



(12)发明专利申请

(10)申请公布号 CN 105897708 A

(43)申请公布日 2016.08.24

(21)申请号 201610203738.7

(22)申请日 2016.03.31

(71)申请人 宇龙计算机通信科技(深圳)有限公司

地址 518057 广东省深圳市南山区高新技术工业园北区酷派信息港1栋6层

(72)发明人 饶志治 张充

(74)专利代理机构 深圳鼎合诚知识产权代理有限公司 44281

代理人 薛祥辉

(51)Int.Cl.

H04L 29/06(2006.01)

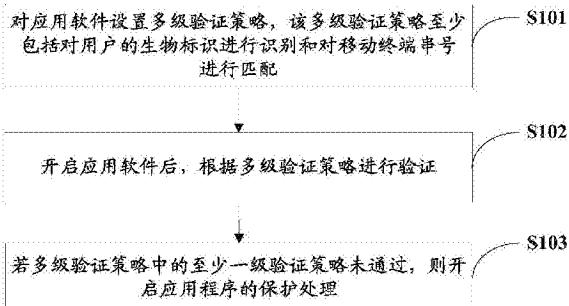
权利要求书1页 说明书7页 附图3页

(54)发明名称

一种信息保护方法及移动终端

(57)摘要

本发明公开一种信息保护方法，该方法包括：对应用软件设置多级验证策略，多级验证策略至少包括对用户的生物标识进行识别和对移动终端串号进行匹配；开启应用软件后，根据多级验证策略进行验证；若多级验证策略中的至少一级验证策略未通过，则开启应用软件的保护处理。本发明通过以上技术方案的实施，能够极大程度的对用户信息进行安全保护，从而提升用户在移动支付、隐私保护等方面的安全性，在一定程度上加强了移动终端在支付、隐私等方面防盗作用。



1.一种信息保护方法,其特征在于,包括:

对应用软件设置多级验证策略,所述多级验证策略至少包括对用户的生物标识进行识别和对移动终端串号进行匹配;

开启应用软件后,根据所述多级验证策略进行验证;

若所述多级验证策略中的至少一级验证策略未通过,则开启所述应用软件的保护处理。

2.如权利要求1所述的信息保护方法,其特征在于,所述用户的生物标识包括用户录入的指纹,所述开启应用软件后,根据所述多级验证策略进行验证具体为:

识别用户录入的指纹,若识别成功,则将所述移动终端串号和所述应用软件中保存的串号进行匹配;若匹配失败,则开启所述应用软件的保护处理。

3.如权利要求1所述的信息保护方法,其特征在于,开启所述应用软件的保护处理具体为:

退出并锁定所述应用软件。

4.如权利要求1或2所述的信息保护方法,其特征在于,开启所述应用软件的保护处理具体为:

获取所述应用软件中存储的用户信息,根据所述用户信息向对应用户发出警告。

5.如权利要求1或2所述的信息保护方法,其特征在于,在对应用软件设置多级验证策略之前还包括:

保存用户的生物标识和移动终端串号。

6.一种移动终端,其特征在于,包括:

设置模块,用于对应用软件设置多级验证策略,所述多级验证策略至少包括对用户的生物标识进行识别和对移动终端串号进行匹配;

验证模块,用于开启应用软件后,根据所述多级验证策略进行验证;

处理模块,用于若所述多级验证策略中的至少一级验证策略未通过,则开启所述应用软件的保护处理。

7.如权利要求6所述的移动终端,其特征在于,所述用户的生物标识包括用户录入的指纹,所述验证模块包括:

验证子模块,用于识别用户录入的指纹,若识别成功,则将所述移动终端串号和所述应用软件中保存的串号进行匹配;若匹配失败,则开启所述应用软件的保护处理。

8.如权利要求6或7所述的信息保护方法,其特征在于,所述处理模块包括:

处理子模块,用于退出并锁定所述应用软件。

9.如权利要求6或7所述的移动终端,其特征在于,所述处理模块还包括:

发送子模块,用于获取所述应用软件中存储的用户信息,根据所述用户信息向对应用户发出警告。

10.如权利要求6或7所述的移动终端,其特征在于,还包括:

存储模块,用于在设置模块对应用软件设置多级验证策略之前,保存用户的生物标识和移动终端串号。

一种信息保护方法及移动终端

技术领域

[0001] 本发明涉及电子设备领域,尤其涉及一种信息保护方法及移动终端。

背景技术

[0002] 目前,在移动终端的使用中已经实现了指纹识别技术,并将指纹识别技术广泛应用于移动支付、极速快拍、打开相关应用软件、移动终端解锁等领域。在移动终端上使用指纹识别给用户带来了不少方便,然而也存在较多安全隐患。由于指纹很容易被盗取,移动终端上仅仅进行指纹识别是不安全的,用户在使用移动终端时往往会有信息被泄露等安全隐患,特别是在打开交流软件类的应用软件、移动安全支付等,指纹被盗会导致用户出现重大的损失。因此,这种仅通过将指纹识别技术应用于移动终端进行信息保护的方法存在很大的不安全性,进而影响用户体验。此外,现有技术中也会采用移动终端串号匹配的方法对信息进行保护,但是,当其他用户获取到该移动终端后能够直接访问该移动终端上的应用软件,并进行信息获取等操作,很容易造成用户信息泄露,导致用户出现重大损失。

发明内容

[0003] 本发明提供一种信息保护方法及移动终端,解决现有技术中仅通过指纹识别技术或移动终端串号匹配技术对用户信息进行保护,导致用户在使用移动终端存储的信息时存在很大的安全隐患,进而影响用户体验的技术问题。

[0004] 为解决上述技术问题,本发明采用以下技术方案:

[0005] 一种信息保护方法,包括:

[0006] 对应用软件设置多级验证策略,所述多级验证策略至少包括对用户的生物标识进行识别和对移动终端串号进行匹配;

[0007] 开启应用软件后,根据所述多级验证策略进行验证;

[0008] 若所述多级验证策略中的至少一级验证策略未通过,则开启所述应用软件的保护处理。

[0009] 进一步地,所述用户的生物标识包括用户录入的指纹,所述开启应用软件后,根据所述多级验证策略进行验证具体为:

[0010] 识别用户录入的指纹,若识别成功,则将所述移动终端串号和所述应用软件中保存的串号进行匹配;若匹配失败,则开启所述应用软件的保护处理。

[0011] 进一步地,开启所述应用软件的保护处理具体为:退出并锁定所述应用软件。

[0012] 进一步地,开启所述应用软件的保护处理具体为:

[0013] 获取所述应用软件中存储的用户信息,根据所述用户信息向对应用户发出警告。

[0014] 进一步地,在在对应应用软件设置多级验证策略之前还包括:

[0015] 保存用户的生物标识和移动终端串号。

[0016] 本发明还提供了一种移动终端,包括:

[0017] 设置模块,用于对应应用软件设置多级验证策略,所述多级验证策略至少包括对用

户的生物标识进行识别和对移动终端串号进行匹配；

[0018] 验证模块，用于开启应用软件后，根据所述多级验证策略进行验证；

[0019] 处理模块，用于若所述多级验证策略中的至少一级验证策略未通过，则开启所述应用软件的保护处理。

[0020] 进一步地，所述用户的生物标识包括用户录入的指纹，所述验证模块包括：

[0021] 验证子模块，用于识别用户录入的指纹，若识别成功，则将所述移动终端串号和所述应用软件中保存的串号进行匹配；若匹配失败，则开启所述应用软件的保护处理。

[0022] 进一步地，所述处理模块还包括：

[0023] 处理子模块，用于退出并锁定所述应用软件。

[0024] 进一步地，所述处理模块还包括：

[0025] 发送子模块，用于获取所述应用软件中存储的用户信息，根据所述用户信息向对应用户发出警告。

[0026] 进一步地，还包括：存储模块，用于在设置模块对应用软件设置多级验证策略之前，保存用户的生物标识和移动终端串号。

[0027] 本发明提供的信息保护方法，对应用软件设置多级验证策略，所述多级验证策略至少包括对用户的生物标识进行识别和对移动终端串号进行匹配；

[0028] 开启应用软件后，根据所述多级验证策略进行验证；若所述多级验证策略中的至少一级验证策略未通过，则开启所述应用软件的保护处理。通过对以上技术方案的实施，能够极大程度的对用户信息进行安全保护，从而提升用户在移动支付、隐私保护等方面的安全性，在一定程度上加强了移动终端在支付、隐私等方面的防盗作用。

附图说明

[0029] 图1为本发明实施例一提供的信息保护方法的流程图；

[0030] 图2为本发明实施例一提供的信息保护方法的具体流程图；

[0031] 图3为本发明实施例三提供的移动终端的模块示意图；

[0032] 图4为本发明实施例三提供的移动终端的细节模块示意图。

具体实施方式

[0033] 应当理解的是，此处所描述的具体实施例仅用于解释本发明，并不用于限定本发明。

[0034] 本发明适用于所有具备生物识别功能、拥有终端串号的移动终端，该移动终端可以以各种形式来实施。例如，本发明中描述的移动终端可以包括智能手机、笔记本电脑、PAD(平板电脑)等移动终端。下面通过具体实施方式结合附图对本发明作进一步详细说明。

[0035] 实施例一：

[0036] 本实施例提供一种信息保护方法，请参见图1，其具体步骤如下：

[0037] S101，对应用软件设置多级验证策略，该多级验证策略至少包括对用户的生物标识进行识别和对移动终端串号进行匹配；

[0038] 具体的，上述应用软件包括但不限于以下几种软件：短信、微信、相册、支付宝，用户可根据自身需求自主设定需要进行信息保护的应用软件列表，同时，该应用软件基于移

动终端实现各种功能。此外，S101步骤中提到的“多级”是指两级或两级以上。进一步地，对应用软件设置多级验证策略，可以理解为设置多层验证标准，若前一验证标准通过，继续执行下一验证标准；若前一验证标准未通过，则终止验证过程。并将该多级验证策略保存至应用软件中以便后续验证。

[0039] 此外，上述移动终端的串号包括但不限于IMEI(国际移动设备标识)、SN码、移动终端马达的编号、芯片的编号，只要能表明移动终端唯一性的串号均可应用于本发明。其中，该IMEI由GSM(全球移动通信协会)统一分配，是由15位数字组成的“电子串号”，它与每个移动终端一一对应，且该标识是全世界唯一的，每一个移动终端在组装完成后都被赋予一个全球唯一的一组号码，这个号码从生产到交付使用都被制造生产的厂商所记录，用于区别各移动终端，通常存储于手机的存储器或CPU(中央处理器)中，优选地，存于EEPROM(俗称“码片”)里，可用于监控被窃或无效的移动终端。例如：当移动终端被盗时，如果知道IMEI码，可以通过移动终端供应商进行终端锁定，即获知被盗之后的手机号码，中止移动终端的通话功能，并获知移动终端的方位。SN(产品序列号)码是产品的身份证号码，用于验证产品的合法身份，保障用户的正版权益，在移动终端中，SN码一般指软件注册码信息，是一个产品出厂的系列号，一个产品只对应一组产品序列号，也具有唯一性。应该明白的是，上述移动终端串号为IMEI仅用于对本实施例进行解释，并不用于限定本发明，本实施例下文中将以IMEI为例对本发明的方案进行解释。

[0040] 对于S101步骤中提到的生物识别技术，包括指纹识别、虹膜识别、脉搏识别等。优选地，本实施例以指纹识别为例进行解释，其整体工作原理是：将一个人同他的指纹对应起来，通过对他的指纹和预先保存的指纹进行比较，就可验证他的真实身份。因为每个人的皮肤(包括指纹在内)纹路在图案、断点和交叉点上各不相同，也即每个人的皮肤纹路是唯一的，且终生不变，依靠这种唯一性和稳定性，实现指纹识别技术。

[0041] S102，开启应用软件后，根据所述多级验证策略进行验证；

[0042] 具体的，基于S101步骤的分析，本实施例以指纹识别和移动终端串号为例对本发明进行解释，但不用于限定本发明。具体的，根据IMEI码和指纹识别技术的特性，通过IMEI码和指纹识别技术对用户存于移动终端的信息进行保护。其具体流程为，用户设定应用列表并保存至移动终端，当然，设定的信息保护方式是，采用本实施例提供的实施方式进行信息保护。然后打开应用列表中的任一应用软件，采集用户的指纹信息并保存至该应用软件中；当用户打开该应用软件时，移动终端首先根据应用软件中保存的指纹信息对当前录入的指纹进行识别。此外，移动终端调用移动终端接口获取当前移动终端的IMEI码，并与该应用软件中保存的IMEI码进行匹配。应该明白的是，对于指纹识别和移动终端的IMEI码匹配，包括但不限于以下三种操作过程：

[0043] 一、指纹识别和移动终端的IMEI同时进行验证；即移动终端在录入用户指纹进行识别的同时，在后台也会获取移动终端的IMEI码与应用软件中保存的IMEI进行匹配，使得用户在解锁应用软件上耗费的时间更短，进而更好的提升用户体验；

[0044] 二、先进行指纹识别，再进行IMEI码匹配；即移动终端先发送请求用户录入指纹的信息，在用户指纹录入完毕之后，将录入的用户指纹与应用软件中采集的指纹进行匹配，若匹配成功，则调用移动终端接口获取移动终端的IMEI码，并与应用软件中保存的IMEI码进行匹配，若匹配成功，则允许用户访问该应用软件，获取相关用户信息；

[0045] 三、先进行IMEI码匹配，再进行指纹识别；即移动终端先调用移动终端接口获取移动终端的IMEI码，然后与应用软件中保存的IMEI码进行匹配，若匹配成功，则发送请求用户录入指纹的信息，在用户指纹录入完毕之后，将录入的用户指纹与应用软件中采集的指纹进行匹配，若匹配成功，则允许用户访问该应用软件，获取相关用户信息。

[0046] S103，若多级验证策略中的至少一级验证策略未通过，则开启应用程序的保护处理。

[0047] 具体的，在对用户指纹信息识别完毕、对移动终端IMEI码匹配完毕之后，若指纹识别失败、移动终端IMEI码匹配失败，则移动终端自动退出并锁定该应用软件，同时，获取应用软件中存储的用户信息，根据用户信息向对应用户发出警告，具体的，自动向应用软件中绑定的手机号发送短信提醒。应当明白的是，锁定该应用软件的时间周期本实施例不做限定，用户可根据自身需要进行自由设定，可以是1分钟，也可以是1小时，甚至用户无法对该应用程序进行再次验证，最大程度的保证用户信息免于泄露或被盗用。

[0048] 进一步地，对于S103步骤，其具体操作过程包括但不限于以下三种：

[0049] 一、指纹识别和移动终端IMEI码匹配同时进行；

[0050] 具体的，在对用户录入的指纹识别失败/成功，且对IMEI码匹配成功/失败后(即二者不会同时验证成功)，移动终端认定用户操作不合法，直接退出并锁定相应应用软件，同时向应用软件绑定的手机号发送短信，提醒指纹识别失败防止用户的账号或重要信息被盗，让用户可以及时采取相应措施。或者，在用户录入的指纹识别成功，且对IMEI码匹配成功后(即二者同时验证成功)，移动终端认定用户操作合法，允许用户访问应用软件，获取用户相关信息。

[0051] 二、指纹识别和移动终端IMEI码匹配存在先后顺序；

[0052] 具体的，先获取移动终端的IMEI码，并与应用软件中保存的IMEI码进行匹配，若匹配失败，则启动应用软件的保护处理，若匹配成功，则发送请求用户录入指纹的信息，用户录入指纹后，对该指纹进行识别，若识别失败，同样启动应用软件的保护处理，若失败成功，则允许用户继续访问该应用软件。或者，先对用户录入的指纹进行识别，若识别失败，则启动应用软件的保护处理，若识别成功，则获取移动终端的IMEI码，将该IMEI码与应用软件中保存的移动终端的IMEI码进行匹配，若匹配失败，同样启动应用软件的保护处理，若匹配成功，则允许用户继续对该应用软件执行后续操作。

[0053] 通过上述步骤，用户能够最大程度的避免移动终端中的信息被泄露，放心、安全的在移动终端上进行操作，从而提升用户的满意度。

[0054] 进一步地，请参见图2，图2为本实施例提供的信息保护方法的具体流程图，其具体保护过程如下：

[0055] S201，采集用户录入的指纹并保存移动终端的串号，也即录入指纹，保存串号；

[0056] 具体的，该串号可以为IMEI码，将用户指纹和IMEI码保存至应用软件，再后续用户访问该应用软件时，可以通过指纹识别和IMEI码匹配对移动终端的重要信息进行保护。

[0057] S202，对用户录入的指纹进行识别，若识别失败，执行3205步骤，若识别成功，执行3203步骤；

[0058] 具体的，对于该步骤的分析，请参见图1中针对S101步骤的分析，本实施例将不再赘述。

[0059] S203,获取移动终端的串号;

[0060] S204,将该串号与应用软件中保存的移动终端的串号进行匹配;也即进行串号匹配,若匹配失败,执行S205步骤,若匹配成功,执行S207步骤;

[0061] S205,退出并锁定应用软件;

[0062] 具体的,锁定应用软件的时间间隔本实施例不做限定,用户可根据自身需要进行自由设定,可以是1分钟,也可以是1小时,甚至用户无法对该应用程序进行再次验证,最大程度的保证用户信息免于泄露或被盗用。

[0063] S206,自动向原绑定手机号发送短信提醒;

[0064] 具体的,原绑定手机号可以理解为用户事先在应用软件中保存的手机号,或者用户在注册应用软件时填写的手机号,移动终端会将该手机号发送短信提醒。当然,对于其他提醒方式如电话提醒等,只要基于本发明提供的方案,均属于本发明保护的范围。发送短信提醒原用户后,原用户可以第一时间获知移动终端中的账号等重要信息被非法访问,让原用户可以及时采取相应措施。

[0065] S207,允许用户继续对该应用软件进行访问。

[0066] 实施例二

[0067] 本实施例基于上述实施例一对本发明提供的信息保护方法做进一步地说明,具体将以以下场景进行解释。在该场景中,移动终端为手机,移动终端的串号为IMEI码,应用软件为支付宝,用户的生物标识为指纹,具体过程如下:

[0068] 用户A的手机被用户B盗用,同时,用户B为避免用户A通过该手机供应商锁定手机并获取手机方位,将该手机的IMEI码进行非法篡改。然后,用户B在访问用户A手机中的支付宝时,移动终端会发出请求用户录入指纹的信息,假设用户B获取到用户A的指纹,成功通过指纹识别,然后手机通过手机接口获取该手机的IMEI码,并与支付宝中之前保存的串号进行匹配,由于用户B之前对手机的IMEI码进行非法篡改,导致手机从接口获取的IMEI码(即当前用户篡改的IMEI码)与支付宝中保存的IMEI码(该IMEI码为用户A存入的未篡改的IMEI码)无法匹配,导致匹配失败。用户B若通过刷机或恢复出厂等方式避免本实施例提供的信息保护操作,则用户A的相关信息同样会被清除,进一步地避免用户A的信息被盗用或泄露。

[0069] 因此,通过本发明提供的信息保护方法的实施,用户在安全支付或保护隐私等方面得到很大改善,能够更安全、放心地在移动移动终端上进行相关操作,而不用担心账户和重要信息泄露,在一定程度上加强了移动终端在支付和隐私等方面的防盗作用。

[0070] 实施例三:

[0071] 请参见图3,图3为本实施例提供的移动终端模块示意图。为了便于说明,仅示出与本发明实施例相关的部分,图3示例的移动终端可以用于实现上述图1示例的信息保护方法,其主要包括:

[0072] 设置模块301,用于对应用软件设置多级验证策略,多级验证策略至少包括对用户的生物标识进行识别和对移动终端串号进行匹配;

[0073] 验证模块302,用于开启应用软件后,根据多级验证策略进行验证;

[0074] 处理模块303,用于若多级验证策略中的至少一级验证策略未通过,则开启应用软件的保护处理。

[0075] 具体的,上述应用软件包括但不限于以下几种软件:短信、微信、相册、支付宝,用

户可根据自身需求自主设定需要进行信息保护的应用软件列表,同时,该应用软件基于移动终端实现各种功能。此外,设置模块301中提到的“多级”是指两级或两级以上。进一步地,对应用软件设置多级验证策略,可以理解为设置多层验证标准,若前一验证标准通过,继续执行下一验证标准;若前一验证标准未通过,则终止验证过程。并将该多级验证策略保存至应用软件中以便后续验证。

[0076] 此外,上述移动终端的串号包括但不限于IMEI(国际移动设备标识)、SN码、移动终端马达的编号、芯片的编号,只要能表明移动终端唯一性的串号均可应用于本发明。其中,该IMEI由GSM(全球移动通信协会)统一分配,是由15位数字组成的“电子串号”,它与每个移动终端一一对应,且该标识是全世界唯一的,每一个移动终端在组装完成后都被赋予一个全球唯一的一组号码,这个号码从生产到交付使用都被制造生产的厂商所记录,用于区别各移动终端,通常存储于手机的存储器或CPU(中央处理器)中,优选地,存于EEPROM(俗称“码片”)里,可用于监控被窃或无效的移动终端。例如:当移动终端被盗时,如果知道IMEI码,可以通过移动终端供应商进行终端锁定,即获知被盗之后的手机号码,中止移动终端的通话功能,并获知移动终端的方位。SN(产品序列号)码是产品的身份证号码,用于验证产品的合法身份,保障用户的正版权益,在移动终端中,SN码一般指软件注册码信息,是一个产品出厂的系列号,一个产品只对应一组产品序列号,也具有唯一性。应该明白的是,上述移动终端串号为IMEI仅用于对本实施例进行解释,并不用于限定本发明,本实施例下文中将以IMEI为例对本发明的方案进行解释。

[0077] 对于设置模块301中提到的生物识别技术,包括指纹识别、虹膜识别、脉搏识别等。优选地,本实施例以指纹识别为例进行解释,其整体工作原理是:将一个人同他的指纹对应起来,通过对他的指纹和预先保存的指纹进行比较,就可验证他的真实身份。因为每个人的皮肤(包括指纹在内)纹路在图案、断点和交叉点上各不相同,也即每个人的皮肤纹路是唯一的,且终生不变,依靠这种唯一性和稳定性,实现指纹识别技术。

[0078] 需要注意的是,对于验证模块302,本实施例以指纹识别和移动终端IMEI码为例对本发明进行解释,但不用于限定本发明。具体的,指纹识别和移动终端的IMEI匹配,包括但不限于以下三种操作过程:

[0079] 一、指纹识别和移动终端的IMEI码同时进行验证;即移动终端在录入用户指纹进行识别的同时,在后台也会获取移动终端的IMEI码与应用软件中保存的IMEI码进行匹配,使得用户在解锁应用软件上耗费的时间更短,进而更好的提升用户体验;

[0080] 二、先进行指纹识别,再进行IMEI码匹配;即移动终端先发送请求用户录入指纹的信息,在用户指纹录入完毕之后,将录入的用户指纹与应用软件中采集的指纹进行匹配,若匹配成功,则调用移动终端接口获取移动终端的IMEI码,并与应用软件中保存的IMEI码进行匹配,若匹配成功,则允许用户访问该应用软件,获取相关用户信息;

[0081] 三、先进行IMEI码匹配,再进行指纹识别;即移动终端先调用移动终端接口获取移动终端的IMEI码,然后与应用软件中保存的IMEI码进行匹配,若匹配成功,则发送请求用户录入指纹的信息,在用户指纹录入完毕之后,将录入的用户指纹与应用软件中采集的指纹进行匹配,若匹配成功,则允许用户访问该应用软件,获取相关用户信息。

[0082] 进一步地,在处理模块303中,若多级验证策略中的至少一级验证策略未通过,开启应用软件保护处理的过程具体为:在对用户指纹信息识别完毕、对移动终端IMEI码匹配

完毕之后,若指纹识别失败、移动终端IMEI码匹配失败,则移动终端自动退出并锁定该应用软件,同时,自动向应用软件中绑定的手机号发送短信提醒。应当明白的是,锁定该应用软件的时间周期本实施例不做限定,用户可根据自身需要进行自由设定,可以是1分钟,也可以是1小时,甚至用户无法对该应用程序进行再次验证,最大程度的保证用户信息免于泄露或被盗用。

[0083] 通过上述各模块执行的操作,用户能够最大程度的避免移动终端中的信息被泄露,放心、安全的在移动终端上进行操作,从而提升用户的满意度。

[0084] 进一步地,请参见图4,图4为本实施例提供的移动终端详细模块示意图,该移动终端包括:存储模块401、设置模块402、验证模块403、处理模块404。

[0085] 存储模块401用于采集用户录入的指纹,保存手机的IMEI码;

[0086] 设置模块402用于对应用软件设置两级验证策略该两级验证策略分别为对用户录入的指纹进行识别和对手机IMEI码进行匹配;

[0087] 验证模块403用于开启应用软件后,根据两级验证策略进行验证;

[0088] 处理模块404用于若指纹识别未通过和/或手机IMEI码未通过,则开启所述应用软件的保护处理;

[0089] 其中,在验证模块403中包括验证子模块4031,用于识别用户录入的指纹,若识别成功,则将所述移动终端串号和所述应用软件中保存的串号进行匹配;若匹配失败,则开启所述应用软件的保护处理。在处理模块404中包括:处理子模块4041,用于退出并锁定应用软件;还包括发送子模块4042,用于获取所述应用软件中存储的用户信息,根据所述用户信息向对应用户发出警告。

[0090] 应该明白的是,对处理子模4041和发送子模块4042执行操作的先后顺序,本实施例不进行限定,可以先进行退出并锁定应用软件的操作,再进行自动向原绑定手机号发送短信提醒的操作;也可以先进行自动向原绑定手机号发送短信提醒的操作,再进行退出并锁定应用软件的操作;甚至二者可同时进行。通过对以上技术方案的实施,能够极大的对用户信息进行安全保护,从而提升用户在移动支付、隐私保护等方面的安全性,在一定程度上加强了移动终端在支付、隐私等方面的防盗作用。

[0091] 以上内容是结合具体的实施方式对本发明所作的进一步详细说明,不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干简单推演或替换,都应当视为属于本发明的保护范围。

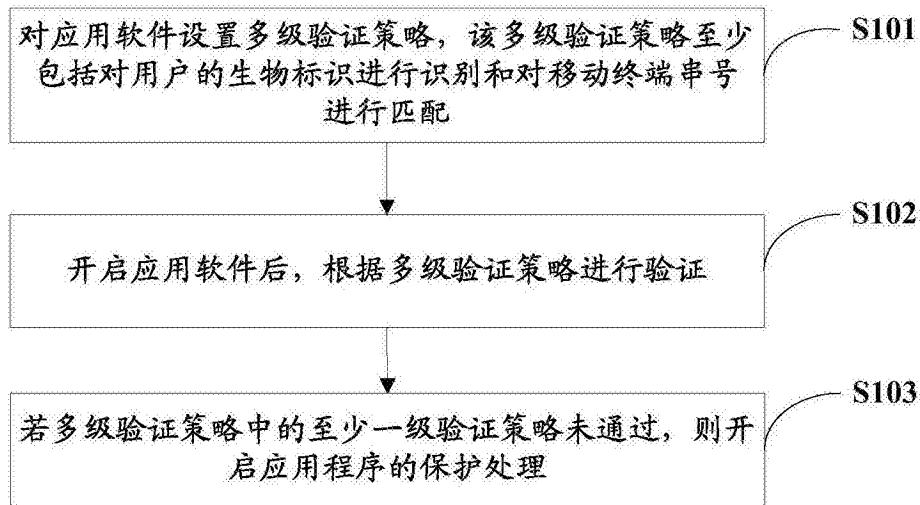
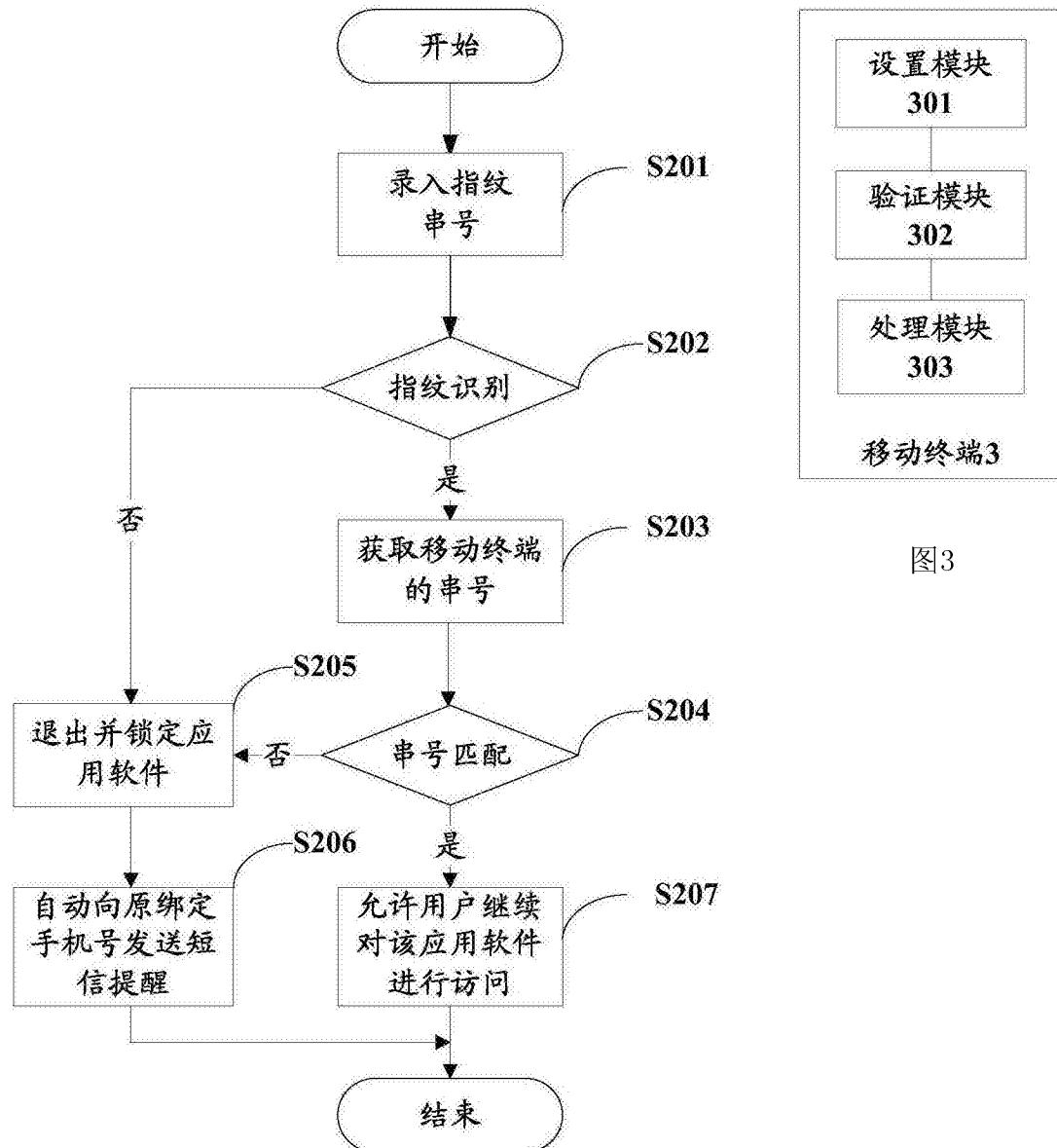


图1



移动终端3

图3

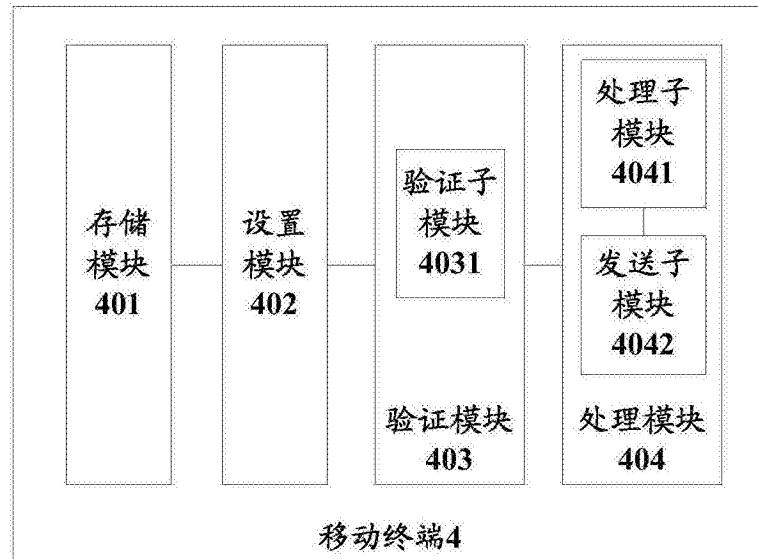


图4