Internship: Detection of copy-move forgeries in digital images

Reference CYBERINSTITUTE-INT-19007

Description
With the increasing popularity and sophistication of photo editing software, our trust on authenticity of digital images is decreasing. Image forgeries can be easily found in our daily life, and have been used, for instance, in advertising and in political and personal attacking. One specific image tampering is the copy-move operation, in which a region of the image is copied and pasted at another position within the same image (see Figure 1 left for an example). In the literature, a number of algorithms have been proposed to detect and locate regions involved in a copy-move forgery [1,2,3]. The objective of the proposed internship is to improve an existing copy-move detection method described in [3], in terms of both forensic performance and algorithmic elegance. The method of [3] is based on dense PatchMatch [4] and gives state-of-the-art detection results.

Figure 1. On left is a copy-move forgery where involved regions are highlighted, in middle is the raw detection result of forgery localization, and on right is the final result after a number of post-processing. The images are extracted from [3].

References:

Within the Grenoble Alpes Cybersecurity Institute, the internship student is expected to accomplish the following tasks, in chronological order.
1. Carry out a brief literature review, mainly on copy-move forgery detection (around 5 scientific papers).
2. Understand the implementation of the method proposed in [3], which is freely available on-line.
3. Improve the method so that it can identify which detected region is the original one and which region is the copy-pasted one. (Currently the method in [3] cannot distinguish them, see Figure 1 right.)
4. Propose an elegant method (i.e., without multiple post-processing as in [3]) to induce a clean and accurate localization map (such as the one in Figure 1 right) from the noisy raw detection map (Figure 1 middle).
5. Integrate the improved method into a multi-detector system for exposing real-world image forgeries.

After completion of this internship, this work can be extended to a Ph.D. thesis.

Prerequisites
We seek excellent candidates enrolled in an Engineering or Master degree with strong background in Mathematics and Image Processing, highly motivated by the proposed research problem, and proficient in Python/Matlab programming. Working language can be either French or English.

Tutors
Dr. François Cayre, Dr. Kai Wang and their Ph.D. students Ludovic Darmet and Ivan Castillo Camacho

Applications
Please send your resume, application letter with two recommendations (including education director), first year master’s degree grades (mandatory) and second year grades (if possible) to cyberalps-contact@univ-grenoble-alpes.fr
For more information on the internship, please contact francois.cayre@gipsa-lab.grenoble-inp.fr or kai.wang@gipsa-
**Location**  
Department of Images and Signals of GIPSA-lab (Grenoble Images Parole Signal Automatique, [http://www.gipsa-lab.grenoble-inp.fr/](http://www.gipsa-lab.grenoble-inp.fr/))

**Starting date**  
February 2019

**Duration**  
5 to 6 months

**Allowance**  
In accordance with existing regulations (approx. 560€/month). Part of travel expenses can be covered.