(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-108754
(P2006-108754A)
(43)公開日　平成18年4月20日(2006.4.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5B017
G06F 21/24	(2006.01)	G06F	12/14	520P	5D044
G11B 20/10	(2006.01)	G06F	12/14	540P	5J104
G11B 20/12	(2006.01)	G06F	12/14	550A	
		G11B	20/10	H	

審査請求 未請求　請求項の数 16　ＯＬ　（全 25 頁）　最終頁に続く

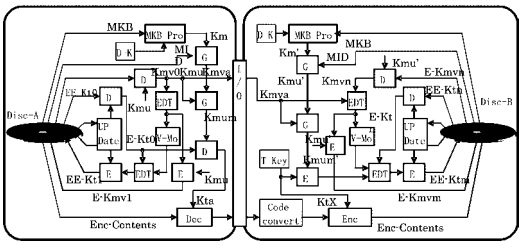
(21)出願番号　特願2004-288469 (P2004-288469)
(22)出願日　平成16年9月30日 (2004.9.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100109900
弁理士　堀口　浩
(72)発明者　小島　正
東京都青梅市新町３丁目３番地の１　東芝デジタルメディアエンジニアリング株式会社内

Ｆターム(参考)　5B017 AA06 BA07 BA08 CA09
5D044 AB05 AB07 BC01 BC04 CC04 DE11 DE17 DE50 GK12 GK17
5J104 AA12 AA16 AA34 EA04 EA09 EA15 EA16 EA18 JA03 NA02 NA27 NA37 PA14

(54)【発明の名称】コンテンツ管理方法及び記録再生装置及び記録媒体

(57)【要約】
【課題】　ＤＶＤとＤＶＤなどのリムーバブル媒体間、ＤＶＤからＨＤＤなどリムーバブル媒体から固定媒体間のムーブを可能にしたコンテンツ管理方法及び記録再生装置を提供する。
【解決手段】　タイトル鍵によって暗号化された暗号化コンテンツと、前記タイトル鍵を暗号化して記録媒体に記録し、再生の際は、前記暗号化されたタイトル鍵を復号化しこれを用いて前記コンテンツを復号化するコンテンツ管理方法において、
　前記タイトル鍵をコンテンツムーブ鍵によって暗号化し、コンテンツを複製させる再には、元の記録媒体からコンテンツムーブ鍵を削除し、暗号化コンテンツと暗号化タイトル鍵は消去しないように管理するコンテンツ管理方法及び記録再生装置。
【選択図】　図６



【特許請求の範囲】
【請求項１】
第１の鍵で暗号化されたコンテンツデータと、第２の鍵と第４の鍵で暗号化され、さらに第３の鍵で暗号化された第１の鍵と、前記第４の鍵で暗号化された第２の鍵及び第３の鍵とが記録された記録媒体から他の記録媒体に前記コンテンツデータを移動させるに際し、
前記記録媒体に記録されている前記暗号化された第２の鍵及び第３の鍵を読み出し、前記第４の鍵を用いて前記第２の鍵及び第３の鍵を復号化し、
前記記録媒体に記録されている暗号化された前記第１の鍵を読み出し、前記第４の鍵、前記複合化された第２の鍵及び第３の鍵を用いて第１の鍵を復号化し、
前記記録媒体に記録されている暗号化された前記コンテンツデータを読み出し、前記復号化された第１の鍵を用いて前記コンテンツを復号化し、
前記複合化されたコンテンツと共に前記第２の鍵を前記他の記録媒体に伝送し、
前記第３の鍵を更新し、
前記第１の鍵を前記第２の鍵と前記第４の鍵を用いて暗号化し、さらに前記更新した第３の鍵を用いて暗号化し、
前記暗号化された第１の鍵を、前記記録媒体に記録されている暗号化された第１の鍵と書き換え、
前記記録媒体に記録されている暗号化された第２の鍵を消去することを特徴とするコンテンツ管理方法。
【請求項２】
前記他の記録媒体から前記記録媒体に前記コンテンツを再び移動させる場合、前記第２の鍵を前記第４の鍵で暗号化し、前記記録媒体に記録することを特徴とする請求項１記載のコンテンツ管理方法。
【請求項３】
前記第４の鍵は、前記記録媒体に固有のメディア固有鍵であることを特徴とする請求項１或いは請求項２記載のコンテンツ管理方法。
【請求項４】
前記第３の鍵は、記録再生ドライブ内でのみ、復号再生及び鍵データ更新、並びに記録処理を許可する、秘匿データであることを特徴とする請求項１乃至請求項３のいずれかに記載のコンテンツ管理方法。
【請求項５】
前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵及び第２の鍵は、暗号化されたデータファイルとして記録媒体に記録される場合、複数の第２の鍵を演算処理して証明データを作成し、暗号化された第１の鍵のデータファイルに組み込んで、第３の鍵で暗号化し、多重暗号化された第１の鍵と暗号化された第２の鍵の証明データで構成された暗号化データファイルとして、前記記録媒体に記録されていることを特徴とする請求項１乃至請求項４のいずれかに記載のコンテンツ管理方法。
【請求項６】
前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵は前記第４の鍵と前記第２の鍵によって合成された暗号鍵で暗号化され、暗号化された第１の鍵のデータファイルとし、前記複数の第２の鍵は、前記第４の鍵で暗号化され、暗号化された第２の鍵のデータファイルとし、暗号化された第１の鍵のデータファイルと、暗号化された第２の鍵のデータファイルは、共に更新された第３の鍵で暗号化され、記録媒体に記録されていることを特徴とする請求項１乃至請求項４のいずれかに記載のコンテンツ管理方法。
【請求項７】
前記暗号化された第１の鍵のデータファイルにおける各鍵の付帯情報として、コンテン

ツデータの識別番号と暗号化された第２の鍵が前記記録媒体に記録されているか、消去されているかを示すフラグが設けられており、
前記暗号化された第２の鍵のデータファイルにおいて、消去された第２の鍵も含めて、各鍵の付帯情報として、コンテンツデータの識別番号と、暗号化された第１の鍵が前記記録媒体に記録されているかを示す識別フラグが設けられていることを特徴とする請求項５或いは請求項６記載のコンテンツ管理方法。
【請求項８】
第１の鍵で暗号化されたコンテンツデータと、第２の鍵と第４の鍵で暗号化され、さらに第３の鍵で暗号化された第１の鍵と、前記第４の鍵で暗号化された第２の鍵及び第３の鍵とが記録された記録媒体から他の記録媒体に前記コンテンツデータを移動させる記録再生装置であって、
前記記録媒体に記録されている前記暗号化された第２の鍵及び第３の鍵を読み出し、前記第４の鍵を用いて前記第２の鍵及び第３の鍵を復号化する復号手段と、
前記記録媒体に記録されている暗号化された前記第１の鍵を読み出し、前記第４の鍵、前記複合化された第２の鍵及び第３の鍵を用いて第１の鍵を復号化する復号手段と、
前記記録媒体に記録されている暗号化された前記コンテンツデータを読み出し、前記復号化された第１の鍵を用いて前記コンテンツを復号化する復号化手段と、
前記複合化されたコンテンツと共に前記第２の鍵を前記他の記録媒体に伝送する伝送手段と、
前記第３の鍵を更新する更新手段と、
前記第１の鍵を前記第２の鍵と前記第４の鍵を用いて暗号化し、さらに前記更新した第３の鍵を用いて暗号化する暗号化手段と、
前記暗号化された第１の鍵を、前記記録媒体に記録されている暗号化された第１の鍵と書き換える書き換え手段と、
前記記録媒体に記録されている暗号化された第２の鍵を消去する消去手段とを具備することを特徴とする記録再生装置。
【請求項９】
前記他の記録媒体から前記記録媒体に前記コンテンツを再び移動させる場合、前記第２の鍵を前記第４の鍵で暗号化し、前記記録媒体に記録することを特徴とする請求項８記載の記録再生装置。
【請求項１０】
前記第４の鍵は、前記記録媒体に固有のメディア固有鍵であることを特徴とする請求項８或いは請求項９記載の記録再生装置。
【請求項１１】
前記第３の鍵は、記録再生ドライブ内でのみ、復号再生及び鍵データ更新、並びに記録処理を許可する、秘匿データであることを特徴とする請求項８乃至請求項１０のいずれかに記載の記録再生装置。
【請求項１２】
前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵及び第２の鍵は、暗号化されたデータファイルとして記録媒体に記録される場合、複数の第２の鍵を演算処理して証明データを作成し、暗号化された第１の鍵のデータファイルに組み込んで、第３の鍵で暗号化し、多重暗号化された第１の鍵と暗号化された第２の鍵の証明データで構成された暗号化データファイルとして、前記記録媒体に記録されていることを特徴とする請求項８乃至請求項１１のいずれかに記載の記録再生装置。
【請求項１３】
前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵は前記第４の鍵と前記第２の鍵によって合成された暗号鍵で暗号化され、暗号化された第１の鍵のデータファイルとし、前記複数の第２の鍵は、前記第４の鍵で暗号化され、暗号化され

た第２の鍵のデータファイルとし、暗号化された第１の鍵のデータファイルと、暗号化された第２の鍵のデータファイルは、共に更新された第３の鍵で暗号化され、記録媒体に記録されていることを特徴とする請求項８乃至請求項１１のいずれかに記載の記録再生装置。

【請求項１４】

前記暗号化された第１の鍵のデータファイルにおける各鍵の付帯情報として、コンテンツデータの識別番号と暗号化された第２の鍵が前記記録媒体に記録されているか、消去されているかを示すフラグが設けられており、

前記暗号化された第２の鍵のデータファイルにおいて、消去された第２の鍵も含めて、各鍵の付帯情報として、コンテンツデータの識別番号と、暗号化された第１の鍵が前記記録媒体に記録されているかを示す識別フラグが設けられていることを特徴とする請求項１２或いは請求項１３記載の記録再生装置。

【請求項１５】

複数の第１の鍵で暗号化された複数のコンテンツデータと、

記録媒体固有の鍵と複数の第２の鍵で暗号化された複数の第１の鍵のデータファイルを第３の鍵で多重暗号化した第１の鍵のデータファイルと、

記録媒体固有の鍵で暗号化された複数の第２の鍵で構成された第２の鍵のデータファイルと、

記録媒体固有の鍵で暗号化された第３の鍵とが記録されたことを特徴とする記録媒体。

【請求項１６】

複数の第１の鍵で暗号化された複数のコンテンツデータと、

記録媒体固有の鍵と複数の第２の鍵で暗号化された複数の第１の鍵のデータファイルを第３の鍵で多重暗号化した第１の鍵のデータファイルと、

記録媒体固有の鍵で暗号化された複数の第２の鍵が第３の鍵で多重暗号化された第２の鍵で構成された第２の鍵のデータファイルと、

記録媒体固有の鍵で暗号化された第３の鍵とが記録されたことを特徴とする記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンテンツデータを管理するコンテンツ管理方法及び記録再生装置に関する。

【背景技術】

【０００２】

従来、デジタル化された情報（例えば、文書、音声、画像、プログラムなど）を記録する媒体として、ＣＤ（コンパクトディスク）やＤＶＤ（デジタルバーサタイルディスク）がある。

【０００３】

このようなデジタル記録媒体では、デジタルデータを記録しているため、記録されたデータを他のデジタル記録媒体に音質や画質の損失なしに容易に複製できる。このような特徴は、複製を大量に作成することが可能となり、複製したディスクを不正に譲渡するなど著作権侵害を誘発する恐れがある。

【０００４】

そこで著作物であるコンテンツを暗号化し、その暗号鍵を秘匿し、他の暗号鍵で暗号化して記録媒体に一緒に記録することによって違法コピーを防止する施策がなされている。しかしながら、最近は暗号化されたままのコンテンツ（以下暗号化コンテンツと記す）を暗号化された暗号鍵（以下暗号化暗号鍵と記す）も含めて、丸ごとデジタル記録媒体に複製する違反者も出現している。

【０００５】

また、デジタルＴＶ放送のように、コンテンツの格納を一箇所の記録媒体のみしか認めない著作権管理方法（コピーワンス）がなされている。この方法では、コンテンツを一箇

所の記録媒体のみに格納を認めているため、元の記録媒体のコンテンツを消去或いは再生不可とすることを前提として、他の記録媒体に複製を許可するいわゆるコンテンツのムーブは認めている。この場合、元の記録媒体では暗号鍵を消去してコンテンツの復号を不可能にすることでコンテンツを再生不可としている。

【０００６】

この方法では、記録媒体には暗号化されたコンテンツはそのまま残っていることになっている。そこでなにがしらの方法で消去したはずの暗号鍵を復活させられると、暗号化された状態のコンテンツを復号化して再生することが可能となってしまう。結果として他の記録媒体に複製したコンテンツを合わせて複数箇所に再生可能なコンテンツが存在してしまう。このような不正行為による暗号鍵の復活を如何に防止するかが重要である。

【０００７】

コンテンツデータをムーブすることを可能とした著作権保護法式として、特許文献１、特許文献２、特許文献３がある。これらの文献には、コンテンツの違法コピー防止技術として、不正コピーがされた場合の暗号鍵リボークシステムや別のデジタル記録媒体に違法コピーができないように、メディアバインド機能を持たせる方法が記載されている。例えば、コンテンツ暗号鍵は別の暗号鍵で暗号化し、暗号化コンテンツと共に同じ記録媒体に記録しているが、正規の行為としてコンテンツを記録媒体間でムーブさせた後、元の記録媒体の消去された暗号化暗号鍵を、不正行為で復活させることを防止する技術が記載されている。

【０００８】

これらの発明は、丸ごとコピーを防ぐ為、記録媒体へのデータ記録再生処理を行なうドライブ内にて行われる、秘匿情報記録再生システムを導入し、ドライブ外からその秘匿情報が見えない構造を採用する方式である。秘匿情報は、暗号鍵管理体系に組み込まれる暗号鍵の一部として構成される為、外部に出される全てのデータを丸ごとコピーしても、暗号化コンテンツの復号はできない。

【０００９】

一方でこれらの発明では、既存のＤＶＤドライブ等が対応不可能になる。特許文献４は、デジタルデータコンテンツを最初にダウンロードする時のみ、コンテンツを暗号化する暗号鍵を、現在のＤＶＤ記録ドライブで採用されている「ＣＰＲＭ：Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ ｆｏｒ Ｒｅｃｏｒｄａｂｌｅ Ｍｅｄｉａ」方式で暗号化した「暗号化暗号鍵ファイル」と更に上記秘匿情報記録再生方式を導入して秘匿情報による暗号鍵で多重暗号化した「多重暗号化暗号鍵ファイル」の二種類生成して記録し、最初にダウンロードされた記録媒体から他の記録媒体にコンテンツムーブを行う場合は、暗号化コンテンツと多重暗号化暗号鍵ファイルのみを記録し、秘匿情報の記録再生が可能なドライブのみムーブ対応可能とする著作権管理方式が記載されている。

【００１０】

このようなシステムによって、最初の記録媒体はＣＰＲＭ対応ドライブであれば再生動作は可能であり、またムーブできないで良ければ、最初のダウンロードもＣＰＲＭ対応による暗号化コンテンツと暗号化暗号鍵の記録のみでも良い為、新規の秘匿情報記録再生機能が無いドライブも、機能限定であるが記録再生を可能とする。この方式の良い点は、ムーブ処理によってコンテンツが他の記録媒体に移動しても、最初のダウンロードした記録媒体は常に再生可能であり、再エンコードムーブによって圧縮比が大幅に変更された結果による品位変更が伴っても、最初の記録媒体には元のコンテンツが記録されている為、安心して再エンコードムーブができる。

【００１１】

しかしながら、デジタルＴＶ放送などはコピーワンスが基本であり、上記方法ではコンテンツが２箇所に存在することから、認められない可能性があり、その様な場合を対応できる技術の考案が期待されていた。

【特許文献１】特開２００３－１３２６２５号公報

【特許文献２】特開２００３－１０９３０２号公報

【特許文献３】特開２００３－１２２６３７号公報
【特許文献４】特開２００４－１８６８２５号公報
【発明の開示】
【発明が解決しようとする課題】
【００１２】
従来、コンテンツを暗号化してその暗号化に使われた暗号鍵も暗号化して、同一の記録媒体に記録しておく、著作権保護システムが利用されている。この場合、違法行為を防止する為、暗号化管理システムに一部の暗号鍵のリボーク機能や、メディアバインド機能を構築し、保護性能を向上させている。このようなシステムでも、記録媒体間でコンテンツ移動を行う場合、コンテンツ移動後に元の記録媒体からは暗号鍵のみを消去することで、コンテンツの消去と同じ行為と見なす方法を取り入れている。
【００１３】
しかし、光ディスクのようなリムーバルでオープンな記録媒体では、事前に暗号鍵が記録されている領域のデータを読み出しておき、正規のコンテンツ移動処理後に、元の記録媒体から消去された暗号鍵を復活させる違法行為をする可能性がある。
【００１４】
現在のＤＶＤレコーダで利用されている著作権保護方式（ＣＰＲＭ）では、最初にＨＤＤ（ハードディスク）に記録しておき、そこからＤＶＤにムーブすることは可能である。しかしながら一旦ＤＶＤに記録されたコンテンツは、他のＤＶＤにムーブしたり再度ＨＤＤにムーブする処理は許可されていない。その理由は、上記のような正規のムーブ処理によって新しくコンテンツが記録された記録媒体を完成した後、ムーブ処理によって暗号鍵が消去された記録媒体を、事前にバックアップしておいた暗号化暗号鍵データで復活させることが可能と思われるからである。このような方法では、如何に高度な暗号器を用いた暗号処理を導入しても、暗号化された一部のデータをそのままコピーすることで、実質の違法コピーが構成されてしまう。
【００１５】
そこで本発明は、ＤＶＤとＤＶＤなどのリムーバブル媒体間、ＤＶＤからＨＤＤなどリムーバブル媒体から固定媒体間のムーブを可能にしたコンテンツ管理方法及び記録再生装置を提供することを目的とする。
【課題を解決するための手段】
【００１６】
上記目的を達成するために、本発明は、第１の鍵で暗号化されたコンテンツデータと、第２の鍵と第４の鍵で暗号化され、さらに第３の鍵で暗号化された第１の鍵と、前記第４の鍵で暗号化された第２の鍵及び第３の鍵とが記録された記録媒体から他の記録媒体に前記コンテンツデータを移動させるに際し、
前記記録媒体に記録されている前記暗号化された第２の鍵及び第３の鍵を読み出し、前記第４の鍵を用いて前記第２の鍵及び第３の鍵を復号化し、
前記記録媒体に記録されている暗号化された前記第１の鍵を読み出し、前記第４の鍵、前記複合化された第２の鍵及び第３の鍵を用いて第１の鍵を復号化し、
前記記録媒体に記録されている暗号化された前記コンテンツデータを読み出し、前記復号化された第１の鍵を用いて前記コンテンツを復号化し、
前記複合化されたコンテンツと共に前記第２の鍵を前記他の記録媒体に伝送し、
前記第３の鍵を更新し、
前記第１の鍵を前記第２の鍵と前記第４の鍵を用いて暗号化し、さらに前記更新した第３の鍵を用いて暗号化し、
前記暗号化された第１の鍵を、前記記録媒体に記録されている暗号化された第１の鍵と書き換え、
前記記録媒体に記録されている暗号化された第２の鍵を消去することを特徴とするコンテンツ管理方法を提供する。
【００１７】

このとき、前記他の記録媒体から前記記録媒体に前記コンテンツを再び移動させる場合、前記第２の鍵を前記第４の鍵で暗号化し、前記記録媒体に記録してもよい。

【００１８】

また、前記第４の鍵は、前記記録媒体に固有のメディア固有鍵であってもよい。

【００１９】

また、前記第３の鍵は、記録再生ドライブ内でのみ、復号再生及び鍵データ更新、並びに記録処理を許可する、秘匿データであってもよい。

【００２０】

また、前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵及び第２の鍵は、暗号化されたデータファイルとして記録媒体に記録される場合、複数の第２の鍵を演算処理して証明データを作成し、暗号化された第１の鍵のデータファイルに組み込んで、第３の鍵で暗号化し、多重暗号化された第１の鍵と暗号化された第２の鍵の証明データで構成された暗号化データファイルとして、前記記録媒体に記録されてもよい。

【００２１】

また、前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵は前記第４の鍵と前記第２の鍵によって合成された暗号鍵で暗号化され、暗号化された第１の鍵のデータファイルとし、前記複数の第２の鍵は、前記第４の鍵で暗号化され、暗号化された第２の鍵のデータファイルとし、暗号化された第１の鍵のデータファイルと、暗号化された第２の鍵のデータファイルは、共に更新された第３の鍵で暗号化され、記録媒体に記録されてもよい。

【００２２】

また、前記暗号化された第１の鍵のデータファイルにおける各鍵の付帯情報として、コンテンツデータの識別番号と暗号化された第２の鍵が前記記録媒体に記録されているか、消去されているかを示すフラグが設けられており、

前記暗号化された第２の鍵のデータファイルにおいて、消去された第２の鍵も含めて、各鍵の付帯情報として、コンテンツデータの識別番号と、暗号化された第１の鍵が前記記録媒体に記録されているかを示す識別フラグが設けられてもよい。

【００２３】

また、本発明は、第１の鍵で暗号化されたコンテンツデータと、第２の鍵と第４の鍵で暗号化され、さらに第３の鍵で暗号化された第１の鍵と、前記第４の鍵で暗号化された第２の鍵及び第３の鍵とが記録された記録媒体から他の記録媒体に前記コンテンツデータを移動させる記録再生装置であって、

前記記録媒体に記録されている前記暗号化された第２の鍵及び第３の鍵を読み出し、前記第４の鍵を用いて前記第２の鍵及び第３の鍵を復号化する復号手段と、

前記記録媒体に記録されている暗号化された前記第１の鍵を読み出し、前記第４の鍵、前記複合化された第２の鍵及び第３の鍵を用いて第１の鍵を復号化する復号手段と、

前記記録媒体に記録されている暗号化された前記コンテンツデータを読み出し、前記復号化された第１の鍵を用いて前記コンテンツを復号化する復号化手段と、

前記複合化されたコンテンツと共に前記第２の鍵を前記他の記録媒体に伝送する伝送手段と、

前記第３の鍵を更新する更新手段と、

前記第１の鍵を前記第２の鍵と前記第４の鍵を用いて暗号化し、さらに前記更新した第３の鍵を用いて暗号化する暗号化手段と、

前記暗号化された第１の鍵を、前記記録媒体に記録されている暗号化された第１の鍵と書き換える書き換え手段と、

前記記録媒体に記録されている暗号化された第２の鍵を消去する消去手段とを具備することを特徴とする記録再生装置を提供する。

【００２４】
このとき、前記他の記録媒体から前記記録媒体に前記コンテンツを再び移動させる場合、前記第２の鍵を前記第４の鍵で暗号化し、前記記録媒体に記録してもよい。
【００２５】
また、前記第４の鍵は、前記記録媒体に固有のメディア固有鍵であってもよい。
【００２６】
また、前記第３の鍵は、記録再生ドライブ内でのみ、復号再生及び鍵データ更新、並びに記録処理を許可する、秘匿データであってもよい。
【００２７】
また、前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵及び第２の鍵は、暗号化されたデータファイルとして記録媒体に記録される場合、複数の第２の鍵を演算処理して証明データを作成し、暗号化された第１の鍵のデータファイルに組み込んで、第３の鍵で暗号化し、多重暗号化された第１の鍵と暗号化された第２の鍵の証明データで構成された暗号化データファイルとして、前記記録媒体に記録されてもよい。
【００２８】
また、前記コンテンツデータは、複数のコンテンツデータが存在し、前記第１の鍵及び第２の鍵は、それぞれ複数のコンテンツデータごとに複数生成され、前記複数の第１の鍵は前記第４の鍵と前記第２の鍵によって合成された暗号鍵で暗号化され、暗号化された第１の鍵のデータファイルとし、前記複数の第２の鍵は、前記第４の鍵で暗号化され、暗号化された第２の鍵のデータファイルとし、暗号化された第１の鍵のデータファイルと、暗号化された第２の鍵のデータファイルは、共に更新された第３の鍵で暗号化され、記録媒体に記録されてもよい。
【００２９】
また、前記暗号化された第１の鍵のデータファイルにおける各鍵の付帯情報として、コンテンツデータの識別番号と暗号化された第２の鍵が前記記録媒体に記録されているか、消去されているかを示すフラグが設けられており、
前記暗号化された第２の鍵のデータファイルにおいて、消去された第２の鍵も含めて、各鍵の付帯情報として、コンテンツデータの識別番号と、暗号化された第１の鍵が前記記録媒体に記録されているかを示す識別フラグが設けられてもよい。
【００３０】
また、本発明は、複数の第１の鍵で暗号化された複数のコンテンツデータと、
記録媒体固有の鍵と複数の第２の鍵で暗号化された複数の第１の鍵のデータファイルを第３の鍵で多重暗号化した第１の鍵のデータファイルと、
記録媒体固有の鍵で暗号化された複数の第２の鍵で構成された第２の鍵のデータファイルと、
記録媒体固有の鍵で暗号化された第３の鍵とが記録されたことを特徴とする記録媒体を提供する。
【００３１】
また、複数の第１の鍵で暗号化された複数のコンテンツデータと、
記録媒体固有の鍵と複数の第２の鍵で暗号化された複数の第１の鍵のデータファイルを第３の鍵で多重暗号化した第１の鍵のデータファイルと、
記録媒体固有の鍵で暗号化された複数の第２の鍵が第３の鍵で多重暗号化された第２の鍵で構成された第２の鍵のデータファイルと、
記録媒体固有の鍵で暗号化された第３の鍵とが記録されたことを特徴とする記録媒体を提供する。
【発明の効果】
【００３２】
暗号化暗号鍵を事前にバックアップしておいても元の媒体では復号化できないようにす

ることで、リムーバブル媒体間、リムーバブル媒体から固定媒体へのムーブ処理を安全に行うことができる。特に、従来のコンテンツムーブ技術では不可能であった、再エンコード（高圧縮処理等で、コンテンツデータ量を削減し、低記録容量の媒体に格納出来るようにした場合等）して、他の記録媒体にコンテンツムーブした場合、再度ムーブ処理で元の記録媒体に戻す事により、高品位データコンテンツに復活させる事
が可能になる。

【発明を実施するための最良の形態】

【００３３】

以下、本発明を実施するための最良の形態について図面を用いて詳細に説明する。なお、本発明は、以下の実施形態に限定されるものではなく、種々選択して用いることができる。

【００３４】

先ず、図１に、本発明の著作権保護方式であるＣＰＲＭの基本構成を示した処理システム図を示す。

【００３５】

図１に示すように、記録媒体であるＤＶＤ－ＲＡＭやＤＶＤ－ＲＷディスクは、事前に複数のデバイス鍵によって暗号化された暗号化暗号鍵ブロック（ＭＫＢ：Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ）とディスク固有ＩＤ（ＭＩＤ：Ｍｅｄｉａ　ＩＤ）が記録されている。

【００３６】

（デジタル記録媒体にコンテンツを記録する）

先ず、ＤｒｉｖｅとＡ／Ｖ－Ｂｏａｒｄ間で認証処理（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を行った後、Ｄｒｉｖｅはディスクに記録されているＭＫＢとＭＩＤを読み出し、Ａ／Ｖ－Ｂｏａｒｄに送る。

【００３７】

次に、Ａ／Ｖ－Ｂｏａｒｄでは、ＭＫＢ－ｐｒｏ処理部に入力されたＭＫＢとＤｅｖｉｃｅ－Ｋｅｙとを用いてメディア鍵（Ｋｍ）を抽出する。

【００３８】

次に、抽出されたメディア鍵（Ｋｍ）とディスクから読み出されたＭＩＤは、ハッシュ函数器のような信号処理部［Ｇ］に入力され、メディア固有鍵（Ｋｍｕ）が生成される。

【００３９】

次に、タイトル鍵（Ｋｔ：Ｔ－Ｋｅｙ）は、暗号化部（Ｅ）に入力され、メディア固有鍵（Ｋｍｕ）にて暗号化されて暗号化タイトル鍵（Ｅ－Ｋｔ）としてディスクに記録される。一方タイトル鍵Ｋｔは暗号化部（Ｅｎｃ）に入力され、コンテンツ（Ｎｅｗ－ｃｏｎｔｅｎｔｓ）を暗号化する。暗号化されたコンテンツ（Ｅｎｃ－Ｃｏｎｔｅｎｔｓ）は記録媒体に記録される。

【００４０】

（デジタル記録媒体からコンテンツを再生する）

先ず、ＤｒｉｖｅとＡ／Ｖ－Ｂｏａｒｄ間で認証処理（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を行った後、Ｄｒｉｖｅはディスクに記録されているＭＫＢとＭＩＤを読み出し、Ａ／Ｖ－Ｂｏａｒｄに送る。

【００４１】

次に、Ａ／Ｖ－Ｂｏａｒｄでは、ＭＫＢ－ｐｒｏ処理部に入力されたＭＫＢと機器が所有するデバイス鍵（Ｄｅｖｉｃｅ－Ｋｅｙ）によってメディア鍵（Ｋｍ）を抽出する。

【００４２】

次に、抽出されたメディア鍵（Ｋｍ）とディスクから読み出されたＭＩＤは、ハッシュ函数器のような信号処理部［Ｇ］に入力され、メディア固有鍵（Ｋｍｕ）が生成される。

【００４３】

次に、ディスクから読み出された暗号化タイトル鍵（Ｅ－Ｋｔ）が復号化部（Ｄ）に入力され、メディア固有鍵（Ｋｍｕ）を用いてタイトル鍵（Ｋｔ）が復号される。

【００４４】
次に、ディスクから暗号化コンテンツ（Ｅｎｃ-Ｃｏｎｔｅｎｔｓ）が復号化部（Ｄｅｃ）に入力され、タイトル鍵（Ｋｔ）で復号されて平文のコンテンツ（Ｃｏｎｔｅｎｔｓ）が再生される。
【００４５】
図２は、記録媒体Ａから記録媒体Ｂにコンテンツを移動するムーブ処理について説明するための図である。記録媒体Ａに記録された暗号化コンテンツは、復号されて記録媒体Ｂ側の記録ドライブに送られる。記録媒体Ｂの記録ドライブは送られてきたコンテンツを再度暗号化して媒体Ｂに記録し、この時のコンテンツを暗号化するためのタイトル鍵を、媒体Ｂのメディア固有鍵で暗号化して記録媒体Ｂに記録する。
【００４６】
記録媒体Ｂ側ドライブにコンテンツが全て送信されたら、記録媒体Ａのドライブは再生動作を止め、記録モードにして記録媒体Ａのコンテンツを暗号化するためのタイトル鍵を消去する。この場合、コンテンツファイルが複数有り、記録媒体Ｂには特定のコンテンツファイルが送られた場合は、送られたコンテンツのコンテンツ暗号化タイトル鍵のみ消去する。このような動作によってムーブ処理が完了する。
【００４７】
図１及び図２で説明したＣＰＲＭ基本構成のみでは、コンテンツが記録媒体Ａから記録媒体Ｂにムーブする前に記録媒体Ａに記録されている暗号化タイトル鍵ファイルを読み出してバックアップしておき、コンテンツのムーブ処理が終了した後に、消去されているはずの暗号化タイトル鍵を、記録媒体Ａにそのまま戻すことで暗号化コンテンツを再生可能に復活させることが可能となる。このような行為はコピーワンスの著作権管理を前提としたコンテンツでは契約に違反した処理となる。
【００４８】
図３に、秘匿情報再生技術を用いてムーブ処理を可能とする著作権保護方式を説明するための図を示す。秘匿情報記録し阿世技術を用いることで暗号化タイトル鍵ファイルを読み出してバックアップしておき記録媒体に戻す行為を防止することができる。図１と同一箇所は同一符号を付している。
【００４９】
（デジタル記録媒体にコンテンツを記録する）
先ず、ＤｒｉｖｅとＡ／Ｖ－Ｂｏａｒｄ間で認証処理を行った後、Ｄｒｉｖｅはディスクに記録されているＭＫＢとＭＩＤを読み出し、Ａ／Ｖ－Ｂｏａｒｄに送る。
【００５０】
次に、Ａ／Ｖ－Ｂｏａｒｄでは、ＭＫＢ－ｐｒｏ処理部に入力されたＭＫＢとＤｅｖｉｃｅ－Ｋｅｙとを用いてメディア鍵（Ｋｍ）を抽出する。
【００５１】
次に、抽出されたメディア鍵（Ｋｍ）とディスクから読み出されたＭＩＤは、ハッシュ函数器のような信号処理部［Ｇ］に入力され、メディア固有鍵（Ｋｍｕ）が生成される。
【００５２】
次に、タイトル鍵（Ｋｔ１’：Ｔ－Ｋｅｙ）は、暗号化部（Ｅ）に入力されメディア固有鍵（Ｋｍｕ）にて暗号化タイトル鍵（Ｅ－Ｋｔ１’）が生成される。
【００５３】
次に、暗号化タイトル鍵（Ｅ－Ｋｔ１’）はドライブ内に送られて秘匿情報信号（ＵＤ：ＵＰ－Ｄａｔｅ）で多重暗号化され多重暗号化コンテンツ暗号鍵（ＥＥ－Ｋｔ１）として記録媒体に記録される。
【００５４】
一方、タイトル鍵（Ｋｔ１’：Ｔ－Ｋｅｙ）は暗号化部（Ｅｃｎ）に入力されコンテンツ（Ｎｅｗ－ｃｏｎｔｅｎｔｓ）を暗号化する。暗号化されたコンテンツ（Ｅｎｃ－Ｃｏｎｔｅｎｔｓ）は記録媒体に記録される。
【００５５】

図３の中心にあるディスクの左側ブロックは、複数の暗号化コンテンツが記録されている記録媒体に、新規の暗号化コンテンツを追加記録するシステムの構成が示されている。

【００５６】

追加して記録する暗号化コンテンツと共に、多重暗号化タイトル鍵（ＥＥ－Ｋｔ）も複数となる。そこで記録媒体に記録されている多重暗号化タイトル鍵（ＥＥ－Ｋｔ０）及び暗号化秘匿情報（Ｅ－ＵＤ０）を事前に読出す。暗号化秘匿情報（Ｅ－ＵＤ０）は復号化部（Ｄ）にて秘匿情報（ＵＤ０）に復号され、この秘匿情報（ＵＤ０）を用いて、多重暗号化タイトル鍵（ＥＥ-Ｋｔ０）を暗号化タイトル鍵（Ｅ－Ｋｔ０）に復号する。この暗号化タイトル鍵（Ｅ－Ｋｔ０）は、コンテンツ暗号ボード側に送られ、編集部（ＥＤＴ）で上記の暗号化タイトル（Ｅ－Ｋｔ１’）を加えてドライブに送る。ドライブ側では、秘匿情報（ＵＤ０）がアップデート部（＊α）にて秘匿情報（ＵＤ１）にアップデートされる。ドライブ側から送られた編集処理された暗号化タイトル鍵は、アップデートされた秘匿情報（ＵＤ１）を用いて暗号化部（Ｅ）にて暗号化され、多重暗号化タイトル鍵（ＥＥ－Ｋｔ１）として記録媒体に記録される。

【００５７】

アップデートされた秘匿情報（ＵＤ１）は、暗号化部（Ｅ）にて暗号化され、暗号化秘匿情報（Ｅ－ＵＤ１）として記録媒体に記録される。

【００５８】

このような処理は、多重暗号化タイトル鍵の書換え動作をする度に更新させ、多重暗号化タイトル鍵は更新される。

【００５９】

図３の右側ブロックは、暗号化コンテンツを再生する時の暗号化コンテンツ復号の構成が示されている。

【００６０】

（デジタル記録媒体からコンテンツを再生する）

先ず、ＤｒｉｖｅとＡ／Ｖ－Ｂｏａｒｄ間で認証処理を行った後、Ｄｒｉｖｅはディスクに記録されているＭＫＢとＭＩＤを読み出し、Ａ／Ｖ－Ｂｏａｒｄに送る。

【００６１】

次に、Ａ／Ｖ－Ｂｏａｒｄでは、ＭＫＢ－ｐｒｏ処理部に入力されたＭＫＢと機器に所持されているＤｅｖｉｃｅ－Ｋｅｙとを用いてメディア鍵（Ｋｍ）を抽出する。

【００６２】

次に、抽出されたメディア鍵（Ｋｍ）とディスクから読み出されたＭＩＤは、ハッシュ函数器のような信号処理部［Ｇ］に入力され、メディア固有鍵（Ｋｍｕ）が生成される。

【００６３】

次に、記録媒体から暗号化秘匿情報（Ｅ－ＵＤ１）が読み出され復号化部（Ｄ）にて秘匿情報（ＵＤ１）に復号される。一方記録媒体から多重暗号化タイトル鍵（ＥＥ－Ｋｔ１）が読み出され、復号化部（Ｄ）に入力され上記秘匿情報（ＵＤ１）を用いて暗号化タイトル鍵（Ｅ－Ｋｔ１）が復号される。

【００６４】

次に、この暗号化タイトル鍵（Ｅ－Ｋｔ１）は、復号化部（Ｄ）に入力され、（ＭＫＢ）と（ＭＩＤ）で生成されたメディア固有鍵（Ｋｍｕ）で復号される。このとき復号されたタイトル鍵は複数有りこのなかから指定のタイトル鍵（Ｋｔ１’）が選択される。

【００６５】

次に、記録媒体から読み出された暗号化コンテンツ（Ｅｎｃ－Ｃｏｎｔｅｎｔｓ）は、タイトル鍵（Ｋｔ１’）で復号されて、平文のコンテンツ（Ｃｏｎｔｅｎｔｓ）が出力される。

【００６６】

この処理と併せて、暗号化タイトル鍵（Ｅ－Ｋｔ１）は編集部（ＥＤＴ）で指定された暗号化タイトル鍵（Ｅ－Ｋｔ１’）が削除されて暗号化タイトル鍵（Ｅ－Ｋｔ２）が生成される。一方復号化部（Ｄ）で復号された秘匿情報（ＵＤ１）は、アップデート部（＊α

）にてアップデートされ秘匿情報（ＵＤ２）が生成される。
【００６７】
編集部（ＥＤＴ）にて編集された暗号化タイトル鍵（Ｅ－Ｋｔ２）は、暗号化部（Ｅ）にてアップデートされた秘匿情報（ＵＤ２）によって暗号化され、多重暗号化タイトル鍵（ＥＥ－Ｋｔ２）として記録媒体に記録される。
【００６８】
アップデートされた秘匿情報（ＵＤ２）は、暗号化部（Ｅ）にて暗号化され、暗号化秘匿情報（Ｅ－ＵＤ２）として記録媒体に記録される。
【００６９】
この処理によって記録媒体にはタイトル鍵（Ｋｔ１’）が削除された状態となるので、暗号化された暗号化コンテンツは復号化できなくなり削除されたことになる。
【００７０】
図３の方式を使えば、タイトル鍵は追加記録やムーブ処理によって常に暗号化が更新変更される為、事前に暗号化タイトル鍵をバックアップしておき、ムーブ後にタイトル鍵が削除されたメディアを、バックアップしてタイトル鍵復活をさせても、秘匿情報雅（ＵＤ）が更新されタイトル鍵を復号できなくなる為、このような暗号鍵復活による違反行為も防止できる。
【００７１】
しかしながら、図３のムーブ機能可能な著作権保護システムでは、ムーブ時コンテンツを圧縮比変更して記録容量が小さな記録媒体にムーブ記録する場合、再び元の高品位なコンテンツデータに復元する事は不可能である。
【００７２】
図４は、図３の著作権保護システムを使って、コンテンツを再エンコード処理した後ムーブ記録した場合の構成を示した図である。
【００７３】
図４は、図３の右側が記載されたＤｉｓｃ－Ａを読み出すドライブ（図４中左側）と、図３の左側が記載されたＤｉｓｃ－Ｂに再エンコードした後に暗号化コンテンツを記録するドライブ（図４中右側）の構成を示したものである。
【００７４】
図３の読み出しで説明した処理によって、Ｄｉｓｃ－Ａから読み出されたコンテンツは、Ｉ／Ｏを介してＤｉｓｃ－Ｂの記録ドライブ（右側）に送られ、先ずコードコンバータ（Ｃｏｄｅ　ｃｏｎｖｅｒｔｏｒ）に入力される。
【００７５】
次に、図３の書き込みで説明した処理によって、コードコンバータからの平文のコンテンツは、再エンコードされてＤｉｓｃ－Ｂに記録される。
【００７６】
図５は、図４で示したコンテンツムーブ処理を説明する図である。ここでは、暗号化コンテンツが１ファイルの場合を例にして、図示したものである。高レート圧縮コンテンツが暗号化されて記録されている記録媒体Ａから、記録媒体Ｂに低レート圧縮コンテンツに再エンコードした後暗号化して記録することで、コンテンツムーブした状態が示されている。
【００７７】
図５に示すように、記録媒体Ａの暗号化されたタイトル鍵は消去され、暗号化コンテンツはファイル管理上消去されたことになる。このように復号する為のタイトル鍵が削除されている為、暗号化されたコンテンツは復活させることはできず、著作権保護を守りつつ、コンテンツを記録媒体間で移動させ、利用形態に適した状態で利用することが可能となる。
【００７８】
一方でムーブ処理は重要な機能であるが、機能を最大限に活用できる再エンコードを取り入れると、元の高品位コンテンツ利用が不可能になる。このように、丸ごとコピー防止

や正規のムーブ処理後にコンテンツタイトル鍵が消去された記録媒体を、違法処理でタイトル鍵を復活させる方法で、消去されたことになっている暗号化コンテンツを復活させる違法コピーは、新しい著作権保護システムを使えば、ムーブ機能は実願できるが、コンテンツの再エンコードのような処理がムーブ処理で利用されると、コンテンツ品位の劣化を元に戻す工程がなくなってしまう。

【００７９】

このような状況を鑑みて、「コンテンツムーブ」と言う機能を、「コンテンツ再生権利ムーブ」という機能に変更した例を説明する。

【００８０】

図６は、本発明の暗号化管理システムの例である。図４と比較すると、新たに「ムーブ鍵：Ｋｍｖ」が追加されている。このムーブ鍵（ＫｍＶ）は、コンテンツを暗号或いは復号するタイトル鍵を暗号或いは復号するために用いるもので、ムーブを行う際タイトル鍵は消去せず、ムーブ鍵を消去することでコンテンツの再生（復号）をできなくするものである。また、このムーブ鍵（Ｋｍｖ）はコンテンツとペアになって記録媒体間を移動し、移動した先の記録媒体では、新たに移動先記録媒体のメディア固有鍵で新規に暗号化され記録される。さらに移動元の記録媒体にコンテンツを戻そうとした場合、移動元の記録媒体には復号ができない状態の暗号化コンテンツが事前に記録されているのでムーブ鍵を移動させるだけで、その暗号化コンテンツを復号可能にできる。その処理動作は次のようなものである。

【００８１】

図６に示すように、先ず、ＤｒｉｖｅとＡ／Ｖ－Ｂｏａｒｄ間で認証処理を行った後、Ｄｒｉｖｅはディスクに記録されているＭＫＢとＭＩＤを読み出し、Ａ／Ｖ－Ｂｏａｒｄに送る。

【００８２】

次に、Ａ／Ｖ－Ｂｏａｒｄでは、ＭＫＢ－ｐｒｏ処理部に入力されたＭＫＢと機器に所持されているＤｅｖｉｃｅ－Ｋｅｙ（Ｄ－Ｋ）とを用いてメディア鍵（Ｋｍ）を抽出する。

【００８３】

次に、抽出されたメディア鍵（Ｋｍ）とディスクから読み出されたＭＩＤは、ハッシュ函数器のような信号処理部［Ｇ］に入力され、メディア固有鍵（Ｋｍｕ）が生成される。

【００８４】

次に、記録媒体に記録されている暗号化されたムーブ鍵（Ｅ－Ｋｍｖ０）が読み出され、復号化部（Ｄ）にて、前記メディア固有鍵（Ｋｍｕ）を用いて復号化されムーブ鍵ファイル（Ｋｍｖ０）が生成される。

【００８５】

次に、このムーブ鍵ファイル（Ｋｍｖ０）の中から移動させようとするコンテンツに対応するムーブ鍵（Ｋｍｖａ）が抽出され、これと信号処理部［Ｇ］で生成されたメディア固有鍵（Ｋｍｕ）とが信号処理部［Ｇ］に入力されメディア固有ムーブ鍵（Ｋｍｕｍ）が生成される。

【００８６】

次に、記録媒体から暗号化秘匿情報（Ｅ－ＵＤ０）が読み出され暗号化部にて秘匿情報（ＵＤ０）に復号される。一方記録媒体から多重暗号化タイトル鍵ファイル（ＥＥ－Ｋｔ０）が読み出され、復号化部（Ｄ）に入力され上記秘匿情報（ＵＤ０）を用いて暗号化タイトル鍵ファイル（Ｅ－Ｋｔ０）が復号される。

【００８７】

この暗号化タイトル鍵ファイル（Ｅ－Ｋｔ０）は、復号化部（Ｄ）に入力され、前記メディア固有ムーブ鍵（Ｋｍｕｍ）を用いて復号化され、移動させようとするコンテンツに対応するタイトル鍵（Ｋｔａ）が生成される。

【００８８】

次に、記録媒体から読み出された暗号化コンテンツ（Ｅｎｃ－Ｃｏｎｔｅｎｔｓ）は、

復号化部（Ｄｅｃ）に入力され、前記タイトル鍵（Ｋｔａ）を用いて復号される。こうして、平文のコンテンツ（Ｃｏｎｔｅｎｔｓ）が出力される。このときコンテンツに対応するムーブ鍵（Ｋｍｖａ）は、平文のコンテンツと共に、インターフェース（Ｉ／Ｏ）を介してＤｉｓｃ－Ｂ側のドライブに送られ、新たに暗号化処理されてＤｉｓｃ－Ｂに記録される。

【００８９】

尚、本発明の範疇ではないが、Ｉ／Ｏを通して出力されるコンテンツデータやムーブ鍵データは、他のデジタルインターフェース規格に準拠して暗号化－復号化が行われ、機器間でのデータ送信における、盗み撮り防止が行われるのは当然である。

【００９０】

コンテンツとムーブ鍵（Ｋｍｖａ）が出力されると、Ｄｉｓｃ－Ａ側では先ずムーブ鍵ファイル（Ｋｍｖ０）は編集部（ＥＤＴ）に入力され、ファイルの中から移動したコンテンツに対応するムーブ鍵（Ｋｍｖａ）を削除し、新たにムーブ鍵ファイル（Ｋｍｖ１）を生成する。次に、このムーブ鍵ファイル（Ｋｍｖ１）は、暗号化部（Ｅ）に入力され、メディア固有鍵（Ｋｍｕ）を用いて暗号化され暗号化ムーブ鍵（Ｅ－Ｋｍｖ１）として記録媒体に記録される。

【００９１】

併せて、ムーブ鍵ファイル（Ｋｍｖ１）はムーブ鍵ベリファイデータ処理部（Ｖ－Ｍｏ）に入力され、ムーブ鍵ベリファイデータ（Ｖ－Ｍｏ１）を生成する。このムーブ鍵ベリファイデータ（Ｖ－Ｍｏ１）と暗号化タイトル鍵（Ｅ－Ｋｔ０）データと合せて編集部（ＥＤＴ）に入力し、暗号化タイトル鍵（Ｅ－Ｋｔ１）が生成される。ただしここでは移動したコンテンツに対応するタイトル鍵（Ｋｔａ）の削除は行わない。

【００９２】

一方復号化部（Ｄ）で復号された秘匿情報（ＵＤ０）は、アップデート部（ＵＰ　Ｄａｔａ）にてアップデートされ秘匿情報（ＵＤ１）が生成される。

【００９３】

編集部（ＥＤＴ）にて編集された暗号化タイトル鍵（Ｅ－Ｋｔ１）は、暗号化部（Ｅ）に入力され、アップデートされた秘匿情報（ＵＤ１）によって暗号化され、多重暗号化タイトル鍵（ＥＥ－Ｋｔ１）として記録媒体に記録される。

【００９４】

アップデートされた秘匿情報（ＵＤ１）は暗号化され、暗号化秘匿情報（Ｅ－ＵＤ１）として記録媒体に記録される。

【００９５】

このように暗号化コンテンツを復号する為のタイトル鍵は、ムーブ処理では削除せず、そのまま元の記録媒体に暗号化されて残る。一方この暗号化タイトル鍵を復号するために必要なムーブ鍵（Ｋｖａ）は元の記録媒体から削除される。したがって暗号化コンテンツを復号するタイトル鍵は、Ｄｉｓｃ－Ａ内の復号可能な鍵を集合させても、ムーブ鍵がない為、タイトル鍵の復号が不可能である。

【００９６】

このようにすることで移動先の記録媒体から元の記録媒体にコンテンツを移動して戻そうとした場合、ムーブ鍵のみを戻すことで、もともと暗号化されて残されているコンテンツを復号化可能状態に戻すことができる。このような処理は、例えば最初の移動においてコンテンツをより情報量の少ないダウンコンバートして移動した場合に、元の記録媒体に戻すことで情報量を元に戻すことを可能とする。すなわちダウンコンバートによって一旦は画質の劣化した映像などをもとに戻すことを可能としている。

【００９７】

次に、Ｄｉｓｃ－Ｂにコンテンツを記録する操作について説明する。

【００９８】

Ｄｉｓｃ－Ｂ側のドライブでは、インターフェース（Ｉ／Ｏ）を介して送られてきた平分のコンテンツデータとムーブ鍵（Ｋｍｖａ）を暗号化する。

【００９９】
先ず、再エンコードされたコンテンツを暗号化部（Ｅｎｃ）に入力し、新たに乱数発生器等で生成したタイトル鍵（Ｋｔｘ）を用いて暗号化し、暗号化コンテンツ（Ｅｎｃ－Ｃｏｎｔｅｎｔｓ）として記録媒体に記録する。
【０１００】
次に、Ｄｉｓｃ－ＢからＭＫＢを読み出し、ＭＫＢ　Ｐｒｏに入力して、機器に固有に設けられているディスク鍵（Ｄ－Ｋ）を用いてデバイス鍵（Ｋｍ’）を抽出する。次に、Ｄｉｓｃ－ＢからＭＩＤを読み出し、前記デバイス鍵（Ｋｍ’）とともに、ハッシュ函数器のような信号処理部［Ｇ］に入力しメディア固有鍵（Ｋｍｕ’）を生成する。
【０１０１】
Ｄｉｓｃ－Ａ側からインターフェース（Ｉ／Ｏ）を介して送られてきたムーブ鍵（Ｋｍｖａ）は、前記メディア固有鍵（Ｋｍｕ’）とともに、ハッシュ函数器のような信号処理部［Ｇ］に入力しメディア固有ムーブ鍵（Ｋｍｕｍ’）を生成する。
【０１０２】
次に、前記乱数発生器等で生成したタイトル鍵（Ｋｔｘ）は、暗号化部（Ａ）に入力され、前記メディア固有ムーブ鍵（Ｋｍｕｍ’）を用いて暗号化され暗号化タイトル鍵（Ｅ－Ｋｔｘ）を生成する。
【０１０３】
次に、Ｄｉｓｃ－Ｂに記録されている他のムーブ鍵ファイル（Ｅ－Ｋｍｖｎ）が読み出され、復号化部（Ｄ）に入力されＤｉｓｃ－Ｂの固有鍵（Ｋｍｕ’）を用いて復号化されてムーブ鍵ファイル（Ｋｍｖｎ）が生成される。このムーブ鍵ファイル（Ｋｍｖｎ）と前記ムーブ鍵（Ｋｍｖａ）とが編集部（ＥＤＴ）に入力され、新たにムーブ鍵（Ｋｍｖａ）が加えられたムーブ鍵ファイル（Ｋｍｖｍ）が生成される。
【０１０４】
このムーブ鍵ファイル（Ｋｍｖｍ）は暗号化部（Ｅ）に入力され、メディア固有鍵（Ｋｍｕ’）を用いて暗号化されて暗号化ムーブ鍵ファイル（Ｅ－Ｋｍｖｍ）が生成され記録媒体に記録される。
【０１０５】
次に、記録媒体から暗号化秘匿情報（Ｅ－ＵＤｎ）が読み出され暗号化部にて秘匿情報（ＵＤｎ）に復号される。一方記録媒体から多重暗号化タイトル鍵ファイル（ＥＥ－Ｋｔｎ）が読み出され、復号化部（Ｄ）に入力され上記秘匿情報（ＵＤｎ）を用いて暗号化タイトル鍵ファイル（Ｅ－Ｋｔｎ）が復号される。
【０１０６】
次に、前記ムーブ鍵ファイル（Ｋｍｖｍ）は、ムーブ鍵ベリファイデータ処理部（Ｖ－Ｍｏ）に入力され、ムーブ鍵ベリファイデータ（Ｖ－Ｍｏｎ）を生成する。このムーブ鍵ベリファイデータ（Ｖ－Ｍｏｎ）と前記暗号化タイトル鍵（Ｅ－Ｋｔｘ）データと合せて編集部（ＥＤＴ）に入力し、暗号化タイトル鍵（Ｅ－Ｋｔｍ）が生成される。ここでは暗号化タイトル鍵（Ｋｔｘ）と、ムーブ鍵ファイル（Ｋｍｖｍ）のベリファイデータ（Ｖ－Ｍｏ）を集合して暗号化タイトル鍵（Ｅ－Ｋｔｍ）を生成されている。
【０１０７】
一方復号化部（Ｄ）で復号された秘匿情報（ＵＤｎ）は、アップデート部（ＵＰ　Ｄａｔａ）にてアップデートされ秘匿情報（ＵＤｍ）が生成される。
【０１０８】
編集部（ＥＤＴ）にて編集された暗号化タイトル鍵（Ｅ－Ｋｔｍ）は、暗号化部（Ｅ）に入力され、アップデートされた秘匿情報（ＵＤｎ）によって暗号化され、多重暗号化タイトル鍵（ＥＥ－Ｋｔｍ）として記録媒体に記録される。
【０１０９】
アップデートされた秘匿情報（ＵＤｍ）は暗号化され、暗号化秘匿情報（Ｅ－ＵＤｍ）として記録媒体に記録される。
【０１１０】

図７は、本発明による複数の多重暗号化タイトル鍵で構成される「Ｔｉｔｌｅ　ｋｅｙ　ｆｉｌｅ」と、複数の暗号化ムーブ鍵で構成される「Ｍｏｖｅ－ｋｅｙ　ｆｉｌｅ」の構成例を示したものである。

【０１１１】

各鍵毎に、コンテンツ番号（コンテンツ識別ＩＤ）と対象コンテンツが記録されているアドレスデータ、多重暗号化されたタイトル鍵（Ｅｎｃ２－Ｋｔｎ：ＥＥ－Ｋｔｎと同じ）に、ムーブ鍵が記録媒体に存在するかの情報等が１組のタイトル鍵情報として構成され、それらが複数集合されている。このファイルには、更にムーブ鍵のベリファイデータが（ＵＤ）で暗号化された（Ｅ－Ｖｅｒｉｆｙ－Ｋｍｖ）データが集合されている。Ｍｏｖｅ－ｋｅｙ　ｆｉｌｅは、コンテンツ番号（コンテンツ識別ＩＤ）とコンテンツが記録されているアドレス情報、Ｅｎｃ－Ｍｏｖｅ　ｋｅｙ（Ｅ－Ｋｍｖ）にタイトル鍵有無情報等が１組となって複数集合して構成されている。ここで、コンテンツがムーブされると、暗号化コンテンツはそのままにして、ムーブされたコンテンツ用ムーブ鍵（Ｅ－Ｋｍｖ）が削除されて新しいＭｏｖｅ－ｋｅｙ　ｆｉｌｅとして修正され、暗号化タイトル鍵ファイルは、一部削除されたムーブ鍵の新規ベリファイデータに変更され、秘匿情報アップデートデータ（ＵＤ）で暗号化が修正され、記録されなおす。

【０１１２】

このように、ムーブコンテンツの対象タイトル鍵は、削除されたムーブ鍵が供給されない限り復号が困難であり、一方ムーブ鍵はムーブ処理後にバックアップされていた暗号化ムーブ鍵ファイルで復活させると、タイトル鍵ファイル側に組み込まれたムーブ鍵ベリファイデータと検出確認が不整合になり、利用できない全てのタイトル鍵が復号できなくなることから、このような不正処理防止が可能になる。

【０１１３】

このような暗号化鍵ファイルを構成すると、ムーブ処理を繰り返す中で、再び同じコンテンツ番号がムーブされてくると、再生復号ができない暗号化コンテンツを利用するか、新たに送られてきたムーブコンテンツを暗号化して記録するか選択するだけで、再エンコードによってデータ品位が劣化しても、元の高品位のデータが記録されている記録媒体にムーブすることで、高品位データ復活が可能になる。

【０１１４】

図８は、複数の記録媒体間をコンテンツがムーブ処理された時の、各記録媒体の状態変移を図示したものである。

【０１１５】

記録媒体Ａに記録されている高品位コンテンツは、再エンコードされて記録媒体Ｂにムーブされる。記録媒体Ｂには低レート圧縮データの暗号化コンテンツと多重暗号化タイトル鍵及び暗号化ムーブ鍵ファイルが記録される。このムーブ処理で、記録媒体Ａは、対象コンテンツ用暗号化ムーブ鍵が削除される。記録媒体Ｂは通常のムーブ処理で記録媒体Ｃにコンテンツがムーブされる。この時、記録媒体Ｂのムーブ鍵は削除される。

【０１１６】

次に、記録媒体Ｃから元の記録媒体Ａにコンテンツがムーブされる場合は、コンテンツ番号が同じであることを確認すると、記録媒体に記録済みの復号が困難な暗号化コンテンツをそのままにして、記録媒体Ｃにあるコンテンツのムーブ処理は行わずにムーブ鍵のみを記録媒体Ａにムーブする。

【０１１７】

この処理によって、記録媒体Ａに記録されている暗号化コンテンツを復号する為のタイトル鍵を復号する条件が整い、結果として元の高品位なコンテンツが記録された記録媒体Ａが復活する。

【０１１８】

図９は、本発明のムーブ処理が可能な著作権保護システムの構成例である。

【０１１９】

基本的動作は図６と同様である。図６がムーブ処理時のコンテンツ供給側ドライブとコ

ンテンツ受取り側ドライブの関係を示したものであるが、図９は、特定ドライブの記録側暗号化処理工程と、読出し側復号処理工程を図示している点が異なる。

【０１２０】

また、コンテンツのエンコード処理等が行われる「ＡＶ　Ｂｏａｒｄ：ＡＶ－Ｂ」と記録再生処理が行われる「Ｄｒｉｖｅ：Ｄｒｖ」に分割して、各暗号化処理の配置関係も示している。

【０１２１】

新規コンテンツは「ＡＶ－Ｂ」で生成されたタイトル鍵（Ｋｔ１’）で暗号化され「Ｄｒｖ」に送られる。（Ｋｔ）は、事前に対象記録媒体から読み出されていた（ＭＫＢ）（ＭＩＤ）から生成された（Ｋｍｕ）と、新規ムーブ鍵（Ｋｍｖ１’）によって生成された（Ｋｍｕｍ）によって暗号化され（Ｅ－Ｋｔ１’）が生成される。同様に新規ブーム鍵（Ｋｍｖ１’）は、事前に対象記録媒体から読み出されていた記録済み暗号化コンテンツ用ムーブ鍵ファイルを（Ｋｍｕ）で復号して、（Ｋｍｖ０）を読み出しておき、先ほどの（Ｋｍｖ１’）と集合して（Ｋｍｖ１）を生成し、（Ｋｍｕ）で暗号化してドライブに送る。同様に対象記録媒体からは、記録済み暗号化コンテンツ用暗号化タイトル鍵ファイルを読み出しておき、「Ｄｒｖ」内で同一記録媒体に記録されている秘匿情報（ＵＤ０）で復号して（Ｅ－Ｋｔ０）として「Ｄｒｖ」から「ＡＶ－Ｂ」に送っておく。

【０１２２】

更に先ほどの（Ｋｍｖ１）のベリファイデータ（Ｖ－Ｍｏ１）を検出しておき、データ編集部「ＥＤＴ」で（Ｅ－Ｋｔ０）と（Ｅ－Ｋｔ１’）に（Ｖ－Ｍｏ１）を集合して（Ｅ－Ｋｔ１）ファイルを構成し、「Ｄｒｖ」に送る。

【０１２３】

ここで、ムーブ鍵ベリファイデータ生成部「Ｖ－Ｍｏ」は、最初に対象記録媒体に記録されている（Ｅ－ｋｔ０）ファイル内の（Ｖ－Ｍｏ０）と、読み出された（Ｅ－Ｋｍｖ０）を復号して得られた（Ｋｍｖ０）に新規の（Ｋｍｖ１’）が加えられて（Ｋｍｖ１）として送られてくるが、（Ｋｍｖ１’）を外した（Ｋｍｖ０）を演算してベリファイデータを検出し、（Ｅ－Ｋｔ０）ファイルに含まれている（Ｖ－Ｍｏ０）と一致するか検出して、記録済みの暗号化コンテンツに不正行為記録が無いかチェックしている。その後に（Ｋｍｖ１）の新規ベリファイデータ（Ｖ－Ｍｏ１）を演算生成し、（Ｅ－Ｋｔ１）ファイルに加える。このようにして、「ＡＶ－Ｂ」から送られてきたデータ（Ｅｎｃ－Ｃｏｎｔｅｎｔ）そのまま記録媒体に記録され、（Ｅ－Ｋｍｖ１）ファイルは前の（Ｅ－Ｋｍｖ０）ファイルが記録されていた所に書き換えられる。

【０１２４】

（Ｅ－Ｋｔ１）は、ドライブ内で、事前に読み出されていた秘匿情報（ＵＤ０）を更新して（ＵＤ１）とし、「Ｄｒｖ」内で（Ｅ－Ｋｔ１）を多重暗号化して（Ｅ２－Ｋｔ１）として記録媒体に記録する。同様に秘匿情報（ＵＤ１）は（Ｋｍｕ）で暗号化し（Ｅ－ＵＤ１）として特殊記録方法で記録媒体に書き換えられる。ここで、「ＡＶ－Ｂ」と「Ｄｒｖ」の関係であるが、ＰＣ（パソコン）ペリフェラル機器である「Ｄｒｖ」と、ＰＣ側に組み込まれている「ＡＶ－Ｂ」では、そのデータ伝送間において、不正行為が行われる可能性が高い。

【０１２５】

そこで、現在は「Ｄｒｖ」と「ＡＶ－Ｂ」では認証処理が行われ、そのデータ伝送においては、認証処理を行なった時のみ有効な時限暗号／復号鍵（Ｂｕｓ－Ｋｅｙ）を使って暗号化伝送を行う。すなわち、認証処理が行われ、相互に不正行為が行われない相手であることが確認されると、データ送り出し側はＢｕｓ－Ｋｅｙで暗号化して送り出し、受取り側はＢｕｓ－ｋｅｙで復号して受け取る。

【０１２６】

図９における「Ａｕｔｈｅｎｔｉｃａｔｉｏｎ」部と各伝送ラインの太線部分はこの処理が行われていることを前程にしている。

【０１２７】

図９におけるデータ読出し復号処理構成に関しては、図６の説明で示したとおりである。記録側処理と同様に「Ｖ－Ｍｏ」部は記録されている（Ｋｍｖ）と（Ｅ－Ｋｔ）ファイル内の（Ｋｍｖ）ベリファイデータから、暗号鍵に不正な書込み処理が無かったかチェックする機能が含まれており、もし関係が一致しない場合は、再生拒否を行う。

【０１２８】

図１０と図１１は、図９のデータ読出し側復号処理工程と記録側暗号処理工程を記録媒体に記録されるデータファイルの関係も含めて詳細に図示したものである。

【０１２９】

図１０にて、ディスクに記録されているデータファイルと暗号化管理システムの関係を説明する。文中における暗号化データの表現を、一部「Ｅ（暗号化した鍵、暗号化されるデータ）」で示し、暗号化される鍵とその暗号化に使った暗号鍵の関係を解かりやすくした。

【０１３０】

事前に記録されている（ＭＫＢ）ファイルは、暗号／復号処理に使われるメディア鍵（Ｋｍ）抽出の暗号化鍵ブロックである。

【０１３１】

（ＭＩＤ）は、現行ＤＶＤ－ＲＡＭ規格などで使われている、ディスク最内周に構成されているＢＣＡ（バーストカッティングエリア）にディスク担体の固有識別情報である。この識別情報を暗号化管理システムに組み込む事で、暗号化が対象記録媒体に対するメディアバインド機能として働くことになる。処理結果として、（ＭＫＢ）から抽出した（Ｋｍ）と（ＭＩＤ）を函数ジェネレータ「Ｇ」で合成して、メディア固有鍵（Ｋｍｕ）を生成している。この（Ｋｍｕ）は、対象メディア固有の暗号鍵として機能する為、その鍵で暗号化されたデータは、他の記録媒体に丸ごと移しても、そのメディアのメディア固有鍵（Ｋｍｕ）が異なる為、復号できないことになる。

【０１３２】

Ｅ（Ｋｍｕ，ＵＤ）は、（ＵＤ）を（Ｋｍｕ）で暗号化して、特殊記録再生方式で記録した秘匿情報データである。（ＵＤ）はコンテンツをムーブ処理する為読み出したり、新規のコンテンツを記録する毎に、更新記録処理する。単なるコンテンツの読出し再生処理では、そのままの記録状態で継続させる。

【０１３３】

Ｅ（Ｋｍｕ，Ｋｍｖ＿Ｉ）ファイルは、ムーブ鍵ファイルである。複数のムーブ鍵が（Ｋｍｕ）で暗号化されて集合したものであり、再生動作では読み出した暗号化ムーブ鍵（Ｅ－Ｋｍｖ）は、（Ｋｍｕ）で復号して指定コンテンツ識別情報から対象ムーブ鍵（Ｋｍｖ）を検出し、（Ｋｍｕ）と函数ジェネレータで合成して（Ｋｍｕｍ）を生成する。ムーブ処理における再生では、（Ｋｍｕｍ）は暗号化タイトル鍵の復号処理後に、ムーブコンテンツ対象ムーブ鍵をコンテンツと共に対で外部に出力すると同時に、対象ムーブ鍵をファイルから削除し、新規のムーブ鍵ファイルとして、（Ｋｍｕ）で暗号化して書き直す。この時、（Ｋｍｕ）暗号化前の新しいムーブ鍵ファイルデータから、新規のベリファイデータを演算生成し、新規のタイトル鍵ファイルデータを集合させるブロックへ送り込む。

【０１３４】

Ｅ（ＵＤ，Ｅ（Ｋｍｕｍ，Ｋｔ＿ｉ））ファイルは、多重暗号化タイトル鍵ファイルである。複数の暗号化タイトル鍵とムーブ鍵ベリファイデータの集合データが、ドライブ内でのみ記録再生処理される秘匿情報（ＵＤ）によって、多重暗号化されたファイルである。再生動作では、ドライブ内で復調される（ＵＤ）で復号され暗号化タイトル鍵ファイル（Ｅ－Ｋｔ）になる。（Ｅ－Ｋｔ）を上記（ｋｍｕｍ）で復号すればタイトル鍵（Ｋｔ）が得られ、指定コンテンツのタイトル鍵（Ｋｔ）をコンテンツ復号部に送る。ムーブ処理再生動作では、（Ｅ－ｋｔ）ファイルにムーブコンテンツ対応ムーブ鍵が削除されたムーブ鍵ファイルによって演算生成されたムーブ鍵ベリファイデータを、（Ｅ－ｋｔ）ファイルに付随している旧ベリファイデータと交換して、新規の（Ｅ－Ｋｔ）ファイルを構成し、ドライブに送って更新された新規の（ＵＤ）データで暗号化して記録媒体に記録する。

即ち、ムーブ処理時は、ムーブコンテンツ対象暗号化タイトル鍵は削除でせず、そのまま残しムーブコンテンツそのもののデータファイルは存在するがタイトル鍵を復号できない旨の情報となる識別コードに変更しておく。当然、コンテンツ削除指令が出た場合は、指定コンテンツの暗号化タイトル鍵は削除し、削除されたコンテンツは存在しないよう他の情報も削除する。

【０１３５】

Ｅ（Ｋｔ，Ｃｏｎｔｅｎｔｓ＿Ｉ）は、暗号鍵（Ｋｔ）で暗号化されたコンテンツファイルである。

【０１３６】

図１１は、新規のコンテンツを記録する場合の記録媒体に記録済みデータファイルと新規ファイルの関係も含めた暗号化管理工程を示した図である。記録では、他のソース現から新規にコンテンツが記録される場合（新規のムーブ鍵を生成）とムーブ処理記録である「（１）ムーブ鍵と対になった新規のコンテンツ記録」「（２）ムーブ鍵データに含まれたコンテンツ番号（コンテンツ識別情報）から、同じ識別番号のムーブ鍵が削除された暗号化コンテンツが記録媒体に存在する事が判明した場合」の３通りの記録が考えられる。これら全ての要求に対して対応可能な記録側暗号管理処理の構成が組まれている。

【０１３７】

事前に記録されている（ＭＫＢ）ファイルは、その利用形態は前記説明の通りである。

【０１３８】

（ＭＩＤ）も前記説明と同じである。

【０１３９】

Ｅ（Ｋｍｕ，ＵＤ）ファイルは、図１０と同様にムーブ鍵ファイル他タイトル鍵ファイルが書き換えられる毎に新規のデータに更新されて（Ｋｍｕ）で暗号化して書きかえられる。

【０１４０】

Ｅ（Ｋｍｕ，Ｋｍｖ＿Ｉ）ファイルは、ムーブ鍵ファイルでムーブ記録や新規のコンテンツが記録される場合に、新しいムーブ鍵が加わって新規ファイルとして、（Ｋｍｕ）で暗号化され書きかえれる。ここで、自身が管理するコンテンツファイルで、全く新しいコンテンツではコンテンツ管理番号（識別ＩＤ）や新規のムーブ鍵を発生させ、記録媒体に記録されているムーブ鍵ファイルに加えて、新しいムーブ鍵ファイルを生成して暗号化の後記録媒体に記録する。入力されたコンテンツに対でムーブ鍵が伴ってきた場合は、記録媒体にコンテンツ番号が一致するものが無いかチェックし、一致する番号がある場合でコンテンツが再エンコードデータで無い場合はコンテンツのデータの記録処理はせず、ムーブ鍵のみをムーブ鍵ファイルに指定の場所に加えて書き換える。一致する番号が無い場合は、新規コンテンツの記録と同様にコンテンツファイルも含めて記録媒体に記録する。但し、この場合はムーブ鍵は送られてきたムーブ鍵を記録コンテンツのムーブ鍵として記録する。

【０１４１】

Ｅ（ＵＤ，Ｅ（Ｋｍｕｍ，Ｋｔ＿Ｉ））ファイルは、タイトル鍵ファイルである。新規のコンテンツ記録の場合は、乱数発生器等で新規にタイトル鍵を発生させ、記録媒体に記録されている他のコンテンツのタイトル鍵と集合させて、新規のムーブ鍵ベリファイデータと合せて、新しいタイトル鍵ファイルとして編集しドライブ内で更新された（ＵＤ）によって多重暗号化して記録する。ムーブ記録においては、コンテンツと対で送られてきたムーブ鍵情報内のコンテンツ番号（識別ＩＤ）を、記録媒体に記録済みのコンテンツ番号情報と比較して、同一コンテンツが記録済みであるかをチェックし、同一コンテンツが記録されている場合は新規のタイトル鍵は発行せず、新規のムーブ鍵ファイルのベリファイデータのみ交換して新規の暗号化タイトル鍵ファイルを生成し、更新された（ＵＤ）で多重暗号化して記録媒体に記録する。コンテンツが記録されていない場合は、新規のタイトル鍵を発行して、入力されたコンテンツの暗号化に用いると同時に、ドライブ内の記録媒体に書かれたいる（ＭＫＢ）（ＭＩＤ）で抽出した（Ｋｍｕ）とコンテンツと対で送られ

てきた（Ｋｍｖ）で生成した（Ｋｍｕｍ）で新規タイトル鍵を暗号化し、記録済みの暗号化タイトル鍵ファイルに加えて新規のタイトル鍵ファイルを構成し、更新された（ＵＤ）で多重暗号化して記録媒体に記録する。

【０１４２】

Ｅ（Ｋｔ、Ｃｏｎｔｅｎｔ＿ｉ）は、（Ｋｔ）で暗号化された複数のコンテンツファイルを意味している。ムーブ時に同一コンテンツが既に記録されている場合は、暗号化コンテンツは記録するかしないか選択する事が出来る。既に記録されている場合で、高品位データである場合は記録しないが、データ品位が同一以下である場合は、ユーザの判断に委ねられる。

【０１４３】

図１２は、本発明によって暗号化コンテンツや暗号化暗号鍵が記録された記録媒体のデータ配置を示したものである。メディアＩＤ（ＭＩＤ）はリードインエリアの更に内周側に設けられたＢＣＡに事前に書き込まれ情報データである。記録再生媒体では、個別にＩＤ番号が記録される為、暗号化管理システムに導入する事で、暗号鍵がメディア毎に固有の鍵となり、暗号化コンテンツが記録された記録媒体にバインドされた状態とする効果が期待できる。（ＭＫＢ）はリードインエリアに事前記録された鍵束で、記録再生装置に個別に配布されているデバイス鍵（Ｄ－Ｋ）で、同一のメディア鍵（Ｋｍ）が抽出出来るような性質を持つ。データエリアの内周側には、本発明のムーブ鍵ファイルと２重暗号化されたタイトル鍵ファイルが記録されている。その外周には暗号化されたコンテンツファイルが記録される。

【０１４４】

図１３は本発明のＵＤ信号埋め込み処理方式を説明する為に図示したものである。

【０１４５】

先ず、記録したいデータは、２Ｋバイトのデータフレーム単位でセクタＩＤ等が付加された後、誤り検出符号（ＥＤＣ）Ｒ０２は生成付加され、Ｓｃｒａｍｂｌｅ処理Ｒ０３に入力される。ここでサーボ系安定化等の理由で同一データ連続防止スクランブル処理３を行なう。このデータは１６Ｄａｔａ　ｆｒａｍｅＤ０３１に入力され、これらデータフレームを１６組集合させる。このデータはＰＯ／ＰＩＲ０５１に入力され、誤り検出訂正符号（ＰＯ／ＰＩ）が生成される。

【０１４６】

次に、このデータはＰＯ　ＩｎｔｅｒｌｅａｖｅＲ０６に入力され、（ＰＯ）がインターリーブ処理で分散配置され１６組の記録セクタによるＥＣＣブロックが構成される。このデータはＳｙｎｃ付加＆変調Ｒ０７に入力され、一定データ長毎に同期信号が付加および変調処理される。このデータはＵＤ置換Ｒ１４に入力され、１６組の物理セクタが生成される。

【０１４７】

一方ＵＤＲ１０、ＵＤ－ＰａＲ１１、変調２Ｒ１３にて、（ＵＤ）信号を特殊変調器で変調されたＵＤをＵＤ置換Ｒ１４にて一部置換する。その後記録媒体書き込みＲ０８を介して記録媒体ＡＤ１に記録される。

【０１４８】

このような処理によって、（ＵＤ）変調信号で置換された部分はメインデータブロックとしてはエラーとなるが、エラー量少ない場合は通常発生するエラーの一部として処理される為、エラー訂正処理によって復元される。一方、特殊変調された（ＵＤ）はドライブ内でのみ設置される特殊復調器によって復調され、同時に特殊変調された（ＵＤ）専用誤り訂正符号によって、誤り訂正処理され（ＵＤ）信号が復調される。

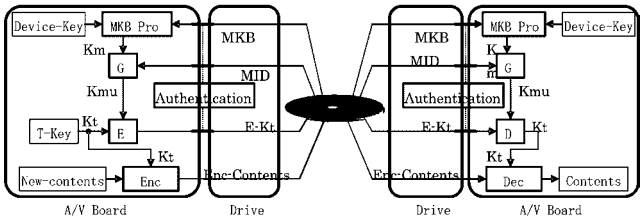
【０１４９】

このような処理によって、（ＵＤ）データはドライブ内でのみ記録再生処理とそのデータの利用が行われる為、外部で操作することができなくなり、秘匿情報としての利用が可能なことから、暗号鍵の更新データに利用すれば、事前にバックアップしておいた暗号化暗号鍵を、消去した暗号化暗号鍵として復活させる不正行為は利用できなくなる。

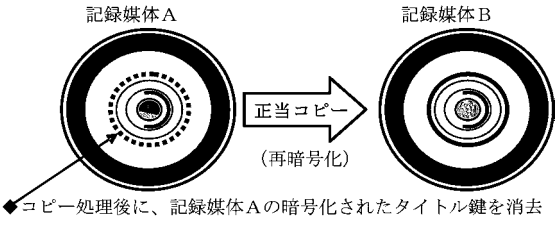
【０１５０】
図１４は、ＤＶＤ方式の１６組の記録セクタで構成されるＥＣＣブロックの図である。
【０１５１】
図１５は、秘匿情報（ＵＤ）を埋め込んだ１物理セクタの関係を示した図である。秘匿情報（ＵＤ）は複数の物理セクタに分散配置されることで、主情報の誤り訂正能力をさほど悪化させること無くして、主情報の復元可能性を向上している。
【０１５２】
図１６と図１７は、本発明の変形例である。
【０１５３】
本発明の図６と図７では、ムーブ鍵とタイトル鍵の関係において、タイトル鍵ファイルを（ＵＤ）でバックアップデータで復活させる不正行為を防止し、ムーブ鍵ファイルのバックアップデータによる不正復活行為は、ムーブ鍵のベリファイデータをタイトル鍵ファイルに組み込む事で、ムーブ鍵のバックアップ不正復活を防止していた。図１６と図１７による本発明の変形では、ムーブ鍵ベリファイデータは利用せず、ムーブ鍵ファイルもタイトル鍵ファイルも（ＵＤ）による多重暗号化処理で、常に記録やムーブ処理時暗号鍵ファイルが（ＵＤ）で更新される方式としている為、バックアップデータによる違反復活は利用できない構成である。他の処理は、図６と図７の処理動作と同じである。
【０１５４】
図１８は、タイトル鍵の暗号化工程の変形例である。
【０１５５】
図６～図１６においては、（Ｋｔ）は（Ｋｍｕ）と（Ｋｍｖ）を函数ジェネレータ（Ｇ）で合成して暗号鍵（Ｋｍｕｍ）を生成し、（Ｋｔ）を暗号化していた。図１８の「方式Ａ」である。
【０１５６】
別の処理としては、（Ｋｔ）を（Ｋｍｕ）で暗号化した後（Ｋｍｖ）で更に多重暗号化し、更に（ＵＤ）で３重暗号化する「方式Ｂ」である。この方式では暗号鍵（Ｋｍｕｍ）は生成しない。即ち、（Ｋｔ）を３重に暗号化する方法である。
【図面の簡単な説明】
【０１５７】
【図１】本発明に用いるＣＰＲＭの基本構成を示した処理システム図。
【図２】本発明に用いるコンテンツ移動に対する記録媒体間の状態を示す図。
【図３】本発明に用いる秘匿情報記録再生技術を用いて、ムーブ処理を可能にする著作権保護方式を示した処理システム図。
【図４】図３に示したシステムを用いて、コンテンツを再エンコード処理した後ムーブ記録した場合の構成を示したシステム図。
【図５】図４で示したコンテンツムーブ処理における、記録媒体の関係を示した図。
【図６】本発明の暗号化管理システム図。
【図７】本発明の複数の多重暗号化タイトル鍵で構成される「Title key file」と、複数の暗号化ムーブ鍵で構成される「Move-key file」の構成例を示した図。
【図８】複数の記録媒体間をコンテンツがムーブ処理された時の、各記録媒体の状態変移を示した図。
【図９】本発明のムーブ処理が可能な著作権保護システム図。
【図１０】図９のデータ読出し側復号処理工程と記録側暗号処理工程を記録媒体に記録されるデータファイルの関係も含めて詳細に示した図。
【図１１】図９のデータ読出し側復号処理工程と記録側暗号処理工程を記録媒体に記録されるデータファイルの関係も含めて詳細に示した図。
【図１２】本発明によって暗号化コンテンツや暗号化暗号鍵が記録された記録媒体のデータ配置を示した図。
【図１３】本発明の秘匿情報信号の埋め込み処理方式を説明するための図。
【図１４】ＤＶＤ方式の１６組の記録セクタで構成されるＥＣＣブロック図。

【図１５】秘匿情報を埋め込んだ１物理セクタの関係を示した図。
【図１６】本発明の変形例による暗号化管理システム図。
【図１７】本発明の変形例による暗号化管理システム図。
【図１８】タイトル鍵の暗号化管理システム図。
【符号の説明】
【０１５８】
Ｒ０１・・・Ｍ－Ｄａｔａ　Ｓｅｌｅｃｔ
Ｒ０２・・・ＥＤＣ生成
Ｒ０３・・・Ｓｃｒａｍｂｌｅ
Ｒ０３１・・・１６Ｄａｔａ　ｆｒａｍｅ
Ｒ０５１・・・ＰＯ／ＰＩ
Ｒ０６・・・ＰＯ　Ｉｎｔｅｒｌｅａｖｅ
Ｒ０７・・・Ｓｙｎｃ付加変調
Ｒ１４・・・秘匿情報置換
Ｒ０８・・・記録媒体書き込み
Ｒ１０・・・秘匿情報
Ｒ１１・・・ＵＤ－Ｐａ生成
Ｒ１３・・・変調

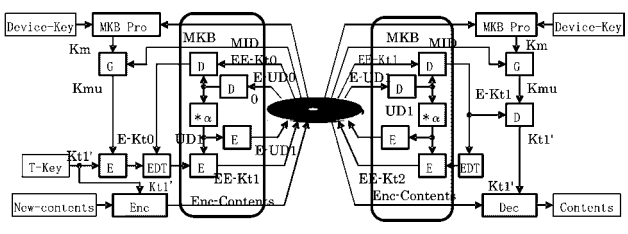
【図１】



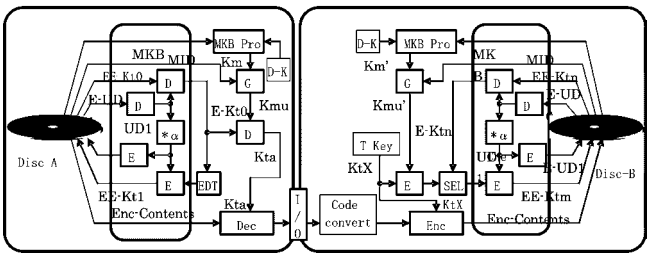
【図２】
記録媒体間のコンテンツ移動



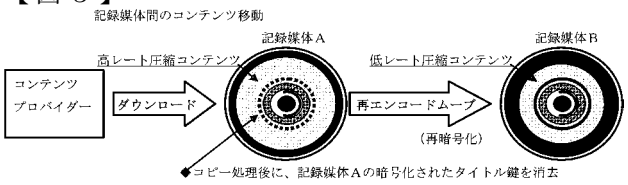
【図３】



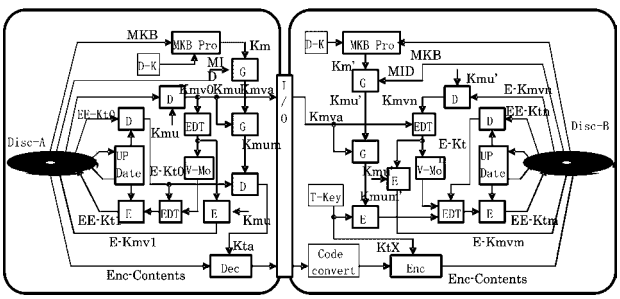
【図４】



【図５】



【図６】



【図７】

Title key File

暗号化タイトル鍵(Kt)のファイル識別コード			
暗号化タイトル鍵の数			
Cont-1	address	Enc2-Kt1	11
Cont- 2	address	Enc2-Kt2	11
Cont- 3	address	Enc2-Kt3	10
Cont-n-1	address	Enc2-Kt(n-1)	11
Cont-n	address	Enc2-Kt(n)	11
RSV(0)	RSV(0)	RSV(0)	00
RSV(0)	RSV(0)	RSB(0)	00
E-Verify-Kmv (Enc V-Mo)			

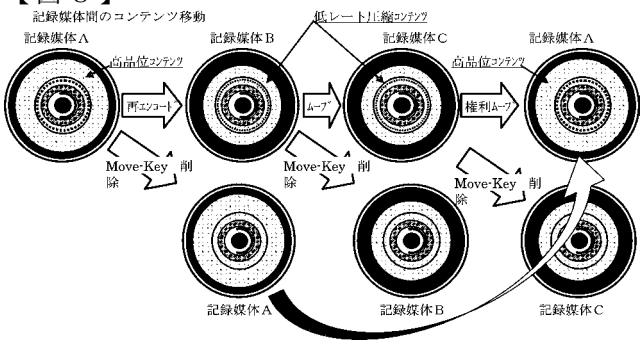
Move-Key File

暗号化ムーブ鍵(Kmv)のファイル識別コード			
Cont 暗号化暗号鍵の数			
Cont-1	address	Enc-Move key1	11
Cont- 2	address	Enc -Move key2	11
Cont-3	address	all=0	01
Cont-n-1	address	Enc -Move key n-1	11
Cont-n	address	Enc -Move key n	11
RSV(0)	RSV(0)	RSV(all=0)	00
RSV(0)	RSV(0)	RSV(all=0)	00

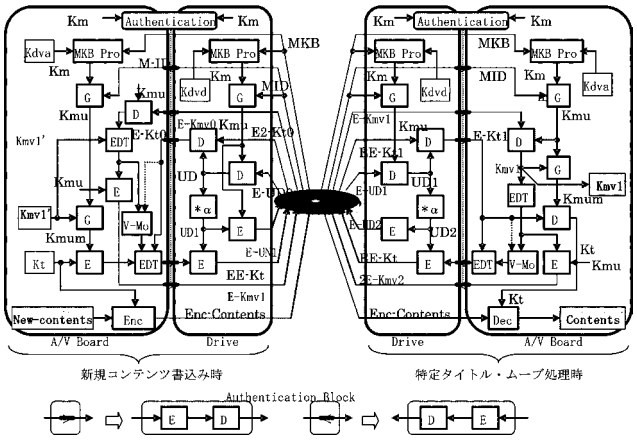
Content-NO address 多重暗号化 Title-Key　Co ntent-NO address 暗号化 Move-Key

Enc-Move key の有無情報　Enc-Title Key の有無情報

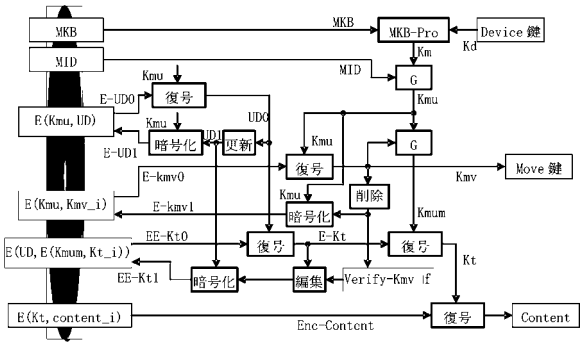
【図８】



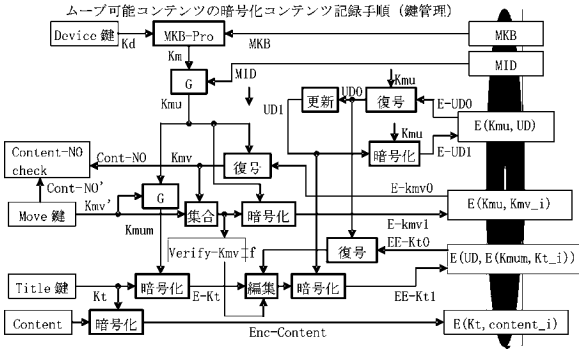
【図９】



【図１０】

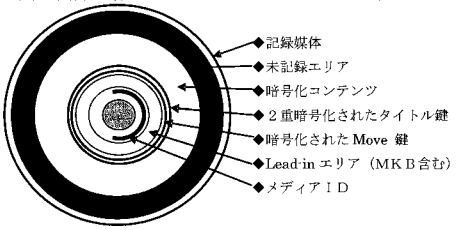


【図１１】

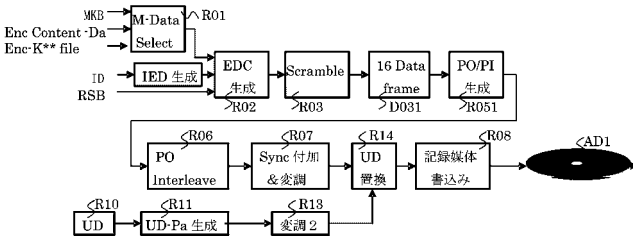


【図１２】

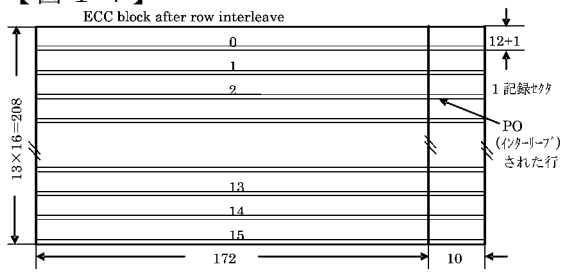
記録媒体に著作権保護コンテンツが記録された場合のデータ配置関係



【図１３】

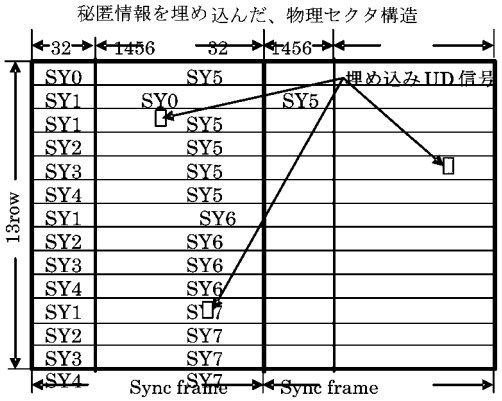


【図１４】

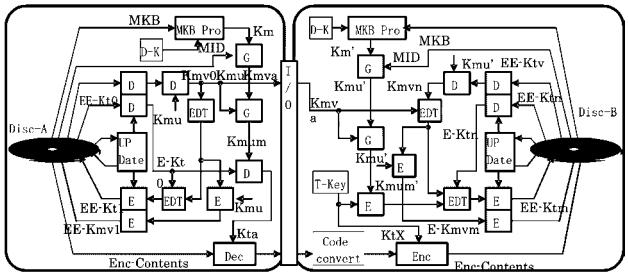


【図１５】

秘匿情報を埋め込んだ、物理セクタ構造



【図１６】



【図１７】

タイトル鍵とムーブ鍵のファイル構造例

Title key File

暗号化タイトル鍵(Kt)のファイル識別コード			
暗号化タイトル鍵の数			
Cont-1	address	Enc2-Kt1	11
Cont-2	address	Enc2-Kt2	11
Cont-3	address	Enc2-Kt3	10
Cont-n-1	address	Enc2-Kt(n-1)	11
Cont-n	address	Enc2-Kt(n)	11
RSV(0)	RSV(0)	RSV(0)	00
RSV(0)	RSV(0)	RSV(0)	00

Content-NO address 多重暗号化 Title-Key

Enc-Move key の有無情報

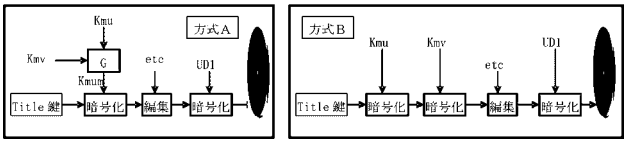
Move-Key File

暗号化ムーブ鍵(Kmv)のファイル識別コード			
Cont 暗号化暗号鍵の数			
Cont-1	address	Enc2-Move key1	11
Cont-2	address	Enc2 -Move key2	11
Cont-3	address	all=0	01
Cont-n-1	address	Enc2 -Move key n-1	11
Cont-n	address	Enc2 -Move key n	11
RSV(0)	RSV(0)	RSV(all=0)	00
RSV(0)	RSV(0)	RSV(all=0)	00

Content -NO address 暗号化 Move-Key

Enc-Title Key の有無情報

【図１８】



フロントページの続き

(51)Int.Cl.	FI		テーマコード（参考）
	Ｇ１１Ｂ	20/12	
	Ｈ０４Ｌ	9/00	６０１Ｂ