Sensor-Assisted Facial Recognition: An Enhanced Biometric Authentication System for Smartphones

JAN 20TH, 2016

论文下载：http://spirit.cs.ucdavis.edu/pubs/conf/shaxun-mobisys.pdf

摘要

人脸识别是一项非常流行的生物认证技术，但是它却很少在实际中使用，尽管大部分的手机都配备了前向摄像头。安全性（2D媒体攻击和虚拟的摄像头攻击）阻碍了在移动设备中使用人脸认证技术。在本文，我们提出了一种新的利用传感器辅助的人脸认证方法。在不牺牲认证速度的前提下，我们通过使用运动传感器和光传感器来抵抗2D媒体攻击和虚拟的

摄像头攻击。在450次实际测试实验，我们可以达到95-97%的检测率和2-3%误报率，比现有的3D人脸认证速度快9倍。

介绍

比起传统的基于证书的认证方法，生物认证拥有很多优点。一般认为生物认证更加安全，因为它的原理是基于“用户是谁”，而生物信息很难被伪造或者被修改。基于证书的认证依赖于“用户知道什么”，而如果这个信息丢失或者被偷会导致身份被盗。另一方面，生物认证使用起来更加容易。

人脸识别是一种非常流行的生物认证技术。由于其准确度高，并且如今的智能手机大部分都有前置摄像头，图像的分辨率高，人脸认证似乎应用前景更加广泛。

然而，实际中人脸认证技术很少被应用于智能手机中，尽管手机配备了前置摄像头。Andriod从4.0版本提供了人脸识别的功能，但是并没有很多用户使用它。除了隐私问题，有两个非常重要的问题阻碍了人脸认证技术的发展。

第一个原因是在安全和易使用之间有权衡。简单的2D人脸识别，很容易被用户的照片欺骗。另外一个改进版是通过在认证过程中要求用户眨眼睛，这个很容易被编辑的图片或者放一段视频欺骗。目前，已经有一些复杂的3D人脸认证技术。然而，这个认证的过程要求用户朝4个方向移动头，时间大约需要30s。由于比输入密码复杂，用户不愿意选择这种认证方案。因此，当前的人脸认证方案不能够同时做到抵抗2D媒体攻击和容易使用。

第二个原因是虚拟的摄像头的可用性。这里，虚拟的摄像头指的是一系列在真实的物理摄像头和操作系统增加一层的软件。这些软件可以做到让操作系统相信一段之前录制的video是实时的网络同步video.

在这篇文章中，我们希望提出了一种新的人脸认证方法,不仅仅更加安全，并且使用起来容易，快速。它能抵抗2D媒体攻击和虚拟的摄像头攻击。同时，认证速度可以与基于证书的方法相媲美，比现有的3D人脸认证方法更快。
文章的贡献在于：

- 提出了传感器辅助的人脸认证系统。提出了检查鼻子角度的方法来抵抗2D媒体攻击。
- 提出了运动-矢量相关的算法来处理虚拟的摄像头攻击。
- 在Galaxy Nexus，Android 4.2.2上实现了算法。该算法在对抗2D媒体攻击和虚拟摄像头攻击上具有高检测率，平均认证时间大约是2秒。

传感器辅助的人脸认证方法

如今的智能手机配备了运动传感器（加速度传感器和回转仪），邻近传感器，罗盘和光传感器。麦克风可以看作声音传感器，GPS可以看作是位置传感器。传统的人脸认证仅仅是通过捕捉用户的人脸图像/视频，然后与预先知道的模板进行比较。
在我们的方案中，除了使用视频摄像头和已有的人脸识别策略，我们使用光传感器和加速度传感器来抵抗2D媒体攻击和虚拟的摄像头攻击。我们的方法仅仅需要用户拿起手机，水平地移动一小段距离，就完成了。我们的方法不需要同步的过程。具体的算法见图2：

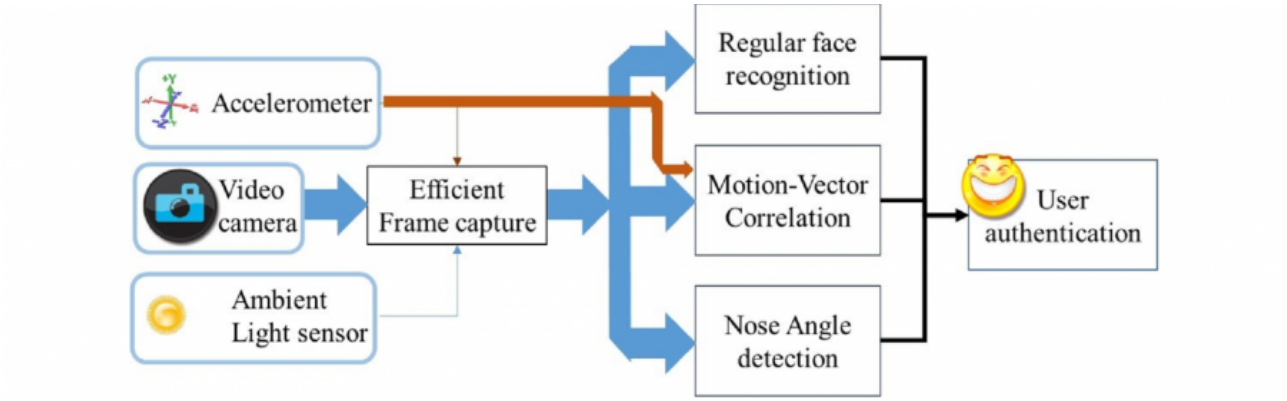

Figure 2 Block diagram of proposed approach. Existing face recognition schemes use 2D frames from smartphone camera to authenticate the user. Our approach builds on top of regular face recognition algorithms to counter 2D media attacks and virtual camera attacks. 2D media attacks are countered by Nose Angle Detection algorithm while virtual camera attacks are countered by Motion-Vector Correlation. The ambient light sensor is used to improve the lightening conditions of face-capture from different angles. The accelerometer sensor is used to select inputs to NAD algorithm and as an input in MVC algorithm

- 定义2D媒体攻击： 攻击者使用包括用户脸的平面照片或者视频片段来欺骗认证系统，使它相信这是一张真实的用户的脸。
- 定义虚拟摄像头攻击： 攻击者利用虚拟摄像头软件制作一段事先录制好的视频，使认证系统相信这段视频是实时捕捉的。攻击者知道认证的全部知识。

鼻子角度的检测

通过摄像头在人脸之前水平的移动，我们已经有了一系列的图片（或者视频帧）。给定一张包含用户脸的图片或者视频帧P。我们通过以下几步对它进行处理（见图4，图略）：

- 灰度转变
- 直方图均衡
- 鼻子检测
- 边缘检测
- 直线拟合

最后，我们可以得到鼻子的角度。如果它是一张真实的脸，当摄像头跨过绿色的线时，角度的方向是反转的。而如果只是平面的照片，方向的变化不会发生。

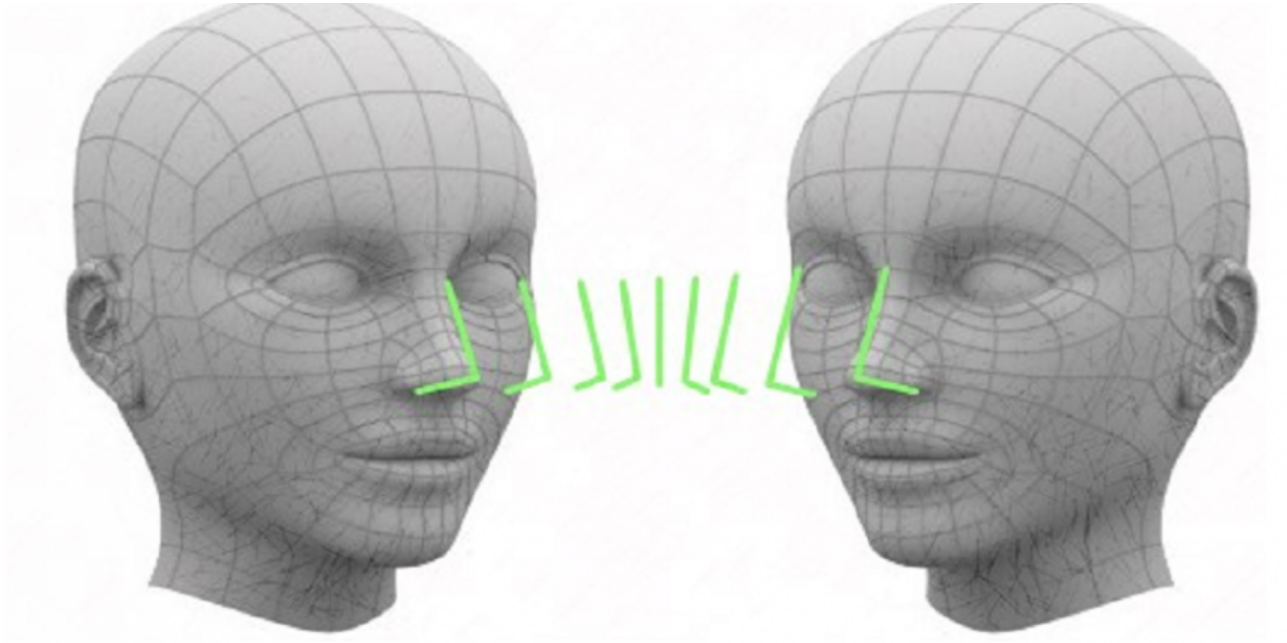

Figure 3. Change of the nose in a sequence of images

具体实现中的一些问题讨论

论如何设定认证开始的时间，如何人脸识别，如何水平移动，如何使用光传感器，最后得到了加速度数值。

处理加速度数值， 评估是否受到2D媒体攻击：

1. 评估重力加速度
2. 去除重力加速度的影响
3. 得到实际的加速度数值
4. 得到移动到最左边的时间和移动到最右边的时间
5. 使用最左边和最右边时间周围的视频帧来检测是否受到2D媒体攻击。

运动-矢量相关

方法的基本思想是从视频里提取晃动，并且与运动传感器的晃动比较。如果这两种晃动匹配，我们可以推测出这个视频是实时捕捉的；否则，它很有可能是虚拟摄像软件事先录制好的视频。重要法则是只是使用小范围的随机晃动。

1. 从视频里提取晃动

- 通过对 Pi 进行处理， 匹配两个连续的图像帧 Pi 和 Pi-1, 进行移动，旋转和放大的操作，然后计算相关系数：

$$r = \frac{\sum_{0\le x<m,0\le y<n}(p_{x,y}-\bar{p})(q_{x,y}-\bar{q})}{\sqrt{\sum_{0\le x<m,0\le y<n}(p_{x,y}-\bar{p})^2}\sqrt{\sum_{0\le x<m,0\le y<n}(q_{x,y}-\bar{q})^2}}$$

- 选出 Pi 之后，再将 Pi 进行操作。将 Pi 分成小块，然后进行水平和垂直的移动来匹配 Pi-1。如果大部分的操作是一样的或者接近，我们用这个值作为 Pi 的晃动；否则我们考虑给每一块分配优先级，最高优先级块的平均调整度作为 Pi-1 的晃动。

2 从加速度数值中提取晃动：去除加速度的Z维

3 计算类似度：

$$\rho = \frac{E[(\vec{\mathcal{A}} - E(\vec{\mathcal{A}}))(\vec{\mathcal{K}} - E(\vec{\mathcal{K}}))]}{\delta_{\vec{\mathcal{A}}}\delta_{\vec{\mathcal{K}}}}$$

性能比较

9个志愿者，每个人执行20次人脸认证的实验。每个志愿者带两张照片和一个片段的视频。每次照片（视频）十次测试, 得到180组真实测试和270组攻击。一半实验是在室内，另外一半是在室外完成。此外，我们对比90次使用3D人脸认证，和90次使用用户名和密码登陆。

- 2D媒体攻击的检测精确度： 该攻击在智能手机或者服务器被检测

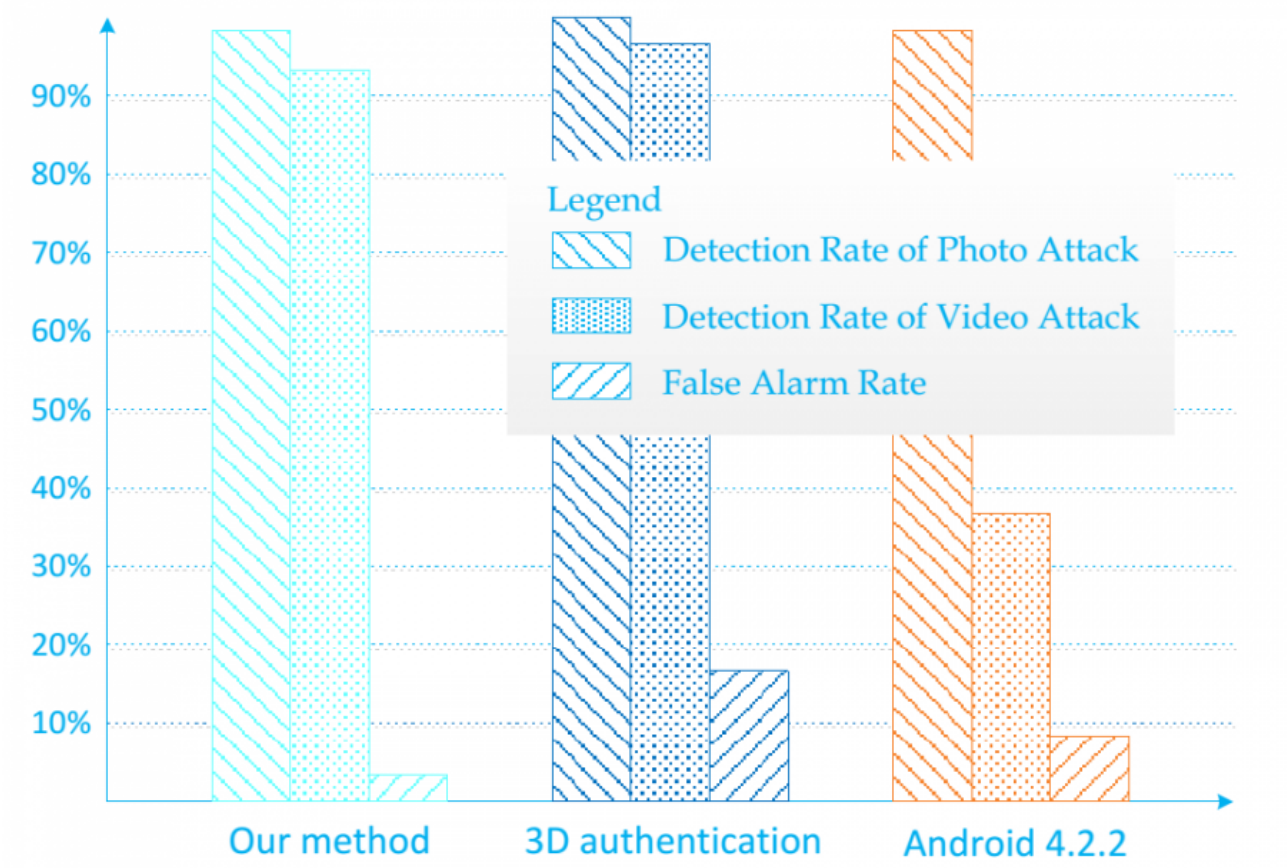

Figure 9: Comparing the detection accuracy with state-of-the-art appraoches

- 虚拟摄像头攻击检测精确度: 该攻击只在服务器被检测，认证的视频和传感器数据实时地从智能手机传给服务器

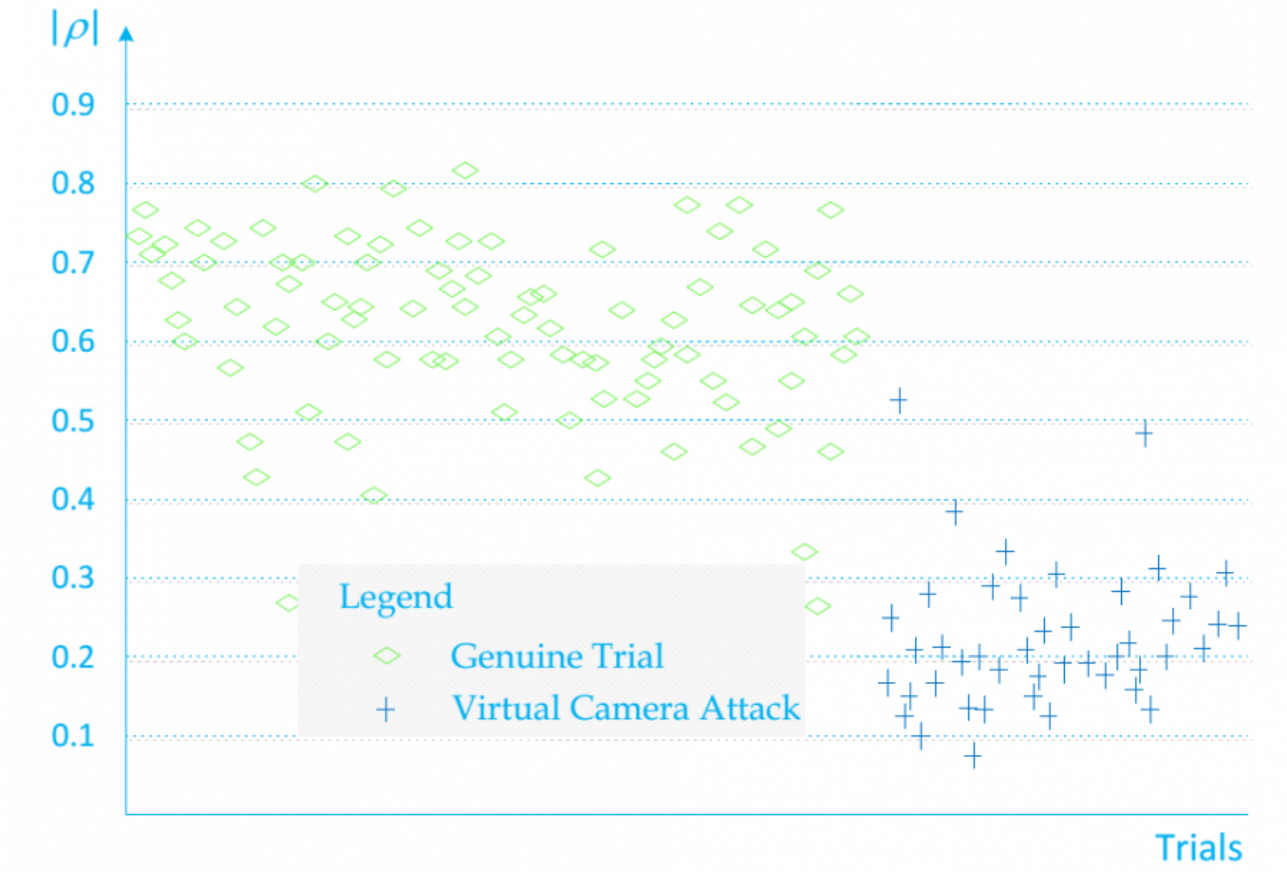

Figure 11: Threshold between attacks and genuine trials

- 认证速度和可用性：

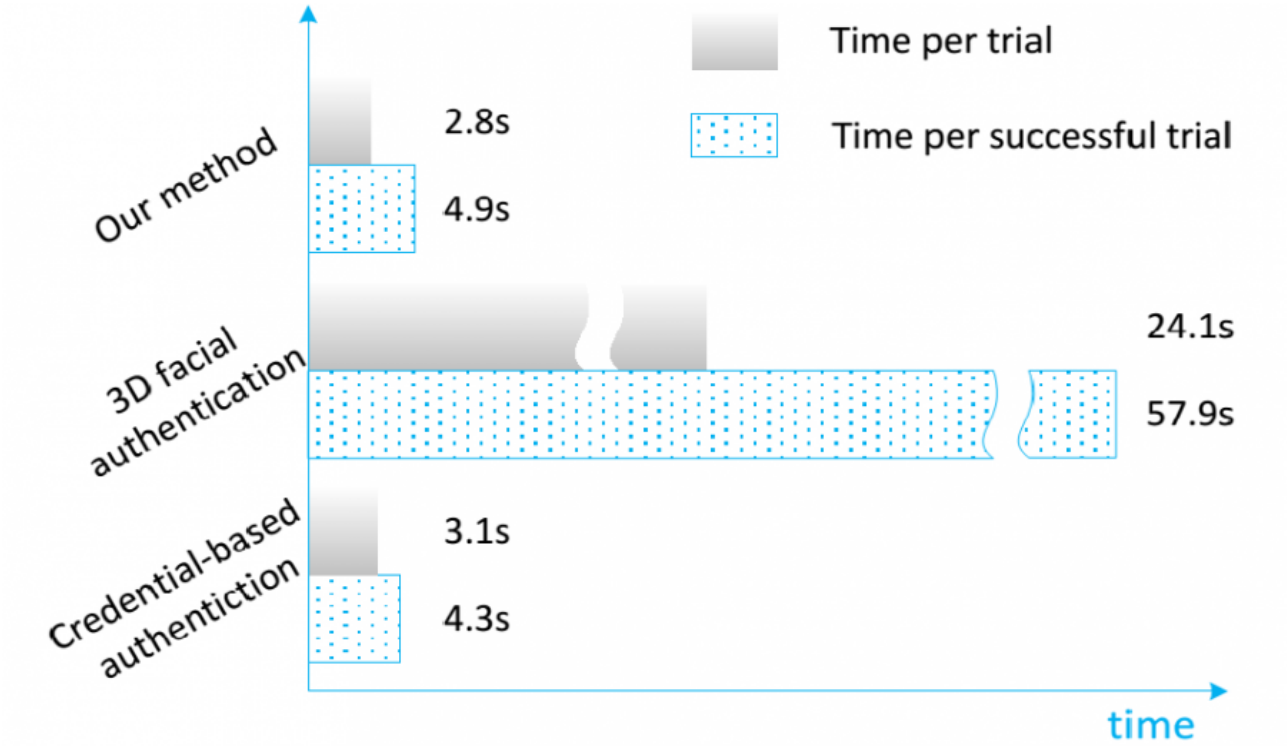

Figure 13: Authentication time comparison

结语

默认的人脸识别方法的准确度会影响该系统的总体的准确度。

提出的安全方案是基于手机里的传感器数据并没有被篡改。在最开始的阶段，我们认为偷了手机的人并不能妥协Android操作系统。攻击者可能通过一个Trojan App来记录视频和传感器的数据，然后重放收集的数据来通过认证。如果用户不安装不信任的App, 这个攻击可以被解决。