Jongheon Jeong

Ph.D. Student @ ALIN Lab in KAIST

KAIST N1-917, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, South Korea

jongheonj@kaist.ac.kr | jh-jeong.github.io | jh-jeong | Jongheon Jeong

Research Interests

I am broadly interested in discovering (if exist) simple priors that would close the gap between neural network and human perception. Many topics are related, particularly on (but not limited to) robustness (or generalization) against distribution shifts, e.g., adversarial examples, natural corruptions, out-of-distribution, and label shifts, to name a few. Ultimately, my research aims to understand why neural networks behave so differently from our brain, and how our brain makes such reliable yet efficient inferences.

Education

Korea Advanced Institute of Science and Technology (KAIST) *Daejeon, South Korea*

M.Sc./Ph.D. in Electrical Engineering *Aug 2017 - Present*

- **Advisor**: Jinwoo Shin
- **Expected graduation date**: August 2023 (or earlier)

Korea Advanced Institute of Science and Technology (KAIST) *Daejeon, South Korea*

B.Sc. in Mathematics and Computer Science (Double major) *Mar 2012 - Aug 2017*

Work Experience

Amazon Web Services (AWS AI) *Bellevue, WA, USA*

Applied Scientist II Intern (Mentor: Yang Zou, Dongqing Zhang, Taewan Kim / Manager: Onkar Dabeer) *Sep 2022 - Dec 2022*

- **Project**: Language-driven zero-/few-shot industrial anomaly detection and localization
- The project outcome [P2] is submitted to CVPR 2023

Amazon Web Services (AWS AI) *Seattle, WA, USA*

Applied Scientist I Intern (Mentor: Yang Zou, Dongqing Zhang / Manager: Onkar Dabeer) *Aug 2021 - Nov 2021*

- **Project**: Representation learning for industrial anomaly detection and localization
- The project outcome [C8] was presented at ECCV 2022 (Tel Aviv, Israel)

XBRAIN Inc. *Seoul, South Korea*

Machine Learning Engineer *Jan 2016 - Feb 2017*

- Built a fully automated pipeline for a systematic exploration of various machine learning algorithm configurations
- Developed a faster AutoML method based on Mondrian forest regression and the Hyperband algorithm [W1]
- Hosted a regular internal seminar on the recent progresses in machine learning for the team members

Publications

Conference / Workshop (*: equal contribution)

[C13/W] Enhancing Multiple Reliability Measures via Nuisance-extended Information Bottleneck *Vancouver, Canada*

Jongheon Jeong, Sihyun Yu, Hankook Lee, Jinwoo Shin *2023*

- IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2023
- A preliminary version appeared at ECCV OOD-CV Workshop 2022
- `tl;dr:` Modeling nuisance information properly can improve out-of-distribution generalization.

[C12] WinCLIP: Zero-/Few-Shot Anomaly Classification and Segmentation *Vancouver, Canada*

Jongheon Jeong*, Yang Zou*, Taewan Kim, Dongqing Zhang, Avinash Ravichandran, Onkar Dabeer *2023*

- IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2023
- `tl;dr:` State-of-the-art zero-shot and few-shot anomaly recognition via CLIP.

[C11] Guiding Energy-based Models via Contrastive Latent Variables *Kigali, Rwanda*

Hankook Lee, **Jongheon Jeong**, Sejun Park, Jinwoo Shin *2023*

- International Conference on Learning Representations (ICLR) 2023 (**Spotlight presentation**)
- A preliminary version appeared at NeurIPS Workshop on Self-Supervised Learning 2022 (**Oral presentation**)
- `tl;dr:` A simple yet effective framework for improving EBMs via contrastive representation learning.

[C10/W] Confidence-aware Training of Smoothed Classifiers for Certified Robustness *Washington, D.C., USA*

Jongheon Jeong*, Seojin Kim*, Jinwoo Shin *2023*

- AAAI Conference on Artificial Intelligence (AAAI) 2023 (**Oral presentation**)
- A preliminary version appeared at ECCV AROW Workshop 2022
- `tl;dr:` A more sensible training method for randomized smoothing by incorporating a sample-wise control of target robustness.

[C9] NOTE: Robust Continual Test-time Adaptation Against Temporal Correlation *New Orleans, LA, USA*

Taesik Gong, **Jongheon Jeong**, Taewon Kim, Yewon Kim, Jinwoo Shin, Sung-Ju Lee *2022*

- Neural Information Processing Systems (NeurIPS) 2022
- `tl;dr:` The first test-time adaptation method concerning temporally correlated, non-i.i.d. streams.

[W5] OpenCoS: Contrastive Semi-supervised Learning for Handling Open-set Unlabeled Data *Tel Aviv, Israel*

Jongjin Park*, Sukmin Yun*, **Jongheon Jeong**, Jinwoo Shin *2022*

- ECCV Workshop on Learning from Limited and Imperfect Data (L2ID) 2022
- `tl;dr:` A contrastive learning based framework to enhance semi-SL methods to also utilize "out-of-class" unlabeled samples.

[C8] SPot-the-Difference Self-Supervised Pre-training for Anomaly Detection and Segmentation *Tel Aviv, Israel*

Yang Zou, **Jongheon Jeong**, Latha Pemula, Dongqing Zhang, Onkar Dabeer *2022*

- European Conference on Computer Vision (ECCV) 2022
- `tl;dr:` (a) VisA - a larger-scale dataset for industrial anomaly recognition, and (b) a novel pre-training method targeting on it.

[C7/W] SmoothMix: Training Confidence-calibrated Smoothed Classifiers for Certified Robustness *Online*

Jongheon Jeong, Sejun Park, Minkyu Kim, Heung-Chang Lee, Doguk Kim, Jinwoo Shin *2021*

- Neural Information Processing Systems (NeurIPS) 2021
- `tl;dr:` Over-confident nearby inputs cause vulnerability in randomized smoothing, and regularizing them improves robustness.

[C6/W] Consistency Regularization for Adversarial Robustness *Online*

Jihoon Tack, Sihyun Yu, **Jongheon Jeong**, Minseon Kim, Sung Ju Hwang, Jinwoo Shin *2021*

- AAAI Conference on Artificial Intelligence (AAAI) 2022
- ICML Workshop on Adversarial Machine Learning (AdvML) 2021 (**Oral presentation**)
- Best Paper Award, Korean Artificial Intelligence Association 2021
- `tl;dr:` Consistency regularization can also prevent robustness overfitting in adversarial training.

[C5] Training GANs with Stronger Augmentations via Contrastive Discriminator *Online*

Jongheon Jeong, Jinwoo Shin *2021*

- International Conference on Learning Representations (ICLR) 2021
- `tl;dr:` A contrastive representation learning, e.g., SimCLR, and GAN can benefit each other when they are jointly trained.

[C4/W] Consistency Regularization for Certified Robustness of Smoothed Classifiers *Online*

Jongheon Jeong, Jinwoo Shin *2020*

- Neural Information Processing Systems (NeurIPS) 2020
- ICML Workshop on Uncertainty & Robustness in Deep Learning (UDL) 2020
- **Qualcomm Innovation Fellowship Korea 2020**
- `tl;dr:` Consistency controls robustness in the world of randomized smoothing, like TRADES in adversarial training.

[C3] CSI: Novelty Detection via Contrastive Learning on Distributionally Shifted Instances *Online*

Jihoon Tack*, Sangwoo Mo*, **Jongheon Jeong**, Jinwoo Shin *2020*

- Neural Information Processing Systems (NeurIPS) 2020
- **Qualcomm Innovation Fellowship Korea 2020**
- `tl;dr:` Contrastive representations are good at detecting OODs, and contrasting also "OOD-like" augmentations further helps.

[C2] M2m: Imbalanced Classification via Major-to-minor Translation *Online*

Jaehyung Kim*, **Jongheon Jeong***, Jinwoo Shin *2020*

- IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2020
- `tl;dr:` Adversarial examples targeting Majority → minority can play as minorities to prevent overfitting from class-imbalance.

[C1] Training CNNs with Selective Allocation of Channels *Long Beach, CA, USA*

Jongheon Jeong, Jinwoo Shin *2019*

- International Conference on Machine Learning (ICML) 2019
- `tl;dr:` Any CNNs can become more efficient by "re-allocating" unnecessary channels to increase the kernel size.

[W1] AutoML Challenge: AutoML Framework Using Random Space Partitioning Optimizer *New York, NY, USA*

Jungtaek Kim, **Jongheon Jeong**, Seungjin Choi *2016*

- ICML Workshop on Automatic Machine Learning (AutoML) 2016

Honors & Awards

2021	**Finalist**, Qualcomm Innovation Fellowship Korea 2021	*Online*
2021	**Best Paper Award**, Korean Artificial Intelligence Association 2021	*Online*
2020	**Winner**, Qualcomm Innovation Fellowship Korea 2020	*Online*
2020	**Top reviewer award (10%)**, Neural Information Processing Systems (NeurIPS) 2020	*Online*
2019	**Travel award**, International Conference on Machine Learning (ICML) 2019	*Long Beach, CA, USA*
2016	**3rd place winner**, Automatic Machine Learning Challenge Final (AutoML5)	*New York, NY, USA*

Invited Talks

"Towards Threat-free Robust Training: From Adversarial to Natural Robustness"

2022 **Vector Institute**, Online

"Learning Robust Representations via Nuisance-extended Information Bottleneck"

2022 **ECCV Workshop on Out-of-distribution Generalization in Computer Vision (OOD-CV)**, Online

"Confidence-aware Training of Smoothed Classifiers for Certified Adversarial Robustness"

2022 **Center for Applied Research in Artificial Intelligence (CARAI)**, Daejeon, South Korea

"SPot-the-Difference Self-Supervised Pre-training for Anomaly Detection and Segmentation"

2022 **Korean Artificial Intelligence Association**, Jeju, South Korea

2021 **Amazon Web Services AI**, Seattle, WA, USA

"Consistency Regularization for Certified Robustness of Smoothed Classifiers"

2021 **Korean Conference on Computer Vision (KCCV)**, Online

"Training GANs with Stronger Augmentations via Contrastive Discriminator"

2021 **ICLR Social: ML in Korea**, Online

"Training CNNs with Selective Allocation of Channels"

2019 **Samsung AI Forum**, Seoul, South Korea

2019 **Korea Computer Congress (KCC)**, Jeju, South Korea

2019 **International Conference on Machine Learning (ICML)**, Long Beach, CA, USA

2018 **NAVER Labs**, Seongnam, South Korea

Professional Services

Conference reviewers

- Neural Information Processing Systems (NeurIPS)
  - **Top 10% Reviewers Award** (2020)
- International Conference on Learning Representations (ICLR)
- International Conference on Machine Learning (ICML)
  - **Expert reviewer** (2021)
- IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)
- AAAI Conference on Artificial Intelligence (AAAI)

Journal reviewers

- International Journal of Computer Vision (IJCV)
- Transactions on Machine Learning Research (TMLR)
- ACM Transactions on Modeling and Performance Evaluation of Computing Systems (ACM ToMPECS)

Teaching Experience

2020	**TA: "Visual Question Answering"**, Samsung DS AI Expert Program	*Yongin, South Korea*
2019	**TA: "Adversarial Examples and Explainable ML"**, SK Hynix ML Program	*Daejeon, South Korea*
2019	**TA: "Adversarial Attacks and Defenses"**, Samsung DS AI Expert Program	*Daejeon, South Korea*
2018	**TA: "Regression Analysis"**, Seongnam-KAIST AI Program	*Seongnam, South Korea*
2017/18	**TA: "Regression Analysis"**, KB-KAIST AI Program	*Seoul, South Korea*