基于AI+计算机视觉的生物识别技术及其在金融安全领域的应用与测评概述

主讲人：龚昊 （岚马克视觉科技技术总监）

上海岚马克视觉科技有限公司

Landmark (Shanghai) Vision Technology

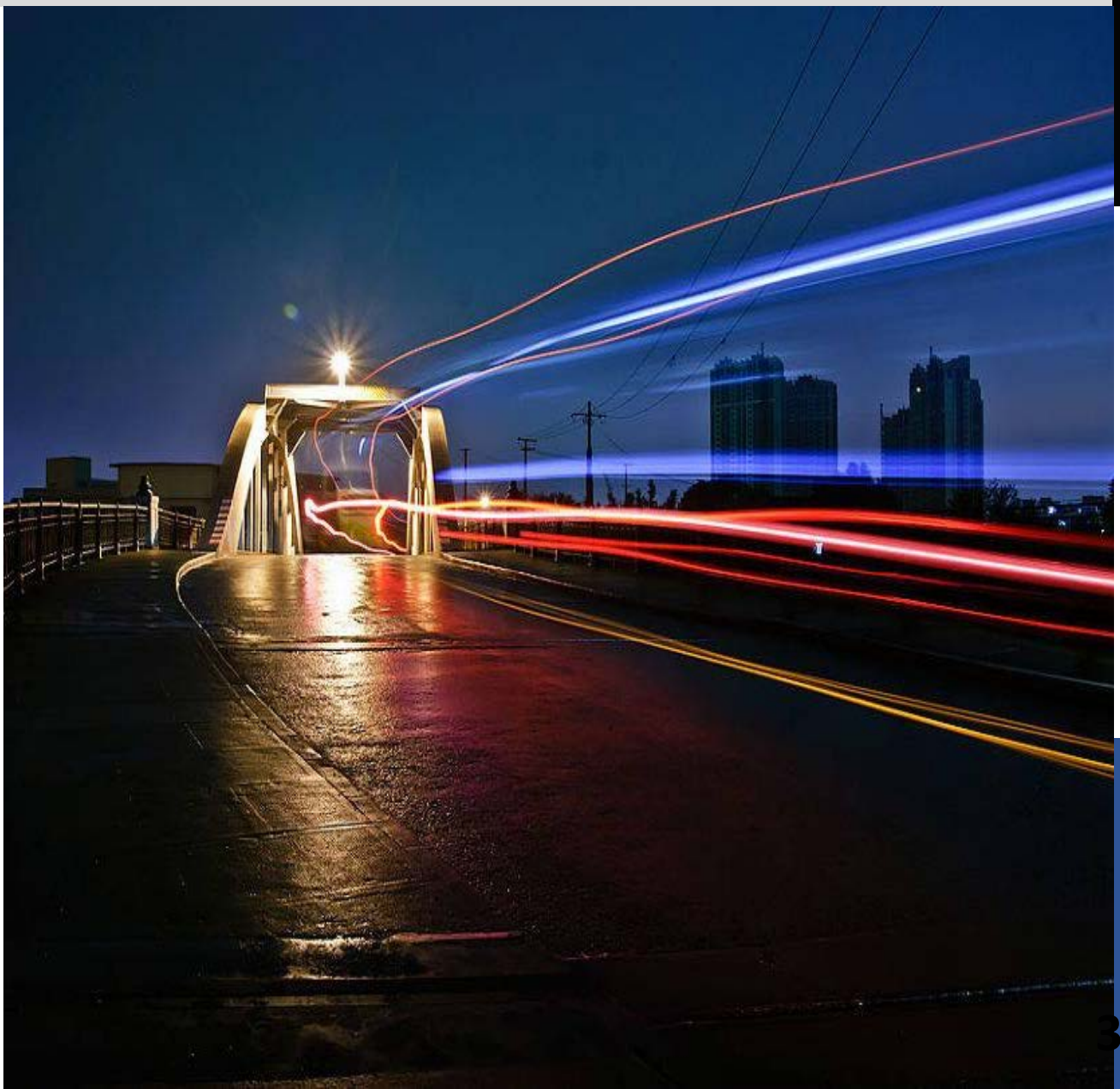
公司简介

上海岚马克视觉科技有限公司是一家专注于计算机视觉技术（Computer Vision, CV）和人工智能（Artificial Intelligence, AI）技术在安防监控、市政建设、餐饮管理等领域智能化升级应用的高科技创新企业。

总部位于上海徐汇，欧洲研发分部位于法国La Rochelle。

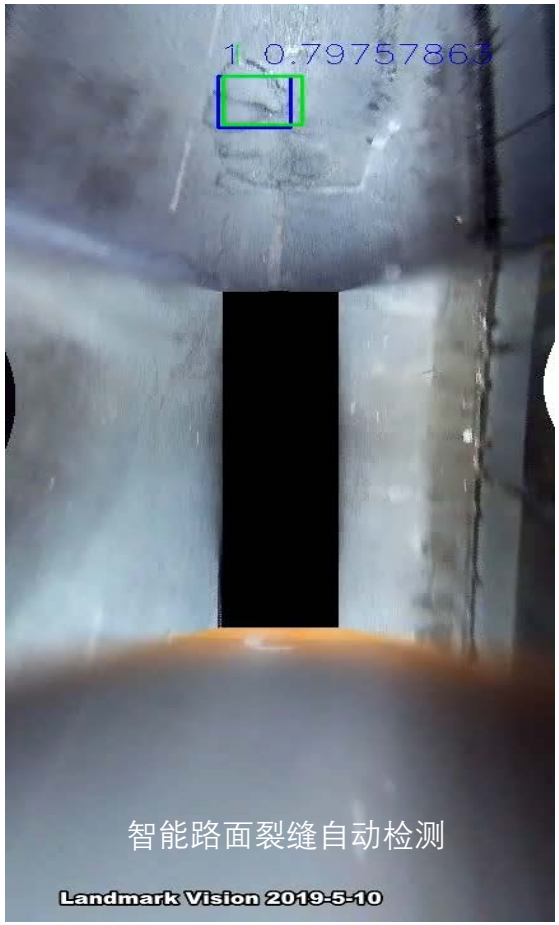
公司简介

市政行业
Municipal Industry



市政运营是城市保证正常运转的基础。**岚马克视觉科技**与上海隧道股份积极合作，利用AI+计算机视觉技术，为市政高效运营提速增效。

公司简介



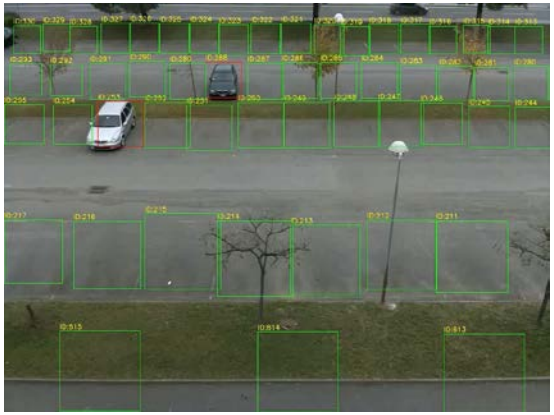
岚马克视觉科技自主开发了基于计算机视觉与深度学习技术的的路面病害自动识别系统。系统借助360°环视技术，可直接同时采样三根车道的路面状况，并通过人工智能技术实现对路面病害的自动检测、分类与识别。

公司简介

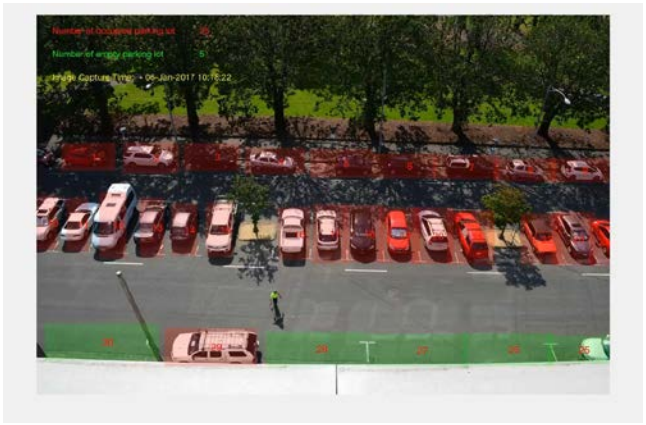

岚马克智慧路内停车解决方案
实现停车“无感出入、无感支付、无人值守”的颠覆式创新，
停车效率提升99%以上、运营成本降低90%以上，
更智能、更简单、更高效！

公司简介

红色：占用
绿色：空闲



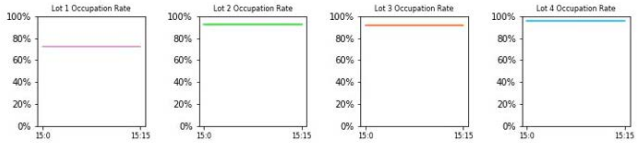
户外停车场（白天多云~傍晚）



户外停车场（白天有阴影）

图表曲线：
车位动态实时占用率（%）

路边停车位（白天有阴影）



路边停车位（白天多云）

餐饮行业
Catering

厨房是餐厅的心脏，直接关系到食物的质量和安全。后厨的数字化智能管理将赋能提升连锁餐饮的品控水准。

岚马克视觉科技与**满记甜品**，**香港米其林龙面馆**等餐饮巨头积极合作，利用AI+计算机视觉技术，为后厨精细化管理赋能。

公司简介

岚马克视觉科技利用餐厅后厨现有的视频系统，对视频数据进行分析。利用计算机视觉/深度学习技术，将工作人员佩戴厨师帽的情况进行实时捕捉。帮助连锁餐饮经营者实现对后厨的精细化管理。

大纲 Outline

客户身份识别和验证是金融服务生态系统的基础，当越来越多的金融服务通过网络来提供时，远程身份识别变得尤其重要，**生物识别技术**在其中扮演着越来越重要的角色。本课程针对目前主流的生物识别技术，包括**人脸、指纹、虹膜、静脉**等识别，

1）科普相关生物识别技术及其背后的基本原理；

2）重点介绍国内外**人脸识别技术**在金融安全领域的应用情况、技术现状以及对应的测试方法；

3）通过分析技术上的难点和困境，对金融级生物识别的发展趋势和应用场景加以探讨。

生物识别技术 Biometrics

生物识别技术 (biometric identification technology) 是指利用人体生物特征进行身份认证的一种技术, 它通过计算机与光学、声学、生物传感器和生物统计学原理等科技手段密切结合, 利用人体固有的生理特性 (如指纹、脸象、虹膜等) 和行为特征 (如笔迹、声音、步态等) 来进行个人身份的鉴定。目前已经发展了指纹识别、人脸识别、虹膜识别、静脉识别等多种主流生物识别技术 (见下表) 。金融领域已广泛应用于银行和证券的远程开户、在线转账、ATM取款、移动支付及保险理赔等。

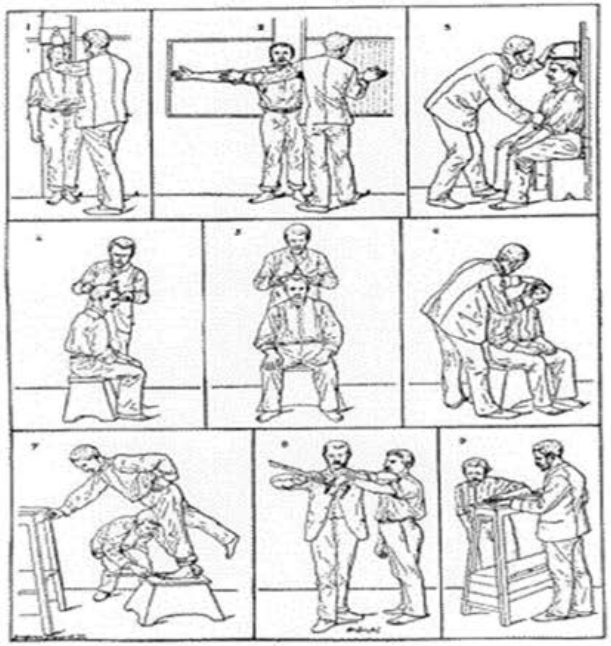
生物识别技术 Biometrics

金融行业的主流生物识别技术及其应用场景

技术类别	人脸识别	指纹识别	虹膜识别	指静脉识别
稳定性	中	高	极高	高
可采集性	高	高	高	高
准确性	中	高	极高	高
是否接触	否	是	是	是
便利性	极高	高	中	高
金融主要应用场景	自助终端、远程身份核查（直销银行、远程业务办理等）、柜面身份核查、移动营销	内部授权、系统登录、移动支付、指纹人证合一	门禁管理、押运管理等高安全要求级别的场景	自助终端集成
发展现状	目前应用最火，创新性十足，但也一直受到各方的质疑	应用最早、最成熟，接受程度较高	处于探索、观察阶段	处于探索阶段
发展契机	相关技术尤其是深度学习的发展与成熟，人脸识别的准确率大大提升，且不一定需要额外的硬件设备	研发较早，且手机等移动终端普遍搭载了指纹模块，新一代身份证也内含指纹信息	相关技术的发展使其硬件设备体积大大减小，且以三星为代表的厂商一直致力于将其加入手机等移动设备中	技术的发展与普及，以及用户的接受性提升

First Biometric System (1882)

Identify repeat offenders

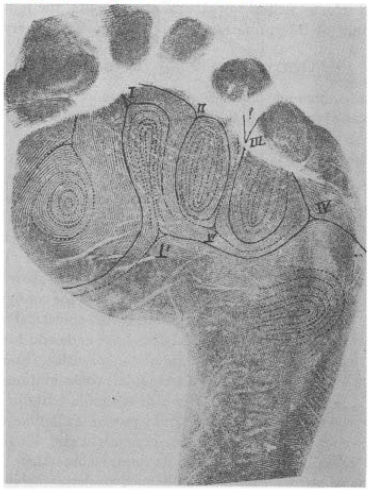


H.T. F. Rhodes, Alphonse Bertillon: Father of Scientific Detection, Harrap, 1956

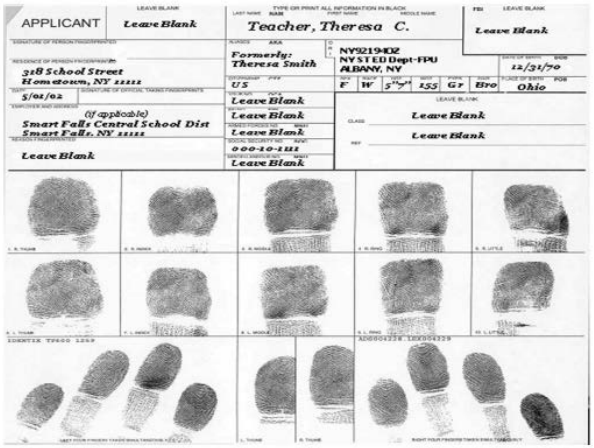
Friction Ridge Patterns

First Automatic Fingerprint identification system (AFIS): ~1980

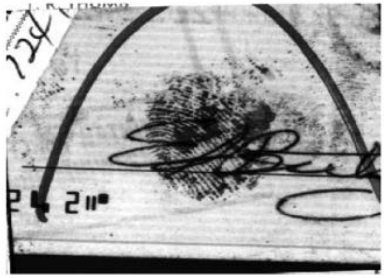
掌纹识别



Cummins and Midlo, Finger Prints, Palms and Soles, Dover, 1961



指纹识别

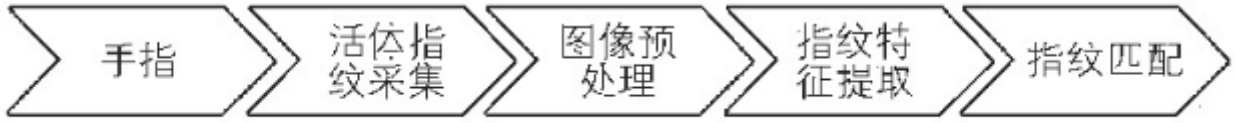


- 现代指纹识别技术的金融领域的应用

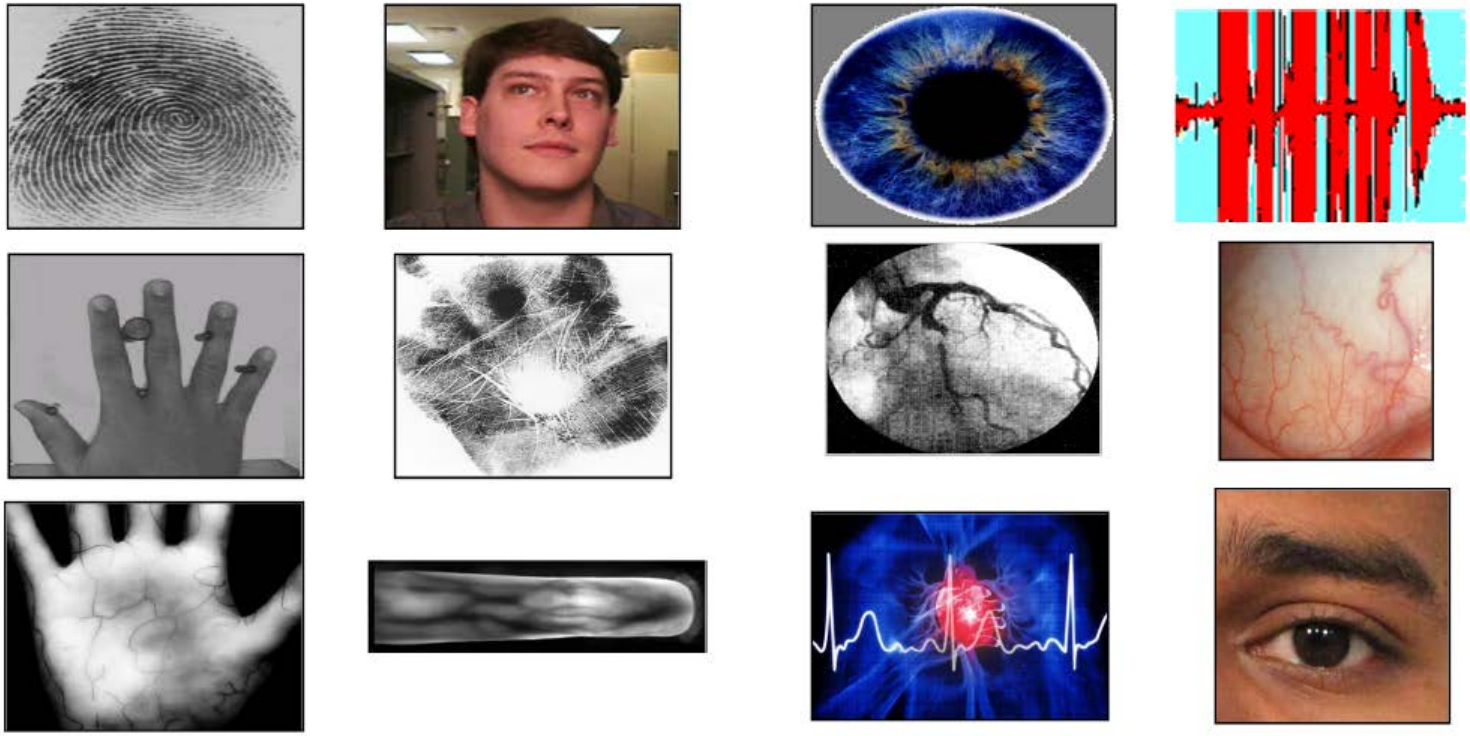
指纹识别技术发展较早, 信息采集方便, 应用范围较为广泛。

- 该技术较早在金融领域应用, 在银行APP登录和支付时也越来越普遍。如国内各大手机银行APP在登录时都是使用指纹, 方便快捷;
- 在公共事业缴费、飞机票购买、在线购物等特定场景, 使用指纹支付, 代替短信验证码使用, 体验更好。
- 其主要流程是通过活体指纹采集、图像预处理、指纹特征提取和指纹匹配等完成受理 (见下图) 。同时, 指纹识别应用于银行核心业务系统、电子签章系统的授权管理, 能够进行责任追溯, 避免通过身份卡或授权码出现滥授权、乱授权等现象。

图3 指纹识别流程图



Beyond Fingerprinting



指静脉识别

指静脉识别技术，顾名思义就是根据手指内的静脉进行识别。而这种技术对人体无害，具有不易被盗取、伪造等特点。与指纹识别技术相比，指静脉隐藏在手指的内部，被复制或盗用的机会几乎没有，受生理和环境因素的影响小，更是克服了指纹识别会遇到的皮肤干燥，油污，灰尘，皮肤表面异常等因素影响。

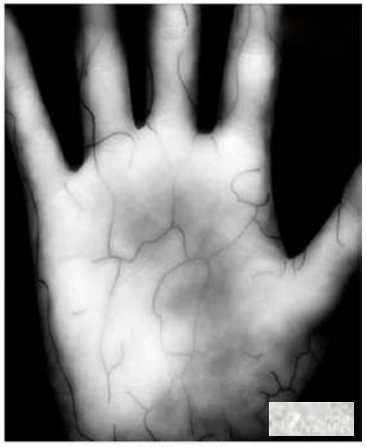
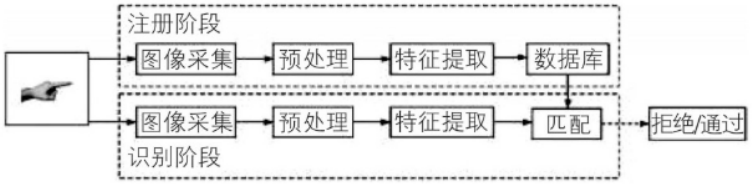
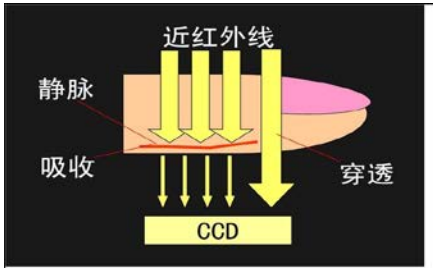
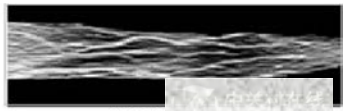

指静脉识别图像

图6 指静脉识别流程图



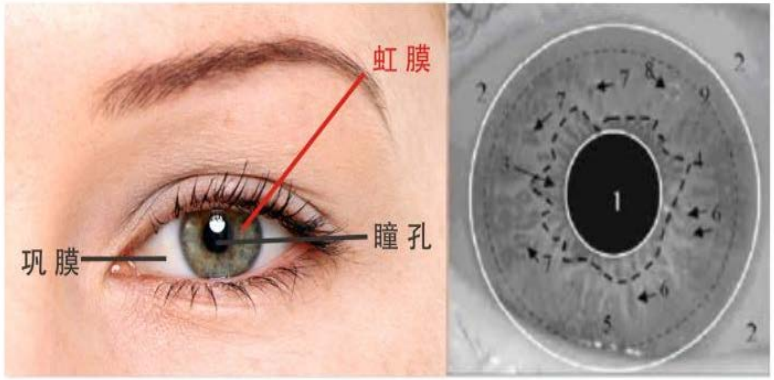



穿透图像


比对后图像

虹膜识别

虹膜识别：通过特定波长的红外线扫描人眼上的虹膜获取图像信息，而每个人的虹膜都是不一样的，所以可以作为生物识别的一种。因为虹膜无法复制，所以从安全性上来说比指纹识别要高很多。



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

虹膜识别检测区域

虹膜识别考勤 对识别姿势和角度有较高的要求

2D人脸识别

人脸识别（Face Recognition）是一种依据人的面部特征（如统计或几何特征等），自动进行身份识别的一种生物识别技术，又称为面像识别、人像识别、相貌识别、面孔识别、面部识别等。通常我们所说的人脸识别是基于光学人脸图像（2D）的身份识别与验证的简称。

生物识别技术在金融业务的具体应用

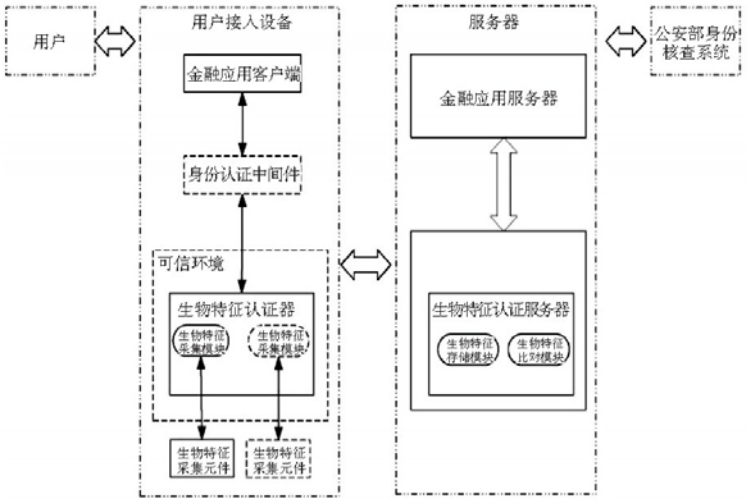
开户。商业银行依靠生物识别技术为客户远程开户，对身份进行识别和鉴定，免去了客户去网点的奔波。

转账。大额转账要去银行柜台办理，采用生物识别技术可方便实现远程自助转账。

取款。如今，很多银行已经实现了“无卡取款”功能，这种无卡取款的模式就是基于生物识别技术。

支付结算。在新零售理念的引领下，无人值守，“刷脸付款”已在国内许多大型超市连锁店陆续推出，

保险理赔。基于生物识别技术的保险理赔通过互联网保险平台采用电子材料上传的方式，机器深度学习在线核保，大大改善了客户理赔体验。



普通的指纹识别，2D人脸识别真的靠谱吗?

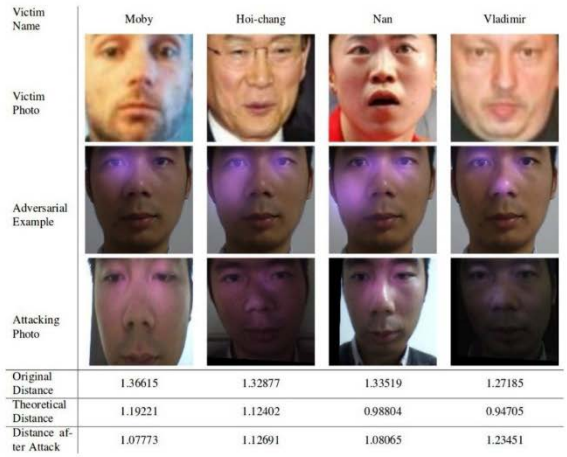
愚弄对抗AI生物识别的手段

指纹硅胶套

隔壁老王3D打印面具

愚弄对抗AI生物识别的手段

看不见的红外光能愚弄脸部识别软件



Victim Name	Moby	Hoi-chang	Nan	Vladimir
Victim Photo				
Adversarial Example				
Attacking Photo				
Original Distance	1.36615	1.32877	1.33519	1.27185
Theoretical Distance	1.19221	1.12402	0.98804	0.94705
Distance after Attack	1.07773	1.12691	1.08065	1.23451

复旦大学和阿里巴巴的研究人员在预印本网站 arxiv 发表论文（PDF），描述了一种能愚弄脸部识别软件的“攻击方法”，他们利用安装在帽檐的红外 LED 灯照亮脸部，投影 CCTV 摄像头能看见但人眼看不见的形状去愚弄识别软件。使用这种方法研究人员欺骗脸部识别软件将任意人的脸识别为音乐家 Moby，韩国政客李会昌等（如图所示）。根据论文摘要，这项研究是为了揭示红外对抗对面部识别构成的严重威胁。研究人员称，利用这种方法，攻击者不仅能躲避监控探头，如果能获得受害者的照片攻击者还能冒充受害者通过脸部识别认证。研究人员称，今天的脸部识别技术远称不上安全和可靠。中国有着最庞大的监控探头集群，并正在广泛应用脸部识别。

比利时天主教鲁汶大学的学生展示了 AI 时代的「隐身术」，只要将一张利用对抗网络生成的图像放在身上，AI 系统就无法检测出这是一个人。论文 arxiv.org/pdf/1904.08653…

Translate Tweet

基于AI+计算机视觉的人脸技术简介

人脸检测跟踪

对任意常见场景，可以在嵌入式设备、移动设备和个人电脑上实现毫秒级的人脸检测。该技术可适应侧脸、遮挡、模糊、暗光、逆光、表情变化、平面内 360° 旋转等各种实际环境，支持彩色、灰度、近红外等各种图像视频类型。

人脸关键点定位

毫秒级别眼、口、鼻轮廓等人脸 21、106、240 个关键点定位，支持不同精度的人脸关键点定位，该技术可适应大角度侧脸、大表情变化、遮挡、模糊、明暗变化等各种实际环境。

人脸身份验证

判断两张照片是否为同一人，在百万分之一的误识别下，准确率超过99%。

人脸属性

准确识别 10 多种人脸属性类别，例如性别、年龄、种族、表情、胡须、面部动作状态等。可以用于广告定向投放或顾客信息分析，让你秒懂客户心。

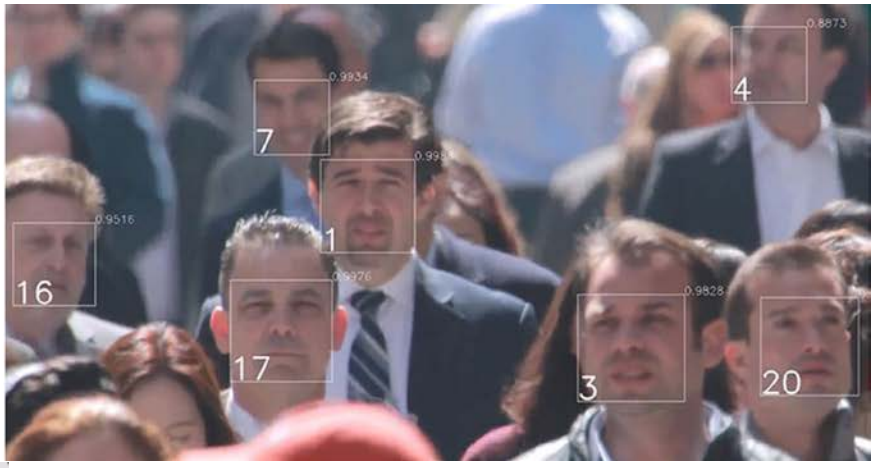
真人检测

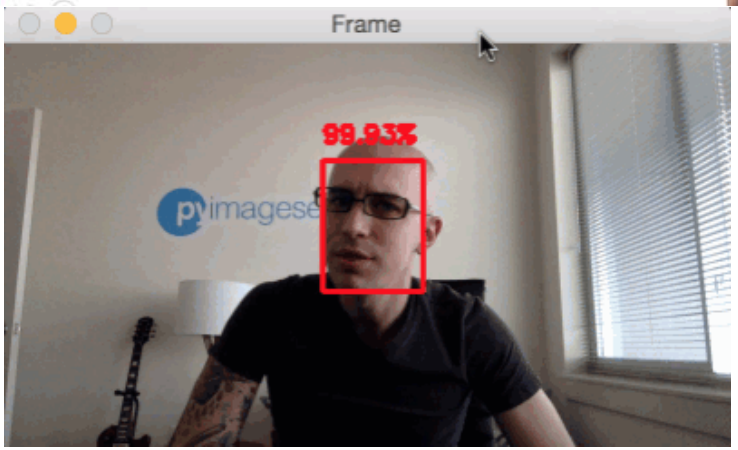
检测摄像头前用户是否为真人操作，配合人脸身份认证，为金融等高安全性要求的严肃应用场景提供真人身份验证。能有效分辨高清照片、PS 、三维模型、换脸等仿冒欺诈。我们针对不同场景需求提供定制化的解决方案。

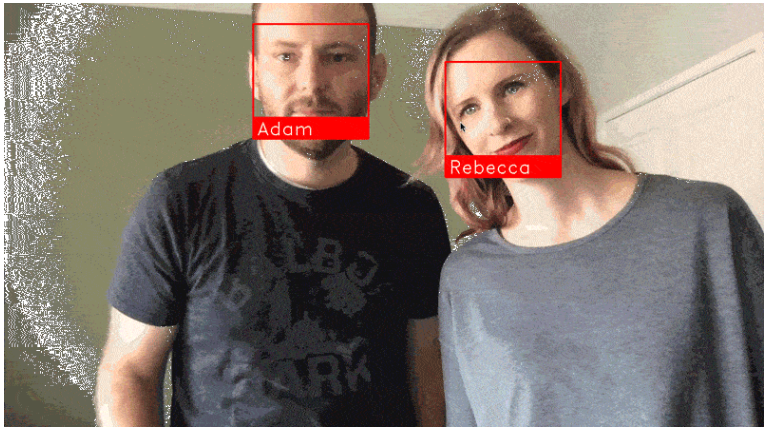
基于AI+计算机视觉的人脸技术简介

人脸检测跟踪识别

对任意常见场景，可以在嵌入式设备、移动设备和个人电脑上实现毫秒级的人脸检测。该技术可适应侧脸、遮挡、模糊、暗光、逆光、表情变化、平面内 360° 旋转等各种实际环境，支持彩色、灰度、近红外等各种图像视频类型。



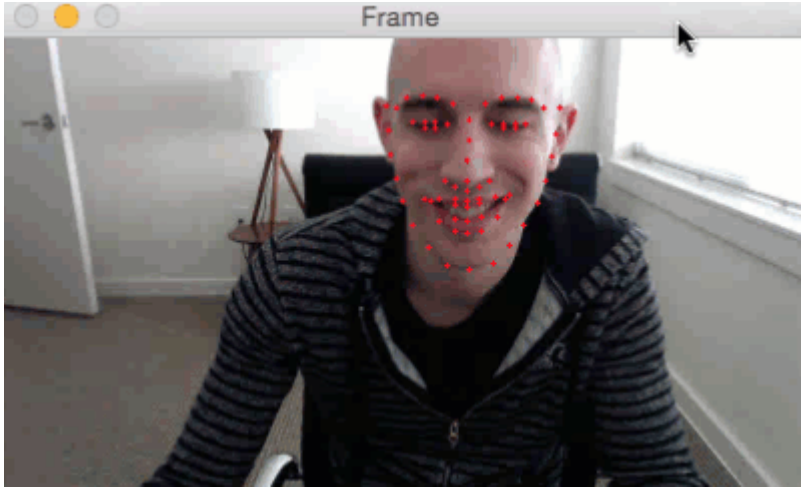




基于AI+计算机视觉的人脸技术简介

人脸关键点定位

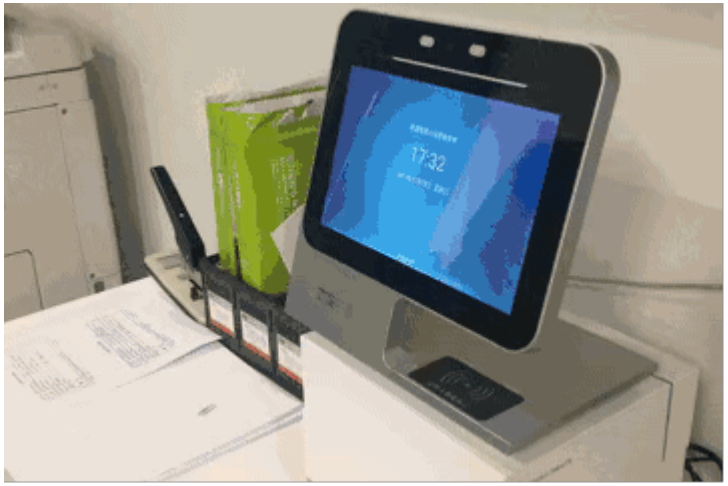
毫秒级别眼、口、鼻轮廓等人脸 21、106、240 个关键点定位，支持不同精度的人脸关键点定位，该技术可适应大角度侧脸、大表情变化、遮挡、模糊、明暗变化等各种实际环境。



基于AI+计算机视觉的人脸技术简介

人脸身份验证

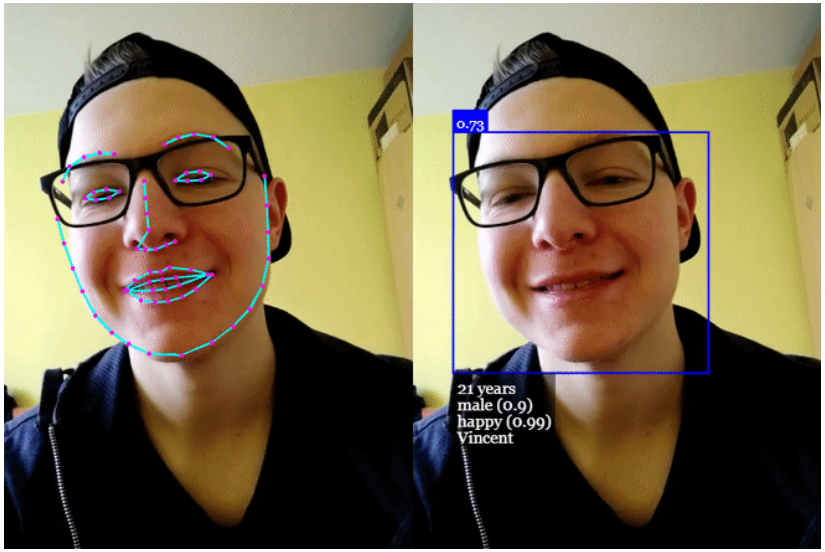
判断两张照片是否为同一人，在百万分之一的误识别下，准确率超过99%。



基于AI+计算机视觉的人脸技术简介

人脸属性

准确识别 10 多种人脸属性类别，例如性别、年龄、种族、表情、胡须、面部动作状态等。可以用于广告定向投放或顾客信息分析，让你秒懂客户心。



基于AI+计算机视觉的人脸技术简介

真人检测

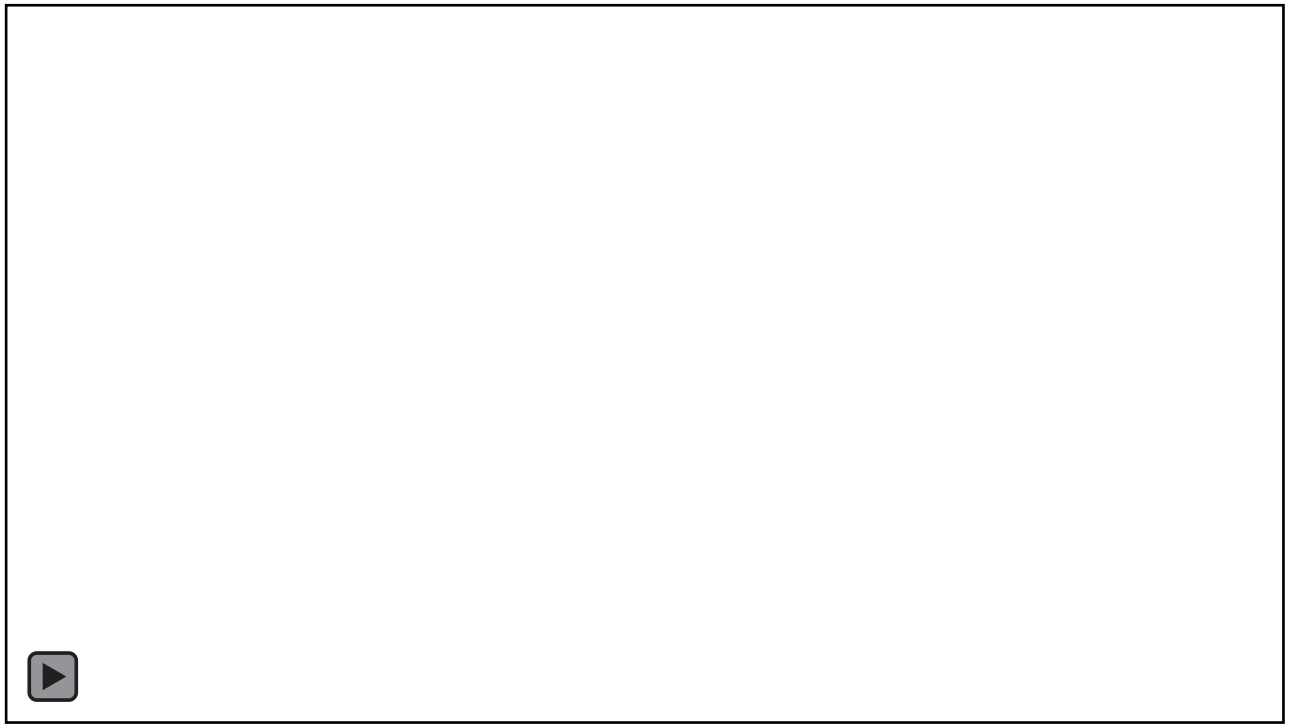
检测摄像头前用户是否为真人操作，配合人脸身份认证，为金融等高安全性要求的严肃应用场景提供真人身份验证。能有效分辨高清照片、PS 、三维模型、换脸等仿冒欺诈。我们针对不同场景需求提供定制化的解决方案。

智能换脸
Faceswap

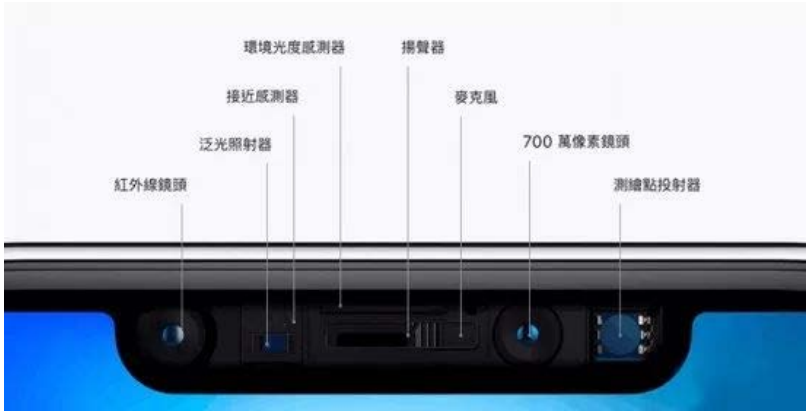
- 3D人脸识别
  - 以iPhone X为代表

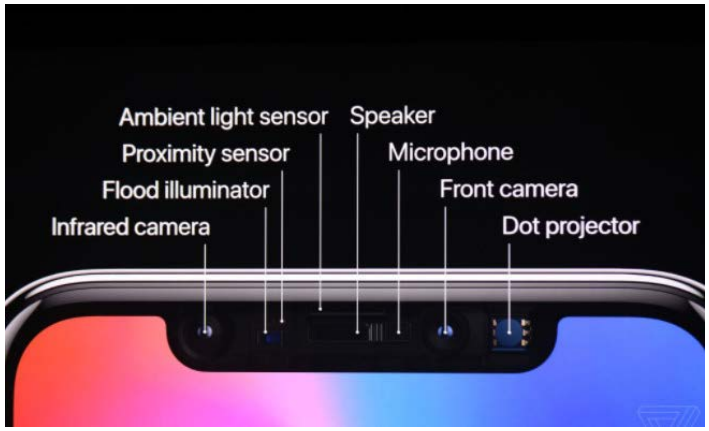
- 2D人脸识别+活体检测
  - 国内某知名人脸识别公司
  - 岚马克视觉科技

3D人脸识别方案--iPhone X



3D人脸识别方案--iPhone X





FaceID 识错率（FAR）号称仅为百万分之一，比起指纹解锁万分之一的错误率，准确率一下提升了20倍。但国外媒体的测试中已经有了同卵双胞胎成功骗过Face ID的案例。

国内某知名人脸识别公司--2D人脸识别金融级整体解决方案

FaceID 金融级整体解决方案

SDK(原生APP)

移动端H5
微信/小程序
第三方渠道APP

PC端网页验证

身份证质量检测

动作活体　炫彩活体

全流程接入体验

双角度活体　视频活体

实时视频会话

动作活体

身份证

OCR识别　“五分类”攻击检测

人脸比对

人脸比对引擎　活体图片校验

屏幕翻拍检测　假脸/合成脸检测

面具检测　换脸检测

数据源

多渠道接入权威数据源

黑白照片　空白照片　无效照片

线上运营

异常数据运营平台

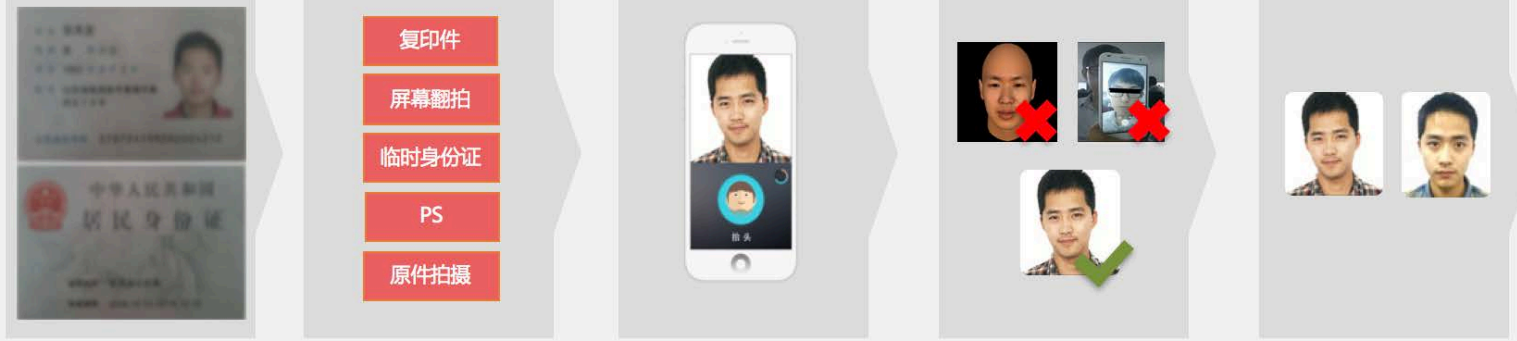
人工标注团队

大数据平台

https://www.faceid.com

SDK　云端

身份验证流程



国内某知名人脸识别公司-- 2D人脸识别金融级整体解决方案

身份证照片采集

通过手机摄像头采集

判断是否有身份证

身份证是否有光斑和阴影

身份证大小是否合适

身份证角度是否合适

- 手机端SDK不直接做OCR的原因？

身份证OCR和分类检测

姓名+身份证号全对的准确率高达99.28%

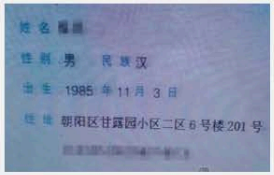
支持全部少数民族身份证识别

身份证原件拍摄

临时身份证

屏幕翻拍

复印件



粗糙PS

身份证识别

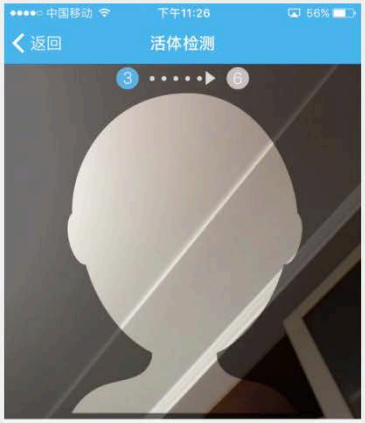
身份证五分类判断

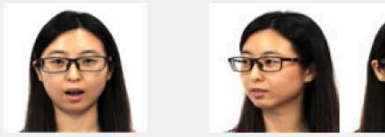
国内某知名人脸识别公司-- 2D人脸识别金融级整体解决方案

动作活体检测

脸部关键点检测和追踪

脸部3D姿态检测和追踪





张嘴

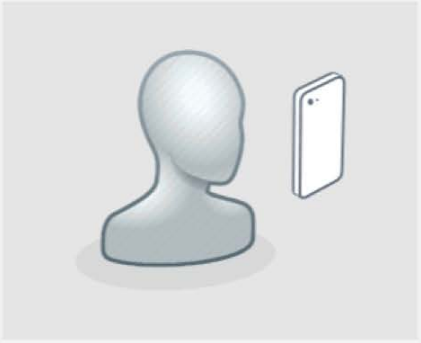
左右摇头

上下摇头

眨眼

国内某知名人脸识别公司-- 2D人脸识别金融级整体解决方案

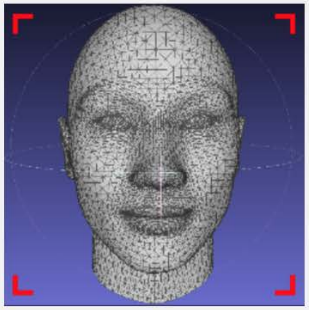
炫彩活体检测



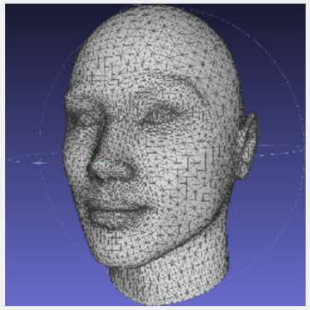
真人检测

屏幕翻拍检测

移动端H5-双角度活体



正面自拍照

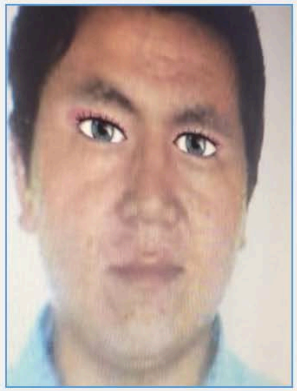


侧面自拍照（20°~30°）

人脸攻击检测

换脸攻击

屏幕翻拍



假脸、面具攻击

人脸识别：技术

Detect → **Alignment** → **Crop** → **DNN** → **Representation**

- 同一个人，表示的距离尽量小；不同的人，表示的距离尽量大

Representation

- **1:1** 检测两张人脸是否是同一个人：Dist(Rep(A),Rep(B)) < 阈值
  不同误识率下，不同的阈值。
- **1:N** 给定一个人脸照片，在数据库中查找与之相似的人脸

人脸比对

误识率	阈值
千分之一	60
万分之一	70
十万分之一	80

本次置信度为75，则：
- 在万分之一的误识率下，是同一个人
- 在十万分之一的误识率下，不是同一个人

提供一体化的综合业务接口

数据源照片筛选

国内某知名人脸识别公司-- 2D人脸识别金融级整体解决方案

人脸验证方案的“攻防战”

- “端+云”联合防范

传统人脸验证方案介绍

- 一套传统经典的2D人脸比对验证系统接入互联网运行后，时刻处于被图像视频“假”人脸愚弄攻击的危险中。

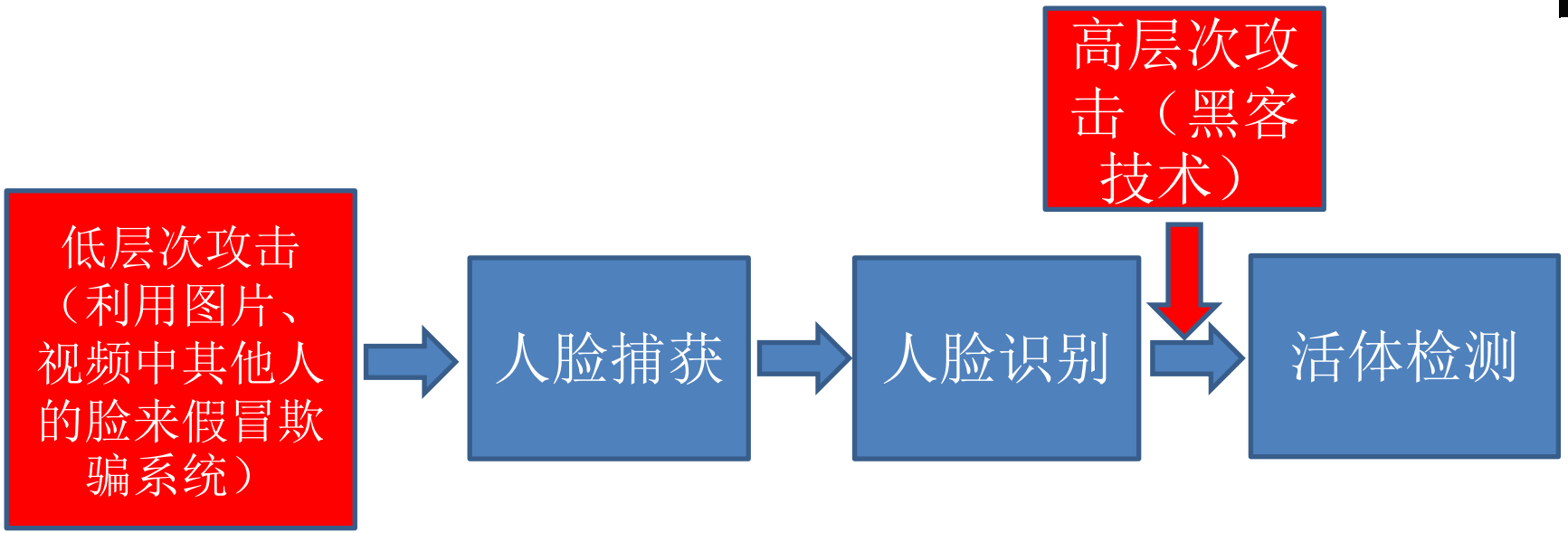


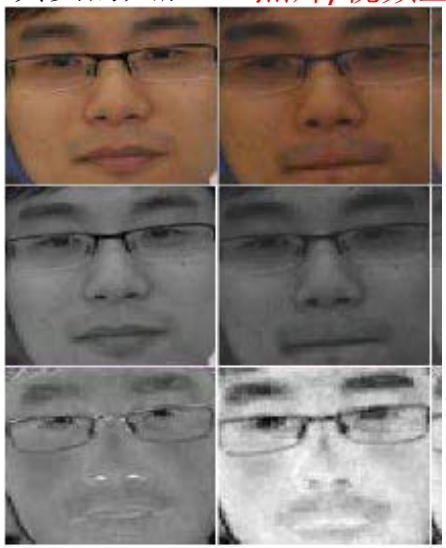
图2：传统人脸验证流程中的潜在风险：人脸识别和活体检测在不同阶段分开独立使用，这样会使得系统在不同阶段更容易地遭受欺诈攻击。

“活体检测”的方法策略

- 1) 头部运动检测; 2) 反光的纹理; 3) 人机交互; 4) 3D感知方法.

1) 头部运动检测

真实的人脸　照片/视频上的人脸

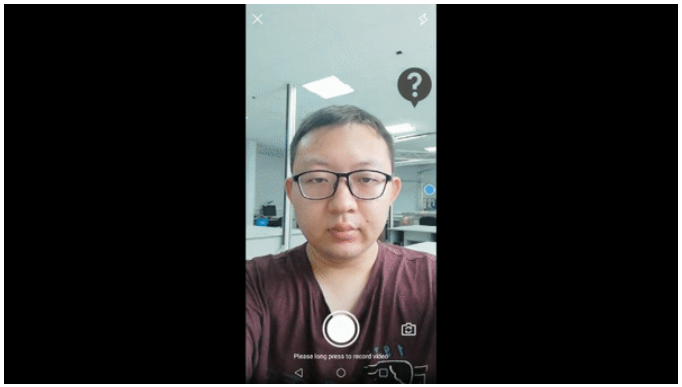


RGB彩色图像

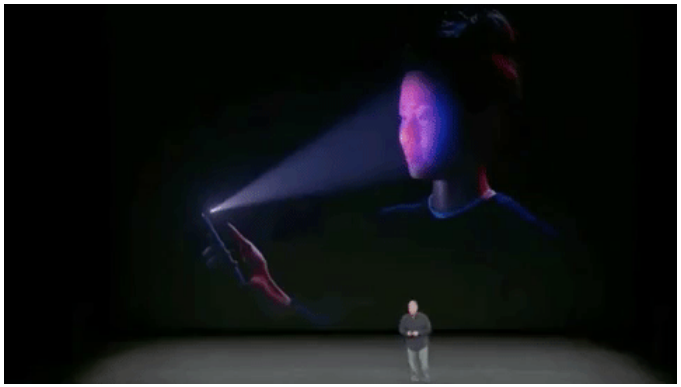
灰度图像

HSV色彩空间分解图像

2) 真实人脸图像的纹理和翻拍（照片/视频）人脸的纹理



3) 根据系统提示要求做出相应的表情



4) iPhoneX基于3D结构光的方案

人脸验证系统的测试评估

- 对于**人脸比对功能**性能的评估指标：准确率 Accuracy，召回率 Recall，误识率FAR (False Accept Rate)

$$\text{Acc} = \frac{TP+TN}{P+N}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{FAR} = \frac{FP}{FP+TN}$$

- TP – 预测结果中，真阳性的样本对的个数
- TN – 预测结果中，真阴性的样本对的个数
- FP – 预测结果中，假阳性的样本对的个数
- FN – 预测结果中，假阴性的样本对的个数
- P – 在测试数据集中所有的正样本对$(= TP + FN)$的个数, 也就是同一个人的所有不同的人脸照片
- N – 在测试数据集中所有的负样本对$(= FP + TN)$的个数, 也就是所有照片都对应不同的人

人脸验证系统的测试评估

- 对于**活体检测功能中表情识别**性能的评估指标：准确率 Accuracy

$$\text{Acc} = \frac{TP+TN}{P+N}$$

- TP – 预测结果中，真阳性的样本对的个数
- TN – 预测结果中，真阴性的样本对的个数
- P – 在测试数据集中所有的正样本对$(= TP + FN)$的个数, 也就是同一个人的所有不同的人脸照片
- N – 在测试数据集中所有的负样本对$(= FP + TN)$的个数, 也就是所有照片都对应不同的人

.

金融级生物识别的发展趋势

（一）**识别技术不断成熟。**随着人工智能、大数据、云计算等技术的加速发展，生物识别技术日渐成熟。

（二）**政策环境持续优化。**全球范围内许多国家和地区高度重视生物识别技术发展，不断加强顶层布局，为技术创新应用提供良好政策环境。

（三）**产业支撑日趋完善。**生物识别技术的发展带动市场需求逐步扩大，产业结构优化升级，产业支撑力度不断增强。

（四）**应用场景逐步拓展。**生物识别技术通过身份特征的数字化和隐形化，为身份核验提供便捷高效的可选替代方案。公安、社保、医疗、教育、交通等行业均已探索生物识别技术的应用。

金融级生物识别的应用的风险和挑战

（一）生物特征易被复制，隐私保护面临严峻形势。生物特征涉及人脸、虹膜、声纹等用户隐私信息，由于固有特性、采集方式、集中存储等原因，导致信息泄露风险较大。

（二）攻击手段不断翻新，技防能力亟需迭代升级。生物识别技术持续快速发展，针对识别算法漏洞的攻击手段也不断翻新。

（三）算法性能仍有局限，应用场景受到一定限制。一是抗噪能力有待提升。二是环境变化影响较大。

（四）算力存储依赖度高，IT基础支撑压力较大。在后端支撑方面，生物识别技术逐步应用，催生出大量视频、图片、音频等非结构化数据的存储、传输和处理需求，亟需基于云计算、大数据等技术的基础计算与存储能力支撑。

金融级生物识别应用的思考

（一）**正确处理安全与创新关系。**安全是技术创新的奠基石，合理的创新是安全发展的助推器。生物识别作为一种新兴的人工智能技术，在金融领域应用仍然面临一定的风险和挑战，应用得当有助于提升金融服务质量和效率，应用不当则可能引发金融风险。

（二）**健全生物识别技术应用治理体系。**生物识别技术应用是一项系统工程，影响面广、复杂度高，关乎百姓切身利益。建议有关部门加强顶层设计与规范引导，不断完善治理体系，多措并举推动生物识别应用健康有序发展。

（三）**强化生物特征信息保护。**利用数据脱敏、隐私计算、分散存储等手段，强化用户生物特征信息全生命周期管理，加强生物特征敏感信息保护。