Macerata, 28 ottobre 2016

I molteplici profili della sicurezza

Iniziativa nell'ambito dell'European Cyber Security Month (ECSM)

Biometria: un nuovo paradigma di autenticazione e identificazione

Francesco Ciclosi

Biometria: definizione

- È l'insieme delle **tecniche automatiche per l'identificazione degli individui** basata sulle loro caratteristiche fisiche e comportamentali

Una nuova modalità di identificazione

- La biometria ci mette a disposizione una nuova modalità **automatica** di identificazione delle persone

PRIMA	ORA
Una cosa che sai (password)	**Quello che sei** (impronta, iride, mano)
Una cosa che hai (documento, chiave, card)	**Quello che fai** (voce, firma)

L'identificazione personale

- È l'operazione che associa un'identità a un individuo
- Può essere distinta in due categorie con funzione e complessità diverse:
  - **Autenticazione** → Verifica dell'identità
  - **Identificazione** → Riconoscimento

L'autenticazione

- L'operazione di verifica dell'identità (**Autenticazione**) equivale a dare risposta alla domanda: *«Sono davvero chi affermo di essere?»*
  - Si tratta di un metodo one-to-one (1:1)
  - Consente di confermare o negare l'identità dichiarata dall'utente

L'identificazione

- L'operazione di riconoscimento dell'identità (**Identificazione**) equivale a dare risposta alla domanda: *«Chi sono io?»*
  - Si tratta di un metodo one-to-many (1:N)
- Un problema di identificazione può essere:
  - **Chiuso** → se si ricerca all'interno di un insieme di identità note
  - **Aperto** → altrimenti

La tecnica positiva e quella Negativa

- L'autenticazione/identificazione può essere:
  - POSITIVA
    - Se si cerca di stabilire con accuratezza **se l'utente è** chi dice di essere
    - Può evitare che più persone utilizzino una singola identità
  - NEGATIVA
    - Se si cerca di stabilire con accuratezza **se l'utente non è** chi dice di essere
    - Può evitare che una persona utilizzi identità multiple

I metodi biometrici di identificazione

- Vengono utilizzate le caratteristiche fisiche e/o comportamentali dell'individuo per identificarlo
  - Tratti fisici
    - Iride, impronta, volto, geometria della mano, ecc.
  - Tratti comportamentali
    - Firma, voce, camminata, ecc.

Metodi biometrici: punti di forza

- Non è possibile dimenticarli o cederli ad altri
- Sono più difficili da falsificare
- Possono garantire un'accuratezza maggiore di quella garantita con i metodi tradizionali
- Possono realizzare l'identificazione negativa
- Quasi azzerano l'esposizione ai reclami e al ripudio

Metodi biometrici: problematiche

- Rispondono con un livello di «matching» e non con una decisione binaria (si o no)
- Non possono essere cambiati a piacimento
- Molte persone non accettano l'utilizzo dei sistemi biometrici (invasione della privacy)
- Non tutte le persone posseggono tutti i tratti
- Hanno un costo più elevato

Le 7 proprietà del tratto biometrico (1/2)

1. Universalità
   - Ogni persona deve possedere il tratto o la caratteristica
2. Unicità
   - Due persone non devono avere lo stesso tratto uguale
3. Permanenza
   - La caratteristica deve essere invariante nel tempo
4. Misurabilità
   - Il tratto deve poter essere esaminato quantitativamente

Le 7 proprietà del tratto biometrico (2/2)

5. Performabilità
   - L'accuratezza dell'identificazione deve essere adeguata e garantibile senza particolari condizioni operative
6. Accettabilità
   - Indica la percentuale di persone che potrebbero accettare l'utilizzo del tratto biometrico
7. Circonvenzione
   - Indica il grado di difficoltà nell'ingannare il sistema con tecniche fraudolente

Scelta dei tratti per l'identificazione

- Non tutti i tratti possono essere utilizzati sia in Autenticazione che in Identificazione
- Solo l'impronta e l'iride sono usati per l'identificazione 1:N, dove N è molto grande
- Mano, volto, voce e firma sono usati solo per:
  - Autenticazione 1:1
  - Identificazione 1:N, con N nell'ordine delle decine

Variazione del tratto

- Il tratto biometrico può variare nell'arco di una vita oppure giorno dopo giorno
- La progettazione di un sistema biometrico deve considerare la varianza propria del tratto scelto
- Le principali cause di variabilità sono:
  - Volto: occhiali, capelli, barba, espressioni
  - Firma: variazioni, disuso, abbellimenti
  - Voce: raffreddore, raucedine

I campioni indipendenti

- Sono il numero di campioni differenti dello stesso tratto che possiamo registrare per ogni persona
- Maggiore è il numero dei campioni indipendenti utilizzati in un sistema biometrico, maggiore sarà la sua accuratezza

10 dita	2 occhi	2 mani
1 volto	1 voce (se non viene associata a una parola chiave	1 firma (teoricamente)

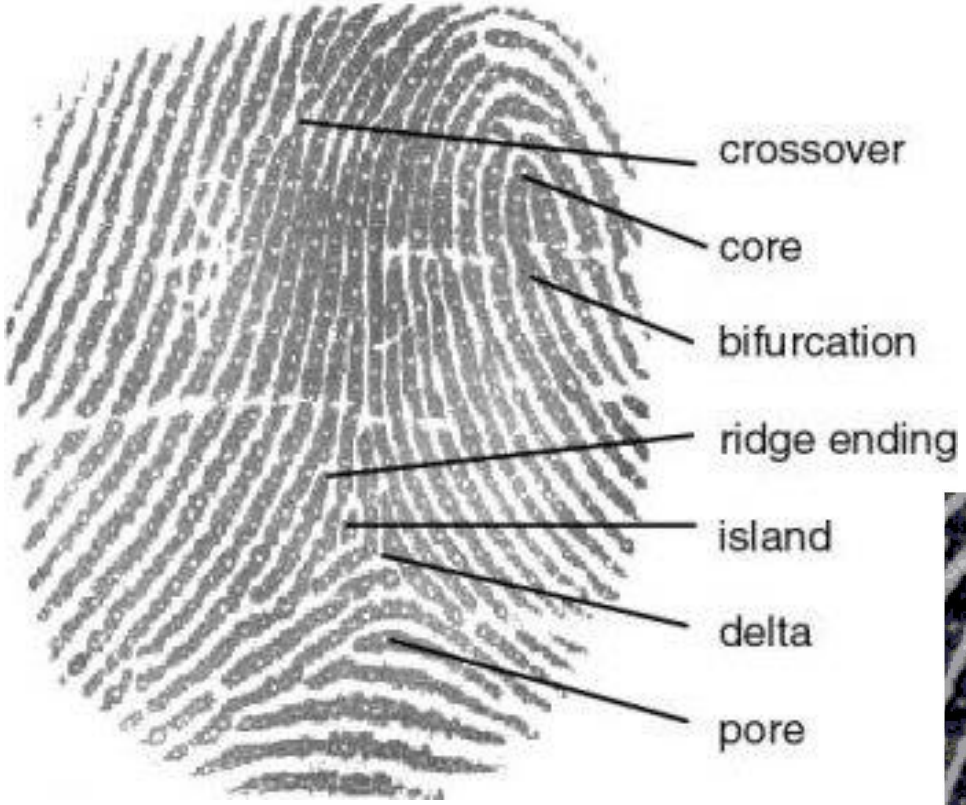
I principali tratti biometrici

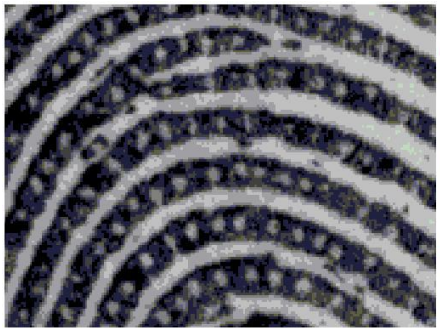
Diffusione dei tratti biometrici

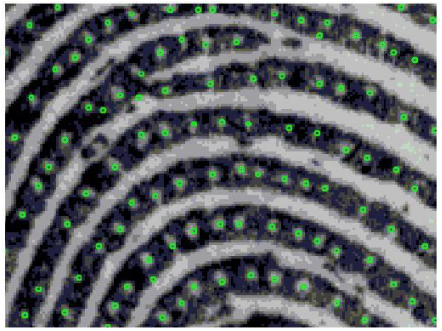
- I tratti maggiormente utilizzati[1] nei sistemi biometrici sono:
  - Impronta - 44%
  - Volto - 19%
  - Geometria della mano - 9%
  - Iride - 7%
  - Voce - 4%
  - Firma - 2%

[1] Dati aggiornati al 2006

L'impronta digitale

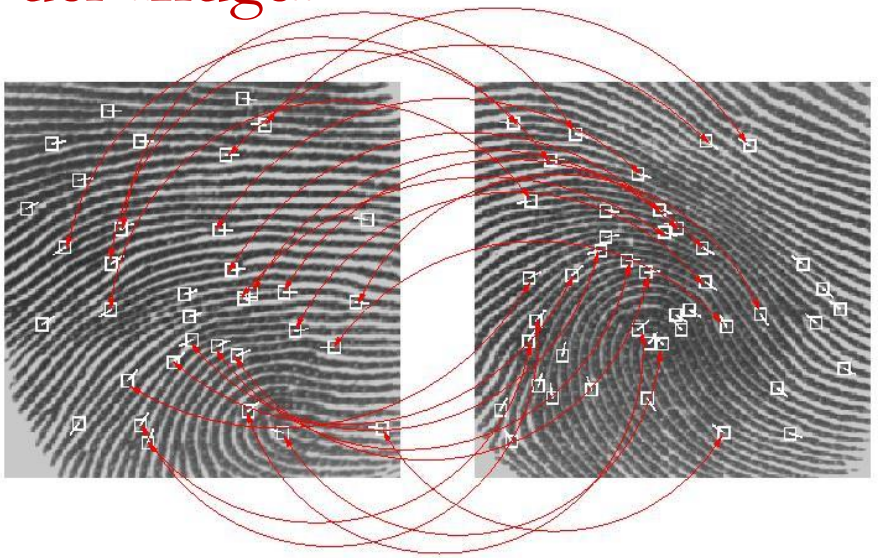






Il riconoscimento dell'impronta digitale

- Avviene secondo tre approcci:
  - Basato su correlazioni
    - Il confronto avviene pixel a pixel
  - Basato sulle caratteristiche dei «ridge»
    - Il confronto avviene «ridge a ridge»
  - Basato sulle minuzie
    - Il confronto avviene «minuzia a minuzia»



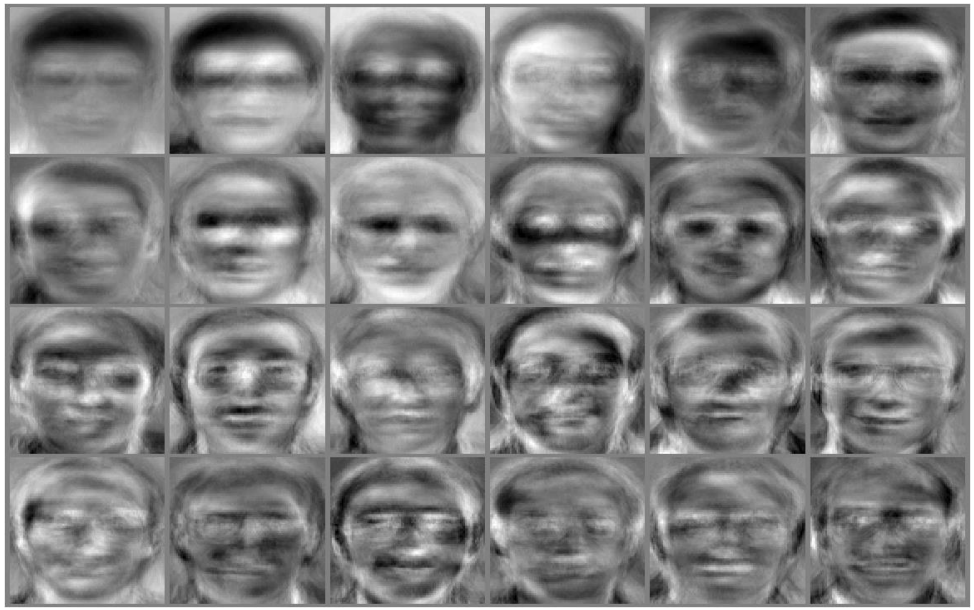
Alcune criticità dell'impronta digitale

- È difficile progettare dei sistemi che riescano a:
  - Funzionare anche con piccoli «overlap»
  - Funzionare anche con diverse condizioni della pelle
  - Funzionare anche con diversi sensori
  - Aumentare la qualità dei campioni utilizzati

Il volto

- È uno dei tratti biometrici meno intrusivi
- Trova tantissime applicazioni pratiche
- È il metodo che normalmente le persone utilizzano per riconoscersi tra di loro

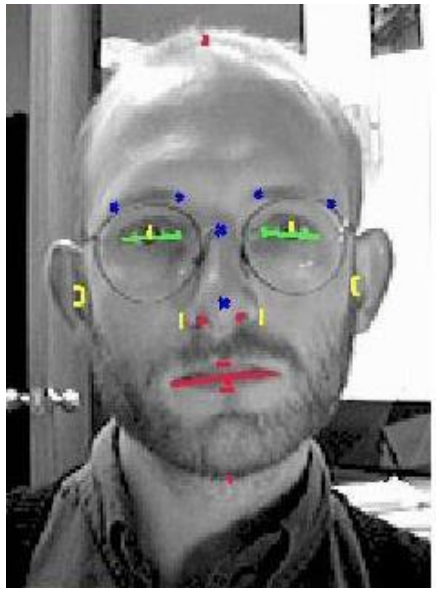
Il riconoscimento del volto: trasformazione

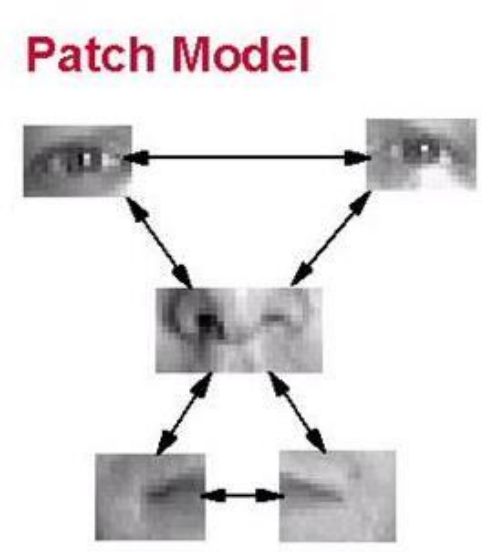


EIGENFACES

- È uno dei due approcci disponibili per il riconoscimento
- Si crea una «base di immagini» che permette di ricostruire un nuovo volto come una somma delle immagini contenute nella base

Il riconoscimento del volto: attributi





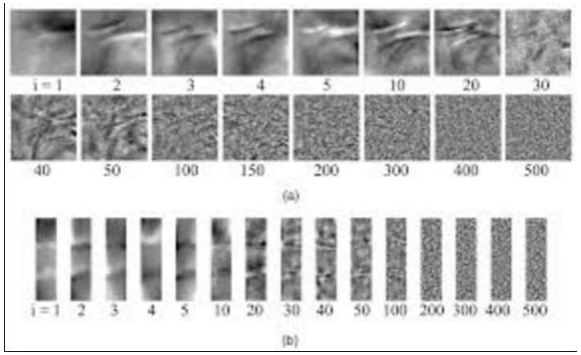
- È uno dei due approcci disponibili per il riconoscimento
- Si localizza il volto in un'immagine e si misurano delle caratteristiche specifiche
  - Ad esempio: lunghezza del naso e della bocca, la distanza fra gli occhi, ecc.

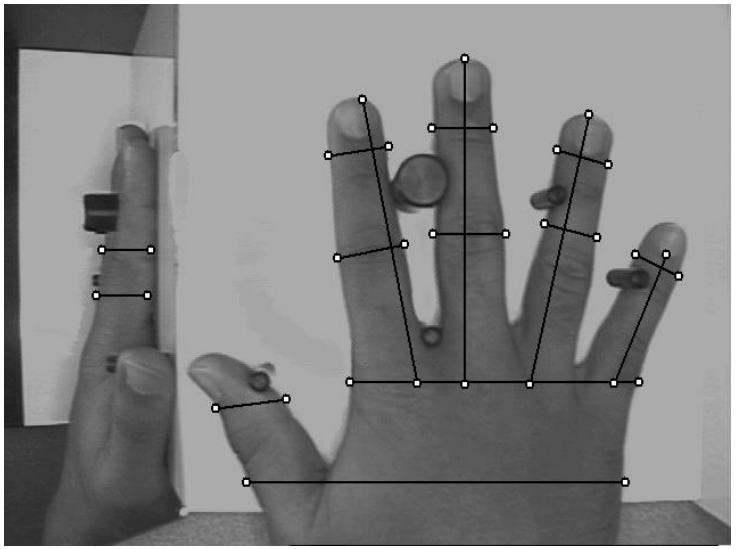
Alcune criticità del volto

- È difficile progettare dei sistemi che riescano a gestire in modo efficace:
  - Espressioni del volto
  - Variazioni della posa
  - Variazioni degli sfondi delle scena
  - Variazioni delle luci della scena
  - Invecchiamento del volto

La geometria della mano

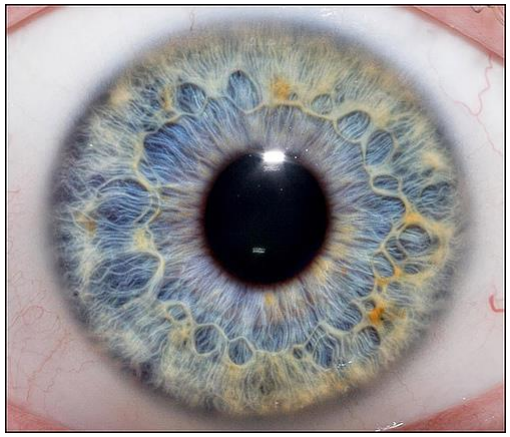
- È un tratto biometrico poco invasivo e quindi generalmente ben accettato dagli utenti
- Offre un discreto livello di accuratezza
- Può lavorare su tre viste:
  - Palmare
  - Laterale
  - Dorsale

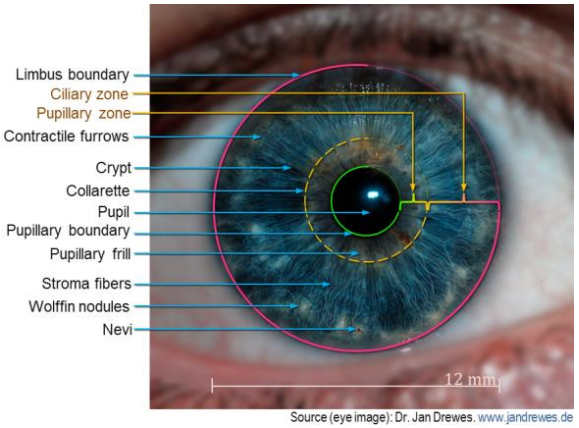




L'iride

- È il tratto biometrico più accurato
- È generalmente percepito come invasivo dagli utenti
- Presenta numerose caratteristiche stabili nel tempo e esistenti già dall'ottavo mese di vita

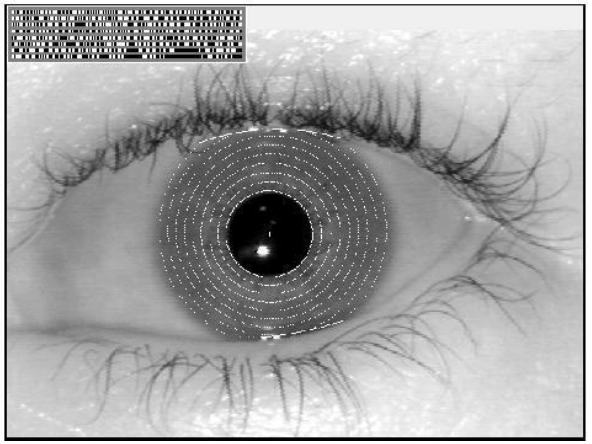


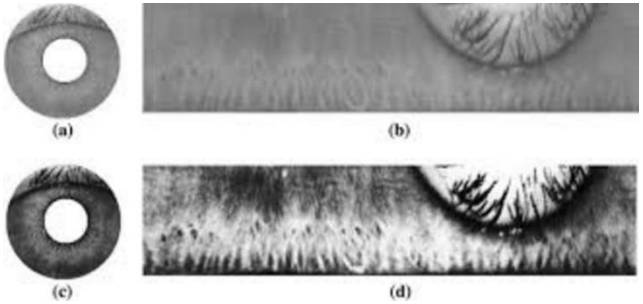


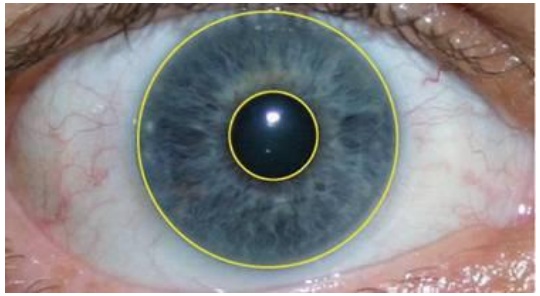
Source (eye image): Dr. Jan Drewes. www.jandrewes.de

Modalità di riconoscimento dell'iride

- Il riconoscimento prevede i seguenti step:
  - Identificazione della pupilla
  - Identificazione dell'iride
  - Rimozione di ciglia e riflessi
  - Linearizzazione dell'iride
  - Creazione dell'IRIS CODE

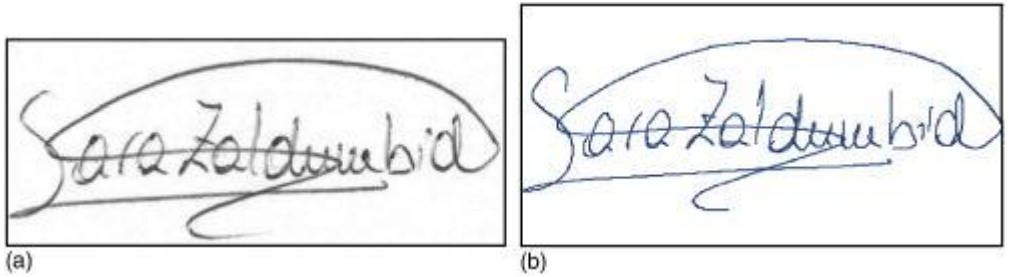






La firma

- È un metodo molto diffuso e semplice
- Presenta una bassa accuratezza
- Il costo del sensore è moderato
- Può utilizzare la firma statica e quella dinamica



La voce

- È un tratto biometrico ben accettato dagli utenti
- L'accuratezza è bassa
- Il costo è moderato
- I campioni richiedono grandi dimensioni
- La resistenza alle frodi è bassa

La soft biometrics

- Utilizza alcuni tratti biometrici che non posseggono tutte le sette caratteristiche necessarie
- Sono usualmente usati in aggiunta ai tratti biometrici classici
  - Genere
  - Colore (della pelle, dei capelli, degli occhi)
  - Peso
  - Altezza
  - Ecc.

Aspetti di privatezza

L'anello debole

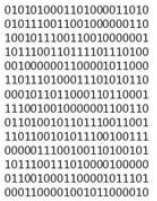
- Anche utilizzando le tecnologie biometriche rimane l'anello debole della catena di identificazione: la fonte!!!
- Un documento biometrico nasce da altri documenti tradizionali
- Non vi sarà mai una prova biometrica iniziale come primo anello della catena
- Questo è l'anello debole

Acquisizione: (template) → Documento

Campione (sample)

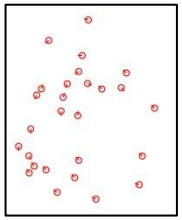
Campione (sample)

Template



Modulo di acquisizione → Controllo della qualità → Modulo di estrazione delle features → 

Tratto

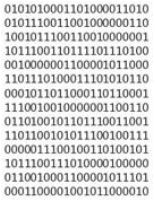


Caratteristiche (features)

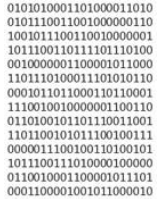
Riconoscimento: autenticazione (con CIE)

Campione (sample)

Template



1 Template



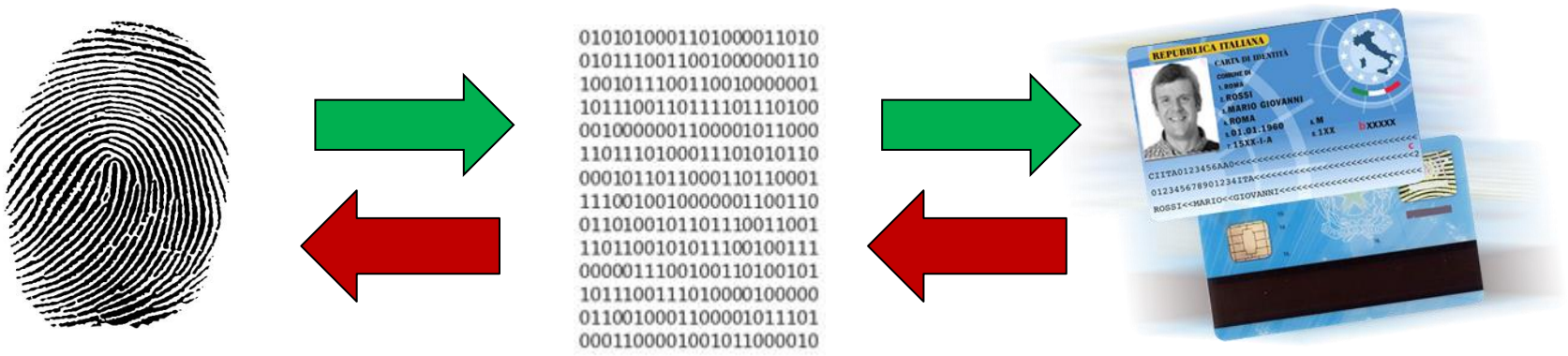
Modulo di acquisizione → Modulo di estrazione delle features → Modulo di confronto (matching) ← 

Tratto

SI / NO

C'è un problema però …

- Moltissimi studi dimostrano che dal template in molti casi è possibile ricostruire una copia molto simile del sample che lo ha generato



Lo smarrimento di un documento d'identità potrebbe determinare la compromissione del tratto biometrico

Le variazioni del tratto e la privacy

- Usare un tratto biometrico che presenta un'alta variabilità nel tempo crea molti falsi negativi (il sistema dice che io non sono io)
- Dall'altra parte protegge l'utente dall'effetto «schedatura permanente»
- In generale è corretto adattare l'invasività del tratto al reale grado di sicurezza richiesto
  - Es.: Centrale nucleare: IRIDE
  - Es.: Filiale bancaria: GEOMETRIA DELLA MANO

I miei contatti

linkedin
http://it.linkedin.com/pub/francesco-ciclosi/62/680/a06/

facebook
https://www.facebook.com/francesco.ciclosi

twitter
@francyciclosi

www
http://docenti.unimc.it/f.ciclosi
http://www.francescociclosi.it