(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 101504710 B
(45)授权公告日 2010.08.11

(21)申请号 200910080695.8

(22)申请日 2009.03.26

(73)专利权人 北京鼎普科技股份有限公司
地址 100086 北京市海淀区北三环西路 43 号 6 区 46 号楼

(72)发明人 于晴 王海洋

(74)专利代理机构 北京元本知识产权代理事务所 11308
代理人 秦力军

(51)Int.Cl.
G06F 21/24(2006.01)
H04B 10/12(2006.01)

审查员 刘邵频

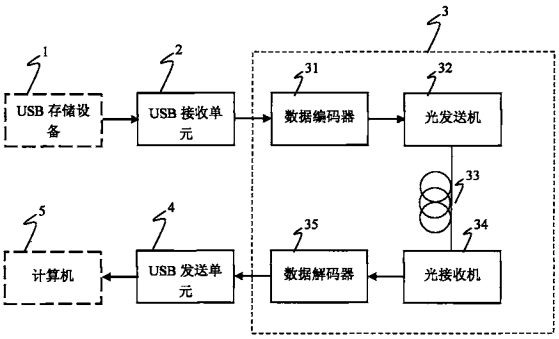
权利要求书 2 页 说明书 5 页 附图 2 页

(54)发明名称

对内网计算机进行安全防护的方法及设备

(57)摘要

本发明公开了对内网计算机进行安全防护的方法及设备。本发明的方法包括以下步骤:A)计算机实时检测插入USB接口的USB设备,一旦确定所检测的USB设备是易泄密设备,就立即禁用所插入的USB设备;B)将USB存储设备经由单向导入设备接入计算机的USB接口,使所述USB存储设备只能经由所述数据单向导入设备向所述计算机单向传输所存储的数据。本发明的上述方法可以防止易泄密设备通过计算机的USB接口得到计算机存储的数据。同时,还可以单向地把易泄密设备的数据传送给计算机,从而实现了计算机至易泄密设备方向的物理隔离。



CN 101504710 B

1. 一种防止计算机数据外泄的方法，包括以下步骤：

计算机实时检测插入 USB 接口的 USB 设备，判断所插入的 USB 设备是否为 USB 鼠标或键盘或数据单向导入设备；

如果判断不是 USB 鼠标或键盘或数据单向导入设备之中的任一个，则禁用所插入的 USB 设备；

如果判断是 USB 鼠标或键盘则允许使用 USB 鼠标或键盘；

如果判断是数据单向导入设备，则允许数据单向导入设备将 USB 存储设备存储的数据传送给计算机。

2. 根据权利要求 1 所述的方法，其中所述数据单向导入设备通过以下步骤将所述 USB 存储设备中存储的数据单向传输给所述计算机：

首先从所述 USB 存储设备中读取其内存储的文件的文件目录；

根据文件目录，选择将要发送给计算机的指定文件；

对所述指定文件的数据进行编码；

单向传送已编码数据；

对所述单向传送的已编码数据进行解码，得到所述指定文件的数据；

然后将指定文件的数据传送给计算机。

3. 根据权利要求 2 所述的方法，其中利用光传输装置单向传送已编码数据，包括：

光发送模块 (32) 将已编码数据信号进行电光转换，变换成光数据信号，然后经由光纤 (33) 单向传输；

光接收模块 (34) 将经由所述光纤传输的光数据信号进行光电转换，还原成所述已编码数据信号。

4. 一种在权利要求 1 至 3 任一项方法中执行数据单向导入的设备，包括：

连接 USB 存储设备 (1)、指定所述 USB 存储设备 (1) 中存储的文件，并对指定文件进行数据发送的 USB 接收单元 (2)；

对所述 USB 接收单元 (2) 发送的数据进行单向传输的单向传输装置 (3)；以及

接收所述单向传输装置 (3) 传输的数据，并将其发送给计算机 (5) 的 USB 发送单元 (4)。

5. 根据权利要求 4 所述的设备，其中所述 USB 接收单元 (2) 包括：

自动检测 USB 存储设备接入的检测模块；

查询所接入的 USB 存储设备中存储的文件，从而得到文件目录信息的查询模块；

根据文件目录信息选择待发送的指定文件，并发出相应指令的若干按键；

根据按键所发出的发送指令，发送所述指定文件的数据的发送模块；以及

进行查询、选择、指令显示的显示器。

6. 根据权利要求 4 或 5 所述的设备，其中所述单向传输装置 (3) 是声、光、电单向传输装置之一。

7. 根据权利要求 6 所述的设备，其中所述单向传输装置 (3) 包括：

对所述 USB 接收单元 (2) 发送的数据进行数据编码的编码器 (31)；

把所述编码器已编码数据信号转换成光信号并进行光发送的光发送机 (32)；

传输所述光信号的光纤 (33)；

接收经由所述光纤传输的光信号并将其转换成电信号，从而得到已编码数据信号的光接收机 (34) ；以及

对所述光接收机输出的已编码数据进行解码的解码器 (35)。

8. 根据权利要求 7 所述的设备，其中所述 USB 接收单元 (2) 和 / 或数据编码器 (31) 由单片机或可编程逻辑器件构成，并且所述 USB 接收单元 (2) 和 / 或数据编码器 (31) 具有对所发送的数据进行缓存的缓存区 ；以及

所述 USB 发送单元 (4) 和 / 或数据解码器 (35) 由单片机或可编程逻辑器件构成，并且所述 USB 发送单元 (4) 和 / 或数据解码器 (35) 具有对所接收的数据进行缓存的缓存区。

对内网计算机进行安全防护的方法及设备

技术领域

[0001] 本发明涉及计算机数据安全防护方法及其设备，特别是防止计算机数据外泄的方法及其数据单向导入的设备。

背景技术

[0002] 现今政府及企事业单位 80％以上的数据以电子格式存放在内部网络中，同时各种移动存储设备的更新也越来越快，敏感信息、秘密数据和档案资料被存贮在移动介质里，大量的秘密文件和资料变为磁性介质，存贮在无保护的移动存储介质中，如果放任不管，任意滥用移动存储介质必将会带来难以估计的损失。近年来屡屡发生的移动存储介质泄密、窃密案件给国家和企事业单位带来了不可估量的损失。

[0003] 另一方面，内网计算机可以通过无线上网，出现内网计算机非法外联的现象，这也会使内网数据外泄。

[0004] 因此，为涉密计算机提供有效、可靠的数据传输解决方案至关重要。

发明内容

[0005] 本发明的一个目的是提供防止计算机数据外泄的方法。

[0006] 本发明的另一目的是提供一种在防止计算机数据外泄方法中执行数据单向导入的设备。

[0007] 本发明一方面利用单向传输，为 USB 存储设备和计算机之间传递数据的桥梁，在保证数据被快速、正确的传输到计算机的同时，有效的保证了计算机中的任何数据不外泄。

[0008] 本发明的防止计算机数据外泄的方法，包括以下步骤 ：

[0009] A) 计算机实时检测插入 USB 接口的 USB 设备，一旦确定所检测的 USB 设备是易泄密设备，就立即禁用所插入的 USB 设备 ；

[0010] B) 将 USB 存储设备经由单向导入设备接入计算机的 USB 接口，使所述 USB 存储设备只能经由所述数据单向导入设备向所述计算机单向传输所存储的数据。

[0011] 上述方法可以防止易泄密设备通过计算机的 USN 接口得到计算机存储的数据。同时，还可以单向地把易泄密设备的数据传送给计算机，从而实现了计算机至易泄密设备方向的物理隔离。

[0012] 其中在所述步骤 A) 中，当计算机检测到所述 USB 设备是数据单向导入设备、USB 鼠标、USB 键盘之外的设备时，则确定所检测的 USB 设备是易泄密设备。

[0013] 其中在所述步骤 B) 中，所述数据单向导入设备通过以下步骤将所述 USB 设备中存储的数据单向传输给所述计算机 ：

[0014] 首先从所述 USB 存储设备中读取其内存储的文件的文件目录 ；

[0015] 根据文件目录，选择将要发送给计算机的指定文件 ；

[0016] 对所述指定文件的数据进行编码 ；

[0017] 单向传送已编码数据 ；

[0018] 对所述单向传送的已编码数据进行解码，得到所述指定文件的数据；

[0019] 然后将指定文件的数据传送给计算机。

[0020] 其中利用光传输装置单向传送已编码数据，包括：

[0021] 光发送模块将已编码数据信号进行电光转换，变换成光数据信号，然后经由光纤单向传输；

[0022] 光接收模块将经由所述光纤传输光数据信号进行光电转换，还原成所述已编码数据信号。

[0023] 上述方法还可以包括：

[0024] 本发明的在防止计算机数据外泄方法中执行数据单向导入的设备包括：

[0025] 连接USB存储设备、指定所述USB存储设备中存储的文件，并对指定文件进行数据发送的USB接收单元；

[0026] 对所述USB接收单元发送的数据进行单向传输的单向传输装置；以及

[0027] 接收所述单向传输装置传输的数据，并将其发送给计算机的USB发送单元。

[0028] 其中所述USB接收单元包括：自动检测USB存储设备接入的检测模块；查询所接入的USB存储设备中存储的文件，从而得到文件目录信息的查询模块；根据文件目录信息选择待发送的指定文件，并发出相应指令的若干按键；根据按键所发出的发送指令，发送所述指定文件的数据的发送模块；以及进行查询、选择、指令显示的显示器。

[0029] 其中所述单向传输装置可以是光、电单向传输装置之一。

[0030] 其中所述单向传输装置包括：对所述USB接收单元发送的数据进行数据编码的编码器；以及把所述编码器已编码数据信号转换成光信号并进行光发送的光发送机；传输所述光信号的光纤；接收经由所述光纤传输的光信号并将其转换成电信号，从而得到已编码数据信号的光接收机；以及对所述光接收机输出的已编码数据进行解码的解码器。

[0031] 所述USB接收单元和/或数据编码器由单片机或可编程逻辑器件构成，两者或两者之一具有对所发送的数据进行缓存的缓存区；以及

[0032] 所述USB发送单元和/或数据解码器由单片机或可编程逻辑器件构成，两者或两者之一具有对所接收的数据进行缓存的缓存区。

[0033] 利用本发明的上述方法和设备可以实现以下技术效果：

[0034] 对所有USB接口、USB设备准确有效的监控，保证了除单向传输设备以及USB鼠标、USB键盘外的其他任何USB设备均不被允许使用，从而切断了通过USB设备外泄计算机数据的渠道。

[0035] 下面结合附图对本发明的原理、细节进行详细说明。

附图说明

[0036] 图1是实现本发明的第一种防止计算机数据外泄方法的流程图；

[0037] 图2是显示执行本发明方法的数据单向导入设备的示意图；

[0038] 图3是本发明的数据单向导入设备的USB接收单元执行检测、查询、指定操作的示意图；

[0039] 图4是本发明的数据单向导入设备的USB接收单元发送指定文件的示意图。

具体实施方式

[0040] 本发明所称的易泄密设备是指能够输出和 / 或下载计算机数据，从而有可能造成计算机数据泄密的 USB 设备，本发明的易泄密设备包括但不限于 ：移动硬盘、U 盘、MP3、MP4、数码相机、打印机等在内的 USB 设备。

[0041] 本发明的防止计算机数据外泄的方法包括以下步骤 ：

[0042] A) 计算机实时检测插入 USB 接口的 USB 设备，一旦确定所检测的 USB 设备是易泄密设备，就立即禁用所插入的 USB 设备 ；本发明的步骤 A) 可以避免利用 USB 设备下载计算机数据的事件发生。

[0043] B) 将 USB 存储设备经由单向导入设备接入计算机的 USB 接口，使所述 USB 存储设备只能经由所述数据单向导入设备向所述计算机单向传输所存储的数据。由于利用单向传输技术，因此本发明的步骤 B) 能够将 USB 存储设备中存储的数据发送给计算机，同时又防止将计算机的数据下载到 USB 存储设备中。

[0044] 在上述步骤 A) 中，当计算机检测到所述 USB 设备是数据单向导入设备或者 USB 鼠标或者 USB 键盘之外的设备时，则确定所检测的 USB 设备是易泄密设备。计算机可以通过 USB 检测软件 (如 USBTrace) 检测 USB 设备的详细信息如硬件 ID，由此确定 USB 设备是否是数据单向导入设备、USB 鼠标、USB 键盘之一，如果不是其中的任何一个，则判定该 USB 设备是易泄密设备。

[0045] 在上述步骤 B) 中，所述数据单向导入设备通过以下步骤将所述 USB 设备中存储的数据单向传输给所述计算机 ：

[0046] 首先从所述 USB 存储设备中读取其内存储的文件的文件目录 ；根据文件目录，选择将要发送给计算机的指定文件，即指定将要发送给计算机的文件 ；对所述指定文件的数据进行编码 ；单向传送已编码数据 ；对所述单向传送的已编码数据进行解码，得到所述指定文件的数据 ；然后将指定文件的数据传送给计算机。

[0047] 本发明可以利用光单向传输装置实现已编码数据的单向传送，这通常包括 ：光发送模块将已编码数据信号进行电光转换，变换成光数据信号，然后经由光纤单向传输 ；光接收模块将经由所述光纤传输光数据信号进行光电转换，还原成所述已编码数据信号。

[0048] 图 1 显示了实现本发明的第一种防止计算机数据外泄方法的流程图，首先计算机实时检测插入计算机 USB 接口的 USB 设备 ；接着判断所插入的 USB 设备是 USB 鼠标或键盘或数据单向导入设备，如果判断不是 USB 鼠标或键盘或数据单向导入设备之中的任一个，则禁用所插入的 USB 设备，如果判断是 USB 鼠标或键盘则允许使用 USB 鼠标或键盘 ；如果判断是数据单向导入设备，则允许数据单向导入设备将 USB 设备存储的数据传送给计算机。

[0049] 本发明的第二种防止计算机数据外泄的方法包括以下步骤 ：

[0050] A) 计算机实时检测插入 USB 接口的 USB 设备，一旦确定所检测的 USB 设备是易泄密设备，就立即禁用所插入的 USB 设备 ；

[0051] B) 将 USB 存储设备经由单向导入设备接入计算机的 USB 接口，使所述 USB 存储设备只能经由所述数据单向导入设备向所述计算机单向传输所存储的数据 ；

[0052] 图 2 显示了在本发明的上述两种方法中执行数据单向传输的设备，图中利用实线框显示本发明设备的结构。如图 3 所示，本发明的执行数据单向传输的设备包括 ：

[0053] 连接 USB 存储设备 1、指定所述 USB 存储设备 1 中存储的文件，并对指定文件进行

数据发送的USB接收单元2；该USB接收单元2可以是具有USB插座的单片机或微计算机，它可以随时发现插入的USB存储设备、对其进行查询，并进行指定文件和发送指定文件的处理。

[0054] 对所述USB接收单元2发送的数据进行单向传输的单向传输装置3；该单向传输装置可以是声、光、电单向传输装置之一。

[0055] 接收所述单向传输装置3传输的数据，并将其发送给计算机5的USB发送单元4。

[0056] USB接收单元2可以包括：自动检测USB存储设备接入的检测模块；查询所接入的USB存储设备中存储的文件，从而得到文件目录信息的查询模块；根据文件目录信息选择待发送的指定文件，并发出相应指令的若干按键；根据按键所发出的发送指令，发送所述指定文件的数据的发送模块；以及进行查询、选择、指令显示的显示器。

[0057] 图3显示了USB接收单元的检测、查询、指定操作。当USB存储设备连接到单向导入设备时，USB接收单元（如单片机Tx MCU）可以立即响应到，通过液晶显示展示给用户界面。Tx MCU上的文件系统在响应到USB设备后，会查询USB设备中的文件，返回其文件信息。通过按键的响应操作查看各级目录，同时在液晶上显示。液晶屏幕采用256*64的分辨率，可以显示四行、每行最多16个汉字。按键包括Enter键（进入一个子目录，或选择）、Exit键（退出到上层目录）、Up键（向上滚动）、Down键（向下滚动）和Cancel键（撤销）。液晶屏幕和按键配合使用，可以查看目录结构、定位文件、选定文件、发送文件或撤销发送。

[0058] 图4显示了USB接收单元的指定文件发送操作。当用户选定好要发送的文件（例如图中的指定文件），通过按键响应操作将文件的存储首地址等信息送到Tx MCU，MCU处理后再通过数据总线将文件信息和内容传送到下级数据处理模块（例如数据缓存模块，以便提供2K Byte的数据缓存），在这个过程中同样离不开文件系统的帮忙。在传送过程中，用户仍然可以通过按键的响应来中断传送，MCU可以通过响应操作告诉下级模块放弃此次发送。

[0059] 当利用单向传输设备上选定文件并按Enter键发送后，终端应用软件自动弹出对话框提示用户选择文件保存的地址，确定目标地址后文件开始传输，并用进度条提示当前数据传输进度。除非用户在单向导入设备上按Cancel键终止数据发送过程，否则数据传输一直进行直至整个文件传送完毕。

[0060] 再参见图2，单向传输装置3包括：对所述USB接收单元2发送的数据进行数据编码的编码器31；把所述编码器已编码数据信号转换成光信号并进行光发送的光发送机32；传输所述光信号的光纤33；接收经由所述光纤传输的光信号并将其转换成电信号，从而得到已编码数据信号的光接收机34；以及对所述光接收机输出的已编码数据进行解码的解码器35。

[0061] USB接收单元2和/或数据编码器31可以由单片机或可编程逻辑器件构成，两者或两者之一具有对所发送的数据进行缓存的缓存区，从而在USB接收单元2与光发送机32之间建立数据缓冲区；以及

[0062] USB发送单元4和/或数据解码器35可以由单片机或可编程逻辑器件构成，两者或两者之一具有对所接收的数据进行缓存的缓存区，从而在USB发送单元4与光接收机34之间建立数据缓冲区。

[0063] 本发明具有以下特点：

[0064] 1、对所有 USB 接口、USB 设备准确有效的监控，保证了除单向传输设备以及 USB 鼠标、USB 键盘外的其他任何 USB 设备均不被允许使用。

[0065] 2、利用光单向传输特性保证了数据的单向传输。在单向倒入设备中利用光的这个特性，实现了数据只能从 USB 存储设备通过单向导入设备传送到计算机上，计算机上的任何数据不能反向回传。

[0066] 3、在 USB 接收器上实现了文件系统，可以获取连接的 USB 存储设备的文件目录结构，并传递给显示模块由液晶屏幕显示，借助液晶屏幕和按键可以查看 USB 存储设备的文件目录结构并自行选择目标文件进行发送。

[0067] 4、在 USB 接收器到光传输模块之间，以及光传输模块到 USB 发送器之间硬件（例如在 USB 接收器和 USB 发送单元中）实现 2K Byte 的数据缓冲区，保证了数据传输的速度和效率。

[0068] 5、在数据单向传输中，进行数据编码和数据解码，从而保证了数据传输的正确性。

[0069] 尽管上文对本发明进行了详细说明，但是本发明不限于此，本技术领域技术人员可以根据本发明的原理进行各种修改。因此，凡按照本发明原理所作的修改，都应当理解为落入本发明的保护范围。

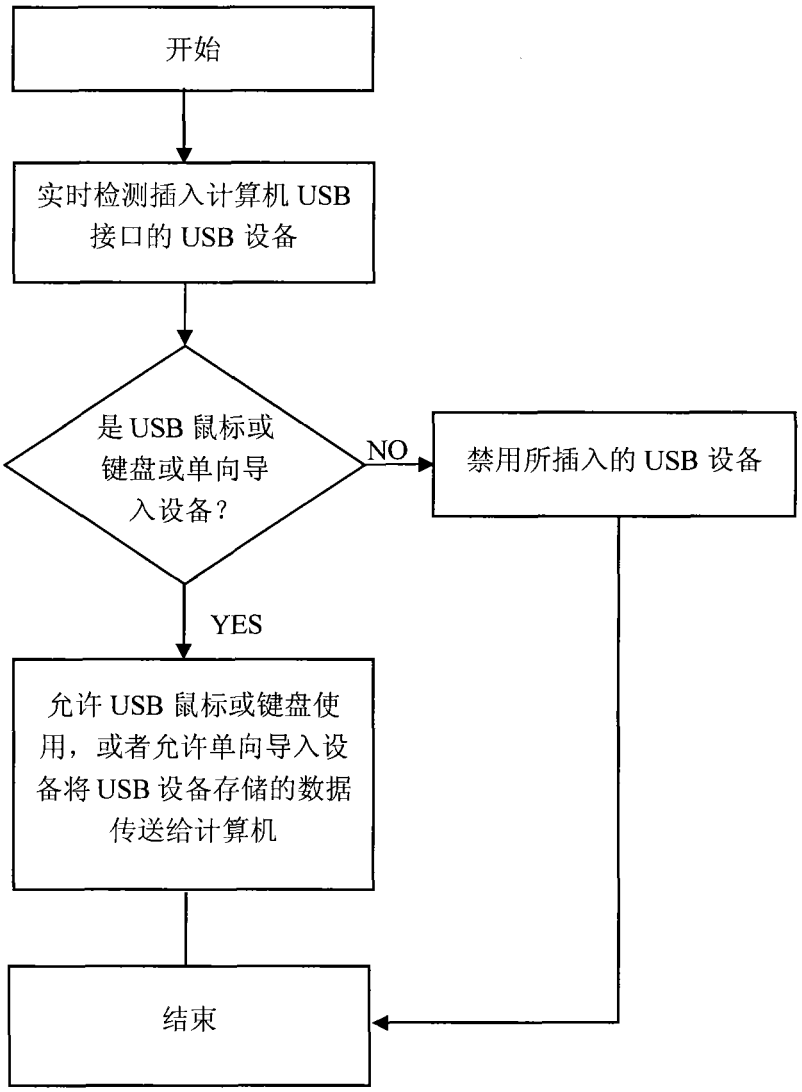

开始
实时检测插入计算机 USB 接口的 USB 设备
是 USB 鼠标或键盘或单向导入设备？
NO
禁用所插入的 USB 设备
YES
允许 USB 鼠标或键盘使用，或者允许单向导入设备将 USB 设备存储的数据传送给计算机
结束

图 1

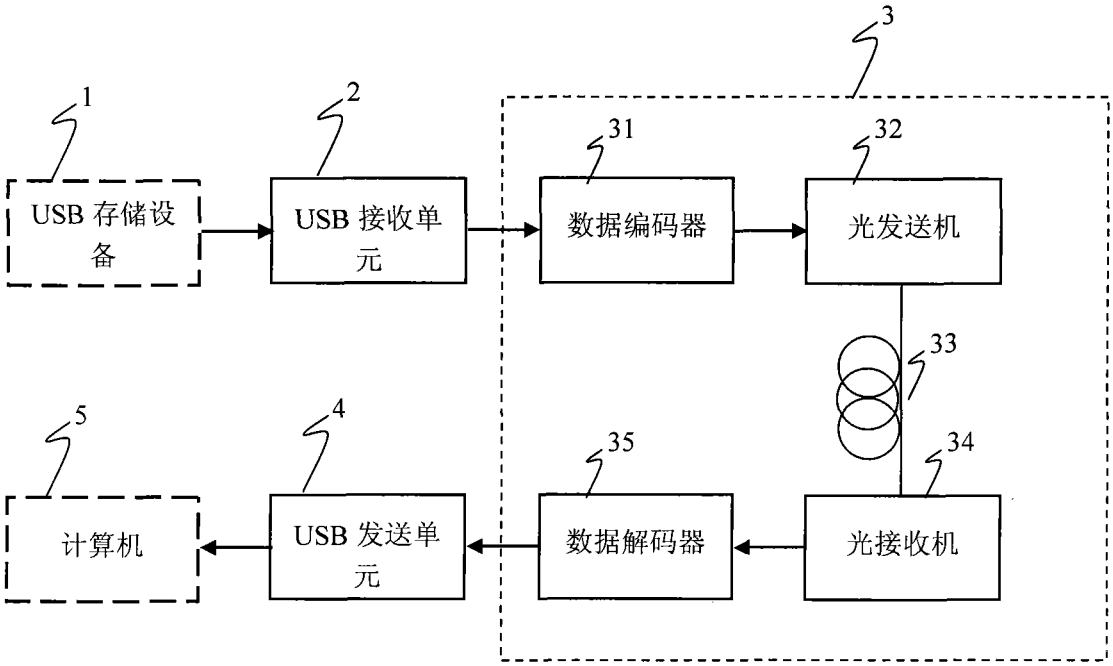

1
2
3
31
32
33
34
35
4
5
USB 存储设备
USB 接收单元
数据编码器
光发送机
光接收机
数据解码器
USB 发送单元
计算机

图 2

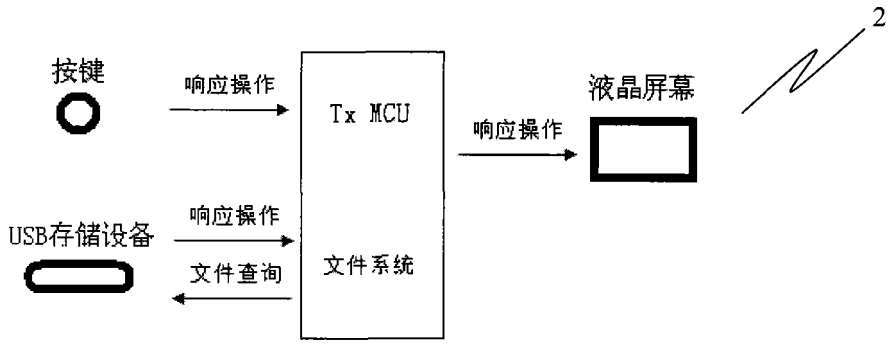

2
按键
响应操作
Tx MCU
液晶屏幕
响应操作
USB存储设备
响应操作
文件查询
文件系统

图 3

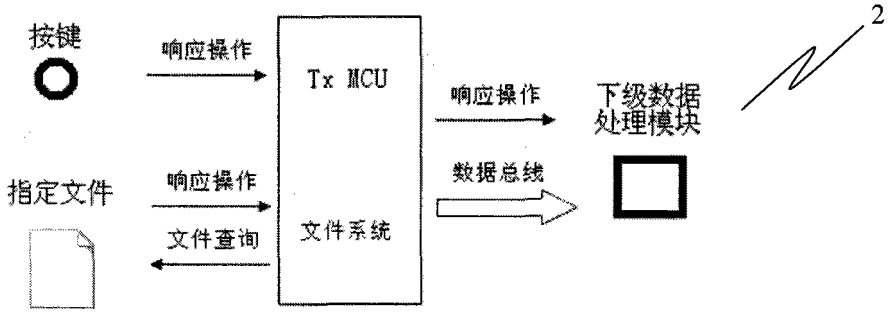

2
按键
响应操作
Tx MCU
响应操作
下级数据处理模块
数据总线
指定文件
响应操作
文件查询
文件系统

图 4