

Deepfake 检测及活体检测实验报告要求

一．实验目的

实现论文提出的方法，检验该方法用于 Deepfake 检测或活体检测中达到的效果

二．实验要求

1. 要求学生在多个伪造人脸或攻击人脸数据集上实验收集实验数据（可网上找源码并调试实现，常用 Deepfake 伪造人脸数据集包括 FaceForensic++，Celeb-DF，DFDC；常用活体检测攻击人脸数据集包括 OULU-NPU，ReplayAttack，CASIA-MFSD）
2. 根据实验数据绘制数据表（如准确率，AUC，ACER），ROC 曲线，loss 函数，提供必要的实验输出数据（如图像示例，识别效果图等）
3. 比较已有的优秀方法，评估该方法在 Deepfake 检测或活体检测中表现
4. 保存实验源码及实验数据并同实验报告一同上交

三．实验步骤

1. 学习文章的算法原理
2. 设计编程算法（可网上找源码），调试并实现文章的方法
3. 收集实验数据，并绘制可视化数据图表
4. 比较实验效果，得出结论

四．实验结果

根据实验数据，绘制数据图表。例子如下：

数据表（保存 excel）：

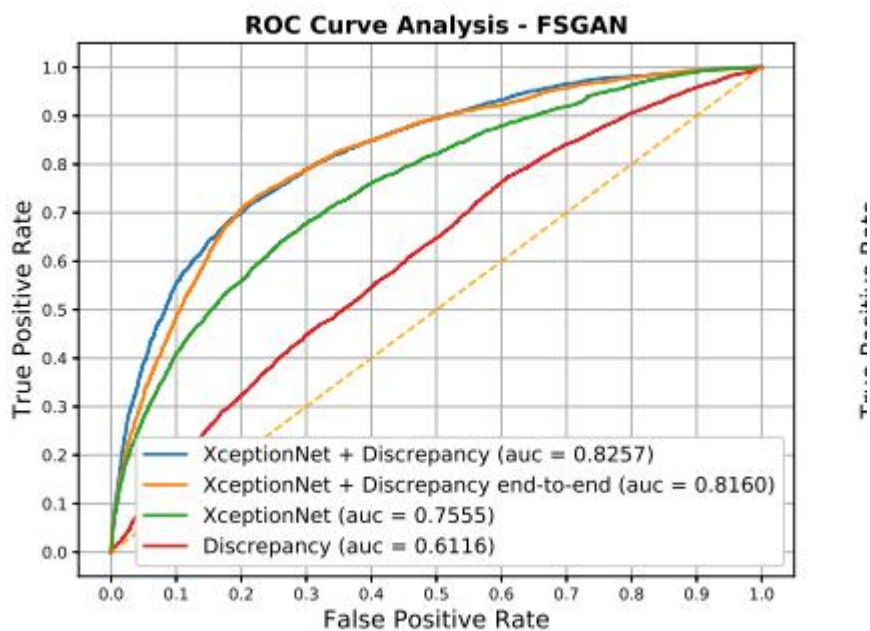
同种方法在不同数据库上的表现效果：

test on	train on sub-datasets				train on ALL dataset					
	DFD	DF	F2F	FS	DFD	DF	F2F	FS	ALL	DFDC
Bayer and Stamm [3]	0.52	0.503	0.505	0.505	0.501	0.52	0.503	0.505	0.5	0.5
Inception ResNet V1 [52]	0.794	0.783	0.788	0.778	0.919	0.638	0.566	0.462	0.774	0.597
Xception [9]	0.98	0.995	0.985	0.98	0.965	0.984	0.984	0.97	0.978	0.612
MesoNet [1]	0.804	0.979	0.985	0.995	0.958	0.822	0.813	0.783	0.909	0.745
DeepRhythm (ours)	0.987	1.0	0.995	1.0	0.975	0.997	0.989	0.978	0.98	0.641

不同方法在同一数据库上的表现效果：

S.No.	Methods	Datasets		
		DF-TIMIT [27]		DFDC [17]
		LQ	HQ	
1	Capsule [35]	78.4	74.4	53.3
2	Multi-task [34]	62.2	55.3	53.6
3	HeadPose [46]	55.1	53.2	55.9
4	Two-stream [50]	83.5	73.5	61.4
5	VA-MLP [32]	61.4	62.1	61.9
	VA-LogReg	77.0	77.3	66.2
6	MesoInception4	80.4	62.7	73.2
	Meso4 [9]	87.8	68.4	75.3
7	Xception-raw [38]	56.7	54.0	49.9
	Xception-c40	75.8	70.5	69.7
	Xception-c23	95.9	94.4	72.2
8	FWA [30]	99.9	93.2	72.7
	DSP-FWA	99.9	99.7	75.5
Our Method		96.3	94.9	84.4

ROC 曲线图：



提供实验相关的数据。

五．结论

综合对比已有的方法及达到的效果，总结文章提出的方法的表现效果。