# 1 设计背景调研

## 1.1 时代背景:网购盛行，电子商务发展迅猛

1990年代以来，随着全球化和信息化进程的加 快，电子商务作为一种新型的消费模式在中国快速 发展，并对城市居民的日常消费和社会生活产生了 重要影响 。根据中国电子商务研究中心的最新 统计报告，2014年中国网络购物交易规模达到2.8 万亿元，同比增长47.4%，占社会消费品零售总额的 10.6%；同时，网络购物用户规模达到3.6亿人，占所 有网民的55.7%。2015年国务院发布《关于大力发 展电子商务加快培育经济新动力的意见》，肯定了 近年我国电子商务的发展成绩，指出电子商务在创 造消费需求、引发投资、开辟就业渠道、提供创新空 间等方面发挥重要作用，并积极推动农业、工业及 服务业行业电子商务的发展。电子商务作为信息 社会的重要消费方式，正在迅速成长，并深刻地影 响着人类生活的方方面面。

## 1.2 软件环境伴随行业:物流行业发展历程

电子商务迅猛发展的同时，企业生产、运作方式也发生翻天覆地的变化。国家邮局的统计数据显示，仅2018年1-2月，全国快递服务企业业务累计完成59.7亿，同比增长31.2%；业务收入累计完成786.9亿元，同比增长30.7%。中国已成为快递大国，据数据显示，截止至2017年底中国快递业务量已经连续四年位居全球第一。统计分析2017年全国快递服务企业业务量累计完成400.6亿件，同比增长28%。近年来，中国快递业务量持续增长。2017年达到近年来历史新高。随着国内快递业务量上涨，快递业务收入也在持续增长。据国家邮政局数据显示，2017年，全国快递服务企业业务收入累计完成4957.1亿元，同比增长24.7%。

## 1.3 物流安全发展的重要节点

2015年10月，李克强总理主持召开国务院常务会议，推进互联网+快递，发展农村电商确实促进快递业发展的措施。

2015年11月，公安部等15部门为了整治寄递物流安全风险隐患，快递包裹实时实名制的措施。快递实名制指寄件人寄快件时需出示本人有效身份证件，并且如实登记寄件人和收件人的姓名、身份证号码、联系电话、住址等个人信息，然后快递业务员将相关信息上传至指定平台进行记录。

快递实名制从长远角度来看，具有可取性和有益性。快递实名制可以增强快递服务的安全性，实现事前预防，匿名使个人处于非公开、非公众的评价 状态，进而导致社会规范难以约束个人的行为，容易诱发违法犯罪，实名的方式会增加寄件人寄件时 的心理压力，在快递实名制下，寄件人迫于被追责，在衡量违法成本后，往往会放弃其违法寄递行为，这就从源头上遏制了非法寄递行为。快递实名制也可以实现事后打击和控制犯罪，在发生快递事故或发现违禁物品后，公安部门可以通过寄件人登记的身份信息锁定违法寄件人，进而 有效的追究寄件人的法律责任，从而有效的打击、控制违法犯罪行为。

## 1.4 公民个人信息权亟需维护

然而，在快递实名制实行的过程中，个人信息却在赤裸的暴露着，公民的个人信息权存在被侵犯的隐患。

淘宝商家利用单号来刷单刷信誉的需求催生了 快递单信息的买卖，一些企业购买用户信息来电话 营销、精准营销，另外一些不法分子购买快递单信 息进行冒领、诈骗、入室抢劫、敲诈勒索等违法犯 罪活动。 一条快递单信息的流转需要经过多个环节，每 一个环节均存在用户个人信息泄露的风险，快递公 司监管存在漏洞，个别快递内部员工为谋取个人利 益，将快递单上用户的个人信息明码标价公开售卖， 圆通、韵达等快递公司都发生过内部员工将快递信 息进行售卖的事件，一些黑客攻入快递公司的系统， 盗取快递单上的个人信息进行违法活动。 快递行业成为个人信息被泄露的重灾区，据权 威机构统计，我国超过七成的网友个人信息被泄露， 快递渠道是主要原因之一。快递个人信息买卖已成 为黑色产业链，通过快递泄露个人信息比通过电信、 网络等其他渠道泄露危害更大，因为快递单收件人、 寄件人的姓名、身份、地址、购买的物品一一对应， 信息真实性更高，一旦被泄露，则使快递用户处于 非常危险的境地

## 1.5 公私权的博弈与平衡-维权策略

快递实名制是一种公共政策，是国家在行使公权力，个人信息权是私权利，快递实名制与个人信息权的关系是互相博弈的关系，即公权力与私权利互相博弈。公权力与私权利的博弈过程，其实是二 者不断寻求最佳配置的过程，也就是博弈均衡过程。

公权力来源于私权利，权利是权力的基础，卢 梭认为个人将自己所有的自然权利都让渡出来组成 社会共同体，公权力行使的最终目的是为了保障私 权利，假若公权力不能有效行使，私权利也会受到 损害。国家在行使公权力时，为了公共利益有时会 对私权利进行一定程度的限制，这种限制是有必要的。公权私权平衡之下，基于安卓平台的二维码快递信息保护系统应运而生。

# 2 设计设备与软件

## 2.1硬件设备

64位Windows10 操作系统的开发计算机一台;Android 8.0.0 测试手机一部;USB 3.0调试线一根。

## 2.2 软件环境

开发IDE:PHPStorm,AndroidStudio; 基础环境:PHP 7.0.12 –nts, Apache/2.4.23 (Win32) , mysql Ver 14.14 Distrib 5.5.53

## 2.3 设计方法

使用PHPStorm在装有支撑环境的开发机开发基于Android平台的二维码快递信息保护系统的录入Server ，绑定服务至ServerIp-Port 80并启动Http服务,提供整套系统的数据支持。

使用AndroidStudio在开发机开发调试基于Android 平台的二维码快递信息保护系统的 识别Client,使用调试线连接Android手机通过adb进行调试修改。

# 3 设计涉及的技术理论支撑

## 3.1 非对称加密与解密

本系统使用非对称加密（RSA）来对字符进行加密解密。与对称加密[算法](https://baike.baidu.com/item/%E7%AE%97%E6%B3%95)不同，[非对称加密算法](https://baike.baidu.com/item/%E9%9D%9E%E5%AF%B9%E7%A7%B0%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95)需要两个[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5)：[公开密钥](https://baike.baidu.com/item/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5)（publickey）和私有密钥（privatekey）。[公开密钥](https://baike.baidu.com/item/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5)与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5)，所以这种算法叫作[非对称加密算法](https://baike.baidu.com/item/%E9%9D%9E%E5%AF%B9%E7%A7%B0%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95)。

如图 1 所示，甲乙之间使用非对称加密的方式完成了重要信息的安全传输。

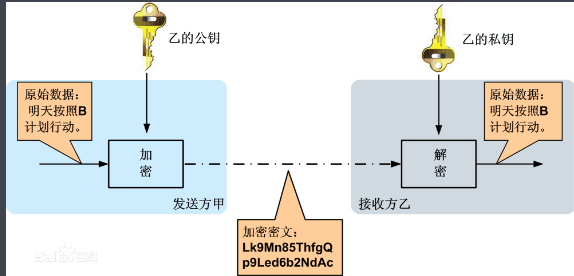


图 1 非对称加解密模拟过程示意图

1、乙方生成一对密钥（公钥和私钥）并将公钥向其它方公开。

2、得到该公钥的甲方使用该密钥对机密信息进行加密后再发送给乙方。

3、乙方再用自己保存的另一把专用密钥（私钥）对加密后的信息进行解密。乙方只能用其专用密钥（私钥）解密由对应的公钥加密后的信息。

在传输过程中，即使攻击者截获了传输的密文，并得到了乙的公钥，也无法破解密文，因为只有乙的私钥才能解密密文。同样，如果乙要回复加密信息给甲，那么需要甲先公布甲的公钥给乙用于加密，甲自己保存甲的私钥用于解密。

## 3.2 Quick Response Code 技术

Quick Response Code techology 是基于最初以存储商品为目的的一维条形码的扩宠，又称二维码的一类分支。对比一维码，二维码在表现形式上略显不同，在水平竖直方向均记载数据;同时二维码有别于前代能记录除了字母数字外的其他信息，在我的涉及中这点表现在存储汉字信息。Quick Response Code 在容错性方面更占优势，在快递转运和配送过程中具有一定的抗销毁能力。

Quick Response Code呈现为正方形，常见为黑白两色。其右上角，左上角以及左下角的较小图案用于帮助解码软件快速定位图案的位置，正是因为如此，用户无需对准无论任何角度都可扫描，数据都可以正常读取。图2是关于Quick Response Code的区域对照功能介绍。

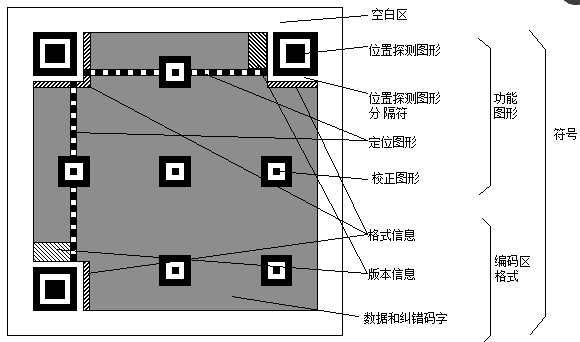


图 2 Quick Response Code 区域功能对照

## 3.3 二维码识别

Zxing是一个开放源码的，用Java实现的多种格式一维或者二维的条码图像处理库，它包含了联系到其他语言的端口，通常使用Zxing生成相应的二维码码以及解码。生成二维码的编码技术是指基于给定内容生成二维条码图片，Zxing可以对生成的二维码的图片格式、各项参数以及二维码类型进行设置生成的图片包含给定的内容，当使用识别设备进行扫描时，能够读出给定的内容。使用Zxing进行编码的步骤主要如下：首先，将所需的Zxing类库中的包导入工程；其次，对需要生成二维条码的给定内容进行编码方式处理，防止在显示中文时出现乱码问题，并指定所生成二维条码图片的路径、名称和文件格式；然后，找到Zxing中二维码QR码所对应的编码类 QR-CodeWriter调用encode方法生成给定内容对应的比特矩阵；最后将比特矩阵转化为制定的图片格式。

二维码处理流程如图 3 所示，若已有二维码图像，直接读取该图像，在此基础上完成解码识别等过程，用户也可按照自己的意愿在文本框里输入汉字或数值等内容，调用Zxing,生成对应的二维码图像。后对图像进行灰度化、加噪平滑、二值化、旋转校正、畸变校正等预处理，并在此基础上再次调用Zxing完成解码识别的过程。

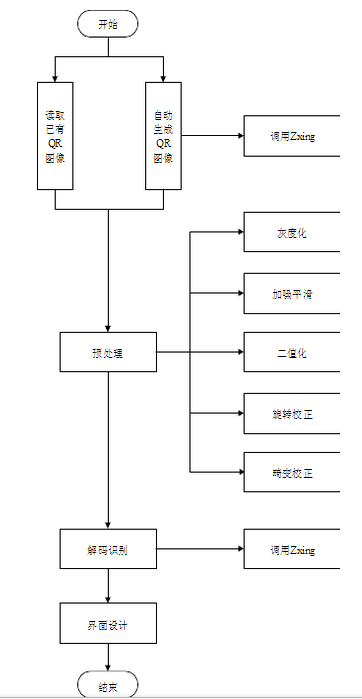


图 3 Qucik Response Code解码流程示意图

# 4 设计过程

## 4.1 Web-ServerSide 服务端设计

基于安卓的物流信息保护系统(SFIPS SF-Information-Protect-System )由web服务端SFES(SF-Express-Server)与安卓client SFMC(SF-Express-Mobile)。

## 4.1.1服务端设计模式

服务端基于MVC(模型-视图-控制器)的方式来组织。MVC是一个设计模式，它强制性的使应用程序的输入、处理和输出分开。使用MVC应用程序被分成三个核心部件：模型（M）、视图（V）、控制器（C），它们各自处理自己的任务。

## 4.1.2服务端应用周期

服务端应用SFES(SF-Express -Server)基于PHP开发,代码架构上引用轻量级面向对象开发的THINKPHP，性能出色且代码精简。

SFEM的生命周期符合软件工程标准，概述共包含如下阶段，详述请参考图3 SFES work-flow

一 加载入口文件

二 加载引导文件

三 注册自动加载

四 加载错误和异常机制

五 应用初始化

六 开始 请求-相应-返回 的处理

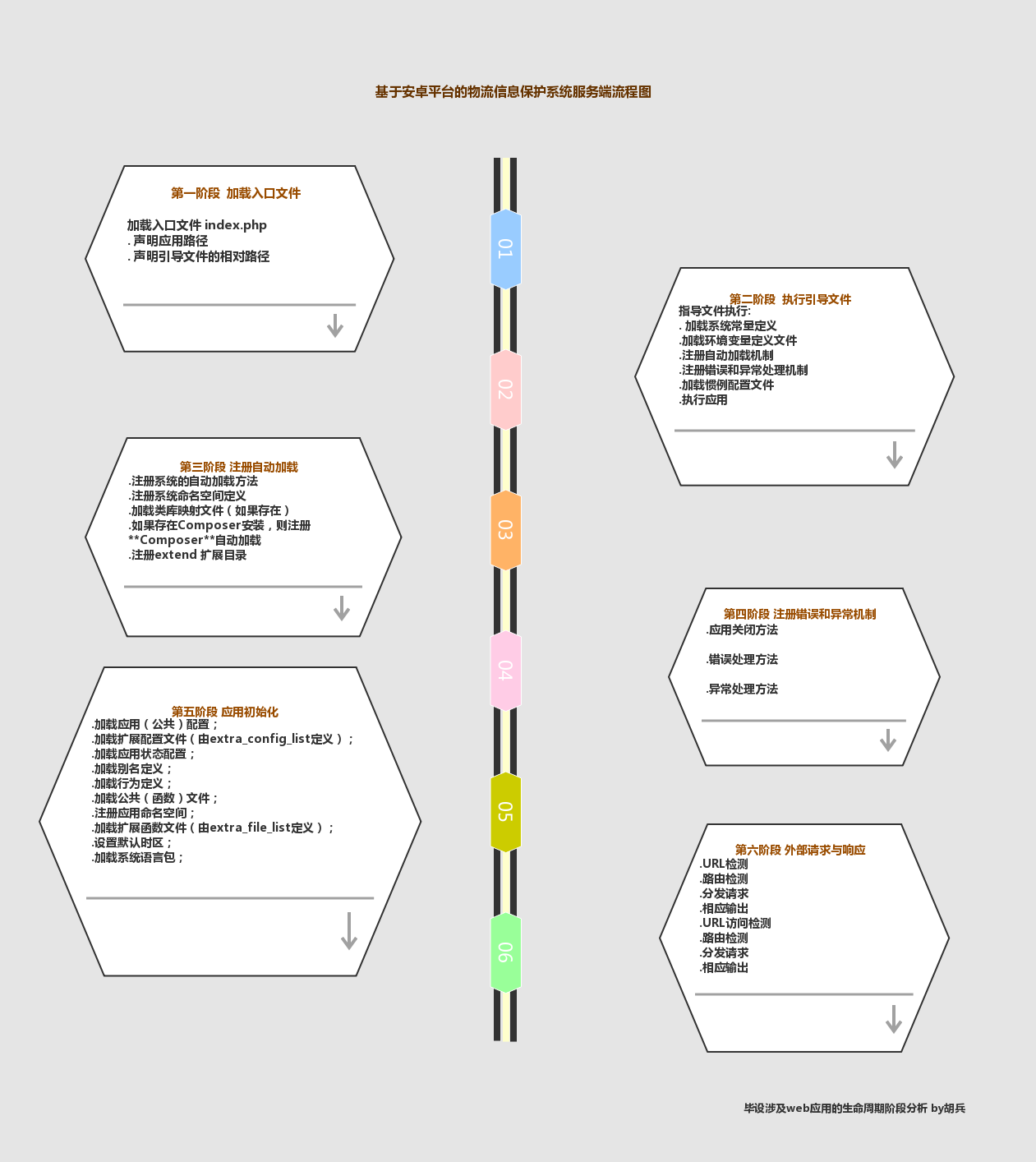


图4 SFES work-flow

## 4.1.3服务端业务逻辑

服务端业务逻辑是根据真实物流行业业务逻辑制定的，对应物流转运过程中的信息入库、中转扫描分流，业务员派件对应服务端揽件生成专属二位快递信息码、靶枪快递码扫描、派送员Mobile Client收件派发。

SFES第一个基础版本 涉及的业务以及延伸业务包含如下

一 身份验证与会话管理

身份认证SFES 采用Session会话管理，为了避免XSRF 攻击，强制要求信息敏感请求HTTP请求方式一致为POST、请求携带携带服务端验证的cookie数据，过滤伪造的请求。Session 使用Redis 维护，高效可靠。

二 快递信息加密处理

二 机密后快递信息的二维化

SFIPS 采用 PHP-Qr-Code (<http://phpqrcode.sourceforge.net/>) 生成二维码面单。PQC支持6级容错和1-40 个各种尺寸的PNG、JPG文件导出类型，PQC支持数据缓存，生成速度可观。

SFIPS 支持单条和excel文件批量导入的方式生成二维码制面单，经过测试生成速度迅速，10000张二维面单生成仅耗时10.25s。

三 二维面单的同步管理

考虑服务器带宽和访问压力，所有的二维面单都存储在骑牛CDN 的云转存节点，数据同步使用开源关系型数据库Mysql ,Mysql 作为企业级的持续存储服务提供者，具有稳定高并发的特性。

**4**.1**.3服务端代码结构**

服务端应用SFES 代码结构如下图5所示

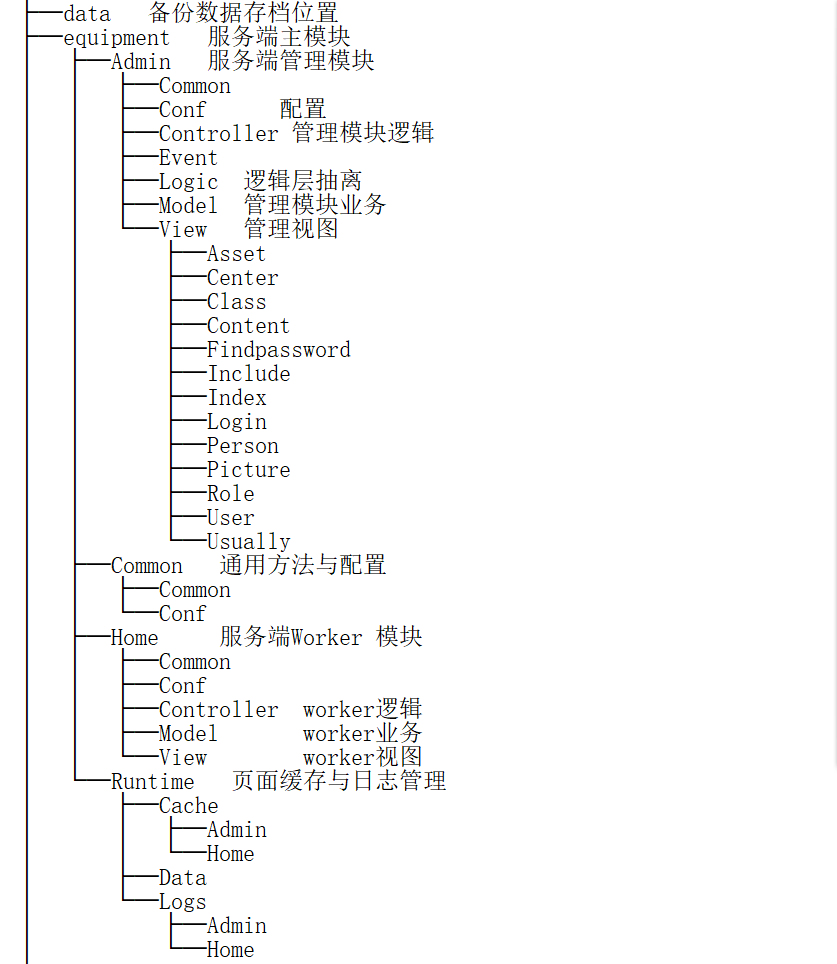


图6 SFES 代码结构a

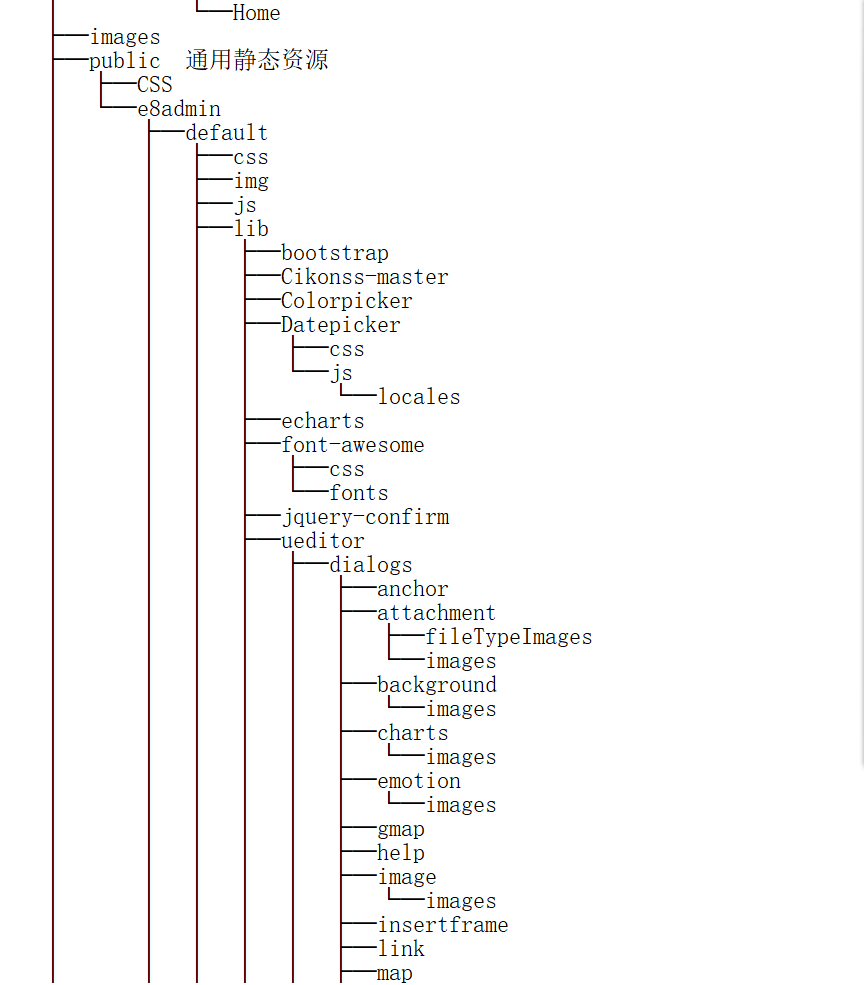


图7 SFES 代码结构 b

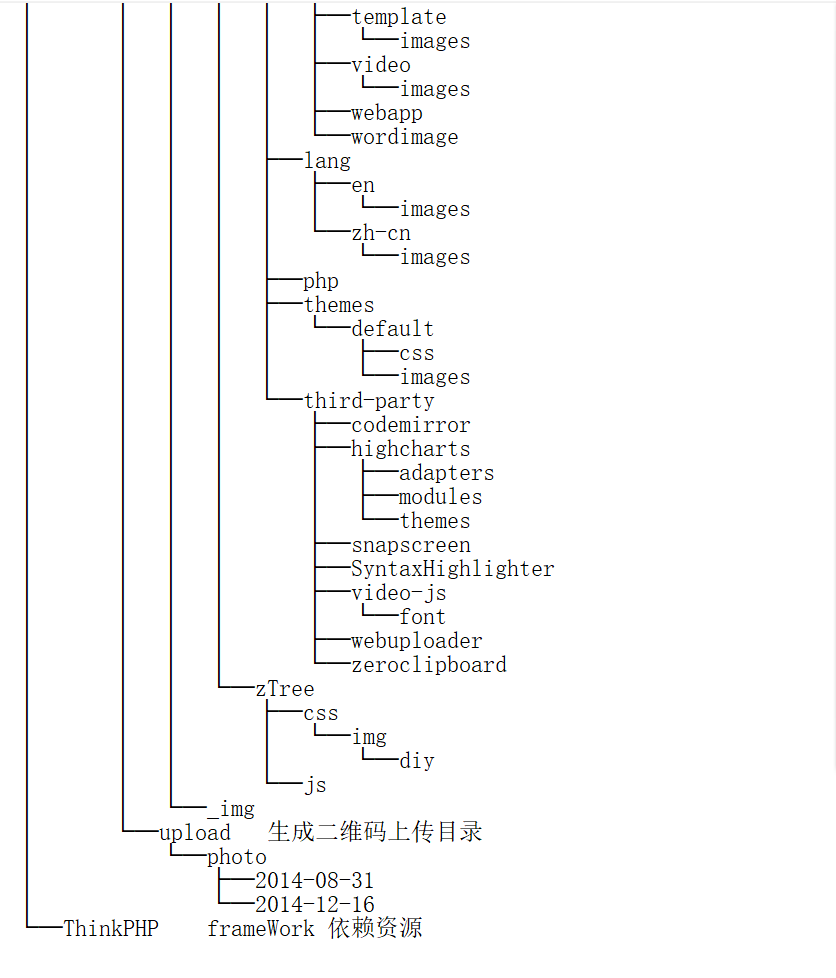


图8 SFES 代码结构 c