(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104182687 B
(45)授权公告日 2016.10.05

(21)申请号 201410377593.3
(22)申请日 2014.08.01
(65)同一申请的已公布的文献号
申请公布号 CN 104182687 A
(43)申请公布日 2014.12.03
(73)专利权人 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)
专利权人 奇智软件(北京)有限公司
(72)发明人 孟齐源 高祎玮
(74)专利代理机构 北京智汇东方知识产权代理事务所(普通合伙) 11391
代理人 康正德 薛峰
(51)Int.Cl.
G06F 21/56(2013.01)

审查员 杨洁

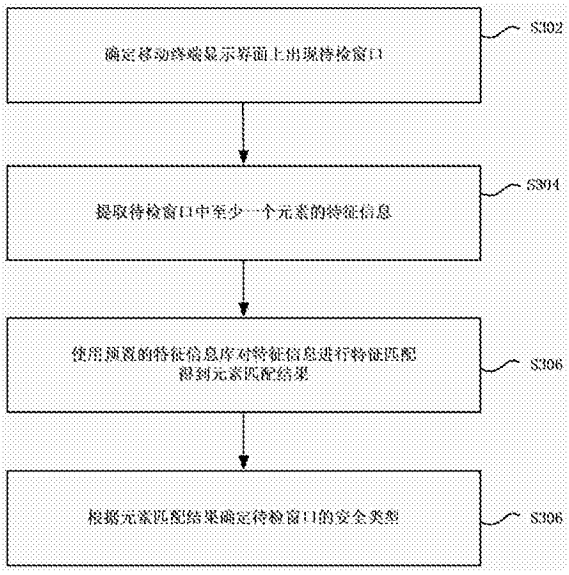
权利要求书2页 说明书10页 附图5页

(54)发明名称

移动终端输入窗口的安全检测方法和安全检测装置

(57)摘要

本发明提供了一种移动终端输入窗口的安全检测方法和安全检测装置。其中基于移动终端界面窗口的安全检测方法包括:确定移动终端显示界面上出现待检窗口;提取待检窗口中至少一个元素的特征信息;使用预置的特征信息库对特征信息进行特征匹配,得到元素匹配结果;根据元素匹配结果确定待检窗口的安全类型,其中特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息。该方案利用显示界面上出现的待检窗口进行窗口元素特征的匹配,防止出现恶意程序通过窗口伪装方法截取用户信息情况,提高了用户信息安全。



CN 104182687 B

1.一种基于移动终端界面窗口的安全检测方法，包括：

确定移动终端显示界面上出现待检窗口；

提取所述待检窗口中至少一个元素的特征信息；

使用预置的特征信息库对所述特征信息进行特征匹配，得到元素匹配结果；

根据元素匹配结果确定所述待检窗口的安全类型，其中所述特征信息库预先保存有支付类软件窗口的元素特征信息和/或恶意样本的窗口的元素特征信息。

2.根据权利要求1所述的方法，其中，确定移动终端显示界面上出现待检窗口包括：

检测所述移动终端中的进程变化；

确定所述进程在移动终端显示界面上生成新窗口。

3.根据权利要求1所述的方法，其中，使用预置的特征信息库中对所述特征信息进行特征匹配包括：

对所述特征信息进行白样本特征匹配和/或黑样本特征匹配。

4.根据权利要求3所述的方法，其中，对所述特征信息进行白样本特征匹配包括：

提取所述待检窗口中元素的文本内容包含的支付关键词，

根据所述支付关键词确定出对应的支付类软件；

将所述待检窗口的元素的特征信息与所述特征信息库中所述对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定所述待检窗口为安全窗口。

5.根据权利要求4所述的方法，其中，所述特征信息库预先保存的所述支付类软件窗口的元素特征信息包括：所述支付类软件的登录窗口的元素特征信息、所述支付类软件的账号绑定窗口的元素特征信息、所述支付类软件的支付窗口的元素特征信息。

6.根据权利要求3所述的方法，其中，对所述特征信息进行黑样本特征匹配包括：

将所述待检窗口的特征信息与所述特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定所述待检窗口为恶意窗口。

7.根据权利要求1至6中任一项所述的方法，其中，

所述待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；

提取所述待检窗口中至少一个元素的特征信息包括：提取所述元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

8.根据权利要求1至6中任一项所述的方法，其中，

所述预置的特征信息库预置于安全分析服务器中，

在对所述特征信息进行特征匹配之前还包括：将所述特征信息上传至所述安全分析服务器。

9.根据权利要求1至6任一项中所述的方法，其中，在提取所述待检窗口中至少一个元素的特征信息之前还包括：

对生成所述待检窗口的进程进行安全扫描，以确定所述进程的样本类型；

在所述进程不属于已知安全进程或已知危险进程中的任一种时，执行提取所述待检窗口中至少一个元素的特征信息的步骤。

10.根据权利要求1至6任一项中所述的方法，其中，在确定所述待检窗口的安全类型之后还包括：

在所述移动终端显示界面上输出与所述安全类型对应的提示信息。

11.一种移动终端输入窗口的安全检测装置，包括：

界面监测模块，适于确定移动终端显示界面上生成出现待检窗口；

特征信息提取模块，适于提取所述待检窗口中至少一个元素的特征信息；

特征匹配模块，适于使用预置的特征信息库中对所述特征信息进行特征匹配，得到元素的匹配结果，并根据元素匹配结果确定所述待检窗口的安全类型，其中所述特征信息库预先保存有支付类软件窗口的元素的特征信息和/或恶意样本的窗口的元素特征信息。

12.根据权利要求11所述的装置，其中，所述界面监测模块还适于：

检测所述移动终端中的进程变化；

确定所述进程在移动终端显示界面上生成新窗口。

13.根据权利要求11所述的装置，其中，所述特征匹配模块包括：

白样本匹配子模块，适于：提取所述待检窗口中元素的文本内容包含的支付关键词，根据所述支付关键词确定出对应的支付类软件；将所述待检窗口的元素的特征信息与所述特征信息库中所述对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定所述待检窗口为安全窗口，和/或

黑样本匹配子模块，适于：将所述待检窗口的特征信息与所述特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定所述待检窗口为恶意窗口。

14.根据权利要求13所述的装置，其中，所述特征信息库预先保存的所述支付类软件窗口的元素特征信息包括：所述支付类软件的登录窗口的元素特征信息、所述支付类软件的账号绑定窗口的元素特征信息、所述支付类软件的支付窗口的元素特征信息。

15.根据权利要求11至14中任一项所述的装置，其中，

所述待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；

提取所述待检窗口中至少一个元素的特征信息包括：提取所述元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

16.根据权利要求11至14中任一项所述的装置，其中，所述特征匹配模块包括：

信息上传子模块，适于将所述特征信息上传至安全分析服务器，所述预置的特征信息库预置于所述安全分析服务器中。

17.根据权利要求11至14任一项中所述的装置，其中，还包括：

进程扫描模块，适于对生成所述待检窗口的进程进行安全扫描，以确定所述进程的样本类型；

所述特征信息提取模块还适于：在所述进程扫描模块的扫描结果为在所述进程不属于已知安全进程或已知危险进程中的任一种时，执行提取所述待检窗口中至少一个元素的特征信息的步骤。

18.根据权利要求11至14任一项中所述的装置，其中，还包括：

安全提示模块，适于在所述移动终端显示界面上输出与所述安全类型对应的提示信息。

移动终端输入窗口的安全检测方法和安全检测装置

技术领域

[0001] 本发明涉及互联网安全领域，特别是涉及一种移动终端输入窗口的安全检测方法和安全检测装置。

背景技术

[0002] 随着网络技术和电子商务的发展，在移动终端上进行网购和电子支付越来越普及，然而移动终端的信息安全成为了影响移动终端网购和电子支付发展的重要阻碍。

[0003] 移动终端的信息安全涉及用户信息的保密、用户资金和支付信息的安全等问题，目前存在一些恶意应用程序，通过盗取终端数据或伪装成正规网购客户端或支付客户端的页面骗取用户信息的方式，骗取用户的银行或支付账号信息进行金融诈骗，导致用户遭受损失。

[0004] 针对以上问题，现有技术中出现了多种针对移动应用软件的扫描方法，常用的方法是使用移动应用软件的静态或者动态特征，与预置的特征库进行匹配，判别进行检测的移动应用软件属于黑名单或者白名单，其中白名单是指已经进过验证的正常应用软件列表，而黑名单是指已经确认为恶意应用程序的列表。然而由于当前移动应用软件的变化速度很快，现有预置特征库的更新速度不能满足新出现的应用程序的检测要求，从而导致出现一些无法判别类型的移动应用，从而不能达到实时有效保护移动终端的信息安全的目的。

发明内容

[0005] 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移动终端输入窗口的安全检测装置和相应的移动终端输入窗口的安全检测方法。本发明一个进一步的目的是要使得通过显示窗口确定是否存在窃取用户信息的安全隐患，保证用户信息安全。

[0006] 本发明另一个进一步的目的是要充分利用显示窗口的各种元素进行判断，确保检测的准确性。

[0007] 依据本发明的一个方面，提供了一种基于移动终端界面窗口的安全检测方法。该基于移动终端界面窗口的安全检测方法包括：确定移动终端显示界面上出现待检窗口；提取待检窗口中至少一个元素的特征信息；使用预置的特征信息库对特征信息进行特征匹配，得到元素匹配结果；根据元素匹配结果确定待检窗口的安全类型，其中特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息。

[0008] 可选地，确定移动终端显示界面上出现待检窗口包括：检测移动终端中的进程变化；确定进程在移动终端显示界面上生成新窗口。

[0009] 可选地，使用预置的特征信息库中对特征信息进行特征匹配包括：对特征信息进行白样本特征匹配和/或黑样本特征匹配。

[0010] 可选地，对特征信息进行白样本特征匹配包括：提取待检窗口中元素的文本内容

包含的支付关键词，根据支付关键词确定出对应的支付类软件；将待检窗口的元素的特征信息与特征信息库中对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定待检窗口为安全窗口。

[0011] 可选地，特征信息库预先保存的支付类软件窗口的元素特征信息包括：支付类软件的登录窗口的元素特征信息、支付类软件的账号绑定窗口的元素特征信息、支付类软件的支付窗口的元素特征信息。

[0012] 可选地，对特征信息进行黑样本特征匹配包括：将待检窗口的特征信息与特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定待检窗口为恶意窗口。

[0013] 可选地，待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；提取待检窗口中至少一个元素的特征信息包括：提取元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

[0014] 可选地，预置的特征信息库预置于安全分析服务器中，在对特征信息进行特征匹配之前还包括：将特征信息上传至安全分析服务器。

[0015] 可选地，在提取窗口中至少一个元素的特征信息之前还包括：对生成窗口的进程进行安全扫描，以确定进程的样本类型；在进程不属于已知安全进程或已知危险进程中的任一种时，执行提取窗口中至少一个元素的特征信息的步骤。

[0016] 可选地，在确定待检窗口的安全类型之后还包括：在移动终端显示界面上输出与安全类型对应的提示信息。

[0017] 根据本发明的另一方面，提供了移动终端输入窗口的安全检测装置。该安全检测装置包括界面监测模块，适于确定移动终端显示界面上生成出现待检窗口；特征信息提取模块，适于提取待检窗口中至少一个元素的特征信息；特征匹配模块，适于使用预置的特征信息库中对特征信息进行特征匹配，得到元素的匹配结果，并根据元素匹配结果确定待检窗口的安全类型，其中特征信息库预先保存有支付类软件类窗口的元素的特征信息和/或恶意样本的窗口的元素特征信息。

[0018] 可选地，界面监测模块还适于：检测移动终端中的进程变化；确定进程在移动终端显示界面上生成新窗口。

[0019] 可选地，特征匹配模块包括：白样本匹配子模块，适于：提取待检窗口中元素的文本内容包含的支付关键词，根据支付关键词确定出对应的支付类软件；将待检窗口的元素的特征信息与特征信息库中对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定待检窗口为安全窗口，和/或黑样本匹配子模块，适于：将待检窗口的特征信息与特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定待检窗口为恶意窗口。

[0020] 可选地，特征信息库预先保存的支付类软件窗口的元素特征信息包括：支付类软件的登录窗口的元素特征信息、支付类软件的账号绑定窗口的元素特征信息、支付类软件的支付窗口的元素特征信息。

[0021] 可选地，待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；提取待检窗口中至少一个元素的特征信息包括：提取元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

[0022] 可选地，特征匹配模块包括：信息上传子模块，适于将特征信息上传至安全分析服

务器，预置的特征信息库预置于安全分析服务器中。

[0023] 可选地，以上移动终端输入窗口的安全检测装置还包括：进程扫描模块，适于对生成窗口的进程进行安全扫描，以确定进程的样本类型；特征信息提取模块还适于：在进程扫描模块的扫描结果为在进程不属于已知安全进程或已知危险进程中的任一种时，执行提取窗口中至少一个元素的特征信息的步骤。

[0024] 可选地，以上移动终端输入窗口的安全检测装置还包括：安全提示模块，适于在移动终端显示界面上输出与安全类型对应的提示信息。

[0025] 本发明的移动终端输入窗口的安全检测方法利用显示界面上出现的待检窗口进行窗口元素特征的匹配，以判别待检窗口是否伪装成安全应用软件的显示窗口，从而防止出现恶意程序通过窗口伪装方法截取用户信息情况，提高了用户信息安全。

[0026] 进一步地，本发明的移动终端输入窗口的安全检测方法，可以采用白样本特征匹配和黑样本特征匹配的方式进行检测，既可以确定待检窗口为安全窗口，也可以确定待检窗口为恶意窗口，提高了安全检测的准确性。

[0027] 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、特征信息和优点能够更明显易懂，以下特举本发明的具体实施方式。

[0028] 根据下文结合附图对本发明具体实施例的详细描述，本领域技术人员将会更加明了本发明的上述以及其他目的、优点和特征信息。

附图说明

[0029] 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：

[0030] 图1是根据本发明一个实施例的移动终端输入窗口的安全检测装置的示意框图；

[0031] 图2是根据本发明一个实施例的移动终端输入窗口的安全检测装置的应用环境图；

[0032] 图3是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的示意图；

[0033] 图4是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的一种可选流程图；以及

[0034] 图5是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的中一个待检窗口的示意图。

具体实施方式

[0035] 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。

[0036] 图1是根据本发明一个实施例的移动终端输入窗口的安全检测装置100的示意框图。该移动终端输入窗口的安全检测装置100一般性地可包括：界面监测模块110、特征信息提取模块120、特征匹配模块130，这些部件可以根据移动终端输入窗口的安全检测装置100的功能和使用环境进行灵活配置，在一些优选的实施例中可以通过增加部件，实现更多的功能已达到不同的技术效果，例如，还可以增加设置进程扫描模块140和安全提示模块150，另外，特征匹配模块130的一种可选结构为包括白样本匹配子模块132、黑样本匹配子模块134、信息上传子模块136。

[0037] 在本实施例的移动终端输入窗口的安全检测装置100中，界面监测模块110可以适于确定移动终端显示界面上生成出现待检窗口，其一种可选的流程为检测移动终端中的进程变化；确定进程在移动终端显示界面上生成新窗口。检测移动终端中的进程可以利用主防技术，注入系统进程内部，获取进程生成窗口的情况。优选地，界面监测模块110可以将带有输入框的窗口作为待检窗口。

[0038] 特征信息提取模块120提取待检窗口中至少一个元素的特征信息，一般显示窗口的元素待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮，对应地，特征信息提取模块120提取的特征信息可以包括以上元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

[0039] 特征匹配模块130可以使用预置的特征信息库中对特征信息进行特征匹配，得到元素的匹配结果，并根据元素匹配结果确定待检窗口的安全类型。以上特征信息库预先保存有支付类软件类窗口的元素的特征信息和/或恶意样本的窗口的元素特征信息，例如特征信息库预先保存的支付类软件窗口的元素特征信息包括：支付类软件的登录窗口的元素特征信息、支付类软件的账号绑定窗口的元素特征信息、支付类软件的支付窗口的元素特征信息，以将支付类软件类窗口的元素的特征信息作为白样本的匹配依据。恶意样本的窗口的元素特征信息可以提取上报的恶意样本的窗口的元素的特征作为黑样本的匹配依据。

[0040] 具体地，白样本匹配子模块132可以提取待检窗口中元素的文本内容包含的支付关键词，根据支付关键词确定出对应的支付类软件；将待检窗口的元素的特征信息与特征信息库中对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定待检窗口为安全窗口。对于安全窗口，本实施例的移动终端输入窗口的安全检测装置100可以不做任何干预，以由用户进行正常操作。

[0041] 黑样本匹配子模块134可以将待检窗口的特征信息与特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定待检窗口为恶意窗口。对于恶意窗口，如果用户在其中输入账号信息等内容有可能被截取，导致信息泄露，因此需要向用户报告，并采取必要的措施。例如通过安全提示模块150在移动终端显示界面上输出与安全类型对应的提示信息。进一步地，还可以采取其他方式进行安全防范，例如将恶意窗口的输入框设置为不可输入，以避免用户在不知情的情况下进行输入，仅在用户忽略提示信息的情况下，回复输入框的输入功能。

[0042] 以上信息匹配过程可以在终端侧进行，也可以利用云端技术在云端进行匹配，例如利用信息上传子模块136将特征信息上传至安全分析服务器，利用预置于安全分析服务器中的预置的特征信息库进行以上信息匹配的过程。一种具体的配置方式为，在终端侧和网络侧分别预置数据库以用于窗口元素的特征匹配，以适用于不同的使用环境。

[0043] 进程扫描模块140可以对生成窗口的进程进行安全扫描，以确定进程的样本类型；特征信息提取模块130在进程扫描模块的扫描结果为在进程不属于已知安全进程或已知危险进程中的任一种时，才执行提取窗口中至少一个元素的特征信息的步骤。也就是说，首先使用进程检测的方式进行筛选，仅在进程检测不能确定安全性时，执行在进行窗口元素的特征匹配的步骤。

[0044] 图2是根据本发明一个实施例的移动终端输入窗口的安全检测装置100的应用环境图，本实施例的移动终端输入窗口的安全检测装置100可以设置于各类移动终端10中，例如智能手机、平板电脑、掌上电脑等中。这些移动终端10可以运行于安卓等操作系统中，本实施例的移动终端输入窗口的安全检测装置100利用对以上操作系统的进程主防确定移动终端显示界面上出现待检窗口，并使用预置于移动终端中保存有窗口元素特征的特征信息库进行特征匹配。以上特征信息库由安全分析服务器30通过移动网络20进行下发，另外，移动终端输入窗口的安全检测装置100还可以将提取出的待检窗口的元素的特征信息通过移动网络20上传，由安全分析服务器30预置于移动终端中保存有窗口元素特征的特征信息库进行特征匹配，并将匹配结果下发给移动终端10，并对恶意窗口进行提示。

[0045] 本发明实施例还提供了一种基于移动终端界面窗口的安全检测方法，该基于移动终端界面窗口的安全检测方法可以由以上实施例介绍的任意一种基于移动终端界面窗口的安全检测装置来执行，以提高移动终端的信息安全性。图3是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的示意图，如图所示，该基于移动终端界面窗口的安全检测方法包括以下步骤：

[0046] 步骤S302，确定移动终端显示界面上出现待检窗口；

[0047] 步骤S304，提取待检窗口中至少一个元素的特征信息；

[0048] 步骤S306，使用预置的特征信息库对特征信息进行特征匹配，得到元素匹配结果；

[0049] 步骤S308，根据元素匹配结果确定待检窗口的安全类型。

[0050] 在以上步骤中，步骤S302可以通过检测移动终端中进程变化确定出现待检窗口，具体可以检测移动终端中进程变化以确定进程在移动终端显示界面上生成新窗口。检测移动终端中进程可以利用主防技术，注入系统进程内部，获取进程生成窗口的情况。由于本实施例所要解决的一个技术问题为防止用户输入的账户信息或支付信息被截取，因此以上待检窗口可以具体是带有输入框的窗口，特别是该输入框的类型为密码框的情况下。又例如新出现的窗口的标题栏中的文字包括有以下关键词：“快捷支付”、“支付宝支付”、“微信支付”、“移动支付”、“手机银行”等，则需要将该窗口作为待检窗口。

[0051] 一般显示窗口的元素待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮，步骤S304提取的特征信息可以包括以上元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

[0052] 步骤S306使用的特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息，也就是既可以识别安全窗口也可以识别危险窗口，对待检窗口采取非黑即白的检测测量。

[0053] 相应地，步骤S306可以包括对特征信息进行白样本特征匹配和黑样本特征匹配两种匹配方式中的任一种或全部两种。

[0054] 例如，特征信息库预先保存的支付类软件窗口的元素特征信息包括以下内容：支

付类软件的登录窗口的元素特征信息、支付类软件的账号绑定窗口的元素特征信息、支付类软件的支付窗口的元素特征信息。步骤S306进行白样本特征匹配的流程可以为：提取待检窗口中元素的文本内容包含的支付关键词，根据支付关键词确定出对应的支付类软件；将待检窗口的元素的特征信息与特征信息库中对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定待检窗口为安全窗口。一个具体的实例为窗口的标题栏中文字为“微信支付”，将该窗口的元素特征与微信客户端中支付界面的元素特征进行匹配，若匹配成功，就可以确认该待检窗口为微信支付窗口，否则就可以认为该待检窗口为恶意窗口或者需要进行进一步检测。

[0055] 步骤S306对特征信息进行黑样本特征匹配的一种流程为包括：将待检窗口的特征信息与特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定待检窗口为恶意窗口。对于恶意窗口，在步骤S308之后还可以在移动终端显示界面上输出与安全类型对应的提示信息，以提醒用户。另外，在出现恶意窗口的情况下，还可以对恶意窗口进行处理，例如屏蔽窗口，将输入框置灰处于不可输入状态等，防止用户进行操作，如果用户的提醒信息进行忽略操作，则恢复窗口。

[0056] 除了利用移动终端上预置的特征信息库进行黑白样本特征匹配之外，本实施例的移动终端输入窗口的安全检测方法还可以将特征信息上传至安全分析服务器，并接收安全分析服务器下发的特征匹配结果，从而利用网络侧的大数据进行匹配，得到的结果更加准确。

[0057] 在步骤304之前，还可以利用移动端的病毒查杀系统对进程的样本进行检测，例如对生成窗口的进程进行安全扫描，以确定进程的样本类型；在进程不属于已知安全进程或已知危险进程中的任一种时，然后执行步骤S304。也就是说，首先使用进程检测的方式进行筛选，仅在进程检测不能确定安全性时，执行在进行窗口元素的特征匹配的步骤。

[0058] 图4是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的一种可选流程图，该流程包括：

[0059] 步骤S402，确定移动终端显示界面上生成新的待检窗口

[0060] 步骤S404，使用移动终端的病毒主防软件判断生成窗口的进程是否为已知的安全进程，若是允许窗口正常运行，若否执行步骤S406；

[0061] 步骤S406，使用移动终端的病毒主防软件判断生成窗口的进程是否为已知的恶意进程，若是向用户进行安全提示，并执行相应安全操作（例如结束进程、删除文件、放入隔离区等），若否，说明无法确定进程安全性，需要进行后续窗口元素特征匹配；

[0062] 步骤S408，判断新生成的窗口是否存在输入框，若否说明该窗口仅为内容显示窗口，可不进行检测；

[0063] 步骤S410，确定窗口为待检窗口；

[0064] 步骤S412，提取窗口元素的特征，具体可以包括以下内容：输入框、标题栏、标签、菜单、操作按钮等元素各自的文本内容、位置信息、链接地址、元素等。

[0065] 步骤S414，使用白样本窗口元素的特征进行匹配，若匹配成功，若是允许窗口正常运行；

[0066] 步骤S416，使用黑样本窗口元素的特征进行匹配，若匹配不成功，可以将元素特征上传至安全分析服务器进行进一步分析；

[0067] 步骤S418，提示窗口安全风险，并对窗口进行安全防范操作，例如将屏蔽窗口，将输入框置灰以处于不可输入状态等，防止用户进行操作，泄露个人信息。以上提示窗口中可以提示出窗口的安全隐患，还可以向用户提供操作选项，例如卸载相关应用、上传安全检测结果、忽略提示等，以便用户自行判断并进行相应操作。

[0068] 执行本发明以上实施例的基于移动终端界面窗口的安全检测方法，判断客户端的界面的类似程度，例如对话框弹出时，可以对对话框里的元素（提示框的类别、标题栏）进行特征判别，比如标题栏是否提示淘宝支付宝登陆，界面栏有没有某种形式的提示框，是不是密码框。又例如在提取出元素的特征串后，可以根据界面里的输入框和文字进行识别，建立类似于判定模型，判定是否是支付或其他金融界面（例如类似于淘宝、微信的登录框，是否是微信支付宝绑定银行卡的界面）。

[0069] 对于安卓系统终端，例如安卓智能手机，提取窗口的元素可以利用类似脚本的语言进行，结合其判定规则进行判定，形成安卓系统显示界面的弹框的判定模型，相对于现有对判断包名签名的识别，本实施例的基于移动终端界面窗口的安全检测方法可以弥补其更新速度不能满足要求的不足。

[0070] 图5是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的中一个待检窗口的示意图，在确定界面上上出现图5所示的窗口后，首先由主防引擎判断生成该窗口的客户端的安全类型（例如对包名、权限信息特征匹配），如果该窗口属于白样本，则可以使该窗口正常运行，如果该窗口属于黑样本，则需要提醒用户安全风险，并提供相应安全措施选项（例如提示卸载，对该应用的弹窗进行拦截等），如果无法确定客户端的安全类型，提取标题栏、标签和输入框的类型，在图5中的标题栏出现“请输入支付密码”，而且标签中也出现金额和银行卡信息，此时需要将以上这些元素的特征（位置、链接地址、文本）与特征库中的黑白窗口元素的特征进行匹配，如果确定这些特征是已知的安全支付窗口，则允许窗口正常运行，如果确定这些特征与伪装成支付窗口的黑样本的特征匹配，则在窗口展示界面上提示风险，并在用户进行进一步操作前，将输入框设置为不可输入。从而防止用户输入的账户信息被截取导致损失。

[0071] 使用本实施例的基于移动终端界面窗口的安全检测方法利用显示界面上出现的待检窗口进行窗口元素特征的匹配，防止出现恶意程序通过窗口伪装方法截取用户信息情况，提高了用户信息安全。

[0072] 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。

[0073] 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，本发明的各个特征信息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信息更多的特征信息。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信息。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。

[0074] 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。除了这样的特征信息和/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)中公开的所有特征信息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)中公开的每个特征信息可以由提供相同、等同或相似目的的替代特征信息来代替。

[0075] 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信息而不是其它特征信息，但是不同实施例的特征信息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。

[0076] 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基于移动终端界面窗口的安全检测装置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。

[0077] 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。

[0078] 至此，本领域技术人员应认识到，虽然本文已详尽示出和描述了本发明的多个示例性实施例，但是，在不脱离本发明精神和范围的情况下，仍可根据本发明公开的内容直接确定或推导出符合本发明原理的许多其他变型或修改。因此，本发明的范围应被理解和认定为覆盖了所有这些其他变型或修改。

[0079] 本发明实施例还提供了A1.一种基于移动终端界面窗口的安全检测方法，包括：

[0080] 确定移动终端显示界面上出现待检窗口；

[0081] 提取所述待检窗口中至少一个元素的特征信息；

[0082] 使用预置的特征信息库对所述特征信息进行特征匹配，得到元素匹配结果；

[0083] 根据元素匹配结果确定所述待检窗口的安全类型，其中所述特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息。

[0084] A2.根据A1所述的方法，其中，确定移动终端显示界面上出现待检窗口包括：

[0085] 检测所述移动终端中的进程变化；

[0086] 确定所述进程在移动终端显示界面上生成新窗口。

[0087] A3.根据A1所述的方法，其中，使用预置的特征信息库中对所述特征信息进行特征匹配包括：

[0088] 对所述特征信息进行白样本特征匹配和/或黑样本特征匹配。

[0089] A4.根据A3所述的方法，其中，对所述特征信息进行白样本特征匹配包括：

[0090] 提取所述待检窗口中元素的文本内容包含的支付关键词，

[0091] 根据所述支付关键词确定出对应的支付类软件；

[0092] 将所述待检窗口的元素的特征信息与所述特征信息库中所述对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定所述待检窗口为安全窗口。

[0093] A5.根据A4所述的方法，其中，所述特征信息库预先保存的所述支付类软件窗口的元素特征信息包括：所述支付类软件的登录窗口的元素特征信息、所述支付类软件的账号绑定窗口的元素特征信息、所述支付类软件的支付窗口的元素特征信息。

[0094] A6.根据A3所述的方法，其中，对所述特征信息进行黑样本特征匹配包括：

[0095] 将所述待检窗口的特征信息与所述特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定所述待检窗口为恶意窗口。

[0096] A7.根据A1至A6中任一项所述的方法，其中，

[0097] 所述待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；

[0098] 提取所述待检窗口中至少一个元素的特征信息包括：提取所述元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

[0099] A8.根据A1至A7中任一项所述的方法，其中，

[0100] 所述预置的特征信息库预置于安全分析服务器中，

[0101] 在对所述特征信息进行特征匹配之前还包括：将所述特征信息上传至所述安全分析服务器。

[0102] A9.根据A1至A8任一项中所述的方法，其中，在提取所述窗口中至少一个元素的特征信息之前还包括：

[0103] 对生成所述窗口的进程进行安全扫描，以确定所述进程的样本类型；

[0104] 在所述进程不属于已知安全进程或已知危险进程中的任一种时，执行提取所述窗口中至少一个元素的特征信息的步骤。

[0105] A10.根据A1至A9任一项中所述的方法，其中，在确定所述待检窗口的安全类型之后还包括：

[0106] 在所述移动终端显示界面上输出与所述安全类型对应的提示信息。

[0107] 本发明实施里还提供了B11.一种移动终端输入窗口的安全检测装置，包括：

[0108] 界面监测模块，适于确定移动终端显示界面上生成出现待检窗口；

[0109] 特征信息提取模块，适于提取所述待检窗口中至少一个元素的特征信息；

[0110] 特征匹配模块，适于使用预置的特征信息库中对所述特征信息进行特征匹配，得到元素的匹配结果，并根据元素匹配结果确定所述待检窗口的安全类型，其中所述特征信息库预先保存有支付类软件类窗口的元素的特征信息和/或恶意样本的窗口的元素特征信息。

[0111] B12.根据B11所述的装置，其中，所述界面监测模块还适于：

[0112] 检测所述移动终端中的进程变化；

[0113] 确定所述进程在移动终端显示界面上生成新窗口。

[0114] B13.根据B11所述的装置，其中，所述特征匹配模块包括：

[0115] 白样本匹配子模块，适于：提取所述待检窗口中元素的文本内容包含的支付关键词，根据所述支付关键词确定出对应的支付类软件；将所述待检窗口的元素的特征信息与所述特征信息库中所述对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定所述待检窗口为安全窗口，和/或

[0116] 黑样本匹配子模块，适于：将所述待检窗口的特征信息与所述特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定所述待检窗口为恶意窗口。

[0117] B14.根据B13所述的装置，其中，所述特征信息库预先保存的所述支付类软件窗口的元素特征信息包括：所述支付类软件的登录窗口的元素特征信息、所述支付类软件的账号绑定窗口的元素特征信息、所述支付类软件的支付窗口的元素特征信息。

[0118] B15.根据B11至B14中任一项所述的装置，其中，

[0119] 所述待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；

[0120] 提取所述待检窗口中至少一个元素的特征信息包括：提取所述元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

[0121] B16.根据B11至B15中任一项所述的装置，其中，所述特征匹配模块包括：

[0122] 信息上传子模块，适于将所述特征信息上传至安全分析服务器，所述预置的特征信息库预置于所述安全分析服务器中。

[0123] B17.根据B11至B16任一项中所述的装置，其中，还包括：

[0124] 进程扫描模块，适于对生成所述窗口的进程进行安全扫描，以确定所述进程的样本类型；

[0125] 所述特征信息提取模块还适于：在所述进程扫描模块的扫描结果为在所述进程不属于已知安全进程或已知危险进程中的任一种时，执行提取所述窗口中至少一个元素的特征信息的步骤。

[0126] B18.根据B11至B17任一项中所述的装置，其中，还包括：

[0127] 安全提示模块，适于在所述移动终端显示界面上输出与所述安全类型对应的提示信息。

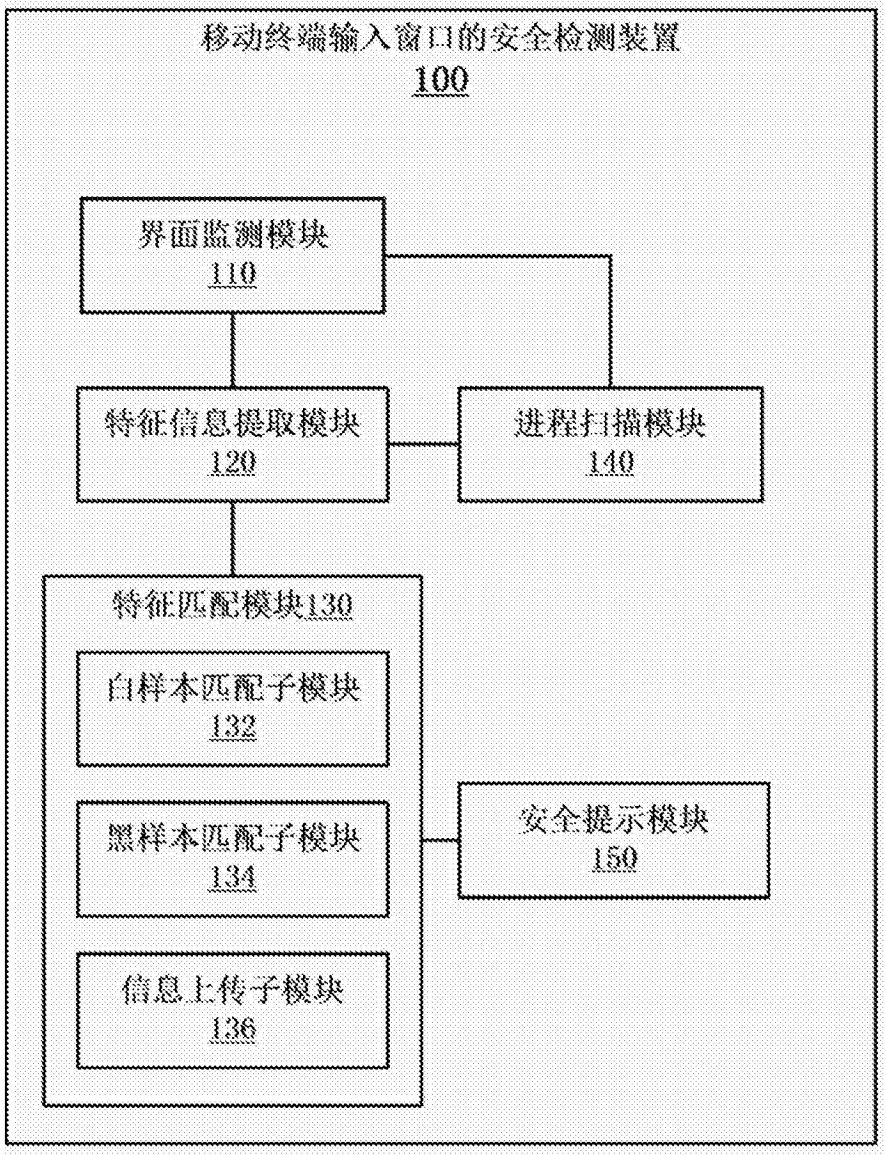

移动终端输入窗口的安全检测装置
100
界面监测模块
110
特征信息提取模块
120
进程扫描模块
140
特征匹配模块130
白样本匹配子模块
132
黑样本匹配子模块
134
信息上传子模块
136
安全提示模块
150

图1

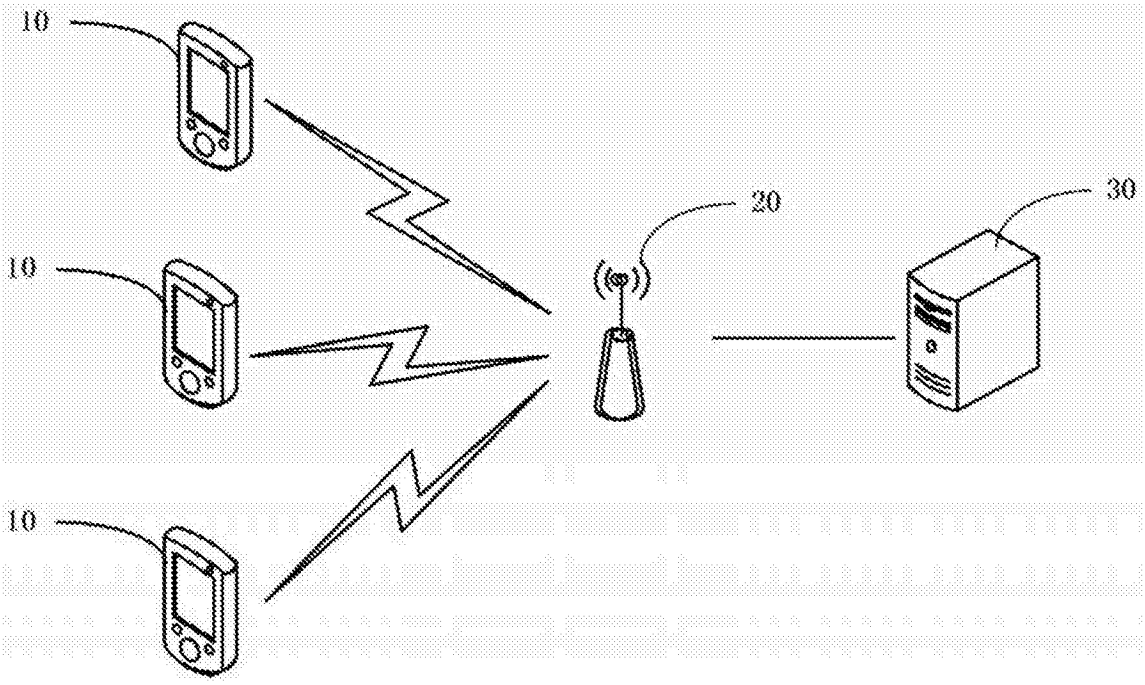


图2

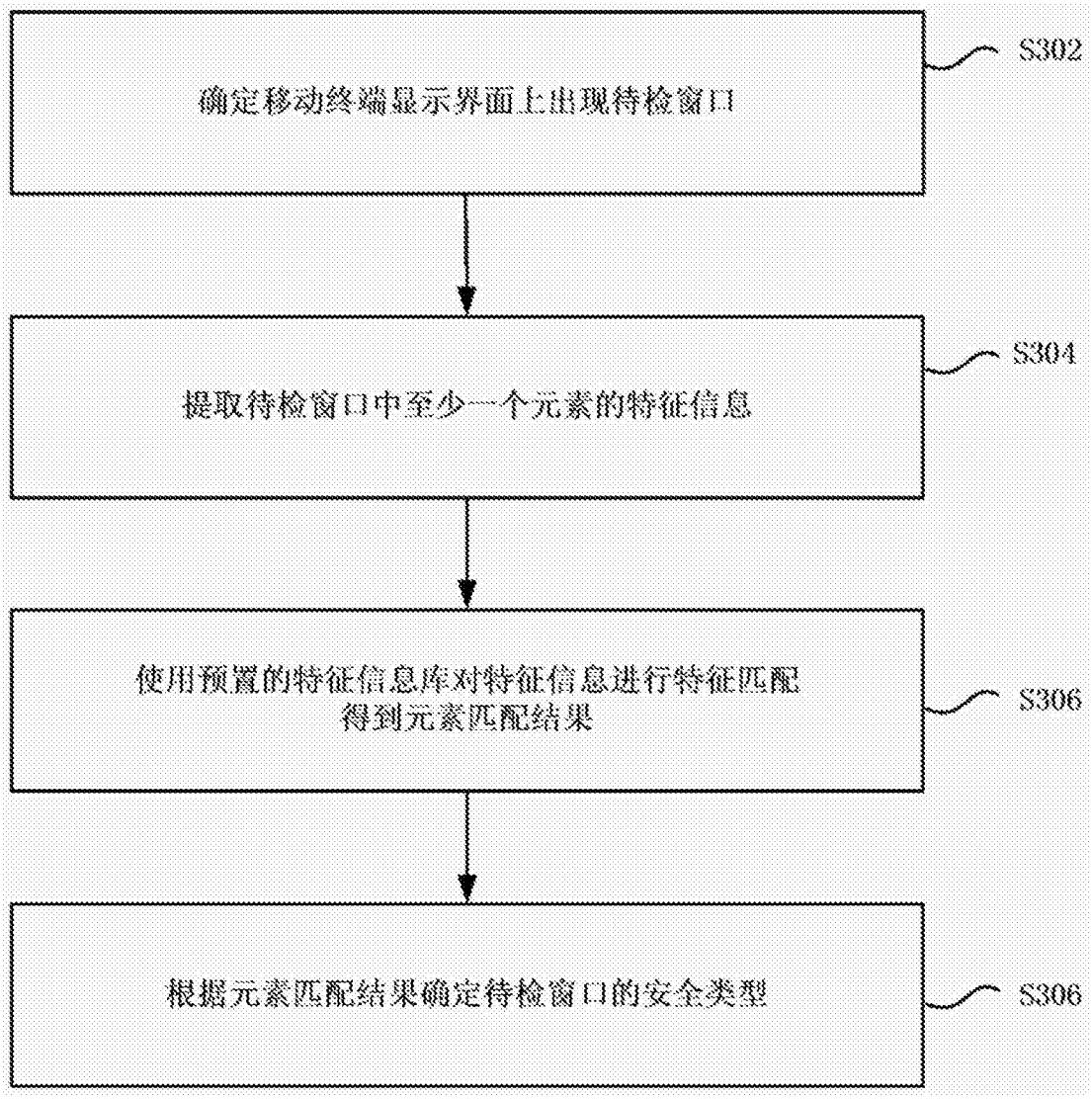

确定移动终端显示界面上出现待检窗口
S302
提取待检窗口中至少一个元素的特征信息
S304
使用预置的特征信息库对特征信息进行特征匹配
得到元素匹配结果
S306
根据元素匹配结果确定待检窗口的安全类型
S306

图3

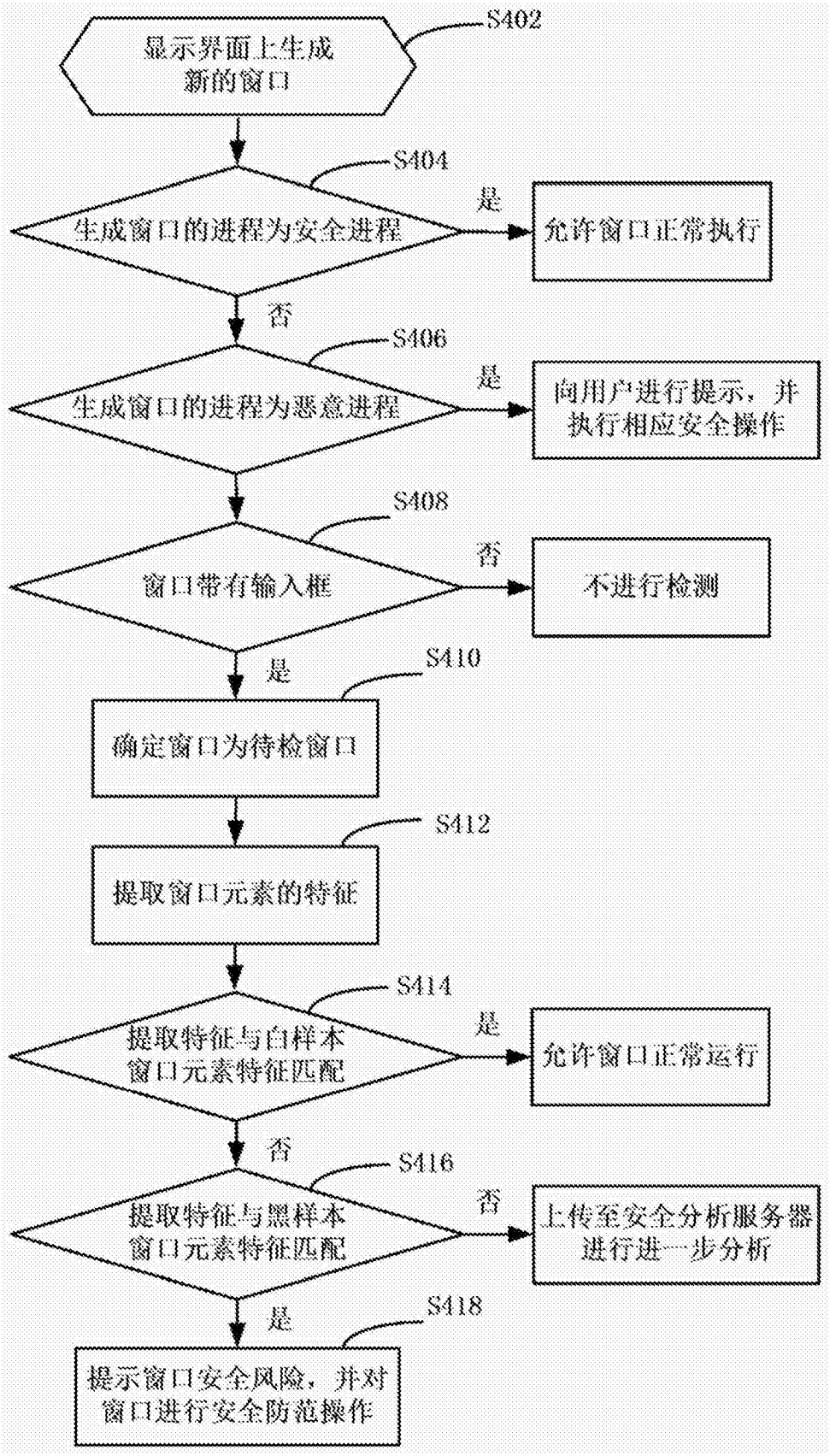

S402
显示界面上生成新的窗口
S404
生成窗口的进程为安全进程
是
允许窗口正常执行
否
S406
生成窗口的进程为恶意进程
是
向用户进行提示，并执行相应安全操作
S408
窗口带有输入框
否
不进行检测
是
S410
确定窗口为待检窗口
S412
提取窗口元素的特征
S414
提取特征与白样本窗口元素特征匹配
是
允许窗口正常运行
否
S416
提取特征与黑样本窗口元素特征匹配
否
上传至安全分析服务器进行进一步分析
是
S418
提示窗口安全风险，并对窗口进行安全防范操作

图4

图5