机器如何识别人脸？

大家对“刷脸”已经司空见惯了，刷脸进站，刷脸取钱，刷脸购物...靠一张脸走遍天下的日子已经离我们越来越近了。那么，机器是如何识别人脸的呢？

从物理角度，机器通过摄像头看到的人脸只不过是一堆像素点，如图 1 所示。在这幅图里，眼睛、鼻子、嘴都是由浓淡不一的点组成。人的视觉系统可以从这堆点里轻松发现五官的形貌，但机器就很困难。怎么办呢？人们首先想到的是帮助机器把这些五官特征抓出来，比如两只眼睛之间的距离、唇部和鼻子的相对位置等等。有了这些“特征”，机器就可以建立分类模型，把不同的人脸区分开了。

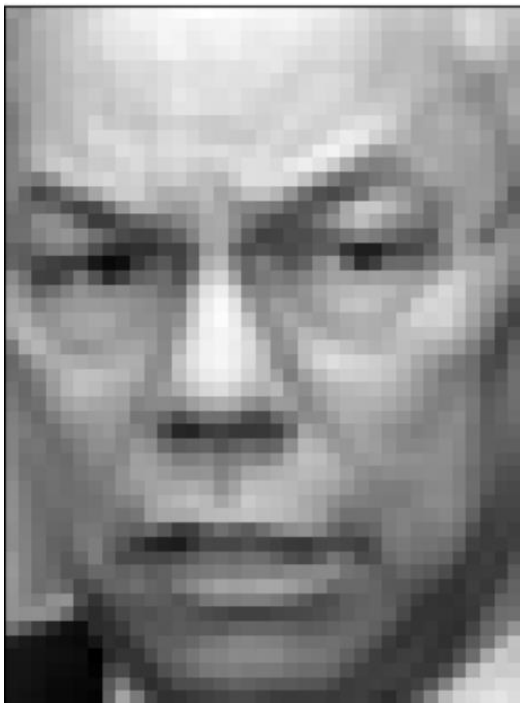

图 1：由一堆像素点组成的人脸图片[1]

图 2：提取出五官特征，再基于这些特征进行人脸识别的方法[1]

这种特征提取很辛苦，因为我们并不知道哪些特征更有效果，只能凭经验尝试。后来，人们发现利用深度神经网络可以将那些最有效的特征提取出来。如图 3 所示，经过一个神经网络，首先得到的是一些线条特征，然后是五官的局部特征，最后是整个脸的特征。研究人员发现，这种从局部到整体的特征学习方式和人的视觉系统很相似，这意味着机器可以通过类人的方式来“察颜观色”了。

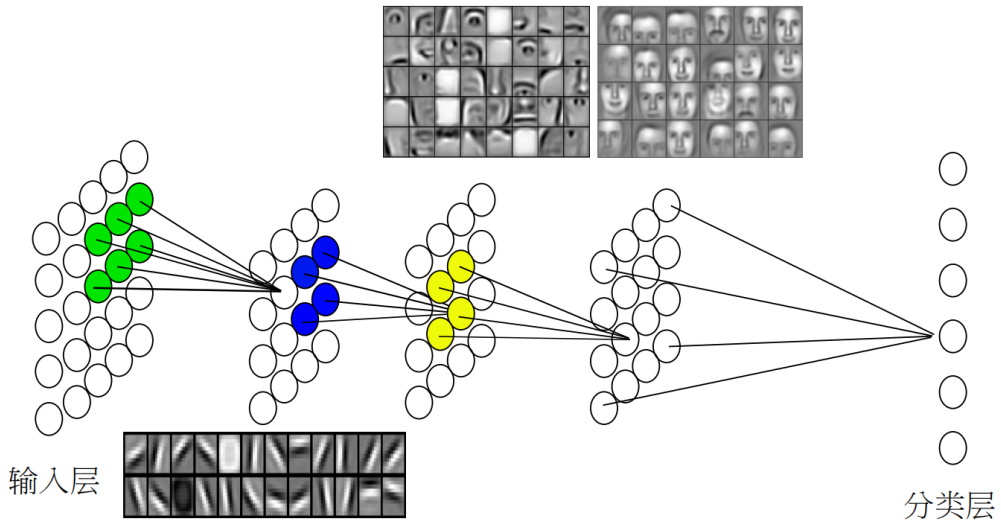

图 3：利用深度神经网络，逐渐学习人脸特征[1]。

利用深度神经网络来识别人脸取得了非常高的精度，但也不是没有问题。例如，由于神经网络内部很复杂，因此很难判断它是如何把一个人识别出来的，如果识别错了也很难说清楚理由。有人就利用这种“黑箱”特性设计了一种攻击手段，如图 4 所示，只要戴上一个特制的眼镜，就可以让机器把自己认成另外一个人。如何对系统行为进行控制并防范可能的恶意攻

击，是研究人员正在努力解决的问题。

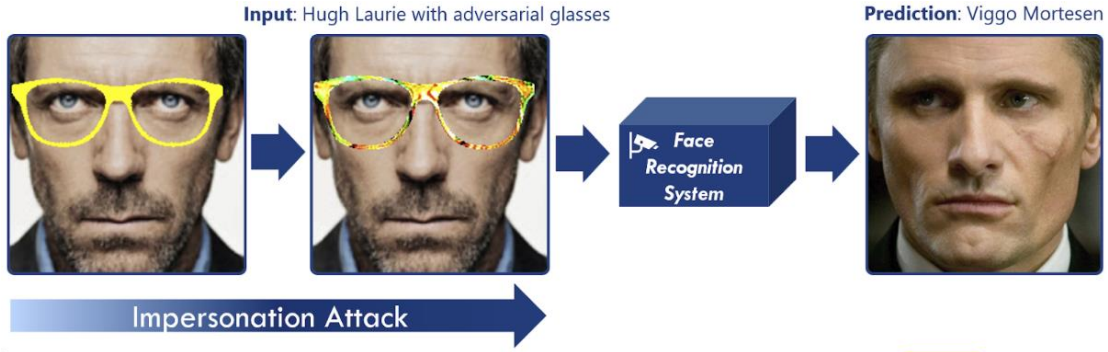

图 3：戴上一个眼镜后，可以骗过人脸识别系统[2]

[1] 王东，“人工智能”，清华大学出版社，2019.10

[2] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, “Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition”, 2016