Alma Mater Studiorum · Università di Bologna

CAMPUS DI CESENA
SCUOLA DI SCIENZE
Corso di Laurea in Ingegneria e Scienze Informatiche

Fusione di impronte: analisi dei problemi di sicurezza e possibili contromisure

Relatore:
Prof.
Raffaele Cappelli

Correlatore:
Dott.
Matteo Ferrara

Presentata da:
Matteo Orzes

Sessione III
Anno Accademico 2014/2015

INDICE

1 INTRODUZIONE 1
2 IL RICONOSCIMENTO DELLE IMPRONTE DIGITALI 3
2.1 I Sistemi Biometrici 3
2.2 Le Impronte Digitali 5
2.2.1 Storia 5
2.2.2 Formazione e individualità delle impronte digitali 6
2.3 Estrazione delle Caratteristiche 9
2.3.1 Orientazione delle creste 9
2.3.2 Frequenza delle creste 10
2.3.3 Enhancement 11
2.3.4 Estrazione delle Minuzie 12
2.4 Confronto di Impronte 13
2.4.1 Confronto basato sulla correlazione 15
2.4.2 Confronto basato su caratteristiche diverse dalle minuzie 15
2.4.3 Confronto basato sulle minuzie 16
3.3.1 Indici di Efficienza di un algoritmo di riconoscimento di impronte 18
3 FUSIONE DI IMPRONTE DIGITALI: PROBLEMATICHE DI SICUREZZA 21
3.1 Descrizione della possibile vulnerabilità 21
3.2 Metodo di Fusione di Impronte 24
3.2.1 Premesse 24
3.2.2 Processo di creazione di Impronte “Double-Identity” 24
3.3 Grado di successo dell’attacco 29
4 STUDIO DI POSSIBILI CONTROMISURE 31
4.1 Utilizzo di minuzie non accoppiate 31
4.1.1 Presentazione delle nuove caratteristiche 33
4.1.2 Test delle caratteristiche presentate 39
4.2 Un Sistema più robusto 43
4.3 Implementazione del sistema 49
5 RISULTATI SPERIMENTALI 53

5.1 Calcolo di massimi e minimi 53
5.2 Ricerca di combinazioni di Pesi Ottimali 53
5.3 Confronto delle Prestazioni su DB1D 57
5.4 Calcolo delle prestazioni definitive su DB1C 58
6 CONCLUSIONI 61
7 BIBLIOGRAFIA 63

1 INTRODUZIONE

Al giorno d'oggi è sempre più comune che vengano utilizzati sistemi biometrici per il riconoscimento dell'identità delle persone. Sistemi di riconoscimento automatico possono essere utilizzati per gestire l'accesso a strutture riservate o, ad esempio, per gestire i controlli alle frontiere e negli aeroporti.

L'uso di questi sistemi dovrebbe incrementare notevolmente la sicurezza della società moderna, ma è veramente così?

Documenti con una caratteristica biometrica associata, sia essa un'immagine facciale o un'impronta digitale, sono sempre più diffusi, ma sono veramente sicuri e infallibili come sembrano?

Un aeroporto che utilizza un sistema ABC (Automated Border Control) è veramente affidabile?

È possibile che un criminale ricercato riesca, con l'aiuto di un complice incensurato, a superare questi controlli?

Come possiamo rendere più sicura la nostra società? Come possiamo individuare e risolvere eventuali falle nella sicurezza?

In questa tesi si esamineranno alcune possibili vulnerabilità dei sistemi di riconoscimento di impronte digitali e si tenterà di migliorare la loro sicurezza nei confronti di una tipologia specifica di attacco che utilizza impronte digitali "artificiali" per permettere ad un criminale di utilizzare il documento di un complice. È stata infatti recentemente dimostrata la possibilità di inserire in un documento elettronico caratteristiche biometriche che lo rendono utilizzabile da due diverse persone. Questa problematica di sicurezza è alla base dell'attacco che verrà analizzato in questa tesi e per il quale si cercheranno contromisure efficaci.

Nel Capitolo 2 si introdurranno i concetti fondamentali del processo di riconoscimento di impronte digitali; successivamente, nel Capitolo 3 verranno esaminate le vulnerabilità del sistema e le problematiche di sicurezza analizzando il metodo di attacco e gli strumenti utilizzati per metterlo in atto. Nel Capitolo 4 si studieranno delle contromisure per rendere il sistema più sicuro e affidabile, analizzando prima un articolo scientifico di recente pubblicazione e, in seguito, ricercando soluzioni nuove ed originali. Infine, nel Capitolo 5, verranno riportati e discussi i risultati ottenuti.

2 IL RICONOSCIMENTO DELLE IMPRONTE DIGITALI

2.1 I Sistemi Biometrici

Nella società moderna, fortemente connessa e mobile, per stabilire l'identità di una persona non è più sufficiente l'uso di password e documenti: questi ultimi possono essere smarriti, mentre le password potrebbero essere scoperte da altre persone, generando un possibile caso di furto di identità.

Per risolvere i problemi sopra citati si può ricorrere all'uso di identificatori che non possano essere condivisi e\o scambiati fra più persone, dato che rappresentano intrinsecamente ogni singolo individuo: un sistema che fa uso di tali identificatori è definito 'Sistema Biometrico'.

Un sistema di riconoscimento biometrico è un sistema informatico che ha la funzionalità e lo scopo di identificare una persona basandosi su caratteristiche biologiche e/o comportamentali. Alcuni esempi sono le impronte digitali, l'iride e il riconoscimento facciale.

Un fattore molto importante per lo sviluppo di un sistema biometrico è scegliere come un individuo verrà riconosciuto. A seconda del contesto d'uso il sistema potrà operare in due diverse modalità: "Verifica" o "Identificazione".

Un sistema di "Verifica" autentica l'identità dell'individuo confrontando la caratteristica biometrica appena estratta con un template biometrico di riferimento precedentemente salvato nel sistema. Effettua, quindi, un confronto uno ad uno per confermare se un determinato individuo è effettivamente chi afferma di essere.

Un sistema di "Identificazione", invece, effettua un confronto uno a molti fra la caratteristica biometrica appena estratta e tutti i template presenti nel database del sistema, avendo come scopo quello di identificare l'identità dell'individuo dal quale è stata estratta la caratteristica. Questo tipo di sistema stabilisce l'identità di un individuo senza che questi debba effettivamente dichiararne alcuna.

I processi principali di un sistema biometrico sono tre: Registrazione, Verifica e Identificazione. Questi tre processi fanno uso dei seguenti moduli: Cattura, Estrazione delle Caratteristiche, Creazione del Template, Pre-selezione, Confronto e Archiviazione dei dati.

La registrazione è il processo responsabile dell'inserimento degli individui all'interno del sistema biometrico. La caratteristica dell'individuo viene prima estratta mediante uno scanner per farne un campione, viene effettuato quindi un controllo di qualità per accertarsi che sia possibile procedere; in seguito, tramite il modulo per l'estrazione delle caratteristiche, verrà prodotto un set di features il quale verrà utilizzato dal modulo di creazione del template per creare il modello campione relativo all'individuo da registrare. Il processo di verifica deve confermare la dichiarazione di una specifica identità da parte di un utente. Durante questa fase, l'individuo fornirà al sistema un identificatore (Pin/Username) per dichiarare una specifica identità; lo scanner biometrico catturerà la caratteristica dell'utente che verrà processata per estrarne un set di features che sarà fornito al Matcher per essere confrontato con il template campione dell'identità da confermare.

Il processo di identificazione confronta il set di caratteristiche dell'individuo con quello di ogni soggetto presente nel database fornendo una lista di possibili identità relative alla persona dalla quale si è estratta la caratteristica biometrica. [1]

2.2 Le Impronte Digitali

Per utilizzare un tratto anatomico o comportamentale come identificatore biometrico è necessario che sia un carattere distintivo e soddisfi i seguenti requisiti: Universalità, Permanenza ed Esigibilità. L'identificatore biometrico per eccellenza sono le impronte digitali.

2.2.1 Storia

Alcuni reperti archeologici evidenziano che i dermatoglifi e, in particolare, le impronte erano utilizzati in passato come forma di identificazione personale.

1665 Marcello Malpighi pubblica il '*De externo tactus organo anatomica observatio',* uno dei primi documenti scientifici riguardanti le creste cutanee.

1823 John Evangelist Purkinje presenta uno schema di classificazione delle impronte secondo il quale queste ultime si possono dividere in nove categorie in base alla struttura generale delle creste.

1856 William Herschel, nel suo lavoro di magistrato in India, utilizzò le impronte nei contratti degli abitanti del luogo; inoltre Herschel si convinse che l'impronta potesse confermare o negare l'identità, grazie alle caratteristiche di unicità dell'impronta e di persistenza nel corso della vita.

1864 Il botanico inglese Nehemian Grew pubblica un documento scientifico che riporta i suoi studi sulla struttura delle creste delle valli e dei pori; siamo di fronte al primo studio scientifico approfondito delle impronte.

1880 Lo scozzese Henry Faulds suggerì l'individualità delle impronte digitali e un loro possibile utilizzo nell'identificazione dei criminali.

1888 Sir Francis Galton introduce il concetto di minuzie per il confronto di impronte.

1899 Edward Henry realizza un sistema di classificazione delle impronte in grado di semplificare molto il processo di identificazione.

Nei **primi anni del ventesimo secolo** le impronte digitali vengono finalmente accettate come metodo di identificazione dell'individuo e trovano applicazione in campo forense per l'identificazione dei criminali.

1960 I database di impronte divengono troppo estesi per effettuare una identificazione manuale, nasce quindi dall'azione congiunta dell'FBI, del dipartimento di polizia di Parigi e dell'"Home Office" Inglese, il primo sistema di identificazione automatica delle impronte digitali.

2.2.2 Formazione e individualità delle impronte digitali

Le impronte digitali sono completamente formate al settimo mese di sviluppo del feto. La struttura delle creste non cambia durante la vita dell'individuo se non per alterazioni quali ferite o abrasioni nella zona interessata.
Questo fattore rende le impronte digitali un ottimo identificatore biometrico.

E' però necessario ricordare che l'assoluta unicità delle impronte digitali non è un fatto dimostrato scientificamente, ma frutto di un'osservazione empirica.

Un' Impronta è formata da una trama di creste (**ridge**) e valli (**valleys**) che disegnano un pattern complesso chiamato '**ridge pattern**', un esempio viene mostrato in Figura 1.

Figura 1: Ridge Pattern

A seconda del livello di dettaglio con il quale analizziamo un'impronta potremo notare differenti caratteristiche, i livelli principali sono tre:

Livello 1, (noto anche come livello globale)

In alcune regioni le creste, che solitamente si dispongono parallelamente, assumono forme particolari. Queste regioni, chiamate singolarità o punti singolari, possono essere classificate in tre tipi: Loop, Delta/Arch e Whorl. Questi tipi di singolarità possono essere riconosciuti dalla loro forma, simile a U, Δ e O. Le spirali/whorl possono essere descritte come due loop uno in fronte all'altro e quindi potrebbero non essere intese come una tipologia di singolarità a se stante. Il centro del loop più a nord è definito punto di Core. Per impronte che non contengono loop o spirali diventa difficile individuare il core, in questi casi viene definito come il punto di massima curvatura delle creste.

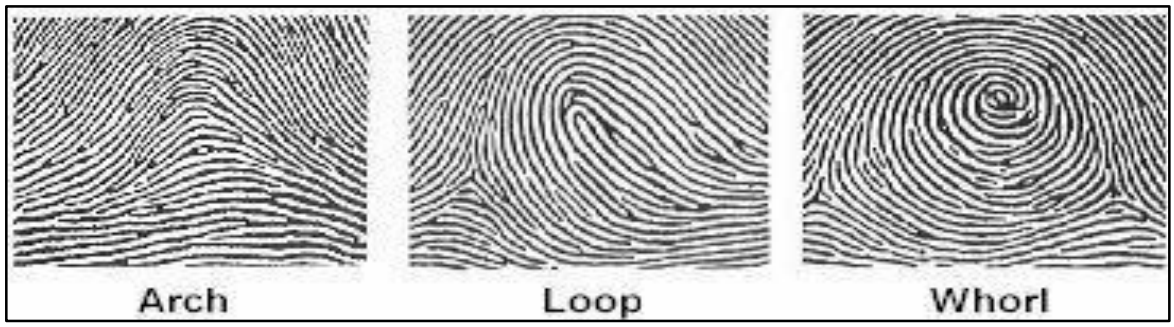


Figura 2: Singolarità primo livello

Livello 2, (anche detto livello locale)

In questo livello si possono individuare le varie caratteristiche delle creste. Le due più importanti ovvero la "biforcazione" (*ridge bifurcation*) e la "terminazione" (*ridge ending*) prendono il nome di minuzie. Le minuzie sono delle discontinuità nella struttura delle creste che furono classificate per la prima volta da Sir Francis Galton: esse non cambiano durante la vita dell'uomo mantenendosi sempre costanti. Si parla di terminazione della cresta quando questa si interrompe bruscamente, si tratta invece di biforcazione quando essa diverge in due rami figli. Esistono vari tipi di minuzie oltre alle terminazioni e biforcazioni ma il modello proposto dall' FBI utilizza al momento le due categorie sopracitate.

Livello 3,

A questo livello si possono osservare dettagli come la forma, la curvatura e la larghezza delle creste, così come altri dettagli quali creste incipienti, abrasioni e pori.
La posizione dei pori è considerata avere un alto valore distintivo e quindi caratterizzante. Ogni cresta è infatti contraddistinta da pori che si estendono per tutta la sua lunghezza, in quantità sufficiente i pori possono essere utilizzati per identificare un individuo.
Le caratteristiche di questo livello richiedono scanner di impronte ad alta risoluzione (1,000 dpi) per essere individuate e quindi non sono ancora molto sfruttate sebbene forniscano informazioni molto importanti. [1]

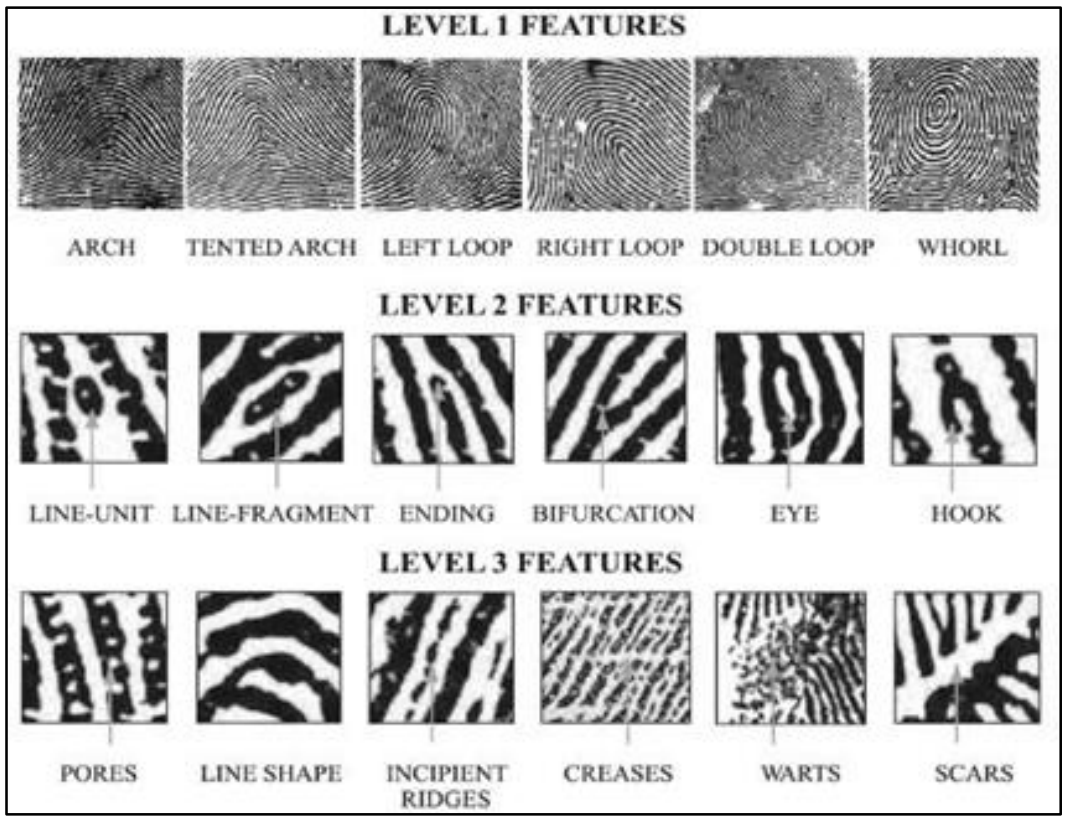


Figura 3: Esempi di Caratteristiche per ciascun livello.

2.3 Estrazione delle Caratteristiche

Le minuzie, ovvero le caratteristiche individuate al livello locale, non mutano durante la vita di un individuo e quindi possono essere utilizzate come tratti distintivi nel processo di confronto di due impronte.

2.3.1 Orientazione delle creste

Per poter estrarre correttamente le minuzie è prima necessario stabilire le orientazioni locali delle creste in questione. L'orientazione locale delle creste al pixel$[x, y]$ viene definita come l'angolo $\Theta[x, y]$ che le creste, in un intorno del pixel$[x, y]$, formano con l'asse orizzontale. Invece di calcolare l'orientazione locale per ogni pixel, molti processi di estrazione delle caratteristiche, effettuano una stima in posizioni precise riducendo i costi e permettendo di ottenere l'orientazione sugli altri pixel tramite interpolazione.

L'immagine delle orientazioni di un'impronta, chiamata anche immagine direzionale, è una matrice **D** in cui ogni elemento Θ_{ij} corrispondente al nodo $[i, j]$ di una matrice quadrata posizionata sul pixel $[x_i, y_j]$. Questa immagine mostra l'orientazione media delle creste in un intorno di $[x_i, y_j]$.

Un valore r_{ij} è associato ad ogni elemento per indicare l'affidabilità dell'orientazione corrispondente: questo valore sarà basso per regioni dell'immagine di scarsa qualità e invece avrà un valore elevato per regioni di alta qualità.

L'approccio più semplice e naturale per l'estrazione delle orientazioni locali è basato sul calcolo del gradiente dell'immagine direzionale. Il gradiente $\nabla(x, y)$ nel punto $[x, y]$ dell'immagine **I** è un vettore bidimensionale $[\nabla_x(x, y), \nabla_y(x, y)]$ dove ∇_x e ∇_y sono rispettivamente le derivate parziali di I in $[x, y]$ rispetto alle direzioni x e y.

L'angolo di fase del gradiente indica la direzione del massimo cambiamento d'intensità dei pixel; la direzione di un possibile bordo che attraversa la regione che ha centro in $[x, y]$ è perpendicolare all'angolo di fase del gradiente in $[x, y]$.

Questo metodo presenta però alcuni svantaggi:

- Non linearità e discontinuità per angoli vicini a 90 gradi.
- Il valore di una singola orientazione è troppo sensibile al rumore per essere considerato affidabile, d'altra parte nemmeno la media di tali valori può essere utilizzata a causa della circolarità degli angoli.
- Il concetto di Orientazione media non è ben definito e univoco. L'orientazione è compresa fra 0° e 180° mentre l'angolo fra 0° e 360°.
  ("qual è la media di due orientazioni ortogonali 0 ° e 90°? 45° oppure 135°?")

Una soluzione al problema della circolarità degli angoli venne proposta da Kass e Witkin nel 1987, l'idea consiste nel raddoppiare gli angoli così che ogni singola orientazione sia codificata dal vettore $d = [r \cdot \cos(2\theta)\,;\, r \cdot \sin(2\theta)]$. [1]

2.3.2 Frequenza delle creste

Si definisce *'frequenza delle creste'* nel punto $[x, y]$ il numero di creste per unità di lunghezza lungo un ipotetico segmento centrato nel punto $[x, y]$ perpendicolare all'orientazione locale in quel medesimo punto.

Un immagine delle frequenze **F**, analogamente all'immagine direzionale vista precedentemente, può essere definita effettuando una stima della frequenze in posizioni discrete e inserendo tali dati in una matrice.

Questa grandezza non solo varia fra impronte differenti ma anche fra regioni diverse della stessa impronta.

Una soluzione di base per il calcolo della frequenze fu proposta nel 1998 da Hong, Wan and Jain e consiste nel contare il numero medio di pixel fra due picchi consecutivi dei livelli di grigio lungo la direzione perpendicolare all'orientazione locale nel punto in esame.

2.3.3 Enhancement

Le prestazioni di algoritmi per l'estrazione delle minuzie e riconoscimento delle impronte digitali sono molto influenzate dalla qualità dell'immagine.

Un immagine di scarsa qualità presenta in genere varie degradazioni quali ad esempio una non continuità delle creste, errori nella separazione di creste parallele e segni dovuti a ferite, tagli o abrasioni. Identificare le creste e, di conseguenza, le minuzie in immagini di questo tipo risulta piuttosto difficile.

Generalmente nell'immagine di un impronta saranno presenti aree differenti che potranno essere divise in tre principali categorie:

- *Regioni Ben Definite*, le creste si possono distinguere chiaramente fra loro.
- *Regioni Recuperabili*, le creste presentano alcuni salti, pieghe e sbavature ma le regioni vicine forniscono informazioni sufficienti sulla struttura della regione in esame.
- *Regioni Irrecuperabili,* le creste sono rovinate da una grande presenza di rumore e distorsioni e le regioni vicine non ne permettono una ricostruzione

Gli algoritmi di Enhancement sono, pertanto, volti a migliorare la qualità dell'impronta per favorire un'estrazione delle caratteristiche che produca risultati maggiormente affidabili.

L'input per un algoritmo di enhancement è solitamente un'immagine a livelli di grigio, mentre l'output può essere un'immagine a livelli di grigio o un'immagine binaria. Operazioni come l'aumento del contrasto, la modifica dell'istogramma o la normalizzazione possono risultare utili per una prima fase di pre-processing utilizzando immagini di impronte. [1]

Altri approcci sono l'Enhancement pixel-wise e il filtraggio contestuale i quali però non verranno trattati nello specifico in questo documento.

2.3.4 Estrazione delle Minuzie

Molti sistemi automatici per il confronto di impronte si basano sull'accoppiamento delle minuzie, quindi risulta di fondamentale importanza che l'operazione di estrazione di queste ultime sia eseguita in maniera corretta.

Molti metodi richiedono che l'immagine venga prima binarizzata; a loro volta molti processi di binarizzazione traggono beneficio dalla previa esecuzione di un processo di enhancement.

L'approccio più semplice di binarizzazione procede stabilendo una soglia globale e impostando il valore dei vari pixel con intensità originale inferiore alla soglia a zero, i restanti ad uno.

Dopo essere state binarizzate le immagini vengono spesso sottoposte ad un processo di thinning che permette di ridurre lo spessore delle creste ad un singolo pixel.

Per la localizzazione delle minuzie nello scheletro ottenuto dal processo di thinning si effettua una scansione dell'immagine per localizzare i pixel corrispondenti alle minuzie.

Si procede poi analizzando il Crossing Number delle varie minuzie ottenute al passo precedente.

Il Crossing Number $Cn(p)$ di un pixel p in un'immagine binaria è definito come la metà della sommatoria delle differenze tra coppie di pixel adiacenti nell'intorno unitario di p:

$$Cn(p) = \frac{1}{2} \sum_{i=1\ldots8} |val(\ p_{i\ mod\ 8}) - val(p_{i-1})|$$

Un pixel p con $val(p) = 1$ è:

- una terminazione se $Cn(p) = 1$
- un punto interno a una cresta se $Cn(p) = 2$
- una biforcazione se $Cn(p) = 3$
- una minuzia più complessa se $Cn(p) > 3$

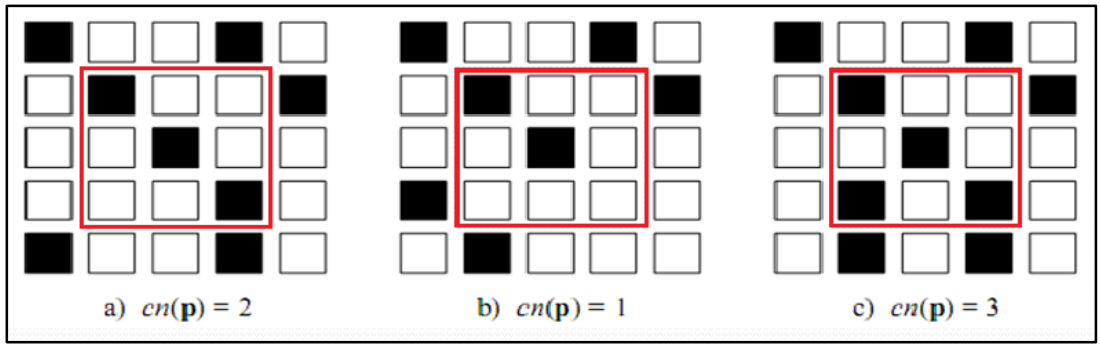


Figura 4: Metodo Crossing Number

2.4 Confronto di Impronte

Un algoritmo di confronto fra impronte generalmente ha come risultato uno score di similarità compreso fra 0 e 1 o una decisione binaria successo/insuccesso. Sono pochi gli algoritmi che operano direttamente sulle immagini in scala di grigio, la maggior parte agisce infatti su una rappresentazione intermedia dell'impronta ottenuta generalmente estraendo dall'impronta le caratteristiche (minuzie). Si definisce quindi 'template' **T** la rappresentazione dell'impronta che è stata ottenuta durante la fase di registrazione e 'input' **I** la rappresentazione dell'impronta con cui deve essere confrontata.

Il confronto di impronte è un'operazione molto problematica soprattutto a causa della grande differenza che si può notare anche fra diverse impronte dello stesso dito.

Le principali cause di queste differenze in un confronto omologo (impronte appartenenti allo stesso dito) sono le seguenti:

- **Spostamento**: lo stesso dito potrebbe essere posizionato in locazioni diverse del sensore durante l'acquisizione e quindi generare una traslazione globale dell'impronta
- **Rotazione**: lo stesso dito potrebbe essere ruotato ad angoli diversi durante acquisizioni differenti generando quindi una rotazione nell'impronta.
- **Sovrapposizione Parziale**: lo spostamento e la rotazione spesso portano parte dell'impronta ad essere al di fuori della linea di vista del sensore.

- **Distorsione non lineare**: a causa dell'elasticità della pelle in diverse acquisizioni dello stesso dito si genereranno distorsioni non lineari dovute alla modalità di posizionamento del dito interessato sul sensore. Per evitare tali problemi il dito dovrebbe essere appoggiato perpendicolarmente al sensore e non dovrebbe essere applicata alcuna forza di torsione o trazione mentre l'impronta viene catturata dal sensore.
- **Pressione e Condizioni della pelle**: per ottenere una rappresentazione accurata delle creste è necessario che queste siano in contatto uniforme con la superficie del sensore, tuttavia, fattori quali la pressione esercitata dal dito sul sensore, secchezza della pelle, sporco, sudore e umidità generano un contatto non uniforme.
- **Rumore**: dovuto per esempio a residui di materiali sul sensore o sul dito del quale si vuole ottenere l'impronta.
- **Errori nell'estrazione delle caratteristiche**: gli algoritmi di estrazione delle caratteristiche introducono spesso errori di misurazione. Vari errori potrebbero essere commessi in una qualunque delle fasi di estrazione delle caratteristiche quali stima dell'orientazione e della frequenza, individuazione delle singolarità, segmentazione dell'impronta dallo sfondo.

Oltre a notare differenze fra impronte dello stesso dito è anche possibile notare somiglianze fra impronte di dita differenti che quindi danno luogo and un confronto eterologo. Queste somiglianze sono soprattutto a livello di struttura globale ed è tuttavia difficile che un gran numero di minuzie provenienti da impronte differenti venga accoppiato. [1]

I diversi approcci al problema del confronto fra impronte possono essere raggruppati in tre differenti gruppi:

- **Confronto basato sulla correlazione**;
- **Confronto basato sulle minuzie**;
- **Confronto basato su altre caratteristiche**.

2.4.1 Confronto basato sulla correlazione

Nel confronto basato sulla correlazione due impronte sono sovrapposte e i valori di correlazione fra diversi pixel sono calcolati per diversi allineamenti, spostamenti e rotazioni.

Una misura intuitiva della diversità di due immagini è la *"Sum of Squared Differences"* (SSD) calcolata fra le intensità dei pixel corrispondenti nelle due immagini.

$$SSD(T,I) = \left||T-I|\right|^2 = (T-I)^T(T-I) = \left||T|\right|^2 + \left||I|\right|^2 - 2T^TI$$

Il posizionamento e l'angolazione del dito non sono noti, quindi è necessario calcolare la correlazione per ogni possibile sovrapposizione, questo porta ad un elevato costo computazionale e ad una bassa tolleranza in casi di distorsione dell'impronta. [1]

2.4.2 Confronto basato su caratteristiche diverse dalle minuzie

E' possibile ricercare altre caratteristiche distintive oltre alle minuzie per effettuare un confronto fra impronte, queste caratteristiche aggiuntive possono essere utilizzate insieme alle minuzie per creare un sistema più robusto e accurato. Spesso estrarre le minuzie da immagini di scarsa qualità risulta difficile è quindi necessario ricercare differenti caratteristiche per confrontare queste immagini. Nel caso di sensori molto piccoli caratteristiche differenti dalle minuzie possono fornire prestazioni migliori. [1]

Le Caratteristiche più utilizzate in queste situazioni sono:

- Grandezza dell'impronta e forma del contorno esterno.
- Numero, tipo e posizione delle singolarità.
- Informazioni relative alla texture locale e globale.
- Valori geometrici e relazioni spaziali delle creste.
- Caratteristiche di livello 3, ad esempio i pori della pelle.

2.4.3 Confronto basato sulle minuzie

Il confronto basato sulle minuzie è l'approccio più noto e utilizzato per il confronto di impronte. A differenza del caso precedente, dove la rappresentazione dell'impronta era l'immagine stessa, nell'approccio basato sulle minuzie le impronte sono rappresentate da vettori di caratteristiche i cui elementi sono le minuzie rilevate nelle impronte in esame.

Ogni minuzia è generalmente caratterizzata dalla sua posizione nell'impronta, dall' orientazione, dalla tipologia e da un indicatore della qualità dell'impronta nella zona circostante.

La gran parte degli algoritmi utilizza la posizione e l'orientazione e quindi ogni minuzia risulta essere una tripletta di valori $m = [x, y, \Theta]$; il Template e l'Input possono essere rappresentati come segue:

$$T = \{m_1, m_2, \dots, m_m\}\ m_i = [x_i, y_i, \Theta_i]\ \ i = 1, \dots, m$$

$$I = \{m'_1, m'_2, \dots, m'_n\}\ m'_j = \left[x'_j, y'_j, \Theta'_j\right]\ \ j = 1, \dots, n$$

Due minuzie m_i, m_j sono considerate accoppiate se la distanza spaziale e la differenza d'orientazione non superano determinate soglie di tolleranza.

Le soglie di tolleranza sono necessarie per compensare i vari piccoli errori introdotti durante le fasi di acquisizione delle impronte e di estrazione delle caratteristiche. Per massimizzare il numero di minuzie accoppiate è necessario allineare prima le due impronte.

Una volta effettuato il confronto per ottenere un indicatore della somiglianza fra le due impronte, una soluzione consiste nel normalizzare il numero delle minuzie accoppiate rispetto al numero medio di minuzie in T ed I. [1]

$$Score = \frac{k}{\frac{n+m}{2}}$$

Per aumentare l'affidabilità di questo punteggio si può ricorrere all'indicatore di qualità di ogni minuzia in modo da dare peso maggiore alle minuzie più affidabili, penalizzando quelle con bassa qualità.

Implementando un allineamento delle impronte prima della fase di accoppiamento delle minuzie si otterranno certamente algoritmi più robusti a costo di una decisamente maggiore complessità computazionale. Mantenere template pre-allineati nel database e allineare le immagini di input prima del confronto potrebbe consistere in una soluzione valida per rendere più veloci ed efficienti i confronti di identificazione (uno a molti).

Effettuare l'allineamento delle impronte è decisamente un'operazione computazionalmente costosa, alcuni algoritmi procedono quindi accoppiando le minuzie localmente.

Effettuare un accoppiamento locale di minuzie consiste nel confrontare due impronte sulla base delle strutture locali di minuzie. Queste strutture locali si basano su attributi che sono invarianti per spostamento, rotazione e altre trasformazioni globali, sono quindi ottime per effettuare un confronto senza alcun tipo di pre-allineamento.

Tuttavia confrontare impronte basandosi solamente sulla disposizione locale delle minuzie porta ad una perdita di informazioni relative alle relazioni spaziali globali che risultano essere particolarmente distintive. L'approccio locale fornisce quindi semplicità, bassa complessità computazionale ed un alta tolleranza alle distorsioni andando però a perdere l'elevato potere discriminante tipico dell'approccio globale.

I benefici di entrambi gli approcci possono essere ottenuti implementando strategie ibride che attuano un accoppiamento delle strutture locali seguito da una fase di consolidamento.

L'accoppiamento delle strutture locali permette di determinare coppie di minuzie a livello locale e derivare da queste varie possibilità di allineamento fra T ed I. La fase di consolidamento è volta a verificare se il grado di somiglianza riscontrato a livello locale si mantiene a livello globale. In caso di impronte particolarmente differenti, la fase di confronto locale può già decretare un rifiuto nell'accoppiamento delle due immagini.

3.3.1 Indici di Efficienza di un algoritmo di riconoscimento di impronte

Nel valutare l'efficienza di un algoritmo di *fingerprint recognition* si esaminano diversi valori, [3] i più utilizzati sono i seguenti:

- **FMR** (*False Matching Rate*)
- **FNMR** (*False Non Matching Rate*)
- **EER** (*Equal Error Rate*)
- **ZeroFMR** (*Zero False Matching Rate*)
- **ZeroFNMR** (*Zero False Non Matching Rate*)

Si definiscono "Genuine" i confronti fra impronte provenienti dallo stesso dito e "Impostor" i confronti fra quelle ottenute da dita differenti.

Quando un sistema biometrico effettua un confronto fra due impronte può commettere due tipologie di errore: False Match (FM) o False Non Match (FNM). Si tratta di False Match quando l'algoritmo classifica come genuine un confronto impostor, viceversa, si parla di False Non Match, se l'algoritmo riconosce come impostor un legittimo confronto genuine. [3]
Per ogni punteggio di somiglianza **'i'** compreso fra 0 e 1 vengono calcolati i seguenti valori:

- **FMR(i)**: rapporto fra il numero di confronti impostor con punteggio di somiglianza più alto di **'i'** ed il numero totale di confronti impostor effettuati.
- **FNMR(i)**: rapporto fra il numero di confronti genuine con punteggio di somiglianza inferiore ad **'i'** ed il numero totale di confronti genuine.

L'**EER** è il valore dove le funzioni Fmr(i) e Fnmr(i) hanno lo stesso valore.

Un passo molto importante, nello sviluppo di un algoritmo di confronto di impronte, è la scelta della **soglia decisionale** che verrà utilizzata per stabilire, in base al punteggio di somiglianza, se il confronto in esame è genuine o impostor.

Nel caso in cui si scegliesse come soglia l'Eer, i valori Fmr e Fnmr sarebbero coincidenti.

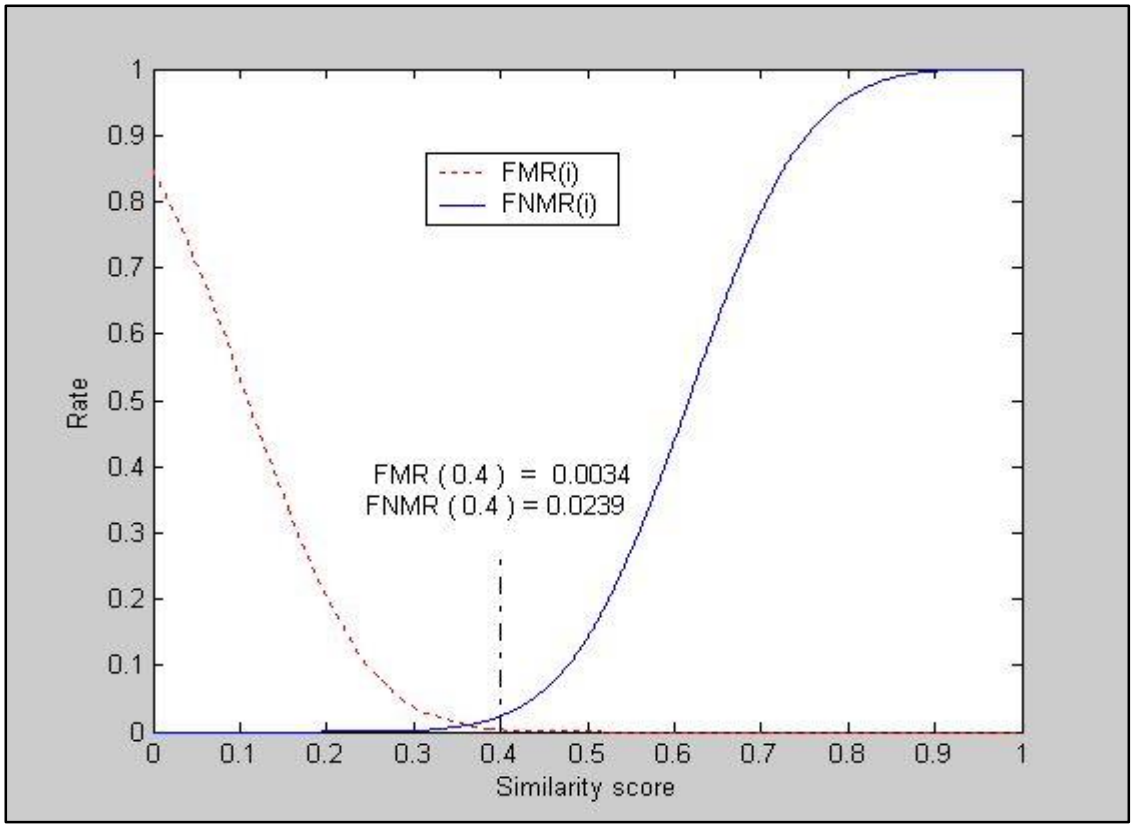


Figura 5: Grafico Fmr e Fnmr

Lo scenario precedente ci mostra che il comportamento di un algoritmo può essere descritto da coppie di valori di Fmr e Fnmr. Sono state definite alcune coppie che vengono spesso usate per descrivere l'accuratezza di un algoritmo.

FMR10, **FMR100**, **FMR1000** e **ZeroFMR** sono i valori di Fmr quando Fnmr è rispettivamente: 0.1, 0.01, 0.001 e 0.

In altre parole queste metriche descrivono che valori di Fnmr aspettarsi quando Fmr è fissato rispettivamente a 10%, 1%, 0.1% e 0%. [3]

3 FUSIONE DI IMPRONTE DIGITALI: PROBLEMATICHE DI SICUREZZA

In questo capitolo si procederà con l'analisi del metodo di fusione di impronte e del conseguente possibile attacco ad un sistema biometrico analizzandone le vulnerabilità e, infine, il grado di successo dell'attacco.

3.1 Descrizione della possibile vulnerabilità

Oggi il riconoscimento di impronte digitali è considerato affidabile e, se un'impronta è acquisita nelle giuste condizioni, è possibile ottenere un ottimo grado di accuratezza. Tuttavia, in alcuni casi, alterazioni intenzionali e non dell'impronta possono influenzare particolarmente le performance del riconoscimento.

Non è raro che due impronte provenienti da individui differenti presentino caratteristiche simili, soprattutto a livello di struttura globale. Alcuni esempi di caratteristiche che, talvolta, vengono valutate 'simili' sebbene provengano da impronte di dita diverse, sono i seguenti:

- Posizione delle Singolarità
- Orientazione locale delle creste
- Frequenza locale delle creste

Alcune alterazioni involontarie dell'immagine, ad esempio deformazioni dell'impronta durante l'acquisizione dovute ad un posizionamento non ottimale sul sensore, possono portare ad un aumento del False Non Matching Rate (FNMR), ovvero la percentuale di utenti autorizzati che vengono erroneamente rifiutati dal sistema, nel caso specifico delle impronte digitali, la percentuale che due impronte provenienti dallo stesso dito vengano giudicate come provenienti da dita differenti.

Figura 6: Impronte che presentano somiglianze globali.

Se è possibile che in natura esistano impronte provenienti da dita diverse che presentano somiglianze a livello globale ed è altresì possibile che alterazioni involontarie delle immagini possano portare un sistema biometrico a non riconoscere un confronto di impronte omologo, dobbiamo aspettarci che sia possibile, mediante alterazioni **intenzionali**, ingannare i moderni sistemi biometrici di riconoscimento delle impronte.

Alterazioni digitali intenzionali ben eseguite possono risultare particolarmente difficili da individuare, anche all'occhio di esperti del settore. Un malintenzionato potrebbe ricorrere ad un espediente di questo tipo per evitare di essere riconosciuto o per utilizzare l'identità di un'altra persona. Tutto ciò rende il problema dell'alterazione di impronte piuttosto difficile da affrontare e rende necessario lo sviluppo di soluzioni ad-hoc per contrastare il problema.

Recentemente la sicurezza nel campo dei documenti elettronici ha avuto dei significativi miglioramenti grazie all'associazione a questi di caratteristiche biometriche.

Sebbene l'unicità dei caratteri biometrici dovrebbe fornire la certezza di un'associazione uno ad uno fra un documento ed il suo proprietario, è stata dimostrata la possibilità di utilizzare una caratteristica biometrica dalla "doppia-identità" con lo scopo di legare allo stesso documento due identità differenti. [2]

In questo lavoro di tesi si studieranno delle contromisure per rendere un sistema di riconoscimento delle impronte digitali robusto e sicuro verso attacchi che puntano ad utilizzare impronte '*Mixed*': queste impronte vengono create mediante l'unione di due differenti impronte 'Legittime' con lo scopo di permettere ad ambedue gli individui dai quali sono state ottenute di utilizzare lo stesso documento di riconoscimento elettronico.

Dinamica dell'attacco:

Prendiamo in esame un aeroporto che utilizza un sistema "Automated Border Control" (ABC) per gestire l'accesso e i controlli. Questo tipo di sistema effettua un controllo automatico basato sulla caratteristica biometrica senza che sia necessaria la presenza di un agente aeroportuale. Ogni individuo che vuole oltrepassare con successo i controlli dovrà essere munito di un passaporto elettronico integrato di impronta digitale.

Un criminale che vuole oltrepassarli ma che non potrebbe mai richiedere un passaporto, perché appunto è un ricercato, si rivolge ad un complice incensurato.

Al momento dell'emissione del passaporto viene memorizzata l'impronta del proprietario e questa fungerà da template per tutte le future verifiche circa il documento in esame. E' proprio in questa fase di creazione del documento (Registrazione\Enrollment) che la prima parte dell'attacco prende atto. Al momento dell'acquisizione dell'impronta, che fungerà poi da template, il complice applica sul suo dito una finta impronta in lattice che riproduce un'impronta "mixed", generata dalla sua impronta e da quella del criminale, che verrà associata al documento elettronico. Questa impronta è costruita in modo che, sia l'impronta del complice che quella del criminale permettano l'autenticazione con il documento elettronico appena creato.

In seguito alla fase di emissione, sia il complice che il criminale potranno utilizzare il documento per attraversare varchi automatici, o ABC, in quanto l'impronta che vi è memorizzata all'interno ha un grado di somiglianza sufficientemente elevato con le impronte di entrambi i soggetti.

3.2 Metodo di Fusione di Impronte

3.2.1 Premesse

Nella sezione seguente verrà illustrato il processo di creazione di Impronte Mixed sviluppato presso il laboratorio di Sistemi Biometrici (BioLab) dell'Università di Bologna. Questo processo verrà illustrato in maniera generale e non è assolutamente da ritenersi parte da me svolta nell'ambito di questa ricerca sperimentale.

Una impronta dalla "doppia-identità", d'ora in poi definita "Mixed", deve rispettare due requisiti fondamentali:

- Le caratteristiche delle due impronte di partenza devono essere combinate in modo che gli algoritmi di riconoscimento di impronte più avanzati attribuiscano erroneamente tale impronta a entrambi i soggetti.
- L'impronta Mixed deve essere 'realistica' dal punto di vista di un osservatore umano, dovrà infatti superare il controllo dell'addetto alla registrazione delle impronte al momento della creazione del documento.

3.2.2 Processo di creazione di Impronte "Double-Identity"

Lo scopo di questo processo è creare una nuova impronta che contenga caratteristiche (Minuzie, Orientazioni e Frequenze) provenienti da due dita differenti.

Date due impronte F^1 e F^2, provenienti da due dita diverse, per produrre una nuova impronta si seguono questi passaggi:

- Le due impronte sono automaticamente sovrapposte per calcolare il miglior allineamento.
- Viene calcolata una "linea di taglio" ottimale, lungo la quale le due impronte verranno effettivamente unite, massimizzando la somiglianza dei "ridge pattern" nelle vicinanze del taglio. Questo renderà l'impronta verosimile all'occhio umano rendendo più semplice passare il controllo dell'addetto alla registrazione.
- Viene generata la nuova impronta.

Figura 7: Impronte di partenza

Si effettua una stima delle orientazioni locali O^1 e O^2, visibile in Figura 8, a partire dalle due impronte di partenza riportate in Figura 7. Si calcolano le orientazioni su blocchi di pixel, lungo gli assi orizzontali e verticali, utilizzando la tecnica basata sul gradiente. Ogni elemento sarà composto da un angolo e da un valore di affidabilità.

Per trovare il miglior allineamento possibile fra le due immagini delle orientazioni locali si effettua una stima di somiglianza per ogni possibile traslazione e rotazione e si ricerca l'allineamento con il punteggio di somiglianza più elevato. Precedentemente sono poste delle soglie, per evitare casi con una sovrapposizione non sufficiente alla creazione della "mixed".

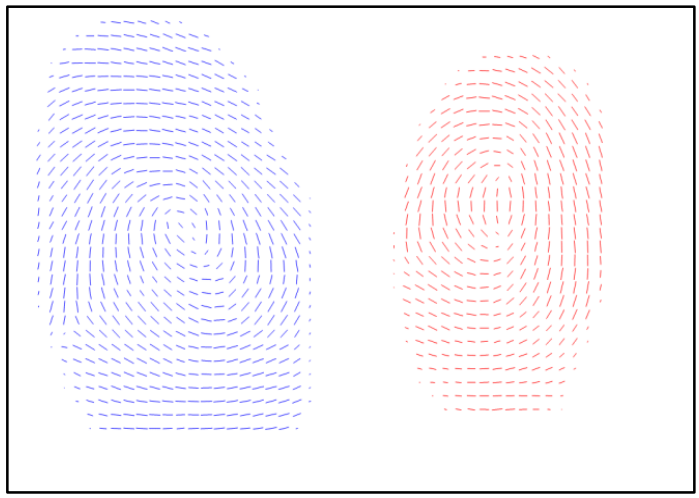


Figura 8: Immagini Direzionali

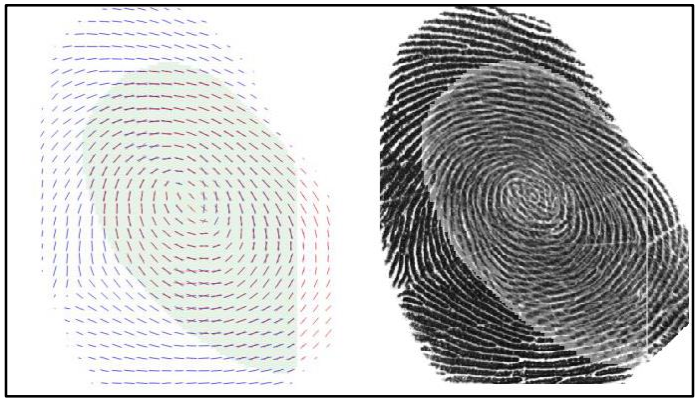


Figura 9: Allineamento basato sulle orientazioni locali

Dall' allineamento, mostrato in Figura 9, viene calcolata la regione di intersezione delle due impronte allineate, su questa regione si eseguono i passi successivi dell'algoritmo.

Figura 10: Intersezione delle due impronte

Per prima cosa viene effettuata una stima delle frequenze locali delle creste, visibile in Figura 11.

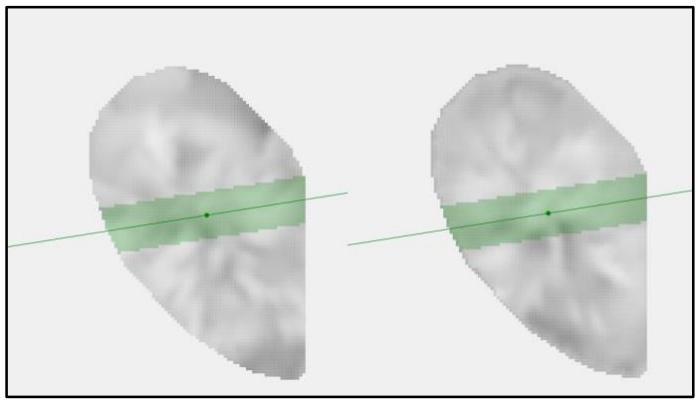


Figura 11: Frequenza locale delle creste stimata sulle regioni di intersezione

Vengono estratti i template di Minuzie, riportati in Figura 12, dalle due immagini risultanti (Figura 10) che ora coincidono perfettamente in dimensione e sono allineate. Ogni minuzia sarà identificata dalla sua posizione sul piano bidimensionale e dall' orientazione.

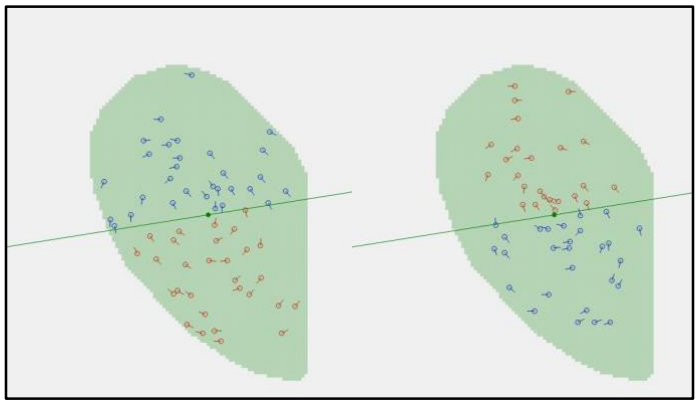


Figura 12: Minuzie estratte dalle regioni di intersezione

Per ogni possibile angolo compreso fra 0 e π viene definita una linea che passa per il baricentro dell'intersezione; per ogni linea definita in questo modo viene calcolato un punteggio basato su tre valori:

- Somiglianza delle orientazioni vicino alla linea (Figura 13)
- Somiglianza delle frequenze vicino alla linea (Figura 11)
- Punteggio di somiglianza calcolato dai due template di Minuzie (Figura 12)

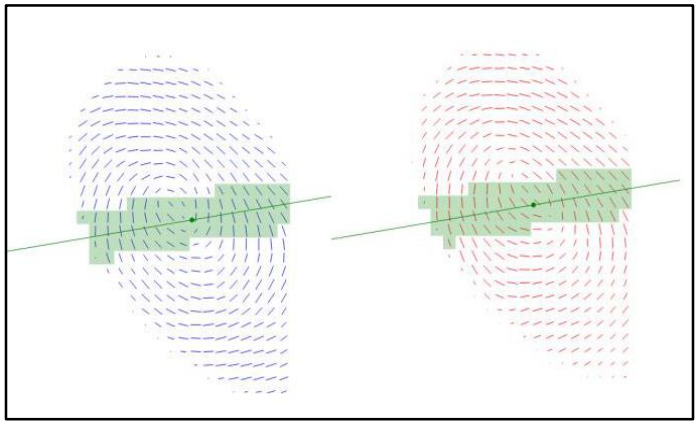


Figura 13: Linea di taglio e immagini direzionali.

Il punteggio risultante è un indicatore della somiglianza dei due "*ridge-pattern*" lungo la linea in esame e del numero di minuzie che saranno presenti nell'immagine "mixed" risultante se la linea attuale viene scelta come "linea di taglio".

Massimizzare i valori relativi a orientazioni e frequenze porta alla creazione di un immagine visivamente realistica, che unisce in maniera convincente le due impronte di partenza.

Il terzo valore è altresì importante in quanto è necessario che l'immagine risultante abbia un numero sufficiente di minuzie provenienti da ambedue i template di partenza, di modo che, quando sarà confrontata con una delle impronte originali, avrà un punteggio di confronto molto elevato dando luogo ad un confronto ritenuto omologo dal sistema.

L'immagine finale (Figura 14) è ottenuta unendo le due intersezioni (Figura 10) lungo la linea di taglio calcolata ai passi precedenti.

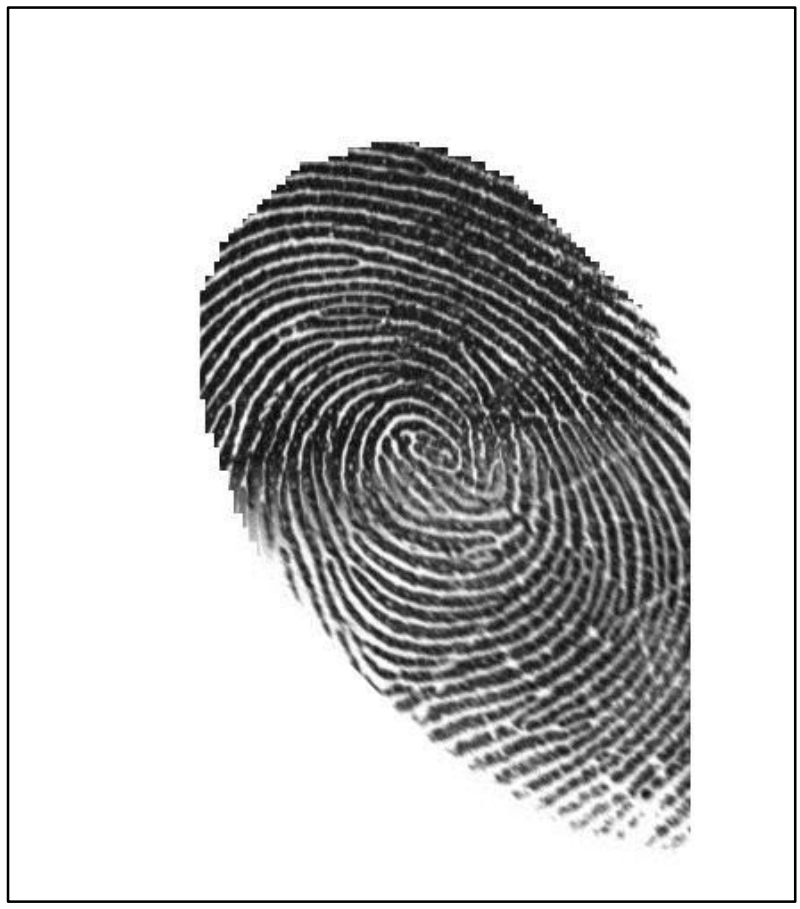


Figura 14: Impronta Mixed completata

3.3 Grado di successo dell'attacco

In questa sezione verranno analizzati dati sperimentali per effettuare una stima del grado di successo dell'attacco ad un sistema di riconoscimento automatico mediante l'uso di impronte "*mixed*".

Per valutare quanto un determinato algoritmo di riconoscimento è robusto rispetto alla tipologia di attacco trattata precedentemente faremo riferimento ai seguenti valori:

- Eer
- Fmr100
- Fmr1000
- Percentuale di successo dell'attacco a Fmr100
- Percentuale di successo dell'attacco a Fmr1000
- Percentuale di successo dell'attacco a Fmr10000

I primi tre valori saranno identificativi dell'accuratezza dell'algoritmo nel caso di confronti Genuine e Impostor, senza che vengano quindi inserite impronte Mixed. I restanti valori indicano la percentuale di successo dell'attacco se come soglia decisionale viene scelta rispettivamente Fmr100, Fmr1000 o Fmr10000.

Il matcher utilizzato per fare questi test è il MatcherMCC fornitomi dal BioLab dell'università di Bologna. [5]

I risultati sono stati ottenuti lanciando un 'tester' sui due differenti database, DB1D e DB1C. I due Database di impronte hanno le seguenti specifiche:

	Numero di dita acquisite	**Impronte per dito**	**Confronti Genuine**	**Confronti Impostor**
DB1C	60	8	1680	1770
DB1D	50	8	1400	1225

	Numero di Mixed create	**Confronti Mixed**
DB1C	60	840
DB1D	50	700

I valori ottenuti utilizzando il Matcher MCC[5], fornitomi presso il BioLab, sono i seguenti:

DB1C *(Database che verrà utilizzato per testare l'efficacia del nuovo algoritmo)*

Eer	**Fmr100**	**Fmr1000**	**Attack Rate**		
			at Fmr100	**at Fmr1000**	**at Fmr10000**
0.55%	0.54%	0.89%	91.79%	88.57%	83.57%

DB1D *(Database di impronte che verrà utilizzato per l'addestramento del nuovo algoritmo)*

Eer	**Fmr100**	**Fmr1000**	**Attack Rate**		
			at Fmr100	**at Fmr1000**	**at Fmr10000**
0.76%	0.79%	0.93%	88.43%	83.00%	76.14%

I risultati ottenuti ci mostrano che, sebbene l'algoritmo in esame abbia prestazioni molto elevate nel caso di confronti Genuine e Impostor (EER, FMR100 e FMR1000), non riesce efficacemente a individuare le impronte mixed. Sula base di queste osservazioni, è corretto affermare che l'attacco ha successo ed è da ritenersi una vera e propria minaccia alla sicurezza degli attuali sistemi biometrici.

Si cercheranno quindi, nel prossimo capitolo, contromisure per rendere l'algoritmo di confronto delle impronte solido rispetto all'impiego di impronte mixed come forma di attacco, cercando, allo stesso tempo, di non peggiorare le prestazioni dell'algoritmo in situazioni normali.

4 STUDIO DI POSSIBILI CONTROMISURE

In questo capitolo saranno analizzate possibili contromisure volte a contrastare l'attacco descritto nel capitolo precedente: inizialmente si analizzerà un articolo scientifico [4] basato sull'uso di minuzie non accoppiate, si procederà infine proponendo soluzioni originali per risolvere il problema in esame.

4.1 Utilizzo di minuzie non accoppiate

In [4] gli autori affermano che l'uso di informazioni discriminanti ottenute dalle minuzie non accoppiate, mostrate in Figura 15, permette di migliorare le prestazioni di un algoritmo di riconoscimento di impronte. Procederemo implementando l'approccio presentato in [4] per valutare se effettivamente le prestazioni migliorano riducendo il grado di successo dell'attacco con impronte "mixed".

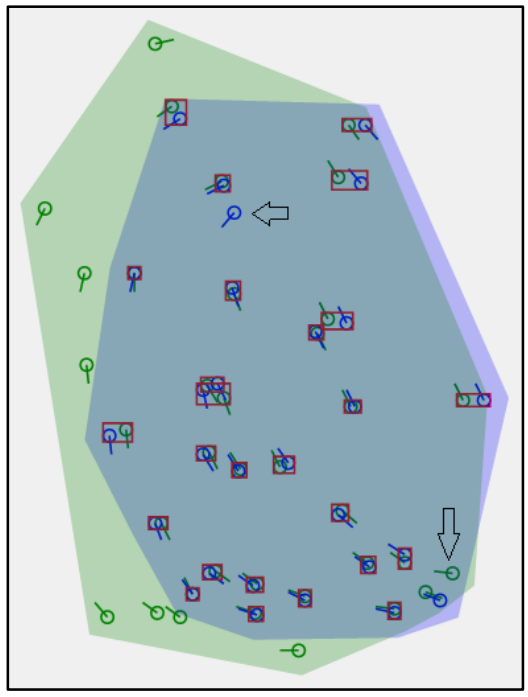


Figura 15: Minuzie non accoppiate

In [4] vengono presentati sette punteggi ausiliari basati sulle minuzie non accoppiate: la combinazione di questi punteggi con il punteggio principale, ottenuto dalle minuzie accoppiate, dovrebbe migliorare le prestazioni del sistema. Le sette caratteristiche esaminate si dividono in 3 categorie:

- Numero relativo di minuzie non accoppiate
- Somiglianza della posizione di coppie di minuzie non accoppiate
- Distribuzione globale delle minuzie non accoppiate

Nell'articolo vengono considerate valide soltanto le minuzie non accoppiate incluse nel poligono convesso costruito su quelle accoppiate con successo: la regione scura in Figura 16.b. Nell'ottica di utilizzare queste caratteristiche per contrastare l'attacco illustrato nella sezione 3.1, in questo lavoro di tesi, verranno considerate valide tutte le minuzie non accoppiate presenti, dopo aver effettuato allineamento e accoppiamento, nell'intersezione delle due impronte come mostrato in Figura 16.a.

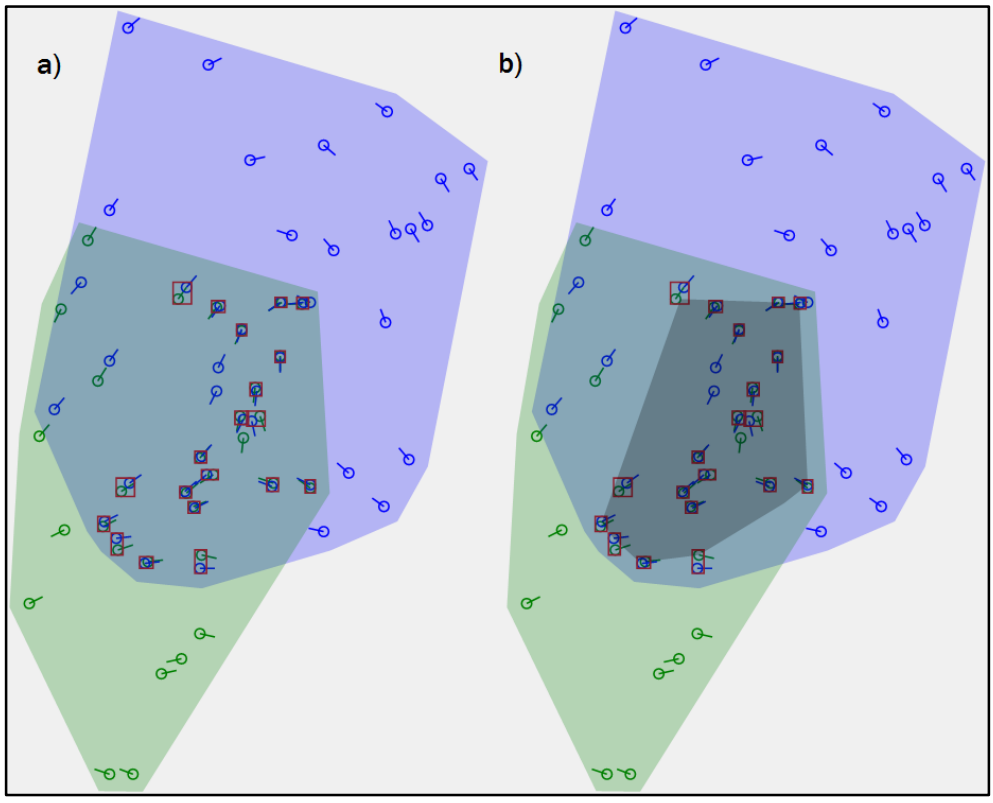


Figura 16: a) Minuzie non accoppiate nell'intersezione delle impronte.
b) Minuzie non accoppiate nel poligono convesso delle Matched.

4.1.1 Presentazione delle nuove caratteristiche

La prima caratteristica che andremo ad esaminare è il rapporto delle minuzie non accoppiate rispetto a quelle che sono state accoppiate con successo. Secondo quanto affermato nell'articolo [4], il numero di tali minuzie in confronti genuine è generalmente minore rispetto a confronti impostor. Si utilizza, quindi, questo rapporto come caratteristica per la creazione del primo punteggio ausiliario (R_u). R_u è calcolato dalla seguente equazione:

$$R_u = \frac{N_1 + N_2}{2N}$$

dove N_1 e N_2 sono rispettivamente il numero delle minuzie non accoppiate nella prima e nella seconda impronta e N rappresenta il numero delle minuzie accoppiate con successo. Più questo punteggio cresce, più sarà probabile che il confronto in atto sia impostor.

Se l'esito del confronto può essere deciso sulla base delle minuzie accoppiate, questa grandezza non sarà necessaria. Quindi, senza effettuare alcun calcolo è possibile assegnare un valore moto basso alla caratteristica se il punteggio principale è superiore alla soglia dei falsi accessi ($th_{zeroFAR}$) e, invece, assegnarne uno elevato nel caso in cui il punteggio principale è inferiore alla soglia dei falsi rifiuti ($th_{zeroFRR}$):

$$R_u = \begin{cases} min_{R_u} & s_0 \geq th_{zeroFAR} \\ \dfrac{N_1 + N_2}{2N} & th_{zeroFRR} < s_0 < th_{zeroFAR} \\ max_{R_u} & s_0 \leq th_{zeroFRR} \end{cases}$$

Il punteggio ausiliario s_1 è calcolato normalizzando la grandezza R_u in modo da ottenere un valore compreso nell'intervallo $[0,1]$:

$$s_1 = \frac{max_{R_u} - R_u}{max_{R_u} - min_{R_u}}$$

In un confronto genuine R_u assumerà un valore esiguo in quanto saranno presenti poche minuzie non accoppiate e quindi, il punteggio s_1, assumerà un valore vicino ad 1; mentre in un confronto impostor il numero delle minuzie accoppiate sarà molto inferiore a quello delle minuzie non accoppiate portando R_u ad un valore molto alto e il punteggio ad abbassarsi drasticamente.

Le prossime caratteristiche analizzate riguardano la "somiglianza di posizione". In un confronto genuine, la maggior parte delle minuzie non accoppiate, dovrebbero trovarsi in posizioni simili, cosa che non succede nei confronti impostor. Si definisce quindi nell'articolo [4] una particolare tipologia di coppie di minuzie.

Nel confronto di due impronte, se una coppia di minuzie non accoppiate (p, q), appartenenti a diverse impronte, soddisfa la seguente equazione, può essere definita una coppia "*tight pair-wise*":

$$d(p,q) = min\{d(p,n)|\forall n \in B\} = \min\{d(m,q)|\forall q \in A\}$$

A e B rappresentano i due set di minuzie non accoppiate nelle due impronte, la funzione *d* misura la distanza Euclidea. Secondo le analisi effettuate nell'articolo [4], in confronti genuine si osserva un aumento del numero delle coppie "*tight pair-wise*" ed una diminuzione della distanza fra le minuzie in esse contenute. Da queste coppie si ottengono due punteggi: il primo (R_p), basato sul numero delle coppie trovate rispetto al totale delle minuzie non accoppiate, il secondo, (D_p), è la distanza media delle minuzie che formano le coppie "*tight par-wise*":

$$R_p = \begin{cases} max_{R_p}, & s_0 \geq th_{zeroFAR} \\ max_{R_p}, & th_{zeroFRR} < s_0 < th_{zeroFAR} \; and \; N_1 + N_2 = 0 \\ \dfrac{2N_p}{N_1 + N_2} & th_{zeroFRR} < s_0 < th_{zeroFAR} \; and \; N_1 + N_2 > 0 \\ min_{R_p}, & s_0 \leq th_{zeroFRR} \end{cases}$$

$$D_p = \begin{cases} min_{D_p}, & s_0 \geq th_{zeroFAR} \\ \dfrac{\sum_{i=1}^{N_p} d(p_i, q_i)}{N_p} & th_{zeroFRR} < s_0 < th_{zeroFAR} \; and \; N_p = 0 \\ max_{D_p}, & th_{zeroFRR} < s_0 < th_{zeroFAR} \; and \; N_p > 0 \\ max_{D_p}, & s_0 \leq th_{zeroFRR} \end{cases}$$

In queste equazioni N_p indica il numero di coppie "*tight pair wise*" individuate mentre N_1 e N_2 sono rispettivamente il numero delle minuzie non accoppiate nella prima e nella seconda impronta.

Da questi valori sono ottenuti il secondo ed il terzo score ausiliari mediante normalizzazione:

$$s_2 = \frac{R_p - min_{R_p}}{max_{R_p} - min_{R_p}}$$

$$s_3 = \frac{max_{D_p} - D_p}{max_{D_p} - min_{D_p}}$$

Si può notare che al crescere di R_p e al diminuire di D_p aumenta la probabilità che il confronto in esame sia genuine: in tali confronti è più facile incontrare coppie "*tight pair wise*" e le minuzie che le compongono saranno particolarmente vicine.

Le restanti caratteristiche si basano sulla distribuzione globale delle minuzie non accoppiate. In confronti genuine, questa distribuzione dovrebbe in qualche modo essere simile fra le due impronte in esame, cosa che, invece, accade raramente in confronti impostor.

Si definiscono quindi, nell'ambito della distribuzione globale, due aspetti: la somiglianza spaziale dei raggruppamenti dei punti e la distanza di Hausdorff.

Riguardo al primo di questi due aspetti vengono considerate tre misure: il centro dell'insieme di punti, la direzione e la forma dell'Ellisse di Deviazione Standard (SDE) costruita sui punti dell'insieme.

Il centro di un raggruppamento di punti è calcolato con la seguente equazione:

$$(\bar{x}_{mc}, \bar{y}_{mc}) = \left(\frac{\sum_{i=1}^{n} x_i}{n}, \frac{\sum_{i=1}^{n} y_i}{n}\right)$$

Per calcolare la direzione Θ dell'ellisse si calcola $\tan\Theta$:

$$\tan\Theta = \frac{\left(\sum_{i=1}^{n} x_i'^2 - \sum_{i=1}^{n} y_i'^2\right) + \sqrt{\left(\sum_{i=1}^{n} x_i'^2 - \sum_{i=1}^{n} y_i'^2\right)^2 + 4\left(\sum_{i=1}^{n} x_i' y_i'\right)^2}}{2\sum_{i=1}^{n} x_i' y_i'}$$

$$\text{dove } x_i' = x_i - \bar{x}_{mc}, \quad y_i' = y_i - \bar{y}_{mc}, \quad \text{i} = 1,2,\ldots,\text{n}$$

Dopo aver calcolato la tangente si può ottenere la direzione:

$$\Theta = \begin{cases} \tan^{-1} t\,, & t \geq 0 \\ \frac{\pi}{2} - \tan^{-1} t\,, & t < 0 \end{cases}$$

$$\text{con} \quad t = \tan\Theta$$

Per ottenere invece la forma dell'elisse si usano le seguenti formule dove δ_l e δ_s sono le deviazioni dei punti lungo gli assi l e s (Figura 15)

$$\delta_l = \sqrt{\frac{\sum_{i=1}^{n}[(x_i - \bar{x}_{mc})\sin\Theta + (y_i - \bar{y}_{mc})\cos\Theta]^2}{n}}$$

$$\delta_s = \sqrt{\frac{\sum_{i=1}^{n}[(x_i - \bar{x}_{mc})\cos\Theta - (y_i - \bar{y}_{mc})\sin\Theta]^2}{n}}$$

Il rapporto fra queste grandezze è rappresentato da $\delta = \frac{\delta_s}{\delta_l}$.

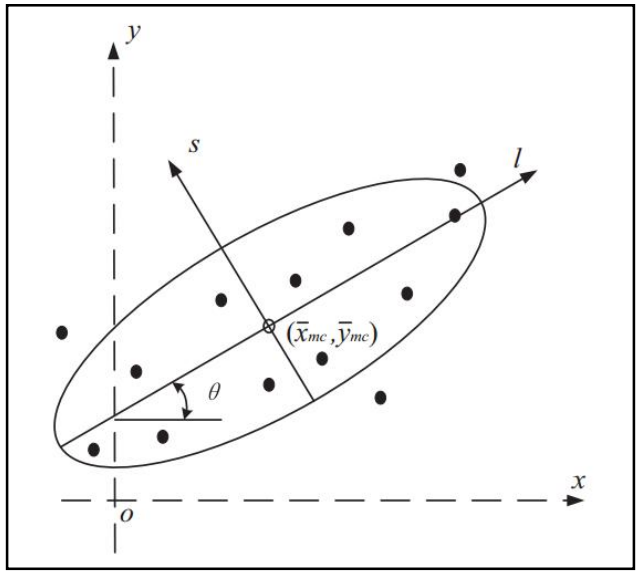


Figura 17: Ellisse di Deviazione Standard

Gli insiemi delle minuzie non accoppiate nelle due impronte vengono utilizzati come raggruppamenti di punti per il calcolo della somiglianza spaziale: si misura cosi la consistenza della distribuzione delle minuzie nelle due impronte in esame. Vengono definite tre caratteristiche ottenibili dai due insiemi di minuzie indicati come A e B:

$$D_c = \sqrt{(\bar{x}_A - \bar{x}_B)^2 + (\bar{y}_A - \bar{y}_B)^2}$$

$$D_\Theta = \cos(\Theta_A - \Theta_B)$$

$$D_\delta = |\delta_A - \delta_B|$$

Tre punteggi ausiliari (s_4, s_5, s_6) possono essere ottenuti normalizzando questi valori per nell'intervallo [0,1].

$$s_4 = \frac{max_{D_c} - D_c}{max_{D_c} - min_{D_c}}$$

$$s_5 = \frac{D_\Theta - min_{D_\Theta}}{max_{D_\Theta} - min_{D_\Theta}}$$

$$s_6 = \frac{max_{D_\delta} - D_\delta}{max_{D_\delta} - min_{D_\delta}}$$

Infine analizziamo i due insiemi di minuzie non accoppiate come set di punti e procediamo al calcolo della distanza di Hausdorff,. Definiti i due insiemi di minuzie come A e B la distanza di Hausdorff $H(A,B)$ è calcolata come segue:

$$h(A,B) = \max_{a \in A} \min_{b \in B} d(a,b)$$

$$h(B,A) = \max_{b \in B} \min_{a \in A} d(b,a)$$

$$H(A,B) = \max\big(h(A,B), h(B,A)\big)$$

Normalizzando $H(A,B)$ otteniamo s_7 e possiamo procedere alla combinazione di tutti i punteggi ausiliari per il calcolo del punteggio finale.

$$s_7 = \frac{max_H - H}{max_H - min_H}$$

Per calcolare il punteggio finale si utilizza un metodo di fusione con pesi che, per ogni punteggio ausiliario, calcola il contributo al punteggio totale sulla base di un peso stabilito. La somma dei pesi dovrà essere uguale ad uno.

$$s_f = \sum_{i=0}^{7} (w_i \times s_i)$$

$$con \sum_{i=0}^{7} w_i = 1$$

4.1.2 Test delle caratteristiche presentate

Si procederà ora ad effettuare dei test e osservare alcuni specifici confronti di impronte per verificare se i punteggi ausiliari illustrati nell'articolo [4] possono essere utili per incrementare la sicurezza del nostro sistema, nei confronti di un attacco con impronte "mixed", senza causare una perdita di prestazioni troppo elevata come, ad esempio, un aumento considerevole dell'FMR100 o dell'FMR1000.

Prima di testare tali punteggi con l'impiego di impronte "mixed", sono stati effettuati dei test nei casi di uso comune per verificarne l'affidabilità. Sono stati calcolati i valori massimi, minimi e medi delle caratteristiche illustrate nella sezione precedente sul database DB1D, dividendo i risultati fra confronti genuine ed impostor.

Tutte le caratteristiche, ad eccezione della prima (R_u), assumono, mediamente, valori migliori per confronti impostor rispetto a confronti genuine, l'esatto opposto delle aspettative. Valori migliori, infatti, dopo la normalizzazioni, genereranno punteggi ausiliari migliori. Questo potrebbe essere dovuto alla scelta di utilizzare, nell'ottica di rendere il sistema robusto verso l'attacco "mixed", tutte le minuzie non accoppiate presenti nell'intersezione.

Valori Medi delle caratteristiche ottenuti su DB1D.

	R_u	R_p	D_p	D_c	D_Θ	D_δ	$Hausdorff$
Genuine	0.247	0.427	33.352	35.297	0.641	0.518	33.659
Impostor	10.999	0.543	14.725	20.445	0.773	0.422	22.138
Affidabile?	SI	NO	NO	NO	NO	NO	NO

N.B. (R_p e D_Θ dovrebbero avere valori più alti per confronti genuine, R_u, D_p, D_c, D_δ e la distanza di Hausdorff, valori più elevati per confronti impostor)

Si ricercheranno ora le motivazioni di questi risultati esaminando alcuni confronti nello specifico.

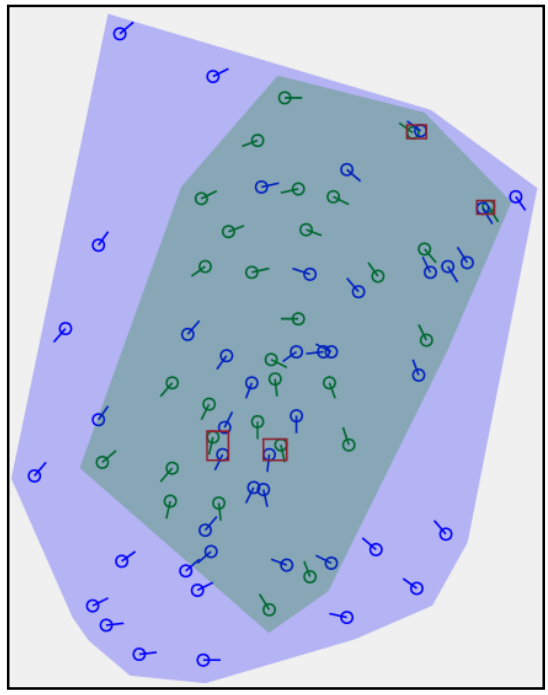


Figura 18: Confronto Impostor

Nel confronto impostor mostrato in Figura 18 possiamo notare che vi sono ben poche minuzie accoppiate con successo, infatti, R_u ha un buon potere discriminante in questo caso. Però, vengono rilevate ben 14 coppie "*tight pair-wise*". I centri degli insiemi di punti relativi alle due impronte sono vicini, le orientazioni delle ellissi costruite su questi ultimi sono simili e la distanza di Hausdorff è molto piccola.

Caratteristiche del confronto Impostor (Figura 16).

R_u	R_p	D_p	D_c	D_Θ	D_δ	$Hausdorff$
6.125	0.571	16.759	22.946	0.950	0.686	15.65

Rispetto alla media dei confronti genuine questo confronto impostor ha punteggi ausiliari migliori per ogni caratteristica ad eccezione di R_u e D_δ.

Procediamo ora esaminando un confronto genuine per comprendere definitivamente se è possibile utilizzare alcune di queste caratteristiche nel tentativo di rendere il sistema più robusto all'attacco.

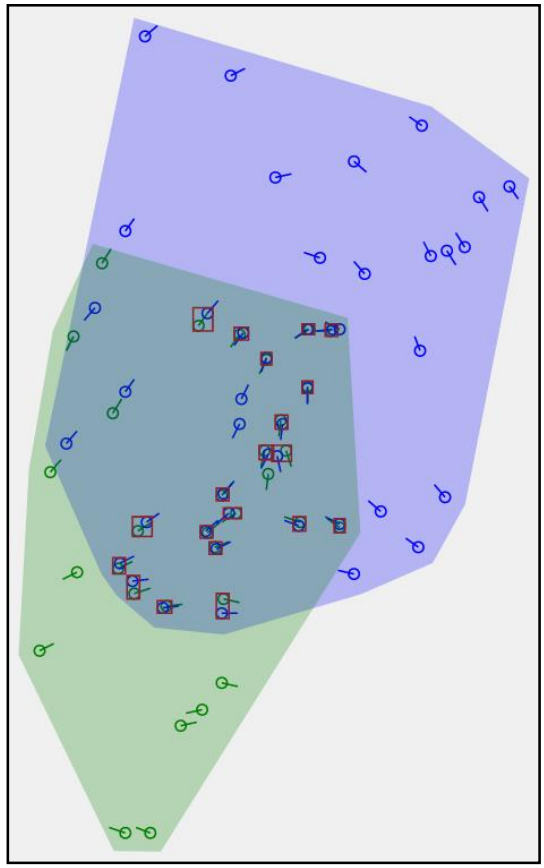


Figura 19: Confronto Genuine

Caratteristiche del confronto Genuine (Figura 19).

R_u	R_p	D_p	D_c	D_Θ	D_δ	$Hausdorff$
0.25	0.6	22.047	26.134	-0.622	1.417	25.317

Da questo confronto notiamo che, R_u assume un valore molto basso, grazie alla presenza di poche minuzie non accoppiate. Delle altre caratteristiche in esame, l'unica ad assumere un valore accettabile, è R_p che, però, non era stata utile nel caso del confronto Impostor (Figura 16). Le altre caratteristiche producono punteggi ausiliari non accettabili, poiché penalizzano i confronti genuine rispetto a quelli impostor e quindi peggiorerebbero di molto le prestazioni del nostro sistema.

Questo è probabilmente dovuto al basso numero di minuzie non accoppiate presenti nei confronti genuine: avendo poche minuzie su cui basare le misurazioni, i valori divengono molto sensibili al rumore, cosa che non avviene nel caso dei confronti impostor.

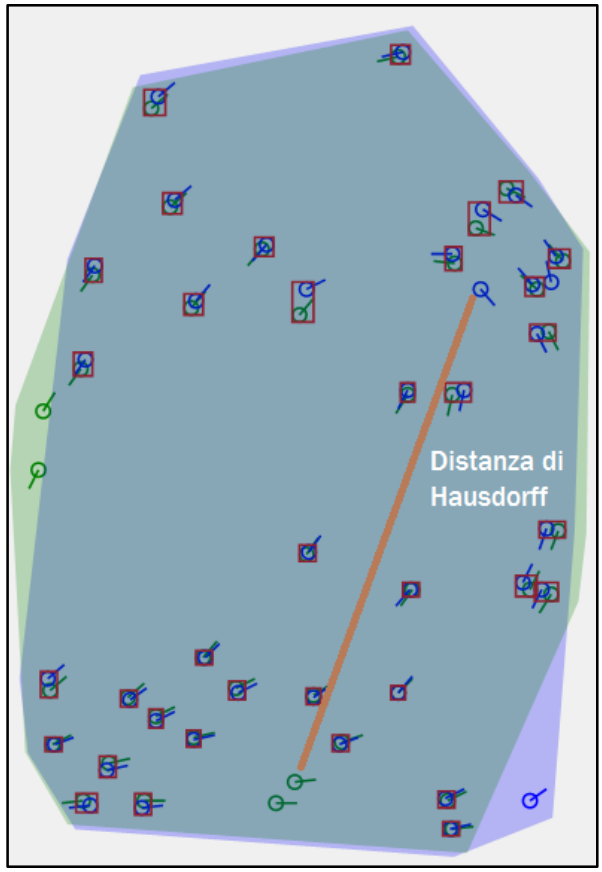


Figura 20: confronto genuine con alta distanza di Hausdorff

Ad esempio, nel caso mostrato in Figura 20, si ottiene un valore molto alto per la distanza di Hausdorff poiché le poche minuzie non accoppiate si trovano molto distanti fra loro.

Calcolare caratteristiche legate a distanze e orientazioni, su di un numero così esiguo di minuzie, non porta risultati attendibili: anche l'introduzione di una sola minuzia falsa dovuta a rumore o errori di estrazione cambia drasticamente il valore delle caratteristiche. Sulla base dei risultati ottenuti mediante il test sui valori medi e dall'osservazione dei casi specifici, si è deciso che la sola caratteristica utilizzabile è R_u , dato che è l'unica che ha presentato risultati soddisfacenti nella maggior parte delle situazioni esaminate.

4.2 Un Sistema più robusto

Nella sezione precedente si è deciso che fra le varie caratteristiche presentate l'unica utilizzabile per il nostro scopo è R_u; in questa sezione, si introdurranno nuove caratteristiche, studiate appositamente in questo lavoro di tesi, per rendere un sistema di riconoscimento più robusto verso l'attacco con impronte "mixed".

Queste nuove caratteristiche sono state ottenute in maniera differente rispetto a quelle presentate nell'articolo[4]. Mentre le caratteristiche presentate precedentemente avevano come obbiettivo migliorare i confronti nel caso generale senza impronte mixed, alcune delle nuove caratteristiche, che verranno introdotte in questo capitolo, sono state pensate osservando direttamente le differenze fra impronte genuine e "mixed".

Dall'osservazione di aree come l'area di intersezione, l'area minima e l'unione delle aree delle due impronte si possono estrarre informazioni discriminanti.

La **prima** delle nuove caratteristiche, A_1, è il rapporto fra l'area di intersezione e l'area minima delle due impronte. Si è osservato che in confronti impostor difficilmente l'allineamento riesce a sovrapporre correttamente le due impronte, mentre, nei casi genuine, l'area di sovrapposizione è molto più grande e talvolta coincidente con l'area minima. Questa caratteristica mira a migliorare il riconoscimento nel caso base senza, però, basarsi sulle minuzie, come, ad esempio, in Figura 21.

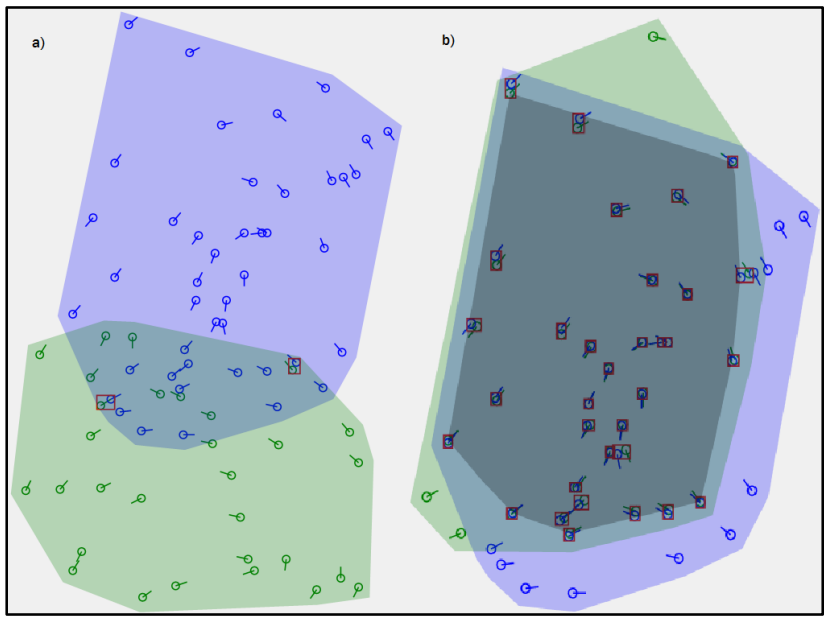


Figura 21 a) confronto Impostor, b) confronto Genuine

La **seconda** caratteristica, A_2, nasce dall'osservazione dei confronti con impronte "mixed": le minuzie accoppiate in questi confronti si concentrano in zone particolari all'interno dell'intersezione delle due impronte: questo è dovuto al processo di creazione delle "mixed" che appunto unisce due metà di impronte diverse lungo una linea di taglio. Da questa osservazione si è deciso, quindi, di utilizzare il rapporto fra l'area del poligono convesso costruito sulle minuzie accoppiate e l'area dell'intersezione delle due impronte. Questa caratteristica è solida, non solo per i confronti mixed, ma anche per discernere fra confronti genuine e impostor: raramente un confronto impostor avrà un poligono costruito sulle minuzie accoppiate con area elevata.

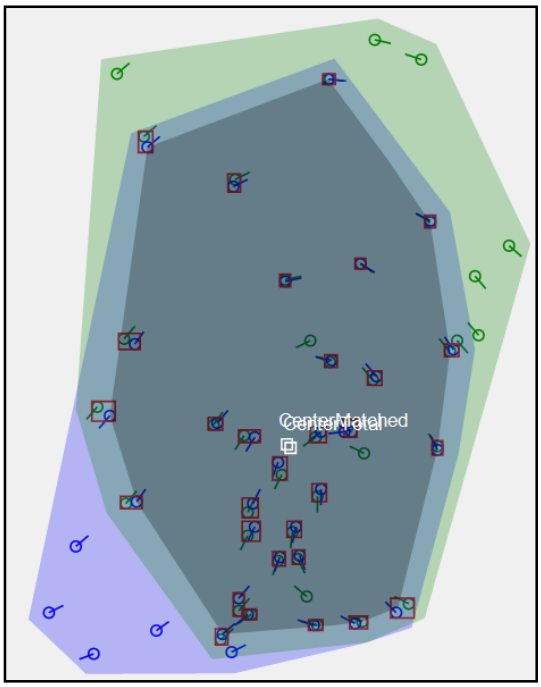


Figura 22: Aree in confronto Genuine

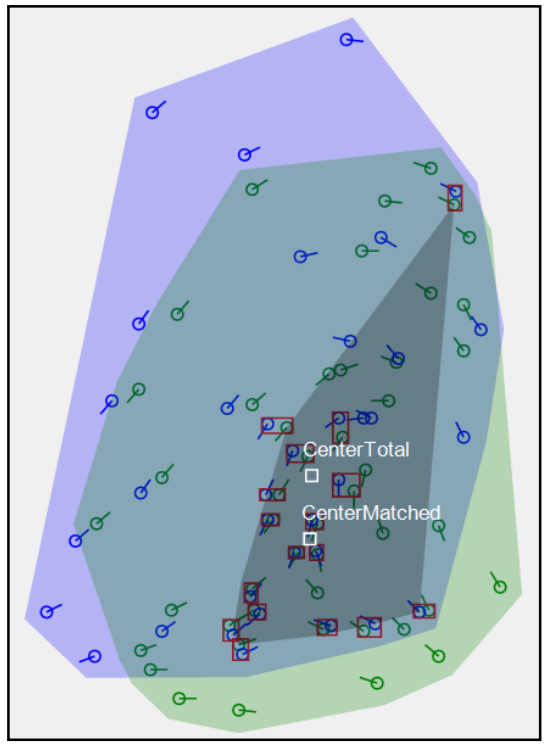


Figura 23: Aree in confronto con impronta "mixed"

Come si può notare dai confronti in Figura 22 e Figura 23, anche se il confronto "mixed" ha un alto numero di minuzie accoppiate rispetto ad un semplice confronto impostor (Figura 18), la distribuzione di queste minuzie fa sì che l'area del poligono costruito su di esse sia minore rispetto a quella ottenuta in un confronto genuine.
Sebbene questa caratteristica presenti un alto potere discriminante per l'individuazione dei

confronti “mixed”, è molto sensibile al rumore e ad errori di estrazione: una singola minuzia falsa potrebbe aumentare molto l’area del poligono in esame. (Figura 25)

La **terza** caratteristica, A_3, viene calcolata come il rapporto fra l’area del poligono convesso costruito sulle minuzie accoppiate e l’area minima delle due impronte. Se l’area del poligono è molto simile all’area minima, come nel caso mostrato in Figura 24, significa che una delle due impronte ha un riscontro pressoché totale con l’altra, cosa che non avviene mai in confronti “mixed”.

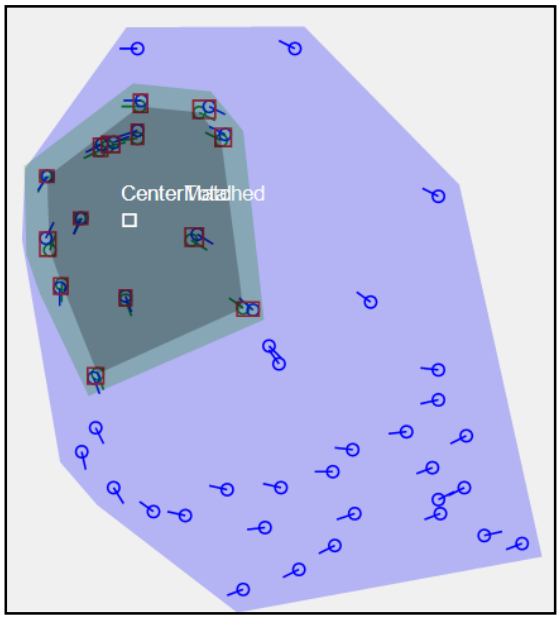


Figura 24: Confronto Genuine dove la terza caratteristica è molto discriminante

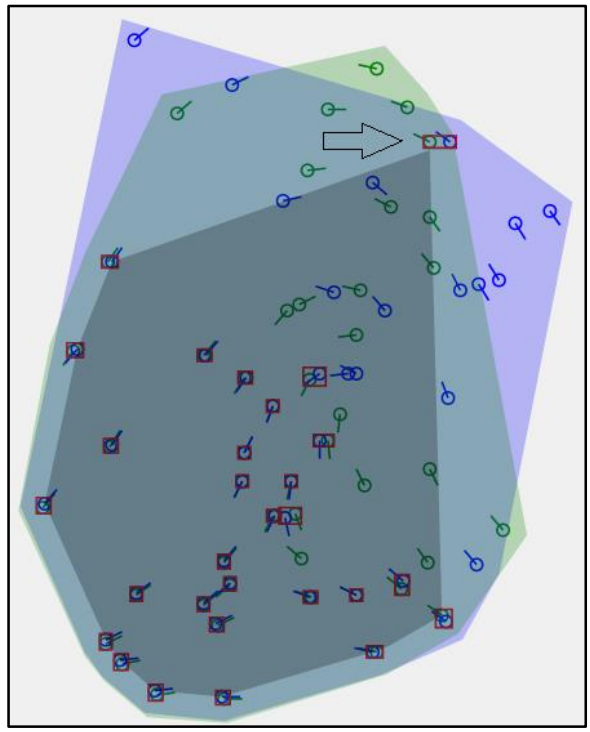


Figura 25: Un casuale falso accoppiamento estende molto l’area del poligono

La **quarta** caratteristica introdotta, A_4, è il rapporto fra l’area di intersezione e l’area dell’unione delle due impronte. In confronti genuine, solitamente, l’area dell’unione delle due impronte è molto ridotta rispetto a confronti impostor dove l’allineamento non è ottimale e le impronte hanno scarsa sovrapposizione, un esempio in Figura 26.

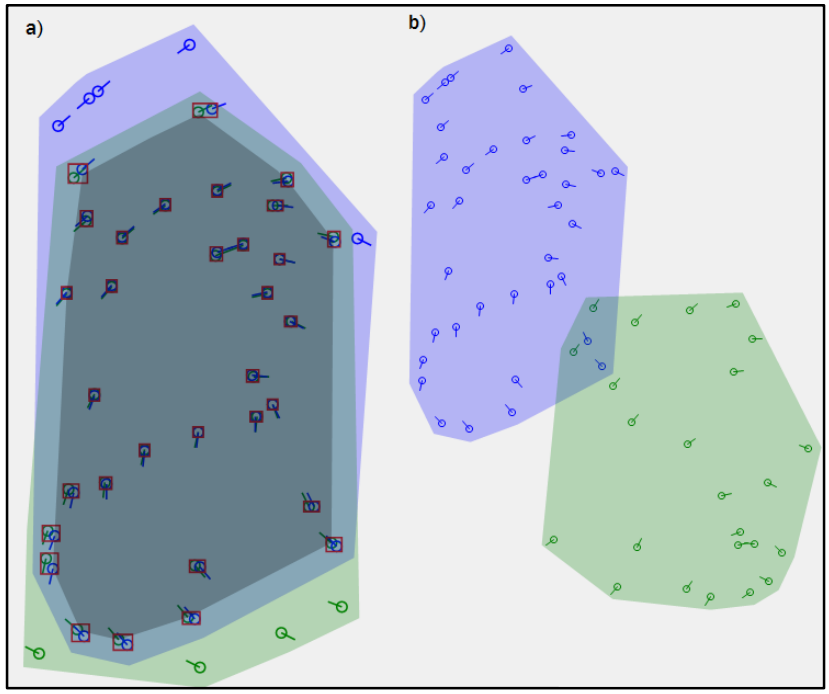


Figura 26: a) confronto genuine, b) confronto impostor

La **quinta** caratteristica, A_5, similmente ad A_4, utilizza l'area dell'unione delle due impronte e viene calcolata come il rapporto fra l'area del poligono convesso costruito sulle minuzie accoppiate e l'area dell'unione delle due impronte. Queste due caratteristiche, come la prima, hanno come obbiettivo migliorare le prestazioni del riconoscimento nel caso base, senza però basarsi sull'analisi delle minuzie, rendendo quindi meno efficaci le impronte "mixed". La loro efficacia dipende fortemente dal metodo di allineamento utilizzato e non forniscono risultati particolarmente stabili.

La **sesta** ed ultima caratteristica introdotta, Dis, non si basa sull' osservazione delle aree, similmente alle caratteristiche D_c, D_Θ e D_δ, osserva la distribuzione globale delle minuzie trattandole come insiemi di punti ed andando a calcolare il centro di questi insiemi.

Questa caratteristica viene calcolata come la differenza fra il centro dell'insieme delle minuzie accoppiate con successo e il centro dell'insieme comprendente tutte le minuzie presenti nell'intersezione delle due impronte. In confronti genuine, dove la maggior parte delle minuzie nell'intersezione sono accoppiate, i due centri saranno molto vicini (Figura 22) se non coincidenti (Figura 24); in confronti impostor, un esempio in Figura 27,

e “mixed” (Figura 23) i due centri saranno più lontani a causa delle presenza di minuzie non accoppiate.

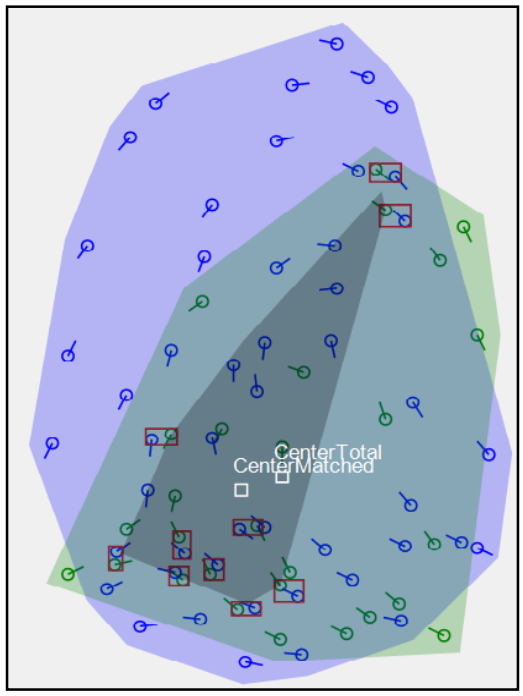


Figura 27: Confronto Impostor con centri degli insiemi distanti.

La caratteristica presenta un buon potere discriminante verso le impronte “mixed” in quanto, non solo tiene conto del numero di minuzie non accoppiate, ma anche della loro posizione e come abbiamo mostrato precedentemente, nei confronti “mixed”, le minuzie accoppiate e quelle non accoppiate tendono a trovarsi in zone ben distinte dell’intersezione. Questa caratteristica, rispetto alle precedenti, è meno sensibile a rumore ed errori di estrazione, fornendo prestazioni più stabili e costanti. A differenza delle caratteristiche precedenti, che per definizione sono comprese fra 0 e 1 e quindi possono essere utilizzate direttamente come punteggi ausiliari, la sesta caratteristica (*dis*) deve essere normalizzata. Per fare ciò si sono calcolati i massimi e i minimi della caratteristica sui confronti genuine del database DB1D, dopodiché è stata utilizzata la normalizzazione inversa in quanto al crescere della distanza cresce la probabilità di un confronto impostor.

$$s_{dis} = \frac{max_{dis} - dis}{max_{dis} - min_{dis}}$$

Di seguito si mostra l'associazione fra pesi, punteggi e caratteristiche.

w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7
s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
mccScore	R_u	A_1	A_2	A_3	A_4	A_5	Dis

Ogni caratteristica genera un punteggio, se necessario viene utilizzata una formula di normalizzazione come, ad esempio, per R_u e Dis .

Per calcolare il punteggio finale si mantiene il metodo di fusione con pesi [4] illustrato precedentemente. Per ogni punteggio ausiliario si calcola il contributo al punteggio totale sulla base di un peso stabilito. La somma dei pesi dovrà essere uguale ad uno.

$$s_f = \sum_{i=0}^{7} (w_i \times s_i)$$

$$con \sum_{i=0}^{7} w_i = 1$$

4.3 Implementazione del sistema

In questa sezione sono descritti i dettagli implementativi e architetturali del sistema. Il sistema è composto da tre ConsoleApplication utilizzate per i test e il calcolo di parametri e punteggi, da una WindowsFormApplication "Viewer" utilizzata per osservare graficamente il confronto di due impronte specifiche e dalla libreria "MixedRobustLibrary".

All'interno della libreria "MixedRobustLibrary", è presente l'implementazione del nuovo matcher per il confronto di impronte e di una classe statica "ClassUtilities" contenente metodi di utilità generale che sono richiamati in diverse applicazioni (come ad esempio per il calcolo delle caratteristiche). "ClassUtilities" fornisce i seguenti metodi:

- *ComputeUnmatchedMinutiae*, conta il numero di minuzie non accoppiate nei due template di minuzie forniti in input.
- *ArrayUnmatchedMinutiae,* crea dei vettori contenenti gli indici di posizione delle minuzie non accoppiate che si trovano nella regione di intersezione.
- *ComputeMatchedMinutiae,* conta il numero di minuzie accoppiate.
- *ArrayMatchedMinutiae,* crea dei vettori contenenti gli indici di posizione delle minuzie accoppiate con successo.
- *ArrayMinDistanceMinutiae,* calcola per ogni minuzia non accoppiata del primo template la distanza minima verso le minuzie de secondo e viceversa.
- *CalculateTemplateConvexHull,* Calcola il poligono convesso sul template di minutiae in input.
- *CalculateCenter,* Calcola il centro dell'insieme di punti in input.
- *ComputePositionSimilarityMinutiae,* calcola il numero di coppie "tight pair-wise" e la loro distanza media per il calcolo delle caratteristiche R_p e D_p presentate in [4].
- *ComputeGlobalDistributionConsistencyMinutiae,* calcola i valori necessari al calcolo delle caratteristiche D_c, D_Θ e D_δ presentate nell'articolo [4].
- *ComputeHausdorffDistance,* calcola la distanza di Hausdorff.
- *ComputeIntersectionArea,* utilizza la libreria esterna Clipper [6] per il calcolo dell'area di intersezione, dell'area minima e dell'area del poligono convesso costruito sulle minuzie accoppiate con successo.

I vari metodi per il calcolo delle caratteristiche sono stati inseriti nella classe statica ClassUtilities, in quanto, devono essere utilizzati da tutte le ConsoleApplication del sistema e dal "Viewer".

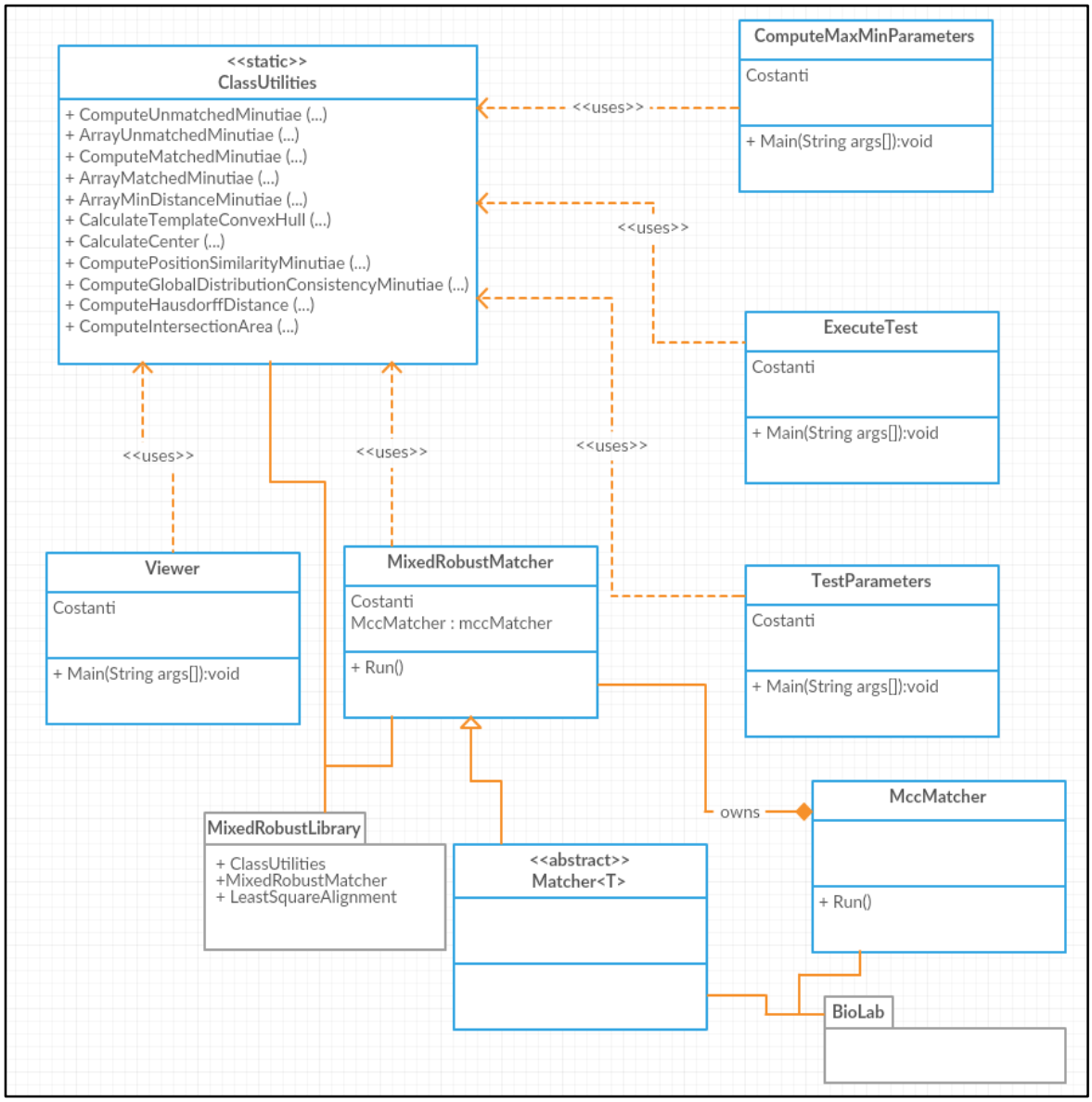


Figura 28: Diagramma riassuntivo del sistema

Durante lo sviluppo del nuovo Matcher, per prima cosa, sono stati implementati i metodi per calcolare i punteggi presentati nell'articolo [4]. Si è rivelato necessario creare una ConsoleApplication ("ComputeMaxMinParameters") per il calcolo dei valori massimi, minimi e medi delle varie caratteristiche per effettuare, in seguito, le normalizzazioni e osservare l'affidabilità dei risultati.

Per il calcolo del punteggio finale si utilizza un metodo di fusione dei vari punteggi ausiliari e di quello ottenuto dalle minuzie accoppiate: per ognuno di essi dovrà essere specificato un peso. E' necessario, quindi, individuare le combinazioni di pesi che migliorino il riconoscimento delle impronte "mixed" e permettano di mantenere ottime prestazioni nel caso generale.

Per individuare queste combinazioni di pesi è stata sviluppata una ConsoleApplication ("Test Parameters") che calcola le prestazioni per ogni configurazione di pesi ammissibile. Utilizzando questa applicazione sono stati calcolati per ogni confronto genuine, impostor e "mixed" del database DB1D, tutti i punteggi ausiliari. Una volta calcolati i punteggi ausiliari, viene lanciato un ciclo che, per ogni combinazione ammissibile di pesi, utilizza i punteggi pre-calcolati per il calcolo dello score finale di ogni confronto.

La ConsoleApplication "ExecuteTest", lancia un test per il calcolo delle prestazioni, in termini di accuratezza, sulla base di una combinazione di pesi fornita e calcola le soglie decisionali per Fmr100, Fmr1000, Fmr10000, ZeroFmr.

Il test avviene nel modo seguente:

- Calcolo dei punteggi per tutti i confronti genuine.
- Calcolo dei punteggi per tutti i confronti impostor.
- Calcolo delle statistiche e delle soglie utilizzando il PerformanceCalculator[7].
- Calcolo dei punteggi per i tentativi di attacco "mixed".
- Calcolo della percentuale di successo dell'attacco.

"ExecuteTest" si occupa, quindi, sia di calcolare le soglie decisionali e le prestazioni sul database di test DB1D, che, in seguito, di effettuare il test con le stesse soglie su DB1C per ottenere le prestazioni su di un database di impronte differente da quello di addestramento.

Il MixedRobustMatcher implementato estende la classe astratta generica Matcher<T> fornita dalla libreria BioLab [7] e incapsula al suo interno mccMatcher [5] che è stato utilizzato per il calcolo del punteggio basato sulle minuzie accoppiate con successo.

Infine è stata sviluppata una WindowsFormApplication "Viewer" che fornisce l'interfaccia grafica per osservare l'estrazione delle minuzie dalle impronte ed il successivo accoppiamento, molto utile per osservare casi specifici e particolari (le immagini dei confronti utilizzate nei capitoli precedenti sono state create con questo strumento).

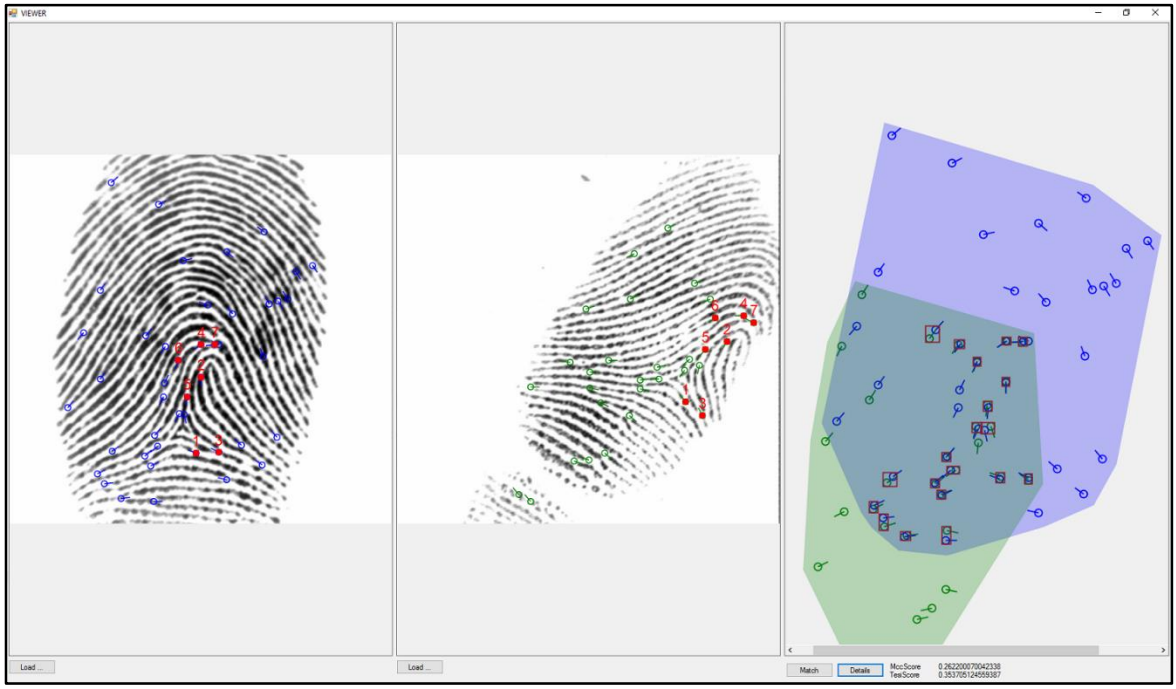


Figura 28: Interfaccia grafica del viewer

5 RISULTATI SPERIMENTALI

In questo capitolo verranno presentati i vari test effettuati e riportati i risultati sperimentali ottenuti dal nuovo matcher implementato, sia in termini di prestazioni nel caso generale, sia nel caso di un attacco con impronte "mixed".

5.1 Calcolo di massimi e minimi

Utilizzando l'applicazione "ComputeMaxMinParameters", sono stati calcolati, sul database di DB1D (utilizzato per il *tuning* dei parametri), i valori massimi e minimi per Ru e Dis che verranno utilizzati per la normalizzazione. Per ottenere risultati più affidabili sono stati scartati il 5% dei valori massimi e minimi in quanto, valori estremi, potrebbero essere stati causati da rumore o piccoli errori al momento dell'estrazione delle minuzie. Queste due caratteristiche sono le uniche che necessitano di essere normalizzate nell'intervallo [0,1], le restanti sono già definite in questo dominio.

	Ru	Dis
Massimo	0.5384	0.1546
Minimo	0.0147	17.7735

5.2 Ricerca di combinazioni di Pesi Ottimali

Nello scegliere i pesi associati ai vari punteggi, il punteggio s_0, ottenuto dalle minuzie accoppiate, deve assumere un valore maggiore di 0.4 per mantenere la sua influenza e minore di 0.75 per permettere ai punteggi ausiliari di avere influenza sufficiente per individuare i confronti con impronte "mixed". Ogni peso ausiliario può assumere valori da 0 a 0.6, le combinazioni ammissibili sono quelle dove la somma dei pesi è uguale ad uno. Sono state esaminate un totale di 318444 combinazioni.

Per ogni combinazione di pesi vengono memorizzati i seguenti valori:

- **EER**
- **FMR100**
- **FMR1000**
- **ZeroFMR**
- **AttackRate**, la percentuale di successo dell'attacco se come soglia decisionale è scelta la soglia per FMR1000.
- **TradeOff**, il rapporto fra il guadagno in termini di riconoscimento delle impronte "mixed" (*Attacco a FMR1000*) e la perdita di prestazioni nel caso base (*FMR1000*).

Analizzando i risultati ottenuti sul database DB1D, le combinazioni di pesi che hanno mostrato la migliore percentuale di riconoscimento delle impronte "mixed" danno molta importanza al terzo punteggio ausiliario (s_3, A_2, w_3), ovvero il rapporto fra area del poligono costruito sulle minuzie accoppiate e l'area d'intersezione delle impronte. Purtroppo, tali combinazioni, peggiorano in maniera non indifferente le prestazioni nel caso generale (FMR1000).

Sono state scelte quattro combinazioni di pesi con cui effettuare i successivi test sul database DB1C:

- quella che, mantenendo il valore di FMR1000 sotto il 3% (soglia stabilita come requisito dalla comunità europea), ha il miglior riconoscimento delle impronte "mixed";
- la combinazione che porta il minor peggioramento possibile alle prestazioni nel caso generale (FMR1000);
- due combinazioni che presentano ottimi valori di TradeOff, per cui a fronte di una piccola perdita di prestazioni (FMR1000) apportano un ottimo guadagno al riconoscimento delle impronte "mixed" (AttackRate).

Le prestazioni di MccMatcher su DB1D sono le seguenti:

EER	**FMR100**	**FMR1000**	**ATTACCO A**		
			FMR100	**FMR1000**	**FMR10000**
0.76%	0.79%	0.93%	88.43%	83.00%	76.14%

Le combinazioni di pesi che sono state selezionate e le relative prestazioni su DB1D sono le seguenti:

Miglior riconoscimento delle impronte mixed

w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7
0.56	0.34	0	0.02	0	0	0	0.08

EER	**FMR100**	**FMR1000**	**ATTACCO A**		
			FMR100	**FMR1000**	**FMR10000**
1.07%	1.14%	2.93%	42.43%	11.71%	7.71%

Miglior mantenimento delle prestazioni nel caso generale

w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7
0.74	0.22	0	0.02	0	0	0	0.02

EER	**FMR100**	**FMR1000**	**ATTACCO A**		
			FMR100	**FMR1000**	**FMR10000**
0.84%	0.86%	0.93%	80.86%	64.43%	45.71%

Miglior TradeOff 'A'

w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7
0.58	0.3	0	0.1	0	0	0	0.02

EER	**FMR100**	**FMR1000**	**ATTACCO A**		
			FMR100	**FMR1000**	**FMR10000**
0.84%	0.86%	1.21%	83.43%	58.00%	30.57%

Miglior TradeOff 'B'

w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7
0.56	0.36	0	0.04	0	0	0	0.02

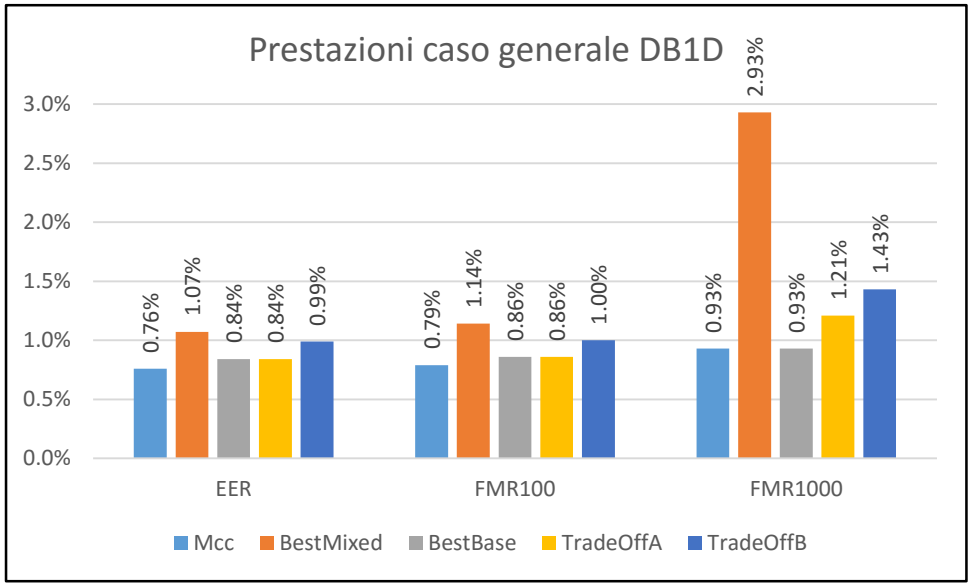
EER	**FMR100**	**FMR1000**	**ATTACCO A**		
			FMR100	**FMR1000**	**FMR10000**
0.99%	1.00%	1.43%	66.29%	38.43%	23.57%

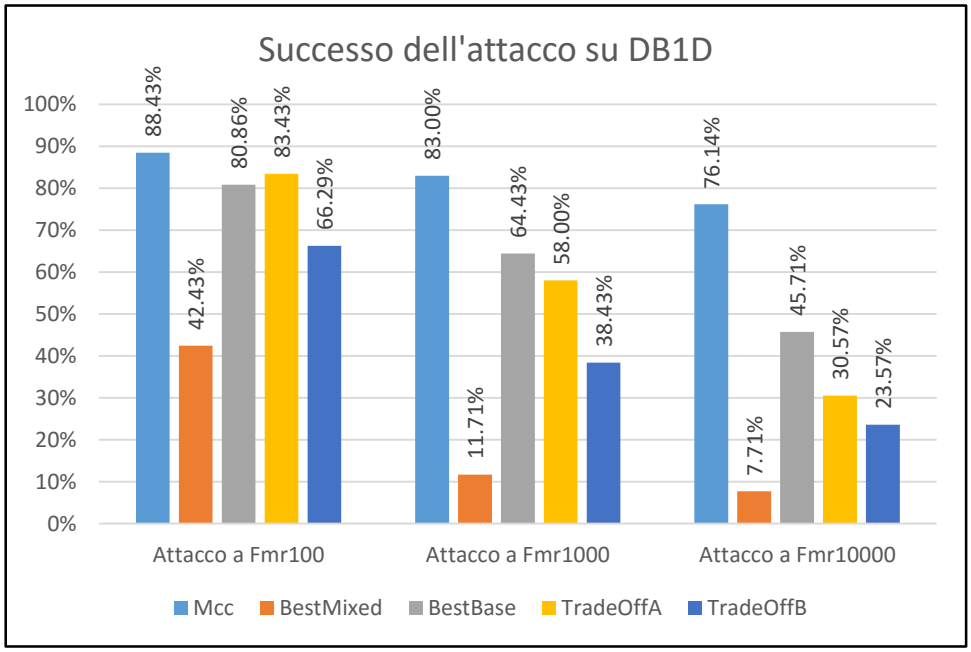
w_0 è il peso del punteggio principale ottenuto da MccMatcher, w_1 è il peso del punteggio ottenuto dalla normalizzazione di R_u, i pesi da w_2 a w_6 sono quelli relativi ai punteggi ricavati dall'osservazione delle aree ($A_1,\ A_2,\ A_3,\ A_4\ e\ A_5$) e, infine, w_7 è il peso del punteggio calcolato dall'osservazione della distribuzione globale delle minuzie.
Dalle combinazioni si può notare che le caratteristiche A_1, A_3, A_4, A_5 non sono efficaci al fine di individuare impronte "mixed".

Mediante l'uso dell'applicazione "ExecuteTest", le soglie decisionali per FMR100, FMR1000, FMR10000 e ZeroFMR sono state calcolate sul database DB1D per ognuna delle 4 combinazioni di pesi scelte. Tali soglie decisionali sono state utilizzate per calcolare le prestazioni ottenute sul database DB1C che verranno mostrate in seguito.

5.3 Confronto delle Prestazioni su DB1D

Nei seguenti grafici vengono confrontate le prestazioni sul database DB1D di MccMatcher e MixedRobustMatcher con le combinazioni di pesi precedentemente presentate.





5.4 Calcolo delle prestazioni definitive su DB1C

Le prestazioni dell'MccMatcher su questo database sono le seguenti:

EER	FMR100	FMR1000	ATTACCO A		
			FMR100	FMR1000	FMR10000
0.55%	0.54%	0.89%	91.79%	88.57%	83.57%

Esamineremo ora i valori ottenuti usando MixedRobustMatcher con le varie combinazioni di pesi e soglie calcolate precedentemente:

Miglior riconoscimento delle impronte "mixed"

EER	FMR100	FMR1000	ATTACCO A		
			FMR100	FMR1000	FMR10000
1.07%	1.13%	1.67%	51.67%	23.10%	15.71%

Miglior mantenimento delle prestazioni nel caso base

EER	FMR100	FMR1000	ATTACCO A		
			FMR100	FMR1000	FMR10000
0.70%	0.60%	0.77%	86.19%	73.33%	55.24%

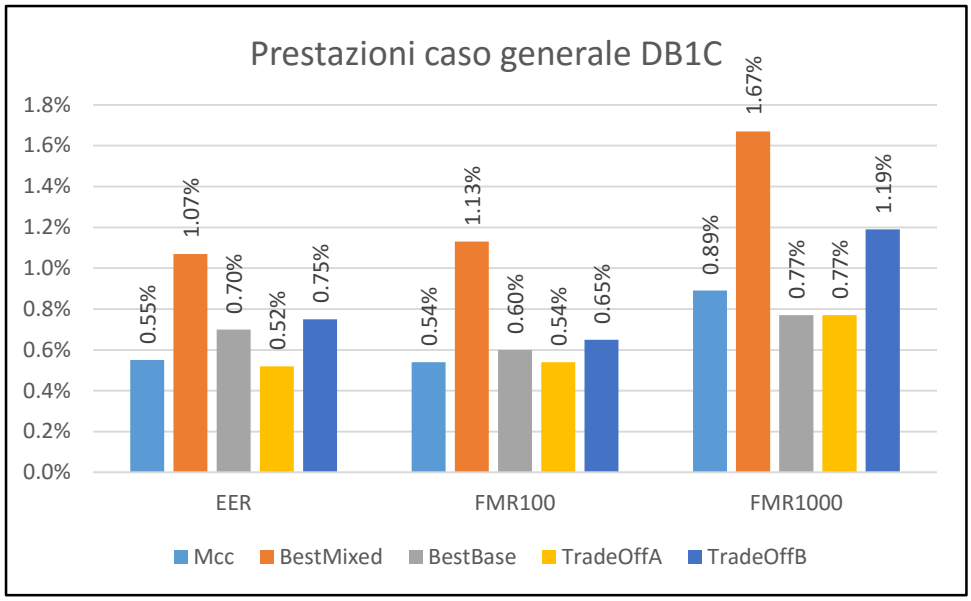
Miglior TradeOff 'A'

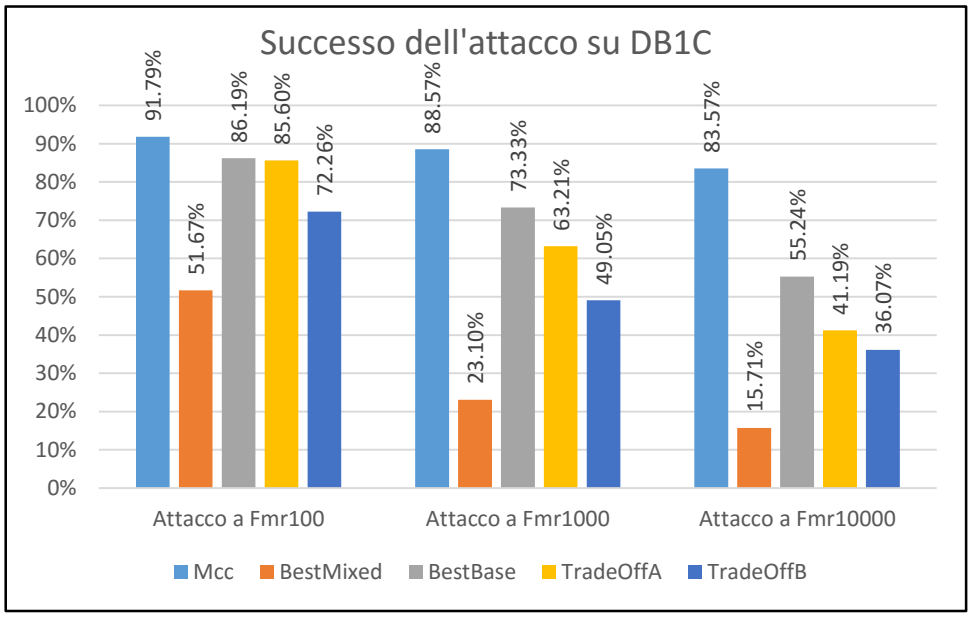
EER	FMR100	FMR1000	ATTACCO A		
			FMR100	FMR1000	FMR10000
0.52%	0.54%	0.77%	85.60%	63.21%	41.19%

Miglior TradeOff 'B'

EER	FMR100	FMR1000	ATTACCO A		
			FMR100	FMR1000	FMR10000
0.75%	0.65%	1.19%	72.26%	49.05%	36.07%

Verranno ora mostrati i grafici che confrontano i risultati ottenuti su DB1C.





Possiamo notare che, nel caso di maggior riconoscimento delle impronte “mixed” (BestMixed), si è raggiunta un’ottima riduzione di successo dell’attacco, passando da un successo nell’ 88.57% dei casi ad un decisamente ridotto 23.10%, ovviamente, a fronte di una perdita di prestazioni nel caso generale (FMR1000 da 0.89% a 1.67%) che, però, rientra nei limiti posti dalla comunità europea per questa tipologia di algoritmi di riconoscimento.

6 CONCLUSIONI

In questa tesi è stato analizzato un potenziale problema di sicurezza dei sistemi di riconoscimento di impronte digitali ed è stata proposta una possibile contromisura.

I dati ottenuti mostrano che è effettivamente possibile rendere un sistema di riconoscimento di impronte robusto rispetto all'attacco con impronte "mixed".

Sono state dapprima analizzate le caratteristiche basate sulle minuzie non accoppiate presentate in [4], procedendo poi a esaminare caratteristiche discriminanti individuate osservando le impronte mixed ed il loro processo di creazione.

Nonostante alcune delle caratteristiche discriminanti studiate e proposte non siano risultate efficaci nei casi di prova considerati, si è raggiunto un ottimo grado di individuazione delle impronte "mixed" a fronte di una ragionevole perdita di accuratezza nel riconoscimento.

Inoltre in alcuni casi, benché alcune delle caratteristiche studiate non abbiano portato particolari miglioramenti nell'individuazione delle impronte "mixed", le stesse hanno leggermente migliorato le prestazioni generali di riconoscimento.

Come è stato mostrato nel Capitolo 3, la problematica di sicurezza legata al tipo di attacco con impronte "mixed" è concreta e attuale e richiede una soluzione tempestiva. Il sistema realizzato in questo lavoro di tesi fornisce una certa protezione da questo tipo di attacchi, tuttavia si può affermare che vi siano ulteriori margini di miglioramento che potrebbero essere ottenuti con approcci differenti da quelli esaminati in questa tesi.

7 BIBLIOGRAFIA

[1] Maltoni, D., Maio, D., Jain, A., Prabhakar, S. , Handbook of fingerprint Recognition, Springer 2009

[2] M. Ferrara, A. Franco, and D. Maltoni, "The Magic Passport," in proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Clearwater, Florida, USA, 2014, pp. 1-7.

[3] http://www.griaulebiometrics.com

[4] "Unmatched minutiae: Useful Information to boost fingerprint recognition" Qing Zhang, Yilong Yin, Gongping Yang

[5] MCC matcher, Laboratorio di biometrica BioLab, Università di Bologna

[6] Clipper Library, Angus Johnson, 31 October 2014

[7] Biometric Library, Laboratorio di biometrica BioLab, Università di Bologna