

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第3651732号
(P3651732)

(45) 発行日 平成17年5月25日(2005.5.25)

(24) 登録日 平成17年3月4日(2005.3.4)

(51) Int. Cl.⁷

F I

G 1 1 B 20/10

G 1 1 B 20/10 H

G 0 6 F 12/14

G 1 1 B 20/10 3 2 1 Z

G 0 6 F 12/14 5 6 0 A

請求項の数 2 (全 13 頁)

(21) 出願番号	特願平9-107541	(73) 特許権者	000003078
(22) 出願日	平成9年4月24日(1997.4.24)		株式会社東芝
(65) 公開番号	特開平10-302393		東京都港区芝浦一丁目1番1号
(43) 公開日	平成10年11月13日(1998.11.13)	(74) 代理人	100058479
審査請求日	平成12年9月18日(2000.9.18)		弁理士 鈴江 武彦
		(74) 代理人	100084618
			弁理士 村松 貞男
		(74) 代理人	100068814
			弁理士 坪井 淳
		(74) 代理人	100092196
			弁理士 橋本 良郎
		(74) 代理人	100091351
			弁理士 河野 哲
		(74) 代理人	100088683
			弁理士 中村 誠

最終頁に続く

(54) 【発明の名称】 再生装置

(57) 【特許請求の範囲】

【請求項1】

C P U と C P U バスとを有する再生装置において、

オリジナルデータを暗号化し暗号化データを所定の受信手段へ所定のインターフェース規格に従って送信する第1の半導体チップを有する送信手段と、

前記送信手段とC P U バスに接続され、所定の送信手段からの暗号化データを前記所定のインターフェース規格に従って受信し暗号化データをC P U バスへ出力する第2の半導体チップを有する受信手段と、

前記第1、第2の半導体チップとにそれぞれ設けられ、前記第1の半導体チップが前記所定の受信手段へ暗号化データを送信する環境にあるか否か、及び前記第2の半導体チップが前記所定の送信手段からの暗号化データを受信する環境にあるか否かを判定し、該環境にある場合、送信、受信を許可する認証手段と、

前記C P U バスに接続され、受信手段から出力されC P U バスを介して入力された暗号化データを復号する第3の半導体チップとを具備し、

前記第1の半導体チップは、C P U とC P U バスを持たない専用の再生装置用のオリジナルデータ暗号化機能と暗号化データの所定のインターフェース規格に従った送信機能とを有する第4の半導体チップとは異なる形状とされ、前記送信手段に前記第1の半導体チップの代わりに前記第4の半導体チップを取り付けられることが防止され、

前記第2の半導体チップは、前記専用の再生装置用の暗号化データの所定のインターフェース規格に従った受信機能と暗号化データの復号機能とを有する第5の半導体チッ

10

20

ブとは異なる形状とされ、前記受信手段に前記第2の半導体チップの代わりに前記第5の半導体チップを取り付けることが防止されることを特徴とする再生装置。

【請求項2】

前記第1の半導体チップと前記第4の半導体チップはピンの配置が異なり、前記第2の半導体チップと前記第5の半導体チップはピンの配置が異なることを特徴とする請求項1記載の再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明はデジタル化された文書、音声、画像、プログラム等のデータの不正コピーを防止する再生装置に関するものである。

10

【0002】

【従来の技術】

最近、マルチメディアの発展に伴って機器のネットワーク化が進み、パーソナルコンピュータ等の汎用計算機間のみならず、オーディオ機器やビデオ機器等のオーディオビジュアル機器（AV機器）とのデータの送受信、ケーブルテレビや衛星放送のデジタル化等、データのデジタル化、ネットワーク化が一般的になりつつある。

【0003】

そこで、コンピュータとAV機器等のデジタル機器との間でデータの送受信を行うためのデジタルインターフェース方式の統一規格が検討されている。その中の一つにIEEE 1394がある。このIEEE 1394については、例えば新エレクトロニクス文庫（2）『次世代シリアルインターフェースIEEE1394がわかる本』エレクトロニクス1997年1月号付録、オーム社、に詳述されている。

20

【0004】

一方、近年デジタル記録再生機器の開発、製品化が進み、画質や音質の劣化なくデータをコピーすることが可能となっている。しかし高画質な複製は、海賊版と呼ばれる不正なコピーを増加させ、著作権が侵害されるという問題がある。このような不正なコピーは確実に防止されなければならない。というのも、インターネットやデジタルVTRやDVD-RAMの出現により、デジタル化された著作物は簡単にコピーされ、不特定多数への配布が可能となり、これによりデジタル画像の著作権者に危機感を与えているからである。

30

【0005】

このため、従来は、データを暗号化して通信または記録保存、読み出しをする暗号化通信または暗号化システムを用いることでこのような不正コピーを防止していた。

【0006】

【発明が解決しようとする課題】

しかしながら、デジタル化された文書、音声、画像、プログラムなどの圧縮されたマルチメディア・データをネットワークやケーブルを介して通信を行うデジタル記録再生システム、また上記デジタルデータを記録保存、読み出しするデジタル記録再生システムにおいては、専用機器であるAV機器のみならず汎用性の高い計算機もが用いられることで次のような問題が発生する。

40

【0007】

すなわち、パーソナルコンピュータ（以下、パソコンともいう）のような汎用計算機を通してマルチメディア・データを再生する場合には、CPUバスを介してデータを処理するため、たとえ上記暗号化技術が用いられていても、暗号が解除された表示出力前のCPUバスを流れるデータコピーすることが可能となる。

【0008】

したがって、ソフトウェア手段でパソコンを制御すれば、上記マルチメディア・データを容易にコピーすることができ、不正なコピーが可能となる。このように、IEEE 1394等のインターフェースを用いて著作物を流通させた場合、パソコン等の計算機が不正コ

50

ピーを助長するものになってしまう。

【0009】

また、コンピュータとAV機器等とのデジタルインターフェース方式の統一規格であるIEEE1394は、その汎用性から広く普及するものと予想されるが、その時にはコンピュータとAV機器等との組み合わせの場合のみでなく、コンピュータのみの場合やAV機器等のみの場合であってもIEEE1394が使用されるものと考えられる。

【0010】

かかる状況にあっては、上記したようにパソコンを使用した場合の不正コピー防止のみならず、コンピュータとAV機器との全体を考慮した不正コピー防止対策を講じなければならない。さもなければIEEE1394における、コンピュータとAV機器等との統一規格としての意義が失われるからである。

10

【0011】

本発明は、このような実情を考慮してなされたもので、AV機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっては、CPUバス上を流れるデータのコピーによる不正なコピーを防止することが可能な再生装置を提供することを目的とする。

【0012】

【課題を解決するための手段】

本発明の一実施態様によれば、CPUとCPUバスとを有する再生装置において、オリジナルデータを暗号化し暗号化データを所定の受信手段へ所定のインターフェース規格に従って送信する第1の半導体チップを有する送信手段と、前記送信手段とCPUバスに接続され、所定の送信手段からの暗号化データを前記所定のインターフェース規格に従って受信し暗号化データをCPUバスへ出力する第2の半導体チップを有する受信手段と、前記第1、第2の半導体チップとにそれぞれ設けられ、前記第1の半導体チップが前記所定の受信手段へ暗号化データを送信する環境にあるか否か、及び前記第2の半導体チップが前記所定の送信手段からの暗号化データを受信する環境にあるか否かを判定し、該環境にある場合、送信、受信を許可する認証手段と、前記CPUバスに接続され、受信手段から出力されCPUバスを介して入力された暗号化データを復号する第3の半導体チップとを具備し、前記第1の半導体チップは、CPUとCPUバスを持たない専用の再生装置用のオリジナルデータ暗号化機能と暗号化データの所定のインターフェース規格に従った送信機能とを有する第4の半導体チップとは異なる形状とされ、前記送信手段に前記第1の半導体チップの代わりに前記第4の半導体チップを取り付けられることが防止され、前記第2の半導体チップは、前記専用の再生装置用の暗号化データの所定のインターフェース規格に従った受信機能と暗号化データの復号機能とを有する第5の半導体チップとは異なる形状とされ、前記受信手段に前記第2の半導体チップの代わりに前記第5の半導体チップを取り付けることが防止されるものである。

20

30

【0013】

本発明は、このような手段を設けたので、半導体チップを交換することによる不正コピーを防止することができる。

【0035】

40

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

(発明の第1の実施の形態)

本発明にかかるデジタル記録再生システムには、マルチメディア・データをネットワークやケーブルあるいは衛星を介して受信し再生出力する場合やDVD-RAM、D-VC RやCDROM-R等から取り出したデータを再生出力する場合等、種々の形態が考えられる。しかし、何れにしてもどこかの段階で暗号化されたデータをIEEE1394により再生手段本体に伝送し、再生手段本体にて暗号を解いて再生出力することとなる。

【0036】

本実施形態では、MPEG2方式で圧縮されたデジタル画像をIEEE1394でつな

50

がれたDVD-RAM, D-VCR等の記録取出部分と、記録再生AVの再生部分やパソコン等の再生機器部分と間でやり取りする場合について説明する。

【0037】

まず、記録再生AVにより記録再生する場合について説明する。

図1は本発明の第1の実施の形態に係るデジタル記録再生システムの一例を示す構成図であり、再生機器部分にDVD-RAM, D-VCR等の専用デジタル記録再生AV機器を用いる場合を示している。

【0038】

この専用デジタル記録再生AV機器100においては、送信機器101によりDVD-RAM等から再生対象となるMPEG2画像103が取出されIEEE1394ケーブル105を介して送信される。また、送信機器101から送信されたデータが専用デジタル記録再生AV機器本体である受信機器102によりディスプレイ120に再生出力されるようになっている。

10

【0039】

送信機器101は、DVD-RAM等からデータ圧縮されたMPEG2画像103を取り出す部分(図示せず)と、IEEE1394のインターフェースの送信チップユニット104とから構成される。

【0040】

一方、受信機器102は、IEEE1394のインターフェースの受信チップユニット106と、MPEG2画像を復号するための処理部107とから構成される。

20

【0041】

送信チップユニット104は、IEEE1394暗号化部109とIEEE1394I/F部110aを具備する。ここで、各部109, 110aは1チップ(1LSI, 複合チップを含む)としての送信チップユニット104内に設けられていてもよいし、各部109, 110aはそれぞれが1チップであり、送信チップユニット104はこれらのチップセットからなっているもよい。

【0042】

一方、受信チップユニット106は、IEEE1394I/F部110bとIEEE1394復号化部111とを具備する。ここで、各部110b, 111も送信チップユニット104の場合と同様に、各部110b, 111はそれぞれが1チップで受信チップユニット106がこれらのチップセットであっても、各部110b, 111が1チップの受信チップユニット106内に設けられていてもよい。

30

【0043】

また、IEEE1394I/F部110aとIEEE1394I/F部110bとは、IEEE1394インターフェース規格にしたがってIEEE1394ケーブル105を介して両者間でデータ伝送を行うものである。

【0044】

ここで、IEEE1394I/F部110bは、自己が設けられるのが専用デジタル記録再生AV機器100であることを認識できる構成となっている。かかる認識はIEEE1394I/F部110bの認識部130によりなされるが、認識部130は、IEEE1394I/F部110bがAV機器用のLSIという情報を保持することで認識するようになっていてもよいし、また、IEEE1394I/F部110bがIEEE1394復号化部111と組み合わせられているということから認識するようになっていてもよい。前述の認識方法は、IEEE1394I/F部110bとIEEE1394復号化部111とが別々のチップとなっているときに特に有効であり、後述の方法はこれらが一体のチップとなっているときに特に有効である。また、その他の認識方法を用いてもよい。

40

【0045】

次に、IEEE1394暗号化部109とIEEE1394復号化部111とによる再生データ103の暗号化及び復号化について説明する。

まず、送信機器101内において、MPEG2画像データ103は暗号鍵Sk(108)

50

を用いて I E E E 1 3 9 4 暗号化部 1 0 9 により暗号化される。暗号化方式は D E S や I D E A 等のブロック暗号でも構わないし、ストリーム暗号、公開鍵暗号でも構わない。本実施形態では、暗号化する鍵と復号化する鍵とが同じである共通鍵暗号方式を用いるものとする。なお、公開鍵方式の場合は、受信機器 1 0 2 から公開鍵を送ってもらい、受信機器 1 0 2 の公開鍵で暗号化すれば良い。この場合、受信機器 1 0 2 は自分が保持している秘密鍵により暗号を解くことになる。

【 0 0 4 6 】

暗号化されたデータは、I E E E 1 3 9 4 I / F 部 1 1 0 a において I E E E 1 3 9 4 で規定されたフォーマットにされる。I E E E 1 3 9 4 ケーブル 1 0 5 を介して受信機器 1 0 2 へ送られる。受信機器 1 0 2 では I E E E 1 3 9 4 I / F 部 1 1 0 b においてデータ 10

【 0 0 4 7 】

さて、ここで I E E E 1 3 9 4 I / F 部 1 1 0 a から I E E E 1 3 9 4 I / F 部 1 1 0 b への正常なデータ伝送が実施できるのは、これらが専用デジタル記録再生 A V 機器用の I / F セットとして正規なものが装着されているからである。すなわち I E E E 1 3 9 4 I / F 部 1 1 0 a と I E E E 1 3 9 4 I / F 部 1 1 0 b とは通信時にお互いの認証を取り合うが、そのときに認識部 1 3 0 の機能により I E E E 1 3 9 4 I / F 部 1 1 0 b がどのようなものであるかが認識され、当該 I / F 部 1 1 0 b が専用デジタル記録再生 A V 機器用の I / F 部でなければ通信が行われなくなっている。 20

【 0 0 4 8 】

このようにして不正な I E E E 1 3 9 4 インターフェースチップが用いられた場合には、送信機器 1 0 1 ~ 受信機器 1 0 2 間の通信ができないようになっているが、受信機器 1 0 2 において受信復号化できた場合にはさらに以下のように処理される。まず、復号された M P E G 2 画像データは M P E G 2 画像を復号するための処理部 1 0 7 において、M P E G 2 圧縮されたデータがデータ復号部 1 1 2 で解凍される。そして、解答データが D / A 変換部 1 1 3 でデジタル信号からアナログ信号に変換されて、例えばディスプレイ装置 1 2 0 へ送られ再生される。

【 0 0 4 9 】

さて、ここで暗号鍵 S k を I E E E 1 3 9 4 ケーブル 1 0 5 を介してどのように共有するかについて説明する。この方法については、例えば D V D - R O M における B U S K e y の共有方式を用いればよい。 30

【 0 0 5 0 】

この B U S K e y の共有方式については、『ニュースレポート DVD-ROM 装置用の標準インターフェースが固まる暗号鍵の安全な交換手順を規定』, 日経エレクトロニクス 1996.11.18 (No.676), pp.13 ~ pp.14 に詳述されている。

【 0 0 5 1 】

この方法では、まず、受信機器 1 0 2 において乱数発生器などでチャレンジ鍵 1 (1 0 バイト長) を生成し、送信機器 1 0 1 へ送る。送信機器 1 0 1 では送られたチャレンジ鍵 1 で K e y 1 (5 バイト長) を生成し、受信機器 1 0 2 では同様にチャレンジ鍵 1 で上記と同じ K e y 1 を生成する。K e y 1 の生成は、一方向性関数などを用いて生成される。次に、送信機器 1 0 1 はやはり乱数発生器を用いてチャレンジ鍵 2 (1 0 バイト長) を生成し、受信機器 1 0 2 へ送る。受信機器 1 0 2 では送られたチャレンジ鍵 2 を用いて K e y 2 (5 バイト長) を生成する。同様に送信機器 1 0 1 では生成したチャレンジ鍵 2 を用いて K e y 2 を生成する。こうして送信機器 1 0 1、受信機器 1 0 2 で K e y 1, K e y 2 が共有できる。そこで、この K e y 1 及び K e y 2 を用いて B U S K e y を生成する。以上のような手順を用いれば、I E E E 1 3 9 4 ケーブル 1 0 5 を介して、ケーブル内を暗号化するための鍵をやり取りする必要もなくなり、安全な鍵共有を図ることが可能となる。さらに、この B U S K e y は毎回変わる K e y 1 及び K e y 2 を用いて作成し、有効なのは 1 回限りである。このようにして安全性を高めている。 40

【0052】

このようにして、専用デジタル記録再生AV機器100の場合には、パーソナルコンピュータと異なりCPUバスを持たないため、暗号を復号する部分と圧縮を復号する部分と受信チップユニット106と処理部107とにわけて構成し、暗号が復号されたデータを圧縮画像の復号部112へ送っても構わない。しかし、図1の構成をパーソナルコンピュータへ適用すれば、暗号が復号されたデータはCPUバスを経由して圧縮画像の復号部へ送られるため、IEEE1394ケーブル105上を暗号化する意味がなくなってしまう。

【0053】

そこで、再生機器部分にパーソナルコンピュータを用いる場合について説明する。図2は本発明の第1の実施の形態に係るデジタル記録再生システムの他の例を示す構成図であり、再生機器部分にパーソナルコンピュータを用いる場合を示している。

10

【0054】

このデジタル記録再生システムにおいては、送信機器201によりDVD-RAM等から再生対象となるMPEG2画像203が取出されIEEE1394ケーブル205を介して送信される。また、送信機器201から送信されたデータがパーソナルコンピュータである受信機器202によりディスプレイ220に再生出力されるようになっている。

【0055】

送信機器201は、DVD-RAM等からデータ圧縮されたMPEG2画像203を取り出す部分(図示せず)と、IEEE1394暗号化部209とIEEE1394I/F部210aとからなるIEEE1394のインターフェースの送信チップユニット204とによって構成されている。

20

【0056】

ここで、IEEE1394暗号化部209、IEEE1394I/F部210a、送信チップユニット204は、受信機器202に対応するものとなっている他、図1で説明したIEEE1394暗号化部109、IEEE1394I/F部110a、送信チップユニット104と同様なものとなっている。

【0057】

一方、パソコンである受信機器202は、CPUバス240に、CPU241、RAM242、ROM243、IEEE1394のインターフェースの受信チップユニット106及びMPEG2画像を復号するための処理部207が接続されてなっている。

30

【0058】

ここで、CPU241は受信機器202を制御するものであり、RAM242及びROM243はCPU241等の動作において使用されるものである。

受信チップユニット206は、IEEE1394I/F部110bからなっており、本実施形態では1チップ(1LSI、複合チップを含む)から構成されている。

【0059】

IEEE1394I/F部210bには、認識部230が設けられており、認識部130は、IEEE1394I/F部210bがAV機器用のLSIという情報を保持することで認識するようになっていてもよいし、また、IEEE1394I/F部210bが受信チップユニット206においてIEEE1394復号化部211と組み合わせられていないということから認識するようになっていてもよい。さらにその他の方法でもよい。

40

【0060】

処理部207は、IEEE1394復号化部211と、データ復号部212と、D/A変換部213とからなっており、データ復号部212及びD/A変換部213は、図1に示すデータ復号部112及びD/A変換部113と同様に構成されている。

【0061】

IEEE1394復号化部211は、暗号を解読し復号化する機能としては図1のIEEE1394復号化部111と同様であるが、その位置が受信チップユニット206でなく処理部207に配置されている。

50

【0062】

送信機器201から受信機器202へのデータ送信における暗号化については、DESやIDEA等のブロック暗号や、ストリーム暗号、公開鍵暗号でも構わない。本実施形態では、専用デジタル記録再生AV機器100の場合と同様、暗号化する鍵と復号化する鍵とが同じである共通鍵暗号方式を用いるものとし、暗号鍵の共有は上記したDVD-ROMにおける鍵共有方式と同様な方式を用いるものとする。

【0063】

このように構成されるパソコンを含むデジタル記録再生システムにおいては、まず、DVD-RAM等から取り出されたMPEG2画像データ203がIEEE1394暗号化部209にて暗号化され、専用デジタル記録再生AV機器100の場合と同様にIEEE1394I/F部210aから受信機器202のIEEE1394I/F部210bに送信される。

10

【0064】

ここで暗号化されたデータは、CPUバス240を經由して処理部207へ送られる。したがって、CPUバス240上を流れるデータをコピーしても、データには暗号がかかっており、また、暗号化に用いた鍵(BUSKey)も上述の通り一時的なものである。したがって、CPUバス240上を流れるデータのコピーでは、当該データを再生できず、後に同データを処理部207へ送ったとしてもBUSKeyが一時的なものであるため再生することは不可能である。

【0065】

一方、正規にCPUバス240を經由して送られた暗号化されたデータは、送信機器201と共有された暗号鍵Sk(208)を用いて復号化部211において復号される。復号されたMPEG2画像データはデータ復号部212で解凍され、D/A変換部213でデジタル信号からアナログ信号に変換されて、ディスプレイ装置220などへ送られる。

20

【0066】

ところで上記場合に、IEEE1394I/F部210aからIEEE1394I/F部210bへの正常なデータ伝送が実施できるのは、これらに正規なものが装着されているからである。具体的にはパソコンやワークステーション等のソフトウェアでコントロール可能なCPUバスをもつ機器を有するデジタル記録再生システム用のI/Fセットとして正規なものということである。すなわち専用デジタル記録再生AV機器100の場合で説明したように、IEEE1394I/F部210aとIEEE1394I/F部210bとは通信時にお互いの認証を取り合うが、そのときに認識部230の機能によりIEEE1394I/F部210bがどのようなものであるかが認識される。そして、当該I/F部210bがパソコン等を用いたデジタル記録再生システム用のI/F部でなければ通信が行われなくなっている。

30

【0067】

このように、IEEE1394インターフェースように、コンピュータとAV機器等との統一規格であるインターフェースを用いた場合には、デジタルデータの再生機器部分としては、パソコン等で代表されるソフトウェアでコントロール可能なCPUバスをもつ機器が用いられる場合と、このようなCPUバスをもたない機器が用いられる場合に大別される。図1に示すシステムは前者の再生機器部分が用いられる場合であり、図2に示すシステムは後者の再生機器部分が用いられる場合である。これらの違いは各認識部130, 230により区別され、それぞれ対応するI/F部110b, 210bが用いられるときのみ正常に動作する。このような区別を確実にを行うことによりコンピュータとAV機器等のいずれも接続できるIEEE1394インターフェースにおいて、再生機器部分にコンピュータとAV機器のいずれを用いての確実に両者を区別し、かつそれぞれに対応するやり方で不正コピーを防止できることとなる。

40

【0068】

上述したように、本発明の実施の形態に係るデジタル記録再生システム及び不正コピーを防止する方法は、コンピュータ等とAV機器等のデジタル機器何れかに対応したIE

50

IEEE 1394 I/F部 110b, 210bと、IEEE 1394 I/F部 110a, 110bに設けられかつI/F部手段 110b, 210bが何れのデジタル機器に対応するかを認識可能とする認識部 130, 230とを具備し、I/F部がその対応するデジタル機器に設けられているときのみ、送信機器 101, 201と受信機器 102, 202間で正常なデータ伝送を行うようにしたので、AV機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合であっても、CPUバス上を流れるデータのコピーによる不正なコピーを防止することができる。

【0069】

このように専用の記録再生AV機器と汎用計算機とで受信ユニットを互換性をなくして汎用計算機のCPUバス 240上を流れるデータをコピーすることによる不正なコピーを防ぐことができる。

10

【0070】

また、本実施形態の半導体装置は、IEEE 1394 I/F部 110b, 210bに認識部 130, 230が設けられたチップを用いたので、当該半導体装置を使用することで上記効果を得ることができる。

【0071】

なお、本実施形態では、D-VCR等の記録機器と、記録再生AV本体やパソコン等の再生機器と間でデータ伝送する場合について説明したが、本発明はこのような場合に限られるものではなく、例えばネットワークや衛星通信を介してデータが伝送されてくる場合にも適用できる。例えば衛星からMPEG2圧縮され暗号化されたデータを受信する場合には送信機器 101, 201に対応するものとしてセットボックス(STB)が設けられることとなるが、セットボックス～受信機器 102, 202間のIEEE 1394によるデータ伝送は、本実施形態の場合と同様に考えることができる。

20

【0072】

また、本発明は、例えばネットワークの接続先が送信機器 101, 201に対応し、再生画像等使用者側には受信機器 102, 202に対応する記録再生AV本体やパソコン等の再生機器のみがあるような場合にも適用できる。

(発明の第2の実施の形態)

上記実施形態で説明したように、専用デジタル記録再生AV機器本体とパーソナルコンピュータとで構成を変えたとしても、パソコンを用いる場合に不正コピー者によって、送信チップユニット 204と受信チップユニット 206のチップセットを送信チップユニット 104と受信チップユニット 106のチップセットに交換されてしまう場合も考えられる。

30

【0073】

本実施形態は、このような場合に対応するものである。

図3は本発明の第2の実施の形態に係るデジタル記録再生システムに使用されるチップ形状の例を示す図である。

【0074】

なお、同図に示すチップ形状を除き本実施形態のデジタル記録再生システムは、第1の実施形態の場合と同様に構成されている。

40

図3(a)は、専用デジタル記録再生AV機器用の送信チップユニット 104, I/F部 110a又は受信チップユニット 106, I/F部 110bの構成例を示している。一方、図3(b)は、パーソナルコンピュータを使用するシステム用の送信チップユニット 204, I/F部 210a又は受信チップユニット 206, I/F部 210bの構成例を示している。

【0075】

このように、専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップの形状として、例えば足の数やボディ部の大きさや形などの形状を変えることで、チップの交換を防止できる。

【0076】

50

上述したように、本発明の実施の形態に係る不正コピーを防止する方法、半導体装置及びデジタル記録再生システムは、専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップの形状として、例えば足の数やボディ部の大きさや形などの形状を変えるようにしたので、半導体装置であるチップの交換を防止でき、第1の実施形態で奏する効果をより一層確実なものとする事ができる。

(発明の第3の実施の形態)

第2の実施形態では、チップ形状を変更することでチップの交換を防止したが、本実施形態は受信機器において、VTR等の専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップの内部処理のコードを変えることにより、受信ユニット(チップ)の交換を実質的に不可能とするものである。

10

【0077】

具体的には、例えばアスキーコード等のチップ内の制御コマンドの割り当てを、AV機器等用とパソコン等用とで異なったものとする。

このように、チップの計上による非互換性だけでなく、内部処理コマンドの違いにより非互換性を担保することができる。

【0078】

したがって、制御コマンドの割り当てが異なっているために、もし交換して使用したとすると、外部からの入力に対してチップ内の処理が異なり、正常な動作をしなくなる。そのため、たとえチップを交換できたとしても利用することは不可能である。

【0079】

上述したように、本発明の実施の形態に係る不正コピーを防止する方法、半導体装置及びデジタル記録再生システムは、専用デジタル記録再生AV機器とパーソナルコンピュータとで使用されるチップの内部処理のコードを変えるようにしたので、半導体装置であるチップの交換を確実に防止でき、第1の実施形態で奏する効果をより一層確実なものとする事ができる。

20

【0080】

また、本実施形態において、例えばチップにCPUが入っているような場合は、言語をZ80とC言語というように異なる言語を用いることにより、上記と同様の効果を持たせることもできる。

(発明の第4の実施の形態)

第2の実施形態では、チップ形状を変更し、第3の実施形態ではチップ内コードを変更することでチップの交換を防止したが、本実施形態は受信機器において、VTR等の専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップのピンにAV機器等かパソコン等かを識別するピンを設けることで受信ユニット(チップ)の交換を実質的に不可能とするものである。

30

【0081】

具体的には、本実施例のチップは、LSIピンの一つが機器認識用のピンとなっており、このピンから入力される信号により自LSIがAV機器等かパソコン等かの正しい機器に接続されたか否かを自己判定し、正しい機器に接続されていないときには動作しないように構成されている。

40

【0082】

例えば受信機器がパーソナルコンピュータである場合には、上記機器認識用のピンの接続先をダミーとし、ピンに対しては信号入力無しとする。一方、受信機器が専用デジタル記録再生AV機器本体である場合には、一定の信号を入力するようにする。

【0083】

したがって、上記一定の信号が入力されるか否かで、チップは自己の対応すべき機器に接続されたかを判定できる。

なお、機器認識用のピンへの入力は、AV機器等かパソコン等かで上記場合と逆にしてもよいし、また例えばHレベル、Lレベル信号で区別するようにする等、種々の形態が考えられる。

50

なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【 0 0 8 4 】

【 発明の効果 】

以上詳記したように本発明によれば、A V 機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっても、C P U バス上を流れるデータのコピーによる不正なコピーを防止することが可能な再生装置を提供することができる。

【 図面の簡単な説明 】

【 図 1 】 本発明の第 1 の実施の形態に係るデジタル記録再生システムの一例を示す構成図。 10

【 図 2 】 本発明の第 1 の実施の形態に係るデジタル記録再生システムの他の例を示す構成図。

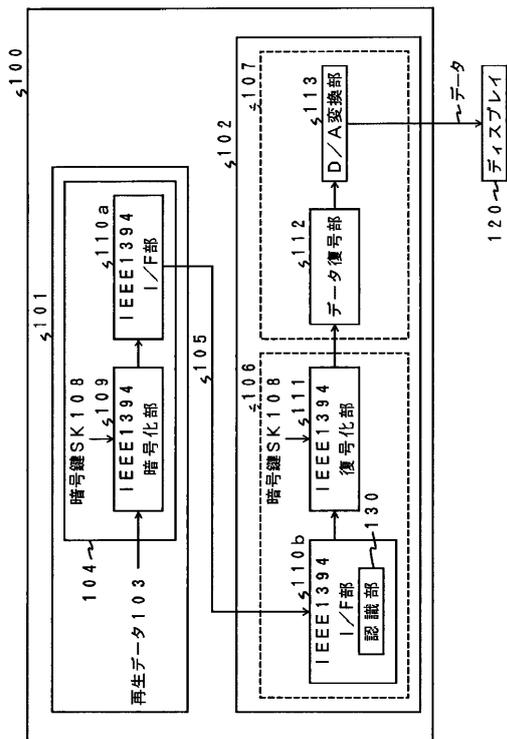
【 図 3 】 本発明の第 2 の実施の形態に係るデジタル記録再生システムに使用されるチップ形状の例を示す図。

【 符号の説明 】

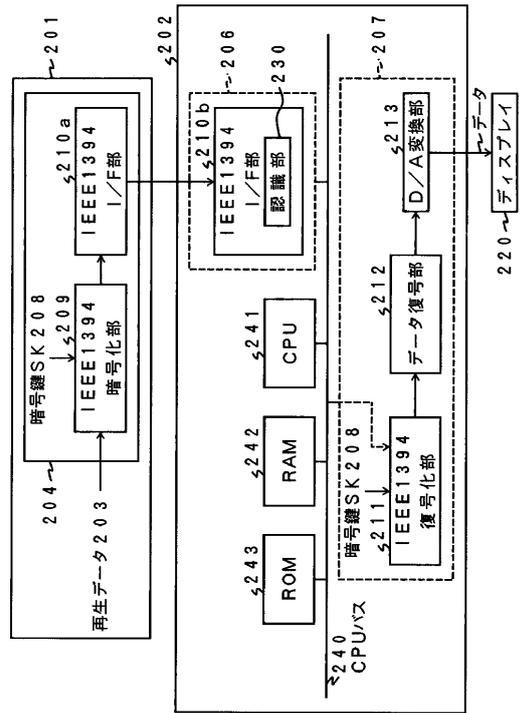
1 0 1 ... 送信機器	
1 0 2 ... 受信機器 (専用デジタル記録再生AV機器本体)	
1 0 3 ... M P E G 2 画像データ	
1 0 4 ... 送信チップユニット	20
1 0 5 ... I E E E 1 3 9 4 ケーブル	
1 0 6 ... 受信チップユニット	
1 0 7 ... 処理部	
1 0 8 ... 暗号鍵 S k	
1 0 9 ... I E E E 1 3 9 4 暗号化部	
1 1 0 a ... I E E E 1 3 9 4 I / F 部	
1 1 0 b ... I E E E 1 3 9 4 I / F 部	
1 1 1 ... I E E E 1 3 9 4 復号化部	
1 1 2 ... データ復号部	
1 1 3 ... D / A 変換部	30
1 2 0 ... ディスプレイ	
1 3 0 ... 認識部	
2 0 1 ... 送信機器	
2 0 2 ... 受信機器 (専用デジタル記録再生AV機器本体)	
2 0 3 ... M P E G 2 画像データ	
2 0 4 ... 送信チップユニット	
2 0 5 ... I E E E 1 3 9 4 ケーブル	
2 0 6 ... 受信チップユニット	
2 0 7 ... 処理部	
2 0 8 ... 暗号鍵 S k	40
2 0 9 ... I E E E 1 3 9 4 暗号化部	
2 1 0 a ... I E E E 1 3 9 4 I / F 部	
2 1 0 b ... I E E E 1 3 9 4 I / F 部	
2 1 1 ... I E E E 1 3 9 4 復号化部	
2 1 2 ... データ復号部	
2 1 3 ... D / A 変換部	
2 2 0 ... ディスプレイ	
2 3 0 ... 認識部	
2 4 0 ... C P U バス	
2 4 1 ... C P U	50

2 4 2 ... R A M
2 4 3 ... R O M

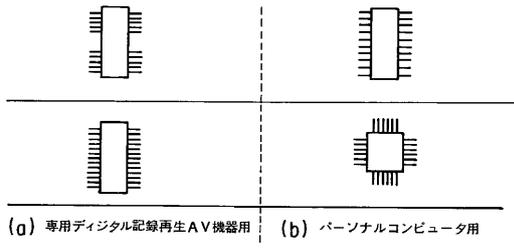
【 図 1 】



【 図 2 】



【 図 3 】



フロントページの続き

- (74)代理人 100070437
弁理士 河井 将次
- (72)発明者 加藤 岳久
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内
- (72)発明者 遠藤 直樹
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内
- (72)発明者 下田 乾二
神奈川県横浜市磯子区新杉田町8番地 株式会社東芝横浜事業所内

審査官 前田 祐希

- (56)参考文献 特開平09-102861(JP,A)
国際公開第97/014249(WO,A1)
特開平07-200414(JP,A)
特開平07-045782(JP,A)
特開平09-017956(JP,A)
特開平06-295200(JP,A)
特開平07-031737(JP,A)
特開平08-305635(JP,A)
特開平09-034797(JP,A)
特開2001-243117(JP,A)

(58)調査した分野(Int.Cl.⁷, DB名)

G11B 20/10

G06F 12/14