The 12th International Conference on Learning Representations

Adversarial AutoMixup

Huafeng Qin[1,*,#], Xin Jin[1,*], Yun Jiang[1], Mounîm A. El-Yacoubi[2], Xinbo Gao[3]

[1] Chongqing Technology and Business University, [2] Telecom SudParis, Institut Polytechnique de Paris

[3] Chongqing University of Posts and Telecommunications

Introduction

- Mixup approaches have been widely applied to improve the generalization ability of DNNs.
- Recently, offline mixup has been gradually replaced by automatic mixup, *e.g.* AutoMix.
- AutoMix aims to obtain, instead of diverse mixed samples, consistent samples w.r.t training data, which may lead to DNNs overfitting.
- We propose *AdAutoMix*, an adversarial automatic mixup augmentation model that aims to generate *challenging* samples to train a robust classifier for image classification. Extensive experiments prove that our method outperforms the SOTA in various classification scenarios.

AdAutoMix

1.Generator: We get $z_n^l \in R^{c\times h\times w}$ from an encoder, and obtain embedding λ map $z_\lambda^l = C(M_\lambda, z_n^l) \in R^{c+1\times h\times w}$, then obtain mixed samples by MB:

$$P_n = Softmax\left(\frac{\Sigma_{i=1,i\neq n}^{N} q_n^T k_i}{\sqrt{d}}\right) v_n \qquad (1)$$

$$x_{mix} = \sum_{n=1}^{N} x_n \times Softmax(P_1, \dots, P_n)_n \qquad (2)$$

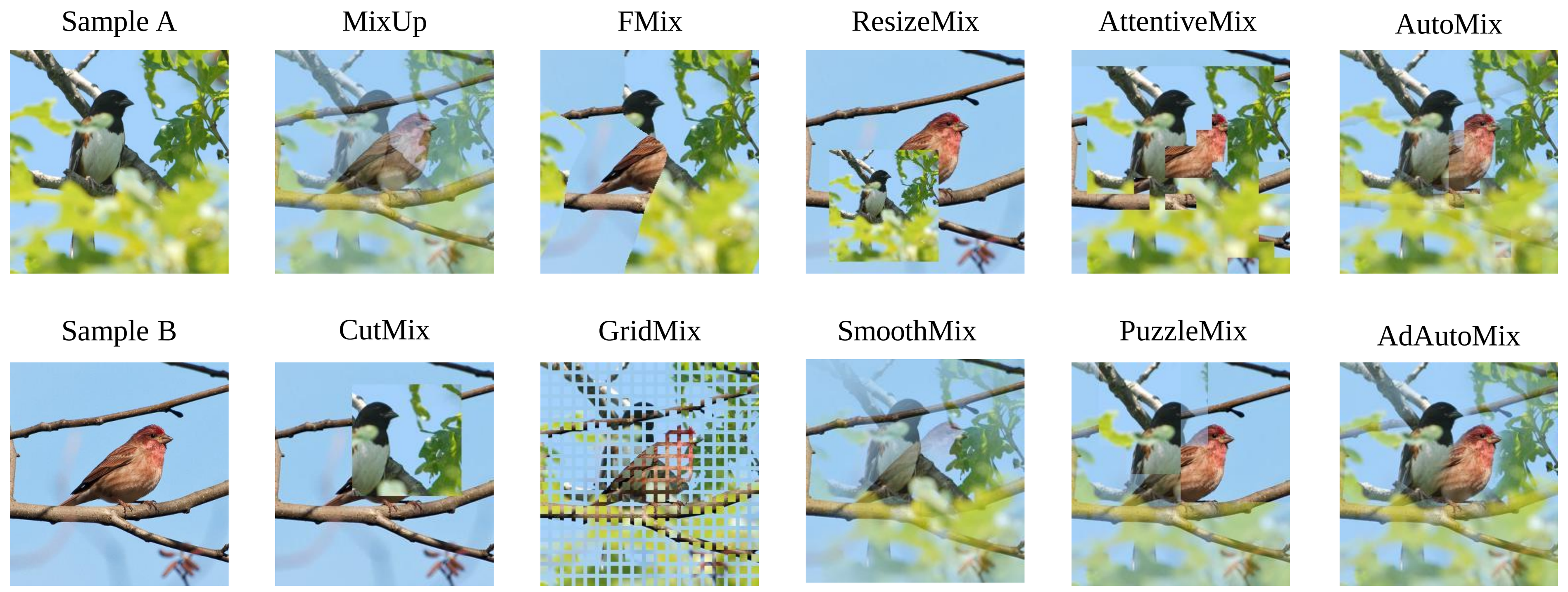

Figure 1. Mixed images of various mixup-based approaches.

2.Adversarial Augmentation: We get a robust classifier by:

$$W,\theta = \underset{w}{argmin}\,\underset{\theta}{max}\begin{pmatrix} L_{amce}(\psi_w, Y) + \alpha L_{mce}(\psi_w, y_{mix}) \\ +(1-\alpha)L_{ace}(\psi_w, Y) \end{pmatrix} \qquad (3)$$

For adversarial training:

$$W,\theta = \underset{w}{argmin}\,\underset{\theta}{max}\begin{pmatrix} L_{amce}(\psi_w, Y) + \alpha L_{mce}(\psi_w, y_{mix}) + \\ (1-\alpha)L_{ace}(\psi_w, Y) - \beta L_{amce}(\psi_{\hat{w}}, Y) + \\ (1-\beta)L_{cosine} \end{pmatrix} \qquad (4)$$

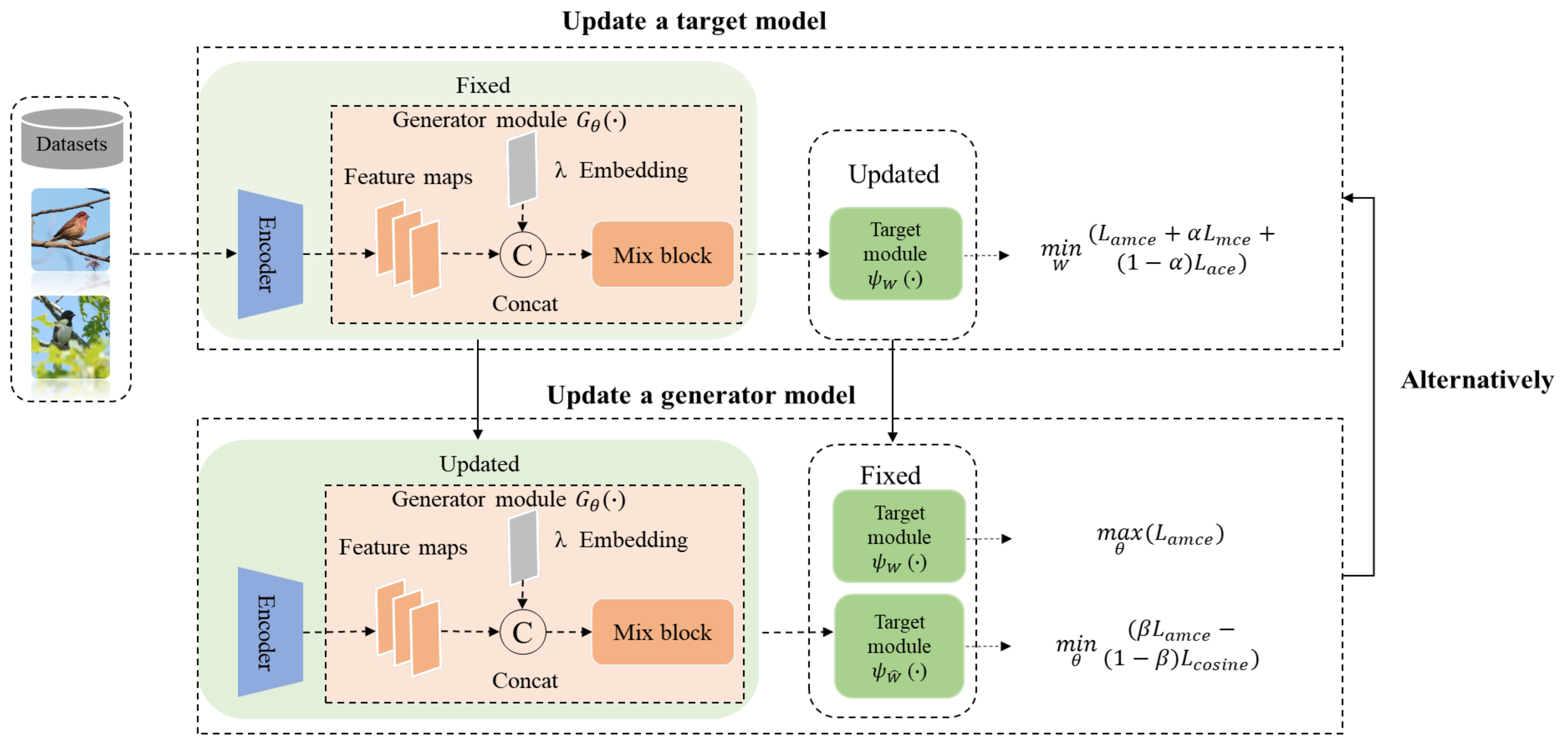

Figure 2. Illustration of AdAutoMix framework. AdAutoMix consists of a Generator module and a Target module.

Experiments

- Image classification experiments compared with other mixup approaches on generic datasets (Tab 1) and fine-grained (Tab 2) datasets.

Table 1. Top-1 accuracy (%)↑ of mixup approaches on CIFAR-100, Tiny-ImageNet and ImageNet-1K with CNN architecture and Transformer architecture.

	CIFAR100		CIFAR100		Tiny-ImageNet		ImageNet-1K		
Method	ResNet18	ResNeXt50	Swin-T	ConvNeXt-T	ResNet18	ResNeXt50	ResNet18	ResNet34	ResNet50
Vanilla	78.04	81.09	78.41	78.70	61.68	65.04	70.04	73.85	76.83
MixUp	79.12	82.10	76.78	81.13	63.86	66.36	69.98	73.97	77.12
CutMix	78.17	81.67	80.64	82.46	65.53	66.47	68.95	73.58	77.17
SaliencyMix	79.12	81.53	80.40	82.82	64.60	66.55	69.16	73.56	77.14
FMix	79.69	81.90	80.72	81.79	63.47	65.08	69.96	74.08	77.19
PuzzleMix	81.13	82.85	80.33	82.29	65.81	67.83	70.12	74.26	77.54
ResizeMix	80.01	81.82	80.16	82.53	63.74	65.87	69.50	73.88	77.42
AutoMix	82.04	83.64	82.67	83.30	67.33	70.72	70.50	74.52	77.91
AdAutoMix	**82.32**	**84.22**	**84.33**	**83.54**	**69.19**	**72.89**	**70.86**	**74.82**	**78.04**
Gain	**+0.28**	**+0.58**	**+1.66**	**+0.24**	**+1.86**	**+2.17**	**+0.36**	**+0.30**	**+0.13**

- Robustness.

Table 2. Top-1 accuracy (%)↑ of mixup approaches on CUB-200, FGVC-Aircrafts and Standford-Cars.

	CUB-200		FGVC-Aircrafts		Standford-Cars	
Method	ResNet18	ResNet50	ResNet18	ResNeXt50	ResNet18	ResNeXt50
Vanilla	77.68	82.38	80.23	85.10	86.32	90.15
MixUp	78.39	82.98	79.52	85.18	86.27	90.81
CutMix	78.40	83.17	78.84	84.55	87.48	91.22
ManifoldMix	79.76	83.76	80.68	86.60	85.88	90.20
SaliencyMix	77.95	81.71	80.02	84.31	86.48	90.60
FMix	77.28	83.34	79.36	86.23	87.55	90.90
PuzzleMix	78.63	83.83	80.76	86.23	87.78	91.29
ResizeMix	78.50	83.41	78.10	84.08	88.17	91.36
AutoMix	79.87	83.88	81.37	86.72	88.89	91.38
AdAutoMix	**80.88**	**84.57**	**81.73**	**87.16**	**89.19**	**91.59**
Gain	**+1.01**	**+0.69**	**+0.36**	**+0.44**	**+0.30**	**+0.21**

Table 3. Top-1 accuracy (%)↑ with clean and corruption test dataset and FGSM error (%)↓.

Method	Clean Acc(%)↑	Corruption Acc(%)↑	FGSM Error(%)↓
CutMix	79.45	46.66	88.24
FMix	78.91	50.58	88.35
PuzzleMix	79.96	51.04	80.52
AutoMix	80.02	50.75	82.67
AdAutoMix	**81.55**	**51.44**	**75.66**

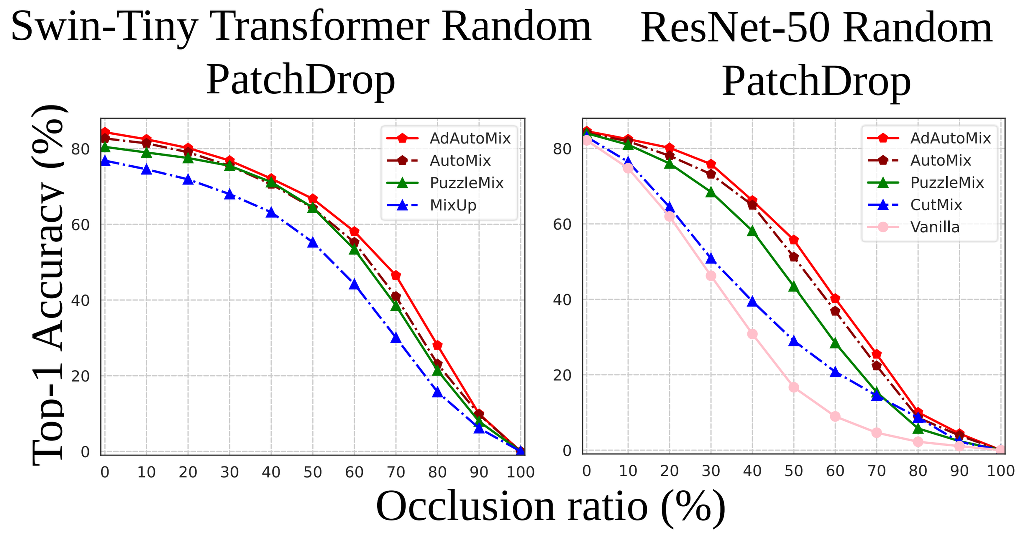

Figure 3. Robustness against image occlusion with different occlusion ratios.

Contact us:

Paper Code HomePage WeChat

I`m searching for a 2025 fall or 2026 spring PhD position, if you are interested, please feel free to contact me !

Chongqing Technology and Business University, China Email: Jinxin20001118@163.com Paper: https://arxiv.org/abs/2312.11954 Code: https://github.com/JinXins/Adversarial-AutoMixup