Krishna Kanth Nakka

+41-787330059 | Switzerland | krishnakanthnakka.github.io | krishkanth.92@gmail.com | LinkedIn | Github

Interests

Machine Learning and Computer Vision: Deep Neural Networks, Adversarial Attacks, Adversarial Robustness, Anomaly Detection, Semantic Segmentation, Object Tracking, Metric Learning, Domain Adaptation, Pose Estimation, Knowledge Distillation, Interpretable Networks, and Deep Generative Networks

Education

Ecole Polytechnique Fédérale de Lausanne (EPFL) **Sep 2017 - Aug 2022**
Ph.D. in Computer Science
Advisors: Dr. Mathieu Salzmann and Prof. Pascal Fua, Computer Vision Lab
Title: Understanding Deep Neural Networks using Adversarial Attacks

Indian Institute of Technology Kharagpur **Jun 2010 - May 2015**
M.Tech with specialization in Signal Processing and Instrumentation,
B.Tech (Honours) in Electrical Engineering (5 year Dual Degree) GPA: 8.89/10.0

Selected Projects

Anomaly Detection in Street-Scene CNNs via Pix2Pix Image-to-Image Translation **ICCV19**
Designed a discrepency generator-based network to detect unusal and rare anomalous objects at pixel-level for street-scene segmentation networks *without* any knowledge of them at training time via Pix2Pix generator.

Learning Cross-Domain Generative Adversarial Perturbations to fool DNNs **NeurIPS21**
Proposed a GAN with mid-level feature separation loss to conduct highly transferable black-box attacks beyond domain (ImageNet, ChestX), tasks (Recognition, Detection), and architectures (CNNs, Transformers). Furthermore, designed an universal attack framework to steer the Visual Object Tracker along arbitrary trajectories.

Improving Adversarial Robustness of CNNs by Discriminative Feature Separation **ACCV20**
Proposed an attention-aware CNN with novel latent feature clustering and separation losses based on metric learning to improve robustness to white-box and black-box attacks.

Rethinking Pose-Appearance Disentanglement in 3D Pose Estimation CNNs **arXiv22**
Proposed a testbed to evaluate the disentanglement of self-supervised pose and appearance latent codes and uncovered that disentanglement is, in fact, far from complete.

Prototypical Networks to interpret CNNs and Diagnose its Failure Modes **ICCVW19**
Proposed a bag-of-words-based interpretable layer to understand the decisions of CNN through activated prototypes, further analyzed the mechanism of adversarial attacks, and designed a detection framework.

Robustness-Performance Tradeoff in Context-dependent Segmentation Networks **ECCV20**
Proposed an indirect local attack framework to fool the dynamic objects like cars and buses by perturbing in far away regions such as roads and buildings and identified that context (dilation, attention, pooling, etc.) as the reason for high vulnerability.

Work Experience

Software Engineer, **Samsung R&D Institute**, Bangalore **Sep 2015 - July 2017**
Prototyped an algorithm to remove reflections from a input video sequence captured in indoor scenes and futher proposed a Context Encoder-Decoder CNN network to directly generate reflection-free images.

Intern, **University of Alberta,** Edmonton **May 2014 - July 2014**
Benchmarked large scale content-based image retrieval methods from first & second-order feature representations.

Intern, **University of Queensland**, Australia **Nov 2013 - Jan 2014**
Developed an exponentially decaying non-uniform sampling scheme to shorten acquisition time in spectroscopy.

Intern, **Philips Research Asia,** Bangalore **May 2013 - July 2013**
Implemented a part-based human detection model using Adaboost based ensemble of weak SVM classifiers.

Publications and Preprints

1. **Krishna Kanth Nakka** and Mathieu Salzmann. **Understanding Pose and Appearance Disentanglement in 3D Human Pose Estimation.** *Under review*

2. **Krishna Kanth Nakka** and Mathieu Salzmann. **Learning Transferable Adversarial Perturbations.***Neural Information and Processing Systems (NeurIPS), 2021*

3. **Krishna Kanth Nakka** and Mathieu Salzmann.**Universal, Transferable Adversarial Attacks for Visual Object Trackers**. *Under review*

4. **Krishna Kanth Nakka** and Mathieu Salzmann.**Towards Robust Fine-grained Recognition by Maximal Separation of Discriminative Features.** *Asian Conference on Computer Vision (ACCV), 2020.*

5. **Krishna Kanth Nakka** and Mathieu Salzmann. **Indirect Local Attacks for Context-aware Semantic Segmentation Networks.** *European Conference on Computer Vision (ECCV)* ***Spotlight 2020.***

6. Krzysztof Lis, **Krishna Kanth Nakka,** Pascal Fua, Mathieu Salzmann and Mathieu Salzmann. **Detecting the Unexpected via Image Resynthesis.** *International Conference on Computer Vision (ICCV), 2019.*

7. **Krishna Kanth Nakka** and Mathieu Salzmann.**Interpretable BoW Networks for Adversarial Example Detection.** *Explainable and Interpretable AI workshop, ICCV 2019.*

8. **Krishna Kanth Nakka** and Mathieu Salzmann. **Deep Attentional Structured Representation Learning for Visual Recognition.** *British Media Vision Conference (BMVC), 2018.*

9. Jonna S, **Nakka KK**, Sahay RR,**Deep learning based fence segmentation and removal from an image using a video sequence.** *International Workshop on Video Segmentation,* ECCV *2016.* ***Oral.***

10. Jonna S, **Nakka KK**, Khasare VS, Sahay RR.**Detection and removal of fence occlusions in an image using a video of the static/dynamic scene.** *Journal of Optical Society of America* (JOSA) *A. 2016.*

Skills

- Languages: Proficient in Python. Familiar with C/C++, HTML, SQL
- Softwares: PyTorch, Tensorflow, Caffe, Keras, MATLAB, Docker, Kubernetes
- Libraries: OpenCV, NumPy, Pandas, Matplotlib

Relavent Courses

Machine Learning, Artificial Neural Networks, Digital Image Processing, Linear Algebra, Probability and Statistics, Distributed Information Systems, Mobile Networks

Teaching Experience

Introduction to Machine Learning, CS233 at EPFL in Fall 2019, Fall 2020, Fall 2021
Machine Learning, CS433 at EPFL in Fall 2018

ML Tools and Algorithms

Linear Regression, Logistic Regression, SVM and Kernel-SVM, Neural Networks, Perceptron, PCA, kMeans, kNN, Boosting, Optimizers, Regularizations, Cost Functions, Activation Functions, Architectures (ResNet, Transformer, LSTM, FasterRCNN, etc.), Autoencoder, VAE, GAN, Attention Models (self-attention), Adversarial Training, Distillation.

Achievements

EDIC PhD Fellowship (2017) to pursue first year of doctoral studies at EPFL
Mitacs Globalink Scholarship to participate in summer internship at University of Alberta
University of Queensland Summer Research Scholarship to conduct research at CAI
MCM Scholarship for 4 years (2010-14) for excellent academic performance at IIT Kharagpur

References

- Dr. Mathieu Salzmann. Senior Researcher, CVLab, EPFL **email:** mathieu.salzmann@epfl.ch
- Prof. Pascal Fua. Professor, Computer Science Department, EPFL. **email:** pascal.fua@epfl.ch