UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Tema d'anno
Sistemi Biometrici

Gabriele Patta
AA. 2022-2023

Indice

1. Premessa 3

2. Studio di fattibilità 4

2.1 Introduzione 4

2.2 Identificazione ed analisi dei requisiti 5

2.3 Tempistiche 7

2.3.1 Panoramica dei costi 8

3. Sviluppo del progetto 9

3.1 Soluzioni commerciali esistenti 9

3.2 Casi d'uso 20

3.3 Il riconoscimento biometrico 21

3.4 Algoritmo 23

3.5 Valutazione delle prestazioni 24

3.6 Analisi dei risultati sperimentali 26

Bibliografia 30

Capitolo 1

Premessa

In merito alla realizzazione del progetto relativo allo svolgimento del tema d'anno, dell'insegnamento di Sistemi biometrici con riferimento all'anno accademico 2021-2022, il presente elaborato intende fornire un quadro preliminare per portare a compimento il suddetto progetto.

L'esecuzione del progetto prevede l'impiego di sistemi di riconoscimento biometrici. Questa tipologia di sistemi rappresenta dei sistemi informatici che riconoscono una persona, determinando la corrispondenza di uno specifico aspetto fisico o comportamentale posseduto da un individuo. In riferimento all'idea progettuale, pertanto, l'obiettivo che si intende raggiungere è quello della messa in opera di molteplici sistemi di riconoscimento biometrico, all'interno di una abitazione domestica per incrementare la sicurezza relativa agli accessi della stessa.

Tali sistemi di riconoscimento biometrico, dovranno pertanto essere integrati, congiuntamente ad alcuni serramenti preesistenti.

Capitolo 2

Studio di fattibilità

2.1 Introduzione

L'effettuazione di uno studio di fattibilità, risponde alla necessità di approfondire e sviluppare un'ipotesi di progetto. Le ipotesi di progetto possono nascere all'interno di processi ben consolidati, come il processo di pianificazione, oppure di più generali iniziative di cambiamento, ad esempio, programmi di miglioramento continuo, reingegnerizzazioni dei processi esistenti o ristrutturazioni organizzative. Le ipotesi di progetto nascono inevitabilmente generiche e non sufficientemente verificate e valutate. Affinché il progetto possa effettivamente essere realizzato è necessario sviluppare l'idea progettuale su piani differenti.

Le finalità generali devono concretizzarsi in specifici risultati attesi, la soluzione prevista deve essere approfondita fino ad individuare un insieme dettagliato di prodotti e servizi da acquisire, dovranno essere presenti anche ipotesi sui tempi di realizzazione, nonché delle stime iniziali dei costi da intraprendere, al fine di poter stimare l'onere economico e il tempo complessivo di durata per il completamento.

Nelle fasi preliminari del progetto che si intende realizzare, quando le risorse in gioco sono ancora limitate e riguardano solo ricerche è altresì possibile realizzare semplici prototipi o sperimentazioni, al fine di apprezzare maggiormente le valutazioni effettuate. Una volta concluso tale studio di fattibilità, attraverso gli elementi messi in evidenza dallo stesso, la decisione di intraprendere il progetto in esame sarà più chiara e semplice.

2.2 Identificazione ed analisi dei requisiti

La necessità di definire i progetti e formalizzarli secondo uno schema comune, condiviso e predefinito, vale per tutti i progetti di informatizzazione, tuttavia la necessità di un vero e proprio studio di fattibilità è indicata quando siano presenti rischi significativi. Per questo motivo lo studio di fattibilità, nasce sempre in presenza di una "idea progettuale" già esistente, che ha già individuato, gli elementi essenziali della questione, l'area di intervento, le principali iniziative previste, nonché gli obiettivi di fondo.

In questa fase preliminare, si procede ad identificare dapprima l'insieme dei requisiti utente, ovvero le esigenze per cui si intende realizzare tale progetto. Successivamente, si procede all'analisi degli stessi requisiti, per poter generare i requisiti di sistema che costituiranno le cosiddette specifiche.

L'abitazione presso la quale si intende realizzare il progetto in esame, presenta due serramenti in legno: il primo possiede accesso comune con altri condomini, mentre il secondo presenta un accesso indipendente all'interno di un giardino di proprietà del committente. Lo scopo del progetto, riguarda l'utilizzo di quattro sistemi di riconoscimento biometrico, nella fattispecie quelli di verifica, in quanto tali sistemi, effettuano un confronto tra la caratteristica biometrica di una persona con quella del suo modello già memorizzato nel sistema. Viene effettuato un confronto "uno a uno" per verificare che l'identità dell'individuo dichiara di possedere sia effettivamente corretta. In aggiunta, si rendono necessari ulteriori quattro sistemi di controllo degli accessi, complementari, basati sull'inserimento di un codice numerico al fine di permettere la *Multi-factor Authentication* (MFA) [1].

I quattro sistemi di riconoscimento biometrico e i sistemi di controllo degli accessi, vengono suddivisi in due coppie per ciascun serramento per permettere l'accesso sia dall'esterno che dall'interno. Dal momento in cui diversi sistemi sia di riconoscimento sia di controllo degli accessi, saranno ubicati esternamente all'edificio, si rende necessario l'utilizzo di scatole di derivazione con grado di protezione *Ingress Protection* (IP). Quest'ultimo permette una protezione garantita dallo standard *International Electrotechnical Commission* (IEC) 60529, impiegando scatole di derivazione con grado IP 66, poiché permettono di essere completamente ermetici a polveri e fumi, forti getti d'acqua proveniente da qualsiasi direzione e dall'acqua di mare.

Suddetti sistemi di autenticazione verranno pertanto azionati e pilotati attraverso due microcontrollori – preferibilmente Arduino UNO – rispettivamente uno per ciascun serramento, in cui ognuno di questi dovrà interfacciarsi con un sensore di impronte digitali biometrico di tipologia ottica ed una tastiera di piccole dimensioni per l'immissione del codice numerico. Per permettere lo sblocco del serramento in caso di una corretta autenticazione, sarà necessario avvalersi di due

servomotori, uno per ciascun ingresso, di tipologia elettrica e in corrente continua che verranno azionati attraverso il microcontrollore.

La letteratura in materia relativa ai sistemi biometrici, suggerisce l'utilizzo di un sistema di accesso indipendente nel momento in cui entrambi i sistemi sia di riconoscimento sia di controllo degli accessi dovessero fallire [2]. Tale sistema risulta infatti già essere presente in ciascun serramento ed è rappresentato da una serratura con chiavistello.

2.3 Tempistiche

La realizzazione di uno studio di fattibilità deve essere necessariamente un'attività di breve durata, data l'urgenza di arrivare alla produzione del documento ed il suo carattere sintetico e direzionale. L'impegno complessivo in giorni/persona necessario alla redazione dello stesso può variare significativamente, soprattutto in base alla tipologia ed entità del progetto. Di seguito si riporta una previsione dei tempi stimati per il completamento delle diverse attività. Si prevede una durata complessiva di 30 giorni per l'espletamento delle attività di progettazione, l'esecuzione dei lavori e del collaudo, articolate in 14 giorni per la fase di progettazione, 7 giorni per la fase di esecuzione e 7 giorni per la fase finale di collaudo.

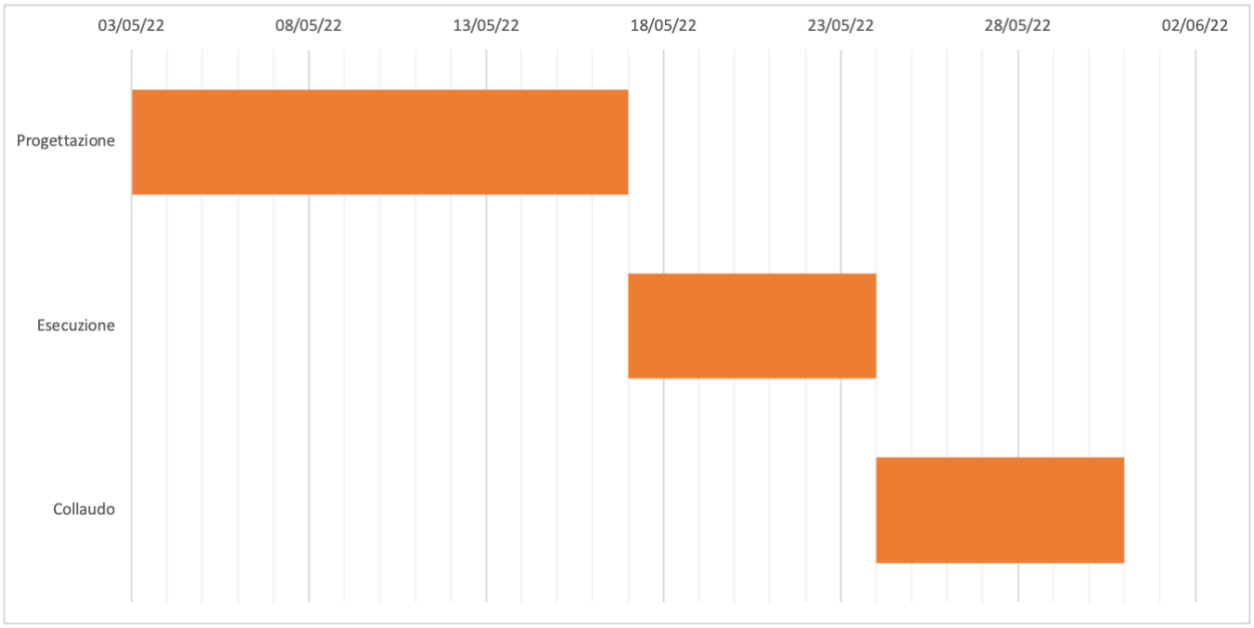

Figura 1.1 Prospetto diagramma di Gantt per realizzazione progetto

2.3.1 Panoramica dei costi

Per quanto riguarda invece i costi preventivati, vengono riportati di seguito in forma tabellare:

Componente	**Quantità**	**Costo** (cadauno)
Microcontrollore	2	€ 27
Servomotore (60kg)	2	€ 37
Sensore impronte digitali	4	€ 19
Tastierino numerico	2	€ 3
Scatola derivazione IP-66	4	€ 15
Componentistica elettrica	n.d	€15
	TOTALE	€ 285

Importo IVA escl. € 222.3

Capitolo 3

Sviluppo del progetto

3.1 Soluzioni commerciali esistenti

Verranno analizzate le soluzioni commerciali esistenti attualmente sul mercato in relazione alla natura del progetto descritto nel presente elaborato. Attraverso questa panoramica, sarà possibile poter apprezzare quali tecnologie e implementazioni sono impiegate dai rispettivi produttori *leader* del mercato. Le soluzioni evidenziate sono pertanto:

1. MorphoAccess SIGMA Lite – IDEMIA [3][4]
2. EP30 – Anviz [6][7]
3. HON-FIN4000MIK-100K – Honeywell [9]
4. ENTR – ASSA ABLOY [11][12]
5. YDF40 – Yale Home [14]

1. MorphoAccess SIGMA Lite – IDEMIA

Il lettore biometrico SIGMA Lite è una soluzione realizzata da IDEMIA ed è indicata per scenari aziendali che coinvolgono un gran numero di utenti. Viene riportata una illustrazione di seguito, mentre successivamente saranno riportate a corredo le caratteristiche tecniche:

Figura 1.2 Lettore biometrico MorphoAccess SIGMA Lite - IDEMIA

Caratteristiche tecniche del prodotto:

- **Tipologia sensore biometrico:** Ottico
- ***Duress finger prevention***
- ***Fake fingerprint detection* attraverso confronto statistico di immagini**
- **Tipo di identificazione:** 1:N attraverso *closed-set*
- **Tempo di riconoscimento:** ~ 1 secondo

- **CPU**: ARM Cortex-A9 core 1GHz
- **Sistema operativo**: Linux
- **Certificazione**: FBI PIV IQS (*Personal Identity Verification – Image Quality Specification*)
- **Connettività**: Ethernet, RS485, USB, Modulo Wi-Fi opzionale
- **Alimentazione**: 12-24V DC, oppure in alternativa PoE (*Power over Ethernet*), compatibilità con *switch* tipo PoE+
- **Archiviazione**: 512 MB *Flash*, 512 MB RAM con capacità di memorizzazione di 500 utenti e relativi *template*, espandibile da 3000 a 10000 utenti e relativi *template* (necessaria licenza supplementare), 1.000.000 di transazioni (*Log*)
- ***Input/Output***: Interfaccia Wiegand In & Out, *Open Supervised Device Protocol* (OSDP), relè per la porta, 2 *input* del tipo *General purpose*, 2 *output* del tipo *General purpose*
- ***Switch tamper***
- ***Ingress Protection***: IP65
- ***Impact Protection***: IK08
- **Dimensioni**: h. 156 mm, w. 68 mm, d. 62 mm
- **Peso**: 280 grammi
- **Categoria prodotto**: *Indoor/Outdoor*
- **Costo [5]**: € 330, € 253 (Modulo Wi-Fi opzionale), € 118 licenza supplementare per supporto da 3000 a 10000 utenti

2. EP30 - Anviz

Il lettore biometrico EP30 viene prodotto dalla società Anviz e rappresenta una soluzione per il controllo degli accessi all'interno di scenari aziendali che coinvolgono un gran numero di utenti. Viene riportata una illustrazione di seguito, mentre successivamente saranno riportate a corredo le caratteristiche tecniche:

Figura 1.3 Lettore biometrico EP30 - Anviz

Caratteristiche tecniche del prodotto:

- **Tipologia sensore biometrico:** Ottico
- **Tipo di identificazione:** 1:N attraverso *closed-set*
- **Tempo di riconoscimento:** < 0,5 secondi
- **CPU**: 1GHz
- **Sistema operativo**: Linux
- **Connettività**: TCP/IP, RS485, Mini USB, Modulo Wi-Fi opzionale
- **Alimentazione**: 12V DC

- **Archiviazione**: Capacità di memorizzazione di 3000 utenti e relativi *template* 50000 transazioni (*Log*)
- ***Input/Output***: Interfaccia Wiegand In & Out, relè per la porta
- **Dimensioni**: h. 165 mm, w. 73 mm, d. 37 mm
- **Peso**: 100 grammi
- **Categoria prodotto**: *Indoor*
- **Costo [8]**: € 156

3. HON-FIN4000MIK-100K – Honeywell

Il lettore biometrico FIN4000MIK-100K realizzato dalla Honeywell rappresenta una soluzione per il controllo degli accessi all'interno di scenari aziendali che coinvolgono un gran numero di utenti. Viene riportata una illustrazione di seguito, mentre successivamente saranno riportate a corredo le caratteristiche tecniche:

Figura 1.4 Lettore biometrico FIN4000MIK-100K - Honeywell

Caratteristiche tecniche del prodotto:

- **Tipologia sensore biometrico:** Ottico
- ***Fake fingerprint detection* attraverso confronto statistico di immagini**
  Live fingerprintj detection
- **Tipo di identificazione:** 1:N attraverso *closed-set*
- **Tempo di riconoscimento:** 1:150,000 *match*/secondo
- **CPU**: 1.2 GHz quad-core
- **Sistema operativo**: *Embedded*
- **Connettività**: Ethernet, RS485
- **Alimentazione**: 12V DC
- **Archiviazione**: 2 GB *Flash*, 256 MB RAM con capacità di memorizzazione di 100000 utenti e relativi *template*, 1.000.000 di transazioni (*Log*)
- ***Input/Output***: Interfaccia Wiegand In & Out, *Open Supervised Device Protocol* (OSDP), relè per la porta
- ***Switch tamper***
- ***Ingress Protection***: IP67
- **Dimensioni**: h. 201 mm, w. 71 mm, d. 44 mm
- **Categoria prodotto**: *Indoor*/*Outdoor*
- **Costo [10]**: € 2250

4. ENTR – ASSA ABLOY

La soluzione realizzata da ASSA ABLOY a differenza delle precedenti, si posiziona nel segmento delle serrature *smart* in quanto è azionabile localmente ed in remoto attraverso dispositivi mobili quali *smartphone* e similari. Rappresenta un'alternativa al classico cilindro con chiavistello presente in una porta. Viene riportata una illustrazione di seguito, mentre successivamente saranno riportate a corredo le caratteristiche tecniche:

Figura 1.5 Lettore biometrico con tastierino numerico ENTR – ASSA ABLOY

Caratteristiche tecniche del prodotto:

- **Tipologia sensore biometrico:** Piezoelettrico
- **Sistema operativo**: *Embedded*

- **Tipo di identificazione:** 1:N attraverso *closed-set*
- **Connettività**: Wi-Fi @ 2.4 GHz con crittografia AES128
- **Alimentazione**: 2x batterie AA oppure alimentatore opzionale 12V 1A
- **Memorizzazione impronte digitali utenti supportati**: 20 e relativi *template*
- **Riconoscimento utente**: Biometria oppure PIN attraverso tastierino
- ***Ingress Protection***: IP55
- **Dimensioni**: h. 140 mm, w. 50 mm, d. 40 mm
- **Peso**: 160 grammi
- **Categoria prodotto**: *Indoor/Outdoor*
- **Costo [13]**: € 294

5. YDF40 – Yale Home

La serratura prodotta dalla Yale si colloca anch'essa nel segmento delle serrature *smart* in quanto è azionabile localmente ed in remoto attraverso dispositivi mobili quali *smartphone* e similari. Rappresenta un'alternativa al classico cilindro con chiavistello presente in una porta. Viene riportata una illustrazione di seguito, mentre successivamente saranno riportate a corredo le caratteristiche tecniche:

Figura 1.6 Lettore biometrico con tastierino numerico YDF40 - Yale

Caratteristiche tecniche del prodotto:

- **Tipologia sensore biometrico:** Ottico
- **Sistema operativo**: *Embedded*
- **Tipo di identificazione:** 1:N attraverso *closed-set*
- **Connettività**: Bluetooth, Modulo Wi-Fi (opzionale)
- **Alimentazione**: 2x batterie AA oppure alimentatore opzionale 12V 1A
- **Memorizzazione impronte digitali utenti supportati**: 100 e relativi *template*
- **Riconoscimento utente**: Biometria oppure PIN attraverso tastierino
- **Dimensioni**: h. 176 mm, w. 66 mm, d. 31.5 mm
- **Categoria prodotto**: *Indoor*
- **Costo [15]**: € 564

3.2 Casi d'uso

Si procede pertanto nell'identificazione di alcuni semplici casi d'uso nei quali applicare il sistema di riconoscimento sotto esame:

- Apertura e accesso

  In questo primo scenario si trova un ambiente familiare nel quale i residenti dell'abitazione, rappresentano gli utenti legittimi e registrati all'interno del *database* del sistema biometrico. L'impronta digitale immagazzinata è quella del pollice destro. Il loro obiettivo è quello di sbloccare il serramento nel quale è installato il sistema di riconoscimento per poter accedere all'esterno dell'abitazione (oppure potervi accedere dall'esterno). Nel momento in cui uno dei residenti si presenta al sistema biometrico, per essere validato, appone l'impronta digitale del pollice destro. Il sistema procede quindi nella verifica e validazione dell'identità presentatagli ed allo sblocco del serramento.

- Accesso negato

  Nel secondo scenario, sempre domestico, l'utente legittimo si presenta al sistema biometrico per la verifica dell'identità ma non viene correttamente riconosciuto come tale, bensì come impostore e pertanto gli viene negato l'accesso all'abitazione. In questo caso, l'utente potrà nuovamente eseguire la procedura di verifica attraverso la sottoposizione della propria impronta digitale oppure potrà in alternativa ricorrere ad inserire un codice PIN personale che provvederà a garantirgli l'accesso, nonostante il sistema biometrico lo abbia precedentemente rifiutato. Tale soluzione permette di eseguire un *bypass* sul sistema di riconoscimento biometrico. Ciascun PIN utente è differente da quello degli altri utenti per motivi di sicurezza.

- *Blackout*

  In questo terzo ed ultimo scenario, domestico, si fa fronte ad un eventuale *blackout* elettrico che interrompe il funzionamento dei sistemi di riconoscimento. Gli utenti legittimi provvederanno pertanto ad utilizzare la serratura pre-esistente con chiavistello per garantirsi l'accesso e di conseguenza accedere all'abitazione.

3.3 Il riconoscimento biometrico

Un sistema biometrico rappresenta concretamente un sistema di riconoscimento di *pattern* che acquisisce dati di natura biometrica da un individuo, attraverso l'estrazione di un insieme di caratteristiche (*feature set*) insite nei dati acquisiti, successivamente procederà nel confrontare questo insieme di caratteristiche con un insieme di *template* contenuti all'interno di un *database*. In base allo scenario nella quale tale sistema verrà impiegato, il sistema biometrico potrà operare in modalità di "verifica" oppure in modalità "identificazione" [16].

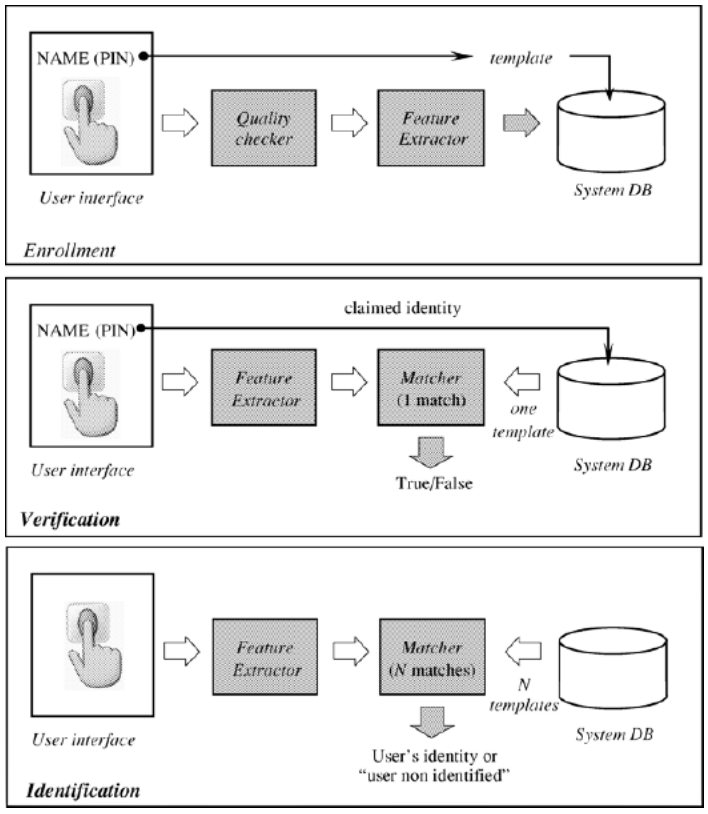

Figura 1.8 Diagramma a blocchi delle differenti fasi condotte dal sistema biometrico

Nella modalità di verifica, il sistema valida l'identità di una persona, confrontando i dati biometrici acquisiti con uno o più *template* immagazzinati all'interno del *database* del sistema. Un individuo che desidera essere riconosciuto,

asserisce un'identità, solitamente attraverso un PIN, *username*, oppure ancora una *smart card* ed il sistema in oggetto, eseguirà pertanto un confronto "uno a uno" per determinare se l'identità presentata sia vera oppure falsa: per esempio, il dato acquisito, appartiene a Bob? [17].

In modalità di identificazione, invece, il sistema riconoscerà un determinato individuo, eseguendo una ricerca del *template* fornito su tutti gli utenti presenti all'interno del *database*, per un possibile riscontro (*match*). Di conseguenza verranno eseguiti dei confronti "uno a molti" per determinare l'identità dell'individuo che sta eseguendo l'accesso senza la necessità da parte dell'utente di asserire alcuna identità, andando pertanto a rispondere alla domanda: a chi appartiene questo dato biometrico? (oppure tale ricerca potrà fallire, se il soggetto non è stato registrato all'interno del *database* attraverso una fase precedente detta *enrollment*).

3.4 Algoritmo

L'algoritmo individuato [18] per eseguire il riconoscimento delle impronte digitali, fa parte della famiglia degli algoritmi che si basano sul riconoscimento delle minuzie [19]. Questi metodi permettono di estrarre le minuzie dai due *template* oggetto del confronto, sotto forma di un insieme di punti in due dimensioni per ciascun *template.* Tali algoritmi consistono principalmente nell'ottenere un allineamento tra il *template* e l'insieme di minuzie fornito in *input* che portano ad individuare il maggior numero di coppie di minuzie comuni tra i due campioni sottomessi. Poiché l'immagine che rappresenta il *template* può influenzare in maniera importante le prestazioni di riconoscimento, nonché il grado di accuratezza dello stesso, prima di estrarre le minuzie, l'algoritmo esegue una fase di *pre-processing* sull'immagine. In questa fase viene pertanto applicato il filtro di Gabor [20] che permetterà di ridurre il rumore presente inizialmente nel *template* in analisi.

Nell'algoritmo presentato, l'estrazione delle minuzie avviene utilizzando il rilevatore di Harris poiché permette di migliorare l'accuratezza nella distinzione degli angoli dai bordi dell'immagine [21]. Successivamente viene applicato un altro algoritmo di *feature detection* chiamato ORB (*Oriented FAST and rotated BRIEF*) [22] che permette di rilevare e descrivere le caratteristiche locali dai campioni sottomessi. Infine durante l'ultima fase, si esegue la cosiddetta *feature matching* e si applica un *brute-force matcher* [23] che attraverso il calcolo della distanza di Hamming, valuta la distanza presente tra due impronte digitali differenti, applicando un determinato valore di soglia (*threshold*). Un valore inferiore nella distanza significa un maggior grado di somiglianza tra due *template* e quindi un maggior grado di riconoscimento.

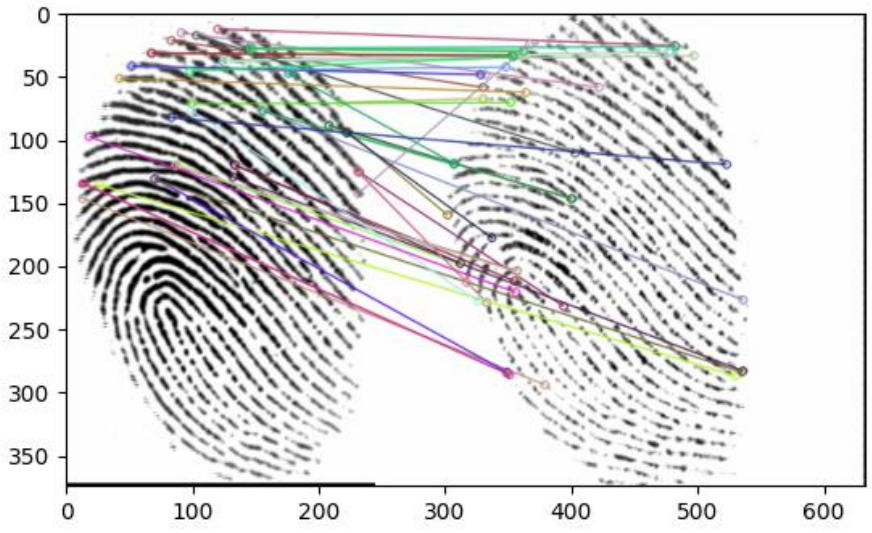

Figura 1.9 *Output* e *matching* tra due impronte

3.5 Valutazione delle prestazioni

Nei sistemi di riconoscimento automatico la corrispondenza tra due impronte digitali viene espressa in termini di un coefficiente di similarità che corrisponde alla probabilità che le due impronte in analisi appartengano allo stesso individuo. Affinché si possa determinare tale valore è necessario definire sia una metrica di similarità sia un valore di soglia (*threshold)* [24].

La suddetta metrica di similarità stabilisce le regole attraverso cui calcolare il coefficiente di similarità, tipicamente questo valore risulta proporzionale al numero di minuzie corrispondenti nelle due impronte. Il valore di soglia rappresenta invece quel valore minimo al di sopra del quale due impronte vengono considerate "simili".

È importante evidenziare che esiste una importante distinzione tra i tradizionali metodi di autenticazione come per esempio *password* oppure PIN (*Personal Identification Number*) alfanumerici e la biometria. Nel primo caso, una volta digitati, il risultato del controllo può assumere solo valori di vero oppure falso con estrema precisione, per via della bassa complessità dell'algoritmo. Diversamente per i sistemi che utilizzano la biometria, nella tecnica di riconoscimento, il valore deve essere ulteriormente giudicato per poter stabilire definitivamente la positività o negatività della verifica.

Di conseguenza l'algoritmo che esegue la verifica può commettere uno sbaglio con una determinata percentuale poiché possono esistere due o più individui che possiedono caratteristiche fisiche molto vicine tra loro; in questo modo il procedimento di calcolo non sarà in grado di distinguere tali caratteristiche a causa del suo grado di approssimazione. Per questo motivo, un utente può non essere riconosciuto positivamente. La causa è la scarsa tolleranza verso i disturbi presenti nel *template*, acquisito durante la fase di scannerizzazione (per esempio a causa di un leggero movimento del dito durante il riconoscimento dell'impronta).

Le misure accennate, pertanto vengono chiamate tolleranza di Tipo I (*False Rejection Error*) e di Tipo II (*False Acceptance Error*). Tali misure hanno un elevato impatto sulle prestazioni del sistema biometrico, poiché l'errore cosiddetto FRR (*False Rejection Rate*) di Tipo I causa frustrazione nell'utente legittimo durante la fase di verifica, mentre al contempo l'errore FAR di Tipo II lascia aperta la porta alla frode da parte di utenti impostori [25].

Gli errori di Tipo I e di Tipo II vengono spesso tradotti graficamente in curve per apprezzare la sensibilità del sistema: idealmente queste due curve dovrebbero entrambe tendere a zero per qualche dato valore di soglia, in questo modo le prestazioni dovrebbero mostrare un forte incremento generale. Le distribuzioni dei due errori FAR e FRR sono due quantità legate da una corrispondenza inversa: maggiore è la soglia imposta per il riconoscimento positivo, minore è la probabilità di accettare erroneamente un impostore, ma allo stesso è anche maggiore la possibilità di rifiutare per errore il legittimo proprietario di un dato *template*.

Queste due curve mostrano anche un punto di intersezione, il cosiddetto EER (*Equal error rate*) ed è questo punto che indica il valore nel quale i due errori si presentano con la stessa percentuale di frequenza. Costituisce un buon indicatore ed anche il più utilizzato per valutare e determinare l'efficacia del sistema biometrico.

L'accuratezza del sistema è tanto maggiore quanto più risulta basso il valore dell'EER.

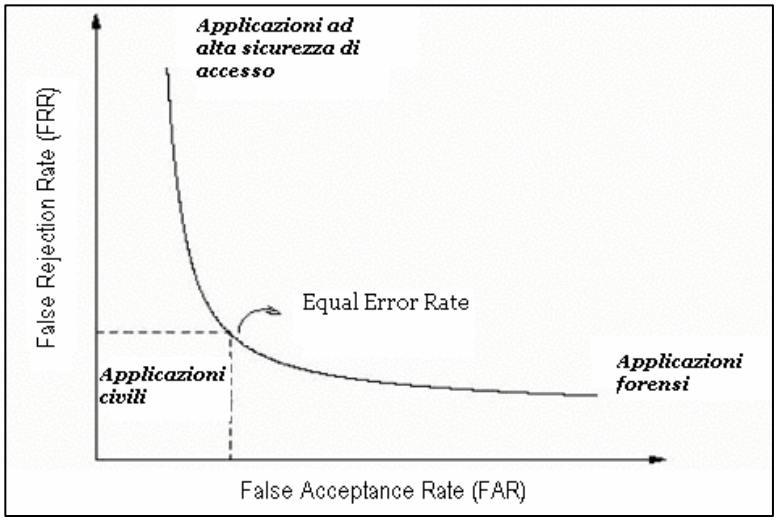

Figura 2.1 FRR, FAR e applicazioni biometriche nella curva ROC

Nella figura 2.1 viene mostrato l'andamento di FAR e FRR nei sistemi di riconoscimento: in applicazioni dove la sicurezza rappresenta l'obiettivo principale sarà fondamentale disporre di un valore di falsa accettazione (FAR) molto basso, come per esempio negli ambienti militari; al contrario in applicazioni forensi, sarà importante cercare di non escludere alcun criminale che presenta un'impronta digitale simile a quella trovata sul luogo del crimine, pertanto un valore (FRR) basso. Di conseguenza, la diminuzione degli errori del Tipo I incrementa la presenza di quelli del Tipo II e viceversa.

La curva presente nella figura è chiamata ROC (*Receiver Operating Curve*) e per la prima volta venne utilizzata per le rilevazioni dei segnali *radar* nella seconda guerra mondiale: oggi giorno viene spesso utilizzata per osservare con facilità il *tradeoff* tra il FAR e l'FRR.

3.6 Analisi dei risultati sperimentali

Per valutare e quantificare l'efficacia dell'algoritmo utilizzato, sono stati condotti numerosi *test* su uno dei quattro *database* di dominio pubblico, ampiamente utilizzati ed apprezzati nel panorama scientifico ed accademico legato ai sistemi biometrici. L'Università di Bologna coadiuvata dall'Università del Michigan, dall'Università di San Jose e l'Università autonoma di Madrid hanno realizzato un importante competizione chiamata *Fingerprint Verification Competition* (FVC) [26].

Il *database* utilizzato nei *test* è il "DB2_A" dell'edizione 2006 in quanto possiede un totale di 140 impronte digitali con dimensione 400 × 560 pixel. Ciascuna impronta presenta 12 campioni per acquisizione e tali acquisizioni sono state svolte con dei sensori ottici.

Il valore di soglia (*threshold*) che è stato utilizzato durante i *test* all'interno dell'algoritmo di cui sopra è 0,3.

Lo schema utilizzato per il confronto ha computato dapprima tutti i possibili confronti di utenti genuini per determinare il valore di FRR [27] al fine di investigare la percentuale del numero di rifiuti da parte del sistema sugli utenti legittimi. Il numero totale dei confronti eseguiti è stato 9240.

$$FRR = \frac{Falsi\ rifiuti}{Totale\ confronti} * 100$$

Successivamente si è proceduto a determinare il valore di FAR [28] per comprendere la percentuale del numero di false accettazioni da parte del sistema su utenti considerati impostori o non abilitati. Il numero totale dei confronti eseguiti è stato 9730.

$$FAR = \frac{False\ accettazioni}{Totale\ confronti} * 100$$

Infine si è determinato il valore di EER [29], il quale rappresenta il valore nel quale i due errori FRR e FAR sono uguali.

$$EER = \frac{FAR + FRR}{2}$$

Di seguito vengono pertanto riportati i risultati dei *test* eseguiti:

Soglia (*threshold*)	**FRR (%)**	**FAR (%)**	**EER (%)**
0,3	12,56 %	45,36 %	28,96 %

Bibliografia

[1] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.

[2] Bundesamt für Sicherheit in der Informationstechnik. (2021). Technical Guideline for Biometric Authentication Components in Devices for Authentication. BSI, TR-03166.

[3] IDEMIA. (2021). MorphoAccess SIGMA Lite series brochure #1.
Disponibile in:
https://biometricdevices.idemia.com/sfc/servlet.shepherd/document/download/0690X00000E6RkEQAV

[4] IDEMIA. (2021). MorphoAccess SIGMA Lite series brochure #2.
Disponibile in:
https://www.idemia.com/wp-content/uploads/2021/04/sigma-range-idemia-brochure-202104.pdf

[5] IdentityOne. (2021). Store for MorphoAccess SIGMA Lite.
Disponibile in:
https://store.identityone.net/products/morphoaccess-sigma-lite

[6] Anviz. (2021). EP30 IP fingerprint and RFID access control terminal.
Disponibile in:
https://www.anviz.com/product/ep30.html

[7] Anviz. (2021). EP30 brochure #1.
Disponibile in:
https://www.anviz.com/file/download/9263.html

[8] OrbitaDigital. (2022). Store for EP30.
Disponibile in:

https://www.orbitadigital.com/en/cctv/access-controls/anviz/access-control/23371-anviz-ep30-anviz-autonomous-biometric-reader-fingerprints-rfid.html

[9] Honeywell. (2018). HON-FIN4000MIK-100K brochure.
Disponibile in:
https://www.security.honeywell.com/me/-/media/SecurityME/Resources/ProductDocumentsME/HON-FIN4000MIK-100K-pdf.pdf

[10] Sieuthivienthong. (2022). Store for HON-FIN4000MIK-100K.
Disponibile in:
https://www.sieuthivienthong.com/dau-doc-van-tay--the-tu--ma-so-honeywell-hon-fin4kmik-100k-32678.html

[11] ASSA ABLOY. (2018). ENTR promotional website.
Disponibile in:
https://www.assaabloy.com/gh/en/solutions/products/home-security/digital-door-locks/entr

[12] ASSA ABLOY. (2018). ENTR datasheet.
Disponibile in:
https://eshop.assaabloyopeningsolutions.nz/media/B2BUserGuide/ENTR_Smart_Lock_Solution_Catalogue.pdf

[13] Amazon. (2022). Store for ENTR.
Disponibile in:
https://www.amazon.de/-/en/Abloy-Keyboard-Smart-Biometric-Motorized/dp/B01L25E2W8

[14] Yale. (2021). YDF40 smart lock brochure.
Disponibile in:
https://www.yalehome.com/my/en/product-assets/smart-lock/yale-access-app-smart-lock/assets/documents/yale-access-leaflet/Yale%20YDF40A%20Product%20Leaflet.pdf

[15] Amazon. (2022). Store for YDF40.
Disponibile in:
https://www.amazon.com.br/Yale-05423001-2-Fechadura-BiométricaEmbutir/dp/B076T7L7Q6

[16] Jain, A.K., Ross, A. and Prabhakar, S. An Introduction to Biometric Recognition. (2004). IEEE Transactions on Circuits and Systems for Video Technology, 14, 4-20.

[17] J. L. Wayman. (2001). Fundamentals of biometric authentication technologies, Int. J. Image Graphics, vol. 1, no. 1, pp. 93–113.

[18] GitHub. (2017). Python Fingerprint Recognition.
Disponibile in:
https://github.com/kjanko/python-fingerprint-recognition

[19] Sahu, D., & Shrivas, R. (2016). Fingerprint Reorganization Using Minutiae Based Matching for Identification and Verification.

[20] Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: algorithm and performance evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(8), 777–789.

[21] Harris, C., & Stephens, M. (1988). A combined corner and edge detector. In Proc. of Fourth Alvey Vision Conference, 147–151.

[22] E. Rublee, V. Rabaud, K. Konolige and G. Bradski. (2011). ORB: An efficient alternative to SIFT or SURF. International Conference on Computer Vision, 2011, pp. 2564-2571.

[23] OpenCV. (2016). Documentation.
Disponibile in:
https://docs.opencv.org/3.4/dc/dc3/tutorial_py_matcher.html

[24] Wayman, J.L., Jain, A.K., Maltoni, D., Maio, D., eds. (2005). Biometric Systems, Tech- nology, Design and Performance Evaluation. Springer.

[25] Maltoni, D., Maio, D., Jain, A.K., & Prabhakar, S. (2003). Handbook of Fingerprint Recognition. Springer Professional Computing.

[26] R. Cappelli, M. Ferrara, A. Franco and D. Maltoni, Fingerprint verification competition 2006. (2006). Biometric Technology Today, vol.15, no.7-8, pp.7-9.

[27] Bourjot, M., Perrier, R., & Mainguet, J. (2017). Comparison of fingerprint authentication algorithms for small imaging sensors.

[28] Precise Biometrics AB. (2014). White paper on Understanding Biometric Performance Evaluation.

Disponibile in:
https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation-QR.pdf

[29] Romain Giot, Mohamad El-Abed, Christophe Rosenberger. (2013). Fast computation of the performance evaluation of biometric systems: application to multibiometric. Future Generation Computer Systems, Elsevier, pp.10.