(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113076859 A
(43)申请公布日 2021.07.06

(21)申请号 202110344185.8

(22)申请日 2021.03.31

(71)申请人 深圳供电局有限公司
地址 518000 广东省深圳市罗湖区深南东路4020号电力调度通信大楼

(72)发明人 叶振豪 邓彬 郝蛟 何山 胡亚荣 朱翎 李浩然 汪文达 张蕾

(74)专利代理机构 深圳汇智容达专利商标事务所(普通合伙) 44238
代理人 徐文城

(51)Int.Cl.
G06K 9/00(2006.01)
G06K 9/62(2006.01)
G06F 16/783(2019.01)
G06F 21/32(2013.01)
G06Q 50/26(2012.01)

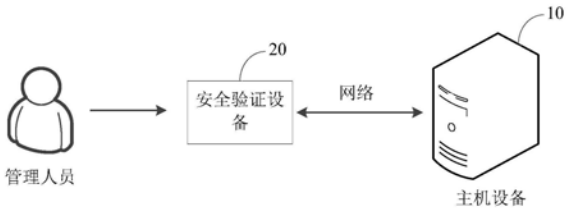
权利要求书2页 说明书11页 附图3页

(54)发明名称

人脸识别的安全监控方法及系统、电子设备、存储介质

(57)摘要

本发明公开了一种人脸识别的安全监控方法及系统、电子设备、存储介质，该方法包括：接收安全验证设备发送的身份验证请求，并根据所述身份验证请求获取待验证的人脸图像；提取所述待验证的人脸图像的人脸特征；将所述人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息；根据所述人员身份信息获取权限信息，并根据所述权限信息判断是否具有通过所述安全验证设备的权限；当具有通过所述安全验证设备的权限，向所述安全验证设备发送验证通过指令。通过本发明，可以有效保障整个数据中心的安全。



CN 113076859 A

1.一种人脸识别的安全监控方法,其特征在于,包括:

接收安全验证设备发送的身份验证请求,并根据所述身份验证请求获取待验证的人脸图像;

提取所述待验证的人脸图像的人脸特征;

将所述人脸特征与数据库中预先存储的人脸数据进行匹配,当匹配成功时,根据匹配的人脸数据获取人员身份信息;

根据所述人员身份信息获取权限信息,并根据所述权限信息判断是否具有通过所述安全验证设备的权限;

当具有通过所述安全验证设备的权限时,向所述安全验证设备发送验证通过指令。

2.根据权利要求1所述的方法,其特征在于,在所述接收安全验证设备发送的身份验证请求后,所述方法还包括:

获取所述安全验证设备关联的任务执行设备,并根据所述身份验证请求获取待执行的任务;

在所述向所述安全验证设备发送验证通过指令后,所述方法还包括:

根据所述待执行的任务生成控制指令,并向所述任务执行设备发送所述控制指令,所述控制指令用于控制所述任务执行设备执行所述任务。

3.根据权利要求2所述的方法,其特征在于,在所述根据所述权限信息判断是否具有通过所述安全验证设备的权限之后,所述方法还包括:

获取所述待执行的任务的安全级别;

当所述安全级别高于预设级别时,根据所述权限信息判断是否具有执行所述任务的权限;

所述根据所述待执行的任务生成控制指令,并向所述任务执行设备发送所述控制指令,包括:

当具有执行所述任务的权限时,根据所述待执行的任务生成控制指令,并向所述任务执行设备发送所述控制指令。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:

采集一个或多个监控设备拍摄的视频数据;

对所述视频数据进行人脸识别,确定每个视频数据中包含的人员身份信息;

当检测到所述视频数据中包含无法确定人员身份信息的可疑人员时,生成告警信息。

5.根据权利要求4所述的方法,其特征在于,在所述确定每个视频数据中包含的人员身份信息之后,所述方法还包括:

根据所述人员身份信息及视频数据对各个人员进行定位,并生成与所述人员身份信息对应的位置记录信息;

当检测到所述位置记录信息中出现可疑位置时,标记出现所述可疑位置的人员身份信息为可疑人员,并生成告警信息。

6.根据权利要求4或5所述的方法,其特征在于,所述生成告警信息,包括:

确定所述可疑人员的当前位置信息,并根据所述当前位置信息生成告警信息,所述告警信息用于在显示设备中显示所述可疑人员的当前位置信息,并播放包含所述可疑人员的视频数据。

7.根据权利要求1所述的方法，其特征在于，所述方法还包括：

采集一个或多个环境安全设备的设备参数；

根据所述设备参数对环境安全进行监控；

当检测到出现环境安全隐患时，定位存在安全隐患的环境位置，并生成告警信息。

8.一种基于人脸识别的安全监控系统，其特征在于，包括：

接收模块，用于接收安全验证设备发送的身份验证请求，并根据所述身份验证请求获取待验证的人脸图像；

特征提取模块，用于提取所述待验证的人脸图像的人脸特征；

匹配模块，用于将所述人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息；

权限判断模块，用于根据所述人员身份信息获取权限信息，并根据所述权限信息判断是否具有通过所述安全验证设备的权限；

发送模块，用于当具有通过所述安全验证设备的权限，向所述安全验证设备发送验证通过指令。

9.一种电子设备，包括存储器及处理器，所述存储器中存储有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器实现如权利要求1至7任一所述的方法。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至7任一所述的方法。

人脸识别的安全监控方法及系统、电子设备、存储介质

技术领域

[0001] 本发明涉及监控技术领域，具体涉及一种人脸识别的安全监控方法及系统、电子设备、计算机可读存储介质。

背景技术

[0002] 随着业务的飞速发展，数据中心的规模也越来越庞大而复杂，为保障整个数据中心的正常运行，需要对数据中心下的各类基础设施管理对象进行监控管理。数据中心涉及的设备及数据多且复杂，如何有效保障整个数据中心的安全成了当下亟需解决的难题。

发明内容

[0003] 本发明的目的在于提出一种人脸识别的安全监控方法及系统、电子设备、计算机可读存储介质，以有效保障整个数据中心的安全。

[0004] 为实现上述目的，本发明第一方面提出一种基于人脸识别的安全监控方法，包括：

[0005] 接收安全验证设备发送的身份验证请求，并根据所述身份验证请求获取待验证的人脸图像；

[0006] 提取所述待验证的人脸图像的人脸特征；

[0007] 将所述人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息；

[0008] 根据所述人员身份信息获取权限信息，并根据所述权限信息判断是否具有通过所述安全验证设备的权限；

[0009] 当具有通过所述安全验证设备的权限时，向所述安全验证设备发送验证通过指令。

[0010] 可选地，在所述接收安全验证设备发送的身份验证请求后，所述方法还包括：

[0011] 获取所述安全验证设备关联的任务执行设备，并根据所述身份验证请求获取待执行的任务；

[0012] 在所述向所述安全验证设备发送验证通过指令后，所述方法还包括：

[0013] 根据所述待执行的任务生成控制指令，并向所述任务执行设备发送所述控制指令，所述控制指令用于控制所述任务执行设备执行所述任务。

[0014] 可选地，在所述根据所述权限信息判断是否具有通过所述安全验证设备的权限之后，所述方法还包括：

[0015] 获取所述待执行的任务的安全级别；

[0016] 当所述安全级别高于预设级别时，根据所述权限信息判断是否具有执行所述任务的权限；

[0017] 所述根据所述待执行的任务生成控制指令，并向所述任务执行设备发送所述控制指令，包括：

[0018] 当具有执行所述任务的权限时，根据所述待执行的任务生成控制指令，并向所述

任务执行设备发送所述控制指令。

[0019] 可选地，所述方法还包括：

[0020] 采集一个或多个监控设备拍摄的视频数据；

[0021] 对所述视频数据进行人脸识别，确定每个视频数据中包含的人员身份信息；

[0022] 当检测到所述视频数据中包含无法确定人员身份信息的可疑人员时，生成告警信息。

[0023] 可选地，在所述确定每个视频数据中包含的人员身份信息之后，所述方法还包括：

[0024] 根据所述人员身份信息及视频数据对各个人员进行定位，并生成与所述人员身份信息对应的位置记录信息；

[0025] 当检测到所述位置记录信息中出现可疑位置时，标记出现所述可疑位置的人员身份信息为可疑人员，并生成告警信息。

[0026] 可选地，所述生成告警信息，包括：

[0027] 确定所述可疑人员的当前位置信息，并根据所述当前位置信息生成告警信息，所述告警信息用于在显示设备中显示所述可疑人员的当前位置信息，并播放包含所述可疑人员的视频数据。

[0028] 可选地，所述方法还包括：

[0029] 采集一个或多个环境安全设备的设备参数；

[0030] 根据所述设备参数对环境安全进行监控；

[0031] 当检测到出现环境安全隐患时，定位存在安全隐患的环境位置，并生成告警信息。

[0032] 本发明第二方面提出一种基于人脸识别的安全监控系统，包括：

[0033] 接收模块，用于接收安全验证设备发送的身份验证请求，并根据所述身份验证请求获取待验证的人脸图像；

[0034] 特征提取模块，用于提取所述待验证的人脸图像的人脸特征；

[0035] 匹配模块，用于将所述人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息；

[0036] 权限判断模块，用于根据所述人员身份信息获取权限信息，并根据所述权限信息判断是否具有通过所述安全验证设备的权限；

[0037] 发送模块，用于当具有通过所述安全验证设备的权限，向所述安全验证设备发送验证通过指令。

[0038] 本发明第三方面提出一种电子设备，包括存储器及处理器，所述存储器中存储有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器实现如第一方面所述的方法。

[0039] 本发明第四方面提出一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面所述的方法。

[0040] 上述的一种基于人脸识别的安全监控方法及系统、电子设备、计算机可读存储介质，具有以下有益效果：

[0041] 根据安全验证设备发送的身份验证请求获取待验证的人脸图像，提取待验证的人脸图像的人脸特征，并将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息，再根据人员身份信息获取权限信息，并根据权

限信息判断是否具有通过安全验证设备的权限，当具有通过安全验证设备的权限，向安全验证设备发送验证通过指令，可通过人脸识别对人员身份进行验证，并验证人员的权限，能够提高安全性，有效保障整个数据中心的安全。

[0042] 本发明的其它特征和优点将在随后的说明书中阐述。

附图说明

[0043] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0044] 图1为本发明的一个实施例中基于人脸识别的安全监控方法的应用场景图。

[0045] 图2为本发明的一个实施例中基于人脸识别的安全监控方法的应用场景图。

[0046] 图3为本发明的一个实施例中基于人脸识别的安全监控方法的流程图。

[0047] 图4为本发明的一个实施例中验证是否具有执行任务的权限的流程图。

[0048] 图5为本发明的一个实施例中通过视频数据检测人员安全性的流程图。

[0049] 图6为本发明的一个实施例中基于人脸识别的安全监控系统的框图。

[0050] 图7为本发明的一个实施例中电子设备的框图。

具体实施方式

[0051] 以下将参考附图详细说明本公开的各种示例性实施例、特征和方面。另外，为了更好的说明本发明，在下文的具体实施例中给出了众多的具体细节。本领域技术人员应当理解，没有某些具体细节，本发明同样可以实施。在一些实例中，对于本领域技术人员熟知的手段未作详细描述，以便于凸显本发明的主旨。

[0052] 图1为一个实施例中基于人脸识别的安全监控方法的应用场景图。如图1所示，主机设备10可通过网络与安全验证设备20建立连接，其中，主机设备10可以是计算机等终端设备，也可以是服务器。安全验证设备20可对工作人员进行身份验证，通过摄像头采集工作人员的人脸图像，并向主机设备10发送身份验证请求。主机设备10接收安全验证设备20发送的身份验证请求，可根据身份验证请求获取待验证的人脸图像。主机设备10提取待验证的人脸图像的人脸特征，并将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息。主机设备10可根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备20的权限，当具有通过安全验证设备20的权限时，可向安全验证设备20发送验证通过指令。

[0053] 图2为另一个实施例中基于人脸识别的安全监控方法的应用场景图。如图2所示，安全验证设备20可与关联的任务执行设备30连接，主机设备10则可通过网络分别与安全验证设备20及任务执行设备30建立连接。主机设备10接收安全验证设备20发送的身份验证请求，可获取该安全验证设备20关联的任务执行设备30，并根据身份验证请求获取待执行的任务。主机设备10在向安全验证设备20发送验证通过指令后，可根据待执行的任务生成控制指令，并向任务执行设备30发送该控制指令。任务执行设备30根据该控制指令可执行该任务。

[0054] 如图3所示，在一个实施例中，提供一种基于人脸识别的安全监控方法，可应用于上述的主机设备，包括以下步骤：

[0055] 步骤310，接收安全验证设备发送的身份验证请求，并根据身份验证请求获取待验证的人脸图像。

[0056] 安全验证设备可用于对人员的身份进行验证，验证通过的人员可被确定为安全人员，验证不通过的人员可被确定为可疑人员，以保障安全性。在一些实施方式中，安全验证设备可包括摄像头、显示屏等，其中，摄像头可用于采集人员的人脸图像，显示屏则可用于显示采集的人脸图像，还可显示验证结果等。可以理解地，安全验证设备也可仅包括摄像头，也可包括除摄像头、显示屏以外的部件。

[0057] 安全验证设备通过摄像头采集待验证的人脸图像，可根据该人脸图像生成身份验证请求，并向主机设备发送身份验证请求。主机设备可对解析的身份验证请求进行解析，得到发送该身份验证请求的安全验证设备对应的设备标识，以及待验证的人脸图像，其中，设备标识可用于标识安全验证设备的身份，例如，设备标识可为安全验证设备的MAC(Media Access Control，媒体介入控制层)地址、设备编号，也可为IP(Internet Protocol，网际互连协议)地址等，但不限于此。

[0058] 步骤320，提取待验证的人脸图像的人脸特征。

[0059] 主机设备获取待验证的人脸图像，可对该人脸图像进行识别，并提取人脸图像的人脸特征，可选地，可先对人脸图像进行人脸检测，确定人脸区域，并提取人脸区域的特征向量作为人脸特征，人脸特征可组成人脸的轮廓形状、五官形状及五官位置等，从而可进行人脸识别。检测人脸区域和提取人脸特征的算法在此不作限定，例如，可通过各式的卷积神经网络提取人脸特征等。作为一种实施方式，人脸特征可包括像素点的坐标及像素值等，像素点的坐标可指的是特征对应的像素点在图像中的图像坐标，像素值则可以是特征对应的像素点的RGB(红、绿、蓝)值，还可以包括亮度等信息。

[0060] 步骤330，将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息。

[0061] 主机设备的数据库中可预先存储有大量工作人员的人脸数据，以及与每个人脸数据匹配的人员身份信息，人员身份信息可包括人员姓名、工号、岗位等信息。在数据库中存储有人脸数据及人员身份信息的工作人员可被确定身份，可认为是可信任的人员。

[0062] 主机设备可将提取的人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，也即，在数据库中可以找到与人脸特征匹配的人脸数据时，可根据该匹配的人脸数据获取人员身份信息，该人员身份信息可作为待验证的人脸图像对应的人员身份信息。在一个实施例中，主机设备可分别计算人脸特征与预先存储的各个人脸数据的相似度，并从相似度大于阈值的人脸数据中，选取相似度最高的人脸数据作为匹配的人脸数据。可以理解地，该阈值可根据实际需求进行设定，例如88％、90％、91％等，在此不作限定。

[0063] 在一些实施例中，当在数据库中查找不到与提取的人脸特征匹配的人脸数据时，可确定待验证的人脸图像对应的人员为可疑人员，其人员身份信息未录入数据库中。主机设备可向安全验证设备发送不通过指令，安全验证设备根据不通过指令可确定人员的人脸没有验证通过，则该人员无法执行进一步地操作或任务。主机设备还可生成告警信息，并将告警信息发送至显示终端。显示终端可对告警信息进行展示，例如，可显示“出现可疑人员”

的告警信息，也可通过语音等方式播放告警信息等，以方便管理人员获取情况，提高管理效率。

[0064] 步骤340，根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备的权限。

[0065] 主机设备获取提取的人脸特征对应的人员身份信息，可获取该人员身份信息对应的权限信息，该权限信息可用于表示工作人员对各个设备的操作权限。可选地，权限信息可包括设备标识及对应的操作权限，其中，操作权限可用数字、字母或符号等进行表示，例如，具备权限为1，不具备权限为0等，但不限于此。对于不同的工作人员，对不同设备的操作权限可不同。可获取安全验证设备的设备标识，并根据权限信息查询与安全验证设备的设备标识对应的权限，判断是否具有通过安全验证设备的权限。

[0066] 步骤350，当具有通过安全验证设备的权限时，向安全验证设备发送验证通过指令。

[0067] 当判定工作人员具有通过安全验证设备的权限时，主机设备可向安全验证设备发送验证通过指令，安全验证设备通过对工作人员的身份验证，且工作人员可进行后续的操作。若判定工作人员不具有通过安全验证设备的权限，则可向安全验证设备发送不通过指令，安全验证设备根据不通过指令可确定人员的人脸没有验证通过，则该工作人员无法执行进一步地操作或任务。进一步地，该不通过指令可包括权限不通过信息，安全验证设备可对不通过信息进行显示，方便工作人员可获知不具备权限进行操作的情况。

[0068] 在本申请实施例中，根据安全验证设备发送的身份验证请求获取待验证的人脸图像，提取待验证的人脸图像的人脸特征，并将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息，再根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备的权限，当具有通过安全验证设备的权限，向安全验证设备发送验证通过指令，可通过人脸识别对人员身份进行验证，并验证人员的权限，能够提高安全性。

[0069] 如图4所示，在一个实施例中，在步骤310接收安全验证设备发送的身份验证请求之后，还包括以下步骤：

[0070] 步骤402，获取安全验证设备关联的任务执行设备，并根据身份验证请求获取待执行的任务。

[0071] 不同安全验证设备可关联不同的任务执行设备，任务执行设备可以为用于执行各式任务的电子设备，例如，可以为机房的门、查看监控数据的计算机、调节温度的控制器等，但不限于此。主机设备接收安全验证设备发送的身份验证请求，该身份验证请求除了包括安全验证设备的设备标识及待验证的人脸图像外，还可包括待执行的任务。主机设备可根据安全验证设备的设备标识获取与安全验证设备关联的任务执行设备的标识，该关联关系可预先存储在主机设备中。待执行的任务即为该关联的任务执行设备需要执行的任务，例如，机房的门的待执行的任务可为开启门或关闭门，查看监控数据的计算机的待执行的任务可为显示所有机房的湿度监控数据等。可以理解地，上述示例中的安全验证设备关联的任务执行设备，以及任务执行设备的待执行的任务仅用于说明，在本申请实施例中不作限定。

[0072] 步骤404，根据待执行的任务生成控制指令，并向任务执行设备发送所述控制指

令，控制指令用于控制任务执行设备执行所述任务。

[0073] 主机设备在数据库中查找到与提取的人脸特征匹配的人脸数据，获取人员身份信息，并根据该人员身份信息确定具有通过安全验证设备的权限，可说明该人员身份信息对应的工作人员具备对任务执行设备进行操作的权限。主机设备在向安全验证设备发送验证通过指令后，可根据待执行的任务生成控制指令，并向任务执行设备发送该控制指令。任务执行设备可根据接收的控制指令执行该待执行的任务。例如，任务执行设备为机房的门，可向该机房的门发送开启的控制指令，机房的门在接收到该控制指令后，自动开启。

[0074] 在一个实施例中，在确定具备对任务执行设备进行操作的权限后，可根据人员身份信息判断是否具备控制任务执行设备执行待执行的任务的权限。对于同一任务执行设备上执行的不同任务，可能具备有不同的权限。例如，任务执行设备为查看监控数据的计算机，执行的任务可包括查看整个数据中心的监控视频、查看所有机房的湿度监控数据、查看设备的功率等，对于同一工作人员，可能具备查看所有机房的湿度监控数据及查看设备的功率的权限，而不具备查看整个数据中心的监控视频的权限，但不限于此。

[0075] 在一个实施例中，主机设备可获取待执行的任务的安全级别，并判断待执行的任务的安全级别是否高于预设级别。不同任务对应的安全级别可不同，以区分不同任务的安全需求，安全级别越高，可说明任务所需的安全性越强。若待执行的任务的安全级别小于或等于预设级别，可判定该待执行的任务所需的安全性较低，可直接根据待执行的任务生成控制指令，并向任务执行设备发送该控制指令，以控制任务执行设备执行任务。

[0076] 当待执行的任务的安全级别大于预设级别时，主机设备可根据权限信息判断是否具有控制任务执行设备执行该任务的权限。当确定工作人员具有控制任务执行设备执行待执行的任务的权限时，主机设备可在向安全验证设备发送验证通过指令后，根据待执行的任务生成控制指令，并向任务执行设备发送该控制指令，以控制任务执行设备执行任务。

[0077] 在本申请实施例中，可进一步验证控制任务执行设备执行任务的权限，并控制任务执行设备执行任务，可有效提高安全性。

[0078] 如图5所示，在一个实施例中，上述基于人脸识别的安全监控方法，还包括以下步骤：

[0079] 步骤502，采集一个或多个监控设备拍摄的视频数据。

[0080] 为了保障整个数据中心的安全，在数据中心内的各个区域可分别设置有监控设备，该监控设备可包括摄像头等，监控设备可拍摄现实场景图像，生成监控视频，并将视频数据上传至主机设备，以通过视频对整个数据中心的安全进行监控。

[0081] 步骤504，对视频数据进行人脸识别，确定每个视频数据中包含的人员身份信息。

[0082] 主机设备可获取各个监控设备拍摄的视频数据，可对视频数据进行分析。作为一种实施方式，可对视频数据进行人脸识别，识别视频数据中包含的人员，并确定每个人员的人员身份。视频数据中可包括多帧视频图像，提取每一帧视频图像的图像特征，可将图像特征输入人脸识别模型中，通过人脸识别模型检测视频图像中是否包含人脸。当检测到人脸识别模型中包含人脸，可提取人脸特征，并将人脸特征与预先存储的人脸数据进行匹配，并根据与人脸特征匹配的预先存储的人脸数据获取人员身份信息，确定对应的人员身份。

[0083] 步骤506，当检测到视频数据中包含无法确定人员身份信息的可疑人员时，生成告警信息。

[0084] 当人脸特征查找不到匹配的预先存储的人脸数据时，即检测到无法确定人员身份信息的人员，可判定视频数据中出现无法确认人员身份的人员，并将该无法确定人员身份的人员标记为可疑人员。主机设备检测到可疑人员时，可生成告警信息，并将告警信息发送至显示终端。显示终端可对告警信息进行展示，例如，可显示“出现可疑人员”的告警信息，也可通过语音等方式播放告警信息等，但不限于此。

[0085] 在一个实施例中，主机设备确定每个视频数据中包含的人员身份信息后，还可根据人员身份信息及视频数据对各个人员进行定位，并生成与人员身份信息对应的位置记录信息。主机设备可根据每个人员活动的现实环境，对视频数据中包含的各个人员进行定位，获取与各个人员身份信息对应的位置信息。当检测到人员处于非正常区域时，也即，当检测到位置记录信息中出现可疑位置时，可将该出现可疑位置的人员身份信息标记为可疑人员。例如，人员A的正常工作范围为1号楼，但检测到人员A的位置记录信息中出现3号楼，该位置属于非正常工作范围，属于可疑位置，则可将人员A标记物可疑人员。进一步地，可对各个区域进行安全级别划分，级别越高，可表示区域的安全重要程度越高，信息越机密。当检测到位置记录信息中出现可疑位置时，可进一步判断该可疑位置所属的区域的安全级别是否高于预设级别，若是高于预设级别，则可将该出现可疑位置的人员标记为可疑人员。

[0086] 主机设备可根据位置记录信息获取可疑人员的当前位置信息，并根据可疑人员的当前位置信息生成告警信息。主机设备检测到可疑人员后，可通过调用监控设备实时对可疑人员进行跟踪，以确保实时获取可疑人员的位置信息。显示终端可展示告警信息，展示可疑人员的当前位置信息，例如，可显示告警信息：“2号楼1层出现不明身份的人员”。显示终端还可从主机设备获取包含可疑人员的视频数据，并进行显示。管理人员可以快速且直接地获知可疑人员的位置，以方便进行人员排查，提高安全性。

[0087] 在本申请实施例中，可通过对视频数据进行人脸识别，确定每个视频数据中包含的人员身份信息，以检测可疑人员，可保证整个数据中心的人员安全性。

[0088] 在一个实施例中，除了人员安全外，还可对数据中心的环境安全进行监控，环境安全可包括消防安全、漏水安全等，还可包括设备的运行环境安全，例如设备的运行环境的温度、湿度等。主机设备可一个或多个环境安全设备的设备参数，该环境安全设备可包括消防设备、漏水检测设备，以及温度传感器、湿度传感器等各式传感器等。设备参数可以为环境安全设备的运行参数，不同环境安全设备的设备参数可不同。例如，温度传感器的设备参数可为检测的温度值，漏水检测设备的设备参数可为漏水参数，漏水参数可用于表示是否发生漏水等，但不限于此。主机设备可根据设备参数对环境安全进行监控，根据设备参数判断是否出现安全隐患。可预先设备参数的正常值区间，不同环境安全设备的设备参数可对应不同的正常值区间。可将采集的设备参数与对应的正常值区间进行比对，当设备参数不处于对应的正常值区间内时，可判定出现安全隐患。

[0089] 当环境安全设备的设备参数不处于对应的正常值区间内，即检测到出现环境安全隐患，可确定该设备参数不处于对应的正常值区间内的环境安全设备的位置信息，从而对存在安全隐患的环境进行定位，获取存在安全隐患的环境位置，并生成告警信息。主机设备可将告警信息发送至显示终端。显示终端可展示告警信息，并展示存在安全隐患的环境位置，例如，可显示告警信息：“3号楼3层的第5机房出现漏水”等。可以理解地，出现安全隐患的情况有多种，在此不作限定。

[0090] 在本申请实施例中，还可对环境安全进行监控，提高安全性。

[0091] 在一个实施例中，提供一种基于人脸识别的安全监控方法，包括以下步骤：

[0092] 步骤(1)，接收安全验证设备发送的身份验证请求，并根据身份验证请求获取待验证的人脸图像。

[0093] 步骤(2)，提取待验证的人脸图像的人脸特征。

[0094] 步骤(3)，将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息。

[0095] 步骤(4)，根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备的权限。

[0096] 步骤(5)，当具有通过安全验证设备的权限时，向安全验证设备发送验证通过指令。

[0097] 在一个实施例中，在步骤接收安全验证设备发送的身份验证请求之后，上述方法还包括：获取所述安全验证设备关联的任务执行设备，并根据所述身份验证请求获取待执行的任务；在步骤向安全验证设备发送验证通过指令之后，上述方法还包括：根据待执行的任务生成控制指令，并向任务执行设备发送所述控制指令，控制指令用于控制所务执行设备执行该任务。

[0098] 在一个实施例中，在步骤根据所述权限信息判断是否具有通过所述安全验证设备的权限之后，上述方法还包括：获取待执行的任务的安全级别；当安全级别高于预设级别时，根据权限信息判断是否具有执行任务的权限；步骤根据待执行的任务生成控制指令，并向任务执行设备发送所述控制指令，包括：当具有执行任务的权限时，根据待执行的任务生成控制指令，并向任务执行设备发送控制指令。

[0099] 在一个实施例中，上述方法还包括：采集一个或多个监控设备拍摄的视频数据；对视频数据进行人脸识别，确定每个视频数据中包含的人员身份信息；当检测到视频数据中包含无法确定人员身份信息的可疑人员时，生成告警信息。

[0100] 在一个实施例中，在步骤确定每个视频数据中包含的人员身份信息之后，上述方法还包括：根据人员身份信息及视频数据对各个人员进行定位，并生成与人员身份信息对应的位置记录信息；当检测到位置记录信息中出现可疑位置时，标记出现可疑位置的人员身份信息为可疑人员，并生成告警信息。

[0101] 在一个实施例中，步骤生成告警信息，包括：确定可疑人员的当前位置信息，并根据当前位置信息生成告警信息，告警信息用于在显示设备中显示可疑人员的当前位置信息，并播放包含可疑人员的视频数据。

[0102] 在一个实施例中，上述方法还包括：采集一个或多个环境安全设备的设备参数；根据设备参数对环境安全进行监控；当检测到出现环境安全隐患时，定位存在安全隐患的环境位置，并生成告警信息。

[0103] 在本申请实施例中，根据安全验证设备发送的身份验证请求获取待验证的人脸图像，提取待验证的人脸图像的人脸特征，并将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息，再根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备的权限，当具有通过安全验证设备的权限，向安全验证设备发送验证通过指令，可通过人脸识别对人员身份进行验证，并

验证人员的权限，能够提高安全性。

[0104] 如图6所示，在一个实施例中，提供一种基于人脸识别的安全监控系统600，该系统600包括接收模块610、特征提取模块620、匹配模块630、权限判断模块640及发送模块650。

[0105] 接收模块610，用于接收安全验证设备发送的身份验证请求，并根据身份验证请求获取待验证的人脸图像。

[0106] 特征提取模块620，用于提取待验证的人脸图像的人脸特征。

[0107] 匹配模块630，用于将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息。

[0108] 权限判断模块640，用于根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备的权限。

[0109] 发送模块650，用于当具有通过安全验证设备的权限，向安全验证设备发送验证通过指令。

[0110] 在本申请实施例中，根据安全验证设备发送的身份验证请求获取待验证的人脸图像，提取待验证的人脸图像的人脸特征，并将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息，再根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备的权限，当具有通过安全验证设备的权限，向安全验证设备发送验证通过指令，可通过人脸识别对人员身份进行验证，并验证人员的权限，能够提高安全性。

[0111] 在一个实施例中，上述安全监控系统600除了包括接收模块610、特征提取模块620、匹配模块630、权限判断模块640及发送模块650外，还包括任务获取模块。

[0112] 任务获取模块，用于获取安全验证设备关联的任务执行设备，并根据身份验证请求获取待执行的任务。

[0113] 发送模块650，还用于根据待执行的任务生成控制指令，并向任务执行设备发送控制指令，控制指令用于控制任务执行设备执行任务。

[0114] 在一个实施例中，权限判断模块640，还用于获取待执行的任务的安全级别，当安全级别高于预设级别时，根据权限信息判断是否具有执行任务的权限。

[0115] 发送模块650，还用于当具有执行所述任务的权限时，根据待执行的任务生成控制指令，并向任务执行设备发送所述控制指令。

[0116] 在本申请实施例中，可进一步验证控制任务执行设备执行任务的权限，并控制任务执行设备执行任务，可有效提高安全性。

[0117] 在一个实施例中，上述安全监控系统600除了包括接收模块610、特征提取模块620、匹配模块630、权限判断模块640、发送模块650及任务获取模块，还包括采集模块、告警模块及定位模块。

[0118] 采集模块，用于采集一个或多个监控设备拍摄的视频数据。

[0119] 匹配模块630，还用于对视频数据进行人脸识别，确定每个视频数据中包含的人员身份信息，

[0120] 告警模块，用于当检测到视频数据中包含无法确定人员身份信息的可疑人员时，生成告警信息。

[0121] 定位模块，用于根据人员身份信息及视频数据对各个人员进行定位，并生成与人

员身份信息对应的位置记录信息。

[0122] 告警模块,还用于当检测到位置记录信息中出现可疑位置时,标记出现可疑位置的人员身份信息为可疑人员,并生成告警信息。

[0123] 在一个实施例中,告警模块,还用于确定可疑人员的当前位置信息,并根据当前位置信息生成告警信息,告警信息用于在显示设备中显示可疑人员的当前位置信息,并播放包含可疑人员的视频数据。

[0124] 在本申请实施例中,可通过对视频数据进行人脸识别,确定每个视频数据中包含的人员身份信息,以检测可疑人员,可保证整个数据中心的人员安全性。

[0125] 在一个实施例中,上述安全监控系统600除了包括接收模块610、特征提取模块620、匹配模块630、权限判断模块640、发送模块650、任务获取模块、采集模块、告警模块及定位模块,还包括监控模块。

[0126] 采集模块,用于采集一个或多个环境安全设备的设备参数。

[0127] 监控模块,用于根据设备参数对环境安全进行监控。

[0128] 告警模块,还用于当检测到出现环境安全隐患时,定位存在安全隐患的环境位置,并生成告警信息。

[0129] 在本申请实施例中,还可对环境安全进行监控,提高安全性。

[0130] 图7为一个实施例中电子设备的结构框图。如图7所示,在一个实施例中,该电子设备700可以是服务器,也可以是计算机等终端。电子设备700可以包括一个或多个如下部件:处理器710和存储器720,存储器720可存储有一个或多个应用程序,一个或多个应用程序可以被配置为由一个或多个处理器710执行,一个或多个程序配置用于执行如上述的方法。

[0131] 处理器710可以包括一个或者多个处理核。处理器710利用各种接口和线路连接整个电子设备700内的各个部分,通过运行或执行存储在存储器720内的指令、程序、代码集或指令集,以及调用存储在存储器720内的数据,执行电子设备700的各种功能和处理数据。可选地,处理器710可以采用数字信号处理(Digital Signal Processing,DSP)、现场可编程门阵列(Field—Programmable Gate Array,FPGA)、可编程逻辑阵列(Programmable Logic Array,PLA)中的至少一种硬件形式来实现。处理器710可集成中央处理器(Central Processing Unit,CPU)、图像处理器(Graphics Processing Unit,GPU)和调制解调器等中的一种或几种的组合。其中,CPU主要处理操作系统、用户界面和应用程序等;GPU用于负责显示内容的渲染和绘制;调制解调器用于处理无线通信。可以理解的是,上述调制解调器也可以不集成到处理器710中,单独通过一块通信芯片进行实现。

[0132] 存储器720可以包括随机存储器(Random Access Memory,RAM),也可以包括只读存储器(Read-Only Memory)。存储器720可用于存储指令、程序、代码、代码集或指令集。存储器720可包括存储程序区和存储数据区,其中,存储程序区可存储用于实现操作系统的指令、用于实现至少一个功能的指令(比如触控功能、声音播放功能、图像播放功能等)、用于实现上述各个方法实施例的指令等。存储数据区还可以存储电子设备700在使用中所创建的数据等。

[0133] 可以理解地,电子设备700可包括比上述结构框图中更多或更少的结构元件,在此不进行限定。

[0134] 在一个实施例中,还提供一种计算机可读存储介质,其上存储有计算机程序,计算

机程序被处理器执行时实现如上述实施例描述的方法。

[0135] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一非易失性计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)等。

[0136] 如此处所使用的对存储器、存储、数据库或其它介质的任何引用可包括非易失性和/或易失性存储器。合适的非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM),它用作外部高速缓冲存储器。作为说明而非局限,RAM以多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDR SDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)。

[0137] 以上已经描述了本发明的各实施例,上述说明是示例性的,并非穷尽性的,并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下,对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择,旨在最好地解释各实施例的原理、实际应用或对市场中的技术改进,或者使本技术领域的其它普通技术人员能理解本文披露的各实施例。

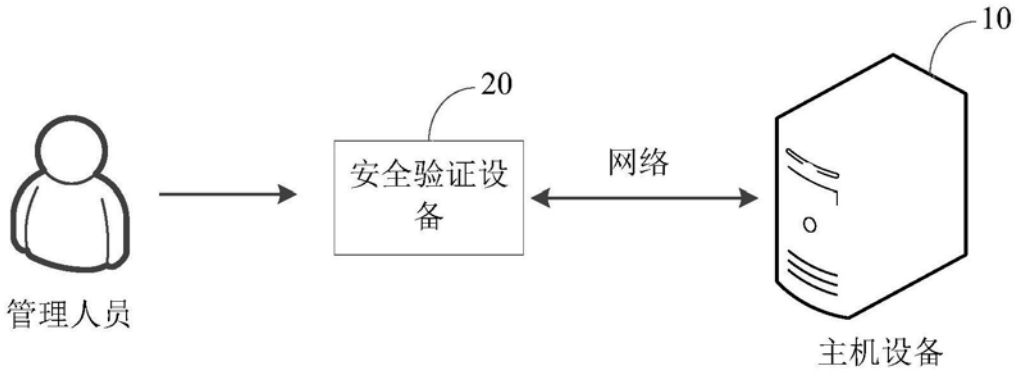

10
20
安全验证设备
网络
管理人员
主机设备

图1

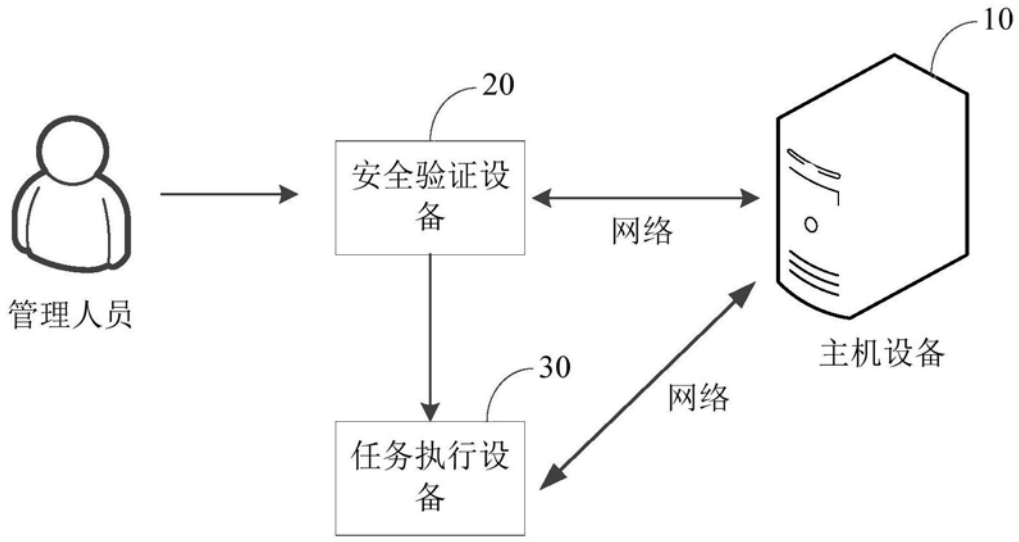

10
20
安全验证设备
网络
管理人员
主机设备
30
网络
任务执行设备

图2

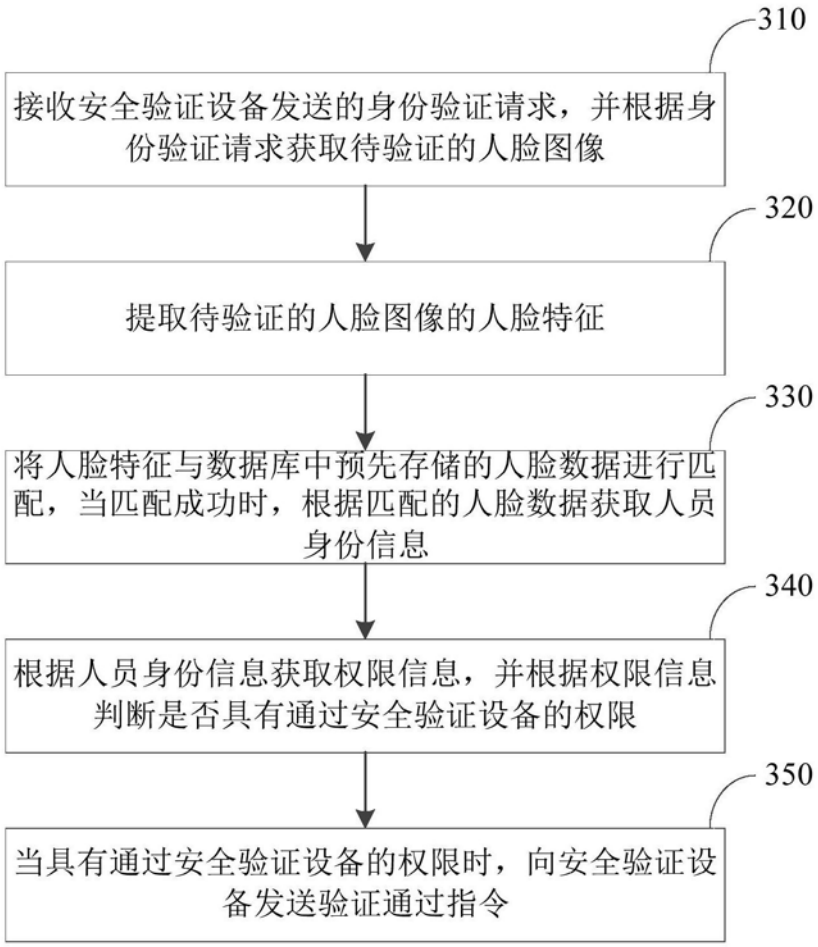

310
接收安全验证设备发送的身份验证请求，并根据身份验证请求获取待验证的人脸图像
320
提取待验证的人脸图像的人脸特征
330
将人脸特征与数据库中预先存储的人脸数据进行匹配，当匹配成功时，根据匹配的人脸数据获取人员身份信息
340
根据人员身份信息获取权限信息，并根据权限信息判断是否具有通过安全验证设备的权限
350
当具有通过安全验证设备的权限时，向安全验证设备发送验证通过指令

图3

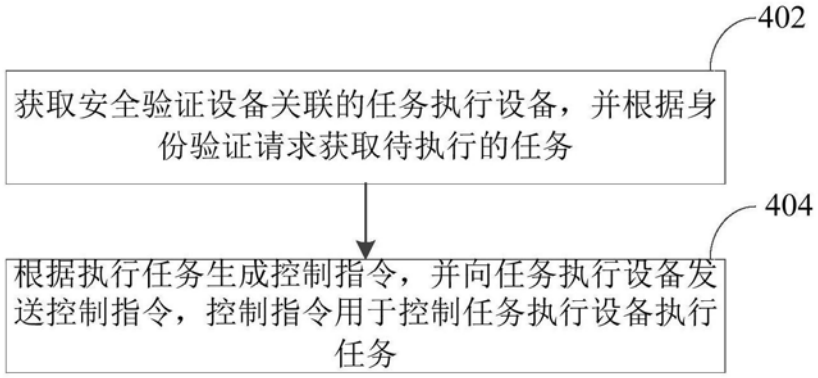

402
获取安全验证设备关联的任务执行设备，并根据身份验证请求获取待执行的任务
404
根据执行任务生成控制指令，并向任务执行设备发送控制指令，控制指令用于控制任务执行设备执行任务

图4

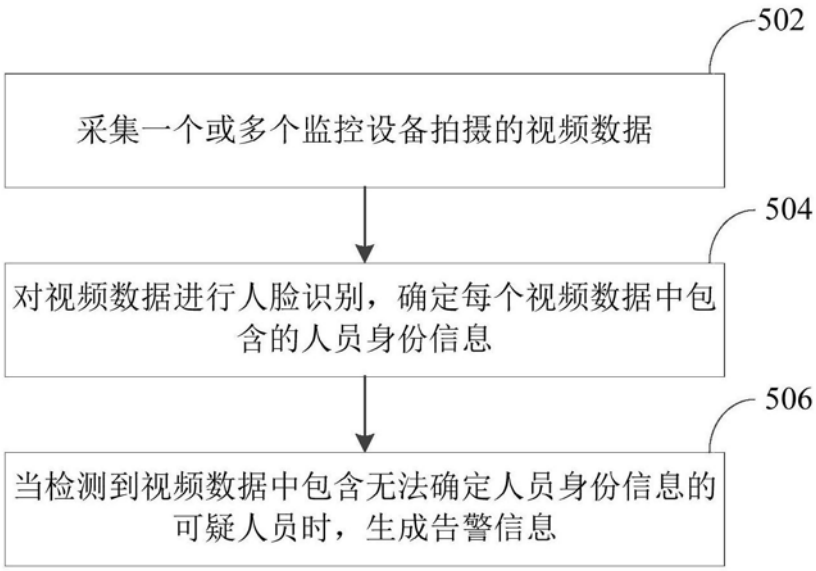

502
采集一个或多个监控设备拍摄的视频数据
504
对视频数据进行人脸识别，确定每个视频数据中包含的人员身份信息
506
当检测到视频数据中包含无法确定人员身份信息的可疑人员时，生成告警信息

图5

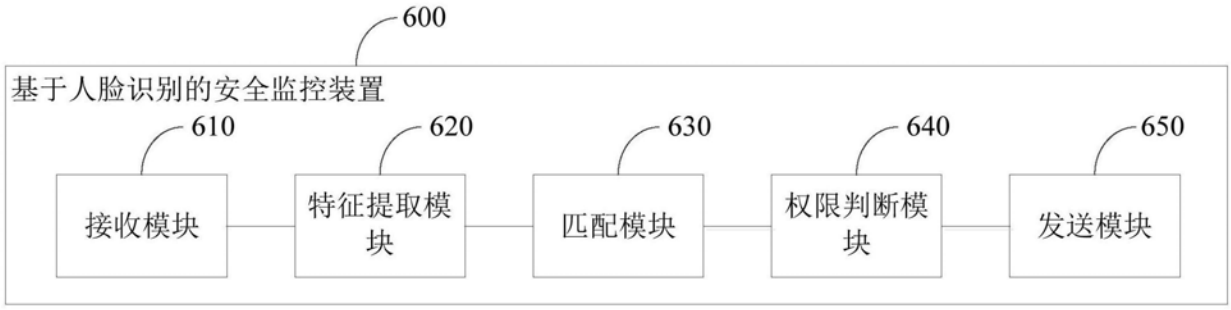

600
基于人脸识别的安全监控装置
610
接收模块
620
特征提取模块
630
匹配模块
640
权限判断模块
650
发送模块

图6

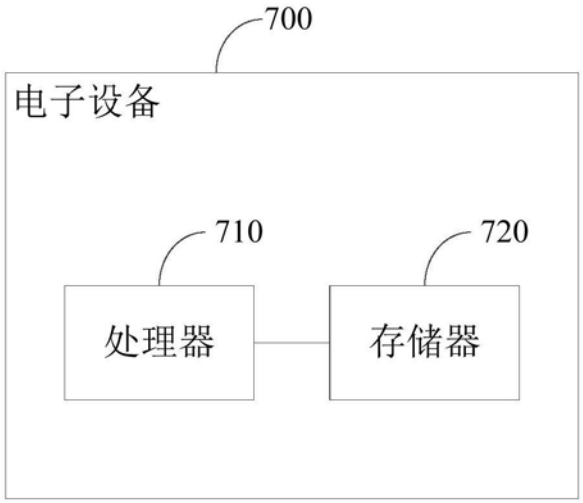

700
电子设备
710
处理器
720
存储器

图7