Towards Privacy-preserving Federated Learning in Multi-Task Learning from Multiple Datasets

Master 2/Ecole d'Ingénieur Internship

Expected starting: February/March 2024 (6 months)

Keywords

Deep learning, multi-task learning, Federated learning, disjoint datasets, remote sensing

Context and objectives

In recent years, deep neural networks have been successfully adopted in almost every application domains of computer vision, including remote sensing for earth observation. The vast number of remote sensing images captured from frequent satellite passes or aerial acquisition, however, are not readily usable to train deep networks developed for generic vision problems due to the lack of task-specific annotations and possible domain gaps.

On the other hand, the individual development efforts of various research groups for their particular problems result in cluttered annotations and modalities: each dataset is typically annotated for a few tasks while many tasks may be related to one another and could be jointly learned to leverage complementary information and improve their performance. Coupling solving different but related tasks, or well-known in the ML community as multi-task learning, has also gained increasing attention in the remote sensing community. As multi-task learning aims to predict different targets from the same inputs, it typically requires annotations of all the target tasks for each input example to learn the interrelationship at the shared encoder by optimizing all tasks at the same time.

Obtaining extra annotations to maintain multi-task datasets, however, add extra burden to the development process. Recently, it has been shown in the vision community that that multi-task learning could be beneficial even when the tasks are partially annotated [3]. Training a network for multiple task while the training examples are annotated for a single task can improve the performance of both tasks. Such discovery could be of interest to explore for the benefit of remote sensing community.

This project is aimed to research the combination of different datasets annotated for different tasks which may follow different statistical distributions to benefit and improve performance of one another. To that end, we will focus on the object detection, i.e. bounding boxes prediction, and semantic segmentation tasks, which are closely related yet not trivial to combine due to differences in spatial structure and information granularity: object detection predicts bounding-box coordinates at object instance level while semantic segmentation provides per-pixel predictions of category including amorphous regions. A general scheme is shown in Figure 1. Another challenge of the project is to bridge possible domain gaps between the participating datasets with possible approaches including generative models (GANs, diffusion models, etc.). The above objectives should be targeted by putting dataset security and privacy at the center of any strategies proposed and adopted.

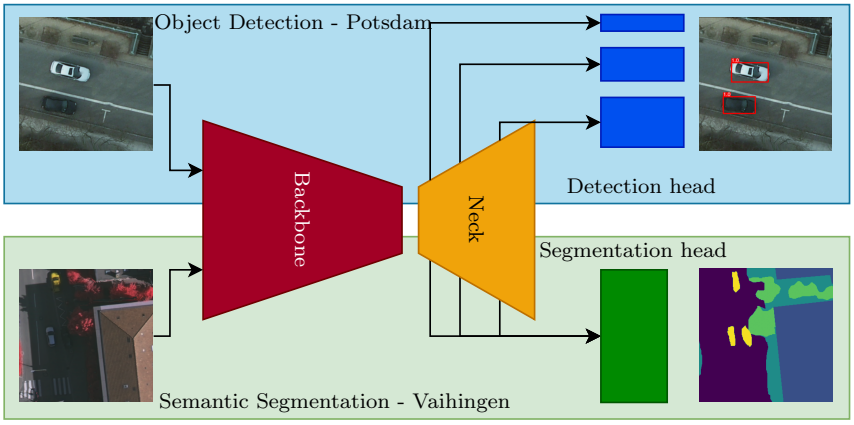

Figure 1: The general scheme of multi-task learning with partially annotated datasets simulated using the ISPRS benchmark [5]: the Postdam subset is assumingly annotated only with object detection thus can only train the detection subnet and Vaihingen subset semantic segmentation. The feature encoder (backbone and neck) is shared among the tasks.

Work program (expected)

In order to address the aforementioned objectives, a tentative work program is given below.

- Literature study and implement of state-of-the-art object detection and semantic segmentation as single task learning, e.g. DETR [2], FCOS [6], SegFormer [9], etc.
- Literature study and implement methods to secure data privacy, e.g. privacy-preserving federated learning [10, 1]
- Evaluation STL vs. MTL on benchmark datasets such as iSAID [7, 8], DIOR [4],
- Improvement of existing solutions and/or development of novel methods, starting with ISPRS data [5] and extended to other benchmark datasets.
- Evaluation STL vs. MTL over Federated learning with privacy-preserving goal.
- Dissemination: Master thesis, publication + source codes (highly recommended target).

Required background and skills

- Student in computer science and/or machine learning and/or signal & image processing;
- Python programming and familiarity with deep learning framework (Pytorch/Tensorflow);
- Highly motivated and passion in research.

Supervision

The expected intern will join the OBELIX research group (`www.irisa.fr/obelix`) from IRISA (UMR 6074) is located in the UBS (Université Bretagne Sud) campus in Vannes 56000, France. He/She will be jointly supervised by:

- Dr. Hoàng-Ân Lê[1], Postdoctoral researcher, IRISA/OBELIX
- Dr. Minh-Tan Pham[2], Assistant Professor (Maître de Conférences) at UBS, IRISA/OBELIX

[1] `https://lhoangan.github.io/about`
[2] `https://sites.google.com/site/mtanpham89`

Application

Position to be filled as soon as possible **(call closed on December 15, 2023)**. Send your detailed CV + Motivation letter + Master transcripts to {hoang-an.le,minh-tan.pham}@irisa.fr. Potential candidates will be contacted for interview.

References

[1] Barış Büyüktaş, Gencer Sumbul, and Begüm Demir. Federated learning across decentralized and unshared archives for remote sensing image classification. *arXiv preprint arXiv:2311.06141*, 2023.

[2] Nicolas Carion, Francisco Massa, Gabriel Synnaeve, Nicolas Usunier, Alexander Kirillov, and Sergey Zagoruyko. End-to-End Object Detection with Transformers. In *Proceedings of the European Conference on Computer Vision (ECCV)*, 2020.

[3] Hoàng-Ân Lê and Minh-Tan Pham. Data exploitation: multi-task learning of object detection and semantic segmentation on partially annotated data. In *British Machine Vision Conference (BMVC)*, 2023.

[4] Ke Li, Gang Wan, Gong Cheng, Liqiu Meng, and Junwei Han. Object detection in optical remote sensing images: A survey and a new benchmark. *ISPRS Journal of Photogrammetry and Remote Sensing*, 159:296–307, 2020.

[5] F Rottensteiner, G Sohn, J Jung, M Gerke, C Bailard, S Benitez, and U Breitkopf. The ISPRS benchmark on urban object classification and 3D building reconstruction. In M Shortis, N Paparoditis, and C Mallett, editors, *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, pages 293–298, Melbourne, Australia, aug 2012. International Society for Photogrammetry and Remote Sensing (ISPRS).

[6] Zhi Tian, Chunhua Shen, Hao Chen, and Tong He. FCOS: A simple and strong anchor-free object detector. 2021.

[7] Syed Waqas Zamir, Aditya Arora, Akshita Gupta, Salman Khan, Guolei Sun, Fahad Shahbaz Khan, Fan Zhu, Ling Shao, Gui-Song Xia, and Xiang Bai. iSAID: A Large-scale Dataset for Instance Segmentation in Aerial Images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 28–37, 2019.

[8] Gui-Song Xia, Xiang Bai, Jian Ding, Zhen Zhu, Serge Belongie, Jiebo Luo, Mihai Datcu, Marcello Pelillo, and Liangpei Zhang. DOTA: A Large-Scale Dataset for Object Detection in Aerial Images. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, jun 2018.

[9] Enze Xie, Wenhai Wang, Zhiding Yu, Anima Anandkumar, Jose M Alvarez, and Ping Luo. Segformer: Simple and efficient design for semantic segmentation with transformers. In *Neural Information Processing Systems (NeurIPS)*, 2021.

[10] Jiang Zhu, Jun Wu, Ali Kashif Bashir, Qianqian Pan, and Yang Wu. Privacy-preserving federated learning of remote sensing image classification with dishonest-majority. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2023.