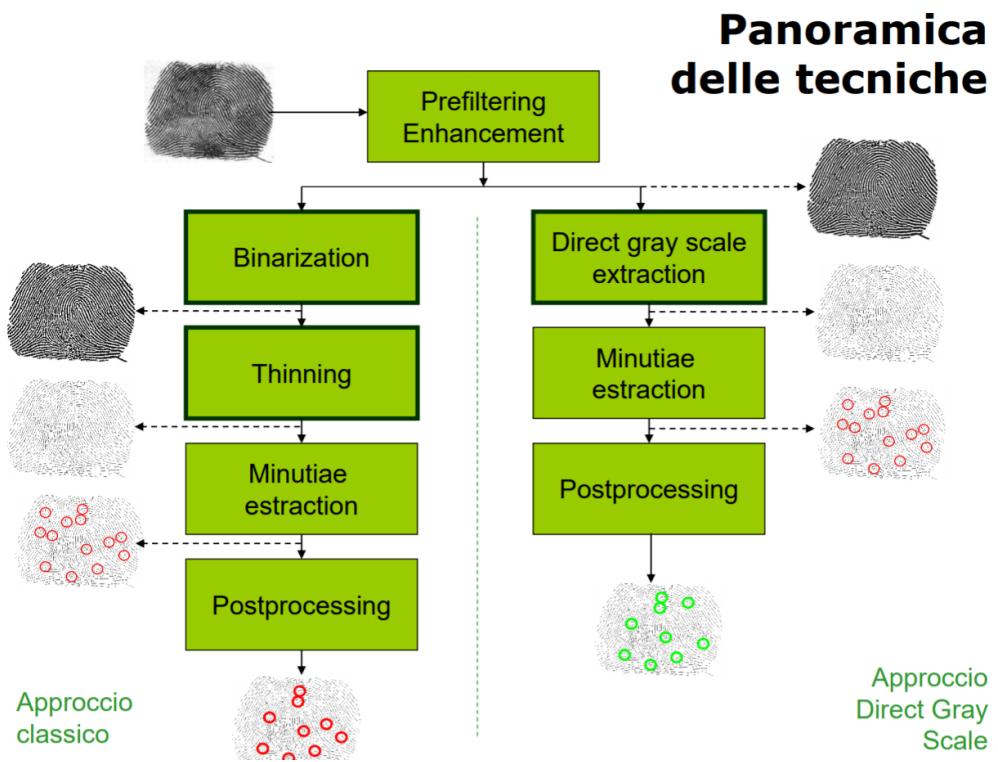
### Classificazione delle impronte

- Usando Core/Delta e/o OFFC si arriva a err.= 3-5%
- Notare come **abbassando il numero di classi**
  1. **si alzi il #campioni necessari da scansionare** (P.R. ottenibile sale. Es. 20->28)
  2. **si abbassi l'errore di classificazione** (il problema di classificazione è più semplice)

### Core detection: metodo delle normali

- I **punti di core** possono essere **calcolati intersecando le normali**
- Se seguendo N ridge e calcolando M normali abbiamo un numero sufficientemente alto di **intersezioni in un intorno di un punto** allora abbiamo trovato un **core**
- Core/Delta detection: **metodo di Poincare**
  - I punti singolari possono essere individuati controllando il valore dell'indice di Poincare calcolato in ogni punto i,j della immagine lungo una curva di Np punti
  - indice =  $\frac{1}{2}$  --> Core
  - indice =  $-\frac{1}{2}$  --> Delta

### Livello II



### Sequenza classica per l'estrazione

- La tecnica classica prevede:
  1. Enhancement
  2. Binarization
  3. Thinning
  4. Minutiae extraction
  5. Post processing

### Metodi di binarizzazione

- I metodi di binarizzazione portano una immagine in toni di grigio in una **immagine in bianco e nero dove sono evidenziati i ridge**

- I metodi classici di **binarizzazione a soglia** e **a soglia locale** nel caso delle impronte non funzionano in modo robusto

### Thinning

- L'operazione di thinning corrisponde ad **ridurre progressivamente le linee dell'immagine binarizzata fino allo spessore di 1 pixel** (scheletro dell'immagine)
- L'algoritmo deve anche (se possibile) riempire i buchi nei ridge per non creare profili tipo biforazioni spurie

### Come identificare la minuzia

- Esaminando l'intorno di ogni punto lungo un ridge di una immagine scheletrizzata è immediato trovare se siamo su fine riga o una biforcazione, basta contare le intersezioni lungo il perimetro della matrice 3x3 attorno al punto
  - Una intersezione → fine riga
  - Due intersezioni → ridge passante
  - Tre intersezioni → biforcazione

### Metodi di post processing

- I moduli di post processing servono per **rimuovere le minutiae spurie** introdotte dai moduli precedenti per errore
- Esistono due categorie principali di post processing
  - Structural post-processing**
    - tipicamente basati su regole
    - Controllano le caratteristiche dello scheletro adiacente alla minutia candidata ad essere tenuta o scartata
  - Minutiae filtering in the gray-scale domain**
    - I moduli di post processing basati sui toni di grigio analizzano la regione dell'immagine a toni di grigio adiacente alla minutia da tenere o scartare
    - Si possono usare vari algoritmi per effettuare questo controllo. Come reti neurali allenate a riconoscere le vere minutiae da quelle false
    - In ogni caso gli algoritmi preposti devono imparare a **riconoscere dei pattern di grigio**
    - Direct Gray Scale Extraction:
      - Si sceglie un **insieme di punti di partenza con una griglia**
      - Si **segue ogni ridge** dal punto di partenza **fino a quando si trova un fine riga o una biforcazione**
      - Si usa una **strategia di labellizzazione** per evitare di seguire più volte lo stesso ridge

### Livello III

- Tipicamente si studiano le posizioni dei pori attraverso
  - Segmentazione
  - Operatori morfologici
- Pori possono essere aperti e chiusi

### "Spoofing e anti-spoofing"

#### Fake finger

- E' possibile ricreare la superficie dell'impronta con vari materiali (gelatina, gomma, silicone)

- partendo da una impronta presa (“lifted”) da una scena
- da una immagine rubata da un sistema
- da un dito reale di una “talpa”

#### **Test di vitalità per sensori ottici**

- il **flusso sanguigno e la sua pulsazione** possono essere rilevati **mediante la luce riflessa o trasmessa attraverso il dito**
- la **temperatura e la sua distribuzione** può indicare se il dito è vivo, morto o fasullo
- un **meccanismo di acquisizione differenziata per le creste ed i solchi** per resistere ad attacchi con immagini 2D fasulle
- I sensori ad alta risoluzione (>700 dpi) rivelano dettagli del terzo III difficili da imitare in un dito artificiale
- La pelle del dito cambia colore per effetto della pressione

#### **Test di vitalità per sensori allo stato solido**

- La **differenza di potenziale tra due specifici punti** della muscolatura del dito (miografia) può essere utilizzata per distinguerlo da un dito morto
- La misurazione della **impedenza** del dito può essere utile per verificare la vitalità del dito
- La **sudorazione** continua di un dito e la sua evoluzione temporale sul sensore è un altro ottimo test di vitalità

#### **Generazione sintetica di impronte**

- Sono disponibili in letteratura dei generatori di impronte sintetiche che, partendo da numeri causali, sono in grado di generare immagini di impronte perfettamente verosimili

## **Sistemi biometrici basati sull'iride**

#### **Caratteristiche dell'iride e sensori**

#### **Panoramica della applicazione**

- Considerato come il **tratto biometrico più accurato** in assoluto **dopo il DNA**
- Poco gradito dagli utenti per la sua “percepita” invasività
- L'iride presenta **caratteristiche numerosissime e stabili nel tempo**
- **Inizia a crearsi dal terzo mese nel feto, processo completato al 7 mese, ma stabili dal secondo anno in poi**
- Sistema piuttosto **complesso e costoso**, ma **difficile da frodare**
- L'iride è la parte colorata, ovvero la membrana piatta che sta tra la cornea e il cristallino

#### **Unicità dell'iride**

- Esattamente come per il caso delle impronte, **non esistono due iridi uguali**
- Durante la formazione dell'iride si hanno delle componenti causali che producono un pattern di righe, tagli, pieghe (le feature iridee) assolutamente unico e distinguibile
- Anche i gemelli omozigoti hanno iridi diverse

#### **Quale luce per acquisire l'iride?**

Le feature che maggiormente sono interessanti per il sistema biometrico **si vedono meglio con luce IR** piuttosto che con luce visibile

#### **Quale sensore per acquisire l'iride?**

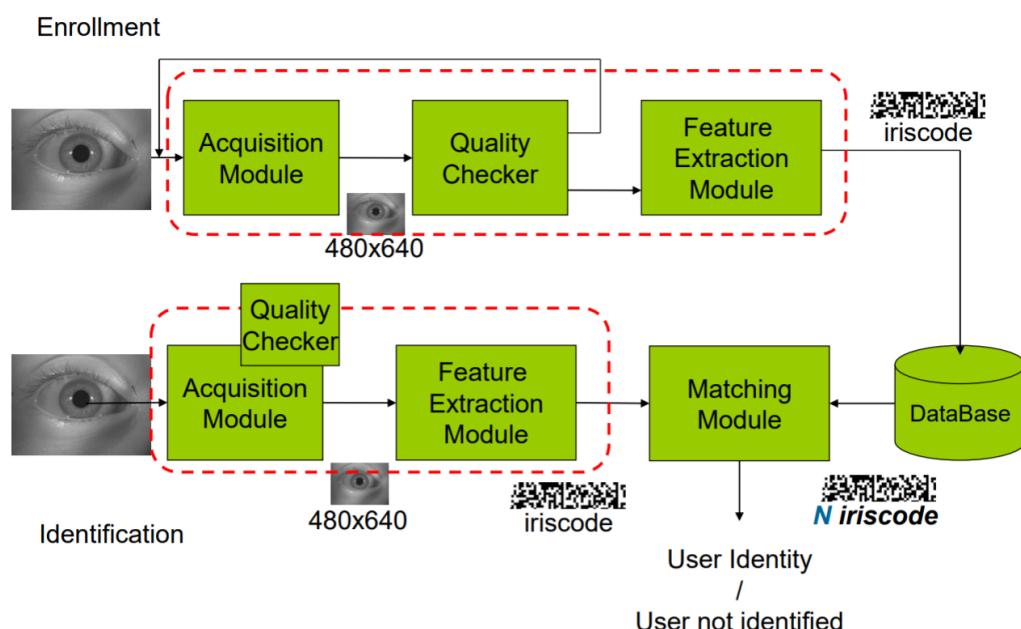
- Per catturare i complessi dettagli dell'iride, il sistema di acquisizione deve poter **risolvere con almeno 70 pixel il raggio dell'iride (di solito 100-140pixel)**
- Si usano **CCD monocromatici** (almeno 640x480) capaci di acquisire nel vicino infrarosso (NIR)

- E' necessario usare **telecamere con ottiche variabili** per trovare l'occhio nel volto e poi zoomare verso l'occhio per acquisirlo alla massima risoluzione possibile

## Rappresentazione delle iridi

### Struttura dei moduli secondo Dougman

## Struttura dei moduli secondo Dougman



### Dalla immagine iride al template

- I più moderni sistemi per il riconoscimento basati sull'iride rappresentano l'iride come una stringa di bit, spesso chiamata **IRISCODE**
- Perché la conversione avvenga correttamente moltissimi fattori sono da tenere in conto ed è un problema complesso

### La sequenza dei passi principali

- Passi che ci permettono di passare da una immagine di un occhio ad un IRISCODE:
  - individuazione dei centri e raggi della pupilla e dell'iride**
  - rimozione** della parte non utile occupata dalle **iridi e delle ciglia**
  - linearizzazione** dell'iride
  - trasformazione** dell'iride **linearizzata** con le 2D Gabor Wavelet
  - trasformazione delle fasi della trasformata wavelet in bit, ovvero **l'IRISCODE**

### Calcolo dei centri e raggi di iride e pupilla

- Trovare l'occhio** (tendenzialmente la pupilla) nell'immagine del volto
- Eseguire una **acquisizione corretta dell'iride** (almeno 70 pixel a fuoco lungo il raggio)
- Trovare la pupilla**
- Trovare il **raggio esterno dell'iride**
- Rifinire** le stime

### Rimozione di palpebre e ciglia

- Occorre segmentare solo la parte utile dell'iride, "marcando" l'immagine dove invece sono presenti **ciglia, palpebre, riflessi esterni, zone di basso contrasto o sfocate**
- Se manca più del 50% dell'iride occorre riacquisire l'iride

## Linearizzazione dell'iride

- Individuati raggi e centri si procede alla fase di unwrapping dell'iride (linearizzazione)
- Si fissano le dimensioni dei settori dell'iride
  - numero delle corone
  - delta angolo di scansione
- Ogni pixel dell'iride linearizzata nasce da una interpolazione del corrispondente settore nell'iride

## Calcolo dell'iris code

- Avendo l'iride linearizzata l'espressa nelle coordinate  $\rho$  (raggio) e  $\theta$  (angolo) si calcola con una formula
- L'iride linearizzata è convoluta con delle funzioni gaussiane (basi della demodulazione)
- $\omega$  è chiamata la frequenza della wavelet,  $\alpha$  e  $\beta$  sono la larghezza del filtro
- *"The detailed iris pattern is encoded into a 256-byte "IrisCode" by demodulating it with 2D Gabor wavelets, which represent the texture by phasors in the complex plane. Each phasor angle is quantized into just the quadrant in which it lies for each local element of the iris pattern, and this operation is repeated all across the iris, at many different scales of analysis"*

## Proprietà dell'iris code

- La codifica dell'iride è eseguita in uno spazio 2D adimensionale di coordinate polari
  - questo rende la codifica invariante rispetto:
    - alla dimensione dell'iride
    - allo zoom dei sistemi ottici
    - alla dilatazione dell'iride dovuta alla luce
- Le funzioni wavelet usate in demodulazione sono parametrizzate con 4 gradi di libertà (dimensione, orientamento e 2 coordinate posizionali) che possono variare in alcune "ottave"
  - questo garantisce che più scale di dettagli verranno "colte" nella codifica (iris code si fa su più scale)
- L'unica informazione estratta dall'iride con l'Iriscode dipende dalla fase; questo la rende invariante rispetto a:
  - contrasto della immagine
  - livello di grigio medio dell'immagine
  - illuminazione presente
- La descrizione di fase è molto compatta, di solito bastano 256 byte per rappresentare una iride, più 256 byte di controllo per escludere i bit nati dove nell'immagine vi erano degli artefatti come:
  - riflessi delle luci ambientali sull'iride (in realtà sulla cornea)
  - ciglia sovrapposte
  - palpebre
  - regioni con troppo poco contrasto, quindi con dati non "deboli"
- La probabilità di ogni bit dell'Iriscode di essere 1 è del 50%, questo rende l'Iriscode un codice a massima entropia

## Algoritmi di enhancement e prefiltraggio

### Quality checker

Controllo qualità del sample: focus assessment

- Per poter avere un tempo di integrazione breve, occorre fare entrare molta luce nell'obiettivo, ma questo implica una focale non adatta a riprendere bene a fuoco l'iride
- Il fuoco dell'iride viene quindi controllato con dei filtri software

- L'effetto di sfocatura di una immagine dovuto ad un sistema ottico può essere parzialmente riconvertito applicando un filtro di deblur che si comporta al "contrario" della parte del sistema ottico che produce la sfocatura
  - Il **filtro di deblur** tende ad aumentare le **frequenze alte** dell'immagine che erano state attenuate dal blur
  - Il controllo del fuoco per una immagine monocromatica a 640x480 con un processore RISC a 300MHz e la maschera (kernel) 8x8 impiega 15 ms, quindi può essere eseguito a livello di frame

#### *Controllo qualità del sample: acquisizioni fuori fuoco*

- Se l'immagine è troppo mossa occorre scartarla in quanto l'Iriscode risultante sarebbe composto solo da bit casuali dipendenti dal rumore del CCD
- Il controllo se la parte in alta frequenza dello spettro dell'iride è oltre una soglia prefissata corrisponde a verificare se è presente una sufficiente quantità di "dettagli fini" maggiore di una soglia

#### *Contrast adjustment*

- Non si usano particolari prefiltraggi nel caso dell'iride
- In alcuni casi si applica un contrast stretching per migliorare il contrasto e quindi la intelligenza dell'immagine da parte degli operatori

### Feature Extraction Module

#### *Come trovare l'iride*

- Dougman propone:
  - cercare nell'immagine (estrazione di un massimo) ...
  - i centri di contorni di variazioni di grigio di forma circolare (l'integrale lungo un cammino circolare di derivata radiale)
- **Operatore integro differenziale di Dougman**
- In particolare abbiamo:
  - **l'operatore** nel modulo **si comporta** complessivamente come un filtro di circular edge detection, ossia un **riconoscitore di bordi circolari** che produce **valori alti quando incontra un cerchio vicino al perimetro di esplorazione circolare in  $x_0$ ,  $y_0$  e raggio  $r$**

#### *Estrazione delle palpebre*

- Modificando l'operatore integro differenziale per le iridi si possono trovare le palpebre
- Immaginando le palpebre come una parte di una parabola, il cammino di integrazione diventa una parabola e non più il cerchio

#### *Estrazione delle ciglia*

- Le ciglia si possono individuare (segmentazione, wavelet, ecc.) sfruttando questa conoscenza a priori
  - le ciglia **devono partire dalla posizione individuata delle palpebre**
  - le ciglia **risultano sempre più scure rispetto all'iride**
  - la loro dimensione minore (**larghezza**) è **facilmente stimabile**
- È molto importante individuare ogni parte dell'immagine che non sia iride per non inserire in enroll una informazione errata!

### Algoritmi di matching (Matching module)

#### **Distribuzione dei bit in un singolo Iriscode**

- Il grafico mostra la **probabilità in un iriscode che l' i-esimo bit al suo interno sia 1 oppure 0**
- Il fatto che le probabilità siano **uniformemente livellate intorno al 50%** significa che l'iriscode è (quasi) un **codice a massima entropia**

### Come sono legati i bit in un singolo iriscode

- Sono presenti delle correlazioni fra i bit all'interno dell'iriscode
- Questo perché la struttura è auto-predittiva
  - un taglio radiale si incontra in altre "corone" di analisi
- Queste correlazioni limitano i veri gradi di libertà in un iriscode:
  - in altre parole non è vero che l'iriscode nasce come un numero binario "del tutto casuale"
  - alcuni gruppi di bit portano ad incontrare nell'iriscode maggiore probabilità altri gruppi di bit

### Alcuni fattori che aumentano la variabilità intraclasse

- Rotazioni della testa
- Variazioni dello zoom delle ottiche
- Dilatazione della pupilla

### Algoritmi di matching per gli Iriscode

- La **comparazione** è effettuata fra Iriscode di 256 byte attraverso il **calcolo della distanza di Hamming**
- La distanza di Hamming **conta i bit in disaccordo fra le due stringhe**, e li normalizza al numero totale di **bit N**
  - però così prendo dentro anche le ciglia e lo sporco in generale. Troverò molta distanza che è data da rumore, quindi devo applicare una maschera
  - Se vi sono occlusioni dell'iride (palpebre, riflessi, ciglia) dovremmo aver preparato le maschere di oscuramento delle zone (vedi algoritmi in M4U2L1) dove non vi è informazione utile (maskA, maskB)
  - **Andremo a togliere dal calcolo della distanza di Hamming** le zone da non considerare

### Velocità del matching di Iriscode

- L'esecuzione degli AND e degli XOR può avvenire a blocchi di bit pari alla lunghezza di parola del processore (tipicamente almeno 32bit)
- Questo rende il **matching assolutamente veloce**
- È possibile **parallelizzare la ricerca** anche su DB di enormi dimensioni
- Il sistema in teoria potrebbe funzionare anche su scala nazionale (una iride per individuo)
- Esempi
  - su un processore a 300MHz si riescono ad eseguire 100000 comparazioni al secondo
  - **su un server a 3 GHz si arriva a 1 milione di Iriscode comparati in un secondo**

### Rotazioni dell'Iriscode

- In teoria, due Iriscode calcolati dall'iride della stessa persona dovrebbero avere distanza di Hamming=0
- In realtà **fra due acquisizioni** perfettamente eseguite a pochi istanti una **dall'altra si può osservare uno spostamento di ±1 posizione del pattern nei due template**
- Per questo motivo **si fanno 3 comparazioni e si sceglie il minimo valore di matching fra le tre come valore finale**

### Algoritmi matching e prestazioni

#### Tassi di errore del sistema

- In letteratura sono presenti studi sia teorici sia applicativi che mostrano dei tassi di errore nulli!
- Altri studi indicano **FTE=7%**
- E il FNMR? FNMR verifica=6%, FNMR di identificazione su 1,4 milioni di individui <0.001
- Comparazioni
  - Verifica identità (al primo tentativo): **FMR=0% FNMR=4%**
  - Verifica identità (su 3 tentativi): FMR=0% FNMR=0.4%

- NIST: the most accurate one-to-one matcher yields an FNMR (False NonMatch Rate) of 0.0057 (about 1 in 175) at an FMR of 10–5 (1 in 100 000).
- Submissions from four other participants (NeuroTechnology, DeltaID, Tiger IT, and Decatur) follow closely behind with FNMRs between 0.0066 (1 in 152) and 0.0070 (1 in 143).

### Svantaggi della tecnica

- L'utente deve essere collaborativo e stare esattamente ad una predeterminata distanza dal sensore
- I costi del sensore e del sistema sono alti
- Le immagini possono essere di bassa qualità e provocano errori di "failure to enroll"
- In recenti test si arriva al **7% di scansioni fallite** (occhio umido, lenti a contatto rigide, ciglia lunghe, pupille dilatate, postumi della chirurgia della cataratta, tremori dell'iride)

### Quanti bit significativi nell'Iriscode?

- La distribuzione delle comparazioni di iridi diverse è perfettamente aderente ad un binomiale con 249 gradi di libertà e  $p=0.5$
- Questo significa che gli Iriscode mediamente distano in numero di bit come dei numeri casuali di **249 bit**
- Fissiamo la soglia al 31%. La probabilità che due persone abbiano in comune il 31% di 249 bit casuali è infinitesima

### Progettazione della soglia?

- Se possiamo stimare la distanza di hamming fra iriscode di diversi (impostori) con la bernulliana vista, possiamo calcolare quanti tentativi dovremmo fare per trovare il primo FALSE MATCH (ovvero un impostore che entra!)
  - Distanze tabulate, oppure:
- **Basandoci sul modello a distribuzione binomiale è possibile calcolare la soglia della distanza di Hamming che meglio divide le distribuzioni rinormalizzandola su queste condizioni:**
  - Adattamento del criterio in base alla dimensione **N** del DB per evitare accumulazione della probabilità di False Match
  - **Rinormalizzazione della distanza di Hamming quando solo la n di bit sono disponibile a causa delle occlusioni**

### Perché le distribuzioni reali non sono simmetriche?

- In generale: le stime viste in tabella sono OTTIMISTICHE e la vera probabilità di False Match in realtà dipende dalla qualità delle ottiche! Occorre procedere ad un test sul campo sempre!
- In ogni caso, ad oggi, i sistemi basati su Iriscode sono i sistemi biometrici "livescan" più accurati esistenti

### Come sono le distribuzioni di occhi geneticamente uguali?

- Sono stati confrontati fra loro due le due iridi di 324 persone ottenendo una distribuzione del tutto uguale (media, varianza, ecc.) a quella dei confronti fra persone diverse!
- Questo significa che, a parte il colore, gli occhi DX e SX sono diversi tanto quanto quelli di persone diverse per l'Iriscode

### Iride nel visibile e spoofing/antispoofing

#### Iride nel visibile

- Nel visibile non sempre si possono usare flash e sorgenti lum. adeguate → **Luce ambientale**
- Vi sono molte feature sfruttabili anche nel VIS
- Gli occhi scuri nel VIS sono più problematici e offrono meno dettagli utili al riconoscimento.

#### Watch list

- l'iride si presta meglio ad **applicazioni con livelli di sicurezza e dimensioni maggiori**

- In particolare, il bassissimo tasso di FMR (“dire che tu sei un altro”) dei sistemi basati sull’iride rende la **tecnica perfetta per la scansione di enormi DB anche a livello nazionale**
- Attualmente l’iride è l’unico sistema che offre la scansione realtime di una singola iride (pochi secondi) con un DB di milioni di iridi, o di una **watch list centralizzata**

### **Problemi di privacy**

- L’exploit di Daugman (riconoscimento con iride da foto ad alta risoluzione nel visibile a 18 anni di distanza) mostra la possibilità del pericolo di screening di massa dagli archivi di foto (governativi, social...)
- ENORME PROBLEMA DI PRIVACY NEL FUTURO

### **Frodi attuabili sul sistema**

- In realtà esistono moltissimi (non banali) modi di frodare un sistema biometrico:
  1. attaccare i canali di comunicazione del sistema (**replay attacks**) specialmente il canale di comunicazione dal sensore al sistema
  2. **attaccare dei moduli specifici** (sostituire il modulo SW di estrazione di caratteristica o il modulo di matching con un Cavallo di Troia)
  3. **attaccare il DB con tutti i dati di enrollment**
  4. **ingannare il sensore**, di solito presentando una iride finta

### **Attacchi al sensore**

- Una iride falsificata mediante una lente a contatto stampata presenta molte delle caratteristiche di liveness
- Il processo di stampa della lente porta una periodicità nella trama della stampa che si rileva nello spettro di potenza 2D del segnale può essere sfruttato per antispoofing

### **Possibili controlli**

#### *tempi di reazione della pupilla*

- La pupilla **reagisce alle variazioni di luce ambientali**, un occhio finto no
- Inoltre la velocità di contrazione e dilatazione sono diverse ed hanno un andamento prefissato

#### *spettrometria e termografia dell’occhio*

- Usando **illuminatori a frequenze ottiche diverse** è possibile avere in tempo reale una **spettrografia dell’iride**
  - Attraverso dei sistemi di classificazione che analizzano lo spettrogramma dell’iride **si stima il materiale di cui è composta**, questo permette di controllare se è di tipo organico o plastico, se contiene acqua, grassi, pigmenti melaninici ecc. oppure è una pellicola fotografica o carta ecc.
- Anche una **immagine termografica** permette di capire se abbiamo di fronte **tessuti a temperatura corretta!**

### **Generazione sintetica di iridi**

- Sono disponibili tecniche per la generazione sintetica di iridi mediante algoritmi basati su “Markov random fields” iterativi
- Sono tecniche di generazione sintetica di pattern
  - si parte da piccole porzioni di immagine reale (primitive)
  - si crea una matrice casuale
  - le primitive vengono mischiate casualmente agendo su un independent random field in modo iterativo
- Sono disponibili anche tecniche a multistrato che imitano la vera fisiologia dell’iride

- Nuovi sviluppi anche con Convolutional Neural Networks.

## Sistemi basati sul volto

### Introduzione alla biometria del volto

#### Sistemi biometrici basati sul volto

- Impiegati sia per la **verifica della identità**, sia per l'**identificazione**
- Classificazione
  - 2D
    - immagine fissa
    - video o tante immagini fisse
    - colori
    - toni di grigio
  - 3D
    - scansione laser
    - illuminazione controllata

#### Vantaggi

- Ottimo compromesso fra **accettabilità da parte dell'utente** e prestazioni in accuratezza
- **Dispositivi di input facilmente posizionabili** ed adatti a **molti condizioni operative**
- Permette l'**acquisizione non consenziente** (videosorveglianza, ...)

#### Svantaggi

- I sistemi basati sul volto soffrono di **elevata variabilità intraclass**
  - Illuminazione
  - Posa
  - **variazioni dell'aspetto dell'individuo** (dimagrimento, **invecchiamento**, ...)
  - occlusioni (peli, cappelli, occhiali, veli, ...)
- **Possibile ingannare i sensori** non dotati di meccanismi di antispoofing
- Tecnologia matura per i sensori, ma non per gli algoritmi che sono in continua evoluzione

#### Non solo identification/verification

- Molte degli algoritmi che presenteremo non servono solo per produrre sistemi biometrici per identificazione e verifica della identità ma anche per:
  - riconoscimento delle **espressioni facciali**
  - riconoscimento del **movimento delle labbra** (anche per multimodalità e **controllo antispoofing**)
  - applicazione di computer grafica (sintesi e/o animazione)
  - creazione di protesi preintervento
- Quindi uso non solo biometrics ma anche biometry

#### Fasi principali

1. face detection
2. face segmentation
3. face tracking
4. face normalization
5. feature extraction

## 6. matching

### Similitudine interclasse per il volto

- Similitudine fra volti:
  - Gemelli
  - fratelli, genitori (enroll distanti nel tempo)
  - sosia

### Standard per il template

- Tutti i venditori di sistemi biometrici hanno il loro algoritmo per la creazione del template, spesso segreto e/o sotto brevetto
- **Non è possibile interoperabilità fra i sistemi** (caso opposto di quello delle impronte digitali nel caso delle minuzie) **a meno che** due stati **si passino le foto originali e non i template**
- L'ICAO impone da molti anni regole sul formato delle foto per i Machine Readable Travel Document (MRTD) fra cui proprio gli ePassport
  - Per immagini facciali lo standard è una **fotografia a colori scannerizzata a 300 dpi con almeno 90 pixel fra gli occhi ed una dimensione approssimativa di 643 kB**
  - **La dimensione può essere ridotta a 112kB con una minima compressione**

### Compressione per le immagini facciali

- Il sistema di **compressione** delle immagini facciali usato sono gli **standard JPEG e JPEG2000**
- **Con questi algoritmi** si riesce ad avere lo **standard di risoluzione** dimensione richiesto dalla ICAO **con 12kB**
  - Sotto queste dimensioni di memoria l'immagine è troppo degradata per essere usata con efficacia nel sistema biometrico
- Nei futuri ePassport l'immagine dovrebbe aggirarsi proprio intorno a 15kB-20kB
- Riassumendo:
  - Usando la compressione più opportuna si arriva a questi valori per il **sample compresso**
    - **volto per ePassport con JPEG2000: 15kB-20kB**
    - **impronte compresse con WSQ:10kB**
    - **iride compressa:30Kb**

### Passive biometric identification

Normale telecamera da video sorveglianza + Surv. Tool + Face tracking + Identification

### Algoritmi di prefiltraggio ed estrazione di caratteristica

#### Sensori per i volti 2D

- I sensori per la scansione del volto (2D) sono tipicamente basati su CCD
  - fotocamere
  - telecamere
  - webcam
  - scanner per acquisizioni off-line
  - termografi
  - dispositivi multispettrali
- In caso di scarsa illuminazione o illuminazione non uniforme è molto **meglio utilizzare telecamere nel vicino infrarosso (NIR)**

#### Face detection

- Primo passo della catena, occorre rintracciare il volto/i volti da una scena senza nessun prerequisito particolare

- Possono cambiare le condizioni di luce:
  - intensità
  - direzione
  - banda spettrale
- I volti possono avere diversi:
  - colore
  - posizione
  - scala
  - posa
  - espressione

### Approcci alla face detection

- L'obiettivo è quello di individuare il volto/i volti nella scena per arrivare a ricostruire l'immagine sul piano normale a quello di osservazione attraverso operazioni quali
  - **stima dei parametri del volto**
  - **traslazione e correzione della scala**
  - **rotazione**
- Molti approcci sulla localizzazione del volto sono **basati su modelli** molto semplici del volto in termini **geometrici** o di **texture**
- Questi modelli permettono di trovare nelle immagini le regioni che “fittano” meglio il modello e quindi dove è maggiore la probabilità che vi sia un volto

### Face detection – color based

- Nel caso di **immagini a colori** uno degli schemi più diffusi è il seguente:
  - 1. Lighting Compensation**
  - 2. Skin Tone Detection**
    - La skin tone detection viene effettuata controllando **quali bit dell'immagine appartengono ad una regione determinata dello spazio colore che evidenzia meglio le differenze**
    - Vengono messi a 1 i pixel che appartengono solo a una regione dello spazio colore
  - 3. Localization of Facial Features** (occhi, bocca, contorno del viso)
    - La **rilevazione della posizione degli occhi e della bocca** viene effettuata **sottraendo immagini espresse in appositi spazi colore (Y,Cr,Cb)** che ne possano mettere in evidenza le caratteristiche cromatiche peculiari insieme a **filtraggi morfologici**
  - 4. aggregazione dei risultati**

### Face detection – Haar feature

- Il metodo delle feature basate sulle funzioni di Haar consiste nel **cercare nelle immagini delle regioni che presentano particolari valori delle trasformate di Haar**
- Le trasformate di Haar sono **funzioni che prendono il valore di differenze fra i valori di grigio di 2/3 zone** (di area, posizione ed orientamento diverso)
  - Le posizioni dei massimi ed i massimi delle trasformate sono caratteristiche utili per decidere se è presente un volto (differenze colore tra linea con occhi e subito sotto, o linea verticale tra naso e a dx e sx di esso...)
  - Esistono svariate trasformate con diversa forma e orientamento

### Face tracking

- Quando si ha a che fare con un **video** si parla di face tracking
- Non è esattamente come fare del face detection in ogni frame

- **si hanno maggiori informazioni da un filmato** (i volti non possono essersi spostati di molto da un frame all'altro)
- **avendo almeno 2 frame è possibile effettuare una previsione sullo spostamento del volto o sulle sue deformazioni**

## Estrazione di caratteristica e matching

### Estrazione di features

- feature estratte dalla immagine totale
  - Principal Component Analysis (PCA)
  - Indipendent Component Analysis (ICA)
  - Linear Discriminat Analysis (LDA)
  - Support Vector Machines (SVM)
  - Kernel Methods (KM)
  - Trace traform (TF)
  - PCANET, CNN
- feature estratte dalla regione dell'immagine
  - Local Feature Analysis (LFA)
  - Gabor Wavelet

### Metriche per il matching

- distanze euclidee
- reti neurali (anche Deeplearn)
- Elastic Bunch Graph Matching (EBGM)
- template matching

### Analisi lineare di un sottospazio delle facce

- Lo spazio delle facce costruito con **immagini row** ( $pxq$ ) ha una **dimensionalità troppo elevata**
- Le facce possono risiedere in uno sottospazio limitato. Il modo di stabilire il sottospazio crea il metodo di analisi
- $X_{PCA} = W^T X$  **Trovare una trasformazione lineare  $W$  che mappa il vettore di immagini  $X$  in  $R^n$  in un sottospazio di dimensione  $l$  molto più limitata ( $l < n$ )**
- Il matching avverrà sulle feature  $X_{PCA}$  e non sulle immagini  $X$

### Analisi lineare di un sottospazio mediante PCA

- Problema: come possiamo **ridurre le dimensioni dello spazio** e nello stesso tempo **“separare meglio” i punti?**
- Prima soluzione possibile: la tecnica **Principal Component Analysis**
- La PCA per prima cosa **cerca una rotazione dello spazio** (ancora la dimensionalità non cambia) **che permette di separare meglio le classi**. In altre parole **la PCA cerca una rototraslazione che permette di “mettere” la variabilità dei dati tutta nei primi parametri**
- Notare come variano le distribuzioni degli stessi punti sugli assi  $X = (x_1, x_2)$  e  $X_{PCA} = (X_{PCA,1}, X_{PCA,2})$

### La PCA è molto utile!

- La PCA è una tecnica utilissima in molti contesti anche biometrici
  - In generale **serve a ridurre lo spazio dei dati ingresso senza bisogno di sapere la label dei dati (come nella classificazione)**
  - Permette partendo **da molti dati anche molto diversi fra loro di ottenere un numero minore di nuove variabili molto descrittive**
  - Si usa per esempio in data visualization per scendere a 2D e 3D partendo da dati ND

- Si usa con le reti neurali e modelli di Machine Learning in ingresso (regolarizzazione / normalizzazione) e al loro interno per ridurre lo spazio delle feature

### Vantaggi e svantaggi della PCA

- Vantaggi
  - decorrela massimamente qualunque insieme di punti nello spazio di uscita  $X_{PCA}$
  - **compatta la maggior parte della energia (varianza) nel minor numero di coefficienti di trasformazione** (i valori in  $W^T$ )
  - **minimizza l'errore quadratico medio (MSE) tra i dati ricostruiti  $X_{PCA}$  e i dati originali  $X$**
  - **minimizza l'entropia totale dei dati  $X_{PCA}$**
- Svantaggi
  - non ci sono algoritmi veloci per la sua implementazione
  - è un **algoritmo costoso in termini di risorse computazionali per il calcolo degli autovalori, autovettori e delle matrici di covarianza**
  - $W^T$  non è una trasformazione fissata, occorre calcolarla per ogni tipo di “statistica dei dati” (non proprio quindi per ogni nuovo dataset)

### Significato degli autovalori nella PCA

- Le facce contenute nel face space possono essere esaminate in uno spazio a dimensionalità ridotta
- Inizialmente la PCA esegue una rototraslazione in uno spazio con lo stesso numero di dimensioni, ma gli autovettori non hanno la stessa importanza (hanno valore decrescente)
- **Se usiamo solo nella ricostruzione i primi M riusciamo probabilmente a classificare ancora le facce mediante la loro distanza**
- **Più è grande il valore dell'autovettore, maggiore è la sua importanza nella ricostruzione dei dati** nello spazio delle feature della PCA ( $X_{PCA}$ )

### Significato delle Autofacce

- Verification. Ogni volto del DB può essere ricostruito perfettamente con una combinazione lineare di autofacce. Se un nuovo volto viene ricostruito male, allora: 1) non è un volto 2) è un impostore

### Considerazioni sulle autofacce

- Le autofacce sono una tecnica base, che poi è stata raffinata in molti modi per superare i suoi evidenti svantaggi
  - **non usano l'informazione di classe** (apprendimento non supervisionato), e lavorano solo sulla distribuzione dei punti nello spazio delle facce, indipendentemente se appartengono alla stessa persona oppure no
  - **soffrono delle variazioni di**
    - illuminazione
    - posa della testa
    - allineamento
    - espressioni facciali
- **Una tecnica basata sulle autofacce e che tiene conto dell'informazione delle classi è la Linear Discriminant Analysis**

### Altri metodi di estrazione delle feature e matching

- I metodi di analisi locale lavorano invece sul **riconoscimento, misurazione e confronto dei dettagli** del volto:

- **misure del naso, bocca, distanza occhi**, ecc.
- **valori ritornati da particolari funzioni di trasformazione** (local Gabor Wavelet, Haar Wavelet, ...)
- I metodi chiamati “**model based**” estraggono non una feature singola, ma **adattano un modello sulla faccia, ne trovano i coefficienti e vanno a confrontarli con quelli delle facce usate in enrollment**

### Graph matching

- Nei metodi di **Graph matching** il **volto è rappresentato come una rete di nodi** (feature vectors) sui punti peculiari del volto
- Servono **almeno 2 immagini per trovare il modello del volto** (grafo)
- I **features vectors si trovano usando la risposta nell'immagine di 2D Gabor wavelet** con diverso orientamento e scala
- La **comparazione di due facce è eseguita misurando quanto “sforzo” è necessario fare per adattare un grafo all'altro “tirando” i nodi** che però sono legati da un modello **elastico**

### Spoofing e anti-spoofing

#### Alcuni limiti oggettivi e tipi di attacchi

- Il volto può essere coperto da peli o indumenti (in enrollment o verification)
  - non accettare acquisizioni se la percentuale coperta supera quella necessaria per garantire l'accuratezza certificata del sistema
- Una maschera di pelle artificiale (utile anche per il 3D)
  - tecniche termografiche o spettrometriche basate su illuminazione a diverse lunghezze d'onda per rilevare la pelle
- Una immagine di un volto stampata o proiettata con uno schermo
  - controllo tridimensionalità
  - controllo sincronia tratti biometrici indipendenti (esempio variazioni volto e voce durante il parlato)
- Un filmato di un volto proiettato con audio
  - controllo tridimensionalità
- In tutti i casi (stampa o monitor):
  - è possibile la rilevazione della matrice di stampa o pixel mediante l'analisi della trasformata di fourier (presentato nelle lezioni precedenti)
  - usare tecniche termografiche o spettrometriche basate su illuminazione a diverse lunghezze d'onda per controllare la presenza della pelle

#### Un esempio di attacco: **Hill Climbing**

- Problema generale:
  - “E’ possibile ricreare un sample da dei template memorizzati in un sistema?”
- Risposta:
  - “SI! Basta avere **accesso al match score**”
- Si usa la tecnica di “Hill climbing”
  - si inizia con un **sample del tutto casuale**
  - si **portano delle piccole modifiche che incrementino il match score**
  - si **prosegue finché si riesce ad aumentare il match score**

#### Contromisure (non efficaci) alla tecnica Hill Climbing

- “...allowing only discrete increments of score to be returned to the application eliminates this method of attack” Quindi **usando quantizzazione per il match score ritornato** (quantizzandolo)

- l'idea di base è che molte modifiche all'immagine non produrrebbero cambiamenti del match score, quindi l'algoritmo "non saprebbe come arrampicarsi sulla collina"
- RISULTATO: le tecniche di "**modified hill climbing**" funzionano lo stesso!

### Controllo della sincronia parlato – movimenti labbra

- Il sistema chiede all'utente di fronte al sensore di pronunciare una frase (casuale) richiesta dal sistema
- Il sistema misura la variazione dei movimenti delle labbra nel tempo controllando se si sta cercando di ingannare il sistema con un fantoccio/maschera rigida/immagine proiettata nel sensore

### Facial fingerprinting (Infrared identification)

- Si iniziano a sviluppare progetti per sensori e tecnologie per il facial fingerprinting (non near IR)
- La **mappa di vene e capillari al di sotto del volto** può essere rilevata da **telecamere ad infrarosso** ad alta risoluzione, diventando un **nuovo tipo di tratto biometrico**
  - assolutamente unico
  - difficilmente falsificabile
  - non intrusivo
  - assolutamente accurato
- Può funzionare come mappa 2D, ma sarà possibile arrivare alla mappa 3D dei capillari

### Attacco con immagini

- **controllo istogrammi colore**
  - Il controllo avviene controllando la distribuzione dei colori negli istogrammi
- controllo di pattern – effetto moirè
  - Avvengono dei **particolari «battimenti» di colore quando con una camera si inquadrano stampe o display**
  - Si possono vedere **direttamente nella immagine** inquadrata o nella **trasformata di Fourier** della immagine stessa
  - **Picchi ripetuti nello spettro** = pattern di moirè → prob. Fake!

### Near Infrared Antispoofing

- La visione **near IR** offre un punto di vista diverso e più robusto rispetto alle condizioni ambientali
- I **display o le superfici stampate** in VISIBILE diventano non usabili per attacchi con camere Near IR
- Un ulteriore layer: VIS + IR + analisi 3D
  - Dispositivi in grado di scansionare il volume con dati 3D degli oggetti (Kinect, RealSense, ecc.) possono migliorare le capacità antispoofing

## Sistemi basati sul volto 3D

### Sensori e caratteristiche del tratto in 3D

#### Acquisizione 3D mediante scanner laser

- Acquisizione 3D mediante scanner laser
- Attraverso la geometria spaziale (nota) del sistema si ricostruisce la superficie dalle "fettine" presenti in ogni frame del filmato
- Occhi chiusi !!

#### Acquisizione 3D mediante luce strutturata

- Si illumina il volto da riprendere con proiettore in grado di produrre un fascio di luce strutturata ed una/due telecamera/e
- Con i sistemi "coded light" si proiettano in successione temporale tanti pattern binari con bande sempre più fini

- Il sistema ricostruisce la tridimensionalità usando la deformazione delle bande nell'immagine

### Acquisizione 3D mediante diverse viste

- I sistemi chiamati **2,5D** riescono a riprodurre la superficie 3D del volto da tante immagini del volto prese da angoli diversi usando una normale telecamera
- Con un passaggio successivo, altri sistemi riescono a ricostruire un **vero modello 3D** del volto partendo dalle immagini 2,5D
  - bastano 5 buone immagini iniziali
  - riescono a rimuovere il rumore e riempire i buchi
  - riescono a ridurre il numero di poligoni ad un valore richiesto
- **ATTENZIONE:** esistono i “**face modeler**” che appiccicano la faccia 2D su un modello a priori 3D standard uguale per tutti
- **Non acquistare un face modeler** di questo tipo per **fare biometria** (ecco perché costano poco!)

### Vantaggi e svantaggi dei sistemi 3D

- VANTAGGI DEL 3D
  - **invarianza alla luce ambiente** (usano luce IR propria)
  - sono **maggiormente tolleranti** rispetto ai **colori di sfondo, il trucco del viso, gli accessori** ecc.
  - **invarianti rispetto a piccoli spostamenti angolari** del volto (anche fino a 30 gradi)
  - la precisione di alcuni sistemi permette di distinguere due gemelli omozigoti
  - **capacità realtime** (acquisizioni, elaborazione e matching **fino a 12 volte per secondo**)
  - **bassi valori di False Rejection Rates (FRR)**, anche se il **False Acceptance Rate (FAR)** è molto basso (es: .0001)
- SVANTAGGI DEL 3D
  - **costo dei sensori** e dei sistemi molto maggiore
  - **Il soggetto** deve essere **collaborativo**

### Confronto sensori 2D e 3D

- I sistemi 3D pur non garantendo una completa invarianza rispetto alle variazioni del volto presentano una situazione migliore
- Nessun sistema basato sul volto assicura una completa invarianza rispetto a questi fattori

### Algoritmi di matching 3D - Accuratezza sistemi 2D e 3D

#### Confronto fra 2 template 3D

- Il confronto fra due volti con tecniche 3D passa per i seguenti passaggi classici
  - se il volto 3D non è direttamente acquisito dal sensore, allora da multiple stills si ottiene la rappresentazione 3D dei volti da confrontare
  - i volti vengono sovrapposti (es. rototraslazioni) fino a trovare la migliore sovrapposizione delle superficie
  - si valuta il grado di sovrapposizione con una soglia
- Il match prevede l'individuazione di 3 punti di riferimento nelle immagini per facilitare la corretta sovrapposizione ed eventualmente anche un passaggio di “fine alignment”

#### Face Recognition Vendor Test

- Sistema yitu-000 arrivando a FNMR =0.033 @FMR=1E-06
- Sistema 3divi-001 arrivando a FTE (Failure To Enroll) = 0.0007 = 1/1428 foto di documenti

#### Esempio di sistemi commerciali (con sensore 3D)

- Windows Hello face authentication **FAR=0.001%@ 5%FRR**

## Confronto con umani

- Si è creato il seguente insieme di confronti (Stimuli): 240 coppie di facce, 120 maschi e 120 femmine, 50% facce "facili" e 50% facce "difficili"
  - 3 algoritmi sono stati capaci di fare meglio dei supervisori umani nel dataset "difficile"
  - Tutti (tranne uno in una regione di funzionamento della curva ROC) fanno meglio dell'uomo su dataset "facili"

## Critiche verso il Face Recognition (FR)

- Gli **errori** (FNMR@FMR, CMC, classificazione dei tratti di soft computing) sono tuttavia **ancora abbastanza alti da creare un effetto di protezione da «errore del sistema» su schedature a scala metropolitana** e nazionali nel FR... ....tuttavia meglio iniziare a preparare la consapevolezza e le legislazione..

## Spoofing e anti-spoofing per il volto 3D

### Controllo del volto 3D usando un sistema 2D

- Partendo dal sensore più semplice ovvero la **camera visibile 2D** → è possibile eseguire **shape from motion**
- Es: ZoOm (Facetech) → avvicinare il telefono
- 3D FaceMap: Con 1 video da 2s sono possibili 3 risultati:
  - Verifica Liveness
  - 3D della superficie
  - Riconoscimento 3D volto

### Tipi di attacchi di spoofing

- 2D paper photos & digital images
- High resolution videos
- Image swap-in after liveness check
- Paper masks with eye & mouth cutouts
- Hollywood masks, wax figures & lifelike dolls
- Photos or video frames animated into avatars
- Video projections on 3D heads
- **Sleeping users with closed eyes**
- Impostors, lookalikes & doppelgangers”

### Tecniche di antispoofing

- **Epidermide e volto simulati**
  - Nel campo delle protesi e dei materiali sintetici che emulano il corpo umano sono stati fatti grandi passi avanti: 3D Printed Latex Masks
- **Spoofing IR + Visibile → Apple Face ID**
  - 2D infrared images mounted on 3D mask made of stone powder
- **Spettrometria e termografia del volto**
  - **Usando illuminatori a frequenze ottiche diverse** è possibile avere in tempo reale (parziale) analisi spettrografica del volto
    - Attraverso dei **sistemi di classificazione che analizzano i dati spettrografici** si stima il **materiale** di cui è composto
      - tipo organico, se contiene acqua, grassi, ecc.
      - o **plastico**, pigmenti, gomma, silicone, ecc.
  - Anche una immagine termografica permette di capire se abbiamo di fronte tessuti a temperatura corretta!

- Il costo dei sensori termografici sta rapidamente scendendo nel tempo
- **Battito delle palpebre tramite analisi del flusso ottico**
  - Avendo un sensore con elevati FPS (>30) e risoluzione è possibile verificare
    - 1) **Assenza di pattern da effetto Moirè** → non abbiamo un video
    - 2) **Movimento delle palpebre** compatibile per direzione ed entità a quello naturale
  - Un **attacco con maschera** con ritagli per mostrare gli occhi vivi viene **identificato da «salti» del flusso ottico causate della discontinuità dei fori fra le parti mobili (occhi) e fisse (maschera)**
  - Anche i **bordi di uno schermo** usato per un attacco **mostrano «salti» di flusso ottico usabili per anti-spoofing**

## Biometria a contatto

### Mano e palmo

#### Introduzione

- Tratto biometrico **molto ben accettato dagli utenti** perché poco invasivo
- Presente dal 1979 sul mercato (**tecnologia matura**)
- Offre un **discreto livello di accuratezza** senza dover chiedere all'utente sample molto critici per la privacy come l'iride o l'impronta
- Offre la **possibilità di funzionare in modo multimodale** controllando più aspetti come immagini, misure, pattern delle vene ecc.

#### Applicazioni

- L'utente deve essere **collaborativo**
- I sistemi possono anche essere centralizzati coprendo di fatto gli accessi anche a grandi aree (aeroporti, basi militari, laboratori...)
- Sono sistemi **veloci**, adatti principalmente per il **controllo degli accessi**
- Sono sistemi impiegati anche per le applicazioni del tipo **“time and attendance”** cioè per il **controllo delle presenze sui luoghi di lavoro**
- «Preferita» dal nostro **Garante della privacy**

#### Vantaggi e svantaggi

- Vantaggi
  - Tecnologia consolidata
  - Sensore robusto
  - **Dimensioni del template molto ridotte**
  - Minore impatto sulla privacy degli utenti
- Svantaggi
  - Costo (circa 1000 euro)
  - Dimensione e peso notevoli
  - Sensibilità a forte luce diurna

#### Sensori

- Di solito si lavora su tre viste:
  - Palmare
  - Laterale
  - Dorsale
- Tipi di sensori
  - Scanner (anche <180dpi)

- CCD camera (media risoluzione)
  - Visibile
  - IR e termografi (usata anche per Analisi immagine termica per **controllo "liveness"** e **misurazione delle vene**)

### Pegs or Pegs-free

- In commercio esistono dispositivi con dei pioli per il corretto posizionamento delle mani ed altri senza
- **Con i pioli** il sistema diventa **più accurato** perché **si riduce la variabilità intraclass del sample** essendo forzato ad essere posizionato nella giusta posizione
- Con i pioli però l'utente deve imparare il corretto posizionamento della mano

### Alcuni tipi delle circa 90 features estraibili

- **Misura delle lunghezze** degli elementi
- **Confronto delle immagini delle parti** con tecniche simili a autofacce (ritaglio solo parti come dita e palmo)
- **Immagine termica** per la rilevazione del **pattern delle vene**
- Studio delle **linee della pelle**

### Passi per il matching

1. **Peg removal**
  - conoscendo la posizione fissa dei pioli è facile sottrarli alle immagini per avere a disposizione solo la mano
2. **Estrazione dei contorni**
  - si usa un **algoritmo a soglia adattativa** per segmentare l'immagine e trovare il contorno esterno della mano
3. **Estrazione delle dita ed allineamento:**
  - **le 5 dita vengono estratte dal profilo ed allineate separatamente** a partire da posizioni standard. Questo rende il matching maggiormente veloce
4. **Matching:**
  - **le curve delle due mani da confrontare già allineate** sul riferimento vengono **trasformate in gruppi di punti**
  - il matching lavora **individuando coppie di punti e misurando la loro distanza**. La loro **distanza media** è chiamata **Mean Alignment Error (MAE)**
  - se il **MAE è minore di una soglia** prefissata l'utente è considerato **un genuino** altrimenti come un impostore

### Eigenfingers

- In un modo assolutamente simile al metodo della autofacce da un database di immagini di mani (scanner) è possibile ricostruire le dita ed il palmo mediante Eigenfinger

### Standard e accuratezza dei sistemi

- Un test governativo riporta un EER di circa il 3%, in altre valutazioni più recenti si parla di
  - **FTE = 2%** (Failure to Enroll)
  - **FNMR=1,5%** corrispondente ad un **FMR=1,5%**

## Firma, Retina, Voce

### Biometria della firma

#### Riconoscimento della firma

- Ragionevolmente unica non solo dal punto di vista ma anche per una serie di caratteristiche

- Velocità di scrittura
  - Punti nei quali si esercita più pressione
  - Angolo d'inclinazione della penna,
  - Accelerazione del movimento;
  - Numero di volte che la penna viene sollevata dalla carta.
- Maggiore applicazione negli ambienti bancari e finanziari
  - **Firma off-line:** Tipicamente apposta su un documento cartaceo poi scansionato
  - **Firma online:** l'utente appone la propria firma con una penna speciale o **su una tavolletta elettronica in grado di rivelare i parametri descritti** che portano alla creazione di un template le cui dimensioni sono intorno ai **1500 byte** (online).

### **Firma online**

- Tracciati dei parametri nel tempo che sono comparati in sede di matching
  - Distanze relative spazio-temporali dei punti singolari
- Punti singolari dei tracciati
  - Inversioni di moto
  - Cuspidi delle curve
  - Intersezioni delle linee
- Tecniche di confronto
  - Distanze euclidee
  - Hidden Markov Model
  - Correlazione di segnale
  - Classificatori bayesiani
  - Reti neurali

### **Firma offline**

- Solo a disposizione l'immagine della firma come sample iniziale
  - Dimensione del **template offline** può raggiungere **1MB** se il template è la firma scansionata, diversamente può ridursi.
- Tecniche di confronto:
  - Studio degli istogrammi delle proiezioni orizzontali e verticali dei toni di grigio
  - Dislocazione dei tratti all'interno dell'area della firma secondo il metodo "**Extended shadow code**". Questa tecnica permette di codificare la firma in un codice sovrapponendo una serie di matrici di segmenti sulla firma e andando a verificare le intersezioni della firma con i segmenti della maschera.

### **Pro e contro**

- Punti di forza:
  - Hardware poco costoso
  - Buona accettabilità da parte degli utenti
  - Difficilmente falsificabile (nel caso della firma online)
- Punti di debolezza:
  - Instabilità temporale del campione (elevata variabilità **intraclasse**, stessa persona)
  - Dimensioni del template (**1,5MB**)
  - Numero limitato di applicazioni adatte
  - Si hanno problemi per firme molto brevi o troppo semplici (elevata similitudine **interclasse**, tra persone diverse)

## Applicazioni

- **Banche e transazioni finanziarie:** per esempio i requisiti della Association for Payment Clearing Services (APACS) richiedono un **FRR uguale a al 0.001%** ed un **FAR pari al 5%**.
  - Ad oggi non si hanno sistemi commerciali che garantiscono questi requisiti. In ogni caso esistono delle banche che usano questi sistemi per aiutare l'operatore e vengono usati come avvertimento o “**second reading**” ossia un secondo parere che si affianca a quello che esprime l'operatore.

## Biometria della retina

### Riconoscimento della retina

- Pattern dei vasi presenti sulla retina
  - La tessitura delle vene della retina è **già completa al momento della nascita e rimane quasi completamente stabile per tutta la durata della vita**
- La distribuzione sulla retina dei vasi è principalmente **casuale e assolutamente univoca**
  - Il pattern di vene parte dal nervo ottico, ma le successive diramazioni sono pressoché casuali

### Acquisizione ed estrazione di caratteristiche

- Sensore deve essere posizionato a breve distanza dall'occhio per avere una corretta acquisizione del tratto
- Con metodi molto simili a quelli delle impronte digitali vengono **ricercate le minutiae della retina e memorizzate in un template**.
- In alcune versioni commerciali, il pattern delle vene viene convertito in un codice a barre circolare

### Pro e contro

- Punti di forza:
  - Molto efficiente
  - Stabile
  - Difficile da contraffare
  - Difficilmente alterabili da parte di fattori esterni
- Svantaggi:
  - Difficilmente applicabili in applicazioni commerciali
  - Viene rilevato dagli utenti come intrusivo
  - Sentito come pericoloso per la vista
  - Elevato costo dei sensori

### Retica

- Individua il centro del nervo ottico ed esegue delle **scansioni dei toni di grigio lungo circonferenze concentriche**
- Attraverso una comparazione a soglia adattativa è possibile **convertire questo andamento in un insieme di bit** (1 se l'intensità è sopra la soglia, 0 altrimenti)

## Biometria della VOCE

### Voice Recognition

- **Speech Recognition:** Recognition of what is spoken (texts, phrases, numbers, etc.)
- **Speaker Recognition:** Recognition of the identity of the person who is speaking

### Sistemi basati sul riconoscimento vocale

- Irido tra **biometria fisiologica e comportamentale**

- Conformazione della gola e della laringe
  - Tono umorale
- Accesso fisico e logico
- Attività investigative
  - Senza cooperazione
- Fino ad oggi il riconoscimento vocale avviene in 3 modalità
  - Auditivo (un esperto ascolta due tracce vocali e le identifica)
  - Semiautomatico (un esperto controlla feature estratte dalla voce di due persone, ad esempio spettrogrammi, forme d'onda ecc.)
  - **Riconoscimento completamente automatico**

### **Speaker Rec.: Acquisizione della voce**

- **Microfono**
- **Telefono:** Aumenta la fruibilità della tecnologia ma rende il processo biometrico molto più complesso a causa della drastica riduzione di informazioni dovuta alla **limitata banda destinata alla voce su linea telefonica**
- **Cooperativa**
  - Registrazione da parte dell'utente di una **frase predefinita** (ad esempio una sequenza di numeri) per un certo numero di volte
  - **Text dependent** (è noto il parlato, oppure **tutti gli individui che hanno fatto l'enrollment hanno detto una frase uguale**)
  - **Text indipendent** (**non si conosce nulla** del parlato): **30s -1m** per avere una accurata identificazione
- **Non cooperativa:** La identificazione avviene in modo «covert» senza informare o che ne sia a conoscenza l'interessato

### **Caratteristiche generali della voce**

- Diverse caratteristiche si possono estrarre dalla voce: da quelle linguistiche fino a quelle acustiche sonore di basso livello
  - **Alto livello:**
    - **Caratteristiche lessicali e sintattiche** come la co-occidenza delle parole o dei fonemi
  - **Livello intermedio:**
    - **Qualità della voce**
  - **Basso livello:**
    - **Energia del suono nelle varie bande spettrali**

### **Estrazione e confronto delle caratteristiche**

- Passi principali effettuati per lo Speaker Rec.:
  - **Prefiltraggio**
    - **Pre-enfasi** (si **evidenziano le frequenze alte** dello spettro che sono naturalmente attenuate dall'apparato di fonazione)
    - **Windowing** (**operazioni sulla finestra di analisi per permettere agli algoritmi DFT** che realizzano la **trasformata discreta di Fourier del segnale di lavorare correttamente** senza introdurre artefatti dovuto al fatto che il segnale vocale non è periodico)
  - **Elaborazione delle feature statiche** (ad esempio MFCC) **e dinamiche** (le variazioni che avvengono fra i quanti di tempo elementari della analisi)
  - **Modellazione del parlatore**

- o Comparazione dei modelli e decisione

#### **Speaker Rec.: Pro e contro**

- Punti di forza
  - o Tecnologia basata su un **hardware di larga diffusione**
  - o **Buona accettabilità** da parte degli utenti
- Punti di debolezza
  - o Possibilità **Lunghi tempi di enrollment**
  - o **Elevate dimensioni del template (circa 1MB)**
  - o **Sensibilità a rumori di fondo**
  - o **Variabilità intraclass** dovuta a malattie o condizioni ambientali
  - o **Facilità di falsificazione** del tratto

#### **Signal Requirements**

- The front end frequency response must be flat within +/-4 dB over the range of **100 Hz to 8 kHz**
- minimum sampling rate recommended for digitized speech is **11025 Hz**
- **Resolution > 16-bit** (for optimum recognition accuracy)
- Signal to noise ratio (SNR) :
  - o **median SNR is approximately 18-20 dB**
  - o no more than 10% of samples have SNR<15dB.

#### **Speaker Rec.: Feature Extraction**

- Most common feature extraction techniques:
  - o MFCC (Mel-frequency cepstral coefficients)
    - MFCC features : around 99% accuracy
    - MFCC features are proven to be one of the best performing features for voice recognition
  - o PLP (Perceptual linear prediction)
  - o RASTA-PLP (Relative Spectral Transform-PLP)
    - RASTA-PLP: 94-95% accuracy
  - o Wavelet based features
  - o Neural network based features

#### **Speech Recognition Performance**

- Accuracy of speech recognition: word error rate (WER)
  - o Accuracy (%) =  $1 - WER = (S+D+I)/N$ 
    - L'accuratezza è il numero di parole capite bene sul numero delle parole dette

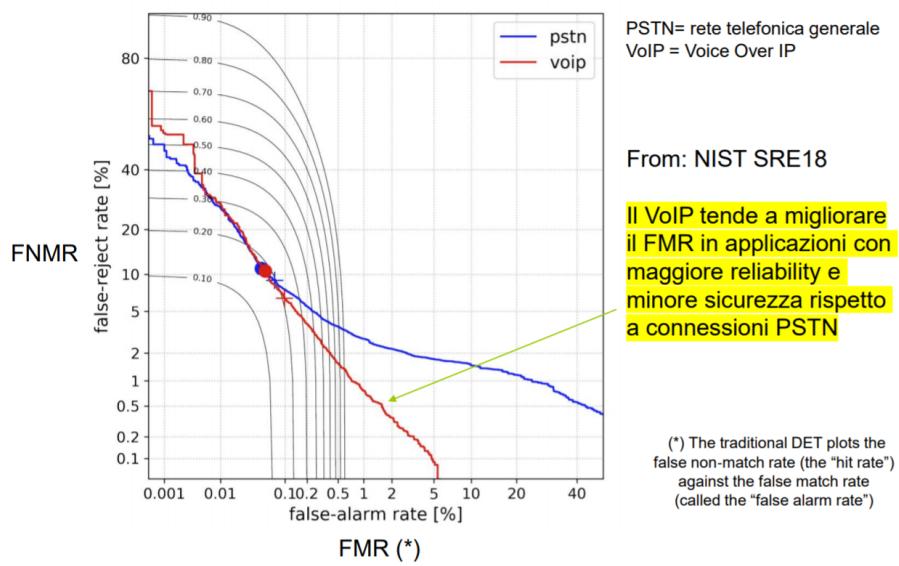
#### **Speaker Identification**

- Rank(N) accuracy (CMC)
  - o Ranking Error is a metric related to Identification Problem (1:n).
  - o Given a query template the goal is to find the genuine similar template in a stored database of templates from n individuals.
  - o Generally that goal is solved by comparing the query template with all the stored templates and select the comparisons with highest similarity value as candidates to be the target of searching.
  - o **Rank(N) is sometimes called Cumulative Match Characteristic (CMC) curve.**
- DEFINITION of Rank(N): the ratio of query templates for which genuine comparisons are among the n comparisons with highest similarity value in database.

- PROCEDIMENTO:
  - Prendo 1 template
  - Faccio N comparazioni
  - Prendo n score più simili
  - Vi è un genuino? Si=1; No=0
  - Rifaccio con gli altri utenti e medio il tutto ottengo → Rank(n)
- IDEAL SYSTEM: highest values be always assigned to genuine comparisons. Ranking is the metric that measures the error rate of select impostors templates as most similar.
- The three most used are:
  - Rank(1) [identification]
  - Rank(10) ...
  - Rank(50) [screening]

### Esempio di curva DET per la voce

### Esempio di curva DET per la voce



- Il VoIP tende a migliorare il FMR in applicazioni con maggiore reliability e minore sicurezza rispetto a connessioni PSTN

### Effetto dei secondi di enrollment sulla curva DET per la voce

- Oltre i 30s non migliora più

## DNA Orecchio Autovalutazione

### DNA - Uso nella biometria

#### Introduzione alla biometria del DNA

- Le caratteristiche dei sistemi di riconoscimento degli individui basati sul DNA pongono questa metodologia come la più accurata nel panorama biometrico
- Trova applicazioni
  - di tipo prettamente biometrico
  - scienze mediche
  - scienze ambientali
  - ricerche storiche
  - scienze forensi

- In questa lezione vediamo come il DNA possa essere usato come tecnica biometrica e con quali **precauzioni** debba essere usato
  - per **garantire l'attendibilità** del risultato
  - per **evitare usi impropri delle informazioni** contenute nel sample
- Per quanto le tecniche basate sul DNA vengano usate in tutto il mondo nei tribunali per condannare persone in base alle evidenze genetiche delle tracce ritrovate sulle scene del crimine, ad oggi **non esiste un metodo di stima statistica per valutare quanto è affidabile l'associazione** fra i campioni
  - il livello di certezza è considerato da tutti gli esperti come assolutamente elevato, ma non vi sono ancora metodi statistici standard per valutare la rarità/diffusione in un profilo genetico e quindi la certezza di attribuzione
  - Viene controllata che vi sia una “profile rarity” > 1/10M (a parte i gemelli omozigoti)
- La **produzione di sensori allo stato solido** per analisi del DNA basate sulla tecnica dei microarray e la loro crescente diffusione **fa prevedere in un futuro prossimo una diffusione dei sistemi biometrici basati sul DNA sempre maggiore** ed in nuovi campi, prima governativi e poi commerciali
- E’ una tecnica relativamente giovane, le impronte si usano dal 1900, **il DNA come identificativo biometrico è stato usato per la prima volta intorno al 1984**
  - Jeffreys et al. crearono la tecnica Restriction Frangement Polymorphism (RFLP) che gli permise di vedere il genoma come “DNA fingerprint”
  - I termini correntemente in uso sono
    - DNA typing
    - DNA profiling
  - Nel 1986 Mullis arrivò alla tecnica della **Polymerase Chain Reaction (PCR)**, una tecnica ora facilmente automatizzabile che **permette di “amplificare” la porzione di DNA del campione** fino ad arrivare ad un comodo template di comparazione fra DNA (Premio Nobel per la PCR nel 1993)
- Polymerase Chain Reaction (PCR): **Ogni ciclo il sistema raddoppia la copia dei frammenti.** → È critica la **quantizzazione del campione iniziale perché sbagliare il numero di cicli crea un errore molto grande** sulla quantità finale di DNA

## Vantaggi e svantaggi del DNA

- Vantaggi
  - è la tecnica più accurata a disposizione
  - al contrario degli altri tratti biometrici (impronte, iride, mano, voce, ecc.) con il DNA bastano poche cellule
  - a differenza di tutti gli altri tratti biometrici, con il DNA è possibile scoprire una associazione anche fra sample di consanguinei
- Svantaggi
  - analisi non in real-time, servono alcuni minuti/ore
  - non è ancora completamente automatizzata
  - analisi costosa (da 200 dollari fino a 2000 dollari nel caso di analisi forensi)

## Cosa è il DNA?

- Acido desossiribonucleico -> coppie di basi tenute insieme dal legame molecolare tra di loro
- La doppia elica è la forma naturale per il DNA che si trova di solito nel nucleo delle cellule dell'uomo
- Il DNA è un polimero, ovvero una lunga molecola di unità base ripetute
- Le unità ripetute sono chiamte nucleotidi e possono essere solo di 4 tipi
  - Adenine (A)
  - Cytosine (C)
  - Guanine (G)

- Thymine (T)

## Gene

- I **geni** corrispondono a **porzioni di genoma localizzate in precise posizioni all'interno della sequenza di DNA** e contengono le informazioni necessarie per codificare molecole funzionali (RNA o proteine).

## Replicazione del DNA

- Il processo naturale di duplicazione cellulare (e quindi anche del DNA) si chiama mitosi
- Nei cromosomi vi sono circa 100000 geni appaiati
- **Ogni gene ha fino a 100 versioni diversi chiamati alleli**, anche se per la maggior parte delle persone sono sempre gli stessi

## Che feature si estraggono dal DNA

- In alcune **regioni del DNA (loci)** vi sono dei **pattern di basi ripetuti**, ma ripetuti un numero di volte diverso in ogni individuo. Questo tipo di DNA è chiamato **DNA satellite**.
- Le ripetizioni sono chiamate «**sequenze tandem**»
- La vera **feature biometrica** quindi è il **numero di ripetizioni in un locus**
- Con queste feature **non è possibile scoprire malattie genetiche** ecc.. Non è come avere tutte le informazioni di tutti i geni!

## Satelliti e STR

- Le **porzioni di DNA con ripetizioni chiamate satelliti** si dividono in
  - **Macro satelliti (>100bp)**
  - **Mini satelliti (10-100bp)**:
    - Chiamati anche Variable Tandem Repeat (VNTR)
  - **Micro satelliti (1-9bp)** <- biometria attuale DNA
    - Chiamati anche Short Tandem Repeat (STR)

## Allele

- **una delle forme alternative che un gene può assumere nel medesimo locus cromosomico**; spesso l'effetto di uno dei due alleli (detto *dominante*) è prevalente ai fini dell'espressione del carattere, rispetto a quello dell'altro allele (detto recessivo).

## Quali dati mettiamo nel template

- Il famoso Combined DNA Index System (**CODIS**) FBI database usa per il suo template:
  - 13 soli loci in tutti i cromosomi (dal 2017 sono 20 loci)
  - **conteggia gli STR**
- Al 2020 il Codis (USA) contiene i dati di oltre 14 milioni di individui

## Passi principali

- Collection (es. tampone)
- Specimen Storage
- Extraction
- Quantitation - La fase di quantizzazione è fondamentale:
  - troppo poco DNA significa perdere degli alleli
  - troppo DNA provoca malfunzionamenti nei kit
- Multiplex PCR
- STR Typing
- Interpretation of Results

- Database (Storage & Searching)
- Calculation of Match Probability
  - probabilità di aver avuto delle Short Tandem Repeat con lo stesso numero del coding

### Principio base

- Il DNA è un polimero carico elettrostaticamente quindi viene attirato dai campi elettrici
- Si possono separare dei segmenti di DNA in base alla loro lunghezza mettendoli in un gel posto in un campo elettrico (**elettroforesi**)
- Ogni segmento di DNA ha lunghezza diversa e carica si muove a velocità diverse nel agarose-gel

### Lettura del gel tramite laser

- Sample preparation
- Sample injection
- Sample preparation
- Size separation
  - Colpito con Argon ion LASER (488nm)
  - Fluoresenza passa per un ABI Prism spectograph che causa Color Separation
- Sample Detection (sul CCD Panel (with virtual filters))
- Sample Interpretation

### Genotipizzazione

- Dai tracciati che arrivano i software per la genotipizzazione e l'esperto producono e controllano tutti i dati per il template da confrontare e/o memorizzare

### Valori estratti

- PROBLEMA:
  - esistono moltissimi problemi sperimentali che possono provocare dei **falsi picchi di alleli o farli scomparire!!!**  
Anche in questo caso si parla di ARTEFATTI
  - Da questo punto di vista **anche il DNA può sbagliare!!**

### Omozigoti e identificazione

- Durante lo sviluppo possono intervenire mutazioni somatiche che vanno a differenziare il DNA (per le femmine anche la inattivazione del cromosoma X).
- Solo **pochi laboratori capaci di analisi molto avanzate trovano** in modo affidabile le **piccolissime differenze del DNA degli omozigoti.**

### Orecchio (Altri sistemi monomodali)

#### Vantaggi e svantaggi

- VANTAGGI
  - Tratto **spesso nascosto**
    - difficile da copiare → privacy compliant
  - **Non si conoscono attacchi** realistici su questo tratto
  - Esposto lateralmente → **usabile quando il volto è laterale** e non funzionano i sistemi classici
  - **Implementabile su molti device**
    - Cellulari
    - Portatili

- Webcam
- SVANTAGGI
  - Non standard (no ISO, ecc.)
    - Interoperabilità Volto -> Orecchio
  - Occlusioni
  - Non sempre applicabile

### State dell'arte

- Lo studio dell'orecchio 40 anni (impronte in CSI)
  - Ancora oggi è presente in letteratura dibattito se questa possa essere una prova impugnabile in tribunale al pari di una impronta o come la prova del DNA.
- I sistemi basati sull'orecchio (immagini 2D) esistono e mostrano tassi di errore EER di che vanno dal 6% di alcuni anni fa a recenti risultati prossimi a un EER del 4%.

### Diversità del tratto fra gli individui separazione interclasse

- Non siamo abituati a vedere le differenze fra le orecchie di persone diverse, ma sono evidenti
- Un lavoro scientifico (Iannelli) su 10000 orecchie ha trovato la perfetta separazione degli individui (anche fra gemelli)

### Ear localization and normalization

- È possibile usare solo alcuni tipi di face detector capaci di lavorare con i volti ruotati

### Feature extraction (ear template)

- EIGEN EARS (come autofacce)
- Estrazione mediante contorni e Diagrammi di Voronoi
  - Confronto fra 2 template
- Distanze dal centro dei punti principali
  - Non semplice e ben automatizzabile selezionare i punti specifici
- GABOR FILTERS Linear Binary Patterns

## Biometria della digitazione della tastiera e schermi

### Keystroke dynamics

- persone diverse battano la tastiera in modi diversi
- L'analisi della digitazione e firma online sono simili
  - tratti biometrici comportamentali
  - molto variabili nel tempo ed in base alle condizioni dell'individuo
  - considerati poco invasivi
  - acquisibili da sensori economici
  - Le tecniche di matching possono essere simili e richiedono degli allineamenti temporali

### Behavioural biometrics

- Keystroke Dynamics
- Swapping su schermo, mouse
  - Movimenti delle dita sullo schermo di persone diverse

### Comportamento dell'utente sul terminale

- In aggiunta esistono anche dei metodi che vanno ad identificare le persone in base al comportamento in un ambiente software oppure rispetto al sistema operativo.

- Per esempio, si può analizzare come viene usata la tastiera o il mouse, come si passa da una applicazione all'altra, come si accede ai menu a tendina ecc.
- Con il solo comportamento **non è SEMPRE possibile usare questi metodi per verificare una identità all'atto del logon** sul sistema (troppo poca informazione)
- Possono certamente essere **utili per verificare se**, durante il lavoro, **il terminale è utilizzato proprio dalla persona titolare dell'account**, oppure l'account è stato “prestato” o usato in modo non autorizzato dal titolare
- Prime evidenze **anche su pochi tocchi** (tastiera o schermo)

### **Keystroke dynamics biometrics → Two factors authentication**

- La possibilità di estrarre il template direttamente intanto che viene digitato la password di fatto rende possibile una istantanea identificazione a due fattori
- +OTP → 3 fattori

### **Estrazione delle feature**

- Le tecniche biometriche basate sul keystroke dynamics si impiegano per regolare l'accesso ai terminali in quanto non serve nessun sensore se non la tastiera stessa del terminale
- Le feature locali che si possono estrarre sono tipicamente le seguenti:
  - **tempo di latenza fra due pressioni**
  - **tempo di battitura del tasto** (tempo nel quale il tasto rimane premuto)
- Feature meno interessanti, ma che possono essere usate a corredo delle precedenti, sono:
  - la **velocità globale** di battitura
  - da **frequenza degli errori**
  - **l'uso di tasti non QWERTY** come il numpad, il tastierino ecc..
  - **l'uso del tasto “Shift”** piuttosto che il “Caps lock” per battere le lettere maiuscole
  - **la forza di battitura** dei tasti (impraticabile sulle tastiere normali)

### **Feature globali**

- Esistono anche in questo caso delle feature a **livello globale**, ovvero **che si possono calcolare solo quando tutta la sessione di battitura è finita**.
- Si tratta, in questo caso, delle **associazioni di tasti**, sia analizzate a **livello statico** (ad esempio, **quante volte è stata usata la coppia di tasti “ALT” e “TAB”**), oppure tenendo conto della **dinamica** (ad esempio, **quale è il tempo medio e la sua varianza che intercorre fra la battitura della coppia di tasti “ALT” e “TAB”**).

### **Punti di forza**

- Usando questi sistemi per regolare l'accesso dei terminali **non vi è necessità di un sensore**, ma è sufficiente la tastiera del terminale. I **sistemi** sono quindi **di tipo software**.
- Sono **molto ben accettati dall'utente** e considerati come non invasivi. (Io sono per la privacy.... Possibile sistema covert)
- Possono essere impiegati **anche senza la collaborazione dell'utente**, o addirittura senza che l'utente se ne accorga

### **Punti di debolezza**

- **Bassa accuratezza**
- Queste informazioni possono essere **usate per migliorare i tempi di rottura delle password**
- **Cambiando la tastiera**, spesso i **tempi cambiano** (per esempio cambiando da tastiera del PC a quella del notebook) oppure tenendo fra le dita una penna o solo impugnando una tazza con l'altra mano.
- **Ferite sulle mani o traumi possono rallentare ed influenzare la battitura** (per esempio una pallonata su un dito)

## Attacco su canale SSH

- È possibile perché esistono protocolli di trasmissione, come ad esempio il protocollo SSH, che **trasmettono immediatamente un pacchetto ogni volta che viene premuto un tasto**. In questo modo è possibile “intercettare” la password in base ai **tempi di latenza** che sono fedelmente rispecchiati dall’invio di pacchetti nella LAN
- I tempi di latenza da soli non riescono a dare abbastanza informazione da estrarre immediatamente la password, ma **restituiscono delle probabilità sulle coppie di lettere che permettono ai motori di generazione delle password di ridurre i tempi di successo di attacco di un fattore 50** per password alfanumeriche di 8 caratteri.

## Impronta e palmo unconstrained (o almeno less-constrained)

Unconstrained and less-constrained biometrics

- **Unconstrained** biometrics =
  - **Uncooperative** subjects
  - **Uncontrolled** scenarios
- **Less-constrained** biometrics, features:
  - **Touchless**
  - **Higher distances**
  - **Natural light conditions**
  - **On the move**

### Touchless fingerprints

#### Contactless fingerprint: Advantages

- **Less-constrained**
- **Absence of distortions** (of the skin) in the finger images
  - In contact-based fingerprints are due to different pressures of the finger on the sensor • More robust to dust and dirt
- **More user acceptance**
- **Possibility to use** the recognition methods in mobile devices with **standard CCD cameras**

#### Contactless fingerprint: Cons & Challenges

- Partially compatible with AFIS
- Complex background
- Sensible to lighting
- Sensible to position
- Systems based on 2D samples can present distortions
- Longer computational time

## PALM e PALM PRINT (Contact e Contact-less 2D e 3D)

#### Palmpoint recognition

- Biometric systems based on the features of the palm
  - Area from the wrist to the base of the fingers
- Several different features, visible with different resolutions
  - Geometrical features
  - Principal lines
  - Wrinkles
  - Delta points

- Minutiae
- Level 3 features

## Features

- Recognition algorithms:
  - Ridge based
  - Line based
  - Subspace-based
    - E.g., based on PCA
  - Statistical
    - E.g., descriptor-based
  - Coding-based
    - E.g., binarization of filter response

## Touchless vs touch-based

- Pros touchless:
  - **Less distortion**
  - **No dirt**
  - **Increased user acceptability**
- Cons touchless:
  - **Low contrast**
  - **Complex background**
  - **Sensible to lighting**
  - **Sensible to position**

## Contactless 2D Palmpoint

### Contactless palmpoint: VANTAGGI

- Less-constrained
- Low resolutions (< 200 dpi)
- Increased user acceptability
- Robust
  - Distortion
  - Dirt
- Multibiometric system
  - Combination with fingerprint, finger shape, hand shape, etc.

### Contactless palmpoint: SVANTAGGI

- High accuracy features not always usable (e.g., minutiae)
- Low contrast
- Complex background
- Sensible to lighting
- Sensible to position

## Methods

- Recognition algorithms:
  - Ridge based
  - Line based

- Subspace based
- Statistical
- Coding based

### Palm in Near infrared (Palm Vein)

Fujitsu PalmSecure: “A false acceptance rate below 0.00001 per cent (1 in 10 million) and false rejection rate of 0.01 per cent (1 in 10,000) make PalmSecure one of the most accurate biometric authentication system currently available on the market”

### 3D Palm acquisition (Using 2 cameras)

#### Palmpoint recognition: 3D (vs 2D)

- Pros of 3D:
  - Robust to lighting, occlusions, noise
  - Robust to spoofing attacks
  - Invariant to position and distance
  - Can use also 2D information
- Cons of 3D:
  - Complex device
  - Can be expensive

## Progettazione, valutazione e confronto di sistemi biometrici

### Documento «Best Practices ...»

- Il documento “Best Practices in Testing and Reporting Performance of Biometric Devices” è stato considerato uno “standard de facto” fino alla recente introduzione dello standard vero e proprio ISO/IEC 19795-1 “Information technology – Biometric performance testing and reporting” che lo incorpora quasi interamente
- Il documento è molto utile come guida per progettare degli esperimenti e delle valutazioni sui sistemi biometrici

### Struttura del documento

1. Introduction
2. Definitions
3. Planning the evaluation
4. Data collection
5. Analysis
6. Uncertainty of estimates
7. Reporting performance results

### Diverse valutazioni

- Un sistema biometrico può essere valutato sotto diversi aspetti:
  - Technology Evaluations
    - DB dati pubblici Test algoritmici.
  - Scenario Evaluations
    - Stanze attrezzate per valutare diverse tecnologie
  - Operational Evaluations
    - Sistema completo in deployment

Definizione ISO delle valutazioni

- **Technology evaluation**

- Offline evaluation of one or more algorithms for the same biometric modality using a pre-existing
- **Scenario evaluation**
  - Evaluation in which the end-to-end system performance is determined in a prototype or simulated application
- **Operational evaluation**
  - Evaluation in which the performance of a complete biometric system is determined in a specific application environment with a specific target population
  - vai a provare la poolazione e tutto il sistema in un ambito che è fedele a quello reale di applicazione finale controlliamo anche che la soglia fissata sia corretta e non rompa troppo le scatole

### Technology Evaluations

- I DB pubblici vengono creati
  - Prove eseguite “in laboratorio” con algoritmi (anche a livello di prototipo)
  - Prove eseguite su Database di sample
- Valutazioni indipendenti **sequestred**
  - Meccanismo del rilascio
    - Prevedono il rilascio di una piccola quantità di dati per **effetturare il “tuning” degli algoritmi (DATASET A)**.
    - Gli algoritmi sono poi rilasciati, e **vengono controllati su dei dati “sequestered”, non noti precedentemente (DATASET Q)**
    - Di solito **si confrontano algoritmi diversi** in modo comparativo **tutti con il DATASET Q**
  - (Se nessuno barca) questo permette di **minimizzare overfitting** nei sistemi.

### Scenario Evaluations

- I test controllano un **sistema biometrico completo in condizioni che simulano l’applicazione sul campo**
- Di solito **si testano diverse combinazioni di sensori e di algoritmi**
  - L’obiettivo è quello di **capire le combinazioni migliori per creare il sistema finale da implementare/comprare**

### Operational Evaluations

- Simile alla prova in condizioni di “scenario” ma eseguita
  - **su una specifica applicazione**
  - **con uno specifico algoritmo**
  - **sul posto esatto della applicazione**
  - si impiegano gli **utenti finali** della applicazione
- Si ottengono i risultati più vicini a quelli che compariranno nella applicazione finale
- I test di tipo operational di solito **non sono facilmente ripetibili** in quanto non è possibile ricreare esattamente le stesse condizioni in altri esperimenti di verifica

### Online evaluation

- Online: pertaining to execution of enrolment and matching at the time of image or signal submission
  - Online testing has the advantage that the biometric sample can be immediately discarded, saving the need for storage and for the system to operate in a manner different from usual.

### Offline Evaluation

- Offline: pertaining to execution of enrolment and matching separately from image or signal submission

- Collecting a corpus of images or signals for offline enrolment and calculation of matching scores allows greater control over which attempts and template images are to be used in any transaction.
- With scenario and operational testing, online transactions might be simpler for the tester (the system is operating in its usual manner) and, although recommended, storage of images or signals is not absolutely necessary.

### Intervallo di confidenza dei parametri

- Il documento specifica come calcolare i tassi di errore e tutti parametri del sistema
- I tassi di errore non significano quasi nulla se non è possibile **associare ad ogni misura il suo intervallo di confidenza**
- In altre parole ogni parametro è il risultato di una stima (esempio una media) che deve essere corredata dalla valutazione del suo intervallo di confidenza (**deviazione standard oppure varianza**)
- Gli intervalli di confidenza vengono costruiti di solito non da esperimenti, ma da un **modello statistico che descrive meglio possibile l'esperimento**

## Progettazione, valutazione e confronto di sistemi biometrici

### Comparazione sistemi biometrici

#### Comparazione dei sistemi

- La comparazione dei sistemi avviene confrontando i valori tipici delle figure di merito analizzate durante il corso
  - Numeri puri come EER, FAR, FTE, FTM
  - Descrittive ad esempio
    - distribuzione dei genuini  $p_n(t)$
    - distribuzione degli impostori  $p_m(t)$ , ecc..
  - **Meglio** Tipicamente quali eventualmente esprese in funzione della soglia biometrica  $t$  quali:  $FMR(t)$ ,  $FNMR(t)$ , ROC, DET, CMC
- La comparazione maggiormente efficace è quella che può avvenire esaminando le curve ROC (o similmente DET) dei due sistemi.

#### ROC = 1 – DET

- La curva DET e la curva ROC mostrano le stesse informazioni.
  - Riferendoci ad autenticazione positiva, la DET mette l'attenzione sul FNM (genuini che non entrano) mentre la ROC mette in evidenza 1-FNM (quanti genuini che riescono ad entrare)

#### Riassunto sulla comparazione di DET

- Le figure mostrano come la comparazione di sistemi eseguita **basandosi solo sul EER non sia sempre corretta**
- Occorre **decidere la regione di funzionamento del sistema nei termini di FNMR o FMR** e poi vedere negli intervalli di interesse quale sistema si comporti meglio
  - Richiedere al committente un range di FMR o FNMR al quale vorrebbe far lavorare la applicazione, o farlo ragionare su questo...

#### Accuratezza in identificazione: Cumulative Match characteristic (CMC)

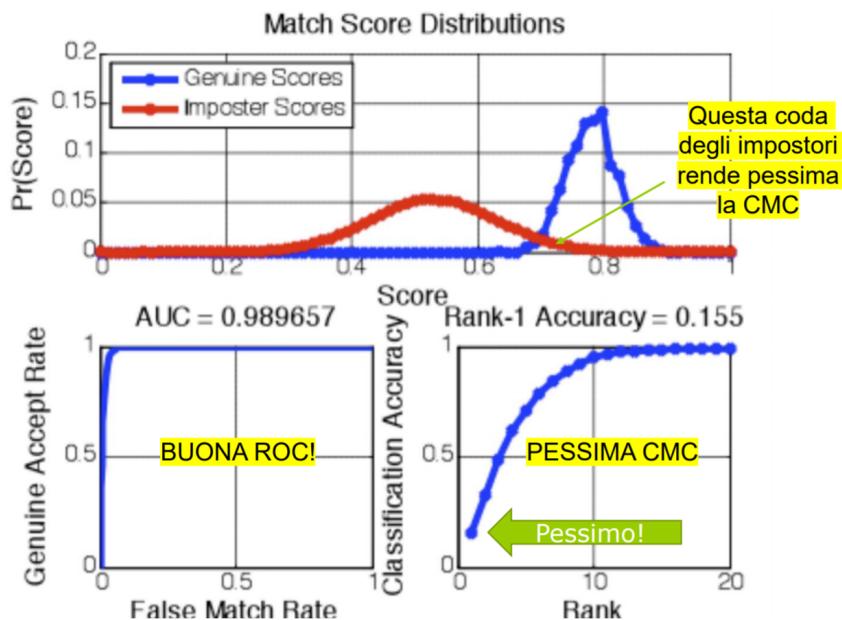
- Nel contesto della identificazione si può valutare il grafico CMC
  - Es:
    - N persone nel DB

- Per ogni individuo  $k$  ordino gli  $r$  (=rank) individui più simili a  $k$
- Conto quante volte il sig.  $k$  era negli  $r$  trovati per tutti  $N$
- o Nota
  - Si usano solo gli score, non si usa nessuna soglia

### Legame fra distribuzioni DET e CMC

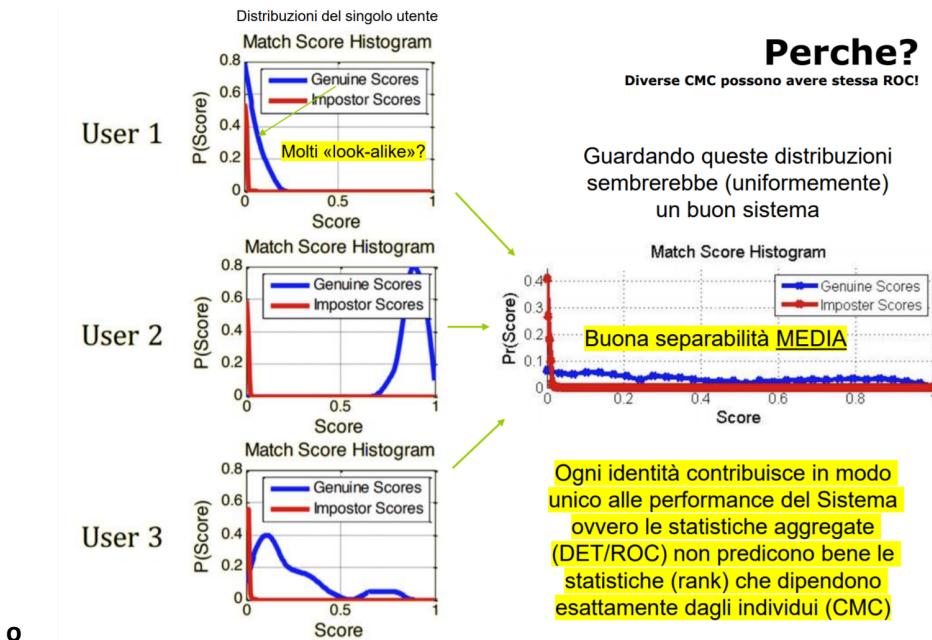
- Distribuzioni **MOLTO ben separate** produrranno poi una **buona ROC/DET** e una **buona CMC**
- Buona ROC → non è detto Buona CMC

## Buona ROC → non è detto Buona CMC



o

- Diverse CMC possono avere stessa ROC!



o

### Distribuzioni: $d'$

- $d'$  la misura del grado di separazione presente fra le distribuzioni degli impostori e dei genuini calcolato considerando le loro medie e deviazioni standard
- Anche il parametro  $d'$  da solo non è del tutto esauriente in quanto si possono trovare situazioni molto diverse con stesso  $d'$

## Indici aggiuntivi: Security, Convenience

### Security and Convenience

- Le zone della curva DET
  - con basso FMR → regione di Security
  - con basso FNMR → regione di Convenience
  - Attorno al EE (bisettrice) abbiamo le applicazioni civili normali
- Definizioni (in autenticazione positiva):
  - Security =  $1 - FAR(t)$
  - Convenience =  $1 - FRR(t)$

### Regione di sicurezza

- Il sistema tende
  - **bassa possibilità che un utente non abilitato possa entrare** in un'area riservata
  - potremo avere un **più alto tasso di utenti abilitati che non entrano al primo tentativo**, ma che dovranno mostrare più volte il loro tratto biometrico al sensore per poter entrare.
- Esempio di applicazione: **accesso struttura critica**

### Regione di convenienza

- Il sistema tende
  - a **non far perdere tempo agli utenti abilitati** in quanto con bassa probabilità **un utente abilitato non entrerà al primo tentativo**
  - mentre avremo **un tasso leggermente più alto di utenti non abilitati che entreranno nell'area controllata**.
- Esempio di applicazione: **tornello del pagamento della metropolitana**

## Standard ISO per la biometria

### ISO/IEC 19794

- **Si occupa dell'interscambio dei dati biometrici fra istituzioni e aziende.** Parti:
  - Biometric Data Interchange Formats
    - Part 1: Framework
    - Part 2: Finger Minutiae Data Part
    - Part 3: Finger Pattern Spectral Data
    - Part 4: Finger Image Data
    - Part 5: Face Image Data
    - Part 6: Iris Image Data
    - Part 7: Signature/Sign Behavioral Data
    - Part 8: Finger Pattern Skeletal Data

### Chi sono gli «Standard body»

- Sono **organismi internazionali/istituzioni che regolano per es. tutti gli standard per i protocolli in uso** con il nostro Bancomat o i terminali POS, i protocolli di sicurezza nelle trasmissioni su canale crittato quale la PKI, ecc
- In biometria sono importanti

- International Organization of standardization (**ISO**), International Eletrotechnical Commission (**IEC**)
- Esistono anche dei “**body informali**” i quali rappresentano **gruppi di grandi aziende** che si occupano di sistemi biometrici (**Lobbying**).
  - Biometric Consortium
  - BioApi Consortium

### Standard BioAPI

- Lo standard BioAPI già dal 2000 contiene le **specifiche di interazione dei moduli componenti il sistema biometrico**.
  - Fornisce un **modello di autenticazione ad alto livello per ogni tecnologia biometrica** disponibile sul mercato
  - Public domain, Open source
  - Platform/OS independent
- Include le **specifiche delle funzionalità** di
  - Enrollment
  - Verification
  - Identification

**delle interfacce con i DB in modo tale di permettere al Biometric Service Provider (BSP) di gestire template nel DB** nel modo ottimale.
- **BSP** è un termine generale che indica **il modulo che gestisce le funzionalità biometriche verso i moduli HW e i layer software necessari** delle unità
- Fornisce primitive per permettere all'applicazione di gestire la acquisizione dei campioni **anche su sistemi distribuiti**, ovvero come gestire l'acquisizione su un modulo “client” ed invece l'Enrollment, l'Identification e la Verification sul un modulo server.

### Progettazione di un sistema monomodale

#### Problema della progettazione

- È un problema molto complesso:
  - Vi sono **molti parametri** di giudizio
  - I **parametri sono difficilmente stimabili**

#### 8 domande per scegliere il tratto

- Ecco una sequenza di 8 domande da farsi per poter scegliere il opportunamente il tratto da usare per il sistema biometrico
- È una applicazione di **autenticazione o identificazione?**
  - Se identificazione occorre controllare le proprietà di
    - scalabilità
    - unicità del tratto
- È un sistema **attended** (semiautomatico) o **unattended** (completamente automatico)
  - Se attended
    - occorre prevedere una persona sempre di fianco al sensore di acquisizione
    - se l'applicazione è remota o posta in una situazione ambientale “ostile” o “insicura” potrebbe non essere possibile richiedere sempre la presenza di un operatore al controllo della acquisizione

- **Gli utenti sono abituati/allenati?** Possono essere convinti ad allenarsi?
  - Le evidenze sperimentali mostrano che le performance (accuratezza e assenza di retry) migliorano notevolmente se gli utenti
    - imparano come “farsi acquisire”
    - sono collaborativi al rispetto delle procedure/consigli per l’acquisizione del tratto
  - Questo è particolarmente vero per alcuni tratti biometrici (le impronte, il volto,...) ed indifferente per altri (retina,...)
- È un sistema **aperto o coperto/nascosta** (overt/covert)?
  - Alcuni tratti biometrici non possono essere acquisiti senza mettere a conoscenza il soggetto
    - Possono esistere dei motivi legali legati alla privacy
    - Per le caratteristiche del tratto biometrico (soft biometrics derivata da intervista, impronta, iride)
- I soggetti sono **collaborativi o non-collaborativi?**
  - Se i soggetti sono non-collaborativi (es.: terroristi, frodatori, alcuni detenuti) è necessario usare tratti biometrici che non possono essere cambiati.
  - Evitare i tratti biometrici comportamentali (la voce può essere facilmente alterata rispetto alla iride)
- Quali sono i requisiti sulla **capacità di memorizzazione del sistema**?
  - I tratti biometrici hanno template da memorizzare che possono variare moltissimo (da pochi byte per le impronte a molti Kbyte per la voce)
- Quanto sono stringenti le **richieste sulle performance** (accuratezza, velocità, distanze di acquisizione,...)?
  - Ad esempio è possibile unire 2 tratti veloci in un sistema multimodale per ottenere l’accuratezza richiesta che uno solo dei tratti non potrebbe garantire
- Quali tipi di tratti biometrici sono **accettati dalla popolazione** degli utenti?
  - L’accettazione varia molto in base livello culturale, etico, sociale, religioso ed igienico della popolazione
  - Esempio: non è possibile imporre un sistema per i volti in un paese dove il 50% della popolazione non vuole mostrare il volto

Tabelle comparative

Maturità, dimensioni, costo,....

## Maturità, dimensioni, costo,....

	Finger	Face	Voice	Iris	Hand	Signature
Maturity	very high	medium	medium	medium	high	medium
Sensor type	contact	non obtrusive	non obtrusive	non obtrusive	contact	contact
Sensor size	small	small	very small	medium	large	medium
Sensor cost	< \$200	< \$50	< \$5	< \$300	< \$500	< \$300
Template size	< 500	< 1,000	2,000	256	< 100	200
Scalability	high +	medium	low	very high	low	high -

1:1 Matching properties						
#FA per 10K (@FRR=10%)	0.1	10	300	0.001	10	300
#FA per 10K (@FRR=1%)	10	1,000	1,000	0.1	100	1,000
Template size (bytes)	500	1,000	2,000	250	100	200

Da aggiornare  
anno per anno (\*)

(\*) Non confondere questi numeri generali con gli standard per i documenti biometrici

Fattori di progetto VS Tratti ordinati

<b>Effortless</b>	<b>Iris &gt; Face &gt; Finger &gt; voice</b>
<b>Accurate</b>	<b>Iris &gt; Finger &gt; Face &gt;~ Voice</b>
<b>Inexpensive</b>	<b>Voice &gt; Finger / Face &gt; Iris</b>

Che livelli di accuratezza sono da impostare?

- Quali sono i livelli di FNMR e FMR da richiedere al sistema sulla singola comparazione (1:1) nelle varie condizioni (assumendo FTA=FTE=0)?
- Ecco alcuni ordini di grandezza che sono considerati come necessari
  - Autenticazione
    - FNMR = 0.1%
    - FMR = 0.1%
  - Identificazione su larga scala (1 Milione di ID)
    - FNMR = 10%
    - FMR < 0.0001% (sbagliare meno 1 errore su 1 M match)

- Screening (500 ID)
  - FNMR = 1%
  - FMR = 0.001%

## Piattaforme e Biometrics as a Service

### Biometria in cloud

#### Biometric Services Platform

- Come estensione del BSP (Biometric Service Provider) si hanno anche le **Biometric Services Platform**:
  - *modular, open platform used to enable a biometric system with advanced biometric data processing and management functionality in a web services architecture*

#### Biometrics as a Service (BaaS)

- Make or buy? Nuove soluzioni per fare riconoscimento biometrico basate su cloud
- Vanno a **semplificare installazione, uso, gestione e manutenzione** del sistema biometrico
- **Abbassano i costi ed i tempi per iniziare ad usare un sistema biometrico**, specialmente per grandi organizzazioni
  - Da un budget decisamente alto verso una semplice fee per utente/identificazione/ecc.
- **Necessitano di connessioni affidabili** o il servizio viene interrotto...

#### BaaS – Pro e Contro

- Alcune caratteristiche trasversali alle varie soluzioni disponibili in commercio (**punti a favore**)
  - scalabilità
  - cost-effectiveness
  - reliability,
  - hardware agnostic, se cambia il sensore HW a me non interessa, ci penserà il produttore a farlo andare
  - Permette accesso ubiquo a dati privati e servizi
- Altri punti (**critici**)
  - Forte dipendenza dal fornitore per prezzi e contratti (ma è più facile cambiare fornitore)
  - **Privacy, liste di proscrizione, usi non concordati, ...**

## Sistemi multimodali

### Sistemi multibiometrici e multimodali: Metodi avanzati di fusione

#### Svantaggi dei sistemi monomodali

- Rumore presente nei dati in ingresso
  - ad esempio condizioni ottimali di illuminazione per il volto, o di umidità per le impronte, ...
- Variabilità intra-classe
  - variazioni di posa nel volto, raffreddore nella voce, ferite su un polastrello, ...
- Limitata distintività del tratto biometrico
  - forma della mano, firma online, ...
- Non universalità del tratto
  - tasso di Failure to enroll, malattie, fobie, ...
- Attacchi sul sensore
  - dita in silicone, trucco e maschere, registratori,...

## Sistemi multimodali

*"Multimodal biometric systems are those which utilize, or are capable of utilizing, more than one physiological or behavioral characteristic for enrollment, verification, or identification"*

### I sistemi multimodali sono più accurati

- È perfettamente assodato in letteratura che i sistemi biometrici multimodali siano più accurati dei sistemi che li compongono
- Prendiamo ad esempio un sistema basato su impronte, mano e volto: la **curva ROC del sistema multimodale presenta errori minori in tutta la sua estensione**

### Vantaggi e svantaggi dei sistemi multimodali

- VANTAGGI
  - usare **N tratti biometrici** al posto di uno solo permette di **estrarre informazione per aumentare le performance del matching**
  - si **aumenta la copertura della popolazione riducendo il Failure to Enroll rate**
    - gli utenti che non possono registrarsi usando un tratto possono optare per gli altri
  - sono **un efficace metodo antispoofing**
    - è molto **più difficile ingannare contemporaneamente più sensori**
- SVANTAGGI
  - sono **più costosi** essendo composti da più unità biometriche
  - sono **più lenti in acquisizione** (occorre **acquisire più tratti**)

### Cosa si può unire? (Multibiometrico)

- **Multiple sensors**
  - optical and capacitance sensors
- **Multiple biometrics**
  - face and fingerprint
- **Multiple units**
  - right index and middle fingers
- **Multiple snapshots**
  - two attempts or two templates of right index finger
- **Multiple matchers**
  - minutiae and non-minutiae based matchers

### Quali tratti unire?

- **Alcuni** esempi di combinazioni di tratti biometrici sono spazialmente vicini (per esempio iride e volto) per praticità di acquisizione, altri sono distanti per garantire la assoluta indipendenza dei tratti biometrici

### Terminologia usata in letteratura

**Modo = tratto (es: 1 dito, 1 occhio, 1 mano)**

- In letteratura all'interno della macrodistinzione monomodale/multimodale si usano sotto-categorie (alcune volte non usate correttamente)

- **Monomodale**, con una eventuale piccola distinzione:

- **Unibiometric**: singolo tratto biometrico
  - **Unimodal**: una singola immagine, una singola rappresentazione, un singolo matcher

- **Multimodale** (multimodal): usa tratti biometrici scorrelati (es: impronta e volto)
- **Multibiometrico**: cappello generale che comprende multimodale e sistemi con tratti biometrici debolmente correlati, scorrelati, sensori diversi, software diversi,...

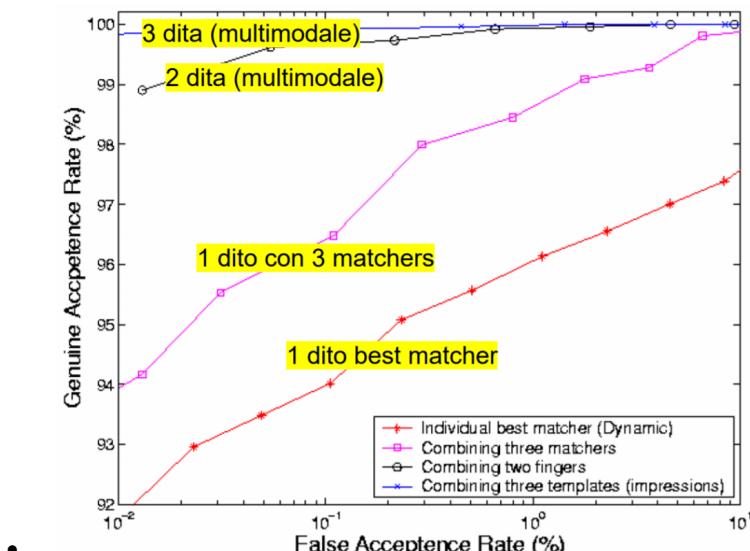
## Tecniche di datafusion biometrica

### Schemi classici

- Multimodale
  - Fusione a livello di feature
  - Fusione a livello di matchscore
- Multibiometrico
  - Fusione a livello di matchscore

### Fusione a livelli diversi

- L'incremento di accuratezza maggiore si verifica **usando 3 templates, poi l'uso di due dita, e successivamente vengono le combinazioni di matcher diversi**
- Questo risultato è generale, **meglio usare sample indipendenti se possibile**



- 

### Metodi di fusione del match score

- La **regola della somma** si è dimostrata in grado di aumentare sempre le prestazioni nei test
  - $S = w_1s_1 + w_2s_2 + w_3s_3$
  - **Un metodo di fusione semplice ed efficace è quella a livello di matchscore con somma**
- Vi sono **2 filosofie** diverse per unire i match score  $s_1, s_2, \dots, s_n$ : **classificazione** e **combinazione**
- Il **classificatore** è un **modulo** che avendo in ingresso i  $s_1, s_2, \dots, s_n$  produce direttamente l'**uscita impostore/genuino**
  - reti neurali, Knn, classificatore lineari, SVM, ad albero,...
  - questi sistemi per poter fissare i parametri necessitano di dati e di una fase di allenamento (trained classifier)
    - Non ho una soglia che posso regolare
- Il **combinatore/regressore** è un **modulo** che **combina in modo lineare, non lineare, logico/combinatorio i valori  $s_1, s_2, \dots, s_n$  e passa un unico valore  $S$  al decisore finale** (che può essere di nuovo un classificatore o una semplice soglia come abbiamo già visto)
  - AND/OR, funzioni, votazione, max, min, ...
  - Reti neurali e regressori

## Normalizzazione degli score

- Per confrontare fra loro correttamente i valori di diversi matcher fra loro (valori di distanza fra template) è necessario eseguire prima una operazione di normalizzazione prima di fare la regola della somma faccio la normalizzazione e studio gli score, guardo le distribuzioni ed omogenizzo il significato
- Serve per
  - **omogenizzare il significato** (per esempio s1 è una similarità ed invece s2 è una distanza)
  - **riportare alla stessa scala** le uscite s1, s2, ... sn (ad esempio le uscite possono una variare fra 0 e 100 ed un'altra fra 0 e 1000)
  - **uniformare le distribuzioni** dei valori (spostare i valori medi e le variazioni per uniformarle con quelle di tutti gli altri valori di match score)
- Meglio tenere sempre conto della
  - **robustezza** (un valore molto diverso, magari provocato da un errore non deve stravolgere la normalizzazione)
  - **efficienza** (occorre normalizzare avendo dei parametri stimati, che però devono essere vicini a quelli reali dei match score, altrimenti la normalizzazione non è corretta)

## Funzioni di normalizzazione

- **Normalizzazione min-max**
  - dati i match score  $\{s_k\}, k=1, 2, \dots, n$  si ottiene il match score normalizzato
- Normalizzazione **decimale o logaritmica**
  - da usarsi quando ci sono degli ordini di grandezza di diversità o di un fattore logaritmico uso la logaritmica se ho un valore che mi schizza ad infinito
- **Z score**
- **Mediana e Deviazione Assoluta della Mediana**
- **Funzione Sigmoidale doppia**
  - serve per limitare a destra e sinistra senza far propagare all'infinito, tanto ormai ho capito che andrà così.

Min-max e Z score sono efficienti. Mediana e la sigmoidale doppia sono robuste.

## Integrazione di sistemi commerciali

- In questo test viene mostrato come si comporta un sistema multimodale che fonde 3 diversi sensori commerciali per l'impronta (V1, V2, V3) ed un sistema basato sul volto
- **Combination of V1, V2, V3 & Face is not always better than combination of V2 & Face**

## Tecniche avanzate di datafusion per sistemi multimodali

### Sistemi multimodali gerarchici

- Nei **sistemi multimodali gerarchici** (Sequential pattern recognition) avvengono **acquisizioni biometriche in cascata a seconda del risultato dell'identificazione precedente**
  - si aggiungono sempre più metodi di autenticazione per ogni fase non andata a buon fine
- In **verification riducono il tempo di verifica**
- In **identificazione permettono mediante "pruning"** di ridurre le porzioni da analizzare del DB (indexing)
- **Per ridurre il tempo medio di verifica, occorre acquisire per primi i tratti biometrici maggiormente accurati**
- In altre applicazioni è l'utente che sceglie che tratto mostrare

## Fusione a livello di feature

- Non è sempre facile riuscire a realizzare una efficace fusione delle informazioni a livello di feature. La principale causa è la **eccessiva eterogeneità fra le features** (per esempio, volto con autofacce e impronta con minuzie)
- Di solito è possibile quando si estraggono da tutti i tratti biometrici delle feature numeriche (vettori)
  - Esempio
    - si estraggono le feature
      - mano (14 lunghezze)
      - volto (25 coefficienti delle autofacce)
    - si normalizzano le feature
    - si concatenano i due vettori
    - si calcola
      - la distanza euclidea fra i template concatenati
      - si calcola la distanza anche delle singole feature
    - si uniscono tutti i risultati con un classificatore o un combinatore con soglia

## Parametrizzazione specifica per il singolo utente

- Esistono **due approcci** per aumentare ancora le **prestazioni** se viene tenuto conto delle **caratteristiche singolari** di ogni utente
  - **ogni utente ha una distanza dagli impostori personalizzata**
    - **ogni utente può quindi avere la sua soglia di decisione personalizzata per ogni tratto biometrico**
  - **ogni utente produce delle acquisizioni biometriche dei tratti con qualità diversa**
    - si possono **pesare diversamente i tratti biometrici** tenendo conto
      - della **qualità di acquisizione in enrollment** per ogni utente
      - dell'**errore di quel tratto biometrico** (ad esempio facciamo pesare di più le **impronte** del volto nella decisione finale)
- In altre parole, si hanno **due set di parametri di progettazione in un sistema biometrico multimodale:** le **soglie dei matching** ed i **loro pesi**
- Dalle **distribuzioni di due genuini** possiamo andare a **calcolare la soglia perfetta per ognuno** per avere un **FRR** desiderato per esempio del 1%
  - Se erano **score di impostori** → **controllavo il FAR**

## Modalità di integrazione della soft biometrics

- Alcuni i tratti chiamati di “**soft biometric**” possono essere usati in aggiunta
  - genere
  - colore della pelle
  - colore dei capelli
  - colore degli occhi
  - peso
  - altezza
  - ...
- L'integrazione corretta di un sistema di soft-biometrics è a valle del modulo biometrico primario
- Esempio: dalla impronta dell'utente viene estratto il **template x** e la misura della sua **altezza y**
  - Il **modulo di matching primario ritorna una match score** che possiamo interpretare come la **probabilità che l'input x corrisponda all'individuo ω**
  - (l'individuo che, fra tutti nel DB, ha il matchscore più alto) ossia  $P(\omega|x)$ .
  - Dobbiamo quindi progettare il **Post Processing Module**

- o Sceglieremo una funzione che rappresenti al meglio i valori dati dalla formula di Bayes per tutti gli utenti ovvero  $P(\omega | x,y)$

## Esempi di sistemi multimodali

### Sistemi multimodali per il volto

- I sistemi innovativi per il riconoscimento del volto basati su “**multiple images**” o su “**2.5D faces**” sono di fatto dei sistemi **multibiometrici**
- Grazie alla fusione delle informazioni sono riusciti a compiere un grosso passo in avanti rispetto ai primi sistemi anche di soli 5 anni fa

### Sistema BioID

- Il produttore BIOID commercializza un prodotto che
  - o **controlla la sincronia fra il parlatore ed i movimenti delle labbra** (tratti correlati)
  - o effettua il **riconoscimento del volto** (tratto indipendente dalla voce o dai movimenti delle labbra)
- Il **controllo della sincronia aumenta la robustezza del sistema** contro gli attacchi
- La **multimodalità dei tratti indipendenti incrementa l'accuratezza del sistema complessivo**

### Sistema Iride+Retina

- Il sistema Iride + Retina implementa **due delle più accurate e resistenti agli attacchi tecnologie** presenti sul mercato
- **Ad oggi è impossibile riuscire a falsificare allo stesso tempo i due tratti superando i test di liveness** disponibili su questi sistemi