(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 104113626 A
(43)申请公布日 2014.10.22

(21)申请号 201410300178.8

(22)申请日 2014.06.26

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 谭少卿

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 兰淑铎

(51)Int.Cl.
H04M 1/663(2006.01)
H04L 29/06(2006.01)

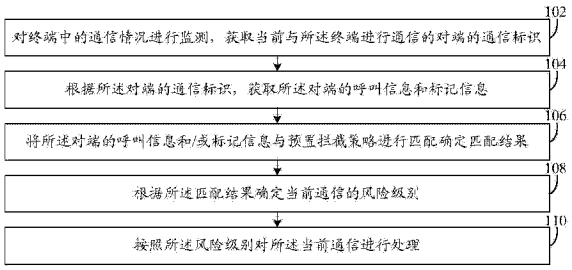
权利要求书2页 说明书17页 附图3页

(54)发明名称

一种通信处理方法和系统

(57)摘要

本发明公开了一种通信处理方法和系统，其中，所述方法包括：对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识；根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息；将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果；根据所述匹配结果确定当前通信的风险级别；按照所述风险级别对所述当前通信进行处理。通过本发明解决了安全类软件对陌生通话号码的处理完全依赖于用户的标记结果，由于标记结果不准确而导致的对陌生通话号码处理不准确的问题。



CN 104113626 A

1. 一种通信处理方法，其特征在于，包括：

对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识；

根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息；

将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果；

根据所述匹配结果确定当前通信的风险级别；

按照所述风险级别对所述当前通信进行处理。

2. 如权利要求 1 所述的方法，其特征在于，

所述呼叫信息包括：所述对端的呼出和呼入的次数，所述对端呼出和呼入时的通话时长，所述对端呼出和呼入时的响铃时长，所述对端进行通话时的时间分布信息，所述对端发送和接收短信的次数，所述对端的通信标识被添加至联系人和被添加至黑名单的次数中的至少一种；

所述标记信息包括：所述对端的通信标识被标记为恶意和/或垃圾来电的次数，所述对端的通信标识在确定为恶意和/或垃圾网址的页面上出现的次数，使用所述对端的通信标识发送的短信被标记为恶意和/或垃圾短信的次数中的至少一种。

3. 如权利要求 2 所述的方法，其特征在于，所述将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

若所述对端的呼出次数和呼入次数之比大于第一设定值时，确定所述当前通信与预置拦截策略匹配；和/或，

若所述对端发送短信的次数和接收短信的次数之比大于第二设定值时，确定所述当前通信与预置拦截策略匹配；和/或，

若所述对端的通话操作次数和短信操作次数之比大于第三设定值时，确定所述当前通信与预置拦截策略匹配；其中，所述通话操作次数包括所述对端的呼出和/或呼入的次数；所述短信操作次数包括所述对端发送和/或接收短信的次数。

4. 如权利要求 2 所述的方法，其特征在于，所述将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

若所述对端的通信标识被添加至联系人的次数小于第四设定值时，确定所述当前通信与预置拦截策略匹配；和/或，

若所述对端的通信标识被添加至黑名单的次数大于第五设定值时，确定所述当前通信与预置拦截策略匹配。

5. 如权利要求 2 所述的方法，其特征在于，所述将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

若所述对端呼出时的通话时长小于第一设定时长的次数大于第六设定值时，确定所述当前通信与预置拦截策略匹配；和/或，

若所述对端呼入时的通话时长小于第二设定时长的次数大于第七设定值时，确定所述当前通信与预置拦截策略匹配；和/或，

若所述对端呼出时的响铃时长小于第三设定时长的次数大于第八设定值时，确定所述当前通信与预置拦截策略匹配；和/或，

若所述对端呼入时的响铃时长小于第四设定时长的次数大于第九设定值时，确定所述当前通信与预置拦截策略匹配；和/或，

若所述对端进行通话时的时间分布满足设定时间分布时，确定所述当前通信与预置拦截策略匹配。

6. 如权利要求 2 所述的方法，其特征在于，所述将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

若所述对端的通信标识被标记为恶意和 / 或垃圾来电的次数大于第十设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

若所述对端的通信标识在确定为恶意和 / 或垃圾网址的页面上出现的次数大于第十一设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

若使用所述对端的通信标识发送的短信被标记为恶意和 / 或垃圾短信的次数大于第十二设定值时，确定所述当前通信与预置拦截策略匹配。

7. 如权利要求 1-6 任一权利要求所述的方法，其特征在于，所述预置拦截策略包括多个子拦截策略；其中，每个子拦截策略分别与对应的呼叫信息和标记信息相匹配。

8. 如权利要求 7 所述的方法，其特征在于，所述将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

根据对端的呼叫信息和 / 或标记信息确定与所述当前通信相匹配的子拦截策略的数量。

9. 如权利要求 8 所述的方法，其特征在于，所述根据所述匹配结果确定当前通信的风险级别，包括：

根据与所述当前通信相匹配的子拦截策略的数量确定当前通信的风险级别；

其中，

当相匹配的子拦截策略的数量大于等于第一阈值时，确定所述当前通信是高危级别；

当相匹配的子拦截策略的数量大于等于第二阈值且小于第一阈值时，确定所述当前通信是风险级别；

当相匹配的子拦截策略的数量大于等于第三阈值且小于第二阈值时，确定所述当前通信是可疑级别；

当相匹配的子拦截策略的数量小于第三阈值时，确定所述当前通信是安全级别。

10. 一种通信处理系统，其特征在于，包括：

通信标识获取模块，用于对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识；

信息获取模块，用于根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息；

匹配模块，用于将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果；

风险确定模块，用于根据所述匹配结果确定当前通信的风险级别；

处理模块，用于按照所述风险级别对所述当前通信进行处理。

一种通信处理方法和系统

技术领域

[0001] 本发明涉及通信技术领域，具体涉及一种通信处理方法和系统。

背景技术

[0002] 用户在日常生活中，经常会接收到一些陌生通话号码的通话请求。由于通话号码是陌生的，因此，用户无法识别出该陌生通话号码的通话请求是正常的通话请求还是骚扰通话请求。用户只有在接通该通话请求后，根据对方传递的具体通话内容才可以判断出该通话请求是否是骚扰通话请求，判断过程被动，造成用户对非必要通话请求的接听，浪费通话时长。

[0003] 目前，一些安全类软件提供了陌生通话号码标记的功能，以手机上的安全类软件为例，具体标记流程如下：安全类软件在用户接通然后挂断陌生号码的通话来电之后弹出一个标记窗口，以使用户通过所述标记窗口对该陌生通话号码进行标记（如，将该陌生通话号码标记为骚扰电话、或广告推销电话、或房屋中介电话、或餐厅电话、或宾馆电话等）。然后，所述安全类软件根据用户的标记对陌生通话号码进行处理。

[0004] 然而，采用上述安全类软件提供的陌生通话号码标记功能对陌生通话号码的处理存在如下问题：

[0005] 所述安全类软件对陌生通话号码的处理完全依赖于用户的标记结果，然而，人为标记过程中往往存在较多误标记和标记不准确的情况，进而造成安全类软件对陌生通话号码的处理不准确的情况。如，当用户在不方便接听通话的时间接收到陌生通话号码的通话请求时，此时用户会认为该通话请求骚扰到自己了，故，用户在接通然后挂断陌生通话号码的通话来电之后，往往会直接将该陌生通话号码标记为骚扰通话，而不会去甄别该陌生通话号码具体是非骚扰电话还是骚扰电话，使得标记结果不准确。

[0006] 且，所述安全类软件总在用户接通然后挂断陌生通话号码来电之后弹出标记窗口，不但打扰用户，影响用户的使用体验，而且也增加了终端系统的操作和处理负担。

发明内容

[0007] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的一种通信处理方法和相应的一种通信处理系统。

[0008] 依据本发明的一个方面，提供了一种通信处理方法，包括：

[0009] 对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识；

[0010] 根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息；

[0011] 将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果；

[0012] 根据所述匹配结果确定当前通信的风险级别；

[0013] 按照所述风险级别对所述当前通信进行处理。

[0014] 根据本发明的另一方面，提供了一种通信处理系统，包括：

[0015] 通信标识获取模块，用于对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识；

[0016] 信息获取模块，用于根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息；

[0017] 匹配模块，用于将所述对端的呼叫信息和／或标记信息与预置拦截策略进行匹配确定匹配结果；

[0018] 风险确定模块，用于根据所述匹配结果确定当前通信的风险级别；

[0019] 处理模块，用于按照所述风险级别对所述当前通信进行处理。

[0020] 本发明提供的一种通信处理方法和系统，通过获取与所述终端进行通信的对端的通信标识，并根据所述通信标识进一步获取所述对端的呼叫信息和标记信息，然后将所述终端的呼叫信息和／或标记信息与预置拦截策略进行匹配确定匹配结果，最后根据所述匹配结果确定当前通信的风险级别，按照所述风险级别对所述当前通信进行处理。本发明对当前通信的判断依赖于所述对端的呼叫信息和／或标记信息，而非依赖于用户人为的对陌生通信标识的标记结果，提高了判断结果的准确性，进而保证了在对当前通信进行处理时的准确度。且，减少了用户的参与度，从而既减轻了终端系统对需要用户参与的操作的处理，减轻了终端系统的操作和处理负担，又避免了对用户的骚扰，提升了用户体验。

[0021] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0022] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0023] 图 1 是本发明第一实施例中一种通信处理方法的流程图；

[0024] 图 2 是本发明第二实施例中一种通信处理方法的流程图；

[0025] 图 3 是本发明第三实施例中一种通信处理方法的流程图；

[0026] 图 4 是本发明第四实施例中一种通信处理系统的结构框图；

[0027] 图 5 是本发明第五实施例中一种通信处理系统的结构框图。

具体实施方式

[0028] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0029] 实施例一

[0030] 参照图 1，示出了本发明第一实施例中一种通信处理方法的流程图。在本实施例中，所述通信处理方法包括：

[0031] 步骤 102，对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的

通信标识。

[0032] 在本实施例中，通信包括但不仅限于：通过终端进行的电话通话、短信，和通过IM(Instant Messaging，即时通讯）软件进行的语音通话、即时消息。其中，常用的IM软件包括：QQ、MSN Messenger、飞信、Skype、新浪UC、Google Talk、阿里旺旺等。

[0033] 其中，对终端中的通信情况进行监测可以包括：监测接入的通信和监测呼出的通信。在当前通信是由终端侧发起时，则所述对端是接收方，所述终端是发送方；在当前通信是由对端侧发起时，则所述终端是接收发，所述对端是发送方。

[0034] 较佳地，当终端是手机终端时，且进行的通信是打电话/接听电话以及收发短信时，所述对端的通信标识可以是所述对端的手机号码。当终端是PC端(Personal Computer，个人计算机）或手机终端，且进行的通信是即时通信会话（如，QQ语音、QQ视频、微信等）时，所述对端的通信标识可以是对端对应的用户的即时通信号码（如，QQ号、微信号等）。

[0035] 步骤104，根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息。

[0036] 步骤106，将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果。

[0037] 步骤108，根据所述匹配结果确定当前通信的风险级别。

[0038] 步骤110，按照所述风险级别对所述当前通信进行处理。

[0039] 综上所述，本实施例所述的通信处理方法，通过获取与所述终端进行通信的对端的通信标识，并根据所述通信标识进一步获取所述对端的呼叫信息和标记信息，然后将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果，最后根据所述匹配结果确定当前通信的风险级别，按照所述风险级别对所述当前通信进行处理。本发明对当前通信的判断依赖于所述对端对应的呼叫信息和/或标记信息，而非依赖于用户人为的对陌生通信标识的标记结果，提高了判断结果的准确性，进而保证了在对当前通信进行处理时的准确度。且，减少了用户的参与度，从而既减轻了终端系统对需要用户参与的操作的处理，减轻了终端系统的操作和处理负担，又避免了对用户的骚扰，提升了用户体验。

[0040] 参照图2，示出了本发明第二实施例中一种通信处理方法的流程图。

[0041] 在本实施例中，可以通过移动终端（如，手机）来执行所述通信处理方法。具体地，

[0042] 用于执行所述通信处理方法的可以是终端的一个功能模块。例如，该功能模块设置于终端的操作系统或者终端的通话应用中，当终端中有来电接入时，通过该功能模块执行所述通信处理方法。

[0043] 或者，用于执行所述通信处理方法的可以是终端中的一个第三方应用或者是第三方应用中的一个功能模块。如：可以是终端中的安全应用（如，360手机安全卫士）中的一个功能模块。在所述第三方应用或第三方应用中的功能模块处于运行状态时，当终端中有来电接入时，可以通过该第三方应用或第三方应用中的该功能模块执行所述通信处理方法。

[0044] 在本实施例中，所述通信处理方法包括：

[0045] 步骤202，第三方应用对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识。

[0046] 步骤204，第三方应用根据所述对端的通信标识，获取所述对端的呼叫信息和标记

信息。

[0047] 较佳地，所述呼叫信息包括但不仅限于：所述对端的呼出和呼入的次数，所述对端呼出和呼入时的通话时长，所述对端呼出和呼入时的响铃时长，所述对端进行通话时的时间分布信息，所述对端发送和接收短信的次数，所述对端的通信标识被添加至联系人和被添加至黑名单的次数中的至少一种。

[0048] 如，在当前通信是使用手机进行的通话时，所述对端的呼叫信息可以包括：所述对端的呼出和呼入的次数，所述对端呼出和呼入时的通话时长，所述对端呼出和呼入时的响铃时长，所述对端进行通话时的时间分布信息，所述对端发送和接收短信的次数，所述对端的通信标识被添加至联系人和被添加至黑名单的次数等全部信息。而在当前通信是使用手机进行的 QQ 语音通话时，所述对端的呼叫信息则可以是所述对端的呼出和呼入的次数，所述对端呼出和呼入时的通话时长，所述对端呼出和呼入时的响铃时长和所述对端进行通话时的时间分布信息等部分信息。所述呼叫信息具体包含的信息内容可以根据实际通信情况确定，本实施例对此不作限制。

[0049] 所述标记信息包括但不仅限于：所述当前来电被标记为恶意和 / 或垃圾来电的次数，所述当前来电在确定为恶意和 / 或垃圾网址的页面上出现的次数，使用所述当前来电的通话号码发送的短信被标记为恶意和 / 或垃圾短信的次数中的至少一种。与前述呼叫信息相似，所述标记信息具体包含的信息内容可以根据实际通信情况确定，本实施例对此不作限制。

[0050] 这里需要说明的是，在本实施例中，当所述通话是通过 IM 软件进行的语音通话时，所述呼叫信息和所述标记信息中的短信可以理解为，通过 IM 软件采用文字进行交互的文本信息。

[0051] 步骤 206，第三方应用对所述呼叫信息和标记信息进行去隐私处理。

[0052] 步骤 208，第三方应用将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果。

[0053] 较佳地，所述步骤 208 具体可以包括：

[0054] S2002、若所述终端的呼出次数和呼入次数之比大于第一设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和 / 或，

[0055] S2004、若所述对端发送短信的次数和接收短信的次数之比大于第二设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和 / 或，

[0056] S2006、若所述对端的通话操作次数和短信操作次数之比大于第三设定值时，第三方应用确定所述当前通信与预置拦截策略匹配。其中，所述通话操作次数包括所述对端的呼出和 / 或呼入的次数；所述短信操作次数包括所述对端发送和 / 或接收短信的次数；和 / 或，

[0057] S2008、若所述对端的通信标识被添加至联系人的次数小于第四设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和 / 或，

[0058] S2010、若所述对端的通信标识被添加至黑名单的次数大于第五设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和 / 或，

[0059] S2012、若所述对端呼出时的通话时长小于第一设定时长的次数大于第六设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和 / 或，

[0060] S2014、若所述对端呼入时的通话时长小于第二设定时长的次数大于第七设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和/或，

[0061] S2016、若所述对端呼出时的响铃时长小于第三设定时长的次数大于第八设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和/或，

[0062] S2018、若所述对端呼入时的响铃时长小于第四设定时长的次数大于第九设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和/或，

[0063] S2020、若所述对端进行通话时的时间分布满足设定时间分布时，第三方应用确定所述当前通信与预置拦截策略匹配；和/或，

[0064] S2022、若所述对端的通信标识被标记为恶意和/或垃圾来电的次数大于第十设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和/或，

[0065] S2024、若所述对端的通信标识在确定为恶意和/或垃圾网址的页面上出现的次数大于第十一设定值时，第三方应用确定所述当前通信与预置拦截策略匹配；和/或，

[0066] S2026、若使用所述对端的通信标识发送的短信被标记为恶意和/或垃圾短信的次数大于第十二设定值时，第三方应用确定所述当前通信与预置拦截策略匹配。

[0067] 这里需要说明的是，在本实施例中，可以根据实际通信情况，从上述步骤S2002-S2026选择对应的一个或多个步骤进行匹配判断。

[0068] 在本实施例中，所述预置拦截策略包括多个子拦截策略；其中，每个子拦截策略分别与对应的呼叫信息和标记信息相匹配。例如，与上述步骤S2002-S2026对应地，在本实施例中，所述预置拦截策略可以包括13个子拦截策略，所述13个子拦截策略与上述步骤S2002-S2026一一对应。

[0069] 较佳地，所述步骤208具体可以包括：根据对端的呼叫信息和/或标记信息确定与所述当前通信相匹配的子拦截策略的数量。如，可以根据上述步骤S2002-S2026确定所述13个子拦截策略中与所述当前通信相匹配的子拦截策略的数量。

[0070] 步骤210，第三方应用根据所述匹配结果确定当前通信的风险级别。

[0071] 在本实施例中，所述步骤210具体可以包括：

[0072] 当相匹配的子拦截策略的数量大于等于第一阈值时，第三方应用确定所述当前通信是高危级别。如，与所述当前通信相匹配的子拦截策略的数量大于等于10时，第三方应用确定所述当前通信是高危级别。

[0073] 当相匹配的子拦截策略的数量大于等于第二阈值且小于第一阈值时，第三方应用确定所述当前通信是风险级别。如，与所述当前通信相匹配的子拦截策略的数量大于等于6且小于10时，第三方应用确定所述当前通信是风险级别。

[0074] 当相匹配的子拦截策略的数量大于等于第三阈值且小于第二阈值时，第三方应用确定所述当前通信是可疑级别。如，与所述当前通信相匹配的子拦截策略的数量大于等于3且小于6时，第三方应用确定所述当前通信是可疑级别。

[0075] 当相匹配的子拦截策略的数量小于第三阈值时，第三方应用确定所述当前通信是安全级别。如，与所述当前通信相匹配的子拦截策略的数量小于3时，第三方应用确定所述当前通信是安全级别。

[0076] 步骤212，第三方应用按照所述风险级别对所述当前通信进行处理。

[0077] 由前所述可知，在本实施例中，所述当前通信的风险级别可以划分为：高危级别、

风险级别、可疑级别和安全级别。这里需要说明的是，当前通信的风险级别可以根据实际情况设置多个级别，包括但不仅限于：高危级别、风险级别、可疑级别和安全级别。

[0078] 较佳地，

[0079] 当所述当前通信是高危级别时，第三方应用对所述当前通信进行风险提示并直接拦截所述当前通信。

[0080] 当所述当前通信是风险级别或可疑级别时，对所述当前通信进行风险提示。

[0081] 当所述当前通信是安全级别时，保持所述当前通信的通话状态。

[0082] 在本实施例中，第三方应用按照所述风险级别对所述当前通信进行处理时的具体处理方式可以是：

[0083] 通过语音播报对所述当前通信进行风险提示；和/或，在终端的拨号盘侧加载风险提示信息并高亮显示。

[0084] 在本实施例中，当所述步骤 210 执行完成之后，还可以执行步骤 214。

[0085] 步骤 214，第三方应用按照所述风险级别对所述当前通信进行风险标识，并保存所述当前通信的通信标识和风险标识。

[0086] 在本实施例中，由于第三方应用按照所述风险级别对所述当前通信进行风险标识，故，所述风险标识可以用来指示判断所述当前通信对应的风险级别。

[0087] 较佳地，当呼出通话的通信标识与保存的通信标识相匹配时，第三方应用可以根据所述风险标识对所述呼出通话进行处理，如进行风险提示。当呼入通话的通信标识与保存的通信标识相匹配时，第三方应用可以根据所述风险标识对所述呼入通话进行处理，如风险提示或拦截等。

[0088] 综上所述，本实施例所述的通信处理方法，通过获取与所述终端进行通信的对端的通信标识，并根据所述通信标识进一步获取所述对端的呼叫信息和标记信息，然后将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果，最后根据所述匹配结果确定当前通信的风险级别，按照所述风险级别对所述当前通信进行处理。本发明对当前通信的判断依赖于所述对端的呼叫信息和/或标记信息，而非依赖于用户人为的对陌生通信标识的标记结果，提高了判断结果的准确性，进而保证了在对当前通信进行处理时的准确度。且，减少了用户的参与度，，从而既减轻了终端系统对需要用户参与的操作的处理，减轻了终端系统的操作和处理负担，又避免了对用户的骚扰，提升了用户体验。

[0089] 进一步地，所述预置拦截策略包括多个子拦截策略，多个子拦截策略分别与所述对端的呼叫信息和/或标记信息一一对应，根据多个子拦截策略的匹配情况综合判断当前通信的风险级别，而非依靠单一参数进行判断，提高了判断结果的准确度和详尽度，进而保证了对当前通信处理的准确度。

[0090] 实施例三

[0091] 结合上述实施例，下面通过一个具体实例对一种通信处理方法的流程进行说明。

[0092] 在本实施例中，所述通话是指通过手机进行通话，执行所述通信处理方法的可以是安装在手机侧的第三方应用（如，通讯录保镖）。参照图 3，示出了本发明第三实施例中一种通信处理方法的流程图。本实施例中，所述通信处理方法包括：

[0093] 步骤 302，通讯录保镖对手机中的来电情况进行监测，获取当前来电的电话号码。

[0094] 步骤 304，通讯录保镖根据所述当前来电的电话号码，获取所述当前来电的呼叫信

息和标记信息。

[0095] 较佳地，所述呼叫信息包括：所述当前来电呼出和呼入的次数，所述当前来电呼出和呼入时的通话时长，所述当前来电呼出和呼入时的响铃时长，所述当前来电进行通话时的时间分布信息，所述当前来电发送和接收短信的次数，所述当前来电的电话号码被添加至联系人和被添加至黑名单的次数中的至少一种。

[0096] 所述标记信息包括但：所述当前来电被标记为恶意和/或垃圾来电的次数，所述当前来电在确定为恶意和/或垃圾网址的页面上出现的次数，使用所述当前来电的电话号码发送的短信被标记为恶意和/或垃圾短信的次数中的至少一种。

[0097] 步骤306，通讯录保镖对所述呼叫信息和标记信息进行去隐私处理。

[0098] 在本实施例中，所述去隐私处理可以是指：删除/隐藏呼叫信息和标记信息中涉及到用户隐私的信息。例如：将呼叫信息和标记信息中指示当前来电的用户的姓名、性别和头像信息的信息删除/隐藏。

[0099] 步骤308，通讯录保镖将所述当前来电的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果。

[0100] 在本实施例中，所述预置拦截策略包括多个子拦截策略。其中，每个子拦截策略具体可以是：

[0101] 子拦截策略1：若所述当前来电的呼出次数和呼入次数之比大于第一设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0102] 子拦截策略2：若所述当前来电发送短信的次数和接收短信的次数之比大于第二设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0103] 子拦截策略3：若所述当前来电的通话操作次数和短信操作次数之比大于第三设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。其中，所述通话操作次数包括所述当前来电呼出和/或呼入的次数；所述短信操作次数包括所述当前来电发送和/或接收短信的次数。

[0104] 子拦截策略4：若所述当前来电的电话号码被添加至联系人的次数小于第四设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0105] 子拦截策略5：若所述当前来电的电话号码被添加至黑名单的次数大于第五设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0106] 子拦截策略6：若所述当前来电呼出时的通话时长小于第一设定时长的次数大于第六设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0107] 子拦截策略7：若所述当前来电呼入时的通话时长小于第二设定时长的次数大于第七设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0108] 子拦截策略8：若所述当前来电呼出时的响铃时长小于第三设定时长的次数大于第八设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0109] 子拦截策略9：若所述当前来电呼入时的响铃时长小于第四设定时长的次数大于第九设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0110] 子拦截策略10：若所述当前来电进行通话时的时间分布满足设定时间分布时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0111] 子拦截策略11：若所述当前来电被标记为恶意和/或垃圾来电的次数大于第十设

定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0112] 子拦截策略 12：若所述当前来电在确定为恶意和 / 或垃圾网址的页面上出现的次数大于第十一设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0113] 子拦截策略 13：若使用所述当前来电的电话号码发送的短信被标记为恶意和 / 或垃圾短信的次数大于第十二设定值时，通讯录保镖确定所述当前来电与预置拦截策略匹配。

[0114] 如，在本实施例中，通讯录保镖分别获取到来电电话号码 A、B、C、D；且分别获取了电话号码 A、B、C、D 对应的呼叫信息和标记信息。通讯录保镖根据电话号码 A、B、C、D 对应的呼叫信息和标记信息确定了：

[0115] 电话号码 A 同时满足子拦截策略 1-11；电话号码 B 同时满足子拦截策略 1-8；电话号码 C 同时满足子拦截策略 1-4；电话号码 D 只满足子拦截策略 1。

[0116] 步骤 310，通讯录保镖根据所述匹配结果确定当前来电的风险级别。

[0117] 在本实施例中，通讯录保镖根据电话号码 A、B、C、D 各自对应满足的子拦截策略的数量，确定：

[0118] 电话号码 A 的风险级别是高危级别；

[0119] 电话号码 B 的风险级别是风险级别；

[0120] 电话号码 C 的风险级别是可疑级别；

[0121] 电话号码 D 的风险级别是安全级别。

[0122] 步骤 312，通讯录保镖按照所述风险级别对所述当前来电进行处理。

[0123] 在本实施例中，通讯录保镖对电话号码 A 的来电进行风险提示并直接拦截。所述风险提示可以是以语音播报形式进行的，也可以是以在拨号盘页面加载并高亮显示风险提示的文字信息的形式进行的。

[0124] 通讯录保镖对电话号码 B 和 C 的来电进行风险提示。用户可以根据风险提示进行相应地操作，如，接通该通话，或挂断该通话。

[0125] 通讯录保镖保持电话号码 D 的来电的通话状态。

[0126] 综上所述，本实施例所述的通信处理方法，通过获取所述当前来电的呼叫信息和标记信息，然后将所述当前来电的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，最后根据所述匹配结果确定当前来电的风险级别，按照所述风险级别对所述当前来电进行处理。本发明对当前来电的判断依赖于当前来电的呼叫信息和 / 或标记信息，而非依赖于用户人为的对陌生通话号码的标记结果，提高了判断结果的准确性，进而保证了在对当前来电进行处理时的准确度。且，减少了用户的参与度，从而既减轻了终端系统对需要用户参与的操作的处理，减轻了终端系统的操作和处理负担，又避免了对用户的骚扰，提升了用户体验。

[0127] 进一步地，所述预置拦截策略包括多个子拦截策略，多个子拦截策略分别与所述当前来电的呼叫信息和 / 或标记信息一一对应，根据多个子拦截策略的匹配情况综合判断当前来电的风险级别，而非依靠单一参数进行判断，提高了判断结果的准确度和详尽度，进而保证了对当前来电处理的准确度。

[0128] 需要说明的是，对于前述的方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依

据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本发明所必需的。

[0129] 实施例四

[0130] 基于与上述方法实施例同一发明构思。参照图4，示出了本发明第四实施例中一种通信处理系统的结构框图。在本实施例中，所述通信处理系统包括：

[0131] 通信标识获取模块402，用于对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识。

[0132] 信息获取模块404，用于根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息。

[0133] 匹配模块406，用于将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果。

[0134] 风险确定模块408，用于根据所述匹配结果确定当前通信的风险级别。

[0135] 处理模块410，用于按照所述风险级别对所述当前通信进行处理。

[0136] 综上所述，本实施例所述的通信处理系统，通过获取与所述终端进行通信的对端的通信标识，并根据所述通信标识进一步获取所述对端的呼叫信息和标记信息，然后将所述终端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果，最后根据所述匹配结果确定当前通信的风险级别，按照所述风险级别对所述当前通信进行处理。本发明对当前通信的判断依赖于所述对端的呼叫信息和/或标记信息，而非依赖于用户人为的对陌生通信标识的标记结果，提高了判断结果的准确性，进而保证了在对当前通信进行处理时的准确度。且，减少了用户的参与度，，从而既减轻了终端系统对需要用户参与的操作的处理，减轻了终端系统的操作和处理负担，又避免了对用户的骚扰，提升了用户体验。

[0137] 参照图5，示出了本发明第五实施例中一种通信处理系统的结构框图。在本实施例中，所述通信处理系统包括：

[0138] 通信标识获取模块502，用于对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识。

[0139] 信息获取模块504，用于根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息。

[0140] 其中，

[0141] 所述呼叫信息包括：所述对端的呼出和呼入的次数，所述对端呼出和呼入时的通话时长，所述对端呼出和呼入时的响铃时长，所述对端进行通话时的时间分布信息，所述对端发送和接收短信的次数，所述对端的通信标识被添加至联系人和被添加至黑名单的次数中的至少一种。

[0142] 所述标记信息包括：所述对端的通信标识被标记为恶意和/或垃圾来电的次数，所述对端的通信标识在确定为恶意和/或垃圾网址的页面上出现的次数，使用所述对端的通信标识发送的短信被标记为恶意和/或垃圾短信的次数中的至少一种。

[0143] 隐私处理模块506，用于在所述信息获取模块504获取所述对端的呼叫信息和标记信息之后，对所述呼叫信息和标记信息进行去隐私处理。

[0144] 在本实施例中，所述去隐私处理可以是指：删除/隐藏呼叫信息和标记信息中涉及到用户隐私的信息。例如：将呼叫信息和标记信息中指示当前来电的用户的姓名、性别和

头像信息的信息删除 / 隐藏。

[0145] 匹配模块 508，用于将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果。

[0146] 在本实施例中，所述匹配模块 508 具体可以包括 ：

[0147] 第一匹配模块，用于在所述对端的呼出次数和呼入次数之比大于第一设定值时，确定所述当前通信与预置拦截策略匹配。

[0148] 第二匹配模块，用于在所述对端发送短信的次数和接收短信的次数之比大于第二设定值时，确定所述当前通信与预置拦截策略匹配。

[0149] 第三匹配模块，用于在所述对端的通话操作次数和短信操作次数之比大于第三设定值时，确定所述当前通信与预置拦截策略匹配。

[0150] 其中，所述通话操作次数包括所述对端呼出和 / 或呼入的次数 ；所述短信操作次数包括所述对端发送和 / 或接收短信的次数。

[0151] 第四匹配模块，用于在所述对端的通信标识被添加至联系人的次数小于第四设定值时，确定所述当前通信与预置拦截策略匹配。

[0152] 第五匹配模块，用于在所述对端的通信标识被添加至黑名单的次数大于第五设定值时，确定所述当前通信与预置拦截策略匹配。

[0153] 第六匹配模块，用于在所述对端呼出时的通话时长小于第一设定时长的次数大于第六设定值时，确定所述当前通信与预置拦截策略匹配。

[0154] 第七匹配模块，用于在所述对端呼入时的通话时长小于第二设定时长的次数大于第七设定值时，确定所述当前通信与预置拦截策略匹配。

[0155] 第八匹配模块，用于在所述对端呼出时的响铃时长小于第三设定时长的次数大于第八设定值时，确定所述当前通信与预置拦截策略匹配。

[0156] 第九匹配模块，用于在所述对端呼入时的响铃时长小于第四设定时长的次数大于第九设定值时，确定所述当前通信与预置拦截策略匹配。

[0157] 第十匹配模块，用于在所述对端进行通话时的时间分布满足设定时间分布时，确定所述当前通信与预置拦截策略匹配。

[0158] 第十一匹配模块，用于在所述对端的通信标识被标记为恶意和 / 或垃圾来电的次数大于第十设定值时，确定所述当前通信与预置拦截策略匹配。

[0159] 第十二匹配模块，用于在所述对端的通信标识在确定为恶意和 / 或垃圾网址的页面上出现的次数大于第十一设定值时，确定所述当前通信与预置拦截策略匹配。

[0160] 第十三匹配模块，用于在使用所述对端的通信标识发送的短信被标记为恶意和 / 或垃圾短信的次数大于第十二设定值时，确定所述当前通信与预置拦截策略匹配。

[0161] 较佳地，在本实施例中，所述预置拦截策略包括多个子拦截策略。其中，每个子拦截策略分别与对应的呼叫信息和标记信息相匹配。即，可以认为每个子拦截策略分别与上述第一至第十三匹配模块相对应。

[0162] 在本实施例中，所述匹配模块 508 在将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果时，具体可以包括 ：

[0163] 根据对端的呼叫信息和 / 或标记信息确定与所述当前通信相匹配的子拦截策略的数量。

[0164] 风险确定模块 510，用于根据所述匹配结果确定当前通信的风险级别。

[0165] 较佳地，所述风险确定模块 510，具体用于根据与所述当前通信相匹配的子拦截策略的数量确定当前通信的风险级别。

[0166] 其中，

[0167] 在相匹配的子拦截策略的数量大于等于第一阈值时，确定所述当前通信是高危级别。

[0168] 在相匹配的子拦截策略的数量大于等于第二阈值且小于第一阈值时，确定所述当前通信是风险级别。

[0169] 在相匹配的子拦截策略的数量大于等于第三阈值且小于第二阈值时，确定所述当前通信是可疑级别。

[0170] 在相匹配的子拦截策略的数量小于第三阈值时，确定所述当前通信是安全级别。

[0171] 处理模块 512，用于按照所述风险级别对所述当前通信进行处理。

[0172] 在本实施例中，所述处理模块 512 可以包括 ：

[0173] 第一处理模块，用于在所述当前通信是高危级别时，对所述当前通信进行风险提示并直接拦截所述当前通信。

[0174] 第二处理模块，用于在所述当前通信是风险级别或可疑级别时，对所述当前通信进行风险提示。

[0175] 第三处理模块，用于在所述当前通信是安全级别时，保持所述当前通信的通信状态。

[0176] 较佳地，所述处理模块 512 在对所述当前通信进行处理时，具体可以包括 ：通过语音播报对所述当前通信进行风险提示 ；和 / 或，在终端的拨号盘侧加载风险提示信息并高亮显示。

[0177] 保存模块 514，用于在所述风险确定模块 510 根据所述匹配结果确定当前通信的风险级别之后，按照所述风险级别对所述当前通信进行风险标识，并保存所述当前通信的通信标识和风险标识。

[0178] 第四处理模块 516，用于在呼出通话的通信标识与保存的通信标识相匹配时，根据所述风险标识对所述呼出通话进行处理。

[0179] 第五处理模块 518，用于在呼入通话的通信标识与保存的通信标识相匹配时，根据所述风险标识对所述呼入通话进行处理。

[0180] 综上所述，本实施例所述的通信处理系统，通过获取与所述终端进行通信的对端的通信标识，并根据所述通信标识进一步获取所述对端的呼叫信息和标记信息，然后将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，最后根据所述匹配结果确定当前通信的风险级别，按照所述风险级别对所述当前通信进行处理。本发明对当前通信的判断依赖于所述对端的呼叫信息和 / 或标记信息，而非依赖于用户人为的对陌生通信标识的标记结果，提高了判断结果的准确性，进而保证了在对当前通信进行处理时的准确度。且，减少了用户的参与度，从而既减轻了终端系统对需要用户参与的操作的处理，减轻了终端系统的操作和处理负担，又避免了对用户的骚扰，提升了用户体验。

[0181] 进一步地，所述预置拦截策略包括多个子拦截策略，多个子拦截策略分别与所述对端的呼叫信息和 / 或标记信息一一对应，根据多个子拦截策略的匹配情况综合判断当前

通信的风险级别，而非依靠单一参数进行判断，提高了判断结果的准确度和详尽度，进而保证了对当前通信处理的准确度。

[0182] 对于上述装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0183] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0184] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0185] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0186] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0187] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0188] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的通信处理设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0189] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领

域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0190] 本发明公开了 A1、一种通信处理方法，包括：

[0191] 对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识；

[0192] 根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息；

[0193] 将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果；

[0194] 根据所述匹配结果确定当前通信的风险级别；

[0195] 按照所述风险级别对所述当前通信进行处理。

[0196] A、如 A1 所述的方法，

[0197] 所述呼叫信息包括：所述对端的呼出和呼入的次数，所述对端呼出和呼入时的通话时长，所述对端呼出和呼入时的响铃时长，所述对端进行通话时的时间分布信息，所述对端发送和接收短信的次数，所述对端的通信标识被添加至联系人和被添加至黑名单的次数中的至少一种；

[0198] 所述标记信息包括：所述对端的通信标识被标记为恶意和 / 或垃圾来电的次数，所述对端的通信标识在确定为恶意和 / 或垃圾网址的页面上出现的次数，使用所述对端的通信标识发送的短信被标记为恶意和 / 或垃圾短信的次数中的至少一种。

[0199] A3、如 A2 所述的方法，所述将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

[0200] 若所述对端的呼出次数和呼入次数之比大于第一设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0201] 若所述对端发送短信的次数和接收短信的次数之比大于第二设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0202] 若所述对端的通话操作次数和短信操作次数之比大于第三设定值时，确定所述当前通信与预置拦截策略匹配；其中，所述通话操作次数包括所述对端的呼出和 / 或呼入的次数；所述短信操作次数包括所述对端发送和 / 或接收短信的次数。

[0203] A4、如 A2 所述的方法，所述将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

[0204] 若所述对端的通信标识被添加至联系人的次数小于第四设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0205] 若所述对端的通信标识被添加至黑名单的次数大于第五设定值时，确定所述当前通信与预置拦截策略匹配。

[0206] A5、如 A2 所述的方法，所述将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

[0207] 若所述对端呼出时的通话时长小于第一设定时长的次数大于第六设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0208] 若所述对端呼入时的通话时长小于第二设定时长的次数大于第七设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0209] 若所述对端呼出时的响铃时长小于第三设定时长的次数大于第八设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0210] 若所述对端呼入时的响铃时长小于第四设定时长的次数大于第九设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0211] 若所述对端进行通话时的时间分布满足设定时间分布时，确定所述当前通信与预置拦截策略匹配。

[0212] A6、如 A2 所述的方法，所述将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

[0213] 若所述对端的通信标识被标记为恶意和 / 或垃圾来电的次数大于第十设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0214] 若所述对端的通信标识在确定为恶意和 / 或垃圾网址的页面上出现的次数大于第十一设定值时，确定所述当前通信与预置拦截策略匹配；和 / 或，

[0215] 若使用所述对端的通信标识发送的短信被标记为恶意和 / 或垃圾短信的次数大于第十二设定值时，确定所述当前通信与预置拦截策略匹配。

[0216] A7、如 A1-A6 任一所述的方法，所述预置拦截策略包括多个子拦截策略；其中，每个子拦截策略分别与对应的呼叫信息和标记信息相匹配。

[0217] A8、如 A7 所述的方法，所述将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果，包括：

[0218] 根据对端的呼叫信息和 / 或标记信息确定与所述当前通信相匹配的子拦截策略的数量。

[0219] A9、如 A8 所述的方法，所述根据所述匹配结果确定当前通信的风险级别，包括：

[0220] 根据与所述当前通信相匹配的子拦截策略的数量确定当前通信的风险级别；

[0221] 其中，

[0222] 当相匹配的子拦截策略的数量大于等于第一阈值时，确定所述当前通信是高危级别；

[0223] 当相匹配的子拦截策略的数量大于等于第二阈值且小于第一阈值时，确定所述当前通信是风险级别；

[0224] 当相匹配的子拦截策略的数量大于等于第三阈值且小于第二阈值时，确定所述当前通信是可疑级别；

[0225] 当相匹配的子拦截策略的数量小于第三阈值时，确定所述当前通信是安全级别。

[0226] A10、如 A9 所述的方法，所述按照所述风险级别对所述当前通信进行处理，包括：

[0227] 当所述当前通信是高危级别时，对所述当前通信进行风险提示并直接拦截所述当前通信；

[0228] 当所述当前通信是风险级别或可疑级别时，对所述当前通信进行风险提示；

[0229] 当所述当前通信是安全级别时，保持所述当前通信的通信状态。

[0230] A11、如 A1 所述的方法，所述对所述当前通信进行处理，包括：

[0231] 通过语音播报对所述当前通信进行风险提示；和 / 或，

[0232] 在终端的拨号盘侧加载风险提示信息并高亮显示。

[0233] A12、如 A1 所述的方法，在所述根据所述匹配结果确定当前通信的风险级别的步骤之后，所述方法还包括：

[0234] 按照所述风险级别对所述当前通信进行风险标识，并保存所述对端的通信标识和所述风险标识。

[0235] A13、如 A12 所述的方法，所述方法还包括：

[0236] 当呼出通话的通信标识与保存的通信标识相匹配时，根据对应的风险标识对所述呼出通话进行处理；

[0237] 当呼入通话的通信标识与保存的通信标识相匹配时，根据对应的风险标识对所述呼入通话进行处理。

[0238] A14、如 A1 所述的方法，在所述获取所述对端的呼叫信息和标记信息的步骤之后，所述方法还包括：

[0239] 对所述呼叫信息和标记信息进行去隐私处理。

[0240] 本发明还公开了 B15、一种通信处理系统，包括：

[0241] 通信标识获取模块，用于对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识；

[0242] 信息获取模块，用于根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息；

[0243] 匹配模块，用于将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果；

[0244] 风险确定模块，用于根据所述匹配结果确定当前通信的风险级别；

[0245] 处理模块，用于按照所述风险级别对所述当前通信进行处理。

[0246] B16、如 B15 所述的系统，

[0247] 所述呼叫信息包括：所述对端的呼出和呼入的次数，所述对端呼出和呼入时的通话时长，所述对端呼出和呼入时的响铃时长，所述对端进行通话时的时间分布信息，所述对端发送和接收短信的次数，所述对端的通信标识被添加至联系人和被添加至黑名单的次数中的至少一种；

[0248] 所述标记信息包括：所述对端的通信标识被标记为恶意和 / 或垃圾来电的次数，所述对端的通信标识在确定为恶意和 / 或垃圾网址的页面上出现的次数，使用所述对端的通信标识发送的短信被标记为恶意和 / 或垃圾短信的次数中的至少一种。

[0249] B17、如 B16 所述的系统，所述匹配模块，包括：

[0250] 第一匹配模块，用于在所述对端的呼出次数和呼入次数之比大于第一设定值时，确定所述当前通信与预置拦截策略匹配；

[0251] 第二匹配模块，用于在所述对端发送短信的次数和接收短信的次数之比大于第二设定值时，确定所述当前通信与预置拦截策略匹配；

[0252] 第三匹配模块，用于在所述对端的通话操作次数和短信操作次数之比大于第三设定值时，确定所述当前通信与预置拦截策略匹配；其中，所述通话操作次数包括所述对端呼

出和 / 或呼入的次数 ;所述短信操作次数包括所述对端发送和 / 或接收短信的次数。

[0253] B18、如 B16 所述的系统,所述匹配模块,包括 :

[0254] 第四匹配模块,用于在所述对端的通信标识被添加至联系人的次数小于第四设定值时,确定所述当前通信与预置拦截策略匹配 ;

[0255] 第五匹配模块,用于在所述对端的通信标识被添加至黑名单的次数大于第五设定值时,确定所述当前通信与预置拦截策略匹配。

[0256] B19、如 B16 所述的系统,所述匹配模块,包括 :

[0257] 第六匹配模块,用于在所述对端呼出时的通话时长小于第一设定时长的次数大于第六设定值时,确定所述当前通信与预置拦截策略匹配 ;

[0258] 第七匹配模块,用于在所述对端呼入时的通话时长小于第二设定时长的次数大于第七设定值时,确定所述当前通信与预置拦截策略匹配 ;

[0259] 第八匹配模块,用于在所述对端呼出时的响铃时长小于第三设定时长的次数大于第八设定值时,确定所述当前通信与预置拦截策略匹配 ;

[0260] 第九匹配模块,用于在所述对端呼入时的响铃时长小于第四设定时长的次数大于第九设定值时,确定所述当前通信与预置拦截策略匹配 ;

[0261] 第十匹配模块,用于在所述对端进行通话时的时间分布满足设定时间分布时,确定所述当前通信与预置拦截策略匹配。

[0262] B20、如 B16 所述的系统,所述匹配模块,包括 :

[0263] 第十一匹配模块,用于在所述对端的通信标识被标记为恶意和 / 或垃圾来电的次数大于第十设定值时,确定所述当前通信与预置拦截策略匹配 ;

[0264] 第十二匹配模块,用于在所述对端的通信标识在确定为恶意和 / 或垃圾网址的页面上出现的次数大于第十一设定值时,确定所述当前通信与预置拦截策略匹配 ;

[0265] 第十三匹配模块,用于在使用所述对端的通信标识发送的短信被标记为恶意和 / 或垃圾短信的次数大于第十二设定值时,确定所述当前通信与预置拦截策略匹配。

[0266] B21、如 B15-B20 任一所述的系统,所述预置拦截策略包括多个子拦截策略 ;其中,每个子拦截策略分别与对应的呼叫信息和标记信息相匹配。

[0267] B22、如 B21 所述系统,所述匹配模块在将所述对端的呼叫信息和 / 或标记信息与预置拦截策略进行匹配确定匹配结果时,具体包括 :

[0268] 根据对端的呼叫信息和 / 或标记信息确定与所述当前通信相匹配的子拦截策略的数量。

[0269] B23、如 B22 所述系统,

[0270] 所述风险确定模块,具体用于根据与所述当前通信相匹配的子拦截策略的数量确定当前通信的风险级别 ;

[0271] 其中,

[0272] 在相匹配的子拦截策略的数量大于等于第一阈值时,确定所述当前通信是高危级别 ;

[0273] 在相匹配的子拦截策略的数量大于等于第二阈值且小于第一阈值时,确定所述当前通信是风险级别 ;

[0274] 在相匹配的子拦截策略的数量大于等于第三阈值且小于第二阈值时,确定所述当

前通信是可疑级别；

[0275] 在相匹配的子拦截策略的数量小于第三阈值时，确定所述当前通信是安全级别。

[0276] B24、如 B23 所述的系统，所述处理模块，包括：

[0277] 第一处理模块，用于在所述当前通信是高危级别时，对所述当前通信进行风险提示并直接拦截所述当前通信；

[0278] 第二处理模块，用于在所述当前通信是风险级别或可疑级别时，对所述当前通信进行风险提示；

[0279] 第三处理模块，用于在所述当前通信是安全级别时，保持所述当前通信的通信状态。

[0280] B25、如 B15 所述的系统，所述处理模块在对所述当前通信进行处理时，具体包括：

[0281] 通过语音播报对所述当前通信进行风险提示；和 / 或，在终端的拨号盘侧加载风险提示信息并高亮显示。

[0282] B26、如 B15 所述的系统，所述系统还包括：

[0283] 保存模块，用于在所述风险确定模块根据所述匹配结果确定当前通信的风险级别之后，按照所述风险级别对所述当前通信进行风险标识，并保存所述对端的通信标识和所述风险标识。

[0284] B27、如 B26 所述的系统，所述系统还包括：

[0285] 第四处理模块，用于在呼出通话的通信标识与保存的通信标识相匹配时，根据对应风险标识对所述呼出通话进行处理；

[0286] 第五处理模块，用于在呼入通话的通信标识与保存的通信标识相匹配时，根据对应风险标识对所述呼入通话进行处理。

[0287] B28、如 B15 所述的系统，所述系统还包括：

[0288] 隐私处理模块，用于在所述信息获取模块获取所述对端的呼叫信息和标记信息之后，对所述呼叫信息和标记信息进行去隐私处理。

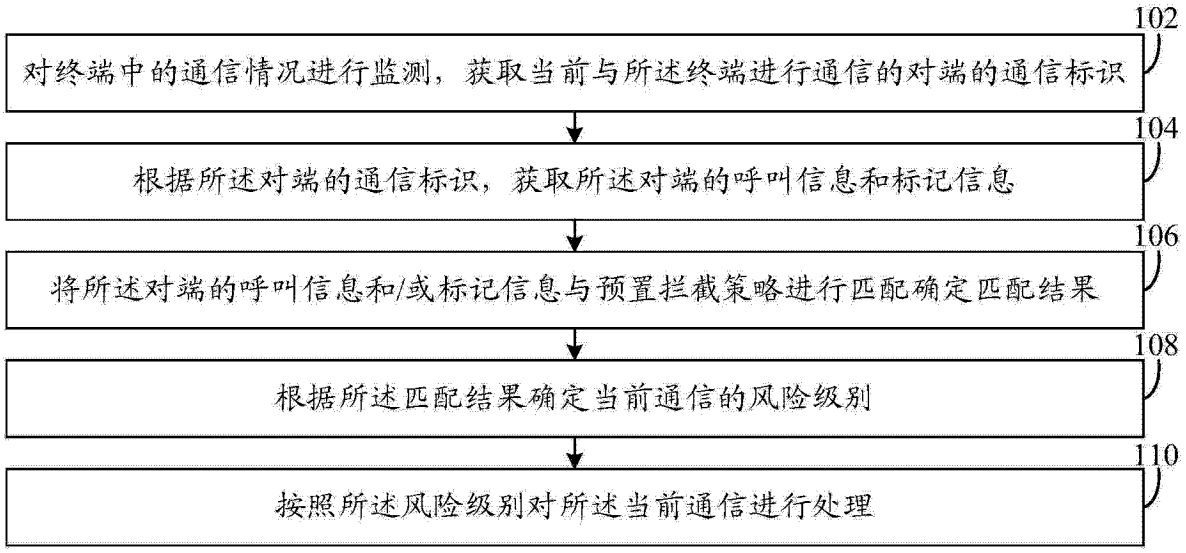

102
对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识
104
根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息
106
将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果
108
根据所述匹配结果确定当前通信的风险级别
110
按照所述风险级别对所述当前通信进行处理

图 1

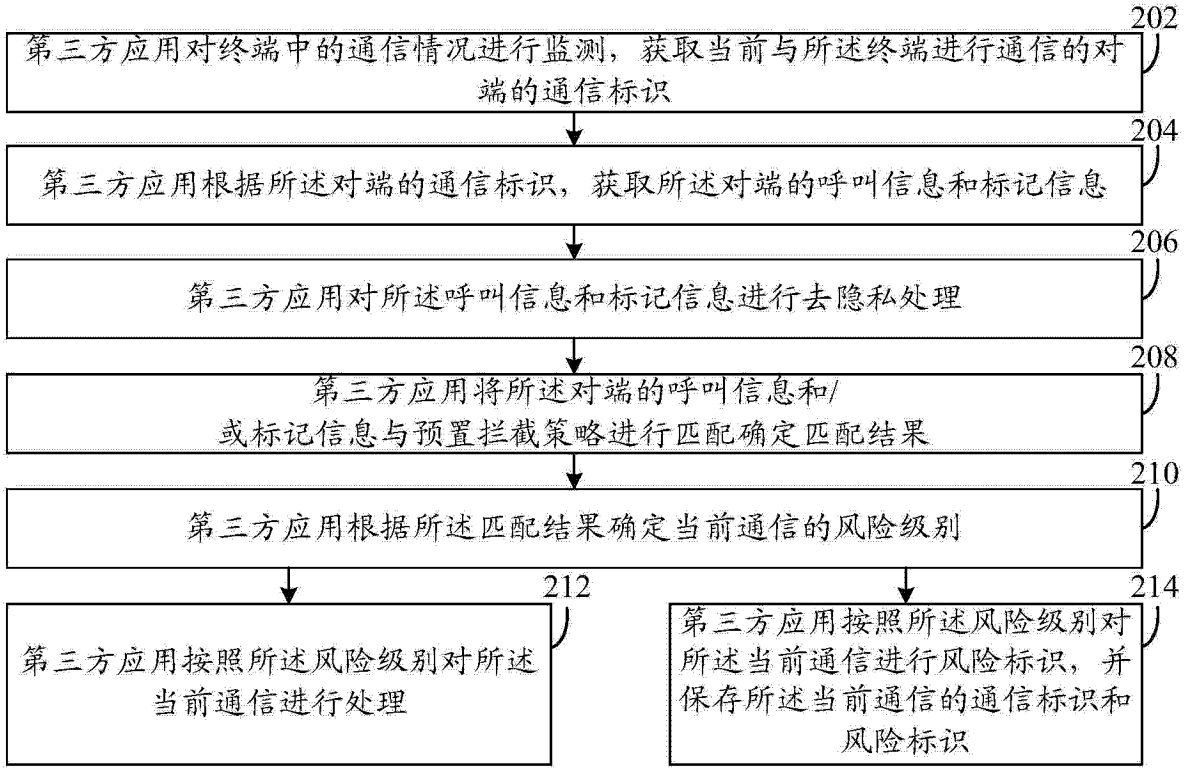

202
第三方应用对终端中的通信情况进行监测，获取当前与所述终端进行通信的对端的通信标识
204
第三方应用根据所述对端的通信标识，获取所述对端的呼叫信息和标记信息
206
第三方应用对所述呼叫信息和标记信息进行去隐私处理
208
第三方应用将所述对端的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果
210
第三方应用根据所述匹配结果确定当前通信的风险级别
212
第三方应用按照所述风险级别对所述当前通信进行处理
214
第三方应用按照所述风险级别对所述当前通信进行风险标识，并保存所述当前通信的通信标识和风险标识

图 2

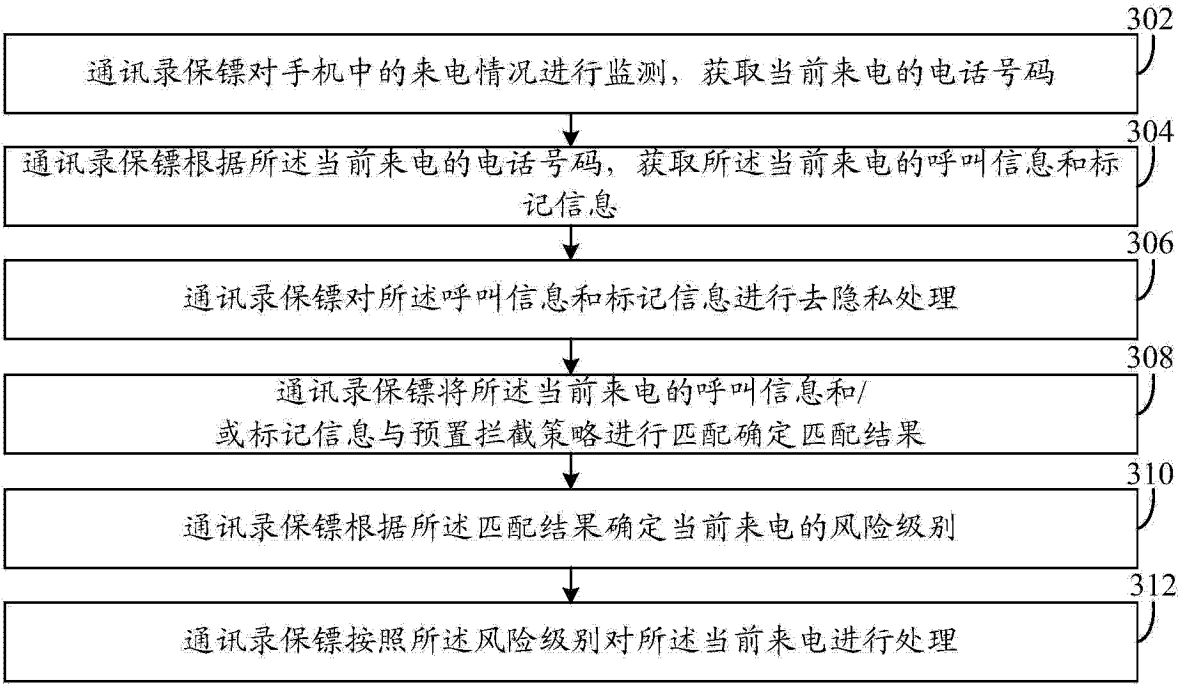

302
通讯录保镖对手机中的来电情况进行监测，获取当前来电的电话号码
304
通讯录保镖根据所述当前来电的电话号码，获取所述当前来电的呼叫信息和标记信息
306
通讯录保镖对所述呼叫信息和标记信息进行去隐私处理
308
通讯录保镖将所述当前来电的呼叫信息和/或标记信息与预置拦截策略进行匹配确定匹配结果
310
通讯录保镖根据所述匹配结果确定当前来电的风险级别
312
通讯录保镖按照所述风险级别对所述当前来电进行处理

图 3

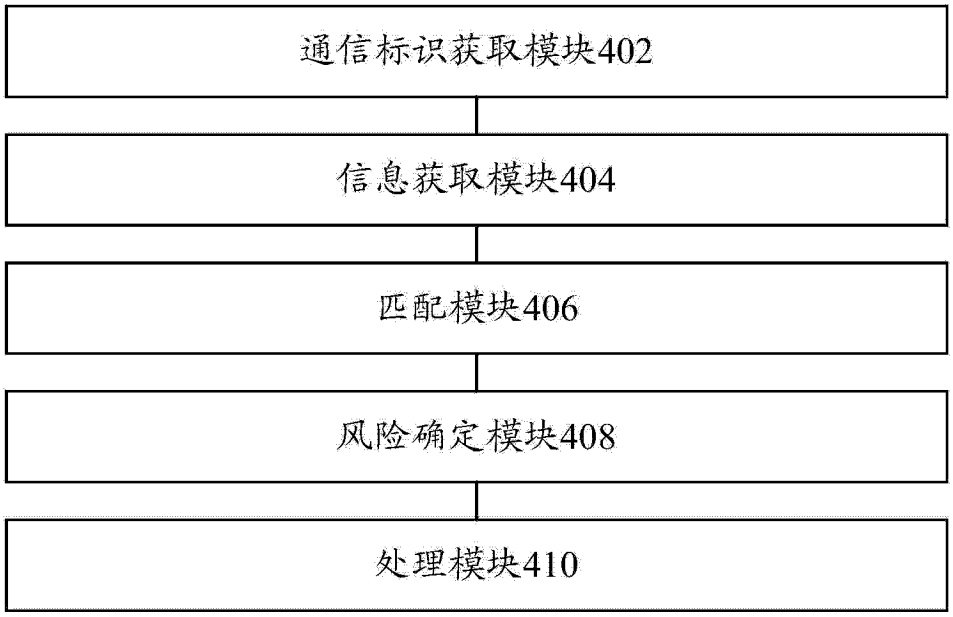

通信标识获取模块402
信息获取模块404
匹配模块406
风险确定模块408
处理模块410

图 4

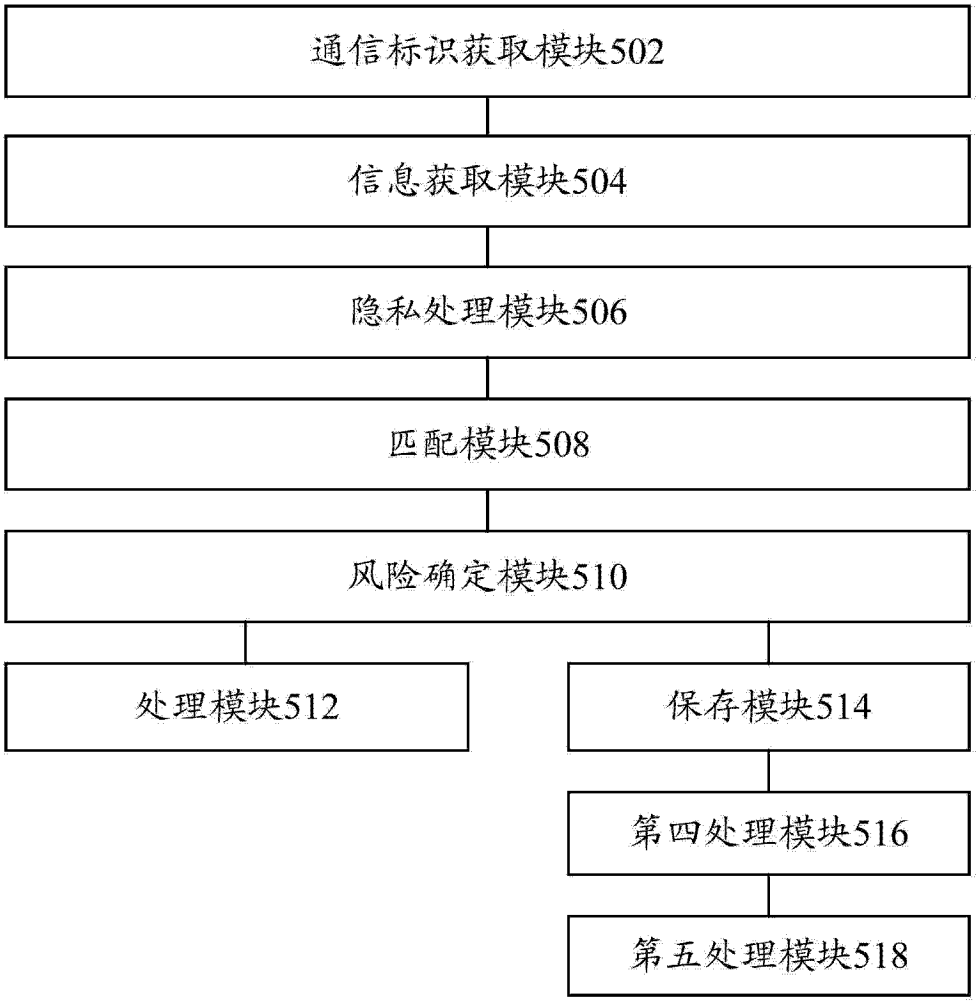

通信标识获取模块502
信息获取模块504
隐私处理模块506
匹配模块508
风险确定模块510
处理模块512
保存模块514
第四处理模块516
第五处理模块518

图 5