(19) **Bundesrepublik Deutschland**
**Deutsches Patent- und Markenamt**

(10) **DE 699 27 545 T2** 2006.07.13

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 951 019 B1**
(21) Deutsches Aktenzeichen: **699 27 545.8**
(96) Europäisches Aktenzeichen: **99 302 866.1**
(96) Europäischer Anmeldetag: **13.04.1999**
(97) Erstveröffentlichung durch das EPA: **20.10.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **05.10.2005**
(47) Veröffentlichungstag im Patentblatt: **13.07.2006**

(51) Int Cl.[8]: ***G11B 20/00*** (2006.01)
***G11B 20/12*** (2006.01)
***G11B 27/10*** (2006.01)

(30) Unionspriorität:
**10238698 14.04.1998 JP**

(84) Benannte Vertragsstaaten:
**DE, FR, GB**

(73) Patentinhaber:
**Hitachi, Ltd., Tokio/Tokyo, JP**

(74) Vertreter:
**Patent- und Rechtsanwälte Bardehle, Pagenberg, Dost, Altenburg, Geissler, 81679 München**

(72) Erfinder:
**Kawamae, Osamu, Yokohama-shi, JP; Takeuchi, Toshifumi, Tokyo, JP; Kimura, Hiroyuki, Hiratsuka-shi, JP; Arai, Takao, Yokohama-shi, JP; Yoshiura, Hiroshi, Tokyo, JP**

(54) Bezeichnung: **Verfahren zur Authentifikation und Datenverarbeitungsvorrichtung**

## Beschreibung

**[0001]** Die vorliegende Erfindung bezieht sich auf eine Vorrichtung zum Wiedergeben von Videodaten und Audiodaten und insbesondere auf eine Vorrichtung zum Widergeben von Daten und die Vorrichtung zum Aufzeichnen von Daten, welche angeordnet sind, um Daten wiederzugeben und/oder aufzuzeichnen von/auf ein Aufzeichnungsmedium, basierend auf Kopierverwaltungsinformation.

**[0002]** Eine DVD-ROM weist ein etwa siebenmal so großes Volumen auf wie eine CD-ROM. Die DVD-ROM kann Programmcodes für PCs wie auch Filmsoftware enthalten, erzeugt durch Komprimierung von Videodaten und Audiodaten. Die DVD schließt auch ein eine DVD-RAM, eine DVD-R und eine DVD-RW als ihr Aufzeichnungsmedium. Diese Aufzeichnungsmedien können eine große Menge an Daten aufzeichnen, was die Möglichkeit von illegalem Kopieren von Software, wie etwa einem Film, mit sich bringt. Diese Art von illegaler Kopie soll verhindert werden. Somit wird eine Technik zur Verhinderung einer illegalen Kopie wichtig. Diese Technik wird in dem Magazin „Nikkei Electronics" beschrieben, herausgegeben am 18. August 1997, Seiten 110 bis 119, veröffentlicht von Nikkei BP Publishing.

**[0003]** Zum Beispiel ist der Film, welcher auf einer DVD-Video-Disk aufgezeichnet ist, typischerweise gemäß dem CSS (content scrambling system) kodiert. Folglich können die kopierten Daten nicht wiedergegeben werden, wenn sie nicht entschlüsselt werden.

**[0004]** In der Tat beschreibt das oben erwähnte Magazin die Wiedergabe eines Mediums, wo Daten voraufgenommen sind, wie etwa eine DVD-Video-Disk. Jedoch beschreibt es nicht die Wiedergabe eines Aufzeichnungsmediums, wo ein Benutzer beliebig Daten aufzeichnen kann.

**[0005]** Im Fall einer Wiedergabe von Daten, die verschlüsselt sind gemäß einem entsprechenden System auf jedem aufzeichnungsfähigen Medium, ist es nötig, den Schritt des Unterscheidens des entsprechenden Aufzeichnungsmediums zu einem ankommenden Wiedergabesignal vorzunehmen, bevor das Widergabesignal entschlüsselt wird. Des Weiteren ist es auch nötig, konkret einen Typ der Daten zu unterscheiden, falls die Datenkopie erlaubt oder verboten ist, bevor die Steuerung ausgeführt wird.

**[0006]** EPO-A-0 977 436, welche Stand der Technik nach Artikel 54 (3) EPÜ ist, offenbart eine Übertragungseinheit und eine Empfängereinheit für digitale ∃-AV-Daten. Die Übertragungseinheit weist vielfache Authentifikationsregeln darin gespeichert auf, und sie wählt eine dieser Regeln für die Authentifikation der zu übertragenden Daten aus. Die Empfängereinheit speichert die gleichen Authentifikationsregeln und wählt die geeignete Regel für eine Authentifikation der empfangenen Daten aus.

**[0007]** Gemäß einem ersten Aspekt der Erfindung ist dort ein Authentifikationsverfahren zur Durchführung einer Authentifikation zwischen Geräten vorgesehen, wenn ein Gerät Eingabedaten erhält, eine nötige Verarbeitung zum Aufzeichnen oder zur Wiedergabe durchführt und verarbeitete Eingabedaten an ein externes Gerät ausgibt, wobei das Authentifikationsverfahren die Schritte aufweist des:
Auswählens, aus einer Vielzahl von Verschlüsselungsverfahren, eines Verschlüsselungsverfahrens zum Verschlüsseln von Daten, die aus den Eingabedaten abgeleitet sind, welche abgeleiteten Daten verarbeitet werden sollen, und
Auswählens, aus einer Vielzahl von Authentifikationsverfahren, eines Authentifikationsverfahrens, welches der Art der Verschlüsselung der abgeleiteten Daten entspricht, wobei das externe Gerät authentifiziert wird unter Verwendung des ausgewählten Authentifikationsverfahrens, und Ausgebens der verschlüsselten Daten.

**[0008]** Gemäß einem zweiten Aspekt der Erfindung ist vorgesehen eine Datenverarbeitungsvorrichtung, welche eine Mehrzahl von Datenverarbeitungsmitteln zum Übertragen von Daten über einen Datenbus aufweist, wobei jedes der Vielzahl von Datenverarbeitungsmitteln eine Vielzahl von Verschlüsselungsmitteln **62** einschließt und ein Verschlüsselungsmittel daraus auswählt, entsprechend einem Typ der Daten, die übertragen werden sollen, um diese Daten zu verschlüsseln, wobei die Mehrzahl von Datenverarbeitungsmitteln jedes eine Mehrzahl von Authentifikationsmitteln einschließt und ein Authentifikationsmittel entsprechend den ausgewählten Verschlüsselungsmitteln auswählt, um ein externes Gerät vor einem Übertragen der Daten durch den Datenbus zu authentifizieren.

**[0009]** In den Zeichnungen ist

**[0010]** Fig. 1 ein Blockdiagramm, welches eine Vorrichtung zum Wiedergeben von Daten zeigt, welche Kopiersteuerinformationen enthalten, gemäß einer Ausführungsform der vorliegenden Erfindung;

**[0011]** Fig. 2 ein Blockdiagramm, welches eine Ausführungsform zeigt, in welcher die Vorrichtung zum Wiedergeben von Daten gemäß der Erfindung bei einem DVD-Antrieb angewandt ist;

**[0012]** Fig. 3 eine Ansicht, welche eine Zusammensetzung von DVD-Sektordaten zeigt als ein Beispiel von Daten, welche Codes enthalten, auf welchen ein Typ eines Aufzeichnungsmediums und eine Verschlüsselungsstruktur von Daten aufgezeichnet sind;

**[0013]** Fig. 4 eine Ansicht, welche eine Zusammensetzung von Identifikations (ID)-Daten einer DVD zeigt;

**[0014]** Fig. 5 ein Blockdiagramm, welches eine Vorrichtung zum Aufzeichnen von Daten zeigt, welche Kopiersteuerinformationen enthalten, gemäß einer Ausführungsform der vorliegenden Erfindung;

**[0015]** Fig. 6 ein Blockdiagramm, welches eine weitere Vorrichtung zum Wiedergeben von Daten zeigt, welche Kopiersteuerinformationen enthalten, gemäß einer Ausführungsform der vorliegenden Erfindung;

**[0016]** Fig. 7 ein Blockdiagramm, welches eine Anordnung zeigt, in welcher eine Vorrichtung zum Wiedergeben von Daten gemäß der Erfindung an einem DVD-Antrieb angewandt ist, so dass das Ausgabesignal mit einem aufzeichnungsfähigen Gerät, wie etwa einer Festplatte, verbunden ist;

**[0017]** Fig. 8 ein Blockdiagramm, welches eine Anordnung zeigt, in welcher eine Vorrichtung zum Ausgeben von Daten auf einen Monitor angewandt ist; und

**[0018]** Fig. 9 ein Blockdiagramm, welches ein System zeigt, das mit jeder Vorrichtung gemäß der vorliegenden Erfindung versehen ist, wie etwa ein Personal Computer.

**[0019]** Fig. 10 ist ein Blockdiagramm, welches eine Datenwiedergabevorrichtung zeigt zum Wiedergeben von Daten, welche Kopiersteuerinformationen enthalten, gemäß einer anderen Ausführungsform der Erfindung.

**[0020]** Im Folgenden wird die vorliegende Erfindung gemäß den Ausführungsformen beschrieben werden mit Bezugnahme auf die angefügten Zeichnungen.

**[0021]** Fig. 1 zeigt eine Vorrichtung zum Wiedergeben von Daten, welche Kopiersteuerinformationen enthalten, gemäß einer Ausführungsform der Erfindung. In dieser Ausführungsform wird ein beschreibbares und wiederzugebendes Medium, wie etwa eine DVD, beschrieben werden. Es ist selbstverständlich, dass dies nicht auf eine optische Disk beschränkt ist, sondern auf jegliche Art von Medium angewendet werden kann, welches Daten speichert.

**[0022]** In Fig. 1 bezeichnet ein Bezugszeichen **1** eine erste Datenwiedergabevorrichtung. Ein Bezugszeichen **2** bezeichnet eine erste Wiedergabeeinheit. Ein Bezugszeichen **3** bezeichnet einen ersten Schalter. Ein Bezugszeichen **4** bezeichnet eine erste Authentifikationseinheit a. Ein Bezugszeichen **5** bezeichnet eine zweite Authentifikationseinheit a. Ein Bezugszeichen **6** bezeichnet eine dritte Authentifikationseinheit a. Ein Bezugszeichen **7** bezeichnet eine zweite Datenwiedergabevorrichtung. Ein Bezugszeichen **8** bezeichnet eine erste Authentifikationseinheit b. Ein Bezugszeichen **9** bezeichnet eine zweite Authentifikationseinheit b. Ein Bezugszeichen **10** bezeichnet eine dritte Authentifikationseinheit b. Ein Bezugszeichen **11** bezeichnet eine erste Entschlüsselungseinheit. Ein Bezugszeichen **12** bezeichnet eine zweite Entschlüsselungseinheit. Ein Bezugszeichen **13** bezeichnet einen zweiten Schalter. Ein Bezugszeichen **14** bezeichnet eine WM-Detektionseinheit. Ein Bezugszeichen **15** bezeichnet eine MPEG-Wiedergabeeinheit. Ein Bezugszeichen **16** bezeichnet eine Dateneingabe. Ein Bezugszeichen **17** bezeichnet eine Datenausgabe. Ein Bezugszeichen **18** bezeichnet einen ersten Datenbus. Ein Bezugszeichen **19** bezeichnet einen ersten Authentifikationsbus. Ein Bezugszeichen **20** bezeichnet einen zweiten Datenbus. Ein Bezugszeichen **21** bezeichnet einen zweiten Authentifikationsbus. Ein Bezugszeichen **22** bezeichnet einen dritten Datenbus. Ein Bezugszeichen **23** bezeichnet einen dritten Authentifikationsbus. Ein Bezugszeichen **124** bezeichnet eine CSS-Authentifikationseinheit a. Ein Bezugszeichen **125** bezeichnet einen CSS-Datenbus. Ein Bezugszeichen **126** bezeichnet einen CSS-Authentifikationsbus. Ein Bezugszeichen **127** bezeichnet eine CSS-Authentifikationseinheit b. Ein Bezugszeichen **128** bezeichnet eine CSS-Entschlüsselungseinheit. Ein Bezugszeichen **129** bezeichnet einen ersten Authentifikationsblock. Ein Bezugszeichen **130** bezeichnet einen zweiten Authentifikationsblock.

**[0023]** Der Betrieb des vorliegenden Systems wird mit Bezugname auf die Fig. 1 und Fig. 2 beschrieben werden.

**[0024]** Die Dateneingabe **16**, gelesen von einer Disk mittels der ersten Datenwiedergabevorrichtung, wie etwa einem DVD-Antrieb, wird entschlüsselt gemäß dem aufgezeichneten Format durch die erste Wiedergabeeinheit **2**. In diesem Entschlüsselungsvorgang arbeitet die erste Wiedergabeeinheit **2**, um einen Typ der Daten zu lesen, welche einen Code einschließen zum Bezeichnen eines Typs des Aufzeichnungsmediums, enthalten in den Daten (z.B. ein Code zum Anzeigen, ob das Aufzeichnungsmedium vorgesehen ist zur Wiedergabe oder beschreibbar), einen Code zum Anzeigen, ob die Datenstruktur verschlüsselt ist oder nicht, und einen Code zum Anzeigen, ob die Daten video- oder audio- oder kopierbeschränkt sind (z.B. ein Code zum Anzeigen einer Kopieerlaubnis, einer Ein-Generationen-Kopieerlaubnis oder eines Kopieverbots). Bei einer optischen Disk kann des Weiteren der Typ des Aufzeichnungsmediums unterschieden werden auf einem Spursignal der Disk. Basierend auf den Stücken der Informationen, die durch die erste Wiedergabeeinheit **2** gelesen werden, wird der erste Schalter **3** so geschaltet, um die entsprechende Authentifikationseinheit zu den gelesenen Daten auszuwählen. Die Authentifikation wird

vorgenommen, um eine Person zu verifizieren, mit welcher die Daten in Zusammenhang sind, und eine Schlüsselinformation wird gesendet/empfangen zum Zweck einer Entschlüsselung. Die empfangen Daten sind durch den Schlüssel verschlüsselt worden, und die Daten werden unter Verwendung des Schlüssels entschlüsselt, um so die Daten zu schützen.

**[0025]** Die erste Authentifikationseinheit a arbeitet, um ein wiedergabegeeignetes Aufzeichnungsmedium zu authentifizieren.

**[0026]** Die zweite Authentifikationseinheit a arbeitet, um ein beschreibbares Aufzeichnungsmedium mit seiner Kopie zu authentifizieren, begrenzt durch Kopierbegrenzungsinformationen. Die dritte Authentifikationseinheit a arbeitet, um ein beschreibbares Aufzeichnungsmedium mit keiner Kopierbeschränkung durch Kopierbeschränkungsinformation zu authentifizieren. Die CSS-Authentifikationseinheit a **124** ist ein Authentifikationsmittel für den DVD-Antrieb zum bestehenden CSS (Content Scrambling System – Inhaltsverschlüsselungssystem). In dieser Ausführungsform ist die CSS-Authentifikationseinheit a **124** beschrieben als eine unabhängige Einheit. Sie kann mit neuen Authentifikationseinheiten kombiniert sein, d.h. der ersten, der zweiten und der dritten Authentifikationseinheit a als ein erster Authentifikationsblock **129**.

**[0027]** Von der Datenwiedergabeeinheit **2** wird angenommen, dass sie ein MPEG-Board ist zum Dekodieren der MPEG-Daten. Die erste Authentifikationseinheit b ist in Entsprechung zu der ersten Authentifikationseinheit a positioniert. Die Authentifikation wird vorgenommen durch den ersten Authentifikationsbus **19**. Falls die Daten nicht korrekt sind, werden die Entschlüsselungsinformationen nicht weitergeleitet, wie es auch den Daten verweigert wird, von dem ersten Datenbus **18** ausgegeben zu werden. In gleicher Weise weisen die ersten und die dritten Authentifikationseinheiten b die gleiche Entsprechung mit den zweiten und dritten Authentifikationseinheiten a auf. Falls die Daten nicht richtig sind, wird keine Authentifikation vorgenommen, und die Datenausgabe wird gestoppt. Hier sind, zur Vereinfachung der Beschreibung, die Authentifikationsbusse und die Datenbusse entsprechend den drei Authentifikationseinheiten. Eigentlich kann die Kombination von einem Authentifikationsbus und einem Datenbus umgeschaltet werden zu jeder Authentifikationseinheit. Die CSS-Authentifikationseinheit b **127** arbeitet, um das MPEG-Board entsprechend zu dem bestehenden CSS zu authentifizieren. In dieser Ausführungsform wird die CSS-Authentifikationseinheit b **127** beschrieben als eine unabhängige Einheit. Sie kann mit den neuen Authentifikationseinheiten kombiniert werden, d.h. der ersten, der zweiten und der dritten Authentifikationseinheit b als ein Authentifikationsblock b **130**.

**[0028]** Die von der ersten Wiedergabevorrichtung **1** zu der zweiten Wiedergabevorrichtung **7** über den ersten Datenbus übertragenen Daten werden zum Zweck des Verhinderns einer Kopie der Daten in der Übertragung verschlüsselt. Die Daten auf dem wiedergabebestimmten Aufzeichnungsmedium sind auf unterschiedliche Art und Weise zu den Daten des Aufzeichnungsmediums verschlüsselt mit einer Kopierbeschränkung, welche durch eine Kopierbeschränkungsinformation vorgegeben ist. Die Daten des beschreibbaren Aufzeichnungsmediums mit keiner Kopierbeschränkung, vorgegeben durch die Kopierbeschränkungsinformationen, sind nicht verschlüsselt, da es nicht erforderlich ist, eine Kopie der Daten zu verhindern. Unter diesen Umständen arbeitet die erste Wiedergabevorrichtung, um den Typ des Aufzeichnungsmediums und die verschlüsselten Daten durch die Wirkung der Authentifikationseinheit zu übertragen. Dabei ist es nicht erforderlich, dass die Daten auf der Disk mit keiner Kopierbeschränkung zum Vermeiden der Kopie der Daten verschlüsselt sind. Falls jedoch keine Authentifikation nur für die Daten vorgenommen wird, ist es schwierig, die Disk mit keiner Kopierbeschränkung und die Disk, welche illegal durch die Kopie der ursprünglich beschränkten Disk kopiert ist, unterscheidend festzustellen. Daher wird die Authentifikation vorgenommen bei einer Disk mit keiner Kopierbeschränkung.

**[0029]** Falls die Authentifkation vorgenommen ist, werden die verschlüsselten Daten zu der zweiten Datenwiedergabevorrichtung **7** übertragen. Der Datenbus, durch welchen die Daten übertragen werden, wird ausgewählt gemäß dem Typ des Aufzeichnungsmediums und der Verschlüsselungsstruktur der von der Authentifikationseinheit übertragenen Daten. Die erste Entschlüsselungseinheit **11** oder die zweite Entschlüsselungseinheit **12** gemäß dem Typ des Mediums und der Verschlüsselungsstruktur werden betrieben, um die Daten zu entschlüsseln. Die entschlüsselten Daten werden zu der MPEG-Widergabeeinheit **15** durch den zweiten Schalter **13** gesendet. Die WM (Water Mark – Wasserzeichen)-Detektionseinheit **14** wird verwendet zum Detektieren zusätzlicher Informationen, eingelagert in die Daten, welche von der MPEG-Wiedergabeeinheit **15** dekodiert sind. In dieser Ausführungsform wird das Wasserzeichen als die zusätzliche Information detektiert. Falls die Kopiersteuerinformationen detektiert werden, wird die Datenausgabe gemäß der Kopiersteuerinformation gesteuert. In dieser Ausführungsform wird die MPEG-Wiedergabeeinheit **75** so gesteuert, um die Ausgabe der Daten zu steuern. Das Steuerungsverfahren ist nicht darauf beschränkt. Zum Beispiel können die Ausgabedaten gesteuert werden, dass sie gestoppt werden oder auf den Bus ausgegeben werden.

**[0030]** Hier sind die erste Wiedergabeeinheit **2**, der erste Schalter **3**, die erste Authentifikationseinheit a

**4**, die zweite Authentifikationseinheit a **5** und die dritte Authentifikationseinheit a **6** auf der gleichen LSI eingebunden, zum Zweck, es schwierig zu machen, die Daten auf dem Übertragungsweg aufzunehmen. Die erste Authentifikationseinheit b **8**, die zweite Authentifikationseinheit b **9**, die dritte Authentifikationseinheit b **10**, die erste Verschlüsselungseinheit **11**, die zweite Entschlüsselungseinheit **12**, der zweite Schalter **13**, die WM-Detektionseinheit **14** und die MPEG-Wiedergabeeinheit **15** sind auf der gleichen LSI eingebunden, zum Zweck, es schwierig zu machen, die Daten auf dem Übertragungsweg aufzunehmen.

**[0031]** Fig. 2 zeigt die Anordnung, in welcher die Datenwiedergabevorrichtung gemäß der vorliegenden Erfindung in dem DVD-Antrieb angewandt wird. Die vorliegende Ausführungsform befasst sich mit einem beschreibbaren und wiedergebbaren Aufzeichnungsmedium, wie etwa einer DVD. Es ist selbstverständlich, dass das Aufzeichnungsmedium nicht auf eine optische Disk beschränkt ist, sondern auf irgendeine Art von beschreibbarem und wiedergebbarem Aufzeichnungsmedium angewandt werden kann.

**[0032]** In Fig. 2 bezeichnet ein Bezugszeichen **24** eine DVD-Disk. Ein Bezugszeichen **25** bezeichnet einen DVD-Antrieb. Ein Bezugszeichen **26** bezeichnet eine Abtasteinheit. Ein Bezugszeichen **27** bezeichnet einen Vorverstärker. Ein Bezugszeichen **28** bezeichnet eine erste Systemsteuereinheit. Ein Bezugszeichen **29** bezeichnet ein MPEG-Wiedergabe-Board. Ein Bezugszeichen **30** bezeichnet eine zweite Systemsteuereinheit. Ein Bezugszeichen **31** bezeichnet einen Konverter. Ein Bezugszeichen **32** bezeichnet einen Monitor.

**[0033]** Ein von der DVD-Disk **24** durch die Abtasteinheit **26** gelesenes Signal wird in die erste Datenwiedergabevorrichtung **1** zugeführt. Die erste Datenwiedergabevorrichtung **1** bestimmt den Betriebszustand unter der Steuerung der ersten Systemsteuereinheit **28**. Der Hauptbetrieb des DVD-Antriebs **25** entspricht dem Vorgang bis zu diesem Punkt. Das von der ersten Datenwiedergabevorrichtung **1** wiedergegebene Signal wird zu der zweiten Datenwiedergabevorrichtung **7** übertragen. Die zweite Datenwiedergabevorrichtung **7** wird betrieben, um den Betriebszustand unter Steuerung der zweiten Systemsteuereinheit **30** zu bestimmen. Die Daten, welche von der zweiten Datenwiedergabevorrichtung **7** wiedergegeben werden, werden durch den Konverter **31** konvertiert und dann in den Monitor **32** ausgegeben, auf welchem die Daten angezeigt werden. Der Vorgang bis zu diesem Punkt entspricht dem Hauptbetrieb des MPEG-Wiedergabe-Boards **29**.

**[0034]** Fig. 3 zeigt eine Zusammensetzung von Sektordaten der DVD als ein Beispiel von Daten, welche Codes enthalten, die einen Typ des Aufzeichnungsmediums und eine Verschlüsselungsstruktur der darauf aufgezeichneten Daten aufweisen. In der DVD werden die Identifikationsdaten, einfach ID genannt, und die Copyright-Verwaltungsinformationen, genannt CPR_MAI, vor den Hauptdaten von 2048 Bytes geschrieben.

**[0035]** Die Copyright-Verwaltungsinformation (CPR_MAI) deckt sowohl die Copyright-Verwaltungsinformationen als auch die Bereichsverwaltungsinformationen ab. Der Einlesebereich beschreibt, ob die Daten eine bestimmte Datenstruktur (entsprechend zu der Verschlüsselungsstruktur) des Copyright-Schutzsystems enthalten oder nicht und ob die Daten auf einem bestimmten Bereich wiedergegeben werden können oder nicht. Der Datenbereich beschreibt, ob der Sektor ein Material mit Copyright enthält oder nicht, ob die Daten eine bestimmte Datenstruktur des Copyright-Schutzsystems aufweisen oder nicht und ob die Daten kopierbeschränkt sind oder nicht (Kopiererlaubnis, Ein-Generationen-Kopiererlaubnis und Kopierverbot).

**[0036]** Fig. 4 zeigt die Zusammensetzung der ID-Daten der DVD.

**[0037]** Die ID enthält für die Wiedergabe bestimmte Daten, bezeichnet als Datentyp, oder einen Hilfscode für einmal speicherbare Daten und mehrfach speicherbare Daten in den ersten vier Bytes der Sektorinformation.

**[0038]** Ein Sektorformattyp beschrieb einen CLV-Formattyp, spezifiziert durch die für die Wiedergabe bestimmte Disk, und die einmal beschreibbare Disk oder einen Zonenformattyp, spezifiziert für eine wiederbeschreibbare Disk. Ein Bereichstyp zeichnet einen Datenbereich, einen Einlesebereich, einen Auslesebereich oder einen Mittenbereich für eine für eine Wiedergabe bestimmte Disk auf. Der Datentyp wird übrig gelassen für die Daten, welche für die Wiedergabe bestimmt sind, oder die einmal gespeicherten Daten (Verknüpfungsdaten) und die wieder speicherbaren Daten.

**[0039]** Fig. 5 zeigt eine Aufzeichnungsvorrichtung zum Aufzeichnen von Daten, welche Kopiersteuerinformationen enthalten, gemäß einer Ausführungsform der vorliegenden Erfindung. Die vorliegende Erfindung befasst sich mit einem beschreibbaren und wiedergebbaren Aufzeichnungsmedium, wie etwa einer DVD. Es versteht sich von selbst, dass das Aufzeichnungsmedium nicht auf eine optische Disk beschränkt ist, sondern auf irgendeine Art von beschreibbarem und wiedergebbarem Medium angewandt werden kann.

**[0040]** In Fig. 5 bezeichnet ein Bezugszeichen **51** eine zweite Datenaufzeichnungsvorrichtung. Ein Be-

zugszeichen **52** bezeichnet eine erste Aufzeichnungseinheit. Ein Bezugszeichen **53** bezeichnet einen vierten Schalter. Ein Bezugszeichen **55** bezeichnet eine zweite Authentifikationseinheit d. Ein Bezugszeichen **56** bezeichnet eine dritte Authentifikationseinheit d. Ein Bezugszeichen **57** bezeichnet eine erste Datenaufzeichnungsvorrichtung. Ein Bezugszeichen **59** bezeichnet eine zweite Authentifikationseinheit c. Ein Bezugszeichen **60** bezeichnet eine dritte Authentifikationseinheit c. Ein Bezugszeichen **62** bezeichnet eine zweite Entschlüsselungseinheit. Ein Bezugszeichen **63** bezeichnet einen dritten Schalter. Ein Bezugszeichen **64** bezeichnet eine WM-Detektionseinheit. Ein Bezugszeichen **65** bezeichnet eine MPEG-Kodiereinheit. Ein Bezugszeichen **66** bezeichnet eine Datenausgabe. Ein Bezugszeichen **67** bezeichnet eine Dateneingabe. Das Bezugszeichen **20** bezeichnet einen zweiten Datenbus. Das Bezugszeichen **21** bezeichnet einen zweiten Authentifikationsbus. Das Bezugszeichen **22** bezeichnet einen dritten Datenbus. Das Bezugszeichen **23** bezeichnet einen dritten Authentifikationsbus.

**[0041]** Die Dateneingabe **67**, wie etwa Videodaten, gelesen von der Disk durch die erste Datenwiedergabevorrichtung, wie etwa einen DVD-Antrieb, und ausgegeben an den Monitor, wird kodiert gemäß dem Format zum Konvertieren und Aufzeichnen der digitalen Daten durch die erste Aufzeichnungseinheit (**52**). Zu dieser Zeit wird der Typ der Daten, wie etwa ein Code für eine Bezeichnung des Typs des Aufzeichnungsmediums (z.B. ein Code zum Bezeichnen, ob das Medium für eine Wiedergabe bestimmt oder beschreibbar ist) gemäß dem Format geschrieben. Als ein anderer Typ von Daten, z.B. der Code zum Bezeichnen, ob die Datenstruktur durch eine Kopiersteuerung verschlüsselt ist, und der Code zum Bezeichnen einer Kopierbeschränkung (z.B. ein Code zum Bezeichnen einer Kopiererlaubnis, einer Ein-Generationen-Kopiererlaubnis oder eines Kopierverbots), wird genauso geschrieben. Als nächstes wird, falls die Daten eine Kopiersteuerung benötigen, die Verschlüsselung basierend auf dem Aufzeichnungsmedium und dem Status der Kopiersteuerung durchgeführt. Dabei wird der dritte Schalter auf die Kopiersteuerungsinformationen so geschaltet, um die Authentifikationseinheit auszuwählen.

**[0042]** Die Wasserzeichendetektionseinheit **64** arbeitet, um die Kopiersteuerinformationen zu detektieren, d.h. zusätzliche Informationen, die zu den Daten hinzugefügt sind, die in die MPEG-Kodiereinheit **65** eingegeben sind. Die Steuerung wird durchgeführt gemäß den Kopiersteuerungsinformationen. Falls z.B. die detektieren Informationen ein Kopierverbot anzeigen, wird die Ausgabe der Aufzeichnungsdaten gestoppt. Falls sie keine Kopierbeschränkung anzeigen, wird der Kodiervorgang ohne Verschlüsselung durchgeführt. In dieser Ausführungsform wird die MPEG-Kodiereinheit **65** bedient, um die Ausgabe der Daten zu steuern. Das Steuerungsverfahren ist nicht darauf beschränkt. Das Verfahren kann sein der Stopp der Ausgabedaten, das Abbrechen der Daten auf dem Bus, usw.

**[0043]** Die zweite Authentifikationseinheit c arbeitet, um das beschreibbare Aufzeichnungsmedium zu authentifizieren, dessen Kopie durch die Kopiebeschränkungsinformation beschränkt ist. Die dritte Authentifikationseinheit c arbeitet, um das beschreibbare Aufzeichnungsmedium zu authentifizieren, dessen Kopie nicht durch die Kopierbeschränkungsinformation beschränkt ist.

**[0044]** Des Weiteren kann, obwohl in dieser Ausführungsform nicht dargestellt, wie die Wiedergabevorrichtung, die Authentifikationseinheit, welche dem bestehenden CSS entspricht, in dieser Ausführungsform enthalten sein. Diese CSS-Authentifikationseinheit kann mit diesen Authentifikationseinheiten als ein Authentifikationsblock kombiniert sein.

**[0045]** Die erste Datenaufzeichnungsvorrichtung ist ein MPEG-Board zum Kodieren der MPEG-Daten.

**[0046]** Die zweite Authentifikationseinheit d weist eine entsprechende Relation mit der zweiten Authentifikationseinheit c auf. Die Authentifikation wird durchgeführt durch die Verwendung des zweiten Authentifikationsbusses **71**. Falls nicht die entsprechende Relation damit aufweisend, wird kein Entschlüsselungsverfahren weitergegeben, und die Ausgabe der Daten von dem zweiten Datenbus **70** wird gestoppt. Die dritte Authentifikationseinheit d weist die entsprechende Relation mit der dritten Authentifikationseinheit c auf. Falls sie nicht die entsprechende Relation damit aufweist, wird keine Authentifikation vorgenommen, und die Ausgabe der Daten wird gestoppt. Hier sind, zur Vereinfachung der Beschreibung, die Authentifikationsbusse für zwei Kombinationen von Authentifikationseinheiten und die Datenbusse zum Übertragen der Daten von den Authentifikationseinheiten als unabhängige Busse beschrieben. Eine Kombination eines Datenbusses und eines Authentifikationsbusses kann für zwei Authentifikationseinheiten umgeschaltet werden.

**[0047]** Die von der ersten Datenaufzeichnungsvorrichtung **51** zu der zweiten Datenaufzeichnungsvorrichtung **57** übertragenen Daten werden zum Zweck des Verhinderns der Kopie der Daten in der Übertragung verschlüsselt. Die Daten, deren Kopie nicht durch die Kopierbeschränkungsinformation beschränkt ist, werden nicht verschlüsselt, da sie keinen Kopierschutz benötigen.

**[0048]** Folglich arbeitet die erste Datenaufzeichnungsvorrichtung **1**, um die verschlüsselten Daten durch die Verwendung der Authentifikationseinheit zu übertragen. Der dritte Schalter **63** wird bedient, um

einen geeigneten der Busse auszuwählen, die die Verschlüsselungseinheit **2** zuzuführen, gemäß den Daten, und die Verschlüsselungseinheit nicht zuzuführen, so dass die richtige Verschlüsselung für die Daten durchgeführt werden kann.

**[0049]** Wenn die Authentifikation vorgenommen ist, werden die Daten als verschlüsselt übertragen. Die Authentifikationseinheit wird ausgeführt, um den Datenbus auszuwählen, dem es gestattet ist, die Daten gemäß dem Typ des Aufzeichnungsmediums und der Verschlüsselungsstruktur der Daten zu übertragen. Dann werden die Daten von der ersten Aufzeichnungseinheit **52** durch den vierten Schalter **53** versandt.

**[0050]** Hier sind die zweite Authentifikationseinheit c **59**, die dritte Authentifikationseinheit c **60**, die zweite Verschlüsselungseinheit **62**, der dritte Schalter **63**, die WM-Detektionseinheit **64** und die MPEG-Kodiereinheit **65** auf der gleichen LSI enthalten, zu dem Zweck, um es schwierig zu machen, die Daten auf dem Übertragungsweg aufzunehmen. Die erste Aufzeichnungseinheit **52**, der vierte Schalter **53**, die zweite Authentifikationseinheit d **55** und die dritte Authentifikationseinheit d **56** sind auf der gleichen LSI enthalten, zu dem Zweck, es schwierig zu machen, die Daten auf dem Übertragungsweg aufzunehmen.

**[0051]** Fig. 6 zeigt eine Vorrichtung zum Wiedergeben von Daten, welche die Kopiersteuerinformation enthalten, gemäß einer anderen Ausführungsform der vorliegenden Erfindung. Diese Ausführungsform verwendet selektiv eine Kombination eines Datenbusses und eines Authentifikationsbusses für alle Authentifikationseinheiten in der in Fig. 1 gezeigten Ausführungsform, obwohl die Ausführungsform in Fig. 1 die entsprechende Kombination eines Datenbusses und eines Authentifikationsbusses zu jeder der Authentifikationseinheiten enthält. In der folgenden Ausführungsform bezeichnen die gleichen Bezugszeichen wie die in Fig. 1 die gleichen Komponenten.

**[0052]** In Fig. 6 bezeichnet ein Bezugszeichen **70** einen vereinten Datenbus. Ein Bezugszeichen **71** bezeichnet einen vereinten Authentifikationsbus. Bezugszeichen **72** bezeichnet einen Schalter zum Umschalten der Authentifikationseinheiten, welche in dem ersten Authentifikationsblock enthalten sind. Ein Bezugszeichen **73** bezeichnet einen Schalter zum Umschalten der Authentifikationseinheiten, die in dem zweiten Authentifikationsblock enthalten sind. Diese Anordnung führt dazu, dass sie es möglich macht, einen Datenbus und einen Authentifikationsbus für alle Authentifikationseinheiten zu bedienen, dabei die Verbindungsleitungen zwischen den Vorrichtungen in der Anzahl zu verringern.

**[0053]** Fig. 7 zeigt die Anordnung, in welcher die Datenwiedergabevorrichtung gemäß der vorliegenden Erfindung angewandt wird bei dem DVD-Antrieb und das Ausgabesignal des DVD-Antriebs mit einem beschreibbaren Gerät, wie etwa einer Festplatte, verbunden ist. Die vorliegende Ausführungsform befasst sich mit dem beschreibbaren und wiedergebbaren Aufzeichnungsmedium, wie etwa einer Festplatte. Es versteht sich von selbst, dass das Aufzeichnungsmedium nicht auf das beschreibbare und wiedergebbare Aufzeichnungsmediumn, wie etwa eine Festplatte, beschränkt ist, sondern bei irgendeiner Art von Gerät verwendet werden kann, welches Daten durch den Datenbus sendet und empfängt.

**[0054]** In Fig. 7 bezeichnet ein Bezugszeichen **80** ein Festplattengerät. Ein Bezugzeichen **81** bezeichnet ein erstes Aufzeichnungsgerät. Ein Bezugszeichen **82** bezeichnet eine Systemsteuereinheit. Ein Bezugszeichen **83** bezeichnet eine Festplatte.

**[0055]** Das von der DVD-Disk **24** durch die Abtasteinheit **26** ausgelesene Signal wird in das erste Datenwiedergabegerät **81** durch den Vorverstärker **27** zugeführt. Das erste Datenwiedergabegerät **81** bestimmt den Betriebszustand unter Steuerung der ersten Systemsteuereinheit **28**. Der Vorgang entspricht bis zu diesem Punkt dem Hauptbetrieb des DVD-Antriebs **25**. Das von dem ersten Datenwiedergabegerät **1** wiedergegebene Signal wird in das erste Datenaufzeichnungsgerät **81** übertragen. Das erste Datenaufzeichnungsgerät **1** legt den Zustand des Aufzeichnungsbetriebs fest unter Steuerung der dritten Systemsteuereinheit **82**. Die Daten, welche von dem ersten Datenaufzeichnungsgerät **81** wiedergegeben werden, werden auf der Festplatte **83** aufgezeichnet. Der Vorgang bis dahin entspricht dem Hauptbetrieb des Festplattengeräts **80**.

**[0056]** Hier erfordert es das Gerät, welches Daten aufzeichnet, die Aufzeichnung gemäß der Kopiersteuerungsinformation zu steuern. Um sicherzustellen, dass das Gerät eine Funktion aufweist, die Aufzeichnung richtig zu steuern, hat das erste Datenwiedergabegerät **1** das zweite Datenaufzeichnungsgerät **81** zu authentifizieren. Die von dem ersten Datenwiedergabegerät **1** zu dem ersten Datenaufzeichnungsgerät **81** gegebenen Daten sind in einer Übertragung verschlüsselt, falls die Daten zu schützen sind. Somit bietet das erste Datenwiedergabegerät **1** und das erste Datenaufzeichnungsgerät **81** Mittel zum Verschlüsseln von Daten, Mittel zum Entschlüsseln von Daten und Mittel zum Weitergeben eines Verschlüsselungsschlüssels. Falls die Authentifikation fehlschlägt, stoppt das erste Datenwiedergabegerät **1** die Datenausgabe zu dem zweiten Datenaufzeichnungsgerät **81**. Falls die Datenausgabe abgeschlossen ist, sind die Daten verschlüsselt und kein Schlüssel wird weitergegeben, so dass die Daten nicht richtig wiedergegeben werden können. Das heißt, dass, falls die verschlüsselten Daten direkt in dem Auf-

zeichnungsgerät aufgezeichnet werden, die Daten nicht richtig wiedergegeben werden können.

**[0057]** Des Weiteren befasst sich die Beschreibung hier mit der Übertragung der Daten mit dem Aufzeichnungsgerät. Über das Wiedergabegerät und das Ausgabegerät, in gleicher Weise, arbeitet der DVD-Antrieb, um zu authentifizieren, ob die Wiedergabe- oder das Ausgabegerät es ermöglichen, den Kopierbetrieb richtig zu steuern zum Zweck eines Schutzes der Daten.

**[0058]** Das Vorsehen dieser Mittel beim Übertragen der Daten macht es möglich, ein Kopieren der Copyright-Daten richtig zu steuern und ein illegales Kopieren oder eine Wiedergabe zu verhindern.

**[0059]** Fig. 8 zeigt die Anordnung, in welcher die Datenausgabevorrichtung gemäß der vorliegenden Erfindung in einem Monitor angewandt ist. Die vorliegende Ausführungsform befasst sich z.B. mit der Monitorausgabe. Es versteht sich von selbst, dass sie nicht auf den Monitor begrenzt ist, sondern auf irgendeine Art von Gerät angewandt werden kann, welches dazu dient, Daten durch den Datenbus zu empfangen und zu senden.

**[0060]** In Fig. 8 bezeichnet ein Bezugszeichen **90** einen Monitor. Ein Bezugszeichen **91** bezeichnet ein drittes Datenverarbeitungsgerät. Ein Bezugszeichen **92** bezeichnet einen Konverter. Ein Bezugszeichen **93** bezeichnet ein Anzeigegerät.

**[0061]** Das MPEG-Board **29** gibt die Daten auf den Monitor **90** aus. Die in den Monitor **90** eingegebenen Daten werden durch den Konverter **31** konvertiert und dann auf den Monitor **32** ausgegeben, auf welchem das Bild angezeigt wird. Der Vorgang bis zu diesem Punkt entspricht dem Hauptbetrieb des Monitors.

**[0062]** Falls die Daten in den Monitor **90** durch den Datenbus **100** eingegeben sind, können die Daten zum Schutz der Daten davor, illegal aufgezeichnet zu werden, verschlüsselt sein. In diesem Fall arbeitet das dritte Datenverarbeitungsgerät **91**, um die Daten zu entschlüsseln und dann die sich ergebenden Daten in den Konverter **92** auszugeben. Das bedeutet, dass das dritte Datenverarbeitungsgerät **91** die entsprechende Authentifikationseinheit zu dem MPEG-Board **29** benötigt. Die Authentifikationseinheit kann arbeiten, um zu authentifizieren, dass die Ausgabe von dem MPEG-Board **29** nur zu dem Anzeigegerät, wie etwa einem Monitor **90**, ausgegeben wird, nicht zu dem Aufzeichnungsgerät. Falls kein Aufzeichnungsgerät angeschlossen ist, werden die Daten nicht illegal kopiert. Somit ist es, wenn die Daten auf den Monitor **90** ausgegeben werden, nicht notwendig, die Daten zu verschlüsseln. Das Vorsehen dieser Mittel beim Weitergeben der Daten führt dazu, dass es möglich gemacht wird, den Kopiervorgang der mit Copyright versehenen Daten richtig zu steuern, dabei ein illegales Kopieren und eine Wiedergabe verhindernd.

**[0063]** Fig. 9 zeigt eine Wiedergabe- oder Aufzeichnungs- und Wiedergabevorrichtung, konfiguriert als ein System, z.B. ein Personal Computer, welches eine Mehrzahl von Datenverarbeitungsmitteln (im Folgenden bezeichnet als „Gerät"), wie etwa die oben erläuterte Datenwiedergabevorrichtung, eine Datenaufzeichnungs- und Wiedergabevorrichtung, usw. aufweist. Der Personal Computer kann die Auslegung dieser Geräte leicht ändern. Somit ist die Kombination dieser Geräte nicht auf die in dieser Ausführungsform beschriebene Kombination beschränkt, sondern sie kann die Kombination all der Geräte betreffen, welche die Daten weitergeben.

**[0064]** In Fig. 9 bezeichnet ein Bezugszeichen **101** ein MPEG-Board. Ein Bezugszeichen **102** bezeichnet einen MO-Antrieb. Ein Bezugszeichen **103** bezeichnet eine Digitalkamera.

**[0065]** Der Personal Computer ist angeordnet, um die Daten unter den Geräten durch den Datenbus **100** weiterzureichen. Die Authentifikation wird zu den Geräten vorgenommen, welche mit dem Datenbus verbunden sind.

**[0066]** Falls keine Authentifikation erreicht wird, ist bestimmt, dass das Gerät keine Funktion einer richtigen Steuerung des Kopiervorgangs vorsieht. Die Datenausgabe wird gestoppt. Zu dieser Zeit, falls es den Daten gestattet ist, lediglich wiedergegeben zu werden, wird die Datenausgabe nur möglich gemacht, falls kein Aufzeichnungsgerät mit dem Datenbus verbunden ist und die verbundenen Geräte nur die Wiedergabefunktion aufweisen.

**[0067]** Falls des Weiteren keine Authentifikation erreicht wird, können die Daten auf dem Datenbus nur weitergegeben werden, falls die Daten, welche weitergegeben werden sollen, keine Kopierbeschränkung aufweisen.

**[0068]** Diese Authentifikationen werden durch die in jedem Gerät vorgesehene Schaltung möglich gemacht. Anstelle dessen kann, in einem solchen Fall wie etwa dem Personal Computer, die Software zur Steuerung jedes Geräts die Authentifikationsfunktion vorsehen. Des Weiteren kann die Authentifikation an dem Betriebssystem zur systematischen Steuerung jedes Geräts vorgenommen werden. Dann kann, gemäß dem authentifizierten Ergebnis, jedes Gerät gesteuert werden.

**[0069]** Wie oben beschrieben, wird die Authentifikation durchgeführt zwischen den Geräten, welche mit dem Datenbus verbunden sind, gemäß dem Typ der

Daten. Gemäß dem Ergebnis kann die Übertragung der Daten gesteuert werden. Das macht es möglich, den Kopiervorgang richtig zu steuern.

**[0070]** Fig. 10 ist ein Blockdiagramm, welches eine Datenwiedergabevorrichtung zum Wiedergeben von Daten zeigt, welche Kopiersteuerinformation enthalten, gemäß einer anderen Ausführungsform der vorliegenden Erfindung. Die Vorrichtung der Fig. 10 ist ein Beispiel, in welchem die Vorrichtung, gezeigt in Fig. 1, ausgebildet ist mit einer Vorrichtung, wie z.B. in Endverbraucher-DVD-Spielern. In solchen Vorrichtungen ist, da es schwierig ist, den DVD-Antrieb mit dem MPEG-Board und umgekehrt auszutauschen, keine Authentifikation erforderlich. Auch wenn die DVD-Signalverarbeitung und eine MPEG-Dekodierung als interne Verarbeitung in demselben LSI ausgeführt werden, ist keine Authentifikation erforderlich, da keine Verbindung zur Außenseite dazu oder davon möglich ist und es auch unmöglich ist, die Signale aus den Datenbussen abzugreifen. In diesen Fällen ist es nicht notwendig, eine Mehrzahl von Authentifikationseinheiten vorzusehen, und eine Wiedergabe kann ausgeführt werden durch Umschalten zwischen einer Mehrzahl der Verschlüsselungseinheiten.

**[0071]** Gemäß der vorliegenden Erfindung wird, in dem Fall eines Wiedergebens der Daten, welche in jeweiliger Art und Weise zu den Typen des Aufzeichnungsmediums und der Kopiersteuerinformation verschlüsselt sind, die entsprechende Authentifikationseinheit zu jeder Verschlüsselungsart richtig geschaltet. Dies macht es möglich, den Entschlüsselungsvorgang gemäß der Verschlüsselungsart vorzunehmen. Des Weiteren wird die Datenausgabe gestoppt, falls keine Authentifikation erreicht wird. Es ist somit möglich, illegal kopierte Daten daran zu hindern, aufgezeichnet und wiedergegeben zu werden.

**[0072]** Zusätzlich macht es die Einbeziehung dieser Funktionen auf der gleichen LSI schwierig, die Daten auf dem Übertragungsweg abzugreifen.

## Patentansprüche

1. Authentifikationsverfahren zur Durchführung einer Authentifikation zwischen Geräten, wenn ein Gerät (**1**, **57**) Eingabedaten (**16**, **67**) erhält, eine nötige Verarbeitung zum Aufzeichnen oder zur Wiedergabe durchführt und verarbeitete Eingabedaten (**17**, **66**) zu einem externen Gerät ausgibt, wobei das Authentifikationsverfahren die Schritte aufweist des:
Auswählens, aus einer Vielzahl von Verschlüsselungsverfahren, eines Verschlüsselungsverfahrens zum Verschlüsseln von Daten, die aus den Eingabedaten abgeleitet sind, welche abgeleiteten Daten verarbeitet werden sollen, und
Auswählens, aus einer Mehrzahl von Authentifikationsverfahren, eines Authentifikationsverfahrens, welches der Art der Verschlüsselung der abgeleiteten Daten entspricht, wobei das externe Gerät authentifiziert wird unter Verwendung des ausgewählten Authentifikationsverfahrens, und Ausgebens der verschlüsselten Daten.

2. Verfahren wie in Anspruch 1 beansprucht, wobei die Vielzahl von Verschlüsselungsverfahren der Auswahl unterzogen wird, basierend auf der Art der Eingabedaten.

3. Verfahren wie in Anspruch 2 beansprucht, wobei die Vielzahl von Verschlüsselungsverfahren der Auswahl unterzogen wird, basierend auf einer Kopiersteuerinformation auf den Daten.

4. Verfahren wie in Anspruch 3, aufweisend den Schritt des Kodierens oder Dekodierens von Bilddaten,
wobei der Schritt des Kodierens oder Dekodierens weiter einschließt den Schritt des Detektierens von zusätzlicher Information, die zu den Daten zugefügt ist, die beim Schritt des Kodierens oder Dekodierens eingegeben sind, und
wobei das Authentifikationsverfahren ein Ausgeben der kodierten Bilddaten in Übereinstimmung mit der zusätzlichen Information steuert, detektiert in dem Schritt des Detektierens.

5. Authentifikationsverfahren wie in Anspruch 1 beansprucht, wobei das Gerät ein Aufzeichnungsgerät einschließt,
wobei das Aufzeichnungsgerät eines von der Mehrzahl von Verschlüsselungsverfahren auswählt und die von dem externen Gerät ausgegebenen Daten unter Verwendung des ausgewählten Verschlüsselungsverfahrens verschlüsselt, und
wobei das Aufzeichnungsgerät mit dem externen Gerät eine Authentifikation ausführt, unter Verwendung einer der Mehrzahl von Authentifikationsverfahren, welches einem Typ des ausgewählten Verschlüsselungsverfahrens entspricht, und, nachdem die Authentifikation bestätigt ist, Daten aufzeichnet, die von dem externen Gerät ausgegeben sind.

6. Verfahren wie in Anspruch 5 beansprucht, wobei die Vielzahl von Verschlüsselungsverfahren einer Auswahl unterzogen wird, basierend auf einer Information, welche einen Typ eines Aufzeichnungsmediums bezeichnet, auf welchem die Daten, die von dem externen Gerät ausgegeben sind, aufgezeichnet werden sollen.

7. Verfahren wie in Anspruch 6, wobei die Vielzahl von Verschlüsselungsverfahren einer Auswahl unterzogen wird, basierend auf einer Kombination von Information, welche einen Typ eines Aufzeichnungsmediums, auf welchem die Daten, die von dem externen Gerät ausgegeben werden, aufgezeichnet werden sollen, und eine Kopiersteuerinformation

über die Daten, die von dem externen Gerät ausgegeben werden, bezeichnet (d.h. in zwei Stellen eingeht).

8. Verfahren wie in Anspruch 7, wobei die Vielzahl von Verschlüsselungsverfahren einschließt einen Verschlüsselungsschritt des Durchführens eines Verschlüsselungsvorgangs, welcher einer Kombination der Infomation entspricht, die einen Typ des Aufzeichnungsmediums bezeichnet, und der Kopiersteuerinformation für die Daten, die von dem externen Gerät ausgegeben werden, um aufgezeichnet zu werden.

9. Verfahren wie in Anspruch 8, wobei die Information, welche einen Typ eines Aufzeichnungsmediums bezeichnet, Information einschließt, welche bezeichnet, ob das Medium für die Wiedergabe gedacht ist oder aufnehmbar, und wobei die Kopiersteuerinformation für die aufzuzeichnenden Daten Information enthält, welche bezeichnet, ob das Medium kopierfrei, kopiergeschützt oder kopiererlaubt ist für nur eine Generation.

10. Verfahren wie in Anspruch 8, wobei die Kombination einschließt zumindest zwei Arten von Informationen, d.h. Information, welche bezeichnet, ob das Medium aufnehmbar und kopiergeschützt oder kopiererlaubt für nur eine Generation ist, und Information, die bezeichnet, ob das Medium aufnehmbar und kopierfrei ist.

11. Authentifikationsverfahren wie in Anspruch 1 beansprucht, wobei
ausgewählt wird aus der Vielzahl von Authentifikationsverfahren zum Durchführen einer Authentifikation mit dem externen Gerät, eines Authentifikationsverfahrens, welches dem Typ der Eingabedaten entspricht, und authentifiziert wird mit dem externen Gerät, unter Verwendung des ausgewählten Authentifikationsverfahrens, und
ausgewählt wird, aus einer Mehrzahl von Verschlüsselungsverfahren, ein Verschlüsselungsverfahren, welches dem ausgewählten Authentifikationsverfahren entspricht, um die abgeleiteten Daten zu verschlüsseln und die verschlüsselten Daten auszugeben.

12. Datenverarbeitungsvorrichtung, welche eine Vielzahl von Datenverarbeitungsmitteln (**29**, **30**) aufweist, zum Übertragen von Daten durch einen Datenbus (**100**, **20**, **22**, **70**, **18**), wobei jedes der Mehrzahl von Datenverarbeitungsmitteln (**29**, **30**) eine Mehrzahl von Verschlüsselungsmitteln (**62**) einschließt und Verschlüsselungsmittel (**62**) davon auswählt, welche einem Typ der Daten entsprechen, die übertragen werden sollen, um die Daten zu verschlüsseln, wobei die Vielzahl von Datenverarbeitungsmitteln (**29**, **30**) jedes einschließt eine Vielzahl von Authentifikationsmitteln (**4**, **5**, **24**, **8**, **9**, **27**) und ein Authentifikationsmittel (**4**, **5**, **24**, **8**, **9**, **27**) auswählt, welches dem ausgewählten Verschlüsselungsmittel (**62**) entspricht, um ein externes Gerät zu authentifizieren, bevor die Daten durch den Datenfluss übertragen werden.

13. Vorrichtung wie in Anspruch 12, wobei die ausgewählten Authentifikationsmittel (**4**, **5**, **6**, **24**, **8**, **9**, **10**, **27**) eine Authentifikation durchführen vor dem Übertragen der Daten und, falls eines oder mehr Datenverarbeitungsmittel (**29**, **30**) nicht erfolgreich bei der Authentifikation ist/sind, ein Ausgeben der Daten zu dem Datenbus (**110**, **20**, **22**, **90**, **18**) stoppen.

14. Vorrichtung wie in Anspruch 12, wobei die ausgewählten Authentifikationsmittel (**4**, **5**, **6**, **24**, **8**, **9**, **10**, **27**) eine Authentifikation ausführen vor dem Übertragen von Daten und, falls eines oder mehr Datenverarbeitungsmittel (**29**, **30**) bei der Authentifikation nicht erfolgreich ist/sind, den Typ der zu dem Datenbus (**100**, **20**, **22**, **70**, **18**) auszugebenden Daten beschränken.

15. Vorrichtung wie in Anspruch 12, wobei die Authentifikationsmittel (**4**, **5**, **24**, **8**, **9**, **27**) eine Authentifikation durchführen vor dem Übertragen der Daten und, falls eines oder mehr Datenverarbeitungsmittel bei der Authentifikation nicht erfolgreich ist/sind, die zu dem Datenbus (**100**, **20**, **22**, **70**, **18**) auszugebenden Daten auf das erfolgreich authentifizierte Gerät (**24**, **4**, **5**, **6**) begrenzen.

16. Vorrichtung wie in Anspruch 12, wobei die ausgewählten Authentifikationsmittel (**4**, **5**, **24**, **8**, **9**, **27**) eine Authentifikation durchführen vor dem Übertragen von Daten und, falls eines oder mehr Datenverarbeitungsmittel bei der Authentifikation nicht erfolgreich ist/sind, die Daten nur ausgeben, falls die auszugebenden Daten, die zu dem Datenbus (**100**, **20**, **22**, **70**, **18**) ausgegeben werden sollen, kopierfrei sind.

17. Vorrichtung wie in Anspruch 12, wobei die ausgewählten Authentifikationsmittel (**4**, **5**, **24**, **8**, **9**, **27**) eine Authentifikation vor dem Übertragen von Daten ausführen und, falls zumindest eines der Datenverarbeitungsmittel bei der Authentifikation nicht erfolgreich ist, ein Ausgeben der Daten zu dem Datenbus (**100**, **20**, **22**, **70**, **18**) stoppen.

Es folgen 9 Blatt Zeichnungen

**Anhängende Zeichnungen**

FIG.1

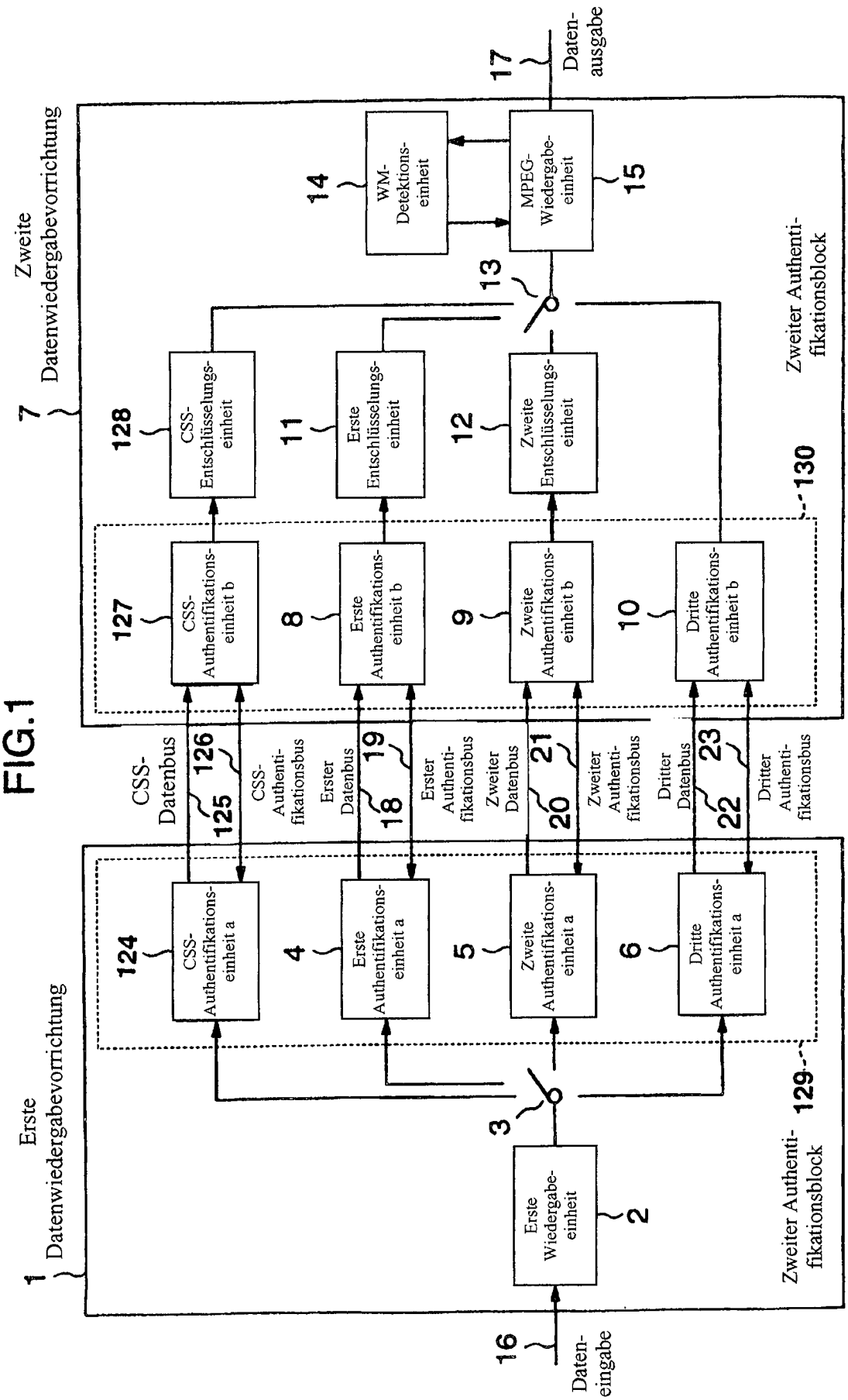
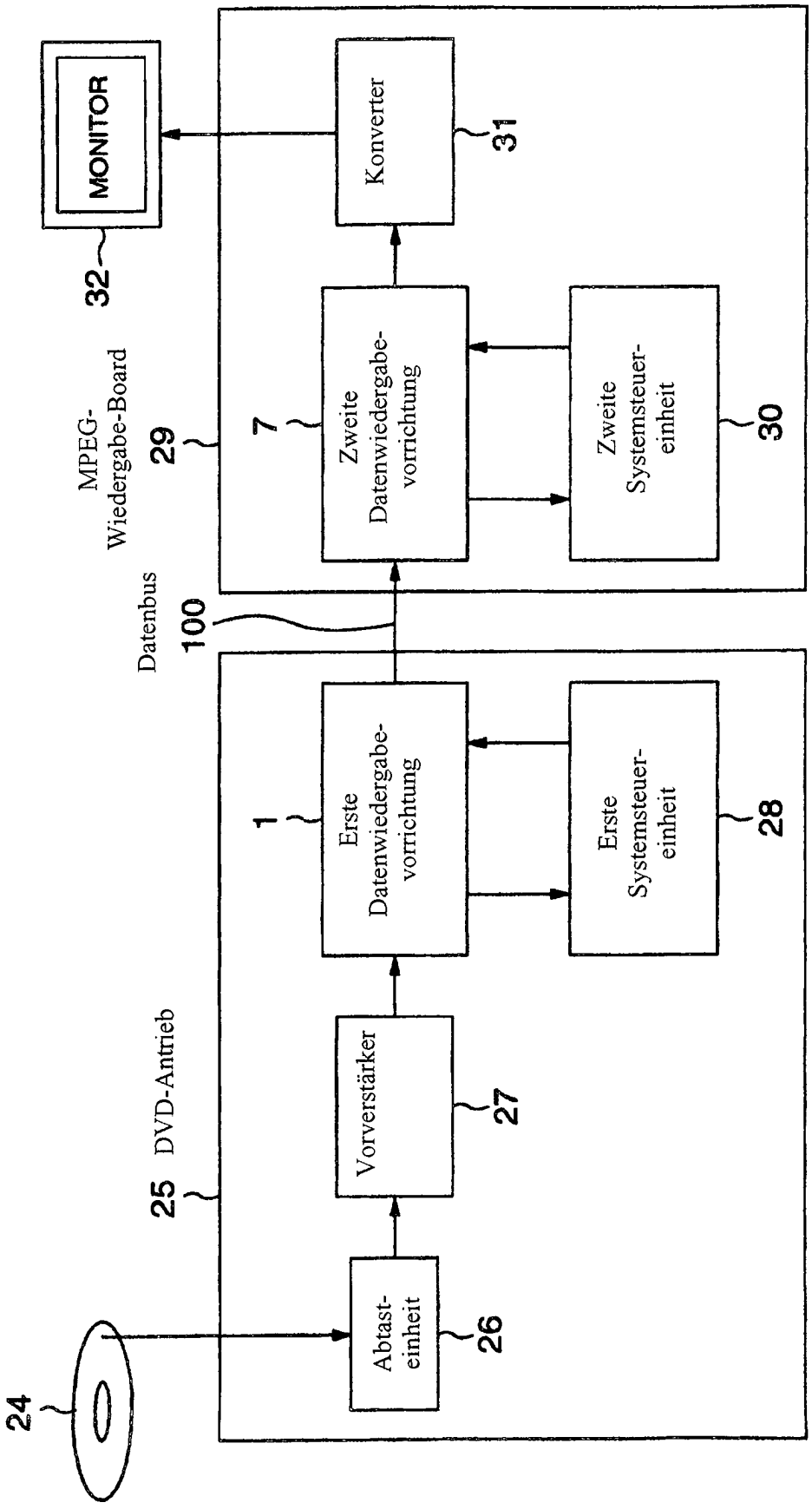


FIG.2


MONITOR
32
Konverter
31
MPEG-
Wiedergabe-Board
29
7
Zweite
Datenwiedergabe-
vorrichtung
Zweite
Systemsteuer-
einheit
30
Datenbus
100
1
Erste
Datenwiedergabe-
vorrichtung
Erste
Systemsteuer-
einheit
28
25
DVD-Antrieb
Vorverstärker
27
Abtast-
einheit
26
24

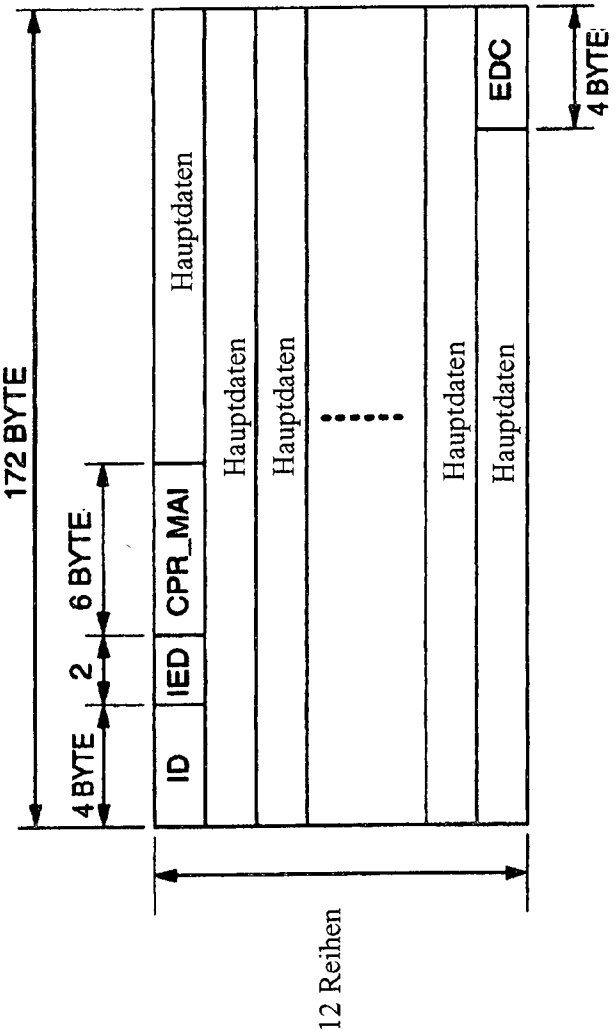

172 BYTE
4 BYTE
2
6 BYTE
ID
IED
CPR_MAI
Hauptdaten
Hauptdaten
Hauptdaten
Hauptdaten
Hauptdaten
EDC
4 BYTE
12 Reihen

FIG.3

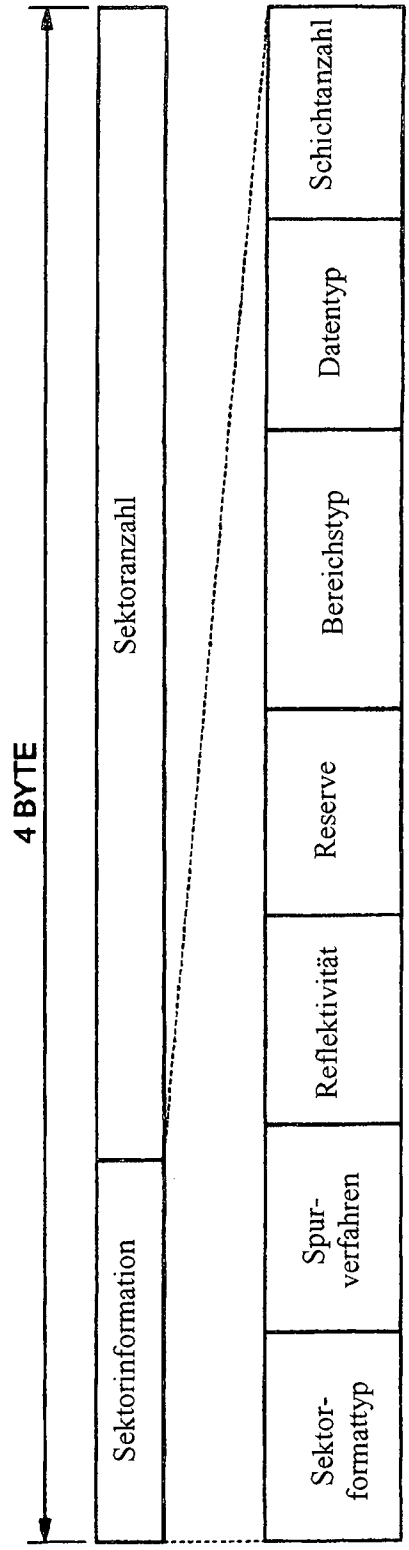

4 BYTE
Sektorinformation
Sektoranzahl
Sektor-formattyp
Spur-verfahren
Reflektivität
Reserve
Bereichstyp
Datentyp
Schichtanzahl

FIG.4

FIG.5

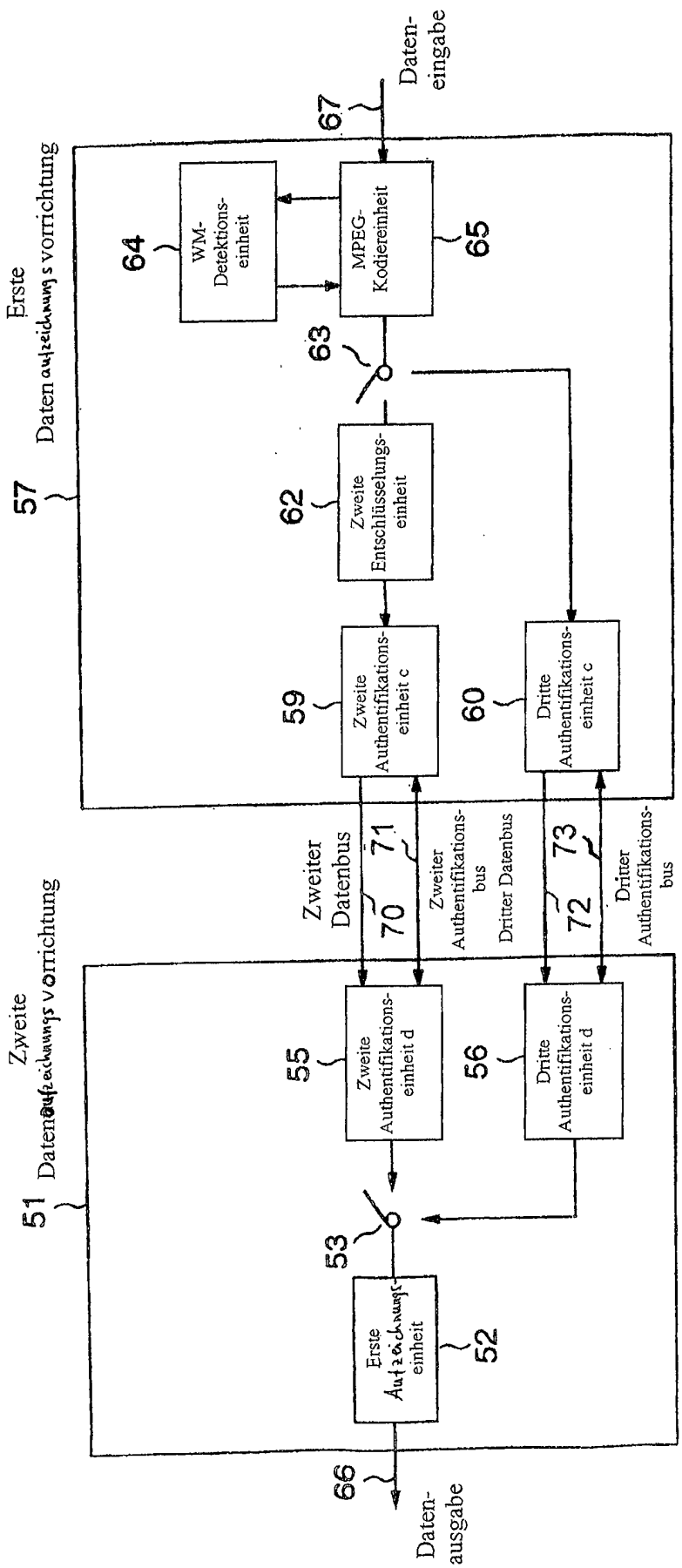

Erste Datenaufzeichnungsvorrichtung
57
Daten-eingabe
67
WM-Detektions-einheit
64
MPEG-Kodiereinheit
65
63
Zweite Entschlüsselungs-einheit
62
Zweite Authentifikations-einheit c
59
Dritte Authentifikations-einheit c
60
Zweiter Datenbus
70
71
Zweiter Authentifikations-bus
Dritter Datenbus
72
73
Dritter Authentifikations-bus
Zweite Datenaufzeichnungsvorrichtung
51
Zweite Authentifikations-einheit d
55
Dritte Authentifikations-einheit d
56
53
Erste Aufzeichnungs-einheit
52
66
Daten-ausgabe

FIG.6

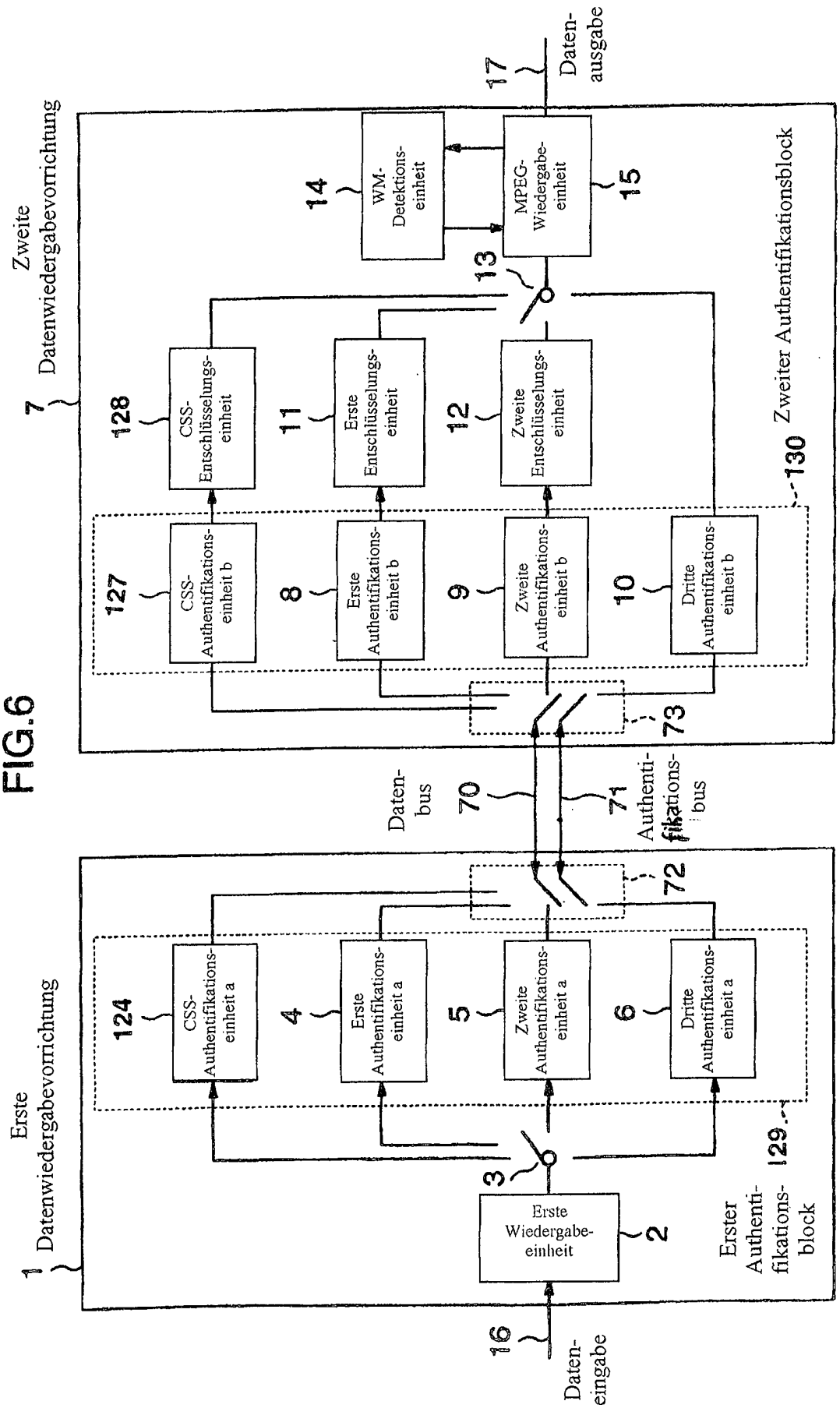

Erste Datenwiedergabevorrichtung
1
Erste Wiedergabe-einheit
2
3
Erster Authentifikations-block
129
CSS-Authentifikations-einheit a
124
Erste Authentifikations-einheit a
4
Zweite Authentifikations-einheit a
5
Dritte Authentifikations-einheit a
6
Daten-eingabe
16
Daten-bus
70
Authentifikations-bus
71
72
73
Zweite Datenwiedergabevorrichtung
7
CSS-Authentifikations-einheit b
127
Erste Authentifikations-einheit b
8
Zweite Authentifikations-einheit b
9
Dritte Authentifikations-einheit b
10
CSS-Entschlüsselungs-einheit
128
Erste Entschlüsselungs-einheit
11
Zweite Entschlüsselungs-einheit
12
13
WM-Detektions-einheit
14
MPEG-Wiedergabe-einheit
15
Daten-ausgabe
17
Zweiter Authentifikationsblock
130

FIG.7

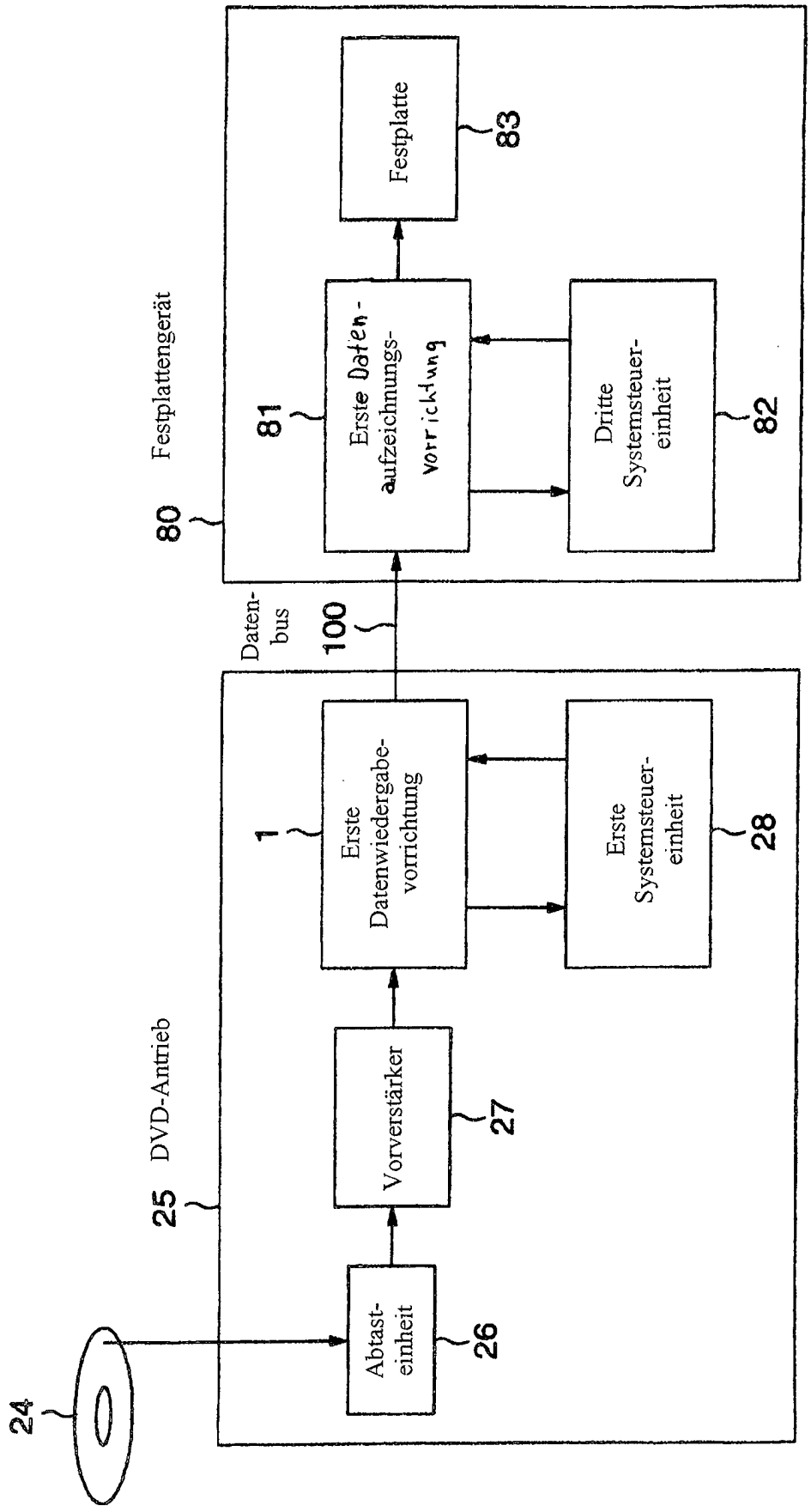

24
DVD-Antrieb
25
Abtast-einheit
26
Vorverstärker
27
Erste Datenwiedergabe-vorrichtung
1
Erste Systemsteuer-einheit
28
Daten-bus
100
Festplattengerät
80
Erste Daten-aufzeichnungs-vorrichtung
81
Dritte Systemsteuer-einheit
82
Festplatte
83

FIG.8

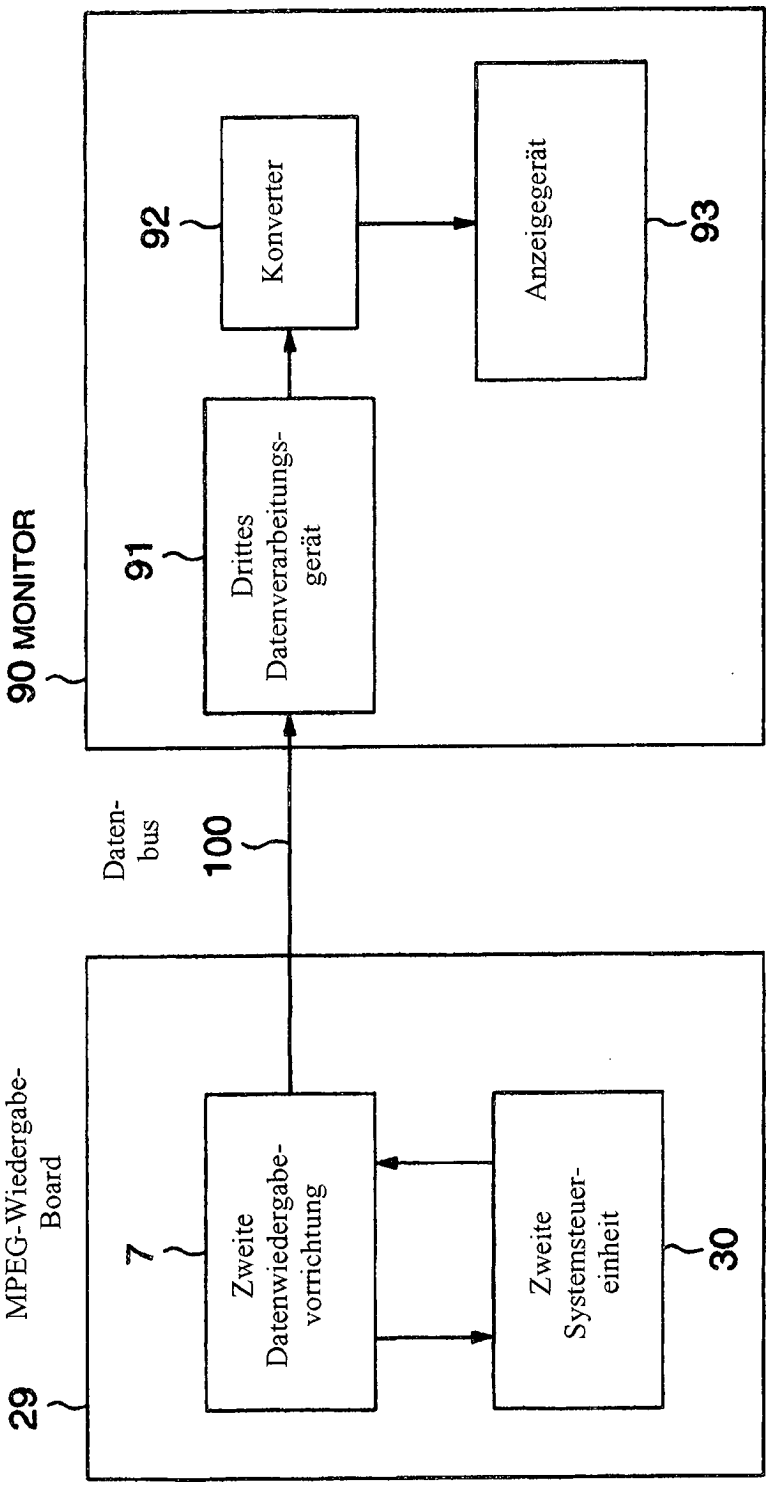

90 MONITOR
91
Drittes Datenverarbeitungs-gerät
92
Konverter
Anzeigegerät
93
Daten-bus
100
MPEG-Wiedergabe-Board
29
7
Zweite Datenwiedergabe-vorrichtung
Zweite Systemsteuer-einheit
30

FIG.9

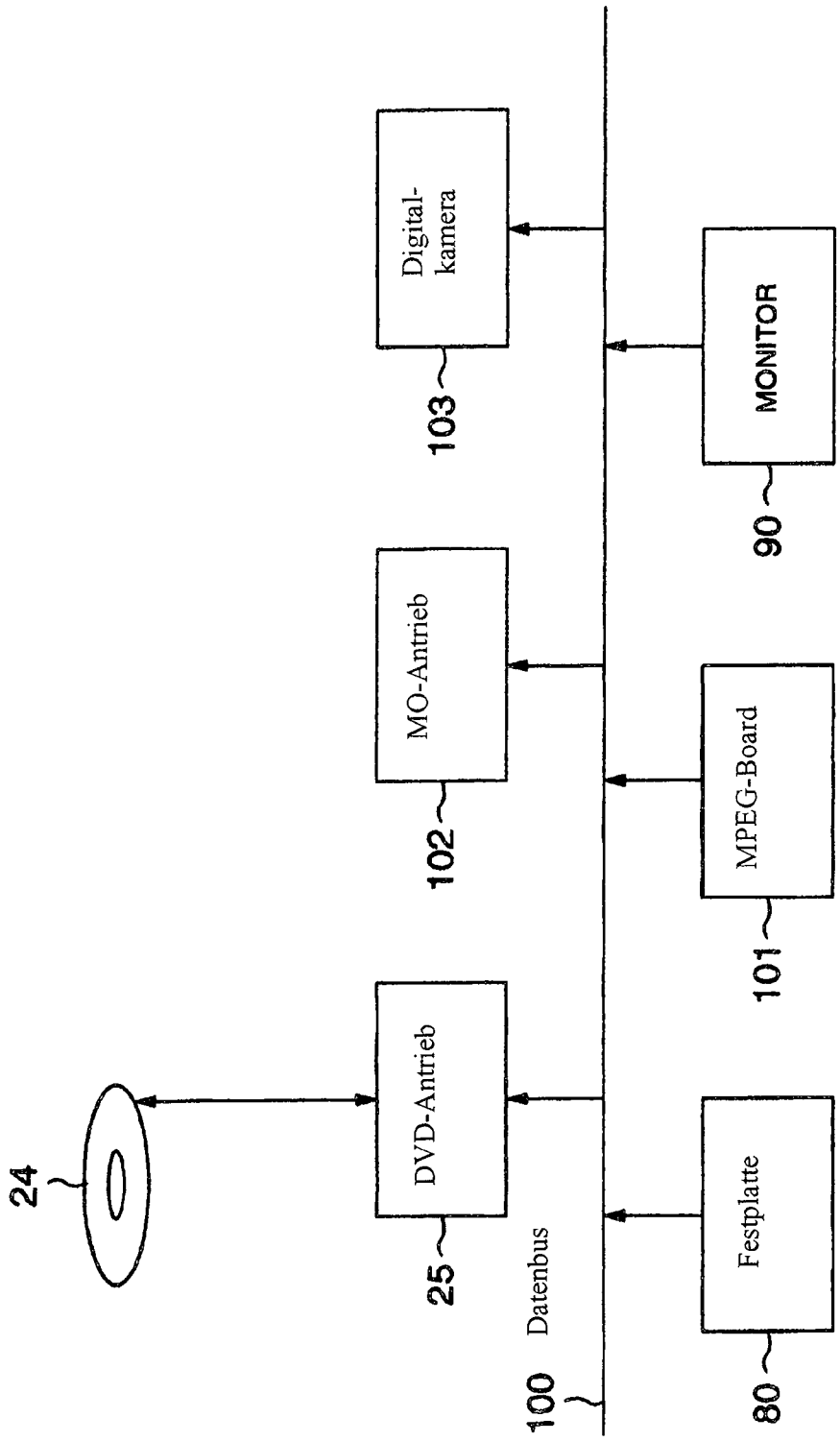
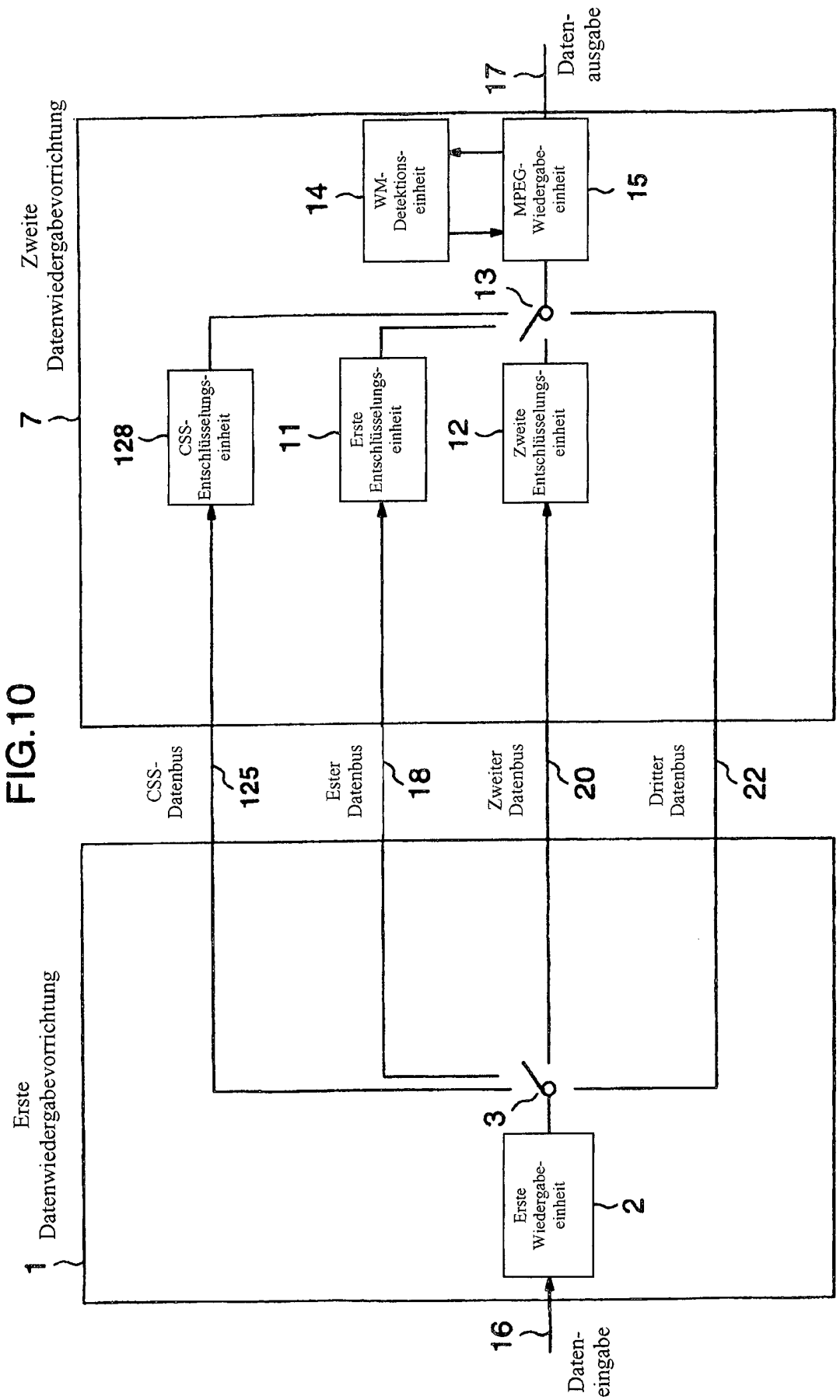

24
DVD-Antrieb
25
MO-Antrieb
102
Digital-kamera
103
MPEG-Board
101
MONITOR
90
Festplatte
80
Datenbus
100

FIG.10


Erste Datenwiedergabevorrichtung
1
Erste Wiedergabe-einheit
2
3
16
Daten-eingabe
CSS-Datenbus
125
Ester Datenbus
18
Zweiter Datenbus
20
Dritter Datenbus
22
Zweite Datenwiedergabevorrichtung
7
128
CSS-Entschlüsselungs-einheit
11
Erste Entschlüsselungs-einheit
12
Zweite Entschlüsselungs-einheit
13
14
WM-Detektions-einheit
MPEG-Wiedergabe-einheit
15
17
Daten-ausgabe