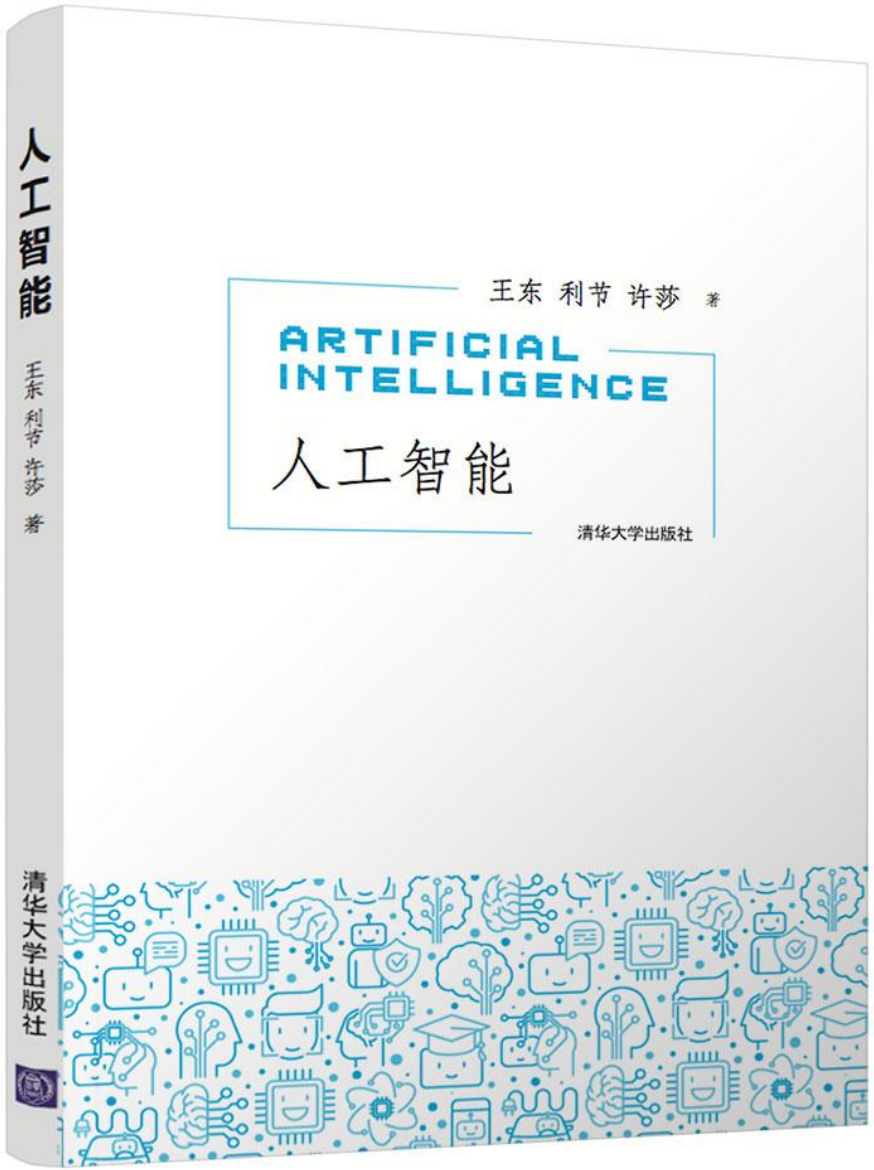
人工智能

王东 & 利节 & 许莎



- 教材名称：人工智能
- 出版社：清华大学出版社
- 作者：王东 利节 许莎

本课程应具备的能力：

- Linux下的基本操作
- python语言基础知识

资源下载：

http://aibook.cslt.org/

认识你的脸

汤志远

改编自利节/王东版本

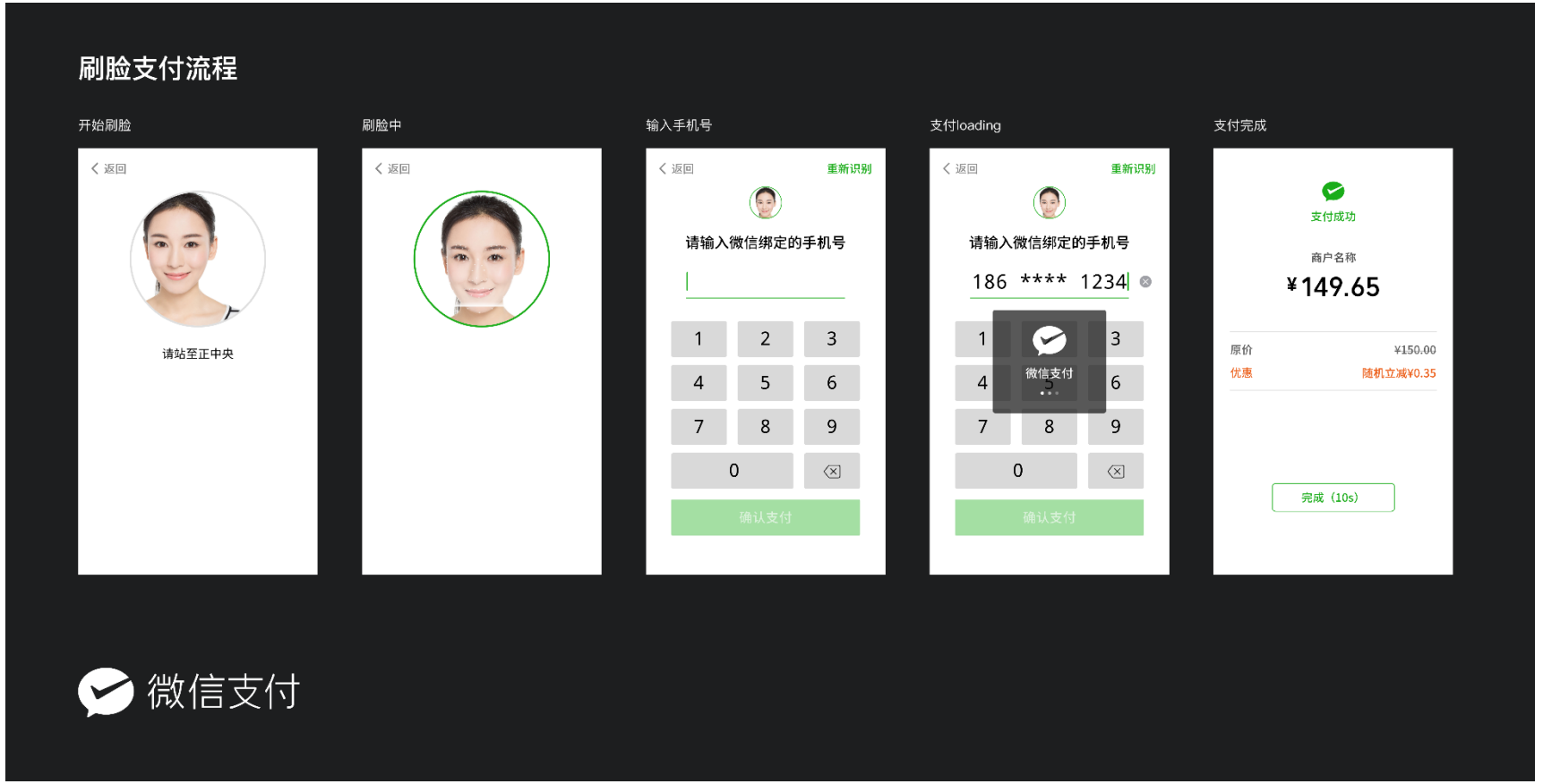
授课提示

1. 本课件60页，建议授课时间180分钟，每页平均3分钟。重点可放在“基于特征脸的人脸识别”和“基于深度学习的人脸识别”两部分内容，以提高学生对常用人脸识别技术相关概念的了解。
2. 若授课时间为90分钟，请去掉非课本内容，对“附注”中所提内容尽量简化，并对具体的技术细节进行缩减。
3. 课件内的视频具有较好的展示效果，可视授课时间长短决定取舍。
4. 建议教授过程中关于“人脸识别技术给生活带来了哪些影响”、“未来的人脸识别技术应用可能有哪些”这一问题进行讨论，激发学生思考。

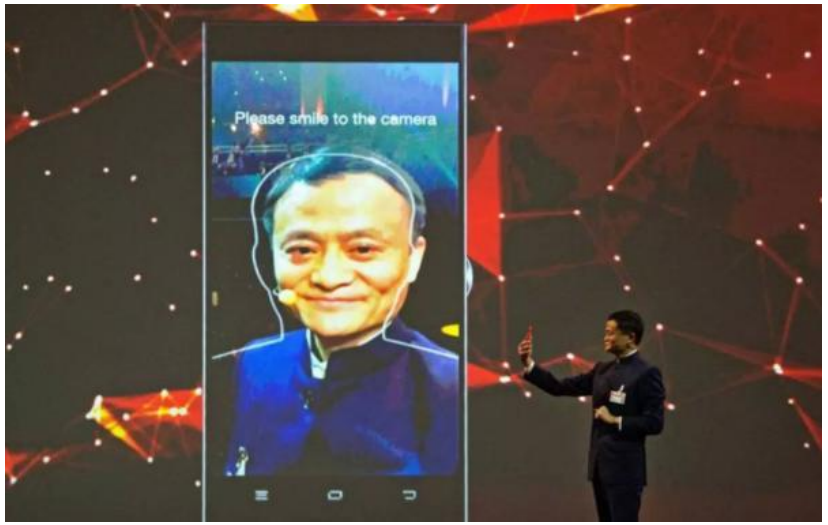
目录

目录

人脸识别概述--什么是人脸识别



人脸识别概述--什么是人脸识别



人脸识别概述--什么是人脸识别

人脸识别概述—隐私安全

- 旧金山禁用人脸识别技术
- 人脸识别第一案：“要脸”or“要安全”？
- 变脸软件ZAO因为隐私问题被工信部约谈

…

工信微报 V

今天 09:52 来自 微博 weibo.com

【工信部就“ZAO”App网络数据安全问题开展问询约谈】9月3日，针对媒体公开报道和用户曝光的“ZAO”App用户隐私协议不规范，存在数据泄露风险等网络数据安全问题，工业和信息化部网络安全管理局对北京陌陌科技有限公司相关负责人进行了问询约谈，要求其严格按照国家法律法规以及相关主管部门要求，组织开展自查整改，依法依规收集使用用户个人信息，规范协议条款，强化网络数据和用户个人信息安全保护。同时，要进一步加强新技术新业务安全评估，切实采取有效措施，积极防范自有业务平台被利用实施电信网络诈骗等风险隐患。

工业和信息化部网络安全管理局将进一步加大工作力度，指导督促相关企业切实履行法律责任，认真做好网络数据和用户个人信息安全保护、行业电信网络诈骗防范治理等工作。 收起全文

人脸识别概述—相关公司

2017 人脸识别技术企业排行榜 TOP20

排名	名称	用途
1	商汤科技	与京东、银联、招商银行、拉卡拉、融360等均有合作；布局智慧城市安防项目；智能视频方面，SenseFace 人脸布控系统已开始广泛落地；以图搜图的图腾系统，已应用在广州、重庆、河北等地的公安局；Faceu 应用 SenseAR 增强现实感引擎；人像背景虚化功能、智能相册中的人脸聚类功能应用在 OPPO、小米等手机。
2	旷视科技	为支付宝客户端提供人脸登录功能支持；为公安部第一研究所提供“网上身份证”人脸识别技术支持；为美图旗下产品提供技术支持；通过人脸识别技术对司机身份进行核验应用到 e 代驾、易到用车、神州租车；旷视智能开放平台 Megvii Cloud 是人工智能开放平台，为开发者提供人脸识别、文字识别、图像识别及其它人工智能能力。
3	云从科技	受邀起草与制定人脸识别国家标准；中国农业银行超级柜台、刷脸取款；安防领域产品已在 22 个省上线实战。
4	依图科技	招商银行、浦发银行、京东金融、360 金控；江苏省公安厅运用依图系统。
5	百度	百度内部正在使用人脸识别闸机，2016 年 11 月与乌镇景区合作，游客刷脸便可自由进出景区；与首都机场签订协议，未来首都机场将实现刷脸登机；与“宝贝回家”公益平台合作利用人脸识别寻找走失儿童；携手雨诺股份 CRM 系统，通过服务集成商 Cella 联合为医药零售行业输出智慧药房解决方案，目前已应用在先声再康连锁药房。
6	阿里	人脸识别技术各模块可通过 API 参数自由组合，服务定制灵活；基于深度学习和海量人脸标注数据，再加阿里云的技术实力，能够提供稳定、可靠的大流量服务；有了人脸识别，可以高效率、高准确率排查未经明星允许而使用其代言的商品，反过来保障阿里妈妈直通车和钻展中明星代言商品的广告效果。
7	腾讯	财付通与公安部所属的全国公民身份证号查询服务中心达成人像比对服务战略合作；优图人脸识别技术将广泛引用于 EMS 的政务、贵重物品和重要文书快递中；在腾讯微证券等产品上应用人脸识别。
8	汉王科技	助力银川市政府应用生物识别技术打造智慧政务平台；助力杭州市国税局实现人脸生物识别比对技术开展“刷脸”办税；在公安刑侦、追逃领域有大量应用；技术授权已与华硕、海尔、长虹、海信、平安银行等达成合作，并推广应用到智能家电、笔记本、移动终端等应用平台。
9	科大讯飞	科大讯飞联合香港中文大学汤晓鸥教授团队，共同推出世界领先的人脸识别技术，提供人脸验证、在线 / 离线人脸检测和人脸关键点检测等功能；联合中国银联和徽商银行发布“声纹 + 人脸”融合认证个人转账应用；科大讯飞在用的身份认证考勤，全国各地分公司通过 app 进行“人脸 + 声纹”打卡即可。
10	川大智胜	2D 人脸识别产品已经推向市场，3D 人脸采集和识别产品主要处于工程样机和产品样机阶段；主要应用领域是公共安全领域，2D 在北京师范大学和四川大学的学生宿舍的门禁系统中应用，铁路认证票查验中在试用，已在成都火车东站试用。
11	阅面科技	“阅客”是软硬件一体化的客群分析终端；“阅邻”提供软硬件一体化智能门禁及刷脸认证解决方案。
12	猎户星空	除门禁、手机等生活化场景外，还应用到猎豹移动旗下的直播产品 Live.me 中，包括后台技术检测识别情色信息、识别官方 Logo 进行广告检测，通过性别、类型等标签对主播进行分类，实现动态的人脸贴图等个性化功能。
13	格灵深瞳	发布面向公安、交通行业的深瞳人眼摄像机 Foveacam，可以在远距离内识别人脸。
14	中科奥森	DeepEyes 双目深度学习人脸识别防伪技术。
15	平安科技	人脸识别技术已应用于 10 多个场景，如接入远程开户、绑卡核身、账户登录、分期购物、人脸考勤、人脸支付等数十种业务场景的 50+ 终端应用中。
16	海鑫智圣	2010 年以“人脸识别监控报警系统”为核心完成了上海世博会园区人脸采集与比对系统建设项目；2012 年成为全国公民身份证号码查询服务中心人像比对认证系统的承建商，支持库容超过 11 亿人；2016 年为石景山区事业单位公开招聘考试首钢技师学院考场引进了 3 台海鑫身份核验设备，实现了考生刷脸进场。
17	飞搜科技	已开发出面向企业的多个在线 API、离线 SDK 的核心产品线，包括人脸检测、人脸特征点定位、人脸识别、名人识别、人脸属性识别和目标 / 场景识别、色情图片识别等。
18	汉柏科技	人脸识别产品上市，推出门禁（GATES）、识别终端（DOORS）、闸机（INS）、桌面终端（ONS）等产品及一系列行业解决方案。
19	人人智能	发布人脸识别硬件模组 aceOS，基于 ARM 芯片研发，可轻松嵌入到智能摄像头等各种终端上面，主要应用于人证、人脸比对等安防领域系统。
20	中德宏泰	“深眸”提供包括人脸识别在内的一整套人像识别技术方案。

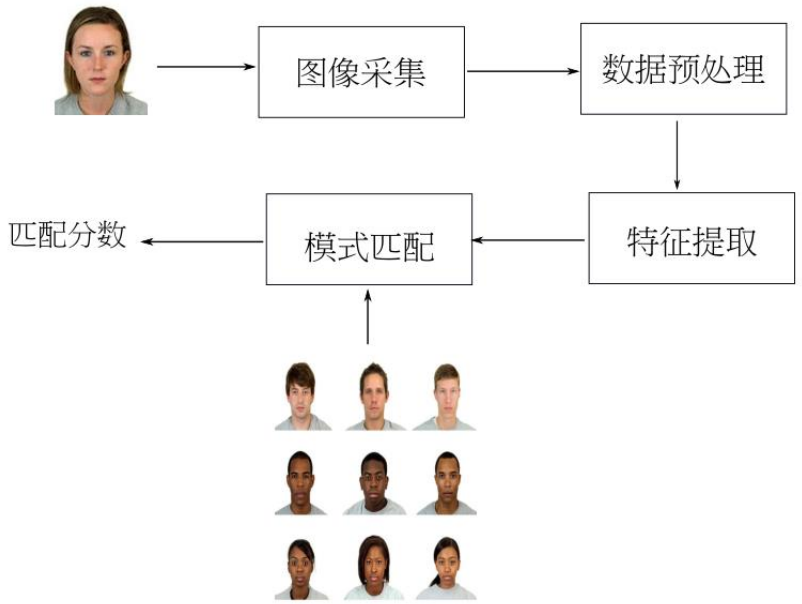
2017《互联网周刊》&eNet研究院选择排行

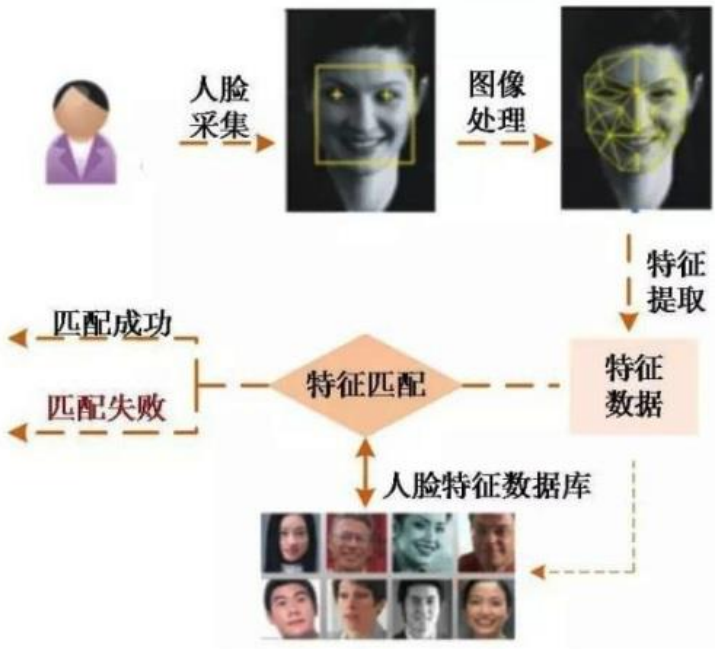
人脸识别概述--什么是人脸识别

人脸识别概述--什么是人脸识别

- **人脸识别**（Face Recognition），简单地说就是通过人的面部照片实现身份认证的技术。
  - 相机拍照、视频截图、证件照；侧面照、远景照（如监控录像）。
- 人脸识别可细分为**两种认证方式**，一种是身份确认（Verification），一种是身份辨认（Identification）。
  - 身份确认：这个人是不是Ta（海关身份认证、ATM 刷脸取款）
  - 身份辨认：哪个人是Ta（刑侦领域的嫌疑人排查）

人脸识别概述--人脸识别系统的基本组成

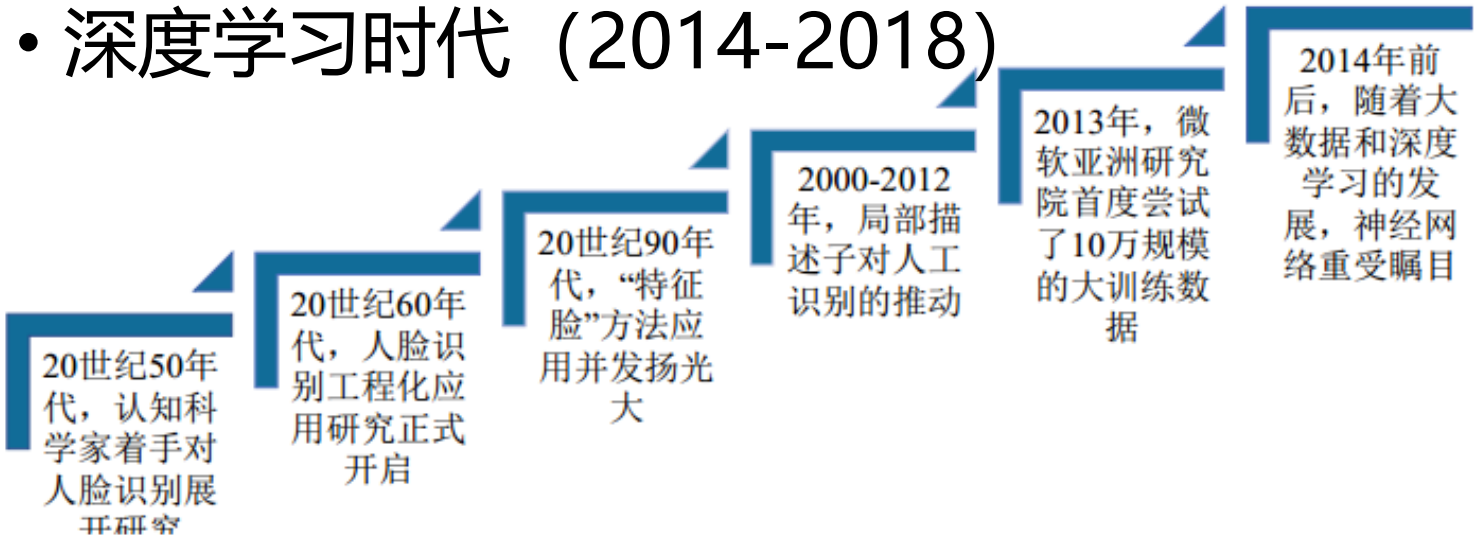


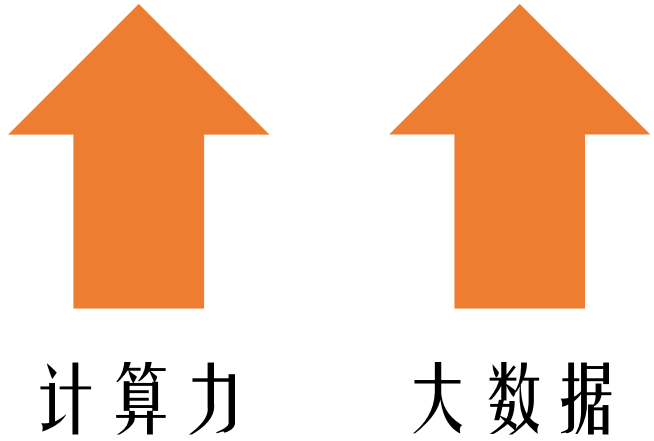


光学设备采集到人脸图像，**预处理**模型对该图像进行一系列预处理工作，将处理后的图像送入**特征提取**模块提取典型人脸特征，最后由**模式匹配**模块与系统中的预存人脸进行对比，得到匹配分数。

人脸识别概述--人脸识别简史

- 心理学和神经学研究
- 模式识别时代（1956-1993）
- 统计模型时代（1993-2000）
- 机器学习时代（2000-2013）
- 深度学习时代（2014-2018）

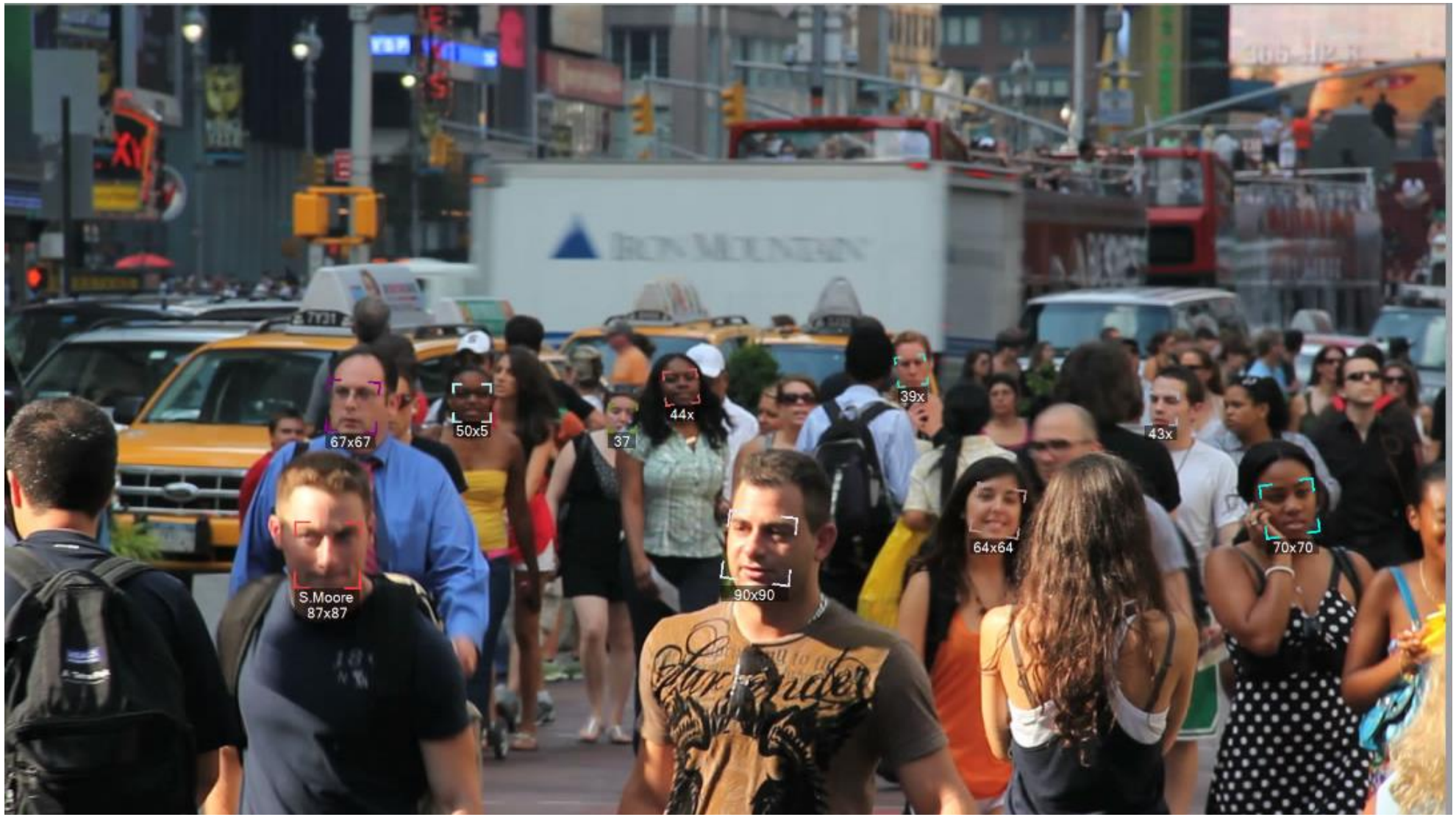


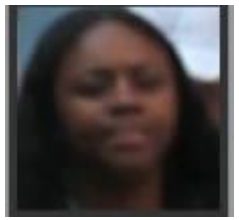


目录

- 人脸识别概述
- 基于特征脸的人脸识别
- 基于深度学习的人脸识别
- 深度神经网络的其他应用

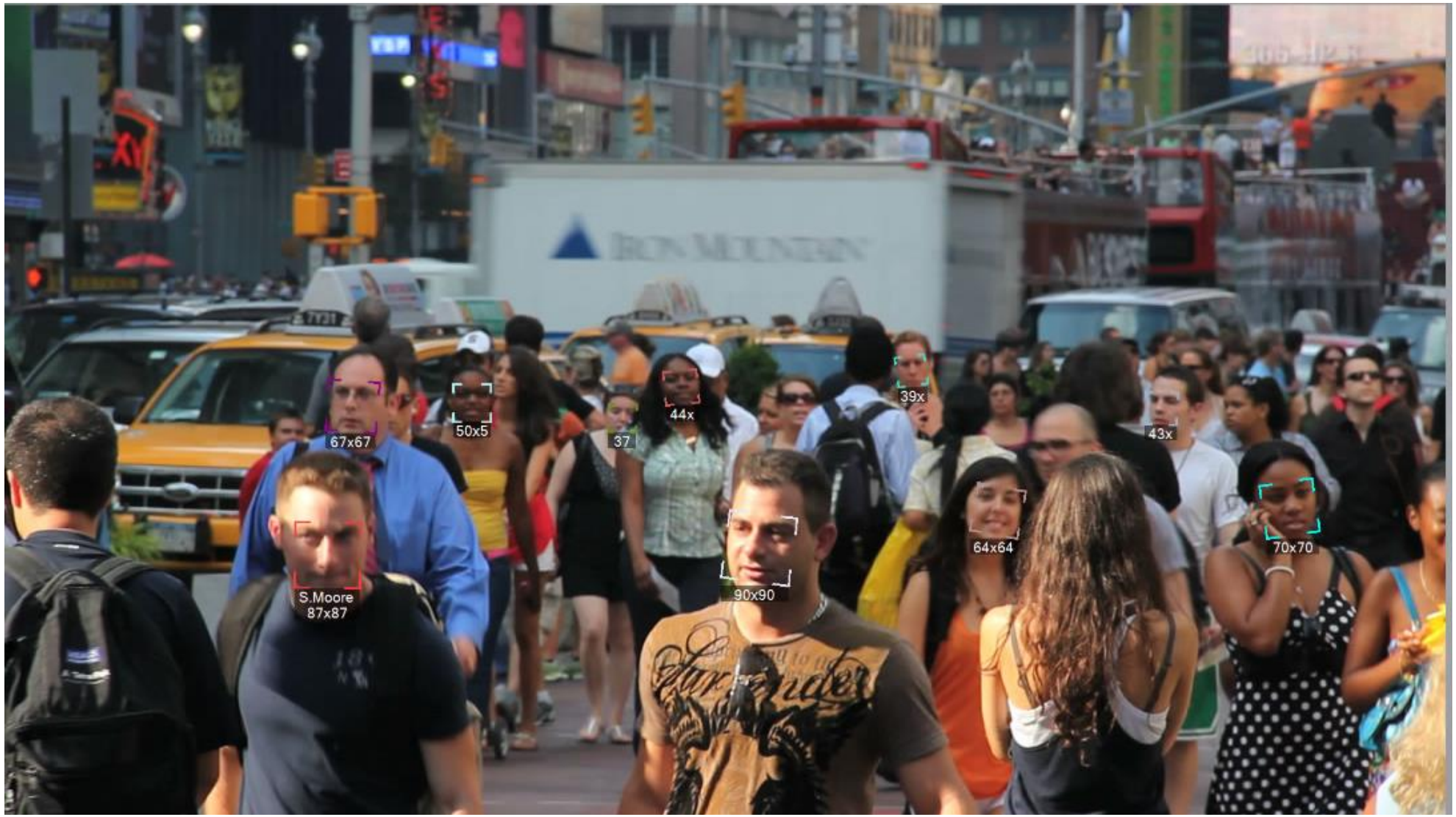
基于特征脸的人脸识别





请大家在左边这张图中找右边这个人。

基于特征脸的人脸识别



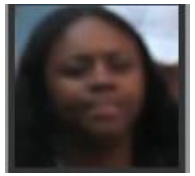
我们换张脸再试试。

基于特征脸的人脸识别

- 大家都很非常快速的找到这两个人，接下来我们思考一下，我们是怎么做到的。其实是有两步得到的。

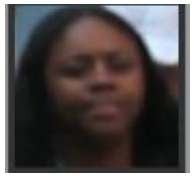
基于特征脸的人脸识别

- 大家都很非常快速的找到这两个人，接下来我们思考一下，我们是怎么做到的。其实是有两步得到的。
- 1）第一步是找出人脸的特征，如性别、肤色、发型、五官的形状等。先来看看左边这个人，估计是女性、黑色皮肤、长头发、短眉毛、瓜子脸。再来看看右边这个人，估计是男性、白色皮肤、短头发，粗眉、方脸。



基于特征脸的人脸识别

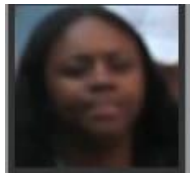
- 大家都很非常快速的找到这两个人，接下来我们思考一下，我们是怎么做到的。其实是有两步得到的。
- 1）第一步是找出人脸的特征，如性别、肤色、发型、五官的形状等。先来看看左边这个人，估计是女性、黑色皮肤、长头发、短眉毛、瓜子脸。再来看看右边这个人，估计是男性、白色皮肤、短头发，粗眉、方脸。



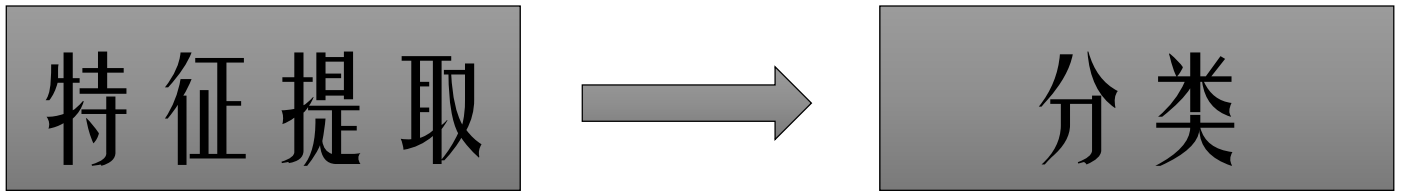
- 2）第二步是根据找到的特征去那张大图里面比对，取比对结果较高的。

基于特征脸的人脸识别

- 大家都很非常快速的找到这两个人，接下来我们思考一下，我们是怎么做到的。其实是有两步得到的。
- 1）第一步是找出人脸的特征，如性别、肤色、发型、五官的形状等。先来看看左边这个人，估计是女性、黑色皮肤、长头发、短眉毛、瓜子脸。再来看看右边这个人，估计是男性、白色皮肤、短头发，粗眉、方脸。



- 2）第二步是根据找到的特征去那张大图里面比对，取比对结果较高的。

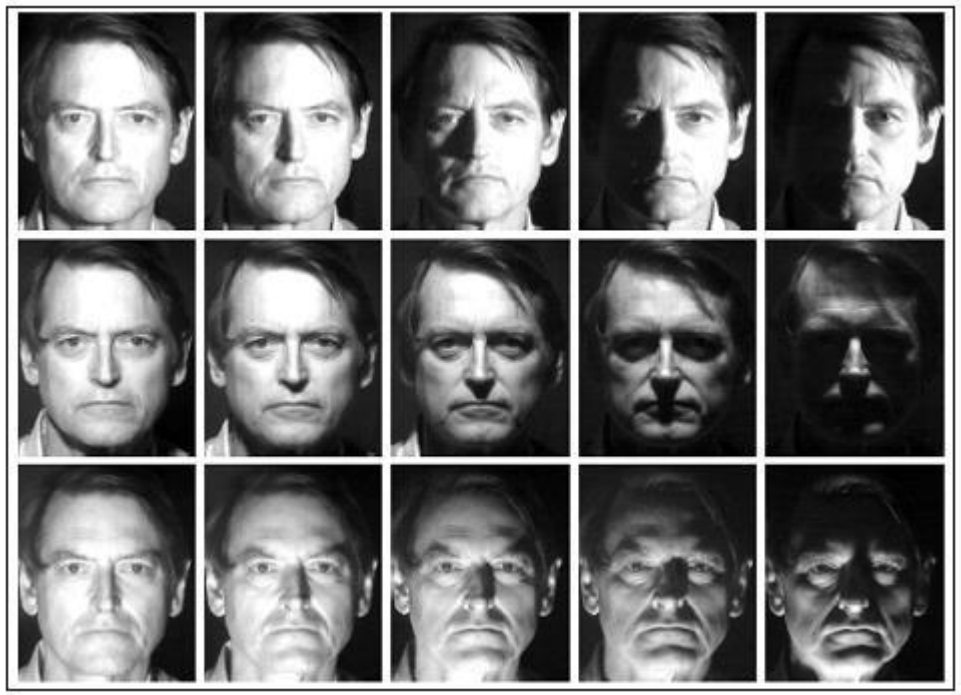


基于特征脸的人脸识别-- 像素

像素（px）是计算机处理图像的基本单位，用像素表示图像是所有图像处理的第一步，让我们感受一下像素表示下的人脸图像。

基于特征脸的人脸识别-- 像素

- 500万像素 有效4915200，像素2560＊1920
- 400万像素 有效3871488，像素2272＊1704
- 300万像素 有效3145728，像素2048＊1536
- 200万像素 有效1920000，像素1600＊1200
- 130万像素 有效1228800，像素1280＊960
- 80万像素 有效786432，像素1024＊768
- 50万像素 有效480000，像素800＊600
- 30万像素 有效307200，像素640＊480



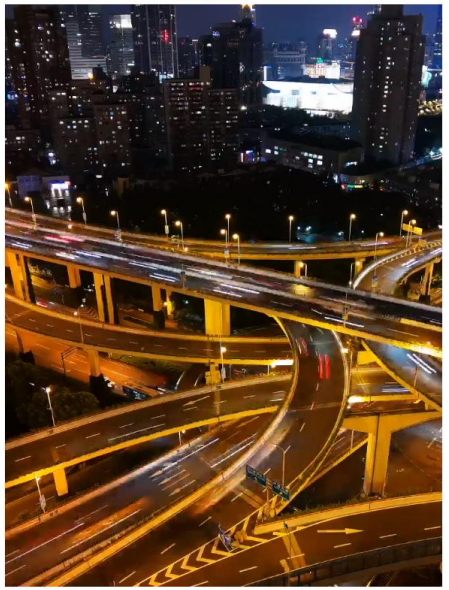
像素越高，图像包含的细节越多，图像看起来越细腻、越清晰

基于特征脸的人脸识别-- 像素

年代	平均像素数（指屏幕上的总像素点）	平均尺寸	平均像素密度
2007	84582	2.3	171
2008	105670	2.5	182
2009	163898	2.8	197
2010	218624	3.1	204
2011	305975	3.6	216
2012	453075	4.1	226
2013	972301	4.6	294
2014	1194295	5	309
2015	1840554	5.2	375
2016	1729815	5.3	368
2017	2276016	5.4	411

4000 万像素电影摄像头

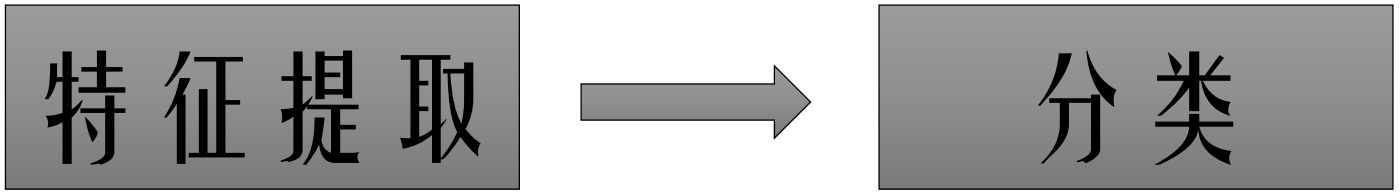
1/1.54 英寸型传感器，支持超高清夜摄，4K 超广角超暗态延时摄影，超高速摄影等电影级摄影功能。



基于特征脸的人脸识别--特征提取

计算机需要从这些像素中认出人脸，必须脱离像素，而寻找更全局的特征，然后再进行判断。

基于特征脸的人脸识别—两步



主成份分析

分类器
（例如：支持向量机）

基于特征脸的人脸识别– 主成分分析(PCA)

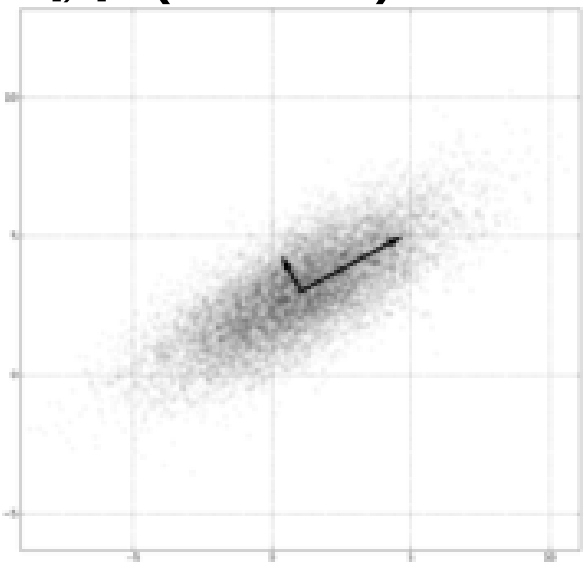
- 将事物表达为向量
- 寻找最有代表性的关键因素
- 去掉无关干扰

基于特征脸的人脸识别– 主成分分析(PCA)

- 将事物表达为向量
- 寻找最有代表性的关键因素
- 去掉无关干扰

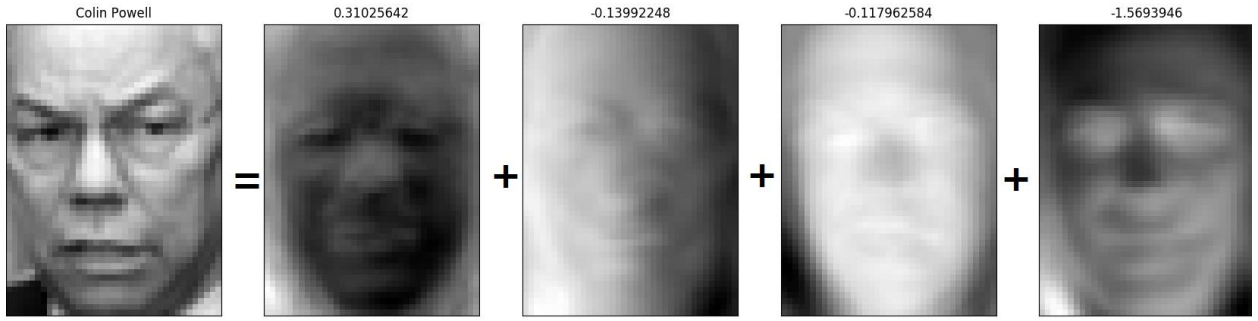
人脸照片≈ 特征脸1 的权重× 特征脸1 + 特征脸2 的权重× 特征脸2 ...

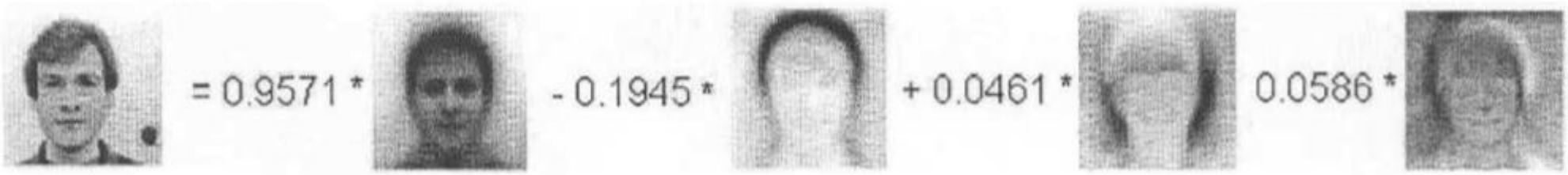
基于特征脸的人脸识别– 主成分分析(PCA)



- 将事物表达为向量
- 寻找最有代表性的关键因素
- 去掉无关干扰

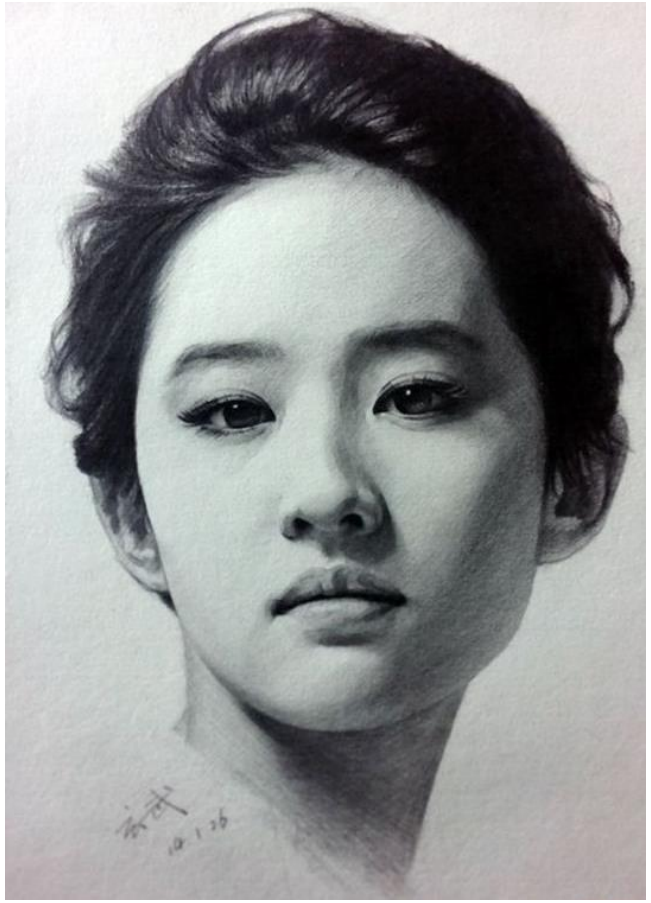
人脸照片≈ 特征脸1的权重× 特征脸1+ 特征脸2的权重× 特征脸2 ...





基于特征脸的人脸识别– 主成分分析(PCA)

类似一个素描的过程



基于特征脸的人脸识别– 主成分分析(PCA)

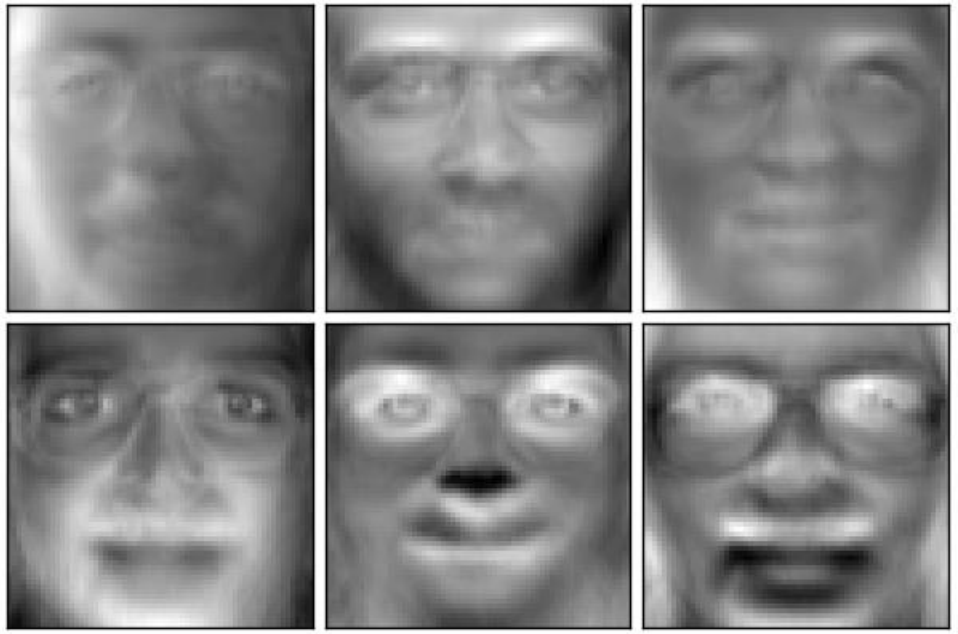
1. 收集所有人脸照片

基于特征脸的人脸识别– 主成分分析(PCA)

1. 收集所有人脸照片
2. 找到最有代表性的平均人脸

基于特征脸的人脸识别– 主成分分析(PCA)

1. 收集所有人脸照片
2. 找到最有代表性的平均人脸
3. 将这张平均脸从所有照片中减去



基于特征脸的人脸识别– 主成分分析(PCA)

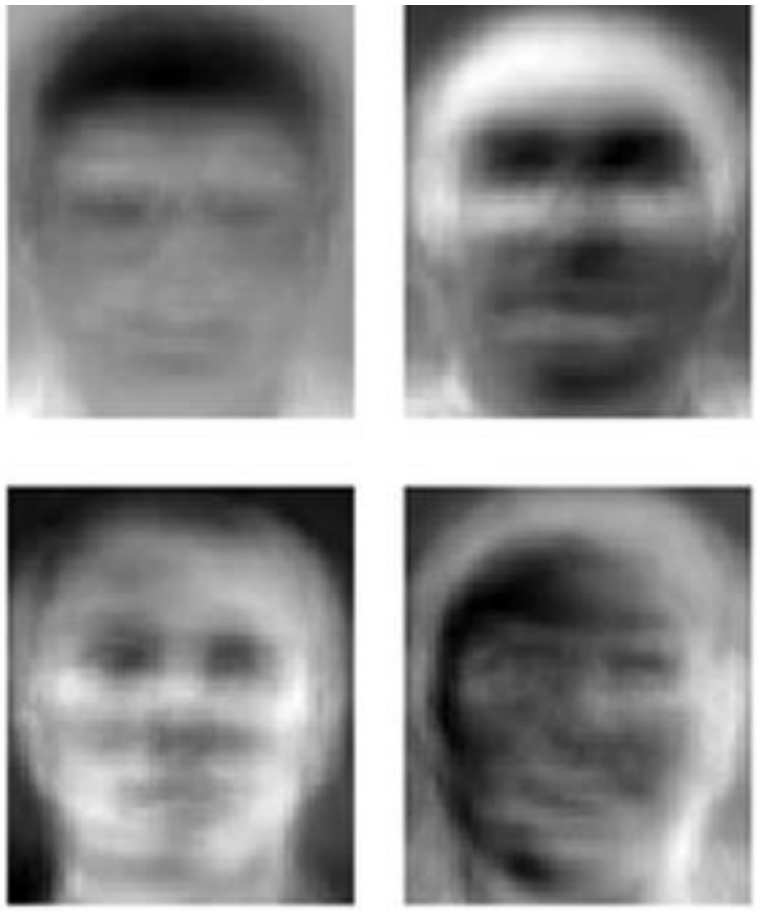
1. 收集所有人脸照片
2. 找到最有代表性的平均人脸
3. 将这张平均脸从所有照片中减去
4. 在照片残差中找到最有代表性的平均人脸(第二主成分)

基于特征脸的人脸识别– 主成分分析(PCA)

1. 收集所有人脸照片
2. 找到最有代表性的平均人脸
3. 将这张平均脸从所有照片中减去
4. 在照片残差中找到最有代表性的平均人脸(第二主成分)

...

重复进行，即可得到一系列主成分，用以代表人脸特征

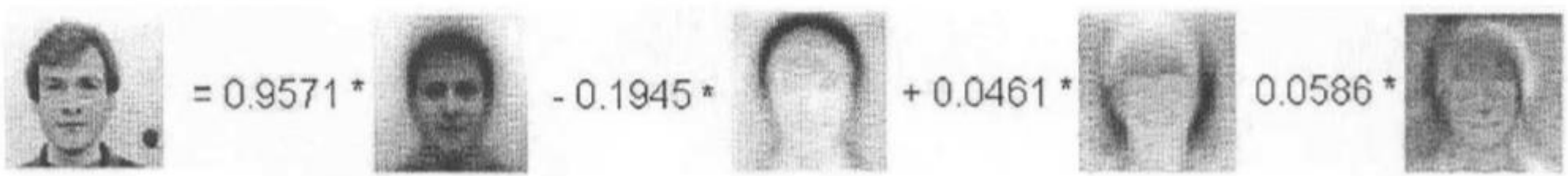


基于特征脸的人脸识别–特征脸

1. 由PCA所提取出的主成分称为“特征脸”（EigenFace）
2. 特征脸用以描述不同人脸的主要差异内容

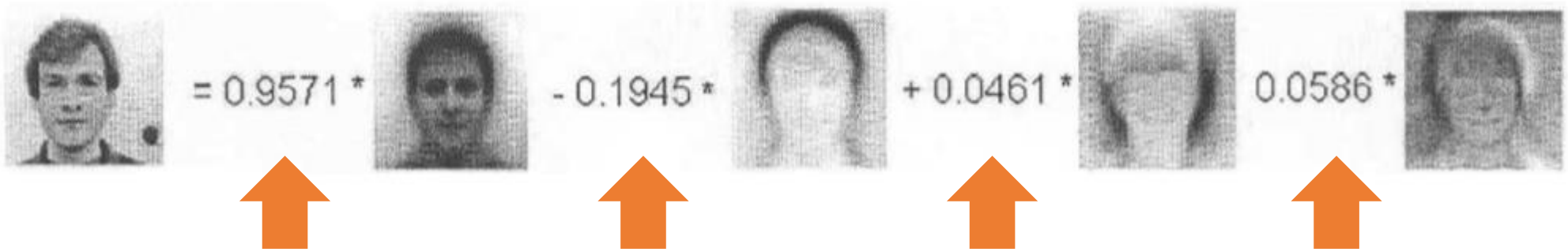
基于特征脸的人脸识别–特征

- 在各个特征脸上的权重即为EigenFace特征



基于特征脸的人脸识别–特征

- 在各个特征脸上的权重即为EigenFace特征



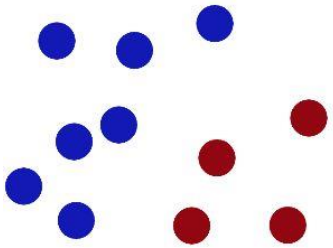
基于特征脸的人脸识别–支持向量机(SVM)

如何把EiganFace方法提取的人脸特征分成不同人呢？常用的分类器之一是SVM。

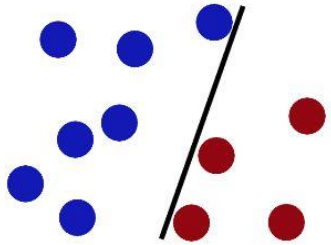
基于特征脸的人脸识别–支持向量机(SVM)

什么是支持向量机？让我们来讲个故事：

在很久以前的古代，一个侠客要去解救困在魔王宫殿里的爱人，魔王和他采用游戏的方式对决，魔王在桌子上似乎有规律放了两种颜色的球，说：“你用一根棍分开它们？要求：尽量在放更多球之后，仍然适用。”

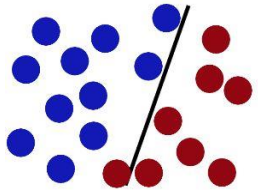


于是，侠客这样放。



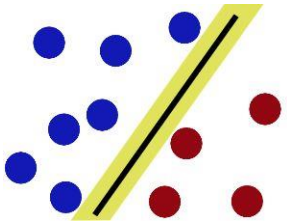
基于特征脸的人脸识别–支持向量机(SVM)

魔王继续往桌上放入更多的球，貌似有球出错了。

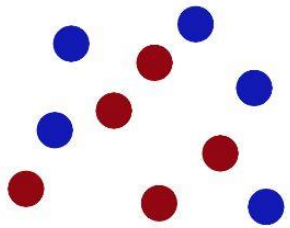


SVM 就是试图把棍绑在最佳的位置，好让棍的两边有可能大的间隙，才能更好的把球分开。

现在即使魔王放了更多的球，棍仍然是一个好的分界线。

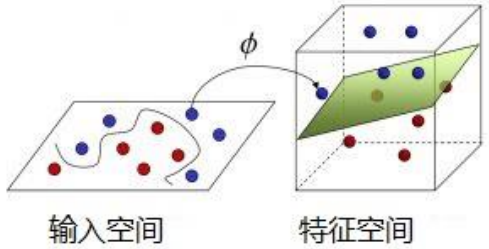


在SVM 工具箱中有另一个更加重要的 **trick**。 魔王看到侠客已经学会了一个trick，于是魔王给了侠客一个新的挑战。

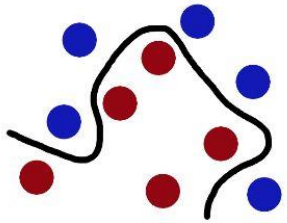


基于特征脸的人脸识别-支持向量机(SVM)

现在，侠客没有棍可以很好帮他分开两种球了，现在怎么办呢？当然像所有武侠片中一样侠客桌子一拍，球飞到空中。然后，凭借侠客的轻功，侠客抓起一张纸，插到了两种球的中间。

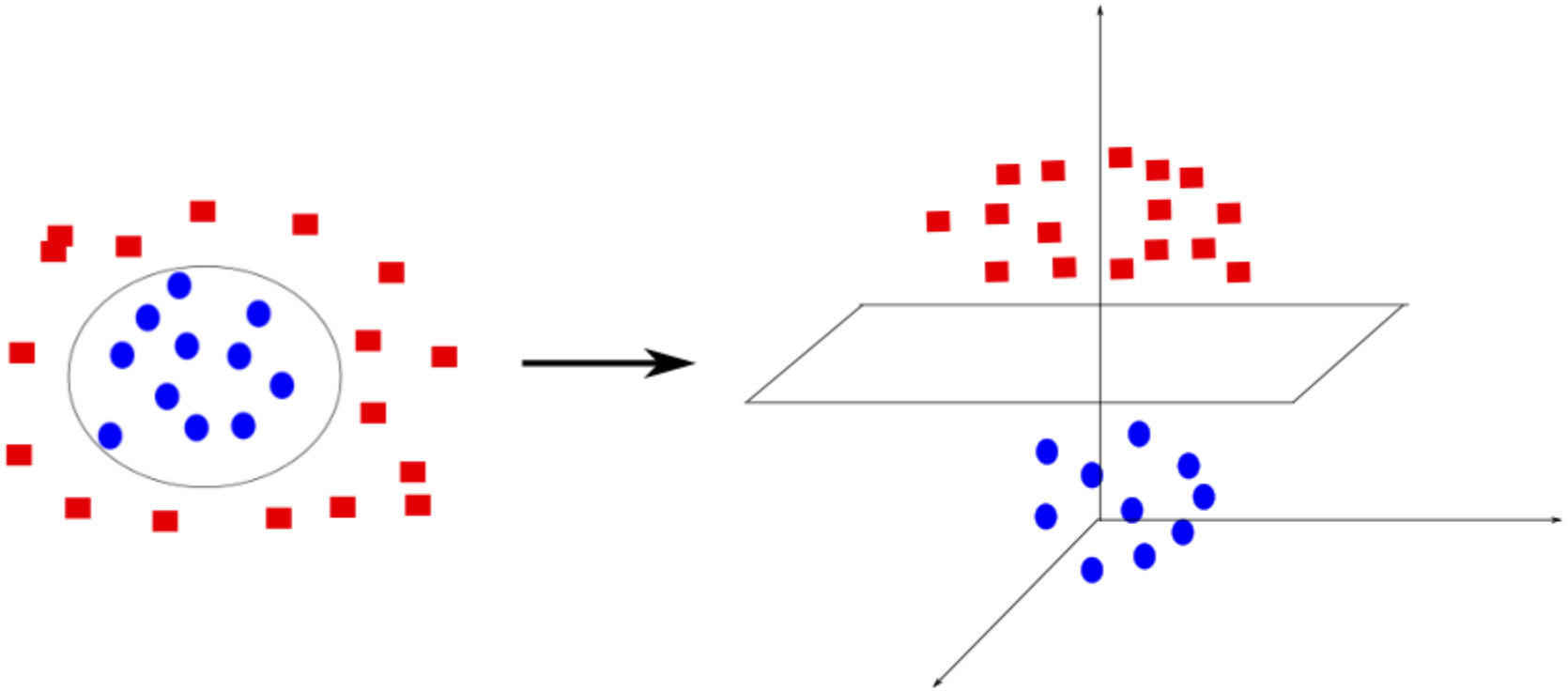


现在，从魔王的角度看这些球，这些球看起来像是被一条曲线分开了。



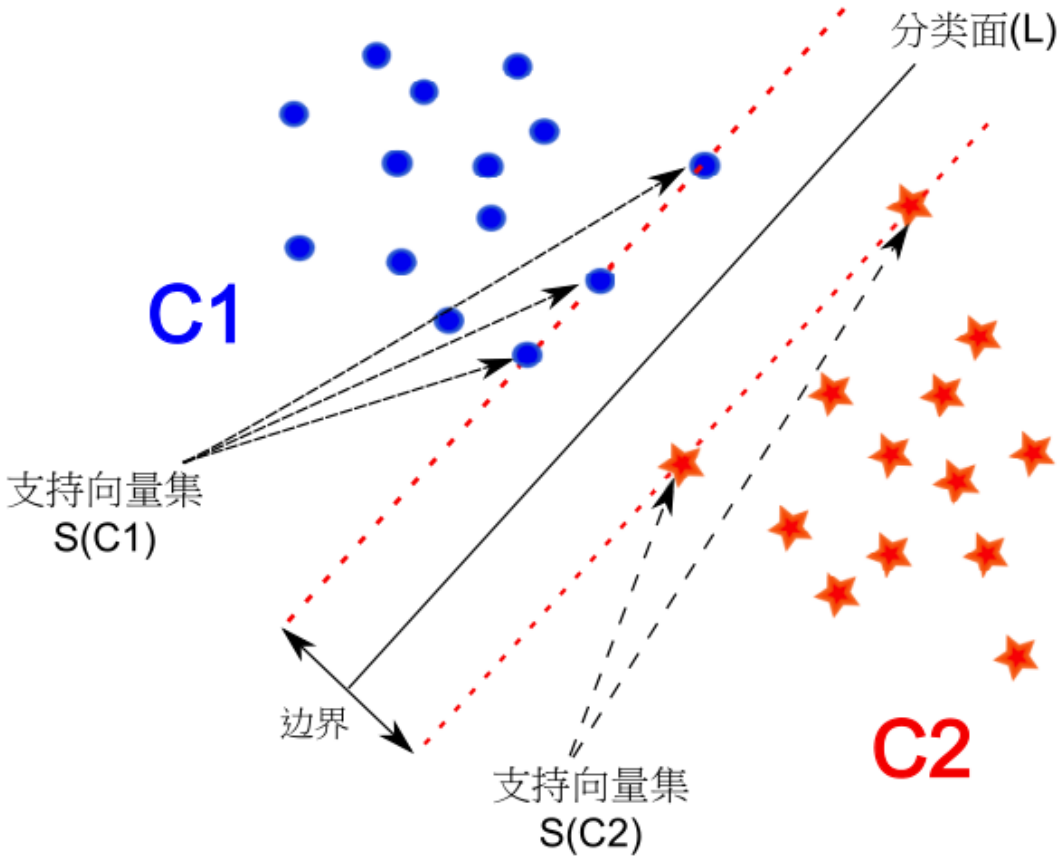
把这些球称为数据（**data**），棍子称为分类器（**classifier**），最大间隙trick 称为寻优（**optimization**），拍桌子称为核处理（kernel process），那张纸称为超平面（**hyperplane**）。

基于特征脸的人脸识别-支持向量机(SVM)



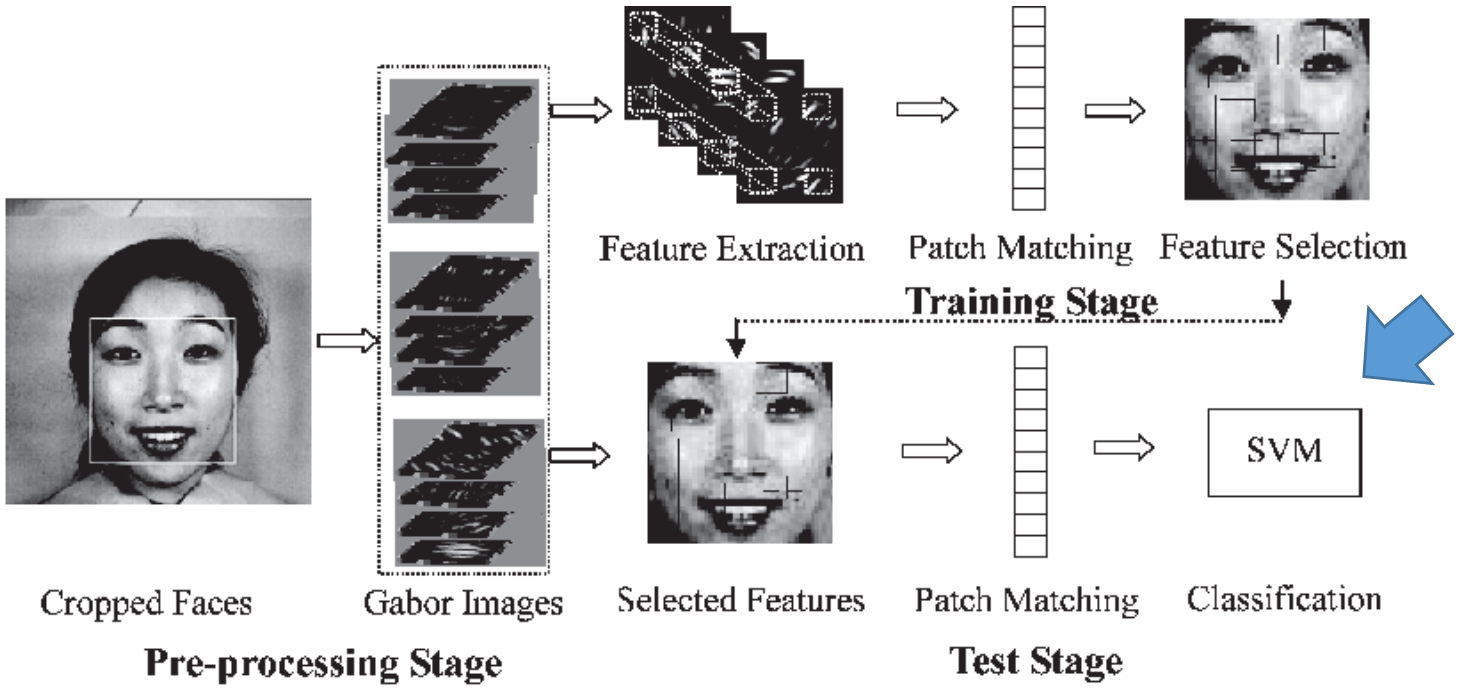
将原始数据映射到新的空间，使其可以“一刀切开“。

基于特征脸的人脸识别–支持向量机(SVM)



一条大河分开了两个村庄，正好在河沿上的住家较支持向量（Support Vector）。

基于特征脸的人脸识别–支持向量机(SVM)

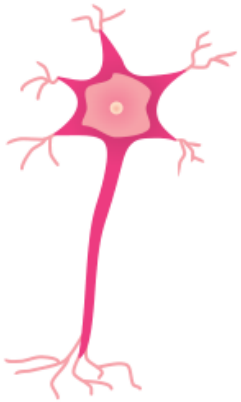


人脸特征放入SVM，就可以把不同人脸区分开了

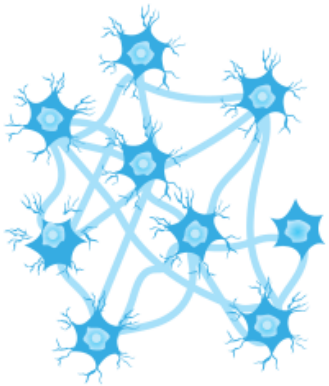
目录

- 人脸识别概述
- 基于特征脸的人脸识别
- 基于深度学习的人脸识别
- 深度神经网络的其他应用

基于深度学习的人脸识别--神经网络



(a)



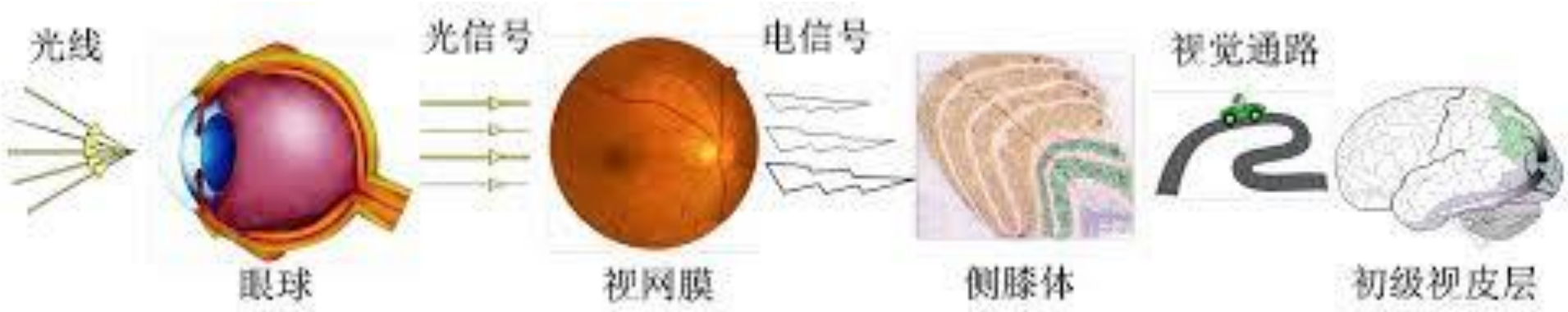
(b)

（a）单个神经元结构，包括细胞体，树突和轴突等结构。
（b）每个神经元通过树突接受上一个神经元传递的神经信息，并通过轴突向下一个神经元继续传递，形成神经网络。

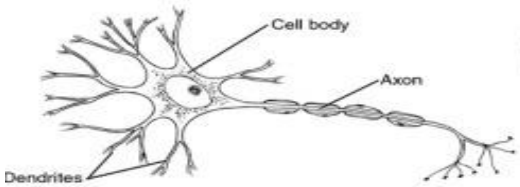
初中生物！

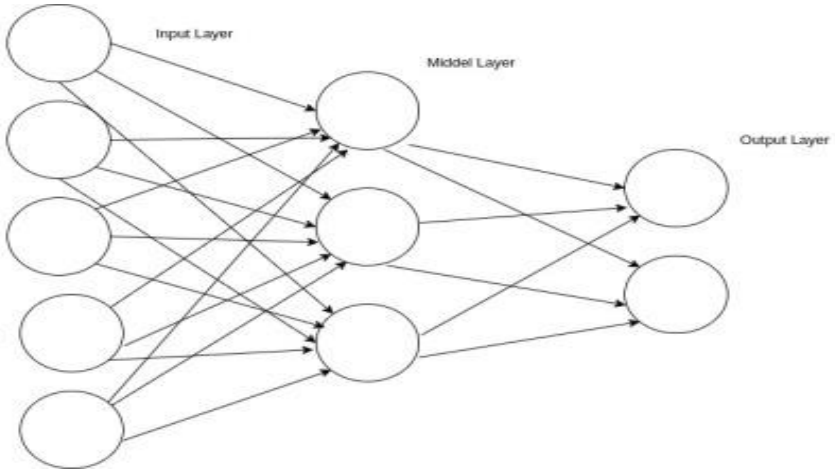
基于深度学习的人脸识别--神经网络

人类视觉系统



基于深度学习的人脸识别--神经网络

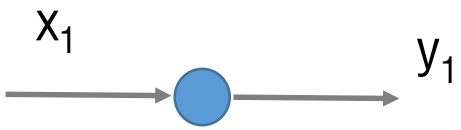




神经网络模型是模仿人类神经系统对信息的处理方式。人的大脑神经元将信息传给另一个神经元的过程，可以描述成数学方程。

基于深度学习的人脸识别--神经网络

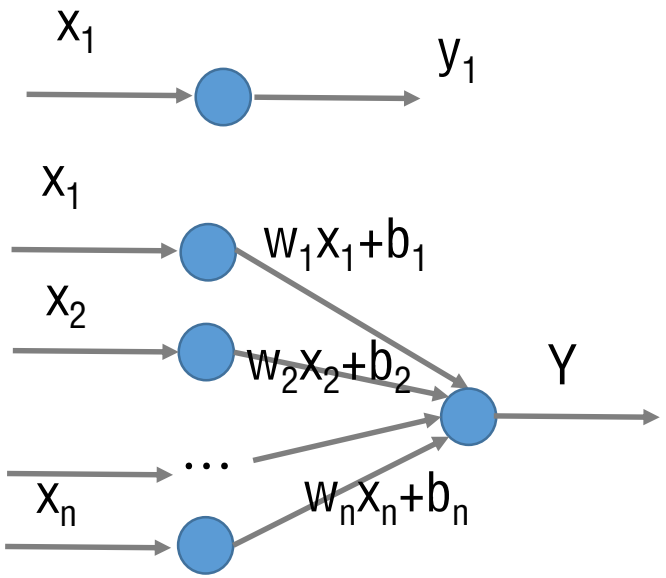
线性模型



当神经元只有1个时：$y_1=w_1x_1+b_1$

基于深度学习的人脸识别--神经网络

线性模型



当神经元只有1个时：$y_1=w_1x_1+b_1$

当神经元为多个时：

$y_1=w_1x_1+b_1$

$y_2=w_2x_2+b_2$

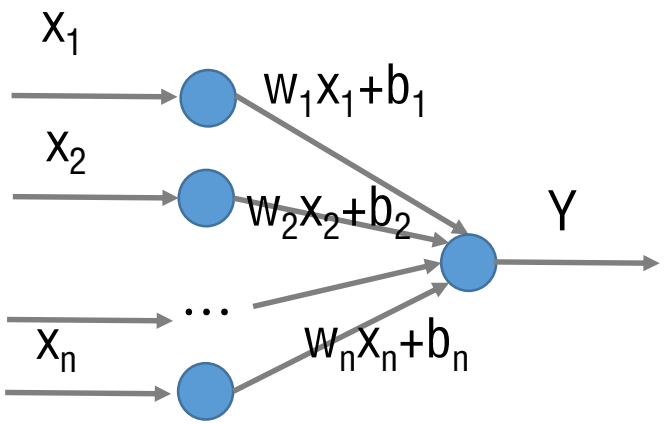
…

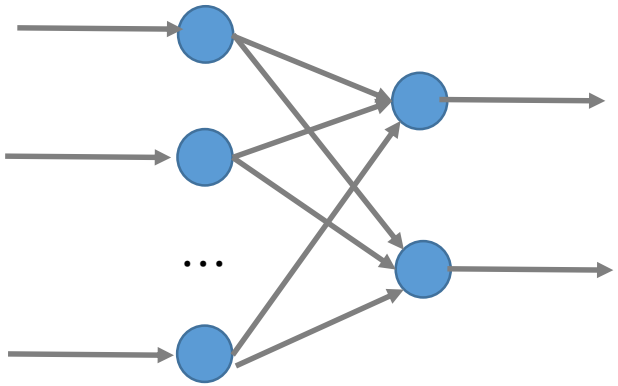
$y_n=w_nx_n+b_n$

$Y=y_1+y_2+...+y_n$

基于深度学习的人脸识别--神经网络

线性模型





当神经元只有1个时：$y_1=w_1x_1+b_1$

当神经元为多个时：

$y_1=w_1x_1+b_1$

$y_2=w_2x_2+b_2$

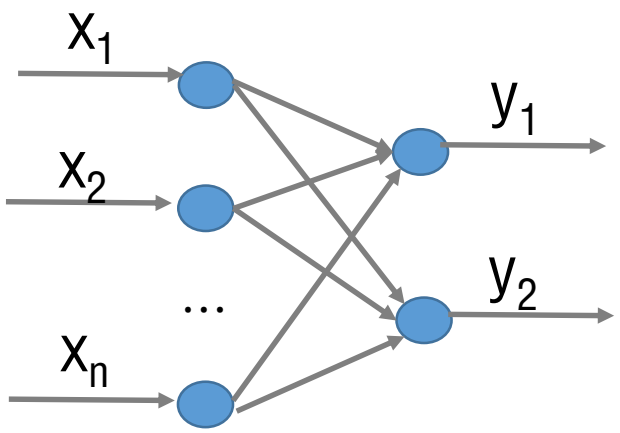
…

$y_n=w_nx_n+b_n$

$Y=y_1+y_2+...+y_n$

那当网络更复杂时，以此类推，大家可以尝试自己写一下这个网络的表达式。

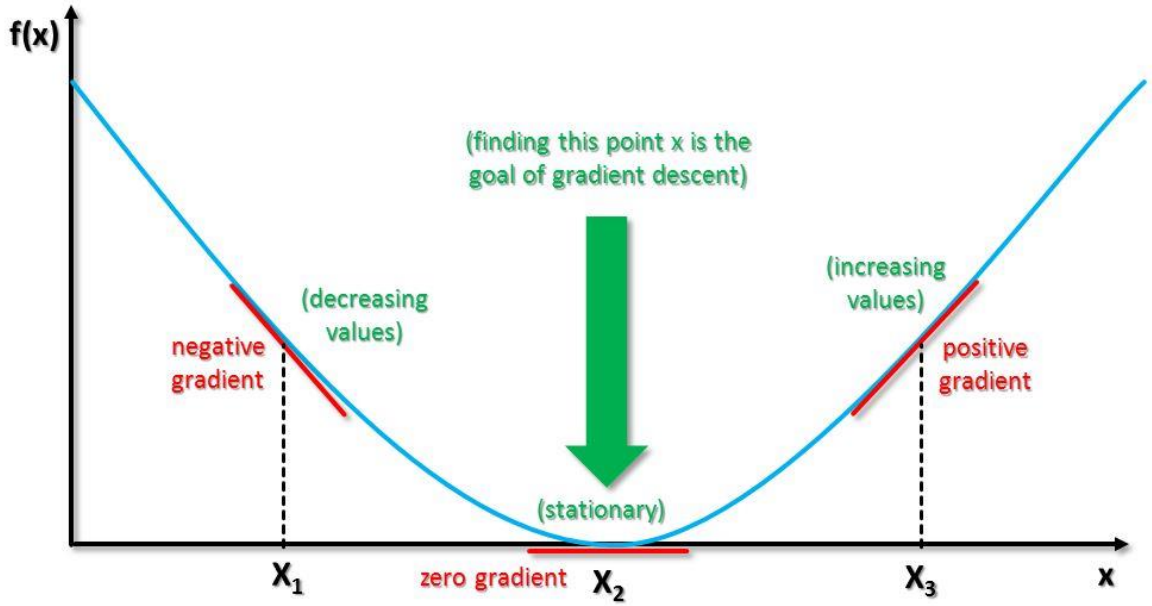
基于深度学习的人脸识别--神经网络



多层感知器（Multiple layer perceptron, MLP）：将传统一层感知器模型扩展到多层即得到多层感知器。

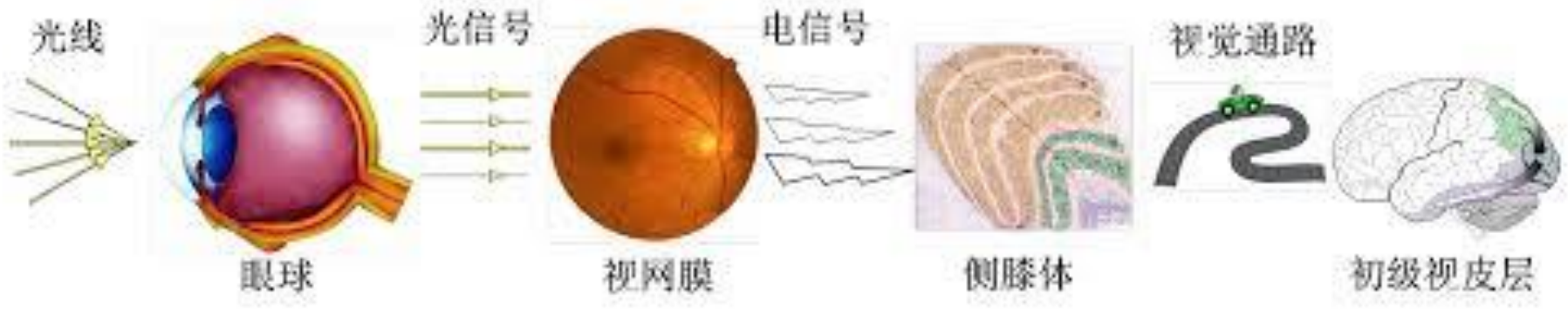
从结构上看，MLP将线性模型的一层网络扩展到多层，每一层输出经过一个非线性变换后作为后一层的输入，由此得到一个信息逐层传导的前向网络（Feed-Forward Network）。

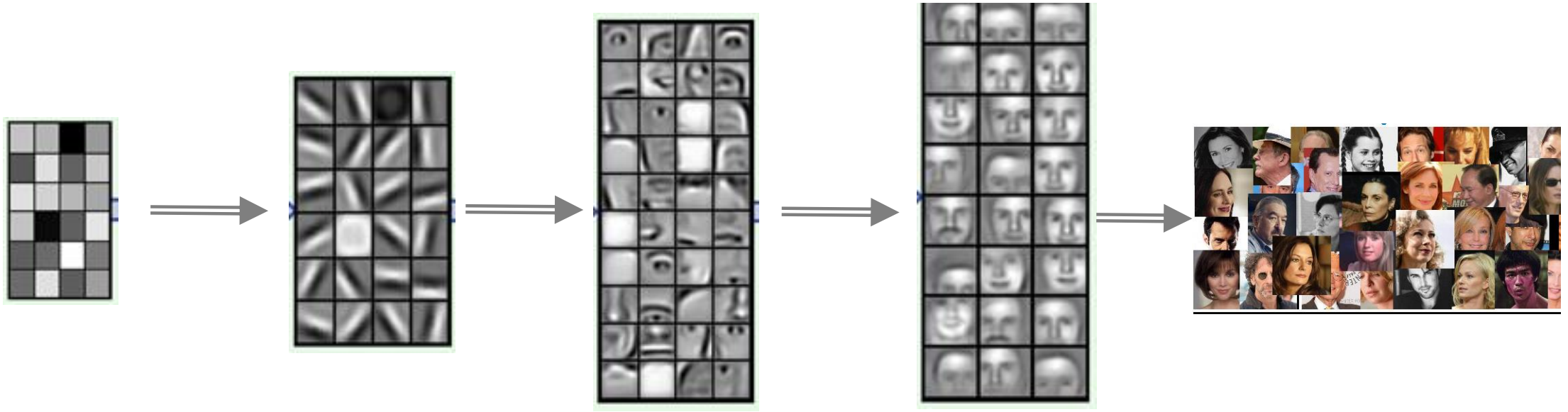
基于深度学习的人脸识别--神经网络



神经网络可训练，训练的目的就是调整参数使得对训练数据的代表性更强。

基于深度学习的人脸识别—卷积神经网络



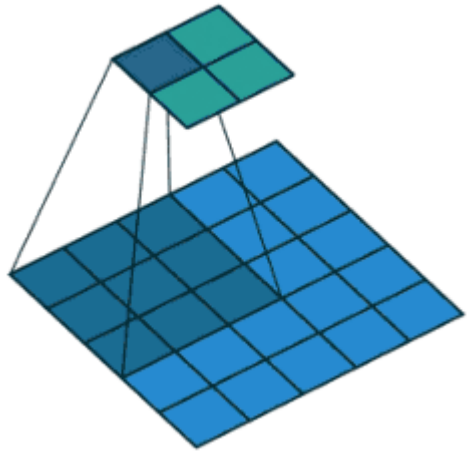


基于深度学习的人脸识别—卷积神经网络

- 卷积

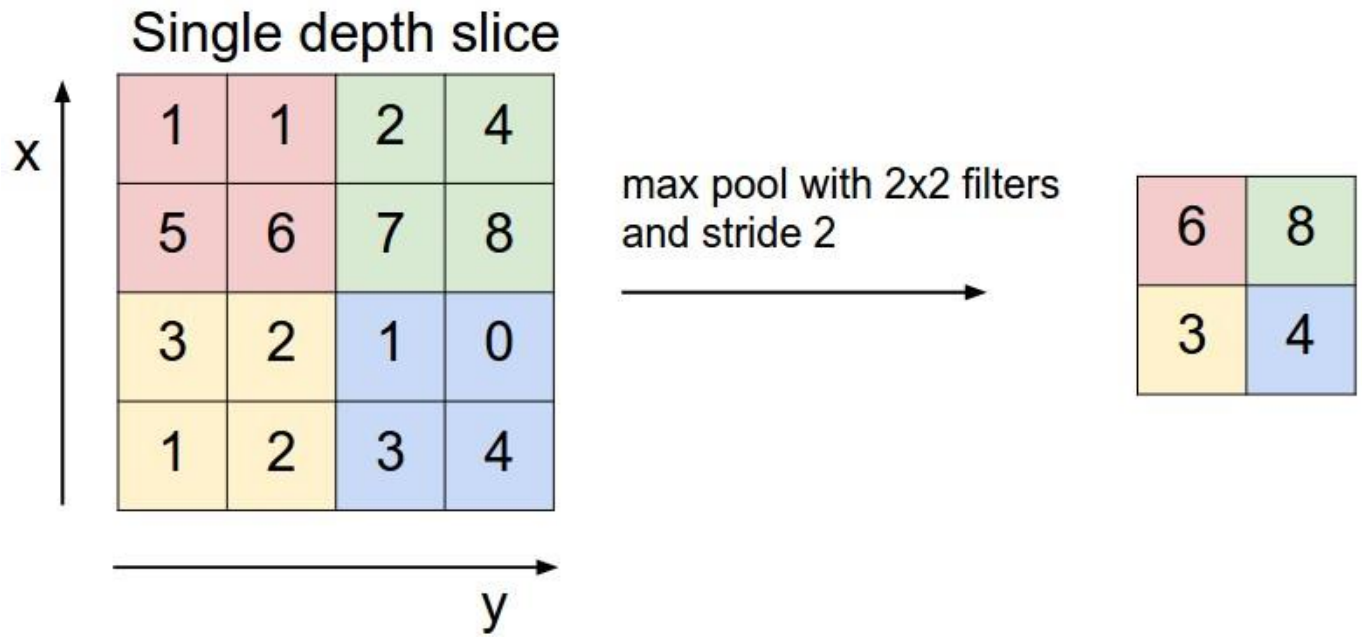
$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} * \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 & 4 & 1 \\ 1 & 2 & 4 & 3 & 3 \\ 1 & 2 & 3 & 4 & 1 \\ 1 & 3 & 3 & 1 & 1 \\ 3 & 3 & 1 & 1 & 0 \end{pmatrix}$$

I K $I * K$



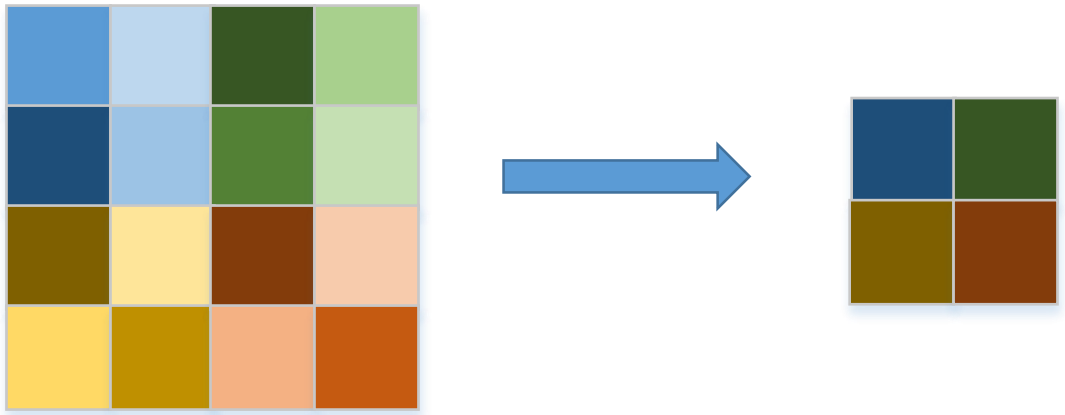
基于深度学习的人脸识别—卷积神经网络

- 池化



基于深度学习的人脸识别—卷积神经网络

- 池化

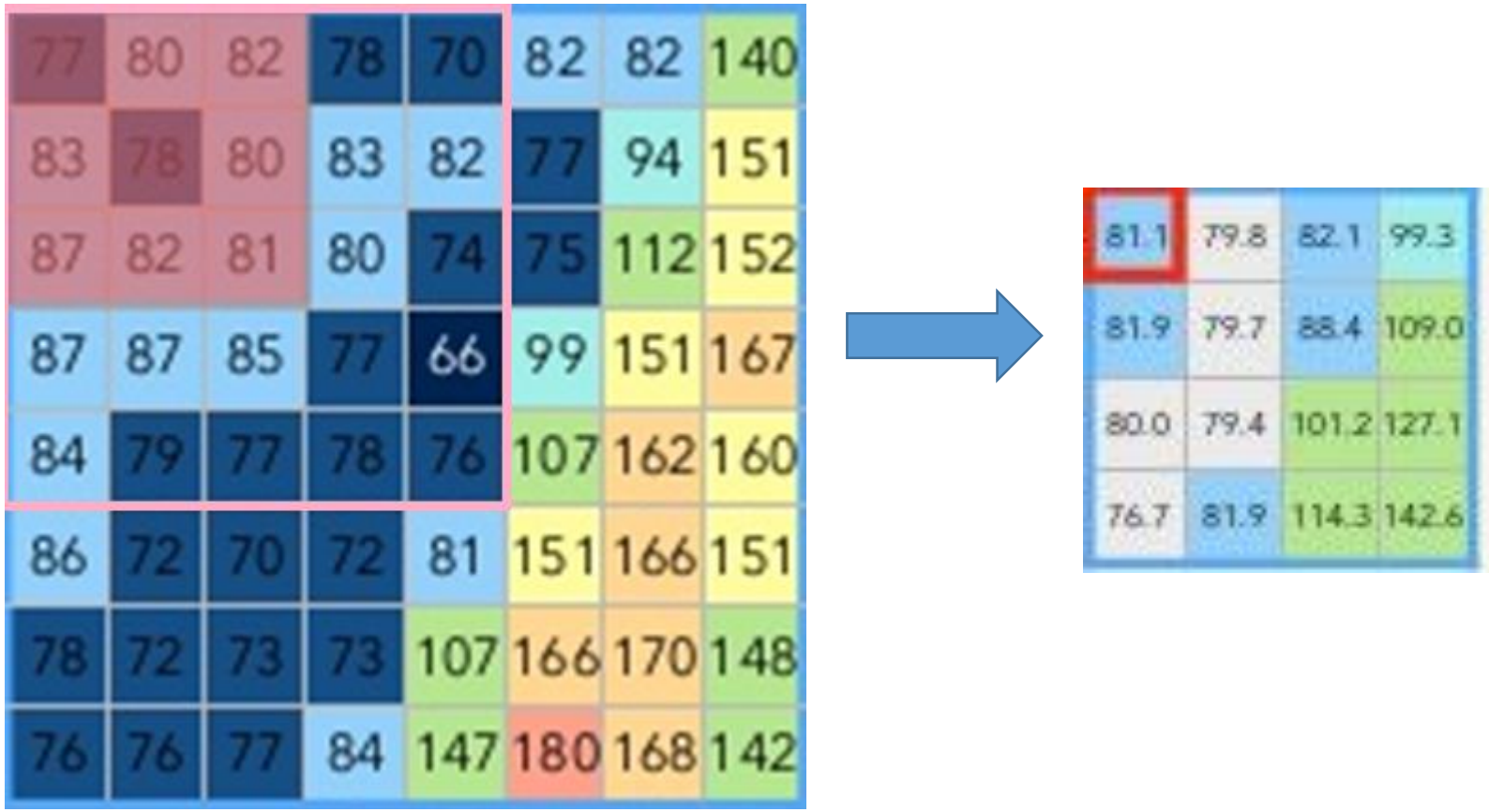


最大化池化为例：

取每四格的最大值，可以看出池化层后并没有很大程度上改变原图片的颜色分布。加入池化层后数据量缩小了很多，更有利于数据的分析，降低计算复杂度。

基于深度学习的人脸识别—卷积神经网络

- 池化

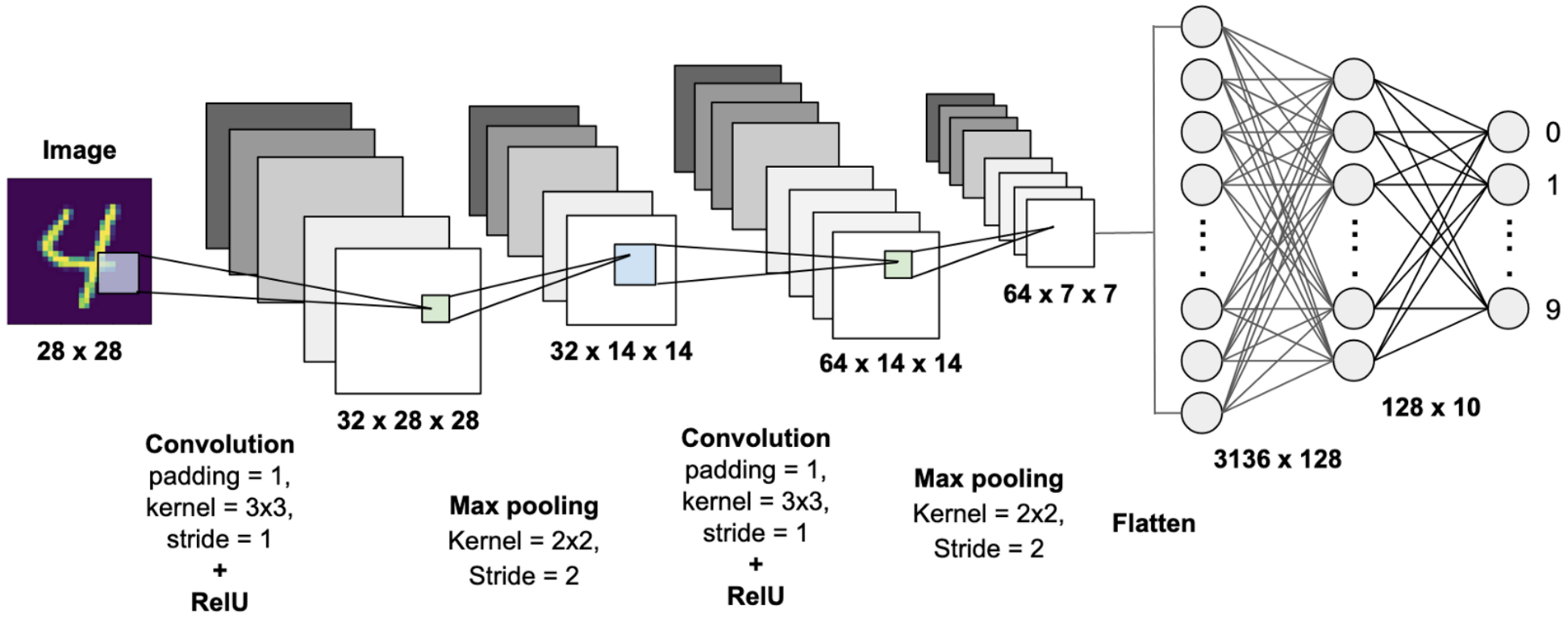


平均值池化为例：

选择5*5的相邻矩形区域的平均值，信息量压缩了很多，简化了计算机的运算。

基于深度学习的人脸识别—卷积神经网络

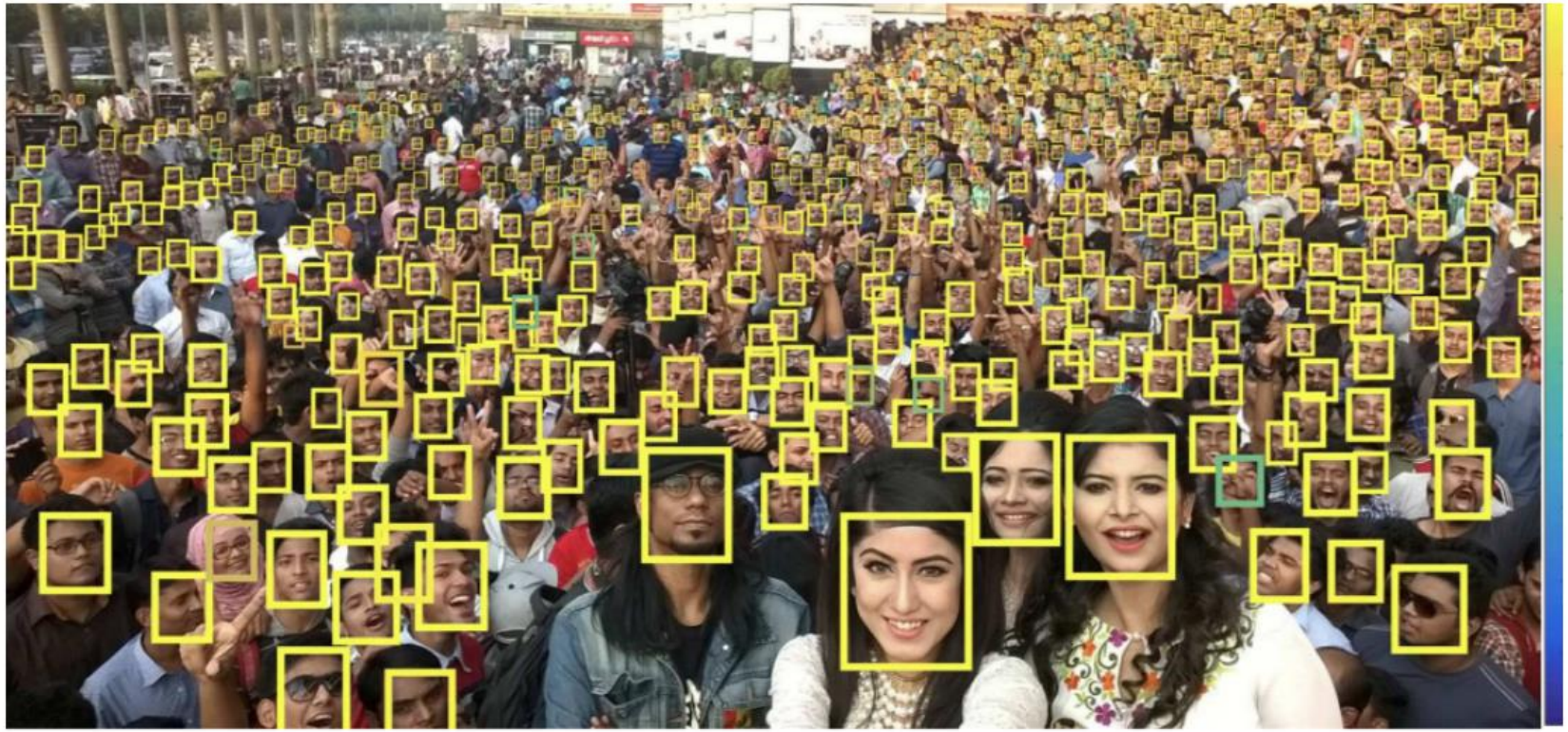
- (卷积+池化)*N



目录

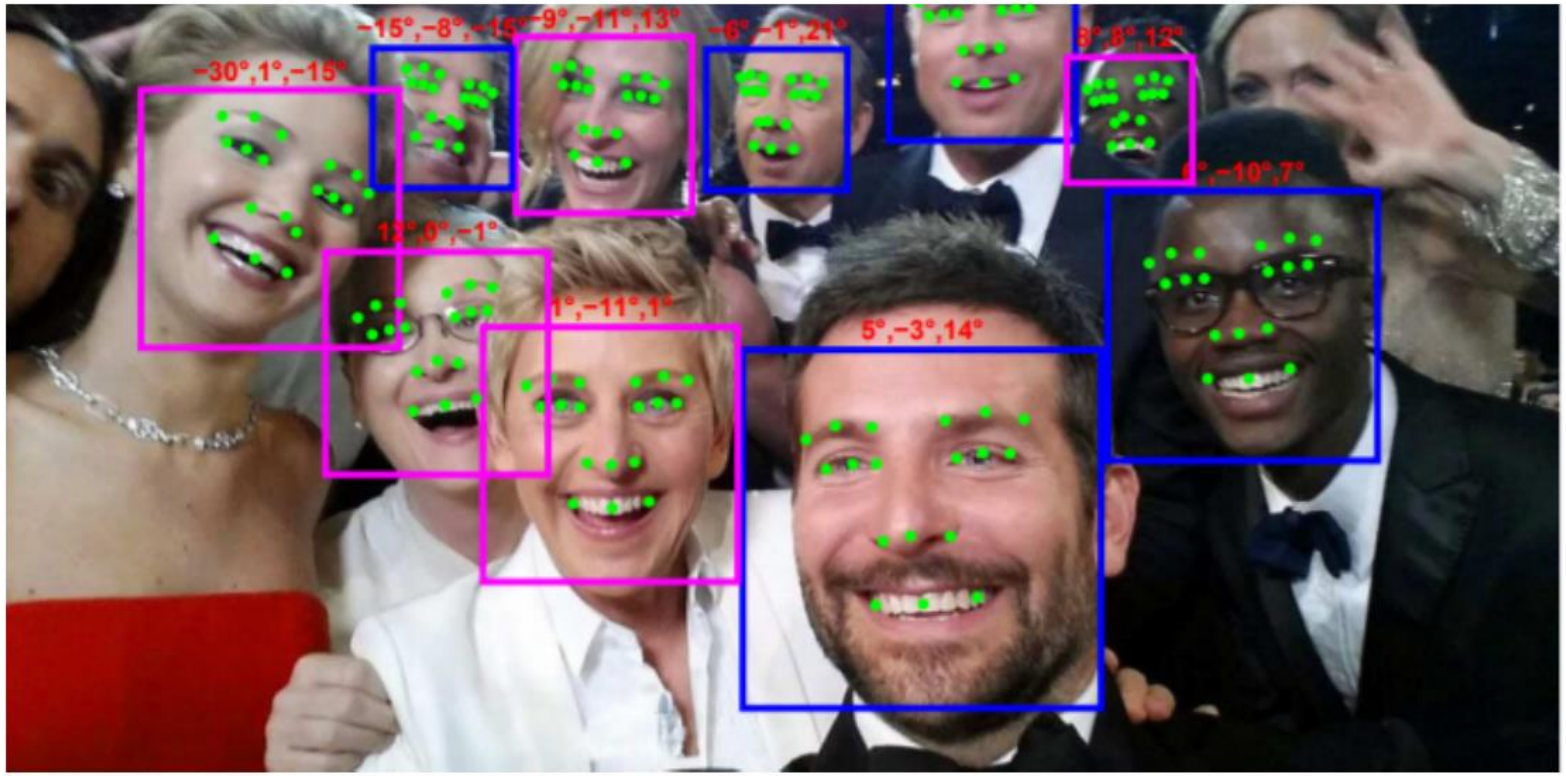
- 人脸识别概述
- 基于特征脸的人脸识别
- 基于深度学习的人脸识别
- 深度神经网络的其他应用

深度神经网络的其他应用—人脸检测



大规模人脸检测

深度神经网络的其他应用—人脸检测

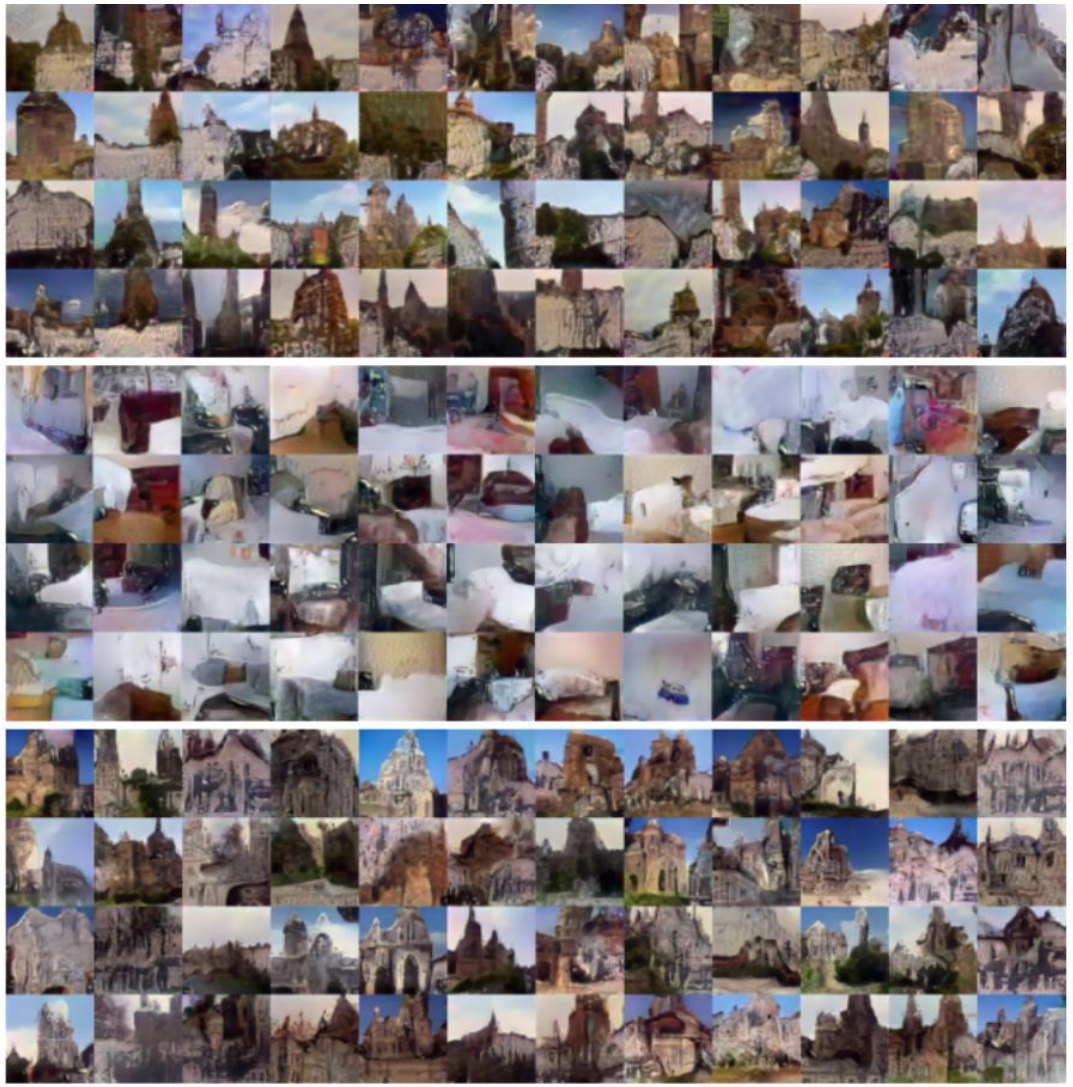


同时包含性别、姿态等检测。

深度神经网络的其他应用—图像生成

机器自动生成人脸图片。

深度神经网络的其他应用—图像生成



机器自动生成自然风景图片。

深度神经网络的其他应用—图像风格转换

深度神经网络的其他应用—换脸

深度神经网络的其他应用—Deepfake换脸

The end