CYBER-CRIME AND COMPUTER FORENSICS
Digital Image Forensics [F4]

REPORT

Anh Duy TRAN
(tranad@eurecom.fr)

1. Objective

In this project, I explored what is Digital Image Forensics (DIF), what are the type of those techniques. Then, I explored some techniques in the publications and write a small tool based on those techniques for DIF.

2. Digital Image Forensics:

Multimedia forensic aim at restoring some of the lost trustworthiness of digital media by developing tools to unveil conspicuous traces of previous manipulations, or to infer knowledge about the source device [1]. Digital image forensics – a kind of multimedia forensics – is a brand-new research field which aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. [2]

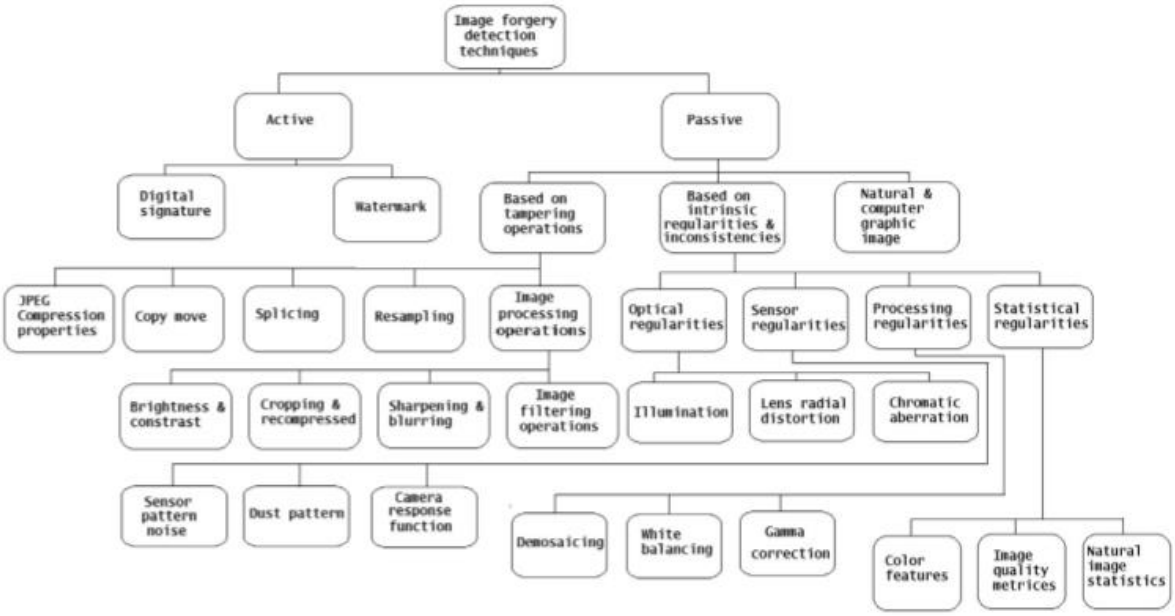
Digital Image Forensics is that branch of multimedia security that, together with Digital Watermarking, aims at contrasting and exposing malicious image manipulation.

DIF aims at providing tools to support blind investigation. This brand-new discipline stems from existing multimedia security-related research domains (e.g. Watermarking and Steganography) and exploits image processing and analysis tools to recover information about the history of an image. Two principal research paths evolve under the name of Digital Image Forensics. The first one includes methods that attempt at answering question a), by performing some kind of ballistic analysis to identify the device that captured the image, or at least to determine which devices did not capture it. These methods will be collected in the following under the common name of image source device identification techniques. The second group of methods aims instead at exposing traces of semantic manipulation (i.e. forgeries) by studying inconsistencies in natural image statistics. We will refer to these methods as tampering detection techniques. [2]

3. Digital Image Forensics:

Image forgery detection aims to verify the authenticity of a digital image. Image authentication solution is classified into two types. (1) Active and (2) Blind or passive. An active forgery detection techniques, such as digital watermarking or digital signatures uses a known authentication code embedded into the image content before the images are sent through an unreliable public channel. By verifying the presence of such authentication code authentication may be proved by comparing with the original inserted code. However, this method requires special hardware or software to insert the authentication code inside the image before the image is being distributed. [3]

Passive or blind forgery detection technique uses the received image only for assessing its authenticity or integrity, without any signature or watermark of the original image from the sender. It is based on the assumption that although digital forgeries may leave no visual clues of having been tampered with, they may highly likely disturb the underlying statistics property or image consistency of a natural scene image which introduces new artifacts resulting in various forms of inconsistencies. These inconsistencies can be used to detect the forgery. This technique is popular as it does not need any prior information about the image. Existing techniques identify various traces of tampering and detect them separately with localization of tampered region. [3]



4. Digital Image Forensics is not Computer Forensics:

Multimedia Forensics in general and Digital Image Forensics in particular is not Computer Forensics. Even though both computer forensics and multimedia forensics explore digital evidence, we believe that they form two distinct sub-categories of digital forensics. This may seem counter-intuitive at first sight, since in any case, the domain of evidence is limited to the set of discrete symbols found on a particular device. In multimedia forensics, however, it is assumed that these discrete symbols were captured with some type of a sensor and therefore the symbols are a digital representation of an incognizable reality. The existence of a sensor that transforms natural phenomena to discrete projections, which are then subject to investigation, implies that multimedia forensics has to be seen as empirical science. This resembles the epistemological argument brought forward in the context of steganography in digitized covers. Literally, a forensic investigator can never gain ultimate knowledge about whether a piece of digital media reflects reality or not. Neither can a sophisticated perpetrator be sure whether his manipulation really has not left any detectable traces. Unlike computer forensics, digital evidence in multimedia forensics is linked to the outside world and cannot be reproduced with machines. Thus, while the principle of transfer does not necessarily apply to computer forensics, it does have a place in multimedia forensics. [1]

5. Small tool for Digital Image Forensics:

I gathered some techniques in some paper and composed the small tools that implement those methods in DIF. The tool does not tell exactly this image is forged/photoshoped/tampered or not (even if some tool can tell exactly forged or not, you can go directly to the top of the world). This tools just give some warning, some weird "information" of the image, visual some strange region of the image to the users. Then, based on that information the users can make the decisions.

Nowadays, the tampered image is more difficult to detect. Many techniques that counter the detection. My tool implements some techniques are a little bit old, but still useful in some image. Some tampered images are easy to detect by these methods but hard to detect by the others. Therefore, we need to combine many techniques to analyze one images.

a. Exposing digital forgeries by EXIF metadata

Every image has the header (EXIF) which contains many information about the image are source device identification, date-time, thumbnail, etc. Analyzing that information and checking the consistency is the one of the methods to check the image is modified or not. That technique is simple and look like 'stupid' but this is the strongest method. We know that, the image with the right header can tell that the image is *right* or *wrong*. But, the image with the wrong header, we can absolutely be sure that image is *wrong*.

In my tool, I extracted the EXIF information and then compare it:

- If the modified date is not the same with the original date: the image has been modified.
- The header contains the tag of some software edited image like Adobe Photoshop, etc.: the image has been modified by those software.
- The image's header is stripped => that's weird.
- The thumbnail and the image are not the same.
- The image has a strange resolution (this does not match with any camera resolution) => the image can be resized or crop.
- Etc.

Gathers that information, the tool gives the WARNING for the users.

b. Exposing digital forgeries from JPEG Ghost [4]

When creating a digital forgery, it is often necessary to combine several images, for example, when compositing one person's head onto another person's body. If these images were originally of different JPEG compression quality, then the digital composite may contain a trace of the original compression qualities.

Based on this idea, we need to compute the different map between 2 different quality images.

The difference image is first averaged across a bxb pixel region:

$$\delta(x, y, q) = \frac{1}{3}\sum_{i=1}^{3}\frac{1}{b^2}\sum_{b_x=0}^{b-1}\sum_{b_y=0}^{b-1}[f(x+b_x, y+b_y, i) - f_q(x+b_x, y+b_y, i)]^2$$

and then normalized so that the averaged difference at each location (x,y) is scaled into the range [0,1]

$$d(x, y, q) = \delta(x, y, q) - \frac{\min_q[\delta(x, y, q)]}{\max_q[\delta(x, y, q)] - \min_q[\delta(x, y, q)]}.$$

This is a simple and yet potentially powerful technique for detecting tampering in low-quality JPEG images. This approach explicitly detects whether part of an image was compressed at a lower quality than the saved JPEG quality of the entire image. Such a region is detected by simply resaving the image at a multitude of JPEG qualities and detecting spatially localized local minima in the difference between the image and its JPEG-compressed counterpart. Under many situations, these minima, called JPEG ghosts, are highly salient and easily detected.

For more detail of this method check it in the publication: Exposing digital forgeries from JPEG ghosts [4]

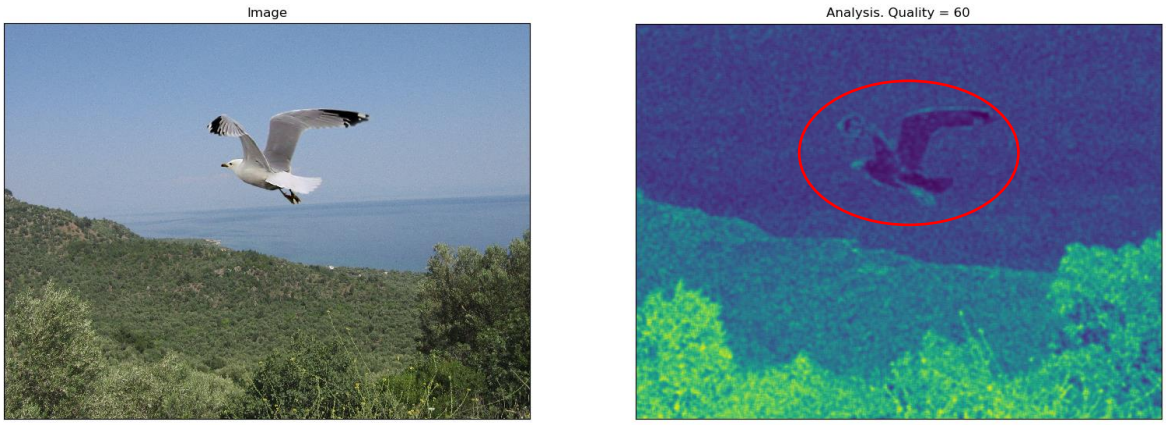
Here is my actual result testing the implementation of this method on my image:

Original Image for all demo:

Original

Tampered

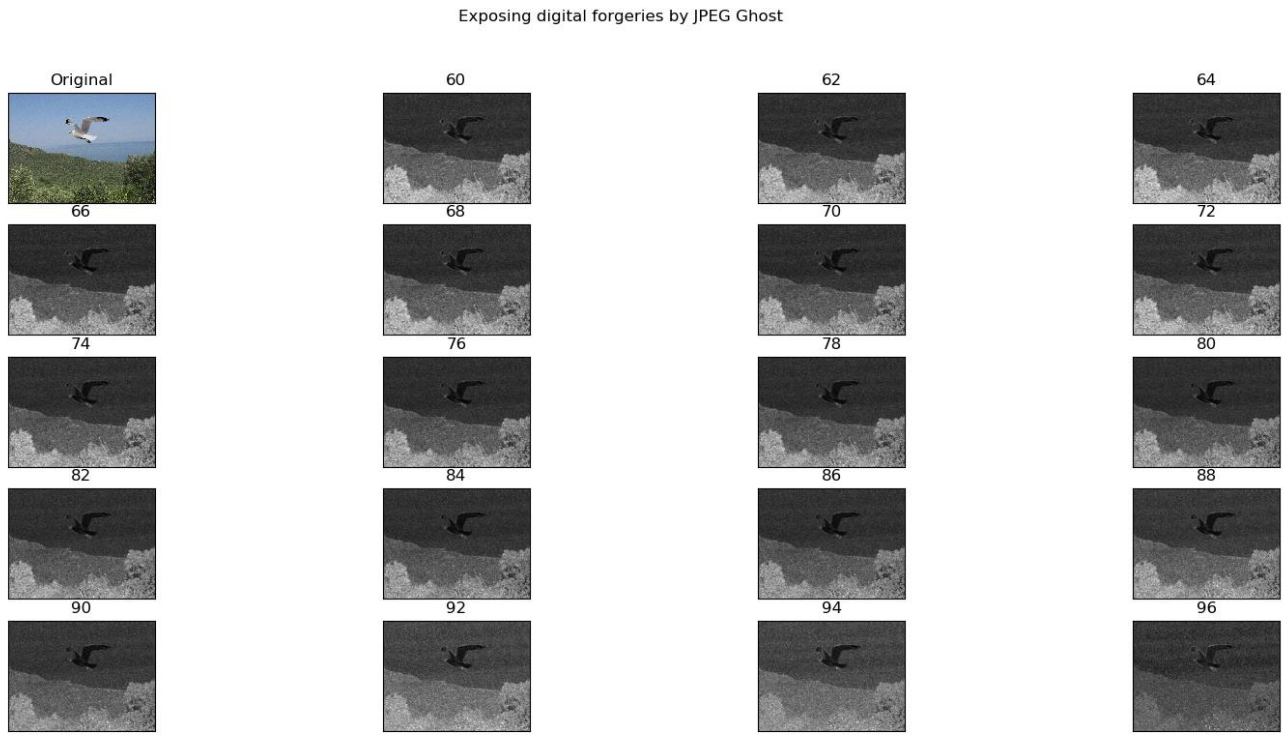
Exposing digital forgeries by JPEG Ghost



Red: Tampered region

The tampered region in this method is the region with strong blue (or black if plot in greyscale). This happens when we choose the correct quality of the tampered region. Then, the different between tampered region and the resaved image with this quality is minimum => small value => dark color.

This method is very hard to choose the best quality, so I proposed the multiple map, that plot many smaller qualities with step of 2 from 60 of the resaved image, then we can see the different more easily.



(This time, I plot in grey-scale)

c. Exposing digital forgeries by noise inconsistencies [5]

A commonly used tool to conceal the traces of tampering is the addition of locally random noise to the altered image regions. The noise degradation is the main cause of failure of many active or passive image forgery detection methods. Typically, the amount of noise is uniform across the entire authentic image. Adding locally random noise may cause inconsistencies in the image's noise. Therefore, the detection of various noise levels in an image may signify tampering.

This method is a segmentation method detecting changes in noise level. The main drawback of the method is that authentic images also can contain various isolated regions with totally different variances. The method can denote these regions as inconsistent with the rest of the image. Therefore, a human interpretation of the output of the method is necessary. Because of these reasons, the proposed method is useful as a supplement to other forgery detection methods rather then a standalone forgery detector.

The proposed method is based on a few main steps:

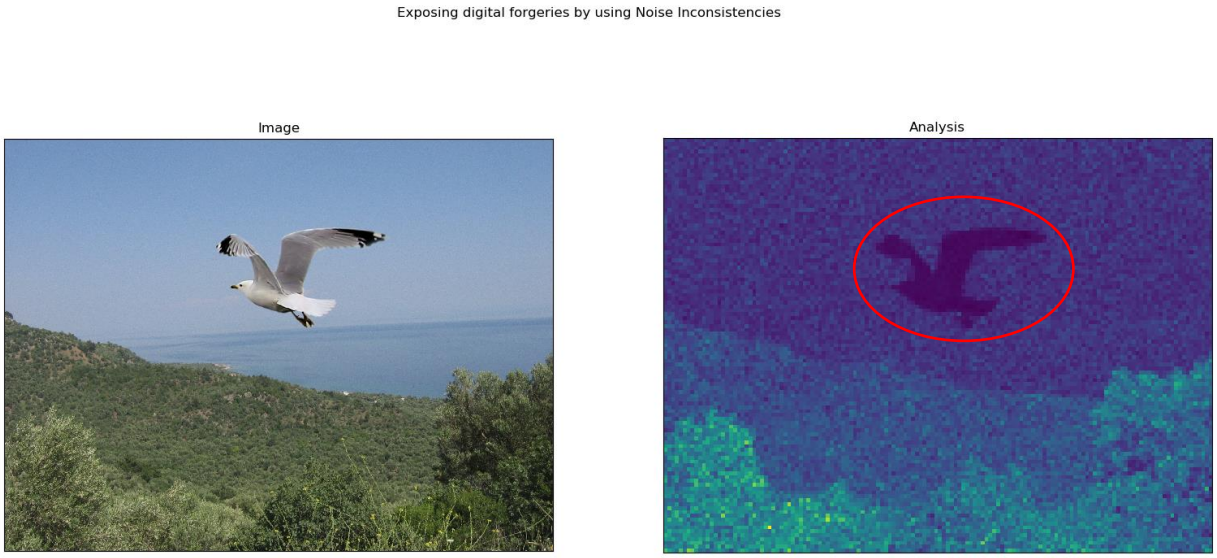
- wavelet analysis,
- tiling sub-band HH1 with non-overlapping blocks,
- blocks noise variance estimation,

$$\hat{\sigma} = \frac{median(|HH_1|)}{0.6745}.$$

- blocks merging.

For more detail of this method check it in the publication: Using noise inconsistencies for blind image forensics [5]

Here is my actual result testing the implementation of this method on my image:



Red: Tampered region

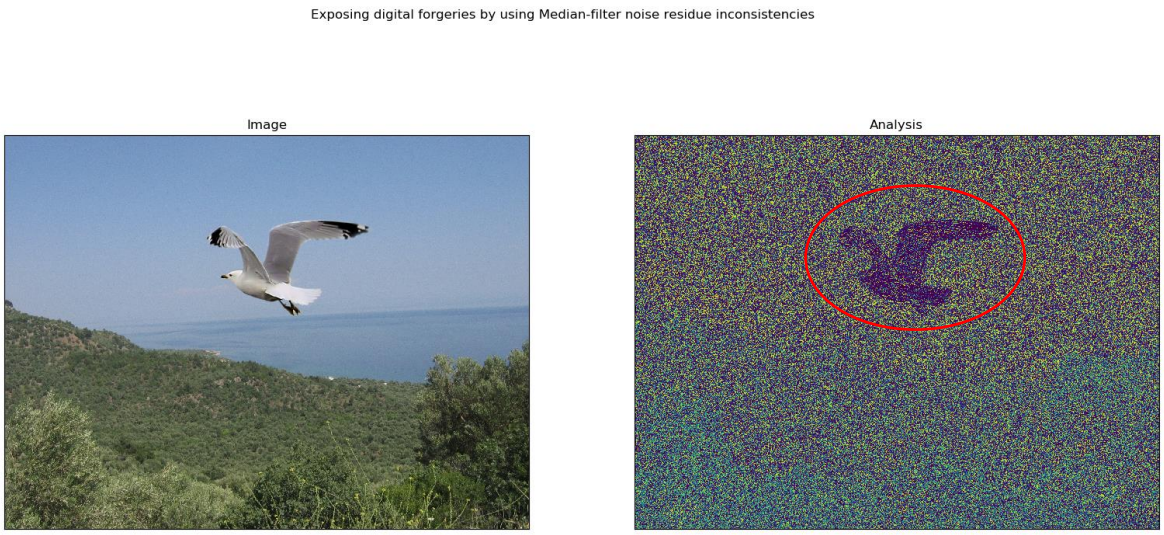
d. Exposing digital forgeries by Median-filter noise residue inconsistencies [6]

Natural images are full of noise. When they are modified this often leaves visible traces in the noise in an image. But seeing the noise in an image can be hard. This method takes a very simple noise reduction filter (a separable Median Filter) and reverses it's results. Rather than removing the noise it removes the rest of the image.

For more detail of this method check it in:

https://29a.ch/2015/08/21/noise-analysis-for-image-forensics [6]

Here is my actual result testing the implementation of this method on my image:



Red: Tampered region

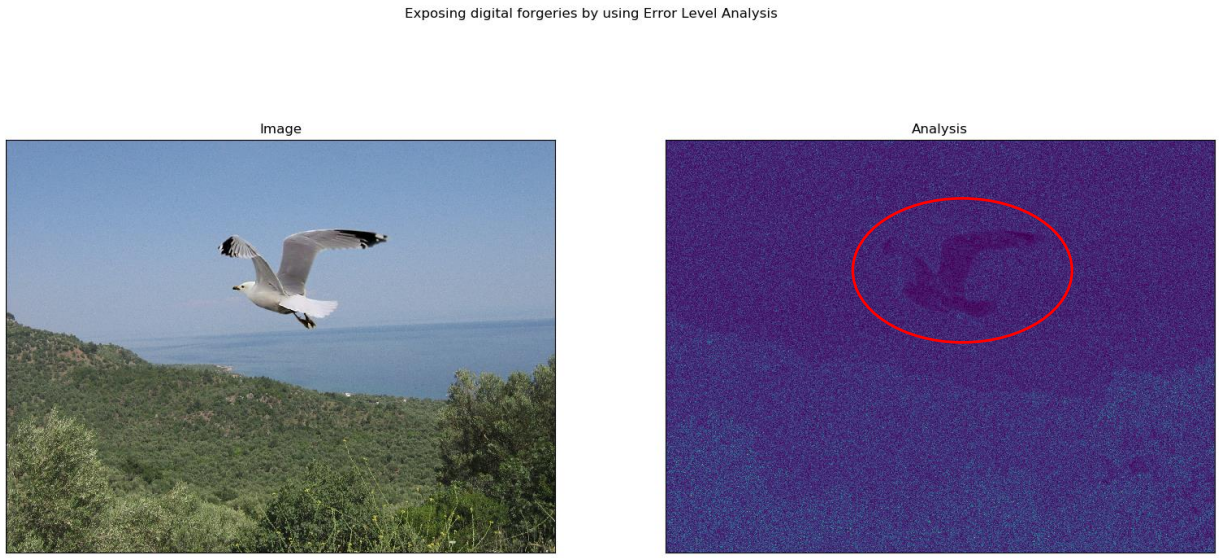
e. Exposing digital forgeries by Error Level Analysis [7]

Error Level Analysis (ELA) permits identifying areas within an image that are at different compression levels. With JPEG images, the entire picture should be at roughly the same level. If a section of the image is at a significantly different error level, then it likely indicates a digital modification.

With ELA, every grid that is not optimized for the quality level will show grid squares that change during a resave. For example, digital cameras do not optimize images for the specified camera quality level (high, medium, low, etc.). Original pictures from digital cameras should have a high degree of change during any resave (high ELA values). Each subsequent resave will lower the error level potential, yielding a darker ELA result. With enough resaves, the grid square will eventually reach its minimum error level, where it will not change anymore.

For more detail of this method check it in: A Picture's Worth: Digital Image Analysis and Forensics [7]

Here is my actual result testing the implementation of this method on my image:



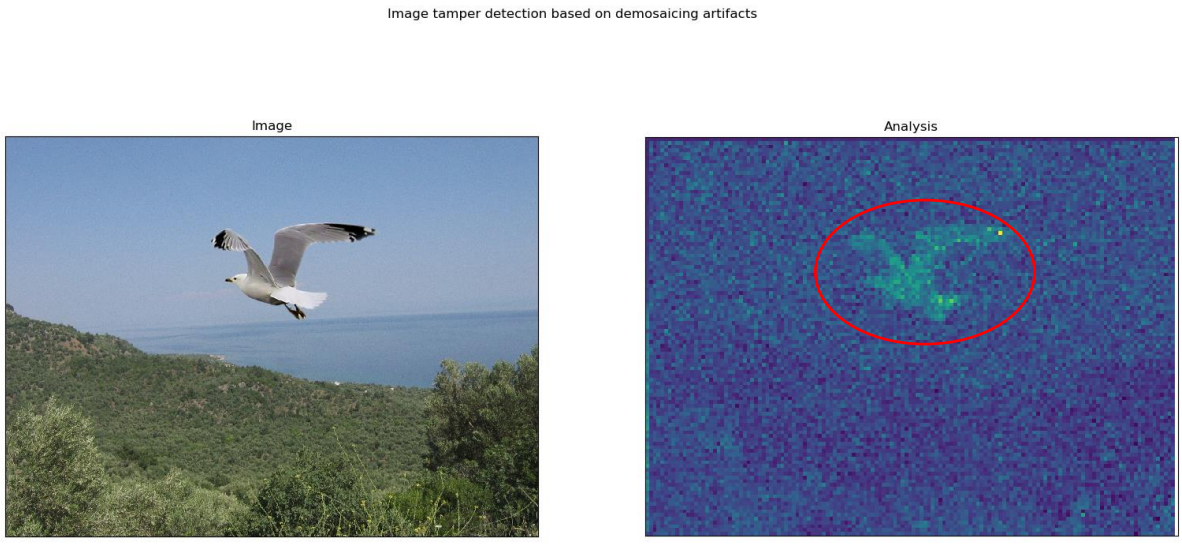
Red: Tampered region

f. Exposing digital forgeries based on demosaicing artifacts

This technique is a tamper detection techniques based on artifacts created by Color Filter Array (CFA) processing in most digital cameras. The techniques are based on computing a single feature and a simple threshold based classifier. My tool implements the first of two approaches in this paper.

For more detail of this method check it in the publication: Image tamper detection based on demosaicing artifact. [8]

Here is my actual result testing the implementation of this method on my image:



Red: Tampered region

REFERENCES

[1]. Böhme R., Freiling F.C., Gloe T., Kirchner M. (2009) Multimedia Forensics Is Not Computer Forensics. In: Geradts Z.J.M.H., Franke K.Y., Veenman C.J. (eds) Computational Forensics. IWCF 2009. Lecture Notes in Computer Science, vol 5718. Springer, Berlin, Heidelberg

[2]. Redi, J.A., Taktak, W. & Dugelay, JL. Multimed Tools Appl (2011) 51: 133. https://doi.org/10.1007/s11042-010-0620-1

[3]. Birajdar, Gajanan & Mankar, Vijay. (2013). Digital image forgery detection using passive techniques: A survey. Digital Investigation. 10. 226–245. 10.1016/j.diin.2013.04.007.

[4]. Farid, Hany. (2009). Exposing digital forgeries from JPEG ghosts. Information Forensics and Security, IEEE Transactions on. 4. 154 - 160. 10.1109/TIFS.2008.2012215.

[5]. Mahdian, Babak & Saic, Stanislav. (2009). Using noise inconsistencies for blind image forensics. Image and Vision Computing. 27. 1497-1503. 10.1016/j.imavis.2009.02.001.

[6]. Forensic Focus - Articles. (2018). Detecting Forged (Altered) Images. [online] Available at: https://articles.forensicfocus.com/2013/08/22/detecting-forged-altered-images/ [Accessed 2 Jun. 2018].

[7] Krawets, Neil. "A Picture's Worth: Digital Image Analysis and Forensics"

[8] Dirik, Ahmet Emir & Memon, Nasir. (2009). Image tamper detection based on demosaicing artifact. Proceedings of IEEE International Conference on Image Processing (ICIP). 1497 - 1500. 10.1109/ICIP.2009.5414611.

[9] FotoForensics Tutorial. http://fotoforensics.com/tutorial.php

[10] Forensic Focus - Articles. (2018). Detecting Forged (Altered) Images. [online] Available at: https://articles.forensicfocus.com/2013/08/22/detecting-forged-altered-images/ [Accessed 2 Jun. 2018].