PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:
H04K 1/00	A1	WO 95/03655
		(43) International Publication Date: 2 February 1995 (02.02.95)

(21) International Application Number: PCT/US94/08322

(22) International Filing Date: 19 July 1994 (19.07.94)

(30) Priority Data:
08/097,767 26 July 1993 (26.07.93) US

(71) Applicant: OAKLEIGH SYSTEMS, INC. [US/US]; 801 East Arques Avenue, Sunnyvale, CA 94086-4522 (US).

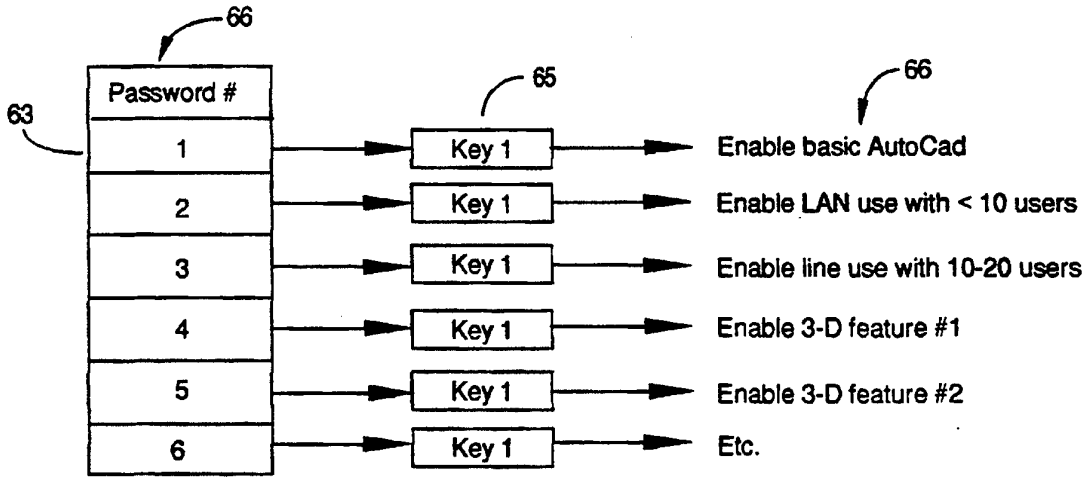
(72) Inventor: KIKINIS, Dan; 20264 Ljepava Drive, Saratoga, CA 95070 (US).

(74) Agent: BOYS, Donald, R.; Central Coast Patent Agency, P.O. Box 187, Aromas, CA 95004 (US).

(81) Designated States: CN, JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: CD PROM ENCRYPTION SYSTEM



(57) Abstract

Encrypted data on a CD-PROM disk is managed by selectively encoding binary digital decryption keys (65) onto the same disk in a separate data area. A decryption key or keys (65) may be programmed onto the disk after manufacture, such as at the point of sale, by selectively obliterating the readability of bits in addressable sectors. A binary digital key (65) is then later recognized as the result of a string of addressable sectors, with one or the other of readable or unreadable sectors being recognized as a logical 1 and the other as a logical 0. In an embodiment, a manufacturer may place several or all versions and features of a large program on a single CD-ROM, encrypted, and later provide keys (65) to enable only selected ones of the features (66) and versions (66) for retrieval.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

--CD PROM ENCRYPTION SYSTEM--

Field of the Invention

The present invention is in the area of Compact Disk Read-Only Memory (CD-ROM) disks and pertains more specifically to programmable access control of data on such disks.

Background of the Invention

CD-ROM is an extension of CD audio, the high-quality disk technology of the music industry. A conventional CD-ROM disk, measuring only 4-3/4 inches in diameter is capable of storing an equivalent of up to 250,000 pages of text, 1,500 floppy disks, 74 minutes of audio, or thousands of images, any of which can be retrieved in seconds by a computer-based CD-ROM player. CD-ROM products are available to users in a wide variety of fields such as library science, education, publishing, online database services, government, banks, insurance, law, engineering, and medicine.

CD-ROM disks typically have a single, spiraling track that is about three miles long. The track is typically read from the inside out. Data on the track is divided into sectors, each equal in length, containing equal amounts of information and having absolute addresses. Fig. 1 illustrates a standard data format. In this format, each sector 13 on CD-ROM disk 11 comprises 2,352 bytes of information with 12 bytes of synchronization, 4 bytes of identification, 288 bytes of error-correction code and 2,048 bytes of data.

A CD-ROM master is made by use of a high-power laser to form a series of tiny indentions in the surface of a blank forming the single spiral track. The pattern and length of the indentions along the track represent the recorded information digitally. The original blank is

used to make a master, typically of wear resistant material, for use in molding replicas, which become the familiar CD-ROM disks. The pattern from the master disk is reproduced on the surface of a polymer substrate, which is then a copy of the original.

The stamped replicas are coated with a highly reflective material, typically vapor deposited aluminum, and a protective coating is applied over the thin reflective film.

Early CD-ROM disks comprised digitized analog information designed to be used primarily in linear format with limited user control of playback. Other CD-ROM disks were programmed to use the disk player's microprocessor and limited internal memory. Today's more highly developed CD-ROM systems provide potentially limitless interactivity as their programs are typically under the supervision of an external computer.

To read CD-ROM data a laser-equipped drive in a CD-ROM player changes its rate of spin, turning the disk more slowly as sectors farther from the disk center are read. As the disk is spinning, the low-power read laser is focused on the spiral track through the thickness of the polymer disk, and reflected light is picked up by a photodetector that converts the presence or absence of indentions into electrical signals interpreted as digital data by the computer. The read laser "sees" the indentions from the side opposite where they wee produced, and therefore sees an indention as a protrusion toward the laser source.

When the read laser encounters the land of an indention, the focused light from the laser is largely scattered, so the light reflected to the photodetector is diminished. In the area where there is no indention from the opposite side, more light is reflected to the photodetector.

Fig. 2 illustrates a series of indentions formed in the surface of a CD-ROM disk 31. Surface 23 is the original disk surface, and level 25 indicates the level of penetration into the original surface of the formed indentions. The Figure is not to scale, as the indentions are almost infinitesimally small in depth relative to the thickness of the disk. The read laser operates in the direction of arrow 24.

CD-ROM, much like other high-density storage systems, relies on channel codes for storage and retrieval of data. The channel code typically used for CD-ROM is called eight-to-fourteen modulation (EFM).

In the EMF system, each time the moving disc translates an "edge" past the laser beam, the reflected light intensity changes, signalling a transition 27 that is decoded as binary 1 by the host's reading system. Binary 0's occur everywhere else, and the number of 0's between "1" transitions is a function of the length along the spiral track of the land between indentions. In operation, the channel code is converted into digital bytes and data blocks by reference to stored look-up tables. The typical system of encoding and decoding is well known in the art.

A complete CD-ROM file system consists of three major components: logical format, which defines the disk's directory structure and operating characteristics through decoder programs that determine such matters as where to find the directory of the files on the CD-ROM disk, how the directory is structured, and how to perform error correction on disk data; origination programs, which write the data on the disk according to the logical format; and destination programs, the reading component on the host computer that understands the logical format and can use it to provide access to the files on the CD-ROM and read and translate the data structure.

Most CD-ROM disks have their own operating systems that respond to calls from a file manager that is exclusively used by CD-ROM. CD-ROM disks also contain their own search decoder programs that define where sectors are located so the computer knows where to locate the stored data. These search decoders typically have a menu-driven interface on the computer. CD-ROM programs typically require 640 kilobytes of computer memory to run, and may allocate their own storage addresses on the computer's hard disk for its data access driver and destination programs.

Nearly all CD-ROM disks and CD-ROM players available today conform to what is known as the High Sierra standard or to a more recent upgrade, the ISO 9660 standard. The connection between CD-ROM players and computers also has been for the most part standardized. CD-ROM players typically use the Small Computer Systems Interface (SCSI) to link with a computer.

CD-ROMs appear to be reasonable and convenient vehicles for marketing large application programs rather than using large numbers of floppy disks. They easily provide enough space and their cost is low, about $.50 a disk when produced in large volumes. The cost of CD-ROM drives is also becoming more reasonable as well.

Despite apparent advantages, there remain some serious drawbacks to use of CD-ROMs for marketing large application packages. The most serious is that there is no reliable method or mechanism whereby comprehensive versions and features may be recorded on a single disk, and only certain portions enabled for a particular customer.

Also the lack of satisfactory copy protection of CD-ROM disks remains a problem. CD-ROM disks are typically shipped with a companion floppy disk that contains data access driver and destination programs that must be

installed on the user's computer in order for CD-ROM to run. The floppy is copy-protected but the CD-ROM disk is not. This method of copy protection is no more effective than copy protection for floppies in general. The contents of CD-ROM can be copied to hard disk and the floppy protection scheme can be defeated by any of a number of available copy programs.

Multi-application packages such as Ethernet, Windows, and AutoCad, and many others, therefore, continue to be furnished on multiple floppy disks. Many of these programs have become so diverse that as many as 20 to 40 floppy disks may be required to install a complete set of programs on a host computer.

What is needed is a means whereby vendors of large and diverse applications can record all of an application on a single CD-ROM, and then selectively enable access of portions of the data at time of purchase. Also a means is needed to copy-protect CD-ROM disks so floppies are not the sole means for protection. With these improvements a vendor could cost-effectively mass-produce one full version of a product on a single CD-ROM disk, have the disk copy-protected, and selectively control use of its applications. The user, who only has to make a one-time purchase of a basic package on a single disk, could have access to other applications on the disk by simply paying the vendor for them as needed.

Summary of the Invention

In an embodiment of the present invention, a method for encrypting data on a compact disk read-only memory CD-ROM disk and enabling retrieval of the data by a host computer is provided, comprising steps of (1) storing data on the disk in the manufacturing process in an encrypted fashion having the data arranged according to an

encryption scheme, and being decryptable by a retrieval routine operable on the host computer using a first digital key; and (2) programming the digital key into the CD-ROM disk after manufacture of the CD-ROM disk by altering selected sectors on the CD-ROM disk to be unreadable by conventional laser read control routines. The digital sequence comprising the digital key is a digital sequence identified by a sequence of readable and unreadable sectors, one of the characteristics of being readable and unreadable being interpreted as logical 1 and the other as logical 0.

In one aspect of the invention, an ability to program codes onto a manufactured CD-ROM disk is provided by a laser device similar to a CD-ROM drive, but having a higher-power laser capable of destroying the readability of the bit pattern in addressable sectors.

In another aspect of the invention multiple features and versions of a large program may be placed on a single CD-ROM disk, and selected portions enabled at point of sale by programming on the disk selected decryption keys. By placing all keys on the disk in an encrypted way, and providing further keys at a later time to a customer, further data may be "unlocked" as needed or paid for.

The data recording aspect of the invention is not limited to providing keys for unlocking encrypted data. Any data may be placed on the disk by the recording technique provided, including operable programs. The method and apparatus of the invention provide a means to effectively copy protect information on CD disks, and to selectively enable portions of encrypted information.

Brief Description of the Drawings

Fig. 1 is an illustration of addressable sector content in the prior art for a sector on a CD-ROM.

Fig. 2 is a section view through a track of a CD-ROM in the prior art, showing indentions for indicating bit transitions.

Fig. 3 is a plan view of a CD-PROM in an embodiment of the present invention, showing data storage and programming regions.

Fig. 4A is an isometric view of a programming device according to an embodiment of the invention.

Fig. 4B is a largely diagrammatical view of internal elements of the programming device of Fig. 4A.

Fig. 4C is a section view of a CD-ROM mounted in the programming device of Fig. 4B and 4A, showing the relative convergence of a focused laser beam in the device.

Fig. 5 is an illustration of the concept of passwords as decryption keys according to an embodiment of the invention.

Fig. 6 is a logic flow diagram indicating the steps in a method of decrypting data according to an embodiment of the invention.

Description of the Preferred Embodiments

The present invention, termed CD-PROM for Compact Disk Programmable Read Only Memory, is in one aspect a means for selectively enabling data on CD-ROM disks after mastering and pressing but before providing the disks to an end user. The data storage capacity of a conventional CD-ROM disk is about 600 megabytes. Of that amount, some few megabytes are typically devoted to the disk's operating system (OS). Typically large applications programs such as Windows, Ethernet, and AutoCad require no more than 100 megabytes of storage area. That leaves nearly 500 megabytes of data storage area free for use in access enablement schemes and other programming.

The present invention involves in one aspect

encoding into a CD-PROM disk, by a unique laser programming means, digital patterns comprising coded passwords that enable access to selected data on the disk.

Fig. 3 is a plan view of a CD-PROM disk 31 according to an embodiment of the present invention. A small region 33 near inside opening 32 is dedicated to the disk's operating system (OS). This OS is automatically loaded on a host computer when a disk is placed in the drive of an attached optical disk player, assuming the computer control system has been configured for the drive. Region 35 on the disk, occupying perhaps 100 megabytes, is used for data storage. In this region all data pertinent to an application may be stored. For example, for a program like AutoCad, all features, versions, etc. are stored in region 35. The size of region 35 is variable, depending on the application.

All of the data in region 35 is encrypted. A multitude of schemes exist for doing such encryptions such as reverse alphabet, letter substitution, word inversion, number-to-letter substitution, and variations of combinations of these and many other methods.

The remainder of the CD-PROM disk, region 37, which may be typically up to about 500 megabytes in usable capacity, is the programming area. In this area passwords are recorded and programming is done. The means of enabling various parts of data region 35 are provided in programming area 37 through.

Fig. 4A is an isometric view of a laser programming device 39 according to an embodiment of the invention. Externally device 39 may appear much like a conventional CD-ROM disk drive. It has in this embodiment a disk tray 41 for receiving a CD-ROM disk 34, an open/close actuator 43, and a dip switch 45. In other embodiments, there me other control actuators as well.

Laser programming device 39 also resembles a

conventional CD-ROM disk drive internally, except where the read laser unit is typically installed, a higher-power laser unit is used that is capable of destroying sectors on a CD-PROM disk. Also, the laser unit in device 39 is controllable to selectively destroy sectors to accomplish a programming function.

Fig. 4B is a largely diagrammatical illustration of internal elements of programming device 39. The electronic circuitry is quite similar to that of a standard CD-ROM disk drives and is not diagrammed in Fig 4B.

To operate programming device 39, a CD-ROM disk 34 is placed in disk drawer 41 with its read side down, that is, the reflective layer is on the side opposite the laser device. A laser system generally indicated by elements 46, comprising a laser, focusing elements, and tracking mechanisms, is located in about the position the corresponding elements would be located in a CD-ROM drive.

Control routines operating on a host computer 57 in this embodiment over a communication link 47 to on-board control circuitry 52 provide control operations to drive programming device 39. The same control routines provide a user-interface on the host computer display, allowing an operator to control and alter the operations of device 39.

In operation a laser beam 49 is selectively enabled from laser emission device 50 when a signal is received from the host. Beam 49 is focused in this embodiment through a prism 51 and an objective lens 53 onto the spiral track of CD-ROM disk 34. Actuators 58 control focusing adjustments, drive 55 spins the CD-ROM disk, and translation actuator 56 shifts the laser system radially along rails to follow the spiral track.

Fig. 4C is an enlarged section through one portion of a spiral track of CD-ROM disk 34 with laser beam 49 focused through the thickness of the disk onto the

indentions in the spiral track. The thickness D1 of a CD-ROM is typically about 1.2 mm, and the depth D2 of the depressions is typically about .12 micrometers. A track is typically about .6 micrometers wide, and the dimension between tracks is typically about 1.6 micrometers. In this section, the disk is shown with a lacquer topcoat 36.

It is seen, then, that the magnitude of the depressions in the surface of the CD-ROM disk is but a very small portion of the thickness of the disk, and the depressions themselves are quite shallow.

Keeping in mind the relative and typical dimensions given above, there are at least two mechanisms by which the energy from laser beam 49 may be concentrated at the spiral track, in a manner that is not injurious to the bulk of the disk, and whereby selected sectors in the track may be altered in a manner to be unreadable by a conventional reading mechanism. One means is by focusing beam 49 at a large included angle A so the power per unit area remains proportionally small until the track region is reached. Another is by selecting the wavelength for the laser to be a wavelength for which the material of the disk is relatively transparent. In different embodiments of the present invention, different combinations are used. Also, the presence of the reflective layer immediately at the track interface is an aid in obliterating data recordation in selected areas, as a portion of the laser energy tends to be reflected at this interface. Moreover, alteration or local destruction of the reflective layer itself by the energy of beam 49 has been found to contribute to the ability to obliterate selected sectors.

In embodiments of the present invention the pattern of sectors destroyed and not destroyed sequentially along the spiral track in region 37 (see Fig. 3) becomes a recognizable digital string for use by the operating system in decrypting data stored in region 35. Literally

any programmed information may then be placed in a selected region on a CD-ROM disk, providing therefrom a CD-PROM disk according to a preferred embodiment of the present invention.

It is not necessary that an enabling password or other programmed data be in a serial sequence. There can be patterns within patterns, and the organization of sectors to produce a single password or data for another purpose might be scattered over entire programming region 37. There may be many passwords on a disk, each capable of enabling a different application.

The concept of password enablement as practiced in embodiments of the present invention is illustrated with the aid of Fig. 5, which shows an index table 61 of passwords 63, each yielding a digital key 65 to enable a selected portion of (for example) a region 37 on a CD-PROM according to an embodiment of the invention. The selected portion keyed by such a password may be an application 66 such as AutoCad, or some other useful, and separable, data group, as indicated in Fig. 5. The individual keys enable separately bootable features or versions of the application.

Such a password table is, of course, a useful mechanism for understanding the selective enablement concept of the present invention. This password table does not really ever get written to memory anywhere. If it did, it could be copied and used to break the code. Instead, the ability to find passwords is programmed into the OS, and the actual passwords are discarded as quickly as used.

A password enablement scheme according to an embodiment of the present invention is flowcharted in Fig. 6. At the start, a CD-PROM disk is inserted in the disk drive at event 67. The OS program is loaded on the computer at event 69. An early function is checking for a

serial number at function 71 (at the discretion of the vendor). In this particular path, if the licensing serial number does not check, the enablement process may be aborted (function 73). The OS in this embodiment next searches programming region 37 for a first password (function 75).

When the OS finds a password at function 77, the password is passed to the decryptors at function 79, and used to unlock data keyed addresses. The system then reads the unlocked data (function 83), typically loading the decrypted data to a location on the host system's hard disk. At function 85 the password is discarded. The discarding function is not necessarily a separate step in the operation, and may be a natural function of the data flow as controlled by the operating system.

After all the passwords are found and the data meant to be accessible is accessed, control passes to end function 89.

"Unlocking" with a password can be as simple as enabling a sequential range of sectors by beginning address and length to be read into memory or it can be extremely complex. An example of a simple unlocking scheme would be the case where a password gives instructions to "read every 5th sector in a range beginning at a specific address." Another scheme could change the unlocking instruction on a daily basis by requiring, for example, "if it is the 23rd hour of the day, a predefined number be added to every 6th sector."

an example of a more complex unlocking scheme could be as follows: The OS looks for password #1, say an 8-bit digital word, and finds it. This password is a key for an algorithm to be loaded that searches for another key in data region 37 in one of 24 different patterns, one pattern for each hour of the day, as determined by querying the clock on the computer. Password #2 is the

actual enabling key that is available from all 24 search patterns or any one of them. The added factor of basing the search on time with the first password effectively adds another layer that a person would have to solve to defeat the system.

In another embodiment of the invention there can be a means of sending an enabling password to a user who wants to access more applications on a CD-PROM disk than he/she originally purchased. In this embodiment a user interface in the form of a query from the computer to enter the actual password would not be needed. Instead the password could be an addition to the CONFIG.SYS file, a keystroke sequence, or other means to enable the OS to find the password key already on the CD-PROM disk to unlock the desired application in data region 37.

An additional feature is the built-in copy-protection that CD-PROM provides with the data on the disk being encrypted. The disk can be copied but the encrypted data will be unusable. With the CD-PROM disk itself copy-protected, the more vulnerable method of providing copy protection on a companion floppy disk is not necessary.

Because of the large capacity of programming region 37, there is a very broad range of possibilities in programming. For instance, the system can be used by companies that sell mailing lists to track the use of the lists. An entire mailing list can be sold on a single CD-PROM together with all the necessary routines to use it to print labels, cards, or even "self-mailers." These companies could charge for a mailing list on CD-PROM based on the number of times the user uses the mailing list. Programming on the CD-PROM disk along with the OS could be used to customize the list to include a fictitious recipient with an address that goes to the vendor. In this way the vendor would receive a mailer addressed to the fictitious party every time the customer uses the

mailing list. This would enable the vendor to keep track of how many times the mailing list is actually being used.

It will be apparent to one skilled in the art that there are many changes that may be made in the embodiments described without departing from the spirit and scope of the present invention. Some alternatives have been described above. For example, provisions may be made to add a secondary level of access control to give the user the option to "pay as you go" for extra applications that are available on the CD-PROM disk. Another variation adds a copy protection scheme to the CD-PROM disk.

There are also a number of equivalent ways the several features described for the invention might be implemented without departing from the spirit and scope of invention as well. For example, the aforedescribed embodiments could be rendered in different sizes. For instance, data bases exist today that are larger than 500 megabytes and can not fit on a single CD-PROM disk. The concept of a single CD-PROM disk presented in this invention could be expanded to the production of a set of CD-PROM disks as a way to accommodate extra large data bases in an orderly manner and still provide enablement control and copy protection on the single disks. Another variation would utilize one or more of the large 12-inch size video disks for CD-PROM storage as dictated by the size of the data base. Many other such alterations fall within the spirit and scope of the invention.

What is claimed is:

1. A method for encrypting data on a compact disk read-only memory CD-ROM disk and enabling retrieval of said data by a host computer, comprising:

storing data on said disk in the manufacturing process in an encrypted fashion having said data arranged according to an encryption scheme being decryptable by a retrieval routine operable on said host computer using a first digital key; and

programming said digital key into said CD-ROM disk after manufacture of said CD-ROM disk by altering selected sectors on said CD-ROM disk to be unreadable by conventional laser read control routines, the digital sequence comprising the digital key being then a digital sequence identified by a sequence of readable and unreadable sectors, one of the characteristics of being readable and unreadable being interpreted as logical 1 and the other as logical 0.

2. The method of claim 1 wherein said programming is accomplished by altering said selected sectors with a focused laser device, focusing the energy of a laser beam on said selected sectors one at a time through the thickness of the material of said CD-ROM disk.

3. A method for storing data on a compact disk read-only memory (CD-ROM) disk and enabling retrieval of said data from said CD-ROM disk by a host computer, comprising steps of:

storing data on the disk in the manufacturing process in an encrypted fashion, a first portion of the encrypted data being arranged according to a first encryption scheme and a second portion of said encrypted data being arranged according to a second encryption scheme, the data in said first portion being decryptable by a retrieval routine using a first digital key, and the data in said second portion being decryptable by said retrieval routine using a second digital key; and

programming at least one of said first and second digital keys into said CD-ROM disk by altering selected sectors on said CD-ROM disk to be unreadable by conventional laser read control routines,the digital sequence comprising the digital key being then a sequence identified by a sequence of readable and unreadable sectors, one of the characteristics of being readable and unreadable being interpreted as logical 1 and the other as logical 0.

4. The method of claim 3 comprising more than two encrypted portions and digital keys, wherein the encrypted data comprises one or more of versions and features of at least one computer application program, and said digital keys are programmed onto said CD-ROM disk to selectively enable one or more of said versions and features.

5. The method of claim 3 wherein said programming is accomplished by altering said selected sectors with a focused laser device, focusing the energy of a laser beam on said selected sectors one at a time through the thickness of the material of said CD-ROM disk.

6. A programming system for after-manufacture programming of data onto a compact disk read-only memory (CD-ROM) disk, comprising:

a general-purpose computer means for operating said programming system;

a CD drive programmer means linked to and drivable by said general-purpose computer means to rotate a mounted said CD-ROM disk and to focus a laser beam on a spiral data track of said mounted CD-ROM disk; and

control means operable by said general-purpose computer for locating selected sectors in said spiral data track, and for selectively operating said laser beam to render bit information in said selected sectors unreadable by conventional

CD-ROM reading means.

7. A programming system as in claim 6 wherein said data comprises encryption keys for rendering encrypted information previously recorded on said CD-ROM disk retrievable by a general-purpose computer operating a CD-ROM drive.

8. A compact disk (CD) programming drive comprising:

drive means for mounting and rotating a CD;

focused laser means for tracking a spiral data track of said CD and for focusing a laser beam on the spiral track;

control means for locating selected sectors in said spiral data track, and for selectively operating said laser beam to render bit information in said selected sectors unreadable by conventional CD-ROM reading means.

9. A CD programming drive as in claim 7 wherein said laser beam is focused through the thickness of the material of said CD.

10. A compact disk programmable read only memory (CD-PROM) disk comprising:

an encrypted portion wherein data is recorded by laser-readable indentions in a spiral track, the data being recorded in each one of plural regions within said encrypted portion by an encryption scheme unique to that region and retrievable by a decryption algorithm based on a decryption key unique to each encrypted region, each said decryption key being a binary digital string; and

a programming portion wherein one or more decryption keys are recorded, each decryption key being a binary digital sequence identifiable by a sequence of readable and unreadable sectors, one of the characteristics of being readable and unreadable being interpreted as logical 1 and the other as logical 0.

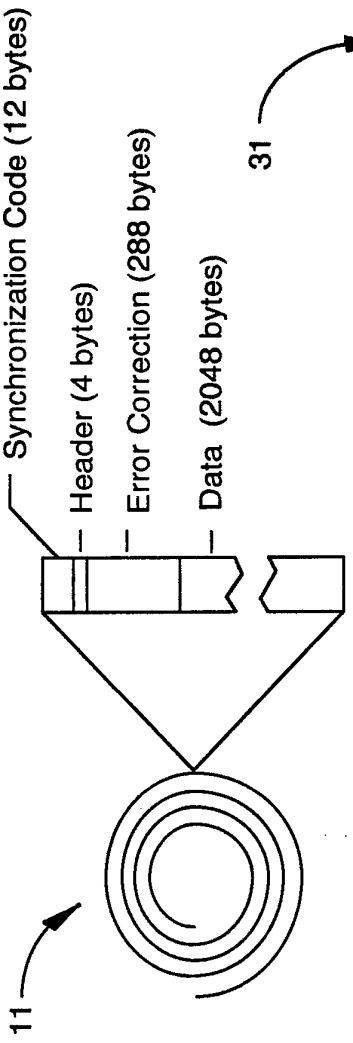


Fig. 1 Prior Art

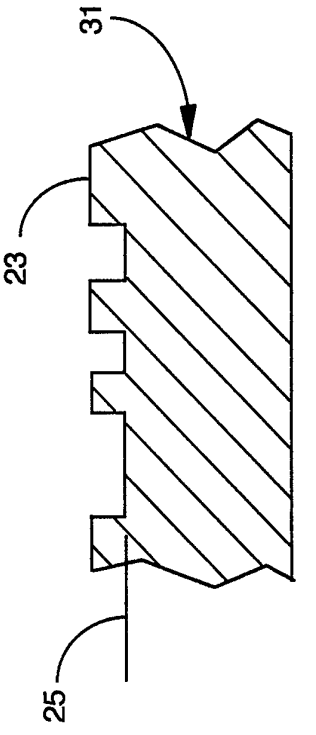


Fig. 2 Prior Art

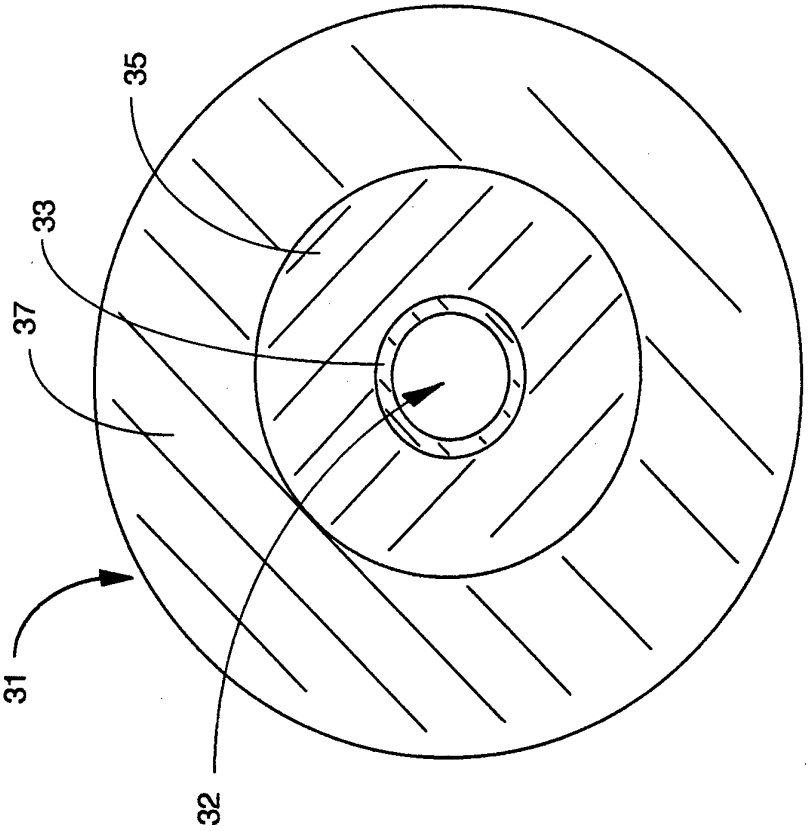


Fig. 3

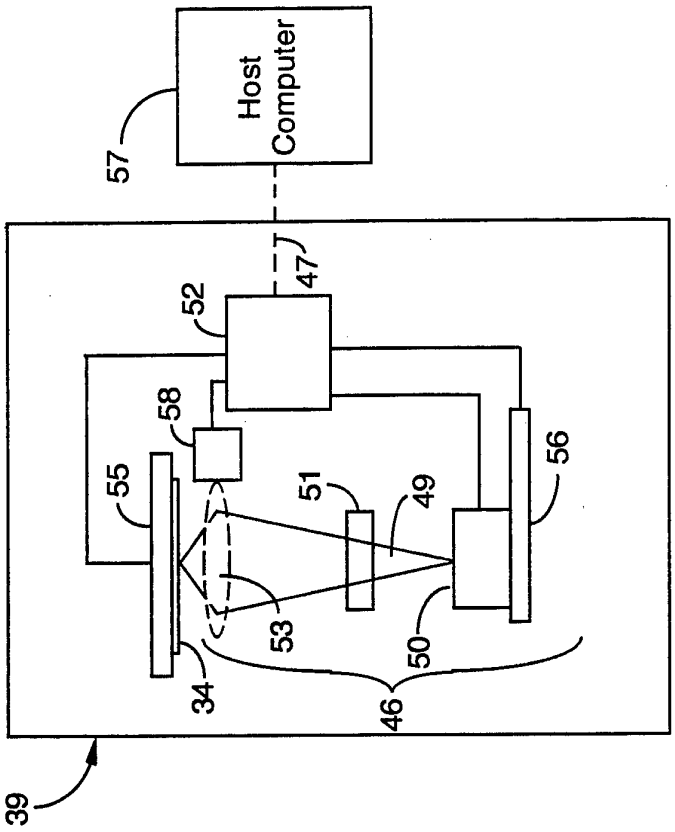


Fig. 4B

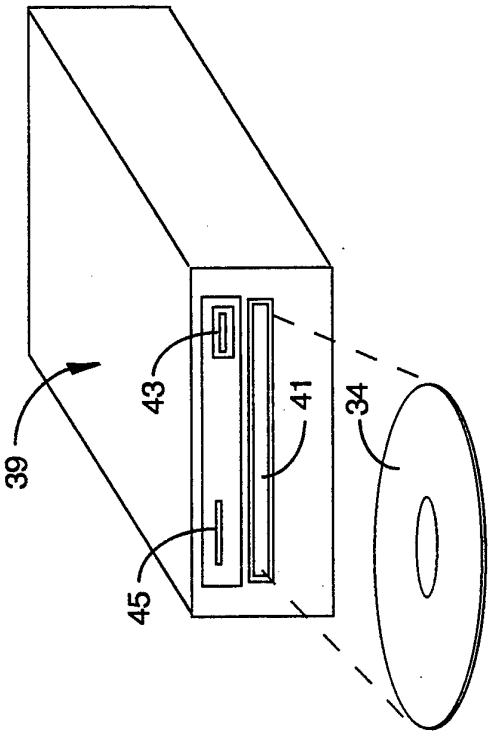


Fig. 4A

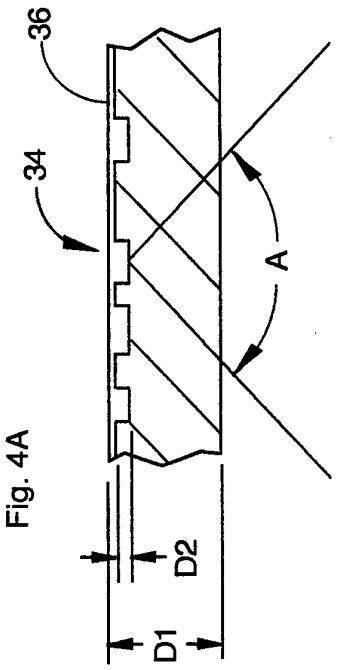


Fig. 4C

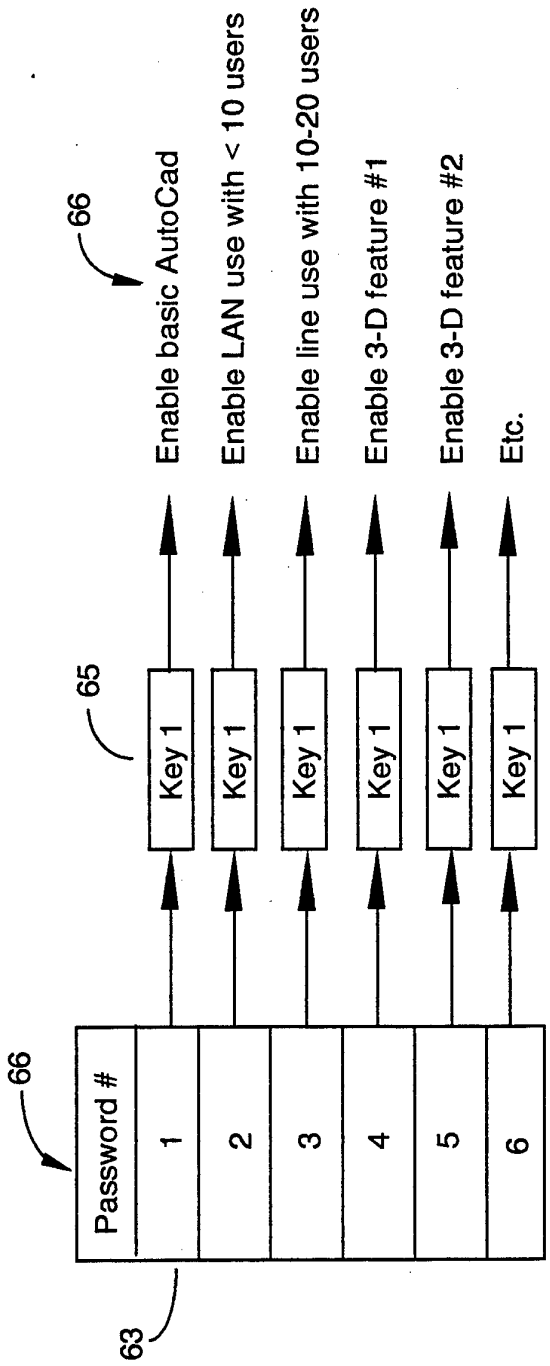

66
Password #
1
2
3
4
5
6
63
65
Key 1
Key 1
Key 1
Key 1
Key 1
Key 1
66
Enable basic AutoCad
Enable LAN use with < 10 users
Enable line use with 10-20 users
Enable 3-D feature #1
Enable 3-D feature #2
Etc.

Fig. 5

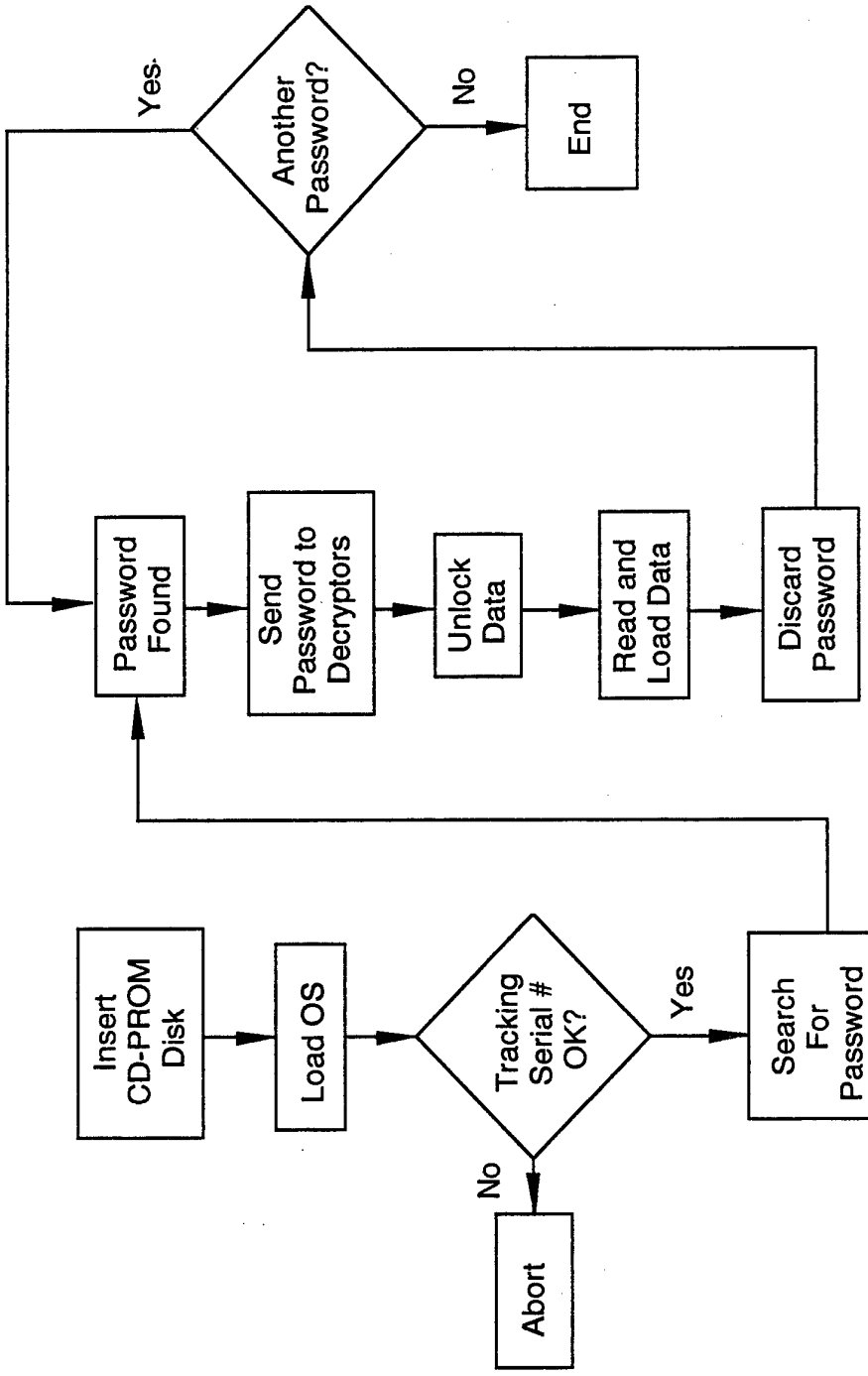

Insert CD-PROM Disk
Load OS
Tracking Serial # OK?
No
Abort
Yes
Search For Password
Password Found
Send Password to Decryptors
Unlock Data
Read and Load Data
Discard Password
Another Password?
Yes
No
End

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/08322

A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) :Please See Extra Sheet.
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/3, 4, 23, 24,25, 49, 50
360/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US, A, 4,695,993 (TAKAGI ET AL.) 22 SEPTEMBER 1987, see column 5 and laser 19	6 and 8-9 --- 1-5, 7 and 10
Y --- A	US, A, 4,644,493 (CHANDRA ET AL.) 17 FEBRUARY 1987, see columns 6-7	1-5, 7 and 10 --- 6 and 8-9
A	WO, A, 88/02202 (KATZNELSON) 24 MARCH 1988	1-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
15 SEPTEMBER 1994

Date of mailing of the international search report
30 SEP 1994

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
TOD R. SWANN
Telephone No. (703) 308-0475

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/08322

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (5):

H04K 1/00

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

380/25