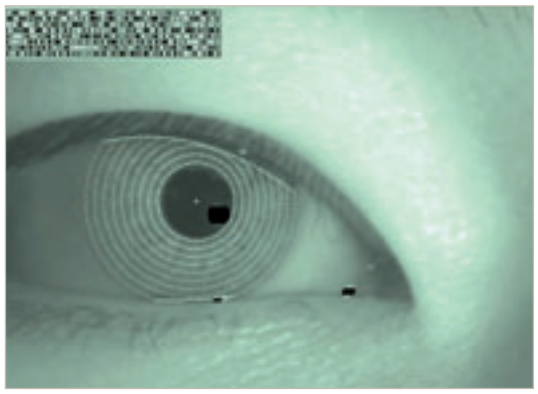
Identificazione biometrica

MASSIMO GIUSSANI

I tradizionali metodi di verifica degli accessi basati su password sono inficiati dalla presenza di un anello debole ineludibile: l'utente. Per essere sicura, una password deve essere difficile da individuare, modificata di frequente e mantenuta riservata; l'utente medio di un sistema informatico aziendale ha però la tendenza a usare password corte e facilmente decifrabili, oppure quando è costretto a usare password robuste con cadenza periodica, le trascrive, spesso su Post-It posizionati in bella vista. Non sorprende, dunque, che gli amministratori di sistema richiedano sistemi di identificazione personale più avanzati.



La scansione dell'iride può contare su un algoritmo molto efficiente che rende molto rapido il confronto con gli altri elementi memorizzati nella base di dati (fonte: Rosistem)

Gli scanner esterni di impronte digitali permettono anche ai sistemi meno aggiornati di sfruttare questa tecnica di identificazione biometrica

L'introduzione dei secure token, come le smart card o le chiavi hardware, ha rappresentato un passo avanti in questo senso, ma una scheda può sempre essere trafugata o duplicata. I sistemi di identificazione basati sulle caratteristiche biometriche (ossia i tratti fisiologici o comportamentali di un individuo) offrono una soluzione elegante trasformando l'utente stesso nell'elemento indispensabile al suo riconoscimento.
L'evoluzione tecnologica e l'abbattimento dei costi dei dispositivi di scansione e di elaborazione hanno infine portato alla diffusione di questi metodi.

DALLA PUNTA DELLE DITA ALLA CIMA DEI CAPELLI

Nella sua accezione più moderna, la biometria è la disciplina che si occupa dei sistemi automatizzati di identificazione basati su caratteristiche fisiologiche, fisico-chimiche o comportamentali. Le caratteristiche fisiologiche più comuni sono le impronte digitali, la fisionomia del volto, i disegni dell'iride, la disposizione dei vasi sanguigni nel fondo dell'occhio e la geometria del palmo della mano. I tratti comportamentali più usati per l'identificazione riguardano lo spettro vocale, la dinamica nell'apposizione di una firma e il modo in cui si digita sulla tastiera. Un sistema di identificazione biometrica è in ultima analisi un sistema di riconoscimento di schemi nei dati raccolti da scanner, telecamere, microfoni, tavolette grafiche, e persino comunissime tastiere. Il costo dei dispositivi di acquisizione è letteralmente crollato negli ultimi anni e non è infrequente imbattersi in PC di fascia media, persino nel segmento consumer, dotati di lettore d'impronte digitali o di un software di riconoscimento facciale abbinato a un'economica Webcam.
Esistono diversi enti nazionali e internazionali che si occupano della standardizzazione dei sistemi di identificazione biometrica in ambito informatico. In particolare ISO e IEC hanno avviato una collaborazione sfociata nell'istituzione del comitato tecnico congiunto JTC 1 che racchiude tutte le standardizzazioni dell'IT; tre sottocomitati sono dedicati alla biometrica: SC17 (che si occupa di smart card e documenti di viaggio), SC27 (che tratta le questioni di sicurezza legate alla biometria) e SC37 (che coordina la standardizzazione vera e propria).

NEGLI OCCHI DI CHI GUARDA

Due dei sistemi più sicuri di identificazione riguardano le variazioni cromatiche dell'iride o la disposizione dei vasi sanguigni del fondo dell'occhio. L'iride, la membrana muscolare che conferisce il colore agli occhi, presenta una struttura che è unica per ogni individuo e si conserva inalterata nel tempo. Le striature, gli anelli, le cripte e i solchi possono allora essere usati per fini identificativi.
La procedura di acquisizione richiede che il soggetto guardi l'obiettivo di una videocamera posta a una distanza variabile tra pochi centimetri e un metro.
Opportuni algoritmi di selezione sono in grado di isolare la forma dell'occhio e da questa estrarre l'immagine della sola iride che viene successivamente depurata e filtrata in maniera da evidenziarne le caratteristiche salienti. Il risultato dell'elaborazione è una sequenza binaria univoca (l'IrisCode è di soli 512 bit) che viene usata per identificare il soggetto o consentire l'accesso al sistema protetto. Questo approccio è stato usato con successo per controllare l'immigrazione negli Emirati Arabi Uniti. I principali svantaggi sono la sensibilità alle condizioni di illuminazione, il costo e le dimensioni delle apparecchiature di acquisizione. La scansione della retina sfrutta i dettagli unici e invariabili della vascolarizzazione del fondo dell'occhio. In questo caso l'acquisizione dell'immagine deve essere fatta a distanza ravvicinata con una fonte di illuminazione a bassa intensità per evitare che la pupilla si contragga. I dispositivi più recenti hanno permesso di ridurre considerevolmente i tempi di scansione rispetto al passato, ma la tecnica presenta il duplice svantaggio di un costo elevato e di una percezione di invasività da parte degli utenti. Negli Stati Uniti è una procedura standard adottata dagli enti militari e governativi.

L'identificazione della geometria della mano si presta all'impiego in ambienti industriali in cui gli operatori possono avere le impronte coperte da polvere, olio o grasso

Tramontata l'era delle password tradizionali, spetta ai sistemi di identificazione biometrica fornire un livello di sicurezza adeguato

UN VOLTO NOTO

Il riconoscimento del volto è la forma di identificazione più naturale tra esseri umani; la sua implementazione al calcolatore, divenuta accessibile a tutti grazie ai progressi dei sistemi di calcolo, permette il riconoscimento anche quando il soggetto non sa di essere 'scrutato'. Le applicazioni in quest'ultimo caso rientrano nell'ambito della gestione della sicurezza, ad esempio negli aeroporti e nei pressi dei cosiddetti 'obiettivi sensibili' del terrorismo. In linea di massima sistemi di riconoscimento facciale possono essere ricondotti a due categorie: locali e

olistici. I metodi locali identificano una serie di punti caratteristici in corrispondenza della posizione degli occhi, della bocca, dei lati del naso e degli estremi degli zigomi; le coordinate assolute producono una griglia di distanze relative che viene impiegata per produrre una struttura matematica, un grafo, unica per ogni volto. Altri algoritmi di identificazione, come il Dynamic Link Matching (DLM) si basano sull'impiego di reti neurali e di trasformate wavelet per la compressione delle informazioni da analizzare. I metodi olistici elaborano l'immagine nel suo complesso; il metodo PCA (Principal Component Analysis), per esempio, scompone l'immagine acquisita in una sovrapposizione pesata di 'autoimmagini' (eigenimages o eigenfaces) in maniera simile alla decomposizione di un vettore nelle sue componenti ortogonali. Al volto da riconoscere viene associato un punto nello spazio n-dimensionale delle immagini e il confronto tra i volti si riduce alla valutazione della distanza tra i relativi punti.

UN CLASSICO: LE IMPRONTE DIGITALI

Il riconoscimento delle impronte digitali avviene per mezzo di un sensore ottico, capacitivo o a ultrasuoni (tipicamente con risoluzione superiore a 500 dpi) che acquisisce il disegno formato dalle creste della pelle. Una volta filtrata ed esaltata, l'immagine viene passata a un algoritmo che isola i tratti caratteristici che le conferiscono l'unicità necessaria all'identificazione. Gli scanner di impronte trovano oggigiorno spazio anche nei PC e nei notebook di fascia media e persino nei dispositivi palmari. Alcune case automobilistiche hanno dotato le proprie vetture di questo tipo di controllo dell'accesso, che presenta il vantaggio di identificare il guidatore per poter regolare sedili, specchietti e climatizzazione in base alle sue esigenze. Uno svantaggio della scansione delle impronte è che richiede una pelle pulita e pertanto non può essere utilizzata efficacemente sul piano di fabbrica. In questo caso si usa una tecnica di riconoscimento della geometria della mano che non richiede dettagli ad alta risoluzione.

TECNICHE PER OGNI GUSTO

Esistono numerose altre tecniche di identificazione biometrica: è possibile utilizzare il pattern formato dai vasi sanguigni del polso, del palmo o del dorso della mano. La scansione con raggi infrarossi si è dimostrata particolarmente robusta nei confronti delle irregolarità superficiali come sporco, sudore, tagli e cicatrici. Anche la tecnica di termografia facciale, strettamente connessa alla vascolarizzazione del volto, è in grado di fornire un elevato grado di accuratezza. Le possibilità sono moltissime e sono stati sviluppati metodi che si basano sulla disposizione dei pori sudoripari della pelle, sulla geometria delle orecchie e del canale auricolare, sulla forma e i movimenti delle labbra e persino sulle striature delle unghie. Un discorso a parte meriterebbero poi le tecniche di identificazione basate sulle caratteristiche comportamentali come il riconoscimento vocale che restituisce un'impronta identificativa sulla base dello spettro sonoro registrato e il riconoscimento dinamico della firma, nel quale si analizza la traiettoria, la velocità e l'accelerazione dei vari tratti, nonché la pressione esercitata.