CMU KAIST

IEEE BIG DATA 2023
15–18 December • Sorrento, Italy

Self-Supervision for Tackling Unsupervised Anomaly Detection: Pitfalls and Opportunities

Leman Akoglu (CMU)

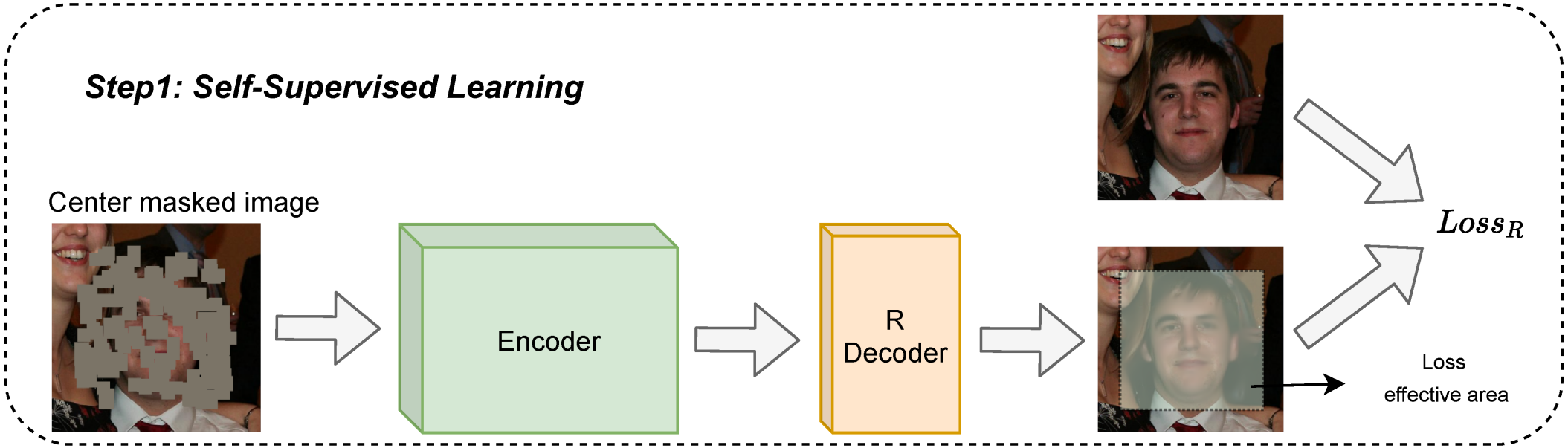
Jaemin Yoo (KAIST)

Outline

1. **Introduction**
2. Part 1: Choice of data augmentation
3. Part 2: Automatic HP selection for SSL
4. Part 3: GenAI and foundation models
5. Conclusion

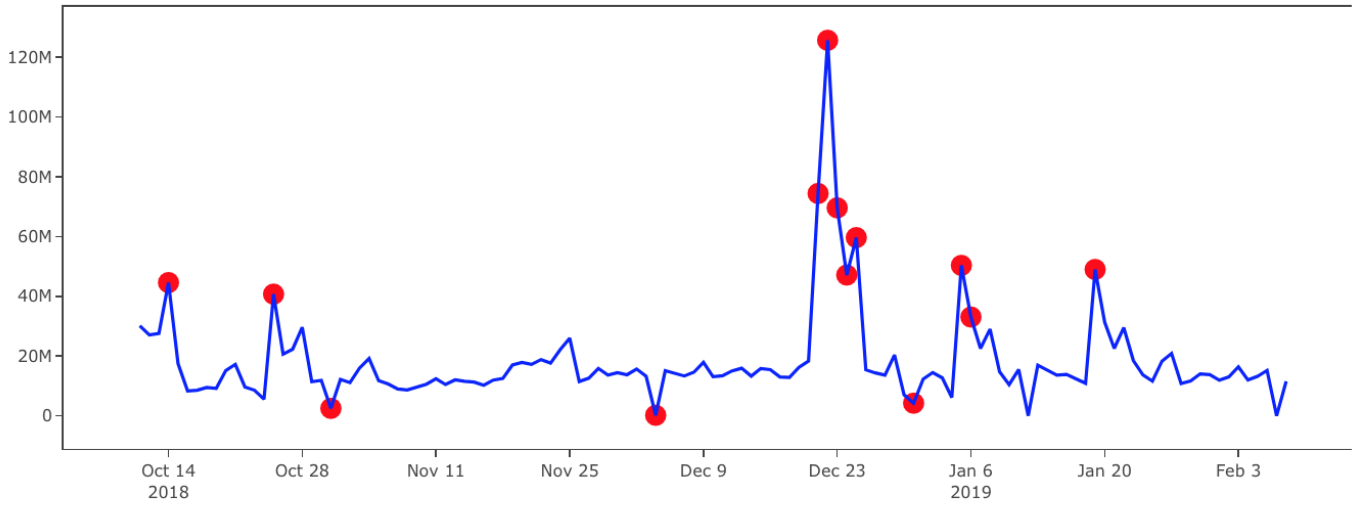
Self-supervised Learning

- **Self-supervised learning (SSL)** is a trending ML paradigm
  - Train a model from vast amounts of unlabeled data
  - Embodied in large language models like OpenAI's ChatGPT



Anomaly Detection

- **Anomaly detection (AD)** is a problem to detect anomalies
  - Basically a binary classification task (normal vs. abnormal)
- AD problems are mostly defined in the **unsupervised setup**
  - Since acquiring labeled anomalies is costly and often impossible



SSL for Unsupervised AD

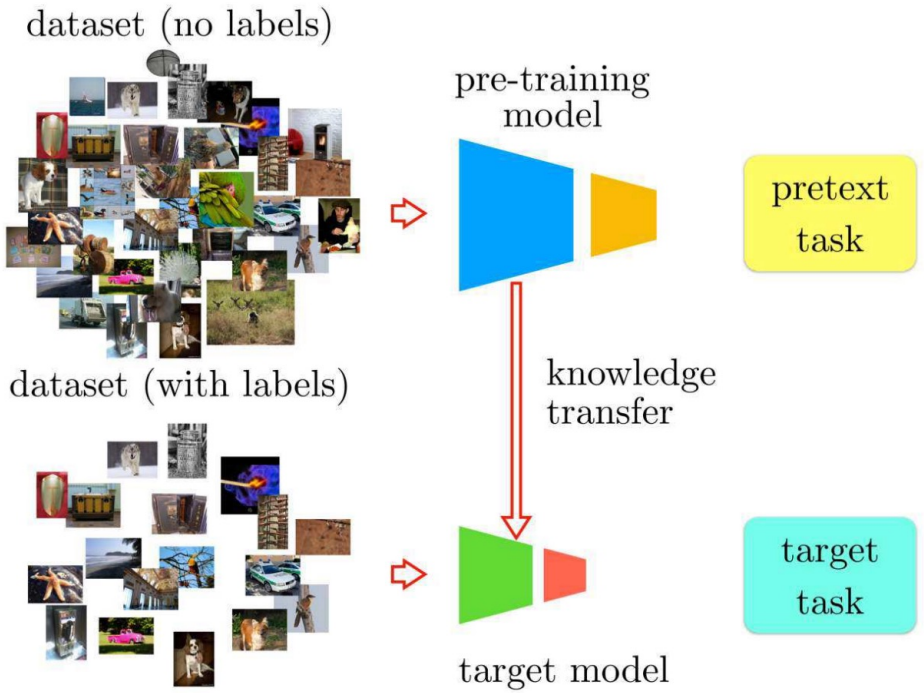
- SSL offers opportunities for many unsupervised AD tasks
- **(Traditional) unsupervised methods:**
  - Assume a **uniform prior** for the anomaly-generating distribution
  - Require a massive number of data to fill in the space
- **SSL for AD:**
  - Create a shift toward various **non-uniform** priors of the anomalies
  - Efficient and effective especially in high-dimensions (e.g., images)

Outline

1. Introduction
2. **Part 1: Choice of data augmentation**
3. Part 2: Automatic HP selection for SSL
4. Part 3: GenAI and foundation models
5. Conclusion

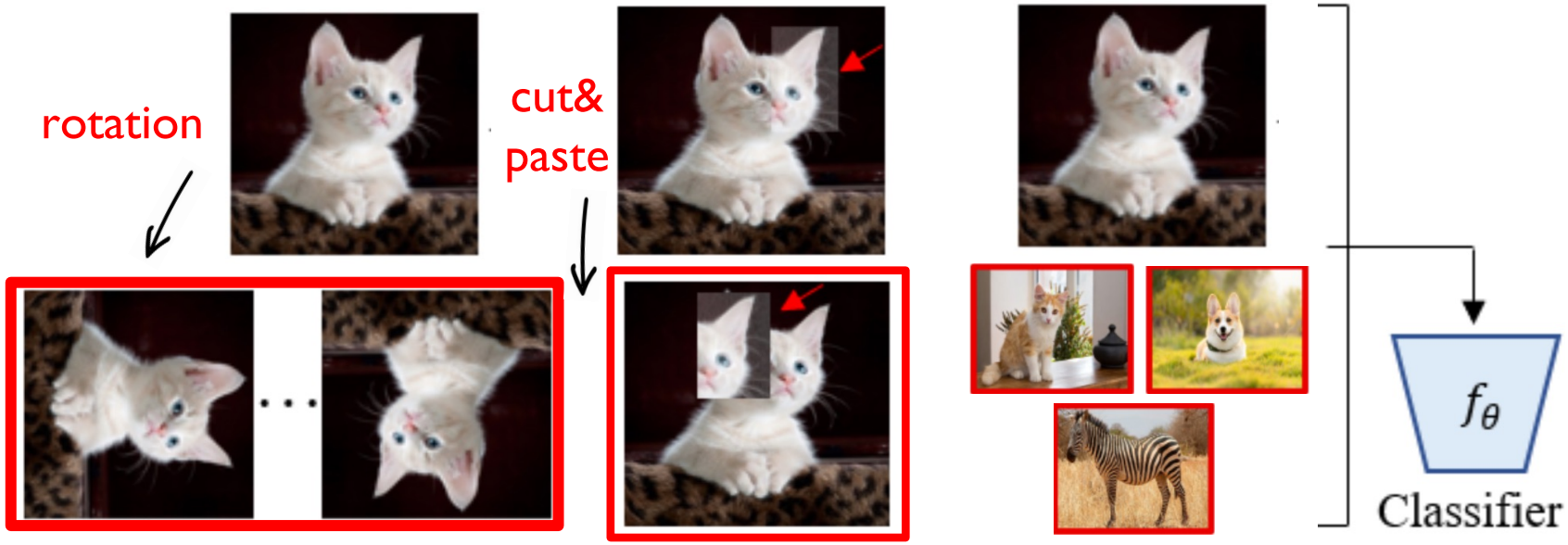
SSL in Supervised ML

- **SSL in (supervised) ML is for generalization**
  - SSL consists of **unlabeled pre-training** and **fine-tuning with labels**



No Fine-Tuning with Labels

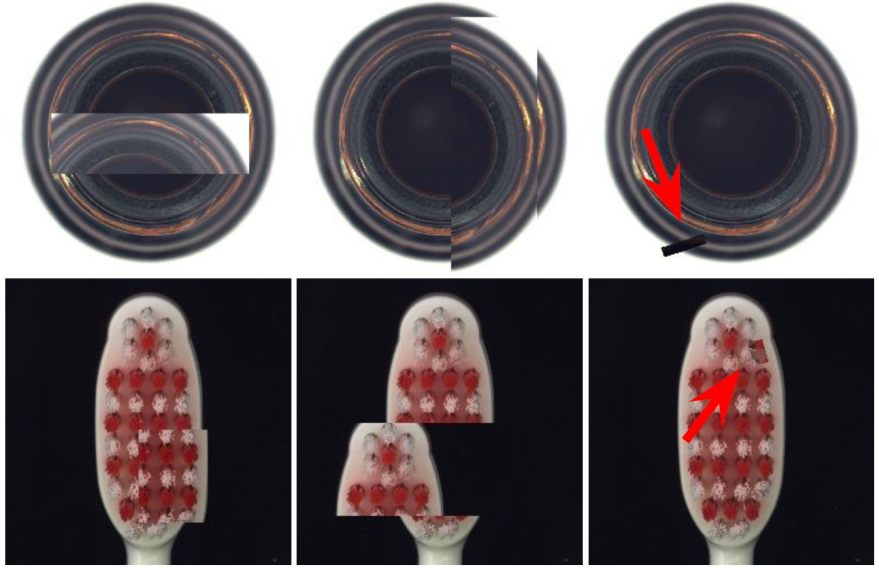
- However, SSL for AD is for **generating pseudo anomalies**
  - No fine-tuning; the generated anomalies determine the performance

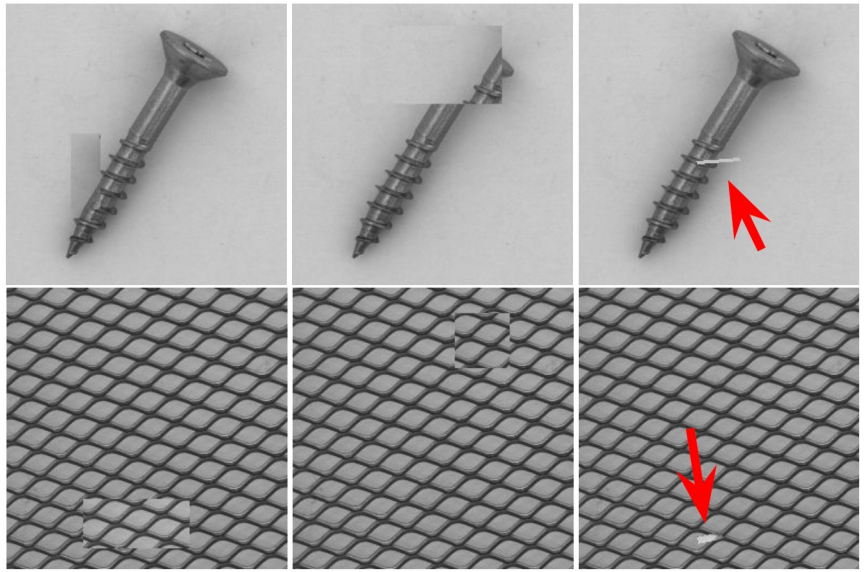


Generating pseudo-labels (via augmentation) (via outlier exposure)

Data Augmentation

- **Data augmentation** determines what anomalies to imagine
  - E.g., CutPaste (Li et al., 2021) was designed for industrial defects





Li et al. “CutPaste: Self-Supervised Learning for Anomaly Detection and Localization.” CVPR 2021

Many Augmentation Functions

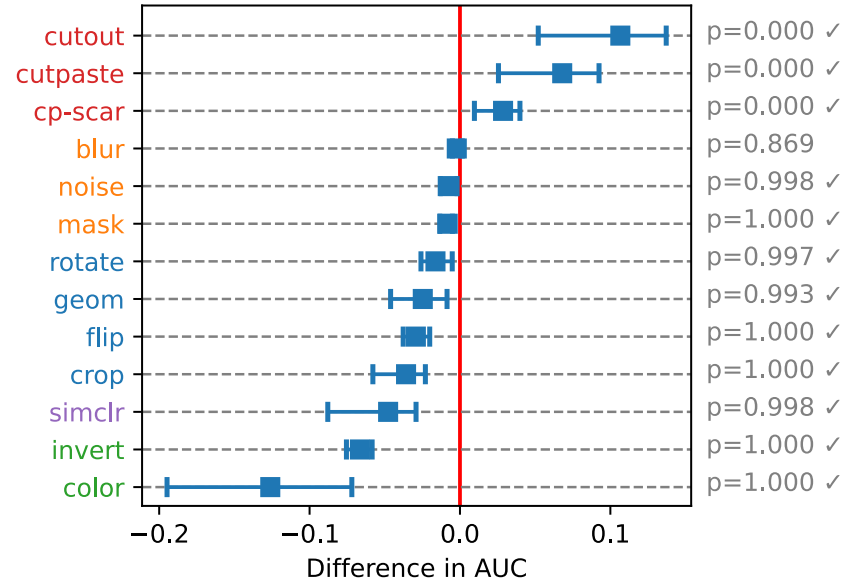
- **Augmentation is an important hyperparameter** (HP) for SSL
  - There are numerous data augmentation functions:

- Geometric: Crop (Chen et al., 2020), Rotate, Flip, and GEOM (Golan & El-Yaniv, 2018).
- Local: CutOut (Devries & Taylor, 2017), CutPaste and CutPaste-scar (Li et al., 2021).
- Elementwise: Blur (Chen et al., 2020), Noise, and Mask (Vincent et al., 2010).
- Color-based: Invert and Color (jittering) (Chen et al., 2020).
- Mixed ("cocktail"): SimCLR (Chen et al., 2020).

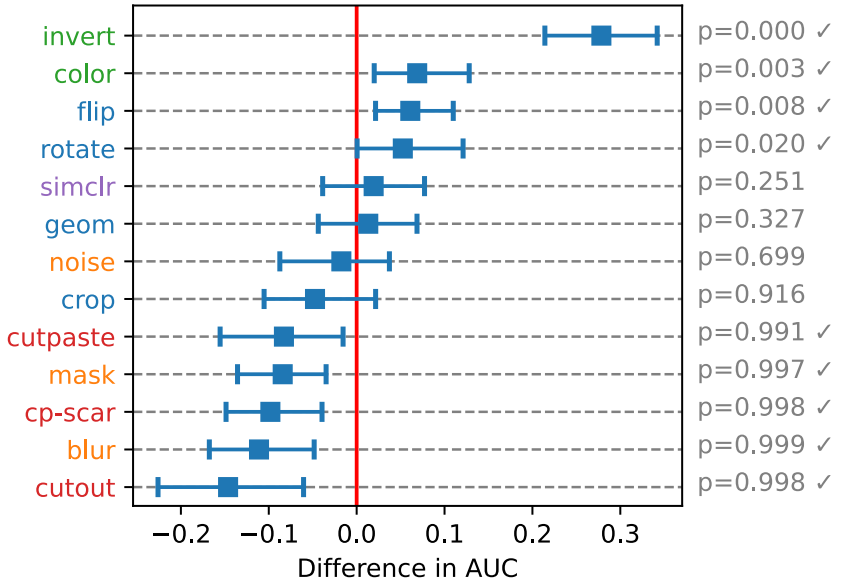
  - Given an AD task, Which one will work? Which one will fail?
  - Conducted a comprehensive study in our work (Yoo et al., 2023)

What Matters is Alignment

- What matters is the **alignment** between aug and gen
  - gen: Underlying mechanism that creates anomalies from normal data



(a) DAE on gen:=CutOut



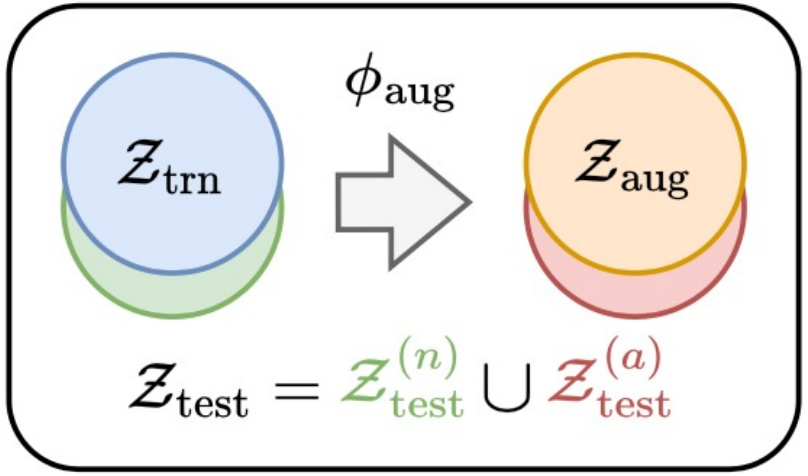
(b) DeepSAD on gen:=Invert

Outline

1. Introduction
2. Part 1: Choice of data augmentation
3. **Part 2: Automatic HP selection for SSL**
4. Part 3: GenAI and foundation models
5. Conclusion

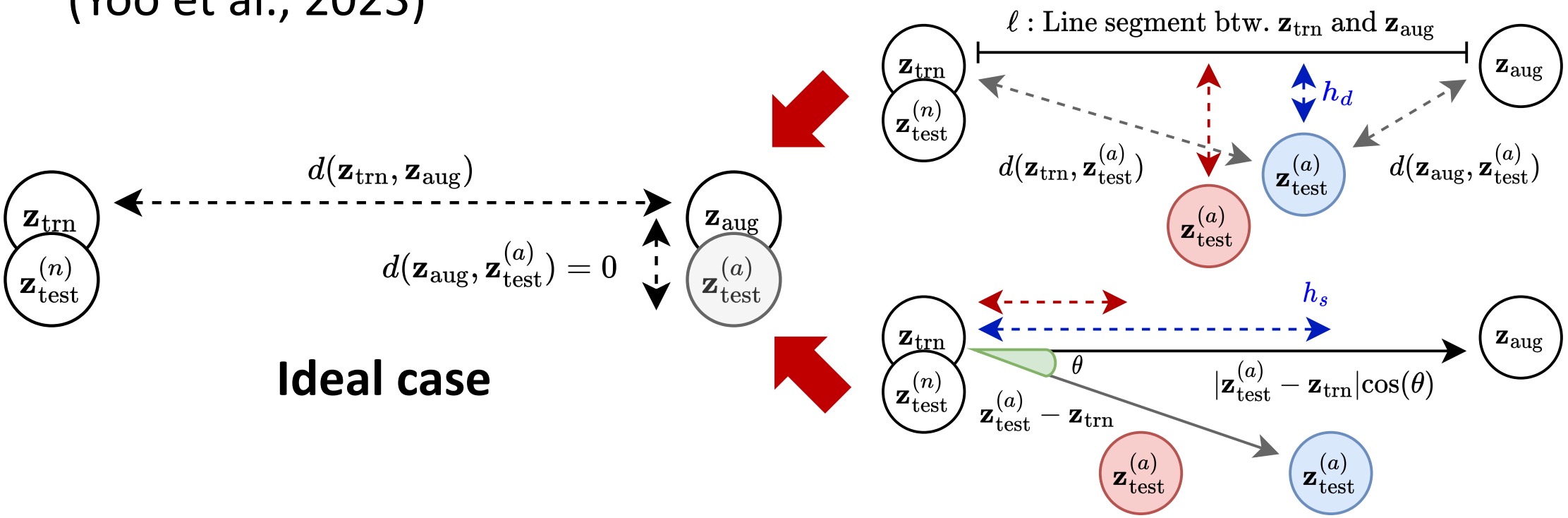
Self-Tuning Anomaly Detection

- **Q:** Can we really tune HPs **imagining unknown anomalies?**
- No, the guiding principle toward self-tuning AD is **transduction**
  - **Idea:** Use test data which contains unlabeled anomalies
  - Find HPs that maximize the alignment between $\mathcal{Z}_{\text{trn}} \cup \mathcal{Z}_{\text{aug}}$ and $\mathcal{Z}_{\text{test}}$



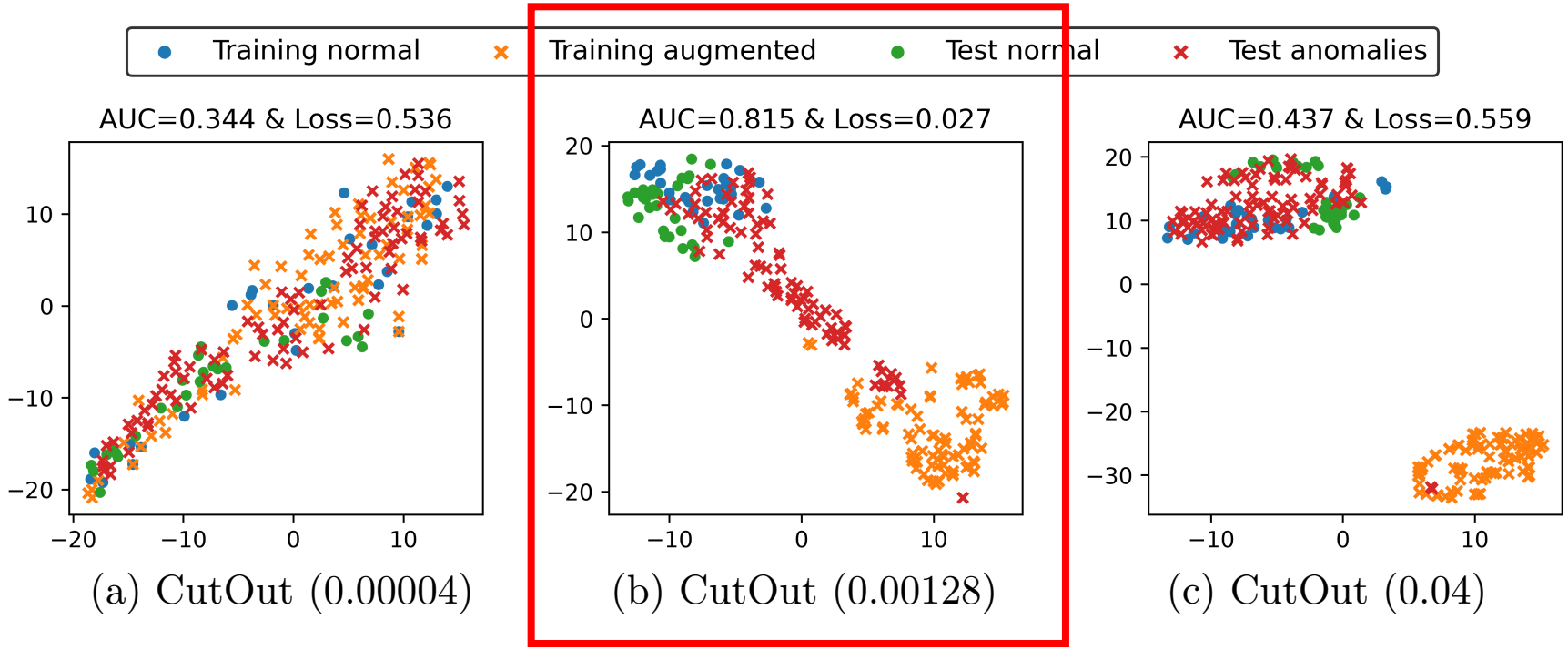
Alignment Validation Loss

- Proposed a **validation loss** that prefers the **blue** over the **red** (Yoo et al., 2023)



Alignment Validation Loss

- Tuned the **patch size** of local augmentation as a HP
  - Embeddings are best separated when the validation loss is minimum

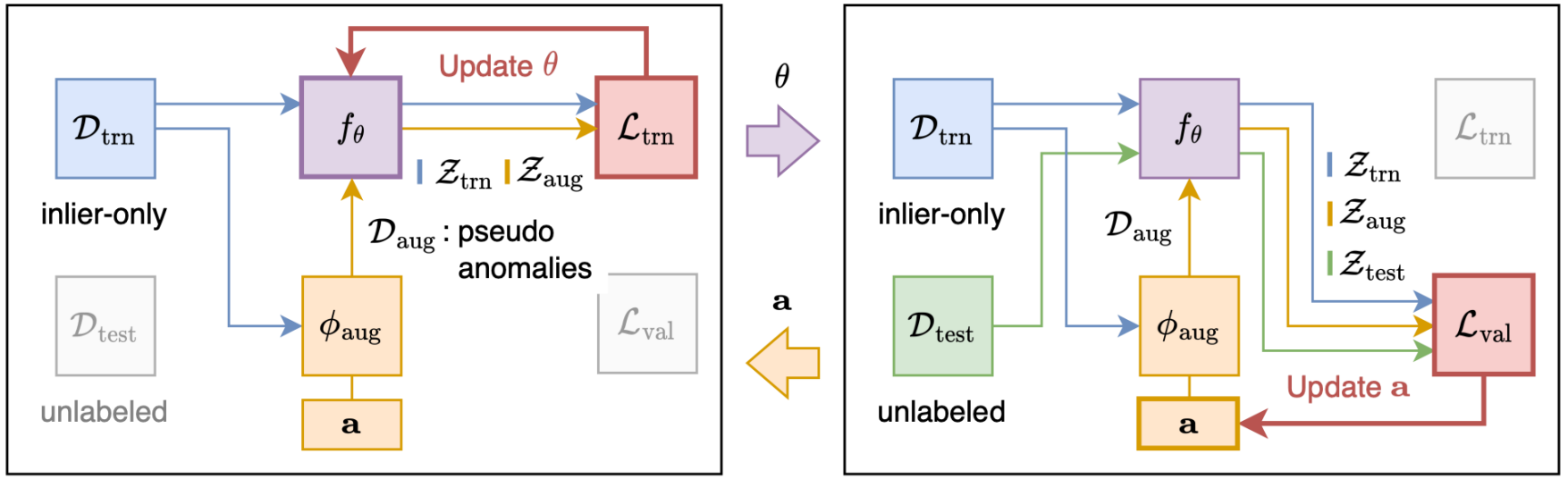


End-to-End Optimization of HPs

- **End-to-end optimization** is made possible with **alternate updates**

1) Train detector f_θ given $\mathbf{a}$
based on the training loss

2) Update $\mathbf{a}$ given fixed f_θ
based on the validation loss



End-to-End Optimization of HPs

- **Case studies:** Effectively learn the patch size through optimization

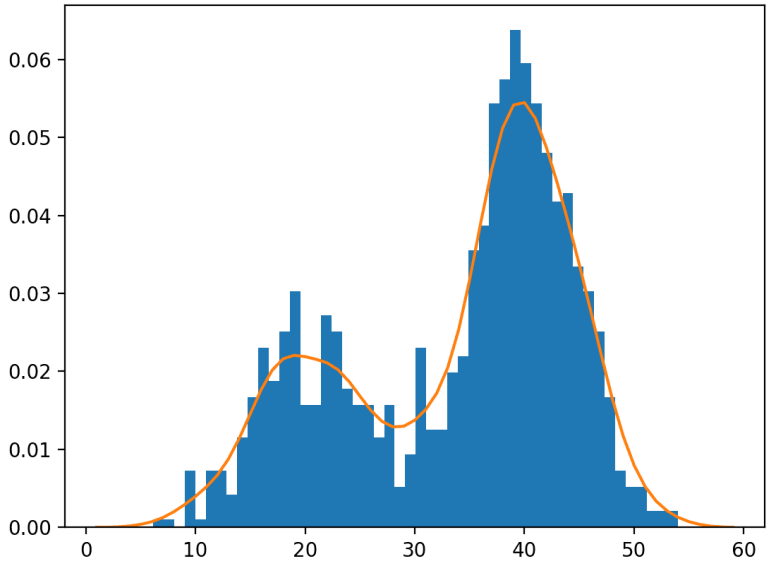
Yoo et al., “End-to-End Augmentation Hyperparameter Tuning for Self-Supervised Anomaly Detection.” arXiv (2023)

Outline

1. Introduction
2. Part 1: Choice of data augmentation
3. Part 2: Automatic HP selection for SSL
4. **Part 3: GenAI and foundation models**
5. Conclusion

Density Estimation

- **Density estimation** is a desired solution to unsupervised AD
  - One can always solve AD with an accurate estimation of $p(x)$
  - More difficult and ineffective than SSL, but hopefully unbiased



Foundation Models for AD

- **Today's generative (or foundation) models:**
  - Achieve outstanding results in learning data distributions
- **Based on:**
  1. Massive amounts of (pre)training data
  2. Large-scale computing power
  3. Highly expressive, billion-scale transformer models

Challenges for Foundation Models

- Main challenge for AD is the **necessity for massive data**
  - Since the data are limited, proprietary, or costly to obtain in many cases
  - E.g., web-lab experiments, accounting data, medical imaging, etc.
- **Democratizing large-scale pre-trained models:**
  - Has the potential to break new ground for AD in various domains

Outline

1. Introduction
2. Part 1: Choice of data augmentation
3. Part 2: Automatic HP selection for SSL
4. Part 3: GenAI and foundation models
5. **Conclusion**

Conclusion

- As a **vision paper**, we summarize our key take-aways as follows:
  1. SSL for AD has the unique challenge of **HP selection**
     - Specifically the choice of a augmentation function
  2. Idea of **transduction** is a key toward fair HP selection
     - Leveraging unlabeled test data to get a sense of true anomalies
  3. **Generative AI** and **foundation models** can be the future of AD
     - Given that massive amounts of training data exist