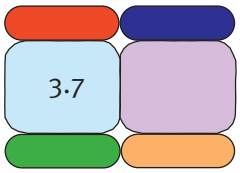
SISTEMI DI IDENTIFICAZIONE PERSONALE

Furio Cascetta
Marco De Luccia

In questo articolo vengono illustrate le principali tecniche utilizzate per il riconoscimento automatico delle persone. Per ogni tecnologia trattata (impronte digitali, riconoscimento dell'iride e della retina, riconoscimento vocale ecc.), viene descritto il principio di funzionamento, i principali vantaggi e i limiti operativi. Infine, vengono riportati i tipici campi di applicazione per ogni tipologia di identificazione personale, evidenziandone i possibili sviluppi futuri.



1. DEFINIZIONI E CLASSIFICAZIONE

Come punto di partenza è importante introdurre alcune definizioni di base e classificare la varie tecnologie di identificazione automatica - in anglosassone *AIDC technologies* (*Automatic Identification and Data Capture*) - evidenziando le loro funzioni e le specifiche capacità. Come si può osservare dalla figura 1 vi è una notevole varietà di tecnologie AIDC oggi disponibili, suddivisibili in due ampie categorie:

a. **trasporto dati (*data carriers*)**: questa categoria comprende le tecnologie finalizzate alla "raccolta, memorizzazione e trasporto" di dati e informazioni (prevalentemente codificati), su opportuni supporti. Appartengono a questa categoria i metodi ottici (principalmente i codici a barre), i metodi basati sulla memorizzazione magnetica (banda magnetica) e quelli basati sulla memorizzazione elettronica (*RFID-tag, smart card, chip, smart label* ecc.);

b. **riconoscimento di aspetti (*feature extraction*)**: questa categoria contiene a sua volta tre sottogruppi a seconda che il tipo di aspetto "estratto" si riferisca a un'immagine di un oggetto o di una persona (sistemi di visione), oppure sia attribuibile a un'azione dinamica della persona (voce, firma, andatura ecc.), oppure, infine, sia associabile a una proprietà chimico-fisica del materiale costituente l'oggetto (per esempio, i complessi composti chimici responsabili degli odori e delle profumazioni).

In questo articolo verranno trattate le principali tecnologie di identificazione delle persone, basate sul *riconoscimento biometrico* (Figura 2), e in particolare:

- *identificazione personale basata sul riconoscimento biometrico di "aspetti statici"*: cattura ed elaborazione di immagini umane (aspetti anatomici), come per esempio impronte digitali, geometria e "impronta" vascolare della mano, geometria del viso, iride, retina;
- *identificazione personale basata sul riconoscimento biometrico di "aspetti dinamici"*: timbro vocale e modo di parlare (analisi spettrale del campo sonoro), firma dinamica (pressione), digitazione (pressione), andatura (passo).

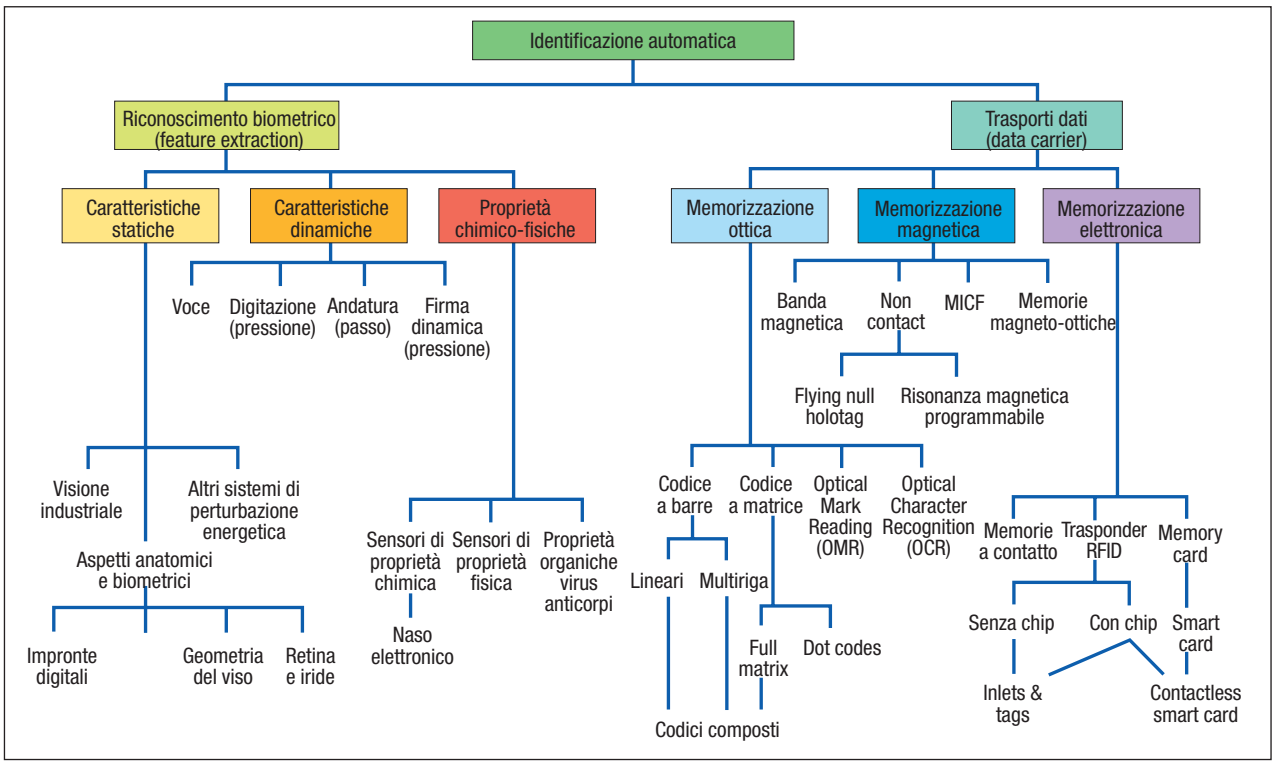


FIGURA 1

Classificazione delle tecnologie di identificazione automatica. (Fonte: AIDC, Automatic IDentification and Data Capture)

Storia della biometria

Per migliaia di anni gli uomini hanno istintivamente utilizzato alcune caratteristiche fisiche (come il volto, la voce, il portamento ecc.) per riconoscersi gli uni con gli altri. Circa a metà dell'800, A. Bertillon, capo della sezione identificazione criminali della polizia di Parigi, sviluppò l'idea di usare alcune misure del corpo umano (altezza, lunghezza delle braccia, piedi, dita, ecc.) per identificare i responsabili dei crimini. Verso la fine del XIX secolo, questa idea di partenza fu ulteriormente sviluppata grazie alla scoperta (dovuta agli studi di F. Galton e E. Henry) del carattere distintivo delle impronte digitali, ovverosia del fatto che queste individuano biunivocamente una persona. Subito dopo questa scoperta, le polizie di tutto il mondo cominciarono ad acquisire e memorizzare in appositi archivi le impronte di criminali, detenuti e sospetti. Inizialmente, le impronte erano "registrate" su supporto cartaceo, inchiostrando i polpastrelli dei soggetti in questione e realizzando il "timbro dell'impronta". Subito dopo questa fase, le forze di *intelligence* e di pubblica sicurezza perfezionarono le loro tecniche per il rilievo, sulle scene del crimine, delle impronte digitali lasciate dai protagonisti di azioni delittuose. In questi anni, la polizia comincia a fare sempre più affidamento su tecniche di indagine scientifiche, che si affiancano e quelle tradizionali (logica deduttiva) nelle investigazioni. Segni evidenti di questo nuovo "approccio scientifico" nel condurre le indagini si riscontrano anche in alcuni famosi personaggi della letteratura poliziesca (per tutti, Sherlock Holmes).
La scienza biometrica comincia, quindi, a essere impiegata nelle attività giudiziarie e anticrimine, così come in applicazioni inerenti la sicurezza di un numero sempre crescente di persone. Oggi, in piena èra digitale, un numero elevatissimo di persone utilizza tecniche di riconoscimento biometrico, non solo nel campo della giustizia, ma anche in applicazioni civili e militari. Le previsioni di alcuni analisti di mercato affermano che, entro il 2010, la maggior parte degli abitanti della Terra avrà a che fare, episodicamente o in maniera continua, con le tecniche di riconoscimento biometrico.

2. TECNICHE DI IDENTIFICAZIONE BIOMETRICA (BIOMETRIC IDENTIFICATION SYSTEMS)

Queste tecniche "intelligenti" di riconoscimento coinvolgono sistemi esperti, reti neurali, sistemi a logica *fuzzy* e lo sviluppo di sofisticate tecniche di elaborazione elettronica (*computing*). I principali vantaggi di queste tecniche, rispetto a quelle convenzionali, sono connessi alla loro capacità di ricordare e di apprendere.
Gli scienziati da tempo si sono prefissi lo scopo di progettare macchine e sistemi in grado

di emulare alcune abilità umane, tra cui quella dell'identificazione basata su riconoscimento biometrico, ovvero dell'identificazione tramite l'acquisizione e successiva elaborazione di immagini.
Le principali aree di interesse delle tecnologie biometriche sono:
- autenticazione e verifica diretta dell'identità personale (prova dell'effettiva identità dichiarata dal diretto interessato);
- identificazione indiretta di una persona per mezzo delle caratteristiche biometriche disponibili.

Le principali caratteristiche fisiologiche o comportamentali che possono essere utilizzate per l'identificazione personale devono soddisfare i seguenti requisiti essenziali (Figura 3):
- *universalità* (ogni individuo deve avere quella caratteristica);
- *unicità* (non è possibile che due persone condividano la stessa identica caratteristica biometrica);
- *permanenza* (la caratteristica biometria deve rimanere immutata nel tempo);
- "*catturabilità*" (nel senso che la caratteristica biometria deve poter essere misurata quantitativamente).

Il termine "biometrico" (*biometrics*) si addice, dunque, allo studio dei metodi automatici per l'identificazione o l'autorizzazione di persone che utilizzano caratteristiche fisiologiche o comportamentali.
Esempi di tecniche biometriche sono il riconoscimento della geometria della mano, delle impronte digitali, dell'immagine dell'iride, dell'immagine del volto, il modo di parlare, il modo di firmare.
Buoni risultati possono ottenersi anche utilizzando la combinazione di più tecniche di riconoscimento.
Esistono altre tecniche per l'identificazione personale, tra cui il confronto di immagini della retina (*retina image comparison*), confronto della traccia vocale (voice matching), confronto del DNA (*DNA matching*), ma non vengono ancora diffusamente utilizzati in virtù della loro complessità.
Ai fini di una classificazione più generale le tecniche di riconoscimento biometrico si suddividono tra quelle che implicano un rico-

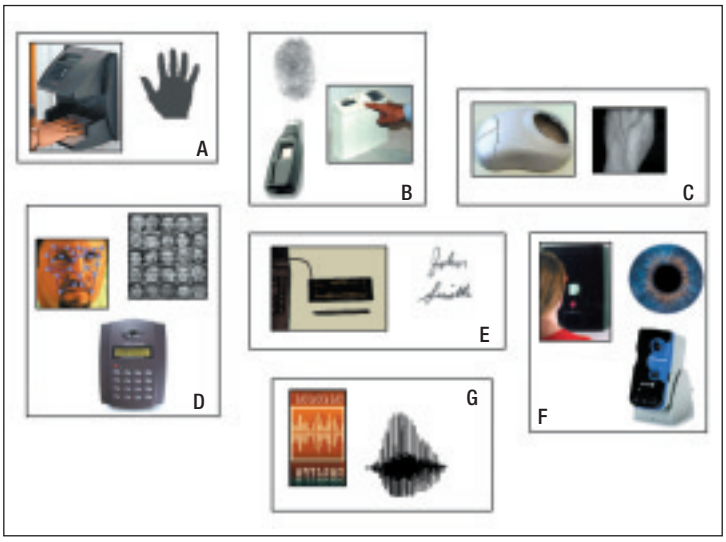


FIGURA 2
Rassegna di alcune tecnologie biometriche

Aspetto biometrico	Impronta digitale	Iride	Voce	Geometria facciale	Geometria della mano
					
Limiti alla universalità	Menomazioni o disabilità	Menomazioni o disabilità	Menomazioni o disabilità	Nessuno	Menomazioni o disabilità
Unicità	Alta	Alta	Bassa	Bassa	Media
Permanenza	Alta	Alta	Bassa	Media	Media
Catturabilità	Media	Media	Media	Alta	Alta

FIGURA 3
Confronto tra alcune tecnologie biometriche in funzione dei requisiti essenziali

noscimento biometrico di *aspetti statici* (impronte digitali, geometria della mano, del volto, dell'iride ecc.), rispetto a quelle basate sul riconoscimento biometrico di *aspetti dinamici* (voce, firma, portamento ecc.).

2.1. Identificazione personale basata sul riconoscimento biometrico di "aspetti statici"

Le principali tecniche "intelligenti" per l'identificazione biometrica tramite il rilievo di aspetti statici sono:

a. riconoscimento delle impronte digitali (*fingerprint recognition*);
b. riconoscimento del volto (*face recognition*);
c. riconoscimento dell'iride e della retina (*iris and retina recognition*);
d. riconoscimento della geometria della mano (*hand recognition*);

2.1.1. Riconoscimento delle impronte digitali (fingerprint recognition)

Usato da oltre 100 anni, il riconoscimento dell'impronta digitale è la più antica tecnica di identificazione personale. I primi studi scientifici sulle impronte digitali risalgono già ai primi del Settecento, ma i fondamenti della moderna identificazione biometria sono stati sviluppati da F. Galton e E. Henry verso la fine dell'Ottocento.

Un'impronta digitale è formata da una serie di compositi segmenti curvilinei. Fu proprio Galton, nei suoi studi, a dimostrare il carattere di unicità e di permanenza delle impronte digitali. Gli studi di Henry, invece, condussero alla prima schematizzazione della struttura globale di un'impronta digitale (il celebre "sistema Henry", per la classificazione delle impronte digitali).

Già nei primi anni del XX secolo, le impronte digitali furono accettate come valido strumento per l'identificazione personale. Ovviamente, l'identificazione manuale tramite impronte digitali è un processo lungo, tedioso e costoso. Per cui già nel 1960, da parte della polizia di Parigi e di Londra, si registrano i primi tentativi di studio per la realizzazione di un sistema automatico di identificazione delle impronte digitali.

In epoca più recente, gli studi pionieristici di Galton e Henry sono stati approfonditi e perfezionati. In sintesi, si può affermare che esistono due particolari "aspetti" che caratterizzano un'impronta digitale: i cosiddetti *punti core* e i *punti delta* (Figura 4).

Lo schema a blocchi di un sistema automatico di autenticazione dell'impronta digitale (AFAS: *Automatic Fingerprint Autentication System*) è rappresentato in figura 5. L'*input* al sistema AFAS è l'immagine dell'impronta digitale e l'identità dell'individuo corrispondente; l'*output* è una risposta SI/NO. Il sistema AFAS confronta l'immagine in input con

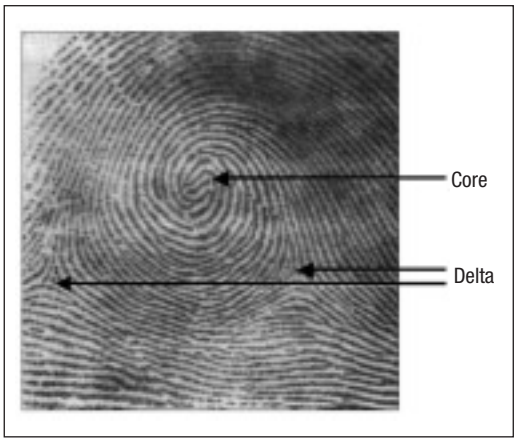


FIGURA 4
Analisi di un'impronta digitale: i punti "core" e i punti "delta"

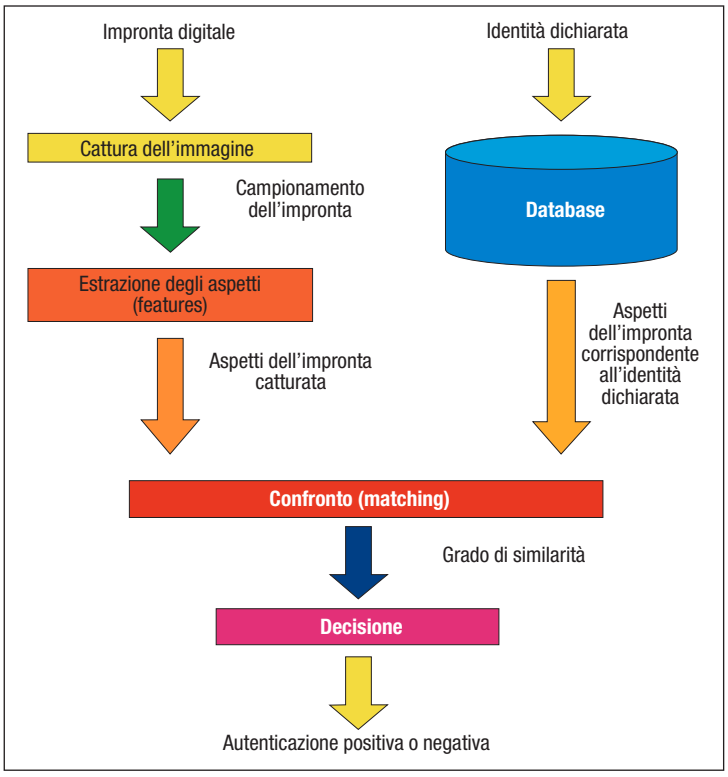


FIGURA 5
Schema a blocchi di un sistema automatico di verifica (autenticazione) dell'impronta digitale (AFAS)

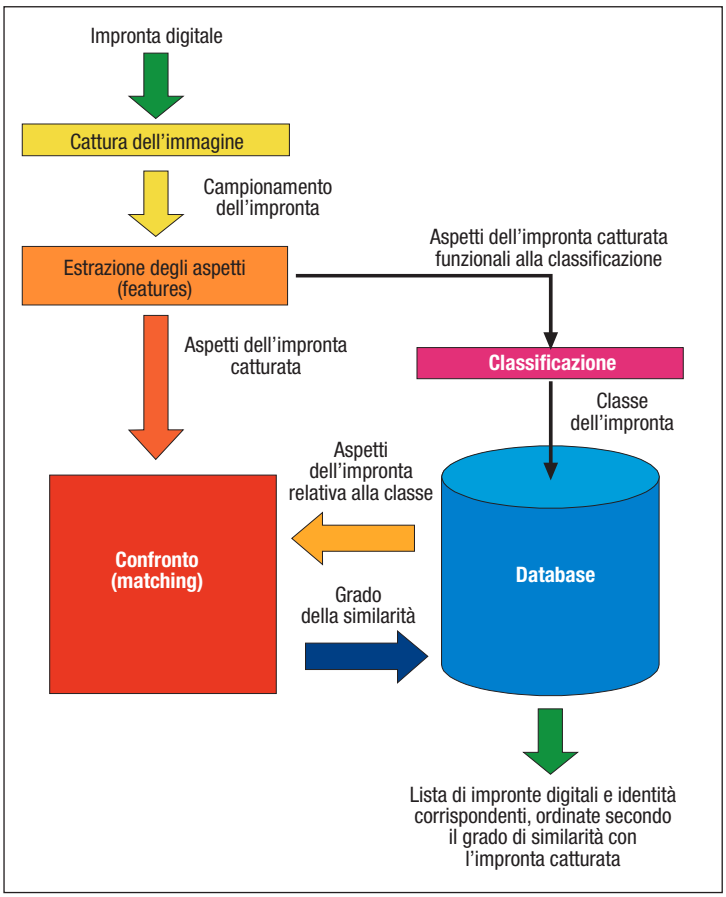


FIGURA 6

Schema a blocchi di un sistema automatico di identificazione dell'impronta digitale (AFIS)

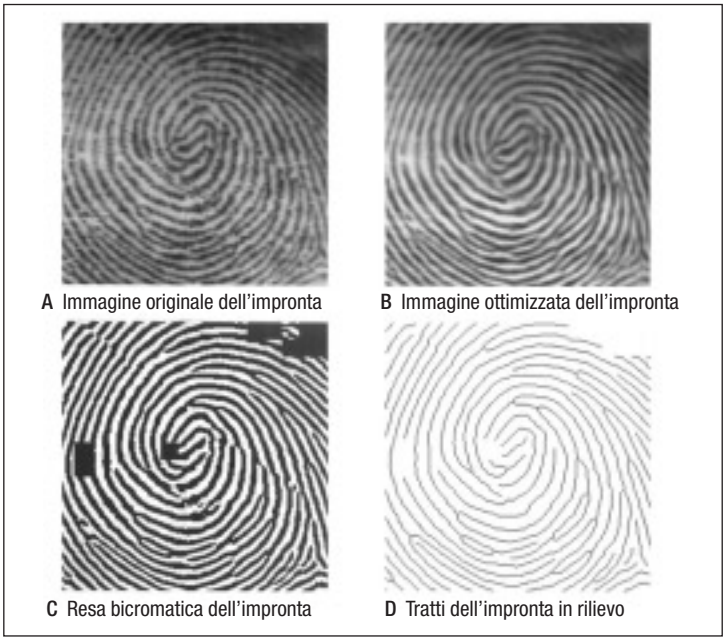


FIGURA 7

Esempio di scansione e di elaborazione elettronica di un'impronta digitale

un'immagine di riferimento memorizzata nell'archivio (*database*) delle identità.
Al contrario, in un sistema AFIS, *Automatic Fingerprint Identification System* (Figura 6) l'input è costituito unicamente dall'impronta digitale e l'output è rappresentato da una lista di identità di persone di cui si dispone registrata l'immagine dell'impronta (nel *database*) con un "punteggio", per ogni identità, che indica la similitudine tra le due impronte digitali.
Il più antico e conosciuto metodo per "catturare" l'immagine delle impronte digitali è quello di spalmare dell'inchiostro sui polpastrelli del soggetti e di realizzarne l'impronta come se fosse un timbro. L'immagine che ne scaturisce può risultare, ovviamente, molto distorta e, quindi, poco attendibile.
Risultati migliori si possono ottenere con sistemi digitali come, ad esempio, l'acquisizione dell'immagine attraverso una microcamera che realizza una scansione (*scanning*) dell'impronta digitale. Anche in questo caso, però, è possibile ottenere immagini distorte a causa della secchezza della pelle, sudore, sporco o umidità. Tipicamente, l'immagine acquisita è a elevata risoluzione (circa 500 dpi).
Una volta acquisita l'immagine dell'impronta digitale (Figura 7), occorre provvedere alcune complesse elaborazioni elettroniche e informatiche (*fingerprint image processing*).

1. *Riconoscimento degli aspetti*: l'impronta viene rappresentata come un'alternanza di segmenti "solchi" e di "valli", intervallate da discontinuità, dette *minutiae*. Lo stesso Galton definì quattro tipi di *minutiae*, successivamente perfezionate e implementate.
2. *Classificazione delle impronte*: ai fini della classificazione delle impronte digitali, esistono quattro diversi approcci:
   - sintattico (*syntactic approach*);
   - strutturale (*structural approach*);
   - rete neurale (*neural network approach*);
   - statistico (*statistical approach*);
3. *Confronto tra impronte digitali*: il confronto è il processo di comparazione e misura di similitudine tra le geometrie di due immagini di impronte digitali. I principali approcci di confronto sono il confronto puntuale e quello strutturale.

2.1.2. Riconoscimento del volto (*face recognition*)

Il riconoscimento del volto è il metodo innato utilizzato dagli uomini per riconoscersi gli uni dagli altri. Le tecniche di riconoscimento del volto, rispetto ad altre tecniche biometriche, presentano il vantaggio di essere non invasive, ovvero di richiedere poca o nulla cooperazione, non essendo soggette a eventuali modifiche di comportamento (volontarie e involontarie) da parte dell'individuo (passivo) sottoposto a riconoscimento.

Grazie alla buona accettabilità da parte degli individui, la tecnica di riconoscimento del volto (*Facial Recognition Technology*) è diventata abbastanza popolare negli USA a partire dalla metà dagli anni '90. Da un punto di vista tecnologico, oltre ai recenti successi dei componenti *hardware* per l'acquisizione delle immagini (microcamere digitali a elevata risoluzione), significativi progressi sono stati ottenuti anche nel campo dello sviluppo dei *software* di riconoscimento.

Le principali tecnologie impiegate nel riconoscimento del volto sono:

- la tecnologia PCA (*Principal Component Analysis*),
- la tecnologia LFA (*Local Feature Analysis*),
- le reti neurali.

In funzione del tipo di applicazione, i sistemi di riconoscimento del volto devono essere progettati e realizzati a seconda del tipo di atteggiamento assunto dall'individuo, che possono essere di tre tipi:

1. *cooperativo*: il soggetto è motivato a utilizzare il sistema per farsi riconoscere e accedere, attraverso appositi varchi (portali, tornelli, porte ecc.), alle aree consentite;
2. *non cooperativo*: se il soggetto è distratto o comunque non si preoccupa né di favorire né di ostacolare il riconoscimento;
3. *ostile o reticente*: quando il soggetto si attiva per evitare il riconoscimento e assume comportamenti evasivi.

Il volto umano è composto da un complesso set di "immagini multidimensionali". Da un punto di vista biometrico, il riconoscimento del volto non è caratterizzato da un'elevata *permanenza*: le molteplici espressioni del volto, l'età, i radicali cambiamenti nel *look* (capelli, barba, baffi ecc.), la presenza di occhiali, sono esempi di caratteri esteriori che possono mutare nel tempo rendendo difficoltoso il riconoscimento facciale. Le caratteristiche "non permanenti" del volto, implicano una notevole complessità di problemi tecnici da risolvere. Ciò nonostante, sono state sviluppate con successo alcune tecniche che consentono di conseguire soddisfacenti e pratici risultati di identificazione personale (*Personal Identification*) a prezzi accessibili.

Oggi le tecniche di riconoscimento del volto vengono utilizzate principalmente in *modalità verifica*, confrontando l'immagine del volto del dichiarante (acquisita in diretta) con quella pre-registrata nel sistema. In modalità identificazione l'impiego è limitato ai piccoli *database*.

2.1.3. Riconoscimento dell'iride e della retina (iris and retina recognition)

Un'ulteriore tecnica di identificazione personale (PI) utilizza la caratteristica visibile dell'iride umano. L'iride è la porzione anulare colorata dell'occhio che circonda la pupilla scura (nera) e racchiusa nei tessuti bianchi del bulbo oculare (*sclera*) (Figura 8). Un sistema di riconoscimento dell'iride richiede un apparato di cattura dell'immagine dell'occhio (anche una tradizionale camera CCD: *Charge Coupled Device*, ovvero "dispositivo

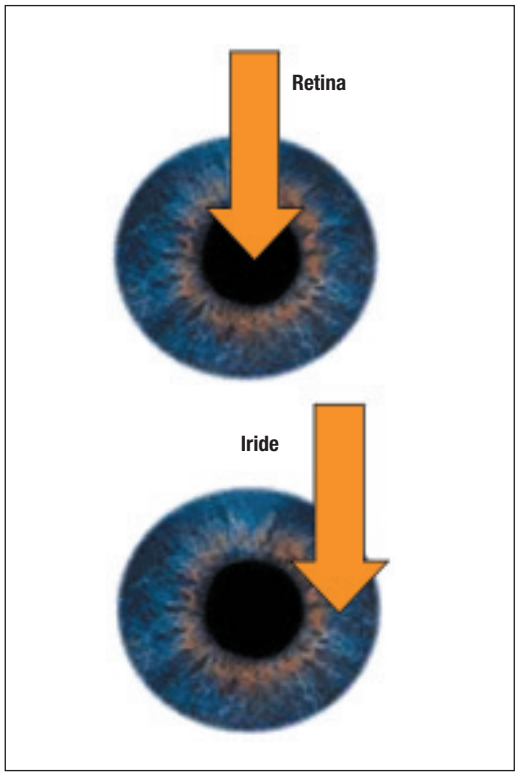


FIGURA 8
Riconoscimento dell'iride e della retina

ad accoppiamento di carica") e l'utilizzo di appropriati *software* che tramite algoritmi isolano e trasformano la porzione dell'iride in elementi caratteristici dell'identità (detti anche "sagome" o *template*).
L'iride umano è composto da tessuti elastici connettivi che si sviluppano completamente già nell'ottavo mese di gestazione. Il colore dell'iride spesso cambia durante il primo anno di vita, sebbene studi clinici hanno dimostrato che una volta stabilizzato il colore assunto dai tessuti dell'iride si mantiene inalterato per tutta la vita. L'iride è relativamente immune dai disturbi ambientali, ad eccezione della risposta istintiva della pupilla alla luce. Un aspetto molto importante, che lo rende particolarmente adatto per l'identificazione biometrica, è che l'iride di ogni individuo possiede una serie di dettagli e di particolari con spiccati caratteri di unicità.
Il riconoscimento dell'iride è una delle poche tecnologie che ben si adatta a essere utilizzata nella "modalità identificazione"; dotata di buona accuratezza viene impiegata principalmente nelle applicazioni di sicurezza. Richiede una certa collaborazione da parte dell'individuo per la cattura di un'adeguata immagine; non essendoci contatto fisico tale tecnologia è fondamentalmente non invasiva.
Il *riconoscimento biometrico della retina* si basa sull'unicità del suo schema vascolare. Già nel 1930 due oftalmologi scoprirono che ogni occhio umano possiede uno schema vascolare unico e stabile nel tempo (non muta durante tutta la vita dell'individuo).
Il sistema é ancora poco utilizzato: ad oggi, vi è un unico produttore di sistemi di scansione della retina. La retina è localizzata all'interno dell'occhio, nella sua parte posteriore. Uno speciale *scanner* illumina la retina, attraverso la pupilla, con una luce nell'infrarosso (IR) e memorizza le informazioni dalla riflessione del contrasto vascolare.
La scansione della retina viene considerata un'eccellente e accurata tecnica di identificazione personale; grazie alla sua "invulnerabilità" è un sistema molto efficace nei casi in cui è richiesta un'assoluta sicurezza nel controllo degli accessi. La tecnologia non è di facile impiego e richiede sia personale esperto, sia la partecipazione dell'individuo da identificare. Viene considerato un metodo piuttosto invasivo, poiché di solito le persone preferiscono evitare un dispositivo che interagisca con i loro occhi, in quanto lo percepiscono come potenzialmente pericoloso. Ciò rappresenterà un limite all'impiego finché non si riuscirà a realizzare una scansione della retina in maniera più *friendly*.
Il riconoscimento biometrico della retina funziona in maniera soddisfacente sia in modalità verifica (autenticazione), sia in modalità identificazione. Questa tecnica, rispetto alle precedenti è piuttosto costosa. In applicazioni dove è necessaria un'estrema sicurezza viene utilizzata e tollerata, mentre non si addice ad applicazioni che coinvolgono il grande pubblico.

2.1.4. Riconoscimento della geometria della mano (hand recognition)

Un sistema di riconoscimento della geometria della mano misura le caratteristiche fisiche (geometriche) della mano (palmo e dita) dell'individuo. La tecnologia principale impiega una telecamera digitale per catturare la *silhouette* dell'immagine della mano, sia il dorso sia il palmo. Alcune misure geometriche (dimensionali, tipo lunghezze, distanze, angoli ecc.) della mano dell'individuo vengono calcolate dal sistema attraverso le immagini acquisite. Il sistema non considera, ovviamente, i dettagli della superficie della pelle (come le impronte digitali).
Sebbene questa tecnologia sia utilizzata con un certo successo da circa 20 anni, è ancora piuttosto dibattuto l'aspetto della "unicità" della geometria della mano: secondo alcuni esperti, infatti, la geometria della mano non è ricca di elementi identificativi univoci così come le impronte digitali o l'iride. Anche l'aspetto della "permanenza" è discusso, poiché molteplici possono essere le cause di insidiose instabilità e cambiamenti nel tempo (età, malattie, incidenti).
Per questi motivi, il riconoscimento della geometria della mano meglio si adatta a esser utilizzato in "modalità verifica" (autenticazione). Considerata un buon compromesso tra prestazioni e facilità d'uso, questa tecnologia viene ritenuta invasiva, poiché richiede un contatto fisico con la mano dell'individuo.

2.2 Identificazione personale basata sul riconoscimento biometrico di "aspetti dinamici"

La categoria degli aspetti biometrici di natura dinamica include l'aspetto che, tradizionalmente, è riconosciuto come uno dei caratteri salienti della persona: la voce. Il *riconoscimento della voce* (*voice recogniton*) è, da sempre, una delle forme principali e più naturali di identificazione dell'individuo interlocutore (si pensi alla storia delle comunicazioni a distanza, prevalentemente basate sulla trasmissione della voce). La sua trasposizione nell'ambito dei processi automatici incontra, quindi, il massimo grado di accettabilità da parte degli utenti, superiore anche alla cattura della geometria del volto e nettamente al di sopra delle altre più intrusive tecnologie biometriche.
Tuttavia, il motivo di questa familiarità con i metodi di riconoscimento vocale è anche la causa principale della loro media accuratezza. La voce umana, infatti, è l'unica tra le caratteristiche biometriche a presentare, oltre a una connotazione tipicamente fisiologica, una sensibile influenza comportamentale legata allo stato psicologico dell'individuo, tale da compromettere entro certi limiti il carattere di unicità dell'impronta vocale. Anche elementi di carattere comportamentale propri della voce (quali velocità ed inflessione della parlata) possono comunque contribuire a un processo di riconoscimento vocale.
La metodologia principale finalizzata all'individuazione dell'impronta vocale di una persona consta nell'analisi del contenuto in frequenze delle onde acustiche risultanti dal flusso d'aria generato nei polmoni, propagato attraverso il condotto tracheale e portato in risonanza dalle corde vocali. Se, da un lato, rumore ambientale e sensori microfonici radicalmente diversi possono condizionare drasticamente l'efficienza del sistema di registrazione e verifica dell'impronta vocale, dall'altro va osservato che le metodologie di riconoscimento della voce possono essere facilmente implementate e gestite, in presenza di risorse tecnologiche esistenti nella maggior parte delle strutture informatizzate.
Un ulteriore limite del riconoscimento vocale, che rende questa tecnica biometrica adeguata e conveniente per sistemi di *verifica e autenticazione* di persone in strutture con un numero contenuto di "utenti registrati" nel database, sta nella permanenza del timbro vocale, modificabile nel lungo termine per l'età o degrado fisiologico, nel breve termine per stress, fenomeni influenzali e allergie.
Va citata, infine, la metodologia di *riconoscimento della firma* (*signature recogniton*), che condivide con il riconoscimento vocale la connotazione dinamica e la perturbazione dovuta alla condizione emozionale della persona. Dall'approccio originario, che prevede la stima degli scostamenti degli aspetti geometrici della firma dal modello registrato, si è passati e metodologie evolute e, appunto, "dinamiche" che tengono conto di altre caratteristiche di esecuzione quali la velocità, la traiettoria, l'accelerazione e, infine, la modulazione della pressione durante la scrittura.

3. ESEMPI DI APPLICAZIONI DEL RICONOSCIMENTO BIOMETRICO

Come già detto in precedenza, le tecnologie di riconoscimento biometrico possono supportare due differenti logiche: la verifica/autenticazione e l'identificazione.
Nella modalità *verifica/identificazione* il sistema automatico valida l'identità dichiarata da una persona comparando le caratteristiche biometriche catturate (*feature extraction*) con dati e le informazioni biometriche pre-registrate nel database del sistema (*template*). Si parla, in questo caso, di *riconoscimento positivo*.
In un sistema automatico tradizionale per l'autenticazione della persona, l'individuo che desidera essere riconosciuto dichiara la sua identità mediante un codice identificativo personale, numerico o alfanumerico (*PIN, login* o *userID*). Questo codice tipicamente viene immesso manualmente nel sistema, tramite digitazione su tastiera o tramite lettura da un supporto di tipo magnetico o "smart card" (*data carriers*) in possesso del soggetto stesso. L'autenticazione è demandata alla verifica della corrispondenza dell'identità dichiarata con una *password*, o *altro codice di accesso*, immessa nel sistema in un secondo momento e compatibile con il livello di accesso richiesto dall'utente.

FIGURA 9

Controllo degli accessi tramite riconoscimento biometrico

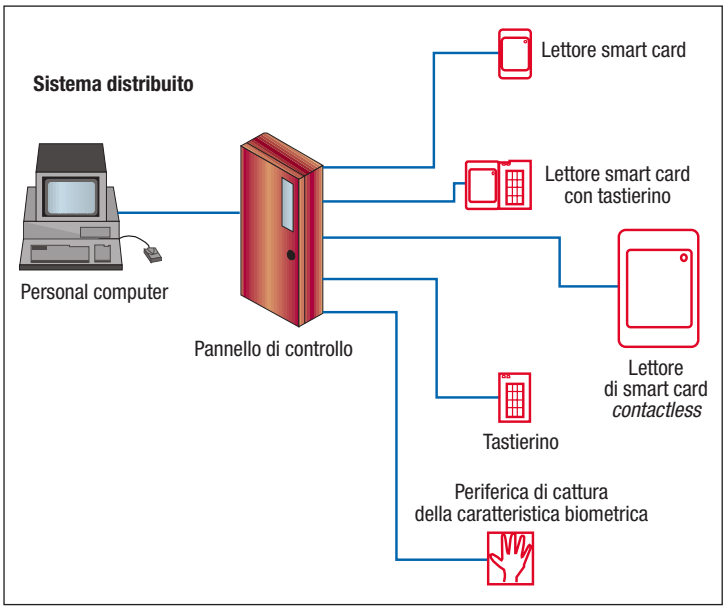


FIGURA 10

Architettura tipo di un sistema di controllo degli accessi tramite identificazione biometrica

Rientrano nei sistemi tradizionali di accreditamento personale le tessere *bancomat*, le *smart card* GSM con *codice di accesso*, le carte di credito ecc.. In tutti questi esempi, l'identità dichiarata dal titolare viene verificata mediante confronto tra da dati immessi nel POS o telefono cellulare e i corrispondenti dati memorizzati nell'archivio telematico. La trasmissione dati tra la postazione periferica (POS o cellulare) e il database centrale avviene mediante connessione telefonica.

Il punto debole di questi metodi di verifica/autenticazione personale è la loro frodabilità, dovuta al fatto che il codice di accesso o password può essere trafugato o dedotto, e quindi utilizzato fraudolentemente da terzi, evidentemente malintenzionate.

Per limitare e mitigare frodabilità, e quindi per migliorare la sicurezza dei sistemi di verifica dell'identità, si possono integrare le tecnologie tradizionali con quelle del riconoscimento biometrico.

Infatti, il criterio informatore per aumentare la sicurezza negli accessi fisici (di persone) o a sistemi remoti (Internet, Intranet, reti telematiche aziendali ecc.) consiste nel sostituire ai codici di accesso alfanumerici le caratteristiche biometriche (*biometric feature*), strettamente identificative del titolare. Per esempio, aspetti fisici come l'impronta digitale o la conformazione dell'iride connotano la persona in maniera inequivocabile e di difficile contraffazione.

Nel seguito, vengono presentate le principali applicazioni delle tecnologie di identificazione biometrica.

❏ *La sicurezza nel controllo degli accessi fisici e informatici* (banche, tribunali, uffici giudiziari e di polizia, impianti militari, settori strategici di industrie, uffici brevetti, R&D -*Research & Development*- ecc.): è possibile realizzare ingressi con tornelli o *gate* di accesso (porte scorrevoli ad apertura automatica), figura 9, inserendo *badge* magnetici in appositi lettori e validando l'identità tramite l'estrazione di una caratteristica biometrica (impronta digitale, iride, geometria della mano) (Figura 10). Oltre all'accesso fisico, l'identificazione biometrica può essere utilizzata per accreditare personale addetto all'utilizzo dei terminali dei sistemi informativi protetti: in questo caso, le postazioni remote sono attrezzate per l'inserimento di smart card e per l'estrazione e l'elaborazione di aspetti biometrici;

❏ *L'accreditamento a servizi o presso istituzioni* (*firma digitale e firma biometrica*): secondo la legislazione italiana (D.P.R. n.513 del 1997 e relativi Regolamenti Attuativi) la *firma digitale* è un sistema che sigla e attesta l'autenticità di un documento trasmesso per via informatica (Internet, posta elettronica, reti locali, memorie portatili ecc.). La firma digitale sta avendo una certa diffusione per tutto ciò che riguarda i rapporti tra il privato e la Pubblica Amministrazione (per esempio, l'art. 31 del-

la Legge 340/2000 prescrive che tutta la documentazione che le imprese devono inviare alle Camere di Commercio sia elettronica e munita di firma digitale), e si prevede che a breve potranno essere usate anche per le transazioni tra privati. La firma digitale, che in realtà è un software di criptatura, viene rilasciata da apposite società dette *certificatori*, autorizzate dall'Autorità per l'Informatica nella Pubblica Amministrazione. Il certificatore comprova l'identità dell'utente e provvede a creare un *certificato di identità* e due *chiavi* personali (una *privata* e una *pubblica*) inserendole in una smart card che riporta in memoria i dati per l'identificazione. Per attivare la smart card l'utente dovrà digitare un codice segreto. Oltre alla smart card, il certificatore fornisce un lettore da collegare a un PC e il relativo software di firma. Il programma ricava dal testo una serie di caratteri (*impronta*) usando una procedura chiamata *funzione di hash* e, usando la chiave privata, esegue la cifratura dell'impronta. Il destinatario del documento deve aver installato lo stesso software; egli riceve l'impronta cifrata, la chiave pubblica (che può solo decifrare e non criptare) e il documento. Egli applicherà la funzione di hash al documento e confronterà il risultato con l'impronta inviatagli (decifrata usando la chiave pubblica); solo in caso di corrispondenza dei due risultati si certifica la paternità e l'integrità del documento (Figura 11). Si sta pensando, per incrementare la sicurezza di accreditamento telematico, di utilizzare alcune caratteristiche biometriche del titolare (firmatario del documento) registrate nella smart card, per avvalorare l'autenticità dei documenti informatici, e delle transazioni commerciali di una certa importanza, veicolati tramite Internet. In questo ambito, si possono considerare molteplici applicazioni, dalla trasmissione di documenti giudiziari in rete, a garanzia dell'identità del giudice estensore, alle varie forme di *banking* e commercio elettronico (*e-commerce*).

❑ *L'anticontraffazione dei documenti d'identità*: la crescente esigenza di sicurezza ha portato molti Stati, tra cui l'Italia, a realizzare documenti d'identità elettronici. Vari progetti pilota sono in atto sia per quanto riguarda le carte d'identità che i passaporti. Le smart card sono in grado di memorizzare, nell'apposito *chip*, molte più informazioni rispetto ai tradizionali dati anagrafici. In questo caso, le tecnologie dei data carriers possono supportare l'inserimento di impronte digitali o immagini di iride/retina, rendendo molto efficiente e sicuro il riconoscimento del titolare, tradizionalmente affidato alla fotografia che accompagna i dati anagrafici. Al di là degli aspetti puramente tecnici, questi sistemi di controllo delle persone sono, da un lato, particolarmente sicuri, dall'altro pongono dei problemi di carattere etico assai dibattuti, inerenti la "schedatura" dell'individuo e i suoi possibili impieghi contrari al rispetto della *privacy*.

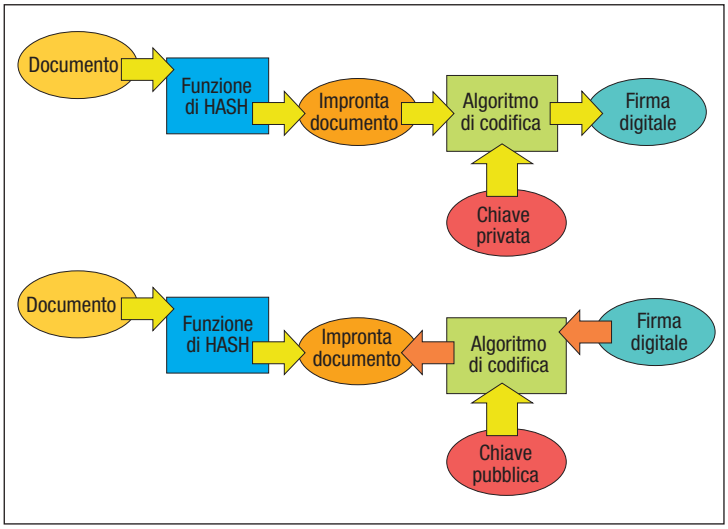


FIGURA 11
Schema logico della "firma digitale"

A tal proposito va ricordato che nel dicembre 2003 è stato presentato presso l'aeroporto di Fiumicino (Roma) il nuovo prototipo di ***passaporto elettronico***. Si tratta all'apparenza di un comune passaporto, nella cui copertina è stato inserito (non visibile all'esterno) un chip che contiene i dati anagrafici, le impronte digitali e la foto del suo possessore. Scopo principale del passaporto elettronico è quello di evitare le contraffazioni dei documenti, potenzialmente pericolose per la sicurezza del Paese: falsificare un documento cartaceo è indubbiamente più facile che riprodurre un chip con microprocessore. Presentandosi alla frontiera, il viaggiatore dovrà poggiare il passaporto elettronico su un apposito dispositivo di lettura, che innanzitutto verificherà che i dati e la foto riportati in stampa sul documento coincidano con quelli registrati nella memoria del chip. Successivamente, il possessore del passaporto dovrà posare il dito indice della mano destra su un altro lettore: in tal

La risposta alla crescente esigenza di sicurezza internazionale e di gestione delle problematiche dell'immigrazione, da parte delle principali organizzazioni internazionali si è tradotta in un significativo impulso allo sviluppo coordinato di tecnologie per la realizzazione di documenti di viaggio a lettura automatizzata o ***passaporti elettronici*** (*e-passport*). Le diverse realtà nazionali, tra le quali la Comunità Europea, hanno prodotto dei protocolli di sviluppo allo scopo di convogliare le risorse progettuali dei fornitori di tecnologia verso le esigenze valutate prevalenti ai fini della sicurezza nell'autenticazione della persona e dell'anticontraffazione del documento di viaggio.
Le linee guida dello sviluppo di e-passport, comuni per le principali realtà nazionali, sono da individuare nell'adozione di memorizzazione elettronica del dato biometrico su smart card, tecnologia *contactless* di lettura del dato, integrazione di un motore per la crittografia del dato direttamente nella smart card. Gli aspetti tecnologici dettagliati, al di là dei citati elementi fondamentali, oltre che i tempi e le modalità di realizzazione, vengono suggeriti in maniera diversa dai differenti enti e istituzioni. La Comunità Europea, che ha stanziato nel 2003 ingenti fondi per uno studio di settore, ha proposto come indicazione di ricerca per i Governi Nazionali la soluzione costituita da un chip inserito nel passaporto contenente impronte digitali e scansioni retinali. Il Governo Italiano ha recepito le indicazioni comunitarie, portando in fase avanzata il progetto citato nel presente articolo, che ha previsto la realizzazione di un impianto, presso l'aeroporto di Fiumicino di autenticazione automatica mediante la lettura in RF di dati biometrici (l'impronta digitale), memorizzati in un chip contenuto nella copertina cartonata del passaporto, da confrontare con l'impronta catturata in tempo reale presso il *gate* aeroportuale.
Se la scelta di un sistema integrato, costituito da chip e antenna e caratterizzato dalla necessaria flessibilità per essere inserito nel tessuto semirigido della copertina del passaporto, accomuna il Governo Italiano a quello degli Stati Uniti, anche in ambito europeo diverse realtà nazionali hanno optato, forse per differenti esigenze di 'percezione' della lettura elettronica, per l'inserimento nel passaporto tradizionale di una tasca dedicata all'alloggiamento della smart card contenente il dato biometrico.
Nell'area istituzionale delle Nazioni Unite, l'ICAO (*Internationa Civil Aviation Organization*) ha suggerito l'impiego di *chip contactless* inseriti nel supporto cartonato e contenenti, come *feature* biometrico, l'immagine del volto della persona: in merito al formato dell'immagine (del volto come dell'impronta digitale), l'organizzazione internazionale si è espressa in maniera contraria alla compressione del dato in JPEG o JPEG 2000, non in uso nei database biometrici, come pure alla vettorializzazione dello stesso in "*template*", per ovviare alla confusione dovuta alle molteplici tecnologie proprietarie per l'estrazione di "*template*" biometrici e relativa lettura. Sul versante dei produttori di *hardware*, la richiesta di *smart card chip* per documenti di viaggio rappresenta una significativa opportunità di mercato in alternativa ai settore trainanti (i sistemi di telefonia GSM e le carte di credito elettroniche, che però interessano prevalentemente l'area europea, per le differenti esigenze tecnologiche nell'accreditamento del terminale telefonico o del pagamento elettronico espresse negli Stati Uniti). È ovvio, quindi, che i principali produttori di smart card rispondano con interesse alle richieste di tecnologia per la realizzazione del passaporto elettronico. La proposte più concrete e affidabili convergono sull'adozione di chip con 64 kbytes di memoria base (al posto dei più diffusi con 32 kbytes), in grado di impiegare 20 Kbytes per conservare l'immagine del volto, 10 kbytes per una prima impronta digitale, altri 10 kbytes per una seconda e i restanti per i dati alfanumerici relativi alla persona e il *software* di gestione. Soluzioni *high end* prevedono, per la smart card, da configurazioni con 300 kbytes di ROM e 128 kbytes di EEPROM fino a 400 kbytes di "sola" EEPROM. La funzione di verifica crittografica del dato biometrico memorizzato può essere effettuata direttamente dalla smart card, se dotata di opportuno *core* di calcolo dedicato.
Il prodotto integrato di massimo livello tecnologico non può che nascere dalla *partnership* tra il produttore di smart card chip e quello del supporto cartonato con l'alloggiamento per il chip, oltre che con la società di sviluppo del codice di crittografia, tale da garantire una catena produttiva efficiente e soprattutto tracciabile in ogni suo stadio.

modo, viene verificato che le impronte digitali catturate "dal vivo" coincidano con quelle registrate sul chip. L'introduzione del passaporto elettronico richiederà ovviamente risorse economiche e tempo, poiché dovrà coinvolgere tutte le Prefetture che dovranno essere dotate di idonee apparecchiature per la registrazione dei dati sul chip inserito nel passaporto. Anche tutti gli aeroporti internazionali dovranno avere gli appositi dispositivi di lettura. Secondo le previsioni del Ministero degli Esteri, i primi documenti della nuova generazione saranno distribuiti verso la fine del 2004. Da un punto di vista del rispetto della *privacy*, tale sistema con verifica diretta "on-site" (senza l'impiego di un database centrale) tra i dati memorizzati sul chip e quelli catturati presenta minori problemi di accettabilità, in quanto il titolare del passaporto detiene il possesso esclusivo dei propri dati biometrici.
In tutte le suddette applicazioni, l'autenticazione avviene attraverso l'acquisizione in diretta di un aspetto biometrico (impronte digitali, iride, ecc.) e la sua verifica, o in locale (pre-memorizzazione su smart-card) o in remoto, attraverso l'accesso al database centrale.
Accanto alla verifica/autenticazione, va citata anche la procedura di *identificazione*, nella quale il sistema automatico confronta l'aspetto biometrico in ingresso con tutti i template memorizzati nel database, senza alcuna dichiarazione d'identità da parte dell'individuo. Questa modalità implica consultazioni di archivi e database anche di notevoli dimensioni. Le applicazioni sono prevalentemente nel campo della giustizia e della pubblica sicurezza (polizia e *intelligence*): da un rilievo di impronta digitale catturata sulla scena di un crimine, è possibile risalire al potenziale criminale andando a interrogare il database dei soggetti schedati. Tale tecnica di identificazione (detta *negative recognition*) viene utilizzata per restringere il campo dei possibili responsabili di un atto criminoso, da milioni di individui a qualche centinaio. Il sistema informatico, infatti, esclude dalla lista dei so-

spetti tutti gli individui "schedati", la cui impronta è palesemente difforme da quella in oggetto. Le impronte giudicate simili e raggruppabili in classi, concorrono a formare sottoinsiemi ridotti, attribuendo a ogni impronta un punteggio (*score*) di similitudine con quella oggetto della ricerca.

4. CONCLUSIONI

L'evoluzione tecnologica dei sistemi di identificazione automatica è in una fase di crescita significativa soprattutto in termini di flessibilità e affidabilità applicativa, lasciando intravedere nella attuale realtà "digitale" una graduale apertura verso campi di applicazione sempre più numerosi, che un tempo richiedevano necessariamente l'intervento e la discrezionalità dell'operatore umano. La strada tecnologica, dunque, può portare in tempi brevi verso obiettivi di maggior sicurezza e semplificazione dei processi in una moltitudine di applicazioni. Tuttavia, al di là dei settori che interessano la sicurezza fisica delle persone, delle comunità e degli Stati, l'elemento moderatore dell'applicabilità dell'identificazione personale è certamente la tutela della *Privacy*. Le recenti reazioni che i consumatori americani hanno espresso, attraverso le loro associazioni, contro gli sviluppatori di tecnologie in grado di tracciare anche soltanto i prodotti preferiti dal singolo individuo nella distribuzione commerciale (mediante l'impiego di *trasponder* in radiofrequenza, ormai soprannominati "spychip"), lasciano intendere come la gestione dell'identità personale e l'accreditamento automatico possano ancor più facilmente essere percepiti come un abuso, quando non strettamente legati alla *security*. La cautela, nell'implementazione dei sistemi di identificazione personale, e la cura del grado di invasività percepita, non solo fisica ma anche nella gestione del dato raccolto, diventano determinanti per le diverse tecnologie di *auto-ID* disponibili, forse più della loro affidabilità ormai consolidata.

Bibliografia

[1] Ashbourn J.: *Biometrics: Advanced Identity Verification, The Complete Guide*. Springer, London, 2000.

[2] Campbell J.: Speaker Recognition: A Tutorial. *Proceedings of the IEEE*, Vol. 85, n. 9, September 1997, p. 1437-1462.

[3] Daugman J.: High Confidence Visual Recognition of Persons By a Test of Statistical Independence. *IEEE Transactions on Pattern Analysis and Machine Intellegence*, 1993, p. 1148-1161. http://www.labs.bt.com/library/papers/PAMIpaper/PAMIpaper.html. Last accessed: 30 July 2001.

[4] Daugman J.: *Wavelet demodulation codes, statistical independence, and pattern recognition*. Institute of Mathematics and its Applications, Proc. 2nd IMA-IP, 2001, p 244-248.

[5] Jain A., Bolle R., Pankanti S., editors: *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, Boston, 1999.

[6] Jain L.C., Halici U., Hayashi I., Lee S.B., Tsutsui S., editors: *Intelligent biometric techniques in fingerprint and face recognition*. CRC Press, Boca Raton – Florida - USA, 1999.

[7] Prabhakar S., Pankanti S., Jain A. K.: *Biometric Recognition: Security and Privacy Concerns*. IEEE Security & Privacy, March-April 2003, p.33-42.

[8] Zhang D.: *Automated Biometrics Technologies and Systems*. Kluwer Academic Publishers, Boston, 2000.

FURIO CASCETTA, professore ordinario presso la Facoltà di Ingegneria della Seconda Università di Napoli. Studioso ed esperto di sistemi di misura, di automazione e controllo, da più di venti anni collabora attivamente con le principali associazioni di categoria del comparto, con i più prestigiosi centri di ricerca nazionali e internazionali del settore e con gli organismi di normazione (sia a livello italiano che europeo).
Dirige la collana editoriale *Misure e Automazione* per l'editore Franco Angeli (Milano).
Collabora a progetti di Alta Formazione, oltre che con l'Università di Napoli, anche con altri Atenei nazionali, tra cui il MIP-Politecnico di Milano, il Politecnico di Bari, l'Università di Palermo, e l'Università Mediterranea di Reggio Calabria.
È autore, o co-autrore, di circa 100 pubblicazioni scientifiche (sia su riviste nazionali che internazionali) e di numerosi libri scientifici , didattici e divulgativi.
fcascett@unina.it

MARCO DE LUCCIA, ingegnere meccanico, da anni collabora con l'area "misure ed automazione" dell'Università di Napoli "Federico II" e della Seconda Università di Napoli. Esperto e appassionato ricercatore nel settore delle nuove tecnologie ICT applicate ai sistemi di misura e telecontrollo. È coautore di articoli tecnici e divulgativi su riviste scientifiche del settore.
marco.deluccia@fastwebnet.it