南京郵電大學
Nanjing University of Posts and Telecommunications

毕业论文答辩

基于证据深度学习的开集行为识别方法设计与实现

学　　校：南京邮电大学

学　　院：计算机学院、软件学院、网络空间安全学院

指导老师：陈蕾 教授

汇报学生：徐梓涵

汇报日期：2024.6.5

汇报提纲

- 背景介绍
- 模型介绍
- 实验结果
- 可视化界面
- 成果简介

背景介绍

南京郵電大學 Nanjing University of Posts and Telecommunications

模型不知道自己不知道

常规训练模型

训练集数据

背景介绍

南京邮电大学 Nanjing University of Posts and Telecommunications

视频中的静态偏差

室外滑冰

室内滑冰

在真实场景中，人的动作通常不在训练数据的分布范围内，这就需要一个模型来识别已知的动作并拒绝未知的动作。但相比于图像数据，人类动作的信息载体视频时间动态和静态偏差都是很不确定的，难以被识别。

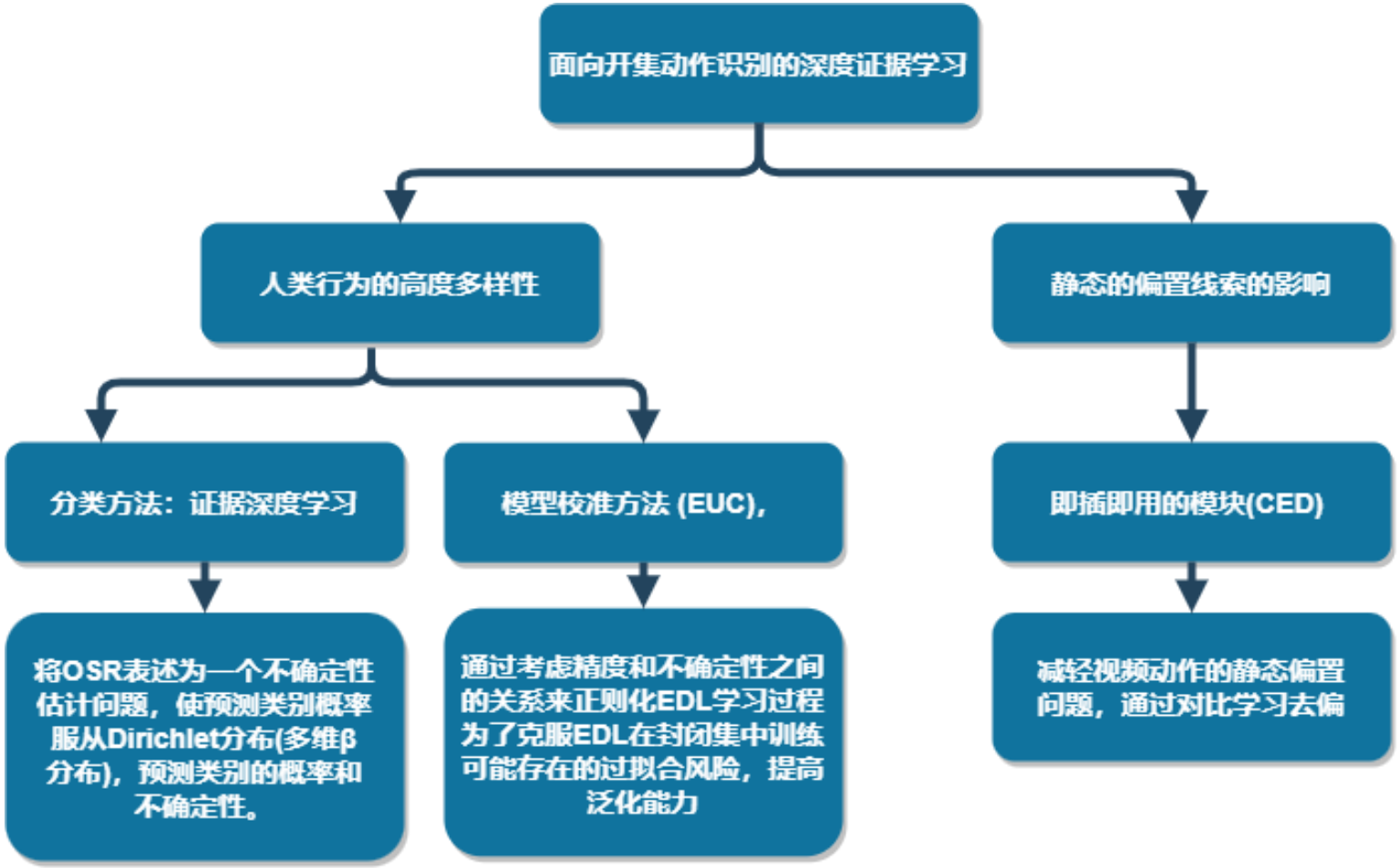
模型介绍

研究课题

难点问题

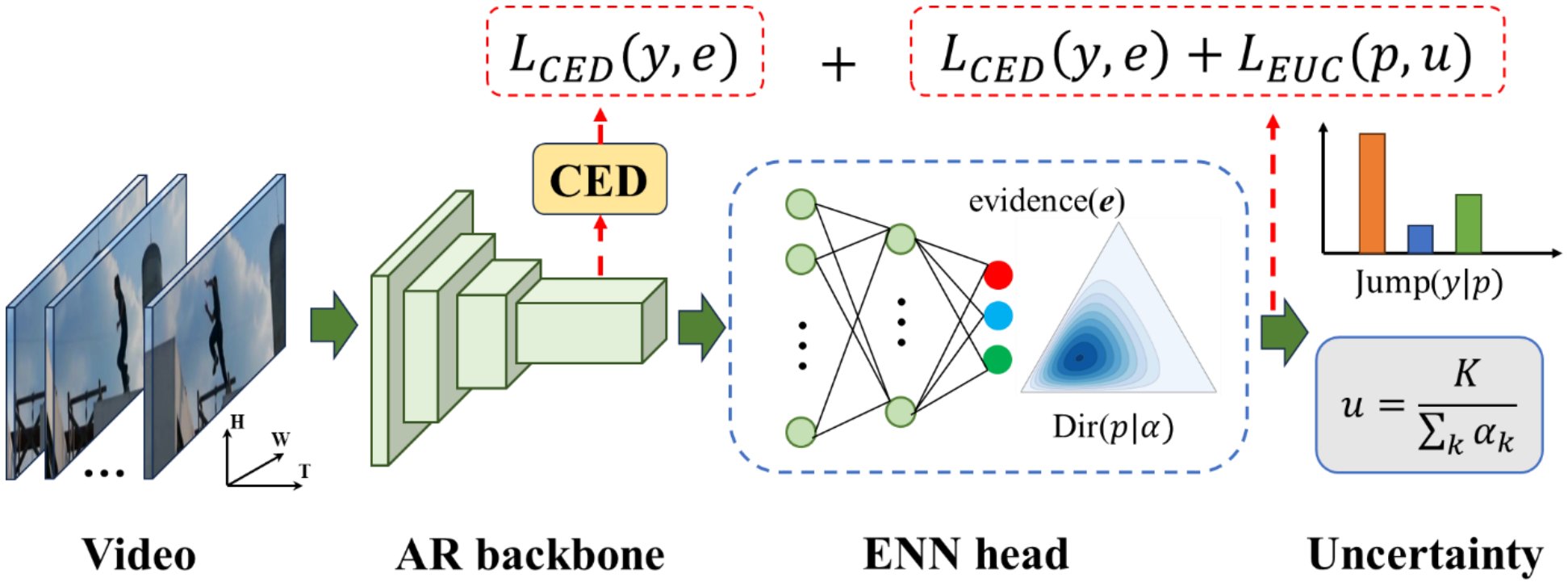
技术路线

研究内容



模型介绍

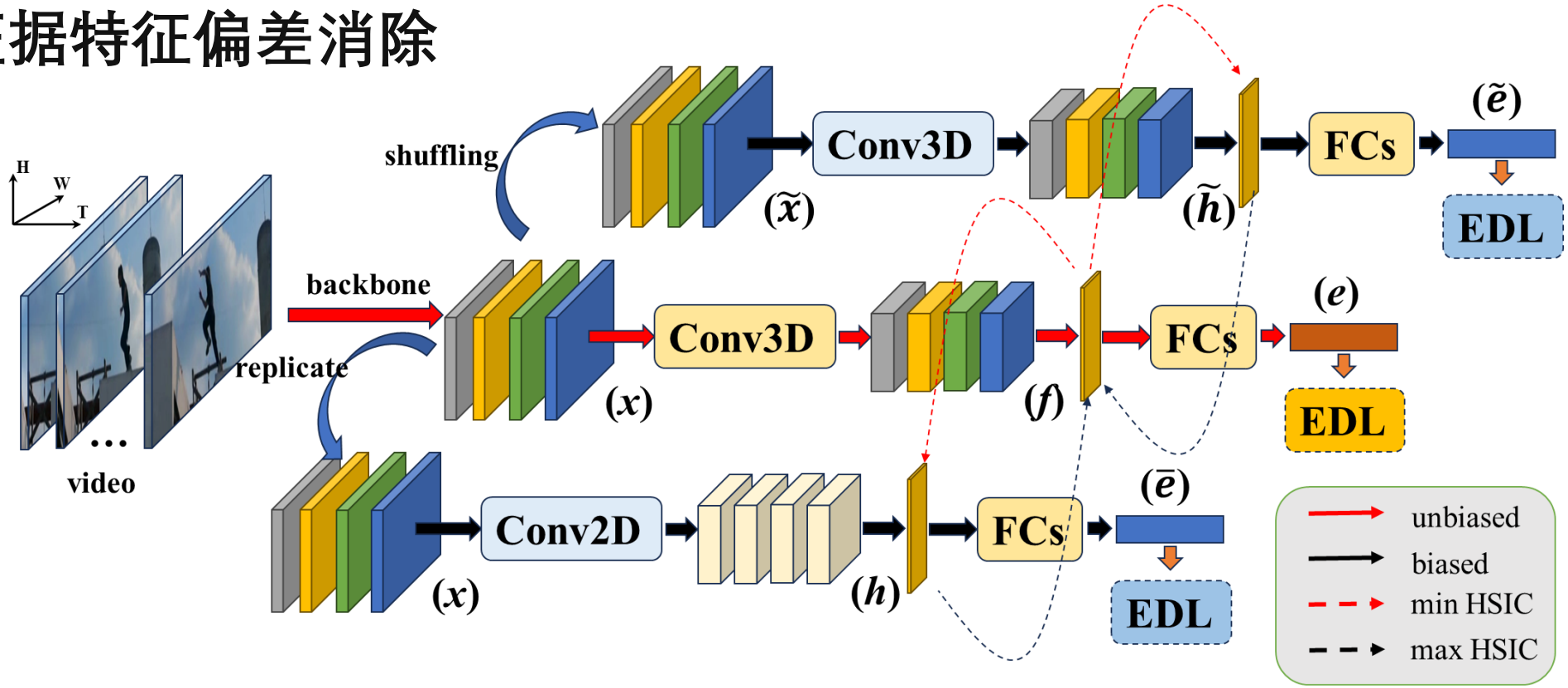
DEAR模型框架



EDL的基本假设：模型输出的分类概率服从狄利克雷分布 (Dirichlet Distribution)，通过最大化观测数据的概率似然，直接估计狄利克雷分布参数。

模型介绍

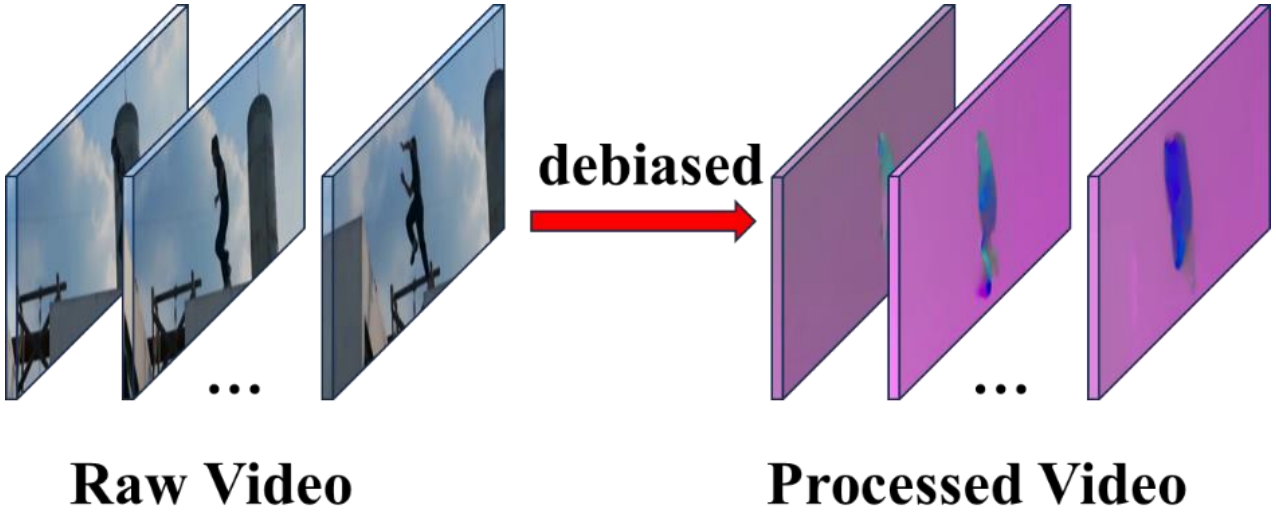
证据特征偏差消除



该模块采用三条并行的特征提取分支，图中的上下两个分支分别采用时序混排 (shuffling) 后的时空特征输入以及2D卷积模块 (Conv2D)，提取丢失了时序特性的特征作为有偏差的特征 (biased feature)，用于引导采用3D卷积 (Conv3D) 的中间分支提取无偏差的特征 (unbiased feature)。

模型介绍

证据特征偏差消除

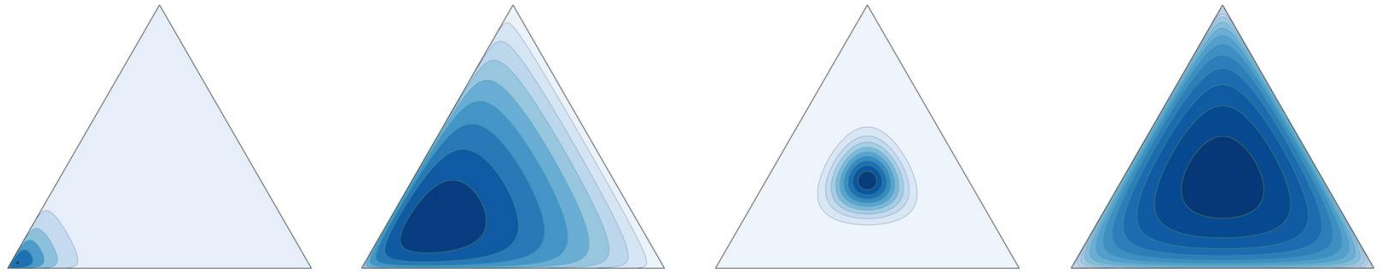


去偏（CED）后视频

对两个目标进行交替优化，使特征h被学习到有偏，从而指导特征f的去偏。在实践中，实验还实施了联合训练策略，旨在联合优化目标，经验发现它可以取得更好的效果。

不确定性校准

由于EDL的目标是一种最大似然估计，具有较高的过拟合风险。在不确定性估计方面，过拟合体现为无论样本是否未知，模型都过于信任分类结果 (over-confident)。而K类别的狄利克雷分布可以通过K-1维的单纯形 (simplex) 来表示狄利克雷概率密度。按照分类的准确性与不确定性，可以有四种组合，以K=3为例，其二维单纯形概率密度如图所示：



$\alpha = [10,1.2,1.2], u = 0.2$ $\alpha = [1.8,1.2,1.2], u = 0.7$ $\alpha = [10,10,10], u = 0.1$ $\alpha = [1.2,1.2,1.2], u = 0.8$

(a)AC (b)AU (c)IC (d)IU

为了鼓励模型学到更好的不确定性，样本的输出应当包含更多的AC和IU，更少的AU和IC

则优化目标：$\max \frac{n_{AC}+n_{IU}}{n_{AC}+n_{AU}+n_{IC}+n_{IU}}$

模型介绍

$$L_{EDL}^{(i)}(y^{(i)}, e^{(i)}; \theta) = \sum_{k=1}^{K} y_k^{(i)} (logS^{(i)} - log(e_k^{(i)} + 1))$$

EDL训练最小化损失函数：对于输入的视频样本x_i，模型$f(x^{(i)};\theta)$输出各类的分类证据$e^{(i)}$，类别标签为$y^{(i)}$

$$L_{EUC} = -\lambda_t \sum_{i \in \{\overline{y_i} = y_i\}} p_i \, log(1 - u_i) - (1 -$$

$$\lambda_t) \sum_{i \in \{\overline{y_i} \neq y_i\}} (1 - p_i) log(u_i)$$

不确定性校准损失函数：退火系数λ_t，定义为$\lambda_t = \lambda_0 exp\{-(ln\lambda_0/T)t\}$

$$L(\theta_f, \varphi_f) = L_{EDL}(y,e;\theta_f, \varphi_f) + \lambda \sum_{h \in \Omega} HSIC(h, f, \theta_f)$$

中间的无偏特征学习分支的损失函数：

第一项为基于EDL的动作分类目标，第二项最小化希尔伯特-施密特独立性准则 (HSIC)

$$L(\theta_h, \varphi_h) = L_{EDL}(y,e_h;\theta_h, \varphi_h) - \lambda \sum_{h \in \Omega} HSIC(f, h, \theta_h)$$

上下两条分支的总损失函数：

第一项EDL分类目标保证特征h有足够的分类判别力而非随机的特征表示，第二项最大化HSIC使h靠近无偏特征f。

实验结果

不同模型在数据集上的表现

模型	top1 准确率	top5 准确率	平均类别准确率
DNN	0.9474	0.9939	0.9469
BNN	0.9448	0.9939	0.9444
EDLNOKL	0.9485	0.9937	0.9476
EDLNOKL AVUC DEBIAS	0.9442	0.9937	0.9434

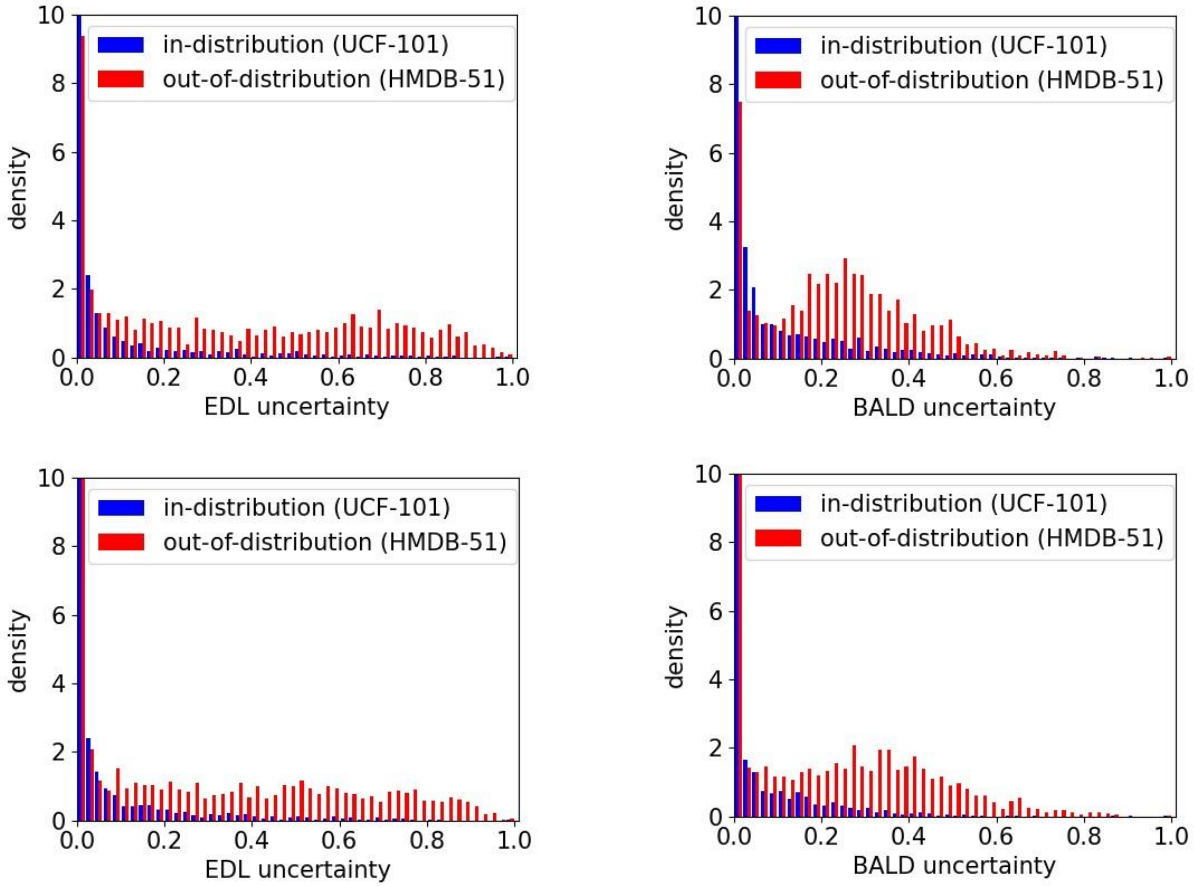
如表所示，在top1准确率（即模型预测的最有可能的类别的准确率）上达到了0.9442的高分，而top5准确率（即模型预测的前五个最可能的类别中至少有一个正确类别的准确率）更是高达0.9937。此外，平均类别准确率（mean class accuracy），这是一个考虑了每个类别样本数量的指标，也达到了0.9434，显示出DEAR模型在不同类别上的表现均衡且准确。

实验结果

Out-of-distribution 检测：

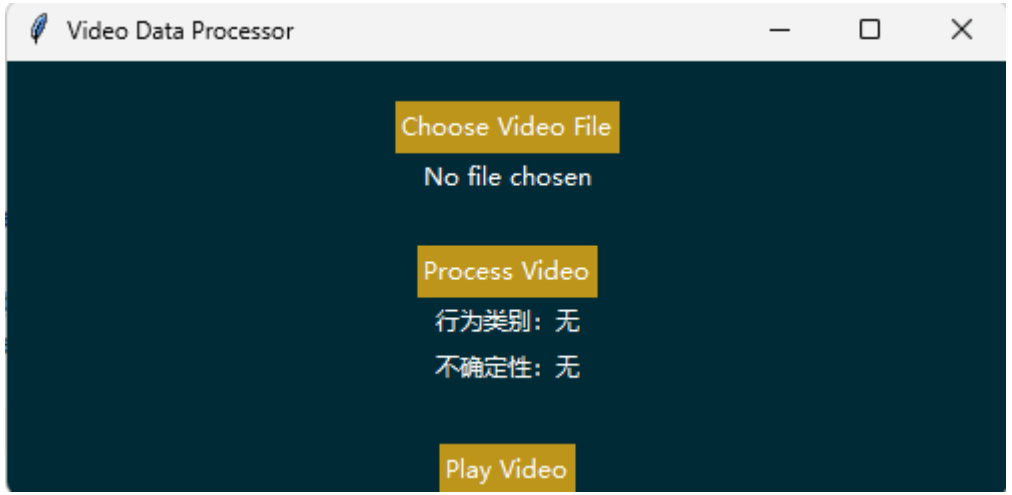
实验目标是区分那些属于已知数据分布内的样本和那些属于未知数据分布外的样本。这与基线方法，如蒙特卡洛Dropout （MC Dropout） 和贝叶斯神经网络的随机变分推断 （BNN SVI）类似，它们都利用模型的不确定性来作为评估样本是否为OOD的指标。DEAR方法结合了EDL不确定度，能够更有效地识别出OOD样本。

具体来说，与那些仅采用L_{EDL} 进行模型训练的标准DEAR方法相比，IND和OOD的不确定性分数更加分离，重叠区域更少，这表明了对OOD样本的不确定性有更高的估计，从而提高了检测性能。这些结果不仅在数字上显著，而且在视觉呈现上也清晰可见，进一步证实了实验方法的有效性。



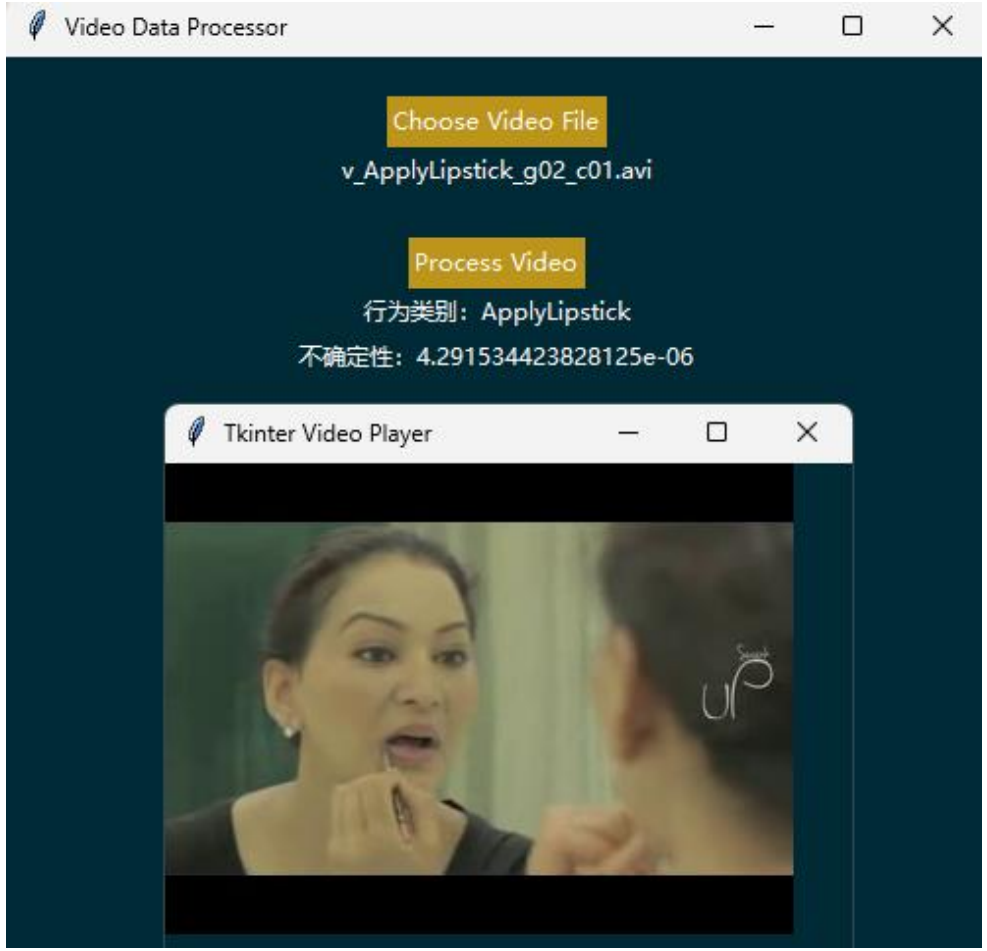
基于不确定性的分布外检测

可视化界面

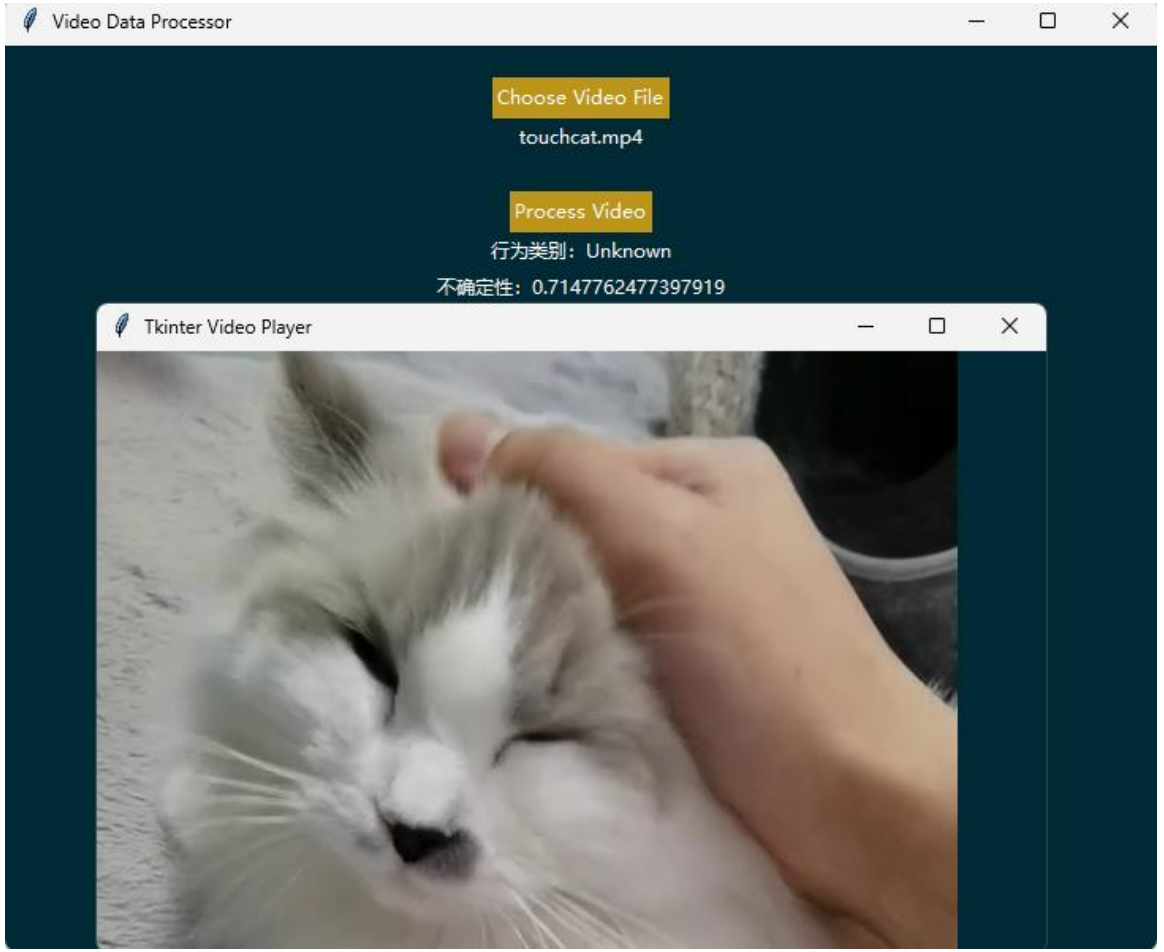


可视化界面如图所示，点击按钮“Choose Video File”可以打开文档选择想要处理的视频文件（支持的格式包括.mp4，.avi，.mov，.mkv），地址信息会保存在一个txt文件中，按钮下方的“No file chosen”在选择完文件后，自动替换为文件地址，这个时候点击按钮“Process Video”，系统会调用已经训练好的模型，对视频文件预处理成可输入的数据并输出视频文件的预测类型和不确定性，下方按钮“Play Video”可播放选择的视频文件。

可视化界面



a. 输入已知类视频



b. 输入未知类别的视频

成果简介

- 证书：
  （1）大学英语六级：576
- 竞赛：
  （1）2023年美国大学生数学建模竞赛MeritoriousWinner（一等奖）
  （2）第十三届蓝桥杯全国软件和信息技术专业人才大赛江苏赛区三等奖
  （3）第十三届全国大学生数学竞赛（非数学类）三等奖
  （4）二零二二年高教社杯全国大学生数学建模竞赛本科组江苏赛区三等奖
  （5）江苏省高等学校第十八届高等数学竞赛本科一级A组三等奖
  （6）南京邮电大学2021年大学生高等数学竞赛本科一级A组二等奖
- 荣誉：
  （1）2021-2022学年二等奖学金
  （2）2021-2022学年三好学生


2023
Mathematical Contest In Modeling
Certificate of Achievement
Be It Known That The Team Of
Zhihao Zhang
Jia Cai
Zihan Xu
With Faculty Advisor
jianxin Dai
Of
Nanjing University of Posts and Telecommunications
Was Designated As
Meritorious Winner


荣誉证书
NO. 2022SH0316
徐梓涵 同学（ B20031626 ）：
在 2021 / 2022 学年中，被评为“三好学生”，特发此证，以资鼓励。
Mr./Ms._____,
You have obtained the Best Student Award for your excellent performance in the 2021/2022 academic year. This certificate of commendation is hereby awarded to you as encouragement.
南京邮电大学
2022年9月


获奖证书
南京邮电大学 徐梓涵 荣获第十三届全国大学生数学竞赛（非数学类）三等奖，特发此证。
编号：CMS（苏）F20212607

Thank you for listening!