Tesi Matteo Sorighe 60/61 - 49007

EEG – ECG per riconoscimento biometrico.

Introduzione.

Capitolo 1.

* Cos’è la biometria.

http://www.treccani.it/enciclopedia/biometria/

<https://it.wikipedia.org/wiki/Biometria>

<https://it.wikipedia.org/wiki/Sistema_di_riconoscimento_biometrico>

Importante: 7 (o 4?) parametri della biometria (ci sono su wiki)

<https://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/>

Biometria mono modale vs multimodale.

Come viene quantificata l’efficacia dei test biometrici.

<https://tecnologia.libero.it/che-cose-la-biometria-e-come-migliora-la-sicurezza-informatica-14748>

* Differenze tra biometrie comportamentali e fisiche (esempi su quali sono una e l’altra).
* EEG ed ECG: mezzi per la biometria sia fisici che comportamentali.

L’utilizzo di ECG ed EEG è solo recente.

Capitolo 2.

* Evoluzione biometria dal 2000 a oggi (articoli su movimento/riconoscimento mani e/o iride)
* Fusione tra biometrie.

<https://link.springer.com/article/10.1007%2Fs10044-016-0568-5>

Capitolo 3.

* Fusione tra ECG ed EEG con analisi dei lavori.

In particolare:

* + Come sono stati acquisiti i segnali (simultaneamente o meno?)
  + Come sono stati estratti i segnali
  + Come sono state fuse le biometrie

Capitolo 4/Conclusioni.

* Il futuro dei sistemi di riconoscimento (dove porterà l’utilizzo e l’evoluzione delle tecniche biometriche)
* Eventualmente cita i lavori che ti hanno colpito di più

Indice.

Introduzione;

Capitolo 1.

1.1 Cos’è la biometria.

1.2 Differenze tra biometrie comportamentali e fisiche.

1.3 EEG ed ECG.

Capitolo 2.

2.1 Evoluzione della biometria: gli anni 2000.

2.2 Fusione tra biometrie.

Capitolo 3.

3.1 Fusione tra ECG ed EEG.

3.2 Analisi dei lavori presentati negli articoli.

Conclusioni.

Considerazioni personali/citazioni articoli particolarmente interessanti.

Futuro dei sistemi di riconoscimento (???)

**Introduzione**.

Nella tesi proposta viene brevemente introdotta la biometria, per poi passare ad un’analisi più in particolare dell’utilizzo di ECG (elettrocardiogramma) ed EEG (elettroencefalogramma) in tale disciplina.

Una volta conclusosi l’excursus iniziale, verranno esaminati e presentati alcuni studi svolti da ricercatori che si occupano di riconoscimento biometrico, secondo il seguente ordine:

* Come sono stati acquisiti i segnali;
* Come sono stati estratti i segnali;
* Come sono state eventualmente fuse le biometrie.

Infine, nelle conclusioni, verranno confrontati i risultati dei lavori presentati e inserite considerazioni personali riguardanti la ricerca svolta e il futuro della biometria.

**Capitolo 1.**

Che cos’è la biometria.

La Treccani definisce la biometria (dal greco *bìos* = “vita” e *métron* = “misura”) come la “disciplina che studia le grandezze biofisiche allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici”.

Storicamente parlando, i primi utilizzi di grandezze fisiche a scopo identificativo sono piuttosto antichi. Sono state ritrovate, per esempio, tavolette d’argilla risalenti all’epoca babilonese con sopra incise (RIVEDERE VERBO) impronte digitali che venivano utilizzate a scopo commerciale (<http://onin.com/fp/fphistory.html>) e documenti della dinastia Qin (Cina, 221-206 a.C.) che includono dettagli sull’utilizzo delle impronte delle mani come prove in caso di furto.

Intesa come scienza però, la biometria, si sviluppa intorno alla seconda metà del XIX secolo in ambito forense. Lo studio delle dimensioni del cranio e delle proporzioni scheletriche ne sono un esempio, così come l’utilizzo delle impronte digitali, che cominciano ad essere raccolte e registrate da parte dei dipartimenti di sicurezza nel tentativo di combattere il crimine.

Ad oggi la biometria vanta varie applicazioni, soprattutto nel campo biologico (studio di caratteristiche tipiche di popolazioni di esseri viventi e di associazioni genetiche tra specie) e medico (epidemiologia, diagnosi medica e farmacologia) e, in tempi più recenti, anche nel campo della sicurezza informatica (sistemi di riconoscimento biometrico).

Ai fini dell’identificazione biometrica possono essere utilizzati diversi parametri fisici, chimici o comportamentali, anche contemporaneamente, purché si rispettino sette determinate specifiche che permettono di valutarne l’idoneità ([Schuckers, 2001] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001):

* Universalità, ogni individuo deve possedere quel tratto;
* Unicità, il tratto deve essere sufficientemente diverso tra diversi individui in modo da identificarli univocamente;
* Permanenza, legata alla maniera con cui il tratto cambia nel tempo;
* Misurabilità, riferita alla facilità con cui il tratto è collezionabile;
* Performance, in riferimento all’affidabilità, velocità e robustezza della tecnologia usata;
* Accettabilità, riferita a quanto e come gli individui accetteranno la tecnologia utilizzata per raccogliere il o i tratti biometrici;
* Circonvenzione, legata alla facilità di un tratto nel poter essere imitato da uno strumento o sostituito.

Mono modale vs multi modale.

La raccolta dei dati basata sui tratti però può incontrare problemi, specialmente nell’utilizzo di sistemi mono modali, ovvero sistemi che misurano un solo tratto specifico (es. la forma dell’iride o l’impronta digitale, entrambe risentono del logoramento biologico). Per superare questo ostacolo si utilizzano sistemi di raccolta multimodali che, come si può intuire dal nome, registrano e incrociano diversi aspetti del singolo individuo sotto esame (L. Hong, A. K. Jain, S. Pankanti, Can multibiometrics improve performance?, in: Proceedings AutoID’99, Summit(NJ), USA, 1999, pp. 59–64). Essi fondamentalmente uniscono più sistemi mono modali in quattro modi: raccogliendo dati sequenzialmente, simultaneamente, una combinazione di questi o in serie, in modo da riferirsi rispettivamente a una modalità di accesso sequenziale oppure parallela, o gerarchica o di integrazione seriale.

//DESCRIVERE UN SOSTEMA BIOMETRICO STANDARD, CAPITOLO 2 DI QUESTO:

<https://pdfs.semanticscholar.org/1c1c/4182c94e307d603443d6b5f966e266403672.pdf>

//

//SI RIPARLA DI MULTIMODALE QUANDO INTRODUCO LA FUSIONE, DECIDERE DOVE METTERE LE COSE//

//COME FUNZIONA UN SISTEMA BIOMETRICO? AUTENTICAZIONE E IDENTIFICAZIONE BIOMETRICA (https://www.gemalto.com/govt/inspired/biometrics)

Performance.

Per quantificare la performance dei sistemi biometrici sono utilizzati i seguenti fattori ([https://web.archive.org/web/20081017165633/http://www.ccert.edu.cn/education/cissp/hism/039-041.html](https://web.archive.org/web/20081017165633/http:/www.ccert.edu.cn/education/cissp/hism/039-041.html)):

- False match rate (FMR, la percentuale di falsi positivi): misura la percentuale di input invalidi che vengono erroneamente accettati;

- False non-match rate (FNMR, percentuale dei falsi negativi): misura la percentuale di input validi che vengono erroneamente rifiutati;

- Receiver operating characteristic (ROC, caratteristica operativa del ricevitore): le curve del ROC descrivono la differenza tra FMR e la FNMR. L’algoritmo di comparazione che viene utilizzato nel sistema decide quando un input può essere considerato accettabile in base a una determinata soglia. Al diminuire della soglia si hanno meno FNMR ma più falsi positivi, viceversa quando la soglia aumenta //Una comune variazione è il “Detection error trade-off” (DET), il quale è ottenuto usando una normale variazione della scala su entrambi gli assi. Questo grafico più lineare enfatizza le differenze per performance maggiori (rari errori). SI PUO’ AGGIUNGERE//;

- Equal error rate (): detto anche crossover error rate, è il punto, generalmente fissato come percentuale, nel quale l’accettazione e il rifiuto di un valore sono uguali. In generale, minore è l’EER di un dispositivo, più preciso egli risulta;

- Failure to enroll rate (): indica quanti tentativi devono essere fatti dal dispositivo in fase di registrazione per accettare un nuovo modello all’interno del database. Spesso e volentieri dovuto alla qualità dei valori in input;

- Failure to capture rate (): indica la probabilità che il sistema fallisca nel riconoscere i dati biometrici correttamente passati ad esso;

- Template capacity (): quantità di dati che il sistema in uso è in grado di memorizzare;

/\*\*tanto che ad oggi esistono sistemi di riconoscimento in grado di distinguere impronte digitali, occhi, forma di orecchie e persino di intere facce. Un comune esempio ne è lo sblocco di uno smartphone, per il quale basta solamente appoggiare un dito nell’apposita area riservata al riconoscimento d’impronta oppure l’inquadratura da parte della fotocamera del volto del proprietario.\*\*/

Biometrie fisiche e comportamentali.

Le caratteristiche biometriche che possono essere raccolte si dividono in due categorie principali: fisiche e comportamentali.

https://www.justaskgemalto.com/en/what-are-physiological-biometrics/

I dati appartenenti alla prima categoria comprendono gli aspetti innati di un soggetto, che nel caso di un essere umano possono essere le impronte digitali, la forma dell’iride, delle orecchie, ecc. Esse non cambiano in un lasso di tempo ragionevolmente breve.

<https://www.ibia.org/>

https://www.justaskgemalto.com/en/what-are-behavioral-biometrics/

Quando si parla invece di biometrie comportamentali si fa riferimento a valori o pattern basati sull’unicità del comportamento di un individuo nei confronti dell’ambiente. Anche quando non sembra, ogni persona si differenzia dagli altri nella maniera in cui esegue un’azione, che sia essa parlare, prendere un oggetto, camminare o scrivere. Riconoscere queste differenze comportamentali tramite una macchina risulta relativamente facile, così come risulta facile ricreare un unico profilo che si differenzia dagli altri grazie a una combinazione di esse.

EEG ed ECG.

\*\*EEG ed ECG sono biometrie sia fisiche che comportamentali, come sono utilizzati per il riconoscimento biometrico?\*\*

Elettroencefalogramma.

<https://it.wikipedia.org/wiki/Elettroencefalografia>

<http://www.bri.ucla.edu/nha/ishn/ab24-2002.htm>

L’EEG è la trasposizione grafica dell’elettroencefalografia di un individuo, che a sua volta è la registrazione dell’attività elettrica dell’encefalo. La tecnica è stata inventata nel 1929 dal medico tedesco Hans Berger.

L’EEG può essere registrato su carta termica o millimetrata, trasmessa a video tramite un monitor o salvata su un’unità di memoria per poter poi essere visionata nuovamente.

Nella pratica, si effettua utilizzando un numero di elettrodi che varia dai 12 ai 20, posti in varie regioni del cranio del soggetto in esame (che può essere anche un animale //link a eeg su animale//) secondo il “sistema internazionale 10-20” (//<https://www.clinph-journal.com/article/S1388-2457(00)00527-7/fulltext>//).

Gli utilizzi principali sono a scopo medico, tramite elettroencefalografia infatti è possibile diagnosticare facilmente svariati problemi quali epilessia, disturbi del sonno, encefalopatie e morte cerebrale. Per quanto riguarda la ricerca, i campi in cui trova applicazione questa tecnica sono principalmente neuro-psicologici, con una particolare attenzione agli ERP (event-related potential <https://it.wikipedia.org/wiki/Potenziale_evento-correlato>) a loro collegati.

Gli EEG (e come vedremo in seguito, anche gli ECG) sono da considerarsi una biometria sia fisica che comportamentale (<https://ieeexplore.ieee.org/abstract/document/6228581/?part=1> DA SCARICARE). L’attività delle onde cerebrali prodotte da un encefalo infatti può essere influenzata da un particolare stimolo esterno.

Elettrocardiogramma.

<https://it.wikipedia.org/wiki/Elettrocardiogramma>

Un elettrocardiogramma è la trasposizione grafica di un’elettrocardiografia. Essa è lo studio dell’attività elettrica del cuore di un individuo. Ogni corpo umano e animale emana piccole correnti elettriche che vengono registrate tramite uno strumento detto elettrocardiografo.

I primi studi relativi all’elettrofisiologia risalgono alla prima metà del XIX secolo: il fisico Carlo Matteucci iniziò a lavorarci all’università di Pisa nel 1836. Più tardi, nel 1842, pubblicò i risultati dei celebri esperimenti a “pila muscolare” della rana. È già nel 1872 che si ha la prima registrazione di un battito cardiaco, registrato però dal polso di un paziente. Il primo approccio al cuore di un paziente si ha invece nel 1887, a Londra, dove il fisiologo August Desiré Wallace utilizza un elettrometro e degli elettrodi posti sul torace e sul dorso del soggetto.

Da allora si è ampiamente affermato come metodo diagnostico data la sua semplicità, affidabilità e sicurezza, diventando la tecnologia più utilizzata nella cardiologia clinica per monitorare frequenza cardiaca, ritmo cardiaco, effetti di farmaci sul cuore e altre problematiche legate al muscolo cardiaco.

In tempi molto recenti gli ECG hanno iniziato ad essere utilizzati anche per il riconoscimento biometrico(<https://www.physionet.org/pn3/ecgiddb/biometric.shtml>)

**Capitolo 2.**

Biometria in tempi recenti: dagli anni ’90 a oggi.

<https://www.biometricupdate.com/201802/history-of-biometrics-2>

Le ricerche in materia negli ultimi trent’anni si sono rivolte in buona parte alla scansione dell’iride, con gli USA in prima linea, anche grazie al possesso di un brevetto da parte dei ricercatori Leonard Flom e Aran Safir, che nel 1987 crearono appunto un sistema di riconoscimento dell’iride. Dagli anni duemila in poi la sfida è il riconoscimento facciale, e anche qui gli Stati Uniti la fanno da pionieri, lanciando nel 1993 il programma FERET (face recognition technology). Sponsorizzato dalla DARPA (Defense Advanced Research Products Agency), il programma nasce con l’intento di incoraggiare lo sviluppo di tecnologie e algoritmi per l’identificazione dei volti. Nel 2000 si tiene il primo FRVT (face recognition vendor test), che segna la diffusione su larga scala dei sistemi di riconoscimento di questo tipo.

Nel 2002 l’ISO istituisce il sottocomitato JTC1/SC37 per supportare la standardizzazione delle tecnologie biometriche generiche. Da lì nascono gli standard per promuovere l’interoperabilità e lo scambio di dati tra applicazioni e sistemi.

Nel 2003 nasce, col supporto della Commissione Europea, l’organizzazione indipendente European Biometrics Forum, con lo scopo di coordinare e promuovere la ricerca e lo sviluppo delle tecnologie biometriche in Europa.

Nel 2004 inizia la FRGC (face recognition grand challange), una sfida lanciata dal governo statunitense con l’obiettivo di migliorare gli algoritmi di riconoscimento facciale.

Nel 2008, sempre negli Stati Uniti, il dipartimento di difesa inizia a lavorare su nuovi database che includono, oltre a impronte digitali, anche scansioni dell’iride, del volto e del palmo delle mani.

Infine, nel 2013, la Apple include uno scanner per impronte digitali nell’iPhone 5S, nel 6, nel 6 Plus, nell’iPad Air 2 e nell’iPad Mini 3, specificando che i dati vengono salvati solo nella memoria locale del dispositivo. Questa mossa spiana la strada alla diffusione dei sistemi di riconoscimento biometrici nel mercato della telefonia.

Fusione tra biometrie.

<https://pdfs.semanticscholar.org/1c1c/4182c94e307d603443d6b5f966e266403672.pdf> preso dall’abstract di questo

<https://pdfs.semanticscholar.org/5c50/c7029e041e7e328263c5b7def2e6b69bc994.pdf> usato per la fusione a livello di sensore

<https://link.springer.com/article/10.1007%2Fs10044-016-0568-5>

<https://pdfs.semanticscholar.org/51bc/a6666108992322e3451c1a712b7413227046.pdf>

<https://www.cse.msu.edu/~rossarun/pubs/RossFusion_AVBPA01.pdf>

Sperimentalmente, nell’utilizzare sistemi di riconoscimento unimodali, si possono incontrare diverse difficoltà, siano esse dovute a dati del sensore rumorosi, ai pochi gradi di libertà, alla non universalità del tratto biometrico considerato o a tassi d’errore non accettabili. Tentare di migliorare le prestazioni di sistemi mono modali risulta controproducente in questi casi proprio a causa dell’ereditarietà di questi problemi. I sistemi multimodali riescono a limitare la pesantezza di questi errori permettendo la raccolta di diversi campioni biometrici dello stesso soggetto. Vien da sé che i sistemi multimodali sono un passo avanti nell’affidabilità dei sistemi di riconoscimento biometrico, permettendo un raggiungimento di performance non arrivabili altrimenti. L’affidabilità di tali sistemi comunque non sta solo nella capacità di raccolta dati, anche la sicurezza ne trae vantaggio, poiché obbligherebbe un eventuale malintenzionato ad effettuare lo spoof di più tratti biometrici simultaneamente. Il principale contro di questi sistemi è l’adeguatezza dello schema di fusione da utilizzare per unire i diversi dati raccolti. //A titolo d’esempio, vedremo un articolo in cui il sistema biometrico registra impronte digitali, volti e forme delle mani dei soggetti, fondendoli e confrontando i diversi processi di fusione in modo da capire quale sia il più adatto alla situazione (DA RILEGGERE). //

Per poter parlare di fusione tra biometrie è necessario chiarire che un sistema biometrico è composto principalmente da quattro componenti:

* Modulo contenente il sensore, che fisicamente acquisisce il dato esaminato, ad esempio un lettore di impronta digitale;
* Modulo di estrazione delle caratteristiche, nel quale si estraggono i valori che caratterizzano la biometria considerata. Ad esempio, nella lettura delle impronte digitali, la posizione e l’orientamento dei punti minutiae sarebbero le caratteristiche da prendere in considerazione;
* Modulo di confronto, nel quale i valori delle caratteristiche raccolti vengono confrontati con quelli registrati nel database, generando un punteggio corrispondente. Per esempio, il numero di punti minutiae coincidenti tra il valore registrato e il database in questo modulo viene computato e trattato come una scala di coincidenza;
* Modulo decisionale, dove viene stabilita l’identità del soggetto esaminato o una presunta identità viene accertata o meno, sulla base della scala di coincidenza generata nel modulo di confronto.

La fusione può quindi essere eseguita su ognuno dei livelli:

* Fusione al livello di sensore: la si effettua integrando dati provenienti da diversi sensori prima che si esegua l’estrazione delle caratteristiche. Per esempio possono essere combinate le informazioni provenienti da una videocamera e un sensore 3D;
* Fusione al livello di estrazione delle caratteristiche: i dati ottenuti da ogni sensore vengono utilizzati per calcolare un “FEATURE VECTOR” (viene tradotto come caratteristica vettoriale, andrebbe bene vettore di caratteristiche o caratteristico? Chiedere al prof). Essendo i caratteri estratti da ogni sensore indipendenti tra loro, è ragionevole concatenare i due vettori in uno di maggiore dimensionalità che restringe il range di coincidenza;
* Fusione al livello di confronto: ogni sistema fornisce una scala di coincidenza nella quale si indica la similarità della caratteristica vettoriale con quella del modello vettoriale. Queste due scale possono essere combinate per stabilire la veracità dell’identità richiesta;
* Fusione al livello decisionale: ogni sensore può registrare più dati biometrici e le risultanti caratteristiche vettoriali, combinate, aumentano la ridondanza di un insieme di classificatori indipendenti;

Le forme di fusione sono fondamentalmente di tre tipi:

1. Rappresentazioni multiple di una singola biometria, dove tipicamente ogni rappresentazione ha il proprio classificatore. La fusione avviene a livello di confronto;
2. Confronti multipli di una singola biometria, nella quale si uniscono più strategie di confronto nel modulo di confronto stesso di un sistema biometrico e si combinano i risultati ottenuti dalle suddette tecniche. Anche questa tipologia di fusione avviene al livello di confronto e nonostante ci siano più comparatori, tutti operano sullo stesso campione biometrico;
3. Fusione biometrica multipla, che indica la fusione di più indicatori biometrici. Questi metodi mirano a migliorare la velocità e l’accuratezza dei sistemi biometrici integrando diversi punteggi di confronto ottenuti da diverse fonti biometriche. È importante, in questa tipologia di fusione, normalizzare i risultati ottenuti dai diversi domini [17]. Essa tipicamente si effettua mappando questi risultati in un dominio comune prima di combinarli.

**Capitolo 3.**

Fusione tra EEG ed ECG. Analisi degli articoli.