Topic 1 Distributed/Federated Learning

❖ Communication-Efficient FL

- **[ICML’24]** Achieving Lossless Gradient Sparsification via Mapping to Alternative Space in Federated Learning
- **[NeurIPS’23]** EvoFed: Leveraging Evolutionary Strategies for Efficient and Privacy-Preserving Federated Learning

❖ Federated Domain Generalization

- **[NeurIPS’23]** StableFDG: Style and Attention Based Learning for Federated Domain Generalization

Topic 2 Robust AI against Domain Shifts/Attacks

❖ Robust AI against Adversarial Attacks

- **[NeurIPS’23]** NEO-KD: Knowledge-Distillation-Based Adversarial Training for Robust Multi-Exit Neural Networks
- **[NeurIPS’21]** Sageflow: Robust Federated Learning against Both Stragglers and Adversaries

❖ OOD Generalization/Calibration

- **[AAAI’24]** Consistency-Guided Temperature Scaling Using Style and Content Information for Out-of-Domain Calibration
- **[ICML’23]** Test-Time Style Shifting: Handling Arbitrary Styles in Domain Generalization

Topic 3 Resource-Efficient AI

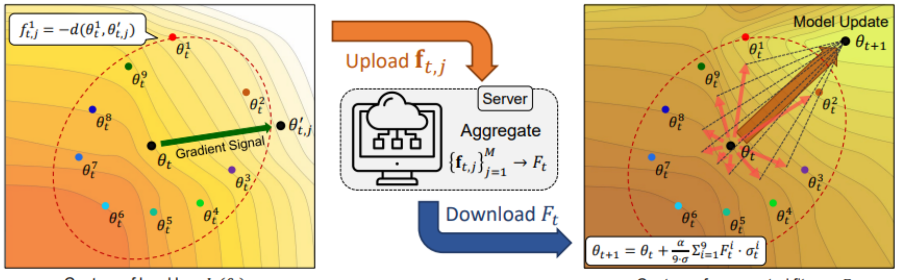
❖ Few-Shot/Round Learning

- **[ICLR’23]** Warping the Space: Weight Space Rotation for Class-Incremental Few-Shot Learning
- **[NeurIPS’21]** Few-Round Learning for Federated Learning

❖ Active Learning

- **[ICLR’23]** Active Learning for Object Detection with Evidential Deep Learning and Hierarchical Uncertainty Aggregation

Evolutionary Strategies for Communication-Efficient FL [NeurIPS'23]



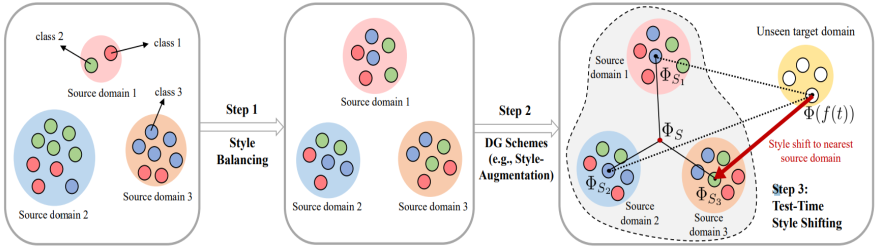
$f^1_{t,j} = -d(\theta^1_t, \theta'_{t,j})$
θ^1_t
θ^9_t
θ^2_t
$\theta'_{t,j}$
θ^8_t
Gradient Signal
θ_t
θ^7_t
θ^3_t
θ^6_t
θ^5_t
θ^4_t
Upload $\mathbf{f}_{t,j}$
Server
Aggregate
$\{\mathbf{f}_{t,j}\}_{j=1}^{M} \to F_t$
Download F_t
Model Update
θ_{t+1}
$\theta_{t+1} = \theta_t + \frac{\alpha}{9 \cdot \sigma}\Sigma_{i=1}^{9} F^i_t \cdot \sigma^i_t$

Contour of local loss $L_j(\theta_t)$

Contour of aggregated fitness F_t

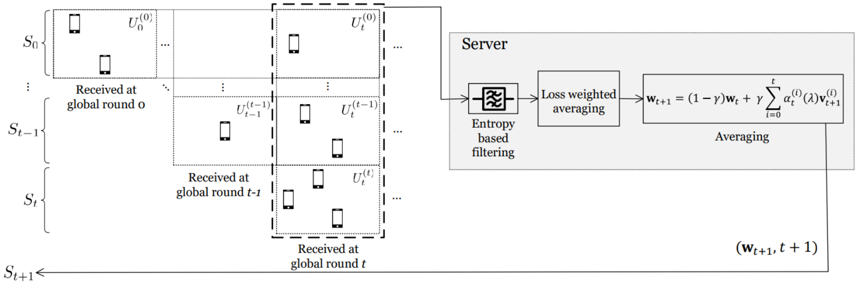
Efficient federated learning via the exchange of lightweight fitness score between devices sharing the same seed

Test-Time Style Shifting for Domain Generalization [ICML'23]



Style-balancing and test-time style shifting to handle arbitrary domains for domain generalization

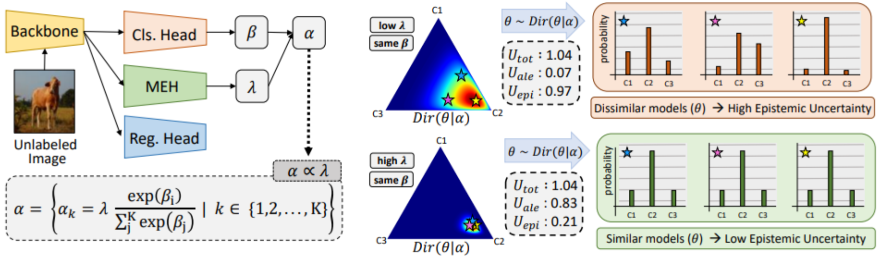
Robust FL against Stragglers and Adversarial Attacks [NeurIPS'21]



S_0
$U_0^{(0)}$
Received at global round 0
S_{t-1}
$U_{t-1}^{(t-1)}$
Received at global round t-1
S_t
$U_t^{(0)}$
$U_t^{(t-1)}$
$U_t^{(t)}$
Received at global round t
Server
Entropy based filtering
Loss weighted averaging
$\mathbf{w}_{t+1} = (1-\gamma)\mathbf{w}_t + \gamma \sum_{i=0}^{t} \alpha_t^{(i)}(\lambda)\mathbf{v}_{t+1}^{(i)}$
Averaging
$(\mathbf{w}_{t+1}, t+1)$
S_{t+1}

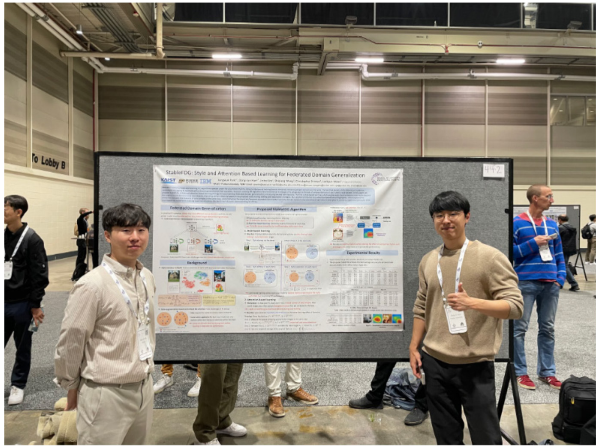
Entropy-based filtering and loss-weighted averaging against adversarial attacks in FL

Active Object Detection with Evidential Deep Learning [ICLR'23]



Box-wise and image-wise informativeness prediction using Bayeisan learning and hierarchical information aggregation

2024.05 Teacher's Day



2024.12 NeurIPS

ICML
Sessions
July 24, 2023
Start Time End Time Session Title Type Room
6:15 PM 8:00 PM Welcome Reception Reception First Floor Main Lobby
6:30 PM 6:45 PM EXPO Attendee Raffle Prize Give Away Reception Exhibit Hall 3
HAWAII CONVENTION CENTER

2023.07 ICML

2023.05 ICLR

We're looking for passionate students. If you have any interest, feel free to contact us! We are excited to have a wonderful time with you in MoonLab.

Contact: jmoon@kaist.edu

2023.01 Winter Workshop