Dr. Ing. Philipp Benz

Room 212, N1, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
phibenz@gmail.com ◇ Website ◇ Google Scholar ◇ LinkedIn ◇ Github

Summary

I am a computer vision and machine learning researcher, with a focus on robust and reliable machine learning. My goal is to build human-like, robust visual perception systems to be deployed in real-world applications. I previously published papers in top-tier conferences such as ICCV, CVPR, NeurIPS, and AAAI and am experienced in various deep learning frameworks.

Education

Ph.D., Electrical Engineering **Mar. 2017 — Aug. 2021**
Korea Advanced Institute of Science and Technology (KAIST), Robotics and Computer Vision Lab (RCV), Republic of Korea
- Advisor: Prof. In So Kweon
- Thesis: A Study on Multiple Aspects of Deep Classifier Robustness

Diploma, Mechanical Engineering **Feb. 2010 — Feb. 2017**
Technical University Kaiserslautern, Chair of mechatronics in mechanical and automotive engineering (MEC), Germany
- Advisor: Prof. Naim Bajcinca
- Thesis: Application and Examination of a Deep Q-learning Algorithm to a Table Tennis Simulation

Awards & Achievements

Outstanding Paper Award **Jun. 2021**
Robustness Comparison of Vision Transformer and MLP-Mixer to CNNs, **CVPR AML-CV**

Top 10 in CVPR-2021 AI Challenge: Unrestricted Adversarial Attacks on ImageNet **Mar. 2021**
Team leader of *AI_Wizzards* placed 9 out of 1558 teams

Qualcomm Innovation Fellowship Korea Award **Dec. 2020**
Understanding Adversarial Examples from the Mutual Influence of Images and Perturbations

Best Demo Presentation Award **Feb. 2020**
Robust Manipulation by Visual Learning, International Workshop on Frontiers of Computer Vision (**IW-FCV**)

Projects

2D/3D visual recognition algorithms for robot manipulation [Video] **2017 — 2021**
- Project: Development of core technology for advanced locomotion/manipulation based on high-speed/power robot platform and robot intelligence, funded by the Ministry of Trade, Industry and Energy, Korea.
- Task: Design and development of 2D/3D object detection algorithms based on an RGB-D sensor as well as the design and generation of a custom dataset for the task.
- Advisors: Prof. Jun-Ho Oh and Prof. In So Kweon

Publications

International Conferences † indicates equal contribution

[1] **Philipp Benz**†, Chaoning Zhang†, In So Kweon, **"Batch Normalization Increases Adversarial Vulnerability and Decreases Adversarial Transferability: A feature perspective"**, *IEEE International Conference on Computer Vision* (**ICCV**), Oct. 2021.

[2] Chaoning Zhang†, **Philipp Benz**, Adil Karjauv, In So Kweon, **"Revisiting Universal Attack against Deep Classifiers"**, *IEEE International Conference on Computer Vision* (**ICCV**), Oct. 2021.

[3] **Philipp Benz**†, Chaoning Zhang†, Adil Karjauv, In So Kweon, **"Universal Adversarial Training with Class-Wise Perturbations"**, *IEEE International Conference on Multimedia and Expo* (**ICME**), Jul. 2021.

[4] Chaoning Zhang†, **Philipp Benz**†, Adil Karjauv, In So Kweon, **"A Survey on Universal Adversarial Attack"**, *International Joint Conference on Artificial Intelligence Survey Track* (**IJCAI**), Aug. 2021.

[5] Chaoning Zhang†, **Philipp Benz**†, Adil Karjauv, In So Kweon, **"Universal Adversarial Perturbations Through the Lens of Deep Steganography: Towards a Fourier Perspective"**, *AAAI Conference on Artificial Intelligence* (**AAAI**), Feb. 2021.

[6] **Philipp Benz**†, Chaoning Zhang†, Adil Karjauv, In So Kweon, **"Revisiting Batch Normalization for Improving Corruption Robustness"**, *IEEE Winter Conference on Applications of Computer Vision* (**WACV**), Jan. 2021.

[7] Chaoning Zhang†, **Philipp Benz**†, Dawit Mureja, Seokju Lee, Junsik Kim, Francois Rameau, Jean-Charles Bazin, In So Kweon, **"ResNet or DenseNet: Introducing Shortcuts to ResNet"**, *IEEE Winter Conference on Applications of Computer Vision* (**WACV**), Jan. 2021.

[8] Chaoning Zhang†, **Philipp Benz**†, Adil Karjauv, Geng Sun, In So Kweon, **"UDH: Universal Deep Hiding for Steganography, Watermarking, and Light Field Messaging"**, *Conference on Neural Information Processing Systems* (**NeurIPS**), Dec. 2020.

[9] **Philipp Benz**†, Chaoning Zhang†, Adil Karjauv, In So Kweon, **"Double Targeted Universal Adversarial Perturbations"**, *Asian Conference on Computer Vision* (**ACCV**), Dec. 2020.

[10] Chaoning Zhang†, **Philipp Benz**†, Tooba Imtiaz, In So Kweon, **"Understanding Adversarial Examples from the Mutual Influence of Images and Perturbations"**, *IEEE International Conference on Computer Vision and Pattern Recognition* (**CVPR**), Jun. 2020.

[11] Chaoning Zhang†, **Philipp Benz**†, Tooba Imtiaz, In So Kweon, **"CD-UAP: Class Discriminative Universal Adversarial Perturbations"**, *AAAI Conference on Artificial Intelligence* (**AAAI**), Feb. 2020.

[12] Ho-Deok Jang, Sanghyun Woo, **Philipp Benz**, Jinsun Park, In So Kweon, "Propose-and-Attend Single Shot Detector", *IEEE Winter Conference on Applications of Computer Vision* (**WACV**), 2020.

[13] Moonyoung Lee, Yujin Heo, Jinyong Park, Hyun-Dae Yang, Ho-Deok Jang, **Philipp Benz**, Hyunsub Park, In So Kweon, Jun-Ho Oh, **"Fast perception, planning, and execution for a robotic butler: Wheeled humanoid m-hubo"**, *IEEE/RSJ International Conference on Intelligent Robots and Systems* (**IROS**), 2019.

[14] Chaoning Zhang, Francois Rameau, Seokju Lee, Junsik Kim, **Philipp Benz**, Dawit Mureja, Jean-Charles Bazin, In So Kweon, **"Revisiting Residual Networks with Nonlinear Shortcuts"**, *The British Machine Vision Conference* (**BMVC**), Sep. 2019.

Selected International Workshops

[1] **Philipp Benz**†, Chaoning Zhang†, Soomin Ham†, Adil Karjauv, In So Kweon, **"Robustness Comparison of Vision Transformer and MLP-Mixer to CNNs"**, *CVPR Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems*, **Outstanding Paper Award**, Jun. 2021.

[2] **Philipp Benz**†, Chaoning Zhang†, Adil Karjauv, In So Kweon, **"Towards Simple Yet Effective Transferable Targeted Adversarial Attacks"**, *ICLR Workshop on RobustML*, May 2021.

[3] **Philipp Benz**†, Chaoning Zhang†, Adil Karjauv, In So Kweon, **"Robustness May Be at Odds with Fairness: An Empirical Study on Class-wise Accuracy"**, *NeurIPS Pre-registration Workshop*, Dec. 2020.

[4] **Philipp Benz**†, Chaoning Zhang†, Tooba Imtiaz, In So Kweon, **"Data from Model"**, *CVPR Workshop on Adversarial Machine Learning in Computer Vision*, Jun. 2020.

Talks

- **Adversarial Transferability and Beyond** - 2D3D.AI [Video] Jul. 2021
- **Adversarial Machine Learning and Beyond** - 2D3D.AI [Video] Dec. 2020

Reviewer & Program Committee

- IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2020 - 2021
- IEEE International Conference on Computer Vision (ICCV), 2021
- Conference on Neural Information Processing Systems (NeurIPS), 2021
- AAAI Conference on Artificial Intelligence (AAAI), 2021
- IEEE Winter Conference on Applications of Computer Vision (WACV), 2021
- Transactions on Information Forensics Security (TIFS), 2021

Technical Skills

Programming/Scripting	Python, Bash, Matlab, C++
Libraries	Pytorch, Keras, Tensorflow, Scikit-learn, Pandas, OpenCV, Matplotlib, Seaborn, ROS
Etc.	Linux, Docker, Microsoft Office, LaTeX, Vim

Language

German	Native proficiency
English	Full Professional Proficiency
Korean	Beginner

Hobbies

- Reading, Movies, Brazilian Jiu Jitsu, Exercise, Guitar