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. 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, parallela, gerarchica o di integrazione seriale.

//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.