[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04Q 7/22 (2006.01)
H04M 1/673 (2006.01)
H04M 11/04 (2006.01)
H04N 7/18 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810068024.5

[43] 公开日 2008 年 11 月 19 日

[11] 公开号 CN 101309479A

[22] 申请日 2008.6.25

[21] 申请号 200810068024.5

[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产业园(北区)梦溪道 2 号酷派信息港(1 号楼)

[72] 发明人 肖永刚 陈维山

[74] 专利代理机构 深圳中一专利商标事务所

代理人 张全文

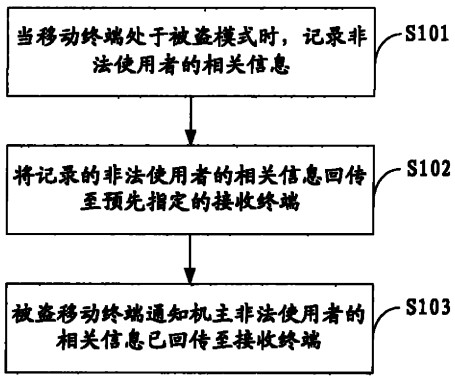
权利要求书 3 页 说明书 8 页 附图 2 页

[54] 发明名称

一种防盗移动终端及其防盗方法

[57] 摘要

本发明适用于移动通信领域，提供了一种防盗移动终端及其防盗方法，所述方法包括下述步骤：当移动终端处于被盗模式时，记录非法使用者的相关信息；将所述非法使用者的相关信息回传至预先指定的接收终端。 由于本发明实施例在移动终端处于被盗模式时，记录非法使用者的相关信息，并将非法使用者的相关信息回传至指定的接收终端，从而为追踪非法使用者提供了较为有效的线索，大大地缩小了侦查范围，有利于非法使用者的抓捕。



1、一种移动终端防盗方法，其特征在于，所述方法包括下述步骤:

当移动终端处于被盗模式时，记录非法使用者的相关信息;

将所述非法使用者的相关信息回传至预先指定的接收终端。

2、如权利要求 1 所述的方法，其特征在于，在所述当移动终端处于被盗模式时，记录非法使用者的相关信息的步骤之前，所述方法还包括:

判断移动终端是否处于被盗模式。

3、如权利要求 1 所述的方法，其特征在于，在所述将所述非法使用者的相关信息回传至预先指定的接收终端的步骤之后，所述方法还包括:

被盗移动终端向预设的报警接收端发送已将非法使用者的相关信息回传至预设的接收终端的通知。

4、如权利要求 1 所述的方法，其特征在于，所述非法使用者的相关信息为照片、录音、录像或通话记录中的一种或多种组合。

5、如权利要求 1 所述的方法，其特征在于，在所述记录非法使用者的相关信息的步骤之前，所述方法还包括:

判断是否接收到记录非法使用者的相关信息的指令，如果是，则记录非法使用者的相关信息。

6、如权利要求 1 所述的方法，其特征在于，在所述记录非法使用者的相关信息的步骤之前，所述方法还包括:

判断非法使用者是否使用移动终端的视频电话，如果是，则记录非法使用者的相关信息。

7、如权利要求 6 所述的方法，其特征在于，所述记录非法使用者的相关信息的步骤具体为:

采集单帧图像并保存;

在预设的时间间隔内采集一次单帧图像并保存;

采集预设时间长度的视频并保存;

在预设的时间间隔内采集一次预设时间长度的视频并保存；或者

不设定记录非法使用者的相关信息的时间长度，持续采集并保存非法使用者的相关信息。

8、一种防盗移动终端，其特征在于，所述移动终端包括:

被盗模式判断单元，用于判断移动终端当前是否处于被盗模式;

相关信息记录单元，用于在所述被盗模式判断单元判定移动终端处于被盗模式时，记录非法使用者的相关信息;

相关信息回传单元，用于将所述相关信息记录单元记录的非法使用者的相关信息回传至预设的接收终端。

9、如权利要求 8 所述的移动终端，其特征在于，所述移动终端还包括:

通知发送单元，用于向预设的报警接收端发送被盗移动终端已将非法使用者的相关信息回传至接收终端的通知。

10、如权利要求 8 所述的移动终端，其特征在于，所述移动终端还包括:

视频电话使用判断单元，用于在所述被盗模式判断单元判定移动终端处于被盗模式时，判断非法使用者是否使用视频电话；此时，

所述相关信息记录单元在所述视频电话使用判断单元的结果为是时，记录非法使用者的相关信息。

11、如权利要求 8 所述的移动终端，其特征在于，所述移动终端还包括:

指令接收判断单元，用于在所述被盗模式判断单元判定移动终端处于被盗模式时，判断是否接收到记录非法使用者的相关信息的指令，此时，

所述相关信息记录单元在所述指令接收判断单元的结果为是时，记录非法使用者的相关信息。

12、如权利要求 8 所述的移动终端，其特征在于，所述相关信息记录单元包括:

相关信息采集单元，用于按照预设的采集方式采集非法使用者的相关信息;

相关信息存储单元，用于存储所述相关信息采集单元采集的非法使用者的

相关信息。

一种防盗移动终端及其防盗方法

技术领域

本发明属于移动通信领域，尤其涉及一种防盗移动终端及其防盗方法。

背景技术

随着移动通信技术的发展，移动终端的使用已越来越普及，各移动终端厂家为了提高其市场竞争力，均在移动终端中集成有多种功能。而用户在使用移动终端时，产生了诸多使用记录，如存储了联系人信息、照片等较为私密的信息，如果移动终端被盗而无法追回，不仅给用户带来经济损失，同时导致用户私密信息的泄漏，因此，移动终端防盗功能成为了人们关注的焦点。

现有技术提供了一种开机密码形式的移动终端防盗方法，其具体过程简述如下：用户预先设定移动终端的开机密码，只有当用户输入了正确的开机密码，移动终端才能够开机并使用，这种移动终端防盗方法只能限制非法使用者使用移动终端，而无法向被盗者提供追回移动终端的线索，也难以追踪到非法使用者，从而无法避免用户的经济损失。

现有技术提供了另一种自动报警形式的移动终端防盗方法，其具体过程简述如下：判断移动终端是否被盗，如果被盗，则移动终端自动将报警信息发送至报警号码。这种移动终端防盗方法难以准确追踪到非法使用者，从而难以从根本上解决移动终端被盗的问题。

发明内容

本发明实施例的目的在于提供一种移动终端的防盗方法，旨在解决现有技术的防盗移动终端难以准确追踪到非法使用者的问题。

本发明实施例是这样实现的，一种移动终端的防盗方法，所述方法包括下

述步骤:

当移动终端处于被盗模式时，记录非法使用者的相关信息;

将所述非法使用者的相关信息回传至预先指定的接收终端。

本发明实施例的另一目的在于提供一种防盗移动终端，所述移动终端包括:

被盗模式判断单元，用于判断移动终端当前是否处于被盗模式;

相关信息记录单元，用于在所述被盗模式判断单元判定移动终端处于被盗模式时，记录非法使用者的相关信息;

相关信息回传单元，用于将所述相关信息记录单元记录的非法使用者的相关信息回传至预设的接收终端。

本发明实施例在移动终端处于被盗模式时，记录非法使用者的相关信息，并将非法使用者的相关信息回传至指定的接收终端，从而为追踪非法使用者提供了较为有效的线索，大大地缩小了侦查范围，有利于非法使用者的抓捕。

附图说明

图 1 是本发明第一实施例提供的移动终端防盗方法的实现流程图;

图 2 是本发明第二实施例提供的移动终端防盗方法的实现流程图;

图 3 是本发明第三实施例提供的移动终端防盗方法的实现流程图;

图 4 是本发明实施例提供的防盗移动终端的结构示意图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

在本发明实施例中，当移动终端处于被盗模式时，通过记录非法使用者的相关信息，并将记录的非法使用者的相关信息回传至预先指定的接收终端，从而使被盗者可以根据非法使用者的相关信息追踪到非法使用者。

图 1 示出了本发明实施例提供的移动终端防盗方法的实现流程，详述如下：

在步骤 S101 中，当移动终端处于被盗模式时，记录非法使用者的相关信息。

在本发明实施例中，非法使用者的相关信息包括但不限于照片、录音、录像或通话记录中的一种或者多种组合。其中照片中包括非法使用者的头像、非法使用者所处环境等，录像中包括非法使用者的图像视频、非法使用者所处环境的图像视频等。

在本发明实施例中，可以采用如下步骤记录非法使用者的相关信息：

移动终端的采集设备采集其当前可视范围内的一帧图像并保存；或者在预设的时间间隔内移动终端的采集设备采集一次其当前可视范围内的一帧图像并保存。

还可以采用如下步骤记录非法使用者的相关信息：

移动终端的采集设备采集其当前可视范围内的预设时间长度的视频并保存；或者在预设的时间间隔内，移动终端的采集设备采集一次其当前可视范围内的预设时间长度的视频并保存。

记录非法使用者的相关信息的步骤还可以为：

不设定记录非法使用者的相关信息的时间长度，持续保存非法使用者的相关信息。

在本发明实施例中，只有在移动终端处于被盗模式时，移动终端才会记录非法使用者的相关信息，而当移动终端处于正常模式时，不需要记录非法使用者的相关信息。因此，在步骤 S101 之前，该方法还包括：

判断移动终端是否处于被盗模式。

其中判断移动终端是否处于被盗模式的方式有多种，如开机身份认证判断方式，或者指令触发判断方式等。

其中开机身份认证判断方式可以是开机密码判断方式，开机指纹认证判断方式等。在本发明实施例中，以开机密码判断方式为例，对开机身份认证判断方式进行说明，其具体过程如下：用户预先设置移动终端的开机密码，当移动

终端被重启时，提示用户输入开机密码，如果移动终端用户输入的开机密码与预设的开机密码不匹配，则判定移动终端处于被盗模式，如果移动终端用户输入的开机密码与预设的开机密码匹配，则判定移动终端处于正常模式。可以理解，在开机密码判断方式中，可以设置允许用户输入密码的次数，当用户输入密码的次数达到预设值，其输入的开机密码仍无法与预设的开机密码匹配时，则判定移动终端处于被盗模式，如果在预设的次数内，用户输入的开机密码与预设的开机密码匹配，则判定移动终端处于正常模式。

指令触发判断方式的具体过程如下：当移动终端接收到机主发送的进入被盗模式的指令时，则移动终端进入被盗模式。其中机主发送进入被盗模式的指令的方式可以是短信、彩信或电子邮件等方式。

在步骤 S102 中，将记录的非法使用者的相关信息回传至预先指定的接收终端。

在本发明提供的实施例中，机主预先指定一个或多个接收终端，该接收终端用于接收被盗移动终端回传的非法使用者的相关信息。

通过采用上述移动终端防盗方法，当移动终端处于被盗模式时，可以通过以照片、录音、录像或通话记录中的一种或者多种组合，记录非法使用者的相关信息，如非法使用者的头像、非法使用者当前所处的环境等，并将记录的非法使用者的相关信息回传至预先指定的接收终端，从而给追踪非法使用者提供了重要线索，给追踪非法使用者带来极大的方便。

为了在接收终端接收到被盗移动终端回传的非法使用者的相关信息时，及时快速的通知被盗移动终端机主，在本发明另一实施例中，在步骤 S102 之后，该方法还包括下述步骤：

在步骤 S103 中，被盗移动终端通知机主非法使用者的相关信息已回传至接收终端。

在本发明实施例中，可以在移动终端中预先设置一个或多个报警接收端，该报警接收端主要用于在移动终端处于被盗模式时，接收移动终端发送的非法

使用者的相关信息已回传至预设的接收终端的通知，以使机主获知移动终端已将非法使用者的相关信息回传至预设的接收终端，从而便于机主查询预设的接收终端获取非法使用者的相关信息，以追踪非法使用者。其中报警接收端可以是用户指定的移动终端、邮箱地址、即时通信客户端等，移动终端可以以短信、彩信或电子邮件等的方式向预设的报警接收端发送上述通知。在本发明实施例中，移动终端向报警接收端发送通知是在移动终端的后台进行的，即移动终端向报警接收端发送通知不需要用户确认或者发送触发指令，因此，非法使用者无法知晓其上述通知的发送，从而更有利于追踪非法使用者。

为了使移动终端记录的非法使用者的相关信息更加有针对性，给追踪非法使用者提供更多有效的信息，图 2 示出了本发明另一实施例提供的移动终端防盗方法的实现流程，详述如下：

在步骤 S201 中，当移动终端处于被盗模式时，判断非法使用者是否使用移动终端的视频电话，如果是，则执行步骤 S202，如果不是，则移动终端被盗方法结束，不再执行以下步骤。

在步骤 S202 中，记录非法使用者的相关信息。

在本发明实施例中，由于非法使用者在使用移动终端的视频电话，因此，在记录非法使用者的相关信息时，可以从非法使用者开始使用视频电话时，就通过视频电话的采集装置采集图片、录像、录音、通话记录等，并保存。由于非法使用者正在使用移动终端的视频电话，因此，采集的图片或者录像中包括非法使用者的头像、所处环境等信息，而采集的录音或者通话记录中包括非法使用者的声音，从而使记录的非法使用者的信息更加具有针对性和有效性。其中视频电话的采集装置采集图片、录像、录音、通话记录等非法使用者的相关信息的具体步骤如上所述，在此不再赘述。

在步骤 S203 中，将记录的非法使用者的相关信息回传至预先指定的接收终端。其具体步骤如上所述，在此不再赘述。

为了在接收终端接收到被盗移动终端回传的非法使用者的相关信息时，及

时快速的通知被盗移动终端机主，在本发明另一实施例中，在步骤 S203 之后，该方法还包括下述步骤：

在步骤 S204 中，被盗移动终端通知机主非法使用者的相关信息已回传至接收终端。

为了使机主可以自由的对被盗移动终端进行控制，图 3 示出了本发明另一实施例提供的移动终端防盗方法的实现流程，其与图 2 所示的被盗移动终端防盗方法的不同指出仅在于采用步骤 S301 替换步骤 S201，其余步骤类似，详述如下：

在步骤 S301 中，当移动终端处于被盗模式时，判断是否接收到记录非法使用者的相关信息的指令，如果是，则执行步骤 S302，如果不是，则移动终端被盗方法结束，不再执行以下步骤。

在步骤 S302 中，记录非法使用者的相关信息。其具体过程如上所述，在此不再赘述。

在步骤 S303 中，将记录的非法使用者的相关信息回传至预先指定的接收终端。其具体步骤如上所述，在此不再赘述。

为了在接收终端接收到被盗移动终端回传的非法使用者的相关信息时，及时快速的通知被盗移动终端机主，在本发明另一实施例中，在步骤 S303 之后，该方法还包括下述步骤：

在步骤 S304 中，被盗移动终端通知机主非法使用者的相关信息已回传至接收终端。

图 4 示出了本发明实施例提供的防盗移动终端的结构，为了便于说明，仅示出了与本发明实施例相关的部分。

被盗模式判断单元 41 判断移动终端当前是否处于被盗模式。在本发明实施例中，可以采用开机身份认证判断方式，或者指令触发判断方式等其他多种判断方式判断移动终端是否处于被盗模式。其中开机身份认证判断方式和指令触发方式的具体过程如上所述，在此不再赘述。

相关信息记录单元 42 在被盗模式判断单元 41 判定移动终端处于被盗模式时，记录非法使用者的相关信息。非法使用者的相关信息包括但不限于照片、录音、录像或通话记录中的一种或者多种组合。其中照片中包括非法使用者的头像、非法使用者所处环境等，录像中包括非法使用者的图像视频、非法使用者所处环境的图像视频等。

其中相关信息记录单元42包括相关信息采集单元421和相关信息存储单元422。相关信息采集单元 421 按照预设的采集方式采集非法使用者的相关信息。其中预设的采集方式可以是采集一次单帧图像、在预设的时间间隔内采集一次单帧图像、采集预设时间长度的视频、在预设的时间间隔内采集一次预设长度的视频或者从头到尾采集。相关信息存储单元 422 存储相关信息采集单元 421 采集的非法使用者的相关信息。

相关信息回传单元 43 将相关信息记录单元 42 记录的非法使用者的相关信息回传至预设的接收终端。其具体过程如上所述，在此不再赘述。

为了在接收终端接收到被盗移动终端回传的非法使用者的相关信息时，及时快速的通知被盗移动终端机主，在本发明另一实施例中，该防盗移动终端还包括通知发送单元 44，该通知发送单元 44 向预设的报警接收端发送被盗移动终端已将非法使用者的相关信息回传至接收终端的通知，以使机主获知该信息，从而更好的追踪非法使用者。

为了使移动终端记录的非法使用者的相关信息更加有针对性，给追踪非法使用者提供更多有效的信息，在本发明另一实施例中，该防盗移动终端还包括视频电话使用判断单元 45，该视频电话使用判断单元 45 在被盗模式判断单元 41 判定移动终端处于被盗模式时，判断非法使用者是否使用视频电话，如果是，则相关信息记录单元 42 记录非法使用者的相关信息，如果否，则相关信息记录单元 42 不记录。

为了使机主可以自由的对被盗移动终端进行控制，在本发明另一实施例中，该防盗移动终端还包括指令接收判断单元 46，该指令接收判断单元 46 在被盗

模式判断单元 41 判定移动终端处于被盗模式时，判断是否接收到记录非法使用者的相关信息的指令，如果是，则相关信息记录单元 42 记录非法使用者的相关信息，如果否，则相关信息记录单元 42 不记录。

在本发明实施例中，当移动终端处于被盗模式时，记录非法使用者的相关信息，并将非法使用者的相关信息回传至预设的接收终端，从而为追踪非法使用者提供了较为有效的线索。同时移动终端向预设的报警接收端发送已将非法使用者的相关信息回传至预设的接收终端的通知，从而使机主可以及时、快速的获取非法使用者的相关信息，给追踪非法使用者赢得了时间。当移动终端处于被盗模式时，如果非法使用者使用移动终端的视频电话，则记录非法使用者的相关信息，从而可以准确的记录非法使用者的头像等较为有效的信息，从而进一步为追踪非法使用者提供了方便。当移动终端处于被盗模式时，机主可以通过向移动终端发送记录非法使用者的相关信息的指令，从而使机主可以自由的控制移动终端记录非法使用者的时间，从而给机主带来方便。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

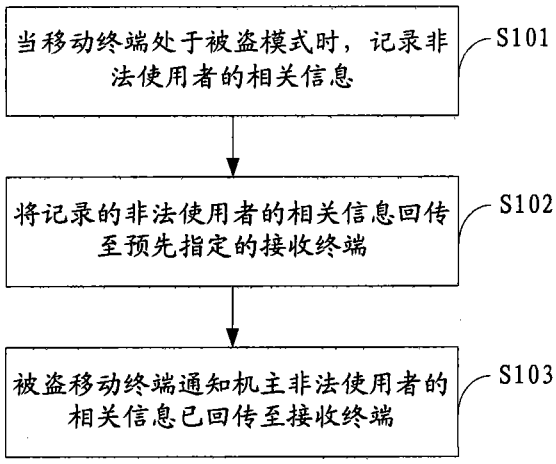

当移动终端处于被盗模式时，记录非法使用者的相关信息
S101
将记录的非法使用者的相关信息回传至预先指定的接收终端
S102
被盗移动终端通知机主非法使用者的相关信息已回传至接收终端
S103

图 1

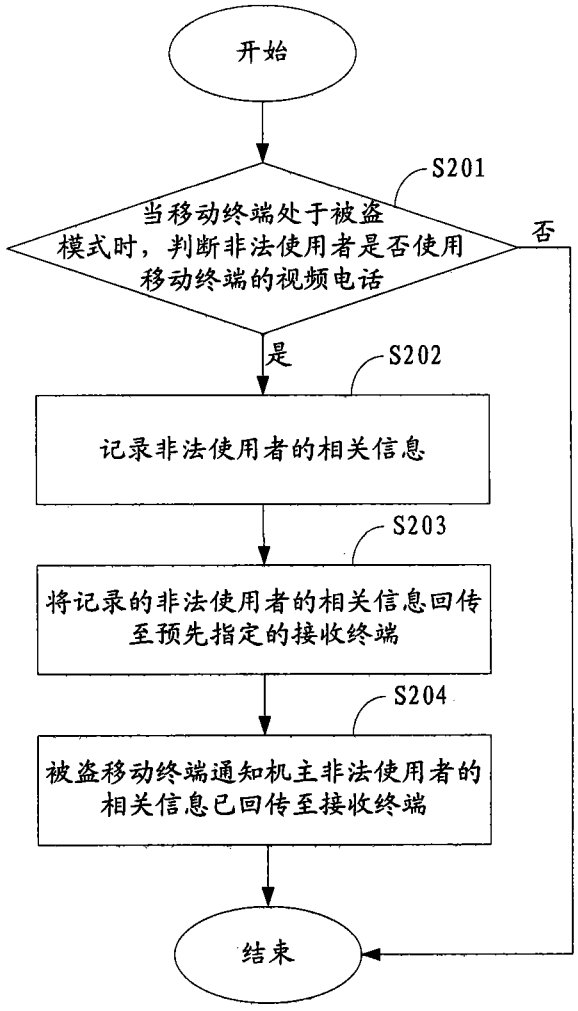

开始
S201
当移动终端处于被盗模式时，判断非法使用者是否使用移动终端的视频电话
否
是
S202
记录非法使用者的相关信息
S203
将记录的非法使用者的相关信息回传至预先指定的接收终端
S204
被盗移动终端通知机主非法使用者的相关信息已回传至接收终端
结束

图 2

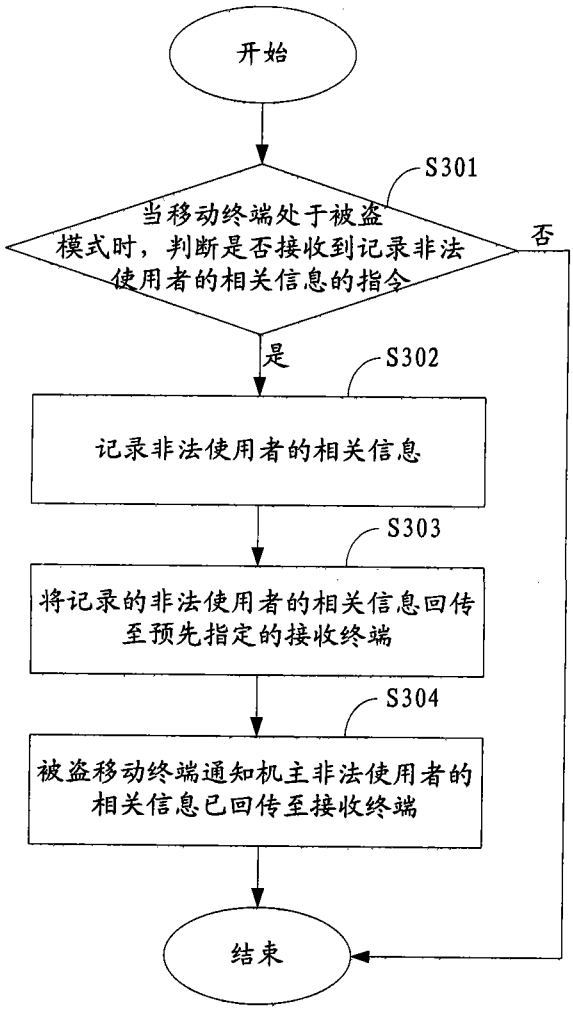

开始
S301
当移动终端处于被盗模式时，判断是否接收到记录非法使用者的相关信息的指令
否
是
S302
记录非法使用者的相关信息
S303
将记录的非法使用者的相关信息回传至预先指定的接收终端
S304
被盗移动终端通知机主非法使用者的相关信息已回传至接收终端
结束

图 3

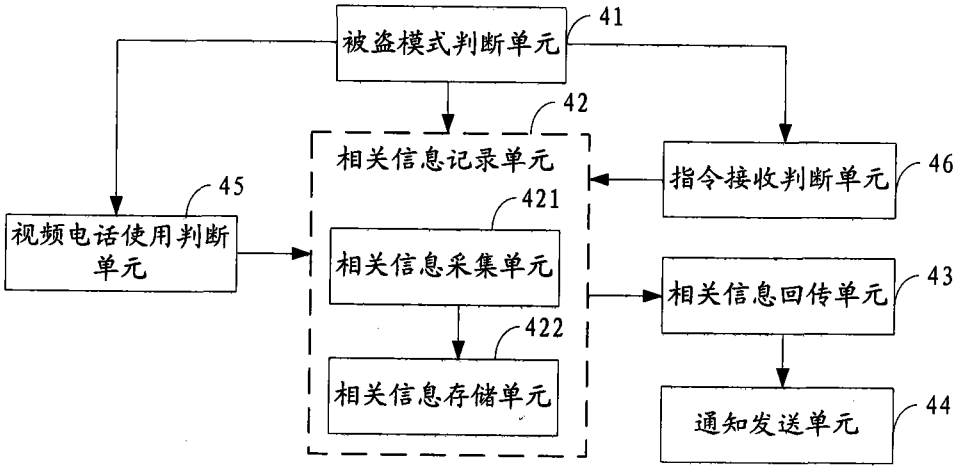

被盗模式判断单元
41
42
相关信息记录单元
421
相关信息采集单元
422
相关信息存储单元
45
视频电话使用判断单元
指令接收判断单元
46
相关信息回传单元
43
通知发送单元
44

图 4