4.人脸识别 核心问题：技术框架、用户痛点、算法模型、开源项目

主要从人脸识别的技术框架、人脸识别的当前发展的用户痛点以及人脸识别主要的算法模型和开源的人脸识别项目这四个方面内容进行系统性的介绍。

章节目标

1）了解人脸识别的技术框架

2）了解人脸识别的技术痛点

3）了解人脸识别的算法模型

4）熟悉人脸识别的开源项目

了解人脸识别的技术框架，主要是分析当我们要去做人脸识别项目的时候，应该从哪几个方面去考虑；了解人脸识别的技术痛点，重点是考虑当前人脸识别技术发展的现状，主要是和当前这个行业的技术标准去对齐我们自身的项目；了解人脸识别的算法模型，介绍当前主流的算法模型；对开源项目的介绍，主要是希望大家能够有一个可以直接入手训练的项目，并且在后续自己的实践项目中有可供参考的内容。课程目标就是“三个了解一个熟悉”。

4.1人脸识别的技术框架

通常，人脸识别技术涵盖了三个方面的内容：人脸检测、人脸对齐和人脸验证。

1）人脸检测。指在一个视频里面或是在一张图片里面，把与人相关的内容区寻找出来。比较形象的表述就是，在一张图像里面，我把人脸用一个聚焦框把它框出来，这就是一个人脸检测的过程。

2）人脸对齐。我们知道，人是一个动物，它的脸在不同的时间点上它的运动状态是不一样的，所以，根据它姿态的差异，当你想对人进行后续识别的时候，就需要对人的姿态进行校正，这样才能保证后面的识别准确率。这就涉及到人脸对齐。

3）人脸验证。包括几个场景：1:1验证、1：n验证。1:1的验证是指找到一个人，它对应那样的一个人。1：n是指在n个人里面找到目标要查询的那个人。

以上三个方面就是人脸识别的主要技术框架，其实，它们在背后采用的技术也是不同的。

4.2人脸识别的技术痛点：活体检测

在2017年“3.15”时，曾经有一个事件报导，百度的人脸识别技术，包括阿里的人脸识别技术都存在一个同样的问题，在活体检测方面存在屏障。具体讲，就是人脸识别摄像头放在那里，当人通过的时候，如果刷自己的脸是可以被正确识别的，但是当我们拿一张照片过去，拿一张它认识的人的照片过去，平面的，同样的机器没有办法区分出人和照片，会让手持照片的人通过。这就带来一个问题，如果有一个人带了你的照片，然后去做支付的时候，他花的将是你账户里面的钱。所以，当时3.15这个事情闹得还是蛮凶的。后来，不同的公司都在做各种澄清和漂白。其中印象比较深的是支付宝，它说我的人脸支付只是手段之一，同时我还要求输入手机号或者是密码的。其实，这也等于变相认可了3.15暴露出来的问题，就是说，在非真人的情况下，人脸识别技术会存在被欺骗的可能。这也是人脸识别的一个技术痛点，称之为活体检测。

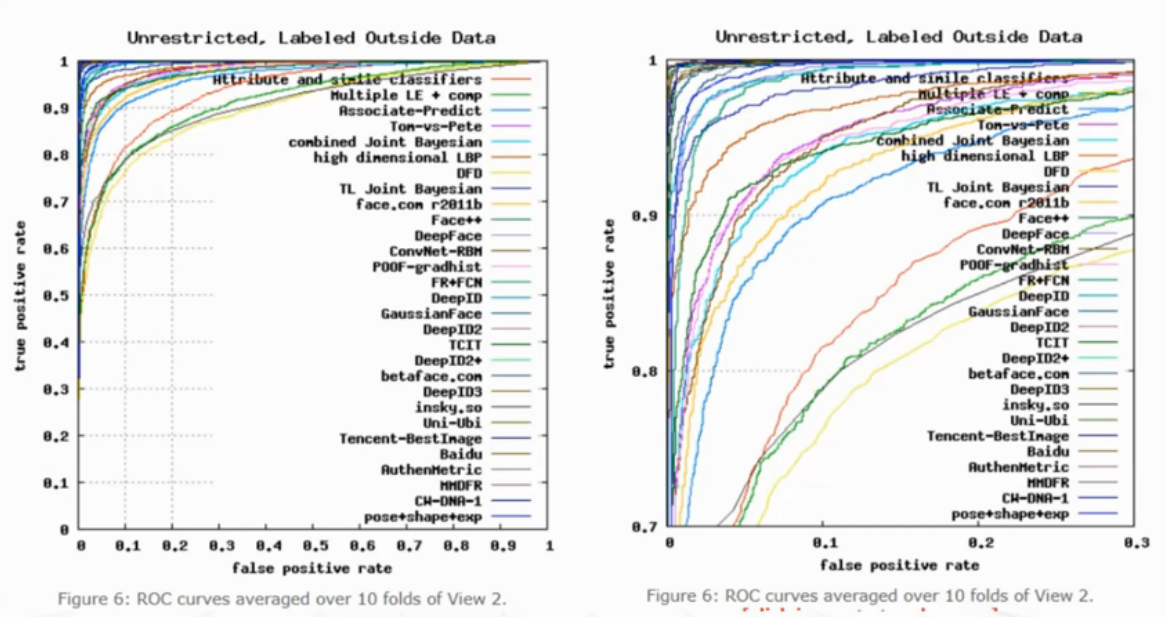
4.3人脸识别的算法模型

以下两张表来自ABCnet组织的人脸识别竞赛项目。近几年来，它有不同的算法模型，这种算法模型基于特定的人脸识别样本会做相应的竞赛。左边一列是算法模型，右边一列是对应的算法识别率。在表中可以看出，前期的准确率一般在84%-85%，到后期基本达到99%左右。当然这里面有很多公司，包括face++，另外还有一套算法模型叫做DeepID,还有baidu，



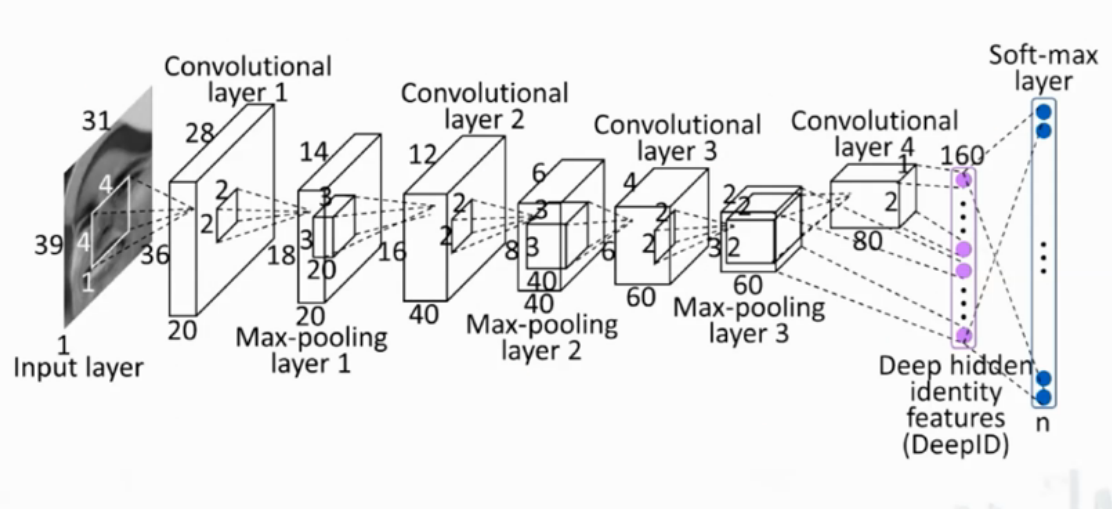
这些参赛组织或模型，都是我们后续可以作为学习和参考的资源。因为，这些算法模型会公布它的算法原理和逻辑，在开源社区里面会有一些这样相应模型算法的实现。针对这样相应算法的实现，我们完全可以把它复用到我们的场景里来。这个时候，我们需要做的是增大训练样本的训练量，然后基于这个样本的训练量来训练自己的模型，再基于自己的模型适配到自己的真实场景里来。

看一下人脸识别模型的发展情况，一图是识别准确率情况，对应了不同的算法模型识别准确率情况，真实准确率和失败准确率。



基础的模型DeepID

DeepID是近几年认可度和效果取得比较好的一套机器视觉模型，它本身分为3个版本DeepID1、DeepID2和当前采用的DeepID3。它采用的主要是卷积神经网络，从前面的input层到中间的卷积层，再到池化层。池化层采用的是最大池化算法。卷积层采用等价变换，最后输出它的适配结果。这个模型的细节，网上有很多的论文和资料可供学习和下载。后续再讲人脸识别的时候会单独对DeepID进行专门的课题介绍，另外关于它的算法原理和实现基础，和它的实践应用都会做深度介绍。作为产品经理这门课，我们了解到有这么一套东西就可以了。这里算是做一下抛砖引玉。



4.4人脸识别的开源项目



开源项目一般是指两个因素，一方面是指开源的人脸识别资源库，即人脸库，另外一方面是指开源的人脸识别的算法模型。表中列出了很多当前比较主流的开源人脸识别资源库，包括WebFace、LFW。然后，这些都是可以作为我们训练人脸识别时可以采用的输入数据资源，可自行下载。开源框架可选择tensorflow、caffe。

4.5想一想：计算机视觉技术还有哪些潜在应用？

技术回顾：主要讲了什么是人脸识别，人脸识别当前的技术瓶颈以及人脸识别当前的主要算法模型和开源资源，需要思考当前的计算机视觉技术还有哪些潜在的应用？我们讲人脸识别、人脸支付都是典型的应用，但是它们只是计算机识别的一部分，还包括很多方面可以探寻。