



(12) 发明专利申请

(10) 申请公布号 CN 102084370 A

(43) 申请公布日 2011.06.01

(21) 申请号 200980121250.8

代理人 刘佳 袁逸

(22) 申请日 2009.04.01

(51) Int. Cl.

(30) 优先权数据

G06F 21/00 (2006.01)

12/060,865 2008.04.02 US

H04W 12/08 (2006.01)

(85) PCT申请进入国家阶段日

2010.12.01

(86) PCT申请的申请数据

PCT/IB2009/005548 2009.04.01

(87) PCT申请的公布数据

W02009/122296 EN 2009.10.08

(71) 申请人 优盖提特拜克有限公司

地址 爱尔兰科克

(72) 发明人 W·菲茨杰拉德 P·伯明翰

F·汉尼根 P·普林德盖斯特

(74) 专利代理机构 上海专利商标事务所有限公

司 31100

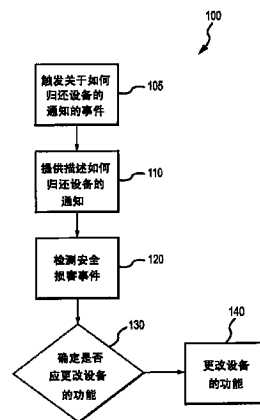
权利要求书 11 页 说明书 20 页 附图 55 页

(54) 发明名称

用于缓解对设备的未授权使用的系统

(57) 摘要

本发明涉及用于检测设备的丢失、偷窃或未授权使用和 / 或作为响应更改该设备的功能的系统和方法。在一个实施例中,设备监视其使用、其局部环境、和 / 或其操作上下文以确定该设备不再处于授权用户的控制之内。该设备可接收更改其功能的通信或生成更改其功能的内部信号,诸如指示该设备进入限制使用模式、监督模式,以提供用于归还该设备和 / 或阻止对数据的未授权使用或未授权访问的指示。附加实施例还解决了用于搜集关于未授权用户的法庭数据以帮助定位未授权用户和 / 或该设备的方法和系统。



1. 一种跟踪及丢失缓解系统,包括:  
移动设备,所述设备包括:  
用户接口,包括显示器和数据输入接口;以及  
与安全机构的通信接口;  
其中所述移动设备被配置成:  
提供关于如何将所述移动设备归还给授权用户的指示;  
检测已发生安全损害事件;以及  
响应于所述安全损害事件更改所述移动设备的功能以缓解所述授权用户失去控制。
2. 如权利要求 1 所述的系统,其特征在于,所述移动设备选自包括以下各项的组:  
膝上型计算机;  
台式计算机;  
移动订户通信设备;  
移动电话;  
个人数字助理(PDA);  
数据平板电脑;  
数码相机;  
摄影机;  
视频游戏机;  
媒体播放器;  
USB 钥匙;  
全球定位系统(GPS);以及  
其组合。
3. 如权利要求 1 所述的系统,其特征在于,所述安全损害事件选自包括以下各项的组:  
所述授权用户失去对所述移动设备的控制;  
所述移动设备的偷窃;  
丢失关于所述移动设备在何处的知识;  
包括电子病毒、电子蠕虫、和电子木马中的至少一者的电子威胁的入侵;  
对所述移动设备中的隐私信息的未授权访问;以及  
以无线服务提供方未授权的方式使用所述移动设备。
4. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过在所述移动设备的当前用户尝试利用所述移动设备时呈现自动消息来更改所述移动设备的功能,其中所述自动消息包括通知以下至少之一:  
所述移动设备已丢失或失窃;  
及时归还所述移动设备将得到酬劳;以及  
所述用户可按压任何按钮发起与安全机构联系;  
提供将所述移动设备归还给所述授权用户的指示。
5. 如权利要求 4 所述的系统,其特征在于,所述消息包括音频消息、文本消息、和视频消息中的至少一者。
6. 如权利要求 4 所述的系统,其特征在于,所述消息是在所述当前用户正利用所述移

动设备来拨出电话呼叫时呈现的。

7. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成在所述移动设备上的任何按钮被按压时发起与安全机构联系。

8. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过调节所述移动设备中的显示照明以将注意力吸引到所述移动设备来更改所述移动设备的功能。

9. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过在所述移动设备中的扬声器上播放不舒适的声音来更改所述移动设备的功能。

10. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过向所述授权用户发送消息来更改所述移动设备的功能,其中所述消息包括选自包括以下的组:

由所述移动设备呼叫的电话号码;

所述移动设备的当前操作状态;

所述移动设备的位置;

所述移动设备已从预定位置移走的陈述;

所述移动设备正在移动中的陈述;

指示在发生安全事件之后所述设备何时被首次使用的日期和时间戳;以及呼叫安全机构以发起找回过程的指示。

11. 如权利要求 1 所述的系统,其特征在于:

所述安全机构进一步包括数据库,所述数据库包括授权用户信息以及相关移动设备信息;并且

所述安全机构进一步配置成

从所述数据库获得关于所述授权用户的偷窃通知记录;以及通过以下至少之一来联系所述授权用户:

向所述偷窃通知记录中指定的电话号码拨出的电话呼叫,从而向所述授权用户提供关于如何联系所述移动设备的当前用户以找回该移动设备的音频指示;以及

向所述偷窃通知记录中指定的地址电子地发送的文本消息,从而向所述授权用户提供关于如何联系所述移动设备的当前用户以找回该移动设备的文本指示;以及

通过常规邮件向所述偷窃通知记录中指定的地址发送的印刷消息,从而向所述授权用户提供关于如何联系所述移动设备的当前用户以找回该移动设备的文本指示。

12. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

获得在发生安全事件时要限制的特征列表;以及

将所述移动设备的功能限于未受限特征。

13. 如权利要求 12 所述的系统,其特征在于,获得要限制的特征列表进一步包括:

由所述授权用户访问 web 界面,所述 web 界面呈现在失去对所述移动设备的控制时能够限制的特征列表;

由所述安全机构接受来自所述授权用户的关于能限制的特征的输入;以及

将接受的输入传递给所述移动设备。

14. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过执行选自包括以下各项的组的命令来更改所述移动设备的功能:

阻止从所述移动设备拨出电话呼叫；  
使从所述移动设备能呼叫的电话号码限于预定号码列表；  
在当前用户能使用所述移动设备之前要求输入口令；  
关闭所述移动设备；  
命令所述移动设备执行使得所述移动设备不能操作的破坏性功能；  
呈现频繁的消息，以提示所述移动设备的当前用户联系安全机构以发起将所述移动设备归还给所述授权用户，所述消息包括文本消息或音频消息中的至少一者；  
在所述移动设备正在使用中时在所述移动设备的扬声器上播放 DTMF 音调；以及  
允许仅向所述移动设备上的联系人列表内的一个或更多个预定号码发起电话呼叫；以及

其组合。

15. 如权利要求 14 所述的系统，其特征在于，要求输入口令进一步包括：

检测无效口令的输入；以及

在所述当前用户能尝试输入另一口令之前引入延迟。

16. 如权利要求 14 所述的系统，其特征在于，所述安全损害事件包括所述授权用户报告所述移动设备失窃或丢失，并且其中所述移动设备加入了防丢失或失窃的保险。

17. 如权利要求 1 所述的系统，其特征在于，所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能：

在所述显示器上提供使当前用户输入用户标识和口令的提示；以及

提供可选择标记，所述标记提供关于如何归还该移动设备的指示，所述指示是无需当前用户输入有效用户标识和口令的情况下提供的。

18. 如权利要求 17 所述的系统，其特征在于，进一步包括：

提示所述当前用户输入标识信息；

接收所述标识信息并将其存储在所述移动设备上；

搜索至所述安全机构的通信连接；以及

将所存储的标识信息传递给所述安全机构。

19. 如权利要求 1 所述的系统，其特征在于，所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能：

锁定订户身份模块以阻止对所述移动设备的自由使用；以及

提示当前用户输入个人解锁代码。

20. 如权利要求 19 所述的方法，其特征在于，进一步包括由所述安全机构将个人解锁代码转发给由所述授权用户指定的预定地址。

21. 如权利要求 1 所述的系统，其特征在于，所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能：

接收来自所述移动设备的当前用户的电话号码；

截取所述移动设备的所述当前用户拨出的呼叫；以及

将所述呼叫路由到所述安全机构和所述授权用户中的至少一者。

22. 如权利要求 1 所述的系统，其特征在于，所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能：

接收所述移动设备正在进行电话呼叫的标记；以及  
提醒所述授权用户和所述安全机构中的至少一者所述移动设备正在进行电话呼叫。

23. 如权利要求 22 所述的系统,其特征在于,进一步包括:

接收接入所述电话呼叫的请求;以及  
和第三方建立与所述电话呼叫的会议连接,其中:  
所述第三方包括所述授权用户和安全机构之一;并且  
所述第三方可主动参与对话或秘密地听取该对话。

24. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

从所述授权用户获得存储在所述移动设备内的在发生安全损害事件时将被加密的数据元素的列表;以及

在发生所述安全损害事件时,用所述安全机构和所述授权用户中的至少一者知道的口令来加密所述数据元素。

25. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

从所述授权用户获得存储在所述移动设备内的在发生安全损害事件时将被删除的数据元素的列表;以及

在发生所述安全损害事件时删除所述数据元素。

26. 如权利要求 25 所述的系统,其特征在于,进一步包括覆写被删除的数据元素预定次数,所述覆写选自包括以下各项的组:

随机数据;  
交替数据值;  
预定数据模式;以及  
其组合。

27. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

从所述授权用户获得存储在所述移动设备内的在发生安全损害事件时将被存档的数据元素的列表;以及

在发生所述安全损害事件时将所述数据元素存档,其中所述数据元素包括以下至少之一:

软件应用;  
数据文件;  
媒体文件;以及  
许可。

28. 如权利要求 27 所述的方法,其特征在于,将所述数据元素存档进一步包括将关于所述数据元素中的一个或更多的许可信息存档。

29. 如权利要求 27 所述的系统,其特征在于,通过将数据传送给所述安全机构以及所述授权用户能访问的设备中的至少一者来将所述数据存档。

30. 如权利要求 29 所述的系统,其特征在于,进一步包括:

由所述授权用户请求从档案检索被存档的数据元素；  
由所述授权用户指定接收所述被存档的数据元素的目的地址；以及  
将所述被存档的数据元素传送到所述目的地址。

31. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

在所述移动设备内建立用于存储一个或多个敏感数据元素的指定位置;

在发生安全损害事件时执行选自包括以下各项的组的功能:

用所述授权用户和安全机构中的至少一者知道的口令来加密所述敏感数据元素中的一个或多个;

删除所述敏感数据元素中的一个或多个;

多次覆写所述敏感数据元素中的一个或多个;以及

将所述敏感数据元素中的一个或多个传送到由所述授权用户指定的地址。

32. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

加密不开放供所述移动设备上运行的操作系统使用的指定文件;

截取用于打开文件的操作系统调用,并且因此:

解密所述文件;以及

打开所述文件;以及

截取用于关闭文件的操作系统调用,并且因此:

关闭所述文件;以及

加密所述文件。

33. 如权利要求 32 所述的系统,其特征在于,进一步包括由所述授权用户指定将被加密的文件类型的列表。

34. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

感测指派给所述移动设备的网络地址;

存储感测到的网络地址;以及

将所述感测到的网络地址传送给所述安全机构。

35. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

从由所述移动设备接收到的一个或多个信号感测至少一个无线网络地址;

存储感测到的网络地址;以及

将所述感测到的网络地址传送给所述安全机构。

36. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

从由所述移动设备接收到的一个或多个信号感测一个或多个无线接入点标识符;

存储所述无线接入点标识符;以及

将所述感测到的无线接入点标识符传送给安全机构。

37. 如权利要求 36 所述的系统,其特征在于,进一步包括基于所传送的无线接入点标识符来确定所述移动设备的位置。

38. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

由所述移动设备接收包括地理位置信息的信号;  
从接收到的信号获得所述地理位置信息;  
将所述地理位置信息存储在所述移动设备上;以及  
将所存储的地理位置信息传送给所述安全机构。

39. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

从安全机构检索位置信息;  
在包括地图的显示器上呈现所述位置信息,所述地图指示所述移动设备随时间的移动。

40. 如权利要求 39 所述的系统,其特征在于,还包括显示获得每个位置信息的时间和日期的标记。

41. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过在所述移动设备中存储在发生安全损害事件之后由所述移动设备呼叫的电话号码来更改所述移动设备的功能。

42. 如权利要求 41 所述的系统,其特征在于,进一步包括将所存储的电话号码传送给所述安全机构。

43. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

激活与所述移动设备通信的相机;  
从所述移动设备中的所述相机捕捉并存储图像;以及  
将所存储的图像传送给所述安全机构。

44. 如权利要求 43 所述的系统,其特征在于,进一步包括停用所述相机以保存电池寿命。

45. 如权利要求 43 所述的系统,其特征在于,进一步包括提示所述移动设备的当前用户采取要求看所述移动设备的活动。

46. 如权利要求 45 所述的系统,其特征在于,所述活动包括以下至少之一:  
提示所述用户在所述移动设备上输入口令;  
在所述移动设备上播放音频序列;  
闪烁所述音频设备上的光源;  
宣告所述当前用户已赢得奖品并请所述当前用户观看奖品兑换细节;以及  
显示视频序列。

47. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

激活与所述移动设备通信的话筒;  
从所述话筒捕捉和存储音频样本;以及

将所存储的音频样本传送给所述安全机构。

48. 如权利要求 47 所述的系统,其特征在于,进一步包括停用所述话筒以保存电池寿命。

49. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

激活与所述移动设备通信的话筒;

发起与所述安全机构的秘密通信会话;以及

将所述话筒捕捉到的音频数据中继给所述安全机构。

50. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

激活与所述移动设备通信的相机;

捕捉视频段;

将所述视频段存储在所述移动设备中;以及

将所述视频段传送给所述安全机构。

51. 如权利要求 50 所述的系统,其特征在于,进一步包括停用所述相机以保存电池寿命。

52. 如权利要求 50 所述的系统,其特征在于,进一步包括提示所述移动设备的当前用户采取要求看所述移动设备的活动。

53. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

激活与所述移动设备通信的相机;

发起与所述安全机构的秘密通信会话;以及

将所述相机捕捉到的视频数据中继给所述安全机构。

54. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

由所述移动设备获得当前用户的声音样本;

将所述声音样本存储在所述移动设备中;以及

将所存储的声音样本传送给所述安全机构。

55. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过激活键记录程序来更改所述移动设备的功能,其中在所述移动设备上按压的每个键的记录被存储在所述移动设备上。

56. 如权利要求 55 所述的系统,其特征在于,进一步包括将所述记录传送给安全机构。

57. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

由所述安全机构和所述授权用户中的至少一者登录远程接入服务,其中所述远程接入服务被配置成与所述移动设备通信;

激活所述移动设备中的应用程序接口以允许远程查看服务将以下至少之一转发给所述远程查看服务:

所述移动设备的当前状态;



所述移动设备的当前位置；  
由与所述移动设备通信的相机捕捉的图像；  
由与所述移动设备通信的相机捕捉的实时视频；  
所述移动设备上按压的键的列表；以及  
所述移动设备上当前运行的服务的列表。

58. 如权利要求 57 所述的方法,其特征在于,进一步包括:  
向所述移动设备传送发起聊天会话的命令;以及  
在所述移动设备上提供允许所述当前用户与所述授权用户和所述安全机构中的至少一者之间的基于文本的交互的界面。

59. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

在所述移动设备与至少一个无线收发机之间发起无线连接;以及  
通过所述至少一个无线收发机将关于所述移动设备的当前位置的信息中继给所述安全机构。

60. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

在所述移动设备与至少一个无线收发机之间发起无线连接;以及  
向所述无线收发机传送指示丢失或失窃设备位于所述收发机能接入的信号范围内的消息。

61. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

在所述移动设备与至少一个无线收发机之间发起无线连接;  
确定所述移动设备与所述至少一个无线收发机之间的所述无线连接的信号强度;  
获得所述至少一个无线收发机的标识标记;以及  
向第二无线收发机传送包括所述至少一个无线收发机的所述标识标记以及所述移动设备与所述至少一个无线收发机之间的所述无线连接的所述信号强度的消息。

62. 如权利要求 61 所述的系统,其特征在于,进一步包括:

向所述第二无线收发机传送指示处于所述第二无线收发机的通信范围内的一移动设备已被报告丢失或失窃的消息。

63. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

在所述移动设备与至少一个无线收发机之间发起无线连接;  
向所述至少一个无线收发机传送消息,所述消息包括所述移动设备的标识标记,并且其中所述消息包括以下至少之一:

对包括所述至少一个无线收发机的物理位置的响应的请求;  
使与所述至少一个无线收发机通信的人报告丢失或失窃设备位于其通信范围内的请求;

所述授权用户的电话号码;  
安全机构的电话号码;以及

向所述安全机构拨出呼叫的请求。

64. 如权利要求 1 所述的系统,其特征在於,所述移动设备进一步配置成通过以下操作来更改所述移动设备的功能:

在所述移动设备与至少一个无线收发机之间发起无线连接;

向所述至少一个无线收发机传送消息,其中所述消息请求提供包括所述至少一个无线收发机的物理位置的响应。

65. 如权利要求 1 所述的系统,其特征在於,所述移动设备被配置成修改所述移动设备上的显示,其中所述显示仅包括关于将所述移动设备归还给所述授权用户和所述安全机构中的至少一者的信息。

66. 如权利要求 65 所述的系统,其特征在於,进一步包括将所述移动设备的特征限制成仅为帮助将所述移动设备归还给安全机构和所述授权用户中的至少一者而操作。

67. 如权利要求 1 所述的系统,其特征在於,所述安全机构被配置成格式化消息以传送给所述移动设备,其中所述消息包括将由所述移动设备解码的命令。

68. 如权利要求 67 所述的系统,其特征在於,所述命令包括禁用所述移动设备的至少一个特征的指示。

69. 如权利要求 67 所述的系统,其特征在於,所述消息选自包括以下各项的组:SMS 文本消息、编码图形图像、音频文件、专用数据文件、CAB 文件、ZIP 文件、加密密钥、文件标识符、替换口令、文件类型、小应用程序、可执行代码片断、可解释脚本、软件更新、及其组合。

70. 如权利要求 67 所述的系统,其特征在於,所述命令包括使用驻留在所述移动设备上的应用来显示通知的指示。

71. 如权利要求 70 所述的系统,其特征在於,所述应用包括 web 浏览器、文本编辑器、图形图像显示器、消息屏幕、或位图显示器中的至少一者。

72. 如权利要求 70 所述的方法,其特征在於,通过浏览器使用驻留在 SIM 卡上的链接以引用来自远程服务器的所述应用。

73. 如权利要求 70 所述的系统,其特征在於,所述应用驻留在所述移动设备中的 SIM 卡上。

74. 如权利要求 67 所述的系统,其特征在於,所述消息隐写地编码在包含数字图像的文件中。

75. 如权利要求 67 所述的系统,其特征在於,所述命令包括发起对关于找回所述移动设备的法庭证据的数据搜集的指示。

76. 如权利要求 75 所述的系统,其特征在於,所述搜集法庭证据进一步包括以下至少之一:

捕捉所述当前用户的身体的至少一部分的图像;

测量所述当前用户的声音样本;

跟踪所述当前用户拨打的电话号码;

跟踪所述当前用户输入的键;

记录所述当前用户访问的网站;以及

记录所述当前用户投递的消息的电子邮件地址。

77. 如权利要求 67 所述的系统,其特征在於,所搜集的法庭信息被传送给所述安全机

构。

78. 如权利要求 67 所述的系统,其特征在于,所述命令在所述当前用户不知道的情况下在所述移动设备中执行。

79. 如权利要求 67 所述的系统,其特征在于,所述移动设备执行所述命令导致向所述当前用户呈现显示,所述显示提供关于如何将所述移动设备归还给所述授权用户和所述安全机构中的至少一者的信息。

80. 如权利要求 1 所述的系统,其特征在于,所述安全机构被配置成:  
确定:

所述移动设备加入了防丢失或偷窃的保险;并且

所述移动设备已被报告丢失或失窃;以及

向所述移动设备传送命令,其中所述命令更改所述移动设备中的功能。

81. 如权利要求 80 所述的方法,其特征在于,更改功能进一步包括以下至少之一:

禁用对所述移动设备的使用;

检测对所述移动设备的尝试使用;以及

跟踪所述移动设备的位置。

82. 一种用于提供更改移动设备的功能的命令的方法,所述方法包括:

由安全机构格式化要传送给移动设备的消息;

在所述消息内隐写地编码用于由所述移动设备执行的命令;以及

将所述消息传送给所述移动设备。

83. 如权利要求 82 所述的方法,其特征在于,进一步包括:

由所述移动设备解码所述隐写地编码的命令,以及

由所述移动设备执行所述命令。

84. 如权利要求 83 所述的方法,其特征在于,所述命令包括禁用所述移动设备的至少一个特征的指示。

85. 如权利要求 83 所述的方法,其特征在于,所述消息选自包括以下各项的组:SMS 文本消息、编码图形图像、音频文件、专用数据文件、CAB 文件、ZIP 文件、加密密钥、文件标识符、替换口令、文件类型、小应用程序、可执行代码、及其组合。

86. 如权利要求 83 所述的方法,其特征在于,所述命令包括发起对关于找回所述移动设备的法庭证据的数据搜集的指示。

87. 如权利要求 86 所述的方法,其特征在于,所述搜集法庭证据进一步包括以下至少之一:

捕捉所述当前用户的身体的至少一部分的图像;

测量所述当前用户的声音样本;

跟踪所述当前用户拨打的电话号码;

跟踪所述当前用户输入的键;

记录所述当前用户访问的网站;以及

记录所述当前用户投递的消息的电子邮件地址。

88. 如权利要求 86 所述的方法,其特征在于,其中所搜集的法庭信息被传送给安全机构。

89. 如权利要求 83 所述的方法,其特征在于,所述命令在所述当前用户不知道的情况下在所述移动设备中执行。

90. 如权利要求 83 所述的方法,其特征在于,所述移动设备执行所述命令导致向所述当前用户呈现显示,所述显示提供关于如何将所述移动设备归还给所述授权用户和所述安全机构中的至少一者的信息。

91. 如权利要求 1 所述的系统,其特征在于,所述移动设备进一步配置成基于通过通信接口从安全机构接收到的命令来更改所述移动设备的功能。

92. 一种跟踪及丢失缓解系统,包括:

移动设备,所述设备包括:

用户接口,包括显示器和数据输入接口;以及

与安全机构的通信接口;

其中所述移动设备被配置成:

提供关于如何将所述移动设备归还给授权用户的指示;

检测已发生安全损害事件;

响应于所述安全损害事件确定是否应当更改所述设备的功能;

响应于所述安全损害事件更改所述移动设备的功能以缓解所述授权用户失去控制。

93. 一种跟踪及丢失缓解系统,包括:

移动设备,所述设备包括:

用户接口,包括显示器和数据输入接口;以及

与安全机构的通信接口,其中:

授权用户可指定替换呼叫方标识标记;

其中所述移动设备被配置成:

提供关于如何将所述移动设备归还给所述授权用户的指示;

检测已发生安全损害事件;

响应于所述安全损害事件确定是否应当更改所述设备的功能;

响应于所述安全损害事件更改所述移动设备的功能以缓解所述授权用户失去控制。

94. 如权利要求 93 所述的跟踪及丢失缓解系统,其中所述呼叫方标识标记包括呼叫方标识数据。

## 用于缓解对设备的未授权使用的系统

### [0001] 所含版权资料申明

[0002] 本专利文档公开内容的一部分包含受版权保护的资料。版权所有人不反对任何人对该专利文献或专利公开内容进行复制,按照其在(美国)专利和商标局的专利文件或记录中的形式,但版权所有人保留其它所有的权利。本文中所标识的所有商标和服务标记为本申请人所拥有。

### [0003] 发明描述

### 发明领域

[0004] 本发明涉及用于响应于设备丢失、失窃或以未授权方式使用而更改电子设备的功能的系统和方法。更改后的功能可促使(1) 返还该设备,和/或(2) 更改设备的操作。本发明还便于监视设备的未授权用户。

### [0005] 发明背景

[0006] 如今,使用电子设备是普遍的。这些设备能提高用户的生产力和生活质量,但它们容易丢失、失窃、或被未授权使用。这些设备的示例有蜂窝电话、便携式数字助理(PDA)、数码相机、膝上型计算机。这些设备往往携带私有、机密和/或难以代替的数据,且丢失这些数据比丢失电子设备更复杂,因为已丢失或失窃的电子设备能在物理上被更换,而存储在此类设备上的数据往往是机密和/或不可代替的。

[0007] 此外,丢失或失窃设备的授权用户(其可能是或可能不是所有者)可能不得不应付后果,诸如由于未授权用户(如本文中所使用的,“未授权用户”意指除了授权用户或获授权用户授权以使用该设备的某人以外的任何人)访问了存储在该设备上的信息造成的信息滥用。此外,在此类设备的所有者或授权用户发现丢失之前可能已流逝了几小时或甚至几天并不罕见,且在该时间期间,未授权用户可能访问敏感数据、盗用信息、或在授权用户的账户上为货物或服务付费。

### 发明内容

[0008] 前述概述和以下详细描述两者均仅是示例性和解释性的,且不限所要求保护的本发明。

[0009] 根据本发明的方法和系统提供以下功能中的一个或多个:(1) 通过提供信息以辅助未授权用户归还设备来提高找回设备的可能性,(2) 更改设备的功能(可任选地包括阻止访问设备上的信息),以及(3) 获得关于未授权用户的信息以改善将标识未授权用户以及定位未授权用户和设备的机会。此外,本发明的系统和方法可提供快速响应以提醒未授权用户该设备放错地方或失窃。

### [0010] 附图简述

[0011] 结合以下解说性附图考虑详细描述和权利要求可获得对本发明的更全面理解。

[0012] 图1是描绘本发明的示例性过程的流程图。

[0013] 图2是关于可在其上作出电话呼叫的设备来描绘本发明的示例性过程的流程图。

- [0014] 图 3 是描绘根据本发明的示例性方法的步骤 120 的子步骤的流程图。
- [0015] 图 4 是描绘根据本发明的示例性方法的步骤 120 的子步骤的流程图。
- [0016] 图 5 是描绘根据本发明的示例性方法的步骤 120 的子步骤的流程图。
- [0017] 图 6 是示出本发明的各种功能的图示, 其中一个或更多个功能可被包括在步骤 140 中。
- [0018] 图 7 是描绘本发明的各种功能的图示, 其中一个或更多个功能可被包括在步骤 680 中。
- [0019] 图 8 是描绘根据本发明的各种方面的示例性系统的框图。
- [0020] 图 9-16 描绘了根据本发明的可在诸如膝上型计算机之类的移动计算设备上提供的示例性通知措施。
- [0021] 图 17-25 描绘了可在蜂窝电话、PDA、或手持移动设备上显示的示例性通知消息。
- [0022] 图 26-37 描绘与如本发明的实施例所例示的主机服务器相关联的示例性屏幕和过程。
- [0023] 图 38-58 解说下载到移动设备上的软件应用的安装和注册。
- [0024] 图 59-64 解说本发明的示出用于从移动设备卸载应用的过程的实施例。
- [0025] 示例性实施例的详细描述
- [0026] 如本文中所使用的, 术语“移动设备”、“移动电子设备”或“设备”一般是指可能丢失或失窃的任何电子设备。移动设备可以是自立设备, 诸如膝上型计算机、台式计算机、移动订户通信设备、移动电话、个人数字助理 (PDA)、数据平板电脑、数码相机、摄影机、视频游戏机、媒体播放器、全球定位系统 (GPS)、通用串行总线 (USB) 钥匙、移动武器、及其组合。移动电子设备也可以是与另一系统或设备集成的任何电子设备。例如, 根据本发明可监视和保护车辆内包含的立体声系统、全球定位系统、或其他电子设备。用于实现本发明的方法的软件可以在任何时间由授权用户通过因特网、SMS 短消息、或以任何其他合适方式间接或直接地 (1) 安装在或 (2) 下载到移动设备上, 并在任何合适时候实现根据本发明的方法。例如, 可在购买设备之后、或甚至在设备丢失或失窃之后, 在购买或下载软件时将软件安装到该设备上。移动设备可能有防丢失或失窃保险, 并且本发明的系统和方法可作为移动设备上的保险策略的一部分或补充而操作。
- [0027] 若加入保险的移动设备受本发明的实施例所提供的锁定和找回服务保护, 则移动设备的授权用户可能有资格付较低的保险费。在另一实施例中, 在针对该策略的索赔可能导致偿还丢失或失窃的移动设备的情况下, 保险公司可命令随加入保险的设备提供找回或锁定服务。因此, 本发明的实施例帮助防止保险欺骗。例如, 若父母买了新电话并为该电话加入防丢失或失窃保险, 父母可能希望将该加入保险的电话给他 / 她的孩子之一并提交偿还被赠送电话的保险索赔, 将其作为丢失或失窃设备来索赔, 由此免除购买新电话的成本。本发明可用于例如通过将所宣称的丢失或失窃电话禁用、检测对所宣称的丢失或失窃电话的尝试使用、或跟踪所宣称的丢失或失窃电话的位置或用户来防止此类欺骗索赔。
- [0028] 在一个实施例中, 结合本发明操作的移动设备包括无线收发机, 其通过诸如无线移动电话网、通用分组无线电服务 (GPRS) 网络、无线局域网 (WLAN)、全球移动通信系统 (GSM) 网络、个人通信服务 (PCS) 网络、高级移动电话系统 (AMPS) 网络、和 / 或卫星通信网络等无线系统与其他系统和设备通信。结合本发明操作的移动设备也可通过任何其他类

型的连接与其他系统和设备通信, 诸如有线因特网连接、无线因特网连接、蜂窝电话网络连接、无线 LAN 连接、无线 WAN 连接、光学连接、USB 连接、移动设备同步端口连接、电力连接和 / 或安全电缆。

[0029] 本发明的系统和方法可用作基于订户的服务的一部分, 以帮助保护和找回各种各样的不同移动设备。授权用户可使用每个设备的唯一性标识符链接到多个移动设备。可提供任何合适标识符, 诸如移动设备的序列号 (或其组合)、数字、字母、字母数字或其他标识符。标识符可用于验证与设备相关联的授权用户的身份, 以及监视移动设备并且倘若其丢失或失窃则提供其找回。在本发明的一个实施例中, 例如标识符和关于相关联授权用户的信息可被存储在存储介质 (诸如移动设备或中央服务器上的存储器) 供将来参考。

[0030] 此外, 根据本发明的系统和方法对不同输入或条件 (包括对变化的威胁等级的感测) 可具有不同响应。例如, 感测到其处于禁区 (诸如在被指派的建筑物的外部或在国外的) 的膝上型设备可通过一种或更多种加密技术来阻止访问, 删除数据或破坏硬驱动以使得数据检索困难或不可能。同一膝上型设备在接收到其丢失在其被指派的建筑物内的信号时可简单地提供描述如何归还该膝上型设备的通知。

[0031] 本文中描绘的方法的元素任何组合和 / 或子集可按任何合适次序以及结合任何合适系统、设备和 / 或过程来实践。本文中描述和描绘的方法可按任何合适方式实现, 诸如通过在移动设备和主机服务器上操作的软件。软件可包括存储在介质 (诸如移动设备或主机服务器的存储器) 中的计算机可读指令, 并且可由一个或更多个处理器运行以执行本发明的方法。

[0032] 现在转到附图, 其目的是为了描述本发明的优选实施例而非限制本发明, 根据本发明的各个方面的示例性方法在图 1-7 中描绘。

[0033] 在图 1 中所示的方法 100 中, 移动设备向授权用户提供描述如何归还该移动设备的通知 (110)。如本文中所描述的, “未授权用户” 意指除授权用户以外的任何人。该通知可按任何方式提供并由任何合适事件触发。例如, 该通知可以是视觉显示或音频信号, 诸如语音。该通知应向未授权用户提供使该未授权用户归还该设备的足够信息, 并且可包括电话号码、地址或电子邮件地址中的一个或更多个。该通知还可提供对归还该设备的酬劳。

[0034] 该通知可按任何合适的方式触发。例如, 授权用户可向该设备发送信号以显示该通知, 或者授权用户可联系将向该设备发送信号以激活该通知的服务。该通知也可自动显示, 例如, 若错误口令被键入预定次数或者若设备感测到其处于某个地理区域中。也可以使用任何其他合适的自触发事件。

[0035] 该设备的另一和可任选特征是检测安全损害事件 (120) 以及响应于安全损害事件确定是否应更改设备的功能 (130)。在恰适的情况下, 若有安全损害事件 (包括设备丢失或失窃), 则更改设备的功能 (140)。

[0036] 提供描述如何归还移动设备的通知

[0037] 在图 1 中描绘的根据本发明的示例性过程 100 中, 事件 105 触发由设备提供描述如何归还该设备的通知 (110)。该通知可按任何方式提供, 诸如通过使用移动设备的显示器、话筒或其他用户接口特征。该特征可包括任何符号、字符、数字、图形、声音 (包括所记录的语音消息和 / 或音乐)、和 / 或任何其他帮助描述如何归还该设备的标记 (例如, 在屏幕上显示的消息)。

[0038] 通知可包括例如提供找回指示的服务的电话号码或授权用户的电话号码、上缴位置或地址、激活移动设备的特征以发起归还过程的指示、提供找回指示的服务的 web 地址、和 / 或包括找回指示的网站的可点击链接中的一个或更多个。通知还可包括若将该设备上缴给找回服务可获得酬劳的消息。在本发明的一个实施例中,通知显示在登录屏幕上(包括归还该设备的机制),以使得其是用户在能访问该设备之前用户最先看到的信息。若授权用户(诸如所有者)担心他们已失去了对设备的控制,则他们可远程地激活移动设备上的应用并确保访问限于仅显示关于如何归还该设备的通知和细节。该办法的一个益处在于保存了位于移动设备上的信息的保密本质,基本上保护了敏感信息不被未授权访问。无线设备的无辜发现者还能够在不必绕过或破解移动设备上的口令以确定授权用户的身份的情况下归还该设备。

[0039] 当提供通知时,提供移动设备已丢失或失窃的单独信号或消息。该通知可帮助移动设备的未授权用户将其归还给其授权用户,并且通知很可能增加未授权用户将这样做的概率,因为他 / 她被提供了恰当的指示或信息。此外,该通知的显著性也可阻止是窃贼的未授权用户偷该移动设备或尝试保留、使用、或出售该移动设备。

[0040] 该通知可被提供给任何人(诸如目前拥有该移动设备的未授权用户)以及其他个人、系统、以及与该移动设备通信的设备。在本发明的一个示例性实施例中,参照图 2,提供描述如何归还移动设备(诸如移动电话)的通知(110)可包括:确定移动设备的当前未授权用户拨打的电话号码(210),呼叫该电话号码(220),以及呈现消息(诸如预先记录的、来自活人的文本或消息)(230)。该消息可包括任何合需信息,诸如该移动设备已报丢失或报失窃、和 / 或帮助发起归还该移动设备的指示。

[0041] 替换实施例可包括呈现 SMS 文本消息、电子邮件消息(例如,发送到当前用户的电子邮件地址)、双音多频(DTMF)音调序列、和 / 或任何其他消息类型。这允许移动设备提示拥有该移动设备的未授权用户他 / 她未被授权使用该设备和 / 或提供关于如何归还该设备的指示。这可以加快归还该移动设备,以及阻止个人从其合法所有者偷窃或保留该设备。

[0042] 通知可使用移动设备的部分或所有用户接口能力来提供。例如,膝上型计算机的通知可包括屏幕上关于其被保护的大幅消息以吸引观察者的注意力、和 / 或通过膝上型设备的扬声器播放的一个或更多个声音(包括音乐、预先记录的语音和警报)。类似地,蜂窝电话可呈现文本显示和 / 或发出声音以指示未授权用户如何归还该设备,或者发出警报声因吸引未授权用户的注意力并使其不想保留该设备。通知可通过与移动设备集成或通信的任何其他用户接口特征诸如打印机来呈现。

#### [0043] 检测安全损害事件

[0044] 在图 1 中所示的示例性方法中,移动设备检测已发生安全损害事件(120)。如本文中所使用的,“安全损害事件”一般是指其中移动设备(或其任何物理或功能部分)处于(或可能处于)授权用户的独占控制以外的任何情形,并且设备可能能够检测多种类型的安全损害事件,在这种情形中,设备可对不同类型的安全损害事件具有不同响应。

[0045] 安全损害事件可以是实际的(例如,移动设备实际上已经失窃)、或感知到的(例如,授权用户不确定移动设备的状态,但认为其可能丢失或失窃)。安全损害事件可包括授权用户失去对移动设备的控制、移动设备被偷、丢失关于移动设备在何处的知识、电子威胁(例如,电子病毒、电子蠕虫、和 / 或电子木马)入侵、对移动设备中的私有信息的未授权访



问或尝试未经授权访问、以未经无线服务提供方授权的方式使用移动设备、设备感测到其处于未经授权位置、输入不正确口令多次、指示移动设备的所有权或安全的损害的任何其他事件。

[0046] 安全损害事件可由移动设备本身检测,并且也可由授权用户直接或者通过与该移动设备通信的安全机构或其他实体、系统或设备间接地报告给该设备。

[0047] 移动设备可以任何方式检测安全损害事件,诸如通过从授权用户或安全机构(诸如政府法律执行组织、私有安全公司、和/或金融机构)接收消息,并且响应于该消息确定已发生安全的破坏。安全机构可以任何合需方式与该移动设备通信,诸如通过在与数据库通信的主机服务器上操作的软件。作为示例,授权用户可向安全机构报告他/她的移动设备丢失并指示安全机构向移动设备发信号通知有安全威胁(即,用户认为移动设备已丢失、失窃、或者可能以其他方式受未经授权访问)。结果,移动设备的功能可被更改(140),如以下进一步讨论的。

[0048] 移动设备可认证来自安全机构的消息的有效性,诸如通过计算该消息的摘要并将摘要值与预先存储的授权摘要值作比较。计算出的摘要值可以通过将收到消息提供给散列算法来产生的,诸如美国国家标准和技术协会联邦信息处理标准发布号 180-1 中指定的 MD5 或 SHA-1 安全散列算法,其公开通过援引全部纳入于此。授权摘要值可以是允许将收到信息标识为来自安全机构的有效传输的任何数字、代码、值、或标识符。所存储的授权摘要值可以在激活丢失/失窃找回服务时以及以任何其他合意方式提供给移动设备。除非授权摘要值匹配所存储的摘要值,否则该消息将得不到认证并且可被丢弃(若合需)。然而,在成功认证该消息时,不一定需要断言移动设备对来自安全机构的消息进行动作。移动设备可以任何其他合需方式认证消息的有效性。

[0049] 移动设备还可通过作为非对称加密算法的一部分用与该消息的发送方相关联的公钥来解密该消息的至少一部分,从而认证来自安全机构或其他源的消息的有效性。非对称加密算法和技术在本领域中是公知的。例如参见 Richard A. Mollin 的 RSA & Public Key Cryptography (RSA 及公钥密码学), CRC 出版社, 2002 年;以及 1983 年 9 月 20 日授权的美国专利号 4,405,829,其公开通过援引全部纳入于此。在解说性示例中,若双方(例如,“Alice”和“Bob”)希望使用公钥密码学安全地通信,任一方通过生成唯一性密钥对来开始,其中这些密钥之一是由这一方保持机密的私钥,另一密钥是可公开分发、仅发布给消息接收方、或通过公钥基础设施可获得的公钥。密钥生成步骤只需要由一方完成一次,只要这一方的私钥不被另一方损害或知晓。若 Alice 希望往 Bob 机密地发送消息,则她可以使用 Bob 的公钥来加密该消息,并且一旦被发送,只有 Bob 能使用 Bob 的私钥来解密和查看该消息。但是若 Alice 也希望 Bob 确保该消息确实来自她,她可在发送前进一步用她的私钥来加密该消息,随后 Bob 的私钥和 Alice 的公钥被用来解密该消息, Bob 肯定知道他是预期接收方且 Alice 是发起该消息的人,并且 Alice 知道只有 Bob 将能够解密和阅读她的消息。

[0050] 可连同本发明的实施例利用这种方案。在一实施例中,使用全双向公钥加密来认证发送方的确是安全机构(举例而言)且指示已发生安全损害事件的消息的接收方的确是预期接收方。替换地,消息可仅用发送实体的私钥来加密并用公钥来解密以加快处理时间。此类加密方案帮助验证安全损害事件通信,既提供对消息的源和目的地的验证,也提供用于向受损害移动设备安全地传送命令的手段。

[0051] 在替换实施例中,经加密或未加密的数据可通过加密传输协议被传送给 / 自移动设备,加密传输协议有诸如与 IEEE 802.11 无线协议相关联的无线加密协议 (WEP、WPA 和 WPA2)。可结合本发明使用任何数目的其他加密方法来加密传达给 / 自移动设备的数据。

[0052] 结合本发明操作的移动设备可使用任何数目的以任何格式的消息从安全机构或其他源接收已发生安全损害事件的信息。例如,本发明的实施例可在 SMS 文本消息、语音邮件消息、电子邮件消息、和 / 或一个或更多个 DTMF 音调的预定序列中接收信息。消息可以是任何合需格式。例如,消息可被包括在具有令牌化格式 (诸如标准 ASCII 文本格式) 或任何其他合适的标准化文件格式的文件中,诸如 MS Word 文档、MS Excel 文件、Adobe PDF 文件、或二进制图片文件 (JPEG、位图等)。此类文件中的数据可按任何方式排序并且可具有任何合适的分隔符、符号、或其他特征。该消息还可具有独特的和 / 或适当格式。

[0053] 在一个实施例中,指示已发生安全损害事件的消息可经由隐写技术被编码在文件中,诸如二进制图片文件,从而查看该文件或图片的任何人可看到可接受的图像,而隐藏消息被编码在该文件的数据中并且可通过恰当的软件技术来访问。例如,通过在以怂恿用户打开消息 / 文件的方式命名的文件 (例如,“HotJessica.JPG”) 中发送图形图像,则移动设备的当前用户可能打开该文件,这随后触发移动设备上的软件扫描该图像文件,由此从该图像文件提取并解码隐写式编码的数据。移动设备随后可解读所解码的数据,并且若指示锁定事件,则该设备可采取预定动作以本文中描述的任何方式部分地或完全地禁用该设备。移动设备上的软件可秘密地执行,其中该应用可执行法庭证据搜集特征,诸如在当前用户正在看刚打开的图像文件时对该用户的脸部拍照,同时当前用户不知道他 / 她被拍照或以其他方式被记录。可经由编码或隐蔽消息发送其他命令,诸如将设备的口令重置为替换的或更安全的口令的命令。

[0054] 消息的格式也可基于用于向移动设备传送消息的方法。例如,在使用无线电话连接向移动设备传送消息的情况下,消息可被格式化为 SMS 文本消息。类似地,消息可被格式化为 XML 记录、电子邮件和 / 或传真。消息可包括多种格式和 / 或多条消息,并且可被格式化为具有不同格式以用各种方法来传输或传送给各种不同移动设备。从安全机构、主机服务器、授权用户或其他源接收到的消息还可包括其他信息,诸如用于如以下所讨论地更改移动设备的功能的指示。

[0055] 在本发明的一个实施例中,移动设备可被配置成采取低功率、静默或待机状态,其中该设备可从授权用户或服务器 (诸如由安全机构管理的服务器) 接收通知。一旦接收到此类通知,移动设备就可基于该通知的内容在适当的时间采取行动。移动设备可退出待机状态以轮询服务器,从而确定是否有通知在等待,并且若如此,则下载该通知的内容并对其进行动作。补充地或替换地,移动设备具有缓冲预设,其能够接收由服务器或安全机构传送的通知,并在适当的时间 (诸如在接收到该消息时或以预定时间间隔) 对该消息的内容进行动作。

[0056] 移动设备还可通过确定该移动设备已与指定同伴设备解除关联来检测安全损害事件。移动设备可与任何合需类型的设备关联。例如,移动电话可以是另一移动电话的同伴设备。这两个移动电话可通过无线连接 (例如,蓝牙连接) 相关联,并且丢失无线连接可用于触发安全损害事件。类似地,在移动设备与多个同伴设备分开时,可触发安全损害事件。

[0057] 移动设备可通过任何合需方式确定它已与同伴设备解除关联,诸如通过测量同伴

设备传送的无线信号的功率电平、以及确定测得功率电平已降到预定阈值水平以下。此外,移动设备可通过向同伴设备传送消息并确定未从该同伴设备接收到满足预定确认准则(例如,预期的确认传输)的消息来确定它已与该同伴设备解除关联。此外,移动设备可在其不能建立与同伴设备的通信链路的情况下、或在同伴设备向该移动设备发送指示应限制对该移动设备的访问的信号的情况下确定它已与该同伴设备解除关联。移动设备可在照明移动设备的至少一个表面的入射光的量不同于预定阈值范围时确定它已与该同伴设备解除关联。例如,若移动设备从诸如钱包、行李箱、皮套或公文包等同伴设备移走,则在该移动设备的至少一个表面上的环境光的增加可被内置传感器检测到,从而指示该设备已从合需位置移走。类似办法可包括在封装移动设备的箱子打开时、或者若移动设备与其同伴设备之间的啮合表面中的光传感器在这两个设备分离或脱离时突然检测到光,则激活安全事件检查。

[0058] 移动设备可按任何合需方式与同伴设备关联,诸如通过经由有线链路和/或无线链路将移动设备与同伴设备配对。可使用任何合需无线链路和通信协议来将移动设备与同伴设备配对。例如,无线链路可包括 ISO 14443 协议、ISO18000-6 协议、蓝牙协议、Zigbee 协议、Wibree 协议、IEEE 802.15 协议、IEEE802.11 协议、IEEE 802.16 协议、超宽带(UWB)协议、IrDA 协议、及其组合。同样,可实现有线链路将移动设备与同伴设备配对,诸如通过使用计算机网络连接、USB 连接、移动设备同步端口连接、电源连接、和/或安全电缆。

[0059] 安全损害事件可与移动设备的硬件改变相关联。例如,在与移动设备通信的硬件身份模块(诸如通用订户身份模块和/或可移动用户身份模块)的标识符不匹配一个或多个预定授权标识符时,可确定安全损害事件。可结合本发明使用任何合需标识符,诸如电子序列号、局域身份标识符、集成电路标识符、国际移动订户标识符、认证密钥标识符、和/或因运营商而异的紧急号码标识符。

[0060] 硬件身份模块标识符可被传送给主机服务器、存储在存储介质(诸如移动设备或主机服务器的存储器)中、或以任何其他合需方式处理。例如,与移动设备的硬件(例如,硬驱动、SIM 卡或其他硬件)相关联的标识符可被用来确定是否有未授权用户正尝试规避保护该移动设备的软件或硬件安全协议。硬件身份模块标识符(以及结合本发明使用的任何其他数据)可用任何合适方式存储,诸如通过使用与移动设备集成或通信的存储器存储设备。硬件身份模块也可以任何其他合需方式被加密、隐藏或保护。

[0061] 安全损害事件可基于移动设备的单个硬件组件的改变,也可基于移动设备的整体硬件配置的改变。例如,诸如膝上型计算机等移动设备的硬件配置可包括特定应驱动、电池、RAM、BIOS 或该膝上型设备的其他组件的身份。膝上型设备的硬件配置可被存储(例如,由中央服务器和/或该移动设备存储)并且随后与该膝上型设备的当前硬件配置作比较(例如,周期性地和/或在发生事件时,诸如硬件组件改变时)。若当前硬件配置与所存储的配置相比已改变了超过预定阈值(例如,两个以上个体组件不同),则可触发安全损害事件。这允许在窃贼可能交换失窃移动设备的组件以尝试规避与所交换的组件相关联的(或其上存储的)安全措施的情况下发出安全损害事件。移动设备的硬件配置的改变(诸如 SIM 卡的改变)可随着时间被跟踪并被报告给安全机构或授权用户以帮助定位该移动设备。

[0062] 可基于对移动设备的使用和/或当前用户的行为来确定安全损害事件。例如,参

照图 3, 确定安全损害事件 (120) 可包括在预定时间段上累积移动设备的使用简档 (310), 累积关于移动设备的持续使用的信息 (320), 以及确定该持续使用是否与该使用简档偏离了预定阈值 (330)。

[0063] 使用简档和所累积信息可包括关于如何使用移动设备的任何合需信息, 诸如从驻留在移动设备中所存储的联系人列表内的号码拨打呼叫的次数与不驻留在该联系人列表内的号码拨打呼叫的次数之比、该移动设备拨出一个或多个呼叫的时辰、按钮按压之间的平均时间间隔、被按压按钮类型、按压按钮时施加的平均压力、预定时间区间内口令被输入错误的次数、口令被输入错误的连贯次数、及其组合。可将授权用户的使用简档与所累积信息作比较以确定授权用户是否仍在控制该设备。移动设备可采取任何合需行动来验证当前用户被授权使用该移动设备, 诸如提示当前用户键入口令, 并在在诸如键入口令前制止对该设备的进一步使用。

[0064] 可在任何合需时间段上编译使用简档。该时间段可包括固定时间段, 或者可以动态地确定 (例如, 随着移动设备被使用而平移时间)。预定时间段可由移动设备的授权用户指定, 以及可由移动设备自己确定。预定时间段可基于任何合需准则, 诸如使用移动设备的方式和 / 或编译使用简档所需的信息量。同样, 其中可累积关于移动设备的持续使用的信息的时间段可以与用户简档相同的方式指定。

[0065] 可比较所累积的持续使用信息和使用简档以确定该持续使用偏离使用简档的程度。可根据任何合需准则选择预定阈值以确定该持续使用是否指示未授权使用。例如, 若该持续使用包括使用简档中通常进行呼叫的时间范围外的显著数目次呼叫, 则该持续使用可能指示未授权使用。类似地, 按钮按压之间的时间间隔 (即, 当前用户使用该移动设备的速度)、被按压按钮的类型、按压按钮时施加的压力、口令被输入错误的次数 (包括连贯次数)、以及其他事件可指示 (单独或组合地) 未授权使用。

[0066] 事件组合可被加权, 以使得安全损害事件的发生基于预定表决阈值。个体事件可被赋予比其他事件更高的重要性, 以使得特定事件的重复发生偏离预定阈值, 而另一事件的单次发生偏离该阈值。例如, 在超过该预定阈值之前, 使用简档的正常时间范围外的呼叫可能需要发生总共 4 次, 而连续 2 次输入错误口令偏离该阈值。类似地, 错误口令输入结合使用简档中的正常时间范围外的两次呼叫可偏离该预定阈值。可以任何合需方式针对预定表决阈值加权或评分各事件。

[0067] 可基于用户提供适当生物测定数据失败来确定安全损害事件。在本发明的一个实施例中, 例如获得对移动设备的当前用户的生物测定测量, 并且将该生物测定测量与先前存储的参考值作比较。在该生物测定测量与先前存储的参考值相差超过预定阈值的情况下, 随后可确定安全损害事件。安全损害事件可基于来自移动设备的当前用户的任何数目个生物测定测量, 诸如指纹扫描、虹膜扫描、视网膜扫描、声音样本、呼吸样本、和 / 或移动设备的当前用户的一部分身体的照片。

[0068] 可基于移动设备的位置来确定安全损害事件。例如, 现在参照图 4, 确定安全损害事件 (120) 可包括获得移动设备的物理位置 (410), 分析该移动设备的物理位置以确定该设备位于未授权区域中 (420), 以及将该移动设备的物理位置与先前存储的位置列表作比较 (430)。

[0069] 移动设备的物理位置可以任何方式获得。例如, 可使用全球定位系统 (GPS)、通过

由移动设备发射的信号三角测量、通过网际协议 (IP) 地址和 / 或跟踪路线、或以任何其他方式来查明移动设备的位置。全球定位系统可包括例如接收机,其检测由具有已知传输时序和 / 或已知位置的发射源发射的信号,并分析在移动设备处接收到的时间编码信号。移动设备也可查明其关于发射源的位置。发射源可以是地面的、移动的、基于空间的、空中的、或其任何组合。在一个实施例中,移动设备可通过接收来自环地轨道中的卫星的信号并解读接收到的地理定位信号来查明其在地球表面上的位置。在另一实施例中,全球定位系统可包括地面天线和接收机的集合,其接收从移动设备发射的信号,并且通过分析移动设备的信号的到达角、到达时间、和 / 或到达时间差,可经由常规多边办法查明移动设备的位置。替换地,移动设备可从诸如蜂窝基站天线等已知地面发射源接收一个或更多个信号,并且通过分析收到信号计算其关于该已知地面发射源的位置。

[0070] 可以任何方式限定授权移动设备在其中操作的区域。例如,该区域可以由边界限定的地理区域、与邮政编码相对应的区域、和 / 或与电话区号相对应的区域。该区域可包括任何数目个分开的个体区域。区域可基于移动设备可操作之处(即,“白名单”)、以及移动设备不可操作之处(即,“黑名单”)来定义。

[0071] 可将移动设备的位置与定义移动设备被授权在其中操作的一个或更多个位置、移动设备没被授权在其中操作的一个或更多个位置、移动设备的功能在其中被至少部分地限制、和 / 或其组合的列表作比较。该列表可由该设备的授权用户和 / 或安全机构定义。在本发明的一个示例性实施例中,中央服务器(诸如图 8 中描绘的主机服务器 860) 监视移动设备的位置并将该设备的位置与先前存储在数据库中的位置列表作比较,以基于移动设备的位置确定是否已发生安全损害事件,以及作为结果是否应修改该设备的功能。该实施例尤其允许移动设备的雇主、父母、及其他“超级用户”定义移动设备在其雇员或孩子手上时应当在其中操作的边界。

[0072] 可基于移动设备的位置来确定安全损害事件。例如,现在参照图 5,确定安全损害事件(120)可包括在第一时间点测量第一环境参数(510),在第二时间点测量第二环境参数(520),将第一环境参数和第二环境参数与预定授权使用条件作比较(530),确定移动设备是否已离开第一位置(540),以及将第一和第二测得环境参数中的至少一者传送给安全机构(550)。

[0073] 如本文中所使用的,“环境参数”一般包括涉及移动设备的环境的任何参数。移动设备可测量以任何合需格式的任何合需环境参数,诸如由移动设备拍摄的图像。数码相机(包括诸如移动电话等其他设备内的相机)以及具有成像能力的其他设备因此可被用来拍摄该移动设备的环境的图像,包括该移动设备周围的物理对象和人。此类图像随后可被用来标识移动设备的位置和 / 或为从其授权用户拿走或保留该移动设备负责的个体。

[0074] 环境参数还可包括来自或关于与该移动设备通信的系统和设备的信息。在本发明的一个实施例中,例如,与移动设备通信的无线接收机可被激活并被用来从该移动设备在不同时间点接收到的一个或更多个信号感测一个或更多个无线网络地址。可比较在不同时间点感测到的网络地址以确定所感测到的网络地址是否变化,并因此确定移动设备是否已移动。

[0075] 环境参数可进一步包括地理位置信息。可从与移动设备通信的全球定位系统(GPS)以及从任何其他合需源测量地理位置信息。在本发明的一个示例性实施例中,移动设

备可接收包括地理位置信息的信号并解码在不同时间点接收到的位置信号。可比较与在不同时间测得的信号相对应的位置以确定移动设备的位置是否已改变、以及两个所采样的位置之间的距离是否超过预定阈值。可类似地测量任何数目个位置样本,并将其与初始位置或后续测得的位置作比较。预定阈值距离可由用户、安全机构和 / 或自动地由该移动设备配置。该实施例因此允许监视移动设备的移动,并且若其移动预定距离以上则发出安全损害事件。

[0076] 在本发明的各种实施例中,在未授权用户尝试篡改移动设备的安全预设时,可检测到安全损害事件。例如,导致确定篡改的条件可包括确定未授权用户尝试屏蔽移动设备的所报告位置;尝试重新路由移动设备中的电子地址;尝试绕过移动设备提供的口令提示;尝试在移动设备上进行蛮力口令攻击;尝试安装旨在阻挠操作系统安全的应用;及其组合。

#### [0077] 更改移动设备的功能

[0078] 在图 1 中描绘的示例性过程中,响应于安全损害事件确定是否应当更改该设备的功能 (130),并相应的更改移动设备的功能 (140)。移动设备的功能可以任何方式来更改并达成任何目的,诸如缓解由于设备的受损害状态产生的伤害、搜集证据以逮捕和定罪窃贼、以及鼓励 / 激励将该设备归还给正当的所有者。参照图 6,更改移动设备的功能 (140) 可包括向当前用户提供通知 (610),抑制移动设备的功能 (620),向授权用户和 / 或安全机构提供通知 (630),更改处理去往和来自移动设备的通信的方式 (640),保护移动设备中的数据 (650),跟踪移动设备 (660),搜集关于移动设备的使用的信息并将其传送给安全机构 (670),以及与其他设备通信 (680)。

[0079] 可响应于安全损害事件以任何方式更改移动设备的功能,包括部分地或完全禁用该设备的特征和 / 或提供安全损害事件之前不可用的功能。在本发明的一个实施例中,例如可更改移动设备的功能以向移动设备的当前用户呈现自动消息 (610)。该自动消息可以是任何格式并且可包含任何合需信息。例如,该自动消息可通知当前用户该移动设备已丢失或失窃、及时归还该移动设备将得到酬劳、和 / 或提供用于将该移动设备归还给授权用户的指示。该自动消息还可通知当前用户可按压该移动设备上的任何按钮以发起找回过程、和 / 或无需键入电话号码就能联系到用于将设备归还给其合法所有者的一方。在这种情况下,移动设备可接受单按钮按压以发起与安全机构或授权用户联系,从而开始找回过程。该消息可以任何方式呈现,诸如音频消息、文本消息、和 / 或视频消息。在本发明的一个实施例中,例如由安全机构向移动设备传送 SMS 文本消息。该文本消息被解码并且一命令被发送给驻留在移动设备上的应用,诸如 web 浏览器、文本编辑器、图形图像显示器、消息屏幕、或位图显示器,和 / 或能够显示通知的任何其他应用。该命令例如可显示预先存储的消息或图像,指示用户关于将设备归还给授权用户。应用可驻留在移动设备内的硬件组件上,诸如安装在移动电话或膝上型计算机中的 SIM 卡。也可在任何合需时间或响应于任何合需事件来呈现该消息,诸如在当前用户尝试利用该移动设备时(例如,通过在移动电话上拨出呼叫)。例如,可在该设备启动时呈现该消息。以此方式,发现丢失设备的用户可在即使该设备尚未与主机服务器(诸如由安全机构操作的主机服务器)建立连接的情况下获得关于归还该设备的信息。

[0080] 可更改移动设备的功能以抑制用户利用该移动设备的能力 (620)。例如,在当前用

户尝试使用该移动设备时,可在该移动设备的扬声器上播放 DTMF 音调序列(例如,对于移动电话)或不舒适的声音。此外,移动设备上的显示器的照明等级可被修改以阻挠对移动设备的使用(例如,通过降低照明等级)和/或将注意力吸引到该移动设备(例如,通过提高照明等级)从而旁观者可注意到该设备或其未授权使用。

[0081] 可响应于安全损害事件抑制移动设备的预定的一组特征,诸如当授权用户报告移动设备被失窃或丢失时。在本发明的一个实施例中,例如可基于在发生安全损害事件时要限制的特征列表来修改移动设备的功能。该特征列表可以任何方式定义,诸如通过授权用户访问 web 接口并选择若移动设备丢失或失窃则要禁用的特征。该特征列表随后可被传送给移动设备并由其存储。可向移动设备提供针对各种安全损害事件的一个或更多个特别配置的特征列表,例如一个列表可指示若电话被报失窃则可禁用该列表上的较多特征,而在电话被报告忘记放在何处时可提供较少限制的列表。以此方式,可基于已发生的安全损害类型针对事件恰当响应提供移动设备的多个特征修改列表。在另一实施例中,若移动设备检测到安全损害事件并且授权用户或经验证安全机构尚未将其他限制特征列表传送给该移动设备,则该移动设备可执行默认安全损害行动列表。举例而言但不限制,默认安全损害行动列表定义在丢失对移动设备的控制时需要改变的移动设备的公共特征。替换地,该特征列表可由用户通过移动设备本身上的软件接口来标识。

[0082] 基于发生安全损害事件,移动设备的功能可从第一特征集合修改为第二特征集合。第一特征集合与第二特征集合之间的差别可基于任何合需准则,诸如使用移动设备的上下文。例如,这些特征集合可基于移动设备所需的安全等级、移动设备正被用于的应用、移动设备的位置、或任何其他上下文因素。

[0083] 可以任何其他合需方式来抑制移动设备的功能。例如,可阻止移动电话拨出电话呼叫、发送电子邮件或文本消息、或进行其他形式的通信。在移动设备包括移动电话的情形中,可从该移动设备呼叫的电话号码可被限于预定号码列表、或仅移动电话上的联系人列表内的一个或更多个预定号码。例如,移动设备可被限于仅允许拨出紧急呼叫、和/或拨出对安全机构的呼叫(例如,用户可按压单个键来拨出对安全机构的呼叫)。此外,可在移动电话正在使用中时在移动设备的扬声器上播放 DTMF 音调,以干扰当前用户使用该移动设备。类似地,可提供频繁的消息(例如,文本消息和/或音频消息),指示移动设备的当前用户联系安全机构以发起将该移动设备归还给授权用户。还可锁定移动电话的订户身份模块(SIM)直至用户输入个人解锁代码。解锁代码可以是授权用户在发生安全损害事件之前已知的,或者可以由安全机构提供给授权用户。此外,授权用户可通过主机服务器(诸如由安全机构操作的服务器)来解锁移动设备。可(部分或全部)禁用移动设备的任何其他功能或对其进行干扰,以减少该移动设备对未授权用户的有用性。

[0084] 可通过在当前用户可使用移动设备之前要求输入口令来抑制移动设备的功能。在输入无效口令的情况下,在当前用户可尝试输入另一口令之前可附加地引入延迟。结合要求口令,可提供给出关于如何归还该移动设备的指示的可选择标记(例如,显示器上的 web 连接和/或按钮)。该指示可在无需当前用户输入有效用户 id 和口令的情况下提供。此外,可提示当前用户输入他或她的标识信息,其被存储在移动设备上并在移动设备有机会作出与安全机构的通信连接时被传送给安全机构。这可允许安全机构定位设备的无辜发现者、以及偷窃该设备的某人。举例而言但不作为限制,该提示可包括通知该设备的当前用户他

们已赢得大奖且需要采取行动才能兑换该奖品的消息。在这种情形中,设备的当前用户可能被怂恿提供本来是用来兑换该虚假奖品但事实上被用于定位和或逮捕当前用户的信息。替换地或者组合地,可向移动设备的当前用户发送带有鼓励当前用户打开消息或文件的名称或图像的图形图像,且在看该文件或图像时,经由隐写技术从该图像解码命令,从而移动设备可执行该命令以缓解失去对该移动设备的控制。

[0085] 移动设备可被明显禁用或完全关机以阻止其使用并帮助阻止未授权用户尝试规避移动设备上的安全保护。在一些情形中,诸如当存储在移动设备上的信息是敏感的时,或者当找回该移动设备(或其数据)的可能性很小时,命令移动设备执行使得该移动设备不能操作的破坏性功能可能是合需的。破坏性功能可包括擦除和/或覆盖移动设备上所存储的数据和软件。破坏性功能还可包括物理地破坏移动设备的硬件,诸如通过命令移动设备释放电荷或电流以破坏移动设备的电子组件。

[0086] 可更改移动设备的功能以向该设备的授权用户、安全机构或其他接收方发送消息(630)。该消息可包括任何合需信息,诸如移动设备呼叫的电话号码、移动设备的当前操作状态、移动设备的位置、指示移动设备已从预定位置移走和/或处于移动中的陈述、指示在发生安全事件之后移动设备被首次使用时的日期和时间戳、和/或呼叫安全机构以发起找回过程的指示。移动设备由此可提供关于其使用和位置的信息以辅助安全机构或授权用户寻找该移动设备。

[0087] 移动设备的授权用户可能不一定知道已发生安全损害事件。为了提醒授权用户已发生安全损害事件,关于授权用户的偷窃通知记录可被存储在中央服务器上以及移动设备本身上以允许联系和通知授权用户。偷窃通知记录可包括关于授权用户的任何合需信息,诸如授权用户的联系信息以及可用于验证授权用户的身份的信息。给授权用户的消息可以是任何格式的并且可包括任何合需信息。例如,可向偷窃通知记录中指定的电话号码拨出电话呼叫,从而向授权用户提供关于如何联系移动设备的当前用户以找回该移动设备的音频指示(来自现场操作者或预记录的)。同样,可电子地发送文本消息、或者可通过常规邮件发送印刷消息到偷窃通知记录中指定的地址,该消息关于如何联系移动设备的当前用户以找回它。该消息可由系统、设备或个人提供,诸如监视移动设备的安全机构和/或该移动设备本身。

[0088] 可更改移动设备关于处理去往和来自该移动设备的通信的功能(640)。除了如上所讨论地禁止或限制去往和来自该设备的通信,未授权用户从该设备作出的通信可被截取并被转发给安全机构、授权用户或其他接收方以辅助标识未授权用户和移动设备的位置。以此方式,本发明将把定向到授权用户的丢失或失窃设备的呼叫路由到由授权用户指定的替换号码;授权用户随后将能够接收到否则会遗漏的呼叫。在移动设备包括移动电话的情形中,未授权用户拨打的电话号码可被记录并被传送给安全机构和/或授权用户,并且可在移动设备正进行电话呼叫时提醒授权用户和/或安全机构。第三方(诸如安全机构)可请求接入该电话呼叫,并且随后建立与该电话呼叫的会议连接。第三方可主动参与该对话或秘密地听取该对话。

[0089] 可通过任何合需方式诸如通过加密来保护移动设备上存储的数据(650)。所存储数据的任何部分可被加密,诸如(例如,通过列表、文件上的标志、文件的位置、或其他方法)指定成在发生安全损害事件时将被加密的文件或其他数据元素。替换地,文件和数据



元素可在它们被创建时加密,从而即使在确定安全损害事件之前它们也不能被未授权用户查看。授权用户可指定要加密的个体文件、以及要加密的文件的类型。除加密之外或作为加密的替换,可从移动设备的文件系统隐藏文件以阻止未授权用户访问它们。授权用户可通过例如独立于移动设备的操作系统的、验证用户被授权访问这些文件的软件应用来访问此类文件。

[0090] 指定的文件可独立于移动设备的操作系统被加密,诸如通过加密/解密文件并允许用户访问它们的独立软件应用。操作系统因此被阻止访问此类文件,从而防止未授权用户利用操作系统中的安全漏洞来查看受保护文件。打开此类文件的操作系统调用可被截取,并且若当前用户被授权访问这些文件则这些文件被打开和解密。类似地,关闭此类文件的操作系统调用可被截取并且独立软件应用关闭和解密这些文件。存储在移动设备上的文件可以任何合需方式来加密和解密,诸如通过安全机构和/或授权用户已知的口令。

[0091] 在本发明的一个实施例中,例如为了提高对移动设备上所存储的数据的保护等级,可修改移动设备上的口令以利用更安全的口令,例如通过使用更长和/或更复杂的口令代码、或在移动设备不受口令保护的情况下设置口令。通常,这些更安全或强度加强的口令被视为将不用户友好且往往不被授权用户用作最初口令。因此,本发明的实施例可取决于移动设备的安全状态和上下文自适应地修改移动设备上的口令的强度。

[0092] 响应于安全损害事件可擦除移动设备上所存储的一些或全部数据以保护其不受未授权访问。可擦除任何合需文件或其他数据元素。例如,授权用户可指定在发生安全损害事件时将被删除的数据元素列表。此外,被删除数据元素可被其他数据覆写以防止对该数据的恢复。被删除的数据可被覆写任何合需次数以及用任何合需数据(诸如随机数据、交替的数据值、预定数据模式、及其组合)来覆写。

[0093] 移动设备上所存储的一些或全部数据可进一步被存档以允许授权用户恢复该数据,即使没找回该移动设备亦然。如同标记为加密和/或删除的文件一样,授权用户可以任何合需方式指定要存档的特定文件或其他数据。授权用户也可指定在安全损害事件的情况下应当将存档的数据发送给哪一个或更多个目的地,诸如安全机构、主机服务器、或授权用户能访问的替换设备(例如,相同类型的另一移动设备或中央数据服务器)。所存档的数据可从移动设备传送给指定目的地,结合在成功传递时加密或删除该数据。授权用户随后可将所存档的数据恢复到代替移动设备,或者可指示将所存档的数据递送给任何其他合需目的地。例如,授权用户可指定可将电子副本或物理副本(例如,存储在便携式存储介质上的所存档数据)递送给哪个目的地址(诸如电子邮件地址或物理邮寄地址)。移动设备上所存储的任何类型的数据都可被存档,诸如文档、电子邮件或电话联系信息、软件应用、媒体文件、和/或照片。此外,涉及一个或更多个数据元素的许可信息可被存档。

[0094] 数据可在任何时间被存档,包括在发生安全损害事件时、根据预定时间表、和或在由授权用户、安全机构、或其他授权实体指定的时间。

[0095] 本发明的系统和方法可将敏感数据存储于指定位置以供在发生安全损害事件时作特殊处理。指定位置可以是存储器中的物理位置、以及通过移动设备的文件系统指定的位置。例如,授权用户可将敏感数据元素存储在移动设备的文件系统上的特殊文件夹中。当发生安全损害事件时,可对该文件夹内的数据元素执行一个或更多个功能,诸如用授权用户和/或安全机构已知的口令来加密这些敏感数据元素中的一个或更多个,删除这些敏感

数据元素中的一个或多个,多次覆写这些敏感数据元素中的一个或多个,和/或将这些敏感数据元素中的一个或多个传送到授权用户指定的地址。对文件的特殊指定尤其允许在安全损害事件的情形中在处理较不敏感的数据之前迅速保护、存档和/或破坏重要数据。

[0096] 可更改移动设备的功能以辅助在发生安全损害事件之后跟踪该设备(660)。例如,移动设备可确定指派给该移动设备的网络地址(包括无线网络地址)、以及来自该移动设备接收到的信号的无线接入点标识符。移动设备可存储该地址和标识符并将其传送给安全机构。安全机构随后可基于这些网络地址和无线接入点标识符来确定移动设备的位置。

[0097] 类似地,移动设备可从GPS或提供地理位置信息的其他源接收信号。来自该信号的地理位置信息可被存储并被传送给安全机构。从移动设备接收到位置信息的安全机构或授权用户可在地图覆盖上呈现该位置以跟踪移动设备的当前位置、以及移动设备的任何位置改变的日期和时间。移动设备位置的地图可通过网站在因特网上提供以允许警察或其他安全机构成员定位该移动设备。

[0098] 可更改移动设备的功能以搜集关于未授权用户正如何使用该移动设备的信息并将该信息提供给授权用户或安全机构以辅助定位该设备和/或未授权用户(670)。例如,在发生安全损害事件之后向其发送消息的电话号码和电子邮件地址可被移动设备存储并被传送给安全机构。移动设备板载的数据捕捉装备(诸如数码相机或话筒)可被用于搜集关于移动设备的用户、移动设备的目前环境的信息。例如与移动设备通信的相机可被激活以捕捉静态图像或视频剪辑,它们可被存储在移动设备中并被传送给安全机构。类似地,可使用话筒来捕捉音频剪辑。诸如相机和话筒之类的数据捕捉装备可被用来获取连续数据样本以帮助定位该设备、抑制未授权用户对数据捕捉设备的使用、和/或耗尽移动设备的电池以减小其对未授权用户的有用性。替换地,数据捕捉设备可被禁用以保持电池寿命和/或防止其被未授权用户使用。

[0099] 为了帮助捕捉未授权用户的脸部图像,移动设备可提示用户采取涉及看该移动设备的活动,诸如提示用户输入口令、播放移动设备上的音序列、闪烁移动设备上的光源、通知当前用户已赢得奖品并指示他/她观看奖品兑换细节、和/或显示视频序列。在当前用户的注意力集中在移动设备上时,可使用相机来捕捉他/她脸部的图像以传送给安全机构。类似地,与移动设备通信的相机或话筒可被激活,结合发起与安全机构的秘密通信会话。移动设备捕捉的静态图像、视频和音频数据随后可被传送给安全机构。安全机构可使用未授权用户的图像/视频来标识他/她(例如,通过将该图像/视频与警局备案照片作比较),并且还可使用该图像/视频来标识移动设备的周围环境。还可从未授权用户的声音(从捕捉到的音频剪辑获取的)的样本来标识未授权用户。

[0100] 如以上所讨论的,发送给/自移动设备的消息可被截取和/或重新路由到安全机构以阻止对该设备的未授权使用并帮助标识未授权用户和/或移动设备的位置。此外,移动设备可被配置成维护在移动设备上按压的每个键的记录,并将该日志传送给授权用户或安全机构。以此方式记录键击可进一步帮助通过捕捉未授权用户输入的用户名、口令、联系人条目以及其他信息标识未授权用户。

[0101] 根据本发明,除了被动地从移动设备接收数据以外,授权用户或安全机构可主动地访问或命令移动设备。安全机构或授权用户可向移动设备传送执行各种功能的命令,以

及提供将由移动设备处理的软件更新、小应用程序 (applet)、可执行代码小节、可解释脚本、或数据元素。因此在发生安全损害事件时以及在任何其他合需时间,可向移动设备提供执行各种任务的软件。

[0102] 在本发明的一个示范性实施例中,安全机构和 / 或授权用户可登录配置成与移动设备通信的远程接入服务并激活移动设备中的应用编程接口,以将移动设备的当前状态、移动设备的当前位置、由与移动设备通信的相机拍摄的图像、由与移动设备通信的相机捕捉的实时视频、移动设备上按压的键列表、和 / 或当前在移动设备上运行的服务列表转发给该远程接入服务。此外,授权用户或安全机构可向移动设备发出命令以发起聊天会话并在移动设备上提供用于实现与当前用户的基于文本的交互的界面。

[0103] 可更改移动设备的功能以与其他设备通信从而辅助定位和找回该移动设备 (680)。例如,现在参照图 7,与其他设备通信 (680) 可包括发起该移动设备与无线收发机之间的无线连接 (710)、通过无线收发机将关于移动设备的当前位置的信息中继到安全机构 (720)、向无线收发机传送消息 (730)、以及向第二无线收发机传送消息 (740)。

[0104] 移动设备可通过无线收发机发起任何设备、系统或个人之间的连接,并且可使用任何合需的通信协议连接到无线收发机。移动设备可连接到任何数目个无线收发机。一旦连接到无线收发机,移动设备就可将关于该移动设备的当前位置的任何合需信息、以及该移动设备上所存储的文件和数据中继到安全机构。例如,发起与连接到因特网的无线接入点 (WAP) 的连接,移动设备可向安全机构发送电子邮件,该电子邮件包括文本和附件以辅助安全机构定位该设备以及逮捕该设备的未授权持有人。类似地,发起与蜂窝电话网络的连接的移动设备可拨打安全机构并通过音频消息和 / 或 DTMF 音调来提供关于移动设备的位置的信息。

[0105] 移动设备可向 (或通过) 与之发起联系的无线收发机提供任何其他合需信息。例如,在本发明的一个实施例中,移动设备可向无线收发机传送指示丢失或失窃设备位于该无线收发机可访问的信号范围内的消息。类似地,移动设备可确定其与无线收发机的无线连接的信号强度,并获得该无线收发机的标识标记 (诸如设备名称、IP 地址、或其他标识符) 并向不同的无线收发机传送包括该标识和信号强度信息的消息。多个无线收发机的信号强度和标识信息随后可被用于三角测量该移动设备的位置。此外,在无线收发机 (或与之通信的设备) 能够确定其自己的物理位置的情况下,移动设备可请求该无线收发机提供其物理位置,该物理位置又可被提供给安全机构。

[0106] 移动设备可向任何数目个无线收发机传送任何其他合需信息。在本发明的一个实施例中,例如,给无线收发机的消息可包括对包括与移动设备通信的无线收发机的物理位置的响应的请求、使与无线收发机通信的人报告丢失或失窃设备位于其通信范围内的请求、授权用户的电话号码、安全机构的电话号码、和 / 或向安全机构拨出呼叫的请求。

#### [0107] 示范性系统

[0108] 图 8 中描绘了与本发明结合使用的示范性系统。该系统可结合图 1-7 中描述的方法以及结合其要素的任何子集或组合来使用。图 8 中所示的系统也可结合本发明的任何其他合适实施例来使用。

[0109] 图 8 中描绘的示范性系统包括移动设备 800,移动设备 800 包括耦合到存储器 820 的处理器 810,存储器 820 可包括易失性存储器、非易失性存储器或其组合。通信模块 830

包括无线收发机 840,用于通过天线 850 与一个或多个服务器 860 及其他实体无线电通信。移动设备还包括耦合到处理器 810 的用户接口 870。移动设备 800 可包括任何合适的电源,诸如电池(未示出)。移动设备 800 可包括任何其他合需组件,诸如全球定位系统(GPS),用于提供用于定位移动设备的地理位置信息。移动设备 800 的一些或所有组件可包括硬件标识模块(未示出)(或与之通信),诸如通用订户身份模块和/或可移除用户身份模块。硬件标识模块可耦合到处理器 810 并且可包括标识符,该标识符可与预定标识符作比较以确定移动设备 800 的硬件是否已更改以及因此是否已发生安全损害事件。硬件标识模块(以及预定标识符)可包括任何合适标识符,诸如电子序列号、局域身份标识符、集成电路标识符、国际移动订户标识符、认证密钥标识符、和/或因运营商而异的紧急号码标识符。标识符可被存储在存储器 820 中并被传送给主机服务器 860 以与预定标识符作比较。

[0110] 移动设备 800 的功能,包括图 1-7 中描绘的方法(全部或部分),可通过处理器 810 执行在移动设备 800 的存储器 820 中所存储的计算机可读指令来实现。存储器 820 可存储任何计算机可读指令和数据,包括软件应用、小应用程序(applet)、以及嵌入式操作代码。在一个示例性实施例中,执行本发明的方法的软件应用包括终止及驻留(TSR)应用(或等效物),其配置成每当移动设备处于操作中时就保持加载在存储器中,这可以帮助阻止对 TSR 的无意或故意删除。该软件应用还可被隐藏(即,在应用列表或任务列表中不可见)和/或保护以免被用户或其他软件过程停止或删除。本发明的实施例的各方面提供防篡改应用以防止未授权用户禁用该应用或以其他方式将该应用从操作状态移除。在一个示例性实施例中,应用可被安装在运行 Symbian 操作系统的移动设备上,藉此正在运行的应用不能被卸载或禁用。

[0111] 此外,软件应用可被配置成以最低程度的底层硬件功能来操作。例如,该应用可在移动设备建立网络连接之前发起。例如当软件应用安装在移动设备的 SIM 卡中并且该应用在移动设备操作系统中的其他软件之前启动时,可提供这种状况。替换地或补充地,诸如链接或 URL(统一资源定位符)之类的数据元素可驻留在 SIM 卡上,并且通过用 URL 或链接启动诸如浏览器之类的应用,该链接或 URL 所引用的应用可从远程服务器被加载到移动设备中和/或直接从远程服务器上执行。

[0112] 可随设备提供执行本发明的方法的软件或由授权用户将该软件下载到移动设备上。移动设备 800 的功能也可通过各种存储机器可读指令的硬件组件来实现,诸如专用集成电路(ASIC)、现场可编程门阵列(FPGA)和/或复杂可编程逻辑器件(CPLD)。根据本发明的各方面的系统可结合软件和/或硬件组件的任何合需组合一起操作。

[0113] 处理器 810 检索并执行存储在存储器 820 中的指令以控制移动设备 800 的操作。可结合本发明使用任何数目和类型的处理器,诸如集成电路微处理器、微控制器、和/或数字信号处理器(DSP)。处理器 820 存储指令、数据、从移动设备 800 传送而来的(或由其接收到的)消息、以及任何其他合适信息。结合本发明操作的存储器 820 可包括不同存储器存储设备的任何组合,诸如硬驱动、随机存取存储器(RAM)、只读存储器(ROM)、闪存、或任何其他类型的易失性和/或非易失性存储器。数据可以任何合需方式存储在存储器 820 中。在本发明的一个实施例中,例如,存储在存储器 820 中的数据被划分成一个或多个逻辑上不相交的群。这些数据群中的每一个用相应的唯一性加密密钥来加密,以防止若单个加密密钥被损害则移动设备上的所有数据都被访问。这还增加了尝试所有可能的加密密钥以

获得成功的“蛮力”尝试将花的时间。数据群可跨多个物理存储介质划分,诸如 RAID 阵列。

[0114] 通信接口 830 与一个或更多个服务器 860 或其他合适实体通信。可结合本发明使用任何合适的通信设备、组件、系统和方法。例如,无线收发机 840 可被配置成使用任何数目和类型的蜂窝协议来通信,诸如通用分组无线电服务 (GPRS)、全球移动通信系统 (GSM)、增强数据率 GSM 演进 (EDGE)、个人通信服务 (PCS)、高级移动电话系统 (AMPS)、码分多址 (CDMA)、宽带 CDMA (W-CDMA)、时分同步 CDMA (TD-SCDMA)、通用移动通信系统 (UMTS)、和 / 或时分多址 (TDMA)。结合本发明操作的移动设备可替换地 (或补充地) 包括无线收发机 (以及相关组件) 以使用无线通信协议的任何其他方法来通信,诸如 ISO 14443 协议、ISO 18000-6 协议、蓝牙协议、Zigbee 协议、Wibree 协议、IEEE 802.15 协议、IEEE 802.11 协议、IEEE 802.16 协议、超宽带 (UWB) 协议、IrDA 协议、及其组合。天线 850 可被配置成发射和接收以任何格式的任何无线信号,并且可包括多个不同天线以使用不同无线协议来发射和接收。

[0115] 通信模块 830 可使用任何其他形式的连接与服务器 860 或另一设备通信,诸如有线因特网连接、无线因特网连接、蜂窝电话网络连接、无线 LAN 连接、无线 WAN 连接、光学连接、USB 连接、移动设备同步端口连接、电力连接和 / 或安全电缆。通信模块 830 可用于与一个或更多个同伴设备通信以监视移动设备 800 的位置或状态 (例如,通过监视移动设备与同伴设备之间的通信链路是否完好),以及与任何数目的其他设备通信以帮助跟踪 / 定位丢失或失窃移动设备 800。

[0116] 移动设备 800 包括用户接口 870。用户接口 870 可包括任何数目的输入设备 (未示出) 以接收来自用户的命令、数据和其他合适输入、以及任何数目的输出设备 (未示出) 以从移动设备 800 向用户提供数据、通知、和其他合适的信息。

[0117] 任何数目的输入设备可被包括在用户接口 870 中,诸如触摸板、触摸屏、和 / 或字母数字按键板,以允许用户向移动设备 800 中输入指令和数据。用户接口 870 可被配置成检测用户对按键板的键施加的压力、以及键按压之间的时间间隔以确定当前用户是否被授权使用该设备。用户接口还可包括话筒以允许用户向移动设备 200 提供音频数据、以及相机以允许移动设备捕捉静态或视频图像。移动设备 200 可包括语音识别软件以处理通过用户接口 870 输入的话语。用户接口 870 还可包括任何数目的合适输出设备,诸如用于视觉地显示信息 (诸如视频和文本) 的显示屏和 / 或用于提供听觉输出的扬声器。移动设备 800 可被配置成通过扬声器向用户提供单词、短语、音调、所记录的音乐、或任何其它类型的听觉输出。如先前所讨论的,在未授权用户尝试使用移动设备 800 时,用户接口 870 可被激活以提供信息和 / 或阻挠移动设备 800 的操作。例如,显示器的照明等级可被调节以将注意力吸引到该移动设备,以及可在扬声器上播放不舒适的和 / 或大声的声音。

[0118] 移动设备 200 可包括一个或更多个被配置成接收生物测定信息的生物测定设备,诸如指纹扫描仪、虹膜扫描仪、视网膜扫描仪、和 / 或呼吸分析仪。也可利用诸如话筒或相机之类的输入设备来执行生物测定分析,诸如语音分析或面部识别。

[0119] 用户接口 870 提供或接收的信息可以为任何恰适的格式。例如,以听觉格式向用户传达信息的用户接口可首先提供数据头,然后是数据值,以向用户标识该数据。用户接口 870 可以任何数目个合需语言来提供信息,不管该信息是听觉地还是视觉地提供的。

[0120] 用户接口还可以机器可读格式向用户提供 / 接收信息。在本发明的一个示例性实

施例中,例如移动设备 800 的用户接口 870 可使用双音多频 (DTMF) 音调来发送和接收消息。移动设备 800 可被配置成发送、接收和处理可以为任何标准格式(诸如 MS Word 文档、Adobe PDF 文件、ASCII 文本文件、JPEG、或其他标准格式)以及任何专用格式的机器可读数据。去往或来自用户接口的机器可读数据也可被加密以保护该数据以防非预期接收和/或不适当使用。在替换实施例中,用户必须输入通行码才能使用移动设备 800 的一些或全部功能。可利用任何其他用户接口特征来允许人类或非人类用户与结合本发明操作的一个或更多设备交互。

[0121] 移动设备 800 可包括任何其他合适的特征、组件和/或系统。例如,移动设备 800 可被配置成通过关闭其组件中更多一些或全部(诸如相机或话筒)来保存其电池的寿命。可响应于安全损害事件以及响应于来自授权用户或安全机构的命令选择性地关闭组件。替换地,移动设备 800 可被配置成过度使用其组件以尽快耗尽电池,从而例如限制移动设备 800 对未授权用户的有用性。

[0122] 移动设备 800 可被配置成实现一个或更多安全措施以保护数据、限制访问、或提供任何其他合需安全特征。例如,移动设备 800 可加密所传送的数据和/或存储在设备自身内的数据。此类安全措施可使用硬件、软件或其组合来实现。可结合本发明利用任何数据加密或保护方法,诸如公钥/私钥加密系统、数据加扰方法、硬件和软件防火墙、防篡改或篡改响应存储器存储设备或用于保护数据的任何其他方法或技术。类似地,可采用口令、生物测定、存取卡或其他硬件、或任何其他系统、设备和/或方法来限制对结合本发明操作的任何设备的访问。

[0123] 主机服务器 860 与移动设备 200、授权用户、未授权用户、安全机构以及其他实体通信以监视和保护移动设备 200 以免未授权使用以及缓解与安全损害事件相关联的伤害。主机服务器 860 可包括任何数目的单独计算机系统、处理器和存储器存储设备、和人类操作者(例如,以应答来自授权用户的报告移动设备的丢失/偷窃的呼叫)以及任何其他合适实体。主机服务器 860 可包括一个或更多个存储关于授权用户和移动设备 200 的信息的数据库 880 或与之通信,以监视和跟踪移动设备 200 以及在发生安全损害事件的情况下向移动设备 200 提供指示。

[0124] 例如,数据库 880 可存储移动设备的使用简档以允许主机服务器 860 上的软件检测对移动设备的持续使用是否偏离使用简档达预定阈值。主机服务器 860 还可接收、处理和存储(例如,在数据库 880 中)来自移动设备 800 的信息。主机服务器 860 可处理以任何格式的任何类型的数据以达成任何目的,诸如接收和处理由移动设备捕捉到的环境参数以如先前所讨论地跟踪移动设备 800 的定位和位置。数据库 880 还可存储用来确定移动设备 800 是否在有效位置(例如,先前所讨论的“白名单”和“黑名单”)中操作的位置信息。

[0125] 与主机服务器 860 通信的数据库 880 还可存储来自移动设备 800 的存档数据以在移动设备 800 丢失或失窃、或移动设备 800 上的数据被(例如,病毒或其他恶意程序)破坏的情况下进行恢复。主机服务器 860 的功能可自动或半自动地执行,诸如通过在一个或更多个计算机系统上操作的软件/硬件、和/或由一个或更多个人类操作者执行。

[0126] 主机服务器 860 可包括一个或更多个系统处理器,其检索并执行存储器中所存储的计算机可读指令以(至少部分地)控制主机服务器 860 的操作。可结合本发明使用任何数目和类型的常规接收机、计算机系统、计算机网络、接收机工作站、微型接收机、大型接

收机、或接收机处理器,诸如集成电路微处理器或微控制器。根据本发明各方面使用的计算机系统可包括操作系统(例如,Windows NT、95/98/2000/XP/Vista、OS2、UNIX、Linux、Solaris、MacOS等)、以及通常与接收机相关联的各种常规支持软件和驱动程序。在某些实施例中,系统处理器可完全或部分地服务或执行专用应用以执行本发明的方法。

[0127] 主机服务器 860 可以任何合需方式被访问,诸如通过因特网上的网站、和/或通过电话网。主机服务器 860 可包括用于与用户、安全机构、计算设备或其他实体通信的任何数目的人类操作者、计算机系统、移动电话、移动计算设备、交互式语音响应(IVR)系统、以及任何其他合适系统和设备。在本发明的一个示例性实施例中,希望订阅提供监视和保护其移动设备的服务的授权用户可访问由主机服务器 860 主存的网站以创建帐户、为该服务付费、标识要保护的一个或多个移动设备、选择该服务的选项、标识在移动设备丢失或失窃的情况下应如何更改该设备的功能(例如,要实现或限制的特征)、选择要在呼叫方 ID 数据流中递送的替换呼叫方标识标记(诸如文本)、报告安全损害事件(诸如该设备的丢失/偷窃)、和/或下载用于在其移动设备上操作以帮助监视和保护该移动设备的软件。替换地,授权用户可在电话网上与自动 IVR 系统和/或人类操作者接口。在移动设备丢失或失窃的情况下,授权用户可与主机服务器 860 接口以报告安全损害事件(即,该设备的丢失/偷窃)、跟踪移动设备的状态/位置、恢复从移动设备存档并由主机服务器 860 存储的数据、和/或提供关于安全损害事件的信息(诸如报告该设备已被授权用户定位)。可如上所讨论地或以任何其他方式保护去往和来自主机服务器 860 的通信(例如,通过加密)。

[0128] 主机服务器 860 可通过丢失或失窃的移动设备或通过其他通信方法与该移动设备的未授权用户通信。主机服务器 860 可通知未授权用户该移动设备丢失或失窃,向未授权用户提供找回信息(诸如运输地址)、以及促进向归还该移动设备的未授权用户递送酬劳。主机服务器 860 还可与移动设备 800 通信以提供软件更新、接收数据以存档、标识要保护的文件或其他数据、以及执行本发明的任何其他方面。

[0129] 主机服务器 860 可由授权用户、电信服务提供方、移动设备监视/跟踪服务提供方、安全机构、和/或任何其他合需实体控制或与之结合地操作。例如,授权用户和安全机构可与主机服务器 860 通信或通过主机服务器 860 通信以监视移动设备 800 以及若其丢失或失窃则找回移动设备 800。主机服务器 860 可被配置成提供关于如何归还丢失/失窃的移动设备 800 的通知、检测安全损害事件、以及确定是否应当更改移动设备的功能以及(若如此则)确定应当更改移动设备 800 的功能的方式,如图 1-7 中所描绘并在先前所讨论的。主机服务器 860 可结合任何其他合需系统、设备、人类操作者、或其他实体来操作。

#### [0130] 操作

[0131] 图 9-64 描绘了根据本发明的示例性实施例的操作的各方面。图 9-16 描绘了根据本发明的可在诸如膝上型计算机之类的移动计算设备上提供的示例性通知措施。如所解说实施例中所示,接近用户通常登录或访问移动计算设备的输入区域提供通知图标或图形。该通知图标或图形伴随有提供关于归还该设备的信息的文本。各种通知消息允许移动设备的发现者看到该设备受结合本发明操作的应用保护,并且提供信息以允许用户归还该设备。例如,现在参照图 13,屏幕 1300 提供了无辜发现者能点击以归还该设备的至网站的链接。类似地,现在参照图 14,屏幕 1400 提供了供该设备的发现者输入他或她的名字(name)、电话号码(phone)、以及电子邮件地址(email)并将该信息提交(submit)给安全机构的输

入区域。图 15 中的屏幕 1500 和图 16 中的屏幕 1600 提供免费电话号码和关于如何归还移动设备的信息。

[0132] 图 17-25 描绘了可在蜂窝电话、PDA、或手持移动设备上显示的示例性通知消息。这些通知消息提醒移动设备的发现者该设备受结合本发明操作的应用保护，并且提供信息以允许用户归还该设备。例如，现在参照图 18 和 22，通知消息可包括用户可选择以归还该移动设备的按钮。图 19、20 和 21 描绘了在所发现移动设备的用户诸如向安全机构拨出呼叫时可显示的通知消息。参照图 23，通知消息可包括与移动设备相关联的标识号以及任何其他合需信息。

[0133] 根据本发明保护的移动设备的用户可与主机服务器接口，诸如通过网站与由安全机构管理的主机服务器接口。图 26-37 描绘与如本发明的实施例所例示的主机服务器相关联的示例性屏幕和过程。用户可被给予签约服务的机会，以根据本发明来保护一个或多个计算设备（图 26-34）。在用户已创建帐户以后，他/她可将软件应用下载到要保护的移动设备，如图 29 中的流程图 2900 描绘的。由此向用户提供关于该安全应用的安装和使用的信息（图 30）。参照图 31，在用户已下载和安装该产品并且已重启移动设备（若需要）之后，一旦网络连接可用，该应用将使用诸如先前从主机服务器获得的标识符标签之类的唯一性标识符启动浏览器去到一网页。如图 32-33 中所示，还通过浏览器屏幕向用户呈现注册信息概述，并且该屏幕可呈现由该服务保护的多个设备的列表。

[0134] 用户可被给予签约服务的机会，以根据本发明来保护一个或多个移动设备。图 34 解说了根据本发明的用于创建帐户以及注册移动设备的示例性过程。用户创建帐户（图 35）、选择移动设备（图 36）、以及完成注册（图 37）。

[0135] 图 38-55 涉及下载到移动设备上的软件应用的安装和注册。用户发起安装程序（图 38）、同意许可协定（图 39）、选择该软件应用在移动设备的文件系统中的目的地（图 40）、以及确认安装该软件应用（图 41）。安装验证该软件应用正确地安装，且若否，则重新发起安装程序（图 42-47）。用户向主机服务器注册该软件应用（图 48-57）。根据本发明保护的移动设备的发现者可定向到由主机服务器主存的网页，其允许发现者报告该移动设备已被找到（图 58）。在合需的情况下，授权用户可从移动设备卸载该应用（图 59-64）。

[0136] 以上所示和所描述的特定实现是为了解说本发明及其最佳模式，且无意以任何方式限制本发明的范围。实际上，出于简明起见，可能没有详细描述这些系统的常规数据存储、数据传输、和其他功能方面。在各附图中解说的付费可包括更多、更少或其他步骤。此外，可以任何合适次序执行各步骤而不会脱离本发明的范围。此外，各附图中示出的连接线意在表示各元件之间的示例性功能关系和/或物理耦合。实践系统中可存在许多替换或附加功能关系或物理连接。

[0137] 可对所公开实施例作出各种改变和改动而不会脱离本发明的范围。这些和其他改变和改动都旨在被包括在本公开如所附权利要求表达的范围之内。



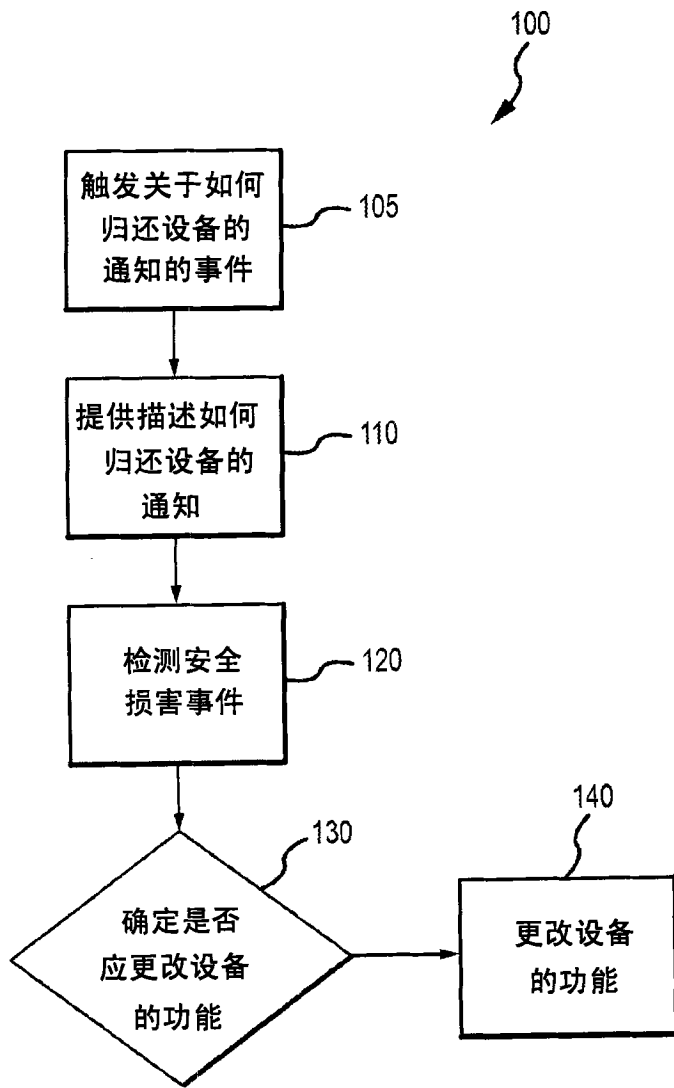


图 1

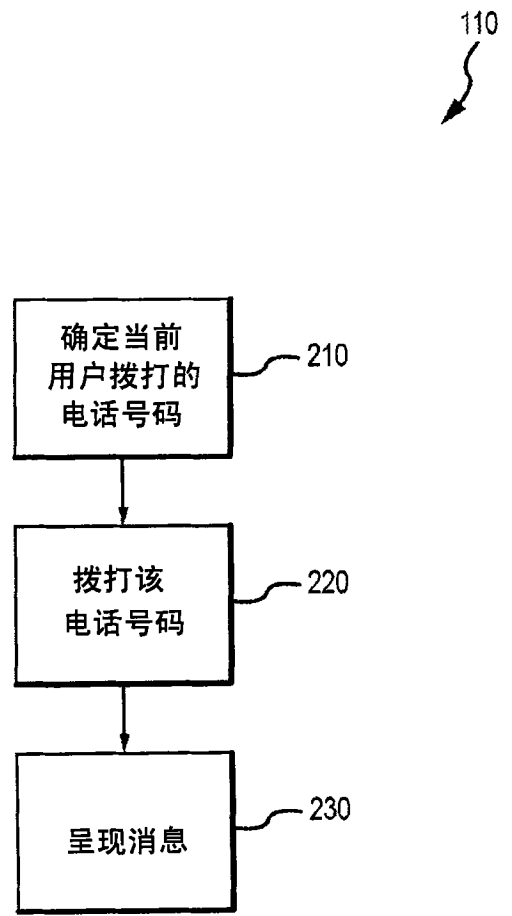


图 2

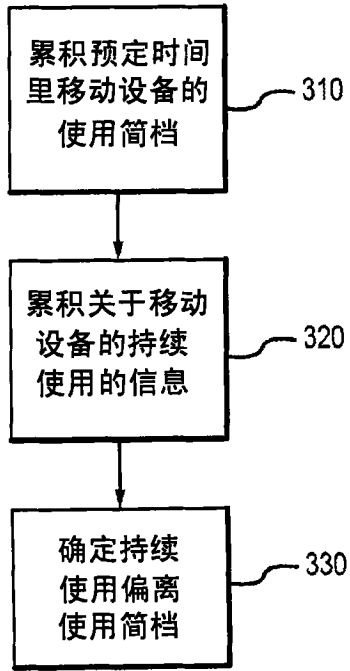
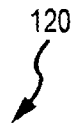


图 3

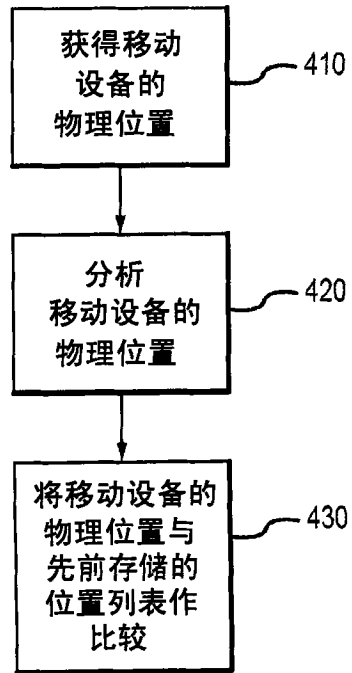


图 4

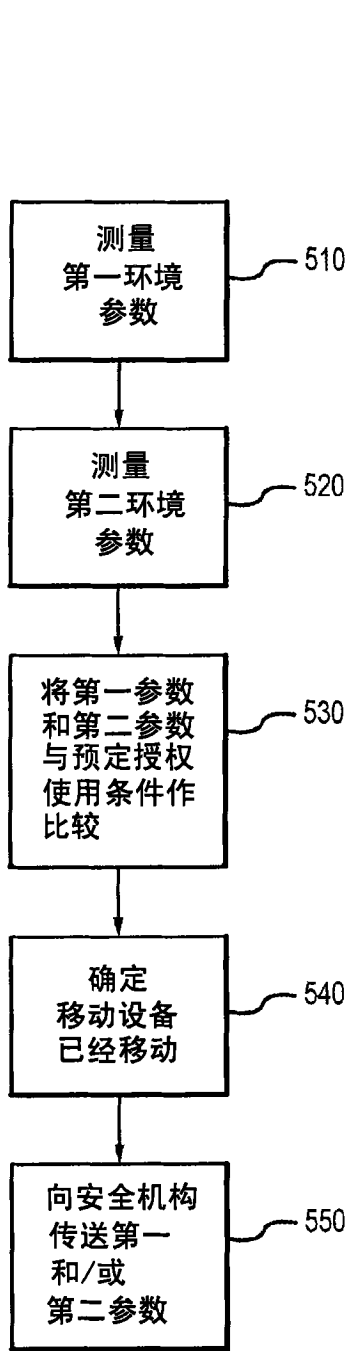


图 5

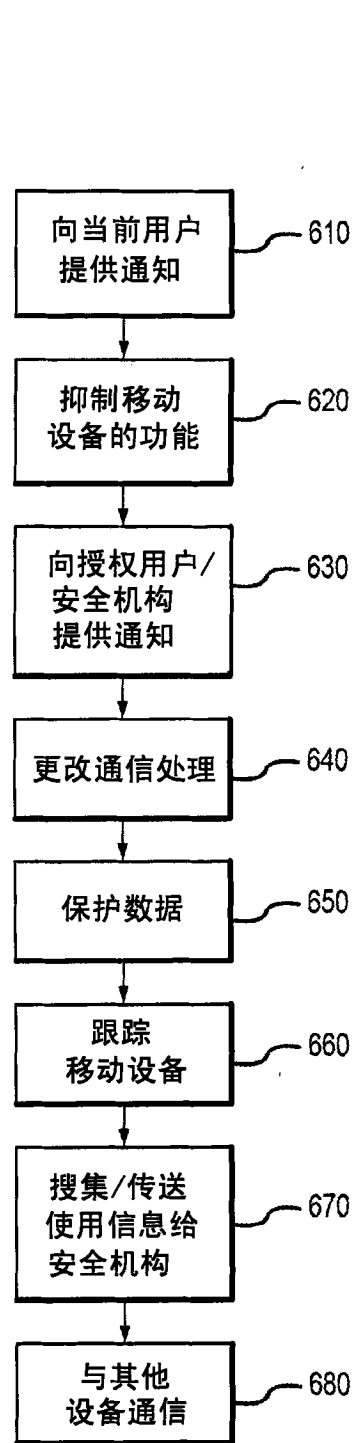


图 6

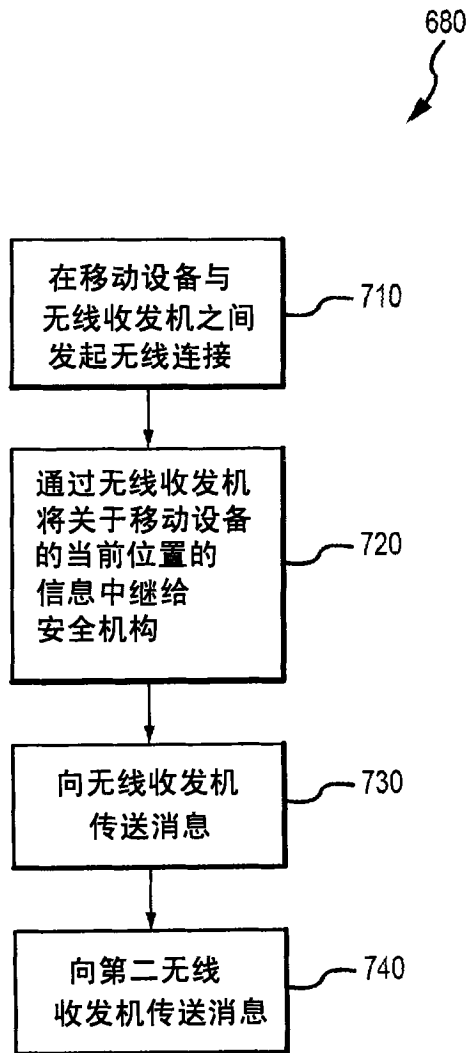


图 7

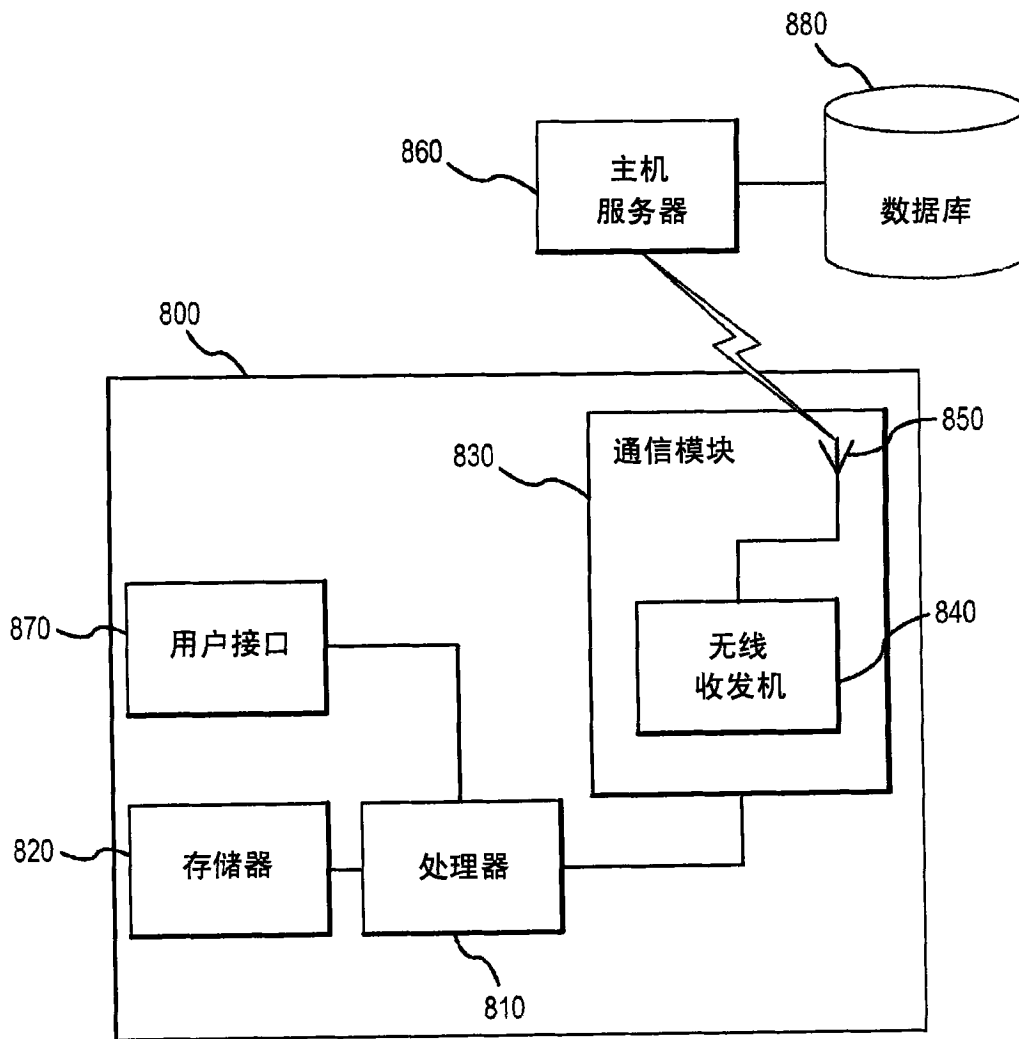


图 8

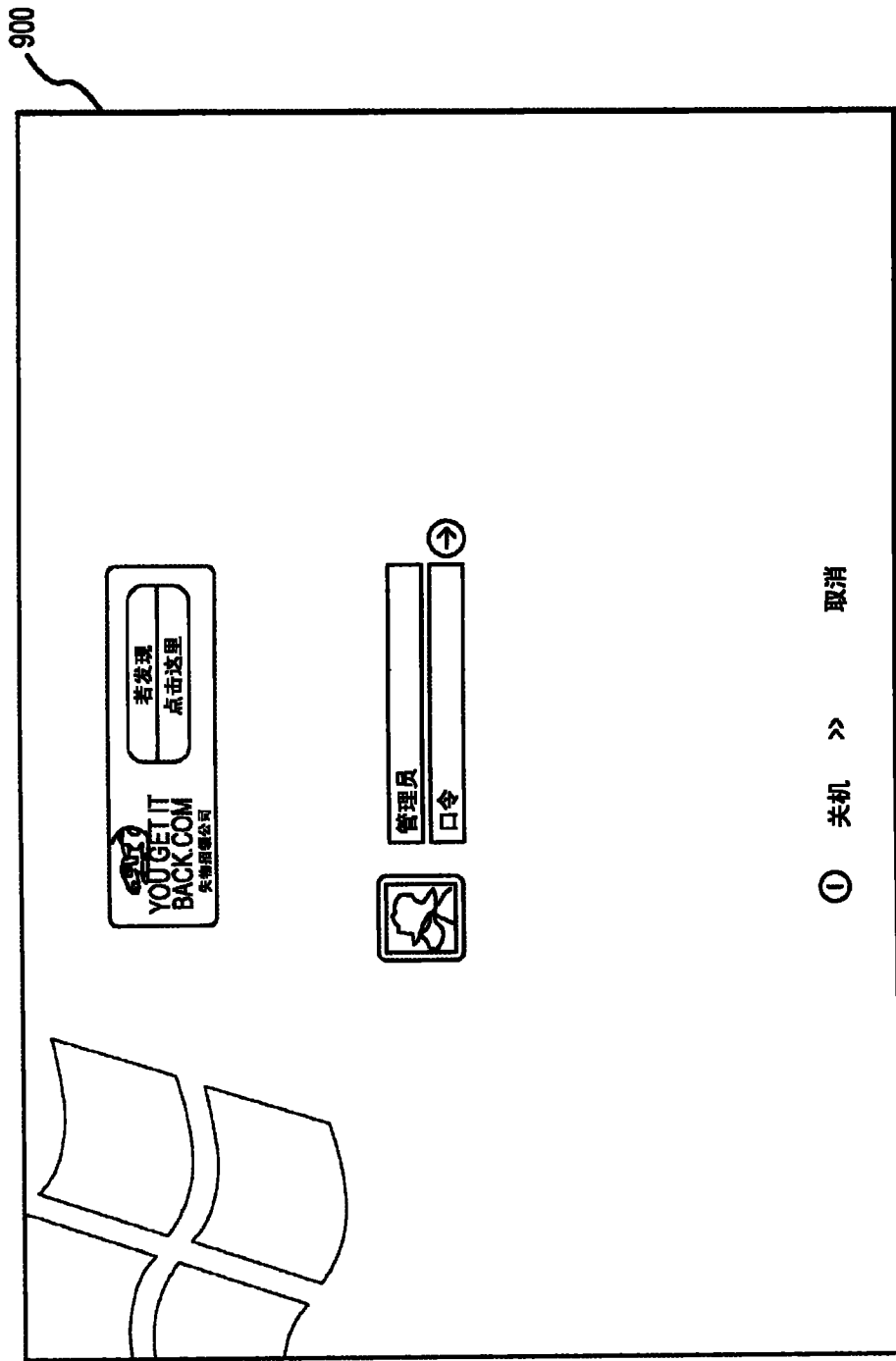


图 9

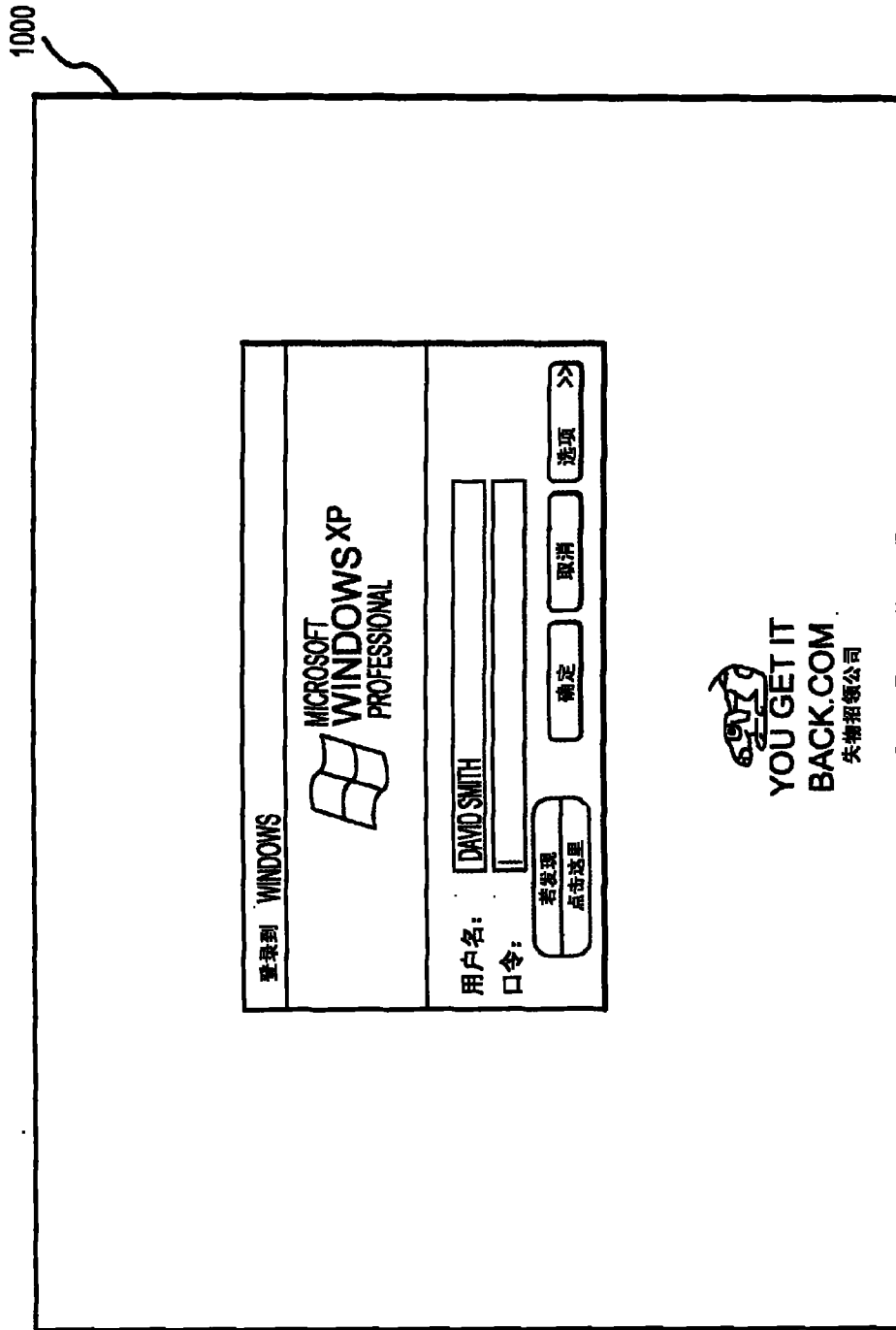
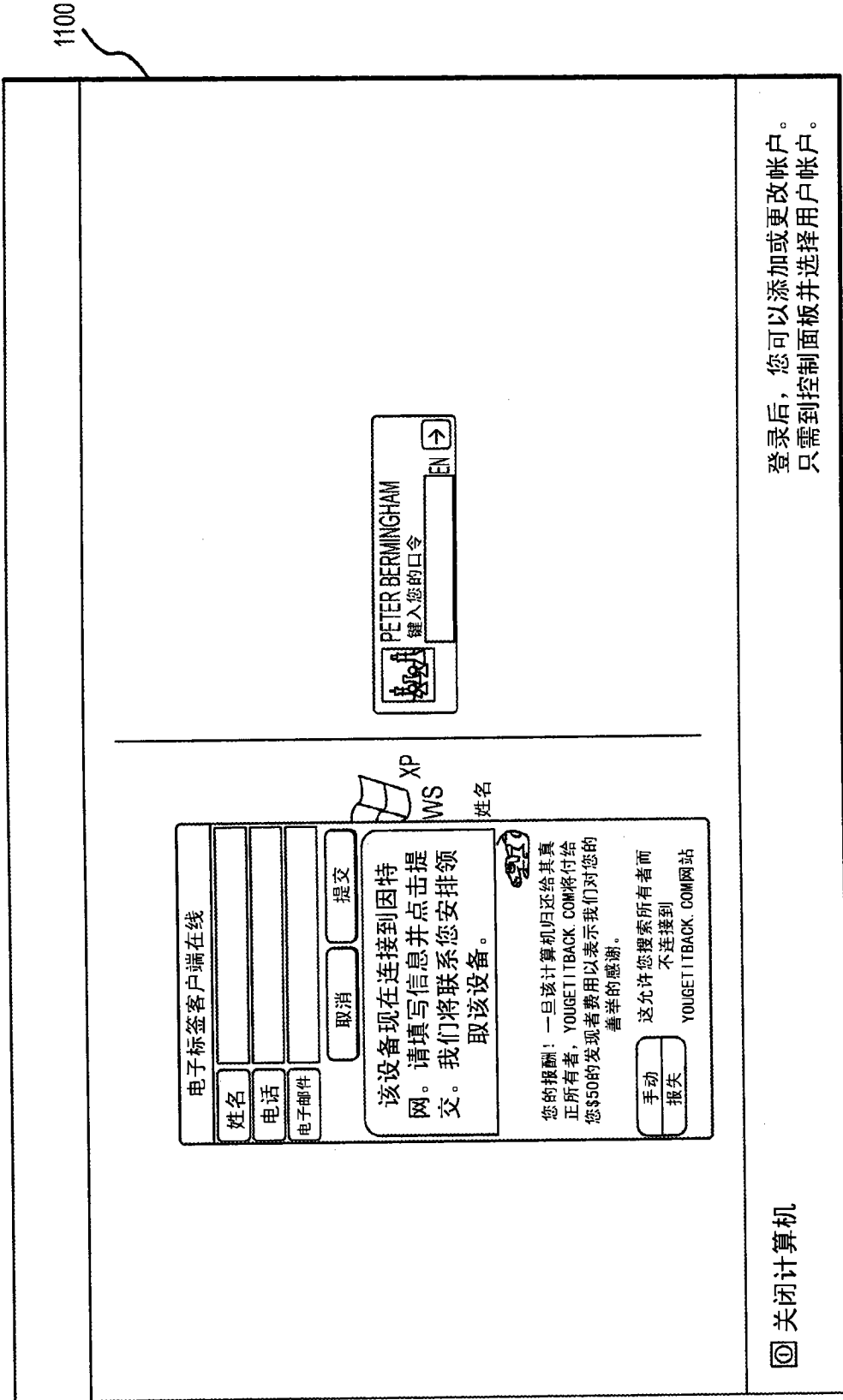


图 10



登录后, 您可以添加或更改帐户。  
只需到控制面板并选择用户帐户。

关闭计算机

图 11



1200

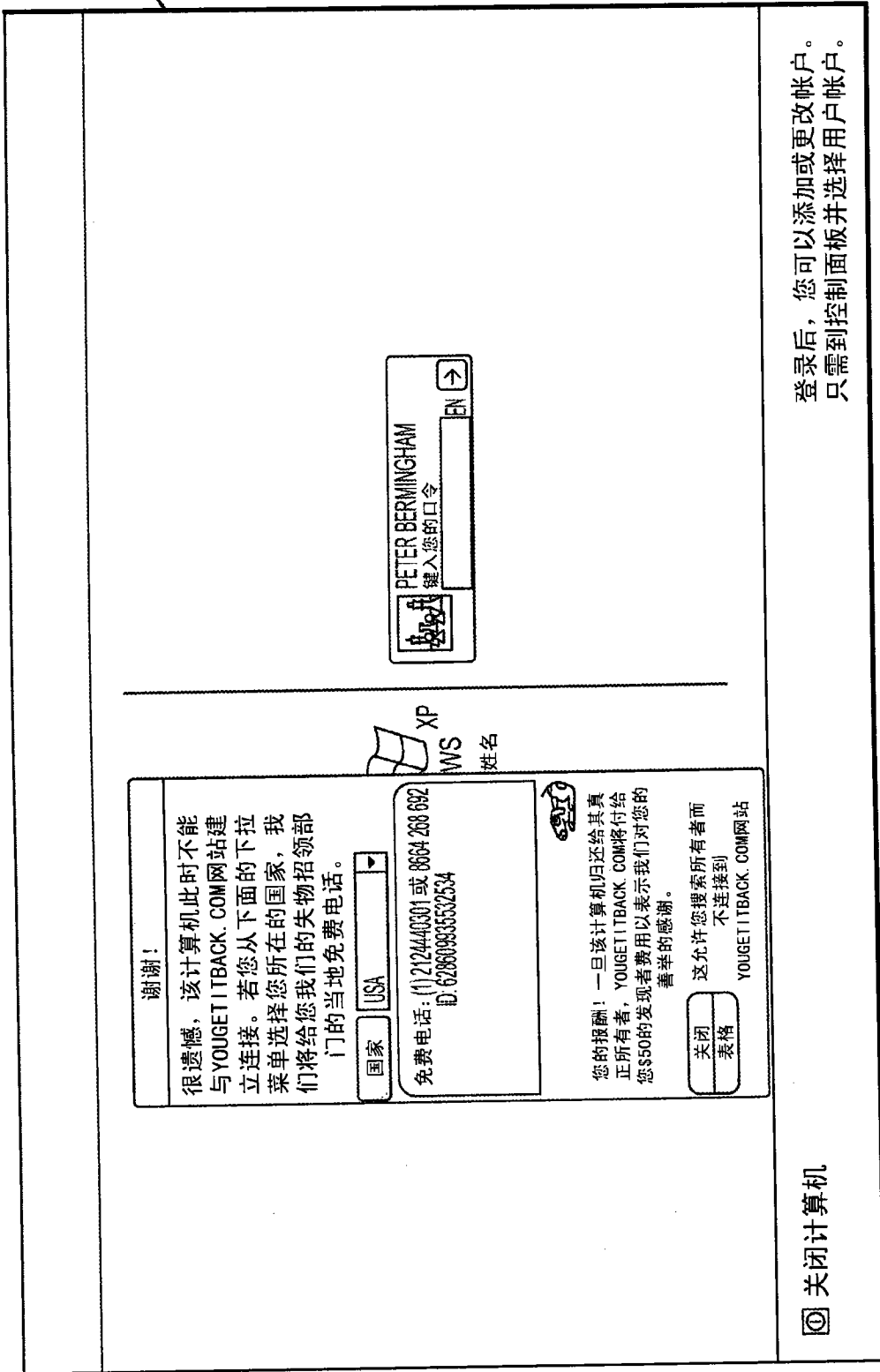
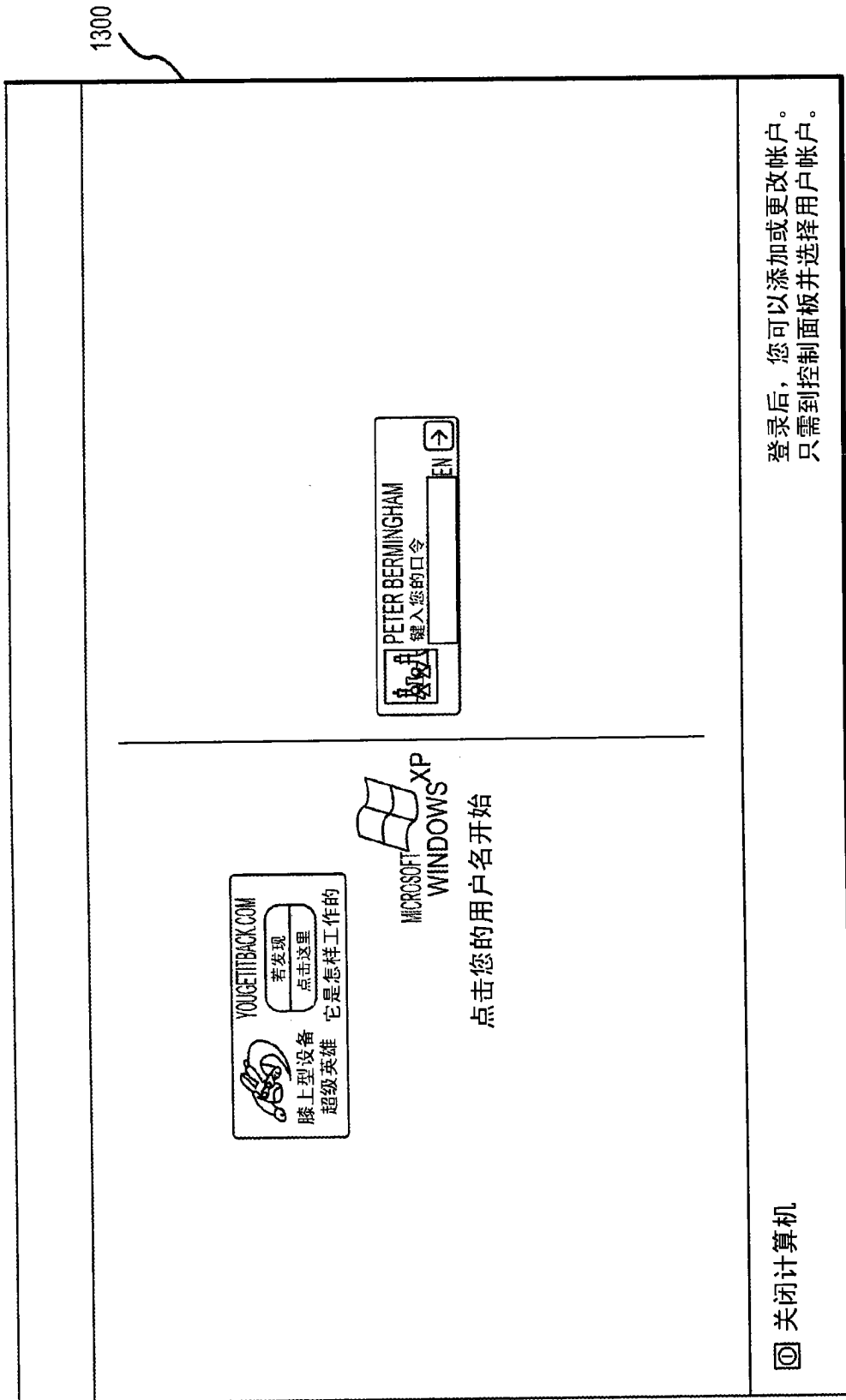


图 12



登录后，您可以添加或更改帐户。  
只需到控制面板并选择用户帐户。

关闭计算机

图 13

1400

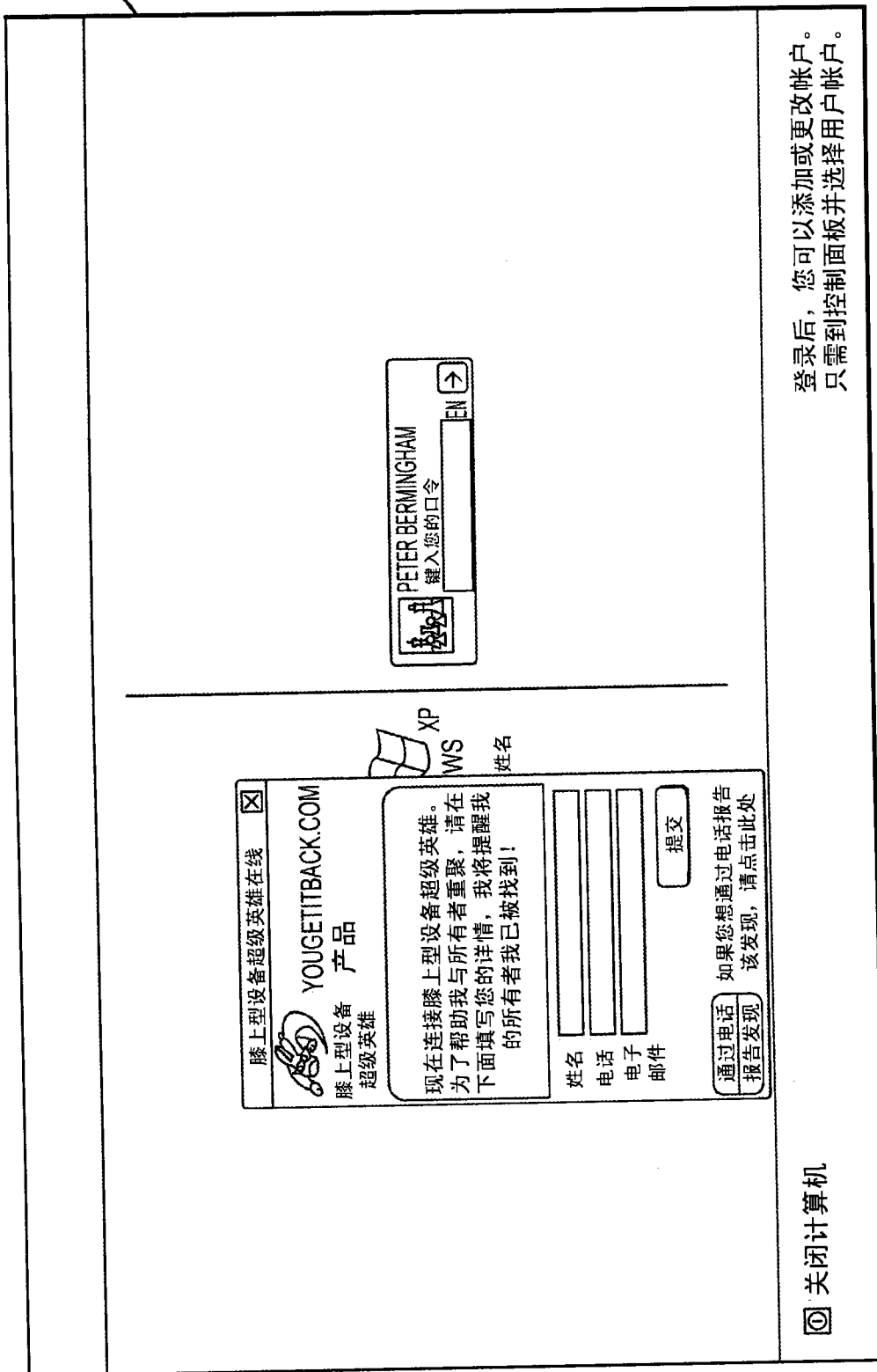
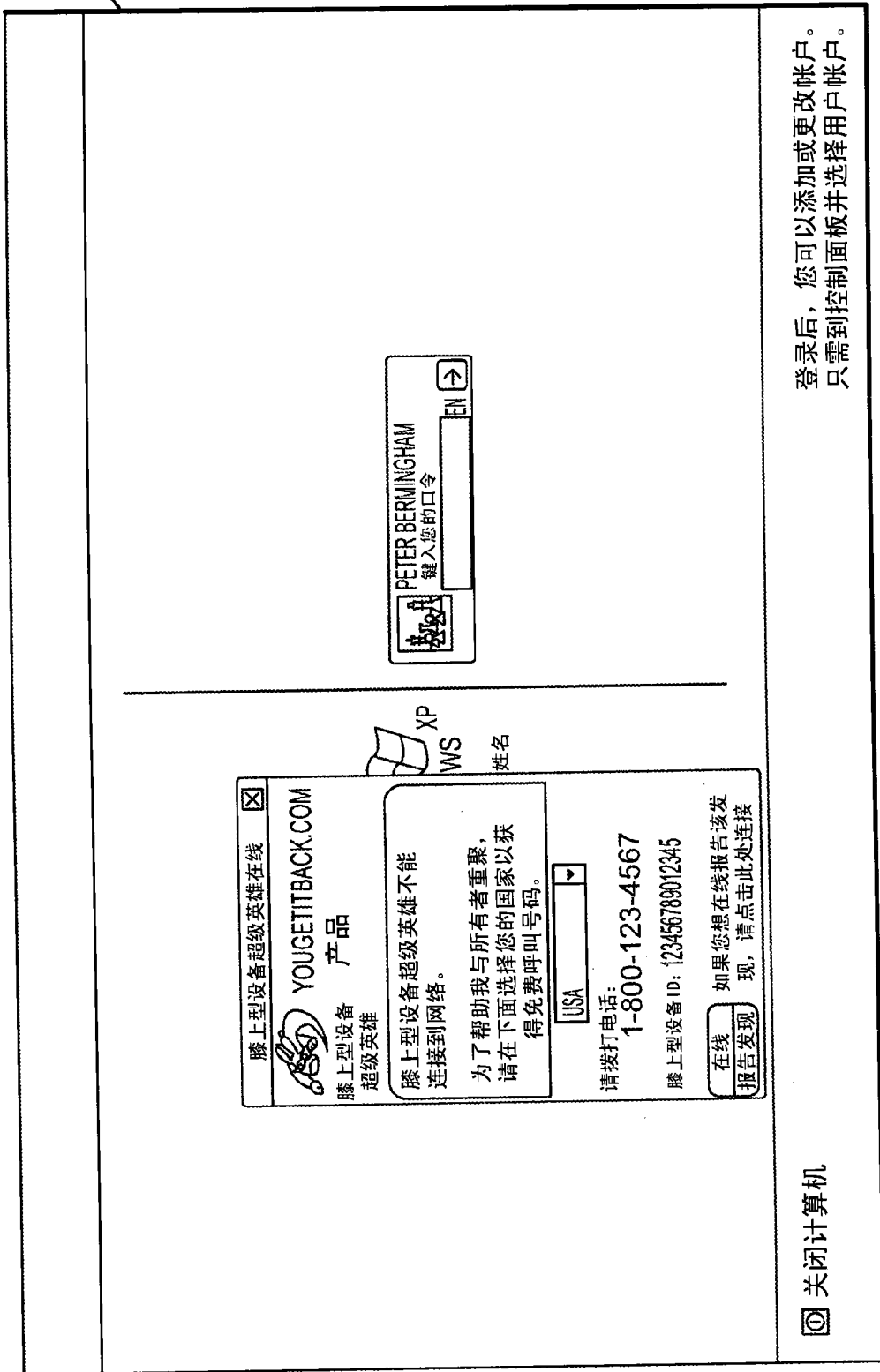


图 14

1500



登录后，您可以添加或更改帐户。  
只需到控制面板并选择用户帐户。

图 15

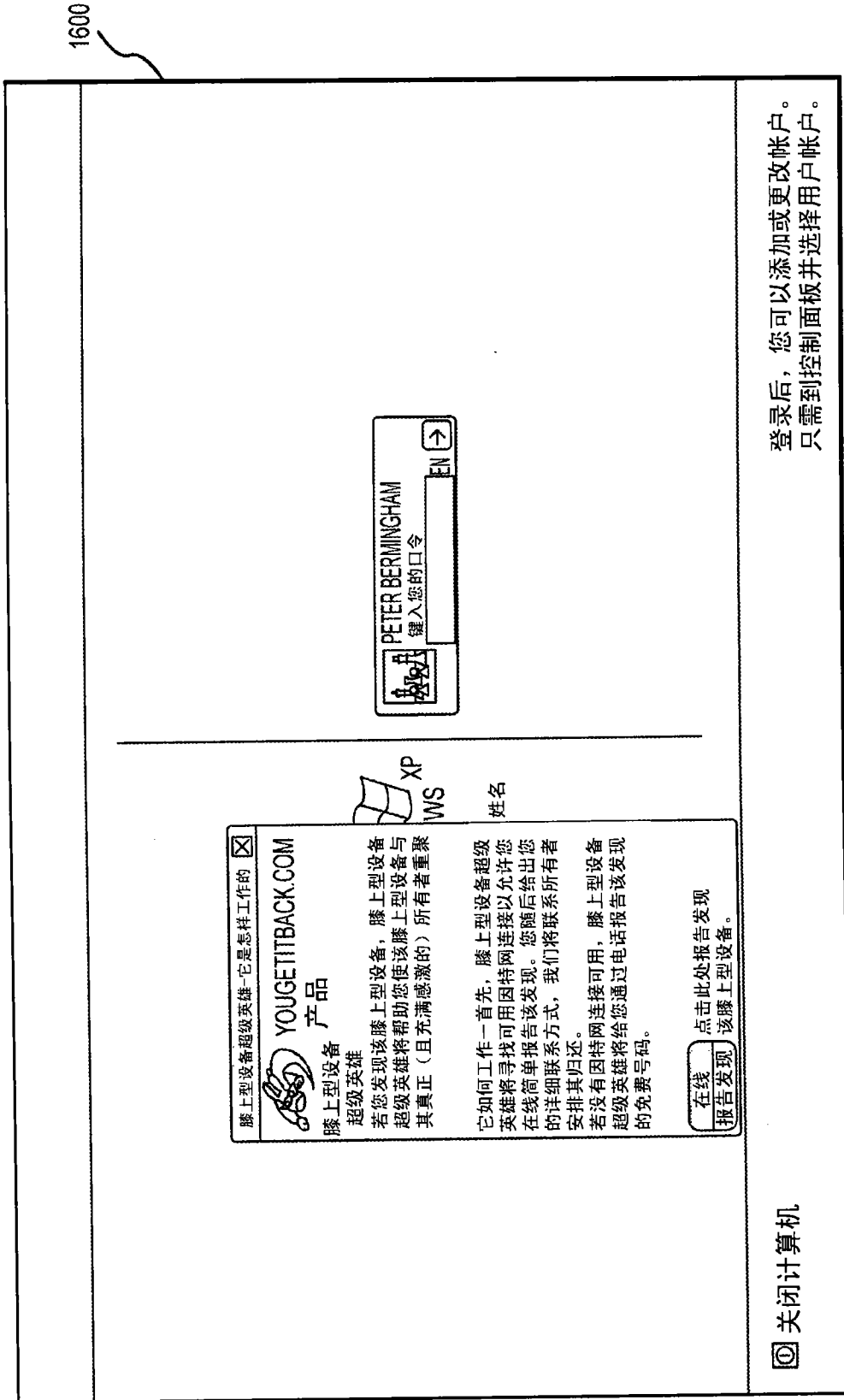


图 16

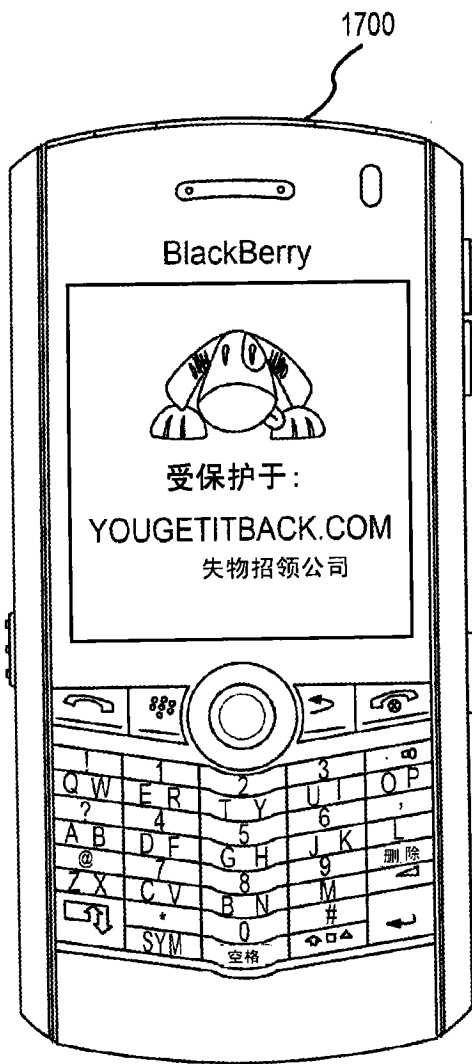


图 17

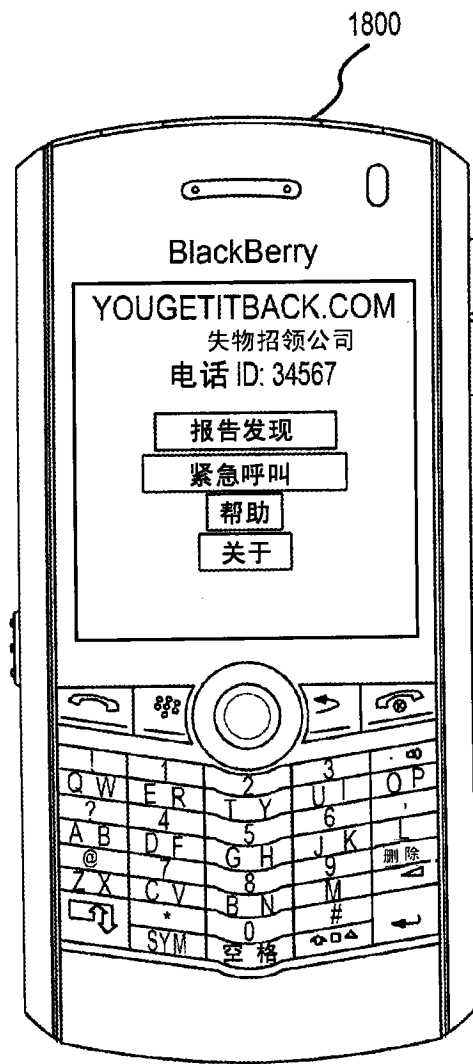
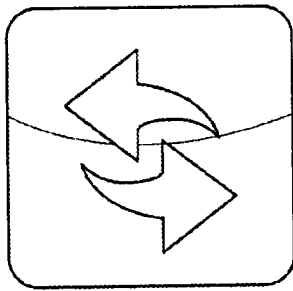


图 18

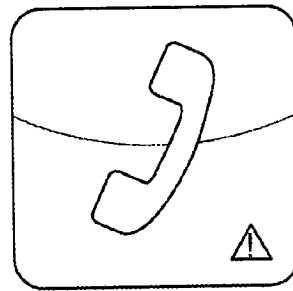


已连接

按下红色按钮结束该呼叫

YOUGETITBACK.COM

图 19



紧急...

按下ALT+END结束该呼叫

YOUGETITBACK.COM

图 20

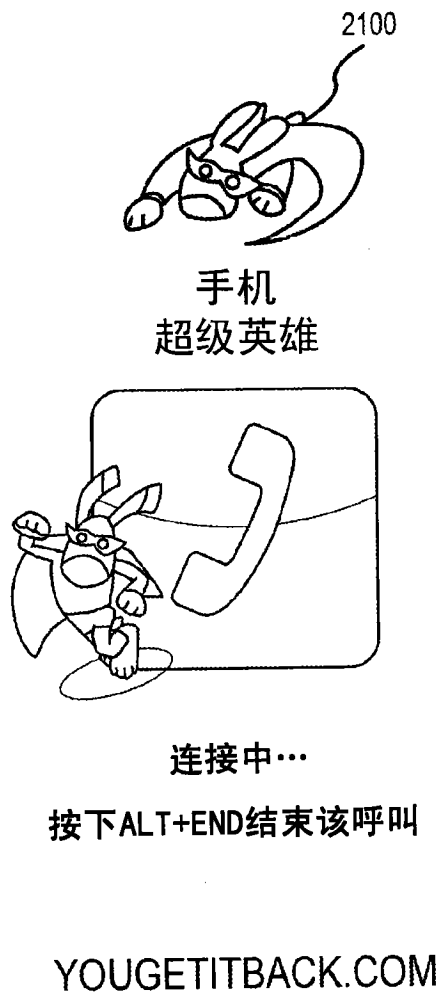


图 21

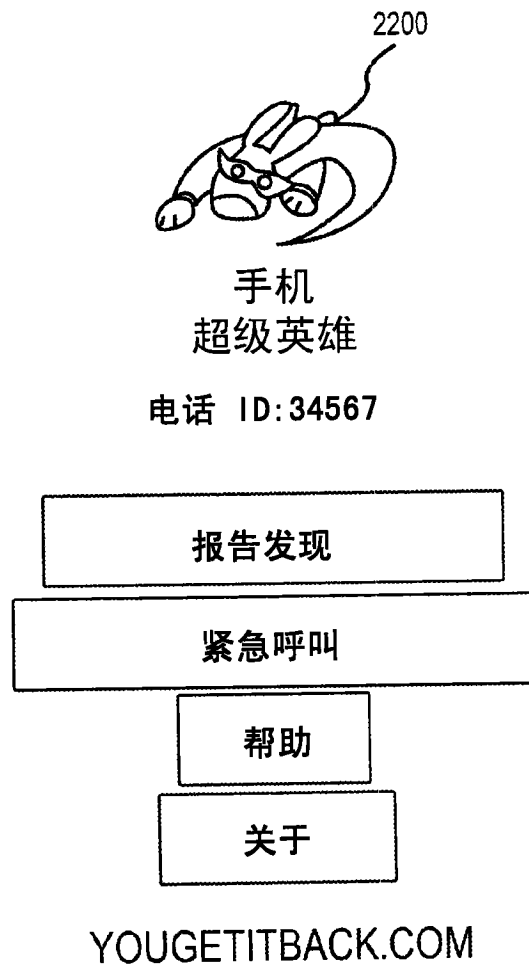


图 22





图 23



图 24

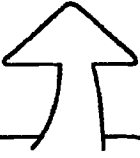


图 25

2600

通过YOUGETITBACK.COM, 高达75%的所有失物得以归还。

## 签约我们的新产品的测试版!



现在签约, 我们将着手为您开通该令人激动的新产品。点击这里查看更多信息以及我们的隐私策略。

姓名:

电子邮件地址:

[退货策略](#) | [使用条款](#) | [隐私策略](#) | [企业服务](#)

图 26

2700

您尚未登录 >> 登录 爱尔兰 << 更改

**YOUGETITBACK.COM** 我发现某物... 我丢失某物...  
失物招领公司 购买标签... 激活标签...

我的保险库 | 商店 | 支持 | 关于我们 | 新闻 | 主页

---

**通过YOUGETITBACK.COM, 高达75%的所有失物得以归还。**

**免费产品下载!**



**膝上型设备  
超级英雄**

现在  
下载!



**手机  
超级英雄**

现在  
下载!

**保护您的膝上型  
设备和移动电话**

您的膝上型设备和手机若丢失, 这些令人激动的新产品将帮助找到它

[关于膝上型设备超级英雄的更多信息 >>](#)

[关于手机超级英雄的更多信息 >>](#)

---

归还报酬  
**800 94 00**  
+44(0)207 1982450  
ID号: 125 800010  
YOUGETITBACK.COM

保护您的  
物品!








**YOUGETITBACK.COM**  
有YOUGETITBACK标签的丢失物品更有可能被归还给您!  
注册用户在其物品被找到时将立即得到提醒。  
现在就为您的物品加标签以便放心!

[购买标签](#) [更多信息...](#)

**免费签约并开始使用YOUGETITBACK  
保险库!**  
发现很难记住关于您的附属物的重要细节? 手机PUK码和PIN号、汽车钥匙、序列号、担保信息... 使用保险库在一个地方存储这些细节和管理您的所有加标签物品。

[签约](#) [更多信息...](#)

---

版权2007 | YOUGETITBACK.COM 保留所有权利

[退货策略](#) | [使用条款](#) | [隐私策略](#) | [企业服务](#)

图 27

2800

**28/64**

登入 爱尔兰 << 更改



**YOUGETITBACK.COM**

失物招领公司

我发现某物...
我丢失某物...

购买标签...
激活标签...

我的保险库 | 商店 | 支持 | 关于我们 | 新闻 | 博客 | 主页

**通过YOUGETITBACK.COM, 高达75%的所有失物得以归还。**

**免费产品下载!**



**膝上型设备  
超级英雄**

现在  
下载!



**手机  
超级英雄**

现在  
下载!

**保护您的膝上型  
设备和移动电话**

您的膝上型设备和手机若丢失, 这些令人激动的新产品将帮助找到它

[关于膝上型设备超级英雄的更多信息 >>](#)

[关于手机超级英雄的更多信息 >>](#)

**激活您的失物招领服务...**  
有人发现您的物品时立即得到通知!

\* 标签ID:

\* 电子邮件:

\* 我是:   
 新客户  
 现有客户

\* 口令:

\* 条款及条件  我已阅读并接受这些条款及条件

**提交**

**保护您的物品**

归还报酬  
**1800 238 0695**

ID号: Y000E0001  
YOUGETITBACK.COM

有YOUGETITBACK标签的丢失物品更有可能被归还给您! 现在就为您的物品加标签以便放心!

使用保险库在一个地方存储这些细节和管理您的所有加标签物品。

[免费签约并开始使用保险库>>](#)

**来自博客的最新消息...**

**电话保险袋**  
发现于LOIC LeMour博客 在外就餐时保护您的电话的巧妙方式。北京的餐馆正发放电话保险袋(小塑料袋), 从而他们在吃东西时能检查其手机而不会将任何东西溅到上面。继续阅读...

[我希望她找到我丢失的物品>>](#)  
[BLACKBERRY在印度可能关机>>](#)  
[更多信息>>](#)

**订阅**

**在阅读器中订阅**

通过电子邮件订阅:  
输入您的电子邮件地址:

**订阅**

由 FeedBurner 投递

版权2007 | YOUGETITBACK.COM 保留所有权利

[退货策略](#) | [使用条款](#) | [隐私策略](#) | [企业服务](#)

图 28

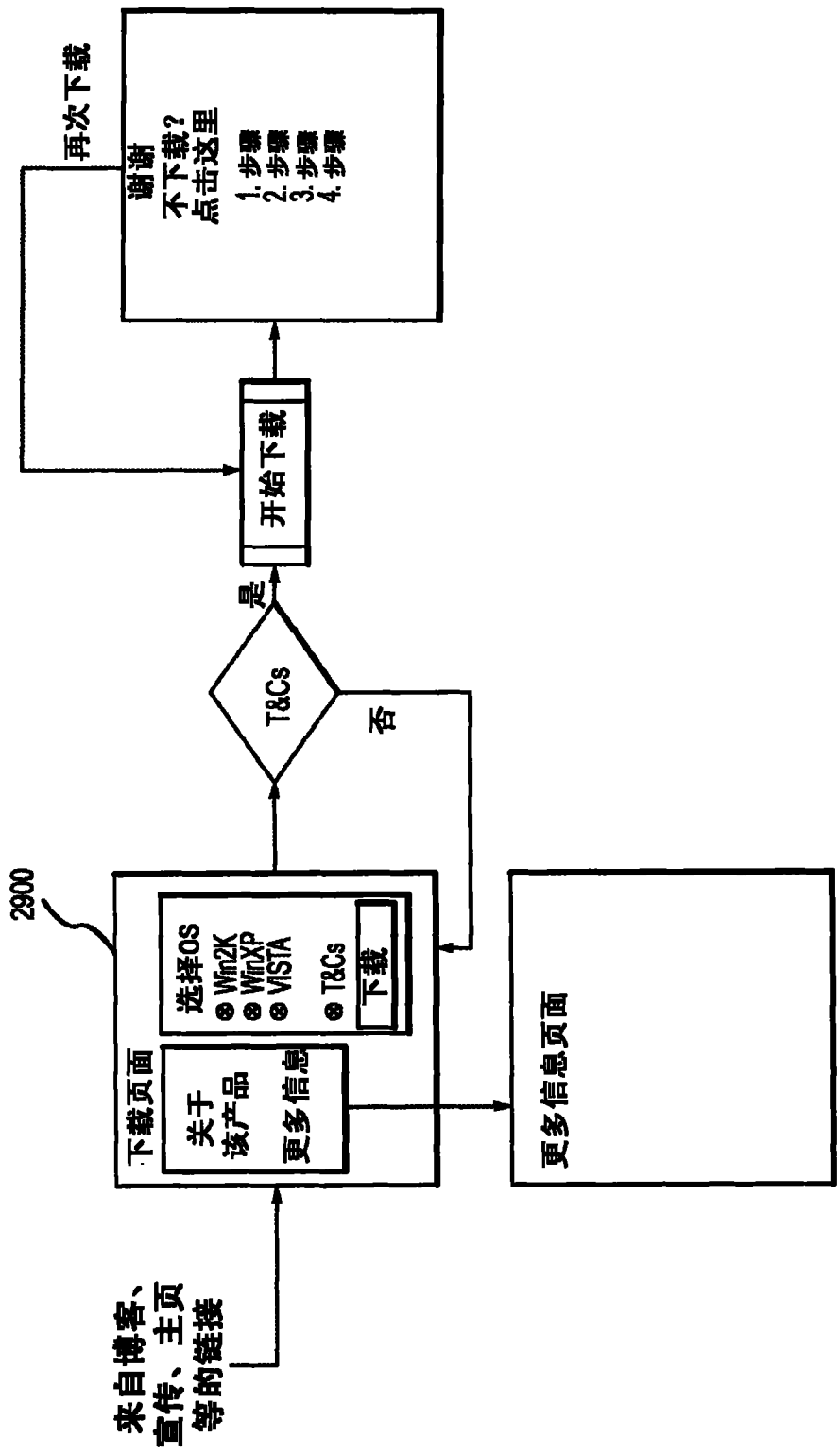


图 29

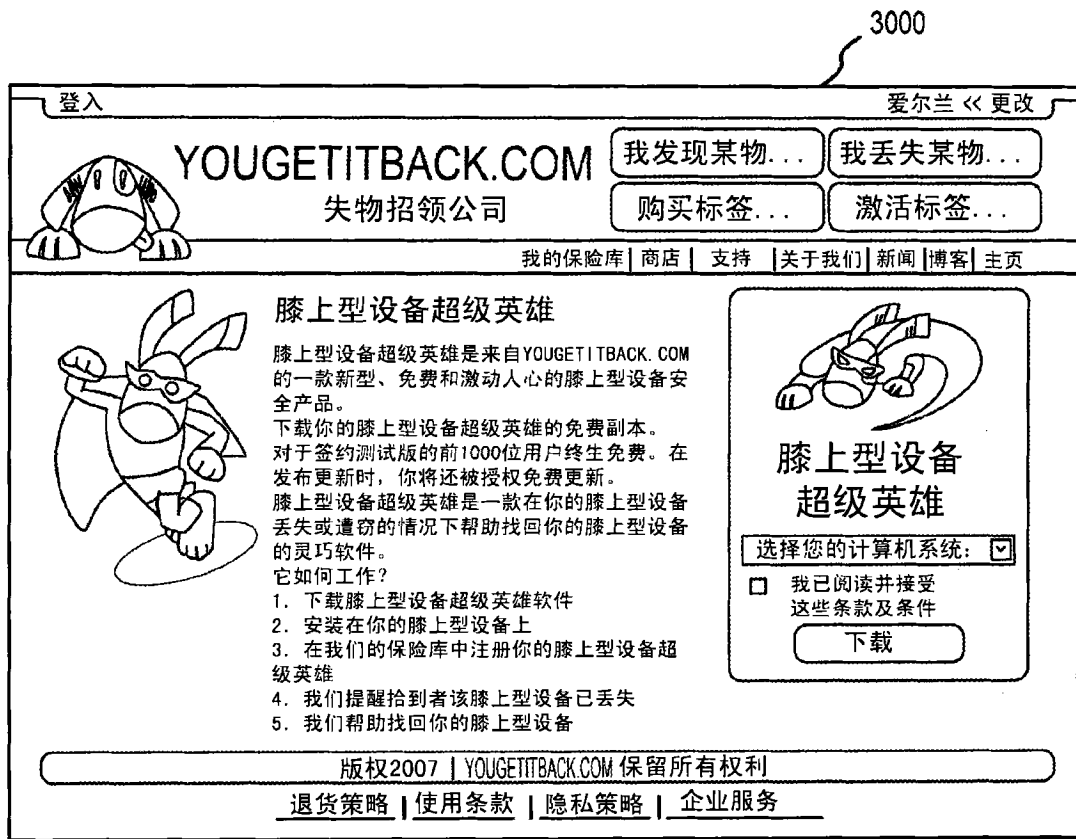


图 30

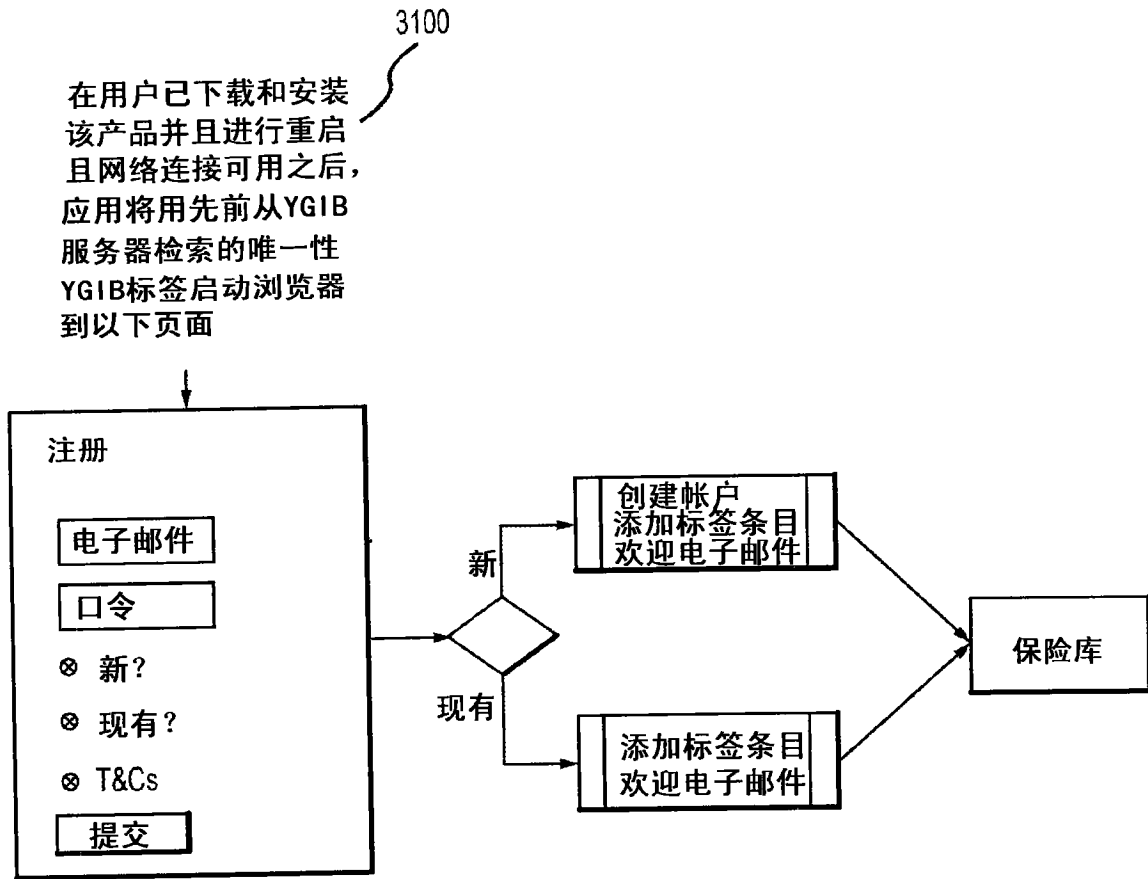


图 31



3200

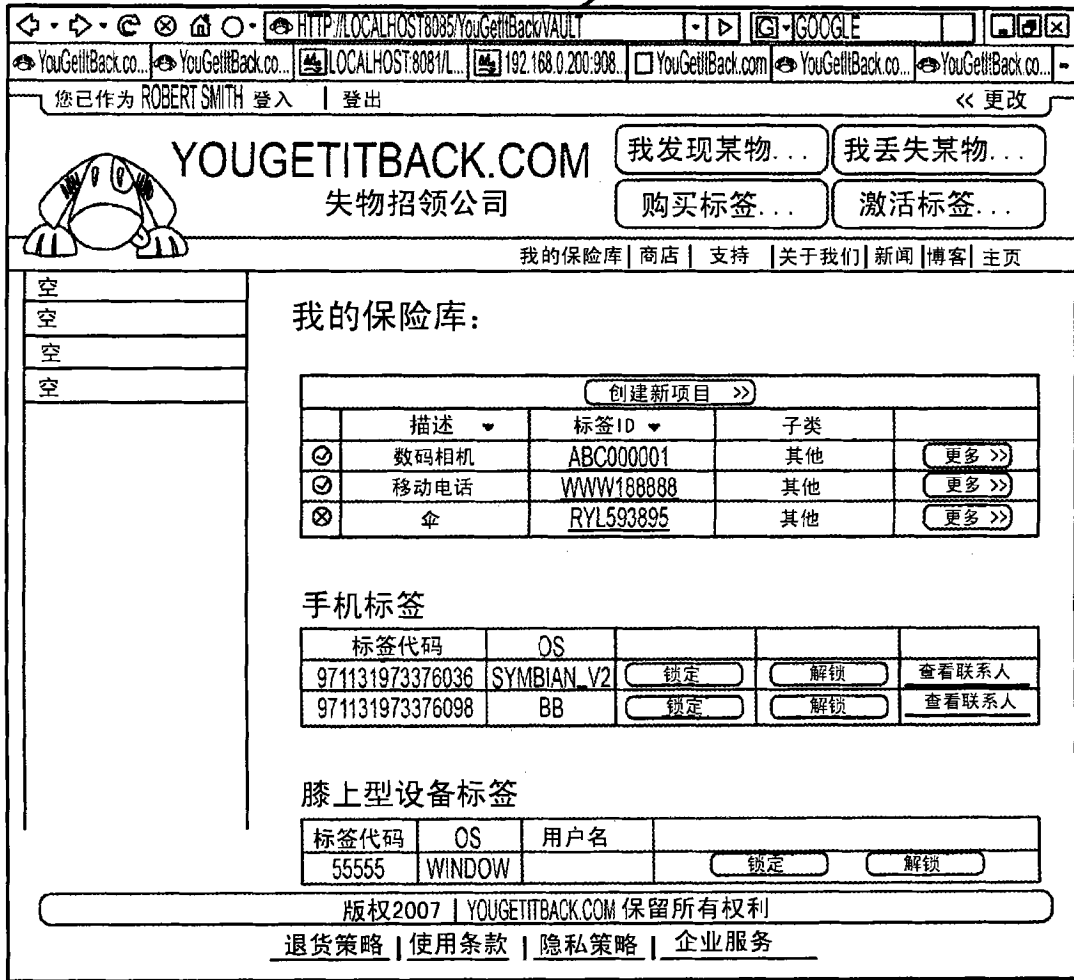


图 32

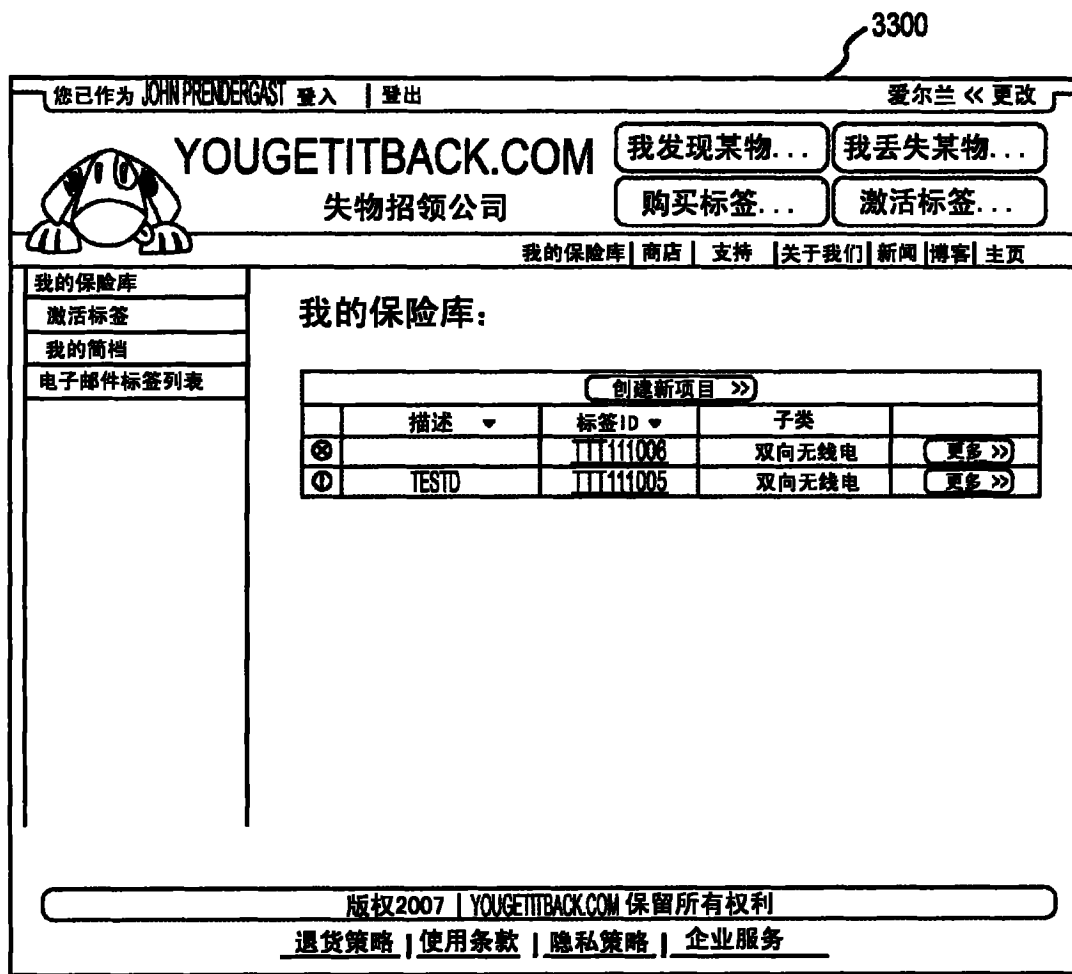


图 33

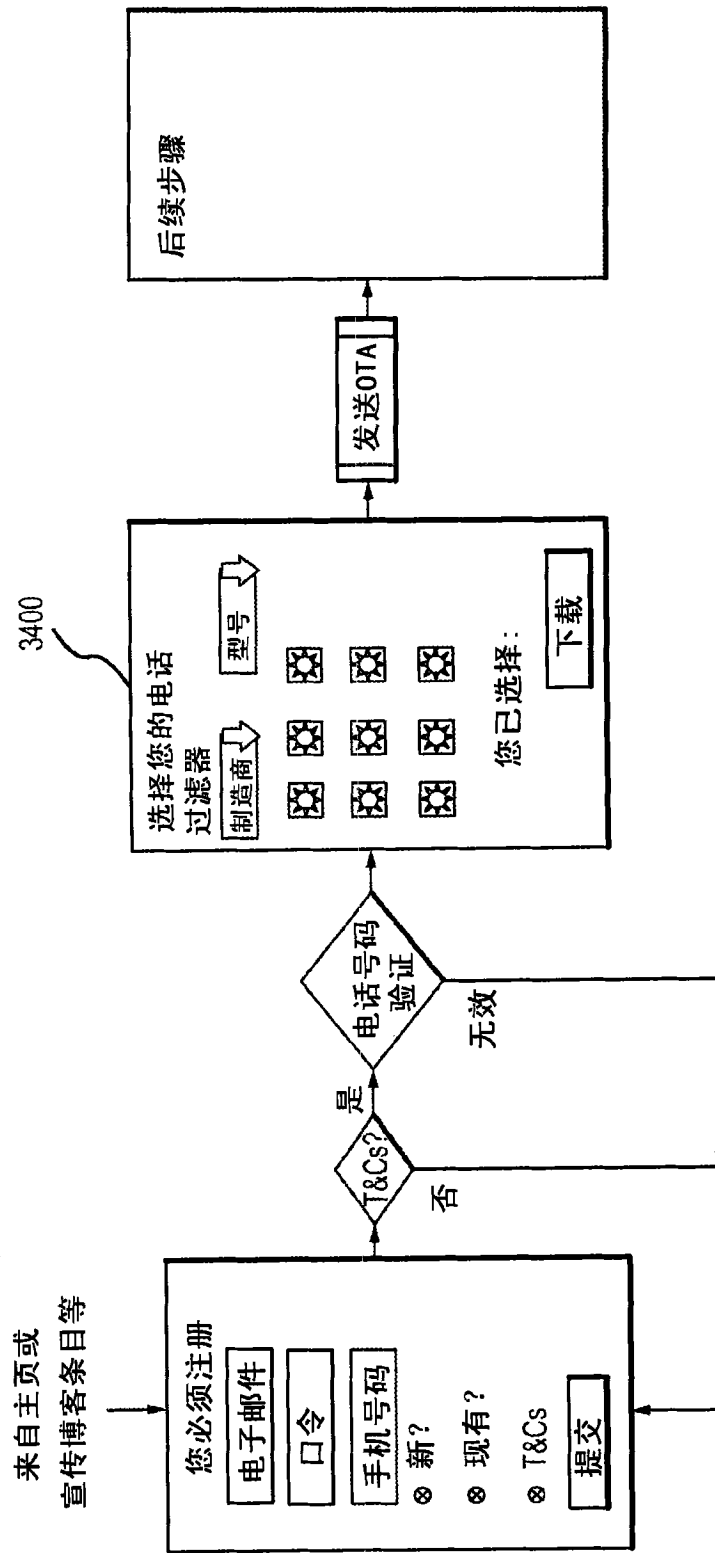


图 34


3500

您尚未登录 >> 登录 爱尔兰 << 更改

**YOUGETITBACK.COM** 我发现某物... 我丢失某物...  
 失物招领公司 购买标签... 激活标签...

我的保险库 | 商店 | 支持 | 关于我们 | 新闻 | 主页

---



手机  
超级英雄  
**测试**

**免费获得手机超级英雄!**

姓名:


选择口令:

手机号码:

我是:  新客户  
 现有客户

条款及条件:  我已阅读并接受  
 这些条款及条件

**下一步**



手机  
超级英雄  
**测试**

---

**手机超级英雄**

手机超级英雄是来自YOUGETITBACK.COM的一款新型、  
 免费和激动人心的手机安全产品。  
 下载你的手机超级英雄的免费副本。  
 先签约测试版的有限数量用户终生免费。在发布更新  
 时，您还将被授权免费更新。  
 手机超级英雄是一款在你的手机丢失时允许您远程地  
 锁定您的手机并允许您备份您的联系人以及将其安全  
 地存储在您自己的私人在线保险库里。若您的手机丢  
 失或失窃，手机超级英雄将帮助您与发现者相聚。  
 它如何工作？

1. 注册该产品
2. 下载手机超级英雄软件到您的手机上
3. 安装在您的手机上
4. 将您的联系人备份到您的安全保险库

图 35

3600

您尚未登录 >> 登录 爱尔兰 << 更改

**YOUGETITBACK.COM** 我发现某物... 我丢失某物...

















失物招领公司 购买标签... 激活标签...


[我的保险库](#) | [商店](#) | [支持](#) | [关于我们](#) | [新闻](#) | [主页](#)

**几乎完成了... 只要选择你的电话型号!**

在下面的下拉菜单中选择你的电话的制造商和型号或者如果你在下面看到你的电话就点击它的图片。当你已选择了你的电话时点击提交按钮。

选择电话的制造商  选择电话型号

 诺基亚 N73	 诺基亚 N72	 诺基亚 N93	 诺基亚 N92
 诺基亚 N92	 诺基亚 N93	 诺基亚 N72	 诺基亚 N73
 诺基亚 N73	 诺基亚 N72	 诺基亚 N93	 诺基亚 N92
 诺基亚 N92	 诺基亚 N93	 诺基亚 N72	 诺基亚 N73



手机  
超级英雄

版权2007 | YOUGETITBACK.COM 保留所有权利

[退货策略](#) | [使用条款](#) | [隐私策略](#) | [企业服务](#)

图 36

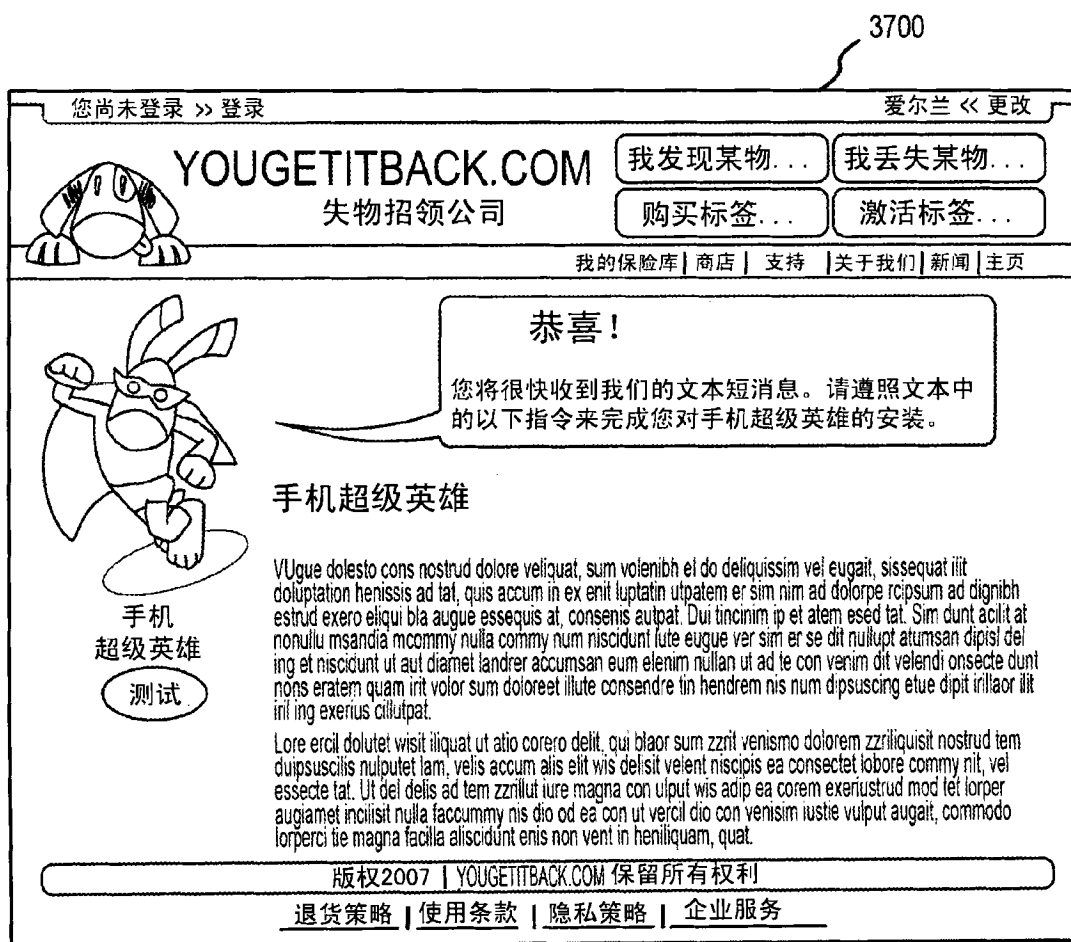


图 37

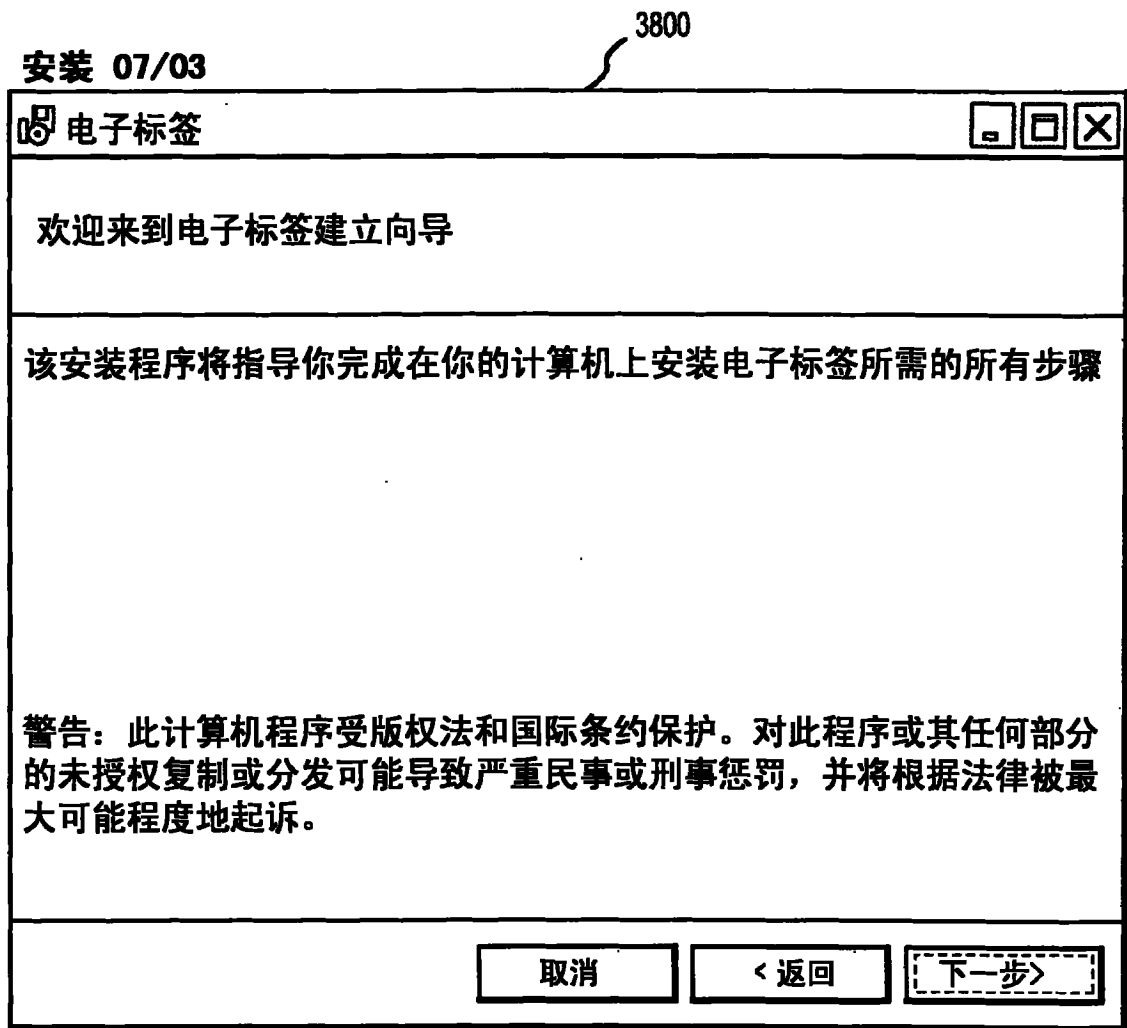


图 38

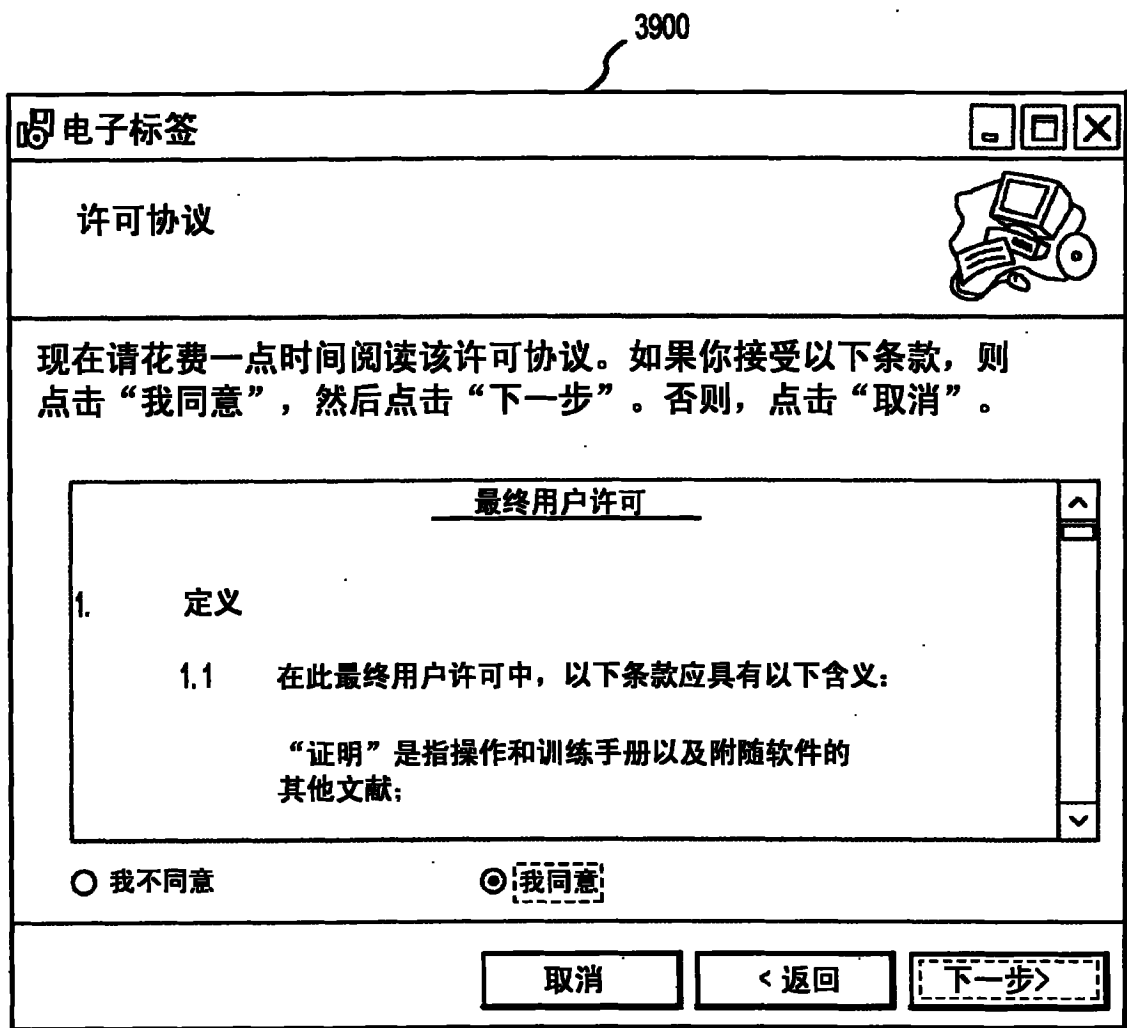


图 39



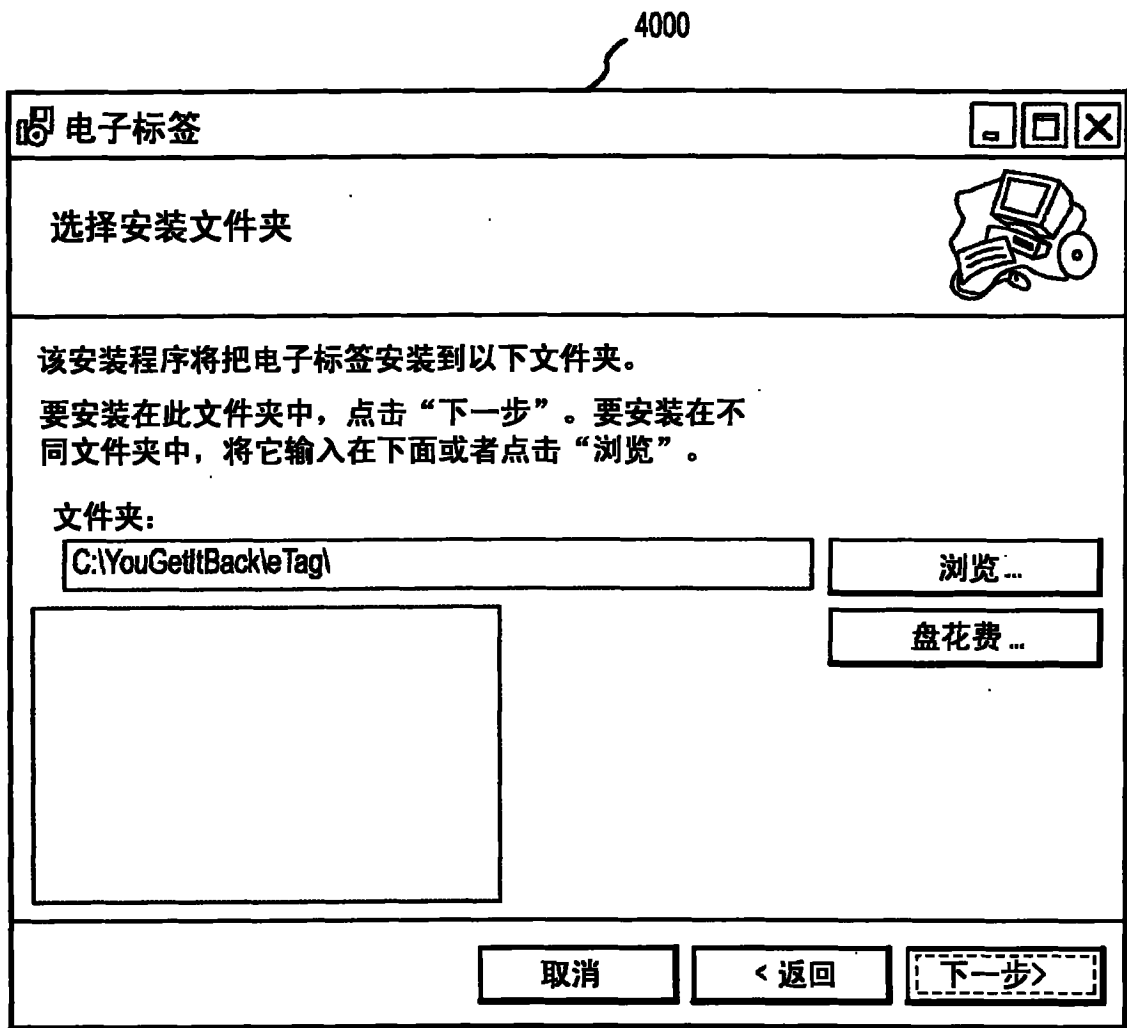


图 40

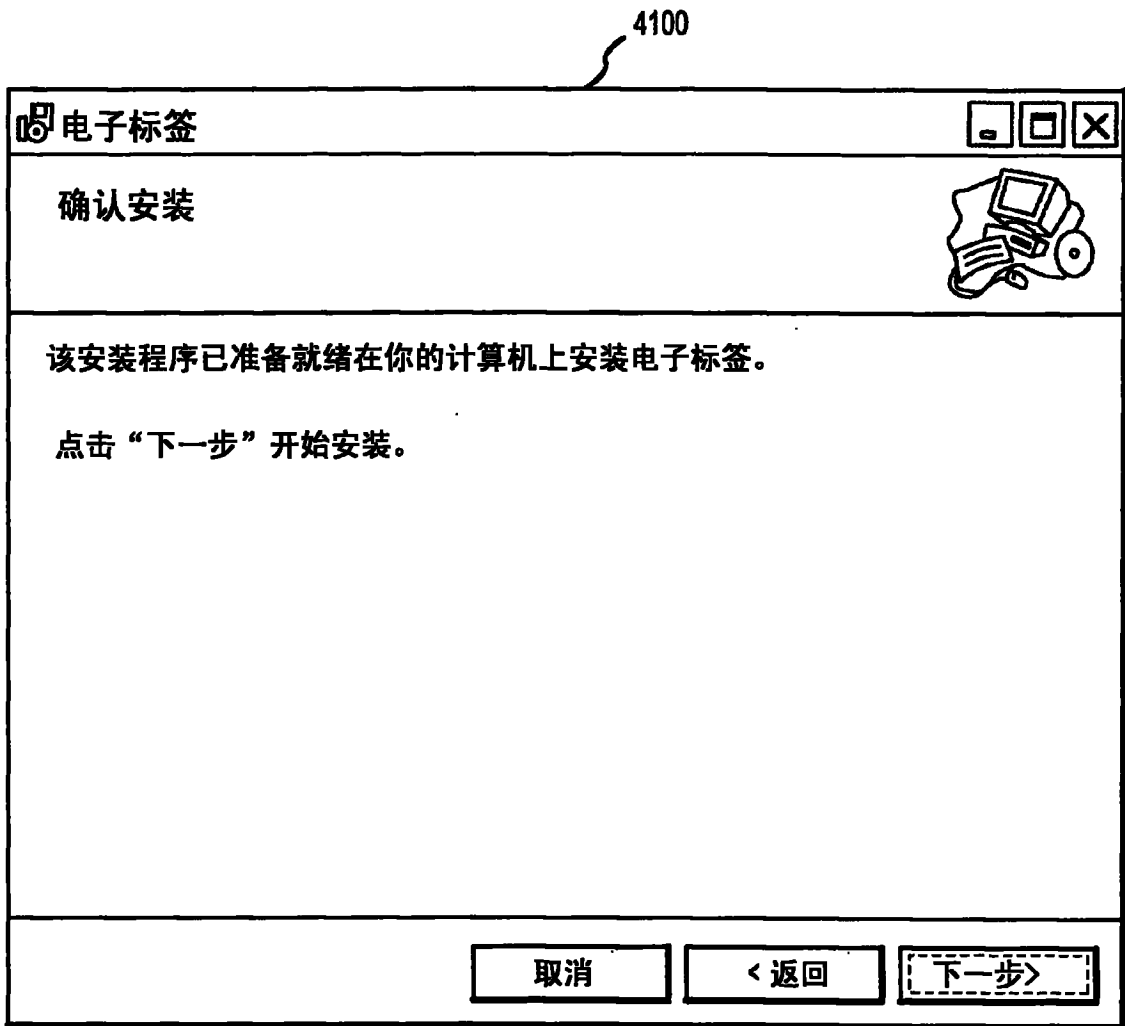


图 41

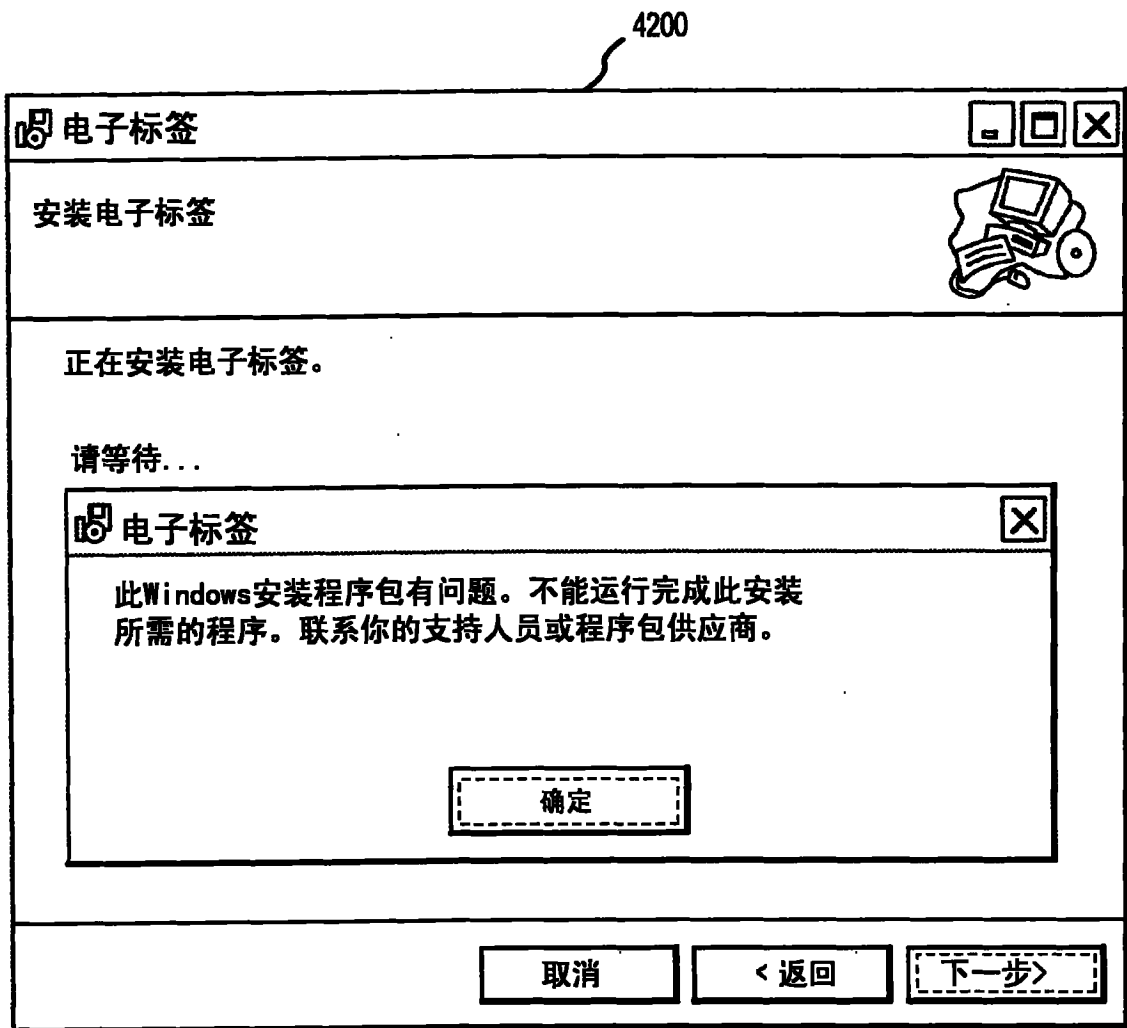


图 42

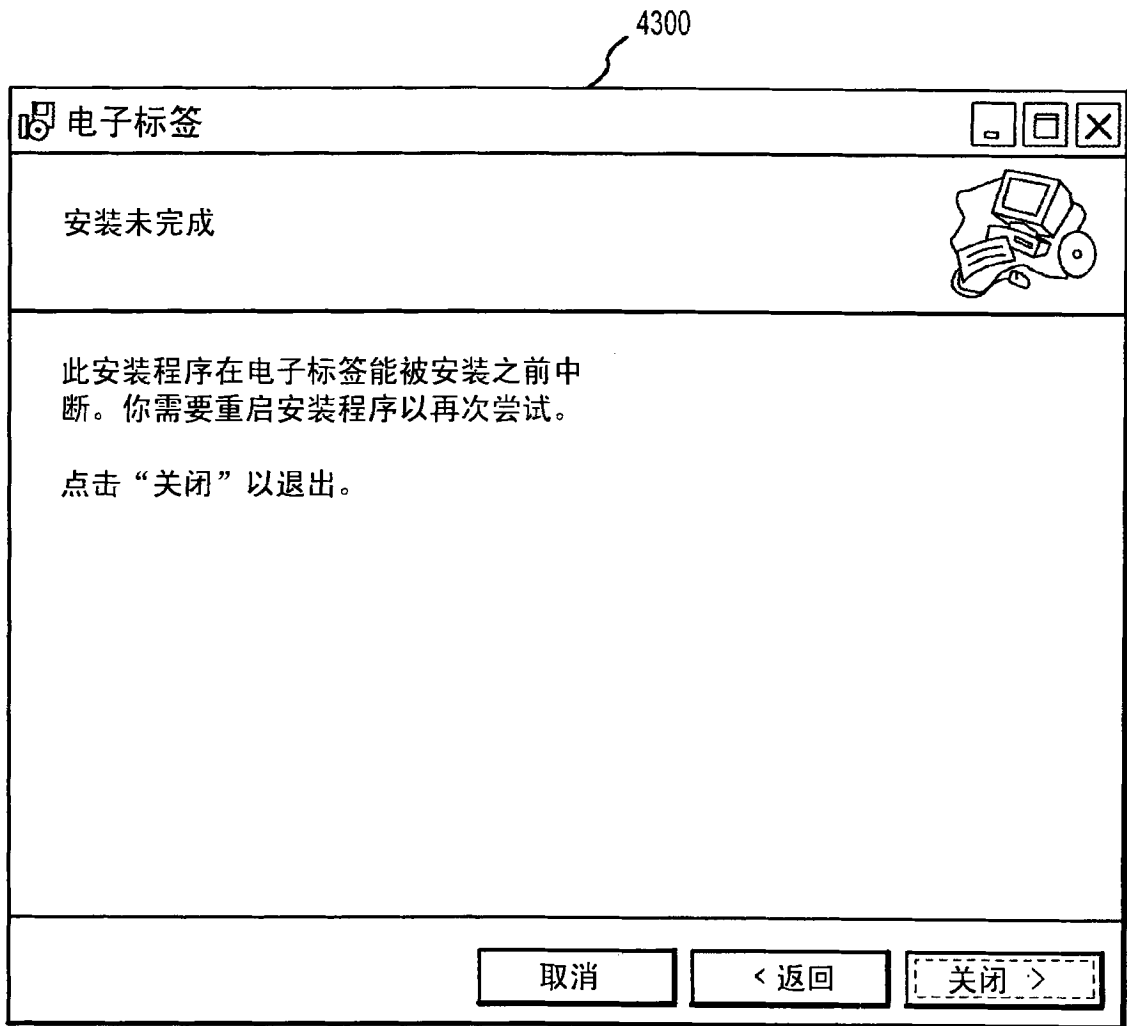


图 43

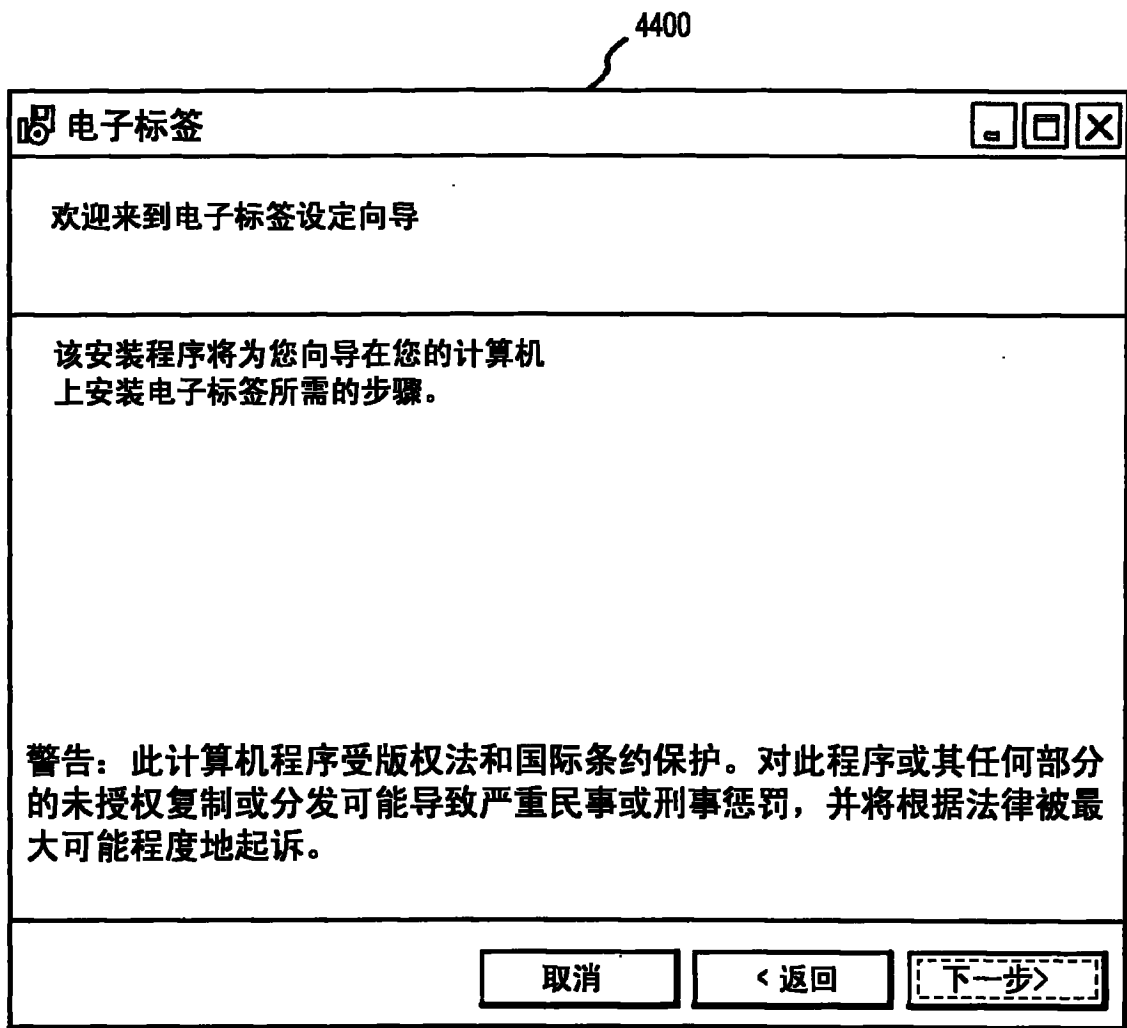


图 44

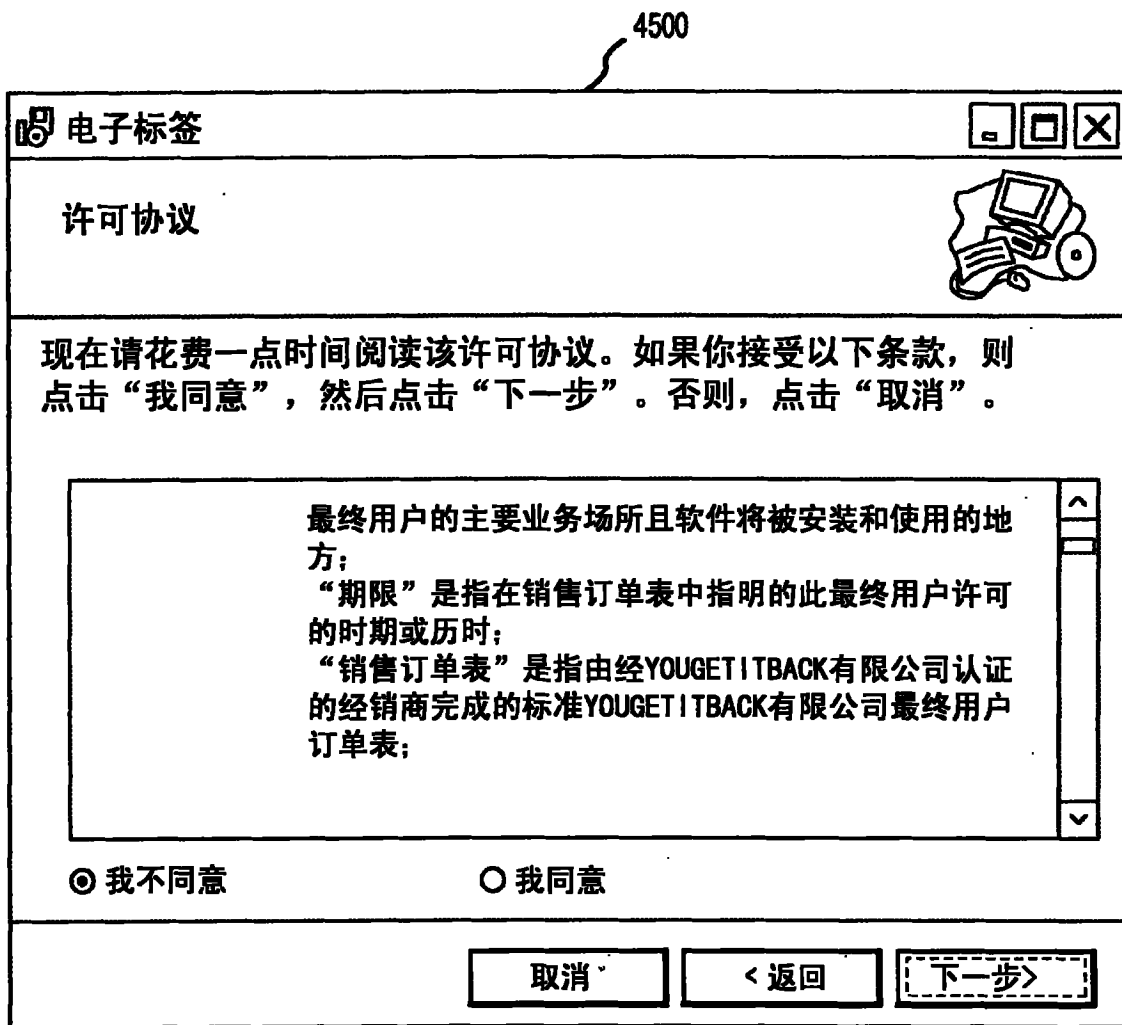


图 45

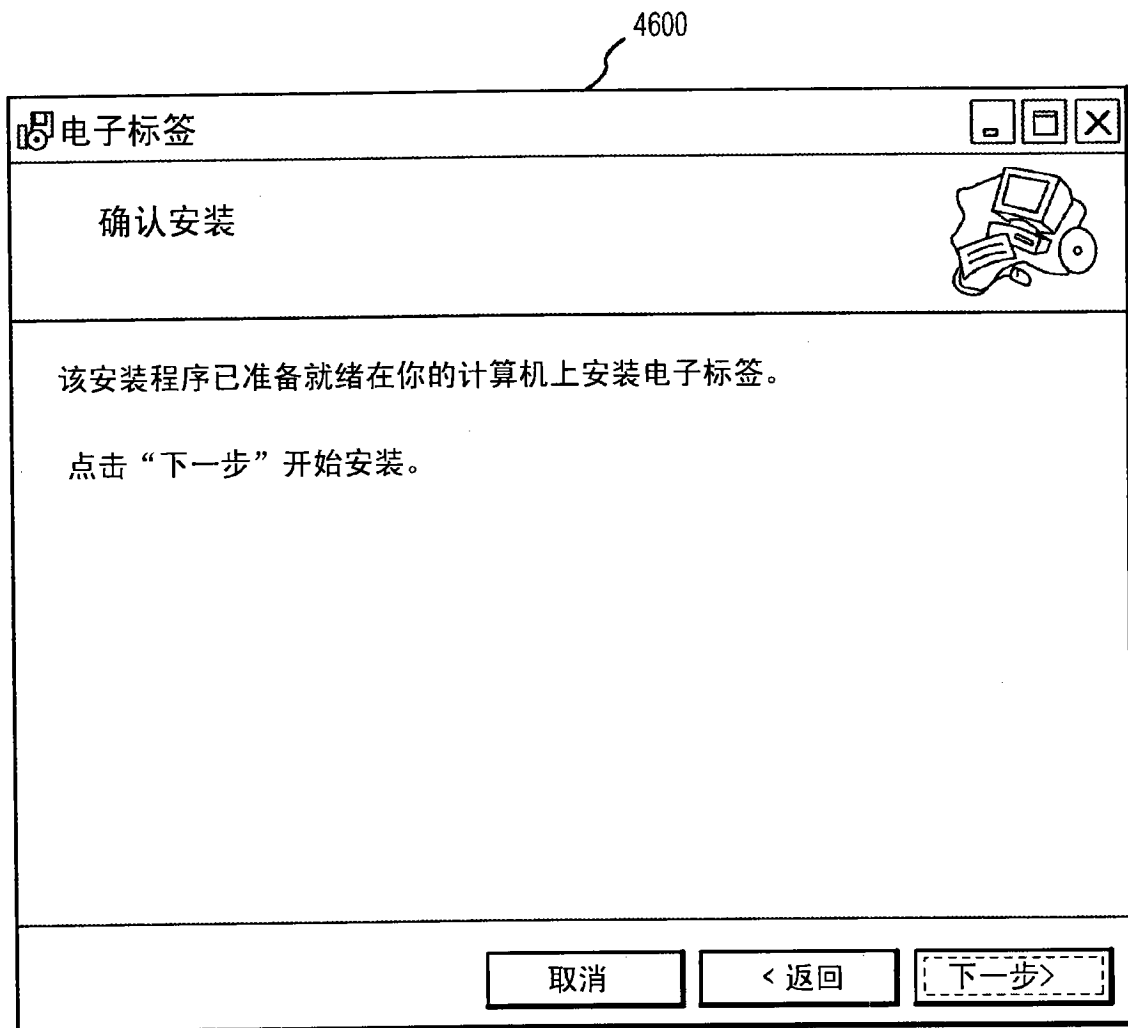


图 46

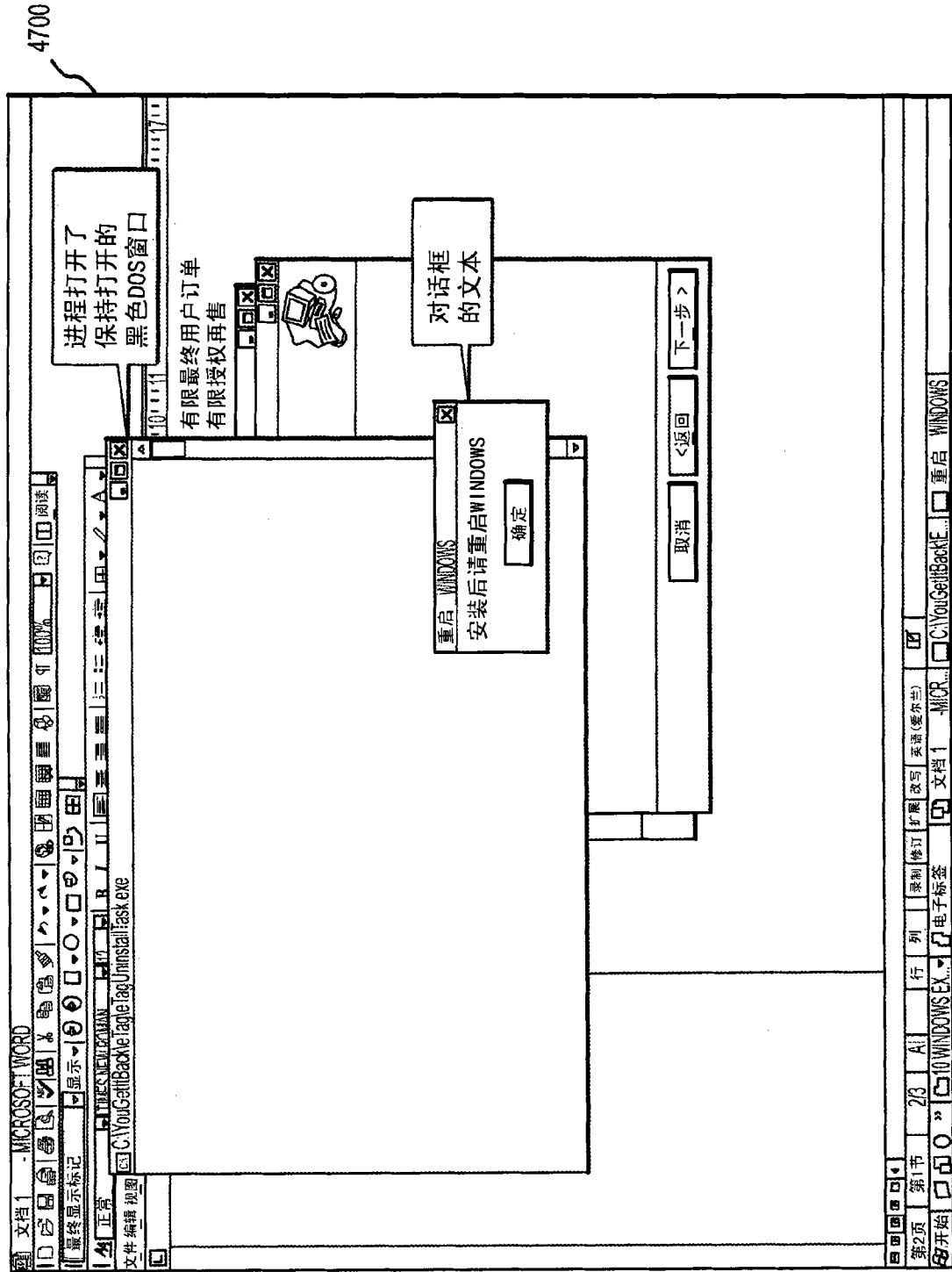


图 47



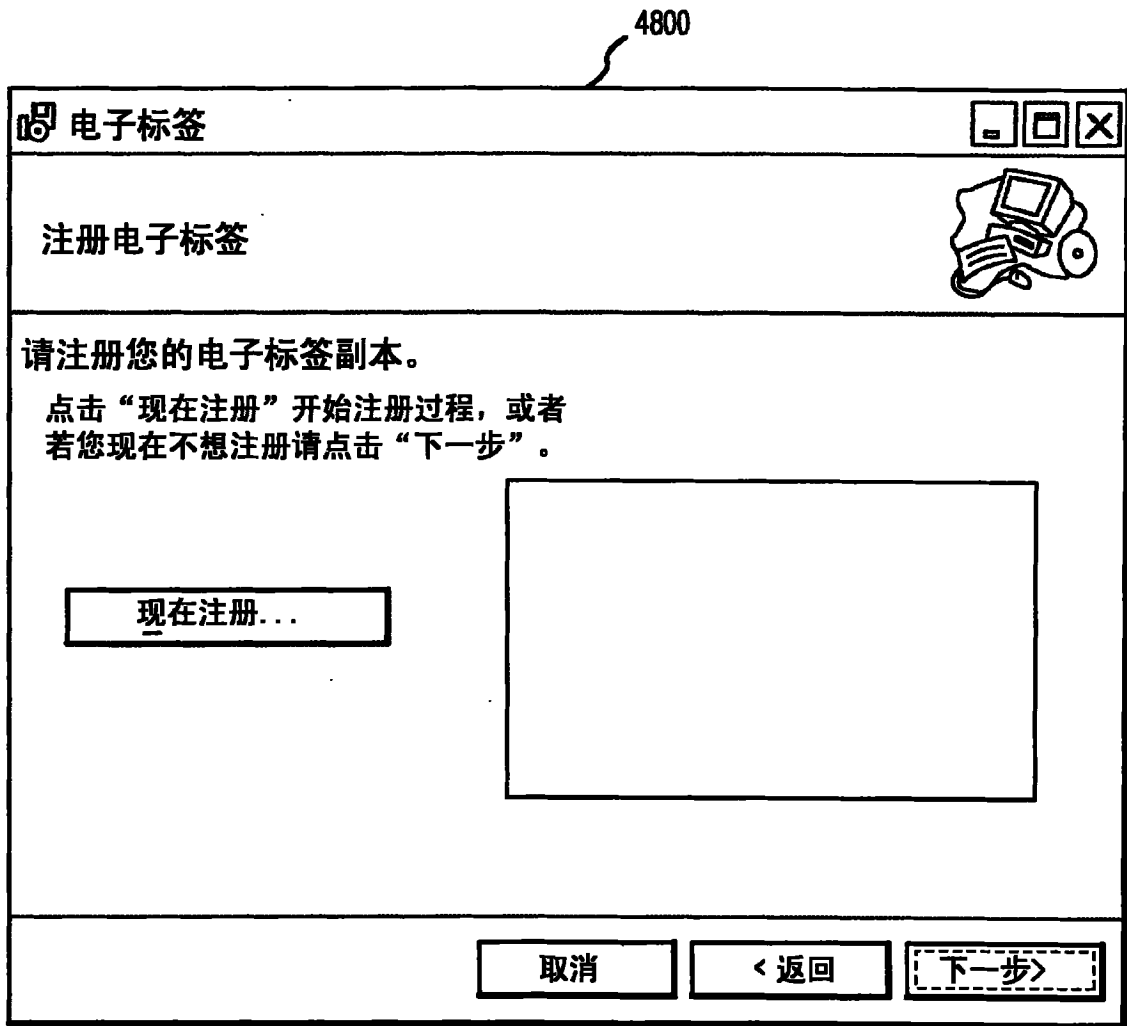


图 48

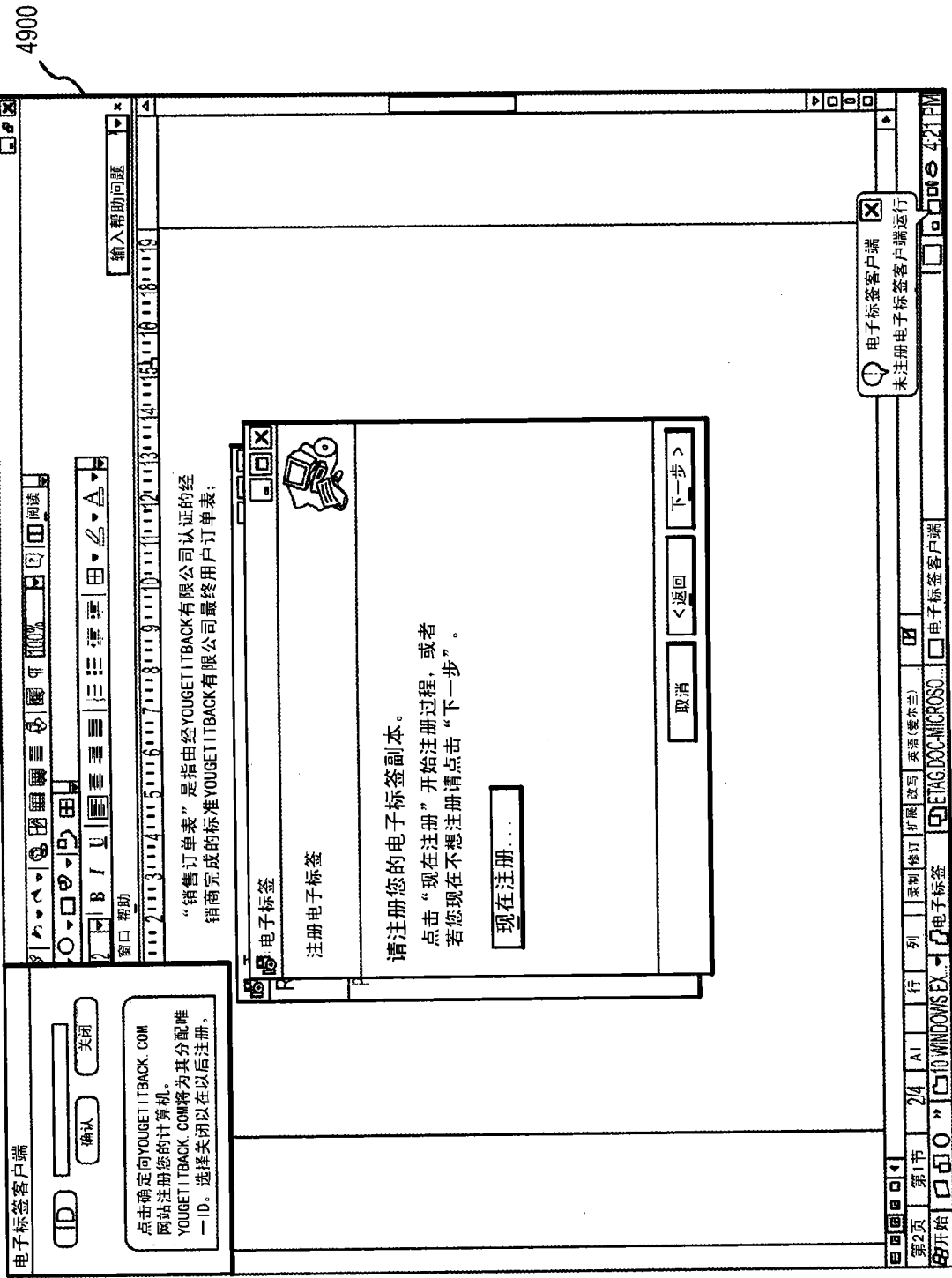


图 49

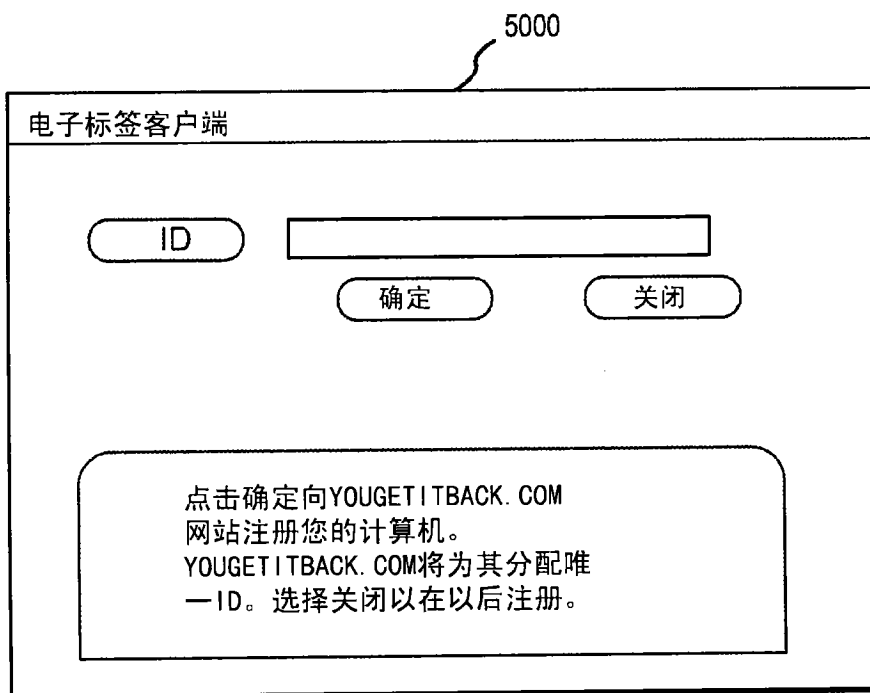


图 50

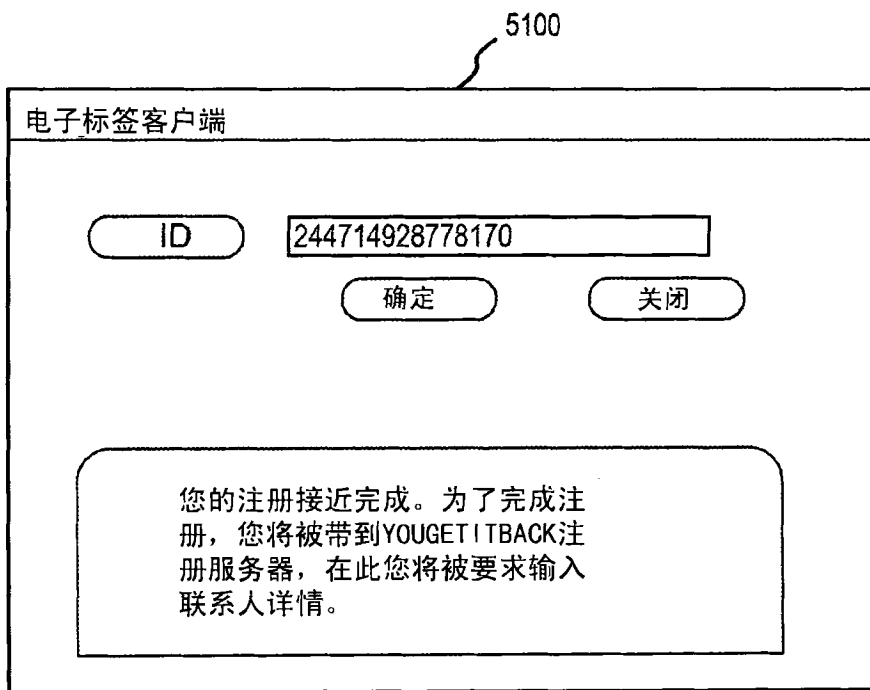


图 51

5200

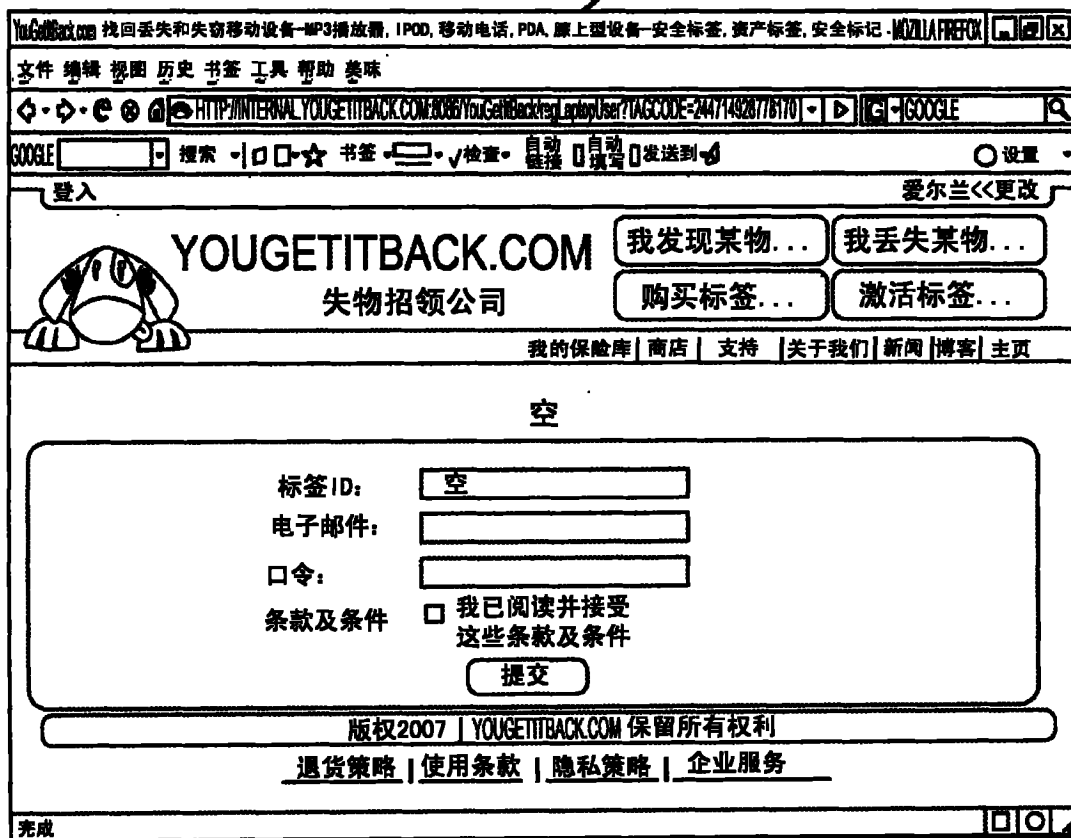


图 52

5300



图 53

5400



图 54



图 55

5600

您已作为 JOHN PRENDERCAST 登入 | 登出 爱尔兰 << 更改

**YOUGETITBACK.COM** 失物招领公司

我发现某物... 我丢失某物...  
 购买标签... 激活标签...

我的保险库 | 商店 | 支持 | 关于我们 | 新闻 | 博客 | 主页

我的保险库

激活标签

我的简档

电子邮件标签列表

### 我的保险库:

创建新项目 >>

	描述	标签ID	子类	
①	护照	MCP001662	护照	<a href="#">更多 &gt;&gt;</a>

护照

状态:

描述:

标签ID:

激活:

过期:

类别:  ▼

制造商:

型号:

序列号:

评述:

报酬:

	描述 ▼	标签ID ▼	子类	
②		TTT111006	双向无线电	<a href="#">更多 &gt;&gt;</a>
②	膝上型设备	MCP001766	膝上型设备	<a href="#">更多 &gt;&gt;</a>
①	TESTD	TTT111005	双向无线电	<a href="#">更多 &gt;&gt;</a>
②	免费测试标签	未激活	双向无线电	<a href="#">更多 &gt;&gt;</a>

版权2007 | YOUGETITBACK.COM 保留所有权利

[退货策略](#) | [使用条款](#) | [隐私策略](#) | [企业服务](#)

图 56



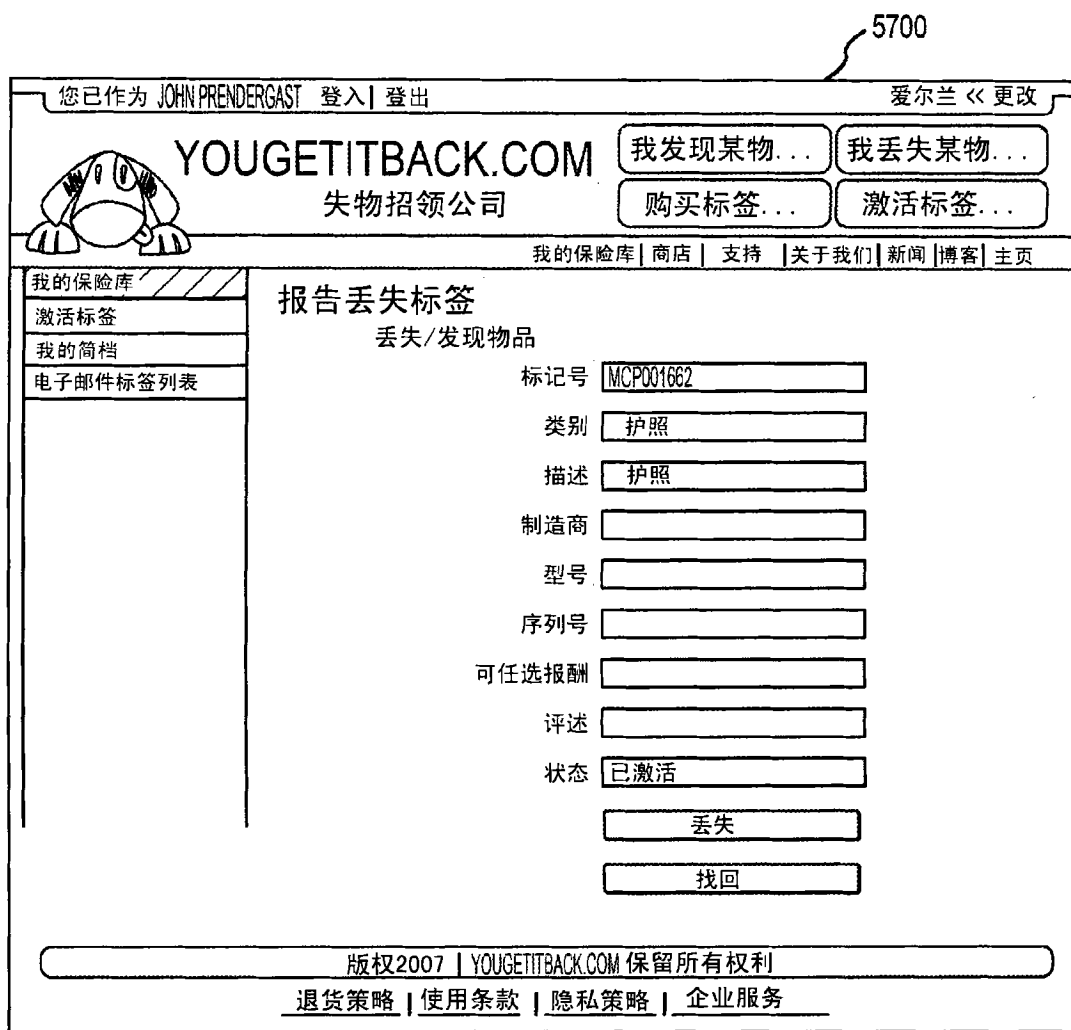


图 57

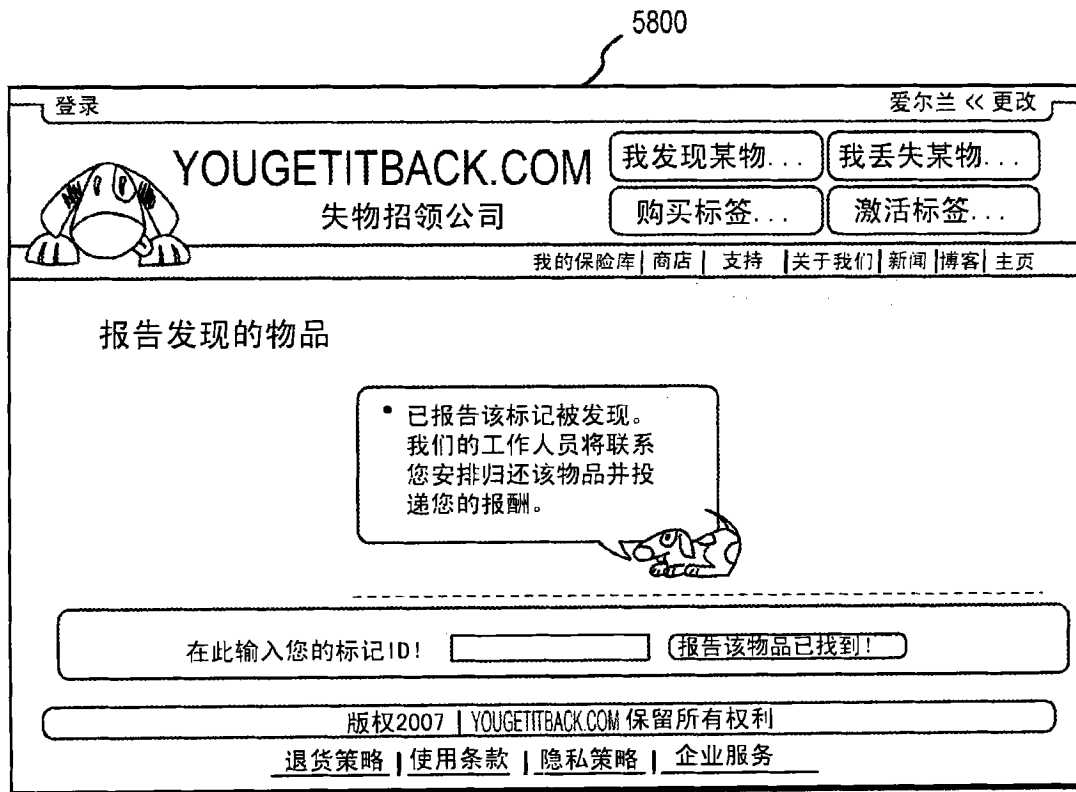


图 58

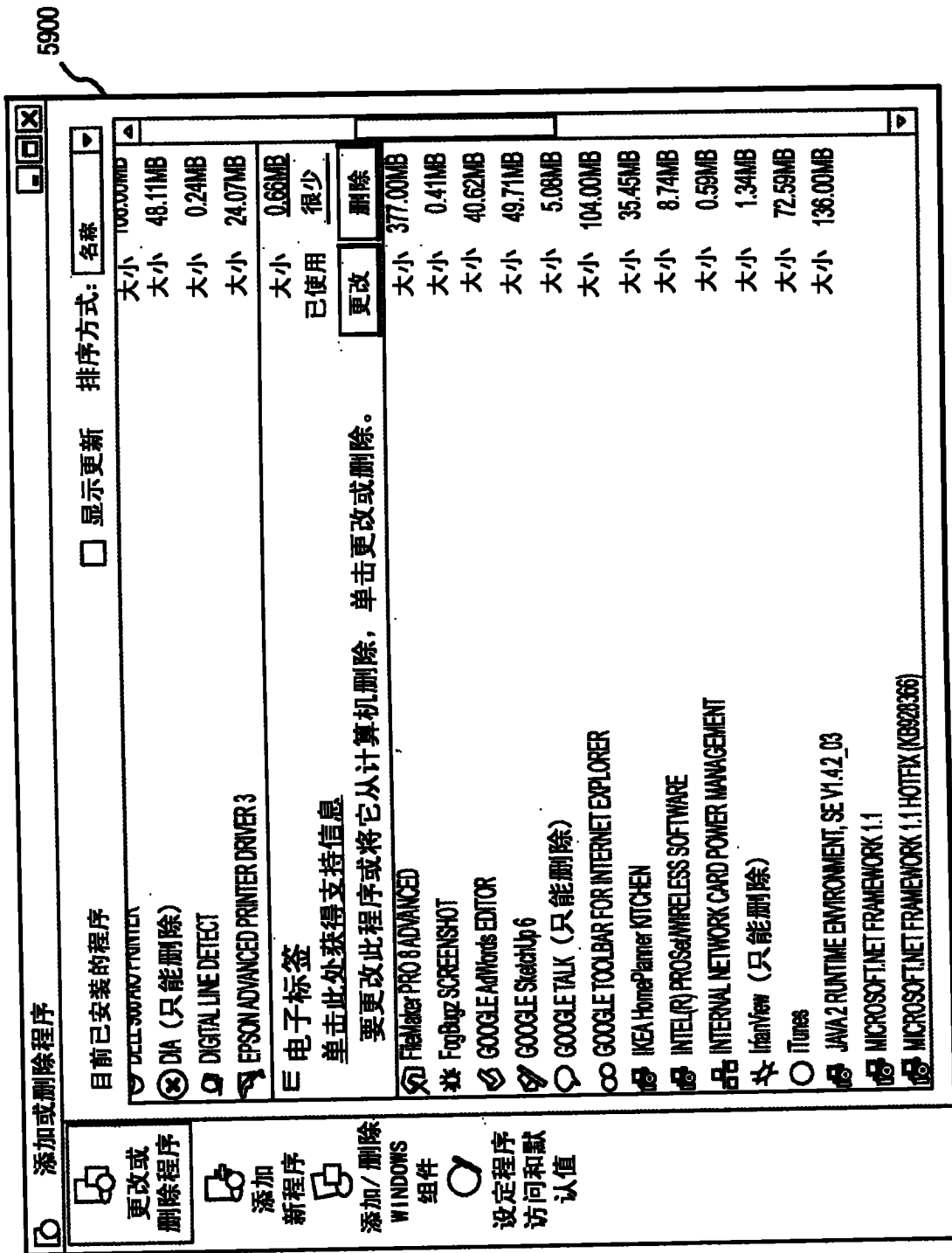


图 59

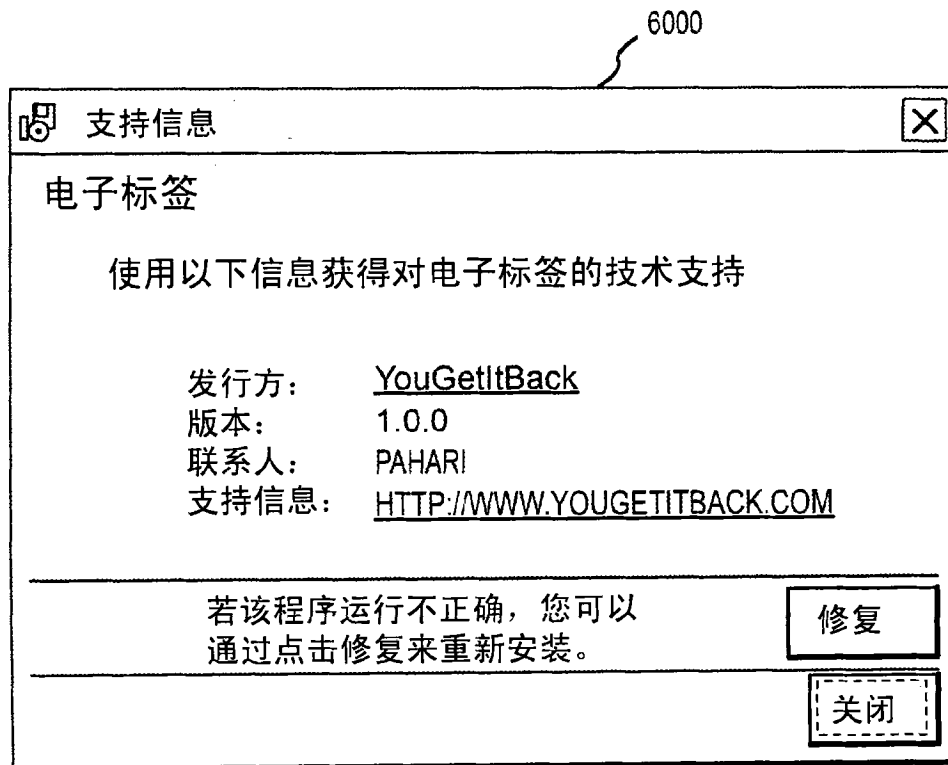


图 60

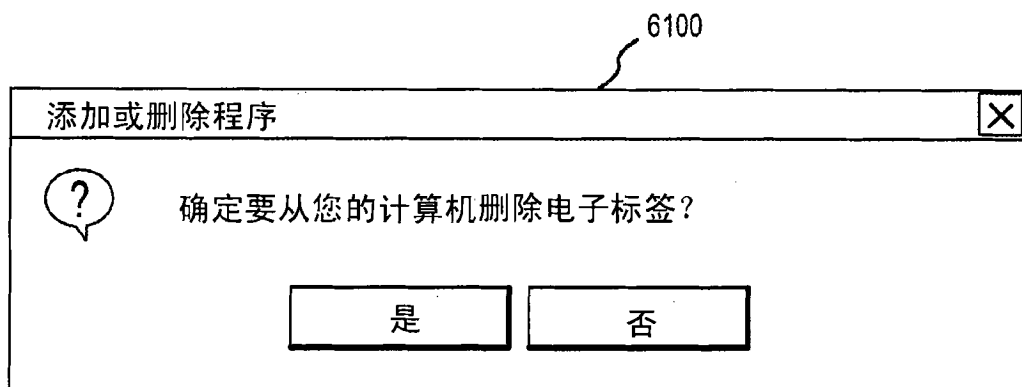


图 61

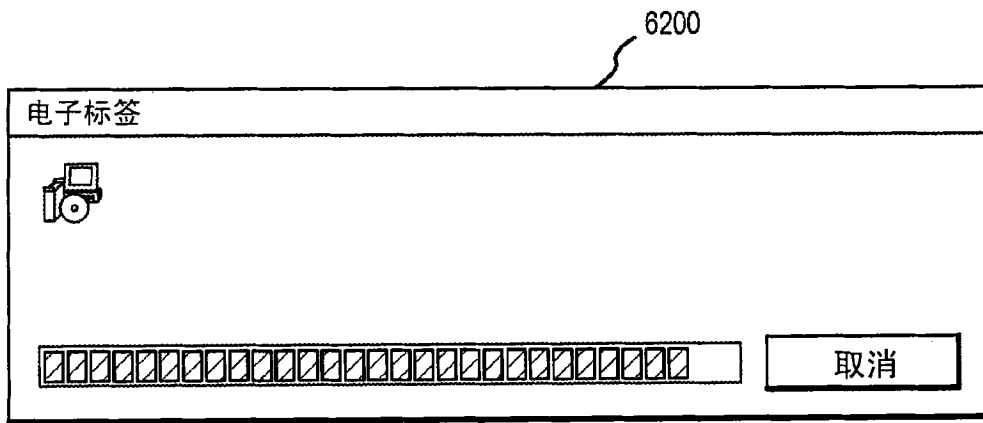


图 62

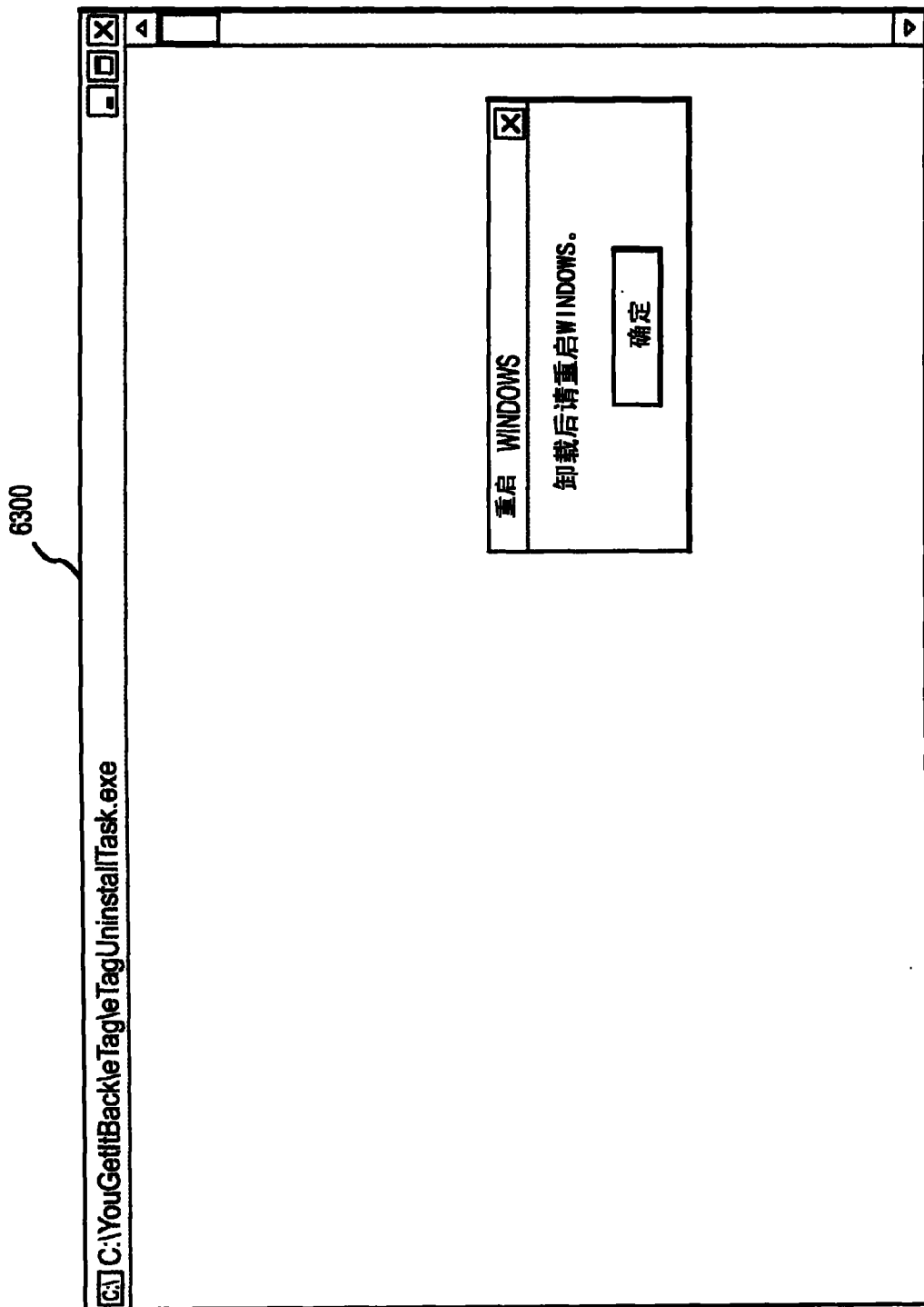


图 63

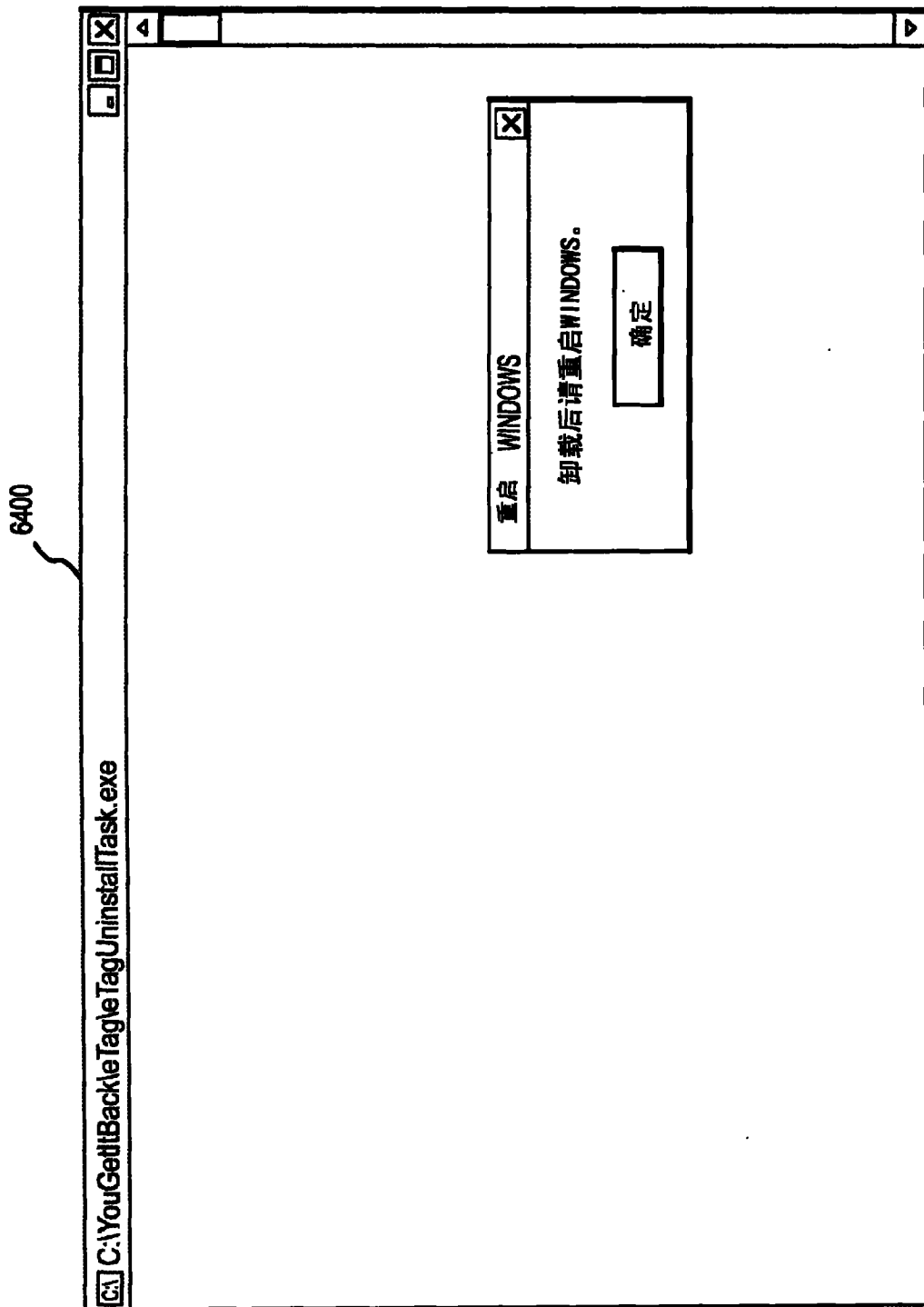


图 64