

Tastiera, Schermi, Palmo touchless

Parte X

# Indice

<b>1</b>	<b>Biometria della digitazione della tastiera e schermi</b>	<b>2</b>
1.1	<i>Keystroke dynamics</i> . . . . .	2
1.1.1	Estrazione delle feature . . . . .	2
1.2	Swapping su schermo . . . . .	3
1.3	Comportamento dell'utente sul terminale . . . . .	4
1.4	Vantaggi e Svantaggi . . . . .	4
1.5	Attacco su canale SSH . . . . .	5
1.5.1	Contromisure . . . . .	5
<b>2</b>	<b>Impronta</b>	<b>6</b>
2.1	Biometria <i>less-constrained</i> e <i>unconstrained</i> . . . . .	6
2.2	Vantaggi e Svantaggi . . . . .	7
<b>3</b>	<b>Palmo</b>	<b>8</b>
3.1	Feature e matching . . . . .	9
3.2	2D palmprint touch . . . . .	10
3.3	2D palmprint touchless . . . . .	10
3.4	2D touchless vein palmprint (IR) . . . . .	11
3.5	Acquisizione del palmo 3D . . . . .	12
3.5.1	Sensori . . . . .	12

# Capitolo 1

## Biometria della digitazione della tastiera e schermi

### 1.1 *Keystroke dynamics*

I sistemi di identificazione basati sulla dinamica della battitura della tastiera (*Keystroke dynamics*) si basano sull'assunzione che **persone diverse battano la tastiera in modi diversi**.

L'analisi della digitazione e della firma online sono simili:

- tratti biometrici **comportamentali**
- **variabili** nel tempo e in base alle condizioni dell'individuo
- considerati **poco invasivi**
- acquisibili con sensori **economici**
- tecniche di matching simili, richiedono **allineamenti temporali**

#### Autenticazione a due fattori

La possibilità di estrarre il template direttamente intanto che viene digitato la password di fatto rende possibile una istantanea identificazione a due fattori.

#### 1.1.1 Estrazione delle feature

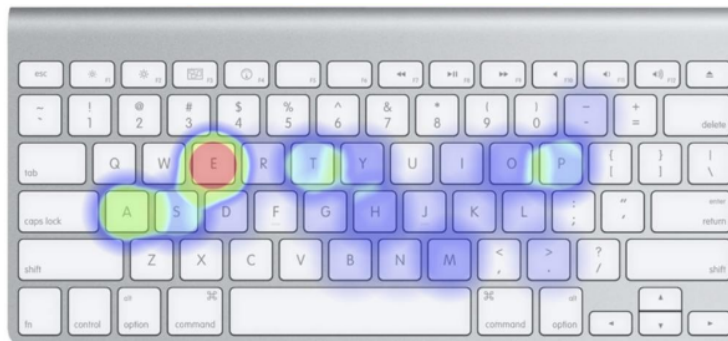
##### Feature locali

Le feature locali che si possono estrarre sono tipicamente le seguenti:

- tempo di **latenza** fra due pressioni
- tempo di **battitura** del tasto (quanto rimane premuto)

Altre feature meno interessanti, ma che possono essere usate a corredo delle precedenti, sono:

- velocità di battitura
- frequenza degli errori
- uso di *shift* o *caps lock*



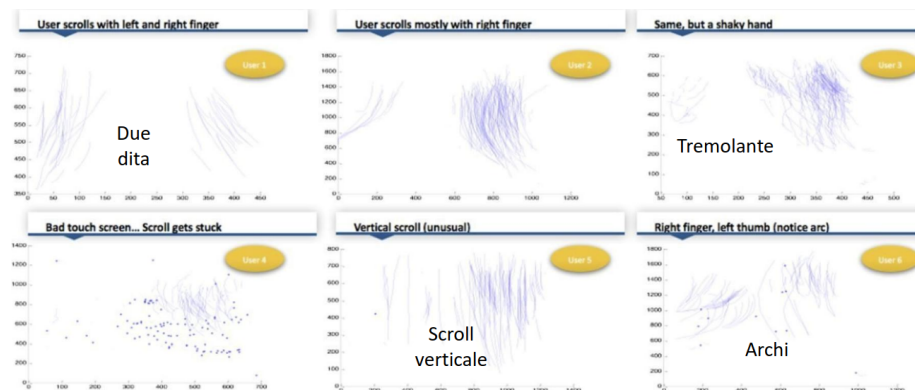
## Feature globali

Esistono anche delle feature globali, ovvero che si possono estrarre solo quando la sessione di battitura è finita.

Si tratta delle **associazioni di tasti** (ad esempio, quante viene usata la coppia ALT + TAB, o il tempo medio che intercorre tra la loro battitura).

## 1.2 Swapping su schermo

Allo stesso modo, persone diverse hanno movimenti delle dita sullo schermo diversi.



## 1.3 Comportamento dell'utente sul terminale

In aggiunta, esistono dei metodi che vanno ad identificare le persone in base al comportamento in:

- ambiente software
- rispetto al sistema operativo

Ad esempio, si può analizzare come viene usata la tastiera o il mouse, come si passa da un'applicazione ad un'altra, come si accede ai menu, ...

→ con il solo comportamento **non è sempre possibile, usando questi metodi, verificare l'identità di una persona** (troppa poca informazione). Tuttavia, è possibile ricavare informazioni utili (ad esempio, se durante il lavoro il terminale è usato proprio da quella persona o da un'altra).

## 1.4 Vantaggi e Svantaggi

- **Vantaggi**
  - Per regolare l'accesso dei terminali non è necessario un sensore, ma basta la tastiera del terminale; i sistemi sono quindi di tipo software
  - Sono considerati non invasivi (anche se lo sono per la privacy)
  - Possono essere impiegati anche senza la collaborazione dell'utente, o addirittura senza che se ne accorga
- **Svantaggi**
  - **bassa** accuratezza
  - queste informazioni possono essere usate per migliorare i tempi di **rottura delle password**
  - **cambiando tastiera**, spesso i tempi cambiano, oppure solo impugnando qualcosa con l'altra mano
  - **ferite o traumi** sulla mano possono influenzare la battitura

## 1.5 Attacco su canale SSH

È possibile perché esistono protocolli, come SSH, che trasmettono immediatamente un pacchetto ogni volta che viene premuto un tasto; in questo modo è possibile intercettare la password e i tempi di latenza.

I tempi di latenza non bastano per estrarre immediatamente la password, ma permettono ai motori di generazione delle password di ridurre i tempi di calcolo.

### 1.5.1 Contromisure

L'idea è di offuscare i dati che passano attraverso il canale SSH:

- **Randomizzazione temporale:** viene introdotto un ritardo casuale per l'invio dei pacchetti
- **Iniezioni di pacchetti *dummy*:** pacchetti vuoti o non necessari, per alterare il ritmo di trasmissione
- **Aggregazione di pacchetti:** si aggregano più pacchetti in un solo, per eliminare la correlazione diretta tra i tempi di battitura e i tempi di invio

## Capitolo 2

# Impronta

### 2.1 Biometria *less-constrained* e *unconstrained*

- *Less-constrained*
  - senza contatto
  - elevata distanza
  - condizioni di luce naturale
  - in movimento
  - ...

→ serve un minimo di cooperazione
- *Unconstrained*
  - soggetti non cooperativi
  - scenari non controllati

## 2.2 Vantaggi e Svantaggi

- **Vantaggi**

- less-constrained
- assenza di distorsioni della pelle nelle immagini delle dita
- più resistente a sporco e polvere
- maggiore accettazione da parte degli utenti

- **Svantaggi**

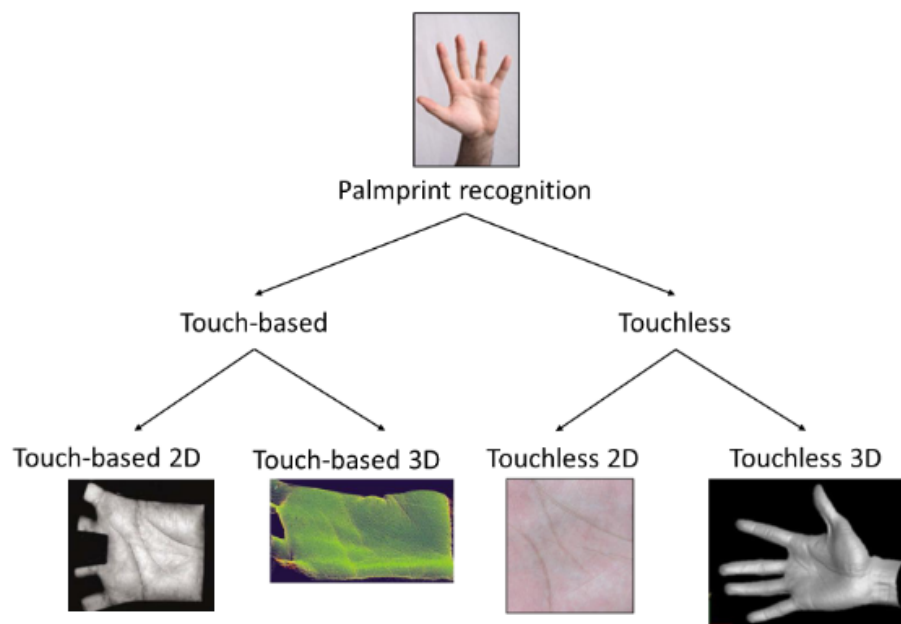
- parzialmente compatibile con i sistemi AFIS
- sfondi complessi da gestire
- sensibile ad illuminazione e posizione (vicino/lontano)
- i modelli 2D possono presentare distorsioni di tipo prospettico
- tempo di calcolo più lunghi





## Capitolo 3

# Palmo



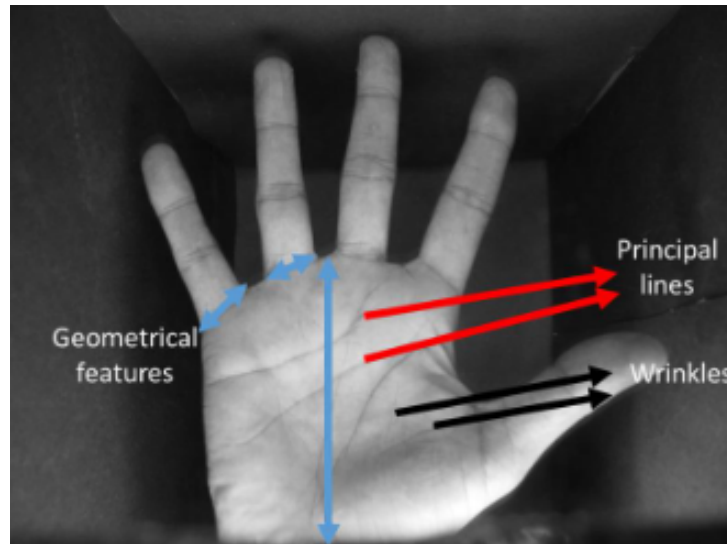
L'area di lavoro tipicamente va dal polso alla base/punta delle dita.

### 3.1 Feature e matching

Tra le feature estratte troviamo:

- Point based
  - delta points
  - se visibili, feature ereditate dalle impronte digitali
- Ridge based
  - ridge principali
- Subspace-based (globali)
  - basate su PCA
- Statistical
- Coding-based

I moduli di matching sono ad-hoc in base al modulo di estrazione delle feature utilizzato, da una semplice metrica euclidea, fino a funzioni complesse e *deep*.



## 3.2 2D palmprint touch

- approccio simile alle impronte
- spesso gli scanner sono multifunzionali e possono acquisire anche impronte a contatto
- si lasciano le tracce delle impronte sullo scanner



## 3.3 2D palmprint touchless

- tendono ad avere minore o uguale accuratezza rispetto ai sistemi a contatto
- i template estratti non sono comparabili con le tecnologie a contatto
- maggiore usabilità
- **non lascia traccia di impronte**
- tecnologie IR per vene e

### Vantaggi

- less-constrained
- risoluzioni basse
- maggiore accettabilità da parte dell'utente
- nessuna traccia sul dispositivo
- robusto a dispersione e sporco
- multibiometrico (combinazione con impronta, forma dita, forma mano, ...)

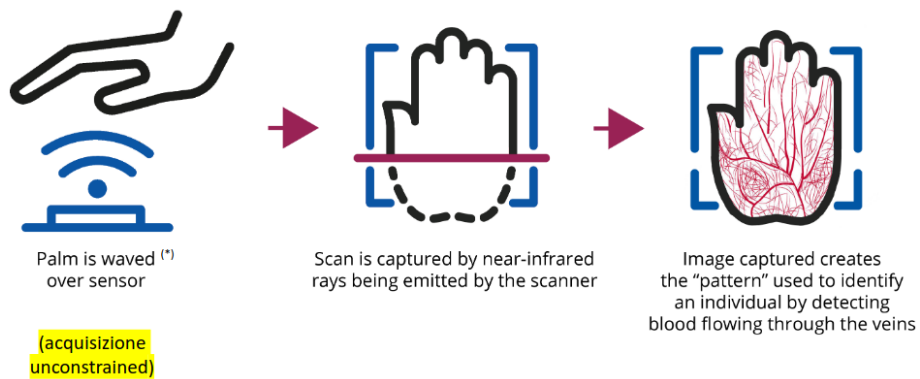
### Svantaggi

- funzionalità ad alta precisione non sempre utilizzabili (minuzie II livello)
- basso contrasto e sfondi complessi; può diventare un problema in ambiente non controllato
- sensibile all'illuminazione
- sensibile alla posizione, rischia di rendere l'immagine non a fuoco



### 3.4 2D touchless vein palmprint (IR)

Categoria particolare dove non si guardano le classiche feature di livello 1 e 2 della epidermide, ma la distribuzione delle vene visibili in infrarosso.



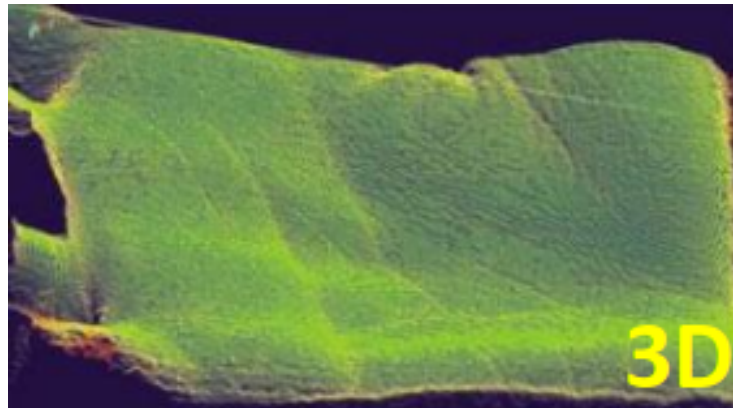
## 3.5 Acquisizione del palmo 3D

- **Vantaggi**

- robusto per illuminazione, occlusioni, rumore
- resistente ad attacchi di spoofing
- invariante a posizione e distanza
- può utilizzare anche informazioni 2D

- **Svantaggi**

- dispositivo complesso
- può essere costoso



### 3.5.1 Sensori

I sensori utilizzano:

- **touch-based**

- luce strutturata

- **touchless**

- laser
- multi-view
  - Per ottenere i dati 3D si può usare sia una telecamera che fa più acquisizioni nel tempo, sia 2 telecamere che fanno una acquisizione multipla