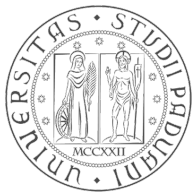


Università degli Studi di Padova

Facoltà di Ingegneria

Corso di Laurea in Ingegneria Informatica

Caratterizzazione e validazione di una applicazione prototipale per autenticazione grafica debole su Android

Laureando

Riccardo Pasqualetto

Relatore

Prof. Michele Moro

Anno Accademico 2012/2013

Alla mia famiglia

Indice

Sommario

L'obiettivo principale di questa tesi riguarda la fase di test e validazione di un'applicazione per sistemi Android, sviluppata da uno studente del corso di Laurea Magistrale, che permette di effettuare autenticazioni biometriche di tipo debole, utilizzando un algoritmo per la classificazione di disegni a mano libera, su forme suggerite. Tramite i test sull'applicazione, eseguiti con l'aiuto di alcuni utenti, utilizzando uno smartphone Android con il programma installato, si sono valutate le forme più adatte ad un'autenticazione sufficientemente robusta e il meno possibile violabile da utenti estranei.
Nella fase di test, inoltre, si sono ottenute alcune informazioni per utilizzare in modo più efficiente l'applicazione.
Per comprendere al meglio i dati e i risultati ottenuti viene fornita una sintesi dell'algoritmo utilizzato e una guida all'uso del programma.

Capitolo 1

Introduzione

I sistemi di autenticazione basati su tecniche biometriche, stanno avendo negli ultimi anni una sempre più crescente diffusione, poiché, usati da soli o a supporto di altre tecniche di autenticazione, forniscono un elevato grado di sicurezza. Attualmente però, nessun sistema riguarda il riconoscimento di un disegno a mano libera; ciò che più si avvicina a questo è il riconoscimento della firma e della scrittura a mano libera. Per questa ragione e per la forte diffusione di dispositivi dotati di touchscreen, è stata sviluppata, da parte di uno studente della Laurea Magistrale in Ingegneria Informatica, un'applicazione per dispositivi Android, con la quale è possibile effettuare delle autenticazioni biometriche basate sul riconoscimento di un semplice disegno a mano libera. L'obiettivo principale di tale progetto riguarda la creazione di un sistema di autenticazione che garantisca il più possibile l'accesso ai legittimi utenti e rifiuti gli impostori.

Dopo la creazione dell'applicazione, non era stato eseguito alcun test riguardante le forme dei disegni che risultassero più efficienti e sicure per un'autenticazione protetta da violazioni.
La ricerca di tali forme è, dunque, l'obiettivo che ci si pone in questa tesi. Per farlo è stata installata l'applicazione su uno smartphone Android, dotato di touchscreen, e si sono eseguiti alcuni test con l'aiuto di quindici persone di età differenti e con varie esperienze con smartphone o tablet touchscreen. Nel quinto capitolo verrà illustrato in dettaglio la modalità di esecuzione dei test. Non avendo accesso al codice sorgente del programma, quest'ultimo non è stato modificato in alcun modo.
Prima di dare uno sguardo ai dati ottenuti, nel secondo capitolo, si fornisce una descrizione generale sul funzionamento dei sistemi di autenticazione biometrica. Nei capitoli successivi invece, viene illustrato, in modo sintetico, l'algoritmo utilizzato e una guida pratica all'uso dell'applicazione. Per

dettagli più approfonditi sull'algoritmo, che sta alla base del programma, si rimanda alla lettura della tesi a cui si è fatto riferimento.

Capitolo 2

Sistemi biometrici

2.1 Biometria

La biometria (dal greco 'bios' = vita e 'metros' = misura), è la disciplina che studia le grandezze biofisiche o comportamentali tipiche degli organismi, allo scopo di misurarne il valore attraverso metodologie matematiche e statistiche e di indurre un comportamento desiderato in specifici sistemi tecnologici. Fra i tratti biometrici fisiologici più comuni vi sono: impronte digitali, geometria della mano, retina, iride e immagini facciali. I tratti biometrici comportamentali più comuni includono: firma, registrazioni vocali e ritmo di battuta su tastiera.

2.2 Sistema biometrico

Un sistema è detto biometrico quando è in grado di riconoscere una persona, ovvero quando riesce a verificare se un individuo è veramente colui che dichiara di essere, sulla base di caratteristiche fisiologiche e/o comportamentali. È costituito da due processi fondamentali: registrazione e riconoscimento.

2.2.1 Registrazione

Il primo processo è la registrazione (enrollment), in cui ogni nuovo utente viene registrato in un database. Viene raccolta l'informazione su una determinata caratteristica di una persona, poi solitamente questa informazione viene fatta passare attraverso un algoritmo che la trasforma in un modello (template) che possa essere immagazzinato nel database. Si noti che il sistema conserva questo template, ma non la misura biometrica originale, come ci si potrebbe aspettare. Rispetto alla misura originale del tratto biometrico,

il template possiede una quantità di informazione più limitata ma sufficiente a riassumere le caratteristiche distintive presenti nella misura originale.

2.2.2 Riconoscimento

Il secondo processo è il riconoscimento o verifica, in cui il sistema prende dagli utenti le misure necessarie, trasforma queste informazioni in un modello, usando lo stesso algoritmo con cui è stato processato il template originale, e compara il nuovo template con il database per stabilire se ci sia una corrispondenza. Il processo di riconoscimento può essere di due tipi:

1. autenticazione (o riconoscimento 1:1): l'utente confronta la sua caratteristica biometrica con il suo modello registrato nel database al momento dell'enrollment. Per fare questo, prima di identificarsi biometricamente, l'utente richiama il proprio modello digitando il codice univoco a lui associato (es. la propria matricola). La fase di riconoscimento in questo caso ha il compito di confermare l'identità di un utente specifico.

2. identificazione (o riconoscimento 1:N): l'utente si confronta con tutta la popolazione degli N utenti presenti nel sistema. Al momento del riconoscimento, il dispositivo confronta la caratteristica biometrica sottopostagli dall'utente con tutte quelle registrate all'interno del database. In questo caso la fase di riconoscimento ha il compito di cercare l'identità di un utente.

2.2.3 Errori

Nell'identificazione possiamo trovarci di fronte a due situazioni:

1. riconoscimento positivo: la persona è vera oppure è un impostore;

2. riconoscimento negativo: il sistema ha sbagliato dando un falso allarme, oppure la persona è realmente un impostore.

Gli errori che quindi possono verificarsi sono di due tipi:

1. Il sistema non riconosce una persona effettivamente autorizzata (falso negativo).

2. Il sistema accetta le persone che non sono effettivamente autorizzate (falso positivo).

2.3 FAR e FRR

Per valutare le prestazioni di un sistema biometrico, vengono utilizzati due indici: FAR (False Acceptance Rate) e FRR (False Rejection Rate), i quali rappresentano rispettivamente la frequenza delle false autenticazioni positive (falsi positivi), date dal mancato riconoscimento di un accesso non autorizzato e la frequenza delle false autenticazioni negative (falsi negativi), date da un mancato riconoscimento di una persona effettivamente autorizzata ad accedere al sistema. Nei sistemi biometrici è possibile aumentare o diminuire la sensibilità, in modo da regolare il rapporto tra falsi negativi e falsi positivi (FRR/FAR). Al variare della soglia di sensibilità del sistema, (o soglia di tolleranza) si ottiene una variazione dei due indici, in particolare con una soglia di sensibilità bassa si ha un elevato numero di falsi positivi (percentuale di FAR elevata), mentre con una soglia alta si ha un numero elevato di falsi negativi (percentuale di FRR elevata). Dunque i due indici sono tra loro inversamente proporzionali. È possibile visualizzare questo tipo di informazioni nel grafico ROC (Receiver Operating Characteristic). In ascissa troviamo i valori della soglia di sensibilità del sistema, mentre in ordinata i valori delle percentuali degli indici FAR e FRR. Possiamo notare poi, che per un certo valore della soglia, è presente un punto in cui le due curve hanno il medesimo valore, questo valore corrisponde al EER (Equal Error Rate). I valori di FAR e FRR saranno utilizzati in questa tesi per valutare e confrontare l'esito dei risultati ottenuti nei test effettuati. Nell'applicazione testata non è possibile modificare la soglia di tolleranza, poiché non è presente questa funzionalità nel programma e non si ha accesso al codice sorgente. Dunque i disegni che verranno confrontati nei vari test, presenteranno FRR e FAR calcolati con la medesima soglia di sensibilità.

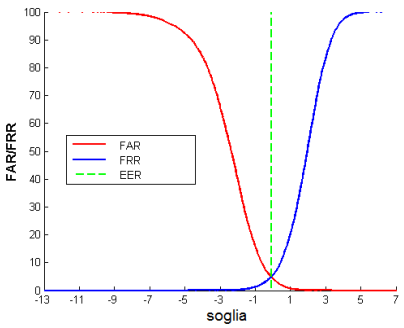


Figura 2.1: Grafico ROC

Capitolo 3

Algoritmo

Per comprendere al meglio i dati raccolti e i risultati ottenuti nei test, è utile dare uno sguardo al funzionamento all'algoritmo utilizzato dal programma.

3.1 Disegno a mano libera

Un semplice disegno a mano libera può sembrare non sicuro per un'autenticazione che sfrutta il riconoscimento grafico, in quanto potrebbe essere copiato, da chiunque, senza troppa difficoltà. L'elemento fondamentale di questo programma, è dato dal fatto che non ha importanza la forma del disegno, ma le modalità con cui lo si è tracciato. Nella fase di inserimento i parametri che vengono memorizzati dal sistema e che consentono di accettare o rifiutare un disegno (gesture) in ingresso, sono i seguenti:

1. Numero di tratti: rappresenta il numero di tratti eseguiti in ciascun disegno.

2. Coordinate x: la sequenza di numeri che rappresentano le coordinate sull'asse delle ascisse delle posizioni assunte dal dito che esegue il disegno sul touchscreen, le quali vengono memorizzate in un array di float con un periodo di campionamento di 23/24 millisecondi.

3. Coordinate y: analoga al precedente ma riferito alle coordinate sull'asse delle ordinate.

4. Il tempo: rappresenta il tempo impiegato a disegnare una gesture, cioè è la differenza tra l'ultimo e il primo valore XY campionati. Se una gesture è composta da più di un tratto, l'intervallo di tempo che intercorre tra l'uno e l'altro è trascurabile, poiché per scelte progettuali esso deve essere molto ristretto.

5. Pressione: questo parametro tiene traccia della pressione esercitata dalle dita sul touchscreen durante l'esecuzione della gesture, è costituito da un valore compreso tra zero (pressione nulla) e uno (pressione massima), campionato in maniera analoga alle coordinate X e Y.

6. Lunghezza: rappresenta la lunghezza globale della gesture, ossia è la somma delle lunghezze dei vari tratti da cui è composto un disegno.

3.2 L'algoritmo

L'algoritmo che sta alla base dell'applicazione, basato sul riconoscimento di un disegno a mano libera, sfrutta i tratti biometrici comportamentali degli utenti ed è costituito da due parti fondamentali: la registrazione e l'autenticazione. Come si è visto in precedenza (in 2.2), queste due parti costituiscono le fasi fondamentali di un sistema biometrico.

3.2.1 Registrazione

Nella procedura di registrazione (enrollment), viene richiesto inizialmente di inserire nome e cognome dell'utente; questi dati vengono salvati in una variabile stringa che verrà poi mostrata nella fase di autenticazione nel caso in cui questa andasse a buon fine. A questo punto l'utente deve tracciare un disegno, l'algoritmo richiederà di eseguirlo per almeno sei volte. La gesture può essere formata da una o più linee ma, anche se non è presente un limite superiore al numero di tratti, va tenuto presente che all'aumentare di questo numero risulta complicato riprodurre correttamente il disegno nelle successive fasi di autenticazione. Ogni disegno poi deve soddisfare due condizioni:

1. la sua lunghezza non deve essere inferiore alla soglia imposta di 1200 punti;

2. il disegno non deve essere già presente nel sistema.

Se una di queste due condizioni dovesse verificarsi, viene lanciato un messaggio di errore e l'applicazione richiederà di inserire un nuovo disegno. Dopo aver tracciato il primo disegno, se non viene segnalato alcun errore, l'applicazione crea un template per questo utente. L'algoritmo continuerà a chiedere di inserire la gesture altre cinque volte. Appena l'utente inserirà il sesto disegno, il sistema deciderà se la qualità dei campioni inseriti è buona, in caso contrario dovranno essere inseriti ulteriori disegni. Per valutare la qualità dei campioni inseriti, l'applicazione cerca di eseguire un'autenticazione

dell'utente con il sesto disegno inserito. Se esso corrisponde ai dati del medesimo utente, allora, la registrazione va a buon fine, viene salvato il template relativo all'utente, e la procedura termina. Se invece l'autenticazione del sesto disegno non va a buon fine, verranno richiesti cinque ulteriori disegni e nell'ultimo sarà eseguita nuovamente una prova di autenticazione. Se questa andrà a buon fine terminerà, altrimenti saranno richiesti altri cinque disegni.

3.2.2 Autenticazione

Nella procedura di autenticazione viene richiesto all'utente di inserire il proprio disegno, memorizzato in precedenza nella fase di registrazione. Dopo aver ricevuto l'input, il sistema lo confronta con tutte le gesture presenti in memoria e se viene trovata una corrispondenza, lancia un messaggio contenente il nome dell'utente associato a quel disegno. Se non vi è alcuna corrispondenza oppure se il disegno non è stato eseguito in modo corretto, l'applicazione lo segnalerà con un avviso indicante il mancato riconoscimento.

L'algoritmo nella procedura di comparazione del disegno, utilizza quattro fasi di controllo, ciascuna delle quali dà come risposta un valore booleano (vero o falso).

1. Numero di linee: in questa fase viene controllato se il numero di tratti del disegno inseriti nell'autenticazione, ha una corrispondenza con il numero di tratti di un template presente in memoria.

2. Coordinate XY: il sistema controlla se l'insieme dei punti del disegno appena tracciato ha una corrispondenza con un template.

3. Valori temporali: viene confrontato il tempo impiegato ad eseguire la gesture, con i tempi dei vari template presenti in memoria.

4. Valori di pressione: vengono confrontati i valori della pressione esercitata sul touchscreen durante l'esecuzione del disegno, con i valori memorizzati nei vari template.

Se uno dei controlli dà una risposta negativa, l'applicazione scarta il template che stava esaminando, procedendo con quello successivo. La procedura termina quando non sono presenti ulteriori modelli da esaminare. Se tutti e quattro i controlli vanno a buon fine, restituendo un valore booleano vero, significa che è stata trovata una corrispondenza con uno dei template presenti in memoria.

Ogni qualvolta un'autenticazione va a buon fine, avviene un'operazione di aggiornamento, ossia, il template presente in memoria, viene sostituito dal disegno appena inserito.

3.3 Soglia

La soglia di tolleranza del sistema è stata imposta in fase di progettazione e non è modificabile durante l'utilizzo dell'applicazione. Tale soglia rimarrà pertanto invariata per tutte le prove che si effettueranno nella fase di test. Il programmatore ha scelto, ai fini della sicurezza, di impostare la soglia in modo da permettere di ottenere un più alto numero di falsi negativi rispetto ad un alto numero di falsi positivi.

Capitolo 4

Guida applicazione

Nei paragrafi seguenti, viene fornita una guida all'uso dell'applicazione, con le immagini delle varie schermate che l'utente potrà visualizzare durante l'utilizzo. Come già visto in precedenza, sono presenti due procedure principali: Registrazione e Autenticazione.

4.1 Schermata Principale

All'avvio dell'applicazione, viene mostrata una schermata dove è possibile scegliere con quale delle due procedure si vuole cominciare: ciò avviene tramite la semplice pressione dei tasti Enrollment e Autentication. Ovviamente se l'utente si trova al primo avvio dopo l'installazione dell'applicazione, in memoria non è presente alcuna gesture, per cui sarà necessario eseguire innanzitutto una procedura di Enrollment.

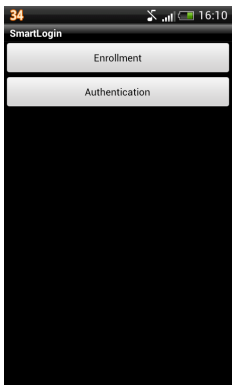


Figura 4.1: Schermata Principale

4.2 Enrollment

La fase di registrazione inizia con una schermata dove sono presenti due campi di immissione testo: entrambi devono essere obbligatoriamente completati con delle stringhe di caratteri (nome e cognome dell'utente) per poter proseguire, premendo il tasto 'Done' si passa alla seconda schermata.(Figura 4.2) A questo punto l'applicazione richiede di inserire la propria gesture, che è bene venga eseguita nel modo più naturale possibile, per essere in grado di riprodurla in modo efficace nella fase di autenticazione. Per confermare e continuare la procedura è necessario premere il tasto 'Done'. Se non viene riportato alcun messaggio d'errore, eventualmente causato da una lunghezza del disegno inferiore alla soglia minima stabilita oppure dalla presenza in memoria di un'identica gesture, verrà richiesto (si veda 3.2.1) di inserire il disegno almeno altre cinque volte.
Se invece si è commesso un errore nel disegnare la gesture è possibile scartare la stessa premendo il tasto 'Discard', ponendo attenzione al fatto che, una volta premuto, si perderanno tutti i dati inseriti fino a quel momento, compresi i dati inseriti nella prima schermata, e si verrà riportati alla Schermata Principale (figura 4.1).

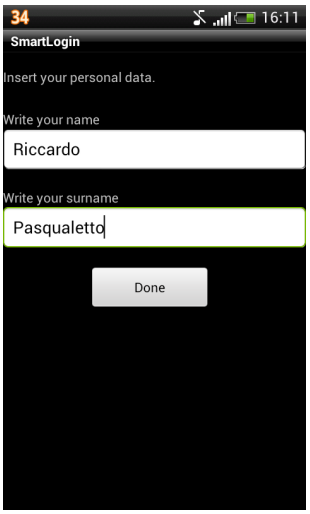


Figura 4.2: campi di testo

Figura 4.3: gesture inserita

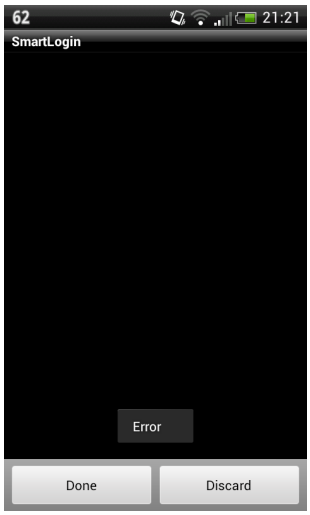


Figura 4.4: errore

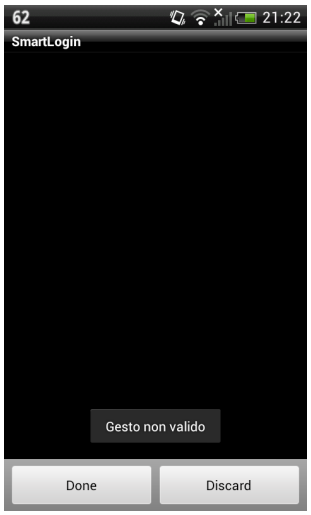


Figura 4.5: gesto non valido

4.3 Authentication

Nella prima e unica schermata della fase di autenticazione (è la stessa presente nella fase di registrazione, figura 4.3), è possibile inserire la propria gesture, cercando di ricrearla il più possibile simile a quella inserita in fase di registrazione, in termini di velocità di esecuzione, forma e pressione esercitata sul touchscreen. Per completare la procedura è necessario premere il tasto Done. A questo punto, se il disegno è stato eseguito nel modo corretto, verrà mostrato un messaggio contenente il nome dell'utente(figura 4.7) a cui era stato associato quel disegno nella fase di registrazione, in caso contrario verrà mostrato un messaggio di mancato riconoscimento della gesture: Gesto non riconosciuto (figura 4.6).

Se nell'inserimento del disegno si è commesso un errore, è possibile scartare lo stesso premendo il tasto Discard, i dati inseriti verranno cancellati e si verrà riportati alla schermata principale dell'applicazione (figura 4.1).

4.4 File Gestures

Tutti i disegni memorizzati in fase di registrazione, vengono salvati in un file nominato Gestures(figura 4.8), lo si può trovare nella directory principale della memory card dello smartphone. Ogni volta che viene inserita una nuova gesture, il file omonimo viene aggiornato. Se dovesse essere necessa-

rio esportare su un altro dispositivo o si volessero eliminare dallo stesso le gesture memorizzate, è possibile agire di conseguenza su questo file.

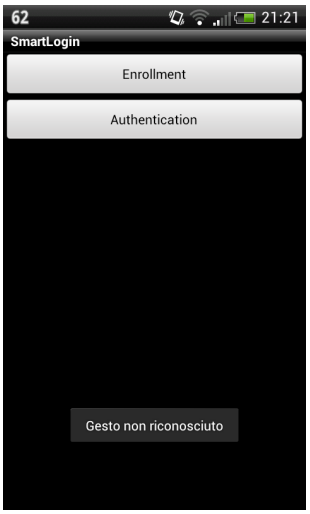


Figura 4.6: non riconosciuta

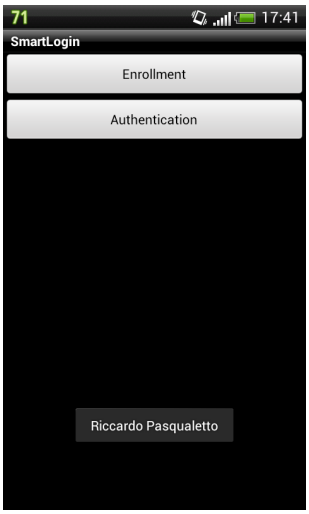


Figura 4.7: riconosciuta

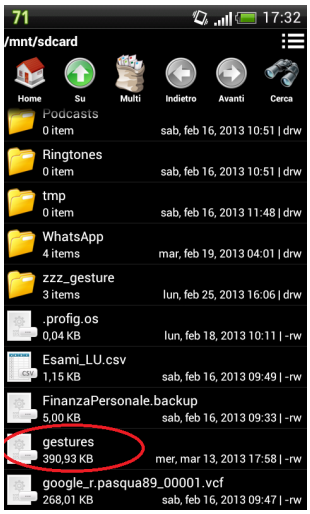


Figura 4.8: file gestures

Capitolo 5

Test

Dopo aver dato uno sguardo generale al programma e all'algoritmo utilizzato dallo stesso, in questo capitolo viene trattato l'argomento essenziale della tesi, ossia la valutazione di quelle forme che più risultano affidabili ai fini di un'autenticazione biometrica, tramite l'inserimento di un disegno a mano libera, sicura e il meno possibile violabile. Per un confronto e una valutazione dei risultati, sono stati calcolati per ogni figura il numero di Falsi positivi e negativi accettati in fase di autenticazione, utilizzando rispettivamente FAR e FRR.

I test sono stati eseguiti utilizzando uno smartphone HTC Desire S, con piattaforma Android versione 4.0 Ice Cream Sandwich.

5.1 Figure

Come primo passo è stato valutato quali tipi di figure utilizzare nei test. Sono state individuate alcune 'classi' di simboli che possono rispecchiare le gesture che un comune utente potrebbe decidere di utilizzare per la propria registrazione e successivamente autenticazione. Le classi scelte sono tre:

1. Simboli conosciuti
2. Lettere
3. Simboli inventati

I simboli, in ciascuna classe, presentano tra loro diversi gradi di difficoltà, dati dalla complessità del disegno, che si ottiene con l'aumentare del numero di lati, con una maggior presenza di linee curve e/o cambi di direzione. Vi

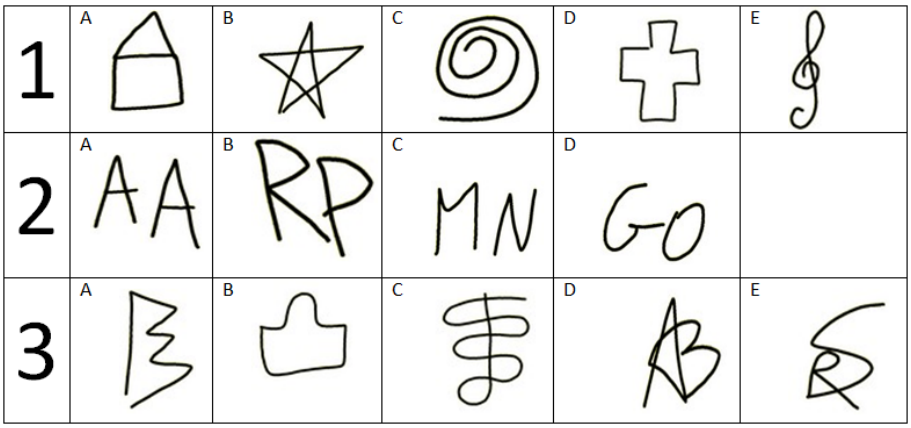


Figura 5.1: classi di simboli

è un limite inferiore alla complessità del disegno, dato da un vincolo giustamente presente nell'applicazione, il quale non permette di disegnare una gesture troppo semplice (si veda 3.2.1). Si vuol far notare che gli ultimi due simboli della classe 'simboli inventati', sono costituiti da due lettere eseguite con un unico tratto e sovrapposte tra loro in un modo particolare.

5.2 Fase di test

5.2.1 Osservazioni preliminari

Nella fase di registrazione è necessario disegnare le gesture nel modo più naturale possibile e in assenza di fattori di disturbo esterni, poiché solo in questo modo sarà possibile riprodurle correttamente ogni qualvolta si effettui un'autenticazione, anche dopo giorni, settimane o mesi. Si osserva però che se un disegno non viene eseguito per un po' di tempo, nelle prime fasi di autenticazione, è molto probabile che, nel tracciare il disegno, si commetta qualche errore in più rispetto alla media. Circa dopo cinque autenticazioni di prova, il numero di autenticazioni positive raggiunge la normalità, cioè raggiunge i valori di FRR (falsi negativi) riportati nelle tabelle in 5.2.3.

Ho eseguito alcuni test di disegno di una figura non troppo complessa (disegno 1A, figura 5.1), eseguendo i vari tratti a velocità diverse e in modo differente da come avrei fatto normalmente. Successivamente ho eseguito dieci autenticazioni ottenendo due rifiuti (falsi negativi). Eseguendo le dieci autenticazioni qualche giorno più tardi, i falsi negativi erano aumentati a sei, dopo circa due settimane non riuscivo ad eseguire alcuna autenticazione

positiva con tale gesture. Va invece rimarcato che lo stesso disegno, tracciato in fase di registrazione nel modo più naturale possibile, dopo un paio di mesi, consente di ottenere, dopo alcune prove di tracciamento iniziali, solamente un falso negativo su dieci. Ho notato poi che, se si presentano agenti esterni di disturbo, ad esempio quando si viaggia su un mezzo pubblico, in equilibrio precario o in presenza di vibrazioni rilevanti, i disegni, soprattutto quelli composti da molti lati, non vengono quasi mai riconosciuti in modo corretto, provocando numerosi falsi negativi. In tali situazioni, infatti, pressione e velocità di esecuzione possono variare rispetto al solito a causa dei fattori di disturbo. Un altro elemento che condiziona la percentuale di autenticazioni negative, cioè la percentuale di falsi negativi (FRR), è la posizione in cui si tiene lo smartphone nel processo di registrazione e successivamente autenticazione. In una fase preliminare dei test avevo eseguito tutte le forme tenendo lo smartphone appoggiato su di un tavolo. Successivamente andando ad eseguire le autenticazioni, tenendo lo smartphone in mano, non ottenevo alcuna risposta positiva da parte del sistema, contrariamente a quanto verificato con lo stesso posato su di un tavolo. Si presenta questa situazione, poiché, la pressione esercitata sullo schermo, nelle due modalità di inserimento descritte, è differente. Affinchè la gesture venga riconosciuta nella fase di autenticazione, è dunque necessario eseguire il disegno con la medesima pressione esercitata in fase di registrazione. Per fare ciò è opportuno quindi mantentere lo smartphone nella stessa posizione in entrambe le fasi.

5.2.2 Esecuzione

I test sono stati eseguiti con persone dai 14 ai 55 anni, maschi e femmine, con differenti esperienze con i touchscreen. Prima di iniziare le prove, ho inserito in memoria le varie figure sopra esposte. Tramite la procedura di registrazione, ogni figura è stata associata ad un diverso nome, come se più utenti si fossero registrati. Successivamente ho effettuato dieci autenticazioni di prova per ciascun disegno, ogni autenticazione non riuscita coincide con un falso negativo, i dati ottenuti sono riportati nelle tabelle (vedi 5.2.3) nella colonna FRR.

All'inizio della fase di test ho chiesto alle persone sottoposte alle prove, di cercare di riprodurre alcuni dei disegni, due per ciascuna classe (in particolare i disegni: 1A, 1B, 2A, 2B, 3D, 3E, si veda figura 5.1), dopo aver solamente mostrato loro le immagini con le forme delle gesture. Dopo alcune prove, l'unico disegno che qualcuno è riuscito a riprodurre in modo corretto, ottenendo una risposta positiva nell'autenticazione, cioè un falso positivo, è stata la stella. In particolare solo due persone su quindici hanno tracciato

correttamente la gesture: in entrambi i casi si sono registrati 4 falsi positivi su 10 tentativi. Gli altri disegni non sono stati in alcun caso riprodotti correttamente, cioè non si è verificato alcun falso positivo. Il risultato di questa prima prova è interessante se messo in relazione con i dati raccolti in seguito e dà conferma del fatto che non sia importante solamente la forma del disegno, ma le modalità con cui lo si è tracciato.

Successivamente ogni persona è stata informata su come eseguire nel modo corretto i vari disegni in termini di velocità di esecuzione, numero di tratti e pressione da esercitare sul touchscreen. Prima di iniziare a tenere traccia delle autenticazioni riuscite, ogni persona ha eseguito 5 prove di autenticazione, nella quale era possibile comprendere al meglio le istruzioni fornitegli ed eventualmente correggere alcuni gesti sbagliati. Infine ogni utente ha eseguito 10 prove di autenticazione per ogni disegno, ogni volta che un'autenticazione andava a buon fine, veniva segnato un falso positivo.

5.3 Dati raccolti

A seguire si possono trovare le tabelle con i dati raccolti durante i test, esse presentano nella prima riga una sigla, corrispondente ad una delle gesture riportate nella figura 5.1 e la percentuale di falsi negativi (FRR) ottenuti con quella gesture, calcolati effettuando 10 prove di autenticazione. Gli utenti sono stati numerati da 1 a 15, ogni numero corrisponde allo stesso utente anche nelle diverse tabelle. Nella colonna denominata 'touch', è stato indicato con un 'si' se l'utente possedeva una buona esperienza con i touchscreen, in caso contrario si è inserito un 'no'. Nella colonna FAR si è indicata la percentuale di falsi positivi ottenuti da ciascun utente in 10 prove di autenticazione. L'ultima riga di ciascuna tabella presenta la media di tutti i valori dell'indice FAR dei vari utenti.

1A		FRR: 10%	
User	**Età**	**Touch**	**FAR%**
1	18	si	50
2	24	si	20
3	20	no	0
4	23	si	20
5	20	no	10
6	28	no	80
7	14	si	100
8	31	si	60
9	29	si	40
10	51	no	10
11	55	no	20
12	16	si	0
13	43	si	20
14	37	si	40
15	27	no	30
FAR% medio:			**33,33**

1B		FRR: 0%	
User	**Età**	**Touch**	**FAR%**
1	18	si	90
2	24	si	50
3	20	no	0
4	23	si	50
5	20	no	10
6	28	no	70
7	14	si	0
8	31	si	60
9	29	si	50
10	51	no	50
11	55	no	40
12	16	si	20
13	43	si	40
14	37	si	70
15	27	no	30
FAR% medio:			**42,00**

1C		FRR: 20%	
User	**Età**	**Touch**	**FAR%**
1	18	si	50
2	24	si	40
3	20	no	0
4	23	si	60
5	20	no	0
6	28	no	60
7	14	si	40
8	31	si	20
9	29	si	20
10	51	no	0
11	55	no	0
12	16	si	0
13	43	si	40
14	37	si	50
15	27	no	0
FAR% medio:			**25,33**

1D		FRR: 30%	
User	**Età**	**Touch**	**FAR%**
1	18	si	20
2	24	si	10
3	20	no	0
4	23	si	20
5	20	no	0
6	28	no	30
7	14	si	10
8	31	si	20
9	29	si	40
10	51	no	0
11	55	no	0
12	16	si	10
13	43	si	0
14	37	si	10
15	27	no	0
FAR% medio:			**11,33**

1E		FRR: 20%	
User	**Età**	**Touch**	**FAR%**
1	18	si	10
2	24	si	10
3	20	no	30
4	23	si	0
5	20	no	0
6	28	no	0
7	14	si	0
8	31	si	10
9	29	si	10
10	51	no	0
11	55	no	0
12	16	si	0
13	43	si	0
14	37	si	0
15	27	no	10
FAR% medio:			**5,33**

3C		FRR: 10%	
User	**Età**	**Touch**	**FAR%**
1	18	si	40
2	24	si	20
3	20	no	0
4	23	si	20
5	20	no	0
6	28	no	0
7	14	si	0
8	31	si	10
9	29	si	20
10	51	no	0
11	55	no	0
12	16	si	0
13	43	si	10
14	37	si	20
15	27	no	10
FAR% medio:			**10,00**

3A		FRR: 20%	
User	**Età**	**Touch**	**FAR%**
1	18	si	30
2	24	si	20
3	20	no	40
4	23	si	10
5	20	no	0
6	28	no	50
7	14	si	10
8	31	si	40
9	29	si	20
10	51	no	50
11	55	no	10
12	16	si	0
13	43	si	20
14	37	si	30
15	27	no	0
FAR% medio:			**22,00**

3B		FRR: 20%	
User	**Età**	**Touch**	**FAR%**
1	18	si	30
2	24	si	0
3	20	no	10
4	23	si	20
5	20	no	0
6	28	no	0
7	14	si	20
8	31	si	30
9	29	si	30
10	51	no	20
11	55	no	0
12	16	si	0
13	43	si	10
14	37	si	20
15	27	no	10
FAR% medio:			**13,33**

2A		FRR: 0%	
User	**Età**	**Touch**	**FAR%**
1	18	si	60
2	24	si	0
3	20	no	10
4	23	si	40
5	20	no	0
6	28	no	30
7	14	si	20
8	31	si	60
9	29	si	30
10	51	no	40
11	55	no	40
12	16	si	0
13	43	si	20
14	37	si	50
15	27	no	10
FAR% medio:			**27,33**

2B		FRR: 10%	
User	**Età**	**Touch**	**FAR%**
1	18	si	60
2	24	si	0
3	20	no	0
4	23	si	60
5	20	no	0
6	28	no	60
7	14	si	20
8	31	si	10
9	29	si	0
10	51	no	20
11	55	no	70
12	16	si	10
13	43	si	30
14	37	si	10
15	27	no	0
FAR% medio:			**23,33**

2C		FRR: 20%	
User	**Età**	**Touch**	**FAR%**
1	18	si	40
2	24	si	60
3	20	no	0
4	23	si	20
5	20	no	0
6	28	no	0
7	14	si	30
8	31	si	40
9	29	si	50
10	51	no	30
11	55	no	10
12	16	si	0
13	43	si	20
14	37	si	30
15	27	no	0
FAR% medio:			**22,00**

3D		FRR: 20%	
User	**Età**	**Touch**	**FAR%**
1	18	si	50
2	24	si	10
3	20	no	0
4	23	si	10
5	20	no	0
6	28	no	40
7	14	si	20
8	31	si	20
9	29	si	10
10	51	no	0
11	55	no	0
12	16	si	0
13	43	si	0
14	37	si	30
15	27	no	0
FAR% medio:			**12,67**

2D		FRR: 10%	
User	**Età**	**Touch**	**FAR%**
1	18	si	10
2	24	si	80
3	20	no	0
4	23	si	40
5	20	no	0
6	28	no	0
7	14	si	0
8	31	si	60
9	29	si	20
10	51	no	30
11	55	no	30
12	16	si	10
13	43	si	20
14	37	si	30
15	27	no	0
FAR% medio:			**22,00**

3E		FRR: 10%	
User	**Età**	**Touch**	**FAR%**
1	18	si	30
2	24	si	20
3	20	no	0
4	23	si	20
5	20	no	0
6	28	no	10
7	14	si	0
8	31	si	0
9	29	si	10
10	51	no	0
11	55	no	30
12	16	si	0
13	43	si	20
14	37	si	30
15	27	no	0
FAR% medio:			**11,33**

5.4 Risultati

È stato valutato che 10 prove di autenticazione per ciascun disegno fossero sufficienti, poiché, già in questo modo, ogni persona era sottoposta ad un totale di 140 autenticazioni, un numero maggiore avrebbe sicuramente portato a cali di attenzione e concentrazione, compromettendo i risultati dei test e lo sforzo richiesto poteva non essere sopportato da tutti.

Si vuole ricordare innanzitutto che ai fini della sicurezza è positivo il fatto che si ottengano dei valori di FAR bassi, poiché sta a significare che un utente estraneo riesce a violare il sistema, effettuando autenticazioni con esito positivo, in pochi casi. Allo stesso modo è positivo il fatto che si ottengano dei valori di FRR bassi, poiché in questo caso l'utente legittimo viene riconosciuto nella maggior parte dei casi, ottenendo poche autenticazioni negative, cioè pochi falsi negativi.

Durante l'esecuzione dei test, molte persone facevano notare la difficoltà ad eseguire alcuni simboli in un determinato modo, differente da come lo avrebbero disegnato di solito, in particolare con le lettere. Alcuni di questi, molto spesso, nell'inserimento del disegno, sforzandosi di eseguire le istruzioni impartitegli, involontariamente lo tracciavano secondo il proprio stile. Coloro i quali, con determinate figure, hanno ottenuto numerose autenticazioni positive, hanno fatto notare che la modalità con cui dovevano tracciare le stesse, era simile a come essi stessi le avrebbero tracciate e quindi le avevano riprodotte facilmente, ottenendo un elevato numero di falsi positivi. Si è riscontrato poi che, tra le persone che non avevano esperienze di touchscreen,

alcune si sono trovate un po' impacciate nell'esecuzione di gran parte dei simboli. Uno dei fattori che determina la riuscita o meno di un'autenticazione, è dato dalla pressione esercitata sul touchscreen, differente da persona a persona e probabilmente dato dal modo in cui un utente muove la mano e le dita sul touchscreen. A tal proposito sono stati riscontrati fondamentalmente due modi di tracciare i disegni:

1. La mano sta ferma, solo il dito si muove per eseguire il disegno.

2. È la mano che si muove e il dito la segue nei movimenti per tracciare il disegno.

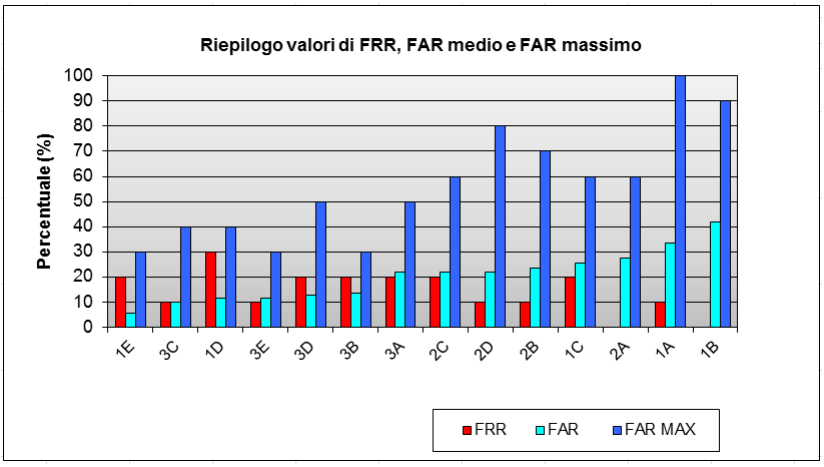
Le gesture sono state memorizzate, dal sottoscritto, seguendo il secondo di questi due metodi. Chi ha eseguito, nella fase di test, i disegni nel primo modo, ha ottenuto poche autenticazioni positive, cioè un numero di falsi positivi molto basso (valori dell'indice FAR bassi).

I simboli inventati sono quelli che hanno creato più 'problemi' a chi si è sottoposto ai test. Con queste figure, cioè, si sono ottenuti pochi falsi positivi, dunque dei bassi valori di FAR. Tali figure quindi, come si osserva nel prossimo paragrafo, risultano vincenti ai fini di un adeguato livello di sicurezza.

5.5 Figure più sicure

Dando uno sguardo alle tabelle con i dati raccolti, per determinare le figure più sicure per un'autenticazione biometrica, è opportuno confrontare i valori di FRR e FAR. Per la sicurezza è innanzitutto preferibile scegliere un simbolo avente l'indice di FAR più basso, poiché esso misura il numero di accessi al sistema da parte di un utente diverso da colui che ha registrato il disegno, cioè il numero di falsi positivi. Le varie gesture hanno degli indici di FRR abbastanza simili, saranno valutate quindi le figure con il più basso FAR; se due figure possiedono lo stesso indice FAR, in ogni caso, sarà da preferire quella con un minore indice FRR. Di seguito è riportata una tabella riassuntiva ordinata in modo crescente, secondo i valori dell'indice FAR medio e un grafico contenente i medesimi valori. Ai primi posti, dunque, troviamo i simboli più adatti ad un'autenticazione sufficientemente sicura e protetta da violazioni. Nella colonna FAR% massimo, è indicato il valore del FAR più alto ottenuto da un utente eseguendo le prove su quella determinata gesture.

SIMBOLI		FRR %	FAR %	FAR MAX %
1E		20	5,33	30
3C		10	10,00	40
3E		10	11,33	30
1D		30	11,33	40
3D		20	12,67	50
3B		20	13,33	30
2D		10	22,00	80
3A		20	22,00	50
2C		20	22,00	60
2B		10	23,33	70
1C		20	25,33	60
2A		0	27,33	60
1A		10	33,33	100
1B		0	42,00	90



Vediamo come le figure appartenenti alla classe dei 'simboli inventati' si trovino ai primi posti, dunque con una frequenza di falsi positivi più bas-

sa. Insieme a queste però troviamo due simboli appartenenti alla classe dei 'simboli conosciuti': 'chiave di violino'(1E) e 'croce'(1D). Rispetto agli altri simboli conosciuti però, presentano alcune difficoltà in fase di riproduzione. Di seguito vengono brevemente descritte. La 'croce', presenta un discreto numero di lati, motivo per il quale è risultato difficile, da parte degli utenti, riprodurlo in maniera corretta, nonostante conoscessero la figura. Ho riscontrato anch'io una certa difficoltà ad ottenere dei risultati positivi nelle autenticazioni, registrando infatti un FRR del 30%, il più alto tra le figure selezionate. All'aumentare dei lati aumenta la probabilità di incorrere in errori di inserimento, in termini di pressione esercitata sul touchscreen e di velocità di esecuzione dei lati della figura. Per tale motivo, si sconsiglia l'utilizzo di figure aventi un numero di lati maggiore a dieci. La 'chiave di violino', sebbene sia un simbolo conosciuto, è risultata la più complessa da riprodurre. Molti utenti che si sono sottoposti al test, non avevano mai disegnato tale figura, infatti hanno riscontrato notevoli difficoltà in fase di inserimento; per questo motivo tale simbolo può essere associato alla classe dei 'simboli inventati'. Chi sapeva disegnare la figura, in tutti i casi aveva una modalità di tracciamento differente dalla mia. Si sono riscontrate comunque delle difficoltà nel disegnarlo, ottenendo una percentuale di falsi positivi molto bassa. Il disegno presenta un unico tratto, alcuni cambi di direzione e linee curve, tali da rendere la figura non facilmente riproducibile, anche dopo un'attenta spiegazione su come eseguirla. Ciò che compromette un'autenticazione positiva, è la velocità con cui devono essere tracciate le linee, e la pressione da esercitare sul touchscreen. A metà classifica troviamo le lettere, tutte all'incirca con la stessa percentuale di FAR medio. Come spiegato nella sezione 5.3, tale risultato è dato dal fatto che non è stato facile, per chi si è sottoposto ai test, adattarsi alle istruzioni impartitegli per tracciare le lettere, alcuni sono stati in grado di inserirle con facilità, trovando un'analogia tra il mio modo di disegnarle ed il loro, ottenendo molti falsi positivi (FAR elevato). Altri invece hanno riscontrato non poche difficoltà, ottenendo un basso numero di falsi positivi. Questa situazione si può riscontrare osservando la colonna indicante il FAR massimo, pur essendoci un FAR medio di circa il 23%, presenta delle percentuali che si aggirano tra il 60% e l' 80%. Agli ultimi posti troviamo i simboli conosciuti, i quali presentano un'analogia con le difficoltà di riproduzione delle lettere, per le modalità di tracciamento diverse da persona a persona. Avendo però una difficoltà di esecuzione minore, sono risultati mediamente più facili da riprodurre, con un conseguente numero di falsi positivi più elevato.

Le figure più sicure e quindi da preferire per un'autenticazione biometrica protetta da violazione, risultano essere quelle della classe dei 'simboli inventati'. Esse infatti presentano un FAR medio e un FAR massimo più basso,

rispetto alle altre classi di simboli. Ciò significa che rispetto agli altri simboli scelti, oltre a presentare mediamente un minor numero di falsi positivi, nessun utente è riuscito ad eseguirli in modo corretto più del 40% delle volte, cioè il FAR massimo è non superiore al 40%.

Ai fini della sicurezza si può dire che siano stati raggiunti dei risultati molto soddisfacenti, dato che un intruso difficilmente riesce a scoprire le modalità precise di tracciamento delle gesture, in termini di pressione da esercitare, velocità e forma delle stesse. Senza queste informazioni è praticamente impossibile riprodurre un disegno e ottenere un'autenticazione positiva. Come visto in 5.2.2, anche solamente conoscendo la forma precisa del disegno nessun utente, che si è sottoposto ai test, è riuscito ad autenticarsi con successo, se non nell'unico caso di una forma molto semplice.

Capitolo 6

Conclusioni

Lo scopo principale della tesi era quello di individuare le figure che risultassero più adatte ad un'autenticazione biometrica sufficientemente protetta da violazioni esterne. Nella fase di test sono stati riscontrati alcuni accorgimenti, che vengono di seguito riproposti, da tenere nella fase di registrazione di una gesture:

1. è essenziale disegnare la gesture nel modo più naturale possibile, per poter riprodurre il disegno anche dopo molto tempo dal primo inserimento;

2. è importante che la posizione assunta dal dispositivo in fase di inserimento del disegno sia la stessa del primo inserimento effettuato in fase di registrazione, se poggiato ad esempio su un tavolo la pressione varia rispetto a quando lo si tiene in mano, compromettendo i risultati nella fase di autenticazione;

3. è opportuno non eseguire figure con un numero di lati troppo elevato, l'aumento di questo, accresce il verificarsi di falsi negativi in fase di autenticazione, soprattutto dopo che è passato diverso tempo dalla fase di registrazione.

4. un altro fattore che può compromettere un'autenticazione positiva è la presenza di agenti di disturbo esterni, ad esempio viaggiando su un mezzo pubblico in presenza di forti vibrazioni o in equilibrio precario, nella fase di inserimento la correttezza della velocità di esecuzione della gesture e della pressione esercitata sul touchscreen possono essere compromesse.

Dal confronto dei risultati ottenuti, si evince che le figure che si addicono di più alle esigenze di sicurezza ricercate, sono quelle appartenenti alla classe

dei 'simboli inventati'. L'aspetto rilevante sul grado di sicurezza che si può ottenere con tali figure è che, impartendo agli utenti che si sono sottoposti ai test, istruzioni precise sulle modalità di tracciare i disegni, in termini di velocità di esecuzione, forma e pressione, si sono ottenute delle percentuali di falsi positivi che si aggirano tra il 10% e il 13%. Le stesse figure invece, non fornendo istruzioni in merito alle modalità di tracciamento, ma solo mostrando un'immagine delle stesse, non hanno presentano alcun falso positivo in fase di autenticazione da parte degli utenti sottoposti al test. Perciò se anche qualcuno scoprisse la forma del disegno, non sarebbe in grado di ottenere un'autenticazione positiva, senza possedere le istruzioni precise sulla modalità di tracciamento. Risulta molto difficile, per un estraneo, riuscire a scoprire tali informazioni, ciò assegna quindi un adeguato grado di sicurezza al sistema di autenticazione.
Abbinando questo sistema di autenticazione biometrico, che sfrutta il riconoscimento di un disegno a mano libera, ad un altro tipo di sistema di autenticazione, ad esempio che sfrutti l'inserimento di una password, si potrebbe raggiungere un livello di sicurezza molto elevato.

Bibliografia

[1] Alessandro Casasola. Tesi Laurea Magistrale in Ingegneria Informatica: DISTINGUISHING FREEHAND DRAWING RECOGNITION FOR BIOMETRIC AUTHENTICATION ON ANDROID-POWERED MOBILE DEVICES.

[2] Enciclopedia della Scienza e della Tecnica. 'Biometria'