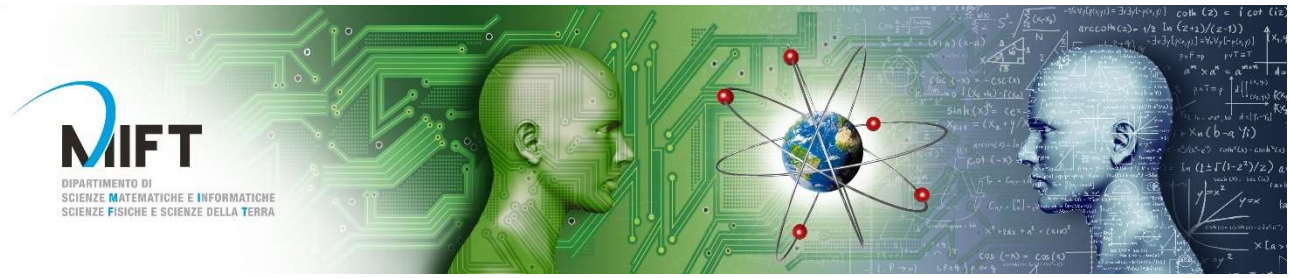
2020

Università degli Studi di Messina



Progetto:

La crittografia nei sistemi biometrici.

Docente:

Giovanna Martino.

Studente:

Giuseppe Primerano.

Sommario

Capitolo 1: Sicurezza informatica.

La sicurezza informatica pone le basi su quelli che sono i meccanismi per la protezione delle informazioni e dei dati sia di un utente privato che di un'azienda il suo compito è quello di definire ed organizzare la riservatezza e l'integrità dei dati, è bene ricordare che non esiste alcuna protezione senza una "politica di sicurezza", la sicurezza informatica va vista come un'operazione che ha bisogno di un continuo aggiornamento dato che gli attacchi che possono colpirla sono sempre più potenti e difficili da prevedere.

1.1 Su cosa si basa la sicurezza informatica

La sicurezza informatica si basa su tre principi fondamentali Confidenzialità, Integrità e Disponibilità. In inglese l'acronimo utilizzato è CIA.

Confidenzialità: riguarda la nostra abilità nel proteggere i dati da tutti gli individui che non sono autorizzati a vederli. Un esempio può essere quello di un ATM per il prelievo del denaro contante, in quel caso sia la persona che il gestore dell'apparato devono mantenere la confidenzialità del PIN che è stato appena inserito. Una violazione della confidenzialità avviene quando la persona non nasconde bene il suo PIN durante la digitazione oppure il gestore dell'ATM non utilizza algoritmi crittografici potenti per nasconderlo. I metodi più usati per garantire la confidenzialità sono crittografia, autenticazione e biometria.

Integrità: per integrità si intende l'abilità nel proteggere i nostri dati da qualsiasi tipo di modifica indesiderata. Per impedire la modifica dei dati vengono utilizzati una serie di permessi che esprimono cosa un utente non autorizzato può oppure non può fare.

Disponibilità: fa riferimento alla capacità di accedere ai nostri dati quando ne abbiamo bisogno. La disponibilità dei dati durante gli ultimi anni sta diventando un settore molto attivo e redditizio dell'informatica basti pensare a tutti i sistemi cloud (esempio: Dropbox, Google Drive, iCloud ecc.) che permettono di caricare file al loro interno ed averli a disposizione quando si vuole, ma anche questi sistemi non sono immuni da attacchi che mirano alla loro sicurezza infatti gli attaccanti riescono a violarli ed ottenere tutte le informazioni in essi contenute per poi chiedere un riscatto agli utenti per riaverle.

Capitolo 2: I sistemi biometrici.

2.1: Cos'è un sistema biometrico.

Tra le tante capacità che l'uomo possiede, quella di poter riconoscere i suoi simili è tra le più affascinanti, il portamento, i tratti somatici del volto, il timbro della voce, spesso sono sufficienti al cervello per ripescare nella memoria dati ed immagini di un passato anche remoto. Gli scienziati sostengono che a volte bastano appena venti millisecondi per riconoscere una persona. Ma la capacità di un individuo di identificare con certezza un suo simile è limitata alle persone che gli sono vicine o che ha conosciuto o frequentato nel tempo. Quindi se le sole capacità del nostro cervello non bastano per riconoscere un individuo, allora bisogna ricorrere alle macchine.

Il termine "biometria" deriva dalle parole greche "bio" (vita) e "metrica" (per misurare). Il sistema biometrico è un sistema informatico che consente di indentificare una persona in base ad alcune sue caratteristiche principali fisiologiche e comportamentali. Si basa su sistemi hardware per l'acquisizione dei dati cui si integrano le componenti software che consentono, attraverso algoritmi matematici, di effettuare l'analisi dei dati, ricostruire l'identità di una persona e riconoscerla. Grazie ai sistemi biometrici si può stabilire l'identità e l'unicità di una persona, infatti se pensiamo ai sistemi basati solo sull' ID e la password si possiedono solo le informazioni per accedere ad un servizio senza conoscere l'identità di chi sta accedendo.

2.2 Caratteristiche principali su cui si basa un sistema biometrico.

Un sistema biometrico si basa principalmente su due caratteristiche: fisiologiche si basate su analisi statistiche e poco variabili nel tempo; comportamentali subiscono

variazioni nel tempo e possono anche essere influenzate da fattori esterni o da particolari condizioni emotive come stress e forti impatti psicologici.

Nel dettaglio:

1) Caratteristiche fisiologiche: ne fanno parte le impronte digitali, il colore e la dimensione dell'iride, la retina, la sagoma della mano e la fisionomia del volto.
2) Caratteristiche comportamentali: sono l'impronta vocale, la scrittura, lo stile di battitura della tastiera il movimento del corpo lo stile e l'andamento della camminata.

2.3 Cenni storici.

Epoca a.C

Le prime tracce di riconoscimenti biometrici sono stati trovati in una grotta che si stima abbia almeno 31.000 anni, dove le pareti erano adornate con dipinti che si riteneva fossero stati creati da uomini preistorici che vivevano lì. Intorno a questi dipinti vi sono numerose impronte di mani che si ritiene abbiano "agito come una firma indimenticabile" del suo autore.

Ci sono anche prove che le impronte digitali sono state usate come marchio di una persona già nel 500 a.C. Anche le transazioni commerciali babilonesi venivano registrate in tavolette di argilla che includevano le impronte digitali.

Nella prima storia egiziana, i commercianti venivano identificati dalle loro descrizioni fisiche per poter distinguere tra commercianti di fiducia e nuovi commercianti.

Epoca dal 1600 al 1800.

Nel 1686, Marcello Malpighi, professore di anatomia all'Università di Bologna, nel suo trattato annotò creste, spirali e anelli per impronte digitali.

Nel 1788, l'anatomista e medico tedesco JCA Mayer scrisse "Anatomical Copper-plate with Appropriate Explanations" contenenti disegni di modelli di pelle di cresta di attrito, osservò che "sebbene la disposizione delle creste della pelle non sia mai duplicata in due persone, tuttavia le somiglianze sono più vicine tra alcune individui". Mayer fu il primo a dichiarare che la pelle della cresta di attrito è unica.

Verso la fine del 1800 fu sviluppato un metodo per indicizzare le impronte digitali che forniva la possibilità di recuperare i record come faceva il metodo Bertillon, ma che si basava su modelli e creste di impronte metriche più personalizzati. Il primo sistema così robusto per l'indicizzazione delle impronte digitali fu sviluppato in India da Azizul Haque per Edward Henry, ispettore generale di polizia a Bengala in India.

Questo sistema, chiamato Henry System, e le sue varianti sono ancora in uso per classificare le impronte digitali.

Nel 1870 Alphonse Bertillon ha sviluppò "Bertillonage" o antropometrie, un metodo per identificare gli individui sulla base di registrazioni dettagliate delle loro misurazioni del corpo, descrizioni fisiche e fotografie. Bertillon notò che sebbene alcune persone potevano cambiare il loro nome, non potevano cambiare certi elementi del loro corpo. Le autorità di polizia di tutto il mondo usarono il suo sistema, il suo utilizzo scomparve rapidamente quando fu scoperto che alcune persone condividevano le stesse misurazioni. Quando poi nel 1903 due fratelli gemelli furono arrestati il sistema portò a degli errori di riconoscimento da questo momento in poi il suo utilizzo scomparve inesorabilmente.

Epoca del 1900.

Durante i primi anni '60 viene implementato il primo sistema di riconoscimento facciale semi-automatico da Woodrow W. Bledsoe sotto contratto con il governo degli Stati Uniti. Questo sistema richiedeva all'amministratore di individuare caratteristiche come occhi, orecchie, naso e bocca sulle fotografie. Inoltre si basava esclusivamente sulla capacità di estrarre punti utili utilizzabili. Venivano calcolate distanze e rapporti rispetto a un punto di riferimento comune che è stato confrontato con i dati di riferimento.

Durante gli anni '70 gli scienziati Goldstein, Harmon e Lesk usarono 21 marcatori soggettivi specifici come il colore dei capelli e lo spessore delle labbra per automatizzare il riconoscimento facciale. Il problema con entrambe queste prime soluzioni fu che le misurazioni e le posizioni venivano calcolate manualmente per risolvere questo problema il Dr. Joseph Perkell, usò i raggi X in questo modo riuscì ad ottenere una comprensione più dettagliata delle complesse componenti comportamentali e biologiche del linguaggio.

Durante gli anni '80 il National Institute of Standards and Technology (NIST) sliluppò il NIST Speech Group per studiare e promuovere l'uso delle tecniche di elaborazione del parlato.

Nel 1984 circa l'esercito americano iniziò a testare la geometria della mano per l'uso nel settore bancario queste distribuzioni si basavano sul concetto di utilizzare la geometria di una mano per l'identificazione.

La valutazione FERET (FacE REcogntion Technology) è stata sponsorizzata dal 1993-1997 dalla Defense Advanced Research Products Agency (DARPA) e dal DoD Counterdrug Technology Development Office Office nel tentativo di incoraggiare lo sviluppo di algoritmi e tecnologie di riconoscimento facciale. Questa valutazione aveva

il compito di valutare i prototipi dei sistemi di riconoscimento facciale e spinse il riconoscimento facciale a un mercato di prodotti commerciali.

Il Dr. John Daugman ha ottenne un brevetto per i suoi algoritmi di riconoscimento dell'iride. Di proprietà di Iridian Technologies, il successore di lriScan, Inc. questo brevetto è la pietra miliare della maggior parte dei prodotti commerciali moderni per il riconoscimento dell'iride.

Il sistema di servizio accelerato per passeggeri di immigrazione e naturalizzazione (INSPASS) era un'implementazione biometrica che consentiva ai viaggiatori di aggirare le linee di immigrazione in determinati aeroporti negli Stati Uniti fino alla sua interruzione avvenuta nel 2004. I viaggiatori autorizzati ricevevano una carta codificata con le informazioni sulla geometria della mano. Piuttosto che essere elaborati da un ispettore dell'immigrazione, i viaggiatori INSPASS presentavano le loro carte con le informazioni codificate e le loro mani al dispositivo biometrico. Dopo la verifica dell'identità rivendicata, l'individuo poteva procedere al gate doganale, così vennero evitate lunghe linee di ispezione e accelerato l'ingresso negli Stati Uniti.

Nel 1996 durante le olimpiadi di Atlanta, Georgia, USA venne fatto un uso pubblico importante della geometria della mano, dove vennero implementati sistemi di geometria della mano per controllare e proteggere l'accesso fisico al Villaggio Olimpico.

Epoca degli anni 2000.

Un sistema di riconoscimento facciale venne installato al Super Bowl del gennaio 2001 a Tampa, in Florida, nel tentativo di identificare le persone "ricercate" che entravano nello stadio. La dimostrazione non trovò individui "ricercati", ma riuscì a identificare erroneamente fino a una dozzina di fan dello sport innocenti. Le successive richieste dei media e del Congresso servirono ad introdurre nella coscienza del grande pubblico sia la biometria che i relativi problemi di privacy. Questo sistema è ancora oggi adottato anche in Italia per garantire che i soggetti sottoposti al regime di DASPO non possano recarsi allo stadio a guardare la partita.

Nel 2004 il Dipartimento della Difesa (DoD) implementò un sistema automatizzato di identificazione biometrica (ABIS). Venne creato per migliorare le capacità del governo degli Stati Uniti di tracciare e identificare le minacce alla sicurezza nazionale. I sistemi di raccolta associati includono la capacità di raccogliere, da combattenti nemici, ribelli e altre persone d'interesse, dieci impronte digitali, fino a cinque foto segnaletiche da diverse angolazioni, campioni vocali (enunciati), immagini dell'iride e un tampone orale per raccogliere il DNA.

Nel 2010 un'impronta digitale derivante dalle prove raccolte nel luogo dell'attentato dell'undici settembre fu abbinata positivamente a un detenuto. L'anno successivo, la CIA usò la tecnologia di riconoscimento facciale per identificare i resti di Osama bin Laden con una certezza del 95 percento.

Nel 2013 Apple.Inc implementa e rilascia il Touch ID una funzione di riconoscimento delle impronte digitali, (resa disponibile su iPhone 5S, iPhone 6 e iPhone 6 Plus, iPad Air 2 e iPad Mini 3). Touch ID è fortemente integrato in Dispositivi iOS, che consentono agli utenti di sbloccare il proprio dispositivo, nonché effettuare acquisti nei vari negozi supportati da Apple (iTunes Store, App Store, iBookstore) e per autenticare Apple Pay online o nelle app. Annunciando la funzione, Apple ha chiarito che le informazioni sulle impronte digitali sono archiviate localmente in una posizione sicura dei processori Apple A7 (in iPhone 5S e iPad mini 3 (APL0698), A8 (in iPhone 6 e iPhone 6 Plus) o A8X (nel chip iPad Air 2), anziché essere archiviate in remoto sui server Apple o in iCloud, rendendo molto difficile l'accesso esterno. Presto questa soluzione venne aggiunta in altri dispositivi della concorrenza tra i quali Samsung, Sony ecc.

Nel 2017 sempre l'azienda Apple.inc con l'uscita dell'iPhone X rilascia una nuova tecnologia di riconoscimento basata sul riconoscimento facciale dell'utente. Oggigiorno è presente assieme all'impronta digitale, in tutti i dispositivi non solo di marchio Apple ma anche della concorrenza per garantire un'autenticazione migliore.

Capitolo 3: Le impronte digitali.

Le prime applicazioni dei sistemi basati sulle impronte digitali vennero utilizzate per controllare l'accesso fisico agli edifici. Oggigiorno le impronte digitali sono utilizzate in tutti i sistemi di riconoscimento ad esempio nelle nuove carte d'identità italiane dove nel momento della richiesta di questo documento l'interessato deve fornire le proprie impronte digitali, ed anche in molti dispositivi elettronici come smartphone, PC, ecc. in quanto garantiscono un velocità di accesso maggiore rispetto all'uso di una password e un'autenticazione migliore per ogni utente in quanto ogni persona sulla Terra ha le proprie impronte digitali. Questo sistema si basa principalmente su tre aspetti:

1) Immutabilità: La configurazione e i dettagli del disegno sono permanenti e non cambiano mai durante la vita.
2) Unicità: La possibilità di variazione del disegno dell'impronta è talmente alta, che non compaiono mai due disegni uguali in diverse dita della stessa persona o in persone differenti.
3) Classificazione: Le possibili variazioni dello schema sono limitate, per cui è possibile una classificazione sistematica di tali configurazioni.

3.1 Composizione di un'impronta digitale.

Un' impronta è costituita da un insieme di linee parallele che alcune volte s'incontrano o s'interrompono formando un disegno detto **cresta.** A partire dalla cresta possono essere ricavate informazioni importanti tra cui le **minuzie**.

Le minuzie possono essere descritte usando un array con un attributo che ne descrive il tipo, l'analisi di quest'ultime permette di memorizzare per ognuna di esse le coordinate e l'angolo per poi essere confrontate con altre minuzie estratte.

Un'altra parte importante di un'impronta è l'area del modello in quanto al suo interno sono presenti le macro caratteristiche che vengono spesso usate nei sistemi biometrici per classificare le impronte.

3.2 Algoritmo per le impronte digitali.

Come molti algoritmi crittografici anche questo è diviso in due passi abbiamo l'**algoritmo di estrazione e l'algoritmo per la corrispondenza.**

Algoritmo di estrazione.

Prende l'immagine dell'impronta digitale la migliora e analizza le caratteristiche dell'impronta basandosi sulle minuzie, l'immagine viene poi codificata in una sequenza di bit e una volta creata la sequenza quest'ultima viene usata per identificare una chiave pubblica più lunga. La codifica dell'impronta digitale deve essere deterministica e tutti i dati aggiuntivi devono essere archiviati assieme alla chiave pubblica. Nei dati aggiuntivi sono presenti informazioni quali: il protocollo per scambiare la chiave (nel caso delle impronte è PGP), il nome del possessore della chiave e infine un certificato auto-firmato. Infine l'algoritmo esegue il diradamento delle prestazioni temporali e il tutto viene inserito all'interno di un database e poi classificato.

Algoritmo per la corrispondenza.

Una volta che l'impronta è inserita nel database bisogna fare una ricerca e vedere se l'impronta è già presente nel database. Vengono in particolare analizzate le posizioni di ciascun punto caratteristico e la struttura dell'impronta. A questo punto Il passo successivo consiste nel sottoporre i dati prodotti in precedenza ad una funzione hash crittografica come la SHA-1 che riceve un input e produce un valore di hash a 160 bit in genere visualizzato come un numero esadecimale lungo 40 cifre; oppure la SHA-2 che usa una struttura di Merkle e una funzione di compressione unidirezionale costruita usando un cifrario a blocchi specializzato. A questo punto l'elaborazione dell'impronta digitale dal punto di vista crittografico è terminata.

Molto spesso però l'output generato dalle funzioni hash deve essere troncato per fornire un'impronta digitale più breve che viene usata per autenticare una chiave pubblica molto più grande. Solitamente la lunghezza di bit di un'impronta digitale varia dai 128 ai 160 bit. Nel momento in cui le impronte digitali servono per fare un'ispezione umana vengono codificate in stringhe esadecimali.

Nella tabella in basso è riportata la probabilità che due impronte siano uguali fra di loro nella prima colonna vengono riportati i nomi degli studiosi che hanno fatto le misurazioni.

Author	P(Fingerprint Configuration)	N=36,R=24,M=72	N=12,R=8,M=72
Galton (1892)	$\frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{2}\right)^R$	1.45×10^{-11}	9.54×10^{-7}
Pearson (1930)	$\frac{1}{16} \times \frac{1}{256} \times \left(\frac{1}{36}\right)^R$	1.09×10^{-41}	8.65×10^{-17}
Henry (1900)	$\left(\frac{1}{4}\right)^{N+2}$	1.32×10^{-23}	3.72×10^{-9}
Balthazard (1911)	$\left(\frac{1}{4}\right)^N$	2.12×10^{-22}	5.96×10^{-8}
Bose (1917)	$\left(\frac{1}{4}\right)^N$	2.12×10^{-22}	5.96×10^{-8}
Wentworth & Wilder (1918)	$\left(\frac{1}{50}\right)^N$	6.87×10^{-62}	4.10×10^{-21}
Cummins & Midlo (1943)	$\frac{1}{31} \times \left(\frac{1}{50}\right)^N$	2.22×10^{-63}	1.32×10^{-22}
Gupta (1968)	$\frac{1}{10} \times \frac{1}{10} \times \left(\frac{1}{10}\right)^N$	1.00×10^{-38}	1.00×10^{-14}
Roxburgh (1933)	$\frac{1}{1000} \times \left(\frac{1.5}{10 \times 2.412}\right)^N$	3.75×10^{-47}	3.35×10^{-18}
Trauring (1963)	$(0.1944)^N$	2.47×10^{-26}	2.91×10^{-9}
Osterburg et al. (1980)	$(0.766)^{M-N}(0.234)^N$	1.33×10^{-27}	3.05×10^{-15}
Stoney (1985)	$\frac{N}{5} \times 0.6 \times (0.5 \times 10^{-3})^{N-1}$	1.2×10^{-80}	3.5×10^{-26}

3.3 Utilizzo pratico delle impronte digitali.

In sistemi come la PKI basata su X.509, le impronte digitali vengono utilizzate principalmente per autenticare le chiavi di root. Queste chiavi di root emettono certificati che possono essere utilizzati per autenticare le chiavi utente. Questo uso dei certificati elimina la necessità di una verifica manuale delle impronte digitali tra gli utenti.

In sistemi come CGA o SFS e maggior parte delle reti peer-to-peer crittografiche, le impronte digitali sono incorporate in formati di indirizzo e nome preesistenti (come indirizzi IPv6, nomi di file o altre stringhe di identificazione). Se indirizzi e nomi vengono già scambiati tramite canali attendibili, quest'approccio consente alle impronte digitali di spostarsi.

In PGP, la maggior parte delle chiavi viene creata in modo tale che ciò che viene chiamato "ID chiave" è uguale rispettivamente ai 32 o 64 bit inferiori di un'impronta digitale della chiave. PGP utilizza gli ID-chiave per vari scopi. Queste non sono, in senso proprio, impronte digitali, poiché la loro breve lunghezza impedisce loro di essere in grado di autenticare in modo sicuro una chiave pubblica. Gli ID chiave a 32 bit non devono essere utilizzati poiché l'hardware corrente può generare l'id chiave a 32 bit in soli 4 secondi.

Un altro uso dell'impronte digitali viene fatto a scopo governativo per il controllo delle frontiere, carte d'identità, registrazione degli elettori ecc. In quanto le impronte digitali sono molto precise e veloci.

Vengono anche usate nel settore bancario per proteggere i dati finanziari degli utenti e fornire transazioni sicure e facili.

3.4 Attacchi alla sicurezza delle impronte digitali.

La principale minaccia alla sicurezza di un'impronta digitale è un attacco *preimage*, in cui un attaccante costruisce una coppia di chiavi; la chiave pubblica ha un hash su un'impronta digitale che corrisponde all'impronta digitale della vittima. L'attaccante potrebbe quindi presentare la sua chiave pubblica al posto della chiave pubblica della vittima così da mascherarsi.

Per prevenire attacchi preimage, la funzione hash crittografica utilizzata su un'impronta digitale deve possedere la proprietà della seconda resistenza preimage.

Una seconda minaccia per alcuni sistemi è un attacco di *collisione*, dove un attaccante costruisce più coppie di chiavi che hanno l'hash sulla propria impronta digitale. Ciò può consentire a un utente malintenzionato di ripudiare le firme che ha creato o causare altra confusione.

Per prevenire ed evitare l'attacchi di collisione la funzione hash deve possedere la proprietà di resistenza alle collisioni.

Un'altra minaccia può arrivare dalle impronte digitali "*troncate*", poiché sebbene sia accettabile troncare l'output della funzione hash per motivi di impronte digitali più brevi e più utilizzabili, le impronte digitali troncate devono però essere abbastanza lunghe da preservare le proprietà pertinenti della funzione hash dagli attacchi a forza bruta. Per evitare l'attacco su impronte troncate la maggior parte di questo tipo d'impronte viene crittografato mediante l'uso di MD5 o SHA-1 non troncati, ma nel 2017 questo tipo di sicurezza è stato violato e quindi molto presto verranno abbandonati gli algoritmi descritti in precedenza a favore di SHA-256 o altri funzioni hash che restituiscono un output maggiore.

In alcuni sistemi inoltre è richiesta una lunghezza delle impronte digitali molto bassa, per proteggere queste impronte vengono usati dei meccanismi che aumentano il costo del calcolo dell'impronta digitale.

3.5 Come ottenere le impronte digitali.

Il primo metodo usato per ottenere le impronte digitali consisteva nell'impregnare le dita della persona con dell'inchiostro, dopodiché veniva fatta una piccola pressione su un foglio bianco per ottenere una copia esatta delle impronte. Nell'epoca moderna con tutte le scoperte scientifiche vengono usati altri metodi basati su diversi tipi di scanner tra i quali troviamo:

- Lo scanner ottico: acquisisce un'immagine visiva dell'impronta digitale utilizzando una fotocamera.
- Lo scanner capacitivo o CMOS: acquisisce utilizzando dei condensatori quindi corrente elettrica per formare un'impronta digitale.
- Lo scanner ad ultrasuoni: acquisisce l'impronta mediante l'uso delle onde sonore ad alta frequenza per penetrare nello strato epidermico della pelle.
- Lo scanner termico: rileva le differenze di temperatura sulla superficie di contatto tra le creste e le valli delle impronte digitali.

Nella maggior parte di dispositivi di elettronica di consumo quali PC, smartphone ma anche dispositivi di domotica vengono usati scanner ottici ad eccezione dell'azienda coreana Samsung che nei suoi prodotti di fascia alta (Galaxy S10, S20 ed altri) preferisce inserire scanner ad ultrasuoni. In tutti questi dispositivi le impronte digitali non vengono salvate in un database ma direttamente in una porzione della memoria del dispositivo per garantire una maggiore velocità di riconoscimento, ma se da una parte abbiamo una maggiore velocità, la sicurezza è minore in quanto gli smartphone sono molto più vulnerabili agli attacchi

4: Il riconoscimento della mano.

Per quanto il sopra citato riconoscimento delle impronte digitali sia sicuro vi è un sistema biometrico che viene definito più sicuro, questo sistema si basa sul riconoscimento del palmo della mano. La mano umana è più distintiva di quanto gli occhi umani possano percepire. Questo carattere distintivo può essere misurato con tecniche di imaging e misurazione basate su computer dove l'identità di un individuo può essere associata al carattere distintivo della sua mano. La geometria della mano o

la tecnologia della forma della mano è considerata la più antica tecnologia biometrica implementata, persino più vecchia dell'implementazione della tecnologia biometrica dell'impronta digitale, i primi studi riguardo questo settore risalgono al 1985. Nel mercato di oggi questo sistema biometrico viene oramai utilizzato da poche aziende, infatti oggi una buona fetta di mercato dei sistemi biometrici è occupata dal riconoscimento delle impronte digitali e dal riconoscimento facciale.

4.1: Come funziona.

La biometria del riconoscimento della mano sfrutta l'idea che la geometria della mano di ciascun individuo sia unica, questo però ancora non è stato provato. Per ottenere le immagini della mano viene utilizzato un lettore di immagini il suo compito è di prendere l'immagine e salvarla, in questo modo è possibile stabilire e verificare l'identità in qualsiasi momento. Un utente che vuole autenticarsi deve prima digitare il proprio PIN e poi mettere la mano sul riconoscitore, grazie all'uso del PIN il sistema capisce a quale immagine già salvata far riferimento. Oltre agli scanner che usano le immagini ne esistono alcuni che sfruttano gli infrarossi per catturare l'immagine. Il funzionamento di questo sistema biometrico si compone di 3 fasi.

1) **Fase di addestramento:** In questa fase l'utente impara a collocare in maniera corretta la mano sullo scanner; vengono rilevate 99 misure della mano del soggetto che concorrono alla creazione di un modello di 9 bytes (ottimo per SmartCard), memorizzato per effettuare i successivi confronti.
2) **Fase di registrazione:** Questa fase influenza il valore del FRR. Per tale motivo a tale fase si fa precedere la fase di addestramento. Il soggetto posiziona tre volte consecutive la mano sullo scanner. Il processore interno effettua una media aritmetica delle tre sagome generando un "impronta media" che sarà usata come modello.
3) **Fase di verifica:** Durante tale fase l'utente digita un PIN e lo scanner rileva l'impronta corrispondente, dopodiché il soggetto pone la mano sullo scanner e viene realizzato il confronto. Tale operazione avviene considerando un indice di similarità che rappresenta la tolleranza entro la quale il sistema considererà la mano accettabile.

4.2: Crittografia applicata al riconoscimento della mano.

Al fine di creare misure di sicurezza adeguate in questo sistema biometrico vengono utilizzati due algoritmi di cifratura a chiave privata AES e DES. Inizialmente per **crittografare** i punti caratteristici delle vene della mano viene usato AES, quindi la chiave privata generata dall'algoritmo AES viene fornita al DES per la crittografia.

Infine il modello biometrico ottenuto e la chiave vengono usati per creare il deposito sfuocato. Per la **decrittografia** la chiave pubblica di DES viene utilizzata per decrittografare la chiave privata dell'algoritmo AES. Successivamente i punti di funzione crittografati vengono decifrati dall'algoritmo AES.

4.3 Vantaggi e svantaggi.

Vantaggi:

- Veloce, semplice, preciso, facile da usare e poco invadente
- Difficile da eludere. Richiederebbe l'intera replica 3D della mano di un soggetto per aggirare il sistema.
- Può essere integrato in altri sistemi come le smart card.
- Elimina la necessità di creare, amministrare o trasportare le carte, quindi riduce i costi, i tempi e gli sforzi complessivi rispetto ai sistemi di frequenza tradizionali.

Svantaggi:

- Caratteristiche biometriche non molto uniche non possono essere sfruttate per applicazioni ad alta sicurezza.
- I lettori di geometria della mano sono molto più costosi rispetto ad altri lettori.
- E' suscettibile a problemi legati all'igiene della mano oppure a problemi legati alla deformità e al gonfiore.

4.4: Confronto tra riconoscimento della mano e riconoscimento delle impronte digitali.

Arrivati a questo punto è giusto fare un confronto tra questi due sistemi biometrici per cercare di capire quale possa essere il migliore in termini di sicurezza. Per farlo è giusto andare a esaminare diversi aspetti di questi sistemi. Partiamo dall' **universalità** in questo aspetto il riconoscimento della mano supera le impronte digitali in quanto quest'ultime possono essere consumate o addirittura mancanti in alcuni individui rispetto al palmo della mano. Poi abbiamo l'**unicità** in questo campo le impronte superano la mano in quanto il carattere distintivo delle impronte è superiore rispetto alla geometria della mano. Riguardo la **permanenza** ovvero la capacità di una caratteristica fisiologica di non cambiare durante la vita di una persona, le impronte digitali sono migliori perché la geometria della mano può cambiare (ad esempio con perdita di peso). Sulle **prestazioni** abbiamo un'altra vittoria delle impronte digitali infatti stimando gli errori, il riconoscimento della mano ne genera di più. Invece per quanto riguarda l'**elusione** questi due sistemi biometrici che sto confrontando

vengono dati alla pari, in quanto un attaccante può riuscire a replicare sia le impronte che la geometria della mano.

Grazie a questa accurata analisi possiamo capire perché oggigiorno il riconoscimento della mano non viene più usato con la stessa frequenza dei tempi passati.

5: Riconoscimento facciale.

Studi sul riconoscimento del volto documentano che gli uomini si concentrano subito su elementi predominanti del volto (naso grande, orecchie sporgenti, ecc.). Per questo motivo ci sono delle **caratteristiche interne** del volto che vengono usate per riconoscere i volti familiari e **caratteristiche esterne** usate per riconoscere volti non familiari. Su questi ragionamenti si basa il riconoscimento facciale usato nei moderni dispositivi elettronici. Un sistema di riconoscimento facciale è una tecnologia in grado di identificare o verificare una persona da un'immagine digitale o da un fotogramma video oppure da una sorgente video. Viene anche descritta come un'applicazione basata sull'intelligenza artificiale in grado di identificare in modo univoco una persona analizzando i modelli in base alle trame e alla forma del viso della persona. Mentre inizialmente era una forma di applicazione per computer, negli ultimi tempi ha visto usi più ampi su piattaforme mobili e in altre forme di tecnologia. Sebbene l'accuratezza del sistema di riconoscimento facciale come tecnologia biometrica sia inferiore al riconoscimento delle impronte digitali è ampiamente adottata grazie al suo processo senza contatto e non invasivo.

5.1: Caratteristiche del riconoscimento facciale.

Per effettuare il riconoscimento facciale si utilizzano delle immagini come spesso capita nei sistemi biometrici. Infatti possiamo dividere il riconoscimento in statico e dinamico: **statico** è caratterizzato da una buona qualità dell'immagine; **dinamico** presenta delle immagini di scarsa qualità con pose irregolari e sfondi invadenti.

Il processo di riconoscimento può essere semplicemente diviso in quattro fasi:

1) **Fase di pre-elaborazione:** consiste nel garantire che l'immagine cui viene applicato il processo di riconoscimento soddisfi alcuni standard richiesti. Solitamente questa fase è svolta dalle apparecchiature atte al prelevamento dell'immagine, tramite meccanismi che tendono ad impedire all'utente di fornire immagini distorte: un esempio possono essere i sensori che permettono di acquisire l'immagine solo quando il soggetto si trovi ad una distanza accettabile.
2) **Fase di localizzazione:** consiste nell'esatta localizzazione del volto o di alcune parti che lo compongono questa fase presenta delle problematiche dovute all'immagine stessa, come la vicinanza alla telecamera, le condizioni di illuminazione, l'allineamento con l'asse verticale e lo sfondo dell'immagine.

3) **Fase di estrazione dei particolari:** è forse il fulcro di tutto il processo di riconoscimento del volto. Una particolare caratteristica utile per distinguere un volto da un altro; può essere estratto dall'immagine tramite processi di varia natura. Solitamente più elevato è il numero di particolari estratti, più alta è la capacità di discernimento tra facce simili. Alcuni particolari interessanti sono, ad esempio, il colore degli occhi.
4) **Fase di riconoscimento:** si concentra più che altro sull'estrazione dei particolari.

5.2: Come avviene l'estrazione dei particolari.

Per estrarre i particolari durante gli anni sono stati creati molti metodi che hanno però tutti un filo conduttore, questo filo conduttore è l'utilizzo della teoria matematica o meglio per riconoscere le immagini vengono spesso utilizzate le matrici.

Sakai ed altri utilizzarono un'immagine digitalizzata a 8 livelli di grigio. Questo sistema si serve di una matrice 3x3 che viene utilizzata per determinare i pixel con la massima intensità in modo da ridurre l'informazione all'essenziale. Questi pixel venivano collegati con segmenti seguendo una sagoma predefinita per definire il contorno del volto.

Reisfeld e Yeshurun descrissero un operatore simmetrico generalizzato da applicare sull'immagine in modo da localizzare gli occhi e la bocca all'interno del viso. La motivazione dell'approccio risiede nella natura simmetrica del volto lungo la linea verticale che passa per il naso. L'operatore applicato determina i punti nell'immagine a cui corrisponde un alto grado di simmetria. Grazie all'operatore la frequenza dei successi è del 95%.

5.3: Tecniche di riconoscimento facciale.

Riconoscimento base: alcuni esempi di questo tipo di riconoscimento possono essere i filtri utilizzati nei social media quali Snapchat e Instagram in cui la fotocamera del dispositivo cerca le caratteristiche del volto tra cui occhi, naso e bocca una volta compiuta la sua ricerca la fotocamera tramite il social usa degli algoritmi per determinare in quale direzione la persona sta guardando se la sua bocca è aperta ecc.

Riconoscimento 3D: questa tecnica di riconoscimento facciale utilizza sensori 3D per acquisire informazioni sulla forma di un viso. Queste informazioni vengono utilizzate per identificare le caratteristiche distintive sulla superficie di un viso, come il contorno delle cavità oculari, del naso e del mento. Un vantaggio del riconoscimento facciale 3D è dato dal fatto che esso non è influenzato dai cambiamenti nell'illuminazione come altre tecniche. Può anche identificare una faccia da una gamma di angoli di visione, inclusa una vista di profilo. I punti di dati tridimensionali di un volto migliorano notevolmente la precisione del riconoscimento del volto. Questa tecnica viene

utilizzata per sbloccare molti smartphone. Vi è anche una variante **2D** che non ha lo stesso livello di sicurezza rispetto a quella tridimensionale infatti nei moderni smartphone che usano lo sblocco facciale in 2D il sistema non riesce a riconoscere chi sia il vero possessore dell'apparecchio, e si sblocca anche se il volto è di una persona che somiglia molto al vero possessore come un fratello un padre ecc., *questa è una cosa che ho potuto constatare di persona.*

5.4: Crittografia nel riconoscimento facciale.

La crittografia nei sistemi di riconoscimento facciale nasce per risolvere un problema legato alla privacy, infatti tutte le immagini relative ai volti vengono salvate all'interno di un database e possono esserci dei rischi di furti d'identità e perdita di privacy. Con la crittografia biometrica anziché archiviare la propria immagine facciale in un database, l'immagine facciale viene utilizzata per crittografare altre informazioni e solo i dati crittografati biometricamente vengono salvati nel database.

Uno degli algoritmi usati per crittografare il riconoscimento facciale è l'HDS. L'obbiettivo è quello di usare un vettore per legare in modo sicuro la chiave crittografica codificata, che genera dati di supporto per l'archiviazione. Ogni componente del vettore viene usato per associare un bit di chiave crittografica (precedentemente posta ad un controllo degli errori). Questo processo si compone di due moduli uno per l'iscrizione che esegue il processo di associazione biometrica e uno per la verifica biometrica. HDS innanzitutto va a codificare la chiave crittografata per la tolleranza di errore, viene quindi associato il vettore, l'associazione viene fatta mediante l'uso dell'operatore logico *XOR*, in questo modo senza accesso alle giuste caratteristiche fisiologiche la chiave crittografata non può essere recuperata, pertanto un eventuale attaccante non può ottenere il vettore. Un utente che voglia sbloccare la chiave deve inviare le proprie caratteristiche facciali per la verifica e poi da queste viene estratto il vettore binarizzato, quest'ultimo viene confrontato con il vettore creato in fase d'iscrizione se corrispondono viene fornita la chiave all'utente.

Una delle cose più importanti da capire è che il volto di qualsiasi persona non può mai essere utilizzato come chiave privata in quanto il volto è pubblico e nemmeno per un efficiente metodo di crittografia l'unica applicazione efficace del sistema biometrico di riconoscimento facciale è quello di poter sbloccare i dispositivi, una sostituzione del vecchio codice PIN. Inoltre questo sistema biometrico non può essere nemmeno usato per l'**autenticazione** infatti per un qualsiasi calcolatore è difficile "dare un nome ad una faccia", ci sono dei sistemi in cui prima l'utente deve dichiarare la propria identità (usando un username) e il sistema si occupa solo di convalidarla attraverso l'immagine del volto

5.5: Vantaggi e svantaggi.

Vantaggi:

- Un vantaggio chiave di un sistema di riconoscimento facciale è che è in grado di identificare la massa. I sistemi progettati correttamente installati in aeroporti, e altri luoghi pubblici possono identificare le persone tra la folla, senza che i passanti siano nemmeno a conoscenza del sistema.

Svantaggi:

- Tra tutte le tecniche biometriche il riconoscimento facciale non è tra i più affidabili ed efficienti.
- Ha i più alti tassi di falsa accettazione e rifiuto.
- Problemi legati alla privacy.