Deepfake是一种换脸技术，可以将图片或视频中A的脸换到B的头上。其名字由深度机器学习（deep machine learning）和假照片（fake photo）组合而成。这项技术不需要操作者具备深厚的专业知识，只要收集到足够素材，AI就可以完成。Deepfake换脸效果逼真，让人难以分辨真假，这也引发了众多伦理和隐私问题。

AI换脸越来越溜儿 谁能阻止它走向堕落

本报记者 **陈 曦**

史泰龙和施瓦辛格两位好莱坞顶级流量功夫巨星最近一次合体出现在大银幕上，还是在2013年上映的《金蝉脱壳》中，这让不少影迷意犹未尽。11月22日，一篇报道称，国外视频网站上一部名为《Step Brother》的电影短片，借助Deepfake技术，把两位巨星的面部替换到了两名小众演员脸上，而且人脸表情自然，毫无痕迹，这让不少网友惊叹：太恐怖。此外，在最近的国内热播剧《了不起的儿科医生》中也使用了这种AI换脸技术。

根据安全分析公司Sensity最新调查结果，自2018年12月以来，Deepfake在线造假视频的数量大约每6个月翻一番，而截至2020年6月，造假视频已经多达49081个，比2019年7月增长了330%。

Deepfake技术让视频换脸变得越来越简单，如何打假“李鬼”，让其避免成为假视频的“帮凶”已成为当务之急。


视觉中国供图

用视频“大变活人”分几步

Deepfake这种技术堪称现代网络“易容术”，是比PS强大很多的动态换脸技术。“目前Deepfake技术已经很成熟了，主要技术分为两个部分，自动编码器和生成对抗网络。”天津大学智能与计算学部教授翁仲铭介绍。

自动编码器是一种神经网络技术，就是把一个人的照片特征抓取出来，然后用数字代表。但是抓取一个人的面部特征时，不可能抓取所有状态下的特征，比如说话、哭和笑等，那么就必须将没有的表情用数字模拟的方式展现出来。通过训练，就可以找出一个最好的用数学方式来呈现照片特征的编码器。

有编码器就需要解码器，解码器会把一串串数字再还原成照片。不同解码器可以在演员身上还原不同照片，比如史泰龙解码器可以还原史泰龙照片，而还原施瓦辛格照片则需要施瓦辛格的解码器。具体操作是先使用编码器分别抽取小众演员和史泰龙的特征，而后再使用史泰龙的解码器还原，从而得到史泰龙的脸和小众演员的表情。

“Deepfake就是在设计、训练精准的编码器和解码器。”翁仲铭介绍，因为编码器是抓取照片的特征，所以基本上只需要一套就可以了。可是解码器就需要训练很久，因为把一连串的数字特征，拼接到小众演员身上，而且要变得很像，就需要长时间训练。以换成史泰龙的脸为例，这个过程需要输入史泰龙600—3000张照片并经过48—72小时来训练深度模型。

“自动编码器做出的照片是否自然真实还需要去判别把关，这就需要生成对抗网络技术。”翁仲铭解释，这包括两个机器学习模型，分别为生成网络和辨别网络。生成网络扮演“造假者”，在模型训练后产生伪造影片；而辨别网络则扮演“检测者”，不断地检视假影片，直至它再辨别不了结果是假的。数据越多，效果越理想，假影片越真实。

换脸门槛越来越低

其实这种动态换脸技术最早是被用于影视后期制作，但是以前影视作品中的人脸交换操作起来非常复杂，只有专业视频剪辑师和公共网关接口专家才能完成，并且需要花费大量时间和精力。

但随着Deepfake这样公开且轻量化技术的出现，这个技术的使用门槛也越来越低了。特别是设计架构Deepfake技术的“大神”将代码上传到了一个自由共享代码的网站Github，让这项技术更容易获得。

利用Deepfake技术，即使是一个对视频剪辑一窍不通的外行，也只需一个强大的GPU（图形处理器）和上百张人物样图，输入至少一个算法，就能完成人脸交换，并且可以制作出非常逼真的视频效果。“普通人在经过一段时间的学习以后，完全能够掌握这项技术。”翁仲铭感叹。

“虽然现在这项技术操作起来简便，但是原来要用软件实现这个过程是非常艰难的。”翁仲铭解释，视频中人是动态的，比如一个60帧（fps）的视频中，每秒钟画面更新60次，如果是PS的话需要处理60张静态图片，然后将其前后连接起来形成一个动态图。一个短视频动辄数分钟，甚至十多分钟，如果按照一分钟处理3600张计算，一个几分钟的短片也要处理多达上万张照片，所以需要强大算力的GPU来支撑。

翁仲铭认为，近些年随着GPU的发展，其算力越来越强大，也使得Deepfake技术处理照片越来越轻松，使用越来越方便。这可能也是2018年12月以来，造假视频成倍增长的原因之一。

以技制技打假“李鬼”还不够

如此强大的“黑科技”采用了最先进的人工智能技术，通过比较简单的运算，就有可能生成以假乱真的视频。但是Deepfake技术在运行几天之后，就遭到了唾弃，被全球封禁，还被世人称为“最邪恶”的技术。

因为太过以假乱真，其破坏力不可估量。事实证明，人们的担心并非杞人忧天。Deepfake第一次亮相就是将《神奇女侠》盖尔·加朵的脸，嫁接到了一部成人电影女主角身上。此外由Deepfake制作的假视频已引发多起刑事案件，甚至卷入政治纷争。

不过再完美的技术也不是无懈可击的，专家们提出了几种辨识Deepfake换脸视频的方法：比如眨眼率，通过Deepfake制作的对象的眨眼率少于正常人；语音和嘴唇运动的同步状况；情绪不符合；模糊的痕迹、画面停顿或变色。不过翁仲铭表示，这些方法，Deepfake通过加强对样本的学习，都可以解决，迟早会有人可以通过Deepfake技术制造出人类用肉眼无法识别的“假脸”。

“也有不少人想到以AI对抗AI。”翁仲铭介绍，美国国防部研发了全球首款“反AI变脸刑侦检测工具”，专门用于检测AI变脸或换脸造假技术。不过，人工智能基金会的研究副主席戴利普承认，现时Deepfake检测算法的准确率，即使可高达97%，但鉴于互联网规模非常大，余下的3%仍然极具破坏力。

目前还有一个识别Deepfake换脸的新思路，叫作“活体取证”，该技术主要是根据分辨率、三维信息、眼动等来区分真假，因为翻拍的照片分辨率和直接从真人上采集的照片在质量、分辨率上比都有差别。

“整个算法遵循的观察规律是：生物信号还没有保存在假视频中，这些信号在生成噪声时也产生了不同的标识。”翁仲铭解释，换句话说，假视频中显示的“人”不会表现出与真实视频中的人相似的心跳模式，通过这种方法可以找到每个生成模型的唯一签名（标识）。值得一提的是，无论遮挡、照明条件如何变化，这些标识在真实视频中是不存在的。利用这些标识可以找到假视频背后的生成模型，然后反过来提高整体的假视频检测精度。

“道高一尺魔高一丈，利用Deepfake技术的人也在不断改进换脸的水平，因此从长远来看，我们必须寻求更有力的方法来维护和证明社交媒体信息的真实性。目前几乎没有任何工具可以帮助读者确信其在网上看到的信息来源可靠，且没有被篡改。”翁仲铭强调，改善这种情况需要从视频发布源头进行管理，比如实名制，同时加强立法，增加网络警察巡逻等，严厉打击这种造假行为。

瞭望站

由“主仆”关系变为“伴侣”关系，专家指出——

下一代机器人 最大特点是人机共融

本报记者 **张 晔**

“人机共融是智能机器人的重要特征，人机交互、人机交流、人机一体的新一代人机共融机器人将引领时代新潮流。”11月27日，在江苏南京举行的2020世界智能制造大会上，中国工程院院士谭建荣表示，与人共融将给未来人机关系带来根本转变，即由“主仆”变为“伴侣”。

2011年，美国启动先进制造业伙伴计划，其中明确指出，下一代机器人将与人类紧密合作，为产业工人、健康服务者、士兵、手术医生以及宇航员等完成复杂任务提供新的能力。

数据显示，2017年，人机共融机器人达到4211台，预计2020年会达到196277台，按照每台10万元计算，与人共融机器人产业规模将在2020年达到19.6亿元。

谭建荣介绍说，智能工业机器人的智能化特征具体表现在单机自主、多机协同、人机共融3个方面，“大数据智能技术带来的是场景识别智能，群体智能技术可以让不同机器人之间互联互通，而混合增强智能技术将实现人机交互拟人化”。

目前，人机共融机器人在汽车、医疗、传统制造业等领域的应用已经不稀奇，江苏省产业技术研究院智能制造技术研究所所长骆敏舟介绍，在技术上，他们已经完成了煎蛋机器人、按摩机器人、咖啡机器人的研究。

谭建荣认为，人机交互方式会随着物联网的更新升级以及人工智能的发展朝三个方面发展，即以用户为中心、个性化的生物识别和全方位的感知。

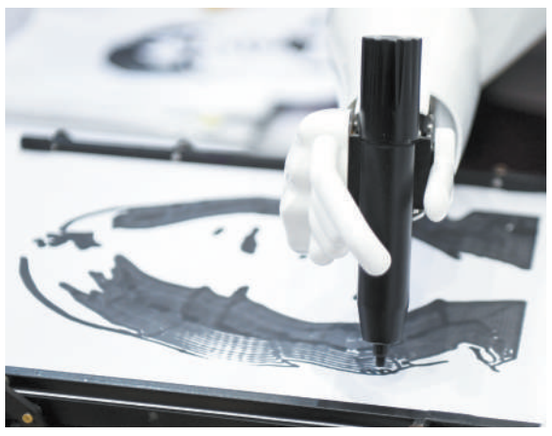
但骆敏舟也提出了自己的顾虑：“与人共融机器人新场景的应用也面临着非常大的挑战，主要有环境、任务、安全和交互4个方面。”比如军事机器人在复杂的环境中能否完成使命，医疗机器人能否在手术中万无一失，机器人进入家庭如何保障人类的安全等。

与挑战重重的服务型人机共融机器人相比，协作机器人是目前共融机器人中推广使用最多的一类。目前，用工成本的增加以及中小企业的自动化需求催生了协作机器人的诞生，我国中小企业有600多万家，提供了接近70%的制造能力，对机器人需求巨大，尤其是在电子、轻工、食品等领域迫切需要重量轻、协作能力强、拖拽示教机器人。

骆敏舟介绍，协作机器人主要为中小企业服务，可以有效降低用工成本，安全性也比较高，还可以帮助企业提高效率。目前，在去毛刺机器人、焊接机器人、喷涂机器人、码垛机器人等方面已经发展较为成熟。

机器人与智能制造密切相关。机器人的研发、制造、应用，是衡量一个国家科技创新和高端制造业水平的重要标志。哈尔滨工业大学机器人研究所所长赵杰介绍，虽然国外先进国家占据机器人先发优势，但要看到的是，当下人工智能、大数据、5G等新技术与机器人的融合，加上政策引导和支持，中国机器人正迎来加速发展的机遇期。但要实现弯道超车，一些行业痛点亟待通过转型升级解决：“这几年坚持下来，国产工业机器人在中国市场的占比总维持在30%左右，但我们的企业几乎没有利润甚至是微利。这种局面必须要改变，我们需要提升产品的性能，让中国机器人进入高质量发展的转型期。”

图说智能



机器画家

12月3日，由中国电子学会主办的2020佛山国际智能机器人博览会在广东佛山潭洲国际会展中心拉开帷幕。本次博览会汇集国内外机器人制造企业，全面展示机器人领域的前沿产品、核心技术以及最新的应用解决方案。图为深圳市智能机器人研究院的参展机器人在作画。

新华社记者 **邓华**摄

人机“攻防”

12月3日，2020世界机器人大赛总决赛在广东佛山与国际智能机器人博览会同期举行。本次大赛聚焦高精尖技术交流、产业技术应用、市场规模影响等方面，围绕科研类、技能类、科普类三大竞赛方向，设共融机器人挑战赛、BCI脑控机器人大赛、机器人应用大赛、青少年机器人设计大赛四大类赛事。图为选手在超级轨迹赛项中。

新华社记者 **邓华**摄

从运输工具到移动生活空间

未来智能汽车不止于出行

新华社记者 **吴 涛 陆 浩**

在广州黄埔区约144平方公里范围内的学校、医院、地铁站等近200个上下车点，市民通过手机App，就可以一键呼叫自动驾驶出租车，享受自动驾驶汽车的乘坐体验。

这是今年6月广州市首批20辆自动驾驶出租车投入运营带来的改变：智能汽车已真实地走进老百姓的生活。

广州市发展和改革委员会总经济师谭虹说，广州市智能汽车产业已构建起涵盖上游、中游以及下游的产业链，集聚上百家代表性企业；全市数十条道路上开放了道路测试，长度超过135公里；已颁发道路测试牌照24张，投放80辆自动驾驶出租车，并启动了自动驾驶公交应用示范线。

记者在12月4日闭幕的世界智能汽车大会上了解到，不仅在广州，智能汽车在全国也在快速发展。在北京、上海、长沙、苏州、武汉等地，各种智能汽车新项目不断涌现。

国家发展和改革委员会国际合作司副司长高健说，截至今年6月，全国17个城市已累计发放约282张自动驾驶道路测试牌照。

据中国汽车工业协会预测，中国将在五年内实现低速驾驶和停车场景下的自动驾驶，在十年内实现更多复杂场景下的自动驾驶。到2040年，道路上行驶的车辆将有四分之三是智能驾驶的车辆。

高健认为，到2025年全球网联汽车数量将接近7400万辆，其中中国网联汽车数量将达到2800万辆。

智能汽车是指通过搭载先进传感器等装置，运用人工智能等新技术，具有自动驾驶功能，逐步成为智能移动空间和应用终端的新一代汽车，被业内视为汽车产业颠覆性技术革命。其代表性的无人自动驾驶技术因自身特性也面临着“毫秒延迟、生死两隔”的挑战。

从我国智能汽车产业看，当前发展也面临不少难题。“智能汽车发展尚处于起步阶段，仍面临多重制约与挑战。需要继续以开放姿态开展智能汽车国际合作，构建更加科学和完善的专业人才培养体系，开展人才储备和梯队建设。”高健说。

中国汽车工业协会总工程师叶盛基说，未来智能网联汽车产业的发展需要海量数据支持，但目前单一车型的数据远不能满足未来L4级以上自动驾驶所需要的数十亿级的数据积累。此外，行业目前还未形成有效的数据共享生态，企业间还处于数据孤岛的状态。

芯片和系统仍面临“卡脖子”问题。国家发展和改革委员会国际合作中心主任黄勇认为，我国智能汽车在底层技术层面还需加快形成自主可控的标准化汽车技术系统和架构体系，解决芯片、软硬件和系统零部件等各类瓶颈。

但市场对我国智能汽车产业依旧充满信心。在与会嘉宾看来，随着中国数字经济的发展，交通数字化、信息化和智能化正让自动驾驶的应用前景变得更加宽广，智能汽车产业正迎来风口期。

会上发布的《2020智能汽车产业研究报告》预测，中国将可能成为全球最大的自动驾驶汽车市场，包括传感器、计算平台和软件在内的自动驾驶系统成本在2023年后将迅速降低，自动驾驶出租车预计将在2025年到2027年之间迎来商用拐点。

以“世界工厂”广东来看，作为全球重要的汽车制造基地，广东正在形成相对完整的智能汽车产业链。在整车领域，依托广汽集团、小鹏汽车、比亚迪等企业，智能汽车龙头效应在不断增强；在自动驾驶系统领域，小马智行、文远知行等初创企业相继落户，正推动L4级别技术的数据快速积累……

未来的出行，可能只需在手机上进行预约，无人驾驶车辆就会出现在你面前，并自动规划最优路线，将你送到目的地。

而随着自动驾驶商业化进程不断加快，尤其在新冠肺炎疫情催化下，自动驾驶商业化场景的探索向载货、多功能车领域不断拓展，承担最后一公里运输的无人配送车、无人清洁车以及矿山、港口等特定场景的商业化应用也开始显现。

“展望未来，智能汽车的商业化应用不仅能弥补劳动力缺口，更是将单纯的运输工具变成承载更多属性和智能的移动生活空间，让人的出行更加便捷、高效和舒适。”叶盛基说。

2020世界智能网联汽车大会室内展区展出的氢燃料电池无人驾驶车辆。

新华社记者 **任超**摄