尊敬的各位老师，各位同学，大家下午好！我是来自软件学院2013级软件工程专业的杨扬，我的研究方向是软件系统设计。我的实习单位是中国科学院深圳先进技术研究院，本次答辩课题为人脸活体检测系统的设计与实现。本次课题是由凌强副教授、曹洋副教授、谢晓华副研究员联合指导。

这是本次答辩的提纲。

首先，我会简要介绍下人脸活体检测系统的选题背景和选题意义；

紧接着，我会展开叙述本次论文的主要工作，包括系统需求分析、系统概要设计、系统详细设计、系统部署与测试4个部分。

最后我会对个人工作以及盲审意见进行总结。

现在将要介绍的是选题背景与选题意义。

本次课题名称是人脸活体检测系统，本课题来源于中科院与深圳市人力资源和社会保障局的合作预研项目，主要为了防止社保养老金发放过程中的冒领现象。

目前，随着人脸识别技术的日趋成熟，人脸识别得到了越来越广泛的应用。人脸特征具有个体差异大，用户体验好，永不丢失等优秀的特性。

但是，由于人脸图像极易被他人获取，如何验证当前人脸的真实性，成为了人脸识别系统必须解决的问题，也关乎人脸识别系统的信息安全。

为了解决这个问题，本次课题设计并实现了人脸活体检测系统，可以检测出仿冒的人脸并且拒绝其验证请求。

接下来，我会展开描述系统需求分析部分。

首先，本系统的设计目标为，预设一套交互式的验证动作，来最大限度地提升仿冒攻击的难度与成本。经过调研，最后选定了眨眼、张嘴和摇头三个动作。

其次，为了防止回放攻击，生成的验证指令的顺序必须是随机的，并且可以保存验证结果以及验证场景，方便管理员进行查询。

本系统的应用场景为，在人脸识别系统的输入端，对所有的输入人脸进行过滤，拦截非法的人脸，保护人脸识别系统的安全。

目前主流的几个仿冒攻击的手段如下所示：照片、石膏模型、面具、视频。

首先，我引入了摇头检测，由于照片中的人脸没法进行摇头动作，因此摇头检测可以有效地检测出照片仿冒的问题。

但是对于立体的石膏模型，摇头检测并不能有效地进行检测，此时就引入了眨眼检测。眨眼是人体正常的生理行为，也是活体的重要指标。系统可以检测在规定时间内，用户是否完成眨眼动作，以此判断输入人脸是否为活体。

这是本系统的用例图，在用例图中，可以清晰地看到，本系统的参与者分为两个角色，其一为用户，其二为管理员。

用户是被检测的对象，可以与系统进行眨眼、张嘴、摇头的行为交互。

而管理员是系统的后台的维护者，可以使用统计数据，训练模型等功能。

这是本系统的非功能性需求。

在本系统中，由于采用交互式的验证方式，因此为了保证用户体验良好，需要满足实时性的需求。

其次高效的验证方式可以尽可能地减少用户的等待时间，良好的健壮性和可维护性也是系统交付质量的重要指标。

下面，我将展开叙述系统的概要设计部分。

人脸活体检测系统使用C/S架构实现，分为客户机端和服务器端。

其中，客户机端负责实际的验证指令的指令并且引导用户做出交互动作。服务器端负责生成随机验证指令，并且负责存储验证结果，在web页面可视化地展示。

这是人脸活体检测系统的模块间通信示意图。

可以看出，在客户机端，控制器模块作为核心，负责调度眨眼检测、摇头检测、张嘴检测三个功能模块，

而三个功能模块在运行过程中又会调用另外3个API模块。

在服务器端，采用传统的MVC结构实现。

接下来，我会展开叙述系统的详细设计部分。

这是本系统的系统总体类图。

其中三个蓝色标示框所指示的部分分别为控制器模块、眨眼张嘴摇头检测模块、以及人脸特征点检测模块。

后续，我将在对上述三个模块的实现做简要阐述。

首先，我将介绍控制器模块。

控制器模块作为整个客户机端的调度中心，会与多个模块进行通信。

在客户机启动后，控制器模块会调用数据通信模块的接口，从服务器拉取版本号、更新训练文件、获取随机指令。然后，调用工厂类，产生实际的功能模块对象，最后执行该对象的主方法。

出于可扩展性的考虑，控制器模块应用了简单工厂模式进行设计，屏蔽了不同验证模块的不一致性，方便后续添加或修改功能模块的实现。

接下来，我会简要介绍下人脸特征点定位模块。

人脸特征点检测模块实现了2012年发表在CVPR上的ESR算法。

首先，需要提取形状索引特征，形状索引特征的本质是一种像素差异特征，它与传统的像素差异特征的区别在于，使用了相对坐标系代替了绝对坐标系，提高了每个样本点的语义一致性。

从下面4幅图像中，可以看到，左侧两幅图像为使用绝对坐标系下的样本点，在不同的人物或者不同表情的图像中，相同坐标的样本点所携带的语义信息并不一致。而在右侧的两幅图像中，由于采用了相对于特征点的坐标系，样本点的语义一致性得到了显著提高。

这是特征点检测算法的模块框架。

通过形状索引特征，可以将每一幅人脸图像映射至到一个向量中，并且修正当前形状，逐步减少误差。

由于每一次修正误差的能力不强，因此采用级联式的连接方式，将多个回归器串联在一起，提升结果精度。

同时，为了提升速度，采用二层级联式的回归器结构，也提高了算法的鲁棒性。

接下来，我将展开叙述眨眼、张嘴、摇头检测模块。

首先是眨眼检测模块。

针对眨眼检测的特点，本系统在构建了一个状态机模型来实现对眨眼动作的检测。

即，把眼睛开闭的状态跳变记为一次眨眼。然后判断在规定的时间内，眨眼数量是否达到或者超过阈值。

接下来是张嘴检测模块。在张嘴检测中，由于用户距离摄像头的距离远近可能会对图像的尺度信息造成干扰。

因此，系统会首先计算用户嘴唇的厚度，再通过嘴唇距离与嘴唇厚度的比值，来计算张嘴幅度。

最后是摇头检测模块。

在摇头检测模块中，系统会首先将图像分割成前景和背景两个部分，然后计算这两个区域的稠密光流。

根据一段时间内光流加权和的相关系数，判断前景和背景的运动一致性，即检测摇头动作是否完成。

接下来，是系统部署与测试部分。

本系统在开发完成后，还进行了完整的测试工作，包括单元测试，集成测试，以及功能测试。

所使用的单元测试框架为Mocha和Should.js，集成测试框架为Mocha和Supertest，所使用的功能测试框架为Cucumber。

在单元测试中和集成测试中，采用的测试方式为，使用mock的方式屏蔽无关模块，验证被测模块的状态是否符合预期。

在功能测试中，采用的测试方法为，使用浏览器接口模拟用户操作，同时验证被测模块是否符合预期。

这是系统的部署环境，本系统的产品环境部署在阿里云服务器上。

因此，对应的部署方式如下：Git代码仓库结合Web hook分别触发持续集成和持续部署插件，实现自动化测试和自动化部署的工作。

这是本系统运行截图。

在左侧为系统客户端的运行界面，右侧为系统web端的**结果可视化界面**和**日志查看页面**。

部署完毕后，本系统还进行了性能测试，各个模块的运行帧率和运行时间如图所示，均符合系统的非功能性需求。

接下来是个人工作总结部分。

在本次论文工作中，我参与了人脸活体检测系统的需求分析以及功能划分的工作，完成了客户机端与服务器端所有模块的设计与开发，并且进行了完善的测试工作。

本系统最大的创新点是使用尽可能简单的交互动作，最大程度上提升了仿冒攻击的难度与成本。

其次，采用基于异步多线程通信的模块化设计，提升了系统的总体性能，优化了用户体验。

最后是对两位盲审专家意见的总结。

这是专家一的盲审意见，左侧是意见的具体内容，右侧在论文中，具体的修改内容。

这是专家二的修改意见，也在论文中的对应部分进行了详尽修改。

以上是我本次答辩的全部内容，谢谢各位老师！