Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608

Ufficio: +39 0521 385510
FAX: +39 0521 386473

E-mail:
info@primasicurezza.com

BIOMETRIA

Fonte: www.eter.it

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608

Ufficio: +39 0521 385510
FAX: +39 0521 386473

E-mail:
info@primasicurezza.com

Introduzione

1.1 Il principio

La necessità di identificare le persone correttamente ed irrevocabilmente esiste da molto tempo.
L'autorizzazione ad entrare in un edificio, ad aprire un armadietto, a varcare un confine, a prelevare denaro da una banca etc. è sempre collegata all'identità di una persona.
È perciò necessario dimostrare tale identità in un modo o nell'altro. Definiamo questa procedura Verifica. Una persona sostiene di essere autorizzata o di avere una determinata identità e ciò deve essere verificato.
È un problema noto alla polizia, per esempio con persone che presentano una carta d'identità sospetta. Tuttavia, la polizia si trova spesso di fronte ad un altro tipo di problema: chi è la persona che ha lasciato una determinata traccia, per esempio un'impronta digitale, oppure chi è questo cadavere. In questo caso si ricerca l'identità di una persona sconosciuta, facciamo quindi una Identificazione. Gli specialisti della Biometria utilizzano l'espressione uno a uno quando si tratta di verifica, oppure uno a tanti quando si tratta di identificazione. Il testo che segue tratta essenzialmente di verifica che è il caso più comune in ambienti non legati all'applicazione della legge.

1.2 Cenni Storici

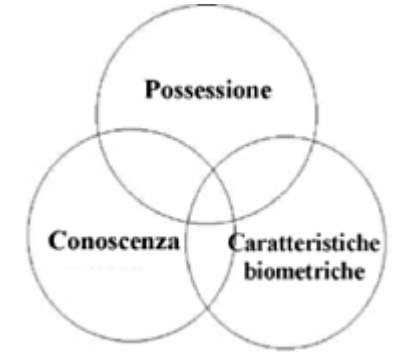


Fig. 1: Metodi di verifica

Probabilmente la più antica attestazione di identità e di autorizzazione basata su mezzi tecnici, e non sul riconoscimento personale, è la chiave meccanica.
In questo caso l'attestazione di identità si basa sul possesso. Tutte le card in plastica leggibili (con sistemi di memorizzazione dati magnetici, elettrici o ottici) sono esempi della stessa categoria.

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Tali metodi di attestazione di autorizzazione hanno raggiunto un livello tecnico elevato ed alcuni di loro sono molto difficili da copiare o da falsificare. Presentano tuttavia uno svantaggio intrinseco: il sistema tecnico è in grado di verificare l'identità e quindi l'autorizzazione della carta o della chiave ma non l'identità del portatore. In altre parole: la card o la chiave in proprio possesso possono essere rubate, perdute o cedute a persone non autorizzate.
Sistemi basati sulla conoscenza anzichè sul possesso hanno il fine di evitare questo problema. La password rappresenta la prima forma di questo tipo di identificazione. Di recente tali metodi sono stati automatizzati mediante l'utilizzo di password di accesso a computer o di codici ID. Non è quindi possibile un uso improprio in seguito a furto ma è pur sempre possibile che qualcuno acquisisca in qualche modo tali informazioni e ne faccia poi un cattivo uso. Malgrado tutte le avvertenze, un certo numero di utenti annota, per fare un esempio, il codice ID delle proprie carte di credito, e questo ne riduce il valore di sicurezza a zero.
La combinazione di possesso e sistemi di conoscenza riduce ulteriormente la possibilità di un utilizzo improprio, ma non elimina il problema principale ovvero che il portatore non è inconfutabilmente identificato. L'unico mezzo per poter identificare una persona inconfutabilmente è quello di riconoscerne automaticamente le caratteristiche personali. Queste sono definite caratteristiche biometriche e la tecnologia alla base di tale identificazione è chiamata Biometria. Esistono molte caratteristiche biometriche che possono essere rilevate. Alcune di queste sono riscontrabili in forma scritta in qualsiasi passaporto. Tuttavia, la rilevazione automatizzata ed il confronto automatizzato con dati immagazzinati in precedenza prevede che le caratteristiche biometriche possiedano le seguenti proprietà:
Invariabilità delle proprietà. Devono essere costanti per un lungo periodo di tempo.
Misurabilità. Le proprietà devono essere tali da poter essere rilevate senza tempi di attesa e altre complicazioni.
Singolarità. Le caratteristiche devono avere proprietà sufficientemente uniche tali da permettere di distinguere una persona da qualsiasi altra.
Accettabilità. L'acquisizione di tali caratteristiche deve essere possibile in un modo accettabile da un'ampia percentuale della popolazione. Sono escluse tecnologie particolarmente invasive, ossia tecnologie che prevedano l'asportazione di una parte del corpo umano o che ne determinino una evidente menomazione.
Riducibilità. I dati acquisiti devono poter essere ridotti ad un file di facile gestione.
Affidabilità. Il procedimento deve garantire un grado elevato di affidabilità e di riproducibilità.
Privacy. Il procedimento non deve violare la privacy della persona.

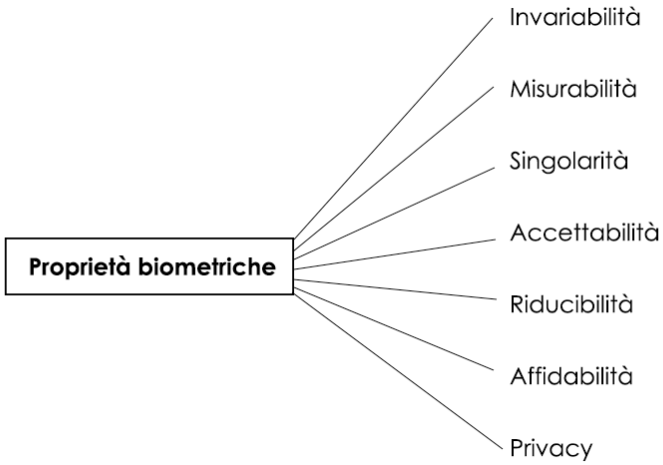


Fig. 2 Requisiti per la selezione delle proprietà biometriche

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Date queste proprietà, il numero di caratteristiche biometriche utilizzabili si riduce ad alcune solamente che sono già state testate nel passato. La tavola che segue ne fornisce una panoramica.

- Caratteristiche Tecnologia di Acquisizione:
  - Invariabilità
  - Singolarità
  - Accettabilità
- Geometria della mano Ottica (IR) Buona 1:1000 Molto buona
- Geometria delle due dita Ottica (IR) Buona 1:1000 Molto buona
- Retina Ottica Molto buona 1:1 milione Non buona (invasiva)
- Iride dell'occhio Ottica Molto buona 1:6 milione Non buona
- Vene
- Superficiali della mano Ottica (IR) Buona Non nota Molto buona
- Firma Dinamica
- (pressione) Non buona 1: 10000 Molto buona
- Voce Elettroacustica Non buona 1: 10000 Buona
- Volto Ottica o IR Buona Non nota Buona
- Impronte digitali Ottica, capacitiva, ecc. Molto buona 1:1 milione Buona

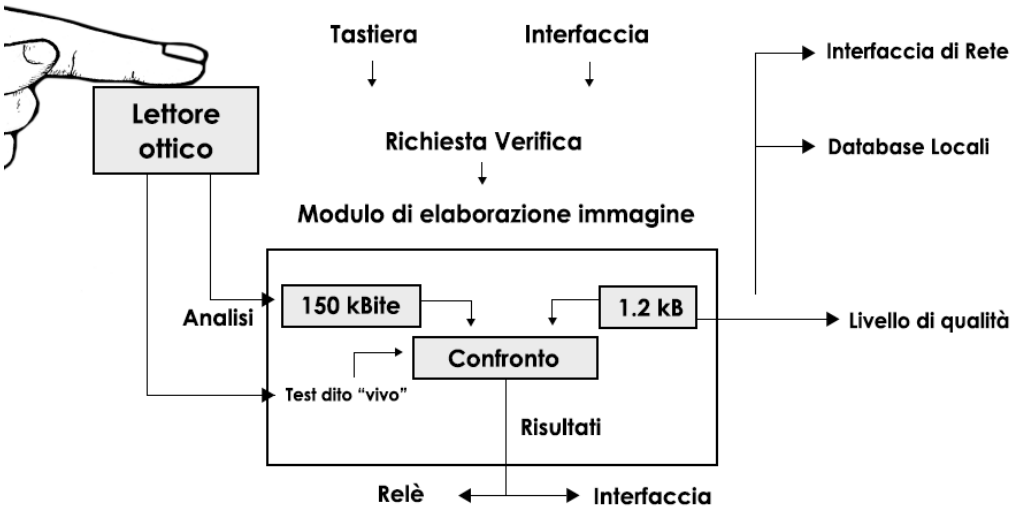
Per una discussione dettagliata dei pro e dei contro di queste tecnologie e dello stato dell'arte, si veda il capitolo successivo. Altre caratteristiche, come per esempio il peso, le dimensioni, il colore degli occhi e dei capelli e proprietà speciali, riscontrabili nei passaporti, non possono essere utilizzate poichè non soddisfano criteri come la singolarità, la misurabilità o l'invariabilità.

2 Presupposti tecnologici

2.1 Registrazione e verifica

Presupposti per verificare l'identità di una persona: La persona deve essere registrata nel sistema come XY, e deve essere memorizzato un file che ne contenga le caratteristiche biometriche. Ogni verifica ha inizio con una registrazione, per esempio nel caso delle verifiche delle impronte digitali:

- Selezione di un codice ID
- Presentazione del dito
- Calcolo del template dell'impronta del dito
- Ulteriori presentazioni del dito



Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Fig.3 Esempio del procedimento di verifica

Adesso può avere luogo il confronto, il quale dimostra se la persona che sostiene di essere XY ha le stesse caratteristiche biometriche. Per fare ciò è necessario:

- Immettere i dati relativi all'identità dichiarata della persona
- Richiamare dalla memoria il file relativo alla persona
- Rilevare le proprietà biometriche
- Confrontare le proprietà rilevate con i dati memorizzati
- Visualizzare e/o utilizzare il risultato
- Fattori importanti sono:
    - Acquisizione chiara e riproducibile
    - Velocità e precisione del confronto

L'elettronica moderna riesce facilmente a rispondere q questi requisiti. La progettazione di questi dispositivi si basa su tecnologia a microprocessori, telecamere miniaturizzate, tecnologia di luce moderna e altro.
La continua diminuzione dei costi dei componenti elettronici ha reso possibile la miniaturizzazione dei dispositivi ed ha permesso una maggiore efficienza ed una maggiore economicità delle unità. Alcuni dei dispositivi reperibili sul mercato sono il risultato di più di 15 anni di sviluppo.
Possiamo senza dubbio affermare che la tecnologia della biometria è ormai matura.

2.2 Valutazione dei sistemi biometrici

Cinque valori sono importanti nella valutazione dei sistemi biometrici:

- Tempo necessario per la registrazione
- Tempo necessario per la verifica
- Falsa Accettazione (False Acceptance Rate, FAR, valore di falsa accettazione, tipo di errore 2), la verifica di una persona che non è registrata
- Falso Rifiuto (False, Reject Rate, FRR, valore di falso rifiuto, o tipo di errore 1), non verifica di una persona registrata.
- Valore di Errore Uguale (Equal Error Rate, EER, il punto in cui il valore di Falsa Accettazione e Falsi Rifiuti si equivalgono.

Benchè questi valori siano considerevolmente migliorati nel corso dell'evoluzione di tutti i sistemi conosciuti, esistono ancora differenze importanti da un sistema all'altro, in parte dovute al metodo di identificazione prescelto. Fino ad ora non esistono standard per i test.
Molto è stato fatto per arrivare alla standardizzazione ma sono state riscontrate varie difficoltà per via della differente natura dei sistemi.
Il valore più difficile da giudicare è il falso rifiuto. I falsi rifiuti dipendono in gran parte dal comportamento dell'utente per questo motivo una standardizzazione sarebbe particolarmente utile.

2.3 Acquisizione delle caratteristiche biometriche (sensori)

Il metodo di acquisizione più diffuso oggigiorno è quello ottico. Nelle maggior parte dei casi, vengono utilizzate telecamere CCD miniaturizzate che rilevano luce visibile o a infrarossi. Il tipo di strumentazione ottica dipende dalla proprietà biometrica rilevata.
Il rilevamento delle impronte digitali prevede il posizionamento del dito su di un prisma mentre l'illuminazione è distribuita in modo tale da riflettere la luce nella sua interezza sulla superficie di posizionamento fatta eccezione per quei punti dove la pelle tocca la superficie di appoggio (riflessione modificata).
La geometria della mano utilizza due telecamere alfine di rilevare le dimensioni delle dita e della mano che è posizionata su di una piastra metallica e adeguatamente illuminata.

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608

Ufficio: +39 0521 385510
FAX: +39 0521 386473

E-mail:
info@primasicurezza.com

L'acquisizione delle proprietà della retina utilizza un raggio di luce che effettua la scansione della retina. I raggi riflessi producono un'immagine in intensità della struttura della retina rilevata.
L'acquisizione delle proprietà dell'iride funziona in modo simile a quella della retina. Il riconoscimento del volto acquisisce un'immagine del volto con una telecamera, a luce visibile o a infrarossi, ed elabora l'immagine per ottenere determinati criteri.
I metodi più recenti, in particolare l'acquisizione delle impronte digitali, tentano di allontanarsi dal rilevamento ottico che necessita di un modulo ottico e quindi limita la miniaturizzazione. Tali metodi utilizzano la temperatura, la pressione e/o la capacità.
La capacità in particolare sembra essere promettente in quanto può essere misurata con un chip in silicio miniaturizzato. Non appena questi metodi otterranno precisione, stabilità ed un costo ridotto, andranno probabilmente ad integrare, se non a sostituire, i metodi ottici esistenti. L'acquisizione della firma utilizza una tavoletta sensibile alla pressione oppure rileva la posizione della penna con sistemi ultrasonici o elettrici.
Il riconoscimento vocale necessita semplicemente di un microfono di qualità sufficiente.

2.4 Calcolo dei template

Una fase importante nel processo di registrazione è il calcolo del template. Il template, successivamente utilizzato nel processo di comparazione durante la verifica, è una riduzione dei dati delle caratteristiche biometriche originarie e dovrebbe:

- essere il più possibile piccolo, ma possedere sufficienti proprietà distintive
- consentire un calcolo rapido
- garantire la singolarità
- essere idoneo ad una verifica rapida

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Quanto più l'algoritmo saprà rispondere a questi requisiti in parte contraddittori, tanto maggiore sarà la qualità del procedimento selezionato. Gli algoritmi di registrazione e verifica risultano dunque essere gli elementi più importanti nella biometria.
I microprocessori disponibili 15 anni fa, agli albori della biometria, rendevano relativamente difficile trovare algoritmi che fossero sufficientemente rapidi e precisi. Anche oggi, molti dispositivi sono collegati ad un PC ad alta velocità che gestisce la vera e propria operazione di comparazione. Dispositivi a sè stanti, ossia dispositivi indipendenti da un PC come quelli di cui necessita un controllo di accesso fisico, erano, nel passato, dotati di ASICs (circuiti integrati per applicazioni specifiche) nei quali era implementato l'algoritmo. I microprocessori più recenti comunque, piccoli e a ridotto consumo energetico, sono sufficientemente potenti per gestire tali algoritmi.
È quindi possibile adesso progettare unità indipendenti senza il costo dell'integrazione in un ASIC.

2.5 Sicurezza della verifica

Alcune applicazioni non sono molto esigenti in termini di sicurezza della verifica (falsa accettazione), sia perchè combinano vari metodi di verifica, sia perchè, per via della loro natura, non necessitano di un elevato grado di sicurezza.
Altre applicazioni, particolarmente quelle destinate ad utilizzi in ambiti governativi, necessitano di un grado di sicurezza assai elevato. Testare la sicurezza di un algoritmo è un compito difficile. Solitamente un singolo utente non è in grado di misurare il valore di Falsa Accettazione di un dato dispositivo, in quanto non è in possesso di migliaia di campioni (persone) per ottenere risultati di una qualche rilevanza statistica. I più noti fornitori di prodotti biometrici utilizzano database di template di notevoli dimensioni e talvolta pubblicano i loro risultati.
Purtroppo non esistono molti istituti indipendenti in grado di effettuare test di sicurezza validi.

3 Apparecchiature per l'utilizzo delle proprietà fisiologiche

3.1 Geometria della mano e delle dita

La geometria della mano è stato uno dei primi metodi apparsi sul mercato. L'unità chiamata ID3I dai Sistemi di Riconoscimento negli USA prevede la presentazione della mano destra e le dita sono posizionate da guide. La dimensione della mano è registrata con telecamera e specchi e, a partire da tale registrazione, viene calcolato un template di 9 byte. Il template è memorizzato insieme ad un codice PIN o al nome della persona. Il dispositivo può essere utilizzato in modalità indipendente e può memorizzare fino a 20.000 template. La verifica consiste nel dichiarare l'identità della persona (per es. la digitazione di un PIN) e nella presentazione della mano, mentre le dimensioni sono confrontate con il template in memoria. I vantaggi principali di tale dispositivo sono la velocità di funzionamento, un template di dimensioni ridotte, buona accettazione da parte degli utenti e l'assoluta non interferenza con la privacy dell'individuo. Sono state tuttavia manifestate perplessità circa l'aspetto igienico del metodo (posizionamento di tutta la mano sulla piastra). Ecco le caratteristiche di tale dispositivo:

- Tempo di registrazione: pochi secondi
- Tempo di verifica: un secondo
- FA: 1 : 1.000
- FR: 1%

Poichè si è trattato del primo dispositivo con un tempo di verifica molto breve, è stato venduto per varie applicazioni. Tuttavia, il valore elevato di Falsa Accettazione (per quanto confutato dai produttori) lo rende non idoneo ad alcune applicazioni. Il dispositivo accetta solo la mano destra. I tecnici che hanno contribuito allo realizzazione del rilevatore della geometria della mano, hanno messo a punto un dispositivo che mette a confronto la geometria di due dita.

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Il suo nome è Digi-2, ed è prodotto in Svizzera. È chiaro che tale dispositivo non controlla l'impronta digitale ma la dimensione delle dita.
L'utilizzo di tale apparecchiatura non è ancora diffuso e le caratteristiche, a parte quelle date dal produttore, sono tuttora sconosciute.

3.2 Controllo delle vene

È risaputo che un gruppo sta lavorando sul controllo del pattern delle vene del dorso della mano. Le vene sono riconosciute con una telecamera a infrarossi e ne viene poi calcolato un template. Non sono note altre caratteristiche.

3.3 Controllo della retina

Un dispositivo noto come Eydentify è conosciuto da più di 10 anni. Tale dispositivo effettua una scansione della retina dell'utente tramite un raggio di luce e calcola un template di 256 byte che viene poi utilizzato per la verifica. Il dispositivo ha le caratteristiche seguenti:

- Tempo di registrazione: 30 secondi
- Tempo di verifica: 0,5 secondi
- FA: 1:1 milione
- FR: 1%

Per la verifica, è necessario che fra il dispositivo e l'occhio vi sia una distanza di circa 10 cm; ecco perchè il posizionamento dell'occhio gioca un ruolo importante. Pare che gli occhiali e le lenti a contatto non influenzino il funzionamento del dispositivo.
La sicurezza contro le contraffazioni è molto elevata. Tuttavia tale dispositivo non riscuote molto successo poichè il metodo non è molto accettabile da parte degli utenti.

3.4 Controllo dell'iride

Viene effettuata una scansione dell'iride dell'occhio umano tramite una camera. L'iride contiene una quantità di proprietà distintive sei volte superiore a quelle della retina o delle impronte digitali. Si tratta quindi di un metodo estremamente affidabile. Il problema del dispositivo è il posizionamento ossia è necessario "perlustrare" l'occhio dell'utilizzatore.
A tutt'oggi sono stati fabbricati solo pochi esemplari di dispositivi del genere e non sono ancora note caratteristiche ben definite. Senza dubbio si tratta di un'idea interessante, ma ci sono, così come per la scansione della retina, dubbi riguardanti l'accettabilità da parte degli utilizzatori.

3.5 Riconoscimento del volto Si conoscono due possibilità:

- riconoscimento delle relative posizioni delle caratteristiche del volto (occhi, naso, bocca, etc.).
- riconoscimento del pattern infrarosso del volto.

Entrambi i sistemi sono stati realizzati in prototipi o in serie ridotta. Non sono note caratteristiche testate. Un problema è l'eliminazione degli effetti dovuti al cambiamento della luce ambiente. Molte università stanno lavorando al miglioramento del sistema.

3.6 Riconoscimento delle impronte digitali

Attualmente, nella maggior parte dei casi, il rilevamento delle impronte digitali è effettuato tramite scansione ottica. Il dito viene posizionato su di un prisma. Là dove la pelle tocca il vetro, la luce viene diffusa anzichè riflessa (riflessione modificata) e l'immagine che ne risulta è rilevata da una telecamera CCD. Sono stati messi a punto altri dispositivi di rilevamento, come quello tramite ultrasuoni, il rilevamento termico/tramite pressione, per capacità . Gli ultrasuoni non sono ancora stati utilizzati per via del costo elevato e gli altri metodi sono ancora in fase di prova. L'elaborazione dell'immagine e la verifica dopo la rilevazione possono essere effettuati in due modi:
Il primo metodo consiste (molto similmente al lavoro della polizia) nell'esaminare le cosiddette minutiae (terminazioni, incavi, biforcazioni, ghiandole sudorifere), che vengono misurate e danno come risultato il

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

template. Alla verifica, viene usato lo stesso procedimento, e il risultato viene messo a confronto con il template in memoria (minutiae matching, confronto delle minutiae).
Il secondo metodo memorizza elementi di immagini selezionate come il template. Alla verifica, tali elementi di immagini sono utilizzati per controllare immagini simili del dito presentato e per verificare che coincidano con il template (pattern matchig, confronto dei pattern)
Entrambi i metodi danno come risultato simili valori di sicurezza, il primo metodo tuttavia necessita di tempi di verifica un po' più lunghi.

- tempo di registrazione: 10 a 30 secondi a seconda del tipo di dispositivo
- tempo di verifica: 1 a 0,5 secondi
- FA: da 1:100.000 a 1:1.000.000 o oltre
- FR: 1% o meno

Sono noti diversi dispositivi del genere. Il primo dispositivo di questo tipo, in ordine cronologico, è probabilmente l'apparecchiatura di Identix Inc., California, che al momento sta presentando la terza e quarta generazione di dispositivi. L'algoritmo di questi dispositivi è operante in un ASIC o in un microprocessore che lo rende indipendente dai PC collegati. Altri sistemi sono Identicator (USA) (che adesso appartiene al gruppo Identix), Morpho Systems (Francia), Startek (Taiwan), Dermoprint (Ungheria), VAI (Italia), Digicomp (Italia) etc. La maggior parte di questi sistemi ha il proprio algoritmo implementato su di un PC. Non molti produttori offrono il cosiddetto rilevamento del dito vivo. Lo scopo di ciò è di inibire la verifica di una copia del dito (per es, un falso al silicone) o, in casi estremi, di un dito tagliato di una persona registrata. Molte proprietà possono differenziare un dito vivo da uno finto o morto ma non tutte sono praticabili perchè

- non sono sufficientemente sicure
- il rilevamento è troppo costoso
- l'impatto tecnico è troppo importante
- necessitano di troppo tempo

il rilevamento non è sufficientemente significativo

3.7 Altre proprietà fisiologiche

Si è cercato spesso di utilizzare proprietà fisiche talvolta veramente insolite. Le seguenti sono state rese note:
Forma dell'orecchio esterno: presenta difficoltà quando l'orecchio è coperto da capelli.
Odore del corpo umano (!)
Struttura del palmo: tale proprietà è spesso utilizzata dalla polizia, ma presenta problemi dovuti a varie ragioni: l'interno della mano è ricurvo, risulta perciò difficile da rilevare ed ha molte informazioni che rendono difficoltosa la selezione.
Queste proprietà non sono rappresentate finora in prodotti disponibili in commercio e non se ne conoscono le caratteristiche.

4 Apparecchiature per utilizzare le proprietà comportamentali.

Il problema principale nell'acquisire ed utilizzare le proprietà comportamentali è la distinzione fra caratteristiche variabili ed invariabili. Per questo motivo tali proprietà sono meno esatte rispetto alle proprietà fisiologiche e sono utili solo in applicazioni molto particolari.

4.1 Firma

L'attrattiva principale di un tale metodo risiede nel fatto che il mondo finanziario utilizza la firma come il metodo di identificazione preferito. I rilevatori biometrici della firma tuttavia non si limitano a controllare l'immagine della firma completa ma anche la dinamica dei movimenti durante la firma. Sono noti vari dispositivi di questo tipo. Il valore di Falsa Accettazione è piuttosto alto (fino al 10%), ma è un valore accettabile per esempio, per applicazioni nel settore bancario, dove si utilizzano parallelamente altri mezzi di identificazione.

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Molte applicazioni non sono idonee in quanto il procedimento necessita di tempo e di spazio ed è inutile nel caso di persone analfabete (paesi in via di sviluppo).

4.2 Riconoscimento vocale

Il vantaggio principale dei sistemi di riconoscimento vocale risiede nel fatto che il sensore è molto semplice e può essere posizionato ovunque: è sufficiente il ricevitore del telefono. Tuttavia i valori di Falsa Accettazione e di Falso Rifiuto sono relativamente alti e ciò significa che il metodo è utile solo se simultaneamente si impiegano altri mezzi di identificazione. I dispositivi di questo tipo analizzano il flusso energetico e l'andamento spettrale del discorso, nella maggior parte dei casi una parola particolare. I dispositivi hanno una tolleranza elevata (quindi un livello di sicurezza relativamente basso) oppure valori di Falso Rifiuto elevati.

4.3 Pressione esercitata sui tasti

Sono stati fatti vari tentativi per utilizzare la pressione esercitata sui tasti delle tastiere dei PC come proprietà distintiva. Due problemi hanno reso difficoltoso questo approccio:

Tastiere di marche diverse possiedono caratteristiche diverse

Le persone non abituate all'utilizzo delle tastiere normalmente non hanno caratteristiche riproducibili del proprio modo di premere i tasti.

Secondo le informazioni in nostro possesso, non esistono al momento prodotti in vendita con tali caratteristiche.

4.4 Sommario

Osservando il mercato negli ultimi 10 anni, questi sono risultati essere i prodotti di maggior successo: Sono stati utilizzati principalmente rilevatori della geometria della mano e sistemi di verifica delle impronte digitali. Sembra che l'utilizzo della mano come mezzo di verifica sia accettato da un pubblico più ampio. La verifica della retina è stata utilizzata solo in ambienti ad alta sicurezza e quindi non ha avuto una gran diffusione. Sono stati fatti importanti tentativi per testare il riconoscimento dell'iride e del volto, a tutt'oggi non si conoscono applicazioni più importanti. Tutti gli altri metodi, per quanto interessanti in casi particolari, non hanno avuto un successo di mercato significativo.

5 Applicazioni

In generale, esistono molte applicazioni possibili per i sistemi biometrici. Il loro vantaggio principale è evidente in tutti i casi in cui la necessità è quella di controllare senza possibilità di dubbio l'identità di una persona. Perchè questo tipo di identificazione non ha ancora fatto passi avanti nel mercato? Ci sono diverse ragioni possibili:

La tecnologia è relativamente nuova. Sebbene le prime unità siano comparse sul mercato 15 anni fa, queste erano ingombranti, lente ed eccessivamente costose

L'evoluzione dei principali sistemi esistenti (per es. la verifica di un utilizzatore di un ATM) necessita di investimenti considerevoli e questo significa che occorre del tempo per implementare i sistemi.

Il costo di un'unità biometrica è ancora considerevolmente più elevato di quello di un lettore di bande magnetiche, sebbene i prezzi stiano diminuendo rapidamente.

Un argomento di cui si sente frequentemente parlare è quello della non accettazione da parte dell'utenza. L'esperienza dimostra tuttavia che questo problema è molto meno rilevante di quanto non si aspetti la maggioranza dei possibili acquirenti.

La mancanza di standardizzazione ha costretto le principali società a ritardare l'implementazione di tali sistemi in quanto non vogliono essere legate ad un singolo produttore con un prodotto proprietario.

Ciò nonostante, negli ultimi anni sono state introdotte alcune applicazioni principali. Eccone di seguito alcuni esempi.

5.1 Controllo degli accessi

I primissimi utilizzatori di sistemi biometrici come mezzi di controllo di accesso a edifici e installazioni sono stati varie organizzazioni militari e clienti con livelli di sicurezza elevati come banche e centrali nucleari.

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Sempre più persone si rendono conto che la biometria presenta vantaggi non solo per le applicazioni ad alto livello di sicurezza. La semplicità di utilizzo ("la chiave è sempre con te") rende questi sistemi molto attrattivi anche per altre applicazioni. Sappiamo di varie industrie e organizzazioni di servizi che hanno introdotto la biometria per controllare l'accesso non solo dei propri dipendenti ma anche di clienti e visitatori. Ci aspettiamo una rapida crescita del numero di applicazioni in questo campo nei prossimi anni. Non sarà comunque mai un mercato di grande volume poichè il numero di unità è solitamente limitato al numero delle entrate.

Esempi

Un centro di gioiellerie con circa 5.500 dipendenti e più di 7.000 visitatori all'anno utilizza rilevatori di impronte digitali. Più di 30 accessi controllati, oltre al banco della reception, sono dotati di dispositivi di rilevamento.

Diverse centrali nucleari integrano il proprio sistema di controllo accessi tramite badge con i sistemi biometrici per proteggere le zone critiche interne.

L'accesso di camion in un porto importante è protetto da rilevatori dalla geometria della mano e, in un aeroporto importante, l'accesso dei camion necessita della verifica delle impronte digitali del conducente.

Le cassette di sicurezza delle banche sono state spesso protette tramite riconoscimento delle impronte digitali o del volto. In questo modo il cliente è in grado di aprire la cassetta di sicurezza senza l'intervento dell'impiegato della banca.

In diverse banche è appena iniziato il controllo dell'accesso alle camere blindate tramite impronte digitali.

5.2 Rilevazione presenze

Gli specialisti ritengono che la frode nei sistemi di rilevazione presenze (timbratura "per conto terzi") corrisponda approssimativamente alla perdita di un'ora di lavoro per dipendente alla settimana. Molti datori di lavoro non accettano una cifra così elevata, comunque sia, la frode viene comunque perpetrata. Particolarmente esposte a questo tipo di frode sono le società con personale a frequente ricambio o comunque temporaneo o stagionale. La biometria applicata ai sistemi di rilevazione presenze elimina completamente questo tipo di frode. Abbiamo calcolato degli esempi che dimostrano che l'eliminazione di questo tipo di frode ha permesso di ripagare l'intero impianto biometrico in 6 mesi. Negli Stati Uniti è stato previsto che nel prossimo futuro circa il 10% di tutti i sistemi di rilevazione presenze saranno dotati di unità biometriche.

Esempi

Una catena di supermercati con 450 punti vendita controlla le ore di lavoro dei circa 7500 dipendenti con un sistema di rilevamento delle impronte digitali. Ciò è particolarmente raccomandabile per un tipo di personale stagionale o con ricambio rapido. Le unità di rilevamento delle impronte digitali devono inviare le informazioni tramite connessione modem dial-up.

I sindacati, che inizialmente protestavano, si sono presto convinti dei vantaggi presentati da un tale sistema, in quanto la frode perpetrata dai datori di lavoro (mancata registrazione delle effettive ore di lavoro) è altresì scomparsa.

Lo State Privacy Committe (commissione per la tutela dei dati personali) ha stabilito che non sussiste violazione della privacy.

5.3 Controlli alle frontiere, carte d'identità e passaporti

Tali applicazioni sono difficili per via della registrazione di un numero enorme di persone. D'altro canto la compatibilità dei sistemi alle varie frontiere di stato è difficile da raggiungere con la mancanza di standardizzazione dei sistemi biometrici.

Esempi

L'aeroporto di Schipol ad Amsterdam è stato il primo aeroporto pilota a controllare e velocizzare l'attraversamento delle frontiere. I frequent flyers potevano comprare una smartcard contenente il template dell'impronta digitale del proprietario che avrebbe permesso loro di evitare il controllo della polizia di frontiera

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608

Ufficio: +39 0521 385510
FAX: +39 0521 386473

E-mail:
info@primasicurezza.com

all'arrivo. Il sistema era limitato ai cittadini della nazione ed è stato soppresso dopo una fase pilota (tecnicamente riuscita), per quello che ci è dato sapere, per ragioni commerciali.
Altri esperimenti pilota sono stati condotti in vari aeroporti degli Stati Uniti e del Canada, alcuni utilizzando la geometria della mano, altri le impronte digitali. Fino ad ora non sono state prese decisioni circa l'introduzione definitiva di questi sistemi. Diversi paesi stanno discutendo progetti miranti a controllare i passaporti e/o le carte di identità biometricamente. Finora nessun paese ha preso decisioni definitive ma sono in corso esperimenti pilota e la discussione dei vari progetti procede.

5.4 Pagamenti della previdenza sociale

Il livello di frode nei pagamenti della previdenza sociale e delle pensioni statali è decisamente alto in molti paesi. I pagamenti vengono corrisposti a persone defunte, a persone non autorizzate e sono frequenti i casi di doppio pagamento. In questo modo lo stato è esposto ad una perdita assai consistente, che in alcuni casi ha raggiunto l'equivalente del totale del denaro da corrispondere. Tuttavia è da osservare che i sistemi di verifica del tipo summenzionato (uno a uno) non contribuiscono ad eliminare la registrazione ripetuta della stessa persona.
Perciò il metodo di verifica uno a uno dovrebbe sempre essere integrato da un controllo accurato (uno a molti) della registrazione nel sistema. Di recente, sono state messe a punto delle soluzioni molto più semplici ed economiche rispetto al cosiddetto AFIS (sistema di identificazione delle impronte digitali automatico) che sono state ideate per il lavoro svolto dalla polizia, ma sono al tempo stesso meno esigenti perchè non richiedono lo stesso livello di qualità necessario nei confronti di natura legale. Gli stessi problemi devono essere risolti con le carte di identità e i passaporti.
Esempi
Il primo paese a controllare i pagamenti della previdenza sociale con i sistemi biometrici è stato il Sud Africa. In questo paese, anche l'analfabetismo ha avuto un certo peso. Altri sistemi del genere sono in fase di introduzione in Spagna e in Colombia. Tutti e tre i sistemi si basano sulle impronte digitali.

5.5 Sicurezza dei computer e delle reti di dati

Gli specialisti sanno che proteggere i dati con delle password, che è il sistema usato più di frequente oggigiorno, è problematico. La maggior parte delle persone, a meno che non sia impossibilitata a farlo, utilizza password banali come la propria data di nascita, il primo nome e così via. Se l'utilizzo di combinazioni banali è escluso dal software e il sistema richiede cambi di password troppo di frequente, si sviluppa la tendenza a scrivere da qualche parte la propria password, che spesso si troverà sulla parte inferiore della tastiera o nel primo cassetto della scrivania.
Questo riduce il valore di sicurezza della password quasi a zero. Siate onesti con voi stessi: avete mai comunicato la vostra password per telefono al vostro collega o alla vostra segretaria per permettere loro di guardare qualcosa sul vostro PC? Sappiamo di esempi in paesi non europei dove le password nei sistemi bancari hanno dato luogo a frodi imponenti. Questo è possibile potenzialmente anche nel mondo occidentale.
I sistemi basati sulle card permettono una maggior sicurezza e per questo motivo sono stati introdotti in una serie di casi anche, senz'altro, per via del prezzo ridotto dei lettori di card. I sistemi di sicurezza basati sul possesso presentano, come già spiegato in precedenza, svantaggi intrinseci. Di recente, i sistemi basati sulla rilevazione delle impronte digitali hanno acquisito notorietà per via delle problematiche legate alla sicurezza dei dati nei computer. Questo potrebbe permettere l'apertura di un mercato importante per i sistemi biometrici.
Esistono tre settori di applicazione principali:
Controllo di accesso ai computer. Questi sistemi proteggono il caricamento del computer, l'accesso al sistema operativo installato (come Windows NT), o l'accesso ad alcune directory del disco fisso.
Controllo di accesso per database e software sui server a cui accedono i client. La sicurezza di questi sistemi richiede anche la sicurezza della trasmissione fra client e server.

Contatto diretto:
Giovanni Svaluto Ferro
+39 331 3382608
Ufficio: +39 0521 385510
FAX: +39 0521 386473
E-mail:
info@primasicurezza.com

Firma elettronica. I sistemi biometrici sono particolarmente idonei per proteggere e controllare transazioni finanziarie su reti informatiche. Un altro obiettivo è la protezione di alcune transazioni che hanno luogo su Internet che è estremamente non sicuro.

Esempi

Le seguenti applicazioni sono state rese note a tutt'oggi. Il provider di database Oracle offre un sistema basato sul rilevamento delle impronte digitali per proteggere biometricamente un server di database. Il terminal di verifica biometrica è installato sul lato client, le informazioni biometriche degli utenti tuttavia sono memorizzate in un database speciale del server.

Al momento del login, viene richiesto all'utente di sottoporsi a verifica dell'impronta digitale. Lo scambio di informazioni biometriche fra il client e il server è protetto da un algoritmo criptato. Una grossa banca asiatica controlla le transazioni dei cassieri i quali devono richiedere l'autorizzazione dei propri responsabili ogni qualvolta la transazione superi certi limiti. Questa autorizzazione viene fornita da un rilevatore di impronte digitali. Questo sembra essere al momento il sistema di verifica biometrica più grosso a livello mondiale: sono state installate più di 2000 unità.

Una banca egiziana sta introducendo un sistema simile.

5.6 Altre applicazioni di verifica

Molte nuove applicazioni sono comparse nel corso degli ultimi due anni. I sistemi biometrici sono utili nei casi in cui si debba ottenere una verifica affidabile di una persona.

Esempi

In un paese che, per ragioni politiche, i rifugiati politici non sono in campi fisicamente protetti, sono stati dotati di smartcard contenenti il template della propria impronta digitale. Viene loro richiesto di presentarsi settimanalmente o anche quotidianamente ad un ufficio registrazione per dimostrare la propria presenza con la card e la verifica dell'impronta digitale. Varie carceri europee sono dotate di sistemi biometrici (geometria della mano e impronte digitali), al fine di identificare i visitatori al momento dell'uscita o di verificare i prigionieri quando lasciano il carcere per qualsiasi ragione, particolarmente nel caso di persone appartenenti a certi gruppi etnici per le quali l'identificazione del volto da parte degli europei risulta difficoltosa.

Un Parlamento europeo con più di 500 delegati ha installato un sistema di votazione che richiede la verifica dell'impronta digitale per ogni voto. Questo significa un alto livello di sicurezza contro le frodi al momento del risultato delle votazioni.