

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
6. März 2003 (06.03.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/019552 A1

(51) Internationale Patentklassifikation⁷: **G11B 20/00**

(21) Internationales Aktenzeichen: PCT/EP02/09392

(22) Internationales Anmeldedatum:
22. August 2002 (22.08.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 40 237.6 22. August 2001 (22.08.2001) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **BRAINSHIELD TECHNOLOGIES, INC.**
[US/US]; 900 Third Avenue, New York, NY 10022 (US).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): **WITTKÖTTER, Erland** [DE/DE]; Koppelstrasse 19, 32257 Bünde (DE).

(74) Anwälte: **BEHRMANN, Niels** usw.; Hiebsch Peege Behrmann, Heinrich-Weber-Platz 1, 78224 Singen (DE).

(81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten (regional): ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

- hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
- hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii) für alle Bestimmungsstaaten

Veröffentlicht:

- mit internationalem Recherchenbericht
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

[Fortsetzung auf der nächsten Seite]

(54) Title: COPY PROTECTION DEVICE

(54) Bezeichnung: VORRICHTUNG ZUM KOPIERSCHUTZ

(57) Abstract: The invention relates to a device for copy protection, particularly of optical data carriers such as CD/DVD. By placing additional coding data within the redundancy area of the logical and/or physical data carrier format, the data carriers are provided with additional identifying characteristics such as watermarks. The additional coding data is not outputted by the playback and reproduction unit due to automated error correction. By bypassing said error correction, an appropriate verification unit can extract the coding data from the random error data shown as digital white noise. Copying of the data carrier by illegal, professional copying devices would lead to the removal of said additional coding and would thereby be a clear criterion for an illegal copy.

(57) Zusammenfassung: Die Erfindung betrifft eine Vorrichtung zum Kopierschutz von insbesondere optischen Datenträgern wie CD/DVD. Durch das Aufbringen von zusätzlichen Kodierungsdaten innerhalb des Redundanzbereiches des logischen und/oder physikalischen Datenträgerformates erhält der Datenträger zusätzliche identifizierende Kennzeichen, wie Wasserzeichen. Aufgrund der automatisierten Fehlerkorrektur werden die zusätzlichen Kodierungsdaten von der Abspiel- und Darstellungseinheit nicht ausgegeben. Eine geeigneten Verifikationseinheit kann durch das Umgehen der Fehlerkorrektur die Kodierungsdaten aus den zufälligen Fehlerdaten, das sich als digitales weisses Rauschen zeigt, extrahiert werden. Das Kopieren des Datenträgers durch illegale, professionelle Kopiereinrichtungen würde zu einem Entfernen dieser zusätzlichen Kodierung führen, und damit ein klares Kriterium für eine illegale Kopie sein.



WO 03/019552 A1



Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Vorrichtung zum Kopierschutz

Die vorliegende Erfindung betrifft eine Vorrichtung zum Kopierschutz von digitale Dokumente tragenden Datenträgereinheiten, insbesondere von optisch lesbaren Datenträgern wie CDs oder DVDs, mit den Merkmalen des Oberbegriffs des Patentanspruchs 1.

Eine derartige Vorrichtung ist beispielsweise aus der deutschen Offenlegungsschrift 43 11 683 bekannt.

Dieser Schrift liegt das sich zunehmend verschärfende Problem der planmäßigen Fälschung bzw. Piraterie von urheberrechtlich wertvollem Inhalt auf gattungsgemäßen Datenträgereinheiten, etwa CDs oder DVDs, zugrunde. Im Gegensatz zu von Einzelpersonen in Einzelstücken bzw. Kleinstauflagen gefertigten Kopien mittels sogenannter beschreibbarer Datenträgereinheiten, welche bereits aufgrund des Charakters der benutzten Schreibmedien problemlos als Fälschungen erkannt werden können, besteht gerade bei in großer Auflage und mittels professioneller Fertigungstechnik gefertigten Datenträgerkopien das generelle Problem, dass so hergestellte Fälschungen, insbesondere bei Verifikationsversuchen außerhalb einer Laborumgebung, nur schwer als Fälschungen erkennbar sind und dementsprechend ein wirkungsvolles Vorgehen gegen Piraterieversuche erschweren.

Beim gattungsbildenden Stand der Technik wird dieses Problem dadurch gelöst, dass durch geeignete Veränderung der Signal- bzw. Datenträgerkennungen auf der betreffenden Datenträgereinheit, also etwa der Pits bzw. Lands auf einer CD, eine charakteristische und damit authentifizierende Kennzeichnung eines -- legal gefertigten -- Datenträgers hergestellt werden kann, die sich typischerweise bei einer illegal gefertigten Kopie nicht so übernehmen lässt und damit als Fälschungshinweis wirkt. Im gattungsgemäßen Stand der Technik gemäß DE 43 11 683 geschieht dies durch vorbestimmte Variationen der Tiefe und Breite der Datenträgerkennungen, die

sich entsprechend durch geeignete visuelle Prüfungsverfahren, insbesondere auch mit bloßem Auge oder mit einem Mikroskop, erkennen lassen, während gleichzeitig die zu Authentifizierungszwecken planmäßig vorgenommenen Modifikationen an den Datenträgerkennungen den eigentlichen digitalen Inhalt, also etwa das Musikstück, unbeeinflusst lassen.

Der Umstand, dass derartige Modifikationen nicht ohne weiteres für eine (illegale) Kopie übernommen werden können, liegt darin, dass illegale Kopien typischerweise dadurch gefertigt werden, dass zunächst in der ansonsten bekannten Weise der digitale (Nutz-) Inhalt des Datenträgers ausgelesen wird und mit diesen Nutzdaten dann wiederum eine neue Datenträgermatrize für das Herstellen der Fälschkopien erzeugt wird. Da jedoch die gattungsgemäß vorgenommenen Modifikationen der Datenträgerkennungen nicht inhaltswirksam sind, sich also beim regulären Auslesen des digitalen Inhalts der Datenträgereinheit nicht bemerkbar machen, werden diese nicht entsprechend zur Herstellung der (Fälschungs-) Matrize übernommen.

Gleichwohl erscheint es bei dem gattungsgemäßen Stand der Technik für eine weite Verbreitung prinzipiell problematisch, dass das Herstellen der schutzerhöhenden visuell sichtbaren Markierungen mit vergleichsweise hohem Fertigungsaufwand verbunden ist, dementsprechend beträchtliche Investitionen in eine Fertigungsinfrastruktur verlangt und damit nicht allen potentiell bedürftigen Interessentenkreisen zugänglich ist. Darüber hinaus besteht ein prinzipielles Problem der aus der DE 43 11 683 bekannten Technologie darin, dass insbesondere mit gängigen Lesemitteln für eine CD oder DVD die zu Sicherungszwecken vorgenommenen Modifikationen nicht elektronisch bzw. digital les- und damit auswertbar sind. Ersichtlich findet bereits eine Unterdrückung der (sich lediglich visuell auswirkenden) Modifikation gemäß gattungsgemäßigem Stand der Technik durch den rein digitalen Lese- bzw. Abtastvorgang der gattungsgemäß beschriebenen CD statt. Insbesondere dieser Umstand macht dann jedoch das planmäßige Prüfen und Testen von DVDs, insbesondere auch bei schlechter Umgebungshelligkeit und bei einer großen

Stückzahl zu testender potentieller Fälschungen, aufwendig und wenig praktikabel.

Auch ist damit zu rechnen, dass die Produzenten illegaler CDs innerhalb kurzer Zeit nach Bekanntgabe eines sichtbaren Sicherheitsmerkmals ebenfalls in der Lage sein werden, dieses Sicherheitsmerkmal zu kopieren. Es besteht dann die Gefahr, dass die Zuverlässigkeit dieses Verfahrens nur von begrenzter Zeit sein wird. Nach einer Verbreitung der Technologie bei den CD-Piraten würde die Wirkung dieses Sicherheitsmerkmals in sein Gegenteil verkehrt, so dass bei den Käufern die Sicherheit leicht vorgetäuscht werden kann, dass es sich beim Produkt um kein Piratenprodukt handelt, obwohl es als illegale Kopie hergestellt worden ist.

Aufgabe der vorliegenden Erfindung ist es daher, eine Vorrichtung zum Kopierschutz von digitale Dokumente tragenden Datenträgereinheiten nach dem Oberbegriff des Patentanspruchs 1 dahingehend weiterzuentwickeln, dass insbesondere auch eine vollautomatisierte bzw. computerisierte und digitale Überprüfung auf unberechtigte Kopie bzw. Fälschung möglich ist, die ferner keine sichtbare und leicht feststellbare Sicherheitsmerkmale aufweist, insbesondere auch in einem mobilen bzw. portablen Umfeld eingesetzt werden kann, wobei gleichzeitig die Voraussetzungen für das Herstellen derartiger mit Schutz erhöhender Wirkung versehener Datenträgereinheiten im Hinblick auf die notwendige Herstellungsinfrastruktur vereinfacht sind.

Die Aufgabe wird durch die Vorrichtung mit den Merkmalen des Patentanspruchs 1 gelöst; zusätzlich wird Schutz beansprucht für eine Verwendung der Vorrichtung nach Patentanspruch 1 auf die besonders relevanten Anwendungsfälle CD und DVD, ferner für ein Verfahren zum Herstellen einer digitalen Datenträgereinheit, die sich zum Betrieb der Vorrichtung gemäß Hauptanspruch eignet, sowie ein Verfahren zum Verifizieren von potentiell gefälschten Datenträgern, welches sich zum Betrieb der Vorrichtung gemäß Hauptanspruch eignet. Jeweils vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen beschrieben.

In erfindungsgemäß vorteilhafter Weise werden durch die Mittel zum Aufbringen der zusätzlichen Codierung solche individualisierenden Merkmale auf die Datenträgereinheit aufgebracht, die nicht inhaltswirksam sind und damit insbesondere auch bei einem bestimmungsgemäßen Abspielen bzw. Darstellen des digitalen Inhaltes keine Inhaltsbeeinflussung bewirken. Gleichzeitig ermöglicht dadurch jedoch die zusätzliche Codierung, dass bei einer unberechtigten (d. h. auf den digitalen Inhalt beschränkten) Kopie der Datenträgereinheit mit nachfolgender Vervielfältigung genau diese zusätzliche Codierung im unberechtigten Kopiervorgang unberücksichtigt bleibt und damit für spätere Verifizierungszwecke als zuverlässiges und unmittelbar aktionsfähiges Unterscheidungsmerkmal zugänglich ist. Diese Technologie steht bewusst im Gegensatz zu sonstigen, möglichen Codierungsdaten, die Bestandteil des digitalen Inhalts sind und damit auch über einen unberechtigten Auslese- und Kopiervorgang ausgelesen und kopiert werden.

In erfindungsgemäßer Weise und in Abgrenzung vom gattungsbildenden Stand der Technik geschieht die Feststellung einer unberechtigten Kopie dadurch, dass die erfindungsgemäßen Verifizierungsmittel einen unmittelbaren und damit automatisierten, einer maschinellen Verarbeitung zugänglichen Überprüfungsvorgang durch unmittelbaren Zugriff auf die zusätzliche Codierung erlauben, nicht nur mit der Möglichkeit, das Vorliegen oder Nicht-Vorliegen der zusätzlichen Codierung festzustellen und damit unmittelbar den Schluss auf eine Fälschung zuzulassen, sondern insbesondere auch eine mögliche Variation oder Veränderung der zusätzlichen Codierung gegenüber einer vorbestimmten und erfindungsgemäß gespeicherten (und damit gesichert abgelegten) ursprünglichen Codierung festzustellen. Hiermit wären insbesondere auch solche (fortgeschrittenen) Missbrauchsversuche unmittelbar erkennbar, bei welchen bereits eine (teilweise oder variierte) Kopie auch der zusätzlichen Codierung im Rahmen eines Missbrauchsversuchs vorgenommen worden ist. Wichtig ist dabei, dass die Verifizierungsmittel den unmittelbaren Zugriff auf die zusätzliche Codierung vornehmen

können und dabei traditionelle Mechanismen, die typischerweise dafür sorgen, dass bei einem regulären Abspielen bzw. Auslesen des digitalen Inhaltes die zusätzliche Codierung unberücksichtigt bleibt und keinen Einfluss auf den Inhalt nimmt, nämlich ansonsten bekannte Fehlerkorrektur- oder Filtermodule, umgangen werden, so dass für den erfindungsgemäßen Verifizierungsvorgang genau diese Unterscheidung mittels der erfassten zusätzlichen Codierung möglich ist. Die generelle Intransparenz eines solchen Vorgehens aus Nutzer- oder Kopiersicht macht einen wesentlichen Vorteil dieser Technologie aus.

Der Umstand, dass erfindungsgemäß eine automatisierbare, digitale Verifizierung durch das direkte Auslesen der zusätzlichen Codierung möglich ist, gestattet es dann, auf einfache und insbesondere auch mobile und portable Weise in großen Umfange Überprüfungen bei potentiell verdächtigen Datenträgereinheiten vorzunehmen, so dass insbesondere auch geeigneten Vollstreckungsbehörden ein Werkzeug zur Verfügung steht, mit welchem unmittelbar, beweisbar und kausal eine rechtswidrige Verletzung feststellbar ist, welche dann die Grundlage für unmittelbar folgende, wirksame Vorgehensmaßnahmen gegen Verletzer, z. B. Durchsuchungen, welche nur bei einem konkreten Nachweis einer Rechtswidrigkeit möglich sein können, erlaubt.

In einer bevorzugten Ausführungsform der Erfindung kann die Verifizierungseinheit publiziert werden, da durch Public-/Private Key Verfahren eine Beziehung innerhalb einer zusätzlichen Kodierung hergestellt werden kann, ohne dass die so bekannt gegebenen Informationen zu einer Verringerung des Sicherheitsverfahrens bzw. zu dessen Kompromittierung führt.

Im Rahmen der vorliegenden Erfindung umfasst dabei der Begriff der digitalen Dokumente oder des elektronischen Dokuments nicht nur die aus aktueller Sicht besonders fälschungsgefährdeten Musik- (Audio-) und Video-Dateien, sondern insbesondere auch (interaktive) Computerspiele, Computersoftware, digitale Text-,

Bild- oder Multimediatdaten, die typischerweise urheberrechtliche Bedeutung besitzen und damit einen schützenswerten Besitzstand darstellen.

Als Datenträger der vorliegenden Erfindung eignet sich nicht nur die beispielhaft bereits herangezogene CD, DVD oder Mini-Disc; potentiell geeignet für die vorliegende Erfindung sind dabei auch Bänder mit Digitaldaten (z. B. DAT) oder sonstige digitale platten- oder bandförmige Speichermedien, die typischerweise zur Distribution urheberrechtlich wertvoller digitaler Dateien benutzt werden, eingeschlossen zukünftig denkbare holographische od. dgl. Speichermedien.

Als zusätzliche Codierung im Rahmen der vorliegenden Erfindung lässt sich zunächst eine grobe Zweiteilung vornehmen: Zum einen ist eine erfindungsgemäße zusätzliche Codierung im Rahmen der logischen Struktur einer Datenträgereinheit möglich, wobei als logische Struktur diejenige Formatstruktur bzw. Organisation der Datenträgereinheit gemeint ist, wie sie in Form von Frames, Sektoren, Tracks usw. in jeweils vorgesehener Weise vorliegt und typischerweise durch Normen od. dgl. Konventionen vorbestimmt ist (etwa Red Book für CDs bzw. CD-DA bzw. Musik CDs im engeren Sinne oder Yellow-Book für CD-XA bzw. CD-ROMs).

Innerhalb einer derartigen logischen Struktur ist das Vorsehen der erfindungsgemäßen zusätzlichen Codierung auf vielfältige Weise möglich, etwa im Nutzdatenbereich (sofern durch zusätzlich vorhandene Korrekturmechanismen der originale digitale Inhalt im Ergebnis unverändert bleibt, d. h. original rekonstruiert, korrigiert, berechnet oder interpoliert wird), ferner in (typischerweise ohnehin redundant vorgesehenen) Fehlerkorrektur- und/oder Kontrolldatenbereichen (auch sog. Subcode-Datenbereichen), ferner in ggf. vorgesehenen zusätzlichen Header-Daten oder in Lead-In-Lead-Out-Datenbereichen (d.h. in Eingangs- bzw. Ausgangsbereichen) usw.. Richtig ist, dass bei einem Aufbringen der zusätzlichen Codierung auf diese Weise erfindungsgemäß die Bedingung jeweils erhalten bleibt, dass die für einen Nutzer auszugebenden digitale Inhaltssignale von

dieser zusätzlichen Codierung unbeeinflusst bleibt, d. h. die entsprechenden gezielt vorgenommenen zusätzlichen Codierungsmaßnahmen in der logischen Struktur entweder im Rahmen der vorhandenen Fehlerkorrektur- und Redundanzstrukturen, was Inhalt anbelangt, unterdrückt werden, oder auf sonstige Weise unberücksichtigt bleiben.

Die im Rahmen der logischen Struktur unterdrückten zusätzlichen Daten können vor der Ausgabe einerseits durch die inhärenten Redundanzdaten korrigiert werden, andererseits können Datenfelder ohne weitere Fehlerkorrektur genutzt werden, die laut der entsprechenden Spezifikation für zukünftige Erweiterungen des Standards vorgesehen sind und auch nur von diesen erweiterten Formaten aktiv verwendet werden, wie beispielsweise die Subcode-Channel R bis W in den entsprechenden Kontrolldatenbereich einer CD.

Dagegen besteht ein zweiter wesentlicher Lösungsaspekt des Vorsehens der erfindungsgemäßen zusätzlichen Codierung darin, diese innerhalb der physikalischen Struktur der Datenträgereinheit, jedoch außerhalb der logischen Struktur vorzusehen. Dies bedeutet, dass erfindungsgemäß Modifikationen der Datenträgerkennungen, für Leseeinheiten lesbar, vorgenommen werden, die außerhalb der Format- und Organisationsstruktur der Datenträgereinheit liegen. Dies könnten beispielsweise zusätzlich eingebrachte, von einem gattungsgemäßen (Laser-) Lesekopf detektierbare Pits bzw. Lands oder Abweichungen von diesen sein, welche außerhalb der logischen Formatstruktur einer CD oder DVD liegen, oder aber solche Datenkennungen, die hinsichtlich der Abmessungen von Pits oder Lands gegenüber dem standardisierten Format abweichen, und damit nicht mehr als normgemäße digitale Kennungen gelten, gleichwohl jedoch (und in Abgrenzung vom gattungsbildenden Stand der Technik) von der typischen Lesesensorik einer CD oder DVD als Signale erfasst und zur Auswertung im Rahmen der Verifizierung bzw. durch die Verifizierung detektiert werden können. Als typisches Realisierungsbeispiel sind relativ zu Pits oder Lands einer CD physikalisch sehr kurze Markierungen (Kennungen) auf der

Datenträgeroberfläche, die zu entsprechend anderen (kurzen) Detektionssignalen führen und signalmäßig eher Defektcharakter haben, so dass sie von traditionellen Fehlerkorrekturmechanismen beim Abspielen unterdrückt bzw. ausgeblendet werden, dagegen jedoch durch die erfindungsgemäßen Verifizierungsmittel les- oder für Verifizierungszwecke auswertbar sind.

Im Rahmen der vorliegenden Erfindung ist zudem die Abspiel- bzw. Darstellungseinheit ein Mittel zum Ausgeben, zum Abspeichern, zum Kopieren, zum Verarbeiten und zum Transferieren von Daten über ein Datenübertragungsnetzwerk wie das Internet, das als auch typische Consumer-Abspieleinheit zur Wiedergabe des digitalen Inhalts zu verstehen, also im Fall von CD oder DVD ein jeweiliger handelsüblicher CD-, DVD-Player, oder von CD-ROM bzw. DVD-RO, welche in handelsüblichen PCs enthalten sind, und welcher in ansonsten bekannter Weise eine (Laser-) Abtasteinheit mit nachgeschalteter Digitalisierung, Pufferung und Fehlerkorrektur aufweist, um selbst Datenträger schlechter Qualität noch in brauchbarer Weise wiederzugeben. In diesem Kontext bestehen erfindungsgemäße Fehlerkorrektur- und Filtereinheiten typischerweise in bekannten Mechanismen, (durch Pressfehler bedingte) Daten- oder Oberflächenfehler, eingeschlossen Kratzer, Staub, Haare, Fingerabdrücke od. dgl., auszugleichen, wobei neben mechanischen Effekten hier vor allem die normgemäß für CD und DVD vorgesehenen Fehlerkorrekturen, basierend auf einem sehr hohen redundanten Datenvolumen, vorgesehen sind. Gängige Fehlerkorrekturen beginnen etwa bei der CRC, bei der geeigneten Codierung (ECC bzw. EDC) bzw. bei konkret verwendeten Rekonstruktionsverfahren wie CIRC oder ACIRC.

Je nach Vorgehensweise der vorliegenden Erfindung bestehen dabei die erfindungsgemäßen Aufbringungsmittel in (typischerweise softwaretechnisch implementierten) Vorrichtungen zum Einbringen bzw. Verankern der zusätzlichen Codierung für die Herstellung einer CD oder DVD (d. h. es findet dann ein gemeinsamer Schritt zur Herstellung des Glasmasters der Matrizie als Herstellungsvorlage statt), oder aber das Aufbringen der

zusätzlichen Codierung erfolgt unabhängig von dem ansonsten bekannten Herstellen der Matrize mit dem digitalen Originalinhalt, durch vorheriges oder nachträgliches Manipulieren entweder der Matrize oder des jeweiligen gepressten Endprodukts, etwa mittels Laser oder Magneteinheit zum Herstellen der erfindungsgemäßen Modifikationen der physikalischen Struktur der Datenträgereinheit.

Insoweit entspricht dann auch das erfindungsgemäße Vorgehen dem Herstellen eines digital wirksamen Wasserzeichens zum Kopierschutz bzw. zur Authentizitätskontrolle, wobei weiterbildungsgemäß durch geeignete inhaltliche Zuordnung bzw. Verknüpfung von Daten mit der zusätzlichen Codierung eine Mehrzahl derartiger digitaler Wasserzeichen ermittel- und feststellbar ist, so dass, wie erfindungsgemäß vorgesehen, eine hierarchisch wirksame Sicherung über mehrere Sicherheitsebenen (bevorzugt unterschieden durch einen Geheimhaltungsgrad der jeweiligen digitalen Verknüpfungen mit der zusätzlichen Codierung) möglich sind.

Wie weiterbildungsgemäß vorgesehen, ist die Realisierung dieser Weiterbildung der Erfindung besonders elegant, wenn zusätzlich eine jede CD individualisierender Datensatz, z. B. in Form einer ansonsten bekannter Weise herzustellender Seriennummer, vorliegt und damit bereits in der Analogie zur Erkennung von Falschgeld eine Überprüfung auf das mehrfache Vorliegen derselben digitalen Kennung, hergeleitet aus Seriennummer und zusätzlicher Codierung, möglich ist.

Dieser Gedanke lässt sich bei Konzeption der einzelnen Wasserzeichen-Erfassungs- und Berechnungsmethoden als System bis hin zu einer Plattform entwickeln, welche dann nahezu beliebige, weiter Schutz erhöhend wirksame Kombinationen und Schutzebenen gestattet, so dass selbst dann, wenn die erfindungsgemäße Sicherheitsarchitektur durch auf tieferen Ebenen wirksame Kopiermechanismen teilweise unterlaufen werden sollte, hier trotzdem das zuverlässige Erkennen von Fälschungen möglich ist.

Im Ergebnis wird durch die vorliegende Erfindung erstmals die Möglichkeit geschaffen, mit geringem zusätzlichen herstellungstechnischen und vor allem in der Überwachung prüftechnischen Aufwand, unberechtigte Kopien auch von professionell in großer Stückzahl hergestellten Datenträgereinheiten zuverlässig zu erkennen und damit zeitnah Bekämpfungsmaßnahmen auszulösen, ohne dass es zum Nachweis einer widerrechtlichen Kopie, wie im Stand der Technik notwendig, besonderer optisch wirksamer Instrumente oder eines speziell geschulten Auges bedarf, oder gar in einer Laborumgebung erst aufwendig der Kopiernachweis geführt werden muss. Vielmehr gestattet es die Vorrichtung gemäß der vorliegenden Erfindung, eine einfach automatisierbare Verifikationsinfrastruktur herzustellen, welche das Potential bietet, das letztendlich auch für die Allgemeinheit schädliche da leistungshinderliche Kopierunwesen, gerade auf dem populären CD- und DVD-Markt, zu unterdrücken.

Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung bevorzugter Ausführungsbeispiele sowie anhand der Zeichnungen; diese zeigen in:

- Fig. 1: ein schematisches Blockschaltbild der in dem Hauptanspruch enthaltenen Herstellungs-, Abspiel und Verifizierungseinheiten gemäß einer ersten, bevorzugten Ausführungsform der Erfindung,
- Fig. 2: ein schematisches Blockschaltbild einer Abspieleinheit und einer Verifikationsvorrichtung gemäß einer ersten, bevorzugten Ausführungsform der Erfindung,
- Fig. 3: eine schematische Darstellung der CD/DVD mit den Lead-In/Lead-Out und Nutzdaten Bereichen,
- Fig. 4: einen exemplarischer Auszug aus der EFM Codetabelle,
- Fig. 5: eine schematische Darstellung zur Konversion von Bytes zu den auf der CD enthaltenen Pits,

- Fig. 6: eine schematische Darstellung der CD/DVD mit einer Beschreibung der Pits/Lands und von darin enthaltenen defektartigen Signalelementen,
- Fig. 7: einen schematischer Aufbau eines einzelnen Frames auf einer CD,
- Fig. 8: einen schematischer Aufbau der Datenbereiche eines Sektors einer CD,
- Fig. 9: ein schematischer Aufbau eines Subcode Channel Bytes auf einer CD,
- Fig. 10: ein schematischer Aufbau eines Subcode Channel Q über einen Sektor,
- Fig. 11: ein schematischer Aufbau einer Musik CD (CD-DA), der aus Musik-Tracks aufgebaut ist,
- Fig. 12: eine schematische Darstellung der CD mit den zusätzlichen Header Daten entsprechend des CD-ROM (Yellow-Book) Formates,
- Fig. 13: ein schematisches Blockschalbild der Einheiten, die zur Herstellung der CD mit den zusätzlichen Kodierungen gemäß einer ersten, bevorzugten Ausführungsform der Erfindung geeignet sind,
- Fig. 14: ein schematisches Blockschalbild der Komponenten mit den einzelnen Einheiten, die zur Herstellung der CD mit den zusätzlichen Kodierungen gemäß einer bevorzugten Ausführungsform der Erfindung geeignet sind,
- Fig. 15: eine schematische Darstellung von zusätzlichen Kodierungen, die in Form von Wasserzeichen, einer Seriennummer oder dergleichen auf einer CD enthalten sein können,
- Fig. 16: ein schematisches Blockschalbild zum Aufbau des Treibers zum Lesen der zusätzlichen digitalen Kodierung gemäß einer ersten, bevorzugten Ausführungsform für die Erfindung,
- Fig. 17: ein schematisches Blockschalbild zur Beschreibung einer Wasserzeichentrenneinheit, mit der mehrere Wasserzeichen aus den zusätzlichen Kodierungsdaten, die auf der CD enthalten sind gebildet werden kann,

- Fig. 18: ein schematisches Blockschaltbild eines Verfahrens zur Herstellung eines Wasserzeichens, bei der ein Wasserzeichen mit einer Serien-Nummer datenmäßig verbunden ist,
- Fig. 19: ein schematisches Blockschaltbild eines Verfahrens zur Auswertung eines Wasserzeichens, bei der ein Wasserzeichen mit einer Serien-Nummer datenmäßig verbunden ist,
- Fig. 20: ein schematisches Blockschaltbild einer Sicherheitsplattform, bei der sicherheitserhöhende Komponenten ausgetauscht werden können.

Die Fig. 1 zeigt das schematische Blockschaltbild einer ersten bevorzugten Ausführungsform mit den wesentlichen Haupt-Funktionskomponenten der vorliegenden Erfindung, nämlich eine Herstellungseinheit (1) mit einerseits Mitteln zum Aufbringen von digitalen Dokumenten, realisiert in ansonsten bekannter Weise als Technologie zum Produzieren der digitalen Datenträger, etwa mittels Glasmaster, und andererseits Mittel (3) zum Aufbringen der zusätzlichen Codierung, wobei diese Mittel entweder unmittelbar auf die Datenträgereinheit (10) wirken, oder aber mittels der Verbindung (7) zur Einheit (2), bei der an geeigneter Stelle in der logischen Struktur des digitalen Dokumentes vor dem abschließenden Erstellen der Datenträgereinheit die zusätzlichen Codierungen in die Aufbringungseinheit (2) eingebracht werden.

Wie zudem aus der Fig. 1 erkennbar ist, wirkt die erfindungsgemäß produzierte Datenträgereinheit mit digitalem Dokument und zusätzlicher Codierung in ansonsten bekannter Weise zusammen mit Mitteln zur Ausgabe (15), die etwa beispielhaft als CD- oder DVD-Spieler realisiert sein können und, typischerweise durch Mischung von Hardware- und/oder Softwarekomponenten, den reinen Inhalt des digitalen Dokumentes wiedergeben und dabei physische und/oder logische Fehler oder Modifikationen ausblenden, korrigieren und interpolieren. Zusätzlich sind zur Benutzung durch jeweils autorisierte Benutzer im Rahmen der Erfindung Mittel zur Verifizierung (20) vorgesehen, die, in nachfolgend zu

beschreibender Weise, eine deutlich über die Abspielmittel (15) hinausgehende Funktionalität aufweisen und insbesondere in der Lage sind, im Rahmen der Erfindung die zusätzliche Codierung in der gewünschten Weise zum Auffinden von unberechtigt hergestellten Kopien zu extrahieren.

Zudem verdeutlicht Fig. 1, das die Abspiel und Darstellungseinheit (15) durch Mittel zur Kommunikations- und Betriebssteuerung (9) erweitert werden kann, die die Mittel zur Verifizierung (20) in einer vor Manipulation abgesicherten Weise abfragen kann, ob der Datenträger ein autorisiertes Exemplar ist. Außerdem können über die Einheit (20) weitere Steuerungsinformationen aus den zusätzlichen Kodierungsdaten extrahiert und an die Kommunikations- und Betriebssteuerung (9) übertragen werden, wie z.B. die Beschränkung der Benutzungsrechte, wie eine Beschränkung bei der Anzahl der Kopien, die Legal von dem Datenträger erzeugt werden dürfen oder dem Recht, das digitale Dokument eine festgelegte Anzahl im Internet zum Tausch anzubieten oder dergleichen. Die Ausgabemittel würden diese dem elektronischen Dokument zugeordnete Nutzungsrechte bzw. Nutzungsrechtsbeschränkungen innerhalb des Abspiel-, Darstellungs-, Kopier- oder Datenübertragungsmodi entsprechend aktivieren oder unterdrückt.

Die Figur 2 verdeutlicht anhand eines Einplatz-Computersystems, wie die vorliegende Erfindung mit Baugruppen und Komponenten eines handelsüblichen PCs realisiert und erweitert werden kann. Ein digitales Dokument (5) wird entsprechend der Fig.2 von einer Datenträgereinheit (10) durch eine Datenträgerlesevorrichtung (12) gelesen. So wird bei einer CD oder einer DVD die Lesevorrichtung durch einen Laser und durch eine Photodiode od.dgl. zur Erkennung von Signalkennungen, die auf der Datenträgereinheit aufgebracht sind und sich als digitale Daten repräsentieren, gelesen. Das gemessene analoge Signal wird mittels eines AD Wandlers in ein digitales Signal transformiert und in eine Sequenz von 1 oder 0 umgewandelt. Damit der Prozessor eines PCs oder eines Players von der Korrektur durch Hardware- und Datenträgernahen Fehlern, Defekten oder

Verunreinigungen befreit ist, werden die Fehler durch spezielle Fehlerkorrekturprozesse einer in Hardware implementierten Korrektureinheit (14) unmittelbar nach dem Lesen korrigiert. Ein Beispiel dieser in Hardware implementierten Fehlerkorrektur wäre die Anwendung eines Tiefpassfilters zur Beseitigung von Fehlern in den Reflexions- oder Absorptionszonen, die dabei kleiner sind, als die typischen Pitlängen oder deren Zwischenbereiche, die sogenannten Lands. Außerdem kann eine Umsetzung von digitalen Signalen mittels EFM Signalisierung so hardwaremäßig implementiert werden, dass die Byte Daten auch bei einzelnen Bitfehlern korrekt rekonstruiert werden können.

Weitere Korrekturen können durch eine in Software implementierte Korrektureinheit (16) durchgeführt werden, die dazu verwendet werden kann, weitere Fehler in den digitalen Daten jeweils durch Prozessoroperationen zu detektieren und welches zudem in der Lage ist, je nach Schwere des Fehlers die entsprechenden defekten Daten zu korrigieren. Die softwaremäßige Fehlerkorrektur wird verwendet, wenn in der Datenträgerleseeinheit verschiedene physikalische und logische Strukturformate enthalten sein können.

Je nach verwendetem Datenträgerlesehardware können auch Korrekturen an den kleinsten abgeschlossenen Dateneinheiten, den Frames, hardwarenah in der Korrektureinheit (14) automatisch durchgeführt werden. Da die Funktion der Fehlerdetektion und der Fehlerkorrektur, sowohl in der Soft- als auch auf der in Hardware enthaltenen sein können, können diese in austauschbarer Weise in beiden Varianten angeboten und verwendet werden. Das in Hardware implementierte Fehlerdetektion- und -korrekturverfahren kann zur Steigerung der Performance und zur Entlastung des Prozessors verwendet werden, während eine Software-implementierte Fehlerdetektion und -korrektur zur Verbesserung der Flexibilität in Bezug auf das Lesen verschiedener Formate verwendet werden kann.

Auch sind hybride Soft- und Hardware Implementationen im Einsatz, bei denen die Fehlerdetektion bei einer Hardware Implementation automatisch durchgeführt wird, während die etwas seltener vorkommenden Fehlerkorrekturen softwaremäßig durchgeführt werden.

Die Daten werden nach der Korrektur anschließend zur Ausgabe durch einen regulären, auf die besonderen softwareseitigen Schnittstellen der Hardware angepassten Treiber (18) übertragen, oder entsprechend eines Prozessorzentrierten Ablauf wird der Treiber (18) durch Mittel zur Ausgabe-, Speicherung oder Verarbeitung (15) mittels entsprechender Softwarekomponenten und Aufrufe in der Treiberschnittstelle zur Datenaufnahme von dem im Datenträgerlesevorrichtung (12) enthaltenen Datenträger (10) aufgefordert.

Bei der erfindungsgemäßen Verifikationseinheit (20) liest die erweiterte Datenträgerlesevorrichtung (26) die auf der Datenträgereinheit (10) enthaltenen Daten ohne die im regulären Betrieb enthaltenen Fehlerkorrekturverfahren und/oder mit einer höheren Empfindlichkeit, so dass die defektartigen Signalkodierungen ebenfalls registriert werden können.

Die von der erweiterten Datenträgerlesevorrichtung (26) gelesenen Daten können durch zusätzliche Tiefpassfilter oder dergleichen verbessert und genauer detektierbar gemacht werden und/oder sofort in ein digitales Signal umgesetzt werden, so dass ein im wesentlichen durch Fehlerkorrekturmaßnahmen unberührtes digitales Signal an den erweiterten Treiber (24) übergeben wird oder die Daten wie in sonst üblicher Weise vom Treiber (24) angefordert werden.

Die Daten werden in der Verifikationsvorrichtung (20) von einer Gültigkeitsüberprüfungseinheit (22) angefordert und weiterverarbeitet. Dabei wird die zusätzliche Kodierung von der inhaltsbezogenen Kodierung getrennt und Wasserzeichendaten und/oder zusätzliche Serien-Nummer und/oder verschlüsselte Zusatzdaten extrahiert, um anschließend durch die Anwendung zusätzlicher Verifikationsverfahren die Informationen zur Gültigkeit oder zur Fälschung der versteckten Sicherheitsmerkmale zu erhalten.

Durch die anschließende Ausgabe des Verifikationsergebnis in einer Ausgabeeinheit (28) kann der Prüfer zu weiteren Maßnahmen veranlasst werden. So können die bei der Prüfung gewonnenen Daten im Falle einer detektierten illegalen Kopie aus Gründen der Beweissicherung in einer Archivierungseinheit (30) abgespeichert werden. Ferner können weitere Daten durch eine

Eingabeeinheit (32) zu dem Beweissicherungsprotokoll hinzugefügt werden. Ferner kann eine mit dem Verifikationsmodul verbundene digitale Signatureinheit zur Erhöhung der Datenintegrität der Beweissicherungsprotokolle zusätzlich mit qualifizierten Zeitstempel und zusätzlicher Smart-Card digital signiert werden, bevor die Prüfprotokolldaten in einer Archivdatenspeichereinheit abgelegt werden.

Auch kann ja nach detektiertem digitalen Dokument oder je nach benutzerseitiger Eingabe in (32) verschiedene Parameter bzw. Extraktionsverfahren für die Gültigkeitsüberprüfungseinheit (22) aus der Parameterspeichereinheit (34) oder verschiedene Treiber aus der Treiberspeichereinheit (36) anstelle des Treibers (24) geladen werden. Entsprechend ausgestaltet kann der Auswahlprozess nach Lesen weniger identifizierender Daten aus dem digitalen Dokument auch automatisch geschehen.

Die Figur 3 zeigt eine CD bzw. DVD mit einem Mittelloch (42) und einem Bereich für den Antrieb und Andruckmechanismus (44) des Players. Die auf der Datenträgereinheit enthaltenen Nutzdaten werden auf einer von innen beginnenden und spiralförmig nach außen laufenden Spur im sogenannten Nutzdatenbereich (40) abgelegt. Jede CD hat zudem einen Eingangsbereich oder Lead-In Bereich (46) in der Steuer oder Metainformationen abgelegt werden. Der Nutzdatenbereich wird entsprechend der Red-book Spezifikation von einem Ausgangsbereich (Lead-Out-Bereich) (48) abgeschlossen, bevor der nichtbeschreibbare Rand (41) der CD erreicht wird. Die Multisession CD erlaubt, dass die CD-ROM mehrere Lead-In und Lead-Out Bereiche enthält, so dass ein Brennen einer CD nicht in einem Prozessschritt durchgeführt werden muss, sondern auch in mehreren Schritten entstehen kann, wobei in einem solchen Fall jeweils ein neuer Lead-In/Lead-Out Bereich mit auf die CD geschrieben werden muss. Da diese Bereiche jeweils mehrere MB groß sein können und die darin enthaltenen Daten einem strengen Format unterliegen, wobei der Datenbereich nicht komplett ausgenutzt wird, kann ein Teil der zusätzlichen Kodierung in diese Bereiche integriert werden, ohne dass die Software, die diese Bereiche auswertet, diese zusätzlichen Kodierungsdaten registriert.

Die Tabelle in Fig. 4 enthält eine Zuordnung von Byte Daten auf eine 14 Bit breite Datenmodulation für ein einzelnes Datenbyte entsprechend der EFM (Eight-in-Fourteen Modulation). Die unter der EFM Spalte enthaltenen Werte sind nur 256 Kombinationen enthalten, von den insgesamt 16384 möglichen Bitkombinationen. Einzelne Bitfehler in der 14 bit Darstellung können mit entsprechenden Zuordnungsverfahren auf das Datenbit umgesetzt werden, was mit der hoher Wahrscheinlichkeit dem zugehörigen Datenbyte dann entspricht. So entspricht 1000010 0100000 dem Bytewert 1. Die Verfahren zur Zuordnung sind z.B. so ausgelegt, dass sie auch einer 1100010 0100000 den Bytewerte einer 1 ebenfalls zuweisen können.

Ein regulärer Treiber mit einer entsprechenden Fehlerkorrektur würde keinen Unterschied zwischen den beiden EFM Kodierungen machen und würde entsprechend den Bytewert 1 an die anfordernden Komponenten übergeben. Da 1 Pit-Fehler möglicherweise verschiedenste Ursachen haben kann, kann zum Verstecken von zusätzlichen Kodierungen 2 oder 3 Pit Änderungen verwendet werden, so dass immer noch eine zuverlässige Zuordnung auf das Originalbyte für die reguläre Fehlerkorrektur möglich ist.

Dagegen kann eine empfindlichere Datenträgerleseseinheit (26) bei Umgehung eventuell vorhandener Fehlerkorrekturen diese zusätzlichen Daten aus der EFM Modulation extrahieren. Da ein Grossteil der Pit/Lands und damit der EFM Änderungen auf tatsächliche Lese- und Materialfehler zurück zuführen ist, sind die verborgenen zusätzlichen Kodierungsdaten in einer als weißes Rauschen anzusehen Menge weiterer, auf echte Fehler und Verunreinigungen zurückzuführenden Datenmenge enthalten.

Die Fig. 5 zeigt, wie auf den Pits (50) als Kette von Reflexions- und Absorptionszonen auf der CD, die schließlich digitalen Signaldaten (52) in Form einer unstrukturiert erscheinenden linearen Kette (54) von Bits („0“ und „1“) entsteht, während ein Synchronisations-Kennzeichen bestehend aus 24 Bit als Pits/Land Kette eine Einteilung der Bitfolge dadurch möglich macht, dass anschließend ein Einteilungsverfahren angewandt werden kann. Durch die Synchronisierung und durch die

Auftrennung in 14 Bit modulierten Daten mit zusätzlichen sogenannten 3 Bit breiten „Merging-Bits“ (55) können anschließend die 14 Bit modulierten Daten (56) extrahiert werden. Durch eine Zuordnung und mit einer darin enthaltenen Bitfehlerkorrektur können aus den 14 Bit Daten (56) schließlich die 8 bit Daten als Bytewerte (58) gewonnen werden.

In Fig. 6 sind die Spuren (65) von Pits (60) und Lands (70) auf einem vergrößerten Ausschnitt einer CD dargestellt, die sich in Richtung des Pfeils (75) dreht. Die Pits haben eine Breite (66) von ca. 0,5-0,6 μm und eine Länge (62) von 0,83- 3,05 μm . Der Abstand zwischen den Spuren (64) beträgt 1,5-1,6 μm . Der fokussierte Laser (68) mit rotem Licht hat eine Wellenlänge von 780 nm. Die Schärfentiefe des Laserstrahls ist ca. 2 μm , so dass aufgrund des Durchmessers des Laserstrahls (68) eines regulären CD-Laufwerks die Defekte der Art (71), (72) und (73) nicht registriert werden können. Diese defektartigen Kennzeichen können auf der Spur (71) in einem Lands-Bereich, zwischen den Spuren (72) und in der Nähe eines Pit Anfang- bzw. Endbereichs (73) sein.

Durch einen Laserstrahl mit einer geringeren Wellenlänge oder mit einem nichtlinearen Fokussierungsverfahren oder einer nichtlinearen Photodetektionsvorrichtung können die defektartigen Pits aber registriert werden und als zusätzliche Kodierung unabhängig von der mit dem Digitalen Dokument verwendeten Kodierung genutzt werden.

Die Daten auf der CD sind, wie in Figur 7. beschrieben, in der kleinsten Datenorganisationseinheit, den Frames (80), zusammengefasst. Jedes Frame beginnt mit einem 24bit Synchronisationsbereich (81) und 3 Merging-bits. Anschließend folgt 1 Steuerungsbyte (82), das wie alle folgenden Bytes in einer EFM Darstellung dargestellt ist und jeweils von 3 Merging-Bits getrennt wird. Der erste Nutzdatenbereich (84) besteht aus 12 Byte gefolgt von dem 1. (1st) Level EDC/ECC Korrekturdaten (85), bestehend aus 4 Bytes. Der zweite Nutzdatenbereich (86) besteht ebenfalls aus 12 Byte, gefolgt von dem 2.(2nd) Level EDC/ECC Korrekturdaten (4 Byte) (87).

Dieses Frame erzeugt durch das Aneinanderreihen von 98 Frames ein Sektor (90).

Die Figur 8 beschreibt den schematischen Aufbau der Sektors (90), wobei die im Nutzdatenbereich (94) enthalten 2.352 Byte Nutzdaten entsprechend der in Fig. 7 beschriebenen Framebereiche (84) und (86) verteilt sind. In dem EDC/ECC Datenbereich (95) sind die 1st Level EDC/ECC und im EDC/ECC Datenbereich (97) sind die 2nd Level EDC/ECC Daten enthalten. Die ebenfalls verteilten 98 Byte Kontrolldaten (92) werden auch Subcode Channel genannt

Die Figur 9 enthält einen einzelnen in jedem Frame enthaltenen Subcode Byte (82). Entsprechend der Konvention werden die Bits mit P bis W markiert. Der Subcode-Channel P (82p) enthält ein Flag, das angibt an welcher Adresse innerhalb des Tracks die Musik oder die Daten beginnen. Der Subcode Channel Q (82q) erlaubt die Adressierung eines Sektors auf einer Disk entsprechend einer im Red-book spezifizierten Weise.

Die Fig. 10 beschreibt den 98bit langen Subcode Channel Q (82Q), der aus 2 Synchronisationsbits (93s), einer 4 Bit langen Typ Information (93j) zum Inhalt und 4 Kontrollbits (93k) zum dann folgenden 72 Bit langen Datenbit-Inhalt (93i) besteht. Abschließend werden 16 Bit zur Error Detektion (CRC) (93c) pro Kanal angehängt.

Die in (95) und (97) enthaltenen Fehlerdetektions und -korrektur Bytes und die in den Subcode Channel enthaltenen CRC Bits (93c) erlauben eine Änderung der Nutz- und Kontrolldaten, so dass bei einer automatisierten Fehlerkorrektur ein regulärer Treiber die Daten fehlerlos erhält, während das Vorhandensein eines Fehlers und die daraus entstehenden Zusatzinformationen als zusätzliche Kodierung durch eine Verifikationseinheit extrahiert werden kann.

Wie bei der EFM Fehlersituation kann die Verifikationseinheit ohne zusätzliche Daten nicht die Fehlerbits erkennen, die auf die zusätzliche Kodierung zurückzuführen sind.

Außerdem werden bei einer Musik- oder Daten-CD (CD-ROM) die Subcode-Channel R bis W nicht verwendet, so dass in diesen Bereichen, bezogen auf die gesamte CD, fast 12 MB abgelegt werden können.

Eine Musik-CD ist entsprechend der Figur 11 aufgebaut, bei der durch die Subcode Channel P die CD in Tracks aufgebaut ist. Sie enthält am Anfang einen Lead-In Bereich (46) und am Ende einen Lead-Out Bereich (48). Dazwischen können bis zu 99 Musik-Tracks (100) befinden. Zwischen den Musikstücken /-tracks können einzelne freie bzw. leere Sektoren (101) abgelegt werden, die keine Nutzdaten enthalten, aber dafür zusätzliche Kodierungsdaten.

Die Figur 12 beschreibt den schematischen Aufbau eines CD-ROM Sektors (110) entsprechend des Mode 1 der Yellow-Book Spezifikation. Durch die höheren Anforderungen in Bezug auf Fehlerfreiheit der Nutzdaten ist der Nutzdatenbereich (94) weiter aufgeteilt. Zusätzlich wird ein 12 Byte Sync Datenfeld (102), ein 4 Byte Header Datenfeld (104) und ein auf 2048 Byte beschränkter Datenbereich für Nutzdaten (105) eingeführt. Die restlichen 288 Bytes dienen der zusätzlichen CD-ROM-spezifischen Fehlerdetektion und -korrektur (106).

Wie bei der absichtlichen Änderung von Originaldaten bei der Herstellung und der Beschreibung dieser Situation in den beiden vorher dargestellten Beispielen werden bei der Benutzung der inhärenten Fehlerkorrekturen die mit der zusätzlichen Kodierungen versehenen Nutz- und Headerdaten durch die Datenfelder (95), (97) und (106) rekonstruiert, wobei ein regulärer Treiber diese darin enthaltenen Zusatzinformationen ignorieren und entsprechend Fehlerkorrigiert ausgeben kann, während die Verifikationseinheit (20) die Zusatzdaten erkennen kann und zusammen mit anderen zufälligerweise ebenfalls mit darin enthaltenen Fehler- und Defektdaten entsprechend extrahiert.

Figur 13 enthält ein Blockschaltbild zur Beschreibung der Herstellung einer mit zusätzlichen Kodierungen versehenen

Datenträgereinheit (10). Die zusätzlichen Kodierungsdaten werden als Wasserzeichen, als Serien-Nummer oder als verschlüsselte Zeichenkette in der Zusatzkodierungsdaten-Erstellungseinheit (130) erzeugt. Die dabei verwendeten Parameter und/oder die daraus entstehenden Daten werden in einer Parameter-Datenspeichereinheit (132) abgelegt und/oder einer Einheit zur Erzeugung von Überprüfungsparameter (126) übergeben, von der die Verifikationseinheit (20) entweder über das Internet oder über Datenträger die entsprechenden Daten zeitnah aktualisiert werden kann.

Die inhaltlich zur Publikation fertiggestellten Musikdaten werden z.B. aus einer Musikdatenspeichereinheit (125) durch eine Merging-Einheit (120) geholt, die für die Gesamtherstellung der auf dem Datenträgereinheiten enthaltenen Daten zuständig ist, wobei diese Einheit somit für das Zusammenführen der Musikdaten und der zusätzlichen Codierungsdaten vor der Erstellung eines entsprechenden Glasmasters bzw. einer Matrizie zuständig ist. Dabei finden die noch nicht durchgeführten EFM Kodierungen statt. Anschließend werden in der Erstellungseinheit (122) die EDC/ECC Fehlerkorrekturwerte berechnet und eine entsprechende Pit-Kodierung auf dem Glasmaster (Matrizie) erzeugt, so dass nach dem aus dem Stand der Technik bekannten Herstellungsverfahren für CDs mit einem Spritz-Preß-Verfahren die CDs bzw. DVDs hergestellt werden, bei der die CDs jeweils aus Polycarbonat mit einer reflektierenden Metallschicht ausgestattet werden, wobei die zusätzlichen, u.ä. der Identifizierung und Erkennung von Piratenware dienenden, Kodierungen in dem Redundanzbereich der Daten enthalten sind.

Zur Vereinfachung der Verwaltung dieser zusätzlichen Kodierungen bei der Herstellung und der späteren Verifikation ist eine Eingabeeinheit (135) vorgesehen, in der zusätzliche Verwaltungsdaten zu den Wasserzeichen, Serien-Nummern oder verschlüsselten Zusatzdaten in dem Datenspeicher und zur Steuerung der Erzeugung der entsprechenden Daten eingegeben werden können.

Alternativ zum Einfügen von zusätzlichen Kodierungen in der Merging-Einheit (120) kann eine Nachbearbeitungseinheit (124) in einem zusätzlichen Schritt z.B. durch einen Laser, der die

zusätzlichen Signalisierungskennzeichen auf den optischen Datenträger an vorher berechneten Positionen brennt, durchgeführt werden, um so die Situation einer defektartigen Signalisierung herzustellen.

Die Figur 14 zeigt ein Blockschaltbild bestehend aus Komponenten, bei dem mehrere Zusatzkodierungsdaten-Ausgabeeinheiten (144) vorgesehen werden können und die Herstellung von Wasserzeichen (150) hinter einer besonders geschützten Sicherheitsinstallation, z.B. einer optionalen Firewall (145), wobei die Auslieferung der entsprechenden zusätzlichen Kodierungsdaten erst auf Anforderung durch eine Dateneingabestation (142) erfolgt. Der Schutz der Komponenten hinter der Firewall entsteht aus der Notwendigkeit, besonders kritische Daten, die ein Kopieren der Wasserzeichen oder dergleichen und eventuell ein legal erscheinendes Piratenprodukt erst möglich macht, vor einer Weitergabe bzw. Verrat entsprechend zu schützen.

Die Daten werden über das Session-Management des Servers (140) geholt, wobei ein Benutzer dem User-Management (146) bekannt sein muss, bevor nach Überprüfung des Benutzerpasswortes durch das User-Access-Management (148) weitere Benutzeraktionen in dem Session-Management (140) freigeschalt werden können. Die auf der Ausgabeeinheit (144) ausgegeben Daten können dort eventuell automatisch weiterverwertet, transformiert und im Rahmen eines Workflows weiterberechnet werden. Die zusätzlichen Kodierungsdaten stammen aus der Zusatzkodierungsdaten-Generatoreinheit (150) oder aus einem Zwischenspeicher, z.B. aus dem des Session Managements (140) oder dergleichen.

Zum beweisfähigem Ablegen der in der Zusatzkodierungsdaten-Generatoreinheit (150) enthaltenen Daten werden die Daten in dem in Figur 14 enthaltenen Beispiel durch eine weitere Zertifizierungseinheit (152) signiert, bevor sie in dem Datenspeicher (155) abgelegt werden, wobei dieser Schritt auch optional übergangen werden kann. Zur Generierung und zur Benutzung von Privaten bzw. Öffentlichen Schlüsseln ist eine Schlüsselerzeugungs- und Benutzungseinheit (154) vorgesehen, bei der entweder der Zusatzkodierungsdaten-Generatoreinheit (150)

mit Schlüsseldaten versorgt wird oder die Private Key Daten auf Wasserzeichenparameter, Serien-Nummer oder dergleichen angewendet werden.

Zusätzlich können alle wichtigen Vorgänge durch ein Log-File Generator und Speichereinheit (164) aufgezeichnet werden, wobei zur zusätzlichen Erhöhung der Sicherheit eine externe Überwachungseinheit (162) hinzugefügt wird, deren Daten ebenfalls nicht nachträglich veränderbar in dem Log-File enthalten sind. Die dabei entstehenden Daten können als ein qualifiziertes Protokoll in einer zertifizierten Log-File Ausgabereinheit (160) lückenlos die Integrität und Manipulationsfreiheit der Servereinheit nachweisen.

Obwohl das Komponentenmodell die Verteilung der Prozesse auf einzelne unabhängige Rechner erlaubt, die über ein Netzwerk miteinander kommunizieren, so ist doch eine Zusammenlegung von einzelnen Aufgaben auf eine geringere Anzahl von Rechnern sinnvoll, so dass die damit verbundene flexible Verteilung durch ein geeignetes Konfigurationsmanagement (165), wie im beschriebenen Beispiel, eine entsprechende Anwendung finden kann.

Die Fig. 15 zeigt in der Gegenüberstellung schematisch Strukturen auf einer im vorliegenden Beispiel als CD oder DVD realisierter Datenträgereinheit in zwei Lese- bzw. Betrachtungsebenen: Die linksseitige Ansicht verdeutlicht eine Datenträgereinheit (10) mit einem digitalen Datenbereich (171) sowie einem zusätzlich vorgesehenen Bereich (180) mit Seriennummer bzw. anderen verschlüsselten Zusatzdaten; die Bezugszeichen (170) geben zwei in ansonsten bekannter Weise hergestellte Wasserzeichendatenbereiche an.

Die rechte Ansicht der Fig. 15 verdeutlicht eine tiefere technische Leseebene der Datenträgereinheit (10), nämlich ohne (weitgehend hardwarebasiert bzw. automatisiert) durchgeführte Bereinigung speziell der Nutzoberfläche im Bereich der digitalen Daten 172 um stets vorhandene, randomisiert angeordnete Störstellen, Fehler, lokale Abweichungen od.dgl. (im weiteren auch als „weißes Rauschen“ (175) bezeichnet).

Die Bezugszeichen (170_a) und (180_a) bezeichnen die ebenfalls vorhandenen zusätzlichen Kodierungsdaten, wie sie in der linken Ansicht enthalten sind, jedoch können diese in der rechten Darstellung nicht unmittelbar von den Daten des weißen Rauschen (175) unterschieden werden.

Wie die Fig. 16 mit einer schematischen Ansicht einer Hard- und Softwareelemente kombinierenden Treibereinheit zur Implementierung der Verifizierungsmittel (20) (vgl. Fig. 2) verdeutlicht, ist es nunmehr möglich, die zwangsläufig vorhandenen physikalischen Gegebenheiten auf einer Datenträgerreinheit (Fig.15) selektiv zu verwerten und so den gewünschten Verifizierungszweck im Rahmen der Erfindung sicherzustellen.

So bieten insbesondere die Einheiten (188) und (189) die Möglichkeit, hardwarebasiert (d.h. in Echtzeit, gleichwohl vergleichsweise unflexibel) Fehlerdetektion und -korrektur vorzunehmen, dies jedoch gemäß einer jeweils aufgebrachten zusätzlichen Codierung selektiv, d.h. gezielt anwähl- bzw. abschaltbar. Entsprechendes gilt für die mit dem Bezugszeichen (186) und (187) bezeichnete softwareimplementierte Fehlerdetektion und -korrektur, so dass mit der gezeichneten Einheit und für ein nachgeschaltetes Dateninterface (185) für eine erweiterte Datenträgerleseeinheit (26) in äußerst flexibler Weise eine Infrastruktur zum maximalen Nutzen der physischen Gegebenheiten auf der Datenträgeroberfläche zur Verfügung steht.

Die Fig. 17 verdeutlicht den Systemzusammenhang: Eine Vorrichtung (200) zum Herausfiltern des weißen Rauschens (Fig. 15) bereinigt den Datenträger (10), gesteuert durch eine geeignete Parameter- und Speichereinheit (215). Das datenmäßige Ausgangsprodukt der Speichereinheit (200), nämlich die um das weiße Rauschen bereinigte Datenträgerabbildung (202), welches nach wie vor jedoch die erfindungsgemäßen zusätzlichen Codierungsdaten (204) enthält, wird dann in der Einheit (205) selektiv auf die betreffenden zusätzlich aufgebrachten Codierungsinformationen untersucht, und es werden diese dann in unabhängige Überprüfungskriterien (abhängig von der Einheit

(215)) aufgeteilt und in der Tabelle (210), wie schematisch gezeigt, abgelegt. Genauer gesagt erfolgt hier eine Erfassung entlang unabhängiger Überprüfungskriterien bestehend aus Parameter zur Kennzeichnung von Wasserzeichen (207), Seriennummern (208) und zusätzlichen Spalten (209) mit der vorteilhaften Wirkung, dass somit eine klar definierte logische Struktur der verschiedenen Wasserzeichen bzw. Markierungen und deren jeweils zugehörige Prüfkriterien zur Verfügung stehen. Es ergibt sich, dass damit die Sicherheit des vorliegenden Kopierschutzverfahrens selbst dann gewährleistet ist, wenn einzelne der zusätzlichen Datenkomponenten bzw. Wasserzeichen entschlüsselt oder offenbart sein sollten, da die in der Tabelle (210) zusammengefassten Inhalt stets durch weitere Überprüfungskriterien erweitert werden, welche üblicherweise nicht vollständig und sämtlichst missbräuchlich realisiert sein können.

Die Fig. 18 und 19 verdeutlichen anhand der dort gezeigten Flussablaufdiagramme die Erzeugung (Fig. 18) der Mehrfach-Wasserzeicheninformationen bzw. deren Auswertung und Überprüfung (Fig. 19), es wird jeweils auf die zugehörigen Erläuterungen der Verfahrensschritte in der anliegenden Bezugszeichentabelle verwiesen, die, wie auch die weiteren Bezugszeichenerläuterungen, in die vorliegende Beschreibung als zur Erfindung gehörig einbezogen gelten soll.

Soweit die Verfahren nach Fig. 18 und 19 betroffen sind, ist bemerkenswert, dass die Auswahl der eine Beziehung zwischen den Wasserzeichen bzw. der Seriennummer herstellenden Schlüssel variabel, randomisiert bzw. insbesondere auch regelbasiert sein kann, ebenso wie die Auswahl bzw. Positionierung des konkreten Aufbringungsmusters der zusätzlichen Codierung.

Diese Variabilität findet sich auch im konkreten Verifizierungsverfahren (Fig. 19), mit den parallel durchgeführten Schritten (242) bis (246), die entsprechend in das tatsächliche Extrahieren und darauf folgende Verifizieren als Eingangsgrößen eingehen.

Die Fig. 20 schließlich setzt wiederum die anhand der Fig. 18, 19 verdeutlichten Herstellungs- bzw. Verifizierungsschritte um in eine entsprechend spezialisierte Vorrichtung gemäß einer weiteren bevorzugten Ausführungsform der vorliegenden Erfindung, die, in Weiterbildung der generischen Strukturen gemäß Fig. 1, spezielle Einheiten zur Variabilität in der Erstellung der Wasserzeichen bzw. deren Zuordnung sowie entsprechend auf der Verifizierungsseite eine große Einfluss- und Parameterbreite zur Maximierung der sicherheitserhöhenden Maßnahmen ermöglicht. Eine -- notwendige und, angesichts der Komplexität und Variantenbreite gemäß Fig. 20, durchaus komplexe -- Kommunikation zwischen den Einheiten wird erfindungsgemäß durch eine geeignete, bevorzugt mobil realisierte Kommunikationsschnittstelle (270) und (275) realisiert, welche insbesondere auch im Hinblick auf missbräuchliche Zugriffe bei dieser Kommunikation geeignet abgesichert ist. Im Datenspeicher (266) laufen so die jeweils konkret eingestellten sicherheitsrelevanten Parameter zusammen und werden zur äquivalenten Einheit 280 auf der Seite der Verifizierungseinheit 20 übertragen.

Die zusätzlichen Kodierungsdaten unterteilen sich in 3 Kategorien: den Wasserzeichen-artigen, den Serien-Nummern-artigen und den verschlüsselten Zusatzdatenartigen Daten.

Die Serien-Nummern Daten oder unverschlüsselte Zusatzdaten, die als zusätzliche Kennzeichen den Serien-Nummern hinzugefügt werden können, sind Daten, die z.B. an einer definierten Stelle (Datenposition), in einem definierten Sektor oder dergleichen in bevorzugter Weise zusammenhängender Form auf dem Datenträger unverschlüsselt abgelegt sind. Die Bedeutung der Daten, die in diesen Feldern gelesen werden können, werden der Verifikations-einheit durch Verfahrensanweisungen und/oder durch Parametersätze kenntlich gemacht.

Die verschlüsselten Zusatzdaten sind wie die unverschlüsselten Serien-Nummer-artigen Daten ebenfalls in definierten Datenträgerpositionen und/oder Sektoren oder dergleichen

abgespeichert, wobei der einzige Unterschied in der Verschlüsselung des entsprechenden Datensatzes liegt.

Sowohl in den unverschlüsselten als auch den verschlüsselten zusätzlichen Kodierungsdatensätzen können Zusatzdaten, wie Parameter, Verfahrensanweisungen oder dergleichen, enthalten sein, mit der die versteckten Wasserzeichen anschließend extrahiert werden können.

Die Entschlüsselung der verschlüsselten Kodierungsdatensätze kann entweder durch öffentlich zugängliche Publik-Key Schlüssel geschehen, so etwa im Fall von vor Manipulation zu schützenden Daten, wie etwa zur Nutzungsbeschränkung des Datenträgers.

Weitere Schlüssel können zur Erhöhung der Sicherheit und Zuverlässigkeit des Verfahrens auch später auf andere, bereits auf Vorrat vorbereitete, Felder angewendet werden, so dass auch dann noch eine Überprüfung durchgeführt werden kann, wenn entsprechende geheime Hinweise zur genauen Implementation der Vorrichtung bekannt wurden.

Die so aus den zusätzlichen Kodierungsdaten in unverschlüsselter und verschlüsselter Form gewonnenen Parameter können in Wasserzeichen Daten umgerechnet werden, und es kann anschließend von der Datenträgerlesevorrichtung entsprechend gezielt nach diesen Daten gesucht werden, ohne das alle Daten, die als weißes Rauschen detektiert, und dabei ggf. aus echten Material- oder Oberflächenfehlern entstanden sind, von dem Datenträger gelesen werden müssen.

Das Wasserzeichen ist ein Signal, dass sich in dem weißen Rauschen beim unkorrigierten, also mit nichtbeabsichtigten Material oder Oberflächen oder sensorischen Fehlern behafteten, Lesen der Daten entsteht. In diesem Sinne sind die hinzugefügten zusätzlichen Kodierungsdaten, deshalb als Wasserzeichen anzusehen, da sie bei einer sehr genauen Abtastung der Oberfläche des Datenträgers und auch bei Kenntnis des Datenträgerformates, nicht-wahrnehmbar sind.

Die Verwendung eines robusten Wasserzeichens ergibt sich aus der Anwendung eines aus der im Stand der Technik hinreichend bekannten Wasserzeichen-Generierungsverfahren.

Die Serien-Nummer-artigen und die verschlüsselten Zusatzdaten müssen nicht zwingend notwendig im Redundanzbereich des CD/DVD Datenträgers enthalten sein, sondern können z.B. auch in den zusätzlichen Subcode-Channel R bis W oder in den Lead-In oder Lead-Out Bereichen außerhalb der Auswertungsbereiche anderer Programme/Prozesse abgelegt werden. Obwohl dieses Vorgehen auch für das Wasserzeichen möglich wäre, bietet sich jedoch in einer sicherheitserhöhenden Weise zumindest das teilweise Abspeichern des Wasserzeichens in dem Redundanzbereich des Datenträgers an, so dass bei einer automatischen Korrektur der Fehlerdaten durch eine nichtautorisierte und über das Vorhandensein eines Wasserzeichens nicht informierte Kopierstelle auch das Wasserzeichen beschädigt sein würde.

Außerdem können sehr wenige Daten, die z.B. nach dem CD Pressprozess durch die im Stand der Technik hinreichend bekannte Verfahren, hinzugefügt werden und eventuell durch eine zusätzliche Verschlüsselung der so aufgebrachten Daten einer vor Manipulation freien Individualisierung einer einzelnen CD erreicht werden, so dass diese Zusatzdaten in erfindungsgemäßer Weise unabhängig von einer Laborumgebung durch die Verifizierungseinheit überprüft werden kann.

Für die Verifizierungseinheit gibt es kein offensichtliches Unterscheidungsmerkmal zwischen einem Material- oder Oberflächendefekt und einem möglicherweise künstlich hinzugefügten zusätzlichen Kennzeichen oder einer entsprechenden zusätzlichen Kodierung, die innerhalb eines Wasserzeichens od. dgl. verwendet werden können.

Daher kann auch jeder natürlich vorhandene Defekt, der von der Verifizierungseinheit in reproduzierbarer Weise detektiert oder ausgelesen werden kann, für die Feststellung der Authentizität einer CD bzw. DVD herangezogen werden und durch die Verknüpfung innerhalb eines vorbestimmten Verfahrens z.B. mit einer Seriennummer oder mit anderen zusätzlichen ggf. verschlüsselten Daten verknüpft werden.

In diesem Sinne müssen die zusätzlichen Kennzeichen nicht künstlich als defektartige Kennzeichen aufgebracht werden, sondern sie können auch durch die Definition eines vorbestimmten Auswahl- und Detektierungsverfahrens selektiv aus inhärent vorhandenen Defektstellen (Datenträgerkennungen bzw. defektartige Signalelemente im Sinne der Erfindung) ausgewählt und damit festgelegt werden. Somit kann bereits durch die Festlegung von Parametern innerhalb des Auswahlverfahrens ein Wasserzeichen definiert und ausgezeichnet sein, welches nicht, wie bei den im Stand der Technik bekannten Wasserzeichen, erst durch extern zusätzlich hinzugefügte Daten oder Kennzeichen entsteht. Durch die prinzipiell zufällig entstehenden Defekte entsteht ein eindeutiges und ohne zusätzlichen Aufwand natürlich verstecktes, aber bei Kenntnis vorbestimmter Parameter, Anweisungen und Benutzung geeigneter Verifizierungs- oder Sensormittel, ein leicht auffindbares Wasserzeichen.

Neben die bereits vorhandenen Defekten können ggf. zusätzliche gezielt platzierte künstliche Kennzeichen eingefügt werden, die dann aber in nicht erkennbarer Weise mit den natürlich vorhandenen Defekten ein, ohne genaue Kenntnis des Auswahlprozesses, prinzipiell nicht erkennbares Muster oder eine nicht erkennbare innere mathematische Relation aufweisen.

Im Gegensatz zu der schnellen leicht automatisierbaren Festlegung, welche Bereiche Wasserzeichencharakteristika haben sollen bzw. welche Bereiche dazu verwendet werden sollen, stellt die Kopie von vorhandenen Oberflächendefekten eine produktionstechnisch wesentliche größere technische Herausforderung für den CD Piraten dar, als für den autorisierten Originalhersteller der CD.

Durch die Nutzung vorhandener Material- oder Oberflächendefekt in der Definition des Wasserzeichens kann eine prinzipiell nicht materiell reproduzierbare Definition oder Version eines Wasserzeichens geschaffen werden, da die eigentliche Definition innerhalb eines geheimen und durch Parameter leicht zu ändernden Definitionsverfahrens liegt.

Die verwendeten Parameter können ebenfalls auf der CD bzw. DVD abgelegt werden, da deren Bedeutung erst durch die

Verifizierungseinheit hergestellt wird. Durch die Variation verschiedener Verifizierungsverfahren kann zudem sehr schnell festgestellt werden, welche Verfahren zur Erkennung von zusätzlichen Kennzeichnungen bekannt wurden, da eine sehr geringe Anzahl von erfolgreichen Übereinstimmungen bei einer gleichzeitigen Nichtübereinstimmung der Kennzeichen innerhalb anderer Verifizierungsverfahren ein klares Anzeichen dafür ist, dass mit großer Wahrscheinlichkeit die übereingestimmten Kennzeichnungsverfahren von Piraten enttarnt wurden.

Das durch die Verwendung der Parameter erkennbar gewordene Wasserzeichen stellt dann ein Dokument dar, dass durch die Verwendung bekannter digitaler Signaturverfahren digital signiert werden kann und dessen Werte innerhalb eines vorbestimmten und ggf. sogar veröffentlichten Bereichs der CD abgelegt wurde.

Die in einem Wasserzeichen oder in der zusätzlichen Kodierung verwendeten oder enthaltenen defektartigen Daten können ebenfalls einer Änderung durch Verschmutzung, Kratzer oder sonstiger Umweltfaktoren unterliegen, so dass auch die hinzugefügten und verwendeten defektartigen, zusätzlichen Kennzeichen eine innere Redundanz aufweisen können, die durch eine EFM-artige Kodierung oder Modulation, durch CRC oder EDC/ECC -artige Korrekturdaten oder durch CIRC oder ACIRC -artige Rekonstruktionsverfahren in der Zuverlässigkeit ihrer datenmäßigen Detektierbarkeit erhöht werden kann.

Eine illegale Kopie eines digitalen Mediums wie einer CD oder DVD bleibt durch die erfindungsgemäße Vorrichtung, Verwendung derselben und durch die Anwendung des erfindungsgemäßen Verfahrens für immer als illegale Kopie erkennbar und dieses unabhängig von zukünftigen Fortschritten bei den Herstellungsverfahren von CD bzw. DVD. Aus diesem Grunde kann durch Anwendung der Erfindung zugrundeliegenden Technologie das produktionstechnische Wettrennen zwischen Originalherstellern und organisierten Piraten technisch als vorläufig und möglicherweise aufgrund der hohen Kosten der technischen Umgehung dieses Schutzverfahrens sogar als dauerhaft entschieden betrachtet werden.

Angesichts der leichten Handhabung einer entsprechenden Überprüfungstechnologie, realisiert insbesondere mit konventioneller PC Technik, kann im Rahmen der Sorgfaltspflicht von Verkäufern, Wiederverkäufer oder Zwischenhändler die stichprobenartige Überprüfung der zum Verkauf angebotenen CD/DVD Produkte erwartet werden, um festzustellen, ob es sich um illegale Ware handelt. Somit kann zusätzlich der Markt für entsprechende illegale digitale Güter mit bestehenden Mitteln beschränkt werden.

Die Zuverlässigkeit des erfindungsgemäßen Kopierschutzverfahrens ergibt sich aus der Tatsache, dass auch ein mit professioneller Fertigungstechnik und Kopiertechnik ausgestatteter CD Pirat nicht in der Lage ist, alle defektartigen Signale, seien sie physikalischen Ursprungs oder in der Abweichung vom logischen Format begründet, fehlerfrei zu klonen. Das Fehlen der zusätzlichen Kodierungen ergibt somit unmittelbar einen Hinweis auf illegale Exemplare eines nichtautorisiert hergestellten Datenträgers.

Bezugszeichentabelle

Die folgende Tabelle enthält eine ergänzende Beschreibung der Bezugszeichen zu den Figuren 1 bis 20 und ist ein Bestandteil der vorliegenden Erfindung und Offenbarung.

Bezugszeichenerklärung**(Beschreibung)**

- | | |
|----|---|
| 1 | Herstellungseinheit; Mittel zur Herstellung einer Datenträgereinheit mit zusätzlichen Kodierungsdaten |
| 2 | Mittel zum Aufbringen von digitalen Dokumenten auf eine Datenträgereinheit |
| 3 | Mittel zum Aufbringen von zusätzlichen Kodierungsdaten auf eine Datenträgereinheit |
| 5 | Digitales Dokument; Elektronisches Dokument |
| 7 | Mittel zum Einfügen der zusätzlichen Kodierungsdaten in eine logischen Datenstruktur |
| 8 | Mittel zum direkten Aufbringen von zusätzlichen Kodierungsdaten auf eine Datenträgereinheit |
| 9 | Mittel zur Kommunikations- oder Betriebssteuerung |
| 10 | Datenträgereinheit; Mittel zur Speicherung von elektronischen Dokumenten und von zusätzlichen Kodierungsdaten |
| 12 | Datenträgerlesevorrichtung; Mittel zum Lesen von digitalen Daten von einer Datenträgereinheit. |
| 14 | Mittel zur Fehlerdetektion und -korrektur, die in Hardware implementiert ist |
| 15 | Mittel zur Ausgabe und zur Darstellung von digitalen Dokumenten |
| 16 | Mittel zur Fehlerdetektion und -korrektur, die in Software implementiert ist |
| 18 | Treiber der Datenträgerlesevorrichtung (12); Mittel zum Lesen von Daten aus dem digitalen Dokumentes |
| 20 | Verifikationsmittel; Mittel zur Verifikation eines autorisiert gefertigten Exemplars einer Datenträgereinheit; Mittel zur Feststellung einer illegalen, nicht-autorisierten Anfertigung eines zu testenden Datenträgers |
| 22 | Gültigkeitsüberprüfungseinheit; Mittel zur Überprüfung der Kriterien, die mit und in den zusätzlichen Kodierungsdaten verknüpft und enthalten sind |
| 24 | Erweiterter Treiber von (26); Softwareschnittstelle zum Lesen von zusätzlichen Kodierungsdaten |

- 26 Erweiteter Datenträgerlesevorrichtung; Mittel zum Lesen von
zusätzlichen Kodierungsdaten von einer Datenträgereinheit
- 28 Ausgabeeinheit; Mittel zur Ausgabe von Daten der Veri-
fikationseinheit
- 30 Archivierungseinheit; Mittel zur Abspeicherung von
Ergebnissen eines Überprüfungsvorgangs
- 32 Eingabeeinheit; Mittel zur Eingabe von Daten in die Ve-
rifikationseinheit
- 34 Parameterspeichereinheit; Mittel zur Speicherung von
Parameterdaten, die von (22) und (24) benutzt werden können
- 36 Treiberspeichereinheit; Mittel zur Speicherung von
Treiberdaten, die in, von und anstelle (ersetzend) von (22)
benutzt werden können
- 40 Nutzungsdatenbereich einer CD bzw. DVD
- 41 Nichtbeschreibbarer Rand der CD bzw. DVD
- 42 Mittelloch der CD/DVD
- 44 Bereich für den Antriebs- und Andrückmechanismus des
Players auf der CD/DVD
- 46 Eingangsbereich (Lead-In) einer Musik-CD
- 48 Ausgangsbereich (Lead-Out) einer CD
- 50 Kette von Pits- und Lands auf einer CD Spur
- 52 Digitales Signal nach Transformation der Pits/Lands durch
einen AD Wandler
- 54 Lineare Kette von Bits, das sich aus dem digitalen Signal
ergibt
- 55 Segmentierte Darstellung von EFM Daten mit 3 Merging-Bits
- 56 Darstellung von Bytedaten in einer 8 in 14 Modulation
- 58 Bytedaten (8 Bit), die bitfehlerkorrigiert sind und an
weitere Fehlerdetektion und -korrektur-Einheiten weiter-
gegeben werden können
- 60 Einzelnes Pit auf einer CD/DVD
- 62 Länge eines Pits auf einer CD
- 64 Abstand zwischen 2 Spuren auf einer CD
- 65 Spur einer CD, auf der die Pits und Lands aneinander
gereiht sind
- 66 Breite eines Pits auf einer CD
- 68 Durchmesser eines fokussierten Laserstrahls eines CD-
Players
- 70 Lands auf einer CD/DVD
- 71 Defektartiges Signalelement auf der Spur einer CD
- 72 Defektartiges Signalelement zwischen den Spuren einer CD

- 73 Defektartiges Signalelement in der Nähe eines Pits, also an dessen Anfang bzw. Ende
- 75 Drehrichtung einer CD
- 80 Frame, als kleinste strukturierte Dateneinheit einer CD, die mit einem EDC/ECC artigen Fehlerkorrektur Mechanismus ausgestattet ist
- 81 Synchronisationsdatenbereich eines Frames
- 82 Steuer- und Kontrollbyte eines Frames, der auch als Subcode Channel bezeichnet wird
- 82p P Bit des Subcode Channel Bytes
- 82q Q Bit des Subcode Channel Bytes
- 82Q 98 bit langes Bitfeld, bestehend aus den 82q Bits aller Frames eines Sektors
- 84 1. Nutzdatenbereich eines Frames
- 85 1st Level EDC/ECC Fehlerdetektions und -korrekturbereich eines Frames
- 86 2. Nutzdatenbereich eines Frames
- 87 2nd Level EDC/ECC Fehlerdetektions und -korrekturbereich eines Frames
- 90 Sektor, der als Dateneinheit aus 98 Frames zusammengesetzt ist
- 92 Kontrollldaten, die aus den Steuerbytes der Frames entsteht, die ein gemeinsamen Sektor bilden
- 93s Synchronisationsbits aus der 82Q Bitkette
- 93j Typ-Informationen zum Inhalt der 82Q Bitkette
- 93k Kontrollbits aus der 82Q Bitkette
- 93i Dateninhaltsbits aus der 82Q Bitkette
- 93c CRC Error Detection Bitkette innerhalb der 82Q Bitkette
- 94 Nutzungsdatenbereich eines Sektors, der aus den Nutzungsdatenbereichen (84), (85) aller Frames, die ein gemeinsamen Sektor bilden zusammengefasst wurden
- 95 Zusammengefasster 1st Level EDC/ECC Datenbereich eines Sektors, der aus den Datenbereichen (85) aller Frames gebildet wird, die zu einem gemeinsamen Sektor gehören
- 97 Zusammengefasster 2nd Level EDC/ECC Datenbereich eines Sektors
- 100 Musik-Track auf einer CD
- 101 Optionale leere/freie Sektoren zwischen den Musik-Tracks
- 102 Sync-Datenfeld eines CD-ROM Mode 1 Sektors
- 104 Header Datenfeld eines CD-ROM Mode 1 Sektors
- 105 Nutzdatenfeld eines CD-ROM Mode 1 Sektors, das aus 2048

Byte Nutzdaten besteht

- 106 CD-ROM Mode 1 spezifische Fehlerdetektion und Korrekturdaten, die die Fehlerfreiheit der Nutzdaten in 105 sicherstellt
- 110 Sektor-Aufbau einer CD-ROM Mode 1 Dateneinheit
- 120 Merging Einheit; Mittel zum Zusammenführen von digitalen Dokumenten und von zusätzlichen Kodierungsdaten, die innerhalb der logischen Struktur des Dokumentenformates eingefügt werden
- 122 Erstellungseinheit; Mittel zur Erstellung der Datenträgereinheit
- 124 Nachbearbeitungseinheit; Mittel zum nachträglichen Aufbringen von zusätzlichen Kodierungsdaten
- 125 Musikdatenspeichereinheit; Mittel zur Speicherung des digitalen Dokumentes
- 126 Einheit zur Erzeugung von Überprüfungsparameter
- 130 Erstellungseinheit für die zusätzlichen Kodierungsdaten.
- 132 Parameter-Datenspeichereinheit; Mittel zum Abspeichern von Parameterdaten, die entweder von der Einheit (130) erzeugt wurden oder an die Einheit (130) zur Erzeugung von zusätzlichen Kodierungsdaten übergeben werden
- 135 Eingabeeinheit; Mittel zur Eingabe von zusätzlichen Daten bei der Herstellung zum Zwecke der Verwaltung oder der Rechteverwaltung oder dergleichen.
- 140 Session Management; Mittel zur Verwaltung verschiedener Benutzerabfragen und Datenanforderungen.
- 142 Dateneingabestation; Mittel zur Anforderung von zusätzlichen Kodierungsdaten und zur Eingabe von zusätzlichen Daten zur Verwaltung, zur Festlegung von Nutzungsrechten oder dergleichen.
- 144 Ausgabeeinheit für Zusatzkodierungsdaten; Mittel zum Empfang, zur Konvertierung und zur automatischen Weiterleitung der Daten
- 145 Firewall; Mittel zum Schutz von vertraulichen und geheimen Daten
- 146 User-Management;
- 148 User-Access-Management; Mittel zur Freigabe eines Benutzers mittels Kennzeichen wie Passwort oder dergleichen.
- 150 Generatoreinheit; Mittel zur Erzeugung von Zusatzkodierungsdaten
- 152 Zertifizierungseinheit; Mittel zur digitalen Signatur von

- digitalen Daten zwecks der Erhöhung der Beweisfähigkeit
- 154 Schlüsselerzeugungs- und Benutzungseinheit; Mittel zur Erzeugung von Private/Public Key Paaren, so wie der Anwendung der Schlüssel auf digitale Daten.
- 155 Datenspeichereinheit; Mittel zum Abspeichern von Daten, die mit der Erzeugung der zusätzlichen Kodierung in direkten Zusammenhang stehen.
- 160 Zertifizierte Log-File Ausgabereinheit; Mittel zur Ausgabe von Daten, die mit einer (qualifizierten) digitalen Signatur versehen sind
- 162 Externe Überwachungseinheit; Mittel zur direkten (Video-) Überwachung aller Sicherheitsrelevanten Einrichtungen
- 164 Log-File Generator; Mittel zur Erzeugung von wichtigen benutzerseitigen Dateneingaben oder automatischen Statusmeldungen
- 165 Konfigurationsmanagement; Mittel zur Konfiguration der Komponenten in der Herstellungseinheit
- 170 Wasserzeichendaten; zusätzliche Kodierungsdaten, die als Daten nicht wahrnehmbar sind und in anderen Daten versteckt sein können
- 170a Wasserzeichendaten auf einer CD; zusätzliche Kodierungsdaten, die auf einem Datenträger in weiteren zufälligen durch fehlerbehaftete Daten entstehenden Zusatzdaten versteckt sind
- 171 Digitale Daten mit Zusatzkodierungen ohne die zusätzlichen, zufälligen Fehlerdaten, also bei Anwendung einer Fehlerkorrektur entstehen
- 172 Digitale Daten mit Zusatzkodierungen und einer Menge von zufälligen Fehlerdaten, die als weißes Rauschen betrachtet werden kann
- 175 Weißes Rauschen; zusätzliche fehlerbehaftete Daten, die auf einem Datenträger durch die fehlende Fehlerkorrektur erst sichtbar werden
- 180 Serien-Nummer-Daten und Verschlüsselte Daten; Daten, die an definierten Stellen/ Sektoren/ Positionen, bevorzugt in zusammenhängender Weise, auf einem Datenträger enthalten sind und nach Kenntnis der entsprechenden Parameter gelesen und als Serien-Nummer-Daten od. dgl. identifiziert werden können
- 180a Serien-Nummer-Daten und Verschlüsselte Daten auf einer CD ohne Anwendung der Fehlerkorrektur; zusätzliche Ko-

- dierungsdaten, die auf einem Datenträger in andern zufälligen fehlerbehafteten Daten versteckt sind
- 185 Treiberinterface; Schnittstelle zum Holen von Daten von einem Datenträger
- 186 Mittel zur Fehlerkorrektur; Mittel, das als Software realisiert ist
- 187 Mittel zur Fehlerdetektion; Mittel, das als Software realisiert ist
- 188 Mittel zur Fehlerkorrektur; Mittel, das als Hardware realisiert ist
- 189 Mittel zur Fehlerdetektion; Mittel, das als Hardware realisiert ist
- 190a Lesen von Datenträgerdaten ohne EDC/ECC und Weitergabe der Daten in die Treiberschnittstelle (185)
- 190b Lesen von Datenträgerdaten nur mit Softwarebasierter Fehlerdetektion und Weitergabe der Daten in die Treiberschnittstelle (185) in nicht-korrigierter Form
- 190c Lesen von Datenträgerdaten nur mit Hardwarebasierter Fehlerdetektion und Weitergabe der Daten in die Treiberschnittstelle (185) in nicht-korrigierter Form
- 200 Vorrichtung zum Herausfiltern von weißem Rauschen von Daten, die von einem Datenträger gelesen werden
- 202 Abbildung der Date von einer Datenträgereinheit nach dem Herausfiltern des weißen Rauschen
- 204 Zusätzliche Kodierungsdaten, die auf einer vom weißen Rauschen gereinigten Datenträgerabbildung enthalten sind
- 205 Vorrichtung zum Trennen der Kodierungsdaten in unabhängige Überprüfungskriterien
- 207 Spalte zum Eintragen von Parameter, die die Wasserzeichen kennzeichnen können
- 208 Spalte zum Eintragen von Serien-Nummern Daten
- 209 Spalte zum Eintragen von zusätzlichen Daten als Parametrisierte Werte
- 210 Tabelle mit unabhängigen Überprüfungskriterien
- 215 Datenspeicher für Parameter, Treiber und Verfahren, die in den Einheiten (200), (205) und (210) benutzt werden
- 222 Verfahrensschritt: Eingabe einer Zeichenkette
- 224 Verfahrensschritt: Eingabe, Erzeugung und Einbringung von Serien-Nummer-Daten
- 226 Verfahrensschritt: Auswahl der verwendeten Schlüssel, mit der die zusätzlichen Kodierungsdaten erzeugt und als

- unabhängige Überprüfungskriterien instanziiert werden können oder Benutzung des Standardschlüssels.
- 228 Verfahrensschritt: Auswahl der Regeln zur Erstellung der zusätzlichen Kodierung, zur Aufbringung der Kodierung und zur Festlegung des Verifikationsverfahrens oder Benutzung der entsprechenden Standardregeln
- 230 Verfahrensschritt: Berechnung des Wasserzeichens mit den in (222) - (228) ausgewählten, als Standard festgelegten oder eingegebenen Werte bzw. Verfahren.
- 232 Verfahrensschritt: Auswahl eines Aufbringungsmusters
- 234 Verfahrensschritt Erzeugung der Gesamtmenge der zusätzlichen Kodierungsdaten inklusive der Positionierungsdaten
- 236 Verfahrensschritt: Zusammenfassung der zusätzlichen Kodierungsdaten mit den Daten des elektronischen Dokumentes inklusive Modulation durch eine Kodetabelle od. dgl. und der Erstellung der auf den Datenträger aufzubringenden logischen Struktur
- 238 Verfahrensschritt: Test der Aufbringung und der Ausführung einer Verifizierung zur Überprüfung der Korrektheit
- 240 Verfahrensschritt: Lesen der zusätzlichen Kodierungsdaten und der Daten, die durch das weiße Rauschen entstanden sind
- 242 Verfahrensschritt: Auswahl des Verifikationsverfahrens und der Verifikationskriterien oder Benutzung der Standardwerte
- 244 Verfahrensschritt: Auswahl des Wasserzeichenextraktionsverfahrens oder Benutzung der Standardverfahrens
- 246 Verfahrensschritt: Auswahl des Serien-Nummerextraktionsverfahrens oder Benutzung der Standardverfahrens
- 248 Verfahrensschritt: Extrahieren des Wasserzeichens entsprechend des gewählten Verfahrens
- 250 Verfahrensschritt: Extrahieren der Serien-Nummer und / oder zusätzlicher verschlüsselter Kodierungen entsprechend des gewählten Verfahrens
- 252 Verfahrensschritt: Verifizieren, ob Wasserzeichen mit Serien-Nummer oder sonstigen Zusatzdaten innerhalb des Verifikationskriteriums übereinstimmt.
- 254 Verfahrensschritt: Ausgabe des Ergebnisses der Überprüfung.
- 260 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Schlüsseldaten
- 262 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Verfahren zur Erzeugung von Wasserzeichen, Serien-Nummer und sonstiger (verschlüsselter) Zusatzdaten

- 264 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Verfahren zur Berechnung der Aufbringungspunkte oder Aufbringungsmuster
- 266 Datenspeicher zur Ausgabe/Abspeicherung verschiedener Parameter/Verfahren
- 268 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Ausgabe-Templates
- 270 Herstellerseitige Kommunikationsschnittstelle für die mobilen Stationen
- 275 Kommunikationsschnittstelle mit dem Server
- 280 Datenspeicher zur Abspeicherung verschiedener Archivierungstemplates, Wasserzeichen-, Serien-Nummer und Zusatzdaten-Extraktionsverfahren, Parameter und Schlüssel; Datenspeicher für spezielle Treiber, Verifikationsverfahren und Ausgabe-Templates
- 282 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Verfahren zur Verifikation und zur Anwendung auf und von Überprüfungskriterien
- 284 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Verfahren zur Extraktion von Wasserzeichen und Serien-Nummern
- 286 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Treiber
- 288 Mittel zum Anbieten, Anwenden und Auswählen verschiedener Ausgabe-Templates
- 290 Management-Einheit zur Steuerung des Anbietens, des Anwendens, der Auswahl, der Aktualisierung der Daten im Datenspeicher und der Kommunikation mit dem Benutzer.

PATENTANSPRÜCHE

1. Vorrichtung zum Kopierschutz von digitale Dokumente tragenden Datenträgereinheiten (10), insbesondere von optisch lesbaren Datenträgern, mit Mitteln zum Aufbringen eines digitalen Inhalts (2) des digitalen Dokuments auf die Datenträgereinheit in einer der Datenträgereinheit zugeordneten physikalischen oder logischen Struktur und Mitteln zum Aufbringen einer zusätzlichen Codierung (3) auf die Datenträgereinheit durch vorbestimmtes Ändern der physikalischen Struktur und/oder der logischen Struktur so, dass bei einem bestimmungsgemäßen Abspiel- und/oder Darstellungsprozess der digitalen Datenträgereinheit (10) durch eine für eine Datenträgereinheit bestimmungsgemäß vorgesehene Abspiel- und/oder Darstellungseinheit (15) die zusätzliche digitale Codierung nicht erfasst wird und keinen Einfluss auf den auszugehenden oder darzustellenden digitalen Inhalt des digitalen Dokuments nimmt, dadurch gekennzeichnet, dass zur Erkennung eines autorisiert gefertigten Exemplars der Datenträgereinheit Verifizierungsmittel (20) vorgesehen sind, die unter Umgehung möglicher, bei der für eine Datenträgereinheit bestimmungsgemäß vorgesehenen Abspiel- und/oder Darstellungseinheit vorhandener Fehlerkorrektur- oder Filtereinheiten, einen unmittelbaren Lesezugriff auf die zusätzliche Codierung ermöglicht und insbesondere eine Feststellung ermöglicht, ob die zusätzliche Codierung vorhanden ist und der zusätzlichen Codierung, wie durch die Aufbringungsmittel aufgebracht, entspricht.
2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die Mittel zum Aufbringen der zusätzlichen Codierung so ausgebildet sind, dass sie innerhalb der logischen Struktur vorbestimmte digitale Änderungen, insbesondere innerhalb eines der strukturihären Redundanzbereichs,

vornimmt, wobei die vorbestimmten digitalen Änderungen so eingebracht sind, dass eine Fehlerkorrektur oder Filterung den digitalen Inhalt des elektronischen Dokuments unbeeinflusst lässt.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Mittel zum Aufbringen der zusätzlichen Codierung (3) so ausgebildet sind, dass sie zusätzliche Daten als vorbestimmte digitale Änderungen von einer oder mehreren der folgenden Arten erzeugen:
 - in Nutzdatenfeldern einer CD oder DVD enthaltende zusätzliche Daten,
 - in Kontrollfeldern (Subcode) einer CD oder DVD enthaltende zusätzliche Daten,
 - in redundanten EFM-artigen Byte-Darstellungen einer auf CD oder DVD abgelegten zusätzliche Daten,
 - in FDC-FCC-Korrekturfeldern abgelegte zusätzliche Daten,
 - in eine Lead-in-Lead-Out-Area einer CD oder DVD eingefügte zusätzliche Daten,zur Änderung von Header-, Nutz- oder Kontrolldaten in vorgestimmter Weise.
4. Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Mittel zum Aufbringen der zusätzlichen Codierung (3) so ausgebildet sind, dass sie in der physikalischen Struktur vorbestimmte Änderungen außerhalb der logischen Struktur in Form von nicht standardisierten Abmessungen entsprechenden Datenträgerkennungen, insbesondere defektartigen Signalelementen, vornehmen und/oder derartige defektartige, in der physikalischen Struktur inhärent vorhandene Signalelemente detektieren, wobei die Datenträgerkennungen bzw. die Signalelemente so ausgebildet sind, dass eine Fehlerkorrektur oder Filterung den digitalen Inhalt des elektronischen Dokuments unbeeinflusst lässt.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Mittel zum Aufbringen der zusätzlichen Codierung (3) so ausgebildet sind, dass sie als zusätzliche Codierung zusätzliche Daten zur Abwandlung einer Frame- und/oder Sektor- und/oder Trackeinteilung einer CD oder DVD erzeugen.
6. Verwendung der Vorrichtung nach einem der Ansprüche 1 bis 5 zum Kopierschutz von digitalen Dokumenten auf CDs, DVs und digitalen Bandmedien.
7. Verfahren zum Herstellen einer digitale Dokumente tragenden Datenträgereinheit, insbesondere Verfahren zum Betreiben der Vorrichtung nach einem der Ansprüche 1 bis 5, gekennzeichnet durch die Schritte:
 - Auslesen des digitalen Inhalt eines digitalen Dokuments aus einer Dokumentspeichereinheit;
 - Erzeugen von Daten einer zusätzlichen Codierung und Ablegen der Daten in einer Codierungsspeichereinheit;
 - Aufbringen des digitalen Inhalts auf die Datenträgereinheit und
 - Aufbringen der zusätzlichen Codierung auf die Datenträgereinheit,wobei die Daten der zusätzlichen Codierung so erzeugt sind, dass sie eine der Datenträgereinheit zugeordnete physikalische und/oder logische Struktur so ändern, dass bei einem bestimmungsgemäßen Abspiel- und/oder Darstellungsprozess der digitalen Datenträgereinheit durch eine für eine Datenträgereinheit bestimmungsgemäß vorgesehenen Abspiel- und/oder Darstellungseinheit die zusätzliche digitale Codierung nicht erfasst wird und keinen Einfluss auf den auszugebenden und darzustellenden digitalen Inhalt des digitalen Dokuments nimmt.
8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass das Aufbringen des digitalen Inhalts auf die Datenträgereinheit vor oder nach dem Aufbringen der zu-

sätzlichen Codierung, insbesondere in Form von zwei getrennten Herstellungsschritten, erfolgt.

9. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass das Aufbringen des digitalen Inhalts zusammen mit dem Aufbringen der zusätzlichen Codierung erfolgt, wobei durch eine auf die Datenträgereinheit physikalisch wirkende Aufbringungseinheit ein gemeinsamer, Daten des digitalen Dokuments und Daten der zusätzlichen Codierung enthaltener Datensatz, bevorzugt in einem einzigen Bearbeitungsvorgang, aufgebracht wird.
10. Verfahren nach einem der Ansprüche 1 bis 7 zur Herstellung einer die digitalen Dokumente tragenden CD oder DVD, dadurch gekennzeichnet, dass der Schritt des Aufbringens der zusätzlichen Codierung das physikalische Verändern einer Signalcodierung auf einer zur Herstellung der CD oder DVD benutzten Matrize, das unmittelbare Verändern einer Signalcodierung auf einer hergestellten CD oder DVD selbst innerhalb einer logischen Datenstruktur der CD oder DVD, oder das unmittelbare Verändern der Signalstruktur der CD oder DVD außerhalb der logischen Struktur der CD oder DVD aufweist.
11. Verfahren zum Verifizieren einer digitale Dokumente tragenden Datenträgereinheit, insbesondere Verfahren zum Betreiben der Vorrichtung nach einem der Ansprüche 1 bis 5, gekennzeichnet durch den Schritt des Erfassens einer zusätzlichen Codierung auf der Datenträgereinheit, die durch vorbestimmtes Ändern der physikalischen und/oder der logischen Struktur der Datenträgereinheit so gebildet ist, dass bei einem bestimmungsgemäßen Abspiel- und/oder Darstellungsprozess der digitalen Datenträgereinheit durch eine für eine Datenträgereinheit bestimmungsgemäß vorgesehene Abspiel- und/oder Darstellungseinheit die zusätzliche digitale Codierung nicht erfasst wird und keinen Einfluss auf den auszugebenden oder

darzustellenden digitalen Inhalt des digitalen Dokuments nimmt, und

- Ausüben einer Mehrzahl von digitalen Rechnungsoperationen auf die Daten der erfassten zusätzlichen Codierung zum Erhalten einer Mehrzahl von voneinander unterschiedlichen digitalen Wasserzeichen.

12. Verfahren nach Anspruch 11, gekennzeichnet durch den Schritt des zusätzlichen Verknüpfens von mindestens einem der berechneten digitalen Wasserzeichen mit einem individualisierenden Kenner der Datenträgereinheit, wobei weiter bevorzugt der individualisierende Kenner in Form einer Seriennummer durch ein Private-/Public-Key-Verfahren in Beziehung mit dem Wasserzeichen gesetzt wird.
13. Vorrichtung nach einem der Ansprüche 1 bis 6, gekennzeichnet durch Mittel zur Kommunikations- oder Betriebssteuerung (9) der abspiel- und/oder Darstellungseinheit so ausgebildet sind, dass abhängig von einem als Reaktion auf die Feststellung von erzeugten Ausgangssignal der Verifizierungsmittel bestimmte Abspiel-, Darstellungs-, Kopier- oder Datenübertragungsmodi der Abspiel- und/oder Darstellungseinheit aktiviert oder unterdrückt werden können.
14. Vorrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Mittel zum Aufbringen einer zusätzlichen Codierung so ausgebildet sind, dass die zusätzliche digitale Codierung Informationen über dem elektronischen Dokument zugeordnete Nutzungsrechte bzw. Nutzungsrechtsbeschränkungen enthält.

Fig. 1

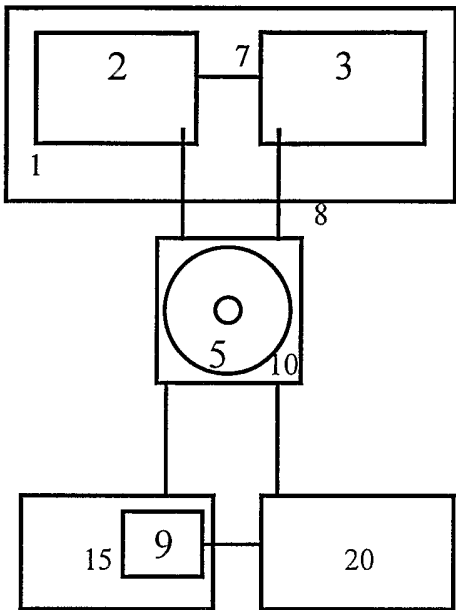


Fig. 2

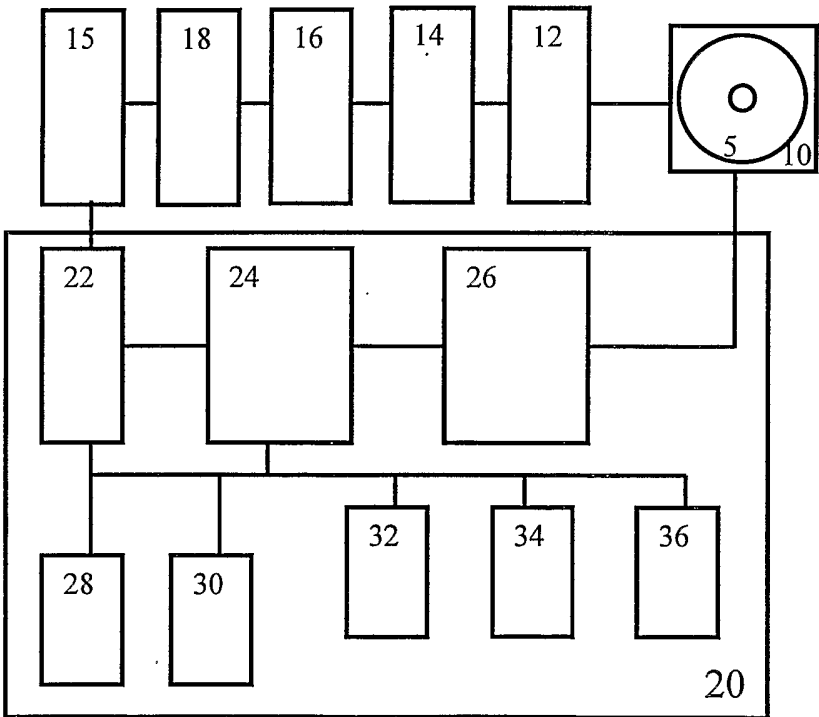


Fig. 3

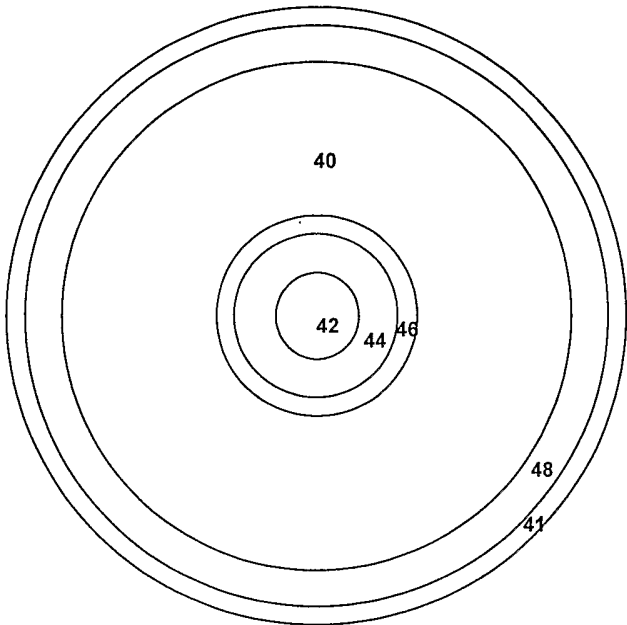


Fig. 4

Data bits	EFM
0000 0000	0100100 0100000
0000 0001	1000010 0000000
0000 0010	1001000 0100000
0000 0011	1000100 0100000
0000 0100	0100010 0000000
0000 0101	0000010 0010000
0000 0110	0001000 0100000
0000 0111	0010010 0000000
0000 1000	0100100 1000000
0000 1001	1000000 1000000
0000 1010	1001000 1000000
.....

Fig. 6

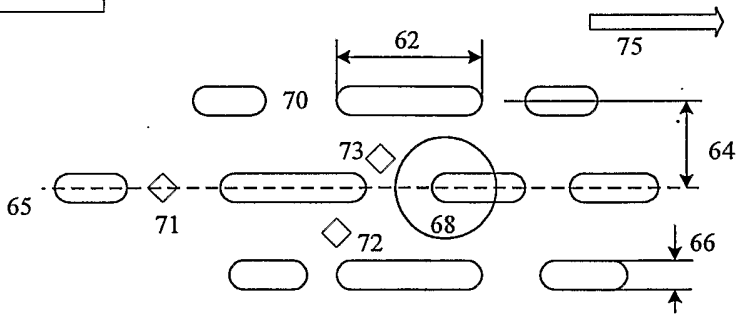


Fig. 7

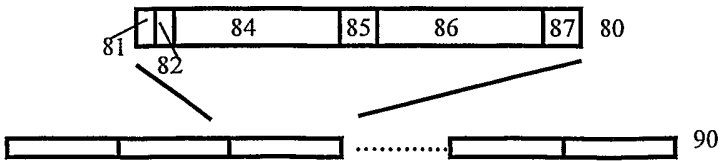


Fig. 5

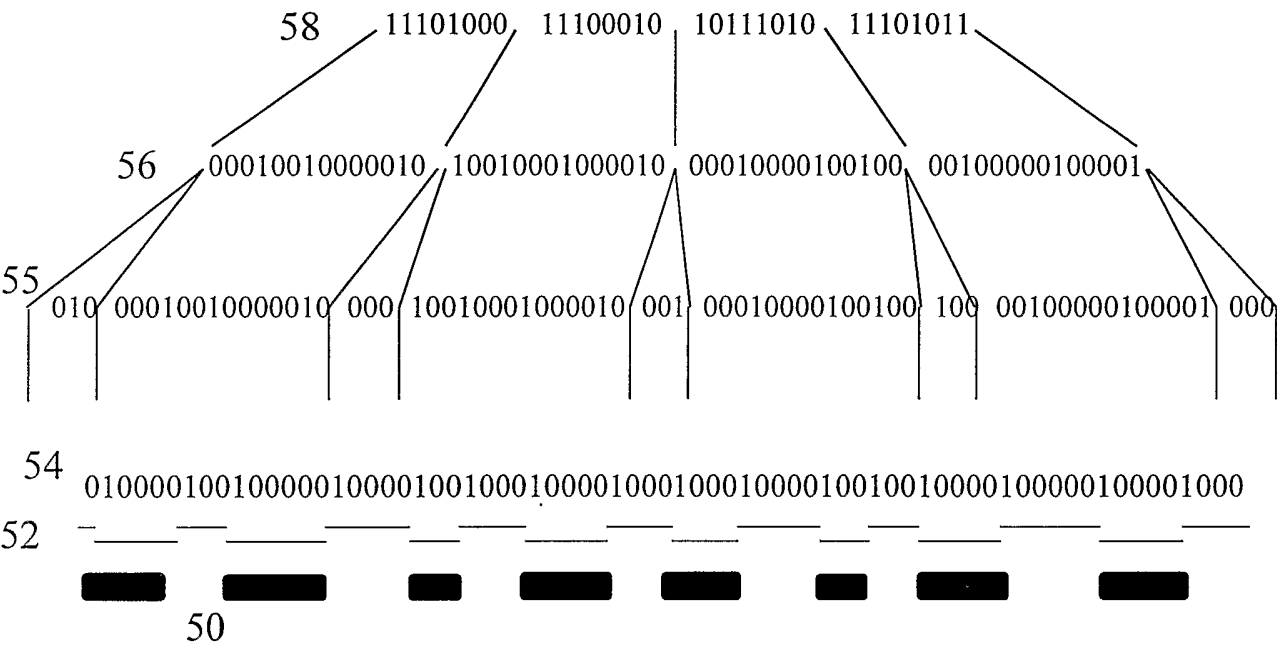


Fig. 8

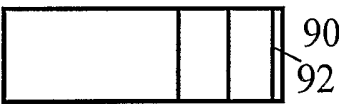


Fig. 9

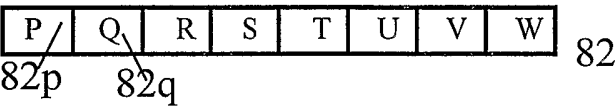


Fig. 10

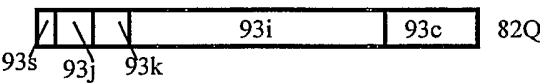


Fig. 11

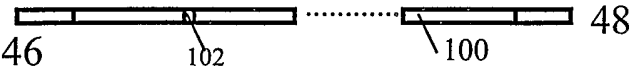


Fig. 12

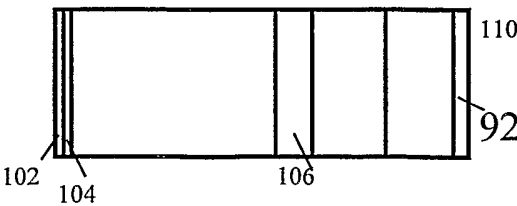
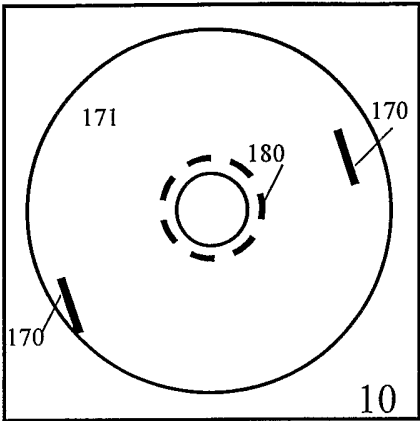


Fig. 15
A



B

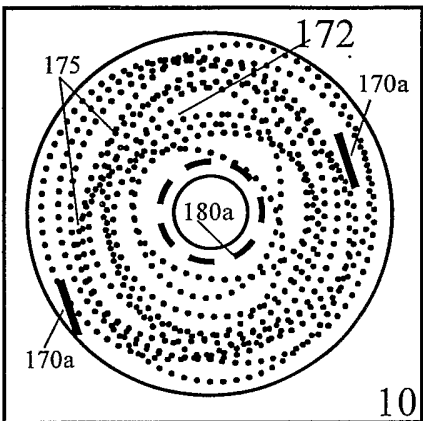
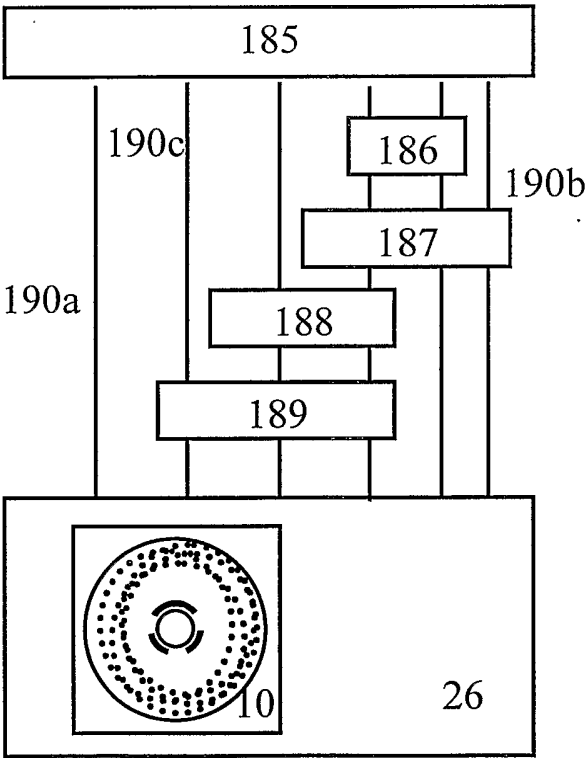


Fig. 16



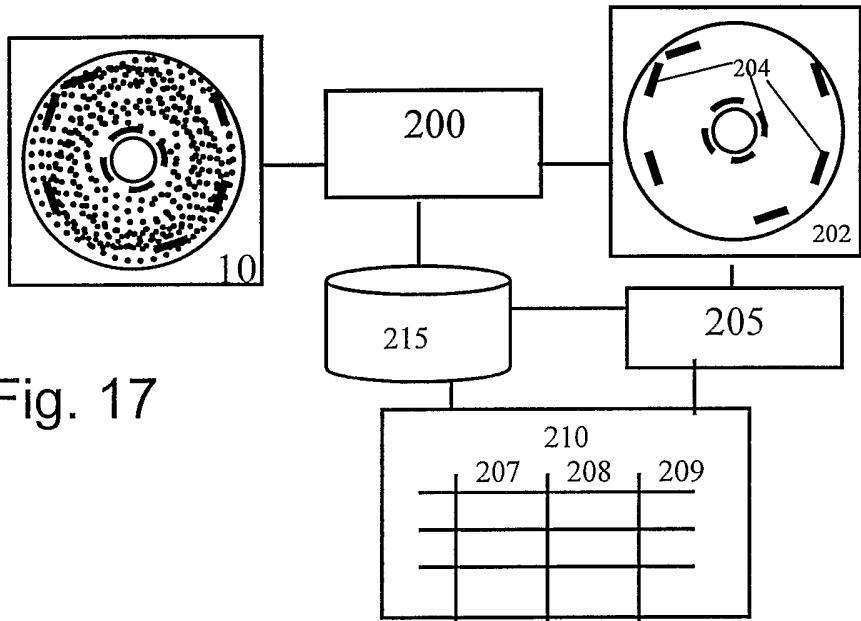


Fig. 17

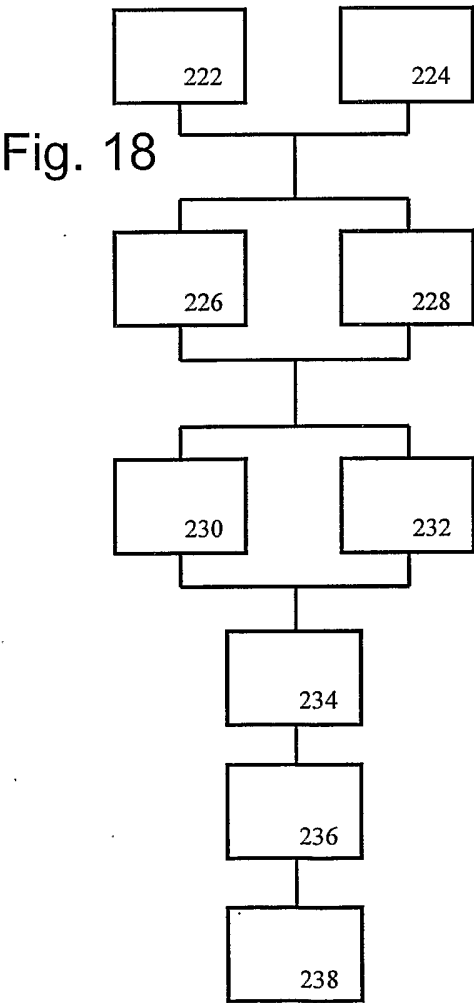


Fig. 18

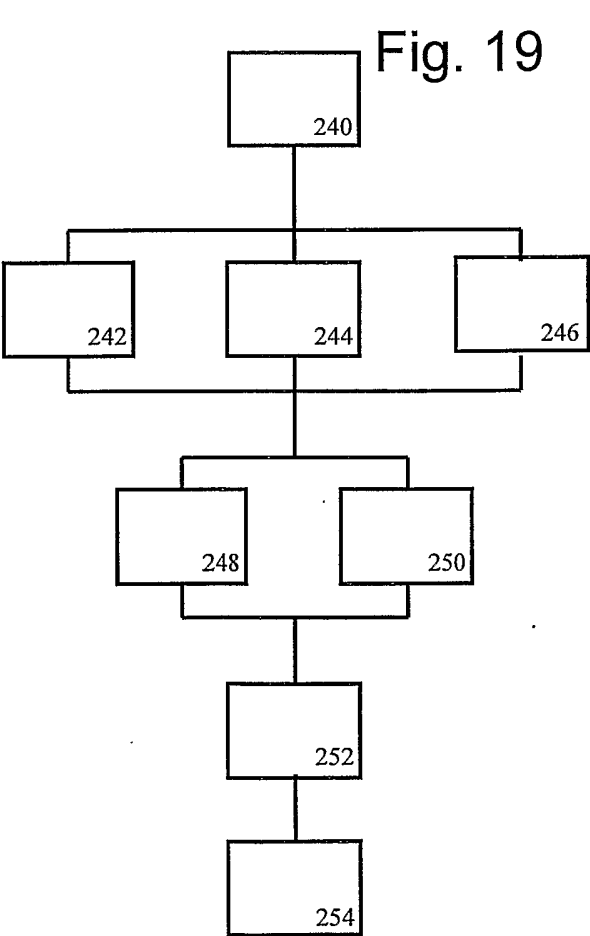
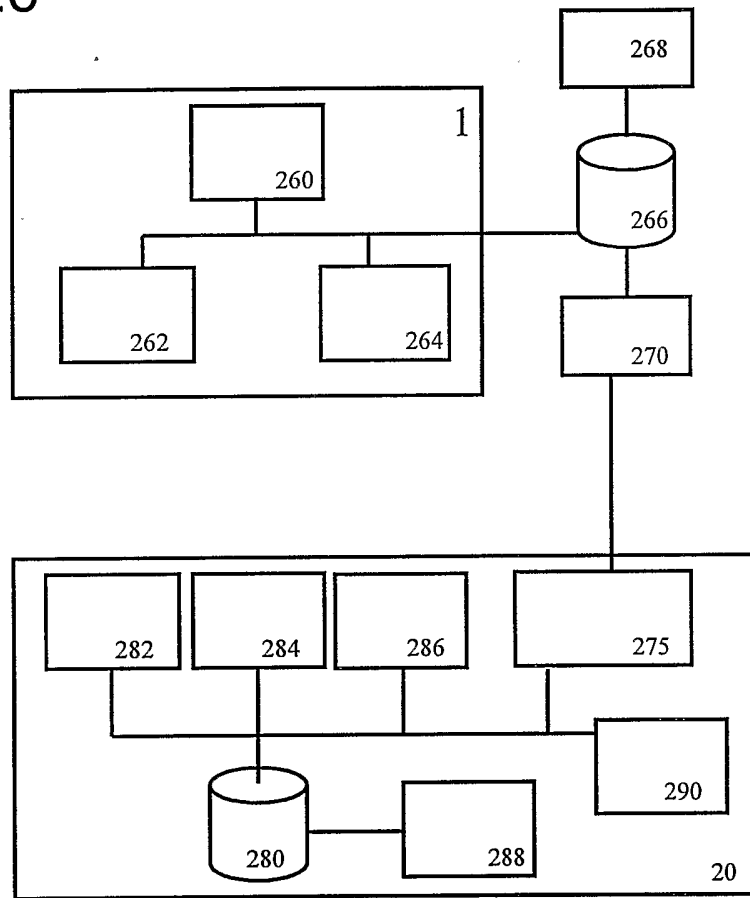


Fig. 19

Fig. 20



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 02/09392

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 62293 A (MACROVISION CORP) 19 October 2000 (2000-10-19) the whole document ----	1-3,6-14
X	EP 0 899 733 A (SONY DADC AUSTRIA AG) 3 March 1999 (1999-03-03) the whole document ----	1-3,6-14
X	GB 2 348 585 A (IBM) 4 October 2000 (2000-10-04) abstract page 1, line 1 -page 2, line 20 ----- -/--	1-3,6-14

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

° Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

13 January 2003

Date of mailing of the international search report

07/02/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Authorized officer

Sucher, R

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/09392

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 908 881 A (TOKYO SHIBAURA ELECTRIC CO) 14 April 1999 (1999-04-14) abstract paragraph '0001! - paragraph '0019! paragraph '0023! - paragraph '0053! figure 1 ----	1-3,6-14
X	EP 0 901 122 A (PIONEER ELECTRONIC CORP) 10 March 1999 (1999-03-10) abstract paragraph '0066! - paragraph '0110! figures 1-5 ----	1-3,6-14
X	WO 99 63538 A (CORP INTERNATIONAL ENTERPRISE; KARITANI SHOGO (US)) 9 December 1999 (1999-12-09) the whole document ----	1-3,6-14
X	WO 98 01852 A (IFUNGA TEST EQUIPMENT B V; BARCHAN JAN (SE)) 15 January 1998 (1998-01-15) the whole document ----	1-3,6-14
X	WO 98 52114 A (IMATION CORP) 19 November 1998 (1998-11-19) the whole document ----	1-3,6-14
X	US 5 930 209 A (SPITZENBERGER UWE ET AL) 27 July 1999 (1999-07-27) abstract column 10, line 18 -column 11, line 17 ----	1-3,6-14
X	US 6 076 165 A (MAENZA GLENN J) 13 June 2000 (2000-06-13) the whole document ----	1-3,6-14
X	EP 0 637 023 A (VICTOR COMPANY OF JAPAN) 1 February 1995 (1995-02-01) abstract column 13, line 20 -column 17, line 29 figures 1-4 ----	1,2,4, 6-14
X	WO 00 74053 A (DILLA LTD C; EDWARDS ROGER (GB)) 7 December 2000 (2000-12-07) the whole document ----	1-3,5-14
P,X	WO 01 61696 A (MACROVISION EUROP LTD; EDWARDS ROGER (GB); HEYLEN RICHARD A A (GB)) 23 August 2001 (2001-08-23) the whole document -----	1,2,5-14

INTERNATIONAL SEARCH REPORT

*Information on patent family members

International Application No

PCT/EP 02/09392

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0062293	A	19-10-2000	AU 4238400 A WO 0062293 A1	14-11-2000 19-10-2000
EP 0899733	A	03-03-1999	EP 0899733 A1 AT 199990 T AU 750499 B2 AU 8194998 A BR 9806518 A CA 2245232 A1 CN 1219728 A DE 69704352 D1 DE 69704352 T2 ES 2155230 T3 JP 11250512 A SG 71803 A1	03-03-1999 15-04-2001 18-07-2002 11-03-1999 13-03-2001 28-02-1999 16-06-1999 26-04-2001 12-07-2001 01-05-2001 17-09-1999 18-04-2000
GB 2348585	A	04-10-2000	CN 1262509 A JP 2000224411 A	09-08-2000 11-08-2000
EP 0908881	A	14-04-1999	JP 11086436 A CN 1211788 A EP 0908881 A2 US 6490683 B1	30-03-1999 24-03-1999 14-04-1999 03-12-2002
EP 0901122	A	10-03-1999	EP 0901122 A2 JP 11154375 A	10-03-1999 08-06-1999
WO 9963538	A	09-12-1999	AU 4100499 A WO 9963538 A1	20-12-1999 09-12-1999
WO 9801852	A	15-01-1998	SE 514352 C2 AT 196561 T DE 69703155 D1 DE 69703155 T2 EP 0907952 A1 ES 2152099 T3 JP 2002500796 T KR 2000023570 A SE 9602656 A SE 9603763 A WO 9801852 A1 TW 444194 B US 6226770 B1	12-02-2001 15-10-2000 26-10-2000 17-05-2001 14-04-1999 16-01-2001 08-01-2002 25-04-2000 06-01-1998 06-01-1998 15-01-1998 01-07-2001 01-05-2001
WO 9852114	A	19-11-1998	AU 7362198 A WO 9852114 A1	08-12-1998 19-11-1998
US 5930209	A	27-07-1999	CA 2232818 A1 EP 0852053 A2 WO 9803973 A2 JP 11514126 T	29-01-1998 08-07-1998 29-01-1998 30-11-1999
US 6076165	A	13-06-2000	NONE	
EP 0637023	A	01-02-1995	JP 2806219 B2 JP 7121907 A AT 223103 T CN 1100549 A ,B	30-09-1998 12-05-1995 15-09-2002 22-03-1995

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 02/09392

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0637023	A		DE 69431225 D1	02-10-2002
			EP 0637023 A1	01-02-1995
			KR 153225 B1	15-12-1998
			SG 42776 A1	17-10-1997
			US 5696757 A	09-12-1997
			JP 3061098 B2	10-07-2000
			JP 7272282 A	20-10-1995
WO 0074053	A	07-12-2000	AU 5088500 A	18-12-2000
			BR 0006159 A	17-04-2001
			CA 2338826 A1	07-12-2000
			CN 1310841 T	29-08-2001
			EP 1101222 A1	23-05-2001
			WO 0074053 A1	07-12-2000
			GB 2355575 A	25-04-2001
			PL 345732 A1	02-01-2002
WO 0161696	A	23-08-2001	AU 3211901 A	27-08-2001
			BR 0104458 A	21-05-2002
			CN 1365496 T	21-08-2002
			EP 1169709 A1	09-01-2002
			WO 0161696 A1	23-08-2001
			NO 20014952 A	12-12-2001
			US 2002159355 A1	31-10-2002

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G11B20/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G11B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 00 62293 A (MACROVISION CORP) 19. Oktober 2000 (2000-10-19) das ganze Dokument	1-3,6-14
X	EP 0 899 733 A (SONY DADC AUSTRIA AG) 3. März 1999 (1999-03-03) das ganze Dokument	1-3,6-14
X	GB 2 348 585 A (IBM) 4. Oktober 2000 (2000-10-04) Zusammenfassung Seite 1, Zeile 1 -Seite 2, Zeile 20	1-3,6-14
	-/-	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

13. Januar 2003

Absenddatum des internationalen Recherchenberichts

07/02/2003

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Sucher, R

G.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 908 881 A (TOKYO SHIBAURA ELECTRIC CO) 14. April 1999 (1999-04-14) Zusammenfassung Absatz '0001! - Absatz '0019! Absatz '0023! - Absatz '0053! Abbildung 1 ---	1-3,6-14
X	EP 0 901 122 A (PIONEER ELECTRONIC CORP) 10. März 1999 (1999-03-10) Zusammenfassung Absatz '0066! - Absatz '0110! Abbildungen 1-5 ---	1-3,6-14
X	WO 99 63538 A (CORP INTERNATIONAL ENTERPRISE; KARITANI SHOGO (US)) 9. Dezember 1999 (1999-12-09) das ganze Dokument ---	1-3,6-14
X	WO 98 01852 A (IFUNGA TEST EQUIPMENT B V; BARCHAN JAN (SE)) 15. Januar 1998 (1998-01-15) das ganze Dokument ---	1-3,6-14
X	WO 98 52114 A (IMATION CORP) 19. November 1998 (1998-11-19) das ganze Dokument ---	1-3,6-14
X	US 5 930 209 A (SPITZENBERGER UWE ET AL) 27. Juli 1999 (1999-07-27) Zusammenfassung Spalte 10, Zeile 18 -Spalte 11, Zeile 17 ---	1-3,6-14
X	US 6 076 165 A (MAENZA GLENN J) 13. Juni 2000 (2000-06-13) das ganze Dokument ---	1-3,6-14
X	EP 0 637 023 A (VICTOR COMPANY OF JAPAN) 1. Februar 1995 (1995-02-01) Zusammenfassung Spalte 13, Zeile 20 -Spalte 17, Zeile 29 Abbildungen 1-4 ---	1,2,4, 6-14
X	WO 00 74053 A (DILLA LTD C; EDWARDS ROGER (GB)) 7. Dezember 2000 (2000-12-07) das ganze Dokument ---	1-3,5-14
P,X	WO 01 61696 A (MACROVISION EUROP LTD; EDWARDS ROGER (GB); HEYLEN RICHARD A A (GB)) 23. August 2001 (2001-08-23) das ganze Dokument -----	1,2,5-14

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 02/09392

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0062293	A	19-10-2000	AU 4238400 A WO 0062293 A1	14-11-2000 19-10-2000
EP 0899733	A	03-03-1999	EP 0899733 A1 AT 199990 T AU 750499 B2 AU 8194998 A BR 9806518 A CA 2245232 A1 CN 1219728 A DE 69704352 D1 DE 69704352 T2 ES 2155230 T3 JP 11250512 A SG 71803 A1	03-03-1999 15-04-2001 18-07-2002 11-03-1999 13-03-2001 28-02-1999 16-06-1999 26-04-2001 12-07-2001 01-05-2001 17-09-1999 18-04-2000
GB 2348585	A	04-10-2000	CN 1262509 A JP 2000224411 A	09-08-2000 11-08-2000
EP 0908881	A	14-04-1999	JP 11086436 A CN 1211788 A EP 0908881 A2 US 6490683 B1	30-03-1999 24-03-1999 14-04-1999 03-12-2002
EP 0901122	A	10-03-1999	EP 0901122 A2 JP 11154375 A	10-03-1999 08-06-1999
WO 9963538	A	09-12-1999	AU 4100499 A WO 9963538 A1	20-12-1999 09-12-1999
WO 9801852	A	15-01-1998	SE 514352 C2 AT 196561 T DE 69703155 D1 DE 69703155 T2 EP 0907952 A1 ES 2152099 T3 JP 2002500796 T KR 2000023570 A SE 9602656 A SE 9603763 A WO 9801852 A1 TW 444194 B US 6226770 B1	12-02-2001 15-10-2000 26-10-2000 17-05-2001 14-04-1999 16-01-2001 08-01-2002 25-04-2000 06-01-1998 06-01-1998 15-01-1998 01-07-2001 01-05-2001
WO 9852114	A	19-11-1998	AU 7362198 A WO 9852114 A1	08-12-1998 19-11-1998
US 5930209	A	27-07-1999	CA 2232818 A1 EP 0852053 A2 WO 9803973 A2 JP 11514126 T	29-01-1998 08-07-1998 29-01-1998 30-11-1999
US 6076165	A	13-06-2000	KEINE	
EP 0637023	A	01-02-1995	JP 2806219 B2 JP 7121907 A AT 223103 T CN 1100549 A ,B	30-09-1998 12-05-1995 15-09-2002 22-03-1995

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 02/09392

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0637023 A		DE 69431225 D1	02-10-2002
		EP 0637023 A1	01-02-1995
		KR 153225 B1	15-12-1998
		SG 42776 A1	17-10-1997
		US 5696757 A	09-12-1997
		JP 3061098 B2	10-07-2000
		JP 7272282 A	20-10-1995
WO 0074053 A	07-12-2000	AU 5088500 A	18-12-2000
		BR 0006159 A	17-04-2001
		CA 2338826 A1	07-12-2000
		CN 1310841 T	29-08-2001
		EP 1101222 A1	23-05-2001
		WO 0074053 A1	07-12-2000
		GB 2355575 A	25-04-2001
		PL 345732 A1	02-01-2002
WO 0161696 A	23-08-2001	AU 3211901 A	27-08-2001
		BR 0104458 A	21-05-2002
		CN 1365496 T	21-08-2002
		EP 1169709 A1	09-01-2002
		WO 0161696 A1	23-08-2001
		NO 20014952 A	12-12-2001
		US 2002159355 A1	31-10-2002