Traitement d'image par Deep Learning

Durée

3 jours.

Participants

Analystes des données, ingénieurs ML.

Prérequis

Bonne connaissance et pratique du Machine Learning avec Python.

Description

Formation avancée spécialisée dans le traitement d'images.

Objectifs pédagogiques

Acquérir les fondamentaux de l'état de l'art en traitement d'image.

Travaux pratiques

Multiples cas d'utilisation avec Keras.

Programme

Rappels : Concepts fondamentaux d'un réseau de neurones

- Réseau de neurones : formalisme, fonctions d'activations ;
- Apprentissage d'un réseau de neurones : fonctions de coût, SGD, Adam ;
- Initialisation et régularisation : orthogonalité à l'initialisation, régularisations L1/L2, politiques de batchs, dropout.

Réseaux convolutifs (*CNNs*)

- Présentation des CNNs : principes fondamentaux et applications ;
- Fonctionnement fondamental d'un CNN : filtre, remplissage et pas de convolution ;
- Quelques exemples classiques : LeNet, VGG, Network in Network ;
- Architectures modernes : ResNet, DenseNet ;
- Transfert d'apprentissage.

Auto-encodeurs et réseaux antagonistes (*GANs*)

- Auto-encodeurs : réduction de dimensionnalité & détection d'anomalie ;
- Présentation des réseaux antagonistes (GAN) ;

- Convergence d'un GAN : WassersteinGAN, BeGAN, distance du terrassier (*Earth Moving Distance*) ;
- Régularisation ;
- Entraînement sans supervision & en semi-supervision.

Cas d'utilisation de la vision par ordinateur moderne

- Détection d'objets ;
- Segmentation d'instances et d'images ;
- Unobfuscation / inpainting ;
- Suivi vidéo avec YoloV4 (*Object Tracking*).

Interprétations de CNN

- Saliency maps ;
- gradconv ;
- occlusion sensitivty ;
- D-Rise (Black-box Explanation of Object Detectors via Saliency Maps. 2021).

Attaques de CNN

- 2004 : Premier papier que j'ai trouvé qui parle d'attaque, Adversarial Classification ;
- 2014: Premier papier d'attaque de CNN, *Intriguing properties of neural networks* ; pour les CNNs ;
- 2016 : attaque par modifications de petits bouts de l'image (lunettes), *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition* ;
- 2017 : attaque par stickers posés sur des paneaux, *Robust Physical-World Attacks on Machine Learning Models* ;
- 2018 : Talk de Percy Liang qui avait beaucoup tourné qui parle des attaques conjointement à l'évaluation.