UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Dipartimento di Informatica "Giovanni Degli Antoni"

Corso di Laurea in

Sicurezza dei Sistemi e delle Reti Informatiche

RICONOSCIMENTO BIOMETRICO DA SEGNALI ELETTROCARDIOGRAFICI TRAMITE DEEP LEARNING

Relatore: Dr. Massimo Walter Rivolta
Correlatore: Prof. Roberto Sassi

Tesi di:
Christian Roy Cuenca
Matricola: 965017

Anno Accademico 2022-2023

Abstract

Tra le tematiche oggi in forte sviluppo sono la sicurezza informatica con l'intelligenza artificiale, questo è dovuto alla crescente interconnessione digitale e la diffusione di tecnologie avanzate che usiamo quotidianamente. La biometria, analizzando tratti unici dell'individuo, può aiutare il riconoscimento degli utenti legittimi e non legittimi in un ambiente sia digitale sia fisico. Tra i metodi tradizionali fortemente usati sono: le impronta delle dita, l'analisi delle iridi degli occhi, l'analisi del comportamento e analisi del volto umano.

Con il progresso della ricerca e della tecnologia, l'attenzione è posta oltre a questi metodi largamente usati per esplorare il potenziale dell'apparato cardiaco umano come fonte di dati biometrici unici che possa essere sfruttata per l'autenticazione sicura d'individui. Questa tesi si inserisce in questo contesto concentrando l'attenzione sullo sviluppo e sull'analisi dei risultati ottenuti per il riconoscimento biometrico basato su segnali elettrocardiografici (ECG) attraverso l'impiego di Reti Neurali Profonde, così a mirare e contribuire alla comprensione e all'implementazione di questi sistemi di riconoscimento biometrico basati su ECG, promuovendo ulteriori sviluppi nella sicurezza informatica.

Questo studio è legato al tirocinio curricolare svolto presso il BiSP Lab dell'Università degli Studi di Milano. L'organizzazione di questo lavoro è quanto segue: Nel capitolo 1 si introduce il contesto della ricerca, definendo la biometria e il suo corretto sviluppo e funzionamento generale, si definisce inoltre i metodi di Machine Learning e il funzionamento generale dell'apparato cardiaco umano. Si presenta lo stato dell'arte e si definiscono gli obbiettivi di questa ricerca. Nel capitolo 2 viene spiegato il materiale e la metodologia usata e si descrivono poi gli esperimenti effettuati. Nel capitolo 3 si riportano i risultati degli esperimenti confrontandoli con la letteratura, si analizza poi scenari di utilizzo pratico e analizzando le relative questioni di sicurezza. Il capitolo 4 è dedicato alla conclusione della ricerca.

Indice

Elenco delle figure

Elenco degli algoritmi

Capitolo 1

Introduzione

Si inizia questa tesi sottolineando l'assoluta importanza della protezione dei dati e servizi ai tempi di oggi, un'epoca in cui la tecnologia domina il nostro modo di vivere e di lavorare. Questa attenzione si estende sia al mondo fisico, come ad esempio ai controlli di sicurezza nei gate degli aeroporti e ai tornelli del trasporto pubblico, che al mondo digitale, compresi siti web governativi, bancari e molte altre risorse online. Non serve che si riportino in questo documento le statistiche di quanto le perdite in termini finanziarie (e in termini dei danni di reputazione) dovute ad attacchi cibernetici siano sempre in aumento negli ultimi anni.

È dunque vitale per un'organizzazione un sistema che sia in grado di riconoscere gli utenti attendibili da eventuali non autorizzati. Infatti un concetto chiave all'interno della cybersecurity è l'Access Control, che mira a prevenire l'uso non autorizzato di risorse, oltre a impedire l'utilizzo di risorse in modo non autorizzato. Questo è essenziale per garantire che solo utenti attendibili abbiano accesso ai dati e ai servizi, mentre gli utenti non autorizzati siano esclusi.

The prevention of unauthorized use of a resource,
including the prevention of use of a resource in an unauthorized manner

Il funzionamento di tale sistema inizia quando un soggetto fa richiesta nel sistema, comincia quindi la fase di identificazione/autenticazione, in base all'identità del soggetto il Reference Monitor potrà dunque concedere o negare l'autorizzazione in base alla politica di accesso imposto dall'amministratore del sistema (Figura 1).

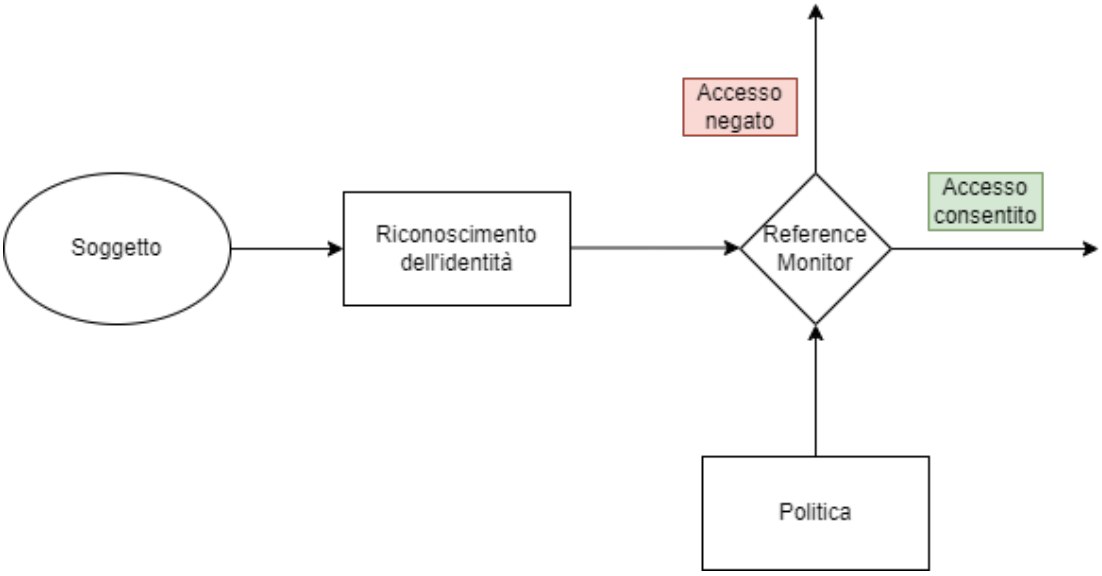


Figura 1: Funzionamento del Reference Monitor.

In questo elaborato ci si concentra sulla fase di identificazione e autenticazione dei soggetti, con particolare riguardo nell'utilizzo della biometria, nonché a un nuovo metodo innovativo di identificazione su cui negli ultimi anni si sta facendo ricerca: il riconoscimento basato su segnali elettrocardiografici. Esplorando questa nuova frontiera nella sicurezza informatica, valuteremo i vantaggi e le sfide legati al suo uso come metodo di autenticazione e la sua applicabilità in diversi contesti attraverso l'uso di tecniche delle Reti Neurali artificiali, con l'obbiettivo di migliorare il campo della cybersecurity.

1.1 Problematica di ricerca

La biometria è un nuovo metodo per identificare le persone: tradizionalmente, il processo di autenticazione e identificazione si basa sull'utilizzo di una combinazione di username e password.

Le caratteristiche fisiche utilizzate nella biometria includono l'iride, l'impronta digitale e il volto. Ognuna di queste caratteristiche è unica per ogni individuo e difficilmente replicabile. Ad esempio, il riconoscimento dell'iride coinvolge la scansione del dell'iride dell'occhio. Il riconoscimento facciale, invece, si basa sulla

distinzione delle caratteristiche facciali, come la forma degli occhi, del naso e delle labbra.

D'altra parte, la biometria comportamentale si concentra su tratti come la voce, la firma e persino la camminata. La voce è una caratteristica distintiva in quanto la struttura delle corde vocali e il modo di parlare variano notevolmente tra le persone. La firma è un'altra caratteristica che può essere utilizzata per l'identificazione poiché le firme manuali sono uniche per ogni individuo. Anche la camminata può essere rilevata attraverso l'analisi della postura e dei movimenti degli arti del corpo.

Confrontando i metodi biometrici e tradizionali, il livello di sicurezza e affidabilità va aumentando all'aumentare del costo del metodo:

	Livello di sicurezza	Costo del metodo
Una cosa che HAI	Basso	Economico
Una cosa che SAI	Medio	Medio
Una cosa che SEI o FAI	Elevato	Costoso

Quelli basati su oggetti (noti anche come token) rappresentano un approccio di sicurezza relativamente semplice ma non privo di sfide. Tali metodi richiedono l'uso di una chiave fisica, che può essere una carta, un badge, o un dispositivo elettronico. Sebbene questi dispositivi possano fornire un certo livello di sicurezza, presentano alcune vulnerabilità significative: ad esempio è possibile perdere o smarrire il token, rendendolo inutilizzabile. Inoltre, essi possono essere rubati o duplicati da individui malevoli.

D'altro canto, i metodi che si basano su password o codici, pur essendo ampiamente utilizzati, presentano anche delle vulnerabilità notevoli. Essi possono essere indovinati da utenti non autorizzati o possono essere soggetti ad attacchi di forza bruta. Inoltre, il furto dell'identità nota come spoofing può essere un problema quando si utilizzano solo password. La semplicità e la familiarità di questi metodi sono spesso bilanciate dalla loro vulnerabilità intrinseca.

In contrasto, i metodi basati su tratti biometrici rappresentano un avanzamento significativo nella sicurezza. Queste caratteristiche sono intrinsecamente legate alla persona e non possono essere dimenticate, perse o rubate da terze parti. Sono estremamente difficili da falsificare o replicare, e questo li rende estremamente

affidabili e difficili da compromettere. L'accuratezza dei sistemi biometrici può superare di gran lunga quella dei metodi tradizionali, riducendo notevolmente il rischio di accessi non autorizzati. Per aumentare ulteriormente la sicurezza, è possibile combinare l'identificazione biometrica con metodi tradizionali come l'autenticazione a due fattori.

Esistono 7 proprietà che caratterizzano un tratto biometrico:

- Universalità, tutte le persone devono possedere questo tratto
- Unicità, il tratto deve essere unico rispetto agli individui
- Permanenza, il tratto non deve variare nel tempo
- Misurabilità, il tratto deve essere misurato quantitativamente
- Performance, l'accuratezza dell'identificazione deve essere adeguata ed essere garantita senza particolari condizione operative
- Accettabilità, % di persone che potrebbero accettare l'uso del sistema biometrico
- Circonvenzione, indica il grado di difficoltà nell'ingannare il sistema con tecniche fraudolente

Confronteremo più in avanti queste proprietà rispetto al riconoscimento biometrico utilizzato con l'elettrocardiogramma.

Definiamo ora due tipi di riconoscimento dell'identità, essi si suddividono in:

- Identificazione, ossia ricerca dell'identità, equivale alla domanda "Chi sono io?" (one-to-many). Può essere:
  - Un problema di identificazione chiuso, dove sono note l'insieme d'identità.
  - Un problema di identificazione aperto, dove non sono note l'identità delle persone coinvolte.
- Autenticazione, ossia la verifica dell'identità dichiarata dal soggetto, corrisponde alla domanda "Sono chi dico di essere?" (one-to-one)

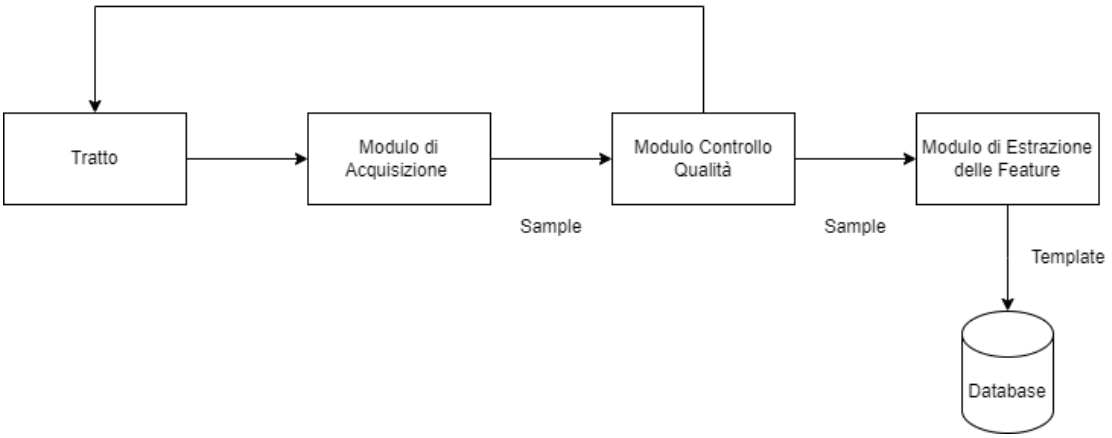


Figura 2: Schema della fase di Enrollment.

Il funzionamento del sistema biometrico può essere diviso in due fasi: Enrollment rappresenta il momento in cui il tratto biometrico di una persona viene inserito nel sistema per la prima volta. Durante questa fase, il sistema acquisisce in modo accurato e dettagliato il tratto biometrico in questione, altrimenti si ripete l'acquisizione. Ma non sempre è possibile rifiutare un sample, in questo caso si applicano metodi di enhancement cercando di estrarre le informazioni che vogliamo (foregorund) dal rumore (background). Da questi dati acquisiti vengono estratti le caratteristiche (feature) e memorizzati nel sistema come un "modello di riferimento" o "template" all'interno di un database (Figura 2).

È importante il passaggio da sample a template poiché permette di rappresentare l'informazione in modo machine-readable per poi calcolare le distanze tra le feature, questo ci consente anche di fornire le informazioni di variabilità interclasse e intraclasse: le prime ci dicono la differenza dei feature tra due soggetti, e le altre la differenza dei feature nella stessa persona. Quello che vogliamo è una alta variabilità interclasse così da discriminare bene i diversi soggetti tra loro, e una bassa variabilità intraclasse per discriminare il singolo soggetto (Figura 3).

La fase di Riconoscimento avviene ogni volta che il soggetto cerca di accedere al sistema. Dunque si acquisisce nuovamente il tratto biometrico del soggetto in modo simile a quanto è stato fatto durante l'Enrollment, se si tratta di Verification l'utente dovrà dichiarare anche la sua identità, talvolta sotto forma di un PIN o documento biometrico come nel caso dei passaporti. Il tratto appena acquisito

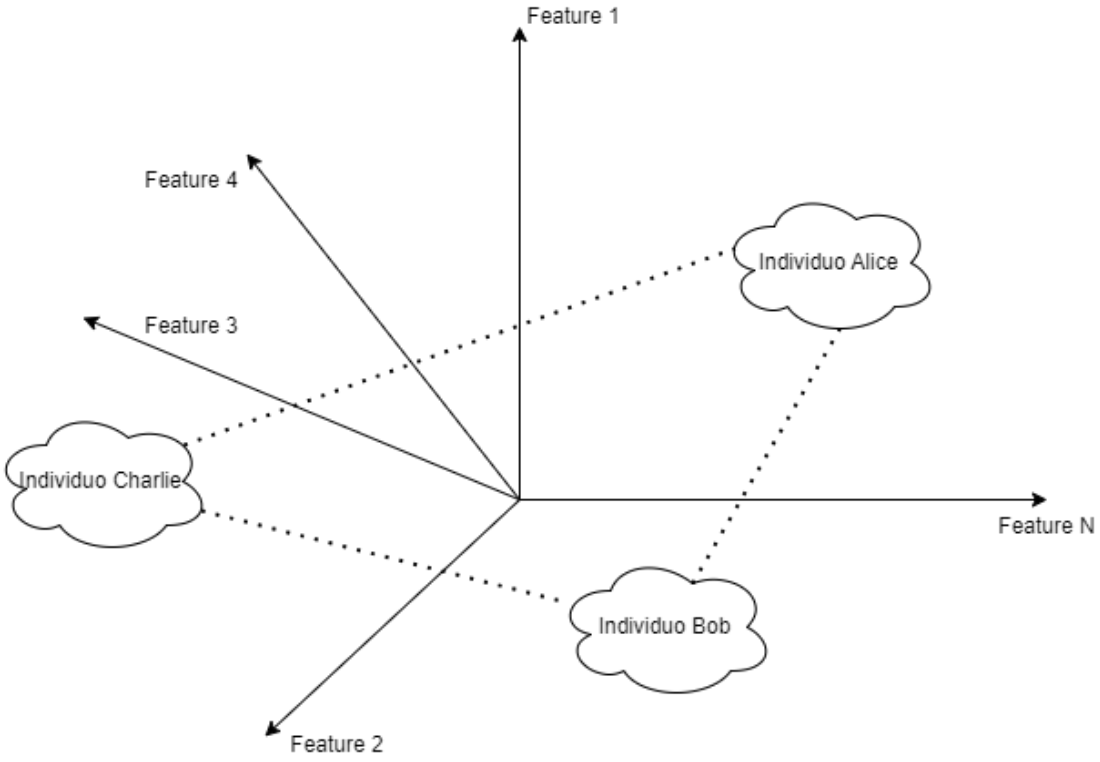
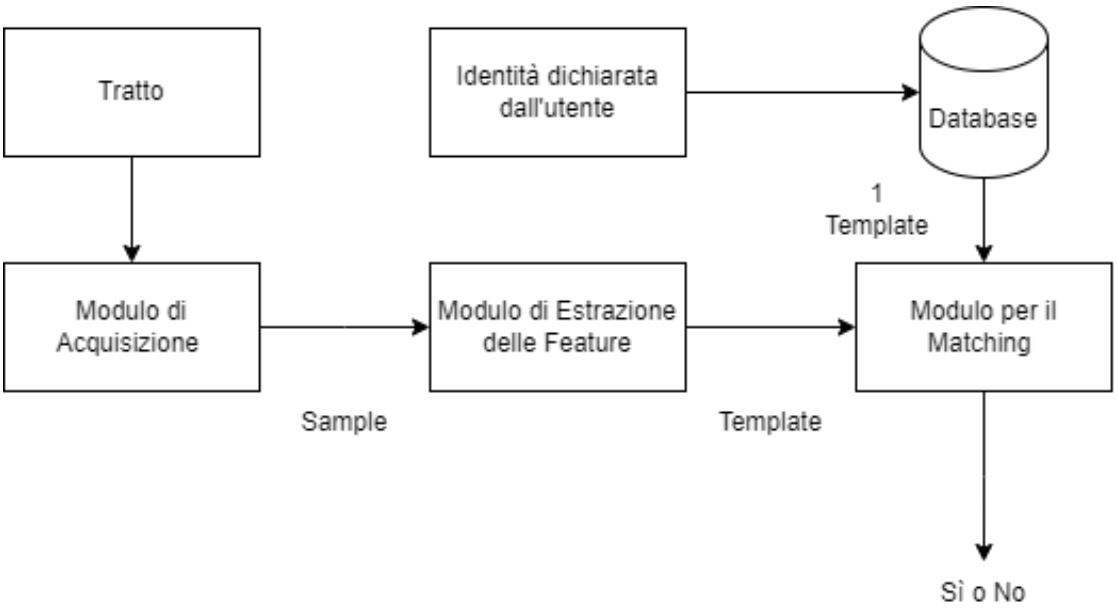


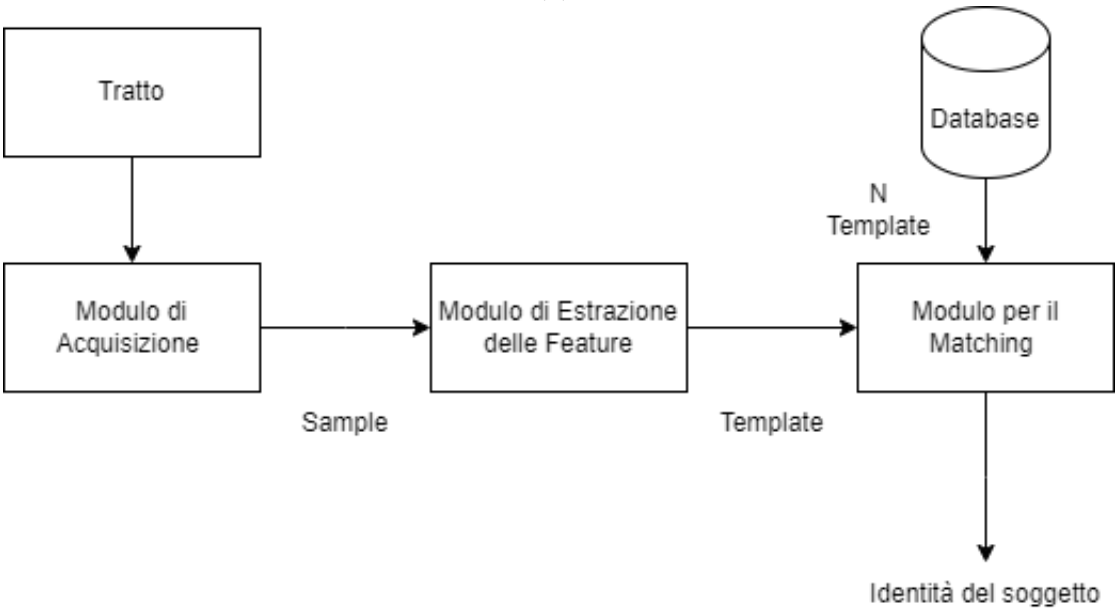
Figura 3: Rappresentazione delle feature in uno spazio N-dimensionale.

viene confrontato con il template della persona precedentemente memorizzato nel database. Nel caso di Identification il tratto appena acquisito sarà invece confrontato con N template presenti nel database. Il risultato del confronto è valutato con una soglia di tollerabilità: questa soglia rappresenta un valore arbitrario che determina quanto il tratto biometrico acquisito deve corrispondere al template per consentire l'accesso. Se il tratto biometrico riconosciuto è sufficientemente simile al template e supera la soglia di tollerabilità, l'accesso è consentito (Figura 4).

La soglia di tollerabilità svolge un importante ruolo nel funzionamento del sistema biometrico. Se è impostata troppo alta significa che il sistema richiede un match quasi perfetto tra il tratto biometrico acquisito e il template memorizzato. Tuttavia, tale precisione estrema è irrealistica poiché durante l'acquisizione possono verificarsi piccoli errori o variazioni legate a rumori ambientali. Quindi in caso di match perfetto probabilmente si è sotto attacco di tipo replay attack, in



(a)



(b)

Figura 4: Schema della fase di Riconoscimento. Verification (a), Identification (b).

cui un malintenzionato è riuscito a inserirsi nella catena di acquisizione usando un sample vecchio.

D'altra parte, se la soglia è impostata troppo bassa, il sistema può diventare poco affidabile, consentendo l'accesso a soggetti non autorizzati. Pertanto, la scelta della soglia di tollerabilità deve essere attentamente bilanciata per garantire sia l'accuratezza nell'identificazione delle persone che l'efficienza operativa del sistema. Nel caso in cui un sistema si sbagli possiamo distinguere due tipi di errori:

- False Match, quando un soggetto che non poteva accedere al sistema è invece entrato perché il Riconoscimento lo ha scambiato per un soggetto legittimo.

$$FM\,Rate = \frac{FM}{Totale\,impostori} \tag{1}$$

- False Non-Match, quando un soggetto legittimo non entra nel sistema perché il Riconoscimento ritiene che il suo template non assomigli a quello registrato.

$$FNM\,Rate = \frac{FNM}{Totale\,genuini} \tag{2}$$

Sia in un grafico distribuzioni tra impostori e genuini come in Figura 5. Sia T la soglia. Il numero delle persone genuini sotto la soglia T (FNMR) deve essere calcolato come un integrale della funzione di curva dei genuini fino alla soglia T.

$$FNMRate = \int_{-\infty}^{T} p_m(s)\,ds \tag{3}$$

Invece, il numero di persone impostori sopra la soglia T deve essere calcolato come integrale partendo dalla soglia T della curva degli impostori.

$$FMRate = \int_{T}^{\infty} p_n(s)\,ds \tag{4}$$

Come abbiamo appena visto la soglia di tollerabilità non è un parametro assoluto, bensì un parametro arbitrario che va regolato in base al problema e alla tecnologia in questione. Non è l'unico parametro usato in biometria, infatti uno dei tanti usati vi anche il Decision Error Tradeoff (DET) che valuta le performance del sistema mostrando come variano FNMR e FMR con la soglia T.

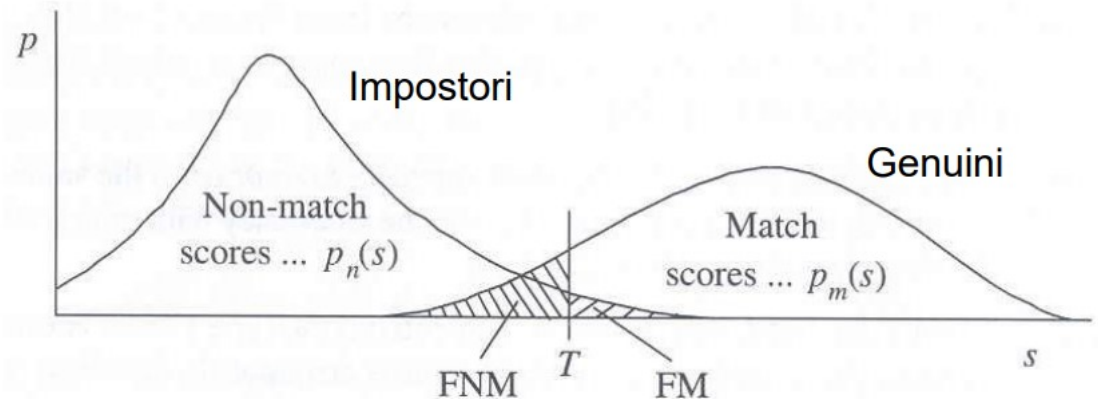


Figura 5: Esempi di distribuzioni delle funzioni impostori (Non-Match) e genuini (Match).

1.2 Deep Learning

Negli ultimi anni grazie al progresso nel settore dell'intelligenza computazionale si sta sempre più facendo uso di metodi di apprendimento automatico applicati alla biometria. Nella programmazione tradizionale si usano gli algoritmi per produrre risultati (soluzioni) attraverso i dati di un problema che si vuole risolvere. $Dati + Algoritmi = Risultato$.

Invece il Machine Learning (un sottoinsieme dell'intelligenza artificiale) crea nuovi algoritmi partendo dai dati e risultati. $Dati + Risultati = Algoritmi$. È una metodologia che insegna al sistema d'imparare dall'esperienza.

Vi sono due metodi di ragionamento di un sistema automatico: Induttivo, ossia un sistema capace di apprendere creandosi delle regole partendo dai dati come esempio. Deduttivo, è un sistema che apprendimento dalle regole già specificate.

Nella biometria si fa uso specialmente il tipo di apprendimento Induttivo, poiché risultata più facile la progettazione partendo da esempi di dati già esistenti per ricavare le regole di riconoscimento (Pattern), invece dell'uso del tipo di apprendimento Deduttivo che necessita di fornire una regola di riconoscimento, ma nessuno riesce veramente a fornire tale equazione formale in base alla teoria.

Il Machine Learning può usare i seguenti tipi di addestramento: Supervisionato, quando il modello apprende da dati in input e anche dai dati in output. Non-Supervisionato il modello apprende i pattern partendo solo da dati in input (non

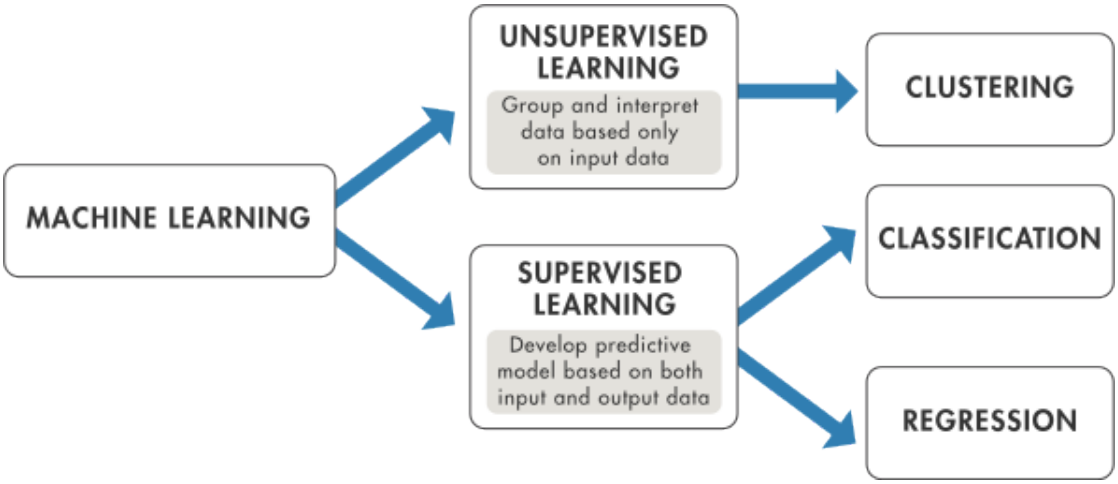


Figura 6: Esempi di tipo di addestramento e di problemi.

viene fornito l'output). Semi-Supervisionato vengono forniti dati in input e in output in modo ridotto.

Vi sono diversi tipi di problemi comuni che il Machine Learning può affrontare:

- Regressione, l'obbiettivo è prevedere un valore numerico continuo. Ad esempio prevedere il prezzo di un immobile in base alle sue caratteristiche (come metri quadrati, numero di stanze, ecc.). Qui il modello deve imparare una funzione che mappa le variabili di input a un valore continuo. Può essere Regressione Lineare altrimenti Non-Lineare.

- Classificazione, l'obiettivo è prevedere un valore numerico discreto per assegnare un'etichetta o una classe a un input. Ad esempio classificare se una e-mail è spam o non spam è un problema di classificazione binaria. La classificazione multiclasse, d'altra parte, coinvolge la suddivisione degli input in più classi distinte (ad esempio, riconoscere il tipo di animale in un'immagine tra gatto, cane o uccello). Qui il modello deve imparare a distinguere tra diverse categorie.

Vi sono molti altri problemi, come ad esempio il Clustering per l'analisi esplorativa dei dati con lo scopo di trovare pattern nascosti o raggruppamenti nei dati. Oppure la Segmentazione per la suddivisione di un'immagine in regioni o pixel specifici. Oppure la Generazione per generare nuovi dati eccetera... (Figura 6).

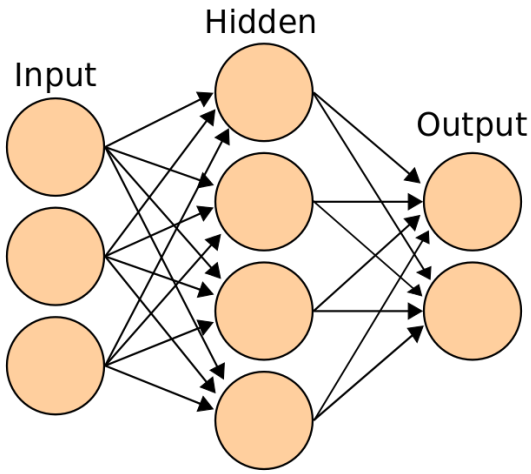


Figura 7: Architettura di una rete neurale.

Noi in biometria affronteremo un problema di classificazione: dato un soggetto vogliamo classificarlo, ossia produrre un valore numerico discreto per distinguerlo a quale identità corrisponde di più.

Uno dei modelli di Machine Learning sono le Reti Neurali, modelli ispirati al funzionamento dei neuroni dell'encefalo umano. Questi modelli consistono in strati (input layer, hidden layer, output layer) di nodi, noti come neuroni artificiali, che sono collegati tra loro da pesi. Durante il processo di addestramento, i pesi dei collegamenti vengono aggiornati in base ai dati di input e output, consentendo alla rete neurale di apprendere pattern complessi e relazioni nei dati (Figura 7).

L'output di un neurone è determinato dal risultato della funzione di attivazione al valore ponderato degli input forniti dai neuroni del layer precedente. Formalmente, se abbiamo un neurone con input $x_1, x_2, \ldots, x_n$ e pesi associati $w_1, w_2, \ldots, w_n$, l'attivazione a è data da $\sigma(w_1 \cdot x_1 + w_2 \cdot x_2 + \cdots + w_n \cdot x_n + b)$, dove b rappresenta il bias.

Vedremo nel dettaglio il funzionamento di attivazione dei layer nel capitolo 2 di questo lavoro.

Il Deep Learning è una forma specializzata di Machine Learning.

$$Deep\,Learning \subset Machine\,Learning \subset Intelligenza\,Artificiale$$

Utilizza anche lui la Rete Neurale ma si differenzia dal fatto che esso usa molteplici hidden layer, da qui il suo nome "Profondo". Una delle tipologie di architetture più comuni è con l'uso di layer per convoluzioni rendendo così l'intera Rete una Convolutional Neural Network (CNN).

Nei sistemi di riconoscimento biometrico basati su elettrocardiogrammi, le reti neurali possono essere addestrate per riconoscere pattern specifici nelle onde elettriche generate dal cuore. Questo approccio offre una flessibilità notevole nel rilevare variazioni individuali nei segnali cardiografici, contribuendo a migliorare l'accuratezza e l'affidabilità del sistema di riconoscimento.

1.3 Sistema cardiovascolare e ECG

Nelle prossime sotto-sezioni, esploreremo in modo veloce il flusso cardiocircolatorio nel sistema umano. Comprenderemo come il cuore pompa il sangue attraverso il corpo, garantendo l'apporto di ossigeno e nutrienti a tutti gli organi e tessuti. Questa comprensione del flusso sanguigno serve per apprezzare il funzionamento complessivo del sistema cardiovascolare ma fondamentale anche per la comprensione del lavoro svolto nell'elaborato.

Successivamente, approfondiremo il funzionamento dell'elettrocardiogramma, che da qui in poi faremo riferimento come ECG. Esso è uno strumento cruciale nella diagnosi e nel monitoraggio delle condizioni cardiache. Esploreremo come funziona, come viene utilizzato per registrare l'attività elettrica del cuore e come fornisce informazioni preziose sulla salute cardiaca. Con una panoramica completa sull'ECG, saremo in grado di analizzare i dati e le tracce elettrocardiografiche in modo più efficace, contribuendo così alla nostra comprensione l'utilizzo di esso nel riconoscimento biometrico.

1.3.1 L'apparato circolatorio e il funzionamento del cuore

L'apparato circolatorio cardiovascolare è costituito dal cuore e dai vasi sanguigni, il suo compito è il trasporto del sangue in tutte le parti del corpo con lo scopo di dare ossigeno e sostanze nutritive alle cellule, trasportare messaggeri chimici (e.g. ormoni) e spostare le sostanze di rifiuto dal metabolismo cellulare. Non solo, infatti

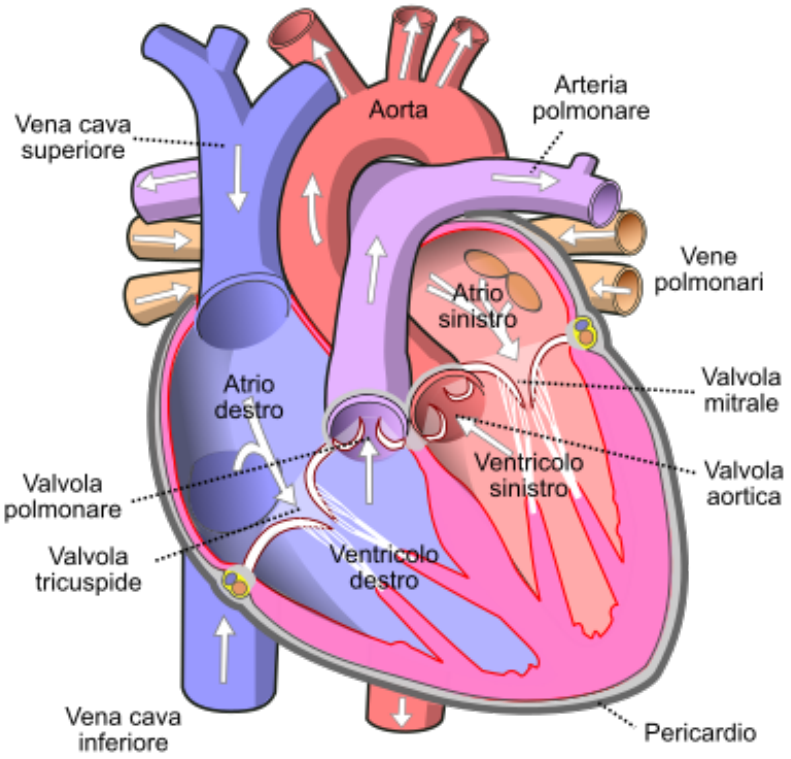


Figura 8: Struttura del cuore [4].

ha anche il compito di proteggere da attacchi da sostanze esterne all'organismo grazie all'azione di alcune cellule speciali e alla presenza di anticorpi. Proprio come la difesa da un attacco in cybersecurity.

L'organo che permette pompare il sangue per raggiungere tutte le nostre cellule del corpo è il cuore. Esso ha forma conica e posizionato leggermente inclinato verso sinistra nel torace tra i due polmoni, la cui prima contrazione inizia dalla quarta settimana di gestazione. In mezzo alla membrana interna e alla membrana esterna che le riveste (chiamate endocardio e pericardio) ha un piccolo spazio che contiene liquido pericardico che protegge dai fenomeni di attrito. La maggior parte della parete cardiaca è rappresentata dal miocardio che è un tessuto muscolare striato e involontario responsabile di generare la forza necessaria per permettere la contrazione ritmica e coordinata del cuore in modo autonomo e ininterrottamente fino alla morte.

La cavità cardiaca è divisa in quattro spazi: le parti superiori sono detti atrio

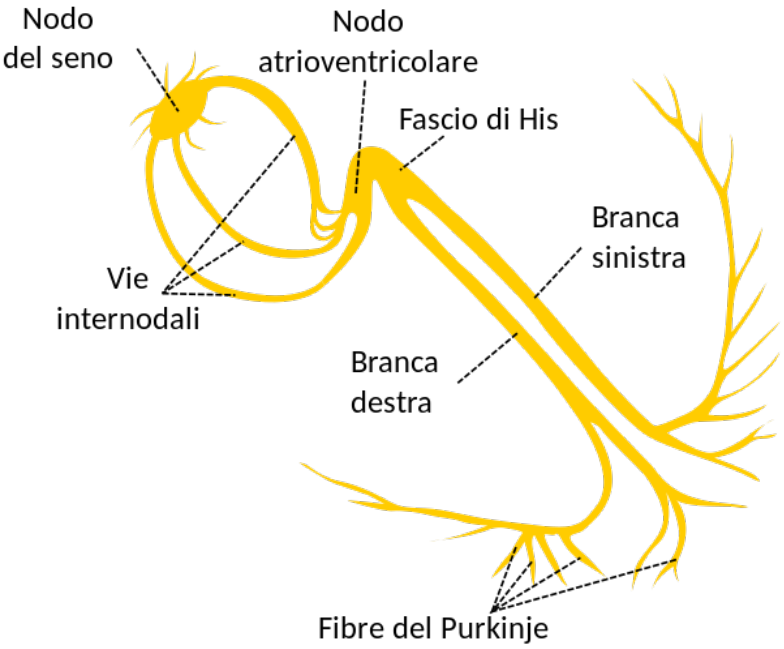


Figura 9: Struttura del sistema di conduzione del cuore, che attraverso impulsi elettrici fa contrarre il cuore [4].

destro e atrio sinistro, quelle inferiori ventricolo destro e ventricolo sinistro. La parte sinistra è separata da quella destra da un setto interatriale e interventricolare che non permette di mescolare il sangue ossigenato della parte sinistra al sangue non ancora ossigenato della parte destra.

Atri e ventricoli della stessa parte sono in comunicazione grazie alle valvole cardiache, componenti meccaniche che permettono solo un flusso unidirezionale così da impedire il reflusso di sangue rispetto alla direzione imposta dalla circolazione sanguigna: si aprono per lasciare passare il sangue e si chiudono per impedire il ritorno. In totale sono quattro: quella che connettono l'atrio e ventricolo destro e costituita da tre lembi valvolari è detta tricuspide, mentre quella che connette atrio e ventricolo sinistro costituita da due lembi valvolari è chiamato bicuspide o mitrale. Le altre si chiamano valvole semilunari, e si trovano fra il ventricolo sinistro e l'arteria aorta e fra il ventricolo destro e l'arteria polmonare sinistro, esse controllano il flusso in uscita dal cuore (Figura 8).

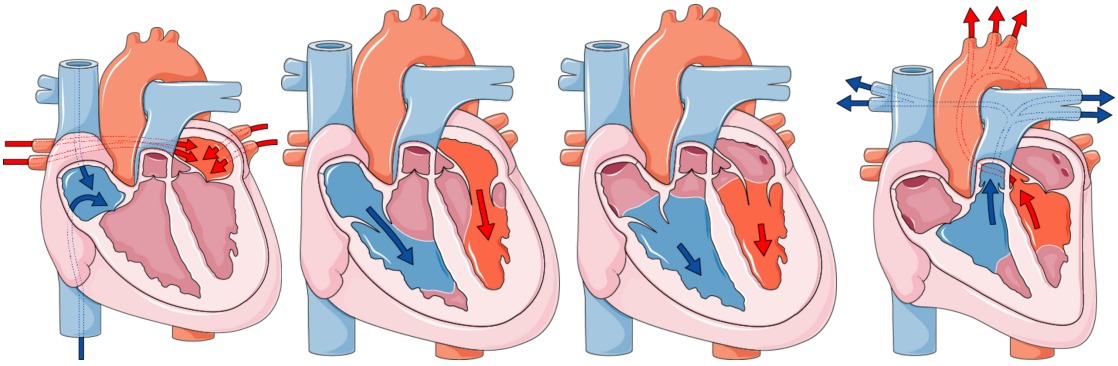
La muscolatura del cuore si contrae spontaneamente e ritmicamente anche se

le connessioni nervose sono interrotte, ciò grazie al sistema di conduzione (Figura 9) che presenta una modifica della muscolatura cardiaca che, andando in ordine, è costituito così: Nodo senoatriale, il pace maker naturale del cuore, è un piccolo ammasso di cellule speciali situato nell'atrio destro allo sbocco della vena cava superiore, ed è responsabile di generare gli impulsi elettrici iniziali che guidano la contrazione. Produce una ritmicità che determina la frequenza cardiaca. Nodo atrioventricolare, situato nella parte inferiore del setto interatriale, riceve il segnale elettrico e a sua volta produce un segnale elettrico che lo fa passare nel fascio atrioventricolare di His estendendolo verso il basso, nel setto interventricolare fino alle fibre di Purkinje all'interno delle pareti ventricolari che fanno contrarre i ventricoli.

A ogni contrazione corrisponde un battito, e l'intervallo di tempo che separa ogni battito costituisce un ciclo cardiaco. Tutti gli eventi del sistema di conduzione sopra esposti costituiscono la contrazione e il rilassamento di entrambi gli atri, più la contrazione e il rilassamento di entrambi i ventricoli. In termini medici si chiamano sistole e diastole. Durante la diastole atriale, gli atri si riempiono di sangue facendo aumentare la pressione e causando alle valvole tricuspide e bicuspide di aprirsi all'inizio della sistole atriale, lasciando fluire il sangue nei ventricoli che si riempiono. Nella fase della diastole ventricolare la pressione si sposta quindi nei ventricoli causando alle valvole atrioventricolari di chiudersi a seguito della sistole ventricolare. Questa sistole fa aprire le valvole semilunari favorendo l'afflusso del sangue nelle arterie (Figura 10).

Tutta questa attività cardiaca è permessa grazie alle speciali cellule del miocardio che permettono la propagazione elettrica: queste cellule mantengono differenze di concentrazione ionica tra l'interno e l'esterno della miocellula, costituendo la base della differenza di potenziale elettrico pari a $\approx -80mV$. Prima di contrarsi, la cellula deve prima produrre un potenziale d'azione, ossia che deve andare in contro a una serie di fasi ai quali il potenziale di membrana passerà da negativo a positivo:

- Fase 0 - Depolarizzazione Rapida, i canali del sodio (Na+) si aprono rapidamente, consentendo all'ioni sodio di entrare nelle cellule cardiache provocando una rapida depolarizzazione della membrana cellulare.



(a) (b) (c) (d)

Figura 10: Fasi del ciclo cardiaco. Diastole atriale, fa riempire gli atri di sangue (a). Sistole atriale, fa aprire le valvole atrioventricolari facendo scorrere il sangue nei ventricoli (b). Diastole ventricolare, punto che fa riempire i ventricoli (c). Sistole ventricolare, fa fluire il sangue nell'aorta e nell'arteria polmonare (d) [4].

- Fase 1 - Riduzione della Depolarizzazione, i canali del sodio si inattivano rapidamente, riducendo l'ingresso di sodio, seguito da un efflusso di ioni cloro e potassio, contribuendo alla riduzione della depolarizzazione.

- Fase 2 - Plateau, i canali del calcio (Ca2+) si aprono, consentendo all'ioni calcio di entrare nelle cellule contribuendo a mantenere la depolarizzazione elettrica per un periodo prolungato, noto come "plateau". È cruciale per evitare che il cuore si contragga troppo rapidamente e consente il tempo necessario per la pompa cardiaca.

- Fase 3 - Ripolarizzazione i canali del potassio (K+) si aprono, consentendo all'ioni potassio di uscire rapidamente dalle cellule. Ciò provoca la ripolarizzazione della membrana cellulare, riportandola allo stato di riposo e preparandola per il successivo potenziale d'azione.

- Fase 4 - Riposo. Le cellule cardiache ritornano allo stato di riposo, in attesa di ricevere un nuovo segnale elettrico.

1.3.2 Elettrocardiogramma

I micro-impulsi di correnti elettriche generati dal miocardio esposti nella precedente sotto-sezione, si diffondono nei tessuti circostanti e possono affiorare sulla superficie cutanea. Piazzando elettrodi sulla pelle e amplificando adeguatamente il segnale è quindi possibile captare e registrare questi impulsi mediante un dispositivo chiamato elettrocardiografo. Questo apparecchio è stato modificato e migliorato da Willem Einthoven[1] e Étienne-Jules Marey nel 1903 per derivazione diretta da un galvanometro a corda [12].

La registrazione grafica degli eventi elettrici del cuore è detta elettrocardiogramma (ECG o EKG[2]), costituisce una grande importanza clinica per permettere la diagnosi di patologie e irregolarità del ritmo cardiaco.

Graficamente è costituita da onde come esposto in Figura 11. Un normale tracciato ECG è caratterizzato di un'onda P che corrisponde all'impulso elettrico generato dal nodo senoatriale. Il segmento P-Q rappresenta il tempo con cui il segnale viaggia dal nodo senoatriale al nodo atrioventricolare. Il complesso QRS è la fase in cui il nodo atrioventricolare genera il suo impulso e rappresenta la depolarizzazione ventricolare: nello specifico, l'onda Q rappresenta la depolarizzazione del setto interventricolare, l'onda R è invece prodotto dalla depolarizzazione della maggior parte della massa ventricolare, e l'onda S rappresenta l'ultima fase della depolarizzazione ventricolare della base del cuore. Durante questo periodo vi è anche la ripolarizzazione degli atri ma tale segnale è oscurato dal complesso QRS. Il segmento S-T riflette la fase di plateau del potenziale d'azione miocardico. L'onda T rappresenta la ripolarizzazione dei ventricoli che avviene immediatamente prima del diastole ventricolare. Il ciclo ricomincia periodicamente per ogni battito cardiaco.

Da un punto di vista pratico il segnale ECG non è un solo tracciato come in Figura 11, ma è un insieme di più tracciati chiamati derivazioni. Le 12 derivazioni rappresentano 12 immagini elettriche prodotte dal cuore da 12 angolazioni diverse. Prevede il collegamento di 10 elettrodi: uno per ogni arto e sei per il torace. Questo permette sei derivazioni sul torace che rappresentano una prospettiva di

[1] Premio Nobel per la medicina nel 1924
[2] Talvolta è usata anche la sigla tedesca

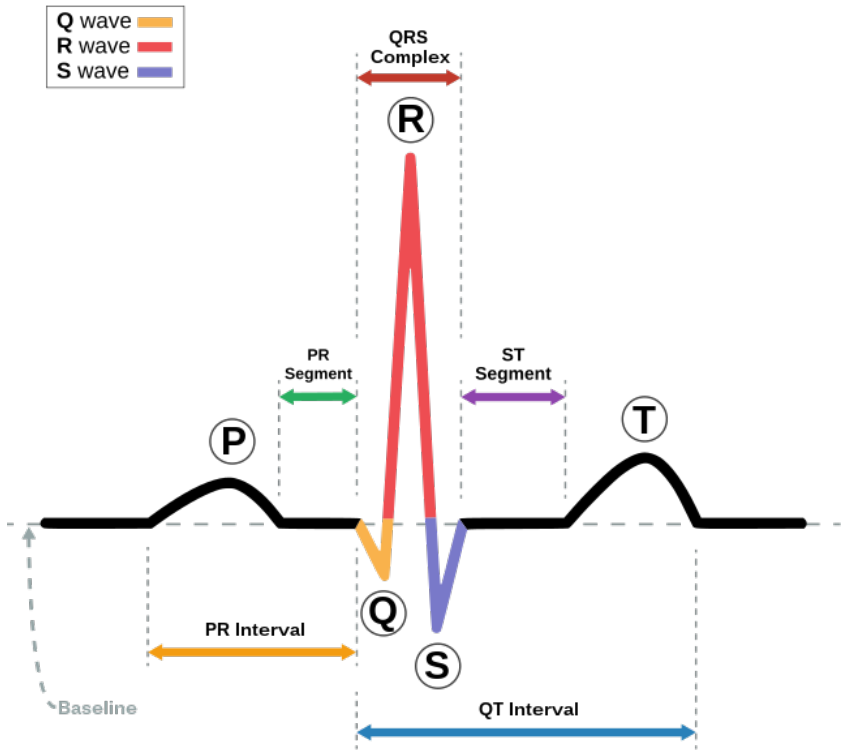


Figura 11: Segnale elettrocardiografico [4].

angolazione verticale del cuore chiamati I, II, III, aVR, aVL, aVF. E sei sul torace che rappresentano la prospettiva orizzontale denominati V_1 fino a V_6 (Figura 12).

La depolarizzazione verso un elettrodo produce una deflessione positiva sul grafico: la depolarizzazione lontano da un elettrodo dà una deflessione negativa. Il contrario avviene per la ripolarizzazione, pertanto i sensori che guardano il cuore da diverse angolazioni possono avere onde che puntano in direzioni opposte.

La combinazione di derivazioni degli arti e precordiali consente agli operatori sanitari di ottenere una visione tridimensionale dell'attività elettrica del cuore. Le varie angolazioni catturate da queste derivazioni permettono d'individuare eventuali anomalie nell'attività elettrica in diverse regioni del cuore. Ad esempio, le derivazioni precordiali sono particolarmente utili per individuare le variazioni nelle pareti anteriori, laterali e inferiori del cuore.

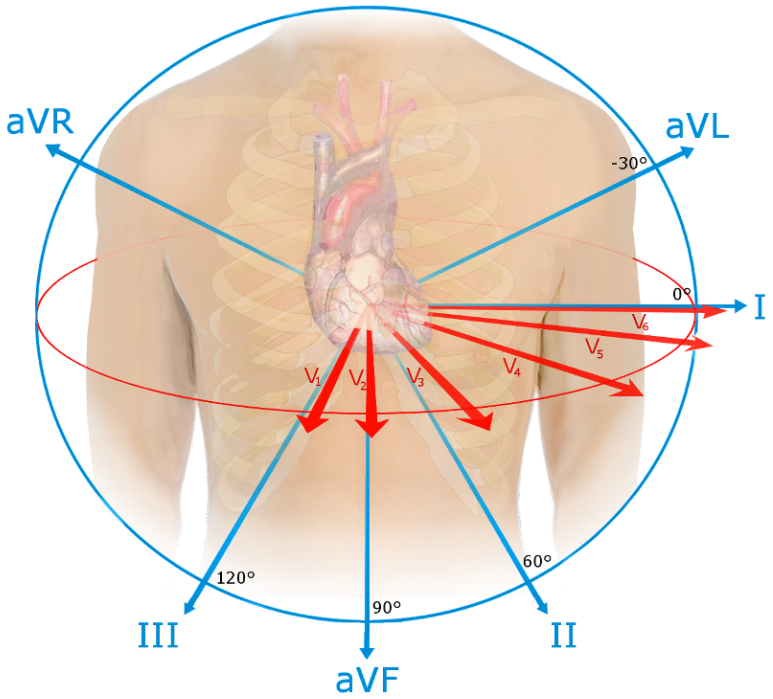


Figura 12: Standard 12 derivazioni. I vettori in rosso rappresentano il cuore sul piano orizzontale, quelli in blu sul piano verticale [4].

1.4 Stato dell'arte

Negli ultimi anni il campo della ricerca ha sempre più dato fiducia nel riconoscimento biometrico da segnali ECG, anche grazie alle sue caratteristiche che lo distingue dai metodi che usano altri tratti biometrici [9]:

- Rilevamento di vita, un segnale ECG può essere rilevato solo da individui viventi.
- Sicurezza, la biometria basata su ECG è particolarmente sicura poiché a oggi è difficile riprodurre artificialmente un battito cardiaco.
- Informazioni aggiuntive, oltre a poter riconoscere un individuo, un segnale ECG può dare informazioni sulle condizioni di salute del paziente e il suo stato emotivo, ad esempio determinare eventuali malattie cardiache e/o il suo livello di stress.

Infatti il vantaggio di ottenere informazioni aggiuntive come quelle relative alla salute del cuore può contribuire notevolmente il miglioramento della vita. Secondo i dati del World Health Organization (WHO), nel 2019 le principali cause di morte sono infarti e la malattie coronariche del cuore, che è dovuto alla difficoltà del cuore a riceve sangue dalle arterie coronarie. Le nuove tecnologie come Internet of Things nell'ambito medico potrebbero aiutare in questo scopo ampliando il telehelth, un tipo di sistema medico smart [2].

La distintività dei segnali ECG di ciascun individuo è determinata da una serie di fattori legati alle caratteristiche fisiche del cuore, i quali a loro volta possono essere influenzati dalla costituzione fisica e dallo stile di vita dell'individuo. Ad esempio, in individui alti e snelli, il cuore tende ad adattarsi alle dimensioni del torace assumendo un profilo più allungato, mentre in individui più bassi il cuore può essere più grande e orientato in modo più trasversale. Le differenze nell'attività fisica di un individuo si riflettono chiaramente nei tracciati ECG. Un soggetto che pratica regolare attività fisica può presentare un andamento distintivo rispetto a uno sedentario. La distintività si estende anche a livello cellulare, influenzata dai cambiamenti ionici nei potenziali elettrici e dai livelli di elettroliti nel plasma. Tutte queste caratteristiche possono produrre variazioni nella forma delle onde e la frequenza cardiaca, offrendo un'ulteriore dimensione di unicità al segnale ECG.

Nonostante i numerosi progressi raggiunti nella letteratura, non esiste ancora un consenso sulla metodologia più appropriata da usare sull'acquisizione come per il riconoscimento del volto. Infatti esiste uno standard dell'ICAO (International Civil Aviation Organization), un'agenzia specializzata delle Nazioni Unite, che definisce uno standard per le acquisizioni d'immagini per il riconoscimento facciale. Il documento specifica requisiti tecnici dettagliati per le immagini utilizzate nei documenti di viaggio, come i passaporti biometrici. Questi requisiti includono specifiche riguardanti l'espressione del viso, che deve essere neutra durante l'acquisizione dell'immagine, stabilisce la posizione del viso nella fotografia in modo che sia possibile ottenere immagini coerenti e confrontabili, stabilisce inoltre requisiti relativi all'illuminazione e all'assenza di ombre per garantire che il viso sia chiaramente visibile e riconoscibile, e definisce le dimensioni esatte della fotografia del viso per garantire uniformità tra i documenti di viaggio emessi da diverse giurisdizioni.

Vi sono tre modalità di acquisizione dell'ECG, come delineato da Ardeti et al. [2]. La modalità *in-the-person* implica l'utilizzo di elettrodi posizionati all'interno del corpo sotto forma di pillole. La modalità *on-the-person*, d'altra parte, prevede comunemente l'applicazione di alcuni elettrodi direttamente sulla superficie del corpo. Infine, la modalità *off-the-person* rileva l'ECG attraverso il contatto sulla superficie cutanea con uno o pochi elettrodi. Quest'ultima modalità non richiede l'uso di gel tra l'elettrodo e la pelle, a differenza del metodo *on-the-person* che spesso irrita la pelle del soggetto. Tuttavia, è più soggetta alla presenza di rumori ambientali.

Nonostante la potenziale problematica legata ai rumori, lo studio [9] ha suggerito che un elettrodo di tipo off-the-person può essere sufficiente per il riconoscimento dell'identità. In particolare, è emerso che il metodo di acquisizione dell'ECG rilevate dalle dita ha dimostrato prestazioni superiori rispetto ad altre tecnologie.

La fase del preprocessing svolge un ruolo vitale per il sistema biometrico: acquisendo un segnale con meno rumori garantisce precisioni migliori. In numerosi ricerche si usano differenti tipi di filtri dei segnali [2] per cercare di attenuare la rumorosità, tuttavia si sottolinea che l'uso eccessivo potrebbe modificare e compromettere il segnale.

Secondo la letteratura, si preferisce la posizione supina dell'utente in fase di acquisizione, ma ciò limita i movimenti in scenari ordinari. Tuttavia si è provato che la posizione da seduto garantisce performance più elevate. Per il tempo di acquisizione c'è un dibattito nel campo scientifico tra le acquisizioni a lungo e a breve termine, ma si è dimostrato che si preferisce quello a breve termine, poiché quello a lungo termine garantisce performance migliori ma fino a un certo punto [9]. Esistono tre categorie di estrazioni delle feature: *Fiducial, Non-Fiducial, Hybrid*. I primi si basano sull'analisi degli intervalli, dell'ampiezza e degli angoli dei punti delle onde P, complesso QRS, e l'onda T dell'ECG. La tecnica basata su Non-Fiducial point segmenta il tracciato in finestre, e include coefficienti di autocorrelazioni. Poi esistono metodi ibridi, che combinano sia tecniche Fiducial che Non-Fiducial localizzando i picchi R [9].

Pereira et al. [9] hanno concluso che un altro fattore che fa dipendere le performance del sistema è la grandezza del database, aumentando le dimensioni, si

riduce l'accuratezza del sistema, tuttavia non in modo drastico. Un altro fattore è quello temporale, più è datato il sample dell'enrollment più l'accuratezza diminuisce. Per quanto riguarda la fase di classificazione, esistono molti metodi proposti nel corso degli anni: Bayesian Network, Linear Discriminant Analysis, Decision Trees, k-Nearest-Neighbors, Support Vector Machines, e Artificial Neural Networks, ognuno con dei vantaggi e svantaggi.

1.5 Contesto del laboratorio

Il laboratorio BiSP (Biomedical Image and Signal Processing Lab) dell'Università degli Studi di Milano è impegnato in una vasta gamma di attività mirate a contribuire all'avanzamento della ricerca e dello sviluppo in ambito biomedico. Le principali aree d'interesse e attività svolte includono:

Elaborazione di immagini e segnali biomedici Sviluppi di metodi e algoritmi avanzati per l'elaborazione di immagini e segnali biomedici. Questa attività include l'analisi, la classificazione e la visualizzazione di dati provenienti da diverse fonti, come ECG, elettroencefalogramma (EEG), segnali accelerometrici, immagini mediche. L'obiettivo è estrarre informazioni significative da queste fonti di dati per comprendere meglio le condizioni di salute, identificare pattern anomali e supportare la diagnosi medica.

Intelligenza computazionale e simulazioni computerizzate Il laboratorio utilizza approcci avanzati di intelligenza artificiale, tra cui reti neurali, algoritmi di data analisys e apprendimento automatico, per affrontare problemi biomedici complessi. Questi metodi consentono di creare modelli matematici e simulazioni di sistemi biologici, consentendo una migliore comprensione dei processi biologici e delle dinamiche fisiologiche. L'impiego dell'intelligenza computazionale contribuisce in modo significativo alla ricerca in settori come la biologia computazionale e la modellazione di patologie.

Applicazioni biomediche Il BiSP collabora attivamente con medici, biologi e ingegneri per sviluppare strumenti innovativi utilizzati nella diagnosi, prognosi e

monitoraggio di una varietà di patologie. Queste applicazioni biomediche possono spaziare dalle malattie cardiovascolari alle patologie neurodegenerative e metaboliche. Il laboratorio mira a tradurre la ricerca e le scoperte scientifiche in soluzioni pratiche che possano avere un impatto positivo sulla salute umana.

Complessivamente, il laboratorio svolge un ruolo essenziale nell'avanzamento delle conoscenze nel campo biomedico e nella promozione di soluzioni innovative che beneficiano la comunità scientifica e medica, nonché la società nel suo complesso. Le sue attività sono incentrate sulla creazione e l'applicazione di strumenti di elaborazione dati avanzati e modelli matematici per affrontare sfide biomediche complesse e migliorare la qualità della vita delle persone.

1.6 Obiettivi della ricerca

Questo lavoro di tesi si propone di valutare le prestazioni di una Rete Neurale Convoluzionale (CNN) nell'ambito del riconoscimento delle identità attraverso segnali ECG. In particolare gli obiettivi principali della ricerca sono:

1. Quantificare l'accuratezza del Modello Neurale:
    (a) Analizzare l'effetto della variazione del numero di soggetti coinvolti nello studio sulla performance del modello neurale.
    (b) Esaminare l'impatto della variazione del numero di derivazioni utilizzate nella registrazione dell'ECG sulla precisione del modello.
    (c) Valutare come la variazione del numero di tracciati ECG acquisiti per ogni soggetto influenzi le prestazioni del modello di riconoscimento.
    (d) Investigare l'effetto della durata del tracciato ECG sulla capacità identificativa della CNN.
2. Analizzare aspetti di sicurezza:
    (a) Esplorare la robustezza del sistema proposto rispetto a possibili attacchi.
    (b) Valutare l'uso di identificazione tramite ECG nel contesto reale.

Attraverso la realizzazione di questi obiettivi, intendiamo contribuire alla comprensione delle potenzialità e delle sfide nel campo del riconoscimento biometrico basato su segnali ECG, fornendo insights utili per l'implementazione pratica di sistemi di sicurezza basati su questa tecnologia.

Capitolo 2

Metodologia di ricerca

In questo capitolo viene descritta parte operativa della Ricerca. Lo scopo del Machine Learning e del Deep Learning è prendere dei dati, fare un modello algoritmico (come una Rete Neurale), per poi trovare pattern nei dati, e usarli per fare predizioni future. Faremo uso di PyTorch, un framework open-source di apprendimento automatico basato sulla programmazione dinamica. È particolarmente noto per la sua flessibilità e facilità d'uso, ed è ampiamente utilizzato sia in ambito accademico che industriale, infatti ad oggi è il primo framework più utilizzato per il Deep Learning[1]. PyTorch utilizza il concetto di tensori come unità fondamentale.

I tensori rappresentano un'astrazione matematica e un concetto chiave nell'ambito della teoria dei campi, dell'analisi funzionale e dell'informatica. Si trattano di strutture matematiche versatili che generalizzano vettori e matrici, permettendo di modellare in maniera efficiente dati multidimensionali. In termini più semplici, un tensore può essere considerato come un contenitore di dati che organizza informazioni in più dimensioni. Ad esempio, un tensore di ordine zero è uno scalare, un tensore di ordine uno è un vettore, un tensore di ordine due è una matrice, e così via... (Figura 13).

In informatica i tensori vengono ampiamente impiegati per rappresentare dati complessi come immagini, sequenze temporali e altri dati multidimensionali, fornendo una struttura efficiente per eseguire operazioni matematiche e apprendere

[1] https://paperswithcode.com/trends

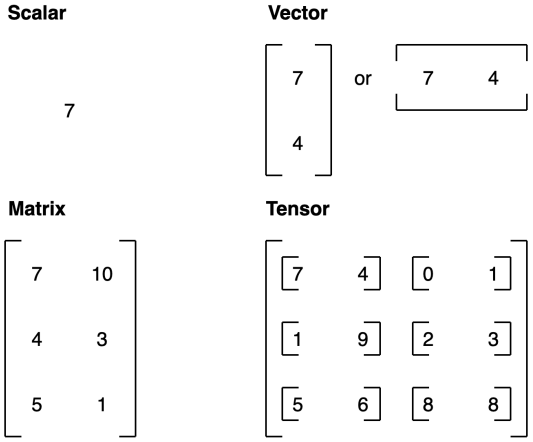


Figura 13: Rappresentazione di un valore scalare, vettore, matrice, tensore.

modelli complessi. Ad esempio consideriamo un'immagine a colori rappresentata in formato RGB. Questa immagine può essere rappresentata come un tensore tridimensionale, dove ogni dimensione corrisponde a un canale di colore (rosso, verde, blu), e le due dimensioni rimanenti rappresentano l'altezza e la larghezza dell'immagine. Supponiamo quindi che l'immagine sia H pixel in altezza, W pixel in larghezza e che sia rappresentata con C canali di colore, il tensore associato sarebbe di forma $[H, W, C]$.

Si farà uso dei tensori nella elaborazione dei dati ECG. Seguiremo il seguente workflow per la costruzione del modello di apprendimento automatico:

1. Preparazione dei dati: in questa fase vengono presi dei dati non solo come immagini ma possono essere anche una tabella di numeri (come un grande foglio di calcolo), immagini di qualsiasi tipo, video, file audio come canzoni o podcast, strutture proteiche, testo e altro ancora... Nel nostro contesto useremo un ampio dataset di dati ECG disponibile al pubblico, e li trasformeremo in tensori.

2. Costruzione del modello: in questa fase si crea un modello per apprendere pattern nei dati, sceglieremo una funzione loss function, un ottimizzatore e costruiremo un ciclo di allenamento.

3. Fare predizioni e valutazione del modello: qui dopo la fase di allenamento, il modello dovrà fare la fase di test sui pattern appresi.

2.1 Il Dataset

Il dataset utilizzato in questa Ricerca è il Smart Health for Assessing the Risk of Events via ECG (SHAREE database) [8] scaricato dalla PhysioNet[2], una piattaforma online dedicata all'accesso e alla condivisione di dati fisiologici e segnali biomedici per la comunità scientifica e di ricerca nel campo della medicina e delle scienze biologiche.

SHAREE è stato concepito con l'obiettivo primario d'investigare la possibilità d'individuare soggetti affetti da ipertensione arteriosa e con un elevato rischio di sviluppare eventi vascolari mediante l'analisi della variabilità della frequenza cardiaca. L'ipertensione arteriosa è una condizione in cui la pressione del sangue nelle arterie è costantemente elevata. Questo può verificarsi quando le arterie sono strette o bloccate, aumentando la resistenza al flusso sanguigno. La ricerca di Melillo et al. [8] mira a identificare indicatori precoci e predittivi che possano contribuire a una migliore gestione e prevenzione delle complicanze cardiovascolari in individui affetti da questa malattia. All'interno di questa iniziativa, SHAREE fa uso delle registrazioni Holter.

Un Holter è un dispositivo portatile che registra l'attività elettrica del cuore in modo continuo e prolungato, solitamente per un periodo di 24 ore. Questo strumento, composto da elettrodi applicati sulla pelle del paziente, cattura in tempo reale il ritmo cardiaco e le eventuali variazioni che possono verificarsi durante le attività quotidiane e il riposo. Queste registrazioni forniscono un quadro dettagliato e continuo del comportamento elettrico del cuore nel corso di una giornata completa, consentendo agli esperti di analizzare in modo approfondito la variabilità della frequenza cardiaca e d'individuare eventuali correlazioni con il rischio di eventi vascolari.

La raccolta di dati del database SHAREE comprende le registrazioni Holter provenienti da 139 pazienti ipertesi selezionati presso il Centro di Ipertensione dell'Ospedale Universitario di Napoli Federico II, Italia. I soggetti sono individui di età pari o superiore a 55 anni (49 donne e 90 uomini, con un'età compresa tra 72 e 87 anni) dopo un periodo di wash-out di un mese dalla terapia antipertensiva.

[2]https://physionet.org/

Nel periodo di follow-up di 12 mesi, 17 pazienti hanno manifestato eventi registrati, tra cui 11 infarti miocardici, 3 ictus e 3 eventi sincopali.

Ciascuna registrazione Holter contiene tre segnali ECG, ciascuno campionato a una frequenza di 128 campioni al secondo con una precisione di 8 bit. Vengono forniti, insieme ai tracciati nella cartella `files/`, anche i file di annotazioni, identificabili dal suffisso .qrs, che sono stati generati mediante l'utilizzo di un rilevatore automatizzato noto come WQRS [13] e non sono stati soggetti a correzioni manuali. Ogni registrazione è accompagnata da informazioni demografiche e cliniche, quali età, sesso, eventuali eventi vascolari, e valori di pressione arteriosa sistolica e diastolica, reperibili nel file info.txt. I leads forniti sono $III, V3, V5$.

Per il nostro obiettivo, usare tracciati ECG di soggetti non sani non è un problema poiché sarà comunque possibile garantire il riconoscimento anche da un tracciato con patologie cardiache. Inoltre, si assume che le registrazioni dei tracciati siano prive di bias di selezione, ossia una distorsione che si verifica quando i partecipanti a uno studio o un'analisi statistica non sono rappresentativi della popolazione di riferimento. In altre parole, assumiamo che il personale che ha registrato l'ECG dai pazienti, lo abbia fatto correttamente e in modo uniforme su tutta la popolazione di interesse.

2.1.1 Preparazione dei dati

In questa fase prepariamo i dati da elaborare nel modello neurale. Attraverso le due primitive di dati che PyTorch fornisce (`torch.utils.data.DataLoader` e `torch.utils.data.Dataset`) costruiremo una classe `HolterDataset` che dovrà restituire i tracciati.

```
1 path = 'files/'
2 dataset= HolterDataset(path)
```

Algoritmo 2.1: Creazione del dataset dal SHAREE dataset

I tracciati di SHAREE sono all'interno di una directory (files/) sono composti da tre file per ciascun paziente che sono identificati con un codice univoco, e.g. per il paziente con codice ID xxxx nella directory avrà `xxxx.dat`, `xxxx.hea`, `xxxx.qrs`.

La classe HolterDataset attraversa la directory specificata e ricava gli ID una sola volta per soggetto. Ricava anche i tracciati ECG tramite l'utilizzo della libreria

`WFDB`[3] della PhysioNet, un insieme di strumenti progettate per leggere, scrivere e manipolare dati provenienti da database di segnali biomedici. Per ogni segnale si considera solo dal 15 minuto del tracciato fino a 10 ore, così da avere tutti i tracciati Holter della stessa lunghezza.

A ogni tracciato vengono applicati due filtri. Filtro Passa-Banda di Butterworth di ordine 3 con frequenze di taglio tra 0.5 Hz e 40 Hz, che aiuta a mantenere solo le componenti del segnale che si trovano nella banda di frequenza specificata (tra 0.5 Hz e 40 Hz). Filtro Elimina-Banda (o notch) di ordine 3 a 50 Hz, per attenuare le componenti del segnale intorno a 50 Hz, che potrebbero essere dovute a interferenze o rumore.

Siccome vogliamo riconoscere i soggetti del nostro stesso dataset (un problema di identificazione chiusa), ogni ECG viene spezzettato in N finestre di tracciati da s secondi ciascuna, con distanza casuale tra loro, così da garantire che ogni soggetto abbia abbastanza materiale per un apprendimento e il riconoscimento dalla Rete Neurale (Figura 14). La classe HolterDataset alla fine del processo, restituisce gli ECG (sotto forma di tensori), l'id e la classe del label come valore intero.

I tracciati originali presentano valori NaN ("Not a Number"), un valore speciale usato per rappresentare un risultato indefinito in operazioni aritmetiche o matematiche. Questo è un problema per la rete neurale, poiché un singolo valore NaN moltiplicato con le matrici propagherà questo risultato, andando a rovinare tutti i valori della rete. Si aggira questo problema applicando l'interpolazione lineare, in parole semplici si tratta di una tecnica che consente di stimare o calcolare i valori intermedi tra due o più punti noti. L'obiettivo è quello di ottenere un'approssimazione di un valore sconosciuto in base a quelli noti. In pratica dove il segnale ECG presenta un NaN, si tira una retta tra le estremità così da sovrascrivere il NaN. Questo comporta a "inventarci" delle feature, ma le probabilità di usare quella parte del segnale sono minime, serve solo a non far propagare i NaN. Per facilitare i nostri esperimenti salviamo i segnali già filtrati e i relativi ID su un file `.npy`, così da evitare di attraversare la directory dove risiedono i dati.

[3]Waveform Database https://wfdb.io/

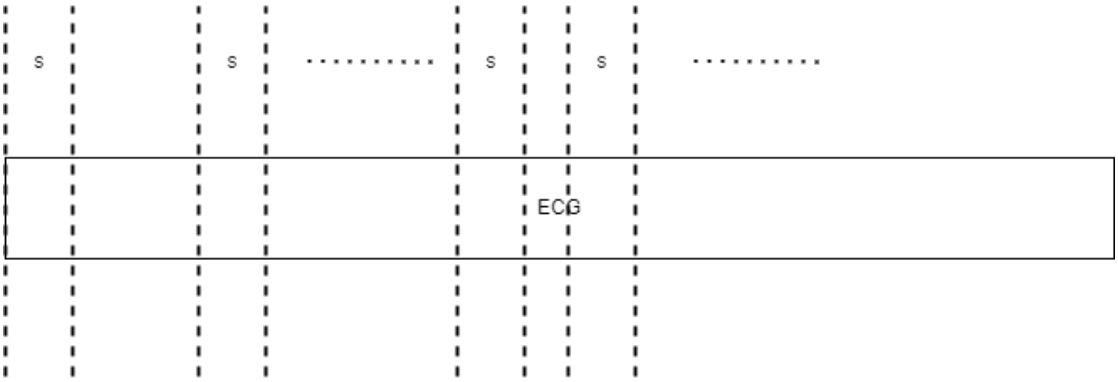


Figura 14: Ogni Holter ECG viene spezzettato in N diversi tracciati da s secondi con distanza casuale tra loro.

2.1.2 Splitting

Una parte fondamentale dello sviluppo di un modello di Rete Neurale è la suddivisione dei dati (splitting): ci servono dati per l'addestramento del modello, dati per la valutazione del modello dopo l'addestramento, e solitamente si fa uso anche di dati per la validazione che serve a validare il modello dopo l'addestramento e prima della valutazione. Possiamo pensarla alla seguente analogia: i dati di addestramento (train data) è il materiale che uno studente universitario studia durante il semestre, i dati di validazione (validation data) è il materiale sul quale lo studente testa le nozioni che ha studiato prima dell'esame, infine i dati per la valutazione (test data) è l'esame sul quale verrà testato lo studente.

Il test data non deve contenere dati già presentati nel train data, altrimenti il modello avrebbe performance elevate, ma non corrette. Faremo lo splitting con `random_split()` di PyTorch del dataset: 50% per il train dataset e 50% per il test dataset.

```
1 train_dataset, test_dataset = random_split(dataset,
2                                            [train_size, test_size])
```

Algoritmo 2.2: Splitting del dataset

Dividiamo ulteriormente ogni dataset con un DataLoader, che suddivide i dataset in batch di dimensioni più piccole, così il modello neurale elaborerà piccole quantità di dati alla volta. Inoltre permette anche il mescolamento dei dataset,

così da presentare in ordine casuale i dati al fine della generalizzazione del modello. In alcuni casi, soprattutto quando si lavora con grandi dataset, può essere vantaggioso parallelizzare il processo di caricamento dei dati per sfruttare appieno le risorse hardware disponibili (ad esempio con l'uso di thread o processi multipli).

```
train_loader = DataLoader(train_dataset,
                          batch_size=16,
                          shuffle=True)
test_loader = DataLoader(test_dataset,
                          batch_size=16,
                          shuffle=False)
```

Algoritmo 2.3: Caricamento del DataLoader

Dopo il DataLoader, l'input fornito al modello saranno gli ECG in tensori nella seguente forma: $[B, L, N]$ dove B è il numero di soggetti per batch, L il numero dei canali (leads), N è la durata di un segnale.

2.2 Modello

Il modello usato in questa ricerca si basa sul lavoro di R. Donida Labati et al., Deep-ECG [6]. La CNN è composta da sei blocchi convolutivi che usano neuroni ReLu (Rectified Linear Units), tre max-polling layer, tre LRN (Local Response Normalization) layers, un dropout layer, un layer fully-connected, e un layer Softmax.

I blocchi convolutivi servono per apprendere automaticamente pattern e strutture rilevanti nei dati multidimensionali in input attraverso l'applicazione di operazioni di convoluzione. I neuroni ReLU rappresentano una funzione di attivazione comunemente utilizzata nelle reti neurali artificiali per permettere la non linearità delle previsioni (siccome il nostro problema non è di tipo lineare). La loro forma matematica è semplice: per ogni input x la funzione ReLU restituisce 0 se x è negativo e x stesso se è positivo, ciò permette la non linearità del modello.

$$ReLU(x) = \max(0, x) \tag{5}$$

I neuroni ReLU si attivano solo se l'input è positivo. Questo significa che rispondono solo a certi tipi di segnali, introducendo una sorta di "soglia" di attivazione.

Il max-pooling è una tecnica di sottocampionamento durante la fase di pooling. Questa operazione è principalmente utilizzata per ridurre la dimensione spaziale di una rappresentazione, riducendo così il numero di parametri e calcoli nelle fasi successive della rete. Opera su ciascuna "finestra" della rappresentazione di input. Questa finestra si muove attraverso la rappresentazione in input con un passo (stride) specificato, e per ogni finestra il max-pooling seleziona il valore massimo tra quelli presenti nella finestra. Nonostante la riduzione delle dimensioni, il max-pooling cerca di conservare le feature salienti dell'input, mantenendo i valori massimi nelle diverse regioni.

I neuroni LRN servono per emulare il concetto di "inibizione laterale" esistente in neurobiologia. È un meccanismo attraverso il quale un neurone inibisce gli altri nella sua vicinanza così da creare un contrasto in quella zona, aumentando quindi la percezione sensoriale. Nel contesto delle reti neurali artificiali aiuta a migliorare la capacità di apprendimento e la generalizzazione del modello riducendo l'overfitting, un fenomeno in cui un modello di machine learning si adatta troppo bene ai dati di addestramento, arrivando a catturare rumori o caratteristiche casuali, e di conseguenza, perde la capacità di generalizzare su nuovi dati non visti. In altre parole, il modello ha imparato i dettagli specifici dei dati di addestramento così bene che diventa inefficace quando si applica a nuovi dati. L'obiettivo quindi del LRN è quello di prevenirne il rischio regolando l'output di ciascun neurone rispetto alle risposte dei neuroni vicini nella stessa mappa di attivazione, utile a normalizzare i neuroni del ReLU. La formula originale [7] è quanto segue:

$$b^i_{x,y} = \frac{a^i_{x,y}}{(k + \alpha \sum_{j=\max(0,i-n/2)}^{j=\min(N-1,i+n/2)} a^2_{x,y})^\beta} \tag{6}$$

Dove b_i è l'output normalizzato del neurone i-esimo alla posizione x, y. a_i è l'input del neurone i-esimo alla posizione x, y. N è la dimensione totale della finestra di normalizzazione. n è la dimensione della finestra locale (spesso è un numero dispari). k, α, e β sono iper-parametri che controllano il processo di normalizzazione, nel DeepECG [6] questi hanno i seguenti valori: $\alpha = 0.0002, \beta = 0.75, k = 1.0, n = 5$.

Anche il Dropout, una tecnica di regolarizzazione comunemente utilizzata, può essere considerato una forma di inibizione laterale. Durante l'addestramento, casualmente si "disattivano" alcuni neuroni, impedendo che la rete diventi dipendente troppo da neuroni specifici e migliorando la robustezza.

Infine, l'ultimo layer è un Softmax che è utilizzato per ottenere una distribuzione di probabilità tra diverse classi che aiuta ad assegnare un'etichetta di classe ad un input. Prima del layer softmax, l'ultimo strato della CNN produce un insieme di valori denominati "logits". Questi logits sono punteggi associati a ciascuna classe di output e non sono ancora normalizzati in una distribuzione di probabilità. Di conseguenza il layer Softmax converte questi logits in probabilità normalizzate utilizzando la funzione softmax: i logits vengono trasformati in probabilità che sommano a 1. Ciascuna probabilità rappresenta la confidenza della rete neurale che l'input appartiene a una specifica classe.

$$Softmax(y_i) = \frac{exp(y_i)}{\sum_{j=1}^{n} exp(y_i)} \tag{7}$$

Dove y_i è il i-esimo vettore in input che consiste in n elementi per n possibili classi.

A livello codice questo modello è stato costruito usando il modulo `torch.nn` di PyTorch, un componente fondamentale per la costruzione e l'addestramento di reti neurali. Questo modulo contiene `nn.Module`, una classe di base per tutte le reti neurali in PyTorch. Il suo metodo `__init__` viene utilizzato per definire i componenti della rete, mentre il metodo `forward` definisce il flusso di dati attraverso la rete. Fornisce anche strumenti per codificare i blocchi dei layer e delle funzioni di attivazione come nn.Linear, nn.Conv1d, nn.ReLU, ecc.

```
1 model=DeepECG(input_shape, hidden_units, output_shape)
```

Algoritmo 2.4: Istanziazione del modello

2.3 Addestramento della Rete Neurale

Prima del ciclo di addestramento della rete è fondamentale settare i parametri della Loss Function e dell'Optimizer.

La Loss Function misura quanto i risultati predetti della rete si discostano dai risultati desiderati (le label reali) per un determinato set di input. L'obiettivo dell'addestramento è minimizzare questo loss, un valore loss più basso indica che la rete sta facendo previsioni migliori. Il modulo torch.nn fornisce alcune Loss Function:

- torch.nn.L1Loss per che misura l'errore medio assoluto (MAE) tra il valore predetto e il valore reale.
- torch.nn.BCELoss calcola il loss per problemi di classificazione binaria utilizzando la sigmoide e la log-likelihood negativa, È utilizzata per problemi di classificazione binaria.
- torch.nn.KLDivLoss (Kullback-Leibler Divergence Loss) che misura la divergenza tra due distribuzioni di probabilità, spesso utilizzata in problemi di apprendimento non supervisionato o nella parte di "autoencoder" delle reti neurali.
- torch.nn.MarginRankingLoss calcola il criterio per prevedere le distanze relative tra gli input, usanto nei problemi di ranking.
- torch.nn.TripletMarginLoss misura il loss tra una tripletta di valori. Una tripletta è composta da a (anchor), p (esempi positivi) e n (esempi negativi), si usa nella determinazione della somiglianza relativa esistente tra i campioni.

C'è ne sono molte altre, tuttavia noi per il nostro specifico problema (classificazione multiclasse) usiamo `torch.nn.CrossEntropyLoss`. Calcola la differenza tra due distribuzioni di probabilità per un insieme fornito di occorrenze o variabili casuali. Viene usato per calcolare la media della differenza dei valori delle predizioni e quelli veri. Il punteggio di entropia incrociata è compreso tra 0 e 1, e un valore perfetto è 0. Questa funzione penalizza le previsioni altamente errate.

$$l(x, y) = L = \{l_1, \ldots, l_N\}^T, l_n = -w_{y_n} \log \frac{exp(x_{n,y_n})}{\sum_{c=1}^{C} exp(x_{n,c})} \tag{8}$$

Dove x è l'input, y è l'obiettivo, w è il peso, C è il numero di classi e N la dimensione del mini-batch.

Invece, l'Optimizer è l'algoritmo utilizzato per aggiornare i pesi della rete in modo da ridurre il loss durante l'addestramento. Il pacchetto `torch.optim` contiene vari ottimizzatori: Adam (Adaptive Moment Estimation), Adagrad (Adaptive Gradient Algorithm), RMSprop (Root Mean Square Propagation), eccetera. Noi useremo `torch.optim.SGD` (Stochastic Gradient Descent), uno dei più semplici. Aggiorna i pesi in modo proporzionale al gradiente negativo della funzione di perdita rispetto a ciascun peso.

```
loss_fn = nn.CrossEntropyLoss()
optimizer = torch.optim.SGD(params=model.parameters(), lr=0.01)
```

Algoritmo 2.5: Setup della Loss Function e dell'Optimizer

Una volta deciso la Loss Function e l'Optimizer, si procede alla costruzione del ciclo di addestramento. Per ogni epoca, che rappresenta un passaggio completo attraverso l'intero set di addestramento, la rete verrà messo in modalità train con `model.train()` e dovrà compiere una serie di passaggi:

1. Pass Forward: il modello neurale riceverà in input un batch del train dataset, nel nostro caso riceverà in ingresso i segnali ECG. Questi segnali verranno passati al metodo forward(), che farà processare i dati nei blocchi di layer del modello. Pass Forward restituirà in uscita le predizioni del modello.

2. Calcolo del Loss: le predizioni del modello verranno confrontate con gli effettivi ID dei pazienti.

3. Retropropagazione del Gradiente: calcolo dei gradienti rispetto ai pesi del modello attraverso la retropropagazione del Loss.

4. Aggiornamento dei Pesi: utilizzo dell'ottimizzatore per aggiornare i pesi del modello in base ai gradienti calcolati.

```
for epoch in range(epochs):
    for signal, id, class_label in train_loader:
        model.train()
        train_pred = model(signal)
        loss = loss_fn(train_pred, class_label)
        optimizer.zero_grad()
        loss.backward()
```

```
8         optimizer.step()
```

Algoritmo 2.6: Addestramento della Rete

2.4 Esperimenti

Dopo aver addestrato la rete neurale, per investigare sugli obiettivi prefissati in questa tesi calcoleremo l'accuratezza al variare dei seguenti parametri: popolazione del dataset, numero di leads, numero di finestre, numero dei secondi di ciascuna finestra. Per ogni variazione teniamo costante i seguenti parametri: epoche di addestramento = 200, learning rate = 0.01, batch = 16, hidden_units = 32.

L'accuratezza delle previsioni saranno calcolate dopo le epoche di addestramento sul test dataset. Come già citato precedentemente, è importante testare le previsioni su dati che il modello non ha ancora visto durante la fase di addestramento, per questo motivo usiamo un dataset diverso. Per fare le previsioni usiamo la funzione `model.eval()` per settare il modello in fase di valutazione.

Per fare le predizioni usiamo la funzione `torch.inference_mode()`, simile al torch.no_grad(). Come il nome suggerisce, nelle previsioni del modello in fase di testing non andranno calcolati i gradienti poiché in questa fare il modello non dovrà apprendere dalle previsioni fatte, di conseguenza non useremo loss.backward() per la retropropagazione e optimizer.step() per l'ottimizzazione. La differenza tra torch.inference_mode() è che questo è relativamente nuovo e garantisce migliore velocità[4]. Quindi nella fase di valutazione il modello dovrà comunque fare il Pass Forward (come abbiamo fatto nella fase di addestramento), calcolare il Loss per vedere dove ha sbagliato, e inoltre calcoleremo la metrica dell'accuratezza.

```
1 model.eval()
2 with torch.inference_mode():
3     for inputs, id, class_label in test_loader:
4         test_pred_logit = model(inputs) # logit
5         test_pred = torch.softmax(test_pred_logit, dim=1).argmax(
  dim=1)
```

Algoritmo 2.7: Previsioni in fase di test

[4]https://pytorch.org/cppdocs/notes/inference_mode.html
https://twitter.com/PyTorch/status/1437838231505096708

Capitolo 3

Risultati e Discussione

Di seguito, al fine di indagare sugli obiettivi di questa tesi, riporteremo i risultati degli esperimenti sotto forma di grafici. Si discutono poi i risultati ottenuti dagli esperimenti con la rete neurale confrontando con la letteratura. Si propone in seguito sviluppi di applicazione pratica e analisi di sicurezza.

3.1 Risultati degli esperimenti

La Figura 15 fornisce una visualizzazione del valore del Loss durante le epoche di addestramento, utilizzando 500 finestre da 2 secondi e considerando due leads (III + $V3$) contemporaneamente per 70 soggetti. Questo grafico dimostra che dopo 200 epoche, la Rete Neurale raggiunge prestazioni significative. Il Loss rappresenta la discrepanza tra le predizioni della Rete Neurale e i valori reali durante una specifica epoca, quindi l'obiettivo principale è ridurre questo valore il più vicino possibile a zero, indicando una previsione accurata: già a partire dall'epoca 50 il Loss inizia a convergere verso lo zero, indicando una rapida approssimazione.

A titolo di esempio, la Figura 16 visualizza i segnali ECG che la rete sta imparando. Tale figura rappresenta i primi tre segnali ECG alla prima epoca di addestramento, dunque è importante notare che in questa fase iniziale, l'immagine mostra ID dei soggetti predetti diversi dai loro effettivi ID. Questo fenomeno è normale nelle prime fasi dell'addestramento, poiché il modello sta ancora imparando a estrarne correttamente le caratteristiche distintive dei segnali ECG. Con il

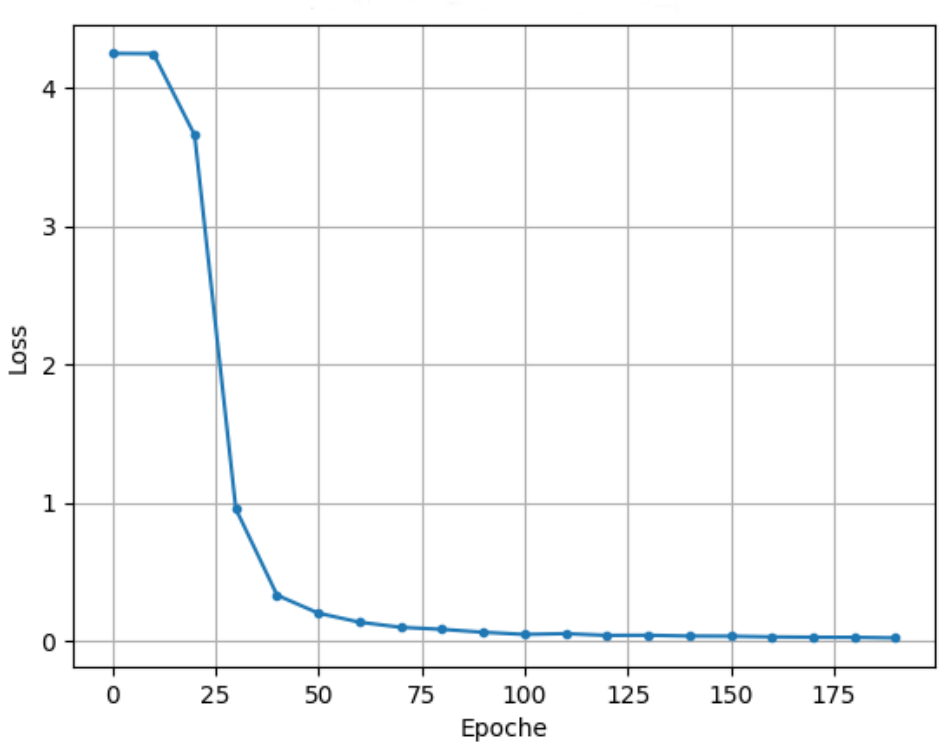


Figura 15: Valori dei Loss nelle epoche di training.

progredire delle epoche ci si aspetta che il modello affini la sua capacità di predire gli ID dei soggetti in modo più accurato.

Tenendo quindi 200 epoche per il training e 500 finestre di ECG per soggetto da 2 secondi, la Figura 17 illustra l'andamento dell'accuratezza delle previsioni sul test_dataset al variare del numero di soggetti coinvolti. È evidente che la curva in verde, rappresentante l'accuratezza delle previsioni utilizzando contemporaneamente due leads (III + V3), registra prestazioni superiori rispetto all'utilizzo dei singoli leads separatamente, ciò è banalmente comprensibile poiché è naturale che se il modello ha più feature da cui estrarre le informazioni garantisce meglio l'apprendimento. Si nota inoltre che all'aumentare dei soggetti da identificare nel dataset, il modello presenta una leggera diminuzione dell'accuratezza, specialmente quando si considera solo il lead $V3$, il quale per l'intero insieme di 139 soggetti,

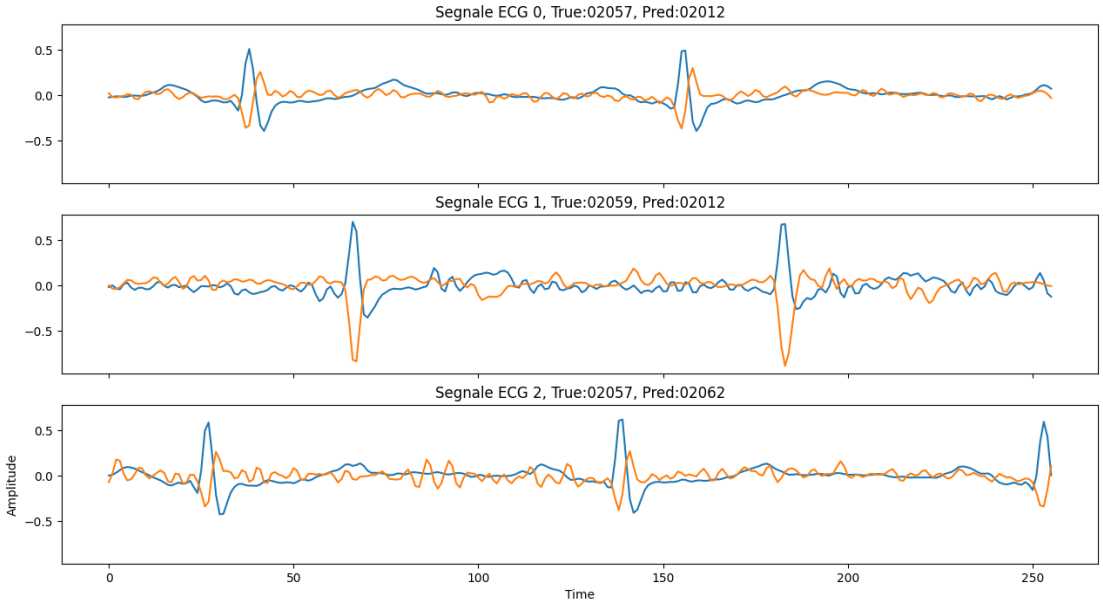


Figura 16: Primi tre segnali del primo batch alla prima epoca di training.

presenta un'accuratezza inferiore al 90%, rispetto al lead III che mostra accuratezza sopra al 92%. Tuttavia, la fusione dei due leads mostra risultati superiori, mantenendo un'accuratezza stabile oltre il 97%.

La Figura 18 analizza le prestazioni di accuratezza relative a 70 soggetti con lead $III + V3$ variando il numero di finestre e mantenendo una durata di 2 secondi ciascuna. Si evince chiaramente che aumentando le finestre di ECG per ogni soggetto corrisponde a un miglioramento delle prestazioni in termini di accuratezza. Con soli 50 finestre l'accuratezza è ancora insufficiente per superare il 5%, ma già con 100 finestre si registra un significativo incremento, e tale tendenza continua a migliorare avvicinandosi al 98-99% con 500 finestre.

Infine, il grafico in Figura 19 mostra il variare dell'accuratezza al variare dei secondi per finestra per 70 soggetti con $III + V3$. Si dimostra che a 50 finestre per soggetto a 1 secondo di tracciato si registra performance al 3.28%, neanche a 100 finestre a 1 secondo sono sufficienti per raggiungere superiori al 9.92%, ma già a 2 secondi comincia ad aumentare al 76.90%. Le prestazioni eccellenti si ottengono con 500 finestre già da 2 secondi con 97.32% fino a 7 secondi con 98.32%.

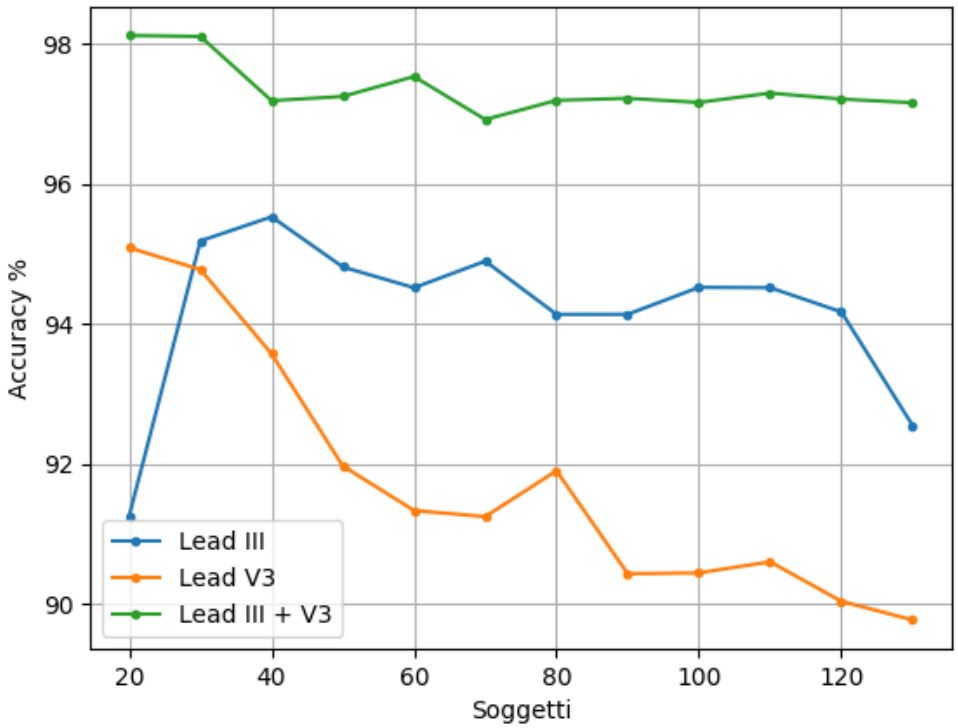


Figura 17: Accuratezza all'aumentare dei soggetti.

3.2 Discussione dei risultati

I risultati ottenuti confermano la fattibilità dell'utilizzo degli ECG come metodo di riconoscimento biometrico.

Abbiamo appurato che l'addestramento della rete neurale concluso dopo 200 epoche, dimostra che l'utilizzo di 500 finestre di ECG per ciascun paziente e con una durata di almeno 2 secondi, permette di raggiungere prestazioni elevate nella fase di identificazione.

Inoltre, un elemento rilevante emerso dall'analisi è che la combinazione delle informazioni provenienti dai leads III e $V3$ contribuisce in modo significativo a stabilizzare e migliorare le prestazioni complessive del modello nell'identificazione, rispetto all'uso di lead separatamente.

Inoltre abbiamo sottolineato come la quantità di finestre temporali gioca un

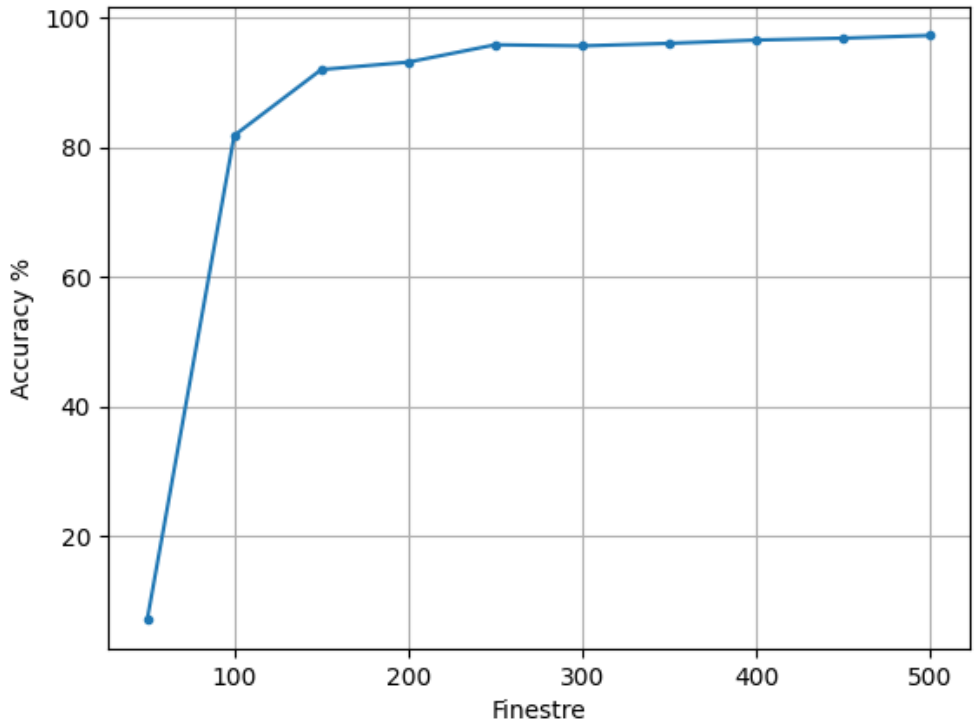


Figura 18: Accuratezza all'aumentare delle finestre per soggetto.

ruolo critico nel processo di apprendimento della rete neurale. I risultati evidenziano che un numero maggiore di finestre temporali è cruciale per ottenere accuratezze considerevolmente più elevate, e questo enfatizza l'importanza di considerare attentamente la durata e il numero di finestre temporali nell'elaborazione del segnale ECG per garantire una migliore precisione delle previsioni.

Gli andamenti dell'accuratezza in relazione al numero di soggetti, come evidenziati nei risultati, sono coerenti con quanto riportato in letteratura [9]. La leggera diminuzione delle performance all'aumentare del numero di soggetti da identificare è un fenomeno già osservato e studiato in contesti simili. Tale tendenza può essere attribuita alla complessità crescente del compito di identificazione quando coinvolge un numero maggiore di soggetti nel dataset. Qui si tratta di variabilità intraclasse e interclasse (come spiegato nel capitolo 1).

Si potrebbe aggirare questa problematica con contesti di autenticazione: se si

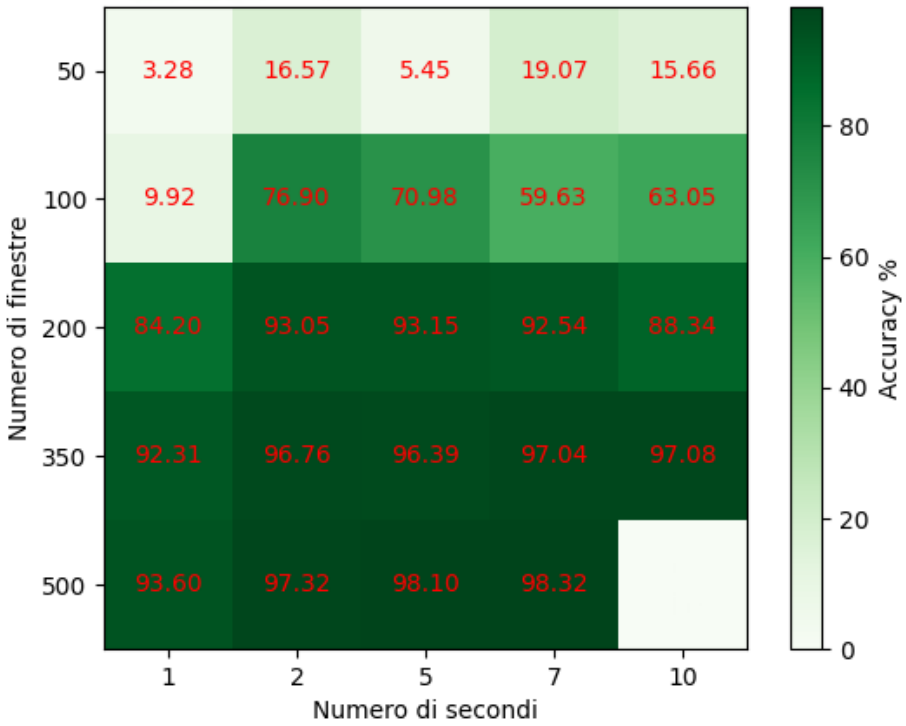


Figura 19: Accuratezza all'aumentare dei secondi delle finestre.

suddividesse il dataset in più dataset più piccoli, al soggetto sarà dunque chiesto di dichiarare la sua identità, sarà poi al sistema la decisione a quale dataset fare riferimento per poi calcolare con il modello il match delle distanze delle feature. Ogni sotto-dataset potrebbe rappresentare un contesto più ristretto, in cui le caratteristiche comuni tra i soggetti sono più evidenti, facilitando così il processo di riconoscimento.

Bisogna anche tenere conto che il dataset utilizzato in questa tesi non provengono da soggetti giovani e sani, ma sono anziani e affetti da ipertensione arteriosa [8]. Le performance nella letteratura dipendono anche da quanto è sano il cuore [9], ad esempio negli esperimenti di Chen et al. i soggetti sani registrano performance del 98.14% rispetto a soggetti anziani con condizioni cardiache con 95.62%. Gli esperimenti di Ghazarian et al. [9] dimostrano una contro tendenza, raggiungendo accuratezza migliori per soggetti con tachicardia sinusale o pazienti diagnosticati

con cambiamenti ST e tachicardia sopraventricolare.

Nella letteratura l'acquisizione ha un ruolo cruciale, Ramos et al. [9] dimostrano che solo muovendo i polsi può causare errori nel riconoscimento. Invece Nobunaga et al. [9] scoprono accuratezza del 99.8% in soggetti mentre fanno attività fisica, contro il 100% in soggetti a riposo, indicando che la loro ricerca è adatto a identificare soggetti in movimento.

Tutte queste caratteristiche, insieme a emozioni che sono sempre in mutamento nell'essere umano, e la postura di acquisizione contribuiscono in modo significativo alle performance [9]. Nella nostra ricerca, l'uso di sistemi Holter ha permesso al modello d'imparare feature da ECG in diversi contesti in cui erano i soggetti nel corso di una loro giornata quotidiana, visto che abbiamo tagliato ogni ECG in piccole finestre a distanza casuale tra loro.

Da menzionare anche la problematica del dataset usato in questa ricerca, secondo la letteratura anche la frequenza di sampling gioca un ruolo nel contribuire nell'accuratezza, in particolare viene usato comunemente un sampling di 500 Hz, siccome cattura più cambiamenti dell'attività cardiaca. In sistemi commerciali datati (come nel nostro caso con 128 Hz) è spesso usare la tecnica dell'interpolazione sui dati [9].

Nel lavoro di Labati et al. [6], prima di processare i tracciati nella rete DeepECG hanno fatto un lavoro di preprocessing diverso dal nostro: loro hanno estratto i complessi QRS più discriminative e i picchi R, cioè hanno considerato i fiducial point del ECG e li hanno concatenati. Noi invece abbiamo considerato tutto il tracciato, ciò ha fatto sì che la rete neurale imparasse a distinguere le feature a prescindere dalla posizione delle onde, favorendo così di apprendere le feature anche con onde shiftate.

3.3 Analisi di utilizzo pratico

Confrontando con le 7 proprietà che caratterizzano un tratto biometrico (esposto nel capitolo 1), abbiamo potuto constatare che l'ECG è Misurabile, raggiungendo ottime Performance nell'accuratezza nel riconoscere gli individui, quindi si ritiene che l'ECG abbia anche la caratteristica dell'Unicità tra gli individui. Inoltre l'Universalità è data dal fatto che tutti gli esseri viventi presentano la capacità di un

cuore che batte, e a oggi non ci sono tecnologie in grado di falsificare un battito artificialmente [6], garantendo così la caratteristica della Circonvenzione.

Investigando sulla caratteristica dell'Accettabilità, gli utenti preferiscono procedure meno invasive possibili [9]. Quindi le procedure On-the-Person, che prevedono elettrodi applicati sulla pelle mediante gel, sono meno favorite rispetto alle procedure Off-the-Person che prevedono uso di elettrodi metallici e senza applicazioni bagnate, inoltre questi elettrodi sono di numero minore (2-3) applicati su polsi, mani o dita. Addirittura le derivazioni provenienti dalle dita hanno prestazioni migliori rispetto a quelle tradizionali [9].

Dai risultati emersi in questa tesi, è fondamentale avere il giusto numero tracciati ECG per raggiungere performance alte, meglio se questi provengono da registrazioni in più scenari in cui gli individui sono soggetti, come nel nostro caso. I dispositivi Holter sono ancora considerati semi invasivi poiché richiedono l'applicazione di più elettrodi da portare addosso per almeno 24 ore. Tuttavia in commercio esistono vari device molti dei quali sono indossabili [9]. Facendo alcuni esempi, esiste il "Shimmer ECG sensor" con elettrodi applicati solo sulla gamba, "Nymi Band" è un bracciale da indossare sul polso, "Kardia by Alicor" sono sensori portatili (praticamente tascabili) e rileva il battito dalle dita. Gli smartwatch sono sicuramente i dispositivi più usati rispetto a quelli elencati precedentemente, molti dei quali hanno anche la funzione di rilevare ECG.

Nella progettazione di un sistema biometrico si deve pensare anche all'operatività in cui si andrà ad applicare. La biometria da ECG è ben diversa dai metodi come riconoscimento facciale o impronte, i contesti ideali sarebbero contesti di continuo autenticazione. Ciò potrebbe risolvere la problematica già evidenziato dalla letteratura [9], quello della stabilità temporale tra il template presente nel DB durante la fase di enrollment e il template nella fase di riconoscimento. I tracciati ECG di queste due sessioni potrebbero differire per molte cause, ad esempio solo già la postura o il livello di idratazione del soggetto [9]. Chee et al. hanno notato che tra enrollment e la fase di riconoscimento con 83.9 giorni e 5.5 giorni di distanza tra loro, si ha un accuratezza rispettivamente del 64.16% e del 92.70%, ciò mostra che più il tempo aumenta tra le due fasi, maggiore è il peggioramento delle performance. Tuttavia dipende anche dalla tipologia di acquisizione, Ramos et al. dimostrano che l'ECG acquisite dalle dita presentano maggiore stabilità nel

tempo [9].

In un contesto di riconoscimento continuo, la rete neurale dovrebbe imparare l'ECG di un soggetto in diverse condizioni in cui si trova durante una routine giornaliera, come un sistema Holter usato in questa ricerca oppure tramite i numerosi tipi di smartwatch, facendo così la rete impara anche le diverse alterazioni dell'ECG in base a molti contesti. Così dopo un numero di tempo ragionevole senza autenticazione, la rete dovrebbe comunque essere in grado a riconoscere l'ECG. Vedendola in un'altra analogia, se si lavora con un collega in modo costante, la nostra rete neurale naturale apprenderebbe il volto del collega così anche se non lo dovessimo rivedere per un paio di mesi, saremo comunque in grado di identificarlo anche in condizioni in cui la faccia non è quella che siamo stati abituati. Naturalmente se a distanza di anni non rivediamo il collega, e il suo volto subisce notevoli modifiche da come lo abbiamo conosciuto, faremo fatica a identificarlo.

L'altro uso pratico di questi dispositivi è il Telehealth, che mira a espandere geograficamente i servizi sanitari [2]. I wearable prima citati possono offrire molti servizi di monitoraggio da remoto sul paziente, come il controllo della temperatura e altri segni vitali. Oltre ai dispositivi indossabili, in anni recenti sui vari play store dei dispositivi vi sono presenti numerose applicazioni riguardante la salute, da qui l'architettura generale prevede l'utilizzo di una interfaccia (spesso applicazione su smartphone) che interagisca in modo wireless sul sensore a contatto sul corpo [2].

3.3.1 Biometria via smartphone e aspetti di sicurezza

L'NFC (Near Field Communication) è un protocollo di comunicazione wireless a corto raggio, quasi tutti i dispositivi mobili hanno questa funzione integrata, anche già nella fascia medio-bassa di smartphone in commercio. Tale protocollo è lo stesso utilizzato nei pagamenti elettronici tramite smartphone, con l'ausilio di applicazioni come Apple Pay o Google Pay. La procedura prevede che il dispositivo emetta il segnale di pagamento mediante NFC, inviandolo al terminale di pagamento POS (Point Of Sale).

Ci si chiede ora "perché non usarlo nella biometria?". In particolare, invece d'inviare il segnale che autorizzi al pagamento bancario, si utilizzi NFC per inviare il segnale biometrico per compiere azioni che richiedono il riconoscimento. L'utente

quindi si autentica tramite i sensori biometrici del proprio dispositivo, e con esito positivo il segnale invierà il segnale al terminale in questione. L'uso potrebbe essere sbloccare serrature o porte, oppure potrebbe addirittura essere l'evoluzione di un nuovo sistema di documento riconoscitivo: l'ufficiale che chiede di dichiarare le nostre generalità potrebbe ottenerli come un esercente riceve un pagamento con il POS, nel caso di ECG il riconoscimento è fatto da smartwatch.

I vantaggi sono gli stessi dell'uso della biometria come esposto nel capitolo 1, tuttavia alcune perplessità sarebbero legate alle vulnerabilità di NFC. Essendo che NFC deriva dalla tecnologia RFID, è quindi soggetta alle stesse minacce [3]:

- Denial of Service. In generale un attacco DoS (Denial of Service) è un tipo di attacco informatico o condizione in cui un sistema diventa inaccessibile o non funziona correttamente a causa di un sovraccarico di traffico intenzionale.

- Interferenze Radio. Una debolezza dei sistemi wireless è la loro sensibilità alle onde radio. Gli attaccanti possono generare interferenze radio che disturbano la comunicazione tra i terminali in questione. Formalmente questo fenomeno è chiamato jamming.

- Attacco man-in-the-middle. Una forma di attacco in cui un aggressore si posiziona tra i terminali al fine d'intercettare e alterare le comunicazioni tra di essi. Questo tipo di attacco è una minaccia alla privacy e alla sicurezza dei dati in quanto l'aggressore può accedere ai dati trasmessi.

- Replay Attack. È un tipo di attacco in cui un aggressore cattura e successivamente ripete una comunicazione legittima al fine di ottenere accesso non autorizzato a risorse protette.

- Malware. Si crede che non ci siano malware in giro, ma secondo i ricercatori della Vrije Universiteit's Computer Systems Group hanno dimostrato che è possibile creare un virus nei tag RFID [10]. Di solito gli attacchi di tipo buffer overflow si verificano come conseguenza dell'uso improprio di linguaggi come C o C++ che non sono memory-safe. Infatti un Buffer Overflow si verifica quando un attaccante mette un input appositamente più lungo del previsto andando a scrivere oltre la porzione di memoria desiderata, lasciando un

codice arbitrario malevole dopo che la funzione ritorna. Anche gli attacchi di tipo Injection sono fattibili: nel caso del RFID non ci saranno query articolate a causa del numero basso di dati trasmettibili, ma sono comunque sufficienti un comando del tipo `;shutdown--`.

Già ricercatori come Derawi et al. [5] hanno già studiato come usare il protocollo NFC nell'ambito biometrico, loro in particolare lo hanno usato per sbloccare una porta. Gli stessi sottolineano l'importanza che il dispositivo non debba essere già infetto da malware, sia lato software che hardware, il che è difficile assicurarlo in dispositivi commerciali a basso costo.

La questione della privacy è particolarmente importante nella biometria: se un tratto biometrico viene rubato non è possibile crearne uno nuovo, i rischi quindi sono molteplici come casi d'impersonificazione, accesso a informazioni personali eccetera... È cruciale quindi proteggere questi dati nel database.

Gli approcci tradizionali usati nella protezione delle password usando le hash non sono adatti poiché il dato biometrico è sempre diverso. La biometria "cancellabile" è un approccio alla sicurezza biometrica che mira a fornire un certo grado di privacy e sicurezza ai dati biometrici degli utenti. L'idea principale è quella di garantire che, in caso di compromissione o accesso non autorizzato, le informazioni biometriche dell'utente possano essere revocate, cancellate o sostituite con nuovi dati. Ci sono diversi metodi per implementare la biometria cancellabile, e uno degli approcci comuni è l'uso di trasformazioni matematiche o crittografiche per generare una rappresentazione "cancellabile" dei dati biometrici. Questa rappresentazione dovrebbe ancora essere utile per l'autenticazione, ma non dovrebbe consentire la ricostruzione dei dati biometrici originali. In questo modo nel database non sarà conservato il tratto biometrico originale ma una versione trasformata.

La biometria tramite segnali ECG, come già citato, non solo permette di riconoscere gli individui, ma contiene informazioni personali come la condizione della salute e dello stile di vita dei soggetti. Chiaramente in un epoca in cui tali informazioni sono sinonimo di business questo è un fattore di grandissima importanza, non a caso, l'industria della sanità è uno dei settori più soggetti ad attacchi informatici.

In letteratura esistono già molti metodi per la cifratura dei segnali ECG: la

crittografia AES (Advanced Encryption Standard) è tra i più usati nella crittografia a chiave pubblica, ma Hameed et al. [1] lo hanno esteso alla cifratura degli ECG. Tuttavia tale soluzione è accettabile solo in ECG senza rumori, e uno dei problemi riguarda anche la ripetitività del segnale, che potrebbe rendere facile la decrittazione. Mathivanan et al. [1] convertono il segnale in codici binari per poi applicare la cifratura. Tutte queste soluzioni non sono adatti alla biometria per i motivi precedentemente esposti, ma metodi ad hoc sono stati confrontati da Merone et al. per l'uso biometrico [1].

Anche le reti neurali possono contribuire alla protezione della privacy. Le Generative Adversarial Networks (GAN) reti neurali che generano dati sintetici. Le GAN sono composte da due reti neurali principali: Generative Network (Generatore) è responsabile di generare nuovi dati, esso prende spesso in input un rumore casuale e produce dati che dovrebbero essere indistinguibili da quelli reali. Il Discriminative Network (Discriminatore) è incaricata di distinguere tra dati reali e dati generati dal generatore. Thambawita et al. hanno sviluppato questa rete con l'obiettivo di proteggere i segnali ECG reali dei pazienti e la loro privacy generando dei DeepFake [11].

Capitolo 4

Conclusioni

Con il progresso della ricerca, gli studi sul riconoscimento biometrico attraverso segnali elettrocardiografici si stanno sempre più espandendo. In questa tesi abbiamo confermato la fattibilità di tale sistema di riconoscimento e raggiunto tutti i risultati prefissati, i quali sono anche in linea con quanto riportato nella letteratura.

Attraverso il popolare framework Pytorch abbiamo sviluppato DeepECG [6] una rete neurale convoluzionale in grado di fare riconoscimento dai segnali elettrocardiografici su SHAREE database [8].

Con questo dataset abbiamo dimostrato che dopo 200 epoche di addestramento della rete neurale sono sufficienti per fare predizioni con accuratezza elevate. Con una popolazione di soggetti numerosa, le performance sono lievemente minori rispetto a una popolazione con pochi individui, la differenza è più evidente se si considerano le derivazioni III e $V3$ separatamente, i quali hanno prestazioni decisamente più scarse rispetto all'utilizzo contemporaneo delle due $III + V3$.

Abbiamo dimostrato che il numero di finestre di ECG per soggetto è un fattore importante, poiché con soli 50 tracciati per soggetto la rete neurale non riesce a fare predizioni accurate. Il numero corretto sarebbe 500 finestre da almeno 2 secondi oppure 350 finestre ma con durata maggiore, il che denota anche come il fattore della durata dei secondi possa influenzare le prestazioni. Quindi in fase di enrollment dei tracciati è importante tenere conto che servono abbastanza dati di registrazioni.

Un lavoro essenziale è la fase di preprocessing dei dati dove abbiamo assicurato

la qualità dei tracciati applicando filtri e rimuovendo valori NaN, inoltre abbiamo tagliato i segnali in finestre a distanza casuale tra loro, questo garantendo le elevate prestazioni ottenute.

Abbiamo fatto un'analisi sull'utilizzo pratico di tale sistema di riconoscimento in scenari reali, proponendo anche un metodo paragonabili ai pagamenti elettronici. Su questi scenari abbiamo fatto analisi in termini di sicurezza, sottolineando l'importanza della protezione della privacy nell'uso biometrico.

Con l'ECG non solo è possibile ricavare l'identità di un individuo ma anche il suo stato di salute e lo stile di vita; tali informazioni hanno un valore economico nella società di oggi, dunque è fondamentale assicurarne la protezione, sia nel lato giuridico grazie a normative come il GDPR sia nel lato tecnico con lo sviluppo di metodi pratici.

In considerazione di tutte le riflessioni precedenti, emerge la necessità imperativa di sviluppare uno standard di acquisizione dei segnali ECG che sia analogo a quelli utilizzati nelle metodologie di biometria facciale. Attraverso linee guida comuni si garantisce la coerenza nei processi di acquisizione, e tale approccio si propone per assicurare non solo prestazioni elevate, ma anche un livello di sicurezza che sia robusto e resiliente contro possibili attacchi informatici.

I risultati ottenuti riguardano le prestazioni della rete neurale nel riconoscere i segnali elettrocardiografici, pertanto non riguardano le prestazioni come sistema biometrico in sé, poiché richiede uno sviluppo hardware e software a 360 gradi. Per i test di tale casistica servono anche più dati di ECG siccome si deve stimare anche l'accuratezza in presenza di impostori. Per la stessa problematica dei dati, non abbiamo potuto quantificare l'accuratezza dei riconoscimento con distanze temporali dall'enrollment.

Un'altra sfida rilevante che si è presentata durante la conduzione di questa ricerca è rappresentata dalla considerevole mole di dati che la rete neurale deve elaborare. Nel corso di questo studio, l'elaborazione è stata effettuata utilizzando un computer personale con un processore Intel i5 di decima generazione e 8 GB di memoria RAM. Pur avendo la possibilità di sfruttare la scheda GPU NVIDIA GeForce MX230 che Pytorch supporta per accelerare i calcoli, l'ottenimento dei risultati richiedeva comunque un significativo investimento di tempo computazionale. A causa di questa problematica, non siamo riusciti a produrre tutti i test

sull'uso del lead $V5$. Ma già usando due leads $III+V3$ abbiamo raggiunto prestazioni eccellenti, quindi si presume che usando tre leads $III + V3 + V5$ si avrebbe raggiunto solo prestazioni migliori.

Va sottolineato che questa problematica si inserisce in un contesto più ampio, in cui lo sviluppo di architetture neurali a livello industriale spesso si confronta con la necessità di risorse computazionali notevoli, inclusa l'energia. L'elaborazione intensiva richiesta per modelli complessi evidenzia la crescente importanza di esplorare soluzioni energetiche più efficienti per garantire uno sviluppo sostenibile di tali tecnologie.

Si rimanda alla repository GitHub dell'autore per i codici usati in questa ricerca: `https://github.com/Sir-Cyborg`.

Bibliografia

[1] Abeer D Algarni, Naglaa F Soliman, Hanaa A Abdallah, and Fathi E Abd El-Samie. Encryption of ecg signals for telemedicine applications. *Multimedia Tools and Applications*, 80:10679–10703, 2021.

[2] Venkata Anuhya Ardeti, Venkata Ratnam Kolluru, George Tom Varghese, and Rajesh Kumar Patjoshi. An overview on state-of-the-art electrocardiogram signal processing methods: Traditional to ai-based approaches. *Expert Systems with Applications*, page 119561, 2023.

[3] Mike Burmester and Breno De Medeiros. Rfid security: attacks, countermeasures and challenges. In *The 5th RFID academic convocation, the RFID journal conference*, 2007.

[4] Wikipedia contributors. Immagini tratte da wikipedia, licenza creative commons. `https://commons.wikimedia.org/`.

[5] Mohammad Omar Derawi, Simon McCallum, Heiko Witte, and Patrick Bours. Biometric access control using near field communication and smart phones. In *2012 5th IAPR International Conference on Biometrics (ICB)*, pages 490–497. IEEE, 2012.

[6] Ruggero Donida Labati, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. Deep-ecg: Convolutional neural networks for ecg biometric recognition. *Pattern Recognition Letters*, 126:78–85, 2019. Robustness, Security and Regulation Aspects in Current Biometric Systems.

[7] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*, 25, 2012.

[8] Paolo Melillo, Raffaele Izzo, Ada Orrico, Paolo Scala, Marcella Attanasio, Marco Mirra, Nicola De Luca, and Leandro Pecchia. Automatic prediction of cardiovascular and cerebrovascular events using heart rate variability analysis. *PLOS ONE*, 10(3):1–14, 03 2015.

[9] Teresa M. C. Pereira, Raquel C. Conceição, Vitor Sencadas, and Raquel Sebastião. Biometric recognition: A systematic review on electrocardiogram data acquisition methods. *Sensors*, 23(3), 2023.

[10] M.R. Rieback, B. Crispo, and A.S. Tanenbaum. Is your cat infected with a computer virus? In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*, pages 10 pp.–179, 2006.

[11] Vajira Thambawita, Jonas L Isaksen, Steven A Hicks, Jonas Ghouse, Gustav Ahlberg, Allan Linneberg, Niels Grarup, Christina Ellervik, Morten Salling Olesen, Torben Hansen, et al. Deepfake electrocardiograms using generative adversarial networks are the beginning of the end for privacy issues in medicine. *Scientific reports*, 11(1):21896, 2021.

[12] Wikipedia. Elettrocardiogramma — wikipedia, l'enciclopedia libera, 2023.

[13] Wei Zong, G.B. Moody, and D. Jiang. A robust open-source algorithm to detect onset and duration of qrs complexes. *Computers in Cardiology*, 30:737 – 740, 10 2003.

Progetto sviluppato presso il Biomedical image and Signal Processing Laboratory

`https://www.bisp.di.unimi.it`