文章编号:1671-4598(2016)02-0225-03 DOI:10.16526/j.cnki.11—4762/tp.2016.02.062 中图分类号:TP273 文献标识码:A

# 基于三重人脸识别身份验证的门禁管理系统设计

孙 伟,刘晓敏,王浩宇,杨海群
(中国矿业大学 信息与电气工程学院,江苏 徐州 221008)

**摘要**:针对目前门禁管理系统存在的身份验证模式较单一、安全级别较低等问题,并且为满足高保密性、高安全性场合的需求,设计了一种基于移动 Android 终端、嵌入式现场终端以及上位机系统的三重身份验证的安全门禁管理系统,并且利用人脸识别技术的独特性进行控制;简单介绍了系统的软件和硬件开发平台、系统整体的网络拓扑结构,给出了系统的整体实现与运行框架,并且详细设计了基于移动 Android 端、嵌入式端以及后台服务器端的 3 个子系统的软件部分,包括流程图设计及各个软件界面设计;进行多次模拟试验,最终给出整个系统的部分运行效果图;结果表明,该系统能够进行三重身份识别验证,准确度较高,运行稳定,能够很好得满足特殊场合的需要,具有良好的实用前景和推广价值。

**关键词**:门禁系统;安卓终端;嵌入式终端;上位机;人脸识别

# Design of Access Control Management System Based on Three Times of Face Recognition Authentication

Sun Wei, Liu Xiaomin, Wang Haoyu, Yang Haiqun
(School of Information and Electrical Engineering, China University of Mine and Technology, Xuzhou 221008, China)

**Abstract**: Against the problems that the current ways of authentication is single and its poor safety performance, and in order to meet the demands of high-security situations, designed an access control management system of three times of authentication based on Android mobile terminals, the embedded terminal and PC system, using unique face recognition for control at the same time. Described the hardware and software development platform of the system, and also described the network topologies and the overall design and implementation of the system. The overall framework of implementation and operation of the system is given then, and the three software portions of Android mobile terminals, the embedded terminal and back-end server software portion are designed in detail, including flow charts and various software interfaces at the same time. After many times of simulation experiments, part of the system running effect diagrams are given in the last. Experiment results show that this system is capable of triple identity verification and has a high recognition rate and runs steadily. It can meet the needs of special occasions well, which means a good practicality and promotional value in the future.

**Keywords**: access control system; Android terminals; embedded terminals; PC; face recognition

## 0 引言

随着计算机网络技术的发展成熟,信息安全越来越受到人们的重视,出现了各种身份识别方法[1]。其中,人脸特征识别具有非接触性、稳定性、独特性等优点而脱颖而出[2]。近年来,智能手机功能不断强大,基于此的识别技术成为又一研究热点,尤其是在一些人流量比较大、安全级别要求较高的地方。因此本文把人脸识别与嵌入式、手机、平板等相融合,设计出一套高安全级别的门禁管理系统。

## 1 开发平台介绍

### 1.1 硬件平台

1)服务器:联想 Y470 型笔记本,CPU 为 core i5、四核、4GB 内存,Win7 操作系统。本文的系统软件开发以及功能仿真均在此服务器上完成。

2)智能移动终端:小米 M3 型号手机,配置为:CPU 为高通骁龙 Snapdragon APQ8064 Pro、四核、CPU 频率为 1.7 GHz,2 GB 内存,前后摄像头,前置 1 300 万像素,后置 200 万像素,Android4.1 操作系统。本文的 Android 平台实际应用测试在此手机上完成。

3)嵌入式终端三星 S3C2410X 处理器采用 32bits 的 RISC ARM920T 核、单独的 16K 指令和数据 cache、内存管理单元 MMU 以支持 WinCE、Linux、EPOC 等操作系统,采用新型总线结构 AMBA (Advanced Microcontroller Bus Architecture),运行频率可达 203 MHz,272FBGA 封装,低功耗高性能设计,适合用于中高档手持终端等应用。

### 1.2 软件平台

1)Matlab 2010a 版本,Matlab 具有很强的数据分析、矩阵计算、系统建模等功能,适合算法仿真与实验,能够实现计算与结果的输出。

2)Eclipse4.2 开发环境,JAVA 语言环境选择 JDK8.0 开发。Eclipse 是基于 JAVA 的可扩展大型的开发平台,它支持 Java、C/C++、PHP 等多种语言。

3)Android SDK (开发工具包) 与 ADT 插件,开发工具包包括开发软件工具包、Android 模拟器等,下载后无需安装,放到指定位置即可,但用 Eclipse 进行 APP 开发时,必须为 Eclipse 安装 ADT,以建立与 sdk 的连接。

4)OpenCV-2.4.6-android-sdk-r2 库文件。OpenCV 是一个跨平台计算机视觉库,提供 Android 系统应用端的接

**收稿日期**:2015-08-18; **修回日期**:2015-08-25。

**作者简介**:孙 伟(1963-),男,江苏徐州人,教授,博士生导师,主要从事复杂过程控制方向的研究

口[3]。选用此库文件以支持 Android 手机端一些图像处理操作。

5) Microsoft Visual C++ 6.0，具有强大的可视化软件开发工具，包括程序向导 AppWizard、编辑器、调试器等。

## 2 系统整体设计

整个门禁管理系统主要由 3 部分组成，包括移动终端、嵌入式终端、后台服务器终端。

系统网络拓扑如图 1 所示。

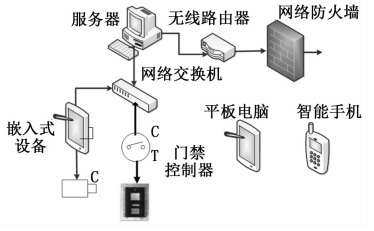


图 1 系统网络拓扑图

手机端的工作是开发 Android 手机 APP，主要功能是根据银行门禁权限的分配，在其权限者手机上安装 APP 软件[4]。软件的主要布局包括密码登录、密码修改、初始数据采集训练、采集图像、图像识别、数据上传等，主要用于验证手机使用者是否是手机持有者；嵌入式终端是常见固定于门禁旁的数据采集、控制设备，主要用于请求进入门禁的图像采集，以及控制门禁的开关；后台服务器终端存放于控制室，用于对移动终端和嵌入式终端上传的照片进行匹配识别，进而与数据库中已分配权限人员进行匹配，若匹配成功，则发送信号到嵌入式设备打开门禁，否则报警，通知相关安保人员[5]。

## 3 系统软件设计

门禁管理系统的总体运行框架如图 2 所示。

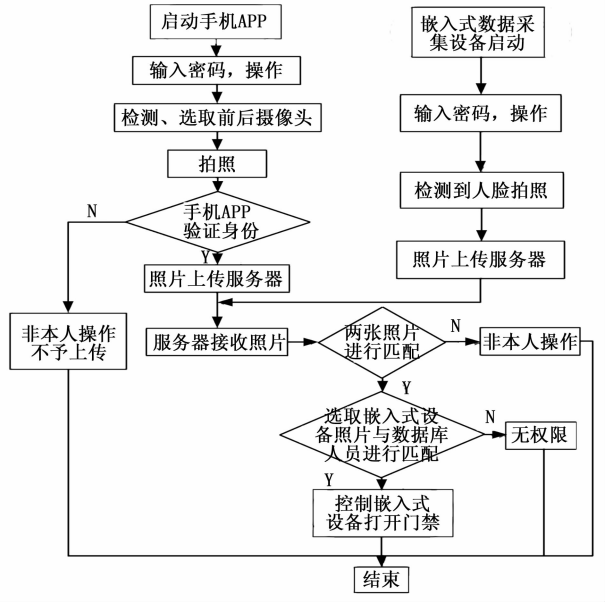


图 2 系统的总体运行框架

### 3.1 移动端软件设计

Android 手机端的主要工作在于 APP 软件的开发，运行流程如图 3 所示。启动软件，若是初次使用，需注册用户名和密码，密码和用户名存储使用 SharedPreferences 方式。注册后登录进入，功能菜单选择包括初次进入图像采集、摄像头选取、密码修改、版本更新等。初次进入图像采集，需采集多张人脸图像进行训练，使用的算法为肤色分割算法和 Sift 算法；摄像头选取主要是检测手机摄像头个数，摄像头调用有多种方式，包括采用 MediaStore、Camera 框架以及 Opencv 中的 JavaVameraView 类进行操作[6]，如果是前后摄像头则可进行选择使用；密码修改需要输入原有密码然后重设新密码，即通过操作修改 SharedPreferences 中的存储值实现；版本更新主要是检测 AndroidManifest. xml 中的版本号，与从服务器获取的最新版本号进行对比，为后期功能添加做准备。手机端 APP 主要界面如图 4 所示。

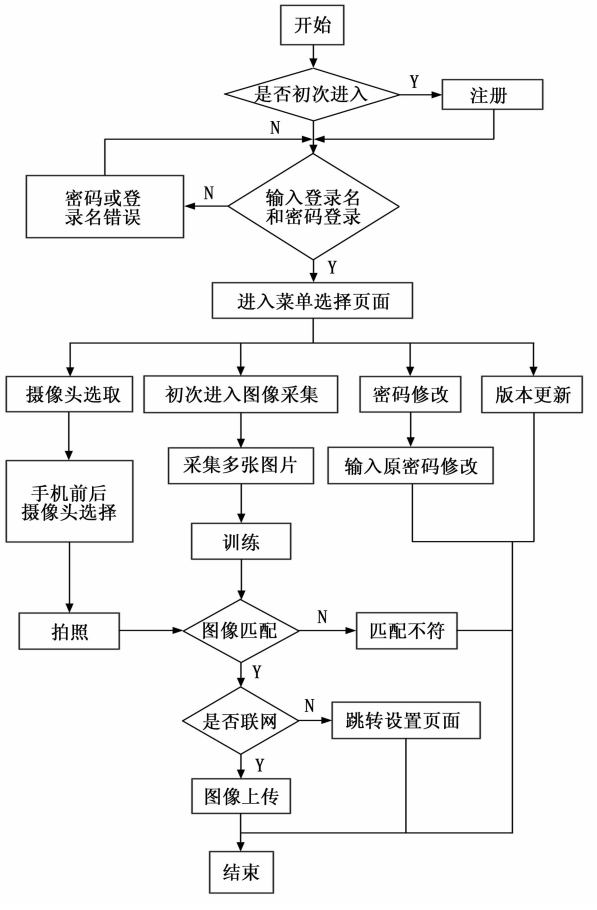


图 3 手机 APP 运行流程图

图 4 (a) 是首次登录软件，需要进行用户名和密码注册，由程序进行保存，联网后上传服务器数据库。图 4 (b) 是登录界面，输入用户名密码登录，为防止非手机持有者使用手机登录，这里选择不记住账户名和密码。登录成功后进入功能菜单选择页面如图 4 (c)，功能包括首次进入时图像采集与训练、训练成功后识别采集、密码修改、版本更新等。选择图像采集按钮会进入图 4 (d) 所示界面，进行照片拍摄，左边按钮用于单张拍摄，中间按钮用于多张连拍，每隔 2 s 采集一次，右边按钮开始训练，若训练成功，之后进入将不再显示此功能项，如图 4 (e) 所示，图片存放于 Android 手机 APP 所使用的 SQLite 数据库中。之后进入界面图 4 (f)，中间部分显示拍摄的照片，选择左边按钮可进行拍摄，选择右边按钮可进


(a) 首次登陆界面　(b) 正常登陆界面　(c) 功能菜单

(d) 图像采集界面　(e) 训练后功能菜单　(f) 识别采集界面

(g) 识别结果显示界面　(h) 密码修改页面

图 4　APP 实现结果图

入识别界面如图 4（g）所示，左边显示采集图像，右边显示模版图像，在下方显示匹配结果及姓名。若选择修改密码按钮则进入图 4（h）界面，需要对原有密码验证后才能修改。若选择版本更新则提示是否有新版本可替换。

### 3.2　嵌入式端软件设计

主要流程如图 5 所示，打开软件后，首先选择验证方式。本系统提供两种验证方式，RFID 射频卡验证和密码验证，主要考虑到进入者没有携带或者忘记密码的情况。验证通过后，进行图像采集、系统拍照，并通过网络上传到后台服务器中[7]。

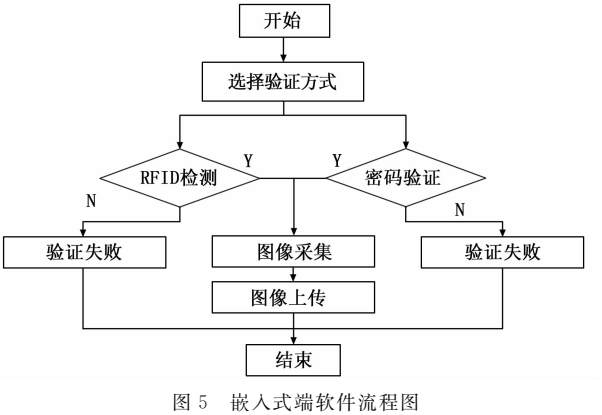


图 5　嵌入式端软件流程图

### 3.3　后台服务器软件设计

选用 VC6.0 软件，用 C＋＋进行编写，软件流程如图 6 所示。

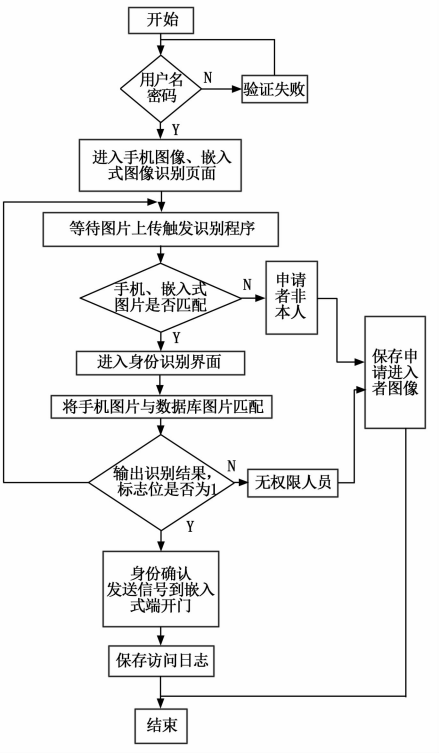


图 6　后台服务器软件流程图

管理人员打开软件输入用户名和密码，登录到手机图片和嵌入式端采集图像匹配识别界面[8]。设置触发程序，当有图片上传时，触发程序开始检测，当检测到手机端和嵌入式端都有图片时开始进行识别匹配，若只检测到一张图片，超过 60 s 后，程序自动开始下一循环，则本次请求无效。若两张图片识别结果不一致，保存到访问失败日志，若识别一致，则上传图像与数据库人脸匹配，这里的图像选用手机端上传的图片，若与数据库中某个人员相匹配，则发送信号到嵌入式端，打开门禁，并在界面上显示姓名职位，若没有与之匹配的人员信息，则保存到访问失败日志[9]。

界面设计包括登录界面、手机端上传图片与嵌入式端上传图片匹配识别界面以及手机端上传图片与数据库人脸匹配界面等。

## 4　实验测试结果

为验证系统所采用算法和所设计的各个程序的可靠性，本文对多个移动设备安装了 APP，在实验室环境下进行现场情况模拟，并且选取了 36 组实验数据，对各个子系统的性能分别进行全面测试。其中，除两组由于实验室光照条件等因素的影响未得以正确识别外，其余测试结果均为良好，正确识别率高达 94.4％。实际中，系统应用场景比较固定，因此光照等因素对系统性能的影响将会大大减小。图 7 是该系统部分测试效果图。

## 5　结束语

文章首先针对硬件部分进行设计，包括手机端、嵌入式端图像采集模块以及后台服务器端；其次针对各子系统进行软件

（下转第 231 页）