



(12) 发明专利

(10) 授权公告号 CN 103295169 B

(45) 授权公告日 2014. 05. 28

(21) 申请号 201310160898. 4

CN 101021919 A, 2007. 08. 22, 全文.

(22) 申请日 2013. 05. 03

审查员 刘永喆

(73) 专利权人 广东裕通科技股份有限公司

地址 510630 广东省广州市天河区中山大道西 136 号裕通大厦 27 层

(72) 发明人 周羽

(74) 专利代理机构 广州嘉权专利商标事务有限公司 44205

代理人 谭英强

(51) Int. Cl.

G06Q 50/16 (2012. 01)

(56) 对比文件

CN 101009018 A, 2007. 08. 01, 全文.

CN 101110728 A, 2008. 01. 23, 全文.

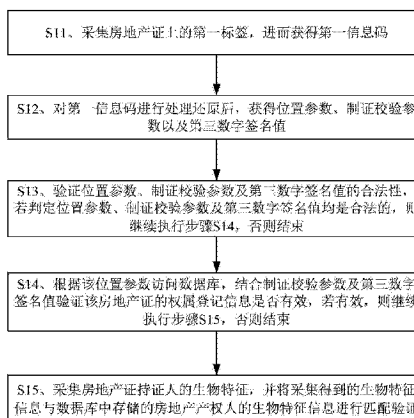
权利要求书3页 说明书12页 附图2页

(54) 发明名称

房地产实人登记信息安全监管方法及系统

(57) 摘要

本发明公开了房地产实人登记信息安全监管方法及系统,该方法包括:采集房地产证上的第一标签,获得第一信息码;对第一信息码进行处理还原,获得位置参数、制证校验参数以及第三数字签名值;验证位置参数、制证校验参数以及第三数字签名值的合法性;验证该房地产证的权属登记信息是否有效;采集房地产证持证人的生物特征,并将其与数据库中存储的房地产权权人的生物特征信息进行匹配验证。本发明可通过采集房地产证上的第一标签以及持证人的生物特征,来验证房地产证以及房地产证持证人的真伪,或通过智能移动终端采集第二标签来进行查询,本发明可对房地产信息进行查询及验证,实现统一监管控制,安全性高,可广泛应用于房地产市场监管领域。



1. 房地产实人登记信息安全监管方法,其特征在于,包括:

S11、采集房地产证上的第一标签,进而获得第一信息码;

S12、对第一信息码进行处理还原后,获得位置参数、制证校验参数以及第三数字签名值;

S13、根据位置参数及制证校验参数的特征,验证位置参数及制证校验参数的合法性,同时对位置参数及制证校验参数进行抽取处理后,将得到的结果与采用第三公钥对第三数字签名值进行解密后得到的结果进行匹配,进而验证第三数字签名值的合法性,若判定位置参数、制证校验参数及第三数字签名值均是合法的,则继续执行步骤 S14,否则结束;

S14、根据该位置参数访问数据库,结合制证校验参数及第三数字签名值验证该房地产证的权属登记信息是否有效,若有效,则继续执行步骤 S15,否则结束;

S15、采集房地产证持证人的生物特征,并将采集得到的生物特征信息与数据库中存储的房地产权权人的生物特征信息进行匹配验证。

2. 根据权利要求 1 所述的房地产实人登记信息安全监管方法,其特征在于,所述步骤 S11 之前还依次包括数据采集步骤、登记步骤及制证步骤,所述数据采集步骤包括:

S01、采集房地产权权人的身份信息以及生物特征信息;

S02、对身份信息、生物特征信息以及采集校验参数进行抽取处理后,采用第一私钥进行加密,生成第一数字签名值,并将采集校验参数、身份信息、生物特征信息以及第一数字签名值发送到信息安全控制子系统;

所述登记步骤包括:

S03、信息安全控制子系统对身份信息、生物特征信息以及采集校验参数进行抽取处理;

S04、将抽取处理得到的结果与采用第一公钥对第一数字签名值进行解密后得到的结果进行匹配,进而验证第一数字签名值的合法性,若判断第一数字签名值为合法的,则继续执行步骤 S05,否则结束;

S05、对身份信息、生物特征信息及登记校验参数进行抽取处理后,采用第二私钥进行加密,生成第二数字签名值,并将身份信息、生物特征信息、采集校验参数、登记校验参数、第一数字签名值以及第二数字签名值存储到数据库中对应的权属登记存储空间上;

所述制证步骤包括:

S06、结合权属登记存储空间上记载的身份信息、生物特征信息、采集校验参数及登记校验参数,验证第一数字签名值及第二数字签名值的合法性,若判断第一数字签名值及第二数字签名值均为合法的,则继续执行步骤 S07,否则结束;

S07、对位置参数及制证校验参数进行抽取处理后,采用第三私钥进行加密,生成第三数字签名值,然后根据位置参数、制证校验参数及第三数字签名值生成用于通过专业设备进行验证的第一信息码;同时对服务接口参数、位置参数及制证校验参数进行抽取处理后,采用第三私钥进行加密,生成第四数字签名值,然后根据服务接口参数、位置参数、制证校验参数及第四数字签名值生成用于通过互联网进行验证的第二信息码;最后将第一信息码及第二信息码存储在权属登记存储空间上;

S08、将第一信息码制成第一标签,同时将第二信息码进行 URL 化后,将得到的 URL 化字符串制成第二标签,进而将房地产权权人的头像印制在房地产证上,并将第一标签及第二

标签记录在房地产证上。

3. 根据权利要求 2 所述的房地产实人登记信息安全监管方法,其特征在于,所述步骤 S08 中将第一标签及第二标签记录在房地产证上,其具体为:

将第一标签及第二标签通过条码、电子芯片、磁条或激光薄膜方式记录在房地产证上。

4. 根据权利要求 2 所述的房地产实人登记信息安全监管方法,其特征在于,所述制证步骤之后还包括查询步骤,所述查询步骤包括:

S21、使用智能移动终端采集房地产证上的第二标签,进而获得 URL 化字符串;

S22、智能移动终端对 URL 化字符串进行解析处理后获得一 URL 地址,以及服务接口参数、位置参数、制证校验参数和第四数字签名值;

S23、智能移动终端访问该 URL 地址,进而将服务接口参数、位置参数、制证校验参数和第四数字签名值发送到查询控制子系统;

S24、查询控制子系统根据服务接口参数、位置参数及制证校验参数的特征,验证服务接口参数、位置参数及制证校验参数的合法性,同时对服务接口参数、位置参数及制证校验参数进行抽取处理后,将得到的结果与采用第三公钥对第四数字签名值进行解密后得到的结果进行匹配,进而验证第四数字签名值的合法性,若判定服务接口参数、位置参数、制证校验参数及第四数字签名值均是合法的,则继续执行步骤 S25,否则结束;

S25、查询控制子系统根据该位置参数,从数据库获得房地产证权属登记的基本信息,并发送到智能移动终端。

5. 根据权利要求 4 所述的房地产实人登记信息安全监管方法,其特征在于,所述步骤 S25 之后还包括步骤:

S26、判断是否接收到进一步查询指令,若接收到进一步查询指令,则执行步骤 S27,否则结束;

S27、验证该智能移动终端是否符合进一步查询的条件,若是,则向该智能移动终端发送房地产证权属登记的所有信息,否则结束。

6. 根据权利要求 1-5 中任一项所述的房地产实人登记信息安全监管方法,其特征在于,该方法还包括权限认证步骤。

7. 房地产实人登记信息安全监管系统,其特征在于,包括数据库、信息安全控制子系统及验证子系统,所述信息安全控制子系统包括第三计算机以及与第三计算机连接的存储模块,所述验证子系统包括第四计算机、验证端生物特征采集仪及标签采集装置;

所述第三计算机分别与第四计算机及数据库连接,所述验证端生物特征采集仪的输出端与第四计算机的第一输入端连接,所述标签采集装置的输出端与第四计算机的第二输入端连接;

还包括数据采集子系统及制证子系统,所述数据采集子系统包括第一计算机、生物特征采集仪及输入装置,所述生物特征采集仪的输出端与第一计算机的第一输入端连接,所述输入装置与第一计算机的第二输入端连接,所述第一计算机与第三计算机连接;

所述制证子系统包括第二计算机,所述第二计算机的输出端分别连接有打印装置及标签记录装置,所述第二计算机与第三计算机连接;

所述数据采集子系统用于对房地产证权属登记信息进行数据采集,所述制证子系统用于制作房地产证,所述生物特征采集仪用于进行生物特征采集,所述打印装置用于将头像

打印到房地产证上,所述标签记录装置用于将生成的标签记录到房地产证上;

所述第一计算机用于进行数据采集综合控制并将采集的数据以及采集校验参数发送到信息安全控制子系统,所述第二计算机用于通过信息安全控制子系统从数据库上获取房地产相关信息并进行处理后生成标签后记录在房地产证上,所述第三计算机用于进行信息安全控制,所述第四计算机用于对房地产证验证进行综合控制处理。

8. 根据权利要求7所述的房地产实人登记信息安全监管系统,其特征在于,所述数据库还依次连接有查询控制子系统及智能移动终端。

9. 根据权利要求7所述的房地产实人登记信息安全监管系统,其特征在于,所述标签记录装置包括条码打印装置、电子芯片读写装置、磁条读写装置或激光薄膜制作装置。

## 房地产实人登记信息安全监管方法及系统

### 技术领域

[0001] 本发明涉及信息安全领域,特别是涉及房地产信息安全的监管方法及系统。

### 背景技术

[0002] 证书、证件或证卡等凭证是人们生活中不可或缺的一部分,是证明人们身份、地位或对财产所有权的重要凭证,而作为人们对房地产所有权凭证的房地产证件,更占据了重要的地位。但是目前各类凭证都或多或少地存在各种安全问题,容易被复制、伪造或盗用,特别是对房地产证件来说,因为各种安全问题而出现的被伪造或盗用等问题,带来的损失尤其严重。因为目前的房地产证件防伪水平一般,假房地产证件往往能做到以假乱真,而且,由于目前房地产证件一般只登记了户主的身份信息,很容易被盗用,即使是登记了户主头像的房地产证件也很容易被人冒用,现有技术无法有效地防止假的持证人冒充房地产产权人。而且,随着社会的发展,房地产的交易、转移也越来越频繁,目前的房地产证件防伪水平低导致在房地产证的制作到后期的查询、变更等方面存在各种漏洞,无法保证房地产登记信息的真实性、安全性。同时,因为目前的房地产信息的不安全性,导致无法进行统一管理、控制;因为无法及时、安全、便捷地查证其登记信息的真伪,反过来又进一步加深了房地产信息的不安全性。

### 发明内容

[0003] 为了解决上述的技术问题,本发明的目的是提供一种可对房地产信息进行统一的监管控制且安全性高的房地产实人登记信息安全监管方法,本发明的另一目的是提供一种可对房地产信息进行统一的监管控制且安全性高的房地产信息安全监管系统。

[0004] 本发明解决其技术问题所采用的技术方案是:

[0005] 房地产实人登记信息安全监管方法,包括:

[0006] S11、采集房地产证上的第一标签,进而获得第一信息码;

[0007] S12、对第一信息码进行处理还原后,获得位置参数、制证校验参数以及第三数字签名值;

[0008] S13、根据位置参数及制证校验参数的特征,验证位置参数及制证校验参数的合法性,同时对位置参数及制证校验参数进行抽取处理后,将得到的结果与采用第三公钥对第三数字签名值进行解密后得到的结果进行匹配,进而验证第三数字签名值的合法性,若判定位置参数、制证校验参数及第三数字签名值均是合法的,则继续执行步骤 S14,否则结束;

[0009] S14、根据该位置参数访问数据库,结合制证校验参数及第三数字签名值验证该房地产证的权属登记信息是否有效,若有效,则继续执行步骤 S15,否则结束;

[0010] S15、采集房地产证持证人的生物特征,并将采集得到的生物特征信息与数据库中存储的房地产产权人的生物特征信息进行匹配验证。

[0011] 进一步,所述步骤 S11 之前还依次包括数据采集步骤、登记步骤及制证步骤,所述

数据采集步骤包括：

[0012] S01、采集房地产产权人的身份信息以及生物特征信息；

[0013] S02、对身份信息、生物特征信息以及采集校验参数进行抽取处理后，采用第一私钥进行加密，生成第一数字签名值，并将采集校验参数、身份信息、生物特征信息以及第一数字签名值发送到信息安全控制子系统；

[0014] 所述登记步骤包括：

[0015] S03、信息安全控制子系统对身份信息、生物特征信息以及采集校验参数进行抽取处理；

[0016] S04、将抽取处理得到的结果与采用第一公钥对第一数字签名值进行解密后得到的结果进行匹配，进而验证第一数字签名值的合法性，若判断第一数字签名值为合法的，则继续执行步骤 S05，否则结束；

[0017] S05、对身份信息、生物特征信息及登记校验参数进行抽取处理后，采用第二私钥进行加密，生成第二数字签名值，并将身份信息、生物特征信息、采集校验参数、登记校验参数、第一数字签名值以及第二数字签名值存储到数据库中对应的权属登记存储空间上；

[0018] 所述制证步骤包括：

[0019] S06、结合权属登记存储空间上记载的身份信息、生物特征信息、采集校验参数及登记校验参数，验证第一数字签名值及第二数字签名值的合法性，若判断第一数字签名值及第二数字签名值均为合法的，则继续执行步骤 S07，否则结束；

[0020] S07、对位置参数及制证校验参数进行抽取处理后，采用第三私钥进行加密，生成第三数字签名值，然后根据位置参数、制证校验参数及第三数字签名值生成用于通过专业设备进行验证的第一信息码；同时对服务接口参数、位置参数及制证校验参数进行抽取处理后，采用第三私钥进行加密，生成第四数字签名值，然后根据服务接口参数、位置参数、制证校验参数及第四数字签名值生成用于通过互联网进行验证的第二信息码；最后将第一信息码及第二信息码存储在权属登记存储空间上；

[0021] S08、将第一信息码制成第一标签，同时将第二信息码进行 URL 化后，将得到的 URL 化字符串制成第二标签，进而将房地产产权人的头像印制在房地产证上，并将第一标签及第二标签记录在房地产证上。

[0022] 进一步，所述步骤 S08 中将第一标签及第二标签记录在房地产证上，其具体为：

[0023] 将第一标签及第二标签通过条码、电子芯片、磁条或激光薄膜方式记录在房地产证上。

[0024] 进一步，所述制证步骤之后还包括查询步骤，所述查询步骤包括：

[0025] S21、使用智能移动终端采集房地产证上的第二标签，进而获得 URL 化字符串；

[0026] S22、智能移动终端对 URL 化字符串进行解析处理后获得一 URL 地址，以及服务接口参数、位置参数、制证校验参数和第四数字签名值；

[0027] S23、智能移动终端访问该 URL 地址，进而将服务接口参数、位置参数、制证校验参数和第四数字签名值发送到查询控制子系统；

[0028] S24、查询控制子系统根据服务接口参数、位置参数及制证校验参数的特征，验证服务接口参数、位置参数及制证校验参数的合法性，同时对服务接口参数、位置参数及制证校验参数进行抽取处理后，将得到的结果与采用第三公钥对第四数字签名值进行解密后得

到的结果进行匹配,进而验证第四数字签名值的合法性,若判定服务接口参数、位置参数、制证校验参数及第四数字签名值均是合法的,则继续执行步骤 S25,否则结束;

[0029] S25、查询控制子系统根据该位置参数,从数据库获得房地产证权属登记的基本信息,并发送到智能移动终端。

[0030] 进一步,所述步骤 S25 之后还包括步骤:

[0031] S26、判断是否接收到进一步查询指令,若接收到进一步查询指令,则执行步骤 S27,否则结束;

[0032] S27、验证该智能移动终端是否符合进一步查询的条件,若是,则向该智能移动终端发送房地产证权属登记的所有信息,否则结束。

[0033] 进一步,该方法还包括权限认证步骤。

[0034] 本发明解决其技术问题所采用的另一技术方案是:

[0035] 房地产实人登记信息安全监管系统,包括数据库、信息安全控制子系统及验证子系统,所述信息安全控制子系统包括第三计算机以及与第三计算机连接的存储模块,所述验证子系统包括第四计算机、验证端生物特征采集仪及标签采集装置;

[0036] 所述第三计算机分别与第四计算机及数据库连接,所述验证端生物特征采集仪的输出端与第四计算机的第一输入端连接,所述标签采集装置的输出端与第四计算机的第二输入端连接。

[0037] 进一步,还包括数据采集子系统及制证子系统,所述数据采集子系统包括第一计算机、生物特征采集仪及输入装置,所述生物特征采集仪的输出端与第一计算机的第一输入端连接,所述输入装置与第一计算机的第二输入端连接,所述第一计算机与第三计算机连接;

[0038] 所述制证子系统包括第二计算机,所述第二计算机的输出端分别连接有打印装置及标签记录装置,所述第二计算机与第三计算机连接。

[0039] 进一步,所述数据库还依次连接有查询控制子系统及智能移动终端。

[0040] 进一步,所述标签记录装置包括条码打印装置、电子芯片读写装置、磁条读写装置或激光薄膜制作装置。

[0041] 本发明的有益效果是:本发明的房地产实人登记信息安全监管方法,通过采集房地产权权人的身份信息、生物特征信息,并对其进行处理后进行数字签名,进而将得到的数字签名值以及房地产权权人的身份信息和生物特征信息等信息存储在数据库中,进而结合数据库上记载的数据生成用于通过专业设备进行验证的第一信息码以及用于通过互联网进行验证的第二信息码,然后分别对第一信息码和第二信息码进行处理,得到第一标签及第二标签并印制在房地产证上,从而可采集第二标签后通过互联网进行查询验证、获取权属登记信息等,或者通过专业设备采集第一标签结合采集房地产证持证人的生物特征,来验证房地产证所记载的权属登记信息以及房地产证持证人的真伪。因此,本方法可对房地产权属登记信息进行查询及管理,实现对房地产信息的统一监管控制,安全性高。

[0042] 而且,本方法在数据采集、数据存储以及获取数据制作房地产证等过程中均采用对应的私钥进行加密生成数字签名值,便于对这些过程事件或数据进行溯源,保证了信息的真实性、完整性,进一步提高了信息监管的安全性。

[0043] 本发明的另一有益效果是:本发明的房地产实人登记信息安全监管系统,可通过

采集房地产产权人的身份信息、生物特征信息,并对其进行处理后进行数字签名,进而将得到的数字签名值以及房地产产权人的身份信息和生物特征信息等信息存储在数据库中,进而结合数据库上记载的数据生成用于通过专业设备进行验证的第一信息码以及用于通过互联网进行验证的第二信息码,然后分别对第一信息码和第二信息码进行处理,得到第一标签及第二标签并印制在房地产证上,从而可通过采集第二标签后通过互联网进行查询验证、获取权属登记信息等,或者通过专业设备采集第一标签结合采集房地产证持证人的生物特征,来验证房地产证所记载的权属登记信息以及房地产证持证人的真伪。因此,本系统可对房地产信息进行查询及管理,实现对房地产权属登记信息的统一监管控制,安全性高。

[0044] 而且,本系统数据采集、数据存储以及获取数据制作房地产证等过程中均采用对应的私钥进行加密生成数字签名值,便于对这些过程事件或数据进行溯源,保证了信息的真实性、完整性,进一步提高了信息监管的安全性。

### 附图说明

[0045] 下面结合附图和实施例对本发明作进一步说明。

[0046] 图 1 是本发明的房地产实人登记信息安全监管方法的流程图;

[0047] 图 2 是本发明的房地产实人登记信息安全监管方法的查询步骤的流程图;

[0048] 图 3 是本发明的房地产实人登记信息安全监管系统的结构框图。

### 具体实施方式

[0049] 参照图 1,本发明提供了房地产实人登记信息安全监管方法,包括:

[0050] S11、采集房地产证上的第一标签,进而获得第一信息码;

[0051] S12、对第一信息码进行处理还原后,获得位置参数、制证校验参数以及第三数字签名值;

[0052] S13、根据位置参数及制证校验参数的特征,验证位置参数及制证校验参数的合法性,同时对位置参数及制证校验参数进行抽取处理后,将得到的结果与采用第三公钥对第三数字签名值进行解密后得到的结果进行匹配,进而验证第三数字签名值的合法性,若判定位置参数、制证校验参数及第三数字签名值均是合法的,则继续执行步骤 S14,否则结束;

[0053] S14、根据该位置参数访问数据库,结合制证校验参数及第三数字签名值验证该房地产证的权属登记信息是否有效,若有效,则继续执行步骤 S15,否则结束;

[0054] S15、采集房地产证持证人的生物特征,并将采集得到的生物特征信息与数据库中存储的房地产产权人的生物特征信息进行匹配验证。

[0055] 进一步作为优选的实施方式,所述步骤 S11 之前还依次包括数据采集步骤、登记步骤及制证步骤,所述数据采集步骤包括:

[0056] S01、采集房地产产权人的身份信息以及生物特征信息;

[0057] S02、对身份信息、生物特征信息以及采集校验参数进行抽取处理后,采用第一私钥进行加密,生成第一数字签名值,并将采集校验参数、身份信息、生物特征信息以及第一数字签名值发送到信息安全控制子系统;

[0058] 所述登记步骤包括:



[0059] S03、信息安全控制子系统对身份信息、生物特征信息以及采集校验参数进行抽取处理；

[0060] S04、将抽取处理得到的结果与采用第一公钥对第一数字签名值进行解密后得到的结果进行匹配,进而验证第一数字签名值的合法性,若判断第一数字签名值为合法的,则继续执行步骤 S05,否则结束；

[0061] S05、对身份信息、生物特征信息及登记校验参数进行抽取处理后,采用第二私钥进行加密,生成第二数字签名值,并将身份信息、生物特征信息、采集校验参数、登记校验参数、第一数字签名值以及第二数字签名值存储到数据库中对应的权属登记存储空间上；

[0062] 所述制证步骤包括：

[0063] S06、结合权属登记存储空间上记载的身份信息、生物特征信息、采集校验参数及登记校验参数,验证第一数字签名值及第二数字签名值的合法性,若判断第一数字签名值及第二数字签名值均为合法的,则继续执行步骤 S07,否则结束；

[0064] S07、对位置参数及制证校验参数进行抽取处理后,采用第三私钥进行加密,生成第三数字签名值,然后根据位置参数、制证校验参数及第三数字签名值生成用于通过专业设备进行验证的第一信息码；同时对服务接口参数、位置参数及制证校验参数进行抽取处理后,采用第三私钥进行加密,生成第四数字签名值,然后根据服务接口参数、位置参数、制证校验参数及第四数字签名值生成用于通过互联网进行验证的第二信息码；最后将第一信息码及第二信息码存储在权属登记存储空间上；

[0065] S08、将第一信息码制成第一标签,同时将第二信息码进行 URL 化后,将得到的 URL 化字符串制成第二标签,进而将房地产产权人的头像印制在房地产证上,并将第一标签及第二标签记录在房地产证上。

[0066] 进一步作为优选的实施方式,所述步骤 S08 中将第一标签及第二标签记录在房地产证上,其具体为：

[0067] 将第一标签及第二标签通过条码、电子芯片、磁条或激光薄膜方式记录在房地产证上。

[0068] 进一步作为优选的实施方式,参照图 2,所述制证步骤之后还包括查询步骤,所述查询步骤包括：

[0069] S21、使用智能移动终端采集房地产证上的第二标签,进而获得 URL 化字符串；

[0070] S22、智能移动终端对 URL 化字符串进行解析处理后获得一 URL 地址,以及服务接口参数、位置参数、制证校验参数和第四数字签名值；

[0071] S23、智能移动终端访问该 URL 地址,进而将服务接口参数、位置参数、制证校验参数和第四数字签名值发送到查询控制子系统；

[0072] S24、查询控制子系统根据服务接口参数、位置参数及制证校验参数的特征,验证服务接口参数、位置参数及制证校验参数的合法性,同时对服务接口参数、位置参数及制证校验参数进行抽取处理后,将得到的结果与采用第三公钥对第四数字签名值进行解密后得到的结果进行匹配,进而验证第四数字签名值的合法性,若判定服务接口参数、位置参数、制证校验参数及第四数字签名值均是合法的,则继续执行步骤 S25,否则结束；

[0073] S25、查询控制子系统根据该位置参数,从数据库获得房地产证权属登记的基本信息,并发送到智能移动终端。

[0074] 进一步作为优选的实施方式,所述步骤 S25 之后还包括步骤:

[0075] S26、判断是否接收到进一步查询指令,若接收到进一步查询指令,则执行步骤 S27,否则结束;

[0076] S27、验证该智能移动终端是否符合进一步查询的条件,若是,则向该智能移动终端发送房地产证权属登记的所有信息,否则结束。

[0077] 进一步作为优选的实施方式,该方法还包括权限认证步骤。

[0078] 参照图 3,本发明还提供了一种房地产实人登记信息安全监管系统,包括数据库、信息安全控制子系统及验证子系统,所述信息安全控制子系统包括第三计算机以及与第三计算机连接的存储模块,所述验证子系统包括第四计算机、验证端生物特征采集仪及标签采集装置;

[0079] 所述第三计算机分别与第四计算机及数据库连接,所述验证端生物特征采集仪的输出端与第四计算机的第一输入端连接,所述标签采集装置的输出端与第四计算机的第二输入端连接。

[0080] 进一步作为优选的实施方式,还包括数据采集子系统及制证子系统,所述数据采集子系统包括第一计算机、生物特征采集仪及输入装置,所述生物特征采集仪的输出端与第一计算机的第一输入端连接,所述输入装置与第一计算机的第二输入端连接,所述第一计算机与第三计算机连接;

[0081] 所述制证子系统包括第二计算机,所述第二计算机的输出端分别连接有打印装置及标签记录装置,所述第二计算机与第三计算机连接。

[0082] 进一步作为优选的实施方式,所述数据库还依次连接有查询控制子系统及智能移动终端。

[0083] 进一步作为优选的实施方式,所述标签记录装置包括条码打印装置、电子芯片读写装置、磁条读写装置或激光薄膜制作装置。

[0084] 下面结合具体实施例对本发明做进一步说明:

[0085] 参照图 3,本发明的房地产实人登记信息安全监管系统的一实施例如下:

[0086] 包括数据库、信息安全控制子系统、验证子系统、数据采集子系统及制证子系统,信息安全控制子系统包括第三计算机以及与第三计算机连接的存储模块,验证子系统包括第四计算机、验证端生物特征采集仪及标签采集装置;

[0087] 数据采集子系统包括第一计算机、生物特征采集仪及输入装置,生物特征采集仪的输出端与第一计算机的第一输入端连接,输入装置与第一计算机的第二输入端连接;

[0088] 制证子系统包括第二计算机,第二计算机的输出端分别连接有打印装置及标签记录装置;

[0089] 第三计算机分别与第一计算机、第二计算机、第四计算机及数据库连接;

[0090] 验证端生物特征采集仪的输出端与第四计算机的第一输入端连接,标签采集装置的输出端与第四计算机的第二输入端连接;

[0091] 数据库还依次连接有查询控制子系统及智能移动终端;

[0092] 标签记录装置包括条码打印装置、电子芯片读写装置、磁条读写装置或激光薄膜制作装置。

[0093] 第一计算机用于进行数据采集综合控制并将采集的数据以及采集校验参数发送

到信息安全控制子系统；第二计算机用于通过信息安全控制子系统从数据库上获取房地产相关信息并进行处理后生成标签后记录在房地产证上；与第三计算机连接的存储模块用于存储不同操作者的基本信息以及相应的权限信息等安全凭证信息，第三计算机用于进行信息安全控制，主要是在系统进行数据采集步骤、登记步骤、制证步骤或验证步骤时加入数字签名步骤和 / 或权限认证步骤，从而达到信息安全控制的目的；第四计算机用于对房地产证验证进行综合控制处理。

[0094] 数据采集子系统用于对房地产证权属登记信息进行数据采集；制证子系统用于制作房地产证；生物特征采集仪用于进行生物特征采集；打印装置用于将头像打印到房地产证上；标签记录装置用于将生成的标签记录到房地产证上；数据库实际上可分为多个权属登记存储空间，每个权属登记存储空间用于存储房地产权属登记信息以及该存储记录相应的操作参数，权属登记信息包括房地产产权人的身份信息、生物特征信息，以及房地产的面积、坐落、结构、楼层、产权的法律状态等，这里，因为房地产的面积、坐落、结构、楼层、产权的法律状态等信息是房地产证的常规属性，因此不单独对其采集及存储进行描述，操作参数包括采集校验参数、登记校验参数、制证校验参数以及在数据采集步骤、登记步骤或制证步骤中生成的各种数字签名值等；验证子系统用于验证房地产证的真伪以及房地产证持有人是否为房地产权人；标签采集装置用于采集房地产证上的标签信息。

[0095] 生物特征采集仪包括照相机、摄像头、指纹采集仪、掌纹采集仪、虹膜采集装置、声纹采集仪器或 DNA 检验仪器等仪器中的一种或多种。相应地，在进行验证时，验证端生物特征采集仪需采用对应的仪器进行采集。本发明中采集到的生物特征包括头像、指纹、掌纹、虹膜、声纹或 DNA 等。

[0096] 智能移动终端用于供房地产证持证人进行信息查询，采集房地产证上的第二标签，进而获得 URL 化字符串后，对 URL 化字符串进行解析处理后获得一 URL 地址，以及服务接口参数、位置参数、制证校验参数和第三数字签名值，然后智能移动终端访问该 URL 地址，进而将服务接口参数、位置参数、制证校验参数和第三数字签名值发送到查询控制子系统。智能移动终端包括可进入互联网的手机、平板电脑等。

[0097] 查询控制子系统用于对智能移动终端的操作进行响应及控制，例如，对智能移动终端返回的位置参数、制证校验参数以及第三数字签名值进行响应及处理。

[0098] 本系统中，标签采集装置是与标签记录装置对应使用的，当标签记录装置采用条码打印装置时，标签采集装置采用条码读取装置；当标签记录装置采用电子芯片读写装置时，标签采集装置可采用电子芯片读写装置；当标签记录装置采用磁条读写装置时，标签采集装置可采用磁条读写装置；当标签记录装置采用激光薄膜制作装置时，标签采集装置可采用激光薄膜识别装置；依次类推。

[0099] 结合上述房地产实人登记信息安全监管系统的实施例，本发明的房地产实人登记信息安全监管方法的一具体实施例如下：

[0100] 房地产实人登记信息安全监管方法，包括数据采集步骤、登记步骤、制证步骤、验证步骤及权限认证步骤，所述制证步骤之后还包括查询步骤，所述数据采集步骤包括：

[0101] S01、采集房地产权人的身份信息以及生物特征信息。

[0102] S02、对身份信息、生物特征信息以及采集校验参数使用杂凑算法抽取处理后，采用第一私钥进行加密，生成第一数字签名值，并将采集校验参数、身份信息、生物特征信息

以及第一数字签名值发送到信息安全控制子系统。

[0103] 步骤 S01 及 S02 是在数据采集子系统中进行的。身份信息包括姓名、性别、身份证种类(身份证、军官证或护照等)、身份证号码等信息;房地产产权人的生物特征信息包括头像、指纹、掌纹、虹膜、声纹或 DNA 等信息。采集校验参数包括进行数据采集的时间以及操作人的标识码等。这里,操作人,指使用数据采集子系统对房地产产权人进行信息采集的操作人。

[0104] 所述登记步骤包括:

[0105] S03、信息安全控制子系统对身份信息、生物特征信息以及采集校验参数使用杂凑算法抽取处理。

[0106] S04、将抽取处理得到的结果与采用第一公钥对第一数字签名值进行解密后得到的结果进行匹配,进而验证第一数字签名值的合法性,若判断第一数字签名值为合法的,则继续执行步骤 S05,否则结束。

[0107] S05、对身份信息、生物特征信息及登记校验参数使用杂凑算法抽取处理后,采用第二私钥进行加密,生成第二数字签名值,并将身份信息、生物特征信息、采集校验参数、登记校验参数、第一数字签名值以及第二数字签名值存储到数据库中对应的权属登记存储空间上。

[0108] 具体地,步骤 S03 及 S04 为:信息安全控制子系统对身份信息、生物特征信息以及采集校验参数使用杂凑算法抽取处理后,得到一个固定长度的数据,如长度为 16 字节的数据;然后根据预设的密钥数据库,寻找到与第一私钥对应的第一公钥,并采用第一公钥对第一数字签名值进行解密后得到一个固定长度的数据,如长度为 16 字节的数据;对这两组固定长度的数据进行匹配,从而根据匹配结果,来验证第一数字签名值的合法性。匹配规则是信息安全控制子系统预先设定的,例如,可设定匹配规则是两组数据相等时,第一数字签名值才是合法的。在本方法的其它步骤中,也可采用与此类似的方法类判断第二数字签名值、第三数字签名值及第四数字签名值等其它数字签名值的合法性。

[0109] 密钥数据库是预先设立的,记载着每个操作人的标志码以及其对应的公钥。而每个操作人的私钥是由操作人自己保管的,可以是采用类似 U 盾的载体存储的,当操作人进行数据采集、登记或制证时,需要将存储有其私钥的载体连接到对应的数据采集子系统、信息安全控制子系统或制证子系统上再进行操作。每一个私钥及其对应的公钥构成一对密钥。本申请中,第一私钥及第一公钥指进行数据采集的操作人所对应的一对密钥,第二私钥及第二公钥指将采集的数据核对后存储到数据库的操作人所对应的一对密钥,第三私钥及第三公钥指进行房地产证制作的操作人所对应的一对密钥。

[0110] 步骤 S05 中,登记校验参数包括进行数据存储的时间以及操作人的标识码等。这里的操作人,指使用信息安全控制子系统将房地产权属登记信息存储到数据库上的操作人。这里,将登记校验参数结合房地产权属登记的其它信息生成第二数字签名值,并存储到数据库中对应的权属登记存储空间上,可对房地产权属登记信息的存储操作人以及操作事件进行追溯。通过验证第二数字签名值的合法性也可以验证房地产权属登记信息的真实性。

[0111] 本发明的数据库是预先建立的用于存储房地产权属登记信息的,可为每一个独立的房地产权属登记操作提供一个独立的存储空间,即权属登记存储空间。

[0112] 所述制证步骤包括：

[0113] S06、结合权属登记存储空间上记载的身份信息、生物特征信息、采集校验参数及登记校验参数，验证第一数字签名值及第二数字签名值的合法性，若判断第一数字签名值及第二数字签名值均为合法的，则继续执行步骤 S07，否则结束；这里，与步骤 S03 及 S04 类似，是对身份信息、生物特征信息以及采集校验参数使用杂凑算法抽取处理后，将抽取处理得到的结果与采用第一公钥对第一数字签名值进行解密后得到的结果进行匹配，进而验证第一数字签名值的合法性；以及对身份信息、生物特征信息以及登记校验参数使用杂凑算法抽取处理后，将抽取处理得到的结果与采用第二公钥对第二数字签名值进行解密后得到的结果进行匹配，进而验证第二数字签名值的合法性。

[0114] S07、对位置参数及制证校验参数使用杂凑算法抽取处理后，采用第三私钥进行加密，生成第三数字签名值，然后根据位置参数、制证校验参数及第三数字签名值生成用于通过专业设备进行验证的第一信息码；同时对服务接口参数、位置参数及制证校验参数使用杂凑算法抽取处理后，采用第三私钥进行加密，生成第四数字签名值，然后根据服务接口参数、位置参数、制证校验参数及第四数字签名值生成用于通过互联网进行验证的第二信息码；最后将第一信息码及第二信息码存储在权属登记存储空间上。将第一信息码及第二信息码存储到数据库上是为了进行备份。制证校验参数包括进行制证的时间以及制证操作人的标识码等。第三数字签名值及第四数字签名值均是采用第三私钥进行加密生成的，区别是两者加密的对象不同，而两者在后续进行验证的过程中，也都采用了第三公钥。

[0115] 服务接口参数包括用于进行查询等各种服务的门户网站地址以及用于区分不同房地产证的服务编码。制作房地产证过程中，也可以将服务接口参数印制在房地产证上，从而可通过门户网站进行查询。

[0116] S08、将第一信息码制成第一标签，同时将第二信息码进行 URL 化后，将得到的 URL 化字符串制成第二标签，进而将房地产产权人的头像印制在房地产证上，并将第一标签及第二标签通过条码、电子芯片、磁条或激光薄膜方式记录在房地产证上。这里，URL 化处理指将位置参数、制证校验参数以及第三数字签名值进行处理后，生成包括 URL 地址的字符串；条码包括条形码及二维码，优先采用二维码，电子芯片包括 RFID 芯片等可进行数据读写的芯片；第二标签为服务标签，用于通过互联网进行验证，例如通过智能移动终端采集第二标签并进行解析处理后，可通过互联网进行验证；第一标签为专业标签，用于通过专业设备进行验证，例如可通过房地产主管部门的权属登记中心的专业设备采集第一标签后进行验证，本发明中专业设备指房地产主管部门设置的用于对标签进行采集的设备，例如本发明中的标签采集装置；这里，将房地产产权人的头像印制在房地产证上时也同时印制了房地产产权人的姓名、服务编号等其它基本信息。将第一标签及第二标签记录到房地产证上时，可对应的在其位置附近印刷其相应的名称，便于识别，例如当第一标签及第二标签均采用二维码时，可在第一标签上方印刷“安全二维码”，在第二标签上方印刷“服务二维码”。

[0117] 步骤 S08 中的印制包括打印或热转移打印等。

[0118] 所述验证步骤包括：

[0119] S11、采集房地产证上的第一标签，进而获得第一信息码。

[0120] S12、对第一信息码进行处理还原后，获得位置参数、制证校验参数以及第三数字签名值。

[0121] S13、根据位置参数及制证校验参数的特征,验证位置参数及制证校验参数的合法性,同时对位置参数及制证校验参数使用杂凑算法抽取处理后,将得到的结果与采用第三公钥对第三数字签名值进行解密后得到的结果进行匹配,进而验证第三数字签名值的合法性,若判定位置参数、制证校验参数及第三数字签名值均是合法的,则继续执行步骤 S14,否则结束;首先按顺序验证位置参数、校验参数及第三数字签名值的合法性,再决定是否继续执行验证操作,可节约操作时间,而且在校验参数不合法的情况下,根本无需对数据库进行进一步访问,提高了安全性。

[0122] S14、根据该位置参数访问数据库,结合制证校验参数及第三数字签名值验证该房地产证的权属登记信息是否有效,若有效,则继续执行步骤 S15,否则结束。例如,根据该位置参数访问数据库,查找到相应的权属登记存储空间,进而验证获得的制证校验参数及第三数字签名值是否与权属登记存储空间所记载的一致,若一致,则证明该房地产证的权属登记信息是有效的,继续执行步骤 S15,否则结束。验证从该房地产证得到的位置参数、校验参数以及第三数字签名值是合法的,并不代表该房地产证的权属登记信息是有效的,因为对房地产证进行注销或更改后,原房地产证对应的权属登记存储空间上存储的信息将被更改、删除或者标记为无效等。因此,这里需要对该房地产证的权属登记信息的有效性进行验证。

[0123] S15、采集房地产证持证人的生物特征,并将采集得到的生物特征信息与数据库中存储的房地产权人的生物特征信息进行匹配验证。通过将采集到的生物特征信息与数据库中存储的房地产权人的生物特征信息进行匹配验证,来验证房地产证持证人是否为房地产权人。当然,这里还可以结合目前常规的检验手段对房地产证的真伪进行鉴别。

[0124] 本申请中,提到的房地产证持证人是指房地产证的持有人,例如交易的另一方或者其它社会公众,并不一定是房地产证上登记的房地产权人。

[0125] 所述查询步骤包括:

[0126] S21、使用智能移动终端采集房地产证上的第二标签,进而获得 URL 化字符串。

[0127] S22、智能移动终端对 URL 化字符串进行解析处理后获得一 URL 地址,以及服务接口参数、位置参数、制证校验参数和第四数字签名值。

[0128] S23、智能移动终端访问该 URL 地址,进而将服务接口参数、位置参数、制证校验参数和第四数字签名值发送到查询控制子系统。

[0129] S24、查询控制子系统根据服务接口参数、位置参数及制证校验参数的特征,验证服务接口参数、位置参数及制证校验参数的合法性,同时对服务接口参数、位置参数及制证校验参数使用杂凑算法抽取处理后,将得到的结果与采用第三公钥对第四数字签名值进行解密后得到的结果进行匹配,进而验证第四数字签名值的合法性,若判定服务接口参数、位置参数、制证校验参数及第四数字签名值均是合法的,则继续执行步骤 S25,否则结束;首先根据服务接口参数、位置参数及制证校验参数等参数的特征,例如参数的长度、字符的属性等,来验证相关参数的合法性,再决定是否继续执行验证操作,当验证服务接口参数、位置参数、制证校验参数是合法的之后,然后再对服务接口参数、位置参数及制证校验参数使用杂凑算法抽取处理后,将得到的结果与采用第三公钥对第四数字签名值进行解密后得到的结果进行匹配,来验证第四数字签名值的合法性,再根据验证结果决定是否执行下一步骤;查询控制子系统通过执行计算机程序来实现本步骤,通过有层次的验证过程,在节约操

作时间的同时,也提高了安全性。

[0130] S25、查询控制子系统根据该位置参数,从数据库获得房地产证权属登记的基本信息,并发送到智能移动终端;本申请中的位置参数指房地产证对应的权属登记存储空间的物理地址或逻辑地址;房地产证权属登记的基本信息包括房地产产权人的姓名、头像、发证机构、发证时间、房地产登记编号等信息。

[0131] S26、查询控制子系统判断是否接收到进一步查询指令,若接收到进一步查询指令,则执行步骤 S27,否则结束。

[0132] S27、查询控制子系统验证该智能移动终端是否符合进一步查询的条件,若是,则向该智能移动终端发送房地产证权属登记的所有信息,否则结束。房地产证权属登记的所有信息包括前面提到的房地产产权人的姓名、头像、发证机构、发证时间、房地产登记编号等信息,还包括房地产产权人的身份证信息、指纹或其它生物特征信息等,以及房地产的面积、坐落、结构、楼层、产权的法律状态等;验证该智能移动终端是否符合进一步查询的条件,可以通过验证智能移动终端的手机号码、唯一的编码、授权码等可以对智能移动终端或其操作者进行标识的标识码来实现的,而且可以结合验证智能移动终端是否可以付费以支付进一步查询的费用等方式来验证其是否符合进一步查询的条件。

[0133] 因此可见,房地产证持有人可以使用手机或其他移动终端执行查询步骤,来进行房地产信息查询,这个查询的基础是建立的数据库以及记录在房地产证上的第二标签。

[0134] 本发明中提到的位置参数、采集校验参数、登记校验参数以及制证校验参数等参数的特征,包括这些参数的定义规则、命名规则、属性等,例如参数的长度、字符的属性等。

[0135] 权限认证步骤不是一个单独的步骤,而是融合在其它步骤中进行权限认证,在数据采集步骤、登记步骤、制证步骤、验证步骤以及查询步骤的每一个子步骤中,均可以先加入权限认证步骤,验证操作者具有操作权限后再执行相应操作,本实施例中,在数据采集步骤、登记步骤、制证步骤及验证步骤中加入了权限认证步骤,权限认证步骤是通过上述房地产实人登记信息安全监管系统中的信息安全控制子系统进行综合控制实现的。在本方法中加入权限认证步骤,确认操作者具有操作权限后再进行操作可以增加监管过程中的安全性,避免非法采集、非法登记、非法制证、非法查询等操作。权限验证可以通过数字证书验证、生物特征验证、授权码验证、口令验证等方式进行。权限认证步骤可以认为是在本方法的任一个或多个子步骤前加入以下操作:

[0136] 验证操作者是否有权限进行操作,若有,则继续执行,否则结束。这里,验证操作者是否有权限进行操作是通过进行数字证书验证、生物特征验证、授权码验证、口令验证等来实现的。

[0137] 显然地,在验证房地产证的真伪时,还可以应用一些现有技术,例如光学光干涉开锁卡、纸质水印、防伪线等,本发明中不对此类现有技术进行详细描述,但是任何采用本发明的技术方案结合此类现有技术手段进行监管的方案都是落在本发明的保护范围中的。

[0138] 本发明将房地产产权人的身份信息以及对其生物特征信息进行数字签名后得到的数字签名值建立的数据库,可便捷、安全地进行查询或验证操作。而且,还可利用该数据库进行一系列监管活动,例如,通过对生物特征信息进行排查锁定,可以迅速地找出数据库中生物特征信息相同的记录,从而便捷地发现同一个人利用不同身份证购房的情况。同时,还可以利用建立的数据库对大范围内的房地产信息进行监管控制,及时发现同一个人在多

地用不同名字、编号的身份证购房的行为。

[0139] 本发明中提到的房地产证指房地产权属证书,包括房屋所有权证、房屋他项权证或房地产权证、房地产他项权证等。

[0140] 在实际操作中,房地产实人登记是按照申请、受理、审核、登簿、发证五个程序进行的。首先,由要进行房地产登记的申请人进行申请,并提供齐全的房地产登记申请材料,包括申请事由、申请人身份信息等;其次,房地产登记机构进行受理,受理程序主要进行以下程序:查验申请主体及申请材料、核对申请登记事项、录入相关信息、采集申请人生物特征等;然后,房地产登记机构执行审核程序,进行以下工作:审核申请材料的一致性及合法性、进行实地查看、公告登记事项等;接着,房地产登记机构执行登簿程序,进行以下工作:按照房地产登记基本单元建立登记簿,然后将房地产的状态、申请人的身份信息以及生物特征信息记录在登记簿上,若为电子登记簿,实际上是将记录的电子登记簿存储在数据库上;最后,房地产登记机构执行发证程序:根据登记簿的记载,制作房地产权属证书及填发登记证明。对应到本发明的房地产实人登记信息安全监管方法,则数据采集步骤体现的是申请、受理、审核 3 个程序,登记步骤体现的是登簿程序,制证步骤体现的是发证程序。

[0141] 以上是对本发明的较佳实施进行了具体说明,但本发明创造并不限于所述实施例,熟悉本领域的技术人员在不违背本发明精神的前提下还可作出种种的等同变形或替换,这些等同的变型或替换均包含在本申请权利要求所限定的范围内。



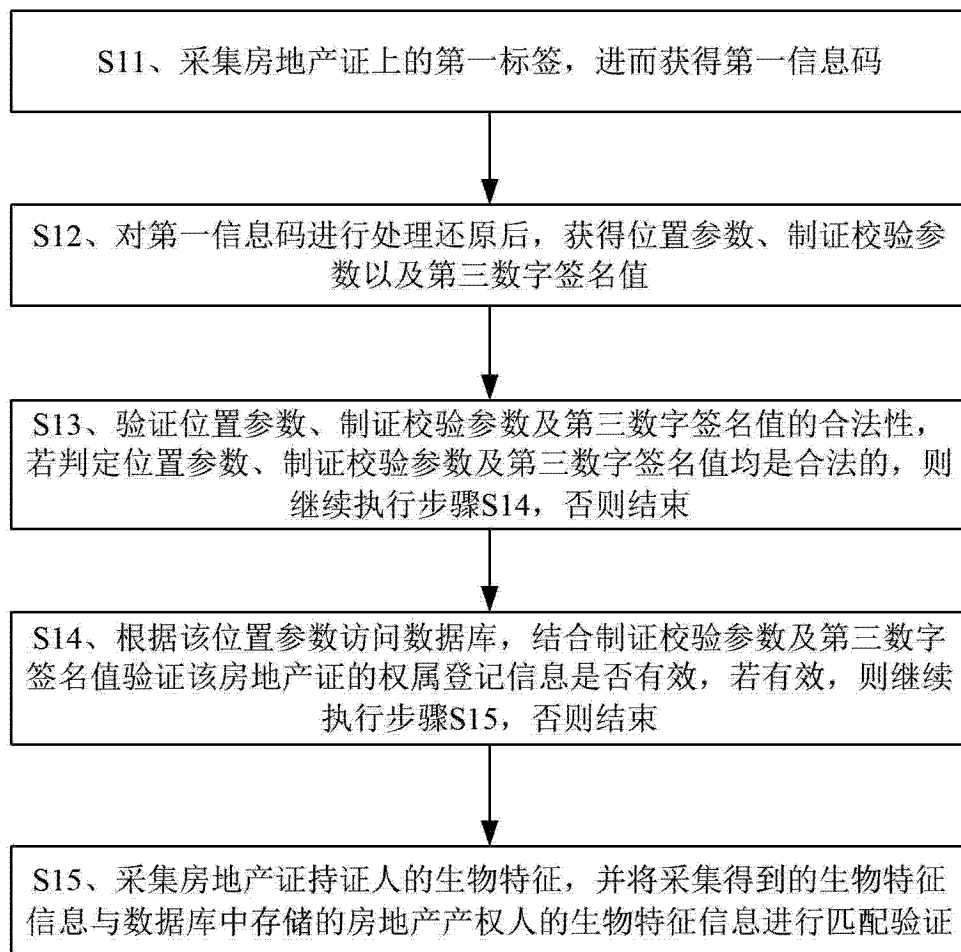


图 1

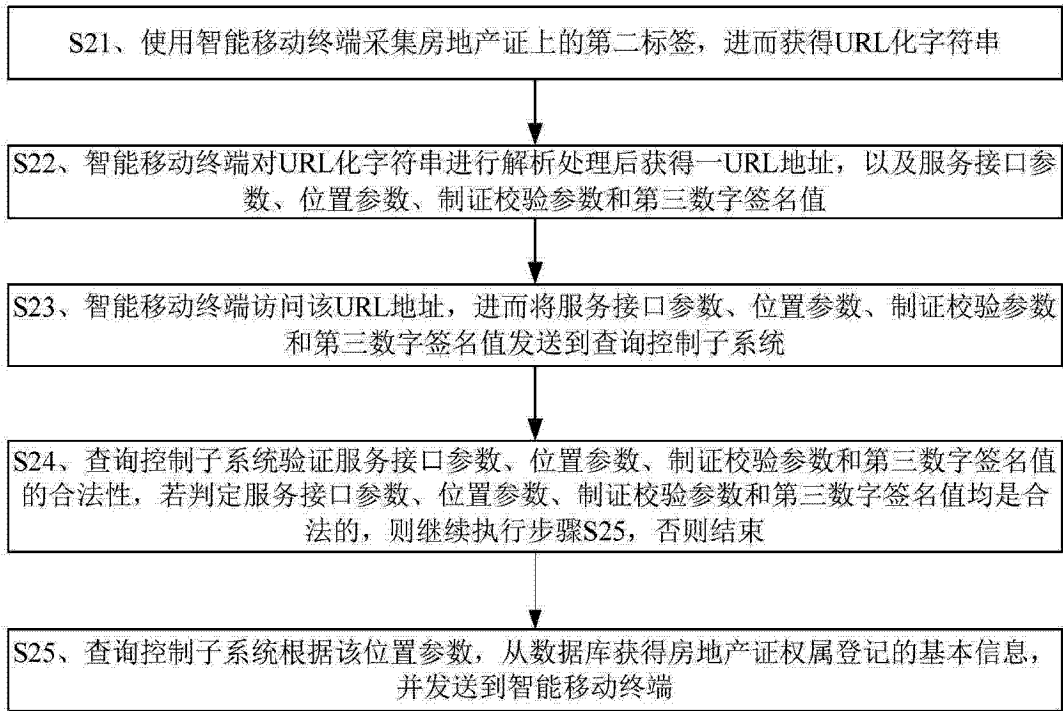


图 2

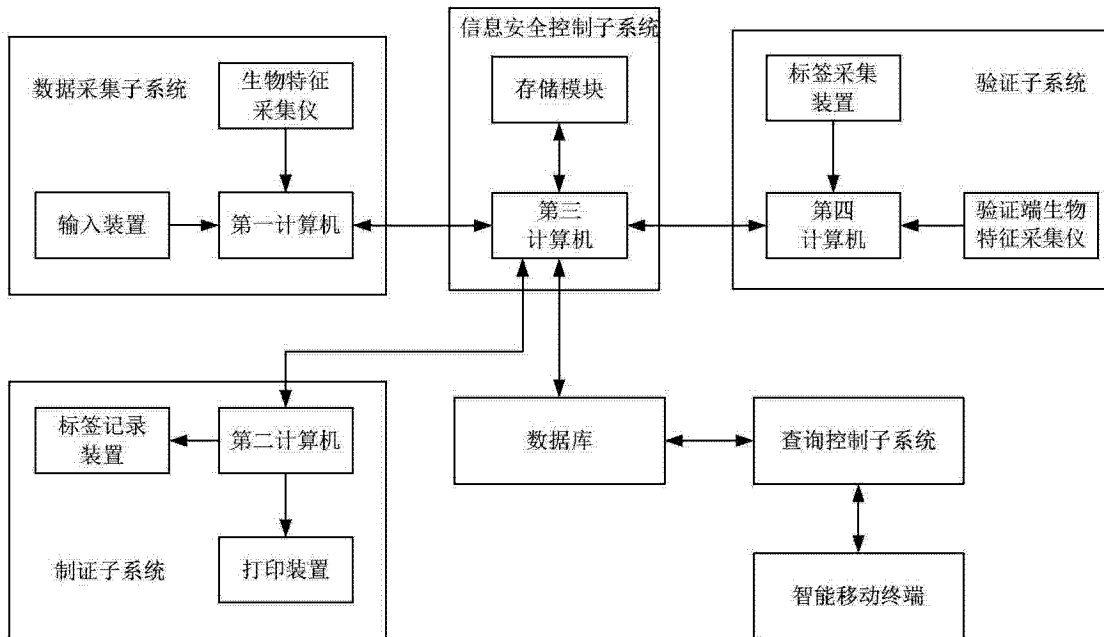


图 3