(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 113678177 A
(43)申请公布日 2021.11.19

(21)申请号 202080025495.7
(22)申请日 2020.10.14
(30)优先权数据
10-2019-0126737 2019.10.14 KR
(85)PCT国际申请进入国家阶段日
2021.09.28
(86)PCT国际申请的申请数据
PCT/KR2020/013966 2020.10.14
(87)PCT国际申请的公布数据
WO2021/075833 KO 2021.04.22
(71)申请人 貂皮技术股份公司
地址 韩国京畿道
(72)发明人 张载淳
(74)专利代理机构 北京弘权知识产权代理有限公司 11363
代理人 许伟群 李少丹
(51)Int.Cl.
G07C 9/00(2020.01)

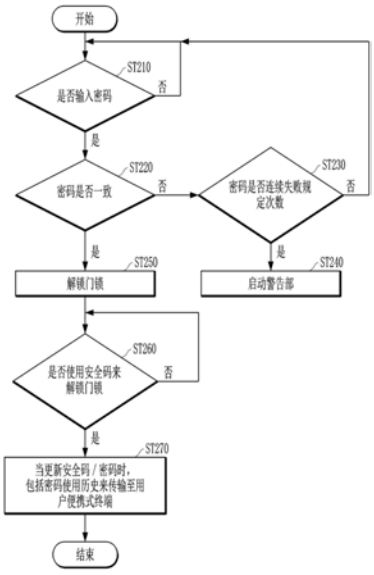
权利要求书4页 说明书13页 附图13页

(54)发明名称

安全性增强门锁及利用该门锁的进出门安全管理系统

(57)摘要

本发明涉及增强安全性的安全性增强门锁及利用该门锁的进出门安全管理系统,可提供存储在用户便携式终端的安全码及用户按键输入密码的双重解锁功能来提高用户便利性,在使用安全码进出后,在门锁本身同时更新安全码和密码,生成互不相同的多个密码,禁止使用过一次的密码的再次使用或者仅在规定时间内允许再次使用,由此,在允许并不拥有存储有安全码的终端的人员的进出的同时防止密码的泄露,便于管理对于包括单身女性家庭的门锁在内的安装在设施中的门锁的多个进出人员,同时,可提供高安全性。



CN 113678177 A

1.一种安全性增强门锁,安装在进出门来对于进出门的开闭进行锁定及解锁,其特征在于,包括:

锁定解锁单元,用于锁定或解锁上述进出门;

小键盘,配置有用于输入密码的多个数字键;

短距离通信模块,通过无线短距离通信网与存储有安全码的用户便携式终端进行通信;

安全码读取部,当上述用户便携式终端进入通信半径内时,读取上述安全码;

密码存储部,用于存储为了开闭上述门锁而设置的上述密码;

安全码存储部,存储用于开闭上述门锁的上述安全码;

锁定解锁控制部,判断在上述安全码读取部中读取的安全码是否与存储在上述安全码存储部的安全码一致或者判断通过上述小键盘输入的密码是否与存储在上述密码存储部的密码一致,在上述安全码一致或上述密码一致的情况下,操作上述锁定解锁单元来将上述进出门切换为解锁状态;以及

安全码/密码更新部,上述锁定解锁控制部判断上述安全码一致来解锁上述锁定解锁单元后,将上述安全码及上述密码均更新并分别存储在上述安全码存储部及上述密码存储部,将更新的安全码及更新的密码传输至上述用户便携式终端。

2.根据权利要求1所述的安全性增强门锁,其特征在于,当更新上述密码时,上述安全码/密码更新部更新为互不相同的多个密码。

3.根据权利要求2所述的安全性增强门锁,其特征在于,使用上述多个密码中的一个来解锁上述锁定解锁单元后,上述锁定解锁控制部废弃相应密码并仅对其他密码执行解锁操作。

4.根据权利要求3所述的安全性增强门锁,其特征在于,上述多个密码均被使用来解锁上述锁定解锁单元后,上述锁定解锁控制部直到下一次更新上述密码为止暂时停止上述密码的使用功能。

5.根据权利要求2所述的安全性增强门锁,其特征在于,使用上述多个密码中的一个来解锁上述锁定解锁单元后,上述锁定解锁控制部将对于相应密码的再次使用时间设置为规定时间内或者将再次使用次数设置为规定次数内,在超出上述再次使用时间或者上述再次使用次数清零后,废弃相应密码并仅对其他密码执行解锁操作。

6.根据权利要求5所述的安全性增强门锁,其特征在于,对于所有上述多个密码,超出上述再次使用时间或者上述再次使用次数清零后,上述锁定解锁控制部直到下一次更新上述密码为止暂时停止上述密码的使用功能。

7.根据权利要求1所述的安全性增强门锁,其特征在于,当更新上述安全码及上述密码并传输至上述用户便携式终端时,上述安全码/密码更新部包括表示上述安全码的使用历史的安全码使用历史信息来传输。

8.根据权利要求7所述的安全性增强门锁,其特征在于,当更新上述安全码及上述密码并传输至上述用户便携式终端时,在存在上述密码的使用历史的情况下,上述安全码/密码更新部包括表示上述密码的使用历史的密码使用历史信息来传输。

9.根据权利要求1所述的安全性增强门锁,其特征在于,上述安全码为电子可读数据,上述密码为表示一串数字的数据,上述安全码/密码更新部向上述用户便携式终端加密传

输更新的上述安全码及更新的上述密码。

10.根据权利要求9所述的安全性增强门锁，其特征在于，当向上述用户便携式终端传输更新的上述安全码及更新的上述密码时，上述安全码/密码更新部包括命令将更新的上述安全码及更新的上述密码中继到远程的安全管理服务器后删除的命令数据来传输。

11.一种进出门安全管理系统，其特征在于，

包括：

安全性增强门锁，包括锁定解锁控制部以及安全码/密码更新部，上述锁定解锁控制部安装在进出门来对于进出门的开闭进行锁定及解锁，判断通过无线短距离通信网从用户便携式终端读取的安全码或用户输入的密码是否与已存储的安全码或密码一致，将上述进出门从锁定状态切换为解锁状态，上述安全码/密码更新部在上述锁定解锁控制部判断上述安全码一致来解锁上述锁定解锁单元后，将上述安全码及上述密码均更新并将更新的安全码及更新的密码传输至上述用户便携式终端；

安全管理服务器，按照上述安全性增强门锁存储并管理上述安全码、上述密码，在通过广域移动通信网从上述用户便携式终端接收上述安全码发布请求或者上述密码发布请求的情况下，进行用户认证过程后，向上述用户便携式终端远程发布上述安全码或上述密码；以及

用户便携式终端，从上述安全性增强门锁接收更新的上述安全码及更新的上述密码并将其中继到上述安全管理服务器，

上述安全管理服务器将从上述用户便携式终端中继的更新的上述安全码及更新的上述密码分别更新在安全码管理数据库及密码管理数据库并管理。

12.根据权利要求11所述的进出门安全管理系统，其特征在于，当更新上述密码时，上述安全码/密码更新部更新互不相同的多个密码。

13.根据权利要求12所述的进出门安全管理系统，其特征在于，使用上述多个密码中的一个来将上述进出门从锁定状态切换为解锁状态后，上述锁定解锁控制部废弃相应密码并仅对其他密码执行解锁操作。

14.根据权利要求13所述的进出门安全管理系统，其特征在于，上述多个密码均被使用而将上述进出门从锁定状态切换为解锁状态后，上述锁定解锁控制部直到下一次更新上述密码为止暂时停止上述密码的使用功能。

15.根据权利要求12所述的进出门安全管理系统，其特征在于，使用上述多个密码中的一个来将上述进出门从锁定状态切换为解锁状态后，上述锁定解锁控制部将对于相应密码的再次使用时间设置为规定时间内或者将再次使用次数设置为规定次数内，在超出上述再次使用时间或者上述再次使用次数清零后，废弃相应密码并仅对其他密码执行解锁操作。

16.根据权利要求15所述的进出门安全管理系统，其特征在于，对于所有上述多个密码，超出上述再次使用时间或者上述再次使用次数清零后，上述锁定解锁控制部直到下一次更新上述密码为止暂时停止上述密码的使用功能。

17.根据权利要求11所述的进出门安全管理系统，其特征在于，当更新上述安全码及上述密码并传输至上述用户便携式终端时，上述安全码/密码更新部包括表示上述安全码的使用历史的安全码使用历史信息来传输，上述安全管理服务器接收通过上述用户便携式终端中继的上述安全码使用历史信息，将其存储在安全历史管理数据库并管理。

18.根据权利要求17所述的进出门安全管理系统，其特征在于，当更新上述安全码及上述密码并传输至上述用户便携式终端时，在存在上述密码的使用历史的情况下，上述安全码/密码更新部包括表示上述密码的使用历史的密码使用历史信息来传输，上述安全管理服务器接收通过上述用户便携式终端中继的上述密码使用历史信息，将其存储在上述安全历史管理数据库并管理。

19.根据权利要求11所述的进出门安全管理系统，其特征在于，上述安全码为电子可读数据，上述密码为表示一串数字的数据，上述安全码/密码更新部向上述用户便携式终端加密传输更新的上述安全码及更新的上述密码。

20.根据权利要求19所述的进出门安全管理系统，其特征在于，上述用户便携式终端将更新的上述安全码及更新的上述密码中继到上述安全管理服务器后在自带的临时存储器中删除其。

21.根据权利要求19所述的进出门安全管理系统，其特征在于，当向上述用户便携式终端传输更新的上述安全码及更新的上述密码时，上述安全码/密码更新部包括命令将更新的上述安全码及更新的上述密码中继到上述安全管理服务器后删除的命令数据来传输。

22.根据权利要求11所述的进出门安全管理系统，其特征在于，

上述用户便携式终端为安装有按照上述安全性增强门锁管理上述安全码或上述密码的使用的门锁管理应用程序的终端，

上述门锁管理应用程序通过上述用户便携式终端上的触摸用户界面提供门锁开启选择按钮，在用户输入上述门锁开启选择按钮的情况下，从上述安全管理服务器接收更新的上述安全码。

23.根据权利要求18所述的进出门安全管理系统，其特征在于，上述用户便携式终端包括管理员便携式终端和访客便携式终端，上述管理员便携式终端与上述安全管理服务器联接来按照上述安全性增强门锁允许上述访客便携式终端是否使用上述安全码。

24.根据权利要求23所述的进出门安全管理系统，其特征在于，当通过用户界面输入对于上述安全性增强门锁的进出记录确认按钮时，上述管理员便携式终端访问上述安全管理服务器来读取上述安全历史管理数据库，按照上述安全性增强门锁向上述管理员便携式终端的画面输出上述安全码使用历史信息及上述密码使用历史信息。

25.根据权利要求13所述的进出门安全管理系统，其特征在于，当通过用户界面输入对于上述安全性增强门锁的密码查看按钮时，上述用户便携式终端在上述用户便携式终端的画面输出依次显示从上述安全管理服务器接收的多个密码的密码查看应用程序页面。

26.根据权利要求25所述的进出门安全管理系统，其特征在于，上述密码查看应用程序页面分别掩蔽来隐藏上述密码，当用户输入与每个上述密码相邻配置的密码查看按钮时，去除上述掩蔽并显示密码。

27.根据权利要求26所述的进出门安全管理系统，其特征在于，上述密码查看应用程序页面还包括与每个上述密码相邻配置的密码共享按钮，当用户输入上述密码共享按钮时，将上述密码传输至预设的或者用户输入的电话号的便携式终端。

28.根据权利要求15所述的进出门安全管理系统，其特征在于，当通过用户界面输入对于上述安全性增强门锁的密码查看按钮时，上述用户便携式终端在上述用户便携式终端的画面输出依次显示从上述安全管理服务器接收的多个密码的密码查看应用程序页面。

29.根据权利要求28所述的进出门安全管理系统，其特征在于，上述密码查看应用程序页面分别掩蔽来隐藏上述密码，当用户输入与每个上述密码相邻配置的密码查看按钮时，去除上述掩蔽并显示密码。

30.根据权利要求29所述的进出门安全管理系统，其特征在于，上述密码查看应用程序页面还包括与每个上述密码相邻配置的密码共享按钮，当用户输入上述密码共享按钮时，将上述密码传输至预设的或者用户输入的电话号的便携式终端。

安全性增强门锁及利用该门锁的进出门安全管理系统

技术领域

[0001] 本发明涉及提供存储在用户便携式终端的安全码及用户输入的密码的双重解锁功能来提高用户便利性并增强安全性的安全性增强门锁以及利用该门锁通用适用于包括单身女性家庭的门锁在内的安装在多个设施的门锁等来容易管理进出人员并以高安全水平执行的进出门安全管理系统。

背景技术

[0002] 通常,门锁为安装在进出门来对于进出门的开闭进行锁定/解锁的装置。普通门锁通过输入密码或读取用户的生物信息来执行锁定及解锁操作。

[0003] 输入密码的方式的门锁较低廉,方便告知其他人(例如,朋友、房东、快递员、抄表员等),但容易通过各种途径泄漏。读取用户生物信息的方式较高昂,未注册人员无法进出,因此具有从根源上阻止了除家庭成员认证的其他人员的进出的问题。作为其他方法,具有通过电子钥匙或电子标签开闭门锁的方式,但因电子钥匙或电子标签容易被盗窃或未经授权的复制等而失能。

[0004] 以2017年为基准,韩国单身女性家庭已超过280万户,预计到2045年将超过380万户。并且,根据韩国统计厅的2016年的调查,单身女性家庭中有46%的女性回答说她们对社会安全感到不安,其中,37%的女性将犯罪列为不安的原因。根据韩国刑事政策研究院的数据,与相同的男性家庭相比,单身女性家庭遭受非法侵入的可能性高11.2倍。并且,根据韩国警察厅,2014年至2017年共发生了7万1868件的非法侵入相关犯罪,在最近4年间,非法侵入的性犯罪共发生1310件,99.8%的加害者为男性。为了构成单身女性家庭的家庭成员,需要加强安全性的同时便于使用的门锁装置。

[0005] 另一方面,安装在地面上的中继器、地面电器设施、路灯配电箱、交通信号控制器等的设施用于与由警察、制造商管理者、维护维修合作公司管理者、地方政府负责人、技术人员等各种人员管理。在这些设施中安装门锁来仅由允许的用户对其进行开闭。通常由多个人员使用过的门锁以通过密码解锁的方式安装,但固定的密码容易泄漏。电子标签或物理钥匙等具有丢失的风险,具有难以管理设施的进出人员的问题。因此,对于由多个用户利用的设施等的门锁也需要高的安全水平,并需要容易管理的新的进出管理系统。

[0006] 韩国授权专利第10-1208744号提出了一种智能安全门锁。在相同的现有文献中,当传输认证的标识(ID)的电子钥匙接近至规定距离内时,若输入安装在门锁的确认按钮,则控制门锁来使其开启。但如上所述,电子钥匙容易丢失,包含在电子钥匙的标识被未经授权的复制的风险高。并且,在用户丢失电子钥匙的情况下,无法开启门锁,需通过特殊程序强制开启门锁,在此过程中,具有耗时相当长的问题。

发明内容

[0007] (发明所要解决的问题)

[0008] 本发明的目的在于,提供如下的安全性增强门锁及利用该门锁的进出门安全管理

系统:增强门锁的安全水平,同时,当更新安全码及密码时,生成互不相同的多个密码,禁止使用过一次的密码的再次使用或者仅在规定时间内允许再次使用,由此允许并不拥有存储有安全码的终端的人员的进出并防止密码的流出。

[0009] (解决问题所采用的措施)

[0010] 本发明一实施例的安全性增强门锁安装在进出门来对于进出门的开闭进行锁定及解锁,其包括:锁定解锁单元,用于锁定或解锁上述进出门;小键盘,配置有用于输入密码的多个数字键;短距离通信模块,通过无线短距离通信网与存储有安全码的用户便携式终端进行通信;安全码读取部,当上述用户便携式终端进入通信半径内时,读取上述安全码;密码存储部,用于存储为了开闭上述门锁而设置的上述密码;安全码存储部,存储用于开闭上述门锁的上述安全码;锁定解锁控制部,判断在上述安全码读取部中读取的安全码是否与存储在上述安全码存储部的安全码一致或者判断通过上述小键盘输入的密码是否与存储在上述密码存储部的密码一致,在上述安全码一致或上述密码一致的情况下,操作上述锁定解锁单元来将上述进出门切换为解锁状态;以及安全码/密码更新部,上述锁定解锁控制部判断上述安全码一致来解锁上述锁定解锁单元后,将上述安全码及上述密码均更新并分别存储在上述安全码存储部及上述密码存储部,将更新的安全码及更新的密码传输至上述用户便携式终端。

[0011] 本发明一实施例的进出门安全管理系统包括:安全性增强门锁,包括锁定解锁控制部以及安全码/密码更新部,上述锁定解锁控制部安装在进出门来对于进出门的开闭进行锁定及解锁,判断通过无线短距离通信网从用户便携式终端读取的安全码或用户输入的密码是否与已存储的安全码或密码一致,将上述进出门从锁定状态切换为解锁状态,上述安全码/密码更新部在上述锁定解锁控制部判断上述安全码一致来解锁上述锁定解锁单元后,将上述安全码及上述密码均更新并将更新的安全码及更新的密码传输至上述用户便携式终端;安全管理服务器,按照上述安全性增强门锁存储并管理上述安全码、上述密码,在通过广域移动通信网从上述用户便携式终端接收上述安全码发布请求或者上述密码发布请求的情况下,进行用户认证过程后,向上述用户便携式终端远程发布上述安全码或上述密码;以及用户便携式终端,从上述安全性增强门锁接收更新的上述安全码及更新的上述密码并将其中继到上述安全管理服务器,上述安全管理服务器将从上述用户便携式终端中继的更新的上述安全码及更新的上述密码分别更新在安全码管理数据库及密码管理数据库并管理。

[0012] (发明的效果)

[0013] 根据本发明的安全性增强门锁及利用该门锁的进出门安全管理系统具有如下的效果:提供存储在用户便携式终端的安全码及用户通过按键输入密码的双重解锁功能来提高用户便利性,在使用安全码进出后,在门锁本身同时更新安全码和密码,生成互不相同的多个密码,禁止使用过一次的密码的再次使用或仅在规定时间内允许再次使用,由此防止密码的泄露,容易管理包括单身女性家庭的门锁在内的安装在设施的门锁的多个进出人员,同时,可提供高安全性。

附图说明

[0014] 图1为例示本发明的安全性增强门锁的框图。

[0015] 图2为示出本发明中的利用安全码的门锁操作例的流程图。

[0016] 图3为示出本发明中的利用密码的门锁操作例的流程图。

[0017] 图4为示出本发明中的使用并废弃多个密码的一例的流程图。

[0018] 图5为示出本发明中的设置密码的使用时间后废弃的一例的流程图。

[0019] 图6为例示本发明的进出门安全管理系统的框图。

[0020] 图7为例示本发明的进出门安全管理方法的数据流程图。

[0021] 图8为例示本发明中的安装在用户便携式终端的门锁管理应用程序的用户认证画面的图。

[0022] 图9为示出本发明中的通过门锁管理应用程序执行门锁开启的例示的图。

[0023] 图10为示出本发明中的通过门锁管理应用程序执行密码查看的例示的图。

[0024] 图11为示出本发明中的通过门锁管理应用程序执行密码使用的例示的图。

[0025] 图12为示出本发明中的通过门锁管理应用程序执行访客管理的例示的图。

[0026] 图13为示出本发明中的通过门锁管理应用程序执行功能设置的例示的图。

具体实施方式

[0027] 参照以下的说明及附图，可更加明确理解本发明的附加目的、特征及优点。

[0028] 在详细说明本发明之前，本发明可谋求各种改变，并且可具有各种实施例，在以下说明并且在附图示出的示例并不是要将本发明限定于特定的实施形态，而是应该理解为包括在本发明的思想及技术范围内包括的所有改变、同等物乃至代替物。

[0029] 在说明某一构件“连接”或者“接触”于另一构件时，可以是直接连接或者接触于其另一构件，但是也应该理解为中间也可存在其他构件。相反，在说明某一构件“直接连接”或者“直接接触”于另一构件时，应该理解为中间不存在其他构件。

[0030] 在本说明书中使用的用语只是为了说明特定的实施例而使用的，并没有要限定本发明的意图。针对单数的表述，除非在文章中有明确定义，否则包括复数的表述。在本说明书中，针对“包括”或者“具有”等的用语，应该理解为只是要指定在说明书上记载的特征、数字、步骤、动作、构件、零部件或者这些的组合的存在，并不提前排出一个或者一个以上的其他特征、数字、步骤、动作、构件、零部件或者这些的组合的存在或者附加可能性。

[0031] 另外，在说明书记载的“…部”、“…单元”、“…模块”等的用语是指处理至少一个功能或者动作的单位，这可通过硬件、软件或者硬件和软件的组合实现。

[0032] 另外，在参照附图的说明中，不论附图标记，针对相同的构件赋予相同的参照附图标记，据此省略重复的说明。在对本发明的说明中，若判断针对相关公知技术的说明使本发明不清楚的情况下，将省略其详细说明。

[0033] 另外，在本原说明书全文中，在某一步骤在另一步骤“上”或者“之前”时，这不仅是某一步骤和另一步骤具有直接的时间序列关系的情况，还包括在两个步骤的顺序上可颠倒时间序列顺序的间接时间序列的情况(诸如，各个步骤之后的混合的步骤)，并且两者具有相同的权利范围。

[0034] 图1为例示本发明的安全性增强门锁的框图。

[0035] 参照图1，本发明的安全性增强门锁由暴露在门锁装置100的外部的小键盘110及手柄120、设置在门锁装置100内部的锁定解锁单元130、警告部140、存储单元150、短距离通

信模块160、安全码读取部170、安全码/密码更新部180以及锁定解锁控制部190构成。

[0036] 在门锁装置100的前表面设置配置有用于输入密码的多个数字键的小键盘110和用于操作进出门的开闭的手柄120。小键盘110可由物理数字小键盘、触摸键、显示支持触摸用户界面(TUI,Touch User Interface)的数字键图标等的触摸屏等构成。与普通门锁相同地,在通过锁定解锁控制部190解锁门锁的瞬间,输出通知解锁状态的语音信号,在此情况下,可在解除手柄120的操作锁定状态的同时用户可操作手柄120来开启进出门。

[0037] 锁定解锁单元130为锁定或解锁进出门的装置。例如,在门锁装置100的内部设置螺线管或电动机,将安装在进出门的门扣前进或后退来使其向形成在门框的门扣槽插入或者从门扣槽后退,由此锁定或解锁进出门。

[0038] 警告部140为发出警告音的蜂鸣器或扬声器,或者可由视觉警告的警告灯、发光二极管(LED)等构成。若在锁定解锁控制部190中判断安全码不一致或者密码不一致,则警告部140输出警告音或者点亮警告灯。

[0039] 存储单元150包括:密码存储部152,用于存储用户指定的密码;以及安全码存储部154,用于存储由后述的安全码/密码更新部180更新的安全码。存储单元150可由闪存等构成。

[0040] 短距离通信模块160为通过无线短距离通信网(Wireless Local Area Network)与用户便携式终端200进行通信的单元。短距离通信模块160可由如射频标识(RFID,Radio Frequency IDentification)、蓝牙(Bluetooth)、无线通信技术(Wi-Fi)、紫蜂协议(Zigbee)等的模块构成。

[0041] 安全码读取部170为用户便携式终端200进入短距离通信模块160的通信半径内时读取安全码的单元。

[0042] 安全码/密码更新部180仅限于锁定解锁控制部190判断安全码一致而将进出门从锁定状态切换为解锁状态之后的情况更新安全码及密码。在锁定解锁控制部190判断密码一致而解锁进出门的情况下,安全码和密码均不更新。安全码/密码更新部180将更新的安全码及密码传输至用户便携式终端200。并且,将更新的安全码存储在安全码存储部154,将更新的密码存储在密码存储部152。

[0043] 安全码为电子可读取数据,是加密的密钥信息。密码为一串数字或表示一串数字的数据。例如,在安全码/密码更新部180中更新的新的密码为对表示一串数字的数据进行加密处理而成。

[0044] 在本发明中,安全码使用一次后更新,是一次性的。并且,更新安全码的主体为并不直接与网络联接的门锁装置,通过用户便携式终端200的中继传输至安全管理服务器500。这提供了如下的优点:能够以高安全水平管理安全码,可防止安全码通过网络泄漏,容易管理安全码。

[0045] 在本发明中,密码具有直到更新安全码为止临时使用的临时性。密码在用户便携式终端200不在时或者用户允许其他人(以下,称为“访客”)进出时使用。密码可使用多个,废弃使用过一次的密码,由此,即使密码被泄漏,也可防止非法侵入。

[0046] 安全码/密码更新部180向用户便携式终端200加密传输更新的安全码及密码。并且,当将更新的安全码及密码中继到安全管理服务器500时,用户便携式终端200可被编程为并不自主存储或者在临时存储器中删除。或者,安全码/密码更新部180可包括将更新的

安全码及密码中继到远程的安全管理服务器500后在用户便携式终端200中删除的命令数据来传输。因此，可防止安全码或密码因用户便携式终端200被黑客攻击而泄漏。并且，在更新安全码的同时更新密码(即使不使用密码)，向密码赋予临时性，由此尽可能防止密码泄漏而引起的非法侵入。

[0047] 锁定解锁控制部190为控制锁定解锁单元130的操作的单元。锁定解锁控制部190判断在安全码读取部170中读取的安全码是否与存储在安全码存储部154的安全码一致，由此控制锁定解锁单元130来使其从锁定状态切换为解锁状态。例如，若用户在用户便携式终端200上运行门锁管理应用程序，则从后述的安全管理服务器500接收新的安全码，安全码读取部170可从用户便携式终端200读取安全码来判断安全码是否一致。

[0048] 或者，锁定解锁控制部190判断用户输入的密码是否与存储在密码存储部152的密码一致，由此控制锁定解锁单元130来使其从锁定状态切换为解锁状态。例如，在用户丢失或未携带用户便携式终端200的状态下，可利用其他便携式终端或如笔记本电脑等的其他通信终端访问后述的安全管理服务器500，可通过用户认证确认新的密码。并且，用户查看密码后，在激活安全性增强门锁100的小键盘110的触摸屏的状态下，若直接输入密码，则锁定解锁控制部190可判断密码是否一致。

[0049] 另外，若安全码或密码不一致，则锁定解锁控制部190启动上述警告部140。

[0050] 其中，锁定解锁控制部190判断密码是否一致来解锁锁定解锁单元130后，判断规定条件来暂时停止密码的使用功能。即，在使用密码并满足规定条件后，仅判断安全码是否一致来操作锁定解锁单元130。

[0051] 并且，通过使用安全码来解锁锁定解锁单元130后，由于是在安全码/密码更新部180中生成新的安全码和密码之后，再次激活密码使用功能。因此，可限制密码的使用来使其具有临时性。

[0052] 其中，当更新密码时，安全码/密码更新部180可生成互不相同的多个密码。例如，若使用6位数密码，则生成“123456”和“345678”两个密码。并且，在更新密码后，锁定解锁控制部190通过下述方式进行控制:针对任意一个密码(例如，“123456”)，对锁定解锁单元130进行解锁操作后废弃相应密码，并以仅针对剩余密码(例如，“345678”)开启门锁。即，废弃使用过的密码，来防止相同的密码被泄漏而再次使用。

[0053] 例如，户主或管理者向维护维修人员告知密码“123456”来允许其进出，可向快递员告知密码“345678”来允许其进出。但是，通过废弃使用过的密码来防止通过相同的密码再次进出，从而可防止密码泄漏引起的犯罪。

[0054] 作为另一例，锁定解锁控制部190还可对任意一个密码(例如，“123456”)设置规定的使用时间。例如，若将发给维护维修人员的密码“123456”的使用时间设置为5分钟，则维护维修人员可在5分钟之内自由进出安装有本发明的门锁的住宅或设施等。但是，在超出使用时间后，废弃相应密码来无法在允许的时间以后再次使用发布的密码，从而可防止通过相同的密码非法侵入。

[0055] 在本发明的安全性增强门锁中，门锁装置并不与网络或移动通信网直接联接。安全性增强门锁仅通过短距离无线通信与用户便携式终端200联接。并且，安全性增强门锁直接更新安全码及密码(一个或互不相同的多个密码)，通过用户便携式终端200的中继将更新的安全码及密码传输至远程的管理服务器500。因此，可防止安全码及密码通过网络泄

漏。

[0056] 本发明的安全性增强门锁具有安全码和密码的双重解锁功能的优点在于，在提供用户便利性的同时增强安全性。用户可利用存储在本人的便携式终端的安全码自由进出。或者，可将临时提供的密码告知其他人来容许授权的用户受限进出。

[0057] 参照图2至图13具体说明提及的本发明的安全性增强门锁的优点及利用该安全性增强门锁的进出门管理系统的优点和具体实施例。

[0058] 图2为示出本发明中的利用安全码的门锁操作例的流程图，图3为示出本发明中的利用密码的门锁操作例的流程图。以下，参照图2及图3说明本发明的安全性增强门锁的操作方法。

[0059] 参照图2，锁定解锁控制部190判断用户便携式终端200是否进入短距离通信模块160的无线通信半径内(步骤ST110)。例如，当用户操作用户便携式终端200来运行专用应用程序(App)时，可激活短距离通信模块160。作为另一例，当检测到用户便携式终端200时，还可激活短距离通信模块160。

[0060] 之后，安全码读取部170从用户便携式终端200读取安全码(步骤ST120)。并且，判断读取的安全码是否与已存储在安全码存储部154的安全码一致(步骤ST130)。若不一致，则如上所述地启动警告部140(步骤ST140)。

[0061] 若在步骤ST130中判断安全码一致，则解锁门锁(步骤ST150)。在此情况下，能够以蜂鸣声或其他语音信号输出门锁的解锁状态。

[0062] 之后，如上所述，安全码/密码更新部180更新安全码及密码，将更新的安全码及密码分别存储在安全码存储部154及密码存储部152(步骤ST160)。并且，对更新的安全码及密码进行加密并传输至用户便携式终端200(步骤ST170)。

[0063] 其中，重要的一点是，在门锁本身更新安全码及密码，并仅通过无线短距离通信网300传输更新的安全码及密码。若门锁通过网络向远程的管理服务器直接传输安全码，则安全码可通过公用网泄漏。但是，每当使用安全码时，本发明的安全性增强门锁自行更新安全码及密码，并且，如后述的进出门安全管理系统，用户便携式终端200仅将更新的安全码及密码中继到远程的安全管理服务器500，并不自行保留，在防止更新的安全码及密码通过网络泄漏的同时并不保留在用户便携式终端，从而可极大地增强安全性。

[0064] 并且，重要的另一点是，即使仅使用安全码，也可在更新安全码的同时更新密码。如上所述，当使用安全码时，在门锁本身同时更新安全码和密码，由此可减少并不更新未使用密码且长时间保存而暴露的风险。

[0065] 参照图3，锁定解锁控制部190判断是否通过小键盘110输入密码(步骤ST210)。若输入密码，则在下一步骤判断输入的密码是否与存储在密码存储部152的密码一致(步骤ST220)。

[0066] 若密码不一致，则判断密码连续不一致的次数是否达到规定次数(例如，5次)(步骤ST230)。若在步骤ST230中判断为“是(Yes)”，则启动警告部140(步骤ST240)。

[0067] 若在步骤ST220中判断为密码一致，则解锁门锁(步骤ST250)。在此情况下，能够以蜂鸣声或其他语音信号输出门锁的解锁状态。

[0068] 在通过密码开启门锁的情况下，锁定解锁控制部190判断规定条件来暂时停止密码的使用功能。即，之后无法通过输入密码开启门锁。在后述内容中参照图4及图5说明使用

过的密码的废弃及暂时停止的具体例。

[0069] 之后，通过使用安全码来判断门锁是否被解锁(步骤ST260)。通过使用安全码来解锁门锁的过程与参照图2说明的内容相同。

[0070] 若通过使用安全码来解锁门锁，则进行图2的步骤ST160及步骤ST170，当更新安全码及密码来将其传输至用户便携式终端200时，包括之前的密码使用历史来传输(步骤ST270)。因此，如后所述，可在远程的管理服务器存储并管理密码的使用历史。

[0071] 图4为示出本发明中的使用并废弃多个密码的一例的流程图，图5为示出本发明中的设置密码的使用时间后废弃的一例的流程图。

[0072] 如前所述，安全码/密码更新部180可在更新安全码和密码的同时生成一个以上的密码。并且，如图4中所例示，锁定解锁控制部190可使多个密码仅分别使用一次或者限制其使用次数。作为另一例，如图5中所例示，锁定解锁控制部190可限制一个密码的使用时间。

[0073] 首先，参照图4，锁定解锁控制部190可在图3的步骤ST250结束之后废弃使用过的密码(步骤ST410)。并且，判断所有密码是否被废弃(步骤ST420)。若存在剩余密码，则进行步骤ST210。若在使用任意一个密码后用户使用安全码，则即使在步骤ST420之后，也可进行步骤ST260。

[0074] 例如，若新生成“123456”和“345678”两个密码且在图3的步骤ST210中输入密码“123456”，则在步骤ST250的解锁门锁之后在步骤ST410中废弃密码“123456”。因为存在剩余密码“345678”，可进行步骤ST210并等待是否输入新的密码。并且，若使用安全码，则进行步骤ST260及步骤ST270来更新安全码和密码。

[0075] 假设在更新安全码和密码之前两个密码“123456”及“345678”均被使用。通过步骤ST410废弃密码“345678”，并满足步骤ST420的条件，因此，锁定解锁控制部190进行步骤ST430来暂时停止密码使用功能(步骤ST430)。

[0076] 之后，直到通过步骤ST260使用安全码为止，无法通过密码解锁门锁。进行步骤ST260及步骤ST270后，发布新的(多个)密码来再次激活通过密码的门锁解锁功能。

[0077] 之后，参照图5，锁定解锁控制部190可在图3的步骤ST250结束之后设置使用过的密码的再次使用时间(步骤ST510)。再次使用时间可通过用户的指定设置。例如，可通过用户在门锁内部输入按钮来输入5分钟至10分钟的时间来设置为密码的再次使用时间。或者，虽未图示，还可设置密码的再次使用次数。

[0078] 在下一步骤中，判断是否超出相应密码的再次使用时间(步骤ST520)。该步骤还可被判断相应密码的再次使用次数是否超出设置次数的步骤代替。在超出再次使用时间之前(或者，超出再次使用次数之前)，可返回步骤ST210来再次使用相应密码。在判断是否超出再次使用时间的过程中，若用户使用安全码，则还可进行步骤ST260。

[0079] 若在步骤ST520中判断为对于任意密码的再次使用时间超出或者再次使用次数清零，则废弃相应密码(步骤ST530)。并且，进行步骤ST540来判断所有密码是否被废弃。若存在剩余密码，则进行步骤ST210。若用户即使在任意步骤的中间使用安全码，则可进行步骤ST260。

[0080] 若在步骤ST540中判断为一个以上的密码均被废弃，则锁定解锁控制部190进行步骤ST550来暂时停止密码使用功能(步骤ST550)。

[0081] 之后，直到通过步骤ST260使用安全码为止，无法通过密码解锁门锁。在进行步骤

ST260及步骤ST270后,可通过发布新的(多个)密码来再次激活借助密码的门锁解锁功能。

[0082] 图6为例示本发明的进出门安全管理系统的框图。以下,参照图6说明本发明的进出门安全管理系统。

[0083] 本发明的进出门安全管理系统包括安全性增强门锁100、用户便携式终端200以及安全管理服务器500。

[0084] 安全性增强门锁100与参照图1至图5说明的内容相同。

[0085] 用户便携式终端200为通过无线短距离通信网300与安全性增强门锁100进行通信且通过广域移动通信网400与安全管理服务器500进行通信的终端。用户便携式终端200可以为用于实现本发明的进出门安全管理系统的专用终端,优选为智能手机。在用户便携式终端200可安装用于管理安全码的专用应用程序。

[0086] 虽未图示,用户便携式终端200包括用于与安全性增强门锁100进行通信的短距离无线通信模块。例如,短距离通信模块可由射频标识、蓝牙、无线通信技术、紫峰协议等的模块构成。并且,用户便携式终端200包括用于与安全管理服务器500进行通信的移动通信模块。例如,移动通信模块可以为通过3G、4G、5G等周知的通信频带执行移动通信的模块、以未知的下一代通信频带执行移动通信的模块。例如,移动通信模块230为在根据全球移动通信系统(GSM,Global System for Mobile communication)、码分多址(CDMA,Code Division Multi Access)、码分多址2000(CDMA2000,Code Division Multi Access 2000)、增强型语音数据优化或仅增强型语音数据(EVDO,Enhanced Voice-Data Optimized or Enhanced Voice-Data Only)、宽带码分多址(WCDMA,Wideband CDMA)、高速下行分组接入(HSDPA,High Speed Downlink Packet Access)、高速上行分组接入(HSUPA,High Speed Uplink Packet Access)、长期演进(LTE,Long Term Evolution)、长期演进-高级(LTE-A,Long Term Evolution-Advanced)等构建的移动通信网上与基站、外部终端、服务器中的至少一个发送或接收无线信号的模块。

[0087] 并且,用户便携式终端200包括用于存储从安全管理服务器500发布的安全码及密码的存储单元。通常,智能手机包括所列的短距离通信模块、移动通信模块、存储器等。并且,用户已经在为移动通信和无线互联网支付费用。即,智能手机安装并运行参照图8至图13后述的门锁管理应用程序,并具有实现本发明的进出门安全管理系统的最佳环境。因此,仅通过向用户使用的便携式终端提供门锁管理应用程序来容易实现在本发明中说明的安全码/密码发布请求、中继、开启门锁、用户管理、门锁功能设置等。

[0088] 在本发明中,用户便携式终端200仅在安全性增强门锁100中将更新的安全码及密码中继到远程安全管理服务器500,并不自行存储。并且,安装在用户便携式终端200的门锁管理应用程序可编程为从安全性增强门锁100向安全管理服务器500传输包括通过图2的步骤ST170更新的安全码及密码和各自的使用历史的信息后,自行删除更新的安全码及密码。

[0089] 安全管理服务器500通过广域移动通信网400与用户便携式终端200进行通信。参照图6,安全管理服务器500包括:安全码管理数据库510,按照安全性增强门锁100存储并管理安全码;密码管理数据库520,按照安全性增强门锁100存储并管理密码;以及安全历史管理数据库530,按照安全性增强门锁100存储并管理安全码及密码的发布历史和使用历史。安全码管理数据库510、密码管理数据库520及安全历史管理数据库530可实现为安装在安全管理服务器500的存储空间或单独管理的数据库服务器。

[0090] 在本发明中，安全管理服务器500并不直接生成安全码及密码。仅存储并管理通过用户便携式终端200中继的安全码及密码(在安全性增强门锁自行更新的安全码及密码)。

[0091] 在存在来自用户便携式终端200的安全码发布请求的情况下，安全管理服务器500在进行认证过程后，将存储在安全码管理数据库510的最新的安全码传输至用户便携式终端200。

[0092] 例如，若用户在用户便携式终端200运行门锁管理应用程序，则自动向安全管理服务器500传输认证请求。安全管理服务器500可通过识别用户便携式终端200的电话号或Mac地址(Mac address)来发布安全码。

[0093] 并且，在用户利用能够上网的计算机终端联接网络的情况下，安全管理服务器500确认用户的账号和密码或者确认公共证书，以向用户提供存储在密码管理数据库520的最新密码。

[0094] 参照图6，本发明的进出门安全管理系统还可包括通过广域移动通信网600与安全管理服务器500或用户便携式终端200联接的警察厅服务器700、监护人便携式终端800或其他服务器或终端等。

[0095] 在用户输入特定按键、按键组合或配置在应用程序运行画面上的紧急通知图标的情况下，安装在用户便携式终端200的门锁管理应用程序可向安全管理服务器500、警察厅服务器700或监护人便携式终端800传输紧急情况消息。例如，在单身女性家庭的成员为了开启进出门而等待或者骚扰者接近进出门的情况下，可将紧急情况消息传输至安全管理服务器500或预先指定的服务器或终端。

[0096] 并且，用户便携式终端200可通过无线短距离通信网300向安全性增强门锁100传输紧急情况消息。在此情况下，安全性增强门锁100停止通过安全码的门锁解锁功能，并将功能转换为仅通过输入密码来解锁门锁。因此，可防止用户便携式终端200被盗而偷盗者未经许可解锁门锁。

[0097] 图7为例示本发明的进出门安全管理方法的数据流程图。以下，参照图7说明构成本发明的进出门安全管理系统的组件之间的数据流。

[0098] 若用户为了开启进出门而在用户便携式终端200上运行门锁管理应用程序，则从用户便携式终端200向安全管理服务器500传输安全码发布请求信号(步骤①)。安全管理服务器500对于用户便携式终端200进行认证过程来发布安全码(步骤②)。

[0099] 在用户便携式终端200接近安全性增强门锁100的短距离无线半径内后用户在应用程序画面上输入开门图标的情况下，或者在安全性增强门锁100中自动激活锁定解锁控制部190的情况下，安全性增强门锁100读取存储在用户便携式终端200的安全码(步骤③)。安全性增强门锁100判断读取的安全码是否与已存储的安全码一致(步骤④)。

[0100] 在代替步骤①至步骤④而用户通过设置在安全性增强门锁100的小键盘110直接输入密码的情况下，还可判断用户输入的密码是否与已存储的密码一致(步骤⑤)。

[0101] 在通过步骤①至步骤④判断安全码一致的情况下，解锁门锁，更新安全码及密码后自行分别存储在安全码存储部154及密码存储部152(步骤⑥)。

[0102] 并且，安全性增强门锁100将更新的安全码及密码传输至用户便携式终端200(步骤⑦)。在此情况下，加密传输更新的安全码及密码，还可传输命令将更新的安全码及密码中继到服务器侧后删除的命令数据。

[0103] 在通过步骤⑤判断用户输入的密码一致的情况下，安全性增强门锁100解锁门锁。并且，在通过输入密码解锁门锁的情况下，立即暂时停止密码使用功能，或者判断是否满足图4及图5的条件来暂时停止密码使用功能。之后，根据图3的步骤ST260判断通过安全码解锁门锁后，根据步骤ST270将在步骤⑦中更新的安全码及密码和之前的密码使用历史传输至用户便携式终端200。

[0104] 在步骤⑦之后，用户便携式终端200将更新的安全码及密码中继到安全管理服务器500(步骤⑧)。在此情况下，用户便携式终端200通过安全性增强门锁100的命令或者门锁管理应用程序的自身功能将更新的安全码及密码中继到安全管理服务器500后，可从内部的临时存储器中删除。

[0105] 安全管理服务器500更新从用户便携式终端200接收的安全码及密码和安全码/密码使用历史等的安全历史(步骤⑨)。在发生下一次安全码发布请求的情况下，安全管理服务器500发布存储在安全码管理数据库510的最新安全码，认证通过网络访问的用户后提供存储在密码管理数据库520的最新的密码。

[0106] 图8至图13为示出本发明中的安装在用户便携式终端的门锁管理应用程序的运行例的图，示出在触摸用户界面显示用户输入窗口、选择按钮等的例。以下，参照该附图以本发明的进出门安全管理系统中的用户便携式终端为中心说明门锁的开闭、密码查看及共享、访客管理、门锁功能设置等。

[0107] 图8为例示本发明中的安装在用户便携式终端的门锁管理应用程序的用户认证画面的图，例示门锁管理应用程序的运行初始画面。参照图8，在用户认证画面的中心上端显示门锁应用程序标志251，上述门锁应用程序标志251为使得用户认知到门锁管理应用程序的运行的形象化的标志。在门锁应用程序标志251的下方显示账号输入窗口253、密码输入窗口255、自动登录检查项目257、管理者登录输入按钮261以及访客登录输入按钮263。

[0108] 账号输入窗口253为用户最初输入的或者输入通过用户的权限授予的账号的窗口。例如，用户账号为通过门锁装置注册的用户的手机号。密码输入窗口255为用于输入用户设置的或者通过门锁装置设置的密码的窗口。自动登录检查项目257为通过用户的输入在自动登录和手动登录之前切换来设置的输入项目。

[0109] 在本发明中，用户根据权限分为管理者和访客。管理者具有可请求发布对于安全性增强门锁100的安全码和密码并允许对于访客发布安全码等的权限。访客可使用有限的安全码，通过管理者调节访客的安全码使用权限。管理者和访客的初始注册步骤互不相同，优选地，管理者利用安全性增强门锁100注册，访客在管理者的允许下注册。

[0110] 管理者通过输入管理者登录输入按钮261来登录，通过安全管理服务器500的认证来使用应用程序。访客通过输入访客登录输入按钮263来登录，以通过管理者设置的有限的功能使用应用程序。在本发明中，“管理员便携式终端”是指通过管理者登录而认证的用户便携式终端，“访客便携式终端”是指通过访客登录而认证的用户便携式终端。

[0111] 图9为示出本发明中的通过门锁管理应用程序执行门锁开启的例示的图，为示出管理员便携式终端中的运行例的图。

[0112] 在进行用户认证后，可输出如图9的门锁开启网页。在门锁开启网页的上端配置：菜单按钮265，用于移动至菜单项目或者运行弹出菜单；门锁名称显示窗口269，用于显示控制对象门锁的名称；以及门锁添加按钮267，可添加控制对象门锁。

[0113] 管理者可执行对于多个安全性增强门锁100的进出管理及访客管理，在各个安全性增强门锁100分配如“门锁23”等的唯一的名称。

[0114] 参照图9，在门锁开启网页的中心配置门锁开启选择按钮271。如图所示，门锁开启选择按钮271以直观地显示门锁开启的图标显示。如图7的步骤①，在用户输入门锁开启选择按钮271的情况下，门锁管理应用程序向安全管理服务器500传输安全码发布请求信号。并且，进行步骤②至步骤④来解锁门锁。之后，进行步骤⑥至步骤⑨，安全管理服务器500通过接收中继的更新的安全码来更新安全码管理数据库510，并可将新的安全码使用历史(及密码使用历史)更新到安全历史管理数据库。

[0115] 另外，门锁开启选择按钮271还可在管理者允许的访客便携式终端上显示。但优选地，图9中例示的进出记录确认按钮273、密码查看按钮275、装置设置按钮277、控制对象门锁移动滑块279、紧急呼叫按钮281等仅显示在管理员便携式终端。

[0116] 参照图9，若通过管理员便携式终端输入进出记录确认按钮273，则门锁管理应用程序访问安全管理服务器500来读取安全历史管理数据库530。并且，切换应用程序页面来在画面输出对于“门锁23”的安全码使用历史信息及密码使用历史信息。

[0117] 若输入密码查看按钮275，则门锁管理应用程序切换为在图10及图11中例示的密码查看应用程序页面，若输入装置设置按钮277，则切换为在图12及图13中例示的门锁设置应用程序页面。

[0118] 控制对象门锁移动滑块279为用于切换为对于其他安全性增强门锁100的门锁开启应用程序页面的输入单元。例如，若用户通过朝向右侧滑动的方式在管理员便携式终端中输入控制对象门锁移动滑块279，则切换为对于“门锁24”的门锁开启应用程序页面。对于“门锁24”的门锁开启应用程序页面以与图9相同的结构配置。

[0119] 紧急呼叫按钮281为用于与预设的联系人通话的按钮。例如，若用户输入紧急呼叫按钮281，则尝试与如妇女安全中心的电话号、119或112等事先设置的电话号通话。或者，如参照图6所说明，还可向警察厅服务器700传输通知事先存储的紧急情况的文字消息。

[0120] 图10及图11为示出本发明中的通过门锁管理应用程序的画面输出密码查看应用程序页面的例的图。参照图10，密码查看应用程序页面依次显示从安全管理服务器500接收的多个密码。例如，如上所述，当从安全性增强门锁100更新安全码及密码时，若更新互不相同的3个密码，则通过用户便携式终端200的中继安全管理服务器500处于更新3个密码的状态。第一密码显示窗口291、第二密码显示窗口293、第三密码显示窗口295显示互不相同的多个密码，但利用如“*”等的掩蔽文字隐藏来显示。在各个密码显示窗口右侧配置密码查看按钮297和密码共享按钮299。

[0121] 在图10的例示中，在用户对于任意一个密码输入密码查看按钮297的情况下，如图11，在去除相应密码的掩蔽文字的同时显示密码。用户可通过直接输入显示的密码来解锁安全性增强门锁100。或者，用户可向其他人告知显示的密码。在此情况下，门锁管理应用程序与安全性增强门锁100执行短距离无线通信，如图11，若对于向用户显示的第三密码“391245”超出规定的使用时间(5分钟至10分钟)，则可传输命令废弃相应密码的命令数据。即，对于已暴露一次的密码设置临时使用时间，由此可加强对于密码暴露的安全性。

[0122] 在图10的例示中，在用户对于任意一个密码输入密码共享按钮299的情况下，门锁管理应用程序可将相应密码传输至事先指定或者用户输入的电话号的便携式终端。例如，

当输入密码共享按钮299时，切换应用程序页面或者出现弹出窗口，并可向切换的应用程序页面或弹出窗口输入所要接收密码的电话号。在此情况下，虽向用户通过掩蔽文字隐藏显示相应密码，但向接收密码共享的其他人显示整个密码。当共享密码时，门锁管理应用程序可向安全性增强门锁100侧传输使用时间限制命令。

[0123] 图12及图13为示出本发明中的通过门锁管理应用程序运行门锁设置应用程序页面的例的图，图12为示出执行访客管理的例示的图，图13为示出执行功能设置的例示的图。

[0124] 参照图12，在门锁设置应用程序页面的画面左上端配置后退按钮351，当输入该按钮时，移动至前一页面(例如，图9的门锁开启应用程序页面)。如图12，当输入画面上端的访客管理按钮353时，加深显示或阳刻显示相应按钮来激活访客管理应用程序页面。

[0125] 如图所示，访客管理应用程序页面在画面输出搜索筛选选择窗口357、搜索词输入窗口359、访客信息显示窗口361、邀请按钮363、参与中的访客显示窗口365、删除按钮367。

[0126] 搜索筛选选择窗口357为选择搜索筛选(例如，姓名、昵称、电话号等)的窗口，搜索词输入窗口359为输入搜索词的窗口。若在搜索筛选选择窗口357中选择“姓名”且在搜索词输入窗口359输入“金**”，则门锁管理应用程序在存储于管理员便携式终端中的列表中搜索相应姓名。并且，在访客信息显示窗口361输出搜索结果。例如，可在访客信息显示窗口361显示搜索的访客的姓名和电话号。若用户通过访客信息显示窗口361确认访客后输入邀请按钮363，则在下方的参与中的访客显示窗口365中列出搜索到的访客。若输出配置在各个访客列表右侧的删除按钮367，则在参与中的访客显示窗口365中移除相应访客。

[0127] 如上所述，在参与中的访客显示窗口365列出的访客是指允许使用安全码的访客。即，如图12的例示，管理者可按照安全性增强门锁100对于多个访客允许或阻止使用安全码。

[0128] 参照图13，在输入画面上端的功能设置按钮355的情况下加深显示或阳刻显示相应按钮来激活功能设置应用程序页面。

[0129] 功能设置应用程序页面从上到下依次显示门锁名称显示窗口371、密码管理画面移动项目375、手动允许切换滑动条377、控制切换滑动条379、门锁删除画面移动项目381。

[0130] 在门锁名称显示窗口371显示作为控制对象的安全性增强门锁100的名称(门锁23)，在其右侧配置修改按钮373。在用户输入修改按钮373的情况下，门锁管理应用程序切换为可修改门锁名称的应用程序页面或者激活弹出窗口。

[0131] 密码管理画面移动项目375为用于切换为管理密码的画面的输入单元，门锁删除画面移动项目381为用于切换为从管理对象移除相应安全性增强门锁的画面的输入单元。

[0132] 手动允许切换滑动条377为对于是否手动允许通过滑动选择开启(ON)/关闭(OFF)的输入项目。若用户朝向左侧移动手动允许切换滑动条377，则关闭手动允许状态，并设置为在图12中例示的参与访客自动接收安全码的状态。若用户朝向右侧移动手动允许切换滑动条377，则开启手动允许状态，并切换为所有访客通过管理者的允许接收安全码的状态。

[0133] 控制切换滑动条379为对于是否控制安全性增强门锁通过滑动选择开启(ON)/关闭(OFF)的输入项目。若用户朝向左侧移动控制切换滑动条379，则关闭控制状态，并设置为在图12中例示的参与访客自动接收安全码的状态。若用户朝向右侧移动控制切换滑动条379，则开启控制状态，并切换为停止向所有访客发布安全码的控制状态。

[0134] 在本说明书中说明的实施例和附图仅是示例说明本发明所包括的技术思想的一

部分。据此，在本说明书公开的实施例并不是用于限定本发明的技术思想，而是用于说明的，不得由这种实施例限定本发明的技术思想的范围，并且这是显而易见的。在本发明的说明书及附图中所包括的技术思想的范围内可被本领域技术人员容易推断出的所有变形示例和具体实施例应被解释为全部包括在本发明的权利范围内。

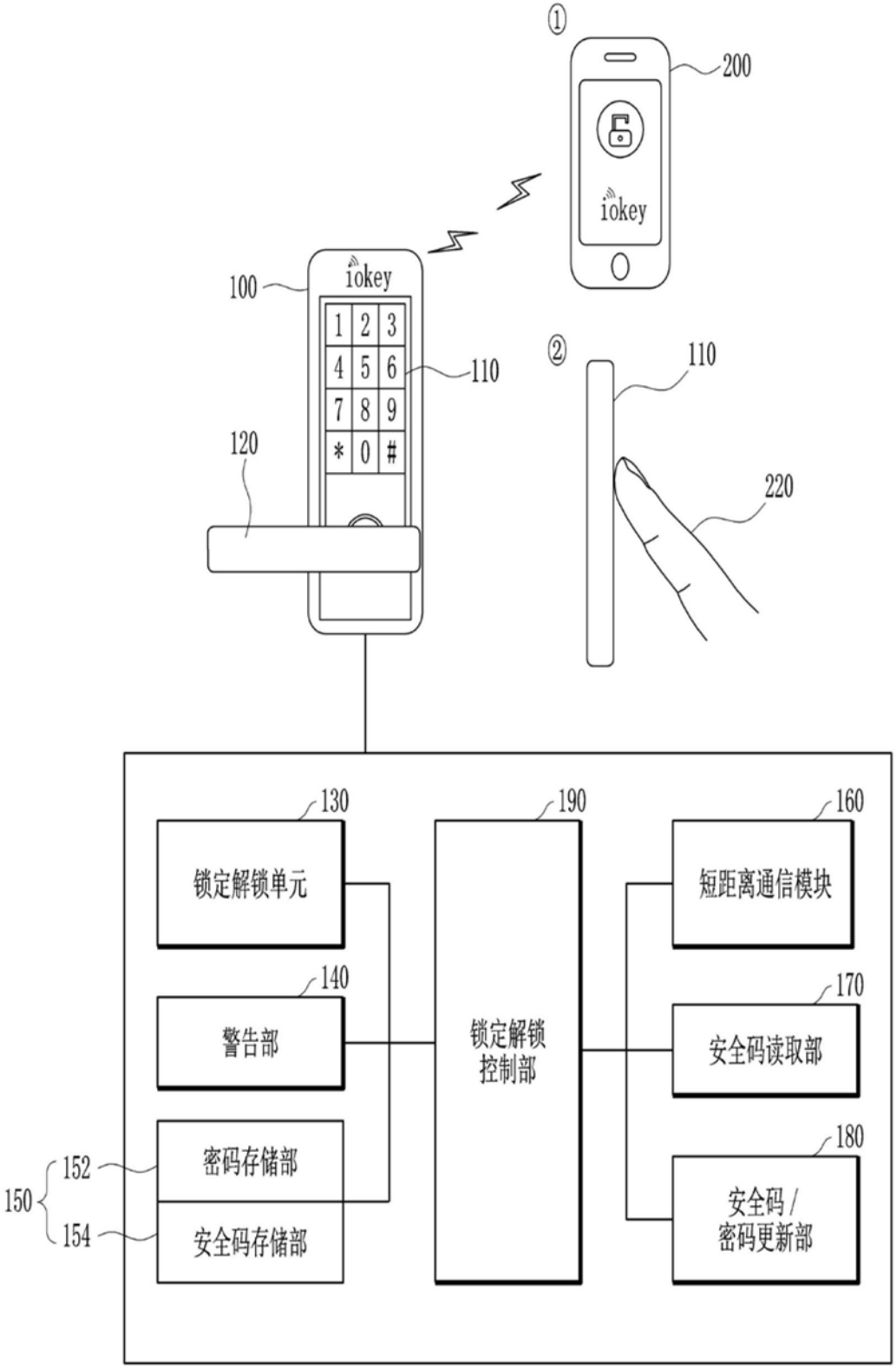

①
200
iokey
100
iokey
1 2 3
4 5 6
7 8 9
* 0 #
110
120
②
110
220
130
锁定解锁单元
140
警告部
150
152
密码存储部
154
安全码存储部
190
锁定解锁
控制部
160
短距离通信模块
170
安全码读取部
180
安全码 /
密码更新部

图1

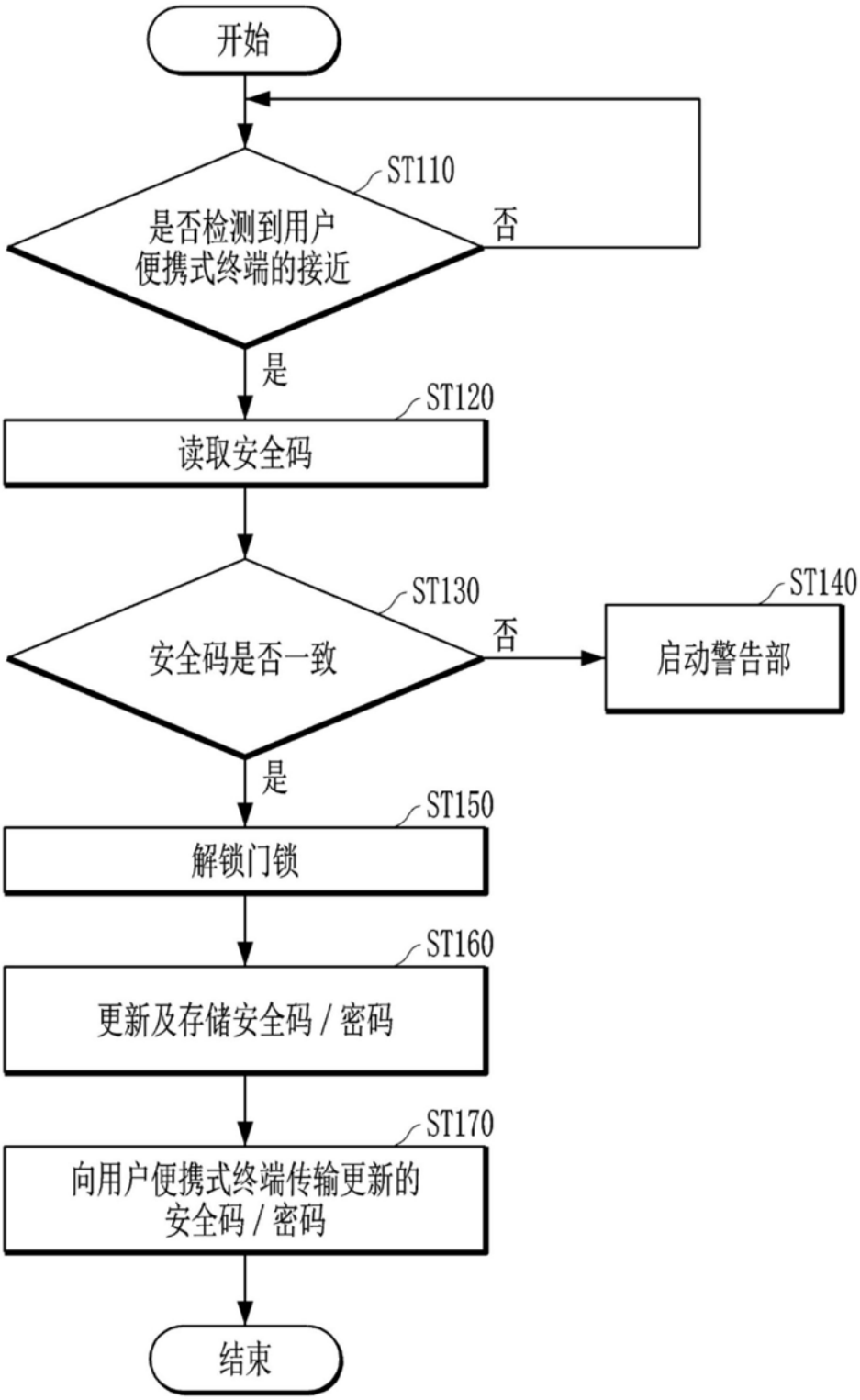

开始
ST110
是否检测到用户
便携式终端的接近
否
是
ST120
读取安全码
ST130
安全码是否一致
否
ST140
启动警告部
是
ST150
解锁门锁
ST160
更新及存储安全码 / 密码
ST170
向用户便携式终端传输更新的
安全码 / 密码
结束

图2

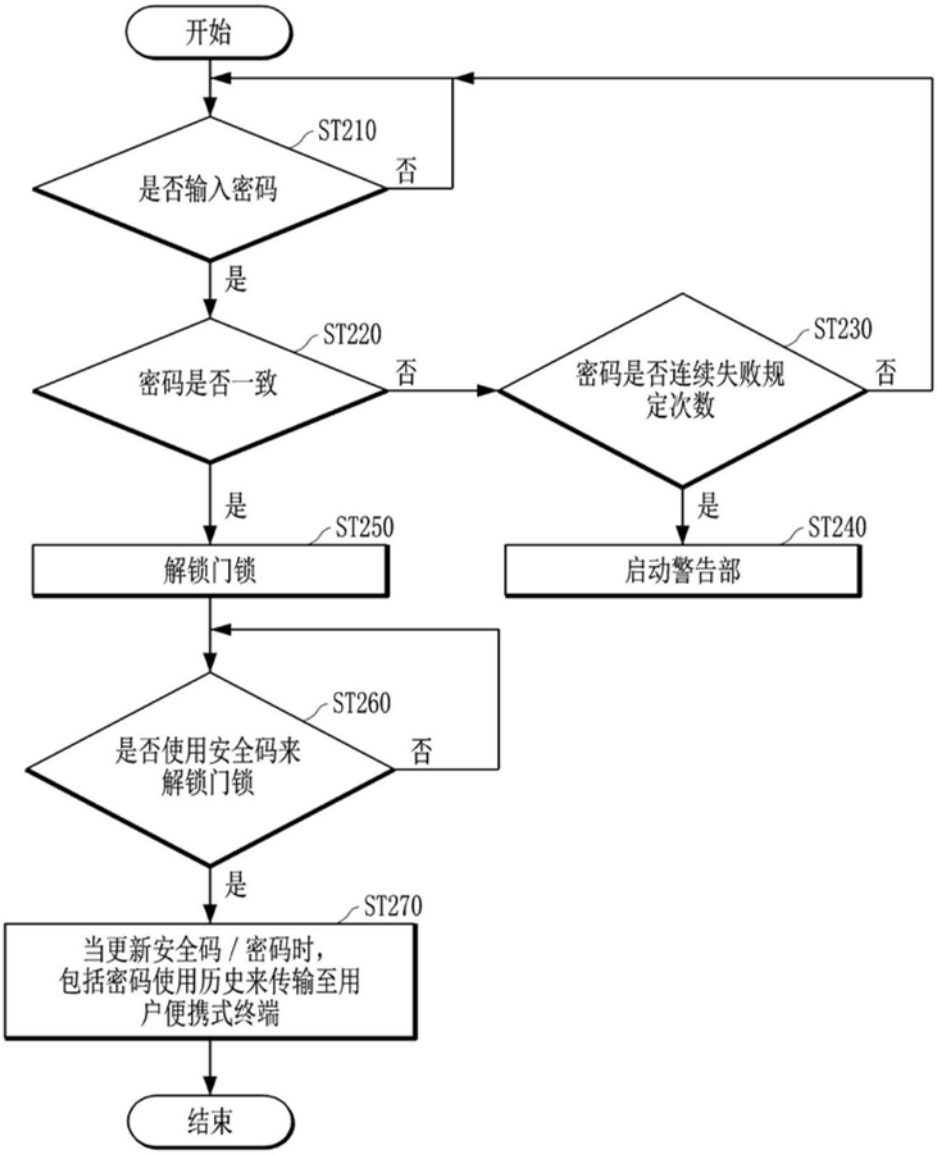

开始
ST210
是否输入密码
否
是
ST220
密码是否一致
否
ST230
密码是否连续失败规定次数
否
是
ST250
解锁门锁
是
ST240
启动警告部
ST260
是否使用安全码来解锁门锁
否
是
ST270
当更新安全码 / 密码时，包括密码使用历史来传输至用户便携式终端
结束

图3

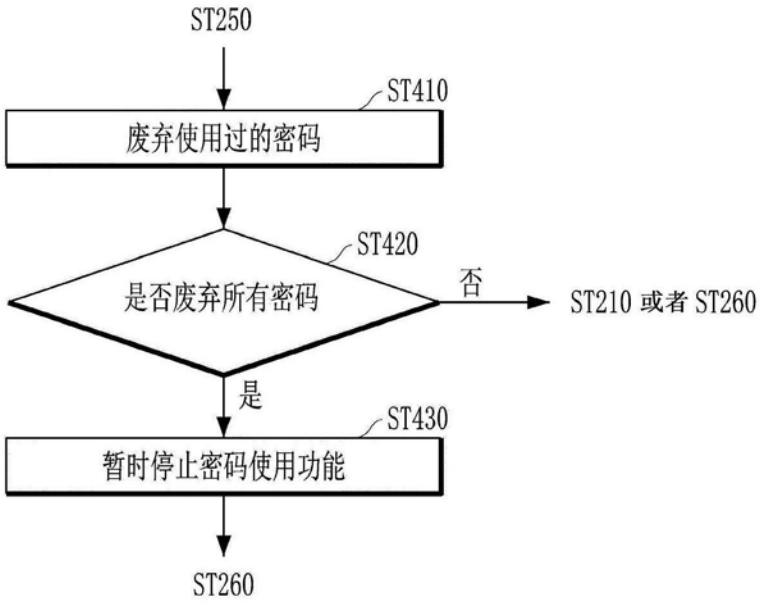

ST250
ST410
废弃使用过的密码
ST420
是否废弃所有密码
否
ST210 或者 ST260
是
ST430
暂时停止密码使用功能
ST260

图4

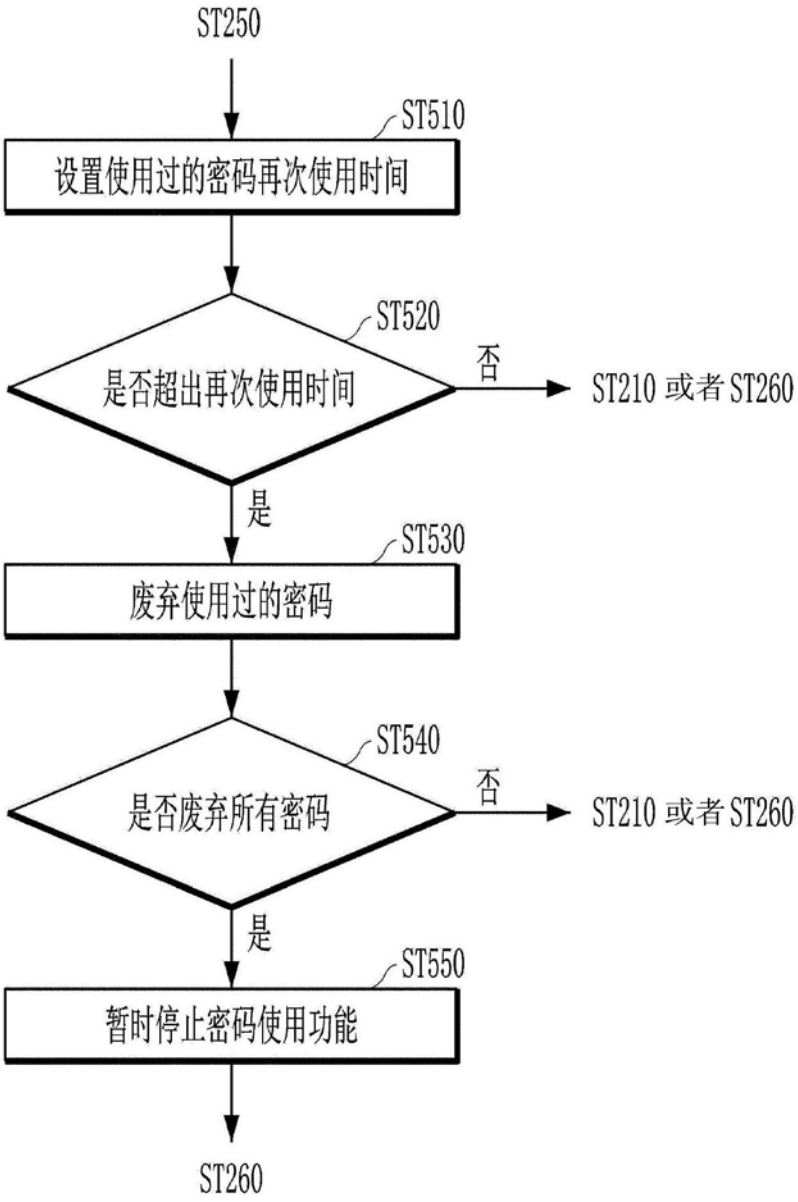

ST250
ST510
设置使用过的密码再次使用时间
ST520
是否超出再次使用时间
否
ST210 或者 ST260
是
ST530
废弃使用过的密码
ST540
是否废弃所有密码
否
ST210 或者 ST260
是
ST550
暂时停止密码使用功能
ST260

图5

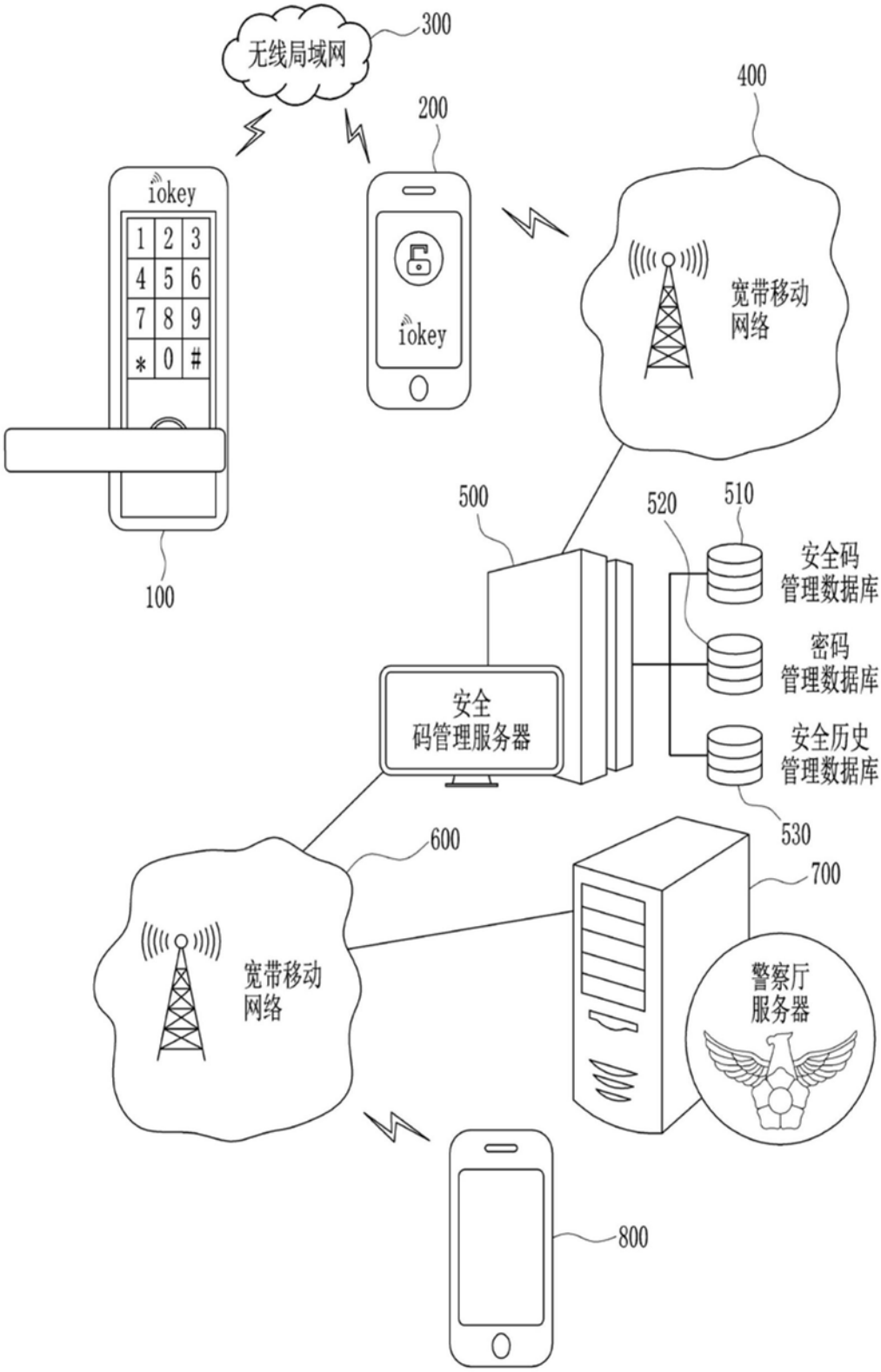

无线局域网
300
200
400
iokey
1 2 3
4 5 6
7 8 9
* 0 #
iokey
宽带移动
网络
100
500
520
510
安全码
管理数据库
密码
管理数据库
安全
码管理服务器
安全历史
管理数据库
530
600
700
宽带移动
网络
警察厅
服务器
800

图6

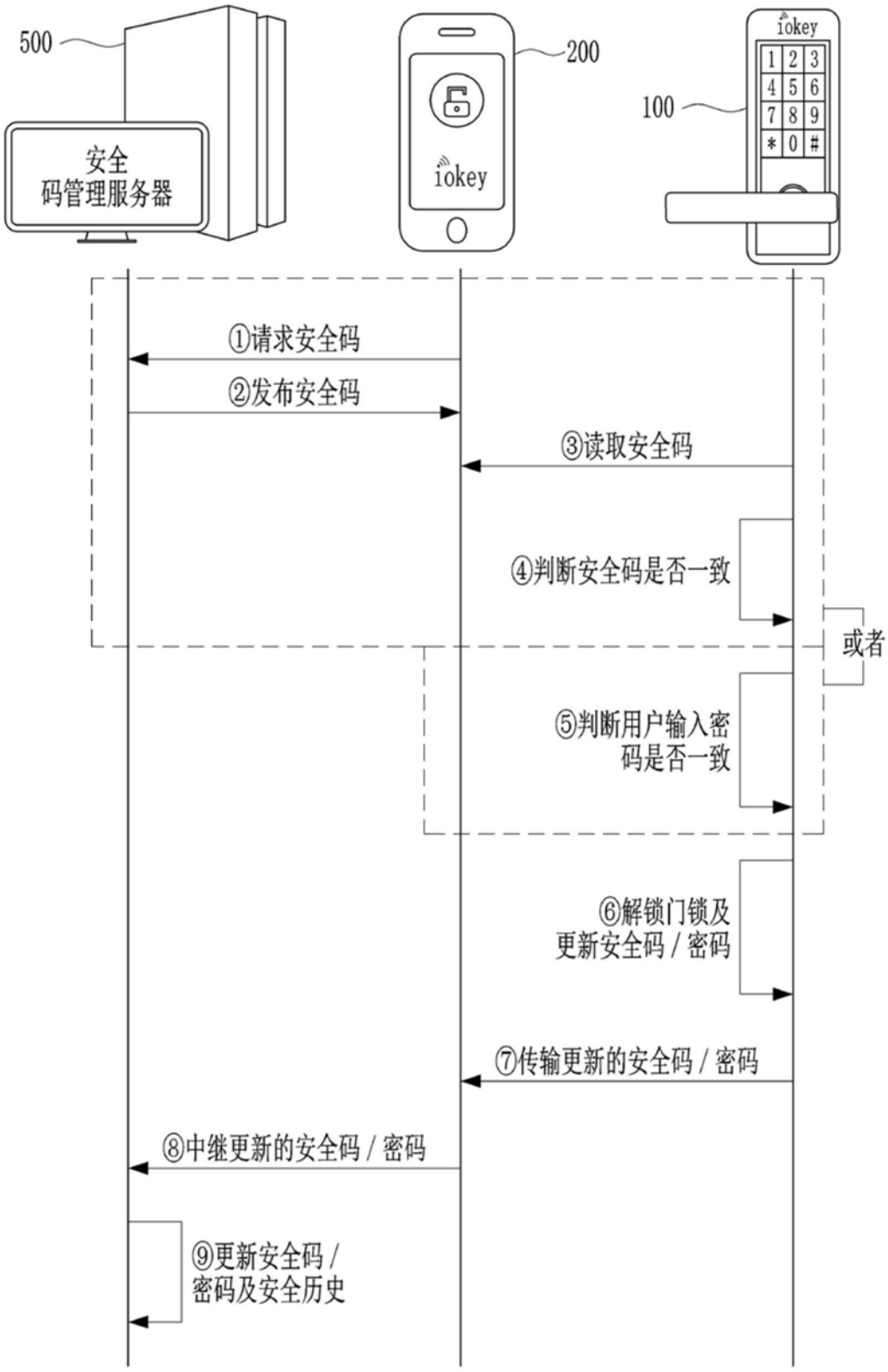

500
安全
码管理服务器
200
iokey
100
iokey
1 2 3
4 5 6
7 8 9
* 0 #
①请求安全码
②发布安全码
③读取安全码
④判断安全码是否一致
或者
⑤判断用户输入密
码是否一致
⑥解锁门锁及
更新安全码 / 密码
⑦传输更新的安全码 / 密码
⑧中继更新的安全码 / 密码
⑨更新安全码 /
密码及安全历史

图7

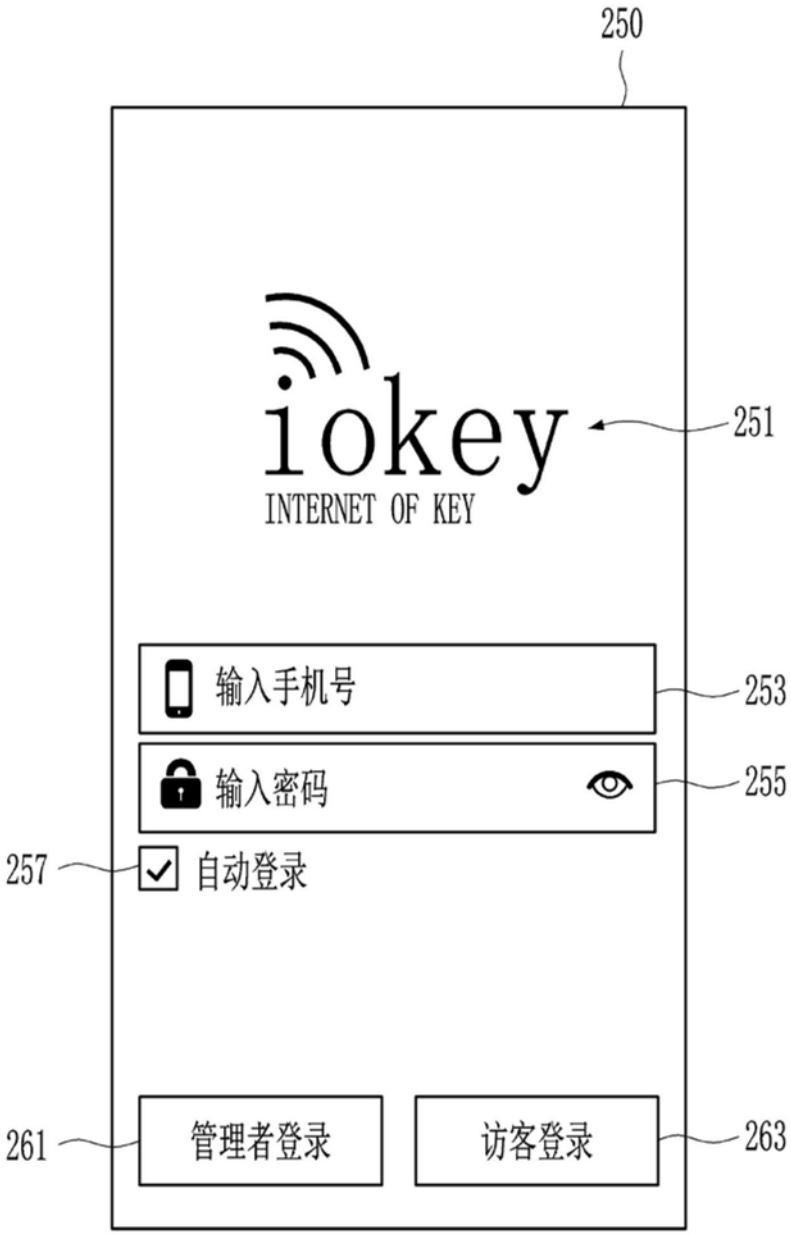

250
iokey
INTERNET OF KEY
251
输入手机号
253
输入密码
255
257
自动登录
261
管理者登录
访客登录
263

图8

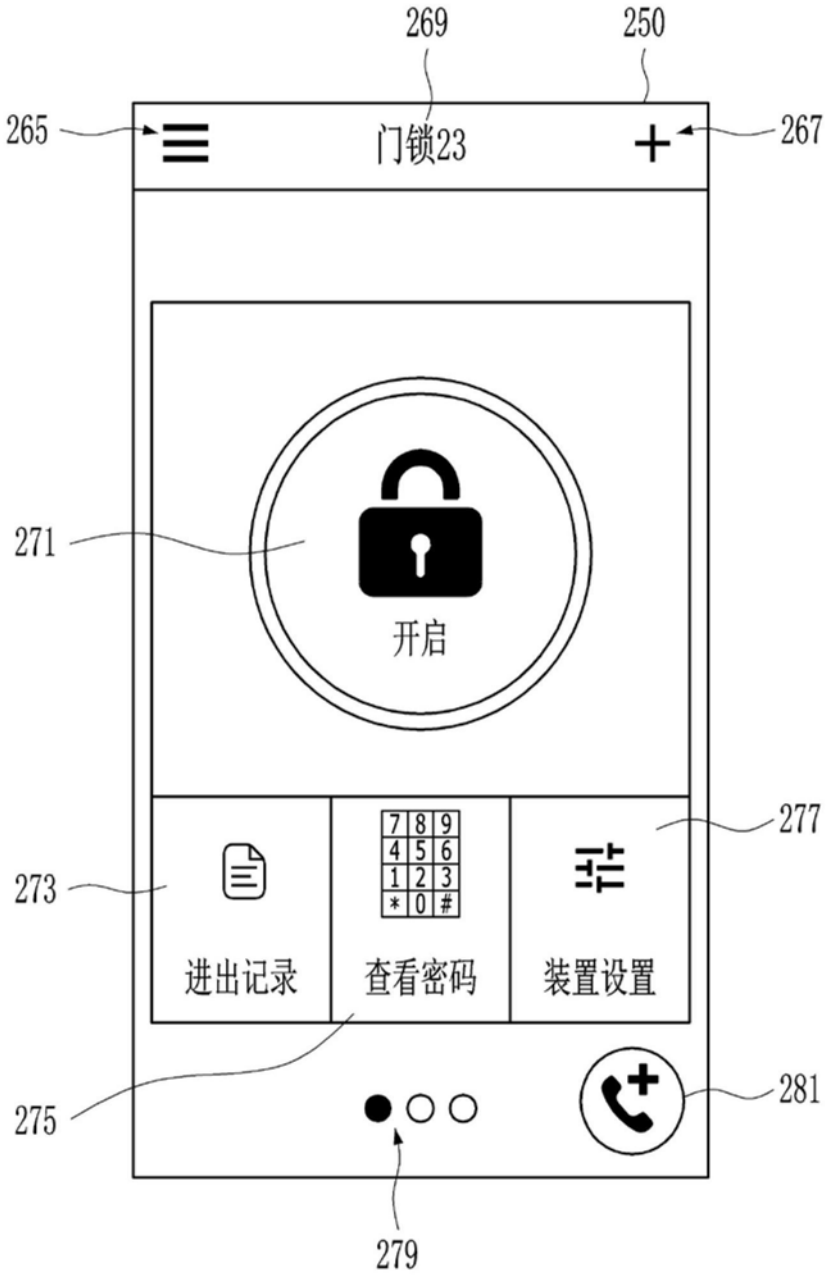


图9

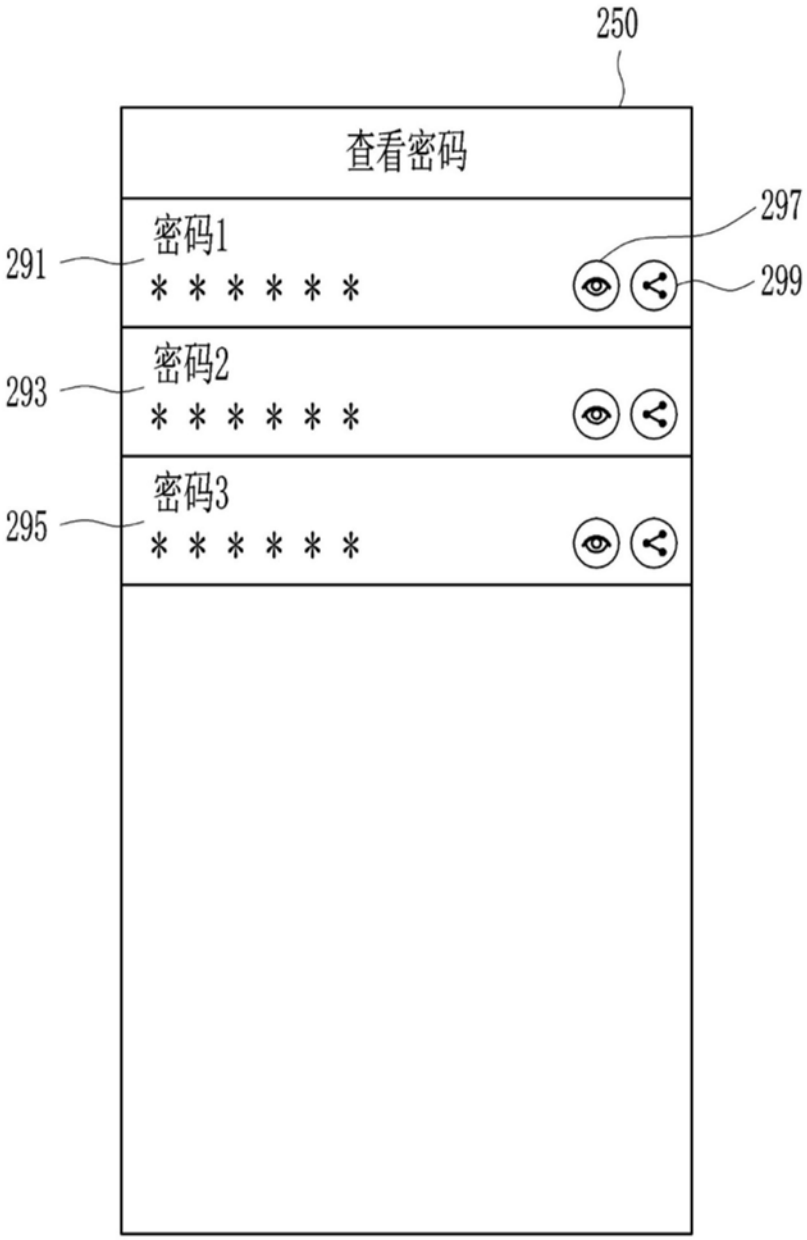


图10

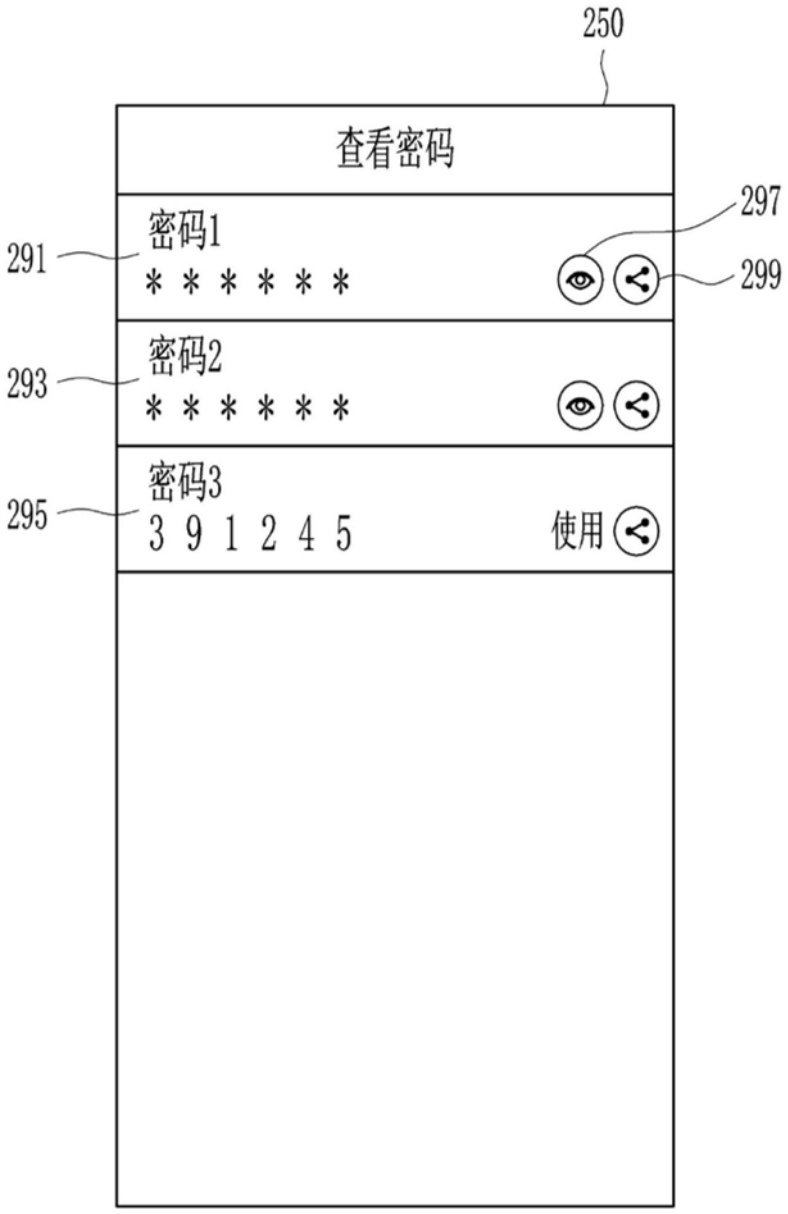


图11

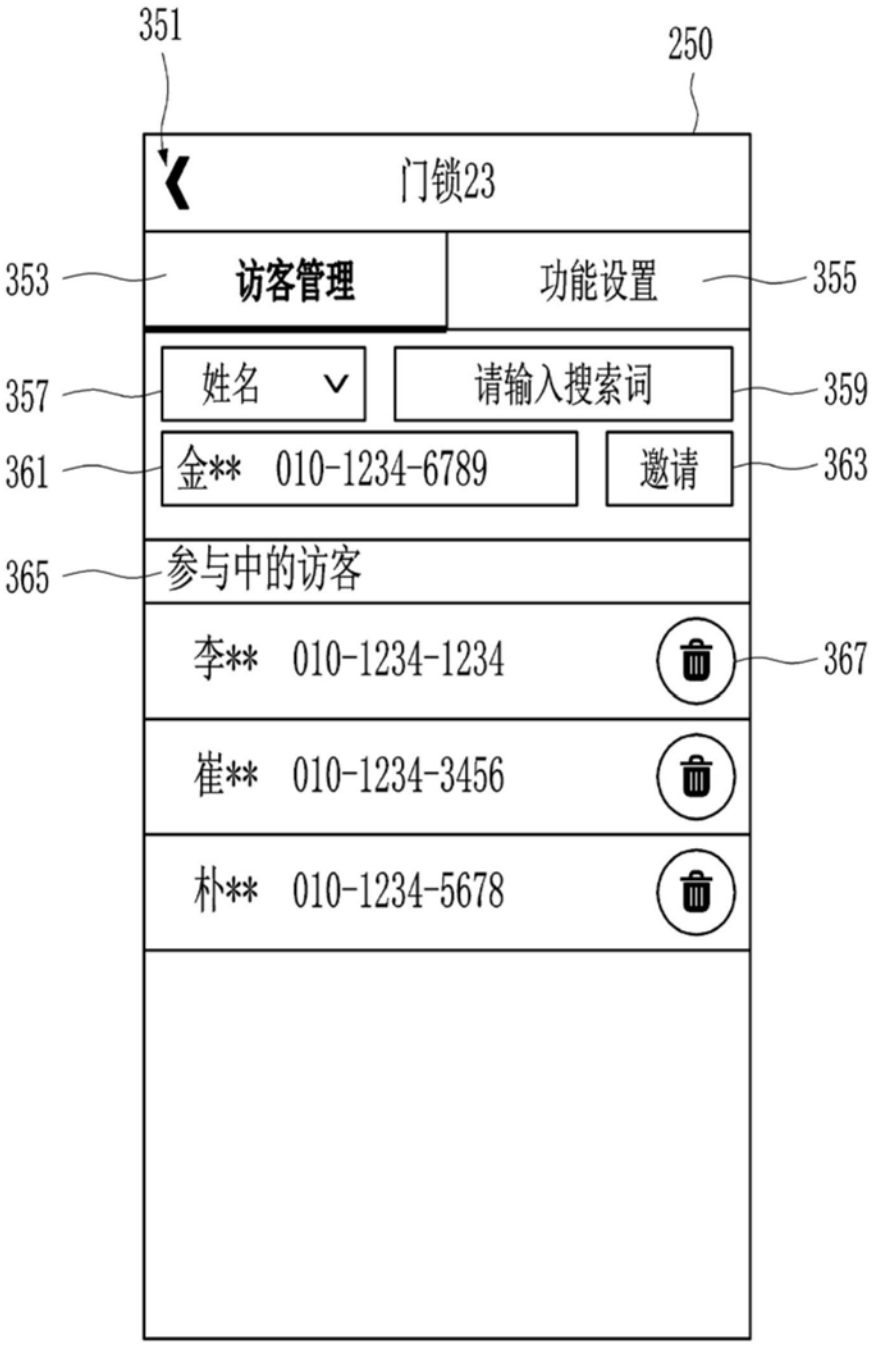

351
250
门锁23
353
访客管理
功能设置
355
357
姓名
请输入搜索词
359
361
金** 010-1234-6789
邀请
363
365
参与中的访客
李** 010-1234-1234
367
崔** 010-1234-3456
朴** 010-1234-5678

图12

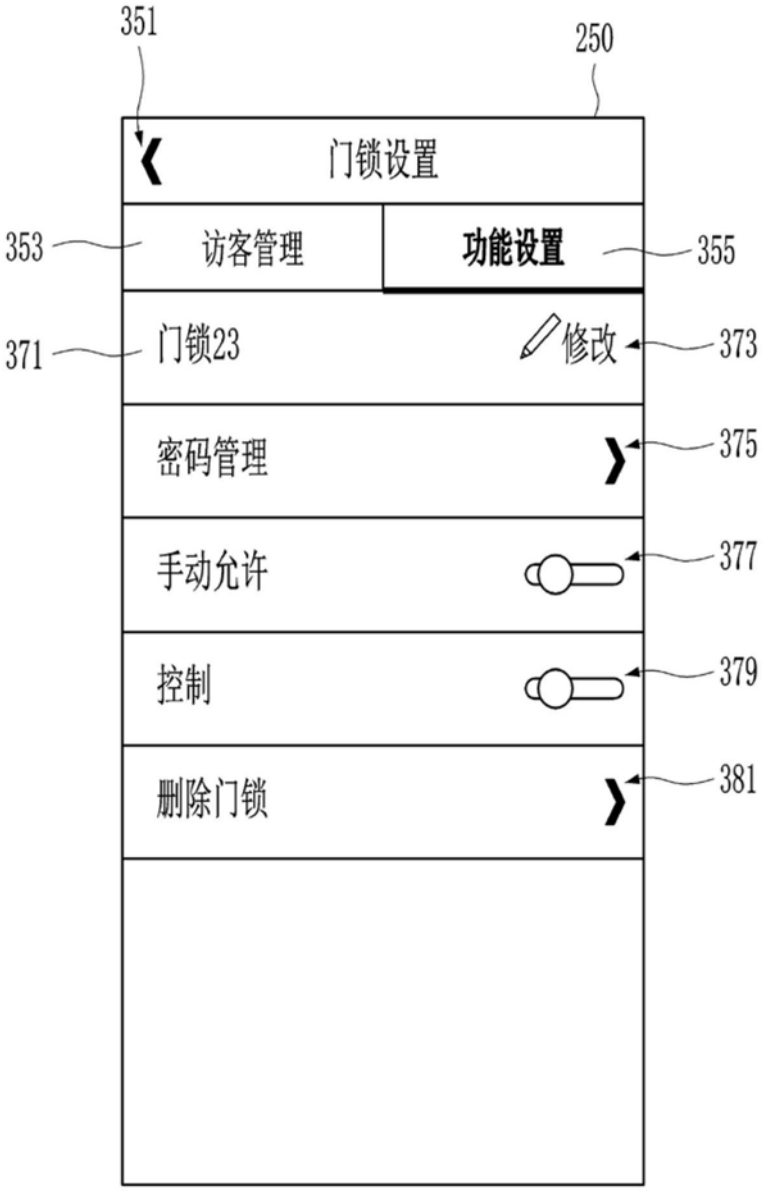

351
250
门锁设置
353
访客管理
功能设置
355
371
门锁23
修改
373
密码管理
375
手动允许
377
控制
379
删除门锁
381

图13