



(12)发明专利申请

(10)申请公布号 CN 108765825 A

(43)申请公布日 2018. 11. 06

(21)申请号 201810526773.1

(22)申请日 2018.05.28

(71)申请人 深圳市零度智控科技有限公司

地址 518000 广东省深圳市罗湖区东门街  
道湖贝路华佳广场7楼DG760

(72)发明人 郭立

(74)专利代理机构 深圳市港湾知识产权代理有  
限公司 44258

代理人 微嘉

(51) Int. Cl.

G08B 13/196(2006.01)

G08B 21/24(2006.01)

G08B 25/01(2006.01)

G06K 9/00(2006.01)

权利要求书2页 说明书11页 附图3页

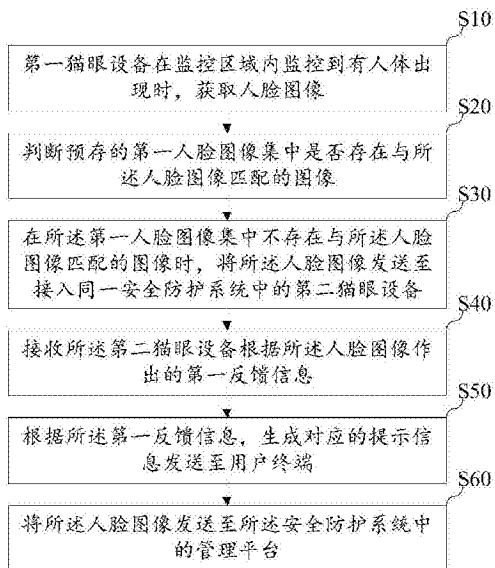
(54)发明名称

安全防护方法、装置、终端设备及计算机可  
读存储介质

(57)摘要

本发明公开了一种安全防护方法、装置、终端设备及计算机可读存储介质。本发明通过建立猫眼设备之间的通信连接,并将能够互相通信的猫眼设备均加入到同一个安全防护系统中,从而能够在安全防护系统中的任一猫眼设备(称为:第一猫眼设备)判定其所监控的监控区域内出现了不能确定身份的人时,借助该安全防护系统中其他的猫眼设备(称为:第二猫眼设备)进一步分析确认,当第一猫眼设备接收到第二猫眼设备作出的第一反馈信息时,根据第一反馈信息,生成对应的提示信息发送至用户终端。通过这种猫眼设备之间的协同作业有效扩充了人脸图像的检索库,在不增加小区监控设备的情况下,利用猫眼设备,大大提升了小区的安全力度,促进了小区的智能化发展。

CN 108765825 A



1. 一种安全防护方法,其特征在于,所述方法包括以下步骤:

第一猫眼设备在监控区域内监控到有人体出现时,获取人脸图像;

判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像;

在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,以使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像,所述第二猫眼设备为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备;

接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息;

根据所述第一反馈信息,生成对应的提示信息发送至用户终端。

2. 如权利要求1所述的方法,其特征在于,所述根据所述第一反馈信息,生成对应的提示信息发送至用户终端,具体包括:

在所述第一反馈信息中携带有匹配失败的标识时,生成第一提示信息发送至用户终端,所述第一提示信息包括所述人脸图像;

在所述第一反馈信息中携带有匹配成功的标识时,从所述第二人脸图像集中获取与所述人脸图像对应的身份信息,生成第二提示信息发送至用户终端,所述第二提示信息包括所述人脸图像和所述人脸图像对应的身份信息。

3. 如权利要求2所述的方法,其特征在于,所述根据所述第一反馈信息,生成对应的提示信息发送至用户终端之后,所述方法还包括:

将所述人脸图像发送至所述安全防护系统中的管理平台,以使所述管理平台在预存的可疑人员人脸图像集中搜索是否有与所述人脸图像匹配的图像,并根据搜索结果通知所述安全防护系统的管理人员前去查看。

4. 如权利要求3所述的方法,其特征在于,所述将所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

获取预设的物理位置信息,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

5. 如权利要求4所述的方法,其特征在于,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,所述方法还包括:

接收来自所述用户终端的第二反馈信息,所述第二反馈信息为用户根据所述第一提示信息或第二提示信息作出的反馈;

相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

6. 如权利要求5所述的方法,其特征在于,所述在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,所述方法还包括:

记录所述人脸图像在所述监控区域内停留的时间和/或出现的次数;

相应地,所述在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

在所述第二反馈信息中携带有预警指令,且所述人脸图像在所述监控区域内停留的时间大于预设时长和/或出现的次数大于预设次数时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

7. 如权利要求4至6任一项所述的方法,其特征在于,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,所述方法还包括:

扫描所述监控区域内的人体,生成全身图像,所述全身图像用于确定人体是否携带有危险物品;

相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

将所述全身图像、所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,以使所述安全防护系统的管理人员在前去查看时,携带相应的安防工具。

8. 一种安全防护装置,其特征在于,所述装置包括:

获取模块,用于在监控区域内监控到有人体出现时,获取人脸图像;

判定模块,用于判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像;

第一发送模块,用于在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,以使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像,所述第二猫眼设备为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备;

接收模块,用于接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息;

第二发送模块,用于根据所述第一反馈信息,生成对应的提示信息发送至用户终端。

9. 一种终端设备,其特征在于,所述终端设备包括:存储器、处理器以及存储在所述存储器上并可在所述处理器上运行的安全防护程序,所述安全防护程序配置为实现如权利要求1至7任一项所述的安全防护方法的步骤。

10. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有安全防护程序,所述安全防护程序被处理器执行时实现如权利要求1至7任一项所述的安全防护方法的步骤。

## 安全防护方法、装置、终端设备及计算机可读存储介质

### 技术领域

[0001] 本发明涉及报警监控技术领域,尤其涉及一种安全防护方法、装置、终端设备及计算机可读存储介质。

### 背景技术

[0002] 随着通信网络、计算机、远程控制等技术的发展,智能小区成为未来的发展趋势。

[0003] 目前,大部分新建的小区都在推行智能化,比如每个家庭基本都配置了智能猫眼,小区都配置了监控系统等。

[0004] 但是,目前的智能小区还无法实现多个小区之间监控系统的互通,并且小区中单独安装的监控系统会为了考虑成本,安装的监控设备,如摄像头个数受限,因此,安防力度远远不够,无法真正实现智能小区。

[0005] 上述内容仅用于辅助理解本发明的技术方案,并不代表承认上述内容是现有技术。

### 发明内容

[0006] 本发明的主要目的在于提供一种安全防护方法、装置、终端设备及计算机可读存储介质,旨在解决现有技术中小区安防力度不够,业主参与度低的技术问题。

[0007] 为实现上述目的,本发明提供了一种安全防护方法,所述方法包括以下步骤:

[0008] 第一猫眼设备在监控区域内监控到有人体出现时,获取人脸图像;

[0009] 判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像;

[0010] 在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,以使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像,所述第二猫眼设备为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备;

[0011] 接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息;

[0012] 根据所述第一反馈信息,生成对应的提示信息发送至用户终端。

[0013] 优选地,所述根据所述第一反馈信息,生成对应的提示信息发送至用户终端,具体包括:

[0014] 在所述第一反馈信息中携带有匹配失败的标识时,生成第一提示信息发送至用户终端,所述第一提示信息包括所述人脸图像;

[0015] 在所述第一反馈信息中携带有匹配成功的标识时,从所述第二人脸图像集中获取与所述人脸图像对应的身份信息,生成第二提示信息发送至用户终端,所述第二提示信息包括所述人脸图像和所述人脸图像对应的身份信息。

[0016] 优选地,所述根据所述第一反馈信息,生成对应的提示信息发送至用户终端之后,所述方法还包括:

[0017] 将所述人脸图像发送至所述安全防护系统中的管理平台,以使所述管理平台在预

存的可疑人员人脸图像集中搜索是否有与所述人脸图像匹配的图像,并根据搜索结果通知所述安全防护系统的管理人员前去查看。

[0018] 优选地,所述将所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0019] 获取预设的物理位置信息,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0020] 优选地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,所述方法还包括:

[0021] 接收来自所述用户终端的第二反馈信息,所述第二反馈信息为用户根据所述第一提示信息或第二提示信息作出的反馈;

[0022] 相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0023] 在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0024] 优选地,所述在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,所述方法还包括:

[0025] 记录所述人脸图像在所述监控区域内停留的时间和/或出现的次数;

[0026] 相应地,所述在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0027] 在所述第二反馈信息中携带有预警指令,且所述人脸图像在所述监控区域内停留的时间大于预设时长和/或出现的次数大于预设次数时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0028] 优选地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,所述方法还包括:

[0029] 扫描所述监控区域内的人体,生成全身图像,所述全身图像用于确定人体是否携带有危险物品;

[0030] 相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0031] 将所述全身图像、所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,以使所述安全防护系统的管理人员在前去查看时,携带相应的安防工具。

[0032] 此外,为实现上述目的,本发明还提供了一种安全防护方法装置,所述装置包括:

[0033] 获取模块,用于在监控区域内监控到有人体出现时,获取人脸图像;

[0034] 判定模块,用于判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像;

[0035] 第一发送模块,用于在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,以使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像,所述第二猫眼设备为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备;

[0036] 接收模块,用于接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息;

[0037] 第二发送模块,用于根据所述第一反馈信息,生成对应的提示信息发送至用户终

端。

[0038] 此外,为实现上述目的,本发明还提供了一种终端设备,所述终端设备包括:存储器、处理器以及存储在所述存储器上并可在所述处理器上运行的安全防护程序,所述安全防护程序配置为实现所述安全防护方法的步骤。

[0039] 此外,为实现上述目的,本发明还提供了一种计算机可读存储介质,所述计算机可读存储介质上存储有安全防护程序,所述安全防护程序被处理器执行时实现所述安全防护方法的步骤。

[0040] 本发明通过建立猫眼设备之间的通信连接,并将能够互相通信的猫眼设备均加入到同一个安全防护系统中,从而能够在安全防护系统中的任一猫眼设备(称为:第一猫眼设备)判定其所监控的监控区域内出现了不能确定身份的人时,借助该安全防护系统中其他的猫眼设备(称为:第二猫眼设备)进一步分析确认,当第一猫眼设备接收到第二猫眼设备作出的第一反馈信息时,根据第一反馈信息,生成对应的提示信息发送至用户终端。通过这种猫眼设备之间的协同作业有效扩充了人脸图像的检索库,在不增加小区监控设备的情况下,利用猫眼设备,大大提升了小区的安全力度,促进了小区的智能化发展。

## 附图说明

[0041] 图1为本发明实施例方案涉及的硬件运行环境的终端设备的结构示意图;

[0042] 图2为本发明安全防护方法第一实施例的流程示意图;

[0043] 图3为本发明安全防护方法第二实施例的流程示意图;

[0044] 图4为本发明安全防护装置的功能模块示意图。

[0045] 本发明目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

## 具体实施方式

[0046] 应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0047] 参照图1,图1为本发明实施例方案涉及的硬件运行环境的终端设备的结构示意图。

[0048] 该终端设备可以是各种类型的智能猫眼设备或者其他图形采集出来设备,此处不再一一列举,也不做具体限制。

[0049] 为了便于理解该终端设备的具体工作,以下结合图1进行具体说明。

[0050] 如图1所示,该终端设备可以包括:处理器1001,例如中央处理器(Central Processing Unit,CPU),通信总线1002、用户接口1003,网络接口1004,存储器1005。其中,通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括可触摸显示屏,可选地,用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如无线保真(Wireless-Fidelity,WI-FI)接口、蓝牙接口等)。存储器1005可以是高速RAM存储器,也可以是稳定的存储器(non-volatile memory),例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0051] 此外,值得一提的是,在具体实现中,各终端设备之间的通信连接可以根据需要选择合适的网络接口1004。

[0052] 以猫眼设备为例,比如在猫眼设备仅需要与同一楼层的其他猫眼设备通信连接

时,可以基于局域网(Local Area Network,LAN)利用蓝牙、WI-FI等无线接口或有线接口连通,在猫眼设备需要与整个小区或附近小区的其他猫眼设备通信连接时,可以基于城域网(Metropolitan Area Network,MAN)利用WI-FI接口或有线接口连通,在猫眼设备需要与整个城市,甚至更大范围内的其他猫眼设备通信连接时,可以基于广域网(Wide Area Network,WAN)利用WI-FI接口或有线接口连通。

[0053] 需要说明的是,以上仅为举例说明,对本发明的技术方案并不构成任何限定,在具体应用中,本领域的技术人员可以根据需要进行设置,本发明对此不做限制。

[0054] 此外,本领域技术人员可以理解,图1中示出的结构并不构成对终端设备的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0055] 因此,如图1所示,作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及安全防护程序。

[0056] 在图1所示的终端设备中,网络接口1004主要用建立终端设备与其他终端设备、安全防护系统以及用户终端之间的通信连接;用户接口1003主要用于接收用户的输入指令,如用户根据提示信息作出的反馈信息;所述终端设备通过处理器1001调用存储器1005中存储的安全防护程序,并执行以下操作:

[0057] 第一猫眼设备在监控区域内监控到有人体出现时,获取人脸图像;

[0058] 判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像;

[0059] 在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,以使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像,所述第二猫眼设备为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备;

[0060] 接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息;

[0061] 根据所述第一反馈信息,生成对应的提示信息发送至用户终端。

[0062] 进一步地,处理器1001可以调用存储器1005中存储的安全防护程序,还执行以下操作:

[0063] 在所述第一反馈信息中携带有匹配失败的标识时,生成第一提示信息发送至用户终端,所述第一提示信息包括所述人脸图像;

[0064] 在所述第一反馈信息中携带有匹配成功的标识时,从所述第二人脸图像集中获取与所述人脸图像对应的身份信息,生成第二提示信息发送至用户终端,所述第二提示信息包括所述人脸图像和所述人脸图像对应的身份信息。

[0065] 进一步地,处理器1001可以调用存储器1005中存储的安全防护程序,还执行以下操作:

[0066] 将所述人脸图像发送至所述安全防护系统中的管理平台,以使所述管理平台在预存的可疑人员人脸图像集中搜索是否有与所述人脸图像匹配的图像,并根据搜索结果通知所述安全防护系统的管理人员前去查看。

[0067] 进一步地,处理器1001可以调用存储器1005中存储的安全防护程序,还执行以下操作:

[0068] 获取预设的物理位置信息,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0069] 进一步地,处理器1001可以调用存储器1005中存储的安全防护程序,还执行以下操作:

[0070] 接收来自所述用户终端的第二反馈信息,所述第二反馈信息为用户根据所述第一提示信息或第二提示信息作出的反馈;

[0071] 相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0072] 在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0073] 进一步地,处理器1001可以调用存储器1005中存储的安全防护程序,还执行以下操作:

[0074] 记录所述人脸图像在所述监控区域内停留的时间和/或出现的次数;

[0075] 相应地,所述在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0076] 在所述第二反馈信息中携带有预警指令,且所述人脸图像在所述监控区域内停留的时间大于预设时长和/或出现的次数大于预设次数时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0077] 进一步地,处理器1001可以调用存储器1005中存储的安全防护程序,还执行以下操作:

[0078] 扫描所述监控区域内的人体,生成全身图像,所述全身图像用于确定人体是否携带有危险物品;

[0079] 相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0080] 将所述全身图像、所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,以使所述安全防护系统的管理人员在前去查看时,携带相应的安防工具。

[0081] 本实施通过上述方案,通过建立猫眼设备之间的通信连接,并将能够互相通信的猫眼设备均加入到同一个安全防护系统中,从而能够在安全防护系统中的任一猫眼设备(称为:第一猫眼设备)判定其所监控的监控区域内出现了不能确定身份的人时,借助该安全防护系统中其他的猫眼设备(称为:第二猫眼设备)进一步分析确认,当第一猫眼设备接收到第二猫眼设备作出的第一反馈信息时,根据第一反馈信息,生成对应的提示信息发送至用户终端。通过这种猫眼设备之间的协同作业有效扩充了人脸图像的检索库,在不增加小区监控设备的情况下,利用猫眼设备,大大提升了小区的安全力度,促进了小区的智能化发展。

[0082] 基于上述硬件结构,提出本发明安全防护方法实施例。

[0083] 参照图2,图2为本发明安全防护方法第一实施例的流程示意图。

[0084] 在第一实施例中,所述安全防护方法包括以下步骤:

[0085] S10:第一猫眼设备在监控区域内监控到有人体出现时,获取人脸图像。

[0086] S20:判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像。

[0087] 本实施例中所说的第一人脸图像集中的人脸图像具体是指业主在安装第一猫眼设备后,预先在第一猫眼设备内部的存储区域中录入的人脸图像,比如家庭成员、亲戚朋



友、物业人员等的人脸图像,此处不再一一列举,也不做具体限制。

[0088] S30:在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备。

[0089] 需要说明的是,本实施例中第一猫眼设备在确定所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,是为了使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像。

[0090] 应当理解的是,上述所说的第二人脸图像集中的人脸图像的添加方式与第一人脸图像集中的人脸图像的添加方式大致相同,此处不再赘述。

[0091] 另外,本实施例中所说的第二猫眼设备具体为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备。

[0092] 应当理解的是,在具体实现中,第一猫眼设备在确定所述第一人脸图像集中不存在与所述人脸图像匹配的图像,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备时,可以根据需要同时发送给多个第二猫眼设备,也可以依次发送给多个,比如在发送给的第一个第二猫眼设备没有搜索到匹配的图像时,发送给安全防护系统的下一个第二猫眼设备,直到安全防护系统中所有的第二猫眼设备都进行了搜索。

[0093] 此外,在具体实现中,安全防护系统中还包括其他的安防设备,比如小区内设置的摄像头、烟雾感应器、报警铃等,此处不再一一列举。

[0094] 此外,第一猫眼设备与第二猫眼设备之间的通信连接可以根据需要选择。

[0095] 比如,在第一猫眼设备仅需要与同一楼层的第二猫眼设备通信连接时,可以基于局域网(Local Area Network,LAN)利用蓝牙、WI-FI等无线接口或有线接口连通。

[0096] 还比如,在第一猫眼设备需要与整个小区或附近小区的第二猫眼设备通信连接时,可以基于城域网(Metropolitan Area Network,MAN)利用WI-FI接口或有线接口连通。

[0097] 还比如,在第一猫眼设备需要与整个城市,甚至更大范围内的第二猫眼设备通信连接时,可以基于广域网(Wide Area Network,WAN)利用WI-FI接口或有线接口连通。

[0098] 同理,第一猫眼设备与安全防护系统及用户终端的通信连接也可以按照上述需求选取合适的方式连接。

[0099] 需要说明的是,以上仅为举例说明,对本发明的技术方案并不构成任何限定,在具体应用中,本领域的技术人员可以根据需要进行设置,本发明对此不做限制。

[0100] S40:接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息。

[0101] 具体的说,所述第二猫眼设备根据所述人脸图像作出的第一反馈信息可以是人脸图像搜索成功的信息,比如通过添加匹配成功的标识来表示搜索成功。

[0102] 或者,是人脸图像搜索失败的信息,比如通过添加匹配失败的标识来表示搜索识别。

[0103] 关于匹配成功的标识和匹配失败的标识,本领域的技术人员可以根据需要设置,此处不做限制。

[0104] S50:根据所述第一反馈信息,生成对应的提示信息发送至用户终端。

[0105] 具体的说,在所述第一反馈信息中携带有匹配失败的标识时,生成第一提示信息发送至用户终端;在所述第一反馈信息中携带有匹配成功的标识时,从所述第二人脸图像

集中获取与所述人脸图像对应的身份信息,生成第二提示信息发送至用户终端。

[0106] 需要说明的是,本实施例中所说的第一提示信息具体可以包括所述人脸图像,第二提示信息具体可以包括所述人脸图像和所述人脸图像对应的身份信息。

[0107] 应当理解的是,在具体实现中,发送至用户终端的提示信息还可以包括其他内容,本领域的技术人员可以根据需要添加,此处不做限制。

[0108] 通过上述描述不难发现,本实施例中提供的安全防护方法,通过建立猫眼设备之间的通信连接,并将能够互相通信的猫眼设备均加入到同一个安全防护系统中,从而能够在安全防护系统中的任一猫眼设备(称为:第一猫眼设备)判定其所监控的监控区域内出现了不能确定身份的人时,借助该安全防护系统中其他的猫眼设备(称为:第二猫眼设备)进一步分析确认,当第一猫眼设备接收到第二猫眼设备作出的第一反馈信息时,根据第一反馈信息,生成对应的提示信息发送至用户终端。通过这种猫眼设备之间的协同作业有效扩充了人脸图像的检索库,在不增加小区监控设备的情况下,利用猫眼设备,大大提升了小区的安全力度,促进了小区的智能化发展。

[0109] 进一步地,如图3所示,基于第一实施例提出本发明安全防护方法的第二实施例,在本实施例中,在根据所述第一反馈信息,生成对应的提示信息发送至用户终端之后,进一步地,第一猫眼设备需要将所述人脸图像发送至所述安全防护系统中的管理平台,如图3中的步骤S60。

[0110] 在S60中:将所述人脸图像发送至所述安全防护系统中的管理平台。

[0111] 需要说明的是,在本实施例中,第一猫眼设备在根据所述第一反馈信息,生成对应的提示信息发送至用户终端之后,通过将所述人脸图像发送至所述安全防护系统中的管理平台,从而可以使所述管理平台在预存的可疑人员人脸图像集中搜索是否有与所述人脸图像匹配的图像,并根据搜索结果通知所述安全防护系统的管理人员前去查看,进而大大提升了小区的安防力度。

[0112] 此外,为了方便管理人员能够及时赶到可疑人员所在的地点,及时阻止可疑人员作出不法行为,第一猫眼设备在将所述人脸图像发送至所述安全防护系统中的管理平台时,还可以获取预设的物理位置信息,然后将所述物理位置信息和所述人脸图像一同发送至所述安全防护系统中的管理平台。

[0113] 应当理解的是,在具体实现中,如果第一猫眼设备具备定位功能,则用户无需提前预设物理位置信息,第一猫眼设备会在发送人脸图像至所述安全访问系统中的管理平台时,自动启动内部的定位模块,然后通过获取定位模块确定的定位信息得当前的物理地址信息。

[0114] 需要说明的是,以上仅为举例说明,对本发明的技术方案并不构成任何限定,在具体应用中,本领域的技术人员可以根据需要进行设置,本发明对此不做限制。

[0115] 进一步地,为了避免管路人员在管理平台中的人脸图像集中不存在该人脸图像,但该人脸图像实质并非可疑人员或不法分子时前去查看,增加管理人员的工作负担,在具体实现中,第一猫眼设备子在将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,可以先确定是否接收到了来自所述用户终端的第二反馈信息。若接收到了来自所述用户终端的第二反馈信息,并且所述第二反馈信息中携带有预警指令,则将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0116] 具体的说,上述所说的第二反馈信息为用户根据所述第一提示信息或第二提示信息作出的反馈,其主要是用来表示用户是否能够确定该人脸图像的身份信息。

[0117] 如果该人脸图像是用户认识的朋友,只是之前没有将其的人脸图像存储到第一人脸图像集中,此时用户反馈给第一猫眼设备的第二反馈信息中,可以携带的为访客为正常访客的指令,这样第一猫眼设备就不会获取物理位置信息,也不会将该访客的人脸图像发送至安全防护系统中的管理平台。

[0118] 如果该人脸图像该用户不认识,或者是用户能够确定的当前某些案件的犯罪嫌疑人,此时用户反馈给第一猫眼设备的第二反馈信息中,携带的则是预警指令,这样第一猫眼设备才会获取物理位置信息,并将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,以使管理人员前去查看。

[0119] 此外,为了能够辅助安全防护系统中的管理平台确定出现在第一猫眼设备的监控区域内的人为可疑人员,第一猫眼设备在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,还可以记录所述人脸图像在所述监控区域内停留的时间和/或出现的次数。然后在所述第二反馈信息中携带有预警指令,且所述人脸图像在所述监控区域内停留的时间大于预设时长和/或出现的次数大于预设次数时,再将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0120] 进一步地,为了保证管理人员的安全,在将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台之前,第一猫眼设备还可以进一步扫描所述监控区域内的人体,生成全身图像。

[0121] 需要说明的是,此处对监控区域内的人体进行扫描,生产全身图像,主要是为了根据所述全身图像确定人体是否携带有危险物品,如尖锐的物体(刀、棍棒等)、点火装置等,此处不再一一列举,对此也不做限制。

[0122] 相应地,在将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台时,还会将得到的全身图像发送至所述安全防护系统中的管理平台,以使所述安全防护系统的管理人员在前去查看时,携带相应的安防工具。

[0123] 通过上述描述不难发现,本实施例中提供的安全防护方法,通过将猫眼设备与安全防护系统中的管理平台结合,并在管理平台中建立统一的可疑人员图像管理库,从而可以方便各个小区共享,进而达到及时确认来访者身份,并在确定其为可疑人员或不符合分子时,及时通知管理人员前去查看,进一步提升的小区的安防力度,促进了智能小区的发展。

[0124] 此外,本发明实施例还提出一种安全防护装置。如图4所示,该安全防护装置包括:获取模块4001、判定模块4002、第一发送模块4003、接收模块4004和第二发送模块4005。

[0125] 其中,获取模块4001,用于在监控区域内监控到有人体出现时,获取人脸图像。判定模块4002,用于判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像。第一发送模块4003,用于在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,以使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像。接收模块4004,用于接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息。第二发送模块4005,用于根据所述第一反馈信息,生成对应的提示信息发送至用户终端。

[0126] 此外,需要说明的是,本实施例中所说的第二猫眼设备具体为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备。

[0127] 应当理解的是,在具体实现中,第一发送模块4003在将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备时,可以根据需要同时发送给多个第二猫眼设备,也可以依次发送给多个,比如在发送给第一个第二猫眼设备没有搜索到匹配的图像时,发送给安全防护系统的下一个第二猫眼设备,直到安全防护系统中所有的第二猫眼设备都进行了搜索。

[0128] 此外,在具体实现中,安全防护系统中还包括其他的安防设备,比如小区内设置的摄像头、烟雾感应器、报警铃等,此处不再一一列举。

[0129] 需要说明的是,以上仅为举例说明,对本发明的技术方案并不构成任何限定,在具体应用中,本领域的技术人员可以根据需要设置,本发明对此不做限制。

[0130] 通过上述描述不难发现,本实施例中提供的安全防护装置,通过建立猫眼设备之间的通信连接,并将能够互相通信的猫眼设备均加入到同一个安全防护系统中,从而能够在安全防护系统中的任一猫眼设备(称为:第一猫眼设备)判定其所监控的监控区域内出现了不能确定身份的人时,借助该安全防护系统中其他的猫眼设备(称为:第二猫眼设备)进一步分析确认,当第一猫眼设备接收到第二猫眼设备作出的第一反馈信息时,根据第一反馈信息,生成对应的提示信息发送至用户终端。通过这种猫眼设备之间的协同作业有效扩充了人脸图像的检索库,在不增加小区监控设备的情况下,利用猫眼设备,大大提升了小区的安全力度,促进了小区的智能化发展。

[0131] 需要说明的是,以上所描述的工作流程仅仅是示意性的,并不对本发明的保护范围构成限定,在实际应用中,本领域的技术人员可以根据实际的需要选择其中的部分或者全部来实现本实施例方案的目的,此处不做限制。

[0132] 另外,未在本实施例中详尽描述的技术细节,可参见本发明任意实施例所提供的安全防护方法,此处不再赘述。

[0133] 此外,本发明实施例还提出一种计算机可读存储介质,所述计算机可读存储介质上存储有安全防护程序,所述安全防护程序被处理器执行时实现如下操作:

[0134] 第一猫眼设备在监控区域内监控到有人体出现时,获取人脸图像;

[0135] 判断预存的第一人脸图像集中是否存在与所述人脸图像匹配的图像;

[0136] 在所述第一人脸图像集中不存在与所述人脸图像匹配的图像时,将所述人脸图像发送至接入同一安全防护系统中的第二猫眼设备,以使所述第二猫眼设备在第二人脸图像集中搜索是否有与所述人脸图像匹配的图像,所述第二猫眼设备为所述安全防护系统中除所述第一猫眼设备之外的任一猫眼设备;

[0137] 接收所述第二猫眼设备根据所述人脸图像作出的第一反馈信息;

[0138] 根据所述第一反馈信息,生成对应的提示信息发送至用户终端。

[0139] 进一步地,所述安全防护程序被处理器执行时还实现如下操作:

[0140] 在所述第一反馈信息中携带有匹配失败的标识时,生成第一提示信息发送至用户终端,所述第一提示信息包括所述人脸图像;

[0141] 在所述第一反馈信息中携带有匹配成功的标识时,从所述第二人脸图像集中获取与所述人脸图像对应的身份信息,生成第二提示信息发送至用户终端,所述第二提示信息

包括所述人脸图像和所述人脸图像对应的身份信息。

[0142] 进一步地,所述安全防护程序被处理器执行时还实现如下操作:

[0143] 将所述人脸图像发送至所述安全防护系统中的管理平台,以使所述管理平台在预存的可疑人员人脸图像集中搜索是否有与所述人脸图像匹配的图像,并根据搜索结果通知所述安全防护系统的管理人员前去查看。

[0144] 进一步地,所述安全防护程序被处理器执行时还实现如下操作:

[0145] 获取预设的物理位置信息,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0146] 进一步地,所述安全防护程序被处理器执行时还实现如下操作:

[0147] 接收来自所述用户终端的第二反馈信息,所述第二反馈信息为用户根据所述第一提示信息或第二提示信息作出的反馈;

[0148] 相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0149] 在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0150] 进一步地,所述安全防护程序被处理器执行时还实现如下操作:

[0151] 记录所述人脸图像在所述监控区域内停留的时间和/或出现的次数;

[0152] 相应地,所述在所述第二反馈信息中携带有预警指令时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0153] 在所述第二反馈信息中携带有预警指令,且所述人脸图像在所述监控区域内停留的时间大于预设时长和/或出现的次数大于预设次数时,将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台。

[0154] 进一步地,所述安全防护程序被处理器执行时还实现如下操作:

[0155] 扫描所述监控区域内的人体,生成全身图像,所述全身图像用于确定人体是否携带有危险物品;

[0156] 相应地,所述将所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,具体包括:

[0157] 将所述全身图像、所述物理位置信息和所述人脸图像发送至所述安全防护系统中的管理平台,以使所述安全防护系统的管理人员在前去查看时,携带相应的安防工具。

[0158] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0159] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0160] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在如上所述的一个

存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,空调器,或者网络设备等)执行本发明各个实施例所述的方法。

[0161] 以上仅为本发明的优选实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

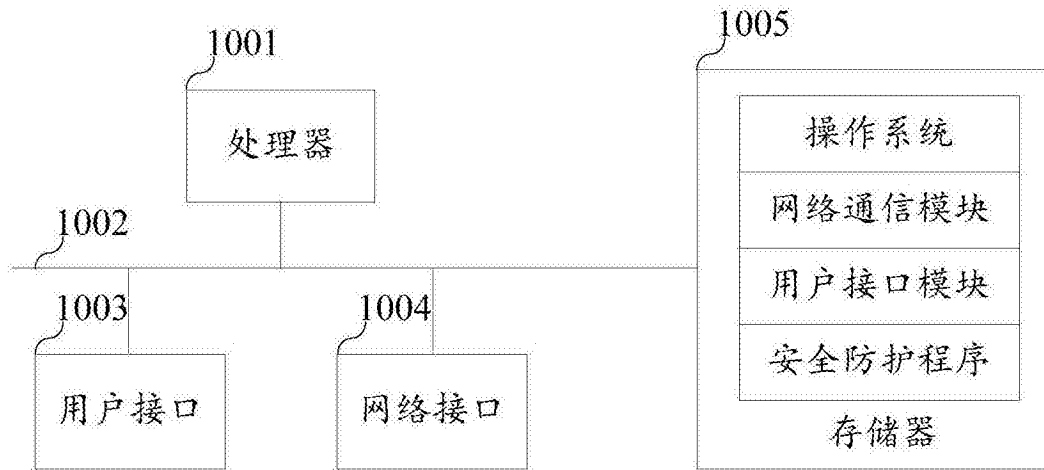


图1

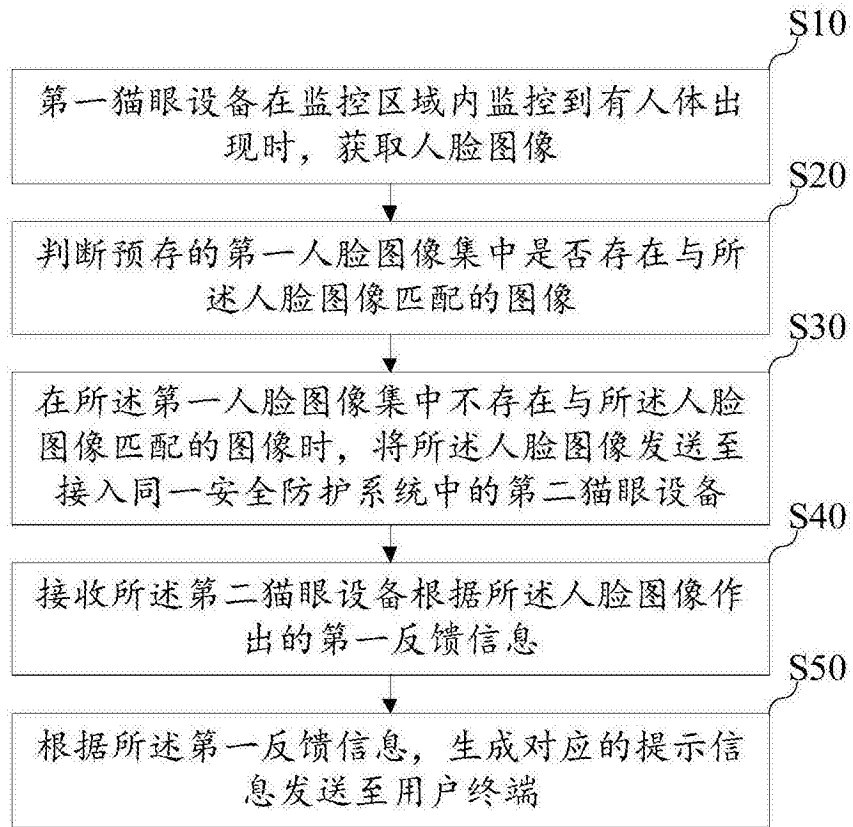


图2

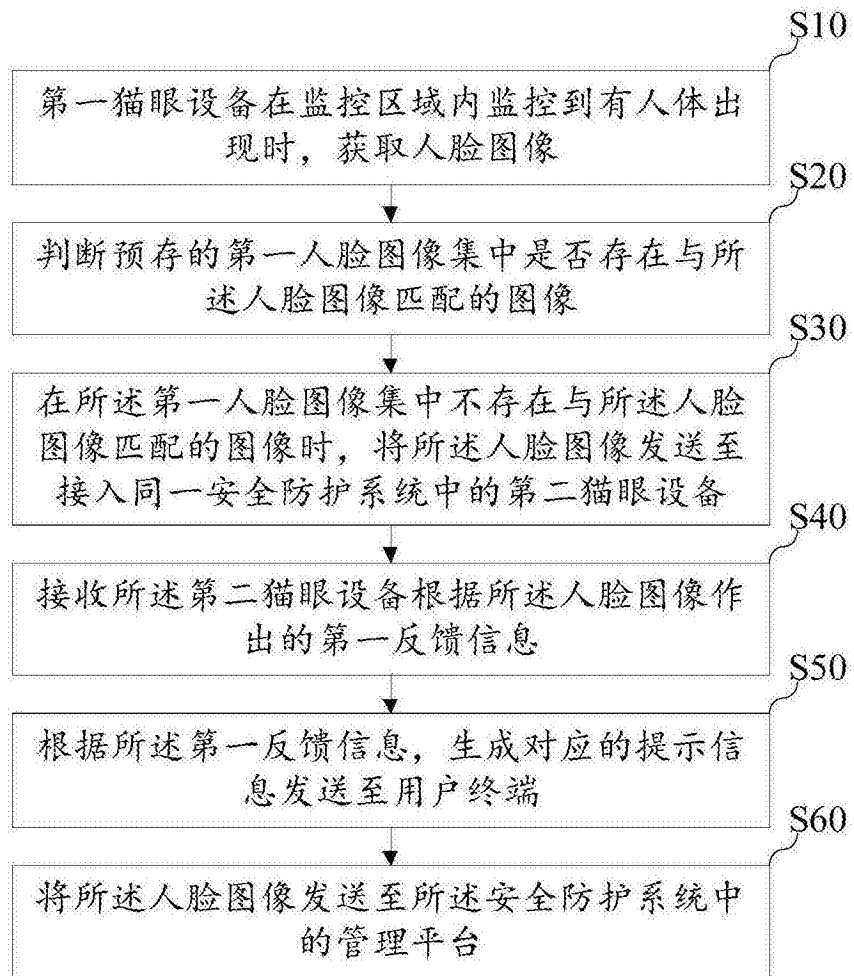


图3



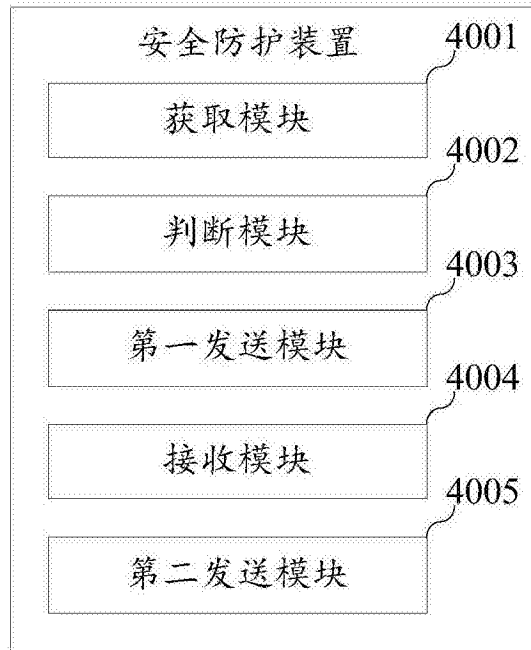


图4