Relazione Tecnica
Analisi Forense Immagini Digitali

Andrea Cannella

2 giugno 2011

Indice

Elenco delle figure

1 Premessa

Il lavoro è stato svolto seguendo le best practice dell'analisi forense. I file acquisiti sono stati duplicati per evitare manomissioni dei file originali. Si allegano a questa relazione copia dei file originali e dei file modificati in seguito al lavoro svolto.

2 Software

Ai fini dell'analisi forense del materiale multimediale pervenuto, ci si è avvalsi del supporto dei seguenti strumenti software.

2.1 Amped5

Amped Five é un software abbastanza completo per l'elaborazione di immagini e filmati per applicazioni forensi, investigative e di intelligence.

2.2 JPEGsnoop

JPEGSnoop è un semplice programma che consente di capire se un'immagine è stata modificata in qualche modo. L'applicazione legge i dati exif per

consentire di farsi un'idea delle condizioni di scatto. Dopo acquisisce le informazioni sul tipo di compressione utilizzata e le confronta con le applicazioni più famose.

2.3 Jeffrey's Exif Viewer

Si tratta di un tool on line che permette la visualizzazione dei dati presenti nell'Exif dei file JPEG.

3 Analisi Forense

3.1 Prima immagine

3.1.1 File 1 gentsp.png

Figura 1: Prima immagine - Originale

3.1.2 Obiettivi Analisi

Il file presenta un rumore periodico. Obiettivo dell'analisi è quindi rimuovere il rumore.

3.1.3 Analisi

Al fine di rimuovere il rumore presente si è analizzata la trasformata di Fourier. La DFT (Discrete Fourier Transformat) è una trasformata che ci permette di passare al dominio delle frequenze. Dall'analisi della DFT sono emersi dei punti rumorosi. Eliminati essi l'immagine è risultata nitida e senza rumore. Il problema è stato individuato e rimosso con successo. In allegato a questa relazione il report generato da Amped5 e l'immagine ottenuta.

Figura 2: Prima immagine - Dopo miglioramento

3.2 Seconda immagine

3.2.1 File 2 perspective license plate.jpg

3.2.2 Obiettivi Analisi

L'immagine in esame presenta due auto. Obiettivo dell'analisi, previa verifica dell'EXIF al fine di garantire con ragionevole certezza la non alterazione dell'immagine digitale, è stata la ricostruzione della targa di uno dei due veicoli.

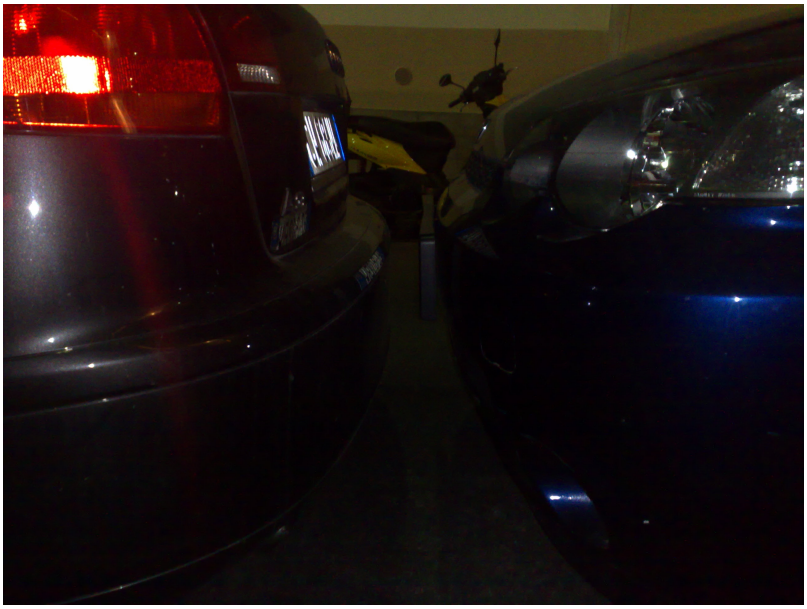

Figura 3: Seconda immagine - Originale

3.2.3 Exif Analysis

Dall'analisi dell'Exif è emerso che l'immagine è stata scattata con la fotocamera integrata in un cellulare Nokia N95 il 23 Ottobre 2008. Report completo allegato.

3.2.4 Step

- Importazione dell'immagine in Amped5
- Correzione della Prospettiva al fine di rendere più chiara la targa del veicolo

3.2.5 Analisi

Il veicolo è verosimilmente un'Audi A3. L'analisi effettuata tramite il software Amped5 ha portato al risultato di una targa del tipo: CW625WA. Facendo una verifica sul sito dell'Agenzia delle Entrate, questa targa corrisponde ad un veicolo Euro 4 con Motore di Cilindrata Cilindrata 1968 cc e potenza 103 KW. L'Audi A3 monta un motore con queste caratteristiche. Inoltre facendo un'analisi temporale non si notano incongruenze in quanto la foto è stata scattata il 23/10/2008 e l'auto immatricolata il 27/06/2005.

Per cui con ragionevole certezza possiamo dire che la nostra analisi ha avuto esito positivo.

Figura 4: Seconda immagine - Risultato

3.3 Terza immagine

3.3.1 File 3D_20110525_010.jpg

3.3.2 Obiettivi Analisi

L'immagine da esaminare prevede la stima dell'altezza del peluche di Homer Simpson a partire da altezze note.

3.3.3 Exif Analysis

Dall'analisi dell'Exif è emerso che l'immagine è stata scattata con la fotocamera integrata in un cellulare Nokia N900 il 25 Maggio 2011. Report completo allegato.

3.3.4 Analisi

L'immagine era ruotata. Quindi il primo passo da fare prima di effettuare misurazioni sull'immagine è stata la rotazione di 90 gradi. Per la misurazione si sono preliminarmente impostati diversi assi sui quali basare la misurazione

Figura 5: Terza Immagine - Originale

3D. In particolare si sono scelti come assi gli spigoli dell'armadietto presente. La difficoltà riscontrata riguarda la scelta dell'asse x. Inoltre il peluche è appoggiato su una confezione di gessetti con il coperchio leggermente sollevato. Ciò non ha semplificato l'analisi. Non son stati scelti come riferimenti per gli assi fogli o fotografie in quanto l'errore umano di chi ha appeso tali fogli o foto potrebbe compromettere maggiormente la stima. In base a questa scelta degli assi si è poi passati a considerare come misura di riferimento l'altezza della scatola di gessetti stimata in 8,5 cm in base a ricerche effettuate sugli store di materiale per ufficio su Internet. Da ciò si è potuto stimare che l'altezza del peluche di Homer Simpson è di 27,393 cm (circa 28 cm).

A Allegati Prima immagine

A.1 Report Amped5

Amped Five Report

Report generation: 2011-06-02 12:06:33 User: Administrator Workstation: localhost

Project File: C:Documents and SettingsAdministratorMy DocumentsFourier-giornale.a5p Summary:

Chain 1: Image Loader

1. Image Loader: Loads an image from file. (File) 2. Fourier: Removes periodic noise and interferences in the Fourier domain. 3. Image Writer: Writes the current image to a file. (File)

Details:

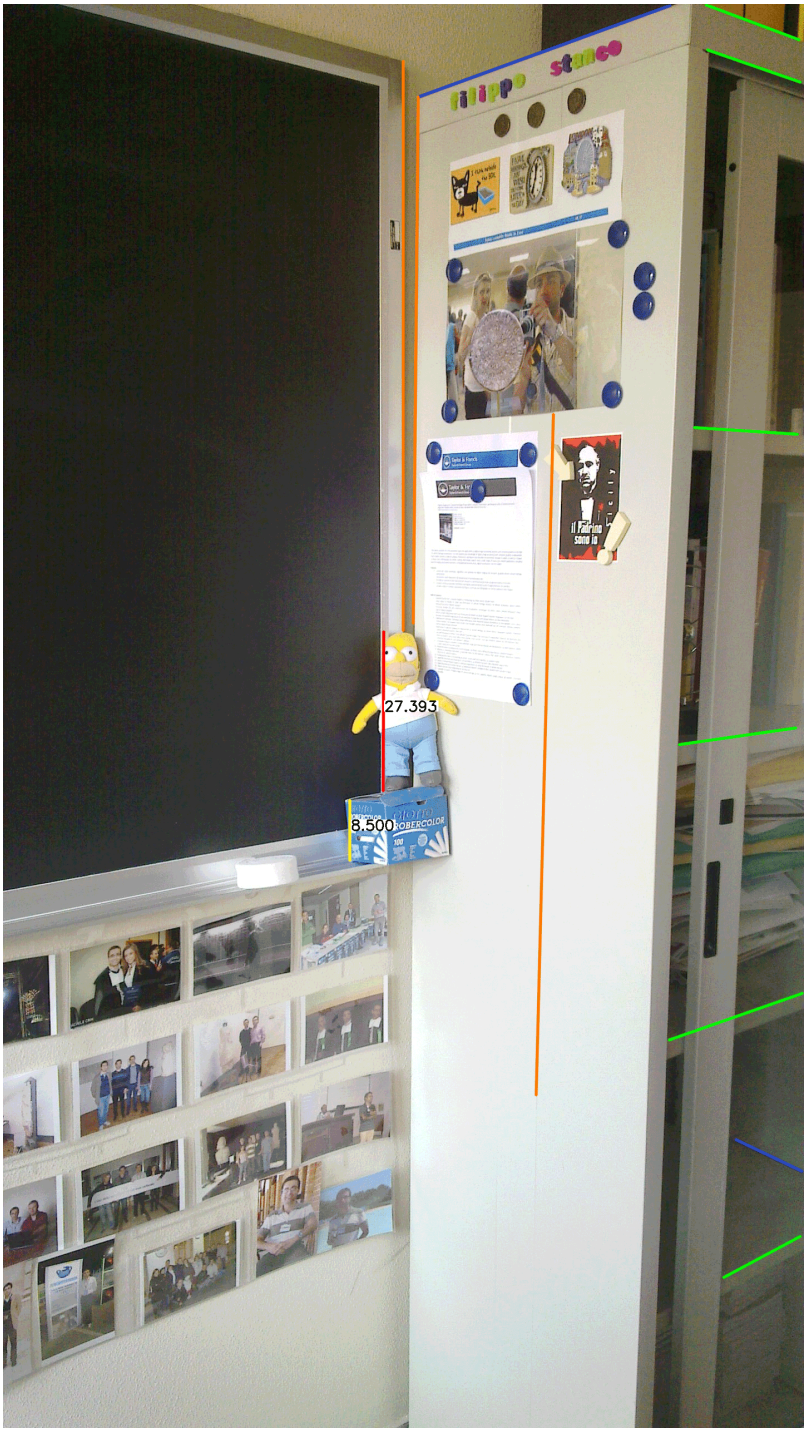

Figura 6: Terza Immagine - Assi e misurazione

Chain 1: Image Loader

1. Image Loader Loads an image from file.

Details: Image Loader renders an image file, that can be encoded in a variety of formats, to a bitmap that can be displayed and processed.

Parameters: Path:
/vmware-hostShared FoldersMy DesktopCF Seconda Prova Itinerecaso021 gentsp.png

The path of the file to be loaded; it can be given as relative to the position of the project or as an absolute path. This setting could be modified by the project properties from the menu Edit-¿Project Properties.

Hashcode: 08CD5D5EB167C2578A8F85E8EB8E6A88

The hash code of the file, calculated with the MD5 algorithm, is a unique and secure identifier used to verify the integrity of the file to be loaded.

2. Fourier Removes periodic noise and interferences in the Fourier domain.

Details: Fourier filters image in the frequency domain, which allows to remove parts of the spectrum where interferences and/or periodic noise are located. This is done by setting to zero the module of selected areas of the spectrum and then calculating its inverse Fourier transform with the inverse DFT algorithm.

Parameters: Output: Image (IFFT)

Domain of the output image.

Selections: (97,119,4,4); (160,138,4,4);

Regions of the spectrum to be removed.

Selection: Whole image.

Region of the image on which the filter is applied.

References: Anil. K. Jain, Fundamentals of Digital Image Processing, Prentice Hall, pp. 145-150, 1989.

3. Image Writer Writes the current image to a file.

Details: Image Writer encodes the current frame to the specified file with the chosen format.

Parameters: Path:
/vmware-hostShared FoldersMy DesktopCF Seconda Prova Itinerecaso021 gentsp110601234627.tif

Path of the image to save.

Image Format: Tiff

Image format to save to.

Quality: 90

Quality of the image to save (the bigger is the better is).

Hashcode: 4CEF22161F2F8A7A014E9C4BFC4484F1

The hash code of the file, calculated with the MD5 algorithm is a unique and secure identifier used to verify the integrity of the file to be loaded.

B Allegati Seconda immagine

B.1 Exif

Basic Image Information Camera: Nokia N95 8GB Lens: 5.6 mm Exposure: Auto exposure, 1/17 sec, f/2.8, ISO 800 Flash: Auto, Fired Date: October 23, 2008 7:26:15PM (timezone not specified) (2 years, 7 months, 7 days, 19 hours, 57 minutes, 15 seconds ago, assuming image timezone of US Pacific) File: 1,944 x 2,592 JPEG (5.0 megapixels) 450,852 bytes (0.43 megabytes) Image compression: 97% Color Encoding: WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac web browsers will treat the colors randomly. Images for the web are most widly viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

advertisement

(ad loading) advertisement is not related to image being inspected I'm giving ads a try; let me know what you think Extracted 320 x 240 12-kilobyte "Composite:ThumbnailImage" JPG Displayed here at 100% (1/66 the area of the original)

Click image to isolate; click this text to show histogram Main JPG image displayed here at 17% width (1/33 the area of the original)

Click image to isolate; click this text to show histogram

Here's the full data:

EXIF — this group of metadata is encoded in 14,935 bytes (14.6k) Exif Image Size 2,592 x 1,944 Make Nokia Camera Model Name N95 8GB Orientation Horizontal (normal) Y Cb Cr Positioning Centered Exposure Time 1/17 F Number 2.8 ISO 800 Exif Version 0220 Date/Time Original 2008:10:23 19:26:15 2 years, 7 months, 7 days, 19 hours, 57 minutes, 15 seconds ago Create Date 2008:10:23 19:26:15 2 years, 7 months, 7 days, 19 hours, 57 minutes, 15 seconds ago Components Configuration Y, Cb, Cr, - Shutter Speed Value 1/17 Aperture Value 2.8 Light Source Flash Flash Auto, Fired Focal Length 5.6 mm Maker Note Unknown (2,480 bytes binary data) Flashpix Version 0100 Color Space sRGB Custom Rendered Normal Exposure Mode Auto White Balance Auto Digital Zoom Ratio 1 Scene Capture Type Standard Gain Control High gain up Compression JPEG (old-style) Resolution 300 pixels/inch X Resolution 72 Y Resolution 72 Thumbnail Length 11,851 File — basic information derived from the file. File Type JPEG MIME Type

image/jpeg Exif Byte Order Little-endian (Intel, II) Encoding Process Baseline DCT, Huffman coding Bits Per Sample 8 Color Components 3 File Size 440 kB Image Size 2,592 x 1,944 Y Cb Cr Sub Sampling YCbCr4:2:2 (2 1) Composite This block of data is computed based upon other items. Some of it may be wildly incorrect, especially if the image has been resized. Aperture 2.8 Shutter Speed 1/17 Thumbnail Image (11,851 bytes binary data) Focal Length 5.6 mm Light Value 4.1 ExifTool Warning Error rebuilding maker notes (may be corrupt) Warning [minor] Unrecognized MakerNotes

B.2 Report Amped5

Amped Five Report

Report generation: 2011-06-02 12:06:57 User: Administrator Workstation: localhost

Project File: C:Documents and SettingsAdministratorMy DocumentsAudi-CW685WA.a5p Summary:

Chain 1: Image Loader

1. Image Loader: Loads an image from file. (File) 2. Correct Perspective: Removes the perspective effect on a plane of interest in the image. 3. Image Writer: Writes the current image to a file. (File)

Details:

Chain 1: Image Loader

1. Image Loader Loads an image from file.

Details: Image Loader renders an image file, that can be encoded in a variety of formats, to a bitmap that can be displayed and processed.

Parameters: Path:
/vmware-hostShared FoldersMy DesktopCF Seconda Prova Itinerecaso022 perspective license plate.jpg

The path of the file to be loaded; it can be given as relative to the position of the project or as an absolute path. This setting could be modified by the project properties from the menu Edit-¿Project Properties.

Hashcode: 56B0704ED2CC8149B8C9587A7C45EE81

The hash code of the file, calculated with the MD5 algorithm, is a unique and secure identifier used to verify the integrity of the file to be loaded.

2. Correct Perspective Removes the perspective effect on a plane of interest in the image.

Details: Correct Perspective maps a desired quadrangular region to a rectangular one, which allows to see the plane of interest as the plane of the image was parallel to it. Pixel values are interpolated with a bicubic algorithm.

Parameters: Source Points: 937, 344, 1068, 355, 1107, 504, 993, 561

Coordinates of the four angles of the polygon, selected in clockwise direction starting from the upper-left corner.

Selection: x = 783, y = 344, Width = 439, Height = 218;

Region of the image on which the filter is applied.

References: Anil. K. Jain, Fundamentals of Digital Image Processing, Prentice Hall, pp. 320-322, 1989.

3. Image Writer Writes the current image to a file.

Details: Image Writer encodes the current frame to the specified file with the chosen format.

Parameters: Path:
/vmware-hostShared FoldersMy DesktopCF Seconda Prova Itinerecaso022 perspective license plate110601234443.tif

Path of the image to save.

Image Format: Tiff

Image format to save to.

Quality: 90

Quality of the image to save (the bigger is the better is).

Hashcode: FE5B68E7E013202C09BE65AE5181DF81

The hash code of the file, calculated with the MD5 algorithm is a unique and secure identifier used to verify the integrity of the file to be loaded.

Selection: x = 783, y = 344, Width = 439, Height = 218;

Region of the image on which the filter is applied.

B.3 Dati Veicolo (Agenzia delle Entrate)

`http://www1.agenziaentrate.it/servizi/bollo/calcolo/propostapagamentosemplice.htm?targa=CW685WA&tiposervizio=PropostaPagamentoSemplice&categoria=01-autoveicolo`

Tipo veicolo:01-autoveicolo
Targa:CW685WA
Dati relativi al veicolo
Regione:Friuli V.G.
Cilindrata:1968 cc
Potenza:103 KW
Direttiva Euro:4
Alimentazione:Gasolio
EcoDiesel:Si
Cavalli:
Posti:4
Portata:* kg

Peso: kg
Numero Assi:
Categoria:autovettura
Data immatricolazione:27/06/2005
Codice uso:privato trasporto persone

C Allegati Terza immagine

C.1 Exif

Basic Image Information Camera: Nokia N900 Lens: 5.2 mm Exposure: Auto exposure, Not Defined, 1/32 sec, f/2.8, ISO 100 Flash: none Date: May 25, 2011 12:15:08PM (timezone not specified) (7 days, 5 hours, 27 minutes, 1 second ago, assuming image timezone of US Pacific) File: 1440 x 2560 JPEG (3.7 megapixels) 574,074 bytes (0.55 megabytes) Image compression: 95% Color Encoding: WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac web browsers will treat the colors randomly. Images for the web are most widly viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

advertisement

(ad loading) advertisement is not related to image being inspected I'm giving ads a try; let me know what you think Main JPG image displayed here at 18% width (1/32 the area of the original)

EXIF — this group of metadata is encoded in 4,640 bytes (4.5k) Exif Image Size 2560 x 1440 Make Nokia Camera Model Name N900 Orientation Rotate 90 CW Modify Date 2011:05:25 12:15:08 7 days, 5 hours, 27 minutes, 1 second ago Y Cb Cr Positioning Centered Exposure Time 1/40 F Number 2.8 Exposure Program Not Defined ISO 100 Exif Version 0210 Date/Time Original 2011:05:25 12:15:08 7 days, 5 hours, 27 minutes, 1 second ago Components Configuration Shutter Speed Value 1/32 Aperture Value 2.8 Light Source Unknown Flash No Flash Focal Length 5.2 mm Maker Note Unknown (4,096 bytes binary data) Flashpix Version 0100 Color Space sRGB Custom Rendered Normal Exposure Mode Auto White Balance Auto Digital Zoom Ratio 1 Scene Capture Type Portrait Gain Control None Contrast Normal Resolution 300 pixels/inch Saturation Normal File — basic information derived from the file. File Type JPEG MIME Type image/jpeg Exif Byte Order Little-endian (Intel, II) Encoding Process Baseline DCT, Huffman coding Bits Per Sample 8 Color Components 3 File Size 561 kB Image Size 2,560 x 1,440 Y Cb Cr Sub Sampling YCbCr4:2:0 (2 2) Composite This block of da-

ta is computed based upon other items. Some of it may be wildly incorrect, especially if the image has been resized. Aperture 2.8 Shutter Speed 1/40 Focal Length 5.2 mm Light Value 8.3 ExifTool Warning Error rebuilding maker notes (may be corrupt) Warning [minor] Unrecognized MakerNotes

C.2 Report Amped5

Amped Five Report

Report generation: 2011-06-02 12:06:06 User: Administrator Workstation: localhost

Project File: C:Documents and SettingsAdministratorMy DocumentsMeasure-Simpson.a5p Summary:

Chain 1: Image Loader

1. Image Loader: Loads an image from file. (File) 2. Rotate: Rotates the image. 3. Measure 3d: Computes world measurements from single images by the 3D reconstruction of the scene and by using a known distance as reference. 4. Image Writer: Writes the current image to a file. (File)

Details:

Chain 1: Image Loader

1. Image Loader Loads an image from file.

Details: Image Loader renders an image file, that can be encoded in a variety of formats, to a bitmap that can be displayed and processed.

Parameters: Path:
/vmware-hostShared FoldersMy DesktopCF Seconda Prova Itinerecaso023D_20110525_010.jpg

The path of the file to be loaded; it can be given as relative to the position of the project or as an absolute path. This setting could be modified by the project properties from the menu Edit-¿Project Properties.

Hashcode: CB9AD0D024EDDFDCC9968A8E6B48532D

The hash code of the file, calculated with the MD5 algorithm, is a unique and secure identifier used to verify the integrity of the file to be loaded.

2. Rotate Rotates the image.

Details: Rotate rotates the image by the given angle. If the rotation angle is not multiple of 90 degrees, the selected interpolation algorithm is used, otherwise the original pixel values are only transposed.

Parameters: Angle: -90

Rotation angle.

Do not resize: enabled

If checked, the image keep their original size, although part of the actual data could finish outside of the visible area.

Interpolation: Bicubic

The interpolation algorithm used to reconstruct the image data.

References: Anil. K. Jain, Fundamentals of Digital Image Processing, Prentice Hall, pp. 320-322, 1989.

3. Measure 3d Computes world measurements from single images by the 3D reconstruction of the scene and by using a known distance as reference.

Details: Measure 3d computes world distances directly on the image. The measure estimation algorithm is based on the Single View Metrology (SVM) approach described by Criminisi, Reid and Zisserman in Single View Metrology. The SVM is based on the fact that some image lines, which are parallel in the world, join in a point in the image, named vanishing point, due to the perspective. The vanishing points themselves are obtained by identifying, thanks to the geometric information (two or more lines for each x/y/z direction) provided by the user, sets of 3D points (x,y,z) that belong to the segment lines for each direction of interest. The scene perspective can be reconstructed from vanishing points: transforming the geometric information into a system of linear constraints on the coordinates of the 3D points and using the 2D observations (the known distance) to further constrain the 3D points. As result, 3D measurements may be computed from a single perspective view of a scene given only these minimal geometric informations determined from the image. Since the input quantities and the transformations are uncertain, the output measurements are uncertain too. The validity of the Single View Metrology approach is assessed by the Monte Carlo statistical tests: it determines how the uncertainty propagates from input to output of the computation chain and estimate the measurement accuracy.

Parameters: X-axis: 748, 166, 1199, 2, 1317, 2041, 1436, 2098

The set of the pixel coordinates of the lines which are defined by the user in the x direction of the scene.

Y-axis: 1263, 1, 1431, 64, 1295, 2289, 1433, 2215, 1197, 1862, 1437, 1778, 1215, 1331, 1425, 1301, 1242, 761, 1428, 773, 1266, 82, 1433, 140

The set of the pixel coordinates of the lines which are defined by the user in the y direction of the scene.

Z-axis: 737, 1113, 746, 166, 958, 1961, 989, 737, 719, 102, 719, 1126

The set of the pixel coordinates of the lines which are defined by the user in the z direction of the scene.

Reference axis direction: 2

The x/y/z direction along which a metric information is known (some reference distances are known).

Reference line: 623, 1539, 623, 1431

The pixel coordinates of the image segment in the x/y/z direction which are used as reference.

Reference length: 8.50000

The real-world distance (m, cm, mm, yd, ft, in...) between the endpoints of the reference line.

Measure type: 0

Type of the measurement which can be estimated from the image. Normal and Differential are the possible values.

Output line: 683, 1414, 684, 1128

The pixel coordinates of the target of the measurement.

Output projection line: Not used.

The pixel coordinates of the projection of the target of the measurement on the reference plane (only if Measure Type = Differential).

Output length: 27.39288

The real-world value (m, cm, mm, yd, ft, in...) of the output of the measurement.

Output error: 0.72460

The uncertainty (m, cm, mm, yd, ft, in...) associated with the output measurement.

References: A. Criminisi, I. Reid, and A. Zisserman, Single View Metrology, in International Journal of Computer Vision, vol. 40, no. 2, pp. 123-148, Nov. 2000.

4. Image Writer Writes the current image to a file.

Details: Image Writer encodes the current frame to the specified file with the chosen format.

Parameters: Path:
/vmware-hostShared FoldersMy DesktopCF Seconda Prova Itinerecaso023D_20110525_010110601

Path of the image to save.

Image Format: Tiff

Image format to save to.

Quality: 90

Quality of the image to save (the bigger is the better is).

Hashcode: 78AFD1DC5D89BB03CED8472F0D308829

The hash code of the file, calculated with the MD5 algorithm is a unique and secure identifier used to verify the integrity of the file to be loaded.