



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 601 25 489 T2** 2007.10.04

(12) **Übersetzung der europäischen Patentschrift**

(97) **EP 1 203 376 B1**

(51) Int Cl.⁸: **G11B 20/00** (2006.01)

(21) Deutsches Aktenzeichen: **601 25 489.9**

(86) PCT-Aktenzeichen: **PCT/EP01/00310**

(96) Europäisches Aktenzeichen: **01 907 443.4**

(87) PCT-Veröffentlichungs-Nr.: **WO 2001/056026**

(86) PCT-Anmeldetag: **11.01.2001**

(87) Veröffentlichungstag
der PCT-Anmeldung: **02.08.2001**

(97) Erstveröffentlichung durch das EPA: **08.05.2002**

(97) Veröffentlichungstag
der Patenterteilung beim EPA: **27.12.2006**

(47) Veröffentlichungstag im Patentblatt: **04.10.2007**

(30) Unionspriorität:

177863 P	24.01.2000	US
536945	28.03.2000	US

(84) Benannte Vertragsstaaten:

DE, ES, FR, GB, IT

(73) Patentinhaber:

**Koninklijke Philips Electronics N.V., Eindhoven,
NL**

(72) Erfinder:

**EPSTEIN, Michael, NL-5656 AA Eindhoven, NL;
MCDERMOTT, M., Robert, NL-5656 AA Eindhoven,
NL**

(74) Vertreter:

Volmer, G., Dipl.-Ing., Pat.-Anw., 52066 Aachen

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG ZUM SCHUTZ EINES INHALTS VOR UNERLAUBTER VER-
VIELFÄLTIGUNG**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

HINTERGRUND DER ERFINDUNG

1. Gebiet der Erfindung

[0001] Diese Erfindung betrifft hauptsächlich das Gebiet der Konsumelektronik und insbesondere den Schutz von kopiergeschütztem Inhaltmaterial.

2. Beschreibung des Stands der Technik

[0002] Die unerlaubte Verbreitung von urheberrechtlich geschütztem Material beraubt den Inhaber des Urheberrechts der ihm zustehenden Lizenzgebühren für dieses Material und kann dem Anbieter dieses unerlaubt verbreiteten Materials zu Gewinnen verhelfen, die zur fortgesetzten unerlaubten Verbreitung ermuntern. Angesichts der Leichtigkeit der Informationsübertragung durch das Internet sind Inhaltmaterialien, die als kopiergeschützt vorgesehen sind, wie z.B. künstlerische Interpretationen oder sonstige Materialien mit eingeschränkten Verbreitungsrechten, leicht der unerlaubten Verbreitung in großem Umfang ausgesetzt. Das MP3-Format zur Speicherung und Übertragung von komprimierten Audiodateien hat die Verbreitung von Audioaufzeichnungen im großem Ausmaß möglich gemacht, da eine 30 oder 40 Megabyte große digitale Audioaufzeichnung eines Songs zu einer MP3-Datei mit 3 oder 4 Megabyte komprimiert werden kann. Mit einer typischen 56 kbps-Wählverbindung ins Internet kann diese Datei in ein paar Minuten in den Computer eines Benutzer heruntergeladen werden. Daher kann eine arglistige Person Songs von einer originalen und legalen CD lesen, die Songs in das MP3-Format codieren und die MP3-codierten Songs zur unerlaubten Verbreitung im großen Umfang im Internet bereitstellen. Alternativ dazu kann eine arglistige Person einen direkten Einwähldienst zum Herunterladen des MP3-codierten Songs anbieten. Die illegale Kopie des MP3-codierten Songs kann dann mit Software oder Hardwaregeräten wiedergegeben werden, oder kann entkomprimiert und auf eine beschreibbare CD gespeichert werden, um auf einem konventionellen CD-Player abgespielt zu werden.

[0003] Mehrere Systeme wurden vorgeschlagen, um die Vervielfältigung von kopiergeschütztem Inhaltmaterial zu begrenzen. Die „Secure Digital Music Initiative“ (SDMI) und andere befürworten die Verwendung von „digitalen Wasserzeichen“, um rechtmäßiges Inhaltmaterial zu kennzeichnen. EP 0981901 „Embedding auxiliary data in a signal“ (Einbetten von Hilfsdaten in ein Signal) vom 1. März 2000 an Antonius A.C.M. Kalker offenbart eine Technik, um elektronisches Material mit Wasserzeichen zu versehen. Wie sein Gegenstück, das Wasserzeichen in Papier, ist ein digitales Wasserzeichen im Inhaltmaterial eingebettet, um erkennbar, aber unauffällig zu sein.

Eine akustische Wiedergabe einer digitalen Musikaufzeichnung, die ein Wasserzeichen enthält, ist von einer Wiedergabe der gleichen Aufzeichnung ohne das Wasserzeichen im Wesentlichen nicht zu unterscheiden. Doch ein Wasserzeichenerkennungsgerät ist in der Lage, diese zwei Aufnahmen auf der Basis des Vorhandenseins oder der Abwesenheit des Wasserzeichens zu unterscheiden. Weil bestimmtes Inhaltmaterial nicht kopiergeschützt sein kann und daher kein Wasserzeichen zu enthalten braucht, kann die Abwesenheit eines Wasserzeichens nicht benutzt werden, um legales Material von illegalem zu unterscheiden. Im Gegenteil deutet die Abwesenheit eines Wasserzeichens darauf hin, dass der Inhalt legal frei kopiert werden darf.

[0004] Auch andere Kopierschutzsysteme sind verfügbar. Zum Beispiel offenbart die europäische Patentschrift EP09066700 „Method and system for transferring content information and supplemental information relative thereto“ (Verfahren und System zum Übertragen von Inhaltsinformation und diesbezüglicher Zusatzinformation) vom 7. April 1999 an Johan P.M.G. eine Technik zum Schutz von urheberrechtlich geschütztem Material durch Verwendung eines Wasserzeichen-„Tickets“, das steuert, wie oft das geschützte Material wiedergegeben werden kann.

[0005] Eine genaue Vervielfältigung des mit Wasserzeichen versehenen Materials wird dazu führen, dass das Wasserzeichen in der Kopie des mit Wasserzeichen versehenen Materials wiedergegeben wird. Eine ungenaue oder verlustreiche Vervielfältigung kann aber keine Wiedergabe des Wasserzeichens in der verlustreichen Kopie des Materials zur Folge haben. Einige Schutzsysteme, einschließlich jener der SDMI, haben dieses Merkmal der verlustreichen Vervielfältigung genutzt, um auf der Basis des Vorhandenseins oder der Abwesenheit eines geeigneten Wasserzeichens legales Material von illegalem Material zu unterscheiden. Im SDMI-Szenario werden zwei Arten von Wasserzeichen definiert. „Robuste“ Wasserzeichen und „fragile“ Wasserzeichen. Ein robustes Wasserzeichen ist eines, von dem zu erwarten ist, dass es einer verlustreichen Vervielfältigung widerstehen kann, die ausgelegt ist, um einen wesentlichen Teil des Originalinhalts zurückzuhalten, wie z.B. eine MP3-Codierung einer Audioaufzeichnung. Das heißt, wenn die Wiedergabe genug Information behält, um eine angemessene Wiedergabe der Originalaufzeichnung zu gewährleisten, bleibt auch das robuste Wasserzeichen erhalten. Ein fragiles Wasserzeichen zum anderen ist eines, von dem zu erwarten ist, dass es durch eine verlustreiche Vervielfältigung oder sonstige unerlaubte Eingriffe beschädigt wird.

[0006] Im SDMI-System zeigt das Vorhandensein eines robusten Wasserzeichens an, dass das Inhalts-

material kopiergeschützt ist, und das Fehlen oder die Beschädigung eines entsprechenden fragilen Wasserzeichens bei Vorhandensein eines robusten Wasserzeichens zeigt an, dass das kopiergeschützte Material auf irgendeine Weise verfälscht wurde. Ein SD-MI-fähiges Gerät ist konfiguriert, um die Wiedergabe von mit Wasserzeichen versehenem Material bei einem beschädigten Wasserzeichen oder bei einem erkannten robusten Wasserzeichen, aber abwesenden fragilen Wasserzeichen zu verweigern, außer, wenn die Beschädigung oder die Abwesenheit des Wasserzeichens auf einen „SDMI-zertifizierten“ Prozess zurückzuführen ist, wie z.B. eine SDMI-Komprimierung von kopiergeschütztem Material zur Verwendung auf einem tragbaren Abspielgerät. Der Einfachheit halber wird der Begriff „wiedergeben“ hierin verwendet, um jede Verarbeitung oder Übertragung des Inhalts einzuschließen, wie z.B. das Abspielen, Aufzeichnen, Umwandeln, Validieren, Speichern, Laden und dergleichen. Dieses System dient dazu, die Verbreitung von Inhaltsmaterial über MP3 oder andere Komprimierungstechniken zu begrenzen, hat jedoch keine Wirkung auf die Verbreitung von nachgemachten unveränderten (unkomprimierten) Vervielfältigungen von Inhaltsmaterial. Dieser eingeschränkte Schutz gilt als kommerziell tragbar, weil die Kosten und der Aufwand des Herunterladens einer extrem großen Datei zum Erhalt eines Songs dazu neigen, vor dem Diebstahl von unkomprimiertem Inhaltsmaterial abzuschrecken.

KURZDARSTELLUNG DER ERFINDUNG

[0007] Eine Aufgabe der Erfindung ist die Ausweitung des Schutzes von kopiergeschütztem Material, um den Schutz von unkomprimiertem Inhaltsmaterial einzuschließen.

[0008] Diese Aufgabe und andere werden durch die Wahl einer ausreichenden Zahl von Datenelementen zum Einschluss in einen Datensatz erfüllt, um vor einer Übertragung des gesamten Satzes über einen Kommunikationsweg mit begrenzter Bandbreite wie das Internet abzuschrecken. Der Datensatz schließt einen Gesamtheitsparameter ein, der benutzt wird, um zu bestimmen, ob die Gesamtheit der Daten vorhanden ist. In einer bevorzugten Ausführungsform ist der Gesamtheitsparameter ein Hash-Wert, der auf Wasserzeichen jedes Datenelements basiert. Zur Wiedergabe werden die Wasserzeichen der Datenelemente im vorliegenden Material gelesen, und ein Hash-Wert wird auf der Basis der vorliegenden Wasserzeichen berechnet. Eine Ungleichheit zwischen dem berechneten Hash-Wert und dem Gesamtheits-Hash-Wert, der im Datensatz enthalten ist, zeigt an, dass weniger als die Gesamtheit der Daten vorliegt, und die Wiedergabe wird verweigert.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0009] Die Erfindung wird Bezug nehmend auf die beiliegenden Zeichnungen ausführlich und beispielhaft beschrieben, wobei:

[0010] [Fig. 1](#) ein erfindungsgemäßes Beispielsystem zum Schutz von kopiergeschütztem Inhaltsmaterial veranschaulicht.

[0011] [Fig. 2](#) eine erfindungsgemäße Beispieldatenstruktur zeigt, die eine Bestimmung des Vorhandenseins einer Gesamtheit eines Datensatzes erleichtert.

[0012] [Fig. 3](#) ein Beispielflussdiagramm für einen erfindungsgemäßen Codierer zeigt, der einen Datensatz und einen dem Datensatz entsprechenden Gesamtheitsparameter erzeugt und speichert.

[0013] [Fig. 4](#) ein Beispielflussdiagramm eines erfindungsgemäßen Decodiersystems zeigt, das Inhaltsmaterial in Abhängigkeit von einer Prüfung des Vorhandenseins einer Gesamtheit eines Datensatzes wiedergibt.

[0014] In allen Zeichnungen beziehen sich gleiche Bezugszeichen auf vergleichbare oder entsprechende Merkmale oder Funktionen.

AUSFÜHRLICHE BESCHREIBUNG DER ERFINDUNG

[0015] Zum einfacheren Verständnis wird die Erfindung hierin im Kontext digital aufgezeichneter Songs dargestellt. Wie für den Fachmann hervorgeht, ist die Erfindung auf jede aufgezeichnete Information anwendbar, die über einen Kommunikationsweg mit begrenzter Bandbreite übertragen werden kann. Statt Songs von einem Album kann das jeweilige Inhaltsmaterial zum Beispiel auch ein Dateneintrag in einer größeren Datenbank sein.

[0016] Vor dem Diebstahl eines Gegenstands kann abgeschreckt werden, indem der Diebstahl zeitraubender oder aufwendiger gemacht wird als der Wert des geraubten Gegenstands. Zum Beispiel wird oft ein durch Schrauben am Boden befestigter Safe verwendet, um kleine Wertgegenstände zu schützen, weil der Aufwand, der erforderlich ist, um den Safe zu stehlen, typischerweise den Gewinn übersteigt, der durch den Diebstahl des Safes zu erwarten ist. Die mitanhängige US-Patentschrift mit dem Titel „Protecting Content from Illicit Reproduction by Proof of Existence of a Complete Data Set“ (Schutz des Inhalts vor unerlaubter Vervielfältigung durch Nachweis des Vorhandenseins eines kompletten Datensatzes) lehrt das Wählen und das Einbinden von Datenelementen in einen Datensatz, dessen Größe ausreichend genug ist, um vor einer Übertragung des Datensatzes

über ein bandbreitenbegrenztes Kommunikationssystem wie z.B. das Internet abzuschrecken, und wird durch Bezugnahme hierin aufgenommen. Diese Parallelanmeldung lehrt das Einbinden von Datenelementen in den Datensatz durch Erzeugen eines Wasserzeichens, das einen Datensatz-Gesamtheitsparameter enthält, und das Einbetten dieses Wasserzeichens in jeden Abschnitt jedes Datenelements. Die Parallelanmeldung lehrt auch den Einschluss eines abschnittsspezifischen Parameters (eine Zufallszahl, die jedem Abschnitt zugewiesen ist) in das Wasserzeichen.

[0017] Wie dem Fachmann bekannt ist, basiert ein Wasserzeichensystem wie bei der Verwendung von Wasserzeichen in Geldscheinen auf der Annahme, dass ein Wasserzeichen von einem illegalen Hersteller nicht leicht nachgemacht werden kann. Auch eine Anzahl anderer Sicherheitssysteme wie z.B. kopiebegrenzende Systeme auf der Basis von Tickets stützten sich auf definierten Wasserzeichen. Die Erzeugung eines spezifisch bewerteten Wasserzeichens für das Sicherheitssystem der Parallelanmeldung kann mit anderen Sicherheitssystemen in Konflikt stehen oder kann mehr Ressourcen verbrauchen, als lohnend erscheint.

[0018] Erfindungsgemäß wird die Gesamtheit des Datensatzes mit einer Gesamtheitsüberprüfungstechnik geprüft, die keine Erzeugung von spezifischen Wasserzeichen erfordert. Ein Gesamtheitsparameter wird bei der Erzeugung des Datensatzes erzeugt, auf der Basis einer Zusammensetzung von Sicherheitskennungen, die jedem Datenelement im Datensatz zugewiesen sind. Die Sicherheitskennung jedes Datenelements ist so konfiguriert, dass eine Änderung des Datenelements zu einer Änderung der Sicherheitskennung führt. Wenn der Datensatz zur Wiedergabe vorgelegt wird, wird eine entsprechende Sicherheitskennung für jedes Datenelement auf der Basis des vorgelegten Datenelements bestimmt, und ein entsprechender Gesamtheitsparameter wird berechnet. Wenn der berechnete Gesamtheitsparameter nicht dem Gesamtheitsparameter entspricht, der zum Datensatz gehört, wird die anschließende Wiedergabe der vorliegenden Datenelemente verhindert. Im Kontext digitaler Audioaufzeichnungen ist ein entsprechendes Abspiel- oder Aufzeichnungsgerät konfiguriert, um die Wiedergabe eines Einzelsongs in Abwesenheit des Gesamtinhalts der CD zu verweigern. Die Zeit, die zum Herunterladen eines ganzen Albums auf einer CD in unkomprimierter digitaler Form benötigt wird, kann selbst bei DSL- und Kabelmodemgeschwindigkeiten mehr als eine Stunde lang dauern, je nach Netzauslastung und anderen Faktoren. Indem das Vorhandensein des Gesamtinhalts der CD bei Download-„Kosten“ von mehr als einer Stunde gefordert wird, wird die Wahrscheinlichkeit eines Diebstahls eines Songs durch eine weite Verbreitung im Internet erheblich reduziert.

[0019] Wie oben erläutert, sind einige Kopierschutzsysteme vorgeschlagen worden, wobei urheberrechtlich geschütztes Material wie z.B. ein Song mit einem im Wesentlichen einmaligen eingebetteten Wasserzeichen aufgezeichnet wird. Im Kontext solch eines Kopierschutzsystems verwendet eine bevorzugte Ausführungsform dieser Erfindung das eingebettete Wasserzeichen jedes Songs als die Sicherheitskennung, unter der Annahme, dass das eingebettete Wasserzeichen eine fragile Komponente einschließt, die verändert wird, wenn das zugehörige Inhaltsmaterial modifiziert wird. Wie oben erwähnt, stützen sich zum Beispiel bestehende SDMI-Sicherheitssysteme auf ein fragiles Wasserzeichen, das verändert wird, wenn der Song einer MP3-Komprimierung unterzogen wird.

[0020] Es können alternative Techniken verwendet werden, um eine Sicherheitskennung zu bestimmen oder zu erzeugen. In einer Umgebung ohne Wasserzeichen zum Beispiel kann eine Prüfsumme oder eine ziemlich einmalige Kennung des Datenelements als Sicherheitskennung verwendet werden, unter der Voraussetzung, dass die Kennung vom Inhalt des Datenelements abhängig ist. Für zusätzliche Sicherheit kann ein Hash-Wert der Kennung benutzt werden, um die Schwierigkeit der Ersetzung eines kurzen Datenelements zu erhöhen, das die gleiche Sicherheitskennung hat wie das Originaldatenelement. Der Einfachheit halber ist die Erfindung hier mit dem Musterbeispiel eines fragilen Wasserzeichens als der Sicherheitskennung dargestellt, auch wenn dem Fachmann angesichts dieser Offenbarung Sicherheitskennungen einfallen werden, die Prüfsummen, Hash-Werte, digitale Signaturen und dergleichen einschließen.

[0021] [Fig. 1](#) zeigt ein Beispielblockdiagramm eines erfindungsgemäßen Schutzsystems **100**. Das Schutzsystem **100** umfasst einen Codierer **110**, der Inhaltsmaterial auf ein Medium **130** codiert, und einen Decoder **120**, der das Inhaltsmaterial vom Medium **130** wiedergibt. Der Codierer **110** umfasst einen Selektor **112**, der Inhaltsmaterial von einer Quelle wählt, und einen Rekorder **114**, der dieses Material auf das Medium **130** aufzeichnet. Der Selektor **112** kann zum Beispiel konfiguriert sein, um Inhaltsinformation zu sammeln, die Songs entspricht, die zu einem Album zusammengestellt sind. Der Rekorder **114** formatiert, codiert und speichert die Information auf geeignete Weise auf das Medium **130**, mit Hilfe von Techniken, die dem Fachmann bekannt sind.

[0022] Erfindungsgemäß wählt der Selektor **112** Datenelemente, die zum Datensatz hinzugefügt werden sollen, bis die Größe des Datensatzes als groß genug gilt, um vor einer nachfolgenden Übertragung des Datensatzes über einen Kommunikationskanal mit begrenzter Bandbreite abzuschrecken. Diese „abschreckende Größe“ ist ein subjektiver Wert und

von der angenommenen verfügbaren Kommunikationsbandbreite, dem Übertragungsverlust usw. abhängig. Auch andere Kriterien können verwendet werden, um zu bestimmen, ob dem Datensatz weitere Datenelemente hinzugefügt werden sollen. Wenn die Datenelemente zum Beispiel Songs einer bestehenden Albensammlung entsprechen, werden typischerweise alle Songs zum Datensatz hinzugefügt, ungeachtet dessen, ob die Größe des Datensatzes die bestimmte abschreckende Größe überstiegen hat. Wenn alle Songs der Albensammlung gewählt wurden und das abschreckende Größenkriterium noch nicht erreicht ist, können andere Datenelemente gewählt werden, um die erforderliche abschreckende Größe anzuhäufen. Zum Beispiel können Datenelemente, die Zufallsdatenbits enthalten, zum Datensatz hinzugefügt werden, um seine Größe zu erhöhen. Diese Zufallsbits werden typischerweise als Außerband-Daten, CD-ROM-Daten und dergleichen gespeichert, um zu verhindern, dass die von einem konventionellen CD-Player als hörbare Töne wiedergegeben werden. Alternativ dazu können die Datenelemente andere Probesongs umfassen, die zum Kauf anderer Alben anregen sollen, oder Bild- und Videoabschnitte, die sich auf das aufgezeichnete Inhaltmaterial beziehen. Dementsprechend kann auch Werbematerial wie z.B. Angebote von Internetzugangsanbietern in die aufgezeichnete Information des Datenträgers eingeschlossen werden. Diese und andere Mittel zum Vergrößern der Größe eines Datensatzes werden dem Fachmann angesichts dieser Erfindung einfallen. Ferner können ein oder mehrere Datenelemente spezifisch in den Datensatz eingeschlossen werden, um die Sicherheit dieses Systems zu erhöhen, zum Beispiel durch Einfügen von Wasserzeichen, die mit der anfänglichen Auswahl der im Datensatz enthaltenen Datenelemente ohne Beziehung sind. Erfindungsgemäß wird ein Gesamtheitsparameter auf der Basis jedes im Datensatz enthaltenen Datenelements erzeugt. Die Entfernung oder Änderung eines der Datenelemente, einschließlich der Zufallsabschnitte, des Werbematerials und dergleichen, die hinzugefügt wurden, um die Größe des Datensatzes zu vergrößern oder um die Sicherheit des Gesamtheitsparameters zu verbessern, führt zu einem anderen entsprechenden Gesamtheitsparameter und kann verwendet werden, um die nachfolgende Wiedergabe von Datenelementen von einem Datensatz mit einem anderen Gesamtheitsparameter zu verhindern.

[0023] Erfindungsgemäß umfasst der Codierer **110** einen Binder **116**, der einen Gesamtheitsparameter bestimmt, der wirkt, um die Parameter mit jedem Datenelement zu verbinden, das vom Selektor **112** zum Einschluss in den Datensatz gewählt wurde. In einer bevorzugten Ausführungsform ist der Gesamtheitsparameter ein Hash-Wert, der auf einer Zusammensetzung einer Gesamtheit der Daten basiert. Wie oben erläutert, basiert der Gesamtheitsparameter

bevorzugt auf Sicherheitskennungen, die jedem Datenelement im Datensatz angehören, auch wenn der Gesamtheitsparameter auf Unterabschnitten jedes Datenelements basieren kann. Das heißt zum Beispiel im Kontext eines digital aufgezeichneten Songs, dass jeder Abschnitt eines Songs eine einmalige Kennung aufweisen kann und der Gesamtheitsparameter auf einer Zusammensetzung dieser Abschnittskennungen basieren kann. Dementsprechend kann der Gesamtheitsparameter ein Prüfsumme sein, die auf jeder der einzelnen Dateneinheiten einschließlich jedes Datenelements basiert. Der Einfachheit halber wird der Begriff Datenelement nachstehend verwendet, um sich auf das Element zu beziehen, dem die Sicherheitskennung angehört, ungeachtet von der Struktur des Inhalts des Datensatzes.

[0024] Im Kontext der Audioaufzeichnungen und Konsumprodukte wird die Verwendung eines Wasserzeichens als Sicherheitskennung bevorzugt, weil Wiedergabegeräte oft mit zahlreichen Fehlermaskierungstechniken konfiguriert sind und den wahren Inhalt der Datenelemente auf dem Aufzeichnungsmedium nicht genau wiedergeben können. Zum Beispiel wird ein falsch gelesener Sektor auf einer Disk während der Wiedergabe oft durch einen früheren Sektor ersetzt, wobei der Vorrang auf die Erzeugung eines stetigen Tonflusses gelegt wird, statt auf eine unterbrochene Wiedergabe von richtigen Tönen. In solch einer Umgebung kann eine Sicherheitskennung, die auf das Vorhandensein jedes einzelnen Bits im Datenelement basiert, nicht praktisch sein. Wasserzeichen und Wasserzeichensysteme sind zum anderen ausgelegt, um eine genaue Darstellung des erkannten Wasserzeichens zu ergeben, unabhängig von der Fehlermaskierung und anderer Effekte, die die Genauigkeit der vorgelegten Daten beeinträchtigen können.

[0025] Der erfindungsgemäße Decoder **120** umfasst einen Renderer **122** und ein Gatter **124**, das von einem Gesamtheitsprüfer **126** gesteuert wird. Der Renderer **122** ist konfiguriert, um Information von einem Mediumlesegerät wie z.B. einem CD-Leser **132** abzurufen. Wie wohlbekannt, ruft der Renderer **122** die Information ab, indem er einen Speicherortindex spezifiziert, und in Antwort darauf stellt der Leser **132** die Daten bereit, die sich am spezifizierten Speicherortindex auf das Medium **130** befinden. Die Daten an zusammenhängenden Stellen des Mediums **130** werden blockweise gelesen, indem ein Speicherortindex und eine Blockgröße spezifiziert werden.

[0026] Die gestrichelten Linien in [Fig. 1](#) veranschaulichen einen beispielhaften Songextraktor **142**, der einen Song aus dem Medium **130** extrahiert und ihn an einen beispielhaften CD-Imitator **144** übergibt, der einen möglichen illegalen Download des Songs über das Internet darstellt. Der CD-Imitator **144** steht zum Beispiel für ein Softwareprogramm, das in Ant-

wort auf einen konventionellen CD-Lesen-Befehl Information ausgibt. Alternativ dazu kann die vom Songextraktor empfangene Information auf ein CD-Medium geschrieben sein und dem konventionellen CD-Leser **132** zugeführt werden. Wie oben erwähnt, ist die Verwendung des CD-Extraktors **142** wahrscheinlich, da durch die absichtlich große Größe des Inhalts des Mediums **130** vor der Übertragung der Gesamtheit des Inhalts des Mediums abgeschreckt werden soll.

[0027] Erfindungsgemäß ist der Gesamtheitsprüfer **126** konfiguriert, um Daten vom Medium **130** zu erhalten, typischerweise über den Renderer **122**, um zu bestimmen, ob die Gesamtheit des Datensatzes vorhanden ist. Der Renderer **122** ist konfiguriert, um das Wasserzeichen oder eine sonstige Sicherheitskennung zu bestimmen, die zu den vom Medium **130** gelesenen Datenelementen gehört. Der Gesamtheitsprüfer **126** verwendet die Sicherheitskennung, um zu bestimmen, ob die Gesamtheit des Datensatzes dem Renderer **122** zur Verfügung steht, wie weiter unten erläutert.

[0028] [Fig. 2](#) veranschaulicht eine Beispieldatenstruktur **200** zum Speichern von Datenelementen in einen Datensatz, die eine Bestimmung erleichtert, ob die Gesamtheit der Originaldaten vorhanden ist, unter der Voraussetzung, dass ein Wasserzeichen als Sicherheitskennung verwendet wird. Eine Spur **210**- und Abschnitt **220**-Struktur ist dargestellt, die mit der Speicherstruktur konventioneller CD- und anderer Speichermedien konsistent ist. In der Beispieldatenstruktur **200** ist ein Wasserzeichen **230**, das jeder Spur zugewiesen ist, in jedem Abschnitt **220** eingebettet. Die Spur **0** weist ein Wasserzeichen WO auf, die Spur **1** ein Wasserzeichen W1, und so weiter. Alternative Wasserzeichensysteme sind dem Fachmann bekannt, einschließlich einzelner Wasserzeichen, die jedem Abschnitt **220** zugewiesen sind. Im Beispiel von [Fig. 2](#) ist ein Hash **240** einer Zusammensetzung der Wasserzeichen W0, W1, ... Wn in der Datenstruktur **200** gespeichert, bevorzugt als Außenbanddaten (OBD). Dieser Hash **240** kann zum Beispiel im Inhaltsverzeichnis einer typischen CD gespeichert sein, als „CD-ROM“-Daten in einer gemischten Audio-Daten-CD, als ein separater und einziger Datenabschnitt, als ein falscher Song, der nur Daten enthält, und so weiter. Bevorzugt schließen die Wasserzeichen eine Kombination aus robusten und fragilen Wasserzeichen ein, so dass eine Entfernung oder Änderung des robusten Wasserzeichens eine Beschädigung des entsprechenden Datenelements bewirkt und eine Änderung eines Datenelements die Beschädigung des entsprechenden fragilen Wasserzeichens bewirkt.

[0029] Wieder auf [Fig. 1](#) Bezug nehmend, wenn die echte oder illegale Kopie der Inhaltsinformation dem Renderer **122** vorgelegt wird, empfängt der Gesamt-

heitsprüfer **126** vom Renderer **122** jedes Wasserzeichen, auf welchem der Gesamtheitsparameter basiert. Der Gesamtheitsprüfer **126** berechnet einen Gesamtheitswert mit demselben Algorithmus, den vom Codierer **110** verwendet wurde, um den Gesamtheitsparameter zu berechnen. Im Beispiel von [Fig. 2](#) ist der Gesamtheitswert ein Hash der Wasserzeichen, die vom Renderer zugeführt wurden, unter Verwendung derselben Hash-Funktion, die verwendet wurde, um den Gesamtheitsparameter **240** zu erzeugen. Der Gesamtheitsprüfer **126** empfängt den Gesamtheitsparameter **240** vom Renderer **122** und vergleicht ihn mit diesem berechneten Hash der zugeführten Wasserzeichen. Wenn der Gesamtheitsparameter **240** und der berechnete Hash nicht übereinstimmen, verhindert der Gesamtheitsprüfer **126** über das Gatter **124** die Wiedergabe der nachfolgenden Datenelemente aus der offenbar illegalen Quelle.

[0030] In einer bevorzugten Ausführungsform wird der Gesamtheitsparameter auch mit dem Inhaltsverzeichnis für den Datensatz verbunden, weil der Gesamtheitsprüfer **126** das Inhaltsverzeichnis verwendet, um die Zahl der Spuren und die Zahl der Abschnitte in jeder Spur zu bestimmen. Diese Verbindung dient dazu, eine Ersetzung eines verkürzten Datensatzes zu verhindern, der zum Beispiel einen Einzelabschnitt pro Spur umfasst. Alternativ dazu kann angenommen werden, dass die Größe eines erfindungsgemäßen Datensatzes eine spezifizierte Mindestzahl von Abschnitten enthält. Mit dieser Annahme kann der Gesamtheitsprüfer konfiguriert werden, um die Wiedergabe des Inhaltsmaterials zu verhindern, wenn die Gesamtzahl der Abschnitte, die in einem verkürzten Inhaltsverzeichnis enthalten sind, sich nicht auf dieses spezifizierte Minimum beläuft.

[0031] Auch andere Sicherheitssysteme, die in [Fig. 1](#) nicht dargestellt sind, können verwendet werden, um das Gatter **124** zu steuern, einschließlich solcher, die sich auf den Wert der einzelnen Wasserzeichen stützen, wie z.B. das oben genannte europäische Patent EP983687A2, das ein Wasserzeichen-"Ticket" verwendet, das steuert, wie oft das geschützte Material wiedergegeben werden darf. Das heißt, durch Verwendung bestehender oder vordefinierter Wasserzeichen, wie z.B. das oben erwähnte „Ticket“, zum Erzeugen des Gesamtheitsparameters ist die erfindungsgemäße Datenstruktur mit anderen Systemen kompatibel, die diese Wasserzeichen verwenden oder spezifizieren. Das Beispielgatter **124** wurde zum leichteren Verständnis dargestellt. Verschiedene Techniken können verwendet werden, um die Wiedergabe des Materials zu verhindern, einschließlich einer direkten Steuerung des Renderers **122**, einer Steuerung eines anderen Geräts, wie z.B. einer Stromversorgung zum Renderer **122**, und so weiter.

[0032] Je nach dem gewünschten Sicherheitsgrad

in Bezug auf die Zeit, die benötigt wird, um diese Sicherheit zu erreichen, kann die Zusammensetzung der Wasserzeichen auf weniger als allen verfügbaren Wasserzeichen basieren. Zum Beispiel kann ein Satz Gesamtheitsparameter definiert werden, wobei jeder Gesamtheitsparameter einem vordefinierten Teilsatz der verfügbaren Wasserzeichen entspricht. Zum Beispiel kann ein Teilsatz von Wasserzeichen jedes andere Wasserzeichen, jedes dritte Wasserzeichen, jedes Wasserzeichen, das nicht durch zwei, drei oder sieben teilbar ist, oder andere Wasserzeichensammlungen umfassen, die allen fähigen Decodern allgemein bekannt sein können. Eine algorithmisch bestimmte Auswahl von Mitgliedern jedes Teilsatzes wird bevorzugt, so dass ein fähiger Decoder unabhängig vom gerade vorliegenden Datensatz die Mitglieder jedes Teilsatzes von Wasserzeichen bestimmen kann. Der Decoder **120** in diesem Beispiel wählt aus dem Gesamtheitsparametersatz nach dem Zufallsprinzip einen (oder mehrere) als den zu prüfenden Gesamtheitsparameter aus und führt die Prüfung auf der Basis des Teilsatzes von Wasserzeichen durch, der dem zufällig gewählten Gesamtheitsparameter entspricht. Selbst, wenn jeder Gesamtheitsparameter nur das Vorhandensein eines Teilsatzes des Datensatzes prüft, muss eine illegale Kopie des Datensatzes die Gesamtheit des Datensatzes enthalten, weil die Auswahl des zu prüfenden Teilsatzes von Wasserzeichen bei der Wiedergabe des Materials bestimmt wird. Eine illegale Kopie des Datensatzes, die zum Beispiel jeden anderen Song eines Albums enthält, kann von einigen Sätzen Wasserzeichen als vollständig geprüft werden, wird aber von anderen Sätzen Wasserzeichen, wie z.B. einem Satz aus jedem dritten Wasserzeichen im Originaldatensatz, als unvollständig geprüft. In einer bevorzugten Ausführungsform wird der Satz der Gesamtheitsparameter so definiert, dass jedes Wasserzeichen in mindestens einem entsprechenden Teilsatz von Wasserzeichen enthalten ist. Um eine umfassende Prüfung zu gestatten, entspricht einer der Gesamtheitsparameter in einer bevorzugten Ausführungsform dem Satz aller Wasserzeichen.

[0033] [Fig. 3](#) zeigt ein Beispielflussdiagramm für einen erfindungsgemäßen Codierer **110**. Die Schleife **310-335** erzeugt einen Datensatz, der eine Sammlung von Datenelementen enthält, wie oben beschrieben. Für jedes gewählte Datenelement wird in **320** ein Sicherheitselement erzeugt, außer, wenn in **315** bereits ein Sicherheitselement für dieses Datenelement vorhanden ist. Zum Beispiel kann ein digital aufgezeichneter Song ein oder mehrere Wasserzeichen enthalten, die im Song eingebettet sind, wie oben erläutert. Auf dem Gebiet der Datenverarbeitung kann eine Prüfsumme für jedes Datenelement erzeugt werden. Auf dem Video-Gebiet kann ein Parameter eines bestimmten Blocks, wie die niederwertigsten Bits einer Codierung des Blocks innerhalb jedes unabhängigen Einzelbilds, als ein Sicherheitselement

verwendet werden. Der Wert des Sicherheitselements wird zur Verwendung in Schritt **352** temporär gespeichert, was nicht dargestellt ist, um einen oder mehrere Gesamtheitsparameter zu erzeugen. Bei der Wahl jedes Datenelements wird in Schritt **330** die summierte Größe des Datensatzes berechnet. Nachfolgende Datenelemente werden zum Datensatz hinzugefügt, bis in Schritt **335** die Größe als ausreichend erachtet wird, um für die spätere Übertragung über einen bandbreitenbegrenzten Kommunikationskanal abschreckend zu sein, wie oben erläutert. Jeder Abschnitt wird in **340** mit seiner Sicherheitskennung auf das Medium gespeichert.

[0034] Die Schleife **350-359** erzeugt und speichert einen oder mehrere Gesamtheitsparameter auf das Medium, zur Verwendung durch einen Decoder, um bei einer nachfolgenden Kopie einiger oder aller Datenelemente des Datensatzes zu bestimmen, ob eine Gesamtheit des Datensatzes vorliegt. Um eine schnelle statistische Prüfung zu erleichtern, dass eine Gesamtheit der Daten vorhanden ist, wird, wie oben erläutert, ein Satz Gesamtheitsparameter erzeugt, wobei jeder Gesamtheitsparameter des Gesamtheitsparametersatzes einem Teilsatz von Datenelementen innerhalb des Datensatzes entspricht. Bevorzugt kann der jedem Gesamtheitsparameter entsprechende Teilsatz von Datenelementen algorithmisch bestimmt werden, so dass die Entsprechung in jedem Decoder bestimmt werden kann. Alternativ dazu kann eine „Mitgliederliste“, die für jeden Gesamtheitsparameter den zugehörigen Teilsatz von Datenelementen auf explizite Weise oder algorithmisch definiert, auf das Medium aufgezeichnet werden. In **352** wird der Gesamtheitsparameter erzeugt, der zum entsprechenden Teilsatz von Datenelementen gehört. In einer bevorzugten Ausführungsform ist dieser Gesamtheitsparameter ein Hash der Sicherheitskennungen jedes Datenelements im Teilsatz der Datenelemente, die zum Gesamtheitsparameter gehören. In **354** wird dieser Gesamtheitsparameter auf das Medium gespeichert, bevorzugt in einer sicheren Form, wie z.B. ein eingebettetes Wasserzeichen oder ein Element, das mit einem anderen Element wie z.B. einem Inhaltsverzeichnis verbunden ist. [Fig. 4](#) zeigt ein Beispielflussdiagramm für einen erfindungsgemäßen Decoder **120**. Es wird angenommen, dass der Prozess von [Fig. 4](#) aufgerufen wird, nachdem bestimmt wurde, dass ein angefordertes Datenelement, wie z.B. ein Song von einer CD, ein Mitglied eines kopiergeschützten Datensatzes ist, zum Beispiel durch das Vorhandensein eines Wasserzeichens, eines Eintrags im Inhaltsverzeichnis und so weiter. In **410** wird ein Gesamtheitsparameter aus dem zum Datensatz gehörigen Satz von Gesamtheitsparametern gewählt. Wenn nur ein Gesamtheitsparameter zur Auswahl verfügbar ist, wird er gewählt. Der gewählte Gesamtheitsparameter wird in **420** gelesen. Wie oben erwähnt, ist dieser Gesamtheitsparameter auf dem Gebiet der digitalen Audioaufzeichnungen bevorzugt

ein Hash aus einem zusammengesetzten Teilsatz von Wasserzeichen, der zum gewählten Gesamtheitsparameter gehört: $H'(W(e,1), W(e,2), \dots, W(e,m))$, wobei e ein Index ist, der dem gewählten Gesamtheitsparameter entspricht, m die Zahl der Wasserzeichen im Teilsatz ist und der Indexstrich ($'$) einen Wert bezeichnet, der vom Medium gelesen wird; wenn das dem Decoder vorliegende Material die Originalaufzeichnung ist, sind die Werte mit Indexstrich und die Werte ohne Indexstrich gleich. In **430** wird jedes der Wasserzeichen ($W'(e,1)$, $W'(e,2), \dots, W'(e,m)$) gelesen, die im Teilsatz von Wasserzeichen enthalten sind, der zum gewählten Gesamtheitsparameter gehört, und in **440** wird ein Gesamtheitswert auf der Basis einer Zusammensetzung dieser Wasserzeichen $H(W'(e,1), W'(e,2), \dots, W'(e,m))$ mit dem gleichen Prozess berechnet, der verwendet wurde, um den Gesamtheitsparameter in der Originalaufzeichnung zu erzeugen. Wenn dieser berechnete Gesamtheitswert in **445** nicht gleich dem gelesenen Gesamtheitsparameter ist, was eine Änderung des Inhaltsmaterials oder des Gesamtheitsparameters impliziert, wird die Wiedergabe des Songs in **490** verhindert. Wenn dieser berechnete Gesamtheitswert dem gelesenen Gesamtheitswert entspricht, kann über **455** bis **410** ein anderer Zufalls-gesamtheitswert gewählt und geprüft werden, bis ausreichend Sicherheit erreicht wurde, dass die Gesamtheit des Datensatzes vorliegt. Wie oben erwähnt, entspricht in einer bevorzugten Ausführungsform einer von Gesamtheitsparametersätze einer Zusammensetzung aus allen Wasserzeichen, und absolute Sicherheit, dass die Gesamtheit des Datensatzes vorliegt, kann gewonnen werden, indem beim ersten Eintritt in Block **410** dieser Gesamtheitsparameter gewählt wird. Wenn in **455** ausreichend Sicherheit gewonnen wurde, dass die Gesamtheit des Datensatzes im wiederzugebenden Material vorliegt, wird das gewählte Datenelement in **460** wiedergegeben. Andere Datenstrukturen, die auf anderen Sicherheitskennungssystemen basieren, werden auf eine dem jeweiligen System entsprechende Weise verarbeitet.

[0035] Um die mit dem obigen Prüfungssystem einhergehende Verzögerung zu minimieren, kann vorausgesetzt, dass der CD-Leser **132** dem Renderer **122** die Information mit einer Geschwindigkeit größer als die zur Wiedergabe benötigte Geschwindigkeit zuführen kann, der Decoder **120** von [Fig. 1](#) so aufgebaut sein, dass die Wiedergabe des Inhaltsmaterials gestartet wird, während die Wasserzeichen gelesen werden, und die Wiedergabe dann abgebrochen wird, sobald bestimmt wird, dass der berechnete Gesamtheitswert nicht mit dem entsprechenden gespeicherten Gesamtheitsparameter übereinstimmt.

[0036] Das vorstehend veranschaulicht lediglich die Prinzipien der Erfindung. Dem Fachmann werden verschiedene Anordnungen einfallen, die, obwohl sie

hierin nicht ausdrücklich beschrieben oder dargestellt wurden, den Prinzipien der Erfindung entsprechen und daher im Rahmen der Erfindung liegen. Zum Beispiel zeigen die oben dargestellten Beispiele jeden Teil des aufgezeichneten Materials als Bestandteil eines Datensatzes. In einer alternativen Ausführungsform können aus Leistungsgründen gewählte Datenelemente oder gewählte Teile von Datenelemente verwendet werden, um den Datensatz zu formen. Zum Beispiel kann der Schluss von Songs nicht Bestandteil des „Datensatzes“ sein, wie hierin definiert, weil der Wasserzeichenprozess auf einer festen Blockgröße für jedes Wasserzeichen basieren kann, oder auf jede redundante Kopie des Wasserzeichens. Wenn zum Beispiel das Wasserzeichen oder ein anderer Parameter für eine zuverlässige Aufzeichnung zehn Sekunden einer Aufzeichnung in Anspruch nimmt, wird der Rest ((die Länge des Songs) modulo (10 Sekunden)) auf das Medium aufgezeichnet, aber nicht in den „Datensatz“ aufgenommen, dessen Gesamtheit geprüft wird. Dementsprechend kann Werbematerial auf dem Aufzeichnungsmedium eingeschlossen, aber absichtlich aus dem Datensatz ausgeschlossen sein, so dass es frei kopiert und woanders wiedergegeben werden kann. Es ist auch anzumerken, dass die Beispielflussdiagramme dazu dienen, das Verständnis zu erleichtern, und die spezielle Anordnung und Schrittfolge veranschaulichend sind. Zum Beispiel werden in den Entscheidungsblöcken zum Bestimmen der Entsprechung einfache Gleichheiten dargestellt, während abhängig von den speziellen Techniken, die angewandt werden, um die Parameter zu codieren und zu decodieren, die Bewertung, ob das gelesene Element einem bestimmten Element entspricht, verschiedene Zwischenprozesse umfassen kann. Diese Prozesse können zum Beispiel eine Entschlüsselung von Elementen auf der Basis bestimmter Schlüssel, Fuzzy-Logik oder statistische Prüfungen umfassen, um zu bestimmen, ob zwei Werte „nah genug“ sind, um eine Entsprechung zu implizieren, und dergleichen. Varianten wie diese und weitere werden für den Fachmann angesichts dieser Erfindung ersichtlich sein und sind im Umfang der folgenden Ansprüche eingeschlossen.

Legende der Zeichnungen

Bezugszeichenliste

[Fig. 1](#)

110	Codierer
112	Selektor
114	Rekorder
116	Binder
120	Decoder
122	Renderer

124	Gatter
126	Gesamtheitsprüfer
132	CD-Leser
content source	Inhaltsquelle
rendered content	wiedergegebener Inhalt
142	Song-Extraktor
144	CD-Imitator

[Fig. 2](#)

Track	Spur
Sect.	Abschnitt

[Fig. 3](#)

310	Ein Datenelement wählen
315	Ist Sicherheitskennung vorhanden?
320	Sicherheitskennung für dieses Datenelement erzeugen
330	Gesamtheitsgröße summieren
335	Gesamtheitsgröße > abschreckende Größe?
340	Jeden Abschnitt mit Sicherheitskennung auf Medium speichern
350	Für jedes Mitglied des Gesamtheitssatzes ($i = 1, \dots, \#Sätze$)
352	Gesamtheitsparameter $E(i)$ auf der Basis einer Zusammensetzung von Sicherheitskennungen des Teilsatzes von Datenelementen dieses Gesamtheitsmitglieds
354	Gesamtheitsparameter $E(i)$ auf Medium speichern
350	Nächstes Mitglied
Yes	Ja
No	Nein

[Fig. 4](#)

410	Einen Gesamtheitsparameter $E(i)$ aus dem Satz von Gesamtheitsparametern nach dem Zufallsprinzip wählen
420	Gesamtheitsparameter $E(i)$ lesen [= $H'(W(e,1), W(e,2), \dots, W(e,m))$]
430	Jedes dem Gesamtheitsparameter $E(i)$ entsprechende Wasserzeichen lesen ($W'(e,1), W'(e,2), \dots, W'(e,m)$)
440	Hash der gelesenen Wasserzeichen berechnen $H(W'(e,1), W'(e,2), \dots, W'(e,m))$
445	Berechneter Hash $H(W'(e,1), \dots, W'(e,m)) =$ gelesener Hash $H'(W(e,1), \dots, W(e,m))$?
455	Ausreichend Sicherheit?
460	Gewählten Song wiedergeben
490	Wiedergabe des Songs verweigern
Yes	Ja
No	Nein

Patentansprüche

1. Verfahren zur Abschreckung vor einem Diebstahl von Inhaltmaterial, umfassend:

das Sammeln (310-335) einer Vielzahl von Datenelementen (210), die das Inhaltmaterial einschließen, um einen Datensatz einer Größe zu formen, die groß genug ist, um vor einer nachfolgenden Übertragung des Datensatzes über einen Kommunikationskanal mit begrenzter Bandbreite abzuschrecken, wobei jedes von der Vielzahl von Datenelementen (210) eine zugehörige Sicherheitskennung (230) aufweist, die so konfiguriert ist, dass eine Änderung des Datenelements (210) eine Änderung der Sicherheitskennung (230) bewirkt, das Erzeugen (352) eines Gesamtheitsparameters (240) auf der Basis einer Vielzahl der Sicherheitskennungen (230); und das Einschließen (354) des Gesamtheitsparameters (240) in den Datensatz, um eine Verhinderung der Verarbeitung eines aus der Vielzahl von Datenelementen (210) gewählten Datenelements (210) in Abwesenheit einer Gesamtheit des Datensatzes zu erleichtern.

2. Verfahren nach Anspruch 1, wobei der Gesamtheitsparameter (240) einen Hash-Wert einer Zusammensetzung der Vielzahl von Sicherheitskennungen (230) umfasst.

3. Verfahren nach Anspruch 1, wobei die Sicherheitskennung (230) mindestens eines einschließt von:
einem Wasserzeichen, das in das entsprechende Datenelement (210) eingebettet ist
einem Hash-Wert, der auf dem entsprechenden Datenelement (210) basiert.

4. Verfahren nach Anspruch 3, wobei das Wasserzeichen einschließt:
ein robustes Wasserzeichen, das so konfiguriert ist, dass eine Entfernung des robusten Wasserzeichens eine Beschädigung des entsprechenden Datenelements (210) bewirkt, und
ein fragiles Wasserzeichen, das so konfiguriert ist, dass eine Änderung des entsprechenden Datenelements (210) eine Beschädigung des fragilen Wasserzeichens bewirkt.

5. Verfahren nach Anspruch 1, wobei die Vielzahl von Datenelementen (210) eine Vielzahl von mindestens einem umfasst von: digital codiertem Audioinhalt, digital codiertem Videoinhalt.

6. Verfahren nach Anspruch 1, wobei der Gesamtheitsparameter (240) mit einem Inhaltsverzeichnis verbunden wird, der zum Datensatz gehört.

7. Verfahren nach Anspruch 1, außerdem umfassend:
das Erzeugen (350-359) einer Vielzahl von anderen Gesamtheitsparametern, wobei jeder von der Vielzahl der anderen Gesamtheitsparameter auf einer zugehörigen Vielzahl von Sicherheitskennungen

(230) basiert, und das Einschließen (354) der Vielzahl der anderen Gesamtheitsparameter in den Datensatz, um eine Verhinderung der Verarbeitung jedes Datenelements (210) in Abwesenheit einer Gesamtheit des Datensatzes zusätzlich zu erleichtern.

8. Verfahren zum Decodieren von Inhaltsmaterial von einer Quelle, umfassend:
das Lesen (420) eines dem Inhaltsmaterial entsprechenden Gesamtheitsparameters (240) von der Quelle,
das Lesen (430) einer Vielzahl von Sicherheitskennungen (230) von der Quelle, auf denen der Gesamtheitsparameter (240) basiert, wobei jede Sicherheitskennung (230) einem Datenelement (210) des Inhaltsmaterials entspricht,
das Bestimmen (440) eines Gesamtheitswerts auf der Basis der Vielzahl von Sicherheitskennungen (230),
das Wiedergeben (460) des Inhaltsmaterials von der Quelle in Abhängigkeit von einer Entsprechung (445) zwischen dem Gesamtheitswert und dem Gesamtheitsparameter (240).

9. Verfahren nach Anspruch 8, wobei das Lesen (420) des Gesamtheitsparameters (240) eine Zufallsauswahl (410) aus einem Satz von Gesamtheitsparametern einschließt, wobei jeder Gesamtheitsparameter (240) des Gesamtheitsparametersatzes einen zugehörigen Satz von Sicherheitskennungen (230) aufweist.

10. Verfahren nach Anspruch 8, wobei der Gesamtheitsparameter (240) einen Hash-Wert einer Zusammensetzung der Vielzahl von Sicherheitskennungen (230) einschließt.

11. Verfahren nach Anspruch 8, wobei die Sicherheitskennung (230) mindestens eines einschließt von:
einem Wasserzeichen, das in das entsprechende Datenelement (210) eingebettet ist
einem Hash-Wert, der auf dem entsprechenden Datenelement (210) basiert.

12. Verfahren nach Anspruch 11, wobei das Wasserzeichen einschließt:
ein robustes Wasserzeichen, das so konfiguriert ist, dass eine Entfernung des robusten Wasserzeichens eine Beschädigung des entsprechenden Datenelements (210) bewirkt, und
ein fragiles Wasserzeichen, das so konfiguriert ist, dass eine Änderung des entsprechenden Datenelements (210) eine Beschädigung des fragilen Wasserzeichens bewirkt.

13. Verfahren nach Anspruch 8, wobei die Vielzahl von Datenelementen (210) eine Vielzahl von mindestens einem einschließt von: digital codiertem

Audioinhalt, digital codiertem Videoinhalt.

14. Verfahren nach Anspruch 8, wobei der Gesamtheitsparameter (240) mit einem Inhaltsverzeichnis verbunden wird, das zum Inhaltsmaterial gehört.

15. Speichermedium (130), das konfiguriert ist, um Inhaltsmaterial zu enthalten, wobei das Speichermedium (130) umfasst
eine Datenstruktur (200), umfassend:
eine Vielzahl von Datenelementen (210), wobei jedes Datenelement (210) eine zugehörige Sicherheitskennung (230) aufweist, und
einen Gesamtheitsparameter (240), der von einer Vielzahl der Sicherheitskennungen (230) abhängig ist; und
wobei
jede Sicherheitskennung (230) von der Vielzahl der Sicherheitskennungen (230) so konfiguriert ist, dass eine Änderung des Datenelements (210) eine Änderung der Sicherheitskennung (230) bewirkt, und
der Gesamtheitsparameter (240) eine Bestimmung erleichtert, ob in einer nachfolgenden Kopie mindestens eines Teils der Vielzahl von Datenelementen (210) eine Gesamtheit der Vielzahl von Datenelementen (210) vorhanden ist.

16. Speichermedium (130) nach Anspruch 15, außerdem umfassend eine Vielzahl von anderen Gesamtheitsparametern, wobei jeder von der Vielzahl der anderen Gesamtheitsparameter von einer zugehörigen Vielzahl von Sicherheitskennungen (230) abhängig ist.

17. Speichermedium (130) nach Anspruch 15, wobei der Gesamtheitsparameter (240) einen Hash-Wert einer Zusammensetzung aus der Vielzahl von Sicherheitskennungen (230) einschließt.

18. Speichermedium (130) nach Anspruch 15, wobei
die Sicherheitskennung (230) mindestens eines einschließt von:
einem Wasserzeichen, das im entsprechenden Datenelement (210) eingebettet ist
einem Hash-Wert, der auf dem entsprechenden Datenelement (210) basiert.

19. Speichermedium (130) nach Anspruch 18, wobei
das Wasserzeichen einschließt:
ein robustes Wasserzeichen, das so konfiguriert ist, dass eine Entfernung des robusten Wasserzeichens eine Beschädigung des entsprechenden Datenelements (210) bewirkt, und
ein fragiles Wasserzeichen, das so konfiguriert ist, dass eine Änderung des entsprechenden Datenelements (210) eine Beschädigung des fragilen Wasserzeichens bewirkt.

20. Speichermedium (**130**) nach Anspruch 15, wobei die Vielzahl von Datenelementen (**210**) eine Vielzahl von mindestens einem umfasst von: digital codiertem Audioinhalt und digital codiertem Videoinhalt.

21. Speichermedium (**130**) nach Anspruch 15, wobei der Gesamtheitsparameter (**240**) mit einem Inhaltsverzeichnis verbunden ist, das zum Datensatz gehört.

22. Codierer (**110**) von Inhaltmaterial, umfassend:
 einen Selektor (**112**), der konfiguriert ist, um eine Vielzahl von Datenelementen (**210**) zu wählen, die das Inhaltmaterial enthalten, um einen Datensatz mit einer Größe zu formen, die groß genug ist, um vor der nachfolgenden Übertragung des Datensatzes über einen Kommunikationskanal mit begrenzter Bandbreite abzuschrecken,
 wobei jedes von der Vielzahl von Datenelementen (**210**) eine zugehörige Sicherheitskennung (**230**) aufweist, die so konfiguriert ist, dass eine Änderung des Datenelements (**210**) eine Änderung der Sicherheitskennung (**230**) bewirkt,
 einen Binder (**116**), der konfiguriert ist, um auf der Basis einer Vielzahl der Sicherheitskennungen (**230**) einen Gesamtheitsparameter (**240**) zu erzeugen, der eine Bestimmung erleichtert, ob eine Gesamtheit der Vielzahl von Datenelementen (**210**) vorhanden ist, und
 einen Rekorder (**114**), der konfiguriert ist, um den Gesamtheitsparameter (**240**) mit der Vielzahl von Datenelementen (**210**) zu kombinieren, um einen auf sich selbst zurückweisenden Datensatz zu formen, der auf ein Aufzeichnungsmedium gespeichert wird.

23. Codierer (**110**) nach Anspruch 22, wobei der Binder (**116**) ferner konfiguriert ist, um den Gesamtheitsparameter (**240**) mit einem Inhaltsverzeichnis zu verbinden, der zum Datensatz gehört.

24. Codierer (**110**) nach Anspruch 22, wobei der Binder (**116**) ferner konfiguriert ist, um eine Vielzahl von anderen Gesamtheitsparametern zu erzeugen, wobei jeder von der Vielzahl der anderen Gesamtheitsparameter auf einer zugehörigen Vielzahl von Sicherheitskennungen (**230**) basiert, der Rekorder (**114**) ferner konfiguriert ist, um die Vielzahl der anderen Gesamtheitsparameter mit dem Datensatz zu kombinieren, um eine Verhinderung der Verarbeitung jedes Datenelements (**210**) in Abwesenheit einer Gesamtheit des Datensatzes zu erleichtern.

25. Decoder (**120**) von Inhaltmaterial, umfassend:
 einen Renderer (**122**), der konfiguriert ist, um zu empfangen:
 einen Gesamtheitsparameter (**240**), der dem Inhaltmaterial entspricht, und

eine Vielzahl von Sicherheitskennungen (**230**), auf denen der Gesamtheitsparameter (**240**) basiert, wobei jede Sicherheitskennung (**230**) ein Datenelement (**210**) des Inhaltmaterials entspricht, einen Gesamtheitsprüfer (**126**), dessen Betrieb mit dem des Renderers (**122**) gekoppelt ist und der konfiguriert ist, um einen Gesamtheitswert auf der Basis der Vielzahl von Sicherheitskennungen (**230**) zu bestimmen, und eine Wiedergabe des Inhaltmaterials von der Quelle abhängig von einer Entsprechung zwischen dem Gesamtheitswert und dem Gesamtheitsparameter (**240**) zu verhindern.

26. Decoder (**120**) nach Anspruch 25, wobei: der Renderer (**122**), ferner konfiguriert ist, um den Gesamtheitsparameter (**240**) auf der Basis einer Zufallsauswahl aus einem Satz von Gesamtheitsparametern zu empfangen, wobei jeder Gesamtheitsparameter (**240**) des Gesamtheitsparametersatzes einen zugehörigen Satz von Sicherheitskennungen (**230**) aufweist.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

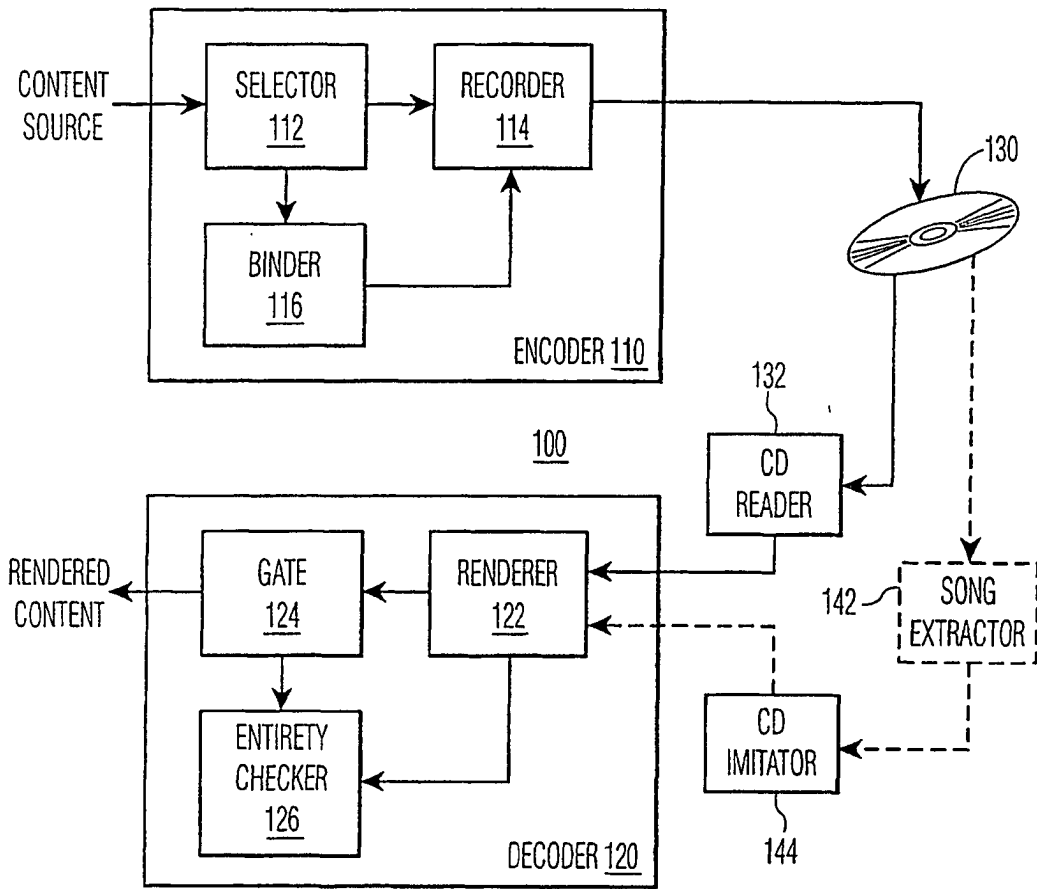


FIG. 1

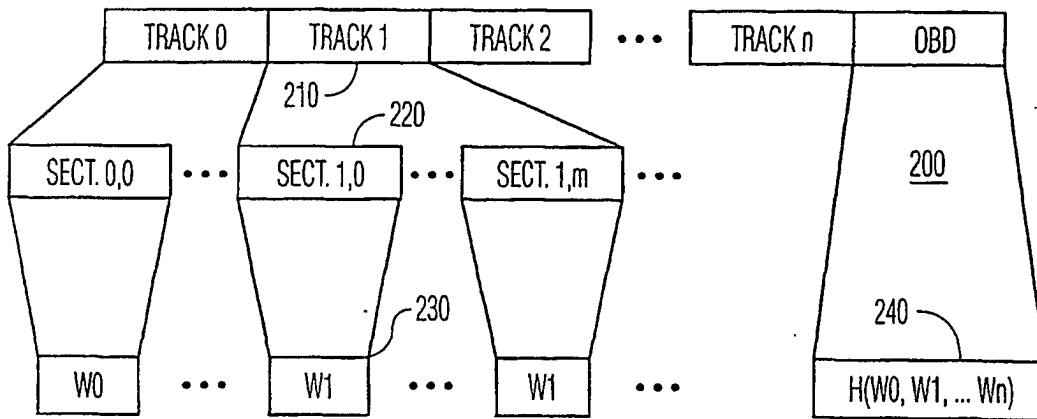


FIG. 2

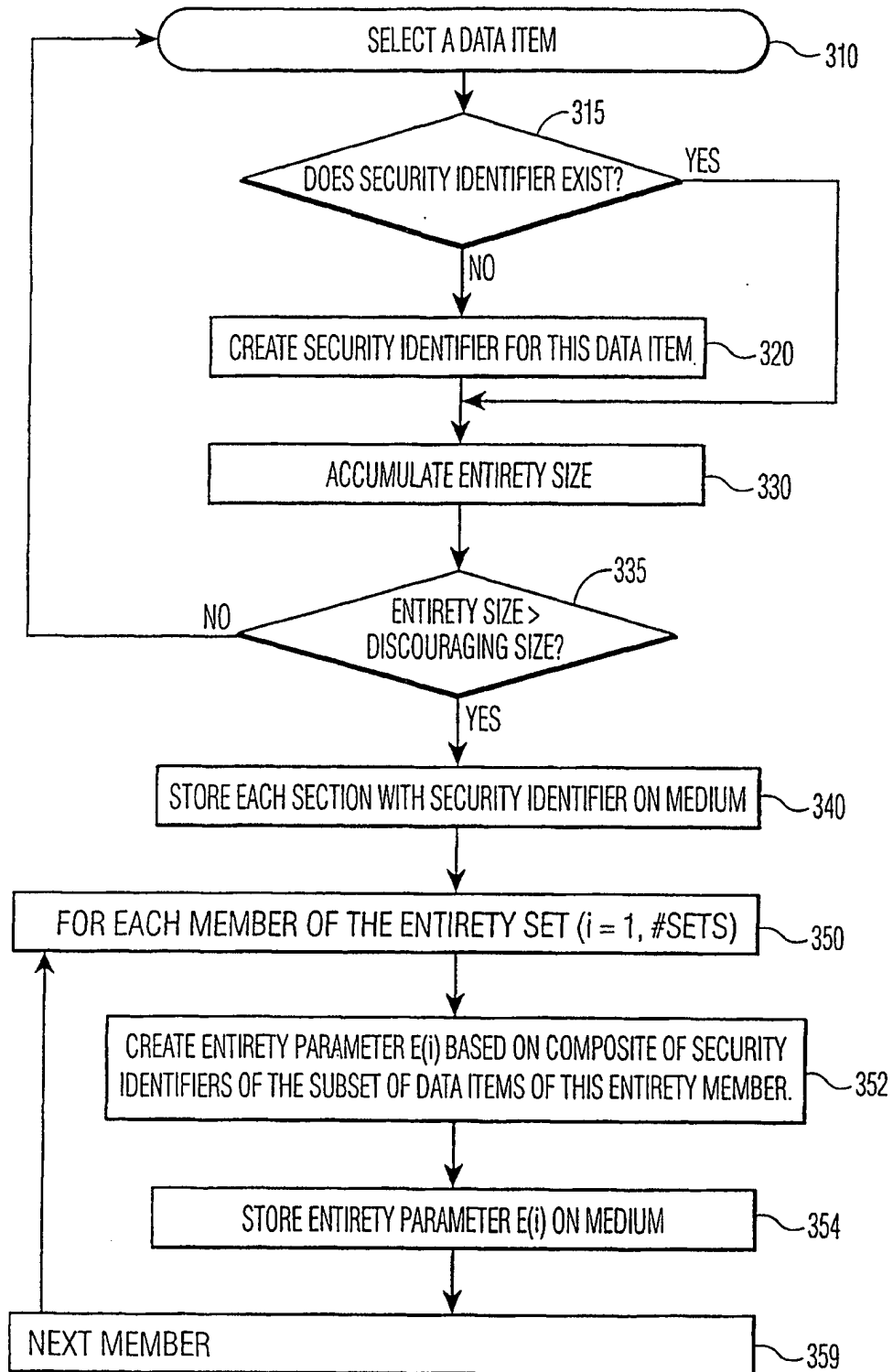


FIG. 3

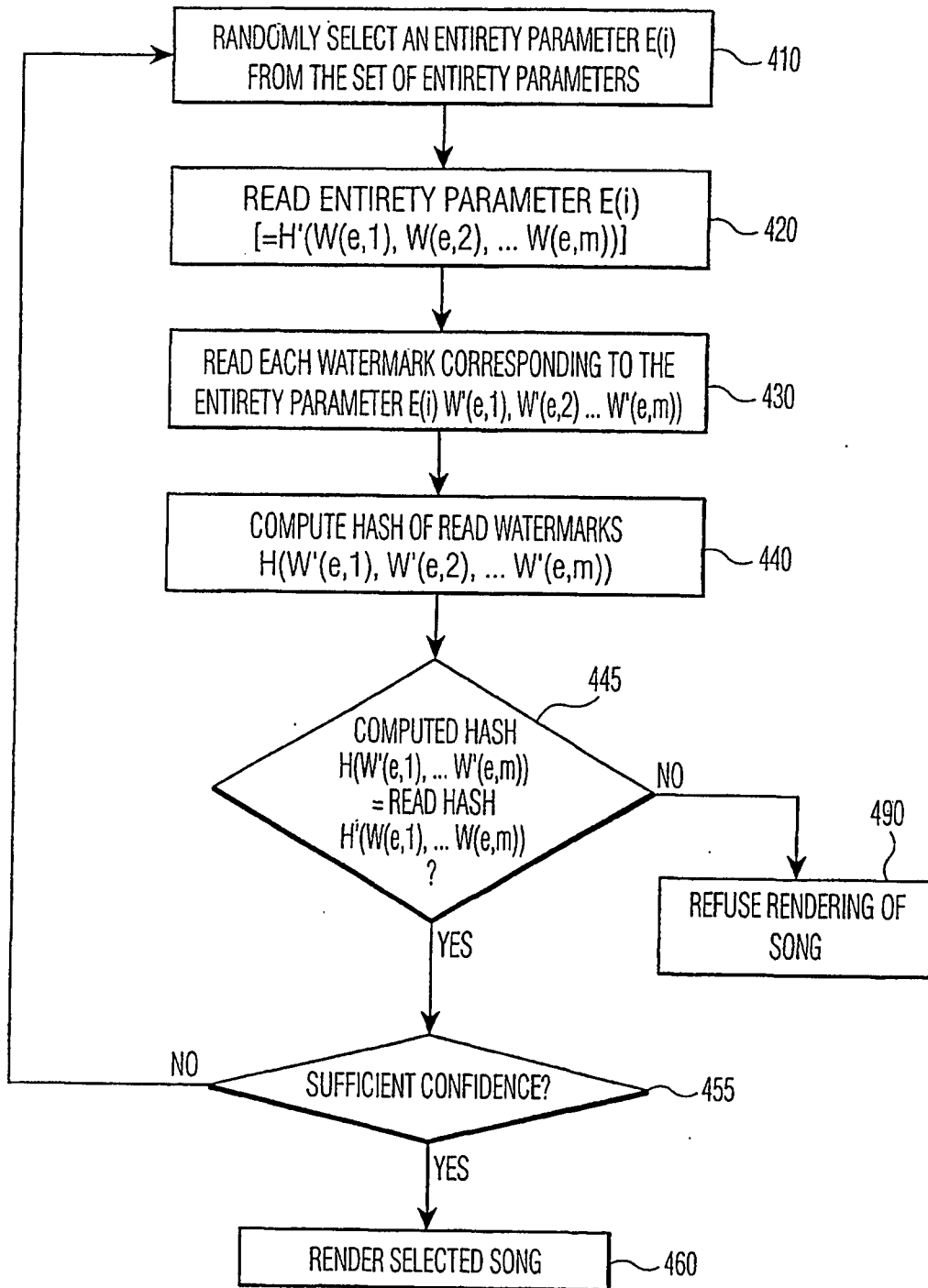


FIG. 4