

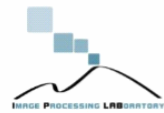
Digital Forgery (e non solo...)

S. Battiato

Dipartimento di Matematica e Informatica,
Università di Catania

Image Processing LAB - <http://iplab.dmi.unict.it>

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



INDIZI: La barba, bocca sono molto sfocati e con una risoluzione molto bassa, mentre i capelli sono più definiti, con risoluzione e contrasto maggiori. Poi al centro della fronte c'è una macchia chiara, che più che un riflesso sembra una pennellata. Identico riflesso del flash (su orecchio dx)

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Overview

- What is a Forgery?
 - Using Graphical Software
 - The content has been modified
 - The context has been modified
- Unsupervised method for forgery detection
- The JPEG Standard
- Exif Informations
 - Thumbnails Analysis
- JPEG DCT Techniques
 - Measuring Inconsistencies of Block Artifact
 - Digital Forgeries From JPEG Ghosts
- Forgery Camera Based

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



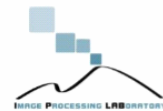
What is a Forgery?

- “Forgery” is a subjective word.
- An image can become a forgery based upon the context in which it is used.



- An image altered for fun or someone who has taken a bad photo, but has been altered to improve its appearance cannot be considered a forgery even though it has been altered from its original capture.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



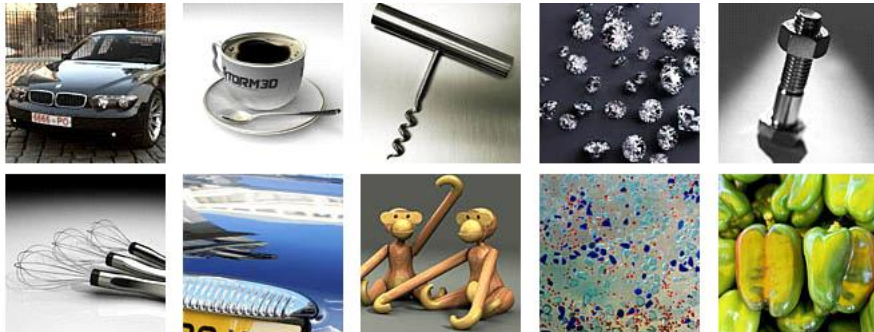
What is a Forgery?

- The other side of forgery are those who perpetuate a forgery for gain and prestige
- They create an image in which to dupe the recipient into believing the image is real and from this be able to gain payment and fame
- Three type of forgery can be identified:
 - An image that is created using graphical software
 - An image where the content has been altered
 - An image where the context has been altered

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Using graphical software



Can you tell which among the array of images are real, and which are CG?

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Using graphical software



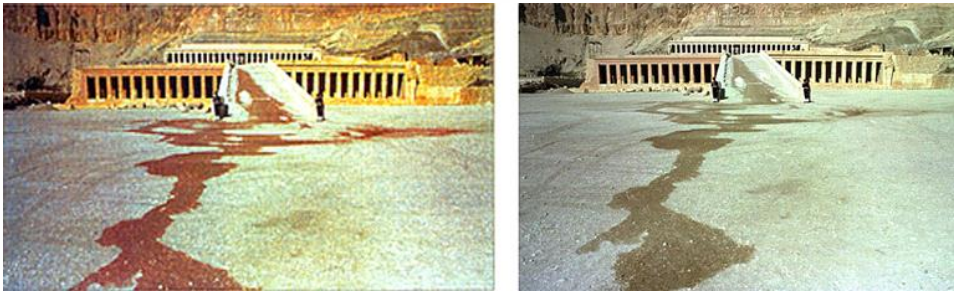
<http://www.autodesk.com/eng/etc/fakeorfoto/about.html>

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



The content has been altered

- Creating an image by altering its content is another method
- Duping the recipient into believing that the objects in an image are something else from what they really are!
- The image itself is not altered, and if examined will be proven as so.



November 1997: After 58 tourists were killed in a terrorist attack at the temple of Hatshepsut in Luxor Egypt, the Swiss tabloid Blick digitally altered a puddle of water to appear as blood flowing from the temple.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



The context has been altered

- Objects are be removed or added, for example, a person can be added or removed
- The easiest way is to cut an object from one image and insert it into another image - image editing software makes this a simple task
- By manipulating the content of an image the message can drastically change its meaning.
- An example is this altered image which could be used to influence events in foreign countries which are not aware of manipulation.

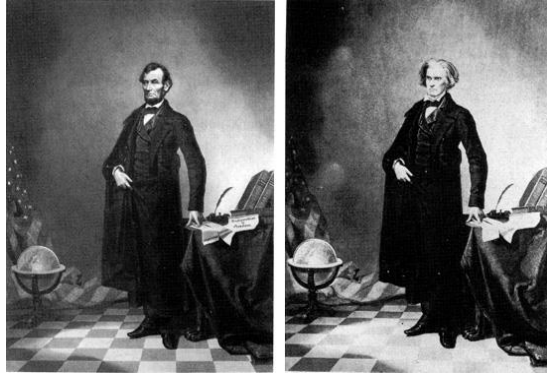


Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Altering Images

- Altering images is not new - it has been around since the early days of photography
- The concepts have moved into the digital world by virtue of digital cameras and the availability of digital image editing software



circa 1860: This nearly iconic portrait of U.S. President Abraham Lincoln is a composite of Lincoln's head and the Southern politician John Calhoun's body.

- The ease of use of digital image editing software, which does not require any special skills, makes image manipulation easy to achieve.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



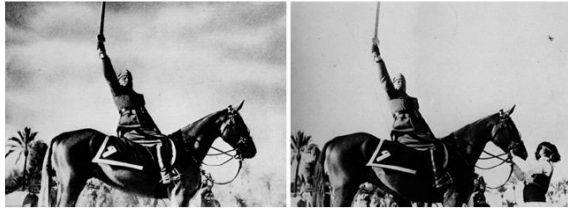
1930 circa: Stalin ricorreva abitualmente all'aerografo al fine di rimuovere i suoi nemici dalle fotografie. In questa fotografia un commissario venne rimosso dal documento originale.



1937: Nella seguente fotografia Adolf Hitler fece rimuovere Joseph Goebbels (il secondo a destra).



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



1942: Benito Mussolini fece rimuovere dalla illustrazione originale il soldato che domava il suo cavallo, al fine di rendere più epica la scena che lo ritraeva.

Giugno 1994: Questa fotografia alterata di OJ Simpson venne pubblicata sulla copertina della rivista Time Magazine, subito dopo il suo arresto per omicidio. In effetti la fotografia risultò alterata rispetto all'immagine originale che comparve sulla copertina della rivista Newsweek. La rivista Time venne accusata di aver manipolato la fotografia al fine di rendere la figura di Simpson più scura e minacciosa.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Aprile 2003: Questa composizione di un soldato Inglese a Basra, che gesticola verso un civile iracheno indicandogli di restare coperto, è apparsa sulla copertina del Los Angeles Times, subito dopo l'invasione dell'Iraq. Brian Walski, un fotografo dello staff del Los Angeles Times e un veterano della notizia con trenta anni di esperienza alle spalle, è stato licenziato in tronco dal suo editore per aver fuso due dei suoi scatti al fine di migliorare la composizione.

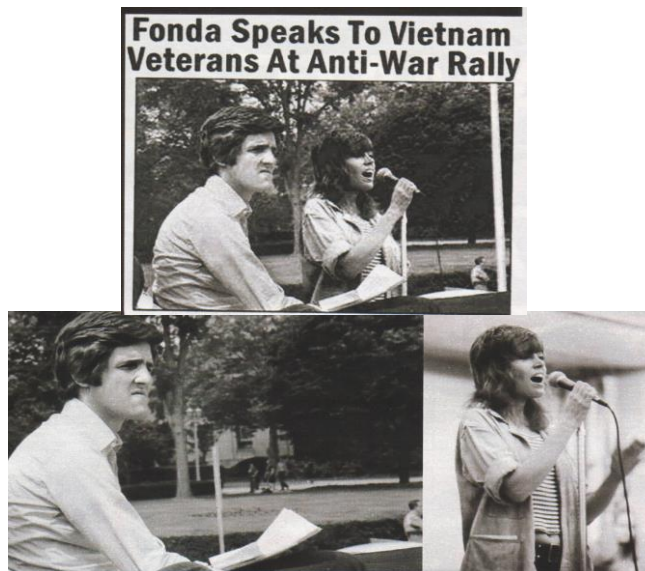


Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Off-side (Febbraio 2011)



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Altri esempi famosi

www.cs.dartmouth.edu/farid/research/digitaltampering

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Sydney Conman who
photoshopped
pictures of himself
with famous people
gets 12 years' jail
<http://www.smh.com.au>



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

WorldPhotoPress 2012



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Esperti a confronto...

Sono stati contattati degli «esperti» forensi che hanno stabilito che: che sì la foto è stata ritoccata, in quanto a luce e colori, così da renderla più *forte*, ma sostanzialmente non si tratta di un'immagine **composita** (confronto con il raw).

Il ritocco in colori e intensità luminosa è un discorso a parte, ricade nelle scelte della giuria del WPP sull'accettare o meno una foto in stile **Instagram**.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Estratto del rapporto:

1. **XMP Analysis.** The XMP analysis reflects an incomplete understanding of the Photoshop metadata and also paraphrases the contents in a misleading way. The referenced block of metadata merely indicates that the file was adjusted in the Adobe Photoshop Camera Raw module on multiple occasions before it was opened in Photoshop and then saved out as a JPEG. In fact, this metadata does not track whether multiple files were composited.
2. **Error Level Analysis.** The forensic analysis of the JPEG compression as performed by error level analysis (ELA) does not provide a quantitative or reliable analysis of photo manipulation. This analysis frequently mis-identifies authentic photos as altered and fails to identify altered images, and as such is not a reliable forensic tool.
3. **Shadow Analysis.** The shadow analysis is flawed in its logic and conclusions. It is true that linear constraints that connect points on an object with their corresponding points on the shadow should intersect at a single point (assuming the presence of a single light source). The location of this intersection point, however, cannot be used to reason about the elevation of the light in the scene. The intersection point is simply the projection of the light source into the image plane. This projected location can be anywhere in the image (including below the ground plane) depending on where the photographer is oriented relative to the sun.“

Dr. Hany Farid

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Negativo vs. Sensore: due epoche a confronto

Nel vecchio mondo della fotografia analogica, un'immagine era, in genere, considerata una prova d'evidenza attendibile. Allo stato attuale non esistono tecniche automatiche “perfette” che permettono l'esatta individuazione di manomissioni delle immagini digitali.

Per questo motivo le fotografie digitali non sono, in genere, attendibili ai fini di prove d'evidenza, se non con i dovuti accorgimenti “formali” e “procedurali”.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Negativo vs. Sensore: due epoche a confronto

In epoca “pre-digitale”, possiamo affermare che molto raramente veniva messa in dubbio la veridicità di una immagine. Era comunque abitudine, allorquando era necessario corredare un fascicolo di indagine di alcune fotografie, depositare anche i negativi delle stesse. Prassi voleva che questa accortezza fosse sufficiente per mettersi al riparo da contestazioni in merito all'originalità della fonte di prova. Inoltre, poter fornire l'intero rullino da cui erano state estratte le immagini, impediva di omettere qualche scatto “scomodo”, dato che la pellicola li contrassegnava in ordine cronologico

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Negativo vs. Sensore: due epoche a confronto

L'odierna «diffidenza» discende dalle diverse tecniche di formazione dell'immagine tra i due tipi di apparati.

- Nelle fotocamera analogiche la pellicola veniva impressionata dalla luce proveniente dal sistema di lenti, dopodiché essa costituiva una sorta di “matrice” dell'immagine, da cui si potevano estrarre quante copie si desiderava, tutte (a parte lievi variazioni cromatiche determinate dai dosaggi dei reagenti per lo sviluppo, mai uguali in due operazioni distinte) identiche all'originale.
- Nel sensore delle fotocamera digitali (che in senso lato sostituisce la pellicola) l'immagine semplicemente “transita” prima di essere salvata nella memoria (dopo essere stata fra l'altro elaborata). Al termine del processo di acquisizione questa viene salvata ma può anche essere subito cancellata se non soddisfa il gusto dell'operatore. La “matrice originale” di una immagine in un certo senso non esiste più.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Alterazione delle fotografie analogiche: Mito o Realtà?

In realtà, anche i negativi potevano essere alterati, sia agendo fisicamente sulla pellicola, asportandone delle parti o aggiungendone altre e poi sviluppando il negativo modificato, oppure duplicando il negativo con apposita strumentazione, applicando delle opportune maschere per nascondere od inserire i particolari voluti.

Tecniche di rilevazione (certe)

- Esamina del negativo modificato per notare i ritocchi
- Esamina delle diverse caratteristiche (grana, spessore) del negativo-copia, di solito mai del tutto identici a quelli dei rullini delle fotocamere.

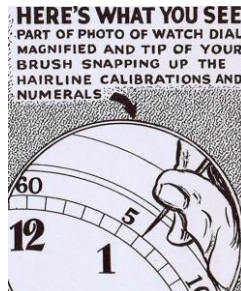
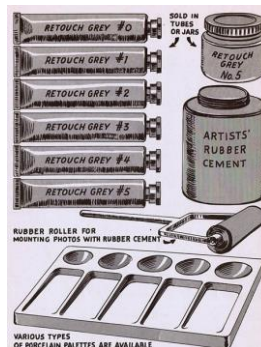
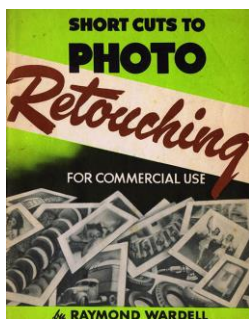
Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Alterazione delle fotografie analogiche: Mito o Realtà?

Queste presunte modifiche sulle fotografie analogiche non erano alla portata dell'utente generico, ma richiedevano conoscenze specifiche, abilità, e strumentazione adatta.

Nel mondo digitale invece l'autenticità e quindi la validità di una immagine o di un video presenta una «sfida» più difficile: non vi sono segni su un negativo, o spessori di pellicole da controllare, ma dati e tracce digitali, statistiche da interpretare in modo non sempre univoco e con una certa dose di «incertezza».

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



DON'T DO TOO MUCH!
IN OTHER WORDS IF THE "BOSS MAN" JUST ASKS FOR A FEW SLIGHT TOUCHES DO EXACTLY THAT, AS CAREFULLY AS YOU CAN. DON'T PLAN A MAJOR OPERATION THAT WILL TAKE YOU ALL DAY.

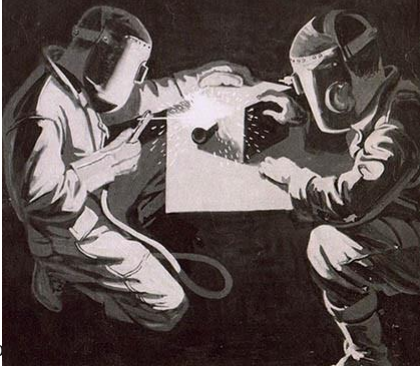
<http://petapixel.com/2013/05/08/how-photographers-photoshopped-their-pictures-back-in-1946/>

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

DARKNESS DRAMATIZES

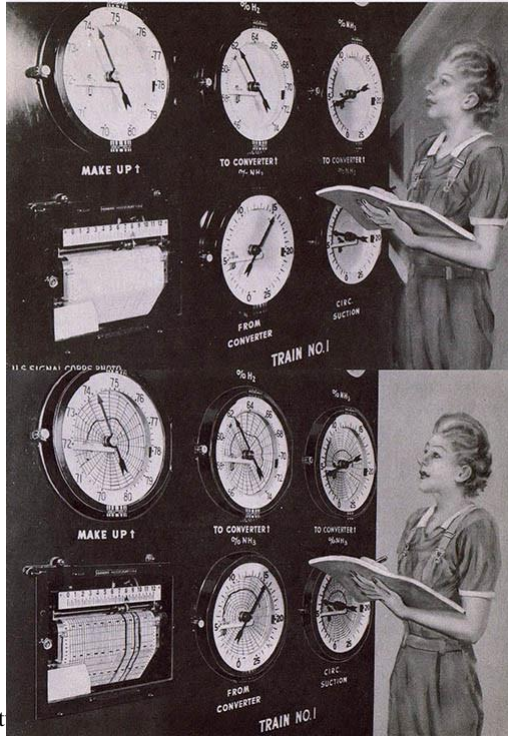


STANLEY CORDE PHOTO BY U.S. ARMY



Co

MARKS ON DIALS MUST SHOW



Bat

"GLAMORIZE" THIS PICTURE

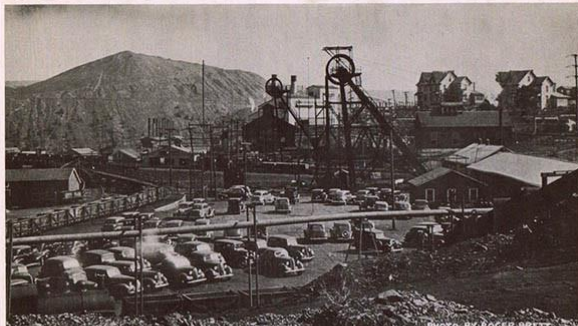
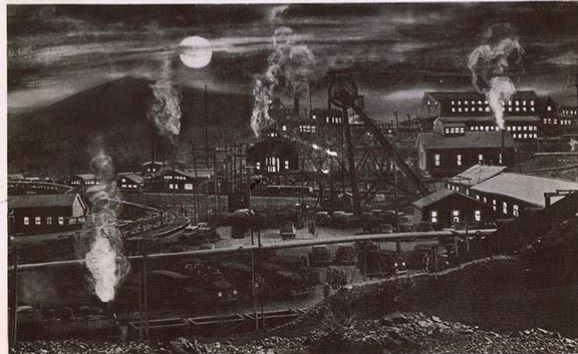


PHOTO BY ROGER BREYER

YOU COULD PUT IN BUSY FIGURES AND HAVE SMOKE AND STEAM COMING FROM CHIMNEYS AND SWITCHING ENGINE; ALSO CHANGE SOME CARS INTO LOADED TRUCKS

STUDY MAGAZINES FOR METHODS OF ILLUSTRATING INDUSTRIAL ACTIVITY BELOW WE SHOW HOW TO TRANSFORM A DAYLIGHT PICTURE INTO A MOONLIGHT



Computer Forensics A

Digital Forgery

- E' possibile utilizzare tecniche per la detection automatica di eventuali manipolazioni “maliziose” delle immagini digitali?
- E' stato coniato il termine “*Photoshopping*” per denotare l'azione volta a falsificare digitalmente medicine, scene di guerra, ed in generale immagini digitali di qualsiasi natura (“Photoshop Forensic”, Cynthia Baron 2008).

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Digital Forgery



(a) Original



(d) Tampered region, TIFF



(b) Forgery



(f) Tampered region, JPEG 90

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Digital Forgery



G2 Original



G2 Forgery



Regions detected as forged

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

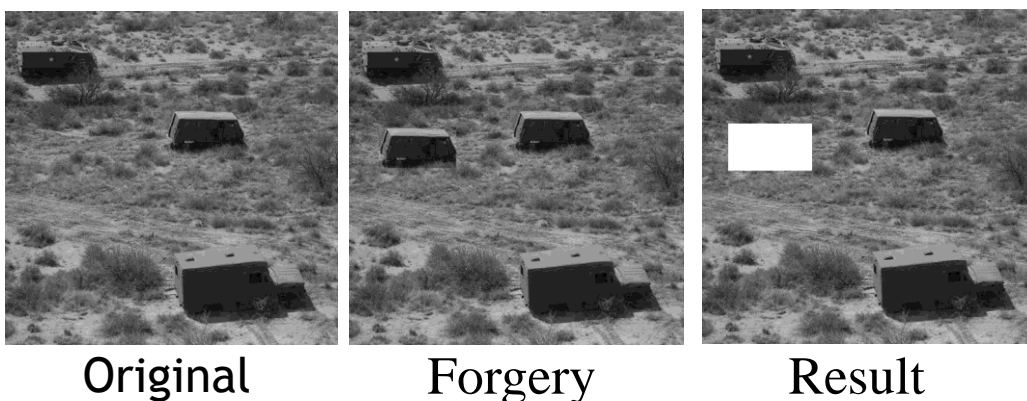
How does it work?

- Pixel-based
 - Cloning, Resampling, Splicing
 - Statistical
- **Format Based (JPEG,)**
- **Camera Based**
 - Chromatic Aberration
 - *Color Filter Array*
 - *Camera Response*
 - *Sensor Noise*
- Physics based
 - Light Direction, Light Environment
- Geometric Based
 - **Principal Point**

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Copy-Paste Forgery

The Copy and Paste forgery detection is mainly based on the research of blocks which looks like repeated into the image. If the amount of adjacent repeated blocks are higher than an heuristic threshold the region is likely to be altered.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Resampling

Al fine di generare una contraffazione convincente, molto spesso si ricorre ad operazioni di **ridimensionamento**, **rotazioni**, **oppure deformazioni di porzioni di immagini**. Per esempio quando si crea un fotomontaggio con due persone, una delle due deve essere manipolata per raggiungere dimensioni compatibili con la risoluzione dell'altra.

Questo procedimento richiede di **ricampionare** l'immagine di partenza in una nuova griglia di destinazione, generando in questo modo delle correlazioni periodiche nei dintorni dei pixel manomessi. La presenza di queste **correlazioni**, normalmente **inesistenti**, è utilizzata per individuare questo tipo di manomissione

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Un esempio reale (2006)



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Come procedere in casi reali..

Se si hanno dei sospetti sulle aree clonate è sufficiente prendere in input l'immagine, le coordinate utili ad individuare una data area di ricerca e la regione (o patch) di cui si vogliono individuare i possibili cloni oltre che i range relativi alle possibili trasformazioni geometriche considerate. L'area di ricerca individua l'area entro cui ricercare gli eventuali cloni della patch ad esclusione della stessa patch (qualora fosse essa stessa inclusa nella zona di ricerca).

I **parametri** relativi alle trasformazioni specificano invece i valori da utilizzare per ciascuna trasformazione geometrica considerata.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Come procedere in casi reali..

Esempi di possibili trasformazioni sono le seguenti:

- Rotazione
- Scala lungo l'asse x
- Scala lungo l'asse y
- Crop sui 4 lati
- Flip orizzontale

Mediante analisi visiva ed utilizzando apposite procedure di ispezione virtuali ci si può concentrare, caso per caso, sulle trasformazioni più pertinenti, limitando anche il relativo range di ricerca. Il crop sui 4 lati viene utilizzato in tutti i casi ed ha lo scopo di compensare possibili errori commessi dall'utente durante la definizione della patch da ricercare. Il crop permette dunque di aumentare o ridurre le dimensioni della patch quando i bordi di quest'ultima non si riescono a definire in maniera precisa.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Come metrica di similarità si può in genere ritenere sufficiente ai nostri scopi la media delle differenze in valore assoluto, in gergo **MAE (Mean Absolute Error)**, tra la regione di input e il suo possibile “clone”.

Questo valore numerico (che varia tra 0 e 255) misura quanto due regioni siano tra loro simili tenendo conto della differenza pixel per pixel delle regioni corrispondenti. Un valore di MAE pari a zero indica la perfetta corrispondenza: le due regioni sono uguali.

Valori prossimi allo zero o comunque molto piccoli indicano un alta probabilità che le due regioni siano copia l’una dell’altra.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Camera-based



Le scanalature impresse dalle canne delle pistole sui proiettili collegano, con un certo grado di confidenza, una pallottola ad una ben determinata arma da fuoco.

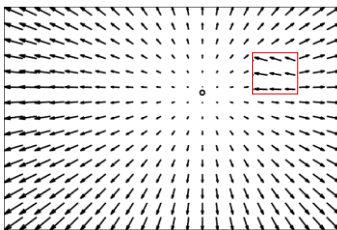
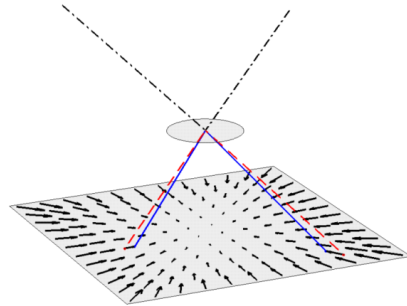
Sfruttando la stessa filosofia, sono state sviluppate delle tecniche di digital forensics che, basandosi su determinati **artefatti** introdotti dai vari stadi dell’elaborazione dell’immagine all’interno delle fotocamere, determinano un collegamento **univoco** tra fotocamera e immagine.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Chromatic Aberration

The refraction of light in two dimensions. Polychromatic light enters the lens and emerges at an angle which depends on wavelength.

As a result, different wavelengths of light, two of which are represented as the red (dashed) and the blue (solid) rays, will be imaged at different points. The vector field shows the amount of deviation across the image.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Geometric based: Light Direction

- Shown on the left are three forgeries: the ducks, swans, and football coach were each added into their respective images.

- Shown on the right are the analyzed regions superimposed in white, and spheres rendered from the estimated lighting coefficients.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Format Based:JPEG

- La prima regola fondamentale dell'indagine forense è ovviamente quella della conservazione dei dati originali. Per questo motivo la compressione lossy delle immagini JPEG può essere considerata il peggior nemico dell'analista forense. Il caso vuole che proprio questa caratteristica, di "perdita dei dati", sia utilizzata come ottimo strumento per l'individuazione delle manomissioni.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

La Quantizzazione

- La maggior parte delle macchine fotografiche digitali memorizzano gli scatti in formato JPEG. Questo schema di compressione lossy permette di stabilire, in qualche modo, un "grado" di compressione dei dati. Di solito, sono i produttori di fotocamere a stabilire i differenti "gradi" di compressione selezionabili, in funzione a statistiche che bilanciano qualità e dimensioni finali dei files.
- Queste differenze possono essere utilizzate per identificare la sorgente (Modello di fotocamera, produttore) di un'immagine.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

The JPEG Standard

- JPEG stands for an image compression stream of bytes;
- JFIF (JPEG File Interchange Format) stands for a standard which define:
 - Component sample registration
 - Resolution and aspect ratio
 - Color Space
- **ExIF** allows to integrate further information into the file

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Exif: some details

Exchangeable image file format (Exif) is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras.

The specification uses the following existing file formats with the addition of specific metadata tags: JPEG DCT for compressed image files, TIFF for uncompressed image files, and RIFF WAV for audio files. It is not supported in JPEG 2000, PNG, or GIF.

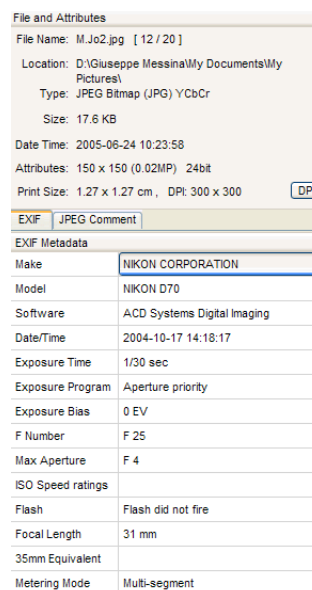
This standard consists of the Exif image file specification and the Exif audio file specification.

Source wikipedia

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Exif Informations

- ExIF allows to integrate further information into the file.
- The information usually contained into a standard ExIF are:
 - Dimensions of the image
 - Date and Time of Acquisition
 - Features about acquisition:
 - Exposure-time , Exposure Bias, F-Number, Aperture, ISO, Focal length, GPS coordinates etc.
 - Thumbnail preview (a small picture which would be equal to the original picture).
- The ExIF information checking has demonstrated the possibility of immediate forgery detection.
- In effect if the constructor is known several ExIF data must match to fixed values.



The screenshot shows a 'File and Attributes' window for a file named 'M.Jo2.jpg'. It displays various file properties such as location, type, size, and date. Below this, the 'EXIF' tab is selected, showing a table of 'EXIF Metadata' with fields like Make, Model, Software, Date/Time, Exposure Time, and more.

EXIF Metadata	
Make	NIKON CORPORATION
Model	NIKON D70
Software	ACD Systems Digital Imaging
Date/Time	2004-10-17 14:18:17
Exposure Time	1/30 sec
Exposure Program	Aperture priority
Exposure Bias	0 EV
F Number	F 2.5
Max Aperture	F 4
ISO Speed ratings	
Flash	Flash did not fire
Focal Length	31 mm
35mm Equivalent	
Metering Mode	Multi-segment

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

I metadati XMP

L'Extensible Metadata Platform (XMP) è lo standard di metadati utilizzato dalle applicazioni **Adobe**. I metadati memorizzati in altri formati, ad esempio Exif, IPTC (IIM), GPS e TIFF, vengono sincronizzati e descritti con lo standard XMP in modo da poter essere visualizzati e gestiti più facilmente. Ad esempio, le regolazioni apportate alle immagini con Adobe Camera Raw vengono memorizzate come metadati XMP. Lo standard XMP è basato sull'**XML**.

Maggiori dettagli sono disponibili su:

http://help.adobe.com/it_IT/aftereffects/cs/using/WS7D166319-4319-4f7d-BCF2-28B26E30FB5C.html

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Thumbnail

La maggior parte delle fotocamere memorizza negli EXiF data un thumbnail (in JPEG) dell'intera immagine ad utilizzare per preview veloci.

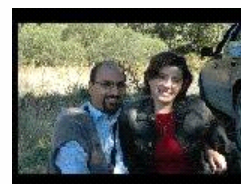
Che succede in caso di forgery (malizioso o meno)?

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Thumbnails Analysis

- Using the following image we can extract the thumbnail through simple ExiF tools, web sites or open source codes, like:
 - **Opanda IExif**
(<http://www.opanda.com>)
 - **Camera Summary**
(<http://camerasummary.com/>)
 - **Jeffrey's Exif Viewer**
(<http://regex.info/exif.cgi>)
 - **JPEGSnoop**
(<http://www.impulseadventure.com/photo/jpeg-snoop.html>)
 - **Jhead version**
(<http://www.sentex.net/~mwandel/jhead/>)
- These tools permit to identify data that have not been removed by inexperienced users.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Thumbnail
Original
Size



IMAGE PROCESSING LABORATORY

Source Camera Identification

On the most obvious and simplest level, one could inspect the **Electronic File** itself and look for clues in headers or any other attached or associated information. For instance, the **EXIF** header contains information about the digital camera type and the conditions under which the image was taken (exposure, date and time, etc.).

It is FUNDAMENTAL to highlight that metadata can be easily manipulated

;(

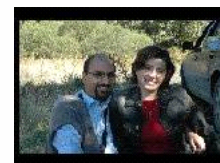
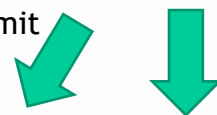
See also:

Eric Kee, Micah K. Johnson and Hany Farid -Digital Image Authentication from JPEG Headers (2011) IEEE TIFS

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Thumbnails Analysis

- Furthermore the Exif analysis permits to extract (if present) a further detailed preview of the image which is placed at the end of the JPEG file, and is present only in High-end Cameras.
- This preview is much more detailed and permit also to identify persons.



Thumbnail
Original Size

Comput



Casi Famosi

Cat Schwartz

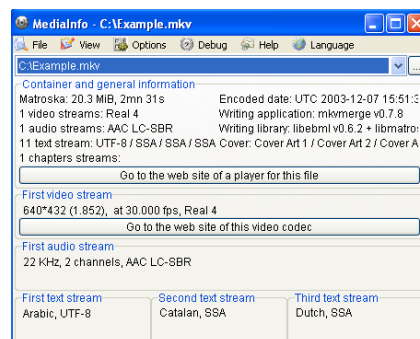


<http://www.welcometowallyworld.com/cat-schwartz/>

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Unsupervised Exif Analyzer

- <http://no.spam.ee/~tonu/exif>
- EXIF Phun by ascii (www.ush.it)
- Anche per audio e Video: **MediaInfo**
(<http://mediainfo.sourceforge.net>)



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

EXif for Stolen Camera

Many cameras save serial number information in the EXIF data of every photo you take.

stolencamerafinder

find your photos, find your camera



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

JPEG: La Quantizzazione

La maggior parte delle macchine fotografiche digitali memorizzano gli scatti in formato JPEG.

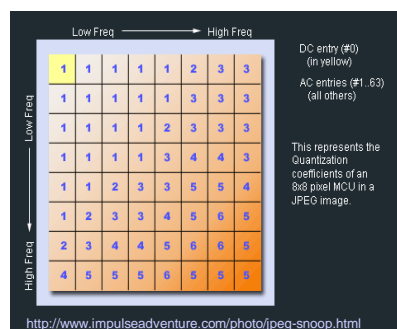
Questo schema di compressione lossy permette di stabilire, in qualche modo, un “grado” di compressione dei dati. Di solito, sono i produttori di fotocamere a stabilire i differenti “gradi” di compressione selezionabili, in funzione a statistiche che bilanciano qualità e dimensioni finali dei files.

Queste differenze possono essere utilizzate per identificare la sorgente (Modello di fotocamera, produttore) di un’immagine

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

JPEG as Source Camera Identification

Additional information can be obtained from the **Quantization Table** in the **JPEG** header. This header data, however, may **not be available** if the image is **Resaved** in a different format or recompressed.



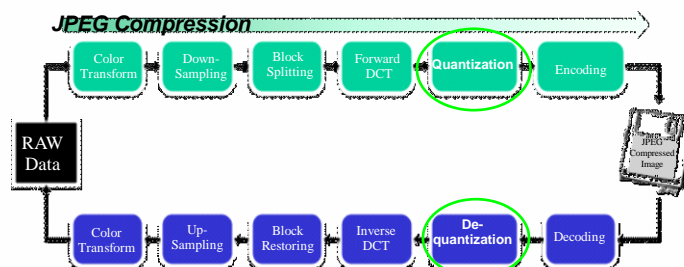
Another problem is the **Credibility** of information that can be easily replaced.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

JPEG Compression

- Converting an image into JPEG is a six step process:
 - The image is converted from raw **RGB data into YCbCr**;
 - A **downsampling** is performed on chrominance channels;
 - The channels are splitted into **8x8 blocks**;
 - A **Discrete Cosine Transform** is applied;
 - The DCT coefficient are **Quantized** (lossy) using fixed tables;
 - Finally an entropy coding (lossless **compression**) is applied and the image is said to be JPEG compressed

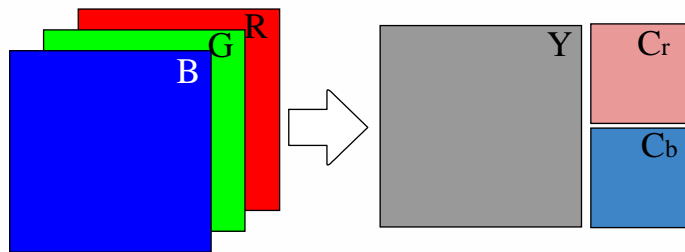


Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

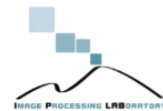


Color Conversion & Downsampling

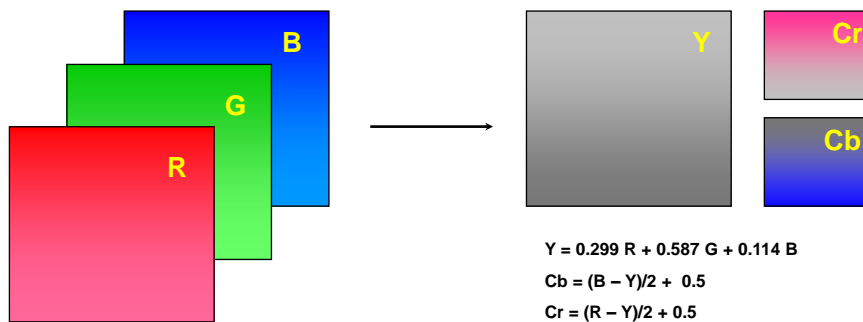
- First, the image is converted from **RGB** into a different colors space called **YCbCr**.
- The Y component represents the brightness of a pixel, the Cb and Cr components represent the chrominance (split into blue and red components).
- The Cr and Cb components are usually downsampled because, due to the densities of color- and brightness-sensitive receptors in the human eye, humans can see considerably more fine detail in the brightness of an image (the Y component) than in the color of an image (the Cb and Cr components).



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Color Transform



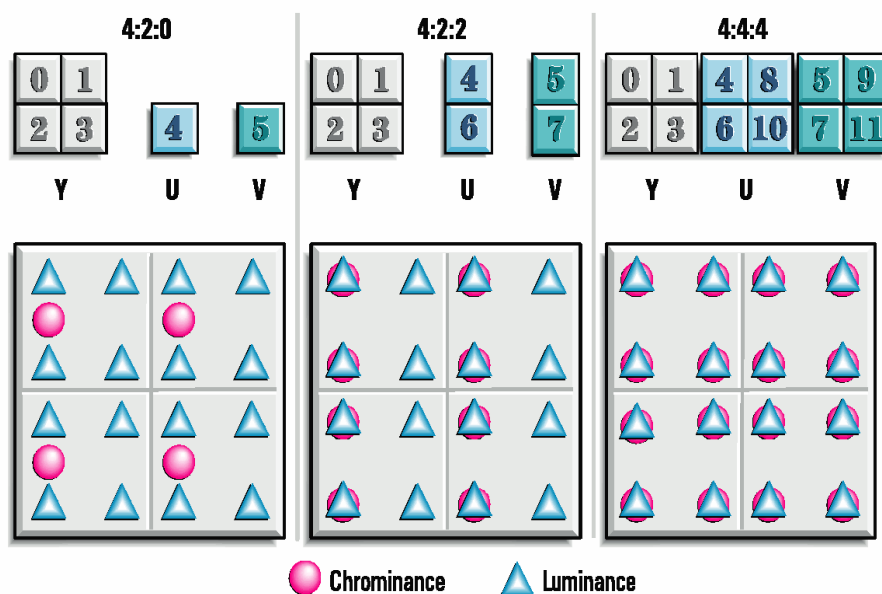
The human eye is more sensitive to luminance than to chrominance. Typically JPEG throw out $\frac{3}{4}$ of the chrominance information before any other compression takes place. This reduces the amount of information to be stored about the image by $\frac{1}{2}$. With all three components fully stored, 4 pixels needs $3 \times 4 = 12$ component values. If $\frac{3}{4}$ of two components are discarded we need $1 \times 4 + 2 \times 1 = 6$ values.

Example:



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

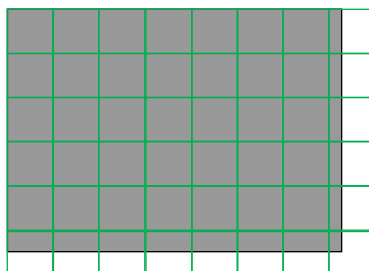
Chrominance subsampling



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Blocks 8x8

- After subsampling, each channel must be split into **8x8 blocks** of pixels.
- If the data for a channel does not represent an integer number of blocks then the encoder must fill the remaining area of the incomplete blocks with some form of dummy data.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Discrete Cosine Transform

- Next, each component (Y, Cb, Cr) of each 8x8 block is converted to a frequency-domain representation, using a normalized, two-dimensional type-II discrete cosine transform (DCT).

- As an example, one such 8x8 8-bit subimage might be:

52	55	61	66	70	61	64	73
63	59	55	90	109	85	69	72
62	59	68	113	144	104	66	73
63	58	71	122	154	106	70	69
67	61	68	104	126	88	68	70
79	65	60	70	77	68	58	75
85	71	64	59	55	61	65	83
87	79	69	68	65	76	78	94

- Before computing the DCT of the subimage, its gray values are shifted from a positive range to one centered around zero.
- For an 8-bit image each pixel has 256 possible values: [0,255]. To center around zero it is necessary to subtract by half the number of possible values, or 128.

$$\frac{2^{bit}}{2} = \frac{2^8}{2} = 2^7 = 128$$



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Discrete Cosine Transform

- Subtracting 128 from each pixel value yields pixel values on [-128,127] and we obtain the following matrix.

-76	-73	-67	-62	-58	-67	-64	-55
-65	-69	-73	-38	-19	-43	-59	-56
-66	-69	-60	-15	16	-24	-62	-55
-65	-70	-57	-6	26	-22	-58	-59
-61	-67	-60	-24	-2	-40	-60	-58
-49	-63	-68	-58	-51	-60	-70	-53
-43	-57	-64	-69	-73	-67	-63	-45
-41	-49	-59	-60	-63	-52	-50	-34

- The next step is to take the two-dimensional DCT, which is given by:

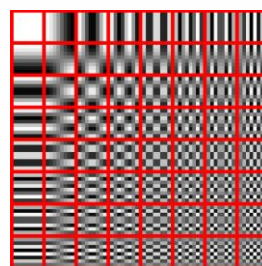
$$G_{u,v} = \alpha(u)\alpha(v) \sum_{x=0}^7 \sum_{y=0}^7 g_{x,y} \cos \left[\frac{\pi}{8} \left(x + \frac{1}{2} \right) u \right] \cos \left[\frac{\pi}{8} \left(y + \frac{1}{2} \right) v \right]$$

where

- u is the horizontal spatial frequency, for the integers $0 \leq u < 8$.
- v is the vertical spatial frequency, for the integers $0 \leq v < 8$.

- $\alpha_p(n) = \begin{cases} \sqrt{\frac{1}{8}}, & \text{if } n = 0 \\ \sqrt{\frac{2}{8}}, & \text{otherwise} \end{cases}$ is a normalizing function

- $g_{x,y}$ is the pixel value at coordinates (x, y)
- $G_{u,v}$ is the DCT coefficient at coordinates (u, v)



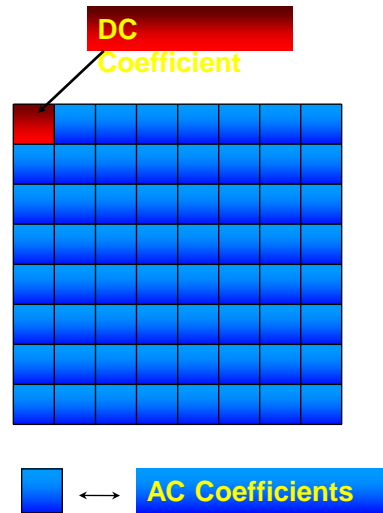
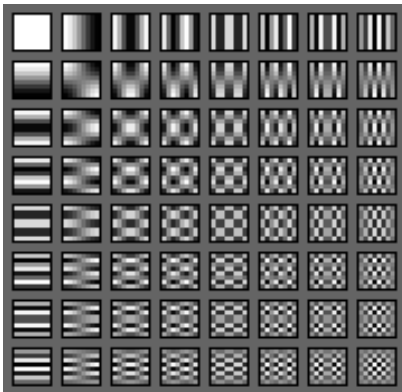
The DCT transforms 64 pixels to a linear combination of these 64 squares. Horizontally is u and vertically is v .

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



DCT basis

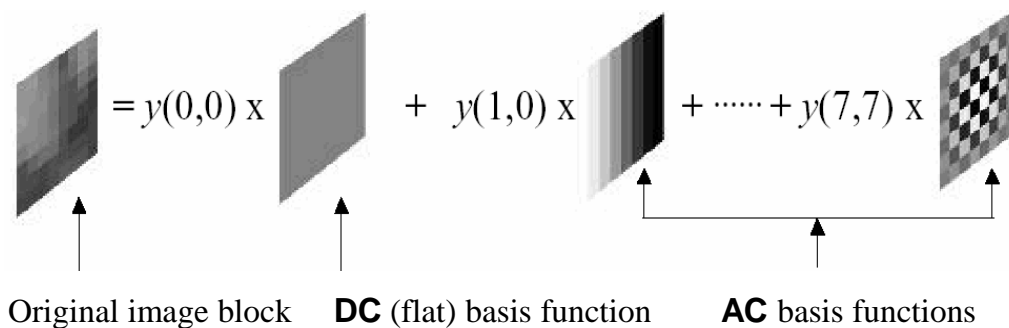
The 64 (8 x 8) DCT basis functions:



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

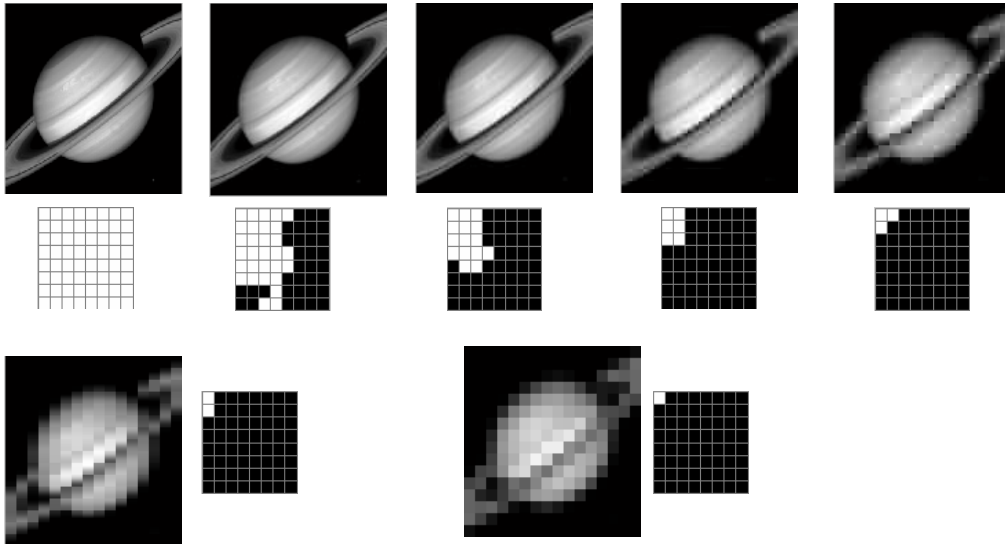
Image Representation with DCT

DCT coefficients can be viewed as weighting functions that, when applied to the 64 cosine basis functions of various spatial frequencies (8 x 8 templates), will reconstruct the original block.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

DCT example



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

DCT Coefficients Quantization

- The DCT coefficients are quantized to limited number of possible levels.
- The Quantization is needed to reduce the number of bits per sample.

Example:

101000 = 40 (6 bits precision) ®
Truncates to 4 bits = 1000 = 8 (4 bits precision).

i.e. $40/5 = 8$, there is a constant $N=5$, or the *quantization or quality factor* .

Formula:

$$F(u, v) = \text{round}[F(u, v) / Q(u, v)]$$

– $Q(u, v) = \text{constant} \Rightarrow$ Uniform Quantization.

– $Q(u, v) = \text{variable} \Rightarrow$ Non-uniform Quantization.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Standard Q-tables

Eye is most sensitive to low frequencies (upper left corner), less sensitive to high frequencies (lower right corner)

Luminance Quantization Table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Chrominance Quantization Table

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

The numbers in the above quantization tables can be scaled up (or down) to adjust the so called **Quality Factor QF**. (i.e. $Q^*(u,v) = QF \times Q(u,v)$)

Custom quantization tables can also be put in image/scan header.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Quantized DCT

$$X = \begin{bmatrix} 168 & 161 & 161 & 150 & 154 & 168 & 164 & 154 \\ 171 & 154 & 161 & 150 & 157 & 171 & 150 & 164 \\ 171 & 168 & 147 & 164 & 164 & 161 & 143 & 154 \\ 164 & 171 & 154 & 161 & 157 & 157 & 147 & 132 \\ 161 & 161 & 157 & 154 & 143 & 161 & 154 & 132 \\ 164 & 161 & 161 & 154 & 150 & 157 & 154 & 140 \\ 161 & 168 & 157 & 154 & 161 & 140 & 140 & 132 \\ 154 & 161 & 157 & 150 & 140 & 132 & 136 & 128 \end{bmatrix}$$

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

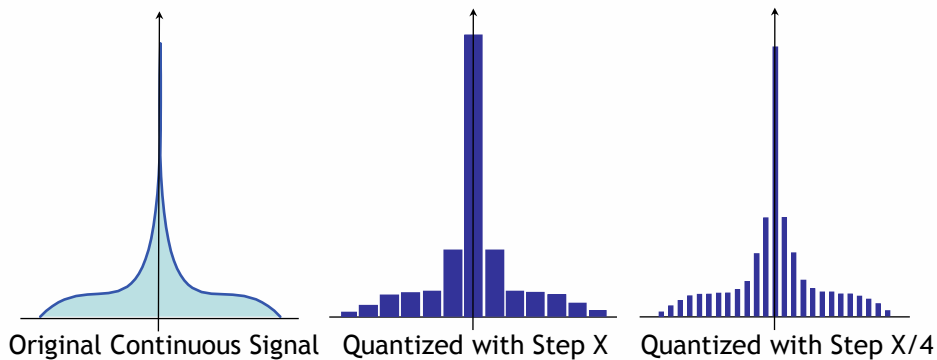
$$Y = \begin{bmatrix} 214 & 49 & -3 & 20 & -10 & -1 & 1 & -6 \\ 34 & -25 & 11 & 13 & 5 & -3 & 15 & -6 \\ -6 & -4 & 8 & -9 & 3 & -3 & 5 & 10 \\ 8 & -10 & 4 & 4 & -15 & 10 & 6 & 6 \\ -12 & 5 & -1 & -2 & -15 & 9 & -5 & -1 \\ 5 & 9 & -8 & 3 & 4 & -7 & -14 & 2 \\ 2 & -2 & 3 & -1 & 1 & 3 & -3 & -4 \\ -1 & 1 & 0 & 2 & 3 & -2 & -4 & -2 \end{bmatrix}$$

$$Z = \begin{bmatrix} 13 & 4 & 0 & 1 & 0 & 0 & 0 & 0 \\ 3 & -2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$z_{ij} = \text{round}(y_{ij} / q_{ij})$$

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Quantization



- The Quantization is usually used to convert continuous signal to a discrete space.
- In the example above we have processed a continuous signal, by using a larger quantization step X (thus reducing drastically the numbers of samples), and a smaller step X/4 which introduce more samples and is much more similar to the continuous signal.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Quantization Tables

- A typical quantization matrix, as specified in the original JPEG Standard, is as follows:

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

- The quantized DCT coefficients are computed with

$$B_{j,k} = \text{round} \left(\frac{G_{j,k}}{Q_{j,k}} \right) \text{ for } j = 0, 1, 2, \dots, N_1 - 1; k = 0, 1, 2, \dots, N_2 - 1$$

where G is the unquantized DCT coefficients; Q is the quantization matrix above; and B is the quantized DCT coefficients.

- Using this quantization matrix with the DCT coefficient matrix from above results in:
For example, using -415 (the DC coefficient) and rounding to the nearest integer

$$\text{round} \left(\frac{-415}{16} \right) = \text{round}(-25.9375) = -26$$

-26	-3	-6	2	2	-1	0	0
0	-2	-4	1	1	0	0	0
-3	1	5	-1	-1	0	0	0
-4	1	2	-1	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Quantization Tables

- The standard fixes that each image must have between one and four quantization tables.
- The most commonly used quantization tables are those published by the Independent JPEG Group (IJG) in 1998.
- These tables can be scaled to a quality factor Q .
- The quality factor allows the image creation device to choose between:
 - Larger, higher quality images
 - Smaller, lower quality images.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99
17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Quantization Tables

- For example, we can scale the IJG standard table using $Q=80$ by applying Eq. (2) to each element in the table. The resulting values are the following scaled quantization tables

6	4	4	6	10	16	20	24
5	5	6	8	10	23	24	22
6	5	6	10	16	23	28	22
6	7	9	12	20	35	32	25
7	9	15	22	27	44	41	31
10	14	22	26	32	42	45	37
20	26	31	35	41	48	48	40
29	37	38	39	45	40	41	40
7	7	10	19	40	40	40	40
7	8	10	26	40	40	40	40
10	10	22	40	40	40	40	40
19	26	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40

- Note that the numbers in this table are lower than in the standard table, indicating an image compressed with these tables will be of higher quality than ones compressed with the standard table. It should be noted that scaling with $Q=50$ does not change the table.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Quantization Tables

- The different QT could be classified into the following categories:
 - **Standard Tables:**
Images which use scaled versions of the QT published by Independent JPEG Group (IJG) standard;
 - **Extended Tables:**
Same as Standard Tables but have three tables instead of two. The third table is a duplicate of the second;
 - **Custom Fixed Tables:**
Images containing non-IJG QT that do not depend on the image being processed (Adobe Photoshop);
 - **Custom Adaptive Tables:**
These images do not conform to the IJG standard. In addition, they may change, either in part or as a whole, between images created by the same device using the same settings. They may also have constants in the tables; values that do not change regardless of the quality setting or image being processed.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Quantization Tables For Ballistics

“Considering only QT is not sufficient to discriminate between different source cameras, but it could be useful to clearly identify altered images.”

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Forgeries Identification through DCT

- The research activity in such area has started through the analysis of correlations between QT and DCT coefficients.
- Two techniques are under investigation regarding such aspect:
 - Detecting Forgeries by **Measuring Inconsistencies of Block Artifact**;
 - Exposing Digital Forgeries From **JPEG Ghosts** (under study);

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Measuring Inconsistencies of Block Artifact

- As manufacturers typically use different JPEG QT to balance compression ratio and image quality, the blocking artifact introduced in the images could be different.
- When creating forgeries, the resulted tampered image may inherit different kind of compression artifacts from different sources.
- These inconsistencies, if detected, could be used to check image integrity.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



DCT histograms anomalies

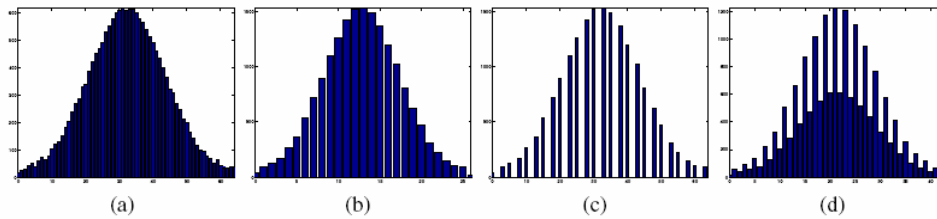


Fig. 4. The left two figures are histograms of single quantized signals with steps 2 (a) and 5 (b). The right two figures are histograms of double quantized signals with steps 5 followed by 2 (c), and 2 followed by 3 (d). Note the periodic artifacts in the histograms of double quantized signals.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Estimated Quantization Table

1	1	1	1	1	1	1	2
1	1	1	1	1	1	1	2
1	1	1	1	1	1	2	2
1	1	1	1	1	2	2	3
1	1	1	1	2	2	3	3
1	1	1	2	2	3	3	3
1	1	2	2	3	3	3	3
2	2	2	3	3	3	3	3

Original QT

2	1	1	1	1	1	3	2
1	1	1	1	1	3	3	1
1	1	1	1	2	3	1	1
1	1	1	1	3	3	3	3
1	1	1	3	1	1	3	3
1	1	3	1	3	4	4	4
1	3	4	3	5	4	6	4
3	1	1	4	4	4	4	4

Estimated QT

1	0	0	0	0	0	2	0
0	0	0	0	0	2	2	-1
0	0	0	0	1	2	-1	-1
0	0	0	0	2	1	1	0
0	0	0	2	-1	-1	0	0
0	0	2	-1	1	1	1	1
0	2	2	1	2	1	3	1
1	-1	-1	1	1	1	1	1

Differences between the two tables.

- Here is an example of estimated quantization table onto a Canon 400D tampered image.
- Some slight differences have been found in the Estimated Q-Table.

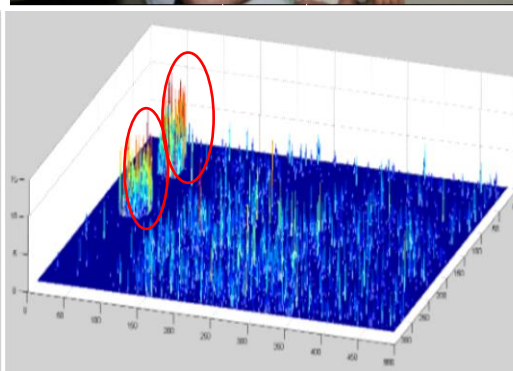
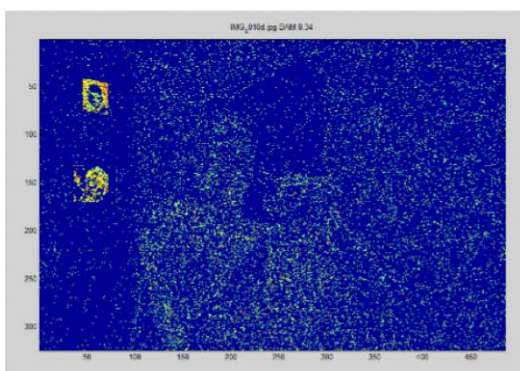


Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



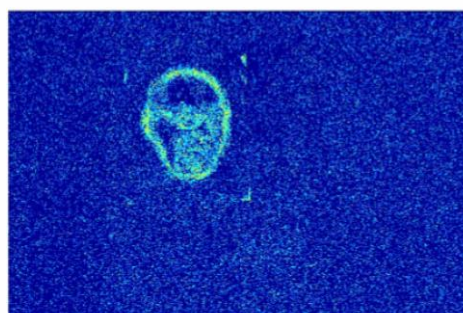
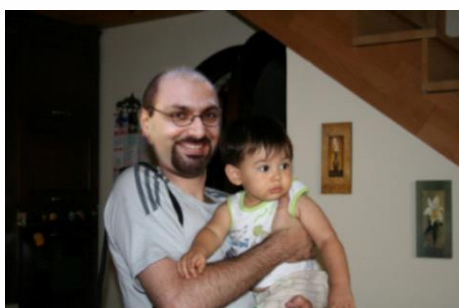
Results 1/4

- By taking into account such anomalies the following error map has been generated.
- The map clearly underlined the part of the image that contain forgeries (max value 14.7).

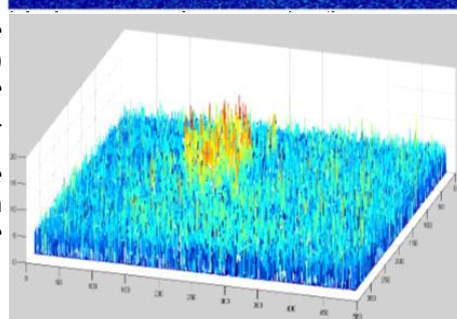


Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Results 2/4



- In this experiment we have taken a face from a different (downsampled image) we have removed the background of the picture and pasted it over the original face.
- During the process of cancelling the background the corners have been coarsely removed, as visible in the error map (max value 18.3).

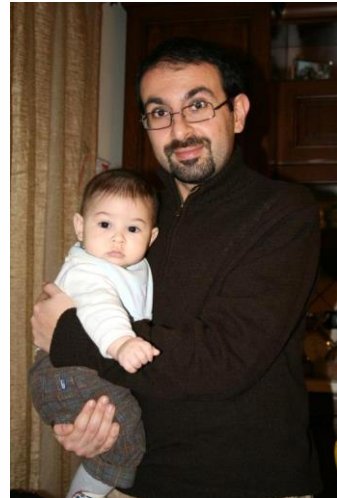


Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

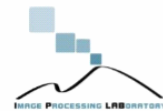
IMAGE PROCESSING LABORATORY

Results 3/4

Original Images



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Results 3/4

Tampered Image

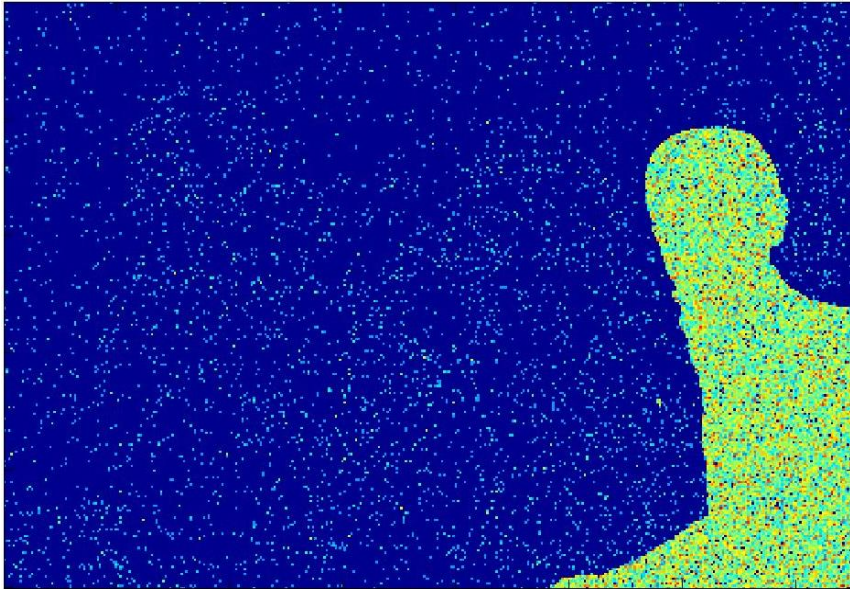


Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



Results 4/4

Estimated Map.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Manuale operativo....

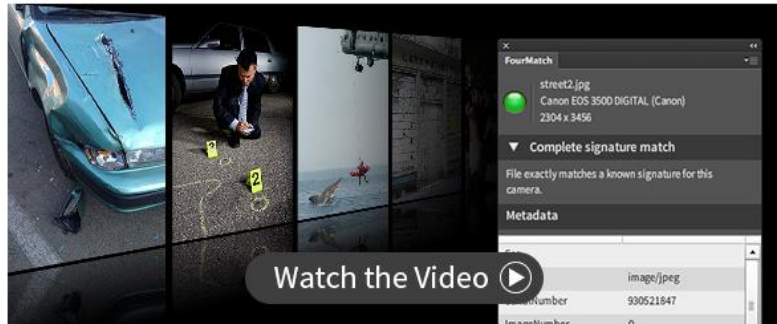
Analizzare nell'ordine:

- Proprietà del file
- Metadati (EXIF, XMP, ecc)
- Thumbnail
- Parametri di codifica
- Verificare se tutto coincide con quello dichiarato (Modello Camera, risoluzione, tabelle di codifica, ecc.)
- Anomalie nei contenuti
 - Cut&Paste
 - Luce
 - ...

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Software

Need Evidence a Photo Is Real?

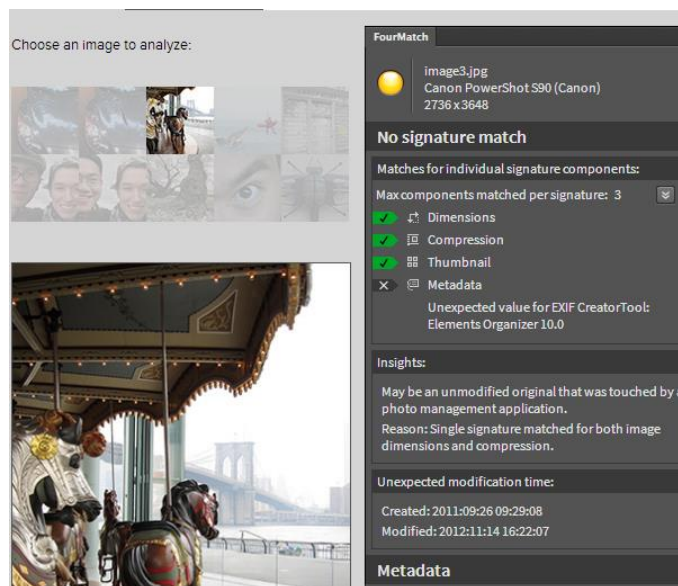


FOURMATCH™ Authenticate images instantly.

FourMatch is an extension for Adobe Photoshop that instantly analyzes any open JPEG image to determine whether it is an untouched original from a digital camera. Now, you can quickly identify files that have not previously been edited.

<http://www.fourandsix.com/fourmatch/>

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



<http://www.fourandsix.com/fourmatch/>

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Digital Camera Identification: Camera based methods

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Identificazione della Camera



Fingerprint basato su:

- Pattern legato al rumore del sensore;
- Dati derivati dal particolare formato (raw, EXIF, codifica JPEG, ecc.);
- Alibi?

Camera identification

Reliable identification of the device used to acquire a particular digital image is especially prove useful in the court for establishing the origin of images presented as evidence.

Forensic methods capable of determining that two clips came from the same camcorder or that two transcoded versions of one movie have a common source will obviously help investigators draw connections between different entities or subjects and may become a crucial piece of evidence in prosecuting the *pirates*.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Obiettivo



(a) Canon 1



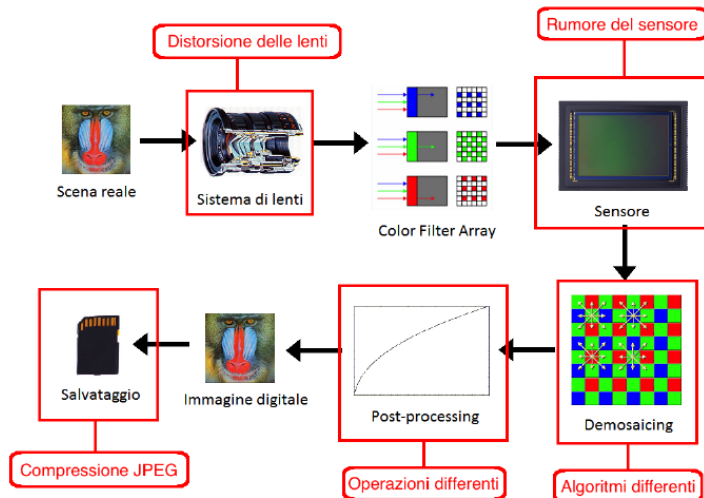
(b) Canon 2



(c) Casio

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Typical Imaging Pipeline



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

CFA Color Filter Array

- La maggior parte delle macchine fotografiche è equipaggiata con un singolo sensore che cattura le immagini attraverso un Color Filter Array (un filtro a griglia dei colori). La pluralità dei filtri CFA è composta da una griglia che alterna i tre colori Rosso, Verde e Blu, posizionata direttamente sul sensore. Poiché, con questo sistema, è possibile catturare solo un canale per pixel, per ottenere un'immagine a colore occorre ricostruire le due componenti mancanti per ogni singolo pixel (**Demosaicing**).

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

CFA Color Filter Array

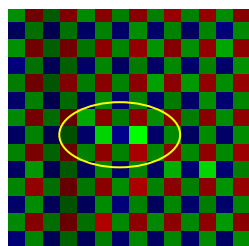
- Trascurando la metodologia utilizzata al fine di ricreare i tre piani di colore, l'interpolazione, in genere, introduce specifiche correlazioni statistiche tra sottoinsiemi di pixel, in ognuno dei tre canali. Poiché il filtro CFA è una griglia con una tessitura periodica, queste correlazioni avranno un andamento periodico. Sfruttando questa **periodicità** è possibile individuare un tipo di firma digitale associata all'interpolazione del colore.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Existing Approaches (1)

Analisis of the *pixels defect* (spike pixels or dead pixels).

This method represent a reliable camera identification even from lossy JPEG compressed images. Some cameras do not contain any defective pixels or they are eliminated by post-processing algorithms on-board.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Existing approaches (2)

- Ogni banda di colore dell'immagine, mostra dei tratti e degli **schemi definiti** a prescindere dal contenuto dell'immagine stessa che dipendono da:
 - la configurazione del **Color Filter Array**
 - l'algoritmo utilizzato per il **demosaicing**;
 - l'elaborazione/trasformazione del **colore** (fase di post-processing).
- Per individuare le differenze che risultano essere presenti fra immagini catturate con fotocamere differenti occorre estrarre **34 caratteristiche** da ogni immagine, divise in due grandi gruppi:
 - Misure relative al **colore**
 - Misure relative alla **qualità** dell'immagine
- La classificazione avviene tramite un classificatore **SVM**

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

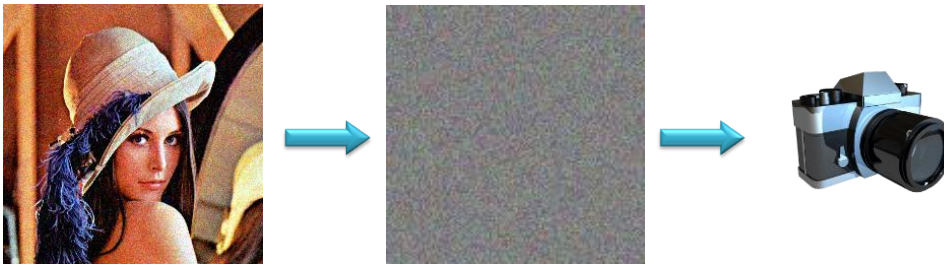
Existing approaches (2)

- Camera identification based on ***supervised learning***.
- Each image is represented using a vector of numerical ***features*** (e.g., average pixel values, RGB pairs correlation, wavelet domain statistics, image quality metrics,...) extracted from it. These features are then trained by a multi-class SVM classifier (support vector machine) to distinguish images from different cameras

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Camera source identification noise based

Sensor output carries not only pure signal but also various noise components. Sensor noise model could be used as a representative feature for cameras.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Noise

Durante tutto il processo di acquisizione ed elaborazione, l'immagine può essere affetta da rumore o imperfezioni di diversa natura.

Il rumore nelle immagini digitali si evidenzia in prevalenza come una certa granulosità o puntinatura monocromatica (luminance noise) e/o come puntini o macchioline colorate (chroma noise) evidenti soprattutto nelle aree uniformi come il cielo, o in aree scure con poco dettaglio. L'effetto è molto simile a quello delle immagini da pellicola ad alta sensibilità.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Image noise

Image noise is a random, unwanted, fluctuation of pixel values in an image. There are numerous sources of imperfections and noise that enter into various stages of the image acquisition process. Main noise sources are:

Photon Shot Noise:

occurring when a finite number of photons is small enough to give rise to detectable statistical fluctuations in a measurement.

Dark Current (Thermal Noise)

this type of noise exists even when the sensor is not exposed to any incident light, and increases as the temperature of the sensor increases.

Readout noise (Bias Noise)

It is the noise generated during the readout of the sensor and does not depend on the shooting conditions

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Image noise

Reset Noise

happens when resetting the pixel, prior charge accumulation. Pixel does not exactly reset to zero.

Pattern Noise

A deterministic component that stays approximately the same if multiple pictures of the exact same scene are taken.

Quantization Noise

The analogue to digital converter in each column introduces noise due to the quantization process.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Quando il sensore acquisisce una scena, anche nelle migliori condizioni di illuminazione, l'immagine digitale mostrerà comunque piccole variazioni di intensità tra i singoli pixel, a causa delle numerose fonti di rumore che intervengono nel processo di formazione dell'immagine.

Come precedentemente accennato, il rumore è composto da una componente casuale che dipende dal photon shot noise, rumore termico, ecc., e una componente fissa, dovuta al **pattern noise**, che **lascia una traccia pressoché identica** su tutte le immagini acquisite con lo stesso sensore.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

In particolare, ogni fotocamera digitale possiede un sensore lievemente differente dalle altre dello stesso modello, per via di un “disturbo” univoco e riconoscibile, ciò permette di identificare il sensore a partire dalle immagini, sfruttando la stessa idea che ci consente di distinguere le tracce univoche lasciate dalle canne delle armi da fuoco sui proiettili.

Il disturbo generato nelle immagini è legato sia al sensore in sé, che alle minuzie nella costruzione e nell'assemblaggio di ogni dispositivo. Questo assicura una differenza tra singoli dispositivi sufficiente a rendere improbabile la presenza di due camere che generino il medesimo disturbo, proprio come avviene per le impronte digitali.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Sensor identification using pattern noise

Between the different noise source presented, pattern noise differs from the other because of its deterministic properties, thus can be used for camera identification. Pattern noise consists of two main components which are:

Fixed Pattern Noise (FPN) and
Photo Response Non-Uniformity Noise (PRNU)



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

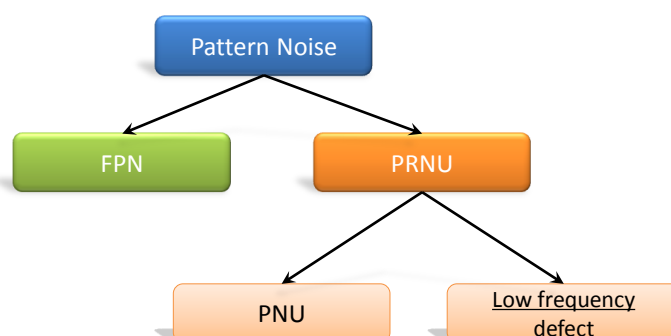
Pattern noise

Main component of the fixed pattern noise (FPN) is due to dark currents which refers to pixel-to-pixel differences when the sensor array is not exposed to light.

Photo-response nonuniformity noise (PRNU), is composed by:

pixel non-uniformity (PNU), which is defined as by sensitivity of pixels to light and it is primarily caused by the imperfections in the sensor manufacturing process.

low frequency defect, due to light refraction on dust particles and optical surfaces and zoom settings.



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Sensor identification using pattern noise

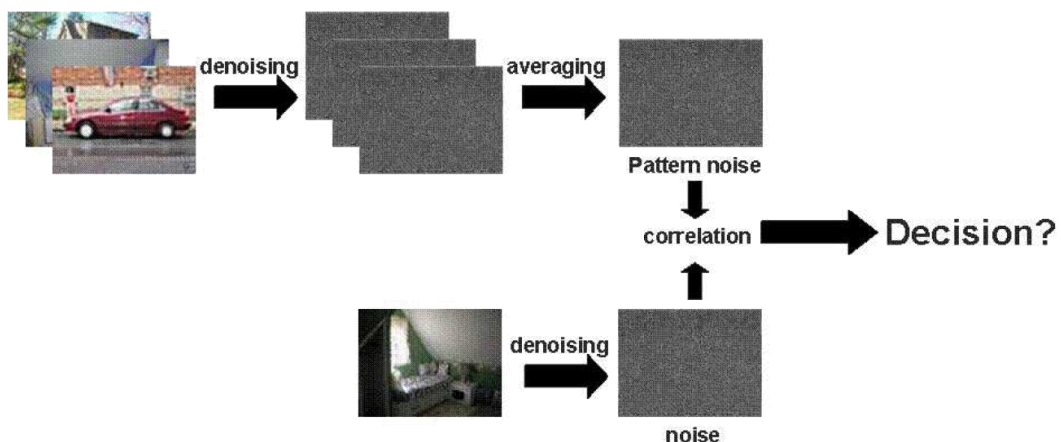
Pixel non-uniformity noise (PNU) associated with a sensor can be used for source identification in the following way:

Extract the *reference pattern* using a denoising algorithm from a set of images captured by the same camera. Reference pattern must be averaged to eliminate random component of the noise.

Determine whether a given image is captured by a digital camera verifying that the noise pattern extracted from the individual image is *correlated* with the reference pattern of the digital camera. A decision is made based by comparing the measured correlation statistic to a pre-determined decision threshold.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Sensor identification using pattern noise



Computer Forensics A.A. 2012-2013 - Prof. S. Battiato



(a) Originale



(b) Rumore residuo

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

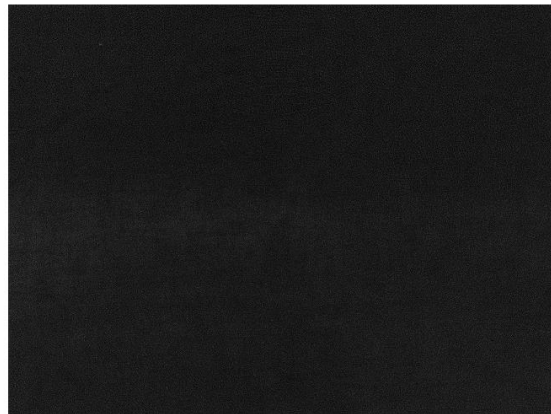
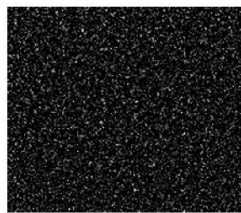
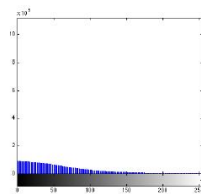


Figura 2.3: Esempio di impronta digitale.



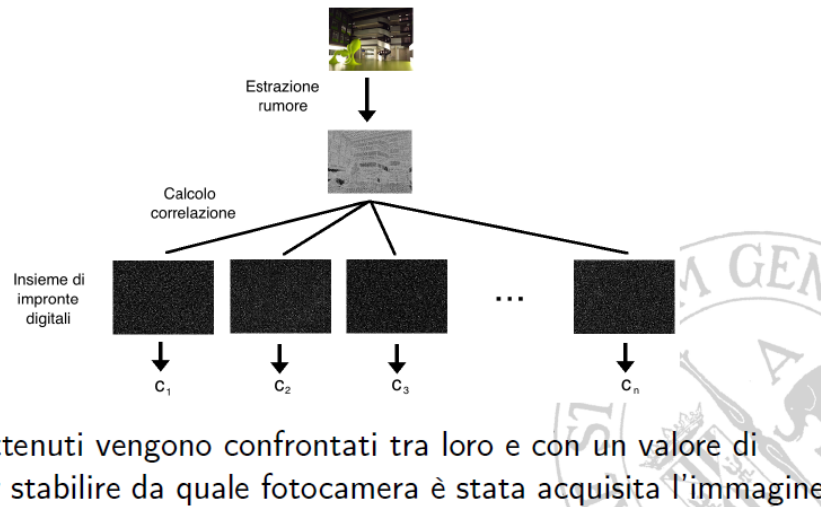
(a) Particolare



(b) Istogramma

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

- Occorre calcolare un valore di **correlazione** fra il rumore estratto dall'immagine in esame e le impronte digitali calcolate



- I valori ottenuti vengono confrontati tra loro e con un valore di soglia per stabilire da quale fotocamera è stata acquisita l'immagine

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Sensor identification using pattern noise

This method provide good results, and is quite reliable also using:

- images with different level of *JPEG compression* (low, medium and high)

- images processed using point-wise operator such as brightness/contrast adjustment or gamma correction.

- images acquired by two cameras of the same brand and model.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

La procedura appena descritta è la più semplice e nota. Recentemente sono state proposte diverse migliorie e piccole varianti che rendono l'algoritmo di identificazione ancora più affidabile. Alcuni autori hanno presentato delle tecniche attraverso le quali è possibile migliorare la stima del reference pattern, che fanno uso di piccoli training set e utilizzano particolari procedure di classificazione.

Una implementazione open source di questa tecnica è disponibile su

<http://sourceforge.net/projects/prnucompare/>

Operazioni di post-processing applicate ai reference pattern stimati, inoltre, possono ridurre la correlazione tra reference pattern di fotocamere della stessa marca e modello, riducendo quindi ulteriormente il numero di errori della procedura.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Forging and malicious processing

Intentionally removing the pattern noise from an image to prevent identification. The easiest way to prevent a simple detection of the reference pattern are slight rotation, possibly combined with other processing that might include resizing, cropping, and filtering.

Extracting the noise and copying it to another image to make it appear as if the image was taken with a particular camera. This kind of malicious processing is more difficult: requires to remove pattern noise from the image that we want forging and add to it the reference pattern noise of another camera, avoiding to create visible artifacts.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

AntiForensics

Fortunatamente l'eliminazione del pattern noise, o la sovrapposizione dello stesso su un'immagine, sono operazioni abbastanza complesse, soprattutto per un non esperto. Se l'alterazione non è ben fatta, infatti, si potrebbe rischiare, di aggiungere artefatti che potrebbero far risaltare il tentativo di manomissione, e comunque di non riuscire ad ingannare l'algoritmo di identificazione.

D'altra parte, purtroppo, operazioni molto elementari sull'immagine, come un crop o una rotazione potrebbero rendere l'immagine irriconoscibile. In rete, ad esempio, è possibile trovare siti come questo: <http://www.instructables.com/id/Avoiding-Camera-Noise-Signatures/>

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

References

- J.D. Kornblum, "Using JPEG quantization tables to identify imagery processed by software", Digital investigation Journal, n.5 (2008), pp.S21-S25;
- H. Farid, "Digital Image Ballistics from JPEG Quantization", (2006) <http://www.cs.dartmouth.edu/~farid/publications/tr06a.pdf>
- N. Krawetz, "Hacker Factor Solutions" <http://www.hackerfactor.com/>
- Kharrazi, M., Sencar, H. T., and Memon, N.: "Blind Source Camera Identification" Proc. ICIP' 04, Singapore, October 24-27, 2004.

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

References

- Geradts, Z., Bijhold, J., Kieft, M., Kurosawa, K., Kuroki, K., and Saitoh, N.: “*Methods for Identification of Images Acquired with Digital Cameras*” Proc. of SPIE, Enabling Technologies for Law Enforcement and Security, vol. 4232, pp. 505-512, February 2001.
- Jan Lukas, Jessica Fridrich, and Miroslav Goljan, “*Digital camera identification from sensor noise*” IEEE Transactions on Information Security and Forensics, vol. 1(2), pp. 205-214, June 2006
- S. Bayram, H. T. Sencar, and N. Memon, “*Improvements on source camera-model identification based on CFA interpolation*” Proc. of WG 11.9 Int. Conf. on Digital Forensics, 2006
- M. Chen, J. Fridrich, and M. Goljan “*Source Digital Camcorder Identification Using Sensor Photo-Response Non-Uniformity*”, Proc. of SPIE, January 2007

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

References

- Cynthia Baron, **Adobe Photoshop Forensics**, Course Technology PTR, 2007, ISBN-13: 978-1598634051
- G. Reis, **Analisi Forense con Photoshop** - - Apogeo - 2008 ISBN: 9788850327447
- IEEE **Signal Processing Magazine** Vol 2, 2009 - Special Issue on *Digital Forensic*

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

Contacts

For further information

Image Processing Lab

Università di Catania

<http://iplab.dmi.unict.it>

Email:

battiato@dmf.unict.it

Computer Forensics A.A. 2012-2013 - Prof. S. Battiato

