鉴别伪造图片

人工智能思维与伦理课程

2021.09

鉴别伪造图片

真实图片

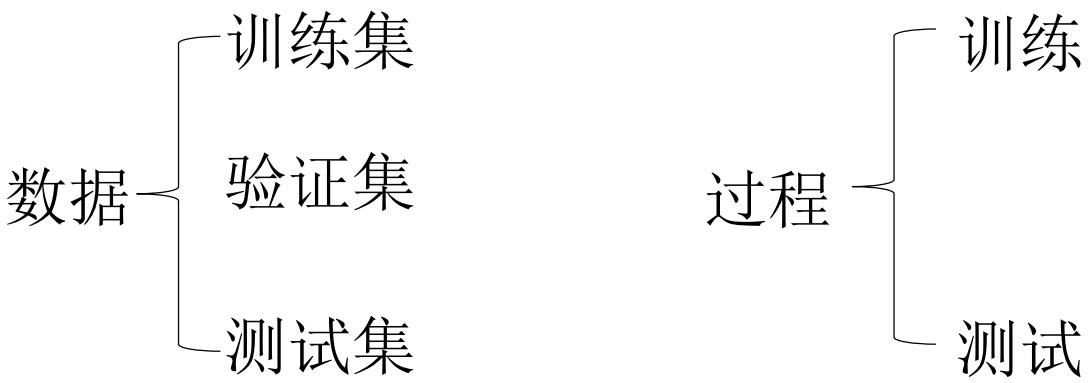
伪造图片

流程

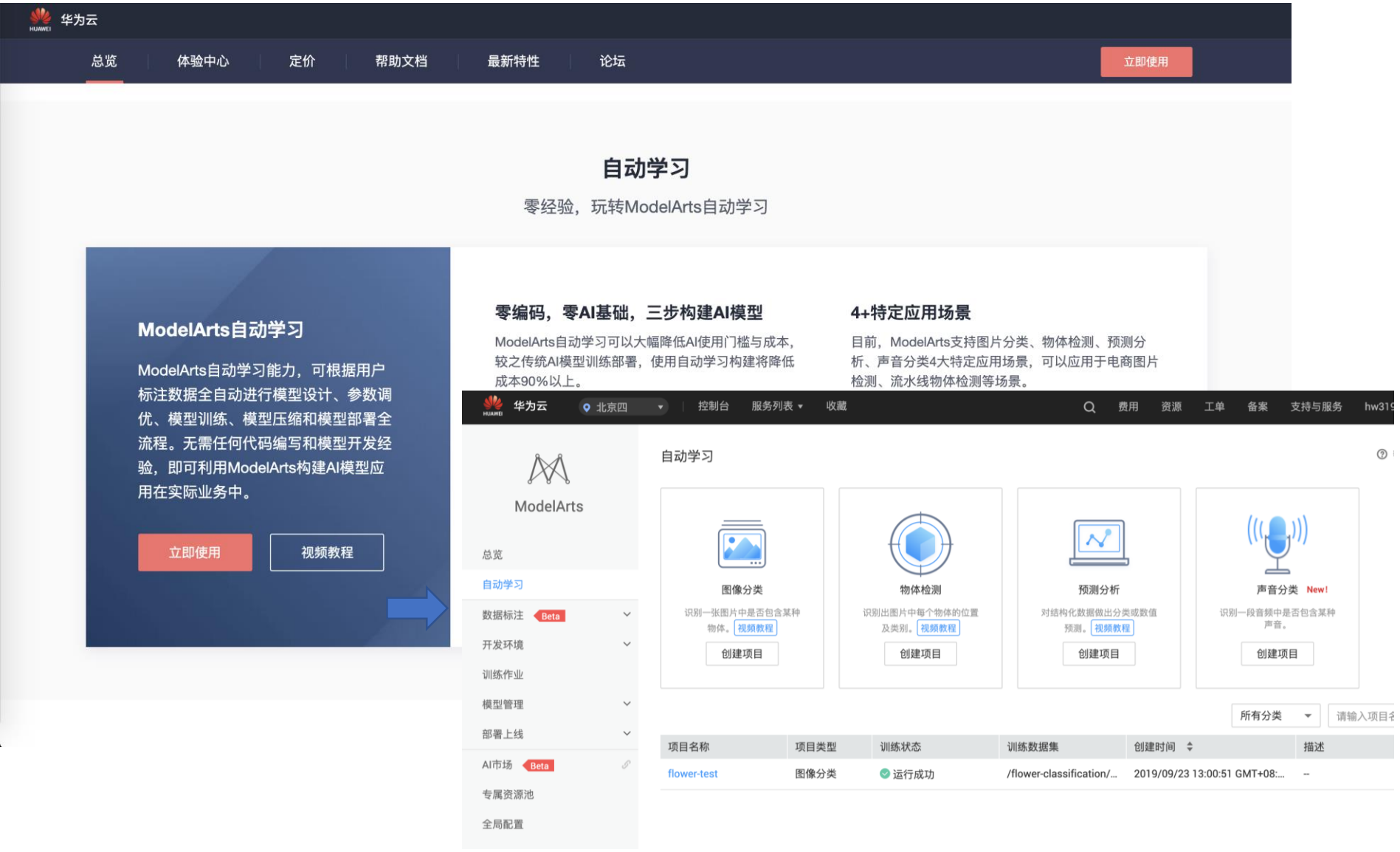
- 从百度网盘下载Casia数据集。real文件夹包含800张真实图片，fake文件夹包含462张伪造图片。网盘链接：https://pan.baidu.com/s/1lb9YPp24t5xhLmHFgAUDrw 提取码：46s9
- 采样若干张真实图片和伪造图片（比如400张真实图片，400张伪造图片）作为训练集(其中一部分会被划归为验证集)，其他图片作为测试集。
- 分类任务demo:

  https://bbs.huaweicloud.com/videos/58cae67982ba42efa806df5d6b9569d8

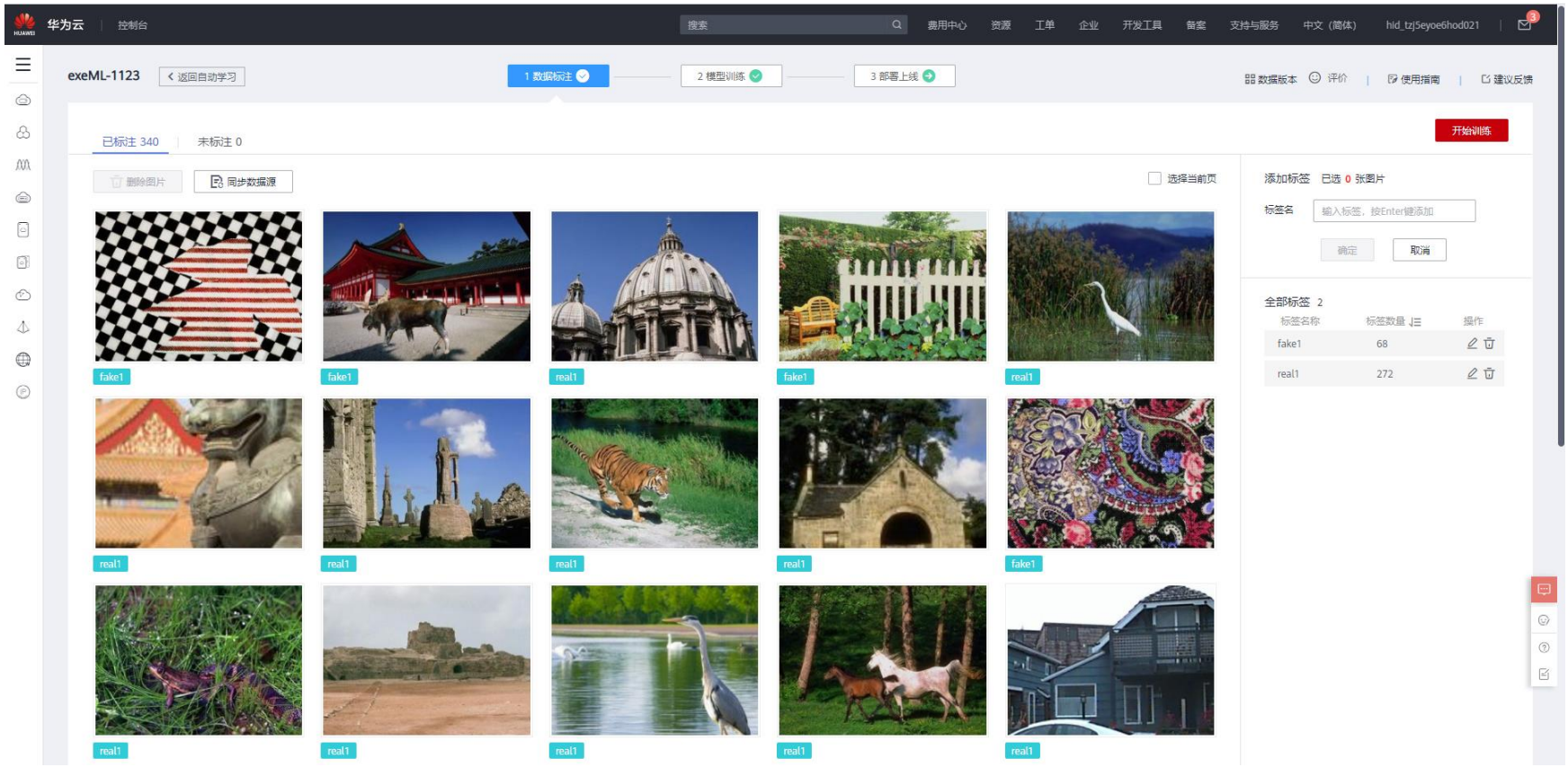
流程



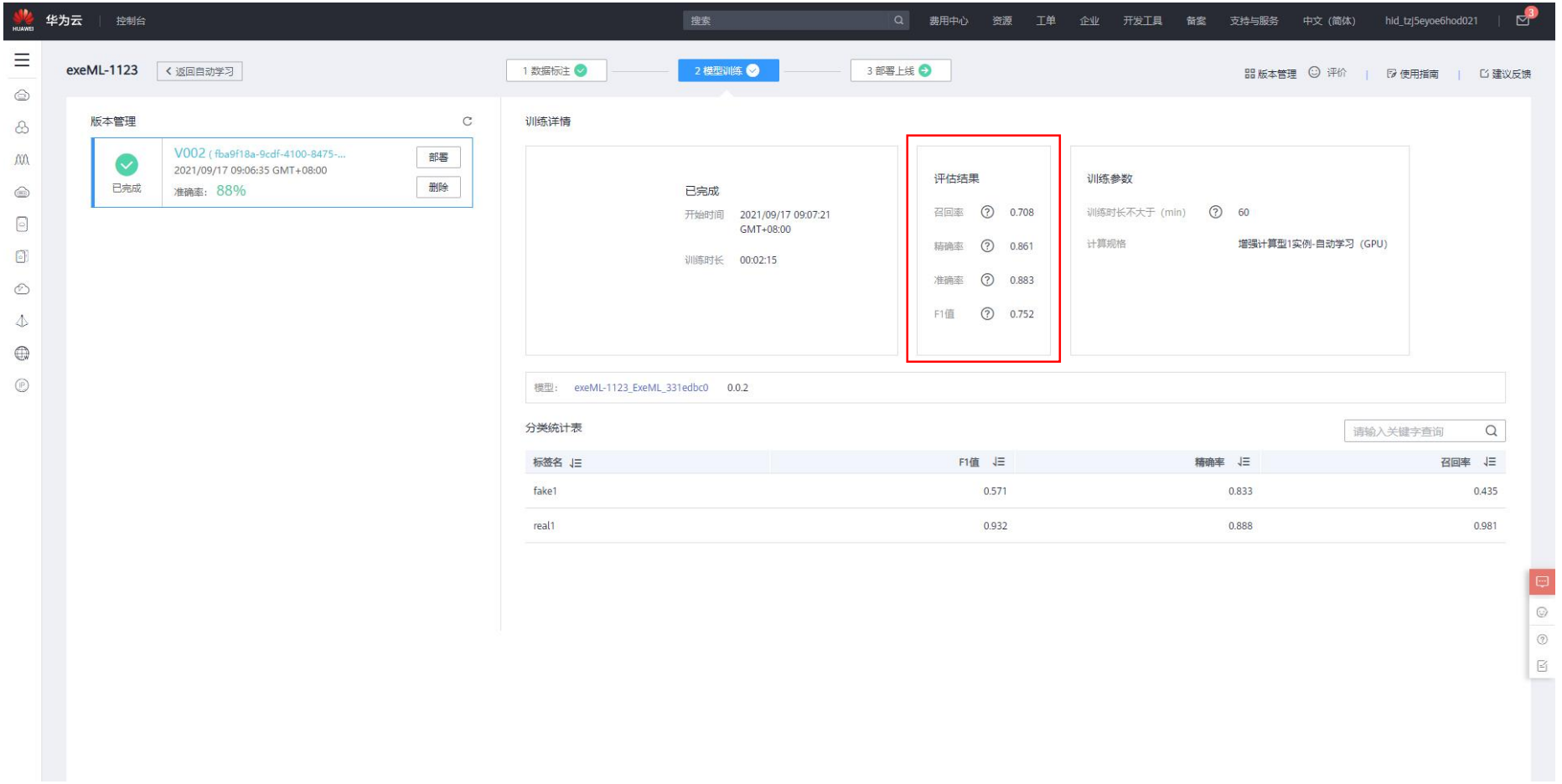
1. 进入华为云ModelArts->自动学习界面，选择图像分类
   https://www.huaweicloud.com/product/modelarts.html



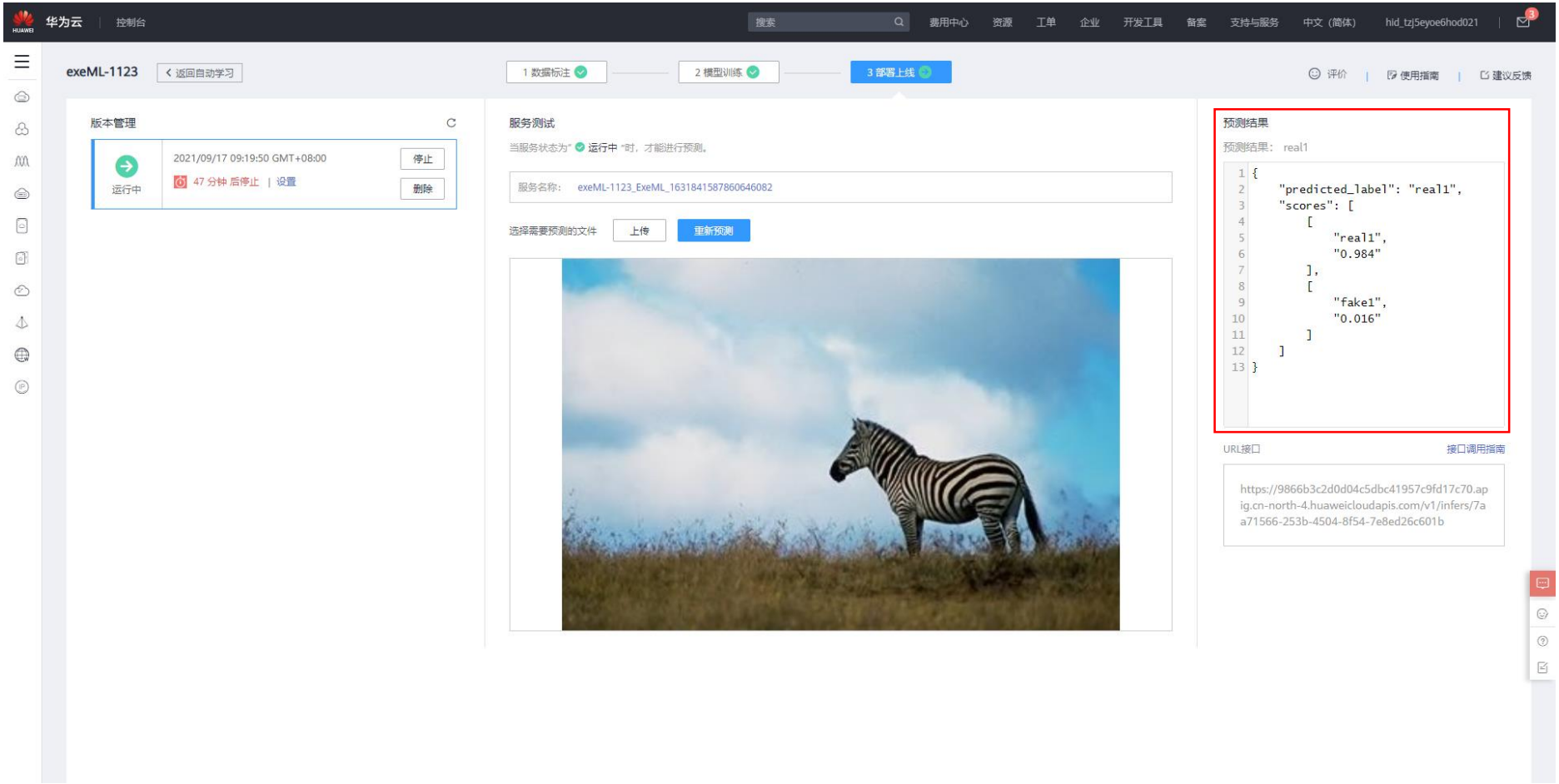
2. 上传数据后，标注数据，点击开始训练。



3. 训练完成后查看训练结果并部署测试



4. 上传测试图片（也可以是自己PS的图片）



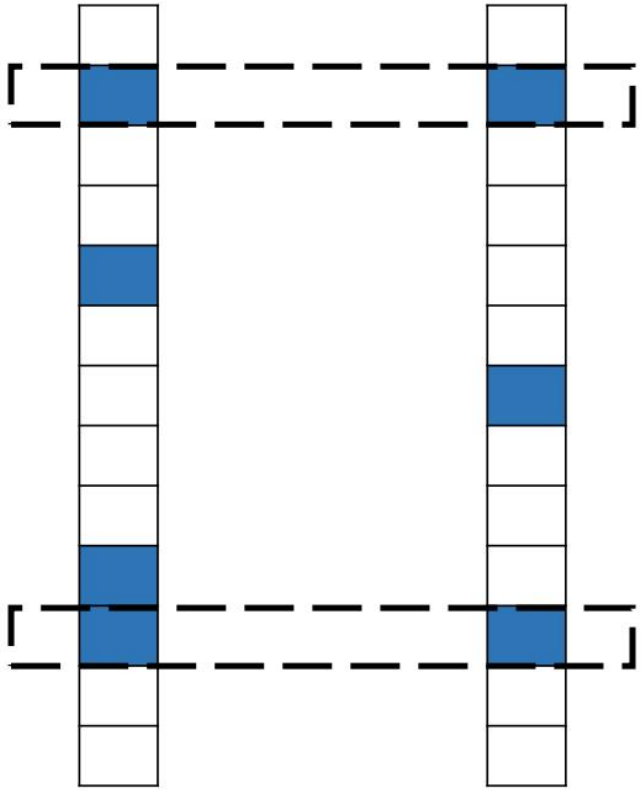
要求

- 理解召回率(recall),精确率(precision),准确率(accuracy), F1值(F1-score)的含义。
- 尝试使用不同数量的训练图片，尝试用不同比例的真实图片和伪造图片，观察并分析验证集(validation set)上的性能。
- 观察并分析测试图片的预测结果，总结失败案例(failure case)。
- 提交至少5页A4纸，五号字体（12pt）的实验报告，pdf格式。

要求

:1 伪造图片　　:0 真实图片

ground-truth $\mathbf{y}$　　predicted $\tilde{\mathbf{y}}$



精确率(precision): $\frac{|\mathbf{y}\cap\tilde{\mathbf{y}}|}{|\tilde{\mathbf{y}}|} = 0.66$

召回率(recall): $\frac{|\mathbf{y}\cap\tilde{\mathbf{y}}|}{|\mathbf{y}|} = 0.5$

F1值(F1-score): $\frac{2|\mathbf{y}\cap\tilde{\mathbf{y}}|}{|\mathbf{y}|+|\tilde{\mathbf{y}}|} = 0.57$

$$F_1 = \frac{2}{\frac{1}{\text{Precision}} + \frac{1}{\text{Recall}}}$$ 调和平均