Image processing and deep learning

Contact: Gergő Bognár, bognargergo@staff.elte.hu, bogqaai@inf.elte.hu (Teams)

Goals: Combination of traditional image processing methods and deep learning approaches in order to solve complex image processing problems. Development environment: Matlab and Python (numpy/pytorch).

Topics:

1. **Object detection, semantic segmentation (in progress, possible to join)**
   Implementation of model-based and deep learning approaches for object detection and segmentation in images; application to real-world datasets, including camera images, orthophotos, satellite images, etc. (see [1, 2] for example datasets). Combination of image feature extraction methods, state-of-the-art convolutional networks (like AlexNet, VGG, GoogLeNet, YOLO), and deep learning techniques (like transfer learning). See also: [3]

2. **CT tumour detection and segmentation**
   Implementation of model-based and deep learning approaches for CT segmentation, and to tumour detection in particular. Evaluation on public human lung CT datasets (e.g. RIDER [4]).

3. **Adversarial machine learning**
   Adversarial machine learning investigates attacks and defenses on machine learning methods (see [5]). The basic observation is that deep neural network are significantly discontinuous and sensitive to their input: well-crafted, but hardly perceptible perturbations of the input data may cause serious misclassifications (see [6]). The task is to apply and develop adversarial attacks for deep learning methods used for object detection and segmentation, and then develop defense methods against these attacks, which possibly leads to more reliable and robust methodology.

References:

[1] **Kaggle**. Online: https://www.kaggle.com/datasets (accessed 16 September 2023)

[2] **Earth Observation Database**. Online: https://eod-grss-ieee.com/dataset-search (accessed 16 September 2023)

[3] A. Kirillov et al. **“Segment Anything.”** (2023), arXiv: 2304.02643

[4] **RIDER Lung CT** on *Cancer Imaging Archive*. Online: https://wiki.cancerimagingarchive.net/display/public/rider+lung+ct (accessed 16 September 2023)

[5] L. Huber. **“A friendly intro to adversarial attacks.”** Online: https://towardsdatascience.com/fooling-neural-networks-with-adversarial-examples-8afd36258a03 (accessed 16 September 2023)

[6] C. Szegedy et al. **“Intriguing properties of neural networks.”** (2014), arXiv: 1312.6199