

METHOD AND SYSTEM FOR SECURING OPTICALLY DISCERNABLE DATA
ON A DATA STORAGE DEVICE

Background of the Present Invention

Field of the Present Invention

The present invention relates in general to a method and system for data security and more particularly, to an improved method and system for securing access to optically discernable data on a data storage device. Still more particularly, the present invention provides a method and system for storing data of two different security levels on a single data storage device.

Description of the Related Art

With the proliferation of the compact disc, a meaningful way has been established for wide distribution of large amounts of data in both computer and consumer industries. Of the types of compact discs (CDs) that are currently available, three include Audio CD (CD-DA), Data CD (CD-ROM) and Video CD (DVD). On a CD-ROM, large amounts of data may represent application programs, operating systems, and general information typically utilized by a computer. The CD-DA and DVD typically contain audio visual information designed for presentation by consumer devices such as compact disc players and DVD players for utilization with a stereo and/or video display. CD-ROM drives and DVD drives may also be included within a computer.

Secure distribution of data on a compact disc and



166166



G00002

other optical storage media is a problem identified within the industry, especially with the growth of the writable compact disc drive which allows computer owners to copy data onto a compact disc. The owners of the copyright of content being distributed by compact disc have sought solutions to protect their intellectual property rights and prevent unauthorized use or copying of proprietary data originally stored on a compact disc. One measure which manufacturers have taken to protect CD-ROM data is the use of a "software key" which must be entered for the user to access the data stored on the CD-ROM. The software key is typically a multi-digit number included with the CD-ROM documentation or written directly on the CD-ROM cover. The use of such software keys does not restrict the number of copies of data on a compact disc which may be made and does not restrict the purchaser of a compact disc from allowing others to make copies of the data.

In the case of DVD, as DVD content owners release DVD titles world-wide, it is often necessary to control the time of distribution in different geographical regions. Controlling geographical timing today is accomplished by specially encoding each DVD with a special region bit that, when detected, allows the DVD to be played on a corresponding DVD player which is distributed in that particular region. However, this methodology may be easily circumvented by obtaining a DVD player for the particular region in which the special region bit is programmed.

It is therefore desirable, for the reasons

26 JUL 2002

-3-

illustrated above and many others, that a method of securing data on all types of compact discs be implemented such that the compact disc content owners may control the use of data stored on the compact disc.

Summary of the Present Invention

It is therefore one object of the present invention to provide a method and system for data security.

It is another object of the present invention to provide improved system and method for securing access to optically discernable data on a data storage device.

It is yet another object of the present invention to provide system and method for storing data of two distinct security classifications on a single data storage device.

The foregoing objects are achieved as is now described. A method and system for securing access to optically discernable data embedded within a data storage device is provided. To secure access, it is first determined if there is registration data stored on an electronic storage device affixed to a data storage device, in response to insertion of the data storage device into a reader. The registration data is thereafter compared with user identification data. The optically discernable data embedded within the data storage device is then read in response to the registration data matching the user identification data, such that access to optically discernable data on a data storage device is only permitted by proper identification.

A data storage device is provided which includes a substrate, optically discernable data, and an electronic

26 JUL 2002

-5-

storage device. The optical discernable data is embedded within the substrate and adapted to be read when the substrate is manipulated by an optical reader. The electronic storage device is mounted to the substrate and utilized to store electronically alterable data, such that data of two distinct security classifications may be stored on the same data storage device.

Brief Description of the Drawings

The novel features believed characteristic of the present invention are set forth in the appended claims. The present invention itself, however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts an illustrative diagram of a representative hardware environment according to the method and system of the present invention;

Figure 2 illustrates a functional block diagram of a representative hardware environment according to the method and system of the present invention;

Figure 3 depicts a high level illustrative block diagram of a "smart card" according to the method and system of the present invention;

Figure 4 illustrates a high level illustrative block diagram of a smart compact disc according to the method and system of the present invention;

Figure 5 depicts a high level logic flowchart of the method of installing registration data on a smart CD-ROM for permitting installation of software from the smart CD-ROM according to the method and system of the present invention;

26 JUL 2002

Figure 6 illustrates a high level logic flowchart of the method of uninstalling ownership of a smart compact disc according to the method and system of the present invention;

Figure 7 depicts a high level logic flowchart of the method of installing registration data on an smart audio compact disc for access to audio data on the smart audio compact disc according to the method and system of the present invention;

Figure 8 illustrates a high level logic flowchart of the method of installing registration data on a smart DVD disc according to a geographic location according to the method and system of the present invention; and

Figure 9 depicts a high level logic flowchart of the method of uninstalling of ownership of a smart DVD disc according to the method and system of the present invention.

Description of the Preferred Embodiment

With reference now to the figures and in particular with reference to **Figure 1**, there is illustrated a diagram of a representative hardware environment of a data processing system 10 which utilizes an operating system installed therein. Data processing system 10 comprises processor unit 12, keyboard 14, mouse 16, and video display (or monitor) 18. Keyboard 14 and mouse 16 constitute user input devices, and video display 18 constitutes an user output device. Mouse 16 is utilized to control cursor 20 displayed on screen 22 of video display 18. Data processing system 10 supports a Graphical User Interface (GUI) which allows a user to "point-and-click" by moving cursor 20 to an icon or specific location on screen 22 via mouse 16 and then depressing one of the buttons on mouse 16 in order to perform a user command. Floppy disk drive 24, smart compact disk drive 26, and smart card reader 47 provide access for processor unit 12 to external data storage devices.

With reference now to **Figure 2**, there is depicted a functional block diagram of data processing system 10 illustrated in **Figure 1**. Processor unit 12 includes a system bus 28 to which various functional blocks are attached and by which communications among various functional blocks are accomplished. Microprocessor 30, connecting to system bus 28, is supported by read only memory (ROM) 32 and random access memory (RAM) 34, both of which are connected to system bus 28.

ROM 32 contains, among other code, the Basic Input/Output System (BIOS) or other firmware, which controls certain basic hardware operations, such as interactions of hard disk drive 36 and floppy disk drive 24. RAM 34 is the main memory within which the operating system having the present invention incorporated and other application programs operate within. A memory management device 38 is connected to system bus 28 for controlling all Direct Memory Access (DMA) operations such as paging data between RAM 34 and hard disk drive 36, floppy disk drive 24, or smart compact disc drive 26. An application program which directs the implementation of the present invention may be provided to data processing system 10 for storage in a storage medium such as hard disk drive 36 via a variety of signal-bearing media which include, but are not limited to writeable storage media such as a floppy disk 40 which may be readable by floppy disk drive 24 for storage into the storage medium of data processing system 10. Application programs can be written in a variety of programming languages supported by the operating system, including but not limited to C++.

Referring still to **Figure 2**, an I/O adapter 42 is illustrated connected to system bus 28 for providing an interface for data storage peripheral devices such as data storage system 44. Additional I/O adapters may be included to expand the storage capacity accessible by data processing system 10.

The term "smart card" will be periodically utilized in the following description as is well known in the art.

In addition, the term "smart chip" and "smart card accepting device" are also utilized. A smart card generically refers to a card formed of a plastic body with a micromodule embedded in a special cavity. A smart chip generically refers to the micromodule embedded in the smart card, typically an electronic storage device which contains electronically alterable data. A smart card accepting device reads data from and writes data to the smart chip within the smart card.

A smart card accepting device 47 is depicted including a smart card 70 inserted therein which enables microprocessor 30 to communicate therewith. Smart card accepting device 47 may also be incorporated with modem 50 or other PCIMCI slots, as is well known in the art. In addition, a smart chip, may be embedded in the hardware of processor unit 12 in addition to or in place of smart card accepting device 47. Furthermore, similar accepting devices as smart card accepting device 47 may also accept secure cards or PCIMCA cards which are also known, like smart card 70, to be equipped with security features to prevent access to and tampering with data in the memory of the card.

New to the art, smart compact disc drive 26 is illustrated including a data storage device such as a smart compact disc 46, inserted therein. Compact disc drives and other optical storage medium readers for accessing data on CD-ROM, CD-AD and DVD are well known in the art, however the smart compact disc drive 26 also includes a smart chip reader/writer 27 which reads data from and writes data to an electronic storage device or

26 JUL 2002

-11-

smart chip mounted on smart compact disc 46 in the same manner as a smart card accepting device. Smart chip reader/writer 27 may electronically alter data stored within the electronic storage device.

A biometric device 52 may be utilized to provide user identification data in such forms as an eye scan, voice recognition or fingerprint detection. Such user identification data may be stored in one of the data storage devices of processor unit 12, including hard disk drive 36 and smart card 70. User identification may be utilized as a password for access to data processing system 10.

Other peripheral devices such as optical storage media, printers, etc. may also be added to data processing system 10. In addition, other readers of storage media such as game cartridge readers or other electronic media readers may be incorporated herewith. Further, a communications adapter 48 may be utilized to communicate with other data processing systems (not shown). Communications adapter 48 may support modem 50 or a network link (not shown), such as an ethernet link, which allows data processing system 10 to communicate with other data processing systems. Modem 50 allows data processing system 10 to communicate with other data processing systems over the Internet through data transfer lines including but not limited to public switched telephone network (PSTN) or ISDN lines. In addition to modem 50, communications adapter 48 may support other communication devices such as a network link connected to a local area network (LAN).

To complete the description of processor unit 12, there are three input/output (I/O) controllers, namely, keyboard controller 54, mouse controller 56 and video controller 58, all of which are connected to system bus 28. As their names imply, keyboard controller 54 provides the hardware interface for keyboard 14, mouse controller 56 provides the hardware interface for mouse 16, and video controller 58 provides the hardware interface for video display 18. **Figures 1 and 2** represent a typical general purpose computer, however may also be incorporated within video display systems, audio sound systems and other data processing systems which provide for accessing data stored on a data storage device containing optically discernable data, particularly a compact disc.

With reference now to **Figure 3**, there is illustrated a high level illustrative diagram of a smart card which may be utilized with the method and system of the present invention. Smart card 70 includes a credit card size plastic encasing as depicted at reference numeral 71 with a standard smart chip 72 embedded within in such a manner for smart chip 72 contacts to be exposed. Smart chip 72 is preferably a static electronic storage device, including an integrated circuit or microprocessor with associated memory and memory control logic. An operating system is embedded within smart chip 72. Upon application of power, smart chip 72 is initialized and begins operating.

The size of smart card 70 is determined by an

international standard (ISO 7816). A direction indicator is typically designated on the exterior of smart card 70, such as direction indicator 75, in order that the user may insert smart card 70 into a smart card reader in the proper direction. The ISO 7816 standard also defines the physical characteristics of the plastic including the temperature range and flexibility, position of the electrical contacts and how smart chip 72 communicates with a smart card reader. Smart chip 72 is approximately 13mm by 12mm with a thickness less than .5mm.

Smart cards are becoming an international standard as a portable data storage and retrieval device for applications such as user identification data, an electronic purse and credit card. A smart card can typically be designed for three levels of security including anyone holding the smart card, the smart card holder only, and a third party only. A smart card which does not require a password may be utilized by anyone holding the smart card. For example, a medical smart card with a patient's name and blood type may be accessible without a password. A card holder smart card may only be utilized if a user identification number or other password data is correctly entered. For example, user verification data for an eye scan may be included in a smart card where the eye scan must match the user verification data on the card for access to data stored within the smart card. Finally, a third party may issue a smart card on which the data may only be accessed by the third party. For example, if a smart card contains an electronic purse, only the issuing bank may reload the purse. Such a smart card may also include a password

verification scheme for only allowing the smart card holder to make purchases with the electronic purse.

A smart card may be designed to include information which is read only, added only, updated only, or with no access available. Multiple types of memory may be included in order to facilitate the types of information included on a smart card. For example, four types of memory in addition to read-only access memory (ROM) which may be included on smart card are programmable: read only memory (PROM), erasable programmable ROM (EPROM), electrically erasable PROM (EEPROM), and random access memory (RAM).

With reference still to **Figure 3**, preferably, smart chip 72 is provided with eight contact points for input/output of signals and voltage. A Vcc signal is illustrated at reference numeral 74 where Vcc is the supply voltage applied to smart chip 72 to drive smart chip 72 and is typically 5 volts. A GND signal is depicted at reference numeral 80 which provides a ground reference against which the Vcc voltage potential is measured. A RST signal is depicted at reference numeral 76 where RST is the signal line that is utilized to initiate the state of the microprocessor after power is applied. Next, a CLK signal is illustrated at reference numeral 78 where the CLK signal is utilized to drive the logic of smart chip 72. A Vpp signal is depicted at reference numeral 82 where Vpp is the high voltage supply signal supplied to smart chip 72 that is necessary to program the EPROM memory and other events requiring a voltage supply greater than Vcc. Next, an I/O connector

is illustrated at reference numeral 84 which is a serial input/output connector by which smart chip 72 receives and outputs data and commands. The two signal pads 86 and 88 are undefined at present.

Referring now to **Figure 4**, there is depicted a pictorial illustration of smart compact disc 46 according to the method and system of the present invention. Smart compact disc 46 is a standard compact disc in size and function as is well known in the art. Smart compact disc 46 includes a substrate with an optically discernable data storage area 60 and a non-optical area 62. Optically discernable data storage area 60 is preferably embedded with optically discernable data. Smart compact disc 46 also includes at least one smart chip 72 or other electronic storage device. Optically discernable data storage area 60 and smart chip 72 may contain data of two distinctly different security classifications. Also, in the embodiment illustrated, two smart chips 72 and 73 are included where each smart chip is positioned in order to balance the weight of the other smart chip such that smart compact disc 46 may spin properly. However, in other embodiments, an alternate device to smart chip 73 may be positioned across from smart chip 72 in order to balance the weight of smart chip 72.

With reference now to **Figures 5-9**, there are depicted high level logic flowcharts which illustrate the method of the present invention. It should be appreciated by those skilled in the art that **Figures 5-9** represent a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical

manipulation of physical quantities. Usually, although not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared and otherwise manipulated. It has proven convenient at times by those skilled in the art to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be born in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

Further, the manipulations performed are often referred to as terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary or desirable in most cases in any of the operations described herein which form part of the present invention; the operations are machine operations. Useful machines for performing operations of a preferred embodiment of the present invention include data processing systems such as general purpose digital computers, video display systems, audio sound systems or other similar devices. In all cases the distinction between the method operations and operating a computer and the method of computation itself should be born in mind. The present invention relates to method steps for operating a processor unit such as processor unit 12 of **Figure 2**, in processing electrical or other physical signals to generate desired physical signals.

With reference now to **Figure 5**, there is illustrated

a high level logic flowchart of the installation of registration data on a smart chip mounted to a smart compact disc, particularly a smart CD-ROM, if not previously registered. In addition, in the process, an owner may be permitted to install software stored on the smart CD-ROM. As illustrated, the process described in **Figure 5** begins at block 90 and thereafter passes to block 92. A plurality of triggers in the operation of microprocessor 30 may trigger the process which begins at block 90. For example, upon detecting a smart compact disc, the process may be triggered.

Block 92 illustrates the reading of user identification data from a smart card. The user identification data may include the smart card holder's name, address, phone number along with other user data which can be stored on a smart compact disc to identify ownership. In the present process and in those following, a smart chip containing user identification data may also be embedded in the data processing system wherefrom user identification data may be read. In addition, another method of gathering user identification data for storage on a smart chip mounted to a compact disc, is through any user identification data collected by the data processing system during installation of the operating system for the data processing system. If required, as is typical with a smart card, user identification data may be accessed by password or by data gathered from a biometric device, such as biometric device 52.

After block 92, the process passes to block 94.

Block 94 depicts the reading of any registration data from the smart chip mounted to the smart compact disc. Thereafter, the process passes to block 96. Block 96 illustrates the determination of whether or not registration data has been previously installed on the smart chip mounted to the smart compact disc. If registration data for the smart chip needs to be installed, the process passes to block 98. Otherwise, the process passes to block 106 if the registration data for the smart chip has been previously installed.

Still referring to **Figure 5**, block 98 depicts the copying of user identification data to the smart chip for storage as registration data. User identification data is transferred to the smart chip mounted to the smart compact disc and stored in memory associated with the smart chip. Thereafter, the process passes from block 98 to block 100. Block 100 illustrates the decrementing of the install counter by one. The install counter is stored within memory associated with the smart chip which is not accessible by the user. The install counter contains a preset number of copies of software stored on the smart compact disc which may be made by a user. After block 100, the process passes to block 102. Block 102 depicts the installation of software programs from the smart compact disc to a data storage device as will be understood by one well known in the art. The software is unlocked for access once the smart compact disc has been properly registered. Thereafter, the process returns.

With reference still to **Figure 5**, block 106

26 JUL 2002

-19-

illustrates the comparison of user identification data from the smart card with registration data from the smart chip mounted to the smart compact disc. Thereafter, the process passes from block 106 to block 108. Block 108 depicts the determination of whether or not the user identification data matches the registration data. If it is determined that the user identification data does match the registration data, then the process passes to block 110. If the user identification data does not match the registration data, the process passes to block 112. Block 110 illustrates the determination of whether or not the install counter is equal to zero. If the install counter is equal to zero, then no additional copies of the software may be obtained by the owner to which the smart compact disc is registered and the process passes to block 112. If the install counter is not equal to zero, the process passes to block 100. Block 112 depicts the displaying of an error message if the software cannot be installed because proper identification has not been supplied. Thereafter, the process returns.

Referring now to **Figure 6**, there is illustrated a high level logic flowchart of the method of the uninstallation of the ownership of a smart compact disc, particularly a smart CD-ROM with software embedded therein, according to the method and system of the present invention. As illustrated, the process described in **Figure 6** begins at block 120 and thereafter passes to block 122. A plurality of triggers in the operation of microprocessor 30 may trigger the process which begins at block 120. For example, upon detecting a user request to

uninstall ownership of a smart compact disc, the process may be triggered.

Block 122 illustrates the reading of user identification data from a smart card. After block 122, the process passes to block 124. Block 124 depicts the reading of registration data from a smart chip mounted to a smart compact disc. Thereafter, the process passes from block 124 to block 126. Block 126 illustrates the determination of whether or not registration data has been previously installed on the smart chip mounted to the smart compact disc. If registration data for the smart chip needs to be installed, the process passes to block 128. Block 128 depicts the displaying of an error message since the smart chip does not have a record of any previous software installation. At block 126, if the registration data for the smart chip has been previously installed, the process passes to block 130.

With reference still to **Figure 6**, block 130 illustrates the comparison of user identification data from the smart card with registration data from the smart chip mounted to the smart compact disc. Thereafter, the process passes from block 130 to block 132. Block 132 depicts the determination of whether or not the user identification data matches the registration data. If the data matches, the process passes to block 134. If the data does not match, the process passes to block 140. Block 140 illustrates the displaying of an error messages because proper identification has not been supplied.

Referring still to **Figure 6**, block 134 depicts the

incrementing of the install counter by one. Thereafter, the process passes from block 134 to block 136. Block 136 illustrates the determination of whether or not the install counter has reached its maximum. The maximum number of copies which may be made of data stored on a compact disc is preset by the smart compact disc manufacturer. For each copy, registration data must be stored to properly register the compact disc. If the install counter is determined to have reached a maximum, then the process passes to block 142. Block 142 depicts the erasing of the registration data from the smart chip. Thereafter, the process passes to block 138. Block 138 illustrates the uninstallation of software programs. The uninstall program process is included such that a consumer may sell a smart compact disc containing software to another individual without retaining a copy of the software.

With reference now to **Figure 7**, there is illustrated a high level logic flowchart of a process for the registration of a smart compact disc, particularly an Audio-CD, for access to audio data on the smart compact disc according to the method and system of the present invention. As illustrated, the process described in **Figure 7** starts at block 150 and thereafter passes to block 152. A plurality of triggers in the operation of microprocessor 30 may trigger the process which begins at block 150. For example, upon detecting a smart compact disc, the process may be triggered.

Block 152 illustrates the reading of user identification data from a smart card. As previously

described, user identification data may also be obtained from other sources such as a smart chip embedded in the hardware, or from user identification data collected during the installation of an operating system. After block 152, the process passes to block 154. Block 154 depicts the reading of any registration data from a smart chip mounted to a smart compact disc. Thereafter, the process passes to block 156. Block 156 illustrates the determination of whether or not registration data has been previously installed on the smart chip mounted to the smart compact disc. If registration data for the smart chip needs to be installed, the process passes to block 158. Otherwise, if the registration data for the smart chip has been previously installed, the process passes to block 164.

Referring still to **Figure 7**, block 158 illustrates the copying of user identification data to the smart chip for storage as registration data. Thereafter, the process passes from block 158 to block 162. Block 162 illustrates the playing of the smart compact disc whereafter the process returns.

With reference still to **Figure 7**, block 164 depicts the comparing of user identification data from the smart card with registration data from the smart chip. Thereafter, the process passes from block 164 to block 166. Block 166 illustrates the determination of whether or not the user identification data matches the registration data from the smart chip. If the data matches, then the process passes to block 162. If the data does not match, the process passes to block 168.

Block 168 depicts the displaying of an error message because proper identification has not been supplied.

The process of **Figure 7** not only protects unauthorized duplications of data, but also provides security for deterring smart compact discs from theft. For example, many stores allow customers to listen to the music stored on a compact disc before making a purchase. However, there is risk that the compact disc can be easily stolen since the compact disc casing includes the security protection. However, if in-store copies of a smart compact discs are registered to the store and all machines for playing the smart compact discs are embedded with smart card user identification data, then the smart compact discs may be played in the store, but would be useless if removed.

Referring now to **Figure 8**, there is illustrated a high level logic flowchart of the method for installing ownership registration of a smart compact disc, particularly a smart DVD disc, according to the method and system of the present invention. As illustrated, the process described in **Figure 8** begins at block 180 and thereafter passes to block 182. A plurality of triggers in the operation of microprocessor 30 may trigger the process which begins at block 180. For example, upon detecting a smart compact disc, the process may be triggered.

Block 182 illustrates the reading of user identification data from a smart card. After block 182, the process passes to block 184. Block 184 depicts the

reading of registration data from a smart chip mounted to a smart compact disc. Thereafter, the process passes to block 186. Block 186 illustrates the determination of whether or not registration data has been previously installed on the smart chip affixed to the compact disc. If registration data for the smart chip needs to be installed, the process passes to block 188. If registration has been previously installed, the process passes to block 200.

With reference still to **Figure 8**, block 188 illustrates the comparison of geographic user identification data from the smart card and geographic registration data from the smart chip mounted to the smart compact disc. The smart chip includes a geographic region in which the smart compact disc is intended for use. Thereafter, the process passes from block 188 to block 190. Block 190 depicts the determination of whether or not the geographic data matches. If the geographic data matches, then the process passes to block 192. However, if the geographic data does not match, the process passes to block 204 which depicts the display of an error message if the smart compact disc is outside the geographic area. Block 192 illustrates the copying of user identification data to the smart chip for storage as registration data. Thereafter, the process passes from block 192 to block 198. Block 198 illustrates the initiation for playing the DVD whereafter the process returns.

Referring still to **Figure 8**, block 200 depicts the comparison of user identification data from the smart

card with registration data from the smart chip mounted to the smart compact disc. Thereafter, the process passes to block 202. Block 202 illustrates the determination of whether or not the user identification data matches the registration data. If the data matches, then the process passes to block 198 and proceeds as previously described. Otherwise, the process passes to block 204 and proceeds as previously described.

}

With reference now to **Figure 9**, there is illustrated a high level logic flowchart of the method for the uninstallation of ownership of a smart compact disc according to the method and system of the present invention. As illustrated, the process described in **Figure 9** begins at block 210 and thereafter passes to block 212. A plurality of triggers in the operation of microprocessor 30 may trigger the process which begins at block 210. For example, upon detecting a user request to uninstall ownership of a smart compact disc, the process may be triggered.

Block 212 illustrates the reading of user identification data from a smart card. After block 212, the process passes to block 214. Block 214 depicts the reading of registration data from a smart chip mounted to a smart compact disc. Thereafter, the process passes from block 214 to block 216. Block 216 illustrates the determination of whether or not registration data has been previously installed on the smart chip mounted to the smart compact disc. If registration data for the smart chip needs to be installed, the process passes to block 218. Block 218 depicts the displaying of an error

message since the smart chip does not have a record of any previous software installation. If the registration data for the smart chip has been previously installed, the process passes to block 220.

With reference still to **Figure 9**, block 220 illustrates the comparison of user identification data from the smart card with registration data from the smart chip mounted to the smart compact disc. Thereafter, the process passes from block 220 to block 222. Block 222 depicts the determination of whether or not the user identification data matches the registration data. If the data matches, the process passes to block 224. However, if the data does not match, the process passes to block 226. Block 226 illustrates the displaying of an error messages because proper identification has not been supplied.

Referring still to **Figure 9**, block 224 depicts the erasure of the registration data from the smart chip. The uninstall registration data process is included such that a consumer may release ownership of a compact disc, particularly audio CD or DVD, to another individual. The DVD smart chip may also include a counter for controlling the number of times a DVD may be viewed for rental purposes. During the uninstall process, the counter would be reset.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein

without departing from the spirit and scope of the invention. For example, in the processes of the present invention, user identification data is obtained from a smart card or a smart card chip embedded in hardware. However, in other embodiments, user identification data may be obtained from other sources, already described such as user identification data embedded within a data processing system. In addition, user identification data may be obtained from other sources including not limited to biometric data, where in order to gain access to the compact disc, the compact disc owner must identify themselves through an eye scan or other biometric data gathering method where the user identification data is stored in the smart chip affixed to the compact disc.

In addition, for example, although the present invention has been described with focus on utilizing a data storage device comprising optically discernable data, such as a compact disc, other optical storage devices may also utilize the method and system of the present invention without departing from the spirit of the invention. In addition, other electronic storage devices may be utilized in place of a smart chip.

In addition, for example, although aspects of the present invention have been described with respect to a data storage system executing software that directs the method of the present invention, it should be understood that the present invention may alternatively be implemented as a computer program product for use with a data processing system. Programs defining the functions of the present invention can be delivered to a data

processing system via a variety of signal-bearing media, which include, without limitation, non-writable storage media (e.g., CD-ROM), writable storage media (e.g. a floppy diskette or hard disk drive), and communication media, such as computer and telephone networks including ethernet. It should be understood, therefore, that such signal-bearing media, when carrying or encoding computer readable instructions that direct the method functions of the present invention, represent alternative embodiments of the present invention.

CLAIMS

1. A method of securing access to optically discernable data embedded within a data storage device, said method comprising the steps of:

determining if there is registration data stored on an electronic storage device affixed to a data storage device in response to said data storage device inserted into a reader;

comparing said registration data with user identification data; and

reading said optically discernable data embedded within said data storage device in response to said registration data matching said user identification data, such that access to optically discernable data on a data storage device is only permitted by proper identification.

2. The method of securing access to optically discernable data stored on a data storage device according to claim 1, further comprising the step of:

updating registration data stored on said electronic storage device when said optically discernable data is accessed for tracking a number of access made to said optically discernable data on said data storage device.

3. The method of securing access to optically discernable data stored on a data storage device according to claim 2, further comprising the step of:

restricting access to said optically discernable data after a predefined amount of accesses to said optically discernable data have been made.

4. The method of securing access to optically discernable

data stored on a data storage device according to claim 1, further comprising the step of:

storing registration data on said electronic storage device if there is not registration data stored on said electronic storage device affixed to said data storage device.

5. The method of securing access to optically discernable data stored on a data storage device according to claim 4, wherein said step of storing registration data on said electronic storage device if there is not registration data stored on said electronic storage device affixed to said data storage device further comprising the steps of:

accessing said user identification data; and
utilizing said user identification data as registration data for storage on said electronic storage device.

6. The method of securing access to optically discernable data stored on a data storage device according to claim 5, wherein said step of accessing user identification data further comprises the steps of:

detecting a smart card; and
accessing said user identification data from said smart card.

7. The method of securing access to optically discernable data stored on a data storage device according to claim 4, wherein said step of storing registration data on said electronic storage device if there is not registration data stored on said electronic

26 JUL 2002

storage device affixed to said data storage device further comprising the steps of:

comparing a particular geographic region contained within said user identification data with a predetermined geographic region stored on said electronic storage device; and

in response to said particular geographic region contained within said user identification data matching said predetermined geographic region stored on said electronic storage device, permitting storage of registration data on said electronic storage device.

8. The method of securing access to optically discernable data stored on a data storage device according to claim 1, wherein said step of comparing said registration data with user identification data further comprises the step of:

accessing said user identification data.

9. The method of securing access to optically discernable data stored on a data storage device according to claim 8, wherein said step of accessing said user identification data further comprises the steps of:

detecting a smart card; and

accessing said user identification data from said smart card.

10. The method of securing access to optically discernable data stored on a data storage device according to claim 8, wherein said step of accessing said user identification data further comprises the steps

26 JUL 2002

- 32 -

of:

detecting a smart chip associated with said reader where said user identification data is stored on said smart chip; and

reading said user identification data from said detected smart chip.

11. The method of securing access to optically discernable data stored on a data storage device according to claim 8, wherein said step of accessing said user identification data further comprises the steps of:

obtaining said user identification data from user data collected during the installation of an operating system which controls said reader.

12. The method of securing access to optically discernable data stored on a data storage device according to claim 1, further comprising the step of:

changing said registration data on said electronic storage device.

13. The method of securing access to optically discernable data stored on a data storage device according to claim 12, said step of changing said registration data on said electronic storage device further comprising the steps of:

uninstalling any copies of said optically discernable data;

erasing said registration data from said electronic storage device.

14. A system for securing access to optically discernable data embedded within a data storage device, said system comprising:

means for determining if there is registration data stored on an electronic storage device affixed to a data storage device in response to said data storage device inserted into a reader;

means for comparing said registration data with user identification data; and

means for reading said optically discernable data embedded within said data storage device in response to said registration data matching said user identification data, such that access to optically discernable data on a data storage device is only permitted by proper identification.

- 34 -

15. The system for securing access to optically discernable data stored on a data storage device according to claim 14, further comprising:

means for updating registration data stored on said electronic storage device when said optically discernable data is accessed for tracking a number of access made to said optically discernable data on said data storage device.

16. The system for securing access to optically discernable data stored on a data storage device according to claim 15, further comprising:

means for restricting access to said optically discernable data after a predefined amount of accesses to said optically discernable data have been made.

17. The system for securing access to optically discernable data stored on a data storage device according to claim 14, further comprising:

means for storing registration data on said electronic storage device if there is not registration data stored on said electronic storage device affixed to said data storage device.

18. The system of securing access to optically discernable data stored on a data storage device according to claim 17, wherein said means for storing registration data on said electronic storage device if there is not registration data stored on said electronic storage device affixed to said data storage device further comprises:

means for accessing said user identification data;

- 35 -

and

means for utilizing said user identification data as registration data for storage on said electronic storage device.

19. The system for securing access to optically discernable data stored on a data storage device according to claim 18, wherein said means for accessing user identification data further comprises:

a smart card reader for accessing said user identification from a smart card.

20. The system for securing access to optically discernable data stored on a data storage device according to claim 17, wherein said means for storing registration data on said electronic storage device if there is not registration data stored on said electronic storage device affixed to said data storage device further comprises:

means for comparing a particular geographic region contained within said user identification data with a predetermined geographic region stored on said electronic storage device; and

means for permitting storage of registration data on said electronic storage device in response to said particular geographic region contained within said user identification data matching said predetermined geographic region stored on said electronic storage device.

21. The system for securing access to optically discernable data stored on a data storage device

according to claim 14, wherein said means for comparing
said registration data with user identification data
further comprises:
 means for accessing said user identification data.

26 JUL 2002

22. The system for securing access to optically discernable data stored on a data storage device according to claim 21, wherein said means for accessing

said user identification data further comprises:

a smart card reader for accessing said user identification from a smart card.

23. The system for securing access to optically discernable data stored on a data storage device according to claim 21, wherein said means for accessing

said user identification data further comprises:

means for detecting a smart chip associated with said reader where said user identification data is stored on said smart chip; and

means for reading said user identification data from said detected smart chip.

24. The system for securing access to optically discernable data stored on a data storage device according to claim 21, wherein said means for accessing

said user identification data further comprises:

means for obtaining said user identification data from user data collected during the installation of an operating system which controls said reader.

25. The system for securing access to optically discernable data stored on a data storage device according to claim 14, further comprising:

means for changing said registration data on said electronic storage device.

26. The system for securing access to optically discernable data stored on a data storage device according to claim 25, said means for changing said registration data on said electronic storage device further comprising:

means for uninstalling any copies of said optically discernable data;

means for erasing said registration data from said electronic storage device.

27. A program product for securing access to optically discernable data embedded within a data storage device, said program product comprising:

a data processing system usable medium; and

a data storage device control program encoded with said data processing system usable medium that, in response to a compact disc inserted into a compact disc drive:

determines if there is registration data stored on an electronic storage device affixed to a data storage device;

compares said registration data with user identification data;

reads said optically discernable data embedded within said data storage device in response to said registration data matching said user identification data, such that access to optically discernable data on a data storage device is only permitted by proper identification.

28. The program product of claim 27, wherein said data storage device control program updates registration data

stored on said electronic storage device when said optically discernable data is accessed for tracking a number of access made to said optically discernable data on said data storage device.

29. The program product of claim 28, wherein said data storage device control program restricts access to said optically discernable data after a predefined amount of accesses to said optically discernable data have been made.

30. The program product of claim 27, wherein said data storage device control program stores registration data on said electronic storage device if there is not registration data stored on said electronic storage device affixed to said data storage device.

31. The program product of claim 30, wherein said data storage device control program accesses said user identification data and utilizes said user identification data as registration data for storage on said electronic storage device.

32. The program product of claim 31, wherein said data storage device control program accesses said user identification data from a smart card.

33. The program product of claim 30, wherein said data storage device control program compares a particular geographic region contained within said user identification data with a predetermined geographic region stored on said electronic storage device and

- 40 -

in response to said particular geographic region contained within said user identification data matching said predetermined geographic region stored on said electronic storage device, permits storage of registration data on said electronic storage device.

34. The program product of claim 27, wherein said data storage device control program accesses said user identification data.

35. The program product of claim 34, wherein said data storage device control program accesses said user identification data from a smart card.

36. The program product of claim 34, wherein said data storage device control program detects a smart chip associated with said reader where said user identification data is stored on said smart chip and reads said user identification data from said detected smart chip.

37. The program product of claim 34, wherein said data storage device control program obtains said user identification data from user data collected during the installation of an operating system which controls said reader.

38. The program product of claim 27, wherein said data storage device control program changes said registration data on said electronic storage device.

39. The program product of claim 38, wherein said data

26 JUL 2002

- 41 -

storage device control program uninstalls any copies of
said optically discernable data and erases said
registration data from said electronic storage device.