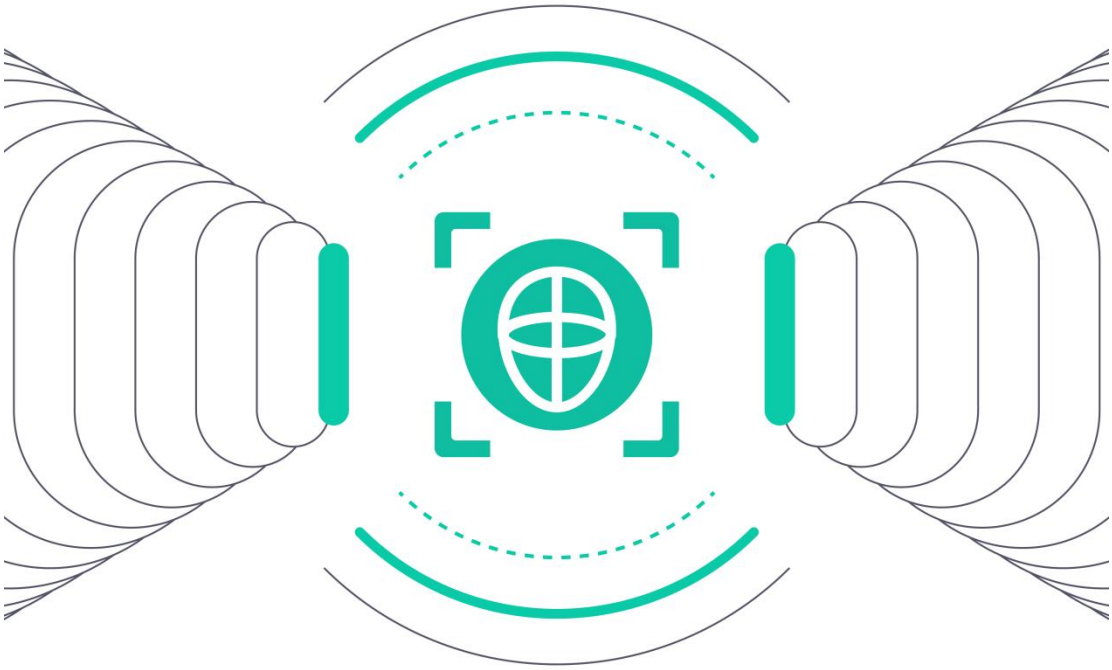
顶象
DING XIANG

人脸识别安全白皮书

【2022.9】



www.dingxiang-inc.com

版权说明

编委成员

编委成员（排名不分前后）

陈树华、戴义正、宋文利、张晓科、张祖凯、史博、沈嘉迪。

目录

一 什么是人脸识别？

1.1 概念介绍

人脸识别是基于人面部特征数据进行身份识别的一项生物特征技术，用于手机解锁、身份验证、上班打卡、刷脸进社区、刷脸考勤、刷脸乘车、刷脸购物等，在金融、医疗、安检、支付、文娱等诸多领域得到普及，为数字经济社会发展和人们日常生活带来了新机遇。

人脸与指纹、虹膜等生物特征均具有唯一性、难以复制性，采集和使用上具有非接触性、非强制性、多并发性、隐藏性和简单易用性等特点。通过影像设备或模块，捕捉或采集含有人脸的图像或视频，并能够自动进行跟踪、分析、检测、识别的一系列技术。人脸识别是一个集人工智能、机器识别、机器学习、模型理论、专家系统、视频图像处理等多种专业技术，是生物特征识别的最新应用。

1.2 人脸识别系统的组成

人脸识别系统主要由人脸采集、人脸检测、人脸图像预处理、人脸特征提取、人脸图像匹配、人脸图像识别等六部分组成。

1.2.1 人像采集

主要是通过设备或模块，自动搜索、跟踪并拍摄人脸图像、视频流等。

1.2.2 人像检测

主要在采集到的图像、视频流中，准确标定出人脸的位置、大小、五官形象，并将有用的信息挑出来，用于人脸识别的预处理。

1.2.3 人像预处理

基于人脸检测结果，对人脸图像进行处理并预特征提取。包含，对图像灰度校正、噪声过滤、光线补偿、灰度变换、直方图均衡化、归一化、几何校正、滤波以及锐化等。

1.2.4 人像特征提取

人脸器官包含眼睛、鼻子、嘴巴、下巴、眉毛、耳朵、头发等，基于人脸器官的形状、描述以及之间的距离、特性勾勒出人脸分类的特征数据。人脸识别系统基于人脸的视觉、像素统

计、图像变换系数以及图像代数等特征，对人脸器官特征数据进行提取，然后对人脸进行特征建模。

1.2.5 人像匹配

提取的人脸图像的特征数据与数据库中存储的特征模板进行搜索匹配，通过设定一个阈值，当相似度超过这一阈值，则把匹配得到的结果输出。

数据库的人脸图像并非是人像图像的原图或视频，经过特征处理、运算后，存储为一个个数字模型、数字编码。

1.2.6 人像识别

人脸识别就是将待识别的人脸特征与已得到的人脸特征模板进行比较，根据相似程度对人脸的身份信息进行判断。人脸识别包括两个技术环节：人脸检测和人脸识别。

1.3 人脸识别的应用及不足

1.3.1 人脸识别的应用

人脸识别已经应用在社区住宅的门禁，地铁、公交、高铁的闸机，疫情防控的电子哨兵，公司的考勤打卡，零售消费中的售货机，银行开户、支付、转账、消费，保险理赔，账户注册以及公共安全等，生产、生活、工作、学习的各个方面。

《2021 人脸识别行业白皮书》显示，2021 年中国人脸识别市场规模为 56 亿元，预计 2022 年达到 68 亿元，到 2024 年突破 100 亿元；年均保持 23%增速。其中，人脸识别应用最多是安防占 54%，其次是金融占 16%。此后分别是娱乐 10%、医疗 7%、电商零售 6%、出行 3%、政务 2%、其他 2%。

1.3.2 人脸识别的不足

人脸识别的过程就是在采集或提取的人脸图像特征与数据库中预先的模板进行照、匹配，根据相似度与提前设定的阈值结果比较。如果满足阈值，则系统判别相符，业务执行确认、通过、安全等操作；如果未满足设定的阈值，则系统判别不相符，业务则拒绝、退出等操作。

人脸识别受算法及检测影响较大。首先，很多人脸识别算法采用手工提取特征方式，受人为经验、获取的图像数量、质量、种类影响较大，这就导致不同人脸识别算法人脸特征选取差异大，直接影响人脸识别准确率。因此，人脸识别模型泛化性、准确率等参差不齐。

其次，活体检测利用硬件设备或软件算法判断图像采集设备捕捉到的人脸图像是否来源于活

体。人脸活体检测主要包含基于人的嘴部、眼部、头部的行为动作，以及摄像头、3D 结构等硬件设备辅助进行检测，基于皮肤和其他材质光谱反射率差异判定真假人脸，并利用多光谱信息，判别人脸与图像、头模、平面、视频的差异。

二 身边的人脸安全事件

由于人脸识别技术运用主体的技术条件和管理水平良莠不齐，不法分子甚至会开发作弊工具来破解、干扰、攻击人脸识别技术背后的应用和算法，进而引发盗窃、诈骗、侵入住宅等犯罪，危及被害人的数据安全、财产安全乃至人身安全。

2.1 卫浴门店自动抓取人脸信息

2021 年央视“3·15”晚会点名某卫浴门店收集人脸数据的问题。该卫浴门店在全国上千家门店，每个门店安装有人脸识别功能的摄像头，消费者只要走进门店，在不知情的情况下，就会被摄像头抓取并自动生成编号，标注顾客第几次到店、男女、年龄等信息。所涉收集人脸数据，能通过人脸识别信息解决精准营销，抓取的人脸数据信息累计上亿。

2.2 安防公司泄露人脸信息

2019 年 2 月，深圳某“AI+安防”公司人脸识别数据库缺乏保护，导致大规模的数据泄露。该数据库包含了超过 256 万用户的信息，包括身份证号码、地址、出生日期、识别其身份的位置。

2.3 人脸信息被大量低价兜售

2019 年媒体报道，人脸信息在网上被公开兜售，5000 多张人脸图片打包只要 10 元钱。更有报道，大量社群和境外网站进行真人人脸识别视频的贩卖。“价高质优”的验证视频百元一套，动态软件将人脸照片制作成“动态视频”只要几元，以完成各类线上业务人脸识别的验证。

2.4 小偷戴面具骗过小区门禁

2019 年，济南某小区接连遭窃。警方发现，小偷使用从网上购买的“人皮面具”通过小区门禁，轻松进入。

2.5 现场打印人像照片登录他人账号

2017 年“315”晚会上，主持人在技术人员支持下，仅凭观众自拍照就现场“换脸”破解了“刷脸登录”认证系统。

2.6 睡梦中账号被刷脸登录

2021 年，28 岁男子黄某辉趁前女友董某熟睡，翻开董某的眼皮，通过人脸识别，登录账号，分多次从董某的花呗、借呗、支付宝余额和银行卡转走人民币共 15.41 万元，最后通过套现将这些钱转到自己手机上。最终，男子黄某辉被判处有期徒刑三年六个月，并处罚金人民币 2 万元。

2.7 储户深夜被刷脸盗取百万元存款

2022 年 7 月，两大银行爆出的人脸识别系统漏洞，多名储户的数百万存款被异地“刷脸”盗取。

2.8 人脸信息遭冒用储户莫名背上贷款

2021 年，广州互联网法院通报了一起因为“刷脸”引发的借款纠纷。客户王兰（化名）在遗失了身份证后，却被人冒用身份通过银行的“人脸识别”贷款，导致王兰因逾期被告上了法庭。经司法笔迹鉴定，认为案涉客户签名并非王兰本人签署，手机号码亦未曾登记在王兰名下。最终，法院驳回银行全部诉讼请求。

2.9 黑灰产盗用人脸信息疯狂借贷

2020 年 10 月，四川警方查处一个上百人的诈骗团伙。该团伙购买大量人脸视频，借助“僵尸企业”“空壳公司”，为 6000 多人人包装公积金信息，然后向多家银行申请公积金贷款，最终带来 10 亿多元的坏账。

2.10 破解人脸系统进行虚假打卡

2021 年底，“考勤打卡神器”的新闻刷屏网络。就职于某保险公司的梁女士，每天无需到公司上班，通过屏蔽摄像头影像采集、拦截无线网络检测，并对 GPS 劫持，伪造虚假的 LBS 地理位置。在进行相关设置后，代理人输入自己的工号、上传照片，在家里就能完成每日打卡并拿到全勤奖。

三 人脸面临的三类安全隐患

可以清楚地看到，人脸识别技术带来人们便利的同时，也要带来的各类各类风险。基于以上风险案例，人脸识别主要面临信息泄露、算法不精准和应用遭破解三类安全隐患。

3.1 人脸信息泄露

人脸是重要的隐私信息，利用业各种技术和手段，在未经同意允许或批准的前提下，通过公开或非法手段，收集、保存、盗取正常的人脸数据，一旦信息出现泄露，不仅被不法分子进行用于诈骗，更可能被反复贩卖牟利。

3.2 人脸识别算法不精准

戴上眼镜、帽子、面具，或者制作高仿模型、将 2D 人脸照片 3D 建模、利用 AI 技术将静态照片变成动态照片等多种技术均，骗过人脸识别算法和活体监测算法。

3.2.1 虚假人脸

使用静态照片、通过播放预录制动态视频、利用图像处理或三维建模软件将照片转换为动态视频，混淆人脸识别判断。

3.2.1 人脸改造

戴上眼镜、帽子、面具等伪装手段，或者制作高仿模型、将 2D 人脸照片 3D 建模、照片活化等方式，骗过人脸识别检测。

3.2.3 技术换脸

通过 AI 算法，将视频中的人物面容替换为他人面容。或者通过 AI 换脸技术，将一张普通的静态照片，转化生成一张表情生动的人脸，甚至可以轻松地贴在另一个人的脸上，随着另一个人的动作和表情自动变化。

3.3 人脸识别系统不安全

破解人脸识别应用或安全保护，篡改验证流程、通讯信息，劫持访问对象、修改软件进程，将后台或前端的真数据替换为假数据，以实现虚假人脸信息的通过。

3.3.1 破解系统代码

破解人脸识别系统代码、人脸识别应用的代码，篡改人脸识别代码的逻辑，或者注入攻击脚本，改变其执行流程，人脸识别系统按照攻击者设定的路径进行访问、反馈。

3.3.2 劫持摄像头

通过入侵人脸识别设备，或在设备上植入后门，通过刷入特定的程序来劫持摄像头、劫持人脸识别 App 或应用，绕过人脸的核验。

3.3.3 篡改传输报文

通过破解入侵人脸识别系统或设备，劫持人脸识别系统与服务器之间的报文信息，对人脸信息进行篡改，或者将真实信息替换为虚假信息。

四 人脸风险背后的网络黑灰产

4.1 什么是网络黑灰产？

机械工业出版社出版的《攻守道-企业数字业务安全风险与防范》一书中，对黑灰产有明确的定义：*网络黑灰产是指利用计算机、网络等手段，基于各类漏洞，通过恶意程序、木马病毒、网络、电信等形式，以非法盈利为目的规模化、组织化、分工明确的群体组织。彼此分工明确、合作紧密、协同作案，每一环节都有不同的牟利和运作方式，形成一条完整的产业链。*

以大规模牟利为目的网络黑灰产，熟悉业务流程以及防护逻辑，能够熟练运用自动化、智能化的新兴技术，不断开发和优化各类攻击工具，不断发起各类欺诈攻击。

数据显示，国内黑灰产从业人员近 200 万，每年造成的业务损失达数千亿元。

4.1 黑灰产的特点

顶象与信通院联合发布的《业务安全白皮书——数字业务风险与安全》分析，网络黑灰产有四大团伙性、复杂性、隐蔽性和传染性四大特点。

4.1.1 团伙性

企业面临的数字业务风险越来越有计划、有预谋，业务欺诈分子彼此分工明确、合作紧密、协同作案，形成一条完整的产业链。他们熟悉企业各项业务流程，了解企业的需求、风控规则及业务漏洞，能够娴熟的运用移动互联网、云计算、人工智能等新技术进行业务欺诈操作。相较于个体欺诈，团伙欺诈行为更难侦测和识别，传统的反欺诈工具无法从全局视角洞察欺诈风险。

4.1.2 复杂性

业务风险欺诈不断变化，手段更迭快速，新攻击手段对既有的防控措施进行了调整甚至免疫，传统措施不能及时对新风险进行识别和预警。

4.1.3 隐蔽性

网络黑灰产对移动互联网、云计算、人工智能等新技术利用娴熟，风险欺诈手段日益复杂多变，数字化技术更便于业务风险团伙伪造、消除源头、路径，让业务风险的源头更加隐蔽，让取证更加困难。

4.1.4 传染性

数字化响应快，覆盖范围广，跨界、跨区域交叉特征明显，风险传播速度快，涉众广，传染性强，且多个业务风险叠加。当某个平台的业务上出现该风险，会被迅速复制到其他业务平台上。以往业务风险传染性以天计算，现在以分钟计算，传染性传播性大增。

4.2 国家对于黑灰产的治理

4.2.1 最高人民法院表示严惩

2021 年 5 月，最高人民法院举行新闻发布会，公布互联网十大典型案例，并表示通过案件裁判严惩网络刷单炒作信用、身份盗用、“薅羊毛”等网络灰黑产业及不诚信行为。

4.2.2 公安部连续开展整治

公安机关持续加大对“薅羊毛”、刷单炒信等网络黑产违法犯罪活动的打击整治力度，不断压缩此类违法犯罪空间。2021 年，“净网 2021” 专项行动，共抓获行业“内鬼”6000 余名，打掉关停接码、打码、解封、养号、非法交易网络平台 80 余个，收缴“猫池”、卡池设备 1 万余台，查获关停涉案网络账号 1000 余万个，对网络账号黑色产业链发起凌厉攻势。

4.2.3 网信办修改管理规定

2021 年 1 月，网信办发布《移动互联网应用程序信息服务管理规定》修订意见，明确表示，应用程序提供者应当规范经营管理行为，不得通过虚假宣传、捆绑下载等行为，或者利用违法和不良信息诱导用户下载，不得通过机器或人工方式刷榜、刷量、控评，营造虚假流量。

4.2.4 中国信通院出台安全建设标准

2022 年 6 月，中国信通院联合顶象等多家发布《业务安全能力要求》标准体系，对业务安全场景进行分类梳理，提出相应的安全能力要求，为国内企业有效识别和防护业务风险提供了指引和行业准绳。

4.3 针对人脸的安全保障

4.3.1 《个人信息保护法》

2021 年 11 月 1 日实施的《个人信息保护法》第五条规定：处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。
第十三条明确规定：符合下列情形之一的，个人信息处理者方可处理个人信息。
（一）取得个人的同意；
（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；
（三）为履行法定职责或者法定义务所必需；
（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；
（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；
（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；
（七）法律、行政法规规定的其他情形。

4.3.2 《反电信网络诈骗法》

将于 12 月 1 日实施的《反电信网络诈骗法》，对通信、互联网、金融有详细的治理规定。

第十九条 互联网服务提供者对监测识别的异常账号应当采取重新核验、限制功能、暂停服务等处置措施。互联网服务提供者应当根据公安机关、电信主管部门要求， 对涉案电话卡、涉诈高风险电话卡所关联注册的有关互联网账号采取关停等处置措施。

第二十条 网信、工信、公安等部门应当建立健全移动互联网应用程序备案机制。为应用程序提供封装、分发服务的，应当登记并核验应用程序开发运营者的真实身份信息，核验应用程序的功能、用途，支持实现对封装、分发的全程溯源。网信、工信、公安等部门和电信业务经营者、互联网服务提供者应当加强对分发平台以外途径下载传播的涉诈应用程序重点监测、及时处置。

第二十六条 任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、银行账户、支付账户、互联网账号;不得为非法买卖、出租、出借的上述卡、账户、账号提供实名核验帮助。对实施前款行为的单位和个人及相关组织者，可以采取限制其有关卡、账户、账号功能、暂停新业务等惩戒措施。对惩戒措施有异议的，可以提出申诉。具体办法由国务院公安部门

会同国务院有关主管部门规定。

第二十七条 国家支持电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者研究开发有关电信网络诈骗反制技术措施，用于监测、识别和处置涉诈信息、活动。国家金融、通信、互联网行业主管部门和公安部门等应当统筹推进跨行业、企业技术措施建设，推进涉电信网络诈骗样本信 息数据共享。对依据本法有关技术措施，针对异常情形采取的限制、暂停服务等处置措施，有关单位、个人可以向作出决定或者采取措施的有关部门、单位提出申诉。有关部门、单位应当建立完善申诉渠道，对提出的申诉及时核查，核查通过的，应当及时解除有关措施。

4.3.3 最高人民法院的司法解释

2021 年 7 月，最高人民法院发布《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》。解释明确规定，在宾馆、商场、车站、机场、体育场馆、娱乐场所等经营场所、公共场所违反法律、行政法规的规定，使用人脸识别技术进行人脸验证、辨识或者分析，应当认定属于侵害自然人人格权益的行为。

《规定》明确， 有下列情形之一，信息处理者主张其不承担民事责任的，人民法院依法予以支持：(一)为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需而处理人脸信息的；(二)为维护公共安全，依据国家有关规定在公共场所使用人脸识别技术的；(三)为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理人脸信息的；(四)在自然人或者其监护人同意的范围内合理处理人脸信息的；(五)符合法律、行政法规规定的其他情形。

2022 年两会上最高人民法院表示，最高法院针对一个具体问题专门出台一个司法解释是不多见的。司法规范“刷脸”，体现的是法院依法维护个人信息安全的鲜明态度，就是专门回应大家对人脸信息安全的担忧，作出了相应的规范。

4.3.4 中国信通院“可信人脸应用守护计划”

2021 年 4 月 7 日，中国信息通信研究院云计算与大数据研究所倡议发起成立“可信人脸应用守护计划”。顶象等多家公司入选第二批“可信人脸应用守护计划”成员单位，将与各界通力合作，积极探索人脸应用治理与发展的可信指引，助力人脸识别应用安全发展，共建可信的人脸应用生态。

4.3.5 “人脸识别第一案”的宣判

2019 年 4 月，消费者郭某支付 1360 元购买杭州野生动物世界“畅游 365 天”双人年卡，确定指纹识别入园方式。2019 年 7 月、10 月，野生动物世界两次向郭某发送短信，通知年卡入园识别系统更换事宜，要求激活人脸识别系统，否则将无法正常入园。郭某认为人脸信息属于高度敏感个人隐私，不同意接受人脸识别，要求园方退卡。双方因协商未果，2019 年 10 月 28 日，郭某向杭州市富阳区人民法院提起诉讼。

2021 年 4 月 9 日，“人脸识别第一案”终审判决。判决野生动物世界赔偿消费者郭某合同利益损失及交通费共计 1038 元，并删除郭某办理指纹年卡时提交的包括照片在内的面部特征信息，以及指纹识别信息。

五 人脸安全解决方案

人脸识别遭遇的威胁攻击包含人脸信息泄露、算法不精准、应用遭破解。风险隐患是一个点，安全防护需要一个面。因此，在人脸识别安全方面，需要在多方面加强防护，提升整体安全能力。

5.1 人脸信息安全保障

5.1.1 采集告知

人脸信息采集时，在人脸识别设备处设置显著标识，向个人信息主体告知处理规则。依据《个人信息保护法》完善隐私政策，将涉及人脸信息等个人敏感信息的条款重点标出。

5.1.2 加大惩戒

加大对人脸信息采集、存储、加工、传输各环节违规行为的惩戒力度。对于滥采、滥用的，需适当加大惩戒力度，形成有效震慑，增强公众的安全感。

5.1.3 定期销毁

建立人脸信息定期销毁机制，要求人脸信息本地化存储的同时，在一定周期内定期销毁相关数据。

5.2 人脸识别精准度的提升

5.2.1 增加算法检测

基于纹理的方法分析人脸图像样本中的微观纹理图案，进一步增强照片和真人的识别度；通过计算头发而非面部的傅里叶光谱，增强人脸视频检测的精准度。

5.2.2 增加唇语检测

除了点头、眨眼、转头等动作外，可以随机要求被检测者做几个连续性动作，并判断彼此连贯性。同时，增加唇语活体检测。系统给出的一组随机数字，根据摄像头捕获到的嘴唇动作特征，进一步核验是真人还是录制的视频。

5.2.3 颜色漫反射检测

人脸识别系统根据捕获到的图像的纹理、光线、背景、屏幕反射等特征，判断是否是真人。例如，通过在设备的屏幕上叠加不同颜色的背景，使屏幕对应颜色的光线映射到人脸上，这些漫反射的光线与打印照片、屏幕显示照片等的反射有明显区别。

5.2.4 红外摄像头扫描

通过近红外激光器的光线投射，再由专门的红外摄像头采集，由此得到人脸三维结构，进而辅助判别人脸真伪。

5.3 人脸识别系统安全保障

5.3.1 客户端安全

对人脸识别应用、App、客户端进行代码混淆、加密加壳、权限控制，做好终端环境安全检测，检查设备是否有代码注入、关键 API 遭 hook、root/越狱等风险，防范 API 接口、摄像头被篡改劫持。

5.3.2 通讯传输安全

对数据通讯传输混淆加密，防止信息传输过程中遭到窃听、篡改、冒用。

5.3.3 部署全链路风控

风控决策引擎能够全面检测设备环境，实时发现注入、二次打包、劫持等各类风险及异常操作，增强人脸识别从源头到应用的预警、拦截、防护能力。

5.3.4 专属模型构建

基于历史业务沉淀的数据，搭建专属的风控模型，为发现潜在风险、未知威胁、保障人脸识别安全提供策略支撑。

六 人脸识别系统的安全能力要求

6.1 需要有设备层面的安全感知能力

需要拥有基于设备指纹、操作行为、AI 策略模型的应用端、智能设备层面的安全感知的能力，包括环境风险感知、运行攻击感知。

6.2 需要有设备威胁的即时处置能力

除了通过传统的加固混淆技术，弥补应用开发中所产生的安全漏洞和潜在隐患外，还需要具备基于风险感知，进行多维分析，并提供与终端、业务紧密结合的响应处置的能力。

6.3 需要闭环的防御处置流程能力

业务人员关心当前是否存在安全问题、应用有没有漏洞、运行时有没有攻击、攻击来源发生在哪、能否进行有效监控及预警、能否定位到攻击位置、是否可以进行关联分析？所以，对环境风险、运行时攻击、异常行为的监测、预警、具有威胁时自动触发防护策略及处置、关联关系挖掘、以及数据沉淀的闭环处置流程是切实必要的。

6.4 需要满足监管合规要求

多个监管部门文件明确提出，人脸识别应用“要求利用终端威胁态势感知、客户端环境安全监测等技术及时发现并阻断恶意行为”、“应支持监控开户行为偏离多数用户的一般习惯，如在异常时间段、异常网络地址、异常地理位置等”，因此满足合规要求至关重要。

七 针对人脸识别系统的安全产品

7.1 顶象防御云

顶象防御云基于多年实战经验和技术产品，拥有丰富的技术工具、数万个安全策略及数百个业务场景解决方案，具有情报、感知、分析、防护、处置的能力，提供模块化配置和弹性扩容，助企业快速、高效、低成本构建自主可控的业务安全体系。

7.1.1 情报

30000+风险源，智能平台实时分析，防御策略实时推送，实现从感知到防控 0 空档。

7.1.2 策略

深耕 24 个行业，剖析 94 个场景 ，洞悉 188 类风险，沉淀 4445 条策略和 17170 个规则。

7.1.3 数据

自有的机器学习平台内置 100+种算法组件，可高效处理相关数据并作为情报中防御手段实现风控产品的对抗升级。

7.1.4 业务安全感知防御平台（移动版）

通过对移动端 100+风险项及异常行为的分析识别，及时发现针对摄像头劫持、设备伪造等风险，并提供从风险识别、预警处置、黑样本沉淀的闭环管理。具有可脱离决策引擎单独使用、轻量化、即时性强、数据开放能力高的特点。

7.1.5 设备指纹

通过对上网软硬件生成唯一指纹信息，支持安卓、iOS、H5、公众号、小程序，可有效侦测模拟器、刷机改机、ROOT 越狱、劫持注入等风险。具备 100%的唯一性、稳定性大于 99.99%、响应时间小于 0.1 秒、崩溃率小于 1/10000 特点。

7.1.6 端加固

基于虚机源码保护专利技术，为安卓、iOS、H5、小程序提供全方位的安全保护，有效防御调试、注入、多开、内存 Dump、模拟器、二次打包和日志泄露等攻击威胁。独有“蜜罐”功能、保护 Android 16 种数据和文件，提供 7 种加密形式，率先支持对 iOS 免源码加固。

7.2 顶象业务安全感知防御平台（移动版） 的特点

顶象业务安全感知防御平台基于威胁探针、流计算、机器学习等先进技术，集设备风险分析、运行攻击识别、异常行为检测、预警、防护处置为一体的主动安全防御平台，能够实时发现摄像头遭劫持、设备伪造等恶意行为，有效防控各类人脸识别系统风险。

7.2.1 威胁可视化

针对环境风险、运行攻击，可以将识别的风险标签展示在控制台，并支持按时间查询风险趋势、风险对应的设备型号分布、系统版本分布等维度数据。

今日
本周
本月
2022-08-01 ~ 2022-08-30
调试版APK
请求数量
25
调试风险
请求数量
20
注入攻击
请求数量
18
GPS篡改
请求数量
15
Hook风险
请求数量
11
内存篡改
请求数量
9
Janus漏洞
请求数量
8
读屏软件
请求数量
5
运行攻击风险请求数量
调试版APK
调试风险
注入攻击
GPS篡改
Hook风险
内存篡改
Janus漏洞
读屏软件
运行攻击趋势
60
40
20
0
2022-08-22
2022-08-23
2022-08-24
2022-08-25
手机型号分布Top10
HUAWEI
54
Apple
43
vivo
9
samsung
5
次数
系统版本分布Top10
IOS 14.6
43
droid unknow
40
Android 11
23
Android 7.1.2
5
次数

7.2.2 威胁可追溯

每一步攻击以及命中的防御策略及处置，都可以在基于需求定制和回放，让所有行为有迹可查。

请求时间	风险等级	风险类型	用户ID	IP地址	操作
2022-09-01 15:43:30:949	风险请求	hook		10.1.3.73	

序号	策略名称	策略模式	策略状态	优先级	执行结果	操作
1	云手机_云模拟器风险_高	规则匹配	上线	6	正常请求	
2	设备_检测存在hook风险_高	规则匹配	上线	6	风险请求	

2022-09-01 15:43:30:770	风险请求	hook	10.1.3.73	
2022-09-01 15:43:30:598	风险请求	hook	10.1.3.73	
2022-09-01 15:43:30:445	风险请求	hook	10.1.3.73	
2022-09-01 15:43:30:292	风险请求	hook	10.1.3.73	
2022-09-01 15:43:30:129	风险请求	hook	10.1.3.73	
2022-09-01 15:43:28:343	风险请求	云模拟器	10.1.3.73	

7.2.3 设备关联分析

基于历史数据、关联分析生成的设备画像，全面呈现出当前设备的所有历史请求，包含出现过的风险标签、常用地址、关联 IP 等情况。

7.2.4 多账户管理

满足多业务数据隔离需求，支持一级、二级等多级机构配置或下发不同策略。

7.2.5 覆盖 App、H5、小程序、公众号

注入劫持、驱动篡改、人脸识别绕过、监控嗅探、账号泄露、越狱 Root、浏览器伪造、禁用 Cookie、篡改禁用 UA、伪造访问设备、异常风险进程。

7.2.6 独有主动防御机制

移动态势感知提供了与终端、业务紧密结合的响应处置能力。在客户端进行响应处置，第一时间在终端处置对应的风险，对于高等级风险或者核心操作可以采取此种方式。与业务、风控系统结合，把终端发现的风险，以及对应的策略分析结果输出给业务/风控体系，再结合业务流程进行人工处置、加黑等操作。

7.2.7 开放数据接入

有效对接公有云数据对接，提供名单数据管理、指标特征管理、威胁情报管理、设备指纹探针等管理，并能够根据需求进行自定义处置，能够直接应用于企业自有的决策引擎、机器学

习平台，提升整体风控产品的防控能力。

7.2.8 支持防御策略和处置自定义

黑名单、云端数据，提供特征、使用模型、指纹策略和风险画像的输出，能够直接应用于企业自有的决策引擎、机器学习平台，提升整体风控产品的防控能力。

7.2.9 全流程防控

事前通过客户端安全、设备指纹技术、反欺诈侧进行进行风险防范，事中基于态势监控、设备与系统告警、多维度策略、实时决策和实施处置进行风险防控，事后基于审查设置、设备画像分析、关联关系挖掘、样本数据沉淀等进行风险分析与挖掘。

八 顶象护航人脸识别系统的安全实践

8.1 为保险公司挽回 500 万代理费用

以顶象近日拦截发现的“考勤打卡神器”为例。该工具是破解了某保险公司的官方 App，通过屏蔽摄像头影像采集、拦截无线网络检测，并对 GPS 劫持，伪造虚假的 LBS 地理位置。在进行相关设置后，代理人输入自己的工号、上传照片即完成“考勤打卡”。

目前，顶象移动态势感知防御系统已在多家保险公司应用。其中，在某保险公司省级分公司部署后，当月发现 10000+名代理人通过劫持人脸信息进行虚假考勤打卡，当月拦截阻止超过 15 万次风险操作，为分公司挽回 500 万元的代理费用。

8.2 保障银行案线上信贷安全

某区域银行的手机银行将业务嵌入到不同的生活场景中，让用户在生活场景中产生金融需求。疫情期间，在保障客户日常金融需求的同时，该区域银行手机银行提供了多种疫情相关金融、生活类服务，提升用户使用频次和用户粘性。在大幅提升用户便捷体验的同时，该手机银行却也遭遇到一起用户人脸信息被冒用骗取贷款的事件。不法分子收集、保存、盗取正常的人脸人像数据和敏感个人信息，然后仿冒被盗用申请贷款，骗取银行资金。

顶象业务安全感知防御平台能够及时发现设备指纹异常、模拟器检测、多开检测、注入、Hook 检测等异常，有效分辨正常用户及黑灰产的设备特征，增强手机银行的风险感知能力。并通过网银、手机银行、微信银行、网贷 App 等非柜面渠道的唯一标识，对手机银行做实时监测，进一步保障手机银行安全性，良好满足《移动金融客户端应用软件安全管理规范》管理要求。

8.3 为出行公司降低 39%营销费用

某出行公司拥有 1 亿多用户，活跃用户超过 1000 万，作为典型的移动互联网公司，在市场拓展和老用户回馈活动中，遭遇到薅羊毛、垃圾注册等风险，不仅用户合法权益受损，更影响业务正常运营。

基于顶象防御云，该公司建立一套营销拓展反欺诈防控体系。能够有效识别司机刷单、乘客逃单等异常用户和违法操作，同时进一步提升 App 安全性，增强黑灰产破解攻击能力。应用后，当周发现并定位 10 万+异常风险设备，拦截 90 多万次异常操作，营销精准率提升 45%，营销成本降低 39%。

九 关于顶象

9.1 顶象简介

顶象是国内领先的业务安全公司，旨在帮助企业构建自主可控的业务安全体系，解决伪造、盗取、劫持、破解等业务欺诈风险，防范化解各类网络黑灰产攻击，让业务更加健康稳定，助力企业创新与增长。

顶象自主研发了一站式业务安全感知防御云，包括设备指纹、无感验证、实时决策、端加固、安全感知防御平台等产品，在银行、电商、航空、出行、游戏、教育、旅游、媒体、政务、智能制造等行业积累了丰富的实战经验，沉淀了数万条业务策略和数百个场景化应用方案，能够为企业构建覆盖事前、事中、事后全生命周期的安全体系，提供情报、感知、分析、策略、防护、处置等服务。

顶象总部位于中国北京，在杭州、南京、广州、深圳、上海、成都、西安、济南设有分部，是 CNNVD（国家信息安全漏洞库）、CICSVD（国家工业信息安全漏洞库）、CNCERT（国家互联网应急中心）技术支撑单位和信创工委会会员单位，先后获得红杉资本、嘉实投资、晨兴资本、东方弘泰资本的数亿元投资。

公司 70%为技术人员，主要来自腾讯、阿里巴巴、百度、Google 等国际一流企业，均为专注安全、金融、人工智能、风控与大数据领域的资深技术专家。

9.2 部分客户

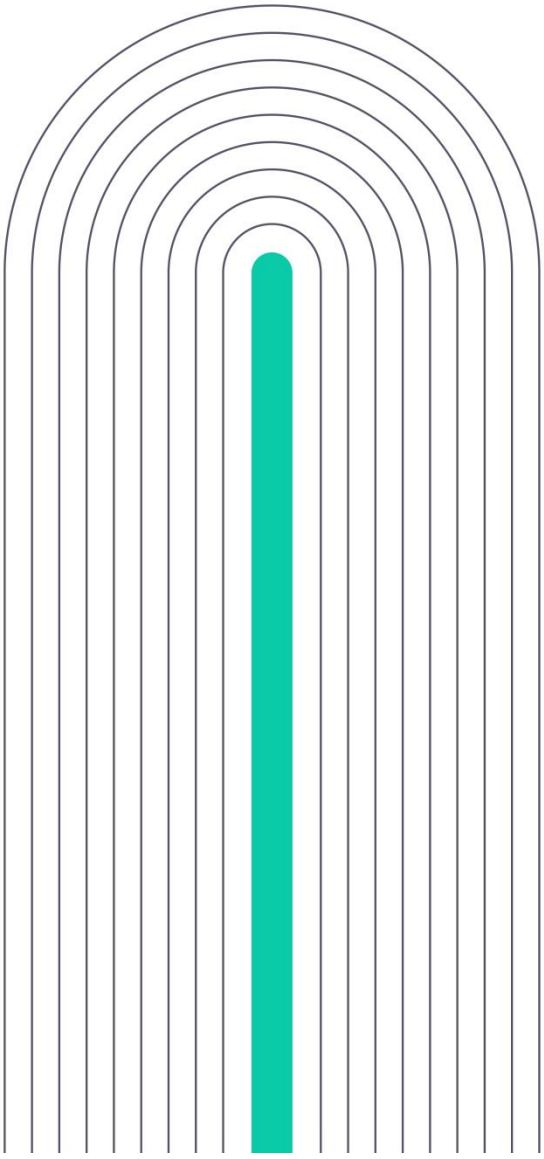

衣
meili
食
饿了么
美菜
Angel
行
Travelsky
中国东方航空
山东航空
MG
海航航空
喜马拉雅航空
车300
加油宝
UBIKE
AIR MACAU 澳门航空
昆明航空
T3出行
深圳地铁
住
LEJU 乐居
贝壳
华住会
婴
babytree
玩
悠英网络
游艺网
多乐游戏
漫客时代
3K游戏
雷龙科技
TU 途游游戏
贵诚网络
天天酷玩 tthw.cc
悦世界 YEAH WORLD
时空游侠
购
京客隆
MOJOY
回收宝
爱库存
商原集团
爱上街
学
洛基英语
娱
芒果tv
笑果
手机
oppo
vivo
车
理想
BYD
上汽集团
工
腾讯云
阿里云
ZALL 卓尔智联
ZTO 中通快递
HIKVISION
徐工信息
亿点连报
易安联
云客 yunkecn.com
中信云网有限公司
易维 Ewill
易路 eRoad
自营云
小i机器人
基地
BITMAIN
居
Haier
Midea
游
千寻位置
同程旅游
金融
中国银联
中国民生银行
浦发银行 SPD BANK
华夏银行
南京银行
宁波银行
齐鲁银行 QILU BANK
蓝海银行
众邦银行 Z-BANK
东风金融
辽宁振兴银行
新闻
界面新闻
新世相
友
Soul APP
公共
中国移动 China Mobile
国家电网 STATE GRID
中国卫通集团股份有限公司
政务
深圳市人力资源和社会保障局
IPE
朝阳区公众环境研究中心

9.3 联系我们

邮件：marketing@dingxiang-inc.com
电话：400 8786123
网址：www.dingxiang-inc.com

www.dingxiang-inc.com

顶象公众号



顶象 DING XIANG