UNIVERSITÀ
DEGLI STUDI
FIRENZE

Advances on Multimedia Forensics
Introduction

Prof. Alessandro Piva

Dept. of Information Engineering

University of Florence (Italy)

alessandro.piva@unifi.it

Alessandro Piva

Problem & Motivation

- How much can we trust digital visual content?
- visual signals are the preferred means to get access to information
  - immediacy : images are a fundamental part of web-documents
  - supposed objectivity: it is still common for people to trust what they see, rather than what they read.

Alessandro Piva

Motivation

- When observing an image or a video on a web site, often people do not realize that such media have undergone a long series of transformations before appearing in its current form.

Alessandro Piva

Problem & Motivation

- We are living in a world where seeing is no longer believing – the technology that allows for digital media to be manipulated and distorted is developing at break-neck speeds.

- *With the advent of high-resolution digital cameras, powerful personal computers and sophisticated photo-editing software, the manipulation of photos is becoming more common.*

- The use of a fake image - image of a scene that wasn't captured as the image would imply – is common in several fields.

Alessandro Piva

Problem & Motivation: gossip

- 2007: The French Magazine Paris Match altered a photograph of French President Nicolas Sarkozy by removing some body fat. The magazine said it had tried adjusting the lighting on the picture. "The correction was exaggerated during the printing process," the magazine said.

Alessandro Piva

Problem & Motivation: news

- After it came to light that a September 2013 photo of the conflict in Syria had been modified to remove a video camera that was visible in the frame, the Associated Press terminated its relationship with Pulitzer-prize-winning freelance photographer Narciso Contreras.

Alessandro Piva

Problem & Motivation: propaganda

- July 2008: the image of an Iranian missile test, coming from the web site of the media arm of Iran's Revolutionary Guards, appeared on the front page of many major newspapers.
- After the publication of this photo, it was revealed that the second missile from the right was digitally added to the image in order to conceal a missile on the ground that did not fire.

Alessandro Piva

Published image

Alessandro Piva

Authentic image

Alessandro Piva

Manipulations

Alessandro Piva

Problem & Motivation: sport

- **February 2011:** Spanish sports newspaper *AS* published this photo as evidence of an offside violation in a match between Spanish teams Athletic Bilbao and Barcelona.

Alessandro Piva

Problem & Motivation: sport

- The original shows that a defender had been digitally removed from the photo, and thus no violation occurred.

- *AS* apologized saying that it was caused by an infographics error.

Manipulated image and original one

Alessandro Piva

Problem & Motivation: commercial

- Photo retouchers can dramatically alter a person's appearance.

Kee E , Farid H PNAS 2011;108:19907-19912

Alessandro Piva

Problem & Motivation: fashion

- Photo retouchers can subtly alter a person's appearance.

photo editing [before (top row) and after (bottom row)].

Kee E , Farid H PNAS 2011;108:19907-19912

14

Alessandro Piva

Problem & Motivation: scientists

- Also the scientific community has been experiencing the ease of image manipulation in journal publications.

- Impact of image processing software in science was addressed in 2005 in an article in journal *Nature*: in 1990, 2.5% of contentions examined by the U.S. Office of Research Integrity, which monitors scientific misconduct, involved suspect scientific images. By 2001, the trend was impressively increasing reaching nearly 26%.

Alessandro Piva

Problem & Motivation: CG or Real ?

- It is becoming everyday most difficult to distinguish computer

http://area.autodesk.com/fakeorfoto/challenge

Alessandro Piva

Well…

Alessandro Piva
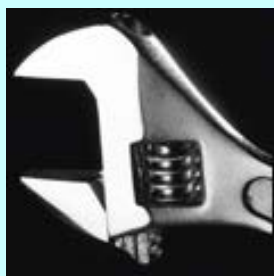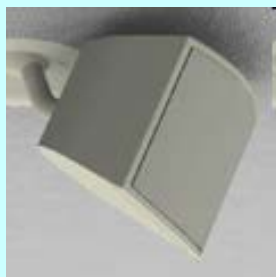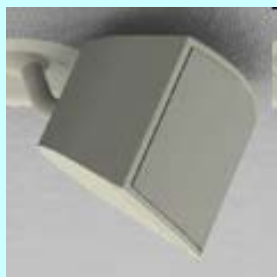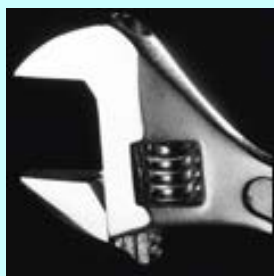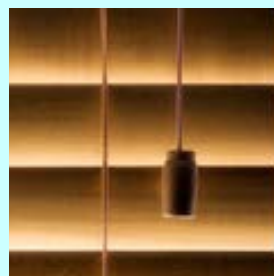
Image history

- As shown by all the presented examples, the growth in image and video tampering is having a significant impact in our daily life and in our society.

- Thus, there is an ever increasing interest in processing tools supporting the authentication of the image history

Alessandro Piva

Image history verification

Available tool for the analysis of image history and integrity:

- Visual analysis of the image content
- Analysis of the image file
- Analysis through processing techniques of the image content

Alessandro Piva

Visual analysis of the image content

- Our perception is the first line of defense at identifying fake images.

- Look at this example:
  - The cat is obviously too big.
  - The man should have leaned backwards more to properly hold a cat of this weight.

Alessandro Piva

Visual analysis of the image content

- But our perception can fail to detect a fake image if there is no cause for suspicion:

- photorealistic computer graphics rendered using Autodesk 3-D Max Studio.

- Expertise is needed to detect well done modifications

Alessandro Piva

Analysis of the image file

Image file composed by:

- Header with Metadata =
  "description of the content"

- Data =
  "image samples"

- Image formats
    - **JPEG**   (lossy compression)
    - **TIFF** (lossless compression)
    - **RAW** (no standard)

Make	Canon
Model	Canon PowerShot A50
Orientation	top, left side
X Resolution	180 dots per inch
Y Resolution	180 dots per inch
Resolution Unit	Inch
Date/Time	2000:01:25 04:41:26
Shutter Speed Value	1/32 sec
Aperture Value	F5.6
Exposure Bias Value	0
Subject Distance	1.684 metres
Metering Mode	Center weighted average
Flash	No flash fired

10	10	10	10	10	10	10	10
10	10	10	50	50	10	10	10
10	10	50	90	90	50	10	10
10	50	90	90	90	90	50	10
10	50	90	90	90	90	50	10
10	10	50	90	90	50	10	10
10	10	10	50	50	10	10	10
10	10	10	10	10	10	10	10

Image metadata

- Some metadata is written by the camera and some is input by the photographer and/or the editing software.

- Mostly used: EXIF or EXchangeable Image File Format
  - Established by JEIDA (Japan Electronic Industry Development Association http://it.jeita.or.jp/jhistory/index-e.html)
  - The metadata tags defined in the Exif standard cover a broad spectrum of information

Alessandro Piva

EXIF: important data

- Camera brand and model
- Date/time acquisition
- Date/time of last modification
- Image Processing Software used
- JPEG quantization table

- All these data can thus be used to understand the history of the image; let's see in detail the content of EXIF data.

Alessandro Piva

EXIF data

- Let's consider the EXIF of this JPEG image:

Alessandro Piva

EXIF data

- I took the original image and resized it to 50%, that is from 4272x2848 pixels to 2136x1424 pixels by using the GIMP image processing tool.

- The image was then resaved in JPEG format.

- Let's now check the EXIF of the new image.

Alessandro Piva

EXIF data

- Date of last modification changed, different from acquisition one

Alessandro Piva

EXIF data

New image size

Alessandro Piva

EXIF data: can we trust them?

- Not a maintained standard

- Most image editors damage or remove the Exif metadata to some extent upon saving.

- The standard defines a proprietary and manufacturer-specific MakerNote tag, which allows camera manufacturers to place any custom metadata in the file.

- Standard only for TIFF or JPEG —no provision for a "raw" type which is a direct data dump from the sensor device.

- Many cameras also capture video, but no Exif provision for video files.

Alessandro Piva

EXIF data: can we trust them?

- Exif is very often used in images created by scanners, but the standard makes no provisions for any scanner-specific information.

- Photo manipulation software sometimes fails to update the embedded thumbnail after an editing operation.

- There is no way to record time-zone information along with the time, rendering stored time ambiguous.

Alessandro Piva

EXIF data: can we trust them?

- The are several free tools such as ExifTool or Opanda Power Exif that allow to remove or modify the Exif tag, so it is possible to hide the presence of modifications into the image.

Conclusion:

- only the analysis of EXIF tag does not prove if the image is authentic.

Alessandro Piva

Tools for image authentication

- Scientific community is very active in this field, coming up with several methods for authentication and integrity verification of digital images.

- approaches divided into active and passive techniques.

Alessandro Piva

Tools for image authentication

- Active approaches require that the acquisition device generates some information added to the digital image.

- Passive techniques just analyze the digital image as it is, without any a priori information.

Tools for image authentication

Active approaches:

Cryptographic Digital Signature:

– Extract features for generating authentication signature at source side and verify image integrity by signature comparison at the receiver side.

• Fragile Digital Watermarking

– Insert a digital watermark at the source side and verify watermark integrity at the detection side.
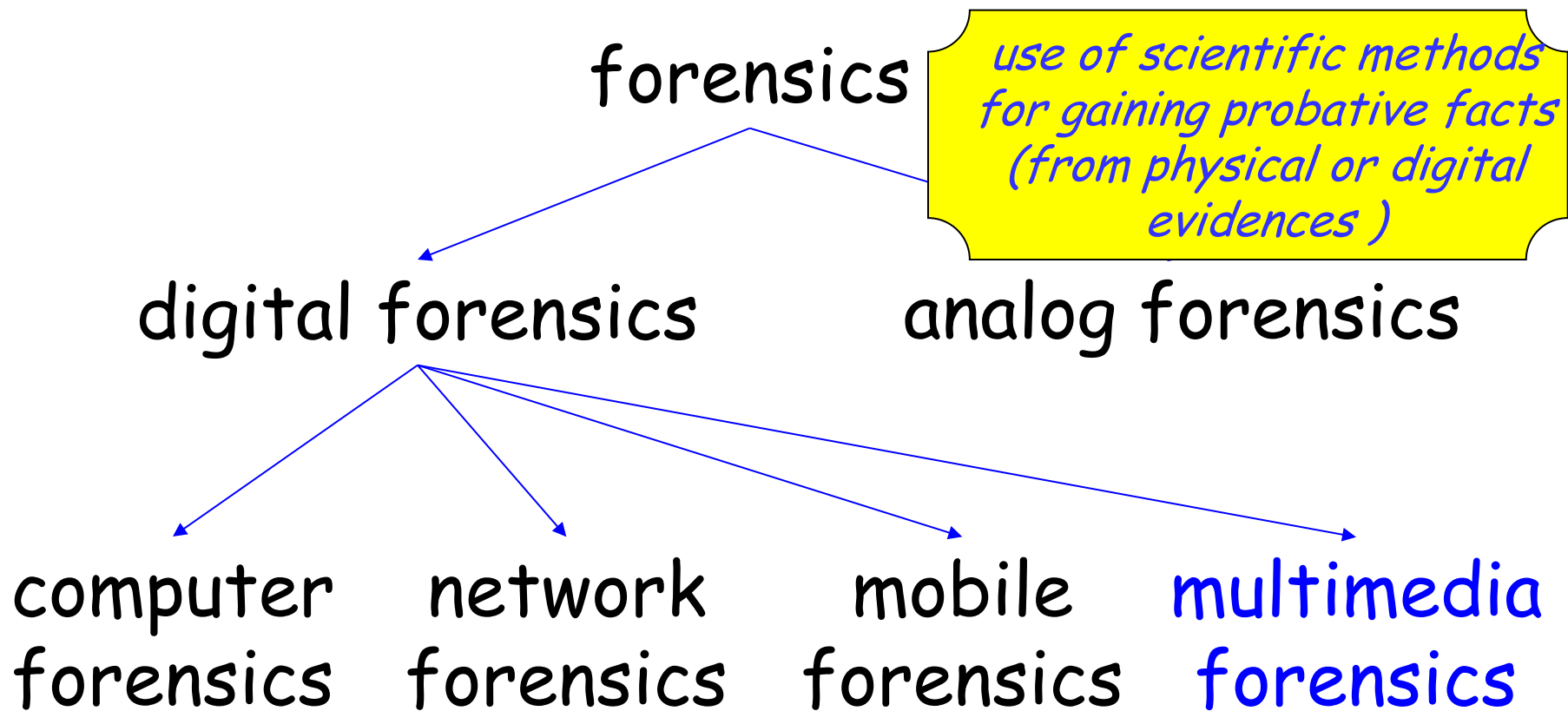
Active Approaches

- Effective if we have:
  - A specially equipped and trustworthy camera that inserts the watermark or computes the signature
  - A secure watermarking /signature algorithm
  - A widely accepted watermarking / signature standard
  - Watermark that does not degrade image quality

Alessandro Piva

Tools for image authentication

Passive or blind approaches

- Multimedia forensics
  - A branch of forensics
  - Without any prior information, verifying whether an image is authentic or not.
  - Advantages:
    - No need for watermark embedding or signature generation at the source side.
    - No need for a standard
    - No need for a priori knowledge about the acquisition device

Alessandro Piva

Forensic Science: forensics

forensics

use of scientific methods
for gaining probative facts
(from physical or digital
evidences)

digital forensics   analog forensics

computer   network   mobile   multimedia
forensics   forensics   forensics   forensics

Alessandro Piva

Digital Forensics

- In the Report from the First Digital Forensic Research Workshop (DFRWS) - **2001**, was given the definition for the Digital Forensic Science, so to include all the scientific methodologies:

> ### Digital Forensic Science
> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Alessandro Piva

Multimedia Forensics

- Inherent traces – characteristic artifacts - (we define them as digital fingerprints or footprints) are left behind in a digital media during the creation and any other process.

- Conventionally, footprints are considered as undesired effects. Considerable efforts spent to reduce these artifacts.

Alessandro Piva

Multimedia Forensics

We reverse this perspective completely:

footprints are not artifacts to remove

but

footprints are considered as an asset

i.e., a source of additional information about the multimedia object history, which can be leveraged to reconstruct the processing chain applied to the audio-video digital object.

- History of a digital content can be reconstructed by analysing these traces

Alessandro Piva

Image Forensics

- Given a digital image, image forensics techniques try to answer a number of forensic questions related to:

- source identification
  - What is the origin of the image ?
  - Developed techniques retrieve information on the source device at different levels.

- integrity verification / tampering detection
Has the image suffered some processing ?

Alessandro Piva

Source identification

- Level 1

  – Which CLASS
    of device?

digital camera

computer generated

scanner

cell phone
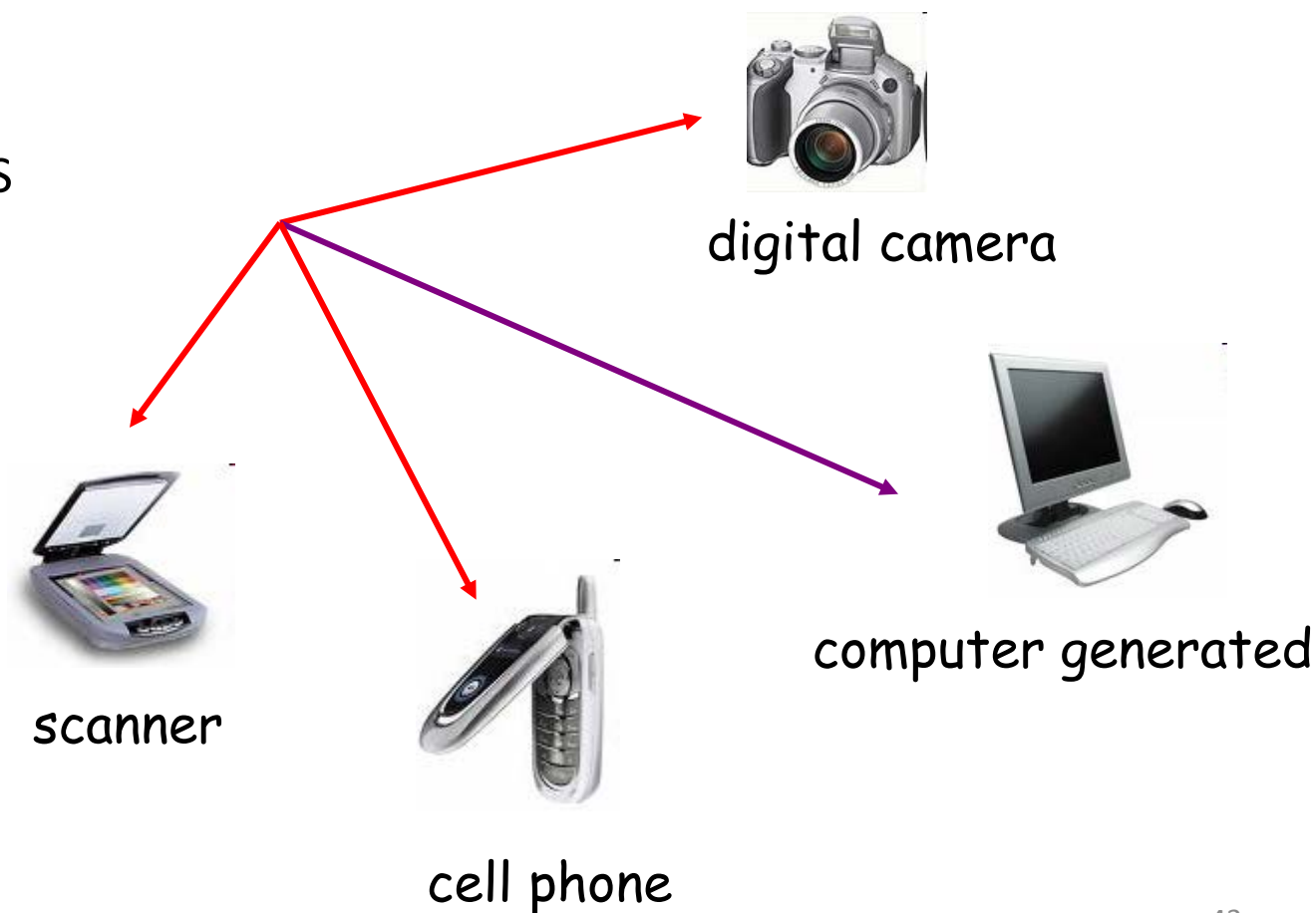
Source identification

- Level 2
- We know the picture was taken by a camera...
  - Which BRAND / MODEL ?

Nikon?
Canon?
Pentax?

Coolpix P80?
Coolpix S500?

Alessandro Piva

Source identification

- **Level 3**

  – Which SPECIFIC DEVICE took the picture?

    Which *Coolpix* P60?

Serial Number
000111101

Serial Number
000111103

Serial Number
000111106

Alessandro Piva

Tampering detection

- Image semantic content can be altered:
  - By altering the colors or other features of an image through simple image processing techniques like histogram modification or contrast enhancement:

1994: the image of murderer OJ Simspon which appeared on the cover of the magazine Time (right) was altered in brightness and color to make the subject look more menacing. The original was published by the magazine Newsweek (left).

Alessandro Piva

Tampering detection

- Image semantic content can be altered:
  - by removing undesired objects
  - Forgers need to "fill" the region of the image from which the object has been removed. A typical solution in this case is to copy a portion of the same image and replace with it the void left from the deletion (copy-move technique)

Original

Tampered

Alessandro Piva
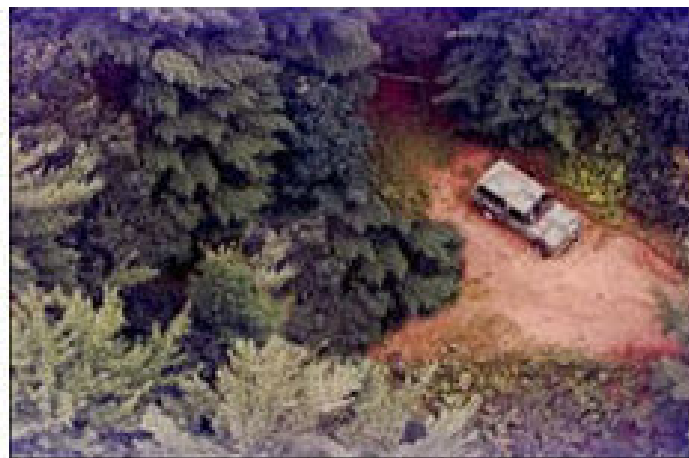
Tampering detection

- Image semantic content can be altered:
  - by adding new content, usually coming from another image
  - *Image splicing* consists of the composition of an image using parts of one or more parts of images

Alessandro Piva

Tampering detection

- Generally, when an image is forged, no visual artifacts are introduced in the digital image and it is hard to disclose the manipulation at simple visual inspection.

- However, the underlying image statistics are heavily affected, thus allowing forgery to be treacable.

Alessandro Piva

Digital traces

- Which are those inherent traces – characteristic artifacts left behind in a digital media during the creation and any other process ?

- We need to look at the life cycle of a digital image ….

Alessandro Piva

Digital Image Life Cycle
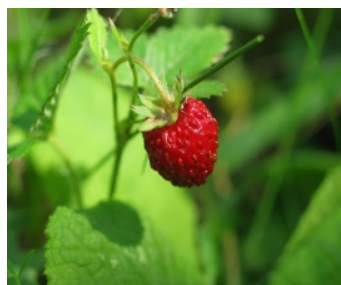
RAW digital image
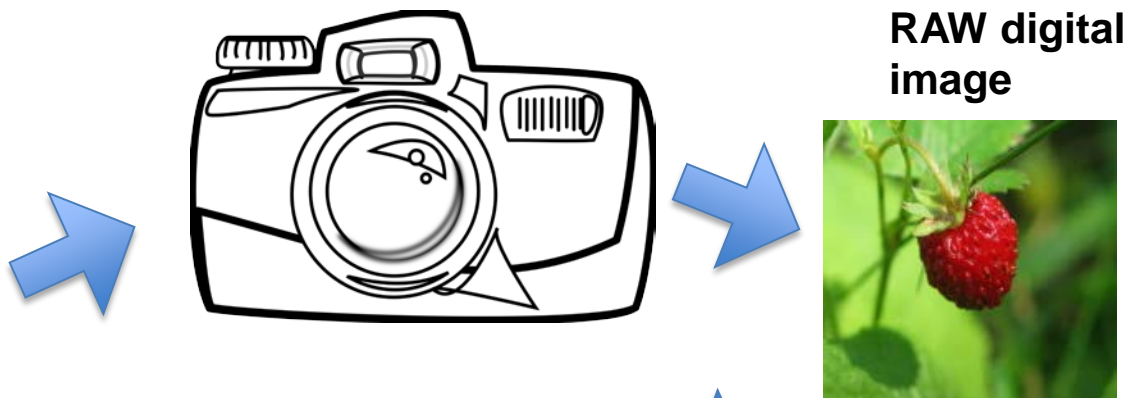
real scene
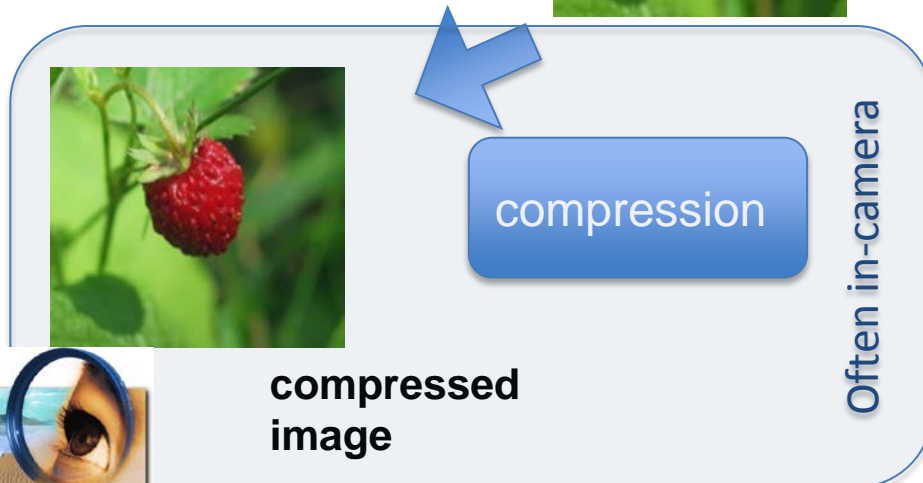
compression

Often in-camera

compressed image

final digital image

Adobe Photoshop 7.0

Alessandro Piva
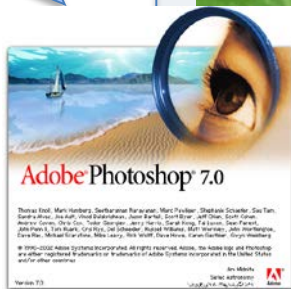
Acquisition through an imaging system

- The image acquisition pipeline is common for most of the commercially available devices; 3 steps:

- an *optical system* focusing energy reflected from an object,

- a *sensor* which measures the amount of energy,

- *in-camera processing* that converts it into a digital image.

Optical system

CCD or CMOS sensor

in-camera software processing

Alessandro Piva
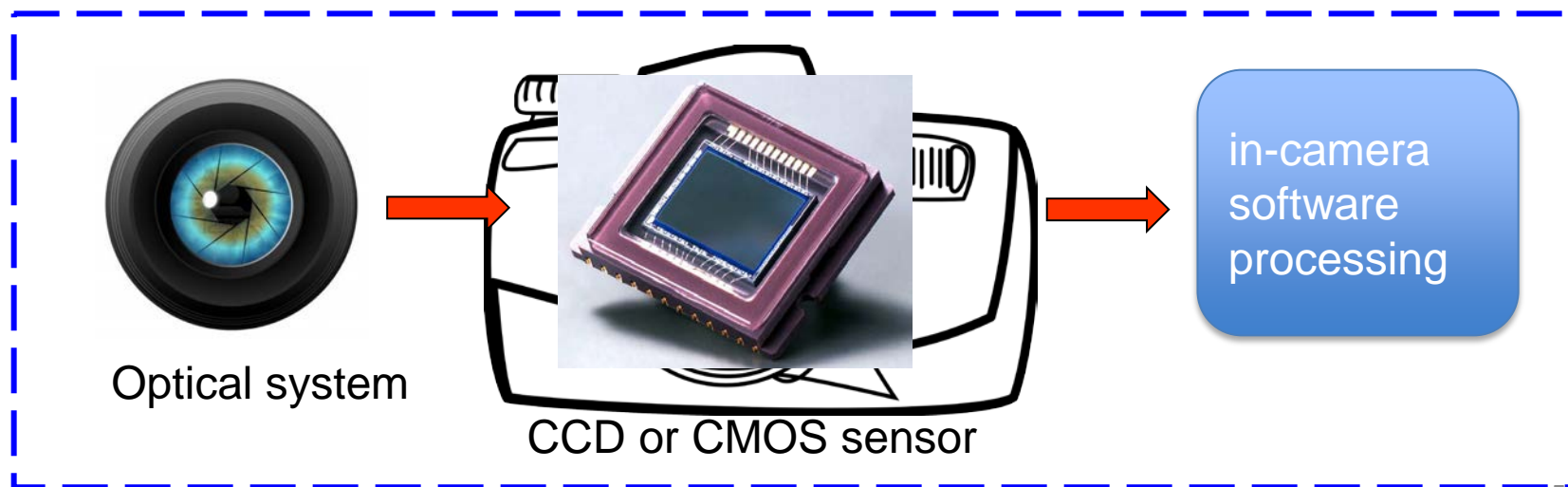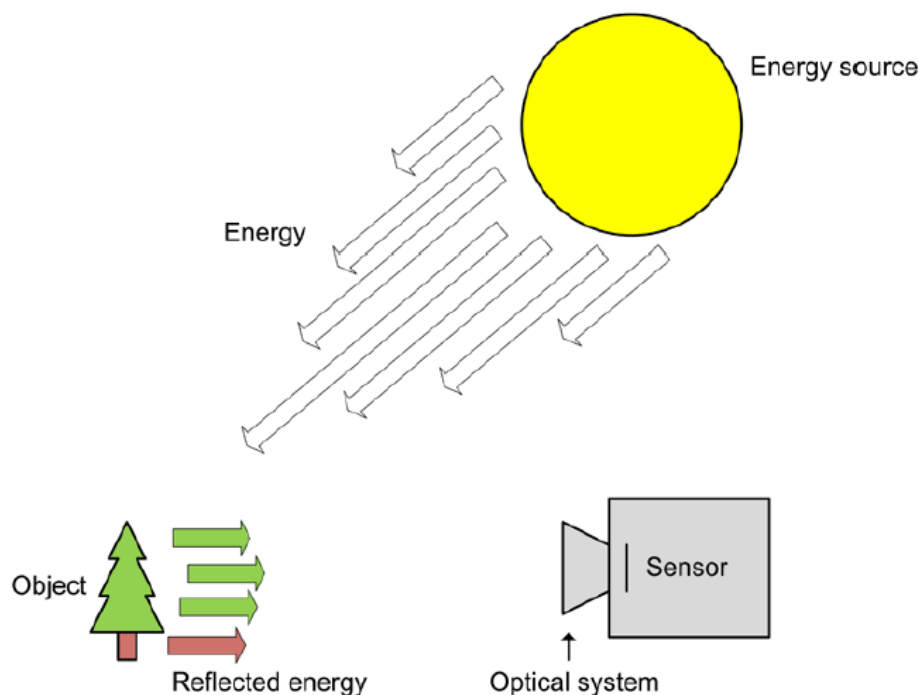
Energy source

- To capture an image we need some kind of energy source to illuminate the scene

  energy of interest is light or more generally *electromagnetic waves*.
  - An electromagnetic (EM) wave can be described as massless entity, a *photon*, whose electric and magnetic fields vary sinusoidally.

  The light reflected from the object now has to be captured by the camera.

Lens

- One of the main ingredients in the optical system is the lens, a piece of glass which focuses the incoming light onto the sensor.

In the figure, three light rays are illustrated for two different points. All three rays for a particular point intersect in a point to the right of the lens. Focusing such rays is exactly the purpose of the lens.

Alessandro Piva
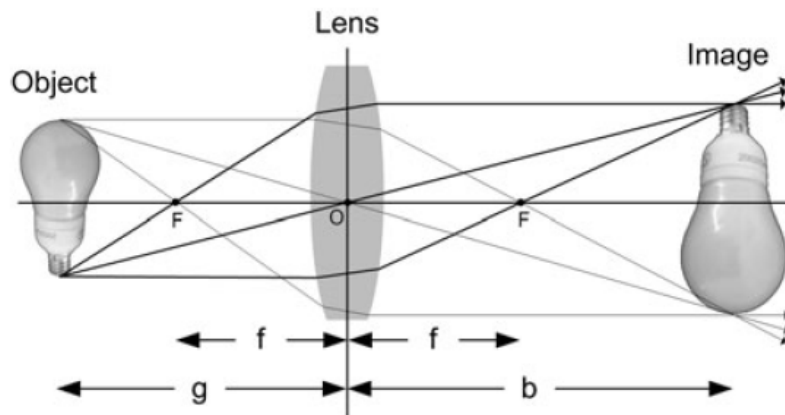
Optical aberration

- Optical systems, however, deviate from previous ideal models in that they fail to perfectly focus light.

- The resulting effect is known as optical aberration: it occurs when light from one point of an object does not converge into a single point after transmission through the system.

    - Monochromatic aberrations are caused by the geometry of the lens or mirror and occur both when light is reflected and when it is refracted. They appear even when using monochromatic light, hence the name.

    - Chromatic aberrations are caused by dispersion, the variation of a lens's refractive index with wavelength. They do not appear when monochromatic light is used.

Alessandro Piva

Chromatic aberration

- It manifests itself as "fringes" of color along boundaries that separate dark and bright parts of the image, because each color in the optical spectrum cannot be focused at a single common point.
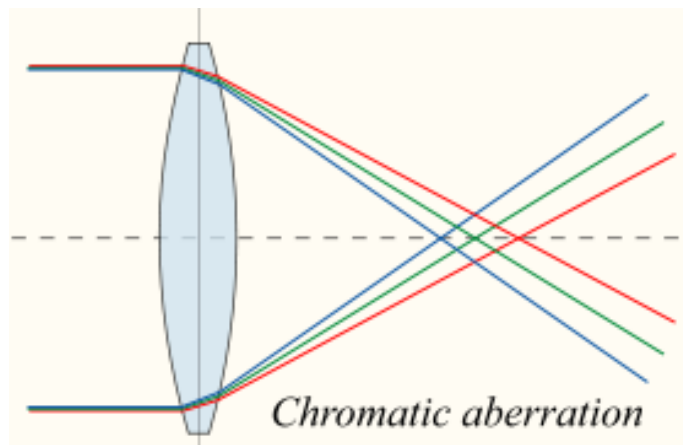
Severe purple fringing can be seen at the edges of the horse's forelock, mane, and ear.


Chromatic aberration

Chromatic aberration
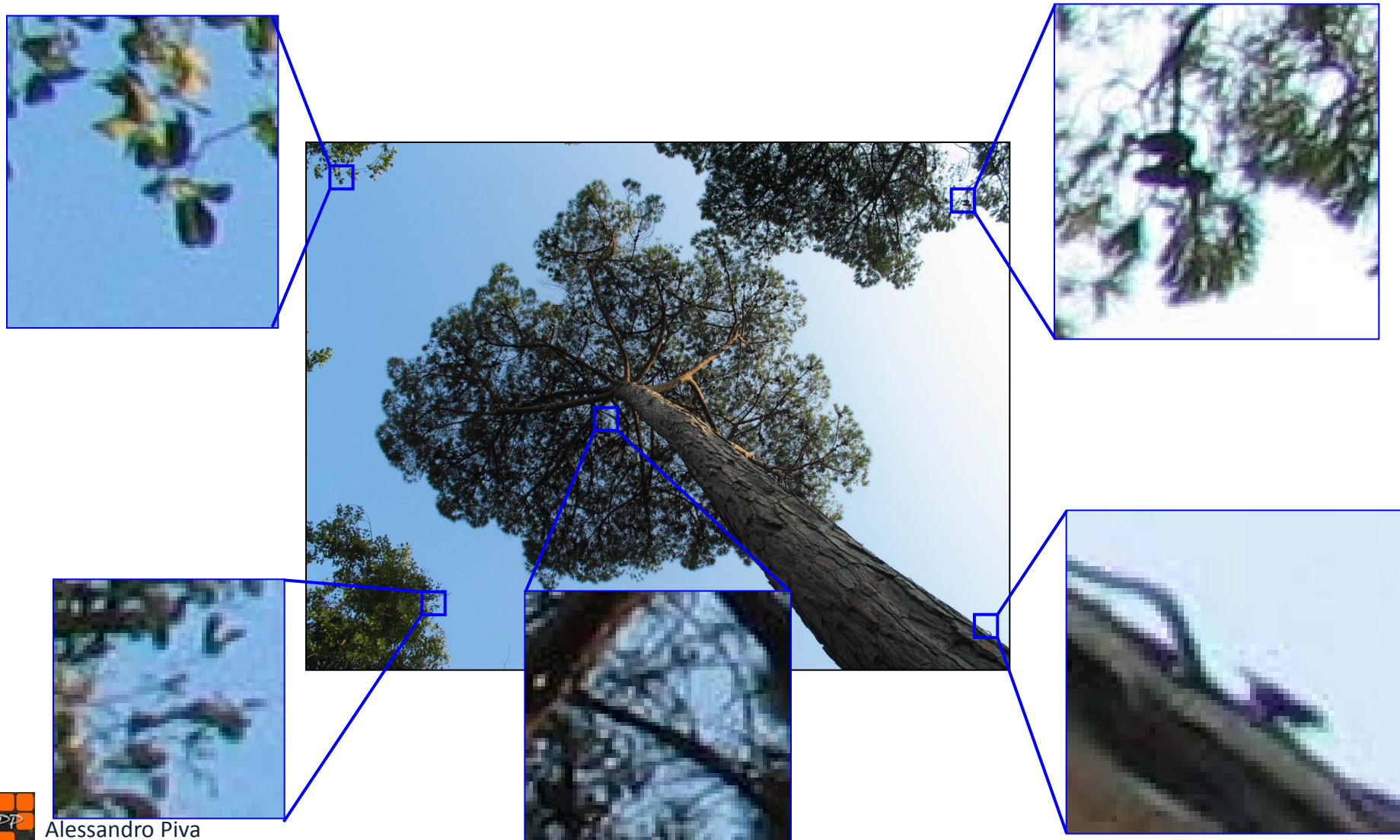
Sensor

An image sensor consists of a 2D array of cells, each capable of gathering incident light and converting that into a voltage, which in turn is converted into a digital number.
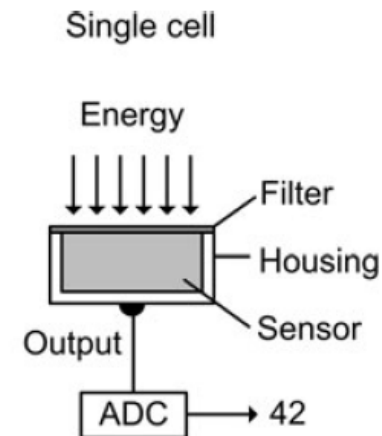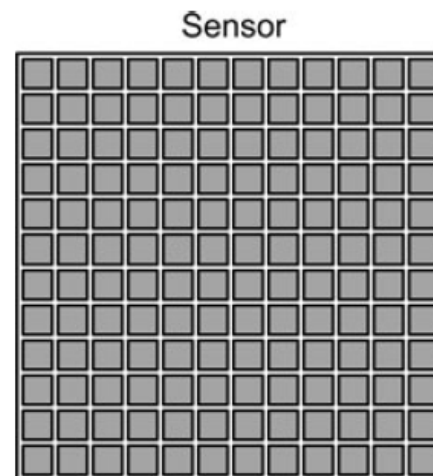
- The more incident light the higher the voltage and the higher the digital number.

- When the camera is to capture an image, light is allowed to enter and charges start accumulating in each cell. After a certain amount of time, known as the *exposure time*, and controlled by the *shutter*, the incident light is shut out again.

Alessandro Piva

Sensor Noise

- There exist two types of imaging sensors commonly found in digital cameras, camcorders, and scanners:
  - charge-coupled device (CCD)
  - metal-oxide semiconductor (CMOS).
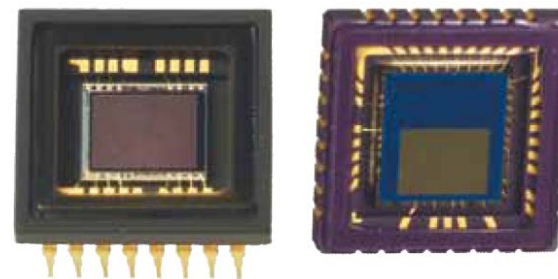
- Both consist of a large number of photo detectors, made of silicon, that capture light by converting photons into electrons.

- The accumulated charge is transferred out of the sensor, amplified, and then converted to a digital signal in an A/D converter.

- Imaging sensors have been shown to introduce various defects and to create noise in the pixel values.

  - Photo Response Non Uniformity (PRNU).

Alessandro Piva

Color Filter Array (CFA)
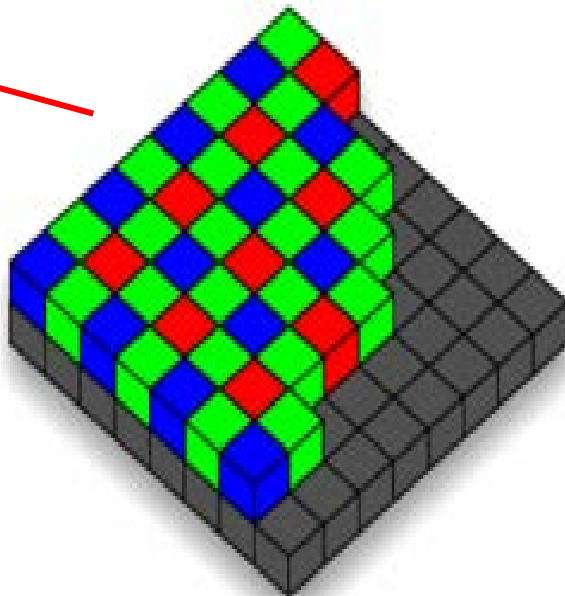
- A color image consists of 3 channels containing samples from different red, green, and blue.

- Most digital cameras are equipped with a single CCD or CMOS sensor and capture color images using a color filter array .

- At each pixel location only a single color sample is captured.

Alessandro Piva

Color Filter Array (CFA)

Resulting patterns

Color Filter Array

$$\tilde{R}(x,y) = \begin{cases} S(x,y) & \text{if } S(x,y) = r_{x,y} \\ 0 & \text{otherwise} \end{cases}$$

$$\tilde{G}(x,y) = \begin{cases} S(x,y) & \text{if } S(x,y) = g_{x,y} \\ 0 & \text{otherwise} \end{cases}$$

$$\tilde{B}(x,y) = \begin{cases} S(x,y) & \text{if } S(x,y) = b_{x,y} \\ 0 & \text{otherwise} \end{cases},$$

Let S(x,y) denote the acquired signal

- At each pixel location only a single color sample is captured.

Alessandro Piva
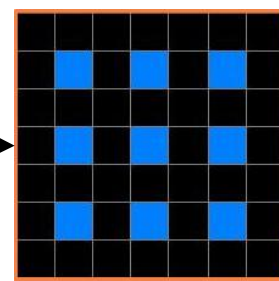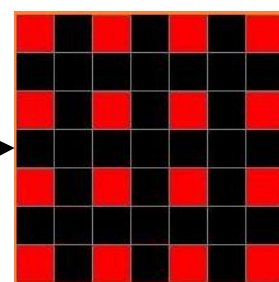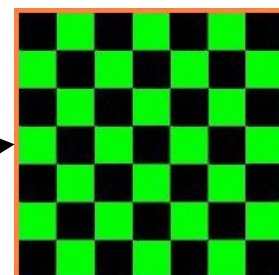
Color Filter Array (CFA)

- The <u>specific</u> mosaic of red, green and blue pixels depends on the <u>producer</u>, and several arranges are possible (previous slide refers to the Bayer array, the most frequently used one)

- Technique able to find the camera's color array pattern allow to determine the brand and model of the camera from which an image was captured.

Bayer

Diagonal Bayer

Diagonal

Striped

Pseudo-random Bayer

Alessandro Piva
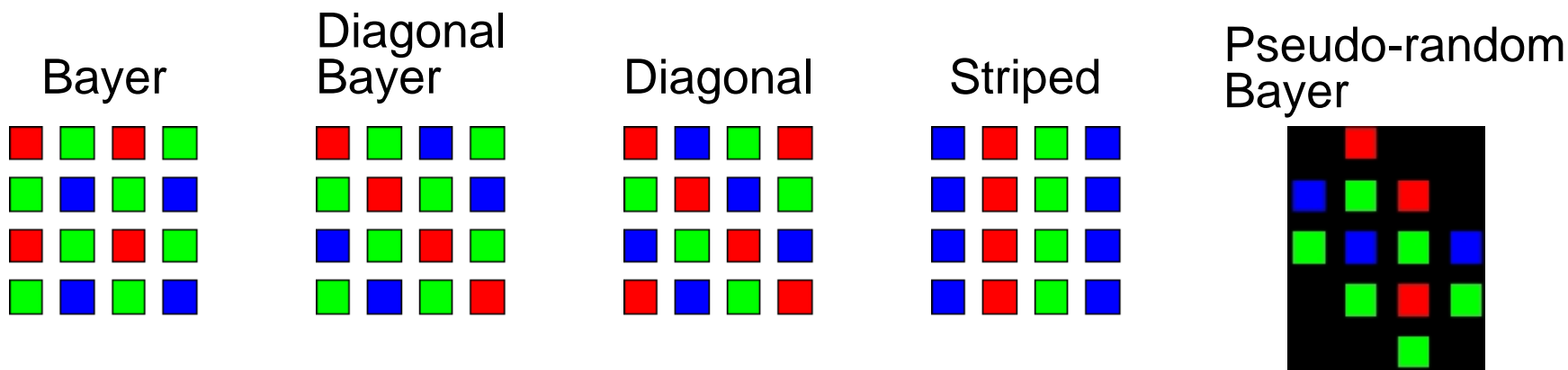
Color Filter Array (CFA)

- Since only a single color sample is recorded at each pixel location, the other two color samples must be estimated from the neighboring samples in order to obtain a three-channel color image.

- The estimation of the missing color samples is referred to as CFA interpolation or demosaicking.
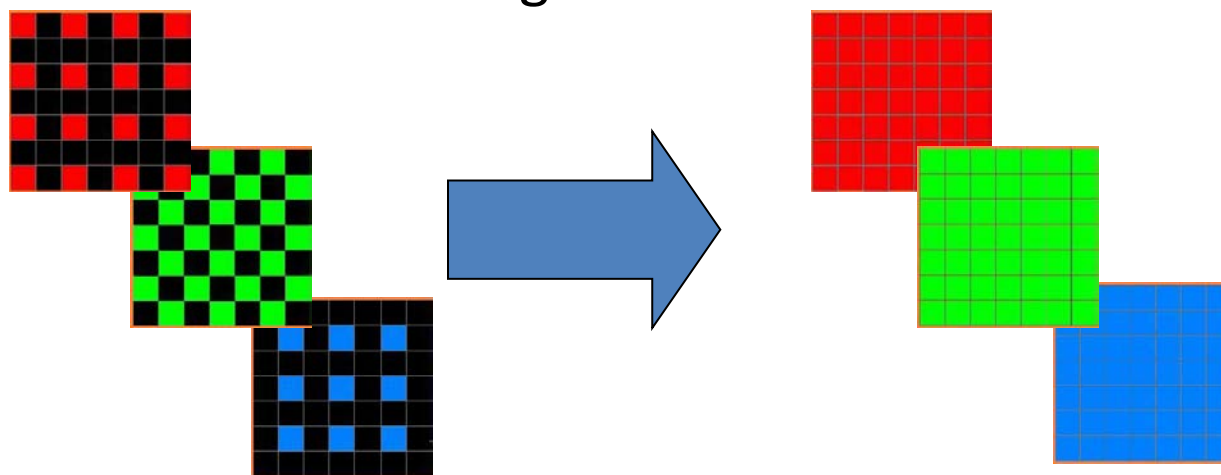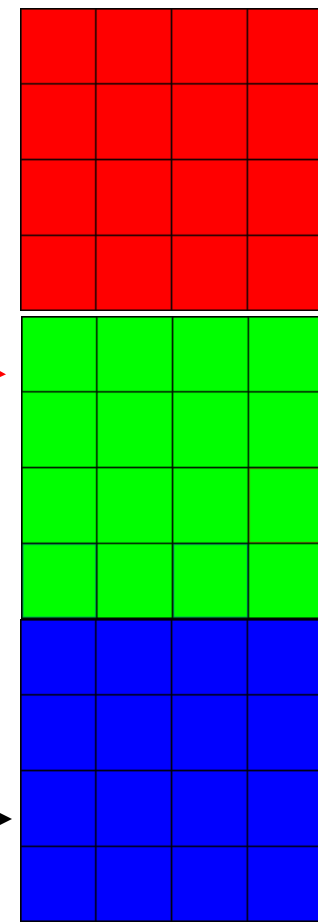
Alessandro Piva

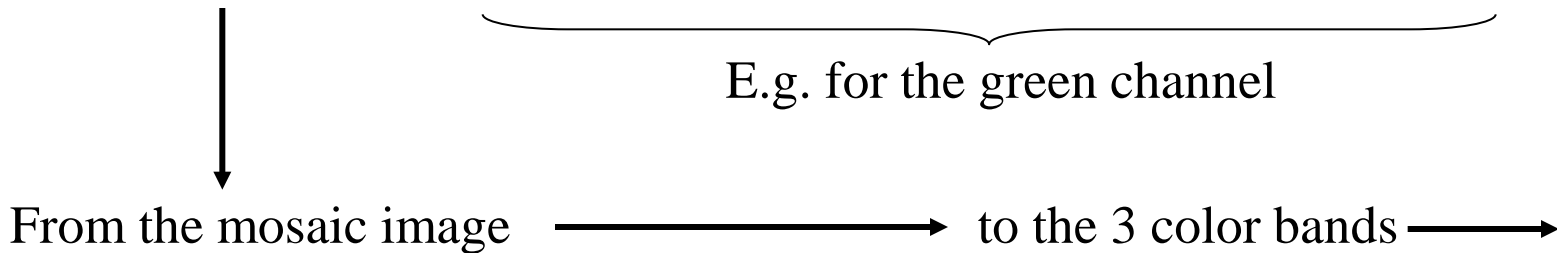# Color Filter Array (CFA)

E.g. for the green channel

From the mosaic image ⟶ to the 3 color bands ⟶

e.g. with linear interpolation …

Color Filter Array (CFA)

- CFA interpolation has been extensively studied and many methods have been proposed.

- The simplest methods for demosaicking are kernel-based interpolation methods that act on each channel independently.

- These methods can be efficiently implemented as linear filtering on each color channel.

  - That is, each interpolated pixel is correlated to a weighted sum of pixels in a small neighborhood centered about itself.

$$
\begin{aligned}
R(x,y) &= \sum_{u,v=-N}^{N} h_r(u,v)\tilde{R}(x-u,y-v) \\
G(x,y) &= \sum_{u,v=-N}^{N} h_g(u,v)\tilde{G}(x-u,y-v) \\
B(x,y) &= \sum_{u,v=-N}^{N} h_b(u,v)\tilde{B}(x-u,y-v),
\end{aligned}
$$

Alessandro Piva

Color Filter Array (CFA)

- Many other CFA interpolation algorithms:

  - smooth hue transition, median filter, gradient-based, adaptive color plane, and threshold-based variable number of gradients.

- Each CFA interpolation algorithm introduces specific statistical correlations between a subset of pixels in each color channel.

- Since the color filters in a CFA are typically arranged in a periodic pattern, these correlations are periodic.

Alessandro Piva

In-camera processing

This signal undergoes additional in-camera processing :

- the signal from each color channel is adjusted for gain (scaled by a factor g, different for each color band) to achieve proper white balance.

- the colors are further adjusted to display correctly on a computer monitor through gamma correction (an exponentiation by a factor γ)

in-camera software processing

Alessandro Piva

Acquisition footprints

- Each of the previous stages of the camera introduces imperfections or intrinsic patterns which leave tell-tale footprints in the data.

- Possible uses of acquisition fingerprints:
  - Camera brand / model identification
  - Individual device identification (*image ballistic*)
  - Tampering detection

Acquisition footprints for Camera brand / model identification

- Despite the similarity in their architectures, the processing details at all stages vary widely from one manufacturer to other, and even in different camera-models produced by the same manufactures.

- E.g., demosaicing algorithm and the CFA pattern remain proprietary to each digital camera-model, and the variations in the interpolated pixel values can be exploited to classify the images as originating from a certain class of digital cameras.

$$R(x,y) = \sum_{u,v=-N}^{N} h_r(u,v)\tilde{R}(x-u,y-v)$$

$$G(x,y) = \sum_{u,v=-N}^{N} h_g(u,v)\tilde{G}(x-u,y-v)$$

$$B(x,y) = \sum_{u,v=-N}^{N} h_b(u,v)\tilde{B}(x-u,y-v),$$

Assuming that each camera manufacturer uses different interpolation kernels and/or different weighting coefficients.

Alessandro Piva

Acquisition footprints for Camera brand / model identification

Fig. 5 – Sample set of pictures taken by five camera-models. (a) Canon Powershot A80 (b) Datron DC4300 (c) HP Photosmart 635 (d) Kodak Easyshare LS420 (e) Sony Cybershot DSC-P72.

Table 2 – Confusion table for five cameras

		Predicted				
		Canon	Datron	HP	Kodak	Sony
Actual	Canon	73	6	0	10	8
	Datron	4	88	0	3	1
	HP	0	0	96	4	1
	Kodak	16	4	2	78	5
	Sony	7	2	2	5	85

5 camera models: Canon Powershot A80, Datron DC4300, HP Photosmart 635, Kodak Easyshare LS420 and Sony DSC-P72. For each camera, we captured 200 images at default settings from the same scene. Detection accuracy is measured to be 84.8%; Kodak and Canon camera-models are likely to use similar interpolation algorithms as they are misclassified among each other.

Alessandro Piva

Acquisition footprints for Individual device identification (image ballistic)

- Like the grooves made in gun barrels - to impart a spin to the projectile for increased accuracy and range - introduce distinct markings to the bullet fired, and can therefore be used to link a bullet with a specific handgun, similarly, some traces can represent a signature of the individual device into the image.

- E.g. PRNU noise is distinctive of each single sensor unit;

- We can determine if an image under investigation was taken with a given camera (provided the camera is available), by generating the PRNU-based fingerprint and mathcing with the noise extracted from the camera.

Alessandro Piva

Acquisition footprints for Individual device identification (image ballistic)

Image under analysis

Camera Noise References
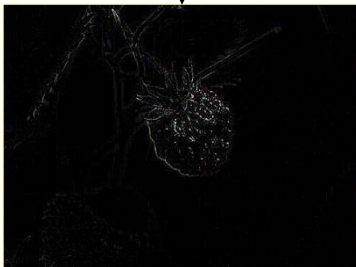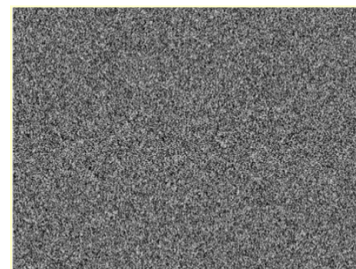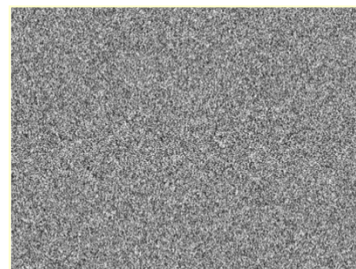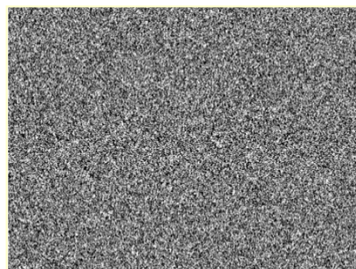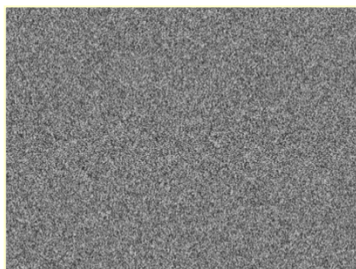
Extracted Noise

LOW correlation

HIGH correlation

LOW correlation

LOW correlation

Alessandro Piva

72
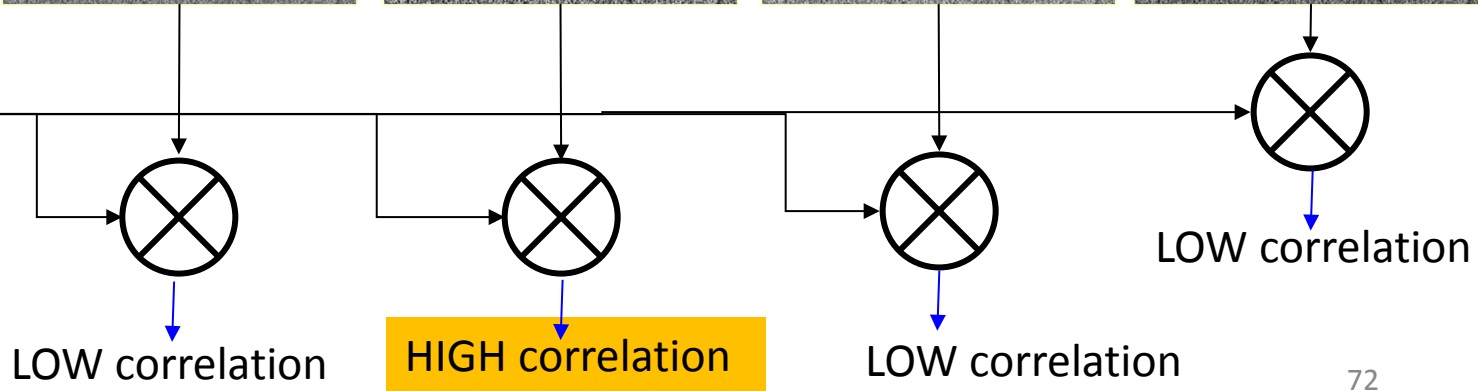
Acquisition footprints for tampering detection

- the presence of inconsistencies in these artifacts can be taken as evidence of tampering.

- E.g., manipulations of a part of an image will lead to inconsistencies in the chromatic aberration.

- For a 2-D lens and sensor, chromatic aberration is seen as fringes of colour around the image and have a typical spatial (radial) configuration.
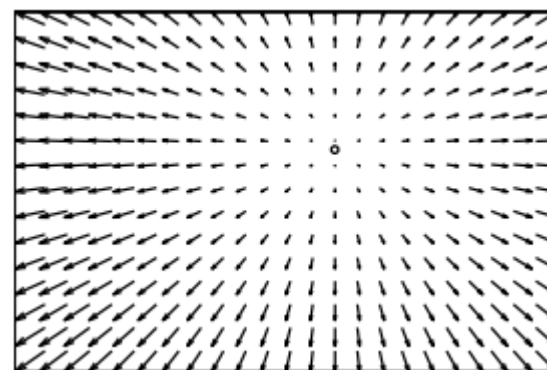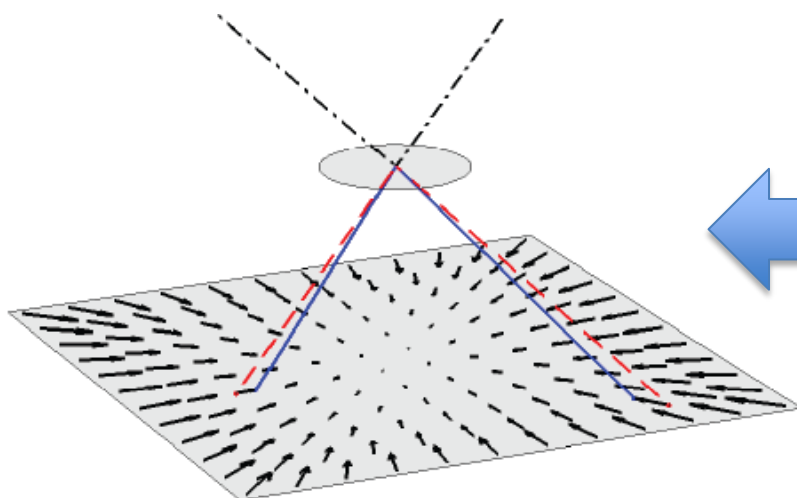
vector field showing deviation across the image between R and B.

Aless

Acquisition footprints for tampering detection

original image
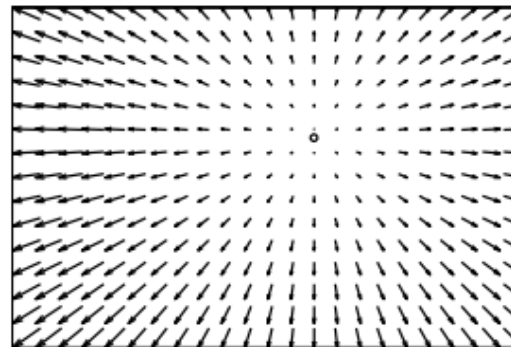
vector field estimated from original image
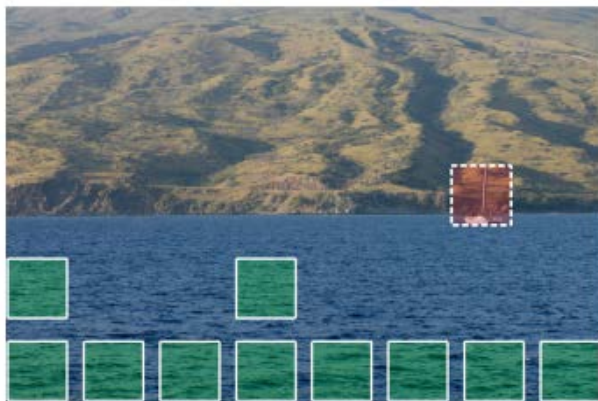
tampered image
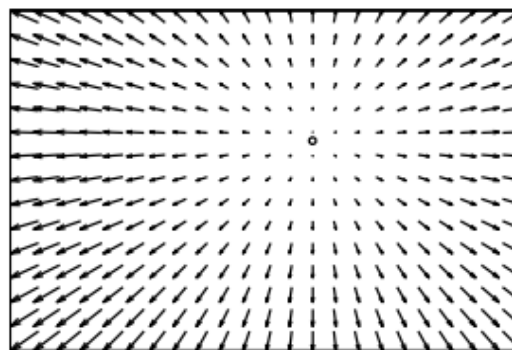
vector field estimated
from green blocks
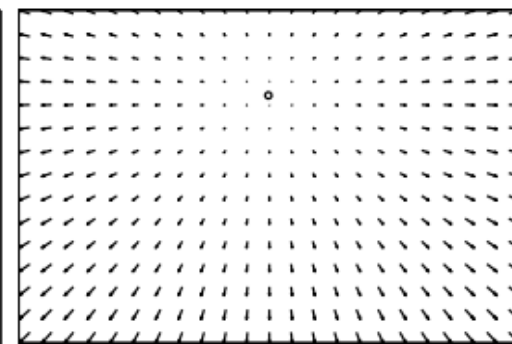
vector field estimated
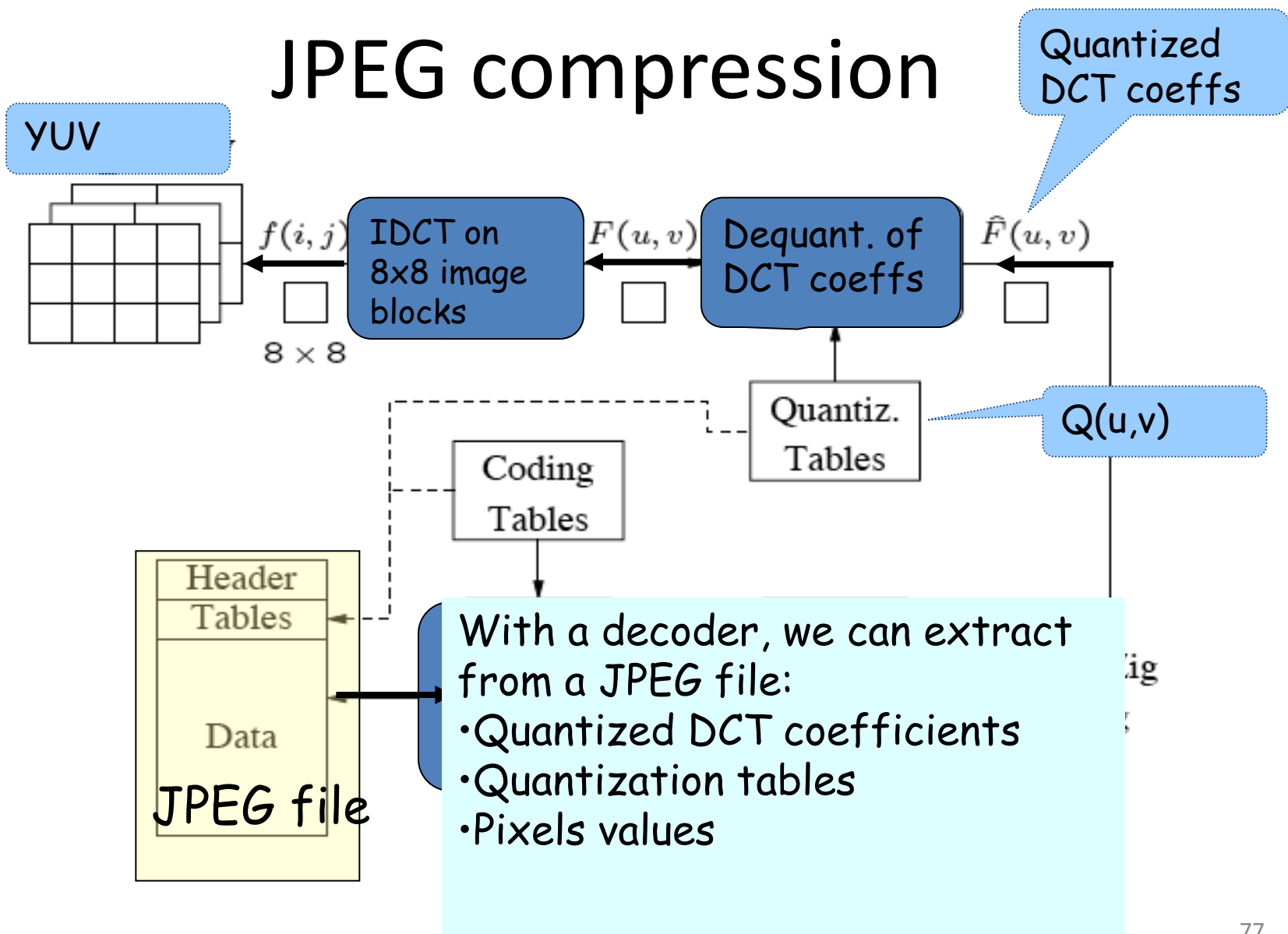from red block

Alessandro Piva

Compression

- Purpose is to represent images/videos with less data to save storage costs or transmission time, by removing redundant data, i.e. data not perceived by the human eye.

- Carried out directly in-camera, or by means of an image processing software.

- for commercial devices JPEG format is usually preferred.
  - It introduces a lossy compression

Alessandro Piva

JPEG compression

JPEG file

Alessandro Piva

JPEG compression

Quantized DCT coeffs

YUV

IDCT on 8x8 image blocks

$f(i,j)$ $F(u,v)$

Dequant. of DCT coeffs

$\hat{F}(u,v)$

8×8

Quantiz. Tables

Q(u,v)

Coding Tables

Header Tables

Data

JPEG file

With a decoder, we can extract from a JPEG file:
- Quantized DCT coefficients
- Quantization tables
- Pixels values

77

Alessandro Piva
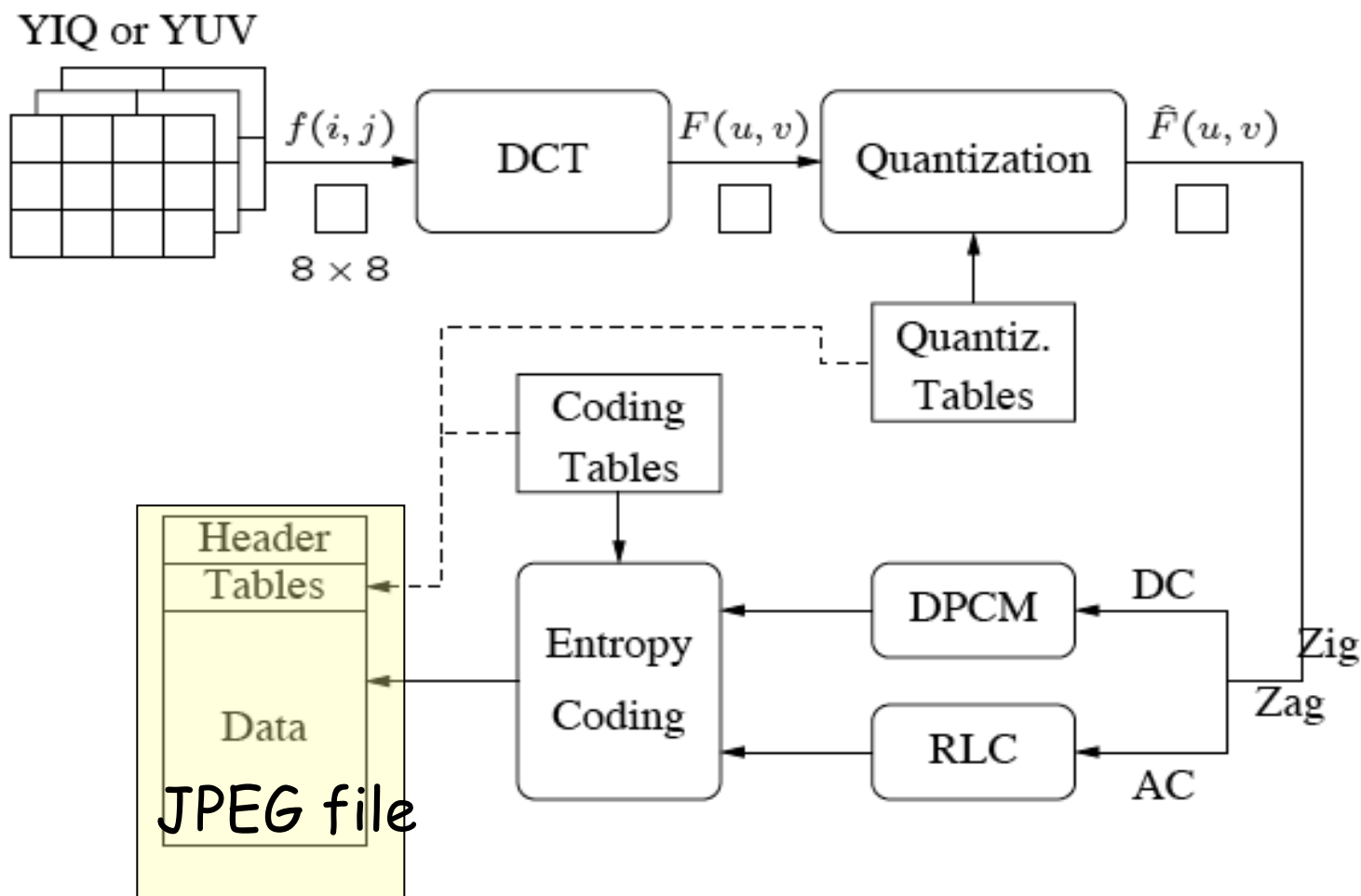
Compression footprints

- Lossy compression inevitably leaves characteristic footprints, related to the specific coding architecture.

- In particular, to understand if an image was JPEG compressed, it is possible to look for :

  - Compression artifacts left in spatial domain

  - Compression artifacts left in frequency domain

Alessandro Piva

Compression artifacts in spatial domain

- Baseline JPEG works with 8x8 image blocks, individually transformed and quantized;

- artifacts appear at the border of neighboring blocks in the form of horizontal and vertical edges.

- Even "light" compression may leave small but consistent discontinuities across block boundaries

Alessandro Piva

Compression artifacts in frequency domain

8x8 DCT $\xrightarrow{F(u,v)}$ Quantization $\xrightarrow{F_Q(u,v)}$

$$F_Q(u,v) = Round\left(\frac{F(u,v)}{Q(u,v)}\right)$$

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
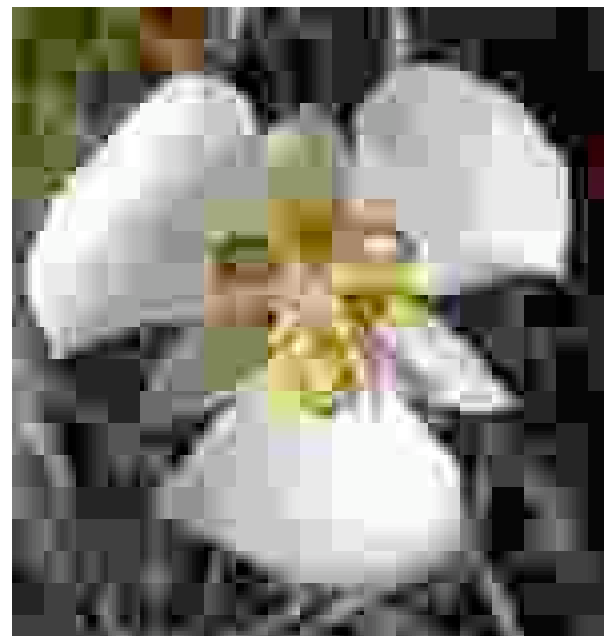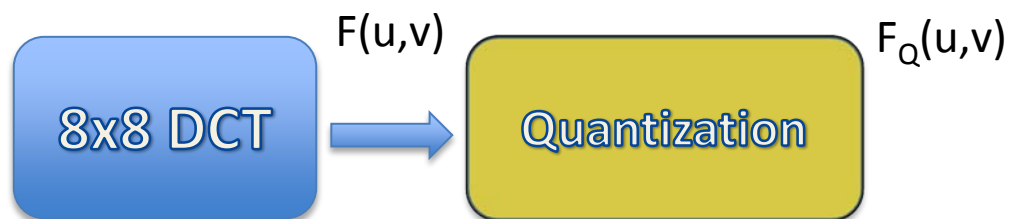
forces the value of each DCT coefficient to be an integer multiple of Q(u,v)

- Though the process of rounding and truncating the decompressed pixel values perturbs the DCT coefficients, their values typically remain clustered around integer multiples of Q(u,v).

Alessandro Piva

Compression artifacts in frequency domain

- It leaves traces we can find in the histogram computed by collecting from each 8x8 block the DCT coefficients having same frequency (u,v)
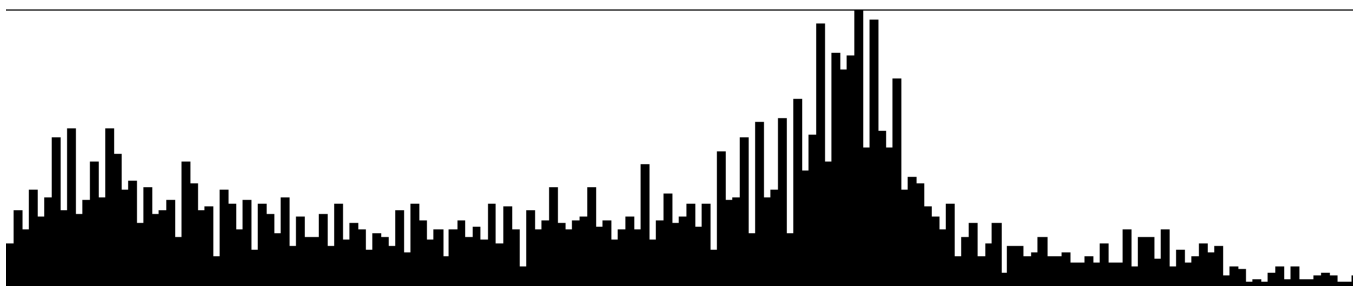
$$F_Q(2,1) = Round\left(\frac{F(2,1)}{12}\right)$$

Uncompressed

JPEG Compressed
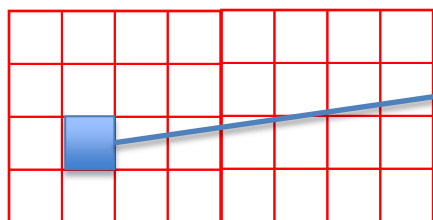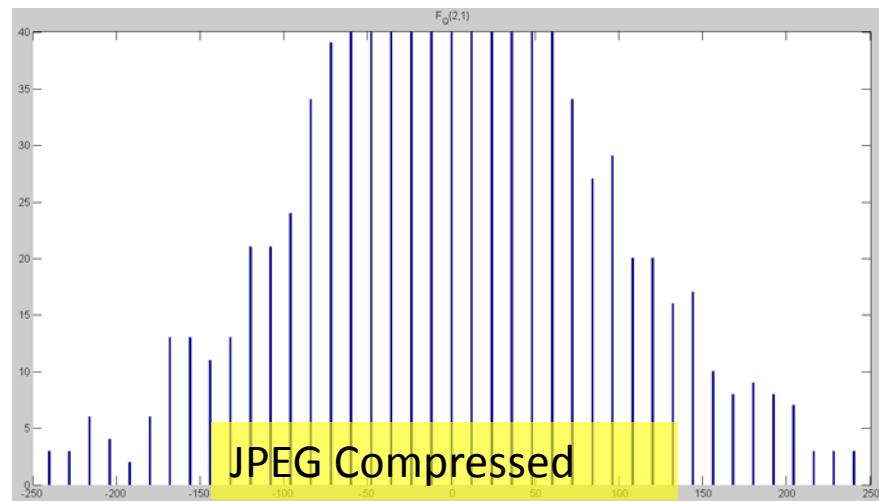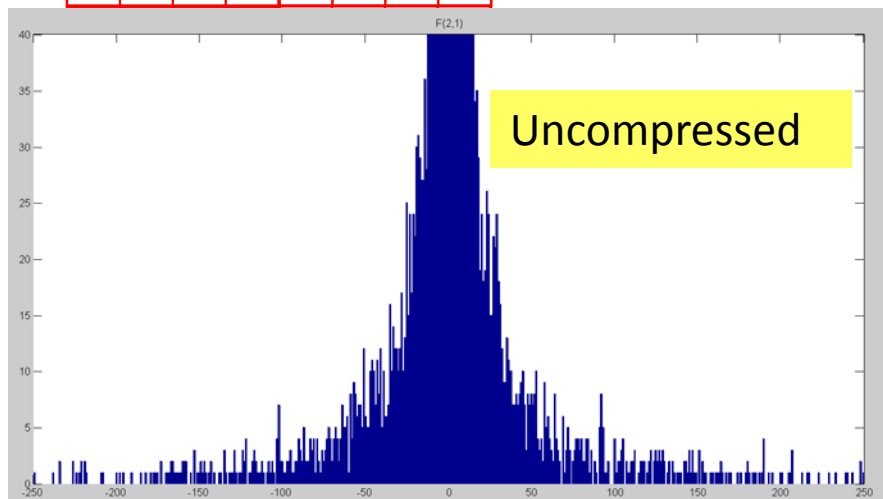
The distortion of such a behaviour can be used to detect the presence of tampering.

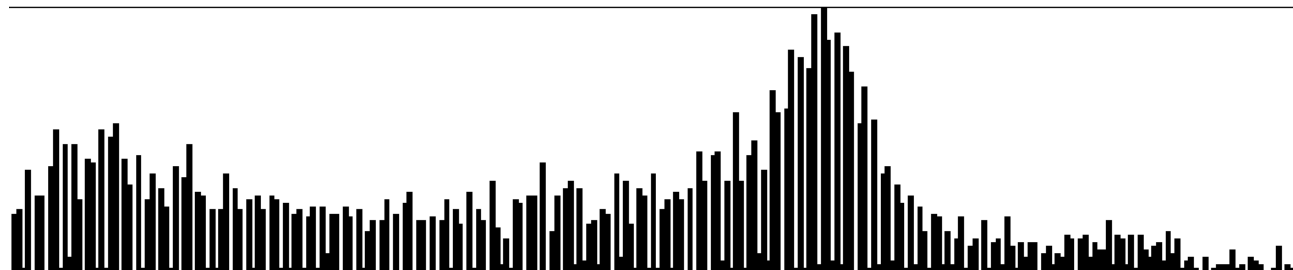Alessandro Piva

Compression artifacts in frequency domain

- Second compression leaves different new traces in the histogram of DCT coefficients having same frequency (u,v)
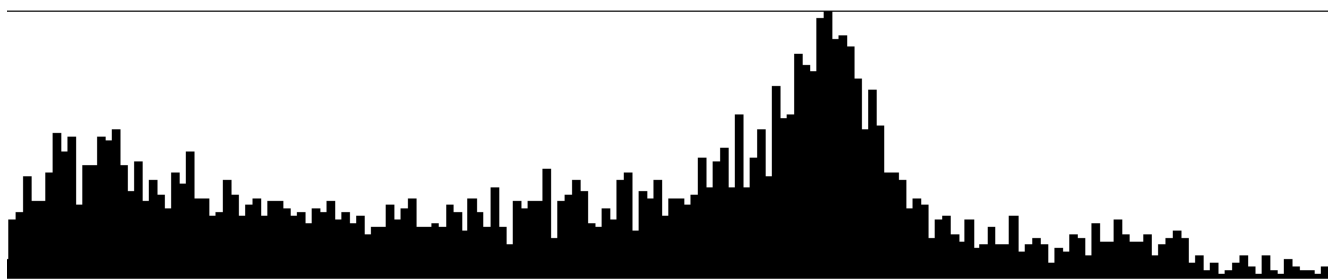
- image single JPEG with QF 75

- double JPEG with QF 85 followed by 75

- double JPEG with QF 75 followed by 85

82

Alessandro Piva

Compression footprints

- Possible uses of compression fingerprints:
  - Camera / Software identification
  - Image history reconstruction
  - Tampering detection

Alessandro Piva

Compression footprints for Camera / Software identification

- Each hw/sw implementation can have its own Q table
- Matching with Q in EXIF it is possible to find the camera / software that generated the JPEG image.

EXIF – quantization table

NIKON - COOLPIX P4 (FINE)

Photoshop - (Save As 10)

http://www.impulseadventure.com/photo/jpeg-quantization.html

Alessandro Piva

Compression footprints for image history reconstruction

- In the image under analysis is in an uncompressed format, we can state that it is native in this format if no compression artifacts are found.
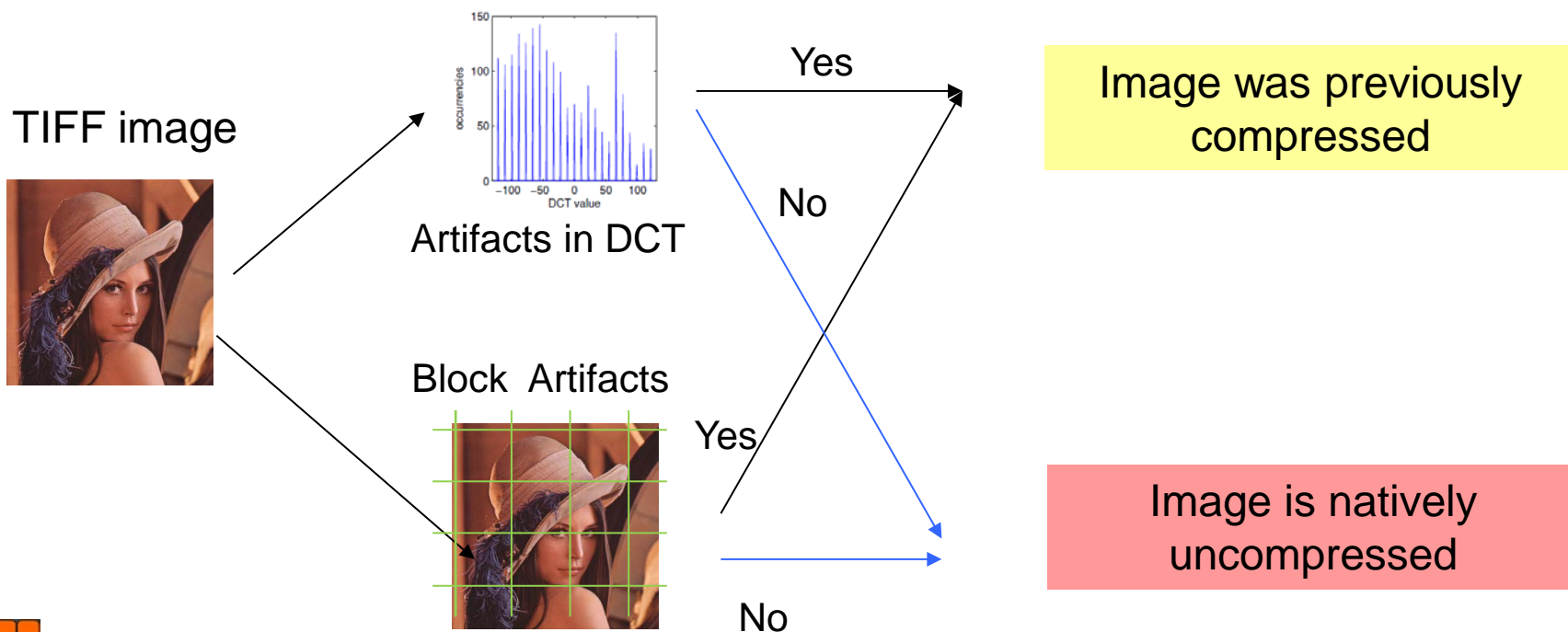
TIFF image

Artifacts in DCT

Block Artifacts

Yes

No

Yes

No

Image was previously compressed

Image is natively uncompressed

Alessandro Piva

Compression footprints for Tampering detection

- The presence of inconsistencies in the coding artifacts present into an image can be taken as evidence of local tampering.

- Any manipulation requires that an image be loaded into a photo-editing software program and resaved.
    - It is likely that both the original and manipulated images are stored in this format.
- In this scenario, the manipulated image is compressed twice, so these traces are indication that a possible tampering is present.

Alessandro Piva

Editing footprints

Stored image

- each processing applied to the digital image, even if not visually detectable, modifies specific statistics at a pixel level or at a semantic level, leaving peculiar traces accordingly to the processing itself.

Main classes of tampering :
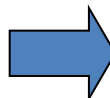
- Cloning (copy-move)
- Image splicing
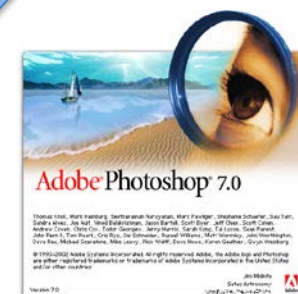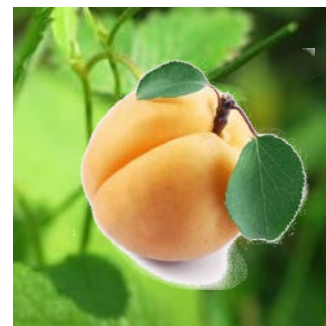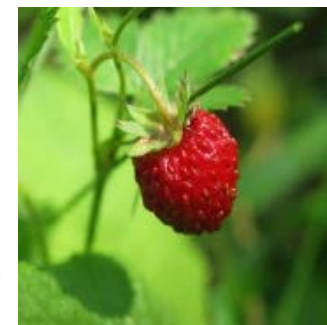
Final edited image

Cloning or copy-move forgery

- a part of the image is copied and pasted on another part of the same image, to duplicate an object, or to conceal a person or an object in the scene.

Original

Tampered

- tampered region exhibits same characteristics as the copied part: IDEA: look for **similar** features occurring more than once in the image

Alessandro Piva

Image splicing forgery

- To create a convincing forgery, it is necessary to geometrically correct, change colors/illumination of the subject to be spliced.

Image splicing forgery

- So methods to detect traces left by these operations have been studied.

- Two approaches:

  - Detection on the whole image: we assume the operation is applied to the whole image, so the trace is present in all the image

  - Localization on parts of the image: we assume the operation is applied to the pasted part only, so the trace is present only in a part of the image – usually unknown, then a localization is needed.

- Let's see a couple of examples

Alessandro Piva

Contrast enhancement detection

- histogram of natural images has a smooth envelope, without abrupt transitions to/from zero or peaks,

- histogram in contrast enhanced images is generally more spread and shows typical peaks-and-gaps artifacts
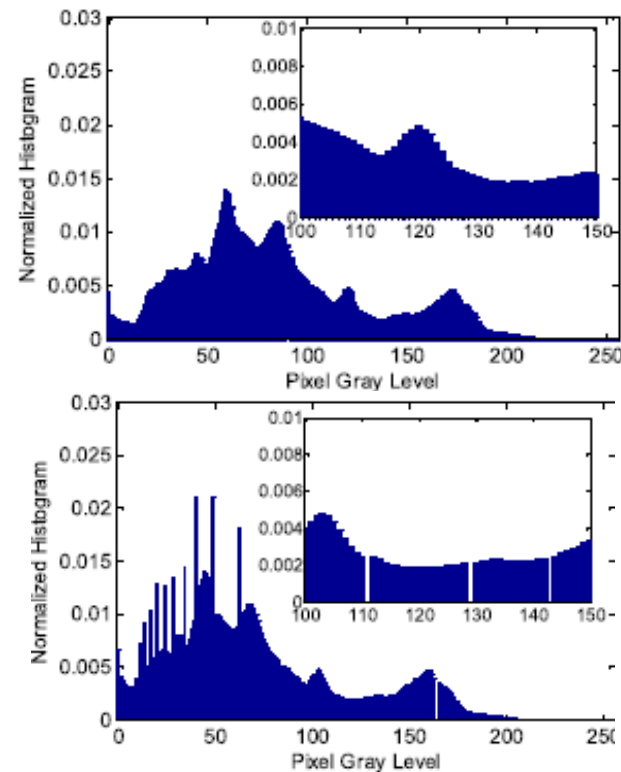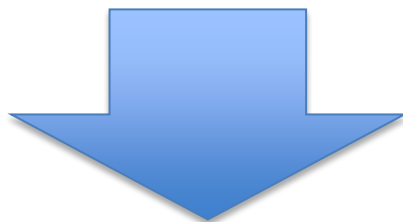
Traces left on first-order statistics, i.e. a statistical analysis of the image histogram can reveal it.

Alessandro Piva

Contrast enhancement localization
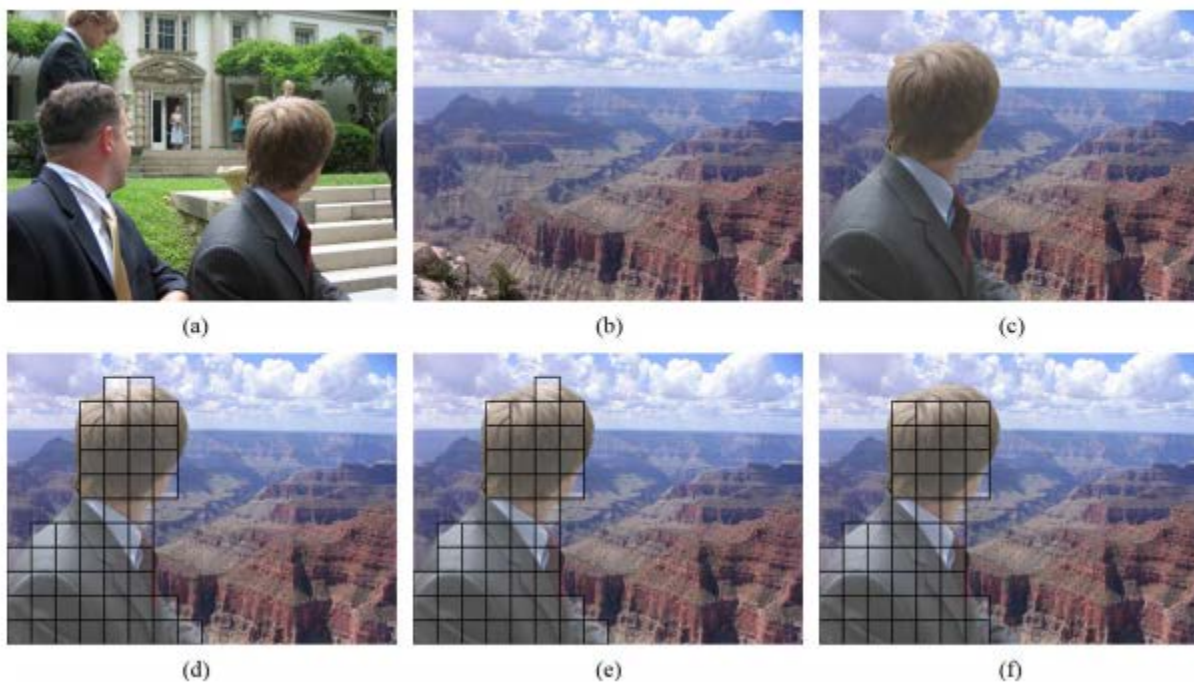
(a) unaltered image from which an object is cut, (b) unaltered image into which the cut object is pasted, (c) the composite image, (d) red layer blockwise detections, (e) green layer blockwise detections, and (f) blue layer blockwise detections. Blocks detected as contrast enhanced are highlighted and boxed

Alessandro Piva

Resampling detection

- Image interpolation tries to achieve a best approximation of a pixel's intensity based on the values at neighboring pixels .

- It creates periodic dependencies between groups of neighboring samples.

P-map : Pixel probability of being correlated to its neighbors
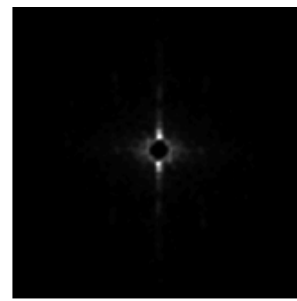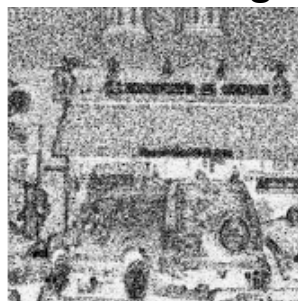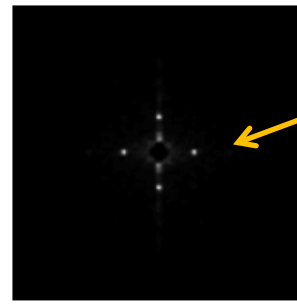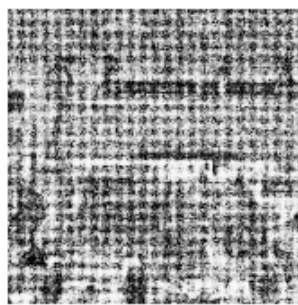
Fourier Transform of P-map

Original image

Image upsampled of 5%
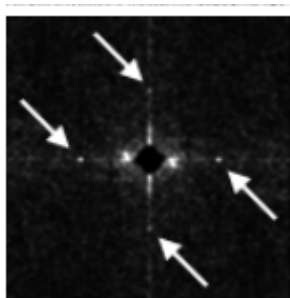
Peaks indicate presence of periodicity due to resampling

Alessandro Piva

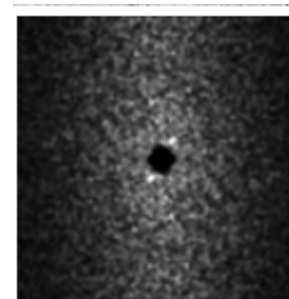# Resampling localization
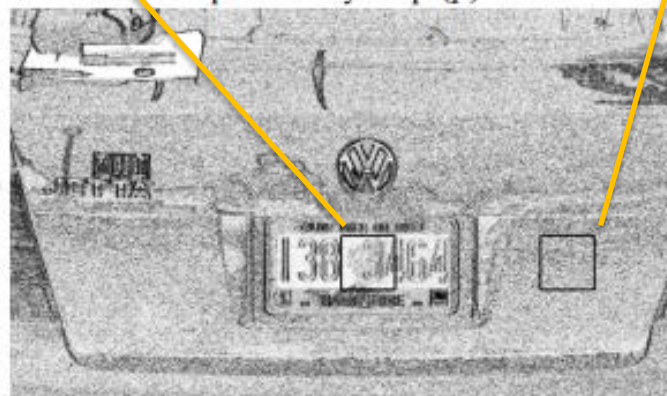
- splicing in a new license plate number:

original

forgery

Peaks indicate presence of periodicity due to resampling

probability map (p)

FFT of P-map of the 2 blocks

References

- A. Piva, "An Overview on Image Forensics" ISRN Signal Processing, vol. 2013, Article ID 496701, 2013.

- Signal Processing Magazine, 26 (2), March 2009, Special Section – Digital Forensics

Alessandro Piva