[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*H04Q 7/32 (2006.01)*
*H04L 9/32 (2006.01)*
*H04L 29/06 (2006.01)*

[12] 发明专利申请公布说明书

[21] 申请号 200610109988.0

[43] 公开日 2007 年 3 月 21 日

[11] 公开号 CN 1933629A

[22] 申请日 2006.8.25
[21] 申请号 200610109988.0
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 卢红旗

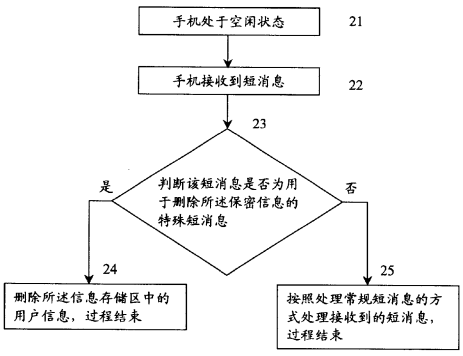
[74] 专利代理机构 北京凯特来知识产权代理有限公司
代理人 郑立明
权利要求书 3 页 说明书 8 页 附图 3 页

[54] 发明名称

# 移动终端内用户存储信息的保护方法及装置

[57] 摘要

本发明涉及移动终端的防盗技术，尤其涉及一种移动终端内用户隐私信息的保护方法及装置。 用户可将需要保护的重要信息(含隐私信息)存放于专用的存储区内并加设密码，如要访问该存储区，必须通过合法身份验证。 另外，本发明还通过向某手机发送特殊短消息，自动删除存储于该手机的所述信息存储区内的信息，从而进一步确保用户存储在该手机上的重要、隐私信息的安全性，特别是在用户丢失该手机的情况下。



1、一种移动终端内用户存储信息的保护方法，其特征在于，包括:

A、在移动终端内设置专用的信息存储区，该存储区用于存放需要保护的用户信息;

B、设置进入所述信息存储区的访问密码;

C、根据所述访问密码对访问者身份的合法性进行验证，并允许合法访问者进入所述信息存储区。

2、根据权利要求1所述的方法，其特征在于，包括:

所述信息存储区位于所述移动终端的闪存Flash存储器中。

3、根据权利要求1所述的方法，其特征在于，所述步骤A包括:

根据移动终端内存使用状况，从高地址向低地址依次存储所述需要保护的信息;

或者，从低地址向高地址依次存储所述需要保护的信息。

4、根据权利要求1所述的方法，其特征在于，所述步骤B包括:

在必要时，修改原先设置的所述访问密码。

5、根据权利要求1所述的方法，其特征在于，所述步骤C包括:

C1、若访问者提供的密码与所述访问密码一致，则该访问者合法，允许所述访问者进入所述信息存储区对该区信息进行查看或编辑操作。

6、根据权利要求5所述的方法，其特征在于，所述步骤C还包括:

C2、允许访问者在规定次数内多次输入密码接受合法性身份验证，并在其中一次验证通过后，执行步骤C1;否则，所述访问者非法，拒绝该访问者的访问

7、根据权利要求1至6之一所述的方法，其特征在于，所述方法还包括:

发送要求删除所述信息存储区内信息的特殊短消息到所述移动终端，并删除所述移动终端内所述信息存储区中存储的信息。

8、根据权利要求7所述的方法，其特征在于，包括:

所述特殊短消息具有预先设置的格式。

9、一种移动终端内用户存储信息的保护装置，其特征在于，包括:

专用存储单元，用于存放需要保护的用户信息;

密码设置单元，用于设置并保存访问所述专用存储单元内存储信息的访问密码，并将所述访问密码提供给合法性验证单元;

合法性验证单元，用于根据所述访问密码对访问者身份的合法性进行验证，并允许合法访问者进入所述信息存储区。

10、根据权利要求9所述的装置，其特征在于，包括:

所述信息存储区位于所述移动终端的闪存Flash存储器中。

11、根据权利要求9所述的装置，其特征在于，所述合法性验证单元具体包括:

输入密码接收单元，用于接收访问者输入的待验证密码，并触发验证次数控制单元;

验证次数控制单元，用于判断所述待验证密码的输入次数是否超过规定的最大验证次数，如果是，结束访问过程；否则，触发验证单元;

验证单元，用于从所述输入密码接收单元获取所述待验证密码，并与所述访问密码对比，若两者一致，则所述访问者为合法用户，允许所述访问者进入所述信息存储区访问该区信息；否则，所述访问者为非法用户，结束访问过程。

12、根据权利要求9所述的装置，其特征在于，所述装置还包括:

特殊短消息格式设定单元，用于设定特殊短消息格式，所述特殊短消息为用于删除所述信息存储区内信息的短消息;

特殊短消息识别单元，用于根据所述特殊短消息的格式，判断接收到的短消息为特殊短消息，并触发删除信息单元；

删除信息单元，用于删除所述信息存储区内的信息。

# 移动终端内用户存储信息的保护方法及装置

## 技术领域

本发明涉及移动终端的防盗技术，尤其涉及一种移动终端内用户隐私信息的保护方法及装置。

## 背景技术

手机产品价格的下降以及产品自身的便捷特点，使手机成为日益普及的电子产品。据了解，目前全世界手机用户总量已经超过10亿，并仍在呈现不断增长的趋势。手机的普及以及手机自身易于携带的外形也带来一些问题，如容易遗失或被盗。这类问题在造成用户直接经济损失的同时，可能导致用户存储在手机上的隐私信息，如通讯录、短信、电子邮件，甚至是各种重要资源的帐号及密码等信息的泄漏的问题。非法用户由于能够轻易获取上述隐私信息而给手机合法用户带来更大的损失与麻烦。

目前，有关手机防盗的技术包括以下几种:

（1）法国专利FR2791509给出一种通过为手机设定开机密码防止手机被盗后非法使用的技术。

（2）中国专利200310113647.7与03124196.4给出通过对手机中的SIM（用户识别模块）作保护，防止手机丢失后，其中的SIM卡被非法使用的技术。

（3）专利申请号为03148202.3以及专利号为01802972.8的专利，该两个文件给出手机丢失后自动向失主报失的技术。

上述现有技术中，没有针对手机丢失后，阻止非法用户使用及窥视原先合法用户存储在该手机上的隐私信息。

## 发明内容

本发明提供一种移动终端内用户隐私信息的保护方法及装置，从而实现对移动终端内存储的用户私人信息的保护。

本发明的目的通过以下技术方案实现。

一种移动终端内用户存储信息的保护方法，包括:

A、在移动终端内设置专用的信息存储区，该存储区用于存放需要保护的用户信息;

B、设置进入所述信息存储区的访问密码;

C、根据所述访问密码对访问者身份的合法性进行验证，并允许合法访问者进入所述信息存储区。

所述信息存储区位于所述移动终端的闪存Flash存储器中。

所述步骤A包括:

根据移动终端内存使用状况，从高地址向低地址依次存储所述需要保护的信息;

或者，从低地址向高地址依次存储所述需要保护的信息。

所述步骤B包括:

在必要时，修改原先设置的所述访问密码。

所述步骤C包括:

C1、若访问者提供的密码与所述访问密码一致，则该访问者合法，允许所述访问者进入所述信息存储区对该区信息进行查看或编辑操作。

所述步骤C还包括:

C2、允许访问者在规定次数内多次输入密码接受合法性身份验证，并在其中一次验证通过后，执行步骤C1；否则，所述访问者非法，拒绝该访问者的访问

所述方法还包括：

发送要求删除所述信息存储区内信息的特殊短消息到所述移动终端，并删除所述移动终端内所述信息存储区中存储的信息。

所述特殊短消息具有预先设置的格式。

一种移动终端内用户存储信息的保护装置，包括：

专用存储单元，用于存放需要保护的用户信息；

密码设置单元，用于设置并保存访问所述专用存储单元内存储信息的访问密码，并将所述访问密码提供给合法性验证单元；

合法性验证单元，用于根据所述访问密码对访问者身份的合法性进行验证，并允许合法访问者进入所述信息存储区。

所述信息存储区位于所述移动终端的闪存Flash存储器中。

所述合法性验证单元具体包括：

输入密码接收单元，用于接收访问者输入的待验证密码，并触发验证次数控制单元；

验证次数控制单元，用于判断所述待验证密码的输入次数是否超过规定的最大验证次数，如果是，结束访问过程；否则，触发验证单元；

验证单元，用于从所述输入密码接收单元获取所述待验证密码，并与所述访问密码对比，若两者一致，则所述访问者为合法用户，允许所述访问者进入所述信息存储区访问该区信息；否则，所述访问者为非法用户，结束访问过程。

所述装置还包括：

特殊短消息格式设定单元，用于设定特殊短消息格式，所述特殊短消息

为用于删除所述信息存储区内信息的短消息;

特殊短消息识别单元，用于根据所述特殊短消息的格式，判断接收到的短消息为特殊短消息，并触发删除信息单元;

删除信息单元，用于删除所述信息存储区内的信息。

由上述本发明给出的技术方案可见，本发明能够有效实现对移动终端内所存储的用户私人信息的保护，并在用户丢失诸如手机类移动终端后，有效保护该手机中存储的用户私人信息。该保护作用主要体现在以下方面，即本发明在移动终端，如手机的存储设备中设置用户私人信息的存储区，并为该区设置访问密码；当用户丢失手机，本发明通过向所述手机发送特殊短消息的方式，自动删除该手机上用户私人信息存储区的所有信息，从而进一步保护用户信息。

## 附图说明

图1是本发明具体实施方案给出的对所述访问者进行合法性身份验证的流程图;

图2是本发明具体实施方案给出的通过特殊短消息自动删除用户隐私信息过程图;

图3是本发明具体实施方案给出的进入用户隐私区系统实现结构示意图;

图4是本发明具体实施方案给出的通过短消息删除用户隐私的系统实现结构示意图。

## 具体实施方式

本发明主要是在移动终端，如手机的存储器中设置专用的信息存储区，并设置进入所述信息存储区的访问密码；当访问者要求访问所述信息存储区

时，要求该访问者输入待验证的密码；当所述待验证密码与所述访问密码一致时，才允许该通过合法性验证的合法访问者访问存放于所述信息存储区的信息。

并且，本发明还通过向某手机发送特殊短消息，自动删除存储于该手机的所述信息存储区内的信息，从而进一步确保用户存储在该手机上的重要、隐私信息的安全性，特别是在用户丢失该手机的情况下。

本发明中，所述专用的信息存储区可设置于手机中的Flash（闪存）存储器中。在手机存储器中设置信息存放区的方法包括：根据目前手机内存的使用状况，从高地址向低地址存放信息，或者从低地址向高地址存放信息。如图1所示，假设用户手机中的Flash存储器空间为128Mbyte，则可将该存储器中上半个空间划为所述信息存储区，即所述Flash存储器中由0xFFFFFFF至0x8000000的存储地址可用于存储用户信息。这一按照地址划分依次存储信息的做法能够便于用户存储大量的用户认为需要保密的信息。所述信息存放区具体可用于存放的用户信息包括但不限于通讯录、短信、备忘录、邮件、各种重要资源的帐号与密码等用户认为需要保密的信息。并且，为所述信息存储区设置访问密码，该访问密码用于对访问者的身份进行合法性验证，并且移动终端用户可选择定期或不定期修改该访问密码。

结合附图1具体说明本发明对所述访问者进行合法性身份验证的过程：

步骤11、手机处于空闲状态；

步骤12、访问者（合法或非法）要求访问手机中所述信息存储区的信息；

访问者可通过人机交互界面确认该要求访问步骤。

步骤13、手机系统要求访问者输入身份验证密码；

步骤14、所述访问者输入待验证密码；

步骤15、手机系统对比预先设置的所述访问密码与所述待验证密码，对所述待验证密码作合法性验证，如果两者一致，执行步骤16；否则，执行步骤17；

步骤16、所述访问者的身份合法，允许该访问者进入所述信息存储区，察看或编辑其中的信息，访问者身份合法性验证过程结束；

步骤17、根据预先设置的最大验证次数，判断本次密码验证次数是否超过所述最大验证次数，若超过，执行步骤19；否则，执行步骤18；

其中，若没有预先设置的所述最大验证次数，则默认所述最大验证次数为一次。

步骤18、手机系统提示密码错误，并允许重新输入待验证密码，在所述访问者重新输入待验证密码后，执行步骤15；

步骤19、确认所述访问者身份非法并禁止准入，执行步骤110；

步骤110、手机回到空闲状态。

如果用户手机丢失，而用户希望对存放在所述手机中信息存放区的信息给予保护，本发明提供进一步的保护方法，即通过向丢失的手机发送特殊短消息，及时删除所述信息存储区上存储的用户信息。

结合附图2说明通过发送特殊短消息删除所述用户信息的过程：

步骤21、手机处于空闲状态；

步骤22、手机接收到短消息；

步骤23、根据该短消息的形式判断该短消息是否为用于删除所述保密信息的特殊短消息，如果是，执行步骤24；否则，执行步骤25；

该特殊短消息的格式可定义为：进入信息存储区密码“+”删除信息密码，在这一格式中，前者即为进入所述信息存储区的所述的访问密码，后者在不另行设定时可默认为与前者一致。

步骤24、删除所述信息存储区中的用户信息，过程结束；

步骤25、按照处理常规短消息的方式处理接收到的短消息，过程结束。

本发明还提供一种如图3与图4所示的移动终端内存储信息的保护装置，包括以下功能的各个单元：

（1）专用存储单元

用于存放需要保护的用户信息。

所述专用存储单元位于所述移动终端的闪存Flash存储器中。

（2）密码设置单元

用于设置并保存访问所述专用存储单元内存储信息的访问密码，并将所述访问密码提供给合法性验证单元；

（3）合法性验证单元

用于对访问者身份的合法性进行验证，并允许合法访问者进入所述信息存储区。

所述合法性验证单元具体包括：

输入密码接收单元

用于接收访问者输入的待验证密码，并触发验证次数控制单元；

验证次数控制单元

用于判断所述待验证密码的输入次数是否超过规定的最大验证次数，如果是，结束访问过程；否则，触发验证单元；

验证单元

用于从所述输入密码接收单元获取所述待验证密码，并与所述访问密码对比，若两者一致，则所述访问者为合法用户，允许所述访问者进入所述信息存储区访问该区信息；否则，所述访问者为非法用户，结束访问过程。

（4）特殊短消息格式设定单元

用于设定特殊短消息格式，所述特殊短消息为用于删除所述信息存储区内信息的特殊短消息；

（5）特殊短消息识别单元

用于根据所述特殊短消息的格式，判断接收到的短消息为特殊短消息，并触发删除信息单元；

（6）信息删除单元

用于删除所述信息存储区内的信息。

本发明能够有效实现对移动终端内所存储的用户私人信息的保护，并在用户丢失诸如手机类移动终端后，有效保护该手机中存储的用户私人信息。该保护作用主要体现在以下方面，即本发明在移动终端，如手机的存储设备中设置用户私人信息的存储区，并为该区设置访问密码；当用户丢失手机，本发明通过向所述手机发送特殊短消息的方式，自动删除该手机上用户私人信息存储区的所有信息，从而进一步保护用户信息。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求书的保护范围为准。

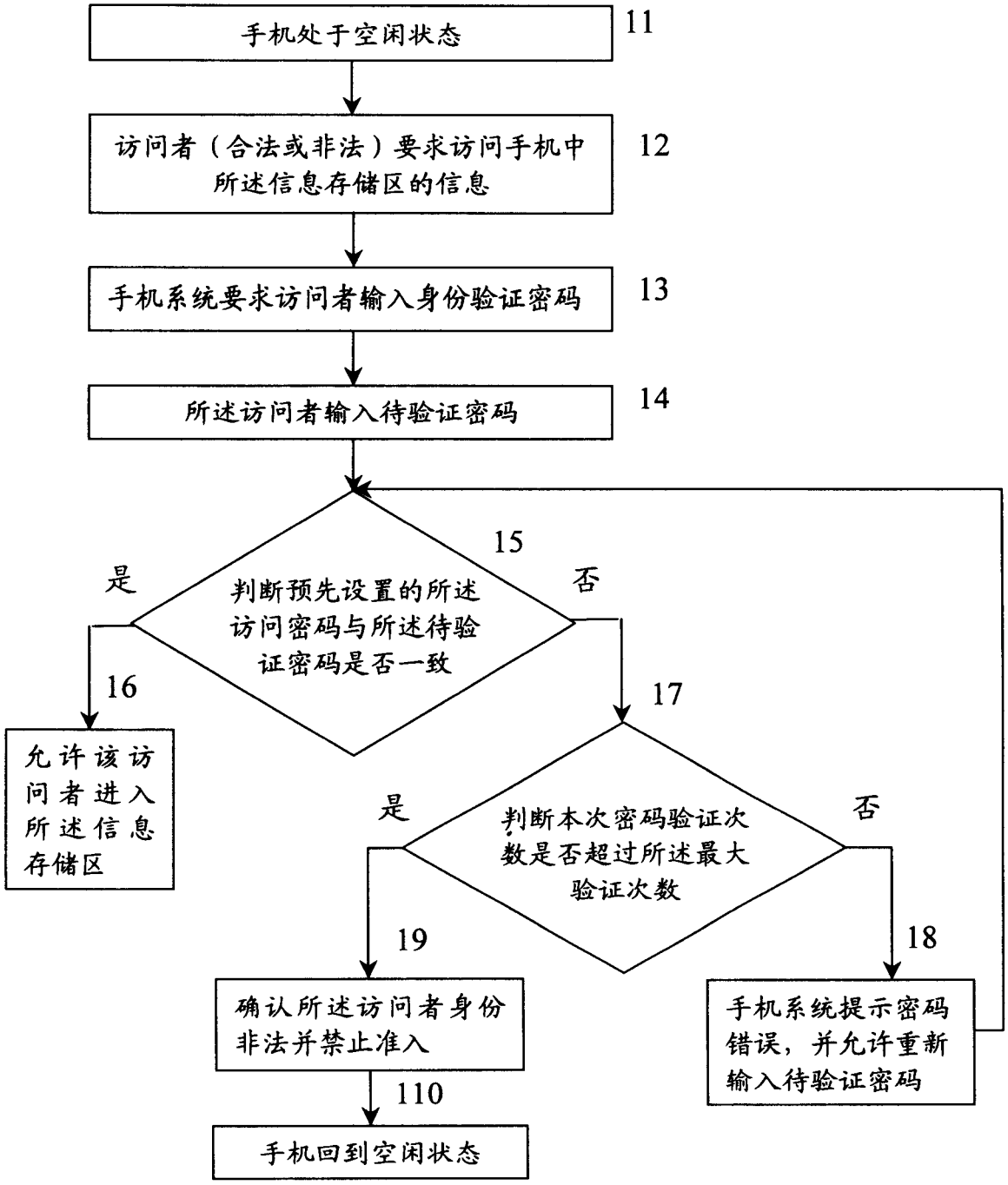

手机处于空闲状态
11
访问者（合法或非法）要求访问手机中所述信息存储区的信息
12
手机系统要求访问者输入身份验证密码
13
所述访问者输入待验证密码
14
判断预先设置的所述访问密码与所述待验证密码是否一致
15
是
否
16
允许该访问者进入所述信息存储区
17
判断本次密码验证次数是否超过所述最大验证次数
是
否
19
18
确认所述访问者身份非法并禁止准入
手机系统提示密码错误，并允许重新输入待验证密码
110
手机回到空闲状态

图1

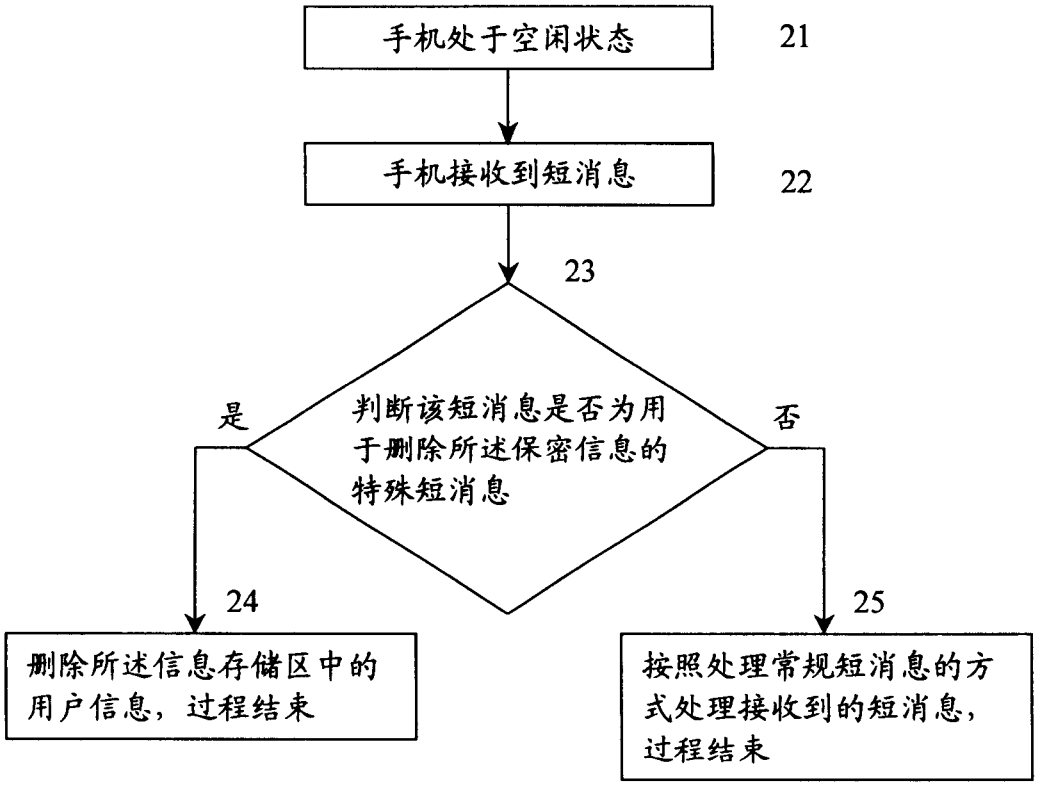

手机处于空闲状态
21
手机接收到短消息
22
23
判断该短消息是否为用于删除所述保密信息的特殊短消息
是
否
24
删除所述信息存储区中的用户信息，过程结束
25
按照处理常规短消息的方式处理接收到的短消息，过程结束

图2

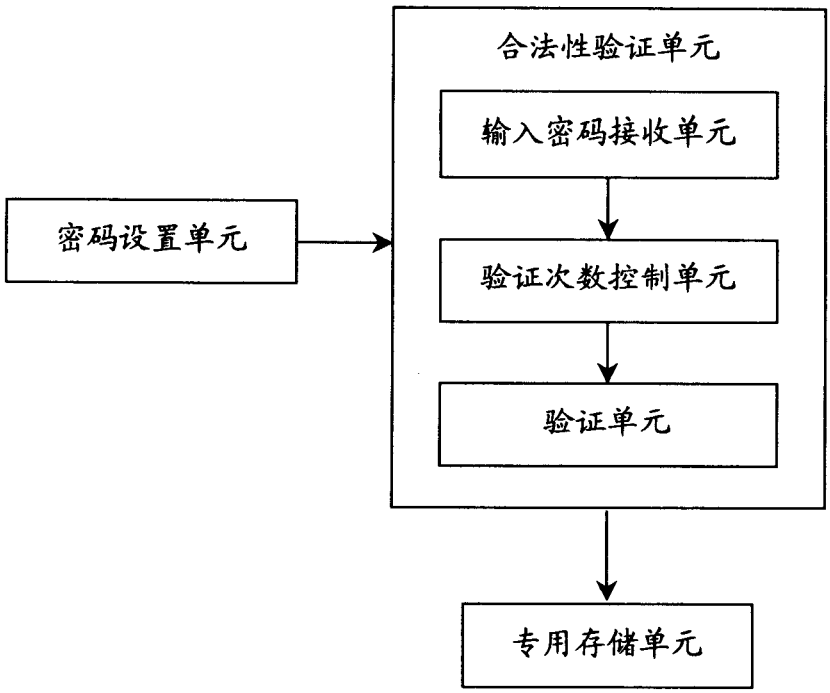

合法性验证单元
输入密码接收单元
密码设置单元
验证次数控制单元
验证单元
专用存储单元

图3

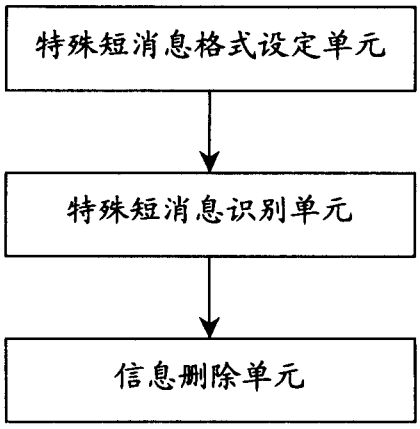

特殊短消息格式设定单元
特殊短消息识别单元
信息删除单元

图4