(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 669 580 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
10.06.1998 Bulletin 1998/24

(51) Int Cl.[6]: **G06F 12/14**, G06F 1/00, G06D 1/00

(21) Application number: **95102120.3**

(22) Date of filing: **16.02.1995**

(54) **Data security apparatus**

Gerät zur Sicherung von Daten

Appareil de sécurité de données

(84) Designated Contracting States:
DE ES FR GB IT

(30) Priority: **28.02.1994 JP 30590/94**

(43) Date of publication of application:
30.08.1995 Bulletin 1995/35

(73) Proprietor: **SEGA ENTERPRISES, LTD.**
Tokyo 144 (JP)

(72) Inventors:
- **Ohba, Toshihiro, c/o Sega Enterprises, Ltd.**
Tokyo (JP)
- **Asai, Toshinori, c/o Sega Enterprises, Ltd.**
Tokyo (JP)

(74) Representative: **Eisenführ, Speiser & Partner**
Martinistrasse 24
28195 Bremen (DE)

(56) References cited:
EP-A- 0 449 242
WO-A-91/03011
US-A- 4 937 864

EP 0 669 580 B1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a data security apparatus for providing protection of the contents of a ROM storing, e.g., game program data against any illegal execution, copy or analysis.

Description of the Related Arts

Early simple video game machines allowed users to play only a single video game realized by game program data stored in a memory fixedly arranged within the machine body. However, recently developed and widespread game machines tend to include a removable ROM which has stored game program data so that the users can play variously different games merely by replacing the ROM with another. Such a ROM can be of a cartridge type like a ROM cartridge in which a dedicated circuit is enclosed in a small case, or alternatively be in the form of a CD-ROM using an optical storage medium, which are fully utilized depending on their respective advantages.

The ROM cartridge or CD-ROM storing an extremely popular game program may be often marketed at a high price since the supply is unlikely to catch up with the demand for that article. For this reason, a case just goes on and on where the contents of the ROM are unlawfully copied and put on the market. Furthermore, in the case of arcade game machines in game centers, a ROM board composed of a circuit overlying a substrate is used as the game program storage ROM. Due to its removability from the machine body, such a ROM board may also be possibly subjected to a risk that the contents thereof are copied and stolen for business use.

In order to deal with this, typical ROM data undergo an analysis or copy limitation processing, while simultaneously the game machine is provided with a data security device for limiting the execution of a game program stored in the ROM which has not undergone that processing. Description will now be given of such a data security device, by way of example, fitted to a game machine for CD-ROM's.

First of all, data stored in a commonly marketed CD-ROM (hereinafter referred to as a commercial CD) have the following configuration. In a commercial CD 18, as shown in Fig. 7, game program data 18d are stored with the insertion of a special code 18a not permitting any analysis or copy without using a dedicated apparatus.

A computer of a commercial game machine, on the other hand, is equipped with a security check means for checking the presence or absence of the special code 18a in the commercial CD 18 to permit only a program with the special code 18a to be executed. Thus, as long as it is a regular commercial CD 18 with the special code 18d inserted therein, the execution of its program data 18d is permitted by the security check means so that the game program data 18d can be executed by use of the normal commercial game machine. Even though a commercial CD 18 includes illegally copied program data 18d, the special code 18a is not permitted to be copied onto the CD, and hence an attempt to execute the program data 18d within in the CD by a commercial game machine will be in vain due to the presence of the security check means.

Nevertheless, the conventional data security apparatus as described above involves the following problems. Although the contents of game program data are to be securely protected from any illegal copy, analysis or execution by persons not having a legitimate title, it is convenient for a regular developer of the game program (namely a person having the legitimate title) to ensure an easy execution of the contents since he must check at all times how the created game is executed. A machine used for the check is preferably a commercial one identical in type to the machines actually manipulated by users, rather than a dedicated one which would require an additional cost for fabrication. Also in terms of checking whether the game can be played with a pleasure from the users viewpoint, it is desirable to perform the check with a commercial game machine.

As described hereinabove, however, the commercial game machine is typically fitted with the security check means for checking the presence or absence of a special code, with the result that the machine will not permit the execution of a game program without a special code under development. Moreover, the special code has an extremely complicated configuration so as to prohibit any analysis or copy, and hence will take significant time and labor to create. Accordingly, creation of a further special code, if needed each time a new game software is developed, might possibly delay the development of game programs.

WO-A-9103011 representing the closest prior art from which the invention proceeds discloses an electronic semiconductor memory system which has a normal PROM type application program storage replaced by a chip requiring accessing at least in part in a coded manner different from normal access sequencing in order correctly to extract check or identifier information. Further use of the memory system will be denied for other than correct extraction of the check or identifier information, and the memory system itself can be disabled by hard logic and a fuse should an order of abstraction be attempted other than the coded manner. An EEPROM with flags is used to enable access.

From EP-A-0 389 184, it is known an electronic information processing method and device, wherein an electronic information input via an input means is divided into first and second groups e.g. representing information which may not be modified except by a skilled operator, and information which may be modified freely. If a request for modification of one of the information

elements is input via the input means, a judging means determines, on the basis of controlling information in a controlling information area, whether the information element belongs to the first or second group. If it belongs to the first, a display means displays one of the display elements as e.g. a warning to the operator that the information element may be modified only by a skilled operator. A password system may be provided to identify such a skilled operator.

After password checking, the information of the operator is stored to bypass the capability test when that operator next attempts to modify the information.

In a method and structure for providing computer security and virus prevention according to EP-A-0 449 242, an uniquely formatted floppy diskette is used as an access diskette and serves as a hardware key to gain access.

US-A-4 937 864 discloses a debug routine accessing system using special keys in the form of floppy disks for unlocking debug routines embedded in the operating software of a reproduction machine, each debug routine having a key number, with the floppy disks having various key numbers for different ones of the debug routines so that on insertion of a selected disk in the machine floppy disk port, the key number is read from the disk and compared with the key numbers of the various debug routines until a match is found enabling the debug routine represented by the key number to be accessed.

SUMMARY OF THE INVENTION

The present invention was conceived to solve the problems involved in the prior art as described above. It is therefore the object of the present invention to provide a data security apparatus ensuring a secure prevention of illegal execution, analysis, or copy of the data by a person having no legitimate title, while simultaneously facilitating the execution of the data by a legitimately entitled person.

In order to achieve the above object, according to the present invention as defined in claim 1, there is provided a data security apparatus inteded to be provided in a data processor for processing main data, said apparatus including an input means for inputting the main data from a removable storage medium, a data execution means for executing the main data input through said input means, a main data readout means and a security check means for checking the presence or absence of a special code on said removable main data storage medium and for permitting said readout means to read out only the main data by said input means when the checking has verified the presence of the special code, said data security apparatus being characterized by a release means responsive to data being input through said input means from a first removable storage medium for detecting that said first removable storage medium is a release storage medium, and means, upon said detection, for releasing said readout means to permit said readout means to read the main data of a subsequently introduced second removable data storage medium without checking the presence of said special code.

Further advantageous embodiments are defined in the dependent claims.

In the apparatus of the invention as defined in claim 1, upon inputting main data through the input means from the main data storage medium, the release means release the read out means control function of the security check means. Then, if the main data are input through the input means from the main data storage medium, the read out means will read out the main data which is in turn transferred to the execution means. As a result, by previously inputting the release data, it is possible to execute even main data not subjected to a predetermined processing.

Further, the main data storage is removably provided in the data processor so as to allow an extensive utilization by the user. In case the main data in such storage medium are once not subjected to a predetermined processing due to the circumstances such as, for example, a legal copy by a person having no legitimate title, the read out means control function of the security check means works to prevent the data from being unlawfully executed.

On the contrary, the release data storage medium is removably provided in the data processor, and hence only the legitimately entitled person is permitted to execute the trial data as long as the person having the legitimate title secretly holds the release data storage medium. This means that by loading the release data storage medium into the data processor, there can be released the read out means control function of the security check means. Thus, if after such release, the data processor is loaded with the main data storage medium not subjected to a predetermined processing due to the circumstances, for example, that it is under trial manufacture, the main data can be put into execution.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of the present invention will become more apparent from the following description in conjunction with the accompanying drawings, in which:

Fig. 1 is an explanatory diagram showing a data configuration in a trial CD for use in an embodiment of the present invention;

Fig. 2 is an explanatory diagram showing a data configuration in a KEY-CD for use in an embodiment of the present invention;

Fig. 3 is a block diagram depicting a configuration of an embodiment of the present invention;

Fig. 4 is an explanatory diagram depicting the contents of a flag storage means in the Fig. 3 embodiment;

Fig. 5 is a circuit block diagram in the Fig. 3 embodiment;

Fig. 6 is a flowchart illustrating a procedure of the processing in Fig. 3 embodiment; and

Fig. 7 is an explanatory diagram illustrating a data configuration of a commercial CD.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

1. Embodiment

An embodiment of the present invention defined in claims 1 through 6 will now be described with reference to the drawings. A readout means in claim 1 can be a program data readout means; release data KEY-CD data; a storage medium for main data a trial CD or a commercial CD; and a storage medium for release data a KEY-CD. ID data in claim 3 can be KEY-ID and DISC-ID, while a flag in claim 4 a security flag. A predetermined processing applied to main data in claim 1 means an action of inserting a special code into the same CD.

An apparatus of this embodiment is intended to be implemented on a computer of a video game machine, and a set of functions of the apparatus can be implemented by operating the computer using a predetermined procedure represented in the form of a program. It is however to be appreciated that all or part of the functions of the apparatus may be implemented on a dedicated electronic circuit. A set of functions of the apparatus will be described hereinbelow with reference to a block diagram represented in terms of means as well as a virtual circuit block diagram depicting a hardware configuration. It is to be noted that a circuit of the game machine serving as a game implementation means in this embodiment is configured in accordance with the prior art techniques, and hence the description thereof will be omitted.

1-1. Configuration

A configuration of this embodiment will now be explained in detail. First, explanation will be given of a data configuration within a CD-ROM in the process of trial manufacture (hereinafter referred to as a trial CD 1). Referring to Fig. 1, the trial CD 1 is shown including game program data 1d together with an identifier DISC-ID 1b differing depending on the manufacturer. For the purpose of saving time and labor required for the manufacture and improving the working efficiency, the trial CD includes no special codes. In order to enable such a trial CD 1 without a special code to execute a program, in this embodiment, another CD-ROM (hereinafter referred as a KEY-CD 2) different from the trial CD 1 is used. That is, the KEY-CD 2 is first set into a CD drive of the game machine so that the data in the KEY-CD 2 are read out to thereby allow the function of a security check means to be released. Afterwards, the KEY-CD 2 within the CD drive is replaced with the trial CD 1 of which data are in turn read out.

Then, description will be given of a data configuration within the KEY-CD 2 used for such release of the function of the security check means. Referring to Fig. 2, the KEY-CD 2 is shown including a special code 2a not permitting any analysis or copy without using a dedicated apparatus. The special code 2a is data in response to which input the security check means provided in a commercial game machine will permit the readout of a game program in the same manner as in the conventional example. Within the KEY-CD 2 is also stored an identifier KEY-ID 2b differing depending on the manufacturer of the game program. The identifiers KEY-ID 2b and DISC-ID 1b of the same manufacturer are correspondent with each other. Within the KEY-CD 2 is further stored KEY-CD data 2c serving to release the security check means' function for checking the presence or absence of a special code. The KEY-CD 2 may store additional program data 2d.

On the contrary, a security section 3 provided in the game machine is configured as follows. As shown in Fig. 3, an input means 4 for inputting information stored in the CD-ROM is connected via a security check means 5 to a program data readout means 6. The security check means 5 serves a function to check the presence or absence of a special code within the CD to control the readout of program data by the program data readout means 6. The program data readout means 6 is coupled to a game implementation means 11. The program data readout means 6 serves to read out program data stored in the CD to provide as its output to the game implementation means 11.

The security check means 5 is further coupled to an ID detection means 8 for detecting the identifiers DISC-ID 1b AND KEY-ID 2b contained in the CD. The ID detection means 8 is coupled to an ID storage means 9 for storing the KEY-ID 2b detected. The ID detection means 8 is coupled to an ID collation means 10 for collating the DISC-ID 1b detected with the KEY-ID 2b stored in the ID storage means 9, the ID collation means in turn being coupled to the program data readout means 6.

A flag storage means 7 is coupled to the security check means 5. As shown in Fig. 4, the flag storage means 7 stores a security flag 7a and a readout enabling flag 7b. A flag refers herein to an indicator for controlling a switch point on a program. The security flag 7a, when it is on, allows the special code check function of the security check means 5 to be in ready state. The readout enable flag 7b, when it is on, allows the program data readout function of the program data readout means 6 to be in ready state. It will be noted that the following setting is previously made in accordance with a predetermined program so as to ensure the execution of a procedure indicated in Operation which will be descried later. Immediately after energizing the game machine body, the security flag 7a and the readout enabling flag 7b are respectively set to be on and off, whereas once

the identifier KEY-ID 2b is stored into the ID storage means, the security flag 7a and the readout enabling flag 7b result in off and on, respectively, by virtue of the KEY-CD data 2c. In addition, when the identifiers KEY-ID 2b and DISC-ED1b have been coincident with each other as a result of collation, the readout enabling flag 7b is set to become on.

Description will now be given of a simplified diagram of a hardware configuration in accordance with this embodiment. Referring to Fig. 5, used as the input means 4 is a CD-ROM drive (hereinafter referred to as a CD drive 12). The CD drive 12 is coupled to a CD drive control circuit 13 for implementing the program data readout means 6. The CD drive control circuit 13 is connected through a CD data buffer 14 to a game machine circuit 15 acting as the game implementation means 11.
With the CD drive circuit 13 is coupled a security circuit 16 for implementing the security check means 5, the ID detection means 8 and the ID collation means 10. With the security circuit 16 is coupled a memory 17 for implementing the flag storage means 7 and the ID storage means 9.

1-2. Operation

Operation of this embodiment having the above configuration will now be described with reference to a flowchart of Fig. 6 depicting a procedure. First of all, the power is turned on (step 501). Then, the security flag 7a becomes on (step 502) and the readout enabling flag 7b becomes off (step 503). Then, when the user sets the KEY-CD 2 into the CD drive 12, the security flag 7a is checked by the security check means 5 (step 504). Since the security flag 7a is on in this case, control advances to step 505 in which the security check means 5 checks whether the special code 2a is present or not. Since the set KEY-CD 2 includes the special code 2a, control advances to step 506 in which the ID detection means judges whether the set CD is the KEY-CD 2 or not. The set CD is judged to be the KEY-CD 2 when both the judgment of the presence or absence of the special code 2a in step 505 and the detection (judgment of the presence or absence) of the KEY-ID 2b by the ID detection means 8 are positive. Upon detecting the KEY-ID 2b from the KEY-CD 2 in this manner, the thus detected KEY-ID 2b is stored in the ID storage means 9 (step 507). After the storage of the KEY-ID 2b into the ID storage means 9, the KEY-CD data 2c will cause the security flag 7a to be off (step 508) and then the readout enabling flag 7b on (step 509).

Then, when the user replaces the KEY-CD 2 within the CD drive 12 with the trial CD 1, the replacement of the CD is detected in step 510, followed by the return to the step 503 to repeat the subsequent processing. Since in this case the security flag 7a has already become off in the step 508, control jumps from the step 504 to step 514. At that time, the DISC-ID 1b within the trial CD 1 is detected by the ID detection means 8. By the ID collation means 10, the thus detected DISC-ID 1b is collated with the KEY-ID 2b stored in the ID storage means 9 (step 514). If the DISC-ID 1b and the KEY-ID 2b coincide with each other due to the ID's from the same source (step 515), control advances to step 516 step in which the readout enabling flag 7b is allowed to become on.

Thereafter, the trial CD 1 remains unchangedly set in the CD drive 12, and hence it is judged in the step 510 that no CD change has taken place, resulting in the advancement to step 511. In step 511, if the program data readout means 6 has received a readout command derived from a predetermined program, then control advances to step 512, whereas if not, it returns to step 510. After the reception of the command, it is checked in step 512 whether the readout enabling flag 7b is on or not. Since in the step 516 the readout enabling flag 7b results in on as long as the DISC-ID 1b of the trial CD 1 is coincident with the KEY-ID 2b of the KEY-CD 2, control advances to step 513. Through the above procedure, the program data 1a within the trial CD 1 are allowed to be read out by the program data readout means 6 (step 513), whereby the game program is output to the game machine circuit 15 to implement the game.

If in the step 515 the DISC-ID 1b of the trial CD 1 is not coincident with the KEY-ID 2b of the KEY-CD 2, then control returns to the step 505. At that time, since the trial CD 1 includes no special codes, control jumps to the step 510, leaving the readout enabling flag 7b off. Then, in the step 512 the readout enabling flag 7b is judged to be off, causing control to return to 510. Thus, the readout of the program data 1d is prohibited until the trial CD 1 having the DISC-ID 1b coincident with the KEY-ID 2b is set into the CD drive 12.

It is to be appreciated that this embodiment will naturally allow the commercial CD 18 to be set for the implementation of a game in the same manner as in the conventional example. The following is a procedure needed to implement the game by setting the commercial CD 18 into the CD drive 12. Due to the fact that the commercial CD 18 inherently includes the special code 18a, control passes through the steps 501 to 505 in the same manner as the above example. Then, it is judged in the step 506 the commercial CD 18 set into the CD drive 12 is not the KEY-CD due to the lack of the KEY-ID, and hence control jumps to the step 509 causing the readout enabling flag 7b to be on. The subsequent procedure is substantially the same as the case of the above trial CD 1. Since the readout enabling flag 7b results in on in the step 509 as described above, the readout of the program data 18d can be performed through the steps 510 to 513.

In case of an illegally copied CD-ROM (hereinafter referred to as an illegal copy CD), the readout of the program data is restricted under the following procedure. Above all, the illegal copy CD has no special codes inserted therein. Even if such illegal copy CD is set into the CD drive 12, the procedure from the step 501 to the step 504 will be executed in the same manner as the

above example. However, it is judged in the step 505 whether the special code is present or not, resulting in the jump to step 510 due to the lack of the special code. The subsequent procedure is the same as the case of the trial CD until it is checked in the step 512 that the readout enabling flag 7b remains off. In consequence, the readout of the program data is not permitted.

1-3. Effect

The effect of this embodiment as described hereinbefore is as follows. The provision of this embodiment into the commercial game machine will ensure that the special code check function of the security check means 5 is switched off by use of the KEY-CD 2, whereupon the game can be executed regardless of the trial CD 1 having no special codes. Accordingly, in the process of the development of a game software, an experimentally created game can be readily executed using the commercial game machine to test or confirm the game, thereby ensuring an effective and smooth development.

Also, due to the lack of the special code, the illegal copy CD is not permitted to implement the game on the commercial game machine without using KEY-CD 2, thereby preserving the security of the game program.

Alternatively, the release means may be implemented by a mechanical switch. However, the implementation thereof by flag on and off which is a programming technique will ensure an easier change in setting.

Furthermore, unless the KEY-ID 2b stored in the KEY-CD 2 is coincident with the DISC-ID 1b in the trial CD 1, the game is not permitted to be put into execution. Accordingly, if respective development manufacturers or respective developers have an individually different KEY-CD 2, it is impossible to use the KEY-CD 2 as a master key capable of reading every CD's, thereby highly increasing the security.

Also, a single KEY-CD 2 conveniently stores both the KEY-CD data 2c for releasing the function of the security check means 5 and the KEY-ID 2b for ID collation, which will contribute to the time-saving input of the KEY-CD data 2c and the KEY-ID 2b. In addition, a single trial CD 1 advantageously stores both the game program data 1D and the DISC-ID 1b, which will eliminate the necessity to separately input the DISC-ID 1b and the program data 1d. This will ensure an easy and prompt check of the trial CD 1 by the developer as well as an improved efficiency of the game development.

2. Other Embodiments

It is to be construed that the present invention is not limited to the above-described embodiment, and the connection, arrangement, setting, etc., of each function block may be appropriately modified. For instance, the program data 2d does not necessarily need to be provided within the KEY-CD 2. To further increase a reliability of security, a plurality of DISC-ID's 1b and a plurality of KEY-ID's 2b may be respectively provided within the trial CD 1 and the KEY-CD 2 so that the program data are not to be read out without coincidence of all the ID's.

In the case of requiring only the security based on the special code, a setting may be employed in which no use is made of the above-described DISC-ID 1b and the KEY-ID 2b. In this case, there is no need to store the ID's within the CD-ROM's and to provide the game machine with the ID detection means 8, whereupon the KEY-CD 2 can be used as if a so-called master key.

Further, the data security apparatus of the present invention is applicable not only to the game machines but also to ordinary computers. Therefore, besides the CD-ROM the storage medium can be, for instance, a ROM cartridge, a ROM board, a floppy disk, a RAM card, a magnetic tape, a magneto-optic disc. Also, other than the CD drive 12 the input means 4 can be, for instance, a floppy disc drive, a RAM card drive, a magnetic tape drive, an optical disc drive, or a magnetic disc drive.

The storage means such as the flag storage means 7 and ID storage means 9 can be implemented in a free manner, for instance, may be implemented on a main memory or on an external memory. Alternatively, a CPU register or a cash memory is also available. The memories 17 to implement thereon the flag storage means 7 and the ID storage means 9 may be the same or different in type.

In addition to the flag on/off implementation, the release means can be implemented using other programming techniques or using the mechanical switch as described earlier.

Moreover, it is also possible for the steps constituting each procedure in this embodiment to change the sequence of execution, or to perform a simultaneous execution of a set of steps, or to execute the set of steps in different sequence, insofar as it is allowable in the light of their natures.

3. Effect of the Invention

According to the present invention as described hereinabove, a release means is provided for temporarily releasing the function of the security check means, to thereby propose a data security apparatus capable of securely preventing data stored in a storage medium from being illegally executed, analyzed, or copied by a person not having a legitimate title, while simultaneously facilitating the execution of the data by a person having the legitimate title.

Claims

1. A data security apparatus (3) intended to be provided in a data processor for processing main data (1d, 2d, 18d), said apparatus including

an input means (4, 12) for inputting the main data from a removable storage medium (1, 2,18),
a data execution means (11, 13, 15) for executing the main data (1d, 2d, 18d) input through said input means (4, 12),
a main data readout means (6), and
a security check means (5, 16) for checking (505) the presence or absence of a special code (18a) on said removable main data storage medium (18) and for permitting said readout means (6) to read out only the main data (1d, 18d) by said input means (4, 12) when the checking has verified the presence of the special code (18a),

said data security apparatus being characterized by:

a release means responsive to data being input through said input means (4, 12) from a first removable storage medium (2) for detecting (505, 506) that said first removable storage medium (2) is a release storage medium, and
means, upon said detection, for releasing (504, 514-516) said readout means (6) to permit said readout means (6) to read the main data (1d) of a subsequently introduced second removable data storage medium (1) without checking the presence of said special code (18a).

2. A data security apparatus according to claim 1, wherein
said main data storage medium (1) and said release data storage medium (2) store coincident or unco-incident ID data,
said apparatus further comprising:

an ID detection means (8) for detecting ID data (1b, 2b) input through said input means (4, 12),
an ID storage means (9) for storing the ID data (1b, 2b) detected by said ID detection means (8), and
an ID collation means (10) for allowing said main data readout means (6) to readout the main data (1d) from said subsequently introduced second data storage medium (1) only when the ID data (1b) stored in said data storage medium (1) are coincident with the ID data (2b) stored in said release data storage medium (2).

3. A data security apparatus according to claim 2 wherein

said main data (1b, 18b) are game program data, and wherein
said data processor is a game machine having a computer, and wherein
said release means, said flag storage means (7), said ID detection means (8), said ID storage means (9) and said ID collation means (10) are implemented on said computer of said game machine.

4. A data security apparatus according to anyone of the preceeding claims, wherein
said release means includes a flag storage means (7) for storing a flag for controlling an actuation of the function of said security check means (5, 16).

5. A data security apparatus according to anyone of the preceeding claims, wherein

said data storage medium (1) and said release data storage medium (2) are each a CD-ROM, and
said input means comprises a CD-ROM drive (12).

Patentansprüche

1. Datensicherheitsvorrichtung (3), welche vorgesehen ist, um in einem Datenprozessor zur Verarbeitung von Hauptdaten (1d, 2d, 18d) bereitgestellt zu werden, wobei die Vorrichtung beinhaltet:

eine Eingabeeinrichtung (4, 12) zum Eingeben der Hauptdaten von einem entnehmbaren Speichermedium (1, 2, 18),
eine Datenausführungseinrichtung (11, 13, 15) zum Ausführen der Hauptdaten (1d, 2d, 18d), welche durch die Eingabeeinrichtung (4, 12) eingegeben werden,
eine Hauptdaten-Ausleseeinrichtung (6) und

eine Sicherheitsprüfeinrichtung (5, 16) zum Prüfen (505) des Vorhandenseins oder Nichtvorhandenseins eines besonderen Kodes (18a) auf dem entnehmbaren Hauptdaten-Speichermedium (18), und um der Ausleseeinrichtung (6) zu erlauben, die Hauptdaten (1d, 18d) durch die Eingabeeinrichtung (4, 12) nur dann auszulesen, wenn die Prüfung das Vorhandensein des besonderen Kodes (18a) verifiziert hat, wobei die Daten-Sicherheitsvorrichtung gekennzeichnet ist durch:

eine Freigabeeinrichtung, welche auf Daten reagiert, die durch die Eingabeeinrichtung (4, 12) von einem ersten entnehmbaren Speichermedium (2) eingegeben werden, zum Erfassen (505, 506), daß das erste entnehmbare Speichermedium (2) ein Freigabe-Speichermedium ist, und
eine Einrichtung zum Freigeben (504, 514-516)

der Ausleseeinrichtung (6) nach der Erfassung, um der Ausleseeinrichtung (6) zu erlauben, die Hauptdaten (1d) eines anschließend eingefügten zweiten entnehmbaren Datenspeichermediums (1) zu lesen, ohne das Vorhandensein des besonderen Kodes (18a) zu prüfen.

2. Daten-Sicherheitsvorrichtung nach Anspruch 1, bei welcher das Hauptdatenspeichermedium (1) und das Freigabe-Datenspeichermedium (2) übereinstimmende oder nicht übereinstimmende ID-Daten speichern, wobei die Vorrichtung weiterhin umfaßt:

eine ID-Erfassungseinrichtung (8) zum Erfassen von ID-Daten (1b, 2b), welche durch die Eingabeeinrichtung (4, 12) eingegeben werden,
eine ID-Speichereinrichtung (9) zum Speichern der ID-Daten (1b, 2b), welche durch die ID-Erfassungseinrichtung (8) erfaßt werden, und
eine ID-Zusammentragungseinrichtung (10), um der Hauptdaten-Ausleseeinrichtung (6) zu erlauben, die Hauptdaten (1d) von dem anschließend eingeführten zweiten Datenspeichermedium (1) nur dann auszulesen, wenn die ID-Daten (1b), welche auf dem Datenspeichermedium (1) gespeichert sind, mit den ID-Daten (2b) übereinstimmen, welche in dem Freigabe-Datenspeichermedium (2) gespeichert sind.

3. Datensicherheitsvorrichtung nach Anspruch 2, bei welcher die Hauptdaten (1b, 18b) Spielprogrammdaten sind, und wobei der Datenprozessor ein Spielgerät mit einem Computer ist und wobei die Freigabeeinrichtung, die Flag-Speichereinrichtung (7), die ID-Erfassungseinrichtung (8), die ID-Speichereinrichtung (9) und die ID-Zusammentragungseinrichtung (10) in dem Computer des Spielgerätes implementiert sind.

4. Datensicherheitsvorrichtung nach einem der vorstehenden Ansprüche, bei welcher die Freigabeeinrichtung eine Flag-Speichereinrichtung (7) zum Speichern eines Flags zum Steuern einer Wirkung der Funktion der Sicherheits-Prüfeinrichtung (5, 16) beinhaltet.

5. Datensicherheitsvorrichtung nach einem der vorstehenden Ansprüche,

bei welcher das Datenspeichermedium (1) und das Freigabe-Datenspeichermedium (2) jeweils eine CD-ROM sind, und
die Eingabeeinrichtung ein CD-ROM-Laufwerk (12) umfaßt.

Revendications

1. Appareil de sécurité de données (3) prévu pour être inséré dans un processeur de données afin de traiter des données principales (1d, 2d, 18d), ledit appareil comprenant

des moyens d'entrée (4, 12) afin d'entrer les données principales depuis un support de stockage amovible (1, 2, 18),
des moyens d'exécution de données (11, 13, 15) afin d'exécuter les données principales (1d, 2d, 18d) entrées par l'intermédiaire desdits moyens d'entrée (4, 12),
des moyens de lecture de données (6) principales, et
des moyens de vérification de la sécurité (5, 16) pour vérifier (505) la présence ou l'absence d'un code spécial (18a) sur ledit support de stockage de données principales amovible (18) et pour permettre auxdits moyens de lecture (6) de ne lire que les données principales (1d, 18d) par lesdits moyens d'entrée (4, 12) lorsque la vérification a confirmé la présence du code spécial (18a),

ledit appareil de sécurité de données étant caractérisé par :

des moyens de libération sensibles aux données entrées par l'intermédiaire desdits moyens d'entrée (4, 12) depuis un premier support de stockage (2) amovible afin de détecter (505, 506) que ledit premier support de stockage (2) amovible est un support de stockage à libération, et
des moyens, lors de ladite détection, destinés à libérer (504, 514-516) lesdits moyens de lecture (6) afin de permettre auxdits moyens de lecture (6) de lire les données principales (1d) d'un support de stockage de données (1) amovible introduit ultérieurement sans vérifier la présence dudit code spécial (18a).

2. Appareil de sécurité de données selon la revendication 1. dans lequel ledit support de stockage (1) de données principales et ledit support de stockage (2) de données à libération stockent des données d'identification coïncidant ou non,
ledit appareil comprenant en outre :

des moyens de détection d'identification (8) pour détecter des données d'identification (1b, 2b) entrées par l'intermédiaire desdits moyens d'entrée (4, 12),
des moyens de stockage d'identification (9) pour stocker les données d'identification (1b, 2b) détectées par lesdits moyens de détection

d'identification (8) et,
des moyens de classement d'identification (10) pour permettre auxdits moyens de lecture (6) de données principales de lire les données principales (1d) depuis ledit second support de stockage de données (1) introduit ultérieurement seulement lorsque les données d'identification (1b) stockées dans ledit support de stockage de données (1) coïncident avec les données d'identification (2b) stockées dans ledit support de stockage de données (2) à libération.

3. Appareil de sécurité de données selon la revendication 2, dans lequel

lesdites données principales (1b, 18b) sont des données de programme de jeu, et dans lequel ledit processeur de données est une console de jeux ayant un ordinateur, et dans lequel lesdits moyens de libération, lesdits moyens de stockage d'indicateur (7), lesdits moyens de détection d'identification (8), lesdits moyens de stockage d'identification (9) et lesdits moyens de classement d'identification (10) sont mis en oeuvre sur ledit ordinateur de ladite console de jeux.

4. Appareil de sécurité de données selon l'une quelconque des revendications précédentes, dans lequel

lesdits moyens de libération comprennent des moyens de stockage d'indicateur (7) afin de stocker un indicateur pour contrôler l'activation de la fonction desdits moyens de vérification de la sécurité (5, 16).

5. Appareil de sécurité de données selon l'une quelconque des revendications précédentes, dans lequel

ledit support de stockage de données (1) et ledit support de stockage de données (2) à libération sont chacun un CD-ROM, et
lesdits moyens d'entrée comprennent un lecteur de CD-ROM (12).

FIG. 1

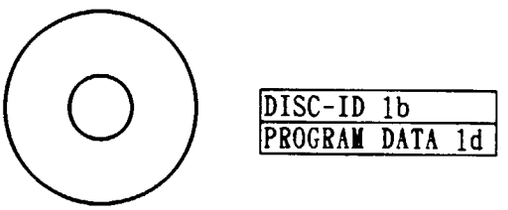

DISC-ID 1b
PROGRAM DATA 1d
TRIAL CD 1

FIG. 2

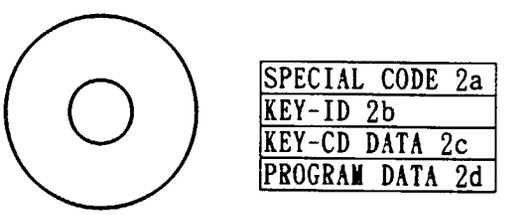

SPECIAL CODE 2a
KEY-ID 2b
KEY-CD DATA 2c
PROGRAM DATA 2d
KEY-CD 2

FIG. 3

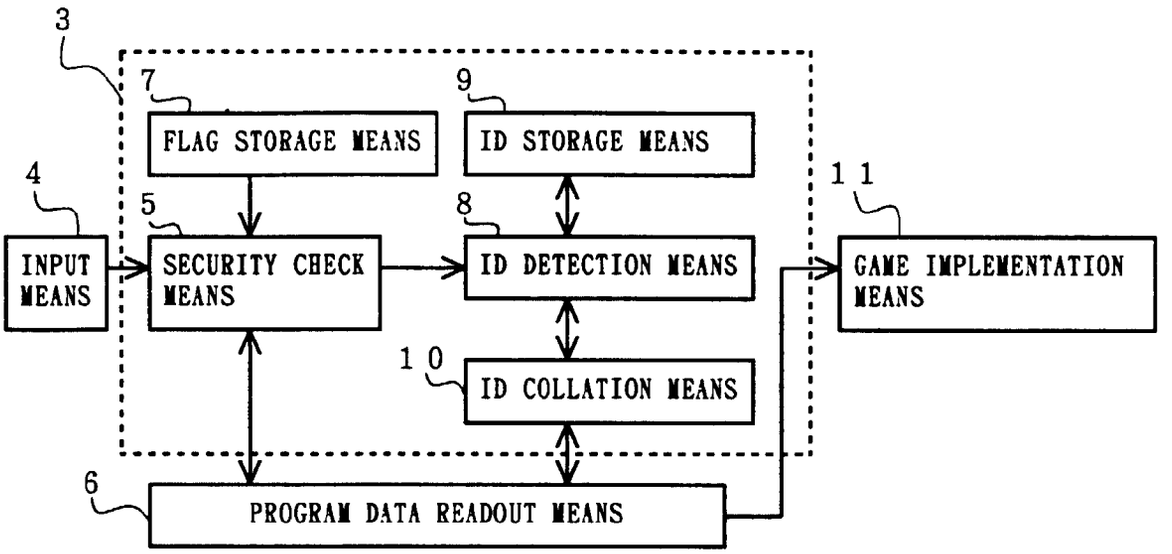


FIG. 4

FLAG STORAGE MEANS 7

SECURITY FLAG 7a
READOUT ENABLING FLAG 7b

FIG. 5

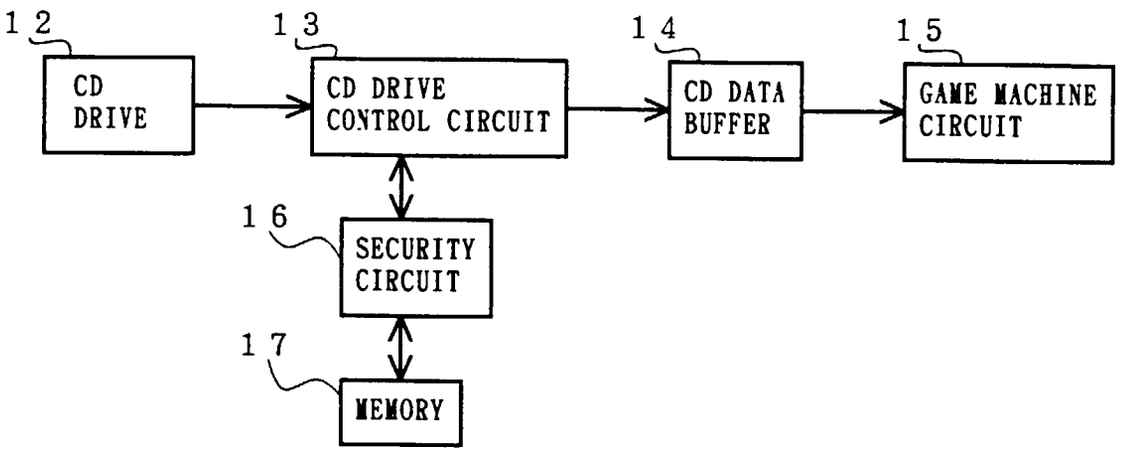
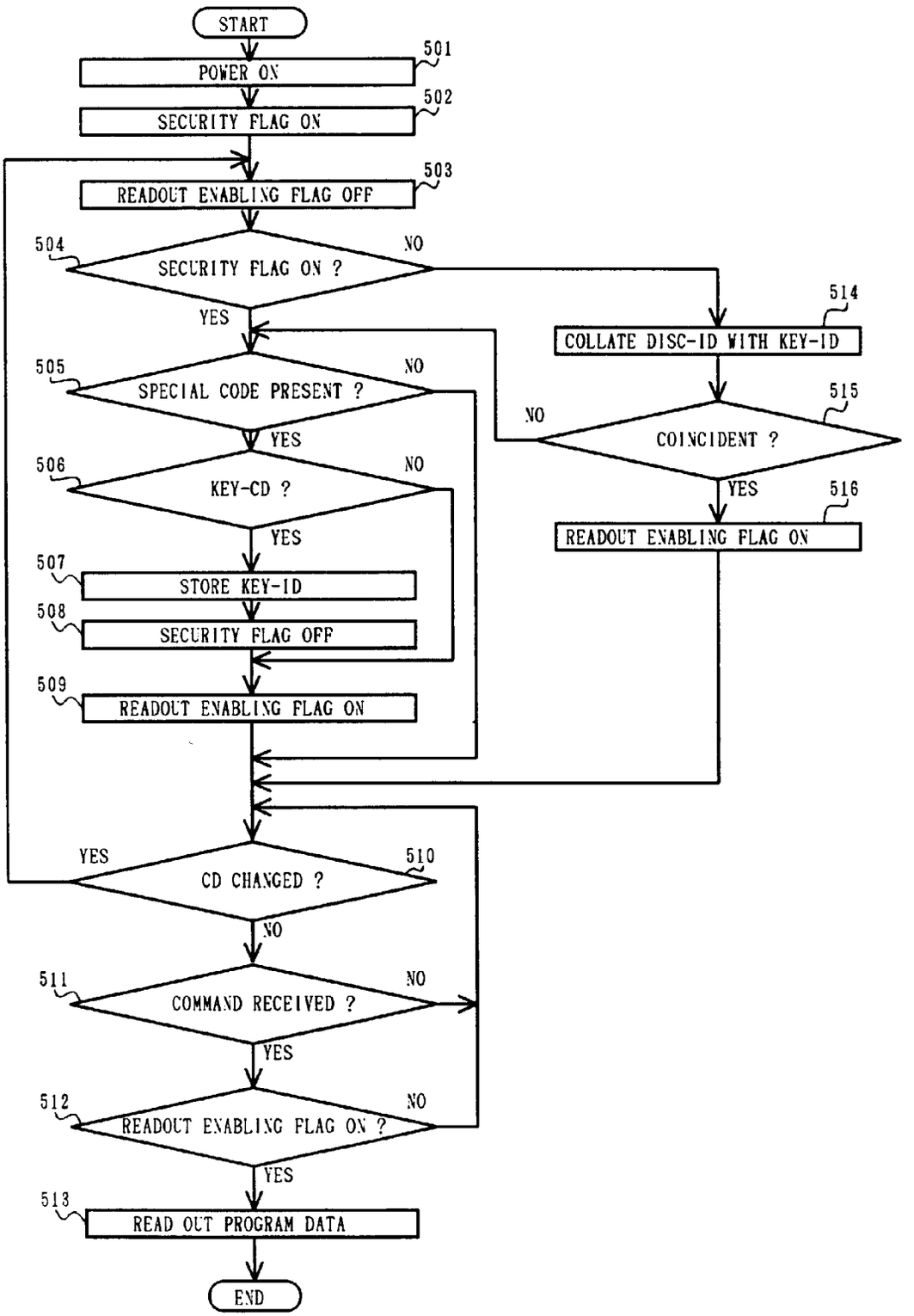
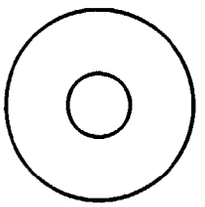

12
CD DRIVE
13
CD DRIVE CONTROL CIRCUIT
14
CD DATA BUFFER
15
GAME MACHINE CIRCUIT
16
SECURITY CIRCUIT
17
MEMORY

FIG. 6


START
POWER ON
501
SECURITY FLAG ON
502
READOUT ENABLING FLAG OFF
503
SECURITY FLAG ON ?
504
NO
YES
SPECIAL CODE PRESENT ?
505
NO
YES
KEY-CD ?
506
NO
YES
STORE KEY-ID
507
SECURITY FLAG OFF
508
READOUT ENABLING FLAG ON
509
COLLATE DISC-ID WITH KEY-ID
514
COINCIDENT ?
515
NO
YES
READOUT ENABLING FLAG ON
516
CD CHANGED ?
510
YES
NO
COMMAND RECEIVED ?
511
NO
YES
READOUT ENABLING FLAG ON ?
512
NO
YES
READ OUT PROGRAM DATA
513
END

F I G. 7



COMMERCIAL CD 18