Relazione Tecnica

Seconda Prova

Studente Luigi di Corrado
667/003106

Image Forensics

Premessa

Le operazioni eseguite in questa relazione sono state effettuate su delle copie dei file reperto che sono stati ricevuti all'interno di un archivio in formato "rar". Tutti i rapporti generati con i software sono allegati nella cartella " Rapporti". Tutte le immagini processate sono allegate nella cartella " Immagini".

Introduzione dei software utilizzati

Cominciamo introducendo i due software che utilizzeremo durante lo svolgimento dell'analisi dei reperti, AMPED five e JPEG Snoop

Amped Five
versione di prova

Amped Five è un software di elaborazione video sviluppato per venire incontro alle esigenze dell'ambito investigativo, forense e della pubblica sicurezza. Si tratta di uno strumento completo per elaborare ed analizzare immagini e filmati in formato digitale. Alcune delle principali funzionalità di Amped Five sono:

- Caricamento, salvataggio, elaborazione e conversione di immagini, sequenze di immagini e filmati.
- Aggiunta, configurazione, spostamento, modifica di un numero illimitato di filtri in tempo reale anche durante la riproduzione di un filmato.
- Applicazione automatica della stessa sequenza di filtri a file differenti.
- Modifica istantanea di qualsiasi passo dell'elaborazione con visualizzazione immediata del risultato.
- Generazione automatica di report dell'elaborazione.

Altre informazioni sono reperibili dal sito: http://www.amped.it/

JPEG Snoop
versione 1.5.2

JPEG Snoop è un piccolo software che analizza i dati Exif della foto e grazie all'identificazione della compressione usata esegue un confronto per stabilire se la foto è stata ritoccata o meno.
Altre informazioni sono reperibili dal sito:
http://www.impulseadventure.com/photo/jpeg-snoop.html

Autenticità dei reperti

Prima di iniziare ad analizzare i file bisogna calcolare l'**Hash** code di essi, in questo modo sarà possibile dimostrare che il file soggetto alle operazioni è unico e autentico, quindi resterà una prova valida ed attendibile per il processo.

L'archivio "caso06.rar" contiene tre file immagine di tipo jpg elencati di seguito:

- 2 perspective license plate.jpg
- 144_445917165.jpg
- 3D_IMG_0933.jpg

Rispettando l'ordine dell'elenco, utilizzeremo per comodità i nomi **Reperto1, Reperto2** e **Reperto3** per identificare i file sopracitati.

Utilizzando Amped Five abbiamo calcolato i codici di Hash dei file:

- Reperto1 = 56B0704ED2CC8149B8C9587A7C45EE81
- Reperto2 = F0492E533512499AB696879E27466337
- Reperto3 = AA6E0BE4B0560C160D81AF2766985641

Image Forensics

Iniziamo definendo alcuni obbiettivi da compiere per ogni reperto ricevuto.

Obiettivi

- Analizzare i dati Exif dei file.
- Recuperare informazioni utili per l'individuazione di luoghi, veicoli ed eventuali soggetti presenti.
- Generare un rapporto.

Svolgimento delle operazioni

Reperto1

Iniziamo ad anailizzare il primo file ("2 perspective license plate.jpg")
Hash code: **56B0704ED2CC8149B8C9587A7C45EE81**

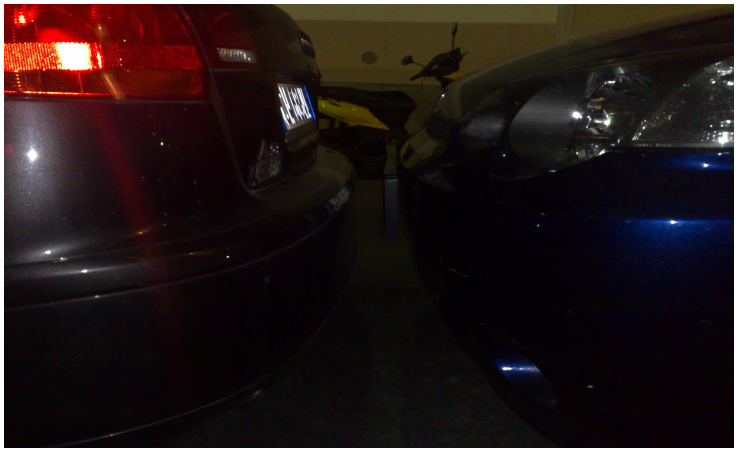

Figura 1 – il file "2 perspective license plate.jpg" aperto

La foto mostra la parte posteriore di un'auto e subito dopo la parte anteriore di una seconda vettura, si nota subito che la targa di quest'ultima viene riflessa sul telaio della prima auto.
Prima di iniziare il recupero delle targhe, controlliamo se questo file ha subito delle modifiche utilizzando JPEG Snoop.

Il risultato prodotto dal programma è il seguente:

```
*** Searching Compression Signatures ***

  Signature:           0155D875C95B74D0F3C5835A62516F48
  Signature (Rotated): 01D38A25358EB7649A254E19F1D46600
  File Offset:         0 bytes
  Chroma subsampling:  2x1
  EXIF Make/Model:     OK    [Nokia] [N95 8GB]
  EXIF Makernotes:     OK
  EXIF Software:       NONE

  Searching Compression Signatures: (3327 built-in, 0 user(*) )

          EXIF.Make / Software         EXIF.Model                          Quality           Subsamp Match?
          -------------------------    ----------------------------------  ----------------  --------------
     CAM:[NIKON                    ] [E2500                            ] [FINE            ] Yes
     CAM:[Nokia                    ] [N73                              ] [                ] Yes
     CAM:[OLYMPUS OPTICAL CO.,LTD  ] [C2000Z                           ] [                ] Yes
     CAM:[OLYMPUS OPTICAL CO.,LTD  ] [C3040Z                           ] [                ] Yes
     CAM:[PENTAX                   ] [PENTAX Optio 550                 ] [                ] Yes
     CAM:[Research In Motion       ] [BlackBerry 8100                  ] [                ] Yes
     CAM:[SEIKO EPSON CORP.        ] [PhotoPC 3000Z                    ] [                ] Yes
     SW :[IJG Library              ]                                     [085             ]
     SW :[Picasa                   ]                                     [085 (Normal)    ]
     SW :[ZoomBrowser EX           ]                                     [medium          ]

    The following IJG-based editors also match this signature:
     SW :[GIMP                     ]                                     [085             ]
     SW :[IrfanView                ]                                     [085             ]
     SW :[idImager                 ]                                     [085             ]
     SW :[FastStone Image Viewer   ]                                     [085             ]
     SW :[NeatImage                ]                                     [085             ]
     SW :[Paint.NET                ]                                     [085             ]
     SW :[Photomatix               ]                                     [085             ]
     SW :[XnView                   ]                                     [085             ]

  Based on the analysis of compression characteristics and EXIF metadata:

  ASSESSMENT: Class 4 - Uncertain if processed or original
              While the EXIF fields indicate original, no compression signatures
              in the current database were found matching this make/model
```

Figura 2 – Risultato di Jpeg spoon sul reperto 1

Questi dati indicano che la foto è stata scattata da un dispositivo mobile *Nokia N95 da 8Gb,* dai confronti eseguiti dal programma, risulta una valutazione di livello 4, significa che il programma è incerto se la foto è stata ritoccata o meno, ciò fa presumere che l'immagine sia originale (solitamente una valutazione di Livello 1 o 2 , indica che l'immagine è ritoccata).
Passiamo adesso al recupero delle informazioni utilizzando Amped Five, iniziamo un nuovo progetto e carichiamo il file.

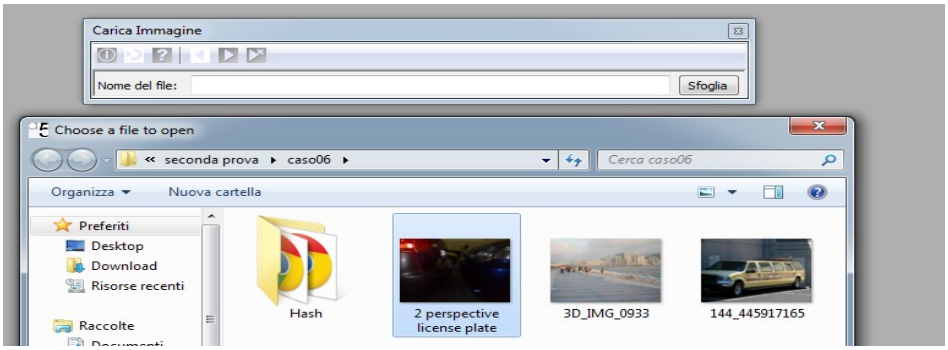

Figura 3 – Caricamento del file su Amped five

Come avevamo sopracitato, ci sono due targhe da identificare, una delle quali è riflessa sul telaio della prima auto. Iniziamo dalla targa posteriore dell'auto a sinistra.
Utilizzeremo un filtro per sistemare la prospettiva della targa in modo da renderla più leggibile.

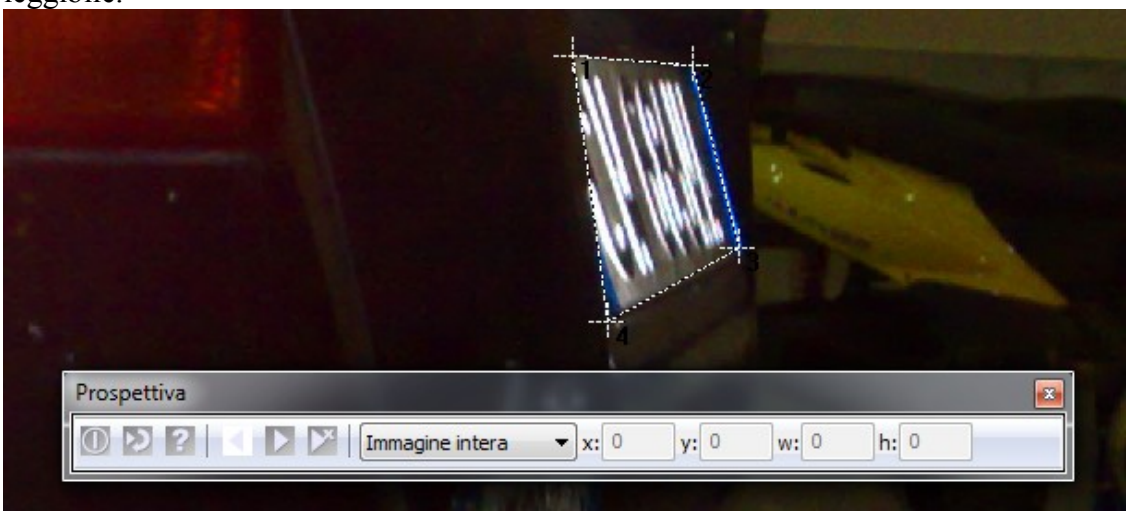

Figura 4 – Impostazione del filtro per modificare la prospettiva

L'utilizzo del filtro " Prospettiva" ci indica di scegliere quattro punti dove applicare l'effetto. Questi punti devono essere presi in un ordine ben preciso, il primo punto deve essere preso in alto a sinistra, il secondo in alto a destra, il terzo in basso a destra e il quarto in basso a sinistra.
Applicando il filtro otteniamo questo risultato:

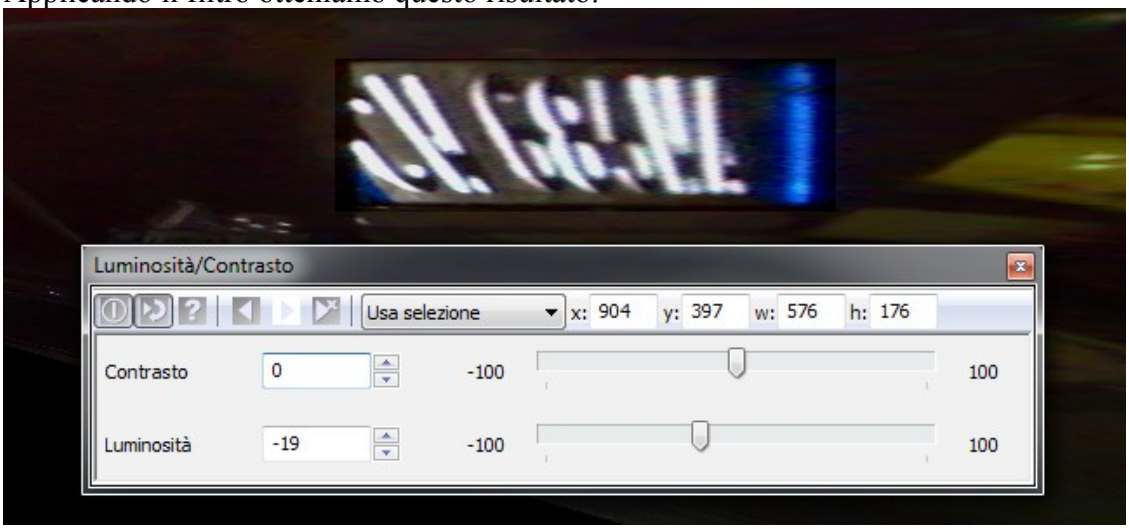

Figura 5 – La targa posteriore con la nuova prospettiva

Adesso la nostra targa risulta più leggibile, sistemando un po la luminosità riusciamo a identificare i simboli che la compongono, **CW 685WA**

Gli stessi passi vanno eseguiti per la targa riflessa sul telaio, ma bisogna tenere presente alcuni accorgimenti. Essendo riflessa su una superfice lucida e non piana, la targa risulterà "specchiata" e distorta. Applicando l'effetto specchio possiamo ottenere i simboli, scritti nella giusta direzione.

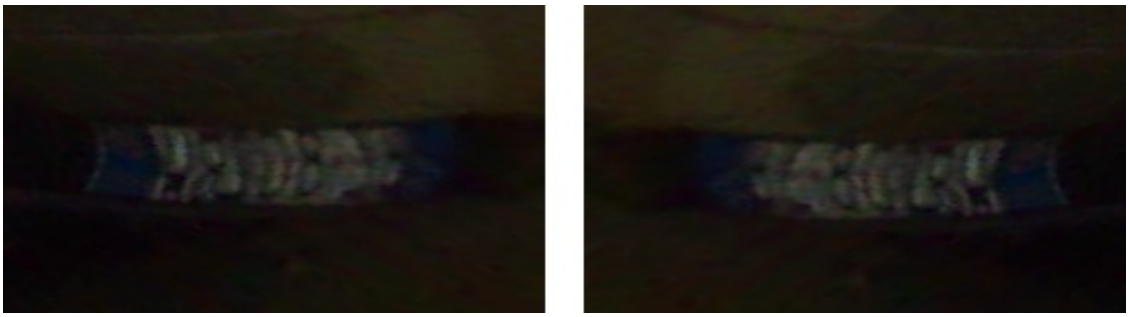

Figura 6 – A sinistra la targa riflessa sul telaio , A destra è stato applicato l'effetto specchio

Ecco che si inizia a intravedere qualcosa, applicando una " Maschera di contrasto " possiamo aumentare ulteriormente i dettagli e la qualità.

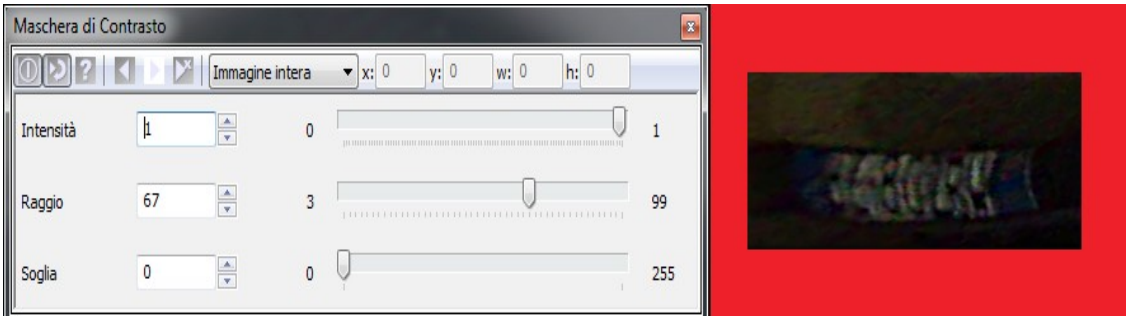

Figura 7 – La targa è più nitida dopo aver applicato la Maschera di Contrasto

Schiariamo un po l'immagine regolando luminosità e contrasto e aggiustando le curve.

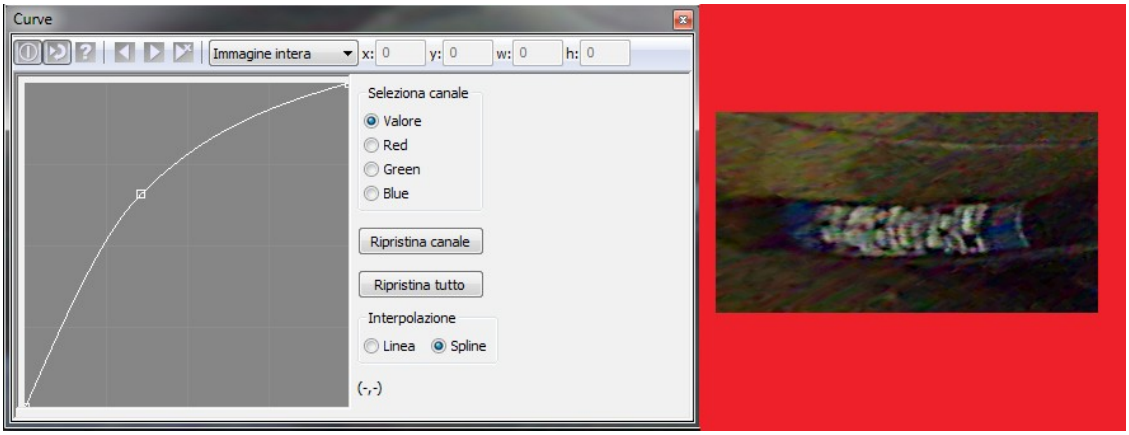

Figura – 8 Situazione finale dopo le varie regolazioni

Adesso la targa è abbastanza leggibile : **BZ 802RW**

Come fase finale Generiamo il rapporto e scriviamo l'immagine su file,sempre dal programma, File > Genera Report, per scrivere l'immagine usiamo la funzione " Scrivi Immagine " presente all'interno della cartella " scrivi file " di Amped e utilizziamo un formato non compresso (TIFF o BMP).

Come premesso le immagini processate ed i report dei software sono allegati e presenti nella cartella "Immagini" e "Rapporti".

Reperto2

Passiamo adesso al secondo file (“144_445917165.jpg”)
Hash code: **F0492E533512499AB696879E27466337**

Figura 9 – Il Reperto 2 raffigura un'auto straniera

Anche questa foto ha una targa in prospettiva e oscurata, controlliamo se è stata modificata.

```
*** Searching Compression Signatures ***

  Signature:           0182408A81A4ABF04D4A34A8A5E98C58
  Signature (Rotated): 012D821C6AB210E2A753BE053B8F55D0
  File Offset:         0 bytes
  Chroma subsampling:  2x2
  EXIF Make/Model:     NONE
  EXIF Makernotes:     NONE
  EXIF Software:       NONE

  Searching Compression Signatures: (3327 built-in, 0 user(*) )

          EXIF.Make / Software        EXIF.Model                          Quality           Subsamp Match?
          -------------------------   ---------------------------------   ---------------   --------------
     CAM:[SONY                      ] [CYBERSHOT U                      ] [               ] Yes
     SW :[Adobe Photoshop 7.0       ]                                     [Save As 07       ]
     SW :[Apple Quicktime           ]                                     [0466-0467        ]
     SW :[Digital Photo Professiona]                                      [05               ]
     SW :[IJG Library               ]                                     [075              ]
     SW :[MS Paint                  ]                                     [                 ]
     SW :[MS Visio                  ]                                     [                 ]
     SW :[ZoomBrowser EX            ]                                     [low              ]

    The following IJG-based editors also match this signature:
     SW :[GIMP                      ]                                     [075              ]
     SW :[IrfanView                 ]                                     [075              ]
     SW :[idImager                  ]                                     [075              ]
     SW :[FastStone Image Viewer    ]                                     [075              ]
     SW :[NeatImage                 ]                                     [075              ]
     SW :[Paint.NET                 ]                                     [075              ]
     SW :[Photomatix                ]                                     [075              ]
     SW :[XnView                    ]                                     [075              ]

  Based on the analysis of compression characteristics and EXIF metadata:

  ASSESSMENT: Class 1 - Image is processed/edited
```

Come risulta dal rapporto di Jpeg spoon, la valutazione ha avuto esito di livello 1 e quindi l'immagine è stata modificata. Presumiamo che la modifica apportata riguardi la zona dove è presente la targa, dove potrebbe essere stato applicato un filtro per renderla più buia.
Carichiamo il nuovo reperto su Amped, con la funzione di "Ritaglia" ritagliamo la parte di immagine interessata (la targa) e aumentiamo un po la luminosità sistemando la curva per ottenere questo risultato:

Figura 10 - la targa risulta piu chiara ma è molto sfocata

Notiamo che l'immagine è molto sfocata e ci sono pochi dettagli, i pixel sembrano mossi sicuramente si tratta di una lieve sfocatura da movimento. Applichiamo il filtro per rimuovere la " sfocatura da movimento" e poi utilizziamo la Prospettiva per allineare bene la nostra targa.

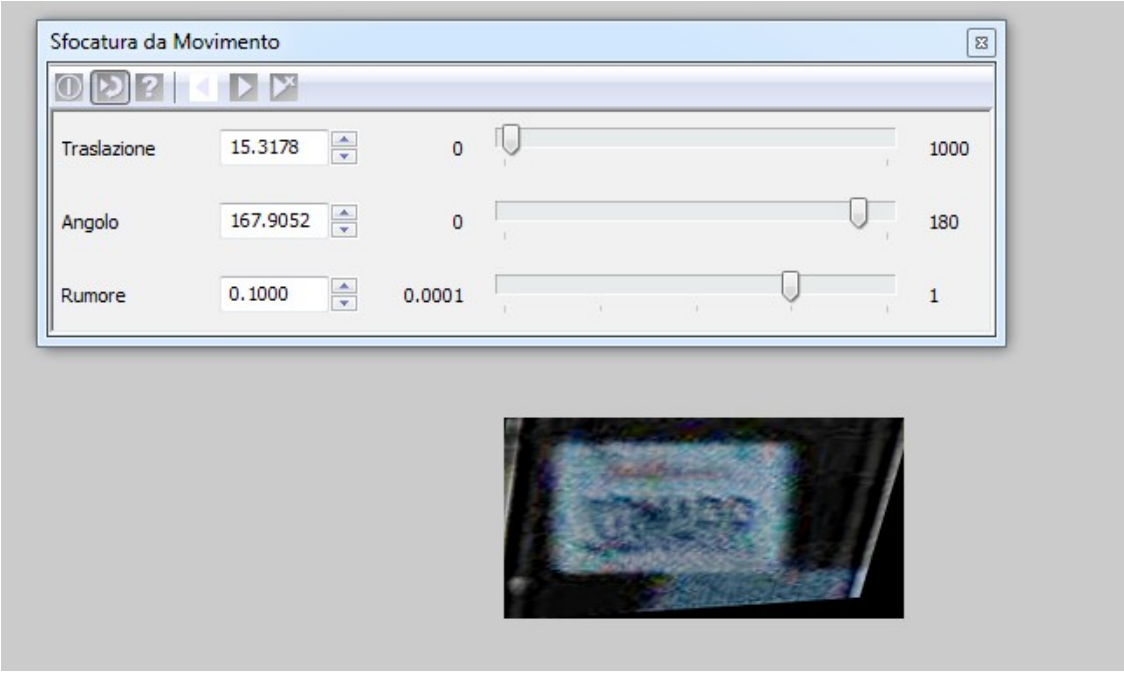

Figura 11 – Applicazione del filtro per rimuovere la sfocatura da movimento

Purtroppo non possiamo migliorare oltre o rischiamo di peggiorare la qualità. Dal risultato ottenuto presumiamo che la targa sia **SONARR**.
Salviamo e Generiamo il rapporto e scriviamo l'immagine.

Reperto3

Concludiamo con l'ultimo file dell'archivio (“3D_IMG_0933.jpg”)
Hash code: **AA6E0BE4B0560C160D81AF2766985641**

Figura 12 – foto scattata da un turista

Questo file mostra una foto scattata da un presunto turista, essa raffigura un gruppo di persone che passeggiano in una zona portuaria. Il nostro compito questa volta sarà quello di ricostruire la scena ed effettuare delle misure. Prima di iniziare le misure controlliamo i dati exif del file.

```
*** Searching Compression Signatures ***

  Signature:           01A84EC0DDFAE937A0336DB825C85028
  Signature (Rotated): 01A9B171AA8560DD8EA55A93D29361E4
  File Offset:         0 bytes
  Chroma subsampling:  2x1
  EXIF Make/Model:     OK   [Canon] [Canon DIGITAL IXUS 120 IS]
  EXIF Makernotes:     OK
  EXIF Software:       NONE

  Searching Compression Signatures: (3327 built-in, 0 user(*) )



ASSESSMENT: Class 4 - Uncertain if processed or original
            While the EXIF fields indicate original, no compression signatures
            in the current database were found matching this make/model
```

Questa foto è stata scattata da una Canon Digital IXUS 12 IS e anche questa volta la valutazione del programma è di livello 4 quindi potrebbe essere originale.

Apriamo un nuovo progetto con Amped e carichiamo l'immagine.
Premesso che quando si effettuano delle misurazioni in un'immagine si deve tenere in considerazione che il mondo reale non è planare, ma è una complessa struttura tridimensionale. Inoltre, la stima di distanze relative al mondo reale è complicata dal fatto che, nel processo di produzione di un'immagine, lo spazio tridimensionale viene proiettato in un'immagine bidimensionale, con eventuali perdite di informazione. E' necessario perciò, ricostruire la geometria tridimensionale della scena e misurare alcune delle sue caratteristiche mediante il filtro " Misurazione 3d".

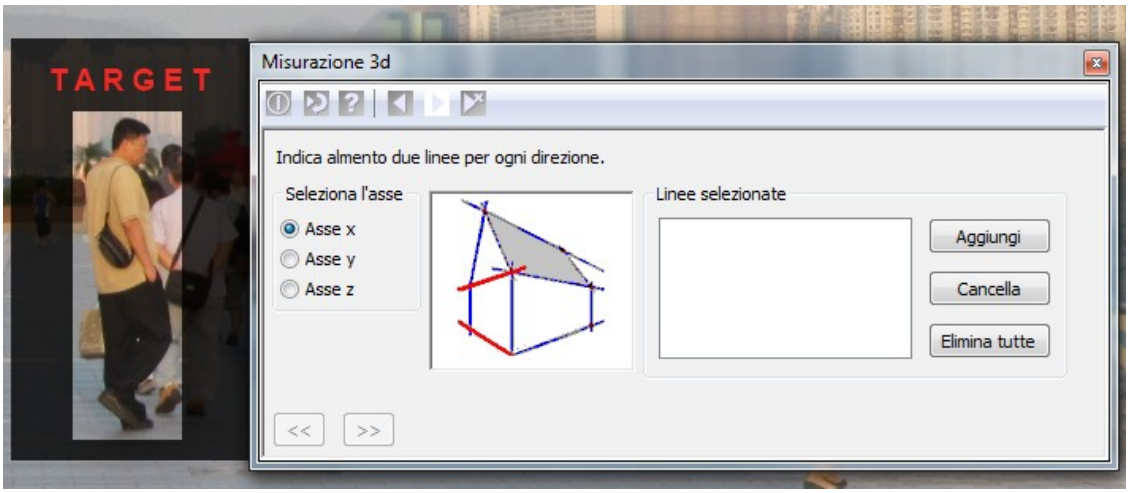

Figura 13 - Finestra di impostazioni per la funzione di Misurazione 3D; accanto l'obbiettivo

Esaminiamo la prima fase della configurazione del filtro: la ricostruzione della scena. Ricostruire la scena significa recuperare l'informazione relativa alla tridimensionalità della scena a partire dall'immagine. A tal fine è necessario identificare alcune informazioni strutturali relativi agli oggetti della scena, in particolare è necessario specificare un insieme di linee per ciascuna dimensione dello spazio tridimensionale. Queste linee devono giacere sullo stesso piano ed essere parallele nel mondo reale.

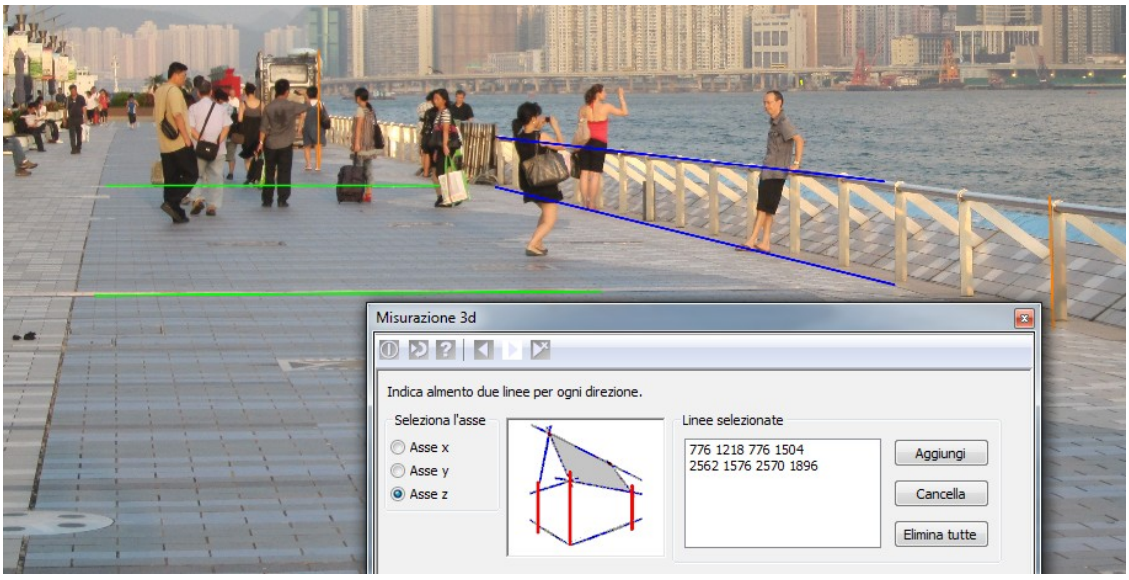

Figura 14 – Ricostruzione della scena tridimensionale

Le linee blue rappresentano l'Asse X, quelle verdi l'Asse Y e le arancioni l'Asse Z.

Fatto ciò possiamo passare alla fase successiva:la definizione della distanza di riferimento. Dato che vogliamo misurare l'altezza della persona illustrata nell'immagine, dovremo utilizzare l'asse Z come asse di riferimento e specificare nell'immagine due punti di cui conosciamo la distanza. Prendiamo come riferimento per i due punti, uno dei paletti verticali a destra della ringhiera tracciando i due punti partendo dal basso verso l'alto e ipotizziamo che sia alto 80cm.

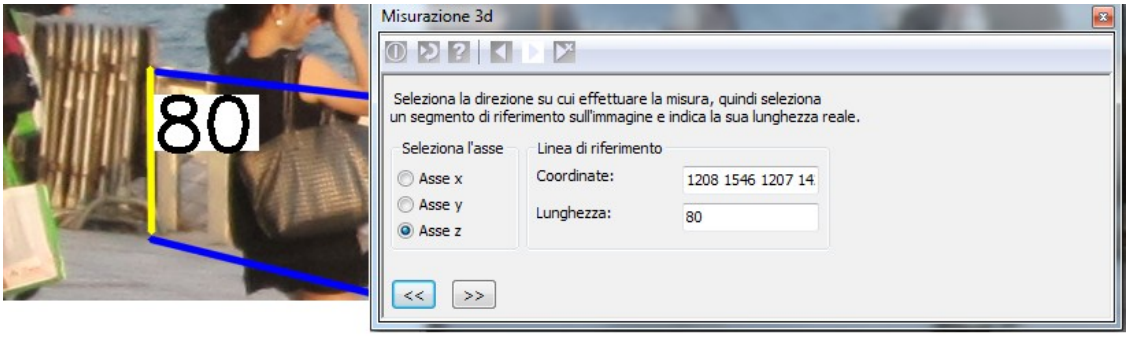

Figura 15 – Altezza di riferimento

Infine come fase finale possiamo tracciare la linea di misurazione per ricavare l'altezza del nostro individuo, partendo dalla pianta del piede come primo punto, fino ad arrivare al capo della testa come secondo punto. Verrà visualizzata l'altezza ipotetica calcolata in base alle linee che abbiamo tracciato nelle fasi precedenti e ci verrà fornito anche un margine d'errore.

Figura 16 - Risultato delle misure

Nel nostro caso l'individuo misura **182,113cm** con un margine di errore del **6,037cm**. Salviamo il progetto e generiamo il rapporto.

Conclusioni

Reperto 1 – Hash (56B0704ED2CC8149B8C9587A7C45EE81):

- **Targa 1 – CW 685WA**
- **Targa 2 – BZ 802RW**

Reperto 2 – Hash (F0492E533512499AB696879E27466337):

- **Targa – SONARR**

Reperto 3 – Hash (AA6E0BE4B0560C160D81AF2766985641):

- **Misura di riferimento = 80 cm**
- **Misura dell'uomo = 182,113 cm**
- **Errore = 6,037 cm**

Glossario

Hash Code: Hashcode del file, calcolato con l'algoritmo MD5. Tale codice è un identificatore, unico e sicuro, utilizzato per verificare l'integrità del file da caricare.

Exif: Exchangeable image file format è una specifica per il formato di file immagine utilizzato dalle fotocamere digitali. I tag di metadato definiti nello standard Exif coprono un vasto spettro includendo:

- Informazioni di date ed ora. Le fotocamere digitali registrano la date e l'orario corrente in questi metadati.
- Impostazioni della fotocamera. Queste includono informazioni statiche come il modello ed il produttore della fotocamera, ed informazioni varie per ciascuna immagine come l'orientamento, l'apertura, la velocità dello scatto, la lunghezza focale, il bilanciamento del bianco, e le informazioni di velocità ISO impostate.
- Una miniatura per visualizzare un'anteprima sul display LCD della fotocamera, nei file manager, oppure nei software di foto ritocco.
- Descrizioni ed informazioni di copyright.

Maggiori informazioni: http://it.wikipedia.org/wiki/Exchangeable_image_file_format

Disponibile per chiarimenti

Catania li 02/06/2011
Luigi di Corrado