种是接入实时换脸的视频。前者目前的制作成本非常低，有公开成熟的应用可以支持该项工作；后者虽然没有发现有公开的应用，但也有非常成熟的技术手段可以支撑。做成一段视频的时间和设备、算力等因素相关，当前技术可以做到实时产出结果。基于目前的技术能力，替换前的原始视频图像在面部清晰、正脸无遮挡、无夸张动作等条件下，会展示出比较好的效果。

不过在萧子豪看来，“诈骗成功率接近 100%”的结论要打个问号——目前人们看到的报道都是已经被骗的案例，但不代表在实际发生过程中，所有的诈骗行为最终都成功了。诈骗成功率是由很多因素决定的，不完全由诈骗分子的技术能力决定，个人的反诈意识也是重要因素。但不能否认，深度合成技术在一定程度上模糊了真与假的认知边界，使得识破诈骗的难度变得更高了。

知道创宇业务安全产品线总经理鄢晓玲在接受《新民周刊》专访时指出，无论是之前的 AI 语音、AI 换脸，还是现在由 AIGC 生成的语音、视频，它们底层用的都是同样的算法和技术。ChatGPT 的发布和开放，很大程度上带动了 AIGC 的开源社区的活跃度，从而涌现出了大量的开源模型和成熟产品。以前的图文比较割裂，但现在的技术就像“大脑”一样，可以让图文音视等多个模态，完美地结合起来，并自如地去切换和应用，从而能更容易地生成那些逼真的诈骗素材。

> 从理论上来说，**技术的提升导致了诈骗率的提高。**

“原来只能生成一些相对来说比较静态的，或者是固定套路、固定话术的内容，但是现在有了一些底层的知识和一些预设的身份以后，你就可以跟 AI 数字人自如地对话了，这在以前是做不到的，只会在影视剧的制作中使用类似的技术。”在鄢晓玲看来，现在一下子推出了那么多成熟的应用和产品，让普通人都能轻易上手，也就使得骗子更容易制作出逼真的音视频素材去进行诈骗，“从理论上来说，技术的提升导致了诈骗成功率的提高”。

下图：在 2019 年，国内出现过一款换脸软件“ZAO”，许多明星、名人遭到恶搞、被造黄谣。

普通人只有被骗的份儿?

一键换衣、制作不雅视频等等，包括之前在互联网上广为流传的特朗普被捕照片，现在的 AI 生成的东西太真实了。实际上，目前 AI 已经可以批量制作大量的视频，制作多段替换成同一人物的视频，也可制作同时替换为多位人物的视频。

作为普通人，我们可能根本无法识别。

比如，一些微商团队发布明星的祝福、宣传视频来发展下线，其中不少视频并非明星真实录制，而是运用了 AI 换脸、AI 语音合成等技术制作而成，不少人信以为真而选择加入，结果陷入骗局；还有一些人利用 AI 生成图片、视频进行裸聊诈骗，要求受害者下载 App 进而将其手机通讯录拷贝过来，后续以此为要挟进行敲诈，很多人中招。

那么，有没有一些小技巧可以帮助普通人去进行初步的识别呢?

萧子豪建议，如果遇到这类疑似 AI 换脸诈骗的情况，可以在视频时有意识地引导对方做一些动作，如大幅度的摇头或张嘴。就目前的 AI 伪造水平来讲，仍然没办法在有遮挡及人脸偏转的情况下，生成无瑕疵的视频效果。

“我觉得让对方张嘴是一个比较有效的方式，比如看对方的牙齿结构是否清晰、舌头形状是否完整，很多不法分子可能只考虑对正脸做个建模，但没有建模嘴巴、牙齿跟舌头。如果骗子技术手段较弱，那么我们有可能发现对方面部边缘或者牙齿的瑕疵，从而识别出 AI 换脸。不过，这个方法对于识别出‘高水平’的不法分子，还存在难度。”萧子豪表示。

如果疑似是声音伪造，可以试一下与对方用方言交流。不过，这个方法同样难不倒高水平不法分子，目前方言合成方法和工具也非常丰富，音色很稳定、自然度也很高。最好的办法可能是可以追问几个只有你与对方之间才知道的私密信息，