

(12) 发明专利申请

(10) 申请公布号 CN 102968835 A

(43) 申请公布日 2013. 03. 13

(21) 申请号 201210462697. 5

(22) 申请日 2012. 11. 16

(71) 申请人 中国舰船研究设计中心

地址 430064 湖北省武汉市武昌区紫阳路
268 号

(72) 发明人 闵绍荣 李明辉

(74) 专利代理机构 湖北武汉永嘉专利代理有限
公司 42102

代理人 胡建平

(51) Int. Cl.

G07C 9/00(2006. 01)

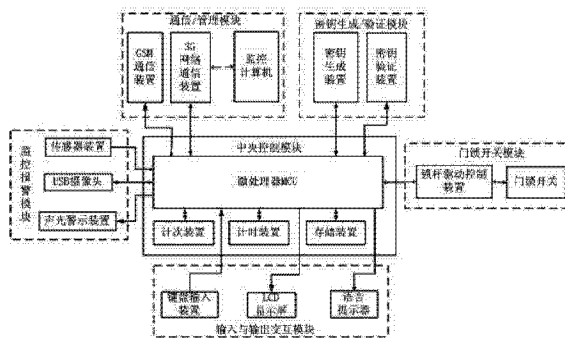
权利要求书 1 页 说明书 8 页 附图 6 页

(54) 发明名称

一种大容量远程授权数字门锁管控系统

(57) 摘要

本发明涉及一种大容量远程授权数字门锁监控系统,该系统包括:中央控制模块,用于生成并发送系统控制信息;通信/管理模块,用于无线、网络通信以及系统管理设置;密钥生成/验证模块,用于加密生成随机动态密钥,以及验证房客输入的房门密钥;门锁开关模块,用于在房客密钥验证合法后开启门锁;监控报警模块,当检测到异常情况时,进行报警和视频监控;输入与输出交互模块,用于数据输入和显示系统提示信息。本发明应用于大容量房门授权管理领域,通过无线网络通信、动态随机密钥生成和以及多种防盗监控报警措施,可快速实现远程门锁授权管理与控制,同时提高了房门的防盗性和安全性。



1. 一种大容量远程授权数字门锁监控系统,其特征在于:包括:中央控制模块,用于生成并发送系统控制信息;通信/管理模块,用于无线、网络通信以及系统管理设置;密钥生成/验证模块,用于加密生成随机动态密钥,以及验证房客输入的房门密钥;门锁开关模块,用于在房客密钥验证合法后开启门锁;监控报警模块,当检测到异常情况时,进行报警和视频监控;输入与输出交互模块,用于数据输入和显示系统提示信息。

2. 如权利要求1所述的监控系统,其特征在于:所述中央控制模块包括微处理器MCU、计时装置、计次装置和存储装置;所述的微处理器MCU,负责对通信/管理模块、密钥生成/验证模块、门锁开关模块、监控报警模块和输入与输出交互模块的逻辑控制;所述的计次装置与微处理器MCU信号连接,用于记录房客输入密钥时的错误次数;所述的计时装置,用于记录发送随机动态密钥后所经过的时间;所述的存储装置与微处理器MCU相连接,用于存储系统管理信息以及监控信息。

3. 如权利要求2所述的监控系统,其特征在于:所述微处理器MCU为ARM嵌入式微处理器。

4. 如权利要求2所述的监控系统,其特征在于:所述通信/管理模块包括:GSM通信装置、3G网络通信装置和监控计算机;所述的GSM通信装置与中央控制模块的微处理器MCU相连接,用于系统与管理员的移动通信终端进行无线通信;所述3G网络通信装置与微处理器MCU相连接,用于将管理/记录/监控数据封装,传输到监控计算机端,同时接收管理员控制指令;所述的监控计算机,由无线接收发送终端、数据接收发布网站、数据库组成,用于Web服务器接收数据、发布监控信息、管理/控制门锁系统设置。

5. 如权利要求1所述的监控系统,其特征在于:所述密钥生成/验证模块包括:随机密钥生成装置和密钥验证装置,所述的随机密钥生成装置,通过加密算法计算生成随机动态密钥;所述的密码验证装置,通过对应的解密算法计算生成验证密码,验证房客输入的密钥是否正确。

6. 如权利要求1所述的监控系统,其特征在于:所述门锁开关模块包括:锁杆驱动控制装置和门锁开关装置。

7. 如权利要求2所述的监控系统,其特征在于:所述监控报警模块包括:传感器装置、USB摄像头、声光警示装置;所述传感器装置与微处理器MCU信号连接,用于监测非法操作并将报警信号传至中央控制模块;所述USB摄像头与中央控制模块连接,用于报警信号存在时记录视频信息;所述的声光警示装置通过I/O连接与微处理器MCU连接,用于发出报警信息。

8. 如权利要求1所述的监控系统,其特征在于:所述输入与输出交互模块,包括键盘输入装置、LCD显示屏和语音提示器。

一种大容量远程授权数字门锁管控系统

技术领域

[0001] 本发明涉及一种监控系统,特别是一种大容量远程授权数字门锁管控系统。

背景技术

[0002] 随着因特网技术与无线通信技术的发展,对于那些门锁众多且异地分布辽阔的应用场合,如全国连锁酒店/宾馆、军队营房/仓库、大学城宿舍、异地连锁出租公寓等,它们都具有一些共同的特点,即房间众多、分布广、房间使用者具有流动性和变换性。同时它们都存在共同的不足,即不能支持基于电子商务支付/预订和远程直接授权使用。目前的预订方式仅支持远程电话/网络预订,但仍需要住房者当面向柜台员办理支付和领取钥匙。同时房主也无法异地远程对房门进行数字钥匙授权和结束授权。为了解决上述问题,本发明是提供一种大容量远程授权数字门锁管控系统。

[0003] 本发明还可以应用于某些军事领域,例如美国航空母舰有 3000 多个舱室,而舰员是不断更换的,普通的房门钥匙管理手段是很难胜任的。又例如大型军营的营房管理控制等。

发明内容

[0004] 为了解决现有技术存在的问题,本发明提供了一种大容量远程授权数字门锁管控系统,能够实现远程门锁的管理控制。

[0005] 本发明的技术方案为:一种大容量远程授权数字门锁监控系统,包括:中央控制模块,用于生成并发送系统控制信息;通信/管理模块,用于无线、网络通信以及系统管理设置;密钥生成/验证模块,用于加密生成随机动态密钥,以及验证房客输入的房门密钥;门锁开关模块,用于在房客密钥验证合法后开启门锁;监控报警模块,当检测到异常情况时,进行报警和视频监控;输入与输出交互模块,用于数据输入和显示系统提示信息。

[0006] 按上述方案,所述中央控制模块包括微处理器 MCU、计时装置、计次装置和存储装置。

[0007] 所述的微处理器 MCU,负责对通信/管理模块、密钥生成/验证模块、门锁开关模块、监控报警模块和输入与输出交互模块的逻辑控制。

[0008] 按上述方案,根据本系统涉及到的数据处理和逻辑控制要求,所述微处理器 MCU 优先选用 ARM 嵌入式微处理器。

[0009] 所述的计次装置与微处理器 MCU 信号连接,用于记录房客输入密钥时的错误次数。若记录的错误次数大于程序设定值,则向中央控制模块发出信号,暂停密钥验证并进行语音提示。

[0010] 所述的计时装置,用于记录发送随机动态密钥后所经过的时间。如果记录时间超过程序设置的密钥生存周期,则原生成的密钥则会被判定无效。

[0011] 所述的存储装置与微处理器 MCU 相连接,用于存储系统管理信息以及监控信息。所述的系统管理信息包括房主指定的电话号码、身份验证码、短信发送次数、短信发送频率

等,所述的监控信息包括视频监控信息、房客出入信息、报警监控信息。

[0012] 按上述方案,所述通信/管理模块包括:GSM 通信装置、3G 网络通信装置和监控计算机。其中 GSM 通信装置,通过 RS232 串口与中央控制模块的微处理器 MCU 相连接,用于系统与管理员的移动通信终端进行无线通信。管理员可通过 GSM 通信向系统发送指令,获取房门密钥、监控信息以及进行系统管理设置,对应的,GSM 通信装置向管理员返回其所需的信息。

[0013] 所述的 3G 网络通信装置,通过串行通信接口与微处理器 MCU 相连接,负责将管理/记录/监控数据按照通信协议封装,通过无线网络方式传输到监控计算机端,同时接收管理员控制指令,对系统进行管理/控制。

[0014] 按上述方案,所述的 3G 网络通信装置支持 TD-SCDMA、WCDMA 和 CDMA2000 标准,串行通信接口采用 RS232 接口或 UART 接口,逻辑接口均定义为双工串行通信。所述的监控信息包括视频监控信息、房客出入信息以及报警信息。

[0015] 所述的监控计算机,由无线接收发送终端、数据接收发布网站、数据库组成,用于 Web 服务器接收数据、发布监控信息、管理/控制门锁系统设置。所述的无线接收发送终端接收 3G 网络通信装置发送的监控信息,通过数据接收发布网站解析处理,并存储于数据库中,以网页形式发布监控信息。房主可以以管理员的身份授权登录,浏览监控信息,发送控制指令,以获取房门密钥和进行系统设置。所述的无线接收发送终端采用与 3G 网络传输装置相对应的通信接口协议,使用串行数据电缆与 PC 机服务器连接,串行数据电缆接口采用 UART/RS232 接口或 USB 接口,所述的数据库包括 XML 数据库和 SQL 数据库,XML 数据库存储最新接收的监控数据,并覆盖旧数据,提高网页实时刷新效率;同时将接收到的新监控数据存储于 SQL 数据库,用于历史记录查询。

[0016] 按上述方案,所述密钥生成/验证模块包括:随机密钥生成装置和密钥验证装置。所述的随机密钥生成装置,通过加密算法计算生成随机动态密钥;所述的密码验证装置,通过对应的解密算法计算生成验证密码,验证房客输入的密钥是否正确。

[0017] 上述随机动态密钥可为 20 位数字/符号编码,加密算法可为 AES(高级加密标准)、DES(数据加密标准)、MD5 等国际标准中的一种。所述加密算法和解密算法是分别固化在随机密钥生成装置和密码验证装置上的,只可以读取,不能拷贝,并采用防盗用技术,即当有非法用户试图复制加解密算法时,则加解密算法自动被擦除。

[0018] 按上述方案,所述门锁开关模块包括:锁杆驱动控制装置和门锁开关装置,锁杆驱动控制装置用于房客密钥验证合法后将锁杆驱动至缩进位置,将门打开。锁杆驱动控制装置可为各种已知的机制驱动装置,如齿轮驱动、电机驱动等。门锁开关装置,用于开关门锁,其锁杆与锁杆驱动控制装置相连接。

[0019] 按上述方案,所述监控报警模块包括:传感器装置、USB 摄像头、声光警示装置。

[0020] 所述的传感器装置,包括压力传感器、震动传感器、冲击传感器、倾斜传感器,通过 I/O 接口与微处理器 MCU 信号连接,用于遭遇强行开锁,如撬门、撞门等非法操作时,将报警信号传至中央控制模块。

[0021] 所述的 USB 摄像头,通过 USB 接口与微处理器 MCU 相连接,具有红外夜视功能,在黑暗环境下仍可进行图像采集工作。所述的 USB 摄像头只在房客开启房门、检测到报警信号时工作。所述的 USB 摄像头内部集成了 CMOS 光学感应器件和基于 DSP 的图像预处理模

块,能够实现图像滤波等预处理功能,采集到的视频以 YUV420 的采样格式经过微处理器 MCU 的控制,经过压缩编码处理,存储于存储装置,并通过 3G 网络通信装置,进行数据封装,发送至监控计算机端。

[0022] 所述的声光警示装置通过 I/O 连接与微处理器 MCU 连接,由专用警示灯、扬声器、驱动电路组成。中央控制模块的控制信号经过驱动电路,转化为音频、光电信号输出,推动警示灯频繁闪烁、扬声器鸣叫,起到告警防盗的作用。

[0023] 按上述方案,所述输入与输出交互模块,包括键盘输入装置、LCD 显示屏、语音提示器。

[0024] 所述的键盘输入装置,通过 I/O 接口与微处理器 MCU 相连接,用于房客输入管理员所告知的房门密钥;

所述的 LCD 显示屏,通过 LCD 显示接口与微处理器 MCU 相连接,用于显示系统提示信息;

所述的语音提示器,通过音频输出接口与微处理器 MCU 相连接,用于语音提示系统信息。

[0025] 所述各个模块中的装置均采用一总电源供电,以提供所需的电源需求,如微处理器 MCU 3.3V/5V,传感器装置 3.3V,USB 摄像头 5V 等。

[0026] 与现有技术相比,本发明具有以下有益效果:

(1) 本发明使用无线通信和可变密钥技术,管理员可远程通过 GSM 通信(如手机)或 3G 网络两种通信方式获取房门的随机动态密钥,根据房客的住房时间,设置密钥的生存周期,此外可远程控制门锁的打开/关闭,记录房客的出入信息、设置房主管理信息等,实现了大容量远程房门数字化授权管理。

[0027] (2) 本发明使用 USB 摄像头和多种传感器作为监控工具,当有异常状况发生时,系统能够利用短信、电话等方式,向管理员报警,同时将房门监控信息通过无线网络方式传输到监控计算机端,管理员可以通过手机,PDA 或者联网的 PC 等各种网络终端设备,随时随地观看监控场景。当有重大案件发生时,监控信息可以作为犯罪证据。

[0028] (3) 本发明使用 3G 无线网络作为网络数据传输信道,相比其它 2G 无线传输方式(GPRS、CDMA 等),覆盖范围更广,传输速度更快,同时系统在没有异常发生时不进行录像、监控信息传输,且对监控视频进行了压缩编码处理,网络传输流量小,节省了成本和功耗。

[0029] (4) 本发明支持大容量、异地远程房门控制授权管理,能应用于全国连锁酒店/宾馆、异地连锁租赁公司、大学城宿舍管理、部队营房、航空母舰舱室等多种行业领域,具有良好的发展前景。

附图说明

[0030] 1. 图 1 是本发明一个实施例的系统结构示意图。

[0031] 2. 图 2 是本发明一个实施例的无线数据通信示意图。

[0032] 3. 图 3 为本发明一个实施例的 GSM 通信控制流程图。

[0033] 4. 图 4 为本发明一个实施例的门锁开关控制流程图。

[0034] 5. 图 5 为本发明一个实施例的监控报警控制流程图。

[0035] 6. 图 6 为本发明一个实施例的 3G 网络通信控制流程图。

[0036] 7. 图 7 为本发明一个实施例的监控计算机控制流程图。

具体实施方式

[0037] 下面结合附图对本发明做进一步阐述和说明：

如图 1 所示,本发明是一种大容量远程授权数字门锁监控系统,主要包括六个组成模块:通信/管理模块、密钥生成/验证模块、门锁开关模块、中央控制模块、监控报警模块以及输入与输出交互模块。

[0038] 其中,中央控制模块,用于生成并发送系统控制信息;中央控制模块包括微处理器 MCU、计时装置、计次装置和存储装置;所述的微处理器 MCU,负责对通信/管理模块、密钥生成/验证模块、门锁开关模块、监控报警模块和输入与输出交互模块的逻辑控制;所述的计次装置与微处理器 MCU 信号连接,用于记录房客输入密钥时的错误次数;所述的计时装置,用于记录发送随机动态密钥后所经过的时间;所述的存储装置与微处理器 MCU 相连接,用于存储系统管理信息以及监控信息。

[0039] 所述的微处理器 MCU,负责对其它模块的逻辑控制。根据本系统涉及到的数据处理和逻辑控制要求,优先选用 ARM 嵌入式微处理器作为系统的处理单元,在图像处理、数据传输等方面具有很好的性能,并支持多种外围设备和网络协议栈,间接的降低了开发难度。

[0040] 所述的计次装置与微处理器 MCU 信号连接,用于记录房客输入密钥时的错误次数,若记录的错误次数大于程序设定值(如 3 次),则向中央控制模块发出信号,暂停密钥验证并进行语音提示。

[0041] 所述的计时装置,用于记录发送随机动态密钥后所经过的时间,如果记录时间超过程序设置的密钥生存周期(如 20 天),则原生成的密钥则会被判定无效;所述的密钥生存周期可根据房客的住房时间进行设置,如房客需要居住 35 天并得到了管理者的授权,密钥生存周期则设置为 35 天,过期后原房间密钥被判定为无效,房客也就失去了进入房门的资格。

[0042] 所述的存储装置采用廉价大容量的 SD 卡作为外围存储设备,通过 SD/MMC 卡接口与微处理器 MCU 相连接,用于存储系统管理信息以及监控信息。所述的系统管理信息包括房主指定的电话号码、身份验证码、短信发送次数、短信发送频率等;所述的监控信息包括视频监控信息、房客出入信息、报警监控信息。

[0043] 通信/管理模块包括:GSM 通信装置、3G 网络通信装置和监控计算机。用于无线、网络通信以及系统管理设置。

[0044] 所述的 GSM 通信装置,通过 RS232 串口与中央控制模块的微处理器 MCU 相连接,用于系统与管理员的移动通信终端(如手机、PDA 等)进行无线通信。管理员可通过 GSM 通信向系统发送指令,获取房门密钥、监控信息以及进行系统管理设置,对应的,GSM 通信装置向管理员返回其所需的信息。

[0045] 所述的 3G 网络通信装置,通过串行通信接口与微处理器 MCU 相连接,负责将管理/记录/监控数据按照通信协议封装,通过无线网络方式传输到监控计算机端,同时接收管理员控制指令,对系统进行管理/控制。所述的 3G 网络通信装置支持 TD-SCDMA、WCDMA 和 CDMA2000 标准,串行通信接口采用 RS232 接口或 UART 接口,逻辑接口均定义为双工串行通信。所述的监控信息包括视频监控信息、房客出入信息以及报警信息。

[0046] 所述的监控计算机,由无线接收发送终端、数据接收发布网站、数据库组成,作为 Web 服务器接收数据、发布监控信息、管理 / 控制门锁系统。所述的无线接收发送终端接收 3G 网络通信装置发送的监控信息,通过数据接收发布网站解析处理,并存储于 XML 数据库和 SQL 数据库中,以网页形式发布监控信息。房主可以以管理员的身份授权登录,浏览监控信息,发送控制指令,以获取房门密钥和进行系统设置。所述的无线接收发送终端采用与 3G 网络传输装置相对应的通信接口协议,使用串行数据电缆与 PC 机服务器连接,串行数据电缆接口采用 UART/RS232 接口或 USB 接口,所述的数据库包括 XML 数据库和 SQL 数据库,XML 数据库存储最新接收的监控数据,并覆盖旧数据,提高网页实时刷新效率;同时将接收到的新监控数据存储于 SQL 数据库,用于历史记录查询。

[0047] 密钥生成 / 验证模块包括:随机密钥生成装置和密钥验证装置,用于加密生成随机动态密钥,以及验证房客输入的房门密钥。

[0048] 所述的随机密钥生成装置,通过加密算法计算生成随机动态密钥(20 位数字 / 符号编码);所述的密码验证装置,通过对应的解密算法计算生成验证密码,验证房客输入的密钥是否正确。所述的加密算法可为 AES (高级加密标准)、DES (数据加密标准)、MD5 等国际标准中的一种。所述加密算法和解密算法是分别固化在随机密钥生成装置和密码验证装置上的,只可以读取,不能拷贝,并采用防盗用技术,即当有非法用户试图复制加解密算法时,则加解密算法自动被擦除。

[0049] 门锁开关模块包括:锁杆驱动控制装置和门锁开关装置,用于在房客密钥验证合法后开启门锁。

[0050] 具体来说,锁杆驱动控制装置,用于房客密钥验证合法后将锁杆驱动至缩进位置,将门打开,锁杆驱动控制装置可为各种已知的机制驱动装置,如齿轮驱动、电机驱动等;门锁开关装置,其锁杆与锁杆驱动控制装置相连接。

[0051] 监控报警模块包括:传感器装置、USB 摄像头、声光警示装置,当检测到异常情况时,进行报警和视频监控;

所述的传感器装置,包括压力传感器、震动传感器、冲击传感器、倾斜传感器,通过 I/O 接口与微处理器 MCU 信号连接,用于遭遇强行开锁,如撬门、撞门等非法操作时,将报警信号传至中央控制模块。

[0052] 所述的 USB 摄像头,通过 USB 接口与微处理器 MCU 相连接,具有红外夜视功能,在黑暗环境下仍可进行图像采集工作。所述的 USB 摄像头只在房客开启房门、检测到报警信号时工作。所述的 USB 摄像头内部集成了 CMOS 光学感应器件和基于 DSP 的图像预处理模块,能够实现图像滤波等预处理功能,采集到的视频以 YUV420 的采样格式经过微处理器 MCU 的控制,经过压缩编码处理,存储于存储装置,并通过 3G 网络通信装置,进行数据封装,发送至监控计算机端。

[0053] 所述的声光警示装置通过 I/O 连接与微处理器 MCU,由专用警示灯、扬声器、驱动电路组成。中央控制模块的控制信号经过驱动电路,转化为音频、光电信号输出,推动警示灯频繁闪烁、扬声器鸣叫,起到告警防盗的作用。

[0054] 输入与输出交互模块包括键盘输入装置、LCD 显示屏和语音提示器,用于数据输入和显示系统提示信息。

[0055] 所述的键盘输入装置,通过 I/O 接口与微处理器 MCU 相连接,用于房客输入管理员

所告知的房门密钥；

所述的 LCD 显示屏,通过 LCD 显示接口与微处理器 MCU 相连接,用于显示系统提示信息；

所述的语音提示器,通过音频输出接口与微处理器 MCU 相连接,用于语音提示系统信息。

[0056] 以上各个模块中的装置均采用一总电源供电,以提供所需的电源需求,如微处理器 MCU 3.3V/5V,传感器装置 3.3V,USB 摄像头 5V 等。

[0057] 如图 2 和图 1 所示,管理员可通过移动通信设备(如手机、PDA 等)或互连网络发送无线指令获取房门密钥,系统 GSM 通信装置 /3G 网络通信装置接收指令并传至中央控制模块,控制密钥生成装置加密生成随机动态密钥,通过对应通信方式返回给管理员,进一步地,房主可设置密钥生存周期;当房客输入房门密钥时,USB 摄像头工作,微处理器 MCU 对接收的视频压缩 / 编码 / 存储,通过 3G 网络通信装置传输至监控计算机端,同时密钥验证装置对输入密钥进行验证,若正确则控制锁杆驱动装置开启门锁;当传感器装置检测到异常情况时,向微处理器 MCU 发出报警信号,在中央控制模块控制下,开启声光报警,摄像头开始录像、视频处理、网络传输,同时通过 GSM 通信向远程管理者发送报警提示;监控计算机端通过无线接收发送终端接收监控数据,并存储于 XML 和 SQL 数据库中,以网页形式发布监控信息,管理员可随时随地登录查看管控记录;此外,管理员可通过两种通信方式发送指令,控制系统或进行系统设置。

[0058] 如图 3 所示,本发明的 GSM 通信控制流程包括以下步骤:

(1) 判断是否接收到房主发送的无线指令,若是则进行房主身份验证,身份验证的内容包括房主指定的通信号码(如手机号码)以及房主的身份验证码,该信息均可在系统设置中进行修改。若身份验证正确,则进行指令分析,指令分析的结果有以下三种:①获取房门密钥 ②获取监控信息 ③系统管理设置。

[0059] (2) 若指令分析为获取房门密钥,则向密钥生成装置发出控制指令,使用加密算法生成随机动态密钥,并通过 GSM 通信装置返回该密钥,同时根据房主设置的密钥生成周期,控制计时装置开始计时。

[0060] (3) 若指令分析为获取监控信息,则读取中央控制模块的存储装置,通过 GSM 通信无线发送至房主移动通信终端。所述的存储装置存储信息包括:房主身份信息、系统设置信息、房客出入信息、视频监控信息以及报警记录信息。

[0061] (4) 若指令分析为系统管理设置,则分别进行房主身份设置、通信设置、房间信息设置,房主身份设置包括房主身份验证码、房主移动通信号码;通信设置包括短信发送次数、短信发送频率、电话拨打次数;房间信息设置包括房门编号、地理位置、房客信息。

[0062] (5) 指令分析完成后,将通信内容以及系统设置内容存储到存储装置中,方便日后查询,然后等待下一次循环。

[0063] 如图 4 所示,本发明的门锁开关控制流程包括以下步骤:

(1) 检测键盘输入装置,是否有密钥输入,若有则进入到步骤(2),否则返回继续检测等待。

[0064] (2) 控制打开 USB 摄像头,开始视频监控,依次对采集到的视频进行压缩编码、存储、3G 网络传输。所使用的压缩算法为 H.264 视频压缩算法,监控视频经网络传输至监控计

计算机端。

(3) 查询计时装置,检测房门密钥是否到期,若是则进行语音、文字提示(如“您的房门密钥已过期,请输入新密钥,或与房主联系”),然后返回等待新密钥输入;若否则进入下一步骤。

[0065] (4) 密钥验证装置对输入密钥进行验证,若正确则控制锁杆驱动装置,将房门打开,进入下一个步骤;若否,则先进行语音、文字提示(如“房门密钥输入错误,您还有 X 次机会重新输入新密钥”),然后判断验证次数是否超过阈值,若是则暂停密钥验证,进入步骤(5),若否则返回等待新密钥输入。

[0066] (5) 关闭摄像头,记录本次开门信息,并通过 3G 网络传输至监控计算机端。

[0067] 如图 5 所示,本发明的监控报警控制流程包括以下步骤:

(1) 检测传感器装置与微处理器相连的 I/O 端口有没有输入信号,若有则进入下一步骤,若无则返回等待报警信号输入。

[0068] (2) 打开摄像头开始视频监控,采集到的视频经过压缩编码、本地存储,利用 3G 网络传输至监控计算机端;同时控制声光传感装置进行声光报警;另一方面,向系统设置的房主通信号码发送短信、拨打电话,予以告警提示。

[0069] (3) 判断是否停止报警措施,若无报警信号输入,且报警措施设置的时间已到(如声光警示时间为 3 分钟、短信发送次数为 3 次),则关闭摄像头,停止声光报警,并记录本次报警信息,经 3G 网络传输至监控计算机端。最后返回等待下一次报警信号输入。

[0070] 如图 6 所示,本发明的 3G 网络通信控制流程包括以下步骤:

(1) 模块初始化,包括服务器 IP 地址设置、串口端口设置、波特率设置等,接着采用 PPP 协议与移动运行商建立连接,然后采用 TCP/IP 协议与监控计算机连接,若连接成功,则分别进行实时监听串口数据(步骤 2)、监听接收指令(步骤 3),否则继续连接。

[0071] (2) 实时监听串口数据:若串口接收到中央控制模块传递的数据,则按照通信协议对数据进行 TCP 封装,无线发送至监控计算机端;若串口没有接收到数据,则继续等待;若串口数据成功发送至监控计算机端,则返回等待下一次串口数据输入。

[0072] (3) 监听接收指令:若接收到管理员发送的指令,则首先进行指令分析,分析的结果包括:获取房门密钥与进行系统设置。根据分析结果分别处理,处理步骤如图 3 所分析,这里不再赘述。指令分析处理完毕后,返回等待新的指令消息。

[0073] 如图 7 所示,本发明的监控计算机控制流程包括以下步骤:

(1) 监控计算机端的无线接收发送终端,通过串行通信接口与 PC 服务器相连,因此首先进行串口初始化,包括串行端口、数据传输波特率、数据校验位设置等,然后与 3G 通信网络装置建立连接,若连接成功,则分别进入到监听接收数据(步骤 2)、监听发送数据(步骤 3),否则重新建立连接。

[0074] (2) 监听接收数据:若有串口数据输入,首先根据数据传输格式,判断数据是否合法,若合法则按照通信协议解析数据,将监控数据分别存储于 XML 数据库和 SQL 数据库,并以网页的形式发布监控信息,房主可以以管理员的身份,通过互联网进行登录访问,查看房门的监控信息;若接收到的串口数据判断为非法,则丢弃该数据,返回等待下一次串口数据输入。

[0075] (3) 监听发送数据:若管理员需要通过 3G 网络发送指令获取房门密钥和进行系统

设置管理,首先判断串口是否有指令数据发出,若有则按照通信协议进行数据封装、发送,否则等待串口数据输出。

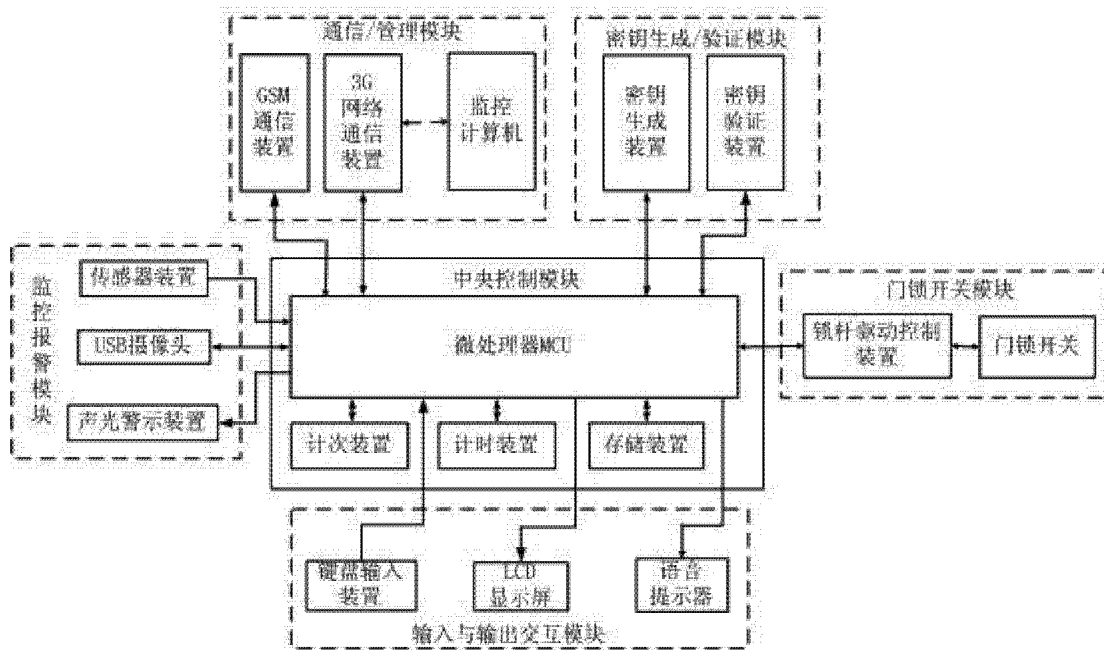


图 1

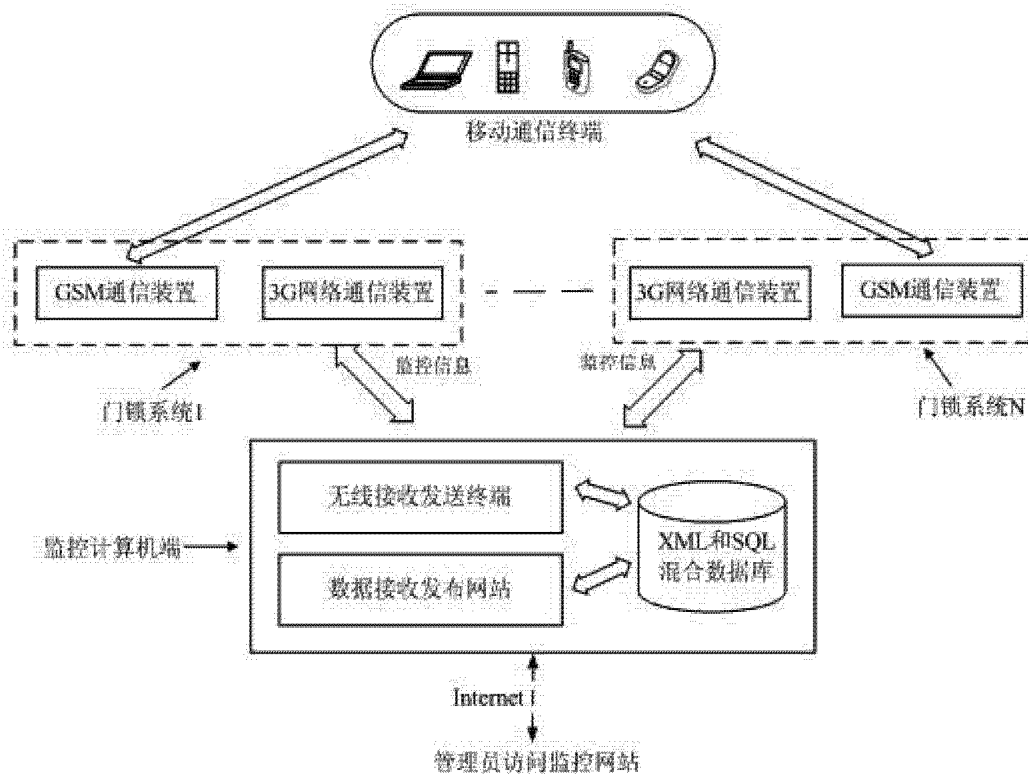


图 2

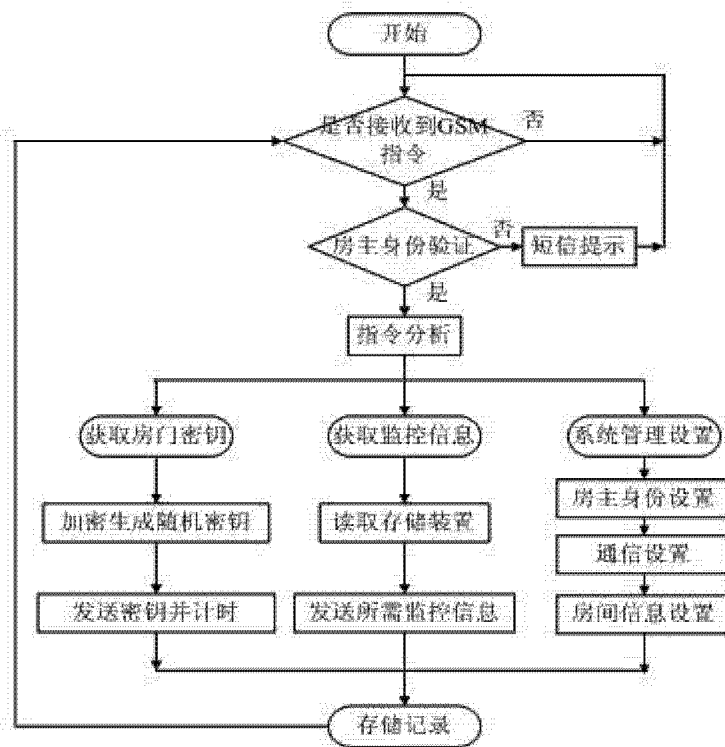


图 3

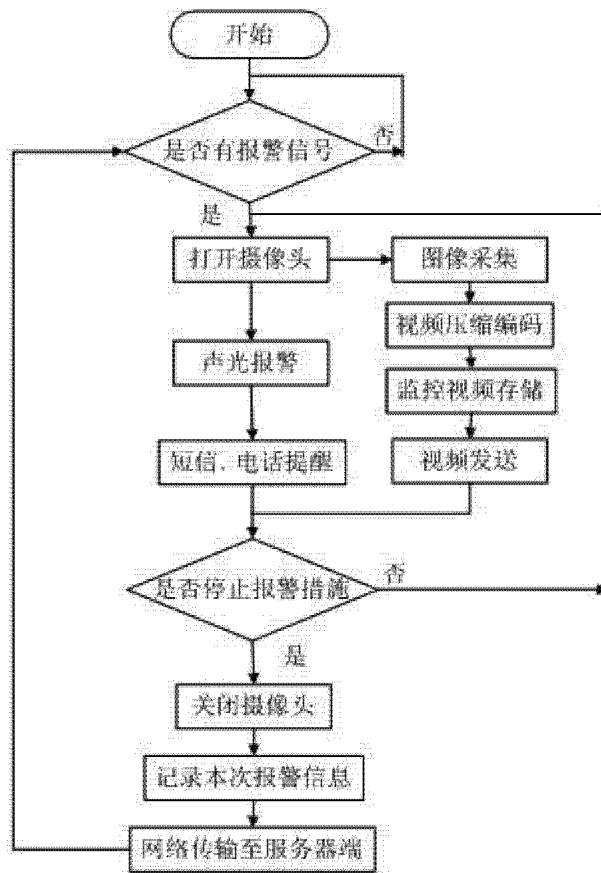


图 4

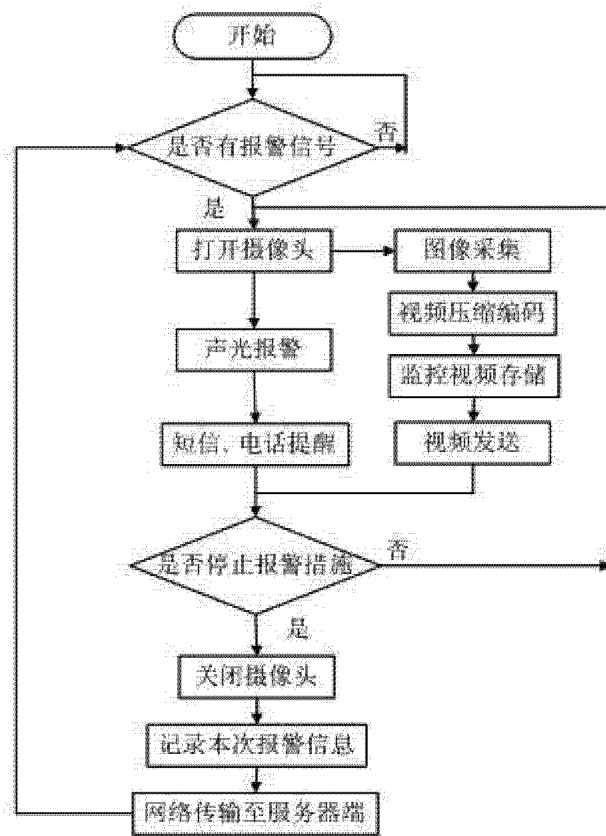


图 5

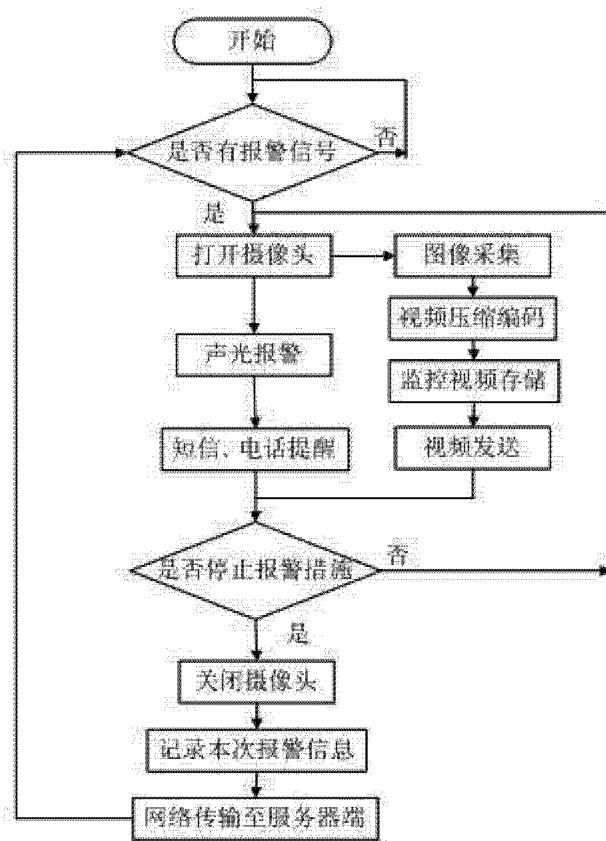


图 6

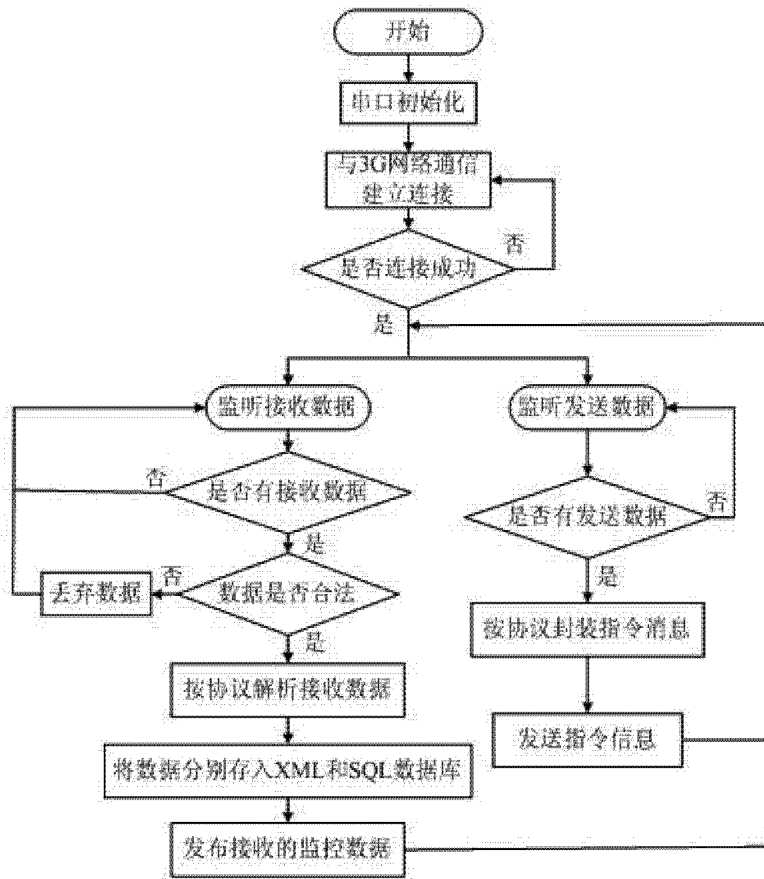


图 7