京东安全

格物致知 聚力安全

2017第五届京东安全峰会

打劫行走的活体密码

About me

- 小灰灰，百度安全实验室 XLab 安全研究员，硬件安全/AI安全
- 曾负责百度应急响应/0day分析/代码审计/安全监控体系建设
- 不知名摄影师，Adobe Photoshop 认证级
  - 为生物识别分析提供大量
    - 理论基础
    - 图像处理经验
    - 实验器材

为什么要做这个分享

- 做一些不一样的
  - 身边牛太多 web牛/渗透牛/二进制牛/移动牛
  - 研究资料貌似很少
  - 所有人都认为他们很安全　实际呢?
  - 让大多数人都能听懂、感兴趣
  - 推一些普遍的安全风险
  - 有得显摆

  - 宝宝心里苦

  - PS：部分内容不宜对外，PPT无法分享，见谅
  - （这个是删减版）

内容

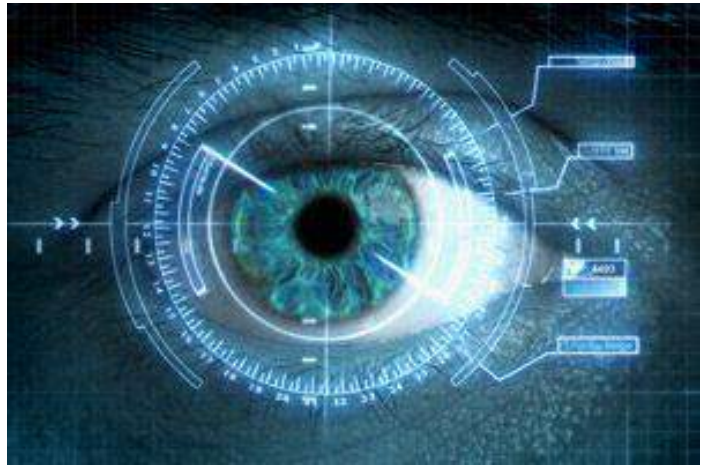
- 先放结论：
  - 经我们研究测试，常见的生物特征识别都存在易于获取、易于伪造的风险，反而变得更加不安全。

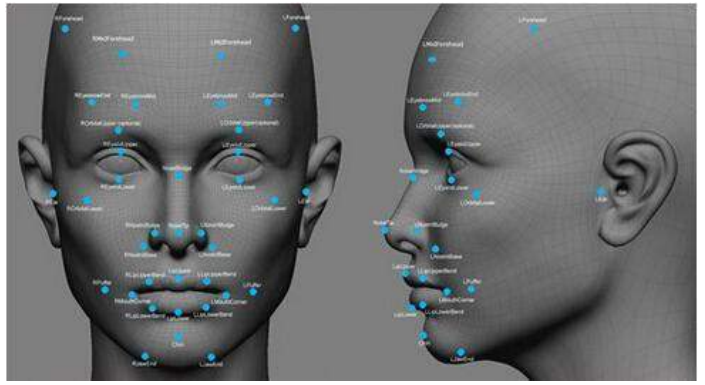
- 介绍生物特征识别
- 常见生物特征 指纹、虹膜、人脸、静脉的：
  - 结构、识别原理、匹配算法
  - 绕过方法及演示
- 思路总结及安全建议

什么是生物特征识别

- 通过计算机利用人体所固有的生理特征（指纹、虹膜、人脸、DNA等）来进行个人身份鉴定的技术

- 技术
  - 指纹
  - 人脸
  - 虹膜
  - 指静脉（首次展示！）
  - 声音（请右转参考深度学习）
  - DNA（唯一无能为力的）
  - 手型（形状识别）
  - 掌纹（类似指纹）
  - 掌静脉（类似指静脉）
  - ……





每个人所认为的更安全的方式

- 密码学中认证：
  - 我是谁（指纹、虹膜、面部、习惯）
  - 我有什么（token、证书、U盾、手机验证码）
  - 我知道什么（密码、安全问题、订单、好友）
- 密码难记/输入；token、证书也不方便

- 各种生物特征识别技术出现，更加认可，方便
  - 唯一性?
  - 无法被看见（甚至表皮下），所以就无法被偷走?
  - 检测设备只认活的，伪造是不可能的?
  - 单一使用

实际上反倒更不安全

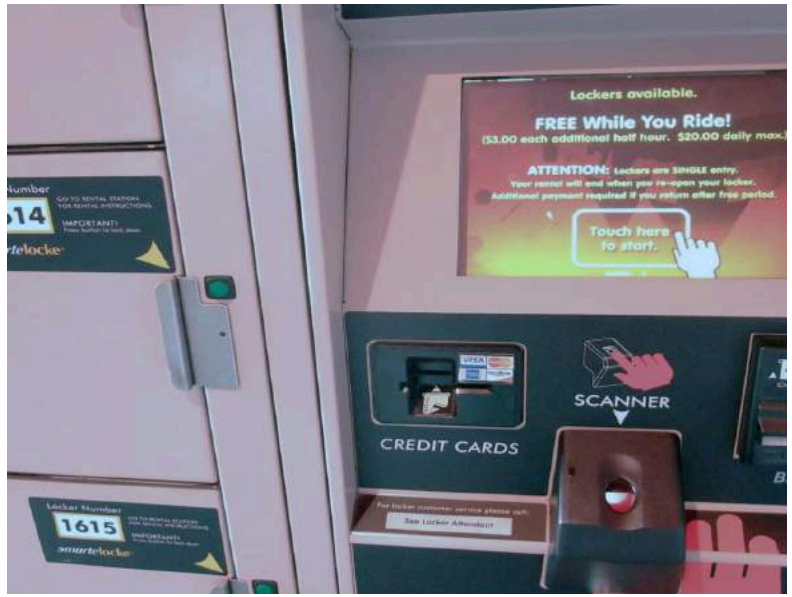
- 设备需要验证，它也需要先看见的
  - 它怎么看见，我们就照做
  - 甚至比它更酷炫
- 看见了不代表克隆出来
  - 并不需要完全一样的活物，看起来样子一样就行了
- 人家会检测是不是活的啊
  - 噱头，实际上并没有，已有的也很好绕过
- 完了，。。。好像确实不安全哦

一种研究思路

- 目标：当然是bypass掉某种生物特征识别：特征符合并允许通过

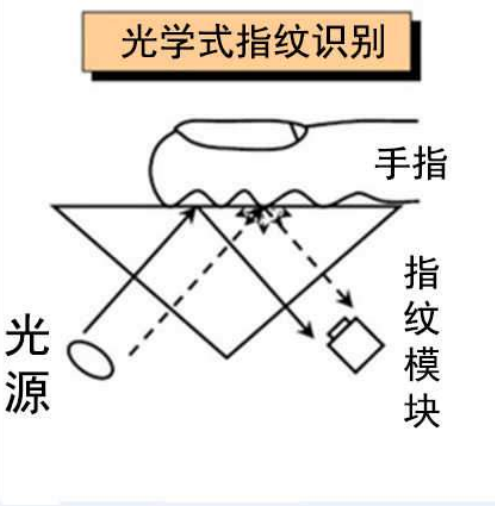
- 方法：
  - 控制传感器“看”到的内容
    - 得到目标正确通过时的特征内容
    - 用更加简单的介质（不是生物体本身）体现出正确特征的样子，骗过传感器

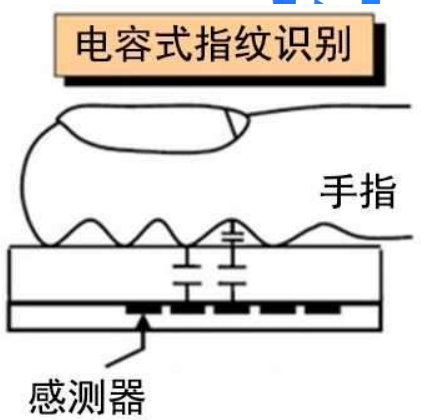

继续

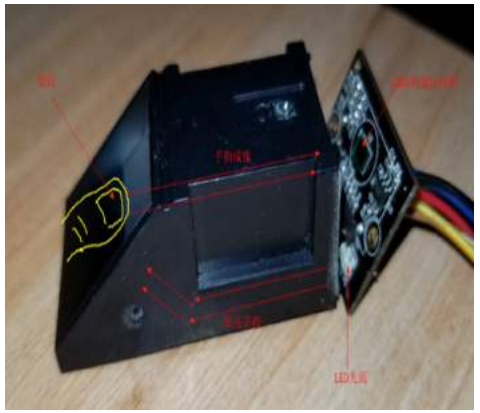

Lockers available.
FREE While You Ride!
ATTENTION:
Touch here to start.
SCANNER
CREDIT CARDS
1615

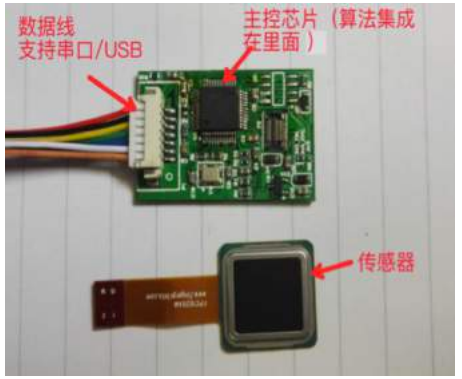
指纹识别

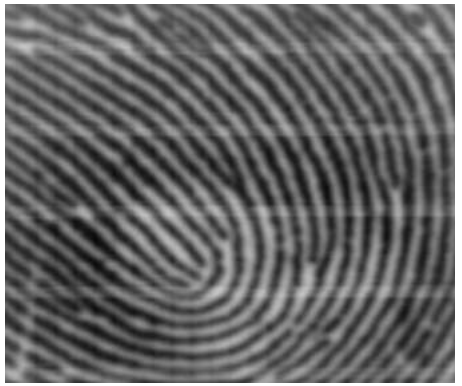
- 分类
  - 光学、电容
- 识别过程
  - 指纹图像获取
  - 预处理
  - 图像增强
  - 特征提取、比对





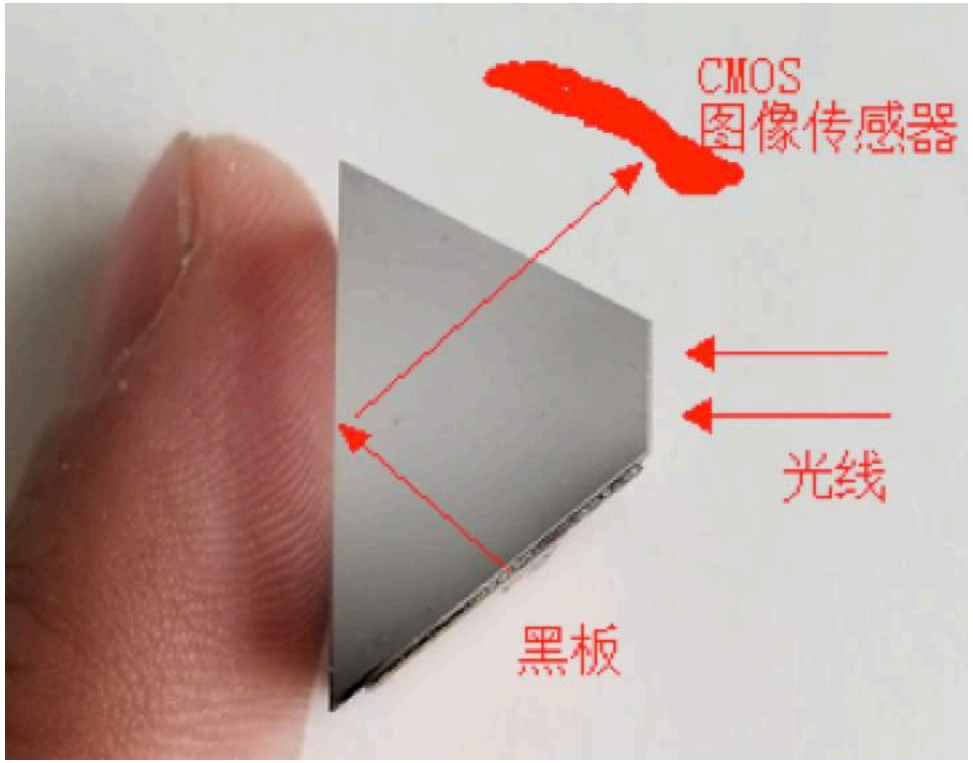


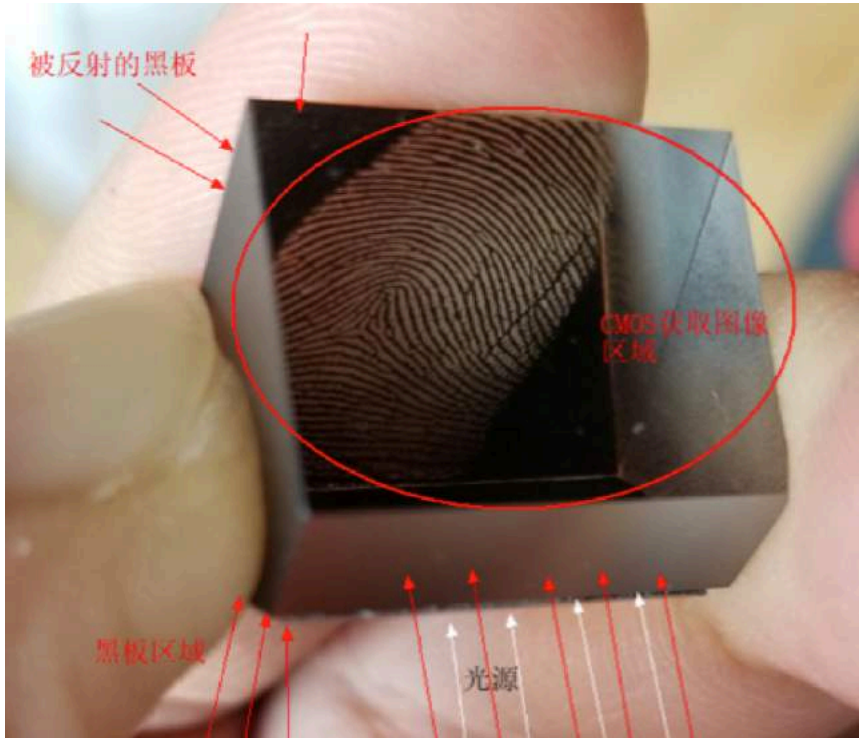




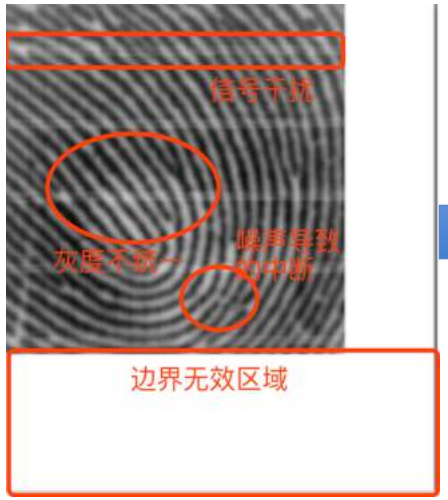
如何获取到图像的

- 光学折射原理
- 电荷感应

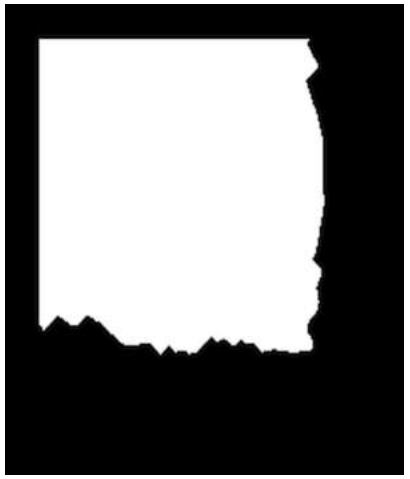




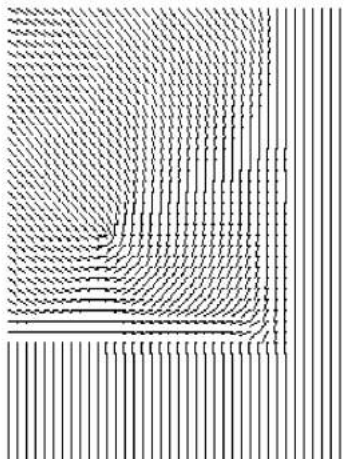
如何进行比对



捕获原始图像



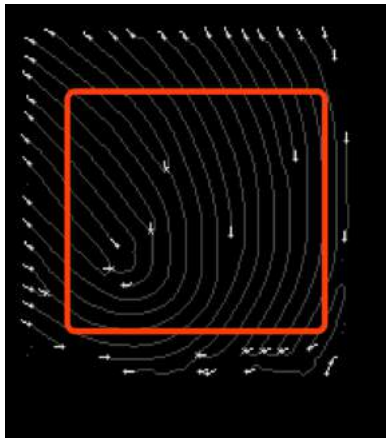
预处理



计算方向场

图像增强

二值化、细化



特征提取

注册存储特征/
验证比对特征

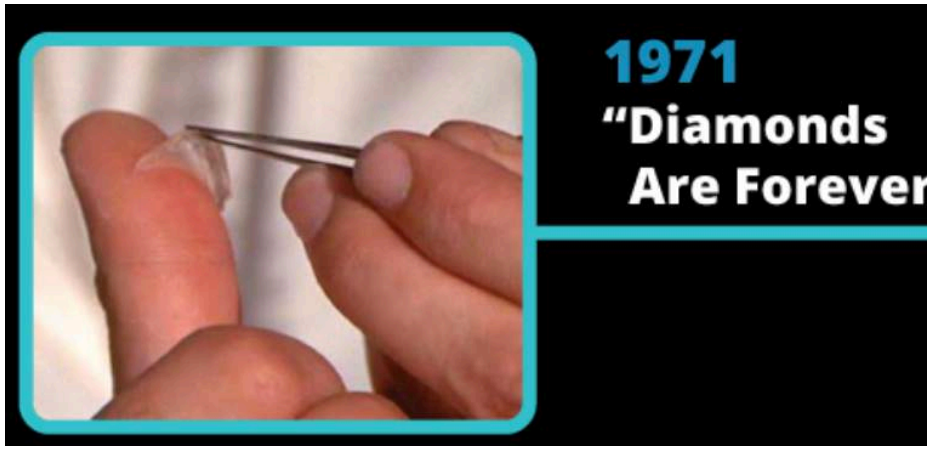
关键点

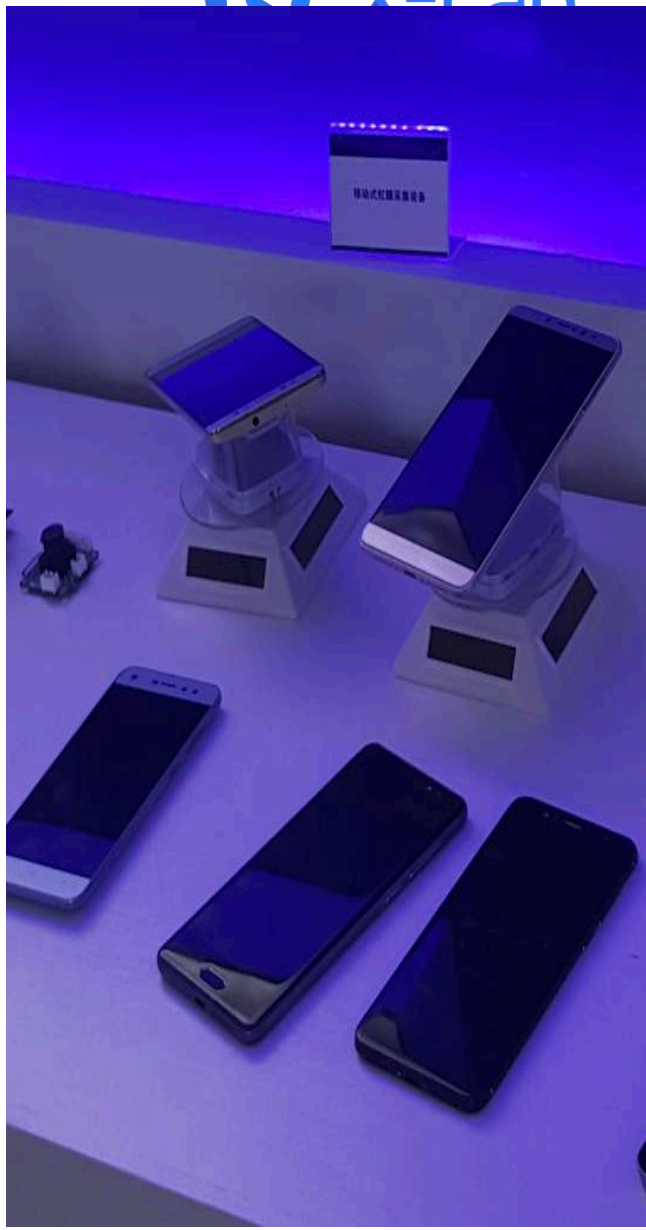
- 图像增强算法
  - Gabor滤波器
  - 符合人的视觉特征
  - 明暗/频率/方向变化，进行修复
  - 直观上感受：顺着指纹的纹理，把间断点修复、把粗细均匀、把干扰点去除
- 特征点选取、匹配
  - 交汇、末端、单独点
  - 去除边界
  - 删去过多特征点

- 结论：让传感器看到正确的特征点即可

想办法绕过

- 电影中的场景
- 现实中的利用
  - 局限性：只能自己复制自己的手指，没有攻击场景
  - 给我们了启发
- 比对指纹开发模块获取到的图像，不断测试





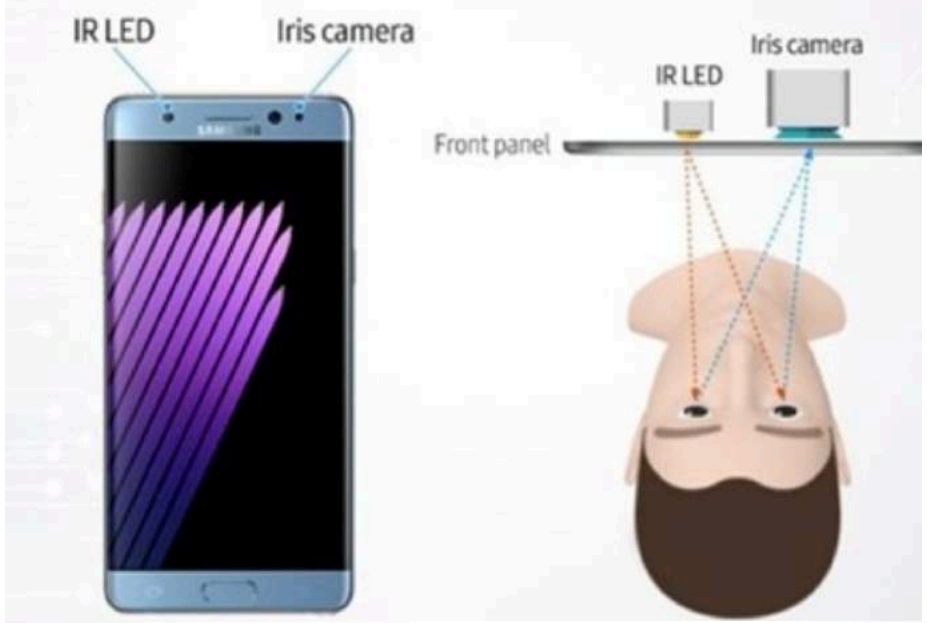

MATCH
Unlock

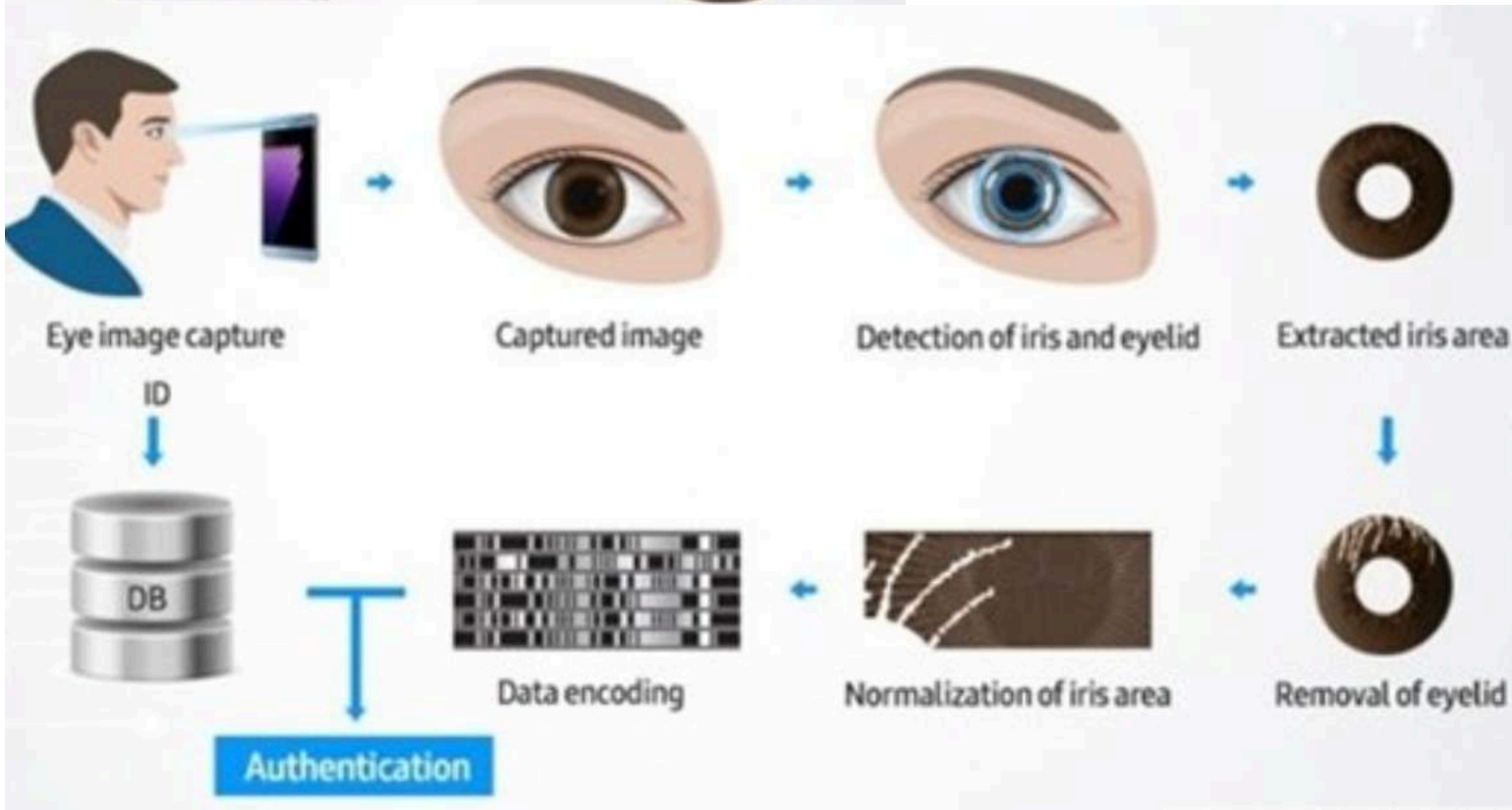
虹膜识别

- 关于人眼的虹膜：

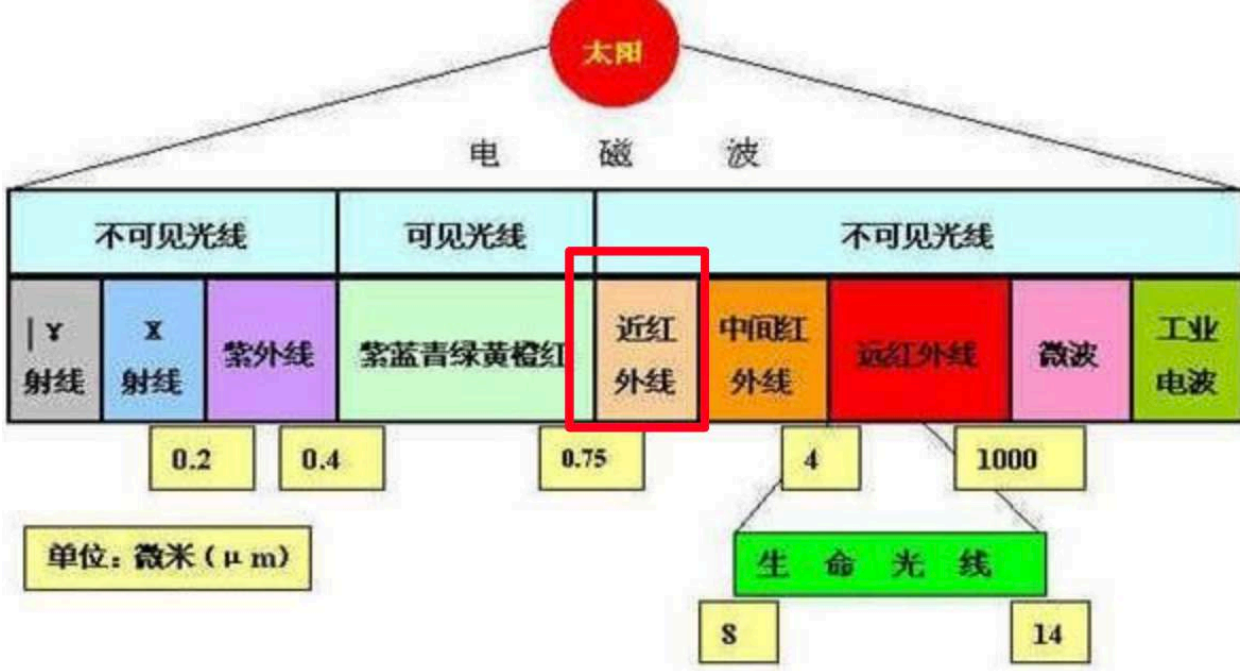
1、瞳孔
2、巩膜
3、瞳孔区域
4、神经花圈
5、睫状区域
6、放射状沟线
7、隐窝
8、色素点
9、向心沟

- 识别过程：
  - 红外光照射眼球
  - 红外摄像头捕捉虹膜图像
  - 利用算法进行定位
  - 其余和指纹类似
    - 归一化、图像增强（gabor滤波）、特征提取





关于红外线

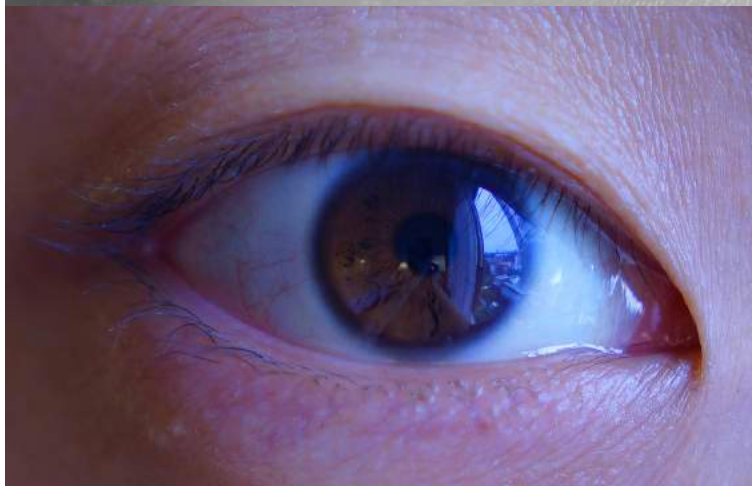


- 红色之外的光线 不可见
- 具有一定的穿透性
- 夜视仪、遥控器、监控
- 人体不同组织对红外吸收程度不一样，可以产生意想不到的效果
  - 虹膜识别
  - 静脉识别

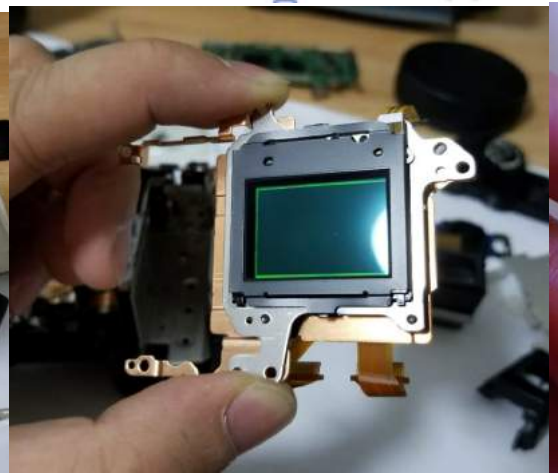
- 如何制造并捕捉红外呢?
  - 840nm红外LED
  - 改造相机

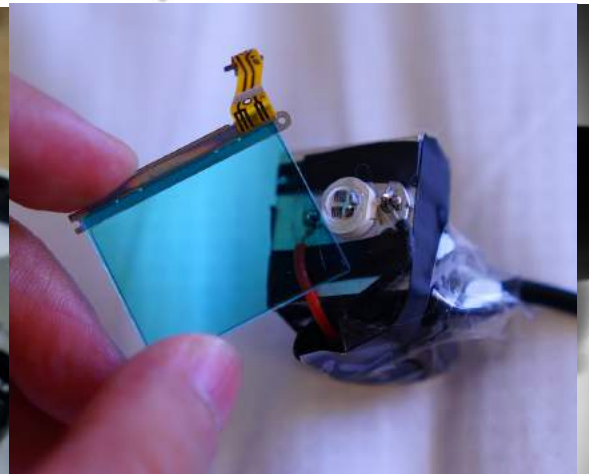
首先，需要一台红外相机

- CMOS/CCD本身具备捕获近红外的能力
  - 大多被封印了
  - 需要去除低通滤镜
  - 同时加上840nm红外截止镜
  - 实现了十米外取人的虹膜

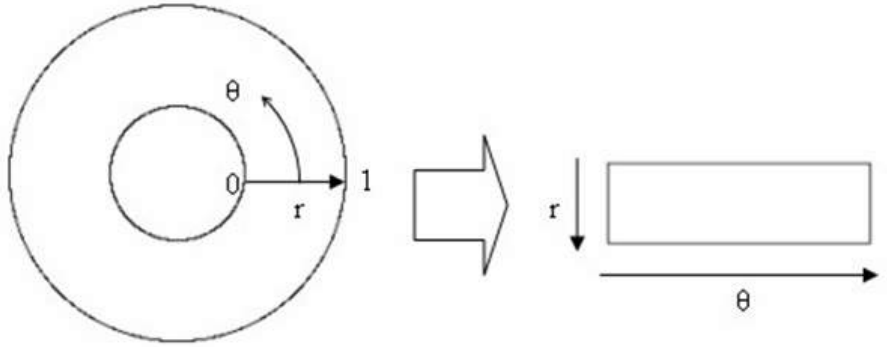


"You need a camera that can capture infrared light (used in the video), which is no longer available in the market. Also, you need to take a photo of the owner's iris and steal his smartphone. It is difficult for the whole scenario to happen in reality."

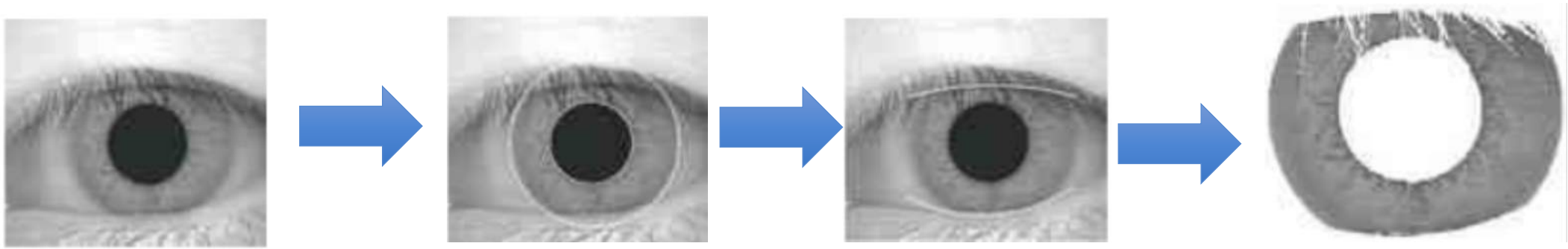




识别处理算法

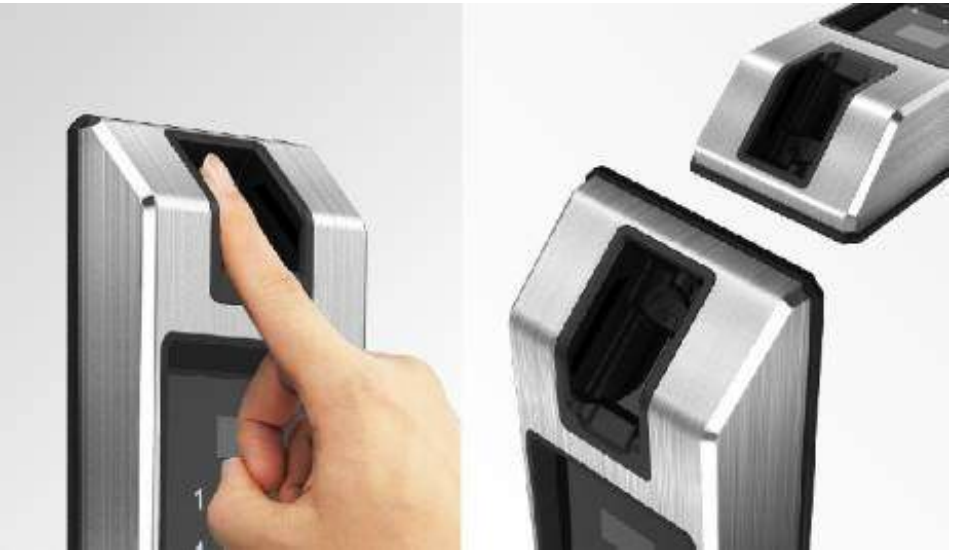


- Hough变换、二维gabor 滤波、汉明码对比



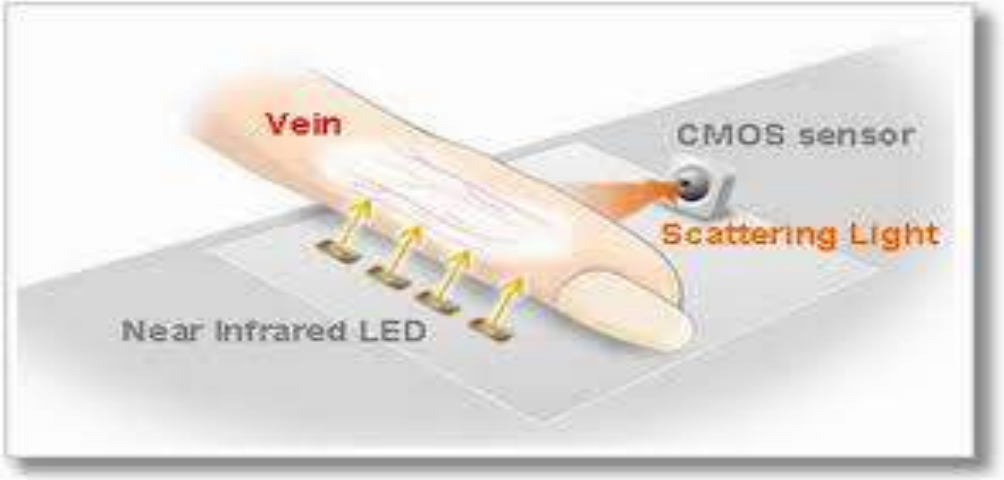
图像获取　定位　眼睑检测　睫毛检测

虹膜特征码提取　归一化




XTeller

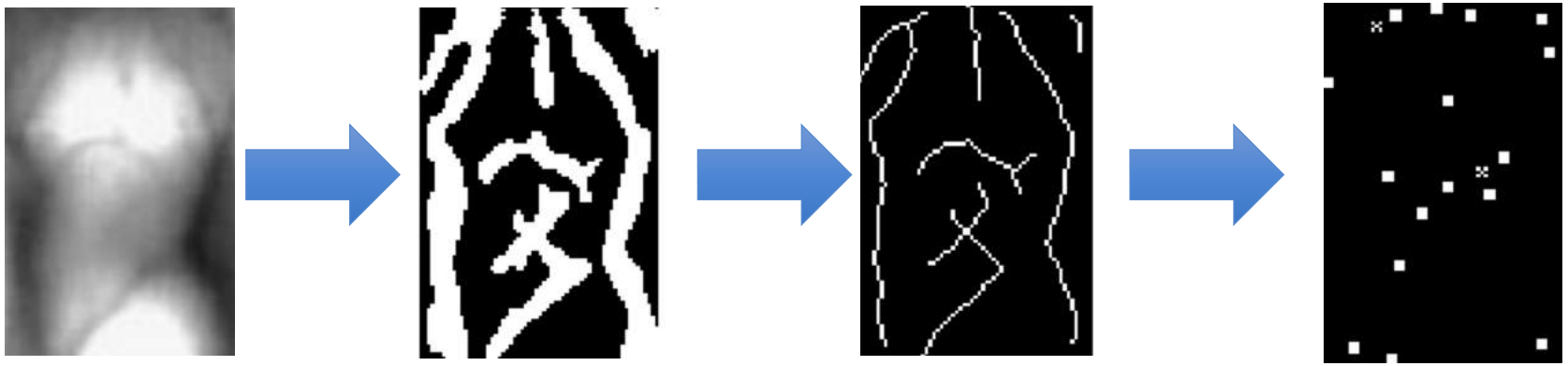
指静脉识别



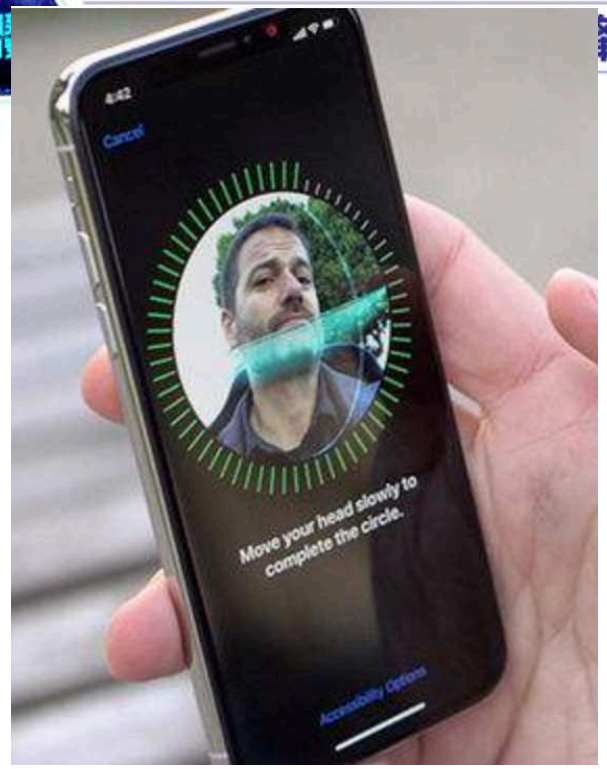
- 对手指照射近红外光
- 血管中血红蛋白对近红外光吸收，颜色加深
- 对静脉进行采集
- 滤波器对静脉脉络进行处理

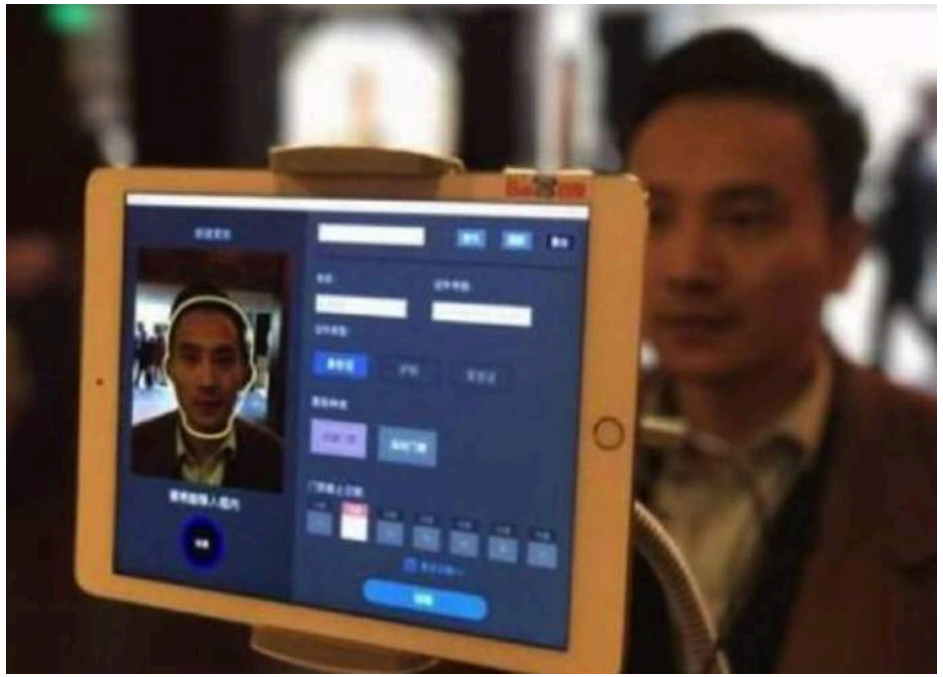
识别处理算法

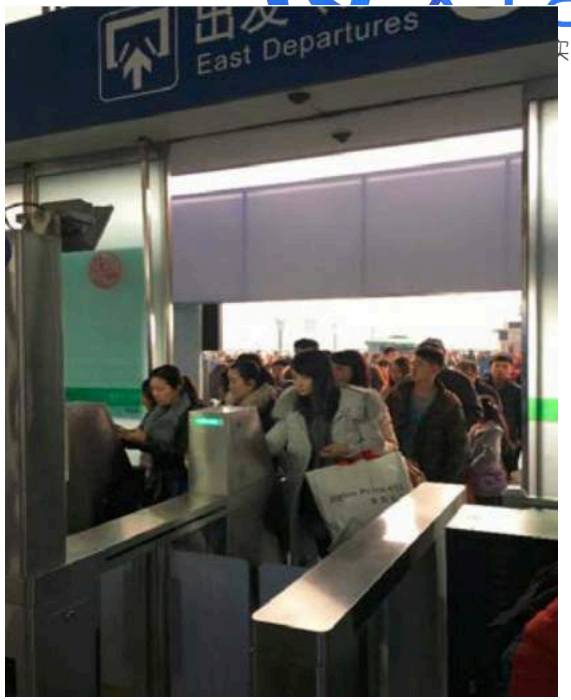
- 由于应用范围少，处理方式不统一
  - 图像增强：高斯滤波、gabor滤波、曲波变换等
  - 静脉分割：边缘检测、全局自适应阈值分割、方向谷形检测、分类器等



图像获取　图像增强/静脉分割　细化　特征提取


Cancel
Move your head slowly to complete the circle.
Accessibility Options

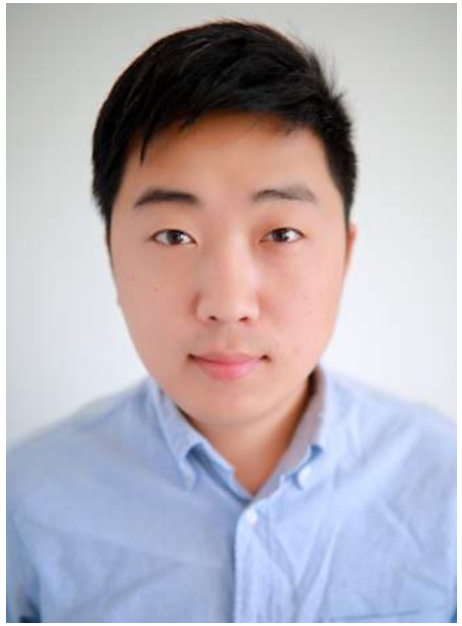


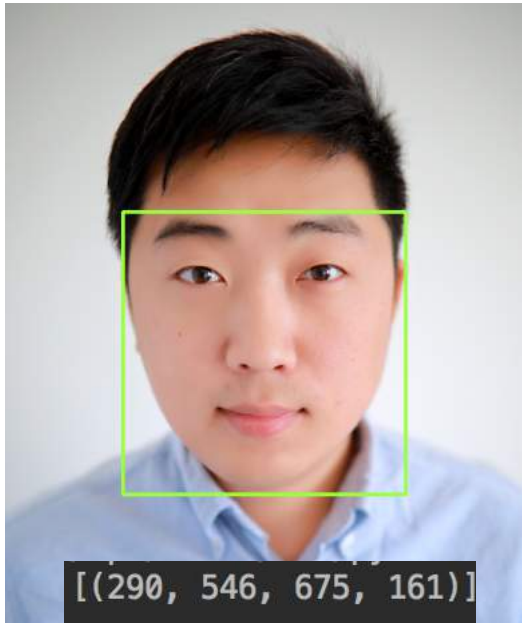

East Departures

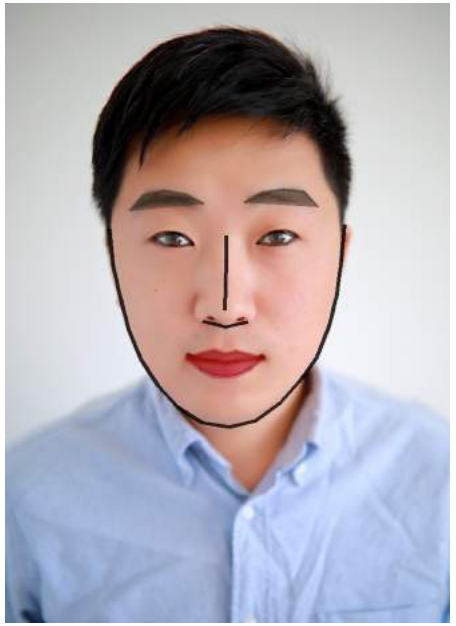

刷脸
开启即视为同意《人脸使用协议》
刷脸登录
脸部拍摄
眨眨眼
点头登录

人脸识别

- 单依靠摄像头实现（FaceID除外，单讲），传统算法&深度学习
- 运用了最多活体检测的生物识别（虽然准确率最低，1:1够用）
- 关键：人脸范围检测、特征点提取







```
nose_bridge
[(350, 371), (350, 410), (349, 449), (348, 488)]
left_eye
[(238, 376), (257, 367), (279, 369), (298, 385), (277, 388), (255, 386)]
nose_tip
[(313, 505), (331, 509), (350, 514), (367, 510), (385, 506)]
chin
[(167, 360), (172, 415), (184, 469), (197, 519), (216, 565), (243, 606),
right_eye
[(400, 383), (418, 367), (440, 365), (460, 372), (444, 384), (421, 386)]
bottom_lip
[(411, 563), (388, 581), (366, 591), (348, 593), (331, 591), (310, 582),
right_eyebrow
[(379, 319), (408, 303), (441, 298), (473, 302), (495, 326)]
left_eyebrow
[(199, 332), (221, 307), (254, 300), (286, 306), (315, 321)]
top_lip
[(288, 563), (312, 555), (332, 550), (350, 556), (366, 551), (387, 557),
```

总结

- 各种生物识别类似：
  - 传感器采集图像 --》 算法处理优化 --》 提取特征点 --》 比对
- 攻击方法也类似：
  - 用其他设备捕获到生物特征 --》 寻找可以让传感器看到类似特征的介质（纸、屏幕、光敏垫...） --》 优化特征，欺骗传感器
- 攻击能成功的原因：
  - 二维传感器信息少，容易获取、欺负
  - 活体检测太弱，甚至没有

- 都能远程打击
- 红外技术大量应用，可以重点关注

总结

- 风险：
  - 成本：都很低
  - 单一的生物识别容易被绕过，甚至设备直接提供了指纹等信息
  - 绕过是一方面，现有生物特征的易被泄露可能是更大的风险
    - 生物特征数量有限，且终生无法更改
    - 拿到特征最重要，活体可以慢慢绕，总会有方法

- 建议：
  - 厂商：增强模块的活体检测能力
  - 服务提供商：在敏感操作时，采用多因素认证，同时多使用基于风控的识别方法
  - 个人：手机保护好
  - ALL：是否需要重新认识生物特征识别在身份认证、访问控制中的功能?


THANK YOU!