(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 102024101 A
(43)申请公布日 2011.04.20

(21)申请号 200910190421.4

(22)申请日 2009.09.17

(71)申请人 黄金富
地址 518026 广东省深圳市福田区金田路 3037 号金中环商务大厦 27 层 2705 室

(72)发明人 黄金富

(51)Int.Cl.
G06F 21/00(2006.01)
H04W 12/02(2009.01)

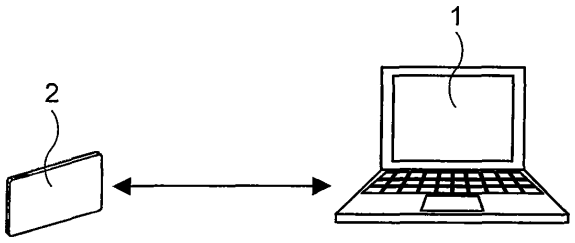
权利要求书 2 页 说明书 6 页 附图 3 页

(54)发明名称

采用自动上锁来保护电子设备防止被人盗用的方法

(57)摘要

一种采用自动上锁来保护电子设备防止被人盗用的方法，用于手机、PDA、计算机、笔记本型计算机等电子设备(1)，所述方法使用可发出身份信息的无线身份识别装置(2)作为电子设备(1)合法用户的凭证，在电子设备(1)内设置监控程序监察无线身份识别装置(2)所发出的身份信息，当监控程序在连续一段指定时间（例如指定时间为5秒）接收不到无线身份识别装置(2)发出的身份信息时，监控程序操控该电子设备(1)进入受保护状态，使该电子设备(1)暂停响应只供合法用户进行的操作，当监控程序再次收到从无线身份识别装置(2)发出的身份信息时，监控程序操控该电子设备(1)从受保护状态返回原来的状态，并恢复响应用户进行的操作。



CN 102024101 A

1. 一种采用自动上锁来保护电子设备防止被人盗用的方法，可用于手机、 PDA、计算机、笔记本型计算机等电子设备 (1)，其特征在于，所述的方法包括使用一可发出身份信息的无线身份识别装置 (2) 作为电子设备 (1) 的合法用户凭证，并在电子设备 (1) 上设置用于与该无线身份识别装置 (2) 通讯的无线通讯装置，以及，在电子设备 (1) 内设置监控程序，该监控程序通过无线通讯装置接收和监察无线身份识别装置 (2) 所发出的身份信息，当监控程序在连续一段指定时间接收不到无线身份识别装置 (2) 所发出的有效身份信息时，监控程序操控该电子设备 (1) 进入受保护状态。

2. 如权利要求 1 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的方法还包括电子设备 (1) 进入受保护状态后，当监控程序通过无线通讯装置接收到从无线身份识别装置 (2) 所发出的有效身份信息时，监控程序操控该电子设备 (1) 从受保护状态返回原来的状态。

3. 如权利要求 1 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的方法还包括电子设备 (1) 通过无线通讯装置向无线身份识别装置 (2) 发出识别信息，当所述的无线身份识别装置 (2) 接收不到所述的电子设备 (1) 发出的识别信息时，无线身份识别装置 (2) 会发出提示信息，提示用户该无线身份识别装置 (2) 收不到电子设备 (1) 的信息。

4. 如权利要求 1 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的无线识别装置 (2) 是射频识别标签，以及，所述的无线通讯装置是射频识别标签阅读器。

5. 如权利要求 1 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的无线识别装置 (2) 是非接触式智能卡，以及，所述的无线通讯装置是无线智能卡阅读器。

6. 如权利要求 1 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的电子设备 (1) 是计算机，包括台式计算机和笔记本型计算机，以及，所述的无线识别装置 (2) 是手机、或无线耳机、或个人数码助理。

7. 如权利要求 1 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的电子设备 (1) 是手机、或个人数码助理，以及，所述的无线识别装置 (2) 是无线耳机。

8. 如权利要求 6 或 7 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的电子设备 (1) 内的无线通讯装置是蓝牙装置，所述的无线识别装置 (2) 设有与所述无线通讯装置相通讯的蓝牙装置。

9. 如权利要求 6 或 7 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的电子设备 (1) 内的无线通讯装置是 WiFi 装置，所述的无线识别装置 (2) 设有与所述无线通讯装置相通讯的 WiFi 装置。

10. 如权利要求 6 或 7 所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的电子设备 (1) 内的无线通讯装置是 WAPI 装置，所述的无线识别装置 (2) 设有与所述无线通讯装置相通讯的 WAPI 装置。

11. 如权利要求 1 至 10 任一项所述的采用自动上锁来保护电子设备防止被人盗用的方法，其特征在于，所述的方法还包括使用一对 PKI 密钥对电子设备 (1) 与无线身份识别装

置 (2) 之间传送的身份信息和识别信息进行加密和解密，其中，无线身份识别装置 (2) 设有该对 PKI 密钥的其中一条 PKI 密钥，而电子设备 (1) 设有对应的另一条 PKI 密钥，以及，无线身份识别装置 (2) 通过其 PKI 密钥将传送给电子设备 (1) 的信息进行加密后才传送，并通过其 PKI 密钥将接收到的信息进行解密，以及，电子设备 (1) 通过其 PKI 密钥将传送给无线身份识别装置 (2) 的信息进行加密后才传送，并通过其 PKI 密钥将接收到的信息进行解密。

采用自动上锁来保护电子设备防止被人盗用的方法

【技术领域】

[0001] 本发明涉及一种采用自动上锁来保护电子设备防止被人盗用的方法。

【背景技术】

[0002] 随着计算机和电子技术的发展，采用这些技术的电子设备也越来越普及，例如手机、PDA、笔记本型计算机、台式计算机等，已经成为很多人生活上的必需品，这些电子设备上很多时会储存有用户的一些个人资料或机密资料，例如手机、PDA 等会储存有用户的电话簿、电邮等，又例如笔记本型计算机、台式计算机等可能会储存有一些商业上的机密资料，虽然可以在电子设备上加上密码保护来限制只准合法用户查阅，但是这会令合法用户每次操作电子设备前都要输入密码，非常不方便。 此外，一些金融机构、政府机关等的工作人员，经常要处理一些机密资料，很多时工作人员都是通过计算机去存取数据库中的机密资料，为了保护这些机密资料，工作人单即使离开计算机很短时间，都要将计算机退出已登录的数据库，防止在离开期间被人偷偷查阅机密资料，到工作人员回到计算机继续工作时，又要重新输入密码登入数据库，才能存取数据库中的机密资料，非常不便。

【发明内容】

[0003] 本发明的目的，在于提供一种采用自动上锁来保护电子设备防止被人盗用的方法，只要合法用户离开电子设备，电子设备就会自动上锁，暂停响应只供合法用户进行的操作。

[0004] 本发明的目的是这样实现的，采用这样一种采用自动上锁来保护电子设备防止被人盗用的方法，可用于手机、PDA、计算机、笔记本型计算机等电子设备 (1)，其特征在于，所述的方法包括使用一可发出身份信息的无线身份识别装置 (2) 作为电子设备 (1) 的合法用户凭证，并在电子设备 (1) 上设置用于与该无线身份识别装置 (2) 通讯的无线通讯装置，以及，在电子设备 (1) 内设置监控程序，该监控程序通过无线通讯装置接收和监察无线身份识别装置 (2) 所发出的身份信息，当监控程序在连续一段指定时间 (例如指定时间为 5 秒) 接收不到无线身份识别装置 (2) 所发出的有效身份信息时，监控程序操控该电子设备 (1) 进入受保护状态，将该电子设备 (1) 上锁，使其暂停响应只供合法用户进行的操作。 此外，所述的方法还包括电子设备 (1) 进入受保护状态后，当监控程序通过无线通讯装置接收到从无线身份识别装置 (2) 所发出的有效身份信息时，监控程序操控该电子设备 (1) 从受保护状态返回原来的状态，将该电子设备 (1) 开锁，使其恢复响应只供合法用户进行的操作。

[0005] 这样就实现了本发明的目的。

[0006] 使用本发明的采用自动上锁来保护电子设备防止被人盗用的方法，可以取代电子设备 (1) 上原来的密码保护，合法用户只要随身携带无线身份识别装置 (2)，就可无限制地操作电子设备 (1)，而当合法用户离开电子设备 (1)，电子设备 (1) 在连续一段指定

时间接收不到合法用户身上携带的无线身份识别装置 (2) 所发出的有效身份信息，就会立即操控电子设备 (1) 上锁，使其进入受保护状态，暂停响应只供合法用户进行的操作指令，使其他人无法使用该电子设备 (1)，从而保护电子设备 (1) 不被人盗用。

【附图说明】

[0007] 图 1 是本发明的第一实施例的示意说明图；

[0008] 图 2 是本发明的第二实施例的示意说明图；

[0009] 图 3 是本发明的第三实施例的示意说明图；

[0010] 图 4 是本发明的第四实施例的示意说明图；

[0011] 图 5 是本发明的第五实施例的示意说明图；

[0012] 图 6 是本发明的第六实施例的示意说明图；

[0013] 图 7 是本发明的第七实施例的示意说明图；

[0014] 图 8 是本发明的第八实施例的示意说明图；

[0015] 图 9 是本发明的第九实施例的示意说明图；

[0016] 图 10 是本发明的第十实施例的示意说明图。

[0017] 图中，相同的数字代表相同的装置、部件器件，方法步骤用带数字和箭头的直线所标出。 附图是示意性的，用以说明本发明的方法的主要特征。

【具体实施方式】

[0018] 下面结合附图，对本发明的方法作进一步详细说明。

[0019] 参阅图 1，图 1 是本发明的第一实施例的示意说明图，图 1 示出的包括有电子设备 (1) 和无线身份识别装置 (2)，其中，无线身份识别装置 (2) 作为电子设备 (1) 的合法用户凭证，电子设备 (1) 上设置有用于与该无线身份识别装置 (2) 通讯的无线通讯装置，无线身份识别装置 (2) 内储存有身份信息，可以通过无线电信号将这身份信息向外发送，以及，在电子设备 (1) 内设置监控程序，该监控程序通过无线通讯装置接收和监察无线身份识别装置 (2) 所发出的身份信息，当监控程序在连续一段指定时间 (例如指定时间为 5 秒) 接收不到无线身份识别装置 (2) 所发出的有效身份信息时，监控程序操控该电子设备 (1) 进入受保护状态，将该电子设备 (1) 上锁，使其暂停响应只供合法用户进行的操作，例如通过滑鼠键盘等操控电子设备 (1)，通过显示屏查阅电子设备 (1) 所储存的资料等等。 此外，在电子设备 (1) 进入受保护状态后，当监控程序通过无线通讯装置再次接收到从无线身份识别装置 (2) 所发出的有效身份信息时，监控程序操控该电子设备 (1) 从受保护状态返回原来的状态，将该电子设备 (1) 开锁，使其恢复响应只供合法用户进行的操作。

[0020] 在设置方面，无线身份识别装置 (2) 内储存有用于认证合法用户身份的身份信息，并将这身份信息与电子设备 (1) 进行配对，电子设备 (1) 接收到这配对的身份信息，就可以确认合法用户的身份，让合法用户使用该电子设备 (1)。在第一实施例中，无线识别装置 (2) 可以采用射频识别标签 (Radio Frequency Identification，简称 RFID)，包括带有电池的射频识别标签及不带电源的射频识别标签，而电子设备 (1) 上的无线通讯装置可以采用射频识别标签阅读器，这射频识别标签与射频识别标签阅读器的有效阅读距离不

能过短，也不能太长，最适合的有效阅读距离为 1 至 3 米。 这样合法用户只要随身携带这射频识别标签，就可以使用电子设备 (1)，当合法用户离开电子设备 (1) 距离 3 米以外时，电子设备 (1) 读取不到射频识别标签内的身份信息，就可以立即进入受保护状态，将电子设备 (1) 上锁，并暂停响应从输入装置输入的操作指令，保护电子设备 (1) 不会被其他人盗用。 此外，所述的无线识别装置 (2) 也可以采用非接触式智能卡，而所述的无线通讯装置则可以采用无线智能卡阅读器，都可很好地实现本发明的目的，都是属于本发明的保护范围。

[0021] 参阅图 2 至图 5，图 2 是本发明的第二实施例的示意说明图，图 3 是本发明的第三实施例的示意说明图，图 4 是本发明的第四实施例的示意说明图，图 5 是本发明的第五实施例的示意说明图，图 2 至图 5 中示出本发明的不同实施例子。 在第二实施例与第一实施例相比，不同之处在于第二实施例的电子设备 (1) 是手机；在第三实施例中，电子设备 (1) 是计算机，包括台式计算机和笔记本型计算机，而无线识别装置 (2) 是手机；在第四实施例中，电子设备 (1) 与第三实施例同样是计算机，但无线识别装置 (2) 采用无线耳机；在第五实施例中，电子设备 (1) 是手机，而无线识别装置 (2) 采用无线耳机；此外，在第三实施例中，可以采用个人数码助理 (Personal Digital Assistant，简称 PDA) 作为无线识别装置 (2)，而在第五实施例中，可以采用个人数码助理作为电子设备 (1)，都可很好地实现本发明的目的。 继续参阅图 1 至图 5，图 1 至图 5 示出的第一至第五实施例中，电子设备 (1) 可以是笔记本型计算机、台式计算机、手机、个人数码助理等等需要保护只供合法用户使用的设备，而无线识别装置 (2) 可以是射频识别标签、无线耳机、手机、个人数码助理等等可以方便合法用户随身携带的装置。

[0022] 参阅图 6，图 6 是本发明的第六实施例的示意说明图，图 6 示出的第六实施例中，电子设备 (1) 是计算机，包括台式计算机和笔记本型计算机，而无线识别装置 (2) 是无线耳机，此外，图 6 中还示出了手机 (3)，该手机 (3) 在本实施例中是同时担任无线识别装置 (2) 和电子设备 (1) 的双重角色，其中，手机 (3) 与电子设备 (1) 之间，手机 (3) 担任了无线识别装置 (2) 的角色，而手机 (3) 与无线识别装置 (2) 之间，手机 (3) 担任了电子设备 (1) 的角色。 本实施例的优点是合法用户只要随身携带了无线耳机，就可以同时防止计算机和手机 (3) 被人非法使用，而且更可以于无线耳机没电时，以手机 (3) 来担任作为操作该计算机的合法用户身份凭证的无线识别装置 (2)。

[0023] 继续参阅图 1 至图 6，图 1 至图 6 示出的各实施例中，电子设备 (1) 与无线识别装置 (2) 之间是采用无线通讯方式通讯，可以采用不同规格标准的通讯装置来实现它们之间的通讯，包括采用以下其中的任一项来实现它们之间的通讯：

[0024] ◆所述的电子设备 (1) 内的无线通讯装置是蓝牙装置，所述的无线识别装置 (2) 设有与所述无线通讯装置相通讯的蓝牙装置。

[0025] ◆所述的电子设备 (1) 内的无线通讯装置是 WiFi 装置，所述的无线识别装置 (2) 设有与所述无线通讯装置相通讯的 WiFi 装置。

[0026] ◆所述的电子设备 (1) 内的无线通讯装置是 WAPI 装置，所述的无线识别装置 (2) 设有与所述无线通讯装置相通讯的 WAPI 装置。

[0027] 本发明的更进一步改进，是增加防止丢失电子设备 (1) 功能，实现这改进的方法包括电子设备 (1) 通过无线通讯装置向无线身份识别装置 (2) 发出识别信息，当所述的

无线身份识别装置 (2) 接收不到所述的电子设备 (1) 发出的识别信息时，无线身份识别装置 (2) 会发出提示信息，提示用户该无线身份识别装置 (2) 收不到电子设备 (1) 的信息。这样用户只要随身携带无线身份识别装置 (2)，当用户离开电子设备 (1) 时，无线身份识别装置 (2) 就会立即向用户发出提示信息，提示用户不要遗下电子设备 (1) 以避免丢失。

[0028] 参阅图 7 至图 10，图 7 是本发明的第七实施例的示意说明图，图 8 是本发明的第八实施例的示意说明图，图 9 是本发明的第九实施例的示意说明图，图 10 是本发明的第十实施例的示意说明图，图 7 至图 10 示出的各实施例是采用 PKI 密钥来加强安全性的改进，所采用的方法包括使用一对 PKI 密钥对电子设备 (1) 与无线身份识别装置 (2) 之间传送的身份信息和识别信息进行加密和解密，其中，无线身份识别装置 (2) 设有该对 PKI 密钥的其中一条 PKI 密钥，而电子设备 (1) 设有对应的另一条 PKI 密钥，以及，无线身份识别装置 (2) 通过其 PKI 密钥将传送给电子设备 (1) 的信息进行加密后才传送，并通过其 PKI 密钥将接收到的信息进行解密，以及，电子设备 (1) 通过其 PKI 密钥将传送给无线身份识别装置 (2) 的信息进行加密后才传送，并通过其 PKI 密钥将接收到的信息进行解密。

[0029] 继续参阅图 7，图 7 中示出了包括如下的 A 组步骤，是由无线身份识别装置 (2) 发起认证双方身份的步骤，具体的 A 组步骤如下 ：

[0030] A1. 无线身份识别装置 (2) 随机产生一随机数，以其 PKI 密钥将无线身份识别装置 (2) 的身份信息连同随机数加密后传送给电子设备 (1) ；

[0031] A2. 电子设备 (1) 以其 PKI 密钥将收到的信息解密还原出身份信息和随机数，然后以其 PKI 密钥将随机数和身份信息连同电子设备 (1) 的识别信息加密后传回无线身份识别装置 (2) ；

[0032] A3. 无线身份识别装置 (2) 以其 PKI 密钥将传回来的信息解密还原出身份信息和随机数及识别信息，核对随机数无误后，就确认了电子设备 (1) 的身份，然后随机产生一新的随机数，然后以其 PKI 密钥将身份信息连同新产生的随机数及识别信息加密后传送给电子设备 (1) ；

[0033] A4. 电子设备 (1) 以其 PKI 密钥将收到的信息解密还原出身份信息和随机数及识别信息，核对身份信息和识别信息无误后，就确认了无线身份识别装置 (2) 的身份 ；

[0034] 电子设备 (1) 以其 PKI 密钥将随机数和身份信息连同电子设备 (1) 的识别信息加密后传回无线身份识别装置 (2)，然后转到步骤 A3。

[0035] 继续参阅图 8，图 8 中示出了包括如下的 B 组步骤，与图 7 的实施例相比，主要不同之处在于图 8 的实施例中，是由电子设备 (1) 发起认证双方身份的步骤，具体的 B 组步骤如下 ：

[0036] B1. 电子设备 (1) 随机产生一随机数，以其 PKI 密钥将电子设备 (1) 的识别信息连同随机数加密后传送给无线身份识别装置 (2) ；

[0037] B2. 无线身份识别装置 (2) 以其 PKI 密钥将收到的信息解密还原出识别信息及随机数，然后以其 PKI 密钥将随机数及识别信息连同无线身份识别装置 (2) 的身份信息加密后传回无线电子设备 (1) ；

[0038] B3. 电子设备 (1) 以其 PKI 密钥将传回来的信息解密还原出识别信息及随机数和身份信息，核对随机数无误后，就确认了无线身份识别装置 (2) 的身份，然后随机产生一新的随机数，然后以其 PKI 密钥将识别信息连同新产生的随机数和身份信息加密后传

送给无线身份识别装置 (2)；

[0039] B4. 无线身份识别装置 (2) 以其 PKI 密钥将收到的信息解密还原出识别信息及随机数和身份信息，核对识别信息和身份信息无误后，就确认了电子设备 (1) 的身份；

[0040] 无线身份识别装置 (2) 以其 PKI 密钥将随机数及识别信息连同无线身份识别装置 (2) 的身份信息加密后传回电子设备 (1)，然后转到步骤 B3。

[0041] 继续参阅图 9，图 9 中示出了包括如下的 C 组步骤，与图 8 的实施例相比，主要不同之处在于图 9 的实施例中，电子设备 (1) 和无线身份识别装置 (2) 各自产生自己的随机数来进行认证步骤，具体的 C 组步骤如下：

[0042] C1. 电子设备 (1) 随机产生一随机数甲，以其 PKI 密钥将电子设备 (1) 的识别信息连同随机数甲加密后传送给无线身份识别装置 (2)；

[0043] C2. 无线身份识别装置 (2) 以其 PKI 密钥将收到的信息解密还原出识别信息和随机数甲，并随机产生一随机数乙，然后无线身份识别装置 (2) 以其 PKI 密钥将随机数甲和识别信息连同无线身份识别装置 (2) 的身份信息和随机数乙加密后传回电子设备 (1)；

[0044] C3. 电子设备 (1) 以其 PKI 密钥将传回来的信息解密还原出识别信息和随机数甲及身份信息和随机数乙，核对随机数甲无误后，就确认了无线身份识别装置 (2) 的身份，然后随机产生一新的随机数甲，然后以其 PKI 密钥将识别信息连同新产生的随机数甲及身份信息和随机数乙加密后传送给无线身份识别装置 (2)；

[0045] C4. 无线身份识别装置 (2) 以其 PKI 密钥将收到的信息解密还原出识别份信息和随机数甲及身份信息和随机数乙，核对识别信息及身份信息和随机数乙无误后，就确认了电子设备 (1) 的身份；

[0046] 无线身份识别装置 (2) 随机产生一新的随机数乙，然后以其 PKI 密钥将随机数甲及识别信息连同无线身份识别装置 (2) 的身份信息和随机数乙加密后传回电子设备 (1)，然后转到步骤 C3。

[0047] 继续参阅图 10，图 10 中示出了包括如下的 D 组步骤，与图 9 的实施例相比，主要不同之处在于图 10 的实施例中，是由无线身份识别装置 (2) 发起认证双方身份的步骤，具体的 D 组步骤如下：

[0048] D1. 无线身份识别装置 (2) 随机产生一随机数甲，以其 PKI 密钥将无线身份识别装置 (2) 的身份信息连同随机数甲加密后传送给电子设备 (1)；

[0049] D2. 电子设备 (1) 以其 PKI 密钥将收到的信息解密还原出身份信息和随机数甲，并随机产生一随机数乙，然后电子设备 (1) 以其 PKI 密钥将随机数甲和身份信息连同电子设备 (1) 的识别信息和随机数乙加密后传回无线身份识别装置 (2)；

[0050] D3. 无线身份识别装置 (2) 以其 PKI 密钥将传回来的信息解密还原出身份信息和随机数甲及识别信息和随机数乙，核对随机数甲无误后，就确认了电子设备 (1) 的身份，然后随机产生一新的随机数甲，然后以其 PKI 密钥将身份信息连同新产生的随机数甲及识别信息和随机数乙加密后传送给电子设备 (1)；

[0051] D4. 电子设备 (1) 以其 PKI 密钥将收到的信息解密还原出身份份信息和随机数甲及识别信息和随机数乙，核对身份信息及识别信息和随机数乙无误后，就确认了无线身份识别装置 (2) 的身份；

[0052] 电子设备 (1) 随机产生一新的随机数乙，然后以其 PKI 密钥将随机数甲及身份信

息连同电子设备 (1) 的识别信息和随机数乙加密后传回无线身份识别装置 (2)，然后转到步骤 D3。

[0053] 以上已经详细说明本发明的特征，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。

[0054] 本发明的采用自动上锁来保护电子设备防止被人盗用的方法，可以防止电子设备 (1) 被人盗用，合法用户只要随身携带无线身份识别装置 (2)，就可无限制地如常操作电子设备 (1)，只要合法用户离开电子设备 (1)，电子设备 (1) 就会立即上锁并进入受保护状态，使其他人无法使用该电子设备 (1)，直至合法用户回到电子设备 (1) 前，电子设备 (1) 就会立即恢复原来状态，合法用户又可以无限制地如常操作电子设备 (1)。 此外，当合法用户离开电子设备 (1) 时，无线身份识别装置 (2) 更会发出提示信息，提示用户不要遗下电子设备 (1) 以避免丢失。

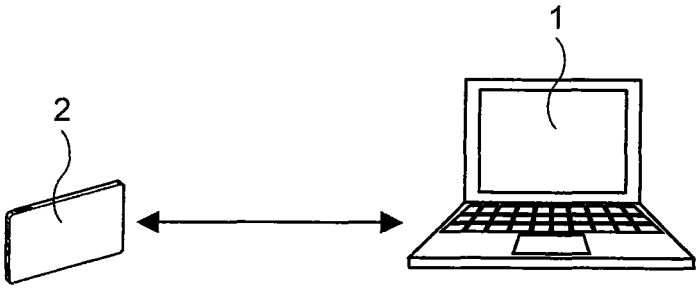


图 1

图 2

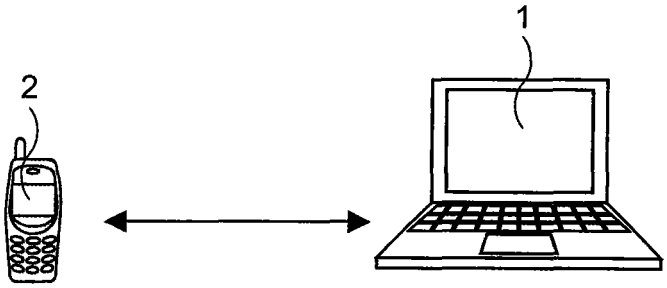


图 3

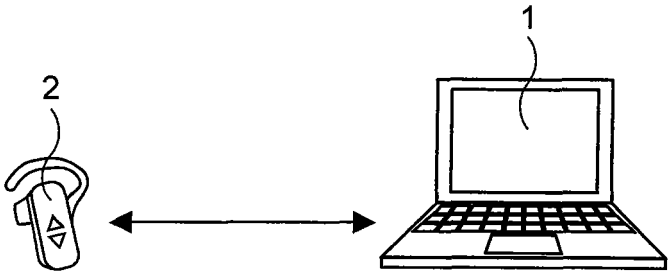


图 4

图 5

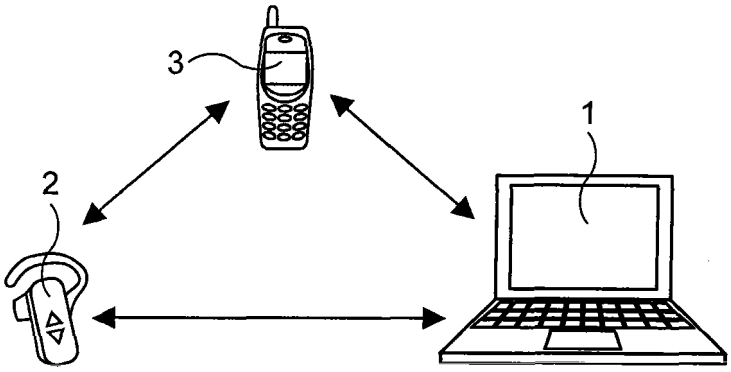


图 6

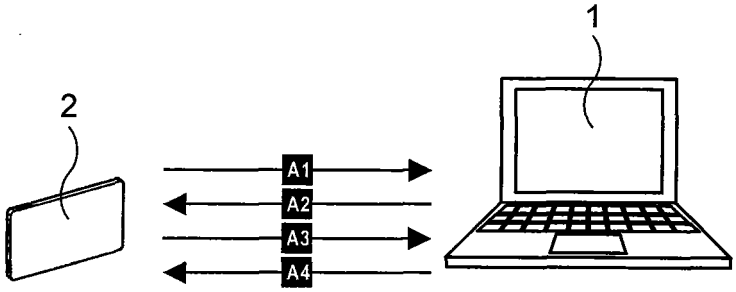


图 7

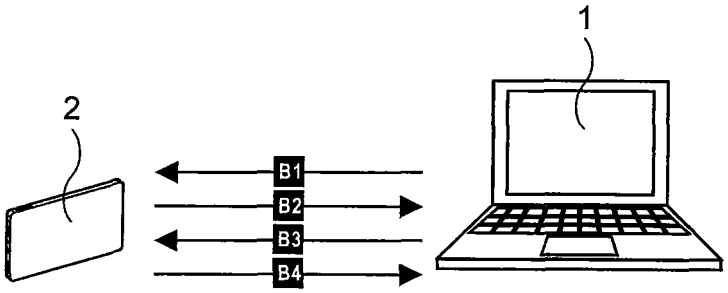


图 8

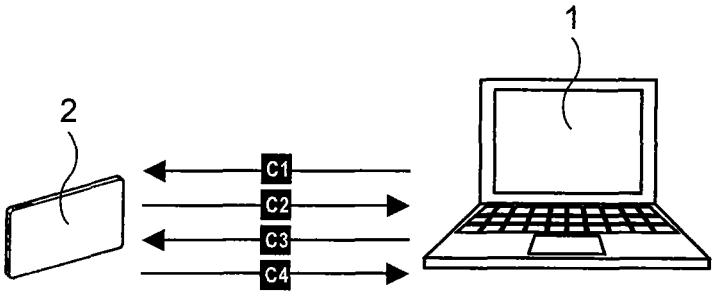


图 9

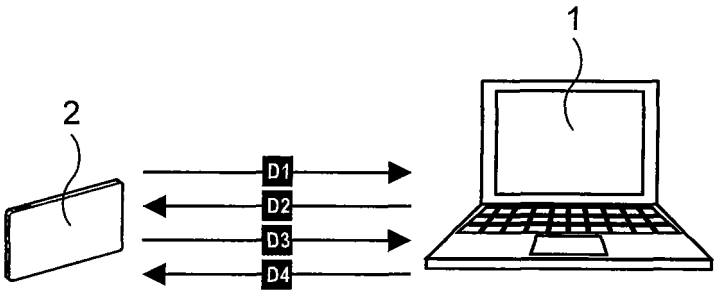


图 10