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

(11) EP 0 447 043 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
23.08.2000 Bulletin 2000/34

(21) Application number: **91301379.3**

(22) Date of filing: **21.02.1991**

(51) Int. Cl.^{7}: **G06F 1/00**, A61K 31/12, A61K 31/345, A61K 31/38, A61K 31/44, A61K 31/47, A61K 31/19, A61K 31/275, C07C 205/45, C07C 317/24 // C07C49/217, C07C49/235, C07C49/248, C07C49/255, C07C49/258, C07C49/567, C07C49/577, C07C65/36, C07C65/40, C07C233/31, C07C235/84, C07C255/56, C07C309/73, C07C309/66, C07C65/38, C07D307/71, C07D333/44, C07D213/50, C07D215/14

(54) **Security system for software**
Softwaresicherheitssystem
Système de sûreté de logiciel

(84) Designated Contracting States:
DE FR GB IT

(30) Priority: **16.03.1990 JP 6563290**

(43) Date of publication of application:
18.09.1991 Bulletin 1991/38

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

(72) Inventor: **Matsubara, Taku**
Ota-ku, Tokyo, 144 (JP)

(74) Representative:
Lloyd, Patrick Alexander Desmond et al
Reddie & Grose
16 Theobalds Road
London WC1X 8PL (GB)

(56) References cited:

EP-A- 0 048 586	**EP-A- 0 080 244**
EP-A- 0 206 704	**US-A- 4 454 594**

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

BACKGROUND OF THE INVENTION

[0001] This invention relates to a video game machine having a means of storage for a software program connected in a flexible manner to a computer, in particular a video game program cartridge. More specifically, this invention relates to a cartridge with flexible connection, having a security system, to determine whether the cartridge/software is an authentic product or not.

[0002] Examples of a software control system of an external storage device which function as a means to store software that was used in the past, include patent applications published in the Japanese Patent Disclosures under numbers 61-296433 and 62-331.

[0003] To summarise the inventions published in the Japanese Patent Disclosures, a software cartridge and a hardware main unit are provided with the same security chip so that, if the same data is used, control is implemented by the software that operates the main hardware unit.

[0004] EP 0,080,244 discloses a system that discourages the use of computer equipment with software that is not approved for such use by the manufacturer. A microprocessor compares data stored in a RAM and the contents of a data table in a game ROM with a field of reference data which is recorded at location in a further ROM. If the comparison indicates that the data stored for input to the video display is different from that stored in the reference table, the microprocessor enters an endless loop which alternately clears the screen and presents a display as defined in the data table.

[0005] EP 0,048,586 discloses a random access memory arrangement.

[0006] EP 0,206,704 discloses a system for determining the authenticity of software in an information processing apparatus. Microprocessors in a main unit and an external memory are synchronised and execute the same arithmetic operation. The results of the operation are exchanged and each device compares the results of its own operation with that of the other device. If the results coincide, the software is considered authentic.

SUMMARY OF THE INVENTION

[0007] The invention provides a video game machine and its method of operation as set out in the independent claims.

[0008] An embodiment of the invention provides a security lock for a means of storage of software, such as a cartridge or a similar device, only through the software used by the means of storage of the software, specifically by using for this purpose only a ROM (read only memory) that is mounted inside the cartridge.

[0009] The security lock of this embodiment of the invention is used with a game machine that displays the content of a game through a video display device, and it uses a video game system comprising a means of storage for storing the game programs as software that is connected in a flexible manner to this game machine.

[0010] Consequently, according to this embodiment of the invention, it becomes specifically possible to ensure security simply through the ROM that is mounted inside the cartridge, as a means of security that takes advantage of the means to store software in a cartridge or a similar device. At the same time, it is also possible to ensure security of the means to store the software in a manner that corresponds to the progress of the game. In addition, there is no need for software on the side of the game machine, since this security is ensured solely by the hardware, which is an advantage of this invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011]

Figure 1 is a simplified block diagram of one embodiment of this invention;

Figure 2 is a block circuit diagram of a security part according to an embodiment of the present invention;

Figure 3 is a timing chart explaining operation of the security part according to an embodiment of the present invention; and

Fig. 4 is a timing chart explaining operation of the security part according to an embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0012] Fig. 1 is a block diagram of an embodiment of the present invention. Number 1 of Figure 1 is a video display device of a TV receiver or a similar device, and 2 is a game machine for video games connected to display device 1. If display is a liquid crystal display (LCD), or a similar type, it can be mounted into game machine 2.

[0013] Number 3 is a cartridge or a similar means of storage, which is connected in a flexible manner to game machine 2, and which stores game programs in the form of software. Means of storage 3 can be a compact disk, or it can also be a magnetic tape, a floppy disk, or a similar ROM (read only memory) or RAM (random access memory) device. Means of storage 3 is also provided with a storage part 31 that stores the security code, which is a special code used to ensure security and make the decision whether the cartridge/software is a genuine product or not).

[0014] Number 4 is a controller for manual operation, connected to game machine 2, which serves to control the content of the game that is displayed on the screen of display device 1.

[0015] Number 21 is a video controller, which forms a part of game machine 2 and connects to display device 1. Reference item 22 is an I/O interface, also forming a part of game machine 2, which is connected to controller 4.

[0016] Video controller 21, I/O interface 22, and means of storage 3 of a cartridge or a similar device are connected to a CPU 24 that processes the signal through a bus-line 23. A security device 25 connects to bus-line 23, as well as to CPU 24. Operation of the embodiment of Fig. 1 can now be described using the following application example, in which means of storage 3 of game software, is connected to the game machine 2. When the power source, not shown on the figure, is turned on, CPU 24, or signal processing unit, starts reading a special security code received from storage part 31 of storage means 3, while at the same time the security code is being written to a security device 25. Approximately simultaneously with the writing of this security code the security code is compared with a special security code that has been input in advance into game machine 2. If both security codes are identical, video controller 21 will start operating. One can then use the game machine 2 as usual, since the content of the game will be displayed on display device 1.

[0017] If both security codes are not identical, a reset signal 26 will be output to signal processing unit 24 from security device 25, which operates the video controller 21. As a result of this reset signal, the operation of signal processing unit 24 will be stopped, and the content of the game will not be displayed on display device 1.

[0018] In other words, the system is such that unless a specific security code from storage part 31 is entered to security machine 25 when accessing video controller 21, which determines whether it is possible to operate the game machine 2, signal processing unit 24 will be brought to a stop.

[0019] Fig. 2 shows a block diagram of security device 25. Number 251 on the figure represents a 4 byte memory, connected to a data bus 231, which forms a part of bus-line 23. Memory 251 stores the security code received from storage part 31 of means of storage 3. In addition, an output from memory 251 is connected to the input of memory 251, to enable repeated reading of the output security code in memory 251.

[0020] A comparator 252 is connected to the output from memory 251. The memory output is compared to a special security code of, for example, SEGA that is present in game machine 2, and comparator 252 outputs a determination signal S1, determining whether the codes are identical or not. A holding circuit 253 retains the determination signal S1, and is connected to the output from comparator 252.

[0021] Number 254 is a check holding circuit, connected to the output of holding circuit 253, and retaining the output signal S2. Finally, the output terminal of check holding circuit 254, which is connected to signal processing unit 24, sends a reset signal 26.

[0022] Number 256 on Figure 2 represents the first decoder, connected to address bus 232, forming a part of bus-line 23. As shown in Figure 3, when address signal (A1) for input of the security signal is present, decoder 256 sends signal (D1) and (D2) to memory 251 and to holding circuit 253, respectively.

[0023] Number 257 on Figure 2 is the second decoder, connected to address bus 232 forming a part of bus-line 23. As shown in Figure 3 and Figure 4, when the address signal (A2) from the video controller 21 is present, decoder 257 sends signal (D2) to check holding circuit 254.

[0024] When a power source (not shown) is switched on, as seen in Figure 3, the output (S2) from holding circuit 253 is set to "0", while at the same time the output 26 of check holding circuit 254 is set to "1", so that signal processing unit 24 of the CPU enables support of normal operations.

[0025] In this mode, when the address signal (A1) of the writing of the security code is present, as in the code signal "SEGA" of the security data, the code signal, for example, "SEGA" is written to memory 251 by the output signal (D1) of decoder 256, while at the same time it is compared to the special security code SEGA of game machine 2, and if these codes match, the output (S1) of the comparator 252 will be changed to "1", and retained in the holding circuit 253 through the output signal (D1) of decoder 256. See Figure 3.

[0026] Furthermore, as seen in Figure 3, the address signal (A1) is divided into two signals. Since signal processing unit 24 of the CPU was designed for 16 bits, if the security data is for instance "SEGA", a 2 byte division is required.

[0027] When address signal (A2) from video controller 21 is present, as is shown on the right side of Figure 3, the output (S2) of the holding circuit 253 is checked by the output signal (D2) of decoder 257, and retained by check holding circuit 254.

[0028] In other words, when the output (S2) of holding circuit 253 is "1", it will be retained by check holding circuit 254. When output 26 of check holding circuit 254 is retained as "1", signal processing unit 24 of the CPU supports normal operation.

[0029] When there is a different situation than the one described above, for instance when the code signal written to memory 251 differs from the security code SEGA that is held by game machine 2, as seen in Figure 4, the result is that the output (S1) of comparator 252 and the output (S2) of holding circuit 253 are retained as "0", and when the address signal (A2) of the video controller 21 is present, the output signal (S2) of holding circuit 253 will be checked by the output signal (D2) of decoder 257, and held by check holding circuit 254. In other words, when the output (S2) of holding circuit 253 is "0", it will be retained by check holding circuit 254. Specifically, output 26 of check holding circuit 254 will be changed to "0", and signal processing unit 24 of the CPU stops running normal operations.

[0030] Consequently, as is clear from the explanation above, each time address signal (A2) of video controller 21 is present, or, to put it another way, each time video controller 21 is accessed, it is possible to check whether the means of storage 3, for instance a cartridge, is genuine or not.

[0031] Further, in the middle of game playing, the operations of Figure 3 may be performed. Therefore, it becomes possible to check whether the means of storage (3) is genuine as the game progresses.

[0032] The effect of this invention is that it becomes possible to ensure security and determine if the cartridge/software is a genuine product or not simply through the software or the means of software storage, specifically, simply through the ROM that is mounted inside the cartridge, as a means of security that takes advantage of the means to store software in a cartridge or a similar device. At the same time, another effect of this invention is that it is also possible to ensure security of the means to store the software in a manner that corresponds to the progress of the game. In addition, there is no need for software on the side of the game machine, since this security is ensured solely by the hardware, which is an advantage of this invention.

[0033] A preferred embodiment of the present invention has now been described. Variations and modifications will be readily apparent to those of skill in the art. For this reason, the invention should be construed solely according to the claims.

Claims

1. A video game machine (2) having a signal processing means (24) for executing a game program stored in an external storage means (3), said external storage means also storing a first security code and being detachably coupled with said video game machine, said video game machine (2) comprising:

   a video controller (21) for outputting an image signal generated through the execution of said game program under operation by said signal processing means (24);
   storage means (251) for storing said first security code received from said external storage means(3); and
   comparing means (252) for comparing said first security code received from said external storage means (3) with a second security code that has been input into said video machine (2) in advance;
   characterised by a security means (25) for preventing said video controller (21) from outputting an image signal if the first security code does not agree with said second security code when said signal processing means (24) accesses said video controller (21) during execution of said game program.

2. The video game machine of claim 1, wherein said security means (25) prevents said video controller (21) from outputting an image signal by outputting a reset signal to said signal processing means (24).

3. A method for verifying authenticity of external storage means in a video game machine (2) comprising a signal processing means (24) for executing a game program stored in external storage means (3), said external storage means also storing a first security code and detachably coupled with said video game machine (2), and a video controller (21) for outputting an image signal generated through the execution of said game program under operation by said signal processing means (24);
   the method comprising:

   storing, in a storage means (251) in said video game machine (2), said first security code received from said external storage means (3); and
   comparing said first security code received from said external storage means (3) with a second security code that has been input into said video game machine (2) in advance;
   characterised by providing security means (25) for preventing said video controller (21) from outputting an image signal if the first security code does not agree with said second security code when said signal processing means (24) accesses said video controller (21) during execution of said game program.

4. The method of claim 3, wherein said security means (25) prevents said video controller from outputting an image signal by outputting a reset signal to said signal processing means (24).

Patentansprüche

1. Videospielautomat (2) mit einer Signalverarbeitungseinrichtung (24) zum Ausführen eines in einem externen Speichermittel (3) gespeicherten Videoprogramms, wobei das externe Speichermittel auch einen ersten Sicherheitscode speichert und abnehmbar mit dem genannten Videospielautomat gekoppelt ist, wobei der genannte Videospielautomat (2) folgendes umfaßt:

   Videocontroller (21) zum Ausgeben eines Bildsignals, das bei Betrieb von der genannten Signalverarbeitungseinrichtung (24) durch die Ausführung des genannten Spielprogramms erzeugt wird,
   Speichermittel (251) zum Speichern des

genannten ersten, von dem genannten externen Speichermittel (3) erhaltenen Sicherheitscodes,

Vergleichsmittel (252) zum Vergleichen des genannten ersten, von dem genannten externen Speichermittel (3) erhaltenen Sicherheitscodes mit einem zweiten Sicherheitscode, der im voraus in den genannten Videoautomat (2) eingegeben wurde,

gekennzeichnet durch ein Sicherheitsmittel (25) zum Verhindern, daß der genannte Videocontroller (21) ein Bildsignal ausgibt, falls der erste Sicherheitscode nicht mit dem genannten zweiten Sicherheitscode übereinstimmt, wenn die genannte Signalverarbeitungseinrichtung (24) während der Ausführung des genannten Spielprogramms auf den genannten Videocontroller (21) zugreift.

2. Videospielautomat nach Anspruch 1, bei dem das genannte Sicherheitsmittel (25) verhindert, daß der genannte Videocontroller (21) ein Bildsignal ausgibt, indem es ein Rücksetzsignal an die genannte Signalverarbeitungseinrichtung (24) sendet.

3. Verfahren zum Verifizieren der Echtheit externer Speichermittel in einem Videospielautomat (2), der eine Signalverarbeitungseinrichtung (24) zum Ausführen eines in einem externen Speichermittel (3) gespeicherten Videoprogramms, wobei das genannte externe Speichermittel auch einen ersten Sicherheitscode speichert und abnehmbar mit dem genannten Videospielautomat (2) gekoppelt ist, und einen Videocontroller (21) zum Ausgeben eines Bildsignals aufweist, das bei Betrieb von der genannten Signalverarbeitungseinrichtung (24) durch die Ausführung des genannten Spielprogramms erzeugt wird, wobei das Verfahren folgendes umfaßt:

Speichern des genannten ersten, von dem genannten externen Speichermittel (3) erhaltenen Sicherheitscodes in einem Speichermittel (152) in dem genannten Videospielautomat (2), und

Vergleichen des genannten ersten, von dem genannten externen Speichermittel (3) erhaltenen Sicherheitscodes mit einem zweiten Sicherheitscode, der im voraus in den genannten Videospielautomat (2) eingegeben wurde,

gekennzeichnet durch das Bereitstellen eines Sicherheitsmittels (25) zum Verhindern, daß der genannte Videocontroller (21) ein Bildsignal ausgibt, falls der erste Sicherheitscode nicht mit dem genannten zweiten Sicherheitscode übereinstimmt, wenn die genannte Signalverarbeitungseinrichtung (24) während der Ausführung des genannten Spielprogramms auf den genannten Videocontroller (21) zugreift.

4. Verfahren nach Anspruch 3, bei dem das genannte Sicherheitsmittel (25) verhindert, daß der genannte Videocontroller ein Bildsignal ausgibt, indem es ein Rücksetzsignal an die genannte Signalverarbeitungseinrichtung (24) sendet.

Revendications

1. Machine de jeux vidéo (2) ayant un moyen de traitement de signaux (24) pour exécuter un programme de jeu stocké dans un moyen de stockage externe (3), ledit moyen de stockage externe stockant aussi un premier code de sécurité et étant couplé de manière détachable à ladite machine de jeux vidéo, ladite machine de jeux vidéo (2) comprenant :

un contrôleur vidéo (21) pour sortir un signal d'image généré durant l'exécution dudit programme de jeu dans le cadre du fonctionnement dudit moyen de traitement de signaux (24) ;

un moyen de stockage (251) pour stocker ledit premier code de sécurité reçu à partir dudit moyen de stockage externe (3) ; et

un moyen de comparaison (252) pour comparer ledit premier code de sécurité reçu à partir dudit moyen de stockage externe (3) à un deuxième code de sécurité qui a été entré dans ladite machine vidéo (2) à l'avance ;

caractérisé par un moyen de sécurité (25) pour empêcher ledit contrôleur vidéo (21) de sortir un signal d'image si le premier code de sécurité ne correspond pas audit deuxième code de sécurité quand ledit moyen de traitement de signaux (24) sollicite ledit contrôleur vidéo (21) durant l'exécution dudit programme de jeu.

2. Machine de jeux vidéo selon la revendication 1, dans laquelle ledit moyen de sécurité (25) empêche ledit contrôleur vidéo (21) de sortir un signal d'image en sortant un signal de remise à zéro allant audit moyen de traitement de signaux (24).

3. Procédé pour vérifier l'authenticité du moyen de stockage externe dans une machine de jeux vidéo (2) comprenant un moyen de traitement de signaux (24) pour exécuter un programme de jeu stocké dans un moyen de stockage externe (3), ledit moyen de stockage externe stockant aussi un premier code de sécurité et étant couplé de manière détachable à ladite machine de jeu vidéo (2), et un contrôleur vidéo (21) pour sortir un signal d'image généré durant l'exécution dudit programme de jeu dans le cadre du fonctionnement dudit moyen de

traitement de signaux (24) ;

le procédé comprenant :

le stockage, dans un moyen de stockage (251), dans ladite machine de jeux vidéo (2), dudit premier code de sécurité reçu à partir dudit moyen de stockage externe (3) ; et

la comparaison dudit premier code de sécurité reçu à partir dudit moyen de stockage externe (3) à un deuxième code de sécurité qui a été entré dans ladite machine de jeux vidéo (2) à l'avance ;

caractérisé par la fourniture d'un moyen de sécurité (25) pour empêcher ledit contrôleur vidéo (21) de sortir un signal d'image si le premier code de sécurité ne correspond pas audit deuxième code de sécurité quand ledit moyen de traitement de signaux (24) sollicite ledit contrôleur vidéo (21) durant l'exécution dudit programme de jeu.

4. Procédé selon la revendication 3, dans lequel ledit moyen de sécurité (25) empêche ledit contrôleur vidéo (21) de sortir un signal d'image en sortant un signal de remise à zéro allant audit moyen de traitement de signaux (24).

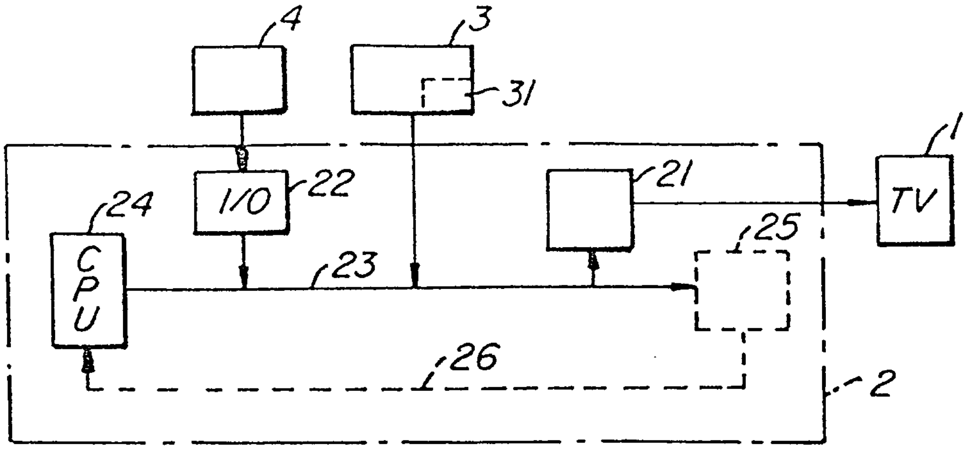
4
3
31
1
TV
I/O
22
21
24
C
P
U
25
23
26
2

FIG._1.

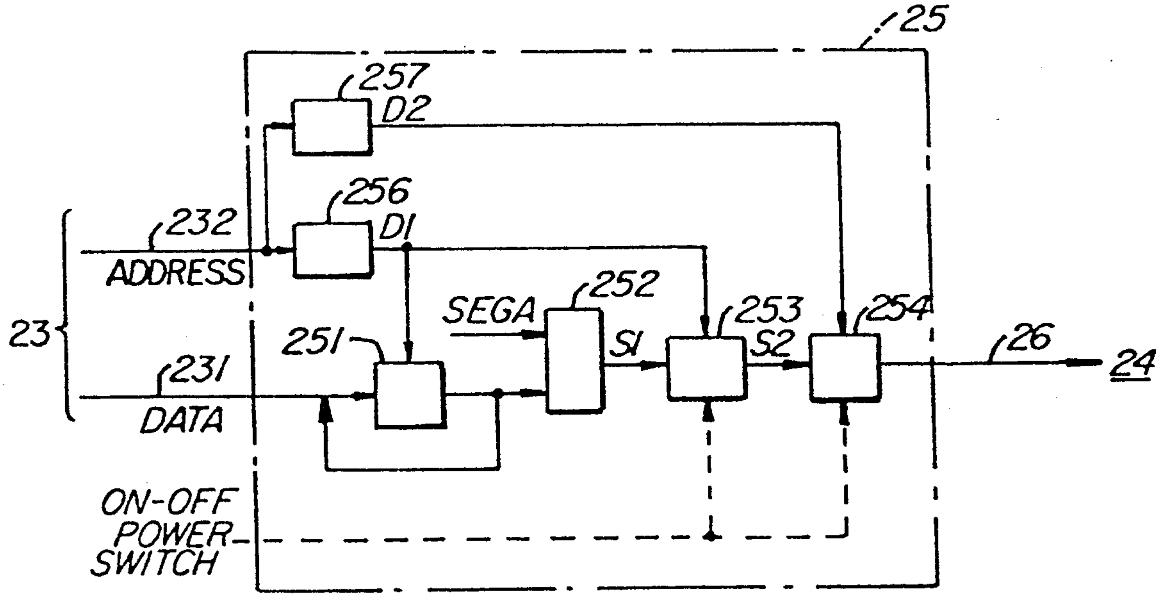
25
257
D2
256
D1
232
ADDRESS
23
252
SEGA
253
254
251
S1
S2
26
24
231
DATA
ON-OFF
POWER-
SWITCH

FIG._2.

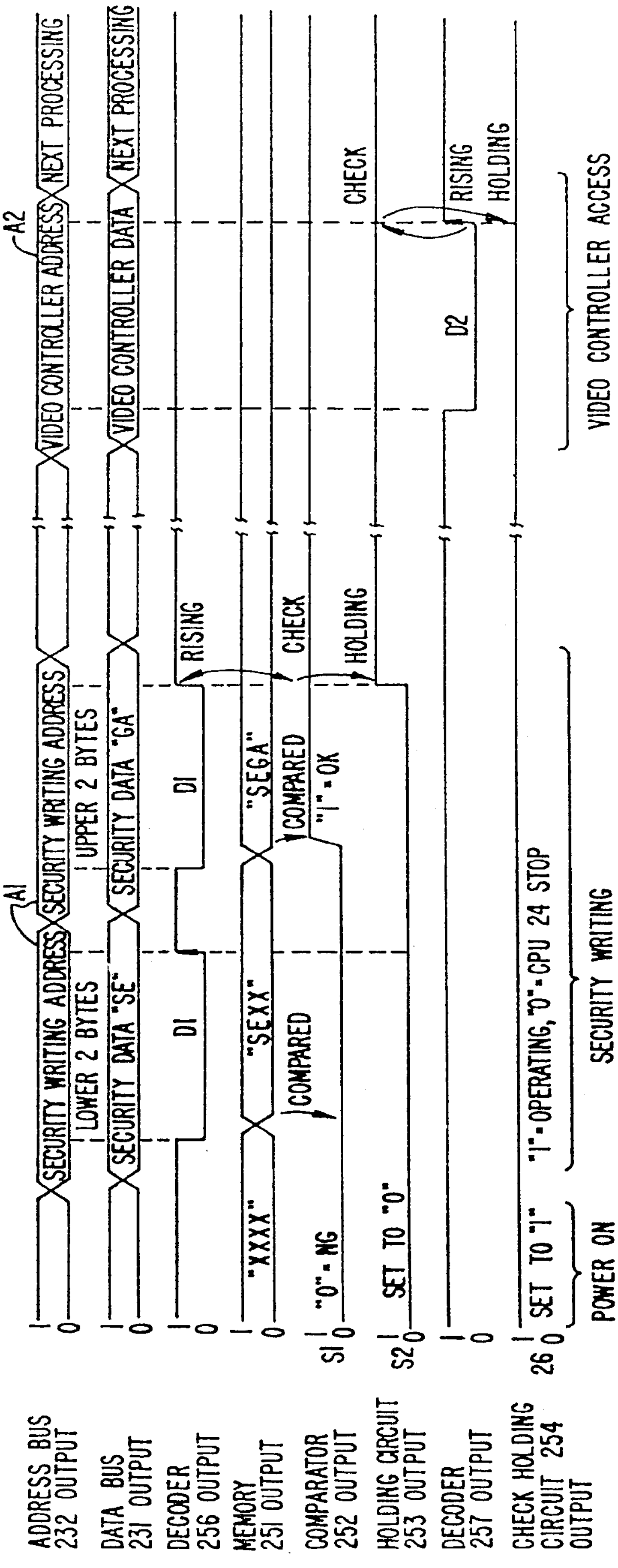
ADDRESS BUS 232 OUTPUT
DATA BUS 231 OUTPUT
DECODER 256 OUTPUT
MEMORY 251 OUTPUT
COMPARATOR 252 OUTPUT
HOLDING CIRCUIT 253 OUTPUT
DECODER 257 OUTPUT
CHECK HOLDING CIRCUIT 254 OUTPUT
1
0
S1
S2
26
A1
A2
SECURITY WRITING ADDRESS
SECURITY WRITING ADDRESS
VIDEO CONTROLLER ADDRESS
NEXT PROCESSING
LOWER 2 BYTES
UPPER 2 BYTES
SECURITY DATA "SE"
SECURITY DATA "GA"
VIDEO CONTROLLER DATA
NEXT PROCESSING
D1
D1
RISING
"XXXX"
"SEXX"
"SEGA"
COMPARED
COMPARED
CHECK
"0"=NG
"1"=OK
SET TO "0"
HOLDING
CHECK
D2
RISING
HOLDING
SET TO "1"
"1"=OPERATING, "0"=CPU 24 STOP
POWER ON
SECURITY WRITING
VIDEO CONTROLLER ACCESS

FIG._3.

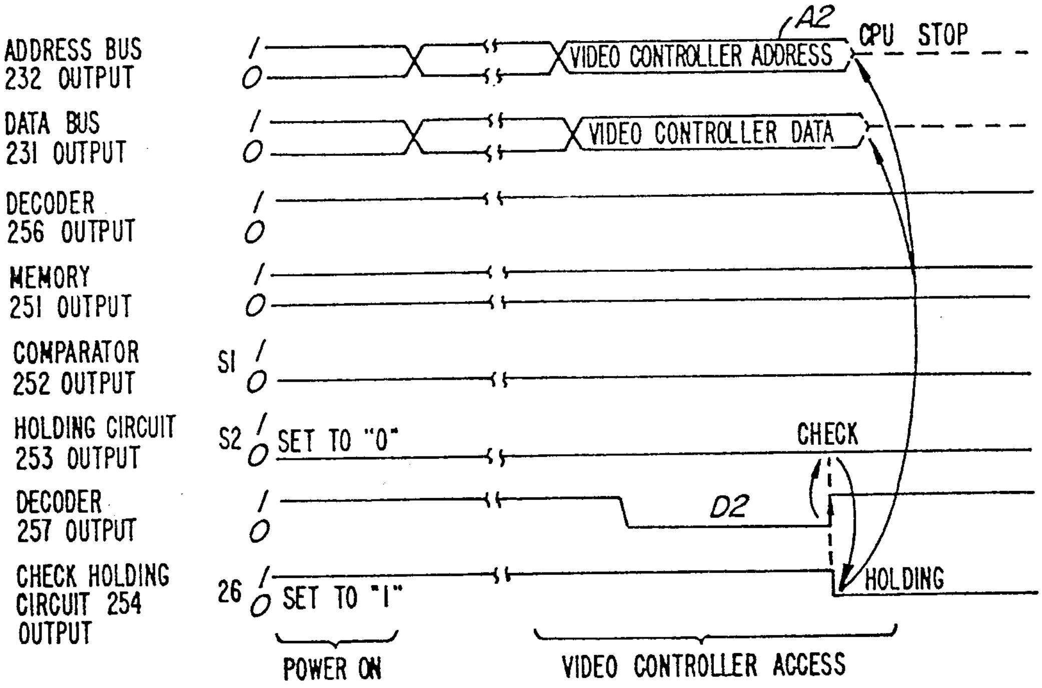
ADDRESS BUS
232 OUTPUT
DATA BUS
231 OUTPUT
DECODER
256 OUTPUT
MEMORY
251 OUTPUT
COMPARATOR
252 OUTPUT
HOLDING CIRCUIT
253 OUTPUT
DECODER
257 OUTPUT
CHECK HOLDING
CIRCUIT 254
OUTPUT
1
0
S1
S2
26
A2
CPU STOP
VIDEO CONTROLLER ADDRESS
VIDEO CONTROLLER DATA
SET TO "0"
CHECK
D2
SET TO "1"
HOLDING
POWER ON
VIDEO CONTROLLER ACCESS

FIG._4.