眼见不一定为实
人工智能换脸如何“以假乱真”

人工智能换脸，曾经只会困扰名人，如今却能直接影响到我们普通人的财产安全。

伪造人脸盗号、转账的新闻不在少数。今年8月，就有两名犯罪嫌疑人因使用手机软件制作人脸识别动态视频，并“伪装”登录他人的网络账号盗取资金而被警方抓获。

另一则相关新闻提到，由于制作简单，一个视频价格仅为2元至10元，“客户”往往是成百上千元地购买，牟利空间巨大。

据悉，这类案件的非法获利额高达几千元至几十万元不等，全国各地已经发生了多起类似案件。甚至有不法分子利用银行的人脸识别授权功能，再通过木马病毒拦截短信验证码盗取存款，有的涉案总金额超过200万元。


“3D面具”技术

骗不过人，可以骗摄像头

人工智能换脸，术语是“深度伪造”，是把“深度学习”和“伪造”组合在一起，用AI把一个人的人脸换到另一个人的照片或视频当中的技术。

围绕人工智能换脸这一话题，有相当多的“犯罪应用”，包括且不限于：

1.攻击刷脸验证：直接从支付宝、微信钱包、贷款软件里，伪造他人信息套现；

2.制作虚假色情图片或视频：诈骗、敲诈勒索或损坏他人名誉；

3.实时换脸通话：盗号并诈骗号主亲友；

4.制造虚假信息：蒙骗投资者等；

5.发布假新闻：煽动民众、引起混乱恐慌、打击商业对手、制造股市动荡等。

在这当中，刷脸验证与普通人关系最大。因为它验证的是一个人的身份，一旦这个信息被突破，你的资产安全与信息安全都会受到威胁，很容易在网络上“裸奔”。

除了“深度伪造”技术，还有相当多的方法可以干扰人脸识别认证，比如造一个“人工智能眼镜”：在一篇图像识别领域的经典文献中，研究者通过数学运算设计了一种特定的“眼镜”，戴上就可以让一个人被人工智能技术识别认成另外一个人。

另外一种哄骗检测设备的方式是3D面具。

国外某公司曾在2019年年底声明，对于微信、支付宝的刷脸支付和火车站的人脸识别闸机，都可以戴着3D面具伪装成别人通过。

人工智能换脸，特别在哪？

以前对普通人来说，上述技术还不必过于担心，因为它们有着各种各样的缺陷：比如以往的“人工智能眼镜”主要是针对静态图片识别，无法突破动态人脸识别；而“人脸面具”需要定制，价值不菲且制作工艺复杂，用在普通人身上性价比并不高。

但人工智能改变了一切，简直把造假成本降到了“白菜价”。

伴随视频越短、像素越低、实时性要求（需要实时换脸还是可以制作完视频再发出）越低、欺骗对象警惕性越低、可用素材（就是目标人物的多角度照片、视频）越多，造假成本就越低。

举个例子，同样是一个人说话，之前可以利用某项技术直接将脸换成另一个人的脸（一些影视剧中可以看到），动作还算流畅，但“塑胶感”严重，一眼就能看出不是真人的视频。

这项技术训练的人工智能模型，就可以做出以假乱真的效果。可能只有在认真反复地观看下，才会发现：刚刚这个人额头的皱纹是不是在闪？

针对“人脸识别”，“深度人脸识别”软件就便宜很多。因为攻破“人脸识别”不需要最“精细”，“深度人脸识别”技术只需要一个清晰度一般的几秒钟的视频即可。

而制作后的更精细的视频，则可以用于其他的诈骗用途，并且这种造假是一种“一本万利”的买卖。在设备与算法齐全后，造假者就可以根据不同的情境与需求，批量生产假视频。

普通人能怎么办

当人工智能换脸进入普通人的生活，我们能做些什么来应对跟它相关的不法行为呢？

“骗”机器的换脸，咋办？

针对刷脸验证身份这一类场景，伪造的视频需要通过的是人脸识别系统的自动验证，或者说“骗过”机器。所需的视频时间短（几秒钟以内）、动态简单（只有少量固定动作、甚至有些系统仅仅识别图片）、没有实时要求，从技术上来讲是相对简单的，识别端也不在真人的掌控之中。

对于这类情况，普通人能做的就是平时守护好自己的个人信息（包括人脸信息），并且尽量采用多种方式结合的身份验证。

密码、指纹、手机号，能选的验证方式都选上。虽然自己也会麻烦点，但是相当于多了几道保险，全部被同时攻破的可能性还是小很多的。

如果不幸被盗刷，立刻报警，配合警察追踪不法分子、追回违法所得，同时上报平台，让平台获取更多的信息来修补漏洞、升级系统。

“骗”真人的换脸，咋办？

欺骗真人的人工智能换脸，比如面对个人的勒索、诈骗，还有面对大众的虚假新闻，则显得更加隐蔽和多样化。

从根本上来说，有了人工智能换脸技术以后，普通人面对图像信息都应该多留个心眼，不能一味相信“眼见为实”。

如果被人用伪造的裸照、不雅视频勒索，不要回应，直接报警。

这类犯罪的人工智能换脸目标就是受害人，所以只要看到的人知道自己没有拍过此类照片、视频，就可以判断该视频或图片是伪造的。其最大的难点反而在于不要自乱阵脚，不要因为害怕而向不法分子交付钱财。

如果被人用伪造的视频诈骗，比如骗子盗了你朋友的号，用人工智能换脸跟你实时通话借钱。这个时候，多渠道验证就很重要，可以通过社交平台、邮箱、短信、电话等去验证是否是朋友本人，不要因为对方看起来很着急就不假思索地打钱。

在观看网上的新闻、视频时，多查查新闻来源是否可靠，尤其是名人讲话。这些名人们可用于机器学习的训练集太多了，仿造高精度视频很容易。

据“科普中国”

新闻链接

识别小技巧

还有一些小诀窍，可以帮助你更好地判断一个视频是不是人工智能换脸伪造的：

关注脸型

多看看脸的大小、形状、下颚线位置，尤其是动起来的样子，和本人是否一致。

关注皱纹

毕竟每个人的皮肤情况和皱纹走向都是不一样的，人工智能模型仅凭一些照片（而且不一定是最近的照片），生成的皱纹很难跟本人一模一样。

一个人皮肤过于光滑、皱纹过多，或者全脸皮肤状况不一致（比如额头很多皱纹、脸颊却很光滑），一段视频中年龄感不一致（一会儿看着年轻一会儿看着年长），都可能是伪造视频的特征。

关注背景

看看这个背景是不是平时用的背景，背景和人的衔接是不是自然，背景本身有没有变形等。

关注光影

人工智能换脸生成的视频并不遵循现实世界的物理光影规则，因此面部的阴影、眼镜的反光等，都可能出卖伪造的视频。

关注五官位置和大小

人工智能伪造的视频可能会出现五官忽大忽小、位置飘移的现象。

关注面部特征

如果这个人脸上有痣、疤痕等，它们看起来都在正确的位置吗？

关注头发

发量、发际线看起来真实吗？头发边缘看起来自然吗？

关注动态

比如眨眼的频率和方式是否正常，眉毛和嘴的运动是否是平时的样子；转头（尤其是转到90度的侧面）的时候有无变形，脸部被遮挡的时候遮挡物是否清晰可见。

以上这些都是一些辨别人工智能伪造视频的要点。