



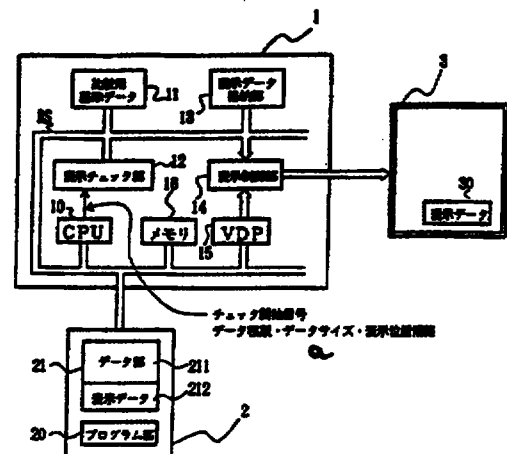
(51) 国際特許分類6 G06F 9/06, 12/14	A1	(11) 国際公開番号 WO96/24894 (43) 国際公開日 1996年8月15日(15.08.96)
(21) 国際出願番号 PCT/JP96/00251 (22) 国際出願日 1996年2月7日(07.02.96) (30) 優先権データ 特願平7/20132 1995年2月8日(08.02.95) JP (71) 出願人 (米国を除くすべての指定国について) 株式会社 セガ・エンタープライゼス (SEGA ENTERPRISES, LTD.)[JP/JP] 〒144 東京都大田区羽田1丁目2番12号 Tokyo, (JP) (72) 発明者: および (75) 発明者/出願人 (米国についてのみ) 大脇秀隆(OWAKI, Hidetaka)[JP/JP] 長嶋 毅(NAGASHIMA, Takeshi)[JP/JP] 彦山幸俊(KAGEYAMA, Yukitoshi)[JP/JP] 〒144 東京都大田区羽田1丁目2番12号 株式会社 セガ・エンタープライゼス内 Tokyo, (JP) (74) 代理人 弁理士 林 恒徳(HAYASHI, Tsunenori) 〒222 神奈川県横浜市港北区新横浜3-9-5 第三東昇ビル 3 階 林・土井国際特許事務所 Kanagawa, (JP)		(81) 指定国 AU, BR, CA, CN, JP, KR, MX, RU, <u>SG</u> , US, 欧州特許(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). 添付公開書類 国際調査報告書 9611703-1 IPOs' copy

(54) Title: INFORMATION PROCESSOR HAVING SECURITY CHECK FUNCTION

(54) 発明の名称 セキュリティチェック機能を有する情報処理装置

(57) Abstract:

Programs to be executed in an information processor and output data to be displayed are stored in an external storage device, and the information processor has a security check function for more reliably checking the authentication of the programs to be executed. The information processor, having a CPU for executing and controlling the programs, is connected to the external storage device and a display for displaying the output data. The output data stored in the external storage device is displayed on the display under the control of the program during its execution. The output data and reference comparison data stored in the information processor are compared with each other and when they do not coincide, the operation of the CPU of the information processor is interrupted to discontinue the execution of the program.



- 11 ... reference data for comparison
 12 ... display check portion
 13 ... display data storage portion
 14 ... display control portion
 16 ... memory
 20 ... program portion
 21 ... data portion
 212 ... display data
 a ... check start signal, data type, data size, display position information

(57) 要約

情報処理装置本体において実行すべきプログラムと表示すべき出力データが外部記憶装置に格納され、情報処理装置本体は、実行すべきプログラムの真偽性をより確実にチェックするセキュリティチェック機能を有する。プログラムを実行制御するCPUを有する情報処理装置本体は、外部記憶装置及び前記出力データを表示する表示装置に接続され、プログラムの実行中に、このプログラムの制御の下で外部記憶装置に記憶される前記出力データを表示装置に表示する。且つ出力データと、情報処理装置本体において記憶している基準比較データとを比較し、不一致の場合に、情報処理装置本体のCPUの動作を停止し、以降プログラムの実行を不能とする。

情報としての用途のみ

PCTに基づいて公開される国際出願をパンフレット第一頁にPCT加盟国を特定するために使用されるコード

AL	アルバニア	DE	ドイツ	LI	リヒテンシュタイン	PL	ポーランド
AM	アルメニア	DK	デンマーク	LC	セントルシア	PT	ポルトガル
AT	オーストリア	EE	エストニア	LR	レソト	PR	プエルトリコ
AU	オーストラリア	FI	フィンランド	LS	レソト	RU	ロシア
AZ	アゼルバイジャン	FR	フランス	LT	リトアニア	SE	スウェーデン
BA	ボスニア・ヘルツェゴビナ	GB	イギリス	LU	ルクセンブルグ	SG	シンガポール
BB	バルバドス	GG	ガイアナ	LV	ラトヴィア	SI	スロベニア
BE	ベルギー	GR	ギリシャ	MC	モナコ	SK	スロバキア
BG	ブルガリア	GU	グアム	MD	モルドヴァ	SN	セネガル
BJ	ベナン	HE	ヘンリクスランド	MG	マダガスカル	SS	スーダン
BY	ベラルーシ	IL	イスラエル	MK	マケドニア	TD	チュニジア
CA	カナダ	IS	アイスランド	ML	マリ	TG	トーゴ
CF	中央アフリカ共和国	IT	イタリア	MN	モンゴル	TM	トルクメニスタン
CG	コンゴ	JP	日本	MR	モーリタニア	TR	トルコ
CH	スイス	KE	ケニア	MW	マラウイ	TT	トリニダード・トバゴ
CI	コート・ジボアール	KR	韓国	MX	メキシコ	UG	ウガンダ
CM	カメルーン	KZ	カザフスタン	NE	ニジェール	UZ	ウズベキスタン
CN	中国			NL	オランダ	VN	ベトナム
CZ	チェコ共和国			NZ	ニュージーランド		

- 1 -

明 細 書

セキュリティチェック機能を有する情報処理装置

技術分野

- 5 本発明は、実行すべきプログラムの真偽性をチェックするセキュリティチェック方法、更にこのセキュリティチェック機能を有する情報処理装置、この情報処理装置に使用されるビデオ信号制御回路及びプログラム格納装置に関する。

10

背景技術

- マイクロプロセッサの高速化に伴い、各種形態の情報処理装置が提供され、且つこの情報処理装置において実行されるプログラムについても種々形式の媒体により提供されている。

15

- 特に、ビデオゲーム機器等の情報処理装置においては、実行されるゲームプログラムは、半導体読み取り専用メモリ（ROM）に記憶されてカートリッジに収納された形式、あるいはCD-ROMの形式で提供されることが多い。

20

- ここで、ビデオゲーム機器業界においては、ビデオゲーム機器本体とともにゲームプログラムの優劣により、その普及が左右される。したがって、優れたゲームプログラムが、正当な権限のない第三者により複写あるいは
- 25 、模倣され、販売される場合は、ゲームプログラムの開

- 2 -

発者利益を失わせるとともに、顧客の信頼を削ぐ事となる。

そこで、プログラムの真偽性をチェックし、不正なプログラムについては、情報処理装置において、実行を阻止するセキュリティチェック機能を備えることが提案され、且つ実施されている。

たとえば、従来例として米国特許4,442,486（以下486特許と略記する）、4,454,594（以下594特許と略記する）、4,462,076（以下076特許と略記する）あるいは日本国特許出願公開昭公報昭62-3331号（以下331号公報と略記する）等に記載の技術がある。

上記の486特許に記載される技術では、プログラムに特許或いは特許出願等の表示を瞬時間行うための表示信号を生成する内容を含ませ、当該瞬時間表示される内容が装置本体内に記憶している参照信号と一致するか否かにより、プログラムの真偽性を判断するようにしている。

また、594特許に記載される技術も、486特許に記載の技術と同様であり、プログラムを記憶する外部メモリの特定位置に記憶される内容を読み出し、この内容、例えば商標を表示し、次いで本体装置に記憶している参照データと一致するか否かを判断する。そして、これらが一致しない場合は、プログラムの実行が阻止される。

076特許に記載の技術は、上記486特許及び59

4 特許と同様であり、外部メモ리카ートリッジの所定アドレスのデータと本体側の参照データとを比較する。一方、実質的な外部メモリと本体側との接続を行う前に、権利の所有者情報を表示する。

- 5 その後、上記参照データの比較一致がある場合に、外部メモ리카ートリッジを真正なものとしてゲームの実行制御を行うようにしている。

更に、331号公報では、特に本体装置の本来の動作を開始する前に、外部記憶装置において、記憶された真偽判定のためのプログラムを実行させる。同時に本体装置においても真偽判定のためのプログラムを実行させる。これら双方の真偽判定のためのプログラム実行の結果が一致する場合に、本体装置の本来の動作を能動化させるものである。

- 15 このように従来の情報処理装置におけるセキュリティチェックは、ゲームプログラム等のプログラムの実行前にセキュリティコード等の一致を判断することにより行われている。そして、プログラムの実行が開始されると、プログラムの実行中は、セキュリティチェックを行わない、若しくは行い得ないものとなる。

このために、プログラムの一連の繋がりにおいて、セキュリティチェック処理のステップが何らかの方法により多くは、不正手段により、不能化されたり、バイパスされた場合には、その後のプログラムのステップの実行
25 がセキュリティチェックなしに可能となるものであった

。

更に、上記 4 8 6 特許、5 9 4 特許或いは 0 7 6 特許におけるセキュリティチェックの方法では、商標等の表示データを瞬時的に表示させているが、単に表示しているのみであり、実際に正しい商標等の画像が表示されているか否かの情報処理装置による判別は、行われていなかったし、行い得る構造ではなかった。

しかも、上記の通りセキュリティチェック処理のステップが何らかの方法により不能化されたり、バイパスされた場合には、所定のデータの表示が行われず、プログラムの真偽の判断が出来なくなるという問題が存在していた。

発明の開示

したがって、本発明の第一の目的は、情報処理装置において実行されるソフトウェア（プログラム）が真正なものか否かを確認することが容易、且つ確実である情報処理装置及びその方法を提供することにある。

更に本発明の第二の目的は、不正なプログラムの製作、販売を法的に確実に防止出来る情報処理装置及びその方法を提供することにある。

また、本発明の第三の目的は、出力データの画像もしくは音声による出力表示が外部記憶装置に記憶されているプログラムに基づくものであるとして、その出力表示が違法性を明示することを可能とする情報処理装置及び

その方法を提供することにある。

- 更にまた、本発明の第四の目的は、プログラムの真正を確認するセキュリティチェック処理をバイパスする不正行為を不能化することを防止し得る情報処理装置及び
- 5 その方法を提供することにある。

また、本発明の第五の目的は、セキュリティチェック処理の途中で不正な（真正でない）プログラムに置き換える不法行為を防止し、上記第四の目的をより確実にする情報処理装置及びその方法を提供することにある。

- 10 更に、本発明の第六の目的は、上記第一乃至第五の目的に適應する外部記憶装置を提供することにある。

- 上記第一の目的に対応する情報処理装置は、プログラム及び出力データが記憶された外部記憶手段と着脱自在に接続されるとともに、外部記憶手段から読み込んだ出力データを表示する出力手段に接続される情報処理装置
- 15 であって、外部記憶手段から読み込んだプログラムを実行するCPUと、基準比較データを記憶する内部記憶手段と、外部記憶手段から読み込んだ出力データと該基準比較データとを比較し、これらが不一致の場合にエラー
- 20 処理信号を発するセキュリティチェック手段とを有することを特徴とするセキュリティチェック機能を有する。

- また、上記第一の目的に対応するセキュリティチェック方法は、プログラム及び出力データが記憶された外部記憶手段からプログラム及び出力データを読み込む第一
- 25 のステップと、外部記憶手段から読み込んだプログラム

に含まれる表示チェック開始命令に基づき、チェック開始信号を出力する第二のステップと、チェック開始信号が出力される時、外部記憶手段から読み込んだ出力データと基準比較データとを比較し、これらが不一致の場合
5 にエラー処理信号を発する第三のステップと、エラー処理信号に基づき、プログラムの少なくとも一部の実行を阻止する第四のステップを有する。

かかる構成において、映像もしくは音声出力として出力表示される出力データがセキュリティチェックの比較
10 対象とされる。これにより真正でないプログラムの実行を確実に阻止することが可能である。

更に、第二の目的に対応する情報処理装置は、前記出力データが、この出力データの前記出力手段への表示が正当な権原を有しない者の使用を禁止し得るものである
15 ことを特徴とする。

また、上記第二の目的に対応するセキュリティチェック方法は、前記第三のステップにより、前記出力データと基準比較データとが一致する時に、前記出力データを表示する制御信号を発生し、更に、この制御信号に基づ
20 き出力データを表示する第五のステップを有することを特徴とする。

かかる構成により、出力データが商標等である場合、その表示が正当な権原を有しない者の使用を禁止し得るものであり、したがって不正なプログラムの製作、販売
25 を法的に禁止することが可能である。

更にまた、上記第三の目的に対応する情報処理装置は、前記基準比較データと比較される出力データを格納する出力データ格納手段を有し、出力データは前記外部記憶手段に記憶されたプログラムに従って、外部記憶手段
5 から出力データ格納手段に転送され格納される。

また、上記第二の目的に対応するセキュリティチェック方法は、前記第一のステップにより、前記外部記憶手段に記憶される出力データを、前記プログラムに従って、読み込むことを特徴とする。

10 かかる構成により、外部記憶装置に記憶されているプログラムに従って、出力データがデータ格納手段に転送され、格納されるので、出力データの出力表示が外部記憶装置に記憶されているプログラムによるものであり、違法性を明確化させることが可能である。

15 更に、上記第四の目的に対応する情報処理装置は、前記セキュリティチェック手段が、前記CPUの動作中に、前記出力データと基準比較データとの比較を繰り返して行うことを特徴する。

また、上記第四の目的に対応するセキュリティチェック方法は、前記第三のステップにより、前記出力データと基準比較データとの比較が前記プログラムの実行中に繰り返されることを特徴とする。

かかる構成により、プログラムの実行中にセキュリティチェックのための比較が繰り返し実行されるので、セ
25 キュリティチェックをバイパスする等の不正行為を防止

できる。

また、上記第五の目的に対応し、情報処理装置は、前記出力データが、前記セキュリティチェック手段によるデータ比較が行われる前に前記外部記憶手段から前記出力データ格納手段に転送され記憶され、セキュリティチェック手段によるデータ比較及び前記出力手段による出力表示の後、該出力データ格納手段から消去される。

上記第五の目的に対応するセキュリティチェック方法は、前記第五のステップによる出力データの表示の後に、読み込んだ該出力データを消去する第六のステップを有する。

かかる構成により、繰り返しの比較チェックのために新たに出力データを読み込むことが必要となる。したがって、セキュリティチェック処理の途中で不正な（真正でない）プログラムに置き換える不法行為が防止され、上記第四の目的をより確実に達成する。

更に、本発明の第六の目的に対応する情報処理装置に着脱自在に接続される外部記憶装置では、情報処理装置において実行されるプログラムと、情報処理装置により表示制御される出力データを有し、出力データはこのプログラムに従って、情報処理装置への読み込みが制御される。

かかる構成により、外部記憶装置は、上記第一乃至第五の目的に適応可能となる。

図面の簡単な説明

図 1 は、本発明の実施例ブロックである。

図 2 は、表示制御部の構成例を示すブロックである。

図 3 は、CPU の動作フローである。

5 図 4 は、表示チェック部の動作フロー（その 1）である。

図 5 は、表示チェック部の動作フロー（その 2）である。

図 6 は、表示制御部の制御部の動作フローである。

10 図 7 は、表示データ格納部の構成例ブロックである。

図 8 A、図 8 B は、表示データの説明のための図であり、図 8 A は表示パターンの一例を示し、図 8 B は、当該表示パターンに対応するメモリの bit 情報を示す。

15 図 9 は、カラー表示データの表示方法を説明する図である。

図 10 は、本発明の他の実施例であるビデオ信号制御回路の構成を示す図である。

20 図 11 は、図 10 のビデオ信号制御回路により表示制御されるセキュリティチェックのための表示ロゴの一例を示す図である。

発明を実施するための最良の形態

以下、好ましい実施例を図面に従い説明する。尚、図において、同一または類似の部分には、同一の参照番号
25 または記号を付して説明する。

- 1 0 -

図 1 は、本発明の一実施例の構成ブロック図であり、
実施例として情報処理装置をゲーム機に適用した場合に
ついて示す。図において、1 は、情報処理装置本体とし
てのゲーム機本体であり、バス B S を通して C P U 1 0
5 、比較用基準データ格納メモリ 1 1、表示チェック部 1
2、表示データ格納部 1 3、表示制御部 1 4、ビデオデ
ィスプレイプロセッサ (V D P) 1 5 及び作業用メモリ
1 6 が接続されている。

2 は、外部記憶装置としてのゲームカートリッジであ
10 り、コネクタによりゲーム機本体 1 と着脱可能に接続さ
れる。ゲームカートリッジ 2 は、内部に R O M を収納し
、ゲーム実行のためのデータ格納領域 2 1 とゲームプロ
グラム格納領域 2 0 を有している。

尚、以下の説明において、ゲームカートリッジ 2 及び
15 内部に収容される R O M として説明するが、これは C D
駆動装置及び C D - R O M に置き換えることも可能であ
る。

データ格納領域 2 1 は、主にゲーム実行時に表示され
るキャラクタ等のデータを格納するデータ部 2 1 1 と、
20 本発明にしたがいセキュリティチェックのために表示さ
れる表示データを格納する表示データ部 2 1 2 を有する
。

ここで、表示データは、後に説明するようにゲーム機
本体 1 で使用される真正なプログラムであることを意味
25 するデータであり、例えばゲーム機本体 1 の製造者の商

- 1 1 -

標等の画像に関するデータ、あるいは、音声による表示データである。

また、必要に応じてより高いセキュリティ性を持たせるために表示データを圧縮して格納することも可能である。

更に、ゲームプログラム格納領域 20 に記憶されるゲームプログラムには、その一部として、本発明にしたがい、CPU 10 の制御の下に、少なくとも表示データ部 212 から表示データを読み出し、ゲーム機本体 1 の表示データ格納部 13 に転送し記憶させる制御命令が含まれている。

上記のように表示データを圧縮して表示データ部 212 に格納する場合は、この圧縮表示データを解凍するための解凍プログラムがゲームプログラム格納領域 20 にゲームプログラムの一部として格納されてもよい。また、ハードウェアにより解凍を行う場合は、ゲーム機本体 1 もしくは、ゲームカートリッジ 2 に解凍回路を設ける構成とすることが可能である。

図 1 において、更に 3 は表示装置である。表示装置 3 は、ゲーム機本体 1 の表示制御部 14 からの映像信号を受け、表示部に所定の表示を行う。特に、本発明にしたがいゲームカートリッジ 2 から読み出し、転送記憶した表示データ 30 が表示装置 3 の所定位置に表示される。

尚、以下実施例において、本発明のセキュリティチェックのための表示データの表示を画像として表示装置 3

- 1 2 -

に表示する場合を例に説明するが、本発明はこれに限定されない。

即ち、先に説明したように、ゲーム機本体 1 で使用される真正なプログラムであることを意味するデータとして映像データの他、音声データも含まれる。したがって、音声データである場合は、音声出力によりデータが表示されることは、言うまでもない。

表示制御部 1 4 の詳細と、表示装置 3 を含む本発明にしたがう表示データ 3 0 を表示するための構成が、更に図 2 に示される。図 2 において、表示制御部 1 4 は、制御部 1 4 0、セレクト 1 4 1 及び D/A 変換回路 1 4 2 を有して構成される。

図 3 乃至図 6 は、それぞれ CPU 1 0、表示チェック部 1 2 及び表示制御部 1 4 の制御部 1 4 0 の動作フローである。以下これらの動作フローを参照しながら、図 1、図 2 の詳細について更に説明する。

図 3 において、ゲームの開始に際し、ゲーム機本体 1 の図示しない電源スイッチが投入されると（ステップ S 1）、CPU 1 0 は、ゲームカートリッジ 2 のプログラム格納領域 2 0 からゲームプログラムを読み込み、ゲーム処理を行う（ステップ S 2）。

CPU 1 0 に読み込まれたゲームプログラムには、所定タイミングで表示チェック開始を指示する命令が含まれている。したがって、CPU 1 0 はこの表示チェック開始命令の有無をチェックする（ステップ S 3）。

ここで、表示チェック開始のタイミングは、システムとして任意に設定可能である。例えば、ゲーム進行の過程でのゲームシーンの切り替わり時を表示チェック開始のタイミングとしてゲームプログラムに命令を記述しておくことが可能である。

表示チェック開始の命令があると（ステップ S 3 : Yes）、CPU 10 は、読み込まれたゲームプログラムに記述される格納命令を実行する（ステップ S 4）。即ち、ゲームプログラムの格納命令にしたがい、ゲームカートリッジ 2 の表示データ格納領域 21 から表示データを読出し、表示データ格納メモリ 13 に転送し、記憶する。

次いで、CPU 10 は、表示チェック部 12 にチェック許可信号を出力する（ステップ S 5）。このチェック許可信号には、チェック開始信号、データ種類、データサイズ、表示位置情報が含まれている。

CPU 10 からのかかる動作が、ゲームが終了するまで繰り返される（ステップ S 6）。

ここで、データ種類は、比較用基準データメモリ 11 に予め複数種の基準データが記憶されており、その内の一種の種類の基準データを特定する情報である。データサイズは、表示データ 30 を表示装置 3 に表示する際に、そのサイズを可変に出来る機能を有している場合に、そのサイズを指定する情報である。

更に、表示位置は、表示データ 30 を表示装置 3 に表

示する際に、その表示位置を可変にできる機能を有する時、その表示位置を指定する情報である。

図 4 は、チェック開始信号、データの種別、データサイズ、表示位置情報が含まれるチェック許可信号を CPU 10 から受ける表示チェック部 12 の第一の動作フローである。

表示チェック部 12 は、基本構成として、タイマーカウンタ機能と比較回路機能を有する専用のロジック回路あるいは、CPU により構成される。ゲーム機本体 1 の電源が投入されると動作を開始し、タイマーカウンタの計数をスタートする（ステップ S 20）。

表示チェック部 12 をロジック回路で構成する場合は、CPU 10 からのチェック許可信号の入力をトリガとしてセキュリティチェック（データ比較）のための比較論理が求められる。また CPU で構成する場合は、データ比較プログラムをゲーム機本体 1 の ROM（図 1 においては、図示省略されている）に格納しておき、CPU 10 からのチェック許可信号の入力をトリガとして、表示チェック部 12 において、このデータ比較プログラムを実行してセキュリティチェック（データ比較）が行われる。

ついで、タイマーカウンタがウォッチドグタイマーの機能を果たし、所定計数値、即ち所定時間が経過したか否かが判断される（ステップ S 21）。

タイマーカウンタが所定計数値まで既に到達している

場合には、所定期間においてCPU 10が、ゲームカートリッジ2のプログラム格納領域20から正しくプログラムを読み出せないことを示す。あるいは、プログラムが真正のものではなくプログラムにセキュリティ解除ルーチンを有してなく、またはセキュリティを解除するキーデータ（表示データ）を有していないためにセキュリティを正当に解除できない状態にあることを示す。

この場合は、エラー処理の対象となる（ステップS28）。エラー処理の対象となる場合は、それ以降セキュリティチェックは行われず、表示チェック部12はエラー処理信号として例えば、CPU 10に対してホルト信号を発する。これによりCPU 10は動作を停止し、ゲームプログラムの実行が不能となる。

一方、ステップS21の判断において、タイマーカウンタが所定計数値に到達していない場合は、CPU 10から許可信号が送られているか否かが判断される（ステップS22）。CPU 10から許可信号が送られていない場合は、継続してタイマーカウンタが計数アップされる（ステップS23）。

20 一方、許可信号が送られている場合は、セキュリティチェックが開始される（ステップS24）。ここで、セキュリティチェックは、本発明にしたがい次のように行われる。

図1において、ゲームカートリッジ2に収容されるROM内のプログラム格納領域20に記憶されるゲームプ

- 1 6 -

プログラムに含まれる命令により、CPU 10は、表示データ部 212の表示データを読み出し、RAMで構成される表示データ格納部 13に転送記憶する。

同時に、CPU 10は、ゲームプログラムに含まれる
5 チェック開始命令に基づき、データ種類、データサイズ、表示位置情報を含むチェック開始信号を表示チェック部 12に送る。

データ種類、データサイズ、表示位置情報の意義は、既に説明した通りである。更に、表示データは、たとえ
10 ば、同じ意味のセキュリティの表示であっても、ゲーム機器が使用される国の言葉に対応して表示することが必要である場合がある。

このために、データ種類は、当該ゲームカートリッジ
2の表示データ部 212に記憶される表示データが、異なる国の言葉に対応する複数種の表示データのいずれであるかを指定する情報をも含む。したがって、ゲーム機
15 本体 1のROMで構成される比較基準データ格納部 11には、複数種の比較基準データが記憶されている。

ここで、表示チェック部 12から表示制御部 14に出
20 力される表示データの内、特にデータサイズ及び表示位置データは、これを不正に操作することにより、目視できないサイズや画面に表示しきれないサイズにしたり、表示装置 3の有効画面外に表示位置を移動することが可能である。

25 このためにリミッタを設け、かかるデータサイズ及び

表示位置に対する不正操作を防止することが望ましい。
このリミッタの設定により、表示装置 3 の画面に収まり
切れない過大なデータサイズや目視可能な最小のデータ
サイズに満たないデータサイズが表示チェック部 12 か
5 ら出力された場合に、これを表示装置 3 の画面内に収ま
り目視可能な適当なデータサイズに置き換える機能を有
する。

図 4 の動作フローに戻ると、表示チェック部 12 にお
いて、CPU 10 から送られるデータ種類が特定する比
10 較基準データを比較基準データ格納部 11 から読出し、
表示データ格納部 13 に転送記憶された表示データとの
比較チェックが開始される（ステップ S 24）。

比較チェックの結果、比較基準データと表示データ格
納部 13 に転送記憶された表示データが一致しない場合
15 は、ゲームカートリッジ 2 は、真正なものとは判断され
ず、エラー処理（ステップ S 28）の対象となる。

このエラー処理は、先に説明したタイマーカウンタが
所定計数値に到達している場合（ステップ S 21 : Y e
s）の処理と同様であり、強制的に CPU 10 の動作を
20 停止する。これにより、以降のゲームプログラムの実行
が阻止される。

一方、比較チェックの結果、比較基準データと表示デ
ータが一致する場合は、ゲームカートリッジ 2 は、真正
なものと判断される。次いで、表示データ格納部 13 に
25 転送記憶されている、ゲームカートリッジ 2 の表示デー

タ領域 2 1 2 からの表示データが所定時間経過後に消去される（ステップ S 2 6）。

このように表示データが消去されるのは、次の理由にある。表示データを消去しない場合は、最初に表示データが表示データ格納部 1 3 に格納されると、それ以降何度セキュリティチェック（データの比較）を繰り返しても常にチェック結果は、「データの一致」ということになる。

したがって、本発明に従い、プログラムの実行中に繰り返しセキュリティチェックをする意義がなくなる。その結果、途中で何らかの不正行為により、不正な（真正でない）プログラムが実行される虞がある。これにより、上記の通り表示データの消去により、かかる不正行為を禁じることが可能である。

15 尚、この表示データの消去は、データ比較で一致が確認されてからモニタ画面で遊戯者がその表示を容易に確認できる程度の所定時間経過後に行われる。また、表示データの消去は、プログラムの改ざん等による抜け道をより確実に防止するために、専用の回路を本体装置 1 側に設け、ハード的に強制に行われることが好ましい。

ここで、上記の表示データの消去は、表示データ格納部 1 3 に格納された表示データをクリアーすること即ち、オール“0”のパターンを書き込みことにより、あるいは、先に格納されている表示データと異なるパターンのデータを
25 のデータを書き込むことにより可能である。

更に、上記の表示データの消去の際、タイマーカウンタがリセットされ（ステップS27）、フローの始まり（ステップS20）に戻り、タイマーカウンタの初期値からのカウントを再開始する。

- 5 従って、タイマーがタイムアップする前にセキュリティチェックが繰り返し実行され、表示データと比較基準データとが一致している間は、エラー処理（ステップS28）が行われることはない。逆に、タイムアップ前に
- 10 チェック許可信号がなければ、不正プログラムと判断され、エラー処理が行われる。

以上説明した実施例においては、チェック許可信号がCPU10から表示チェック部12に送られる都度、所定時間内に繰り返し、セキュリティチェックが行われる。

- 15 尚、図4の動作フローでは、ステップS21において、タイマーカウンタが所定値に到達している場合には、ただちにエラー処理（ステップS28）を行うようにしている。これに対して、図5に示す別の実施例動作フローのように、タイマーカウンタが所定値に到達している
- 20 場合であってもチェックを開始し（ステップS24）、表示データの一致判断（ステップS25）を行うようにしてもよい。

- 真正でないゲームプログラムにより、タイマーカウンタが所定値に到達している場合は、セキュリティチェックの結果においても、表示データの一致とはならず
- 25

- 2 0 -

ラー処理（ステップ S 2 8）を行うことになる。他の動作については、図 4 の動作フローの実施例と同様である。

ここで、上記の通り、表示チェック部 1 2 における比較基準データと表示データとの比較チェックの結果が、両者が一致するものである場合、ゲームカートリッジ 2 に格納されるゲームプログラムは、真正なものと見做される。

一方、ゲームプログラム自体が不法にコピーされたものである場合も、上記の表示チェック部 1 2 における比較結果は、両者が一致するものとなる。したがって、かかる場合も後に続くゲームプログラムの実行が可能となる。

しかし、この場合は、表示データを表示装置 3 に表示させること自体が、正当な権原を有しない者に対し、禁止しうるもの、例えば、商標等の表示データとすることにより、不法なコピー行為を禁止することが可能となる。

何故ならば、正当な権原を有しない者による商標等の表示データを表示装置 3 に表示させる行為は、明らかな商標等に基づく権利侵害となるからである。

図 6 は、表示制御部 1 4 内の制御部 1 4 0（図 2 参照）の動作フローである。先に図 1 に関して説明したように、CPU 1 0 から表示チェック部 1 2 に対し、チェック開始信号が送られる際に、データ種類、データサイズ

、表示位置情報が送られる。

表示チェック部 1 2 は、チェック開始信号に基づき表示オン／オフ信号とともにデータサイズ、表示位置情報 1 2 0 を表示制御部 1 4 内の制御部 1 4 0 に送る。表示
5 制御部 1 4 は、表示データ格納部 1 3 からの表示データを映像信号 1 3 0 として入力する。

更に、表示制御部 1 4 は、ビデオディスプレイプロセッサ (VDP) 1 5 からゲーム画像データを映像信号 1 5 0 として入力する。表示制御部 1 4 において、表示デ
10 ータ格納部 1 3 からの映像信号 1 3 0 と VDP 1 5 からの映像信号 1 5 0 は、セクタ 1 4 1 に入力される。

ここで、本発明と直接に関連しないので、ビデオディスプレイプロセッサ (VDP) 1 5 の詳細な構成及び動作の説明は、省略するが、既存のビデオゲーム装置にお
15 いて使用される周知構成のデバイスであり、CPU 1 0 に対し、I/O デバイスとして存在する。レジスタ、カラー RAM、スクロール量設定 RAM 等を有し、これらとともに更に外部に付属されるビデオ RAM を制御する制御ブロックを有して構成され、表示装置 3 に表示され
20 るビデオ画像データを合成して映像デジタル信号として出力する。

また VDP 1 5 からは、垂直、水平同期信号 1 5 2 が映像デジタル信号と同期して出力され、制御部 1 4 0 に入力される。制御部 1 4 0 は、表示チェック部 1 2 から
25 の表示オン／オフ信号に基づき、同期信号 1 5 2 に同期

- 2 2 -

してセレクト信号 1 4 3 を出力する。

このセレクト信号 1 4 3 は、セクタ 1 4 1 に入力され、映像信号 1 3 0 と 1 5 0 を切替え出力するためのものである。この切替え動作は、図 6 の動作フローに対応して説明される。

まず、制御部 1 4 0 は、表示チェック部 1 2 からの表示オン／オフ信号がオンか否かを判断する。表示オン／オフ信号がオンである場合は、表示データ格納部 1 3 からの表示データの映像信号を表示するタイミングであるか否かが判断される（ステップ S 3 1）。

このステップ S 3 1 における判断は、表示チェック部 1 2 からの表示データのデータサイズ、表示位置信号 1 2 0 に基づき且つ、VDP 1 5 からの同期信号 1 5 2 をもとに表示データの表示タイミングか否かが判断される。

表示データの表示タイミングである場合は、セレクト信号 1 4 3 により表示データ格納部 1 3 からの表示データの映像信号 1 3 0 が選択される（ステップ S 3 2）。一方、表示データの表示タイミングでない場合は、セレクト信号 1 4 3 により VDP 1 5 からの映像信号 1 5 0 が選択される（ステップ S 3 3）。

このようにして、セレクト信号 1 4 3 により選択され、セクタ 1 4 1 から表示データの映像信号 1 3 0 及び VDP 1 5 からの映像信号 1 5 0 が出力され、次いで D/A 変換回路 1 4 2 に入力する。

D/A変換回路142は、デジタル信号である映像信号130及び映像信号150をアナログ映像信号144に変換する。そしてこの変換されたアナログ映像信号144は、同期信号152とともに表示装置3に入力され、所定の表示が行われる。

尚、上記ステップS32において、表示チェック部12からの表示データの表示タイミングと、表示チェック部12におけるセキュリティチェック（データの比較）とは、必ずしも一対のものである必要はない。表示チェック部12におけるセキュリティチェックは、比較的短時間の間隔で行い、画面の表示は、その表示をしても支障の無い時に、表示チェック部12におけるセキュリティチェック後に表示するようにしてもよい。

この制御のためには、例えば、表示チェック部12において、表示制御部14に送る表示オン/オフ信号120の送出タイミング、あるいは表示制御部14の制御部140からのセレクト信号143の出力タイミングを予め所定の制御周期に設定することにより可能である。

図7乃至図9は、表示データの一例に基づき、表示データ格納部13の構成及び表示データの表示方法を説明する図である。

図7に示すように表示データ格納部13は、RAMで構成されるメモリ131とシフトレジスタ133で構成される。メモリ131は、表示チェック部12からのアドレス信号120が順次入力される。シフトレジスタ1

- 2 4 -

3 3 には、表示チェック部 1 2 からのラッチ信号及びシフト信号 1 2 1 が入力される。

ここで、今、図 8 A に示すように、表示データのパターンが "S" である場合を考える。図 8 A の 7 ~ 0 ビットとアドレス 0 ~ 7 によって特定される 6 4 画素で構成される 8 × 8 のマトリクスの範囲が表示データ領域である。

この 8 × 8 のマトリクスの範囲中、黒点により表示データのパターン "S" が表されている。この表示パターンに対応して、メモリ 1 3 1 のビット情報が図 8 B のように表される。即ち、表示データのパターン "S" を形成する黒点に対応して、メモリ 1 3 1 の対応するビット位置は、"1" にセットされている。

図 7 に戻り、表示チェック部 1 2 からアドレス 1 2 0 として、アドレス信号 (3) がメモリ 1 3 1 に入力する場合を考えると、メモリ 1 3 1 の対応するアドレスのビット情報即ち、"0 0 1 0 0 0 0 0" がデータ 1 3 2 として読み出される。

これが表示チェック部 1 2 からのラッチ信号によってシフトレジスタ 1 3 3 にラッチされ、ラッチされたデータ 1 3 2 は表示チェック部 1 2 からのシフト信号によって 7 ビット目を先頭に順次 1 ビットずつ表示制御部 1 4 に映像信号 1 3 0 として送られる (図 7、1 2 1 参照)。

この映像信号 1 3 0 は、表示制御部 1 4 において、す

でに説明したようにセクタ 1 4 1 を通して表示装置 3 に表示データ 3 0 として表示される。

図 9 は、表示データをカラー表示する場合の表示データ格納部 1 3 のメモリ 1 3 1 とシフトレジスタ 1 3 3 の構成を説明する図である。表示データを構成する各ビットに対し、R : G : B の組み合わせで所定の色が表示される。

したがって、図 8 B のビット情報を R : G : B 用に 3 枚のメモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B として用意する。更に、シフトレジスタ 1 3 3 は、3 枚のメモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B のそれぞれに対応してシフトレジスタ 1 3 3 - R、1 3 3 - G、1 3 3 - B が用意される。

所定の色を構成する R : G : B ごとに 3 枚のメモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B の所定アドレスとビットに対応するビット位置に "1" がセットされる。したがって、メモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B のそれぞれからビット情報が読み出されてシフトレジスタ 1 3 3 - R、1 3 3 - G、1 3 3 - B にラッチされる。

シフトレジスタ 1 3 3 - R、1 3 3 - G、1 3 3 - B にラッチされた R : G : B ごとのビット情報は、図 7 で説明したと同様にカラー映像情報として表示制御部 1 4 に送られる。

表示制御部 1 4 においては、図 2 において説明したと

同様にして表示装置 3 にカラー映像情報が送られ、これにより表示装置 3 において、表示データがカラー表示される。

尚、上記実施例において、エラー処理時に表示チェック部 12 が発するエラー処理信号としては、上述したホルト信号の他に CPU 1.0 に対するリセット信号やゲーム装置本体 1 全体を対象とするシステムリセット信号とすることも可能である。

但し、これらのリセット信号をエラー処理信号として表示チェック部 12 が出力する場合には、リセット後に不正プログラムが再実行されることを防止するために、そのエラー処理信号出力が継続的に保持されることが望ましい。

上記したように、先の実施例では、商標等の表示データと比較基準データとの比較の結果一致する場合に、表示を行うことを前提としている。これに対し、図 10 は、他の実施例として、基準比較データとカートリッジ 2 から読みだした表示データとの比較チェックが開始されると所定時間、読みだした表示データが真正なデータであるか否かに関わらず表示装置 3 への表示を継続するように制御するビデオ信号制御装置の構成例を示す。かかる構成により、より明確に観察者に表示データが表示されていることの認識が容易となる。

図 10 に示すビデオ信号制御装置は、具体例として半導体の 1 チップ上に形成され、太い破線 5 に囲まれたビ

ビデオ信号制御回路 5、アドレスデコーダ 6、VDP 15
(図 1 参照)からの表示データが入力される FIFO メ
モリ 7、ピクセルフォーマット変換回路 8 及びデジタル
アナログ変換回路 9 を有して構成される。

- 5 更に、ビデオ信号制御回路 5 は、データ表示用回路 5
0、セキュリティチェック開始制御回路 5 1、データ比
較回路 5 2 及びセキュリティロックタイマー 5 3 を有す
る。

図 1 0 においては、ゲーム機本体を構成するためにビ
10 デオ信号制御装置に接続される、図 1 に示される CPU
1 0、ワークメモリ 1 6 及び VDP 1 5 に相当する回路
装置は、図示省略されている。

図 1 0 の動作は、基本的に先の図 1 の実施例と同様で
あるが、固有の動作特徴を有する。したがって、必要に
15 より図 1 を参照しながら図 1 0 の動作を以下に説明する
。

デジタルアナログ変換回路 9 は、図 2 において説明し
た表示制御部 1 4 (図 1 参照)のデジタルアナログ変換
回路 1 4 2 に対応し、基本的機能としてデジタルのビデ
20 オ信号をアナログビデオ信号に変換して表示装置 3 に R
G B 信号を送る回路である。

更に、図 1 0 のデジタルアナログ変換回路 9 は、VDP
1 5 からのビデオ信号を FIFO メモリ 7 及びピクセル
フォーマット変換回路 8 を通して入力するとともに、
25 後に説明するデータ表示用回路 5 0 の出力を入力する。

これらを表示装置 3 に表示するためのアナログビデオ信号に変換する機能を有する。

図 1 0 において、セキュリティカーソル格納用 R O M 1 1 0 は、図 1 の比較用基準データを記憶する書き込み専用メモリ 1 1 に相当する。ここでセキュリティカーソルとして表示されるロゴは、一例として図 1 1 に示すごとく 3 2 × 1 6 画素の単色で表される S E G A の表示である。

カラーレジスタ 1 1 1 及び、1 1 2 は、このセキュリティカーソルを構成する画素の内、それぞれ “ 1 ” の画素及び “ 0 ” の画素のカラーを指定する情報を格納するレジスタである。

例えば、“ 1 ” の画素は、黒字に青で表示され、“ 0 ” の画素は黒地と同色に表示される。これらの色を特定するコードが、セキュリティカーソルを構成する画素数分がカラーレジスタ 1 1 1 及び、1 1 2 に格納される。カラーレジスタ 1 1 1 及び、1 1 2 は、セキュリティカーソル格納用 R O M 1 1 0 と同様に読出専用のメモリで構成され、セキュリティカーソル格納用 R O M 1 1 0 及びカラーレジスタ 1 1 1、1 1 2 には、上記セキュリティカーソル及び対応する画素のカラー指定情報が予め格納されている。

参照数字 6 は、C P U 1 0 から送られるアドレス信号をデコードしてビデオ信号制御装置における対象となる回路に対し、イネーブル信号を送り動作を活性させるデ

コード回路である。

ここで、ゲームカートリッジ 2 に収容される ROM 内のプログラム格納領域 20 に記憶されるゲームプログラムに含まれる表示チェック命令を CPU 10 が検知すると、CPU 10 からデータ表示用回路 50 の後に説明する各メモリを指定する CPU アドレスとともに、ゲームカートリッジ 2 から読み込んだ表示データが CPU データとしてビデオ信号制御装置に送られる。

図 10 のビデオ信号制御装置において、データ表示用回路 50 が図 1 の表示データ格納部 13 に対応する。データ表示用回路 50 は、CPU 10 から送られる表示データ中のセキュリティカーソルのビットマップパターンを記憶するカーソル RAM 130 を有する。更に CPU 10 から送られる表示データ中には、セキュリティカーソルの表示位置及び表示カラー指定情報が含まれている。したがって、データ表示用回路 50 には、更にこれらの情報を格納する X、Y ポジションレジスタ 131、132 及びカラーレジスタ 133、134 を有している。

ここでアドレスデコーダ 6 は、CPU 10 から送られる表示データ格納部 13 即ち、データ表示用回路 50 を指定する CPU アドレスを受信する。アドレスデコーダ 6 は、これをデコードし、カーソル RAM 13、X、Y ポジションレジスタ 131、132 及びカラーレジスタ 133、134 を活性化するトリガ信号であるイネーブル信号を出力する。

- 3 0 -

イネーブル信号は、5つのオアゲート102を通して、カーソルRAM130、X、Yポジションレジスタ131、132及びカラーレジスタ133、134に送られる。

- 5 したがって、カーソルRAM130、X、Yポジションレジスタ131、132及びカラーレジスタ133、134は、それぞれ、CPUデータである表示データ中のセキュリティカーソルの表示パターン、その表示位置及び表示カラー情報を格納することが可能となる。
- 10 したがって、カーソルRAM130、X、Yポジションレジスタ131、132及びカラーレジスタ133、134に格納された表示データは、デジタルアナログ変換回路9に導かれる。

- ここで、カーソルRAM130に格納されたビットマップデータで構成されるセキュリティカーソルのロゴが、各画素がカラーレジスタ133、134に格納されたカラー指定コードに対応するカラーを有し、X、Yポジションレジスタ131、132に格納されたデータで指定される表示位置に、表示が行われるようにアナログビデオ信号に変換されて表示が開始される。
- 15
- 20

- ここで、カーソルRAM130に格納されたセキュリティカーソルを構成するビットマップの各ビットの上記カラーレジスタ133、134に格納されたカラー指定コードに対応するカラー表示は、次のように行われる。
- 25 セキュリティカーソルを構成するビットの論理値が“0

- 3 1 -

”である時、カラーレジスタ133の出力が選択され、
反対にビットの論理値が“1”である時、カラーレジスタ134の出力が選択され、それぞれのカラーレジスタにより指定されるカラーコードに対応するRGB信号に
5 変換される。

更に、カーソルRAM130、X、Yポジションレジスタ131、132及びカラーレジスタ133、134への表示データ等の格納が完了し、上記のようにセキュリティカーソルの表示が開始されると、CPU10は、
10 チェックスタート駆動回路100を選択するCPUアドレス信号をアドレスデコーダ6に送る。したがってチェックスタート駆動回路100が選択されチェックスタート信号を出力する。

次いで、チェックスタート信号を契機としてセキュリティチェックタイマー101が、計数を開始する。セキュリティチェックタイマー101の出力は、所定の計数値まで計数する間は、オア回路102を通してCPU10からの各回路への新たな書き込みを禁止する論理値を
15 出力する。

したがって、タイムアップまでの所定時間上記のようにデータ表示用回路50からの同じ表示データの出力により同じセキュリティカーソルの表示が継続する。セキュリティチェックタイマー101が計数完了（タイムアップ）した時、CPUデータの新たな書き込みの禁止が
20 解除される。
25

- 3 2 -

即ち、セキュリティチェックタイマー 101 は、セキュリティチェック開始と同時に動作し、チェック開始からタイムアップまでの所定時間（実施例として約 1 秒）カーソル RAM 130 に対する書き込みを禁止する。

5 この結果、カーソル RAM 130 に格納されている表示データが上記所定時間継続して表示される。これにより、比較チェック終了までの間だけ真正な表示データをカーソル RAM 130 に書き込み、画面表示が視認され前に、データを書き換えることが出来なくなる。

10 したがって、不正ソフトであっても、チェック開始後、商標等のロゴが所定時間表示されることになる。この不正ソフトによるロゴの表示は、明らかに商標侵害、あるいは不正競争行為を構成するものである。

一方、チェックスタート駆動回路 100 からのスタート
15 ト信号は、同時にデータ比較回路 52 の各要素回路に対してトリガ信号として与えられる。したがって、比較回路 12 は、このトリガ信号を契機としてデータ表示用回路 50 のカーソル RAM 130 及びカラーレジスタ 133、134 に格納された表示データと、データ比較回路
20 52 のセキュリティカーソル RAM 110 及びセキュリティカラーレジスタ 111、112 からの比較基準用セキュリティデータを読み込み、これらを比較する。比較回路 12 は、一致を検知する場合、論理“1”、不一致の時は論理“0”を出力する。

25 更に、データ比較回路 52 において、X ポジションチ

- 3 3 -

エック回路 1 3 5 及び Y ポジションチェック回路 1 3 6
を有し、それぞれデータ表示用回路 5 0 の X ポジション
レジスタ 1 3 1、Y ポジションレジスタ 1 3 2 からセキ
ュリティカーソルの表示開始位置の X 座標位置及び Y 座
5 標位置のデータを読み込み、予め設定されている許容表
示範囲即ち、X ポジション範囲及び Y ポジション範囲と
比較する。

X 座標位置及び Y 座標位置のデータが許容表示範囲に
ある時は、X ポジションチェック回路 1 3 5 及び Y ポジ
10 ションチェック回路 1 3 6 からそれぞれ論理 " 1 " が出力
される。許容表示範囲にない時は、論理 " 1 " が出力
される。

アンド回路 1 3 7 は、比較回路 1 2、X ポジションチ
ェック回路 1 3 5 及び Y ポジションチェック回路 1 3 6
15 からの出力が入力され、これら全ての論理が " 1 " であ
る時、カートリッジ 2 は真正なプログラム 2 0 を格納し
ていると判断出来る。

この時、アンド回路 1 3 7 はタイマー初期化信号を出
力し、セキュリティロックタイマー 5 3 の計数値を初期
20 値例えば " 零 " に戻し、再び計数を開始する。これによ
りセキュリティロックタイマー 5 3 の計数が所定の計数
値に達するまでの時間が延長される。

このようにセキュリティロックタイマー 5 3 は、セキ
ュリティカーソルを視認可能に所定時間表示するために
25 設けられているセキュリティチェックタイマー 1 0 1 と

異なり、プログラムの実行中に繰り返しセキュリティチェックの実行を行わすために設けられてる。そして、真正ソフトが使用されている間は、タイムアップ前に必ずリセットされる（初期値に戻される）ので、常に作動状態（計数状態）とされる。

この為に、真正ソフトは、セキュリティロックタイマー 53 がタイムアップする前に、セキュリティチェックが行われるように作成されている。尚、実施例として、途中にリセットされない時にセキュリティロックタイマー 53 がタイムアップするまでの所定時間は、約 15 分に設定される。

比較チェックの結果が不一致であった場合は、リセットされないでタイムアップし、デジタルアナログ変換回路 9 に対して表示オフ信号を出力する。これにより下記に説明するように、全ての表示が不能となる。

また、真正な表示データをカーソル RAM 130 に書き込まないようにする等の不正処理を行う不正ソフトの場合にも、セキュリティロックタイマー 53 は、リセットされない。このため、同様にセキュリティチェックタイマー 101 のタイムアップ前に、セキュリティロックタイマー 53 がタイムアップして表示オフ信号が出力が出力されて、全ての表示が禁止される。

データ表示用回路 50 のカーソル RAM 130 の出力は、VDP 15（図 1 参照）から出力される表示データより最優先のビットマップデータとして予め設定されて

いる。したがって、セキュリティロックタイマー 5 3 が所定の計数値に達するまでの期間、カーソル R A M 1 3 0 に格納されるセキュリティ表示のロゴデータ、例えば図 1 1 に示すようなロゴマークが、X、Y ポジションレジスタ 1 3 1、1 3 2 で特定される位置にカラーレジスタ 1 3 3、1 3 4 で特定されるカラーで表示される。

一方、アンド回路 1 3 7 の入力のいずれかが論理 " 0 " である場合は、カートリッジ 2 に格納されるプログラム 2 0 は不正なものであると判断する。

10 かかる場合は、アンド回路 1 3 7 から初期化信号は出力されずに、セキュリティロックタイマー 5 3 は、計数をそのまま継続する。そして、所定の計数値まで達した時、デジタルアナログ変換回路 9 から表示オフ信号が出力される。

15 表示オフ信号は、デジタルアナログ変換回路 9 に入力され、F I F O メモリ 7 及びピクセルフォーマット 8 を通してデジタルアナログ変換回路 9 に入力される、V D P 1 5 から出力されたビデオ信号のアナログビデオ信号への変換を阻止する。

20 これにより、セキュリティチェックによりカートリッジ 2 に格納されるプログラム 2 0 が不正なものであると判断される場合は、V D P 1 5 から出力されるビデオデータ信号は表示が禁止され、以降のゲームの継続が不可能となる。

25 尚、上記図 1 0 の実施例において、デジタルアナログ

変換回路 9 の回路の一部としてデータ比較回路 5 2 の機能を一体にして構成することが可能である。この場合は、アナログビデオ信号に変換される直前即ち、表示装置 3 に対して出力される直前のデータをチェックできるので、セキュリティチェック処理のバイパスや、セキュリティチェック開放後の表示データの解読等を極めて困難とする事が可能である。

産業上の利用可能性

10 以上実施例にしたがい説明したように、本発明は、ゲームカートリッジ 2 に記憶された表示データをゲーム機本体 1 に送り、且つこの表示データを前記ゲームカートリッジ 2 に記憶されたゲームプログラムの制御の下にゲーム機本体 1 と接続される表示装置 3 に表示を行うよう
15 している。

したがって、かかる表示データの表示の有無、表示される表示データの内容からゲームカートリッジ 2 及びそこに記憶されるゲームプログラムの真偽性を容易に判断することが出来る。

20 同時に、本発明にしたがいゲーム機本体 1 において、ゲームプログラムの実行中（ゲームの実行中）に繰り返して、ゲームカートリッジ 2 に記憶される表示データと比較基準データとを比較することにより、例えセキュリティチェックの過程を故意的にバイパスするように修正
25 される場合であっても、確実にゲームプログラムの真偽

性を容易に判断できる。

且つ真正でないと判断される場合は、ゲーム機本体 1
の CPU 10 の動作を強制的に止め、以降真正でないと
判断されるゲームプログラムの実行を阻止することが可
5 能である。これにより不法に複写、作成されたプログラ
ムの使用を阻止することが出来る。

尚、上記実施例は、ゲーム機を例としているが本発明
は、これら実施例に限定されるものではなく、一般的な
情報処理装置本体、外部記憶装置及び表示装置を有する
10 ものであれば、本発明が適用可能である。

更に、本発明と目的、効果を同じにする均等物も、本
発明の保護の範囲に含まれるものである。

請 求 の 範 囲

1. プログラム及び出力データが記憶された外部記憶装置と、

該外部記憶装置が着脱自在に接続され、

5 該外部記憶装置から読み込んだプログラムを実行するCPUと、

基準比較データを記憶する内部記憶装置と、

該外部記憶手段から読み込んだ出力データと該基準比較データとを比較し、これらが不一致の場合にエラー処

10 理信号を発するセキュリティチェック装置とを含む情報処理装置本体及び

該情報処理装置本体が該外部記憶装置から該読み込んだ出力データを表示する表示装置を

有して構成されることを特徴とするセキュリティチェッ

15 ク機能を有する情報処理装置。

2. 請求項1において、前記出力データは、該出力データの
前記出力装置への表示が正当な権原を有しない者の
使用を禁止するものであることを特徴とする情報処理装
置。

20 3. 請求項1又は2において、更に

前記基準比較データと比較される出力データを格納する出力データ格納装置を有し、該出力データは前記外部記憶装置に記憶されたプログラムに従って、該外部記憶装置から該出力データ格納装置に転送され格納されるも

25 のであることを特徴とする情報処理装置。



4. 請求項 1、2 又は 3 において、

前記セキュリティチェック装置は、前記 CPU の動作中に、前記出力データと基準比較データとの比較を繰り返して行うものであることを特徴とする情報処理装置。

5. 請求項 3 又は 4 において、

前記出力データは、前記セキュリティチェック装置によるデータ比較が行われる前に前記外部記憶装置から前記出力データ格納装置に転送記憶され、該セキュリティチェック装置によるデータ比較及び前記出力装置による
10 出力表示の後、該出力データ格納装置から消去されるものであることを特徴とする情報処理装置。

6. プログラム及び出力データが記憶された外部記憶装置から該プログラム及び該出力データを読み込む第一のステップと、

15 該外部記憶装置から読み込んだ該プログラムに含まれる表示チェック開始命令に基づき、チェック開始信号を出力する第二のステップと、

該チェック開始信号が出力される時、該外部記憶装置から読み込んだ出力データと基準比較データとを比較し
20 、これらが不一致の場合にエラー処理信号を発する第三のステップと、

該エラー処理信号に基づき、該プログラムの少なくとも一部の実行を阻止する第四のステップを有することを特徴とする情報処理装置におけるプログラムのセキュリティ
25 ティチェック方法。



7. 請求項 6 に記載のセキュリティチェック方法において、

前記第三のステップにより、前記出力データと基準比較データとが一致する時に、前記出力データを表示する
5 制御信号を発生し、更に、該制御信号に基づき該出力データを表示する第五のステップを有することを特徴とする情報処理装置におけるプログラムのセキュリティチェック方法。

8. 請求項 6 又は 7 に記載のセキュリティチェック方法
10 において、

前記第一のステップにより、前記外部記憶装置に記憶される出力データを、前記プログラムに従って、読み込むことを特徴とする情報処理装置におけるプログラムのセキュリティチェック方法。

15 9. 請求項 6、7 又は 8 に記載のセキュリティチェック方法において、

前記第三のステップにより、前記出力データと基準比較データとの比較が前記プログラムの実行中に繰り返されることを特徴とする情報処理装置におけるプログラム
20 のセキュリティチェック方法。

10. 請求項 8 又は 9 に記載のセキュリティチェック方法において、更に

前記第五のステップによる出力データの表示の後に、読み込んだ該出力データを消去する第六のステップを有
25 することを特徴とする情報処理装置におけるプログラム



のセキュリティチェック方法。

1 1. 情報処理装置本体に着脱自在に接続される外部記憶装置であって、該情報処理装置本体において実行されるプログラムと、該情報処理装置本体により表示制御される出力データが格納され、該出力データは該プログラムに従って、該情報処理装置への読み込みが制御されることを特徴とする外部記憶装置。

1 2. 請求項 1 1 に記載の外部記憶装置において、

前記情報処理装置は、ビデオゲーム装置であって、前記出力データは、該出力データの表示自体が、前記プログラムの使用権原のない者の違法を意味するものであることを特徴とする外部記憶装置。

1 3. 請求項 1 2 に記載の外部記憶装置において、

前記出力データが前記プログラムの使用権原を与えるものの所有する商標であることを特徴とする外部記憶装置。

1 4. 請求項 1 1 に記載の外部記憶装置において、

前記情報処理装置は、ビデオゲーム装置であって、前記出力データは、前記プログラムにしたがって、該ビデオゲーム実行過程において、所定の時点毎に表示されるように制御されることを特徴とする外部記憶装置。

1 5. 第一のビデオ信号と該第一のビデオ信号より高い表示優先度を有する第二のビデオ信号の表示を制御するビデオ信号制御装置であって、

25 該第二のビデオ信号の表示データと比較されるべき基



準表示データを格納する読出専用メモリと、

該第二のビデオ信号の表示データと該読出専用メモリから読みだされる基準表示データを比較する比較回路と

- 5 該比較回路が該第二のビデオ信号の表示データと該基準表示データとの不一致を検出する時、所定時間後に該第一のビデオ信号の表示を禁止するように制御する回路を有することを特徴とするビデオ信号制御装置。

16. 請求項15において、更に、

- 10 前記第二のビデオ信号の表示期間が観察者により認識可能の時間であるように制御する回路を有することを特徴とするビデオ信号制御装置。

17. 請求項15において、

- 15 前記第二のビデオ信号の表示データは、ビットマップパターンの所定のセキュリティカーソルと、該セキュリティカーソルの表示位置を指定するデータを含み、

前記比較回路は、該セキュリティカーソルの表示位置を指定するデータと、前記基準表示データに含まれる基準表示位置を指定するデータとを比較し、

- 20 該セキュリティカーソルの表示位置が該基準表示位置の範囲内にはない時は、前記所定時間後に前記第一のビデオ信号の表示を禁止するように制御する回路により該第一のビデオ信号の表示を禁止することを特徴とするビデオ信号制御装置。

- 25 18. 請求項17において、



前記ビットマップパターンは、観察者に観察可能の固定の大きさで前記第二の表示データが表示されるように前記読出専用メモリに記憶されることを特徴とするビデオ信号制御装置。

5 19. 請求項 17 において、

前記ビットマップパターンの所定のセキュリティカーソルを、特定のロゴマークとしたことを特徴とするビデオ信号制御装置。



図1

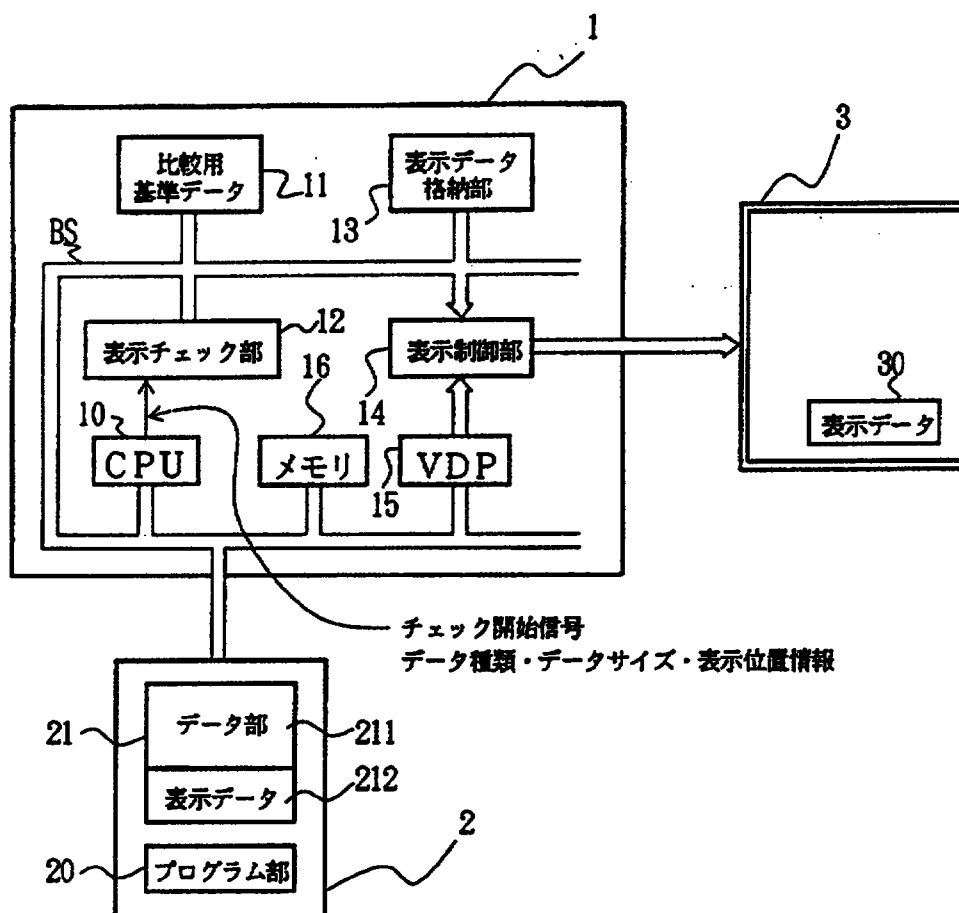


図 2

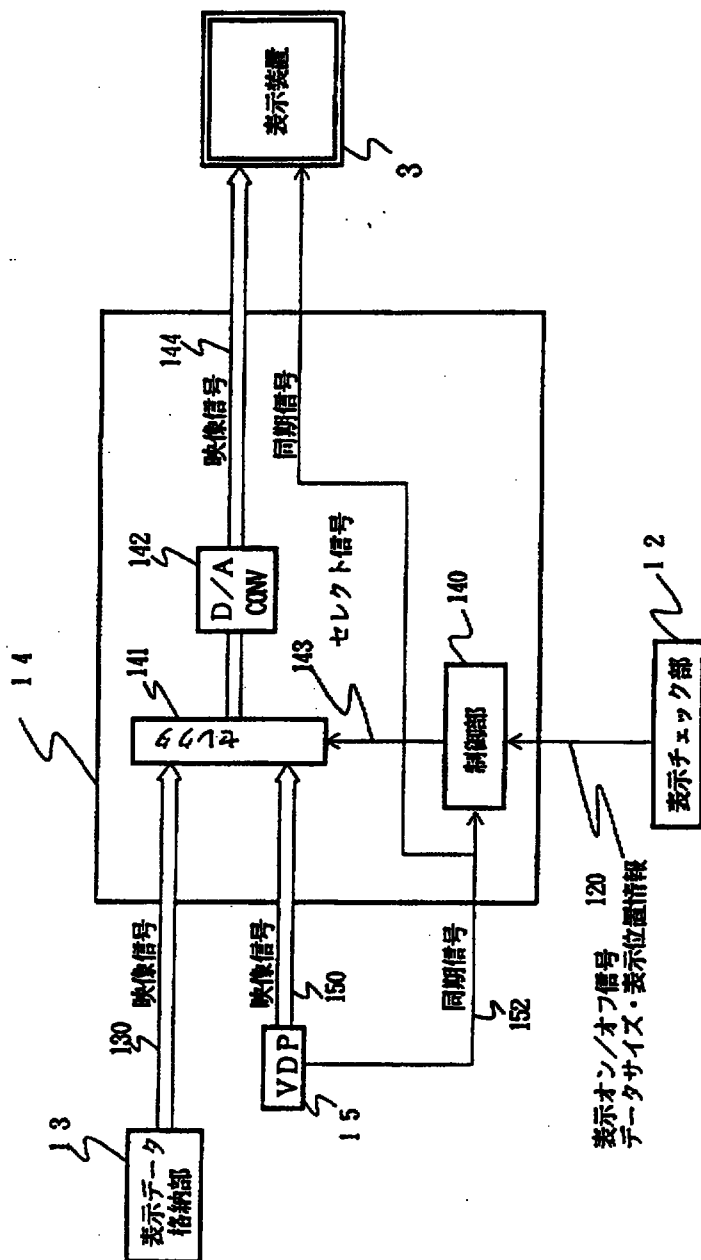
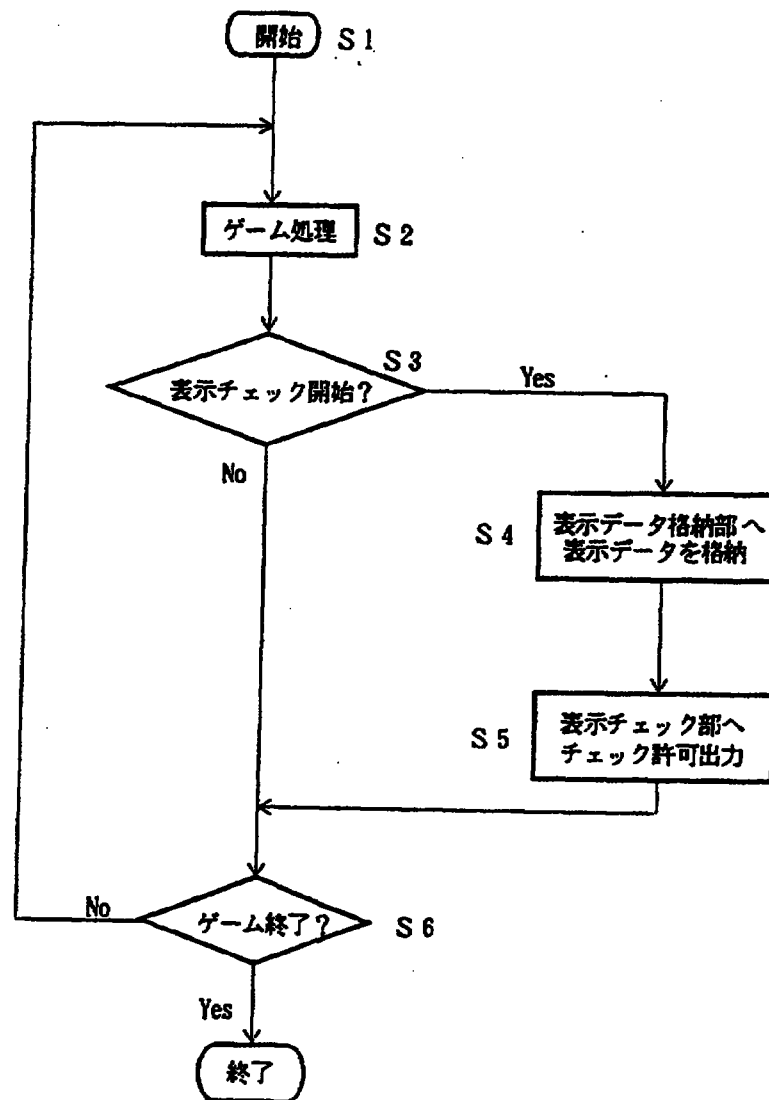


図 3

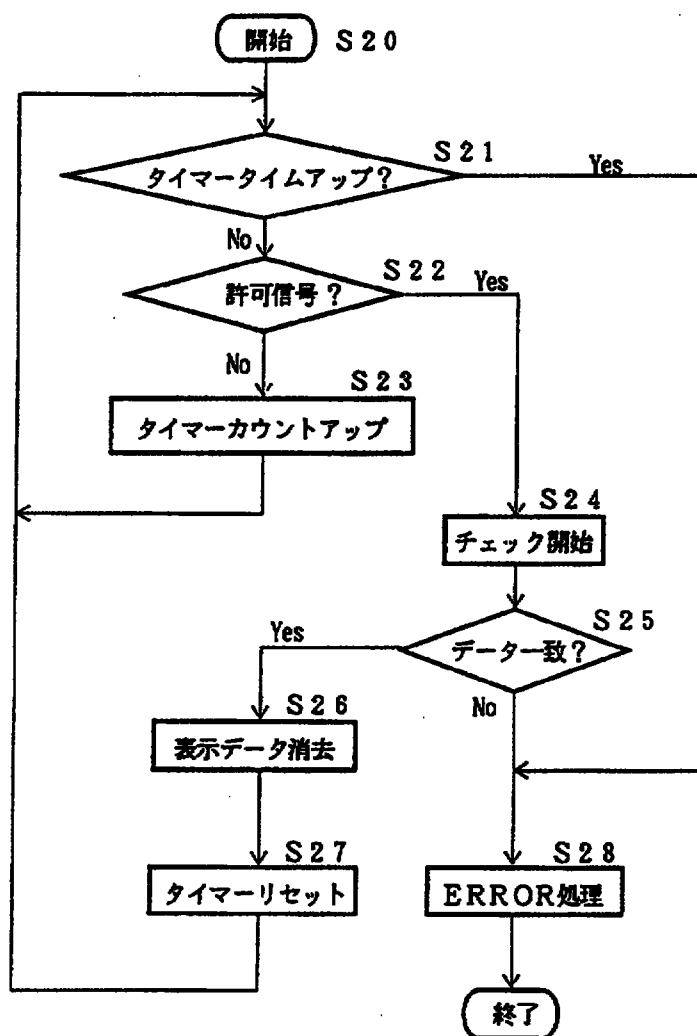
CPU



4/11

図4

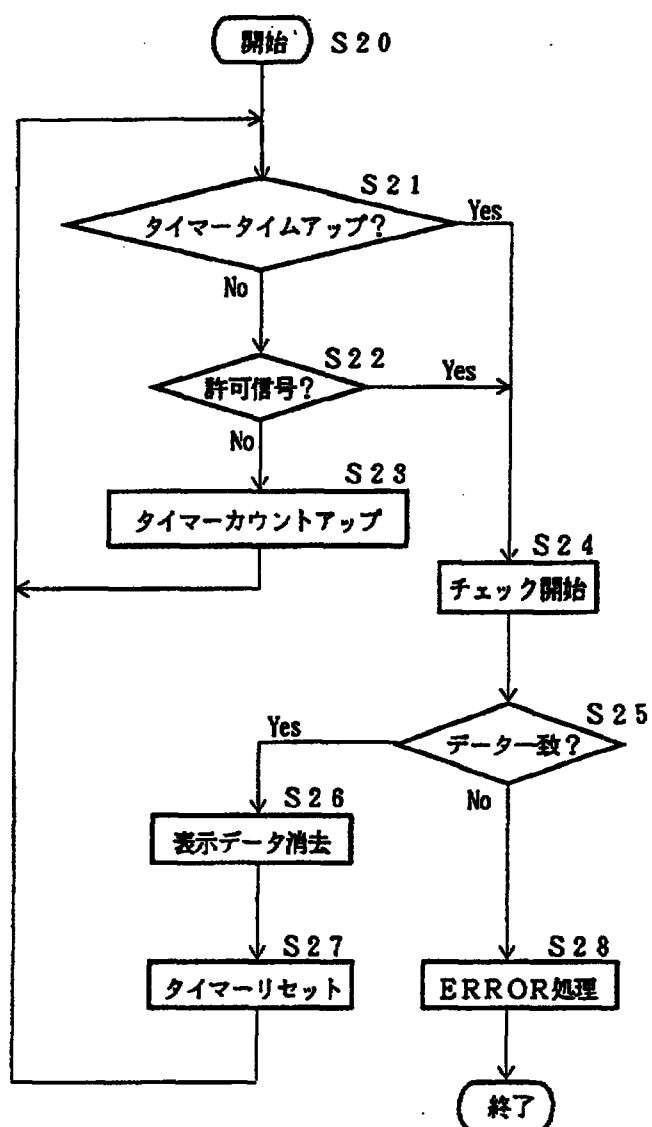
表示チェック部



5/11

図5

表示チェック部



6/11

図 6

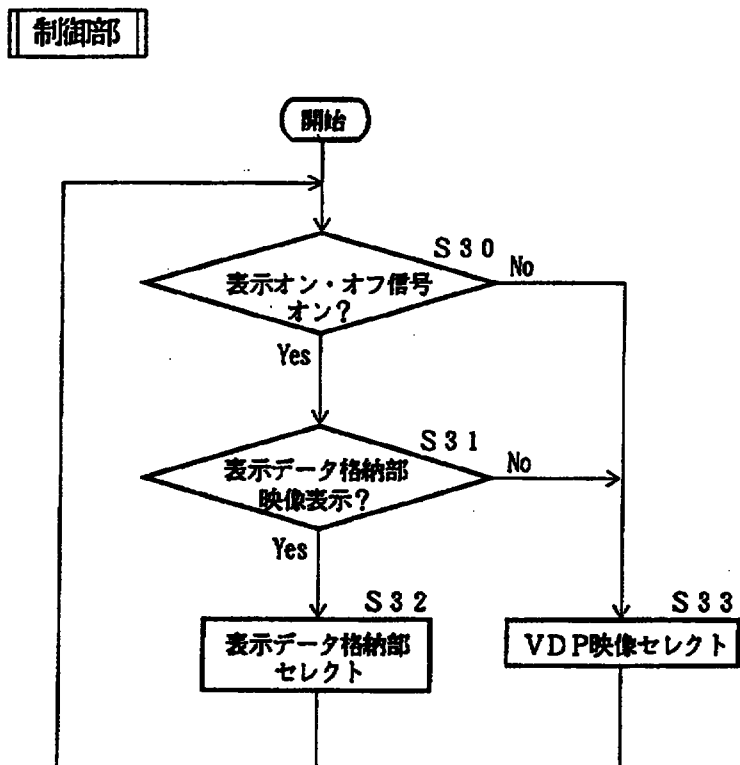


図7

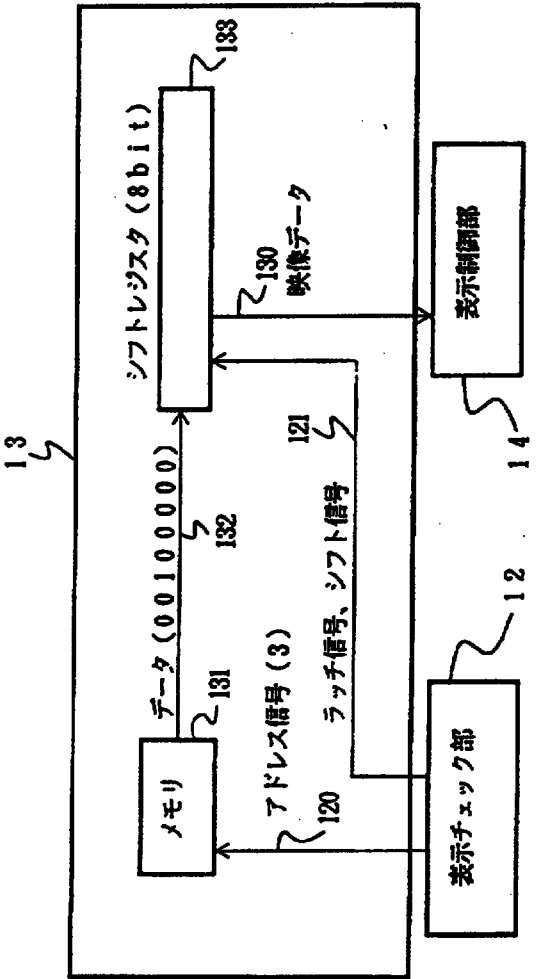


図8B

		bit							
		7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	0	0	0	0
2	0	0	0	1	0	0	1	0	0
3	0	0	0	1	0	0	0	0	0
4	0	0	0	1	0	0	0	0	0
5	0	0	0	1	0	0	1	0	0
6	0	0	0	1	0	0	0	1	0
7	0	0	0	1	0	0	1	0	0

図8A

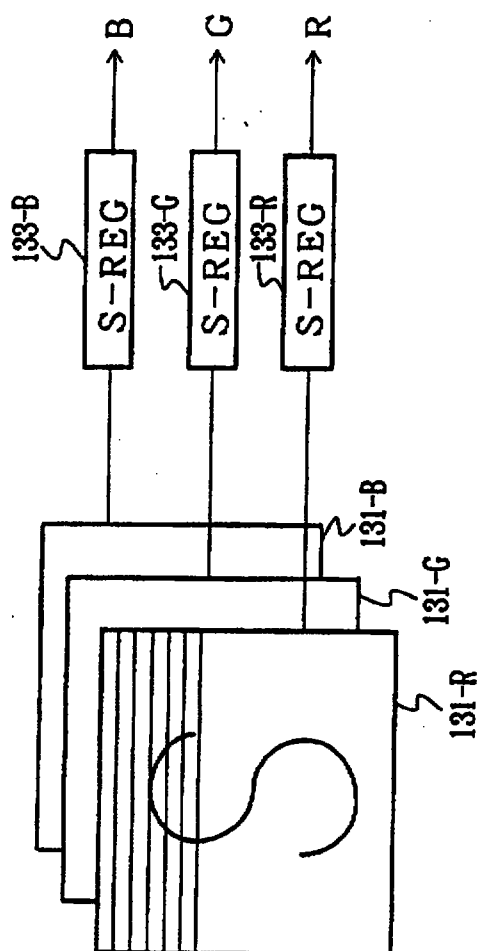
		bit							
		7	6	5	4	3	2	1	0
0									
1									
2									
3									
4									
5									
6									
7									

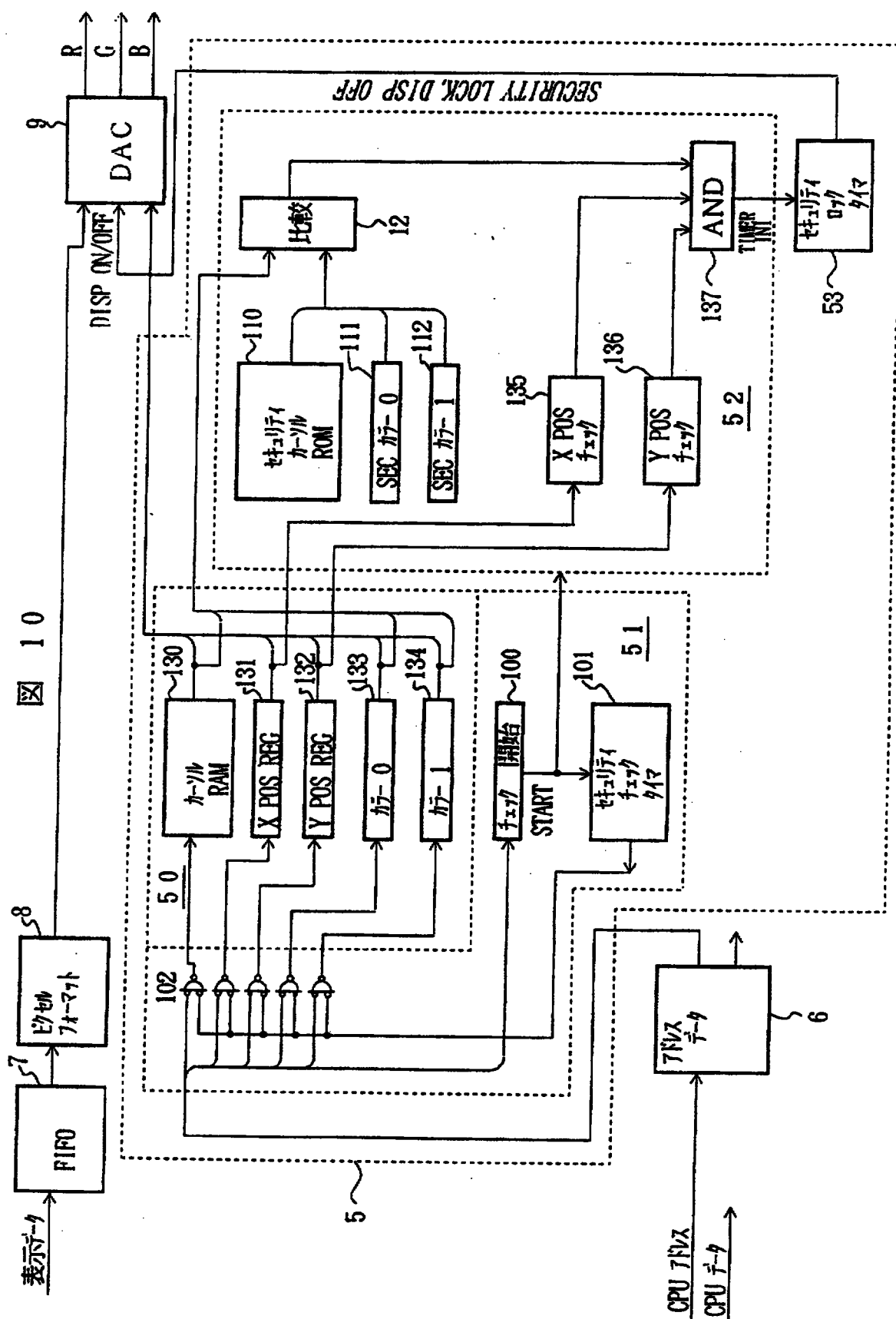
アドレス



9/11

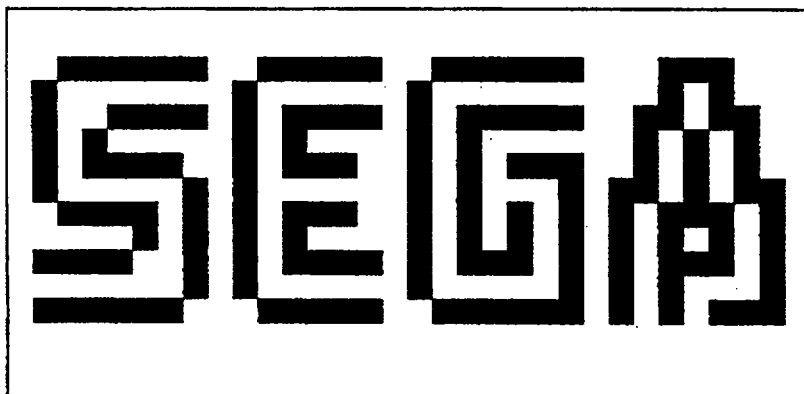
図 9





11/11

図 11



TITLE OF THE INVENTION
Information Processing Apparatus With
Security Checking Function

5

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a security checking method for ascertaining the authenticity of a program that is to be executed, to an information processing apparatus having such a security checking function, and
10 to a program storage device that is employed for the information processing apparatus.

Related Arts

As the processing speed of microprocessors is being
15 increased, information processing apparatuses of various types are being provided, and programs for execution by such information processing apparatuses are also being provided on many types of recording media.

Especially for information processing apparatuses,
20 such as video game machines, the media employed for the distribution of game programs that are to be executed are usually cartridges, in which are packaged semiconductor read only memory (ROM) chips on which programs are recorded, or CD-ROMs.

25 In the video game business, not only is the superiority of a video game machine important, but also the relative excellence of a video game affects the distri-

bution of game programs. If an excellent game program can be copied, or imitated, and sold by a third party who is not authorized to do so, the value to a developer of that game program is lost and the confidence of customers in the products of the developer is also deteriorated.

Therefore, security checking functions for examining the authenticity of programs and for preventing the execution of illegal programs have been proposed for information processing apparatuses, and have been implemented.

Such prior art techniques are described in, for example, USP 4,442,486 (hereinafter abbreviated as "USP486"), USP 4,454,594 (hereinafter abbreviated as "USP594"), USP 4,462,076 (hereinafter abbreviated as "USP076"), and Japanese Unexamined Patent Publication No. Sho 62-3331 (hereinafter abbreviated as a "331 publication").

In the technique disclosed in USP486, a program includes data for generating a display signal to momentarily display a patent number or a patent application number. The authenticity of the program is ascertained by examining the data for the generation of the momentary display to determine whether they match a reference signal that is stored in an information processing apparatus.

The technique disclosed in USP594, which is the same as that in USP486, reads data that are stored in a spe-

cific location in an external memory in which a program is stored, displays the read data, such as a trademark, and determines whether or not the data match reference data that are stored in an information processing apparatus. When the data do not match, execution of the program is blocked.

The technique disclosed in USP076, which is the same as the techniques in USP486 and USP594, compares data at a predetermined address in an external memory cartridge with reference data stored in an information processing apparatus. Before substantially connecting the external memory to the apparatus, information concerning an authorized owner is displayed.

When the data matches the reference data, the external memory cartridge is regarded as an authentic one, and execution of a game is enabled.

Further, in the 331 publication, especially before a main operation of an information processing apparatus is begun, a program that is stored in an external memory device to ascertain program authenticity is executed by the external memory device. At the same time, a program for ascertaining program authenticity is executed by the information processing apparatus. When the results obtained by the execution of both programs for ascertaining program authenticity match, the main operation of the apparatus is activated.

The conventional security checking function for an

information processing apparatus is performed by determining whether security codes, etc., match before a program, such as a game program, is executed. Once the execution of a program has begun, further security checking is not performed, or else can not be performed, for the duration of the execution of the program.

In a sequence of a program, therefore, steps for security checking processing are disabled or bypassed by some means, usually illegally, and as a result, the following steps in the program are performed though without the security check.

In addition, according to the security checking method described in USP486, USP596 or USP076, display data, such as a trademark, are merely displayed momentarily; the information processing apparatus neither checks to determine whether or not the correct image of a trademark, etc., is actually displayed, nor is it designed to do so.

Further, as is described above, when the steps for processing the security checking are disabled or bypassed in some manner, specific data can not be displayed and the authenticity of a program can not be examined.

SUMMARY OF THE INVENTION

It is therefore a first object of the present invention to provide an information processing apparatus that easily and securely confirms whether or not software (a



program) that is to be executed by the information processing apparatus is an authentic program, and a method therefor.

5 It is a second object of the present invention to provide an information processing apparatus that can legally and securely prevent the manufacture and sale of illegal programs, and a method therefor.

10 It is a third object of the present invention to provide an information processing apparatus that assumes that displaying of display data using an image or sound is based on a program that is stored in an external storage device and that enables the display of a specific illegal, and a method therefor.

15 It is a fourth object of the present invention to provide an information processing apparatus that can prevent the execution of an illegal procedure that disables and bypasses the security checking that is intended to confirm program authenticity, and a method therefor.

20 It is a fifth object of the present invention to provide an information processing apparatus that, to more certainly achieve the fourth object, prevents the execution of an illegal procedure that replaces a program with an unauthentic (false) program during security checking, and to a method therefor.

25 It is a sixth object of the present invention to provide an external memory device that is adapted for the first through the fifth objects.



To achieve the first object, an information processing apparatus having a security checking function, which is to be connected detachably to an external memory means for storing a program and display data, and an output
5 means for displaying data that are read from the external memory means, comprises:

a CPU for executing a program that is read from the external memory means;

10 internal memory means for storing comparison reference data; and

security checking means for comparing the comparison reference data with the display data that are read from the external memory means.

15 Further, to achieve the first object, a security checking method comprises:

a first step of reading a program and display data from an external memory means in which the program and the display data are stored;

20 a second step of outputting a check start signal based on a display check start command included in the program read from the external memory means;

a third step of comparing the display data read from the external memory means with comparison reference data when a check start signal is output, and of generating an
25 error signal when the display data do not match the comparison reference data; and

a fourth step of, in response to the error signal,



preventing execution of at least one part of the program.

With this arrangement, data that are output and displayed as a video image or sound are to be compared for a security check. Through this process, a counterfeit program can be prevented from being executed.

To achieve the second object, an information processing apparatus displays data on an output means to inhibit the use of a program by an unauthorized person.

To achieve the second object, a security checking method further comprises a fifth step of, when the display data match the comparison reference data at the third step, generating a control signal for displaying the display data, and of displaying the output data based on the control signal.

With the above described structure, when the display data is a trademark, etc., by the display of the display data the use of a program by unauthorized persons can be inhibited, and the manufacture and sale of counterfeit programs can be legally inhibited.

To achieve the third object, an information processing apparatus comprises display data storage means for storing display data that are compared with the comparison reference data, and the display data are transferred from the external memory means to the display data storage means and are stored therein in accordance with a program that is stored in the external memory means.

To further achieve the third object, using a security



checking method the display data that are stored in the external memory means at the first step are read in consonance with the program.

5 With this arrangement, since the display data are transferred to and stored in the data storage means in consonance with a program that is stored in the external memory device, the display of the display data can be performed by a program that is stored in the external memory device, and what is illegal can be clarified.

10 To achieve the fourth object, in an information processing apparatus, the security checking means repeatedly compares the display data with the comparison reference data during an operation performed by the CPU.

15 To achieve the fourth object, using a security checking method comparison of the display data with the comparison reference data at the third step is repeatedly performed during the execution of the program.

20 With this arrangement, since the comparison for security checking is repeated throughout the operation of a program, an illegal act, such as bypassing security checking, can be prevented.

25 To achieve the fifth object, in an information processing apparatus, the display data are transferred from the external memory means to, and are stored in, the display data storage means before the security checking means performs a data comparison, and after the data comparison by the security checking means and the output



and display of the data by the output means are completed, the data are erased from the display data storage means.

To achieve the fifth object, a security checking
5 method further comprises a sixth step of, after the display data are displayed at the fifth step, erasing the display data.

With this structure, display data must be newly read for repeated comparison checks. Therefore, an illegal
10 act by which a program is replaced with a counterfeit (unauthentic) program is prevented during the security checking process, and the fourth object can be achieved more certainly.

To achieve the sixth object, in an external memory
15 device, which is detachably connected to an information processing apparatus, are stored a program to be executed by the information processing apparatus and display data to be displayed by the information processing apparatus, and the display data are read by the information processing
20 ing apparatus in consonance with the program.

With the above structure, the external memory device can be adapted for the first through the fifth objects.

BRIEF DESCRIPTION OF THE DRAWINGS

25 Fig. 1 is a block diagram for one embodiment of the present invention;

Fig. 2 is a block diagram illustrating an example



arrangement for a display controller;

Fig. 3 is a flowchart for the operation of a CPU;

Fig. 4 is a flowchart I for the operation of a display checking section;

5 Fig. 5 is a flowchart II for the operation of the display checking section;

Fig. 6 is a flowchart for the operation of a control section in the display controller;

10 Fig. 7 is a block diagram illustrating an example arrangement for a display data storage section;

Figs. 8A and 8B are diagrams for explaining display data, with Fig. 8A showing one example of a display pattern, and with Fig. 8B showing memory bit information that corresponds to the display pattern;

15 Fig. 9 is a diagram for explaining a method for displaying color display data.

Fig. 10 is a block diagram illustrating a video signal control circuit of another example of the present invention.

20 Fig. 11 is a diagram illustrating a logo example for security check, controlled by the video signal control circuit of Fig. 10.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

25 The preferred embodiments of the present invention will now be described while referring to the accompanying drawings. The same reference numbers or symbols are used

to denote corresponding or identical components.

Fig. 1 is a block diagram illustrating the arrangement of one embodiment of the present invention in which an information processing apparatus is applied to a game machine. A game machine 1, which serves as an information processing apparatus, has internally a CPU 10, a comparison reference data memory 11, a display check section 12, a display data storage section 13, a display control section 14, a video display processor (VDP) 15, and a work memory 16 that are mutually connected by a bus BS.

A game cartridge 2, which serves as an external memory device, is detachably connected to the game machine 1 by a connector. Inside the game cartridge 2 is mounted a ROM wherein there are a data storage area 21 and a game program storage area 20 for the execution of a game .

Although in the following explanation a game cartridge 2 and its internally mounted ROM are employed as an external memory device and its memory, they can be replaced by a CD disk drive and a CD-ROM.

The data storage area 21 has a data portion 211 for storing data, such as characters, that are usually displayed during the execution of a game, and a display data portion 212 for storing data that are displayed for security checking according to the present invention.

The display data indicate an authentic program that

is used in the game machine 1, as will be described later, and include, for example, data concerning an image, or data for sounds, such as a trademark of a distributor of the game machine 1.

5 The display data can be compressed and stored, as needed, to provide greater security.

 According to the present invention, a game program that is stored in the game program storage area 20 partly includes, at the least, a control command for reading
10 display data from the display data portion 212, and for transferring the data to the display data storage section 13 of the game machine 1 for storage therein.

 When the display data are compressed and stored in the display data portion 212 as described above, a decom-
15 pression program for decompressing the compressed display data may be stored as one part of the game program in the game program storage area 20. When hardware is employed for data decompression, a decompression circuit can be arranged in the game machine 1 or in the game cartridge
20 2.

 A display device 3 in Fig. 1 receives a video signal from the display control section 14 of the game machine 1, and provides a specific display on its display portion. In particular, display data 30, which have been
25 read from the game cartridge 2 and have been transferred to and stored in the display data storage section 13 according to the present invention, are displayed at a

predetermined position of the display device 3.

Although, in the embodiment, data are displayed as an image on the display device 3 for security checking by the present invention, display data for the present invention are not limited to an image.

In other words, as is previously described, not only video data, but also speech data are included as data indicating that an authentic program is being used in the game machine 1. When the display data are speech data, the data are naturally used to produce sounds.

In Fig. 2 are shown the details of the display controller 14 and the arrangement, including the display device 3, for displaying the display data 30 according to the present invention. The display control section 14 includes a controller 140, a selector 141 and a D/A converter 142.

Figs. 3 through 6 are flowcharts for the operations performed by the CPU 10, the display check section 12 and the controller 140 of the display control section 14. The details in Figs. 1 and 2 will now be described while referring to the flowcharts.

In Fig. 3, when a power switch (not shown) of the game machine 1 is turned on to begin a game (step S1), the CPU 10 reads a game program from the program storage area 20 of the game cartridge 2, and executes the program (step S2).

The game program that is read by the CPU 10 includes

a command for instructing the start of display checking at a predetermined timing. Therefore, the CPU 10 makes a search to determine whether or not the display checking start command is present (step S3).

5 The timing for starting the display checking can be set arbitrarily. For example, the changing of a game scene as the game advances can be regarded as a time at which to start the display checking. Such a command can be described in the game program.

10 When there is a display checking start command (step S3: Yes), the CPU 10 executes a storage command described in the read game program (step S4). That is, in consonance with the storage command for the game program, the CPU 10 reads display data from the display storage
15 area 21 of the game cartridge 2, and transfers the data to and stores it in the display data memory 13.

Following this, the CPU 10 outputs a checking enable signal to the display checking section 12 (step S5). The check enable signal includes a check start signal, data
20 type information, data size information, and display position information.

The above operation is repeated by the CPU 10 until the game is over (step S6).

The data type information specifies one of the reference data types that are stored in advance in the comparison reference data memory 11. The data size information
25 designates a display data size for the display data 30

before they are displayed on the display device 3, if a function for varying the size of the display data 30 is included.

5 The display position information specifies the position for the display data 30 on the display device 3 when a function for varying the display position is included.

Fig. 4 is a first flowchart for the processing by the display checking section 12 following the receipt from the CPU 10 of a checking enable signal that includes a
10 checking start signal, data type information, data size information, and display position information.

The display checking section 12 is essentially constituted by a special logic circuit that has a timer counter and a comparator, or a CPU. When the game machine 1 is powered on, the timer counter starts counting
15 (step S20).

When the display checking section 12 is constituted by a logic circuit, comparison logic is calculated for security checking (data comparison) by using the input of a checking enable signal from the CPU 10 as a trigger.
20 When the display checking section 12 is constituted by a CPU, a data comparison program is stored in the ROM (not shown in Fig. 1) of the game machine 1. With the input of a checking enable signal from the CPU 10 as a trigger,
25 the display checking section 12 executes that data comparison program to perform security checking (data comparison).

Then, since the timer counter serves as a watched-dog timer, a check is performed to determine whether or not the count by the timer counter has reached a predetermined count value, i.e., whether or not a predetermined time period has elapsed (step S21).

When the count by the timer counter has reached the predetermined count value, this means that the CPU 10 could not correctly read a program from the program storage area 20 in the game cartridge 2 within the predetermined time period. Or this means that a program is not authentic and the security for the program can not be legally unlocked because the program does not have a security release routine, or does not have key data (display data) for releasing the security.

This event is processed as an error (step S28). In such a case, performance of the security checking is halted, and the display checking section 12 generates, for example, a halt signal that is forwarded to the CPU 10 as an error signal. In response to this signal, the CPU 10 halts the operation and the execution of the game program is discontinued.

If, at step S21, the count by the timer counter has not yet reached a predetermined count value, a check is performed to determine whether or not an enable signal has been transmitted from the CPU 10 (step S22). When an enable signal has not been transmitted from the CPU 10, the timer counter continues counting (step S23).

When an enable signal has been transmitted from the CPU 10, the security checking is begun (step S24). The security checking is performed as follows according to the present invention.

5 In Fig. 1, in response to a command that is included in a game program, which is stored in the program storage area 20 in the internally provided ROM in the game cartridge, the CPU 10 reads display data from the display data portion 212 and transfers the data to the display
10 data storage section 13, which is a RAM.

At the same time, in response to a checking start command that is included in the game program, the CPU 10 transmits to the display checking section 12 a checking start signal that includes data type information, data
15 size information, and display position information.

The definitions for the data type, data size, and data position information have been given above. The data must be displayed in the language of a country in which a game machine is used even though security display
20 data have the same meaning.

The data type information, therefore, also includes information that indicates for indicating which data of a plurality of display data that correspond to different languages are stored in the display data portion 212 of
25 the game cartridge 2. Thus, a plurality of different types of comparison reference data are stored in the comparison reference data storage section 11, the ROM, of

the game machine 1.

Among the display data that are output from the display checking section 12 to the display control section 14, the data size information and the display position information especially can be varied by an illegal operation, with the data display size being so changed that it can not be discerned or that it can not be displayed within a valid screen, and the display position being moved to a point outside the limits of a valid screen for the display device 3.

It is, therefore, preferable that a limiter be provided to prevent such illegal modifications of the data display size and the display position. By the provision of the limiter, even when data for a display that is smaller in size than a minimum discernible size or that is larger in size than a maximum display screen size is output by the display checking portion 12, the data for display can be altered to provide a display having an appropriate discernible size.

Referring back to the flowchart in Fig. 4, the display checking section 12 reads, from the comparison reference data storage section 11, comparison reference data that is specified in consonance with the data type, which is transmitted from the CPU 10. The display checking section 12 begins to compare the received reference data with the display data that are transferred to and stored in the display data storage section 13 (step S24).

As a result of the comparison, when the reference data does not match the display data that is stored in the display data storage section 13, it is assumed that the program in the game cartridge 2 is unauthorized, and
5 an error process is performed (step S28).

This error process is performed in the same manner as when the timer counter has counted a predetermined value (step S21: Yes), and the operation of the CPU 10 is forcibly halted. Thus, further execution of the game
10 program is prevented.

When, as the result of a comparison, the reference data is found to match the display data, it is assumed that the game cartridge 2 contains an authorized program. Then, the display data that have been transferred from
15 the display data portion 212 of the game cartridge 2 to the display data storage section 13 and stored therein are erased following a predetermined time (step S26).

The display data are erased for the following reason. If the display data are not erased, once the display data
20 are stored in the display data storage section 13, the result of the security checking (data comparison) is always "the data match," no matter how often the security checking is repeated.

Therefore, repeating the security checking throughout
25 the execution of a program according to the present invention would be meaningless, as an unauthorized (false) program could be performed as a result of the

execution of an illegal procedure during the operation. For this reason, the erasure of display data is performed, as is described above, to prevent the execution of such an illegal procedure.

5 It should be noted that the display data is erased only after the lapse of a predetermined time that is long enough to permit an observer to easily confirm by looking at the monitor that the data match. Further, it is preferable that a special circuit be provided in the game
10 machine 1 so that hardware can be employed to forcibly erase the display data so as to more surely avoid loop-holes that permit the illegal alteration of a program.

 Here, the erasing of the display data is performed by clearing the display data previously stored in the display data storage section 13, namely overwriting all "0"
15 bits or overwriting a different pattern of bits on the display data.

 The timer counter is reset before the display data is erased (step S27). Program control then returns to the
20 beginning of the routine (step S20), at which point the timer counter restarts the count at an initial value.

 Therefore, as long as each repetition of the security checking procedure is performed before the time counted by the timer has expired, and as long as the display data
25 matches the reference data, the error process (step S28) is not performed. On the contrary, when a checking enable signal is not transmitted before the time counted

by the timer has expired, a program is regarded as an illegal program, and the error process is performed.

As is explained above, in this embodiment, each time a checking enable signal is transmitted from the CPU 10 to the display checking section 12, a repetition of the security checking is performed within a predetermined time.

In the flowchart in Fig. 4, when, at step S21, the count by the timer counter has reached a predetermined value, the error process (step S28) is immediately performed. However, as is shown in the flowchart for another embodiment, even when a timer counter has counted up to a specific value, security checking may be performed (step S24) to determine whether or not display data matches reference data (step S25).

When for an unauthentic game program the timer counter has counted up to the predetermined value, the security checking does not result in the matching of the display data, and an error process (step S28) is performed. The other processes are the same as in the flowchart in Fig. 4 for the previous embodiment.

When as the result of a comparison by the display checking section 12 it is determined that the reference data match the display data, a game program that is stored in the game cartridge 2 is regarded as authentic.

On the other hand, if, for an illegal game program copy, the result of the comparison by the display check-

ing section 12 shows that the two sets of data match, the performance of the game program can therefore be continued.

In this case, however, illegal copying can be inhibited by displaying data on the display device 3, such as the data for a trademark, that can inhibit the use of the program by an unauthorized person.

The fact that data for a trademark is displayed on the display device 3 indicates the apparent infringement by an unauthorized person of the rights accruing to the trademark.

Fig. 6 is a flowchart for the operation of the controller 140 (see Fig. 2) in the display control section 14. As is previously explained while referring to Fig. 1, when a checking start signal is transmitted from the CPU 10 to the display checking section 12, data type information, data size information, and display position information are also sent.

In response to the checking start signal, the display checking section 12 transmits a display ON/OFF signal, information 120 for a data size, and a display position to the controller 140 of the display control section 14. The display control section 14 receives display data as a video signal 130 from the display data storage section 13.

In addition, the display controller 14 receives game image data as a video signal 150 from the video display

processor (VDP) 15. In the display control section 14, the video signal 130, from the display data storage section 13, and the video signal 150, from the video display processor 15, are input to the selector 141.

5 The detailed arrangement and the operation of the video display processor 15 will not be given as they are not directly related to the present invention. The video display processor 15 in this embodiment is a device with a well known structure that is employed for a current
10 video game machine, and serves as an I/O device for the CPU 10. The video display processor 15 includes a register, a color RAM, and a scroll distance setup RAM, and also has a control block for controlling an externally attached video RAM. With this arrangement, the video
15 display processor 15 synthesizes video image data that are displayed on the display device 3 and outputs the resultant data as a video digital signal 150.

From the video display processor 15, vertical and horizontal sync signals 152 are synchronously output with
20 the output of a video digital signal 150, and are input to the controller 140. In consonance with the display ON/OFF signal from the display checking section 12, the controller 140 outputs a select signal 143 synchronously with the sync signals 152.

25 The select signal 143 is sent to the selector 141 to switch video signals 130 and 150 and to output them. The switching operation will be explained while referring to

the flowchart in Fig. 6.

First, the controller 140 determines whether or not the display ON/OFF signal from the display checking section 12 indicates an ON state. When the display
5 ON/OFF signal indicates an ON state, a check is performed to determine whether or not it is time to display a video signal for the display data from the display data storage section 13 (step S31).

The decision for the display data timing at step S31
10 is made based on the data size and display position signal 120 for the display data from the display checking section 12, and is further based on the sync signal 152 from the video display processor 15.

When it is time to display the data, the video signal
15 130 for the display data from the display data storage section 13 is selected in consonance with the select signal 143 (step S32). When it is not time to display the data, the video signal 150 from the video display processor 15 is selected in consonance with the select
20 signal 143 (step S33).

In this manner, in consonance with the select signal 143, the selector 141 outputs to the D/A converter 142 either the video signal 130 or 150 for the display data.

The D/A converter converts the digital video signal
25 130 or 150 into an analog video signal 144. The analog video signal 144 is transmitted together with the sync signal 152 to the display device 3, where a predetermined

display is performed.

At step S32, the timing for displaying display data from the display checking section 12, and the performance of security checking (data comparison) by the display checking section 12 are not necessarily paired. The security checking by the display checking section 12 is performed at comparatively short intervals, and a screen display may be performed after the display checking section 12 has performed the security checking and when nothing is affected by that display.

This operation can be performed in such a manner that, for example, a timing at which the display checking section 12 sends the display ON/OFF signal 120 to the display control section 14, or a timing at which the select signal 143 is output from the controller 140 of the display control section 14, is set in advance so that it conforms to a predetermined control cycle.

Figs. 7 through 9 are diagrams for explaining the arrangement of the display data storage section 13, and a method for displaying display data, by using one display data example.

As is shown in Fig. 7, the display data storage section 13 includes a memory 131, a RAM, and a shift register 133. An address signal 120 is sequentially input from the display checking section 12 to the memory 131. Latch signal and shift signal 121 are input from the display checking section 12 to the shift register

133.

Let us consider a case wherein the pattern for the display data is an "S" as is shown in Fig. 8A. A display data area in Fig. 8A is a region encompassing an 8 x 8 matrix that is composed of 64 pixels, whose locations are specified by employing bits 7 through 0 and addresses 0 through 7.

In the 8 x 8 matrix region, display data pattern "S" is represented by black dots. In consonance with this display pattern, the bit information in the memory 131 is represented as is shown in Fig. 8B. In other words, the bit positions in the memory 131 that correspond to the black dots that form the display data pattern "S" are set to "1."

Referring back to Fig. 7, when an address signal (3) is input as the address signal 120 from the display checking section 12 to the memory 131, bit information at a corresponding address in the memory 131, i.e., "00100000," is read as data 132.

The data 132 is latched in the shift register 133 by the latch signal from the display checking section 12. In consonance with the shift signal from the display checking section 12, the latched data 132 are transmitted as a video signal 130 to the display control section 14, bit by bit beginning with bit seven (see 121 in Fig. 7).

The video signal 130, which is relayed via the selector 141, is displayed on the display device 3 as the

display data 30, as is previously described.

Fig. 9 is a diagram for explaining the structure of the memory 131 for the display data storage section 13 and the shift register 133 when color data are displayed.
5 A specific color is displayed for each bit of display data in the R:G:B combination.

The bit information in Fig. 8B is prepared as a set of three memories, 131-R, 131-G and 131-B, for the R:G:B combination. In addition, the shift registers 133-R,
10 133-G and 133-B are prepared that correspond to the memories 131-R, 131-g and 131-B.

In order for each R:G:B combination to represent a specific color, a "1" is set in the positions that correspond to the predetermined addresses and bits for the
15 memories 131-R, 131-G and 131-B. Bit information are read from the memories 131-R, 131-G and 131-B and are latched in the shift registers 133-R, 133-G and 133-B, respectively.

The bit information for R:G:B that is latched in the
20 shift registers 133-R, 133-G and 133-B is transmitted as color video information to the display control section 14, as is described while referring to Fig. 7.

The display control section 14 transmits the color video information to the display device in the same
25 manner as is explained while referring to Fig. 2, and the data are then displayed in color on the display device 3.

In the above embodiments, an error signal that the

display checking section 12 generates during the error process can be other than the above described halt signal, and may be either a reset signal for the CPU 10, or a system reset signal for the entire game machine 1.

5 When the display checking section 12 outputs such a reset signal as an error signal, however, it is preferable that the error signal output be continuous in order to prevent re-execution of a counterfeit program after the system is reset.

10 As explained above, the display data are displayed, when the display data such as a trademark coincide with the comparison reference data. Contrarily, an embodiment shown in Fig. 10 is a video signal control device which controls to display the display data read out from the
15 cartridge 2, no matter if the display data are authentic or not, for a predetermined period after the comparison of the display data read from the cartridge 2 with the comparison reference data is started. Therefore, it becomes easier for an observer to recognize whether or
20 not the display data is actually displayed for the predetermined period. The video display control device shown in Fig. 10 can be formed on a semiconductor chip, and includes a video signal control circuit surrounded by a
25 thick broken line 5, an address decoder 6, a FIFO memory 7 to which display data sent from the VDP 15 (see Fig. 1) are inputted, a pixel format conversion circuit 8 and a digital analog converter 9.

Further, the video signal control circuit 5 includes a data display circuit 50, security check start control circuit 51, a data comparator 52 and a security lock timer 53.

5 The circuits, such as the CPU 10, the work memory 16 and the VDP 15 shown in Fig. 1, which are connected to the video signal control device to form a console of a video game system, are not shown in Fig. 10 for simplifying explanation. The operation in the embodiment of
10 Fig. 10 is fundamentally the same as that of Fig. 1, but has some features in operation. The features in the embodiment of Fig. 10 will now be explained as follows, referring to Fig. 1, if needed.

15 The digital analog convertor 9 corresponds to the D/A convertor 142 of the display control section 14 (see Figs. 1, 2), and has a fundamental function of converting a digital video signal to an analog video signal, and sends a RGB signal corresponding to the analog video signal to the display device 3.

20 The digital analog convertor 9 of Fig. 10 receives a digital video signal sent from the VDP 15 via the FIFO memory 7 and the pixel format convertor 8, and an output signal of the data display circuit 50 which is explained later, to convert the signals to analog signals as ex-
25 plained above.

In Fig. 10, a security cursor storage ROM 110 corresponds to the read-only memory 11, as explained in Fig.

1, in which comparison reference data are stored. A logo that is displayed as a security cursor is "SEGA," represented as a simple color in a 32 x 16 pixel grid, as is shown in Fig. 11 as one example.

5 Color registers 111 and 112 are registers in which is stored information for designating colors of "1" and "0" for each of pixels that constitute the security cursor.

For example, pixel "1" is displayed in blue on a black background and pixel "0" is displayed in the same color as the black background. Codes that specify these colors are stored in the color registers 111 and 112 in a number that is equivalent to the number of pixels that constitute the security cursor. The color registers 111 and 112 are constituted by a read-only memory, as is the security cursor storage ROM 110. The security cursor and information for colors of corresponding pixels are stored in advance in the security cursor storage ROM 110 and the color registers 111 and 112.

20 An address decoder 6 decodes an address signal that is received from the CPU 10, and transmits, to a destination circuit in a video signal controller, an enable signal to activate the circuit.

When the CPU 10 has detected a display checking command, which is included in a game program that is stored in the program storage section 20 of the ROM in the game cartridge 2, the CPU 10 transmits to the video signal controller a CPU address for designating the

memories, which will be described, of a data display circuit 50, and display data, which have been read from the game cartridge 2, as CPU data.

5 In the video signal controller of Fig. 10, the data display circuit 50 corresponds to the display data storage section 13 in Fig. 1. The data display circuit 50 has a cursor RAM 130, in which are stored bit map patterns for the security cursor that are included in display data that are sent from the CPU 10. The display
10 data that are received from the CPU 10 also include the display position for the security cursor and display color information. Therefore, the data display circuit 50 further includes an X position register 131, a Y position register 132, and the color registers 133 and
15 134, in which the above described information is stored.

The address decoder 6 receives, from the CPU 10, a CPU address for designating the display data storage section 13, i.e., the data display circuit 50. The address decoder 6 decodes the CPU address, and outputs an
20 enable signal as a trigger signal to activate the cursor RAM 130, the X and Y position registers 131 and 132, and the color registers 133 and 134.

The enable signal is sent via five OR gates 102 to the cursor RAM 130, the X and Y position registers 131
25 and 132, and the color registers 133 and 134.

Therefore, the display pattern for the security cursor, its display position information, and the display

color information of the display data, which are the CPU data, can be stored, respectively, in the cursor RAM 130, the X and Y position registers 131 and 132, and the color registers 133 and 134.

5 Following this, the display data that are stored in the cursor RAM 130, the X and Y position registers 131 and 132, and the color registers 133 and 134 are transmitted to a digital analog converter 9.

10 The logo of the security cursor, which is constituted by bit map data that are stored in the cursor RAM 130, is converted into an analog video signal, so that the individual pixels of the logo are represented by the colors corresponding to the color codes that are stored in the color registers 133 and 134, and are displayed at the
15 display positions that are designated by the data stored in the X and Y position registers 131 and 132.

Bits of the bit map, which constitutes the security cursor in the cursor RAM 130, are displayed in colors, which correspond to the color codes stored in the color
20 registers 133 and 134, in the following manner. When the logical value of a bit of the security cursor is "0," the output of the color register 133 is selected. When the logical value of a bit is "1," the output of the color register 134 is selected. The output signal is converted
25 into an RGB signal that corresponds to a color code that is designated by the selected color register.

When the display data have been stored in the cursor

RAM 130, the X and Y position registers 131 and 132, the color registers 133 and 134, and, when the display of the security cursor is begun in the above described manner, the CPU 10 transmits a CPU address signal for selecting a checking start driver 100 to the address decoder 6. The
5 checking start driver 100 is thus selected and outputs a checking start signal.

Sequentially, in response to the checking start signal, a security checking timer 101 begins counting.
10 The security checking timer 101 outputs a logical value for inhibiting the writing by the CPU 10, via the OR circuit 102, of new data to the individual circuits until the counts by the security checking timer 101 reaches a predetermined value. Therefore, by outputting the same
15 display data from the data display circuit 50, the same security cursor is continuously displayed until the security checking timer 101 reaches the predetermined value.

When the counting by the security checking timer 101
20 has been completed (when the time has expired), the inhibition of the writing of new CPU data is removed.

Namely, the security check timer 101 starts counting and outputs an inhibiting signal to AND gates 102, so that writing to the cursor RAM 130 is inhibited for a
25 predetermined period, for example one second.

The display data stored in the cursor RAM 130 is continuously displayed for the predetermined period, and

therefore, a display data can be written in the cursor RAM 130 only during the checking period and rewriting of display data is inhibited before an observer can recognize the displayed display data.

5 Consequently, even a logo such as a trademark included in an illegal program is displayed for the predetermined period when the security checking is started, so that the display of the trademark would constitute infringement on the trademark right or violation
10 of the unfair competition law.

 A checking start signal from the checking start driver 100 is transmitted as a trigger signal to the individual circuits in a data comparator 52. Upon the receipt of the trigger signal, a comparison circuit 12
15 reads the display data, which are stored in the cursor RAM 130, and in the color registers 133 and 134 in the data display circuit 50, and comparison reference security data that are stored in a security cursor RAM 110, and
20 in security color registers 111 and 112 in the data comparator 52, and compares these data. When the data match, the comparison circuit 12 outputs a logical value of "1," and when the data do not match, it outputs a logical value of "0."

 The data comparator 52 also includes an X position
25 checking circuit 135 and a Y position checking circuit 136. These circuits 135 and 136 respectively read X coordinate data and Y coordinate data for a security

cursor display start position from the X position register 131 and the Y position register 132 in the data display circuit 50. The circuits 135 and 136 compare these position data with permissible display ranges that are set in advance, i.e., with an X position range and a Y position range, respectively.

When the X coordinate and Y coordinate position data are within the permissible display ranges, the X position checking circuit 135 and the Y position checking circuit 136 output a logical value "1." When the X and Y coordinate data are not within the permissible ranges, a logical value "0" is output.

An AND circuit 137 receives the outputs of the comparison circuit 12, the X position checking circuit 135, and the Y position checking circuit 136. When all of these logical values are "1," it is assumed that an authentic program 20 is packaged in the cartridge 2.

Then, the AND circuit 137 outputs a timer reset signal and the count value for a security lock timer 53 is reset to an initial value, for example, "0" to begin a new counting sequence. Through this process, a time duration until the count by the security lock timer 53 has reached a predetermined value is extended.

As understood above, the security lock timer 53 is provided to execute repeatedly a security checking during the operation of a game program, differently from the security check timer 101 which is provided to display a

security cursor for a predetermined period. The security lock timer 53 is made active, or state of counting, as far as an authentic program is executed because it is necessarily reset to an initial value.

5 The authentic program has to be designed to start security checking before the security lock timer 53 completes counting or the predetermined period has been expired. As an example, the predetermined period, that is, the period until the security lock timer 53 completes
10 counting is set about 15 minutes.

 If the result of comparison is that a display data does not coincide with the comparison reference data, the AND gate 137 outputs a display OFF signal to the digital analog convertor 9, as the security lock timer 53 is not
15 reset. This makes it disable to display any data on the display device 3, as explained as follows.

 Further, in such a case that an illegal program could not write an authentic display data into the cursor RAM 130, the security lock timer 53 is not reset, and there-
20 fore, the security lock timer 53 becomes time-up or reaches a certain count value to output the display OFF signal and then any display of display data is inhibited.

 The output of the cursor RAM 130 in the data display circuit 50 is set in advance as bit map data having
25 higher priority than display data that are output by the VDP 15 (see Fig. 1). In the period before the count by the security lock timer 53 has reached a predetermined

value, data for a logo, for example, the logo shown in Fig. 11, that are stored in the cursor RAM 130 for displaying the security cursor, is displayed in the colors that are specified by the color registers 133 and 134, and at a position that is designated by the X and Y position registers 131 and 132.

When either input to the AND circuit 137 is "0," it is assumed that the program 20 packaged in the cartridge 2 is counterfeit.

In such a case, a reset signal is not output from the AND circuit 137, and the security lock timer 53 continues counting. When the count value reaches a predetermined value, a display OFF signal is output by the security lock timer 53.

The display OFF signal is sent to the digital analog converter 9, so that a video signal, which is transmitted from the VDP 15 to the digital analog converter 9 via an FIFO memory 7 and a pixel format 8, is prevented from being converted into an analog video signal.

As is described above, when it is assumed through the security checking that the program 20 packaged in the cartridge 2 is counterfeit, the display of a video data signal from the VDP 15 is inhibited, and the execution of the game is discontinued.

In the embodiment in Fig. 10, the function of the data comparator 52 can be integrally provided as one part of the digital analog converter 9. In this case, im-

mediately before data are converted into an analog video signal, i.e., immediately before data are output to the display device 3, the data can be examined, so that it is extremely difficult to bypass the security checking process, or to decode display data after they have been subjected to security checking processing.

As is described above in the embodiments, according to the present invention, display data that are stored in the game cartridge 2 are transmitted to the game machine 1, and in consonance with a game program that is stored in the game cartridge 2, the display data are displayed on the display device 3, which is connected to the game machine 1.

Thus, the authenticity of a game cartridge 2 and of a game program can be easily confirmed by the presence on the display of the display data and the data contents that are displayed.

At the same time, according to the present invention, the game machine 1 repeatedly compares display data that are stored in the game cartridge 2 with reference data during the execution of the game program (during the operation of the game). Even when the security checking process is altered for the purpose of bypassing it, the authenticity of the game program can be easily determined.

When a game program is not authentic, the operation

of the CPU 10 of the game machine 1 is forcibly halted to prevent the further execution of the unauthentic game program. In this manner, the use of an illegally copied program can be prevented.

5 Although a game machine has been employed as an example in the above embodiments, the present invention is not limited to these embodiments, and can be applied to any common information processing apparatus having an external storage device and a display device.

10 In addition, an equivalent system that is employed for the same purpose and provides the same effect as the present invention falls within the scope of the present invention.



THIS SHEET HAS BEEN
REPLACED

What is claimed is:

1. An information processing apparatus having a security checking function, comprising:

5 an external memory device for storing a program and display data;

an information processing console to which said external memory device being detachably connected, including,

10 a CPU for executing the program that is read out from said external memory device,

an internal memory device for storing comparison reference data, and

15 a security checking device for comparing with said comparison reference data with said display data that are read out from said external memory device; and

a display device for displaying the display data that are read out from said external memory device.

2. The information processing apparatus according to claim 1,

20 wherein the fact that said display data are displayed on said display device means infringement by an unauthorized person of a legal right accruing to the display data.

25 3. The information processing apparatus according to claim 1 or 2,

wherein said information processing console further





THIS SHEET HAS BEEN
REPLACED

includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU controls to transfer and store said display data from said external memory device to said display data storage device in accordance with the program that is stored in said external memory device.

4. The information processing apparatus according to claim 1, 2 or 3,

10 wherein said security checking device repeatedly compares said display data with said comparison reference data, during the CPU executing the program that are read out from the external storage device.

15 5. The information processing apparatus according to claim 3 or 4,

 wherein said display data are transferred from said external memory device to and are stored in said display data storage device before said security checking device performs data comparison, and after said data comparison by said security checking device and the display of said display data by said display device are completed, said display data are erased from said display data storage device.

25 6. A security checking method for checking authenticity of a program in an information processing apparatus, comprising:





THIS SHEET HAS BEEN
REPLACED

a first step of reading a program and display data out from an external memory device in which said program and said display data are stored;

5 a second step of outputting a checking start signal based on a display checking start command included in said program read out from said external memory device;

a third step of comparing said display data read out from said external memory device with comparison reference data when a checking start signal is output, and
10 generating an error signal when said display data do not match said comparison reference data; and

a fourth step of, in response to said error signal, preventing execution of at least one part of said program.

15 7. The security checking method according to claim 6, further comprising a fifth step of, when said display data match said comparison reference data at said third step, generating a control signal for displaying said display data, and displaying said display data based on
20 said control signal.

8. The security checking method according to claim 6 or 7,

wherein said display data that are stored in said external memory device are read in at said first step in
25 consonance with said program.

9. The security checking method according to claim 6, 7

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

or 8,

wherein comparison of said display data with said comparison reference data at said third step is repeatedly performed during the execution of said program.

5 10. The security checking method according to claim 8 or 9, further comprising a sixth step of, after said display data are displayed at said fifth step, erasing said display data that have been read in.

10 11. An external memory device, which is detachably connected to an information processing console, for storing a program, to be executed by said information processing console, and display data, to be displayed under control by said information processing console, and from which said display data are read in said information processing console in consonance with said program.

15 12. The external memory device according to claim 11, wherein said information processing console is a video game machine, and wherein said display data that are displayed on a display device inhibits the use of a program by an unauthorized person.

20 13. The external memory device according to claim 12, wherein said display data are a trademark for a party that is authorized for said program.

25 14. The external memory device according to claim 11, wherein said information processing apparatus is a video game machine, and wherein said display data are displayed

This Sheet Has Been Replaced





according to said program each predetermined timing during an execution of a video game.

15. A video signal control device for controlling the display of a first video signal and a second video signal which has a priority of displaying to the first video
5 signal, comprising:

a read-only memory for storing a reference display data which is compared with a display data of said second video signal;

10 a comparing circuit for comparing the reference display data with said display data of the second video signal;

a control circuit for inhibiting the display of said first video signal after a predetermined time has
15 elapsed, when said comparing circuit detects that the reference display data does not coincide with the display data of the second video signal.

16. The video signal control device according to claim 15,

20 wherein there is further comprised a timing circuit for controlling the period of displaying said second video signal, during which an observer can recognized the display data of the second video signal.

17. The video signal control device according to
25 claim 15,

wherein said display data of the second video signal





THIS SHEET HAS BEEN
REPLACED

includes a security cursor constituted by a bit map
pattern and a display position at which the security
cursor is displayed, said comparing circuit compares the
display position of the second video signal with a
5 reference display position data which is included in said
reference display signal, and said control circuit in-
hibits the display of the first video signal when the
display position of the security cursor is not present
within a allowable display area which is defined by the
10 reference display position.

18. The video signal control device according to
claim 17,

15 wherein said bit map pattern is stored in said read
only memory, with a fixed largeness so that an observer
can recognize the second display data.

19. The video signal control device according to
claim 17,

wherein said security cursor constituted by the bit
map pattern is a specific logo mark.

20

This Sheet Has Been Replaced



ABSTRACT

An information processing apparatus has a security checking function for ascertaining the authenticity of a program to be executed, and the program and display data to be displayed are stored in an external storage device. 5 The information processing apparatus, which has a CPU for executing a program, is connected to the external storage device and a display device for displaying the display data. During the execution of the program, the display data stored in the external storage device are displayed 10 on the display device in consonance with that program. The display data are compared with comparison reference data that are stored in the information processing apparatus. When the two sets of data do not match, the 15 operation of the CPU of the information processing apparatus is halted, and further execution of the program is prevented.

This Sheet Has Been Replaced



FIG. 1

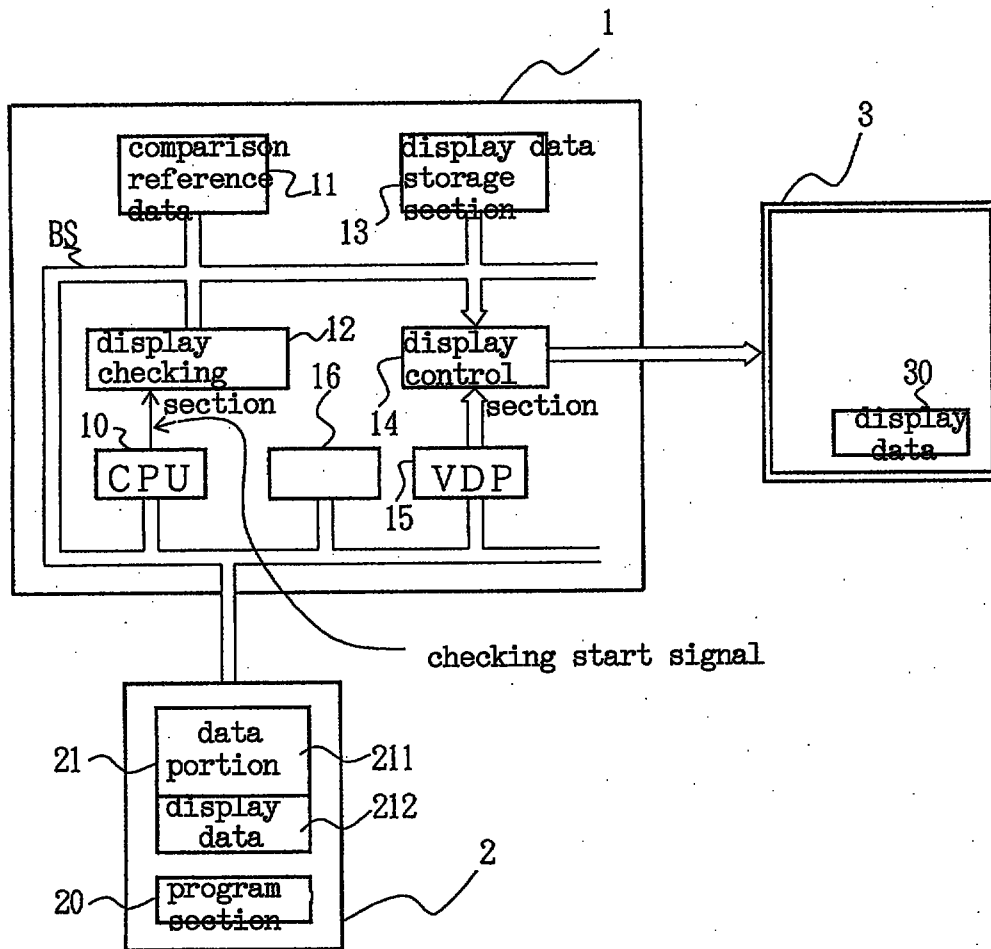


FIG. 2

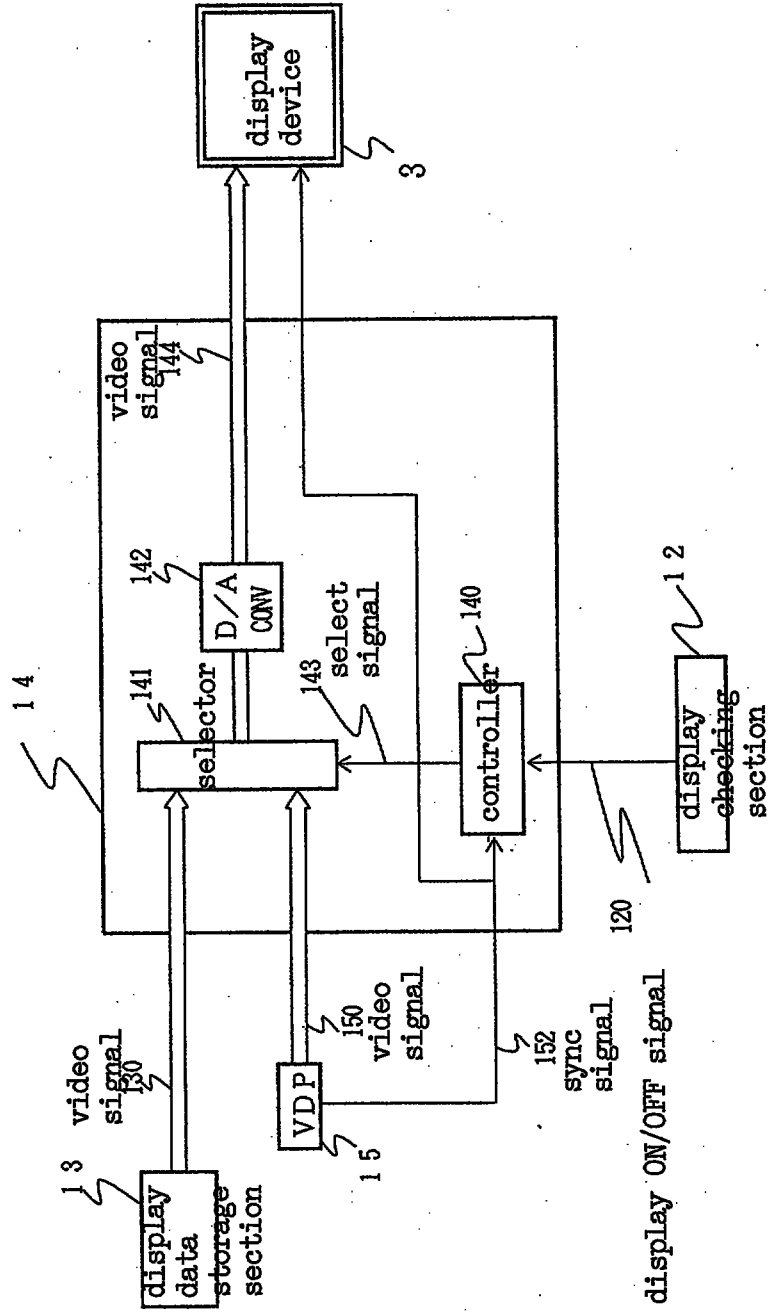


FIG. 3

CPU

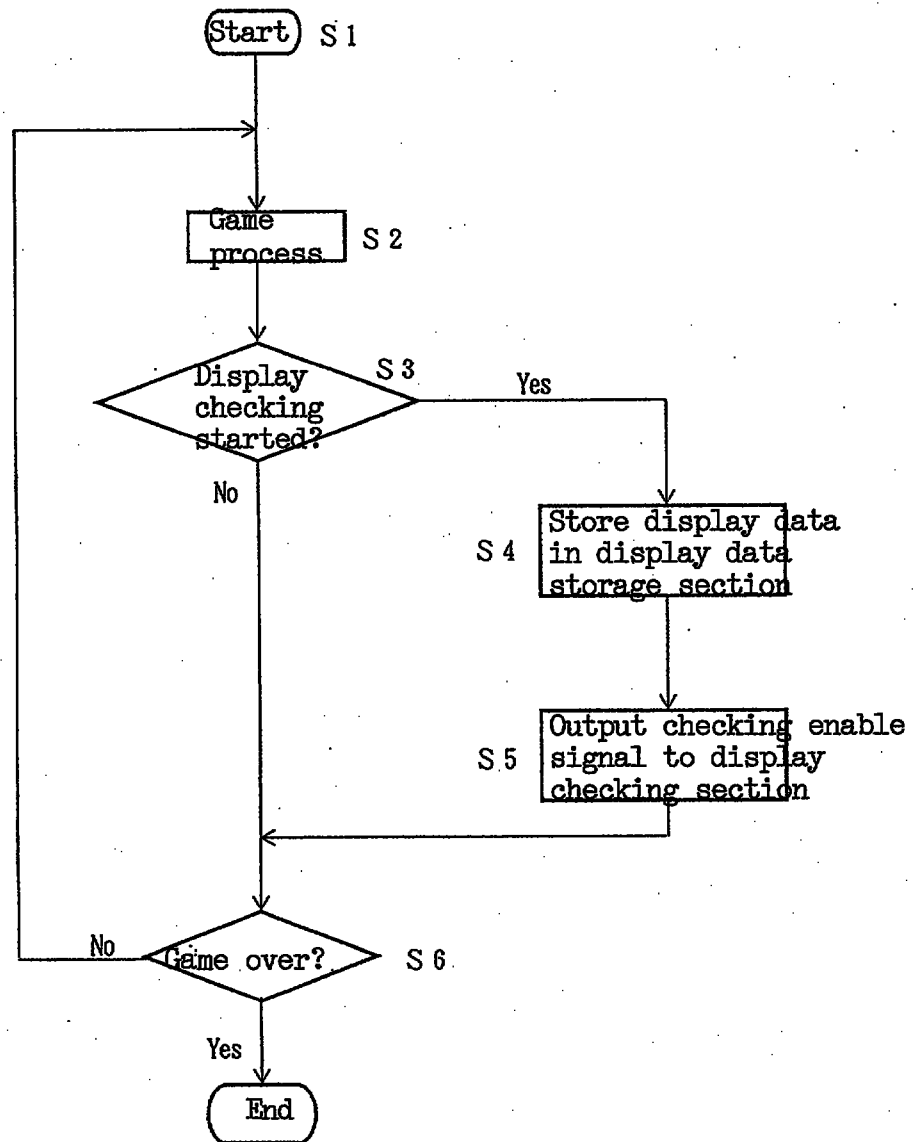


FIG. 4

Display checking
section

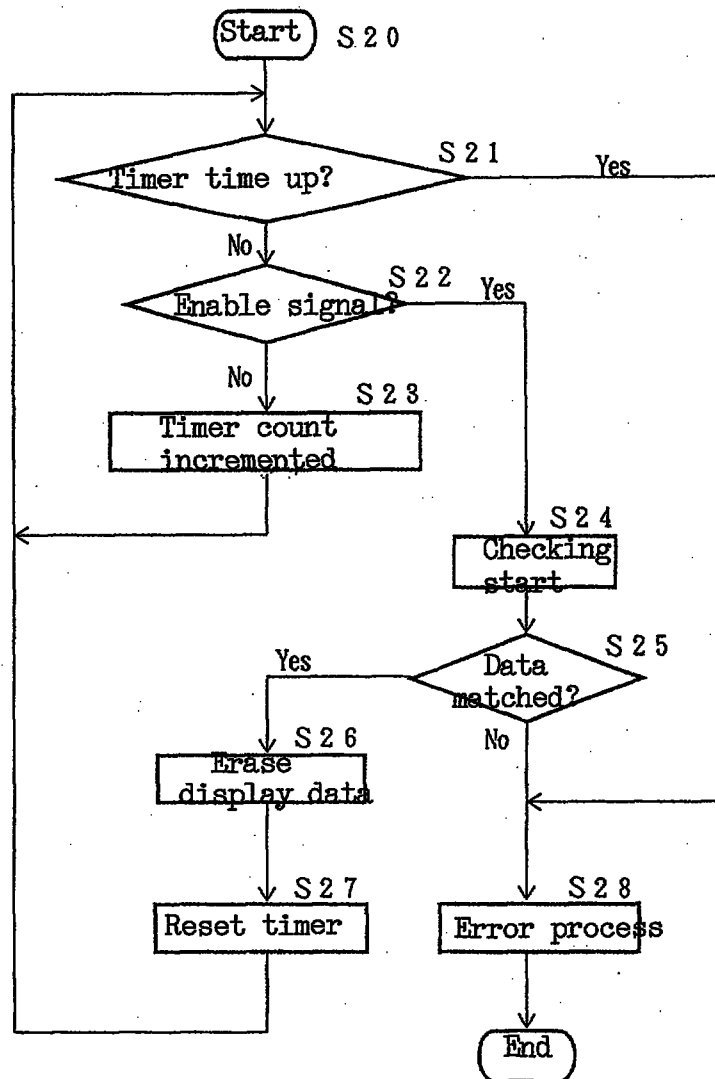


FIG. 5

Display checking
section

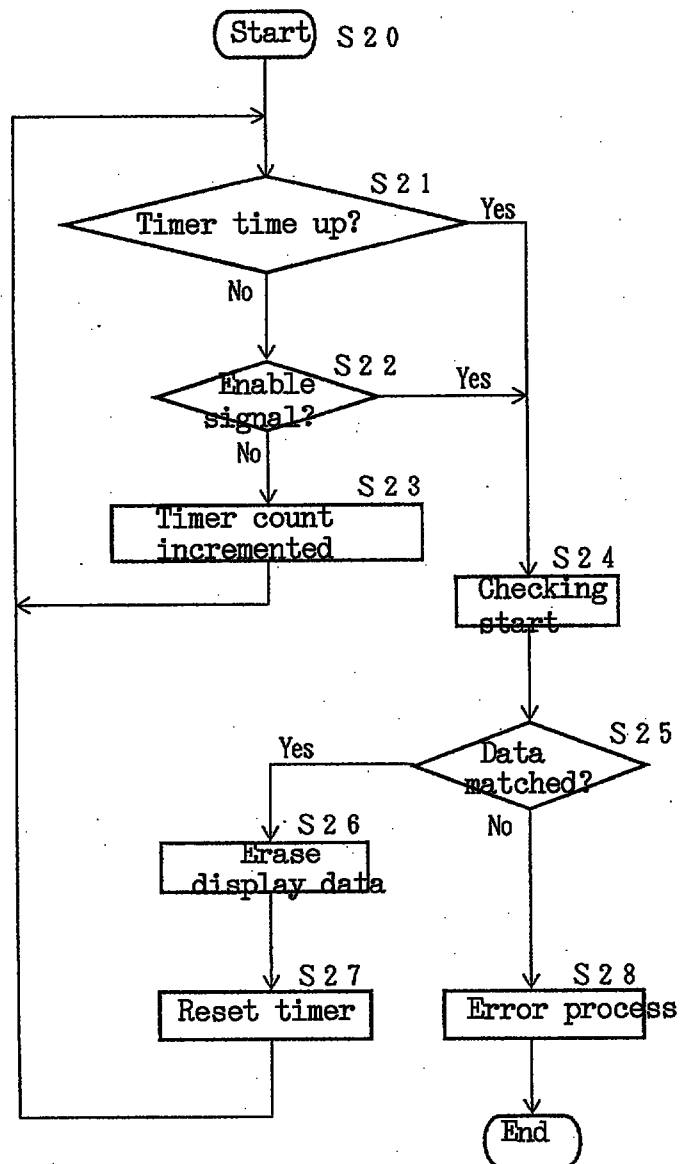


FIG. 6

Controller

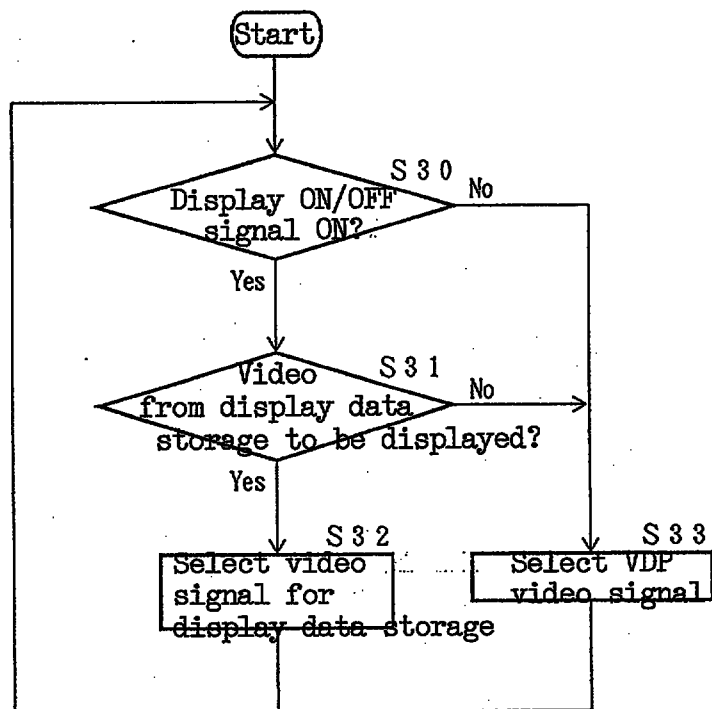


FIG. 7

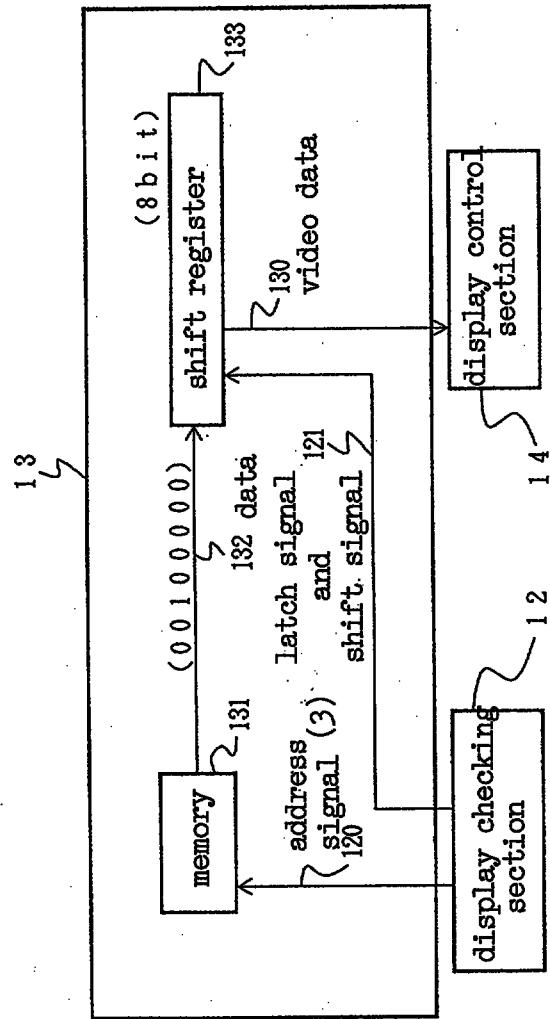


FIG. 8A

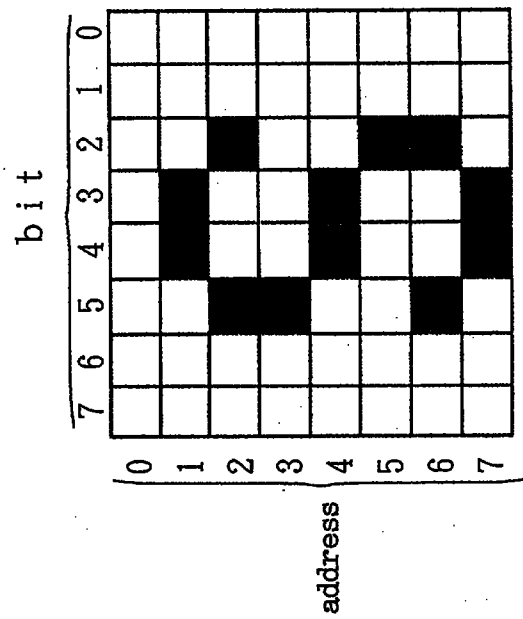
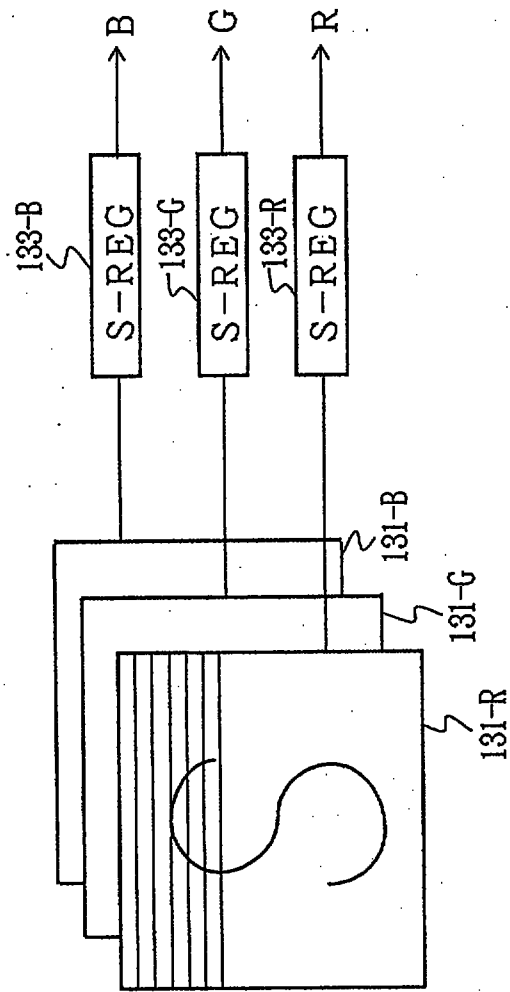


FIG. 8B

bit							
7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0
0	0	0	1	1	0	0	0
0	0	1	0	0	1	0	0
0	0	1	0	0	0	0	0
0	0	0	1	1	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0

FIG. 9



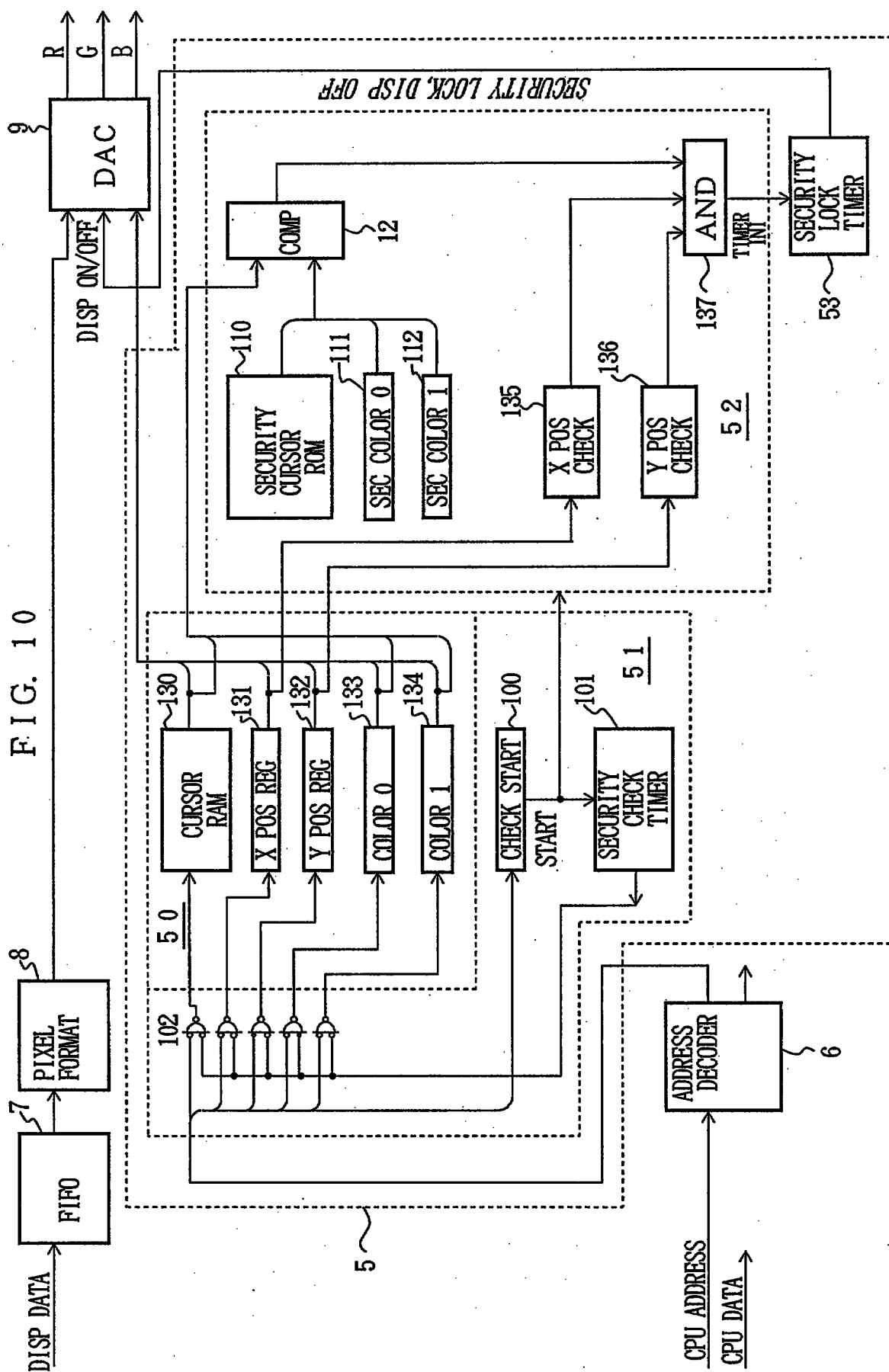
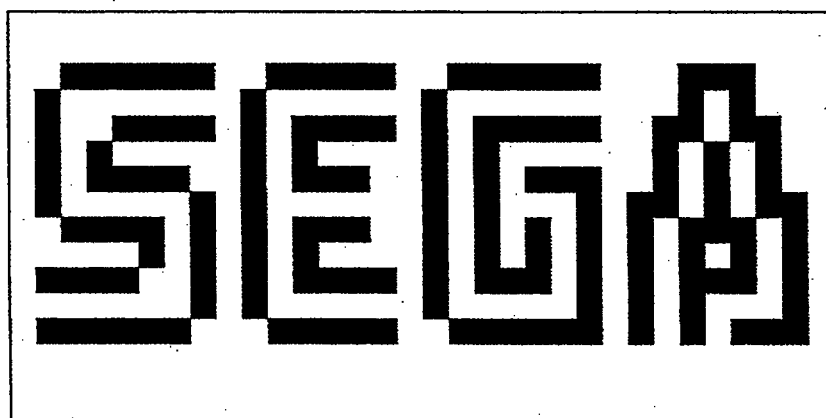


FIG. 11





THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

07 OCT 1996

- 40 -

1. An information processing apparatus having a security checking function, comprising:

an external memory device for storing a program and display data;

an information processing console to which said external memory device is detachably connected, including,

a CPU for executing the program that is read out from said external memory device,

an internal memory device for storing comparison reference data, and

a security checking device for repeatedly comparing said comparison reference data with said display data read out from said external memory device as the CPU executes said program read out from said external memory device; and

a display device for displaying the display data that are read out from said external memory device.

2. The information processing apparatus according to claim 1,

wherein the fact that said display data are displayed on said display device means infringement by an unauthorised person of a legal right accruing to the display data.

3. The information processing apparatus according to claim 1 or 2,

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU transfers and stores said display data from said external memory device to said display data storage device in accordance with the program that is stored in said external memory device.

4. The information processing apparatus according to claim 3,

wherein said display data are transferred from said external memory device to and are stored in said display data storage device before said security checking device performs data comparison, and after said data comparison by said security checking device and the display of said

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

07 OCT 1996

- 41 -

display data by said display device are completed ~~said~~ display data are erased from said display data storage device.

5. A security checking method for checking authenticity of a program in an information processing apparatus, comprising:

a first step of reading a program and display data out from an external memory device in which said program and said display data are stored;

a second step of outputting a checking start signal based on a display checking start command included in said program read out from said external memory device;

a third step of comparing said display data read out from said external memory device with comparison reference data when a checking start signal is output, and generating an error signal when said display data do not match said comparison reference data; and

a fourth step of, in response to said error signal, preventing execution of at least one part of said program.

6. The security checking method according to claim 5, further comprising a fifth step of, when said display data match said comparison reference data at said third step, generating a control signal for displaying said display data, and displaying said display data based on said control signal.

7. The security checking method according to claim 5 or 6,

wherein said display data that are stored in said external memory device are read in at said first step in consonance with said program.

8. The security checking method according to claim 5, 6, or 7,

wherein comparison of said display data with said comparison reference data at said third step is repeatedly performed during the execution of said program.

9. The security checking method according to claim 7 or 8, further comprising a sixth step of, after said display

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

07 OCT 1996

- 42 -

data are displayed at said fifth step, erasing said display data that have been read in.

10. An external memory device, which is detachably connected to an information processing console, for storing a program, to be executed by said information processing console, and display data, to be displayed under control by said information processing console, and from which said display data are read in said information processing console in consonance with said program.

11. The external memory device according to claim 10, wherein said information processing console is a video game machine, and wherein said display data that are displayed on a display device inhibits the use of a program by an unauthorised person.

12. The external memory device according to claim 11, wherein said display data are a trademark for a party that is authorised for said program.

13. The external memory device according to claim 10, wherein said information processing apparatus is a video game machine, and wherein said display data are displayed according to said program each predetermined timing during an execution of a video game.

14. A video signal control device for controlling the display of a first video signal and a second video signal which has a priority of displaying to the first video signal, comprising:

- a read-only memory for storing a reference display data which is compared with a display data of said second video signal;

- a comparing circuit for comparing the reference display data with said display data of the second video signal;

- a control circuit for inhibiting the display of said first video signal after a predetermined time has elapsed, when said comparing circuit detects that the reference display data does not coincide with the display data of the second video signal.

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

07 OCT 1996

- 43 -

15. The video signal control device according to claim 14,

wherein there is further comprised a timing circuit for controlling the period of displaying said second video signal, during which an observer can recognised the display data of the second video signal.

16. The video signal control device according to claim 14,

wherein said display data of the second video signal includes a security cursor constituted by a bit map pattern and a display position at which the security cursor is displayed, said comparing circuit compares the display position of the second video signal with a reference display position data which is included in said reference display signal, and said control circuit inhibits the display of the first video signal when the display position of the security cursor is not present within an allowable display area which is defined by the reference display position.

17. The video signal control device according to claim 16,

wherein said bit map pattern is stored in said read only memory, with a fixed largeness so that an observer can recognise the second display data.

18. The video signal control device according to claim 16,

wherein said security cursor constituted by the bit map pattern is a specific logo mark.

19. The information processing apparatus according to claim 1, wherein said display data are read out from said external memory device only once when said CPU executes said program.

20. The information processing apparatus according to claim 1, wherein said display data are read out from said external memory device repeatedly as said CPU executes said program.

21. The information processing apparatus according to claim 1, wherein said display data are displayed on said

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

07 OCT 1996

- 44 -

display device only once when said CPU executes said program.

22. An information processing apparatus having a security checking function, comprising:

an external memory device for storing a program and display data;

an information processing console to which said external memory device is detachably connected, including,

a CPU for executing the program that is read out from said external memory device,

an internal memory device for storing comparison reference data, and

a security checking device for comparing said comparison reference data with said display data read out from said external memory device; and

a display device on which the CPU displays said display data in accordance with the program stored in said external memory device.

23. The information processing apparatus according to claim 22,

wherein said display data displayed on said display device depicts a representation of a legal right which is associated with an external memory device authorised for use with said information processing console.

24. The information processing apparatus according to claim 22,

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU transfers and stores said display data from said external memory device to said display data storage device in accordance with the program that is stored in said external memory device.

25. The information processing apparatus according to claim 22, wherein said display data are read out from said external memory device only once when said CPU executes said program.

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

07 OCT 1996

- 45 -

26. The information processing apparatus according to claim 22, wherein said display data are read out from said external memory device repeatedly as said CPU executes said program.

27. The information processing apparatus according to claim 22, wherein said display data are displayed on said display device only once when said CPU executes said program.

28. An information processing console having a security checking function, comprising:

a CPU for executing a program received externally of said console;

an internal memory device for storing comparison reference data; and

a security checking and display control device for repeatedly comparing comparison reference data with display data received externally of said console as the CPU executes said externally received program, and controlling the display of said externally received display data on a display device.

29. The information processing console according to claim 28,

wherein said display data displayed on said display device depicts a representation of a legal right which is associated with said externally received program which is authorised for use with said information processing console.

30. The information processing console according to claim 28,

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU stores said externally received display data to said display data storage device in accordance with said externally received program.

31. The information processing console according to claim 30,

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

- 46 -

REPLACEMENT SHEET

07 OCT 1996

wherein said display data are stored ~~in said display~~ data storage device before said security checking device performs said data comparison, and after said data comparison by said security checking device and the display of said display data by said display device are completed, said display data are erased from said display data storage device.

32. The information processing console according to claim 28, wherein said display data are externally received only once when said CPU executes said program.

33. The information processing console according to claim 28, wherein said display data are externally received repeatedly as said CPU executes said program.

34. The information processing console according to claim 28, wherein said display data are displayed on said display device only once when said CPU executes said program.

35. The information processing console according to claim 28, wherein said display data are externally received from an external memory device.

36. The information processing console according to claim 28, wherein said program is externally received from an external memory device.

37. An information processing console having a security checking function, comprising:

a CPU for executing a program received externally of said console;

an internal memory device for storing comparison reference data; and

a security checking and display control device for comparing comparison reference data with display data received externally of said console, and controlling the display of said externally received display data on a display device in accordance with said externally received program.

38. The information processing console according to claim 37,

This Sheet Has Been Replaced





THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

07 OCT 1996

- 47 -

wherein said display data displayed on said display device depicts a representation of a legal right which is associated with said externally received program which is authorised for use with said information processing console.

39. The information processing console according to claim 37,

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU stores said externally received display data to said display data storage device in accordance with said externally received program.

40. The information processing console according to claim 37, wherein said display data are externally received only once when said CPU executes said program.

41. The information processing console according to claim 37, wherein said display data are externally received repeatedly as said CPU executes said program.

42. The information processing console according to claim 37, wherein said display data are displayed on said display device only once when said CPU executes said program.

43. The information processing console according to claim 37, wherein said display data are externally received from an external memory device.

44. The information processing console according to claim 37, wherein said program is externally received from an external memory device.

This Sheet Has Been Replaced



07 JUN 1999

information processing apparatus is performed by determining whether security codes, etc., match before a program, such as a game program, is executed. Once the execution of a program has begun, further security checking is not performed, or else can not be performed, for the duration of the execution of the program.

In a sequence of a program, therefore, steps for security checking processing are disabled or bypassed by some means, usually illegally, and as a result, the following steps in the program are performed though without the security check.

In addition, according to the security checking method described in USP486, USP596 or USP076, display data, such as a trademark, are merely displayed momentarily; the information processing apparatus neither checks to determine whether or not the correct image of a trademark, etc., is actually displayed, nor is it designed to do so.

Further, as is described above, when the steps for processing the security checking are disabled or bypassed in some manner, specific data can not be displayed and the authenticity of a program can not be examined.

07 JUN 1999

SUMMARY OF THE INVENTION

It is an object of the present invention to ameliorate one or more disadvantages of the prior art.

According to one aspect of the present invention there is provided an information processing apparatus having a security checking function, comprising:

an external memory device for storing a program and display data;

an information processing console to which said external memory device is detachably connected, including,

a CPU for executing the program that is read out from said external memory device,

an internal memory device for storing comparison data, and

a security checking device for comparing said comparison reference data with said display data read out from said external memory device in response to a checking start signal, said checking start signal being based on a display checking start command included in said program read out from said external memory device; and

a display device for displaying the display data that are read out from said external memory device if said display data read out from said external memory device matches said comparison reference data,

wherein said security checking device repeatedly compares said display data with said comparison reference data as the CPU executes said program read out from said external memory.

07 JUN 1999

According to another aspect of the present invention there is provided a security checking method for checking authenticity of a program in an information processing apparatus, comprising:

a first step of reading a program and display data out from an external memory device in which said program and said display data are stored;

a second step of outputting a checking start signal based on a display checking start command included in said program read out from said external memory device;

a third step of comparing said display data read out from said external memory device with comparison reference data when a checking start signal is output, and generating an error signal when said display data do not match said comparison reference data; and

a fourth step of, in response to said error signal, preventing execution of at least one part of said program,

wherein comparison of said display data with said comparison reference data at said third step is repeatedly performed during the execution of said program.

According to still another aspect of the present invention there is provided an external memory device, which is detachably connected to an information processing console, for storing a program, to be executed by said information processing console, and display data, to be displayed under control by said information processing console, and from which said display data are read in said information processing console in consonance with said program, wherein said display data are displayed according to said program each predetermined time during an execution of said program.

THIS SHEET HAS BEEN
REPLACED

7

REPLACEMENT SHEET

07 JUN 1999

According to still another aspect of the present invention there is provided a video signal control device for controlling the display of a first video signal and a second video signal which has a priority of displaying to the first video signal, comprising:

a read-only memory for storing a reference display data which is compared with a display data of said second video signal;

a comparing circuit for comparing the reference display data with said display data of the second video signal;

a control circuit for inhibiting the display of said first video signal after a predetermined time has elapsed, when said comparing circuit detects that the reference display data does not coincide with the display data of the second video signal; and

a timing circuit for controlling the period of displaying said second video signal, during which an observer can recognize the display data of the second video signal,

wherein said display data of the second video signal includes a security cursor constituted by a bit map pattern and a display position at which the security cursor is displayed, said comparing circuit compares the display position of the second video signal with a reference display position data which is included in said reference display data, and said control circuit inhibits the display of the first video signal when the display position of the security cursor is not present within an allowable display area which is defined by the reference display position.

According to still another aspect of the present invention there is provided an information processing apparatus having a security checking function, comprising:

an external memory device for storing a program and display data;

This Sheet Has Been Replaced



07 JUN 1999

an information processing console to which said external memory device is detachably connected, including,

a CPU for executing the program that is read out from said external memory device,

an internal memory device for storing comparison reference data, and

a security checking device for comparing said comparison reference data with said display data read out from said external memory device in response to a checking start signal, said checking start signal being based on a display checking start command included in said program read out from said external memory device; and

a display device on which the CPU displays said display data in accordance with the program stored in said external memory device if said display data read out from said external memory device matches said comparison reference data,

wherein said security checking device repeatedly compares said display data with said comparison reference data during the execution of the program by the CPU.

According to still another aspect of the present invention there is provide an information processing console having a security checking function, comprising:

a CPU for executing a program received externally of said console;

an internal memory device for storing comparison reference data; and

a security checking and display control device for repeatedly comparing comparison reference data with display data received externally of said console in response to a checking start signal, said checking start signal being based on a display checking start command included in said externally received program, as the CPU executes said

07 JUN 1999

externally received program, and controlling the display of said externally received display data on a display device.

According to still another aspect of the present invention there is provided an information processing console having a security checking function, comprising:

a CPU for executing a program received externally of said console;

an internal memory device for storing comparison reference data; and

a security checking and display control device for repeatedly comparing comparison reference data with display data received externally of said console in response to a checking start signal, said checking start signal being based on a display checking start command included in said externally received program, and controlling the display of said externally received display data on a display device in accordance with said externally received program, during the execution of the program by said CPU.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram for one embodiment of the present invention;

Fig. 2 is a block diagram illustrating an example

07 JUN 1999

Claims

1. An information processing apparatus having a security checking function, comprising:

an external memory device for storing a program and display data;

an information processing console to which said external memory device is detachably connected, including,

a CPU for executing the program that is read out from said external memory device,

an internal memory device for storing comparison data, and

a security checking device for comparing said comparison reference data with said display data read out from said external memory device in response to a checking start signal, said checking start signal being based on a display checking start command included in said program read out from said external memory device; and

a display device for displaying the display data that are read out from said external memory device if said display data read out from said external memory device matches said comparison reference data,

wherein said security checking device repeatedly compares said display data with said comparison reference data as the CPU executes said program read out from said external memory.

2. The information processing apparatus according to claim 1,

wherein the fact that said display data are displayed on said display device means infringement by an unauthorized person of a legal right accruing the display data.

3. The information processing apparatus according to claims 1 or 2,



07 JUN 1999

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU transfers and stores said display data from said external memory device to said display data storage device in accordance with the program that is stored in said external memory device.

4. The information processing apparatus according to claim 3,

wherein said display data are transferred from said external memory device to and are stored in said display data storage device before said security checking device performs data comparison, and after said data comparison by said security checking device and the display of said display data by said display device are completed, said display data are erased from said display data storage device.

5. A security checking method for checking authenticity of a program in an information processing apparatus, comprising:

a first step of reading a program and display data out from an external memory device in which said program and said display data are stored;

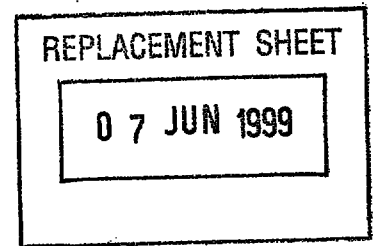
a second step of outputting a checking start signal based on a display checking start command included in said program read out from said external memory device;

a third step of comparing said display data read out from said external memory device with comparison reference data when a checking start signal is output, and generating an error signal when said display data do not match said comparison reference data; and

a fourth step of, in response to said error signal, preventing execution of at least one part of said program,



* C L M S *



wherein comparison of said display data with said comparison reference data at said third step is repeatedly performed during the execution of said program.

6. The security checking method according to claim 5, further comprising a fifth step of, when said display data match said comparison reference data at said third step, generating a control signal for displaying said display data, and displaying said display data based on said control signal.

7. The security checking method according to claim 5 or 6,

wherein said display data that are stored in said external memory device are read in at said first step in consonance with said program.

8. The security checking method according to claim 7, further comprising a sixth step of, after said display data are displayed at said fifth step, erasing said display data that have been read in.

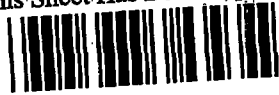
9. An external memory device, which is detachably connected to an information processing console, for storing a program, to be executed by said information processing console, and display data, to be displayed under control by said information processing console, and from which said display data are read in said information processing console in consonance with said program, wherein said display data are displayed according to said program each predetermined time during an execution of said program.

10. The external memory device according to claim 9, wherein said information processing console is a video game machine, and wherein said display data that are displayed on a display device inhibits the use of a program by an unauthorized person.

11. The external memory device according to claim 10, wherein said display data are a trademark for a party that is authorized for said program.



This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

43

REPLACEMENT SHEET

07 JUN 1999

12. A video signal control device for controlling the display of a first video signal and a second video signal which has a priority of displaying to the first video signal, comprising:

a read-only memory for storing a reference display data which is compared with a display data of said second video signal;

a comparing circuit for comparing the reference display data with said display data of the second video signal;

a control circuit for inhibiting the display of said first video signal after a predetermined time has elapsed, when said comparing circuit detects that the reference display data does not coincide with the display data of the second video signal; and

a timing circuit for controlling the period of displaying said second video signal, during which an observer can recognize the display data of the second video signal,

wherein said display data of the second video signal includes a security cursor constituted by a bit map pattern and a display position at which the security cursor is displayed, said comparing circuit compares the display position of the second video signal with a reference display position data which is included in said reference display data, and said control circuit inhibits the display of the first video signal when the display position of the security cursor is not present within an allowable display area which is defined by the reference display position.

13. The video signal control device according to claim 12,

wherein said bit map pattern is stored in said read only memory, with a fixed size so that an observer can recognize the second display data.

14. The video signal control device according to claim 12,



* C L N S *

07 JUN 1999

wherein said security cursor constituted by the bit map pattern is a specific logo mark.

15. The information processing apparatus according to claim 1, wherein said display data are read out from said external memory device only once when said CPU executes said program.

16. The information processing apparatus according to claim 1, wherein said display data are read out from said external memory device repeatedly as said CPU executes said program.

17. The information processing apparatus according to claim 1, wherein said display data are displayed on said display device only once when said CPU executes said program.

18. An information processing apparatus having a security checking function, comprising:

an external memory device for storing a program and display data;

an information processing console to which said external memory device is detachably connected, including,

a CPU for executing the program that is read out from said external memory device,

an internal memory device for storing comparison reference data, and

a security checking device for comparing said comparison reference data with said display data read out from said external memory device in response to a checking start signal, said checking start signal being based on a display checking start command included in said program read out from said external memory device; and



07 JUN 1999

a display device on which the CPU displays said display data in accordance with the program stored in said external memory device if said display data read out from said external memory device matches said comparison reference data,

wherein said security checking device repeatedly compares said display data with said comparison reference data during the execution of the program by the CPU.

19. The information processing apparatus according to claim 18,

wherein said display data displayed on said display device depicts a representation of a legal right which is associated with an external memory device authorized for use with said information processing console,

20. The information processing apparatus according to claim 18,

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU transfers and stores said display data from said external memory device to said display data storage device in accordance with the program that is stored in said external memory device.

21. The information processing apparatus according to claim 18,

wherein said display data are read out from said external memory device only once when said CPU executes said program.

22. The information processing apparatus according to claim 18, wherein said display data are read out from said external memory device repeatedly as said CPU executes said program.

23. The information processing apparatus according to claim 18, wherein said display data are displayed on said display device only once when said CPU executes said program.



07 JUN 1999

24. An information processing console having a security checking function, comprising:

a CPU for executing a program received externally of said console;
an internal memory device for storing comparison reference data; and
a security checking and display control device for repeatedly comparing comparison reference data with display data received externally of said console in response to a checking start signal, said checking start signal being based on a display checking start command included in said externally received program, as the CPU executes said externally received program, and controlling the display of said externally received display data on a display device.

25. The information processing console according to claim 24,

wherein said display data displayed on said display device depicts a representation of a legal right which is associated with said externally received program which is authorized for use with said information processing console.

26. The information processing console according to claim 24,

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU stores said externally received display data to said display data storage device in accordance with said externally received program.

27. The information processing console according to claim 26,

wherein said display data are stored in said display data storage device before said security checking device performs said data comparison, and after said data comparison by



* C L M S *

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

47

REPLACEMENT SHEET

07 JUN 1999

said security checking device and the display of said display data by said display device are completed, said display data are erased from said display data storage device.

28. The information processing console according to claim 24, wherein said display data are externally received only once when said CPU executes said program.

29. The information processing console according to claim 24, wherein said display data are externally received repeatedly as said CPU executes said program.

30. The information processing console according to claim 24, wherein said display data are displayed on said display device only once when said CPU executes said program.

31. The information processing console according to claim 24, wherein said display data are externally received from an external memory device.

32. The information processing console according to claim 24, wherein said program is externally received from an external memory device.

33. An information processing console having a security checking function, comprising:

a CPU for executing a program received externally of said console;

an internal memory device for storing comparison reference data; and

a security checking and display control device for repeatedly comparing comparison reference data with display data received externally of said console in response to a checking start signal, said checking start signal being based on a display checking start command included in said externally received program, and controlling the display of said externally received display data on a display device in accordance with said externally received program, during the execution of the program by said CPU.

34. The information processing console according to claim 33,



THIS SHEET HAS BEEN
REPLACED

48

REPLACEMENT SHEET

07 JUN 1999

wherein said display data displayed on said displayed device depicts a representation of a legal right which is associated with said externally received program which is authorized for use with said information processing console.

35. The information processing console according to claim 33,

wherein said information processing console further includes a display data storage device for storing the display data that are compared with said comparison reference data, and said CPU stores said externally received display data to said display data storage device in accordance with said externally received program.

36. The information processing console according to claim 33, wherein said display data are externally received only once when said CPU executes said program.

37. The information processing console according to claim 33, wherein said display data are externally received repeatedly as said CPU executes said program.

38. The information processing console according to claim 33, wherein said display data are displayed on said display device only once when said CPU executes said program.

39. The information processing console according to claim 33, wherein said display data are externally received from an external memory device

40. The information processing console according to claim 33, wherein said program is externally received from an external memory device.



THIS SHEET HAS BEEN
REPLACED

REPLACEMENT SHEET

49

07 JUN 1999

INFORMATION PROCESSING APPARATUS WITH SECURITY CHECKING FUNCTION

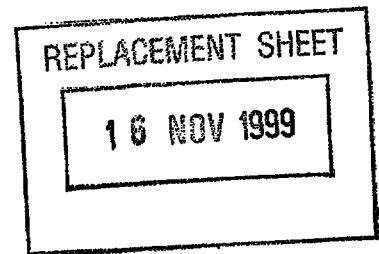
ABSTRACT

An information processing apparatus has a security checking function for ascertaining the authenticity of a program to be executed, and the program and display data (30) to be displayed are stored in an external storage device. The information processing apparatus, which has a CPU (10) for executing a program, is connected to the external storage device and a display device (3) for displaying the display data (30). During the execution of the program, the display data (30) stored in the external storage device are displayed on the display device (3) in consonance with that program. The display data (30) are compared with comparison reference data (11) that are stored in the information processing apparatus. When the two sets of data do not match, the operation of the CPU (10) of the information processing apparatus is halted, and further execution of the program is prevented.

Fig. 1

This Sheet Has Been Replaced





According to still another aspect of the present invention there is provided a video signal control device for controlling the display of a first video signal and a second video signal which has a priority of displaying to the first video signal, comprising:

a read-only memory for storing a reference display data which is compared with a display data of said second video signal;

a comparing circuit for comparing the reference display data with said display data of the second video signal;

a control circuit for inhibiting the display of said first video signal after a predetermined time has elapsed, when said comparing circuit detects that the reference display data does not coincide with the display data of the second video signal; and

a timing circuit for controlling the period of displaying said second video signal, during which an observer can recognize the display data of the second video signal,

wherein said display data of the second video signal includes a security cursor constituted by a bit map pattern and a display position at which the security cursor is displayed, said comparing circuit repeatedly compares the display position of the second video signal with a reference display position data which is included in said reference display data, and said control circuit inhibits the display of the first video signal when the display position of the security cursor is not present within an allowable display area which is defined by the reference display position.

According to still another aspect of the present invention there is provided an information processing apparatus having a security checking function, comprising:

an external memory device for storing a program and display data:

16 NOV 1999

12. A video signal control device for controlling the display of a first video signal and a second video signal which has a priority of displaying to the first video signal, comprising:

a read-only memory for storing a reference display data which is compared with a display data of said second video signal;

a comparing circuit for comparing the reference display data with said display data of the second video signal;

a control circuit for inhibiting the display of said first video signal after a predetermined time has elapsed, when said comparing circuit detects that the reference display data does not coincide with the display data of the second video signal; and

a timing circuit for controlling the period of displaying said second video signal, during which an observer can recognize the display data of the second video signal,

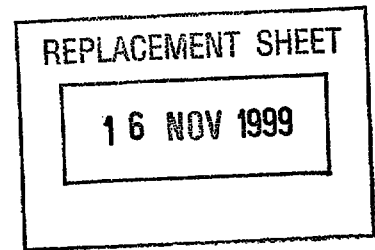
wherein said display data of the second video signal includes a security cursor constituted by a bit map pattern and a display position at which the security cursor is displayed, said comparing circuit repeatedly compares the display position of the second video signal with a reference display position data which is included in said reference display data, and said control circuit inhibits the display of the first video signal when the display position of the security cursor is not present within an allowable display area which is defined by the reference display position.

13. The video signal control device according to claim 12,

wherein said bit map pattern is stored in said read only memory, with a fixed size so that an observer can recognize the second display data.

14. The video signal control device according to claim 12.





said security checking device and the display of said display data by said display device are completed, said display data are erased from said display data storage device.

28. The information processing console according to claim 24, wherein said display data are externally received only once when said CPU executes said program.

29. The information processing console according to claim 24, wherein said display data are externally received repeatedly as said CPU executes said program.

30. The information processing console according to claim 24, wherein said display data are displayed on said display device only once when said CPU executes said program.

31. The information processing console according to claim 24, wherein said display data are externally received from an external memory device.

32. The information processing console according to claim 24, wherein said program is externally received from an external memory device.



INFORMATION PROCESSING APPARATUS WITH SECURITY CHECKING FUNCTION

ABSTRACT

An information processing apparatus has a security checking function for ascertaining the authenticity of a program to be executed, and the program and display data (30) to be displayed are stored in an external storage device. The information processing apparatus, which has a CPU (10) for executing a program, is connected to the external storage device and a display device (3) for displaying the display data (30). During the execution of the program, the display data (30) stored in the external storage device are displayed on the display device (3) in consonance with that program. The display data (30) are compared with comparison reference data (11) that are stored in the information processing apparatus. When the two sets of data do not match, the operation of the CPU (10) of the information processing apparatus is halted, and further execution of the program is prevented.

Fig. 1