Publication: Xinhua.Net Online
Date: 09 December 2019
Headline: Beware! Waving your hands in pictures may result in fingerprint theft 当心！挥手照片可能泄露指纹信息

Beware! Waving your hands in pictures may result in fingerprint theft 当心！挥手照片可能泄露指纹信息

你流传到网上的照片、视频，若被拿来做人脸识别，极有可能被解锁；挥手的照片，也有可能泄露指纹信息……在12月6日—8日召开的第15届信息安全与密码学国际会议上，有专家接受记者采访时表示，面部身份验证、指纹等生物识别手段，容易受到面部伪造等手段的攻击，建议将生物识别认证与其他辅助认证手段相结合，保护用户信息安全，而容易被大家忽视的人脸失真信息，也可以反其道而行之进行身份识别。

每天，大量的个人图片和视频都会出现在网上，这给一些黑客提供了可乘之机。“身份验证系统已经广泛应用于真实世界的各种应用程序中，然而，面部身份验证通常容易受到攻击，我们的照片、视频或3D 虚拟人脸模型，会被黑客拿来欺骗面部身份验证系统。”新加坡管理大学（SMU）安盛网络安全讲座教授邓慧杰说，他曾做过试验，“发布在网上的个人照片，能成功解锁70%的用户面部识别”。

在邓慧杰看来，有些人脸识别系统并不安全，例如，虽说认证时会要求用户点头、眨眼，“但黑客可以借助视频解锁人的面部的三维信息，或者把照片上的眼睛、嘴巴抠掉，用软件去模拟动态特征来解锁”。

近日发布的《人脸识别落地场景观察报告（2019年）》显示，许多场景的人脸识别设备没有提供隐私政策或用户协议，公众无法在知情同意的前提下使用。例如在一些设置了人脸识别摄像头的商场内，消费者甚至不知道自己会被拍摄。

一边是道高一尺魔高一丈的解锁技术，一边却是难以察觉的“丢脸”困境，如何保护用户信息安全？邓慧杰介绍，目前，有研究开始建构人脸更为健全的生物信息，例如用红外、热源检测人脸的血脉信息，查看是否有真实的血液流动。

最近，邓慧杰在一个学术会议上发表一种新技术，他在人脸上采集了66个点位的信息，将手机置于距离人脸20厘米的位置后，开始拉远到40厘米，移动的过程中，拍摄下人脸从失真到逼真的画面。“我们一般拍照时，很少会拍自己失真的画面，因为画面是失真扭曲的，但这可以作为身份验证的信息，66个点位之间的影像距离，会随着手机的拉远，逐渐发生变化，这些失真的信息对每个人也是独一无二的，目前难以被攻克。”邓慧杰说，将这些人脸信息采集下来后，他们还会将信息输入机器学习的模型，让机器去计算、验证。

同时，他建议，不能把生物识别作为唯一的认证办法，“一定要有其他的辅助认证手段，例如口令短信、检测身份的智能硬件、保密问题等”。（金凤）