Stefano Rizzoli

ALTERNATIVE NON TESTUALI ALL'AUTENTICAZIONE

Tecniche Biometriche

Indice

1. Abstract

Il primo sistema biometrico risale al 1900, quando Alphonse Bertillon inventò un procedimento di identificazione dei criminali basato sull'antropometria[1] e sul fatto che l'ossatura rimane invariata dal ventesimo anno di vita.
Tutte le misurazioni erano effettuate con strumenti creati all'occorrenza ed era tenuta traccia dei tratti somatici, confrontati con modelli prestabiliti, per creare una scheda di ogni individuo.
La tecnica fallì quando furono riscontrati due detenuti con misure identiche. [Jcu]

Al giorno d'oggi i sistemi più utilizzati sono le impronte digitali, la scansione dell'iride ed il riconoscimento vocale.
Nel corso del *paper* verranno introdotti ed analizzati i principali metodi, mettendo in particolare evidenza le tecniche realizzative e le vulnerabilità risolte e quelle persistenti.

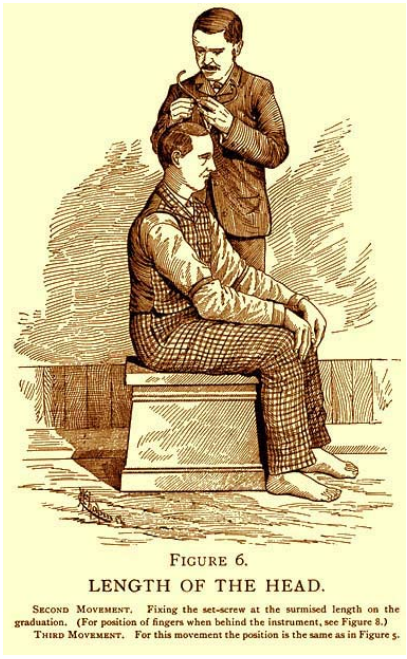


FIGURE 6.
LENGTH OF THE HEAD.
SECOND MOVEMENT. Fixing the set-screw at the surmised length on the graduation. (For position of fingers when behind the instrument, see Figure 8.)
THIRD MOVEMENT. For this movement the position is the same as in Figure 5.

Fig. 1.1. Alphonse Bertillon intento in una misurazione del cranio.

2. Introduzione: metodi di autenticazione a confronto

Il concetto di autenticazione può essere spiegato come l'identificazione di qualcuno o qualcosa: nel caso di autenticazione di persone si vuole riconoscere un utente autorizzato ad usufruire di un determinato servizio, nel caso di autenticazione di informazioni, il concetto si estende a garantire che il messaggio[2] sia stato spedito dal mittente asserente e che non sia stato sostituito o modificato. [Sim88]

Le tecniche di autenticazione si basano su tre criteri:
- Qualcosa che si conosce (i.e. password)
- Qualcosa che si possiede (i.e. smart card)
- Qualcosa che 'si è' (i.e. biometriche)

2.1. Limiti dei metodi basati su *token*

I primi due metodi hanno in comune la caratteristica di basarsi sui cosiddetti *token*, ossia qualcosa di esterno alla persona che si deve autenticare e che rappresenta la principale debolezza, in quanto può essere perso, sottratto, dimenticato, carpito o prestato a persone non autorizzate, indebolendo il sistema.
Gli svantaggi a cui sono soggette queste due tecniche possono essere originati da

[1] Lo studio statistico dei caratteri misurabili del corpo umano
[2] Per messaggio si intende il flusso di informazioni oggetto di autenticazione

una scorretta gestione del *token* (i.e. una password scelta in maniera ovvia - ossia facile da intuire; una password scritta o una smart card ceduta a terzi) o veri e propri attacchi mirati alle vulnerabilità del sistema.
Per esempio l'attacco di *eavesdropping* (o *sniffing*), cioè la visione della battitura di una password o di un codice oppure gli attacchi legati allo studio dei database delle chiavi di accesso (attacchi *offline*).

Un significativo vantaggio dei segnali biometrici è che questi sono considerevolmente più lunghi di una password o una frase di accesso, variando da alcune centinaia di bytes fino a oltre un megabyte.
In un sistema basato su password l'estensione a simili dimensioni porterebbe ad avere frasi o parole con notevoli problemi di usabilità, le biometriche garantiscono invece la stessa velocità e semplicità di un sistema con brevi chiavi di accesso.

Inoltre vi sono alcune 'scomodità' che possono portare ad uno scorretto utilizzo dei sistemi tradizionali, come per esempio la necessità di modificare le password ad intervalli regolari o la richiesta di uno strumento di accesso diverso da sistema a sistema.

Le tecniche biometriche (letteralmente: "misurazione di esseri viventi") mirano ad aggirare queste limitazioni sfruttando il rilevamento di caratteristiche umane ritenute uniche da individuo a individuo (anche se vedremo che saranno necessarie alcune assunzioni), che non possono essere prestate, rubate o dimenticate e la cui realizzazione artificiale è complessa e dispendiosa.

3. Prestazioni di un sistema biometrico

Rispetto alla verifica di una password, il confronto di diverse istanze della stessa caratteristica biometrica non è mai completamente coincidente; quando un utente si sottopone all'autenticazione viene valutato il grado di similarità fra la biometrica rilevata e l'immagine di riferimento presente nel database.
Il risultato di questo confronto è detto 'grado di similarità' (*match score*), che viene comparato alla 'soglia di accettazione' t, oltre la quale l'autenticazione è considerata avvenuta.

Vi sono tre metriche di valutazione di un sistema biometrico:

- False Reject Rate (FRR)
- False Acceptance Rate (FAR)
- Failure to Enrol Rate (FTER)

3.1. False Reject Rate (FRR)

Il tasso di falso rifiuto misura il numero di volte che un utente autorizzato viene ingiustamente respinto dal sistema e nell'autenticazione basata su biometriche corrisponde al *denial of access*.
Un FRR accade quando non vi è un sufficiente grado di similarità fra l'immagine presente nel database e quella appena catturata; le cause possono essere legate a variazioni della biometrica nell'utente (nella lettura delle impronte digitali possono

influire la condizione della pelle, eventuali ferite o i cambiamenti dovuti all'età) e portano alla ripetizione - in numero limitato - del processo di autenticazione.

$$FRR = \frac{\text{Total False Rejection}}{\text{Total True Attempts}}$$

Il falso rifiuto è solitamente compreso fra il 2% ed il 5%.

3.2. False Acceptance Rate (FAR)

Il tasso di false accettazioni misura il numero di volte che un utente non autorizzato viene erroneamente accettato dal sistema, attraverso un inesatto *matching* con un *template* presente nel database.

$$FAR = \frac{\text{Total False Acceptance}}{\text{Total False Attempts}}$$

Questo tipo di errore è molto influente negli accessi basati su biometriche e generalmente è compreso fra lo 0,1% e lo 0,5%. [KKP]

FRR e FAR sono inversamente proporzionali: se un sistema richiede un alto grado di sicurezza, la soglia t dovrà essere considerevolmente alta, eliminando la maggior parte di intrusioni di impostori ma causando un'alto tasso di *denial of access*.
Al contrario, un basso livello di t eviterà il *denial of access* ma farà aumentare la probabilità di intrusioni.

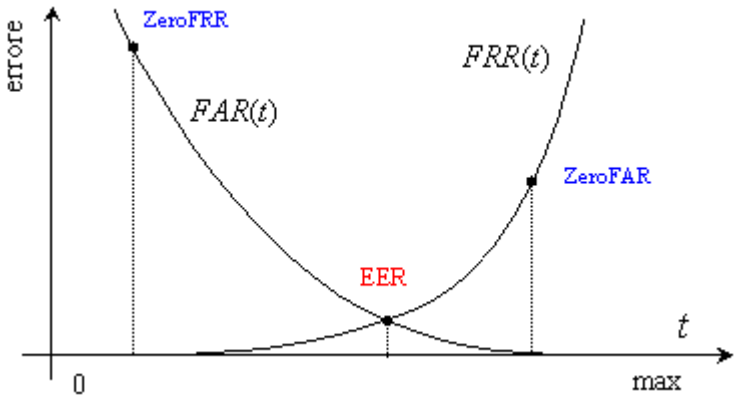


Fig. 3.1. False accettazioni (FAR) e falsi rifiuti (FRR) in funzione della soglia t di accettazione del sistema. Il EER (Equal Error Rate) è il punto in cui FAR ed FRR sono equivalenti

3.3. Failure to Enrol Rate (FTER)

Il tasso di fallimento nella registrazione è riscontrabile in due casi: da una parte corrisponde a registrazioni inefficaci a causa di errori umani che non permettono al sistema di avere sufficienti dati per l'autenticazione (i.e. una pressione eccessiva del dito sul sensore o un elevato rumore di fondo nel riconoscimento vocale), dall'altra parte comprende tutti gli utenti che non sono in grado di generare *template* efficienti e quindi non possono utilizzare questa tecnica di autenticazione.
Ciò accade perché le biometriche richiedono dati particolareggiati e sufficientemente distintivi, e se la soluzione può essere l'abbassamento della qualità in fase di registrazione, anche in questo caso si corre il rischio di compromettere il livello di sicurezza del sistema.

3.4. Termini di paragone fra biometriche

Oltre alle metriche prestabilite per la valutazione del livello di sicurezza di sistemi basati su biometriche, vi sono vari altri fattori che determinano l'usabilità e la qualità delle diverse possibili tecnologie di riconoscimento biometrico.

- ✓ **Universalità** - il grado di presenza e disponibilità della caratteristica biometrica nelle persone.
- ✓ **Unicità** - quanto una caratteristica è ritenuta unica da soggetto a soggetto.
- ✓ **Permanenza** - quanto la caratteristica biometrica alla base di un sistema rimane immutata nel tempo.
- ✓ **Accettabilità** - quanto un utente è disposto ad utilizzare una determinata tecnologia; un metodo intrusivo è certamente meno accettato di uno che rispetti maggiormente la privacy.
- ✓ **Accuratezza** - il compromesso fra False Reject Rate e False Acceptance Rate; ogni sistema può richiedere un livello diverso, in generale deve limitare entrambi gli errori.
- ✓ **Incidenza di errore** - quali cause sono alla base degli errori nella registrazione o nella verifica di un *template*.
- ✓ **Semplicità** - quanto una tecnologia biometrica è *user friendly*; quanto cioè è correttamente utilizzabile da utenti non specificatamente istruiti all'uso.

4. Verso i metodi: alcune distinzioni

Sono distinguibili due categorie di caratteristiche biometriche:

- Fisiologiche
- Comportamentali

Le prime sono quelle fisiche e stabili (impronte digitali, retina, volto, ecc), mentre per comportamentali si intendono quelle legate alla personalità di un individuo (riconoscimento della voce, della grafia, della dinamica di battitura su tastiera).
Le caratteristiche comportamentali sono più economiche di quelle fisiologiche, ma anche meno robuste, in quanto non necessariamente sono uniche da individuo ad individuo.

4.1. Inizializzazione delle biometriche

Un concetto fondamentale nella comprensione dei sistemi biometrici è quello di *template*.
Un *template* è il risultato della registrazione presso il sistema, consistente in alcune immagini ed elaborazioni matematiche delle stesse che vengono memorizzate, possibilmente criptate, quando per la prima volta un utente utilizza il sistema e sono il termine di paragone per i successivi confronti in fase di autenticazione.
E' essenziale che la qualità delle immagini sia alta, poiché interferenze come rumore o luce di sottofondo possono influenzare la cattura.
I *template* possono essere salvati sul sistema o su una smart card, rendendo in questo caso minimo il rischio di *repudiation.*
Per approfondimenti sulla strutturazione di un sistema biometrico si veda [Ril02].

5. Un metodo fisiologico: le impronte digitali

5.1. Caratteristiche biometriche

Le impronte digitali sono immutabili e permanenti negli anni e sono composte da un insieme di linee dette creste (*ridge lines*) che tracciano un disegno detto *ridge pattern*.

Le creste seguono dei percorsi caratterizzati dalle minuzie (*minutiae*), che sono i veri elementi di distinzione delle impronte digitali e sono classificabili a seconda della forma e dell'andamento in archi, spire, laghi, curve, creste isolate, attraversamenti, terminazioni e biforcazioni di creste.

In una singola impronta ci sono fino a 100 minuzie, anche se la maggior parte dei sistemi ne utilizza solo 12 per il riconoscimento.

E' molto importante sottolineare che il *template* non memorizza l'immagine delle impronte, ma un'elaborazione matematica delle minuzie. [CGN94]

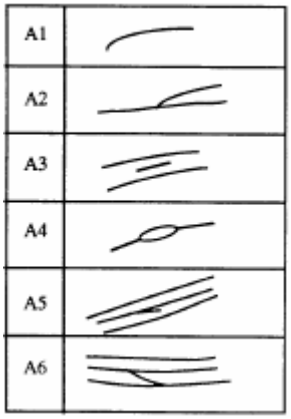


Fig. 5.1. I diversi e più comuni andamenti delle creste nelle impronte digitali

5.2. Metodi di acquisizione

L'acquisizione delle impronte digitali al giorno d'oggi differisce dalla tecnica tradizionale dell'impronta di un dito macchiato di inchiostro su un foglio di carta; esistono diversi metodi basati su sensori e scanner.

Un primo tipo di scanner utilizza un sistema ottico di lenti e prismi ed un sensore CCD in grado di rilevare i punti di contatto dell'epidermide - quindi le creste - con la superficie di lettura; in queste aree le particelle d'acqua sulla pelle assorbono la luce e rendono nera l'immagine, dove non vi è contatto la luce viene riflessa e lascia bianca l'immagine.

Un altro tipo di scanner è detto *capacitive* e consiste in una piastra di silicio con una matrice di micro-celle, ognuna delle quali è un sensore che rileva una porzione di impronta.

Questo metodo è di dimensioni più ridotte rispetto allo scanner ottico ma richiede piastrine di alta qualità per poter avere una definizione sensibile dell'immagine, una manutenzione più accurata e, da questi due fattori, un costo maggiore. [GalIta02]

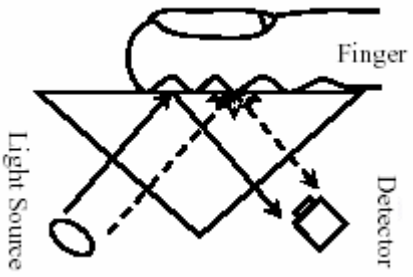


Fig. 5.2.1. Lettura dell'impronta effettuata con scanner ottico

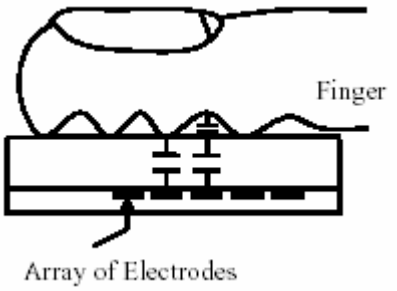


Fig. 5.2.2. Lettura dell'impronta effettuata con scanner *capacitive*

Altri sistemi prevedono l'utilizzo di sensori termici che costruiscono un ologramma secondo il calore generato dalla pelle o sensori ad ultrasuoni, ma sono tecniche ritenute ancora inaffidabili in quanto compongono in alte percentuali delle immagini errate o imperfette.

5.3. Estrazione e verifica delle informazioni

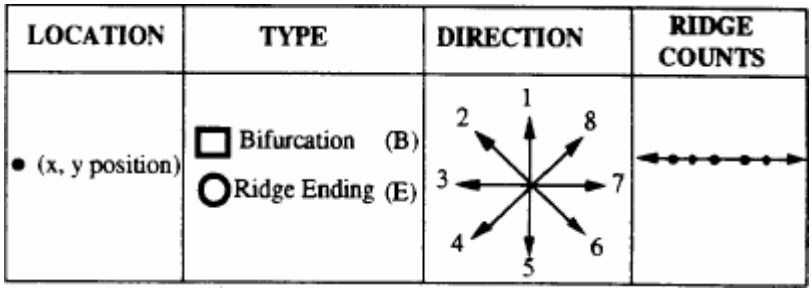
Come detto in precedenza, il template originato da questa tecnica consiste in una serie di informazioni ricavate dall'elaborazione dell'immagine acquisita, inizialmente di risoluzione 512 x 512.
Lo scopo dei diversi passi di raffinamento è determinare il tipo delle creste e la loro posizione, orientamento e quantità.

Un primo passo è la soluzione dei problemi legati alle imperfezioni dell'immagine, che si manifestano sotto forma di zone e creste non contigue e non sempre possono essere migliorate; in questi casi - anche in virtù della ridotta percentuale di informazioni che il sistema richiede, rispetto a quante una procedura ne fornisca - si scartano le aree che presentano impurità e non si considerano in fase di processamento.

Un successivo stadio consiste nel creare una mappa topologica di ogni impronta, individuando, localizzando e contando le minuzie.
Questa fase porta ad un sistema detto *Coincident Sequence* [CGN94] che cataloga le caratteristiche delle impronte secondo i campi:

- Tipo di cresta
- Locazione della cresta nell'immagine secondo le coordinate (X, Y)
- Orientamento della cresta
- Numero di creste che una linea immaginaria attraverserebbe, da una caratteristica ad un'altra (i.e. il conteggio delle creste)

#Caratteristica	Tipo*	Locazione	Orientamento*	Conteggio
1	B	150, 200	7	- 2 4 2 5 6
2	B	275, 202	6	- - 0 4 6 0
3	E	325, 277	2	- - - 5 9 1



* Fig. 5.3. Le proprietà che ogni caratteristica deve avere, secondo lo schema di *Coincident Sequence*

Per avere una sequenza corrispondente occorre che almeno quattro caratteristiche siano esaminate ed abbiano una coincidenza secondo i criteri dello schema sopra riportato e preferibilmente provengano da altrettanti quadranti dell'immagine.

Un passo successivo è detto *thinning* (sfoltimento) ed utilizza le informazioni su forma e posizione delle creste ottenute per trasformare l'immagine iniziale in un'altra priva di imperfezioni, pori e creste di diverso spessore.
Questa operazione viene eseguita da algoritmi che generalmente lavorano sulla definizione delle linee, assottigliandole mantenendone la forma; per dettagli si vedano [Kwo88, Ros76].

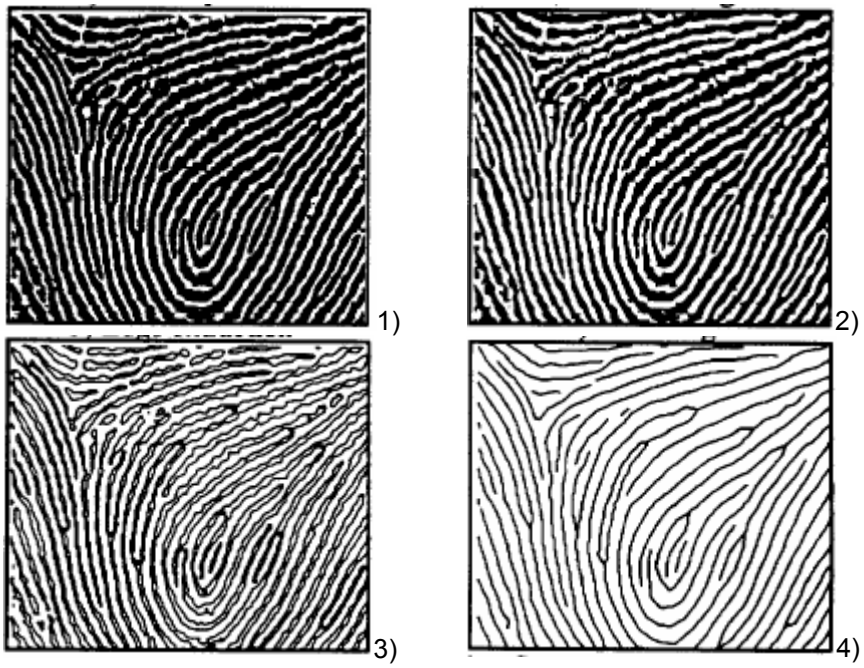


Fig. 5.4. Le fasi del processamento dell'immagine catturata: 1) l'immagine elaborata dallo scanner ottico; 2) l'immagine filtrata; 3) l'estrazione delle creste; 4) l'immagine raffinata.

5.4. Vantaggi e limiti del metodo

- ✓ **Universalità** - media.
- ✓ **Unicità** - alta: anche in gemelli monozigoti la probabilità di avere due individui con le stesse impronte digitali è di 1 su 10^{20}.
- ✓ **Permanenza** - alta: le impronte sono eterne e durature.
- ✓ **Accettabilità** - media.
- ✓ **Accuratezza** - alta: l'EER (vedi paragrafo 2.2) è basso.
- ✓ **Incidenza di errore** - influiscono sui falliti riconoscimenti di una impronta la mancanza di umidità delle dita, lo sporco ed i cambiamenti di elasticità dovuti all'età.
- ✓ **Semplicità** - alta: non serve alcun particolare posizionamento del dito sul sensore.

Va considerato che, se da un lato il sistema è in grado di lavorare solo su una bassa percentuale delle informazioni che vengono introdotte in una registrazione, dall'altro vi è il rischio di non poter effettuare operazioni di autenticazione in caso di infortunio al dito utilizzato nella creazione del *template*.
Un'ovvia soluzione è l'utilizzo, almeno in fase di registrazione, di più di un dito, per garantire la (quasi) completa disponibilità di utilizzo del sistema; in questo caso è frequente l'abbinamento della tecnica biometrica a quella delle smart card, con la

registrazione del *template* sulla carta e la verifica dell'impronta del possessore in fase di autenticazione.
Per uno studio completo sulla cooperazione dei due metodi si veda [HMNWW00].

5.4.1. Un possibile attacco al sistema di impronte digitali

Escludendo i cosiddetti attacchi di 'forza bruta', che in questo campo possono essere la violenza verso l'utente per costringerlo ad eseguire l'autenticazione - e che in altre forme saranno esaminati più avanti - un possibile ed interessante studio [Mat02] è stato condotto per testare la possibilità di creazione di una falange artificiale con le impronte digitali di un utente regolarmente registrato presso il sistema.

L'insidia sfrutta gli scanner ottici che, rispetto a quelli termici o *capacitive*, tendono a non discriminare fra dita vere e altre di silicone create artificiosamente.
Il procedimento consiste nell'ottenere subdolamente il negativo dell'impronta di un utente su di una pallina di plastica ammorbidita, stringendogli la mano o nascondendo la pallina sulla piastra di autenticazione; in seguito si versa sul calco ottenuto un liquido gelatinoso che una volta rappresosi reca l'impronta digitale e la forma di falange.

L'esperimento consiste poi nel verificare su 11 diversi sistemi con quale frequenza si riescono a distinguere i seguenti 4 casi:

1) Registrazione con dito vero - Verifica con dito vero
2) Registrazione con dito vero - Verifica con dito artificiale
3) Registrazione con dito artificiale - Verifica con dito vero
4) Registrazione con dito artificiale - Verifica con dito artificiale

Nei casi 1) e 4) la maggior parte dei sistemi ha avuto riscontro elevato, nei casi 2) e 3) le autenticazioni positive sono diminuite ma, soprattutto con scanner ottici, hanno avuto percentuali considerevolmente alte.
Per i dettagli si faccia riferimento a [Mat02].

6. Un metodo comportamentale: il riconoscimento vocale

6.1. Caratteristiche biometriche

Il riconoscimento vocale è probabilmente la tecnica biometrica più naturale in quanto non intrusiva e quindi largamente accettata dagli utenti.
Oltre ad aspetti comportamentali come l'onda acustica prodotta, le misurazioni coinvolgono anche aspetti fisiologici, come la cavità orale e la forma della laringe.
Nella rilevazione del suono il rumore di sottofondo ha un alto impatto sulla qualità della cattura ed è fondamentale la cooperazione dell'utente.

Esistono diversi criteri di autenticazione con riconoscimento vocale, fra cui metodi basati su testo (il riconoscimento si basa su una frase prestabilita), semplici e accurati ma inclini a frodi legate alla registrazione della password o all'uso di sintetizzatori vocali, e sistemi indipendenti dal testo, in cui l'accuratezza è leggermente minore, ma garantisce minore intrusione e soprattutto può essere

integrato in un dialogo, essere eseguito in parallelo ed invocato in qualunque momento.

6.2. Le fasi del riconoscimento

Indipendentemente dal criterio scelto, il processo di riconoscimento può essere diviso in diversi passi funzionali.

6.2.1. Identificazione

Si vuole determinare l'identità del parlatore in base alla sua voce, potendo riconoscere gli utenti non registrati (sistema detto aperto).
Questo processo è del tipo "molti-a-molti" e l'accuratezza dell'identificazione è inversamente proporzionale alla quantità di utenti registrati.
In questa fase il sistema può restituire una lista di n identità che maggiormente si accostano all'utente che si autentica o, altrimenti, viene implementata la possibilità di rifiutare un utente, da utilizzare in fase di verifica.

6.2.2. Verifica

In questa fase l'operazione diventa "uno-a-molti", in quanto consiste nel verificare l'identità asserita da colui che effettua il rilevamento della propria voce.
L'accuratezza di questo processo è ora indipendente dal numero di utenti presenti nel database del sistema, piuttosto è strettamente legato alla qualità del suono e del segnale prodotto.
Un accorgimento in questo senso è porre il sistema nelle stesse condizioni per tutti gli utenti: stesso tipo di microfono, stesse condizioni di rumore di sottofondo.

6.2.3. Registrazione

L'acquisizione e la creazione dei campioni della voce di un utente prevede l'inserimento di un PIN e la ripetizione della frase di accesso per 4 volte.
In analogia con le impronte digitali, le cosiddette 'impronte vocali' richiedono una quantità minima di caratteristiche per la creazione del modello, ed in generale maggiore è la quantità dei dati catturati, maggiore è l'accuratezza dell'impronta risultante.
Il discorso registrato viene segmentato all'interno del sistema in specifiche unità fonetiche divise per grado di omogeneità, per i dettagli sulla gestione e l'utilizzo dei modelli matematici utilizzati si rimanda a [BMS98].

6.3. Un'implementazione: Biometrica Conversazionale

L'identificazione basata su un discorso rientra nella categoria dei metodi di riconoscimento vocale indipendenti dal testo: vengono verificate acusticamente delle risposte date dall'utente in un dialogo con il sistema.
Le domande sono scelte a caso fra quelle precedentemente registrate e verifica ed identificazione si basano sia sul riconoscimento acustico che sulla correttezza delle risposte.
Un rilevante vantaggio di questo metodo è la scrematura dell'insieme di utenti possibili, in base alle domande e alle relative risposte, assumendo che l'utente sia collaborativo.

- *"Pronunci il suo nome"*
- "Sono John Doe"
- *"Da dove chiama?"*

- "Mi trovo a Manhattan"

Dopo una prima serie di domande il sistema può generare la lista di n-migliori candidati (si veda par. 6.2.1), oppure possono essere generate altre domande per discriminare ulteriormente.
Una seconda serie di domande invece è mirata a verificare l'identità dell'utente ponendo domande generate casualmente in base alle informazioni raccolte in fase di registrazione o durante precedenti transazioni.

Il sistema per la verifica di entrambi gli aspetti del metodo è composto da un motore di riconoscimento delle impronte vocali e un altro che, gestito dal "Verbal Indentification and Verification Agent" (VIVA server) verifica la correttezza delle risposte contenute nel database e ricevendo la decodifica del discorso dell'utente.

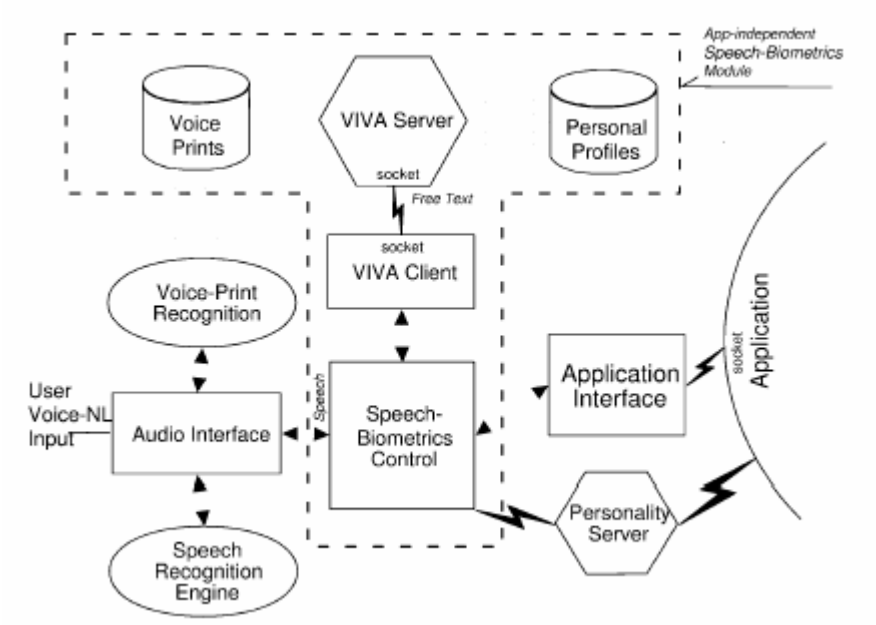


Fig. 6.1. Il sistema di Verbal Indentification and Verification Agent

Il modulo di controllo analizza il responso legato alle impronte vocali e decide se accettare l'utente, continuare la verifica sottoponendolo ad altre domande o rifiutarlo a causa di troppe risposte errate o imprecise o di una scarso *match* acustico. [BMS98]

6.4. Vantaggi e limiti del metodo

Rimanendo nell'analisi del sistema specifico presentato, un notevole vantaggio è l'utilizzo di informazioni personali e quindi note solo all'utente che si autentica, ma contemporaneamente facili da ricordare; in confronto le password non possono permettere una simile semplicità, in quanto se composte da stringhe non casuali sono semplici da indovinare o soggette ad attacchi di tipo *dictionary attack*.
In più il sistema è flessibile e dinamico: la durata della sessione di verifica può variare a seconda dell'andamento della stessa ed è trasparente e non intrusiva.
Secondo questo concetto, il grado di sicurezza è configurabile: si possono in prima istanza determinare le quote di minime risposte esatte e di massime risposte errate per ogni sessione, in aggiunta è possibile dare maggiore rilievo alla parte di valutazione acustica o di valutazione del contenuto delle risposte.

La qualità del riconoscimento vocale generico è altamente suscettibile di disturbi di sottofondo prodotti dall'ambiente o dall'utente stesso, come colpi di tosse e chiarimenti di voce.
Nel primo caso il disturbo, oltre ad inquinare il suono, può modificare anche il tono del parlatore che, per compensare il rumore, può alterare la propria voce e non essere riconosciuto.

Questo metodo, inoltre, è soggetto ai cosiddetti *replay attacks* (si veda cap. 8), che possono costringere ad utilizzare ogni volta frasi di accesso diverse.
Il sistema, ottimo in ambienti simulati, è quindi non particolarmente efficiente nell'applicazione reale, ed inoltre presenta alcune lacune dal punto di vista prettamente fisiologico, come evidenziato nei primi tre campi della seguente lista:

- ✓ **Universalità** - media.
- ✓ **Unicità** - bassa: la probabilità di trovare due soggetti con voce simile è cospicua; legare il riconoscimento vocale a fattori come domande poste dal sistema è una valida soluzione.
- ✓ **Permanenza** - bassa: la voce cambia per questioni legate allo sviluppo ma soprattutto per patologie come un semplice raffreddore o anche sbalzi di umore.
- ✓ **Accettabilità** - alta.
- ✓ **Accuratezza** - alta: tassi di FRR comuni sono tra 0,8% e 1,3%; tassi di di FAR fra il $5*10^{-12}$% e il $2*10^{-6}$%.
- ✓ **Incidenza di errore** - rumore, raffreddori e agitazione.
- ✓ **Semplicità** - alta.

7. Altre tecniche biometriche

7.1. Geometria della mano

Il sistema di verifica della geometria della mano utilizza una sorgente di luce, una macchina fotografica digitale, uno specchio ed una superficie con cinque guide per il corretto posizionamento della mano.
Nell'immagine catturata vengono incluse circa 90 caratteristiche della parte superiore e laterale della mano, come forma, lunghezza, spessore e superficie, mentre nella creazione del *template* tridimensionale del database vengono ignorati dettagli come impronte digitali, linee e segni.

Questo metodo si basa sulla modellatura della mano e garantisce un'unicità piuttosto bassa in quanto trascura le caratteristiche più significative di una mano, valutandone altre soggette a cambiamenti dovuti ad età e patologie.
D'altro canto questo sistema è uno dei più veloci (richiede appena un secondo a riconoscere un utente), utilizza *template* di meno di 10 byte ed è uno dei meno invasivi, risultando alquanto appropriato per controlli frequenti e senza particolari esigenze di sicurezza, rispettando al contempo la privacy. [Ash94]

- ✓ **Universalità** - bassa.
- ✓ **Unicità** - bassa: analizza dati piuttosto generici.
- ✓ **Permanenza** - media: dovuta all'età e a malattie, come l'artrite.

- ✓ **Accettabilità** - alta.
- ✓ **Accuratezza** - alta.
- ✓ **Incidenza di errore** - sono principali responsabili ferite, tagli ed i cambiamenti dovuti all'età.
- ✓ **Semplicità** - alta: la superficie di appoggio è come un calco per il corretto posizionamento.

7.2. Riconoscimento del volto

Questa tecnica presenta diverse implementazioni, tutte ancora in fase di sviluppo e perfezionamento.

Il metodo di riconoscimento bidimensionale usa una macchina fotografica che memorizza in un codice a barre bidimensionale alcuni dati legati alle misurazioni del volto, come la distanza fra occhi e naso, tra le tempie e fra mento e attaccatura dei capelli.

Un altro sistema si basa sulla termografia: mediante una macchina fotografica ad infrarossi viene misurata una ristretta superficie facciale - detta 'tatuaggio vascolare' - su cui è valutato il *pattern* termico originato dal flusso del sangue nelle arterie.

Le tecniche di riconoscimento facciale sono considerate inaffidabili in quanto non permettono il riconoscimento in caso di modifiche ai tratti del volto e camuffamento.

- ✓ **Universalità** - alta: sfrutta caratteristiche possedute dalla grande maggioranza delle persone.
- ✓ **Unicità** - bassa.
- ✓ **Permanenza** - media: oltre all'età, anche fattori estetici, come la barba, possono modificare i lineamenti.
- ✓ **Accettabilità** - media.
- ✓ **Accuratezza** - alta.
- ✓ **Incidenza di errore** - influiscono la luce, ma soprattutto eventuali ostacoli al rilevamento, come capelli, occhiali ed i cambiamenti dovuti all'età.
- ✓ **Semplicità** - media.

7.3. Scansione dell'iride

L'iride rappresenta per gli occhi ciò che le impronte digitali rappresentano per le mani; essa infatti è definita da una struttura unica e molto dettagliata caratterizzata da puntini, anelli, striature, solchi, corone, fibre, filamenti e mappe vascolari.
A differenza delle impronte digitali stesse, l'iride - la parte colorata dell'occhio che circonda la pupilla - è isolata e protetta dall'esterno, essendo posta dietro alla cornea e all'umore vitreo.

Il riconoscimento e la lettura avvengono con l'utente posizionato a circa un metro da una videocamera CCD che cattura le informazioni, localizzando prima il contorno esterno dell'iride, poi cercando quello interno, di confine con la pupilla, quindi realizzando tre immagini.

Come una delle principali proprietà dell'iride è la totale casualità nella formazione delle minuzie e della struttura dell'iride stessa, anche l'operazione di estrazione di

informazioni dalle immagini memorizzate nel database è legata a parametri ed operazioni stocastiche; per il metodo dei "Filtri Bidimensionali di Gabor" si rimanda a [DauDow94].

- ✓ **Universalità** - alta.
- ✓ **Unicità** - alta: anche in gemelli monozigoti la probabilità di trovare due iridi uguali è di 1 su 10^{78}.
- ✓ **Permanenza** - alta.
- ✓ **Accettabilità** - media: sebbene sia scarsamente intrusiva, in quanto non richiede contatto fisico con l'apparecchio rilevatore.
- ✓ **Accuratezza** - molto alta: test effettuati per la British Telecommunications hanno rilevato frequenze di FAR per 1 ogni 1,7 milioni di casi e FRR per 1 ogni 950 mila casi. [ErbSan99]
- ✓ **Incidenza di errore** - mancanza di luce e scorretto posizionamento.
- ✓ **Semplicità** - media: richiede un attento posizionamento al fine di evitare errori.

8. Conclusioni

L'autenticazione basata su tecniche biometriche evita, come abbiamo visto, numerose lacune di sicurezza ed usabilità dei metodi tradizionali; restano, però, alcuni difetti ai quali ne vanno aggiunti altri legati alla natura e alle implementazioni di queste tecnologie.

8.1. L'impatto del *denial of access*

Diversamente dai metodi tradizionali, le biometriche possono accettare impostori e rifiutare utenti autorizzati; questo aspetto si riflette sull'usabilità del sistema e sulla fiducia che l'utente può provare nei confronti di queste tecnologie.

Possibili strategie di riduzione del FRR (cioè il denial of access - si veda par. 3.1) sono in primo luogo l'abbinamento di più di una tecnica biometrica per stabilire l'accettazione o meno dell'utente.
Altrimenti si può agire sulla soglia su cui si basa la decisione di autenticare o rifiutare un utente: si può renderla 'dinamica' e variabile a seconda della confindenzialità (i.e. del grado di sicurezza) della transazione che si andrà ad eseguire, renderla variabile a seconda dell'abilità dell'utente di rendersi affidabile o infine creando, anziché una sola soglia, due differenti limiti e quindi tre stati dell'autenticazione: *match*, *non-match* e 'dubbio'.
Se i primi due casi sono noti, la terza possibilità si colloca fra la soglia di accettazione e quella di rifiuto e viene risolta chiedendo all'utente un'ulteriore verifica tramite l'inserimento di una password.
Questo, oltre a limitare il D.o.A., aumenta cospicuamente il livello di sicurezza. [Ril02]

8.2. Le vulnerabilità cui le biometriche sono soggette

Volendo paragonare un sistema biometrico con uno di autenticazione basato su password, le componenti possono essere riconosciute simili: scanner e sensori sono come la tastiera, il sistema di crittografia si può paragonare a quello per l'estrazione

delle caratteristiche, vi sono i comparatori di *template* e di password e questi stessi elementi risiedono nei relativi database.

Ecco quindi che gli attacchi immaginabili in un sistema tradizionale possono essere presenti anche in uno legato alle biometriche.

Per esempio l'estrattore di caratteristiche può essere attaccato da un 'cavallo di Troia' che produca un set di caratteristiche modellato dall'utente malizioso.

Altrimenti si può agire sul comparatore (*matcher*) per forzarlo a stabilire una soglia di accettazione insicura.

Altri attacchi agiscono sui canali di comunicazione fra le diverse componenti del sistema, per cui si rimanda a [BCR01]; inoltre nel paragrafo 5.4.1 è stato presentato un attacco al sensore, consistente nel presentare una biometrica (in quel caso un set di impronte digitali) finta.

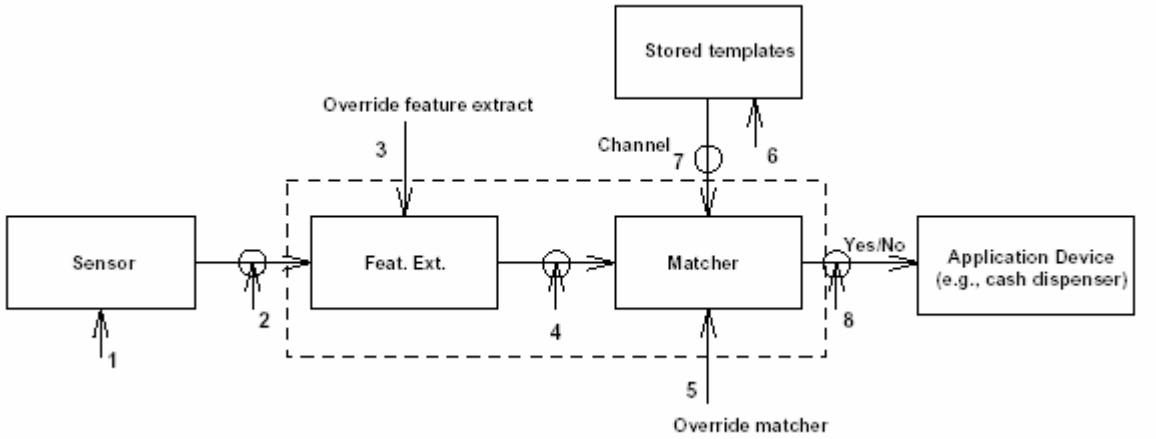


Fig. 8.1. Possibili punti di attacco in un generico sistema biometrico

Uno degli attacchi a cui però le biometriche sono più soggette è però il cosiddetto '*replay attack*', che consiste nel sottrarre un *template* al database per poi reinserirlo successivamente.

Una possibile soluzione è l'implementazione di una 'sfida' all'immagine in fase di cattura, consistente nel richiedere alcuni pixel in ingresso e restituirne altri scelti attraverso una funzione nota solo al sistema.

Oppure si possono crittografare le immagini in ingresso e arricchirle con informazioni nascoste in grado di far riconoscere al sistema quali informazioni in ingresso sono autentiche e quali no.

In conclusione, le tecniche biometriche sono una soluzione interessante, affidabile e valida, sia per chi utilizza un sistema, sia per chi si occupa di aspetti legati alla sicurezza.

Dovendo riassumere i principali vantaggi dei metodi, da un lato emerge la comodità di essere in prima persona lo strumento di autenticazione, dall'altro la possibilità di configurare il grado di sicurezza del sistema.

9. Bibliografia

[Ash94] J. Ashbourn; *Practical Implementation of Biometrics-based on Hand Geometry*, The Institution of Electrical Engineers, London, 1994.

[BCR01] R.M. Bolle, J.H. Connell, N.K. Ratha; *An Analysis of Minutiae Matching Strength*, IBM Research Center, New York, 2001.

[BMS98] H.S.M. Beigi, S. Maes, J. Sorensen; *A Frame-based Statistical Method for Speaker Recognition*, Proceedings RLA2C, 1998.

[CGN94] B.D. Costello, C.A. Gunawardena, Y.M. Nadiadi; *Automated Coincident Sequencing for Fingerprint Verification*, The Institution of Electrical Engineers, London, 1994.

[CMN01] U.V. Chaudhari, S.H. Maes, J.Navratil; *Conversational Speech Biometrics*, IBM Research Center, New York, 2001.

[DauDow94] J. Daugman, C. Downing; *Recognizing Iris Texture by Phase Demodulation*, The Institution of Electrical Engineers, London, 1994.

[ErbSan99] J.H. Erbetta, S. Sanderson; *Authentication for Secure Environments Based on Iris Scannino Technology*, 1999.

[GalIta02] E. Galli, G.F. Italiano; *Tecniche Biometriche*, Università di Tor Vergata, Roma, 2002.

[GLT02] E. Grosso, A. Lagorio, M. Tistarelli; *Understanding Iconic Image-based Face Biometrics*, DIBEV, 2002.

[HMNWW00] H.C. Ho, Y.S. Moon, K.L. Ng, S.F. Wan, S.T. Wong; *Collaborative Fingerprint Authentication by Smart Card and a Trusted Host*, IEEE, Hong Kong, 2000.

[KKP] A.T. Khader, J. Korczak, N. Poh; *The Key Concepts of Biometrics*, [http://hydria.u-strasbg.fr/~norman/BAS/key_concepts.htm]

[Jcu] “Alphonse Bertillon”, in *Pictures of Health: Body Politic*. [http://www.maps.jcu.edu.au/hist/stats/bert/]

[Kwo88] P.C.K. Kwok; *A Thinning Algorithm by Contour Generation*, Communications of the ACM, Vol. 31, No. 11, 1988.

[LiuSil00] S. Liu, M. Silverman; *A Practical Guide to Biometric Security Technology*, 2000.
[http://computer.org/itpro]

[Mat02] T. Matsumoto; *Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies - a Case Study for User Identification*, Yokohama, 2002.

[Ril02] L. Rila; *Denial of Access in Biometrics Based Authuenication Systems*, Infrasec, London, 2002.

[Ros76] A. Rosenfield; *A Note on Thinning*, IEEE Transactions on Systems, Man and Cybernetics, pp. 226-228, 1976.

[Sim88] G.J. Simmons; *A Survey of Information Authentication*, Proceedings of the IEEE, Vol. 76, No. 5, 1988.

9.1. Riferimenti iconografici

Fig. 3.1.: Tratta da Biometria.it
http://www.biometrika.it/wimages/farfrr.gif
[inserita il 21/05/2003]

Fig. 5.1.: Tratta da [CGN94]
[inserita il 23/05/2003]

Fig. 5.2.1.: Tratta da [Mat02]
[inserita il 24/05/2003]

Fig. 5.2.2.: Tratta da [Mat02]
[inserita il 24/05/2003]

Fig. 5.3.: Tratta da [CGN94]
[inserita il 23/05/2003]

Fig. 5.4.: Tratta da [CGN94]
[inserita il 23/05/2003]

Fig. 6.1.: Tratta da [CMN01]
[inserita il 27/05/2003]

Fig. 8.1.: Tratta da [BCR01]
[inserita il 29/05/2003]