Biometria e Sicurezza Informatica

In questa rubrica non abbiamo mai affrontato l'argomento Biometria. Vi sono varie ragioni per cui abbiamo rimandato sino ad oggi l'affrontare questo tema. Non possiamo ovviamente in questa sede entrare in dettagli tecnici su specifiche implementazioni informatiche della biometria, e neanche eseguire test o valutazioni di tecniche e procedure, cose che pochi laboratori sono in grado di fare e non sempre senza difficoltà. Uno degli scopi di questa rubrica è quello di cercare di essere pratici, alle volte sin troppo, ed in linea con questa idea cercheremo in questo e futuri articoli, di discutere alcuni punti essenziali da tenere in considerazione nell'implementare sistemi informatici che coinvolgono elementi biometrici.

Biometria per cosa?

La biometria è ovviamente legata al processo di autenticazione. Pur rischiando di risultare noiosi, vogliamo ripetere in questa sede le basi di questo processo. L'autenticazione nei confronti di un processo/servizio informatico consta usualmente di 3 passaggi:

1. l'identificazione
2. l'autenticazione propria
3. l'autorizzazione.

Nella prima fase chi (o cosa se è un processo) vuole avere accesso, dichiara le proprie generalità. Nella seconda fase il sistema verifica che le generalità siano vere, ovvero verifica che il dichiarante sia proprio chi dichiara di essere. Nell'ultima fase, autenticato il richiedente, il sistema gli fornisce le credenziali opportune per poter svolgere il proprio lavoro. Ovviamente la seconda fase è quella che ci interessa in questa sede.

Per poter verificare le generalità bisogna già conoscere qualche cosa di distintivo, unico o segreto, di chi si vuole autenticare. Generalmente l'autenticazione può essere fatta basandosi su

1. qualche cosa che si ha

2. qualche cosa che si sa
3. quello che si è.

Nel primo caso chi deve autenticare ha in comune con l'autenticando un oggetto, tipicamente una chiave rispetto ad una serratura, e l'autenticità è basata sull'*unicità* della coppia chiave/serratura e sulla non *copiabilità* della chiave. Nel secondo caso quello che è in comune è una *informazione segreta*, quale una password. In questo caso non è detto che il segreto debba essere noto nello stesso modo ad entrambi, ad esempio nel caso delle password il sistema può conoscerne solo l'impronta della password, oppure può conoscere la chiave pubblica corrispondente alla chiave privata posseduta dall'autenticando. Il terzo caso è il regno della biometria, di nuovo ci si basa sull'*unicità* e non *copiabilità* delle caratteristiche usate per l'autenticazione, come nel primo caso, e non sulla loro segretezza, ma questa volta non si usano oggetti ma le caratteristiche fisiologiche o comportamentali della persona. E' d'uopo una osservazione: alcuni distinguono tra caratteristiche biometriche fisiologiche, quali impronte digitali, forma del viso, della mano ecc., e caratteristiche comportamentali, quali la scrittura, l'andatura ecc. E' abbastanza chiaro che in realtà le due classi non sono totalmente indipendenti, ad esempio caratteristiche comportamentali dipendono da quelle fisiologiche come illustrato dall'andatura che dipende dalla forma e lunghezza delle gambe, del bacino eccetera.

Tornando al processo di autenticazione, in ogni caso è necessario che chi autentica e chi è autenticato si siano messi d'accordo preventivamente in modo che chi poi deve verificare l'autenticazione abbia nella propria base dati le informazioni per validare i dati ricevuti. La fase iniziale di *registrazione* (enrolment) è quindi molto importante e lo è ancora di più nel caso della biometria ove le caratteristiche da verificare possono essere mutevoli.

Il processo di registrazione

Ovviamente tutti i sistemi biometrici cercano di individuare delle caratteristiche il più possibile immutabili del corpo umano, ma oltre alle caratteristiche umane vanno tenute in conto le condizioni

di rilevamento delle stesse. Prendiamo come semplice esempio quello della voce: la nostra voce cambia con il tempo, ma cambia anche se siamo raffreddati ed in molte altre circostanze. Se la mutabilità della voce è ovvia, anche molte altre caratteristiche fisiologiche cambiano sia in modo irreversibile sia solo temporaneamente. Anche la forma della mano o la geometria del viso sino alle impronte digitali sono soggette a modifiche piccole o grandi, temporanee o irreversibili. Lo stesso vale per le caratteristiche comportamentali, basta ricordare che alcuni Istituti Bancari chiedono che la firma venga ri-depositata ogni 5 anni. Ne consegue che le caratteristiche biometriche da rilevare devono essere date non dall'immagine fisiologica completa o la registrazione completa del comportamento, ma aspetti salienti e poco mutabili dello stesso. Quindi nel processo di registrazione dell'informazione biometrica è necessario estrarre in modo molto accurato questa informazione.

Ma ciò non basta. Un sistema biometrico deve tener conto non solo di questi fattori ma anche del modo in cui viene fatta la rilevazione. Tornando all'esempio della voce, se il campione iniziale è registrato in camera anecoica e poi la autenticazione è fatta in spazi aperti con rumore di fondo, vento eccetera, è possibile che nulla funzioni. Lo stesso vale per l'impronta digitale. L'immagine dell'impronta registrata dal rivelatore dipende dall'angolazione verticale ed orizzontale, dalla centratura, dalla pressione del dito, ma anche dalla umidità ambientale, dalla sudorazione istantanea, dalla presenza di creme od altre sostanze sulla pelle, eccetera.

Quindi la registrazione dei campioni iniziali, che creano la base dati di autenticazione, deve essere fatta tenendo conto delle condizioni reali di utilizzo degli stessi, ed in molti casi questo non è un compito facile. Per questo il processo iniziale prevede una fase di verifica della qualità del campione, seguito dall'estrazione delle caratteristiche distintive e la loro memorizzazione in forma matematica in un *Template di riferimento*, si veda la Figura 1. Un tipico processo di registrazione è composto come prima fase dalla registrazione di alcuni campioni della stessa caratteristica biometrica. Il ripetere l'operazione assolve anche il compito di istruire la persona all'utilizzo dell'apparecchiatura ed, ad esempio, al corretto posizionamento rispetto ad essa. Il processo di verifica della qualità controlla se i campioni iniziali sono sufficientemente simili e se da essi si può

estrarre un unico campione di riferimento che permetterebbe l'autenticazione per tutti loro. E' fondamentale che il campione registrato nella base dati sia di alta qualità, il che significa che da un lato deve permettere di identificare la caratteristica biometrica, ovvero essere molto simile a qualunque campione rilevato della stessa persona, dall'altra parte deve essere unico, ovvero deve essere molto difficile che un campione appartenente ad un altra persona venga confuso con questo. Il successo di un qualunque sistema di autenticazione biometrico dipende grandemente sulla qualità dei campioni registrati nella base dati.

Si noti che ciò dipende molto dalle persone che formano gli utenti del sistema biometrico. Sono state individuate tre classi di utenti che si discostano dall'utente medio (utente che fornisce dati di buona qualità) ed a cui bisogna prestare particolare attenzione al momento della registrazione:

1. GOAT (capre): sono utenti che non riescono a fornire campioni di buona qualità, sia per problemi di bassa qualità intrinseca (fisiologica o comportamentale) che per difficoltà di interazione con l'apparecchiatura, in particolare due misure successive della stessa caratteristica biometrica di un utente di questa classe possono risultare troppo diverse da poter essere identificate;
2. SHEEP (pecore): sono utenti che forniscono campioni privi o poveri di segni distintivi o unici, che si prestano quindi a essere confusi con campioni di altri ed ad essere facilmente imitati;
3. WOLF (lupi): sono utenti che dimostrano particolare abilità a produrre caratteristiche biometriche che imitano quelle di altri utenti, ed in particolare a farsi scambiare per utenti *sheep*.

Da questa discussione emerge un fatto fondamentale che bisogna sempre tenere in considerazione quando si utilizza un sistema biometrico. Tutte le volte che un utente si autentica fornendo un campione biometrico, viene fornito un campione *diverso*. A seconda del tipo di caratteristica rilevata, del modo di rilevazione, del tipo di utenti eccetera, la differenza fra i campioni forniti dallo

stesso utente può essere minore o maggiore, ma statisticamente i campioni sono sempre diversi. Quindi al momento dell'autenticazione biometrica la domanda che possiamo porre è quanto simile è il campione fornito rispetto a quello presente nella base dati, e non se i due campioni sono identici.

Biometria in Sicurezza Informatica

Considerando ora i modi in cui è possibile utilizzare le tecniche biometriche in informatica.

L'uso che noi facciamo come uomini dell'autenticazione biometrica è diverso dal classico schema informatico in tre punti: identificazione, autenticazione e autorizzazione. Infatti se incontriamo per strada una persona conosciuta, la riconosciamo dall'aspetto del viso. Di solito la persona che incontriamo non ci dice il proprio nome e solo dopo noi verifichiamo se quel nome corrisponde all'immagine che abbiamo in memoria. Avviene tutt'al più l'esatto contrario, nel caso l'immagine non ci sia nota, o siamo in dubbio, chiediamo il nome alla persona. E' possibile utilizzare la biometria in informatica nello stesso modo, ed in realtà questa è la modalità che tutti intuitivamente associamo all'uso della biometria. Dobbiamo quindi distinguere nettamente tra sistemi biometrici di riconoscimento, che funzionano in questo modo, e quelli di autenticazione che funzionano secondo la procedura informatica.

Sistemi 1 a N

I sistemi biometrici di riconoscimento od identificazione sono detti sistemi biometrici *1 a N* e funzionano secondo il seguente procedimento (Fig. 2). Una volta preparata la base dati, ogni misura (*Template corrente*) viene confrontata con tutti i dati presenti (*Template di riferimento*) e vengono individuati i dati che più le assomigliano. Poiché è impossibile che ci sia un match esatto, il sistema biometrico fornisce un set di possibili identità ognuna con un indice di confidenza, ovvero una percentuale di similarità, che indica quanto il Template corrente si avvicina a quello di riferimento. Questo procedimento ha però molti inconvenienti. Il primo è che se la base dati è grande, sono

necessarie molte risorse per confrontare ogni Template corrente con tutti quelli di riferimento. Per limitare il numero di possibili identificazioni, si introduce di solito una *soglia minima* sulla percentuale di similarità, ma questo non garantisce che l'identificazione sia unica, anzi in casi estremi il sistema può anche fornire con la stessa percentuale di similarità più di una identificazione. Per ottenere un risultato unico si può scegliere la identificazione con la percentuale di similarità più alta, scegliendo a caso se ve ne sono più di una con lo stesso valore massimo. Si noti però che alcuni algoritmi forniscono solo la *prima* identificazione che supera la soglia minima.
In conclusione, in molte situazioni la precisione odierna di questi sistemi non è ancora tale da poter dare una risposta univoca del tipo: 'è la tal persona' oppure 'non è presente nella base dati' al 99,99...%.
Vi è comunque molto interesse per questo tipo di sistemi, ad esempio per la lotta al terrorismo le autorità americane studiano un sistema per riconoscere i volti di noti terroristi all'interno degli aeroporti. Come per tutti i sistemi biometrici, vi sono due rischi:

1. *Falso Positivo:* ovvero che il sistema scambi un onesto cittadino per un terrorista, in altre parole vi è un match errato del Template corrente con un Template di riferimento nella base dati, con un sufficiente livello di confidenza; le conseguenze ovviamente non sono piacevoli per l'onesto cittadino che sicuramente viene arrestato e passa qualche brutta ora in prigione;
2. *Falso Negativo*: in questo caso il sistema non riconosce un vero terrorista, ovvero il match magari c'è stato ma per le condizioni ambientali, gli occhialoni, i capelli tinti ed i movimenti rapidi che hanno fornito immagini di bassa qualità, il livello di confidenza è troppo basso, ed il risultato è stato scartato dal sistema.

Sistemi 1 a 1

L'altra modalità di utilizzo della biometria segue la procedura informatica usuale ed è detto processo biometrico *1 a 1* (Fig. 3). Pertanto chi deve autenticarsi fornisce al sistema prima la propria identità e poi il sistema rileva i dati biometrici. Nella base dati del sistema, ad ogni identità

è associato il relativo Template biometrico di riferimento, quindi al momento dell'autenticazione il sistema deve confrontare solo il Template corrente con quello unico presente in memoria per quella identità. E' chiaro che in questo caso il lavoro del sistema è molto più semplice e richiede relativamente poche risorse. La risposta del sistema biometrico è il livello di confidenza di eguaglianza, ovvero la percentuale di similarità, tra il Template corrente e quello di riferimento presente nella base dati. E' necessario di nuovo introdurre una soglia minima per il livello di confidenza, sopra la quale si considerano uguali i due campioni. Questo parametro è cruciale, e ne discuteremo approfonditamente in un prossimo articolo.

Si noti come in questo caso è naturale affiancare alla biometria una secondo metodo di autenticazione. In pratica l'idea più semplice è username + password + impronta digitale, ma sistemi informatici avanzati di autenticazione all'accesso o rilevazione delle presenze possono coinvolgere tecnologie più avanzate. A mo' di esempio teorico ed un po' estremo, consideriamo una carta a radiofrequenza RFID che può anche portare un chip crittografico con chiave segreta (quali ad esempio Mifare e Calypso) associata ad esempio alla rilevazione della forma della mano o di una impronta digitale. In questo caso si realizzano tutte e tre i metodi di autenticazione. La persona deve possedere un token fisico ad averlo con se (la carta RFID), ed il primo scopo del token è quello di fornire al sistema una identità. Nella carta è poi mantenuto un segreto, la chiave segreta, che autentica il token (non la persona!) in maniera sicura. Infine la misura della caratteristica biometrica assicura sulla identità del possessore/portatore del token. In pratica l'utente deve avere nel portafoglio la carta RFID ed effettuare solo la misura biometrica visto che la lettura della carta avviene automaticamente all'avvicinarsi al punto di misura biometrica.

L'esempio che abbiamo appena citato, carta RFID più misura biometrica, non vuole essere un suggerimento ma solo un esempio teorico un po' estremo di cosa sia possibile, ed ha molti altri problemi associati all'uso dei sistemi in radiofrequenza: dalle problematiche relative alla Privacy all'effettiva sicurezza delle piattaforme RFID. Non è ovviamente questa la sede per discutere di questo argomento, comunque molto interessante ed attuale. In pratica, possiamo sostituire la carta RFID con una smartcard, l'unica differenza con quanto descritto precedentemente è che l'utente

deve effettuare due operazioni, prima la lettura della smartcard, con la digitazione del relativo codice PIN, e poi la misura biometrica.

Misurare un Sistema Biometrico

Per essere pratici in questa esposizione, consideriamo un sistema biometrico di tipo 1 a 1, ovvero che data una identità debba verificare se i dati biometrici misurati, che formano il *Template corrente*, corrispondono al *Template di riferimento* presente nella base dati per quella specifica identità. Come abbiamo detto, la verifica ha successo se la percentuale di similarità (indice di confidenza di uguaglianza) tra i due Template è superiore ad una certa soglia.

Popolazioni, statistiche ed errori

Supponiamo di fare un esperimento. Prendiamo una popolazione di utenti, qualche migliaio di persone, che sia *statisticamente rappresentativa del genere umano o di una certa popolazione*. Assegnamo a ciascuno una identità e registriamo nel sistema biometrico il Template di riferimento per ciascuno. L'esperimento consiste nel far autenticare dal sistema tutte le persone con il vincolo che ognuno ha un solo tentativo a disposizione. (A parte il vincolo sul numero dei tentativi, questo è quello che succede ogni mattina usando un sistema biometrico per il controllo degli accessi/rilevazione delle presenze.) Per ogni persona registriamo la percentuale di similarità tra i due Template, e poi facciamo un grafico che riporta il numero di persone rispetto al valore dell'indice. Il risultato è un grafico simile a quello in Fig. 4.

In questa figura abbiamo posto la soglia ad un certo valore arbitrario, si noti che nel nostro esperimento alcune persone non sono state riconosciute ed autenticate dal sistema. Sono gli errori di tipo *False Non Match Rate* FNMR (o *False Rejection Rate* FRR) e sono indicati dall'area grigia. Ovviamente se spostassimo la soglia più in basso, tutti gli utenti sarebbero autenticati.

Prima di abbassare la soglia, facciamo però un ulteriore esperimento. Prendiamo sempre lo stesso campione di persone e le facciamo autenticare di nuovo con un solo tentativo, ma questa volta ogni

persona deve dichiarare l'identità di un altro. Facciamo un grafico come prima e lo mettiamo insieme a quello precedente ottenendo la Fig. 5.

Ovviamente per la maggior parte degli utenti impostori, la percentuale di similarità è molto bassa, ben al di sotto della soglia. Ma come prima c'erano degli errori di non riconoscimento, ora ci sono degli errori di riconoscimento, i *False Match Rate* FMR (o *False Acceptance Rate* FAR), indicati dall'area nera in figura. Se il problema precedente era noioso, utenti veri non accettati, questo è invece un grave problema di sicurezza, vi sono impostori che riescono a superare il sistema di controllo biometrico. Come si vede dalla Fig. 5, se alziamo la soglia per ridurre a zero i FMR, aumentiamo i FNMR e viceversa. In altre parole, la dipendenza di FMR e FNMR dalla soglia è inversa, come è indicato chiaramente in Fig. 6.

Alcune considerazioni

La situazione descritta dalle figure 4, 5 e 6, è quella attuale dei sistemi biometrici. Anche se fosse possibile costruire un sistema biometrico per cui le due distribuzioni in Fig. 5 non si sovrapponessero dando quindi la possibilità, posizionando la soglia in mezzo, di ottenere zero FMR e zero FNMR, bisogna sempre ricordarsi che un sistema biometrico da solo un livello di confidenza di identificazione e mai la certezza. Ritorneremo su questo punto in un prossimo articolo. In questa sede vogliamo approfondire la discussione sul significato delle tre figure. In Fig. 6 abbiamo indicato altri tre parametri di interesse. Il primo è ZeroFNMR che da il valore di FMR quando FNMR è zero, ovvero la percentuale di false accettazione quando posizioniamo la soglia in modo da avere statisticamente nessun rifiuto di utenti veri. Analogamente ZeroFMR è il valore di FNMR quando FMR è zero, ovvero la percentuale di falsi rifiuti quando posizioniamo la soglia in modo da avere statisticamente nessuna accettazione di impostori. E' ovvio che conviene posizionare la soglia tra questi due punti.

Un altro punto ritenuto interessante è quello in cui la soglia è posizionata in modo che FNMR e FMR sono uguali (Fig. 6). Il valore di FNMR e FMR quando sono uguali è detto *Equal Error Rate*

(ERR). E' ovvio che più basso è il valore di ERR più piccole sono le aree grigia e nera in Fig. 5. Per questo motivo alcuni ritengono che ERR sia un buon parametro per valutare in modo assoluto la qualità di un sistema biometrico.

In realtà le cose non sono così semplici. Prima di tutto, una popolazione reale di un sistema biometrico è di solito molto diversa da un gruppo rappresentativo del genere umano. E' un dato di fatto che esistono in molte realtà gruppi quasi esclusivamente femminili dedicati a lavori di ufficio, gruppi quasi esclusivamente maschili con lavori manuali eccetera. Per alcuni tipi di sistemi biometrici, oltre alla popolazione influisce anche l'ambiente in cui il sistema è installato. E' chiaro che le risultanti curve simili a quelle delle nostre figure possono, e spesso sono, diverse in forma e proporzioni, e se le curve si modificano anche di poco, il valore di ERR può cambiare anche molto.

C'è poi una domanda ancora più importante che dobbiamo porci. Per i nostri scopi, la scelta del valore di soglia corrispondente al punto ERR è la più appropriata? In altre parole, per cosa ci serve il sistema biometrico? Se dobbiamo garantire la massima sicurezza per l'accesso ad un sistema militare, siamo interessati ovviamente a far lavorare il sistema vicino al punto in cui FMR è zero (si veda la Fig. 7). Questo vorrà sicuramente dire che alcuni utenti veri avranno difficoltà a farsi autenticare e dovranno riprovare più volte la procedura, o addirittura usare procedure alternative manuali. Ma se la massima sicurezza è il nostro scopo, questi svantaggi devono essere sopportati. All'estremo opposto, consideriamo il caso in cui utilizziamo un sistema biometrico per identificazione (1 a N), come ad esempio per l'identificazione (Forensic) di terroristi negli aeroporti. In questo caso ci interessa ridurre il più possibile il numero di non riconoscimenti, quindi lavorare vicino al punto in cui FNMR è zero, ovviamente accettando il rischio di sbagliare persona e identificare come terrorista un onesto cittadino.

Quindi per ogni individuale applicazione di sistemi biometrici è necessario creare e valutare i parametri e le curve sulla base della reale popolazione, delle reali condizioni di lavoro e del tipo di utilizzo del sistema. Da queste considerazioni ne segue che non sempre è significativo per la nostra applicazione reale il valore di ERR indicato dai produttori e valutato spesso per un campione di

popolazione ed in condizioni di lavoro a noi ignote.

Dalla discussione fatta, risulta quindi importante la scelta del parametro di soglia. Alcuni prodotti permettono di associare al momento della registrazione di un utente, cioè della creazione del Template di riferimento, una soglia individuale. Questo permette di avere una più precisa regolazione del sistema e quindi di ridurre FNMR o FMR. Bisogna però stare molto attenti a non abusare di questa possibilità. Ad esempio nel caso di autenticazione con impronte digitali, non bisogna abbassare troppo la soglia individuale per una persona che ha delle caratteristiche fisiologiche di bassa qualità altrimenti un impostore che si spacciasse per questa persona avrebbe molte possibilità di essere autenticato. In altre parole, abbassare la soglia per una persona con caratteristiche biometriche di bassa qualità riduce sì il FNMR per questa persona, ovvero la probabilità di non essere autenticato, ma aumenta corrispondentemente l'associato FMR, e quindi la probabilità che un impostore sia autenticato al posto suo. Quando è possibile fissare delle soglie individuali, è quindi necessario individuare a priori il valore minimo e massimo accettabili per la soglia e scegliere un valore vicino al massimo per persone con caratteristiche biometriche di alta qualità, e vicino al minimo per persone con caratteristiche biometriche di bassa qualità. In ogni caso è sempre necessario predisporre delle procedure manuali sostitutive del processo biometrico.

Aspetti di Sicurezza di un Sistema Biometrico

Nelle sezioni precedenti abbiamo illustrato alcuni fattori importanti nel comprendere il funzionamento di un sistema biometrico, quali il ruolo del parametro di soglia, di FMR, FNMR e EER. Vogliamo qui approfondire alcuni altri aspetti che caratterizzano il funzionamento di un sistema biometrico che ci chiariranno meglio quale sicurezza un sistema biometrico può offrire.

Cosa è un Template

Ogni sistema biometrico si basa sulla registrazione di caratteristiche fisiologiche e/o comportamentali in un *Template*. In pratica, data una misura di solito analogica come potrebbe

essere una scansione o fotografia del viso, ne vengono estratti una serie di numeri che la caratterizzano. Ad esempio per il volto si estraggono le misure delle distanze ed angoli tra vari punti, quali gli zigomi, il naso ecc.; per le impronte digitali si estraggono le posizioni (relative) delle minuzie, ovvero le terminazioni o biforcazioni delle linee della pelle. L'insieme dei numeri estratti da una misura biometrica forma un Template. Di norma la dimensione di un Template è tra i 10 Byte e qualche KByte a seconda della tecnologia e del tipo di sistema biometrico. E' abbastanza ovvio che due misure biometriche della stessa caratteristica biometrica di una persona non sono quasi mai perfettamente identiche. Pertanto il processo di estrazione delle caratteristiche dalla misura deve essere il più possibile indipendente dalle variazioni accidentali della misura stessa.

D'altra parte non è solo un problema degli algoritmi matematici utilizzati, ma le differenze tra misure di una caratteristica biometrica della stessa persona dipendono molto dal tipo di caratteristica scelta. Non solo, a seconda della caratteristica biometrica utilizzata varia di molto *l'unicità* per individuo. Ad esempio si ritiene che la voce, la firma, la geometria della mano siano caratteristiche non uniche di un solo individuo, ovvero vi possono essere persone diverse con la stessa voce, firma ecc. Al contrario la retina, l'iride e la stessa impronta digitale sono ritenute uniche per ogni individuo.

Il punto che vogliamo sottolineare è che ogni sistema biometrico è soggetto al rischio che date due misure di persone diverse si ottengano due Template molto simili, che va confrontato con il fatto che due misure diverse della stessa persona producono due Template che possono anche essere non troppo simili. I fattori principali di questa dicotomia sono sia nella caratteristica fisiologica o comportamentale misurata, che nel processo di estrazione dei dati salienti dalla misura.

Infine, per ogni tipo di sistema biometrico, è necessario introdurre una funzione matematica che sia in grado di confrontare due Template e indicare di quanto si assomigliano. Ovviamente la qualità di un sistema biometrico dipende molto da questa funzione matematica. Si noti che nei prodotti commerciali i formati dei Template e le funzioni che li gestiscono sono spesso proprietari e non noti pubblicamente.

Sicurezza dei Template

Parlando di Template sorge subito una domanda relativa alla loro sicurezza: dato un Template è possibile ricostruire una immagine della caratteristica biometrica? Si usa pensare che la trasformazione tra una misura biometrica ed il Template non sia reversibile. Recenti risultati sulle impronte digitali [4] indicherebbero invece il contrario. E' chiaro che la sicurezza del Template, sia quello di riferimento nella base dati del sistema, che quello corrente usato per la autenticazione o identificazione, devono essere protetti. Il furto, la perdita o il rendere pubblici i Template, oltre alle ovvie problematiche di privacy, potrebbero portare alla ricostruzione della caratteristica biometrica che li ha generati, od almeno ad una caratteristica biometrica praticamente indistinguibile da quella originale, ad esempio per tentativi ripetuti (brute force) o, qualora fosse possibile, con la reversione del Template. Pertanto le basi dati dei Template e tutte le fasi del processo di autenticazione biometrica devono essere protetti con le opportune tecniche crittografiche e di sicurezza informatica.

Per aumentare la sicurezza intrinseca dei Template sono allo studio metodi per creare Template cifrati o in cui sono presenti hash dei dati. Ad esempio un gruppo di ricerca di IBM ha recentemente annunciato [5] di aver sviluppato dei nuovi metodi crittografici per rendere irreversibili ed uniche le informazioni contenute nei Template.

Resistenza alla contraffazione

Un altro punto da valutare per la sicurezza di un sistema biometrico è quanto sia facile contraffare la caratteristica biometrica. Hanno fatto scalpore sui giornali un paio di anni fa le notizie di un gruppo universitario giapponese in grado di costruire impronte digitali false usando gelatina ed altri ingredienti acquistati in supermercati. Alcune tecniche biometriche sono facile da contraffare, o meglio è molto difficile creare rilevatori in grado di distinguere una caratteristica biometrica contraffatta, ad esempio una immagine, da quella reale. Altre tecniche sono intrinsecamente molto più resistenti alla contraffazione, quale lo scanning della retina. Ad esempio, ove la rilevazione

richiede il contatto con la pelle umana, si stanno sviluppando tecniche per capire se quello che si accosta al sensore sia veramente un corpo umano vivente oppure una replica in gelatina od altro materiale inerme. Nello scegliere ed implementare un sistema biometrico, bisogna quindi anche tenere conto di quanto sia facile per un impostore costruire una copia della caratteristica fisiologica ed in questo modo ingannare il sistema.

Furto d'identità

Supponiamo che malgrado le nostre precauzioni, qualcuno riesca a rubare una copia del Template di riferimento di una persona. Indipendentemente dal fatto che il ladro sia in grado di costruire una falsa caratteristica biometrica, vi è un problema molto grave. Nel caso in cui il ladro si impadronisse del file di password, o rubasse una smartcard, una volta accortisi del furto bisogna immediatamente rimuovere le credenziali trafugate dalla base dati ed emettere nuove credenziali, nuove password, nuove smartcard eccetera. Se il furto però è quello del Template della nostra impronta digitale, possiamo si rimuovere il Template dalla base dati bloccando l'accesso, ma non possiamo cambiare le impronte digitali della persona. L'aumento del livello di sicurezza nella identificazione di una persona fornito dalla biometria, ha un inconveniente molto grave, appunto la non sostituibilità delle caratteristiche biometriche. Una volta che il furto di identità delle caratteristiche biometriche è avvenuto, non è possibile rimediare. Questo ovviamente richiede che siano prese misure molto elevate a protezione del Template.

Il furto del Template, o peggio ancora dell'immagine pre-Template, non è l'unico modo in cui si può ottenere un furto d'identità biometrica. Anzi, il modo più semplice è quello di prelevare una copia dell'immagine biometrica direttamente dalla persona, ad esempio prendendone le impronte digitali, la forma della mano, una fotografia, od una registrazione delle voce eccetera. Ovviamente le misure di sicurezza informatiche possono poco per contrastare questo rischio.

Unicità del Template

Il furto del Template può anche avere lo scopo di immettere il Template trafugato in un'altra base dati, ad esempio per sostituire un Template nella base dati di un organo di polizia. Oppure un malintenzionato può creare un Template con un sistema biometrico simile a quello dell'azienda a cui vuole accedere, e poi inserire nella base dati dell'azienda il proprio Template, senza ovviamente passare per la fase di registrazione. Si noti che anche se il formato dei Template è proprietario, questa operazione è in teoria possibile con la sola disponibilità dell'opportuno hardware. Per ridurre questo rischio si stanno studiando tecniche per rendere non solo irreversibili ma anche unici i Template in ogni base dati [5]. L'idea è di utilizzare opportune tecniche crittografiche tali da ottenere che anche usando le stesse funzioni matematiche per creare il Template dall'immagine biometrica e confrontare due Template, un Template presente in una base dati non corrisponda al Template della stessa caratteristica biometrica della stessa persona in un'altra base dati. L'idea di base è simile all'uso del *salt* nei file di password: il salt è un numero casuale che fa sì che diverse impronte della stessa password siano diverse, quindi anche se due utenti hanno la stessa password in chiaro, nel file di password compaiono due impronte diverse.

La biometria come chiave segreta

Una applicazione della biometria che sarebbe veramente molto interessante ed utile è quella dell'utilizzo di caratteristiche fisiologiche come chiave segreta. Potremmo ad esempio pensare di utilizzare un Template, che in fondo non è altro che un numero, come chiave segreta per cifrare dei dati, e distruggere il Template una volta effettuata la cifratura. L'unica possibilità per decifrare i dati dovrebbe essere quella di eseguire nuovamente la misura biometrica in modo da ottenere il Template/chiave. E' ovvio che questo non è possibile per il fatto che ogni misura biometrica genera un Template simile ma non identico al precedente. Come abbiamo ripetuto spesso in questi articoli, uno dei punti principali delle tecniche biometriche è il fatto che l'identificazione tra Template corrente e quello di riferimento è fatta sulla base della percentuale di similarità tra i due, o livello di confidenza di uguaglianza. Non è quindi possibile utilizzare direttamente la biometria per generare

chiavi segrete. Una volta fissata la soglia, un sistema biometrico 1 a 1 fornisce solo un Si od un No. Vi sono sistemi commerciali che associano la biometria alla gestione di chiavi segrete. Di solito il loro funzionamento è il seguente: sull'elaboratore vi è una base dati di chiavi segrete generate casualmente e gestite dall'applicazione biometrica, l'applicazione biometrica permette l'utilizzo delle chiavi segrete solo se la misura biometrica produce un Si, ovvero un match tra il Template corrente e quello di riferimento. Si noti che le chiavi segrete sono in realtà mantenute sull'elaboratore, e potrebbero anche essere direttamente accessibili a chi ha accesso all'elaboratore ad esempio come amministratore.

Andrea Pasquinucci
pasquinucci@ucci.it

Riferimenti Bibliografici

[1] Biometric System Lab, Università di Bologna, http://bias.csr.unibo.it/research/biolab/

[2] Anil K. Jain, Arun Ross e Salil Prabhakar, *An Introduction to Biometric Recognition*, http://biometrics.cse.msu.edu/JainRossPrabhakarCSVT_v15.pdf

[3] Per informazioni su Mifare si veda ad esempio http://www.mifare.net/ (e ISO14443 A), per Calypso si veda ad esempio http://www.calypsonet-asso.org/

[4] Arun Ross, Jidnya Shah e Anil K. Jain, *Towards Reconstructing Fingerprints From Minutiae Points*, (SPIE Proc March 2005), http://www.csee.wvu.edu/~ross/pubs/RossReconstruct_SPIE05.pdf

[5] Si veda ad esempio http://punto-informatico.it/p.asp?i=54622&r=PI, http://www.biometricgroup.com/in_the_news/08_29_05_2.html o http://www.computerworld.com.au/index.php/id;260154133;fp;16;fpid;0; si vedano anche www.site.uottawa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf, http://chris.fornax.net/biometrics.html,

http://www.ibgweb.com/reports/public/reports/templates_images.html

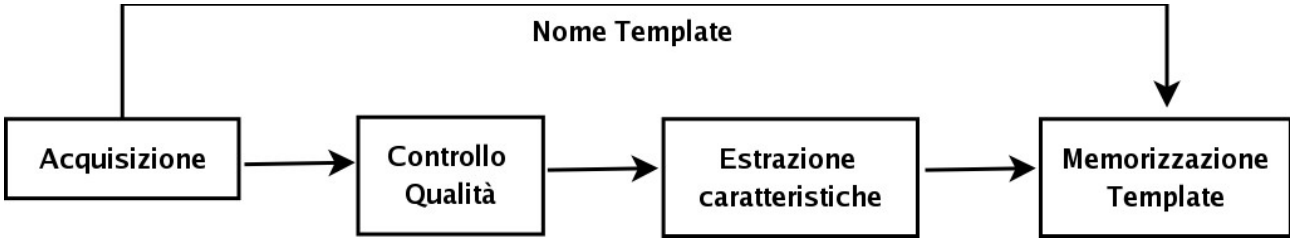

Fig. 1 Il processo di registrazione (enrolment)

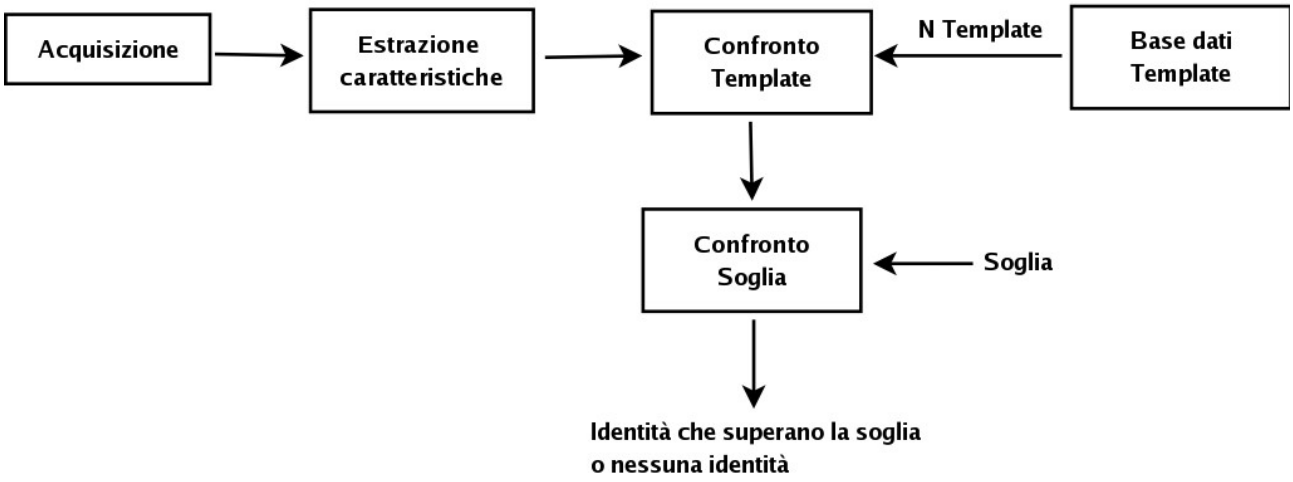

Fig. 2 Schema di processo biometrico 1 a N

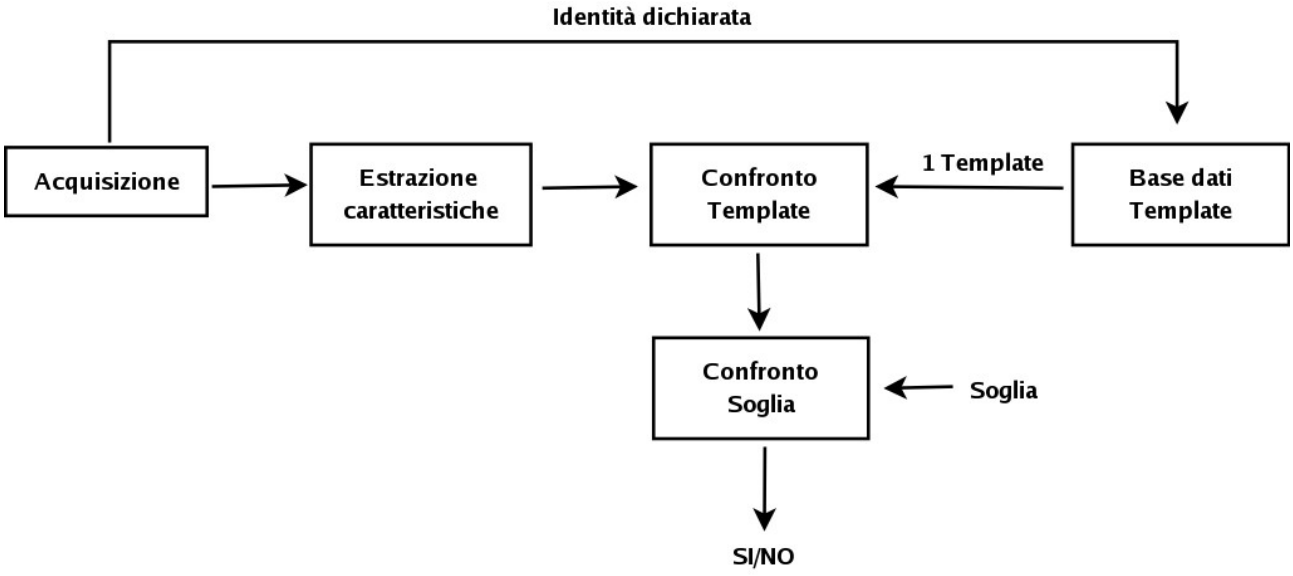

Fig. 3 Schema di processo biometrico 1 a 1

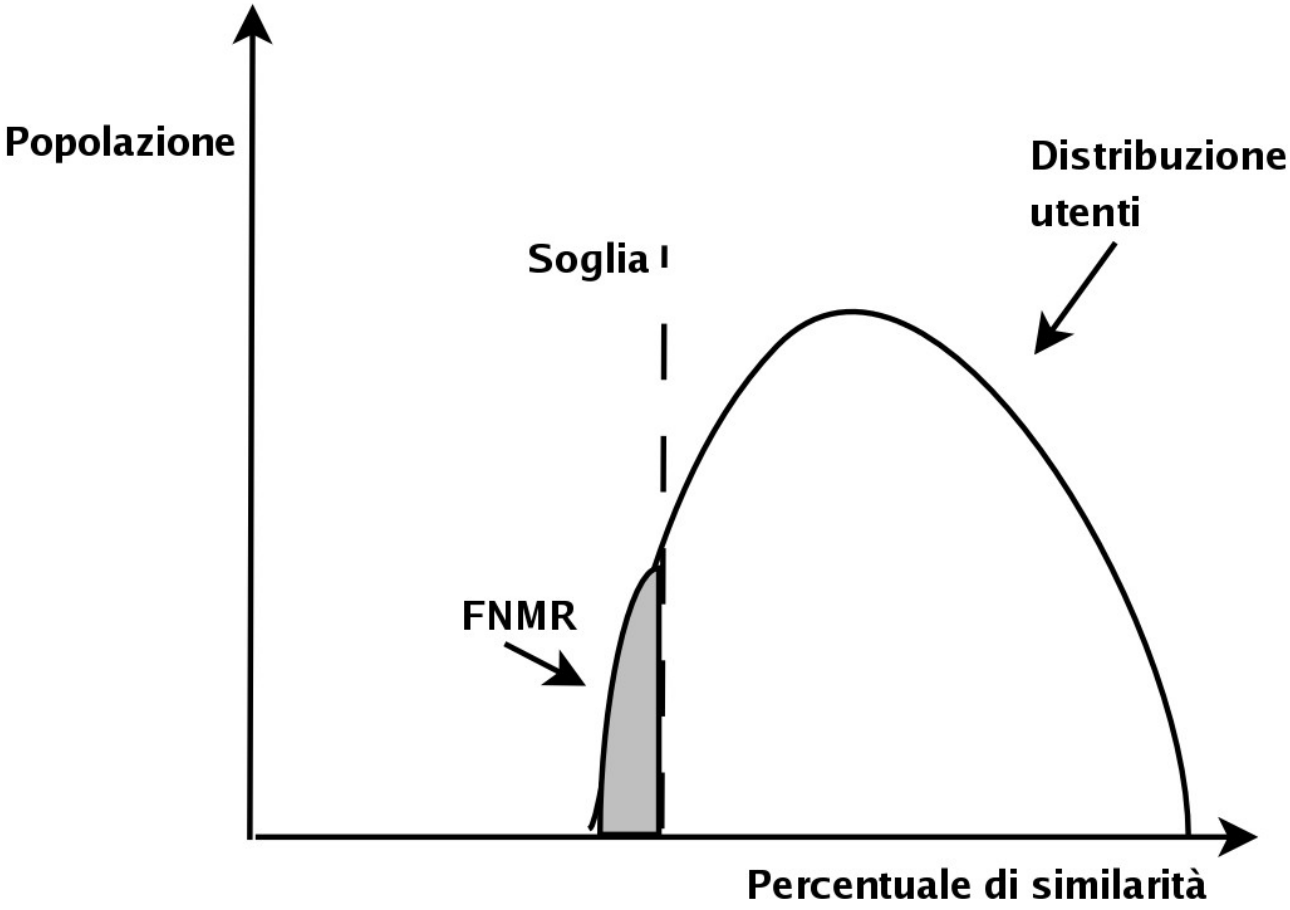

Fig. 4 Distribuzione della popolazione reale rispetto all'indice di confidenza di uguaglianza dei due Template

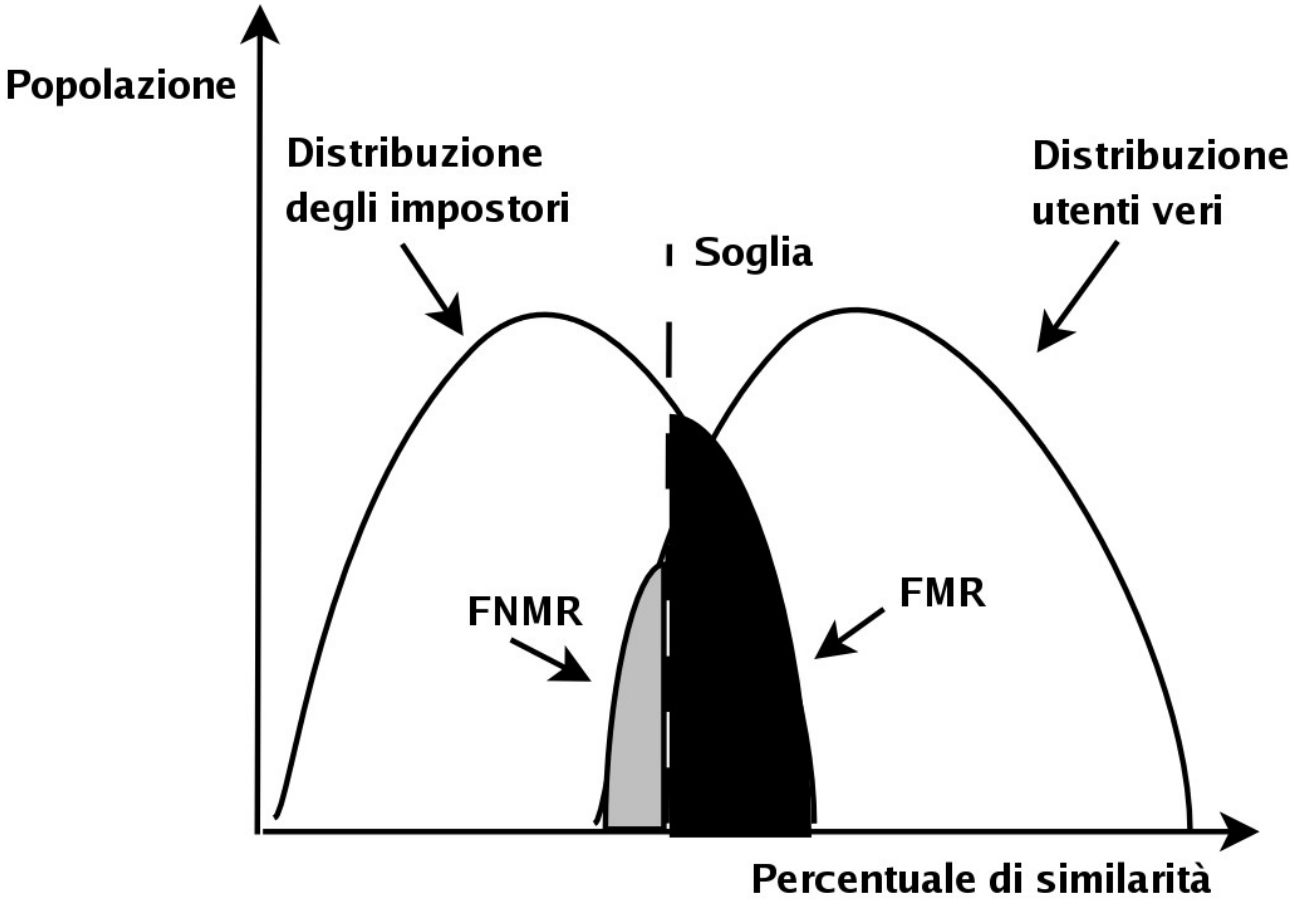

Fig. 5 Distribuzione della popolazione reale e degli impostori rispetto all'indice di confidenza di uguaglianza dei due Template

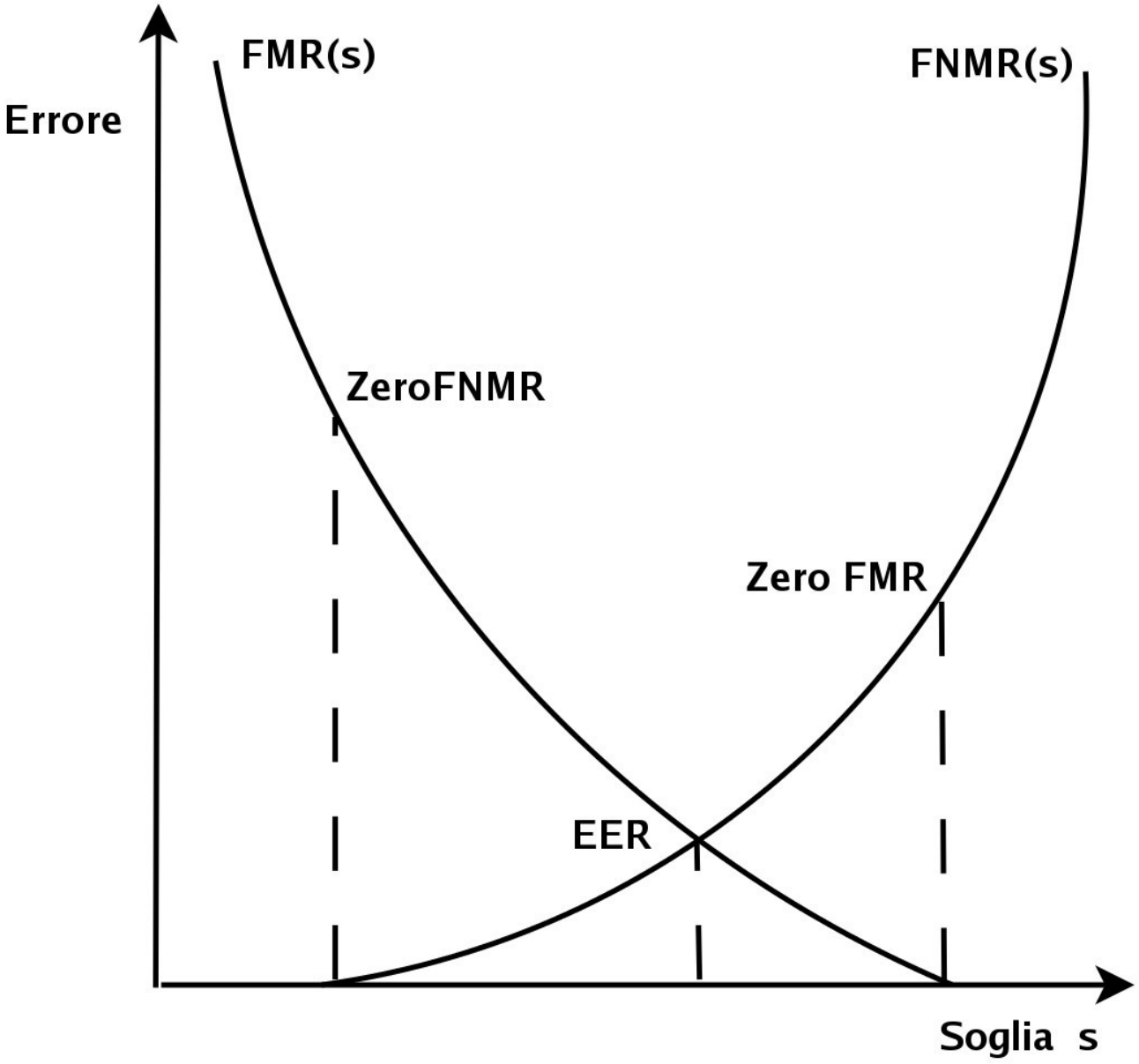

Fig. 6 Dipendenza di FMR e FNMR dal valore di soglia scelto.

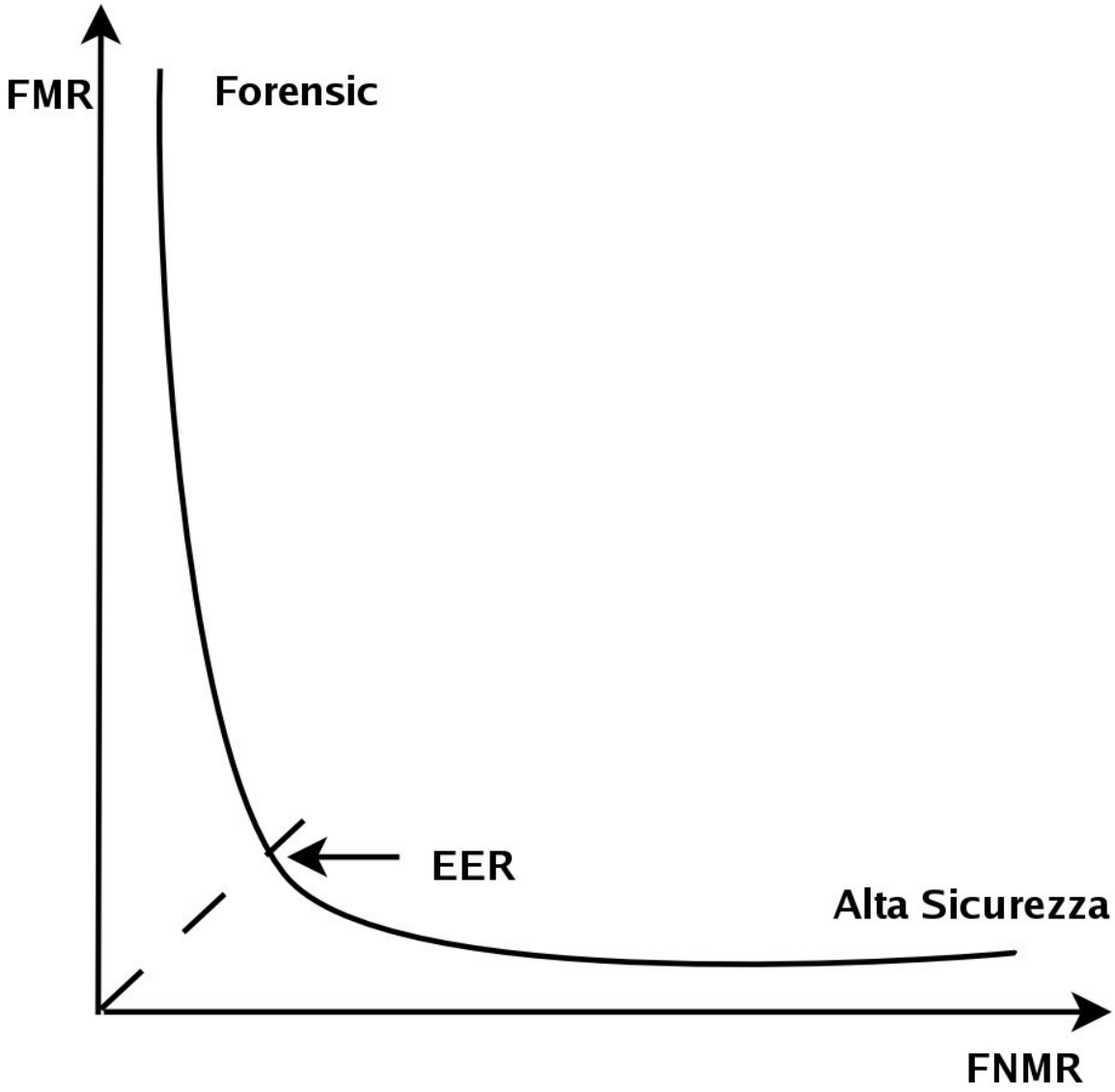

Fig. 7 Dipendenza di FMR da FNMR e loro applicazioni