耳听为虚 眼见不为实！揭秘AI换脸诈骗

山东省广播电视局广播电视监测中心

胡顺淑 侯明轩 李梦雅 王绍宁

随着科技的飞速发展，人工智能技术在各个领域都展现出了惊人的潜力，其中，AI换脸技术因其独特魅力而备受关注。然而，这项技术的普及也带来了新的安全挑战——“眼见不实、耳听也是虚”的AI换脸诈骗。

1. 诈骗案例

1.企业诈骗

这是最常见的AI换脸诈骗类型之一。诈骗者利用AI技术，将企业高管的面部换到自己的视频通话中，然后冒充高管向公司员工或合作伙伴发出指令，要求转账或透露敏感信息。2019年，一家英国能源公司就因此被骗走了24.3万美元。诈骗者通过AI换脸技术冒充公司CEO，向财务经理发出紧急转账指令，导致公司损失惨重。

2.名人诈骗

诈骗者使用AI技术，将名人的面部换到虚假的视频中，然后通过社交媒体或电子邮件向粉丝或支持者发送请求，要求捐款或提供个人财务信息。2020年，有报道指出，某知名演员的面部被AI技术换到了一段虚假的筹款视频中，试图骗取观众的捐款。

3.情感诈骗

在一些案例中，诈骗者使用AI技术，将受害者的伴侣或亲人的面部换到虚假的视频中，然后通过视频聊天或社交媒体向受害者发送请求，试图获取财务信息或进行情感操控。这类诈骗通常利用受害者的情感脆弱性，使他们更容易上当。

4.勒索诈骗

诈骗者使用AI技术，将受害者的面部换到不雅的视频中，然后威胁受害者，要求支付赎金，否则将公开这些视频。这类诈骗利用了受害者的羞耻感和恐惧心理，使他们更容易屈服于勒索。

1. 识别技巧

1.面部动作异常

AI换脸技术在面部表情和动作的同步上往往存在缺陷。仔细观察视频中人物的面部表情，尤其是眼睛和嘴巴的微小动作。如果发现表情僵硬、不自然，或与人物的语音和情感不匹配，那可能就是AI换脸的迹象。例如，眨眼频率、微笑时的嘴角弧度等，都可能与正常情况不符。

2.瞳孔不自然变化

在AI换脸的视频中，人物的眼睛往往会出现闪烁或不自然的光斑。这是因为AI在处理眼部区域时可能遇到困难，无法完美复制真实的瞳孔反射。如果瞳孔在不同光线条件下反射异常，或者瞳孔大小在视频中不自然地变化，这可能是AI换脸的标志。

3.背景与人物不协调

AI换脸视频中，人物与背景的融合可能会出现瑕疵，比如光影不一致、边缘模糊或比例失调。例如，人物的阴影与背景不匹配，或者衣服颜色在视频中不自然地变化等。

4.面部动作存在瑕疵

AI换脸视频中，人物的唇形与所说的话可能不匹配，或者声音与面部表情不符。如果视频中人物头部转动或者面部被手部等其他物品遮挡、触摸时存在不协调现象，那可能就是AI换脸的视频。注意观察人物的唇形和发音是否同步，声音的音调、语速是否与面部表情相匹配。

5.专业工具检测

Deepfake Detection Challenge（DDC）等专门用于检测AI换脸视频的工具，可以对可疑视频进行检测。这些工具通常基于深度学习算法，能够分析视频特征，判断是否为AI换脸视频。

1. 防范策略

1.保持警惕和怀疑态度

在收到疑似AI换脸的视频时，不要轻易相信，应多方核实信息。如果视频内容涉及敏感或重要信息，更应提高警惕。

2.加强个人信息保护

避免个人信息被不法分子利用进行AI换脸诈骗。定期更改密码，不随意泄露个人信息，尤其是面部照片和视频，这些都是AI换脸诈骗的重要原料。

3.提高公众意识

通过教育和培训提高公众对AI换脸诈骗的认识和防范能力。了解AI换脸技术的基本原理，掌握识别虚假视频的方法，可以有效降低受骗风险。

4.寻求专业帮助

如果怀疑自己可能成为AI换脸诈骗的受害者，应立即向警方或相关专业机构求助。他们有专业的知识和工具，可以帮助你确认信息的真实性，采取相应的应对措施。

面对AI换脸诈骗这一新型网络威胁，我们需要提高警惕、加强个人信息保护、提高公众意识和寻求专业帮助。让我们携手构建一道坚实的防线，共同构建一个更加安全可靠的数字世界。