(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 105787400 A
(43)申请公布日 2016.07.20

(21)申请号 201610105124.5

(22)申请日 2016.02.25

(71)申请人 上海斐讯数据通信技术有限公司
地址 201616 上海市松江区思贤路3666号

(72)发明人 刘佳星

(74)专利代理机构 上海硕力知识产权代理事务所 31251
代理人 郭桂峰

(51)Int.Cl.
G06F 21/88(2013.01)
G06F 21/32(2013.01)
G06F 21/62(2013.01)

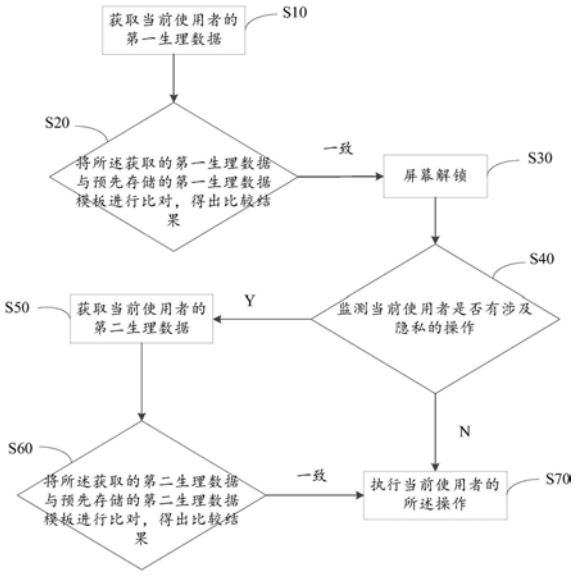
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种基于移动终端的安全防护方法及系统

(57)摘要

本发明公开了一种基于移动终端的安全防护方法及系统，包括：步骤S10获取当前使用者的第一生理数据；步骤S20将获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果，若一致，则执行步骤S30；步骤S30屏幕解锁；步骤S40监测当前使用者是否有涉及隐私的操作，若是，则执行步骤S50，若否，则执行步骤S70；步骤S50获取当前使用者的第二生理数据；步骤S60将获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果，若一致，则执行步骤S70；步骤S70执行当前使用者的操作。利用生理数据唯一性的特点保障用户的资金及隐私安全。



CN 105787400 A

1.一种基于移动终端的安全防护方法,其特征在于,包括:

步骤S10获取当前使用者的第一生理数据;

步骤S20将所述获取的第一生理数据与预先存储的第一生理数据模板进行比对,得出比较结果,若一致,则执行步骤S30;

步骤S30屏幕解锁;

步骤S40监测当前使用者是否有涉及隐私的操作,若是,则执行步骤S50,若否,则执行步骤S70;

步骤S50获取当前使用者的第二生理数据;

步骤S60将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对,得出比较结果,若一致,则执行步骤S70;

步骤S70执行当前使用者的所述操作。

2.一种如权利要求1所述的基于移动终端的安全防护方法,其特征在于,所述步骤S20还包括:

将所述获取的第一生理数据与预先存储的第一生理数据模板进行比对,得出比较结果,若不一致,则执行步骤S81;

步骤S81判断所述获取的第一生理数据与所述预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值,若是,则执行步骤S90;若否,则执行步骤S10;

步骤S90发送当前使用者的信息至预设的邮箱地址。

3.一种如权利要求1所述的基于移动终端的安全防护方法,其特征在于,所述步骤S60还包括:

将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对,得出比较结果,若不一致,则执行步骤S82;

步骤S82判断所述获取的第二生理数据与所述预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值,若是,则执行步骤S90;若否,则执行步骤S10;

步骤S90发送当前使用者的信息至预设的邮箱地址。

4.一种如权利要求2或3所述的基于移动终端的安全防护方法,其特征在于,所述步骤S90还包括:

步骤S91获取当前使用者的位置信息;

所述步骤S90中所述当前使用者的信息包括:

当前使用者的位置信息,和/或,所述获取的第一生理数据,和/或,所述获取的第二生理数据。

5.一种如权利要求4所述的基于移动终端的安全防护方法,其特征在于,还包括:

步骤S100清除移动终端的所有数据;

步骤S110自动关闭移动终端。

6.一种基于移动终端的安全防护系统,其特征在于,包括:

生理数据获取模块,获取当前使用者的第一生理数据,以及,获取当前使用者的第二生理数据;

存储模块,存储第一生理数据模板,以及,存储第二生理数据模板;

比较模块,与所述生理数据获取模块、存储模块电连接,将所述获取的第一生理数据与

预先存储的第一生理数据模板进行比对，得出比较结果，以及，将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果；

解锁模块，与所述比较模块电连接，当所述获取的第一生理数据与预先存储的第一生理数据模板的比较结果一致时，屏幕解锁；

监测模块，与所述解锁模块、生理数据获取模块电连接，监测当前使用者是否有涉及隐私的操作；

执行模块，与所述比较模块、所述监测模块电连接，当所述获取的第二生理数据与预先存储的第二生理数据模板的比较结果一致时，执行当前使用者的所述操作，以及，监测当前使用者没有涉及隐私的操作时，执行当前使用者的所述操作。

7.一种如权利要求6所述的基于移动终端的安全防护系统，其特征在于，还包括：

次数判断模块，与所述比较模块、所述生理数据获取模块电连接，判断所述获取的第一生理数据与所述预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值，以及，判断所述获取的第二生理数据与所述预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值；

所述次数判断模块还包括：

次数存储子模块，存储所述比较结果不一致的次数的预设值。

8.一种如权利要求7所述的基于移动终端的安全防护系统，其特征在于，还包括：

发送模块，与所述次数判断模块、所述生理数据获取模块电连接，并当所述比较结果不一致的次数达到预设值时，发送当前使用者的信息至预设的邮箱地址。

9.一种如权利要求8所述的基于移动终端的安全防护系统，其特征在于，所述发送模块还包括：

位置获取子模块，获取当前使用者的位置信息，所述当前使用者的信息进一步包括所述位置信息；

邮箱存储子模块，存储预设的邮箱地址。

10.一种如权利要求8或9所述的基于移动终端的安全防护系统，其特征在于，还包括：

数据清除模块，与所述发送模块电连接，清除移动终端的所有数据；

关机模块，与所述数据清除模块电连接，自动关闭移动终端。

一种基于移动终端的安全防护方法及系统

技术领域

[0001] 本发明涉及移动终端安全领域，尤其涉及一种基于移动终端的安全防护方法及系统。

背景技术

[0002] 随着移动终端的普及与互联网技术的不断发展，越来越多的用户选择把自己的银行卡与手机绑定，实现快捷支付；而用户的个人隐私也会在使用时存储在手机中，以便下次快速访问。因此，关于移动终端的安全性问题变得尤为重要，当手机丢失、被盗时，都有可能使用户的资金被他人盗刷，同时也导致一些个人隐私被泄露。

[0003] 现有的移动终端中，用户会设置锁屏密码以保护手机，但对于专业一点的人士来说，密码型屏幕锁较容易被破解，还是会对用户的个人隐私及资金产生一定的威胁。

[0004] 另外，现在有的移动终端也会有防盗系统，当多次输入错误的密码后，自动开启前置摄像头以获取当前使用者的照片发送给用户，但只要当前使用者有意识地避开前置摄像的工作范围就不会对其产生影响。

发明内容

[0005] 本发明的目的是提供一种基于移动终端的安全防护方法及系统，提高移动终端的使用安全，进一步保护用户的资金和隐私安全。

[0006] 本发明提供的技术方案如下：

[0007] 一种基于移动终端的安全防护方法，包括：步骤S10获取当前使用者的第一生理数据；步骤S20将所述获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果，若一致，则执行步骤S30；步骤S30屏幕解锁；步骤S40监测当前使用者是否有涉及隐私的操作，若是，则执行步骤S50，若否，则执行步骤S70；步骤S50获取当前使用者的第二生理数据；步骤S60将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果，若一致，则执行步骤S70；步骤S70执行当前使用者的所述操作。

[0008] 进一步优选地，所述步骤S20还包括：将所述获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果，若不一致，则执行步骤S81；步骤S81判断所述获取的第一生理数据与所述预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值，若是，则执行步骤S90；若否，则执行步骤S10；步骤S90发送当前使用者的信息至预设的邮箱地址。

[0009] 进一步优选地，所述步骤S60还包括：将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果，若不一致，则执行步骤S82；步骤S82判断所述获取的第二生理数据与所述预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值，若是，则执行步骤S90；若否，则执行步骤S10；步骤S90发送当前使用者的信息至预设的邮箱地址。

[0010] 进一步优选地，所述步骤S90还包括：步骤S91获取当前使用者的位置信息；所述步

骤S90中所述当前使用者的信息包括:当前使用者的位置信息,和/或,所述获取的第一生理数据,和/或,所述获取的第二生理数据。

[0011] 进一步优选地,还包括:步骤S100清除移动终端的所有数据;步骤S110自动关闭移动终端。

[0012] 本发明还提供一种基于移动终端的安全防护系统,包括:生理数据获取模块,获取当前使用者的第一生理数据,以及,获取当前使用者的第二生理数据;存储模块,存储第一生理数据模板,以及,存储第二生理数据模板;比较模块,与所述生理数据获取模块、存储模块电连接,将所述获取的第一生理数据与预先存储的第一生理数据模板进行比对,得出比较结果,以及,将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对,得出比较结果;解锁模块,与所述比较模块电连接,当所述获取的第一生理数据与预先存储的第一生理数据模板的比较结果一致时,屏幕解锁;监测模块,与所述解锁模块、生理数据获取模块电连接,监测当前使用者是否有涉及隐私的操作;执行模块,与所述比较模块、所述监测模块电连接,当所述获取的第二生理数据与预先存储的第二生理数据模板的比较结果一致时,执行当前使用者的所述操作,以及,监测当前使用者没有涉及隐私的操作时,执行当前使用者的所述操作。

[0013] 进一步优选地,还包括:次数判断模块,与所述比较模块、所述生理数据获取模块电连接,判断所述获取的第一生理数据与所述预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值,以及,判断所述获取的第二生理数据与所述预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值;所述次数判断模块还包括:次数存储子模块,存储所述比较结果不一致的次数的预设值。

[0014] 进一步优选地,还包括:发送模块,与所述次数判断模块、所述生理数据获取模块电连接,并当所述比较结果不一致的次数达到预设值时,发送当前使用者的信息至预设的邮箱地址。

[0015] 进一步优选地,所述发送模块还包括:位置获取子模块,获取当前使用者的位置信息,所述当前使用者的信息进一步包括所述位置信息;邮箱存储子模块,存储预设的邮箱地址。

[0016] 进一步优选地,还包括:数据清除模块,与所述发送模块电连接,清除移动终端的所有数据;关机模块,与所述数据清除模块电连接,自动关闭移动终端。

[0017] 与现有技术相比,本发明的有益效果在于:

[0018] 1、解锁和涉及隐私操作时,验证用户的生理数据,生理数据可以为人脸识别数据、声音数据、指纹数据等,与现有的仅仅密码保护移动终端相比,生理数据的唯一性更能够确保移动终端的安全性;同时,屏幕解锁和隐私操作需要验证的生理数据不相同,进一步保证了用户资金、个人隐私的安全使用。

[0019] 2、用户可以预先设置自己的防盗邮箱,在屏幕解锁时,当输入的生理数据与预先存储的数据不匹配的次数达到一定值时,系统会自动把当前使用者输入的生理数据发送到防盗邮箱,便于移动终端的主人追踪,由于生理数据的唯一性,能够快速确定偷盗者的身份,追回失物。

[0020] 3、当移动终端失窃时,移动终端可能处于待机状态,也可能处于正常操作系统的情况,为了进一步保障用户的资金、个人隐私的安全,涉及到资金和个人隐私的操作时,需

要再次验证生理数据，若当前使用者并非用户本人，错误的生理数据无法与预先存储的生理数据匹配，则不能执行隐私操作；同时也规定了容许错误的次数，若达到一定值，则会把获取的错误的生理数据发送到防盗邮件，便于移动终端的主人确定偷盗者身份，拿回失物；另外，锁屏和隐私操作需要验证的生理数据不同，进一步确保了移动终端的安全使用。

[0021] 4、利用GPS可以获取当前使用者的位置信息，发送位置信息和获取的生理数据给防盗邮箱，不仅可以确定偷盗者的身份，也能快速定位其所在的位置，便于移动终端的主人尽快找回丢失的物品。

[0022] 5、当输入的生理数据不匹配时，发送相关信息至防盗邮箱后，移动终端会自动清除所有的数据，即恢复出厂设置，并关机；即使不能追回失物，清除数据也保证了移动终端主人的资金及个人隐私不会被他人获取，最大限度的挽回用户的损失。

[0023] 本发明的基于移动终端的安全防护方法及系统，利用生理数据唯一性的特点保障用户的资金及隐私安全；若验证失败，发送获取的错误的生理数据和位置信息也使用户能够确认偷盗者的身份及当前位置，便于失物找回；另外，验证失败后自动清除移动终端数据的设置，进一步保证了用户资金和隐私的安全性，当由于种种原因无法顺利追回失物时，最大限度地挽回了用户的损失。

附图说明

[0024] 下面将以明确易懂的方式，结合附图说明优选实施方式，对一种基于移动终端的安全防护方法及系统的上述特性、技术特征、优点及其实现方式予以进一步说明。

[0025] 图1是本发明基于移动终端的安全防护方法一个实施例的流程图；

[0026] 图2是本发明基于移动终端的安全防护方法另一个实施例的流程图；

[0027] 图3是本发明基于移动终端的安全防护系统一个实施例的结构示意图；

[0028] 图4是本发明基于移动终端的安全防护系统另一个实施例的结构示意图。

[0029] 附图标号说明：

[0030] 1.生理数据获取模块，2.存储模块，3.比较模块，4.解锁模块，5.监测模块，6.执行模块，7.次数判断模块，8.次数存储子模块，9.发送模块，10.邮箱存储子模块，11.位置获取子模块，12.数据清除模块，13.关机模块。

具体实施方式

[0031] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对照附图说明本发明的具体实施方式。显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图，并获得其他的实施方式。

[0032] 为使图面简洁，各图中只示意性地表示出了与本发明相关的部分，它们并不代表其作为产品的实际结构。另外，以使图面简洁便于理解，在有些图中具有相同结构或功能的部件，仅示意性地绘示了其中的一个，或仅标出了其中的一个。在本文中，“一个”不仅表示“仅此一个”，也可以表示“多于一个”的情形。

[0033] 图1是本发明基于移动终端的安全防护方法一个实施例的流程图。如图1所示，本实施例中，提供了一种基于移动终端的安全防护方法，包括：步骤S10获取当前使用者的第

一生理数据;步骤S20将获取的第一生理数据与预先存储的第一生理数据模板进行比对,得出比较结果,若一致,则执行步骤S30;步骤S30屏幕解锁;步骤S40监测当前使用者是否有涉及隐私的操作,若是,则执行步骤S50,若否,则执行步骤S70;步骤S50获取当前使用者的第二生理数据;步骤S60将获取的第二生理数据与预先存储的第二生理数据模板进行比对,得出比较结果,若一致,则执行步骤S70;步骤S70执行当前使用者的操作。

[0034] 在本实施例中,用户点亮移动终端的显示屏时,需要验证用户的生理数据进行屏幕解锁,解锁时需要验证的第一生理数据为脸部数据,通过移动终端的前置摄像头利用人脸识别技术采集当前使用者的脸部数据,若匹配,则移动终端成功解锁,当前使用者可以顺利进入操作系统中操作移动终端;当使用者有涉及到隐私操作时,为了进一步提高移动终端的安全性,需要再次验证当前使用者的生理数据,隐私操作和屏幕解锁需要验证的生理数据不同,第二生理数据为指纹数据,只有匹配成功,才能操作移动终端上的隐私操作。涉及隐私的操作可包括:联系人,短信,图片,社交软件,第三方支付软件,银行软件等。

[0035] 在其它实施例中,在利用生理数据解锁屏幕前,也可以再加一步输入密码,利用密码和生物数据双重保护移动终端,只有两者都对时,才能成功解锁屏幕终端,进入系统操作。生理数据可以为脸部数据、指纹数据、声音数据等。屏幕解锁时需要验证的第一生理数据和涉及隐私操作时需要验证的第二生理数据可以用户人为设定,例如:可以设置第一生理数据为指纹数据,第二生理数据为脸部数据和声音数据,第二生理数据也可以只设置为脸部数据,或,声音数据;只要保证第一生理数据和第二生理数据不同即可,不对它们的数量进行限定。

[0036] 在本发明的另一个实施例中,除与上述相同的部分外,步骤S20还包括:将获取的第一生理数据与预先存储的第一生理数据模板进行比对,得出比较结果,若不一致,则执行步骤S81;步骤S81判断获取的第一生理数据与预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值,若是,则执行步骤S90;若否,则执行步骤S10;步骤S90发送当前使用者的信息至预设的邮箱地址。

[0037] 优选地,步骤S60还包括:将获取的第二生理数据与预先存储的第二生理数据模板进行比对,得出比较结果,若不一致,则执行步骤S82;步骤S82判断获取的第二生理数据与预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值,若是,则执行步骤S90;若否,则执行步骤S10;步骤S90发送当前使用者的信息至预设的邮箱地址。

[0038] 具体的,用户可以预先自行设定容错次数和防盗邮箱地址,例如,当输错次数达到3次时,就发送当前使用者输入的生理数据至防盗邮箱地址。当用户丢失自己的移动终端时,可以检查其设置的防盗邮箱,查看是否有相关邮件,若有,利用生理数据唯一性的特点可以快速确定偷盗者,便于警察寻找犯罪嫌疑人、追回失物。

[0039] 若第一生理数据设置为需要指纹验证,当输入的指纹数据错误达到3次时,移动终端就自动把获取的错误的指纹数据发送至防盗邮箱地址;另外,移动终端也可以后台开启前置摄像头获取当前使用者的照片,把获取的照片和错误的指纹数据一起发送至防盗邮箱地址,尽可能提供足够的线索,便于警察破案。

[0040] 优选地,步骤S90还包括:步骤S91获取当前使用者的位置信息;步骤S90中当前使用者的信息包括:当前使用者的位置信息,和/或,获取的第一生理数据,和/或,获取的第二生理数据。

[0041] 具体的，当验证失败的次数达到预设值时，移动终端可以后台打开GPS定位系统，获取当前的位置，把获取的所有生理数据和当前的位置信息发送至防盗邮箱地址，使偷盗者的位置及身份被快速确认，便于失物的找回。

[0042] 优选地，还包括：步骤S100清除移动终端的所有数据；步骤S110自动关闭移动终端。

[0043] 具体的，在发送出相关信息至防盗邮箱后，移动终端会自动清除其内部的所有数据，即恢复出厂设置，完成后，自动关机。虽然发送了能够获取到的所有线索，但凡事都有不确定性，不一定保证移动终端能够被用户找回，清除所有的数据保证了用户在无法找回其设备的情况下避免其资金、个人隐私的泄露，造成更大的损失。

[0044] 图2是本发明基于移动终端的安全防护方法另一个实施例的流程图。如图2所示，本实施例中，提供了一种基于移动终端的安全防护方法，包括：步骤S10获取当前使用者的第一生理数据；步骤S20将获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果，若一致，则执行步骤S30，若不一致，则执行步骤S81；步骤S30屏幕解锁；步骤S40监测当前使用者是否有涉及隐私的操作，若是，则执行步骤S50，若否，则执行步骤S70；步骤S50获取当前使用者的第二生理数据；步骤S60将获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果，若一致，则执行步骤S70，若不一致，则执行步骤S82；步骤S70执行当前使用者的操作；步骤S81判断获取的第一生理数据与预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值，若是，则执行步骤S90，若否，则执行步骤S10；步骤S82判断获取的第二生理数据与预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值，若是，则执行步骤S90，若否，则执行步骤S10；步骤S90发送当前使用者的信息至预设的邮箱地址；步骤S90还包括：步骤S91获取当前使用者的位置信息；步骤S100清除移动终端的所有数据；步骤S110自动关闭移动终端。

[0045] 具体的，在屏幕解锁和隐私操作时验证不同生理数据来确保移动终端的安全，保证了即使偷盗者拥有用户的一种生理数据，例如：指纹数据，也不能完完整整地操作整个移动终端，获取移动终端上的所有数据，进一步保障了数据的安全性。验证多种生理数据是指，人脸识别技术、指纹识别技术、声音识别技术等，这种验证的设置，让想使用移动终端的人不得不提供其生理数据以进入系统或执行隐私操作。当移动终端被盗时，避免了有些人在破解密码后，利用小技巧逃脱移动终端防盗系统监控的情况，在保障移动终端使用安全的同时，能够获取足够的线索，方便后续失物的追踪和拿回。当获取的生物数据没有照片时(即当前使用者在没有进入脸部识别的流程前，输入的信息错误次数就达到预设值)，移动终端可以后台自动启动前置摄像头拍摄当前使用者的照片，然后把先前获取的生理数据、位置信息和后台自动获取的照片一起发送至防盗邮箱

[0046] 图3是本发明基于移动终端的安全防护系统一个实施例的结构示意图。参见图3，本实施例提供了一种基于移动终端的安全防护系统，包括：生理数据获取模块1，获取当前使用者的第一生理数据，以及，获取当前使用者的第二生理数据；存储模块2，存储第一生理数据模板，以及，存储第二生理数据模板；比较模块3，与生理数据获取模块1、存储模块2电连接，将获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果，以及，将获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果；解锁模块4，与比较模块3电连接，当获取的第一生理数据与预先存储的第一生理数据模板的比

较结果一致时，屏幕解锁；监测模块5，与解锁模块4、生理数据获取模块1电连接，监测当前使用者是否有涉及隐私的操作；执行模块6，与比较模块3、监测模块5电连接，当获取的第二生理数据与预先存储的第二生理数据模板的比较结果一致时，执行当前使用者的操作，以及，监测当前使用者没有涉及隐私的操作时，执行当前使用者的操作。

[0047] 具体的，生理数据获取模块1可以为移动终端上的前置摄像头(获取脸部数据)、麦克(获取声音数据)、指纹识别区域(获取指纹数据)；用户可以在第一次使用移动终端的时候就存入自己的多种生理数据；当以后进行解锁、隐私操作时，就会将当前获取的生理数据与预先存入的生理数据进行比较，只有正确时，才会顺利解锁、执行隐私操作。

[0048] 优选地，还包括：次数判断模块7，与比较模块3、生理数据获取模块1电连接，判断获取的第一生理数据与预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值，以及，判断获取的第二生理数据与预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值；次数判断模块7还包括：次数存储子模块8，存储比较结果不一致的次数的预设值。

[0049] 具体的，用户可以自行设定允许输错生理数据的次数，若达到这个次数，就可以允许移动终端进行防盗操作，确保移动终端在丢失的情况下能够提供尽量提供线索便于追回。

[0050] 优选地，还包括：发送模块9，与次数判断模块7、生理数据获取模块1电连接，并当所述比较结果不一致的次数达到预设值时，发送当前使用者的信息至预设的邮箱地址。

[0051] 优选地，发送模块9还包括：位置获取子模块11，获取当前使用者的位置信息，所述当前使用者的信息进一步包括所述位置信息；邮箱存储子模块10，存储预设的邮箱地址。

[0052] 具体的，当生理数据输错的次数达到一定值，移动终端后台自动运行GPS定位系统确定当前的位置信息，把当前获取的所有生理数据和当前的位置信息发送到用户预先设置的防盗邮箱，便于用户通过此邮箱查看相关线索，以确定偷盗者和当前的位置。

[0053] 优选地，还包括：数据清除模块12，与发送模块9电连接，清除移动终端的所有数据；关机模块13，与数据清除模块12电连接，自动关闭移动终端。

[0054] 俗话说，万事皆有可能，即使尽量提供了线索，并不能保证移动终端一定能够寻回，清除移动终端上的数据，即，使移动终端恢复出厂设置的这种设定，进一步保证了用户资金和个人隐私的安全性，在移动终端无法追回时，避免了更大的损失。

[0055] 图4是本发明基于移动终端的安全防护系统另一个实施例的结构示意图。参见图4，本实施例提供了一种基于移动终端的安全防护系统，包括：生理数据获取模块1，获取当前使用者的第一生理数据，以及，获取当前使用者的第二生理数据；存储模块2，存储第一生理数据模板，以及，存储第二生理数据模板；比较模块3，与生理数据获取模块1、存储模块2电连接，将获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果，以及，将获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果；解锁模块4，与比较模块3电连接，当获取的第一生理数据与预先存储的第一生理数据模板的比较结果一致时，屏幕解锁；监测模块5，与解锁模块4、生理数据获取模块1电连接，监测当前使用者是否有涉及隐私的操作；执行模块6，与比较模块3、监测模块5电连接，当获取的第二生理数据与预先存储的第二生理数据模板的比较结果一致时，执行当前使用者的操作，以及，监测当前使用者没有涉及隐私的操作时，执行当前使用者的操作；次数判断模块7，与

比较模块3、生理数据获取模块1电连接，判断获取的第一生理数据与预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值，以及，判断获取的第二生理数据与预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值；次数判断模块7还包括：次数存储子模块8，存储比较结果不一致的次数的预设值；发送模块9，与次数判断模块7、生理数据获取模块1电连接，并当所述比较结果不一致的次数达到预设值时，发送当前使用者的信息至预设的邮箱地址；发送模块9还包括：位置获取子模块11，获取当前使用者的位置信息，当前使用者的信息进一步包括所述位置信息；邮箱存储子模块10，存储预设的邮箱地址；数据清除模块12，与发送模块9电连接，清除移动终端的所有数据；关机模块13，与数据清除模块12电连接，自动关闭移动终端。

[0056] 具体的，在涉及到屏幕解锁和隐私操作时，在通过密码验证后，利用移动终端上的各种装置再次验证当前使用者的生理数据，由于生理数据的唯一性的特点，不容易被破解，达到了保障移动终端的使用安全。

[0057] 本发明利用生理数据的唯一性，在现有密码保护的基础上，进一步加强了对移动终端的安全保护，且利用多种生理数据的组合验证，更增加了防护安全。

[0058] 应当说明的是，上述实施例均可根据需要自由组合。以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

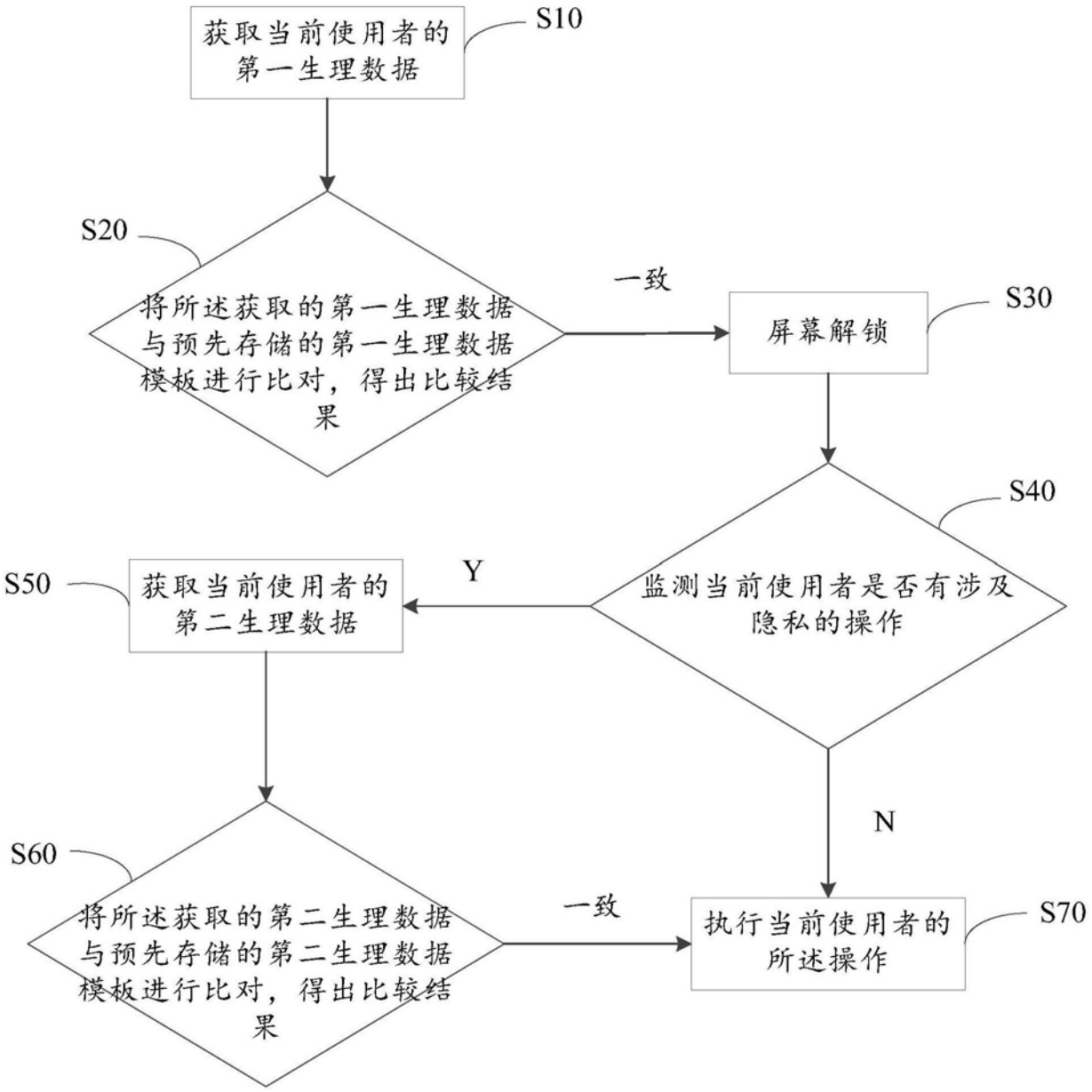

获取当前使用者的第一生理数据
S10
S20
将所述获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果
一致
屏幕解锁
S30
监测当前使用者是否有涉及隐私的操作
S40
Y
获取当前使用者的第二生理数据
S50
N
S60
将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果
一致
执行当前使用者的所述操作
S70

图1

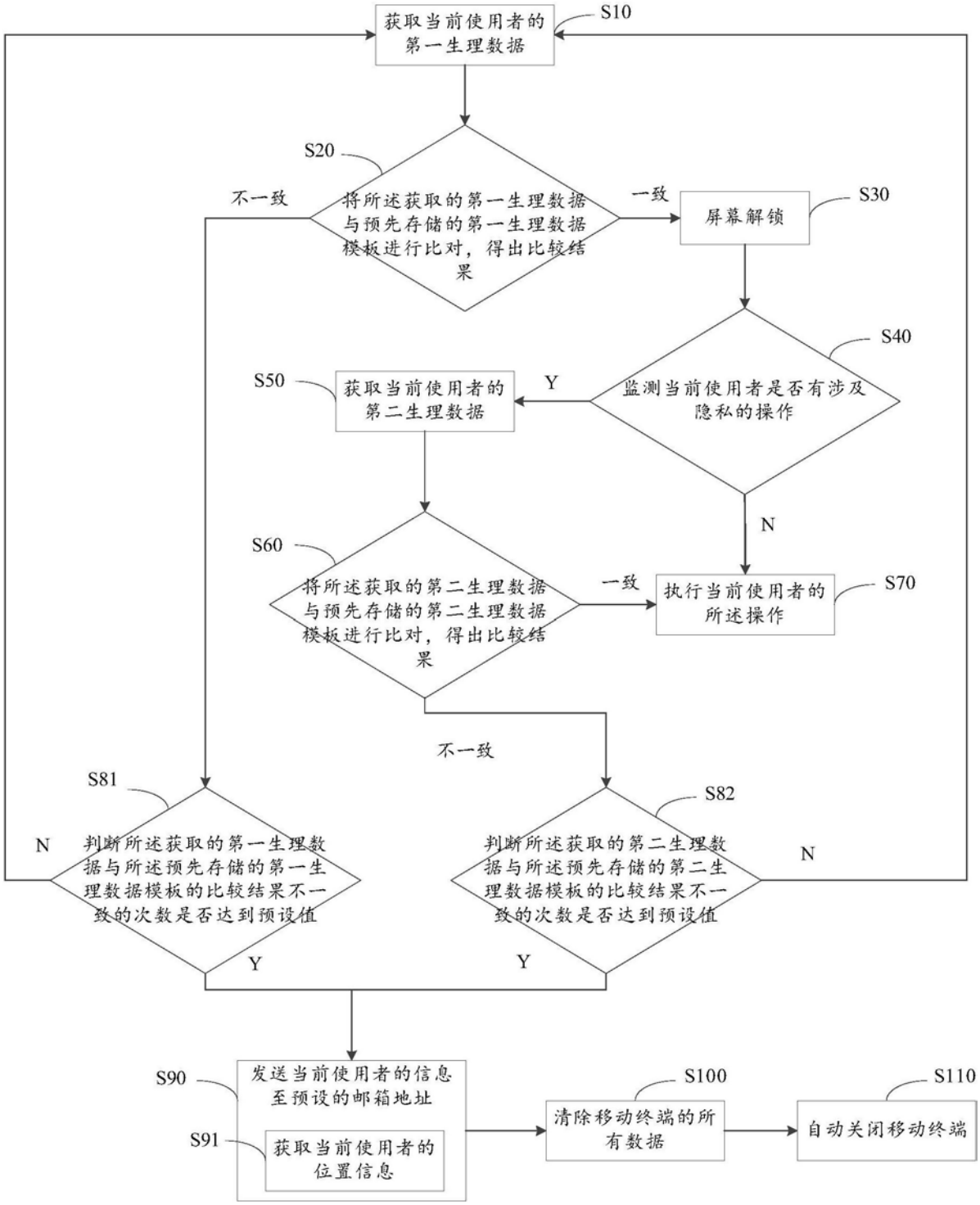

获取当前使用者的第一生理数据
S10
S20
将所述获取的第一生理数据与预先存储的第一生理数据模板进行比对，得出比较结果
不一致
一致
屏幕解锁
S30
S40
监测当前使用者是否有涉及隐私的操作
Y
S50
获取当前使用者的第二生理数据
N
S60
将所述获取的第二生理数据与预先存储的第二生理数据模板进行比对，得出比较结果
一致
执行当前使用者的所述操作
S70
不一致
S81
判断所述获取的第一生理数据与所述预先存储的第一生理数据模板的比较结果不一致的次数是否达到预设值
N
Y
S82
判断所述获取的第二生理数据与所述预先存储的第二生理数据模板的比较结果不一致的次数是否达到预设值
N
Y
S90
发送当前使用者的信息至预设的邮箱地址
S91
获取当前使用者的位置信息
S100
清除移动终端的所有数据
S110
自动关闭移动终端

图2

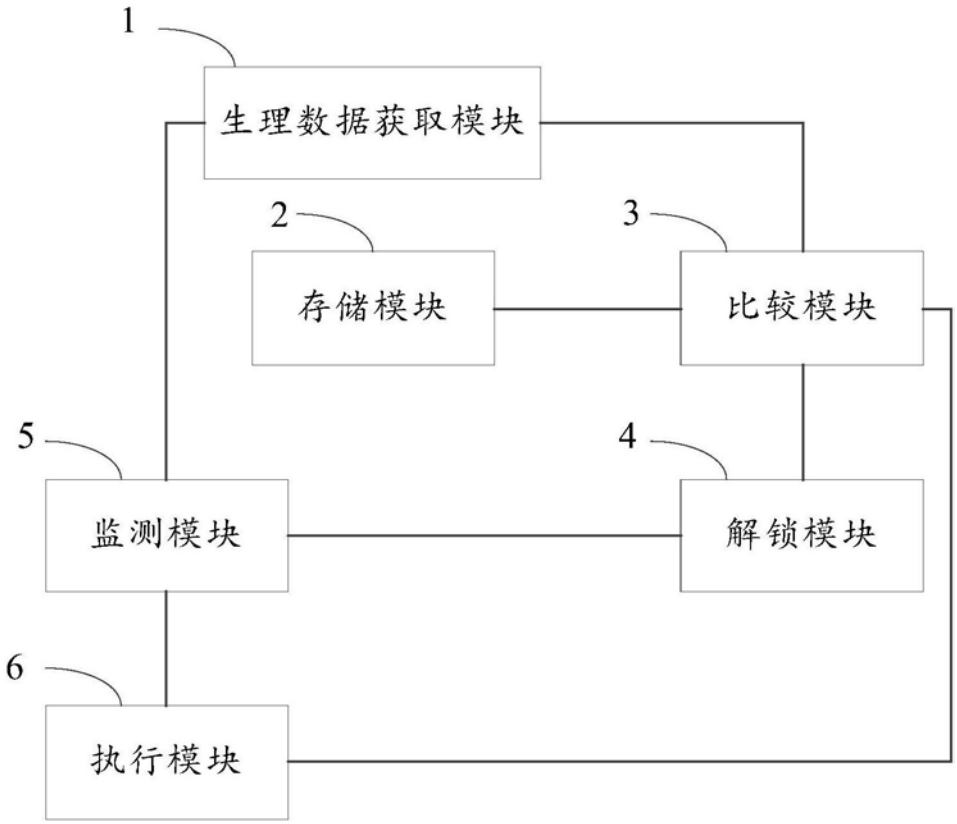

1
生理数据获取模块
2
存储模块
3
比较模块
5
监测模块
4
解锁模块
6
执行模块

图3

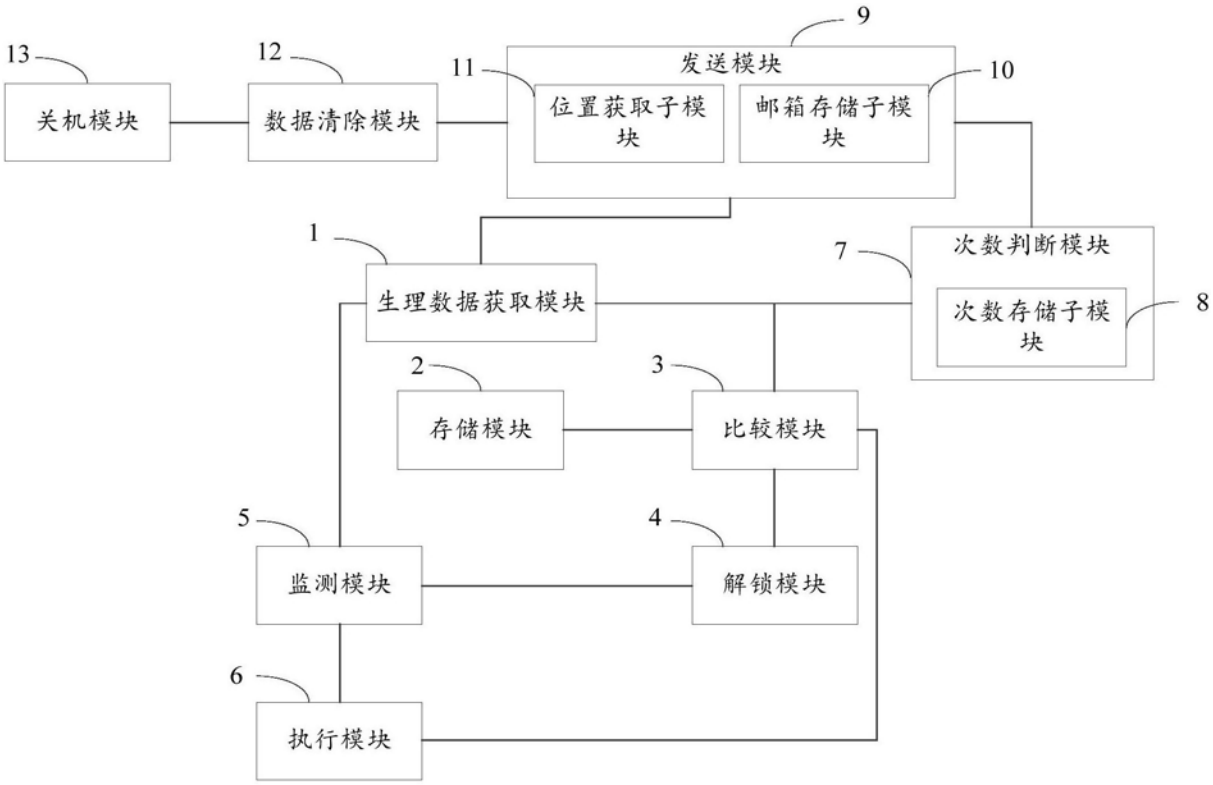

9
13
12
11
发送模块
10
关机模块
数据清除模块
位置获取子模块
邮箱存储子模块
1
次数判断模块
7
生理数据获取模块
次数存储子模块
8
2
3
存储模块
比较模块
5
4
监测模块
解锁模块
6
执行模块

图4