Università degli Studi di Pavia

Facoltà di Ingegneria

Dipartimento di Informatica e Sistemistica

Biometrica per la Sicurezza

Relatore:
Chiar.mo Prof. Marco Ferretti

Tema di Laurea
di Fabio Bossi

Anno Accademico 2001/2002

A mia madre,
che ha sempre creduto in me ...

A mio padre,
sempre nei miei pensieri ...

Ringraziamenti

Desidero rivolgere un sentito ringraziamento al Prof. Marco Ferretti per avermi dato la possibilità di approfondire questo argomento di tesi e per avermi indirizzato durante il percorso.

Ringrazio l'Ing. Federico Guerrini per la disponibilità e la competenza.

Grazie a tutti i compagni del Laboratorio CAD che sono stati piacevole compagnia in questi mesi.

Sommario

Prefazione

La crescente richiesta di sicurezza, derivante anche dai recenti accadimenti a livello mondiale, ha portato in primo piano la necessità di utilizzare tecniche di identificazione dell'individuo che superino i limiti delle metodologie di riconoscimento impiegate fino ad oggi. In particolare si cerca di creare un legame stretto fra l'individuo e le autorizzazioni che gli sono connesse. Questo obbiettivo è oggi perseguibile utilizzando le caratteristiche fisiche della persona, così da poter sopperire ai problemi connessi alla sicurezza per cause dipendenti dai comportamenti della persona stessa o da azioni fraudolente.

Struttura

Questo lavoro si prefigge l'obiettivo di chiarire quali siano le motivazioni che introducono l'uso di tecniche biometriche per l'accesso a sistemi protetti, in sostituzione a quelle di uso tradizionale, focalizzando l'attenzione su quelle tecniche che, compatibilmente con la possibilità di implementazione su larga scala, permettono l'identificazione dell'utente. Viene infine effettuata un'analisi dell'introduzione della biometrica per usi legali e vengono prospettate possibili applicazioni nella nostra società.

Nel primo capitolo si introducono le motivazioni che spingono verso un approccio biometrico nel settore della sicurezza e le problematiche che ne derivano.
Nel secondo capitolo si effettua una panoramica sulle principali tecniche biometriche, introducendo la possibilità di loro combinazioni al fine di ottenere un miglioramento delle prestazioni.

Nel terzo capitolo si approfondiscono due particolari tecniche biometriche, il riconoscimento dell'impronta digitale e il riconoscimento dell'iride, che attualmente sono ritenute le migliori candidate per l'implementazione di sistemi di identificazione su larga scala.

Nel quarto capitolo si vagliano le possibilità di combinare la chiave biometrica con la firma digitale, mostrando quali sono i problemi di carattere legale e mettendo in luce le problematiche inerenti la privacy.

Nel quinto ed ultimo capitolo si presentano alcune implementazioni di sistemi di sicurezza realizzate utilizzando tecniche biometriche, si prospettano possibili scenari futuri e vengono fatte alcune considerazioni sulle prospettive di sviluppo.

1 Introduzione alla biometrica

L'identificazione personale ai fini di consentire un accesso controllato ad informazioni, luoghi o sistemi a chi ne è effettivamente autorizzato, è stata attuata nel tempo utilizzando varie tecniche. Tradizionalmente i sistemi di verifica si sono basati su ciò che si possedeva o ciò che si sapeva. Questi meccanismi si sono concretizzati ai giorni nostri nell'uso di carte magnetiche e a chip in un caso, di PIN e password nell'altro. Tali metodologie presentano però evidenti punti di debolezza, differenti a seconda della scelta del mezzo di autenticazione: possibilità di furto o di perdita per i primi, di dimenticanza o di scoperta per i secondi. Per tutte queste tipologie esiste inoltre il problema del prestito non autorizzato che abbassa notevolmente il grado di sicurezza generale. Un ulteriore limite si può individuare nelle condizioni valutate. Le tecniche di accesso tradizionale consentono di verificare se l'utente abbia le "carte in regola" per accedere al sistema e non se effettivamente lo stesso ne sia autorizzato.

1.1 Sistemi biometrici

L'idea dei sistemi biometrici è di spostare l'attenzione sull'accertamento di chi è la persona che sta richiedendo un certo servizio, e di verificarne quindi l'effettiva autorizzazione. Tali passi inoltre devono poter essere attuati in modo automatico, minimizzando l'intervento di personale specializzato. Questo meccanismo viene implementato tramite misurazioni e confronti delle caratteristiche biologiche dell'individuo con altre precedentemente registrate e convalidate. Possiamo

distinguere tali caratteristiche a seconda della particolare natura in due campi principali: fisiologico e comportamentale.
Diamo ora un'idea della tipologia di elementi che vengono presi in considerazione nei due tipi di approccio:

1. Caratteristiche biometriche fisiologiche
   - Impronte digitali.
   - Retina/iride.
   - Mano.
   - Volto.
2. Caratteristiche biometriche comportamentali
   - Voce.
   - Grafia.
   - Stile di battitura.

Si rilevano inoltre due tipi di impieghi differenti per un sistema biometrico: l'identificazione e la verifica. La prima consiste nel determinare se l'impronta biometrica di una persona può essere associata ad una di quelle presenti nell'archivio, la seconda cerca di determinare se corrispondono l'impronta biometrica della persona in esame e l'impronta individuata in archivio tramite la dichiarazione di identità della persona stessa.

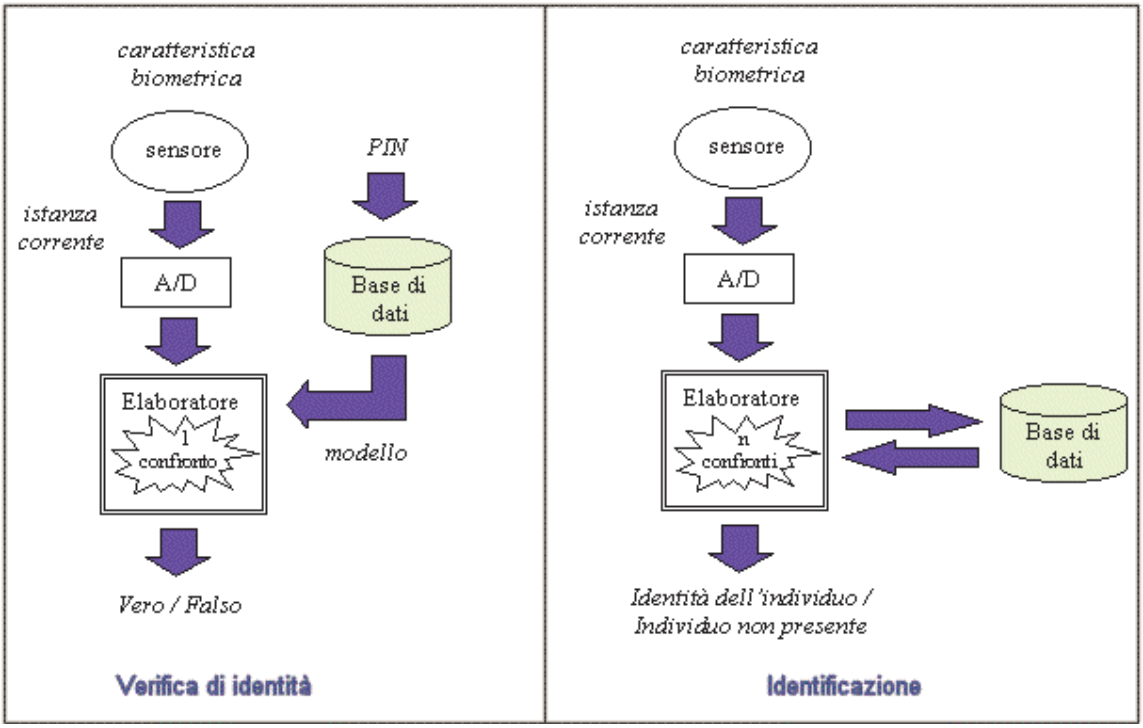

Figura 1.1 Schema del processo di verifica e di identificazione [BKA]

Osservando il differente schema di gestione nel diagramma di *Figura 1.1*, si può notare come nell'identificazione si faccia uso di uno schema di confronto uno a molti, mentre nella verifica sia sufficiente quello uno a uno. Ne consegue direttamente che le specifiche sulle caratteristiche rilevate e quelle sui sistemi di calcolo saranno differenti. Non tutte le impronte biometriche sono in grado di permettere l'identificazione a causa della diversa capacità di essere discriminanti; inoltre anche quelle che sono adatte alla verifica, a volte costringono a lavorare su un database contenuto, sia per garantire la capacità di riconoscere rilevazioni di individui differenti, sia per fornire una risposta in tempi accettabili.

1.2 Modello biometrico ideale

Le peculiarità fisiche o i comportamenti che potrebbero essere considerati accettabili per la realizzazione di un modello biometrico devono idealmente prendere in considerazione le seguenti proprietà:

- Universalità: la caratteristica biometrica da valutare deve essere posseduta da tutti i membri della popolazione.
- Unicità: ogni firma biometrica deve differire da quella di ogni altro membro della popolazione.
- Invarianza: la firma digitale non deve variare nelle diverse condizioni di rilevamento e nel tempo.
- Misurabilità: le caratteristiche dovono essere misurabili quantitativamente e facilmente ottenibili.
- Performance: si riferisce all'accuratezza di riconoscimento raggiungibile e alle risorse necessarie per il conseguimento.
- Accettazione: in riferimento al grado di accettazione del sistema di rilevazione biometrica da parte dei membri della popolazione.
- Robustezza: quanto il sistema biometrico si presta a tentativi di accesso fraudolento.

1.3 Cosa misurare?

La maggiore differenza tra un sistema biometrico e un sistema ad accesso tradizionale è il tipo di risposta che viene fornita a seguito di un'interrogazione. Immettendo una password il sistema deve verificare la corrispondenza esatta e dare una risposta di tipo booleano: si (chiave esatta), no (chiave sbagliata). Nella acquisizione di un'impronta biometrica, a causa di fattori esterni e tecnologici, si presenteranno delle differenze tra la registrazione e i rilevamenti successivi che rendono necessaria una risposta di tipo probabilistico. Un sistema biometrico ci dice quindi quanto la rilevazione corrente è simile a quella salvata nel database. Il

problema immediatamente successivo è l'identificazione della soglia su cui il sistema dovrà operare le scelte di accettazione o rifiuto dell'impronta biometrica. Le diverse tarature verranno operate a seconda che ci si trovi in necessità di alta o bassa sicurezza.

1.4 Struttura generale del modello biometrico

Ogni sistema biometrico possiede una struttura che può essere così schematizzata:

1. **Fase di registrazione (enrollment).**

   Si acquisiscono una o più istanze della caratteristica biometrica da cui si estrae un modello che viene registrato nel database del sistema. Queste operazioni si eseguono una sola volta.

   In dettaglio questa sezione si suddivide nelle seguenti:

   - Scansione della caratteristica biometrica.

     La qualità della prima acquisizione è cruciale per le successive autenticazioni. Dunque si necessita la presenza di personale specializzato che dia indicazione agli utenti che, avendo in generale poca dimestichezza con questo tipo di rilevazioni, si mostrano diffidenti verso le apparecchiature compromettendo il buon esito della rilevazione.
   - Creazione di una rappresentazione digitale detta modello o template.

     Dopo la rilevazione le misure vengono processate, il loro numero varia da una a più a seconda della natura biometrica della stessa. In taluni casi sono utilizzate più misurazioni per poi combinarle al fine di ottenere un modello valido. Importante rilevare che le caratteristiche biometriche non sono generalmente salvate e comparate come immagini grezze, piuttosto ne vengono estratte le particolarità per poi lavorare su queste ultime filtrando i rumori di rilevazione. Ciò consente di diminuire le dimensioni del modello e di conseguenza di aumentare l'efficenza nella comparazione.
   - Registrazione del modello.

La registrazione del modello dell'impronta biometrica è forse la fase più delicata per via dell'importanza delle scelte da operare. Anzitutto ci si deve chiedere con quali modalità salvare il modello. Data la sensibilità dei dati trattati e le possibili conseguenze sulla privacy, le informazioni dovranno essere crittografate. La seconda domanda è dove salvarlo. Qui le scelte possono essere le seguenti: in una chip-card, in un database centrale, in una workstation locale o direttamente nel dispositivo di acquisizione. Diamo ora un'idea di quelle che sono alcune limitazioni delle diverse soluzioni. Nel caso si lavori in un sistema che debba gestire un elevato numero di utenti, le ultime due tipologie non sono applicabili per questioni di dimensioni fisiche e di potenza di calcolo necessaria. Con una gestione tramite un database centrale bisognerà tenere conto del fatto che i dati saranno comunque soggetti a possibili furti e usi non leciti. Il salvataggio all'interno di un chip può essere una buona soluzione, a patto però di firmare digitalmente il modello salvato e di operare delle tecniche di protezione che tengano conto degli attacchi basati sui guasti.

2. **Fase di identificazione.**

   Questa fase viene ripetuta per ogni transazione che richieda l'autenticazione dell'utente. La risposta consisterà in un'accettazione o in un rifiuto da parte del sistema.

   Anche questa sezione può essere suddivisa nelle seguenti:

   - Scansione della caratteristica biometrica.

     Questa acquisizione sarà la base per il calcolo dell'impronta biometrica che dovrà essere comparata con il modello precedentemente salvato nel sistema; è intuitivo che per ottenere buone prestazioni in termini di riconoscimento, sarà necessario utilizzare lo stesso tipo di apparecchiatura di acquisizione e le stesse condizioni di contorno presenti nell'acquisizione di riferimento. Da tenere in considerazione il fatto che questa fase avviene generalmente in modo completamente automatico, si possono avere dunque problemi di rilevazione dovuti ad un non corretto interfacciamento/posizionamento dell'utente rispetto al dispositivo.

- Creazione di una rappresentazione digitale.

  Questa operazione è essenzialmente la stessa già eseguita nella fase di registrazione, l'unica differenza è il numero di rilevazioni che qui si limita ad una, fornendo quindi un'impronta meno precisa.
- Confronto con il modello o i modelli salvati per la verifica dell'identità e decisione.

  Con quest'ultima operazione si effettua quella che è la comparazione tra l'impronta rilevata e il modello acquisito, in particolare si ha una sola comparazione nel caso della verifica e n comparazioni in quello dell'identificazione. La decisione booleana viene presa in base alla soglia scelta, di cui si parlerà nel prossimo paragrafo.

1.5 Misura delle performance

Le performance di un sistema biometrico vengono valutate in funzione dei seguenti parametri: dimensioni, velocità e accuratezza.
Le dimensioni del modello estratto hanno rilevanza in relazione al dispositivo di archiviazione usato, si pensi ad esempio alle smart-card che sono dotate di memoria limitata.
La velocità con cui il sistema dà una risposta positiva o negativa è discriminante riguardo il possibile impiego nell'identificazione piuttosto che nella verifica.
L'accuratezza è un parametro piuttosto critico da determinare a causa dell'approccio probabilistico che i sistemi biometrici adottano nella scelta; vediamo dunque di illustrare i criteri utilizzati e le loro problematiche.
I tipi di errore che un sistema biometrico può commettere sono essenzialmente due:

- False accettazioni: un utente non autorizzato viene autenticato dal sistema perché la sua impronta risulta abbastanza simile ad un modello precedentemente archiviato.

- Falsi rigetti: un utente autorizzato viene rifiutato dal sistema perché la sua impronta non risulta abbastanza simile al modello con cui è stata comparata.

Questi errori possono essere rappresentati in un grafico introducendo i due indici corrispondenti: indice di falsa accettazione (FAR) ed indice di falso rigetto (FRR).
Un importante parametro nella taratura di un sistema biometrico è la soglia di sicurezza t. Dalla *Figura 1.2* si può vedere che spostandosi lungo t variano i parametri FAR e FRR, in questo modo si può adattare il sistema, nei limiti delle sue capacità, a diverse necessità di sicurezza.

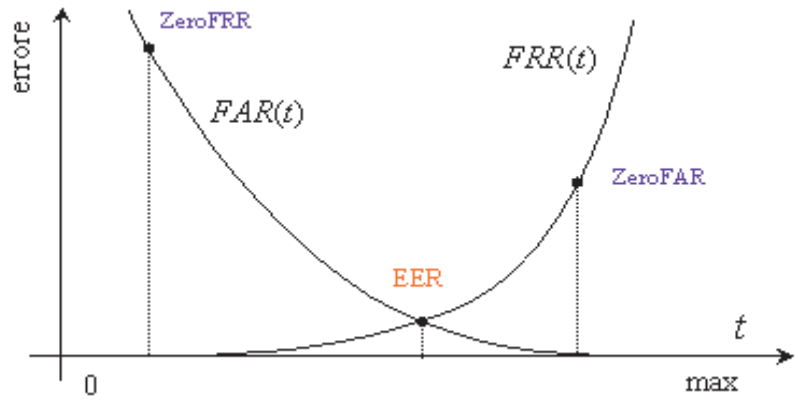

Figura 1.2 Grafico FAR-FRR [BKA]

Proseguendo in questa direzione, alzando cioè la soglia, il sistema tenderà a diminuire le false accettazioni a discapito di un aumento di falsi rigetti, attenuando invece la soglia si tenderà a non avere falsi rigetti pagando il prezzo in perdita di sicurezza.
Come si vede dall'andamento grafico, i due parametri variano in modo inversamente proporzionale; il loro punto di intersezione viene definito indice di uguaglianza degli errori (EER) ed è caratteristico di ogni implementazione biometrica. In teoria questo indice dovrebbe esprimere l'accuratezza per comparare sistemi diversi, in realtà la sua utilità è limitata. Anzitutto, i produttori dei dispositivi di acquisizione non dichiarano le condizioni sotto cui sono eseguiti i test, si deve tenere in considerazione la predisposizione ed il condizionamento degli individui utilizzati per le prove, inoltre non vi è omogeneità tra gli algoritmi utilizzati per il calcolo degli indici.

In merito al trattamento della soglia, si possono trovare varie tipologie di sistemi che adottano politiche diverse. Alcuni sono impostati in modo da ricevere una soglia di lavoro e restituire una risposta booleana ai software di gestione, altri restituiscono invece un indice compreso all'interno di un certo intervallo che fornisce una stima del grado di somiglianza delle impronte verificate, demandando quindi ogni decisione [MAT+00].

1.6 Standard biometrici

Uno dei maggiori problemi nella diffusione delle tecnologie biometriche è stato l'alto grado di disomogeneità dei sistemi in produzione. Purtroppo oltre a registrare problemi di intercambiabilità delle componenti dei sistemi, a causa delle diverse interfacce e impronte di tecnologie biometriche, si evidenziano anche limiti legati al proliferare di formati proprietari fra loro concorrenti. Da qualche hanno comunque, gli sforzi dei produttori e dei consorzi di standardizzazione si sono concentrati per dar vita al BioAPI Consortium che è stato presentato nell'aprile 1998, e tra il 1998 stesso e il 1999 ha accolto le preesistenti organizzazioni, quali la BAPI, la HA-API e la SVAPI. Nel marzo 2000 sono state pubblicate le prime specifiche, mentre una loro seconda versione, la 1.1, è disponibile dal marzo 2001. L'intendimento delle BioAPI Specification è fornire un modello generico di autenticazione biometrica di alto livello che sia adatto ad ogni forma di tecnologia biometrica. Questo modello comprende le funzioni base di registrazione, verifica e identificazione, fornendo inoltre le interfacce necessarie per la gestione dei database ai moduli BSD (fornitori di servizi biometrici). Vengono infine fornite le primitive che permettono la gestione delle fasi di registrazione e identificazione su server.

Le API biometriche cercano quindi di fornire una base certa agli integratori e agli utenti che vogliano indirizzarsi verso questa tecnologia, garantendo inoltre semplicità di integrazione usando tecnologie diverse ed interfaccia comune, possibilità di non restare legati nel tempo ad una data tecnologia e possibilità di estensione e dialogo tra applicazioni differenti.

1.7 Problematiche ed utilizzi delle tecniche biometriche

Gli aspetti da analizzare in rapporto a questa tecnologia sono numerosi, tra questi sicuramente il costo, l'accuratezza di riconoscimento, la resistenza a tentativi di intrusione esterna e l'integrazione tra sistemi analoghi.
L'uso di questo approccio rispetto a quello tradizionale, introduce alcune problematiche di non poco peso. Oltre quelle che si possono immaginare essere di tipo implementativo o comunque dipendenti dalla tecnologia, possiamo individuarne altre che si collocano all'interno della sfera sociale, tra queste una certa diffidenza verso tecniche di rilevazione invasiva, verso metodologie di identificazione già applicate per mantenere il rispetto della legge e verso la diminuzione della privacy.

1.7.1 I dati biometrici non sono segreti

Un punto essenziale da comprendere quando si parla di dati biometrici è che, per loro stessa natura, non possono essere segreti. Chiunque potrebbe essere in grado di rilevare le nostre impronte digitali da un bicchiere o un'immagine della nostra iride da una foto a nostra insaputa. Ciò che rende sicuro un riconoscimento biometrico è la fiducia che si ha nel sensore di rilevazione, ossia il credere che in un certo momento il sensore preposto stia rilevando effettivamente l'impronta della persona da autenticare. In questo contesto acquistano importanza fondamentale le tecniche di protezione impiegate sia per un eventuale colloquio intercorrente tra applicazione e apparecchio al fine di verificare l'autenticità di quest ultimo, sia per la trasmissione delle informazioni.

1.7.2 Rilevazione della vita

Se si deve aver fiducia nel sensore preposto all'acquisizione dell'impronta, bisogna che questo sia robusto verso tentativi di accesso fraudolento. Deve quindi essere in grado di distinguere tra un caratteristica biometrica valida ed una il cui scopo è

frodare il sistema. Nasce quindi la necessità vi identificare se gli elementi soggetti a rilevazione biometrica siano riprodotti artificialmente o, nel caso siano autentici, se siano o meno privi di vita.

I metodi usati per la verifica della vita sono numerosi e dipendono strettamente dalla tecnologia correlata. Alcune tecniche biometriche fanno uso di un simil protocollo di domanda-risposta di derivazione dall'ambiente crittografico, viene cioè richiesta una certa azione all'utente, che deve rispondere con l'esecuzione della stessa. Il sistema di acquisizione può ad esempio richiedere di compiere un certo movimento, nel caso di riconoscimento del viso, oppure di pronunciare certe parole, nel caso di riconoscimento della voce o del movimento delle labbra. In altri casi la verifica della vita avviene grazie a caratteristiche intrinseche dell'elemento da misurare. Alcuni esempi possono essere i seguenti:

- rilevazione del contatto fisico con l'apparecchiatura di acquisizione. Vengono rilevate la temperatura e la conducibilità elettrica.
- riconoscimento di riflessi spontanei della parte sottoposta a misurazione. Nel rilevamento dell'iride si verificano le variazioni della dimensione delle pupille oculari a seguito di esposizione luminosa. Nel riconoscimento del viso si verifica il variare delle espressioni al trascorrere del tempo.

Ritenere una rilevazione biometrica affidabile non è un concetto assoluto. Il grado di fiducia in un apparecchio di acquisizione non è da attribuirsi totalmente alla tecnologia anti-frode utilizzata, notevole importanza riveste il luogo di posizionamento e l'eventuale supervisione presente.

1.7.3 Crittografia e certificati

La crittografia applicata alla biometrica ha contribuito in modo notevole alla diffusione di questa tecnologia. La sensibilità dei dati trattati pone come elemento irrinunciabile la sicurezza in tutti i casi in cui si rende necessaria la trasmissione o l'archiviazione degli stessi.

Nei casi di autenticazione per l'accesso a sistemi, la validazione della rilevazione può essere effettuata dal dispositivo o dal server cui è collegato. Nel primo caso i dati non si muovono fisicamente dall'apparecchio e la sicurezza dello stesso dovrà quindi essere garantita dal costruttore. Nel secondo caso invece è necessario implementare un canale sicuro tra il rilevatore e il server poiché vi deve essere un trasferimento , non essendo possibile basare il riconoscimento sul suo hash (un codice generato a partire da un insieme di dati e utilizzato per verificare eventuali successive modifiche degli stessi). Per aumentare la sicurezza si deve inoltre sia crittografare e firmare digitalmente il campione biometrico, sia essere sicuri dell'apparecchio con cui si sta colloquiando. Per raggiungere questo secondo obiettivo alcuni dispositivi permettono un'autenticazione forte tramite una chiave segreta con il protocollo di domanda-risposta.

Per quanto concerne il problema inverso, ossia l'applicazione della biometrica alla crittografia, sembra che il campo di utilizzo più promettente sia l'uso per la protezione delle chiavi. Questo è il punto debole di molti sistemi, infatti le chiavi segrete o private spesso sono protette da password semplici, o ancora peggio lasciate in chiaro. L'utilizzo delle impronte biometriche per lo sblocco di smart-card su cui sono archiviate le chiavi può permettere un elevato grado di sicurezza, anche in virtù della possibilità di eseguire algoritmi all'interno del chip senza che quindi la chiave debba circolare nel sistema.

Un uso che si sposa con questa implementazione è il salvataggio della chiave privata per la firma digitale in una smart-card con circuito di rilevazione biometrica. Diventa così possibile utilizzare l'impronta biometrica, generalmente l'impronta digitale, per lo sblocco della chiave che consentirà di firmare un documento o un software tramite un certificato.

1.7.4 Costi

Negli anni passati l'alto costo di queste tecnologie è stato un deterrente per la loro diffusione. Oggi, grazie all'integrazione dei componenti elettronici, alla diminuzione

dei prezzi del software e alla crescente richiesta di sicurezza, si sta assistendo ad un notevole sviluppo di strumenti usati quotidianamente. Si trovano infatti in commercio pc portatili con sensori integrati per il riconoscimento dell'impronta digitale, kit di sviluppo per la comunicazione di dispositivi di rilevazione con software proprietario e il supporto nativo inizia a fare la sua comparsa nei principali sistemi operativi.
Questo parametro è direttamente correlato al tipo di sicurezza richiesta ed in particolare influenzato dal costo dei seguenti componenti:

- Dispositivo hardware di acquisizione.
- Mantenimento del database.
- Ricerca e test del sistema biometrico
- Installazione e integrazione del sistema.
- Educazione dell'utente alle nuove modalità.
- Gestione delle eccezioni pere gli utenti che presentano problemi di rilevazione.
- Mantenimento del sistema.

1.7.5 Cenni in materia di privacy

Il problema della privacy è un argomento molto dibattuto anche dalle nostre istituzioni ed in molti casi rallenta il diffondersi nella società della biometrica. La gente teme l'uso che può essere fatto delle informazioni rilevate dai sistemi biometrici, in particolare è concezione comune aver paura di poter essere rintracciati e sorvegliati in ogni momento da agenzie governative o da persone con intenzioni poco lecite. In realtà, a ben guardare, tramite l'uso di carte di credito, bancomat e cellulari siamo potenzialmente già sotto controllo. Il punto della questione è però il seguente: se un PIN di una scheda dovesse essere carpito, è possibile cambiarlo, nel caso delle impronte biometriche invece la perdita di sicurezza si prolungherebbe per tutta la vita dell'individuo. Bisogna quindi stabilire fino a che punto i benefici portati dall'identificazione di una persona possano compensare la perdita di anonimato.

2 Tecniche biometriche

Questo capitolo sarà dedicato ad una panoramica di quelle che sono le principali tecniche biometriche, in studio ed in essere, evidenziandone le caratteristiche e i campi di utilizzo.

2.1 Impronte digitali

La verifica delle impronte digitali è il metodo attualmente più diffuso per il riconoscimento personale. Il suo utilizzo si riscontra già in tempi passati quando in oriente veniva usata per identificare l'autore di un documento. Oggigiorno la sua implementazione più consolidata è legata all'applicazione del rispetto della legge.
Vi è un'ampia varietà di approcci utilizzati sia per l'acquisizione sia per l'analisi dell'impronta. La scansione infatti può essere effettuata con dispositivi tecnicamente differenti, fra i quali i più noti sono i sensori ottici, capacitivi e ad ultrasuoni. Per quanto riguarda l'analisi, la maggior parte delle implementazioni si focalizzano sull'individuazione delle minuzie (ossia, caratteristiche individuali uniche all'interno del modello dell'impronta digitale) o sull'individuazione ed il confronto di uno schema comune. Il basso costo di alcune tipologie di sensori di rilevazione e il loro alto grado di integrazione, hanno dato una spinta notevole a questa tecnologia, che sta beneficiando della crescente richiesta di sicurezza. Le sue caratteristiche la rendono adatta, oltre che alla verifica, anche all'identificazione, con un grado di accuratezza medio-alto. Problematiche si possono individuare nella difficoltà di rilevazione delle impronte di tipologie di persone con particolari caratteristiche

fisiche, ad esempio secchezza della pelle, calli e menomazioni. Rimane comunque una delle migliori candidate per l'utilizzo nella vita quotidiana, grazie anche alla tecnologia elettronica che ha permesso un alto grado di miniaturizzazione e quindi di integrazione in apparecchi di dimensioni contenute.

2.2 Iride

Allo stato attuale è da ritenersi la tecnica più precisa in circolazione. Meno invasiva rispetto al riconoscimento della retina (è sufficiente l'acquisizione dell'immagine tramite telecamera ad una distanza di 40-50 cm), risulta robusta a condizionamenti esterni. Grazie infatti alla metodologia adottata per la verifica, sono ininfluenti fattori di disturbo quali possono essere occhiali, lenti a contatto (anche colorate) e scarsa illuminazione (se non nella misura in cui influenza la dilatazione della pupilla), inoltre la sua struttura rimane praticamente inalterata al trascorrere del tempo. Il suo alto grado di sicurezza garantisce l'assenza di false accettazioni, è inoltre possibile l'identificazione anche con database di grosse dimensioni date le buone performance che la contraddistinguono. La tecnologia attuale non permette l'integrazione in sistemi portatili di piccole dimensioni. In previsione futura, comunque, questa dovrebbe essere una delle tecniche più promettenti.

2.3 Retina

Meno apprezzata della precedente da parte degli utenti a causa della distanza a cui si deve posizionare l'occhio rispetto all'apparecchio di rilevazione (meno di 10 cm) e a causa della necessità di focalizzare un punto preciso all'interno di un visore.

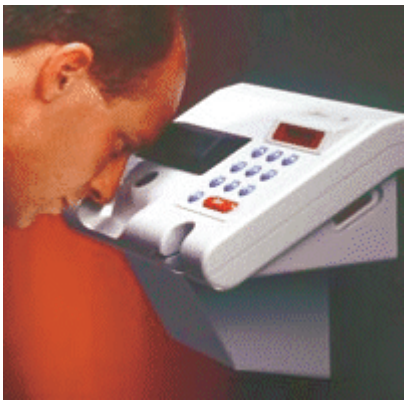

Figura 2.1 Rilevazione della retina [UMD]

Si basa sull'acquisizione e la verifica dell'immagine della mappa vascolare della retina dell'occhio a seguito di illuminazione tramite un fascio a bassa intensità di luce infrarossa. Data la complessità della rilevazione, che necessita della supervisione di un operatore, cui si aggiungono le difficoltà nel caso di persone dotate di occhiali (fissare un punto preciso nell'area di rilevazione per chi viene privato degli apparecchi di correzione visiva non è cosa facile) e il prezzo elevato delle apparecchiature, il suo uso è confinato a necessità di alta sicurezza, dove tale aspetto ha più peso dei notevoli costi connessi. Può essere usata sia per la verifica che per l'identificazione, anche se l'uso consueto è quasi esclusivamente di verifica. Il riconoscimento è molto accurato, tanto da non provocare false accettazioni, per contro i falsi rigetti sono sensibili data la difficoltà nell'acquisire una perfetta immagine della retina.

2.4 Geometria della mano

Consiste nella verifica delle misure e della conformazione della mano. Il sistema è economico e necessita di pochi byte per il salvataggio della firma. I dispositivi di acquisizione sono stati implementati con diversi tipi di tecniche, sia a sensori meccanici che ottici. In aggiunta spesso sono dotati di rilevazione di conduzione elettrica per assicurare il reale contatto della mano sulla superficie preposta.

Figura 2.2 Rilevazione 3D della geometria della mano [BSL]

Indicato solo per sistemi di verifica a causa della bassa capacità di discriminazione. La firma, costituita da 9 byte, viene generata su un numero ristretto di caratteristiche della mano, non permette quindi la distinzione di geometrie simili al crescere del numero dei record. Questa tecnologia è ritenuta un primo passo obbligato per molti progetti biometrici, soprattutto per organizzazioni che necessitano frequenti accessi ma con un grado di sicurezza non elevato. Soffre di alcuni problemi che ne hanno limitato l'utilizzo a piccole realtà, tra questi possiamo indicare le variazioni della geometria della mano dovute al trascorrere del tempo o a vari tipi di patologie fisiche oltre ad un certo grado di rifiuto psicologico della gente a appoggiare il palmo dove molti altri la posano.

2.5 Viso

Il riconoscimento delle caratteristiche facciali è forse una delle tecnologie con più fascino e meno repulsione psicologica da parte degli utenti. Il processo di riconoscimento si è sviluppato recentemente in due aree principali: la metrica facciale e il metodo delle autofacce (eigenfaces). La prima consiste nella rilevazione della posizione degli attributi facciali (posizione degli occhi, del naso, della bocca) e delle distanze tra gli stessi. Il secondo è basato sulla suddivisione in categorie in base al

grado di somiglianza con un insieme fisso di 150 autofacce. Questa tecnica ha delle somiglianze con la creazione degli indentikit sviluppata dalla polizia, con la differenza che il processo è automatizzato e basato su un'immagine reale.

Tale tecnologia si può considerare economica, fornisce inoltre buoni risultati in ambiente controllato. Purtroppo è molto sensibile alle variazioni di luminosità dell'ambiente, alle differenti espressioni e posizioni del viso, ad accessori quali gli occhiali e a variazioni dell'aspetto come ad esempio l'acconciatura. I fattori precedenti possono rendere necessario eseguire nel tempo nuovi registrazioni per gli individui in questione.

Dal punto di vista tecnico, l'elaborazione delle immagini richiede un'elevata potenza di calcolo, con la conseguenza di un orientamento verso processori dedicati di costo elevato. In aggiunta, in caso di database di grosse dimensioni le prestazioni sono scadenti. Di conseguenza questo tipo di sistemi non sono adatti all'identificazione e, in caso di necessità di alto grado di sicurezza, neppure alla verifica. Bisogna inoltre sempre tener presente che a causa della mancanza di contatto fisico con l'individuo da analizzare, sono necessarie contromisure che evitino tentativi di imbroglio del sistema di rilevazione, per esempio test di vita sull'immagine acquisita. Progressi potranno sicuramente essere portati dai miglioramenti sugli algoritmi usati nel processo di generazione dell'immagine.

2.6 Firma

Questa tecnologia, basata sull'unicità dello stile di scrittura di ogni persona, può essere sicuramente considerata la soluzione più naturale al problema dell'autenticazione. I sistemi attuali fanno uso del riconoscimento dinamico o di una sua combinazione con il riconoscimento statico.

Per riconoscimento dinamico si intende la valutazione delle caratteristiche dinamiche proprie dello stile di scrittura, per esempio la pressione esercitata sulla biro, la velocità di esecuzione della firma, l'inclinazione della penna, le accelerazioni verticali e

orizzontali. Il suo punto di forza è l'impossibilità di trarre tali informazioni dalla sola visione della firma risultante.

Nel riconoscimento statico vengono invece presi in considerazione una serie di fattori legati alla firma statica, quali ad esempio la densità delle lettere, gli incroci delle righe, i rami, gli archi.

Figura 2.3 Densità delle lettere [SOF02]

I sistemi che utilizzano solo il riconoscimento dinamico, senza prestare quindi attenzione alla firma risultante, possono autenticare persone la cui firma risulta significativamente differente dall'originale. Quelli che utilizzano una combinazione con il riconoscimento statico hanno il vantaggio di minimizzare da un lato le false accettazioni, dall'altro di contenere i falsi rigetti [SOF02].

Vi sono problemi nell'accuratezza del riconoscimento dovuti alle differenze con cui una persona scrive a causa di diversi fattori esterni o psicologici, di conseguenza il grado di sicurezza connesso è medio. L'uso combinato con altre tecniche di riconoscimento potrebbe avere notevoli sbocchi.

I campi di applicazione sono molteplici. Per citarne solo alcuni, possiamo ricordare l'uso per la conferma dei pagamenti tramite carte di credito o in ambito e-commerce, l'uso nelle transazioni finanziare, l'autenticazione di ricette mediche.

2.7 Voce

Il riconoscimento della voce trova un buon impiego nelle autenticazioni necessarie via linea telefonica e una solida base nel buon grado di accettazione degli utenti. Si differenzia rispetto al riconoscimento delle frasi perché il suo scopo è capire chi pronuncia le parole e non individuare quali parole si siano pronunciate.

Il riconoscimento può essere dipendente dalla frase o basarsi sul libero parlato. I sistemi più sicuri [MAT+00] utilizzano un sistema di controllo domanda-risposta, chiedendo all'utente di pronunciare alcune parole secondo un ordine casuale, implementando quindi oltre alla verifica dell'identità dell'utente, il test di vita.
Il riconoscimento vocale soffre di numerose limitazioni. Persone diverse possono avere voci simili, inoltre una stessa persona può essere soggetta a variazioni di timbro vocale dovute ad un cattivo stato di salute, a condizionamenti emozionali ed all'età. Alle problematiche precedenti si aggiungono quelle dipendenti dai rumori di fondo nell'ambiente e, in caso di comunicazione remota, dai disturbi sulla linea.
Il grado di sicurezza connesso è medio, può fornire prestazioni interessanti se combinato con altri riconoscimenti biometrici di costo contenuto.

2.8 Tecniche biometriche multiple

Ogni riconoscimento biometrico soffre per sua natura di alcune limitazioni. L'accuratezza è inferiore a quella desiderata; con un accesso tradizionale infatti, utilizzando un codice di autenticazione corretto ed escludendo possibili errori di digitazione, si ottiene un'accettazione sicura dal sistema, in caso di accesso biometrico invece, un'impronta valida non garantisce l'accesso, come una non valida non viene necessariamente rifiutata.
Il processo si focalizza su una particolare caratteristica fisiologica o comportamentale da misurare, tuttavia il controllo di una sola di queste non sempre è sufficiente per l'identificazione; un chiaro esempio è la verifica del viso nel caso di due gemelli.
Altri svantaggi sono la possibilità che la caratteristica prescelta non sia presente, o comunque non sia leggibile, nella totalità della popolazione.
Per porre in parte rimedio a questi problemi e per incrementare di conseguenza le prestazioni nelle applicazioni, la logica conseguenza è stata la realizzazione di sistemi che integrassero più di una tecnica biometrica, gestendo poi una strategia di accettazione o rifiuto dell'utente. Alcuni esempi sono: la realizzazione di un sistema commerciale che combina il riconoscimento del viso, della voce e del movimento

della labbra [FRI+00], lo studio teorico e l'implementazione pratica di un sistema che combina il riconoscimento del viso a quello dell'impronta digitale [LIN+99]. In entrambi i casi è stato mostrato come le prestazioni in termini di accuratezza e di resistenza alla frode siano superiori a quelli ottenibili dalle medesime misurazioni biometriche prese singolarmente.
Le tecniche biometriche multiple hanno avuto possibilità di sviluppo negli ultimi anni grazie alla caduta dei prezzi che ha interessato sia tecnologia per la costruzione dei sensori sia la parte software.

Viene riportata di seguito una tabella riassuntiva delle proprietà delle tecniche biometriche analizzate nel capitolo. Ricavata nei tratti fondamentali da un articolo pubblicato su una rivista di settore [LIU+01], è stata modificata tenendo in considerazione i recenti sviluppi e le opinioni espresse nelle letture di bibliografia [ETC] [RUG02].

Tabella riassuntiva

Caratteristica	***Impronte digitali***	***Iride***	***Retina***	***Geometria della mano***	***Viso***	***Firma***	***Voce***
Facilità d'uso	Alta	Media	Bassa	Alta	Media	Alta	Alta
Incidenza di errore	Secchezza, sporcizia, età	Scarsa illuminazione	Occhiali, lenti a contatto	Menomazioni, età	Illuminazione, età, occhiali, capelli	Modifica della firma, umore	Rumore, malattie
Accuratezza	Alta	Molto alta	Molto alta	Alta (su DB di dimensioni ridotte)	Alta	Alta	Alta
Accettazione dell'utente	Media	Media	Bassa	Media	Alta	Molto alta	Alta
Livello di sicurezza	Alto	Molto alto	Alto	Medio	Medio	Medio	Medio
Stabilità nel tempo	Alta	Alta	Alta	Media	Media	Media	Media

3 Impronte digitali e iride

In questa sezione si vogliono analizzare in dettaglio metodologie, problematiche e prospettive di quelle tecniche che oggi consentano di implementare sistemi biometrici di autenticazione forte e che allo stesso tempo non siano ritenute invasive, in particolare si focalizzerà l'attenzione sul riconoscimento dell'impronta digitale e dell'iride.

3.1 Impronte digitali

Fra tutte le tecniche biometriche esistenti, la verifica dell'impronta digitale è il metodo attualmente più diffuso, sia per ragioni storiche, sia per la facilità con cui si può integrare nei sistemi. Grazie all'introduzione e alla diffusione dei sensori capacitivi, si è verificato un notevole abbassamento dei prezzi (un sensore di questo tipo, anche per l'acquisto di una sola unità, costa meno di 50 dollari [VER]), inoltre il grado di miniaturizzazione raggiunta ne ha consentito l'uso in apparecchi di utilizzo quotidiano, quali computer portatili e cellulari.

3.1.1 Sistemi di rilevazione delle impronte digitali

La struttura di un sistema biometrico basato sulle impronte digitali è schematizzato in *Figura 3.1*.

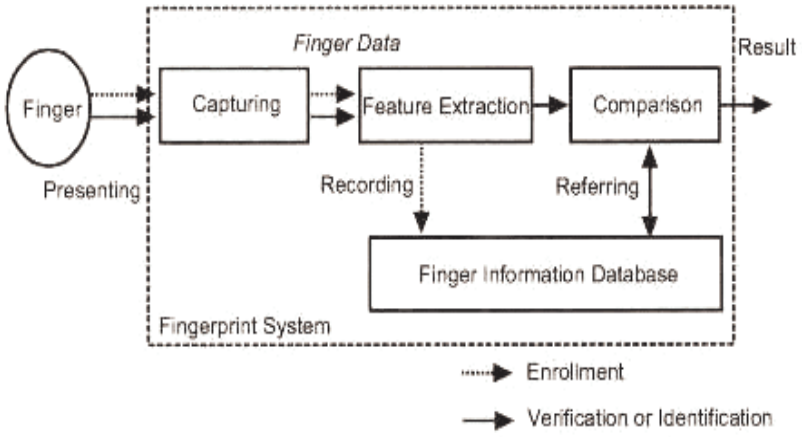

Figura 3.1 Tipica struttura di un sistema biometrico basato sulle impronte digitali [MAT+02]

Quando si è nella fase di registrazione, l'apparecchio di rilevazione cattura l'immagine del dito e le informazioni connesse (rilevazione della vita o altre misurazioni di interesse), ne estrae le caratteristiche e salva il modello costruito in un database. Se si è nella fase di verifica/identificazione, le caratteristiche estratte vengono comparate con il modello precedentemente salvato, la risposta consiste in un rifiuto o un'accettazione in riferimento ad un certo modello.

Le dimensioni dell'impronta rilevata per le successive comparazioni variano a seconda del formato proprietario utilizzato, comunque usualmente sono comprese tra 24 byte e 1 Kbyte.

3.1.2 Processo di rilevazione

L'impronta digitale è costituita da un insieme di linee in rilievo e spazi posizionati sul polpastrello; alle prime si dà il nome "creste" (ridge), alle seconde "valli" (valley). La loro struttura è unica per ogni individuo, (può essere quindi una buona base di partenza per una caratteristica biometrica). L'analisi delle sue proprietà ha portato a due approcci differenti per quanto concerne ciò che si deve rilevare e in seguito confrontare per poter autenticare un utente: l'individuazione di caratteristiche globali e di caratteristiche locali.

Nella prima l'attenzione è rivolta alla struttura di alto livello, si considerano infatti le linee di flusso disegnate dall'andamento delle creste per individuare le seguenti caratteristiche globali:

- Modello delle creste (ridge pattern): il loro andamento traccia delle figure in cui si possono riconoscere forme particolari. Negli anni i gruppi di ricerca ne hanno identificate molte, le più comuni sono comunque arco (arch), semi-corona (loop) e bidelta concentrico (whorl).

1. Loop

   Risulta essere la struttura più comune rilevabile nelle impronte digitali, si può infatti riscontrare nel 65% delle acquisizioni [DPI]. Sono identificabili dalla curva molto stretta tracciata dalla cresta.

Figura 3.2 Loop [VIT99]

2. Arco

   La sua struttura è composta da una cresta che traccia una curva più aperta di quella formata dal loop.

Figura 3.3 Arco [VIT99]

3. Ricorre in circa il 30% delle immagini rilevate [DPI], consiste in una cresta che disegna un cerchio completo.

Figura 3.4 Bidelta concentrico [VIT99]

- Area del modello (pattern area): corrisponde alla parte dell'impronta che racchiude tutte le caratteristiche globali, è delimitata dalle due linee più esterne (definite type lines), identificate in *Figura 3.5* come linea A e B.

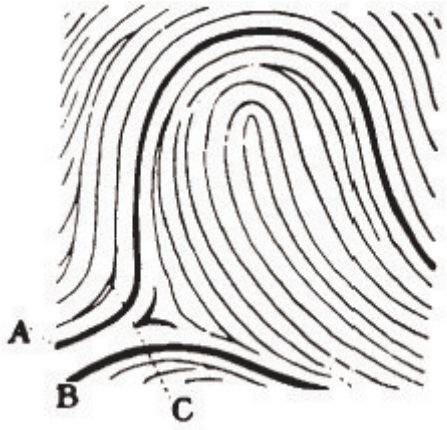

Figura 3.5 Pattern area [DPI]

- Core: è un punto posizionato approssimativamente al centro dell'impronta e viene usato come riferimento per la lettura e la classificazione.
- Delta: è il punto della prima biforcazione posizionato di fronte al punto di divergenza delle due type lines (punto C di *Figura 3.5*).
- Numero delle creste (ridge count): è il numero di creste che si contano tra il delta e il core.

Nelle caratteristiche locali si ricercano alcuni comportamenti anomali delle creste, nella fattispecie i principali sono le terminazioni e le biforcazioni. I punti identificati da queste particolarità vengono definite "minuzie".

Le caratteristiche utilizzate per identificare le minuzie sono le seguenti:

1. Tipo: a partire da terminazioni e biforcazioni vengono definite una serie di elementi caratteristici.
   - Terminazione (ridge ending): si dice di una cresta che termina bruscamente.
   - Biforcazione: il punto in cui una cresta si divide in due.
   - Punto o isola: una cresta tanto corta da sembrare un punto.
   - Lago (enclosure): una cresta che si divide in due e poi si riunisce, creando una zona chiusa al cui interno non ci sono altre creste.

- Cresta corta: una cresta di piccole dimensioni, ma non tanto da essere considerata un punto.

2. Orientamento: si riferisce alla particolare direzione posseduta dalla minuzia in oggetto.
3. Frequenza spaziale: si riferisce a quanto lontano si trovano le creste nella vicinanza della minuzia.
4. Curvatura: si riferisce al tasso di cambiamento dell'orientazione della cresta nel punto in questione.
5. Posizione: indica le coordinate piane della minuzia in senso assoluto o relativamente al delta e al core.

Un'impronta è costituita da circa 100 minuzie; tipicamente un apparecchio commerciale ne rileva tra 20 e 30, che sono comunque considerate sufficienti per un'identificazione certa. L'FBI ha infatti dimostrato che non possono esistere due individui con più di 8 minuzie uguali, la corte europea comunque ne richiede 12 per un'identificazione non ambigua [ITF].

Sia nella tecnica basata sulla ricerca di minuzie sia in quella basata sulla correlazione si possono riscontrare alcuni difetti; la prima risente della difficoltà di estrazione delle minuzie in immagini di bassa qualità, inoltre prescinde totalmente dalla struttura globale delle creste e delle valli, la seconda invece è affetta da problemi di traslazione e rotazione, inoltre è più facilmente ingannabile da immagini contraffatte. Recentemente alcuni studi hanno mostrato come una rilevazione basata sulla minuzie combinata con un'analisi della struttura porti a sostanziali miglioramenti delle prestazioni in termine di indici FAR e FRR (vedi *Paragrafo 1.5*) [JAI+01].

3.1.3 Dispositivi di rilevazione

La scansione dell'impronta digitale può essere effettuata con dispositivi tecnicamente differenti, tra questi si evidenziano i sensori ottici, a chip di silicio e ad ultrasuoni.

Tali apparecchi di rilevazione hanno caratteristiche diverse sia per quanto riguarda le dimensioni, sia per ciò che concerne la robustezza a fattori esterni.
Vediamo brevemente quali sono i rispettivi punti di forza e di debolezza.

1. Lettori ottici

Sono basati sui cambiamenti di riflessione nel punto di contatto delle linee dell'impronta. Le dimensioni sono approssimativamente 5 * 5 * 10 cm, questo ne preclude l'uso in apparecchi di dimensioni contenute quali portatili, cellulari, etc..

Figura 3.6 Rilevatore ottico Sony [IOS]

La possibilità di miniaturizzazione è limitata a causa della necessità di integrare nell'apparecchio la sorgente luminosa, la superficie di riflessione e il sensore fotosensibile (oggi rappresentato generalmente da una camera CCD o CMOS). Sono affidabili ma necessitano di pulizia per evitare la formazione di impronte residue causate dal grasso e dalla polvere. Soffrono inoltre di una certa distorsione dovuta alla necessità di focalizzare l'immagine in uno spazio di dimensioni contenute. Tale distorsione è facilmente correggibile via software, purtroppo ogni apparecchio produce una distorsione diversa, non è quindi possibile elaborare un processo di aggiustamento di carattere generale. Non sono ingannabili da immagini 2D, ma gli artefatti tridimensionali ricavati dalla calchi dell'impronta rappresentano un serio problema [MAT+02] nonostante molti modelli oggi incorporino sensori per la rilevazione della vita.

2. Lettori a chip di silicio

La loro diffusione sta conoscendo un notevole incremento dovuto al basso costo e all'elevata possibilità di miniaturizzazione.

Già presenti nei lettori ottici sotto forma di sensore fotosensibile, sono realizzati eliminando la parte propriamente ottica (sorgente luminosa, prisma e lente) e mettendo a contatto la superficie del chip direttamente col dito. La struttura consiste in una matrice di pixel ed un trasduttore che converte le informazioni fisiche in elettroni. Le varie tipologie si differenziano per le caratteristiche prese in considerazione nella misurazione, ne conseguono i seguenti tipi di sensori:

- A pressione: questo tipo di rilevatori misurano la pressione esercitata dal dito durante il processo di autenticazione tramite l'uso di trasduttori basati su materiale piezo-elettrico. La sensibilità è risultata però essere molto bassa, inoltre, una volta rivestiti con una pellicola protettiva, l'immagine ottenuta è poco definita. Per queste motivazioni non vi sono stati sviluppi industriali in questa direzione.

- Capacitivi: si basano sulla differenza di potenziale che si rileva fra le valli e le creste dell'impronta digitale a contatto con una distesa di capacitori. Attualmente risulta la scelta di maggiore tendenza tra i produttori, poiché permette di ottenere buoni risultati di accuratezza contenendo i costi grazie alla realizzazione sul solo wafer di silicio e grazie alle dimensioni ridotte (circa 15 * 15 * 1,5 mm).

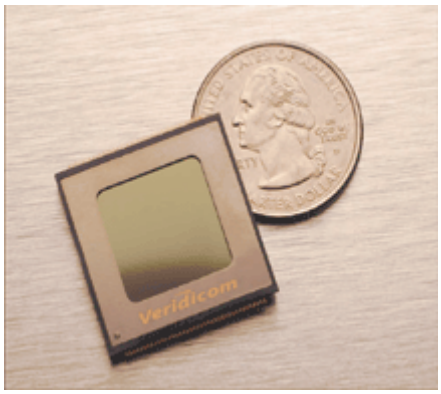

Figura 3.7 Chip Veridicom [VER]

Proprio la necessità di contenere le dimensioni per ridurre l'uso della parte del wafer di silicio occupata e di conseguenza del costo del chip, porta all'insorgere di problemi di riconoscimento. Riducendo l'area di silicio si riduce anche la finestra di rilevazione, provocando esclusioni di parti dell'impronta e favorendo difficoltà nel corretto posizionamento del polpastrello. Questi chip sono affetti inoltre da problemi nella rilevazione dell'immagine dovuti all'umidità, ne consegue che pelli troppo secche o troppo grasse vengono mal gestite. Un notevole svantaggio si può rilevare nella sensibilità alle scariche dovute a campi elettrostatici, la pellicola di rivestimento dei chip è infatti di dimensioni micrometriche per contenere la distanza fra il dito e i capacitori, favorendo quindi questo tipo di fenomeni.

- Termici: sono in grado di trasformare la differenza di temperatura in differenza di potenziale. Al contatto del polpastrello con il chip, viene rilevata la temperatura delle creste e viene assunta la temperatura delle valli uguale a quella dell'ambiente. Si è in grado quindi di rilevare l'immagine dell'impronta, che tuttavia scompare nell'arco di un decimo di secondo a causa del raggiunto equilibrio termico tra chip e dito.

3. Lettori ad ultrasuoni

Attualmente una sola compagnia [USN] propone soluzioni basate su questa tecnologia e ne detiene i relativi brevetti. Il maggiore vantaggio di questa tecnica consiste nell'uso di onde sonore in alta frequenza che consentono di ottenere un'immagine reale della superficie sotto scansione sfruttando la differente impedenza acustica di pelle, aria e superficie sottocutanea, senza soffrire delle limitazioni proprie della rilevazione ottica. L'immagine ottenuta tramite ultrasuoni non risente quindi di sporcizia sulle dita o sul lettore e di abrasioni sulla pelle, inoltre l'accuratezza della stessa consente la rilevazione delle impronte anche di soggetti difficili quali bambini o anziani.

Le dimensioni richieste dai lettori sono relativamente ampie (circa 15*15*20 cm) e la presenza di parti meccaniche tende a rendere questi apparecchi pesanti e rumorosi.

La temperatura operativa inoltre si posiziona tra i 10 e i 32 °C, limitandone l'utilizzo a luoghi chiusi.
Il costo di questa apparecchiatura risulta piuttosto elevato restringendone quindi i campi di applicazione. Tuttavia bisogna tenere presente che, a fronte di un tempo di rilevazione dell'immagine di circa un secondo, si ottiene un'accuratezza e una precisione tali da non rendere necessaria nella quasi totalità dei casi una riscansione, caso abbastanza frequente con altri tipi di lettori. Questo comportamento può consentire di velocizzare le operazioni di autenticazione, guadagnando tempo in caso di accesi frequenti.

3.1.4 Problematiche inerenti alla contraffazione

L'introduzione della biometria nei sistemi ad accesso controllato ha l'obbiettivo aumentare il grado di sicurezza generale. Per questo motivo risulta di importanza fondamentale che gli apparecchi di rilevazione dell'impronta siano in grado di distinguere tra caratteristiche biometriche valide e fasulle. Le situazioni che si possono presentare in fase di rilevazione sono le seguenti:

1. Il dito presentato è quello registrato: nonostante il dito appartenga al legittimo utente, vi è il rischio che sia costretto alla misurazione contro la sua volontà, per esempio sotto minaccia, sotto l'effetto di droga o in stato di incoscienza. Una soluzione potrebbe essere combinare la rilevazione biometrica con altre tecniche di controllo, quale può essere la richiesta di un PIN, in questo modo verrebbero però meno alcune delle motivazioni principali che hanno spinto all'introduzione delle tecniche biometriche.
2. Il dito non è registrato: l'utente tenta di accedere al sistema sfruttando le similitudini che la sua caratteristica biometrica può avere con quella di un utente legittimo. Generalmente questo caso viene gestito dai diversi sistemi tramite l'accuratezza della rilevazione e quindi in definitiva tramite gli indici FAR e FRR, la probabilità di falsa accettazione cambia però conoscendo l'approccio

all'autenticazione del sistema in questione. Tale attacco si basa infatti sulla correlazione tra lo schema delle categorie globali della propria impronta (archi, loop e bidelta concentrici), reale o modificata chirurgicamente, e quello dell'impronta di un utente registrato. Risulta utile quindi accompagnare il controllo della similitudine tra le suddette categorie all'individuazione di caratteristiche particolari all'interno delle stesse (minuzie).

3. Il dito è registrato ma è stato amputato: questo tipo di attacco moralmente ripugnante ma già purtroppo attuato in passato, può essere inficiato tramite l'utilizzo della rilevazione della vita.
4. Il dito è un clone artificiale di quello registrato: come detto in precedenza, non essendo i dati biometrici segreti, e a maggior ragione l'impronta digitale, è possibile realizzare dita artificiali, o comunque rivestimenti sintetici da applicare alle dita, con materiali che tentino di ingannare gli apparecchi di rilevazione. La rilevazione dei parametri vitali è sicuramente il metodo per scoraggiare questo tipo di attacco
5. Altri casi: esistono metodi di attacco che si basano sulla possibilità di provocare errori nell'apparecchio di rilevazione agendo direttamente sull'hardware tramite tecniche opportune (fault-based attack). In alcuni casi è possibile forzare il rilevatore a consentire l'accesso ad esempio tramite l'irradiazione del lettore tramite particolari luci lampeggianti, tramite l'umidificazione del dito artificiale con particolari sostanze umide, facendolo vibrare oltre i suoi limiti di tolleranza. Questo tipo di attacchi ben conosciuto dai produttori, deve essere gestito in fase di progettazione e realizzazione dell'apparecchiatura stessa.

Le situazioni elencate ai punti 2 e 5 dipendono essenzialmente dal livello di accuratezza raggiunto e dalla robustezza dell'hardware a fattori esterni, esaminiamo invece il problema della rilevazione della vita.

Le tecniche implementate si basano generalmente sull'analisi di una o più delle seguenti caratteristiche [VAN+00], di cui vengono anche descritte alcune problematiche:

- Temperatura: questo tipo di misurazione è poco efficacie, infatti a causa delle diverse condizioni ambientali in cui il dispositivo di rilevazione si trova ad operare, si è costretti a lasciare un notevole margine di oscillazione tra la temperatura minima e massima ammissibili per evitare un indice di falsi rigetti troppo elevato. Ne consegue l'impossibilità di distinguere tra dita reali e rivestimenti artificiali.
- Conduttanza: anche questa caratteristica non consente elevata affidabilità, la resistenza può infatti variare anche di un ordine di grandezza a seconda che il dito sia il condizioni ambientali ottimali o in condizioni di gelo che ne determinino un'elevata secchezza. Un materiale siliconico inumidito opportunamente può ingannare il sensore.
- Battito del cuore: tecnica che può risultare efficacie, anche se bisogna tener conto che alcune persone possono avere pulsazioni cardiache molto fuori media. In alcuni casi il sensore potrebbe non rilevare battito nel periodo di controllo, rifiutando quindi un accesso autorizzato.
- Costante dielettrica relativa: anche questa caratteristica dipende, come la conduttanza, dall'umidità del dito, è necessario lasciare quindi un certo margine di errore. Tramite alcuni accorgimenti è possibile utilizzare sostanze per inumidire il dito artificiale, in modo che durante l'evaporazione portino lo stesso ad avere una misurazione simile a quella di un dito reale.
- Pressione del sangue: per la misurazione di questa caratteristica è necessario il contratto in due differenti punti del corpo. Questo svantaggio si unisce a quello già segnalato nella rilevazione del battito cardiaco.
- Rilevazione dello strato sotto il tessuto epidermico: sostanzialmente questa è la tecnica utilizzata dai rilevatori ad ultrasuoni. Per ingannare questo tipo di sensore è necessario conoscere esattamente cosa misura e qual è l'indice di riflessione dei materiali sotto verifica, per poi riprodurre artificialmente condizioni analoghe.

Le numerose problematiche sopra elencate dipendono in buona parte dalle numerose condizioni d'uso per cui si richiede il funzionamento dei sensori, questo

significa che in condizioni particolari o controllate alcuni dei problemi in precedenza indicati siano trascurabili.

Recentemente è stato mostrato [MAT+02] come sia possibile realizzare con tecniche accessibili, un dito artificiale in materiale gelatinoso che permetta di ingannare la maggior parte degli apparecchi oggi in commercio. In questa pubblicazione viene mostrato come la realizzazione possa avvenire sia per rilevazione diretta (l'impronta viene acquisita tramite calco del dito su materiale gommoso), sia tramite rilevazione indiretta (l'impronta viene acquisita da un'immagine residua tramite microscopio digitale). Come risultato gli undici lettori scelti, equamente suddivisi in lettori ottici e capacitivi (quelli cioè più diffusi sul mercato), hanno ritenuto il dito artificiale accettabile e l'autenticazione è avvenuta con una probabilità compresa tra il 68 e il 100%.
Risulta interessante notare come le dita realizzate in lattice non siano accettate dai lettori capacitivi, mentre quella realizzata con questo materiale gelatinoso si. Probabilmente questo comportamento diverso è dovuto all'umidità e alla resistenza elettrica non rilevabili nel dito in silicone. Possiamo di seguito vedere la *Tabella 3.1* che mostra le diversità di rilevazione per le proprietà accennate tra un dito vivo, uno in silicone e uno in materiale gelatinoso.

	Umidità ***%***	***Resistenza elettrica*** ***MΩ/cm***
Dito vivo	16	16
Dito in gelatina	23	20
Dito in silicone	Non misurabile	Non misurabile

Tabella 1 Caratteristiche della dita [MAT+02]

Viene anche evidenziato come il grafico descritto dalla frequenza di risonanza al variare della pressione esercitata sul lettore sia nettamente differente nel caso di un dito vero rispetto a quello di un dito artificiale.

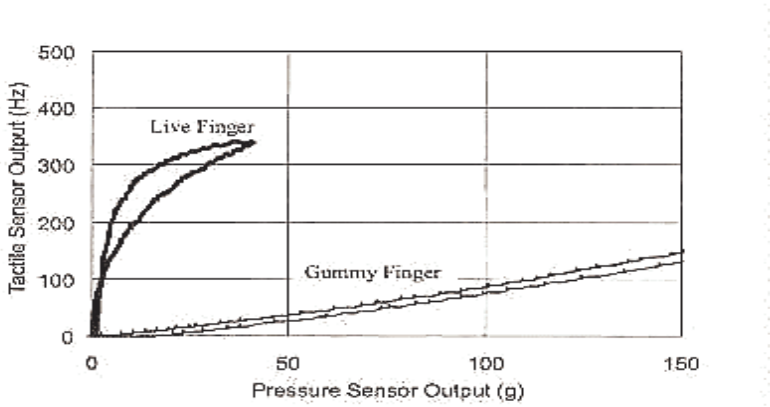

Figura 3.8 Grafico di conformità [MAT+02]

La rilevazione della vita non è un argomento da sottovalutare, soprattutto per una caratteristica biometrica quale l'impronta digitale che, come mostrato, è facilmente riproducibile. Purtroppo la politica dei costruttori non favorisce la chiarezza nell'approccio a questo problema; nella maggior parte dei casi infatti non vengono dichiarate quali siano le contromisure adottate per evitare accettazioni di dita non autentiche. Questo atteggiamento di protezione tramite l'occultamento delle informazioni sulla struttura, non dovrebbe mai essere usato, infatti come insegna la crittografia, a fronte di un breve periodo di successo, viene favorita la spinta verso la retroingegneria che spesso porta alla forzatura di sistemi con metodi non previsti dagli ideatori.

3.2 Iride

In questa sezione si metteranno in evidenza le caratteristiche che rendono il riconoscimento dell'iride una delle tecnologie con più prospettive per il futuro. Si cercherà di analizzare la tecnica implementata per l'estrazione della chiave biometrica e le metodologie di confronto, nonché le possibili applicazioni.

L'iride, organo colorato posto intorno alla pupilla, è ricca di singolarità che la rendono unica, persino le due iridi di uno stesso soggetto sono completamente diverse fra loro.

Tipicamente nel processo di scansione necessario per la creazione della chiave biometrica (detta *iriscode*) vengono prese in considerazione circa duecento caratteristiche distintive; alcune di queste sono: solchi di contrazione, fibre e filamenti di collagene, cripte, corone, striature, fissurazioni, fosse, legamenti arcuati, creste e anelli.

Possiamo individuare alcune delle proprietà che rendono l'iride potenzialmente superiore alle altre tecnologie biometriche:

- Unicità: la ricchezza in termini di quantità di dati estraibili (266 caratteristiche), consente di avere un elevato valore di discriminazione. Statisticamente è stato calcolato che approssimativamente la probabilità di avere due *iriscode* identici è di circa 1 su 10^{78} [VIT99].
- Stabilità nel tempo: la struttura dell'iride praticamente non si modifica al trascorrere del tempo, l'organo inoltre è protetto dalla cornea che lo ripara dagli agenti esterni, infine l'iride non è soggetta a malattie conosciute che possano modificarne l'aspetto.
- Impossibilità di alterazione: attualmente non è possibile modificare la struttura fisica dell'iride ed in ogni caso il rischio connesso sarebbe molto elevato. Inoltre la continua fluttuazione della pupilla al variare delle condizioni luminose, rende complicato l'uso di artifizi atti ad ingannare il sistema.
- Semplicità di rilevazione: l'immagine viene catturata ad una distanza compresa tra i 15 e i 46 cm, non vi è quindi contatto fisico tra l'apparecchio e l'utente, l'illuminazione avviene generalmente con una luce di color magenta a bassa intensità, non fastidiosa quindi per la persona.

3.2.1 Sistemi di rilevazione dell'iride

Un sistema di rilevazione dell'iride è costituito in generale dai componenti illustrati in *Figura 3.9*.

Una video camera di tipo CCD acquisisce l'immagine dell'iride, questa viene preprocessata per localizzarne la posizione e si effettua una conversione in coordinate polari. Tramite una demodulazione wavelet 2D viene estratta una rappresentazione delle minuzie la cui risultante viene usata per effettuare un test di indipendenza statistica tra l'impronta acquisita e una di quelle presente nel database, fornendo un parametro che permette la conferma o meno dell'identificazione.

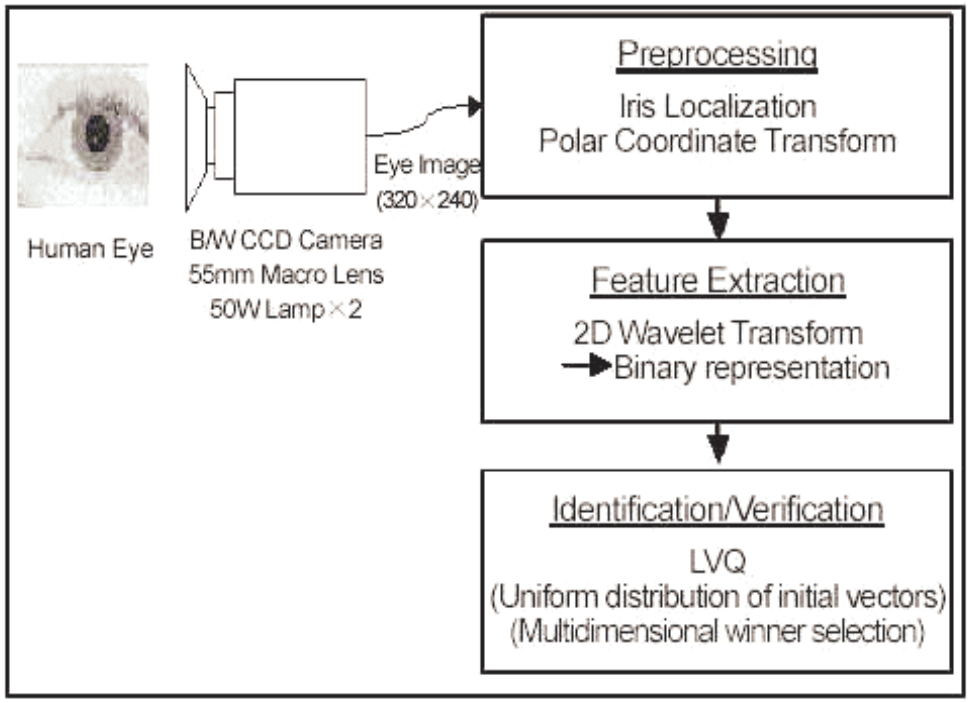

Figura 3.9 Struttura di un sistema per il riconoscimento dell'iride

3.2.2 Come funziona il riconoscimento dell'iride

Il riconoscimento dell'iride si basa sull'identificazione delle minuzie che la contraddistinguono, da queste si ricava l'*iriscode*. La rilevazione si ottiene per via ottica e l'illuminazione può avvenire tramite luce normale o vicina all'infrarossa. La dimensione dell'*iriscode* è di 512 byte, di cui una metà descrive le caratteristiche rilevate nell'acquisizione, l'altra controlla il processo di comparazione [WIL01]. Pur essendo questa dimensione ragionevole rispetto alla chiave di altre tecniche

biometriche, racchiude una quantità di informazioni (244 caratteristiche, dette anche "gradi di libertà") tale da permettere un'identificazione praticamente certa.
L'algoritmo di creazione dell'*iriscode* è stato ideato da John Daugman [DAU] che lo ha brevettato nel 1994; attualmente il codice sorgente e i suoi aggiornamenti sono posseduti dall'Iridian Technologies, che provvede a fornire l'eseguibile e i diritti d'uso alle società interessate. Analizziamo ora quali sono i passi su cui si basa questo algoritmo.

- **Individuazione dell'immagine dell'iride**

Il primo passo consiste nella localizzazione dell'iride. Una telecamera riprende l'occhio dell'utente, la messa a fuoco viene realizzata misurando lo spettro della trasformata 2D di Fourier per ogni fotogramma catturato e aggiustando di conseguenza la posizione della lente per ottenere un'immagine di qualità superiore. Dopo la sua trasformazione in toni di grigio, il software cerca di ottenere i contorni e le coordinate dell'iride e della pupilla, spesso infatti le due non sono concentriche. Una volta definiti i contorni della larghezza di un singolo pixel, vengono individuati e marcati i contorni delle palpebre; ciò che si ottiene è la parte di iride visibile (*Figura 3.10).*

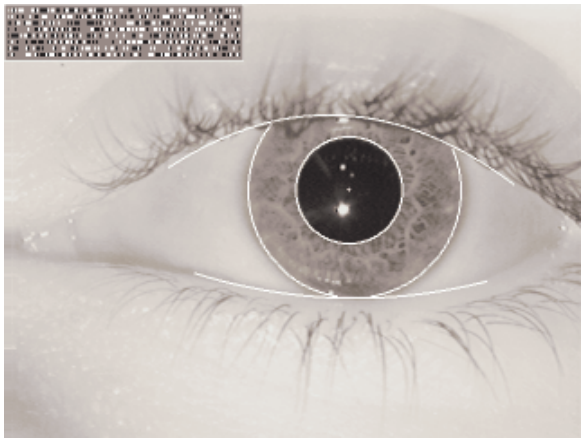

Figura 3.10 Individuazione dell'iride e relativo iriscode [DAU]

- **Codificare le caratteristiche dell'iride tramite una demodulazione wavelet 2D**

La struttura dell'iride viene demodulata per estrarne le informazioni sotto forma di sequenza di fasori (vettori nel piano complesso) attraverso l'uso delle wavelet 2D di Gabor. I fasori, che giaciono in uno dei quattro quadranti, vengono quantizzati per settare i bit all'interno dell'*iriscode* (*Figura 3.11*). Questo processo viene effettuato lavorando in un sistema di coordinate polari adimensionali che è invariante all'ampiezza dell'iride ed alla dilatazione della pupilla.

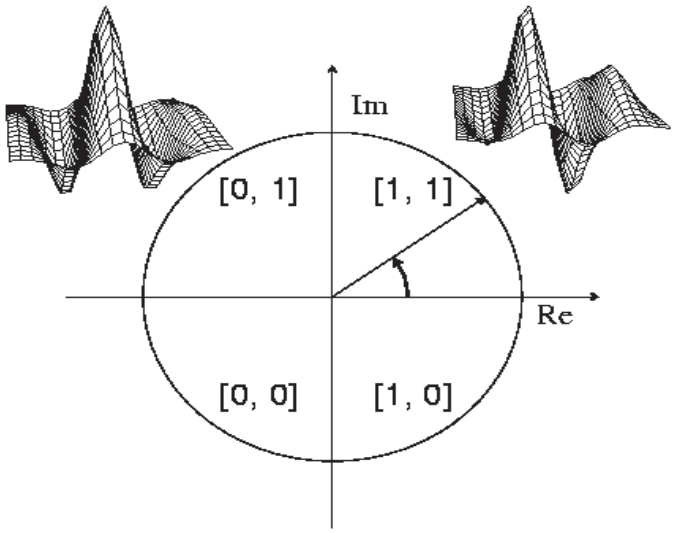

Figura 3.11 Settaggio dei bit nell'iriscode [DAU]

La sequenza di codifica dei quadranti di fase rappresentata da una serie di bit è mostrata nella parte in alto a sinistra della *Figura 3.10*. I bit di fase sono in totale 2048 (256 byte) e sono calcolati per ogni iride. L'algoritmo di Daugman prevede inoltre il calcolo di una maschera costituita dallo stesso numero di bit che tiene conto delle regioni dell'iride non significative. In altre parole vengono oscurate le parti coperte dalle palpebre, soggette a deformazioni dovute alle lenti a contatto o contenenti riflessi di vario genere, in modo che non vengano prese in considerazione dalla demodulazione.

Il riconoscimento dell'iride viene effettuato utilizzando solo le informazioni inerenti alla fase, trascurando quelle dipendenti dall'ampiezza di vettori che avrebbero introdotto elementi correlati con il contrasto, con l'illuminazione e con il fattore di ingrandimento della lente; inoltre questa scelta si mostra efficiente nell'analisi delle immagini sfocate, la fasi risultano infatti statisticamente simili a quelle che si sarebbero ottenute con un'immagine nitida. Questa proprietà ha il vantaggio non trascurabile dell'impossibilità di confondere due iridi diverse solo a causa della scarsa qualità dell'immagine.

- **Test di indipendenza statistica**

La chiave del riconoscimento dell'iride si basa sul fallimento di un test di indipendenza statistica. L'elevato numero di gradi di libertà su cui si lavora porta ad affermare che il test fallisce solo se si stanno confrontando le fasi estratte da due immagini della stessa iride.

Il procedimento si basa sui codici calcolati dalle due iridi da confrontare e sulle due corrispondenti maschere. In sostanza viene eseguito un XOR tra i due codici, questo permette di verificare differenze tra le fasi, poi viene fatta l'intersezione con le maschere delle due iridi per eliminare le parti non significative, infine il risultato viene normalizzato rispetto all'intersezione delle due maschere. Lavorando in norma otteniamo una misura della dissomiglianza tra le due iridi, definita come distanza di Hamming:

$$HD = \frac{\| (codeA \otimes codeB) \cap maskA \cap maskB \|}{\| maskA \cap maskB \|}$$

Il termine "code" identifica il codice ricavato dalle due iridi a confronto (A e B), "mask" identifica le corrispondenti maschere.

Le conclusioni limite che si possono trarre dalla distanza di Hamming risultante sono le seguenti: se HD è 0 le due iridi a confronto si sono rilevate identiche, se è 1 vi è una totale incorrelazione. In campo operativo se il test è stato effettuato su due iridi differenti la distanza è circa 0,5, se invece si è lavorato su due campioni della

stessa iride la distanza è compresa tra 0,05 e 0,1. La soglia che differenzia un utente autorizzato da un impostore viene assunta a 0,342 (*Figura 3.12*).

La particolare struttura del test ne favorisce la parallelizzazione dei confronti (su una workstation Sun con CPU a 300 Mhz le prestazioni sono pari a circa 100000 iridi al secondo).

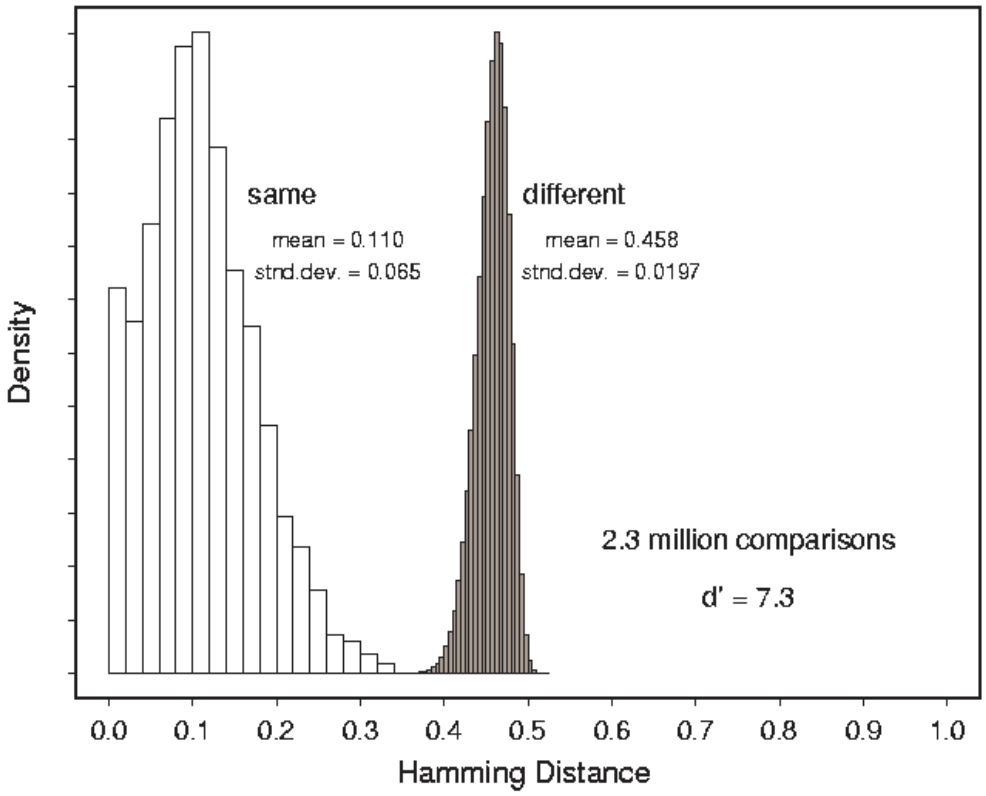

Figura 3.12 Ambiente di decisione per il riconoscimento dell'iride [DAU]

- **Riconoscere l'iride senza tener conto di dimensioni, posizione e orientamento**

La rappresentazione di una struttura di riconoscimento deve essere robusta alle differenze di rilevazione dovute ai fattori esterni. Nel caso dell'iride i fattori che possono influire sono: l'ingrandimento ottico dovuto alle lenti della videocamera, le dimensioni della pupilla, la posizione che assume all'interno dell'immagine acquisita e il suo orientamento. I primi tre problemi sono risolti grazie alla scelta di un sistema di riferimento polare in cui la variabile radiale compresa tra il bordo della pupilla e il

limbo dell'occhio varia in un intervallo unitario, ne consegue che si lavora con due variabili adimensionali. L'invarianza all'orientamento si ottiene calcolando un codice costituito dalle fasi estratte dall'iride sotto forma di una singola rappresentazione in forma canonica, questa viene poi comparata discretizzandone l'orientamento tramite il cambiamento ciclico della sua variabile angolare.

- **Prestazioni**

Le prestazioni fornite dal riconoscimento dell'iride sono ottime sotto diversi aspetti. Esaminando l'indice di falsa accettazione (FAR), possiamo notare (*Figura 3.13*) come nel punto di posizionamento della soglia (HD = 0,342) il valore di probabilità calcolato sia di 1 su 1,2 milioni. Questa scelta è piuttosto conservativa tenendo conto che nella maggior parte delle comparazioni con esito positivo, la l'HD si posiziona vicino allo 0,08, dove abbiamo una probabilità di falsa accettazione di circa 1 su 10^{48}.

HD	False Accept Probability	False Reject Probability
.28	1 in 10^{12}	1 in 11,400
.29	1 in 10^{11}	1 in 22,700
.30	1 in 6.2 billion	1 in 46,000
.31	1 in 665 million	1 in 95,000
.32	1 in 81 million	1in 201,000
.33	1 in 11 million	1in 433,000
.34	1 in 1.7 million	1in 950,000
.342	1 in 1.2 million	1 in 1.2 m
.35	1 in 295,000	1 in 2.12 m
.36	1 in 57,000	1 in 4.84 m
.37	1 in 12,300	1 in 11.3 m

Figura 3.13 Distanza di Hamming e probabilità di errore [WIL01]

La velocità del processo di riconoscimento dipende sia dalla velocità del processore, sia dalla dimensione del database, comunque grazie alla strutturazione del test e alla possibilità di parallelizzazione, si ottengono risposte nell'arco di 2 – 3 secondi, anche in caso di sistemi di grandi dimensioni (milioni di utenti registrati).

La fase di registrazione ha una durata che generalmente è di 1 – 2 minuti; questa dipende da alcuni fattori, tra cui il tipo di apparecchiatura preposta alla rilevazione

(aggiustamento automatico o tramite comandi vocali impartiti all'utente), la predisposizione psicologica del soggetto e la capacità del personale, nel caso sia previsto, nell'indirizzarlo.

Per aumentare la qualità della registrazione è buona norma che l'utente non faccia uso degli occhiali; le lenti a contatto non procurano invece disturbi. Durante le seguenti fasi di riconoscimento sarà invece indifferente l'uso di occhiali da vista, lenti a contatto, lenti colorate e di molti tipi di occhiali da sole.

Il grafico di confidenza (*Figura 3.12*) è stato ricavato lavorando su milioni di comparazioni, eseguendo inoltre le prove di registrazione e verifica con differenti condizioni al contorno. Sono quindi stati eseguiti i test con condizioni di luce variabili, con e senza lenti o occhiali, con apparecchi di rilevazione di modelli diversi. I risultati mostrano comunque un alto grado di confidenza sia nella rilevazione di utenti autorizzati, sia di impostori.

3.2.3 Apparecchi di rilevazione

Le apparecchiature per la rilevazione dell'iride si distinguono principalmente in due categorie, una che gestisce la sicurezza nell'accesso alle informazioni e l'altra la sicurezza per l'accesso fisico a luoghi protetti.

- Sicurezza delle informazioni

Per garantire la protezione di dati sensibili, vengono utilizzati sistemi composti da un dispositivo di rilevazione collegato al computer, che viene utilizzato sia per la verifica sia per la registrazione, e dal software di gestione. Questa soluzione permette di eliminare l'uso di utente e password per l'accesso al PC, tagliando inoltre i costi connessi alla gestione delle stesse, che in azienda è stata stimata essere tra i 200 e i 300 dollari annui per utente [IRI].

In *Figura 3.14* possiamo vedere un esempio di dispositivo di autenticazione con funzionalità aggiunte di videocamera adatte anche alla videoconferenza. Le dimensioni sono piuttosto ridotte (4,2 * 9 * 7,4 cm), consentendone tranquillamente

il trasporto con computer portatili. L'utilizzo di questo tipo di dispositivi permette inoltre l'accesso sicuro a database e, se supportato, l'autenticazione via web in caso di banking, trading o acquisti online.

Figura 3.14 Dispositivo di controllo per l'accesso alle informazioni [ITI]

- Accesso fisico

Alcune tipologie di sistemi sono studiate per controllare l'acceso fisico in zone o edifici protetti. Questo tipo di realizzazioni generalmente si compongono di un apparecchio dedicato alla registrazione e collegato ad un server preposto al salvataggio delle impronte, e di uno o più dispositivi esterni utilizzati per consentire l'autenticazione degli utenti.

Figura 3.15Dispositivo di controllo per l'accesso fisico [ITI]

Il loro utilizzo, destinato ad ambienti di grandi dimensioni, deve essere valutato attentamente, i server contenenti le informazioni segrete devono essere protetti tramite firewall e sistemi crittografici a causa della natura distribuita di questo tipo di applicazioni. Spesso infatti le connessioni tra server e dispositivi periferici avvengono via rete tramite protocollo TCP/IP, esponendo i dati a possibili attacchi esterni.

3.2.4 Vantaggi e svantaggi

Riassumiamo brevemente quali sono i vantaggi e gli svantaggi nell'uso di questa tecnica biometrica.

Vantaggi nell'uso del riconoscimento dell'iride:

- E' un organo interno protetto dalla retina.
- La conformazione è visibile esternamente, il metodo di rilevazione non è quindi invasivo.
- La sua struttura possiede un elevato grado di casualità (244 gradi di libertà) che la rendono unica e non confondibile.
- Le variazioni delle dimensioni della pupilla forniscono la possibilità di un controllo fisiologico.
- Non si modifica al trascorrere del tempo.
- Le prestazioni offerte in termini di velocità sono calcolabili e risultano ottime.

Svantaggi nell'uso del riconoscimento dell'iride:

- L'obbiettivo da acquisire è di dimensioni ridotte (circa 1 cm) e la distanza dal soggetto ne complica la rilevazione.
- Il soggetto durante la rilevazione è in movimento.
- La localizzazione della sua struttura deve avvenire su una superficie curva, umida e con riflessi.
- Può essere oscurata da lenti o occhiali.
- Le palpebre ne occludono parzialmente la superficie.
- La pupilla varia di dimensione.

4 Uso delle chiavi biometriche in ambito legale

Negli ultimi anni molti sforzi sono stati concentrati per definire un modello di documento elettronico che avesse valore legale. L'Italia è stato il primo paese al mondo che abbia formalizzato questa necessità; nel Decreto del Presidente della Repubblica (DPR) n. 513 del 10 novembre 1997 e nel successivo DPR n. 445 del 28 dicembre 2000 (che ne ha incorporato le disposizioni), vengono tracciate le norme che disciplinano l'uso di quella che viene definita "firma digitale", le cui modalità tecniche sono elencate nel Decreto del Presidente del Consiglio dei Ministri (DPCM) dell'8 febbraio 1999.

4.1 La firma digitale

La legislazione italiana consente l'uso legale di documenti anche in formato elettronico. Al fine di consentirne la verifica della paternità e dell'integrità è previsto l'uso della "firma digitale" che firma appartiene alla categoria più generale delle "firma elettroniche", definita e disciplinata dalla direttiva europea del 13 dicembre 1999 (n. 1999/93/CE). Nello specifico la comunità europea attua la seguente distinzione:

- Firma elettronica (semplice). Costituita da "dati in forma elettronica, allegati oppure connessi tramite associazione elettronica ad altri dati elettronici ed

utilizzata come metodo di autenticazione" (art. 2 n. 1 della direttiva). Questa definizione permette l'uso di qualsiasi metodo o tecnologia per la firma di un documento informatico, ad esempio è possibile eseguire una digitalizzazione di una firma manoscritta o dell'immagine di un'iride ed apporla sul documento elettronicamente.

- Firma elettronica avanzata. Definita come "una firma elettronica che soddisfi i seguenti requisiti: a) essere connessa in maniera unica al firmatario; b) essere idonea a identificare il firmatario; c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo; d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati" (art. 2 n. 2 della direttiva). Usando questa seconda definizione sono precluse le possibilità concesse dalla firma elettronica semplice, infatti nell'apposizione dell'immagine di una firma o di un dato biometrico in calce ad un documento, il firmatario non può conservarne il controllo esclusivo, inoltre non vi è legame col documento che consenta di identificarne una eventuale modifica.
- Firma elettronica sicura. L'appellativo sicura viene introdotto in quanto creata con un dispositivo di firma che soddisfi specifici requisiti indicati nell'allegato III della direttiva stessa.

La "firma digitale", cui si fa riferimento nell'ordinamento italiano, è basata sulla tecnologia di cifratura dei dati ed appartiene all'insieme della "firma elettronica avanzata" definita dalla comunità europea. In dettaglio è il risultato di un processo di calcolo che, a partire da un documento informatico e da alcune informazioni strettamente associate alla persona, ossia una coppia di chiavi asimmetriche, produce un nuovo documento che attesta la volontà del firmatario di sottoscrivere l'originale.

L'introduzione della biometrica sotto forma di chiave che si possa utilizzare per la cifratura o sotto forma di elemento sbloccante di una smart-card che custodisca la chiave privata per la generazione della firma elettronica, è stato proposto sotto varie forme e studiato nelle problematiche implementative [HAC+00]. Nel DPR 445/2000 si fa riferimento alla "chiave biometrica" che viene descritta come "la sequenza di

codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente". La collocazione di questa definizione vuole portare l'attenzione su questa tecnologia al fine di evitare l'equivoco, peraltro abbastanza frequente, di ritenere che l'utilizzo della sola impronta biometrica sia sufficiente per l'avvio delle operazioni connesse alla generazione della firma digitale. Prescindendo dalle questioni tecniche, possiamo osservare come nella definizione di chiave biometrica si faccia riferimento ad un meccanismo di verifica dell'identità della persona, ben lontano quindi dalla pretesa di esprimere un consenso rispetto ai documenti elettronici, quale è invece lo scopo della firma digitale. Non è ragionevolmente possibile attribuire una manifestazione di volontà ad azioni quali guardare verso un punto fisso o appoggiare il dito su una superficie.

Questo non esclude però la possibilità che le chiavi biometriche possano essere utilizzate per l'attivazione di processi serializzati o ripetitivi di generazione della firma digitale, a condizione però che tale processo sia riconducibile chiaramente alla volontà del sottoscrittore.

In merito all'espressione di consenso, negata in linea di principio ad un riconoscimento biometrico, si può ipotizzare di collocare su un diverso piano la tecnica biometrica basata sul riconoscimento della firma. Questa deriva l'espressione di volontà direttamente dalla firma manoscritta e ne mantiene il valore legale, inoltre utilizzata in combinazione con altre tecniche più affidabili (impronte digitali), potrebbe garantire ottime prestazioni. Questa soluzione sembra però non essere stata presa in considerazione nelle stesure tecniche del governo, che sembra puntare su una tecnica biometrica unica, piuttosto che su un uso di più tecniche combinate.

4.2 Carta di Identità Elettronica (CIE)

L'esigenza di informatizzare i rapporti tra apparati statali e cittadini, trova una prima risposta concreta nella realizzazione di un documento elettronico che incorpora le

funzionalità delle innumerevoli tessere e documenti utilizzati attualmente e prende il nome di carta di identità elettronica.

I suoi principi ispiratori sono i seguenti:

- Sicurezza dello strumento.
- Utilizzo come carta multiservizi.
- Interoperabilità nella pubblica amministrazione (PA) a livello nazionale.

Nel DPCM n. 437/99 contenente il "regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico" relativamente al DPR n. 513/97, si specifica quali siano i dati che debbano essere inclusi e quali invece possano essere inclusi.

La CIE deve contenere:

- I dati identificativi della persona.
- Il codice fiscale.
- I dati di residenza.
- La cittadinanza.
- La fotografia.
- L'eventuale indicazione di non validità ai fini dell'espatrio.
- Il codice numerico identificativo del documento, codice del comune di rilascio, data del rilascio e data di scadenza.
- La sottoscrizione del titolare o di uno degli esercenti la potestà genitoriale o la tutela.

Può contenere:

- I dati desunti dalle liste elettorali e comunque tutti quelli necessari per la certificazione elettorale e altri dati al fine di razionalizzare e semplificare l'azione amministrativa.

- Le informazioni e le applicazioni occorrenti per la firma digitale secondo quanto stabilito dalle regole tecniche di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513, nonché gli elementi necessari per generare la chiave biometrica.

Dalle linee guida formulate per i comuni che hanno iniziato la sperimentazione della CIE [LGC], si apprende che all'interno della stessa vengono salvati i dati biometrici del richiedente (in particolare foto, impronta, firma) sotto forma di immagini. Attualmente non è fatta menzione alcuna in merito alla possibilità di inserire "gli elementi necessari per generare la chiave biometrica", peraltro questa affermazione è ritenuta ambigua [CAM0101], non essendo chiaro, in senso tecnico, quale tipo di elementi si intenda e con quali caratteristiche biometriche si debba operare. Bisogna inoltre rilevare, come il DPR n. 513/97 prevedesse l'eventualità di memorizzare la "chiave biometrica" all'interno della CIE, peraltro l'eventuale inserimento del modello biometrico rilevato darebbe "l'esclusiva" al primo fornitore di dispositivi di lettura incaricato, non esistendo attualmente un formato di archiviazione aperto.

4.3 Implicazioni nella società

L'introduzione dell'uso di dati biometrici per espletare rapporti in formato elettronico con le pubbliche amministrazioni e con gli enti privati, mette in luce alcuni problemi inerenti la riservatezza dei dati stessi. Un dato biometrico è legato indissolubilmente alla persona che lo possiede, quindi la necessità che il suo uso sia ben regolamentato è un requisito fondamentale perché non vengano lesi i diritti personali. L'accesso da parte di un ente ai dati contenuti negli archivi può essere utile ed esemplificativa, non può peraltro essere indiscriminata. Si evidenzia quindi la necessità di prevedere diversi livelli di accesso alle informazioni che consenta alle varie amministrazioni di accedere alle stesse solo in misura delle finalità connesse e con l'assenso del cittadino interessato [GPVN9901].

Negli ultimi anni diverse società hanno adottato sistemi ad accesso controllato basato su tecniche biometriche, tuttavia la mancanza di una chiara regolamentazione ha favorito confusione e cause giudiziarie. Un episodio chiarificatore è il seguente: una nota azienda di credito che per motivi di sicurezza aveva installato un dispositivo che rilevasse l'impronta digitale associata all'immagine del viso dell'utente all'ingresso delle filiali. Nonostante le indicazioni che specificassero il mantenimento limitato nel tempo dei dati rilevati, il Garante [GPVD01] ha stabilito che le misure adottate violassero il principio di proporzionalità tra gli strumenti impiegati e le finalità prospettate, sentenziando l'uso di mezzi che comportassero minori problemi per la tutela dei diritti e della dignità delle persone interessate. L'istituto è stato di conseguenza costretto a rimuovere i sistemi installati e a fornire conferma della cancellazione dei dati biometrici acquisiti.

Con il Decreto Legislativo n. 467 del 28 dicembre 2001 a consolidamento della legge n. 675 del 31 dicembre 1996 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali), il Garante ha posto parzialmente chiarezza sulle procedure e le condizioni che regolamentano l'implementazione di sistemi ad accesso controllato e dei dati acquisiti, anche se un riferimento specifico alle tecniche biometriche non è ancora presente.

5 Campi di applicazione

Le ricerche sulle applicazioni biometriche sono state inizialmente sviluppate per impieghi in situazioni di necessità di alta sicurezza (ambienti militari) e di rispetto della legge (agenzie governative). Con l'abbassamento dei costi e con la diffusione nella società dell'informatizzazione, si sono create le condizioni per l'estensione della biometrica a campi di utilizzo quotidiano.

5.1 Applicazioni biometriche

Le applicazioni potenziali sono innumerevoli e di grande attualità, tra queste possiamo elencare:

- Commercio elettronico: sicurezza nell'identità di chi effettua una compravendita di oggetti e servizi per via telematica.
- Banking e trading: gestione sicura del conto bancario e di transazioni finanziarie.
- Uso legale: conferma di identità in remoto, blocco di accesso a documenti riservati.
- Uso assicurativo: prevenzione da frodi assicurative e reclami non autorizzati.
- Uso medico: accesso sicuro alle cartelle cliniche, indicazioni di responsabilità in caso di prescrizioni non conformi.
- Pagamento carta di credito: verifica dell'identità per gli acquisti in luogo e via telematica.
- Sicurezza in rete: verifica dell'identità per accessi LAN e WAN.

- Accesso controllato: monitorazione degli accessi in aree riservate o a beni privati.
- Smart-card: controllo dell'accesso a strumenti che si basano su questa tecnologia per il funzionamento o alle informazioni contenute.

Mostriamo ora una panoramica su alcune implementazioni pratiche che sono state sviluppate e rese operative negli ultimi anni.

Al padiglione fiere di Milano in novembre si terrà una mostra internazionale sul tema "Sicurezza 2002". Al suo interno verranno presentati prodotti del comparto della sicurezza e automazione degli edifici, tra cui alcuni utilizzano per la prevenzione approcci biometrici. Nel campo della prevenzione per gli istituti di credito possiamo ad esempio segnalare il sistema BioBank, sviluppato dalla Cometa s.n.c. come dispositivo antirapina a registrazione biometrica. L'approccio si svolge nei seguenti passi: viene rilevata l'impronta digitale e le viene associata un'immagine dell'utente acquisita tramite telecamera digitale, vengono controllati i parametri indispensabili consentendo quindi l'accesso alla banca, i due dati biometrici vengono salvati in archivi separati. Questo sistema è garantito per essere conforme alle direttive del Garante per la privacy, consente inoltre, in caso di atti contro il rispetto della legge, di fornire alle forze dell'ordine i dati necessari all'identificazione.

Un settore in cui l'uso della biometrica si sta diffondendo rapidamente a causa della forte necessità di sicurezza, è quello aeroportuale.
Nel giugno di quest anno nel quartiere fieristico padovano, si è tenuta la prima edizione del salone italiano per gli operatori, battezzata col nome "Airlogic". Uno dei settori espositivi (Airlogic Data) è stato riservato completamente ai sistemi informatici dedicati alla vita e alla sicurezza aeroportuale. Tra le novità presentate, spicca il sistema di riconoscimento del viso che verrà installato nella nuova aerostazione di Venezia, consentendo l'accesso ad alcune aree riservate solo al personale autorizzato che abbia precedentemente effettuato un'operazione di registrazione. Si ritiene che tale sistema consentirà in futuro di confrontare i profili dei passeggeri con quelli delle liste terroristiche internazionali posizionando le

telecamere lungo le corsie di imbarco. In merito all'operatività del sistema, il viceministro per le infrastrutture e i trasporti Ugo Martinat ha annunciato l'introduzione entro due anni di una carta biometrica che consentirà la creazione di corsie preferenziali per i viaggiatori abituali.

Nell'ottobre 2001 ha suscitato grande interesse l'implementazione in Olanda di un sistema di riconoscimento basato sull'iride sviluppato in collaborazione con le forze di polizia. Grazie alla precisione e affidabilità garantita da questa tecnica, l'aeroporto Schiphol di Amsterdam è stato in grado di porre in essere un sistema di verifica automatica che consente ai passeggeri abituali in possesso della *Privium card* (per un costo di € 99) di non usare più il passaporto per spostamenti all'interno della Comunità Europea, l'identità viene accertata confrontando l'impronta della loro iride con quella registrata nel pass.

Questo stesso sistema è attualmente in fase di sperimentazione a Rotterdam, dove lo si vuole utilizzare per il riconoscimento degli immigranti, così da ridurre il carico di lavoro degli uffici e nel contempo i tentativi di frode. Inoltre uno degli scopi di questo progetto è fungere da modello per i futuri passaporti.

Nel febbraio del 2002, nell'aeroporto Heathrow di Londra, è stata annunciata la sperimentazione del riconoscimento dell'iride per la durata di cinque mesi. Questa procedura verrà attivata sulla tratta transatlantica che collega Londra al nord America e sarà utilizzata al fine di snellire le pratiche inerenti il controllo del passaporto per i viaggiatori abituali. Prima della partenza l'utente verrà sottoposto ad una fase di registrazione e il modello sarà salvato nel database del servizio immigrazione, all'arrivo un dispositivo automatico controllerà la corrispondenza e in caso positivo consentirà l'accesso. Durante questa fase di sperimentazione ai passeggeri sarà comunque richiesto il possesso del passaporto.

Un approccio alternativo ai precedenti è quello in sperimentazione attualmente nell'aeroporto Gatwick, uno dei più grandi del regno unito. Per velocizzare e semplificare l'identificazione dei passeggeri e i controlli di sicurezza, è stato installato un sistema di rilevatori biometrici basati sulla doppia impronta digitale. Le informazioni rilevate sono salvate in una smart-card che viene consegnata al

passeggero, questi ne farà uso per il ritiro del biglietto di imbarco e successivamente alla barriera che controlla l'accesso all'aeroplano.

Dal gennaio 2002 il governo britannico ha disposto l'acquisizione delle impronte digitali per gli stranieri che richiedono la cittadinanza. La motivazione addotta è l'identificazione rapida di coloro che assumono comportamenti illegali, per esempio facendo più volte domanda per ottenere benefici. Si è calcolato che con le vecchie procedure la difficoltà delle verifica ha portato al governo inglese una perdita dovuta a frode trenta volte superiore rispetto al costo della messa in opera di questo sistema.

Gli usi della biometrica illustrati negli esempi precedenti avevano come obbiettivo la sicurezza in situazione di potenziale alto rischio, vi sono però altre implementazioni che si adattano piuttosto a condizioni di uso quotidiano.

Nel campo del riconoscimento vocale in aprile sono state annunciate due implementazioni per l'accesso sicuro ai cellulari. La prima azienda costruttrice a sperimentare questa soluzione sarà la Mitsubishi Electric Telecom, che ne farà uso nel modello "Trium Mondo GSM/GPRS". Il sistema richiederà la pronuncia di una frase o una parola all'accensione del telefono e l'autenticazione avverrà rispetto ad un modello di riferimento salvato nella memoria della SIM card. La soluzione basata sull'uso di questa tecnologia ormai consolidata, dovrebbe contenere i costi e contemporaneamente mantenere una buona flessibilità nei meccanismi per la salvaguardia della privacy e della sicurezza.
In Svezia, più precisamente in una scuola di Stoccolma, nel periodo compreso tra il febbraio e il giugno 2001 è stato sperimentato un sistema di autenticazione ai personal computer per gli studenti. Le motivazioni che hanno spinto verso questa tecnologia, sono essenzialmente due:

- Si è verificato che almeno uno studente per classe dimentica la password, con una conseguente perdita di tempo per consentire allo stesso di tornare in condizione di operatività.

- Si è constatato l'uso non lecito di password degli studenti più giovani da parte dei più vecchi, con il fine di navigare in rete in siti non permessi.

La tecnologia scelta è stata il riconoscimento delle impronte digitali e il tipo di rilevatori adottato si divide tra sistemi ottici e al silicio a seconda delle diverse necessità di interfacciamento al PC.
Dopo il successo del progetto pilota, un numero sensibile di scuole della capitale ha fatto richiesta per l'installazione di questo sistema in sostituzione del tradizionale.

5.2 Conclusioni

L'introduzione della tecnologia biometrica nei sistemi di autenticazione si fonda su solide basi. L'uso delle tecniche ad accesso tradizionale introduce una serie di problematiche inerenti la sicurezza quali perdita, furto, falsificazione, prestito non autorizzato, queste eventualità generano ingenti perdite sia in termini di costo, sia di perdita di dati personali con le conseguenze connesse. Inoltre tali tecniche non controllano l'effettiva identità dell'utente che richiede l'accesso. La biometrica tenta di risolvere questi problemi.
Il numero di codici che una persona che vive nella nostra società è costretta a ricordare, cresce continuamente; bancomat, carta di credito, PIN telefonici, codici di accesso alla banca sono solo alcuni dei servizi che richiedono l'uso della nostra memoria. La possibilità di dimenticarne qualcuno, anche se temporaneamente, è elevata. In alcuni casi non è del tutto possibile tenerli a mente, pensiamo ad esempio ad una chiave utilizzata per la cifratura di documenti o per la generazione della firma digitale. Ne segue che l'alternativa obbligata è scrivere questi codici in qualche luogo sicuro. Il problema è che non esiste un luogo sicuro, sarà quindi necessario cifrare il documento contenente questi dati tramite una chiave, che dovrà essere necessariamente semplice perché la si possa ricordare, e quindi poco sicura.
La chiave biometrica viene generata dalle caratteristiche proprie dell'individuo, non vi è quindi possibilità che sia soggetta alle problematiche precedentemente elencate.

L'approccio biometrico introduce comunque nuove e controverse questioni, vediamo di riassumerle e analizzarle nei punti seguenti:

- Mancanza di un unico standard supportato dall'industria.

  Il problema dell'omogeneità delle strutture di gestione e dell'interfacciamento è ormai un tema caldo da anni. Con la creazione del BioAPI Consortium e l'introduzione delle specifiche BioAPI 1.1 nel marzo 2001 si è compiuto un passo importante in questa direzione, ne è prova anche il gran numero di società a livello mondiale che vi hanno aderito. Nonostante questo le implementazioni proprietarie sono ancora molto diffuse, provocando allo stato attuale una frammentazione del mercato.
- Applicazione su popolazioni limitate.

  Questa affermazione vuole intendere la capacità discriminatoria che una certa tecnica biometrica consente. A seconda delle informazioni che si possono estrarre dalla caratteristica biometrica e dell'algoritmo usato per la comparazione delle chiavi, tecniche biometriche diverse sono adatte ad usi diversi. Alcune consentono un alto grado di sicurezza e possono essere impiegate per l'identificazione, altre solo per la verifica, altre ancora per la verifica su database di dimensioni contenute. I diversi indirizzi di una certa tecnica biometrica non possono essere considerati limitazioni a prescindere; se si dovesse discriminare fra una popolazione di un milione di individui, non sarà opportuno utilizzare il riconoscimento della geometria della mano, come non lo sarebbe stato utilizzare un codice di identificazione a sedici bit con una tecnica tradizionale.
- Decisione probabilistica.

  La risposta di un sistema biometrico non indica mai una certezza assoluta, ma esprime il grado di somiglianza tra la chiave mostrata e quella salvata in precedenza. Ne consegue che un utente autorizzato non sarà necessariamente autenticato e viceversa. Questa caratteristica, più o meno marcata a seconda del grado di sicurezza richiesto al sistema, può provocare malumori a coloro che si vedono rifiutare l'accesso senza apparente motivo, bisogna però ricordare che non sono infrequenti errori di digitazione di utente o password da parte degli utenti

durante la fase di accesso e, generalmente, con frequenza superiore ai rigetti biometrici.

- Problema di protezione dei dati.

  Questa problematica nel caso di transizione su rete, non è certo un elemento introdotto dalla biometrica, ma questa tecnologia ne mette in luce aspetti più profondi. Bisogna tenere presente che l'intercettazione da parte di un estraneo della nostra chiave biometrica, mette a rischio l'utilizzo di quel canale per un periodo di tempo prolungato (in sostanza per la vita dell'individuo, o comunque per il tempo d'uso di quel tipo di chiave). Per questo motivo è di estrema importanza che il canale su cui viaggiano i dati sia criptato e che la chiave sia crittografata.

- Rischio di perdita della privacy.

  Probabilmente l'aspetto più sentito sia dagli operatori del settore, sia dal resto della popolazione. Il fatto che la misurazione dei nostri parametri fisici siano registrate, pone problemi inerenti i diritti e la dignità delle persone. Il timore principale è la possibilità da parte di agenzie governative o di malintenzionati, di monitorare le nostre azioni e la nostra vita privata. In realtà questa eventualità è già possibile, inoltre con l'archivio unificato che porterà la carta d'identità elettronica saranno possibili controlli incrociati su scala nazionale.

Per quanto riguarda l'identificazione, le tecniche biometriche che ne sono adatte devono possedere determinate caratteristiche, quali buona accuratezza, elevata capacità discriminante e prestazioni, in termine di velocità di confronti, accettabili. Inoltre, per pensare ad una diffusione massiccia nella società, devono essere poco invasive. Le tecniche che rispondono a queste caratteristiche sono essenzialmente due: il riconoscimento dell'iride e delle impronte digitali. La prima è senz'altro la più accurata e in condizioni di necessità di alta sicurezza è probabilmente l'unica scelta possibile. La seconda offre buone prestazioni, anche se soggetta, a differenza dell'iride, a possibilità di falsificazione, ha però un grosso vantaggio in termine di dimensioni dei rilevatori e di costi di implementazione.

In campo legislativo la legge italiana è ancora ambigua circa l'eventuale uso di tecniche biometriche, i contesti in cui possono essere utilizzate e le modalità di applicazione. Attualmente vi è uniformità nell'aver definito la chiave biometrica come un mezzo di sola identificazione personale, precludendone quindi l'applicazione nel campo della firma digitale, richiedendo questa un'espressione di volontà.

In conclusione, la biometrica attualmente sembra essere l'evoluzione naturale dei sistemi tradizionali in conseguenza di un miglioramento delle tecnologie, accompagnato da una diminuzione dei costi. Le diverse necessità probabilmente favoriranno un diffondersi di sistemi differenti, adatti a soddisfare bisogni differenti. Il maggiore impedimento alla sua diffusione riguarda i problemi connessi alla privacy, tuttavia l'uso di una buona politica sociale insieme a forti garanzie per la tutela dei cittadini dovrebbero incrementare notevolmente l'accettazione pubblica.

Bibliografia

[1999/93/CE] Direttiva del Parlamento Europeo e del Consiglio dell'Unione Europea, **"Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 Relativa ad un quadro comunitario per le firme elettroniche"**, *Gazzetta Ufficiale* delle Comunità europee L. 13 del 13 dicembre 1999.

[AIP] Autorità per l'Informatica nella Pubblica Amministrazione, http://www.aipa.it

[BIO01] BioAPI Consortium, **"BioAPI Specification Version 1.1",** March 2001, http://www.bioapi.org/BIOAPI1.1.pdf (verificato in data giugno 2002).

[BKA] Biometrika, http://www.biometrika.it

[BRA00] Chiara Braghin, **"Biometric Authentication"**, University of Helsinki, Department of Computer Science, October 2000, http://www.cs.helsinki.fi/u/asokan/distsec/documents/braghin.ps.gz (verificato in data maggio 2002).

[BSL] Biometric System Lab - University of Bologna – Italy, http://www.csr.unibo.it/research/biolab.

[CAM0599] Manlio Cammarata, **"Firme digitali, canali sicuri e chiavi biometriche"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma

digitale", maggio 1999, http://www.interlex.it/docdigit/regole8.htm (verificato in data agosto 2002).

[CAM0101] Manlio Cammarata, **"Sulla rete siamo tutti criminali?"**, InterLex – Diritto Tecnologia Informazione, sezione "Tutela dei dati personali - Legge 675/96", gennaio 2001, http://www.interlex.it/675/contrglo.htm (verificato in data agosto 2002).

[CAM0102] Manlio Cammarata, **"Il Governo cancella un vanto per l'Italia"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma digitale", gennaio 2002, http://www.interlex.it/docdigit/recepimento.htm (verificato in data agosto 2002).

[CAM0702/1] Manlio Cammarata, **"Troppa confusione sulle firme 'elettroniche' - 1"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma digitale", luglio 2002, http://www.interlex.it/docdigit/confusion.htm (verificato in data agosto 2002).

[CAM0702/2] Manlio Cammarata, **"Troppa confusione sulle firme 'elettroniche' - 2"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma digitale", luglio 2002, http://www.interlex.it/docdigit/confusion2.htm (verificato in data agosto 2002).

[CAM1299] Manlio Cammarata, **"La rivoluzione informatica va avanti, l'Italia è pronta?"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma digitale", dicembre 1999, http://www.interlex.it/docdigit/cartadid.htm (verificato in data agosto 2002).

[CIE1PR] Gruppo di lavoro Carta d'Identità Elettronica, **"Il Processo di Autenticazione in Rete"**, AIPA – Anasin – Assinform – Assintel, http://www.aipa.it/attivita%5B2/carta%5B16/docum[1/circuito.pdf (verificato in data settembre 2002).

[DAU] John Daugman, **"How Iris Recognition Works"**, University of Cambridge, The Computer Laboratory, http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.ps.gz (verificato in data giugno 2002) .

[DEG1299] Luca-Maria de Grazia, **"La carta elettronica: una legge-quadro"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma digitale", dicembre 1999, http://www.interlex.it/docdigit/degraz9.htm (verificato in data agosto 2002).

[DPCM02/99] Decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999, **"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513."**, *Gazzetta Ufficiale* 15 aprile 1999 n. 87.

[DPCM 437/99] Decreto del Presidente del Consiglio dei Ministri n.437 del 22 ottobre 1999, **"Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, n. 191."**, *Gazzetta Ufficiale* n. 277 del 25 novembre 1999.

[DPI] Digital Persona Inc., http://www.digitalpersona.com, **"Guide to Fingerprint Identification"**, http://www.digitalpersona.com/Solutions/solutionspdfs/guidetofingerprint.pdf, (verificato in data agosto 2002).

[DPR445/2000] Decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000, **"Disposizioni legislative in materia di documentazione amministrativa. (Testo A)."**, *Gazzetta Ufficiale* n. 42 del 20 febbraio 2001 - Supplemento ordinario n. 30.

[DPR513/97] Decreto del Presidente della Repubblica n. 513 del 10 novembre 1997, **"Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59."**, *Gazzetta Ufficiale* n. 60 del 13 marzo 1998.

[ETC] EyeTicket Corporation, http://www.eyeticket.com, **"Biometric Technology Comparison Matrix"**, **http://www.eyeticket.com/company/biometric.html** (verificato in data agosto 2002).

[FRI+00] Robert W. Frischholz, Ulrich Dieckmann, **"BioID: A Multimodal Biometric Identification System"**, IEEE Computer, Vol. 33, No. 2, pp. 64-68, February 2000.

[GPV] Garante per la Privacy, http://www.garanteprivacy.it.

[GPVD0301] Garante per la Privacy, **"Videosorveglianza – Raccolta di impronte digitali associate ad immagini per l'accesso a banche"**, Decisione del Garante, 07 marzo 2001.

[GPVD0901] Garante per la Privacy, **"Videosorveglianza e dati biometrici – Rilevazioni biometriche presso istituti di credito"**, Decisione del Garante, 28 settembre 2001.

[GPVN5300] Garante per la Privacy, **"Carta d'identità elettronica e archivi delle pubbliche amministrazioni. Il Garante chiede maggiori garanzie per i cittadini"**, Newsletter del Garante n. 53, 11-17 settembre 2000.

[GPVN9901] Garante per la Privacy, **"Il Garante: i rischi della carta d'identità elettronica"**, Newsletter del Garante n. 99, 14-21 ottobre 2001.

[HAC+00] Gaël Haechez, Francois Koeune, Jean-Jacques Quisquarter, **"Biometrics, Access Control, Smart Cards: a not so Simple Combination"**, In Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000), Bristol, United Kingdom, Kuwer Academic Publishers, pp. 273-288, September 2000, http://www.dice.ucl.ac.be/crypto/publications/2000/Biometrics.pdf (verificato in data maggio 2002).

[ILX] InterLex – Diritto Tecnologia Informazione, http://www.interlex.it

[IOS] I/O Software Inc., http://www.iosoftware.com.

[ITF] Infineon Technologies, http://www.infineon.com, **"Infineon Technologies-Frequently Asked Questions"**, http://www.infineon.com/cmc_upload/documents/028/946/FREQUENTLYASKEDQUESTIONS.pdf (verificato in data luglio 2002).

[ITI] Iridian Technology Inc., http://www.iridiantech.com.

[JAI+99] Anil K. Jain, Salil Prabhakar, Arun Ross, **"Fingerprint Matching: Data Acquisition and Performance Evaluation"**, Michigan State University - Department of Computer Science and Engineering, March 1999, http://www.cse.msu.edu/publications/tech/TR/MSU-CPS-99-14.ps.Z (verificato in data giugno 2002).

[JAI+01] Anil Jain, Arun Ross, Salil Prbhakar, **"Fingerprint Matching Using Minutiae and Texture Features"**, Michigan State University - Department of Computer Science, May 2001, http://www.cse.msu.edu/publications/tech/TR/MSU-CSE-01-17.ps (verificato in data giugno 2002).

[LAW98] George Lawton, **"Biometrics: A New Era in Security"**, IEEE Computer, Vol. 31, No. 8, pp. 16-18, August 1998.

[LGC] Bull, Finsiel, Getronics, H.P., Siemens Informatica, **"Linee Guida per i Comuni – Stazione Emissione – Progetto di Sperimentazione CIE"**, Ministero dell'Interno, maggio 2000, http://www.pianoegov.it/UserFiles/243.pdf (verificato in data settembre 2002).

[LIN+99] Lin Hong, Anil Jain, Sharath Pankati, **"Can multibiometrics improve performance"**, Michigan State University – Computer Science and Engineering, issue 39, December 1999, http://www.cse.msu.edu/publications/tech/TR/MSU-CSE-99-39.ps (verificato in data giugno 2002).

[LIU+01] Simon Liu, Mark Silverman, **"A Practical Guide to Biometric Security Technology"**, IEEE IT Professionaal, Vol. 3, No. 1, pp. 27-31, January/February 2001.

[LUI1200] Piero Luisi, **"La chiave di accesso alla pubblica amministrazione digitale"**, InterLex – Diritto Tecnologia Informazione, sezione "Pubblica amministrazione e open source", dicembre 2000, http://www.interlex.it/pa/luisi1.htm (verificato in data agosto 2002).

[MAC1199] Enrico Maccarone, **"Le chiavi biometriche"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma digitale", novembre 1999, http://www.interlex.it/docdigit/maccaro4.htm (verificato in data agosto 2002).

[MAT+00] Václav Matyáš Jr., Zdeněk Říha , **"Biometric Authentication Systems"**, Masaryk University - Faculty of Informatics, November 2000, http://www.fi.muni.cz/informatics/reports/files/older/FIMU-RS-2000-08.pdf (verificato in data maggio 2002).

[MAT+02] Tsutomu Matsumoto, Hiroyuki Matsumotu, Koji Yamada, Satoshi Hoshino, **"Impact of Artificial "Gummy" Fingers on Fingerprint Systems"**, Yokohama National University - Graduate School of Environment and Information Sciences, May 2002, http://cryptome.org/gummy.htm, http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf (verificati in data luglio 2002).

[PAN+00] Sharath Pankanti, Ruud M. Bolle, Anil Jain, **"Biometrics: The Future of Identification"**, IEEE Computer, Vol. 33, No. 2, pp.46-49, February 2000.

[PHI+00] P. Jonathon Phillips, Alvin Martin C.L. Wilson, Mark Przybocki, **"An Introduction to Evaluating Biometric Systems"**, IEEE Computer, Vol. 33, No. 2, pp.56-63, February 2000.

[RUG0102] Franco Ruggeri, **"Gli errori tecnici dello schema di recepimento"**, InterLex – Diritto Tecnologia Informazione, sezione "Firma digitale", gennaio 2002, http://www.interlex.it/docdigit/ruggieri1.htm (verificato in data agosto 2002).

[RUG02] Thomas Ruggles, **"Comparison of Biometric Techniques"**, California Welfare Fraud Prevention System Requirements, http://biometric-consulting.com/bio.htm (verificato in data luglio 2002).

[SCH+00] Dirk Scheuermann, Scarlet Schwiderski-Grosche, Bruno Struif, **"Usability of Biometrics in Relation to Electronic Signatures"**, GMD – German National Research Center for Information Technology - Institute for Secure Telecooperation (SIT), Semptember 2000, http://www.sit.fhg.de/english/SICA/sica_projects/project_pdfs/eubiosig.pdf (verificato in data agosto 2002).

[SOF02] SoftPro GmbH & Co. KG, **"SoftPro – The Signature Professionals",** http://www.signplus.com/e/download/factfile_digital_and_classic_signature.doc (verificato in data luglio 2002).

[TIL00] Catherine J. Tilton, **"An Emerging Biometric API Industry Standard"**, IEEE Computer, Vol. 33, No. 2, pp. 130-132, February 2000.

[UMD] UMD Technology Inc., http://www.umdtech.com.

[USN] UltraScan Corporation, http://www.ultra-scan.com.

[VAN+00] Tom van der Puttte, Jeroen Keuning, **"Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned"**, Atos Origin, September 2000, http://www.keuning.com/biometry/Biometrical_Fingerprint_Recognition.pdf (verificato in data agosto 2002).

[VER] Veridicom Inc., **"Veridicom - Catalogue of Solutions"**, http://www.veridicom.com, http://www.veridicom.com/products/Veridicom_Catalogue_Short_06.20.pdf (verificato in data agosto 2002).

[VIT99] Jordi Vitrià, **"Sistemes Biomètrics"**, Centre de Visió per Computador, May 1999, http://www.cvc.uab.es/~jordi/biometvisio.pdf (verificato in data Agosto 2002).

[WIL01] Gerald O. Williams, **"Iris Recognition Technology"**, Iridian Technology Inc., 2001, http://www.argus-solutions.com/IrisRecogWilliams.pdf (verificato in data agosto 2002).

[ZAG01] Raimondo Zagami, **"La Firma Digitale"**, Convegno organizzato da ITA s.r.l. sul tema "La Firma Digitale", novembre 2001, http://www.amcorteconti.it/relazione_zagami.pdf (verificato in data Agosto 2002).

Questa pagina vuole essere un ringraziamento a ruota libera, con un ordine pressoché casuale, riguardo la mia vita e chi la colora.

voglio anzitutto ringraziare la Tizi, che mi ha sopportato (e non è facile) e sostenuto in questi anni.

grazie a Erica, perché è la mia sorellina.

grazie ai miei compagni Paolo, Fabri e Beppe, per il tempo passato insieme e inoltre:

grazie al pablo perché vicino a lui scorgo il significato di potenza,

grazie al brissio perché quattro chiacchere alle 2 del mattino possono portare lontano,

grazie al beps perché quando berrò una camomilla prima di andare a letto, avrò nostalgia dei nostri discorsi.

grazie a dany, perché l'oltrepò per qualcuno ha un significato in più.

grazie all'ale, per una serie di ragioni, di cui forse la più importante è che è l'ale.

grazie all'Alessandra, perché le voglio bene.

grazie al Marco, perché non so se l'ho mai ringraziato a sufficienza per avermi dato una mano e sostenuto negli anni.

grazie a Cristian, perché le sua perseveranza atletica mi è di stimolo a fare lo stesso.

grazie a Cristiano, perché io, lui e Bruce condividiamo la stessa passione.

grazie a Ezio e a Claudio, perché alcune persone dicono di non avere amici ma sbagliano nel dimostrarlo.

grazie al bremb, perché se esiste un mito è lui.

grazie a Emanuele e ai suoi appunti, cui devo l'aver passato Ottimizzazioni e quindi, in definitiva, la possibilità di scrivere queste pagine.

grazie a fede, ad alle, a Erika.

grazie alla Paola.

grazie alla rosy, alla susy e al gaboch, grazie alla vale, grazie a Sergio e alla naty, grazie a Gloria, grazie alla lucy, grazie alla Silvia (e auguri), grazie alla Carola, grazie a Susanna.

grazie al bido, perché ci basta una sola occhiata per capirci.

grazie a tutti i miei familiari (in senso esteso), che da anni attendevano questo momento.

grazie di cuore tutti coloro che mi vogliono bene (e sono tanti), e che magari (sicuramente) mi sono scordato di citare (abbiate comprensione, sono le ore 04:03).

grazie al vento che mi ha dato la possibilità di assaporare i piaceri della vela e del windsurf.

grazie a me perché non ho mollato ...

Questa tesi è stata realizzata utilizzando OpenOffice.org