Title: Securing deep learning results using the a contrario method: application to mass detection in satellite imagery

Summary of the thesis

Neural networks have revolutionized image analysis, particularly in the fields of object detection and image classification. One limitation of deep networks is that it is difficult to know their ability to generalize to new images, especially when the training base is small. The problem is therefore to statistically assess the validity of a detection. The thesis will develop a statistical detection method (based on a contrario) to assess the confidence of each detection. Assessing the confidence of neural network detection on new examples will allow us to evaluate the generalizability of an object detector. The methodology will be tested in real life applications, for detecting objects in satellite images.

Context of the thesis

The thesis will be carried out in collaboration with DGA (Directorate General of Armaments) and industrial actors (startup and R&D environments). The doctoral student will work at the CMLA (http://cmla.ens-paris-saclay.fr/).

- Thesis supervisors: Raffaele Grompone, Sébastien Drouyer
- Ecole Doctorale Jacques Hadamard, Université Paris-Saclay
- Duration: 3 years
- Premises: CMLA, Ecole Normale Supérieure Paris-Saclay
- Master's degree in image processing, signal processing, mathematics or computer science required.
- Languages: French or English
- In view of the industrial collaborations, the remuneration of the thesis will be increased by 25% compared to the school / CNRS scholarships.

Application

If you are interested, please contact us on grompone@cmla.ens-cachan.fr and drouyer@cmla.ens-cachan.fr.

Description

In image processing, the performance of object detection and recognition algorithms has grown considerably thanks to deep learning. In public benchmarks such as COCO or Kitti, algorithms using deep learning are now the state of the art. However, these approaches have several limitations. One of the major problems is that the results given by neural networks are not interpretable: when they work, it is very difficult to know why because they often consist of millions of parameters. A direct consequence is that it is difficult to predict the ability of the detector to generalize. To counter these effects, public benchmarks often concentrate hundreds of thousands or even millions of annotated images. However, when you have a specific application and want to train networks to detect objects that do not exist in public benchmarks, it is often not possible to create databases with such large sizes.

It is also possible to deceive neural networks by adding a noise adapted to the images. Antagonistic examples illustrate this problem: while a neural network succeeds in correctly classifying an image, the addition of a specific noise, invisible to the human observer, misleads the same network.
Overall, it therefore appears that the robustness of neural networks in the face of new examples or simply in the presence of noise is difficult to assess. In addition, neural networks do not provide a measure of the reliability of their detections. Such a measure would be equivalent to a FDR (false detection rate) or NFA (number of false alarms).

The thesis project is based on the assumption that the so-called a contrario theory can make a decisive contribution to this problem. The principle of non-accidentality refers to the fact that relationships between independent elements take on meaning when it seems unlikely that they are the result of chance. This principle is formalized in the a contrario theory, which is used in computer vision to determine detection thresholds in accordance with non-accidentality. In its simplest form, this theory automatically sets a threshold to differentiate a signal (what you want to detect) from noise in the image.

The purpose of this project is therefore to combine neural networks and a contrario theory to both evaluate and improve the robustness of neural networks and to apply them to massive satellite Earth remote monitoring tasks. This thesis project falls within the framework of the MRIS 2019 priority theme "Content Processing and Analysis", in the Information Engineering and Robotics field.