(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 106815905 A
(43)申请公布日 2017.06.09

(21)申请号 201611076752.1

(22)申请日 2016.11.29

(71)申请人 深圳智乐信息科技有限公司
地址 518000 广东省深圳市南山区沙河街道侨城东路锦绣花园一期倚海阁28B

(72)发明人 张哲文

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
G07C 9/00(2006.01)

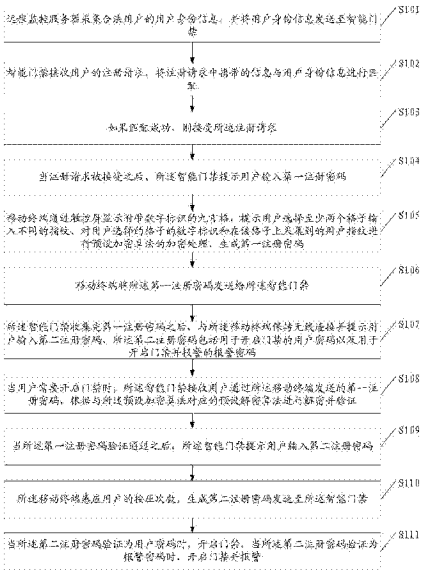
权利要求书2页 说明书7页 附图2页

(54)发明名称

一种基于移动终端验证的方法及系统

(57)摘要

本发明实施例公开了一种基于移动终端验证的方法及系统，方法包括：远程监控服务器采集合法用户的用户身份信息并发送至智能门禁；智能门禁接收用户的注册请求并与用户身份信息进行匹配；如果匹配成功，则接受注册请求；智能门禁提示用户通过移动终端输入第一注册密码和第二注册密码，第一注册密码为加密后的双指纹密码，第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码，第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码；当用户需要开启门禁时，智能门禁验证第二注册密码为报警密码时则报警。采用本发明，可提高智能门禁的安全性和便利性。



CN 106815905 A

1.一种基于移动终端验证的方法，其特征在于，包括：

远程监控服务器采集合法用户的用户身份信息，并将用户身份信息发送至智能门禁；

所述智能门禁接收用户的注册请求，将注册请求中携带的信息与用户身份信息进行匹配；

如果匹配成功，则接受所述注册请求；

当注册请求被接受之后，所述智能门禁提示用户输入第一注册密码；

移动终端通过触控屏显示附带数字标识的九宫格，提示用户选择至少两个格子输入不同的指纹，对用户选择的格子的数字标识和在该格子上采集到的用户指纹进行预设加密算法的加密处理，生成第一注册密码；

移动终端将所述第一注册密码发送给所述智能门禁；

所述智能门禁收集完第一注册密码之后，与所述移动终端保持无线连接并提示用户输入第二注册密码，所述第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码，且所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码；

当用户需要开启门禁时，所述智能门禁接收用户通过所述移动终端发送的第一注册密码，根据与所述预设加密算法对应的预设解密算法进行解密并验证；

当所述第一注册密码验证通过之后，所述智能门禁提示用户输入第二注册密码；

所述移动终端感应用户的按压次数，生成第二注册密码发送至所述智能门禁；

当所述第二注册密码验证为用户密码时，开启门禁，当所述第二注册密码验证为报警密码时，开启门禁并报警。

2.如权利要求1所述的方法，其特征在于，当所述第二注册密码验证为报警密码时，还包括：

远程监控服务器通过监控摄像头对用户及其身边人员进行人脸识别并放大人脸进行拍照，保存人脸识别的结果以及拍摄的照片。

3.如权利要求1所述的方法，其特征在于，还包括：

所述智能门禁将所述第一注册密码和所述第二注册密码发送至所述远程监控服务器保存；

当所述智能门禁进行更换时，所述远程监控服务器将保存的密码数据发送至更换后的智能门禁。

4.如权利要求1所述的方法，其特征在于，当所述第二注册密码验证为报警密码时，还包括：

所述移动终端后台拨打用户预先设定的求救号码。

5.如权利要求1-4任一项所述的方法，其特征在于，所述九宫格中的格子随机排列，所述预设加密算法和所述预设解密算法为非对称密钥，且所述预设加密算法和所述预设解密算法关联并同时动态变化。

6.一种系统，其特征在于，包括：

远程监控服务器，用于采集合法用户的用户身份信息，并将用户身份信息发送至智能门禁；

所述智能门禁，用于接收用户的注册请求，将注册请求中携带的信息与用户身份信息

进行匹配;如果匹配成功,则接受所述注册请求;当注册请求被接受之后,所述智能门禁还用于提示用户输入第一注册密码;

移动终端,用于通过触控屏显示附带数字标识的九宫格,提示用户选择至少两个格子输入不同的指纹,对用户选择的格子的数字标识和在该格子上采集到的用户指纹进行预设加密算法的加密处理,生成第一注册密码;以及将所述第一注册密码发送给所述智能门禁;

所述智能门禁收集完第一注册密码之后,与所述移动终端保持无线连接并提示用户输入第二注册密码,所述第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码,且所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码;当用户需要开启门禁时,所述智能门禁还用于接收用户通过所述移动终端发送的第一注册密码,根据与所述预设加密算法对应的预设解密算法进行解密并验证;当所述第一注册密码验证通过之后,所述智能门禁提示用户输入第二注册密码;

所述移动终端还用于感应用户的按压次数,生成第二注册密码发送至所述智能门禁;

所述智能门禁还用于当所述第二注册密码验证为用户密码时,开启门禁,当所述第二注册密码验证为报警密码时,开启门禁并报警。

7.如权利要求6所述的系统,其特征在于,所述远程监控服务器还用于:

当所述第二注册密码验证为报警密码时,通过监控摄像头对用户及其身边人员进行人脸识别并放大人脸进行拍照,保存人脸识别的结果以及拍摄的照片。

8.如权利要求6所述的系统,其特征在于,所述智能门禁还用于:

将所述第一注册密码和所述第二注册密码发送至所述远程监控服务器保存;

所述远程监控服务器还用于:

当所述智能门禁进行更换时,所述远程监控服务器将保存的密码数据发送至更换后的智能门禁。

9.如权利要求6所述的系统,其特征在于,当所述第二注册密码验证为报警密码时,所述移动终端还用于后台拨打用户预先设定的求救号码。

10.如权利要求6-9任一项所述的系统,其特征在于,所述九宫格中的格子随机排列,所述预设加密算法和所述预设解密算法为非对称密钥,且所述预设加密算法和所述预设解密算法关联并同时动态变化。

一种基于移动终端验证的方法及系统

技术领域

[0001] 本发明涉及智能门禁技术领域，尤其涉及一种基于移动终端验证的方法及系统。

背景技术

[0002] 在门禁系统的发展历程中，密码门禁系统是最原始的，也是最简单，成本最小的，但由于其安全性能比较低，因此渐渐的淡出门禁系统的领域。之后，刷卡门禁系统或者卡片感应门禁系统由于具有耐用、性价比好、读取速度快等优势，故成为当前门禁系统的主流。然而近年来，由于移动终端的飞速发展，其智能性可以为用户带来极大的便利，越来越多的智能门禁开始与移动终端配合来进行门禁的开启。

[0003] 移动终端进行验证的方法虽然先进，但是用户可能丢失被不法份子盗用。此外，用户也可能被威胁不得已使用自己的移动终端来开门。随着智能门禁的不断发展，在传统的门禁系统中，控制器通过接受一定的数据进行身份认证后，即控制开关门的动作。这种门禁系统发送给控制器的数据通常都是用户的移动终端的特定信息。但是无法判断用户使用移动终端进行验证的时候是否是自愿或是遭受胁迫。而在银行、海关、监狱或其它机要部门，对门禁控管的安全要求是很高的，当发生异常情况的时候智能门禁如果只能开门，那么其安全性还是远远不够的。

发明内容

[0004] 本发明实施例所要解决的技术问题在于，提供一种基于移动终端验证的方法及系统。以解决智能门禁安全性不够的问题。

[0005] 为了解决上述技术问题，本发明实施例第一方面提供了一种基于移动终端验证的方法，包括：

[0006] 远程监控服务器采集合法用户的用户身份信息，并将用户身份信息发送至智能门禁；

[0007] 所述智能门禁接收用户的注册请求，将注册请求中携带的信息与用户身份信息进行匹配；

[0008] 如果匹配成功，则接受所述注册请求；

[0009] 当注册请求被接受之后，所述智能门禁提示用户输入第一注册密码；

[0010] 移动终端通过触控屏显示附带数字标识的九宫格，提示用户选择至少两个格子输入不同的指纹，对用户选择的格子的数字标识和在该格子上采集到的用户指纹进行预设加密算法的加密处理，生成第一注册密码；

[0011] 移动终端将所述第一注册密码发送给所述智能门禁；

[0012] 所述智能门禁收集完第一注册密码之后，与所述移动终端保持无线连接并提示用户输入第二注册密码，所述第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码，且所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码；

[0013] 当用户需要开启门禁时，所述智能门禁接收用户通过所述移动终端发送的第一注册密码，根据与所述预设加密算法对应的预设解密算法进行解密并验证；

[0014] 当所述第一注册密码验证通过之后，所述智能门禁提示用户输入第二注册密码；

[0015] 所述移动终端感应用户的按压次数，生成第二注册密码发送至所述智能门禁；

[0016] 当所述第二注册密码验证为用户密码时，开启门禁，当所述第二注册密码验证为报警密码时，开启门禁并报警。

[0017] 本发明实施例第二方面提供了一种系统，包括：

[0018] 远程监控服务器，用于采集合法用户的用户身份信息，并将用户身份信息发送至智能门禁；

[0019] 所述智能门禁，用于接收用户的注册请求，将注册请求中携带的信息与用户身份信息进行匹配；如果匹配成功，则接受所述注册请求；当注册请求被接受之后，所述智能门禁还用于提示用户输入第一注册密码；

[0020] 移动终端，用于通过触控屏显示附带数字标识的九宫格，提示用户选择至少两个格子输入不同的指纹，对用户选择的格子的数字标识和在该格子上采集到的用户指纹进行预设加密算法的加密处理，生成第一注册密码；以及将所述第一注册密码发送给所述智能门禁；

[0021] 所述智能门禁收集完第一注册密码之后，与所述移动终端保持无线连接并提示用户输入第二注册密码，所述第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码，且所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码；当用户需要开启门禁时，所述智能门禁还用于接收用户通过所述移动终端发送的第一注册密码，根据与所述预设加密算法对应的预设解密算法进行解密并验证；当所述第一注册密码验证通过之后，所述智能门禁提示用户输入第二注册密码；

[0022] 所述移动终端还用于感应用户的按压次数，生成第二注册密码发送至所述智能门禁；

[0023] 所述智能门禁还用于当所述第二注册密码验证为用户密码时，开启门禁，当所述第二注册密码验证为报警密码时，开启门禁并报警。

[0024] 实施本发明实施例，具有如下有益效果：

[0025] 通过将智能门禁、移动终端和远程监控服务器连接构成智能门禁系统，用户通过智能门禁和远程监控服务器在确认用户身份后进行注册，确保用户身份的正确性；然后由移动终端和智能门禁配合录入第一注册密码以及第二注册密码；用户可以通过验证密码的方式开启门禁，由于第一注册密码为双指纹密码，因此安全性更高，且使用了加密后的双指纹密码作为第一注册密码，非法分子更难破解，安全性也更高；而由于加入了第二注册密码，因此相对于单一密码的方式，安全性更高，且第二注册密码的输入方式为数字或不同预设时间内分别按压不同次数，如果按压则隐秘性较强，且第二注册密码包括用户密码和报警密码，利于用户被威胁时，隐秘的报警，充分提升了智能门禁的安全性。

附图说明

[0026] 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。

[0027] 图1是本发明实施例一种基于移动终端验证的方法的流程示意图；

[0028] 图2是本发明实施例一种系统的组成示意图。

具体实施方式

[0029] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0030] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0031] 请参照图1，为本发明实施例一种基于移动终端验证的方法的流程示意图，在本实施例中，所述方法包括以下步骤：

[0032] S101，远程监控服务器采集合法用户的用户身份信息，并将用户身份信息发送至智能门禁。

[0033] 可选地，用户身份信息包括用户生物特征信息、身份证信息、照片、手机号码、个人设定密码中的至少一个，为了确保用户身份的正确性，可以多种信息结合使用，以便录入系统的为合法用户的信息。

[0034] S102，智能门禁接收用户的注册请求，将注册请求中携带的信息与用户身份信息进行匹配。

[0035] S103，如果匹配成功，则接受所述注册请求。

[0036] S104，当注册请求被接受之后，所述智能门禁提示用户输入第一注册密码。

[0037] S105，移动终端通过触控屏显示附带数字标识的九宫格，提示用户选择至少两个格子输入不同的指纹，对用户选择的格子的数字标识和在该格子上采集到的用户指纹进行预设加密算法的加密处理，生成第一注册密码。

[0038] 可选地，所述九宫格中的格子随机排列。这样可以避免被非法分子查看用户使用的哪些手指的指纹，也无法确定格子的数字标识。

[0039] 由于需要输入至少两个不同的指纹，因此安全性比常规单一指纹的安全性更高。且所述九宫格中的格子可以随机排列。这样每次用户输入的位置都发生变化，不易被其他非法用户盗用。例如，用户选择了在九宫格中的1格输入右手食指指纹，在6格输入右手中指指纹，则用户在验证密码时可同时以右手食指敲击1格，右手中指敲击6格，当然，也可以先以右手食指敲击1格，再以右手中指敲击6格，1格和6格的位置每次可能发生变化，且在解锁时输入指纹的顺序可以相同也可以不同，本发明实施例不作任何限定。

[0040] S106，移动终端将所述第一注册密码发送给所述智能门禁。

[0041] S107，所述智能门禁收集完第一注册密码之后，提示用户输入第二注册密码，所述

第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码，且所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码。

[0042] 单一的生物密码安全性较低，存在被复制盗用的可能，现有的智能门禁采用上述单一密码非常容易发生密码被非法人员获取的情况，因此，在本实施例中，引入第二注册密码用以提高密码的安全性。第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码，且所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码。这样，用户在正常使用时，可以输入用户密码正常开启智能门禁，也可以在被威胁时输入报警密码，在开启门禁的同时由智能门禁报警，为了提高安全性，此处的报警为秘密报警，所述秘密报警的实现方式通常是，门禁连接设置在保安室的报警铃，通过开关信号控制警铃报警，而威胁份子并不知道报警已经发生，也可以由远程管理服务器实时接收门禁的报警，向保安室报警或通过连接在远程监控服务器的调制解调器拨打110报警，或者还可以直接由智能门禁的调制解调器后台拨打110报警。本发明实施例不作任何限定。

[0043] 报警密码与用户密码不同，当报警密码为数字密码时，其可以是比用户密码位数更少的数字密码，例如用户密码为5位，报警密码为1位，用户输入完之后按确认键即可被智能门禁接收并判定为报警密码进行报警处理。而当报警密码为按压密码时，第一预设时间和第二预设时间可以相同也可以不同，第一次数和第二次数可以相同也可以不同，例如，第一个5秒钟内按压3次，第二个3秒内按压4次等。当第一预设时间到达后，移动终端可以通过“嘀”的声音提示用户。将按压移动终端触控屏作为第二注册密码，且此处的按压和触摸或敲击不同，按压可以在持续触摸触控屏的时候进行按压，移动终端通过压力感应器感应压力大小来判断按压次数，而触摸次数和敲击次数则不同，因此按压操作隐秘性较强，不易被查看或听取后盗用；且按压必须在第一注册密码验证之后才具备可用性，因此在第一注册密码未验证通过时，无需处理检测到的按压，可以避免去处理用户误操作或无意识操作。虽然设置了两个密码，但是用户输入十分方便简单，只需在扫描输入双指纹之后按压移动终端触控屏即可，相对单一的密码，既提高了智能门禁的安全性，又避免了复杂流程带来的麻烦，用户使用体验较佳。且第二注册密码不是一个时间内的单一按压，隐秘性更强，可以提高第二注册密码的复杂度和安全度。

[0044] S108，当用户需要开启门禁时，所述智能门禁接收用户通过所述移动终端发送的第一注册密码，根据与所述预设加密算法对应的预设解密算法进行解密并验证。

[0045] 可选地，所述预设加密算法和所述预设解密算法为非对称密钥，且所述预设加密算法和所述预设解密算法关联并同时动态变化。

[0046] 其中，对称密钥加密也叫秘密/专用密钥加密(Secret Key Encryption,SKE)，即发送和接收数据的双方必须使用相同的/对称的密钥对明文进行加密和解密运算。非对称密钥加密也叫公开密钥加密(Public Key Encryption,PKE)，是指每个人都有一对唯一对应的密钥：公开密钥和私有密钥，公钥对外公开，私钥由个人秘密保存；用其中一把密钥来加密，就只能用另一把密钥来解密。发送数据的一方用另一方的公钥对发送的信息进行加密，然后由接受者用自己的私钥进行解密。公开密钥加密技术解决了密钥的发布和管理问题，是目前商业密码的核心。使用公开密钥技术，进行数据通信的双方可以安全地确认对方

身份和公开密钥，提供通信的可鉴别性。

[0047] 可选地，所述加密算法和解密算法对应且同时动态变化。例如，可以协商多套对应的加解密算法，然后是每次使用时约定使用其中一套，移动终端可以通过发送算法标识信息来告知智能门禁。这样动态变化的加解密算法可以进一步提升系统的安全性。

[0048] 通过发送加密后的指纹信息作为第一注册密码可以为系统提供双层防护，第一层由加密算法构成的解密防护，第二层是由指纹信息的唯一性和复杂性构成的复杂计算防护，使得非法分子无法破解或模拟移动终端发送给智能门禁的信号，保证了系统的安全。

[0049] S109，当所述第一注册密码验证通过之后，所述智能门禁提示用户输入第二注册密码。

[0050] S110，所述移动终端感应用户的按压次数，生成第二注册密码发送至所述智能门禁。

[0051] S111，当所述第二注册密码验证为用户密码时，开启门禁，当所述第二注册密码验证为报警密码时，开启门禁并报警。

[0052] 可选地，当所述第二注册密码验证为报警密码时，还可以由远程监控服务器通过监控摄像头对用户及其身边人员进行人脸识别并放大人脸进行拍照，保存人脸识别的结果以及拍摄的照片。便于后续追踪威胁份子。

[0053] 可选地，当所述第二注册密码验证为报警密码时，还包括：

[0054] 所述移动终端后台拨打用户预先设定的求救号码。进一步丰富报警的方式，提高安全性。

[0055] 可选地，所述移动终端为手机、平板电脑或可穿戴设备。

[0056] 在本实施例中，通过将智能门禁、移动终端和远程监控服务器连接构成智能门禁系统，用户通过智能门禁和远程监控服务器在确认用户身份后进行注册，确保用户身份的正确性；然后由移动终端和智能门禁配合录入第一注册密码以及第二注册密码；用户可以通过验证密码的方式开启门禁，由于第一注册密码为双指纹密码，因此安全性更高，且使用了加密后的双指纹密码作为第一注册密码，非法分子更难破解，安全性也更高；而由于加入了第二注册密码，因此相对于单一密码的方式，安全性更高，且第二注册密码的输入方式为数字或不同预设时间内分别按压不同次数，如果按压则隐秘性较强，且第二注册密码包括用户密码和报警密码，利于用户被威胁时，隐秘的报警，充分提升了智能门禁的安全性。

[0057] 可选地，除了智能门禁本地保存第一注册密码和第二注册密码进行验证之外，还可以通过远程监控服务器进行验证。虽然远程监控服务器进行验证可能效率会稍慢，但是可以进一步提升安全性，尤其在智能门禁出现故障无法验证时，通过远程监控服务器进行验证，可以进一步提升系统工作的稳定性。

[0058] 可选地，当智能门禁损坏或需要进行系统更新，需要更换智能门禁时，所述智能门禁将所述第一注册密码和所述第二注册密码发送至所述远程监控服务器保存；

[0059] 当所述智能门禁进行更换时，所述远程监控服务器将保存的密码数据发送至更换后的智能门禁。

[0060] 从而确保更换前后用户数据的完整性和安全性。

[0061] 当密码多次验证失败后如3次，则智能门禁可以在一段时间内断开与移动终端的连接，或者在一段时间内拒绝移动终端的密码验证请求。

[0062] 请参照图2，为本发明实施例一种系统的组成示意图，在本实施例中，所述系统包括：远程监控服务器200、移动终端300和至少一个智能门禁100。智能门禁100包括用于为远程监控服务器200提供监控画面的摄像头，以及用于解密及验证密码的验证模块。远程监控服务器200包括显示器和用于存储数据的服务器，移动终端包括用于收集用户指纹的收集模块、对指纹进行加密的加密模块以及触控屏。

[0063] 具体地，远程监控服务器200，用于采集小区住户的用户身份信息，并将用户身份信息发送至智能门禁100；

[0064] 所述智能门禁100，用于接收用户的注册请求，将注册请求中携带的信息与用户身份信息进行匹配；

[0065] 如果匹配成功，则接受所述注册请求；

[0066] 当注册请求被接受之后，所述智能门禁100还用于提示用户输入第一注册密码；

[0067] 移动终端300，用于通过触控屏显示附带数字标识的九宫格，提示用户选择至少两个格子输入不同的指纹，对用户选择的格子的数字标识和在该格子上采集到的用户指纹进行预设加密算法的加密处理，生成第一注册密码；以及将所述第一注册密码发送给所述智能门禁；

[0068] 所述智能门禁200还用于收集完第一注册密码之后，与所述移动终端300保持无线连接并提示用户输入第二注册密码，所述第二注册密码为数字密码或为第一预设时间内按压移动终端触控屏第一次数以及第二预设时间内按压移动终端触控屏第二次数的按压密码，且所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码；当用户需要开启门禁时，所述智能门禁100还用于接收用户通过所述移动终端发送的第一注册密码，根据与所述预设加密算法对应的预设解密算法进行解密并验证；当用户需要开启门禁时，所述智能门禁100还用于接收用户通过所述移动终端发送的第一注册密码，根据与所述预设加密算法对应的预设解密算法进行解密并验证；当所述第一注册密码验证通过之后，所述智能门禁200提示用户输入第二注册密码；

[0069] 所述移动终端300还用于感应用户的按压次数，生成第二注册密码发送至所述智能门禁；

[0070] 所述智能门禁200还用于当所述第二注册密码验证为用户密码时，开启门禁，当所述第二注册密码验证为报警密码时，开启门禁并报警。

[0071] 可选地，所述九宫格中的格子随机排列。

[0072] 所述预设加密算法和所述预设解密算法为非对称密钥，且所述预设加密算法和所述预设解密算法关联并同时动态变化。

[0073] 可选地，所述远程监控服务器200还用于：

[0074] 当所述第二注册密码验证为报警密码时，通过监控摄像头对用户及其身边人员进行人脸识别并放大人脸进行拍照，保存人脸识别的结果以及拍摄的照片。

[0075] 所述智能门禁100还用于：

[0076] 将所述第一注册密码和所述第二注册密码发送至所述远程监控服务器200保存；

[0077] 所述远程监控服务器200还用于：

[0078] 当所述智能门禁100进行更换时，所述远程监控服务器200将保存的密码数据发送至更换后的智能门禁。

[0079] 可选地，当所述第二注册密码验证为报警密码时，所述移动终端300还用于后台拨打用户预先设定的求救号码。

[0080] 所述移动终端为手机、平板电脑或可穿戴设备。

[0081] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其它实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0082] 通过上述实施例的描述，本发明具有以下优点：

[0083] 通过将智能门禁、移动终端和远程监控服务器连接构成智能门禁系统，用户通过智能门禁和远程监控服务器在确认用户身份后进行注册，确保用户身份的正确性；然后由移动终端和智能门禁配合录入第一注册密码以及第二注册密码；用户可以通过验证密码的方式开启门禁，由于第一注册密码为双指纹密码，因此安全性更高，且使用了加密后的双指纹密码作为第一注册密码，非法分子更难破解，安全性也更高；而由于加入了第二注册密码，因此相对于单一密码的方式，安全性更高，且第二注册密码的输入方式为数字或不同预设时间内分别按压不同次数，如果按压则隐秘性较强，且第二注册密码包括用户密码和报警密码，利于用户被威胁时，隐秘的报警，充分提升了智能门禁的安全性。

[0084] 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，简称ROM)或随机存储记忆体(Random Access Memory，简称RAM)等。

[0085] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。


远程监控服务器采集合法用户的用户身份信息，并将用户身份信息发送至智能门禁
S101
智能门禁接收用户的注册请求，将注册请求中携带的信息与用户身份信息进行匹配
S102
如果匹配成功，则接受所述注册请求
S103
当注册请求被接受之后，所述智能门禁提示用户输入第一注册密码
S104
移动终端通过触控屏显示附带数字标识的九宫格，提示用户选择至少两个格子输入不同的指纹，对用户选择的格子的数字标识和在该格子上采集到的用户指纹进行预设加密算法的加密处理，生成第一注册密码
S105
移动终端将所述第一注册密码发送给所述智能门禁
S106
所述智能门禁收集完第一注册密码之后，与所述移动终端保持无线连接并提示用户输入第二注册密码，所述第二注册密码包括用于开启门禁的用户密码以及用于开启门禁并报警的报警密码
S107
当用户需要开启门禁时，所述智能门禁接收用户通过所述移动终端发送的第一注册密码，根据与所述预设加密算法对应的预设解密算法进行解密并验证
S108
当所述第一注册密码验证通过之后，所述智能门禁提示用户输入第二注册密码
S109
所述移动终端感应用户的按压次数，生成第二注册密码发送至所述智能门禁
S110
当所述第二注册密码验证为用户密码时，开启门禁，当所述第二注册密码验证为报警密码时，开启门禁并报警
S111

图1

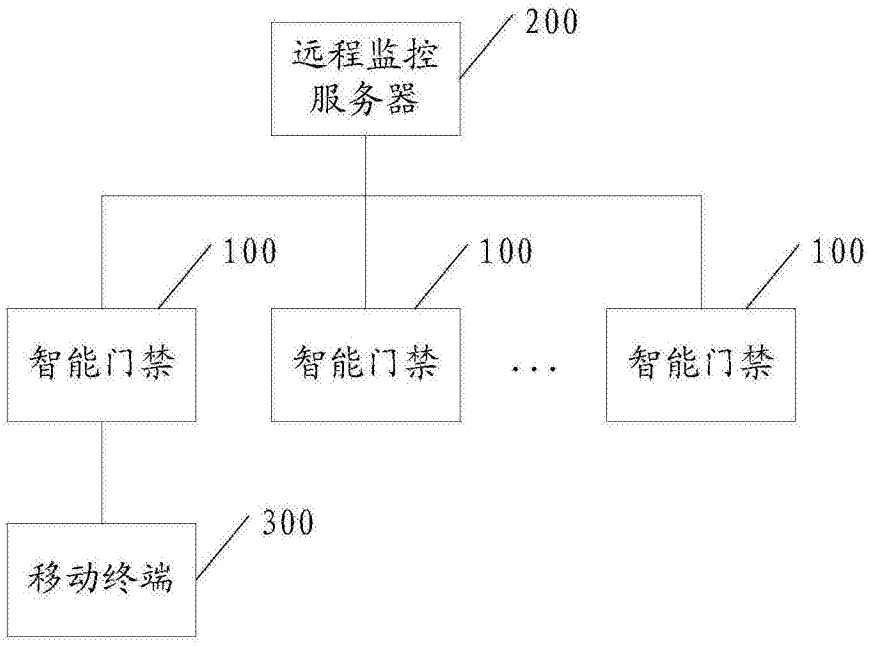


图2