

VIRTUAL WRITE PROTECTION SYSTEM

[0001] BACKGROUND

[0002] Technical Field: The invention relates generally to optical media used for information storage, and drives for recording optical media used for information storage.

[0003] Digital optical media are used for a variety of purposes and a variety of information, for example, entertainment data, such as audio and video, and computer data, such as text files and numerical data files. In many instances it is desirable to protect the recorded data from intentional or accidental overwriting. For preventing this, optical media typically includes a bit to indicate the media is write protected or in the case where the disc is in a cartridge or media carrier with a tab or other mechanical switch in the cartridge or carrier. In the case of a write protect bit on the media, the state of the bit must be changed before writing can occur. Unfortunately, some optical media allows only a limited number of overwrites or in the case of write-once media no overwrite. In the case of rewritable media with a limited number of overwrites, the information recorded in an area with too many overwrites becomes unreliable, while write-once media requires reserving a large area to accommodate the likely number of changes to the write protect bit. There is an ongoing need for a write protection system that takes into account the limitations of some media that allow limited or no overwrites.

[0004] BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figure 1 illustrates an example system in which the invention may be implemented.

[0006] Figure 2A illustrates an example system containing multiple pieces of write protection information contained within a single data structure including one piece of information to indicate an allowed virtual status, a different piece of information to indicate an write protect ON/OFF, information to indicate the presence of a password and a password recorded on a disc in the system of figure 1.

[0007] Figure 2B illustrates an example system containing multiple pieces of write protection information contained in multiple data structures including one piece of information to indicate an allowed virtual status, a different piece of information to indicate an write protect ON/OFF, information to indicate the presence of a password and a password recorded on a disc in the system of figure 1.

[0008] Figure 3A is a flow chart of an example embodiment of a method for using the write protect system of figure 2A in which there is only the write protect On/Off information.

[0009] Figure 3B is a flow chart of an example embodiment of a method for using the write protect system of figure 2A in which there is write protect On/Off information and includes password control.

[0010] Figure 4A is a flow chart of a second example embodiment of a method for using the write protect system of figure 2A or 2B without the Virtual On/Off.

[0011] Figure 4B is a flow chart of an example embodiment of a method for using the complete write protect system of figure 2A or 2B.

[0012] DESCRIPTION

[0013] For some digital optical media for information storage, for example some Compact Discs (CD's), Digital Versatile Discs (DVD's), and blue laser formats (HD-DVD's and Blu-ray), each data surface has a land and groove structure, with lands and/or grooves. User information (for example, audio data, video data, or computer data) may be recorded in the grooves, on the lands, or both. The disc may be divided into regions used to record user data and a different region used to record other non-user forms of data including control or format data, etc.. Either form of data is usually recorded according to

its smallest recordable unit that includes both the normal data plus error correction information, addressing information, etc, typically referred to as an ECC block, for example DVD's have the smallest recording unit as 37,856 bytes of which 32,768 bytes are the normal or user data portions of the ECC block. Because the minimum recording unit is so large, it typically includes additional and often critical information beyond the information used to indicate write protection on the disc. Rewriting a particular ECC block an excessive number of times will cause the ECC block to eventually become difficult to read causing critical information to be lost.

[0014] In example embodiments of the invention, all of the write protection information may not need to be changed before allowing recording to the other areas of the disc. This is allowed after confirmation of the user at some point in time essentially making the write protection a virtual feature that does not require changing the actual bits on the disc. Having a virtual bit means you do not have to change the physical write protect bit of the disc before writing to the disc. Without the virtual bit, you must change the physical write protect bit. In a first example, the write protection system uses a single item of information to indicate the write protection status such that the single item of information has an inherent virtual nature. In a second example, there is additional information to indicate that the write protection information is virtual or not. In a third example, a password function is included to control changing of information.

[0015] Figure 1 illustrates an example embodiment of a system including a drive 100, an optical disc 102, and an user input device 106. An optical head 104 reads and write data on the disc 102 through a lens system 106. A controller 108 transforms signals from the optical head 104 into digital information. The digital information includes user data and non-user data. The controller 108 is in communication with a host device 110. The drive 100 may be part of the host 110, or optionally the drive may be a peripheral device connected to the host by a cable as illustrated, or optionally the drive may be a peripheral device and communicate with the host wirelessly. The host 110 including a drive 100 may be a computer or other devices including optical disc recorders that record video programming. The user input device 106 may be a keyboard or remote control device.

[0016] Figure 2A illustrates a data structure 200 containing write protection information on the disc 102. In the example of figure 2A, the write protection information consists of a write protection On/Off information 210, a password On/Off information

220, a password 224 and a virtual On/Off information 230. In various embodiments, some of these elements may not be present. For example, the system may not use a password thereby omitting the password On/Off information 220 and a password 224. Or the write protection On/Off 210 may always be considered virtual and does not need to be physically changed on the media prior to recording on the disc. In this case, there is no need for virtual On/Off information 230. When the user attempts to write to the disc or at some point after inserting the disc into the drive or device, the system must request confirmation and only after receiving the confirmation may the disc be recorded. The confirmation may occur immediately before attempting to write or at time or some earlier time, such as when the system has successfully determined the state of the write protection indicator 210.

[0017] Further, the user may set the drive, software or device to not request the confirmation for this disc or any disc. This can be accomplished by saving a setting on the optical disc 102 or in the drive, software

[0018] Figure 2B illustrates a variation of figure 2A, except that the write protection On/Off information 210 is contained in a separate data structure 250.. Other embodiments may have different information recorded in one or more separate data structures 250.

[0019] Figure 3A is a flow chart of an example embodiment of a method for using the write protect system of figure 2A in which there is only the write protect On/Off information for a representative situation when the system receives a request to write to the media from an end-user.. Block 300 starts with loading media into the present system. The media could be any such digital optical media such as CD's, DVD's, one of the blue-laser formats (HD-DVD and Blu-ray), or other similar optical media. Block 310 collects the read/write protect indicator that is stored on the media loaded in block 300. Decisional block 320 determines whether the WrtProt bit is set. If YES, control is passed to block 330 to allow the system to receive user input to permit writing before passing control to block 320. If the WrtProt bit is set, the decisional block 320 passes control to block 340 to perform write media.

[0020] Figure 3B illustrates a flow chart of an example embodiment of a method for using the write protect system of figure 2A in which there is write protect On/Off information and includes password control. Block 300 starts with loading media into the present system. Block 310 collects the read/write protect indicator that is stored on the

media loaded in block 300. Decisional block 320 determines whether the WrtProt bit is set. If no, control is passed to block 350, which requires the additional step of accepting a password from the user before writing to the disc is permitted. Decisional block determines whether the password entered by the user is correct. If the password is correct, control is passed to block 340 to perform write media. If the password entered is incorrect, the user is notified (block 370) before control is passed to block 340. If the WrtProt bit is set, decisional block 320 passes control to block 340 to perform write media.

[0021] Figure 4A illustrates a flow chart of a second example embodiment of a method for using the write protect system of figure 2A or 2B without the Virtual On/Off. Block 300 starts with loading media into the present system. Block 310 collects the read/write protect indicator that is stored on the media loaded in block 300. Decisional block 320 determines whether the WrtProt bit is set. If no, control is passed to decisional block 400 to determine whether the Virtual Write Protect bit is set. If no, control is passed to block 420 to allow the system to receive user input to permit writing before control is passed to block 340. If the Virtual Write Protect bit is set, the control is passed to block 410 to turn off the WrtProt bit. If the WrtProt bit is set, decisional block 320 passes control to block 340 to perform write media.

[0022] Figure 4B illustrates a flow chart of an example embodiment of a robust method for using the complete write protect system of figure 2A or 2B. Block 300 starts with loading media into the present system. Block 310 collects the read/write protect indicator that is stored on the media loaded in block 300. Decisional block 320 determines whether the WrtProt bit is set. If no, control is passed to block 350, which requires the additional step of accepting a password from the user before writing to the disc is permitted. Decisional block determines whether the password entered by the user is correct. If the password entered is incorrect, the user is notified (block 370) before control is passed to block 340. If the password is correct, control is passed to decisional block 400 to determine whether the Virtual Write Protect bit is set. If no, control is passed to block 420 to allow the system to receive user input to permit writing before control is passed to block 340. If the Virtual Write Protect bit is set, the control is passed to block 410 to turn off the WrtProt bit. If the WrtProt bit is set, decisional block 320 passes control to block 340 to perform write media.

[0023] While the present invention has been illustrated and described in connection with the preferred embodiments, it is not to be limited to the particular structures shown. It should be understood by those skilled in the art that various changes and modifications may be made within the purview of the appended claims without departing from the true scope and spirit of the invention in its broader aspects.

CLAIMS

What is claimed is:

1. A drive for optical media, comprising:
 - a controller, the controller receiving write protection information from recorded media and receiving user approval to record on the media to allow recording on the media without modifying the write protection on the disc.
2. The system of claim 1 where the user approval may be set as a default for future optical media.
3. The system of claim 1 where data password function is included.
4. An optical medium, comprising:
 - write protection information for the media;
 - information specifying whether a drive writing the optical medium is permitted to write without first turning off said write protection information.
5. A method of recording on media without modifying write protection on a disc comprising:
 - collecting a write protection indicator from a medium that is loaded onto a drive;
 - determining a value of the write protection indicator on the medium;
 - determining whether a user password is required by the drive;
 - collecting a virtual protection indicator from the medium;
 - determining a value of the virtual write protect indicator on the medium; and
 - performing a predetermined function based any one of the values determined.