Editoriale

La Digital Forensics - Il metodo scientifico delle IT nelle attività investigative

Nelle attività investigative sono in crescente aumento le applicazioni di tecniche informatiche sempre più sofisticate finalizzate a supportare il compito di esperti impegnati nella ricerca della verità in vicende criminose il cui responsabile è spesso ignaro di lasciare tracce della sua presenza o della sua identità. A maggior ragione tali tecniche si applicano ai crimini informatici, ovvero a quei reati che si compiono mediante lo stesso mezzo informatico e vengono facilitati dall'uso di tutte le possibilità offerte dalla rete, ove è diventato sempre più praticabile il furto di identità e la frode di informazione. Infatti, la scala globale di diffusione delle informazioni fornisce l'occasione di incrementare i reati informatici. mettendo ovviamente in crisi preoccupante la tutela della privacy di tutti gli utenti. Oggi gli attuali terminali di comunicazione, dai computer ai cellulari, dagli ATM (Bancomat) al Telepass, si affacciano su una stessa grande rete, ma entrando in Internet, le informazioni che ogni navigatore lascia sono sufficienti per far catturare la sua identità, e non tutti sembrano essere consapevoli di questo rischio. Inoltre, il crescente uso delle TIC (tecnologie dell'informazione e della comunicazione) nelle diverse organizzazioni crea spesso la necessità di cercare la "prova del computer" (o "computer evidence"), composta da tracce lasciate in sistemi o programmi applicativi e accesso a banche dati, in modo da consentire attività investigative di diversa natura, sia all'interno delle imprese sia in ambito forense. Esistono, perciò, diversi tipi di indagini:

- *interne alle società, anche per valutare danni arrecati;*
- *per scoprire atti di spionaggio, terrorismo e frodi di diversa natura;*
- *per evidenziare violazioni dei diritti di accesso;*
- *scoprire le finalità di inoltro di posta malevola (spam e phishing);*
- *a sostegno di un pubblico ministero o della polizia investigativa;*
- *a supporto di indagati e imputati (consulenze tecniche di parte).*

Per poter procedere ad analisi valutative utili e ripetibili, è necessario esaminare reperti costituiti da elementi certi, che possono essere ottenuti mediante il "congelamento" della prova. In altri termini questi elementi non devono essere degradati da passaggi impropri ma soprattutto non devono perdere i riferimenti temporali e in certi casi anche spaziali (in informatica lo spazio è costituito dalla allocazione delle risorse, che possono essere fisiche e logiche).
Affinchè le prove di abusi o reati, a cui dare seguito con un'azione disciplinare o l'apertura di un procedimento civile o penale, siano utilizzabili è necessario che soddisfino criteri di conformità. Le prove raccolte con metodi tradizionali non sempre sono sufficienti a garantire la loro ammissibilità nei procedimenti giudiziari. Si evidenzia, quindi, la necessità di un nuovo approccio per garantire la corretta raccolta delle prove che corrisponde a verifiche di accettabilità, autenticità, completezza e affidabilità. L'esperto di computer-forensics, per offrire la sua opera nella computer-crime (criminalità informatica), è solito preservare, individuare, indagare e analizzare il contenuto memorizzato in qualsiasi supporto o dispositivo di memoria. Tuttavia, queste attività devono essere rivolte non solo ai diversi tipi di computer, ma a qualsiasi apparato elettronico dotato di memoria per archiviare dati. Considerata l'eterogeneità di questi dispositivi all'esperto è richiesto un più ampio spettro di competenze dall'acquisizione delle prove digitali (applicando algoritmi di hash crittografici) all'analisi dei file system, applicazioni e dati (documenti, immagini, e-mail, sms, mms, etc), dall'audio-forensics (trascrizione testuale di una conversazione, estrazione delle formanti per l'analisi parametrica a fini comparativi) alla video-forensics (estrazione di caratteristiche presenti in singole immagini e in sequenze di immagini), dall'analisi di impronte digitali (mediante AFIS) alla identificazione personale mediante confronto di voci e volti (analisi comparativa, sovrapposizione parametrizzata, valutazione del grado di compatibilità), da tecniche e strumenti di intercettazione dei flussi di comunicazione alla tracciabilità personale (mediante dispositivi mobili), dal confronto tra sequenze di DNA alla ricostruzione della scena del crimine e all'analisi dei comportamenti (firma, voce, movimenti).
Per meglio comprendere la complessa interazione tra i diversi settori propri delle tecnologie informatiche e le necessità evidenziate nell'ambito delle attività investigative si è ritenuto utile descrivere questo complesso scenario attraverso la seguente metafora del Metrò:

Scenario della Digital Forensics e dei necessari contributi delle TIC

Molti sono, quindi, i reati che possono usufruire delle tecnologie informatiche e fare ricorso alle diverse tecniche di analisi basate su metodi informatici dalla computer-graphics alla video analisi, dall'audio analisi ai confronti biometrici, dall'information-retrival al data-mining, tutte finalizzate a trasformare gli elementi del crimine, i "reperti", in evidenze del crimine, le "prove", attraverso la identificazione o la tracciabilità personale, poiché tutto deve portare al responsabile di un atto criminoso. Perciò, al fine di acquisire la prova legittima da un computer o desktop o laptop o smartphone o tablet, da un server o un gestore di telefonia o un impianto di videosorveglianza o da programmi che vengono eseguiti all'interno di questi sistemi, all'esperto in digital-forensics si richiede di:

- *acquisire una prova tempestivamente, prima che venga alterata o rimossa;*
- *definire la catena di custodia dei reperti da sottoporre a scansione;*
- *bloccare in scrittura i dispositivi per la protezione dei vari supporti (dati, audio, video);*
- *assicurarsi che i dati originali non possano essere alterati;*
- *eseguire l'hash del supporto originale (firma digitale con riferimento temporale);*
- *copiare bit a bit il flusso di informazioni su altro supporto;*
- *verificare l'hash della copia con l'hash originale;*
- *utilizzare tecniche e strumenti per garantire la ripetibilità del controllo;*
- *garantire la conservazione e l'accesso nel tempo.*

Ovviamente è necessario non ignorare l'alta volatilità delle evidenze in rete, poiché in Internet una informazione può durare un tempo molto breve, trovarsi in un qualunque punto del globo, e perciò può essere facilmente alterata, rimossa, sovrascritta o spostata in altro sito connesso.

Occorrono, quindi, competenze variegate e specifiche sia in ambito legale sia in settori squisitamente tecnici al fine di cercare la "prova" del reato o dell'illecito. I contributi di questo numero speciale di Mondo Digitale, scaturiti da alcune sessioni di Congressi Nazionali AICA (Roma 2009, Salerno 2013) e dal Workshop IT-STAR (Bari 2013), possono far comprendere la grande importanza dell'informatica nelle attività investigative e forensi. Attraverso questo insieme di saperi si è voluto prendere in considerazione alcuni aspetti frequenti dell'analisi forense, in modo da evidenziare tecniche e metodi informatici che caratterizzando la Digital Forensics, una scienza molto ampia che copre settori ancora più complessi rispetto alla Computer Forensics.

Giuseppe Mastronardi

Dipartimento di Ingegneria Elettrica e dell'Informazione

Politecnico di Bari

Strumenti e Metodi della Computer Forensics

N. Bassetti

Abstract. *Descriveremo i metodi e gli strumenti usati nella disciplina della digital forensics. Il focus è sul metodo scientifico e le abilità necessarie per lavorare sui reperti digitali.*

Keywords: Computer forensics, Scientific method, Open source tools

1. Introduzione

La digital forensics è una disciplina relativamente giovane e quindi in constante divenire e legata all'evoluzione dell'hardware e del software.

Si pensi a quanto è cambiato negli ultimi dieci anni, i computer sono diventati sempre più potenti, i sistemi operativi più complessi e differenziati, il mobile (smartphone, tablet, ecc.) ricopre una fetta importantissima, tutto questo implica una condizione di corsa tra gli investigatori digitali e la tecnologia.

Regolare le metodologie da applicare nella fase di acquisizione ed analisi è cosa ardua, poiché non esiste una ricetta, un protocollo definito e definitivo, quindi l'unica via è quella di applicare il metodo scientifico.

2 Il metodo scientifico nella computer forensics

Come per ogni attività forense, anche il repertamento e l'analisi dei dispositivi digitali, deve seguire i dettami della scienza, ossia la verificabilità, la ripetibilità, la misurabilità, la falsificabilità di una tesi e l'uso di strumenti comprovati dalla comunità dei *peers*.

Spesso si pensa che l'informatica sia una mera applicazione di qualche colpo di mouse e di azioni di copia ed incolla, ma non è così, l'informatica forense deve seguire delle regole al fine di garantire e giustificare la *fonte di prova digitale*.

Al fine di raccogliere le fonti di prova informatiche in modo rigoroso, si deve optare per una metodologia che utilizzi che permetta la giustificazione di ogni azione compiuta.

2.1 Le fasi

2.1.1. L'acquisizione

In questa fase lo scopo è quello di rendere un reperto informatico acquisibile il più possibile fedele all'originale, laddove possibile.

Nel caso degli hard disk si adotterà la copia bit a bit, ossia il disco sarà riprodotto su un file immagine, partendo dal suo primo bit sino all'ultimo, questo procedimento garantirà la copia esatta del disco, infine si dovrà applicare una o più funzioni di hash (MD5, SHA1, ecc.), che generano un codice univoco e non invertibile, allo scopo di verificare se la copia sia identica all'originale.

Nel caso dei dispositivi mobili, telefoni, tablet, ecc. Si agirà utilizzando i prodotti, generalmente commerciali, che possono "entrare" nel dispositivo ed effettuare una copia binaria del dispositivo; chiaramente per loro natura, l'acquisizione di questi dispositivi è sempre da effettuare in regime di irripetibilità, poiché sono soggetti a modificazioni, sia pure per il livello di carica della batteria, quindi nel caso dei apparati mobili, il metodo è abbastanza limitato, perché non c'è una tecnologia standard uguale per tutti, perciò ci si deve affidare agli strumenti che sono sul mercato (UFED, Oxygen, XRY,ecc.)

Nel caso di un sistema live, ossia acceso, l'irripetibilità è d'obbligo, quindi si procederà ad una copia forense del disco, da sistema acceso, alla fine della copia, tutti lavoreranno su quella, ma prima di effettuare la copia del disco, si deve procedere con l'acquisire tutti i *dati volatili*, come il dump della RAM, i processi, le connessioni di rete, ecc. seguendo un ordine ben preciso.

La fase d'acquisizione deve garantire che il reperto originale non sia alterato da eventuali scritture, quindi si adottano sistemi hardware come i write blocker e/o sistemi Gnu/Linux come C.A.IN.E. che permette un boot sul sistema indagato, senza "toccare" minimamente il disco originale.

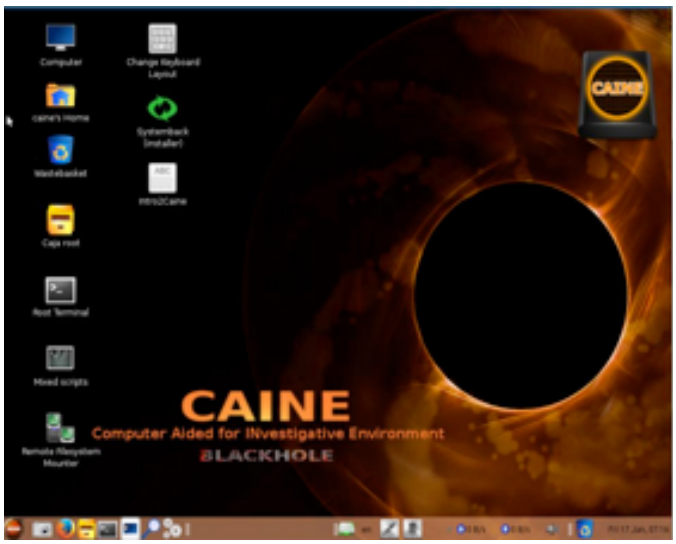


Figura 1 - Live distro forense CAINE

Figura 2 - Write blocker (Wikipedia)

2.1.2. L'analisi

Una volta acquisito il reperto, la fase d'analisi implica l'uso degli strumenti software più disparati, da quelli commerciali, ai freeware ed open source, chiaramente ogni scelta va giustificata e va dichiarato lo strumento adottato, sempre al fine della ripetibilità da parte di terzi che potrebbero voler verificare le evidenze trovate.

Nel caso si usino strumenti commerciali, l'importante è che siano accettati de facto dalla comunità scientifica internazionale, mentre su strumenti open source, sia sviluppati ad hoc dall'analista sia presi da fonti terze, va indicata la sorgente del software o allegato il codice sorgente laddove non fosse pubblicato.

A volte, nella fase d'analisi, è altresì importante, effettuare ricerche, reverse engineering, confrontarsi con esperti internazionali, e riportare anche i loro pareri, la bibliografia e la metodologia utilizzata per raggiungere il risultato.

Ultimo, ma non meno importante aspetto, è quello dedicato al tentativo da parte dell'analista di confutare se stesso, così da poter blindare i risultati ottenuti o prepararsi delle risposte a domande che potrebbero considerare aspetti meno probabili, ma comunque possibili che contestino l'analisi condotta o le risultanze.

2.1.3. Preservazione e reporting

Dopo la fase d'acquisizione, bisogna preservare il reperto con delle metodologie ben precise, prima di tutto la catena di custodia, ossia tener sempre traccia degli spostamenti del reperto e poi effettuare sempre una copia della copia, sulla quale si andrà a lavorare.

Il reporting è la fase in cui si deve stilare la relazione tecnica, che deve esser scritta in maniera semplice e comprensibile, giustificando ogni passaggio e spostando le parti più "tecniche" negli allegati.

Conclusioni

Sarebbe auspicabile possedere una cultura tecnica informatica o ingegneristica, per il semplice fatto che un consulente tecnico di digital forensics è sostanzialmente un tecnico appunto.

In questa materia si affrontano varie branche dell'informatica, file system, database, reti, linguaggi di programmazione, web, social networks, malware, sistemi mobili, insomma un po' di tutto, quindi qualcuno che viene da una lunga gavetta magari da programmatore, poi sistemista, navigatore del web, sempre aggiornato sui nuovi fenomeni e sistemi informativi sarebbe l'optimum, inoltre anche qualche nozione legale come la conoscenza degli articoli 359 c.p.p e 360 c.p.p., la legge 48/2008 oltre che del DPR 115/2002 non sarebbe male, ricordando sempre che un consulente tecnico è un tecnico non è un legale, non è uno criminologo, non è uno psicologo, non è un investigatore nel senso classico, ma una persona che deve dimostrare il come ed il perché ha trovato delle evidenze o fonti di prova digitali, preservando il reperto originale da alterazioni, utilizzando tecniche e strumenti approvati o riutilizzabili da terzi, non inventando nulla che non sia dimostrabile scientificamente e, laddove possibile, ripetibile.

Tutto questo è affrontabile anche da chi non ha una cultura di base, a patto che si impegni molto nello studiare, sperimentare, confrontarsi ed avere la tenacia di affrontare nuove sfide intellettuali, specialmente nell'aggiornarsi costantemente, vista la velocità del progresso tecnologico.

In sostanza, non bisogna accontentarsi di una certificazione privata, di un corsetto, di qualche software *friendly* e saper solo premere qualche pulsante, ma a volte anche scontrarsi con materie ostiche come la matematica, la crittografia, la logica, cose che potrebbero ostacolare qualcuno che magari le aveva lasciate sui libri del liceo e non più bazzicate per anni ed anni finché non ha deciso di essere preda del demone della digital forensics.

Queste considerazioni sono state ispirate dall'osservazione dalla costante crescita di chi si avvicina alla materia in oggetto e di ci lavora; molti bravi lavorano su casi importanti altri bravi sono relegati a ruoli minori, molti blasonati non si sa nemmeno perché lo siano e spesso si sentono di errori pazzeschi da parte di consulenti tecnici, che nonostante queste cialtronate, continuano ad essere ingaggiati da Procure e/o privati, non c'è un protocollo ben definito, non c'è un albo, una certificazione riconosciuta da chi "ingaggia", non c'è unione ,ed a volte stima, anche tra i singoli o i gruppi che si occupano di questo, insomma tutto normale, tutto italico, però colpisce il vedere o sentire di gente che fino ad un paio di anni fa a malapena sapeva cosa fosse un byte e poi si è ritrovata a lavorare su di una disciplina così complessa e così ricca di cultura tecnico/informatica, perciò e per anni di letture e discussioni su CFI (Computer Forensics Italy, una grandissima community dedicata alla digital forensics), abbiamo voluto stilare questi requirements non sufficienti ma sicuramente necessari ad iniziare un percorso da indagatori del bit.

Bibliografia

[Bassetti, 2011] Indagini Digitali – Nanni Bassetti – 2011 Lulu.com.

[AICA 2013] Congresso Nazionale AICA 2013.

[Brian Carrier 2005] File System Forensics Analysis – Addison Wesley Professional

[Cory Altheide,Harlan Carvey] Digital Forensics with Open Source Tools – Syngress Elsevier - 2011.

Biografia

Nanni Bassetti è Laureato in Scienze dell'Informazione a Bari ed è libero professionista specializzato in informatica forense. Ha collaborato come free-lance con molte riviste informatiche nazionali e internazionali e come docente per molti corsi presso enti, scuole e università, ha inoltre scritto articoli divulgativi di programmazione, web usability, sicurezza informatica e computer forensics. Ha lavorato come ausiliario di Polizia Giudiziaria e per alcune Procure della Repubblica oltre che come CTU/CTP per molte analisi forensi informatiche civili e penali. Iscritto all'albo dei C.T.U. presso il Tribunale di Bari, è consulente di parte civile per alcuni casi di risonanza nazionale. Fondatore di CFI - Computer Forensics Italy - la più grande community di computer forensics italiana. Membro fondatore di ONIF (Osservatorio Nazionale Informatica Forense) www.onif.it. Project manager di Caine Linux Live Distro forense. Curatore del sito Scripts4cf dedicato a software per la computer forensics. Ha pubblicato "Internet Web Security – tutta la verità sulla sicurezza del web" nel 2004 con la Duke Editrice e il libro "Indagini Digitali".

Email: nannib@libero.it

Acquisizione e Cristallizzazione di una Prova Digitale

A. Carnimeo

Abstract. *L'acquisizione di una immagine digitale è la chiave di ogni pratica forense. Un'accurata documentazione delle fasi, unita ad una rigorosa aderenza alle procedure ed alle migliori pratiche consolidate, realizzano con successo il processo della acquisizione della prova digitale. Questo articolo focalizza in particolare l'aspetto del congelamento della prova, che è una importante fase della digital-forensic.*

Keywords: Computer forensics, Scientific method, Open source tools

1. Introduzione

L'Acquisizione digitale dell'immagine è il processo di identificazione e documentazione della evidenza digitale originale come ad esempio un hard-disk o un computer e della conservazione della evidenza digitale memorizzata sul supporto fisico.

Il processo di acquisizione è il fondamento della digital-forensic. Il successo di una investigazione nel campo della digital-forensic è totalmente dipendente da una acquisizione corretta e da una documentazione altrettanto precisa relativa alla evidenza digitale.

Se l'acquisizione è stata effettuata in modo improprio ed è scarsamente documentata, qualsiasi evidenza derivante dalla immagine digitale può essere oggetto di contestazione, in fase di dibattimento, durante il processo, ed addirittura può essere anche respinta.

Il presente articolo pertanto ha l'obiettivo di fornire ai cosiddetti esaminatori forensi le conoscenze necessarie per eseguire un'acquisizione corretta dell'immagine digitale.

2 La legislazione italiana relativa alle evidenze digitali

Come per ogni attività forense, anche il repertamento e l'analisi dei dispositivi digitali deve seguire i dettami della scienza, ossia la verificabilità, la ripetibilità, la misurabilità, la falsificabilità di una tesi e l'uso di strumenti comprovati dalla comunità dei *peers*.

Spesso si pensa che l'informatica sia una mera applicazione di qualche colpo di mouse e di azioni di copia ed incolla, ma non è così, l'informatica forense deve seguire delle regole al fine di garantire e giustificare la *fonte di prova digitale*.

Al fine di raccogliere le fonti di prova informatiche in modo rigoroso, si deve optare per una metodologia che utilizzi gli standards esistenti e che permetta la giustificazione di ogni azione compiuta.

Le Procedure per il trattamento delle evidenze digitali non erano regolamentate fino al 2008, da quell'anno, a seguito anche della pressione esercitata dall'Unione Europea, finalmente vi è un nuovo impulso normativo nel settore dell'analisi forense:

Legge 18 marzo 2008, n. 48

Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (GU n. 80 del 4-4-2008 - Supplemento Ordinario n. 79) http://www.parlamento.it/parlam/leggi/08048l.h

Testo finale art. 247 (codice procedura penale)
Casi e forme delle perquisizioni.

1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
   1.1.Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
2. La perquisizione è disposta con decreto motivato.
3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

Testo finale art. 354 (codice procedura penale)
Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro.

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità

Testo finale art. 244 (codice procedura penale)
Casi e forme delle ispezioni.

1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica**,** anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

3. Acquisizione della immagine digitale

Cos'è una immagine digitale? Una immagine digitale, nella forensics, non deve essere confusa con una fotografia acquisita con una fotocamera, ma è una duplicazione bit a bit di dati memorizzati in una data locazione di un media digitale. Essa deve essere verificabile, significando cioè che altra gente può osservare l'immagine digitale ed affermare senza alcun dubbio "si, è lo stesso dato dell'originale". Pertanto, il processo utilizzato per acquisire la prova digitale è assolutamente importante.

Il processo di acquisizione può essere suddiviso in sei fasi fondamentali:

1. Documentazione del processo di acquisizione
2. Identificazione della prova digitale
3. Congelamento della evidenza fisica
4. Documentazione della evidenza fisica
5. Congelamento della evidenza digitale
6. Documentazione della evidenza digitale

4. Documentazione del processo di acquisizione

Da rilevare che dei sei passi elencati precedentemente, tre di essi iniziano con "Documentazione". Documentare quindi è il principale aspetto che deve considerare l'analista forense ed essendo inoltre la parte iniziale del processo di acquisizione, essa può determinare la riuscita o il fallimento di un caso giudiziario. La documentazione deve riguardare:

- La catena di custodia
- I tool standard da utilizzare per l'acquisizione
- Il numero di immagini che devono essere realizzate
- Se deve essere o meno usata la crittografia e di che tipo
- Che tipo di copia deve essere creata
- Cosa sarà documentato e come
- La convenzione sui nomi utilizzati

Il processo relativo alla documentazione può essere anche un semplice documento scritto in Word e gestito da tutto lo staff forense purché tale documento sia già stato testato.Ciò per essere sicuri che tutte le attività vengano affrontate ed affinché tutti gli esaminatori forensi che lo firmeranno,conoscano e seguano pedissequamente le fasi del processo di acquisizione della evidenza digitale.

5. Identificazione della Evidenza Fisica

L'identificazione di una evidenza fisica è una fase che è di per se esplicativa. Ma in cosa consiste? Essa consiste nella comprensione approfondita del device che contiene la evidenza e nella ricerca di ulteriori evidenze connesse con tale device. Ad esempio, ci si deve porre domande del tipo: Ci sono più di un hard-disk. C'è per caso un CD ROM nel CD Player? Vi è per caso un flash drive inserito nel device? Ci sono ulteriori supporti di memorizzazione quali ad esempio un drive di backup connesso o vicino all'evidenza? Le informazioni sono in un cloud? Come funziona il device sotto esame? Vi è manualistica in proposito?

6. Documentazione della Evidenza Fisica

Una volta identificato un pezzo della evidenza fisica vi è necessità di documentarla. Questo significa etichettarla e fotografarla ed inserire importanti informazioni relative alla evidenza, in uno schema. Informazioni importanti per tracciare qualsiasi evidenza fisica sono:

- nome dell'indagine
- numero progressivo della evidenza fisica
- data di identificazione
- data di ricevimento della evidenza fisica
- chi ha ricevuto l'evidenza
- da chi è stata fornita l'evidenza
- il luogo dove è stata ricevuta
- dove è custodita
- tipo di device (workstation, laptop, cellulare, memoria flash)
- marca
- modello
- numero seriale
- assettag
- servicetag
- note (se scheggiato, o se dotato di alimentatore)
- informazioni sul BIOS

7. Congelamento della Evidenza Digitale

Tutto ciò di cui si è discusso sino ad ora è relativo sono attività prodromiche e necessarie per le attività di acquisizione. Per essere chiari, l'acquisizione è il processo usato per conservare la evidenza digitale e i termini sono sinonimi. Una volta che la evidenza fisica è identificata e documentata, gli hard-disk possono essere rimossi, etichettati, fotografati e duplicati.

Vi sono due metodi per ottenere una immagine digitale, la acquisizione statica o post-mortem o la acquisizione live. La acquisizione statica o post-mortem è utilizzata nel caso in cui la evidenza digitale può essere spenta. Essa generalmente comporta la rimozione del media digitale da un computer e la connessione ad un device per la duplicazione.

La acquisizione live è usata nel caso in cui un device non può essere spento o il media non può essere rimosso dal computer o dal supporto su cui è fissata. Essa è tipicamente usata per la acquisizione di una immagine di un server in produzione o di un computer remoto. Vi sono inoltre due tipi di acquisizione digitale, ossia quella logica e quella fisica. Quella logica comporta la conservazione del contenuto presente (in opposizione al contenuto cancellato) memorizzato sul media digitale. Per esempio se abbiamo diverse cartelle

memorizzate su una memoria flash ma si ha necessità di acquisire solo la cartella “Documenti Segreti” e il relativo contenuto, allora possiamo effettuare una acquisizione logica del contenuto. L’acquisizione fisica è il processo di conservazione di tutto il contenuto, sia quello attivo sia quello cancellato, memorizzato sul media digitale. Ogni bit, su ogni settore, è conservato come esso è sul media originale.

Una chiave per creare con successo un’immagine è quella di proteggere sempre il media originale. Esso non deve mai essere alimentato senza la protezione in scrittura. La protezione può esser realizzata via hardware con il tableau T35 o via software come ad esempio con il SAFE (System Acquisition Forensic Environment).

8. Documentazione della Evidenza Digitale

Alla stessa maniera della evidenza fisica è possibile definire la documentazione della evidenza digitale

- nome dell’indagine
- numero progressivo dell’evidenza
- data di identificazione dell’evidenza
- data di ricevimento dell’evidenza
- chi ha ricevuto l’evidenza
- da chi è stata fornita l’evidenza
- il luogo dove è stata ricevuta l’evidenza
- dove è custodita l’evidenza.

9. Calcolo dell’Hash per Cristallizzare la Evidenza Digitale

Una volta che una copia è stata creata, deve essere effettuato il calcolo del valore hash sia sull’originale che sulla copia della evidenza. Alcuni tools usano Message Digest Versione 5 (MD5) e/o il Secure Hash Algorithm (SHA-1) per confermare che il processo di duplicazione è stato condotto correttamente.

Una funzione hash crittografica è una algoritmo sofisticato, ideato per soddisfare le seguenti quattro finalità:

1. essere relativamente semplice nel generare un valore hash, usando un data-set fornito;
2. essere estremamente difficoltoso derivare il data-set originale da un particolare hash-value;
3. essere estremamente difficile cambiare il data-set originale senza modificare anche il risultante hash-value;
4. Essere estremamente difficile che due o più data-set differenti producano lo stesso hash-value.

In un contesto quale quello della computer forensics, la funzione hash assolve a due scopi principali:

1. è un mezzo per dimostrare che l'originale e la sua copia sono identici in quanto producono lo stesso hash-value;
2. è un mezzo per ricercare tra grandi quantità di file quelli di potenziale interesse.

Le funzioni hash di crittografia possono essere implementate da qualsiasi persona. Ciò consente a tutti gli esaminatori forensi di controllare il lavoro di altri dal momento che un dato file dovrebbe produrre lo stesso valore hash quando elaborata attraverso la stessa funzione di crittografia hash.

Sebbene i processi matematici caratterizzanti ogni tipo di algoritmo di hash sono differenti, l'operazione generale è la stessa. Una funzione di crittografia suddivide un file in blocchi maneggevoli e realizza complicate operazioni matematiche per ogni blocco. Una volta che tutti i segmenti di un file, di una cartella o di hard-disk sono stati elaborati attraverso le funzioni di hash, un valore hash è prodotto e consiste in una stringa di valori esadecimali.

Ad esempio, il valore hash generato dall'algoritmo SHA-1 di un file di testo contenente la parola "dog"

e49512524f47b4138d850c9d9d85972927281da0

per contrasto, il valore hash di un file di testo contenente il nome ("Frederick Lane") è:

c0233e5407ac935144b623f3790e666e10c096ce

La lunghezza di un file o la dimensione di un immagine non è un problema. La funzione di crittografia SHA-1 produce un valore hash sempre della stessa lunghezza, indipendentemente se il file in questione è una singola parola o un romanzo. In ogni caso, se un solo carattere di un file è modificato, allora anche il suo valore di hash cambierà.

Una importante cosa da notare circa le funzioni crittografiche è che esse operano solo sul contenuto di un file e non sul nome. Ad esempio, assumendo che il contenuto di una immagine pedopornografica non sia cambiato, la foto produrrà lo stesso valore hash indipendentemente dal nome che ha in quel momento.

Conclusioni

Lo scopo della digital-image-acquisition non è solo quello di ottenere una immagine del disco. Essa è una collezione di passi che tracciano l'evidenza digitale dalla sua origine sino al dibattimento in un processo. Il congelamento della evidenza digitale è la base della digital forensics e una opportuna documentazione è la sua pietra angolare. Per far tutto ciò, l'esaminatore forense deve essere tecnicamente preparato, orientato ai dettagli ed in grado di far fronte alle diverse situazioni o complicazioni che possono sorgere durante la delicata ed importante fase della acquisizione della prova.

Bibliografia

[E-Forensic Magazine 2013] Frederick S. Lane, *Computer Forensic: Images &Integrity*

[DigitalForensic 2011] Alfredo DeSantis, *Digital Forensics* 2011

[E-Forensic Magazine 2013] Thomas Plunkett, *Digital Image Acquisition – Step by Step*

Biografia

Andrea Carnimeo nato nel 1965 a Bari, è laureato in Scienze dell'Informazione con indirizzo Applicativo presso l'Università degli Studi di Bari. Nel 2004 ha conseguito la laurea Specialistica in Informatica presso il Politecnico di Bari. E' un Certified Oracle Database Administrator ed ha ottenuto nel 2010 il Diploma di Alta Formazione in Criminologia Generale Minorile e Penitenziaria presso l'Università degli Studi di Bari. Ha lavorato presso aziende private nel campo industriale ed aerospaziale. Presso la Facoltà di Veterinaria di Bari è stato Professore a Contratto per corsi di Informatica ed ha pubblicato alcuni lavori scientifici nel campo del riconoscimento automatico. Lavora attualmente presso una amministrazione pubblica, dove, negli anni, è stato capoprogetto di sistemi di automazione e controllo a livello nazionale. Dal 2004 si occupa principalmente di sicurezza informatica e di accertamenti tecnici e/o peritali.

Email: acarnimeo@gmail.com

Identificazione Personale in Ambito Forense

A. Paoloni

Abstract. *Il tema dell'identificazione della persona è complesso sia perché le persone non rimangono uguali a se stesse ma in qualche misura mutano di giorno in giorno, sia perché le varie tecniche di identificazione possono essere in vario modo ingannate. Nell'articolo, dopo una rassegna critica delle diverse tecnologie che sono state proposte per l'identificazione personale e delle loro principali applicazioni, si porta la discussione sul tema della decisione, con particolare riferimento all'ambito forense. Infatti se nelle applicazioni commerciali è il sistema che deve decidere se l'identità dichiarata sia o meno confermata, nell'ambito forense la decisione spetta alla Corte di Giustizia e pertanto il sistema, il perito, deve soltanto fornire un dato che supporti o meno la decisione della Corte circa l'identificazione o meno dell'imputato. Conclude l'articolo una nota sui problemi di standardizzazione e di valutazione di sistemi di identificazione biometrici.*

Keywords: Speaker Recognition, Forensic speaker identification, Biometric Identification, voice disguise, language identification

1. Premessa

Alcuni ancora ricordano il processo Bruneri-Canella o dello smemorato di Collegno. La vicenda ebbe inizio il 26 marzo 1926, quando fu arrestato un uomo che tentava di rubare un vaso di bronzo nel cimitero israelitico di Torino. Portato in questura non seppe dare le proprie generalità e fu inviato al manicomio di Collegno. Il direttore dell'istituto decise di far divulgare una sua foto dalla stampa e così il 6 febbraio 1927 la foto dello sconosciuto venne pubblicata sulla popolarissima «Domenica del Corriere». Un certo Renzo Canella, di Verona, credette di riconoscere nello smemorato il fratello Giulio, professore emerito di Filosofia, scomparso nel corso della Grande Guerra. In seguito al commovente riconoscimento da parte della moglie Giulia, il professore fu affidato alla famiglia. La sera del 7 marzo però arrivò alla Questura di Torino una lettera anonima con il seguente messaggio: «State attenti: la persona che si fa passare per il prof. Canella potrebbe essere il pregiudicato Mario Bruneri». Si aprì un

caso giudiziario lungo e complesso che, malgrado cinque processi (5 anni d'indagini, 142 deposizioni, 14 perizie), lascia ancor oggi alcuni interrogativi irrisolti. Non si può sostenere che ai nostri giorni un simile equivoco sarebbe impossibile, perché anche allora la scienza era in grado di accertare l'identità fisica di una persona in quanto erano disponibili ben tre serie di impronte digitali del Bruneri da comparare con le impronte digitali dello smemorato, ma questo non sembrò sufficiente. Ecco cosa dice in un suo libro sul caso [1] il Presidente della Corte di Appello di Firenze a proposito delle impronte:

> *"dopo i perfezionamenti portati nei metodi di raccolta e di lettura delle impronte digitali, intorno alla importanza decisiva di questo mezzo di identificazione personale non è possibile avere, ormai, alcun dubbio. E all'esame delle impronte digitali si fece ricorso anche nel caso Bruneri - Canelli. Dal 1920 al 1922 Bruneri era stato tratto in arresto per ben tre volte, e gli uffici carcerari avevano raccolto ciascuna volta le sue impronte digitali. Senonché quelle del 29 luglio 1920 e del 12 gennaio 1922 erano riuscite chiare, mentre quelle del 28 gennaio 1920 erano alquanto confuse e perciò di incerta lettura.*
>
> *Il perito giudiziale, trascurate queste ultime, fermò la sua attenzione soltanto sulle impronte del 29 luglio 1920 e del 12 gennaio 1922: dopo averle poste confronto con le impronte digitali dello sconosciuto, dichiarò nel modo più esplicito che le impronte dello sconosciuto corrispondevano esattamente quelle di Mario Bruneri.*
>
> *Di opposto avviso furono i periti stragiudiziali. Sollevarono, in primo luogo, il dubbio che raccogliere impronte di Mario Bruneri nel momento del suo ingresso in carcere non si fosse proceduto con tutte le necessarie cautele; in secondo luogo giunsero, attraverso una serie di impugnative e di negazioni, alla conclusione che l'esame comparativo delle impronte digitali di Mario Bruneri e le impronte digitali dello sconosciuto non permetteva di affermare la identità dei due individui."*

2. Sistemi di identificazione

La vicenda sopra riassunta mostra come sia difficile, in alcuni particolari casi, procedere ad una identificazione certa della persona, identificazione che noi operiamo giornalmente quando porgiamo il nostro saluto a conoscenti amici e colleghi, nonché ovviamente ai nostri familiari. Per identificare una persona noi utilizziamo i nostri sensi, in particolare la vista, l' udito e forse anche l'olfatto. Nel limitato ambiente che ci circonda i mezzi di identificazione forniti dai sensi sono certamente più che sufficienti per operare le necessarie distinzioni. Non ci aspettiamo certo, quando incrociamo un nostro coinquilino, che qualcuno si sia sostituito a lui.

La frequentazione quotidiana permette di utilizzare efficacemente, per riconoscere una persona, sia gli aspetti fisiologici, come il colore degli occhi e la forma del naso, sia gli aspetti comportamentali, come il modo di parlare, il taglio dei capelli e il modo di vestire. Quando però la persona si allontana, ovvero quando non abbiamo un abituale frequentazione della stessa, come possiamo

identificarla? E' ben noto che esistono tre vie per il riconoscimento individuale: ci si può basare su qualcosa che si possiede, ad esempio un sigillo (oggi una chiave, una scheda), oppure ci si può basare su qualcosa che si conosce, una parola d'ordine (oggi un pin, una password) o infine ci può basare su qualcosa che si è, sulla cosiddetta impronta biometrica.

La biometria a sua volta fa uso di due diverse tipologie di parametri caratteristici, quelli strettamente fisiologici, come l'impronta digitale, l'iride o le dimensioni del palmo della mano, e quelli appresi o comportamentali che derivano da un'abitudine, come la scrittura, la voce, il modo di camminare o di dattiloscrivere.

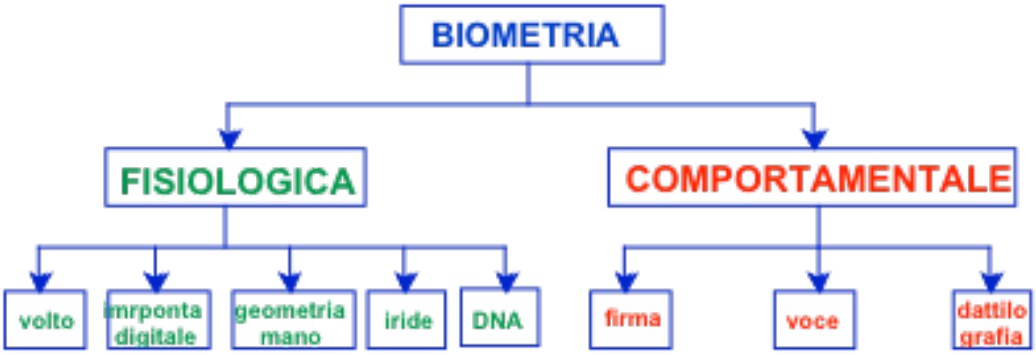


Figura 1 - Tecnologia dei metodi di identificazione

Le caratteristiche biometriche, fisiologiche e comportamentali, sono la base per l'identificazione biometrica [2], [3]. Le caratteristiche fisiologiche variano poco nel tempo mentre le caratteristiche comportamentali possono essere difficili da misurare stante l'influenza su di esse di fatica, stress o stato di salute.

3. Le tecniche

La prima applicazione consapevole della biometria al fine di identificare una persona avviene in ambiente giudiziario. *L'identificazione antropometrica* fu proposta nell' '800 da Alfonse Bertillon e consisteva nella misura di alcune parti del corpo umano: altezza, lunghezza e larghezza della testa, lunghezza e larghezza delle orecchie (v. fig.2) , distanza tra il gomito e l'estremità del dito medio, lunghezza del medio e dell'anulare, lunghezza del piede sinistro, lunghezza del tronco ed estensione delle braccia aperte dall'estremità di un dito medio all'altra. Le probabilità che una particolare misurazione fosse esattamente la stessa per due individui diversi erano di 1 su 4. Le probabilità che due persone diverse condividessero tutte e undici le misure erano pertanto di una su quattro alla undicesima, o una su 4.191.304.

Se corredate di fotografie e precise descrizioni, quelle che Bertillon chiamava "ritratti parlanti", le misurazioni avrebbero potuto distinguere una persona da un'altra. Il punto debole del metodo di Bertillon è la difficoltà di misura. In effetti non è facile misurare in modo ripetibile e con precisione la lunghezza di un dito

o la larghezza di un orecchio e questa difficoltà rende il numero sopra calcolato certamente sovrastimato.

Figura 2 - Misura della lunghezza di un orecchio

Quasi contemporaneamente all'affermarsi del metodo delle misure antropometriche venne proposto un metodo di identificazione di assai maggiore potenza e facilità d'uso: *l'impronta digitale*. Le impronte sono diverse in modo significativo anche nei gemelli monozigoti e l'identificazione tramite impronta può essere compiuta nel giro di pochi minuti e con costi ridotti; questo la rende un identificatore molto importante, anche più del DNA.

Un altro metodo biometrico impiegato nel forense è il riconoscimento della scrittura. Le metodiche utilizzate in questo campo sono numerose e si basano sia su elementi di regolarità sia sull'identificazione di quelli che vengono chiamati "gesti fuggitivi", ovvero peculiarità grafiche dello scrivente.

Un'altra caratteristica biometrica di tipo comportamentale molto utilizzata in ambito forense, è il riconoscimento del parlante. L'importanza di questo identificatore è legato alla grande disponibilità di materiale da identificare stante il generale uso del telefono in ambito criminale. Estorsioni, trattative nei sequestri, accordi per la consegna di droga, tutte queste comunicazioni, quando intercettate, possono dar luogo a dispute sull'attribuzione delle voci. Tali attribuzioni vengono affidate ad un esperto al fine di identificare il parlante sulla base dei campioni di voce forniti dagli imputati. L'attendibilità delle attribuzioni

effettuate con l'analisi acustico-fonetica del segnale vocale dipende molto dalla qualità del campione reso disponibile [4], [5], [6].
Non esiste in questo ambito un preciso limite di qualità e quantità del segnale che imponga di non utilizzare, in una perizia, un campione che non lo rispetti, come invece accade per il numero di minutiae (16) necessarie perché l'attribuzione di un'impronta digitale sia una prova. Gli esperti concordano tuttavia che con una durata del segnale inferiore a 10s o un rapporto segnale/rumore inferiore a 10 dB[1] tali segnali non debbano essere utilizzati nella attribuzioni peritali.

Tecnica	Valore indicativo FRR (%)	Valore indicativo FAR (%)	Costo dispositivi	Dimensioni template di riferimento (Bytes)	Accettazione da parte degli utenti
Impronta digitale	3-7	0.0001-0.001	Medio	300-1200	Media
Geometria della mano	1-10	1	Medio	< 10	Media
Caratteristiche della voce	10-20	2-5	Basso	1500	Alta
Scansione della retina	1	0.01	Molto alto		Bassa
Scansione dell'iride	1-10	~ 0	Alto	512	Alta
Verifica della firma	3-10	1	Medio	1500	Alta
Geometria del volto (verifica identità)	10-20	0.001-1	Medio	Pochi bytes	Alta

Tabella I - Tecnologie biometriche e loro principali caratteristiche

Le applicazioni "civili " del riconoscimento del parlante prevedono metodi di identificazione automatica basati sull'analisi dell'ambito frequenziale del segnale. Questi metodi hanno affidabilità dell'ordine dell'1% di EER (Equal Error Rate), inferiore a quella ottenibile con i metodi acustico-fonetici e comunque inferiori a quelli ottenibili con l'impronta digitale o l'analisi della retina, ma hanno il vantaggio di utilizzare un sensore molto diffuso e disponibile: il telefono.
Anche il sangue ha fornito un elemento utile per le indagini, dapprima grazie alle diversità dei gruppi sanguigni e più recentemente, con i sistemi di identificazione del DNA. Il sangue insieme con altri liquidi organici, come la saliva, rappresenta una traccia spesso decisiva nell'individuazione dei criminali.

Altri metodi di frequente impiego sono il riconoscimento del volto, che può avvenire con diverse metodiche, quella basata sul riconoscimento delle posizioni reciproche delle parti del volto (orecchio, naso, occhi, bocca, ecc.) e quella basata sul riconoscimento del pattern a raggi infrarossi, il riconoscimento della geometria della mano che avviene con un dispositivo che posiziona le dita della mano (destra) su apposite guide; le caratteristiche della mano vengono

[1] Il decibel è una misura del rapporto tra l'intensità di due segnali, nel presente caso il segnale utile e quello disturbante (rumore).

registrate con una telecamera a specchi e a partire da tali immagini viene calcolata una maschera a 9 byte; il metodo basato sulle caratteristiche dell'iride il quale presenta un insieme di particolarità simili alle minutiae dell'impronta digitale, ma assai più numerose (circa 250 contro le 50 di un'impronta completa). L'analisi dell'iride avviene utilizzando un laser a bassa intensità, che effettua la scansione dell'occhio e consente di rilevare le peculiarità dello stesso. Nella Tab. I sono riassunte le principali tecniche biometriche e le loro principali peculiarità mentre nella Fig. 3 si può osservare quale sia il volume di mercato relativo per le diverse tecniche biometriche.

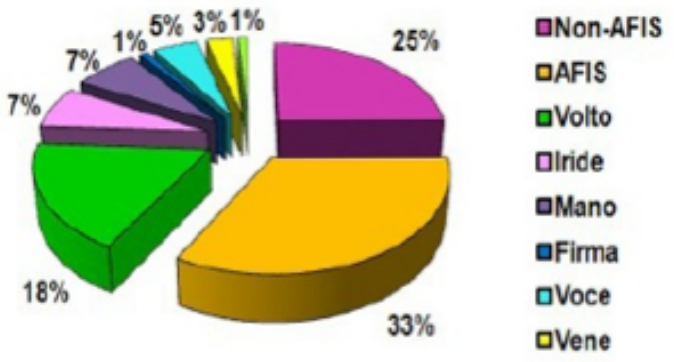


Figura 3 - Mercato mondiale della biometria: tecniche biometriche

4. Applicazioni

L'impiego delle tecniche biometriche nell'identificazione della persona ha applicazioni assai diverse: quelle giudiziarie, orientate a collegare una traccia (impronta, immagine, liquido organico) ad un indiziato; quelle investigative, orientate alla prevenzione del crimine attraverso la sorveglianza di un ambiente sensibile; quelle commerciali, volte a sostituire chiavi e codici con l'autenticazione dell'identità della persona. Nella Fig. 4 sono riportate le principali aree applicative e la rilevanza di ciascuna di esse. Il controllo accessi (33%) e l'uso forense (26%) risultano ai primi due posti e insieme rappresentano il 60% delle applicazioni.

La scelta di una caratteristica biometrica deve tener conto dell' applicazione a cui è dedicata.

Caratteristica peculiare dell'identificazione giudiziaria è che deve, o almeno dovrebbe, essere certa, incontrovertibile, per fornire la prova della colpevolezza del reo. Un'altra caratteristica dell' applicazione forense è che l'identificazione viene affidata ad un esperto che opera con tutti gli indizi di cui può disporre ed ha a disposizione tutto il tempo necessario ad effettuare il confronto [7].

Anche dal punto di vista dell'accettabilità del sistema nell'ambito forense ci si può avvalere di vari metodi coercitivi per far accettare all'imputato la metodica che si rende necessaria per acquisire il campione di confronto.

Nelle applicazioni commerciali o di sorveglianza bisogna tener conto di esigenze diverse: la necessità di identificare la persona in tempo reale, ovvero in tempi molto ristretti, dell'ordine di qualche secondo; la bassa invasività del sistema al fine di renderlo accattabile; il rispetto della privacy; una buona usabilità.

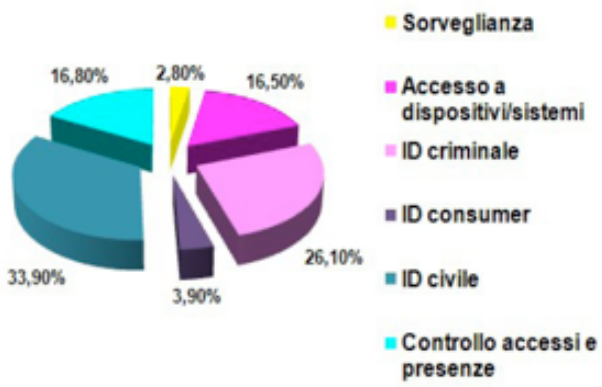


Figura 4 - Mercato mondiale della biometria per applicazioni

Nell'ambito della sorveglianza può essere importante identificare una persona senza che essa ne sia a conoscenza. Quest'ultima caratteristica è presente nei sistemi di riconoscimento vocale e di riconoscimento del volto.

Come si vede in fig. 3 l'impronta digitale è la tecnologia di gran lunga più utilizzata, per la sua alta affidabilità, per la relativa semplicità di impiego, per il basso costo e per la lunga tradizione applicativa che ne prova l'affidabilità; i principali problemi di questa tecnologia sono legati ai sensori che richiedono una costante manutenzione per poter essere efficaci.

5. Problemi di decisione

Come già detto nelle applicazioni giudiziarie non è necessario che l'identificazione avvenga in tempo reale, ma la colpevolezza dell'imputato deve essere provata "al di là di ogni ragionevole dubbio". Questa decisione però non è di competenza dell'esperto, ma della Corte. La letteratura internazionale suggerisce uno schema di decisione di tipo bayesiano: l'esperto, dopo aver effettuato i suoi calcoli, dovrà fornire un moltiplicatore, il rapporto di verisimiglianza, con il quale la Corte aumenterà o diminuirà la probabilità di identificazione che ha ritenuto di assegnare all'imputato prima dell'esame. Il rapporto di verosimiglianza avrà al numeratore la misura della "similarità" tra la caratteristica dell'imputato e quella della traccia, al denominatore la "tipicità", ovvero quanto la caratteristica presa in esame sia rara, al limite unica, all'interno della popolazione di riferimento. La definizione della popolazione di riferimento che influisce in modo rilevante sul risultato dovrebbe essere oggetto di

discussione tra la difesa e l'accusa ma entrambe, accusa e difesa, non sono ancora sufficientemente informati sull'importanza di questo elemento.

Diverso è naturalmente il caso dei sistemi biometrici utilizzati per regolare l'accesso a luoghi o a servizi. In questo caso il sistema dovrà rispondere in tempo reale sulla base di una soglia di discriminazione tra utenti accettati e respinti. Come si osserva in Fig. 5 la posizione della soglia determinerà la percentuale dei falsi rifiuti e delle false accettazioni e pertanto verrà fissata in funzione degli obiettivi che il gestore del servizio si è posto. Aumentare i tasso di rifiuti consente di diminuire il numero delle accettazioni errate, ossia le accettazioni di soggetti non aventi diritto all'accesso, ma inevitabilmente scontenta l'utente registrato quando gli viene opposto un rifiuto.

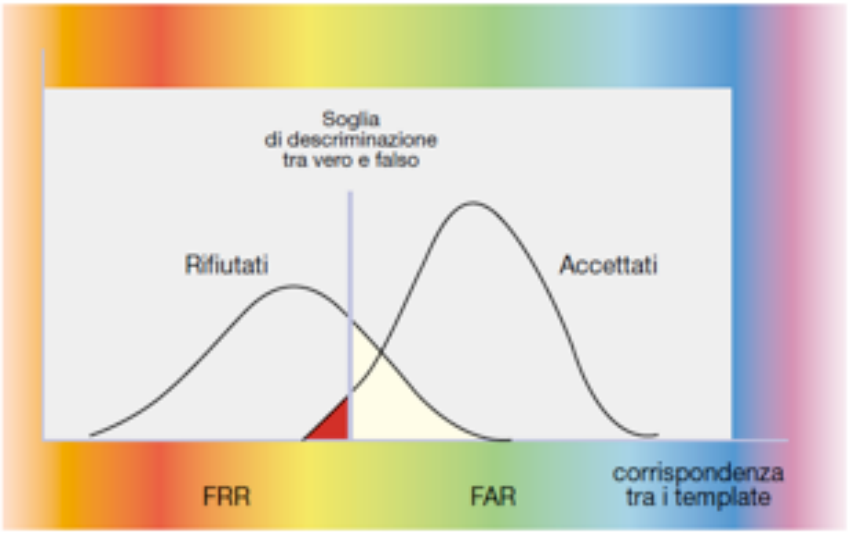


Figura 5 - Soglia di discriminazione

6. Le prestazioni dei sistemi biometrici

Lo sviluppo delle tecnologie biometriche e la loro diffusione nella società, presuppone necessariamente la standardizzazione dei dispositivi e lo sviluppo di adeguate tecniche di valutazione e un opportuno adeguamento legislativo [8].

Il tema della valutazione è di particolare rilevanza, in quanto si è osservato che tra i risultati di laboratorio ottenuti utilizzando basi di dati ricavate in opportune campagne di misura e quelli ottenibili in pratica vi sono sostanziali differenze. La valutazione in laboratorio è in un certo qual modo artificiale, sia perché i risultati ottenuti dipendono dalla base di dati utilizzata, sia perché durante la fase di prova il sistema viene utilizzato in modo ortodosso, mentre nella pratica l'utente può comportarsi in modo del tutto imprevedibile, ad esempio muovendo il dito sul sensore che rivela l'impronta o appoggiando in modo scorretto la mano sul sensore che ne verifica la geometria. Qualsiasi valutazione attendibile della reale efficienza di un sistema non può pertanto prescindere da un test in ambiente reale.

Il problema della standardizzazione delle metodiche di valutazione dei sistemi di identificazione biometrica è stato recentemente avviato in sede ISO con la stesura di apposite raccomandazioni [9] [10]. Nella normativa vengono definite le misure di valutazione, il progetto dei test, l'esecuzione degli stessi, la collocazione dei dati e le modalità di relazione.

Obiettivo è fornire stime più accurate delle prestazioni nelle applicazioni sul campo di questa tecnologia. Tuttavia le norme non tengono conto di aspetti di grande rilevanza, come l'affidabilità, la sicurezza, la vulnerabilità e l'usabilità.

Bibliografia

[1] Vescovi Vincenzo, 1942, "Una causa celebre: Bruneri-Canella" Longo&Zappelli Treviso

[2] A. K. Jain, P. Flynn, A. Ross, 2007, " Handbook of Biometrics", Springer

[3] A. K. Jain, Sept. 6, 2007 "Biometric recognition: Q&A", Nature, Vol. 449, pp. 38-40

[4] Campbell, et al., 2009 "Forensic Speaker Recognition" IEEE Signal Processing Magazine 26 (2): 95-103

[5] Paoloni A.1997, Il riconoscimento del parlatore, Detective&Crime Magazine / Criminalistica – Le indagini fonetiche

[6] Paoloni A., Falcone M., Federico A., 1998, The Parametric Approach in Forensic Speaker Recognition, Proceedings of the COST 250 Workshop on Speaker Recognition by man and machine: directions for forensic applications, Ankara, Turkey, ed. by Demirekler M., Saranli A., Altinçay H., Paoloni A., pp.45-51

[7] Paoloni A.2003, Note sul riconoscimento del parlante nelle applicazioni forensi con particolare riferimento al metodo parametrico IDEM, Rivista Italiana di Acustica, Vol. 27 n. 3-4

[8] CNIPA, settembre 2005, "Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni:indicazioni operative" Quaderno 17

[9] ISO/IEC 19795, 2007, " Information technology - Biometric performance testing and reporting"

[10] ISO/IEC 19792, 2009, " Information technology – Security technology – Security evaluation of Biometrics"

Biografia

Andrea Paoloni, Ingegnere, lavora presso la Fondazione Ugo Bordoni nel campo dell'analisi del segnale vocale, in particolare nel riconoscimento parlante. Ha avuto ruoli di docenza presso l'Università “la Sapienza” di Roma, ed è membro della scuola di Dottorato in Linguistica. Negli anni 1995-1999 è stato chairman del progetto europeo COST250 “Speaker Recognition in Telephony”. Ha collaborato con l'Autorità Giudiziaria in circa cinquecento consulenze, collabora con il RaCIS nello studio delle tecnologie di fonetica forense, è tra gli ideatori del sistema di riconoscimento del parlante denominato IDEM. L'ing. Paoloni è Vicepresidente della commissione ICT dell’Ordine degli Ingegneri, coordinatore del ForumTAL (Forum sul Trattamento Automatico della Lingua), membro dell' IAFPA (International Association of Forensic Phonetic and Acoustic), "permanent guest" dell' ENFSI (European Network of Forwensic Science Institutes) membro dell' "International Speech Communication Association" (ISCA) e dell' ASA (American Association of Acoustic). E' autore o coautore di oltre 200 pubblicazioni, tra le quali il volume “Intercettazioni Telefoniche e ambientali” ed. Centro Scientifico Editore 2007.

Email: pao@fub.it

Illusione e Scienza nella Fonetica Forense: Una Sintesi

M. Grimaldi, S. d'Apolito, B. Gili Fivela, F. Sigona

Abstract. *Questo articolo presenta una sintesi sulla fonetica forense, focalizzando l'attenzione sul problema della comparazione di registrazioni vocali, nella quale un campione intercettato della voce del reo (anonimo) viene comparato con il campione registrato della voce del sospettato o dei sospettati (saggio). Dopo aver discusso i principi fondamentali della fonetica acustica, il presente lavoro pone l'accento sul perché metodi non scientifici, come quello dell'impronta vocale, non siano più accettati dalla comunità scientifica, che si sta invece orientando verso metodi tecnico-scientifici, implementati da software specializzati: nell'ambito di tali metodi, viene infine illustrato quello basato sull'approccio bayesiano e sul calcolo del rapporto di verosimiglianza (Likelihood ratio) per il confronto delle distribuzioni statistiche delle frequenze formantiche e della frequenza fondamentale.*

Keywords: Forensic voice comparison, Speaker identification, Forensic phonetics, Likelihood ratio framework, Bayesian approach

1. Introduzione

Una questione fonetica di rilevanza forense può essere così formulata: qualcuno può essere riconosciuto in base alle caratteristiche della propria voce oltre ogni ragionevole dubbio? In altre parole, si può essere sicuri che la voce intercettata sia proprio quella del sospettato? Una risposta ragionevole è: dipende dal metodo di comparazione applicato.

Questo contributo ha l'obiettivo di fornire un breve quadro critico di come la fruttuosa integrazione di teorie e metodi nel campo della fonetica acustica con le teorie e i metodi propri dell'ingegneria e dell'informatica possa essere utile nel confronto di registrazioni vocali (in letteratura si utilizzano anche le espressioni Forensic Speaker Recognition, FSR, e Technical Forensic Speaker Identification, TFSI, quest'ultima da riterenersi preferibile). In questa sede ci soffermeremo solo sull'aspetto principale della FSR: ovvero la comparazione della voce (rimandiamo a [3] Jessen 2008 per gli altri aspetti, come il voice profiling e l'analisi dell'identificazione del parlante da parte di vittime e testimoni).

In genere, nella comparazione della voce il parlato registrato della voce anonima viene messo a confronto con il parlato registrato della voce nota. Tutte le parti coinvolte (polizia giudiziaria, giudici e avvocati) vogliono sapere se la voce dell'anonimo appartenga alla voce nota. A seconda del sistema legale in cui ci si trova a operare, intercettazioni telefoniche e/o ambientali oppure registrazioni di interrogatori possono essere utilizzate come evidenza nel caso in cui il sospettato sia poco o per nulla collaborativo. In caso contrario, si può anche ricorrere all'acquisizione di ulteriore materiale audio dal sospettato tramite 'saggio fonico' (opportunamente costruito sulla base del materiale intercettato e con esso coerente). Le registrazioni possono quindi essere messe a confronto rispetto a un'ampia varietà di tratti peculiari della voce e sulla base di metodi differenti.

La comparazione della voce può essere richiesta sia dalla Polizia giudiziaria sia da privati al di là di un dibattimento in Tribunale; ma in genere si rende necessario depositare una perizia scientificamente motivata che sarà utilizzata come evidenza in un processo e che deve essere discussa e difesa oralmente in dibattimento da parte dell'esperto responsabile della perizia ([3: 673]. Dal momento che un processo, dopo tutto, è un evento in cui si 'decide' sulla base di evidenze, un modo ragionevole di porre la questione è: qual è la probabilità che, data l'evidenza delle voci comparate, il parlato registrato della voce dell'anonimo e quello della voce nota appartengano alla stessa persona? (cfr. [7])

Prima di rispondere a questa domanda, è necessario capire in modo sintetico come si può descrivere il segnale vocale sulla base di alcuni principi di fisica acustica.

2. In principio era la voce

Per quanto riguarda le vocali, il parlato può essere definito come un segnale periodico prodotto da tre effetti: (i) il movimento periodico delle corde vocali che genera la frequenza fondamentale (F0) correlata con il tono della voce di ciascun individuo; (ii) il rumore prodotto dalla fonazione; (iii) le modificazioni del flusso d'aria da parte degli articolatori all'interno del cavo orale. Questi tre effetti generano uno spettro di frequenza, la cosiddetta *Struttura Formantica.*

La struttura formantica è caratterizzata da una serie di picchi discreti nello spettro di frequenza che sono il risultato dell'interazione tra la frequenza di vibrazione delle corde vocali e le risonanze che si generano all'interno del tratto vocale del parlante. La frequenza di questi picchi, che corrisponde alle frequenze formantiche, come anche la frequenza relativa tra i picchi, varia in base ai differenti suoni realizzati poiché sono coinvolti differenti articolatori (lingua, denti, palato, labbra, ecc.). La struttura formantica del parlato interagisce con la struttura armonica del parlato (rappresentata da multipli interi della frequenza fondamentale). Le armoniche che sono vicine alla frequenza di risonanza del tratto vocale sono chiamate *Formanti*.

Lo spettrogramma rappresenta le componenti del suono in un grafico a tre dimensioni, in cui il tempo è posto sull'asse delle ascisse, la frequenza sull'asse delle ordinate e l'intensità attraverso il maggiore o il minore annerimento delle

frequenze (oppure attraverso una scala di colori). La frequenza di questi picchi, generalmente espressa in Hz, come anche la frequenza relativa tra i picchi, varia in base ai differenti suoni prodotti. La frequenza più bassa è nota come prima formante (F1) e le formanti successive sono la F2, F3, ecc. Generalmente, le vocali sono classificate considerando i primi due picchi dell'inviluppo spettrale [5] vedi Fig.1. La prima formante è inversamente proporzionale al movimento della lingua nella dimensione verticale (alto/basso), mentre la seconda formante riflette il luogo di articolazione nella dimensione orizzontale (anteriorità/posteriorità) del cavo orale. La F2, insieme con la frequenza della terza formante, può dare utili indicazioni sull'arrotondamento delle labbra [9].

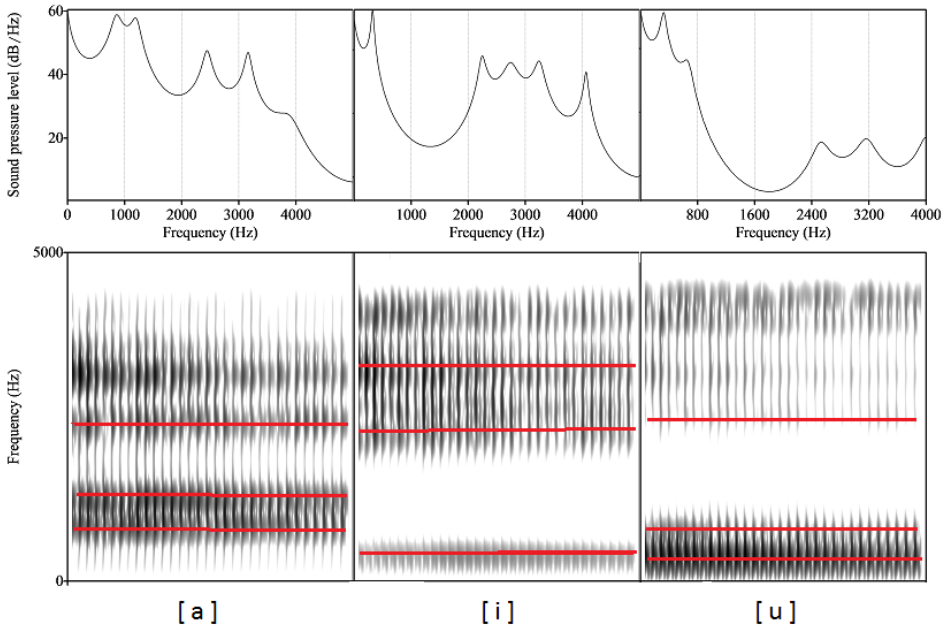


Figura 1 - Inviluppi spettrali (in alto) e spettrogrammi (in basso) delle vocali cardinali [a], [i] e [u] realizzate da un parlante italiano di sesso maschile. Le prime tre formanti sono messe in evidenza dalle linee tratteggiate.

3. L'illusione dell'impronta vocale

Agli inizi degli anni '60 quando ancora i fonetisti non avevano ancora dato un importante contributo nella disciplina, un primo esperimento fu condotto presso i Laboratori Bell [4] in cui si testò se la comparazione visiva degli spettrogrammi poteva essere utile per l'identificazione del parlatore. L'esperimento dimostrò che tale comparazione poteva avere successo. Nel corso del tempo, tuttavia, la maggior parte degli scienziati assunse un atteggiamento scettico sull'affidabilità di questo metodo poiché non era stato sufficientemente validati [8] e in alcuni casi fu respinto in modo completo [2] Bolt et al. [1] hanno criticato il metodo sollevando numerose questioni a riguardo:

1) quando due spettrogrammi sono simili, tale similarità indica che si tratta dello stesso parlante o semplicemente che si tratta della stessa parola pronunciata? 2) le similarità irrilevanti possono fuorviare una giuria composta da persone non esperte?

3) quanto sono costanti i parametri della voce?

4) quanto tali parametri sono caratterizzanti per il soggetto?

5) questi parametri possono essere simulati o camuffati?

Nonostante questo metodo sia stato strenuamente difeso da [10], il 24 luglio del 2007 una risoluzione *dell'Associazione Internazionale di Fonetica Forense e Acustica* (IAFPA) ha definitivamente deliberato che questo metodo è privo di fondamenti scientifici, dichiarando esplicitamente che esso non deve essere utilizzato in ambito forense.

Sfortunatamente, questo metodo risulta ampiamente adottato nei Tribunali italiani, grazie anche al fatto che, ancora oggi, il Codice di Procedura Penale non riconosce la figura del perito in Fonetica Forense ed Acustica (FPA). Contrariamente a quanto accade negli altri paesi stranieri, questo implica che periti e consulenti, nella migliore delle ipotesi, siano ingegneri o tecnici informatici i quali non hanno competenze di linguistica o di fonetica acustica e non sono a conoscenza dei metodi scientifici da utilizzare per il riconoscimento del parlante.

4. Riconoscimento del parlante secondo un metodo scientifico

Come evidenziato in [1], nel moderno approccio alla TFSI l'identificazione del parlante si ispira alla identificazione del DNA, cioè assumendo una prospettiva probabilistica. Occorre, innanzitutto, specificare che la comparazione della voce non avviene sulla base di tutte le proprietà del parlato, ma su solo su determinate peculiarità della voce umana, cioè le prime tre formanti che abbiamo illustrato prima insieme alla frequenza fondamentale delle vocali.

È necessario, inoltre, chiarire un concetto importante: l'esperto forense non deve e non può fornire la probabilità che il parlato registrato dell'anonimo sia stato prodotto dal sospettato. In altre parole, per molteplici ragioni, lo scienziato forense non deve presentare la probabilità di colpevolezza o di non colpevolezza. È compito del giudice giungere a queste probabilità e decidere sulla base di tutte le evidenze forensi (e non) che emergono durante il processo. Allo scienziato forense deve essere solo richiesta la forza dell'evidenza. Al fine di espletare questo compito, lo scienziato forense deve considerare due importanti aspetti: 1) la similarità, cioè stabilire quanto siano simili o differenti i campioni di parlato dell'anonimo e del sospettato rispetto ai parametri di interesse; e 2) la tipicità, cioè stabilire quanto siano tipiche o rare le caratteristiche fonetiche tra i due campioni di parlato rispetto a una popolazione di riferimento. A parità di condizioni, l'evidenza circa l'identità dei due parlanti è più forte tanto più la tipicità è bassa rispetto al caso contrario. Questo approccio si ispira alla teoria Bayesiana e in particolar modo al rapporto di verosimiglianza

- Likelihood Ratio (LR) - [7: 49-54] in cui il rapporto dell'evidenza viene valutato come segue:

$$LR = \frac{P(EH_p)}{P(EH_D)}$$

Il numeratore corrisponde alla probabilità di ottenere una data evidenza E, se i due campioni hanno la stessa origine, mentre il denominatore esprime la probabilità di ottenere una data evidenza se i due campioni hanno una origine differente. Se il LR ha un valore maggiore di 1, maggiore è l'evidenza che i due campioni provengano dallo stesso parlante, mentre se il suo valore è minore di 1 è maggiore l'evidenza che i due campioni provengano da voci differenti. Il numeratore cattura la similarità: se la similarità è alta, la probabilità che la sorgente dei due campioni sia la stessa è anch'essa relativamente alta; se la similarità è bassa, la probabilità che la sorgente dei due campioni sia differente è anch'essa relativamente molto bassa. Il denominatore cattura, invece, l'aspetto della tipicità: se la tipicità è alta, la probabilità che qualcun altro possa aver dato origine alla voce anonima è relativamente alta, mentre se la tipicità è bassa la probabilità che sia stato qualcun altro, piuttosto che il sospettato, è relativamente bassa [3: 682-683].

In base al metodo utilizzato per calcolare il rapporto di verisimiglianza, il numeratore di LR può anche essere espresso come:

$$P(EH_p) = 1 - P.f.rej.$$

Dove P.f.rej indica la probabilità di rifiutare l'identificazione quando la voce dell'anonimo appartiene alla voce nota, mentre il denominatore può essere riscritto come:

$$P(EH_D) = P.f.id$$

Dove P.f.id indica la probabilità di accettare l'identificazione tra la voce dell'anonimo e quella del sospettato quando il campione dell'anonimo non è stato pronunciato dalla voce nota.

Al fine di quantificare la tipicità, è necessario creare o avere accesso ad una popolazione di riferimento basata sulle proprietà del parlato che devono essere utilizzate ai fini della comparazione. Questo è un aspetto fondamentale del LR e che necessità di ulteriori ricerche poiché le banche dati della popolazione di riferimento costruite sulle caratteristiche del parlato sono rare. Ancora più rare sono le banche dati che prendono in considerazione la variazione dialettale. Dal momento che le caratteristiche del parlato possono, in parte, essere determinate da differenze dialettali, queste caratteristiche dovrebbero essere escluse dal punto di vista percettivo e acustico nella comparazione di voci secondo il metodo Bayesiano. Inoltre, una popolazione di riferimento di questo tipo è molto interessante per il *voice profiling*, quando è disponibile solo una

registrazione di una voce anonima senza alcun possibile sospettato. Questo accade spesso durante le prime fasi di investigazione. In una situazione del genere, si può chiedere all'esperto forense di delineare un profilo in base alle caratteristiche della voce e questo può aiutare la polizia a restringere il campo dei possibili sospettati o di trovare il sospettato in base anche ad alcune caratteristiche dialettali.

Il nostro gruppo di ricerca presso il CRIL ha intrapreso un progetto di ricerca su questi aspetti. Si sta sviluppando un software semi-automatico basato sull'approccio Bayesiano del LR insieme alla creazione di una popolazione di riferimento caratterizzata da parametri acustici estratti dalle voci di parlanti di differenti varietà dialettali del Salento (una banca dati in continuo aumento). Nella Fig.2 è riportato uno screenshot del software per il riconoscimento del parlante, in fase di sviluppo al CRIL. L'interfaccia grafica permette di importare le tabelle dei valori formantici, precedentemente elaborate, relative alla voce nota (saggio) e della voce dell'anonimo (anonimo), una banca dati dei campioni registrati, di poter selezionare una qualsiasi combinazione dei parametri che si vuole considerare, i parametri in entrata per il test da eseguire, come anche i grafici relativi alla distribuzione di probabilità delle formanti, calcolata in base a test statistici parametrici multivariati. Il programma può anche esportare un resoconto delle operazioni effettuate da includere nella perizia dell'esperto.

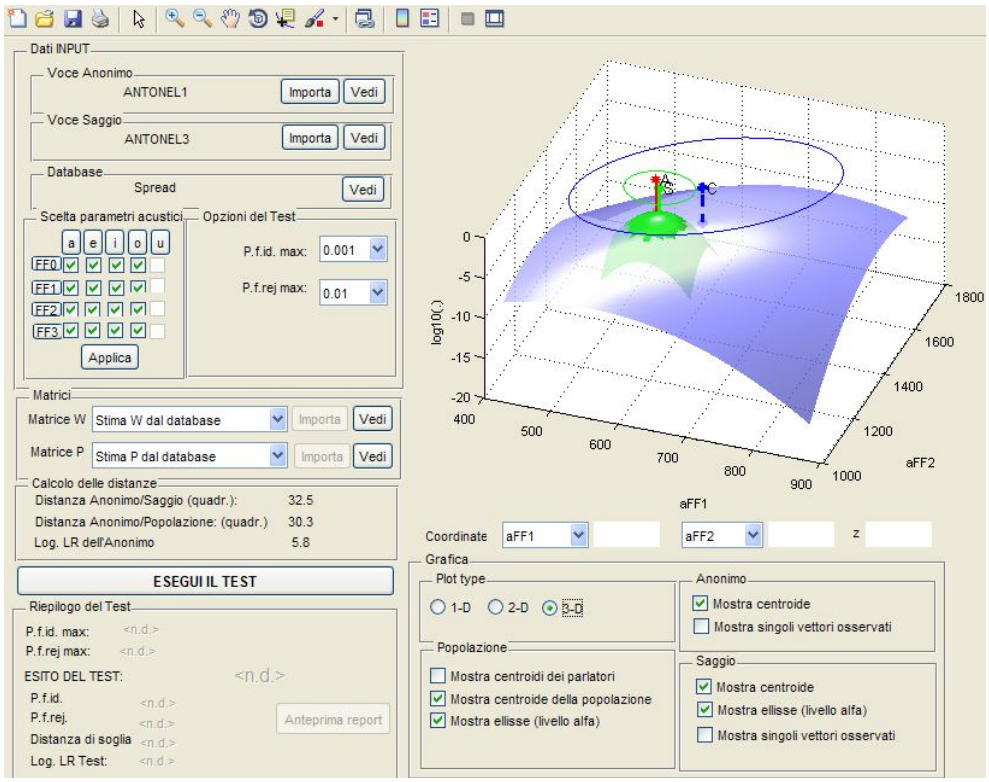


Figura 2: Uno screenshot del software in fase di sviluppo al CRIL

Conclusioni

Il moderno approccio alla TFSI è sempre più consapevole che la comparazione della voce finalizzata al all'identificazione del parlante deve essere eseguita scientificamente adottando il metodo Bayesiano non è solo un modo per comparare similarità e differenze tra determinati parametri acustici di campioni di voci differenti, ma anche il modo di conoscere quanto comuni siano le voci in base ad una popolazione di riferimento. Il ricorso alle conoscenze della fonetica e della linguistica da parte dei modelli ingegneristici ha sicuramente giocato un ruolo importante in questo processo. Ad ogni modo, sarebbe sbagliato dedurre che il LR nell'identificazione del parlante parlante in ambito forense sia ovunque accettato e istituito. Il grado in cui tale approccio è utilizzato, o anche solo compreso (data la sua complessità), differisce da nazione a nazione (cfr. [6: 67-68] per ulteriori dettagli). Allo stesso tempo, non vi è alcun dubbio che, dato l'interesse crescente nella corretta valutazione dell'evidenza relativa all'identificazione forense, ignorare tale approccio è a proprio rischio e pericolo.

Bibliografia

[1] Bolt, R. H. Cooper, F. S., David, E. E., Denes, P. B., Pickett, J. M., Stevens, K. S., Speaker identification by speech spectrograms: some further observations, Journal of the Acoustical Society of America, 54, 2, 1973, 531–53.

[2] Hollien, H., Status report of "voiceprint" identification in the United States, Occasionally, 2, 1977, 29–40.

[3] Jessen, M., Forensic Phonetics, Language and Linguistics Compass 2, 4, 2008, 671–711.

[4] Kersta, L. G., Voiceprint identification, Nature, 196, 1962, pp. 1253–1257.

[5] Peterson, G. E. and Barney, H. L., Control methods used in a study of the vowels, Journal of the Acoustical Society of America, 24, 2, 1952, 175–184.

[6] Rose P., Forensic Speaker Identification, Taylor and Francis, London & New York, 2002.

[7] Rose, P., Forensic speaker recognition at the beginning of the twenty-first century – An overview and a demonstration, Australian Journal of Forensic Sciences, 37, 2, 2005, 4–30.

[8] Stevens, K. N, Carl. E W., Carbonell, J. R. and Woods B., Speaker authentication and identification: A comparison of spectrographic and auditory presentations of speech material, Journal of the Acoustical Society of America, 44, 1968, 1596–1607.

[9] Stevens, K. N., Acoustic phonetics. Cambridge, MA: The MIT Press, 1998.

[10] Tosi, O.I. (1979) Voice Identification: Theory and Legal Applications. Baltimore: University Park Press.

Biografia

Sonia d'Apolito si è laureata in Lingue e Letterature Moderne Euroamericane presso l'Università del Salento nel 2007 e nel 2012 ha conseguito il titolo di Dottore di Ricerca presso l'Università del Salento. Durante gli anni di dottorato si è interessata allo studio delle caratteristiche acustiche ed articolatorie (movimenti della lingua) nella lingua francese. In particolare, sono stati osservati gli aspetti coarticolatori e fonologici (assimilazione di sonorità e del luogo di articolazione) all'interno di sequenze eterosillabiche di sibilanti realizzate da studenti italofoni di francese L2 e da parlanti nativi. L'obiettivo è stato quello di osservare come gli apprendenti italofoni realizzassero sequenze fonotatticamente marcate nella lingua materna e come la loro produzione si differenziasse da quella dei parlanti nativi. I risultati di questo lavoro sono stati presentati a convegni nazionali e internazionali. Attualmente si interessa di fonetica forense con particolare attenzione alla comparazione di voci.

Email: sonia.dapolito@gmail.com

Barbara Gili Fivela è professore associato di Linguistica Generale e Fonetica e fonologia presso l'Università del Salento, è vicedirettore del Centro di Ricerca Interdisciplinare sul Linguaggio (CRIL) e presidente del Corso di Laurea in Scienza e Tecnica della Mediazione Linguistica/Traduzione e Interpretariato della stessa Università. Dal 2010 è anche membro del comitato direttivo dell'Associazione Italiana Scienze della Voce (AISV). Dal 1995, dopo aver svolto attività di ricerca allo CSELT, laboratorio per le telecomunicazioni (oggi NUANCE), ha perfezionato la sua formazione presso la Scuola Normale Superiore di Pisa, specializzandosi nello studio fonetico-fonologico della prosodia; durante il triennio, ha studiato presso il Dipartimento di Linguistica dell'Ohio State University, Columbus (U.S.A.) e svolto attività di ricerca presso l'Universität des Saarlandes, Saarbrücken (Germania), l'IPDS di Kiel (Germania) e l'LPL di Aix-en-Provence (Francia). È autrice di una monografia e di più di ottanta contributi su argomenti di fonetica e fonologia di laboratorio, pubblicati in volumi, atti di convegni e riviste specialistiche nazionali ed internazionali.

Email: barbara.gili@unisalento.it

Mirko Grimaldi è professore associato di Linguistica Generale presso la Facoltà di Lingue e Letterature Straniere dell'Università del Salento, dove insegna anche Psicologia del Linguaggio. Ha ideato e dirige il *Centro di Ricerca Interdisciplinare sul Linguaggio* (CRIL), realizzato grazie a un co-finanziamento della Comunità Europea (PON 2000-2006, Ricerca Scientifica, Sviluppo Tecnologico, Alta Formazione). Il CRIL è il luogo ideale per individuare spazi di ricerca di confine, non ancora ben delineati, fra discipline linguistiche, psicologiche, mediche, ingegneristiche, informatiche e fisiche che, pur partendo da presupposti, metodologie e tradizioni diverse, possono dare un contributo per comprendere non solo la fisiologia del linguaggio ma anche e soprattutto l'organizzazione anatomico-funzionale del linguaggio nel cervello. I suoi interessi di ricerca riguardano: (i) la fonetica, la fonologia e la comparazione della voce; (ii) le basi neurofisiologiche dei processi di percezione e produzione del

linguaggio; (iii) i processi acustici, uditivi e neurofisioligici nell'acquisizione della della seconda lingua; (iv) i processi sociolinguistici e pragmatici nella comunicazione mediata dal computer.
Email: mirko.grimaldi@unisalento.it

Francesco Sigona, nato a Bari nel 1973, si è laureato in ingegneria elettronica presso il politecnico di Bari nel 1998 e successivamente abilitato all'esercizio della libera professione. Ha svolto attività di ricerca nel campo della Quality of Service (QoS) per reti Wireless LAN (IEEE 802.11), presso ST Microelectronics (STM). Dal febbraio 2007 é responsabile tecnico del Centro di Ricerca Interdisciplinare sul Linguaggio (C.R.I.L.) dell'Università del Salento, nel quale è impegnato nel supporto alla ricerca nel campo dell'elaborazione numerica di segnali biometrici relativi alla produzione del parlato (speech/kinematics/ imaging), e nello studio di algoritmi di "forensic voice comparison / speaker identification" con relativo sviluppo di applicazioni software.

Email: francesco.sigona@unisalento.it

SignVerify: Sistema a Supporto dell'Analisi Forense di Firme Manoscritte

G. Pirlo, D. Impedovo, M. Aruci

Abstract. *Questo articolo presenta il sistema SignVerify per l'analisi di firme manoscritte a supporto dell'attività forense. Il sistema infatti ha la finalità di estrarre da immagini di firme manoscritte, autentiche e/o contraffatte, caratteristiche utili per supportare l'esperto forense a giudicare una firma di test. Le caratteristiche estratte, anche se derivate da campioni di firme statiche, sono principalmente riferite ad informazioni legate al processo dinamico di apposizione delle firme.*

I risultati sperimentali ottenuti da immagini di firme manoscritte del CEDAR database, confermano la validità dell'approccio proposto e la sua utilità per finalità di analisi forense.

Keywords: Biometrics, Digital forensics, Handwritten signatures, Preudo-dynamic features

1. Introduzione

La firma manoscritta è l'elemento grafico che ci contraddistingue e ci rappresenta nella società. Le istituzioni amministrative e finanziarie la riconoscono come mezzo legale che permette la verifica dell'identità personale. La firma è infatti un segno apposto manualmente da un individuo su un documento, con l'intento di esprimere la propria conoscenza, accettazione ed approvazione del contenuto. La sua finalità principale è quella di poter essere ricollegabile in maniera univoca all'individuo che l'ha apposta. Essa assume un valore molto importante in ambito giuridico ed è soggetta sempre più frequentemente a perizie da parte di esperti grafologi. Questi esperti, attraverso una corretta metodologia e un'attenta procedura di analisi, verificano l'autenticità di una firma ed a volte anche la capacità di intendere e di volere del firmatario.

Tuttora la verifica delle firme rimane una sfida aperta dato che una firma è giudicata autentica o falsa sulla base di pochi riferimenti. La difficoltà risiede nel

fatto che le firme sono il risultato di un complesso processo che dipende dallo stato psicofisico del firmatario e dalle condizioni in cui avviene l'atto di apposizione della firma.

In questo articolo viene presentato SignVerify , un nuovo sistema automatico di analisi di firme manoscritte. SignVerify fornisce un ausilio al perito grafologo nella sua attività di valutazione del tratto manoscritto attraverso l'estrazione di caratteristiche discriminanti della firma. In particolare, partendo dall'analisi dell'immagine (statica) della firma, SignVerify prende in considerazione caratteristiche pseudo-dinamiche, in grado cioè di valutare il processo dinamico alla base dell'apposizione della firma stessa. Il sistema è in grado quindi di offrire al perito grafologo un insieme di informazioni utili per supportarlo nella sua attività di analisi.

L'articolo è organizzato nel modo seguente. Le sezioni 2 e 3 illustrano rispettivamente alcuni aspetti legati alla firma manoscritta ed alla grafologia peritale. Nella sezione 4 viene descritto il sistema SignVerify con particolare riferimento alle caratteristiche pseudo-dinamiche considerate. La sezione 5 riporta alcuni risultati sperimentali ottenuti utilizzando esempi di firme manoscritte estratte dal CEDAR database. La conclusione dell'articolo è riportata nella sezione 5.

2. la firma manoscritta

La firma manoscritta è un particolare tratto grafico che trae origine da un'azione strettamente individuale che dipende fortemente dalle caratteristiche fisiche e psicologiche del firmatario. A differenza di altri tipi di scrittura, le caratteristiche individuali si rilevano in maniera evidente nella firma manoscritta poiché i segni di cui è composta finiscono per essere appresi e ripetuti con immediatezza istintiva. Questi segni acquistano la loro forma principalmente nella fase di apprendimento scolastico in cui ogni individuo dopo aver imparato a scrivere comincia ad acquisire una propria gestualità specifica nell'apposizione della firma, aumentando la velocità di esecuzione, variando il calibro della scrittura ed effettuando tutti quei movimenti che la rendono unica.

Il grado di personalizzazione grafico di un soggetto non può essere determinato in modo assoluto; ogni stile, infatti, rappresenta per lo scrivente un sistema di scrittura autonomo che, sebbene possa presentare elementi di convergenza rispetto ad altri stili, subisce un'evoluzione di scrittura totalmente differenziata a seconda dell'uso e della preferenza accordata.

È bene precisare che non è possibile per una persona apporre la propria firma manoscritta esattamente nello stesso modo. Il processo di apposizione di una firma, infatti, non solo presenta una variabilità fisica dettata dall'impossibilità neuro-muscolare che un soggetto possa riprodurre, anche volendolo, due firme identiche; non solo è affetto da una variabilità introdotta dalla posizione di scrittura e dalla tipologia degli strumenti di scrittura utilizzati, ma subisce anche modificazioni prodotte dallo stato psicologico e che sono connesse sia al tipo di documento (e al destinatario dello stesso) sia alla volontà dell'autore di essere riconosciuto.

Ogni tentativo di imitazione della grafia altrui, o di dissimulazione della propria, comporta uno sforzo di controllo del gesto scrivente che rende il prodotto grafico artificioso e innaturale. Questo avviene perché l'impiego di attenzione imitativa o dissolutiva non può mantenersi costante e uniforme: è inevitabilmente esposto a cadute di tono e d'intensità e possono comparire nella grafia arresti bruschi, ganci, deviazioni, stacchi, innaturalezze ecc. Infatti, quando lo sforzo è focalizzato sulla forma, il ritmo ne soffre; viceversa, se la concentrazione è focalizzata nell'imitazione del ritmo naturale della scrittura, la precisione nel rendere simili le forme dei caratteri ne soffre.

Le modalità attraverso le quali avviene la falsificazione delle firme sono sostanzialmente le seguenti:

- **Imitazione a mano libera:** effettuata di getto dal falsario a lungo esercitatosi a contraffare la firma da imitare, così da acquisire l'automatismo del movimento d'esecuzione necessario per poterlo tracciare velocemente. È il tipo di imitazione più ingannevole perché il movimento è spontaneo, ma segni di allarme si presenteranno nella pressione, nella diversità dei rapporti dimensionali e nei diversi cambi di direzione.
- **Imitazione pedissequa**: riproduzione di ogni singola lettera dopo averla attentamente osservata, pertanto, in questo caso, saranno presenti una lentezza esecutiva ed un movimento aritmico oltre ad arresti e ritocchi.
- **Imitazione per ricalco**: effettuata ponendo la firma da copiare su una fonte luminosa e ricalcandola su di un altro foglio. Ciò comporta una mancanza di pressione e di rilievo, ed una lentezza esecutiva accompagnata da una falsa continuità.
- **Dissimulazione**: viene messa in atto quando un soggetto pone una firma a nome proprio in maniera diversa dalla propria (ossia è una firma naturale ma non spontanea) per sollevare dubbi sull'autenticità della firma e garantirsi la possibilità in futuro di disconoscerla. In tal caso vi sarà l'esagerazione di alcune caratteristiche proprie della grafia del dissimulatore come le ampiezze, i movimenti e la pressione, oltre alla presenza di punti inutili, tratti coprenti ed una scrittura mista di caratteri diversi.

3. Grafologia peritale

La grafologia peritale si occupa di indagare sull'identità dello scrivente allorquando ci si trova di fronte a contestazioni o a controversie che riguardano l'autenticità di una firma manoscritta. In questi casi il perito assume, quindi, un importante ruolo nell'iter processuale perché può indirizzare le decisioni giudiziarie. Proprio per tale motivo, i periti devono servirsi di un metodo scientifico per la ricerca sistematica e obiettiva della verità. Prima dell'esame della firma contestata, quindi, il perito deve costruirsi una definizione dettagliata sulle abitudini di scrittura dell'ipotetico autore della firma contestata, attraverso l'analisi di un set di prototipi di firme autografe (a volte può anche avere a disposizione dei campioni di firme contraffatte). In questo caso si parla di prototipi di firme e non di manoscritti in generale, perché regola fondamentale

delle perizie grafiche è che i documenti comparativi devono essere "omogenei", e questo significa che le firme devono essere comparate con altre firme.

Il perito, elaborando il set dei prototipi, deve definire un ragionevole "range" di naturale variabilità dell'individuo. Soltanto dopo aver definito le variazioni considerate "normali", il perito potrà dare il giusto peso alle variazioni rilevate nella firma contestata. Nel caso in cui il perito arrivi alla conclusione che la firma non è conforme alle abitudini di firma dell'autore, dovrà chiedersi se possa esserci una possibile spiegazione a tale variazione rispetto alle abitudini del firmatario.

Le principali metodologie utilizzate in grafologia peritale sono riportate brevemente nel seguito:

- **Metodo calligrafico**: Consiste nel confrontare morfologicamente due scritture e valutare la loro somiglianza. Questo metodo appare abbastanza superficiale, riferendosi soprattutto alla forma e alla compatibilità dei parametri fondamentali della grafia.
- **Metodo grafometrico**: Consiste nell'individuazione di elementi misurabili della scrittura e nella loro rappresentazione più utile ai fini della perizia. La tecnica è quindi basata sull'estrazione di caratteristiche quantitative che definiscono un tipo di scrittura. Naturalmente tale metodo ha delle limitazioni, perché, ad esempio, con una sola firma, non sarà possibile rilevare elementi sufficienti per l'analisi statistica del comportamento del firmatario.
- **Metodo grafonomico**: Questo metodo si basa sull'applicazione delle leggi naturali della scrittura. Consiste in quattro operazioni che si svolgono in tempi successivi:
  - Osservazione: processo per mezzo del quale si giunge al rilievo dei caratteri che servono a segnalare l'oggetto in esame;
  - Rilievo dei caratteri della persona: da identificare con la descrizione, con la misura, con la fotografia;
  - Confronto dei caratteri: l'operazione attraverso la quale si verifica la corrispondenza, tra gli scritti esaminati;
  - Giudizio di identità: discenderà dai riscontri e dalle constatazioni in sede di confronto.
- **Metodo grafologico**: Il metodo grafologico studia il tratto manoscritto come un prodotto integrato dell'intera attività neuro-psico-fisiologica dell'uomo, traendone gli elementi dinamici che personalizzano ogni scrittura.

4. SignVerify

SignVerify è un sistema di analisi della firma manoscritta a supporto dell'attività forense sviluppato presso il Dipartimento di Informatica dell'Università degli Studi di Bari. In estrema sintesi il sistema estrae e visualizza delle caratteristiche dalle immagini di firme manoscritte a disposizione (autentiche e/o contraffatte). Come output il sistema fornisce anche dei report in formato .txt e .xls, lasciando poi all'esperto il compito di formulare un giudizio di autenticità di una eventuale firma di test.

Figura1 - SignVerify: Interfaccia Utente

La figura 1 mostra l'interfaccia utente del sistema attraverso la quale è possibile caricare il set di firme autentiche e di firme contraffatte, ed anche il file contenente l'immagine della firma da analizzare. Per ciascuna immagine caricata viene visualizzato il nome e la grandezza in byte del file. L'interfaccia mostra anche le caratteristiche che si desidera selezionare ai fini dell'analisi.

Per la scelta delle caratteristiche estratte dal sistema si è fatto riferimento a caratteristiche di tipo pseudo-dinamiche, cioè caratteristiche derivate dall'immagine (statica) della firma ma che fanno riferimento al processo di apposizione della stessa, nel quale meglio è caratterizzabile il comportamento del firmatario genuino da quello di un ipotetico falsario. In particolare si sono considerate le seguenti caratteristiche:

- entropia dei valori di grigio;
- soglia di Otzu;
- numero di pixel neri;
- descrittori ellittici di Fourier;
- top signature.

Nel seguito sono riportate alcune considerazioni su ciascuna delle caratteristiche estratte.

1) L'entropia dei valori di grigio è definita come:

$$Entropia = -\sum_{i=0}^{255} p_i X \log(p_i)$$

dove: $$p_i = \frac{numero\ di\ pixel\ aventi\ i\ come\ valore\ di\ grigio}{numero\ totale\ di\ pixel}$$

(nel nostro caso si è lavorato con immagini a 256 livelli di grigio).

La figura 2 mostra un esempio dei risultati ottenuti dopo aver applicato l'entropia ad un campione originale e ad un campione contraffatto della stessa firma.

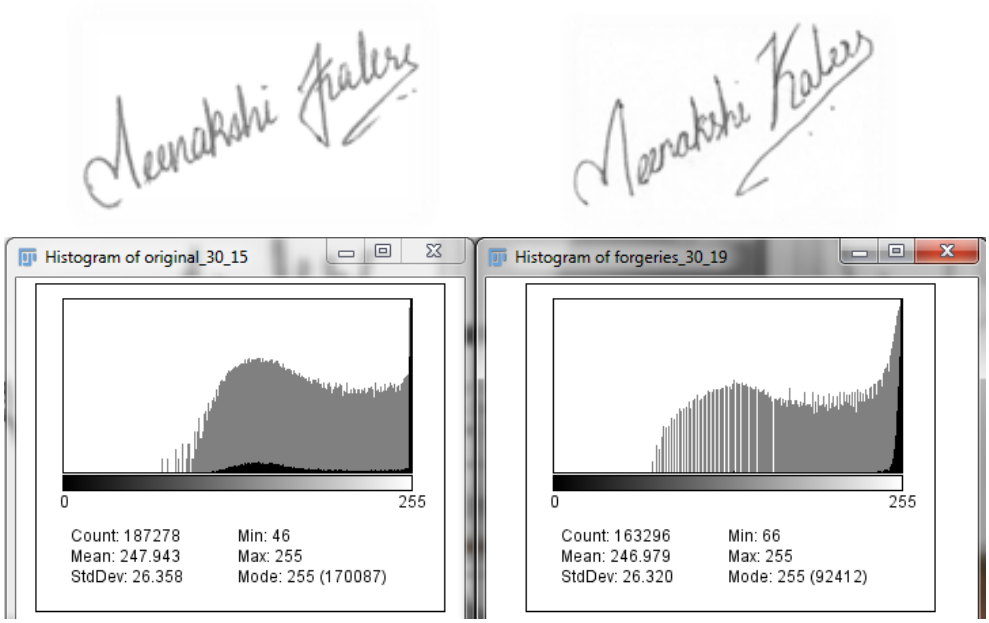


Figura 2 - Caratteristica: Entropia dei livelli di grigio

2) La soglia derivante dal metodo di Otzu, che è in genere utilizzata per la segmentazione di immagini, viene considerata come un'utile caratteristica nel dominio della verifica di firme in quanto fornisce informazioni su specifiche peculiarità del processo di apposizione della firma derivanti dalla pressione, l'angolo di contatto tra la penna e la superficie della carta, la velocità di esecuzione della firma, ecc. La figura 3 mostra lo stesso dettaglio in una firma autentica ed in una contraffatta. Nelle due immagini il valore della soglia di Otzu è pari rispettivamente a 97 e 15

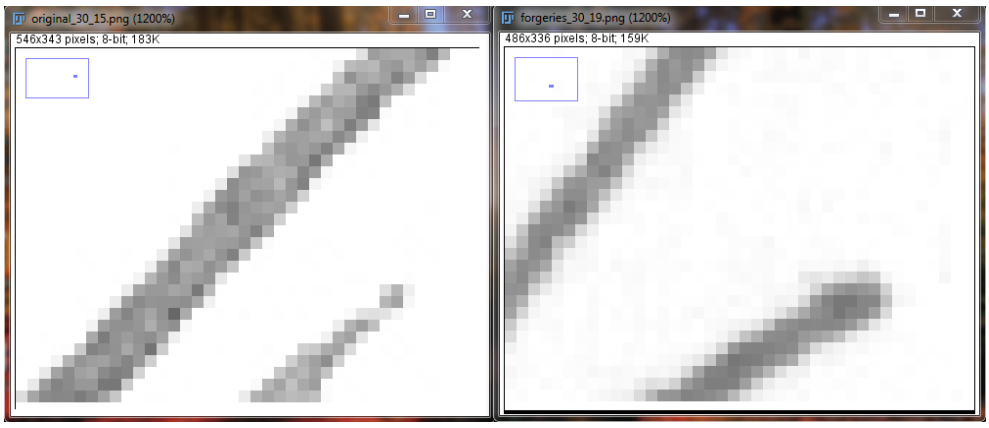


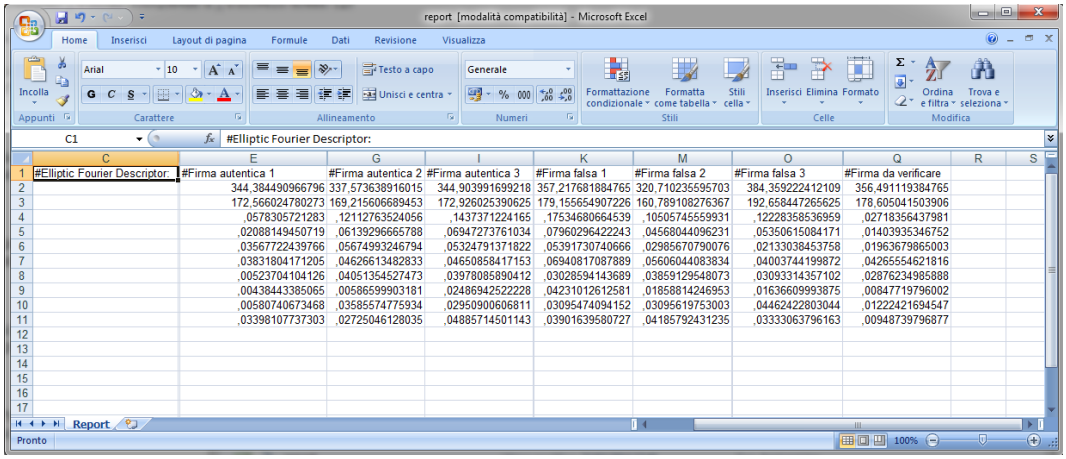
Figura 3 - Caratteristica: soglia di Otzu

3) Il numero di pixel neri è calcolato come il numero di pixel con valore di grigio superiore al valore della soglia di Otzu. Anche questa caratteristica fornisce un' indicazione sulla pressione esercitata in fase di apposizione della firma.

4) I descrittori ellittici di Fourier si ottengono dalla trasformata di Fourier dell'immagine f(x, y) della firma, definita come:

$$J\{f(x,y)\} = F(u,v) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)e^{-12\pi(ux+vy)}dxdy$$

La figura 4 mostra i descrittori ellittici di Fourier estratti da un set di firme genuine



#Elliptic Fourier Descriptor	#Firma autentica 1	#Firma autentica 2	#Firma autentica 3	#Firma falsa 1	#Firma falsa 2	#Firma falsa 3	#Firma da verificare
	344,384490966796	337,573638916015	344,903991699218	357,217681884765	320,710235595703	384,359222412109	356,491119384765
	172,566024780273	169,215606689453	172,926025390625	179,155654907226	160,789108276367	192,658447265625	178,605041503906
	,0578305721283	,12112763524056	,14373712241165	,17534680664539	,10505745559931	,12228358536959	,02718356437981
	,02088149450719	,06139296665788	,06947273761034	,07960296422243	,04568044096231	,05350615084171	,01403935346752
	,03567722439766	,05674993246794	,05324791371822	,05391730740666	,02985670790076	,02133038453758	,01963679865003
	,03831804171205	,04626613482833	,04650858417153	,06940817087889	,05606044083834	,04003744199872	,04265554621816
	,00523704104126	,04051354527473	,03978085890412	,03028594143689	,03859129548073	,03093314357102	,02876234985888
	,00438443385065	,00586599903181	,02486942522228	,04231012612581	,01858814246953	,01636609993875	,00847719796002
	,00580740673468	,03585574775934	,02950900606811	,03095474094152	,03095619753003	,04462422803044	,01222421694547
	,03398107737303	,02725046128035	,04885714501143	,03901639580727	,04185792431235	,03333063796163	,00948739796877

Figura 4 - Caratteristica: Descrittori ellittici di Fourier

5) La top signature considera il profilo superiore della firma e consente di confrontare l'altezza delle lettere della zona intermedia e l'altezza dei tratti di estensione verticale. La figura 5 mostra esempi di top signature estratti da firme vere.

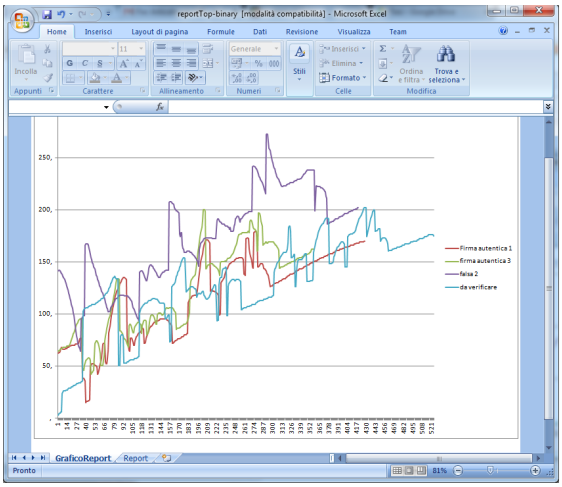


Figura 5 - Caratteristica: top-signatures

La figura 6 mostra un esempio di report prodotto dal sistema dopo l'estrazione di alcune caratteristiche dalle firme caricate.

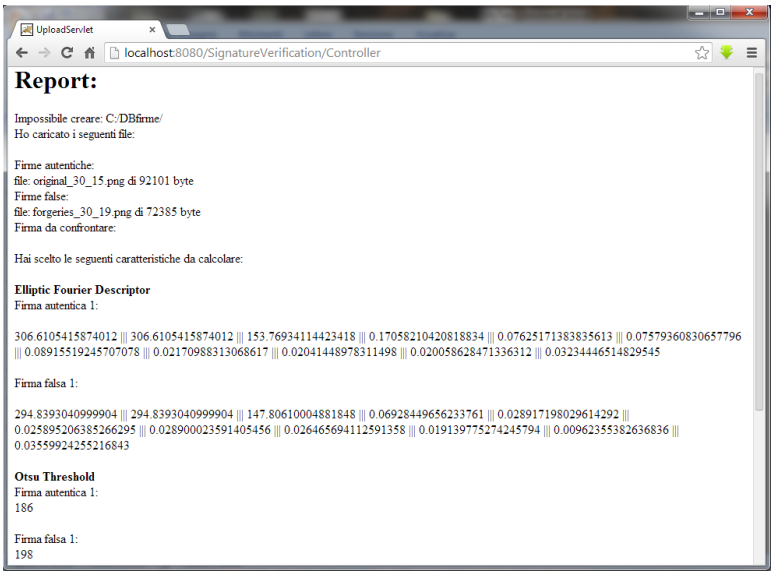


Figure 6 - SignVerify: esempio di report

Per testare il sistema si è utilizzato il dataset di immagini CEDAR, che contiene dati di firme autentiche e firme false. Il dataset è composto da campioni di firme prelevate da 55 persone, ove per ciascuno di essi si hanno 24 campioni autentici e 24 contraffatti, per un totale di 1.320 firme originali e 1.320 false. La figura 7 mostra il risultato del test ANOVA scegliendo 10 firme autentiche e 10 false. In rosso vengono mostrate le varianze tra le firme autentiche e tra le false per ciascuna delle 3 caratteristiche considerate.

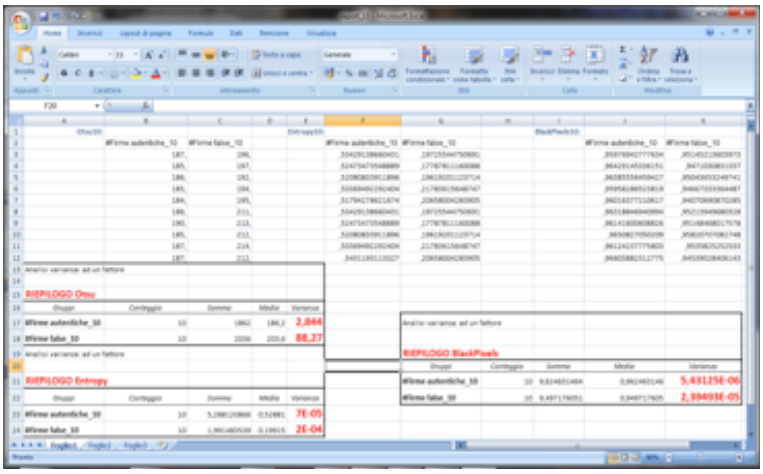


Figure 7 - Risultato del test ANOVA

I risultati ottenuti mostrano che le caratteristiche estratte sono molto utili per evidenziare contraffazioni nelle firme manoscritte. In particolare la pressione e la velocità nelle firme autentiche sono piuttosto stabili. Al contrario la varianza valutata sui campioni contraffatti risulta essere molto più elevata.

Conclusioni

Il sistema presentato in questo articolo, il SignVerify, è uno strumento informatico di analisi molto utile in ambito forense a supportare gli esperti in grafologia nel verificare se le firme, estratte da immagini di firme manoscritte, sono autentiche o contraffatte. Molte sono le ricerche tuttora in corso, sempre più basate su tecniche di intelligenza artificiale e di soft computing, finalizzate a rendere più affidabili tali supporti e consentire una loro maggiore integrazione in applicazioni combinate delle biometrie.

Bibliografia

S. A. Slyter, "Forensic Signature Examination", Charles C.Thomas Publisher, 1995.

E. Crotti, A. Magni, O. Venturini, "La perizia in tribunale, Manuale di consulenza grafotecnica", Franco Angeli ed., 2011.

E. Locard, "Les faux en écriture et leure expertise", Payot, Paris 1959.

B. Vettorazzo, "Grafologia Giudiziaria e perizia grafica", Giuffré editore, 1987.

A. Mucci (ed.), "L'indagine identificativa di scritture", I quaderni di Telèma, Feb. 2004, Media Duemilla.

J.L. Wayman, A.K. Jain, D. Maltoni, D. Maio, "Biometric Systems - Technology, Design and Performance Evaluation", Springer, 2005.

G. Pirlo G, D. Impedovo D, "Cosine Similarity for Analysis and Verification of Static Signatures", IET Biometrics, 2013, pp. 1-8.

D. Impedovo, G. Pirlo, L. Sarcinella, E. Stasolla, C.A.Trullo, "Analysis of Stability in Static Signatures using Cosine Similarity", in Proc. of XIII International Conference on Frontiers in Handwriting Recognition 2012., Los Alamitos, CA:IEEE Computer Society, Bari, Italy, Sept. 18-20, 2012, pp. 231-235,

G. Pirlo, C.A Trullo, D. Impedovo, "A feedback-based multi-classifier system. In: Proc. of th 10th Internationl Conference on Document Analysis and Recognition", Proc. ICDAR 2009, Los Alamitos, CA:IEEE Computer Society, Barcelona, Catalogna, Spain, July 26-29, 2009, pp. 713-717.

http://www.cedar.buffalo.edu/NIJ/publications.html, Signature dataset-CEDAR, University at Buffalo.

M. Nixon, A. Aguado, "Feature Extraction and Image Processing", 3nd Edition, Academic Press, 2012.

G. Pirlo, D. Impedovo, "Adaptive Membership Functions for Hand-Written Character Recognition by Voronoi-based Image Zoning", IEEE Transactions on Image Processing, 2012, vol. 21, pp. 3827-3837.

G. Pirlo, D. Impedovo, "The Verification of Static Signatures by Optical Flow Analysis", 2013, IEEE Transactions on Human-Machine Systems, 2013, Vol. 43, pp. 499-505.

N. Otsu, "A Threshold Selection Method from Gray Level Histogram", IEEE Trans. on Systems, Man and Cybernetics, 1979.

Biografia

Giuseppe Pirlo ha conseguito la Laurea con lode in Scienze dell'Informazione nel 1986 presso l'Università degli Studi di Bari, dove è attualmente professore associato di Sistemi di Elaborazione. E' impegnato in ricerche nei settori del pattern recognition, della biometria, dell'analisi automatica di documenti, dell'e-learning. Ha partecipato a numerosi progetti scientifici di ricerca ed ha pubblicato oltre 200 lavori scientifici. Giuseppe Pirlo è Associate Editor di IEEE Transactions on Human-Machine Systems e del Journal of e-Learning and Knowledge Society oltre ad essere revisore di numerose riviste tra cui IEEE T-PAMI, IEEE T-SMC, IEEE-IP, IEEE T-EC, PR, IJDAR, IPL e di molte conferenze Internazionali come ICPR, ICDAR, ICFHR e ICASSP. E' stato general co-chair di ICFHR 2012 e EAHSP 2013. Editore dello special issue "*Handwriting Recognition and other PR Applications*" della rivista Pattern Recognition, di "*Handwriting Biometrics*" della rivista IEE Biometrics Journal e dello special issue "Steps toward the Digital Agenda: Open Data to Open Knowledge" della rivista Je-LKS. E' editore del volume "Advances in Digital Handwritten Signature Processing", World Scientific, 2014. E' membro IAPR, GIRPR, SIEL, CINI e senior member IEEE.

Email: giuseppe.pirlo@uniba.it

Donato Impedovo ha ricevuto la Laurea con lode ed i Dottorato di Ricerca in Ingegneria Informatica rispettivamente nel 2005 e nel 2009. Impedovo è attualmente responsabile ricerca e sviluppo in DyrectaLab, laboratorio di ricerca accreditato MIUR. Le attività di ricerca si incentrano sui temi del signal processing e del pattern recognition con specifico riferimento ai tratti biometrici. Impedovo si occupa anche di trasferimento tecnologico in ambito IT. Su questi temi, Impedovo è co-autore di oltre 40 aticoli scientifici ed ha ricevuto "The Distinction for the best young student presentation" nel Maggio 2009 alla International Conference on Computer Recognition Systems (CORES – endorsed by IAPR), e l' "award for the Nereus-Euroavia Academic competition on GMES" nell'Ottobre 2012. Impedovo è revisore per Elsevier Pattern Recognition journal, IET Journal on Signal Processing, IET Journal on Image Processing e per molte conferenze Internazionali incluse ICPR e ICASSP. Impedovo è membro IAPR e IEEE.

Email: impedovo@gmail.com

Melisa Aruci ha conseguito la laurea con lode in Informatica presso l'Università degli Studi di Bari nel 2014, sviluppando un lavoro di tesi legato all'analisi di firme biometriche. Il suo settore di ricerca è quello dell'elaborazione di immagini e della biometria con particolare riferimento alle applicazioni legate all'ambito forense ed alla sanità. Attualmente lavora come software developer presso l' azienda AIRIS Solutions.

Email: aruci@uniba.it

Identificazione Personale Mediante Confronto di Volti

G. Mastronardi

Abstract. *L'identificazione del volto umano spesso richiede un approccio basato su diversi metodi di visione artificiale, in grado di risolvere passo dopo passo il problema del confronto tra soggetti ripresi e registrati in sequenze di immagini. Questi metodi consistono nell'identificare e misurare alcune caratteristiche del volto, generalmente strutture facciali antropometriche. In questo articolo, dopo la presentazione del problema e dei principali metodi di confronto per stimare gli indici di identificazione e la loro capacità di discriminazione, viene presentato un protocollo operativo fondamentale per ottenere in modo oggettivo le caratteristiche del volto tese al confronto tra un sospettato e un criminale di riferimento.*

Keywords: Identificazione personale, Analisi morfometrica, Confronto tra volti.

1. Introduzione

I sistemi di videosorveglianza, attualmente molto usati in ambienti pubblici e privati, consentono di memorizzare eventi criminosi su supporti informatici. Molto spesso l'Autorità Giudiziaria e le Forze dell'Ordine richiedono di identificare soggetti avventori di questi eventi mediante i loro tratti somatici e fisionomici. Il problema consiste solitamente nell'isolare un soggetto, appartenente a un gruppo di sospettati, che corrisponde al criminale ripreso, preferibilmente a volto scoperto. Questo processo di identificazione necessita di una coordinazione di competenze tecniche, volte a elaborare e analizzare le immagini registrate [1-5]. I frame più importanti, spesso sono affetti da scarsa qualità, e perciò vengono preliminarmente migliorati attraverso operazioni di esaltazione di livelli e contrasti (crispening e sharpening), ed espanse mediante operatori di ingrandimento con bassa perdita di definizione [6], avendo cura di evitare l'introduzione di artefatti. Le migliori immagini così ottenute permettono di passare alla fase successiva, che consiste nella loro sovrapposizione, tramite miscelazione video tra l'immagine selezionata e i soggetti sospettati, indagati o imputati, possibilmente ripresi dalla stessa telecamera nello stesso posto e nella stessa posizione occupata dal soggetto di riferimento (operazione di

"sovrapposizione parametrizzata") [7-15]. Le coppie di immagini, così ottenute e ingrandite in modo omogeneo, sono utili per le successive valutazioni comparative, che si basano in primis su caratteristiche individualizzanti come nei, cicatrici o altre alterazioni, e poi sulle proporzioni del volto andando a congiungere omologhi punti di rèpere, tra quelli non alterabili dalla mimica facciale (Fig.1).

Speciali algoritmi, fondamentalmente basati su tecniche di soft-computing (Hidden Markov Models, reti neurali e algoritmi genetici), consentono di riconoscere ed estrarre alcune strutture tipiche del volto (occhi, naso, bocca, arcate sopraccigliari, etc), ma il loro grado di approssimazione non consente di utilizzare questi elementi a fini identificativi in ambito forense. Per tale motivo risulta necessario estrarre i suddetti punti di rèpere mediante software che consentono una interazione grafica con i volti ripresi al fine di segnare con precisione tali punti sulle rispettive immagini, estraendone le relative coordinate spaziali. A seguito di tale operazione diventa essenziale, per una valutazione matematico-statistica, estrarre set omologhi di valori assoluti riferiti a distanze reciproche, perimetri e aree dei triangoli costruiti congiungendo tra loro i punti di rèpere precedentemente segnati. Vengono anche calcolati gli indici di compattezza [16-17] e i momenti di ordine superiore [18] come descrittori geometrici del volto, prendendo in dovuta considerazione le deformazioni di tali immagini, spesso determinate dai diversi formati proprietari di memorizzazione su supporti informatici [19].

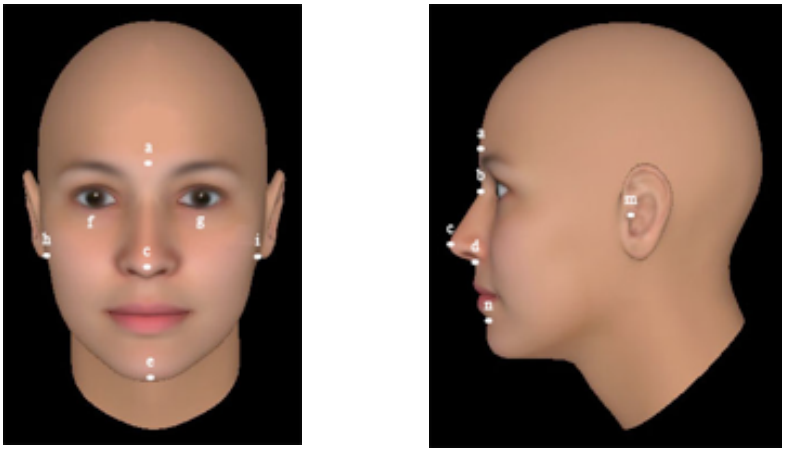


Figura 1 – Punti di rèpere: a) glabella, b) nasion, c) punta naso, d) pinna nasale, e) base mentoniera, f) e g) centro pupille; h) e i) attaccatura lobi; m) meato acustico interno; n) fossetta mentoniera

Questi set di valori consentono la valutazione di un rilevante test delle differenze, in modo tale da esprimere l'identificazione su base statistica. In questo lavoro sono mostrati i metodi numerici e statistici per ottenere i parametri sopra menzionati, con la soglia suggerita al di sopra della quale l'identificazione è altamente probabile.

2. Analisi morfometrica su nuvole di punti omologhi

L'analisi morfometrica effettuata sul confronto di nuvole di "punti omologhi", consente di ottenere risultati statistici meno affetti da errori di misura, determinati dalla soggettiva, seppure esperta, operazione di individuazione dei punti di rèpere. Si riportano di seguito le semplici espressioni matematiche che consentono di calcolare facilmente i set di valori per ciascuno parametro confrontato, quando tale analisi si basa su una campionatura costituita da omologhe nuvole di punti di rèpere.

Sia *n* il numero di punti di rèpere omologhi fissati nella coppia di immagini da analizzare; si ottiene:

$$s(n) = n \cdot (n\text{-}1)/2 \quad e \quad t(n) = t(n\text{-}1) + s(n\text{-}1) \qquad per\ n > 3 \quad con\ t(3) = 1$$

dove *s* e *t*, sono rispettivamente il numero di segmenti e di triangoli ottenibili dalla nuvola di punti individuati. In questo modo è possibile considerare la seguente tabella:

n.ro punti *n*	n.ro segmenti *s*	n.ro triangoli *t*
3	3	1
4	6	4
5	10	10
6	15	20
7	21	35

ove $t(n)=1+\Sigma_i(i)$ per $i = 3, ..., (n\text{-}1)$

Dunque, se x_i e y_i sono le generiche coordinate di un punto della nuvola, la lunghezza del segmento *d*, che connette i punti j e k, è così ottenuta:

$$d_{j,k} = \sqrt{(x_j\text{-}x_k)^2 + (y_j\text{-}y_k)^2}$$

Se i, j e k sono i punti di un generico triangolo, il perimetro *P* e l'area *A* sono così calcolati:

$$P_{i,j,k} = d_{i,j} + d_{j,k} + d_{k,i} \qquad \text{e} \qquad A_{i,j,k} = \frac{1}{2} \cdot Abs\begin{pmatrix} x_i & y_i & 1 \\ x_j & y_j & 1 \\ x_k & y_k & 1 \end{pmatrix}$$

Utile allo scopo è anche l'indice di compattezza *F*, cioè un fattore di forma che descrive l'irregolarità della figura geometrica rappresentata, così definibile:

$$Fi,j,k = Ai,j,k / Pi,j,k^2$$

Espresso preferibilmente con l'area al numeratore, per consentire il calcolo anche in presenza di triangoli degeneri, rappresentati dall'allineamento dei tre vertici, è questo un valore adimensionale che consente di considerare simili due triangoli della stessa forma, indipendentemente dalla loro grandezza, cioè in contesti con fattori di scala differenti.

In merito al modo di calcolare i momenti di ordine superiore, utilizziamo le seguenti formule, calcolando un numero di punti **n** interpolati dal perimetro di ciascun triangolo (da 100 a 500). Dalle coordinate di questi **n** punti calcoliamo le coordinate del baricentro:

$$barx = \frac{\sum_{i=1}^{n} px_i}{n} \qquad bary = \frac{\sum_{i=1}^{n} py_i}{n}$$

Per ciascun punto interpolato calcoliamo la distanza dal baricentro:

$$pd_i = \sqrt{(px_i - barx)^2 + (py_i - bary)^2}$$

Quindi, normalizziamo le distanze come segue:

$$pdn_i = \frac{pd_i}{max}$$

essendo $max = max_i\{pd_i\}$

e si calcola la distanza media **av** dei punti interpolati dal baricentro:

$$av = \frac{\sum_{i=1}^{n} pdn_i}{n}$$

Infine, calcoliamo il momento di ordine **z** per il triangolo selezionato:

$$mom_z = \frac{1}{n} \cdot \sum_{i=1}^{n} \left(pdn_i - av \right)^z$$

Per la valutazione della deviazione standard, per ogni set di parametri sopra menzionati, siano A e B due vettori di *n* componenti omologhi sottoposti a confronto, possiamo ottenere:

$$norma = \frac{1}{N} \cdot \sum_{i=1}^{N} \frac{|a_i - b_i|}{|a_i| + |b_i|} \qquad mediaA = \frac{1}{N} \cdot \sum_{i=1}^{N} a_i \qquad mediaB = \frac{1}{N} \cdot \sum_{i=1}^{N} b_i$$

$$stdevA = \sqrt{\left(\sum_{i=1}^{N} a_i^2 \right) - N \cdot mediaA^2} \qquad stdevB = \sqrt{\left(\sum_{i=1}^{N} b_i^2 \right) - N \cdot mediaB^2}$$

per ottenere, infine, il coefficiente di correlazione dei due vettori A e B:

$$corr = \frac{\left(\sum_{i=1}^{N} a_i \cdot b_i \right) - N \cdot mediaA \cdot mediaB}{stdevA \cdot stdevB}$$

Ora l'esperienza maturata con oltre 200 casi trattati dal 1989 a oggi, suggerisce di conferire particolare significato ai valori della correlazione, che se maggiori dell'80% possono rappresentare una bassa similarità, se maggiori del 90% possono rappresentare una media similarità, e se maggiori del 98% rappresentano un'alta similarità. Ma la sicura identità personale può essere espressa solo quando si ottengono i più alti valori di correlazione per tutti i set di parametri posti a confronto (distanze, perimetri, aree, fattori di forma, momenti).

3. Analisi morfometrica su nuvole di punti sparsi

Altro tipo di analisi morfometrica può essere effettuata confrontando nuvole di punti sparsi, cioè quando non tutti i punti delle due nuvole estratte sono corrispondenti a omologhi punti di rèpere, ovvero quando alcuni punti appartengono anche a differenti strutture del volto.

In questi casi si può fare riferimento alla GHT (Trasformata Generalizzata di Hough) [20-21] che attraverso il calcolo di una matrice di accumulazione (AM), può fornire un significativo indice di similarità, ottenuto dal valore del picco più alto rispetto alla somma dei valori presenti nella suddetta matrice. L'obiettivo di questo metodo è usare un algoritmo di matching in grado di fornire un indice di

similarità tra due nuvole di punti. Tale algoritmo è stato semplificato nel modo seguente: ogni punto è rappresentato da una coppia di coordinate, per ogni punto Pa del set A e per ogni punto Pb del set B si calcola la distanza tra Pa e Pb e si somma tale contributo nella matrice di accumulazione. Un picco isolato in AM rappresenta un alto grado di similarità (Fig.3a).

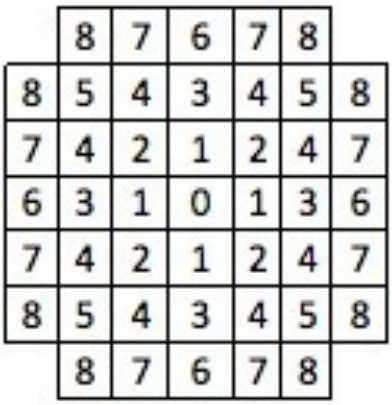


Figura 2 – Finestra di Roberts di ordine 8

Ovviamente, una minima imprecisione nel posizionamento di un punto in uno dei due insiemi può causare rumore nella valutazione, con un conseguente abbassamento del picco in AM. Per irrobustire l'algoritmo rispetto a tale rumore, la modalità di accumulo in AM è stata così modificata: al posto di sommare un singolo contributo alle coordinate calcolate, aggiungiamo il contributo riferito ad un'area del suo intorno, definita dall'utente, corrispondente ad una finestra di Roberts, che consente di scegliere il numero di punti interessati a fornire il loro contributo. L'area scelta per la finestra di Roberts (Fig.2) fornisce una misura della tolleranza al rumore; maggiore è la dimensione della finestra e maggiore è la tolleranza al rumore introdotta.

Una volta calcolata AM, viene estratto un indice di similitudine. Due identici punti nei due set producono un'AM con un valore di massimo assoluto al centro e vari massimi locali con valori più bassi. I massimi locali sono solitamente molto più piccoli del massimo assoluto, ma la differenza dipende dalla finestra di Roberts scelta per il processo di accumulazione. Differenze tra i due set, causano un decremento del valore di massimo assoluto e un incremento degli altri valori. Set di punti senza alcuna correlazione possono produrre anch'essi un massimo assoluto e massimi locali multipli di più alto valore (Fig. 3f). Questo comportamento viene sfruttato per estrarre un indice di similarità.

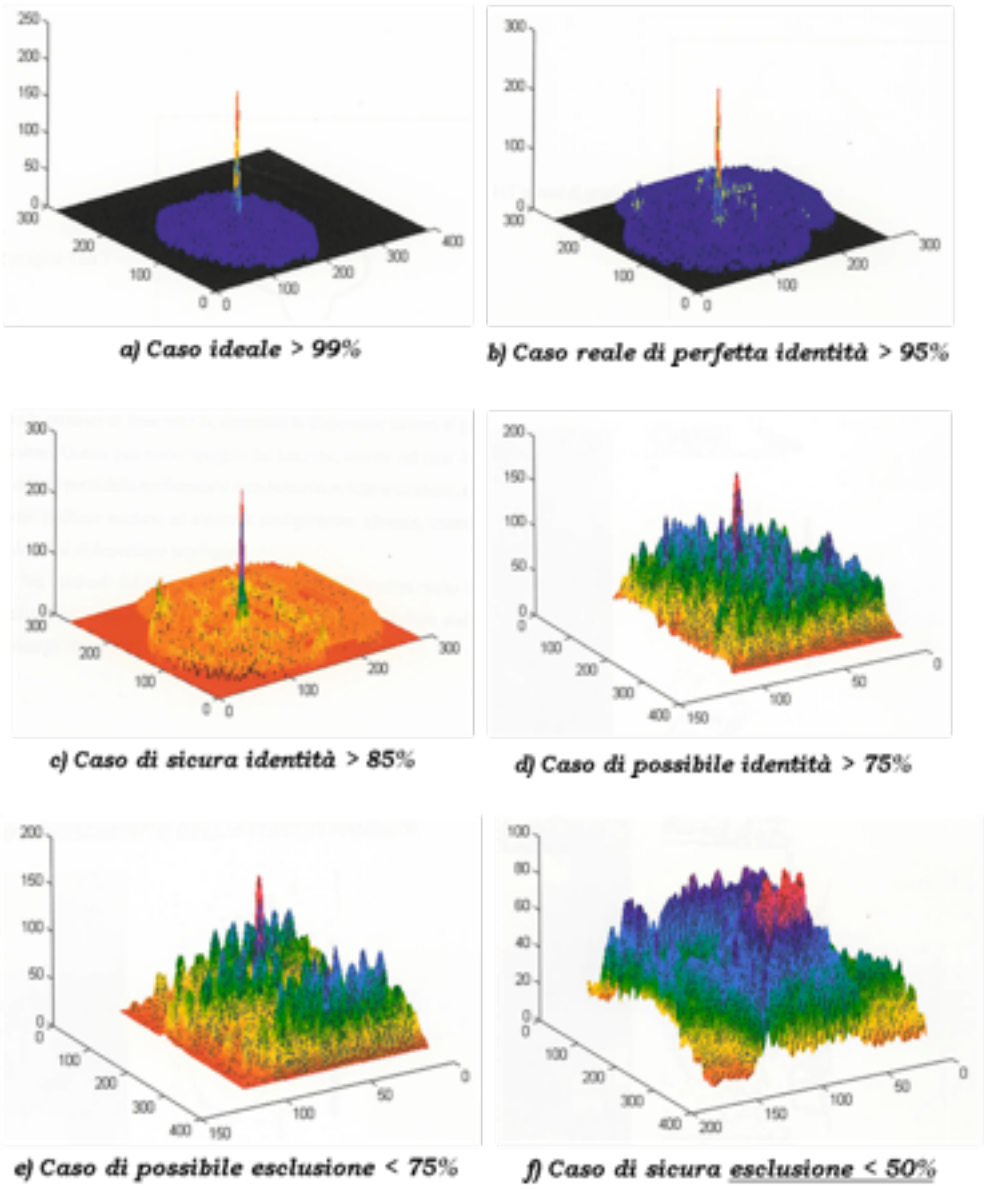


Figura 3 - Rappresentazione 3D della matrice di accumulazione della GHT

4. Analisi morfometrica monodimensionale

Il calcolo e il confronto dei parametri precedentemente menzionati, non sono sempre utili per fornire una robusta capacità di discriminazione. Alcuni metodi usati con successo nell'ambito dell'analisi fonica per il confronto di voci, possono essere impiegati anche per la caratterizzazione di pattern. L'idea di base è convertire, un generico bordo bidimensionale di un'immagine in un

segnale monodimensionale [22], in modo da applicare uno dei due seguenti metodi, considerati robusti e basati su:

1. coefficienti di autocorrelazione [23] o
2. coefficienti LPC (Linear Predictive Coding) [24].

Per il secondo metodo, da una sequenza di campioni estratti da un contorno bidimensionale di un'immagine, è possibile ottenere *m* coefficienti, cosicchè un generico campione *s* può essere rappresentato dalla combinazione lineare dei precedenti *m* campioni della stessa sequenza. Questi coefficienti sono molto utili come descrittori per distinguere le figure e sono anche in grado di ricostruire i bordi dai campioni. Ovviamente, questo metodo è molto dispendioso perché richiede una grande quantità di operazioni, essendo basato sulla soluzione di un sistema di equazioni lineari. Perciò, il primo metodo, quello basato sui coefficienti di autocorrelazione, può risultare più conveniente per il calcolo, ma in entrambi i casi, nella caratterizzazione del pattern, i descrittori ottenuti devono essere indipendenti dalla posizione, l'orientamento e la dimensione dell'oggetto nel frame.

Dunque, i bordi delle figure geometriche rappresentate da una sequenza di pixel contigui mediante coordinate bidimensionali (x_i,y_i), possono anche essere rappresentati come segnali mono-dimensionali. Infatti, ogni forma geometrica, regolare o irregolare, chiusa o aperta, ha un baricentro (X,Y) facilmente calcolabile, come riportato al paragrafo 2, quindi un profilo può essere rappresentato come una sequenza di campioni ottenuti calcolando le distanze d_i di ogni pixel del bordo dal baricentro.

Per le forme geometriche chiuse, per ottenere un vettore distanza indipendente dal punto di inizio dell'acquisizione, come primo punto della sequenza circolare si assume per esempio quello con la più piccola distanza dal baricentro.

Per sopprimere l'ambiguità dell'orientamento dell'acquisizione, oraria o antioraria, vengono considerate entrambe le sequenze. In questo modo due vettori ordinati di distanze punto-baricentro, ottenute andando dalla distanza più piccola in senso orario e viceversa, vanno a rappresentare la forma da testare.

Per entrambi i sopracitati vettori di distanza viene effettuata un'operazione di interpolazione così che le due funzioni di interpolazione vengono ottenute e poi campionate, in modo da rappresentare i due pattern paragonati con lo stesso numero di campioni.

Inoltre, se richiesto, è possibile sottrarre il valore della più piccola distanza da ogni campione ottenendo una prima normalizzazione rispetto alla dimensione minima, corrispondente alla eliminazione del segnale continuo (offset); rapportando i singoli campioni con la nuova distanza massima, è possibile ottenere la completa normalizzazione, potendo così operare con valori di distanza minori dell'unità, e ottenere dimensioni indipendenti dalla grandezza, o fattori di scala, delle forme oggetto di confrontato.

Mediante uno dei due metodi succitati, possiamo ottenere due vettori di coefficienti A1 e A2 per la forma geometrica A e i vettori B1 e B2 per la forma

geometrica B. Quindi, si confrontano A1 con B1 e B2 e A2 con B1 e B2. Per la finale operazione di confronto si calcola il vettore d'errore E costituita dai seguenti elementi:

$$E(i) = abs(a(i) - b(i)) / (abs(a(i)) + abs(b(i))) \qquad (i = 1, \ldots, N)$$

poi, come indice discriminatore possiamo calcolare uno dei seguenti parametri:

$$Norma_1 = \Sigma_i abs(E(i)) / N < 1 \qquad (i = 1, \ldots, N)$$

$$Norma_2 = \Sigma_i E(i)^2 / N < 1 \qquad (i = 1, \ldots, N)$$

essendo N il numero di coefficienti derivati dai valori ricampionati. Naturalmente un indice più basso rappresenta una più alta similarità tra le forme paragonate. Il valore norma può, quindi, generare la probabilità di similarità P (in percentuale):

$$P = (1 - Norma) \cdot 100$$

questo consente di identificare alcuni soggetti tra quelli confrontati, in modo analogo a quanto già esposto nel paragrafo 2.

5. Conclusioni

Le formule impiegate per l'analisi morfometrica, sono state descritte in dettaglio insieme alle funzioni sviluppate e implementate in un software chiamato SISCA (Shape Investigation System by Combined Analysis) [25], il cui uso in molti casi è stato consigliato negli ultimi dieci anni in Italia dall'Autorità Giudiziaria e dalle Forze dell'Ordine.

I metodi e il protocollo operativo presentati, opportunamente impiegati, consentono di raggiungere indici di similarità in grado di distinguere le caratteristiche somato-fisiche e fisionomiche dei soggetti rappresentati in sequenze di immagini, in modo da ottenere una oggettiva identificazione o una sicura esclusione. Naturalmente, si è consci che soltanto una continua sperimentazione può fornire giusti miglioramenti a questi metodi e più opportune interpretazioni ai relativi risultati.

Bibliografia

[1] Jain, A., Bolle, R. and Pankanti, *S., Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1999*

[2] Zhang, D., *Automated Biometrics: Technologies and Systems. Kluwer Academic Publishers*, Dordrecht, The Netherlands, 2000

[3] Scherbakov V.V., Shkolnikov B.V., Moiseenko S.A., Bessarabov I.I.: *Method and algorithm for comparing feature point models of the skull and life time photographs in flow data processing*. 10th International Meeting on Forensic medicine. Alpe Adria Pannonia. Opatija, Croatia, 2001, pp. 83-91

[4] Kresimir, D.I , Mislav, G., *A Survey of Biometric Recognition Methods, In: 46th International SyrnPoSium Electronics in Marine (ELMAR), Zadar, Croatia, 2004*

[5] Balossino N., Siracusa S.: *Parametri discriminatori nel riconoscimento di volti*: Inserto a Polizia Moderna, 1998, pp. 1-18

[6] Mastronardi G., Marino F.*: Quality Enhancement in Image Enlargement. Lecture Note in Computer Science n. 974: Image Analysis and Processing, Springer Ed., sviluppato nell'ambito del Progetto Finalizzato CNR "Sistemi Informatici e Calcolo Parallelo" (report n. 1/167)", 1995*

[7] Introna F. jr, Mastronardi G., La Sala L.: *Identificazione personale di soggetti viventi mediante elaborazione elettronica e confronto computerizzato delle immagini registrate su supporto magnetico (videotapes)*. Rivista Italiana di Medicina Legale XIV, 1992, 517-518

[8] Introna F. jr, Mastronardi G.*, La Sala L.: L'analisi elettronica delle immagini applicata alla identificazione personale. IX Congresso Nazionale della Società Italiana di Criminologia, Modena 13 -15 Aprile 1992*

[9] Introna F. jr, La Sala L., Mastronardi G.*: Identificazione personale mediante confronto computerizzato di immagini registrate su supporto magnetico (videotapes). Corso di Aggiornamento sulle tecniche di indagine, Quaderni del Consiglio Superiore della Magistratura IV Supp. Vol. V, 1993, pp. 84-94*

[10] Introna F. jr, Mastronardi G.: *On human face identification methods. MELECON '96, 8th Mediterranean Electrotechnical Conference. Industrial Application in Power System. Computer Science and Telecommunications. Proceeding Vol. 2, 1996, pp.1101-1103*

[11] Introna F. jr, Mastronardi G., Di Vella G.: *L'identificazione di autori di rapine in banca mediante analisi morfometrica di immagini registrate su supporto magnetico (videotape)*: Esperienza su 39 casi. Medicina legale, quaderni Camerti XX, 1, 1998, pp. 91-99

[12] Introna F. jr, Mastronardi G.: *Identificazione di autori di rapine in banca mediante analisi morfometrica di immagini registrate su supporto magnetico (videotape): Tecnica di indagine*. Medicina legale, quaderni Camerti XX, 1, 1998, pp. 101-112

[13] Introna F. jr, Mastronardi G., Saltarelli G., Giardino N.: *Analisi metrica a fini identificativi del volto umano in proiezione frontale*. Medicina legale, quaderni Camerti XX, 1, 1998, pp. 113-122

[14] Introna F. jr: *Identificazione personale attraverso le tecniche di analisi e sovrapposizione delle immagini*. Trattato di Medicina legale e scienze affini. Giusto Giusti Ed. Vol. II, CEDAM Ed. 1998

[15] Introna F., Mastronardi G., De Donno A.: *Identificazione personale mediante analisi di immagini. Cap. XXXVII in Barbagallo "Le Prove", UTET - Collana "Il diritto Privato nella Giustizia" a cura di P. Cendon, Vol. II, Ed. Wolters Kluver Italia Giuridica, 2007, pp. 1039-1069*

[16] Arlotti. M.A.: *Robot verso il futuro. F. Angeli Ed., Milano, 1992*

[17] Mastronardi G., Introna F.: *Compactness Descriptors for human face 2D-morphometric analysis. In: Proceedings of XII IASTED International Conference on "Applied Informatics", Annecy (France) 17-20 Maggio, 1994*

[18] Marino F., Mastronardi G.: *Classificazione e Identificazione di Pattern Mediante Momenti di Ordini Superiori. II Congresso Nazionale SIMAI (Società Italiana di Matematica Applicata e Industriale), Capri (Italy), June 1994, pp. 430-432*

[19] Mastronardi G., Introna F., Dellisanti Fabiano M., Venosa A.: *Personal Identification of Bank Robbers by Morphometric Image Analysis – An Italian Experience. In: Proceedings of 3.rd IASTED International Conference on "Law and Technology", November 6-7, 2002, Cambridge (Massachusset), USA, pp.108-111*

[20] Ballard, D.H., *Generalizing the Hough Transform to detect arbitrary shapes,* In: Pattern Recognition, Vol. 13, 1981, pp. 111-122

[21] Mastronardi, G., Daleno, D., Bevilacqua, V., Chiaia, G., *2007, Tecniche di identificazione personale basate sulla trasformata generalizzata di Hough applicata a nuvole di punti, In: Proceedings of National Conf. AICA 2007 (Associazione italiana per l'Informatica ed il Calcolo Automatico), Milano (Italy), ISBN 88-901620-3-1.*

[22] Mastronardi G., Introna F.: *Un metodo di identificazione personale basato sull'analisi dei contorni*. Atti Congresso AICA Palermo 21-23 settembre 1994, pp. 1215-1221

[23] Oppenheim A.V., Schafer R.W.: *"Digital Signal Processing", Prentice-Hall, 1975*

[24] Markel J.D., Gray A.H.: *"Linear Prediction of Speech", Springer-Verlag, 1976*

[25] SISCA, Software by eBIS srl, Spin-Off del Politecnico di Bari, 2011

Biografia

Giuseppe Mastronardi è nato nel 1949 a Bari, è laureato in Scienze dell'Informazione all'Università degli Studi di Bari ed è professore ordinario di Sistemi di Elaborazione delle Informazioni al Politecnico di Bari dove insegna Informatica Medica e Sicurezza Informatica nei corsi di Laurea Magistrale in Ingegneria Elettronica e Ingegneria Informatica. Ha pubblicato oltre 120 lavori scientifici su analisi ed elaborazione di segnali e immagini e collabora con comitati di convegni, redazione di riviste e collane di informatica. Ha partecipato a numerosi progetti europei, nazionali e regionali occupandosi di tecnologie per il controllo sicuro degli accessi di persone e mezzi, mettendo a punto alcuni brevetti. Si occupa di tecniche biometriche mettendo a disposizione di Tribunali e Procure, già dal 1978, la sua esperienza acquisita nel confronto di voci e volti assistito da computer, per accertamenti peritali connessi alle intercettazioni telefoniche e alle videoregistrazioni di atti criminosi. Ha costituito nel 2007 la eBIS srl, spin-off universitaria, finalizzata allo sviluppo di soluzioni innovative per l'identificazione personale e applicazioni biomedicali. Per conto dell'AICA, di cui è attualmente Vice Presidente, ha costituito la sezione territoriale AICA-Puglia.

Email: giuseppe.mastronardi@poliba.it

Un metodo di Identificazione Basato sulla Ricostruzione 3D del Padiglione Auricolare

N. Balossino, M. Lucenteforte, L. Piovano, S. Rabellino

Abstract. *La morfologia dell'orecchio varia notevolmente a fronte di rotazioni attorno all'asse corporeo. Il confronto presuppone che le immagini del segmento anatomico siano ottenute come proiezioni di configurazioni spaziali il più possibile aderenti fra loro. E' opportuno pertanto disporre di una ricostruzione tridimensionale da orientare opportunamente; si possono così condurre confronti con immagini di videosorveglianza. Nell'articolo è illustrato il metodo sviluppato dagli autori per la sintesi di orecchi mediante un metodo di mesh morphing.*

Keywords: Forensic identification, Surveillance, Ear biometrics

1. Introduzione

Una consistente serie di studi condotti sulla morfometria del padiglione dell'orecchio ha evidenziato come nel procedimento identificativo questo segmento anatomico possegga, alla stessa stregua delle impronte digitali, requisiti di connotato saliente. Studi di maggior rilievo condotti sull'orecchio sono di Alfred Iannarelli, capo della polizia di un campus universitario ad Hayward. Iannarelli analizzò, nell'arco di alcuni anni ad iniziare dal 1989, oltre 10.000 morfometrie di orecchi e constatò come non ce ne fossero due identiche nemmeno in gemelli monozigoti.

Le ricerche hanno inoltre evidenziato che l'orecchio dopo il quarto mese di vita assume una morfologia che rimane praticamente immutata nel tempo e non subisce alcuna influenza a fronte della variazione dell'espressione facciale. Una leggera variazione della lunghezza del lobo può avvenire per effetto della forza di gravità (si trascurano agenti esterni come orecchini) ma si tratta comunque di variazioni di contenute dimensioni che rimangono tali fino a età avanzata. Nei primi otto anni di vita e dopo i 70 anni la variazione in lunghezza assume valori più elevati rispetto agli altri periodi della vita.

È facile notare come l'orecchio presenti maggior difficoltà descrittiva rispetto al volto. Vi sono infatti numerosi aggettivi che sono usati per descrivere le

caratteristiche salienti di un volto e pochi per l'orecchio. Come abitudine consolidata infatti, si pone maggior attenzione agli aspetti fisionomici del volto di una persona, per poi riconoscerli, mentre si presta ben poca attenzione all'orecchio.

Tenendo in considerazione che le fotografie segnaletiche ritraggono i soggetti nella visione frontale e di profilo destro, l'orecchio destro è generalmente usato come riferimento nel riconoscimento. Occorre però osservare che non si può escludere la variabilità intra-personale, per la quale l'orecchio destro sia diverso da quello sinistro. E' quindi opportuno nei casi di confronto di immagini di videosorveglianza per scopi identificativi non basarsi su trasformazioni di simmetria per recuperare una postura non rilevabile nei dati a disposizione.

Un esempio di utilizzo dell'orecchio per la discriminazione tra soggetti si riferisce a soggetti gemelli per i quali sia stata evidenziata la compatibilità fisionomica e metrica del volto. In questo modo, la constatazione della diversa morfologia dei due orecchi permette una discriminazione effettiva tra i soggetti.

Poiché nel procedimento identificativo si utilizzano immagini di videosorveglianza oppure di OCP (Osservazione, Controllo, Pedinamento) è necessario porre attenzione al fatto che la valutazione dell'aspetto morfologico dell'orecchio è influenzata da variazioni di illuminazione e di postura. Per quanto riguarda la postura, la rotazione del capo attorno all'asse verticale corporeo fornisce all'osservatore rappresentazioni dell'orecchio molto diverse (Fig. 1).

Figura 1

Ne consegue che per condurre una comparazione significativa fra due soggetti è necessario che le immagini siano confrontabili, cioè rappresentino i soggetti in posture molto aderenti e inoltre le immagini siano di buona qualità. Per quanto riguarda le posture può capitare che queste differiscano notevolmente. Disponendo allora del soggetto sotto indagine, si possono acquisire immagini mirate che ricalchino quelle presenti nella videosorveglianza al fine di operare il confronto. Nel caso in cui ciò non sia possibile, si può ipotizzare di disporre di immagini di foto-segnalamento e procedere alla ricostruzione 3D del capo del soggetto, e dell'orecchio, e poi ruotare nello spazio la ricostruzione, ottenendo l'opportuna rappresentazione bidimensionale utile per il confronto.

2. Il metodo proposto

Esistono in commercio software per le ricostruzione tridimensionale di un volto a partire dalla definizione di un insieme di punti di repere detti Facial Definition Point (FDP). Selezionato un modello tridimensionale di partenza, fra quelli disponibili in un data-base, si posizionano su questo un certo numero di punti di repere; il sistema, sulla base delle informazioni fornite dalle fotografie 2D frontali e laterali, adatta sia la metrica del volto sia le caratteristiche fisionomiche mediante tecniche di mesh-morphing. È da notare però che in generale tali strumenti non si occupano della ricostruzione dell'orecchio.

La ricostruzione dell'orecchio sviluppata si basa su due fotografie dell'orecchio (una frontale e una laterale) e sull'utilizzo di particolari funzioni di interpolazione note come Radial Basic Function (RBF). Queste funzioni di interpolazione sono molto efficaci nei casi in cui si disponga di una serie di punti distribuiti nello spazio in maniera non regolare (scattered data) come avviene scegliendo punti di repere sulle fotografie di riferimento. Le RBF, nel caso specifico, permettono la generazione di superfici 3D fedeli alla realtà a partire da una nuvola di punti acquisita e da una mesh generica (template). Il posizionamento dei punti di repere è demandato all'operatore per cui il procedimento di ricostruzione è del tipo semi-automatico.

Il procedimento di ricostruzione si basa sui seguenti passi:

1. Allineamento delle immagini per la vista frontale e laterale: questa fase prevede l'inserimento e l'allineamento di 2 diverse fotografie (viste 2D) all'interno di un software di modellazione tridimensionale. Si ottiene lo scopo creando due piani fra loro ortogonali sui quali vengono mappate le immagini dell'orecchio del soggetto nella visione frontale e laterale. Si noti che per ottenere un risultato significativo nella ricostruzione tridimensionale, occorre che i particolari del segmento anatomico siano allineati così da mantenere le giuste proporzioni, garantendo in questo modo un'esatta corrispondenza tra le viste. La Fig. 2 illustra l'allineamento fra la vista frontale e quella laterale destra di un soggetto.

Figura 2

2. Inserimento di punti di repere sulle viste 2D, mediante l'individuazione di alcuni marker caratteristici sulle diverse parti anatomiche dell'orecchio. L'inserimento viene eseguito operando sia sulla vista frontale sia su quella laterale. L'inserimento dei punti di repere dà luogo a una nuvola di punti. A titolo di esempio in Fig. 3 sono evidenziati quelli della visione laterale.

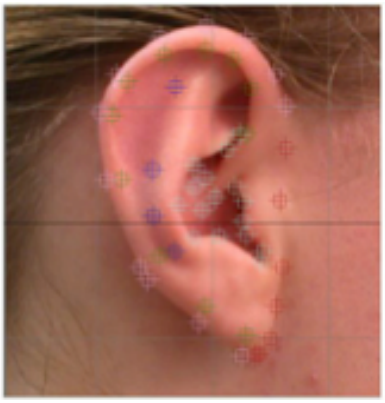


Figura 3

3. Scelta di un modello 3D (template) che approssimi sufficientemente bene, dal punto di vista visivo, l'orecchio che si intende ricostruire. La Fig. 4 riporta la scelta del modello di base dell'orecchio di Fig.3.

Figura 4

4. Scelta e utilizzo della RBF per l'algoritmo di fitting, al fine di adattare il modello 3D ai punti di repere caratteristici definiti nel punto 2. Tali punti sul modello 3D sono così traslati nelle stesse coordinate dei corrispondenti indicati nel passo 2. A tutti gli altri punti del modello 3D dovrà essere applicata una interpolazione e una traslazione coerente con lo spostamento legato ai punti di repere; ciò al fine di ottenere un nuovo modello 3D che si adatti al meglio alle proiezioni 2D delle due viste fotografiche. Per queste elaborazioni si utilizza un opportuno ambiente di calcolo numerico e di visualizzazione. Le sperimentazioni hanno evidenziato che i migliori risultati si ottengono utilizzando come RBF una funzione gaussiana.

5. Per garantire maggior realismo scenico ed enfatizzare l'aspetto di illuminazione e contrasto, alla mesh viene applicata una tessitura (texture), ricavata dalle immagini del soggetto. Questo è ottenuto utilizzando ancora un ambiente di modellazione 3D che offra strumenti per mappare le coordinate u,v,w delle texture nelle corrispondenti coordinate del modello x,y,z. Il risultato è un modello tridimensionale estremamente somigliante alle immagini 2D utilizzate (Fig. 5) .

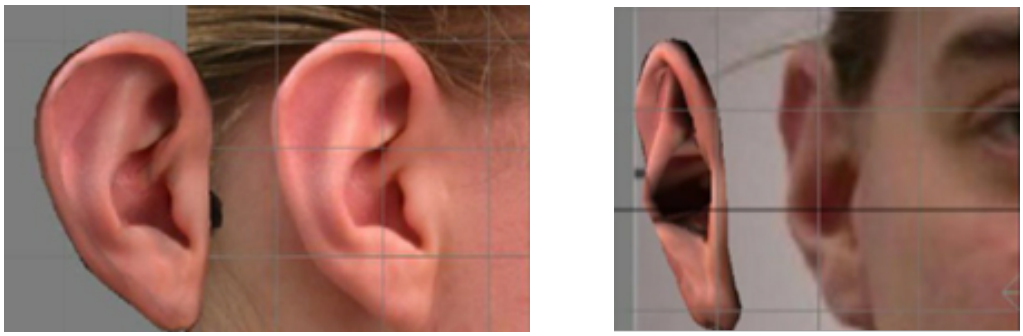


Figura 5

Il modello 3D ottenuto può eventualmente essere combinato con il modello 3D del volto e ruotato in una postura compatibile con quella ricavata dalle immagini di videosorveglianza, rendendo significativo il confronto per formulare un giudizio identificativo. (Fig. 6).

Figura 6

3. Conclusioni e prospettive

La ricostruzione tridimensionale dell'orecchio permette di ottenere immagini confrontabili con quelle di videosorveglianza; è così possibile esprimere, con un maggior livello di confidenza, un giudizio di compatibilità tra l'autore del crimine e l'indagato. La ricostruzione dell'orecchio e il suo eventuale inserimento nel modello 3D del capo fornisce infatti la possibilità di effettuare confronti fisionomici più accurati ed eventualmente di procedere a valutazioni metriche con indici e/o mappe dell'orecchio.

La metodologia proposta richiede un intervento non trascurabile dell'operatore, ma restituisce risultati qualitativamente aderenti alla realtà utili per la verifica o l'attribuzione di identità in ambito forense. Il sistema può essere migliorato per renderlo più facile nell'utilizzo e per fornire funzioni metriche che forniscano una valutazione oggettiva della fedeltà dei modelli 3D ottenuti.

Bibliografia

[1] Iannarelli A., Ear identification , Forensic identification series, Paramont Publishing Company, Fremont, California, 1989.

[2] Farkas L. G., Antropometry of the head and face, Raven Press,1994

[3] Howell Evens J., The external ear as a means of Identification, Transaction of the Medico Legal Society, 1910

[4] Hogstrate A.J., Van den Heuvel, H., Huyben, E., Ear identification based on surveillance camera's images, Netherlands Forensic Institute, 2000

[5] Burger M. and Burger W., Ear biometrics, Biometrics: Personal Identification in Networked Society, ed. Jain A. et al., Kluwer Academic Publishers, 1998.

[6] Bhan B. and Chen H., Human ear recognition by computer, Springer-Verlag, 2008

[7] Balossino N., Lucenteforte M., Siracusa S., Analisi biometria dell'orecchio in ambito forense, Nuove Tecnologie in Medicina, Anno 6, N.1-2, Sirse s.r.l. Editore, 2006.

[8] Furneri F., Sviluppo di metodologie per la ricostruzione 3D del padiglione auricolare mediante funzioni radiali, Tesi di Laurea, Corsi di Studi in Informatica, Università di Torino, AA 2007/2008.

Biografie

Nello Balossino è professore associato presso il Dipartimento di Informatica l'Università degli Studi di Torino. E' co-titolare dei corsi di Elaborazione di Immagini e Visione Artificiale, Modellazione Grafica e Sistemi di Realtà Virtuale presso il corso di laurea in Laurea Magistrale in Realtà Virtuale e Multimedialità. E' docente di Metodi di Identificazione Automatica presso la Scuola di Specialità di Medicina Legale di Torino e di Informatica Investigativa per laurea magistrale in Psicologia Criminologica e Forense dell' Ateneo torinese. Sviluppa ricerche nelle aree di - elaborazione di immagini e riconoscimento di forme applicate alla medicina, alle scienze forense e ai beni culturali; - analisi e realizzazione di moduli prototipali di realtà virtuale applicati all'astronomia, al ricupero riabilitativo, alla didattica, ad ambienti extraterrestri; - procedure per l'attribuzione di identità a soggetti non noti, indiziati come colpevoli di reati.
Collabora con la magistratura come consulente.

Email: nello.balossino@unito.it

Maurizio Lucenteforte è ricercatore presso il Dipartimento di Informatica dell'Università degli Studi di Torino. È titolare di insegnamenti tenuti nel corso di Laurea in Informatica di primo livello e in quello magistrale di Sistemi di Realtà Virtuale e Multimedialità, di cui è co-responsabile di indirizzo. I suoi interessi di ricerca comprendono tematiche di trattamento di immagini, visione artificiale ed elaborazione di dati 3D.

Email: maurizio.lucenteforte@unito.it

Luca Piovano è ricercatore presso CeDint, Università Politecnica di Madrid. I suoi interessi di ricerca riguardano principalmente l'analisi e la rappresentazione di informazioni sia in 2D che in 3D. Ha conseguito il dottorato in Informatica presso l'Università degli Studi di Torino nel 2008, nell'ambito di un programma di ricerca congiunto con l'Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni (IEIIT) del Consiglio Nazionale delle Ricerche (CNR). Ha inoltre lavorato presso Thales Alenia Space Italia, dove ha svolto ricerche nel campo della visione artificiale, con speciale attenzione alle applicazioni di realtà virtuale ed alla rappresentazione 3D di ambienti extra-terrestri.

Email: lpiovano@cedint.upm.es

Sergio Rabellino, laureato in Realtà Virtuale e Multimedialità presso l'Università di Torino , è responsabile dei Servizi ICT del Dipartimento di Informatica della stessa Università, dove coopera con i gruppi di ricerca in Eidomatica ed E-Learning. Specializzato nella integrazione di sistemi, coordina la gestione dei Laboratori Informatici dei Corsi di Laurea in informatica e di diverse piattaforme di elearning.

Email: sergio.rabellino@unito.

Riconoscimento dell'Iride in Condizioni Critiche

M. De Marsico, C. Galdi, M. Nappi, D. Riccio, G. Mastronardi

Abstract. *I sistemi biometrici sono in grado di fornire un livello di sicurezza più elevato rispetto ad altri sistemi di autenticazione basati su password o schede, ma esistono alcuni problemi legati alle caratteristiche della biometria stessa (alcune cambiano nel tempo in modo significativo) o ai dispositivi utilizzati per catturarle (alcuni possono essere indotti in errore o possono avere difficoltà ad acquisire il tratto biometrico) che scoraggiano la loro diffusione. Le biometrie più utilizzate per il riconoscimento automatico di persone sono le impronte digitali e i tratti somatici. Il primo è altamente affidabile ma oneroso dal punto di vista computazionale, mentre il secondo richiede un settaggio ben controllato. Vedremo che l'iride si presta molto meglio di altri dati biometrici per l'identificazione certa, ma che le applicazioni presenti sul mercato fino ad oggi sono state limitate dalla necessità di acquisire l'iride a distanza ravvicinata e con una pur minima cooperazione da parte dell'utente. Per questo motivo, la ricerca sta indagando recentemente sull'uso di sistemi di riconoscimento dell'iride, anche in condizioni critiche, al fine di sviluppare sistemi affidabili in grado di acquisire l'iride a distanza e con poca collaborazione da parte dell'utente, e rendere questo strumento maggiormente utilizzabile nell'ambito della tracciabilità di individui segnalati.*

Keywords: Personal identification, Morphometric analysis, Comparison between faces

1. Panoramica del processo di autenticazione

L'autenticazione può essere eseguita sulla base di uno dei seguenti elementi o su una loro combinazione:

- qualcosa che l'utente conosce (ad esempio, password, numero di identificazione personale (PIN), risposta segreta, pattern);
- qualcosa che l'utente ha (ad esempio, smart-card, carta d'identità, token di sicurezza, token-software, telefono o cellulare);
- qualcosa che l'utente è o fa (ad esempio impronte digitali, volto, andatura).

Gli ultimi sono noti come dati biometrici e verranno discussi in dettaglio più avanti. Per ora vogliamo analizzare brevemente il livello di sicurezza associato a ciascun tipo di elemento di autenticazione o anche di combinazioni.

Come premessa, vale la pena considerare che le password possono essere dimenticate o sottratte da malintenzionati, gli oggetti fisici come distintivi e documenti di identità possono essere persi o rubati, mentre la caratteristiche biometriche difficilmente possono essere rubati e anche il processo di falsificazione è molto più complicata (es chirurgia plastica).

Se consideriamo tutte le possibili combinazioni dei tre fattori di autenticazione, si ottiene la seguente graduatoria, dalla sicurezza più bassa alla più alta:

1. Qualcosa che l'utente conosce;
2. Qualcosa che l'utente ha;
3. Qualcosa che l'utente conosce + qualcosa che l'utente ha (ad esempio, bancomat + PIN);
4. Qualcosa che l'utente è o fa;
5. Qualcosa che l'utente ha + qualcosa che l'utente è o fa (ad esempio passaporto biometrico);
6. Qualcosa che l'utente conosce + qualcosa che l'utente è o fa;
7. Qualcosa che l'utente conosce + qualcosa che l'utente ha + qualcosa che l'utente è o fa.

La Figura 1 mostra i gradi relativi di sicurezza.

Figura 1 - Livelli di sicurezza
(1) qualcosa che l'utente conosce; (2) Qualcosa l'utente ha;
(3) qualcosa che l'utente conosce + qualcosa che l'utente ha; (4) qualcosa che l'utente è o fa;
(5) Qualcosa l'utente ha + qualcosa che l'utente è o fa; (6) qualcosa che l'utente conosce + qualcosa che l'utente è o fa;
(7) qualcosa che l'utente conosce + qualcosa che l'utente ha + qualcosa che l'utente è o fa

La Biometria, quindi, aiuta a garantire un adeguato livello di sicurezza che può essere anche aumentato attraverso la combinazione con altri fattori (riconoscimento multimodale).

2. Panoramica del riconoscimento biometrico

L'autenticazione biometrica è il processo di identificazione umana attraverso le loro caratteristiche fisiologiche o comportamentali. Queste caratteristiche devono essere distintive e misurabili per eseguire il riconoscimento.

Il riconoscimento può essere eseguito in modalità di verifica (corrispondenza 1:1, quando il soggetto afferma un'identità che deve essere verificata), o in modalità identificazione (corrispondenza 1:N, cioè uno contro tutti, quando non c'è rivendicazione preliminare e il sistema deve restituire l'identità del soggetto analizzato). Le biometrie fisiologiche includono impronte digitali, caratteristiche del volto, geometria della mano, DNA, tracciato delle vene, padiglione auricolare, iride e fondo retinico.

Le biometrie comportamentali sono legate al particolare comportamento di una persona e possono essere influenzate dal proprio stato d'animo che includono la firma e il modo di firmare, la parola e il modo di parlare, la velocità di battitura su una tastiera, la postura e l'andatura. Una buona biometria deve soddisfare le seguenti caratteristiche: unicità, permanenza, facilità di utilizzo, buone prestazioni, precisione, basso costo, percezione pubblica positiva. L'iride le soddisfa in modo ottimale quasi tutte.

Unicità: la forma complessa dell'iride può contenere molti elementi distintivi come legamenti arcuati, solchi, creste, cripte, anelli, corona, lentiggini e un collaretto zigzag. E' dimostrato statisticamente che l'iride è più precisa persino del riconoscimento tramite DNA, considerato che la probabilità che due iridi siano identiche è di 1 su 10^{78}.

Permanenza: l'iride comincia a formarsi nel terzo mese di gestazione e le strutture che creano la sua forma sono in gran parte completate entro l'ottavo mese, anche se l'accrescimento del pigmento può continuare nei primi anni dopo la nascita. Poi rimane quasi invariata per tutta la vita. La sua posizione dietro la cornea la protegge dall'ambiente.

***Facilità di utilizzo*:** l'iride è esternamente visibile e il rilevamento automatico degli occhi è un'operazione relativamente semplice.

Prestazioni: il modello ottenuto dall'iride è piccolo e l'estrazione delle caratteristiche e la corrispondenza sull'iride sono operazioni molto veloci.

Precisione: l'iride ha il grande vantaggio matematico che la variabilità del suo modello tra persone diverse è enorme.

Basso costo: dispositivi di riconoscimento dell'iride possono avere costi contenuti anche nei nuovi sistemi di riconoscimento dell'iride in condizioni avverse, poiché utilizzano semplici videocamere.

***Percezione positiva del pubblico*:** anche se l'immagine dell'iride può essere acquisita senza contatto diretto, i sistemi di riconoscimento dell'iride sono ancora percepiti come intrusivi [7].

3. Panoramica dell'iride

Il processo d'identificazione può essere visto come un problema di classificazione. Un tratto biometrico può essere classificato affidabile solo se la variabilità tra differenti istanze di una determinata classe è inferiore alla variabilità tra classi diverse.

Ad esempio immagini della stessa faccia hanno un'elevata variabilità (variabilità intra-classe) a causa di espressioni, ma anche a causa del fatto che trattasi di oggetti attivi tridimensionali (3D) la cui immagine varia con l'angolo di visione, posa, illuminazione, equipaggiamento ed età. Ma è anche vero che la geometria canonica del volto ha una limitata variabilità inter-classe perché volti differenti possiedono lo stesso set basilare di caratteristiche.

Al contrario, la variabilità inter-classe dell'iride è enorme e la variabilità intra-classe è bassa: come oggetto planare, la sua immagine è relativamente insensibile ad angolo di illuminazione, e le variazioni di angolo di visione provoca solo trasformazioni affini. Anche la distorsione del modello non collimante causato dalla dilatazione pupillare è facilmente reversibile [1].

L'elemento più debole del riconoscimento dell'iride è il relativamente basso grado d'accettazione pubblica. Sebbene l'acquisizione dell'iride venga eseguita senza contatto, le applicazioni correlate sono percepite come intrusive. Molti sistemi usano l'illuminazione NIR. Questo tipo di illuminazione viene utilizzato perché non è visibile e permette di illuminare gli occhi senza disturbare gli utenti. Tuttavia, anche se gli studi confermano che alcuni secondi di esposizione a raggi NIR non danneggiano gli occhi in condizioni normali, non è chiaro cosa potrebbe accadere agli occhi o alla pelle con patologie pre-esistenti, o cosa succede se un soggetto viene accidentalmente esposto a raggi NIR per lungo tempo.

Quasi tutti i sistemi commerciali, nel visibile o basati sulla luce NIR, richiedono agli utenti di stare ad una distanza massima di 1 m (di solito molto meno), al fine di acquisire un'immagine dell'iride ad alta qualità. La necessità di condizioni standard e la cooperazione degli utenti, limita ancora i campi di applicazione per il riconoscimento basato sull'iride. Ma è certamente più agevole della riconoscimento basato sul fondo retinico [18], che è certamente più invasivo e richiede un maggior livello di cooperazione da parte dell'utente. Pertanto, sono state proposte nuove tecniche per il riconoscimento disturbato dell'iride. "Noisy Iris" si riferisce alla qualità delle immagini dell'iride su cui viene eseguito il riconoscimento [13]. Essi possono presentare i seguenti problemi:

***Occlusioni*:** palpebre, ciglia, occhiali, capelli, ecc;

***Riflessioni*:** presenza di riflessi disturbanti dovuti agli illuminatori;

***Formato differente*:** riprese ottenute con ottiche differenti e con diverse deformazioni;

Bassa risoluzione: legata al dispositivo di ripresa o alla distanza dalla videocamera;

Diversi colori dominanti: dovuto a condizioni differenti durante l'acquisizione della stessa iride.

Quindi, tali problemi possono sorgere specialmente se il riconoscimento viene eseguito su soggetti a distanza, in movimento, non coscienti dell'acquisizione in atto, in condizioni non standard di illuminazione, o semplicemente quando non viene richiesto un particolare livello di cooperazione da parte dell'utente, cosa che viene invece richiesta per velocizzare il processo di identificazione.

Le fasi di riconoscimento dell'iride disturbata sono gli stessi utilizzati in condizioni controllate, e quindi in sistemi "tradizionali", anche se richiedono approcci diversi a causa di caratteristiche dell'immagine precedentemente menzionate. Tali fasi sono in sequenza: acquisizione, segmentazione, normalizzazione, codifica, corrispondenza.

Acquisizione: rispetto ai sistemi tradizionali, l'acquisizione non è necessariamente eseguita con dispositivi dedicati o videocamera di alta qualità. Immagini dell'iride possono essere ottenute da fotocamere semplici, o attrezzature di acquisizione standard incorporata nel computer o dispositivi mobili. Le condizioni di acquisizione (illuminazione, distanza, posa, ecc) non sono strettamente controllate, contrariamente ai sistemi tradizionali.

Segmentazione: è il processo di identificazione dei confini dell'iride al fine di estrarre solo le informazioni dell'iride dalle immagini dell'occhio. Nei sistemi tradizionali, si tratta di un'operazione relativamente semplice che consiste nel trovare due cerchi che corrispondono con i bordi pupilla-iride e pupilla-sclera. Con l'iride disturbata, la segmentazione è molto più complicata. Si deve tener conto dell'eventuale presenza di occlusioni o riflessi, che devono essere scartati, nel senso che la superficie corrispondente non deve essere considerata per la codifica e il confronto. L'individuazione dei confini è ulteriormente ostacolata dalla bassa risoluzione o presenza di rumore, che rendono confini meno chiara. Per questo motivo i metodi di segmentazione dell'iride disturbata di solito implementa una fase di pre-elaborazione in cui vengono applicati filtri di smoothing (per ridurre il rumore) e/o filtri di miglioramento (per migliorare le caratteristiche, come i confini dell'iride) [5] [3].

Normalizzazione: nei sistemi tradizionali, a causa della condizione di acquisizione controllata, è necessario solo normalizzare la forma segmentata dell'iride. La normalizzazione tipica implica la trasformazione di coordinate cartesiane in quelle polari. Se si tiene conto delle informazioni sul colore, correzione del colore, istogramma di normalizzazione o operazioni simili possono essere risultare utili.

Codifica: questa fase produce un vettore modello o di caratteristiche, cioè, una rappresentazione compatta di un'immagine dell'iride. Le differenze negli algoritmi di estrazione di caratteristiche quando le iridi disturbate vengono processate dipendono dal fatto che in immagini di alta qualità anche piccoli dettagli struttura dell'iride sono facilmente visibili. Al contrario, immagini disturbate possono presentare caratteristiche alterate o meno caratteristiche da osservare. Approcci per l'estrazione di caratteristiche di immagini disturbate analizzano principalmente la texture dell'iride per esempio distribuzione del colore, presenza di regione più chiara o più scura e può anche combinare un certo numero di operatori ognuno applicato a una particolare caratteristica [4].

***Corrispondenza*:** la fase di confronto dipende solo dal tipo di modelli utilizzati.

In Figura 2 è riportata un'illustrazione delle cinque fasi sopra descritte.

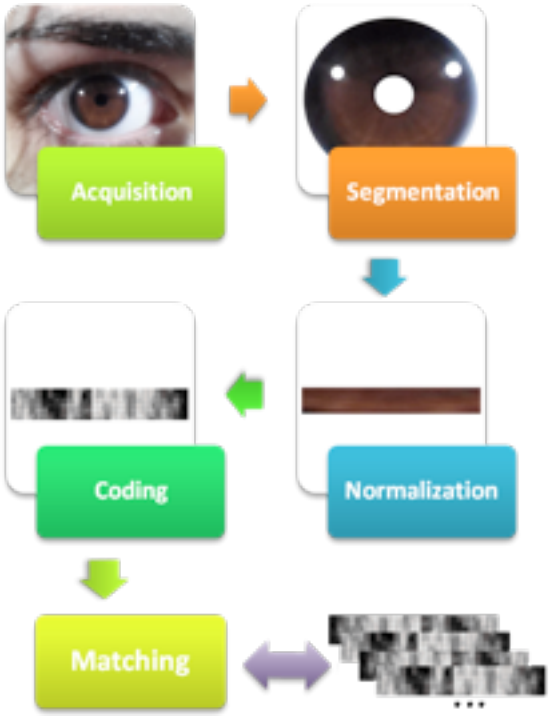


Figura 2 – Sequenza delle fasi utili al riconoscimento dell'iride

Si riportano di seguito alcune iniziative di ricerca volte a valutare i risultati delle ricerche in corso sul riconoscimento dell'iride.

4. ICE

The National Institute of Standards and Technology (NIST) ha condotto e gestito la Iris Challenge Evaluation (ICE). ICE 2005 è stato il primo contesto pubblico per il riconoscimento dell'iride. Gli obiettivi sono di promuovere lo sviluppo di algoritmi di riconoscimento dell'iride e valutare le soluzioni presentate con un protocollo standard per ottenere un confronto significativo delle loro prestazioni [9].

Per ICE 2005 un set standard di elementi sono stati forniti:

- un set di dati disponibile per lo sviluppo di algoritmi;
- un protocollo sperimentale per la misurazione della performance;
- l'algoritmo di base irisBEE.

Il database fornito da ICE, che include 2.953 immagini da 132 soggetti, è stato uno dei più grandi database d'immagini di iride pubblicamente disponibili in quel momento. Tuttavia le sue immagini sono state catturate con l'obiettivo di ottenere campioni di alta qualità, simulando la cooperazione degli utenti nel processo di

cattura dell'immagine. Pertanto, i fattori di disturbo nel database di ICE sono quasi esclusivamente occlusioni e immagini non perfettamente a fuoco [9].

Per ICE 2006, la valutazione delle prestazioni di algoritmi di riconoscimento dell'iride è stata eseguita su dati isolati (dati non visti in precedenza dai ricercatori e sviluppatori).

5. NICE

NICE (Noisy Iris Challenge Evaluation) è nato per promuovere lo sviluppo di soluzioni di riconoscimento. Questa iniziativa di valutazione biometrica dell'iride della Socia Lab. (Soft Computing and Image Analysis Group) dell'Università di Beira Interior (Portogallo), ha ricevuto partecipazioni da tutto il mondo [14]. La competizione è stata eseguita in due fasi:

- NICE.I (2007-2009): ha valutato tecniche di segmentazione dell'iride e tecniche di rilevamento del rumore;
- NICE.II (2009-2011): ha valutato codifica e strategie di corrispondenza per le firme biometrica.

I metodi proposti sono stati testati su un database fornito dallo stesso NICE: UBIRIS.v2 [12]. Il database UBIRIS è uno dei pochi database d'immagini dell'iride che contiene fattori di disturbo realistici che lo rendono adatto per la valutazione dei metodi di riconoscimento dell'iride robusti [9]. È stato sviluppato all'interno del Laboratorio Socia e rilasciato nel settembre 2004.

La caratteristica principale del database UBIRIS.v2 è che le immagini oculari contengono un elevato livello di rumore per simulare condizioni di cattura meno vincolato, ad esempio, l'acquisizione a distanza, in movimento, con la cooperazione minore o in ambienti di imaging dinamici. Un altro aspetto importante di questo database è che le immagini dell'iride sono prese dalla lunghezza d'onda visibile a dispetto dei database controllati in cui l'acquisizione è di solito eseguita sotto illuminazione NIR controllata.

Il database d'immagini NICE contiene:

1. Immagini dell'iride fuori fuoco. A causa della profondità di campo limitata della telecamera.
2. Immagini dell'iride off-angle. Ottenute quando il soggetto non guarda dritto al dispositivo di acquisizione. In questo tipo d'immagini pupilla e iride hanno una forma ellittica che deve essere presa in considerazione durante l'individuazione dei confini di pupilla e iride.
3. Immagini dell'iride ruotate. Quando il corpo/testa del soggetto non è in posizione verticale (naturale).
4. Immagini dell'iride con movimento offuscato. Grazie all'acquisizione in movimento dei movimenti delle palpebre.
5. Occlusione dell'iride dovuta alle ciglia.
6. Occlusione dell'iride a causa delle palpebre.

7. Occlusione dell'iride a causa di occhiali, in particolare montature per occhiali e/o riflessioni sulle lenti.
8. Occlusione dell'iride dovuta alle lenti a contatto. Le lenti a contatto ad elevata potenza ottica possono causare deformazioni non lineari della trama dell'iride.
9. Iride con riflessi speculari. Queste riflessioni appaiono come piccole macchie che ostruiscono la tessitura dell'iride e sono relativamente facili da rimuovere nella fase di segmentazione perché di solito sono molto più leggeri rispetto agli elementi caratterizzanti l'iride.
10. Iride con riflessioni diffuse. Queste riflessioni sono dovute a informazioni riflesse dall'ambiente in cui il soggetto si trova o sta guardando. Esse possono ostruire una gran parte dell'iride.
11. Iride catturata parzialmente. L'acquisizione a distanza e in movimento non garantisce di catturare l'intera iride.
12. Immagini fuori iride. In questo caso il sistema non è riuscito a catturare l'iride. Tuttavia il processo di riconoscimento deve essere in grado anche di capire che nell'immagine scattata non c'è un iride e per esempio richiedere di ripetere l'acquisizione .

Questo database è stato scaricato da oltre 500 utenti (privati e accademici, ricercatori e istituzioni commerciali) provenienti da oltre 70 diversi paesi del mondo [11].

Il dispositivo di acquisizione utilizzato nel catturare immagini dell'occhio del database UBIRIS è una semplice macchina fotografica. I dettagli del quadro dell'immagine sono riportati nella Tabella 1. E' stato installato in un salotto sotto fonti d'illuminazione sia naturali che artificiali. I volontari erano di diverse etnie:

- caucasici latini (circa il 90%)
- neri (8%)
- asiatici (2%).

E' stato loro solo chiesto di camminare a una velocità leggermente più lenta del normale, in una zona compresa fra tre e dieci metri di distanza dal dispositivo di acquisizione, e guardare alcuni segni, situati lateralmente rispetto al campo visivo della telecamera, per simulare il comportamento di un soggetto non cooperativo che non guarda dritto alla telecamera. La grande distanza tra il soggetto e il dispositivo di acquisizione è una delle principali differenze tra il database UBIRIS.v2 e la maggior parte degli altri.

Due sessioni distinte di acquisizione sono state eseguite, ciascuno della durata di due settimane e separate da un intervallo di una settimana. Dalla prima alla seconda sessione, sono state cambiate sia la posizione sia l'orientamento del dispositivo di acquisizione sia le sorgenti di luce artificiale. Circa il 60% dei volontari hanno partecipato ad entrambe le sessioni di acquisizioni (imaging), mentre il 40% ha partecipato esclusivamente alla prima o alla seconda sessione.

Image Acquisition Framework and Set-Up	
Camera = Canon EOS 5D	Colour Representation = sRGB
Shutter Speed = 1/197 sec.	Lens Aperture = F/6.4 - F/7
Focal Length = 400 mm	F-Number = F/6.3 - F/7.1
Exposure Time = 1/200 sec.	ISO Speed = ISO-1600
Metering Mode = Pattern	
Details of the Manually Cropped Resultant Images	
Width = 400 pixels	Height = 300 pixels
Format = tiff	Horizontal Resolution = 72 dpi
Vertical Resolution = 72 dpi	Bit Depth = 24 bit
Volunteers	
Totals = Subjects 261; Irises 522; Images 11 102	Gender = Male: 54.4%; Female: 45.6%
Age = [0,20]: 6.6% [21,25]: 32.9% [26,30]: 23.8% [31,35]: 21.0% [36,99]: 15.7%	Iris Pigmentation = Light : 18.3% Medium : 42.6% Heavy : 39.1%

Tabella 1 - UBIRIS.v2 imaging framework

Sia in NICE.I e NICE.II i partecipanti erano tenuti a presentare una applicazione eseguibile scritta in un qualsiasi linguaggio di programmazione e mandata in esecuzione in modalità autonoma. La valutazione per NICE.I (segmentazione e rilevazione del disturbo) è stata effettuata utilizzando i seguenti set:

1. **Alg** ha indicato l'eseguibile presentato, che esegue la segmentazione delle regioni senza disturbo dell'iride.
2. **$I=\{I_1,\ldots,I_n\}$** è stato il set di dati contenente l'ingresso di close-up delle immagini dell'iride.
3. **$O=\{O_1,\ldots,O_n\}$** sono state le immagini in uscita corrispondenti agli ingressi sopra descritti, tale che **$Alg(I_i)=O_i$**.
4. **$C=\{C_1,\ldots,C_n\}$** erano le immagini dell'iride binarie classificati manualmente, proposta dal Comitato Organizzatore NICE.I. Si deve presumere che ogni **C_i** contiene il risultato della perfetta segmentazione dell'iride e il rilevazione del disturbo per l'immagine in ingresso **I_i**.

Tutte le immagini di **I**, **O** e **C** avevano le stesse dimensioni: **C** colonne e **R** righe.

Sono stati utilizzate due misure di valutazione:

- Il tasso di errore di classificazione **(E^1)**;
- Il tasso di errore di tipo I e tipo II **(E^2)**.

Il tasso di errore di classificazione **(E^1)** di **Alg** sull'immagine in ingresso **$I_i(E_i)$** è dato dalla percentuale di pixel corrispondenti in disaccordo (attraverso l'operatore OR esclusivo logico) su tutta l'immagine:

$$E_i = \frac{1}{c \times r} \sum_{c'} \sum_{r'} O(c', r') \otimes C(c', r')$$

dove **O(c', r')** e **C(c', r')** sono, rispettivamente, i pixel di uscita e immagini di classe.

Il tasso di errore di classificazione (**E^1**) di **Alg** è dato dalla media degli errori nelle immagini di ingresso **E_i**:

$$E = \frac{1}{n} \sum_{i} E_i$$

Il valore di **(E^1)** appartiene all'intervallo [0, 1] ed era la misura di valutazione e classificazione dei partecipanti a NICE.I. In questo contesto, "1" e "0" saranno rispettivamente i valori peggiori e ottimali.

La seconda misura di errore mira a compensare la sproporzione tra le probabilità a priori di pixel di "iride" e "non-iride" nelle immagini. Il tasso di errore di tipo II e di tipo I (**E^2**) dell'immagine è dato dalla media tra i tassi dei i falsi positivi (FPR) e falsi negativi (FNR):

$$E_i = 0.5 * FPR + 0{,}5\ FNR$$

Analogamente al tasso di errore **E^1**, il tasso di errore **E^2** finale è dato dalla media degli errori (Ei) sulle immagini in ingresso.

I migliori 8 partecipanti, che hanno ottenuto i tassi di errore di prova più bassi, sono stati invitati a pubblicare il loro approccio in un numero speciale sulla divisione di immagini dell'iride con lunghezza d'onda visibile catturate a distanza e in movimento (Elsevier, Image and Vision Computing 28 - 2010).

La procedura di valutazione per NICE.II (la strategia di codifica e corrispondenza) è stata la seguente:

- sia **P** l'applicazione utilizzata, che fornisce la dissomiglianza tra le immagini dell'iride segmentata;
- sia **$I=\{I_1,\ldots,I_n\}$** l'insieme di dati contenente le immagini dell'iride in ingresso e siano **$M=\{M_1,\ldots,M_n\}$** le corrispondenti mappe binarie che danno la segmentazione della regione dell'iride senza rumore.

1. **P** riceve due immagini dell'iride (e le corrispondenti mappe binari), e restituisce il valore di diversità tra le iridi corrispondenti: **$P(I_i, M_i I_j, M_j)$ --> D**. **D** dovrebbe essere un valore reale positivo.
2. L'esecuzione di un confronto in regime di "uno contro tutti" per ogni immagine fornisce un set di valori di diversità intra-classe **$D^I=\{D^I_1,\ldots,D^I_k\}$** e un set di valori di diversità inter-classe **$D^E=\{D^E_1,\ldots,D^E_m\}$**, se le immagini catturate sono dalla stessa o da diverse iridi.
3. Il valore di decidibilità **$d'(D^I_1,\ldots,D^I_k,D^E_1,\ldots,D^E_m)$ --> [0, ∞[**, è stato utilizzato come misura di valutazione:

$$d' = | avg(D^I) - avg(D^E)| / sqrt (0.5* (std(D^I)^2 + std(D^E)^2))$$

dove **$avg(D^I)$** e **$avg(D^E)$** stanno a indicare i valori medi dei confronti intra-classe e inter-classe e **$std(D^I)$** e **$std(D^E)$** i corrispondenti valori di deviazione standard.

I partecipanti al contest NICE.II sono stati classificati dal valore più alto (migliore) al valore più bassi (peggiore) di decidibilità [15].

6. MICHE

Un problema più impegnativo è affrontato da MICHE (Mobile Iris CHallenge Evaluation). Come suggerisce il nome, MICHE è una valutazione tecnologia di riconoscimento dell'iride che richiede tutti i passaggi dell'algoritmo di riconoscimento dell'iride su dispositivi mobili (smartphone o tablet). L'utilizzo del riconoscimento biometrico su dispositivi mobili è un tema importante legato alla necessità di un utilizzo sicuro dei servizi critici (ad esempio home-banking) e alla necessità di proteggere i dati sensibili che oggi sono per lo più memorizzati sui nostri smartphone personali o tablet.

L'iride è quindi un candidato naturale per il riconoscimento biometrico su dispositivi mobili per due motivi principali: l'acquisizione dell'iride è poco invadente, e l'iride viene codificata attraverso l'utilizzo di modelli meno pesanti dal punto di vista della memorizzazione.

Contest MICHE, ancora nella sua fase iniziale, è il risultato della collaborazione del Biplab (Biometrico e Image Processing Lab) presso l'Università di Salerno (Italia) e la Socia Lab. (Soft Computing and Image Analysis Group) dell'Università di Beira Interior (Portogallo).

MICHE comprenderà due fasi:

- MICHE I (2013-2014): i partecipanti sono tenuti a fornire sia i loro programmi eseguibili che il set di dati che hanno usato per i loro esperimenti, nonché le caratteristiche dei dispositivi utilizzati per l'acquisizione e collaudo. Essi possono presentare i loro risultati relativi ad una o tutte le fasi del sistema di riconoscimento dell'iride eseguito su un dispositivo mobile (rilevamento, segmentazione, riconoscimento) oltre a presentare le applicazioni di biometria dell'iride su dispositivi mobili.

- MICHE II (2014-2015): i set di dati raccolti saranno utilizzati per costruire un banco di prova integrato per una sfida che sarà accessibile sia per gli autori che nuovi gruppi [16].

L'esecuzione del riconoscimento dell'iride su dispositivi mobili può introdurre molti fattori di rumore durante l'esecuzione dell'acquisizione dovuta al fatto che:

- l'utente può avere bisogno di ottenere l'autenticazione in qualsiasi momento e in qualsiasi luogo, con diverse condizioni di illuminazione, mentre si cammina, si sta in piedi o seduti;
- l'utente tiene il dispositivo mobile con la sua mano e può involontariamente spostare il dispositivo;
- le caratteristiche del dispositivo di acquisizione possono influenzare l'acquisizione: la risoluzione del sensore, la presenza della fotocamera frontale, la possibilità di utilizzare il controllo vocale per scattare la foto, ecc.

Al fine di sviluppare una soluzione robusta per il riconoscimento dell'iride su dispositivi mobili, il database utilizzato per la prova deve simulare le condizioni di acquisizione non controllate appena descritte. Un esempio di tali immagini acquisite da dispositivi mobili è illustrato nella Figura 3.

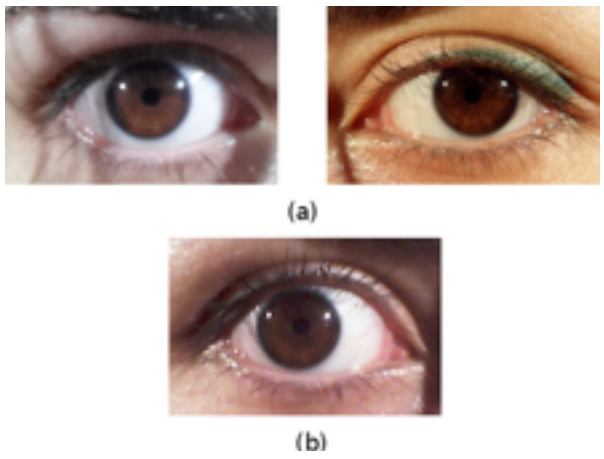


Figura 3 - MICHE I immagini di esempio dell'iride
Immagini acquisite con fotocamere di Samsung Galaxy S4 (a) posteriore a sinistra, frontale a destra;
(b) Immagine catturata con Samsung Galaxy Tab 2 (fotocamera anteriore).

7. Applicazioni commerciali e conclusioni

Le applicazioni commerciali correnti riguardano principalmente il controllo dell'accesso ad aree riservate. I Sistemi di riconoscimento dell'iride in situazione meno controllate sono stati installati in alcuni importanti aeroporti internazionali, soprattutto nel Regno Unito e negli Emirati Arabi. Per esempio, sia l'aeroporto di Gatwick che l'aeroporto di Dubai hanno adottato una soluzione AOptix.

Il sistema di riconoscimento dell'iride della AOptix InSight®VM è stato integrato nell'e-Gates 34 automatizzato al Gatwick South Terminal, al fine di accelerare il processo di controllo dei passaporti, da sempre eseguito manualmente.

Il sistema di riconoscimento dell'iride permette ai passeggeri di essere ripresi ad una distanza di due metri, e loro sono solo tenuti a guardare in un punto specifico indicato sul dispositivo. Un monitor offre ai passeggeri un resoconto testuale indicandogli dove guardare il dispositivo e, infine, ad aprire gli occhi se vi è un problema di occlusione. Il processo di riconoscimento dura pochi secondi. L'illuminazione impiegata è una lampada NIR. Il sistema può eseguire il riconoscimento sia di passeggeri su sedia a rotelle sia di altezza superiore a 2,15 metri.

AOptix InSight®Duo mantiene le stesse caratteristiche di AOptix InSight®VM ma fornisce una combinazione di riconoscimento dell'iride e del volto. E' stato adottato nell'aeroporto di Dubai e probabilmente sarà presto integrato anche a Gatwick [1].

E' interessante sapere che prima di usare prodotti AOptix, gli aeroporti di Gatwick e molti nel Regno Unito hanno adottato un sistema di riconoscimento dell'iride in condizioni controllate. Tuttavia a causa della elevata percentuale di falsi rifiuti e le difficoltà per i passeggeri in fila con l'apparecchiatura di riconoscimento dell'iride, ha portato ad abbandonare il sistema perchè il processo di identificazione impiegava molto più tempo di quello che doveva.

Ciò dimostra la necessità di sviluppare sistemi di riconoscimento dell'iride che richiedono sempre meno collaborazione degli utenti e che sono adatte a qualsiasi tipo di ambiente per poter essere uno strumento valido e veloce ma anche più sicuro rispetto ai sistemi di autenticazione esistenti.

L'iride può essere utilizzato anche in sistemi biometrici multipli. Come già accennato, AOptix InSight®Duo unisce tratti biometrici del viso e dell'iride, ma il riconoscimento dell'iride disturbata può essere anche combinato con altre biometrie o soft-biometry, per esempio informazioni perioculare, analisi dello sguardo, ecc. [17] [6]. Infine, grazie al sempre crescente sviluppo tecnologico in un futuro prossimo l'iride potrà essere catturata a notevole distanza, e possiamo immaginare di integrare le biometrie dell'iride nei sistemi di videosorveglianza per il riconoscimento o la reidentificazione delle persone [8]. Se migliorato dal punto di vista della catturabilità, tale caratteristica biometrica si presterà molto bene alla tracciabilità di individui segnalati, e diventare quindi un valido strumento di indagine da annoverare tra quelli della digital forensics.

Bibliografia

[1] AOptix, Identity Solutions http://www.aoptix.net/identity-solutions/overview

[2] John Daugman, *How Iris Recognition Works*, IEEE Transactions on Systems for Video Technology, vol. 14, no. 1, 2004, pp. 21-30

[3] Maria De Marsico, Michele Nappi, Daniel Riccio, Harry Wechsler: Iris segmentation using pupil location, linearization, and limbus boundary reconstruction in ambient intelligent environments. J. Ambient Intelligence and Humanized Computing 2(2) 2011, pp. 153-162

[4] Maria De Marsico, Michele Nappi, Daniel Riccio: *Noisy Iris Recognition Integrated Scheme*. Pattern Recognition Letters 33(8) 2012, pp. 1006-1011

[5] Maria Frucci, Michele Nappi, Daniel Riccio, Gabriella Sanniti di Baja: *Using the Watershed Transform for Iris Detection*. ICIAP (2) 2013, pp. 269-278

[6] Chiara Galdi, Michele Nappi, Daniel Riccio, Virginio Cantoni, Marco Porta: *A New Gaze Analysis Based Soft-Biometric*. MCPR 2013, pp. 136-144

[7] Michele Nappi, Daniel Riccio, Moderne Tecniche di Elaborazione di Immagini e Biometria, C.U.A. "Cooperativa Universitaria Athena", 2008

[8] Michele Nappi, Harry Wechsler: Robust re-identification using randomness and statistical learning: Quo vadis. Pattern Recognition Letters 33(14) 2012, pp. 1820-1827

[9] Rishabh Parashar, Sandeep Joshi: Comparative Study of Iris Databases and UBIRIS Database for Iris Recognition Methods for Non-Cooperative Environment, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 5, 2012

[10] P. Jonathon Phillips, Kevin W. Bowyer, Patrick J. Flynn, Xiaomei Liu, W. Todd Scruggs, *The Iris Challenge Evaluation 2005*, IEEE Second International Conference on Biometrics: Theory, Applications and Systems, 2008

[11] Hugo Proença, Luís A. Alexandre: *The NICE.I: Noisy Iris Challenge Evaluation – Part I*, IEEE First International Conference on Biometrics: Theory, Applications and Systems, 2007

[12] Hugo Proença, Silvio Filipe, Ricardo Santos, Joao Oliveira, Luís A. Alexandre: The UBIRIS.v2: A Database of Visible Wavelength Iris Images Captured On-the-Move and At-a-Distance. IEEE Trans. Pattern Anal. Mach. Intell. 32(8) 2010, pp. 1529-1535

[13] Hugo Proença: Quality Assessment of Degraded Iris Images Acquired in the Visible Wavelength. IEEE Transactions on Information Forensics and Security 6(1) 2011, pp. 82-95

[14] Hugo Proença, Luís A. Alexandre: Toward Covert Iris Biometric Recognition: Experimental Results From the NICE Contests. IEEE Transactions on Information Forensics and Security 7(2) 2012, pp. 798-808

[15] Hugo Proença, Luís A. Alexandre: Introduction to the Special Issue on the Recognition of Visible Wavelength Iris Images Captured At-a-distance and On-the-move. Pattern Recognition Letters 33(8) 2012, pp. 963-964

[16] Special Issues on Mobile Iris Challenge Evaluation (MICHE I and II) http://www.journals.elsevier.com/pattern-recognition-letters/call-for-papers/special-issues-on-mobile-iris-challenge-evaluation/

[17] Damon L. Woodard, Shrinivas Pundlik, Philip Miller, Raghavender Jillela, Arun Ross: *On the Fusion of Periocular and Iris Biometrics in Non-ideal Imagery*, Proc. of 20th International Conference on Pattern Recognition (ICPR), (Istanbul, Turkey), 23-26 August 2010, pp. 201-204

[18] Vitoantonio Bevilacqua, Lucia Cariello, Marcello Castellano, Donatello Columbo, Domenico Daleno, Massimiliano Dellisanti Fabiano, Marco Giannini, Giuseppe Mastronardi: *Retinal Fundus Biometric Analysis for Personal Identifications*, Advanced Intelligent Computing Theories and Applications. Lecture Notes in Computer Science, Vol. 5227, Springer 2008, pp. 1229-1237

Biografie

Maria De Marsico è nata a Salerno nel 1963 e ha ricevuto la laurea in informatica (con lode) presso l'Università di Salerno nel 1988. Attualmente è ricercatore in informatica presso il Dipartimento di Informatica dell'Università "La Sapienza" di Roma. I suoi interessi principali includono l'elaborazione delle immagini, i sistemi multibiometrici, la human-computer interaction. Dr. De Marsico è membro della ACM e della International Association for Pattern Recognition.

Email: demarsico@di.uniroma1.it

Chiara Galdi è nata nel 1988 e ha ricevuto la laurea in informatica (con lode) presso l'Università di Salerno nel 2012. Attualmente è dottoranda di ricerca sotto la supervisione dell'Università di Salerno e EURECOM (Sophia Antipolis, Francia). E' membro del Gruppo di Ricercatori Italiani in Pattern Recognition (GIRPR) dal 2012. I suoi principali interessi di ricerca includono: biometrica, riconoscimento dell'iride sotto condizioni controllate.

Email: cgaldi@unisa.it

Giuseppe Mastronardi è nato nel 1949 a Bari, è laureato in Scienze dell'Informazione all'Università degli Studi di Bari ed è professore ordinario di Sistemi di Elaborazione delle Informazioni al Politecnico di Bari dove insegna Informatica Medica e Sicurezza Informatica nei corsi di Laurea Magistrale in Ingegneria Elettronica e Ingegneria Informatica. Ha pubblicato oltre 120 lavori scientifici su analisi ed elaborazione di segnali e immagini e collabora con comitati di convegni, redazione di riviste e collane di informatica. Ha partecipato a numerosi progetti europei, nazionali e regionali occupandosi di tecnologie per il controllo sicuro degli accessi di persone e mezzi, mettendo a punto alcuni

brevetti. Si occupa di tecniche biometriche mettendo a disposizione di Tribunali e Procure, già dal 1978, la sua esperienza acquisita nel confronto di voci e volti assistito da computer, per accertamenti peritali connessi alle intercettazioni telefoniche e alle videoregistrazioni di atti criminosi. Ha costituito nel 2007 la eBIS srl, spin-off universitaria, finalizzata allo sviluppo di soluzioni innovative per l'identificazione personale e applicazioni biomedicali. Per conto dell'AICA, di cui è attualmente Vice Presidente, ha costituito la sezione territoriale AICA-Puglia.

Email: mastronardi@poliba.it

Michele Nappi è nato a Castellammare di Stabia nel 1965. Si è laureato in informatica (con lode) nel 1991 presso l'Università di Salerno, si specializzato in tecnologie dell'informazione e della comunicazione nel 1997 presso l'Istituto "C.E. Caianiello" e, sempre nel 1997, ha ricevuto il dottorato in matematica applicata e informatica presso l'Università degli Studi di Padova. Attualmente è professore associato di informatica all'Università di Salerno. I suoi interessi di ricerca includono il Pattern Recognition, l'elaborazione e la compressione di immagini, i database multimediali e la biometrica, la human computer interaction, la realtà virtuale e la realtà aumentata.

Email: mnappi@unisa.it

Daniel Riccio è nato a Cambridge, U.K., nel 1978. Ha ricevuto la laurea e il dottorato in informatica, rispettivamente nel 2002 e nel 2006, presso l'Università di Salerno. Attualmente è ricercatore presso l'Università degli Studi di Napoli "Federico II". I suoi interessi di ricerca includono la biometrica, la compressione frattale delle immagini e l'indicizzazione. Dr. Riccio è un membro della IEEE dal 2012, nonché del Gruppo di Ricercatori Italiani in Pattern Recognition (GIRPR) dal 2004.

Email: daniel.riccio@unina.it

Ricostruzione della Scena del Crimine in 3D

V. Mastronardi, M. Dellisanti Fabiano Vilardi

Abstract. *Il presente lavoro intende descrivere una metodica di supporto alle indagini degli organismi di investigazione scientifica nell'ambito della ricostruzione e dell'analisi delle scene del crimine. In particolare, i software presi in considerazione consentono di ottenere un alto grado di interazione con tali strumenti finalizzati alla ricostruzione tridimensionale*

Keywords: Crime Scenes, Reality Rebulding, Video Content Analysis, 3D Reconstruction Tools.

1. Introduzione

I software di ricostruzione devono essere in grado di rappresentare l'informazione ricavata dai rilievi effettuati da qualunque organismo di investigazione scientifica, partendo da dati, quali fotografie digitali e misurazioni del luogo in esame, al fine di:

- avere una rappresentazione tridimensionale della scena, raffigurata da una o più fotografie di riferimento;
- interagire con la scena tridimensionale rappresentata, inserendo e/o spostando oggetti all'interno di tale modello virtuale;
- sfruttare una libreria, di oggetti e azioni, definita a partire dalle competenze e dai protocolli operativi già utilizzati nell'ambito di indagini tradizionali;
- simulare il comportamento degli oggetti inseriti, sottoposti a leggi fisiche, all'interno della scena virtuale rappresentata.

L'utente dell'applicazione deve essere messo in grado di:

- spostare oggetti già presenti o inseriti nella scena;
- simulare il comportamento degli oggetti presenti nella scena, in base a leggi fisiche (ad es. lanciare un oggetto o cadere sul pavimento);
- vedere i contenuti dell'applicazione da diverse prospettive, anche in modalità stereoscopica.

Tali funzionalità devono costituire, sia pure per brevi linee, una panoramica sui presidi operativi di strumentazione e di tecnologie proprie dell'attuale capitolo della criminologia situazionale. E' anche molto importante programmare una formazione degli operatori del settore mirata all'uso funzionale delle nuove tecnologie, poiché, resta sempre necessario l'elemento più essenziale: l'uomo ben preparato. Si riporta di seguito (Fig.1) un esempio di ricostruzione di scena effettuata mediante un software già molto valido (3DStudio Max vers. 6), nell'ambito di un recente caso che ha coinvolto l'interesse e l'opinione pubblica nazionale e internazionale, l'omicidio di Meredith Kercher avvenuto a Perugia il 1° novembre 2007 [10].

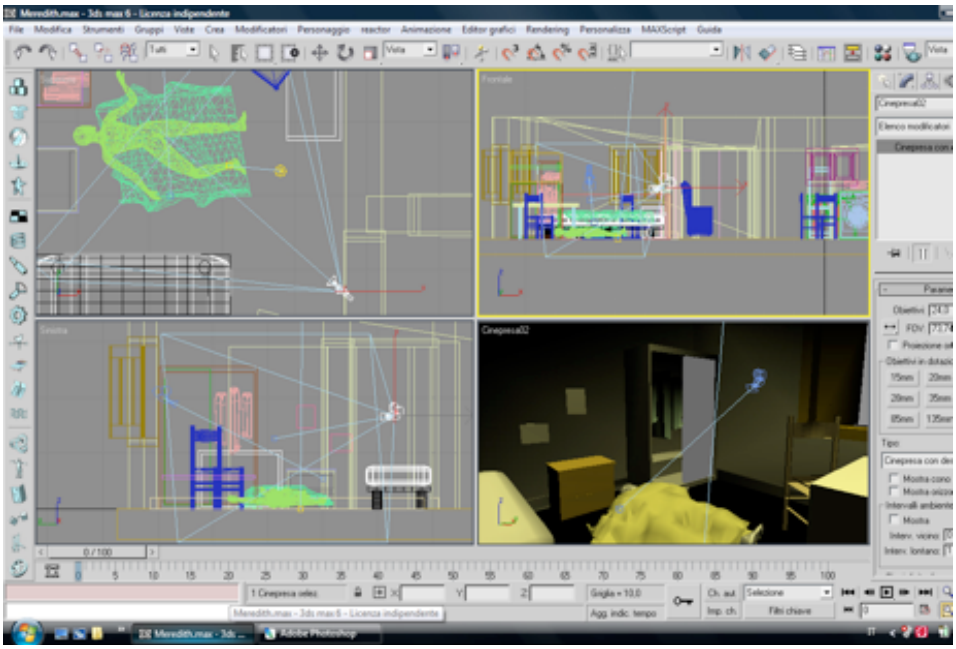


Figura 1 – Ricostruzione della scena ottenuta mediante un Software di rappresentazione 3D (3DStudio Max vers.6)

In questo lavoro si è voluto sintetizzare, per quanto possibile, le principali caratteristiche di applicativi software per la ricostruzione di scene, evidenziando le finalità di analisi in ambito forense, in funzione delle problematiche relative ai parametri che definiscono la qualità di acquisizione delle sequenze video.

2. La Video Content Analysis (VCA)

Dopo l'11 settembre 2001 l'industria ha ricevuto notevoli fondi per lo sviluppo di nuove soluzioni per l'antiterrorismo e l'anticrimine in genere. Per esempio il Governo degli Stati Uniti ha predisposto 37 miliardi di dollari per sistemi di sicurezza per l'Homeland Security, ed ha creato un Ente specifico per amministrare e gestire il programma di applicazione. Infatti, le dimensioni del mercato previsto che consentiranno ampi investimenti nel settore, nonché le esigenze anticrimine di tipo diverso dall'antiterrorismo, amplieranno le capacità e la tipologia dei comportamenti riconoscibili. Ad esempio, il mercato della sicurezza bancaria sta fortemente richiedendo applicazioni automatiche in grado di rilevare i comportamenti connessi alle rapine (volto coperto, mani alzate, scavalcamento bancone, minaccia a mano armata, ecc.). In realtà, il flusso costante dei sistemi di videosorveglianza fornisce dati che richiedono ancora l'intervento umano per l'interpretazione degli eventi, anche se stanno crescendo in numero, funzionalità e affidabilità i sistemi automatici di analisi in tempo reale (classificazione degli oggetti, rilevazione di direzione e moto, calcolo dei tempi d'interazione, etc).

Un sistema capace di interpretare una sequenza video estraendo la semantica di tali informazioni è definito come sistema di Video Content Analysis (VCA) [1] [3], che ha la capacità di analizzare automaticamente il video per rilevare e determinare gli eventi temporali non sulla base di una singola immagine. Come tale, può essere visto come l'equivalente automatizzato della corteccia visiva biologica.

Questa capacità tecnica viene utilizzata in una vasta gamma di settori, tra cui l'intrattenimento, la sanità, il retail, l'automotive, i trasporti, la domotica, la sicurezza e la protezione.

Gli algoritmi possono essere implementati mediante applicativi su macchine di uso generale, o come hardware in unità di elaborazione video specializzate.

Molte funzioni diverse possono essere implementate in VCA. Il Video Motion Detection è, per esempio, una delle forme più semplici in cui viene rilevato un movimento in relazione ad una scena di sfondo fisso. Funzionalità più avanzate includono video-tracking, stima dell'egomotion, identificazione, analisi dei comportamenti o altre forme di percezione della situazione.

I sistemi VCA sono, ovviamente, condizionati dalla qualità video in ingresso, pertanto, il flusso dati è spesso preprocessato mediante algoritmi di video-denoising, stabilizzazione dell'immagine, ottimizzazione del contrasto e super-risoluzione ottenuta mediante tecniche di ricampionamento inter-pixel su più immagini. Questi sistemi VCA sono, di fatto, gli unici che possono essere utilizzati efficacemente per risolvere alcune delle problematiche legate alla

gestione di eventi complessi anche in ambito forense. Questi software possono essere utilizzati in due modalità:

- Analisi video in tempo reale;
- Analisi video a posteriori.

Alcune possibili applicazioni sono:

- Virtual Tripwire (sbarramento virtuale)
- Congestion Detection (rilevamento code)
- Slip & Fall Detection (scivolamento e caduta)
- Directional Alarms (allarmi direzionali)
- Counting in a Crowd (contapersone nella folla)
- Theft Detection in a Crowd (rilevazione furti nella folla)
- Object Detection in a Crowd (rilevazione di specifici oggetti nella folla)
- Small (8x8 px) and Tiny (4x4) Objects Detection (rilevazione di piccoli oggetti)
- Behaviour Analysis & Tracking (analisi comportamentale e tracking)
- Parking Violations Detection (rilevazione di violazioni da parte di veicoli parcheggiati)
- Graffiti & Vandalism Detection (rilevazione di atti vandalici e graffiti)
- Detection in Low Contrast (rilevazione di oggetti in immagini poco contrastate)
- People Tracking (inseguimento di soggetti)
- Face Detection (rilevazione di volti)
- Plate Recognition (riconoscimento targhe automobilistiche)

Chiaramente non tutte le applicazioni sono utilizzabili in tutti i contesti. Ad esempio non ha senso cercare di identificare un “bagaglio abbandonato” in un luogo sovraffollato perché si registrerebbero migliaia di allarmi impropri al giorno. Ben diverso è l’utilizzo del medesimo software in un’area semisterile, come un corridoio dove si presuppone che la gente transiti o presso un binario in una stazione ferroviaria, ove è auspicabile che non si trovino ostacoli oppure oggetti di forme particolari.

Per fornire un esempio di finalità distinte nell’applicazione dei VCA ci riferiamo alla rilevazione automatica di targhe di veicoli. Tali applicativi possono essere utilizzati a fini:

Sanzionatori: (ZTL, eccesso velocità, passaggio con semaforo rosso, sorpassi della striscia continua, guida contromano, sosta vietata, ecc.) che hanno avuto una notevole divulgazione anche grazie agli introiti delle multe che permettono rapidamente alle Amministrazioni appaltanti il recupero dell’investimento (ROI).

Investigativi: ricerca all'interno di black-list di targhe segnalate anche tramite connessione automatica alle banche dati delle F.O. per garantire sicurezza in ambito urbano, o a bordo dei veicoli delle stesse F.O. per la ricerca di auto rubate, ecc.

Le migliori tecnologie permettono l'identificazione di più targhe contemporaneamente all'interno della medesima immagine. Una possibile convergenza delle due applicazioni, sanzionatorie ed investigative, potrebbe permettere di trasformare le telecamere oggi utilizzate ai fini sanzionatori (solitamente installate dai Comuni), in applicazioni real-time, per uso investigativo (Ministero dell'Interno).

Tale integrazione permetterebbe notevoli risparmi sui costi delle infrastrutture, utilizzando quelle già esistenti, oltre a minimizzare i tempi di applicazione di tali sistemi.

Altro esempio può essere costituito dalla catalogazione dei volti. Tali software permettono di catalogare in maniera automatica i volti delle persone, estrapolate dalle immagini mediante algoritmi di face-detection e face-recognition. Queste applicazioni sono particolarmente utili per la gestione a posteriori degli eventi criminosi, potendo così velocemente risalire ai volti e quindi alle identità delle persone coinvolte negli eventi in esame. Per le immagini che si presentano con adeguata definizione è, quindi, possibile ricorrere a software di analisi automatica per l'identificazione di individui già presenti nei database delle Forze dell'Ordine.

3. Trasformazione delle immagini in metadati

Uno modo particolarmente utile, presente in alcuni sistemi VCA evoluti, consiste nel trasformare in tempo reale flussi video in metadati [2]. I metadati sono informazioni costituite da dati numerici associati all'elemento da ricercare in una sequenza di immagini. In questo modo il sistema non analizza le immagini solamente in funzione delle regole di controllo stabilite in fase di configurazione, ma opera in maniera più generale, estrapolando dal video tutte le informazioni che potranno essere analizzate in fase successiva.

Ad esempio, consideriamo un perimetro riferito ad una zona recintata in cui l'operatore, in fase di programmazione, ha definito una regola di analisi per il controllo di un eventuale azione di scavalcamento. In questo caso, usando la tecnica dei metadati, è possibile rilevare a posteriori un diverso tipo di attacco applicando un nuovo "insieme" di regole. Si evita così di dover visionare direttamente tutti i filmati registrati, operazione che richiederebbe un notevole impegno di tempo, soprattutto se riferito ad un elevato numero di telecamere. Analizzare, infatti, 24 ore di video manualmente richiede, ad un operatore allenato, circa 8 ore (poiché al massimo si può interpretare il video sino a 3 volte la velocità della registrazione in tempo reale). Il più veloce algoritmo di video-analisi, eseguito su un processore dedicato, potrebbe fare lo stesso lavoro in circa 2,5 ore, ovvero in un tempo circa 10 volte minore rispetto al tempo di registrazione. Invece, la stessa ricerca effettuata sui metadati potrebbe richiedere solamente un paio minuti.

Quanto detto si applica molto bene ai data-base di volti, poiché, rappresentando questi non attraverso una immagine ma mediante o un insieme di caratteristiche morfologiche o una nuvola di punti associata a questa, si può ottenere in pochi secondi il confronto tra volti ripresi in estemporanea con volti di riferimento (white-list o black-list). Ovviamente, maggiore è la dimensione della campionatura di riferimento e maggiore è il tempo impiegato per il confronto.

4. Descrizione di alcuni ambienti di ricostruzione e analisi

Vengono di seguito riportate le caratteristiche di alcuni applicativi molto usati in ambito forense per la ricostruzione e l'analisi di scene, che, nonostante forniscano funzionalità avanzate, richiedono la gestione da parte di operatori esperti o almeno addestrati.

3DStudio Max

3DStudio Max [4] è un software di modellazione 3D particolarmente evoluto e utilizzato in molteplici ambiti. Non solo consente di modellare oggetti, ma anche di creare animazioni 3D. Mette a disposizione numerosi tool per la simulazione del comportamento dinamico di corpi rigidi e/o elastici, di liquidi e particelle. Consente di lavorare con nuvole di punti e di effettuare operazioni di 3D sculpting (vedi esempio in Fig.1). Dispone inoltre di un motore di scripting in linguaggio Python per codificare sequenze di operazioni.

Poser Pro

Il software Poser Pro [5] consente di realizzare modelli 3D di corpi umani o animali. Non si tratta di un vero e proprio modellatore, poiché i modelli sono precostituiti e raccolti in una ricca libreria di personaggi virtuali già pronti. Tuttavia il software offre notevolissime possibilità di personalizzazione di ciascun personaggio. Poser permette ad esempio di partire da una immagine di un volto e ricavarne la texture da applicare ad un modello tridimensionale, conferendogli un elevato grado di somiglianza e realismo. Analogamente mette a disposizione tools evoluti per la caratterizzazione dei capelli del soggetto virtuale, delle mani, dei vestiti e dei materiali. Sono anche disponibili modelli virtuali con diverse espressioni facciali. I modelli sono tutti articolabili e animabili in maniera realistica. Inoltre, Poser permette di simulare il comportamento dinamico dei tessuti e dei capelli conferendo elevato realismo alle animazioni. I modelli creati in Poser possono poi essere esportati per essere utilizzati insieme a scene e modelli all'interno dei più comuni software di modellazione 3D (Fig.2). Questo strumento può essere considerato come supporto di grande effetto per la ricostruzione animata di scene del crimine, ma, nonostante la sua parametrizzazione, è opportuno non impiegarlo a fini identificativi, poiché pur consentendo la ricostruzione di sembianze e fisionomie riportate dalla reale osservazione dei soggetti, è fortemente condizionato dalla definizione delle immagini di riferimento nonché dalla soggettività del posizionamento dei punti caratterizzanti e basilari per la ricostruzione.

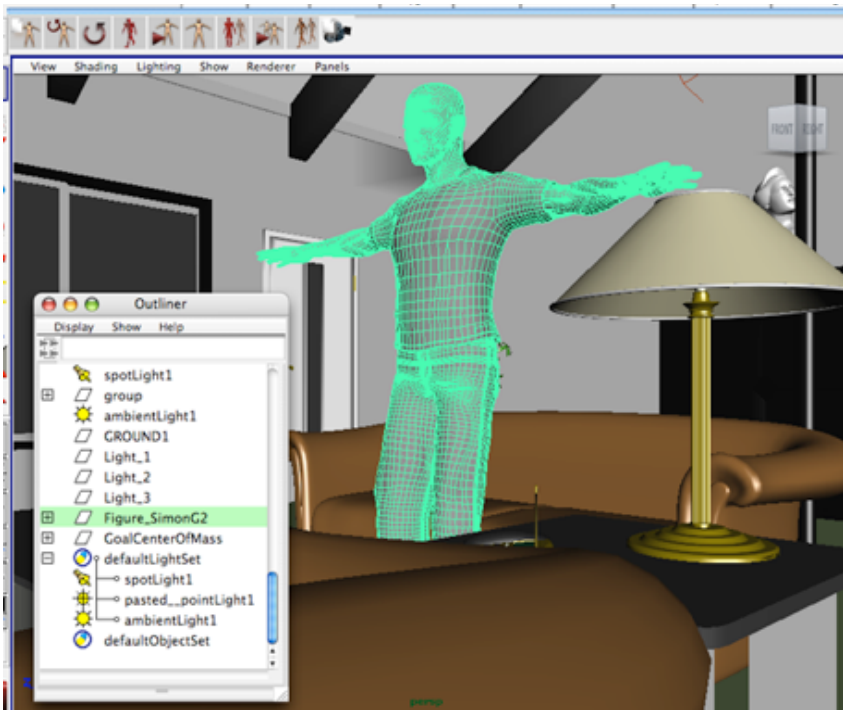


Figura 2 – Esempio di modellazione e posizionamento di un corpo umano

Rhino

Rhinoceros 3D [6] è uno dei più noti ed evoluti software di modellazione 3D basati su NURBS (Non-Uniform Rational Basis Spline). Le NURBS sono modelli matematici adatti alla rappresentazione di curve e superfici. La loro caratteristica è quella di offrire un controllo preciso della curvatura mediante la manipolazione di nodi. Le figure ottenute mediante NURBS sono definite "free forms" (forme libere) poiché non sarebbero ottenibili mediante composizione di forme geometriche semplici. La modellazione free-form offerta da Rhino permette di modellare oggetti complessi e realistici. Tale caratteristica ha reso Rhino molto utilizzato in ambito di design industriale e automobilistico, di reverse engineering ma anche per la ricostruzione 3D di ambienti e oggetti (Fig.3).

DXO Optics Pro

Si tratta di un software di correzione di immagini fotografiche. Come molti altri software offre funzionalità di manipolazione del contrasto, della luminosità e dei colori. Le caratteristiche più interessanti però riguardano il "denoising" ed in particolar modo la "rectification". DXO Optics [7] implementa algoritmi evoluti di "denoising" ovvero di eliminazione o, per meglio dire, di riduzione del rumore. Tali algoritmi cercano nell'intorno di ciascun pixel aree similari dalle quali estrarre pattern ripetibili per incrementare il livello di dettaglio, oppure per calcolare il miglior fattore di variazione del contrasto. Tali algoritmi sono particolarmente efficaci a livello visivo ma il loro approccio è di carattere "predittivo". Cercare di aumentare l'informazione presente in una immagine può introdurre artefatti che, se pure gradevoli alla vista, possono discostarsi, anche

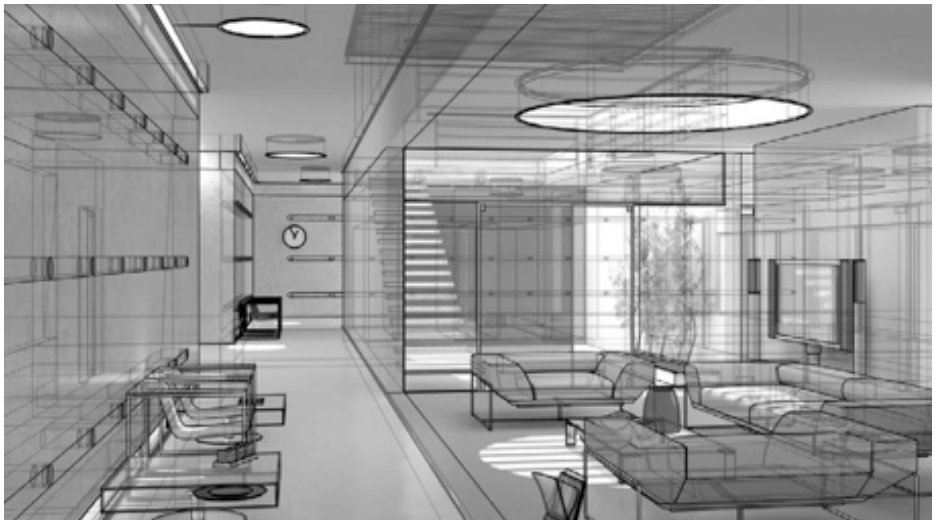


Figura 3 – Esempio di modellazione di una scena 3D

solo nei dettagli, dalla scena reale. Di grandissimo interesse sono invece le funzionalità di "rectification" che permettono di compensare le tipiche distorsioni delle immagini causate dalla curvature delle lenti che compongono l'ottica delle macchine fotografiche. La compensazione può avvenire sulla base delle caratteristiche della lente, immagazzinate nel formato EXIF prodotto dalla maggior parte delle macchine fotografiche, oppure mediante impostazione manuale dei parametri ottici, nel qual caso la distorsione della lente andrebbe misurata oppure valutata con opportuni metodi di calibrazione.

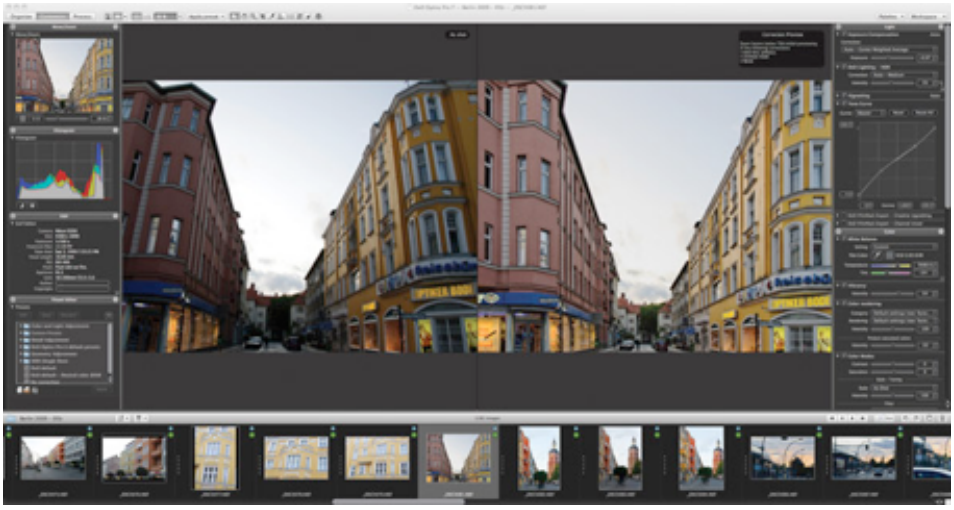


Figura 4 – Esempio di correzione del contrasto e della distorsione introdotta dall'ottica di una fotocamera mediante il software DXO Optics

Canoma

Canoma [8] è un software capace di realizzare modelli 3D a partire da un insieme di foto dello stesso oggetto, o della stessa scena, ripresi da angolazioni differenti. Il software non mette a disposizione alcun automatismo di ricostruzione, ma permette all'utente di modellare la scena direttamente sulle immagini con un approccio di modellazione mediante composizione di primitive, ovvero oggetti tridimensionali semplici come parallelepipedi, piani, coni, sfere, ecc. La modellazione in Canoma è di scarso interesse per l'elevato livello di imprecisione ottenibile, dovuto al fatto che l'utente sceglie i punti notevoli delle primitive ad "occhio" cercando di farli coincidere visivamente con gli analoghi punti nelle foto. Canoma, invece, diviene uno strumento molto interessante se usato in combinazione con un modellatore 3D che consenta di creare il modello della scena a partire da geometrie note. Una volta creato il modello, infatti, è possibile importarlo in Canoma che, dopo una opportuna calibrazione della posizione del modello rispetto alle foto, andrà a generare le texture da applicare a ciascuna superficie della mesh, conferendo all'intera scena 3D un elevato fotorealismo. Canoma non possiede alcuna funzionalità di compensazione della distorsione delle lenti, pertanto, al fine di ottenere risultati ottimali, le immagini dovrebbero essere sottoposte preventivamente a compensazione mediante algoritmi di correzione. Impiegato nel caso dell'omicidio a Gravina di Maria Pia Labianca (1999), ha consentito di rappresentare la modificazione dei luoghi del ritrovamento del cadavere nel corso delle successive indagini, documentate da riprese video effettuate da investigatori autorizzati ed emittenti televisive (Fig.5).

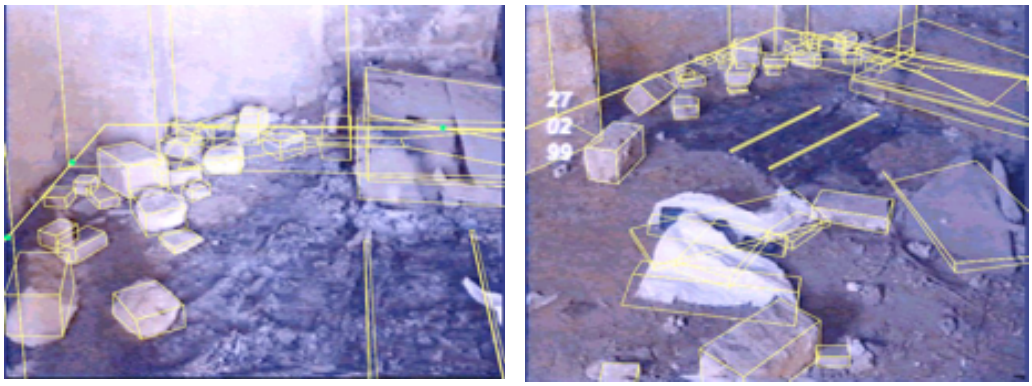


Figura 5 – Esempio di applicazione di Canoma

Mathematica

E' un ambiente di calcolo avanzato [9] molto utile nell'ambito della ricostruzione di scene poiché mette a disposizione strutture, operatori, funzioni e metodi matematici e geometrici componibili in modo da poter implementare algoritmi di ogni tipo ed effettuare calcoli e rappresentazioni multidimensionali utili alla misurazione di oggetti e ambienti anche in uno spazio tridimensionale.

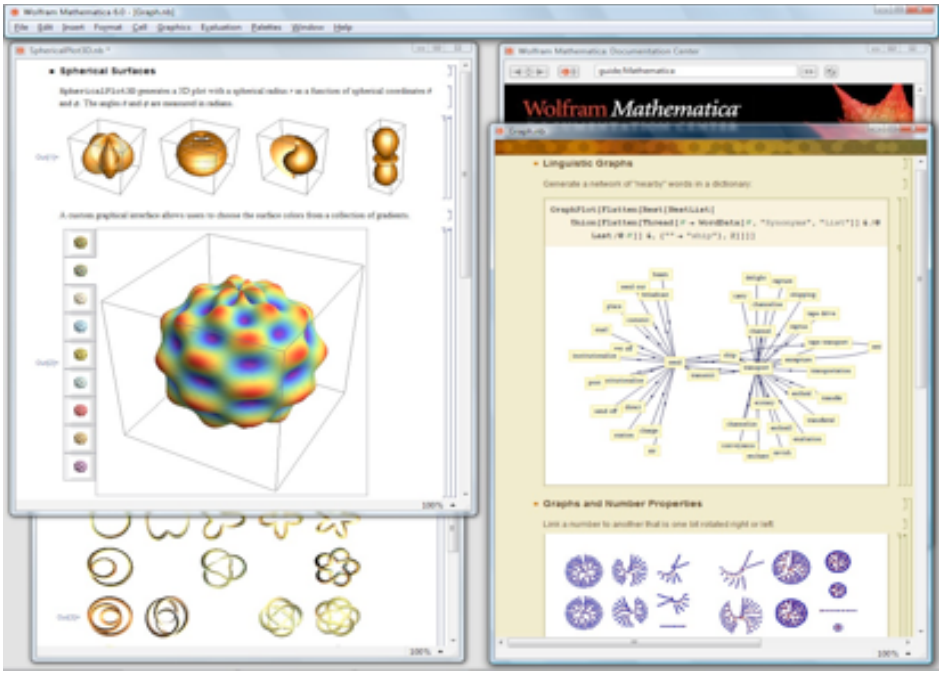


Figura 6 – Rappresentazione di nuvole di punti e di superfici mediante il software Mathematica

5. Conclusioni

Questa veloce panoramica sullo stato dell'arte dell'analisi video illustra le attuali possibilità dei sistemi VCA (Video Content Analysis), indicando le opportunità offerte e i limiti obiettivi della loro applicazione nella ricostruzione e nell'analisi di scene di atti criminosi.

Bibliografia

[1] A.Hanjalic, N.Sebe, E.Chang: "Multimedia Content Analysis, Management and Retrieval: Trends and Challenges"; SPIE Proceedings, vol. 6073, 607301 (15/01/2006)

[2] D.M. Shotton, A. Rodríguez, N. Guil, O. Trelles: "A metadata classification schema for semantic content analysis of videos"; Journal of Microscopy, vol. 205, pp. 33–42 (01/ 01/2002)

[3] N. Dimitrova, H.J. Zhang, B. Shahraray, I. Sezan, T. Huang, A. Zakhor: "Applications of Video-Content Analysis and Retrieval"; IEEE MultiMedia Archive, vol. 9 issue 3, pp. 42-55 (07/2002)

[4] 3DS Max - http://www.autodesk.com/products/autodesk-3ds-max/overview

[5] Poser Pro - http://poser.smithmicro.com

[6] Rhino - http://www.rhino3d.com

[7] DXO Optics Pro - http://www.dxo.com

[8] Canoma - http://www.canoma.com

[9] Mathematica - http://www.wolfram.com/mathematica

[10] V.M. Mastronardi, G. Castellini: “Meredith. Luci e ombre a Perugia”; Collana Crimini e Criminali, Armando Editore, 2009

Biografia

Vincenzo Mastronardi, Psichiatra, Psicoterapeuta, Criminologo clinico, Titolare della Cattedra di “Psicopatologia forense”, Direttore dell’Osservatorio dei Comportamenti e della Devianza”, e del “Master in Scienze Criminologico forensi” presso la Facoltà di Medicina e Odontoiatria della Sapienza Università di Roma (Dipartimento di Neurologia e Psichiatria).Autore di 260 lavori, e 26 libri in tema di criminologia , psicopatologia forense, psicoterapia e sulla “comunicazione” con più case editrici tra cui: Manuale per Operatori Criminologici e Psicopatologi Forensi. Quinta Edizione, Giuffrè Editore, 2012 pp.443, con Sante A. Bidoli, Monica Calderaro Grafologia Giudiziaria e Psicopatologia forense.Metodologia di indagine del falso grafico e la capacità di intendere e di volere dalla grafia. Giurisprudenza. Giuffrè Editore 2010 pp.297., in coll. con G.B. Palermo) Il Profilo Criminologico. Dalla Scena del Crimine ai Profili socio psicologici, Giuffrè ed. 2005 pp.385 con R. De Luca I Serial Killer, Newton & Compton 2013 pp.860 E’ Direttore responsabile della Rivista <<Rassegna di Psicoterapie. Ipnosi. Medicina Psicosomatica. Psicopatologia forense>> dell’Università Sapienza di Roma. Tra gli altri incarichi ricevuti è Docente presso la Scuola Superiore della Magistratura.

Email: vincenzo.mastronardi@gmail.com

Massimiliano Dellisanti Fabiano Vilardi è nato nel 1973 a Bari, è laureato in Ingegneria Elettronica con indirizzo Telecomunicazioni al Politecnico di Bari dove ha conseguito anche il Dottorato in Biomeccanica e dove è stato Professore a Contratto per i corsi di Informatica, Informatica Grafica e Laboratorio di Informatica nei corsi di Laurea in Ingegneria Edile, Ingegneria Edile-Architettura ed Ingegneria Elettronica. Ha pubblicato lavori scientifici nell’ambito della Elaborazione delle Immagini, della Interazione Uomo-Macchina, e della Realtà Virtuale e Aumentata. Si è occupato di Informatica Medica progettando sistemi informatici per la medicina. Nel 2003 ha fondato la Digital Future Engineering per seguire e gestire le installazioni informatiche in alcuni dei più importanti ospedali italiani.

Email: maxdfv@gmail.com

Il Telefono Cellulare come Strumento per la Individuazione Georeferenziata, la Tracciabilità di Soggetti Indagati e il Controllo della Linea Emozionale

R. Cusani, V. Mastronardi

Abstract. *Il telefono cellulare ha da tempo assunto un ruolo fondamentale nel campo investigativo e forense, evidente ormai anche al grande pubblico che segue con interesse dai giornali e dalle televisioni fatti di cronaca connessi alla scomparsa di persone o a crimini rimasti insoluti.*

Ciò si verifica non solo riguardo l'intercettazione delle conversazioni, già largamente in uso per i telefoni 'fissi', ma anche ai fini della ricostruzione degli spostamenti del cellulare ovvero del suo possessore. La rete cellulare permette infatti sia l'inseguimento in tempo reale di un telefono posto sotto sorveglianza, tramite l'analisi dei segnali che esso scambia con le antenne fisse, sia la ricostruzione in differita degli spostamenti basata sui tabulati telefonici forniti dall'operatore di telefonia mobile utilizzato da quel cellulare.

In tale contesto talvolta insorgono curiose anomalie poco note ai non-esperti del settore che se non rivelate opportunamente possono condurre ad interpretazioni erronee riguardo la posizione effettivamente assunta dal telefono, con pesanti riflessi sulla correttezza delle indagini e sulle conclusioni degli investigatori e dei giudici.

Nel presente lavoro vengono introdotti e discussi alcuni di questi fenomeni, con l'obiettivo di fornire un contributo di conoscenza utile agli operatori del settore investigativo e forense. In particolare, viene mostrato come l'informazione di localizzazione offerta dalla conoscenza della antenna cui risulta connesso un telefono cellulare debba essere opportunamente verificata alla luce della conoscenza dei fenomeni sopra menzionati.

Keywords: Localisation, Cellular phone

1. Localizzazione dell'utente nel sistema radiomobile cellulare GSM

Il sistema radiomobile cellulare, sia di tipo GSM che UMTS, presenta una struttura estremamente complicata, per lo più comprensibile solo agli specialisti del settore. Nel seguito faremo riferimento al solo GSM, con considerazioni che in linea di massima risultano valide anche per l'UMTS. Per approfondimenti sul GSM si rimanda ai testi [1][2][3], mentre [4] ne evidenzia alcuni aspetti rilevanti nell'abito processuale.

E' ben noto che un terminale mobile GSM, comunemente indicato come "telefono cellulare" o solamente come "cellulare", comunica connettendosi via radio, tramite le antenne, ad una stazione radio-base (detta BTS o semplicemente stazione-base). Con quest'ultima il cellulare scambia i segnali che preparano e poi danno luogo allo svolgimento della conversazione telefonica, gestendo le varie fasi di inizio, mantenimento e fine della chiamata. I segnali scambiati sono di tipo forma digitale, ovvero sono costituiti da flussi di bit.

Tale meccanismo è possibile solo se il telefono riceve dalla stazione-base un segnale di potenza sufficientemente elevata da permettergli il corretto riconoscimento dei bit di ricevuti e quindi la ricostruzione di un segnale vocale di qualità sufficiente. Se ciò si verifica si dice comunemente che il telefono "riceve segnale" ovvero che è "sotto copertura" da parte della stazione-base, che usualmente è quella geograficamente più prossima al telefono stesso.

E' quindi usuale associare convenzionalmente a ciascuna stazione-base un'area, solitamente assunta di forma circolare oppure esagonale, che denota la porzione di territorio "coperta" da quella stazione-base ovvero all'interno della quale si ritiene debba trovarsi il telefono quando è connesso ad essa. La Figura 1 illustra quanto detto.

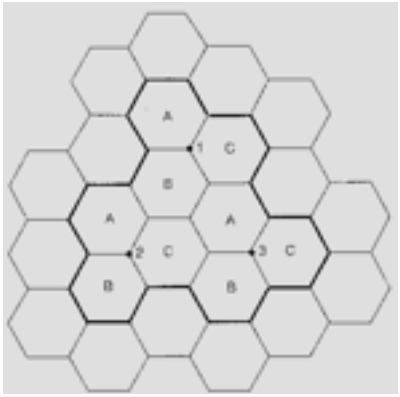


Figura 1 – Rappresentazione schematica della copertura cellulare nel GSM

Una descrizione di questo tipo, seppure utile per una prima comprensione da parte di un lettore non specializzato, rischia di diventare del tutto fuorviante e di portare a conclusioni errate riguardo la capacità di determinare la posizione

effettiva del cellulare sulla base della sola conoscenza della BTS (o anche del "settore" di copertura) cui esso risulta connesso in un determinato istante.

Infatti, nel funzionamento reale del sistema GSM diversi fattori contribuiscono a rendere la situazione molto più complicata.

Nel GSM tutte le BTS emettono costantemente dei segnali che servono da "richiamo" per i cellulari che operano nelle loro vicinanze. Allorquando un cellulare viene acceso, esso opera una "Ricerca Rete" misurando la potenza che riceve dalle diverse BTS circostanti, scegliendo la BTS cui corrisponde la potenza maggiore e "agganciandosi" ad essa.

Se la BTS prevede antenne a settori allora il cellulare si aggancia alla BTS tramite il settore da cui riceve maggiore potenza. Tale dettaglio risulta inessenziale ai fini della discussione proposta in questo documento e quindi viene omesso nel seguito continuando a riferirsi alle BTS piuttosto che, come sarebbe più completo dire, ai settori di BTS.

Usualmente la BTS da cui il cellulare riceve maggiore potenza è quella più vicina, come mostrato nella Figura 2 dove la BTS n.1, la più vicina, è quella effettivamente connessa al cellulare.

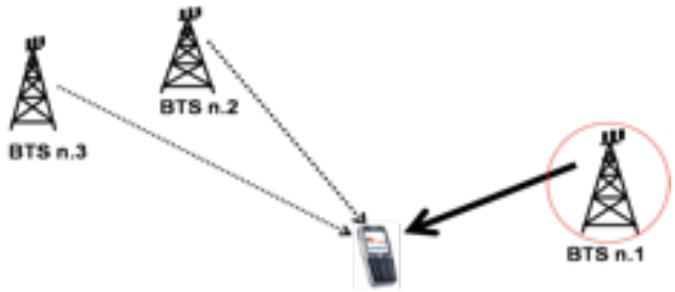


Figura 2 – Il cellulare si aggancia alla BTS da cui riceve la maggiore potenza, la n.1

2. Meccanismi reali di aggancio del telefono cellulare alla stazione-base

In realtà, molto spesso, diverse circostanze portano il cellulare ad "agganciarsi" ad una BTS che non è affatto la più vicina.

Come primo esempio, nel momento in cui avviene la connessione il cellulare potrebbe trovarsi in una posizione tale che la BTS più vicina risulta "nascosta" da un ostacolo fisso quale un edificio, oppure mobile quale un camion parcheggiato o in movimento vicino al cellulare. In tal caso, la potenza ricevuta dalla BTS più vicina risulta minore della potenza ricevuta da una delle BTS più lontane ed il cellulare si "aggancia" ad una di queste ultime, anziché alla BTS più vicina, come mostrato nella Figura 3 dove la BTS n.1, la più vicina, è oscurata dalla presenza di edifici ed il cellulare si "aggancia" alla BTS n.2, più lontana..

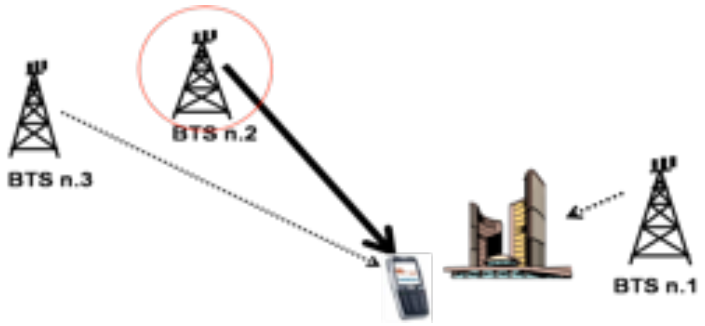


Figura 3 – La presenza di ostacoli induce il cellulare ad agganciarsi alla BTS n.2 anziché alla n.1, più vicina

Come secondo esempio, illustrato in Figura 4, il segnale ricevuto dalla BTS più vicina potrebbe risultare fortemente disturbato da interferenze elettromagnetiche involontariamente generate in prossimità del cellulare da impianti radiotelevisivi in uso a privati o a enti pubblici e da apparecchi di uso comune, quali antifurti elettronici, motori elettrici e ricetrasmettitori domestici per televisione. Poiché ciascuna BTS trasmette su bande di frequenza diverse è possibile che il segnale ricevuto da una BTS più lontana non subisca l'influenza delle stesse interferenze e che quindi il cellulare decida di "agganciarsi" a tale BTS più lontana.

Come terzo esempio, se la BTS più vicina è già impegnata con un gran numero di cellulari operanti nelle sue vicinanze essa rifiuta di farsi "agganciare" dal cellulare, che a questo punto si aggancia ad un'altra BTS che sia invece disponibile.

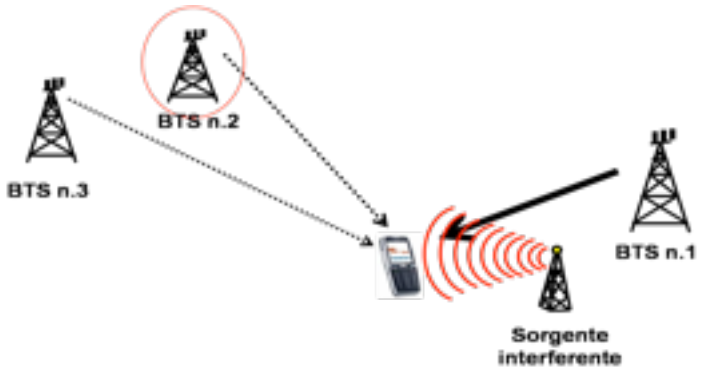


Figura 4 – Una interferenza si sovrappone al segnale ricevuto dalla BTS n.1, la più vicina, ed il cellulare si aggancia alla BTS n.2

In tutti i casi sopra descritti, una volta agganciato ad una BTS lontana il cellulare mantiene tale aggancio anche qualora venissero a cadere i motivi per i quali non si era agganciato alla BTS più vicina. Per il primo esempio di cui sopra, questo può succedere quando il cellulare si sposta anche di pochi metri e la BTS più vicina diventa "visibile" ad esso, oppure si sposta l'ostacolo a tale

visibilità (ad esempio, il camion). Per il secondo esempio, la sorgente di interferenza potrebbe spegnersi oppure il cellulare potrebbe spostarsi, anche di poco, da uscire dall'influenza dell'interferenza stessa. Per il terzo esempio, i cellulari connessi alla BTS più vicina potrebbero spostarsi in una BTS diversa oppure venire spenti, così lasciando la BTS più vicina disponibile ad essere agganciata da altri cellulari.

A tal riguardo, si sottolinea l'esperienza di tutti nel verificare quanto sia sensibile il cellulare a spostamenti di pochi metri, e talvolta anche di pochi centimetri, nel percepire correttamente il segnale emesso dalla BTS.

A dimostrazione di quanto possa essere drastica la situazione sopra descritta, è stato rilevato che un cellulare acceso in una città costiera dell'Adriatico, quale ad esempio Ancona, possa ricevere un forte segnale e quindi "agganciarsi" a una BTS dislocata sulla costa jugoslava. Ciò indurrebbe nell'erronea interpretazione che il cellulare e il suo proprietario si trovino sull'altra sponda del mare!

Più in generale, in situazioni di territorio pianeggiante il cellulare potrebbe trovarsi a decine di chilometri dalla BTS cui risulta "agganciato". D'altra parte, all'interno delle aree urbane sono particolarmente frequenti i fenomeni sopra riportati che inducono il cellulare ad agganciarsi a BTS diverse dalla BTS più vicina.

Il fenomeno dei "cammini multipli"

La situazione reale nello scambio di segnali tra cellulare e BTS risulta ancora più complicata di quanto sopra descritto. Infatti nel collegamento radio dalla BTS verso il cellulare la presenza di ostacoli naturali od artificiali quali colline, avvallamenti, edifici, genera una pluralità di riflessioni dell'onda elettromagnetica emessa. Il segnale ricevuto dal cellulare risulta quindi costituito da un "raggio principale" corrispondente alla traiettoria diretta tra BTS e cellulare detta "linea di vista" o, in inglese, "line of sight" (LOS) seguito da svariati "raggi secondari", che lo raggiungono a brevissima distanza temporale. Identica situazione si manifesta nella trasmissione dal cellulare verso la BTS.

In ciò consiste il fenomeno dei *cammini multipli*, illustrato in Figura 5. In ambiente cittadino la presenza degli edifici rende molto raro che cellulare e BTS siano in linea di vista, il raggio principale è assente ed il collegamento viene assicurato proprio dai "raggi secondari".

La situazione sopra descritta fa insorgere ulteriori dubbi ed ambiguità sul reale posizionamento del cellulare connesso ad una certa BTS o settore di BTS. Nell'esempio di Figura 6 il raggio diretto tra BTS e cellulare trova l'ostacolo insormontabile di un edificio mentre la riflessione contro un altro edificio permette al raggio riflesso di collegare il cellulare con un settore di BTS addirittura in posizione opposta!

Figura 5 – Fenomeno dei cammini multipli nel GSM

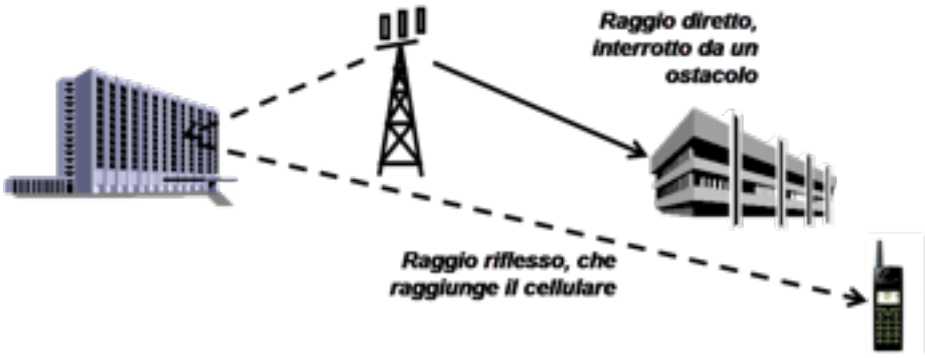


Figura 6 – Collegamento tra BTS e cellulare in direzione opposta

La situazione viene ulteriormente complicata dal fatto che i moderni telefoni cellulari sono dotati di sofisticati sistemi di elaborazione del segnale ricevuto che sfruttano la presenza dei cammini multipli per "rinforzare" il segnale stesso. Non entriamo in dettagli sull'argomento, che risulta altamente specialistico e ben difficile da comprendere per chi non sia altamente specializzato nel settore.

Ai fini della presente relazione è però importante sottolineare come la possibilità del cellulare di "agganciarsi" ad una determinata BTS non dipende solo dalla potenza ricevuta ma anche dalle sue capacità elaborative, per cui un cellulare di ultima generazione e di fascia alta (per intendersi, un cellulare più costoso degli altri) si "aggancia" anche in alcune zone del territorio dove i cellulari di fascia bassa (meno costosi) non riescono ad agganciarsi.

Da quanto riportato nella presente Sezione risulta evidente l'impatto del fenomeno dei cammini multipli, sempre presente in qualunque situazione pratica, nel determinare ulteriori incertezze sulla localizzazione del cellulare.

3. Copertura effettiva offerta da una BTS

L'aggancio con una BTS, sia essa lontana o vicina, avviene a condizione che il segnale ricevuto dal cellulare superi un valore minimo di potenza che garantisce il corretto riconoscimento del segnale ricevuto ovvero dei bit di informazione che rappresentano sia il segnale vocale, gli SMS e la segnalazione ausiliaria scambiata per la messa in opera ed il mantenimento della comunicazione. Tecnicamente, tale valore minimo viene individuato pari a -110dBm ovvero 0,01 miliardesimi di Watt.

Come noto, il segnale emesso dalla BTS vede la sua potenza attenuarsi man mano che si allontana, raggiungendo ciascun punto del territorio circostante con un determinato valore di potenza che diminuisce all'aumentare della distanza. Qualunque posizione del territorio laddove il segnale emesso da quella BTS ha una potenza maggiore dei -110 dBm sopra menzionati costituisce un possibile punto dove si può trovare il cellulare quando risulta connesso a quella BTS, e determina la "copertura effettiva" offerta dalla BTS.

La Figura 7 illustra la "copertura effettiva" di una BTS in ambiente urbano (Roma). Risulta evidente come la coperture effettiva sia moto più estesa di quella teorica e di forma piuttosto complicata molto diversa dalla schematica forma circolare od esagonale quale quella riportata in Figura 1.

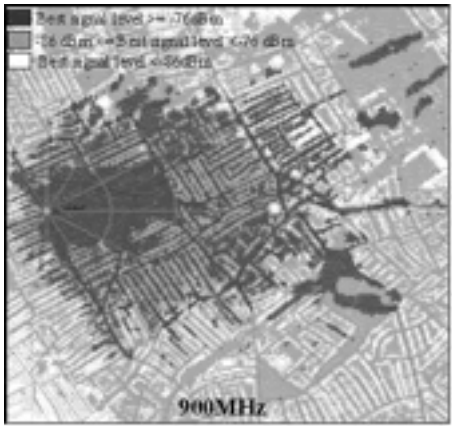


Figura 7 – Livelli di copertura radio (destra) per una BTS situata a Roma

In particolare la Figura 3.1 mostra come la presenza dei palazzi, che fa insorgere il fenomeno dei cammini multipli prima descritto, altera la propagazione del segnale elettromagnetico emesso dalla BTS dando luogo, soprattutto in lontananza dalla BTS stessa, all'alternanza di porzioni di territorio di ridotte dimensioni dove il cellulare riceve o non riceve dalla BTS un segnale sufficientemente elevato (ovvero, come si dice comunemente, "prende" o "non prende").

Tale situazione è già stata richiamata in precedenza come esperienza comune nel rilevare la grossa sensibilità della ricezione GSM rispetto a spostamenti anche di pochi centimetri. Essa è ben nota agli esperti del GSM che progettano

la “copertura” radio del territorio sulla base di concetti, modelli ed analisi di tipo statistico utilizzando allo scopo complessi e costosi programmi software ed archivi contenenti mappe del territorio precise ed aggiornate.

Tra i principali concetti di tipo statistico menzioniamo (vedi, ad esempio, [5]):

- l’attenuazione (“fading”) lenta e veloce
- i modelli di attenuazione in ambiente urbano ed in ambiente rurale
- il “margine di attenuazione”
- la “probabilità di locazione”
- la “probabilità di fuori servizio”.

4. Passaggio da una BTS all’altra (“Handover”)

Quanto descritto in precedenza a proposito della procedura di “aggancio” del cellulare alla BTS si ripete in maniera analoga, seppur con differenze tecniche sulle quali non si ritiene utile soffermarsi in questa sede, ogni qualvolta il cellulare si trova in movimento e, allontanandosi sempre più dalla BTS, percepisce un segnale di potenza decrescente.

In tal caso il cellulare effettua una nuova ricerca della BTS che gli offra il segnale di potenza maggiore, seguendo gli stessi criteri adottati nella procedura di “aggancio” iniziale e quindi scegliendo di agganciarsi ad una BTS che potrebbe non essere affatto quella più vicina, per le stesse cause descritte in precedenza. Tale situazione viene denominata “Passaggio di cella”, in inglese “Handover”, ed è illustrata nella Figura 8 dove si vede che il cellulare, inizialmente agganciato alla BTS n.1, si sposta verso la BTS n.3 finché si aggancia ad essa. In tutto il percorso il cellulare viene “sorvegliato” da tutte e 3 le BTS presenti.

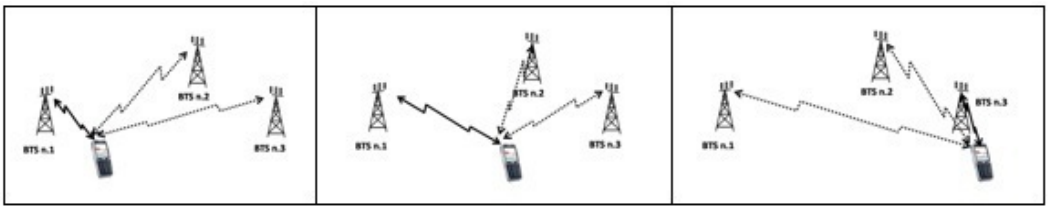


Figura 8 – Procedura di passaggio delle consegne (“Handover”) da una BTS all’altra

5. Conclusioni sulla localizzazione dell’utente nel sistema GSM

Quanto esposto nelle sezioni precedenti conduce alla semplice conclusione che la localizzazione di un cellulare sulla base della conoscenza della BTS (o settore di BTS) cui risulta agganciato lascia margini di dubbi sulla precisione ottenibile, e l’unica affermazione corretta sembra essere che il cellulare “si trova in una posizione non lontana dalla BTS ma forse anche a diversi chilometri da essa”.

Ad esempio, in Figura 9 le tre posizioni a, b e c sono altrettanto plausibili per un cellulare che risulti agganciato alla BTS in posizione centrale.

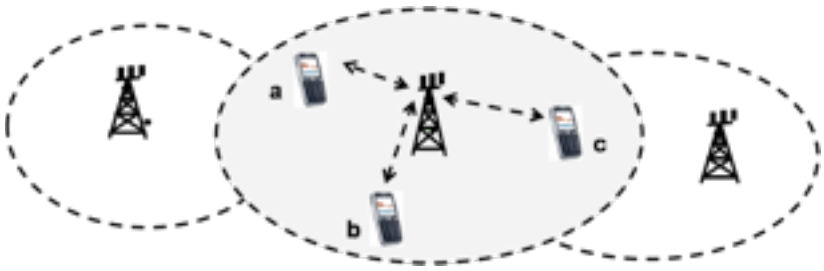


Figura 9 – Posizioni plausibili per un cellulare che risulta agganciato alla BTS

Tale conclusione è pienamente condivisa da tutta la letteratura tecnica internazionale el settore (vedi, ad esempio, [6]).

6. Localizzazione di un telefono cellulare sotto sorveglianza

Se il cellulare viene messo sotto sorveglianza è possibile localizzarlo con notevole precisione. Il principio della triangolazione può essere applicato in questo caso elaborando congiuntamente i segnali che vengono emessi dal terminale mobile e captati da almeno 3 BTS che si trovano nei dintorni (vedi Figura 10).

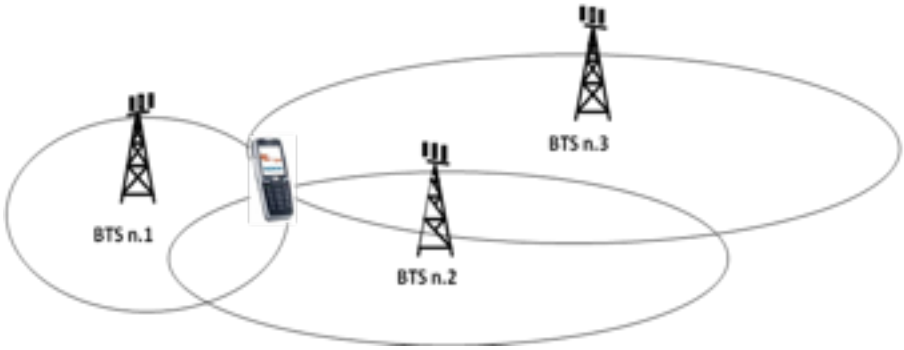


Figura 10 – Impiego della triangolazione per localizzare un terminale GSM

Per poter localizzare con ragionevole sicurezza e precisione un cellulare è quindi necessario disporre di informazioni ben più ampie rispetto alla sola conoscenza della BTS (o settore di BTS) cui esso risulta connesso. Le soluzioni attualmente in uso si basano su misure di potenza e/o di tempi di propagazione effettuate sul segnale emesso dal cellulare e ricevuto sia dalla BTS cui è connesso sia dalle BTS che si trovano nelle vicinanze. Tali misure permettono di valutare la distanza del cellulare rispetto a 3 o più BTS. Complicate procedure tecnico-matematiche basate sul principio della “triangolazione” elaborano tali

informazioni e forniscono una stima “abbastanza” precisa della posizione del cellulare.

Tuttavia, poiché il GSM non è progettato per scopi di localizzazione allora occorre estrarre da ciascuna delle BTS i dati relativi al segnale ricevuto e poi utilizzare opportuni strumenti software od hardware, aggiuntivi rispetto agli apparati GSM esistenti, per effettuare la localizzazione. Normalmente tali dati non sono disponibili né vengono memorizzati, per cui la procedura di localizzazione richiede preventivi accordi con i gestori telefonici per organizzare l’operazione. Non ci addentriamo in dettagli ulteriori, il lettore interessato può fare riferimento, ad esempio, ai documenti [7] [8] [9].

7. Utilizzo delle registrazioni telefoniche per il monitoraggio del P.S.E. (Psicological Stress Evaluation)

Altra utilizzazione quanto mai utile per l’individuazione degli eventuali atteggiamenti di simulazione, menzogna e/o controllo rigido delle espressioni vocali per attività di staging, è l’utilizzo delle registrazioni telefoniche o delle intercettazioni telefoniche ad hoc.

Il P.S.E. (Psicological Stress Evaluation [10]) consiste in un apparecchio portatile che contrariamente al lie detector mediante poligrafo il quale richiederebbe una diretta applicazione al corpo dell’esaminando con la risposta elettrotermica, respiratoria e pressoria, nonché richiederebbe alla singola domanda soltanto una risposta affermativa o negativa (SI/NO), può viceversa effettuare tutto un monitoraggio delle modulazioni di frequenza involontarie della voce risultanti da un microtremore, con frequenza di 8-14 cicli al secondo, che normalmente accompagnano l’attività di ogni muscolo volontario compresi quelli che entrano a far parte della fonazione. Allorquando la situazione diviene stressante, il microtremore è soppresso, finché non viene nuovamente ristabilito il normale stato di serenità.

La valutazione ovviamente deve tener conto del “baser line“, cioè la linea emozionale di base del singolo soggetto, variabile caso per caso, allo scopo di evitare distorte interpretazioni falsate da quello che potrebbe viceversa rappresentare il normale stato emotivo del soggetto in disamina.

Uno dei primi apparecchi venne fornito dai servizi USA in occasione del sequestro Moro al ben preciso scopo di appurare se le telefonate estorsive che giungevano alla famiglia Moro erano degne di attenzione oppure francamente simulate.

Bibliografia

[1] L. Hanzo, R. Steele, The Pan-European Mobile Radio System, 1997.

[2] Dispense del corso di *Comunicazioni Mobili* del prof. Cusani, Università di Roma La Sapienza, 2009

[3] O. Bertazzoli, L. Favalli, *GSM*, Hoepli 1996

[4] S. Y. Willassen, *Forensics and the GSM mobile telephone system*, International Journal of Digital Evidence Spring 2003, Volume 2, Issue 1

[5] A.R. Mishra (ed.), Advanced Cellular Network Planning and Optimisation, 2004

[6] J. Bajada, Mobile Positioning for Location Dependent Services in GSM Networks

[7] F. Luciani, *Analisi delle tecnologie di supporto alla domotica e alla localizzazione in un contesto di utenti mobili*, Tesi di Laurea in Ingegneria delle Telecomunicazioni, Università di Roma La Sapienza, relatore prof. R. Cusani, 2007.

[8] P.N. Pathirana, A.V. Savkin, S. Jha; Location estimation and trajectory prediction for cellular networks with mobile base stations; Vol. 53, Issue 6, Nov. 2004 Page(s):1903 – 1913.

[9] W. Buchanan, J. Munoz, R. Manson, K. Raja; *Analysis and migration of location-finding methods for GSM and 3G networks*; 3G Mobile Communication Technologies, 2004. 3G 2004. Fifth IEE Intern. Conf. on 2004 Page(s):352 – 358

[10] V. Mastronardi, *Il P.S.E: un nuovo strumento per l'accertamento della verità; utilizzazioni in Medicina legale*, Psichiatria e Criminologia. Rassegna di Criminologia, vol. XVII, 1986 Fascicolo 2, Pagine 365-386

Biografie

Roberto Cusani è professore Ordinario di Telecomunicazioni presso il Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni (DIET) della Facoltà di Ingegneria dell'Informazione, Informatica e Statistica, Università degli Studi di Roma "La Sapienza" dove è titolare di corsi di Telecomunicazioni, Comunicazioni Mobili e di Teoria dell'informazione e codici.

Egli opera nel settore dell'ICT (Information and Communication Technologies) occupandosi in particolare di sistemi di telecomunicazione digitali fissi e mobili e di tecnologie per le investigazioni anti-crimine.

Laureatosi in Ingegneria Elettronica, consegue il titolo di Dottore di Ricerca in Ingegneria dei Sistemi e delle Comunicazioni. A seguito di pubblici concorsi diventa prima ricercatore universitario, poi Professore Associato infine Professore Ordinario. Dal 2003 al 2009 è Direttore del Dipartimento. Nel 2000 è consulente per il Governo nella gara per le licenze cellulari UMTS. Nel 2006 fonda il consorzio CRAT per la Ricerca nell'Automatica e nelle Telecomunicazioni. Autore di 4 brevetti internazionali riguardanti apparati per telecomunicazioni.

Autore di un libro sulle radio digitali, uno sui segnali ed uno sui codici per rivelazione e correzione di errori. Autore di più di 150 pubblicazioni scientifiche internazionali.

Responsabile di decine di Contratti e Progetti di Ricerca. Esperto di valutazioni tecnico-economico di progetti di ricerca industriale ed accademica presso enti pubblici e privati. Consulente Tecnico per cause giudiziarie civili e penali.

Email: roberto.cusani@uniroma1.it

Vincenzo Mastronardi, Psichiatra, Psicoterapeuta, Criminologo clinico, Titolare della Cattedra di "Psicopatologia forense", Direttore dell'Osservatorio dei Comportamenti e della Devianza", e del "Master in Scienze Criminologico forensi" presso la Facoltà di Medicina e Odontoiatria della Sapienza Università di Roma (Dipartimento di Neurologia e Psichiatria).Autore di 260 lavori, e 26 libri in tema di criminologia, psicopatologia forense, psicoterapia e sulla "comunicazione" con più case editrici tra cui: Manuale per Operatori Criminologici e Psicopatologi Forensi. Quinta Edizione, Giuffrè Editore, 2012 pp. 443, con Sante A. Bidoli, Monica Calderaro Grafologia Giudiziaria e Psicopatologia forense. Metodologia di indagine del falso grafico e la capacità di intendere e di volere dalla grafia. Giurisprudenza. Giuffrè Editore 2010 pp. 297., in coll. con G.B. Palermo) Il Profilo Criminologico. Dalla Scena del Crimine ai Profili socio psicologici, Giuffrè ed. 2005 pp.385 con R. De Luca I Serial Killer, Newton & Compton 2013 pp.860 E' Direttore responsabile della Rivista <<Rassegna di Psicoterapie. Ipnosi. Medicina Psicosomatica. Psicopatologia forense>> dell'Università Sapienza di Roma. Tra gli altri incarichi ricevuti è Docente presso la Scuola Superiore della Magistratura.

Email: vincenzo.mastronardi@gmail.com