United States Patent [19]

Nakagawa

[11] **Patent Number: 5,070,479**

[45] **Date of Patent: * Dec. 3, 1991**

[54] **EXTERNAL MEMORY HAVING AN AUTHENTICATING PROCESSOR AND METHOD OF OPERATING SAME**

[75] Inventor: **Katsuya Nakagawa**, Kusatsu, Japan

[73] Assignee: **Nintendo Company Limited**, Kyoto, Japan

[*] Notice: The portion of the term of this patent subsequent to Jan. 24, 2006 has been disclaimed.

[21] Appl. No.: **297,105**

[22] Filed: **Jan. 13, 1989**

Related U.S. Application Data

[62] Division of Ser. No. 812,929, Dec. 23, 1985, Pat. No. 4,799,635.

[30] **Foreign Application Priority Data**

Jun. 24, 1985 [JP] Japan 60-138699
Jun. 28, 1985 [JP] Japan 60-143026

[51] **Int. Cl.**[5] **G11B 23/28**
[52] **U.S. Cl.** **395/575**; 380/3
[58] **Field of Search** ... 364/200 MS File, 900 MS File; 380/3, 4, 5; 235/380, 375, 382

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,193,131	3/1980	Lennon et al.	364/200
4,218,738	8/1980	Matyas et al.	364/200
4,310,720	1/1982	Check, Jr.	235/382
4,459,655	7/1984	Willemin	364/200
4,471,216	9/1984	Herve	235/380
4,497,038	1/1985	Diepold-Scharnitzky	364/900
4,523,297	6/1985	Ugon et al.	364/900
4,652,990	3/1987	Pailen et al.	380/24
4,683,553	7/1987	Mollier	380/4
4,723,121	2/1988	van den Boom et al.	235/382
4,755,799	7/1988	Romano	340/543
4,757,468	7/1988	Domenik et al.	364/900
4,862,156	8/1989	Westberg et al.	364/521

FOREIGN PATENT DOCUMENTS

53-17849 6/1978 Japan .

Primary Examiner—Stuart N. Hecker
Assistant Examiner—Rebecca L. Rudolph
Attorney, Agent, or Firm—Nixon & Vanderhye

[57] **ABSTRACT**

A system for determining a truth comprises a main unit which is employed together with an external memory, for example, ROM cartridge, floppy disk or the like. The main unit is operated following a program contained in the external memory. In the external memory and the main unit, the same semiconductor devices, for example, microprocessors are incorporated respectively, and the former device acts as a key device and the latter device acts as a lock device. The key device and the lock device are synchronized with each other, executing the same arithmetic operation following the same program. The results of this operation are exchanged with each other, and the two devices compare the result of operation by their own with the result of operation by the other, respectively. If the both coincide, software is determined to be true and the main unit is allowed to operate, but if not coincide, software is determined to be false and the main unit is left reset intact. Thereby, processing in the information processing apparatus is disabled when the software contained in the external memory is not true.

64 Claims, 10 Drawing Sheets

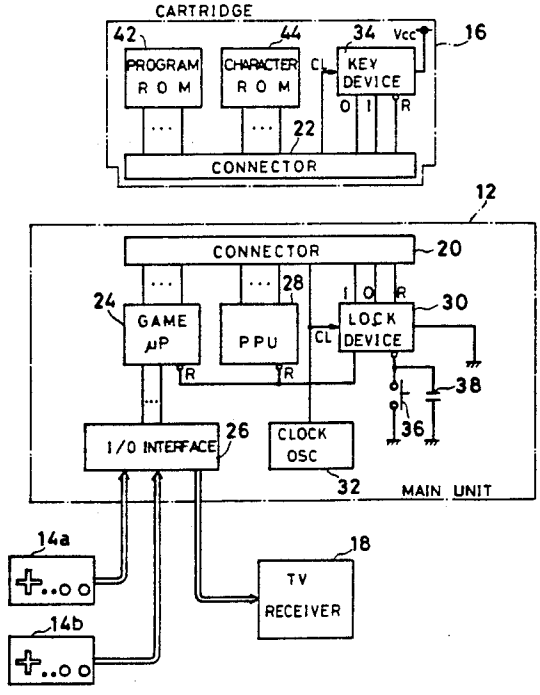


FIG. 1

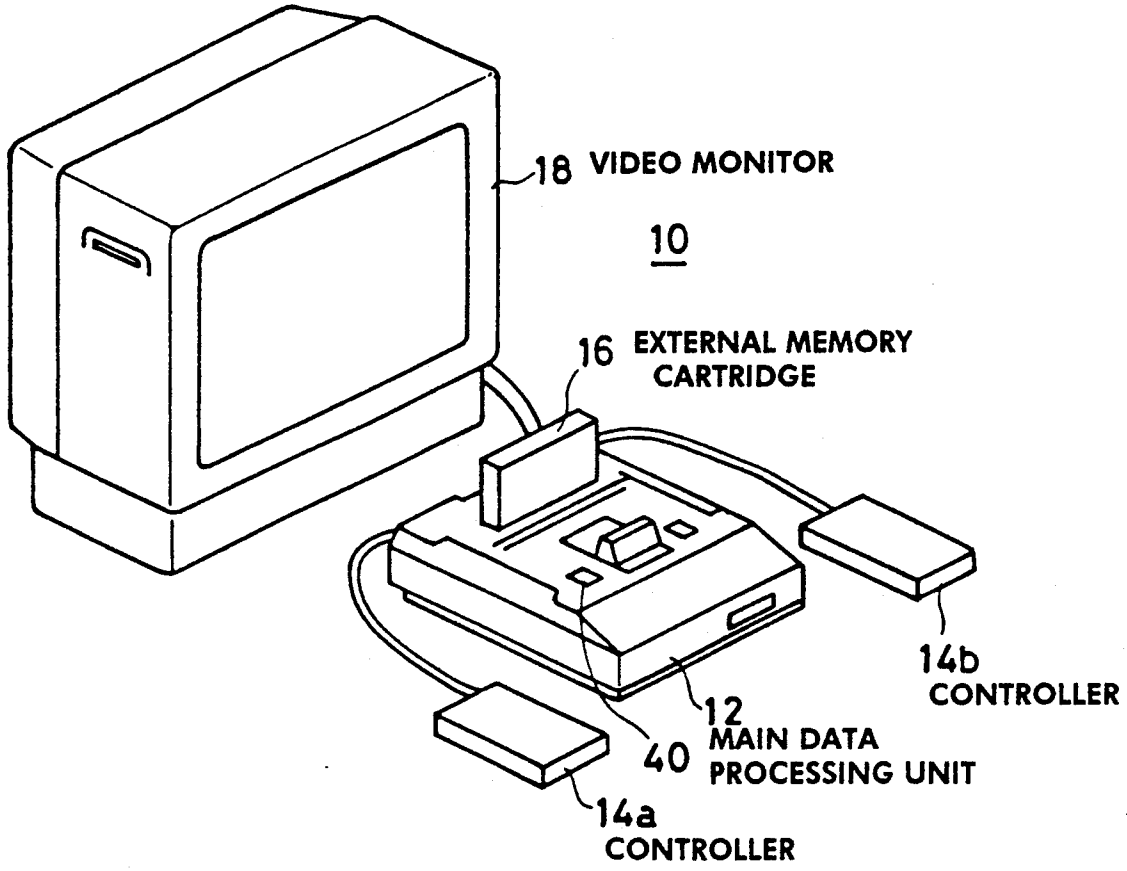


FIG. 6

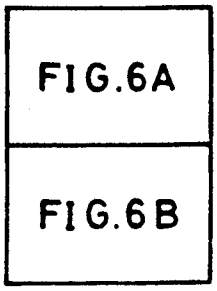


FIG. 7

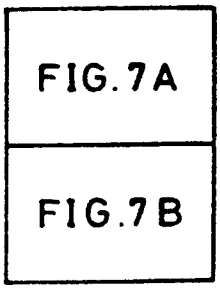


FIG. 2

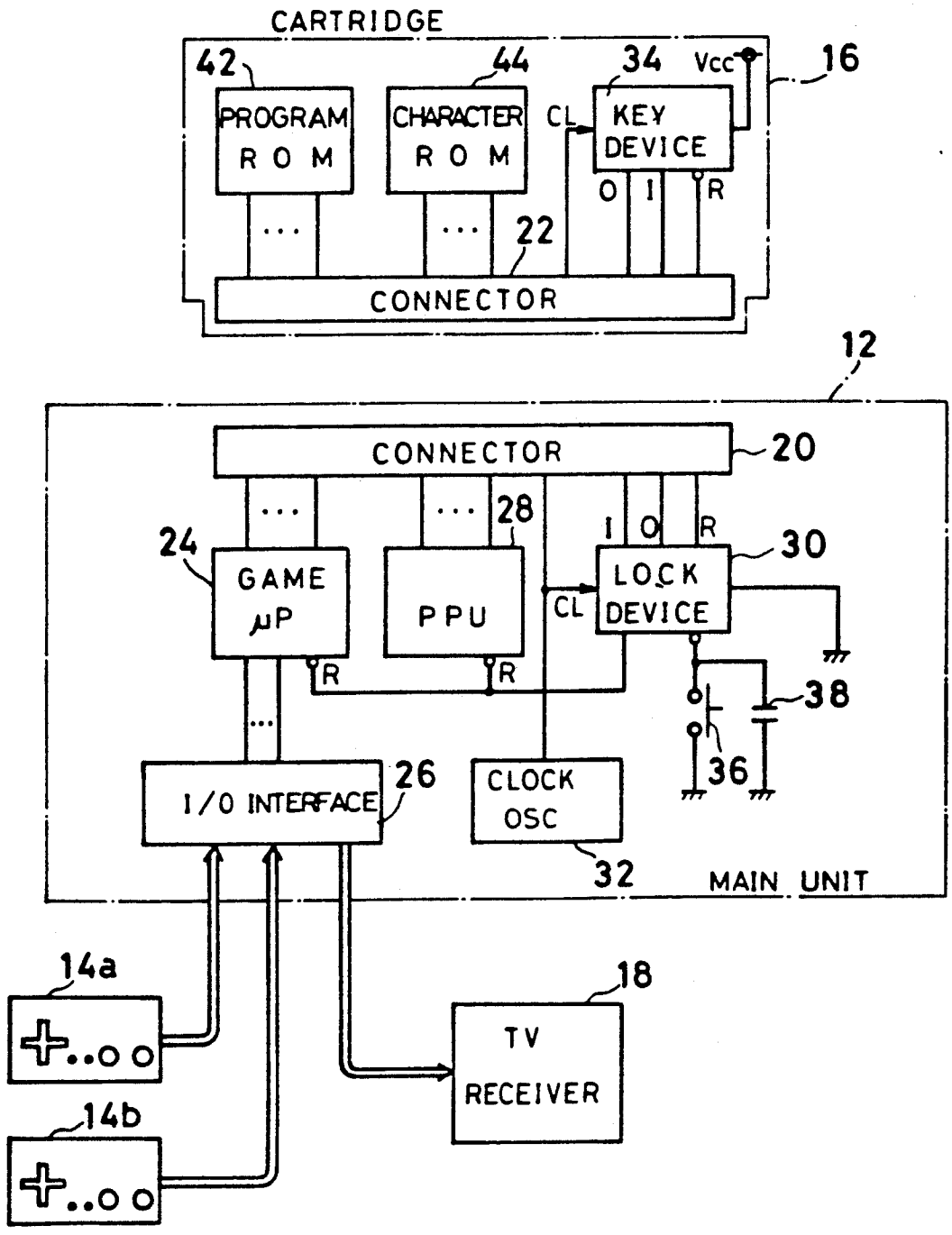

CARTRIDGE
42
PROGRAM ROM
44
CHARACTER ROM
34
Vcc
16
CL
KEY DEVICE
O I R
22
CONNECTOR
12
CONNECTOR
20
28
I O R
24
GAME μP
PPU
CL
LOCK DEVICE
30
R
R
38
36
I/O INTERFACE
26
CLOCK OSC
32
MAIN UNIT
14a
18
TV RECEIVER
14b

FIG. 3

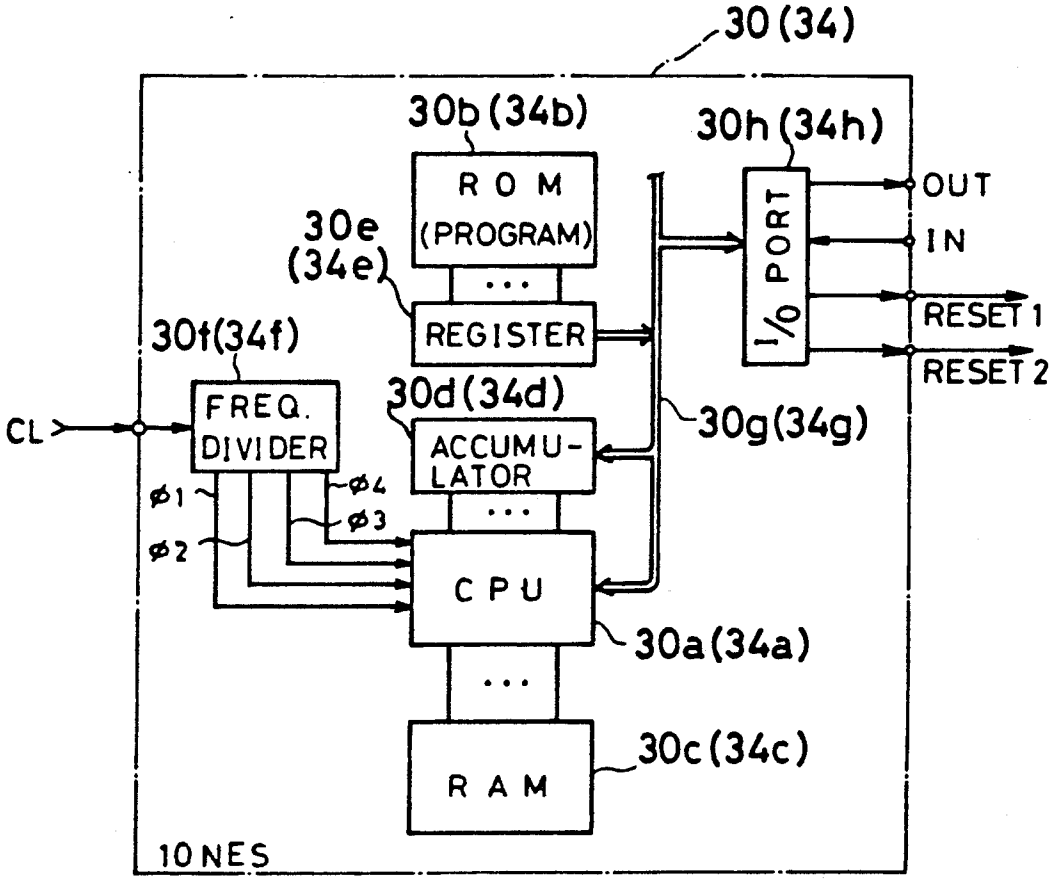

30 (34)
30b (34b)
30h (34h)
ROM (PROGRAM)
30e (34e)
REGISTER
I/O PORT
OUT
IN
RESET 1
RESET 2
30f (34f)
FREQ. DIVIDER
CL
30d (34d)
ACCUMU-LATOR
30g (34g)
φ1
φ2
φ3
φ4
CPU
30a (34a)
RAM
30c (34c)
10 NES

FIG. 4

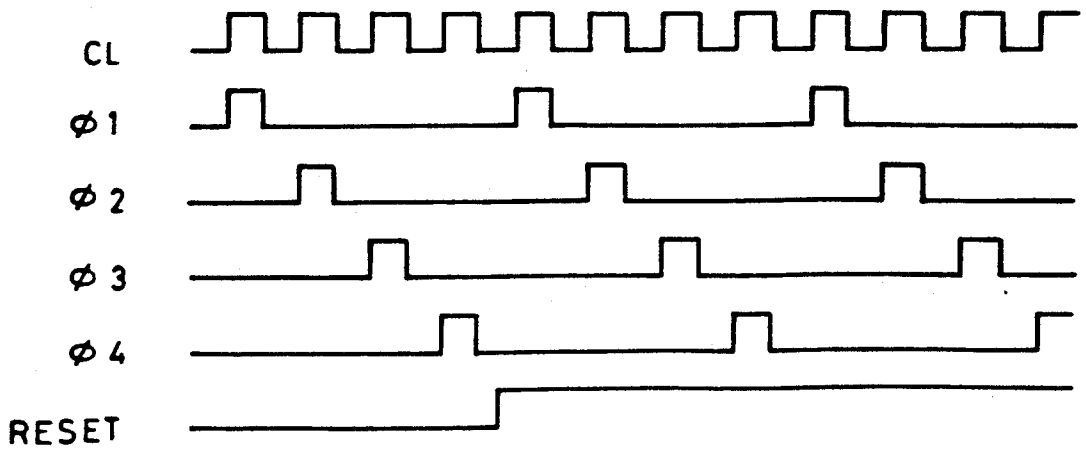

CL
φ1
φ2
φ3
φ4
RESET

FIG. 5

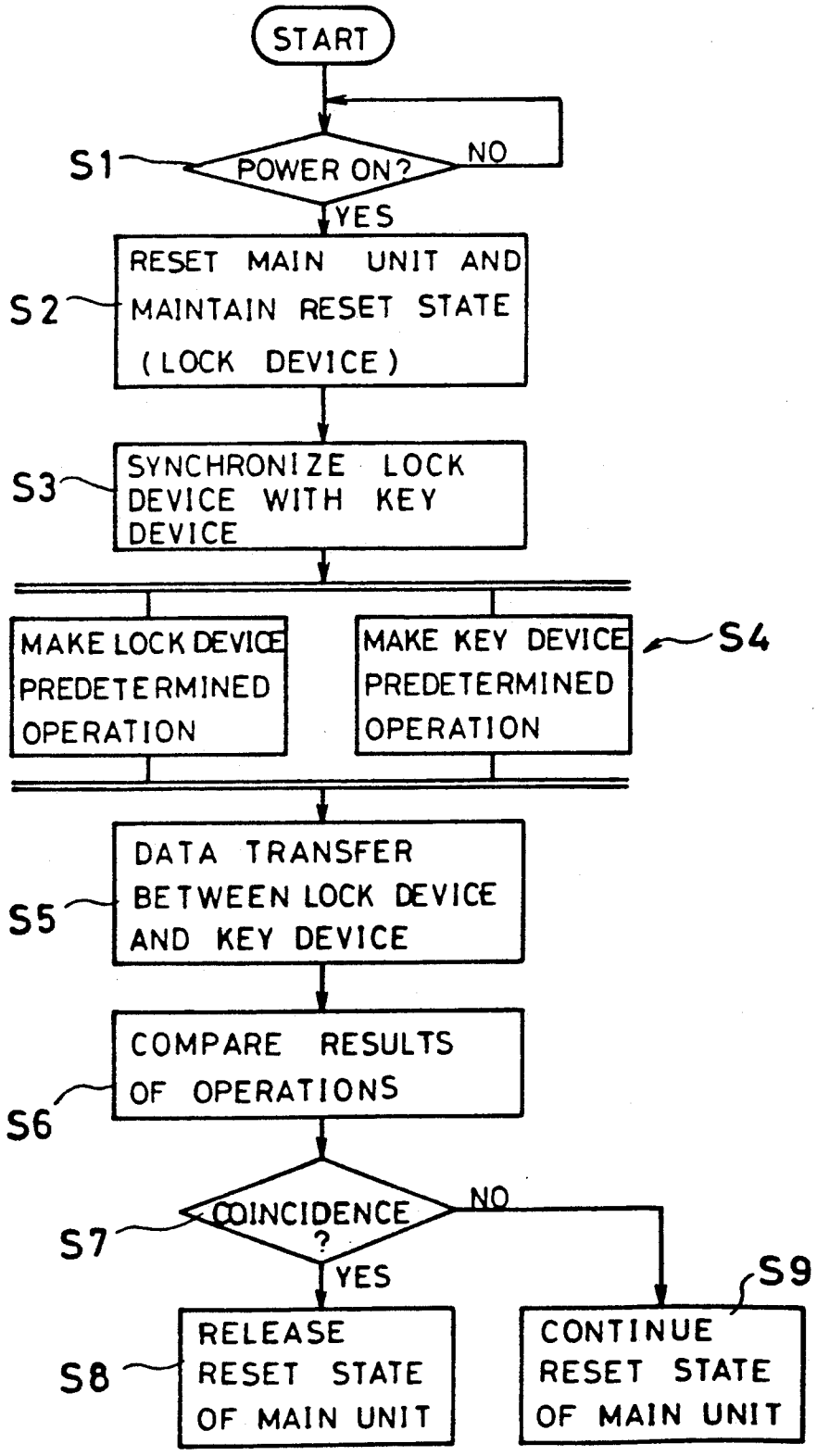

START
S1
POWER ON?
NO
YES
S2
RESET MAIN UNIT AND MAINTAIN RESET STATE (LOCK DEVICE)
S3
SYNCHRONIZE LOCK DEVICE WITH KEY DEVICE
MAKE LOCK DEVICE PREDETERMINED OPERATION
MAKE KEY DEVICE PREDETERMINED OPERATION
S4
S5
DATA TRANSFER BETWEEN LOCK DEVICE AND KEY DEVICE
S6
COMPARE RESULTS OF OPERATIONS
S7
COINCIDENCE ?
NO
YES
S8
RELEASE RESET STATE OF MAIN UNIT
S9
CONTINUE RESET STATE OF MAIN UNIT

FIG. 6A

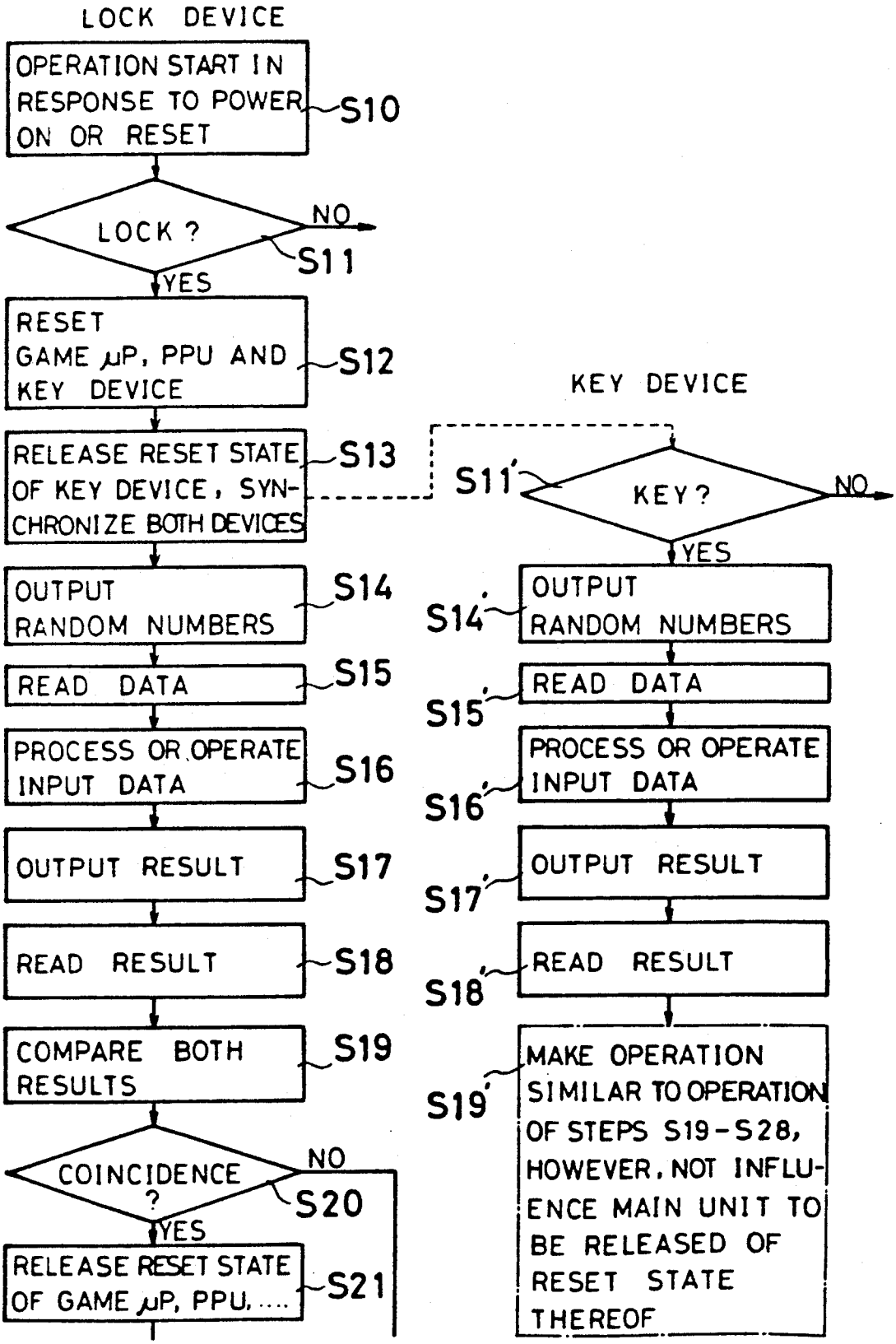

LOCK DEVICE
OPERATION START IN RESPONSE TO POWER ON OR RESET
S10
LOCK ?
NO
S11
YES
RESET GAME μP, PPU AND KEY DEVICE
S12
RELEASE RESET STATE OF KEY DEVICE, SYNCHRONIZE BOTH DEVICES
S13
OUTPUT RANDOM NUMBERS
S14
READ DATA
S15
PROCESS OR OPERATE INPUT DATA
S16
OUTPUT RESULT
S17
READ RESULT
S18
COMPARE BOTH RESULTS
S19
COINCIDENCE ?
NO
S20
YES
RELEASE RESET STATE OF GAME μP, PPU, ...
S21
KEY DEVICE
S11'
KEY ?
NO
YES
S14'
OUTPUT RANDOM NUMBERS
S15'
READ DATA
S16'
PROCESS OR OPERATE INPUT DATA
S17'
OUTPUT RESULT
S18'
READ RESULT
S19'
MAKE OPERATION SIMILAR TO OPERATION OF STEPS S19-S28, HOWEVER, NOT INFLUENCE MAIN UNIT TO BE RELEASED OF RESET STATE THEREOF

FIG. 6B

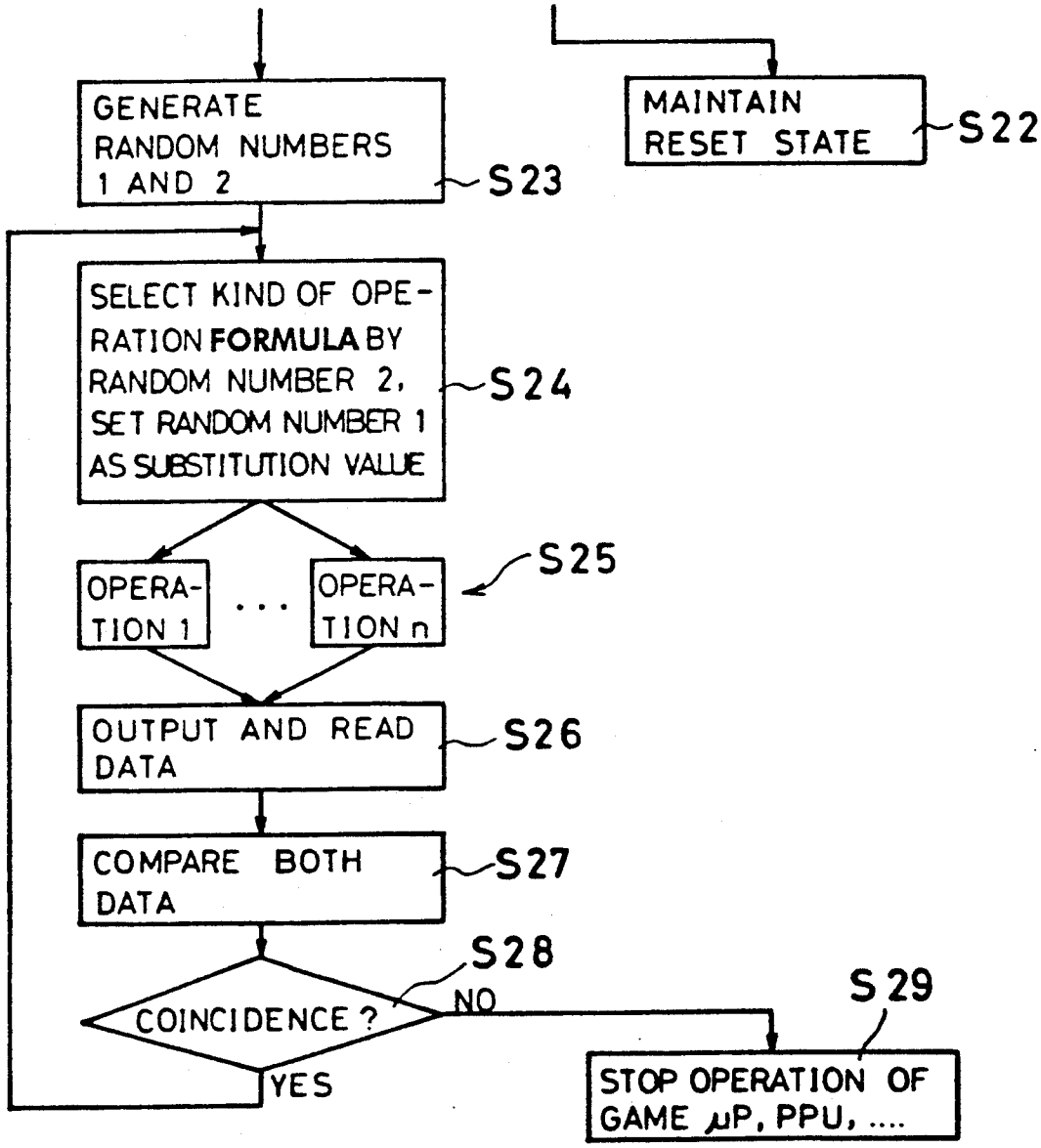

GENERATE RANDOM NUMBERS 1 AND 2
S23
MAINTAIN RESET STATE
S22
SELECT KIND OF OPERATION FORMULA BY RANDOM NUMBER 2, SET RANDOM NUMBER 1 AS SUBSTITUTION VALUE
S24
OPERATION 1
...
OPERATION n
S25
OUTPUT AND READ DATA
S26
COMPARE BOTH DATA
S27
COINCIDENCE ?
S28
NO
YES
S29
STOP OPERATION OF GAME μP, PPU, ...

FIG. 7A

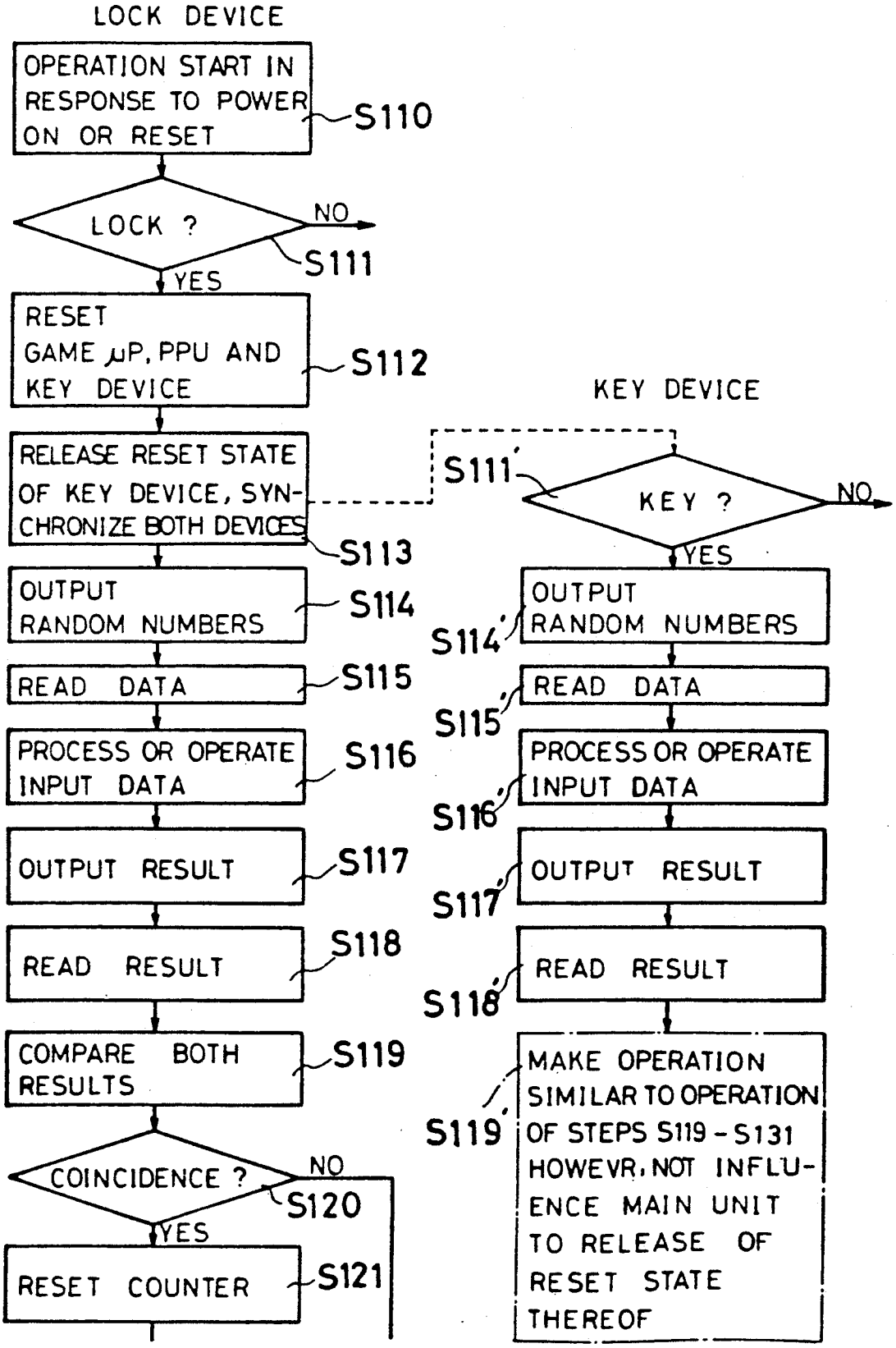

LOCK DEVICE
OPERATION START IN RESPONSE TO POWER ON OR RESET
S110
LOCK ?
NO
S111
YES
RESET GAME μP, PPU AND KEY DEVICE
S112
RELEASE RESET STATE OF KEY DEVICE, SYNCHRONIZE BOTH DEVICES
S113
OUTPUT RANDOM NUMBERS
S114
READ DATA
S115
PROCESS OR OPERATE INPUT DATA
S116
OUTPUT RESULT
S117
READ RESULT
S118
COMPARE BOTH RESULTS
S119
COINCIDENCE ?
NO
S120
YES
RESET COUNTER
S121
KEY DEVICE
S111'
KEY ?
NO
YES
S114'
OUTPUT RANDOM NUMBERS
S115'
READ DATA
S116'
PROCESS OR OPERATE INPUT DATA
S117'
OUTPUT RESULT
S118'
READ RESULT
S119'
MAKE OPERATION SIMILAR TO OPERATION OF STEPS S119 - S131 HOWEVR, NOT INFLUENCE MAIN UNIT TO RELEASE OF RESET STATE THEREOF

FIG.7B

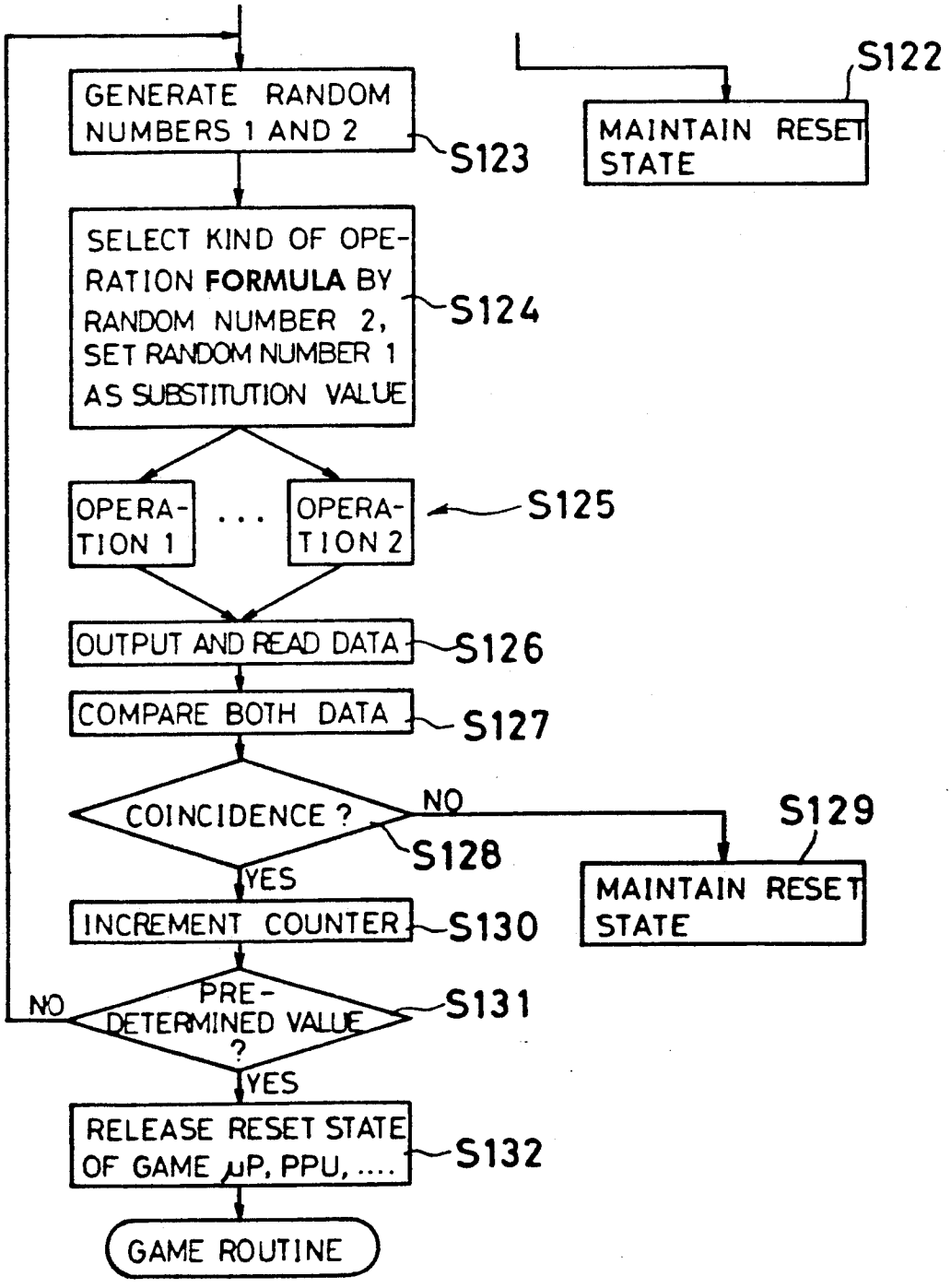

GENERATE RANDOM NUMBERS 1 AND 2
S123
SELECT KIND OF OPERATION FORMULA BY RANDOM NUMBER 2, SET RANDOM NUMBER 1 AS SUBSTITUTION VALUE
S124
OPERATION 1
...
OPERATION 2
S125
OUTPUT AND READ DATA
S126
COMPARE BOTH DATA
S127
COINCIDENCE ?
S128
NO
YES
S129
MAINTAIN RESET STATE
INCREMENT COUNTER
S130
PRE-DETERMINED VALUE ?
S131
NO
YES
RELEASE RESET STATE OF GAME μP, PPU, ...
S132
GAME ROUTINE
S122
MAINTAIN RESET STATE

FIG. 8

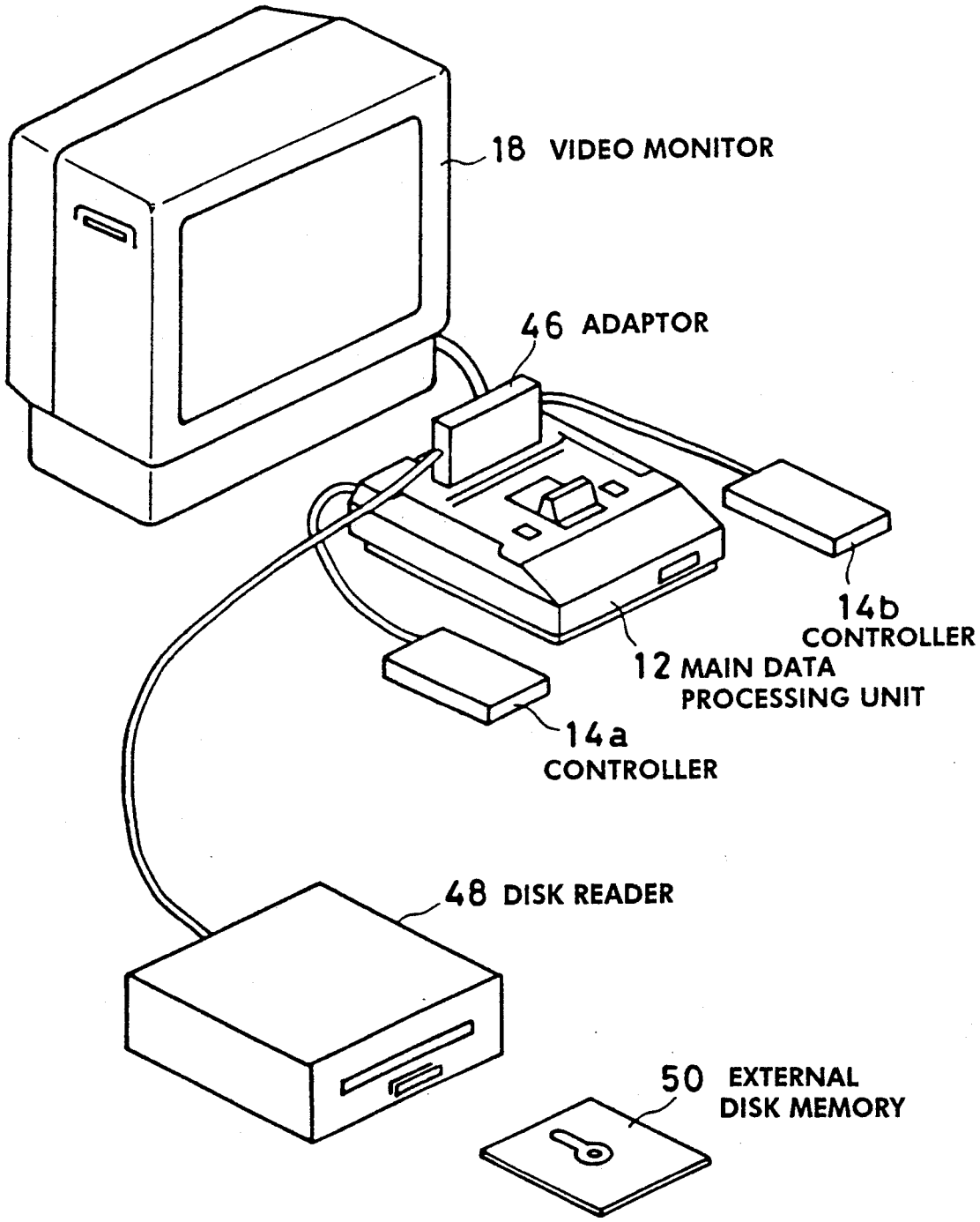

18 VIDEO MONITOR
46 ADAPTOR
14b CONTROLLER
12 MAIN DATA PROCESSING UNIT
14a CONTROLLER
48 DISK READER
50 EXTERNAL DISK MEMORY

FIG. 9

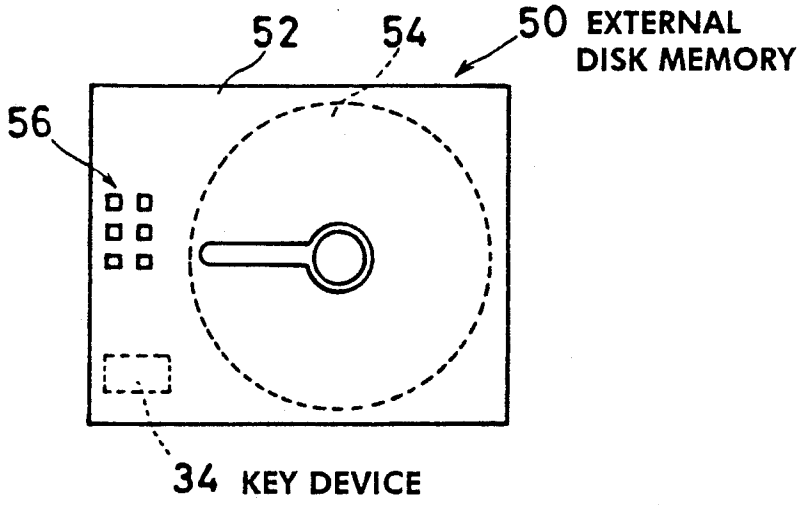
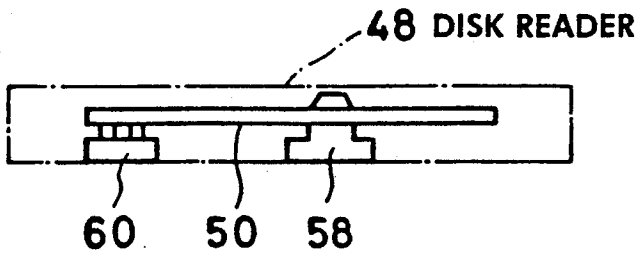

52
54
50 EXTERNAL DISK MEMORY
56
34 KEY DEVICE

FIG. 10


48 DISK READER
60
50
58

EXTERNAL MEMORY HAVING AN AUTHENTICATING PROCESSOR AND METHOD OF OPERATING SAME

This is a divisional application of application Ser. No. 812,929, filed Dec. 23, 1985, now U.S. Pat. No. 4,799,635.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a system for determining authenticity of software in an information processing apparatus. More specifically, the present invention relates to a system for determining whether software contained in an external memory, for example, ROM cartridge, floppy disk or the like, is authorized for use with a main processor unit.

2. Description of the Prior Art

Conventionally, such information processing apparatus are known wherein an external memory is loaded in a main processor unit and the main unit executes a predetermined program according to software contained in this external memory. One example of such a data processing apparatus is the "Nintendo Entertainment System (trade mark)" manufactured and sold by the assignee of the present application. The "Nintendo Entertainment System" which embodies the present invention includes a ROM cartridge, which is shown in the Nintendo publication distributed in the Fall of 1985 entitled "We're Changing the Face of Home Entertainment", copyright 1985. The identical ROM cartridge also is shown in U.S. design patent Des. 294, 020, filed Oct. 7, 1985. This ROM cartridge (external memory) is loaded into a front loading main processor unit (as is also shown in the 1985 Nintendo publication), the main processor unit is connected to a television receiver, and thereby various games can be enjoyed on the screen of the television receiver. A large number of software programs (ROM cartridges) are available for use in such, information processing apparatus. However, such authentic software programs are subject to being imitated and counterfeited and it is desirable to provide a system that enables data processing of only authentic program cartridges.

SUMMARY OF THE INVENTION

Therefore, a principal object of the present invention is to provide a system capable of determining authenticity of software contained in an external memory which is employed together with a main unit in an information processing apparatus. As used herein, authentic means that the software is genuine and authorized for use in the information processing apparatus.

Another object of the present invention is to provide a system for both determining authenticity of software contained in an external memory in an information processing apparatus and enabling data processing in accordance with such software only when it has been determined to be authentic.

An information processing apparatus in which the present invention may be used comprises a main processor unit and an external memory removably connected to this main unit, and wherein the external memory comprises a program (software) for operating the main unit. Associated with external memory is an active device for determining authenticity of the software, and this active device functions as a key device. Another active device is installed in the main unit, and this second active device functions as a lock device. By cooperation of the key device and the lock device, the information processing apparatus is enabled or disabled depending on the authenticity of the external memory which is installed in the main unit, and, if enabled, the apparatus executes a predetermined information processing program according to software contained in the external memory.

In accordance with the present invention, the main processor unit is not enabled unless an authentic external memory (software) is loaded, and therefore the use of a false (not authentic) external memory can be excluded effectively.

In a preferred embodiment in accordance with the present invention, duplicate semiconductor digital processing devices are used as the key device and the lock device. The two digital devices each execute a predetermined data processing program in synchronism. Then, the lock digital processing device compares the result of its processing with the result of the synchronous processing by the key device. In accordance with this preferred embodiment, the authenticity of the software of the external memory can be determined reliably by a simple arrangement of duplicate digital processing devices added to the main unit and the external memory, respectively.

These objects and other objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of the embodiments of the present invention when taken in conjunction with accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a perspective view showing one example of a video game machine as one embodiment of an information processing apparatus in accordance with the present invention.

FIG. **2** is a block diagram showing a circuit configuration of this embodiment.

FIG. **3** is a block diagram showing a circuit configuration of a lock device used in the systems of FIGS. **1** and **2**.

FIG. **4** is a timing chart for explaining operation of FIG. **3** device.

FIG. **5** is a flow chart for explaining the basic operation of the embodiment shown in FIG. **2**.

FIG. **6** shows the physical layout of FIGS. **6**A,B.

FIGS. **6**A,B are flow charts for explaining operation of FIG. **2** in further detail.

FIG. **7** shows the physical layout of FIGS. **7**A,B.

FIGS. **7**A,B are flow charts for explaining an alternative operation of a modified embodiment of FIG. **2**.

FIG. **8** is a perspective view showing another example of a video game machine as another embodiment of an information processing apparatus in accordance with the present invention.

FIG. **9** is an illustrative view showing one example of a floppy disk used for the FIG. **8** embodiment.

FIG. **10** is an illustrative view showing one example of an apparatus for reading data stored on the floppy disk of the FIG. **8** embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. **1** is a perspective view showing one example of a game machine as one embodiment of the information processing apparatus in accordance with the present

invention. Hereinafter, a description of the present invention is made with reference to the game machine shown in FIG. 1. However, it is noted that the present invention is applicable to a variety of information processing apparatus such as a computer, word processor, banking system or the like which employs an external memory, for example, in the form of a cartridge, floppy disk, card or the like.

A game machine **10** comprises a main processor unit **12**, and user controllers **14***a* and **14***b* are connected to this main unit **12**. A cartridge **16** is loaded into the main unit **12** as an external memory. As described in detail later, the cartridge **16** includes a ROM (Read Only Memory) storing a program written for the game machine. The main unit **12** develops a video signal for the game in response to signals from the controllers **14***a* and **14***b* and according to the program contained in the ROM of cartridge **16**, and sends this video signal to a television **18**. The user watches the picture on the screen of the television **18**, operates the controllers **14***a* and **14***b* as required, and thereby executes the game programmed in the ROM cartridge **16**.

In reference to FIG. 2, a connector **20** is installed in the game machine main unit **12**, and this connector **20** is engaged with a connector **22** of the cartridge **16**, and thereby the main unit **12** is connected electrically to the ROM contained in cartridge **16**.

A game microprocessor **24**, for example, the integrated circuit "Z80A" manufactured by Zilog, is mounted on a printed circuit board (not shown) contained in the main unit **12**, and the above-described controllers **14***a* and **14***b* and TV **18** are connected to this microprocessor **24** through an interface **26**.

A PPU (picture processing unit) **28**, an active semiconductor device **30** (lock) for determining the authenticity of the external ROM cartridge **16**, and a clock oscillator **32** are further included in the main unit **12**. The PPU **28** is composed, for example, of an integrated circuit "2C03" manufactured by Nintendo Co. Ltd, Kyoto, Japan, the assignee of the present application, for outputting a video information signal processed by the game microprocessor **24** as a television signal for the TV **18**.

The semiconductor device **30** (lock) is in this embodiment provided by a 4-bit microprocessor, for example, the integrated circuit "lONES" manufactured by Nintendo. A like semiconductor device **34** (key) is mounted on a support structure, such as the printed circuit board (not shown), of the cartridge **16**. A reset switch **36** is connected to the reset terminal R of the semiconductor device **30** (lock). A reset capacitor **38** is further connected to the reset terminal in parallel with the reset switch **36**. The reset capacitor **38** is charged when a power switch **40** (FIG. 1) is turned on, thereby performing a so-called initial reset (power-on-clear) which keeps the semiconductor device **30** in the reset state for a predetermined time.

A ROM **42** for storing the game program (software) and a ROM **44** for generating data defining characters for the game video are mounted on the printed circuit board of the cartridge **16**. This printed circuit board of the cartridge **16** is connected electrically to the printed circuit board of the main unit **12** through the two connectors **20** and **22** as described above.

A clock signal CL from the clock oscillator **32** is applied to semiconductor device **30** (lock) and also to the semiconductor device **34** (key) through connectors **20** and **22**.

As shown in FIG. 2, a predetermined terminal of the semiconductor device **30** is grounded, while a predetermined terminal of the semiconductor device **34** is connected to a power source Vcc. Thereby, these two semiconductor devices **34** and **30** are differently conditioned to assume the role of a key or a lock, respectively.

In order that the two semiconductor devices **30** and **34** exchange data with each other, the respectively corresponding terminals I, O and R are connected to each other through the connectors **20** and **22**. Also, as described above, the common clock Cl is applied to these two semiconductor devices **30** and **34** from the clock oscillator **32**. Accordingly, the two semiconductor devices **30** and **34** are operated so that the respective periods and phases of operation are synchronized completely with each other.

Further detailed description is now made of the semiconductor device **30** in reference to FIG. **3**. The semiconductor device **34** in the cartridge **16** has the same construction as device **30**, and therefore corresponding numbers are shown in parenthesis to avoid duplicate description.

As described above, the semiconductor devices **30** and **34** determined whether the cartridge **16** is authentic or not. The functions of these two semiconductor devices **30** and **34** can be compared to the relationship between a lock and a key. Accordingly, in the following description, the semiconductor device **30** is called a lock device and the semiconductor device **34** is called a key device.

In reference to FIG. **3**, the lock device **30** is composed, for example, of a 4-bit microprocessor, comprising a CPU **30***a* as a data processing means and a ROM **30***b* and RAM **30***c* as semiconductor memories. The ROM **30***b* stores an operating program for the CPU **30***a*, and two arithmetic routines are contained in this operating program. Thus, a plurality of formulas and data of random numbers for arithmetic computation according to such formulas are contained in one operating program. The operating program also includes a program routine for comparing the computation result of the lock device **30** with the result computed by the key device **34** and vice versa, and for determining whether the results agree. The CPU **30***a* of lock device **30** functions as a determining means when these comparison and determination routines are executed.

Furthermore, a control program routine for controlling reset or release of reset of the main unit **12** based on the results of the comparison and determination program routines is contained in the operating program.

An accumulator **30***d* is connected to the CPU **30***a*. A register **30***e* is connected to the ROM **30***b*. This register **30***e* is for temporarily storing the program data accessed from the ROM **30***b*. Furthermore, a frequency divider **30***f* for receiving the clock signal CL from the clock oscillator **32** (FIG. **2**) and dividing the frequency thereof is installed in the lock device **30**, and the ratio of frequency division of the frequency divider **30***f* is set, for example, to $\frac{1}{4}$. The CPU **30***a* executes sequential program steps in response to signals of respective phases $\phi 1$, $\phi 2$, $\phi 3$ and $\phi 4$ from the frequency divider **30***f*.

The CPU **30***a*, the accumulator **30***d* and the register **30***e* are connected by a data bus **30***g*. This data bus **30***g* is connected to an I/O port **30***h*, data is outputted from the I/O port **30***h* to the key device **34**, and data from the key device **34** is received through the I/O port **30***h*. Furthermore, two reset signals RESET **1** and RESET **2**

are outputted from the I/O port 30*h*. The reset signal RESET 1 is given to the key device 34 to reset it. The reset signal RESET 2 is given to the game microprocessor 24 and the PPU 28 which are contained in the main unit 12 to reset them. In order to release the reset states of the key device 34 and the main unit 12, these reset signals RESET 1 and RESET 2 have only to assume the opposite (inverse) state.

Next, a brief description is made on operation of the frequency divider 30*f* in reference to FIG. 4. As described above, the frequency divider 30*f* divides the frequency of the clock CL from the clock oscillator 32 by $\frac{1}{4}$. Accordingly, four signals $\phi 1$, $\phi 2$, $\phi 3$ and $\phi 4$ having different phases respectively are obtained from the frequency divider 30*f*. These signals $\phi 1$–$\phi 4$ are given to the CPU 30*a*. The CPU 30*a* performs operations in sequence in synchronism with these four signals $\phi 1$–$\phi 4$. For example, data from the I/O port 30*h* is read in synchronism with the signal $\phi 1$, and predetermined arithmetic operations (data processing) are performed in response to the signals $\phi 2$ and $\phi 3$. Then, data from the I/O port 30*h* is outputted by the final signal $\phi 4$.

Meanwhile, these signals $\phi 1$–$\phi 4$ are given also to the key device 34, and accordingly, the lock device 30 and the key device 34 are operated in complete synchronism with each other. Specifically, the lock device 30 and the key device 34 have the same number of steps in their operating programs and have the same architecture, including the same hardware and the same clock, and therefore the respective processing cycles coincide completely. Next, a brief description is made of the operation of the embodiment with reference to FIG. 5. Afterwards, a more detailed description of the operation is made with reference to FIG. 6.

First, the cartridge 16 is loaded into the main unit 12, and the power switch 40 (FIG. 1) of the main unit 12 is turned on to start the operation (step S1). In the following step S2, the lock device 30 outputs the reset signal RESET 2 and resets the game microprocessor 24 and the PPU 38 comprised in the main unit 12, holding this state. Thus, no game can be played when the main unit 12 is reset.

Next, in step S3, the lock device 30 is synchronized with the key device 34. A method of synchronization thereof is described in reference to FIG. 4. The machine cycle of the lock device 30 is set so that the reset signal RESET 1 given to the key device 34 from the lock device 30 is outputted between signal $\phi 4$ of certain period of the clock CL and the signal $\phi 1$ of the next period. Consequently, the signal $\phi 1$ is first inputted without fail to the key device 34. Consequently, the key device 34 can start operation from the same machine cycle $\phi 1$ as that of the lock device 30. Thus, in step S3 the lock device 30 is synchronized with the key device 34, and thereafter the respective devices 30 and 34 execute predetermined operations in complete synchronization.

Next, in step S4, predetermined arithmetic operations are performed respectively by the lock device 30 and the key device 34. At this time, the arithmetic operation performed by the lock device 30 and the arithmetic operation performed by the key device 34 are the same. Accordingly, if the cartridge 16 is authentic, the results of the two arithmetic operations performed in this step S4 will be the same.

In step S5, the above-described results of the operations are transferred mutually between the lock device 30 and the key device 34. Then, in step S6, the lock device 30 and the key device 34 compare these two arithmetic operation results respectively. In step S7, if it is determined that these two results coincide (agree, then) in step S8, the lock device 30 releases the reset signals RESET 1 and RESET 2, releasing the reset states of the key device 34 and the main unit 12.

Conversely, in step S7, if it is determined that the results do not coincide, then in step S9, the lock device 30 continues to output the reset signals RESET 1 and RESET 2, and accordingly, the reset states of the key device 34 and the main unit 12 are continued. The operator cannot play the game in this reset state.

Next, further detailed description of the operation is made with reference to FIG. 6. In reference to FIG. 6, if the cartridge 15 is loaded into the main unit 12 and the power switch 40 (FIG. 1) of the main unit 12 is turned on or the reset switch 36 is turned on, the resetting operation of the lock device 30 is performed, and this lock device 30 starts its operating sequence at step S10.

In the following step S11, the lock device 30 determines whether it functions as the lock or as the key. As explained in FIG. 2, this determination is performed by detecting whether the predetermined terminal is grounded or connected to the power source Vcc. In this case, the lock device 30 is determined to function as the lock, but in the case where the determination indicates a key function, for example, due to wiring error, malfunction or the like, an unstable state takes place and no operations are performed at all.

In step S11, when "YES" is determined, in step S12, the lock device 30 outputs the reset signal RESET 2 so that the main unit 12 cannot execute the game program, and the reset state of the main unit 12 is continued. The game microprocessor 24 and the PPU 28 (FIG. 2) are forced to the reset state and disabled until the reset is released in the later-described step S21. And, in this step S12, the reset signal RESET 1 is also outputted to reset the key device 34.

In the next step S13, the lock device 30 releases the reset state of the key device 34, and synchronizes the two devices 30 and 34 with each other as in the above-described step S3 (FIG. 5). Thereby, the two devices 30 and 34 are synchronized with each other, and thereafter the respective devices execute sequential program steps in complete synchronism.

When the reset state of the key device 34 is released in step S13, the key device 34 determines whether it functions as the lock or as the key in the next step S11'. The determination in this step S11' can be made by detecting whether the predetermined terminal of the key device 34 is grounded or connected to the power source Vcc as in the above-described step S11', an unstable state takes place and no operations are performed at all.

When "YES" is determined in step S11', then the operations in the following step S14' and the steps thereafter are executed.

On the other hand, in the lock device 30, the operations in step S14 and thereafter are executed after the step S13 is executed. Accordingly, in the lock device 30 and the key device 34, the very same operations are performed in synchronism, that is, in coincidence as a function of time.

First, the lock device 30 and the key device 34 output data representing random numbers from the respective program ROMs 30*b* and 34*b* (FIG. 3) in step S14 and in step S14'. Output of these random number data is performed using the very same random function. Also, the

conditions determining operation of the random function are the same for the two devices **30** and **34**. Accordingly, when the cartridge is authentic, the data of random numbers generated in the lock device **30** and the data of random numbers generated in the key device **34** should be the same.

Next, in steps **S15** and **S15'**, the lock device **30** and the key device **34** exchange data with each other, and read the data of random numbers generated by the counterpart, respectively. Then, in steps **S16** and **S16'**, the devices **30** and **34** perform the predetermined data processes or arithmetic operations based on the data of random numbers inputted from the counterpart. The arithmetic operations formula used for the first arithmetic operation in these steps **S16** and **S16'** is the same in the two devices **30** and **34**, and therefore the results of these operations become the same when the inputted data of random numbers are the same. Then, in steps **S17** and **S17'**, the lock devices **30** and the key device **34** output the results of arithmetic operations to the counterpart, respectively. Responsively, in steps **S18** and **S18'**, the two devices **30** and **34** mutually receive the results of arithmetic operation outputted from the counterpart. In this case, the lock device **30** and the key device **34** perform the same operation at the same timing, and therefore the results of operation from the counterpart are received at the same timing. Accordingly, in this embodiment, both coincidence of the results of arithmetic operations and coincidence of time that results are received are taken into account to determine authenticity of the cartridge.

Next, in step **S19**, the lock device **30** compares the result of its arithmetic operation against the result of operation produced by the key device **34**, determining whether or not they coincide. As a result of this comparison, if "NO" is determined in step **S20**, the lock device **30** in step **S22** holds the reset state of each circuit in the main unit **12**, namely, the game microprocessor **24** and the PPU **28**. Thereby, the main unit **12** is prevented from executing the game program.

Meanwhile, an alarm may be generated in response to a determination of non-coincidence instead of maintaining a hold of the reset states, or the processing may return to the initial state, namely, the step **S11**.

As a result of the comparison in step **S19**, if "YES" is determined in step **S20**, the lock device **30** releases the reset states of these circuits, namely, the game microprocessor **24** and the PPU **28** in the next step **S21**.

Subsequently, in step **S23**, the lock device **30** generates two data groups, a first and a second, of random numbers based on predetermined random function. Then, in step **S24**, the lock device **30** selects the kind of arithmetic operation formula using the second data of random numbers, and sets the first data of random numbers as the values to be substituted into the arithmetic operation formula. More specifically, in this embodiment, n (positive integer) kinds of arithmetic operation formulas are set in advance in the arithmetic operation program in the ROM **30***b* (FIG. 3), and from among these, an arithmetic operation formula is selected in response to the second data of random numbers. Subsequently, in step **S25**, the selected arithmetic operation is executed using the first and the second data of random numbers.

Operations in these steps **S19**–**S25** are also performed in the same manner at the same timing in the key device **34**. Then, the same random function for generating the first and the second data of random numbers as that used for the lock device **30** is also used in the case of key device **34**. Also, conditions for the random function for generating the first and the second data of random numbers is the same for the lock device **30** and the key device **34** as described above. Accordingly, if the cartridge **16** is authentic, the same arithmetic operation formula is selected for the two devices **30** and **34**, and the results of these arithmetic operations should be the same.

Next, in step **S26**, the lock device **30** passes the results of the arithmetic operation performed in step **S25** to the key device **34**, and also receives the results of the arithmetic operation performed by the key device **34**. A similar operation is performed in the key device **34**. Next, in step **S27** and **S28**, the lock device **30** compares and checks the results of the arithmetic operation by itself against the results of the arithmetic operation received from the key device **34** and determines whether or not they agree, i.e., coincide with each other.

If the cartridge **16** loaded in the main unit **12** is not authentic, the results of the arithmetic operations do not coincide, and therefore, in this case, the lock device **30**, in step **S29**, outputs the reset signal RESET **2**, maintaining the game microprocessor **24** and the PPU **28** of the main unit **12** in the reset state to stop their operations.

On the other hand, when the lock device **30** determines that the result of the arithmetic operation by itself and the result of the arithmetic operation received from the key device **34** coincide with each other, processing returns again to step **S24**, and thereafter the operations in steps **S24**–**S28** are repeated. In other words, in this embodiment, as long as the main unit **12** is operated, the second arithmetic operation program in steps **S24**–**S28** are executed repeatedly, and when a non-coincidence of the results of the arithmetic operations occurs even once, step **S29** is executed and operation of the main unit **12** is stopped.

In addition, the same operations as those in steps **S26**–**S29** are performed in the key device **34**. However, the key device **34** has no effect on resetting and releasing each circuit of the main unit **12** This is because no reset signal is outputted to the main unit **12** from the key device **34**.

As for the operation of the key device **34** corresponding to step **S29**, since chip-select terminal is normally installed in the ROMs **42** and **44** (FIG. 2), this chip-select terminal may be disabled. When the chip-select terminal is disabled, the game microprocessor **24** and the PPU **28** of the main unit **12** cannot access these ROMs **42** and **44**, and therefore continuation of the game operation becomes impossible.

Determination of authenticity of the external memory cartridge can be made only by checking the results of the first arithmetic operations in step **S16** and step **S16'**, but also in the above-described embodiment, the second arithmetic operations and determination of the results thereof in steps **S24**–**S28** are performed repeatedly as long as the main unit **12** is operated, and therefore the determination of authenticity of the cartridge **16** can be made nearly certain. Accordingly, in the case where a cartridge containing ROMs that are non-authentic copies of the ROMs **42** and **44** in the cartridge **16** or a cartridge containing ROMs storing similar programs are used, the software protection scheme cannot be defeated unless the same hardware as provided in the key device **34** is employed. Also, by using devices such as custom ICs or the like which are difficult to obtain

normally, such a protection can be made more complete.

Thus, the protection of programs (software) contained in the cartridge **16** can be made complete by installing the key device **34** for determining the authenticity of the cartridge **16** and determining how it cooperates with the lock device **30** of the main unit **12**, and accordingly any copied or forged cartridge, that is, a cartridge other than an authentic one is blocked from operating in unit **12**.

FIG. **7** is a flow chart showing a modified example of FIG. **6**. Nearly the same hardware as the embodiment in FIG. **6** is employed in this embodiment, and for this FIG. **7** embodiment, though not illustrated, a counter is formed in the RAM **30***c* of the lock device **30** and the RAM **34***c* of the key device **34** (FIG. **3**), respectively. Then, by utilizing this counter, the second arithmetic operation is repeated a predetermined number of times set by this counter.

The operations in steps **S110**–**S120** and **S111'**–**119'** of this FIG. **7** embodiment are the same as those in steps **S10**–**S20** and **S11'**–**S19'** (in FIG. **6**), and therefore duplicate description is omitted here.

If a coincidence of the results of the first arithmetic operations is determined in step **S120**, in FIG. **7** embodiment, the counter formed in the RAM **30***c* of the lock device **30** is reset in step **S121**. The second arithmetic operation is executed in the following steps **S123**–**S128** likewise in steps **S23**–**S28** in FIG. **6**. Then, if a coincidence of the results of the two arithmetic operations is determined in step **S128**, the lock device **30** increments the counter (not illustrated) formed in the RAM **30***c* in the next step **S130**. Then, in the next step **S131**, determination is made of whether or not the value of the counter is the predetermined value. If the counted value of the counter does not reach the Predetermined value, the lock device **30** repeats steps **S123**–**S130**.

Then, if "YES" is determined in step **S131**, that is, if the second arithmetic operation is repeated by the predetermined number of times, the lock device **30** releases the reset states of the game microprocessor **24** and the PPU **28** of the main unit **12** in step **S132** as in step **S21** in FIG. **6**.

In addition, in the embodiment in FIG. **7**, the second arithmetic operation is performed repeatedly by the predetermined number of times in steps **S123**–**S131**, wherein the number of times may be one.

If the results of the first arithmetic operations in steps **S114**–**S116** coincide, the main unit **12** is enabled immediately, and thereafter the second arithmetic operation as shown in steps **S123**–**S131** is repeated When "NO" is determined in step **S128** during the repetition, the main unit **12** is disabled, and if non-coincidence does not occur by repeating the second arithmetic operation, thereafter the main unit **12** may remain enabled until the power switch **40** (FIG. **1**) of the main unit **12** is turned off.

Furthermore, steps **S22** and **S29** in FIG. **6** and steps **S122** and **S129** in FIG. **7** may be modified as follows. Black screen data for wholly blackening the screen of the television receiver **18** and title data for displaying a game title are stored in advance in the ROM **42** of the cartridge **16**. Then, in the above-described step **S22** or **S29** and step **S122** or **S129**, a pulse-reset signal is outputted from the lock device **30**, and thereby the black screen and the title screen are displayed repeatedly in alternating fashion. Thereby the operator is informed that the cartridge **16** is not authentic

In addition, the ROM cartridge **16** is used for an external memory in the above-described embodiment. However, for external memory, a magnetic memory, for example, floppy disk, magnetic card or an optical memory, for example, optical disk or the like may be used in place of cartridge **16**.

FIG. **8** is a perspective view showing another embodiment in accordance with the present invention. This embodiment employs a floppy disk for an external memory. In the configuration of FIG. **1** embodiment, the floppy disk cannot be employed without modification, and therefore in the FIG. **8** embodiment, an adapter **46** is used which has the same shape as that of the cartridge **16** (FIG. **1**) and is made attachable and detachable to the main unit **12**. A disk reader **48** is connected to this adapter **46**. Then, a floppy disk **50** is loaded in this reader **48**. Accordingly, the program (software) written in advance to the floppy disk **50** is read by the reader **48**, and it is sent to the main unit **12** through the adapter **46**.

As shown in FIG. **9**, the floppy disk **50** comprises a case **52** and disc-shaped magnetic sheet **54** supported rotatably in the case **52**. Then, the key device **34** and an electrode **56** for connecting the key device **34** are formed in the case **52**.

As shown in FIG. **9**, inside the reader **48** receiving such a floppy disk **50**, a disk driver **58** is accommodated and also a contact **60** connected to the electrode **56** is installed. Accordingly, the key device **34** installed in the case **52** of floppy disk **50** is connected to the lock device **30** of the main unit **12** through the electrode **56** and the contact **60**.

In the embodiment in FIG. **8**, operation is executed following the program as shown in FIG. **6** or **7** by cooperation of the lock device **30** (FIG. **2**) comprised in the main unit **12** and the key device **34** in the floppy disk **50**, and thereby determination is made whether or not the floppy disk **50** is authentic.

Meanwhile, the lock device **30** (FIG. **2**) may be installed in the reader **48**, not in the main unit **12**. In this case, the reset signal will be given to the main unit **12** from the reader **48**.

Furthermore, in the case where a memory means is comprised in the apparatus itself which is connected to the adapter **46**, for example, in the case where a sound source apparatus comprising a synthesizer ROM or the like is connected, the key device **34** is installed in the adapter **46**, and the operation in FIG. **6** or FIG. **7** may be executed by this key device **34** and the lock device **30** built in the main unit **12**.

In addition, in the above-described embodiment, microprocessors are employed for the lock device **30** and the key device **34**. However, for these devices **30** and **34**, simpler digital arithmetic operation devices may be employed, and further more analog processors may be employed which perform analog processing in place of digital processing. Also, a digital circuit may be employed in either of the lock device **30** and the key device **34** and an analog circuit in the other device.

In the case where the analog circuit is employed, various configurations can be utilized other than the above-described analog processor. For example, determination of the authenticity of the external memory (software) may be performed by a coincidence of frequencies of the clock CL converted by both the lock device and the key device following the same program. Furthermore, pulse signals are outputted from the lock device **30** and the key device **34**, and the duty ratio of

the pulse signals is converted according to a predetermined program, and thereby authenticity can be determined by a coincidence of the duty ratios. Or, for example, determination may be made by a coincidence of levels of integrations of the same saw-tooth waves, and further deferential may be used. Or, authenticity of the external memory can be determined by determining coincidence of the results of analog processes performed by the two devices.

Although the present invention has been described and illustrated in detail, it is clearly understood that the same is by way of illustration and example only and is not to be taken by way of limitation, the spirit and scope of the present invention being limited only by the terms of the appended claims.

What is claimed is:

1. An external memory unit for removable connection to a main video game data processor unit having a video game processing means for executing videographics programs stored in said external memory unit, said video game processing means being capable of being reset, and a dedicated authenticating processing means for executing a first predetermined authenticating program to form an information processing apparatus, said external memory unit comprising:

means for storing a videographics program that is to be executed by said video game processing means;

external authenticating processing means for operating in accordance with a second predetermined authenticating program when said memory unit is connected to the video game data processor unit for verifying that said videographics program stored in said means for storing is authorized for execution by said video game processing means;

means, coupled to said external authenticating processing means and said means for storing, for connecting said external memory unit to said video game data processor unit; and

wherein said external authenticating processor means includes data transfer means coupled to said means for connecting for transferring data related to the results of the execution of said second authenticating program to said dedicated authenticating processing means, whereby the video game processor means in said main video game processor unit is reset unless the results of the execution of the second authenticating program exhibit a predetermined relationship with the results of the first predetermined authenticating program.

2. An external memory in accordance with claim 1, wherein said external authenticating processing means includes clock signal input means, coupled to said means for connecting, for receiving clock signals from said main video game data processor unit, wherein said external authenticating processing means further includes means responsive to said clock signal input means for executing a plurality of instructions in response to each received clock signal.

3. An external memory according to claim 2, wherein said means responsive to said clock signal input means includes frequency divider means for generating a plurality of timing signals each of which initiates the performance of a predetermined processing operation.

4. An external memory according to claim 3, wherein said external authenticating processing means includes means responsive to said plurality of timing signals for receiving data from said dedicated authenticating processing means in response to a first timing signal, for performing predetermined arithmetic operations in response to a second timing signal and for transferring data to said dedicated authenticating processing means in response to a third timing signal.

5. An external memory according to claim 1, wherein said data transfer means further includes input pin means, coupled to said means for connecting, for receiving data related to the results of the execution of said first predetermined authenticating program from said dedicated authenticating processing means and output pin means, coupled to said means for connecting, for transferring data related to the results of the execution of said second predetermined authenticating program to said dedicated authenticating processing means.

6. An external memory according to claim 5, wherein said data transfer means further includes reset pin means for receiving a reset related signal from said dedicated authenticating processing means, said external authenticating processing means including means responsive to said reset related signal for maintaining a reset state or releasing the reset state depending upon the state of the reset related signal.

7. An external memory according to claim 6, wherein said external authenticating processing means includes means responsive to said reset related signal from said dedicated authenticating processing means for releasing its reset state and for synchronizing its operation with the operation of the dedicated authenticating processing means.

8. An external memory according to claim 1, wherein said external authenticating processing means includes means responsive to a clock signal received from said main video game data processor unit for synchronizing its operations with predetermined operations performed by said dedicated authenticating processing means.

9. An external memory according to claim 1, wherein said external authenticating processing means includes a terminal having a predetermined voltage coupled thereto and further includes means responsive to detecting said predetermined voltage for determining the processing operations to be performed by said external authenticating processing means.

10. An external memory according to claim 1, wherein said external authenticating processing means includes means for generating at least one random number in accordance with a predetermined function.

11. An external memory according to claim 10, wherein said means for generating at least one random number includes memory means for storing data representing random numbers and means for reading out at least one random number in accordance with a predetermined function.

12. An external memory according to claim 10, wherein said external authenticating processing means further includes: means for outputting said at least one random number and transferring said at least one random number to said dedicated authenticating processing means via said means for transferring, means for receiving data generated by said dedicated authenticating processing means via said means for transferring; and means for performing predetermined processing operations on said data generated by said dedicated authenticating processing means.

13. An external memory according to claim 12, wherein said predetermined processing operations performed by said external authenticating processing means are performed in time coincidence with corre-

sponding processing operations performed in said dedicated authenticating processing means.

14. An external memory according to claim 12 wherein said external authenticating processing means further includes means for outputting the results of said predetermined processing operations and for transferring the results to said dedicated authenticating processing means.

15. An external memory according to claim 14, wherein said external authenticating processing means further includes means for receiving results of corresponding processing operations performed by said dedicated authenticating processing means.

16. An external memory according to claim 15, wherein said external authenticating processing means further includes means for comparing the results generated by said dedicated authenticating processing means with the results generated by said external authenticating processing means.

17. An external memory according to claim 16 wherein said external authenticating processing means further includes means, responsive to the detection of coincidence between the results generated by said external authenticating processing means and said dedicated authenticating processing means, for selecting at least a further arithmetic operation to be performed.

18. An external memory according to claim 17, further including means for storing indicia representing n arithmetic operations, where n is a positive integer, said means for selecting including, means for generating at least a first number and at least a second number, said at least a first number being used to select an arithmetic operation to be performed and said at least a second number being used to define variable values for said selected arithmetic operation.

19. An external memory according to claim 17, wherein said external authenticating processing means includes means for performing said further arithmetic operation and for outputting a result.

20. An external memory according to claim 19, wherein said further arithmetic operation performed by said external authenticating processing means is performed in time coincidence with a corresponding further arithmetic operation performed by said dedicated authenticating processing means.

21. An external memory according to claim 19, further including means for transferring the results of said further arithmetic operation to said dedicated authenticating processing means and for receiving the results of a corresponding further arithmetic operation from said dedicated authenticating processing means.

22. An external memory according to claim 21, wherein said external authenticating processing means further includes means for comparing the results of the further arithmetic operations performed by said external authenticating processing means and by said dedicated authenticating processor means.

23. An external memory according to claim 17, wherein said external authenticating processing means further includes means for repetitively performing further arithmetic operations.

24. An external memory according to claim 23, wherein said means for repetitively performing further arithmetic operations executes further arithmetic operations during the time period that said video game processing means executes said videographics program.

25. An external memory according to claim 22, wherein said external authenticating processing means includes means responsive to said means for comparing the results of the further arithmetic operations to prevent access to said means for storing a videographics program when the results do not coincide.

26. An external memory according to claim 23, further includes means for counting, and wherein said means for repetitively performing said further arithmetic operations continues performing further arithmetic operations until said means for counting reaches a predetermined value.

27. An external memory system for removable connection to a main data processor unit having a video game processor for executing video game programs stored in said external memory unit, said video game processor being capable of being reset, and a separate authenticating processor for executing a first predetermined authenticating program, said external memory system comprising:

an external memory for storing a videographics program that is to be executed by said video game processor associated with said main data processor unit;

an external authenticating processor for executing a second predetermined authenticating program when said external memory system is connected to the main data processor unit for verifying that said videographics program stored in said external memory is authorized for use in the main data processor unit;

a connector, coupled to said external authenticating processor and said external memory, for interconnecting said authenticating processors and for interconnecting said external memory to said video game processor; and

wherein said external authenticating processor includes a data transfer port for transferring data related to the results of the execution of said second predetermined authenticating program to said separate authenticating processor, whereby the video game processor in said main video game processor unit is reset unless the results of the execution of the second authenticating program exhibit a predetermined relationship with the results of the first predetermined authenticating program.

28. An external memory system in accordance with claim 27, wherein said external authenticating processor includes a clock signal input, coupled to said connector, for receiving clock signals from said main data processor unit, wherein said external authenticating processor executes a plurality of instructions in response to each received clock signal.

29. An external memory system according to claim 28, further including a frequency divider responsive to each received clock signal for generating a plurality of timing signals each of which initiates the performance of a predetermined processing operation.

30. An external memory system according to claim 29, wherein said external authenticating processor responds to said plurality of timing signals by receiving data from said separate authenticating processor in response to a first timing signal, by performing predetermined arithmetic operations in response to a second timing signal and by transferring data to said separate authenticating processor in response to a third timing signal.

31. An external memory system according to claim 27, wherein said data transfer port includes an input pin, coupled to said connector, for receiving data from said

separate authenticating processor, an output pin, coupled to said connector, for transferring data to said separate authenticating processor, and at least one reset pin for receiving a reset related signal from said separate authenticating processor, said external authenticating processor responding to said reset related signal by maintaining a reset state or releasing the reset state depending upon the state of the reset related signal.

32. An external system according to claim **31**, wherein said external authenticating processor responds to said related reset signal from said separate authenticating processor by releasing its reset state and by synchronizing its operation with the operation of said separate authenticating processor.

33. An external system according to claim **27**, wherein said external authenticating processor responds to a clock signal received from said main data processor unit for synchronizing its operation with the operation of said separate authenticating processor.

34. An external system according to claim **27**, wherein said external authenticating processor includes a terminal having a predetermined voltage coupled thereto, wherein said external authenticating processor is operable to detect said predetermined voltage and perform predetermined processing operations in response thereto.

35. An external system according to claim **27**, wherein said external authenticating processor is operable to generate at least one random number in accordance with a predetermined function.

36. An external system according to claim **27**, wherein said external authenticating processor is operable to perform predetermined processing operations in time coincidence with corresponding operations performed by said separate authenticating processor.

37. An external system according to claim **36** wherein said external authenticating processor is operable to output the results of said predetermined processing operations and to transfer the results to said separate authenticating processor.

38. An external system according to claim **37**, wherein said external authenticating processor is operable to receive results of corresponding processing operations performed by said separate authenticating processor and to compare its own results with the results generated by said separate authenticating processor.

39. In a video game processing apparatus including:

a main video data processor unit having:

a video game data processor for executing videographics programs and

a separate authenticating data processor for executing a first predetermined authenticating program; and

an external memory system removably connected to said main video data processor unit and having:

a memory for storing at least one videographics software program to be executed by said video game data processor, and

an external authenticating processor for executing a second predetermined authenticating program;

a method of operating the external memory system and the main video data processor unit to determine the authenticity of said external memory system comprising the steps of:

connecting said external memory system to said main video data processor unit;

placing said video game data processor in a reset state;

executing said first predetermined authenticating program by said separate authenticating processor to determine the authenticity of said external memory;

executing said second predetermined authenticating program by said external authenticating processor to determine the authenticity of said external memory;

transferring data relating to the results of the execution of said second predetermined authenticating program from said external authenticating processor to said separate authenticating processor;

comparing the results of the execution of said first and second authenticating programs;

releasing said video game data processor from said reset state and executing said at least one videographics software program by said video game processor if the results of the execution of the first authenticating program exhibit a predetermined relationship to the results of the execution of the second predetermined authenticating program; and

maintaining said video game data processor in said reset state if the results of the execution of said first authenticating program fail to exhibit a predetermined relationship to the results of the execution of the second predetermined relationship.

40. A method according to claim **39** further including the step of simultaneously transmitting clock signals to said separate authenticating processor and said external authenticating processor.

41. A method according to claim **39** further including the steps of:

inputting clock signals to said separate authenticating processor and said external authenticating processor; and

executing a plurality of instructions in said separate authenticating processor and said external authenticating processor in response to each received clock signal.

42. A method according to claim **41**, wherein said step of executing a plurality of instructions includes the steps of:

receiving data from said separate authenticating processor in response to a first timing signal,

performing predetermined arithmetic operations in response to a second timing signal; and

transferring data to said separate authenticating processor in response to a third timing signal.

43. A method according to claim **39**, wherein said step of transferring data includes the step of transferring data from said separate authenticating processor to said external authenticating processor and from said external authenticating processor to said separate authenticating processor.

44. A method according to claim **39** further including the step of synchronizing the operation of the external authenticating processor with the operation of said separate authenticating processor.

45. A method according to claim **39** wherein said steps of executing said first and second authenticating programs each includes the step of generating at least one random number in accordance with a predetermined function.

46. A method according to claim **45** wherein said step of generating at least one random number includes the step of storing random numbers in a memory device and reading out said random numbers in accordance with a predetermined function.

47. A method according to claim 46, wherein each of said external authenticating processor and said separate authenticating processor reads random data generated by the other processor and performs predetermined processing operations on such data.

48. A method according to claim 47, wherein said predetermined processing operations performed by said external authenticating processor are performed in time coincidence with corresponding operations performed by said separate authenticating processor.

49. A method according to claim 47 further including the steps of outputting the results of said predetermined processing operations and transferring the results to said other processor.

50. A method according to claim 49 further including the step of comparing the results generated by the separate authenticating data processing with the results generated by said external authenticating processor.

51. A method according to claim 50 further including the steps of selecting further arithmetic operations to be performed by said external authenticating processor and said separate authenticating processor in response to detecting coincidence between the results generated by said external authenticating processor and said separate authenticating processor.

52. A method according to claim 51 further including the step of:

storing indicia representing n arithmetic operations, where n is a positive integer, in a memory device associated with each of said external authenticating processor and said separate authenticating processor, and wherein said step of selecting includes, generating at least a first number and at least a second number, and using said at least a first number to select an arithmetic operation to be performed and using said at least a second number to define variable values for said selected arithmetic operation.

53. A method according to claim 51, wherein each of said external authenticating processor and said separate authenticating processor performs said further arithmetic operations and outputs a result.

54. A method according to claim 53, wherein said further arithmetic operations performed by said external authenticating processor are performed in time coincidence with a corresponding further arithmetic operation performed by said separate authenticating processor.

55. A method according to claim 53, wherein said steps of executing said first and second authenticating programs each include the steps of transferring the results of said further arithmetic operations from said separate authenticating processor to said external authenticating processor and transferring the results of said further arithmetic operations from said external authenticating processor to said separate authenticating processor.

56. A method according to claim 55 further including the step of comparing the results of the further arithmetic operations performed by said external authenticating processor with the results of said further arithmetic operation performed by said separate authenticating processor.

57. A method according to claim 51 further including the step of repetitively performing said further arithmetic operations.

58. A method according to claim 51, further including the step of counting the number of times said further arithmetic operations are repetitively performed and wherein said step of repetitively performing said further arithmetic operations is continued until a predetermined count is reached.

59. An external memory according to claim 16, wherein said external authenticating processing means includes means for performing further authenticating operations if said means for comparing indicates coincidence between the results generated by said external authenticating processing means and said dedicated authenticating processing means, whereby said external authenticating processing means is operable to perform further authenticating operations at the same time said videographics program is being executed by said video game processing means.

60. An external memory according to claim 1, wherein said external authenticating processing means includes means for performing authenticating operations while said videographics program is being executed by said video game processing means, whereby authenticating operations are performed during the execution of said videographics program without burdening the video game processing means.

61. An external memory system according to claim 38, wherein said external authenticating processor is operable to execute further authenticating operations if the results generated by said external authenticating processor means and said separate authenticating processor are identical, whereby said external authenticating processor is operable to perform further authenticating operations at the same time said videographics program is being executed by said video game processor.

62. An external memory system according to claim 27, wherein said external authenticating processor is operable to perform authenticating operations while said videographics programs is being executed by said video game processor, whereby authenticating operations are performed during the execution of said videographics programs without burdening the video game processor.

63. A method according to claim 50, further including the steps of releasing said video game processor from said reset state if said results coincide and performing further authenticating operations if said results coincide at the same time said videographics program is being executed by said video game processor.

64. A method according to claim 39, further including the step of continuing to execute said first and second authenticating programs while said videographics program is being executed by said video game processor, whereby authenticating operations are performed during the execution of said videographics program without burdening the video game processor.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,070,479

DATED : December 3, 1991

INVENTOR(S) : Nakagawa

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On page 1 of the patent, immediately following the citation of U.S. Patent No. 4,862,156 and before the "FOREIGN PATENT DOCUMENTS" title, insert the following references:

3,755,641	8/1973	Rackman	200/163
3,772,662	11/1973	Blair	360/60
3,818,190	6/1974	Silverman et al	235/382
3,839,736	10/1974	Hoshall	360/132
3,859,634	1/1975	Perron et al	235/382
3,934,122	1/1976	Riccitelli	340/825.34
4,095,791	6/1978	Smith et al	273/85G
4,117,605	10/1978	Kurland et al	435/319
4,120,030	10/1978	Johnstone	364/200
4,149,027	4/1979	Asher et al	174/52R
4,218,582	8/1980	Hellman et al	178/22
4,268,715	5/1981	Atalla	178/22
4,281,215	7/1981	Atalla	178/22.08
4,295,039	10/1981	Stuckert	253/380
4,352,492	10/1982	Smith	273/1GC
4,384,326	5/1983	Devchoudhury	364/200
4,386,773	6/1983	Bronstein	273/1E
4,430,728	2/1984	Beitel et al	364/900
4,432,067	2/1984	Nielsen	364/900
4,442,486	4/1984	Mayer	364/200
4,446,519	5/1984	Thomas	364/300

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,070,479

DATED : December 3, 1991

INVENTOR(S) : Nakagawa

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

(continued from page 1)

4,454,594	6/1984	Heffron et al	364/900
4,458,315	7/1984	Uchenick	364/200
4,462,076	7/1984	Smith, III	364/200
4,471,163	9/1984	Donald et al	178/22.08
4,492,582	1/1985	Chang et al	434/169
4,500,879	2/1985	Smith, III et al	340/739
4,562,306	12/1985	Chou et al	178/22.08
4,575,622	3/1986	Pellegrini	235/382
4,602,351	7/1986	Shimamura et al	365/52
4,670,857	6/1987	Rackman	380/4
4,680,731	7/1987	Izumi et al	364/900

On Page 1 of the patent, immediately following the citation of Japanese Patent No. 53-17849 and before the "Primary Examiner" line, insert the following reference:

0114522	1/1984	EPO

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,070,479
DATED : December 3, 1991
INVENTOR(S) : Nakagawa

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

(continued from page 2)

Column 15, lines 9, 15, 20, 28, 32, 37, and 42, delete "external system", and insert -- external memory system --.

Column 17, line 17, delete "processing" and insert -- processor --.

Column 18, line 6, delete "51" and insert -- 57 --.

Signed and Sealed this

Twenty-seventh Day of April, 1993

Attest:

MICHAEL K. KIRK

Attesting Officer

Acting Commissioner of Patents and Trademarks