(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 107181742 A
(43)申请公布日 2017.09.19

(21)申请号 201710342131.1

(22)申请日 2017.05.16

(71)申请人 珠海晶通科技有限公司
地址 519085 广东省珠海市唐家湾镇哈工大路1号1栋B201

(72)发明人 夏玥 魏厚武

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 12/14(2006.01)
H04M 1/725(2006.01)
G07C 9/00(2006.01)
B62H 5/00(2006.01)

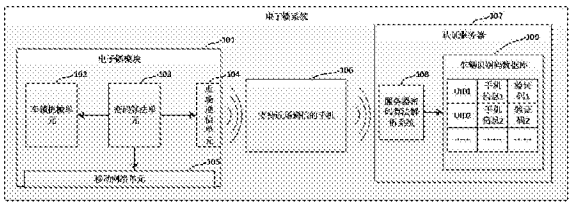
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种共享单车电子锁系统及其开锁方法

(57)摘要

本发明公开了一种共享单车电子锁系统及其开锁方法，所述电子锁系统包括：电子锁模块、支持近场通信的手机和认证服务器。其中，所述的电子锁模块是一种支持近场通信和移动通信方式带有密码算法的电子锁；所述支持近场通信的手机，是具有近场通信技术的智能手机；所述认证服务器包括密码算法解析系统和车辆标识码数据库。本发明利用近场通信技术，增加电子锁和认证服务器之间加密信息交互，提升用户体验，保障信息安全。



CN 107181742 A

1.一种共享单车电子锁系统,其特征在于,包括:电子锁模块,支持近场通信的手机和认证服务器。

2.根据权利要求1所述的一种共享单车电子锁系统,其特征在于,所述的电子锁模块是一种支持近场通信方式和移动通信方式的,带有密码算法及算法流程的电子锁,其包括:车锁机械单元,密码算法单元,近场通信单元,移动通信单元。

3.根据权利要求2所述的电子锁模块,其特征在于,所述的密码算法单元,用于通过对车辆UID(唯一标识码)和随机数进行加密运算,生成随机数密文,并将车辆UID(唯一标识码)验证码的密文通过密码算法进行解密运算,生成车辆UID验证码的明文,并将车辆UID和车辆UID验证码进行配对认证,同时将当前车锁开闭的状态和车辆实时位置通过移动通信单元发送至所述的认证服务器,其中所述的密码算法单元中所包含的密码算法,根据所述电子锁的规格尺寸及功能需求实现一种或多种密码算法,所述的密码算法并不仅限与某一种特定的密码算法,即所有的已存在对称密码算法都可以应用到所述的密码算法系统中。

4.根据权利要求2所述的电子锁模块,其特征在于,所述的近场通信单元,用于利用近场通信技术,将所述的电子锁模块的数据信息通过所述的支持近场通信的手机进行信息交互通信,实现车辆开锁流程的安全认证,该单元将符合NDEF(NFC数据交换格式)的数据信息发送到所述的支持近场通信的手机,所述的支持近场通信的手机会对数据信息通过移动网络连接上所对应的认证服务器。

5.根据权利要求1所述的一种共享单车电子锁系统,其特征在于,所述的支持近场通信的手机,是具有近场通信技术和能够解析符合NDEF(NFC数据交换格式)的智能手机,用于通过具有开锁功能的手机应用软件,利用近场通信技术发送并接收所述电子锁模块的数据信息,通过移动网络连接认证服务器,传递及显示其开锁信息。

6.根据权利要求1所述的一种共享单车电子锁系统,其特征在于,所述的认证服务器包括:密码算法解析系统和车辆识别码数据库。

7.根据权利要求6所述的认证服务器,其特征在于,所述的密码算法解析系统,用于实现车辆UID密文和随机数密文的解密,及车辆UID验证码的加密,当所述的认证服务器接收到随机数密文和车辆UID密文后,通过与所述的密码算法单元中加密算法相同的算法进行解密,从而得到车辆的UID(唯一标识码)和随机数明文;再将车辆UID验证码通过与所述的密码算法单元中加密算法相同的算法进行加密,从而得到车辆UID验证码的密文。

8.根据权利要求6所述的认证服务器,其特征在于,所述的车辆识别码数据库,用于存储所述车辆的UID(唯一标识码),与车辆绑定的手机信息和车辆UID所对应的验证码。

9.一种共享单车的开锁方法,应用于权利要求1至权利要求9的任一项所述的共享单车电子锁系统,其特征在于,包括如下步骤:

a.使用者使用所述的支持近场通信的手机,打开手机应用软件并接触电子锁,手机应用软件通过近场通信功能向所述的电子锁模块发送请求指令;

b.所述电子锁模块接收到请求指令,将车辆UID(唯一标识码)通过所述密码算法单元生成车辆UID的密文EUID,向手机发送车辆UID的密文EUID;

c.所述支持近场通信的手机接收到电子锁UID密文EUID,通过手机应用软件保存该密文,并向所述电子锁模块发送带有随机数R的认证指令;

d.所述电子锁模块接收到带有随机数R的认证指令,将随机数R通过密码算法单元加密

生成E,发送至所述支持近场通信的手机;

e.所述支持近场通信的手机通过手机应用软件将车辆UID密文EUID、随机数R及其密文E、手机号码、手机地理位置信息等手机信息合并发送给所述认证服务器;

f.所述认证服务器内的所述密码算法解析系统通过与所述电子锁模块内的密码算法单元相同的密码算法对车辆UID密文EUID和随机数密文E进行解密,得到车辆UID和随机数R';

g.所述认证服务器内的所述车辆识别码数据库对车辆UID进行索引,同时对随机数R和随机数R'进行比对,若车辆UID索引成功且随机数R和随机数R'比对一致,所述的认证服务器将车辆UID和手机信息绑定并存储于所述的车辆识别码数据库,并将对应的车辆UID验证码V通过所述的服务器密码算法解析系统加密生成车辆UID验证码密文EV,向所述支持近场通信手机中的手机应用软件发送开锁指令和车辆UID验证码密文EV;若车辆UID索引或随机数R和随机数R'比对其中之一不一致,则电子锁认证失败,所述的认证服务器将认证失败信息发送回所述的支持近场通信手机中的手机应用软件;

h.所述的支持近场通信手机通过手机应用软件将开锁指令和车辆UID验证码密文EV发送给所述的电子锁模块;

i.所述的电子锁模块通过所述的密码算法单元将车辆UID验证码密文EV进行解密得到V',验证车辆UID是否与车辆UID验证码V'配对,若配对一致,开锁成功,所述的密码算法单元控制所述的车锁机械单元打开车辆锁体;若配对不一致,开锁失败,所述的电子锁模块将认证失败信息发送至所述的支持近场通信手机中的手机应用软件。

一种共享单车电子锁系统及其开锁方法

技术领域

[0001] 本发明属于共享单车无线通信领域，具体涉及到一种具有近场通信方式、加密算法的电子锁系统及其开锁方法。

背景技术

[0002] 随着共享经济的迅速兴起，共享单车已经成为解决城市公共交通最后一公里最经济、环保的出行方式。当共享单车的盛行，产生了对单车的破坏、据为私有甚至盗窃等行为也逐渐增多；另一方面由于各种共享单车供应商开锁方式的不同，用户开不了锁、需要等长时间开锁或未开锁便开始计费等问题极大影响用户体验。

[0003] 目前共享单车的车锁形式主要分为三种，一种是GPRS电子锁，该电子锁采用GPRS移动网络作为通信方式、GPS作为定位方式，通过手机二维码扫码，手机应用软件将手机信息与车辆信息绑定传输给服务器，服务器通过移动网络通知电子锁开锁，该电子锁耗电高，二维码容易被污损或改写；第二种是蓝牙电子锁，通过手机二维码扫码，电子锁通过与手机蓝牙进行配对，利用手机GPRS和GPS对车辆进行定位和计时扣费，该电子锁对车辆定位和扣费不准确，开锁等待时间长，未使用的车辆无法自身定位容易被盗；第三种是机械锁，通过手机二维码扫码，手机应用软件将手机信息和车辆信息绑定传输给服务器，服务器通过移动网络将车辆的固定开锁密码发送给手机应用软件，用户通过开锁密码打开机械锁。该机械锁的二维码容易被污损或改写，由于密码固定，很容易被破解，车辆容易被盗。

[0004] 解决上述问题，需要一种既具有安全性高又能快速准确开闭锁的电子锁系统。

发明内容

[0005] 本发明针对上述技术问题，提供了一种共享单车电子锁系统及其开闭锁方法，以解决现有共享单车电子锁中易于被破解及用户体验差的问题。

[0006] 本发明解决上述技术问题的技术方案如下：

一种共享单车电子锁系统，包括：电子锁模块，支持近场通信的手机和认证服务器。

[0007] 所述的电子锁模块，是一种支持近场通信方式和移动通信方式的，带有密码算法及算法流程的电子锁，其包括：车锁机械单元，密码算法单元，近场通信单元，移动通信单元。

[0008] 所述的车锁机械单元，用于车辆开闭锁体的机械结构。

[0009] 所述的密码算法单元，用于通过对车辆UID(车辆唯一标识码)和随机数进行加密运算，生成随机数密文，并将车辆UID(车辆唯一标识码)验证码的密文通过密码算法进行解密运算，生成UID验证码的明文，并将车辆UID和UID验证码进行配对认证。

[0010] 所述的近场通信单元，用于利用近场通信技术，将所述的电子锁模块101的数据信息通过所述的支持近场通信的手机105与所述的认证服务器110进行信息交互通信，实现车辆开锁流程的安全认证。

[0011] 所述的移动通信单元，用于通过移动通信网络对车辆实时位置和车锁开闭状态进

行定位和跟踪。

[0012] 所述支持近场通信的手机，是具有近场通信技术和能够解析NFC数据格式的智能手机，用于通过具有开锁功能的手机应用软件，解析所述电子锁模块的数据信息，连接认证服务器，传递及显示其开锁信息。

[0013] 所述的认证服务器，其包括服务器密码算法解析系统和车辆标识码数据库。

[0014] 所述的服务器密码算法解析系统，用于实现对信息进行加解密算法运算。当所述的认证服务器接收到随机数密文和车辆UID密文后，通过与所述的密码算法单元中加密算法相同的算法进行解密，从而得到车辆的UID(唯一标识码)和随机数明文。

[0015] 所述车辆识别码数据库，用于存储所述车辆的UID(唯一标识码)，与车辆绑定的手机信息和车辆UID所对应的验证码等。

[0016] 根据本发明的一方面，还提供了具有一种的开锁方法，应用在上述的电子锁系统中，包括如下步骤：

a.所述支持近场通信的手机通过手机应用软件向所述电子锁模块发送请求指令；

b.所述电子锁模块接收到请求指令，读取存储在所述电子锁模块内部存储器的车辆UID(唯一识别码)，通过密码算法单元中的加密算法生成车辆UID(唯一识别码)的密文EUID，通过近场通信单元发送至所述支持近场通信的手机；

c.所述的支持近场通信的手机接收到电子锁UID密文EUID，通过手机应用软件保存该密文，并向电子锁发送带有随机数R的认证指令；

d.所述的电子锁模块接收到随机数R，将随机数R通过所述的密码算法单元加密生成随机数密文E，将随机数密文E发送至所述支持近场通信的手机；

e.所述支持近场通信的手机通过手机应用软件将车辆UID的密文EUID、随机数R及随机数密文E、手机信息合并发送给所述的认证服务器；

f.所述的认证服务器通过所述的服务器密码算法解析系统对车辆UID的密文EUID和随机数密文E进行解密，得到车辆的UID和随机数R'；

g.所述的认证服务器在所述的车辆识别码数据库中对车辆UID进行索引，同时比较随机数R和随机数R'，若车辆UID索引成功且随机数R和随机数R'比对一致，所述的认证服务器将车辆UID和手机信息绑定并存储于所述的车辆识别码数据库，并将对应的车辆UID验证码V通过所述的服务器密码算法解析系统加密生成车辆UID验证码密文EV，向所述支持近场通信手机中的手机应用软件发送开锁指令和车辆UID验证码密文EV；若车辆UID索引或随机数R和随机数R'比对其中之一不一致，则电子锁认证失败，所述的认证服务器将认证失败信息发送回所述的支持近场通信手机中的手机应用软件；

h.所述的支持近场通信手机通过手机应用软件将开锁指令和车辆UID验证码密文EV发送给所述的电子锁模块；

i.所述的电子锁模块通过所述的密码算法单元将车辆UID验证码密文EV进行解密得到V'，验证车辆UID是否与车辆UID验证码V'配对，若配对一致，则所述的密码算法单元控制所述的车锁机械单元打开车辆锁体；若配对不一致，所述的电子锁模块将认证失败信息发送至所述的支持近场通信手机中的手机应用软件。

[0017] 本发明通过近场通信技术取代原有二维码扫码方式，并加入了电子锁模块与认证服务器之间相互认证和加密安全通信，既解决了原有的开锁二维码易被复制伪造或污损的

缺陷，又让使用者可以容易快速地打开车锁并及时准确计时扣费。同时密码算法系统和相互认证过程的引入提高车锁的破解难度，防止车辆被盗。

附图说明

[0018] 图1为本发明中实施的电子锁系统结构图。

[0019] 图2为本发明实施的共享单车开锁方法流程图。

具体实施方式

[0020] 下面结合附图与具体实施方式对本发明做进一步详细的说明。

[0021] 如图1所示，一种共享单车电子锁系统，包括：电子锁模块101，支持近场通信的手机106，认证服务器107。

[0022] 其中，电子锁模块101是一种支持近场通信方式和移动通信方式的，带有密码算法及算法流程的电子锁，其具体包括：车锁机械单元102，密码算法单元103，近场通信单元104，移动通信单元105。

[0023] 所述的车锁机械单元102，用于车辆开闭锁体的机械结构，该机械结构由所述的密码算法单元所产生的电信号控制，通过也能将开闭锁的状态通过电信号传送至密码算法单元。

[0024] 所述的密码算法单元103，用于通过对车辆UID(唯一标识码)和随机数进行加密运算，生成随机数密文，并将车辆UID(唯一标识码)验证码的密文通过密码算法进行解密运算，生成车辆UID验证码的明文，并将车辆UID和车辆UID验证码进行配对认证，同时将当前车锁开闭的状态和车辆实时位置通过移动通信单元发送至所述的认证服务器。

[0025] 所述的近场通信单元104，用于利用近场通信技术，将所述的电子锁模块101的数据信息通过所述的支持近场通信的手机105进行信息交互通信，实现车辆开锁流程的安全认证。该单元将符合NDEF(NFC数据交换格式)的数据信息发送到所述的支持近场通信的手机，所述的支持近场通信的手机会对数据信息通过移动网络连接上所对应的认证服务器。

[0026] 所述的移动通信单元105，用于通过移动通信网络对车辆实时位置和车锁开闭状态进行定位和跟踪。

[0027] 进一步地，如图1所示，支持近场通信的手机106是电子锁模块101和认证服务器110的通信渠道和显示载体，是具有近场通信技术和能够解析符合NDEF(NFC数据交换格式)的智能手机，用于通过具有开锁功能的手机应用软件，利用近场通信技术发送并接收所述电子锁模块101的数据信息，通过移动网络连接认证服务器107，传递及显示其开锁信息。

[0028] 进一步地，如图1所示，认证服务器107具体包括：服务器密码算法系统108，和车辆识别码数据库109。

[0029] 所述的服务器密码算法解析系统108，用于实现车辆UID密文和随机数密文的解密，及车辆UID验证码的加密。当所述的认证服务器107接收到随机数密文和车辆UID密文后，通过与所述的密码算法单元中加密算法相同的算法进行解密，从而得到车辆的UID(唯一标识码)和随机数明文；再将车辆UID验证码通过与所述的密码算法单元中加密算法相同的算法进行加密，从而得到车辆UID验证码的密文。

[0030] 所述车辆识别码数据库109，用于存储所述车辆的UID(唯一标识码)，与车辆绑定

的手机信息和车辆UID所对应的验证码等。

[0031] 进一步地，如图2所示，本发明还提供了一种共享单车的开锁方法，应用在上述的电子锁系统中，其步骤包括：

步骤S101，使用者使用支持近场通信的手机，打开手机应用软件并接触电子锁，手机应用软件通过近场通信功能向电子锁模块发送请求指令；

步骤S102，电子锁模块接收到请求指令，将车辆UID(唯一标识码)通过密码算法单元生成车辆UID的密文EUID，向手机发送车辆UID的密文EUID；

步骤S103，支持近场通信的手机接收到电子锁UID密文EUID，通过手机应用软件保存该密文，并向电子锁模块发送带有随机数R的认证指令；

步骤S104，电子锁模块接收到带有随机数R的认证指令，将随机数R通过密码算法单元加密生成E，发送至支持近场通信的手机；

步骤S105，手机应用软件将车辆UID密文EUID、随机数R及其密文E、手机号码、手机地理位置信息等手机信息合并发送给认证服务器；

步骤S106，认证服务器内的密码算法解析系统通过与电子锁模块内的密码算法单元相同的密码算法对车辆UID密文EUID和随机数密文E进行解密，得到车辆UID和随机数R'；

步骤S107，认证服务器的车辆识别码数据库对车辆UID进行索引，同时对随机数R和随机数R'进行比对；

如步骤S108所示，如车辆UID存在索引成功且两个随机数比对一致，就进行到步骤S109；若车辆UID索引或随机数R和随机数R'比对其中之一不一致，就进行到步骤S110，电子锁认证失败，认证服务器将认证失败信息发送回支持近场通信手机中的手机应用软件，流程结束；

步骤S109，认证服务器将车辆UID和手机信息进行绑定，通过与电子锁模块内的密码算法单元相同的密码算法将车辆UID验证码V进行加密，生成车辆UID验证码密文EV，向手机应用软件发送开锁指令和车辆UID验证码密文EV；

步骤S111，手机应用软件将开锁指令和车辆UID验证码密文EV发送给电子锁模块；

步骤S112，电子锁模块中的密码算法单元对车辆UID验证码密文EV进行解密，得到车辆UID验证码V'；

如步骤S113所示，若车辆UID与车辆UID验证码V'配对一致，就进行到步骤S114，电子锁模块中的车锁机械单元打开车辆锁体，流程结束；若配对不一致，进行到步骤S115，电子锁模块将认证失败信息发送至支持近场通信手机中的手机应用软件，流程结束。

[0032] 需要说明的是，电子锁模块内部存储器中的密钥与认证服务器中存储的密钥是相同的，并都是使用相同的密码算法。

[0033] 以上对本发明的具体实施进行了描述。需要理解的是，本发明中所提到的密码算法并不仅限于某一种密码算法，即所有的已存在对称密码算法都可以应用到本发明的密码算法系统中；本领域技术人员可以在权利要求的范围内做出各种改进或变形，但这些改进或变形也应视为本发明的保护范围。

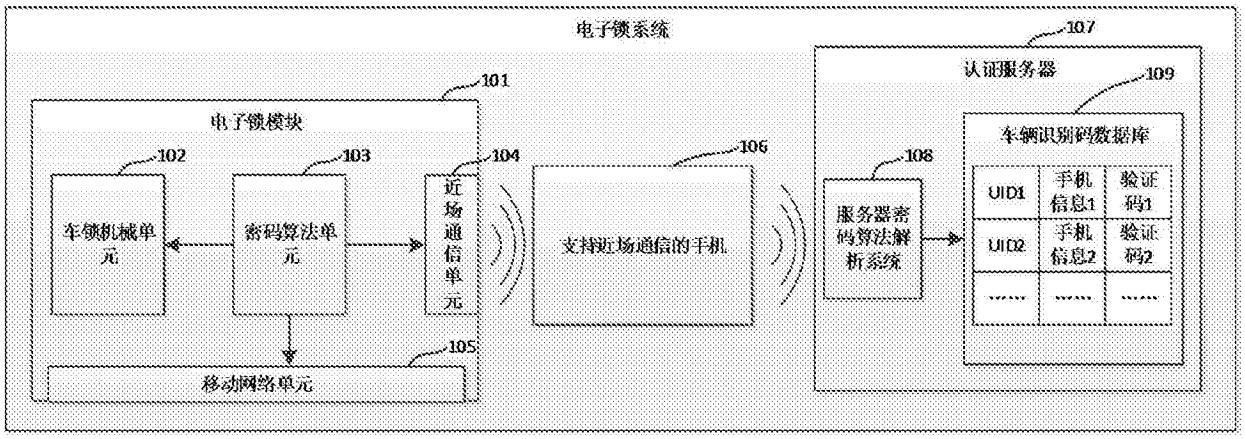

电子锁系统
101
电子锁模块
102
车锁机械单元
103
密码算法单元
104
近场通信单元
105
移动网络单元
106
支持近场通信的手机
107
认证服务器
108
服务器密码算法解析系统
109
车辆识别码数据库
UID1
手机信息1
验证码1
UID2
手机信息2
验证码2
……
……
……

图1

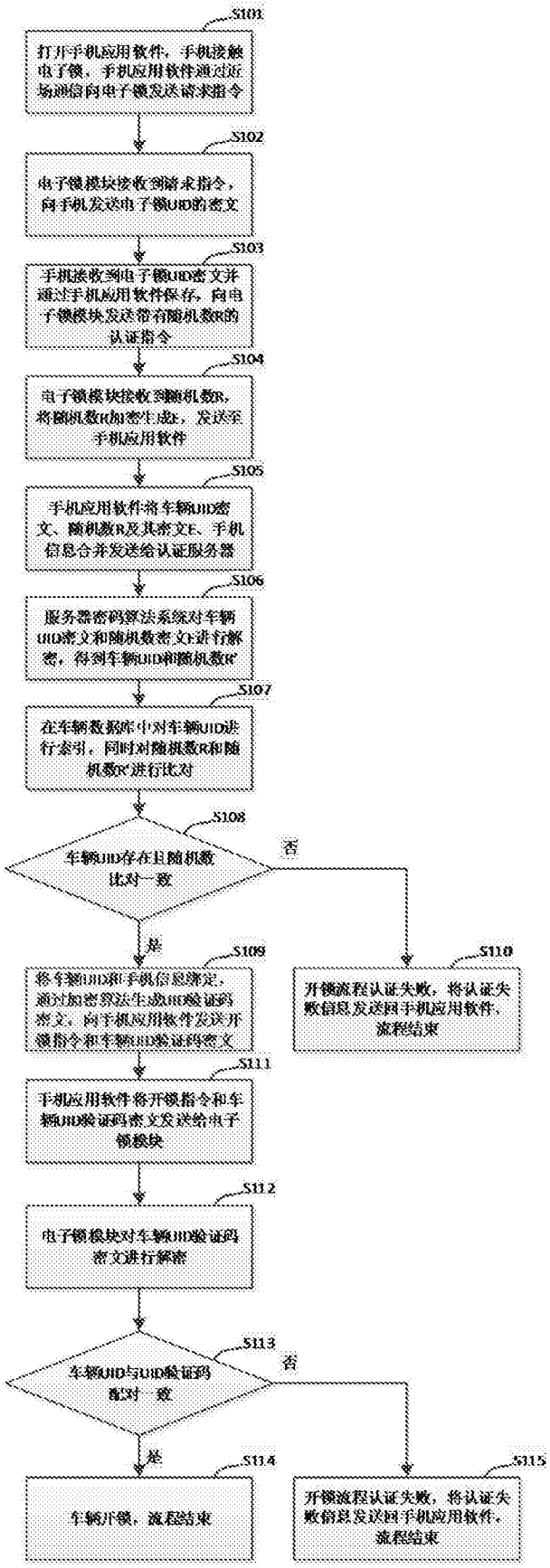

S101
打开手机应用软件，手机接触电子锁，手机应用软件通过近场通信向电子锁发送请求指令
S102
电子锁模块接收到请求指令，向手机发送电子锁UID的密文
S103
手机接收到电子锁UID密文并通过手机应用软件保存，向电子锁模块发送带有随机数R的认证指令
S104
电子锁模块接收到随机数R，将随机数R加密生成E，发送至手机应用软件
S105
手机应用软件将车辆UID密文、随机数R及其密文E、手机信息合并发送给认证服务器
S106
服务器密码算法系统对车辆UID密文和随机数密文E进行解密，得到车辆UID和随机数R'
S107
在车辆数据库中对车辆UID进行索引，同时对随机数R和随机数R'进行比对
S108
车辆UID存在且随机数比对一致
否
是
S109
将车辆UID和手机信息绑定，通过加密算法生成UID验证码密文，向手机应用软件发送开锁指令和车辆UID验证码密文
S110
开锁流程认证失败，将认证失败信息发送回手机应用软件，流程结束
S111
手机应用软件将开锁指令和车辆UID验证码密文发送给电子锁模块
S112
电子锁模块对车辆UID验证码密文进行解密
S113
车辆UID与UID验证码配对一致
否
是
S114
车辆开锁，流程结束
S115
开锁流程认证失败，将认证失败信息发送回手机应用软件，流程结束

图2