

## Interests

Computer Vision, Machine Learning and Deep Learning

## Education

**Ecole Polytechnique Fédérale de Lausanne (EPFL)**

**Sep 2017 - Aug 2022**

Ph.D. in Computer Science

*Advisors: Dr. Mathieu Salzmann and Prof. Pascal Fua*

**Title: Understanding Deep Neural Networks using Adversarial Attacks**

My thesis focuses on the strengths and weaknesses of deep neural networks in safety-critical applications. It explores the topics of interpretable models, transfer-based black-box attacks, attack detection, adversarial defenses, anomaly detection, and disentangled representations.

**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

## Work Experience

**Samsung R&D Institute**, Bangalore

**Sep 2015 - July 2017**

*TL: Dr. Shankar Venkatesan, Advanced Technology Lab*

Prototyped a joint reflection-removal and super-resolution of a video sequence.

**University of Alberta**, Edmonton

**May 2014 - July 2014**

*Under: Prof. Nilanjan Ray, Computing Science Department*

Evaluated large scale image retrieval methods using product quantization of sub-codebooks.

**University of Queensland**, Australia

**Nov 2013 - Jan 2014**

*Under: Prof. Jeffrey Harmer, Center for Advanced Imaging Institute*

Developed an exponentially decaying non-uniform sampling scheme to shorten acquisition time in spectroscopy experiments.

**Philips Research Asia**, Bangalore

**May 2013 - July 2013**

*Under: Dr. Shankar M Venkatesan*

Implemented a part-based human detection model using Adaboost of weak SVM classifiers.

## Awards and Honours

**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

Department **Rank 3** among Masters degree students, EE Department, IIT Kharagpur

Secured All India Rank of **1695** in AIEEE 2010 out of 1,118,000 applicants

## Publications And Preprints

1. **Understanding Pose and Appearance Disentanglement in 3D Human Pose Estimation**  
Krishna Kanth Nakka and Mathieu Salzmann,  
*Under review*
2. **Learning Transferable Adversarial Perturbations**  
Krishna Kanth Nakka and Mathieu Salzmann,  
*Neural Information and Processing Systems, NeurIPS 2021*
3. **Universal, Transferable Adversarial Attacks for Visual Object Trackers**  
Krishna Kanth Nakka and Mathieu Salzmann,  
*Under review*
4. **Towards Robust Fine-grained Recognition by Maximal Separation of Discriminative Features**  
Krishna Kanth Nakka and Mathieu Salzmann,  
*Asian Conference on Computer Vision (ACCV), 2020.*
5. **Indirect Local Attacks for Context-aware Semantic Segmentation Networks**  
Krishna Kanth Nakka and Mathieu Salzmann,  
*European Conference on Computer Vision (ECCV) Spotlight 2020. (Top 5%)*
6. **Detecting the Unexpected via Image Resynthesis**  
Krzysztof Lis, Krishna Kanth Nakka, Pascal Fua, Mathieu Salzmann,  
*International Conference on Computer Vision (ICCV), 2019.*
7. **Interpretable BoW Networks for Adversarial Example Detection**  
Krishna Kanth Nakka and Mathieu Salzmann,  
*Explainable and Interpretable AI workshop, ICCV 2019.*
8. **Deep Attentional Structured Representation Learning for Visual Recognition**  
Krishna Kanth Nakka and Mathieu Salzmann,  
*British Media Vision Conference (BMVC), 2018.*
9. **Deep learning based fence segmentation and removal from an image using a video sequence**  
Jonna S, Nakka KK, Sahay RR,  
*International Workshop on Video Segmentation, ECCV 2016. Oral.*
10. **Detection and removal of fence occlusions in an image using a video of the static/dynamic scene**  
Jonna S, Nakka KK, Khasare VS, Sahay RR, Kankanhalli MS,  
*Journal of Optical Society of America (JOSA) A. 2016.*
11. **My camera can see through fences: A deep learning approach for image de-fencing**  
Jonna S, Nakka KK, Sahay RR,  
*Asian Conference on Pattern Recognition ACPR, 2015.*
12. **Towards an Automated Image De-fencing Algorithm Using Sparsity**  
Jonna S, Nakka KK, Sahay RR,  
*International Conference on Computer Vision Theory and Applications, VISAPP 2015.*

13. **3D-to-2D mapping for user interactive segmentation of human leg muscles from MRI data**  
Ray N, Mukherjee S, Nakka KK, Acton ST, Blanker SS,  
*Signal and Information Processing, GlobalSIP 2014.*
14. **Non-uniform sampling in EPR: optimizing data acquisition for Hyscore spectroscopy**  
Nakka KK, YA Tesiram, IM Brereton, M Mobli and JR Harmer,  
*Physical Chemistry Chemical Physics, 2014.*

## **Skills**

- Languages: Proficient in Python. Familiar with C/C++
- Softwares: PyTorch, Tensorflow, Caffe

## **References**

- Dr. Mathieu Salzmann. email: mathieu.salzmann@epfl.ch
- Prof. Pascal Fua. email: pascal.fua@epfl.ch