UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

Tesi di Laurea in Informatica

- Sicurezza nei Sistemi Biometrici

Gabriele Gatti

Argomenti

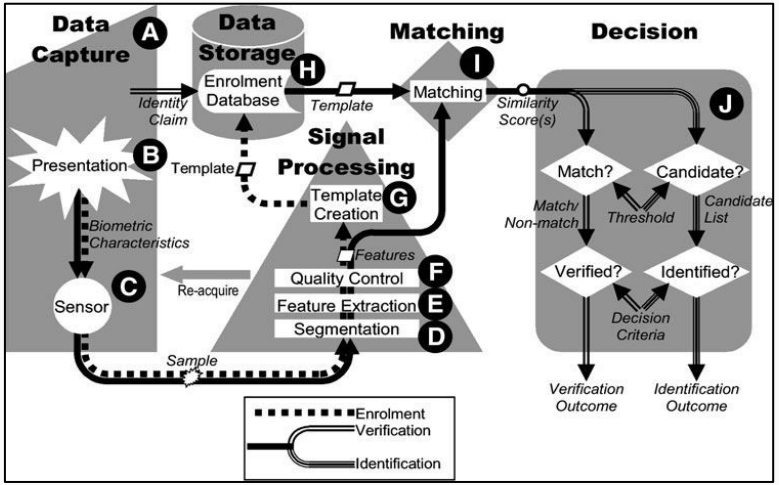
- Sicurezza e Liveness
- Vulnerabilità Biometriche
- Sicurezza dei Templates
- Crittografia Biometrica
- Crittografia Visiva
- Biometrica Cancellabile
- Transportable Asset Protection
- Falsificazione a Sforzo Zero
- Standards di Sicurezza Biometrica
- Sicurezza nella Progettazione del Sistema
- Sistema Operativo Tamper-Proof
- Anti-spoofing – Metodologie di Valutazione
- Anti-spoofing – Facciale
- Anti-spoofing – Databases Facciale
- Anti-spoofing – Impronta Digitale
- Anti-spoofing – Impronta Digitale (Hardware e Software)
- Anti-spoofing – Databases Impronta Digitale
- Anti-spoofing – Iride
- Anti-spoofing – Databases Iride
- Anti-spoofing – Vocale
- Anti-spoofing – Databases Vocale
- Anti-spoofing – Multimodale
- Frodi
- Privacy

Sicurezza e Liveness

- La sicurezza di un sistema biometrico può essere intesa come la sua resistenza agli attacchi attivi.
- Tali attacchi possono essere classificati come attacchi di presentazione (spoofing), in cui l'aspetto del campione biometrico viene fisicamente modificato o sostituito; attacchi di elaborazione biometrica, in cui la comprensione dell'algoritmo biometrico viene utilizzata per causare elaborazioni e decisioni errate; vulnerabilità software e di rete, basate sugli attacchi contro il computer e le reti su cui girano i sistemi biometrici; e attacchi sociali e di presentazione, in cui le autorità che utilizzano i sistemi vengono ingannate.
- E’ stata presentata un'indagine sui problemi della sicurezza e della liveness biometrica (antispoofing), inclusi i framework per classificare e misurare le prestazioni della sicurezza biometrica.
- Gli schemi biometrici codificati vengono esaminati per chiarire la loro promessa di contrastare queste minacce alla sicurezza.
- Nella progettazione dei sistemi di sicurezza e liveness, è importante considerare i requisiti operativi dell'applicazione e le specifiche minacce alla sicurezza contro le quali verrà testata.

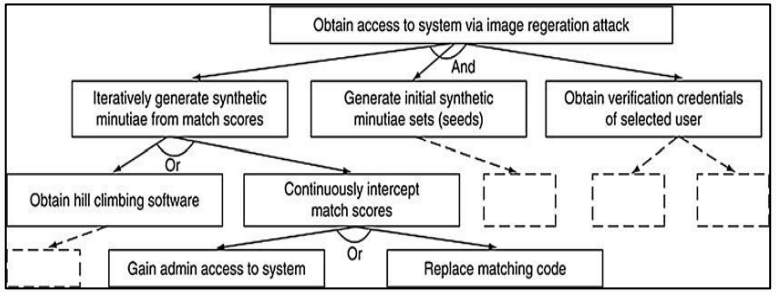
Vulnerabilità Biometriche

- I sistemi biometrici, come tutti i sistemi di sicurezza, hanno delle vulnerabilità.
- Le vulnerabilità sono definite in termini di possibili attacchi attivi contro sistemi biometrici.
- La sicurezza del sistema biometrico è definita dalla sua assenza: una vulnerabilità nella sicurezza biometrica si traduce in un riconoscimento errato o nel mancato riconoscimento corretto degli individui.
- Questa definizione include metodi per accettare falsamente un individuo (spoofing), per ridurre le prestazioni complessive del sistema (denial of service) o per attaccare un altro sistema tramite dati trapelati (furto di identità).
- Viene considerato in dettaglio un modello di elaborazione biometrica e le potenziali vulnerabilità in ogni fase del trattamento: rivendicazione di identità, presentazione, sensore, segmentazione, estrazione di caratteristiche, controllo di qualità, creazione di modelli, archiviazione dei dati, corrispondenza e decisione.



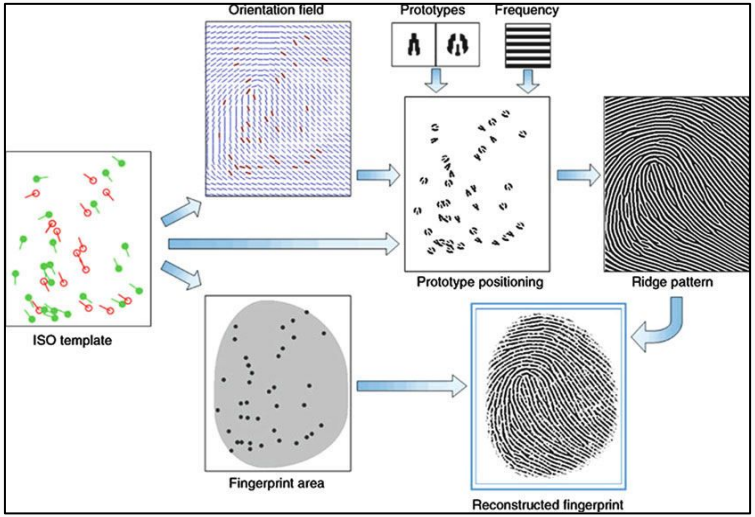
Vulnerabilità Biometriche

- Al fine di comprendere le vulnerabilità di un grande sistema biometrico, vengono spiegati i metodi dell'albero di attacco.
- Vengono forniti quattro esempi di scenari per le applicazioni biometriche: carte d'identità governative, accesso fisico, accesso a computer e rete, e protezione dei contenuti digitali.
- Tuttavia, oltre alle vulnerabilità specifiche della tecnologia biometrica, è importante notare che le vulnerabilità di qualsiasi sistema di sicurezza informatica in rete continuano a essere una preoccupazione; in particolare, tali sistemi sono ingegneria sociale vulnerabile e tutti i problemi di sicurezza che affliggono le moderne reti di computer.
- Le vulnerabilità biometriche devono essere confrontate con quelle dei sistemi che intendono sostituire.
- In molti casi, il sistema biometrico, con le vulnerabilità considerate in questa voce, sarà ancora notevolmente più sicuro delle carte d'identità, delle password o di altri token.
- Inoltre, le combinazioni di dati biometrici con metodi tradizionali (ad es. Biometrico e pin) possono fornire una sicurezza aggiuntiva poiché ciascuno può avere diverse vulnerabilità.



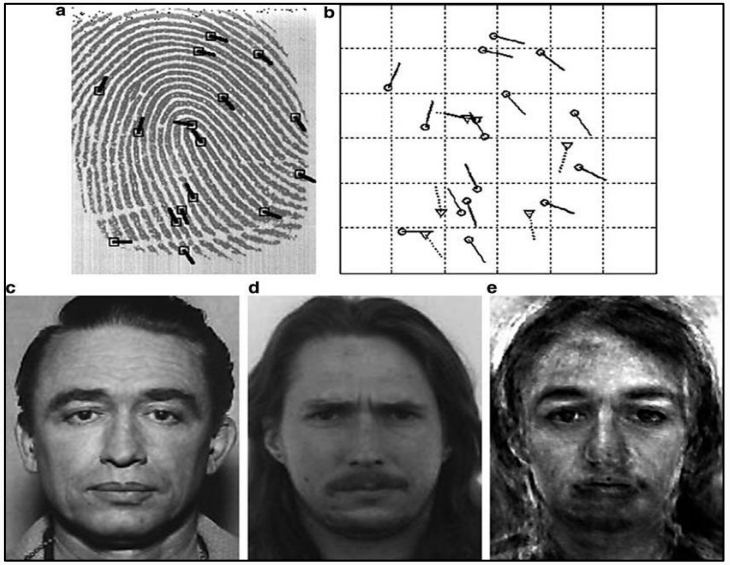
Sicurezza dei Templates

- La sicurezza dei templates si riferisce alle tecniche che consentono la rigenerazione delle immagini registrate dai templates.
- Tale rigenerazione delle immagini pone una vulnerabilità alla sicurezza e alla privacy perché le immagini possono essere utilizzate per falsificare o mascherarsi come individuo registrato.
- La rigenerazione dell'immagine è di due tipi:
  - Il primo si basa sulla decodifica delle caratteristiche nel modello e sulla stima di un'immagine biometricamente ragionevole con le caratteristiche appropriate. I risultati sono stati pubblicati per i templates di impronte digitali, ma tali algoritmi sono facilmente implementabili per il riconoscimento del viso e dell'iride.
  - Il secondo tipo utilizza la capacità di confrontare le immagini con l'obiettivo e ottenere il punteggio di corrispondenza per eseguire scalate in salita (hill climbing) per migliorare in modo iterativo una stima dell'immagine.
- Adeguate misure di sicurezza dei templates biometrici richiedono una forte crittografia di tutti i dati biometrici, inclusi templates e risultati delle corrispondenze.



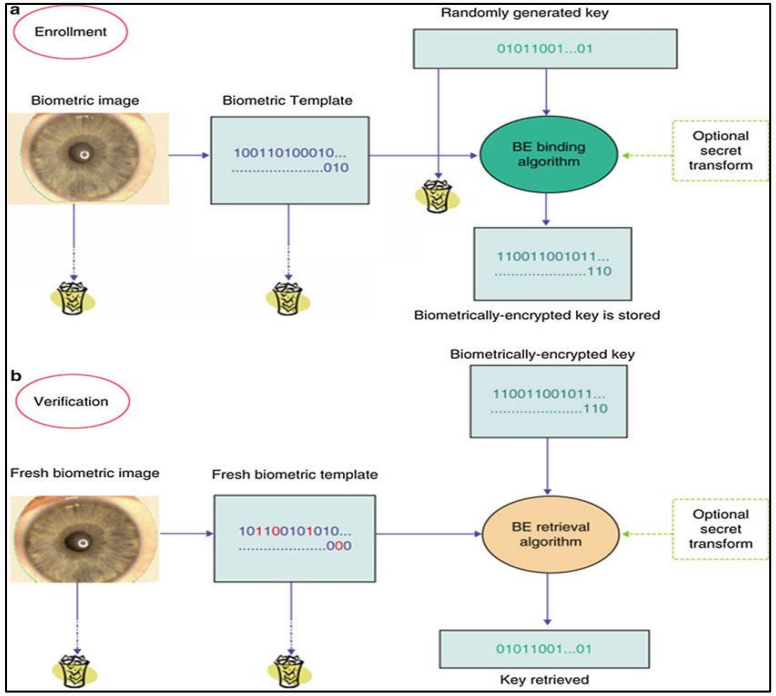
Sicurezza dei Templates

- In tutti i casi testati, un'immagine di alta qualità di un'impronta digitale o di un viso registrato può essere rigenerata se si accede a templates biometrici o per abbinare i punteggi.
- Questa è una forte prova per confutare il fatto che i templates biometrici siano sicuri in modo simile a una funzione hash crittografica.
- Sulla base di questi risultati, una progettazione prudente per la sicurezza biometrica dovrebbe prendere in considerazione qualsiasi dato biometrico che possa potenzialmente "far trapelare" informazioni sulle immagini di origine e fornire un potenziale percorso di attacco.
- Una soluzione parziale è l'uso di tecniche crittografiche per proteggere i dati biometrici nei databases e comunicati sulle reti.



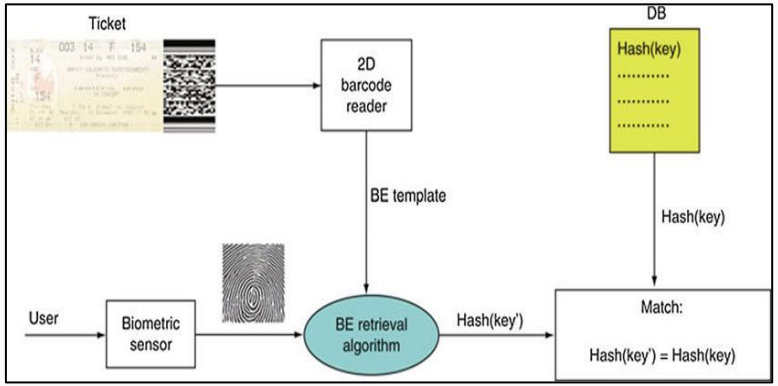
Crittografia Biometrica

- La crittografia biometrica (BE) è un gruppo di tecnologie emergenti che legano in modo sicuro una chiave digitale a una biometrica o generano una chiave digitale dalla biometrica, in modo che non venga memorizzata alcuna immagine o template biometrico.
- Ciò che viene memorizzato è il template BE altrimenti noto come "chiave crittografata biometricamente".
- Di conseguenza, né la chiave digitale né quella biometrica possono essere recuperate dal template BE memorizzato.
- BE è concettualmente diverso da altri sistemi che crittografano immagini o templates biometrici che utilizzano la crittografia convenzionale o memorizzano una chiave crittografica e la rilasciano dopo l'autenticazione biometrica con successo.
- Con BE, la chiave digitale viene ricreata solo se il campione biometrico corretto viene presentato alla verifica.
- L'output della verifica BE è una chiave digitale o un messaggio di errore.
- Questo processo di "crittografia / decrittografia" è confuso a causa della naturale variabilità dei campioni biometrici.



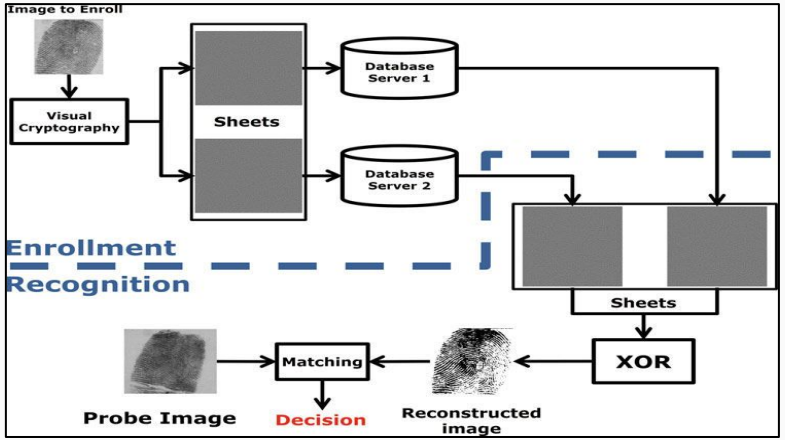
Crittografia Biometrica

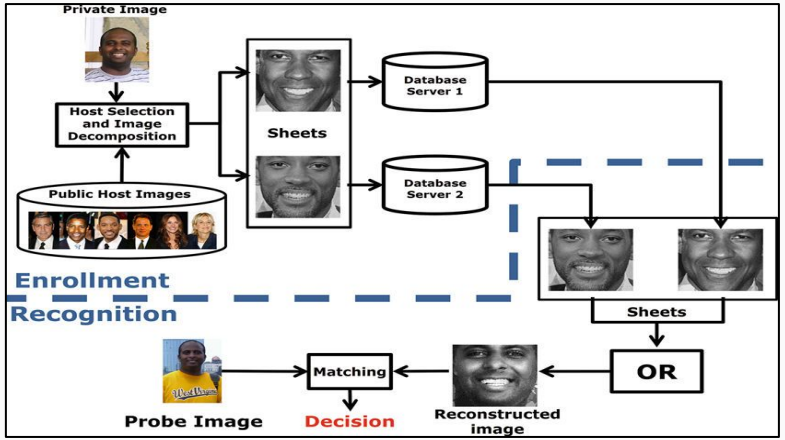
- Attualmente, qualsiasi sistema BE praticabile richiede la memorizzazione dei dati di supporto dipendenti dalla biometria.
- Le tecnologie BE esemplificano i principi fondamentali della privacy e della protezione dei dati approvati in tutto il mondo, come la minimizzazione dei dati, l'empowerment degli utenti e la sicurezza.
- Sebbene l'introduzione della biometria nei sistemi informativi possa comportare notevoli vantaggi, può anche introdurre molte nuove vulnerabilità, rischi e preoccupazioni in materia di sicurezza e privacy.
- Le nuove tecniche di scansione della crittografia biometrica superano molti di questi rischi e vulnerabilità, risultando in un modello che presenta vantaggi sia per la sicurezza che per la privacy.



Crittografia Visiva

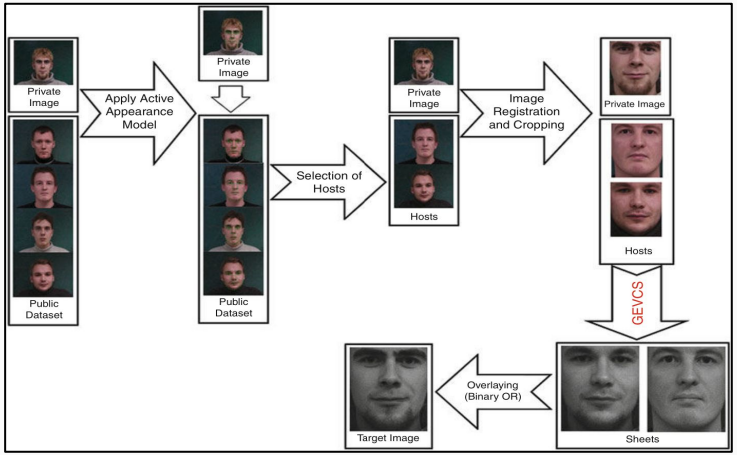
- La crittografia visiva è un metodo per crittografare le informazioni visive, come le immagini, in cui la decrittografia viene eseguita senza la necessità di complessi algoritmi matematici.
- La protezione di un'immagine biometrica memorizzata è di fondamentale importanza perché un tratto biometrico compromesso non può essere facilmente revocato.
- Con questo metodo, un'immagine segreta viene crittografata in n immagini di rumore casuali note come fogli (sheets) in modo che la decrittazione sia possibile solo quando almeno k degli n fogli sono disponibili e combinati utilizzando un operatore logico
- La combinazione di meno di k fogli non rivela l'immagine segreta.
- La crittografia visiva è stata utilizzata per preservare la privacy dei dati biometrici digitali grezzi archiviati in un database centrale.
- Un'immagine biometrica di input (o template) viene scomposta in due componenti in modo che i dati originali possano essere recuperati solo quando entrambi i componenti sono disponibili simultaneamente
- I singoli componenti non possono essere facilmente confrontati con i dati biometrici di input originali, in tal modo deidentificando (cioè oscurando) l'identità dei dati di input.
- Questo approccio è stato testato sulle modalità del viso, delle impronte digitali e dell'iride.

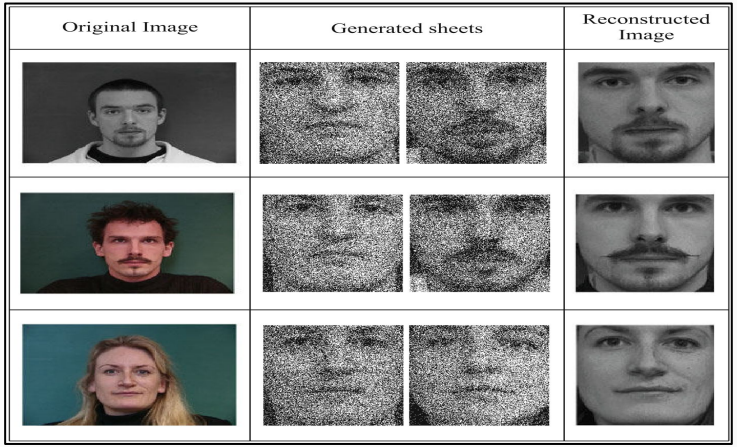




Crittografia Visiva

- Il template biometrico, cioè un'immagine dell'impronta digitale o un codice dell'iride, viene scomposto in due immagini simili al rumore e poiché la disposizione spaziale dei pixels in queste immagini varia da blocco a blocco, è impossibile recuperare il template originale senza accedere a un numero predefinito di condivisioni.
- Quando l'operatore XOR viene utilizzato per sovrapporre le due immagini rumorose, invece dell'operatore OR, viene ripristinato il template binario originale.
- Per preservare la privacy di un database di volti, ciascuna immagine dei volti privati viene scomposta in due immagini di fogli simili a facce indipendenti in modo tale che l'immagine di volti privati possa essere ricostruita solo quando entrambi i fogli sono disponibili contemporaneamente.
- L'algoritmo seleziona prima le immagini hosts che hanno più probabilità di essere compatibili con l'immagine segreta in base alla geometria e all'aspetto.
- GEVCS viene quindi utilizzato per nascondere l'immagine segreta nelle immagini hosts selezionate.
- Test sperimentali su diversi database biometrici hanno dimostrato che la crittografia visiva può essere utilizzata per preservare la riservatezza dei dati biometrici archiviati in un database centrale senza una notevole degradazione nelle prestazioni di riconoscimento biometrico.



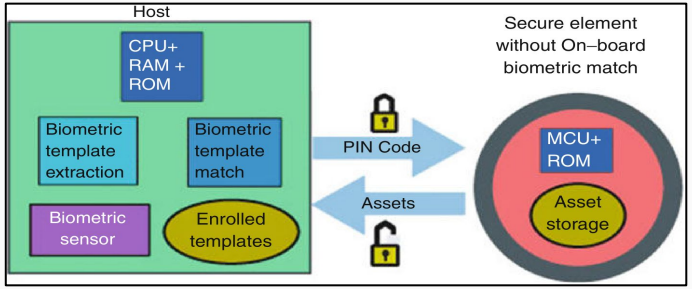


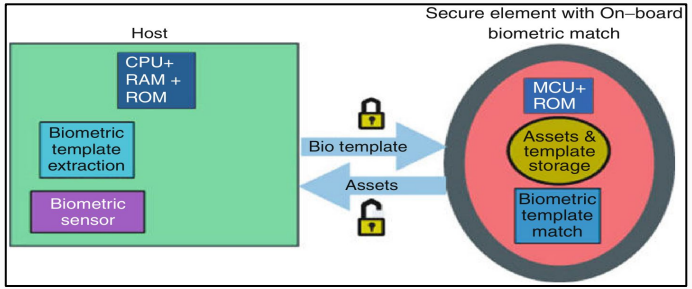
Biometria Cancellabile

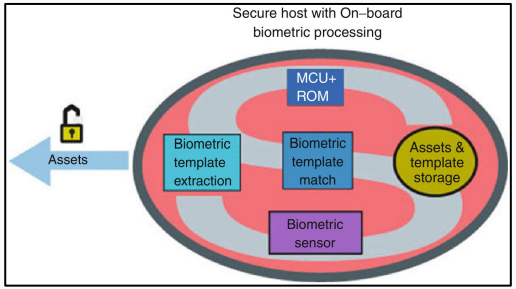
- La biometria cancellabile è progettata per consentire ad un individuo di registrare e revocare un gran numero di campioni biometrici diversi.
- Ogni immagine biometrica è codificata con uno schema di distorsione che varia per ogni applicazione.
- Il concetto è stato sviluppato per affrontare i problemi di privacy e sicurezza che i campioni biometrici sono limitati e devono essere utilizzati per più applicazioni.
- Durante la registrazione, l'immagine biometrica in input è soggetta a una distorsione nota controllata da una serie di parametri.
- Il campione biometrico distorto può, in alcuni schemi, essere elaborato con algoritmi biometrici standard, che non sono consapevoli che le caratteristiche presentate sono distorte.
- Durante l'abbinamento, il campione biometrico vivo deve essere distorto con gli stessi parametri, che devono essere conservati in modo sicuro.
- La natura cancellabile di questo schema è fornita dalla distorsione, in quanto non è il biometrico "effettivo" dell'utente che viene memorizzato, ma semplicemente uno di un numero arbitrariamente grande di possibili permutazioni.
- Una preoccupazione con la biometria cancellabile è la gestione sicura dei parametri di distorsione.

Transportable Asset Protection

- Il Transportable Asset Protection è un mezzo mediante il quale i segreti e i privilegi personali dell'utente, memorizzati in forma digitale su un dispositivo portatile come una smart card o un telefono cellulare, sono protetti dall'accesso e / o dall'uso non autorizzato.
- I beni trasportati sulla propria persona, sono altamente soggetti a furti o perdite, rendendo la necessità di sicurezza molto maggiore.
- L'unica sfida del Transportable Asset Protection è fornire sicurezza e prestazioni adeguate utilizzando le risorse di elaborazione leggere disponibili sul dispositivo mobile in modo portatile e interoperabile.







Falsificazione a Sforzo Zero

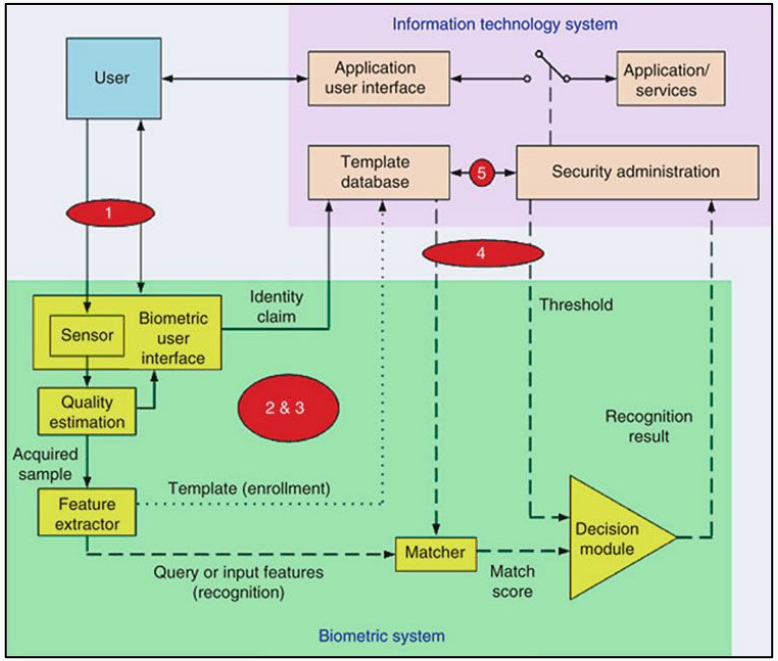
- Un tentativo di impostore è classificato come "sforzo zero" se l'individuo invia la propria caratteristica biometrica come se stesse tentando con successo la verifica rispetto al proprio template, ma il confronto viene effettuato con il template di un altro utente.
- Nel caso della verifica dinamica della firma, un impostore firmerebbe quindi la propria firma in un tentativo a sforzo zero.
- In tali casi in cui gli impostori possono facilmente imitare aspetti del biometrico richiesto, può essere richiesta una seconda misura di impostore basata su "tentativi di impostori attivi".
- Il tentativo di impostore attivo è quello in cui un individuo cerca di abbinare il template memorizzato di un individuo diverso presentando un campione biometrico simulato o riprodotto o modificando intenzionalmente le proprie caratteristiche biometriche.

Standards di Sicurezza Biometrica

- La biometria promette una maggiore fiducia nei processi di autenticazione personale rispetto alle passwords e ai tokens tradizionali (ad es. Chiavi e carte), a causa del collegamento diretto tra la caratteristica biometrica e l'individuo (legame forte) rispetto al collegamento indiretto rappresentato da passwords e tokens (legame debole).
- I sistemi biometrici sono sistemi IT che includono funzionalità di riconoscimento biometrico, con alcuni fattori biometrici specifici.
- Questi includono minacce come lo spoofing e la natura personale dei dati biometrici che richiedono un trattamento speciale.
- Il primo lavoro sugli standards di sicurezza biometrica è stato relativo alla gestione della sicurezza biometrica per il settore dei servizi finanziari.
- Tuttavia, la recente crescita nell'implementazione di sistemi biometrici, in particolare nelle applicazioni di pubblico dominio come passaporti, visti e carte dei cittadini, ha dato un forte impulso allo sviluppo di standards che soddisfino i requisiti globali dei sistemi biometrici e della sicurezza delle applicazioni.
- Di conseguenza, c'è ora uno sforzo concertato da parte dei due principali gruppi di standards coinvolti ISO (International Organization for Standards) / IEC JTC 1 (Joint Technical Committee 1 (IT Standards Committee of ISO)) SC37 (Biometric Standards Subcomm Committee of JTC 1) e SC 27 (sottocomitato per gli standards di sicurezza IT del JTC 1) per collaborare allo sviluppo delle nuove linee guida e standards necessari per implementare i sistemi biometrici in modo sicuro nel mondo moderno.
- Le attuali aree di studio includono:
  - Valutazione biometrica della sicurezza
  - Sicurezza delle transazioni biometriche
  - Protezione dei dati biometrici
  - Guida per la specifica dei requisiti di prestazione per soddisfare le esigenze di sicurezza e usabilità nelle applicazioni che utilizzano la biometria

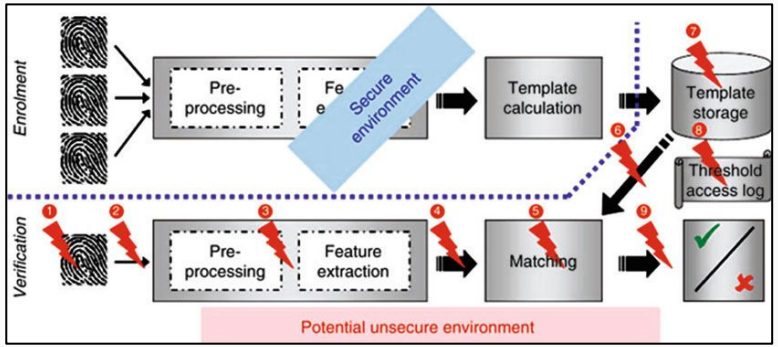
Sicurezza nella Progettazione del Sistema

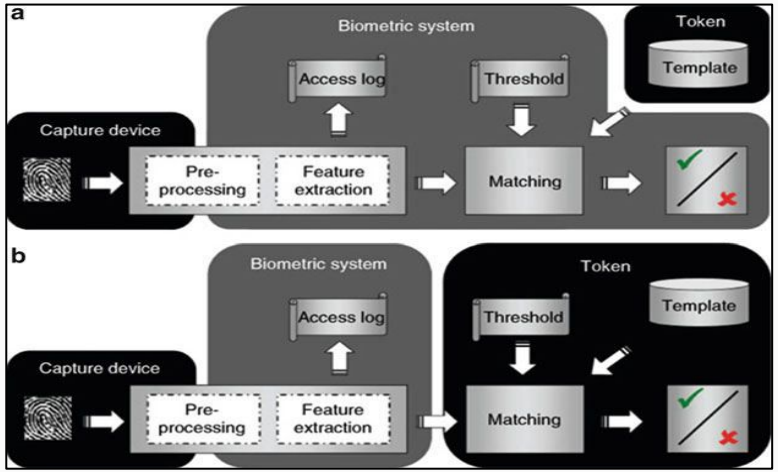
- L'autenticazione delle persone è una delle attività critiche in un sistema di protezione informatica (IT) e il riconoscimento biometrico è una soluzione naturale e affidabile in grado di fornire un'autenticazione sicura.
- Tuttavia, un sistema biometrico è solo un componente della soluzione complessiva della sicurezza IT.
- Per garantire la riservatezza delle informazioni biometriche e l'integrità del sistema biometrico, in fase di progettazione devono essere affrontate diverse questioni di sicurezza.
- Devono essere prese misure adeguate per proteggersi dalle vulnerabilità alle interfacce tra i diversi componenti del sistema di sicurezza e dalle minacce introdotte a causa di un'attuazione e amministrazione improprie del sistema biometrico.
- L'accettazione da parte del pubblico della tecnologia di riconoscimento biometrico dipenderà dalla capacità dei progettisti di sistemi di dimostrare che questi sistemi sono robusti, hanno rapporti inferiori e sono a prova di manomissione.
- Ciò può essere ottenuto valutando la sicurezza del sistema biometrico utilizzando standards di sicurezza IT come il Common Criteria Framework.



Sistema Operativo Tamper-Proof

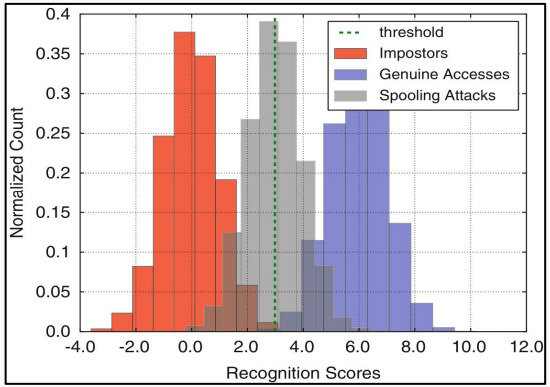
- A causa della sensibilità dei dati biometrici, è necessario considerare la sicurezza nei dispositivi biometrici.
- Uno dei modi per proteggere la privacy è includere un sistema operativo Tamper-Proof, dal design robusto, per non consentire l'esecuzione di codice dannoso.
- L'accesso ai dati e alle procedure interne non è mai consentito senza la dovuta autorizzazione.
- Nelle sue implementazioni più restrittive, questo sistema operativo avrà meccanismi di rilevamento degli attacchi.
- Se l'attacco è di un certo livello, il sistema operativo potrebbe persino cancellare tutto il suo codice e / o dati.
- Il O.S. non consentirebbe l'accesso diretto alle risorse hardware del dispositivo, né a dati temporanei né permanenti.
- Deve anche controllare le diverse fasi di vita del dispositivo e rispettare determinati requisiti.
- Questo tipo di O.S. in tutti i dispositivi biometrici migliorerà la sicurezza dell'intero sistema.
- Sfortunatamente, quando alcune parti del sistema biometrico devono essere implementate in un computer generico con un sistema operativo aperto, applicare queste regole non è facile.

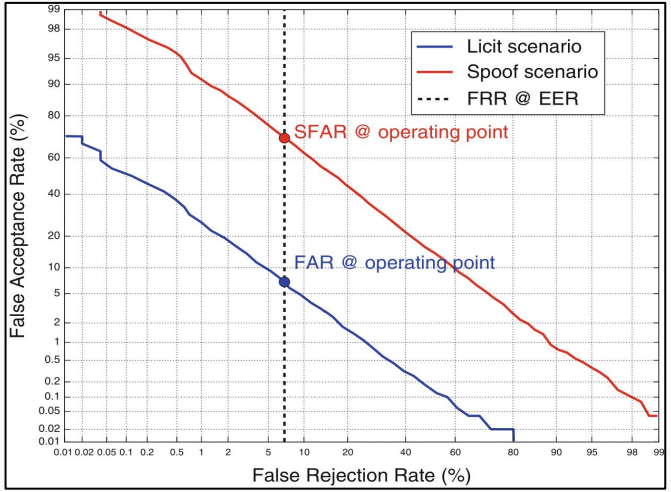




Anti-spoofing – Metodologie di Valutazione

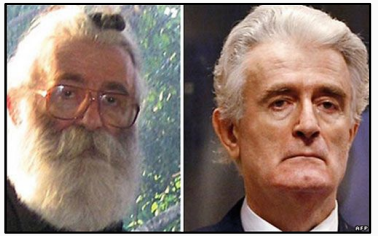
- In seguito alla definizione del compito dei sistemi anti-spoofing di discriminare tra accessi reali e attacchi di spoofing, l'anti-spoofing può essere considerato come un problema di classificazione binaria.
- I database di spoofing e le metodologie di valutazione per i sistemi anti-spoofing sono molto spesso conformi agli standard per i problemi di classificazione binaria.
- Tuttavia, i sistemi anti-spoofing non sono destinati a funzionare autonomamente e il loro scopo principale è proteggere un sistema di verifica dagli attacchi di spoofing.
- Nel processo di combinazione della decisione di un sistema anti-spoofing e di un sistema di riconoscimento, ci si possono aspettare effetti sulle prestazioni di riconoscimento.
- Pertanto, è importante analizzare il problema dell'anti-spoofing sotto l'ombrello dei sistemi di riconoscimento biometrico.
- Ciò comporta alcuni requisiti nella progettazione del database, nonché concetti adattati per la valutazione dei sistemi di riconoscimento biometrico sotto attacchi di spoofing.

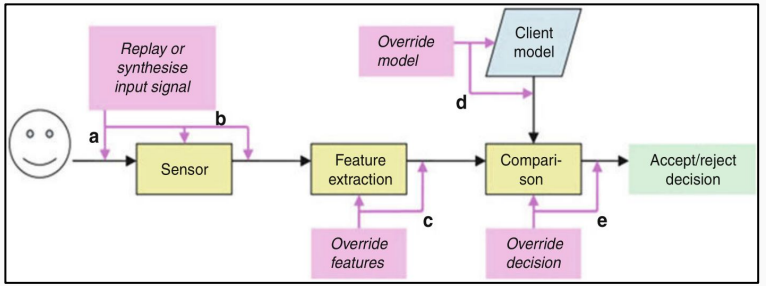


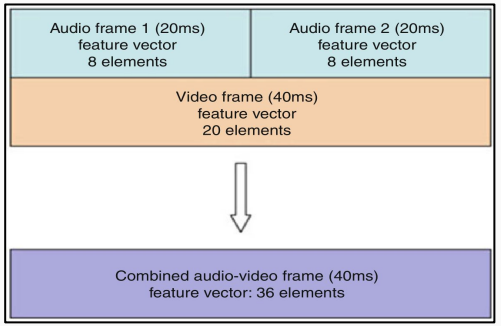


Anti-spoofing – Facciale

- Il processo di verifica se l'immagine del volto presentata a un sistema di autenticazione è reale (cioè, viva) o se è riprodotta o sintetica ("falsificata") e quindi fraudolenta.
- Quando un sistema di autenticazione del volto deve riconoscere il volto di una persona per mezzo di una fotocamera elettronica e del software di riconoscimento delle immagini associato, è importante essere sicuri che la persona che richiede l'autenticazione presenti effettivamente il proprio volto alla fotocamera in quel momento e luogo della richiesta di autenticazione; il volto è presentato in diretta come in televisione in diretta, distinto da un programma di film o cartoni animati.
- Al contrario, un impostore potrebbe provare a presentare una maschera, una fotografia o una registrazione video, mostrando l'immagine del viso di un cliente legittimo alla telecamera per essere falsamente autenticato dal sistema come quel cliente.

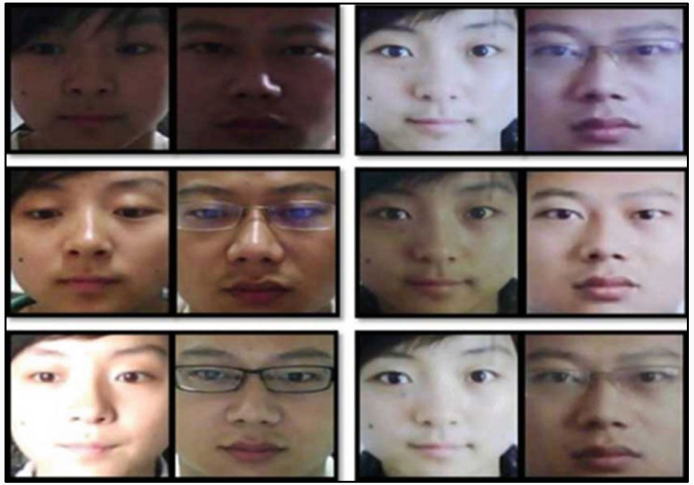






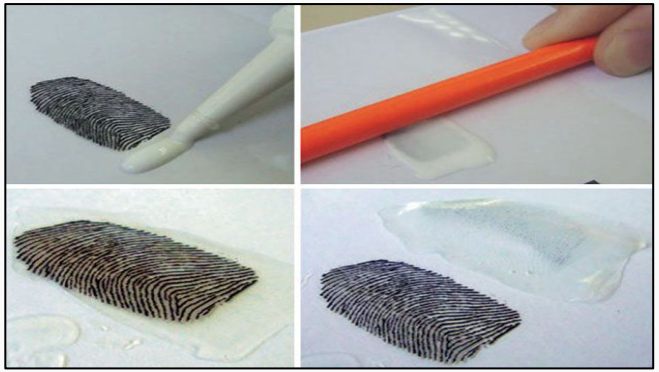
Anti-spoofing – Facciale

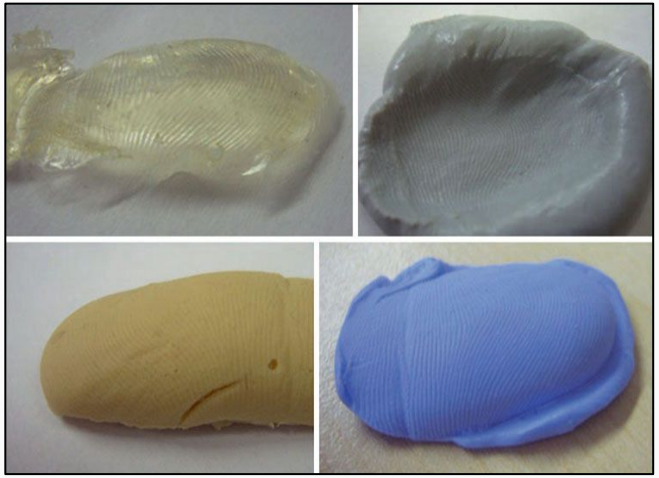
- Questo tipo di minaccia ai sistemi di autenticazione è generalmente noto come replay attack.
- Una minaccia simile è rappresentata dal cosiddetto attacco di sintesi in cui un aggressore costruisce un modello 3D della testa della persona bersaglio da dati fotografici o video al fine di produrre materiale video sintetizzato che mostra il volto del cliente che ruota realisticamente in tre dimensioni.
- Gli attacchi di riproduzione e gli attacchi di sintesi sono noti collettivamente come attacchi di spoofing.
- A sua volta, il liveness assurance, o anti-spoofing, utilizza una serie di misure per ridurre la vulnerabilità dei sistemi di autenticazione facciale alle minacce di attacchi di spoofing.



Anti-spoofing – Impronta Digitale

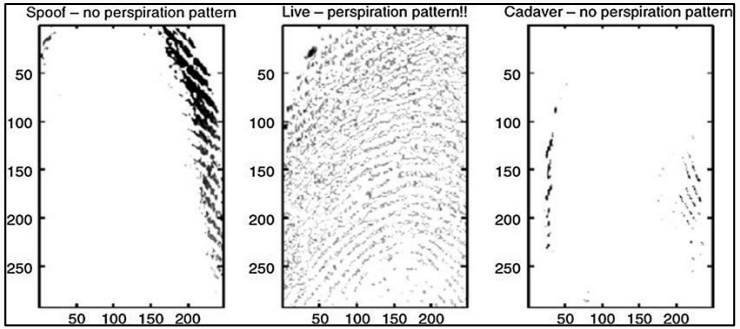
- Il rilevamento delle impronte digitali viene utilizzato per identificare un dito falso, ad esempio un calco in lattice.
- Per estensione, include anche test per rilevare un dito tagliato o morto o un'impronta latente rimanente su un sensore dopo l'uso.
-



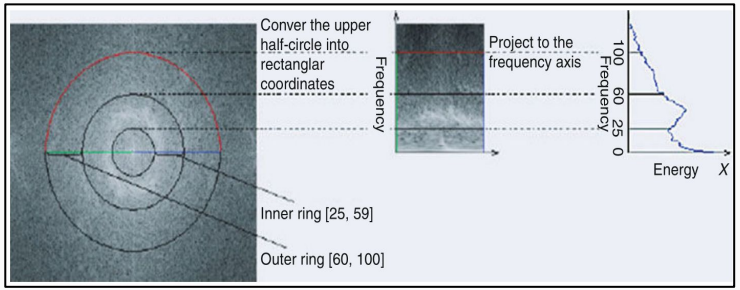


Anti-spoofing – Impronta Digitale (Hardware e Software)

- Le misure di liveness hanno una performance intrinseca, ovvero la capacità di separare lo spoofing dai tentativi live.
- Inoltre, gli algoritmi di liveness hanno altri fattori e considerazioni tra cui facilità d'uso, collezionabilità, accettazione da parte dell'utente, universalità, unicità, permanenza e capacità di spoofing.
- Un fattore difficile da misurare è la capacità di falsificazione, la possibilità che la misura della vivacità possa essere falsificata.
- In questo capitolo viene utilizzato il termine liveness, riconoscendo pienamente che non si tratta di un sistema perfetto e che non è possibile ricreare tutti i possibili tentativi di spoofing per un sistema.
- Inoltre, potrebbero esserci misurazioni, che escludono spoof specifici ma non possono essere mostrate per misurare in modo assoluto la vivacità.
- Ad esempio, possono essere progettati algoritmi in grado di rilevare prontamente immagini contraffatte di silicio, ma non di gelatina.
- In sintesi, è improbabile che qualsiasi sistema misuri perfettamente la vita e sia a prova di spoofing.
- La liveness può essere ridotta a un tentativo di stare un passo avanti rispetto a coloro che intendono sconfiggere il sistema attraverso attacchi di spoofing.
- Metodi come la vivacità o l'anti-spoofing sono fondamentali per la sicurezza e la credibilità dei sistemi biometrici per proteggerli dalle vulnerabilità della sicurezza nella misura necessaria per una particolare applicazione.

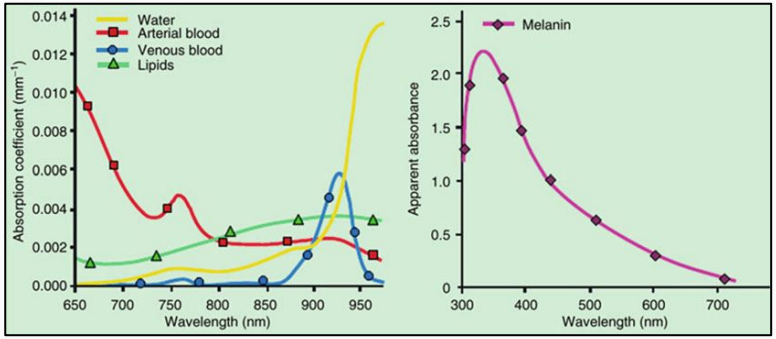


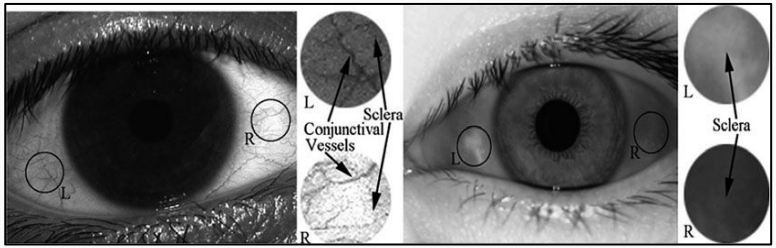
	Ease of use	Collectability	User acceptance	Universality	Uniqueness	Permanence	Spoof-ability
Perspiration	H	H	H	M	L	M	M
Pulse oximetry	L	L	L	H	–	–	H
Multispectral	H	H	M	H	–	–	L
Deformation	L	L	H	M	–	–	M
ECG	L	L	L	H	L	H	H

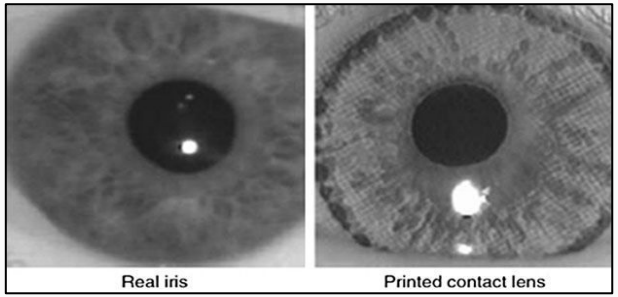


Anti-spoofing – Iride

- Le tecniche anti-spoofing dell'iride sono progettate per contrastare gli attacchi di spoofing fisico lanciati contro i sistemi di riconoscimento dell'iride.
- Tali attacchi sono diretti a livello del sensore e cercano di ottenere l'accesso al sistema presentando un artefatto fisico al dispositivo di acquisizione.
- Nel caso dell'iride, tali artefatti includono l'uso di fotografie, registrazioni video, lenti a contatto stampate, occhi artificiali, ecc.
- I meccanismi anti-spoofing dell'iride hanno lo scopo di accertare che le immagini dell'iride siano state acquisite da un utente vivo e autorizzato presente al momento del transazione.
- In particolare, ci si aspetta che le lenti a contatto con patterns dell'iride hand-printed e stampati rappresentino una minaccia crescente a causa dei miglioramenti della qualità dell'inchiostro e delle tecnologie di stampa.
- Inoltre, le lenti con patterns sono relativamente difficili da rilevare rispetto ad altri metodi di spoofing.
- Pertanto, è fondamentale selezionare un dispositivo che incorpori contromisure di spoofing a un livello di sofisticazione ed efficacia che corrisponda ai requisiti dell'applicazione.
- Poiché le tecniche di spoofing sono in rapida evoluzione e le contromisure hanno solo un ciclo di vita limitato, oltre ai necessari sforzi di ricerca e sviluppo, è di grande importanza eseguire test di robustezza standardizzati e indipendenti dal fornitore e valutare regolarmente il livello generale di sicurezza fornita dai sistemi biometrici.

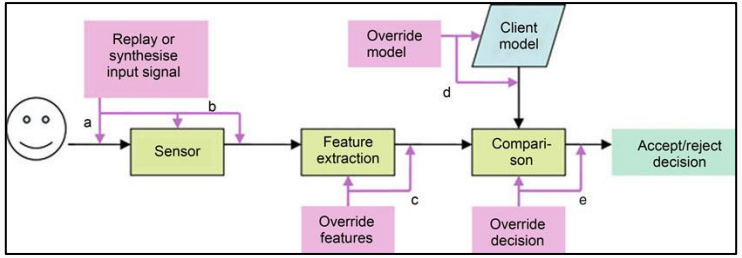


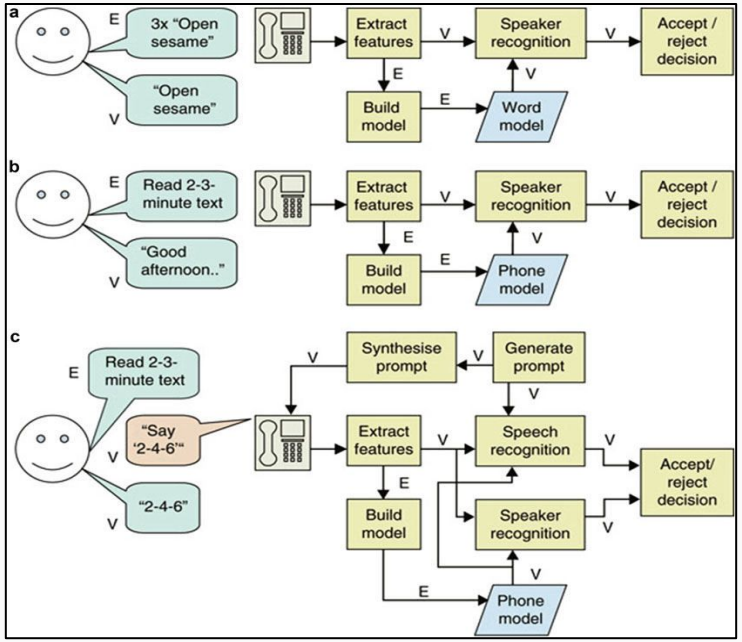




Anti-spoofing – Vocale

- Il processo di verifica se il campione vocale presentato a un sistema di autenticazione è reale (cioè, vivo), o se è riprodotto o sintetico, e quindi fraudolento.
- Quando viene richiesta l'autenticazione tramite un sistema di autenticazione vocale, è importante essere sicuri che la persona che richiede l'autenticazione fornisca effettivamente il campione vocale richiesto al momento e nel luogo della richiesta di autenticazione.
- La voce viene presentata dal vivo come quella di un presentatore radiofonico durante una trasmissione in diretta, distinta da un nastro audio registrato.
- Al contrario, un impostore che cerca l'autenticazione in modo fraudolento potrebbe tentare di riprodurre una registrazione audio di un cliente legittimo o un discorso sintetizzato prodotto per assomigliare al discorso di un cliente legittimo.
- Tali minacce al sistema sono note rispettivamente come attacco replay e attacco di sintesi.
- La garanzia della durata utilizza una serie di misure per ridurre la vulnerabilità di un sistema di autenticazione vocale alle minacce di replay e attacco di sintesi.





Anti-spoofing – Multimodale

- L'anti-spoofing, o rilevamento della liveness, nella biometria multimodale è intesa come la capacità di un sistema biometrico multimodale di rilevare e rifiutare le sperimentazioni di accesso in cui vengono presentati i tratti biometrici di una o due prove di rilevamento.
- Ad esempio, se un utente malintenzionato tenta di accedere a un sistema protetto da verifica personale tramite volto e impronta digitale, inviando il proprio volto e una replica dell'impronta digitale del cliente mirato, il sistema deve essere in grado di rilevare e rifiutare questo attacco.
- La classificazione eseguita da ciascun modulo, indipendentemente, viene combinata da regole di fusione a livello di punteggio o di decisione.
- Così come i sistemi biometrici unimodali, quelli multimodali possono essere attaccati presentando un tratto "falso", cioè una replica artificiale di almeno una delle biometrie del sistema.
- Pertanto, il problema principale consiste nel rifiutare questo tipo di attacco.
- Ciò può essere ottenuto aggiungendo un modulo di rilevamento della liveness a ciascuna modalità biometrica per fornire regole di fusione "solide" contro gli attacchi di spoofing.
- Le regole di fusione del punteggio ad hoc sono in grado di sfruttare le informazioni provenienti da un punteggio di corrispondenza generato quando si confronta un biometrico contraffatto con i relativi modelli originali.
- Finora non sono state riportate evidenze sull'integrazione di algoritmi di rilevamento della liveness multipla e di matching in sistemi multi-biometrici, mentre diverse evidenze sono state riportate nel caso di sistemi monomodali.

Frodi

- La frode è convenzionalmente definita come la deliberata perversione o negazione della veridicità per indurre un altro a cedere qualcosa di valore.
- Nel contesto della biometria, l'elemento di valore è tipicamente un'identità o un privilegio associato a un'identità.
- La frode può assumere una varietà di forme che vanno dal phishing alle truffe all'hacking.
- Nel caso specifico della biometria, la frode può anche consistere nello spoofing o nella presentazione di un artefatto progettato per imitare un biometrico legittimo.
- La riduzione delle frodi in un contesto biometrico implica sia l'uso della tecnologia biometrica per scoraggiare, inibire e mitigare le frodi sia gli sforzi per contrastare lo sfruttamento delle vulnerabilità del sistema biometrico attraverso comunicazioni illegittime.

Privacy

- La privacy è un concetto multidimensionale e in evoluzione, la cui definizione varia a seconda del Paese e della cultura.
- È quindi difficile concordare una definizione precisa che sia universalmente accettata.
- Tuttavia, alcune nozioni di privacy sono diventate abbastanza standard, specialmente tra i paesi industrializzati.
- Questi includono la privacy informativa, fisica, territoriale e delle comunicazioni.
- Di questi, la biometria non solo ha un impatto sulla privacy informativa, ma anche sulla privacy corporea e territoriale.
- Tuttavia, contrariamente alle affermazioni dei libertari civili e al clamore di Hollywood, la biometria non deve essere antitetica alla privacy.
- Infatti, comprendendo le questioni rilevanti, è possibile progettare in un sistema biometrico misure che salvaguarderanno, e persino miglioreranno, la privacy.
- Ciò aumenterà l'accettazione da parte degli utenti dei sistemi biometrici, o almeno renderà tali implementazioni più tollerabili.

UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

GRAZIE PER L'ATTENZIONE