

一种联合检测门禁系统的设计与实现

孙科学^{1,2}, 洪 魁¹, 章康宁³, 王星稚³, 刘 康³

(1. 南京邮电大学 电子科学与工程学院, 江苏 南京 210023;

2. 江苏省射频集成与微组装工程实验室, 江苏 南京 210023;

3. 南京邮电大学 通信与信息工程学院, 江苏 南京 210023)

摘 要:门禁系统作为目前物联网中发展应用较为成熟的产品,与物联网行业的发展密切相关。现在市场上的门禁系统有基于射频识别、指纹识别、密码识别等方式,但单一识别方式较为容易破解。文中设计综合了语音识别、指纹识别、无线数传与 GSM 网络通讯的联合检测门禁系统,系统中由语音识别与指纹识别完成身份认证,无线传输负责系统内通信,GSM 网络通讯作为向外界报警手段。针对系统整体结构,关键技术的开发过程,系统工作流程做了详细介绍,并对系统的双重认证,无线数传分体式设计,加密通信方式等特点进行了总结。提出并设计实现了一种将语音识别、指纹识别相结合的复合认证门禁系统。

关键词:门禁系统;联合检测;语音识别;指纹识别

中图分类号:TP311.1

文献标识码:A

文章编号:1673-629X(2016)01-0155-05

doi:10.3969/j.issn.1673-629X.2016.01.033

Design and Implementation of Joint Detection Access Control System

SUN Ke-xue^{1,2}, HONG Kui¹, ZHANG Kang-ning³, WANG Xing-zhi³, LIU Kang³

(1. College of Electronics Science and Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210023, China;

2. Jiangsu Province Engineering Lab of RF Integration & Micropackage, Nanjing 210023, China;

3. College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Entrance guard system, as a mature product, is closely related to the development of the Internet of Things industry. Now the market includes entrance guard system based on RFID, fingerprint identification, password identification and so on, but the way is relatively easy to identify a single crack. The design proposes an integrated access control combined detection entrance guard system of speech recognition, fingerprint recognition, wireless data transmission and GSM network communications. In the system, the identity authentication is done by speech recognition and fingerprint recognition, a wireless transmission system is responsible for communication, GSM network alarms to the outside world as a means of communication. In view of the overall system structure and key technology development process, the system working process is introduced in detail, and the system of dual certification, wireless digital separation design, encryption communication characteristics are summarized. Present and design a dual authentication entrance guard system combined speech recognition and fingerprint recognition.

Key words: entrance guard systems; joint detection; voice recognition; fingerprint identification

0 引 言

随着当今电子技术,计算机软、硬件技术,通讯技术的快速发展,物联网成为继互联网之后又一新兴行业。目前世界各国已经开始重视物联网的建设,并做

了大量的技术研发和应用工作,使得物联网产业已经成为推动世界经济增长的重要新兴产业^[1]。门禁系统作为目前物联网中发展应用较为成熟的产品,更在一定程度上代表着物联网行业的发展。现在市场上的门

收稿日期:2015-03-29

修回日期:2015-07-01

网络出版时间:2015-11-19

基金项目:国家级大学生创新训练计划(SZDG2014002);南京邮电大学自然科学基金项目(NY214049)

作者简介:孙科学(1981-),男,副教授,研究方向为电子电路设计、嵌入式系统与通信软件设计;洪 魁(1989-),男,研究方向为电子科学与技术。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20151119.1113.072.html>

禁系统有基于射频识别、指纹识别、密码识别等方式,但单一识别方式较为容易破解。门禁系统的组成方式按设计原理分类又分为一体式与分体式。其中一体式由于控制器须安装在门外,所以部分控制线必须露在门外,则有可能会被人暴力破解。分体式中有部分需要连接如小区物业、公司安保等的后台服务器,适合用户群体大的场合,但不适合普通单户家庭。因此,一个多重识别、分体式、低成本的门禁系统是普通家庭安全的最佳选择。

语音识别是指机器通过学习实现从语音信号到文字符号的理解过程,是一种十分重要的人机交互方式^[2-4]。语音识别属于模式识别的一种,分为训练与识别两个过程。训练阶段,系统将人类的语言内容组成语音库存储起来。识别阶段,将人类输入的语言内容同语音库存储内容进行匹配,再将匹配的结果返回^[5-9]。

指纹识别技术是一项生物识别技术。1684 年,英国植物形态学者 Nehemiah Grew 发表了世界上指纹研究的第一篇论文,对指纹的谷线、脊线、汗腺孔的结构进行了系统的分析研究^[10]。自动指纹识别系统 (Au-

tomated Fingerprint Identification System, AFIS), 由于其安全性、可靠性及高效性,使得它在刑侦、信息安全、电子商务等众多领域有着广泛的应用前景^[11-14]。

文中设计并实现了一种集语音识别、指纹识别、无线数传与 GSM 网络通讯为一体的联合检测门禁系统。

1 系统整体设计

系统由前端门禁部分与后端报警部分组成。前端门禁部分通过凌阳 SPCE061A 语音识别模块与 FPM10A 指纹识别模块进行语音与指纹的双重认证,以确认访问者身份,然后通过 NRF905 在特定频段向后端特定地址发送加密报文。后端则根据报文及传感器综合判定访问者是否非法闯入。若非法,则通过 SIM900A 向指定号码发送警报信息,同时蜂鸣器响起,以震慑非法入侵者。若合法,则允许访问者通行,报警部分不作任何操作。基于两部分的无线分体式设计不仅提高了适用范围,也提高了安全系数。系统框图如图 1 所示。

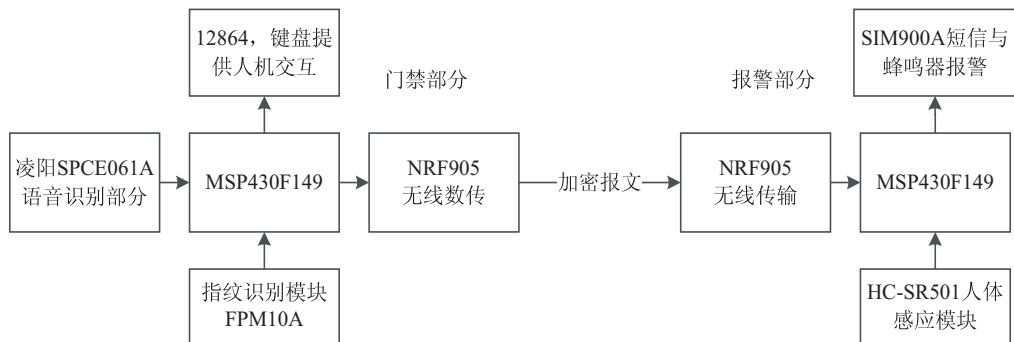


图 1 整体设计实现框图

系统工作过程中,德州仪器(TI)公司的MSP430F149作为系统主控芯片,负责各模块部分通信连接,语音识别使用的是凌阳公司的凌阳SPCE061A,指纹识别由FPM10A完成,无线数传模块选用了挪威NORDIC公司出品的NRF905,GSM网络通讯模块是SIMCom推出新款紧凑型产品—SIM900A,12864液晶屏幕作为人机交互模块,采用了德国原装进口LHI778探头的HC-SR501作为感应装置。

2 系统关键技术详细设计与实现

2.1 语音识别

系统设计中选用了凌阳 SPCE061A 模块来实现语音识别功能,该模块具有 32 768 Hz 的实时时钟以及音频编码 SACM_S240 方式(2.4 kbit/s),可容纳 210 s 语音数据,运行速度快,开发流程便捷。

2.1.1 语音识别功能软件设计

凌阳 SPCE061A 使用集成开发环境 IDE 开发,开发语言为 C 语言,其软件设计过程中需要经历语音命令模型库训练、语音识别、语音提示三个部分。

(1) 语音命令模型库训练时,语音输入采用 SPCE061A 系统通过 MIC 输入模块采集语言信号,然后将之生成模板保存于 SPCE061A 的 32K 字的 Flash 存储器中。文中设计的语音命令共有 5 个,分别是系统唤醒指令、开灯指令、关灯指令、开门指令以及关门指令。

这样既可以保证识别的正确率,也便于存储。同时,由于这五个指令并非是已存储过的固定指令,而是需要用户自由选择以后输入的语音口令,从而实现了语音口令的用户自定义化、动态化,更加提升了系统的安全性、可靠性。语音命令模型库训练流程图如图 2 所示。

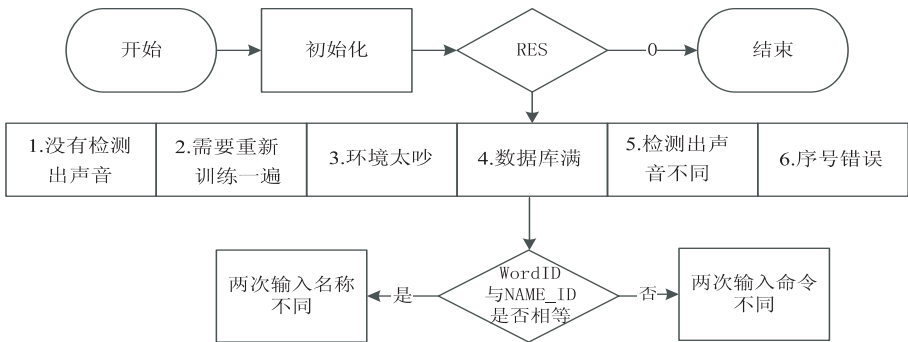


图2 语音命令模型库训练流程图

(2)语音识别和语音提示的程序设计时,首先识别器初始化,初始化完成后将会语音提示系统准备完成。然后,若 SPCE061A 检测到系统唤醒指令,则在向用户语音提示以后,检测输入的语音指令是否匹配之前训练存储的指令,若是,则执行相应命令,如开门、关门;若不是,或者未输入语音指令,则语音提示失败。在该部分设计中,语音提示输出可以使用凌阳公司为用户提供的编制的 API 函数。语音识别和提示软件流程如图3所示。

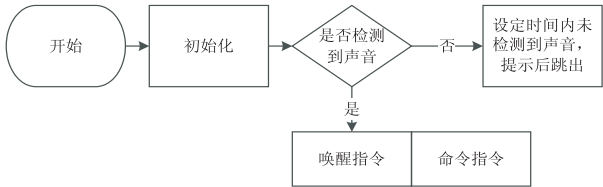


图3 语音识别和语音提示流程图

2.1.2 语音识别功能硬件设计

该设计中语音识别部分使用的是凌阳 SPCE061A 开发板,由 SPCE061A 控制喇叭可以实现语音提示功能,由 MIC 输入模块连接 SPCE061A 实现语音输入。语音识别完成后,SPCE061A 通过 IO 口与门禁部分主控芯片 MSP430F149 通信,返回语音识别的结果。

2.2 指纹识别功能软件设计

指纹识别软件设计中包含指纹的存储与指纹的匹配两个部分。在 IAR 开发环境下,首先新建了名为 FPM10A.h 的头文件,然后在该文件下写入诸如获得指纹图像,将图像转换成特征码存放在 Buffer1 中,将 Buffer1 跟 Buffer2 中的特征码合并成指纹模板等函数,最后在主函数 main.c 中调用函数,以实现相关功能。

而 MSP430F149 依靠 UART0 与 FPM10A 通信,波特率为 57 600 bps。MSP430F149 通过发送规定格式报文至 FPM10A 来控制 FPM10A 完成比对指纹模板、存储指纹模板到相应位置等操作。而 FPM10A 执行完操作后,将会返回包含诸如未识别到手指(手指未在传感器上放好),指纹匹配成功,指纹匹配失败等回文。其报文回文格式如下(以录指纹图像命令为例,其余命令类似):

报文中包头固定不变,模块地址可以自定义,文中设计的模块地址定义为 FF FF。包标识为 01 时,代表 MSP430F149 向 FPM10A 发送的请求命令报文,包标识为 07 时,代表 FPM10A 向 MSP430F149 返回的命令执行结果回文。包长度为包长度字节之后报文长度,包长度字节之后为指令码与校验和,两者合计 3 bytes。指令码为 MSP430F149 向 FPM10A 发送的指令,如 01 代表录指纹图像命令。校验和为模块地址字节之后,校验和字节之前的长度,其中包标识、包长度、指令码三者共计 5 bytes,因此校验和为 05H。确认码为 FPM10A 向 MSP430F149 返回的执行结果,当确认码为 00H,01H,02H,03H 时,分别代表录入成功,收包有错,传感器上无手指以及录入不成功。其他指令的报文格式与此相类似。

(1)指纹的存储过程中,首先 MSP430F149 控制 FPM10A 获得指纹图像,然后将图像转换成特征码存放在 Buffer1 中。为保证输入的准确,再一次获得指纹图像并将图像转换成特征码存放在 Buffer2 中。下一步将两个 Buffer 中的数据转换为指纹特征模板,最后按顺序存储于 FPM10A 中。指纹存储流程图见图4。

(2)指纹的匹配过程中,首先 MSP430F149 控制 FPM10A 获得指纹图像,然后将图像转换成特征码存放在 Buffer1 中,再将 Buffer1 中数据转换为指纹特征模板,然后搜索指纹库并返回结果。

2.3 无线数传

在系统中实现无线数传功能的是 NRF905,门禁部分发送,报警部分接收。软件设计时分别对应使用了 NRF905 的 ShockBurst TX 和 ShockBurst RX 工作模式。初始化时,设置工作频段为 430 MHz,输出功率 10 dB,地址宽度 4 字节,数据长度 32 字节,接收地址为 0xCC,0xCC,0xCC,0xCC,CRC8 位校验。

(1)ShockBurst TX 发送流程设计:首先按 NRF905 的 SPI 接口时序写入接收机地址和传输数据,然后置高 TRX_CE 和 TX_EN,启动 NRF905 的 ShockBurst TX 模式,从而完成数据的发送。数据包发送结束后,NRF905 自动进入空闲模式。

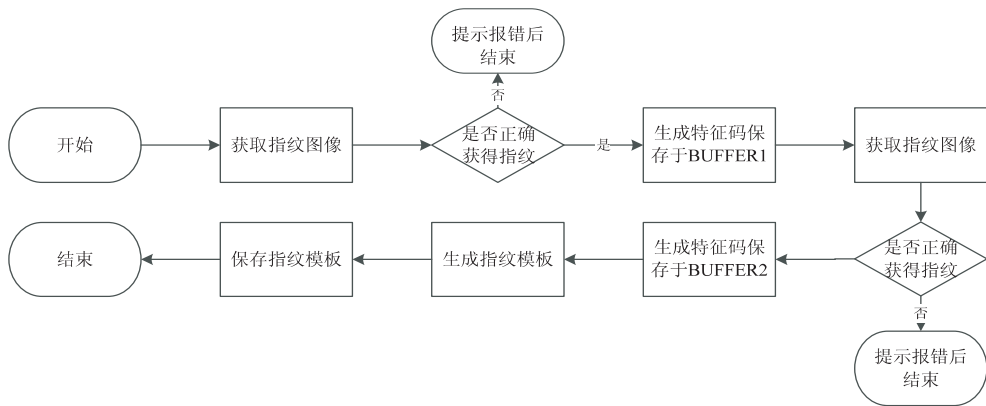


图 4 指纹存储流程图

(2) ShockBurst RX 接收流程设计: 首先置高 TRX_CE, 置低 TX_EN, 启动 ShockBurst RX 模式。650 μ s 后, NRF905 才可以正常接收数据, 注意此处由于 NRF905 启动 ShockBurst RX 模式有延迟, 所以门禁部分无线数传设计中, 系统开放校验码并非发送一次, 而是发送多次, 以此保证报警部分不会丢失门禁部分发送过来的校验码, 加强系统的可靠性。当检测到 430 MHz 频段载波, 且接收地址是 0xCC, 0xCC, 0xCC, 0xCC 时, 读出数据包, 此后 NRF905 进入空闲模式, NRF905 将数据包通过 SPI 接口传输至 MSP430F149 内。

2.4 GSM 网络通信软件设计

选用 SIM900A 来完成系统 GSM 网络通讯的功能。当报警系统判定非法闯入时, MSP430F149 通过 UART0 发送指令控制 SIM900A 向指定号码发送报警短信, 串口通信波特率为 9 600 bps。

硬件设计较为简洁, SIM900A 需要 12 V 供电, 与 MSP430F149 共地之后, 仅需要将 MSP430F149 的 UART0 与 SIM900A 的 TX 与 RX 对应连接即可。

软件设计中, 首先需要通过 AT+CSCS="GSM" 指令设置"GSM"字符集, 延时等待执行后, 设置文本模式, 再根据类似 AT+CMGS="139XXXX8612" 指令设置接收方号码, 此时可以输入短信内容以等待短信的发送, 最后发送 HEX 格式的 1A 启动短信发送流程。

3 系统的工作流程

系统开机以后, 门禁部分首先输入管理员指纹, 赋予权限以方便后期进入系统设置状态, 完成诸如添加访问者等操作, 然后进入门禁部分待机状态, 此时门禁部分默认关门。报警部分则直接进入待机状态, 此时报警部分默认关门。系统有四个状态, 分别是待机状态、系统设置状态、系统开放状态和系统关闭状态。

3.1 待机状态

待机状态时, 门禁部分实时检测语音识别成功标志位, 若失败, 则提示语音识别未完成, 返回待机状态; 若成功, 进入系统选择菜单, 此时可执行用户认证和增

加新用户操作, 相应可分别进入系统开放状态、系统关闭状态以及系统设置状态; 同时, 报警部分实时检测系统开放标志位, 若开放, 则报警部分停留在系统开放状态; 若关闭, 则报警部分系统进入系统关闭状态。

3.2 系统设置状态

系统从待机状态转换过来, 进入到系统选择菜单之后, 可以选择增加新用户操作, 从而进入系统设置状态。首先, 门禁部分验证管理员指纹以获得增加新用户操作的权限。如果管理员指纹验证失败, 提示管理员指纹匹配失败后返回系统选择菜单。如果管理员指纹验证成功, 则提示管理员指纹匹配成功, 并于 5 s 以后执行新用户指纹输入操作, 然后返回系统选择菜单, 系统设置过程结束, 跳出该过程; 在系统设置状态下, 报警部分处于待机状态中, 不执行其他任何操作。

3.3 系统开放状态

系统开始处于待机状态, 首先完成语音识别, 然后系统将从待机状态转换过来, 进入到系统选择菜单之后, 可以选择用户认证操作, 即指纹识别操作。若用户认证成功, 则进入系统开放状态, 此时门禁部分将通过 NRF905 在特定频率向特定地址发送特定的系统开放状态报文, 报警部分接收到该报文后将会进入系统开放状态, 从而用户通过门禁时虽然报警部分检测到有人进入, 但不会报警。系统开放状态流程如图 5 所示。

3.4 系统关闭状态

若语音识别未完成, 则系统处于待机状态, 出现非法通过情况将触发报警。若语音识别完成, 则系统从待机状态转换过来, 进入到系统选择菜单之后, 可以选择用户认证操作, 即指纹识别操作, 若用户认证失败, 则进入系统关闭状态。门禁部分将不会向报警部分发送任何报文, 从而非法访问者将不会获得诸如系统通信频率、收发地址、报文确认码等信息, 有效提高了系统的安全系数。此时若非法访问者闯入屋内, 报警部分将被触发, 蜂鸣器响起以威慑非法访问者, 同时 SIM900A 向特定号码报警。若非法访问者破坏门禁部分, 将不会影响报警部分工作, 从而大大提高系统整体

安全性。若非法访问者用户认证失败后不做下一步行动,门禁部分将返回待机状态。系统关闭状态流程如图6所示。

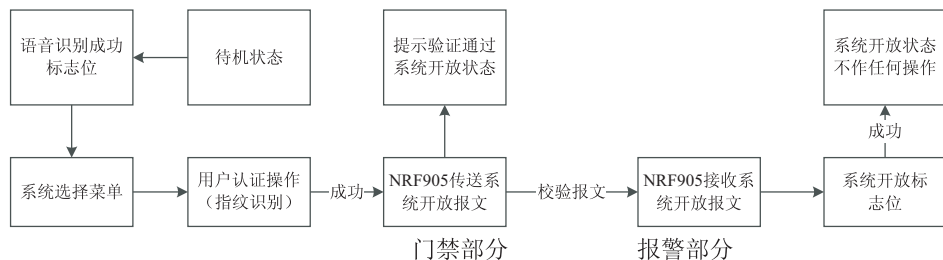


图5 系统开放状态流程图

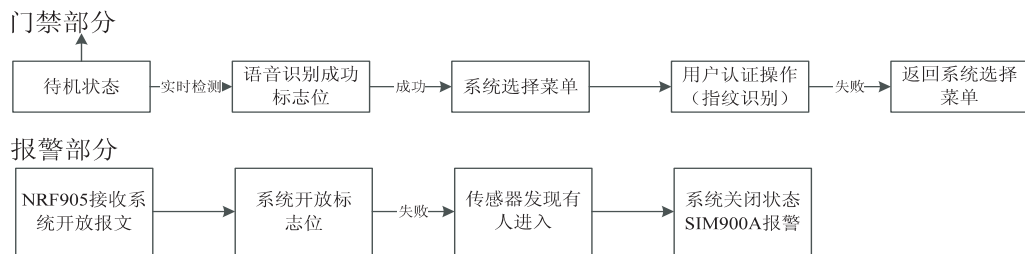


图6 系统关闭状态流程图

4 结束语

文中将语音识别技术和指纹识别技术相结合,提出并设计实现了一种将语音识别、指纹识别相结合的复合认证门禁系统。利用硬件电路实现,并通过测试和分析得出下面的结论:

(1)系统采用双重认证,先进行语音识别,再进行指纹识别。每一次认证都有它特有的识别方式和安全性,各种识别技术相互配合,极大地提高了系统的可靠性。

(2)引入了无线数传技术,使门禁系统中的门禁部分独立于报警部分,相似于“钥匙”与“锁”的关系,而且“锁”是访问者不能接触到的,“钥匙”则只识别特定访问者,从而大大增强了系统的安全性,避免了不法分子外部破坏门禁系统所带来的麻烦。

(3)文中设计是类似于“钥匙”与“锁”的设计,如果没有成功认证,则门禁部分不会向报警部分发送任何信息,且认证成功之后,门禁部分也将只发送足够报警部分识别的解锁报文,而不会一直发送。从而破解者将不会轻易获得诸如门禁部分与报警部分的通信频段、报警部分目标地址、加密报文内的验证码等信息,很大程度上提高了安全性。

参考文献:

- [1] 关勇. 物联网行业发展分析[D]. 北京:北京邮电大学, 2010.
- [2] 石现峰, 张学智, 张峰. 基于HTK的语音识别系统设计[J]. 计算机技术与发展, 2006, 16(10): 37-38.
- [3] 张雄伟, 陈亮, 杨吉斌. 现代语音处理技术及应用[M].


北京:机械工业出版社, 2003.

- [4] Tan Z H, Lindberg B. Advanced in pattern recognition-automatic speech recognition on mobile devices and over communication networks[M]. London: Springer-Verlog, 2008.
- [5] Itakura F. Minimum prediction residual principle applied to speech recognition[J]. IEEE Transactions on Acoustics, Speech and Signal Processing, 1975, 23(1): 67-72.
- [6] Hermansky H. Perceptual Linear Predictive (PLP) analysis of speech[J]. The Journal of the Acoustical Society of America, 1990, 87(4): 1738-1752.
- [7] Hermansky H, Morgan N. RASTA processing of speech[J]. IEEE Transactions on Speech and Audio Processing, 1994, 2(4): 578-589.
- [8] Haque S, Togneri R, Zaknich A. Perceptual features for automatic speech recognition in noisy environments[J]. Speech Communication, 2009, 51(1): 58-75.
- [9] Ishizuka K, Nakatani T. A feature extraction method using sub-band based periodicity and aperiodicity decomposition with noise robust frontend processing for automatic speech recognition[J]. Speech Communication, 2006, 48(11): 1447-1457.
- [10] Lee H C, Gaensslen R E. Advances in fingerprint technology[M]. 2nd ed. New York: Elsevier, 2001.
- [11] 张明, 吴陈, 陈楠. 基于方向滤波的指纹图像增强算法[J]. 微机发展(现更名: 计算机技术与发展), 2005, 15(6): 85-87.
- [12] 郭新星. 自动指纹识别系统关键技术研究[D]. 长沙: 中南大学, 2009.
- [13] 楼顺天, 施阳. 基于Matlab的图像处理[M]. 西安: 西安电子科技大学出版社, 2000.
- [14] 赵海峰. 嵌入式指纹识别系统设计——指纹传感器驱动程序研究[D]. 北京: 北京林业大学, 2009.

一种联合检测门禁系统的设计与实现

作者：[孙科学](#)，[洪樾](#)，[章康宁](#)，[王星稚](#)，[刘康](#)，[SUN Ke-xue](#)，[HONG Kui](#)，[ZHANG Kang-ning](#)，[WANG Xing-zhi](#)，[LIU Kang](#)

作者单位：[孙科学, SUN Ke-xue\(南京邮电大学 电子科学与工程学院, 江苏 南京 210023; 江苏省射频集成与微组装工程实验室, 江苏 南京 210023\)](#)，[洪樾, HONG Kui\(南京邮电大学 电子科学与工程学院, 江苏 南京, 210023\)](#)，[章康宁, 王星稚, 刘康, ZHANG Kang-ning, WANG Xing-zhi, LIU Kang\(南京邮电大学 通信与信息工程学院, 江苏 南京, 210023\)](#)

刊名：[计算机技术与发展](#)

英文刊名：

年，卷(期)：2016(1)

引用本文格式：[孙科学](#). [洪樾](#). [章康宁](#). [王星稚](#). [刘康](#). [SUN Ke-xue](#). [HONG Kui](#). [ZHANG Kang-ning](#). [WANG Xing-zhi](#). [LIU Kang](#) 一种联合检测门禁系统的设计与实现[期刊论文]-[计算机技术与发展](#) 2016(1)