
科研人员提出几何率失真不变性算法实现AI精准跨域判别

作者：writer 来源：中国科学院

本文原地址：<https://www.iikx.com/news/progress/41783.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

科研人员提出几何率失真不变性算法实现AI精准跨域判别

。深度学习模型在训练数据与测试数据分布一致时性能卓越，但在脑机接口、医学影像等实际应用中，会受到受试者个体差异、电极/传感器漂移、采集设备与临床环境变化等因素影响，数据分布发生偏移，导致模型性能大幅下降。近年来，学界利用分布对齐、对抗训练及不变风险最小化等手段，发展了一系列领域泛化算法。然而，主流方法大多聚焦于匹配不同域之间的边缘分布或梯度统计量，在有限样本下易导致对齐失稳甚至坍塌，制约了深度学习模型在真实目标域上的跨域判别能力。

近日，中国科学院过程工程研究所科研团队将信息论中的率失真理论推广到Grassmann流形，提出几何率失真不变性（RDI）算法。

该算法利用深度学习特征在实际分布中的低维几何结构，构建强判别力的分类依据。该框架可使不同来源数据中同一类别的特征方向趋于一致以消除域间偏差，同时控制每个类别特征分布的“体积”，防止其过度坍塌，保留类别间的判别差异。通过与分类任务的联合训练，模型可在保持分类精度的同时，缩小不同来源数据之间的几何差异。

实验结果表明，RDI具备任务自适应的调控能力。面对类别较少的场景，模型会主动扩展有效特征维度以防止信息坍塌。面对类别繁多的复杂场景，则自动压缩冗余信息以提升紧凑性。这种“收放自如”的特性使RDI在面对完全未知的目标域时仍能保持稳定的判别能力。在领域内最具权威的DomainBed标准测试集上，RDI的平均准确率超越了现有主流不变性学习方法，且在CNN与ViT等不同架构上均表现稳健。

该方法将有效解决深度学习模型在跨域数据场景下判别性能骤降的难题，为深度学习模型的跨域泛化问题提供了新的理论视角与解决方案。研究工作为脑机接口等场景的分布偏移问题提供了新的几何视角与算法基础。

相关研究成果发表在ICML

2026上。研究工作得到国家自然科学基金委员会、中国科学院等的支持。

[论文链接](#)

Contact & Cooperation

• liutong@ipe.ac.cn
• liangsen@ipe.ac.cn
• baishuo@ipe.ac.cn



Motivation

- Deep domain adaptation on low-dimensional class-conditional structures. Semantic information lies in their relative geometry and spectrum, not just marginal statistics.
- Existing DG methods (CORAL, IRM, VREx, Fisher algo) statistics but ignore geometric organization.
 - Orthogonal alignment can destabilize discriminative geometry.
 - RM, ill-conditioned alignment or representation collapse.
- Key gap: DG requires joint control of:
 - cross-domain geometric alignment (direct result)
 - special complexity within subspaces (curvature)

Key Idea

- ERM aligns class-conditional subspaces toward an invariant semantic center $\mathbb{E}$ on the Grassmann manifold while resolving spectral complexity via rate control.

$$\mathcal{L}_{ERM}(\mathbf{f}) = \mathbb{E}_{\mathbf{f}} \left[\sum_{c=1}^C \|\mathbf{f}_c - \mathbb{E}\|^2 \right]$$
 - Novel framing: First geometric rate-distortion formulation for DG via Grassmann manifold.
 - Principal representation: Fisher-linearized training capacity with provable top-to-bottom generalization.
 - Theoretical analysis: Test-sample recovery & generalization bound under bounded drift.
 - Architecture-agnostic: consistent gains across ResNet-50, DGCNN, ConvNeXt-V2.

Method

- Empirical (linear) geometry: $\mathbf{A}_k^T \mathbf{A}_k = \sum_{i=1}^n \mathbf{a}_{ki} \mathbf{a}_{ki}^T, \mathbf{A}_k \in \mathbb{R}^{d \times n_k}$

Rate (capacity requirement): $\mathcal{R}_k(\mathbf{A}_k) = \frac{1}{n_k} \sum_{i=1}^{n_k} \log \frac{1}{\lambda_i(\mathbf{A}_k)}$

Key: aggregation across domains:

$$\mathcal{R}(\mathbf{A}) = \frac{1}{n} \sum_{k=1}^K \mathcal{R}_k(\mathbf{A}_k)$$
- Principal angles θ_k between empirical class-conditional subspaces capture the rotation needed to align them. The Grassmann distance $\delta_{G, \mathbf{A}_k}$ aggregates over all k angles.
- Minimax (loss recovery). Under an added criterion, the RM minimizes statistics, with prob $1-\delta$:

$$\hat{\mathbf{A}}_{\mathbf{A}_k}(\mathbf{A}_k) = \arg \min_{\mathbf{A}_k} \left(\frac{1}{n_k} \sum_{i=1}^{n_k} \log \frac{1}{\lambda_i(\mathbf{A}_k)} + \epsilon_{\mathbf{A}_k} \right)$$

Shrinkage (denormalization):

$$\hat{\mathbf{A}}_{\mathbf{A}_k}(\mathbf{A}_k) = \frac{\sqrt{\lambda_{\max}(\mathbf{A}_k)} - \sqrt{\lambda_{\min}(\mathbf{A}_k)}}{\sqrt{\lambda_{\max}(\mathbf{A}_k)} + \sqrt{\lambda_{\min}(\mathbf{A}_k)}} \mathbf{A}_k$$

Final result (denormalization):

$$\hat{\mathbf{A}}_{\mathbf{A}_k}(\mathbf{A}_k) = \frac{\sqrt{\lambda_{\max}(\mathbf{A}_k)} - \sqrt{\lambda_{\min}(\mathbf{A}_k)}}{\sqrt{\lambda_{\max}(\mathbf{A}_k)} + \sqrt{\lambda_{\min}(\mathbf{A}_k)}} \mathbf{A}_k$$

Practical considerations: Without rate control, geometric features, alone retrieved RM $\hat{\mathbf{A}}_{\mathbf{A}_k}(\mathbf{A}_k) \rightarrow$ even with bounded features $\rightarrow$ spectral collapse.

$\rightarrow$ Rate control is necessary, not just beneficial.

Experiments

- Controlled subspace recovery. RDI achieves (a) ground-truth recovery via Grassmann, (b) flexible geometric alignment across domains, and (c) Pareto-optimal operation in the rate-distortion plane. Ablation studies on at least one axis.
- Classification accuracy (%) on DomainShift under training-domain shift (ResNet50, 3 trials).

Model	ERM	VREx	IRM	ERM	ERM	ERM
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0
VREx	80.0	80.0	80.0	80.0	80.0	80.0
IRM	80.0	80.0	80.0	80.0	80.0	80.0
ERM	80.0	80.0	80.0	80.0	80.0	80.0