

[百科] 人脸识别技术

撰稿人:北京斯科德科技有限公司

人脸识别技术是一种通过计算机对人脸图像进行分析识别的技术，主要原理是通过提取图像中的人脸特征点与事先存储在系统中的人脸库进行比对并确定当前人员身份信息。该技术于 20 世纪 60 年代问世，在 21 世纪随着 CPU 计算能力的巨幅提高目前人脸识别技术已经迈入深度学习时代，随着商业化程度的不断加深人脸识别技术已经广泛应用在我们生活中的方方面面，例如门禁安防、金融支付、政务办事、手机解锁、自助服务终端等多种领域。由于人脸特征具备不可伪造性、采集便捷性等优点使得人脸识别技术迅速成为当今使用规模最大的生物识别方式，但是人脸识别技术在给人们带来极大便捷的同时也带来了个人信息滥用等数据安全问题，部分国家以及地区正在陆续出台相应政策以保护公民隐私不受侵害。

中文：人脸识别技术

英文：Face recognition technology

别名：人像识别技术、面部识别技术

核心技术：人脸识别算法①

识别模式：单一人脸识别、多脸识别

自我学习能力：机器学习/深度学习②

活体检测方式：RGB/IR 近红外/动态视频流

使用模式：1:1、1:N、M:N③

部署方式：在线/脱机离线方式

工具外设：摄像头、计算机

性能指标：人脸特征提取耗时、人脸库检索耗时

人脸识别技术特点

每个人的面部特征都是独一无二的并且具备不可伪造性因此面部特征可以作为身份识别的依据。而人脸识别技术正是基于人脸面部特征信息进行身份识别的一种生物识别技术，该技术伴随计算机处理能力的迅猛提高近年来也得到了飞速发展并在多个领域得到广泛应用。人脸识别技术具有便捷性、非接触性、实时性、自我学习性等特点：



人脸识别技术

- **便捷性**：人脸识别过程不需要额外的物理介质（如钥匙、卡片），只需要通过摄像头采集到人脸图像即可完成采集注册以及识别等过程。
- **非接触性**：人脸识别技术是一项非接触式生物识别技术，无需用户与设备产生物理接触即可完成身份识别过程，采用非接触式生物识别技术将有助于提高卫生安全性。
- **实时性**：人脸识别过程通常在几秒钟内实时识别，非常适用于快速身份验证场景。

- 自我学习性：目前人脸识别算法均具备有深度学习能力，可通过自身的不断优化提升识别效率。
- 用户体验好：在便捷性以及非接触性两大特点的加持下，用户只需要站在摄像头前即可完成识别无需特别操作。

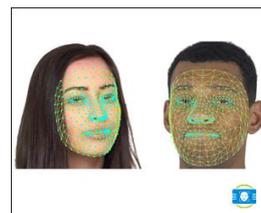
人脸识别技术流程

人脸识别技术工作流程主要由数据采集、人脸检测、特征提取、活体检测、身份识别、结果输出等几部分组成。



人脸识别算法

人脸识别算法是人脸识别技术的核心，负责从人脸图像中提取特征并进行身份识别。随着计算机视觉和机器学习的发展，人脸识别算法不断升级优化，从传统的基于几何纹理特征的算法逐渐发展到了深度学习算法。传统算法主要基于图像处理和模式识别，深度学习算法是利用深度学习模型从大规模数据中学习人脸特征。人脸识别算法有以下重要指标：



人脸识别算法

- 准确率：算法正确识别的人脸数量与总识别尝试次数之比。准确率是评估算法整体性能的基本指标。
- 错误接受率 (FAR)：被错误接受为真实的假冒者数量与总的假冒尝试次数之比，FAR 衡量了算法对非授权人脸的错误接受程度。
- 错误拒绝率 (FRR)：算法未能识别真实人脸的数量与总的真实人脸尝试次数之比，FRR 衡量了算法对真实人脸的错误拒绝程度。
- 计算时间和效率：算法的运行时间和计算资源的消耗，尤其在实时应用中，是重要的考虑因素。

错误接受率 (FAR) / 错误拒绝率 (FRR) 均是生物特征验证系统的识别精度指标之一 [Q1](#)。关于识别算法中的 FAR 以及 FRR 两项参数对于使用效果将会产生很大的影响，通过调整 FAR 与 FRR 参数将提升算法在不同使用场景下的表现。

人脸识别应用模式（1:1 模式、1:N 模式、M:N 模式）

人脸识别技术实际应用中主要分为两大模式即 1:1 模式、1:N 模式。

- 1:1 模式

1:1 模式为身份验证模式，主要目的是为了解决“你是你”，在人脸识别过程开始前系统数据源就已经预先锁定了数据范围为 1 人，通过对被检测对象的面部进行采集并与当前 1 人的数据源做比对，最终核实当前被检测对象是否为本人。该模式主要应用于手机解锁、PC 解锁、机场验票、火车站验票、刷脸支付、酒店入住、刷脸开门、景区验票等场景。

- 1:N 模式

1:N 模式主要目的是为了解决“你是谁”，通过采集被测对象面部信息后在海量人脸库数据源中检索相符合的图像信息最终确定当前被检测人员的身份信息。该模式主要应用于会议签到、门禁安防等场景。

- M:N 模式

M:N 模式是多对多关系，即待检测对象数量大于 1 时需要分别识别出各自身份信息的过程。该模式在监控摄像头场景中由于无法要求用户采用任何形式的配合，故对于检测结果并非一定能够得到。该模式最常用的场景为公安抓逃场景。

模式	核验手段	结果强制性	用户配合度	设备算力要求	安全等级	适用场景
1:1	双重验证	必须给出核验结果	需要用户配合	较低	高	人证合一场景
1:N	单一手段	必须给出核验结果	用户需配合系统看向摄像头	较高	较高	门禁、签到
M:N	单一手段	非必须， <u>监视名单漏报率不得大于 70%</u> Q4	无法要求用户配合	高	-	公安抓逃

人脸识别活体检测

活体检测是人脸识别技术中的一个重要环节，用以确认被检测人脸是真实的、活体的，而不是通过翻拍照片、视频录制、面具模型等方式欺骗系统。在人脸识别技术中常用的活体检测主要有 RGB 活体检测、IR 近红外活体检测、动态视频流活体检测三种方式。



- RGB 活体检测

活体人脸在不同光照条件下会显示微小的颜色变化，可以通过分析 RGB 图像中像素点的色值得到颜色变化信息最终确认当前被检测样本是否为活体，真实活体的面部通常显示出更多的纹理变化。

- IR 近红外活体检测

IR 近红外活体检测是一种利用近红外光谱范围内的光学信息来确认人脸是否为真实活体的方式。IR 传感器可捕捉活体组织产生的微弱热辐射并形成相关图像，根据这一原理，计算机可以分析面部组织的热量分布、血液流动等生物特征来区分被检测样本是否为活体。

- 动态视频流活体检测

动态视频流活体检测是在一段视频流中进行活体检测的方式。在视频采集中通常需要被检测者根据程序随机指令做出相应眨眼睛、张嘴、头部运动等配合来确认被检测样本是否为活体。

方式	外设支持	优点	执行效率	安全等级	用户体验	适用场景
RGB 活体	普通可见光摄像头	无需专用设备，经济性好	高	中	无需特意配合使用体验好	门禁安防/会议签到
IR 活体	专用 IR 摄像头	检测速度快，检测结果可信度高	高	高	用户与 IR 摄像头之间的距离要适中且需要看摄像头	门禁安防/机场通行验证
动态视频流活体	普通可见光摄像头	无需专用设备，检测结果可信度极高	中	高	通过指令要求用户进行相关动作并判断人脸的真实有效性 Q3	金融业务/政务办理

静/动态人脸识别

人脸识别技术中分为静态人脸识别与动态人脸识别两类。静态人脸识别是针对单张图像进行人脸识别，通过人脸识别算法对某张图像进行人脸检测、特征提取、特征比对等过程完成最终的识别结果输出。相对而言，动态人脸识别处理的对象是一段视频，针对视频中的每一帧都要完成静态人脸识别的全过程，由于动态人脸识别比静态人脸识别多了时间维度，通过时序分析最终将多个识别结果进行叠加综合给出最终识别结果。

静态人脸识别与动态人脸识别主要针对的使用场景不同。静态人脸识别主要适用于快速验证通道、自助服务终端机等场景，动态人脸识别主要适用于金融业务办理、政务办理、视频监控行为分析等高安全性或 AI 智能分析场景。

多脸识别

多脸识别是指人脸识别系统具备同时识别多张人脸的能力。传统的人脸识别系统通常专注于单个人脸的检测和识别，但随着技术的发展，越来越多的系统开始支持同时处理多张人脸，实现多脸识别。多脸识别中同样需要以图像或视频作为基础数据输入，系统首先需要对输入图像或视频进行预处理然后通过人脸识别算法对输入源中的数据做人脸检测并提取特征值最后将识别结果标注在图片或实时视频中。多脸识别主要在交通枢纽站、大型会议等场合用于布控抓逃、统计人流量用途。



多脸识别

三维人脸识别

三维人脸识别是指利用人脸的三维形状和深度信息进行识别的技术。相比于传统的二维人脸识别，三维人脸识别在提高准确性和安全性方面有明显优势。但是三维人脸识别技术需要配合带有专用深度感知传感器的摄像头完成人脸信息的注册以及识别环节，在三维人脸识别中注册信息不能通过一张照片完成而是需要配合程序完成指定动作来确保应用程序能够采集到足够的特征信息点。目前三维人脸识别技术在手机解锁、个人 PC 账户登录、刷脸支付等场景中得到了广泛应用。以下是一些关于三维人脸识别与二维人脸识别的对比：



三维人脸识别

分类	二维人脸识别	三维人脸识别
技术原理	使用传统的摄像头获取面部的二维图像，依赖于分析人脸的颜色、纹理等特征进行识别。	使用具备深度感知能力的传感器，获取面部的三维形状和深度信息。

数据获取方式	通过普通摄像头获取的二维图像只包含人脸在水平和垂直方向上的位置信息。	利用深度传感器获取的数据，能够获取面部的三维形状和深度信息。
准确性	在受光照、姿势和遮挡等影响时可能准确性降低。	对光照变化、姿势变化和遮挡等因素具有更强的鲁棒性 ^⑤ ，提高了识别的准确性。
应用场景	对于一些攻击手段，如使用静态照片进行欺骗，抵抗性相对较低。	更适用于对安全性要求较高的场景，如金融领域、高级安保系统等。
成本和设备要求	相对成本较低，使用常规摄像头即可。	需要具备深度感知能力的传感器，相对成本较高。
实时性	通常可以实时进行，适用于快速的人脸识别场景。	需要处理更多的数据，可能稍显滞后，但对于某些场景也可以实现实时性。
复杂性	实施相对简单，适用于各种场景。	系统设计和实施相对复杂，需要更专业的硬件和算法支持。

人脸识别产品的部署形式

人脸识别技术目前已经用在多种硬件上，例如电脑、手机、Android 智能终端机、基于 Linux 操作系统的智能终端机、AI 边缘计算盒、监控摄像头、监控刻录机、物联网终端模块等具有非常丰富的硬件生态。虽然涉及到的硬件种类繁多但人脸识别技术在这些产品上的部署形式可以分为终端形式、终端服务器结合形式、服务器形式三类。

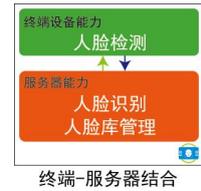
- 终端形式

终端形式指的是人脸识别的全流程均在一台终端上完成，即终端具备本地化全功能人脸识别算法以及本地化人脸数据库。使用这种方式的设备具备单机运行的能力，这类设备硬件通常需要具备较好的处理性能以及存储能力。由于受人脸识别算法能力以及硬件资源的限制通常本地不能建立超大规模的人脸库。



- 终端服务器结合形式

终端服务器结合形式指的是人脸识别的全流程需要终端以及服务器两者配合完成。一般常见的形式为终端负责完成人脸检测环节，将检测到的样本交给服务器完成人脸识别。这种使用方式主要为了满足建立大型人脸库的需求。



- 服务器形式

服务器形式指的是人脸识别的全流程都由服务器来完成，只需要为服务器接入相应图片或视频信息即可。这种形式在监控场景中使用较多，多路摄像头视频信号统一汇总至服务器，服务器根据每路视频信号来完成人脸识别过程。该使用方式主要为了解决大范围多点布控以及海量人脸库问题。



人证合一

人证合一即对当前人员的证件以及面部特征做双重认证。人脸识别技术在该类场景中承载了生物识别这一关键步骤，一般人证合一系统会首先对人员证件进行核验，证件核验通过后再通过人脸识别手段判定当前人员与预先注册人脸是否为同一人。

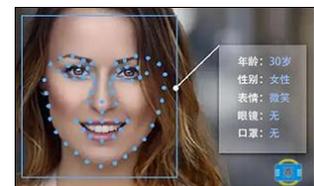
双重认证这一方式主要应用于对安全性要求较高的场景，例如机场控制区通行管理、重点实验室门禁、交通枢纽站旅客实名认证等场景。

验证环节并不局限于身份证也可以是本单位发行的工作证、通行证等其它带有 RFID 射频芯片的证件，除 RFID 以外还可选择扫描纸质条形码手机屏幕二维码等方式。



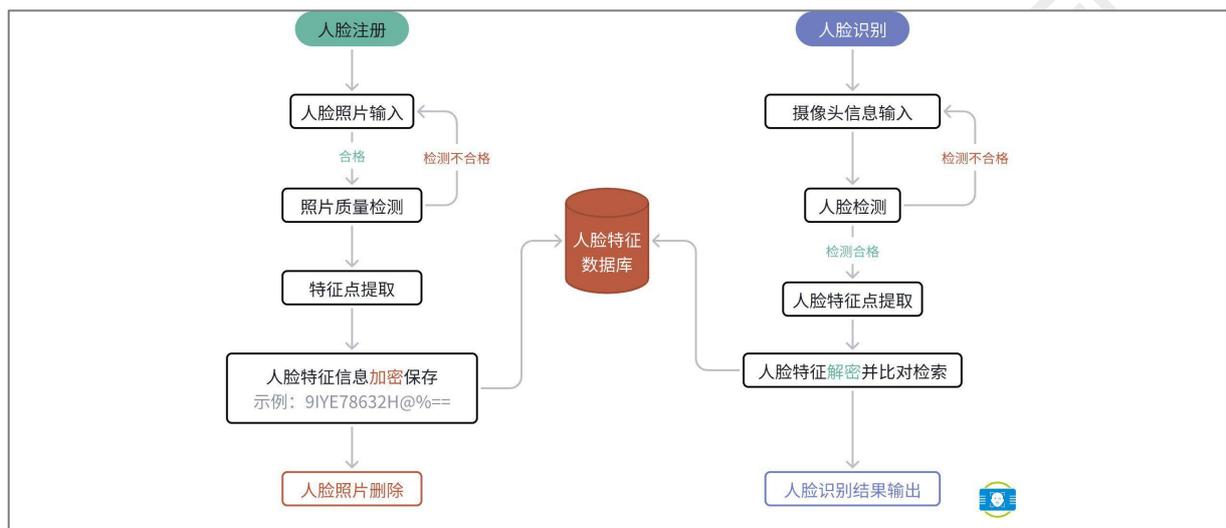
面部属性分析

面部属性分析是人脸识别技术的一个重要应用方向，通过人脸识别算法对面部五官的关键点位进行标注从而可以确认面部五官的位置形态，因此来判定当前人员的性别、年龄、喜怒哀乐、瞳孔方向、有无眼镜等信息。程序通过获取并分析这些面部属性信息可以实现多种复杂场景下的应用。在教育领域，可以通过获取学生面部属性信息来分析学生上课专注度；在线上考试领域，可以通过获取学员面部属性信息来防止学员考试作弊；在交通运输领域，可以通过获取司机面部属性信息来分析司机当前疲倦程度，防止疲劳驾驶带来的安全隐患。

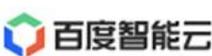


人脸识别数据安全问题

随着人脸识别技术的普及，面部数据的安全性成为一大挑战，不法分子可能通过各种手段窃取到面部数据，导致数据泄露。由于人脸识别对于数据采集的低门槛限制，也引发了人们对于大规模监控、人脸信息滥用、身份追踪等方面的担忧。为了解决这一问题，一些人脸识别技术厂商迅速做出调整，人脸识别全流程中不再保存人脸照片信息而以加密人脸特征值取而代之，经过加密后的人脸特征值不能被还原为一张图片，这样一来即可将人脸识别技术的使用限定在一定范围内。我国也在相关国标文件中发布了有关人脸识别数据存储相关要求中明确指出“应采取加密存储等安全措施存储人脸识别数据”^{Q2}。下面简单介绍一种加密存储人脸识别数据的流程：



主流品牌

 百度智能云	 ArcSoft 虹软	 腾讯云	 华为云
 云从科技	 商汤	 Suceed	 SIGNCARD

应用场景

人脸识别技术的应用场景可按照 1:N 或 1:1 两种使用模式分类：

1:1	1:N	M:N
高安全性场所：政府性会议、机场控制区、交通枢纽核査	考勤签到：单位考勤、会议签到	公安抓逃：机场、火车站、汽车站、演唱会
实名制场合：景区实名制验票、酒店入住	门禁安防：单位内部闸机	智慧交通：路口人流量分析
消费电子领域：手机解锁、刷脸支付	门禁、智能门锁	

注解:

①人脸识别算法：人脸识别算法是一系列用于处理和识别人脸图像的计算机算法，是人脸识别技术的核心。

②机器学习/深度学习：机器学习是人脸识别算法的基础学习模式主要通过数据中学习规律并根据规律做出预测和决策；深度学习侧重于通过深度神经网络来学习复杂的特征表示，深度学习在处理大规模和复杂数据时表现出色。

③1:1、1:N、M:N：这是三种不同的人脸识别技术应用模式，主要针对不同使用场景。1:1 模式即当前识别过程中的人脸库数量为 1 个人的特征，是为了解决当前待检测对象是否为本人；1:N 模式即需要从人脸库中识别出当前待检测对象是谁；M:N 模式即多对多关系，需要将多于 1 个的待检测对象与当前人脸库做对比，识别出待检测对象分别是谁。

④鲁棒性：指的是系统或算法对于外部干扰、噪声、变化或异常情况的稳健性和抗干扰能力。

引用:

Q1 引用自 [中华人民共和国国家标准《生物特征识别防伪技术要求 第 1 部分：人脸识别》](#)

Q2 引用自 [中华人民共和国国家标准《信息安全技术 人脸识别数据安全要求》](#)

Q3 引用自 [中华人民共和国国家标准《信息安全技术 远程人脸识别系统技术要求》](#)

Q4 引用自 [中华人民共和国国家标准《安全防范 视频监控人脸识别系统技术要求》](#)

免责声明:以上内容来源于网络公开信息和自撰，如侵犯您的权利或是有不准确的描述请通知我们。我们将及时删除有关您的内容且我们不对内容的权威性负责。

声明:谢绝同业公司复制或转载，非同业公司可下载使用，请注明出处。