

Data storage device using two types of storage medium

Summary of the invention

- 5 The present invention relates to a data storage device which makes use of two data storage media of different types.

Background of the invention

- 10 Great developments have been underway in recent years in the field of data storage devices. The seminal patent application PCT/SG00/00029 introduced the concept of a data storage device which includes a housing having an integral USB plug and within the housing a non-volatile solid state (i.e. integrated circuit-type) memory device, such as a flash memory. The first such
15 devices, launched in late February 2000 had a capacity of 8MB, and much higher capacities are available now.

- In parallel to this, there has been rapid improvement in hard disk technology, and portable data storage devices of at least several GB are now available,
20 having a size comparable to the solid-state portable data storage devices discussed above.

Summary of the invention

The present invention aims to provide a new and useful data storage device, and algorithms performed by such a device.

5

In general terms, the present invention proposes that a data storage device includes two data storage media: both a hard disk and a non-volatile solid state memory device. Data received by the data storage device for storage is stored both in the hard disk and the non-volatile solid state memory device. Since the
10 data storage is duplicated, if a problem arises with retrieving data from one of the storage media, the data can be retrieved from the other.

Note that hard disks and non-volatile solid state memory devices are vulnerable to different sorts of environmental damage. Thus, data storage device according
15 to the invention is less vulnerable than to damage than a data storage device using only a single data storage medium. This is because in the data storage device proposed by the invention the data has a greater likelihood of survival in at least one of the two data storage media.

20 The data storage device is for connection to a host which controls it using read and write commands, for example according to first driver stored and run in the host. The write and read commands the host generates and transmits to the data storage device may be in a conventional format. In this case, the host does not have to "know" that the data it sends for storage is stored in duplicate

storage media. In response to a write command, the data storage device writes the data to both the data storage media. In the case of a standard read command, the data storage device retrieves the data from one of the hard disk, and sends it to the host.

5

However, in the case that there is a need to retrieve the data from the flash memory, the data storage device can be used in combination with second driver software (e.g. running on a different host to which the portable storage device is connected at that time) to retrieve the data from the flash memory. This second driver software may be arranged to generate read commands in a special format which instruct a read operation from the flash memory, instead of the hard disk.

10

15

The data storage device may be arranged only to implement the special read commands provided that a security procedure is complied with. For example, a password verification operation may be required.

Brief description of the drawings

20

An embodiment of the invention will now be described for the sake of example only with reference to the following figures in which:

Fig. 1 is a schematic block diagram of the embodiment of the invention;

Fig. 2, which is composed of Figs. 2(a), 2(b) and 2(c), is a flow diagram of the data storage and retrieval process carried out by the embodiment of Fig. 1.

5 Detailed description of the drawings

Referring to Fig. 1, an embodiment of the present invention is a data storage device shown having a housing 1, and a USB interface 3 (such as a USB plug but possibly including a USB interface integrated circuit) fixed to the housing 1.

10 The USB interface 3 is for connection to a host (such as a PC), e.g. by plugging the USB plug into a socket of the host. The USB interface 3 is in communication with a controller 5. The controller 5 itself is communication with a flash memory 7 and a hard disk 8. The housing 1 is preferably small enough for the data storage device to be easily portable, such as in a user's pocket. The housing
15 may indeed be small enough to be hidden within the closed fist of a user.

The hard disk 8 is a "removable hard disk drive", in the sense of being in the class of hard disk drivers which are external to the host system. Additionally, the hard disk 8 of the embodiment is optionally removable from the housing 1. This
20 permits the hard disk 8 to be replaced if it is full. Indeed, the hard disk 8 may be one of a plurality of different hard disks which can be inserted into the housing when required. The hard disk 8 is generally present during initialization of the data storage device.

The communication path 9 between the controller 5 and the flash memory 7 and the hard disk 8 includes both one or more data buses and control lines.

Between the controller 5 and the hard disk 8 is an interface which may be an SDIO (secure digital input/output) interface which supports a 4-bit data bus, but
5 in alternative embodiments the interface may be any other media interface, such as an IDE (integrated drive electronics) interface.

The embodiment is used in conjunction with first driver software running on a host which generates read and write commands. This first driver software may
10 take a conventional form. As described below, the data storage device reacts to write commands by writing data sent from the host to both the flash memory 7 and the hard disk 8. The data storage device reacts to a read command by reading data from the hard disk 8 and transmitting to the host. Thus, as far as conventional driver software is concerned, the embodiment functions identically
15 to a known data storage device.

However, the data storage device of the invention may also be operated by a second set of driver software to access the data which is in the flash memory 7. The second driver software has capacity to generate a read command which is
20 in a different format from the read command generated by the first driver software, and which the controller 5 recognizes as a command to read data out of the flash memory 7, and to transmit that data out the data storage device. The controller 5 then performs this operation. The second driver software may optionally be provided on the same host as the first driver software, or

alternatively be on a different host to which the embodiment is connected at that time. The second driver software makes it possible to extract stored data even if the hard disk drive 8 is damaged. Thus, if the data storage device is placed in an environment in which the hard disk 8 is damaged, the data it stores may be
5 retrieved from the flash memory 7 if the flash memory 7 is undamaged.

Of course, if the hard disk 8 is removable, then while it is removed, the data in the flash memory 7 may change (e.g. be overwritten) without corresponding changes being made to the data stored on the hard disk 8. Similarly, if the hard
10 disk 8 is replaced with a new blank hard disk, then clearly the new hard disk does not store data duplicating what is already stored in the flash memory 7. In either case, however, these situations arise because of a user's action, and so the user will be aware that the data stored in the flash memory does not duplicate the data on the hard disk 8. Accordingly, in either case, the user will
15 know not to rely on the backup provided by the flash disk 7.

We now turn to a discussion of the algorithm performed by the data storage device, with reference to Fig. 2. The initial section of the algorithm is shown in Fig. 2(a). When the device is powered up an initialization process is performed
20 in which the device initializes the hard disk 7 (step 1), and the flash device (step 2).

When the device receives a command, in step 3 it then determines whether the command is a write command, a command to read data from the flash 7, or a

command to read data from the hard disk 8. The default for the read operation is that the data will be read from the hard disk 8, so a read command which arrives without containing a marker indicating that it refers to the flash 7, is treated as a read command in respect of the hard disk 8.

5

If step 3 determines that the received command is a command to read data from the hard disk 8, in step 4 is calculates the physical address in the hard disk 8 corresponding to the logical block address (LBA) contained in the read command. In step 5 the controller 5 uses the control lines and the data bus 9 to
 10 send a command to the hard disk 8 to transmit to the controller the data at that physical address, and then the controller 5 transfers data received from the hard disk 8 over the data bus to the external host through the USB interface 3. In step 6 it tests whether this process is complete. If not, it continues the transfer process in step 7, and loops back to step 6. When the determination in
 15 step 6 is positive, the method passes to step 8 in which it waits for a new command. When that new command it received, the method passes again to step 3.

If step 3 determines that the received command is a command to write data, the
 20 method passes to the portion of the algorithm shown in Fig. 2(b). In step 9 the data in the command is stored in a register, to be written subsequently to the memories 7, 8. The command portion of the write command (i.e. the write command minus the data to be written) is stored separately, for subsequent use in determining where the data should be written.

In step 10, the physical address in the flash memory 7 corresponding to a logical address in the write command is calculated. In step 11, the physical address in the hard disk 8 corresponding to the same logical address is
5 calculated. In step 12, the controller 5 sends a command using the control lines to both the flash memory 7 and the hard disk 8 instructing it to store data. Then controller 5 in step 13 writes 512 bytes of the data received from the host to both the flash memory 7 and the hard disk 8. In step 14, the controller 5 test whether it has now sent all the data specified by the write command to the
10 memory devices 7, 8. If not, in step 15 the data writing process continues, and the method loops back to step 14. As soon as the determination in step 14 is positive, the writing process is complete, the method passes back to the section of the flow diagram shown in Fig. 2(a).

15 If step 3 determines that the received command is a command to read data from the flash memory 7 (i.e. a command generated by the second driver software), then it passes to the section of the algorithm shown in Fig. 2(c). In a verification step 16 the controller 9 determines whether the read command included certain security information, such as a password. If not, the read
20 operation fails, and the method passes back to Fig. 2(a). Optionally, the password may be stored in a reserved area of the flash memory 7 itself. Alternatively, the password may be stored in the host.

If the verification step 16 is positive, then in step 17 the controller 5 calculates the physical address in the flash memory. In step 18 the controller 5 uses the control lines and data bus 9 to control the flash memory to transmit the data at that physical address to the controller 5 using the data bus, and then the
5 controller 5 transmits the data to the host out through the USB interface 3. In step 19, the controller 5 determines whether all the requested data has been sent. If so, the read operation terminates, and the method loops back to the section of the algorithm shown in Fig. 2(a). Otherwise, the data transfer procedure continues (step 20), looping back to step 19.

10

Although only a single embodiment of the invention has been described in detail, many variations are possible within the scope of the invention as will be clear to a skilled reader.

Claims

1. A data storage device comprising:
 - (i) an interface for communicating with a host,
 - (ii) a hard disk,
 - 5 (iii) a non-volatile solid state memory device, and
 - (iv) a controller in communication with the interface, with the hard disk and with the non-volatile solid state memory device, the controller being arranged:
 - (i) upon receiving a write command from the host,
10 to send a command to both the hard disk and the non-volatile solid state memory device, the command instructing both the hard disk and the non-volatile solid state memory device to store data, and
to write the data associated with the write command into both the hard disk and the non-volatile solid state memory device,
 - 15 (ii) upon receiving a read command, to obtain the data selectively from the hard disk or the non-volatile solid state memory, and to transmit the data out of the data storage device through the interface.
2. A data storage device according to any preceding claim in which the
20 controller is arranged, upon receiving a read command, to determine from the read command whether the read command relates to the hard disk or the non-volatile storage device.
3. A data storage device according to claim 2 in which, upon determining
25 that the read command relates to the non-volatile storage device, the controller is arranged to initiate a security procedure in which the controller verifies whether security information received from the interface is in accordance with pre-stored security information.
- 30 4. A data storage device according to claim 1, claim 2 or claim 3 in which the hard disk is removable from the data storage device.

5. A method of retrieving data from a data storage device according to any preceding claim, the method including establishing electronic communication between the data storage device and a host, and the host transmitting commands to the data storage device to cause the host to obtain data from the non-volatile solid state memory, and to transmit the data to the host through the interface.
6. A method according to claim 5 further including a step of the host performing a security procedure in relation to the data storage device prior to the data storage device transmitting the data to the host.
7. A method according to claim 6 in which the security procedure employs a password.