Sistemi Biometrici Multimodali e tecniche di Fusione Multi biometrica

Abstract

La Biometria è la scienza e la tecnologia che opera per misurare e analizzare i dati biologici del corpo umano, estraendo un set di caratteristiche dai dati acquisiti e confrontando questo insieme con il modello impostato nel database.

La crescente domanda di sistemi di sicurezza avanzati ha portato ad un interesse senza precedenti nei sistemi di autenticazione basati su biometrie; tra questi i sistemi biometrici basati su un'unica fonte di informazione sono chiamati sistemi **Unimodali**. Sebbene i sistemi Unimodali abbiano ottenuto un notevole miglioramento in termini di accuratezza e affidabilità, spesso soffrono di problemi dovuti a tratti biometrici non universali, suscettibilità allo spoofing biometrico o poca accuratezza causata da dati rumorosi. Quindi, sistemi basati su singola biometria potrebbero non essere in grado di raggiungere le prestazioni desiderate nell'applicazione nel mondo reale.

Uno dei metodi per superare questi problemi è quello di utilizzare sistemi di autenticazione biometrica **Multimodale**, che combinano le informazioni provenienti da più modalità per arrivare a una decisione. Vengono definiti sistemi **biometrici multimodali** quelli che hanno la capacità di utilizzare più di una caratteristica fisiologica o comportamentale per operazioni di **verifica** o **identificazione**.

Alcuni studi hanno dimostrato che un sistema biometrico multimodale può ottenere prestazioni migliori rispetto ai sistemi unimodali. Di seguito discuteremo diverse fonti multimodali, architetture e diverse tecniche di fusione utilizzate nei sistemi biometrici multimodali ed opereremo una panoramica sulle tecnologie ed i risultati attualmente utilizzati ed ottenuti in questo ambito.

Index

Architettura, Biometria, Sistemi Multimodali, Caratteristica vettoriale, Fusione Biometrica, Fonti Biometriche, Sistemi Unimodali, Algoritmi Biometrici.

Autori

1. **Annunziata Gianluca**
   Studente Informatica Magistrale
   Università degli Studi di Salerno
   Fisciano, Salerno, ITALIA

2. **De Rosa Gerardo**
   Studente Informatica Magistrale
   Università degli Studi di Salerno
   Fisciano, Salerno, ITALIA

1. *Introduzione*

I sistemi biometrici sono diventati molto popolari come tool per identificare l'essere umano misurandone le caratteristiche fisiologiche o comportamentali. Le biometrie identificano la persona in base a ciò che la persona è piuttosto che in base a ciò che questa possiede, a differenza dei sistemi di autorizzazione convenzionali come le smart card.

A differenza dei sistemi di identificazione basati sul possesso o sulla conoscenza, gli identificatori biometrici non possono essere dimenticati, indovinati o falsificati.

I sistemi biometrici multimodali sono quelli che utilizzano, o sono in grado di utilizzare, più di una caratteristica fisiologica o comportamentale per la verifica o l'identificazione.

Nel corso degli ultimi decenni tali sistemi hanno avuto un crescente interesse in tutto il mondo e nei più svariati settori, soprattutto in ambito security. Questi sistemi analizzano due o più caratteristiche fisiologiche del corpo umano, quali impronte digitali, retine e iridi oculari, schemi vocali e pattern facciali applicando, infine, un **algoritmo di fusione** che metta insieme i risultati di ogni biometria presa in analisi.

2. *Sistemi Biometrici Multimodali*

Le parole Multi Biometria si riferiscono all'uso di una combinazione di due o più modalità biometriche in un sistema di verifica/identificazione. L'identificazione basata su più dati biometrici rappresenta, ormai, una realtà affermata con molto seguito da parte di aziende e studiosi del settore.

La ragione più convincente per combinare diverse modalità è migliorare il tasso di riconoscimento rispetto ai sistemi Unimodali, ciò può avvenire quando le caratteristiche biometriche di diversi dati biometrici sono statisticamente indipendenti.

Ci sono altri motivi per combinare due o più dati biometrici: uno di questi è che le diverse modalità biometriche potrebbero essere più appropriate per diverse applicazioni nel mondo reale, un altro, invece, è semplicemente la preferenza del cliente.

Tuttavia l'obiettivo principale della multi-biometria è di ridurre uno o più dei seguenti indici:

- False accept rate (**FAR**)
- False reject rate (**FRR**)
- Failure to enroll rate (**FTE**)
- Suscettibilità ad artefatti

L'accuratezza di un sistema biometrico multimodale è infatti misurata in termini di **errori di matching** e **errori di acquisizione**; gli errori di matching sono costituiti da:

- false match rate (**FMR**), quando un impostore viene accettato dal sistema;
- false non-match rate (**FNMR**), quando ad un utente reale viene negato l'accesso;

mentre gli **errori di acquisizione** delle immagini comprendono:

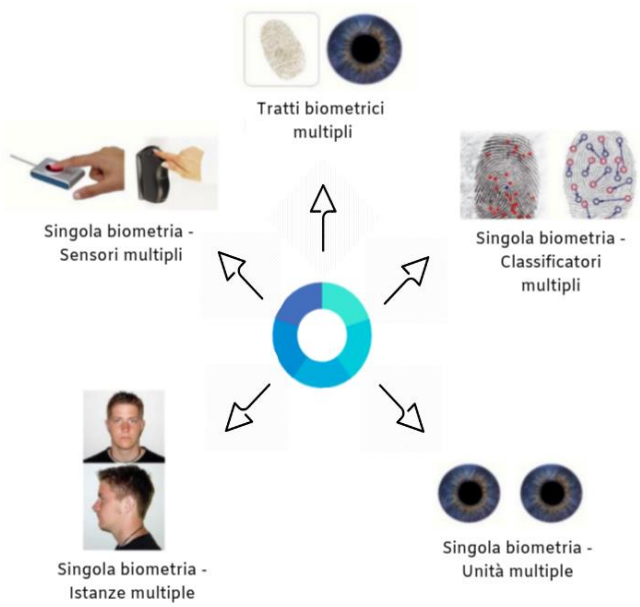
- failure to enrol (**FTE**), o errore di registrazione;
- failure to acquire (**FTA**), o errore di acquisizione.

3. Fonti Multimodali

I sistemi biometrici multimodali non si basano unicamente sull' utilizzo di tante biometrie diverse ma, ad esempio, possono basarsi su poche biometrie utilizzando però più sensori per catturare ogni biometria.

Possiamo quindi distinguere diverse metodologie:

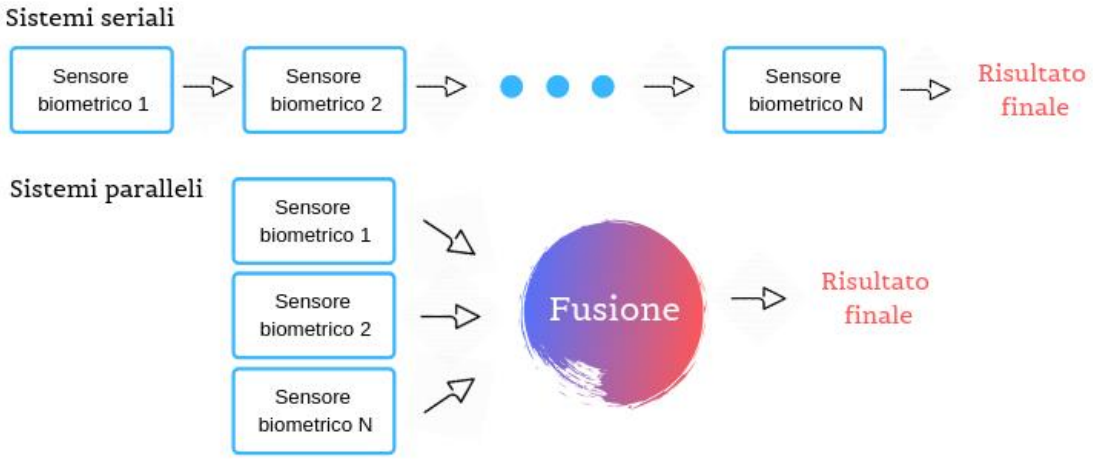
- **Singola biometria / Sensori multipli:** lo stesso tratto biometrico è misurato da due o più sensori; tali sensori potrebbero fornire input molto diversi
- **Singola biometria / Classificatori multipli**: viene utilizzato un singolo tratto biometrico ma nel sistema vengono utilizzati diversi classificatori [esempio: le minuzie e la texture di un solo dito]
- **Singola biometria / Istanze multiple**: viene utilizzato un singolo tratto biometrico, catturato però in diverse istanze leggermente diversa l'una dall'altra [esempio: il volto di una persona viene scansionata a diverse angolazioni]
- **Singola biometria / Unità multiple**: di nuovo, viene utilizzato un singolo tratto biometrico, ma vengono prelevate diverse unità [esempio: occhio sinistro ed occhio destro sono entrambi inseriti nel sistema]
- **Tratti biometrici multipli**: due o più tratti biometrici vengono combinati per identificare l'utente o per verificare che l'utente è presente nel sistema [esempio: impronta digitale e volto dell'utente]



4. *Architetture di sistemi Biometrici Multimodali*

Una volta determinato quali fonti biometriche devono essere integrate, è necessario scegliere l'architettura del sistema biometrico che si vuole realizzare.

Esistono principalmente due tipi di design per sistemi biometrici multimodali, ovvero **sistemi seriali** e **sistemi paralleli**.



Sistemi seriali

Nelle architetture seriali, anche conosciute come architetture a cascata, l'elaborazione dei diversi input avviene in sequenza; pertanto, l'output del primo tratto biometrico influenzerà l'elaborazione del secondo tratto biometrico, e così via via.

Sistemi paralleli

Nelle architetture parallele, l'elaborazione delle informazioni biometriche provenienti dai diversi sensori viene fatta indipendentemente l'una dall'altra; una volta che tutte le informazioni sono state elaborate, i loro i risultati vengono combinati da un sistema di fusione.

5. Modalità di funzionamento

Un sistema multimodale può operare in uno di tre diversi modalità: modalità **seriale**, modalità **parallela** o modalità **gerarchica**.

Nella modalità seriale, l'output di una modalità è tipicamente utilizzato per restringere il numero di possibili identità prima di passare alla modalità successiva, perciò, non è necessario acquisire contemporaneamente i dati biometrici da tutti le fonti, inoltre, il sistema potrebbe decidere l'esito prima che vengano acquisite tutte le biometrie e ciò potrebbe ridurre il tempo complessivo necessario al riconoscimento.

Nella modalità parallela, le informazioni da più modalità sono utilizzate simultaneamente per eseguire il riconoscimento.

Infine, nella modalità gerarchica, i classificatori individuali sono combinati in una struttura simile ad un albero, tale modalità risulta essere molto utile quando il numero dei classificatori è grande.

6. Fusione Multi Biometrica

Nella biometria multimodale usiamo, come si evince dal nome, più di una biometria avendo così accesso a più canali decisionali; per fare ciò in maniera efficiente è necessario progettare un meccanismo in grado di combinare i risultati di classificazione di ciascuna biometria per arrivare infine ad un risultato complessivo; tale meccanismo è chiamato **fusione multi-biometrica**.

Esistono diversi tipi di fusione multi-biometrica suddivise in base ai diversi livelli in cui vengono applicate, ovvero:

- **Sensor Level Fusion**
- **Feature Level Fusion**
- **Matching Score Level**
- **Decision Level**

Le fusioni Sensor e Feature Level sono indicate come **fusioni pre-mapping**, mentre le fusioni Matching Score e Decision Level sono indicate come **fusioni post-mapping**.

Sensor Level Fusion

Nella fusione a livello sensore si combinano i tratti biometrici provenienti dai sensori come scanner di impronte, videocamere, scanner dell'iride ecc. per formare una **biometria composta** e, successivamente, utilizzare la biometria prodotta per il riconoscimento; un esempio di tale fusione è il rilevamento di un segnale vocale utilizzando simultaneamente due microfoni.

Sebbene ci si aspetti che la fusione a tale livello migliori l'accuratezza del riconoscimento, spesso non può essere utilizzato nella multi-biometria a causa dell'incompatibilità dei dati provenienti dai diversi sensori.

Feature Level Fusion

Nella fusione a livello di feature i segnali provenienti da diverse biometrie sono prima sottoposti ad una pre-elaborazione ove vengono estratti dei vettori di feature (**feature vectors**) dalle singole biometrie; usando poi uno specifico algoritmo di fusione, tali vettori vengono combinati per formare un **vettore di feature composito.**

Tale vettore composito verrà, quindi, utilizzato per il processo di classificazione.

Un esempio è concatenare i vettori di feature estratti da biometrie come volto e impronta digitale.

Nel corso degli anni è stato provato che la Feature Level Fusion ha prestazioni superiori rispetto alle fusioni Score Level e Decision Level, ciò perché il livello Feature contiene molte più informazioni sui dati biometrici raccolti.

Tuttavia tale fusione non è sempre applicabile, ad esempio: in molti casi le feature estratte potrebbero non essere compatibili a causa delle differenze delle biometrie stesse, oppure la concatenazione delle feature potrebbe portare ad un feature vector molto grande comportando un aumento del tempo necessario per computarlo, oppure ancora, per operare con vettori di feature level concatenati sono necessari dei classificatori più complessi e difficili da costruire.

Matching Score Level

In questa fusione, invece di combinare i feature vectors estratti dalle biometrie, elaboriamo separatamente ogni biometria calcolandone il punteggio (**matching score**), poi, a seconda della precisione di ciascuna biometria, possiamo fondere i punteggi per calcolare il **punteggio composito** che viene poi inviato all'algoritmo di decisione.

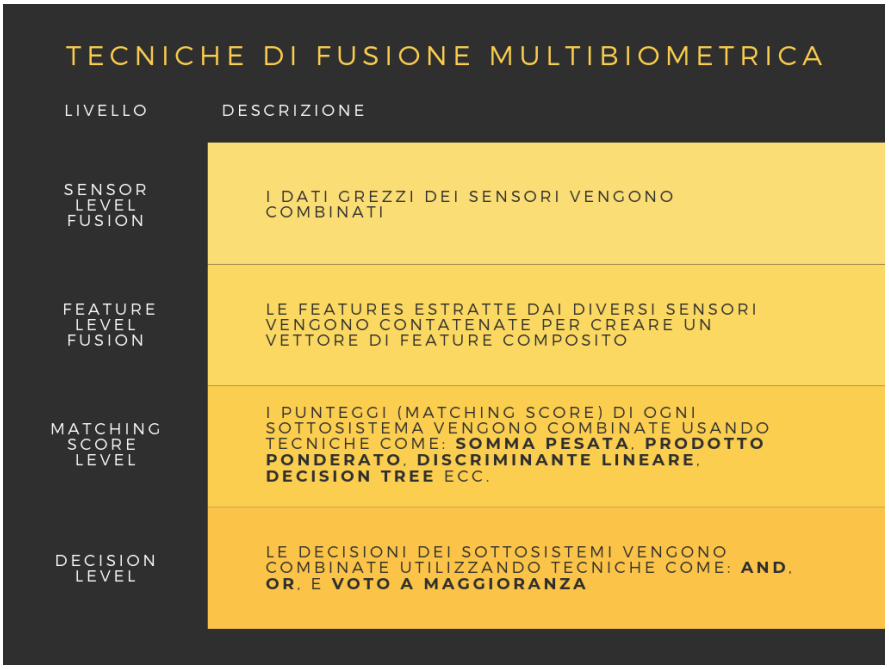
Attualmente, questo sembra essere il livello di fusione più utile per le sue buone prestazioni e per semplicità di realizzazione.

Questa fusione può essere suddivisa in due categorie: **combinazione** e **classificazione**: nel primo approccio, un punteggio scalare è ottenuto normalizzando i punteggi nello stesso intervallo e poi

combinandoli, nell'altro approccio, i punteggi vengono dati in input ad un modulo di classificazione a due livelli tra le due classi **utente Reale** e **Impostore**.

Decision Level Fusion

Ogni biometria viene prima pre-classificata indipendentemente; la classificazione finale si basa sulla fusione degli output delle differenti biometrie. In questo approccio, per ogni biometria viene presa una decisione ad uno stadio avanzato; ciò limita molto il processo di miglioramento della precisione del sistema attraverso il processo di fusione.



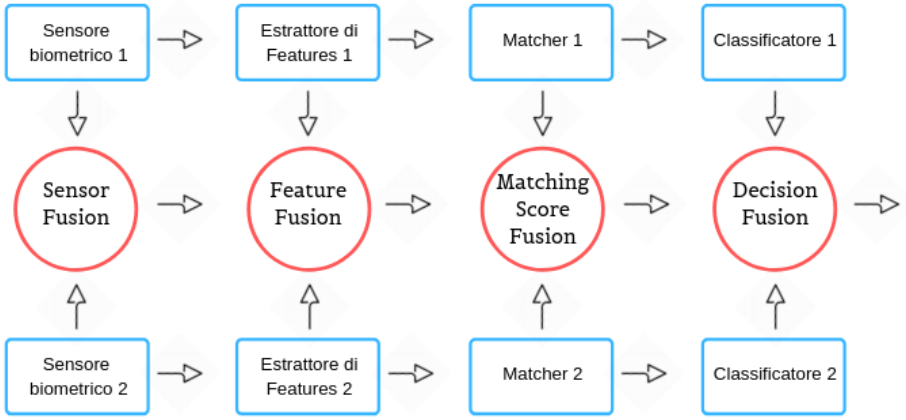
I sistemi multi biometrici possono implementare ognuna di queste tecniche o anche una combinazione di più tecniche di fusione per migliorare le performance del sistema; la scelta dello schema di fusione influenza notevolmente l'accuratezza di un sistema.

Nel mondo accademico viene preferita la Matching Score Level Fusion sia a causa delle problematiche delle altre tipologie di fusione, sia perché è relativamente semplice realizzare dei sottosistemi che decidono autonomamente ed un sistema generale che raccoglie tutte le decisioni dei sottosistemi e le aggrega arrivando ad una decisione complessiva; ciò può essere ottenuto utilizzando un **approccio non adattivo** oppure un **approccio adattivo.**

In un approccio non adattivo, il peso di ciascun sottosistema si basa sul semplice pregiudizio del sottosistema stesso (**bias**); ad esempio in un sistema biometrico multimodale con sottosistemi per impronta digitale e tono vocale, la precisione iniziale del sottosistema di impronta digitale potrebbe essere più alta rispetto al sottosistema del tono vocale; pertanto, si potrebbe assegnare un peso maggiore al sottosistema con maggior precisione.

In un approccio adattivo, invece, il contributo di almeno un sottosistema varia nel tempo in base all'affidabilità dimostrata da tale sottosistema nelle iterazioni precedenti; le ricerche effettuate in questo campo hanno dimostrato che assegnare il peso ai sottosistemi in funzione dei parametri specifici dell'utente rispetto ai parametri comuni porta ad un netto miglioramento della precisione del sistema.

Calcolando una soglia di corrispondenza (**matching threshold**) per ogni utente utilizzando istogrammi cumulativi di punteggi degli impostori per ogni tratto biometrico, è stato osservato un aumento di precisione quando si utilizza una soglia specifica dell'utente rispetto ad una soglia comune; inoltre, imparando il peso specifico dell'utente per ogni caratteristica, un peso ridotto potrebbe essere assegnato ad una caratteristica meno affidabile e un peso maggiore ad una più affidabile, ciò porta ad una riduzione del tasso di errore per quel particolare individuo; ad esempio, in un sistema biometrico multimodale che combina informazioni su impronte digitali e linguaggio, il sistema può ridurre il peso associato al sottosistema del linguaggio quando la qualità del segnale è basso.



7. *Alcuni criteri di valutazione adottati*

Questi criteri rappresentano le modalità tramite le quali le biometrie multimodali vengono valutate tra di loro. Tra di questi vi sono:

- **Fusione delle Decisioni**: Uso di operatori (Es. AND logico e OR) per arrivare ad una decisione finale;
- **Voto**: Usare decisioni individuali come voti per la decisione finale;
- **Fuzzy Fusion**: Uso dei più recenti concetti di logica Fuzzy per ottenere una decisione;
- **Score Combination**: Usare operazioni matematiche per combinare score individuali e confrontare il risultato con una soglia di decisione;

- **Score Classification**: Utilizzare gli score unimodali come dati di input per un classificatore binario (Reti Neurali, SVM, GMM, ...), che prenderà la decisione finale;
- **Dynamic Score Selection**: Usa alcuni dei metodi precedentemente citati e opera una selezione dello score dalla modalità che ritiene più adeguata;

Nessuno dei metodi precedentemente elencati è superiore agli altri, poiché ognuno si adatta meglio ad uno specifico ambiente, specifica soluzione, specifico dataset, specifici sensori e specifici processi.

8. Nuove tecnologie impiegate

Tra le tecnologie più utilizzate per operare fusione multi biometrica, oltre i vari algoritmi di filtering, calcolo degli score e varie distanze, troviamo anche le reti neurali e le SVM.

Le **Reti Neurali** sono modelli semplificati di "cervelli", composte da un alto numero di unità (neuroni) insieme a pesi che misurano la forza delle connessioni tra di essi. Questi pesi hanno l'obiettivo di modellare gli effetti delle sinapsi che connettono un neurone all'altro. Questa tipologia di modelli ha dimostrato di possedere un'ottima abilità nell'imparare skills quali il riconoscimento facciale, leggere e il rilevare semplici strutture grammaticali. Vi sono molti tipi di NN (Reti Residuali, Reti Convoluzionali, …) quelle standard sono formate da diversi strati di neuroni: un input layer, diversi hidden layers ed un output layer. Il primo strato prende l'input e lo distribuisce a quelli successivi che operano tutta la computazione necessaria e passano l'output all'ultimo layer, che consegnerà il dato finale all'utente (nel caso della verifica e identificazione biometrica se accettare o meno il soggetto esaminato).

Le **SVM** sono classificatori discriminanti che performano un mapping non lineare da uno spazio di in input ad uno spazio futuro, dove vengono poi applicate tecniche di regressione lineare; la parte principale nel loro utilizzo è rappresentato dal kernel.

Per essere utilizzare le NN e le SVM devono prima essere allenate con dati etichettati con l'identità di ciascun soggetto.

L'utilizzo di questi strumenti è sempre maggiore in questo campo; l'impiego che se ne fa è molto vario, infatti queste vengono utilizzate sia nelle singole biometrie (riconoscimento facciale, iride ecc.), sia per operare la fusione tra queste e sia ad avvenuta fusione; a seconda della tipologia di quest'ultima.

9. Alcuni classificatori utilizzati

I classificatori sono utilizzati negli algoritmi biometrici ed in quelli di fusione multi biometrica, in particolare quando si tratta di fusione a livello di score; per operare la decisione finale riguardo l'identificazione e la verifica. Tra i più utilizzati vi sono:

- **La somma pesata:** si tratta di un semplice algoritmo che combina gli score dati in input utilizzando una somma pesata per ottenere il punteggio finale; la decisione è poi calcolata comparando lo score con una soglia;
- **Il prodotto pesato:** come il metodo precedente, opera semplicemente moltiplicazione di scores di biometrie unimodali; anche qui la decisione finale viene presa confrontando lo score con una soglia;
- **Le Reti Neurali:** l'input per il primo layer saranno gli score forniti dai moduli unimodali; l'output sarà la decisione finale sull'identità dell'individuo;
- **Le Support Vector Machine:** vengono impiegate in maniera similare alle NN, l'input è rappresentato da score unimodali e l'output sarà la decisione finale;

10. *Analisi di alcuni studi effettuati*

In questa sezione verranno discussi alcuni tra gli studi e gli elaborati concernenti la fusione multi biometrica; la disquisizione sarà divisa principalmente in due, distinguendo gli elaborati volti alla verifica e quelli volti all'identificazione ed infine altri elaborati non inerenti a queste due attività.

Studi di verifica

Per studi di verifica si intende algoritmi il cui scopo è quello di controllare l'identità del soggetto facendo un match con un solo profilo biometrico.

1. Algortimo "Context Weighted Majority Algorithm"

Quest'elaborato, realizzato in **python** nel **2018**, vuole porsi come metodo di verifica in particolare in ambito mobile; le biometrie che prende in esame sono quelle **del volto e della voce**, in particolare utilizzando varianti di pose ed espressioni per il volto e diversi speaker e livelli di rumore per la voce, la metodologia di fusione adottata, infine, è quella al **livello score**.

Lo scopo dell'algoritmo è quello di scegliere i classificatori da tenere in considerazione, calcolando quali sono i migliori per un determinato contesto; per fare ciò opera creando un'estensione del **Weighted Majority Algorithm**, in particolare per ogni classificatore E, da un punteggio d_i che può essere un numero naturale oppure 0 o 1, dati i classificatori e gli score, il meccanismo di fusione opera una decisione finale in base alla funzione:

$$f(d_1, d_2, \ldots, d_n) \text{ Reject } \lesseqgtr \text{ Accept } \theta$$

Dove Θ nella funzione rappresenta la soglia decisionale ed f rappresenta la funzione.

Le modalità che utilizza per operare la classificazione di faccia e voce sono:

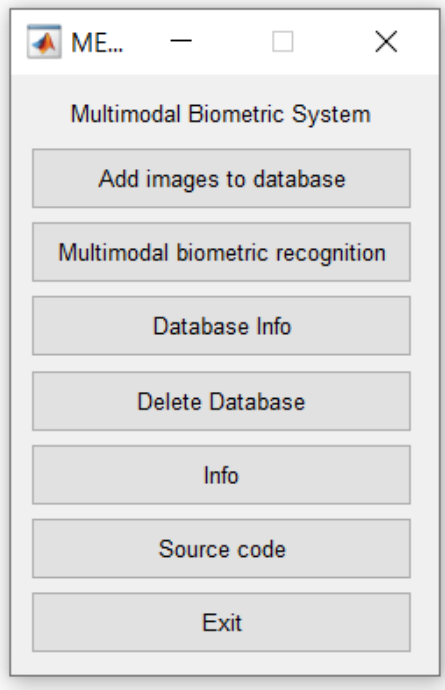
- **VGGFace features** (faccia);
- **MFCC features** (voce);
- **Nearest Neighbour with cosine distance** (faccia);
- **Support Vector Machine.**

Essendo il codice incompleto non è stato possibile controllare il funzionamento degli script, ma l'autore promette che i risultati superino tutti gli altri modelli con cui è stato confrontato; inoltre afferma che rispetto ad essi abbia maggiori capacità adattative e non richieda un'elevata potenza computazionale.

Studi di identificazione

Per studi di identificazione, si intendono algoritmi che hanno come obiettivo quello di identificare un solo soggetto confrontando i suoi dati biometrici con quelli di N profili.

1. **Algoritmo "Multimodal Biometrics"**



Quest'algoritmo scritto in **matlab** utilizza la fusione di **impronte digitali, iride e palmo della mano**.

Il codice è nascosto, ma il funzionamento è esplicitato chiaramente; il tool si avvale di un'interfaccia che richiede il caricamento dei tre dati biometrici di una persona, riguardanti le biometrie menzionate in precedenza e un **ID** da assegnargli.

Una volta ripetuta quest'operazione per N soggetti otterremmo un database formato da N*3 immagini biometriche, a questo punto potremmo effettuare l'operazione di riconoscimento che prevede l'inserimento di altre 3 immagini che l'algoritmo elaborerà e confronterà con quelle presenti nel database creato, per poi restituire l'identità identificata.

2. **Algoritmo “Feature level fusion of Palm print and Palm vein”**

Questo studio, realizzato in **matlab** nel **2016**, utilizza dati biometrici relativi all’impronta palmare e alle vene dei palmi delle mani. I dati sono elaborati in formato .txt, in particolare per ogni soggetto sono presenti 4 immagini e per ognuna di questa vengono estratte **39 features**.

Di seguito viene descritto il calcolo delle caratteristiche:

L’algoritmo carica le immagini, le ridimensiona in un formato **64x64**, le divide in 39 blocchi e calcola prima la **trasformata discreta del coseno** per l’intera immagine, e poi la deviazione standard di ognuno di questi, dopodiché l’inserisce in una matrice e li stampa in un file .txt.

L’operazione di creazione dei .txt viene ripetuta 4 volte, 2 per le fasi di **training** su tutte le immagini dei soggetti, una per **palmprint** ed una per **palmvein**, 2 per le fasi di **testing** su metà delle immagini degli utenti, sempre una per ciascuna biometria.

Dopo avere caricato i file .txt creati in precedenza l’algoritmo di fusione li unisce in un'**unica matrice,** operando cosi una fusione al **livello feature**; ciò avviene sia sui dati di training che quelli di testing, dopo di ciò viene calcolato uno score (**Manhatten, Heillenger, Canbera o Euclidean**) e su questo ed un valore assegnato arbitrariamente, viene poi calcolato la distanza tra i dati di training e quelli di testing.

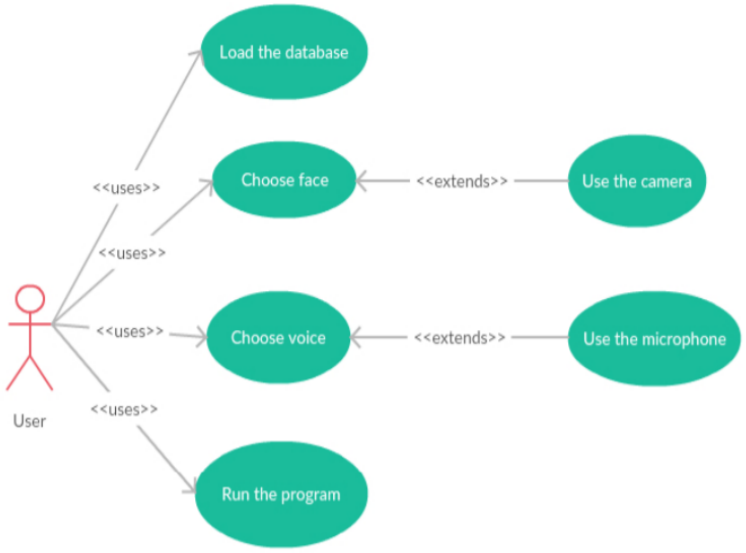
Da ciò risulta un vettore contente in corrispondenza di ogni indice (che rappresenta l’identificativo delle foto utilizzate per training) l’identificativo della foto del soggetto dei dati di testing a cui questa si riferisce.

Studi di identificazione e verifica

1. **Algoritmo “Biometric fusion system for human recognition using face and voice”**

Questo sistema è stato creato in modo da permettere sia l’identificazione che la verifica di un soggetto. I dati biometrici che utilizza provengono da **faccia e voce** e sono prelevati da una camera con microfono, integrati nel sistema.

Di seguito sono illustrate le modalità d’uso:



Questo progetto è stato sviluppato in **C# .NET 4.6**, con l'ausilio di **MSSQL Server 2012** come server e di **FFmpeg** per catturare le immagini; per quanto riguarda il modello di programmazione è stato utilizzato **the iterative waterfall model.**

In questo studio è stata applicata la fusione solo a **decision level**, infatti il programma dopo aver acquisito i dati biometrici separatamente ed aver associato un'identità agli stessi, conserva questi in un database dal quale verranno poi prelevati per effettuare le operazioni di verifica, che avverranno anch'esse in modo disgiunto per poi infine confrontare i risultati ottenuti.

Per elaborare il **face recognition** si passa attraverso le seguenti fasi:

- Normalizzazione;
- Istogramma ed equalizzazione dello stesso;
- Conversione in scala di grigi;
- Applicazione del filtro Gabor;
- Estrazione delle feature dall'istogramma e dal filtro di Gabor;
- Estrazione delle feature facciali impiegando i metodi del passo precedente;
- Classificatore a minima distanza, utilizzato per identificare o verificare il viso.

Per elaborare lo **speech recognition**, invece, si passa attraverso le seguenti fasi:

- Divisione audio in frame della stessa lunghezza;
- Applicazione della finestra gaussiana e di hamming;
- Calcolo del periodogramma;

- Conversione e applicazione del filtro della scala Mel;
- Estrazione delle feature vocali utilizzando i metodi menzionati nei passi precedenti;
- DynamicTimeWarping, utilizzato per identificare o verificare la voce.

Le tabelle di seguito illustrano i **risultati** ottenuti:

SPEECH VERIFICATION RESULTS					
DATASET	WORD	FALSE ACCEPTANCE RATE IN %	FALSE REJECTION RATE IN %	AMOUNT OF VERIFIED PERSONS	DATASET SIZE
SMALL	ALGORITHM	14.40%	23.81%	21	21
SMALL	CLOSE	19.29%	19.05%	21	21
MEDIUM	ALGORITHM	13.49%	23.81%	21	40
MEDIUM	CLOSE	22.95%	19.05%	21	40
LARGE	ALGORITHM	11.74%	19.23%	39	58
LARGE	CLOSE	30.48%	15.38%	39	58

FACE VERIFICATION RESULTS				
DATASET	FALSE ACCEPTANCE RATE IN %	FALSE REJECTION RATE IN %	AMOUNT OF VERIFIED PERSONS	DATASET SIZE
SMALL	31.31%	4.76%	21	21
MEDIUM	26.37%	4.76%	21	40
LARGE	25.17%	3.85%	39	58

Altri studi

1. **Algoritmo “Multi-Biometric Template Protection based on Bloom filters”**

Quest’elaborato, scritto in **Python** nel **2018**, si pone l’obiettivo di aumentare l’irriconoscibilità delle feature prelevate da dati biometrici e basa il suo operato sui **bloom filters**. Questi non sono altro che una maschera atta a trasformare i dati modificando leggermente le loro caratteristiche, in modo da renderli irriconoscibili ed aumentare cosi la privacy dei soggetti.

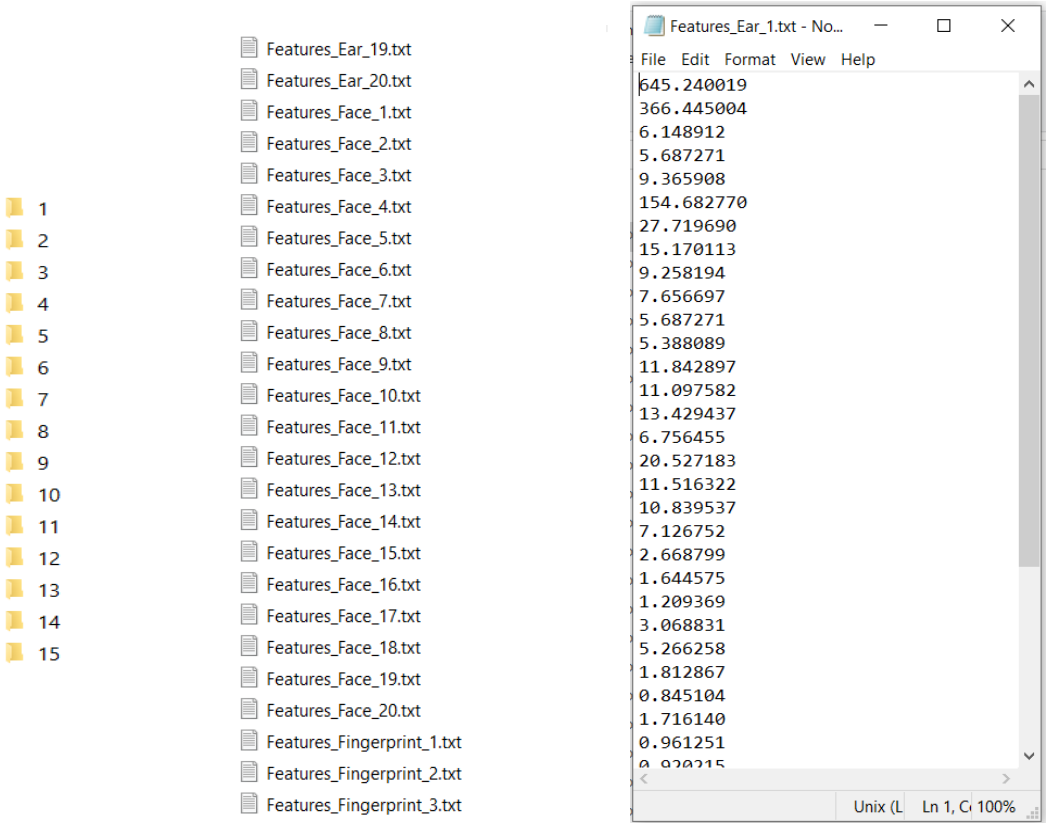
Lo scopo dello studio è quello di elaborare i dati biometrici con i bloom filters e senza, valutando cosi se il grado di protezione maggiore, vale la perdita di dettaglio qualora presente.

Le biometrie prese in esame dallo studio sono quella dell'iride e della faccia, queste sono conservate **in formato binario** in file .txt per garantire l'anonimato dei soggetti che compongono il dataset.
Il programma prodotto è composto da due script, il primo pende in input i due file contenti i DB ed un file con la lista che descrive la tipologia di fusione da effettuare, il secondo invece prende in input i dati fusi, prodotti dal primo script e le cartelle dove verranno conservati gli scores, che giudicheranno la perdita di dettaglio tra i dati protetti e quelli non protetti.
Per confrontare i due dataset viene calcolata uno score utilizzando la **distanza normalizzata di Hamming.**
L'autore afferma tra i risultati, che non è presente perdita di dettaglio tra gli score elaborati e che quindi l'utilizzo dei bloom filter si è rilevato efficace.

11. Calcolo features con dataset progetto FVAB

Dopo aver analizzato vari algoritmi riguardanti la fusione multi biometrica, abbiamo deciso di provare ad eseguire uno di questi su dati e tipologie di biometrie diverse, forniti da noi, per verificare il suo comportamento.
Per cominciare abbiamo identificato lo studio che si sarebbe prestato; abbiamo scelto quindi quello riguardante la fusione dell'impronte dei palmi delle mani e delle vene di questi ultimi, che meglio si prestava ad un'operazione di questo tipo.
Il dataset che abbiamo utilizzato comprendeva l'utilizzo di tre biometrie**: viso, orecchio ed impronte digitali**; i soggetti presenti erano 15 e per ognuno di questi e per ogni biometria erano presenti 20 immagini; per un totale di 60 immagini per soggetto e **300 immagini** in totale.
A questo punto è stato necessario modificare lo script che elaborava il file .txt, secondo le modalità con cui erano stati nominati i vari file e procedere con l'elaborazione dell'algoritmo descritto in precedenza (creazione file .txt ed esecuzione dello script di fusione).

Risultato finale della creazione dei file .txt per ogni soggetto, biometria e immagine:



Tra le migliorie che abbiamo apportato vi è stata quella di poter applicare la fusione di un insieme di **3 biometrie** al posto di 2 e di salvare per ogni soggetto e per ogni biometria il set di feature riguardanti questi ultimi, in modo da avere un vero e proprio dataset ordinato di feature biometriche, favorendo così oltre che un maggior usabilità e comprensibilità anche un incremento della privacy dei soggetti a cui appartenevano le biometrie prelevate.

Apportando altre modifiche all'algoritmo sarebbe possibile utilizzarlo anche per operazioni di **verifica**.

12. Sfide di ricerca e direzioni future

La fusione biometrica ha testimoniato avanzamenti significanti attraverso le ultime due decadi; sviluppo di nuovi algoritmi, sorgenti di informazioni, campi applicativi e dati collezionati. Il dove, quando e come fondere le biometrie è fondamentale, ma per sviluppare funzionanti sistemi biometrici, è richiesto un'implementazione efficiente che si adatti al dominio in cui si trova e disponga per i cambiamenti nei sensori, ambiente, popolazione target, ecc.

Di seguito sono riassunti alcuni dei campi in cui verosimilmente si muoverà la fusione multi biometrica.

Portabilità di soluzioni Multi biometriche

La maggior parte degli algoritmi di fusione possiedono diversi parametri da impostare; anche il più semplice algoritmo di fusione score-level richiede la stima dello score normalizzato e il vettore dei pesi. Dedurre automaticamente i valori da impostare non è quasi mai la scelta giusta, ciò porta alla domanda di come un sistema con un robusto design possa essere facilmente adattato a nuovi contesti. La risposta a questa domanda è stata data in parte dal **Transfer Learning** e **Domain Adaption** ma non si è rilevata sufficiente; le strade da percorrere sono potenzialmente due:

- Utilizzare la fusione biometrica per l'adattamento del dominio;
- Incorporare l'adattamento del dominio nei sistemi multi biometrici esistenti per operare un match in diversi domini.

Design adattivo e sistemi fusi dinamicamente

Nelle applicazioni reali, i sistemi multi biometrici spesso devono operare su dati in larga scala catturati usando diversi sensori attraverso diversi paesi e diverse popolazioni; in più i requisiti di un'applicazione e la natura dei suoi dati può cambiare nel tempo.

In letteratura, tecniche come l'online learning o il co-training hanno dimostrato di aumentare le performance dei sistemi di riconoscimento uni biometrici aggiornandoli ad ogni occasione possibile; ma questa tipologia di tecnica è ancora sconosciuta per quanto riguarda i sistemi multi biometrici. Ciò la rende un'attiva area di ricerca da perseguire, anche se modificare i dati biometrici a seconda dei cambiamenti degli individui, come invecchiamento e annichilimento fisico, è complicato e potenzialmente rischioso (furti d'identità).

Sicurezza e privacy in multi biometria

La ricerca nel campo delle soft biometrics ha creato la possibilità di dedurre altre informazioni da un individuo dai suoi dati biometrici. Quest'informazione può essere utilizzata per migliorare l'accuratezza del riconoscimento, ma può anche violare la privacy e potenzialmente profilare i soggetti protagonisti dei dati.

È evidenti quindi, come il bilancio tra sicurezza e accuratezza è un'altra importante challange che la biometria multimodale deve e dovrà affrontare in futuro

Risolvere conflitti tra le sorgenti di informazioni

La disponibilità di molteplici fonti biometriche e conseguentemente di molteplici pezzi di dati biometrici, non è sempre l'ideale; in alcuni casi le sorgenti biometriche possono offrire decisioni in

conflitto riguardo l'identità di un soggetto: Ad esempio, in un sistema biometrico bimodale, la faccia e le impronte digitali possono generare una lista di identità completamente diversa, oppure in un sistema, metà dei classificatori possono proporre una determinata entità mentre un'altra metà un'altra. In questi scenari è necessario avere dei principi e delle regole per generare delle decisioni; potrebbe essere necessario riacquisire i tratti biometrici oppure considerare gli output delle fonti più affidabili; in ogni caso sono presenti innumerevoli fattori da tenere in considerazione.

Soluzioni multimodali per device personali compatti

Con l'aumento dell'utilizzo degli smartphone e dispositivi wearable ed il bisogno di stabilire l'identità in questi device, è pressante l'opportunità di sviluppare nuovi sensori biometrici.

I dispositivi portatili sono già equipaggiati con un grande numero di sensori (GPS, accelerometro, giroscopio, …) i cui dati possono essere utilizzati per identificare l'identità del soggetto che li utilizza, ma questi sensori sono tipicamente pre-programmati per identificare chi li utilizza, sono vulnerabili ai cambi dei comportamenti degli utilizzatori e non possono essere facilmente trasportati da un device all'altro.

13. Conclusioni

I sistemi biometrici Multimodali, come abbiamo visto, risolvono elegantemente tutti gli inconvenienti dei sistemi Unimodali; combinando molteplici fonti di informazioni è possibile migliorare le performance, le prestazioni, la copertura della popolazione, la difesa allo spoofing e la facilità dell'indicizzazione.

In questo paper abbiamo discusso delle varie architetture dei sistemi multimodali, le loro performance e i loro limiti, approfondendo poi le principali tecniche di fusione applicabili in tali sistemi; infine, abbiamo poi studiato dei sistemi realizzati da altri ricercatori e sviluppatori e confrontando i loro risultati, descritti approfonditamente nei loro paper (quando presenti), con un sistema multi biometrico da noi realizzato modificandone uno già esistente e testandolo con un dataset creato da nostri colleghi.

Dopo aver approfonditamente studiato buona parte della letteratura disponibile per la Multi Biometria e la fusione Multi Biometrica e aver infine sviluppato un applicativo, ci sentiamo soddisfatti del lavoro svolto e condividiamo il crescente interesse per questi argomenti.

References

- *Performance Analysis of Various Fusion methods in Multimodal Biometric (Satya Bhushan Verma, Chandran Saravanan, Associate Professor)*
- *A review of biometric technology along with trends and prospects (J.A. Unar, Woo Chaw Seng, Almas Abbas)*
- [3] *Multi-biometric Convolutional Neural Networks for Mobile User Authentication (Ajita Rattani, Narsi Reddy and Reza Derakhshani)*
- [4] *https://github.com/Adityagupta2590/Feature-level-fusion-of-Palm-print-and-Palm-vein*
- [5] *Multi-biometric template protection based on bloomfilters (Gomez-Barrero, Christian Rathgeba, Guoqiang Lib, Raghavendra Ramachandrab,Javier Galballyc, Christoph Busch)*
- [6] *Context-Aware Fusion for Continuous Biometric Authentication (Divya Sivasankaran1, Mona Ragab Sayed, Terence Sim, Yair Zick)*
- [7] *https://github.com/aleks0and/Biometric-Fusion-System*
- [8] *https://github.com/dasec/multibiometric-bf-btp*
- [9] *https://github.com/palakanmol31/MultimodalBiometricSystem*
- [10] *https://github.com/divSivasankaran/Context-Weighted-Majority-Algorithm*
- [11] *A comprehensive overview of biometric fusion (ManeetSingh, RichaSingh, ArunRoss)*