|  |  |
| --- | --- |
| **文章信息** | **摘要及贡献** |
| **阅读程度**：  精读  **文章标题：**  Adversarial Momentum-Contrastive Pre-Training  **中文标题：**  对抗性对比对抗预训练  **发表于：**  Pattern Recognition Letters  **作者：**  Cong Xu，Min Yang  **单位：**  烟台大学数学与信息科学学院 | 作者引入了两个memory bank分别存储自然样本与对抗样本，步骤如下：   1. 进行两种数据增强 2. 计算loss CCC，第一个C指encoder\_q处理数据增强1，得到自然样本的q，第二个C 指encoder\_k处理数据增强2，得到自然样本的k，第三个C指使用自然样本M1（memory bank1）作为负样本，简单来说就是原moco的损失。（这一步中所有样本均应该通过bn\_clean层） 3. 最大化对比损失求数据增强1的对抗样本。（源代码中不仅求了数据增强1的对抗样本，也求了数据增强2的对抗样本并且都是基于encoder\_q及**bn\_adv**生成的对抗样本，然后数据增强2的对抗样本将经过encoder\_k bn\_adv后被送入memorybank，数据增强1的对抗样本用于后面继续计算损失） 4. 计算lossACA，第一个A指encoder\_q处理数据增强1的对抗样本，得到对抗样本的q，第二个C 指encoder\_c处理数据增强2，得到自然样本的k，第三个A指使用对抗样本M2（memory bank2）作为负样本，注意对抗样本是用encoder\_c处理对抗样本后将特征存入M2。   区别：  第三步中我使用的是最大化样本与原样本的余弦相似度最为损失函数生成对抗样本，并且这个过程中使用MAX（L1 Linf）最大化策略生成对抗样本，这样做第一，使用对比损失生成对抗样本，相当于以数据增强1样本为起点，学习一个与数据增强2样本的余弦相似度（来自encoder\_k）较小的对抗样本，即这个对抗过程远离的目标来自encoder\_k，而我的损失函数是以数据增强1样本为起点，学习一个与自身余弦相似度（来自encoder\_q）较小的对抗样本，更符合对抗训练中基于自身进行最大化的目的，并且在后续微调过程中并不会使用到encoder\_k，因此我的最大化损失更为合理。此外使用MAX策略增加了对抗样本的多样性。原文是两个memory bank，第二步与M1对比，第四步与M2对比，即对抗样本的负样本全是对抗样本，自然样本的负样本全是自然样本。我的方法是将数据增强2的k和对抗样本的k一并纳入memory bank中，这样负样本中一半是自然样本一半是对抗样本，这样更直观地将相近图片的自然样本与对抗样本均聚集到一起。 |
| **摘要** |  |
| 最近提出的对抗性自监督学习方法通常需要大量和长时间的训练来提取鲁棒特征，这将在资源有限的平台上带来沉重的计算开销。  为了帮助网络在更小的批次和更少的时代中学习更强大的特征表示，本文提出了一种新的对抗性动量对比学习方法，该方法分别引入了两个对应于干净样本和对抗性样本的记忆库。  这些内存库可以动态地合并到训练过程中，以跟踪历史小批次之间的不变特征。与之前的对抗性预训练模型相比，该方法在较小的批量和较少的训练周期下取得了较好的性能。此外，在对下游分类任务上进行微调后，该模型在多个基准数据集上优于一些最先进的监督防御方法。 | 实验部分：  第一个实验，验证预训练（也就是MoCo过程无监督训练的结果与ACL方法进行对比），冻结特征提取器，训练一个分类头（且使用正常训练和对抗训练两种方式），并且还统计了运行时间，这里我实在怀疑对正常训练的分类器进行攻击后的攻击效果，然后进行了训练时间上的对比    实验二：微调后与已有的对抗训练进行对比，这里有两个问题，第一没有跟ACL微调后进行对比，第二只跟单范数对抗训练进行比而且此方法对L1范数的攻击防御能力并不佳，第三，微调是使用Trades策略对整个特征提取器微调100轮，这是否有点：    实验三：验证了对更大范数的攻击性能的下降过程。  实验四：消融实验    证明ACA是最好的选择，ACC也还行  AAC比较两种数据增强的对抗样本，拿着自然样本做负样本，当然效果比较差  AAA拿着对抗样本做负样本，这样CCC关注自然样本的聚类，AAA关注对抗样本的聚类，缺少自然样本与对抗样本之间的交互  CAC与CAA告诉我们，当编码器k提取的对抗样本特征不能用来算损失。 |
| ATMOCO与本文的区别：   1. We give insights into why current adversarial contrastive learning algorithms require large batch sizes and long training epochs to reach convergence. Based on this, we explain the necessity of introducing separate memory banks to learn a better query encoder. 意思是当前的对抗对比学习算法需要大的batch\_sizes和长的训练epoch，基于此解释了引入memory bank的重要性，我觉得这个不算是本文的贡献，这个东西可以说kaiming大佬已经解释过了，是显而易见的东西。 | |