

Image forensics

Lo stato dell'arte

Corso di Perfezionamento

“Computer forensics e investigazioni digitali”

Università di Milano - a.a. 2008-2009

Presentazione finale

20 Maggio 2009

Unimi 20 maggio 2009



Definizioni

“Forensics image analysis is the application of the image science and domain expertise to interpret the content of an image or the image itself in legal matters”

(SWGIT – www.fbi.gov)

L'enorme diffusione di dispositivi ottici digitali rende sempre più importanti analisi di questo tipo

Unimi 20 maggio 2009



Documento informatico

Unimi 20 maggio 2009

Dal Decreto Legislativo 7 marzo 2005, n. 82
pubblicato in G.U. del 16 maggio 2005, n. 112 –
S.O. n. 93 “Codice dell’amministrazione digitale”
aggiornato dal D.Lgs. N 159 del 4 aprile 2006
pubblicato in G.U. del 29 aprile 2006, n. 99 – S.O. n.
105 “Disposizioni integrative e correttive al decreto
legislativo 7 marzo 2005, n. 82 recante codice
dell’amministrazione digitale”

documento informatico:

**La rappresentazione informatica di atti, fatti o
datigiuridicamente rilevanti ai sensi del D.P.R.
10/11/1997 n. 513**



Prove – processo civile

Unimi 20 maggio 2009

- Le immagini digitali rientrano nell'ambito dell'art. 2712 c.c. “riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e in genere ogni altra rappresentazione meccanica di fatti e di cose.”
- Pieno valore probatorio fino al disconoscimento. In caso di contestazione rimangono comunque “elementi di prova” che può essere integrato con altri elementi (Cass. Civ. 11/5/05 n. 9884)



Art. 234 C.p.p.

E' consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante **la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.**
(...)

Unimi 20 maggio 2009



Prove

Art. 189 c.p.p. – Prove non disciplinate dalla legge

Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.



Prove

Ammissibilità ed utilizzabilità delle videoriprese nel processo penale

**Cassazione penale, sezioni unite, 28
marzo 2006, n. 26795**

Unimi 20 maggio 2009



Cassazione penale, sezioni unite, 28 marzo 2006, n. 26795

Le sez. unite sono state richieste di dirimere il contrasto fra i vari orientamenti assunti dalle varie sezioni della medesima corte in ordine alla legalità, e correlativamente, alla **utilizzabilità della prova acquisita attraverso la captazione di immagini** in luoghi di privata dimora.

Unimi 20 maggio 2009



Cassazione penale, sezioni unite, 28 marzo 2006, n. 26795

Due orientamenti:

- 1) pacificamente utilizzabili come prova le immagini tratte da riprese visive in luoghi pubblici, sia se avvenute al di fuori del procedimento, sia se avvenute nell'ambito delle indagini di polizia giudiziaria. Tale posizione si giustifica includendo le videoriprese nella categoria delle prove documentali di cui all'art. 234 c.p.p.

Unimi 20 maggio 2009



Cassazione penale, sezioni unite, 28 marzo 2006, n. 26795

2) le riprese visive effettuate in luoghi pubblici nell'ambito delle prove atipiche previste dall'art. 189 c.p.p. tanto se avvenute al di fuori del procedimento, quanto se avvenute nell'ambito delle indagini.

Unimi 20 maggio 2009



Cassazione penale, sezioni unite, 28 marzo 2006, n. 26795

Le s.u. rilevano a tal proposito una certa «confusione concettuale tra la prova documentale dell'art. 234 c.p.p. e la prova atipica dell'art. 189 c.p.p.» al punto che «talvolta si ha l'impressione che le immagini videoriprese siano considerate al tempo stesso documenti e prove atipiche, cioè documenti formati attraverso una prova atipica»

Unimi 20 maggio 2009



Cassazione penale, sezioni unite, 28 marzo 2006, n. 26795

“solo le videoregistrazioni effettuate fuori dal procedimento possono essere introdotte nel processo come documenti e diventare quindi una prova documentale mentre le altre, effettuate nel corso delle indagini, costituiscono, secondo il codice, la documentazione dell’attività investigativa, e non documenti».

Unimi 20 maggio 2009



Cassazione penale, sezioni unite, 28 marzo 2006, n. 26795

[...] l'obiezione non distingue il mezzo di ricerca della prova, costituito dalla ripresa visiva, dalla videoregistrazione, cioè dal supporto sul quale sono fissate le immagini riprese, fonte di prova, e dal mezzo di prova, che è lo strumento attraverso il quale si acquisisce nel processo il contenuto rappresentativo del supporto, vale a dire quello che sarà l'elemento di prova. Il contraddittorio previsto dall'art. 189 c.p.p. non riguarda la ricerca della prova ma la sua assunzione e interviene dunque, come risulta chiaramente dalla disposizione, quando il giudice è chiamato a decidere sull'ammissione della prova».

Unimi 20 maggio 2009



Dispositivi

Unimi 20 maggio 2009

- Sensori
- Fotocamere
- Videocamere
- Telefonini
- PDA
- Etc etc etc



Analisi delle immagini e dei video digitali 1

- Sono “normali” file
- Metodo 1: dal Filesystem (ovviamente non direttamente sulla macchina oggetto di indagine...)
- Viene visualizzato il contenuto ed eventualmente sottoposto ad editing ed elaborazioni per ingrandire od evidenziare punti di interesse.
- Tutte le operazioni sulle immagini (software - e versione – utilizzato, filtri applicati, opzioni attivate...) devono essere documentate e ripetibili dalla controparte.

Unimi 20 maggio 2009



Analisi delle immagini e dei video digitali 2

Unimi 20 maggio 2009

- Metodo 2: Carving da immagini di memorie di massa (si rinvengono le immagini extra-fs: cache, file temporanei, swap...)
- Es: header per i JPEG/JFIS: FFD8 e FF D8 FF 00 rispettivamente
- Ricostruzione (file cancellati, frammentati)
- Best practices (chain of evidence etc)



Procedure

Unimi 20 maggio 2009

In fase di acquisizione: (p. es. durante le indagini)

I supporti vanno identificati, ne va effettuata la copia forense (hash...) garantendone per quanto possibile l'inalterabilità (se si tratta di dispositivi mobili si pongono tutti i problemi del caso). Idealmente si creano subito le copie da consegnare alle parti; si verbalizza tutta l'attività.



Obiettivi dell'analisi

Gli obiettivi dipendono evidentemente dall'obiettivo dell'attività che si sta svolgendo (indagine, perizia, CTU, ATP, perizia di parte.....)

In generale sono di interesse oggetti e persone presenti nelle immagini, sia in primo piano che nello sfondo della scena.

Dal punto di vista prettamente informatico dell'immagine come file, può essere rilevante ricostruire le eventuali manipolazioni a cui è stato sottoposto.



Formati – Format Analysis

- Introduzione (risoluzione, pixel, RGB etc)
- Lossless
 - Raw, TIFF...
- Lossy
 - JPEG / MPEG...
- Meta data
 - EXIF (info sul dispositivo, data e ore, thumbnail, localizzazione...)
 - Altri: standard IPTC
 - Antiforensics: sono in chiaro...

Unimi 20 maggio 2009



JPEG – il formato più diffuso

Occorre esaminare :

- il contenuto cioè lo standard JPEG per la compressione e codifica dei byte dell'immagine in un file;
- lo standard JFIF per l'inserimento nel file jpeg di metadati tecnici per la visualizzazione (risoluzione, spazio colori , thumbnail) e lo scambio tra dispositivi diversi;
- lo standard EXIF per l'inserimento di metadati amministrativi ((marca, modello, seriale, versione del firmware, timestamp, thumbnail opzionale, gps,ecc.)

Unimi 20 maggio 2009



Analisi del contenuto

- Fotogrammetria
 - Oggetti
 - Persone (altezza, lunghezza del passo, anche per l'analisi dell'andatura)
- Ricostruzione di un evento dinamico per mezzo delle immagini (incidenti)

Unimi 20 maggio 2009



Analisi del contenuto

- Riconoscimento di oggetti presenti nella scene
- Classificazione delle scene
- Algoritmi di elezione: Reti Neurali (ANNs)
 - Necessità: ampi db e training dei sistemi...

Unimi 20 maggio 2009



Manipolazioni

- Problema: verificare con una procedura scientificamente valida (e validata....) se un file immagine è stato alterato
- Metodi:
 - Error level analysis
 - Analisi delle fonti di luce
 - Video: id doppie compressioni MPEG
 - Wavelets

Unimi 20 maggio 2009

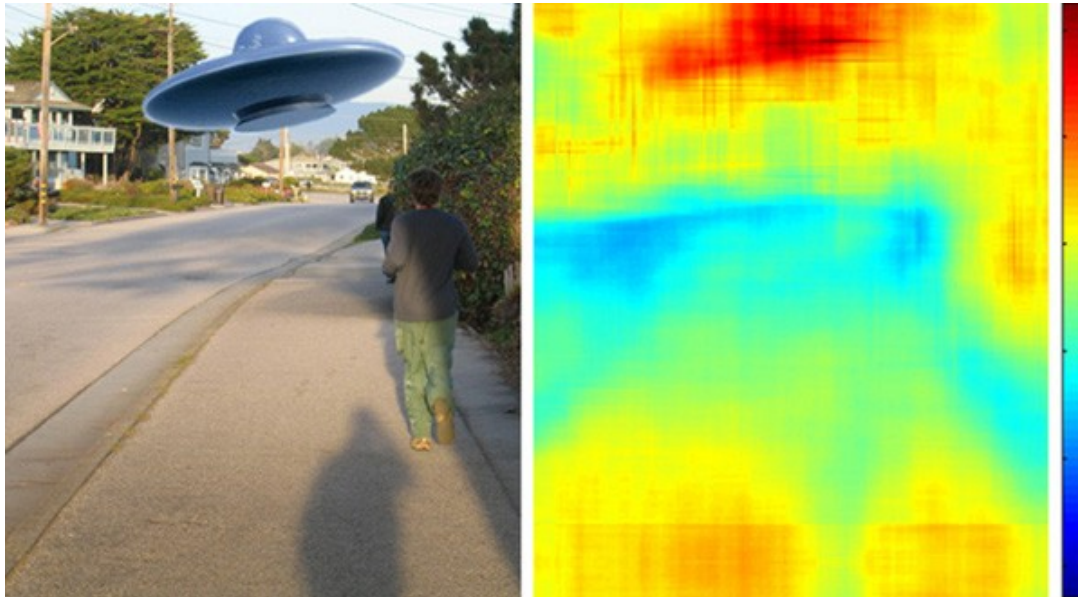


Manipolazioni

Analisi del livello di errore

Farid - <http://www.cs.dartmouth.edu/farid/maat/>

Unimi 20 maggio 2009



Manipolazioni

Analisi delle fonti di luce (light sources analysis)

Farid - <http://www.cs.dartmouth.edu/farid/maat/>

Unimi 20 maggio 2009



Analisi del contenuto

- Classificazione: altre tecniche
- Dominio delle frequenze - DCT

Unimi 20 maggio 2009



Analisi del contenuto

- Riconoscimento biometrico
- Face recognition
 - PCA: analisi delle componenti (vettoriali) principali
 - successo fino al 96%
 - 3D
 - Video based
 - Eigenfeatures method
 - AAM active appearance model



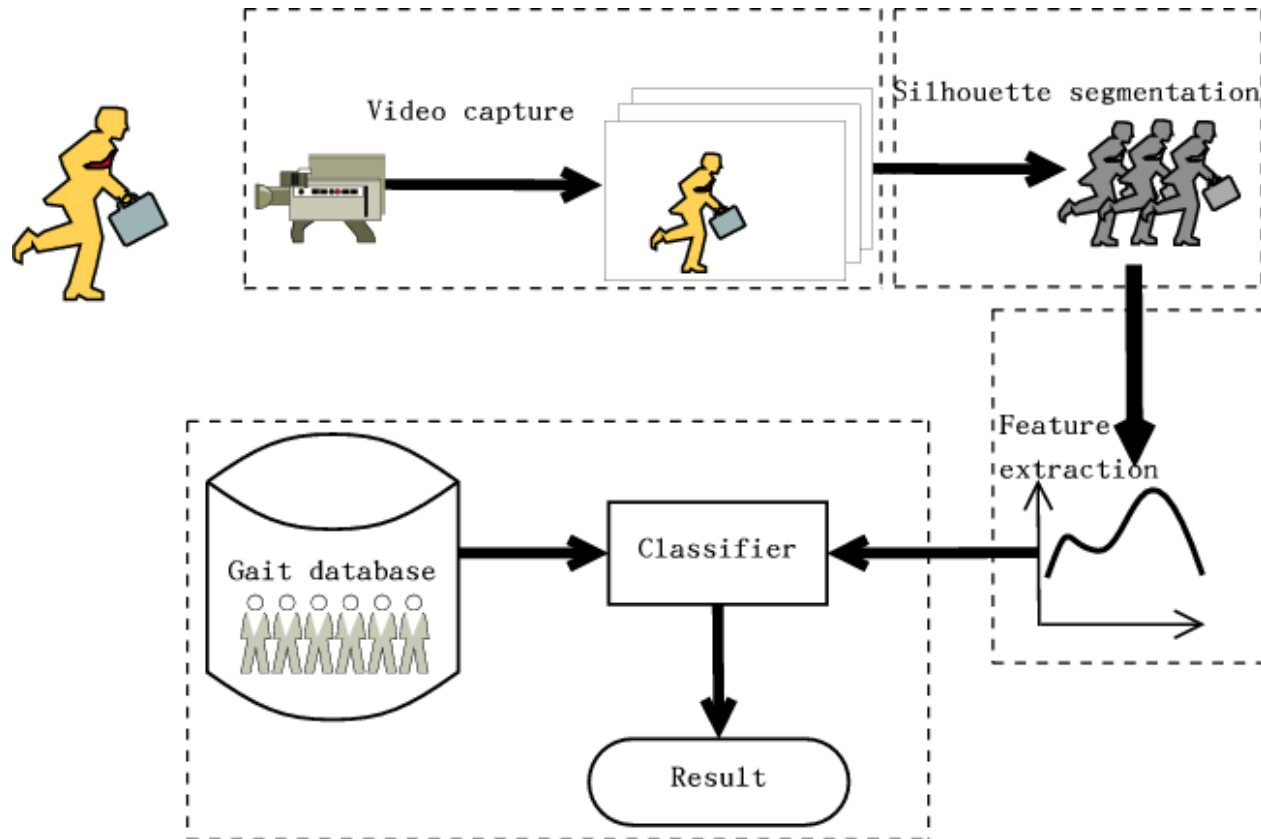
Face recognition: PCA

- 1 – **Preparazione dell'insieme di training**. Immagini delle stesse dimensioni e risoluzione. Le immagini digitali vengono viste matematicamente come matrici oppure tutto l'insieme può essere visto come una grande matrice.
- 2 – **Calcolo** dell'immagine **media** e calcolo delle **differenze** per ogni immagine (matrice) nell'insieme.
- 3 – **Calcolo autovettori e autovalori** (della matrice di covarianza...) Gli autovettori hanno le stesse dimensioni delle immagini originali → sono chiamati *eigenfaces* nella letteratura anglosassone. Gli autovettori **esprimono “quanto” e “come” ogni immagine differisce dalla media**.
- 4 – **Scelta dei componenti principali** dell'insieme di autovettori (e autovalori): quelli con l'autovalore associato più alto. In questo modo si perde informazione ma usualmente bastano 100-150 *eigenfaces* per l'identificazione.
- 5 – Riconoscimento: **si proietta l'immagine (normalizzata e sottratta) da riconoscere sugli autovettori, registrando quanto differisce dalla media**.



Gait recognition

Parametri che possono essere usati per l'identificazione degli individui: spaziali temporali (lunghezza del passo, larghezza del passo, velocità...), cinematici (rotazione delle articolazioni, media degli angoli di rotazione dell'anca/ginocchio/caviglia e tronco/coscia/piede). Alta correlazione inoltre tra lunghezza del passo e altezza (vedi fotogrammetria)



Unimi 20 maggio 2009



Immagini digitali e biometria due esempi in Italia...

Unimi 20 maggio 2009

- Provv. Garante 1/2/2007: “Come già affermato da questa Autorità, l'utilizzo di dati biometrici risulta giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati.” (Nella fattispecie impronta del palmo e foto)
- Deve essere quindi valutata la liceità del sistema, unitamente ai principi di necessità, proporzionalità, finalità e correttezza (artt. 3 e 11 del Codice).
- È possibile trattare dati biometrici dei dipendenti per specifiche e rilevanti finalità, come ad esempio la salute pubblica. È quanto ribadito dal Garante (provvedimento 15/2/2008) nel ritenere lecito e conforme alla disciplina privacy il sistema di rilevazione biometrica proposto da una società di risorse idriche. (impronte digitali)



Image “ballistics”

- Attribuzione di un'immagine digitale al dispositivo che l'ha create
- ID del sensore (sensor noise, pixel difettosi)
- Q Tables – Identificazione della fotocamera o del software che ha creato il file (per i file JPEG)

Unimi 20 maggio 2009



Child Pornography

- Identificazione automatica delle immagini CP
 - % di pixel colorati come la pelle
 - Identificazione scene (applicazione specifica degli algoritmi visti prima)
 - ANN (reti neurali)

Unimi 20 maggio 2009



Off-topic

- Falsificazioni: reali e digitali
- Tecniche di image forensics possono essere applicate all'identificazione di opere d'arte falsificate
- Watermarking: verificare le frodi – tecnica alternativa - meno invasiva - al DRM

Unimi 20 maggio 2009



Image enhancement

- Tecniche per migliorare la visione di immagini e video
- Esempio classico: videosorveglianza
 - Convoluzione del video
 - De-interlacciamento
 - Regolazione contrasto e altri parametri
 - etc



Steganografia

- Cos'è la steganografia: uso la parte di dati meno significativi per nascondere contenuto
- Pixel RGB:
- 10010**010** 00111**001** 10101**110**
- **I bit in rosso possono essere alterati senza che ad occhio nudo si noti un significativo cambiamento nell'aspetto dell'immagine.**
- Steganografia come tecnica di antiforensics: vantaggi (o svantaggi a seconda del punto di vista...)
- Steganalisi



Collegamenti

Unimi 20 maggio 2009

- Per sua natura la disciplina si presta – soprattutto nella parte di analisi del contenuto – a collegamenti con altre discipline forensi e non solo
- Analisi dei contenuti e “information filtering”, soprattutto nelle indagini penali: la necessità dell'intervento di esperti nei vari settori e investigatori → si tratta di attività che porta alla formazione di prove



Bibliografia Breve

Unimi 20 maggio 2009

- Farid, H. - “Digital forensics: how experts uncover doctored images” - Scientific American, Giugno 2008
- Farid, H. - Gli articoli scientifici su:
www.cs.dartmouth.edu/farid/maat/
- Turk, M. e Pentland, A. - “Face recognition using eigenfaces” - Proc. IEEE Conference on Computer Vision and Pattern Recognition: 586–591
- Yu, S. e Tan, T - “Gait recognition” -
www.scholarpedia.org/article/Gait_recognition, 2007
- Gabrini, Davide – JPEG Forensics – 2009 – Presentazione tenuto nell'ambito di questo corso - www.tipiloschi.net

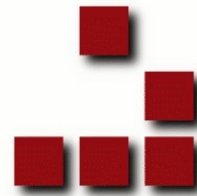


Unimi 20 maggio 2009

Presentazione scaricata dal sito:

www.studioag.eu

Consulenze tecniche e perizie in materia di
informatica e telecomunicazioni.



Contatti:

studio@studioag.eu

Tel. +39 0444 1801364

Fax. +39 0444 1801365

