Biometric System Laboratory
DEIS - Università di Bologna
Corso di Laurea in Scienze e Tecnologie Informatiche (sede di Cesena)
http://biolab.csr.unibo.it

Il termine biometria, che deriva dalle parole greche *bios* (vita) e *metros* (misura), si riferisce allo studio e all'impiego di metodi per rilevare e misurare caratteristiche di organismi viventi e trarne comparativamente classificazioni e leggi. Trova applicazioni in biologia, in medicina, in genetica, nelle scienze agrarie e forestali, nelle scienze ambientali e in altri settori affini. La moderna accezione informatica del termine biometria e, conseguentemente del termine sistema biometrico, fa invece esplicito riferimento all'identificazione automatica o alla verifica dell'identità di una persona sulla base di caratteristiche biologiche. In letteratura spesso si distingue fra:

- sistemi biometrici basati sul riconoscimento d'aspetti statici (o caratteristiche fisiologiche), ovvero che operano una valutazione di caratteristiche fisiche dell'individuo quali: impronta digitale, volto, mano, iride, retina, orecchio, dna,…;
- sistemi biometrici basati sul riconoscimento d'aspetti dinamici, intendendo che operano una valutazione di caratteristiche comportamentali quali: andatura, voce, firma, stile di battitura, …;
- sistemi biometrici basati sul riconoscimento d'aspetti chimico-fisici od organici, intendendo che operano una valutazione di proprietà quali: odore, presenza di virus, d'anticorpi, …

Negli ultimi anni l'interesse per i sistemi biometrici è cresciuto notevolmente sia in ambito accademico che industriale e molti gruppi di ricerca hanno dedicato notevoli risorse allo studio di tecniche efficaci per l'identificazione di persone. Le potenziali applicazioni di questa tecnologia sono, infatti, molteplici e spaziano dal controllo accessi a quello delle presenze, dalla sorveglianza automatica alla protezione di risorse di valore, dalla sicurezza di reti di calcolatori alle transazioni sicure su Internet.

L'uso di caratteristiche biometriche ai fini del riconoscimento presenta numerosi vantaggi rispetto ai tradizionali sistemi d'autenticazione basati sull'utilizzo di PIN e password che possono facilmente essere dimenticati dai legittimi proprietari, ceduti ad altri o rubati da utenti non autorizzati. I sistemi biometrici sono ritenuti oggi molto più affidabili dei sistemi tradizionali, vista la difficoltà di falsificazione delle caratteristiche biometriche.

Questi indiscutibili vantaggi rendono i sistemi biometrici particolarmente indicati in tutte le realtà in cui meccanismi efficaci e affidabili per l'identificazione delle persone sono indispensabili per garantire la sicurezza di tutti. Tuttavia i sistemi biometrici non garantiscono un'accuratezza del 100%, infatti può accadere che per alcuni individui una caratteristica biometrica non possa essere utilizzata per la loro identificazione, le caratteristiche biometriche possono mutare nel tempo, i dispositivi biometrici in alcune circostanze possono risultare non affidabili; a questi problemi la ricerca è chiamata a rispondere con soluzioni efficaci ed efficienti per lo sviluppo del settore.

Il Biometric System Laboratory è stato istituito nel 1994 nella sede universitaria di Cesena, dal Prof. Dario Maio e dal Prof. Davide Maltoni. Attualmente il gruppo è composto da 9 persone che operano stabilmente presso la sede del Corso di Laurea in Scienze e Tecnologie Informatiche di Cesena. Laureandi, studenti di dottorato e

ricercatori stranieri in visita collaborano con il team per la realizzazione di specifici progetti.

Si tratta di uno dei pochissimi centri di ricerca sui sistemi biometrici in Italia ed è indubbiamente uno dei più noti a livello internazionale (ad esempio è il solo centro italiano ad essere segnalato dal Biometric Consortium, l'ente governativo ufficiale degli Stati Uniti per la ricerca sui sistemi biometrici, si veda la pagina web http://www.biometrics.org/research.htm).

Nel corso dei suoi anni di attività il gruppo di ricerca ha maturato notevoli esperienze nello studio, progettazione e test di sistemi biometrici. In particolare, sono state proposte tecniche innovative nell'ambito del riconoscimento di impronte digitali, del volto e della valutazione delle prestazioni di tali sistemi. Importanti collaborazioni sono state avviate con alcuni fra i più prestigiosi centri di ricerca internazionali, fra cui si ricordano: Pattern Recognition and Image Processing Laboratory della Michigan State University, diretto dall'insigne Prof. Anil K. Jain e U.S. National Biometric Test Center - San Jose State University. Tali collaborazioni sono continuamente alimentate mediante visite reciproche, scambi di studenti per periodi di studio all'estero, partecipazione comune a vari progetti e stesura di articoli scientifici e capitoli di libri. Inoltre cooperazioni con aziende operanti nel settore, come ST Microelectronics, Siemens (ora Infineon), Thomson TCS (ora Atmel), e Morpho hanno ulteriormente arricchito l'esperienza del gruppo di ricerca e aumentato la sua visibilità all'estero.

I membri del Biometric System Laboratory hanno partecipato negli anni passati a molteplici progetti nazionali e internazionali, fra cui il progetto europeo BioTest e l'advisory commitee BioWork del progetto europeo BEE. Nell'ultimo decennio, i progetti che vedono la partecipazione del Biometric System Laboratori, sono:

- progetto nazionale MIUR *Per*^{2} ("Sistemi distribuiti di riconoscimento multisensoriale a percezione aumentata per la sicurezza e la personalizzazione d'ambiente") [2003-2004];
- progetto europeo *BioSec* ("Biometric and Security") [2004-2005], finanziato dall'Unione Europea all'interno del Sesto Programma Quadro (IST). BioSec ha coinvolto 23 partner, fra cui prestigiose università di vari stati membri e importanti aziende (Siemens, Atmel, Telefonica, …); al Biometric System Laboratory (unico gruppo di ricerca italiano coinvolto nel progetto) è stato affidato il coordinamento di uno degli otto sottoprogetti ("Performance Evaluation") e la ricerca di nuove tecniche per analizzare la "vivezza del dito", al fine di evitare possibili attacchi a sensori di impronte digitali mediante dita finte;
- progetto nazionale MIUR "Sistemi di Biometria Multi-modale e Riconoscimento di Forme per la Video Sorveglianza e la Sicurezza dei Sistemi Informatici" [2005-2006];
- progetto europeo *BioSecure* [2004-2007]: rete di eccellenza finanziata dall'Unione Europea all'interno del Sesto Programma Quadro (IST);
- progetto europeo *Fidelity* [2012-2016], finanziato dall'Unione Europea all'interno del Settimo Programma Quadro (IST). Fidelity è un progetto di ricerca che coinvolge 19 partner europei e il cui scopo è quello di migliorare la sicurezza e la fruibilità dei documenti biometrici (es. passaporto biometrico), e al tempo stesso fornire una protezione avanzata della privacy dei titolari dei documenti.

Numerosi lavori scientifici sono stati pubblicati su prestigiose riviste internazionali e presentati a conferenze dai componenti del gruppo di ricerca; richieste di copie di tali pubblicazioni da parte di membri della comunità scientifica internazionale giungono frequentemente (in media 500 all'anno).

Nel 2003 è stato pubblicato il libro "*Handbook of Fingerprint Recognition*", di D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, edito dalla Springer New York; si tratta della prima monografia sul riconoscimento automatico delle impronte digitali: il libro ha ricevuto il prestigioso "2003 PSP Award" per la categoria "Computer Science" dalla Association of American Publishers.

Nel 2005 sono stati brevettati due sistemi innovativi per il riconoscimento di dita finte (una delle problematiche più attuali nel settore delle impronte digitali): uno basato sull'analisi della distorsione della pelle e uno basato sul riconoscimento dell'odore.

Nel 2009 è stato brevettato un metodo innovativo per la codifica e il riconoscimento delle impronte digitali.

Nel 2009 è stata pubblicata la seconda edizione del libro "*Handbook of Fingerprint Recognition*", di D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, edito dalla Springer New York. Si tratta di una versione rivista e aggiornata del libro pubblicato nel 2003.

Due membri del gruppo di ricerca hanno fatto parte del "Gruppo di lavoro sulle tecnologie biometriche" istituito dal CNIPA (ora DigitPA) e hanno collaborato alla realizzazione dei *Quaderni CNIPA sulla Biometria* (si vedano i quaderni n. 9, 15 e 17 disponibili all'indirizzo http://www.cnipa.gov.it/site/it-IT/La_Documentazione/Pubblicazioni).

Nel seguito sono brevemente descritte alcune delle più importanti iniziative e dei maggiori risultati di ricerca conseguiti dal Biometric System Laboratory.

Confronto di impronte digitali

Nel 1997 il gruppo di ricerca ha proposto un metodo per l'*estrazione di minuzie* (le caratteristiche delle impronte digitali utilizzate per il riconoscimento) direttamente da immagini a livelli di grigio. Si è trattato di un notevole passo avanti rispetto agli algoritmi esistenti, che richiedono la binarizzazione (trasformazione in bianco e nero) dell'immagine e altre operazioni da effettuare sull'immagine, prima di poter procedere al rilevamento delle minuzie. L'estrazione diretta a livelli di grigio si dimostra essere più efficiente ed accurata rispetto alla tecnica tradizionale. Diversi gruppi di ricerca stranieri hanno utilizzato il metodo proposto come base di partenza per lo sviluppo dei propri sistemi di riconoscimento di impronte.

Nel 2009 il gruppo di ricerca ha proposto (e brevettato) una nuova tecnica per la codifica e il confronto delle impronte digitali: *Minutia Cylinder-Code (MCC)*. La nuova rappresentazione proposta è molto robusta rispetto alla distorsione elastica della pelle e a errori di acquisizione. Dagli esperimenti effettuati il nuovo metodo risulta essere estremamente accurato e veloce (eseguendo fino a 4 milioni di confronti al secondo su un singolo PC).

Classificazione e indicizzazione di impronte digitali

Nel 1999 il Biometric System Laboratory ha presentato un metodo innovativo per la *classificazione di impronte digitali*. Il problema della classificazione delle impronte è molto sentito nelle applicazioni in cui una singola impronta deve essere confrontata con tutte quelle presenti in un database (un caso tipico è quello della ricerca di un'impronta latente trovata sul luogo di un crimine, che deve essere confrontata con tutte quelle presenti in archivio). Poiché i database delle più importanti organizzazioni

investigative contano diversi milioni di impronte, la suddivisione delle stesse in varie classi è fondamentale al fine di restringere il numero di confronti da effettuare (l'impronta da verificare può essere confrontata solo con quelle appartenenti alla stessa classe). Purtroppo la classificazione automatica delle impronte è un problema molto difficile e ancora oggi la classificazione è eseguita in maniera manuale o semi-manuale. Il nuovo metodo presentato dal gruppo di ricerca ha dimostrato prestazioni superiori a tutti quelli pubblicati in letteratura ed è attualmente l'unico algoritmo in grado di soddisfare i requisiti del FBI in termini di errori di classificazione sul database di impronte NIST DB14 (il principale benchmark nel settore).

Nel 2011 il gruppo di ricerca ha presentato un nuovo metodo di classificazione continua (indicizzazione) di impronte digitali basato sul *Minutia Cylinder-code (MCC)*. Gli esperimenti effettuati sui database di impronte NIST DB4 e NIST DB14 hanno mostrato come il nuovo metodo di indicizzazione ottenga risultati di gran lunga superiori rispetto ai metodi fino ad ora pubblicati in letteratura.

FVC (Fingerprint Verification Competition)

Nell'anno 2000, il gruppo di ricerca, in collaborazione con il Prof. A.K. Jain e il Prof. J.L. Wayman, ha organizzato la *prima competizione internazionale fra algoritmi per riconoscimento di impronte digitali*: Fingerprint Verification Competition (*FVC2000*). L'evento ha riscosso un grande successo sia presso il mondo accademico sia in ambito industriale; infatti si è trattato del primo test indipendente delle prestazioni delle tecnologie per il confronto di impronte (di solito ogni azienda fornisce indicatori di prestazioni dei propri sistemi misurati internamente, ma queste misurazioni sono tutt'altro che attendibili). FVC2000 è stata organizzata con il duplice obiettivo di permettere a sviluppatori e ricercatori di confrontare in modo non ambiguo i loro algoritmi e di fornire una panoramica sullo stato dell'arte del settore. L'iniziativa è stata decisamente un successo:

- undici organizzazioni (cinque imprese e sei gruppi di ricerca) hanno partecipato alla gara;
- quattro database di impronte digitali sono stati raccolti;
- i risultati sono stati presentati alla XV International Conference on Pattern Recognition (ICPR2000) a Barcellona;
- un sito web (http://bias.csr.unibo.it/fvc2000) è stato creato e mantenuto aggiornato; il sito ha avuto più di 12.000 visitatori nell'anno 2001;
- un dettagliato rapporto tecnico è stato preparato e reso disponibile via web. Il rapporto è stato richiesto da migliaia di persone, è reso disponibile in decine di siti web sull'argomento e citato come fonte autorevole in numerosi testi specialistici, come l'*Interpol report on fingermarks, shoesole impressions, ear impressions, toolmarks, lipmarks, bitemarks for the period 1998-2001*;
- un CD-ROM contenente i quattro database e i risultati è stato preparato e più di 70 copie sono state acquistate da importanti organizzazioni e aziende del settore;
- molti gruppi di ricerca stanno attualmente utilizzando i database di FVC2000 nei loro esperimenti;
- alcune società che inizialmente non avevano partecipato alla competizione hanno chiesto al Biometric System Laboratory di certificare le prestazioni dei loro sistemi su FVC2000.

L'interesse suscitato da FVC2000 e gli incoraggiamenti ricevuti hanno portato il Biometric System Laboratory a organizzare tre nuove edizioni della competizione: rispettivamente nel 2002 (http://bias.csr.unibo.it/fvc2002), nel 2004

(http://bias.csr.unibo.it/fvc2004) e nel 2006 (http://bias.csr.unibo.it/fvc2006). Il numero di partecipanti alle successive edizioni mostra come il successo dell'iniziativa sia in continua crescita: 31 sono stati gli algoritmi valutati in FVC2002, 67 in FVC2004 e 70 in FVC2006.

Nel 2010 il gruppo di ricerca ha realizzato FVC-onGoing, un innovativo sistema web automatico per la valutazione di algoritmi per il riconoscimento automatico delle impronte digitali. FVC-onGoing è la naturale evoluzione di FVC: ad oggi, oltre 400 partecipanti si sono registrati e più di 1500 algoritmi sono stati valutati dal sistema.

Impronte digitali sintetiche

All'inizio del 2001, il Biometric System Laboratory ha presentato *SFinGe*, il primo metodo al mondo in grado di generare database di impronte digitali artificiali. La generazione di impronte digitali artificiali si inquadra all'interno della necessità (che si sta ponendo con sempre maggior urgenza) del confronto fra i vari metodi di riconoscimento di impronte digitali e della certificazione delle loro prestazioni. Infatti, poiché la percentuale di errore di un sistema di riconoscimento di impronte è solitamente molto bassa, per poterla stimare con sufficiente precisione, è necessario disporre di un database molto grande di impronte digitali "campione". Ad esempio, per poter dichiarare, con una confidenza del 95%, che la probabilità di un metodo di accettare un impostore sia inferiore allo 0.01%, sono necessari circa 1.000.000 di confronti fra coppie di impronte digitali. Inoltre, una volta che un database di impronte campione è stato "utilizzato", ossia un algoritmo è stato sottoposto a test (e ottimizzato) su di esso, per una successiva fase di test, è indispensabile utilizzare un database differente. Raccogliere database d'impronte digitali è un procedimento assai dispendioso in termini di tempo e denaro, inoltre può essere problematico a causa delle leggi sulla privacy che in alcune nazioni proibiscono la diffusione di informazioni personali come le impronte digitali. Dall'analisi di tali problematiche, all'interno del gruppo di ricerca è nata l'idea di sviluppare un metodo per la generazione di impronte digitali artificiali, in modo da poter creare, a costo praticamente nullo, grandi database di impronte con i quali testare, ottimizzare e confrontare gli algoritmi di riconoscimento.

Due anni di intense ricerche hanno portato alla realizzazione di SFinGe (acronimo di *Synthetic Fingerprint Generator*): si tratta di un metodo in grado di generare immagini di impronte digitali estremamente realistiche, a partire da un certo numero di valori generati casualmente. SFinGe è in grado di simulare diverse impronte dello stesso dito, in modo da poter generare database con cui verificare il funzionamento di algoritmi per il confronto di impronte. Il processo di generazione delle impronte digitali può essere distribuito un maniera automatica su una rete di PC, consentendo di velocizzare la procedura in maniera notevole: con 10 PC connessi in rete è possibile generare un database di un milione di impronte in meno di un giorno!

Il nuovo metodo ha immediatamente suscitato grande interesse da parte della comunità scientifica e industriale internazionale. La versione "base" del programma che implementa il metodo di generazione è stata resa disponibile su web, dietro compilazione di un modulo di richiesta; i ricercatori che hanno richiesto SFinGe sono stati più di 4000, appartenenti alle più svariate organizzazioni, fra cui: *Id3 Semiconductors, Gemplus, IBM India Research Lab, Infineon Technologies, Precise Biometrics, US Army CSLA, Hewlett Packard, IBM T.J.Watson Research Center, Cross Match Technologies, Nec, Oracle, Identix, Agilent Technologies, Visionics, Keyware, Bio-Key*. La versione completa del programma è stata oggetto di

convenzioni con aziende europee, americane e asiatiche, con università straniere e alcuni enti governativi stranieri.

Riconoscimento di dita false

Recenti studi scientifici hanno mostrato come sia possibile ingannare sistemi biometrici mediante riproduzioni artificiali delle caratteristiche biometriche stesse (ad esempio una fotografia del volto, oppure la registrazione della voce). Benché non si tratti di un processo semplice, è stato mostrato come sia possibile falsificare anche un'impronta digitale, creando una riproduzione artificiale del polpastrello in grado di ingannare gli attuali sistemi disponibili in commercio.

Nel 2005 il Biometric System Laboratory ha proposto due metodi innovativi per il riconoscimento di dita false. Il primo si basa sull'elasticità della pelle: all'utente è richiesto di muovere il dito sul dispositivo d'acquisizione in modo da produrre una certa deformazione nel polpastrello, dalla cui analisi è possibile capire se si tratti o meno di una riproduzione artificiale. Infatti la pelle del polpastrello ha caratteristiche di elasticità peculiari dovute sia alla natura della pelle stessa sia alla forma e posizione della falange distale, per cui risulta essere molto difficile riuscire a emulare lo stesso tipo di deformazione con materiali artificiali. Il secondo metodo proposto si basa sull'osservazione che l'odore degli esseri umani è differente da quello dei materiali utilizzati tipicamente per fabbricare impronte artificiali, e quindi un algoritmo di riconoscimento appositamente progettato può discriminare efficacemente impronte vere da riproduzioni artificiali. A tale fine sono stati utilizzati particolari "nasi elettronici" in grado di riconoscere odori complessi.

Entrambe le tecniche sopra descritte sono state brevettate e i principali risultati sono stati presentati alla comunità scientifica in occasione della "International Conference on Biometrics 2006" che si è tenuta a Hong Kong nel mese di gennaio 2006; un articolo sull'argomento è inoltre apparso sulla rivista *NewScientist*.

Qualità degli scanner per impronte digitali

Nel 2008 il Biometric System Laboratory, in collaborazione con il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) ora DigitPA, ha introdotto una nuova definizione di qualità degli scanner per l'acquisizione delle impronte digitali. Prima di allora, il concetto di qualità era strettamente legato alla fedeltà di riproduzione del *pattern* dell'impronta originale e veniva misurata utilizzando le misurazioni usate tradizionalmente per un generico sistema di acquisizione: accuratezza geometrica, rapporto segnale rumore, ecc. La nuova definizione di qualità, introdotta dal gruppo di ricerca, prende in considerazione il concetto di qualità da un punto di vista "operazionale" cioè, considera la qualità come l'abilità che uno scanner per impronte digitali ha di acquisire immagini che massimizzano l'accuratezza dei sistemi di riconoscimento automatici. A partire da questa nuova definizione di qualità, sono stati effettuati una serie di esperimenti che hanno portato alla stesura di un insieme di metriche e di requisiti minimi che gli scanner per impronte digitali devono soddisfare per poter essere utilizzati in particolari ambiti (ad esempio nella Pubblica Amministrazione).

Requisiti minimi per fototessere da utilizzare nei documenti elettronici

Nel 2008 il gruppo di ricerca, in collaborazione con il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) ora DigitPA, ha introdotto una serie di requisiti minimi (e un'applicazione software per verificarli) che una fototessera deve soddisfare per essere inserita in un documento elettronico (ad

esempio carta di identità elettronica o passaporto biometrico). L'osservanza di questi requisiti minimi da parte degli uffici preposti all'emissione di tali documenti permetterà di ottenere un maggior livello di accuratezza durante la fase di riconoscimento automatico del possessore.

Riconoscimento del palmo di una mano

Nel 2012 il Biometric System Laboratory ha proposto un nuovo sistema di riconoscimento automatico del palmo della mano basato su *Minutia Cylinder-Code (MCC)*. Un metodo di estrazione delle caratteristiche del palmo è stato ideato e ottimizzato per poter processare con grande efficienza immagini di palmi di grandi dimensioni. I risultati sperimentali ottenuti mostrano come il sistema proposto sia nettamente superiore agli altri metodi proposti in letteratura sia in termini di accuratezza che di efficienza.

Riconoscimento del volto per applicazioni di ambient intelligence

Il riconoscimento del volto è certamente l'approccio più naturale al riconoscimento di persone in applicazioni di *ambient intelligence*. Le immagini dei volti sono in questo caso acquisite in modo completamente non supervisionato e sono pertanto caratterizzate da un'estrema variabilità in termini di posa, illuminazione e look del soggetto (capelli, barba, trucco, ecc.); il riconoscimento richiede pertanto la progettazione di algoritmi ad hoc, particolarmente robusti e veloci. Inoltre le variazioni del soggetto non possono generalmente essere rappresentate in modo adeguato dal modello dell'utente creato inizialmente a partire da poche immagini di esempio ed è pertanto necessario un aggiornamento continuo del modello. Nel 2010 il gruppo di ricerca ha proposto una nuova tecnica di aggiornamento in grado di arricchire in modo non supervisionato il modello iniziale dell'utente, operando un'analisi di sequenze video acquisite mentre gli utenti svolgono le loro normali attività quotidiane.

Riconoscimento da identikit

Il riconoscimento del volto da identikit è un problema molto interessante dal punto di vista delle possibili applicazioni pratiche. Il confronto diretto tra fotografie segnaletiche e identikit (disegnati da esperti o tramite appositi software) si rivela inefficace a causa della grande differenza che sussiste tra i due tipi di immagini. Presso il laboratorio sono allo studio tecniche innovative per il riconoscimento da identikit, basate sull'estrazione di caratteristiche che accomunino fotografie e identikit e ne rendano possibile un confronto diretto.