



## (12)发明专利申请

(10)申请公布号 CN 106856018 A

(43)申请公布日 2017.06.16

(21)申请号 201611190440.3

(22)申请日 2016.12.21

(71)申请人 英业达科技有限公司

地址 201114 上海市闵行区漕河泾出口加工区浦星路789号

申请人 英业达集团(北京)电子技术有限公司  
英业达股份有限公司

(72)发明人 邱全成

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315

代理人 许志勇

(51)Int.Cl.

G07C 9/00(2006.01)

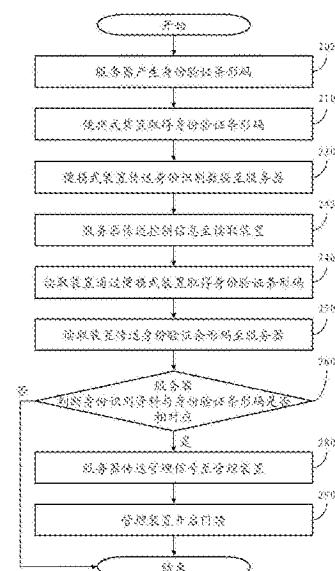
权利要求书2页 说明书8页 附图3页

(54)发明名称

传递身份数据以控制门禁的系统及其方法

(57)摘要

本发明涉及一种传递身份数据以控制门禁的系统及其方法,通过便携式装置直接将身份识别数据传送到服务器,并间接地通过读取装置将身份验证条形码传送到服务器,使得服务器依据便携式装置所传送的身份识别数据以及读取装置所传送的身份验证条形码判断是否产生管理信号并传送给管理装置开启门禁的技术手段,可以避免遗失电子门禁系统的卡片便无法通过门禁系统,并达成提高门禁系统的安全性的技术效果。



1. 一种传递身份数据以控制门禁的方法,所述方法至少包括下列步骤:  
服务器产生身份验证条形码;  
便携式装置取得所述身份验证条形码;  
所述便携式装置传送身份识别数据至所述服务器;  
所述服务器传送控制信息至读取装置,使所述读取装置通过所述便携式装置取得所述身份验证条形码;  
所述读取装置传送所述身份验证条形码至所述服务器;  
所述服务器判断所述身份识别数据与所述身份验证条形码相对应时,传送管理信号至管理装置;以及  
所述管理装置开启门禁。
2. 如权利要求1所述的传递身份数据以控制门禁的方法,其中所述读取装置通过所述便携式装置取得所述身份验证条形码的步骤为:所述读取装置截取所述便携式装置所显示的所述身份验证条形码,或所述读取装置通过无线通信技术接收所述便携式装置所传送的所述身份验证条形码。
3. 如权利要求1所述的传递身份数据以控制门禁的方法,其中所述便携式装置传送所述身份识别数据至所述服务器的步骤为:所述便携式装置拨打电话至所述服务器,使所述服务器将所述便携式装置的手机号码设为所述身份识别数据,或所述便携式装置拨打电话至所述服务器后,通过所述服务器提供的互动语音系统传送所述身份识别数据至所述服务器。
4. 如权利要求1所述的传递身份数据以控制门禁的方法,其中所述方法在所述服务器传送所述控制信息至所述读取装置的步骤之前还包括:所述便携式装置传送所述读取装置的装置识别数据至所述服务器的步骤。
5. 如权利要求1所述的传递身份数据以控制门禁的方法,其中所述方法在所述服务器传送所述管理信号至所述管理装置的步骤之前还包括:所述服务器传送公告信息至所述便携式装置,并判断所述便携式装置是否开启并显示所述公告信息的步骤。
6. 一种传递身份数据以控制门禁的系统,所述系统至少包括:  
便携式装置,用于取得身份验证条形码;  
读取装置;  
服务器,用于接收所述便携式装置所传送的身份识别数据,并传送控制信息至所述读取装置,使所述读取装置通过所述便携式装置取得所述身份验证条形码,并传送所述身份验证条形码至所述服务器,以及用于判断所述身份识别数据与所述身份验证条形码相对应时,产生管理信号;以及  
管理装置,用于在接收到所述管理信号时开启门禁。
7. 如权利要求6所述的传递身份数据以控制门禁的系统,其中所述读取装置截取所述便携式装置所显示的所述身份验证条形码,或通过无线通信技术接收所述便携式装置所传送的所述身份验证条形码。
8. 如权利要求6所述的传递身份数据以控制门禁的系统,其中所述便携式装置是拨打电话至所述服务器,使所述服务器将所述便携式装置的手机号码作为所述身份识别数据,或拨打电话至所述服务器后,通过所述服务器提供的互动语音系统传送所述身份识别数据

至所述服务器。

9. 如权利要求6所述的传递身份数据以控制门禁的系统，其中所述服务器还用于产生与所述身份识别数据对应的新身份验证条形码，且所述便携式装置还用于获取所述新身份验证条形码。

10. 如权利要求6所述的传递身份数据以控制门禁的系统，其中所述服务器还用于传送公告信息至所述便携式装置，并判断所述便携式装置开启并显示所述公告信息时产生所述管理信号。

## 传递身份数据以控制门禁的系统及其方法

### 技术领域

[0001] 本发明涉及一种门禁控制系统及其方法,特别是一种传递身份数据以控制门禁的系统及其方法。

### 背景技术

[0002] 传统门锁是最常见的门禁装置,具有简单、易安装、以及不需电力的优点。同时,在开门的钥匙遗失时,也可以找到开锁的人员打开门锁。但门锁的缺点是钥匙容易遗失,且容易被有经验的小偷轻易地打开。

[0003] 为了避免钥匙遗失的麻烦,以及增加小偷打开门锁的困难度,随着科技的发展,目前电子锁逐渐普及,尤其在有一定出入人数的住宅或办公室等地方几乎都会安装电子锁。目前电子锁大致可分为按键式密码锁、芯片式电子锁、以及磁卡式电子锁三大类。其中,按键式密码锁具有不用携带钥匙与不会遗失钥匙的优点,但密码锁价格高昂,且保密性不佳,容易遭到窃贼侧录或偷窥密码,被通过门禁的风险依然不低;而芯片式电子锁与磁卡式电子锁虽然具有较好保密性的优点,但缺点在于当芯片卡或磁卡等卡片遗失时,用户便无法通过门禁系统,同时也需要更换电子锁的密码,且其他卡片的持有者也需要更新卡片,否则其他卡片持有者也无法通过门禁系统,这将造成其他卡片持有者的困扰。

[0004] 综上所述,可知现有技术中长期以来一直存在遗失电子门禁系统的卡片便无法通过门禁系统的问题,因此有必要提出一种改进的技术手段,来解决这一问题。

### 发明内容

[0005] 有鉴于现有技术存在遗失电子门禁系统的卡片便无法通过门禁系统的问题,本发明公开了一种传递身份数据以控制门禁的系统及其方法,其中:

[0006] 本发明所公开的传递身份数据以控制门禁的系统,至少包括:便携式装置,用于获取得身份验证条形码;读取装置;服务器,用于接收便携式装置所传送的身份识别数据,并传送控制信息至读取装置,使读取装置通过便携式装置取得身份验证条形码,并传送身份验证条形码至服务器,以及用于判断身份识别数据与身份验证条形码相对应时,产生管理信号;管理装置,用于于接收到管理信号时开启门禁。

[0007] 本发明所公开的传递身份数据以控制门禁的方法,其步骤至少包括:服务器产生身份验证条形码;便携式装置获取得身份验证条形码;便携式装置传送身份识别数据至服务器;服务器传送控制信息至读取装置,使读取装置通过便携式装置取得身份验证条形码;读取装置传送身份验证条形码至服务器;服务器判断身份识别数据与身份验证条形码相对应时,传送管理信号至管理装置;管理装置开启门禁。

[0008] 本发明所公开的系统与方法如上,与现有技术之间的差异在于本发明通过便携式装置直接将身份识别数据传送到服务器,并间接地通过读取装置将身份验证条形码传送到服务器,使得服务器依据便携式装置所传送的身份识别数据以及读取装置所传送的身份验证条形码判断是否产生管理信号并传送给管理装置开启门禁,由此解决现有技术所存在的

问题，并可以达成提高门禁系统的安全性的技术效果。

## 附图说明

- [0009] 图1为本发明所述的传递身份数据以控制门禁的系统架构图。
- [0010] 图2A为本发明所述的传递身份数据以控制门禁的方法流程图。
- [0011] 图2B为本发明所述的传送公告信息的附加方法流程图。
- [0012] 附图标记列表
- [0013] 110 便携式装置
- [0014] 120 读取装置
- [0015] 130 服务器
- [0016] 140 管理装置

## 具体实施方式

[0017] 以下将配合附图和实施例来详细说明本发明的特征和实施方式，这些内容足以使任何本领域技术人员能够轻易地充分理解本发明解决技术问题所应用的技术手段并据以实施，由此实现本发明可达成的效果。

[0018] 本发明可以提供通过便携式装置与门禁系统的服务器及读取装置通信，使得服务器判断便携式装置的持有者通过身份认证而控制门禁开启，不再需要钥匙或感应卡。

[0019] 以下先以图1中本发明所述的传递身份数据以控制门禁的系统架构图来说明本发明的系统运作。如图1所示，本发明的系统包括便携式装置110、读取装置120、服务器130和管理装置140。读取装置120可能并不只一个，也就是说本发明的系统可能包括一个或多个读取装置120。

[0020] 便携式装置110可以与服务器130通信，且可以显示数据或可以传送数据给近端装置的装置。便携式装置110包括但不限于手机、平板计算机、笔记本电脑等。

[0021] 便携式装置110负责取得身份验证条形码。便携式装置110所取得的身份验证条形码可以是一维条形码或二维条形码，本发明没有特别的限制。便携式装置110所取得的身份验证条形码也不一定是唯一的，也就是说，不同的便携式装置110可能在同一时间取得相同的身份验证条形码。另外，在部分的实施例中，便携式装置110所取得的身份验证条形码只能使用一次。换句话说，便携式装置110每一次都需要取得不同的身份验证条形码。

[0022] 便携式装置110可以由所包括的储存介质(图中未示)中读取身份验证条形码，但本发明并不局限于以上方式。便携式装置110也可以联机到特定的网络储存空间，例如电子邮箱或网络硬盘，由此下载身份验证条形码。例如，便携式装置110可以从服务器130所传送的多媒体短信中读取出身份验证条形码、也可以从服务器130所传送的电子邮件中读取出身份验证条形码。

[0023] 在部分的实施例中，如果便携式装置110通过服务器130的认证，便携式装置110也可以联机到服务器130下载身份验证条形码，例如，便携式装置110可以将足以让服务器130确认是便携式装置110的识别数据传送给服务器130，并在服务器130确认识别数据正确后，由服务器130下载身份验证条形码，但服务器130认证便携式装置110的方式并不局限于此。其中，上述便携式装置110的识别数据可以是便携式装置110的机身编号、电话号码等足以

代表便携式装置110或便携式装置110的持有者的数据,但本发明并不局限于此。

[0024] 便携式装置110还负责传送身份识别数据至服务器130。其中,上述身份识别数据可以由任意数量的字母或数字任意排列而成,且与便携式装置110的持有者对应,可以代表便携式装置110的持有者,例如,身份识别数据可以是便携式装置110的识别数据、或是便携式装置110的持有者对应服务器130的账号密码等。

[0025] 便携式装置110可以通过电话网络、移动通信网络或无线网络等方式与服务器130连接,由此传送数据或信号至服务器130或接收服务器130所传送的数据或信号,但本发明并不局限于以上方式。举例而言,便携式装置110可以将手机号码作为身份识别数据,例如,便携式装置110可以拨打电话或传送短信至服务器130,使手机号码随着电话信号或短信被传送到服务器130。便携式装置110也可以使用电话网络或使用移动通信网络或无线网络加上拨号应用程序,拨打电话给服务器130,并通过服务器130在电话中所提供的互动语音系统(IVR)将身份识别数据传送给服务器130。便携式装置110也可以通过移动通信网络或无线网络与服务器130直接联机,由此通过互联网将身份识别数据传送给服务器130。

[0026] 另外,便携式装置110也可以将读取装置120的装置识别数据传送到服务器130。一般而言,便携式装置110可以在传送身份识别数据的当次联机中一并传送读取装置120的装置识别数据。读取装置120的装置识别数据通常是由便携式装置110的持有者输入至便携式装置110,但本发明并不局限于以上方式,例如,便携式装置110也可以通过所包括的影像截取单元以及影像识别单元截取并识别读取装置120的装置识别数据。其中,读取装置120的装置识别数据将于稍后进行说明。

[0027] 便携式装置110也可以接收并显示服务器130所传送的错误信息。一般而言,便携式装置110接收自服务器130的错误信息可以表示服务器130无法开启门禁的原因。其中,便携式装置110所接收到的错误信息可以由任意数量的文字、数字或符号等字符任意排列产生,也就是说,便携式装置110所接收到的错误信息可能是一组错误码,也可以是一段文字说明。

[0028] 举例来说,便携式装置110可以接收包括错误信息的短信,也可以通过服务器130所提供的互动语音系统接收到包括错误信息的语音,或是接收到服务器130通过互联网所传送的包括错误信息的数据等。

[0029] 便携式装置110也可以接收服务器130所传送的公告信息,以及开启并显示所接收到的公告信息给便携式装置110的持有者阅读。同时,便携式装置110在开启所接收到的公告信息时,也可以传送通知信息给服务器130,使得服务器130了解公告信息已被便携式装置110的持有者读取。

[0030] 读取装置120与服务器130连接。其中,读取装置120可以通过信号线或电源线等连接线、互联网、或电话网络与服务器130连接,但读取装置120与服务器130的连接方式并没有特别的限制。

[0031] 一般而言,读取装置120被设置在本发明所控制的门扇周围一定距离内,但本发明并不局限于此。在部分的实施例中,读取装置120可能具有装置识别数据或与装置识别数据对应,且读取装置120所具有或与读取装置120对应的装置识别数据可以被标示于读取装置120上或标示在读取装置120的周围。每一个装置识别数据可以表示特定的读取装置120,也就是不同的读取装置120通常具有不同的装置识别数据或与不同的装置识别数据对应。其

中,上述的装置识别数据可以由任意数量的字母或数字等字符任意排列而成。

[0032] 读取装置120负责通过便携式装置110取得身份验证条形码。读取装置120可以通过所包括的影像截取单元(图中未示)截取被便携式装置110的显示屏显示的身份验证条形码,也可以通过蓝牙(Bluetooth)或近场通信(Near Field Communication,NFC)等无线通信技术接收便携式装置110传送的身份验证条形码,但读取装置120通过便携式装置110取得身份验证条形码的方式并不局限于此。

[0033] 读取装置120还负责接收服务器130所传送的控制信息,并将所取得的身份验证条形码传送到服务器130。读取装置120所接收到的控制信息可以是数据或信号的形式,但本发明没有特别的限制,任何可以让读取装置120了解需要将取得自便携式装置110的身份验证条形码传回服务器130的方式都可以在本发明中被使用。

[0034] 读取装置120可以在接收到服务器130所传送的控制信息后,通过便携式装置110取得身份验证条形码,并将所取得的身份验证条形码所送至服务器130。读取装置120也可以在接收到服务器130所传送的控制信息前便先通过便携式装置110取得身份验证条形码,并可以在接收到服务器130所传送的控制信息后,将取得自便携式装置110的身份验证条形码传至服务器130。

[0035] 服务器130负责接收便携式装置110所传送的身份识别数据。服务器130可以通过电话网络、移动通信网络或无线网络等方式与便携式装置110连接,由此传送数据或信号至便携式装置110或接收便携式装置110所传送的数据或信号,但本发明并不局限于以上方式。

[0036] 在部分的实施例中,服务器130可以在接收到身份识别数据后,先验证所接收到的身份识别数据是否合法,若不合法,则可以忽略所接收到的身份识别数据,也就是视同没有接收到身份识别数据。例如,服务器130可以在预先建立的合法名单中搜寻所接收到的身份识别数据,若有在合法名单中搜寻到所接收到的身份识别资料,表示所接收到的身份识别资料合法,反之,则表示所接收到的身份识别资料不合法。

[0037] 服务器130还负责在接收到便携式装置110所传送的身份识别数据后,传送控制信息到读取装置120。在部分的实施例中,服务器130可能同时与多个读取装置120连接,如此,服务器130可以接收便携式装置110所传送的读取装置120的装置识别数据,并传送控制信息给具有所接收到的装置标识符的读取装置或与所接收到的装置识别数据相对应的读取装置120。

[0038] 服务器130还负责接收读取装置120所传送的身份验证条形码,并判断所接收到的身份识别数据与所接收到的身份验证条形码是否相对应。一般而言,服务器130可以在预先建立的对应资料中搜寻是否存在同时符合所接收到的身份识别数据与所接收到的身份验证条形码的记录,例如,服务器130可以从预先建立的对应资料中读出符合所接收到的身份识别数据的所有记录,并比对所读出的记录中是否有符合所接收到的身份验证条形码的记录。若有同时符合所接收到的身份识别数据与所接收到的身份验证条形码的记录存在,则表示所接收到的身份识别数据与所接收到的身份验证条形码相对应,反之,若服务器130预先建立的对应数据中不存在同时符合所接收到的身份识别数据与所接收到的身份验证条形码的记录,表示所接收到的身份识别数据与所接收到的身份验证条形码不对应。但服务器130判断所接收到的身份识别数据与所接收到的身份验证条形码是否相对应的方式并不

局限于以上方式。

[0039] 当服务器130所接收到的身份识别数据与所接收到的身份验证条形码不对应时，服务器130可以产生相对应的错误信息，并传送错误信息给便携式装置110，服务器130也可以不进行任何动作，本发明并没有特别的限制，但服务器130不会传送管理信号至管理装置140。其中，上述管理信号可以是信号或数据的形式，本发明并没有特别的限制，任何可以用来表示开启门禁的方式都可以在本发明中被使用。

[0040] 服务器130还负责在所接收到的身份识别数据与所接收到的身份验证条形码相对应时，产生管理信号，并传送所产生的管理信号给管理装置140。其中，服务器130可以通过信号线或电源线等连接线、互联网、或电话网络与服务器130连接，但服务器130与管理装置140连接的方式并没有特别的限制。

[0041] 在部分的实施例中，服务器130可以在每一次判断所接收到的身份识别数据与所接收到的身份验证条形码相对应时，产生一个新的与所接收到的身份识别数据相对应的身份验证条形码，并将所产生的新身份验证条形码传送到便携式装置110。同时，服务器130也可以更新用来判断所接收到的身份识别数据与所接收到的身份验证条形码是否相对应的对应资料。

[0042] 服务器130也可以传送公告信息到便携式装置110。一般而言，服务器130所传送的公告信息是由任意数量的文字、字母、数字、符号等字符任意排列产生，且公告信息通常是由服务器130的管理者输入或上传至服务器130，但本发明并不局限于以上方式。

[0043] 在部分的实施例中，服务器130也可以判断便携式装置110是否开启并显示公告信息，并在判断出便携式装置110已开启并显示公告信息后，才产生传送到管理装置140的管理信号。一般而言，服务器130可以接收便携式装置110在开启并显示公告信息时所传送的通知信息，并在接收到便携式装置110所传送的通知信息时判断便携式装置110已开启并显示公告信息。

[0044] 管理装置140负责在接收到服务器130所传送的管理信号时，开启门禁。一般而言，管理装置140通常被设置在本发明所控制的门扇周围一定距离内，且管理装置140通常与本发明所控制的门扇通过电线连接，但本发明并不局限于以上方式。

[0045] 接着以第一实施例来解说本发明的运作系统与方法，并请参照图2A中的本发明所述的传递身份数据以控制门禁的方法流程图。在本实施例中，假设便携式装置110为智能手机，但本发明并不局限于此。

[0046] 当用户来到使用本发明的门禁系统前时，用户可以操作便携式装置110取得服务器130所产生的身份验证条形码(步骤202、步骤210)。在本实施例中，假设用户已预先操作便携式装置110或其他装置联机至服务器130通过身份验证并登录所使用的电子邮件账号，服务器130可以加载用户预先登录的电子邮件账号并将所产生的身份验证条形码通过电子邮件传送到用户的电子邮件服务器，用户可以操作便携式装置110联机到电子邮件服务器下载服务器130所传送的电子邮件，并读取包括所下载的电子邮件中的身份验证条形码。

[0047] 在实践中，用户可以在来到使用本发明的门禁系统之前，操作便携式装置110预先取得身份验证条形码，例如，用户可以在前一次通过门禁系统回到家中后便操作便携式装置110取得身份验证条形码，本发明并没有特别的限制。

[0048] 在便携式装置110取得身份验证条形码(步骤210)后，便携式装置110可以将身份

识别数据传送到服务器130(步骤220)。在本实施例中,假设身份识别数据为便携式装置110的电话号码,用户可以操作便携式装置110拨打电话给服务器130所提供的互动语音系统,使得服务器130可以由互动语音系统所接收到的电话响铃信号取得便携式装置110的电话号码,并接通电话。

[0049] 在服务器130取得便携式装置110所传送的身份识别数据后,服务器130可以产生控制信息并传送所产生的控制信息到读取装置120(步骤242)。在本实施例中,假设服务器130可以在传送控制信息到读取装置120后,通过互动语音系统提示用户使用便携式装置110将身份验证条形码提供给读取装置120。但如果服务器130与多个读取装置120连接,则服务器130所提供的互动语音系统在接通电话后,可以提示用户输入读取装置120的装置识别数据,用户可以将被标示在读取装置120的面板上的装置识别数据输入便携式装置110,使得便携式装置110可以通过互动语音系统将读取装置120的装置识别数据传送到服务器130,如此,服务器130可以将控制信息传送给与所接收到的装置识别数据对应的读取装置120。

[0050] 在实践中,如果服务器130有管理一份身份对应表,则服务器130可以在接收到便携式装置110所传送的身份识别数据后,先判断所接收到的身份识别数据是否存在于所管理的身份对应表中,若是,则产生并传送控制信息,但如果服务器判断所接收到的身份识别数据没有存在于所管理的身份对应表中,则服务器130可以通过互动语音系统提示用户身份识别数据不正确,也可以不产生控制信息,或可以不传送任何信息给读取装置120。

[0051] 在读取装置120接收到服务器130所传送的控制信息后,读取装置120可以通过便携式装置110取得身份验证条形码(步骤246),并可以将所取得的身份验证条形码传送到服务器130(步骤250)。在本实施例中,假设用户可以操作便携式装置110在屏幕上显示所取得的身份验证条形码,并将便携式装置110移动到设置于读取装置120的面板上的摄影镜头前方,使得读取装置120可以截取便携式装置110所显示的身份验证条形码。

[0052] 在服务器130接收到读取装置120所传送的身份验证条形码后,服务器130可以判断接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码是否相对应(步骤260)。在本实施例中,服务器130可以在所管理的身份对应表中搜寻同时包括接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码的记录。若服务器130没有在所管理的身份对应表中搜寻到同时包括所接收的身份识别数据与所接收的身份验证条形码的记录,表示接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码没有对应,服务器130可以产生错误信息,并传送所产生的错误信息给便携式装置110,也就是通过互动语音系统将错误信息提示给用户。

[0053] 但如果服务器130在所管理的身份对应表中搜寻到同时包括所接收的身份识别数据与所接收的身份验证条形码的记录,表示接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码相对应,则服务器130可以产生管理信号,并将所产生的管理信号传送到管理装置140(步骤280),管理装置140在接收到服务器130所产生的管理信号后,可以开启门禁。如此,通过本发明,用户将可以使用随身携带的手机等便携式装置110开启门禁,不再需要使用钥匙或感应卡,且由于便携式装置110是使用服务器130所产生的身份验证条形码开启门禁,明显比使用可能被复制的钥匙或感应卡更安全。

[0054] 继续以第二实施例来解说本发明的运作系统与方法,同样请参照图2A。在本实施

例中,同样假设便携式装置110为智能手机。

[0055] 当用户来到使用本发明的门禁系统前时,用户可以操作便携式装置110取得服务器130所产生的身份验证条形码(步骤202、步骤210)。在本实施例中,假设用户可以操作便携式装置110联机服务器130,并在输入账号密码登入服务器130后,下载服务器130所产生的身份验证条形码。

[0056] 在便携式装置110取得身份验证条形码(步骤210)后,便携式装置110可以将身份识别数据传送到服务器130(步骤220)。在本实施例中,若服务器130有管理一份身份对应表,假设在用户操作便携式装置110拨打电话给服务器130所提供的互动语音系统后,互动语音系统可以接通电话,并判断便携式装置110的电话号码不存在于服务器130所管理的身份对应表中后,互动语音系统可以提示用户操作便携式装置110输入身份识别数据,便携式装置110可以将用户所输入的身份识别数据传送到服务器130所提供的互动语音系统。

[0057] 在服务器130取得便携式装置110所传送的身份识别资料后,服务器130可以判断所接收到的身份识别资料是否存在于所管理的身份对应表中,若是,则可以产生控制信息并传送所产生的控制信息到读取装置120(步骤242),并通过互动语音系统提示用户使用便携式装置110将身份验证条形码提供给读取装置120;但如果服务器判断所接收到的身份识别数据没有存在于所管理的身份对应表中,则服务器130可以通过互动语音系统提示用户身份识别数据不正确,并提示用户再次输入身份识别数据,或挂断电话。

[0058] 在读取装置120接收到服务器130所传送的控制信息后,读取装置120可以通过便携式装置110取得身份验证条形码(步骤246),并可以将所取得的身份验证条形码传送到服务器130(步骤250)。在本实施例中,假设用户可以操作便携式装置110使用近场通信将所取得的身份验证条形码传送给读取装置120。

[0059] 在服务器130接收到读取装置120所传送的身份验证条形码后,服务器130可以判断接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码是否相对应(步骤260)。在本实施例中,服务器130可以在所管理的身份对应表中搜寻同时包括接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码的记录。

[0060] 如果服务器130在所管理的身份对应表中搜寻到同时包括所接收的身份识别数据与所接收的身份验证条形码的记录,则服务器130可以判断接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码相对应,并可以产生管理信号,以及将所产生的管理信号传送到管理装置140(步骤280),管理装置140在接收到服务器130所产生的管理信号后,可以开启门禁。如此,通过本发明,用户即使没有携带自己所使用的手机等便携式装置,也可以使用其他人所携带的便携式装置110开启门禁,且由于便携式装置110是通过服务器130的认证后才使用由服务器130提供的身份验证条形码开启门禁,因此,本发明比使用无法认证的钥匙或感应卡更安全。

[0061] 在上述的第一实施例和第二实施例中,在服务器130判断接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码相对应(步骤260)后,服务器130可以如图2B的流程所示,传送公告信息到便携式装置110(步骤271),并判断便携式装置110是否开启并显示所传送的公告信息(步骤275)。在本实施例中,假设便携式装置110可以在开启并显示接收自服务器130的公告信息后,传送通知信息给服务器130,服务器130在接收到便携式装置110所传送的通知信息后,可以判断便携式装置110已开启并显示所传送的公告

信息，并可以产生管理信息，以及将所产生的管理信息传送到管理装置140(步骤280)。

[0062] 此外，在上述第一实施例与第二实施例中，在服务器130判断接收自便携式装置110的身份识别数据与接收自读取装置120的身份验证条形码相对应后，可以产生新身份验证条形码，并通过电子邮件将所产生的新身份验证条形码送到用户的电子邮件服务器，使得用户操作便携式装置110联机到电子邮件服务器下载服务器130所传送的电子邮件，并读取包括所下载的电子邮件中的新身份验证条形码，或是由用户操作便携式装置110成功登入服务器130后，下载服务器130所产生的新身份验证条形码。也就是说，服务器130所产生的身份验证条形码只能使用一次，更加提高门禁系统的安全性。

[0063] 综上所述，可知本发明与现有技术之间的差异在于具有便携式装置直接将身份识别数据传送到服务器，并间接地通过读取装置将身份验证条形码传送到服务器，使得服务器依据便携式装置所传送的身份识别数据以及读取装置所传送的身份验证条形码判断是否产生管理信号并传送给管理装置开启门禁的技术手段，借助这一技术手段可以解决现有技术所存在的遗失电子门禁系统的卡片便无法通过门禁系统的问题，进而达成提高门禁系统安全性的技术效果。

[0064] 再者，本发明的传递身份数据以控制门禁的方法，可实现于硬件、软件或硬件与软件的组合中，也可在计算机系统中以集中方式实现或以不同组件散布于若干互连的计算机系统的分散方式实现。

[0065] 虽然本发明所公开的实施方式如上，但所述的内容并非用于直接限定本发明的专利保护范围。任何本发明所属技术领域中的技术人员，在不脱离本发明所公开的精神和范围的前提下，对本发明的实施的形式上和细节上作些许的改变和修正，均属于本发明的专利保护范围。本发明的专利保护范围，仍须以所附的权利要求所界定的范围为准。

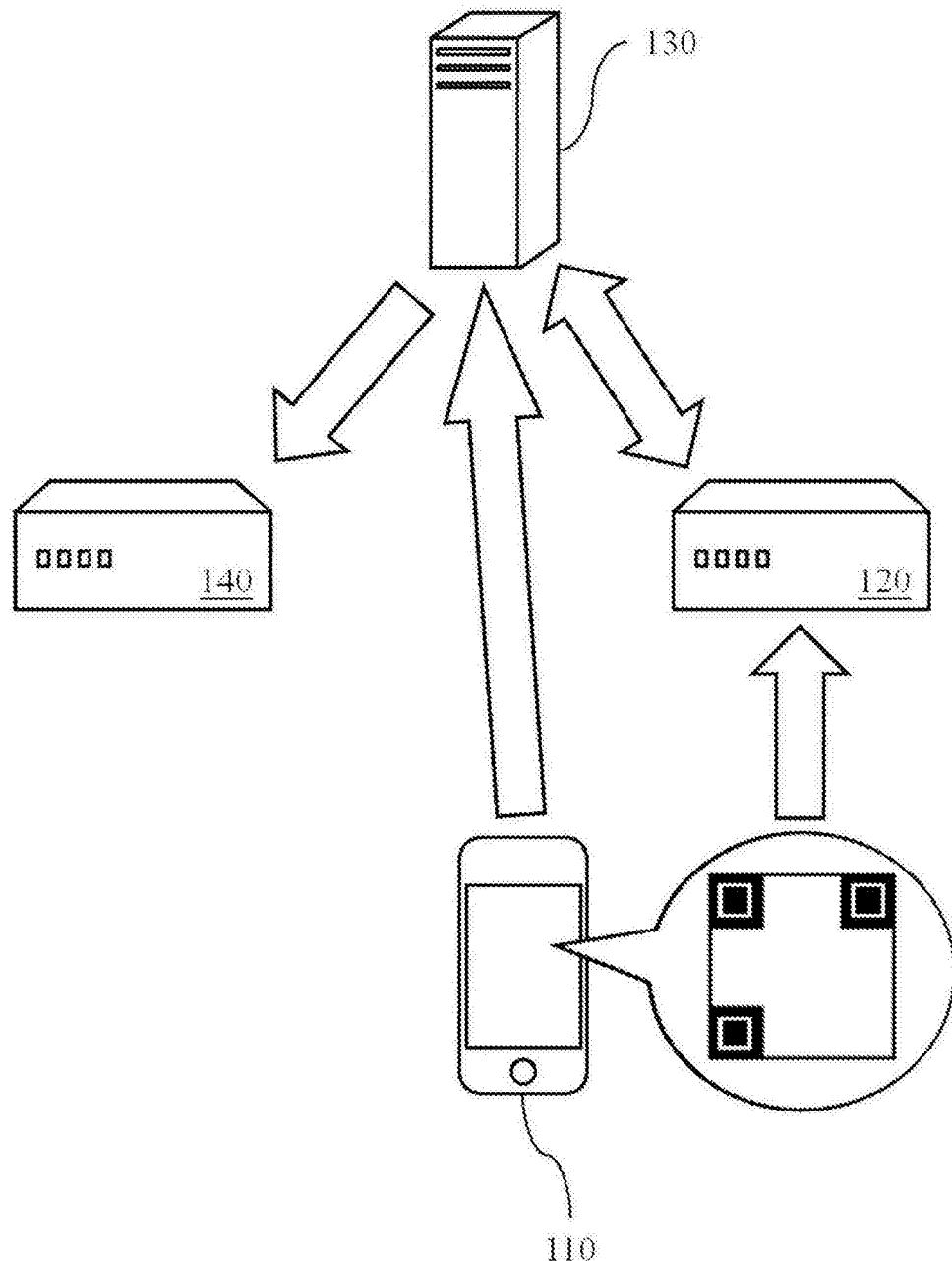


图1

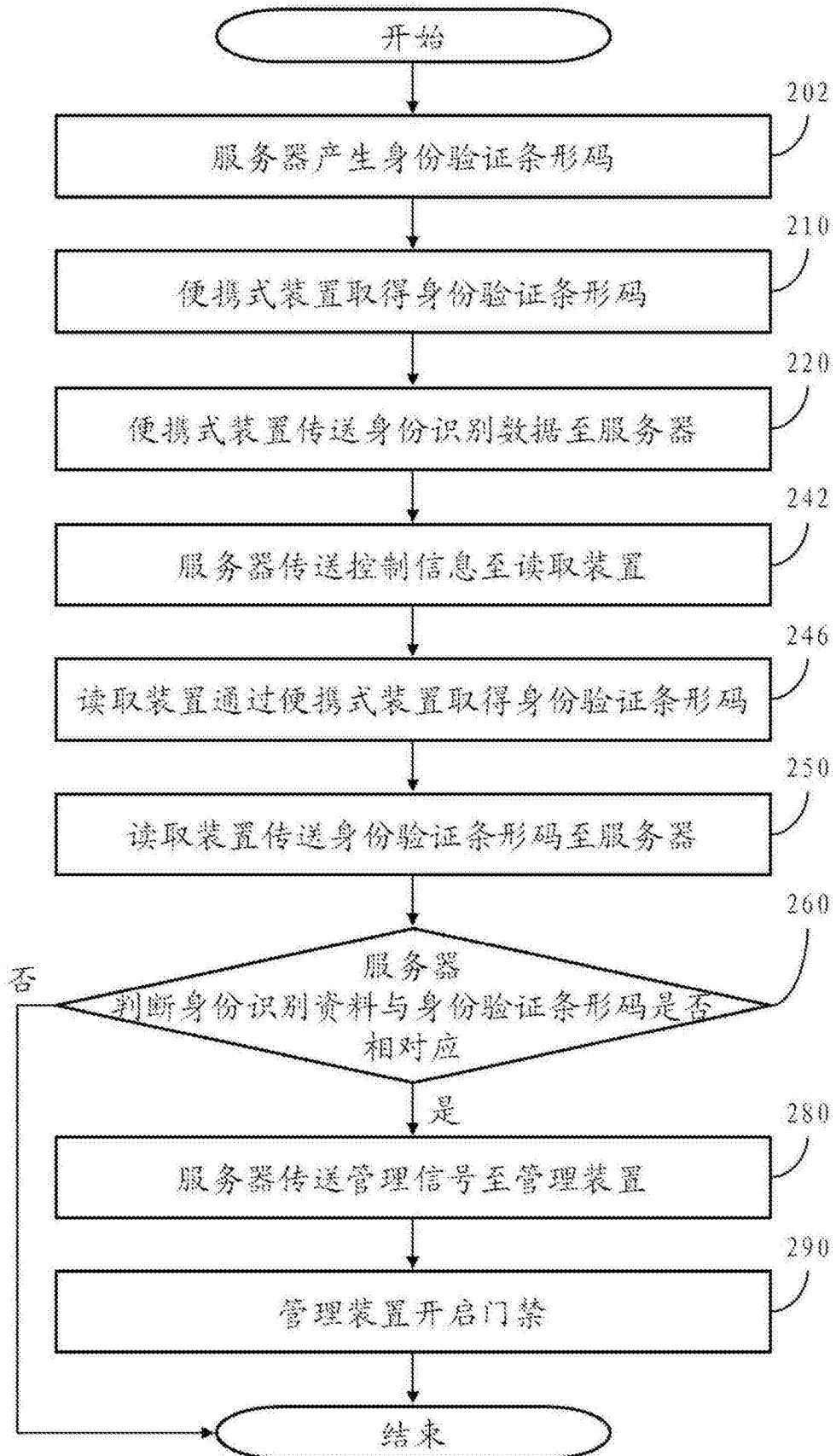


图2A

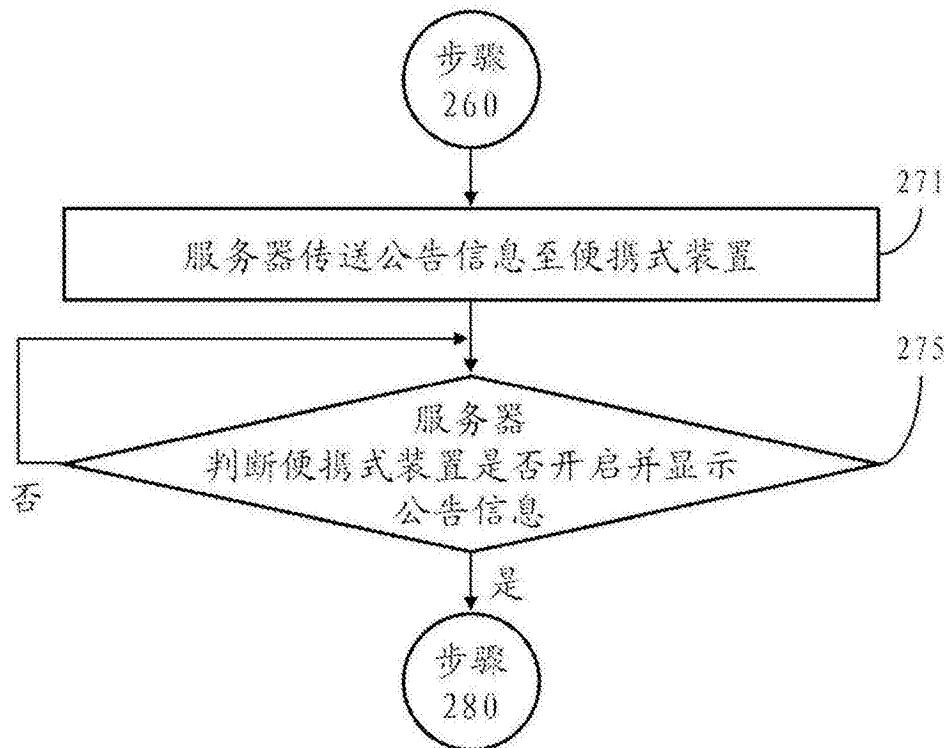


图2B