(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102883323 B
(45)授权公告日 2018.07.27

(21)申请号 201210374448.0

(22)申请日 2012.09.27

(65)同一申请的已公布的文献号
申请公布号 CN 102883323 A

(43)申请公布日 2013.01.16

(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 耿亮

(74)专利代理机构 北京元本知识产权代理事务所 11308
代理人 秦力军

(51)Int.Cl.
H04W 12/06(2009.01)
H04M 1/725(2006.01)

(56)对比文件
CN 101790161 A,2010.07.28,说明书第[0031]-[0037],[0040]-[0041],[0046]-[0054]段.
CN 1933629 A,2007.03.21,说明书第4页第25-26行,第5页第1-3,13-15行.
US 2005164738 A1,2005.07.28,全文.
CN 1606373 A,2005.04.13,全文.
CN 101282534 A,2008.10.08,全文.
CN 101790161 A,2010.07.28,说明书第[0031]-[0037],[0046]-[0054]段.
CN 102307255 A,2012.01.04,全文.

审查员 吕平

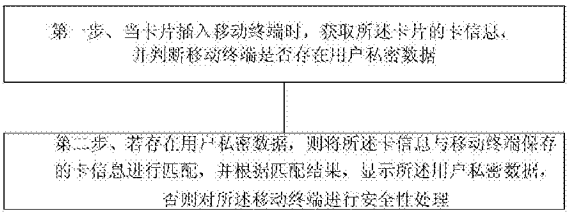
权利要求书1页 说明书5页 附图4页

(54)发明名称

一种保护移动终端用户私密数据的方法和装置

(57)摘要

本发明公开了一种保护移动终端用户私密数据的方法和装置,涉及一种无线终端,所述方法包括:当卡片插入移动终端时,获取所述卡片的卡信息,并判断移动终端是否存在用户私密数据;若判断结果为存在用户私密数据,则将所述卡信息与移动终端保存的卡信息进行匹配,并根据匹配结果,显示所述用户私密数据,以供用户使用;若判断结果为不存在用户私密数据,则对所述移动终端进行安全性处理。本发明能够加强用户私密数据的保护,并且方便用户使用。



CN 102883323 B

1.一种保护移动终端用户私密数据的方法，其特征在于，包括：

当卡片插入移动终端时，获取所插入卡片的卡信息，并判断移动终端是否存在用户私密数据；

若判断结果为存在用户私密数据，则将所插入卡片的卡信息与移动终端保存的卡信息进行匹配处理，并根据匹配处理结果，显示所述用户私密数据，以供用户使用；

若判断结果为不存在用户私密数据，则对所述移动终端进行安全性处理；

其中，当所插入卡片的卡信息与移动终端保存的卡信息不匹配时，利用用户密码信息将所述用户私密数据与卡信息进行绑定。

2.根据权利要求1所述的方法，其特征在于，当所插入卡片的卡信息与移动终端保存的卡信息匹配时，直接显示所述用户私密数据。

3.根据权利要求1所述的方法，其特征在于，当所插入卡片的卡信息与移动终端保存的卡信息不匹配时，利用用户密码将所述用户私密数据与卡信息进行绑定包括：

接收用户后续输入的密码信息，将所述密码信息与移动终端保存的密码信息进行匹配处理；

在所述密码信息与移动终端保存的密码信息匹配时，将所述卡信息与移动终端保存的用户私密数据进行绑定，并显示所述用户私密数据。

4.根据权利要求1所述的方法，其特征在于，当移动终端中不存在用户私密数据时，建立用于保存用户私密数据的用户私密数据单元，并绑定所述用户私密数据单元与卡信息、密码信息。

5.根据权利要求1-4任意一项所述的方法，其特征在于，所述卡信息是IMSI信息。

6.一种保护移动终端用户私密数据的装置，其特征在于，包括：

机卡交互单元，用于当卡片插入移动终端时，获取所插入卡片的卡信息；

用户私密数据单元，用于判断移动终端是否存在用户私密数据，当判断结果为存在用户私密数据时，将所插入卡片的卡信息与移动终端保存的卡信息进行匹配处理，匹配处理结果，并根据匹配处理结果，显示所述用户私密信息，以供用户使用，否则，对所述移动终端进行安全性处理；

其中，当匹配处理结果为所插入卡片的卡信息与移动终端保存的卡信息不匹配时，利用用户密码信息将所述用户私密数据与卡信息进行绑定。

7.根据权利要求6所述的装置，其特征在于，所述装置还包括：

鉴权单元，用于将用户后续输入的密码信息与移动终端保存的密码信息进行匹配，并在匹配时显示所述用户私密数据。

8.根据权利要求7所述的装置，其特征在于，所述用户私密数据单元在用户输入的密码信息与移动终端保存的密码信息匹配时，将所述卡信息与移动终端保存的用户私密数据进行绑定。

9.根据权利要求6或7所述的装置，其特征在于，所述用户私密数据单元还用于在初次建立用户私密数据时，绑定用户私密数据与卡信息、密码信息。

一种保护移动终端用户私密数据的方法和装置

技术领域

[0001] 本发明涉及手机技术领域，特别涉及用户私密数据保护技术，本技术适用于各种无线终端。

背景技术

[0002] 手机是现代人常用的通讯工具，其中包含用户各种私密数据，如消息、记事本信息等。而用户私密数据的安全性需求日益增强。需要较好的技术对用户私密数据进行保护，同时可以方便用户使用。

[0003] 在现有技术中，虽然有此需求，并没有终端实现此功能，需要一些可执行的技术实现此功能。而其中一个理论技术是通过卡中手机号码与用户私密数据绑定增强用户私密数据安全性。但是在协议上规定卡中手机号码是可选项，技术上不能保证所有的卡都能实现对用户私密数据的加密。

[0004] 同时手机号码较为容易获取，当通过借用别人手机获取到用户手机时，通过写卡方式将用户的手机号码写入到卡中，插入终端并开机就可以获取到用户私密数据。不能较好的保护用户私密数据。

[0005] 目前随着运营商资费、手机更新换代，用户根据情况更换不同的卡、购买不同的手机经常发生，需要有一种新的保护用户私密数据的方法，实现对用户私密数据保密、防预览、数据存储空间更换和保护参数的更新等功能。

发明内容

[0006] 本发明的目的在于提供一种保护移动终端用户私密数据的方法和装置，能更好地解决用户私密数据安全性差的问题。

[0007] 根据本发明的一个方面，提供的一种保护移动终端用户私密数据的方法包括：

[0008] 当卡片插入移动终端时，获取所述卡片的卡信息，并判断移动终端是否存在用户私密数据；

[0009] 若判断结果为存在用户私密数据，则将所述卡信息与移动终端保存的卡信息进行匹配，并根据匹配结果，显示所述用户私密数据，以供用户使用；

[0010] 若判断结果为不存在用户私密数据，则对所述移动终端进行安全性处理。

[0011] 优选地，当卡片的卡信息与移动终端保存的卡信息匹配时，直接显示所述用户私密数据。

[0012] 优选地，当卡片的卡信息与移动终端保存的卡信息不匹配时，接收用户后续输入的密码信息，将所述密码信息与移动终端保存的密码信息进行匹配，并在匹配时显示所述用户私密数据。

[0013] 优选地，若所述密码信息与移动终端保存的密码信息匹配，则将所述卡信息与移动终端保存的用户私密数据进行绑定。

[0014] 优选地，当移动终端中不存在用户私密数据时，建立用于保存用户私密数据的用

户私密数据单元，并绑定所述用户私密数据单元与卡信息、密码信息。

[0015] 优选地，所述卡信息是IMSI信息。

[0016] 根据本发明的另一方面，提供的一种保护移动终端用户私密数据的装置包括：

[0017] 机卡交互单元，用于当卡片插入移动终端时，获取所述卡片的卡信息；

[0018] 用户私密数据单元，用于判断移动终端是否存在用户私密数据，当判断结果为存在用户私密数据时，将所述卡信息与移动终端保存的卡信息进行匹配，并根据匹配结果，显示所述用户私密信息，以供用户使用，否则，对所述移动终端进行安全性处理。

[0019] 优选地，所述装置还包括：

[0020] 鉴权单元，用于将用户后续输入的密码信息与移动终端保存的密码信息进行匹配，并在匹配时显示所述用户私密数据。

[0021] 优选地，所述用户私密数据单元还用于当卡片的卡信息与移动终端保存的卡信息不匹配，且用户输入的密码信息与移动终端保存的密码信息匹配时，将所述卡信息与移动终端保存的用户私密数据进行绑定。

[0022] 优选地，所述用户私密数据单元还用于在初次建立用户私密数据时，绑定用户私密数据与卡信息、密码信息。

[0023] 与现有技术相比较，本发明的有益效果在于：

[0024] 本发明提供了一种全新的用户私密数据保护方式，技术实现难度低，安全性高，符合用户实际使用需求。

附图说明

[0025] 图1是本发明实施例提供的保护移动终端用户私密数据的方法流程图；

[0026] 图2是本发明实施例提供的增加或获取移动终端用户私密数据的场景实现流程图；

[0027] 图3是本发明实施例提供的第一次使用用户私密数据保护功能设置示意图；

[0028] 图4是本发明实施例提供的更换不同卡调用原有数据示意图；

[0029] 图5是本发明实施例提供的保护移动终端用户私密数据的装置框图。

具体实施方式

[0030] 以下结合附图对本发明的优选实施例进行详细说明，应当理解，以下所说明的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

[0031] 图1是本发明实施例提供的保护移动终端用户私密数据的方法流程图，如图1所示，包括：

[0032] 第一步、当卡片插入移动终端时，获取所述卡片的卡信息，并判断移动终端是否存在用户私密数据。

[0033] 第二步、若判断结果为存在用户私密数据，则将所述卡信息与移动终端保存的卡信息进行匹配，并根据匹配结果，显示所述用户私密数据，以供用户使用；若判断结果为不存在用户私密数据，则对所述移动终端进行安全性处理。

[0034] 进一步地，当卡片的卡信息与移动终端保存的卡信息匹配时，直接显示所述用户私密数据，当卡片的卡信息与移动终端保存的卡信息不匹配时，接收用户后续输入的密码

信息，并将所述密码信息与移动终端保存的密码信息进行匹配，并在匹配时，显示所述用户私密数据，将所述卡信息与移动终端保存的用户私密数据进行绑定。当移动终端中不存在用户私密数据时，建立用于保存用户私密数据的用户私密数据单元，并绑定所述用户私密数据单元与卡信息、密码信息。也就是说，本发明中用户、终端、卡三方的数据匹配时，才显示对应的用户私密数据，加强了用户私密数据的保护，同时又方便用户使用。

[0035] 进一步地，上述卡信息是IMSI信息。按照协议规定，每张卡的手机号码MSISDN是可选的，而IMSI是必须的，使用IMSI作为判断依据，不会出现各种兼容性技术问题，降低了技术实现难度，更符合实际使用情况。

[0036] 图2是本发明实施例提供的本发明实施例场景实现流程图，如图2所示，包括：

[0037] S102：终端没有插入卡时，不显示任何用户私密数据。

[0038] S104：当终端插入卡时，终端读取卡内的参数信息。

[0039] 本步骤中，所述获取卡中的参数信息，具体为IMSI.此值在卡中属于必须存在的。一般都由运营商提供此值，并写入到卡中，用户较难获取到此信息，所以安全性较高。

[0040] S106：判定移动终端是否已经存在用户私密数据，如果移动终端中保存有以前的用户私密数据，转到步骤S108，如果移动终端中没有保存以前的用户私密数据，转到步骤S112。

[0041] 本步骤具体判断当前移动终端是否有以前的用户私密数据，如果存在，提供窗口提示，供用户选择操作。可以通过此方式，实现不同卡绑定同一用户私密数据。

[0042] S108：如果移动终端已经存在用户私密数据，移动终端将检测卡侧的信息与移动终端中保存的数据是否一致，如果一致转到步骤S122，如果不一致转到步骤S112。

[0043] 本步骤中，所述卡侧的信息是IMSI，具体为判断当前移动终端保存的用户私密数据单元中存在的IMSI，是否和从卡侧获取的IMSI一致。

[0044] S112：移动终端保存卡信息。

[0045] 本步骤中，所述卡信息是IMSI，具体为移动终端将IMSI保存在用户私密数据存储空间内，后续和用户的密码信息以及用户私密数据一起绑定。

[0046] S114：提示用户输入密码并保存。

[0047] 本步骤中，所述密码为用户密码，具体为移动终端将用户输入的密码信息保存至用户私密数据存储空间中，与IMSI、用户私密数据一起绑定。

[0048] S116：在步骤S108的基础上，需要用户输入密码。

[0049] 本步骤中，所述密码为用户密码，用户输入的密码需要与用户私密数据存储空间中保存的用户密码一致。

[0050] S118：判断用户输入的密码和已有用户密码是否匹配，当用户输入的用户密码与用户私密数据中保存的用户密码匹配时，转到S122，否则，转到S124。

[0051] S120：创建新的用户私密数据单元。

[0052] 本步骤中，所述用户私密数据单元是在用户私密数据存储空间中针对特定的卡、用户密码，创建保存用户私密数据的单元。具体为，当IMSI、用户密码都设置完成后，终端在用户私密数据存储空间中创建新的用户私密数据单元，后续用户私密数据都保存在此单元中，并且此单元和IMSI、用户的密码信息绑定。

[0053] S122：显示用户私密数据

[0054] 本步骤中，当判断卡信息IMSI、用户密码与用户私密数据绑定的IMSI、用户密码一致时，或者新创建用户私密数据时，显示所述用户私密数据，用户可以查看此私密数据

[0055] S124：不显示用户私密数据

[0056] 本步骤中，当移动终端没有插卡或者卡侧IMSI、用户密码与用户私密数据单元中存储的IMSI、用户密码不匹配时，不显示此用户私密数据。

[0057] 图3是本发明实施例提供的第一次使用用户私密数据保护功能设置示意图，如图3所示，在移动终端无用户私密数据插入卡时，移动终端提示用户输入用户密码，并在用户密码保存成功后，启用用户私密数据保护功能，用户使用此卡保存用户私密数据。

[0058] 图4是本发明实施例提供的更换不同卡调用原有数据的示意图，如图4所示，在移动终端已有用户私密数据插入非匹配卡时，移动终端提示用户选择复用原有数据还是新建用户私有数据。当用户选择复用原有数据时，移动终端提示用户输入密码，并在密码输入正确时，启用其他用户私密数据保护功能，复用用户私密数据，即用户正确输入用户密码时，可以查看其他卡信息。

[0059] 图5是本发明实施例提供的保护移动终端用户私密数据的装置框图，如图5所示，本发明的实现由四个单元组成，其中包括机卡交互单元、鉴权单元、用户私密数据单元。

[0060] 所述机卡交互单元用于当卡片插入移动终端时，获取所述卡片的卡信息，即实现手机与卡之间的数据读取，并获取用户卡的识别信息IMSI。

[0061] 所述鉴权单元，用于将用户后续输入的密码信息与移动终端保存的密码信息进行匹配，并在匹配时显示所述用户私密数据，即用于保存和验证用户密码，根据用户的输入，可以保存与卡相匹配的用户密码。

[0062] 所述用户私密数据单元，用于判断移动终端是否存在用户私密数据，当判断结果为存在用户私密数据时，将所述卡信息与移动终端保存的卡信息进行匹配，并根据匹配结果，显示所述用户私密信息，以供用户使用，否则，对所述移动终端进行安全性处理。所述用户私密数据单元还用于在初次建立用户私密数据时，绑定用户私密数据与卡信息、密码信息，在卡片的卡信息与移动终端保存的卡信息不匹配，且用户输入的密码信息与移动终端保存的密码信息匹配时，将所述卡信息与移动终端保存的用户私密数据进行绑定。进一步说，所述用户私密数据单元保存从卡里读取的卡信息，存储用户私密数据以及与用户密码相关联，并根据不同的卡与用户密码，调用不同的用户私密数据。比如一个终端有甲乙两位不同人员使用，都在此终端保存了用户私密数据，当终端插入乙的卡，终端会将卡参数和用户输入的密码信息与用户私密数据单元中保存的卡参数和密码信息进行对比，只显示匹配一致的用户私密数据。

[0063] 所述装置的工作流程如下：

[0064] 当用户插入卡时，移动终端获取到卡的IMSI，并且检测移动终端有没有以前的用户私密数据和与此IMSI相匹配的用户私密数据。如果存在用户私密数据，并且与卡参数匹配，则显示用户私密数据。如果存在用户私密数据，并且与卡参数不匹配，则提示用户是否需要将此用户私密数据与卡绑定，如绑定需要输入用户密码匹配。如绑定，并且输入用户密码匹配，则用户私密数据与此卡成功绑定，并显示用户私密数据，反之，用户密码不匹配，绑定不成功。如不绑定，则不需要输入用户密码，可以正常使用其他非保护功能。也就是说，如果终端有以前的用户私密数据，那么会提示用户是否调用以前的用户私密数据，并通过用

户密码的认证，确认是否是合法用户，如是合法用户，显示以前的用户私密数据，否则不显示。如果终端没有用户私密数据，提示用户设置用户私密数据，设置后保存对应的信息。

[0065] 进一步地，当用户更换移动终端后，可以通过终端的外部存储设备将用户私密数据从一个终端转移到另一个终端。而要调用此用户私密数据，仍需要匹配认证数据。

[0066] 综上所述，本发明具有以下技术效果：

[0067] 1、本发明提供了一种全新的用户私密数据保护方式，技术实现难度较低，安全性较高。

[0068] 2、手机号码容易被别人获取和盗用，而IMSI安全性高，本发明通过使用卡的IMSI信息，使用户私密数据较难获取和盗用。

[0069] 3、本发明增加用户密码认证，进一步加强了用户私密数据的保密，并通过实现不同卡调用同一用户私密数据，满足用户基于其他原因更换卡仍可以使用原有数据的能力，符合用户实际使用需求，既方便用户使用，又增加了终端功能。

[0070] 尽管上文对本发明进行了详细说明，但是本发明不限于此，本技术领域技术人员可以根据本发明的原理进行各种修改。因此，凡按照本发明原理所作的修改，都应当理解为落入本发明的保护范围。

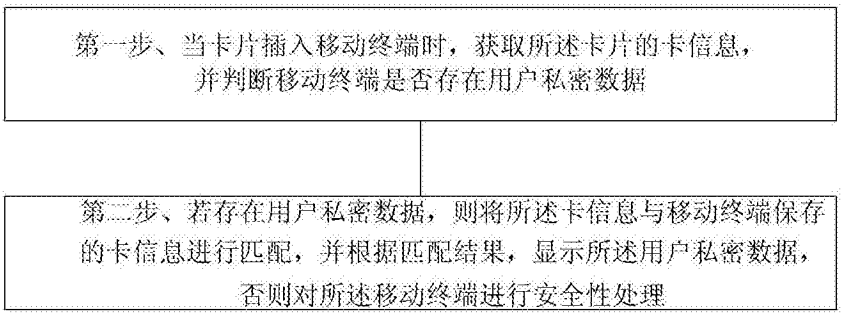

第一步、当卡片插入移动终端时，获取所述卡片的卡信息，并判断移动终端是否存在用户私密数据
第二步、若存在用户私密数据，则将所述卡信息与移动终端保存的卡信息进行匹配，并根据匹配结果，显示所述用户私密数据，否则对所述移动终端进行安全性处理

图1

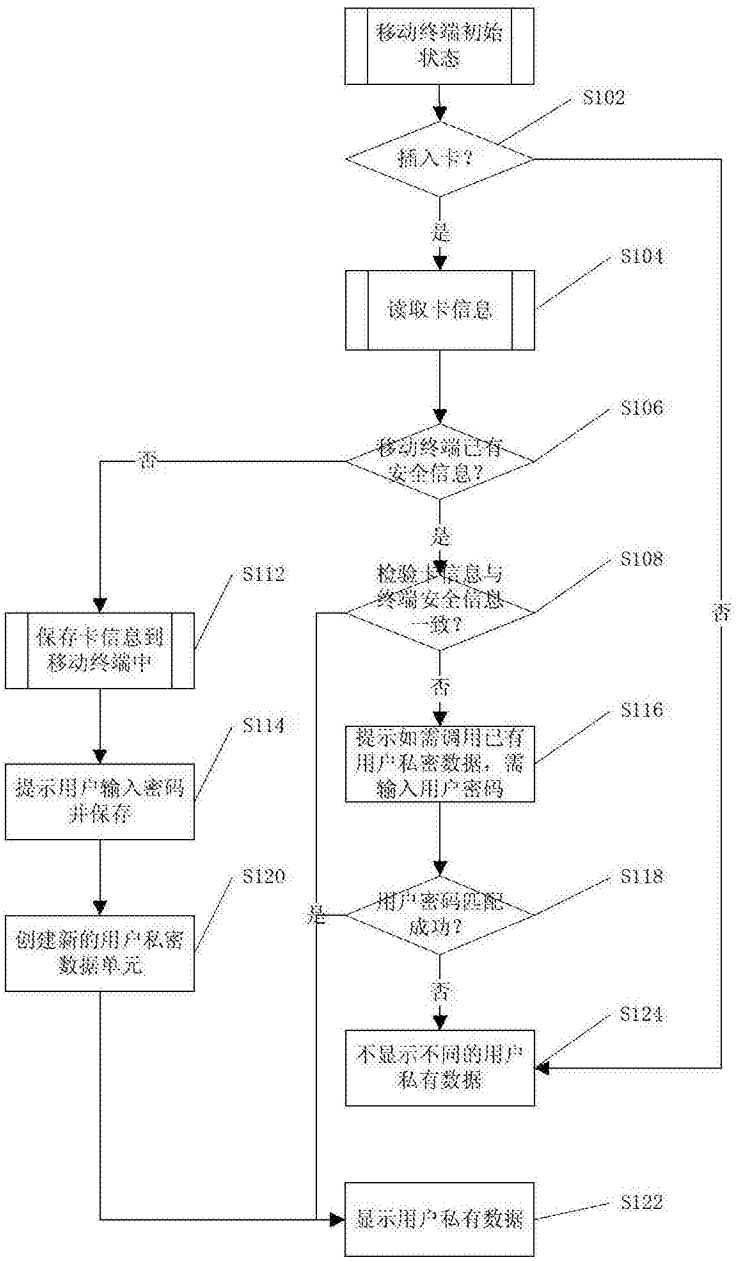

移动终端初始状态
S102
插入卡?
是
否
S104
读取卡信息
S106
移动终端已有安全信息?
否
是
S108
检验卡信息与终端安全信息一致?
否
是
S112
保存卡信息到移动终端中
S114
提示用户输入密码并保存
S120
创建新的用户私密数据单元
S116
提示如需调用已有用户私密数据，需输入用户密码
S118
用户密码匹配成功?
否
是
S124
不显示不同的用户私有数据
S122
显示用户私有数据

图2

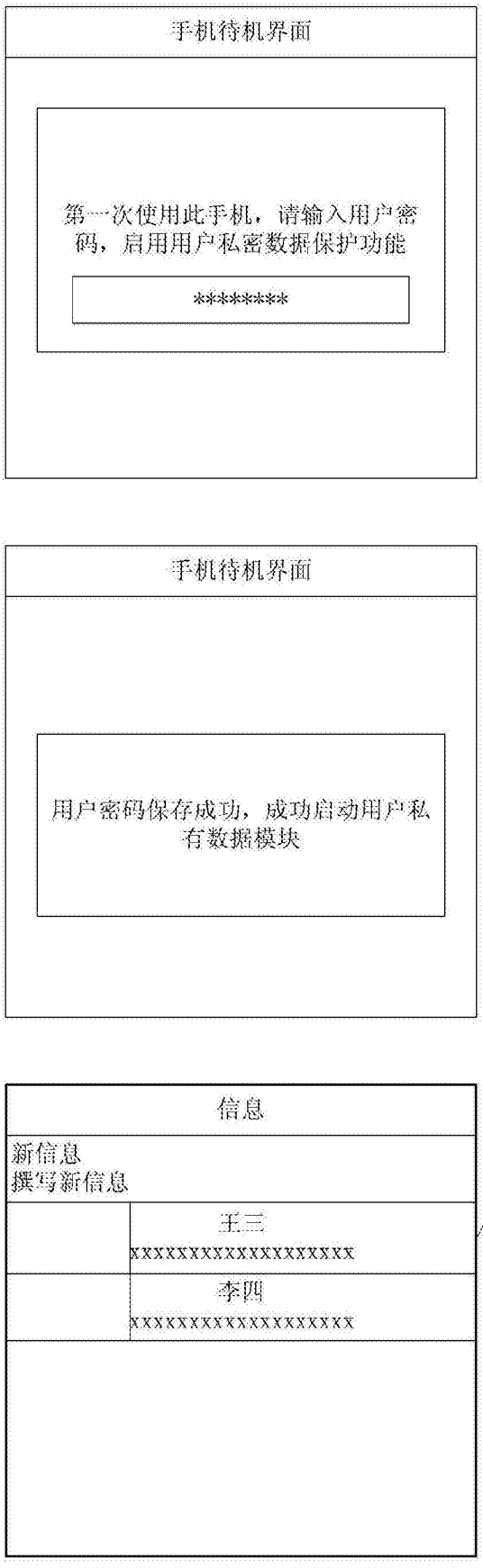

手机待机界面
第一次使用此手机，请输入用户密码，启用用户私密数据保护功能
****
手机待机界面
用户密码保存成功，成功启动用户私有数据模块
信息
新信息
撰写新信息
王三
xxxxxxxxxxxxxxxxxxx
李四
xxxxxxxxxxxxxxxxxxx
用户使用此卡保存的用户私密数据

图3


手机待机界面
此手机已有其他私有数据，请选择启用复用原有私有数据或新建私有数据
是
否
选择“是”
手机待机界面
请输入用户密码，
启用其他用户私密数据保护功能
****
返回上一步
手机待机界面
用户密码正确，复用用户私密数据
信息
新信息
撰写新信息
王三
xxxxxxxxxxxxxxxxxxx
李四
xxxxxxxxxxxxxxxxxxx
用户可以在信息模块查看其他卡信息

图4

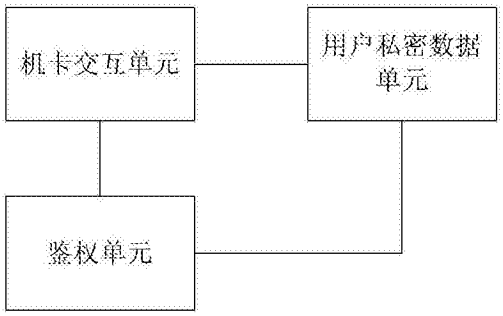


图5