Jan Hendrik Metzen

Senior Expert

I am Senior Expert in Deep Learning at Bosch Center for Artificial Intelligence (BCAI). My primary research focuses on making AI (specifically computer-vision based perception) robust, reliable, and safe. For this, we levarage strong generative models for finding systematic errors of image classifiers on rare subgroups and systematic errors of object detectors. We also identified vulnerabilities of Transformer-based neural network against adversarial patch/token attacks. To counteract such vulnerabilities, we developed architectures that are certifiably robust against patch attacks for image classifiers as well as for semantic segmentation. Furthermore, we proposed methods for adversarially training neural networks to become robust against universal perturbations and universal adversarial patches. In addition, we provide methods for test-time adaptation of neural networks to improve robustness to domain shifts and study the role of shape-biased representations on robustness to common image corruptions.

A different strand of my research is automating machine learning (AutoML), specifically Neural Architecture Search. The latter research field is motivated by the vast design space of neural networks and the diversity of inference hardware. Manually tailoring a neural architecture for every type of hardware is cumbersome and not scalable - hardware-aware neural architecture search can vastly improve design efficiency and thus reduce cost of AI development. See our survey on Neural Architecture Search and a more recent survey on Neural Architecture Search for Dense Prediction Tasks in Computer Vision. Recently, we developed AutoCLIP, a method auto-tuning zero-shot classifiers for vision-language models that improves zero-shot performance across a broad range of domains.

I also love contributing to machine learning libraries, both open source and proprietary. I am a (recently mostly inactive) core contributor of scikit-learn, where I contributed tools for probability calibration of classifiers and for kernel ridge regression. Moreover, I have written a complete redesign of the Gaussian process module for scikit-learn. At BCAI, I am/was involved as core developer for frameworks for deep learning training pipelines, neural architecture search, and robustness evaluation.

I am a member of ELLIS and regularly review for scientific conferences and journals such as ICLR, ICML, NeurIPS, and TMLR. I was senior area chair of the AutoML 2022 conference and co-organizer of the workshops NAS@ICLR 2020 and NAS@ICLR 2021. I have been recognized by ICLR as Highlighted Reviewer in 2022 and Outstanding Reviewer in 2021.

See my personal website for more details.

Böblingen, Germany
janmetzen@mailbox.org
jmetzen.github.io
jan_metzen (Twitter)
jan-hendrik-metzen (LinkedIn)
jmetzen (github)
w047VfEAAAAJ (Google Scholar)

Work

Senior Expert 'Robust Scalable Perception'

Bosch Center for Artificial Intelligence (BCAI), Robert Bosch GmbH
Jan 2020 – Present

Making Deep Learning Perception Safe by Model Auditing and Robust Training and Architectures.

- Robustness of Deep Learning (Systematic Errors, Domain Shift, Adversarial Examples)
- Neural Architecture Search
- Synthetic Data

Research Scientist

Bosch Center for Artificial Intelligence (BCAI), Robert Bosch GmbH
Mar 2016 – Dec 2019

- Adversarial Examples
- Neural Architecture Search

Research Assistant

Robotics Research Group, University of Bremen
Nov 2009 – Feb 2016

- Reinforcement Learning
- Robot Learning
- Bayesian Optimization

Project Leader 'CASCADE'

Robotics Research Group, University of Bremen
Aug 2014 – Jan 2016

Leading the subteam in Bremen of the EU project CASCADE

- Surgical Robotics

Team leader 'Sustained Learning'

Robotics Innovation Center, German Research Center for Artificial Intelligence (DFKI RIC, Bremen)
Jan 2013 – Dec 2015

Leading a team of approximately 10 researchers focusing on robotic learning.

- Robot Learning

Researcher

Robotics Innovation Center, German Research Center for Artificial Intelligence (DFKI RIC, Bremen)
Jul 2007 – Oct 2009

- Brain-Computer Interfaces
- Robot Learning

Research Assistant

Robotics Research Group, University of Bremen
Sep 2006 – Jun 2007

- Reinforcement Learning

Volunteer

Core Contributor

scikit-learn
Jan 2016 – Present

Senior Area Chair

AutoML Conference 2022
Jan 2022 – Dec 2022

Co-organizer

'Neural Architecture Search' workshop at ICLR 2021
Jan 2021 – Dec 2021

Co-organizer

'Neural Architecture Search' workshop at ICLR 2020
Jan 2020 – Dec 2020

Highlighted Reviewer

ICLR 2022
Jan 2022 – Dec 2022

Outstanding Reviewer

ICLR 2021
Jan 2021 – Dec 2021

Regularly Reviewer

ICLR, ICML, NeurIPS, TMLR
Jan 2016 – Present

Member

ELLIS
Jan 2022 – Present

Education

University Bremen, Bremen, Germany

Computer Science
Nov 2009 – Feb 2014

Dr.rer.nat. (PhD)

University Münster, Münster, Germany

Computer Science
Oct 2001 – Aug 2006

Diploma

Awards

Scholarship (2004 - 2006)

Awarded by **Studienstiftung des Deutschen Volkes (German National Academic Foundation)**
Jan 2004

Languages

German
Native speaker

English
Fluent

Spanish
Basic

French
Basic