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

(10) **DE 698 19 924 T2** 2004.09.02

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 018 078 B1**
(21) Deutsches Aktenzeichen: **698 19 924.3**
(86) PCT-Aktenzeichen: **PCT/IB98/01510**
(96) Europäisches Aktenzeichen: **98 942 974.1**
(87) PCT-Veröffentlichungs-Nr.: **WO 99/015970**
(86) PCT-Anmeldetag: **22.09.1998**
(87) Veröffentlichungstag der PCT-Anmeldung: **01.04.1999**
(97) Erstveröffentlichung durch das EPA: **12.07.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **19.11.2003**
(47) Veröffentlichungstag im Patentblatt: **02.09.2004**

(51) Int Cl.[7]: **G06F 12/14**
G06F 1/00

(30) Unionspriorität:
97402237 **25.09.1997** **EP**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Canal + Technologies, Paris, FR

(72) Erfinder:
BENARDEAU, Christian, F-77600 Bussy Saint Georges, FR

(74) Vertreter:
Tiedtke, Bühling, Kinne & Partner GbR, 80336 München

(54) Bezeichnung: **VERFAHREN ZUM SCHUTZ VON AUFGEZEICHNETEN DIGITALEN DATEN**

Beschreibung

[0001] Die Erfindung bezieht sich auf ein Verfahren und eine Vorrichtung zum Schutz von aufgezeichneten digitalen Daten, zum Beispiel zum Schutz von Audio- und/oder visuellen Daten, wie sie auf Kompakt-Disks bzw. CDs, digitalen Video-Disks bzw. Video-CDs oder anderen ähnlichen Trägern aufgezeichnet sind.

[0002] Die Einführung von digitaler Technologie in dem audiovisuellen Gebiet brachte für den Verbraucher im Vergleich zu analogen Technologien insbesondere im Bezug auf die Qualität einer Reproduktion von Ton und Bild und der Haltbarkeit des Trägermediums beträchtliche Vorteile. Die Kompakt-Disk hat so gut wie alle traditionelle Vinylaufzeichnungen ersetzt, und ein ähnlicher Trend wird mit der Einführung von neuen digitalen Produkten erwartet, welche im Allgemeinen auf den Multimedia- und Heimunterhaltungsmarkt, insbesondere die digitale Video-Disk, abgezielt sind.

[0003] Ein mit digital aufgezeichneten Daten in Zusammenhang stehendes spezielles Problem liegt in der Einfachheit ihrer Reproduktion und der daraus entstehenden Möglichkeit zur Piraterie. Eine einzelne digitale Aufzeichnung kann Verwendung finden, um eine beliebige Anzahl von perfekten Kopien ohne irgendeine Abschwächung in der Qualität des Tons oder Bildes anzufertigen. Dieses Problem ist insbesondere mit der Einführung bzw. dem Aufkommen von aufzeichenbaren digitalen Produkten, wie beispielsweise der Mini-Disk oder DAT schwerwiegend, und die Abneigung von Unterhaltungsfirmen Copyrightarbeiten zu lizenzieren, solange dieses Problem bleibt, hat als eine Bremse auf die Einführung von neuen Medienprodukten in den Markt gewirkt.

[0004] Gegenwärtig war die einzige praktikable verfügbare Lösung gegen unautorisierte Reproduktion von Copyrightarbeiten eine Rechtliche, und eine Anzahl an Staaten in Europa und sonst wo haben eine Antipirateriegesetzgebung eingebracht, um die wachsende Anzahl an raubkopierten Filmen, CDs und so weiter zu bekämpfen, die auf den Markt gebracht werden. Aus offensichtlichen Gründen, ist eine rechtliche Lösung aus der Sicht einer vorbeugenden Handlung weniger als optimal.

[0005] Technologische Antikopierlösungen, welche zur Handhabung von audiovisuellen Arbeiten vorgeschlagen wurden, waren extrem einfach bzw. grundlegend, da sie sich beispielsweise auf den Gedanken der Verwendung einer Form von digitalem „Handschlag" zwischen dem Leser bzw. der Leseeinrichtung und dem Trägermedium stützen bzw. angewiesen sind, um so den Ursprung des Aufgezeichneten zu verifizieren. Ein derartiger Schutz ist jedoch nur gegen die niedrigste Stufe von Kopieraktivität effektiv, da das Handschlagssignal auf keinerlei Weise geschützt ist und einfach gelesen und reproduziert werden kann, um eine unautorisierte Kopie in eine scheinbar autorisierte und lesbare Kopie umzuwandeln.

[0006] Computersysteme, welche geheime Schlüssel verwenden, die auf einer Chipkarte gespeichert sind, um den Zugriff auf verschlüsselte Computer-Disk-Daten zu steuern, sind beispielsweise aus US 5 191 611 bekannt. Derartige Systeme besitzen den Nachteil dahingehend, dass die Leseeinrichtung mit beträchtlichen Verarbeitungs- und Speicherfähigkeiten ausgestattet sein muss, um die aufgezeichneten verschlüsselten Blöcke von Daten zu entschlüsseln und zu speichern. Wie verstanden werden wird, sind derartige Systeme im Allgemeinen unbequem, wenn sie zum Schutz von Computerdaten Verwendung finden, und sind sogar noch ungeeigneter zur Anwendung in dem audiovisuellen Gebiet, bei dem eine Leseeinrichtung typischer Weise eine viel kleinere Kapazität zum Verarbeiten und Speichern von Daten im Vergleich zu einem Computer aufweist, bei dem jedoch nichtsdestotrotz ein Echtzeitfluss von Daten aufrechterhalten werden muss.

[0007] EP 0 840 194 ist unter Artikel 54 (3) EPC für den Gegenstand des vorliegenden Patents relevant.

[0008] Es ist das Ziel der vorliegenden Erfindung, die mit dem Stand der Technik in Zusammenhang stehenden Nachteile zu überwinden, und eine effiziente technologische Lösung gegen die unautorisierte Reproduktion von digital aufgezeichneten Copyrightarbeiten, insbesondere in Bezug auf audiovisuelle Arbeiten, zur Verfügung zu stellen.

[0009] Gemäß der vorliegenden Erfindung ist ein Verfahren zum Beschränken des Zugriffs auf aufgezeichnete digitale Daten nach Anspruch 1 zur Verfügung gestellt.

[0010] Für digitale Trägermedien, wie beispielsweise CDs, CD-ROMs und so weiter, hat jede Aufzeichnung eine damit in Zusammenhang stehende Einleitung oder einen Kopf in der Form eines Volume-Deskriptors, welcher grundlegende Informationen im Bezug auf den Speicherentwurf beziehungsweise das Speicherlayout und Zugriffspunkte auf digitale Informationen auf dem Medium, die Menge an auf dem Medium gespeicherten Daten, das Datum der Erzeugung des Trägermediums und so weiter darlegt bzw. festlegt. Diese nur eine kleine Speichermenge einnehmenden Informationen sind nichtsdestotrotz wesentlich für das Lesen des Aufgezeichneten und ohne diese Informationen kann die Leseeinrichtung nicht auf die aufgezeichneten Daten zugreifen.

[0011] Durch Verschlüsseln dieser Informationen und Speichern des Entschlüsslungsschlüssels in einer mit dem Trägermedium in Zusammenhang stehenden integrierten Schaltung schützt die Erfindung gegen unautorisiertes Kopieren des Aufgezeichneten, da die Leseeinrichtung nicht in der Lage sein wird, auf die gespeicherten Daten ohne die entschlüsselten Elemente des Volume-Deskriptors zuzugreifen, und da der hierfür notwendige Schlüssel von der integrierten Schaltung gehalten wird, welche natürlich einem Kopieren widersteht. Auch wenn die gespeicherten nicht verschlüsselten Daten kopiert werden, wird die resultierende Kopie unlesbar, da

der Volume-Deskriptor nur in einer unvollständigen oder vollkommen verschlüsselten Form vorhanden sein wird. Die Entschlüsselung der Volume-Elemente kann innerhalb der integrierten Schaltung derart ausgeführt werden, dass der Schlüssel niemals frei verfügbar gemacht wird.

[0012] Im Gegensatz zu dem zum Schutz von Computerdaten verwendeten Stand der Technik wird nur der Volume-Deskriptor oder die Kopfdaten verschlüsselt/ entschlüsselt, was den Bedarf zum Ausführen von kryptographischen Operationen auf das gesamte Volumen von gespeicherten Daten vermeidet. Wie verstanden werden wird, ist dies insbesondere vorteilhaft, wenn die Erfindung in dem Gebiet von audiovisuellen Vorrichtungen angewendet werden soll, bei denen die Verarbeitungs- und Speicherkapazität einer Leseeinrichtung relativ klein sein kann.

[0013] Bei einem Ausführungsbeispiel ist die integrierte Schaltung in einer mit dem Trägermedium in Zusammenhang stehenden Chipkarte eingebettet, wobei die Chipkarte agiert, um die verschlüsselten Volume-Elemente zu entschlüsseln, und um diese an die Leseeinrichtung weiterzuleiten, um so ein Lesen und/oder Schreiben der aufgezeichneten nicht verschlüsselten Daten zu ermöglichen.

[0014] In diesem Zusammenhang stellt eine Chipkarte eine sichere und haltbare bzw. dauerhafte Einrichtung zur Aufbewahrung des zur Entschlüsselung der Volume-Deskriptor-Elemente notwendigen Schlüssels zur Verfügung. Gleichermaßen sind die Produktionskosten einer derartigen Karte im Vergleich zu beispielsweise dem Preis der Aufzeichnung selbst relativ klein.

[0015] Bei dieser Anmeldung wird der Ausdruck „Chipkarte" verwendet, indem er eine beliebige herkömmliche auf einem Chip basierende Kartenvorrichtung bezeichnet, die beispielsweise einen Mikroprozessor oder ein EEPROM-Speicher zum Aufbewahren des Schlüssels aufweist. In diesem Ausdruck sind auch PCMCIA-Karten und andere tragbare Chip tragende Karten oder Vorrichtungen umfasst, die alternative physische Formen aufweisen, wie beispielsweise die oft bei Fernsehdekodersystemen verwendeten schlüsselförmigen Vorrichtungen.

[0016] Während sie eine insbesondere bequeme Art der Umschließung beziehungsweise Aufnahme der bei der Erfindung verwendeten integrierten Schaltung oder des „Chips" zur Verfügung stellt, ist eine Chipkarte nicht die einzige verfügbare Lösung. Beispielsweise wird der Schlüssel bei einer Realisierung in einer integrierten Schaltung gespeichert, die in dem Gehäuse des digitalen Trägermediums eingebettet ist.

[0017] Die Aufnahme eines Mikroprozessors innerhalb des Gehäuses des Trägermediums ist eine bekannte Technik und wurde beispielsweise in dem Fall von DVHS-Kassetten vorgeschlagen, bei denen eine Gruppe von metallischen Kontakten an einer äußeren Fläche des Kassettengehäuses zur Verfügung gestellt sein kann, wobei die Kontakte zu einer integrierten Schaltung oder einem Chip in dem Inneren des Gehäuses führen. Diese Kontakte können mit einer entsprechenden Gruppe von Kontakten in dem Buchsenteil der Aufzeichnungseinrichtung eingreifen, um eine Kommunikation zwischen der integrierten Schaltung und der Videoaufzeichnungseinrichtung zu ermöglichen.

[0018] Eine derartige Lösung verhindert den Bedarf an dem zur Verfügung Stellen einer Chipkarte oder dergleichen im Zusammenhang mit der Aufzeichnung, und ist folglich von dem Standpunkt des Konsumenten inhärent einfacher. Der Bedarf zum Aufweisen von beispielsweise einem Chipkartenschlitz in der digitalen Leseeinrichtung wird auch vermieden, auch wenn sich die Produktionskosten des Aufzeichnungsmediums natürlich erhöhen werden, um die Einführung einer integrierten Schaltung in dem Gehäuse aufzunehmen, wie die Kosten der Elemente der zum Lesen des Trägers verwendeten Leseeinrichtung ansteigen können.

[0019] Bei einem Ausführungsbeispiel des Schlüssels zum Verschlüsseln und/oder Entschlüsseln der Volume-Deskriptor-Elemente umfasst ein durch eine Herstellungskonstante diversifizierter bzw. mannigfaltig gemachter bzw. breit gefächerter Schlüssel, die einen mit der Identität des Trägermediums oder der aufgezeichneten Daten in Zusammenhang stehenden Wert repräsentiert, beispielsweise eine Serien- oder Chargennummer. Auf diese Weise kann ein einfacher Verschlüsslungsalgorithmus Verwendung finden, der durch die Herstellungskonstante diversifiziert ist, um einen „einzigartigen" Schlüssel und einen einzigartigen verschlüsselten Volume-Deskriptor zur Verfügung zu stellen. Tatsächlich kann für die meisten praktischen Zwecke der selbe Schlüssel für eine gegebene Charge an Aufzeichnungsträgern oder für eine spezielle aufgezeichnete Aufführung bzw. Vorführung erzeugt werden.

[0020] In seiner einfachsten Form kann der bei dieser Erfindung verwendete Schlüsselalgorithmus irgendein Algorithmus einer Anzahl an bekannten symmetrischen Algorithmen, wie beispielsweise DES oder RC2 usw. sein. Bei einem derartigen Fall können die Verschlüsslungs-/ Entschlüsslungsschlüssel als identisch angenommen werden. Es sind andere Ausführungsbeispiele möglich, die beispielsweise öffentliche/private Schlüsselpaare verwenden.

[0021] Bei einer Realisierung des Verfahrens der Erfindung werden die Volume-Elemente von der integrierten Schaltung gemäß einem in der integrierten Schaltung erzeugten und gespeicherten neuen Schlüssel erneut verschlüsselt, wonach die neu verschlüsselten Volume-Elemente durch die Leseeinrichtung auf dem Medium aufgezeichnet werden, was die zuvor verschlüsselten Werte ersetzt. Auf diese Weise wird die Sicherheit des Systems erhöht und die Identifikation der integrierten Schaltung mit der fraglichen Aufzeichnung sichergestellt.

[0022] Der neue Schlüssel kann von der integrierten Schaltung unter Verwendung von beispielsweise einem

Zufalls- oder Pseudozufalls-Nummerngenerator erzeugt werden. Folglich wird, auch in dem Fall einer Charge von zu Anfangs mit dem selben Schlüssel verschlüsselten Aufzeichnungen, der verschlüsselte Volume-Deskriptor mit jedem Abspielen der Aufzeichnung schnell derart mutieren, dass sich keine zwei Aufzeichnungen mit dem selben Schlüssel öffnen werden.

[0023] Bei einem Ausführungsbeispiel wird der von der integrierten Schaltung erzeugte neue Schlüssel durch einen mit der Identität der Leseeinrichtung in Zusammenhang stehenden Wert, beispielsweise seiner Seriennummer, diversifiziert, die durch die integrierte Schaltung von der Leseeinrichtung gelesen wird. Dies ermöglicht, dass die Aufzeichnung nur von dieser speziellen Leseeinrichtung gelesen wird.

[0024] Bei einem Ausführungsbeispiel ist der mit der Identität der Leseeinrichtung in Zusammenhang stehende Wert auf dem Trägermedium gespeichert und wird von der integrierten Schaltung mit dem Wert verglichen, der von der Leseeinrichtung bei aufeinanderfolgenden Lesevorgängen direkt gelesen wird. Bei einer Realisierung kann die integrierte Schaltung den von der Leseeinrichtung gelesenen Wert einfach zurückweisen, wenn dieser nicht mit dem auf dem Medium Gespeicherten übereinstimmt.

[0025] Jedoch kann das System bei einer alternativen Realisierung programmiert sein, um eine Aktualisierung dieses Werts zu erlauben, um beispielsweise die Möglichkeit zuzulassen, dass die Leseeinrichtung ausgetauscht wurde oder kaputt gegangen ist. Bei einem derartigen Ausführungsbeispiel vergleicht die integrierte Schaltung den von dem Trägermedium gelesenen Identitätswert mit dem von der Leseeinrichtung Gelesenen und wirkt, in dem Fall eines Nichtübereinstimmens oder eines Unterschieds zwischen den Beiden, zum Verschlüsseln der Volume-Elemente unter Verwendung des vorhergehenden Leseeinrichtungs-Identitätswerts von dem Aufzeichnungsmedium und danach zum erneut Verschlüsseln der Volume-Elemente unter Verwendung des neuen Leseeinrichtungs-Identitätswerts von der Leseeinrichtung.

[0026] Die neue Leseeinrichtungsidentität kann die vorhergehende Leseeinrichtungsidentität entweder ersetzen oder zusammen mit ihr gespeichert werden. Bei dem ersteren Fall kann, um zu verhindern, dass eine unbeschränkte Anzahl an Leseeinrichtungen auf die Disk zugreifen kann, die integrierte Schaltung programmiert werden, so dass diese Operation nur eine vorbestimmte Anzahl von Malen ausgeführt wird. Bei dem letzteren Fall kann die integrierte Schaltung programmiert werden, so dass ermöglicht wird, dass eine vorbestimmte Anzahl an autorisierten Leseeinrichtungsidentitäten gespeichert wird, um so zu erlauben, dass die Aufzeichnung beispielsweise auf einer Anzahl an dem Benutzer gehörenden Leseeinrichtungen abgespielt werden kann. Mit einer beschränkten Anzahl an Leseeinrichtungsidentitäten kann die integrierte Schaltung sicher eine unbeschränkte Anzahl an Wechseln zwischen den autorisierten Leseeinrichtungen zulassen.

[0027] Die vorliegende Erfindung wurde zuvor weitgehend in Bezug auf den Schutz von zuvor aufgezeichneten Aufzeichnungen, wie beispielsweise zuvor aufgezeichneten CDs, CD-ROMs usw. beschrieben. Jedoch kann die selbe Technik, wie wahrgenommen werden wird, auf unbespielte bzw. leere bzw. unbeschriebene aufzeichenbare Einheiten angewendet werden, und bei einer Realisierung ist das Trägermedium vor seinem ersten Einlegen in die Leseeinrichtung unbespielt, wobei das Vorhandensein der zugehörigen integrierten Schaltung notwendig ist, um die Volume-Elemente zu entschlüsseln, bevor es der Leseeinrichtung erlaubt ist, irgendwelche Daten auf das unbespielte Medium zu schreiben.

[0028] Derartige unbespielte Einheiten besitzen auch eine Gruppe von Volume-Deskriptor-Elementen, von denen einige oder alle, wie zuvor beschrieben, verschlüsselt werden können, um sicherzustellen, dass die Einheiten nur bei dem Vorhandensein des gespeicherten Schlüssels und, falls gewünscht, in einer oder einer ausgewählten Anzahl an Leseeinrichtungen gelesen / aufgezeichnet werden können. Auf diese Weise kann ein Schutz gegen unautorisierte Kopien der letztendlich aufgezeichneten Arbeit erbracht werden, die auf dem Aufzeichnungsmedium in unverschlüsselter Form gespeichert ist.

[0029] Dementsprechend ist es auch zu verstehen, dass, während der Ausdruck „Leseeinrichtung" Verwendung findet, um im Allgemeinen Vorrichtungen zu bezeichnen, die in der Lage sind, im Voraus aufgezeichnete digitale Daten zu lesen, Vorrichtungen umfasst sind, die in der Lage sind, digitale Daten auf das Aufzeichnungsmedium bei denjenigen Ausführungsbeispielen zu schreiben oder aufzuzeichnen, bei denen ein Aufzeichnen derartiger Daten ausgeführt wird.

[0030] Bei einem Ausführungsbeispiel erstreckt sich die Erfindung auf ein Verfahren zum Beschränken des Zugriffs auf aufgezeichnete digitale Daten, bei dem die Daten audio- und/oder visuelle Daten sind. Jedoch wird wahrgenommen werden, dass die Erfindung gleichermaßen zum Schutz von computerverarbeiteten Daten angewendet werden kann.

[0031] Die vorliegende Erfindung erstreckt sich gleichermaßen auf ein Verfahren zur Herstellung eines digitalen Trägermediums und einer integrierten Schaltung, wie sie beispielsweise in einer Chipkarte eingebaut ist, zur Verwendung bei dem Verfahren der vorliegenden Erfindung.

[0032] Nun wird ein bevorzugtes Ausführungsbeispiel der Erfindung anhand eines nur als Beispiel dienenden Beispiels und in Bezug auf die beigefügten Figuren beschrieben. Es zeigen:

[0033] **Fig.** 1 die Schritte bei der Erzeugung eines digitalen Trägermediums, in diesem Fall eine CD-ROM, die einen zumindest teilweise verschlüsselten Volume-Deskriptor und eine den Entschlüsslungsschlüssel enthaltende Chipkarte umfasst; und

[0034] **Fig.** 2 die Schritte, die bei dem Lesen des digitalen Trägermediums ausgeführt werden, dass gemäß **Fig.** 1 verschlüsselt ist.

[0035] Bezugnehmend auf **Fig.** 1 sind die Schritte bei der Herstellung einer digitalen Aufzeichnung einschließlich eines verschlüsselten Volume-Deskriptors gezeigt. Bei Schritt **1** wird ein erster Verschlüsslungsschlüssel Kf erlangt und von einer Herstellungskonstante Cf diversifiziert, um einen „einzigartigen" Schlüssel abzuleiten, welcher mit der fraglichen Aufzeichnung in Zusammenhang steht. Der Verschlüsslungsschlüssel Kf kann aus einem beliebigen für eine Fachperson bekannten symmetrischen Standardverschlüsselungsalgorithmus erlangt werden, wie beispielsweise DES.

[0036] Die Herstellungskonstante Cf kann aus einer Anzahl an mit der fraglichen Aufzeichnung in Zusammenhang stehenden Werten gewählt werden, die beispielsweise die Seriennummer des Aufzeichnungsmediums umfassen. Jedoch kann die Herstellungskonstante Cf bei einem vereinfachten Ausführungsbeispiel eine mit der Herstellung einer Charge von CD-ROMs in Zusammenhang stehende Chargennummer repräsentieren, oder sogar eine Seriennummer entsprechend der Katalognummer eines Films, einer musikalischen Aufführung usw., der/die auf der CD-ROM aufgezeichnet ist.

[0037] In dem letzteren Fall wird der selbe digitale Schlüssel beispielsweise für alle aufgezeichneten Versionen der selben Aufführung oder dem selben Film erzeugt. Auch wenn sie weniger sicher ist als die Realisierungen, bei welchen eine Herstellungskonstante auf der Grundlage des Aufzeichnungsmediums selbst Verwendung findet (beispielsweise der CD-ROM-Serien- oder -Chargennummer), kann das von diesem Ausführungsbeispiel zur Verfügung gestellte Sicherheitsniveau nichtsdestotrotz für kommerzielle Zwecke ausreichend sein.

[0038] Der aus dem Diversifizieren des ersten Schlüssels Kf erlangte „einzigartige" Verschlüsslungsschlüssel wird dann bei Schritt **3** verwendet, um eins oder mehr Elemente des mit dem fraglichen Aufzeichnungsmedium in Zusammenhang stehenden Volume-Deskriptor V zu verschlüsseln. Wie in der Einleitung erwähnt, ist die Verwendung eines Volume-Deskriptors in dem Gebiet von digitalen Aufzeichnungen ein in der Technik gut bekanntes Konzept. Ein derartiger Deskriptor beinhaltet eine Anzahl an Elementen, die Eigenschaften des Aufzeichnens beschreiben (gespeicherte Datenmenge, Layout von digitalen Blöcken von Informationen bei dem Aufzeichnen usw.), die von der Leseeinrichtung zu lesen und Zusammenzufügen sind, bevor die Aufzeichnung abgespielt werden kann.

[0039] Das Format des Volume-Deskriptors für ein gegebenes digitales Aufzeichnungsmedium (CD, CD-ROM, DVD usw.) wird im Allgemeinen von einem internationalen Standard oder einer internationalen Norm bestimmt, um eine Kompatibilität zwischen verschiedenen Leseeinrichtungen sicherzustellen. In dem Fall von CD-ROMs wird beispielsweise das Format des Volume-Deskriptors von dem internationalen Standard ISO 9660 bestimmt, auf welchen sich die Leseeinrichtung der vorliegenden Anmeldung bezieht.

[0040] Wenn gewünscht, können alle diese Informationen bei einem Ausführungsbeispiel der vorliegenden Erfindung verschlüsselt werden. Jedoch kann, da ein Teil der Informationen in dem Volume-Deskriptor für alle standardisierten Aufzeichnungen effektiv unveränderlich sein wird, eine effizientere Lösung auf die Verschlüsslung von nur bestimmten Elementen des gesamten Volume-Deskriptors gegründet werden.

[0041] Beispielsweise können in dem Fall einer CD-ROM die an den Achtbitzeichenpositionen 129 bis 190 des Volume-Deskriptors gefundenen Daten, wie in Tabelle 4 des Standards ISO 9660, verschlüsselt werden. Bei diesen Positionen werden die folgenden Daten gefunden:

129 bis 132	Größe eines Logikblocks
133 bis 140	Größe einer Pfadtabelle
141 bis 144	Position eines Auftretens einer Pfadtabelle des Typs L
145 bis 148	Position eines optionalen Auftretens einer Pfadtabelle des Typs L
149 bis 152	Position eines Auftretens einer Pfadtabelle des Typs M
153 bis 156	Position eines optionalem Auftretens einer Pfadtabelle des Typs M
157 bis 190	Aufzeichnen eines Indexes für den Quellenindex

[0042] Wie wahrgenommen werden wird, ist die Erfindung, während der Deskriptor hier in Bezug auf eine CD-ROM-Disk beschrieben wird, gleichermaßen auf andere Formate von digitalen Aufzeichnungen von audiovisuellen oder Multimediatyp-Daten einschließlich derartiger Deskriptoren, wie beispielsweise digitale Video-Disks oder dergleichen, anwendbar.

[0043] Wieder bezugnehmend auf **Fig.** 1 werden die ausgewählten Elemente des Volume-Deskriptors V von dem Trägermedium **2** gelesen und bei Schritt **3** von dem diversifizierten Schlüssel Kf verschlüsselt. Die resultierenden verschlüsselten Elemente des Volume-Deskriptors, hier durch E1(V) bezeichnet, finden danach Verwendung, um die Originalelemente V auf dem Träger **2** zu ersetzen. Das auf diese Weise gebildete Trägerme-

dium umfasst unverschlüsselte digitale Daten, die zusammen mit einem teilweise oder vollständig verschlüsselten Volume-Deskriptor den Großteil der fraglichen Aufzeichnung repräsentieren. Wie klar sein wird, kann die Aufzeichnung nicht ohne einen äquivalenten Entschlüsslungsschlüssel gelesen werden.

[0044] Um einem autorisierten Benutzer zu ermöglichen, auf die Daten auf dem Träger zuzugreifen, ist es notwendig, den Benutzer mit dem Schlüssel Kf und dem Diversifizierer Cf auszustatten. Bei dem vorliegenden Ausführungsbeispiel sind die Werte Kf, Cf in dem EEPROM einer an einer Chipkarte montierten integrierten Schaltung gespeichert. Die Chipkarte wird mit der Aufzeichnung derart verkauft, dass der legitimierte Benutzer die fragliche Aufzeichnung hören oder betrachten kann. Der Vorgang der Verschlüsslung wird nachstehend ausführlicher beschrieben. Ohne den Entschlüsslungsschlüssel sind irgendwelche von der Aufzeichnung angefertigte Kopien unlesbar. Wie verstanden werden wird, können die auf der Chipkarte gespeicherten Informationen nicht einfach kopiert werden, und es kann eine Beliebige einer Anzahl an Techniken, die aus anderen Gebieten bekannt sind, in welchen Chipkarten Verwendung finden (Bank, Telefonkarten usw.), verwendet werden, um einen unautorisierten Zugriff auf die Entschlüsslungsdaten zu verhindern.

[0045] Bei einem alternativen Ausführungsbeispiel kann der Schlüssel in einer integrierten Schaltung gespeichert sein, die in dem Körper oder dem Gehäuse des digitalen Auszeichnungsmediums eingebettet ist. Ein Einbauen eines Mikroprozessors innerhalb des Gehäuses eines Aufzeichnungsmediums ist eine bekannte Technik und wurde beispielsweise in dem Fall von DVHS-Kassetten vorgeschlagen, bei denen eine Gruppe von metallischen Kontakten an einer äußeren Fläche des Kassettengehäuses zur Verfügung gestellt sein kann, wobei die Kontakte zu einer elektronischen Schaltung führen, wie beispielsweise einer integrierten Schaltung oder einem Chip in dem Inneren des Gehäuses. Diese Kontakte können mit einer entsprechenden Gruppe von Kontakten in dem Buchsenteil des Rekorders bzw. der Aufzeichnungseinrichtung eingreifen, um eine Kommunikation zwischen der integrierten Schaltung und dem Videorekorder zu ermöglichen.

[0046] Ein derartiges Ausführungsbeispiel ist gleichermaßen resistent zu unautorisiertem Kopieren, da ein Besitz der physischen Aufzeichnung in der Form, in welcher sie an den Benutzer verkauft wurde, eine notwendige Bedingung zum Abspielen der aufgezeichneten Daten ist.

[0047] Nun werden unter Bezugnahme auf **Fig.** 2 die bei der Entschlüsslung und dem nachfolgenden erneut Verschlüsseln der Volume-Elemente V eingeschlossenen Schritte beschrieben. Wie zuvor erwähnt, sind die Werte des Verschlüsslungsschlüssels Kf und des Diversifizierers Cf in einer integrierten Schaltung gespeichert, die an einer mit dem Trägermedium **2** in Zusammenhang stehenden Chipkarte **4** montiert ist. Um die Aufzeichnung zu lesen, werden die Chipkarte **4** und der Träger **2** in die geeigneten Schlitze bei einer Leseeinrichtung **5** eingeführt beziehungsweise eingelegt. Chipkartenleser sind gut bekannt und die Modifikation von CD-ROM- oder DVD-Leseeinrichtungen, dass sie beispielsweise einen Chipkartenschlitz umfassen, würde ein relativ einfacher Schritt in Hinblick auf den Herstellungsvorgang sein.

[0048] Wie bei dem Verschlüsslungsverfahren von **Fig.** 1 wird der Schlüssel Kf durch die Herstellungskonstante Cf diversifiziert, wird bei Schritt **6** in der Chipkarte **4** gespeichert, und der resultierende diversifizierte Schlüssel wird bei Schritt S7 verwendet, um die von dem Trägerelement **2** gelesenen verschlüsselten Elemente E1(V) zu entschlüsseln. Der Entschlüsslungsvorgang wird innerhalb der Chipkarte ausgeführt und danach werden die entschlüsselten Volume-Elemente V bei Schritt **8** der Leseeinrichtung **5** zugeführt, um so ein Lesen der Aufzeichnung zu erlauben.

[0049] Bei seinem einfachsten Ausführungsbeispiel werden die verschlüsselten Volume-Elemente E1(V) in dem Träger **2** zurückgehalten und der selbe Schlüssel Kf und die Konstante Cf, die auf der Karte **4** gespeichert sind, können bei allen zukünftigen Lesevorgängen der Aufzeichnung Verwendung finden. Jedoch werden die entschlüsselten Volume-Elemente bei einem bevorzugten Ausführungsbeispiel danach bei Schritt **9** erneut verschlüsselt, um einen neuen verschlüsselten Wert E2(V) zu bilden, der auf dem Träger **2** über den anfänglichen Wert E1(V) geschrieben wird.

[0050] Die Volume-Elemente V werden unter Verwendung eines Schlüssels auf der Grundlage einer Zufallsnummer R erneut verschlüsselt, die von einem Zufalls- oder Pseudo-Zufalls-Nummerngenerator **10** innerhalb der integrierten Schaltung der Chipkarte selbst erzeugt werden. Die Zufallsnummer R wird auf der Chipkarte gespeichert, um ein nachfolgendes Entschlüsseln der Volume-Elemente bei dem nächsten Lesevorgang der Aufzeichnung zu erlauben. Auf diese Weise erlaubt das vorliegende Ausführungsbeispiel die schnelle Individualisierung von Karte und Aufzeichnung, sogar bei dem Fall einer Charge von Aufzeichnungen, die zu Anfangs unter Verwendung des selben Schlüssels Kf und des Diversifizierers Cf codiert werden.

[0051] Bei einer bevorzugten Variation wird der Zufallsnummernschlüssel selbst bei Schritt **11** unter Verwendung eines von der Leseeinrichtung **5** gelesenen Werts, beispielsweise seiner Seriennummer Ns, diversifiziert. Der Diversifizierwert Ns wird zusammen mit den erneut verschlüsselten Volume-Elementen E2(V) auf dem Träger **2** gespeichert. Bei diesem Ausführungsbeispiel wird der Wert Ns auf der Chipkarte **4** zusammen mit der Zufallsnummer R gespeichert.

[0052] Bei dem nächsten Lesevorgang der Aufzeichnung liest die Chipkarte **2** die Seriennummer Ns von der Leseeinrichtung **5** zusammen mit den Werten E2(V) und Ns, die auf dem Träger **2** gespeichert sind. Unter der Annahme, dass die selben Werte der Seriennummer Ns von der Leseeinrichtung **5** und dem Träger **2** gelesen

werden, erzeugt die Chipkarte dann den Entschlüsslungsschlüssel aus dem gespeicherten Zufallsnummernwert R und dem Diversifizierer Ns, um die Volume-Elemente V zu entschlüsseln, um so ein Lesen der Aufzeichnung zuzulassen bzw. zu erlauben. Wie zuvor, wird dann eine neue Zufallsnummer erzeugt, und es wird ein neuer verschlüsselter Wert der Volume-Elemente erzeugt und auf den Träger **2** geschrieben.

[0053] Liest die Chipkarte **2** nicht die selben Werte der Seriennummer Ns von dem Träger **2** und der Leseeinrichtung **5**, zeigt dies an, dass nun eine verschiedene Leseeinrichtung zum Lesen der Aufzeichnung Verwendung findet. Auch wenn dies eine unautorisierte oder betrügerische Verwendung der Aufzeichnung anzeigt, kann dies auch einfach anzeigen, dass der Benutzer seine Leseeinrichtung ausgetauscht hat, oder eine Anzahl an Leseeinrichtungen aufweist.

[0054] Folglich wird, während die Chipkarte einfach programmiert werden kann, um den von der Leseeinrichtung gelesenen Wert Ns zurückzuweisen und ein Verschlüsseln der Volume-Elemente zu verweigern, ein alternatives Ausführungsbeispiel bevorzugt, bei welchem eine beschränkte Anzahl an verschiedenen Leseeinrichtungen auf die Daten zugreifen kann. Bei einem derartigen Ausführungsbeispiel ist die Karte derart programmiert, dass für den Fall einer Nichtübereinstimmung zwischen den Werten der Seriennummer Ns die von dem Träger gelesene Seriennummer Verwendung findet, um den Zufallsschlüssel zu diversifizieren, so dass die Volume-Elemente korrekt entschlüsselt werden.

[0055] Danach wird die von der Leseeinrichtung gelesene neue Seriennummer Ns verwendet, um die Elemente erneut zu verschlüsseln, und diese neue Seriennummer wird zusammen mit den erneut verschlüsselten Volume-Elementen auf dem Träger gespeichert. Bei diesem Ausführungsbeispiel ersetzt die neue Seriennummer die vorhergehende Seriennummer. Die Karte kann mittels einer Kennung oder dergleichen programmiert werden, um eine beschränkte Anzahl an Austauschen (beispielsweise 1 oder 2) der Seriennummer auf dem Träger zu erlauben. Nachdem diese Nummer durchgelassen wurde, wird die Karte alle nachfolgenden Austausche zurückweisen, da sie entschieden hat, dass eine betrügerische Verwendung der Aufzeichnung stattfindet.

[0056] Bei einem alternativen Ausführungsbeispiel kann die Karte programmiert werden, um die Seriennummer von beliebigen neuen Leseeinrichtungen in einer Liste auf dem Träger zu speichern. Bei jedem Lesevorgang prüft die Karte, um festzustellen, ob die Seriennummer der Leseeinrichtung der der zuletzt verwendeten Leseeinrichtung entspricht, das heißt der Lesevorrichtungs-Seriennummer, die zum Verschlüsseln des Volume-Deskriptors bei der letzten Aufzeichnung Verwendung fand. Wenn nicht, wird die zum Verschlüsseln der Volume-Elemente bei dem letzten Lesevorgang verwendete Seriennummer von dem Träger zur Verwendung bei dem Verschlüsseln der Volume-Elemente gelesen.

[0057] Die Karte prüft auch, um festzustellen, ob die Seriennummer der gegenwärtigen Leseeinrichtung einer bereits auf dem Träger gespeicherten Nummer entspricht. Wenn nicht, wird eine neue „autorisierte" Seriennummer zu der Liste hinzugefügt. Diese neue Seriennummer wird dann verwendet, um die Zufallsnummer während dem erneut Verschlüsseln der Volume-Elemente für den nächsten Lesevorgang zu diversifizieren.

[0058] Sobald die Liste einen bestimmten Schwellwert erreicht, beispielsweise 2 oder 3 autorisierte Leseeinrichtungen, kann die Karte dann verweigern, irgendeine weitere Seriennummer zu der Liste hinzuzufügen und kann gleichzeitig verweigern, die entschlüsselten Volume-Elemente an die Decodiereinrichtung weiterzuleiten. Dieser Vergleich kann sogar vor dem Entschlüsselungsschritt derart stattfinden, dass die Karte für den Fall das Entschlüsseln der Volume-Elemente zurückweisen wird, dass die Leseeinrichtungsnummer nicht auf der vervollständigten Liste von autorisierten Leseeinrichtungen gefunden wird.

[0059] Im Vergleich zu dem Ausführungsbeispiel, bei welchem die Seriennummern sequentiell übereinander geschrieben werden, besitzt dieses Ausführungsbeispiel den Vorteil, dass ein Benutzer zwischen beliebigen der Leseeinrichtungen in der Liste eine unbeschränkte Anzahl an Malen passieren kann, wie es vernünftiger Weise von einem Benutzer ohne irgendwelche betrügerische Absichten nachgefragt werden kann.

[0060] Für eine Fachperson werden Variationen der zuvor beschriebenen Realisierungen offensichtlich sein. Beispielsweise wird es, während die Erfindung insbesondere in Bezug auf eine zuvor aufgezeichnete Disk oder Vorrichtung beschrieben wurde, klar sein, dass die selben Prinzipien auf leere beziehungsweise unbespielte Träger angewendet werden können, wie beispielsweise unbespielte digitale Disks oder Kassetten, da derartige Vorrichtungen nichtsdestotrotz mit einem Volume-Deskriptor ausgestattet sind, welche in Zusammenhang mit einer Chipkarte oder dergleichen, wie zuvor beschrieben, verschlüsselt werden können.

[0061] Bei dem ersten Einlegen des Mediums in die Disk, wird das Vorhandensein der zugehörigen integrierten Schaltung notwendig, um die Volume-Elemente zu entschlüsseln, bevor es der Leseeinrichtung erlaubt ist, irgendwelche Daten auf das unbespielte Medium aufzuzeichnen oder zu schreiben. Das Vorhandensein der integrierten Schaltung wird auch bei allen zukünftigen Lesevorgängen des Mediums obligatorisch sein, um so das unbegrenzte Kopieren von irgendwelchen tatsächlich auf dem Medium aufgezeichneten Informationen zu verhindern.

[0062] Wie zuvor, können die entschlüsselten Volume-Deskriptor-Elemente auf dem Träger erneut verschlüsselt und erneut aufgezeichnet werden, beispielsweise unter Verwendung eines zufällig erzeugten Schlüssels und unter Berücksichtigung irgendwelcher Änderungen der Informationen, die in den Volume-Deskriptor-Elemten beinhaltet sind, die mit der Änderung der Zusammensetzung des Trägers in Beziehung stehen, wie bei-

spielsweise von einer unbespielten Einheit zu einer aufgezeichneten Einheit oder zwischen zwei auf dem Träger vorgenommenen aufeinanderfolgenden Aufzeichnungen.

Patentansprüche

1. Verfahren zum Einschränken eines Zugriffs auf aufgezeichnete digitale Daten auf einem digitalen Trägermedium (**2**) unter Verwendung einer einen ersten Entschlüsselungsschlüssel (Kf) enthaltenden integrierten Schaltung, mit Verschlüsseln von einem oder mehr Elementen eines Volume-Deskriptors (V) des Trägermediums mit einem entsprechenden Verschlüsselungsschlüssel (Kf), Aufzeichnen der verschlüsselten Volume-Deskriptor-Elemente zusammen mit den unverschlüsselten Daten auf dem Trägermedium und, bei Zugreifen auf das digitale Trägermedium, Verwenden des Entschlüsselungsschlüssels der integrierten Schaltung, um die verschlüsselten Elemente des Volume-Deskriptors zu entschlüsseln, und um diese Elemente einem Leser (**5**) zuzuführen, um das Lesen und/oder Schreiben von unverschlüsselten Daten auf dem /das Trägermedium zuzulassen, **dadurch gekennzeichnet**, dass das eine oder die mehr Elemente des Volume-Deskriptors eine Voraussetzung für den Zugriff auf die unverschlüsselten Daten auf dem Trägermedium sind.

2. Verfahren zum Einschränken eines Zugriffs auf aufgezeichnete digitale Daten nach Anspruch 1, bei welchem die integrierte Schaltung in einer Chipkarte (**4**) eingebettet ist, die mit dem Trägermedium (**2**) in Zusammenhang steht, wobei die Chipkarte die Entschlüsselung der verschlüsselten Volume-Elemente und deren Weitergabe an den Leser bewirkt, um ein Lesen und/ oder Schreiben der aufgezeichneten Daten zuzulassen.

3. Verfahren zum Einschränken eines Zugriffs auf aufgezeichnete digitale Daten nach Anspruch 1, bei welchem der erste Schlüssel (Kf) in einer integrierten Schaltung gespeichert ist, die in dem Gehäuse des digitalen Trägermediums eingebettet ist.

4. Verfahren zum Einschränken eines Zugriffs auf aufgezeichnete digitale Daten nach einem der Ansprüche 1 bis 3, bei welchem der erste Schlüssel einen Schlüssel (Kf) umfasst, der durch eine Herstellungskonstante (Cf) breit gefächert ist, die einen Wert darstellt, der mit der Identität des Trägermediums oder den aufgezeichneten Daten in Zusammenhang steht.

5. Verfahren zum Einschränken eines Zugriffs auf aufgezeichnete digitale Daten nach einem der Ansprüche 1 bis 4, bei welchem der erste Schlüssel (Kf) mit einem symmetrischen Verschlüsselungsalgorithmus verwendbar ist.

6. Verfahren zum Einschränken eines Zugriffs auf aufgezeichnete digitale Daten nach einem der Ansprüche 1 bis 5, bei welchem die Volume-Elemente (V) von der integrierten Schaltung gemäß einem in der integrierten Schaltung erzeugten und gespeicherten neuen Schlüssel (R) erneut verschlüsselt werden, wobei die erneut verschlüsselten Volume-Elemente danach von dem Leser auf dem Medium unter Ersetzung der zuvor verschlüsselten Werte aufgezeichnet werden.

7. Verfahren zum Einschränken eines Zugriffs auf aufgezeichnete digitale Daten nach einem der vorangehenden Ansprüche, bei welchem das Trägermedium (**2**) vor seinem ersten Einlegen in den Leser unbespielt ist, wobei das Vorhandensein der zugehörigen integrierten Schaltung erforderlich ist, um die Volume-Elemente zu entschlüsseln, bevor es dem Leser erlaubt ist, irgendwelche Daten auf das unbespielte Medium zu schreiben.

8. Verfahren zur Herstellung eines digitalen Trägermediums und einer integrierten Schaltung zur Verwendung bei dem Verfahren nach einem der Ansprüche 1 bis 7, mit Verschlüsseln von einem oder mehr Elementen des mit dem Trägermedium in Zusammenhang stehenden Volume-Deskriptors mittels eines ersten Schlüssels und Speichern eines Äquivalents des zum Entschlüsseln des Volume-Deskriptors erforderlichen ersten Schlüssels in einer mit dem Trägermedium in Zusammenhang stehenden integrierten Schaltung.

9. Verfahren zur Herstellung eines digitalen Trägermediums und einer integrierten Schaltung nach Anspruch 8, bei welchem die integrierte Schaltung in einer mit dem digitalen Trägermedium in Zusammenhang stehenden Chipkarte eingebettet ist.

10. Verfahren zur Herstellung eines digitalen Trägermediums und einer integrierten Schaltung nach Anspruch 8, bei dem die integrierte Schaltung in dem Gehäuse des digitalen Trägermediums eingebettet ist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

Fig.1.

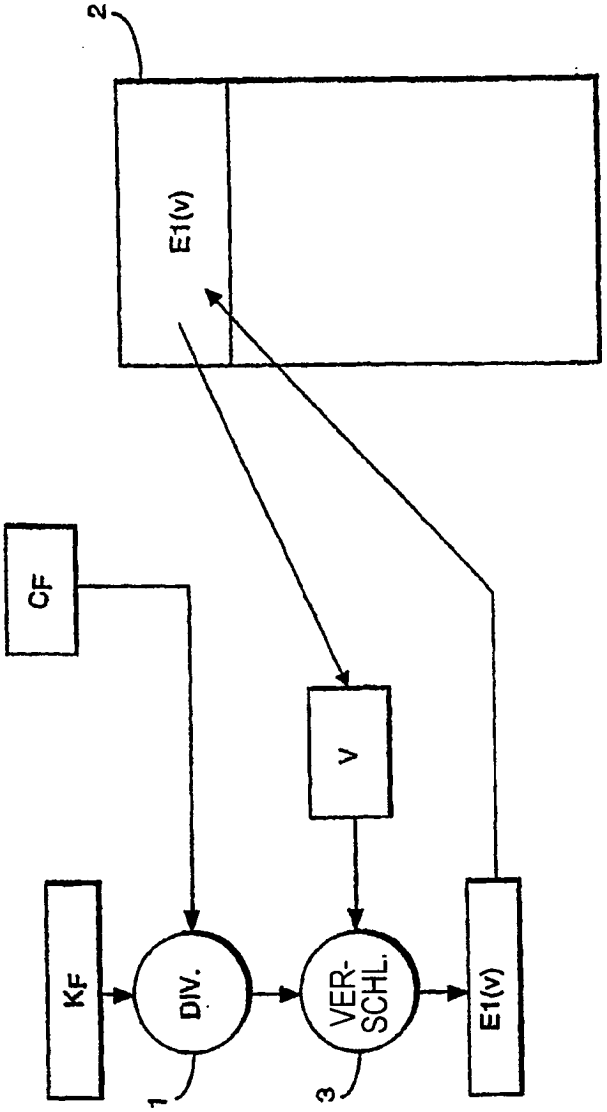
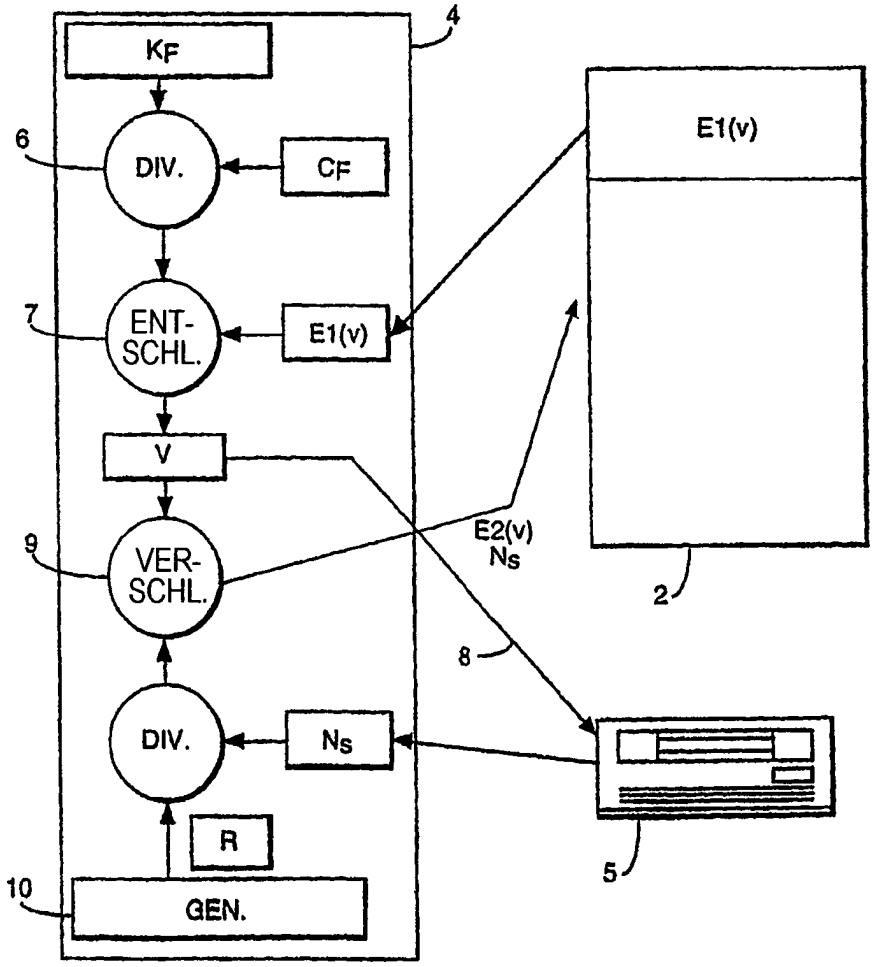


Fig.2.


4
KF
6
DIV.
CF
7
ENT-
SCHL.
E1(v)
V
9
VER-
SCHL.
E2(v)
Ns
8
DIV.
Ns
R
10
GEN.
E1(v)
2
5