Hunmin Yang (양훈민)

Email: hmyang@kaist.ac.kr
Personal Website
Mobile: +82-10-8447-1009

Senior AI Researcher @ ADD
PhD Candidate @ KAIST

Yuseong P.O. Box 35, Daejeon 34186, Republic of Korea
291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

Research Interest

- **Trustworthy Machine Learning & Computer Vision**
  - My research focuses on developing safe and reliable artificial intelligence to enable safe model deployment in real-world applications. To achieve this, I work at the intersection of machine learning and computer vision. My current interests include transferable adversarial attacks, domain generalization, and representation learning.

Experience

- **Agency for Defense Development (ADD)** — Daejeon, Korea
  Senior AI Researcher — *Jan 2020 - Present*
  - **D-CAM**: Adversarial attack & defense techniques for robust AI
  - **D-GEN**: Synthetic data generation framework for training AI
- **Agency for Defense Development (ADD)** — Daejeon, Korea
  AI Researcher — *May 2017 - Dec 2019*
  - **D-NET**: Large-scale AI inference platform with Hadoop-Spark
- **Agency for Defense Development (ADD)** — Daejeon, Korea
  Specialized Research Staff (Military Service) — *Feb 2014 - May 2017*

Education

- **Korea Advance Institute of Science and Technology (KAIST)** — Daejeon, Korea
  PhD in Mechanical Engineering — *Sep 2021 - Present*
  - Research Area: Machine Learning & Computer Vision
  - Advisor: Kuk-Jin Yoon
- **Korea Advance Institute of Science and Technology (KAIST)** — Daejeon, Korea
  MS in Mechanical Engineering — *Feb 2012 - Feb 2014*
  - Research Area: 3D Sound Perception
  - Advisor: Youngjin Park
- **Royal Melbourne Institute of Technology (RMIT)** — Melbourne, Australia
  Exchange Student (High Distinction) — *Feb 2011 - Aug 2011*
- **Korea Advance Institute of Science and Technology (KAIST)** — Daejeon, Korea
  BS in Mechanical Engineering (Magna Cum Laude) — *Feb 2007 - Feb 2012*

Publications

- **Hunmin Yang**, Jongoh Jeong, Kuk-Jin Yoon. Prompt-Driven Contrastive Learning for Transferable Adversarial Attacks. In *European Conference on Computer Vision (ECCV)*, 2024. (**Oral, top 2.3%**)

- Junhyeong Cho, Kim Youwang, **Hunmin Yang**, Tae-Hyun Oh. Object-Centric Domain Randomization for 3D Shape Reconstruction in the Wild. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshop on Foundation Models*, 2024.

- **Hunmin Yang***, Jongoh Jeong*, Kuk-Jin Yoon. FACL-Attack: Frequency-Aware Contrastive Learning for Transferable Adversarial Attacks. In *Association for the Advancement of Artificial Intelligence (AAAI)*, 2024.

- Junhyeong Cho, Gilhyun Nam, Sungyeon Kim, **Hunmin Yang**, Suha Kwak. PromptStyler: Prompt-driven Style Generation for Source-free Domain Generalization. In *IEEE/CVF International Conference on Computer Vision (ICCV)*, 2023.

- Naufal Suryanto, Yongsu Kim, Harashta Tatimma Larasati, Hyoeun Kang, Thi-Thu-Huong Le, Yoonyoung Hong, **Hunmin Yang**, Se-Yoon Oh, Howon Kim. ACTIVE: Towards Highly Transferable 3D Physical Camouflage for Universal and Robust Vehicle Evasion. In *IEEE/CVF International Conference on Computer Vision (ICCV)*, 2023.

- **Hunmin Yang**, Se-Yoon Oh, Junhyeong Jo. Synthetic Image Generation for Deep Neural Networks. In *NVIDIA GPU Technology Conference (GTC)*, 2023. (**Spotlight**)
- Naufal Suryanto, Yongsu Kim, Hyoeun Kang, Harashta Tatimma Larasati, Youngyeo Yun, Thi-Thu-Huong Le, **Hunmin Yang**, Se-Yoon Oh, Howon Kim. DTA: Physical Camouflage Attacks using Differentiable Transformation Network. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2022.
- Jeonghun Kim, Kyungmin Lee, Hyeongkeun Lee, **Hunmin Yang**, Se-Yoon Oh. Camouflaged Adversarial Attack on Object Detector . In *21th International Conference on Control, Automation and Systems (ICCAS)*, 2021.
- **Hunmin Yang**, Se-Yoon Oh, Taewon Kim, Ki-Jung Ryu. D-GEN: A Deep Learning Data Generation Framework For Artificial Intelligence. In *NVIDIA GPU Technology Conference (GTC)*, 2020.
- Kyungmin Lee, **Hunmin Yang**, Se-Yoon Oh. Adversarial Training on Joint Energy Based Model for Robust Classification and Out-of-Distribution Detection. In *20th International Conference on Control, Automation and Systems (ICCAS)*, 2020.
- Eunchong Kim, Kanghyun Park, **Hunmin Yang**, Se-Yoon Oh. Training Deep Neural Networks with Synthetic Data for Off-Road Vehicle Detection. In *20th International Conference on Control, Automation and Systems (ICCAS)*, 2020.
- Hyeongkeun Lee, Kyungmin Lee, **Hunmin Yang**, Se-Yoon Oh. Applying FastPhotoStyle to Synthetic Data for Military Vehicle Detection. In *20th International Conference on Control, Automation and Systems (ICCAS)*, 2020.
- Kanghyun Park, Hyeongkeun Lee, **Hunmin Yang**, Se-Yoon Oh. Improving Instance Segmentation using Synthetic Data with Artificial Distractors. In *20th International Conference on Control, Automation and Systems (ICCAS)*, 2020.
- **Hunmin Yang**, Se-Yoon Oh, Ki-Jung Ryu. Accelerating Distributed Deep Learning Inference on multi-GPU with Hadoop-Spark. In *NVIDIA GPU Technology Conference (GTC)*, 2019. (**Oral**)
- **Hunmin Yang**, Se-Yoon Oh, Ki-Jung Ryu. Scalable Distributed Deep Learning Inference on Multi-GPU with Hadoop-Spark. In *NVIDIA GPU Technology Conference (GTC)*, 2019.
- Se-Yoon Oh, **Hunmin Yang**, Ki-Jung Ryu. Optimal Distributed Inference on Multi-GPU Processing System. In *NVIDIA GPU Technology Conference (GTC)*, 2019.
- Se-Yoon Oh, **Hunmin Yang**, Ki-Jung Ryu. Optimal Experimental Design Approach for Machine Learning Process. In *17th International Conference on Control, Automation and Systems (ICCAS)*, 2017.

Patents

Machine Learning & Synthetic Image Generation

- **Hunmin Yang**, Se-Yoon Oh. Training data generation method and apparatus for deep learning model. kr 10-2613781, 2023.
- **Hunmin Yang**, Ki-Jung Ryu, Se-Yoon Oh. Apparatus and method for deep learning based on mixing virtual and real data. kr 10-2198088, 2020.
- **Hunmin Yang**, Ki-Jung Ryu, Se-Yoon Oh. Apparatus and method for learning machine learning models based on virtual data. kr 10-2086351, 2020.
- **Hunmin Yang**, Se-Yoon Oh, Seongbaek Jo. Apparatus and method for enhancing learning capability for machine learning. kr 10-2053202, 2019.
- **Hunmin Yang**, Ki-Jung Ryu, Se-Yoon Oh. Method and apparatus of improving self-supervised learning performance utilizing synthesized data. kr 10-2032519, 2019.
- **Hunmin Yang**, Ki-Jung Ryu, Se-Yoon Oh. Method and Apparatus of adding artificial object for improving performance in detecting object. kr 10-1972095, 2019.
- **Hunmin Yang**, Se-Yoon Oh, Seongbaek Jo. Apparatus and method for generating learning image in game engine-based machine learning. kr 10-1947650, 2019.

AI Security & Adversarial Robustness

- Se-Yoon Oh, **Hunmin Yang**, Hyeongkeun Lee, Kyungmin Lee, Jeonghun Kim. Method and Apparatus for optimizing adversarial patch, computer-readable storage medium and computer program. kr 10-2445215, 2022.
- Hyeongkeun Lee, Jeonghun Kim, Kyungmin Lee, **Hunmin Yang**, Se-Yoon Oh. Method and Apparatus for optimizing adversarial patch, computer-readable storage medium and computer program. kr 10-2414146, 2022.

- Jeonghun Kim, Se-Yoon Oh, Hyeongkeun Lee, Kyungmin Lee, **Hunmin Yang**. Apparatus and method for optimizing adversarial patch based on natural pattern for stealthiness against human vision system. kr 10-2380154, 2022.
- Hyeongkeun Lee, **Hunmin Yang**, Jeonghun Kim, Kyungmin Lee, Se-Yoon Oh. Method, apparatus computer-readable storage medium and computer program for determining adversarial patch position. kr 10-2360070, 2022.

Big Data & Database

- **Hunmin Yang**, Ki-Jung Ryu, Se-Yoon Oh. Method and apparatus of building NoSQL database for signal processing. kr 10-2002360, 2019.
- **Hunmin Yang**, Ki-Jung Ryu, Se-Yoon Oh. Method and apparatus of building inverse index DB for high speed searching of moving picture object. kr 10-2014267, 2019.

Honors and Awards

- **Selected as Oral Presentation (top 2.3%)** Oct 2024
  In European Conference on Computer Vision (ECCV)
  - Prompt-Driven Contrastive Learning for Transferable Adversarial Attacks
- **National Grant for Defense Research and Development** Dec 2021
  From the Chief Director of DAPA
  - Synthetic Data Generation for Defense AI
- **Defense Science Award** Aug 2019
  From the Chief Research Director of ADD
  - Improving Distributed Multi-GPU Computing for Large-scale Video Analytics
- **High Achievement Award** Aug 2018
  From the Chief Research Director of ADD
  - Big Data Platform Development and Synthetic Data Generation
- **Excellent Paper Award** Mar 2013
  From the Korea Society for Noise and Vibration Engineering (KSNVE)
  - Sweet Spot Analysis of Linear Array System by Geometrical Approach
- **Scholarship for Academic Excellence** Jun 2007
  From the Korea Human Resource Development Scholarship Association
  - Outstanding Academic Performance
- **Scholarship for Academic Excellence** 2007-2014
  From the Korean Government
  - Tuition free for all semesters in KAIST (BS & MS)

Professional Services

- **Academic Reviewer**
  - IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)
  - IEEE/CVF International Conference on Computer Vision (ICCV)
  - European Conference on Computer Vision (ECCV)
- **Technology Transfer**
  - Synthetic data generation for training AI models → SI Analytics, Jcorp System, JEIOS
  - Physical adversarial camouflage generation for attacking AI models → SmartM2M
  - Big data platform for large-scale AI model inference → XIIlab