《模式识别与机器学习》课程研究项目 2025：

基于 Yale 数据集的人脸识别与拒识系统

一、项目背景与目标

人脸识别是模式识别领域的经典问题，具有重要的理论意义和广泛的应用价值。本项目中，你们将在经典的 Yale 人脸数据集上，构建一个完整的人脸识别系统。该系统不仅需要能够识别已知个体，还需要具备“拒识”（rejection）能力，即能够判断输入的测试人脸是否来自数据集中的已知个体，若否则应拒绝识别。这更符合实际应用场景中系统需要面对未知人员的情况。

核心目标：

1. 实现一个能够对 Yale 数据集中已知个体进行准确识别的人脸识别算法。

2. 为该算法增加“拒识”功能，使其能够有效判断测试样本是否属于数据集外（Out-of-Distribution, OOD）的人脸。

3. 深入理解并比较传统机器学习方法与深度学习方法在该任务上的性能、复杂度和优缺点。

4. 撰写一份结构清晰、分析深入的项目报告，展示你的设计思路、实验过程和结论。

二、数据集

1. 主数据集 Yale Face Database

网址：http://cvc.cs.yale.edu/cvc/projects/yalefaces/yalefaces.html

2. 外部测试集（用于测试拒识能力）

- 方案 A（推荐）：从其他人脸数据集中选取部分人物图像，如 ORL、CroppedYaleB 数据集的部分子集。
- 方案 B：在互联网上谨慎收集少量非 Yale 数据集中的人脸图像（需确保版权合规，并处理为与 Yale 数据集相似的灰度、尺寸和背景）。

- 目的：用于模拟“未知人员”，评估系统拒识性能。

三、项目任务与要求

任务 1：数据预处理与特征工程（基础部分）

(1)读取并可视化 Yale 数据集，理解其结构。

(2)设计并实现数据预处理流程，可能包括：人脸检测与对齐（若使用，需说明方法）、图像尺寸归一化、灰度归一化、直方图均衡化等。

(3)**（传统方法路径）**若采用传统方法，需设计并实现特征提取方案，例如：全局特征（PCA、LDA）、局部特征（LBP、HOG 等）、对特征进行可视化分析。

(4)**（深度学习方法路径）**若采用深度方法，需设计数据增强策略（如用于训练的小幅度旋转、平移、噪声添加等），以增加模型鲁棒性。

任务 2：识别与拒识算法设计与实现（核心部分）

(1)构建识别模型

①传统方法：采用合适的分类器（如 SVM、k-NN、贝叶斯分类器等）在提取的特征上进行训练。需详细说明分类器选择理由及参数调优过程。

②深度学习方法：设计或选用一个卷积神经网络模型。

- **方案 A（特征提取+分类器）：**使用预训练模型提取深度特征，然后使用传统分类器进行识别。
- **方案 B（端到端训练）：**在 Yale 数据集上微调一个预训练人脸识别网络（如 FaceNet, VGGFace, ResNet-based models），或从头搭建训练一个小型 CNN。
- 需详细说明网络结构、损失函数（如交叉熵、Triplet Loss 等）、优化策略。

(2)实现拒识机制

①阈值法：为识别模型的输出（如分类概率、与最近邻的距离、相似度得分）设定阈值。低于阈值则判为“未知”。

②密度估计法：使用一类分类（One-Class Classification）模型，如 One-Class SVM、高斯混合模型，对已知类进行密度估计。

③基于深度置信度的方法：对于深度学习模型，可研究利用 Softmax 置信度、预测熵，或基于特征空间距离（如与类原型的距离）来构建拒决策略。

④单独训练一个二分类器：将“已知类”视为正样本，“未知类”（来自外部测试集）视为负样本，训练一个二分类器来判断是否属于已知集。

⑤要求：必须实现至少一种拒识机制，并分析其原理和阈值选择策略。

任务 3：实验设计与性能评估（分析部分）

（1）数据集划分：对 Yale 数据集进行合理的训练集/验证集/测试集划分（如按人物 ID 分层划分）。确保测试集中的人物在训练集中已出现。

(2)评估指标

①识别性能：在已知类测试集上，报告准确率、精确率、召回率、F1-score 及混淆矩阵。

②拒识性能：在包含外部测试样本的混合测试集上，报告：**已知类的召回率**，系统正确接受已知类样本的比例；**未知类的拒绝率**，系统正确拒绝未知类样本的比例；**ROC 曲线与 AUC 值**，以“属于已知类”为正例绘制。

(3)对比与分析

系统分析算法在光照、表情变化下的稳定性；对比不同拒识机制的效果；如果时间允许，鼓励对传统方法和深度学习方法进行对比实验，并从模型大小、训练时间、识别精度、拒识能力、可解释性等多角度进行讨论。

四、项目提交资料

1.完整代码（仅提供电子版）：包含数据预处理、模型训练、评估和可视化所有步骤的、注释清晰的源代码（Python 为主）。需提供独立的 README 文件说明运行环境依赖和步骤。

2.项目报告（PDF 格式，**提供电子版和纸质版**），**使用研究生院相关模板。**报告内容包括：

- **标题、姓名、学号。**
- **摘要：**简要概述项目目标、方法、主要结果和结论。
- **引言：**阐述项目背景、意义及任务定义。

- **相关工作**：简要介绍所选用的核心算法及相关研究。
- **方法**：详细描述你的算法流程，包括预处理、特征提取、模型构建、拒识策略等。
- **实验**：详细说明实验设置、数据集划分、评估指标、参数设置和对比实验设计。
- **结果与分析**：通过图表展示结果，并对结果进行深入讨论和分析。
- **结论**：总结项目工作，指出创新点与不足，并提出可能的改进方向。
- **参考文献**。

五、时间安排建议

2026 年 1 月 5 日前，以班级为单位提交。

六、评分标准

- **算法实现与完整性（40%）**：代码能否正确运行，是否实现了所有核心要求（识别+拒识），代码质量与结构。
- **报告质量（30%）**：报告结构的完整性、逻辑的清晰性、分析的深度、图表的规范性。
- **创新性与深入性（20%）**：是否在方法选择、对比实验、结果分析等方面体现出独立思考与深入探索。
- **复现与文档（10%）**：README 清晰，环境与依赖明确，结果可复现。

请独立完成项目，鼓励交流思路，但代码和报告必须原创。