

信息安全工程课题研究

|  |  |
| --- | --- |
| 题目： | Face认证验活方案报告 |

|  |  |
| --- | --- |
| 成 员： | 孙媛、杨法偿、汪蕴哲、吴勃志 |
| 院 系： | 软件与微电子学院 |
| 导师姓名： | 孙惠平 |

二〇一七年 十月

# **目录**

[**目录** 1](#_Toc496643262)

[第一章 选题背景 2](#_Toc496643263)

[第二章 产品现状 3](#_Toc496643264)

[第三章 研究现状 4](#_Toc496643265)

[第四章 主要思路 6](#_Toc496643266)

[第五章 项目分工 9](#_Toc496643267)

[第六章 项目计划 10](#_Toc496643268)

# 第一章 选题背景

2016年，旷视科技CEO印天荣登福布斯颁发的亚洲30岁以下领袖人物企业科技人物排行榜榜首，只有29岁的他，和团队一起开发出了世界上最顶尖的人脸识别技术，用户登录网络账户时，完全可以通过面部识别代替输入密码，不到一秒钟的工夫就能实现身份认定。人工智能的商业价值和竞争激烈程度都不断上涨，印奇在接受扬子晚报紫牛新闻记者采访时底气十足：“未来，我们要做中国人创办的世界上最伟大的人工智能公司。

2017年7月，国家把人工智能上升到战略高度，《新一代人工智能发展规划》发布，其中提到，新一代人工智能发展分三步走的战略目标，到2030年使中国人工智能理论、技术与应用总体达到世界领先水平，成为世界主要人工智能创新中心，人脸识别作为人工智能的分支之一，必定也将水涨船高。

2017年 7月8日，由阿里巴巴开发的国内首家无人零售超市在浙江杭州国际博览中心亮相，无人超市的收费系统，采用多模态生物识别，是指整合或融合两种及两种以上生物识别特征，利用多重生物识别技术的独特优势，这其中就包括了人脸、指纹、虹膜甚至是骨骼分析等方式。通过多种技术+数据分析，能够使认证和识别过程更加精准、安全。

2017年9月13日凌晨1点在Apple Park新总部史蒂夫·乔布斯剧院2017苹果秋季新品发布会上发布的苹果十周年特别版本，之所以命名为“X”是因为2017年恰逢苹果十周年，“X”在罗马数字中就代表了数字10。这个特别的版本去除了传统的指纹识别按键，采用了全新的人脸识别方式进行屏幕解锁 ，也必定暗示着以后手机解锁的趋势。

# 第二章 产品现状

2016年12月，北京西站在部分通道正式启用自助验证验票系统，旅客持车票和身份证，通过人脸识别技术确认之后，可以进站候车。旅客需要先取出二代身份证和蓝色磁卡车票，将遮挡面部的口罩、墨镜等摘掉。将身份证和车票要叠放在一起，同时放入机器的插口中，然后面向摄像头稍作停留等待机器进行识别。只要票、证、人相符，闸门就会开启，旅客只要取出身份证和车票就可以通过了。通过后，再进行安检进站。不过还是有限制，刷脸通道也不是什么票都能用，还有一些限制条件。如，没有磁性的红色纸质车票不能使用，持有减价车票学生票、残疾人票、军人票、使用家长身份证购买的小孩票和使用非二代身份证购票的都不能使用。这个系统提高了验证验票效率，助力2017年春运。

2017年10月，国庆长假期间，河南洛阳龙门石窟通过“互联网+”的深度融合，在十一前夕实行刷脸入园，游客只需在 微信购票时上传一张正面照片，便可在经过闸机时，被自动放行，成为全国首家智慧景区。

2017年3月，北京天坛公园厕所试点安装“人脸识别厕纸机”，目的是防止个别大爷去偷厕纸，拿厕纸的时候必须刷脸，刷一次只出60厘米，十分钟之内不能拿第二次。在试用该机器的三天时间内，平均每天的厕纸使用量减少了80%。

2017年9月，某中学为了应对学生经常忘带饭卡的情况，学校食堂采用了刷脸支付的方式进行支付，这大大提高了学生购餐速度，平均每个人只需8秒时间，同时解决了学生忘带饭卡的情况。

2017年，纪录片《辉煌中国》热播，该纪录片第五集《共享小康》，对“中国天网”监控可以实时监测识别系统进行了曝光。该系统可以实时监测区分出机动车，非机动车和行人，并能准确识别出非机动车的种类，以及行人的年龄、性别、穿着。

# 第三章 研究现状

**3.1 技术研究现状**

目前的主要应用方向依照技术可以分为2D人脸识别，3D人脸识别，脸部分析生物验活。这三种技术针对的攻击类型分别是静态图片攻击，视频攻击，3D打印面罩攻击（VR虚拟攻击）。而近些年，算法和深度学习的应用增加了未来人脸识别验证的稳定性。

国内外很多生产商都在提高人脸识别可靠性方面做了很多工作。比较著名的是2012年安卓系统根据静态图片攻击设计的眨眼验活，而该设计最后收效甚微。攻击者利用一张睁眼和一张闭眼的照片轻易攻击了系统。其他的特征识别例如虹膜识别，伪装者可以通过隐形眼镜迷惑验证设备。指纹识别的检测系统目前仍然无法有效防止指纹倒模的攻击手段。脸部识别机器除了普通的技术攻击，民间的高超的化妆技术也是一大挑战，更有甚者为了通过安检话费巨资整容，此类攻击基本很难通过现有的技术手段解决。

这充分说明我们需要的不仅仅是识别形态特征，而是需要找到稳定可靠的便于安全识别的相关的特征。

**3.2 现有解决方案**

从单纯的人脸识别看，目前面临的主要有两大挑战：

1. 预留照片数量有限
2. 被识别的对象识别动作不可控。

通常来讲，传统的攻击主要是通过动作眨眼，唇语，动眼球等动作可以有效预防。而现在社交网络大量的照片让传统的防御手段效果变差。同时也有人从社交网络下载图片并通过VR虚拟的方式完美的攻击了很多的商业用人脸识别设备。中高像素提供了纹理质地的素材，一般的不同照片提供了3D模型素材，完成攻击并不需要太多数量的照片。另外，该类检测对于光线的要求也非常高，通常完美的光线需求也是非常难满足的。

也有研究指出，通过手持手机设备的方式验活，该种方式通过计算脸部距离和实际距离变化的匹配度确实能一定程度的防止入侵。可实际上对于该类整张图精确距离的计算，算法要求非常高，因为采样点过多，错误的累积效应导致很难达到要求的精确度。在移动图片的同时，图片上抖动等因素会产生很多噪声，降噪手段也是很大的问题。但是，越是复杂的验证手段越是对攻击手段提出了更高的要求，也能从另外一个角度降低攻击成功率。

人类脸部存在相似性，不同个体之间的区别不大，所有的人脸的结构都相似，甚至人脸器官的结构外形都很相似。这样的特点对于利用人脸进行定位是有利的，但是对于利用人脸区分人类个体是不利的。在加上化妆的掩盖及双胞胎的天然相似性更增加了识别的难度。

　　其次是人脸存在易变性，人脸的外形很不稳定，人可以通过脸部的变化产生很多表情，而在不同观察角度，人脸的视觉图像也相差很大，另外，人脸识别还受光照条件(例如白天和夜晚，室内和室外等)、人脸的很多遮盖物(例如口罩、墨镜、头发、胡须等)、年龄等多方面因素的影响。大量的情景信息很难储存在原有的空间里，目前有提出利用基因分析等算法应对这种需要大量记忆且会发生细微变化的场景。

同时随着待识别的人数的增加、出现张得比较像的人的概率增加等情况逐渐增多，原有的人脸识别已满足不了实际的应用。现有的深度学习技术在这些方面有了很大的提升，可是又对我们机器的硬件的计算能力提出了更高的要求。我们能否通过已有的条件在不增加太大硬件复杂度的情形下，实现人脸识别的优势并且有效防止验证攻击的入侵是一个非常重要的问题。并且该类问题也有着很大的商业价值。

**3.3 可能的解决方案**

一些研究也给出了一些该领域可能有用的解决方案。

1. 利用闪光灯的不同亮度判断当前图片是否为真人，并且闪光灯要求必须随机发出不同亮度的光才能保证被模仿的程度降低。而这里虽然有效防御了可能的攻击但是对于闪光灯的硬件要求大大提高，市场上几乎没有闪光灯随机提供亮度的手机，这为该想法的可操作性提供了难度。
2. 通过检测脉搏心跳等方式确认被测试者是否为真人验证或者网络攻击。而这种检测方式也是通过镜头拍摄返回给机器的方式进行，只要加上一些颜色差异这种方式同样是容易被攻击的。除非开发出全新的设备例如直接检测出皮下组织的某些仪器，确实可以提供一个全新的验活领域，可是研发成本非常高，可普及程度也很低。也许会随着未来科技的发展用较低的成本实现该想法。
3. 红外线检测，目前少量的win10系统已经提供了类似服务，该种服务类型识别度高而且不容易被伪造尤其是最近有人提出的VR虚拟攻击，由于该类攻击无法提供红外线检测，可以非常有效的识别该类攻击，仍然是囿于硬件的限制，目前该项技术的发展受到了很大的限制。

如果想要安全等级尽可能高识别出尽可能多的入侵者，那么多会造成更大的错误拒绝风险。一些文章也提到，目前的研究来看，最靠谱的解决方案是提供一些非公开的不容易被轻易获取的图片源才能更成功的解决该类问题。

综合各研究的结果，我们认为，在现有的情况下，最大限度的发挥已有硬件的优势创造出识别率更高更便捷的验证方式才是最优的解决方案。

# 第四章 主要思路

基于以上的背景、产品和研究现状，我们对人脸识别的验活进行了深入的思考。要实现验活的目的，需要获取相关的信息来做确认。信息来源，硬件上，由于定位是手机平台，在不考虑让手机增加特殊传感器之类的硬件条件下，我们能用的是摄像头、加速器、陀螺仪等传感器；软件上，有方法如上面的研究现状看到，有实时互动、分析加速器数据、分析光学特征等。要对抗的攻击包括照片攻击、视频攻击和VR攻击。

从安全的角度来看，人脸识别的方式，我觉得在理论上是无法做到绝对安全的。最简单的，如果3D打印出一个被攻击者的人脸，套在攻击者的头上，人脸识别是无法辨别这种伪装的。基于这些考虑，我们设计的方案，考虑的角度是尽量保证有一定的安全性，而不是绝对的安全，其次是保证方案的易用性和可行性，在不增加手机硬件条件情况下使得用户容易且较安全的使用这个人脸识别。

基于以上的设计条件和设计原则思考，对于验活的实现，我们提出了以下几个方案：

1. **实时互动。**手机与用户互动，结合眨眼、张嘴、转头角度等一系列动作，手机随机的要求用户做出其中一种组合动作，以此完成验活。通过这一系列动作，每个动作的次数可选择多次，那么就可以组合出一个较大的密码空间，来较好的抵御视频攻击。这个方案是在前人研究的眨眼、转头验活的方案基础上改进的。因为单纯的眨眼或者转头，密码空间较小，很容易被视频攻击成功。安全性上，该方案其实还是较弱的；可行性上，较容易实现，实用起来时会跟其他人脸识别一样受周围光线和环境的影响；易用性上，当要求的动作次数过多时，用户体验差，验证时间过长。
2. **基于人眼反射成像的原理验活。**我们知道，人眼是会反射眼前的景象的，而照片或视频中的人眼是无法反射眼前的景象的。基于这个原理，这个方案是这么设计的：人脸识别捕抓人脸照片时，手机屏幕中用纯色背景显示字母或数字等随机信息，用户眼睛盯着摄像头，捕抓到的照片会可以看到手机屏幕中的信息。**从安全性**上看，只要手机显示的信息足够随机，无论是照片、视频或者VR攻击，都无法提前准备好相应的图像进行伪装攻击。有人会想，在照片或视频中人眼处放一个凸镜子之类的东西来模拟人眼的反射，这种攻击是有可能实现的。对抗这个攻击可能需要结合闭眼的动作才能抵御；**从可行性**上看，目前的手机相机的像素以及焦距可能还不太满足要求。一般前置摄像头靠太近拍，手机无法聚焦，图像是模糊的；靠太远，手机屏幕在整个照片中的比例过小，导致图像识别分析很困难。目前来看，手机屏幕信息如果是只显示一些较简单的数字、笔画或者颜色，是可能做到的，但这样密码空间小，安全性也低了。从长远的角度看，这个方案还是有一定的意义的，目前手机前置摄像头发展为双摄的可能性较大，双摄一般都会带一个微距摄像头。这种情况下，该方案就能有较大用处，因为此时人眼可靠近摄像头拍摄，捕抓到的照片中人眼占的比例会大很多，人眼中的手机屏幕信息就很容易分析了，显示的信息也可以更复杂，从而提高密码空间，增加安全性；**从易用性**看，该方案不需要用户做动作，只需要在验活过程人眼抵近摄像头拍摄即可。验证时间也会较短。



1. **基于人眼视线焦点的随机性验活。**该方案是这样的：手机在屏幕上随机的产生三个位置点，然后手机摄像头跟踪人眼的瞳孔转向，并相应的在手机屏幕中产生一个鼠标状的动点随瞳孔而动，人转动眼球去使得动点到达三个位置点，以此完成验活。**从安全性**上看，照片、视频攻击对这个方案都不能成立，因为照片中的眼球无法转动，而视频中眼球无法按要求把动点转到位置点。VR攻击有可能成立，但是目前来看VR攻击的成本和难度还是相对较高的。**从可行性**来看，这个实现起来应该是可行的，不需要增加其他硬件，目前大部分的手机摄像头条件都能满足要求，软件上也有算法能做到相应的功能。**从易用性**上看，需要用户转动眼球，稍微减弱了用户体验效果，验证时间也会变长。但，有附加效益，就是可以保护视力哈。



1. **基于生物应激反应行为验活**。这个方案尚未完善，仅供思考。举个例子，比如通过闪屏发出强光，使真实用户发生眨眼等应激反应的行为，捕抓那个瞬间前后的人脸情况，从而区别照片和视频。因为视频或照片攻击很难像人一样很快做出反应，要抓准那个时机放出录好或拍好的应激反应图像。

以上是我们提出的四个方案，对每个方案的安全性、可行性、易用性都做了一定的分析。综合来看，我们认为方案二和方案三更适合作为我们此次深入研究的方向，其中方案二的硬件条件还不成熟，未来有机会能实用化。方案三相对而言，会更可行一些。

# 第五章 项目分工

孙媛：负责前期研究现状的调查，资料收集、阅读以及分析，总结出实行方案以及做可行性分析，与其他成员共同参与应用的开发。

杨法偿：负责产品现状的调查，收集API，并通过做实验分析API的可用性，与其他成员共同参与应用的开发。

汪蕴哲：负责产品的需求分析，收集API，并通过做实验分析API的可用性，与其他成员共同参与应用的开发。

吴勃志：负责整个项目的方案策划以及论文的策划，与其他成员共同参与应用的开发。

# 第六章 项目计划

**第一阶段（2017年10月17日 - 2017年10月24日）：**

资料收集阶段，阅读项目相关的论文，对目前的研究现状、该方向的研究方法和实现方案有基本的了解，并提出自己的想法。目前已完成。

**第二阶段（2017年10月25日 - 2017年11月15日）：**

实验阶段，广泛尝试不同API，通过做实验最终选出能用于本项目的API，并根据实验结果排除不可行的方案。

**第三阶段（2017年11月16日 - 2017年12月13日）：**

实现阶段，将可行方案确立后，开始APP的开发，根据市场调查，我们选择了Android作为开发平台，所有组员将参与到应用的最终实现，并在开发完成后对其进行测试和Bug排除。

**第四阶段（2017年12月14日 - 2018年1月14日）：**

论文撰写阶段，将完成的APP投入应用，根据APP的使用情况分析经验和教训，并撰写论文。