(19) österreichisches patentamt

(10) **AT 500 500 B1 2012-11-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 1062/2005
(22) Anmeldetag: 23.06.2005
(45) Veröffentlicht am: 15.11.2012

(51) Int. Cl. : ***G11B 7/00*** (2006.01)
G11B 20/10 (2006.01)

(30) Priorität:
24.06.2004 JP P2004-185897 beansprucht.

(56) Entgegenhaltungen:
JP 2001283537 A JP 3157875 A
US 2002018412 A

(73) Patentinhaber:
SONY CORPORATION
TOKYO (JP)

(54) **VORRICHTUNG UND VERFAHREN ZUR ÜBERPRÜFUNG VON DATEN AUF SPEICHERMEDIEN**

(57) Die vorliegende Erfindung betrifft ein System für die Verifizierung von Daten, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind. Das System enthält eine Daten-Wiedergabeeinheit, um Daten wiederzugeben, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind, eine Erzeugungseinheit für Wiedergabe-Verifizierungsdaten, um eine Berechnung durchzuführen, die auf jenen Daten beruht, die von der Daten-Wiedergabeeinheit wiedergegeben werden, um Wiedergabe-Verifizierungsdaten zu erzeugen, sowie eine Daten-Vergleichseinheit, um die Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten zu vergleichen, die man durch das Ausführen einer Berechnung erhält, die auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

AT 500 500 B1 2012-11-15

Beschreibung

SYSTEM, VERFAHREN UND COMPUTERPROGRAMM ZUM VERIFIZIEREN VON DATEN AUF EINEM INFORMATIONS-AUFZEICHNUNGSTRÄGER

QUERVERWEISE AUF BEZUG HABENDE ANWENDUNGEN

[0001] Die vorliegende Erfindung enthält ein Fachgebiet, das sich auf die Japanische Patentanmeldung JP 2004-185897 bezieht, die im Japanischen Patentamt am 24. Juni 2004 eingereicht wurde und auf deren Gesamtinhalt hier Bezug genommen werden soll.

HINTERGRUND DER ERFINDUNG

1. GEBIET DER ERFINDUNG

[0002] Die vorliegende Erfindung betrifft ein System, ein Verfahren sowie ein Computerprogramm zum Verifizieren von Daten, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind. Im Besonderen betrifft die Erfindung ein System, ein Verfahren sowie ein Computerprogramm, um eine Information mit großer Betriebssicherheit zu verifizieren, während ein hoher Sicherheitsgrad beibehalten wird, wobei die Information einen Inhalt, der hinsichtlich des Urheberrechts geschützt werden soll, sowie einen Kodeschlüssel enthält, die auf einem Informations-Aufzeichnungsträger gespeichert sind und vor undichten Stellen geschützt werden sollen.

2. BESCHREIBUNG DES STANDS DER TECHNIK

[0003] Softwaredaten (später als Inhalt bezeichnet), beispielsweise Tondaten, etwa eine Musikspur, Bilddaten, etwa ein Film, ein Programm für Spiele oder ein Anwendungsprogramm, können als digitale Daten auf einem Aufzeichnungsträger gespeichert werden, beispielsweise auf einer Blu-Ray Disc unter Verwendung eines Blue-Lasers, auf einer DVD (digital versatile disc), einer Mini-Disc (MD) oder einer Compactdisc (CD). Im Besonderen kann auf einer Blu-Ray Disc mit hoher Dichte aufgezeichnet werden. Auf einer Blu-Ray Disc kann ein großer Video-Inhalt in Form von hochwertigen Daten aufgezeichnet werden.

[0004] Ein digitaler Inhalt, der auf verschiedenen Informations-Aufzeichnungsträgern aufgezeichnet wurde, wird an die Benützer verkauft. Der Benützer verwendet einen Personalcomputer (PC) oder eine Abspieleinheit, beispielsweise einen Plattenspieler, um den Inhalt wiederzugeben oder anzuwenden.

[0005] Im Allgemeinen befinden sich die Rechte von vielen Teilen des Inhalts, beispielsweise von Datengruppen für Musik und Bilder, im Besitz ihrer Autoren bzw. ihrer Großhändler. Beim Vertrieb wird die Verwendung des Inhalts eingeschränkt, wobei dies bedeutet, dass die Erlaubnis zu ihrer Anwendung nur berechtigten Benützern übertragen wird, um ein unberechtigtes Kopieren zu verhindern.

[0006] Bei digitalen Aufzeichnungsgeräten und Aufzeichnungsträgern können Daten, beispielsweise Bilddaten und Tondaten, mehrmals aufgezeichnet und wiedergegeben werden, ohne sie zu beeinträchtigen. Unglücklicherweise treten oft folgende Probleme auf: über das Internet werden unberechtigte Kopien des Inhalts verteilt; CD-Rs, die unberechtigte Kopien des Inhalts enthalten, d.h. Raubkopien der Platten, werden vertrieben; und der Inhalt wird auf den Festplatten von PCs von unberechtigten Benützern unerlaubt gespeichert, wobei der kopierte Inhalt unerlaubt verwendet wird.

[0007] DVDs und Aufzeichnungsträger mit hoher Kapazität, die Blue-Laser verwenden, die entwickelt wurden, können eine große Menge von Daten, die einem oder mehreren Filmen entsprechen, als digitale Information speichern. Da es möglich wird, eine Bildinformation als digitale Information zu speichern, wird die Herausforderung zur Verhinderung von unberechtigtem Kopieren immer wichtiger, um die Besitzer des Urheberrechts zu schützen. Um ein unbe-

rechtigtes Kopieren von digitalen Daten zu verhindern, stehen bei digitalen Aufzeichnungsgeräten und Aufzeichnungsträgern verschiedene Techniken im praktischen Betrieb, die ein unerlaubtes Kopieren verhindern.

[0008] Bei der Herstellung von Informations-Aufzeichnungsträgern, beispielsweise von CDs oder DVDs, benötigt jeder Aufzeichnungsinhalt eine Vielzahl von Funktionseinheiten, beispielweise den Eigentümer des Inhalts, den Herausgeber des Inhalts, einen Plattenhersteller und ein Schlüssel-Verwaltungszentrum (Schlüssel-Ausgabezentrum: KIC) für das Verwalten und die Ausgabe von Schlüsseln für die Verschlüsselung einer notwendige Information, wobei die Information zwischen den Einheiten verteilt und verifiziert wird, um den Informations-Aufzeichnungsträger herzustellen.

[0009] Beispielsweise verifiziert ein Plattenhersteller, der als Plattenherstellungsfirma arbeitet, Daten, die vom Herausgeber des Inhalts geliefert werden, um ein Verfahren für die Aufzeichnung von Daten auf jeder Platte auszuführen. Zusätzlich führt der Plattenhersteller ein Verifizierungsverfahren durch, um zu überprüfen, ob die auf jeder Platte aufgezeichneten Daten mit jenen Daten übereinstimmen, die aufgezeichnet werden sollen. Dieses Verfahren wird aufgrund eines Prüfverfahrens ausgeführt, bei dem Daten, die von jeder aufgezeichneten Platte wiedergegeben werden, mit jenen Daten verglichen werden, die aufgezeichnet werden sollen. Beim oben erwähnten Daten-Verifizierungsverfahren können wiedergegebene Daten undicht sein, die verifiziert werden sollen. Wenn eine Undichtheit bei Daten auftritt, kann der Eigentümer, der die Rechte des Inhalts besitzt, keinen Gewinn machen.

[0010] Im Zusammenhang mit Fig. 1 sollen nunmehr eine typische Plattenherstellung und Datenverifizierung beschrieben werden. Fig. 1 zeigt ein Schlüssel-Verwaltungszentrum (Schlüssel-Ausgabezentrum: KIC) 101, um ein Verfahren für die Verwaltung und die Ausgabe von Schlüsseln auszuführen, eine Inhalt-Bearbeitungseinrichtung 102, beispielsweise ein Studio, um den Inhalt zu bearbeiten, sowie eine Aufzeichnungsträger-Erzeugungseinrichtung 110, die als Plattenherstellungsanlage arbeitet. Die Aufzeichnungsträger-Erzeugungseinrichtung 110 empfängt einen Kodeschlüssel, der vom Schlüssel-Verwaltungszentrum 101 ausgegeben wird, sowie eine den Kodeschlüssel betreffende Information, beispielsweise eine Information über die Erzeugung des Schlüssels, vom Schlüssel-Verwaltungszentrum 101. Zusätzlich empfängt die Aufzeichnungsträger-Erzeugungseinheit 110 den bearbeiteten Inhalt, der auf einer Platte aufgezeichnet werden soll, sowie eine den Inhalt betreffende Information von der Inhalt-Bearbeitungseinrichtung 102.

[0011] In der Aufzeichnungsträger-Erzeugungseinrichtung 110 führt eine Daten-Erzeugungseinheit (Formatierer) 111 ein Verfahren aus, um den Kodeschlüssel und die den Kodeschlüssel betreffende Information, die vom Schlüssel-Verwaltungszentrum 101 empfangen werden, sowie den bearbeiteten Inhalt, der von der Inhalt-Bearbeitungseinrichtung 102 empfangen wird, auf einem Informations-Aufzeichnungsträger (Platte) 112 in einem vorgegebenen Format aufzuzeichnen. Zu diesem Zeitpunkt führt die Daten-Erzeugungseinheit 111, falls dies erforderlich ist, ein Verfahren aus, um den Inhalt unter Verwendung des Kodeschlüssels zu verschlüsseln, der vom Schlüssel-Verwaltungszentrum 101 empfangen wird, und zeichnet die verschlüsselten Daten auf dem Informations-Aufzeichnungsträger 112 auf.

[0012] Der Inhalt sowie verschiedene Informationseinheiten des Kodeschlüssels werden auf jedem Informations-Aufzeichnungsträger aufgezeichnet. Daraufhin führt die Aufzeichnungsträger-Erzeugungseinrichtung 110 ein Verifizierungsverfahren durch, um zu prüfen, ob Daten, die auf dem Informations-Aufzeichnungsträger 112 aufgezeichnet sind, gültig sind. Alle aufgezeichneten Platten oder Stichproben von Platten werden dem Verifizierungsverfahren unterworfen.

[0013] Das Verifizierungsverfahren wird so ausgeführt, dass Daten, die von einer Daten-Wiedergabeeinheit (Abspieleinheit) 113 wiedergeben werden, sowie Daten, die von der Daten-Erzeugungseinheit 111 stammen, d.h. zwei Datenströme, einer Aufzeichnungsträger-Verifizierungseinheit (Plattenprüfstufe) 114 zugeführt werden, um die beiden Datenströme zu vergleichen.

[0014] Beim Ausführen des Verifizierungsverfahrens werden die Daten des Inhalts und der Kodeschlüssel, die vor undichten Stellen geschützt werden sollen, als Daten, die verglichen werden sollen, in einem Datenpfad zwischen der Daten-Erzeugungseinheit 111 und der Aufzeichnungsträger-Verifizierungseinheit 114 sowie zwischen der Daten-Wiedergabeeinheit 113 und der Aufzeichnungsträger-Verifizierungseinheit 114 übertragen. Wenn Daten auf irgendeinem Datenpfad durch ein Abhören ausfließen, kann der Gewinn des Eigentümers, der die Rechte für den Inhalt besitzt, verloren gehen.

ZUSAMMENFASSUNG DER ERFINDUNG

[0015] In Übereinstimmung mit der vorliegenden Erfindung ist es, wenn man die oben erwähnten Umstände betrachtet, erwünscht, dass ein System, ein Verfahren und ein Computerprogramm geliefert werden, um Daten, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind, mit großer Betriebssicherheit sicher verifizieren zu können, wobei die Verifizierung der Daten bei der Erzeugung des Informations-Aufzeichnungsträgers erfolgt, auf dem verschiedene Inhalte aufgezeichnet sind, die im Hinblick auf das Urheberrecht sicher verwaltet werden müssen.

[0016] Gemäß einer Ausführungsform der vorliegenden Erfindung wird ein System für die Verifizierung von Daten geliefert, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind. Das System weist folgende Elemente auf: eine Daten-Wiedergabeeinheit, die Daten wiedergibt, die auf dem Informations-Aufzeichnungsträger aufgezeichnet sind, eine Erzeugungseinheit für Wiedergabe-Verifizierungsdaten, die eine Berechnung durchführt, die auf jenen Daten beruht, die von der Daten-Wiedergabeeinheit wiedergegeben werden, um Wiedergabe-Verifizierungsdaten zu erzeugen, eine Daten-Vergleichseinheit, um die Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten zu vergleichen, die man durch das Ausführen einer Berechnung erhält, die auf Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0017] Gemäß dieser Ausführungsform der vorliegenden Erfindung führt die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten eine Berechnung durch, bei der eine Einwegfunktion auf jene Daten angewandt wird, die vom Informations-Aufzeichnungsträger wiedergegeben werden, um ein Ergebnis der Berechnung als Wiedergabe-Verifizierungsdaten an die Daten-Vergleichseinheit abzugeben. Die Daten-Vergleichseinheit vergleicht die von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugten Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf jene Daten angewandt wird, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0018] Gemäß dieser Ausführungsform der vorliegenden Erfindung gibt die Daten-Wiedergabeeinheit verschlüsselte Daten, die auf dem Informations-Auszeichnungsträger gespeichert sind, an die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten ab. Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten führt eine Berechnung durch, bei der eine Einwegfunktion auf die verschlüsselten Daten angewandt wird, um ein Ergebnis der Berechnung als Wiedergabe-Verifizierungsdaten an die Daten-Vergleichseinheit abzugeben. Die Daten-Vergleichseinheit vergleicht die Wiedergabe-Verifizierungsdaten, die von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugt werden, mit Aufzeichnungs-Verifizierungsdaten, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf verschlüsselte Daten angewandt wird, die in jenen Daten enthalten ist, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0019] Gemäß dieser Ausführungsform der vorliegenden Erfindung weist die Daten-Wiedergabeeinheit weiters eine Daten-Entschlüsselungseinheit auf, um verschlüsselte Daten zu entschlüsseln, die in jenen Daten enthalten sind, die vom Informations-Aufzeichnungsträger wiedergegeben werden. Die Daten-Wiedergabeeinheit gibt unverschlüsselte Daten, die von der Daten-Entschlüsselungseinheit entschlüsselt wurden, an die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten ab. Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten führt eine

Berechnung aus, bei der eine Einwegfunktion an die unverschlüsselten Daten angewandt wird, um ein Ergebnis der Berechnung als Wiedergabe-Verifizierungsdaten an die Daten-Vergleichseinheit abzugeben. Die Daten-Vergleichseinheit vergleicht die Wiedergabe-Verifizierungsdaten, die von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugt werden, mit Aufzeichnungs-Verifizierungsdaten, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf unverschlüsselte Daten angewandt wird, bei denen es sich um jene Originaldaten handelt, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0020] Gemäß dieser Ausführungsform der vorliegenden Erfindung berechnet die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten einen Meldungs-Auswahlkode (message digest code MDC), der auf jenen Daten beruht, die von der Daten-Wiedergabeeinheit wiedergegeben werden. Die Daten-Vergleichseinheit vergleicht den Meldungs-Auswahlkode (MDC), den die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugt, mit einem Meldungs-Auswahlkode (MCD), der auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0021] Gemäß dieser Ausführungsform der vorliegenden Erfindung gibt die Daten-Wiedergabeeinheit Daten, die einen verschlüsselten Inhalt sowie eine Schlüsselinformation aufweisen, vom Informations-Aufzeichnungsträger wieder. Die Daten-Vergleichseinheit verifiziert den Inhalt und die Schlüsselinformation aufgrund von Verifizierungsdaten als Ergebnis einer Berechnung, die auf dem verschlüsselten Inhalt oder dem entschlüsselten Inhalt beruht, sowie von Verifizierungsdaten als Ergebnis einer Berechnung, die auf der Schlüsselinformation beruht.

[0022] Gemäß einer anderen Ausführungsform der vorliegenden Erfindung wird ein Verfahren für die Verifizierung von Daten geliefert, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind. Das Verfahren weist Schritte auf, in denen Daten wiedergegeben werden, die auf dem Informations-Aufzeichnungsträger aufgezeichnet sind, eine Berechnung aufgrund der wiedergegebenen Daten ausgeführt wird, um Wiedergabe-Verifizierungsdaten zu erzeugen, und die Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten verglichen werden, die man durch das Ausführen einer Berechnung erhält, die auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0023] Gemäß dieser Ausführungsform der vorliegenden Erfindung erfolgt eine Berechnung, bei der eine Einwegfunktion auf jene Daten angewandt wird, die vom Informations-Aufzeichnungsträger wiedergegeben werden, um Wiedergabe-Verifizierungsdaten als Ergebnis der Berechnung zu erzeugen, wobei die erzeugten Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten verglichen werden, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf jene Daten angewandt wird, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0024] Gemäß dieser Ausführungsform der vorliegenden Erfindung werden verschlüsselte Daten, die auf dem Informations-Aufzeichnungsträger gespeichert sind, wiedergegeben und abgegeben. Eine Berechnung, bei der eine Einwegfunktion auf die verschlüsselten Daten angewandt wird, wird ausgeführt, um als Ergebnis der Berechnung Wiedergabe-Verifizierungsdaten zu erzeugen. Die erzeugten Wiedergabe-Verifizierungsdaten werden mit Aufzeichnungs-Verifizierungsdaten verglichen, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf verschlüsselte Daten angewandt wird, die in jenen Daten enthalten sind, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0025] Gemäß dieser Ausführungsform der vorliegenden Erfindung weist das Verfahren weiters einen Schritt auf, in dem verschlüsselte Daten entschlüsselt werden, die in jenen Daten enthalten sind, die vom Informations-Aufzeichnungsträger wiedergegeben werden, um unverschlüsselte Daten zu erzeugen. Es erfolgt eine Berechnung, bei der eine Einwegfunktion auf die unverschlüsselten Daten angewandt wird, um als Ergebnis dieser Berechnung Wiedergabe-Verifizierungsdaten zu erzeugen. Die erzeugten Wiedergabe-Verifizierungsdaten werden mit Aufzeichnungs-Verifizierungsdaten verglichen, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf unverschlüsselte Daten angewandt wird, bei denen

es sich um Originaldaten handelt, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0026] Gemäß dieser Ausführungsform der vorliegenden Erfindung wird ein Meldungs-Auswahlkode (MDC) aufgrund der wiedergegebenen Daten berechnet. Der Meldungs-Auswahlkode (MDC) wird mit einem Meldungs-Auswahlkode verglichen, der auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0027] Gemäß dieser Ausführungsform der vorliegenden Erfindung werden Daten, die einen verschlüsselten Inhalt und eine Schlüsselinformation enthalten, vom Informations-Aufzeichnungsträger wiedergegeben. Der Inhalt und die Schlüsselinformation werden aufgrund von Verifizierungsdaten als Ergebnis einer Berechnung, die auf dem verschlüsselten Inhalt oder dem entschlüsselten Inhalt beruht, sowie von Verifizierungsdaten als Ergebnis einer Berechnung verifiziert, die auf der Schlüsselinformation beruhen.

[0028] Gemäß einer noch anderen Ausführungsform der vorliegenden Erfindung wird ein Computerprogramm geliefert, um Daten zu verifizieren, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind. Das Computerprogramm weist Schritte auf, in denen Daten, die auf dem Informations-Aufzeichnungsträger aufgezeichnet sind, wiedergegeben werden, eine Berechnung ausgeführt wird, die auf den wiedergegebenen Daten beruht, um Wiedergabe-Verifizierungsdaten zu erzeugen, und die Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten verglichen werden, die man durch das Ausführen einer Berechnung erhält, die auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

[0029] Das Computerprogramm gemäß dieser Ausführungsform der vorliegenden Erfindung kann beispielsweise für ein Computersystem, das verschiedene Programmkodes ausführen kann, über einen vom Computer lesbaren Aufzeichnungsträger geliefert werden, beispielsweise über eine CD, eine FD oder eine MO oder über ein Kommunikationsmedium, z.B. ein Netzwerk. Das Programm wird in einem vom Computer lesbaren Format geliefert, so dass ein Verfahren gemäß dem Programm am Computersystem ausgeführt werden kann.

[0030] Andere Merkmale und Vorteile der vorliegenden Erfindung werden aus der nun folgenden Beschreibung von bevorzugten Ausführungsformen der Erfindung sowie im Zusammenhang mit den beiliegenden Zeichnungen ersichtlich. Bei der vorliegenden Beschreibung besteht ein System aus einer logischen Reihe von Einheiten. Es ist nicht erforderlich, dass sich diese Einheiten im selben Gehäuse befinden.

[0031] Gemäß der Ausführungsform der vorliegenden Erfindung werden Daten von einem Informations-Aufzeichnungsträger wiedergegeben, eine Berechnung aufgrund der wiedergegebenen Daten durchgeführt, um Wiedergabe-Verifizierungsdaten zu erzeugen, und die erzeugten Daten an die Daten-Vergleichseinheit gelegt. In der Daten-Vergleichseinheit werden die Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten verglichen, die als Ergebnis einer Berechnung zur Verfügung stehen, die auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen. Damit können Daten, die man mit einer Berechnung erhält und die sich vom Inhalt oder der Schlüsselinformation unterscheiden, als Verifizierungsdaten verwendet werden, die an die Daten-Vergleichseinheit gelegt werden sollen. Wenn Verifizierungsdaten undicht werden, kann ein Auslaufen von reellen Daten verhindert werden, beispielsweise vom Inhalt oder der Schlüsselinformation.

[0032] Gemäß der Ausführungsform der vorliegenden Erfindung enthalten Verifizierungsdaten, die an die Daten-Vergleichseinheit gelegt werden, keinen Inhalt und keine Schlüsselinformation sondern Auswahl-Werte, die aufgrund des Inhalts und der Schlüsselinformation berechnet wurden, d.h. Meldungs-Auswahlkodes (MDCs). Wenn MDC-Daten auslaufen, laufen kein Inhalt und keine Schlüsselinformation aus. Damit besteht keine Gefahr eines Ausflusses von Daten, die gesichert werden sollen. Die Daten können in einer Hochsicherheitsumgebung verifiziert werden.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0033] In den Zeichnungen zeigt:

[0034] Fig. 1 das Blockschema des Aufbaus eines herkömmlichen Systems zum Verifizieren von Daten auf einem Informations-Aufzeichnungsträger;

[0035] Fig. 2 ein Schema, in dem ein allgemeiner Weg für die Herstellung eines Informations-Aufzeichnungsträgers sowie Bauteile von Datenzulieferern erläutert werden;

[0036] Fig. 3 ein Blockschema des Aufbaus eines Systems für die Verifizierung von Daten auf einem Informations-Aufzeichnungsträger in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung; und Fig. 4 ein Blockschema des Aufbaus eines Systems für die Verifizierung von Daten auf einem Informations-Aufzeichnungsträger in Übereinstimmung mit einer Abänderung der Ausführungsform.

BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0037] Ein System, ein Verfahren und ein Computerprogramm für das Verifizieren von Daten auf einem Informations-Aufzeichnungsträger sollen nunmehr im Zusammenhang mit den Zeichnungen ausführlich beschrieben werden.

[0038] Ein Verfahren zur Herstellung eines Informations-Aufzeichnungsträgers wird nun kurz beschrieben. Bei einer Ausführungsform, die später beschrieben werden soll, wird ein plattenförmiger Aufzeichnungsträger als Beispiel für den Informations-Aufzeichnungsträger beschrieben. Der Informations-Aufzeichnungsträger, auf den die vorliegende Erfindung angewandt werden kann, ist nicht auf einen plattenförmigen Aufzeichnungsträger beschränkt. Der Träger kann verschiedenartige Informations-Aufzeichnungsträger aufweisen, beispielsweise einen optischen Aufzeichnungsträger, einen Magnet-Aufzeichnungsträger, einen Halbleiter-Aufzeichnungsträge und einen Flash-Speicher.

[0039] Nunmehr wird auf Fig. 2 Bezug genommen. Eine Inhalt-Bearbeitungseinheit (Autorenstudio: AS) 202 bearbeitet den Inhalt, der auf einem Informations-Aufzeichnungsträger gespeichert werden soll. Daraufhin erzeugt eine Aufzeichnungsträger-Erzeugungseinheit (Anlage) 300 in einer Massenfertigung Kopien (Nachbildungen) des Inhalts in Form von CDs oder DVDs, die als Träger dienen, der den Benützern geliefert werden soll, wodurch Informations-Aufzeichnungsträger 200 hergestellt werden. Die Informations-Aufzeichnungsträger 200 werden an die Benützer vertrieben. Jeder Informations-Aufzeichnungsträger 200 wird in einem Informations-Verabreitungsgerät 204 eines Benutzers abgespielt.

[0040] Ein Schlüssel-Verwaltungszentrum (Schlüssel-Ausgabezentrum: KIC) 201 gibt Kodeschlüssel, die bei dieser Plattenherstellung, beim Plattenverkauf und bei der Verwendung der Platte benötigt werden, sowie eine den Schlüssel betreffende Information, beispielsweise eine Schlüssel-Erzeugungsinformation, aus und verwaltet sie. Das Schlüssel-Verwaltungszentrum 201 liefert verschiedene Verwaltungsinformationen für die Inhalt-Bearbeitungseinrichtung 202 sowie für die Aufzeichnungsträger-Erzeugungseinheit 300. Aufgrund der Verwaltungsinformation, die vom Schlüssel-Verwaltungszentrum 201 empfangen wird, bearbeitet die Inhalt-Bearbeitungseinheit 202 den Inhalt und die Aufzeichnungsträger-Erzeugungseinheit 300 verschlüsselt den Inhalt und speichert Daten auf einem Informations- Aufzeichnungsträger. Zusätzlich verwaltet das Schlüssel-Verwaltungszentrum 201 einen Kodeschlüssel und gibt ihn aus, der dazu verwendet wird, um den verschlüsselten Inhalt, der auf dem Informations-Aufzeichnungsträger 200 gespeichert ist, über das Informations-Verarbeitungsgerät 204 des Benutzers zu entschlüsseln.

[0041] Ein Verfahren für die Verifizierung von Daten auf einem Informations-Aufzeichnungsträger gemäß der vorliegenden Erfindung soll nunmehr ausführlich im Zusammenhang mit Fig. 3 beschrieben werden. Fig. 3 zeigt das Schlüssel-Verwaltungszentrum 201, um ein Verfahren zum Verwalten und zur Ausgabe von Schlüsseln durchzuführen, die Inhalt-Bearbeitungseinheit 202, beispielsweise ein Studio, um ein Bearbeitungsverfahren für den Inhalt auszuführen, sowie die Aufzeichnungsträger-Erzeugungseinheit 300, die als Anlage für die Plattenherstellung dient.

Die Aufzeichnungsträger- Erzeugungseinheit 300 empfängt einen Kodeschlüssel sowie eine den Kodeschlüssel betreffende Information, beispielsweise eine Schlüssel-Erzeugungsinformation, vom Schlüssel-Verwaltungszentrum 201 und empfängt weiters den bearbeiteten Inhalt, der auf eine Platte geschrieben werden soll, sowie eine den Inhalt betreffende Information von der Inhalt-Bearbeitungseinheit 202.

[0042] Den Schlüssel betreffende Daten, die vom Schlüssel- Verwaltungszentrum 201 erzeugt und dann an die Aufzeichnungsträger-Erzeugungseinheit 300 gelegt werden, enthalten eine Block-Schlüsselinformation (Erneuerungs- Schlüsselblock: RKB), einen Plattenschlüssel (Kd) für eine Platte, andere Kodeschlüssel sowie eine Schlüssel-Erzeugungsinformation. Die Block-Schlüsselinformation ermöglicht den Erwerb eines Schlüssels aufgrund der Gültigkeit einer Lizenz, die sich auf das Gerät des Benützers bezieht (Informationsverarbeitungs-Gerät) in Übereinstimmung mit einem Information-Verteilungssystem, das beispielsweise wie ein hierarchischer Baum aufgebaut ist. Die oben erwähnten, den Schlüssel betreffenden Daten sollen als Schlüsselinformation [CPKeys.DAT] bezeichnet werden.

[0043] Wenn die Schlüsselinformation [CPKeys.DAT] an die Aufzeichnungsträger-Erzeugungseinheit 300 gelegt wird, fügt das Schlüssel-Verwaltungszentrum 201 zur Schlüsselinformation [CPKeys.DAT] einen Verifizierungswert hinzu. Der Verifizierungswert wird aufgrund der Schlüsselinformation [CPKeys.DAT] erzeugt und dient dazu, um die Schlüsselinformation [CPKeys. DAT] zu verifizieren und zu prüfen, ob die Schlüsselinformation [CPKeys.DAT] manipuliert wurde. Beispielsweise wird ein Meldungs-Auswahlkode (MDC) als Verifizierungskode verwendet. Den MDC erhält man durch das Anwenden einer Einwegfunktion (Hash-Funktion) auf Elementdaten der Schlüsselinformation [CPKeys.DAT]. Beispielsweise wird die SHA-1 Hash-Funktion als Einwegfunktion verwendet. Der Verifizierungswert soll mit [MDC(CPKeys.DAT)] bezeichnet werden.

[0044] Anders ausgedrückt: das Schlüssel-Verwaltungszentrum 201 liefert die Schlüsselinformation [CPKeys.DAT] und den Verifizierungswert [MDC(CPKeys.DAT)] für die Aufzeichnungsträger-Erzeugungseinheit 300.

[0045] Die Aufzeichnungsträger-Erzeugungseinheit 300 berechnet einen neuen Verifizierungswert [MDC' (CPKeys.DAT)] aus der Schlüsselinformation [CPKeys.DAT], die vom Schlüssel-Verwaltungszentrum 201 empfangen wird, wobei sie die Einwegfunktion, beispielsweise die SHA-1 Funktion, verwendet, und vergleicht den berechneten Wert mit dem empfangenen Verifizierungswert [MDC(CPKeys.DAT)]. Wenn die Werte miteinander übereinstimmen, bestimmt die Aufzeichnungsträger-Erzeugungseinheit 300, dass die Schlüsselinformation [CPKeys.DAT], die vom Schlüssel-Verwaltungszentrum 201 empfangen wurde, nicht manipuliert wurde, wobei dies bedeutet, dass die Information gültig ist.

[0046] Zusätzlich liefert die Inhalt-Bearbeitungseinheit 202 einen bearbeiteten Inhalt, der auf eine Platte geschrieben werden soll, sowie eine den Inhalt betreffende Information für die Aufzeichnungsträger-Erzeugungseinheit 300. Daten, die von der Inhalt-Bearbeitungseinheit 202 an die Aufzeichnungsträger-Erzeugungseinheit 300 gelegt werden, enthalten einen Inhalt, beispielsweise sich bewegende Bilddaten, sowie eine Steuerinformation für die Wiedergabe des Inhalts. Der bearbeitete Inhalt und die den Inhalt betreffende Information sollen als Inhaltsinformation [Con.DAT] bezeichnet werden.

[0047] Wenn die Inhaltsinformation [Con.DAT] an die Aufzeichnungsträger-Erzeugungseinheit 300 gelegt wird, fügt die Inhalt-Bearbeitungseinheit 202 zur Inhaltsinformation [Con.DAT] einen Meldungs-Auswahlkode (MDC) als Verifizierungswert hinzu. Der Verifizierungswert dient als Daten, um die Inhaltsinformation [Con.DAT] zu verifizieren, d.h., um zu prüfen, ob die Inhaltsinformation [Con.DAT] manipuliert wurde. Den Verifizierungswert erhält man durch das Anwenden einer Einwegfunktion (Hash-Funktion), die der oben erwähnten Funktion ähnlich ist, auf die Inhaltsinformation [Con.DAT]. Der Verifizierungswert soll als [MDC(Con.DAT)] bezeichnet werden.

[0048] Anders ausgedrückt: die Inhalt-Bearbeitungseinheit 202 legt die Inhaltsinformation

[Con.DAT] und den Verifizierungswert [MDC(Con.DAT)] an die Aufzeichnungsträger-Erzeugungseinheit 300.

[0049] Die Aufzeichnungsträger-Erzeugungseinheit 300 wendet die Einwegfunktion, beispielsweise die SHA-1 Funktion, auf die Inhaltsinformation [Con.DAT] an, die von der Inhalt-Bearbeitungseinheit 202 empfangen wird, um einen neuen Verifizierungswert [MDC' (Con.DAT)] zu erhalten, und vergleicht dann den erhaltenen Wert mit dem empfangenen Verifizierungswert [MDC(Con.DAT)]. Wenn die Werte miteinander übereinstimmen, bestimmt die Aufzeichnungsträger-Erzeugungseinheit 300, dass die Inhaltsinformation [Con.DAT], die von der Inhalt-Bearbeitungseinheit 202 empfangen wurde, nicht manipuliert wurde, wo dies bedeutet, dass die Information gültig ist.

[0050] Wie bereits oben erwähnt wurde, verifiziert die Aufzeichnungsträger-Erzeugungseinheit 300 die vom Schlüssel-Verwaltungszentrum 201 empfangene Information sowie die von der Inhalt-Bearbeitungseinheit 202 empfangene Information aufgrund der entsprechenden Verifizierungswerte. Daraufhin zeichnet die Einheit 300 Daten auf jeder Platte 330 auf.

[0051] Bei der obigen Beschreibung wird nur der Meldungs-Auswahlkode als Verifizierungswert verwendet. Zusätzlich kann eine digitale Unterschrift, beispielsweise in Übereinstimmung mit einem öffentlichen Verschlüsselungssystem, gesetzt werden, so dass die Daten durch eine Verifizierung der Unterschrift verifiziert werden.

[0052] Die gültigen Daten, die mit dem oben beschriebenen Verifizierungsverfahren geprüft wurden, werden in Fig. 3 an eine Daten-Erzeugungseinheit (Formatierer) 310 der Aufzeichnungsträger- Erzeugungseinheit 300 gelegt. In der Daten-Erzeugungseinheit 310 werden beispielsweise der Inhalt unter Verwendung jenes Schlüssels verschlüsselt, den das Schlüssel-Verwaltungszentrum 201 liefert, ein Daten- Formatierprozess ausgeführt und Daten auf jeden Informations-Aufzeichnungsträger 330 (Platte) geschrieben. Es werden nicht nur der Inhalt sondern auch verschiedene Schlüsselinformationen einschließlich des oben erwähnten Erneuerungs-Schlüsselblocks (RKB) auf den Informations-Aufzeichnungsträger 330 geschrieben.

[0053] Zusätzlich führt die Aufzeichnungsträger-Erzeugungseinheit 300 ein Verifizierungsverfahren aus, um festzustellen, ob Daten, die auf jedem Informations-Aufzeichnungsträger 330 aufgezeichnet sind, gültig sind. Alle aufgezeichneten Platten oder Stichproben von Platten werden dem Verifizierungsverfahren unterworfen.

[0054] Das Verifizierungsverfahren wird von einer Aufzeichnungsträger-Verifizierungseinheit 320 ausgeführt. Die Aufzeichnungsträger-Verifizierungseinheit 320 weist eine Daten-Wiedergabeeinheit 321, eine Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322, eine Daten-Vergleichseinheit 323 sowie eine Ergebnis-Ausgabeeinheit 324 auf.

[0055] Die Daten-Wiedergabeeinheit 321 gibt Daten wieder, die auf dem Informations-Aufzeichnungsträger 330 aufgezeichnet wurden. Die wiedergegebenen Daten enthalten den Inhalt und die Schlüsselinformation, die verifiziert werden sollen. Anders ausgedrückt: die wiedergegebenen Daten enthalten die Inhaltsinformation, die der oben erwähnten Inhaltsinformation [Con.DAT] entspricht, sowie die Schlüsselinformation, die der Schlüsselinformation [CPKeys. DAT] entspricht.

[0056] Die beiden Datenelemente, die in den wiedergegebenen Daten enthalten sind, sollen als wiedergegebene verschlüsselte Inhaltsinformation [R-Enc_Con.DAT] und als wiedergegebene Schlüsselinformation [R-CPKeys.DAT] bezeichnet werden. Der Ausdruck "R" zeigt an, dass es sich um wiedergegebene Daten handelt, und der Ausdruck "Enc", dass es sich um verschlüsselte Daten handelt. Die Daten-Erzeugungseinheit 310 verschlüsselt den Inhalt und zeichnet dann den verschlüsselten Inhalt auf dem Informations-Aufzeichnungsträger 330 auf. Bei Daten, die von der Daten-Wiedergabeeinheit (Abspielgerät) 321 wiedergegeben werden, handelt es sich um verschlüsselte Daten. In einigen Fällen gibt es viele Datenelemente, die verifiziert werden sollen. In diesem Fall werden die oben erwähnten beiden Datenelemente einfach als Daten beschrieben, die verifiziert werden sollen.

[0057] Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 empfängt die wiederge-

gebene verschlüsselte Inhaltsinformation [R-Enc Con.DAT] sowie die wiedergegebene Schlüsselinformation [R-CPKeys.DAT] von der Daten-Wiedergabeeinheit 321 und erzeugt Verifizierungsdaten.

[0058] Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 führt eine Berechnung aufgrund der wiedergegebenen Daten aus, um Wiedergabe-Verifizierungsdaten zu erzeugen. Im Besonderen berechnet die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 für die wiedergegebene verschlüsselte Inhaltsinformation [R-Enc_Con.DAT] einen Verifizierungswert [MDC(R-Enc_Con.DAT)] aus der wiedergegebenen verschlüsselten Inhaltsinformation [R-Enc_Con.DAT] unter Verwendung der Einwegfunktion, beispielsweise der SHA-1 Funktion, und legt dann den berechneten Wert als Inhalts-Verifizierungswert an die Daten-Vergleichseinheit 323. Zusätzlich berechnet die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 für die wiedergegebene Schlüsselinformation [R-CPKeys.DAT] einen Verifizierungswert [MDC(R-CPKeys.DAT)] aus der wiedergegebenen Schlüsselinformation [R-CPKeys.DAT] unter Verwendung der Einwegfunktion, beispielsweise der SHA-1 Funktion, und legt dann den berechneten Wert als Schlüsselinformations-Verifizierungswert an die Daten-Vergleichseinheit 323.

[0059] Die Daten-Vergleichseinheit 323 führt einen Prüfvorgang aus, in dem jeder Verifizierungswert, der von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 stammt, mit dem entsprechenden Wert verglichen wird, den man von einer Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 der Daten-Erzeugungseinheit 310 erhält.

[0060] In der Daten-Erzeugungseinheit 310 erzeugt die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 Verifizierungsdaten, die auf einer Information beruhen, die auf dem Informations-Aufzeichnungsträger 330 aufgezeichnet werden soll, wobei es sich um eine verschlüsselte Inhaltsinformation [Enc_Con.DAT], die aufgezeichnet werden soll, sowie die Schlüsselinformation [CPKeys.DAT] handelt, die aufgezeichnet werden soll.

[0061] Für die verschlüsselte Inhaltsinformation [Enc_Con.DAT], die aufgezeichnet werden soll, wendet die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 die Einwegfunktion, beispielsweise die SHA-1 Funktion, auf die verschlüsselte Inhaltsinformation [Enc_Con.DAT] an, die aufgezeichnet werden soll, wodurch man einen Verifizierungswert [MDC(Enc_Con.DAT)] erhält. Daraufhin legt die Einheit 311 den erhaltenen Wert als Inhalts-Verifizierungswert an die Daten-Vergleichseinheit 323. Zusätzlich wendet die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 für die Schlüsselinformation [CPKeys.DAT], die aufgezeichnet werden soll, die Einwegfunktion, beispielsweise die SHA-1 Funktion, auf die Schlüsselinformation [CPKeys.DAT] an, die aufgezeichnet werden soll, wodurch man einen Verifizierungswert [MDC(CPKeys.DAT)] erhält. Daraufhin legt die Einheit 311 den erhaltenen Wert als Schlüsselinformations-Verifizierungswert an die Daten-Vergleichseinheit 323 .

[0062] Wie bereits oben erwähnt, legt das Schlüssel-Verwaltungszentrum 201 die Schlüsselinformation [CPKeys.DAT] und den Verifizierungswert [MDC(CPKeys.DAT)] an die Aufzeichnungsträger-Erzeugungseinheit 300. Wenn die Aufzeichnungsträger-Erzeugungseinheit 300 bereits den Verifizierungswert [MDC(CPKeys.DAT)] besitzt, muss die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 keine neuen Verifizierungsdaten erzeugen. Die vorhandenen Daten können als Verifizierungswert an die Daten-Vergleichseinheit 323 gelegt werden.

[0063] Die Daten-Vergleichseinheit 323 führt den Prüfvorgang aus, in dem jeder Verifizierungswert, der von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 geliefert wird, mit dem entsprechenden Wert verglichen wird, der von der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 der Daten-Erzeugungseinheit 310 stammt.

[0064] Anders ausgedrückt: für den Inhalt wird der Verifizierungswert [MDC(R-Enc_Con.DAT)], der von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 geliefert wird, mit dem Verifizierungswert [MDC(Enc_Con.DAT)] verglichen, der von der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 stammt. Wenn die Werte miteinander übereinstimmen, stellt die Daten-Vergleichseinheit 323 fest, dass die wiedergegebenen Daten mit jenen Daten übereinstimmen, die aufgezeichnet werden sollen, und gültige Daten aufgezeichnet werden,

worauf sie ein Ergebnis der Feststellung zur Ergebnis-Ausgabeeinheit 324 ausgibt.

[0065] Was die Schlüsselinformation betrifft, so vergleicht die Daten-Vergleichseinheit 323 den Verifizierungswert [MDC(R-CPKeys.DAT)], den die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 liefert, mit dem Verifizierungswert [MDC(CPKeys.DAT)], der von der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 stammt. Wenn die Werte miteinander übereinstimmen, stellt die Daten-Vergleichseinheit 323 fest, dass wiedergegebene Daten mit Daten übereinstimmen, die aufgezeichnet werden sollen, und gültige Daten aufgezeichnet werden. Die Daten-Vergleichseinheit 323 gibt ein Ergebnis der Feststellung an die Ergebnis-Ausgabeeinheit 324 ab.

[0066] Beim Aufbau gemäß der vorliegenden Ausführungsform enthalten Daten, die von der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 der Daten-Erzeugungseinheit 310 zur Aufzeichnungsträger-Verifizierungseinheit 320 über einen Daten-Übertragungspfad übertragen werden, keine Inhalts- und Schlüsselinformation, sondern Auswahlwerte, die aufgrund des Inhalts und der Schlüsselinformation berechnet werden, d.h. MDCs (Meldungs-Auswahlkodes). Wenn die MDC-Daten auslaufen, laufen der Inhalt und die Schlüsselinformation nicht aus. Es besteht daher keine Gefahr, dass Daten auslaufen, die gesichert werden sollen. Zusätzlich wird ein Auslaufen von Daten verhindert, solange ein Übertragungspfad von der Daten-Wiedergabeeinheit 321 zur Daten-Vergleichseinheit 323 geschlossen ist, um einen Zugriff von außen zu blockieren. Dadurch können die Daten in einer Hochsicherheitsumgebung verifiziert werden.

[0067] Bei dem in Fig. 3 gezeigten Aufbau gemäß der Ausführungsform weist die Aufzeichnungsträger-Verifizierungseinheit 320 vier Bauelemente auf, d.h. die Daten-Wiedergabeeinheit 321, die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322, die Daten-Vergleichseinheit 323 und die Ergebnis-Ausgabeeinheit 324. Bei den Ausgangsdaten der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 handelt es sich um MDC-Daten. Wenn MDC-Daten auslaufen, stellt dies kein Problem dar. Solange der Pfad zwischen der Daten-Wiedergabeeinheit 321 und der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322 gegen einen Zugriff von außen geschützt ist, wird die Sicherheit gewährleistet. Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 322, die Daten-Vergleichseinheit 323 und die Ergebnis-Ausgabeeinheit 324 können über einen typischen Daten-Übertragungspfad verbunden werden, ähnlich dem in der Verbindung zwischen der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 311 und der Daten-Vergleichseinheit 323.

[0068] In Übereinstimmung mit einer Abänderung der Ausführungsform der vorliegenden Erfindung kann das System so aufgebaut werden, dass eine Daten-Wiedergabeeinheit in einer Aufzeichnungsträger-Verifizierungseinheit, aufgrund von entschlüsselten Daten, die von der Daten-Wiedergabeeinheit geliefert werden, nicht nur einen Daten-Wiedergabevorgang, sondern auch einen Daten-Entschlüsselungsvorgang ausführt, wobei die Daten für einen Vergleich dienen. Die Abänderung soll nunmehr im Zusammenhang mit Fig. 4 beschrieben werden.

[0069] Nunmehr soll auf Fig. 4 Bezug genommen werden. In einer Aufzeichnungsträger-Erzeugungseinrichtung führt eine Daten-Erzeugungseinheit (Formatierer) 410 ein Inhalts-Verschlüsselungsverfahren unter Verwendung eines Schlüssels, der beispielsweise von einem Schlüssel-Verwaltungszentrum geliefert wird, sowie einen Daten-Formatierungsprozess aus, wodurch Daten auf einem Informations-Aufzeichnungsträger (Platte) 430 aufgezeichnet werden. Der Inhalt und verschiedene Schlüsselinformationen, beispielsweise ein Erneuerungs-Schlüsselblock (RKB), wie er oben beschrieben wurde, werden auf dem Informations-Aufzeichnungsträger 430 aufgezeichnet.

[0070] Eine Aufzeichnungsträger-Verifizierungseinheit 420 führt ein Daten-Verifizierungsverfahren durch. Die Aufzeichnungsträger-Verifizierungseinheit 420 enthält eine Daten-Wiedergabeeinheit 421, eine Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423, eine Vergleichseinheit 424 sowie eine Ergebnis-Ausgabeeinheit 425.

[0071] Die Daten-Wiedergabeeinheit (Abspielgerät) 421 besitzt eine Daten-Entschlüsselungs-

einheit 422, um ein Verfahren zum Entschlüsseln von wiedergegebenen verschlüsselten Daten auszuführen. Die Daten-Wiedergabeeinheit 421 gibt Daten wieder, die auf dem Informations-Aufzeichnungsträger 430 aufgezeichnet sind. Die Daten-Entschlüsselungseinheit 422 entschlüsselt die wiedergegebenen Daten, die verschlüsselt sind, und gibt dann die entschlüsselten Daten, d.h. unverschlüsselte Daten, an die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 ab. Die Ausgangsdaten enthalten einen Inhalt und die Schlüsselinformation, die dem Verifizierungsvorgang unterworfen werden, beispielsweise die Inhaltsinformation und die Schlüsselinformation.

[0072] Die Daten-Wiedergabeeinheit 421 erzeugt zwei Ausgangs-Datenelemente, d.h. die wiedergegebene Inhaltsinformation [R-Con.DAT] und die wiedergegebene Schlüsselinformation [R-CPKeys.DAT]. Der Ausdruck "R" bedeutet dabei, dass es sich um wiedergegebene Daten handelt.

[0073] Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 empfängt die wiedergegebene Inhaltsinformation [R-Con.DAT] sowie die wiedergegebene Schlüsselinformation [R-CPKeys.DAT] und erzeugt Verifizierungsdaten.

[0074] Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 führt eine Berechnung aufgrund der wiedergegebenen Daten durch, um Wiedergabe-Verifizierungsdaten zu erzeugen. Im Besonderen berechnet die Erzeugungseinheit für Wiedergabe- Verifizierungsdaten 423 einen Verifizierungswert [MDC(R- Con.DAT)] aufgrund der wiedergegebenen Inhaltsinformation [R- Con.DAT] unter Verwendung der Einwegfunktion, beispielsweise der SHA-1 Funktion, und legt dann den berechneten Wert als Inhalts-Verifizierungswert an die Daten-Vergleichseinheit 424. Zusätzlich berechnet die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 einen Verifizierungswert [MDC(R- CPKeys.DAT)] aus der wiedergegebenen Schlüsselinformation [R-CPKeys.DAT] unter Verwendung der Einwegfunktion, beispielsweise der SHA-1 Funktion, und legt dann den berechneten Wert als Schlüsselinformations-Verifizierungswert an die Daten-Vergleichseinheit 424.

[0075] Die Daten-Vergleichseinheit 424 führt einen Prüfvorgang aus, in dem jeder Verifizierungswert, der von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 geliefert wird, mit dem entsprechenden Wert verglichen wird, der von einer Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 in der Daten-Erzeugungseinheit 410 stammt.

[0076] Die Daten-Erzeugungseinheit 410 zeichnet den verschlüsselten Inhalt [Enc_Con.DAT] auf dem Informations-Aufzeichnungsträger 430 auf. Die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 erzeugt Verifizierungsdaten aufgrund einer unverschlüsselten Inhaltsinformation, die noch nicht verschlüsselt wurde.

[0077] Die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 berechnet einen Verifizierungswert [MDC(Con.DAT)] aufgrund einer Inhaltsinformation [Con.DAT] unter Verwendung der Einwegfunktion, beispielsweise der SHA-1 Funktion, und legt dann den berechneten Wert als Inhalt-Verifizierungswert an die Daten-Vergleichseinheit 424. Zusätzlich berechnet die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 einen Verifizierungswert [MDC (CPKeys.DAT)] aus der Schlüsselinformation [CPKeys.DAT], die aufgezeichnet werden soll, unter Verwendung der Einwegfunktion, beispielsweise der SHA-1 Funktion, und legt dann den berechneten Wert als Schlüsselinformations-Verifizierungswert an die Daten-Vergleichseinheit 424.

[0078] Wie bereits oben erwähnt, liefern ein Schlüssel- Verwaltungszentrum und eine Inhalts-Bearbeitungseinrichtung Verifizierungswerte (MDCs), die sich auf Daten beziehen, die zusätzlich zu den gelieferten Daten an die Aufzeichnungsträger-Erzeugungseinrichtung gelegt werden sollen. Die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 kann die gelieferten Verifizierungswerte an die Daten-Vergleichseinheit 424 legen, ohne neue Verifizierungsdaten zu erzeugen.

[0079] Die Daten-Vergleichseinheit 424 führt einen Prüfvorgang aus, in dem jeder Verifizierungswert, den die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 liefert, mit dem

entsprechenden Wert verglichen wird, den die Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 der Daten-Erzeugungseinheit 410 liefert.

[0080] Anders ausgedrückt: im Hinblick auf den Inhalt vergleicht die Daten-Vergleichseinheit 424 den Verifizierungswert [MDC(R-Con.DAT)], den die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 liefert, mit dem Verifizierungswert [MDC(Con.DAT)], der von der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 stammt. Wenn die Werte miteinander übereinstimmen, stellt die Daten-Vergleichseinheit 424 fest, dass die wiedergegebenen Daten mit jenen Daten übereinstimmen, die aufgezeichnet werden sollen, und gültige Daten aufgezeichnet werden, und legt dann das Ergebnis der Feststellung an die Ergebnis-Ausgabeeinheit 425.

[0081] Zusätzlich vergleicht die Daten-Vergleichseinheit 424 für die Schlüsselinformation den Verifizierungswert [MDC(R-CPKeys.DAT)], den die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 liefert, mit dem Verifizierungswert [MDC(CPKeys.DAT)], der von der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 stammt. Wenn die Werte miteinander übereinstimmen, stellt die Daten-Vergleichseinheit 424 fest, dass die wiedergegebenen Daten mit jenen Daten übereinstimmen, die aufgezeichnet werden sollen, und gültige Daten aufgezeichnet werden, worauf sie das Ergebnis der Feststellung an die Ergebnis-Ausgabeeinheit 425 legt.

[0082] Beim oben beschriebenen Aufbau gemäß der Abänderung der Ausführungsform enthalten Daten, die über einen Daten-Übertragungspfad zwischen der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 der Daten-Erzeugungseinheit 410 zur Aufzeichnungsträger-Verifizierungseinheit 420 übertragen werden, keinen Inhalt und keine Schlüsselinformation, sondern Auswahlwerte, d.h. MDCs (Meldungs-Auswahlkodes), die aufgrund des Inhalts und der Schlüsselinformation berechnet wurden. Wenn die MDC-Daten auslaufen, laufen der Inhalt die Schlüsselinformation nicht aus. Damit besteht keine Gefahr, dass Daten auslaufen, die gesichert werden sollen. Solange ein Übertragungspfad von der Daten-Wiedergabeeinheit 421 zur Daten-Vergleichseinheit 424 geschlossen ist, um einen Zugriff von außen zu blockieren, wird ein Auslaufen von Daten verhindert. Damit können Daten in einer Hochsicherheitsumgebung verifiziert werden.

[0083] Bei dem in Fig. 4 gezeigten Aufbau gemäß der Abänderung der Ausführungsform enthält die Aufzeichnungsträger-Verifizierungseinheit 420 vier Bauelemente, d.h. die Daten-Wiedergabeeinheit 421, die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423, die Daten-Vergleichseinheit 424 und die Ergebnis-Ausgabeeinheit 425. Bei den Ausgangsdaten der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 handelt es sich um MDC-Daten. Wenn MDC-Daten auslaufen, stellt dies kein Problem dar. Solange der Pfad zwischen der Daten-Wiedergabeeinheit 421 und der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423 gegen einen Zugriff von außen geschützt ist, ist die Sicherheit gewährleistet. Die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten 423, die Daten-Vergleichseinheit 424 und die Ergebnis-Ausgabeeinheit 425 können über einen typischen Daten-Übertragungspfad verbunden werden, ähnlich dem in der Verbindung zwischen der Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten 411 und der Daten-Vergleichseinheit 424.

[0084] Wie bereits oben erwähnt, wurde die vorliegende Erfindung im Zusammenhang mit der bevorzugten Ausführungsform ausführlich beschrieben. Es ist ersichtlich, dass verschiedene Abänderungen, Kombinationen, Unterkombinationen und Veränderungen von Fachleuten vorgenommen werden können, ohne dadurch vom Geist oder Gebiet der Erfindung abzuweichen. Anders ausgedrückt: es ist ersichtlich, dass die Erfindung nicht auf die bestimmte Ausführungsform beschränkt ist, mit Ausnahme der Festlegung in den angeschlossenen Ansprüchen.

[0085] Eine Reihe von Vorgängen, die in der Beschreibung erläutert wurden, können von einer Hardware, einer Software oder einer Zusammensetzung von diesen ausgeführt werden. Wenn die Vorgänge von einer Software ausgeführt werden, kann ein Programm, das eine Prozessfolge aufweist, in einem Speicher in einem Computer, in dem eine spezielle Hardware installiert ist, installiert und dann ausgeführt werden. Andererseits kann das Programm auf einem All-

zweck-Rechner, der verschiedene Prozesse ausführen kann, installiert und dann ausgeführt werden.

[0086] Beispielsweise kann das Programm vorher auf einer Festplatte oder auf einem nur auslesbaren Speicher (read only memory ROM) aufgezeichnet werden, der als Aufzeichnungsträger dient. Andererseits kann das Programm vorübergehend oder dauernd auf einem austauschbaren Aufzeichnungsträger gespeichert (aufgezeichnet) werden, beispielsweise auf einer Diskette, einem nur auslesbaren Compactdisc-Speicher (CD-ROM), einer magnetooptischen (MO) Platte, einer DVD, einer Magnetplatte oder auf einem Halbleiterspeicher. Der austauschbare Aufzeichnungsträger kann als Softwarepaket geliefert werden.

[0087] Das auf dem oben erwähnten austauschbaren Aufzeichnungsträger aufgezeichnete Programm kann in einem Computer installiert werden. Zusätzlich kann das Programm von einer heruntergeladenen Site zu einem Computer über Funk oder über ein Netzwerk übertragen werden, beispielsweise über ein lokales Netz (local area network LAN) oder das Internet. Im Computer kann das übertragene Programm empfangen und auf einem Aufzeichnungsträger installiert werden, beispielweise auf einer eingebauten Festplatte.

[0088] Verschiedene Prozesse, die in der Beschreibung erläutert wurden, werden in der oben beschriebenen Reihenfolge zeitseriell ausgeführt. Die Prozesse können weiters gleichzeitig oder individuell ausgeführt werden, wie dies notwendig ist, oder in Abhängigkeit vom Durchsatz eines Systems, das die Prozesse ausführt. In der Beschreibung handelt es sich beim System um eine logische Reihe von Einheiten. Es ist nicht notwendig, dass sich die Einheiten im selben Gehäuse befinden.

Patentansprüche

1. System zum Verifizieren von Daten, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind, wobei das System enthält:
   eine Daten-Wiedergabeeinheit, um Daten wiederzugeben, die auf dem Informations-Aufzeichnungsträger aufgezeichnet sind;
   eine Erzeugungseinheit für Wiedergabe-Verifizierungsdaten, um eine Berechnung aufgrund jener Daten durchzuführen, die von der Daten-Wiedergabeeinheit wiedergegeben werden, um Wiedergabe-Verifizierungsdaten zu erzeugen; und eine Daten-Vergleichseinheit, um die Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten zu vergleichen, die man durch das Ausführen einer Berechnung erhält, die auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

2. System gemäß Anspruch 1, wobei
   die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten eine Berechnung durchführt, bei der eine Einwegfunktion auf jene Daten angewandt wird, die vom Informations-Aufzeichnungsträger wiedergegeben werden, um ein Ergebnis der Berechnung als Wiedergabe-Verifizierungsdaten an die Daten-Vergleichseinheit abzugeben, und
   die Daten-Vergleichseinheit die Wiedergabe-Verifizierungsdaten, die von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugt werden, mit Aufzeichnungs-Verifizierungsdaten vergleicht, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf jene Daten angewandt wird, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

3. System gemäß Anspruch 1, wobei
   die Daten-Wiedergabeeinheit an die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten verschlüsselte Daten abgibt, die auf dem Informations-Aufzeichnungsträger gespeichert sind, die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten eine Berechnung ausführt, bei der eine Einwegfunktion auf die verschlüsselten Daten angewandt wird, um ein Ergebnis der Berechnung als Wiedergabe-Verifizierungsdaten an die Daten-Vergleichseinheit abzugeben, und
   die Daten-Vergleichseinheit die von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugten Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten

vergleicht, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf verschlüsselte Daten angewandt wird, die in jenen Daten enthalten sind, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

4. System gemäß Anspruch 1, wobei
die Daten-Wiedergabeeinheit weiters eine Daten-Entschlüsselungseinheit aufweist, um verschlüsselte Daten zu entschlüsseln, die in jenen Daten enthalten sind, die vom Informations-Aufzeichnungsträger wiedergegeben werden, die Daten-Wiedergabeeinheit unverschlüsselte Daten an die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten abgibt, die von der Daten-Entschlüsselungseinheit entschlüsselt wurden,
die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten eine Berechnung ausführt, bei der eine Einwegfunktion auf die unverschlüsselten Daten angewandt wird, um ein Ergebnis der Berechnung als Wiedergabe-Verifizierungsdaten an die Daten-Vergleichseinheit abzugeben, und die Daten-Vergleichseinheit die Wiedergabe-Verifizierungsdaten, die von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugt werden, mit Aufzeichnungs-Verifizierungsdaten vergleicht, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf unverschlüsselte Daten angewandt wird, bei denen es sich um Originaldaten handelt, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

5. System gemäß Anspruch 1, wobei
die Erzeugungseinheit für Wiedergabe-Verifizierungsdaten einen Meldungs-Auswahlkode (MDC) berechnet, der auf jenen Daten beruht, die von der Daten-Wiedergabeeinheit wiedergegeben werden, und
die Daten-Vergleichseinheit den Meldungs-Auswahlkode (MDC), der von der Erzeugungseinheit für Wiedergabe-Verifizierungsdaten erzeugt wird, mit einem Meldungs-Auswahlkode (MDC) vergleicht, der auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

6. System gemäß Anspruch 1, wobei
die Daten-Wiedergabeeinheit vom Informations-Aufzeichnungsträger Daten wiedergibt, die einen verschlüsselten Inhalt und eine Schlüsselinformation enthalten, und
die Daten-Vergleichseinheit den Inhalt und die Schlüsselinformation aufgrund von Verifizierungsdaten, die ein Ergebnis einer Berechnung sind, die auf dem verschlüsselten Inhalt oder dem entschlüsselten Inhalt beruht, sowie Verifizierungsdaten verifiziert, die ein Ergebnis einer Berechnung sind, die auf der Schlüsselinformation beruht.

7. Verfahren zum Verifizieren von Daten, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind, wobei das Verfahren folgende Schritte enthält:
Wiedergeben von Daten, die auf dem Informations-Aufzeichnungsträger aufgezeichnet sind;
Ausführen einer Berechnung, die auf den wiedergegebenen Daten beruht, um Wiedergabe-Verifizierungsdaten zu erzeugen; und
Vergleichen der Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten, die man durch das Ausführen einer Berechnung erhält, die auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

8. Verfahren gemäß Anspruch 7, wobei eine Berechnung durchgeführt wird, bei der eine Einwegfunktion auf jene Daten angewandt wird, die vom Informations-Aufzeichnungsträger wiedergegeben werden, um als Ergebnis der Berechnung Wiedergabe-Verifizierungsdaten zu erzeugen, und
die erzeugten Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten verglichen werden, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf jene Daten angewandt wird, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

9. Verfahren gemäß Anspruch 7, wobei
verschlüsselte Daten, die auf dem Informations-Aufzeichnungsträger gespeichert sind, wiedergegeben und abgegeben werden,
eine Berechnung ausgeführt wird, bei der eine Einwegfunktion auf die verschlüsselten Daten angewandt wird, um als Ergebnis der Berechnung Wiedergabe-Verifizierungsdaten zu erzeugen, und
die erzeugten Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten verglichen werden, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf verschlüsselte Daten angewandt wird, die in jenen Daten enthalten sind, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

10. Verfahren gemäß Anspruch 7, wobei das Verfahren weiters folgenden Schritt enthält:
Entschlüsseln von verschlüsselten Daten, die in jenen Daten enthalten sind, die vom Informations-Aufzeichnungsträger wiedergegeben werden, um unverschlüsselte Daten zu erzeugen, wobei
eine Berechnung ausgeführt wird, bei der eine Einwegfunktion auf die unverschlüsselten Daten angewandt wird, um als Ergebnis der Berechnung Wiedergabe-Verifizierungsdaten zu erzeugen, und
die erzeugten Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten verglichen werden, die als Ergebnis einer Berechnung zur Verfügung stehen, bei der die Einwegfunktion auf unverschlüsselte Daten angewandt wird, bei denen es sich um Originaldaten handelt, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

11. Verfahren gemäß Anspruch 7, wobei
ein Meldungs-Auswahlkode (MDC) aufgrund der wiedergegebenen Daten berechnet wird, und
der Meldungs-Auswahlkode (MDC) mit einem Meldungs-Auswahlkode (MDC) verglichen wird, der auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

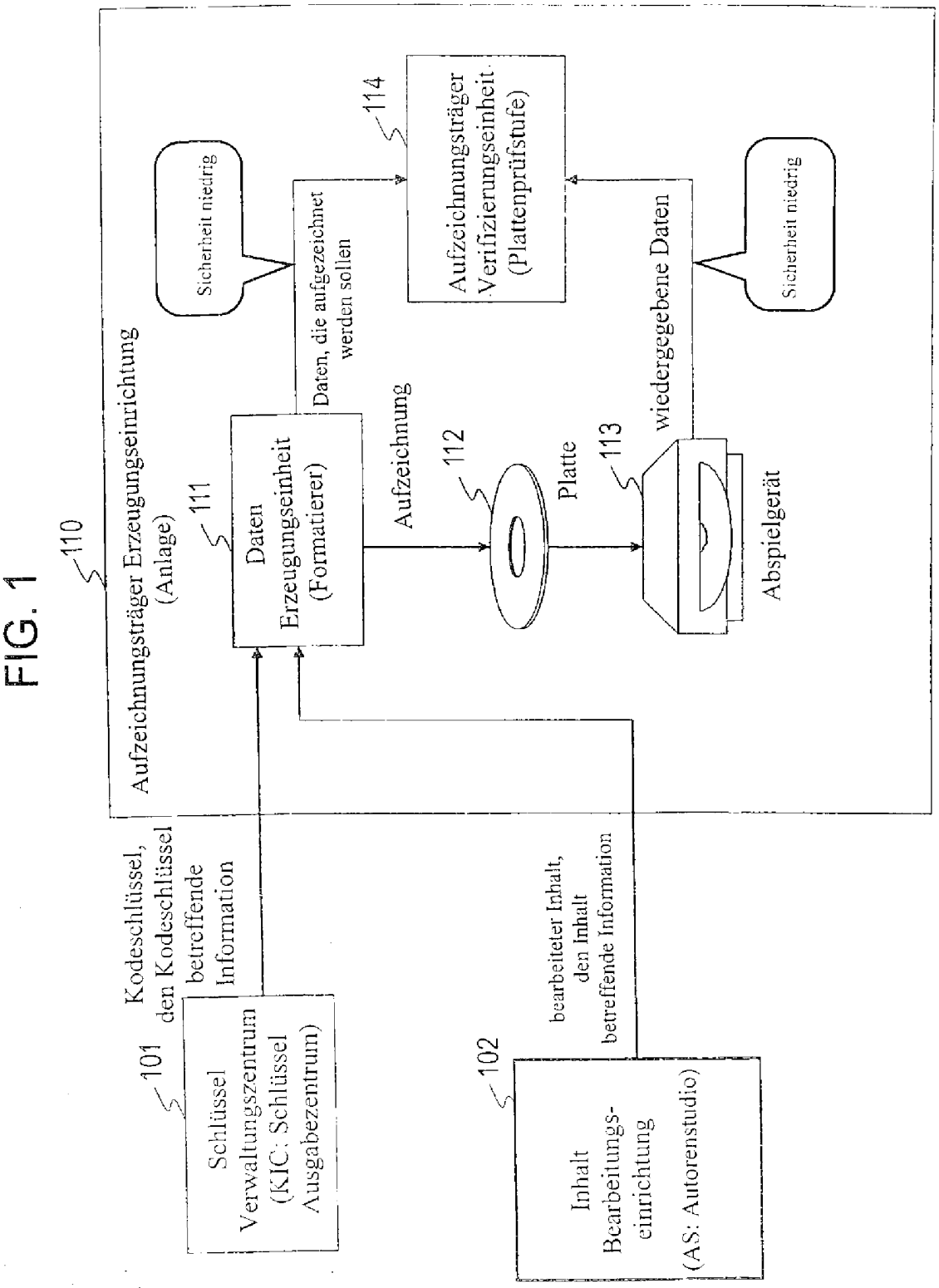
12. Verfahren gemäß Anspruch 7, wobei
Daten, die einen verschlüsselten Inhalt sowie eine Schlüsselinformation enthalten, vom Informations-Aufzeichnungsträger wiedergegeben werden, und der Inhalt und die Schlüsselinformation aufgrund von Verifizierungsdaten, die ein Ergebnis einer Berechnung sind, die auf dem verschlüsselten Inhalt oder dem entschlüsselten Inhalt beruht, sowie von Verifizierungsdaten verifiziert werden, die ein Ergebnis einer Berechnung sind, die auf der Schlüsselinformation beruht.

13. Computerprogramm für die Verifizierung von Daten, die auf einem Informations-Aufzeichnungsträger aufgezeichnet sind, wobei das Programm folgende Schritte enthält:
Wiedergeben von Daten, die auf dem Informations-Aufzeichnungsträger aufgezeichnet sind;
Ausführen einer Berechnung, die auf den wiedergegebenen Daten beruht, um Wiedergabe-Verifizierungsdaten zu erzeugen, und
Vergleichen der Wiedergabe-Verifizierungsdaten mit Aufzeichnungs-Verifizierungsdaten, die man durch das Ausführen einer Berechnung erhält, die auf jenen Daten beruht, die auf dem Informations-Aufzeichnungsträger aufgezeichnet werden sollen.

Hierzu 4 Blatt Zeichnungen

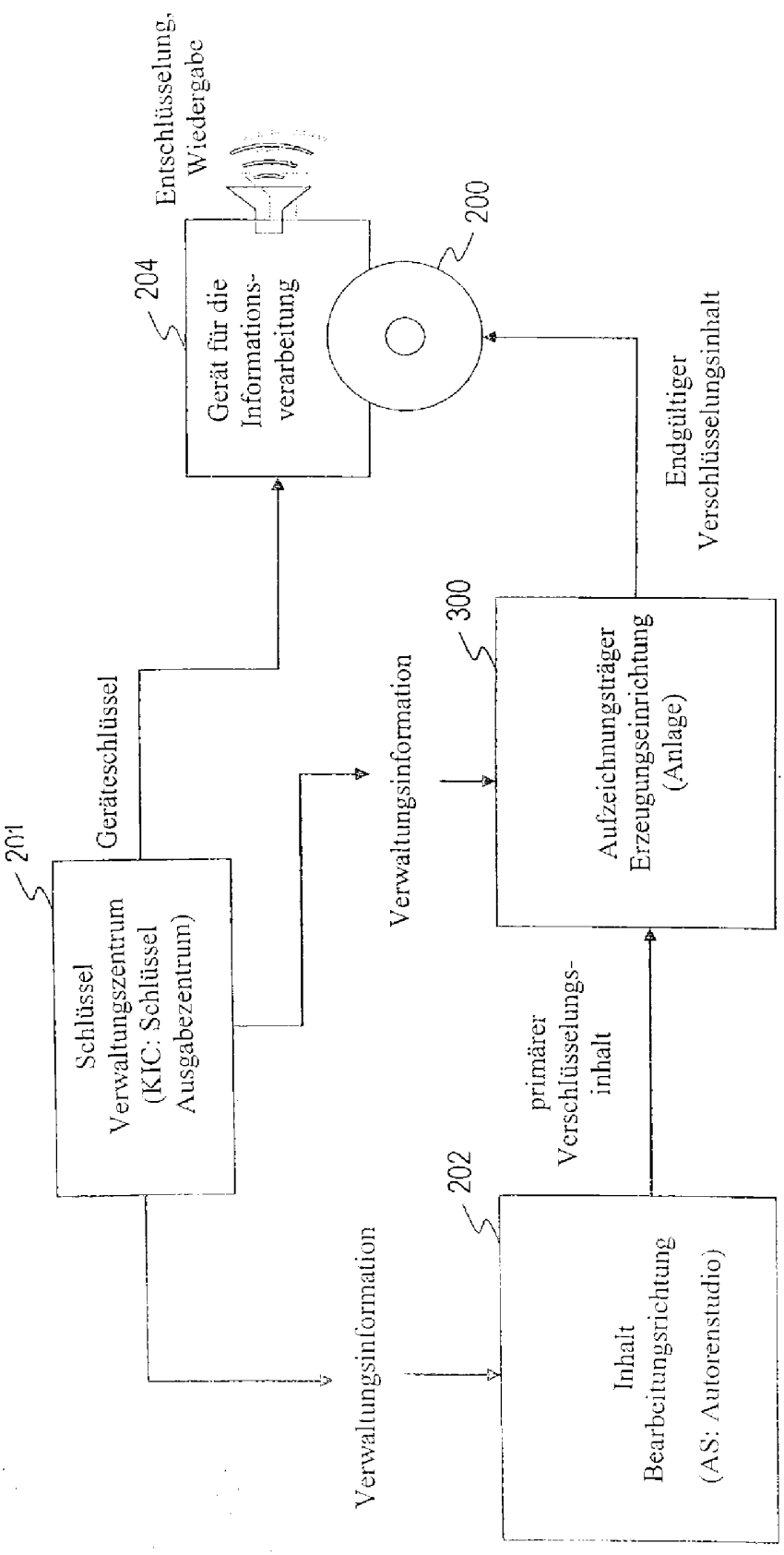
1 / 4

FIG. 1


Aufzeichnungsträger Erzeugungseinrichtung (Anlage)
110
Daten Erzeugungseinheit (Formatierer)
111
Daten, die aufgezeichnet werden sollen
Sicherheit niedrig
Aufzeichnung
112
Platte
113
Aufzeichnungsträger Verifizierungseinheit (Plattenprüfstufe)
114
wiedergegebene Daten
Sicherheit niedrig
Abspielgerät
Kodeschlüssel, den Kodeschlüssel betreffende Information
Schlüssel Verwaltungszentrum (KJC: Schlüssel Ausgabezentrum)
101
bearbeiteter Inhalt, den Inhalt betreffende Information
Inhalt Bearbeitungs-einrichtung (AS: Autorenstudio)
102

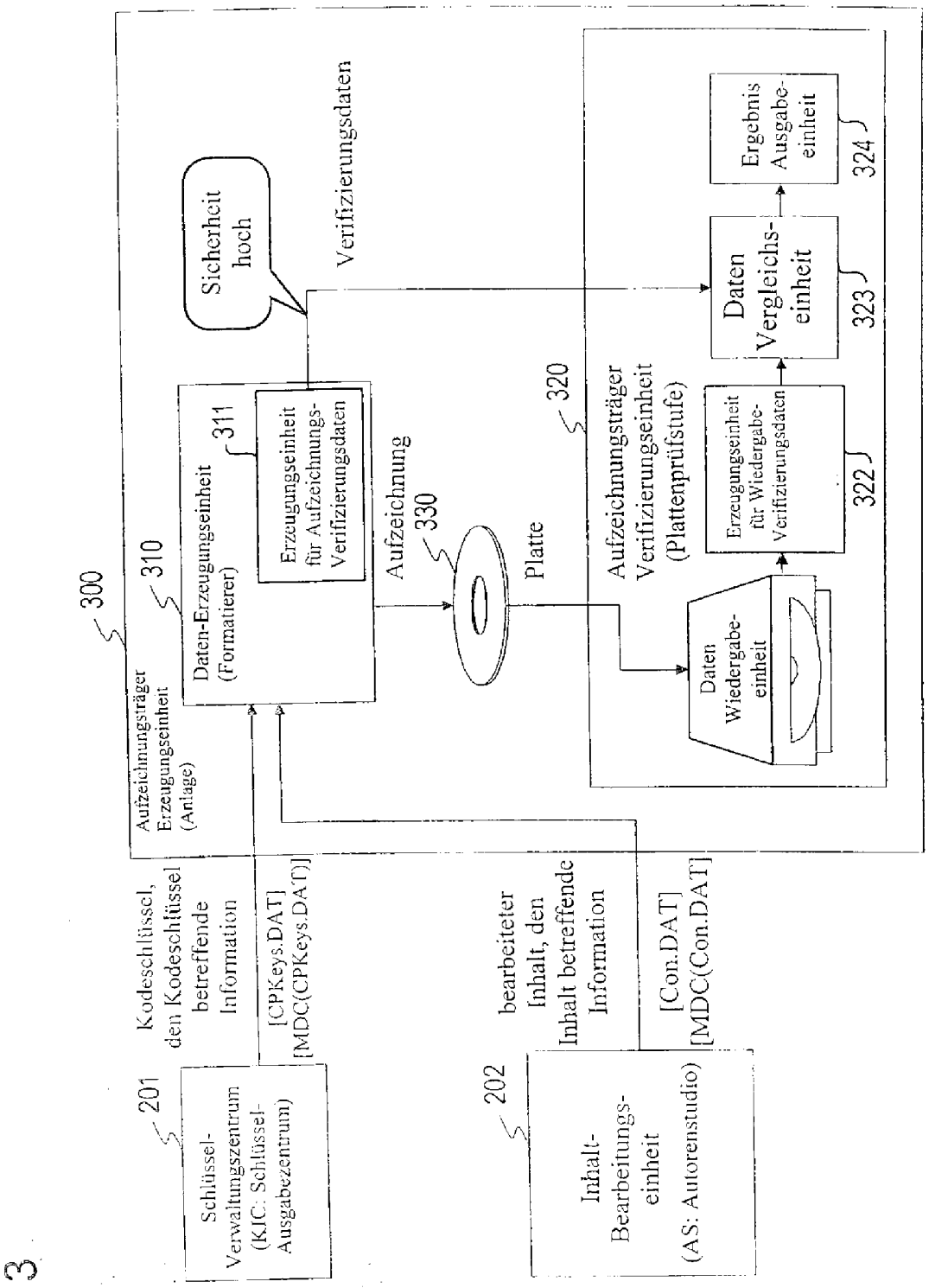
2 / 4

FIG. 2


Entschlüsselung, Wiedergabe
204
Gerät für die Informations-verarbeitung
200
Endgültiger Verschlüsselungsinhalt
300
Aufzeichnungsträger Erzeugungseinrichtung (Anlage)
Verwaltungsinformation
201
Schlüssel Verwaltungszentrum (KIC: Schlüssel Ausgabezentrum)
Geräteschlüssel
primärer Verschlüsselungs-inhalt
202
Inhalt Bearbeitungsrichtung (AS: Autorenstudio)
Verwaltungsinformation

3 / 4

FIG. 3


300
Aufzeichnungsträger Erzeugungseinheit (Anlage)
310
Daten-Erzeugungseinheit (Formatierer)
311
Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten
Aufzeichnung
330
Platte
320
Aufzeichnungsträger Verifizierungseinheit (Plattenprüfstufe)
Daten Wiedergabe-einheit
Erzeugungseinheit für Wiedergabe-Verifizierungsdaten
322
Daten Vergleichs-einheit
323
Ergebnis Ausgabe-einheit
324
Sicherheit hoch
Verifizierungsdaten
Kodeschlüssel, den Kodeschlüssel betreffende Information
[CPKeys.DAT] [MDC(CPKeys.DAT)]
201
Schlüssel-Verwaltungszentrum (KIC: Schlüssel-Ausgabezentrum)
bearbeiteter Inhalt, den Inhalt betreffende Information
[Con.DAT] [MDC(Con.DAT)]
202
Inhalt-Bearbeitungs-einheit (AS: Autorenstudio)

4 / 4

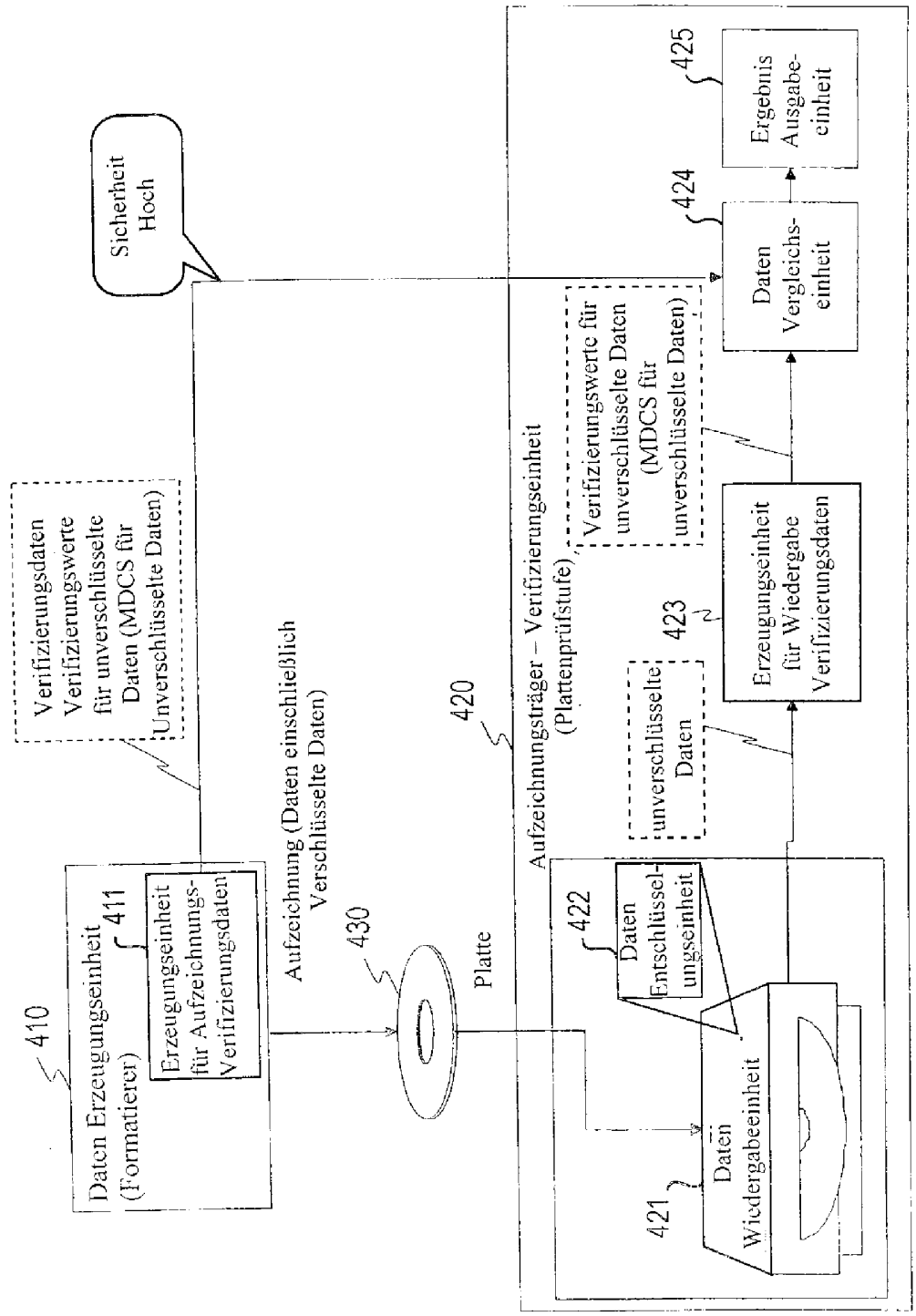

Daten Erzeugungseinheit (Formatierer)
410
Erzeugungseinheit für Aufzeichnungs-Verifizierungsdaten
411
Verifizierungsdaten Verifizierungswerte für unverschlüsselte Daten (MDCS für Unverschlüsselte Daten)
Sicherheit Hoch
Aufzeichnung (Daten einschließlich Verschlüsselte Daten)
430
Platte
420
Aufzeichnungsträger – Verifizierungseinheit (Plattenprüfstufe)
422
Daten Entschlüsselungseinheit
unverschlüsselte Daten
423
Verifizierungswerte für unverschlüsselte Daten (MDCS für unverschlüsselte Daten)
Erzeugungseinheit für Wiedergabe Verifizierungsdaten
Daten Vergleichseinheit
424
Ergebnis Ausgabeeinheit
425
Daten Wiedergabeeinheit
421

FIG. 4