Security of Multimedia Information

by Xiangwei Kong, Yanqin Guo, Bo Wang

Chapter 6. Forensics of Digital Media

Lecturer: Jin HUANG

Digital Forensics

*Some content are from Research and slides of **Alessandro Piva** (Dept. of Information Engineering University of Florence (Italy)).*

People should be sensitive to the following problems:

- Is that true?
- Where does it come from?
- How much/Where it is modified/distorted?

Importance

- Personal: your money, your feeling.
- Society: united or divided, on the correct/wrong way.
  - Media is a kind a weapon!

Importance

- Personal: your money, your feeling.
- Society: united or divided, on the correct/wrong way.
    - Media is a kind a weapon!

Several Typical methods

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

Visual analysis of the image content

Does this image look strange?

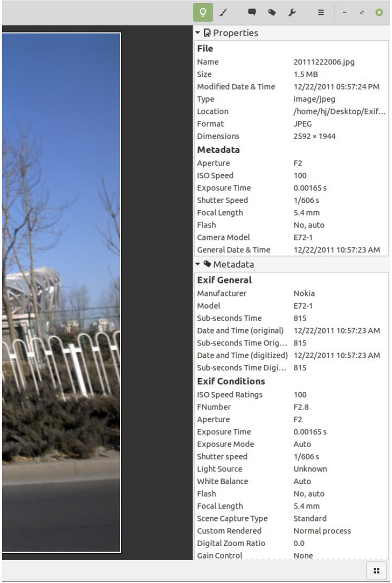
- Ripple, light direction etc.
- Sometimes, needs experts.

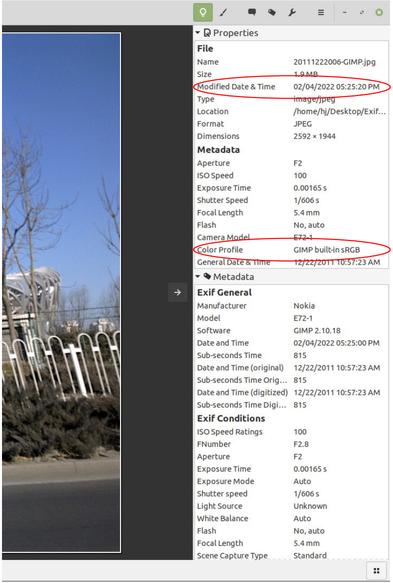
Analysis of the image file

Typically, check EXIF (EXchangeable Image File Format), a metadata.

- Camera brand and model
- Image Processing Software used
- Date/time of last modification
- ...

Example of image metadata





Can we trust Exif?

It can be

- easily removed and faked
- missing or incomplete

Authentication and integrity verification

- Active techniques: the acquisition device generates some information added to the digital image.
- Passive techniques: just analyze the digital image as it is, without any a prior information.

Active methods

- Cryptographic Digital Signature
  - source side: extract features then generating authentication signature.
  - receiver side: verify image integrity by signature.
- Fragile Digital Watermarking
  - source side: add a digital watermark.
  - receiver side: verify watermark integrity.

Passive or blind approaches

I.e. Multimedia forensics.

The key observation:

- Inherent traces – characteristic artifacts (i.e. 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.
  - In multimedia forensics, footprints are considered as an asset.

History of a digital content can be reconstructed by analyzing these traces

Typical tasks of multimedia forensics

- source identification
  - Find the origin.
  - Retrieve information on the source device at different levels.
- integrity verification / tampering detection
  - Has it suffered some processing?
  - Digital tracing.

Source identification

Different level of requirement

- Level 1: which kind of device?
  - scanner, digital camera, phone, webcam, ...
- Level 2: which model of such device?
  - Nikon, Cannon, ...
- Level 3: which one of this model?
  - SN10273847, SN122794846, , SN238792387, ...

Acquisition footprints

- Distortion of lens
- Color Filter Array
- Noise
- ....

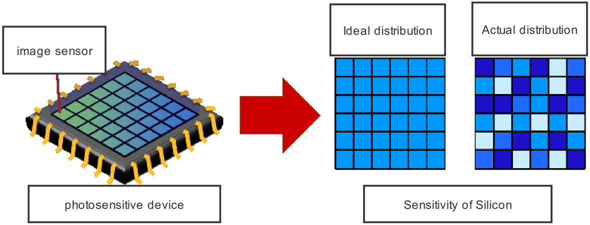
Acquisition footprints

- Distortion of lens
- Color Filter Array
- Noise
- ....

Noise based source identification

There are many imperfections in the process of acquiring images by a digital camera:

- Random noise.
- Pattern noise.
  - inconsistency of the homogeneity and uniformity of the silicon element of the sensor.



Pattern Noise

Characteristics of pattern noise:

- Not affected by environmental factors, such as temperature and humidity.
- It is a deterministic noise for each camera.

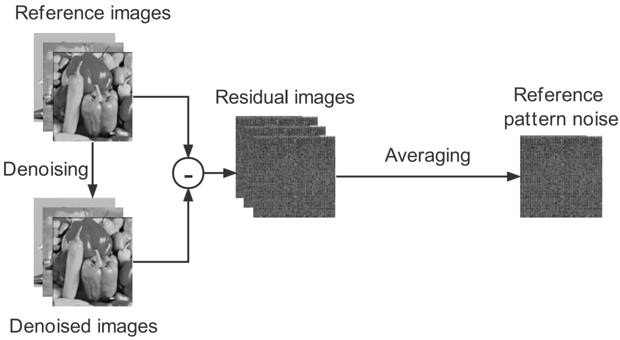
Pattern Noise

Characteristics of pattern noise:

- Not affected by environmental factors, such as temperature and humidity.
- It is a deterministic noise for each camera.

Use it for source identification!

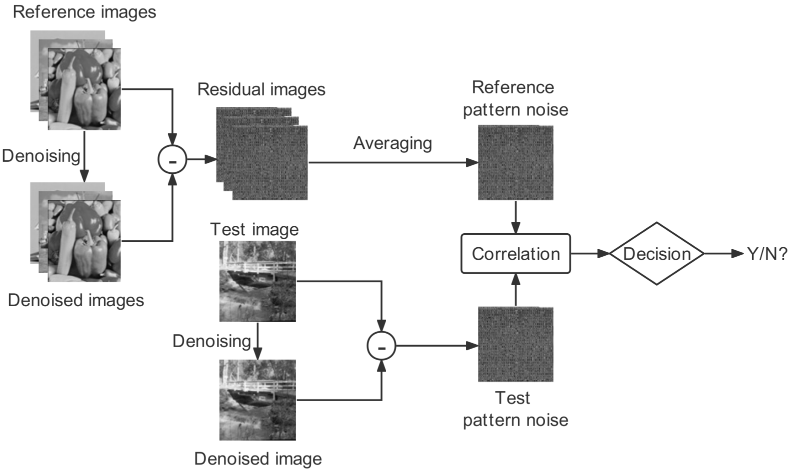
Generate Reference Pattern Noise



Extract reference pattern noise for camera $\mathcal{C}$:

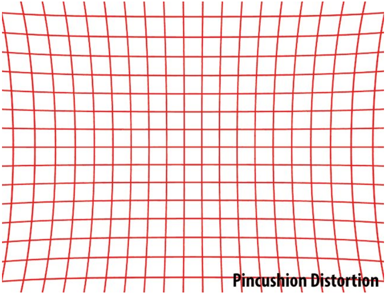
$$N_{ref}^{\mathcal{C}} = \frac{1}{M} \sum_{k=1}^{M} N_k^{\mathcal{C}}$$

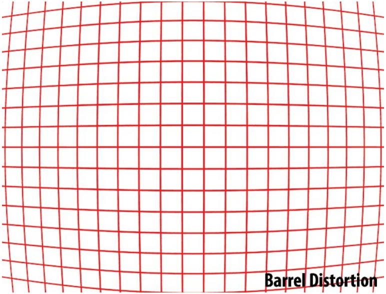
Pipeline

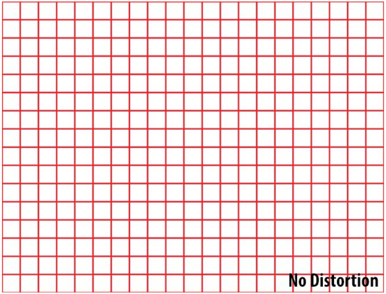


use $z_{cc}(N_{test}, N^{\mathcal{C}}_{ref})$ to compute their correlation.

Distortion of lens

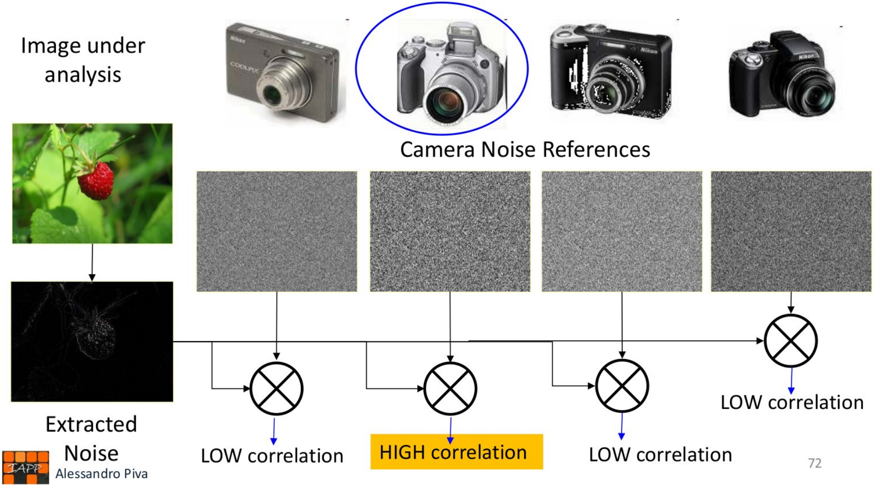






Noise based source identification

From Alessandro Piva's slides



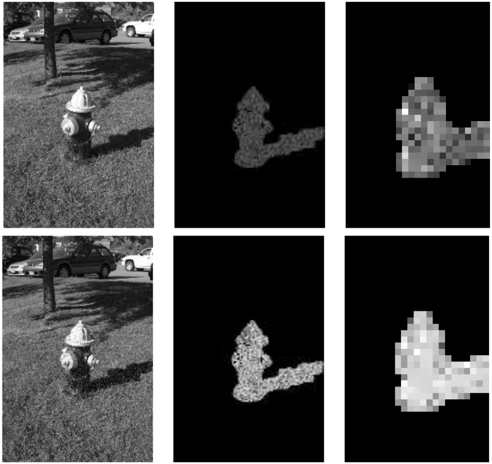
Detection of image splicing

"Statistical Tools for Digital Image Forensics", Popescu, 2005.

- copy-paste in a same image
  - by finding similar blocks
- copy-paste between images
  - by consistency of noise

Copy-paste between images

Idea: Noise is different at different regions
Statistical Tools for Digital Image Forensics, Popescu



Noise estimation

Under the additive noise model:

$$y[t] = x[t] + w[t],$$

where the signal x and noise w are independent and zero-mean, and their variances are S and N respectively, i.e.

$$E\{x^2[t]\} = S$$
$$E\{w^2[t]\} = N$$

The moments

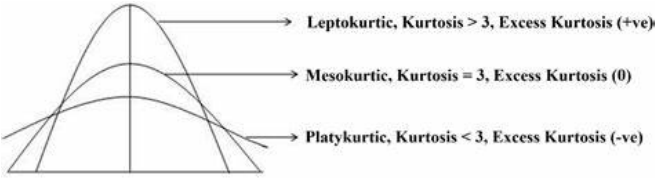
The the second and forth moments:

$$
\begin{aligned}
M_2 &= E\{y^2[t]\} = \frac{1}{N}\sum_{t=1}^{N} y^2[t], \\
&= E\{x^2[t]\} + 2E\{x[t]w[t]\} + E\{w^2[t]\} \\
&= S + N
\end{aligned}
$$

$$
\begin{aligned}
M_4 &= E\{y^4[t]\} = \frac{1}{N}\sum_{t=1}^{N} y^4[t], \\
&= E\{x^4[t]\} + 4E\{x^3[t]w[t]\} + 6E\{x^2[t]w^2[t]\} \\
&\quad + 4E\{x[t]w^3[t]\} + E\{w^4[t]\} \\
&= E\{x^4[t]\} + 6E\{x^2[t]\}E\{w^2[t]\} + E\{w^4[t]\} \\
&= \frac{E\{x^4[t]\}}{E\{x^2[t]\}^2}E\{x^2[t]\}^2 + 6E\{x^2[t]\}E\{w^2[t]\} + \frac{E\{w^4[t]\}}{E\{w^2[t]\}^2}E\{w^2[t]\}^2 \\
&= k_x S^2 + 6SN + k_w N^2
\end{aligned}
$$

Kurtosis (peakedness)

$$k_x = \frac{E\{x^4[t]\}}{E\{x^2[t]\}^2}, \quad k_w = \frac{E\{w^4[t]\}}{E\{w^2[t]\}^2}$$



- If x is not Gaussian, i.e. $k_x \neq 3$,
- and $0 \leq (k_y - 3)/(k_x - 3) \leq 1$,

$$\hat{S} = M_2 \sqrt{(k_y - 3)/(k_x - 3)}$$

$$\hat{N} = M_2 \left(1 - \sqrt{(k_y - 3)/(k_x - 3)}\right)$$

Results

From left to right: image, absolute differences (added noise), estimated local noise variance