(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3758231号

(P3758231)

(45)発行日　平成18年3月22日(2006.3.22)　(24)登録日　平成18年1月13日(2006.1.13)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	540P
G09C 1/00	(2006.01)	G09C	1/00	630A
G11B 20/10	(2006.01)	G09C	1/00	660D
H04L 9/08	(2006.01)	G11B	20/10	H
		H04L	9/00	601A

請求項の数 6　(全 29 頁)

(21)出願番号　特願平8-98950
(22)出願日　平成8年4月19日(1996.4.19)
(65)公開番号　特開平9-97216
(43)公開日　平成9年4月8日(1997.4.8)
審査請求日　平成13年8月22日(2001.8.22)
(31)優先権主張番号　特願平7-189309
(32)優先日　平成7年7月25日(1995.7.25)
(33)優先権主張国　日本国(JP)

前置審査

(73)特許権者　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100067736
弁理士　小池　晃
(74)代理人　100086335
弁理士　田村　榮一
(74)代理人　100096677
弁理士　伊賀　誠司
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】信号記録装置及び方法、並びに信号再生装置及び方法

(57)【特許請求の範囲】

【請求項１】

信号記録媒体に対して暗号化した信号を記録する信号記録装置において、

入力信号を暗号化する少なくとも一つの信号暗号化手段と、

上記少なくとも一つの信号暗号化手段において暗号化された信号の暗号化を解くための鍵情報が配置される場所を指示する鍵格納場所情報を出力する出力手段と、

上記暗号化した信号と上記鍵格納場所情報とを上記信号記録媒体に記録する記録手段とを有し、

上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスを用いるとき、上記鍵情報には、上記信号記録媒体以外の場所に配置された情報を用いることを特徴とする信号記録装置。

【請求項２】

上記鍵情報を暗号化する鍵情報暗号化手段と、

上記鍵情報暗号化手段において暗号化された鍵情報の暗号化を解くための鍵情報が配置される場所を指示する格納情報指示情報を出力する格納情報指示情報出力手段とをさらに具備し、

上記記録手段は、上記暗号化した信号と上記鍵格納場所情報と上記格納情報指示情報とを上記信号記録媒体に記録することを特徴とする請求項１記載の信号記録装置。

【請求項３】

信号記録媒体から暗号化信号を再生する信号再生装置であって、
上記信号記録媒体から上記暗号化信号及び鍵格納場所情報を読み取る読み取り手段と、
上記鍵格納場所情報に基づいて指定された場所に配置された上記暗号化を解くための鍵情報を取り出す取り出し手段と、
上記取り出し手段により取り出された鍵情報を用いて、上記暗号化信号の当該暗号化を解く復号手段とを有し、
上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスが用いられるとき、上記信号記録媒体以外の場所が指定されることを特徴とする信号再生装置。

【請求項４】
上記鍵情報は暗号化されており、上記読み取り手段は、当該鍵情報の暗号化の鍵情報が配置される場所を指示する情報をも読み取ることを特徴とする請求項３記載の信号再生装置。

【請求項５】
信号記録媒体に対して暗号化した信号を記録する信号記録方法において、
入力信号を信号暗号化手段が暗号化する信号暗号化工程と、
上記信号暗号化工程において暗号化された信号の暗号化を解くための鍵情報が配置される場所を指示する鍵格納場所情報を出力手段が出力する出力工程と、
上記暗号化した信号と上記鍵格納場所情報とを記録手段が上記信号記録媒体に記録する記録工程とを有し、
上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスを用いるとき、上記鍵情報には、上記信号記録媒体以外の場所に配置された情報を用いることを特徴とする信号記録方法。

【請求項６】
信号記録媒体から暗号化信号を再生する信号再生方法であって、
上記信号記録媒体から上記暗号化信号及び鍵格納場所情報を読み取り手段が読み取る読み取り工程と、
上記鍵格納場所情報に基づいて指定された場所に配置された上記暗号化を解くための鍵情報を取り出し手段が取り出す取り出し工程と、
上記取り出し工程により取り出された鍵情報を用いて、復号手段が上記暗号化信号の当該暗号化を解く復号工程とを有し、
上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスが用いられるとき、上記信号記録媒体以外の場所が指定されることを特徴とする信号再生方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、コピーの防止や不正使用を阻止するための信号記録装置及び方法、並びに信号再生装置及び方法に関する。

【０００２】
【従来の技術】
近年において、光ディスク等の信号記録媒体の大容量化と普及により、記録されている信号の著作権を保護するために、不法なコピーの防止が重要とされていてきいる。すなわち、ディジタルオーディオデータやディジタルビデオデータの場合には、コピー或いはダビングにより劣化の無い複製物を容易に生成でき、またコンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる著作権の侵害等の弊害が生じてきているのが実情である。

【０００３】
このようなことから、上記不法コピーの防止を目的として、オリジナルの信号記録媒体に

不法コピー防止のための所定のＩＤビットを記録しているものがある。
【０００４】
例えば、いわゆるＲ－ＤＡＴ（Rotary head Digital Audio Taperecoder）と称されるディジタルオーディオ信号記録再生装置における上記不法コピー防止のための方式としては、信号記録媒体としてのディジタルオーディオテープ上に記録されるディジタルオーディオ信号のメインデータエリアに、ディジタルコピーの禁止や段階的な世代コピーを禁止（すなわち世代制限）するための禁止コード（いわゆるＳＣＭＳ：シリアルコピー管理システムの規格の禁止コード）を記録しておき、ディジタルオーディオ信号記録装置がこの禁止コードを検出したときに、新たなディジタルオーディオテープ上への当該ディジタルオーディオ信号のコピー記録を禁止するような方式が採用されている。
【０００５】
また、信号記録媒体に記録された例えばディジタルビデオ信号の不法コピーを防止するためには、上記Ｒ－ＤＡＴにおける記録再生装置間での不法コピー防止の方式と同様に、オリジナルのディジタル記録媒体に不法コピー防止のための所定のＩＤビット（ＣＧＭＳ：コピー世代管理システムの規格の禁止コード）を記録することが考えられる。
【０００６】
さらに、コンピュータデータの場合には、ファイル内容自体を暗号化鍵情報を用いて暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。なおこれは、情報流通の形態として、情報が暗号化されて記録されたディジタル記録媒体を配布しておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものである。
【０００７】
【発明が解決しようとする課題】
ところが、上述したような従来の信号記録媒体用の禁止コードや暗号鍵情報は、特開平５－１７３８９１号公報に示されるように、記録媒体上のユーザからアクセスされるシステム固有の特定の場所に記録されている。なお、上記禁止コードや暗号鍵情報も、通常暗号化されていている。
【０００８】
このように、上記禁止コードや暗号鍵情報の配置がそれぞれの暗号化手法において任意の場所で固定的であると、互換性がなくなる虞れがある。また、禁止コードや暗号鍵情報を固定的に配置すれば、暗号化の手法も固定化されることになり、柔軟性，拡張性に乏しく、フォーマット自身の寿命を縮めてしまう可能性がある。
【０００９】
さらに、暗号鍵情報や禁止コードは、例えばユーザからアクセス可能な場所にあるため、悪意のあるユーザによる解読や不法コピーの対象になりやすかった。
【００１０】
そこで、本発明は上述したような実情に鑑みてなされたものであり、不法解読や不法コピーを困難にする信号記録装置及び方法、並びに信号再生装置及び方法を提供することを目的とする。
【００１１】
【課題を解決するための手段】
本発明に係る信号記録装置は、上述の課題を解決するために、信号記録媒体に対して暗号化した信号を記録する信号記録装置において、入力信号を暗号化する少なくとも一つの信号暗号化手段と、上記少なくとも一つの信号暗号化手段において暗号化された信号の暗号化を解くための鍵情報が配置される場所を指示する鍵格納場所情報を出力する出力手段と、上記暗号化した信号と上記鍵格納場所情報とを上記信号記録媒体に記録する記録手段とを有し、上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスを用いるとき、上記鍵情報には、上記信号記録媒体以外の場所に配置された情報を用いることを特徴としている。

また、本発明に係る信号記録方法は、上述の課題を解決するために、信号記録媒体に対して暗号化した信号を記録する信号記録方法において、入力信号を信号暗号化手段が暗号化する信号暗号化工程と、上記信号暗号化工程において暗号化された信号の暗号化を解くための鍵情報が配置される場所を指示する鍵格納場所情報を出力手段が出力する出力工程と、上記暗号化した信号と上記鍵格納場所情報とを記録手段が上記信号記録媒体に記録する記録工程とを有し、上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスを用いるとき、上記鍵情報には、上記信号記録媒体以外の場所に配置された情報を用いることを特徴としている。

【００１２】

また、本発明に係る信号再生装置は、上述の課題を解決するために、信号記録媒体から暗号化信号を再生する信号再生装置であって、上記信号記録媒体から上記暗号化信号及び鍵格納場所情報を読み取る読み取り手段と、上記鍵格納場所情報に基づいて指定された場所に配置された上記暗号化を解くための鍵情報を取り出す取り出し手段と、上記取り出し手段により取り出された鍵情報を用いて、上記暗号化信号の当該暗号化を解く復号手段とを有し、上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスが用いられるとき、上記信号記録媒体以外の場所が指定されることを特徴としている。

さらに、本発明に係る信号再生方法は、上述の課題を解決するために、信号記録媒体から暗号化信号を再生する信号再生方法であって、上記信号記録媒体から上記暗号化信号及び鍵格納場所情報を読み取り手段が読み取る読み取り工程と、上記鍵格納場所情報に基づいて指定された場所に配置された上記暗号化を解くための鍵情報を取り出し手段が取り出す取り出し工程と、上記取り出し工程により取り出された鍵情報を用いて、復号手段が上記暗号化信号の当該暗号化を解く復号工程とを有し、上記鍵格納場所情報として、上記信号記録媒体上のアドレス及び上記信号記録媒体上に存在しないアドレスの内の、上記信号記録媒体上に存在しないアドレスが用いられるとき、上記信号記録媒体以外の場所が指定されることを特徴としている。

【００１３】

すなわち、本発明によれば、信号記録媒体には鍵情報の場所を指示する鍵格納場所情報を記録し、信号再生の際には当該鍵格納場所情報に基づいて鍵情報を取り出すようにすることで、鍵情報を容易に取り出せないようにしている。

【００１４】

【発明の実施の形態】

以下、本発明に係るいくつかの好ましい実施の形態について、図面を参照しながら説明する。

【００１５】

図１は、本発明の実施の形態となる信号記録装置の一構成例を概略的に示すブロック図である。

この図１において、入力端子１１には、例えばアナログのオーディオ信号やビデオ信号をディジタル変換して得られたデータやコンピュータデータ等のディジタルデータが供給されている。この入力ディジタルデータは、インターフェース回路１２を介して、セクタ化回路１３に送られ、所定データ量単位、例えば２０４８バイト単位でセクタ化される。

【００１６】

このセクタ化されたデータは、スクランブル処理回路１４に送られてスクランブル処理が施される。この場合のスクランブル処理は、同一バイトパターンが連続して表れないように、すなわち同一パターンが除去されるように、入力データをランダム化して、信号を適切に読み書きできるようにすることを主旨としたランダム化処理のことである。

【００１７】

上記スクランブル処理あるいはランダム化処理されたデータは、ヘッダ付加回路１５に送られて、各セクタの先頭に配置されるヘッダデータが付加された後、誤り訂正符号化回路

１６に送られる。
【００１８】
次に誤り訂正符号化回路１６では、データ遅延及びパリティ計算を行ってパリティを付加する。
【００１９】
次の変調回路１７では、所定の変調方式に従って、例えば８ビットデータを１６チャンネルビットの変調データに変換し、同期付加回路１８に送る。同期付加回路１８では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブルールのパターンの同期信号を所定のデータ量単位で付加し、駆動回路すなわちドライバ１９を介して記録ヘッド２０に送っている。
【００２０】
記録ヘッド２０は、例えば光学的あるいは磁気光学的な記録を行うものであり、ディスク状の記録媒体２１に上記変調された記録信号の記録を行う。このディスク状記録媒体２１は、スピンドルモータ２２により回転駆動される。
【００２１】
なお、上記スクランブル処理回路１４は、必須ではなく、また、ヘッダ付加回路１５の後段に挿入して、ヘッダ付加されたディジタルデータに対してスクランブル処理を施して誤り訂正符号化回路１６に送るようにしてもよい。
【００２２】
ここで、セクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、誤り訂正符号化回路１６、変調回路１７、及び同期付加回路１８のいずれか少なくとも１つの回路は、入力に対して暗号化処理を施して出力するような構成を有している。好ましくは、２つ以上の回路で暗号化処理を施すことが挙げられる。
【００２３】
この暗号化処理の鍵情報は、例えば媒体固有の識別情報、媒体の出荷先の地域を表す仕向け情報（Regional Code） や、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報、外部から供給される識別情報等を少なくとも一部に用いることができるものである。上記回路１３～１８の少なくとも１つ、好ましくは２以上で当該鍵情報を用いた入力データに対する暗号化処理が施される。
【００２４】
この場合、回路１３～１８のどの回路において暗号化処理が施されたかも選択肢の１つとなっており、再生時に正常な再生信号を得るために必要な鍵と考えられる。すなわち、１つの回路で暗号化処理が施されていれば、６つの選択肢の１つを選ぶことが必要となり、２つの回路で暗号化処理が施されていれば、２つの回路の組み合わせの数に相当する１５個の選択肢の内から１つを選ぶことが必要となる。６つの回路１３～１８の内の１～６つの回路で暗号化処理が施される可能性がある場合には、さらに選択肢が増大し、この組み合わせを試行錯誤的に見つけることは困難であり、充分に暗号の役割を果たすものである。
【００２５】
さらに、暗号化の鍵情報を所定タイミング、例えばセクタ周期で切り換えることが挙げられる。この所定タイミングで鍵情報の切り換える場合に、切り換えを行うか否かや、切換周期、複数の鍵情報の切換順序等の情報も鍵として用いることができ、暗号化のレベルあるいは暗号の難易度、解き難さ、解読の困難さをさらに高めることができる。
【００２６】
また、上述した鍵情報は、後述する暗号鍵格納場所情報により指示される媒体１０１上の位置、或いは当該媒体１０１上以外の位置に格納されるものである。上記鍵格納場所情報は、例えば上記インターフェース回路１２からＴＯＣ（Table of contents ）生成回路２３を介して端子２４に送られる情報であり、また、インターフェース回路１２から直接的に端子２５に送られる情報である。これらの端子２４、２５からの鍵格納場所情報が、記

録媒体１０１の例えば後述するＴＯＣ領域、或いはその他の所定位置に記録されるようになされている。なお、以下の説明では、ＴＯＣ領域に鍵格納場所情報が記録される場合を例に挙げている。

【００２７】

次に、各回路１３～１８の構成及び暗号化処理の具体例について説明する。

【００２８】

先ず、セクタ化回路１３においては、例えば図２に示すような偶数・奇数バイトのインターリーブ処理を行わせることが挙げられる。すなわち、図２において、上記図１のインターフェース回路１２からの出力を、２出力の切換スイッチ３１に送り、この切換スイッチ３１の一方の出力を偶奇インターリーバ３３を介してセクタ化器３４に送り、切換スイッチ３１の他方の出力をそのままセクタ化器３４に送っている。セクタ化器３４では、例えば入力データの２０４８バイト単位でまとめて１セクタとしている。このセクタ化回路１３の切換スイッチ３２の切換動作を、鍵となる１ビットの制御信号で制御するわけである。偶奇インターリーバ３３は、図３のＡに示すような偶数バイト３６ａと奇数バイト３６ｂとが交互に配置された入力データの１セクタ分を、図３のＢに示すように、偶数データ部３７ａと奇数データ部３７ｂとに分配して出力する。さらに、図３のＣに示すように、１セクタ内の所定の領域３９を鍵情報により特定し、この領域３９内のデータについてのみ偶数データ部３９ａと奇数データ部３９ｂとに分配するようにしてもよい。この場合には、領域３９の特定の仕方を複数通り選択できるように設定することもでき、鍵情報の選択肢をさらに増加させて暗号化のレベルをより高めることもできる。

【００２９】

次に、スクランブル処理回路１４には、例えば図４に示すように、１５ビットのシフトレジスタを用いたいわゆるパラレルブロック同期タイプのスクランブラを用いることができる。このスクランブラのデータ入力用の端子３５には、ＬＳＢ（最下位ビット）が時間的に先となる順序、いわゆるＬＳＢファーストで、上記セクタ化回路１３からのデータが入力される。スクランブル用の１５ビットのシフトレジスタ１４ａは、排他的論理和（ExOR）回路１４ｂを用いて生成多項式$x^{15}+x+1$に従ったフィードバックがかけられ、１５ビットのシフトレジスタ１４ａには、図５に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図５のプリセット値の選択番号は、例えばセクタアドレスの下位側４ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ１４ａからの出力データと端子３５からの入力データとは、ExOR回路１４ｃにより排他的論理和がとられて、端子１４ｄより取り出され、図１のヘッダ付加回路１５に送られる。

【００３０】

ここで、上記生成多項式及びプリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記生成多項式を変化させるには、例えば図６に示すような構成を用いればよい。この図６において、１５ビットのシフトレジスタ１４ａの各ビットからの出力が切換スイッチ１４ｆの各被選択端子に送られ、この切換スイッチ１４ｆは制御端子１４ｇからの例えば４ビットの制御データによって切換制御され、切換スイッチ１４ｆからの出力はExOR回路１４ｂに送られている。このような構成の制御端子１４ｇの制御データを変化させることにより、生成多項式$x^{15}+x^{n}+1$のｎを変化させることができる。また、上記プリセット値を変化させるには、上記図５のプリセット値テーブルの各プリセット値を、例えば１６ビットの識別情報の各ビット値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND）、論理和（OR）、シフト演算等を使用できる。なお、生成多項式を変化させるための構成は図６の構造に限定されず、シフトレジスタの段数や取り出すタップ数を任意に変更してもよい。

【００３１】
次に、ヘッダ付加回路１５について説明する。
先ず、図７はセクタフォーマットの具体例を示しており、１セクタは、２０４８バイトのユーザデータ領域４１に対して、４バイトの同期領域４２と、１６バイトのヘッダ領域４３と、４バイトの誤り検出符号（ＥＤＣ）領域４４とが付加されて構成されている。誤り検出符号領域４４の誤り検出符号は、ユーザデータ領域４１及びヘッダ領域４３に対して生成される３２ビットのＣＲＣ符号から成っている。ヘッダ付加回路１５での暗号化処理としては、同期いわゆるデータシンクに対して、ヘッダのアドレス及びＣＲＣに対して施すことが挙げられる。
【００３２】
セクタの同期すなわちデータシンクに対して暗号化処理を施す一例としては、４バイトの同期領域４２の各バイトに割り当てられたバイトパターンを、図８の「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」にてそれぞれ表すとき、２ビットの鍵情報を用いて、この４バイトの内容をバイト単位でシフトあるいはローテートすることが挙げられる。すなわち、２ビットの鍵が「０」のとき「ＡＢＣＤ」、「１」のとき「ＢＣＤＡ］、「２」のとき「ＣＤＡＢ］、「３」のとき「ＤＡＢＣ」のように切り換えることにより、この鍵が合致しないとセクタの同期がとれなくなり、正常な再生が行えない。なお、上記バイトパターン「Ａ」～「Ｄ」としては、例えばＩＳＯ６４６のキャラクタコード等を使用できる。
【００３３】
ヘッダ領域４３内には、図９に示すように、いわゆる巡回符号であるＣＲＣ４５、コピーの許可／不許可やコピー世代管理等のためのコピー情報４６、多層ディスクのどの層かを示す層４７、アドレス４８、予備４９の各領域が設けられている。この内で、アドレス４８の３２ビットにビットスクランブル、この場合には、ビット単位での転置処理を施すことにより、暗号化が行える。また、ＣＲＣ４５の生成多項式として、$x^{16}+x^{15}+x^{2}+1$ が用いられている場合、第２、第３項のx^{15}、x^{2} の代わりに、x^{15}～ｘに対応する１５ビットを鍵に応じて変化させることが挙げられる。また、ＣＲＣ４５の１６ビットと鍵情報とを論理演算することも挙げられる。
【００３４】
なお、上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダ、あるいは媒体製造装置の固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。
【００３５】
次に、誤り訂正符号化回路１６の具体例を図１０に示す。
この図１０において、誤り訂正符号化の１フレームは１４８バイトあるいは１４８シンボルのデータから成り、上記ヘッダ付加回路１５からのディジタルデータが１４８バイト毎にまとめられて、第１の符号化器であるＣ１エンコーダ５２に供給される。Ｃ１エンコーダ５２では８バイトのＰパリティが付加され、インターリーブのための遅延回路５３を介して第２の符号化器であるＣ２エンコーダ５４に送られる。Ｃ２エンコーダ５４では１４バイトのＱパリティが付加され、このＱパリティは遅延回路５５を介してＣ１エンコーダ５２に帰還されている。このＣ１エンコーダ５２からのＰ、Ｑパリティを含む１７０バイトが取り出されて、遅延回路５６を介し、インバータ部５７ａを有する再配列回路５７を介して出力され、図１の変調回路１７に送られる。
【００３６】
このような誤り訂正符号化回路において暗号化処理を施す場合には、例えば再配列回路５７内のインバータ部５７ａの各バイト毎に、暗号の鍵情報に応じてインバータを入れるか入れないかの選択を行わせるようにすることが挙げられる。すなわち、基準構成においては、２２バイトのＰ、Ｑパリティに対して再配列回路５７のインバータ部５７ａのインバータによる反転が行われて出力されるが、これらのインバータのいくつかを無くしたり、Ｃ１データ側にいくつかのインバータを入れて反転して出力させたりすることが挙げられ

る。

【００３７】

このようなデータ変換を施す場合、基準構成からの違いの程度によって誤り訂正不能確率が変化し、違いが少ないときには最終的な再生出力におけるエラー発生確率がやや高くなる程度であるのに対し、違いが多いときには全体的にエラー訂正が行われなくなって殆ど再生できなくなるような状態となる。すなわち、例えばＣ１エンコーダについて見ると、誤り訂正能力を示す指標であるいわゆるディスタンスが９であるため、最大４バイトまでのエラー検出訂正が行え、消失（イレージャ）ポインタがあれば最大８バイトまでの訂正が可能であることから、違いが５箇所以上あると、Ｃ１符号では常に訂正不可又は誤訂正となる。違いが４箇所の場合は、他に１バイトでもエラーが生じると訂正不可という微妙な状態となる。違いが３、２、１箇所と減少するにつれて、誤り訂正できる確率が増えてゆく。これを利用すれば、オーディオやビデオのソフトを提供する場合等に、ある程度は再生できるが完璧ではなく時々乱れる、といった再生状態を積極的に作り出すことができ、該ソフトの概要だけを知らせる用途等に使用することができる。

【００３８】

この場合、予めインバータの変更を行う場所を例えば２箇所程度規定しておく方法と、変更箇所を鍵情報に応じてランダムに選び、最低個数を２箇所程度に制限する方法と、これらを複合する方法とが挙げられる。

【００３９】

さらに、インバータの挿入あるいは変更位置としては、図１０の再配列回路５７の位置に限定されず、例えばＣ１エンコーダ５２の前段や後段等の他の位置やこれらの位置を組み合わせるようにしてもよい。複数の位置の場合に、異なる鍵を用いるようにしてもよい。また、インバータを用いる以外に、ビット加算や種々の論理演算を用いるようにしてもよい。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【００４０】

ここで、図１１は、上記誤り訂正符号化回路１６の他の具体例として、再配列回路５７内のインバータ部５７ａの後段の位置に排他的論理和（ExOR）回路群６１を挿入し、Ｃ１エンコーダ５２の前段すなわち入力側の位置にもExOR回路群６６を挿入した例を示している。

【００４１】

具体的に、ExOR回路群６１は、Ｃ１エンコーダ５２から遅延回路５６、及び上記再配列回路５７のインバータ部５７ａを介して取り出される１７０バイトのデータ、すなわち情報データ$C1_{170n+169}$～$C1_{170n+22}$及びパリティデータ$P1_{170n+21}$～$P1_{170n+14}$、$Q1_{170n+13}$～$Q1_{170n}$のデータに対して排他的論理和（ExOR）回路を用いたデータ変換を行い、ExOR回路群６６は、１４８バイトの入力データB_{148n}～$B_{148n+147}$に対して排他的論理和（ExOR）回路を用いたデータ変換を行う。これらのExOR回路群６１、６６に用いられるExOR回路は、１バイトすなわち８ビットの入力データと１ビットの制御データで指示される所定の８ビットデータとの排他的論理和（ExOR）をそれぞれとるような８ビットExOR回路であり、このような８ビットExOR回路（所定の８ビットデータがオール１の場合はインバータ回路に相当する）が、ExOR回路群６１では１７０個、ExOR回路群６６では１４８個用いられている。

【００４２】

この図１１においては、１７０ビットの鍵情報が端子６２に供給され、いわゆるＤラッチ回路６３を介してExOR回路群６１内の１７０個の各ExOR回路にそれぞれ供給されている。Ｄラッチ回路６３は、イネーブル端子６４に供給された１ビットの暗号化制御信号に応じて、端子６２からの１７０ビットの鍵情報をそのままExOR回路群６１に送るか、オールゼロ、すなわち１７０ビットの全てを“０”とするかが切換制御される。ExOR回路群６１の１７０個の各ExOR回路の内、Ｄラッチ回路６３から“０”が送られたExOR回路は、再配列

回路５７内のインバータ部５７ａからのデータをそのまま出力し、Ｄラッチ回路６３から“１”が送られたExOR回路は、再配列回路５７内のインバータ部５７ａからのデータを反転して出力する。オールゼロのときには、再配列回路５７内のインバータ部５７ａからのデータをそのまま出力することになる。また、ExOR回路群６６については、１４８個のExOR回路を有し、鍵情報が１４８ビットであること以外は、上記ExOR回路群６１の場合と同様であり、端子６７に供給された１４８ビットの鍵情報がＤラッチ回路６８を介してExOR回路群６６内の１４８個のExOR回路にそれぞれ送られると共に、Ｄラッチ回路６８はイネーブル端子６９の暗号化制御信号により１４８ビットの鍵情報かオールゼロかが切換制御される。

【００４３】

この図１１の例において、ExOR回路群６１は、Ｃ１エンコーダ５２から遅延回路５６、インバータ部５７ａを介して取り出される１７０バイトのデータとしての情報データ$C1_{170n+169}$～$C1_{170n+22}$及びパリティデータ$P1_{170n+21}$～$P1_{170n+14}$、$Q1_{170n+13}$～$Q1_{170n}$のデータに対して排他的論理和（ExOR）回路を用いたデータ変換を行っているが、パリティデータについてはデータ変換を行わず、残り１４８バイトの情報データ$C1_{170n+169}$～$C1_{170n+22}$に対して、１４８ビットの鍵情報に応じたデータ変換を行わせるようにしてもよい。

【００４４】

この図１１の回路においても、上記図１０の場合と同様な作用効果が得られることは勿論である。また、ExOR回路群６１、６６のいずれか一方のみを使用するようにしたり、いずれか一方あるいは双方の選択も暗号化の鍵として用いるようにすることもできる。

【００４５】

なお、上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダあるいは媒体製造装置の固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。

【００４６】

なお、上記データ変換手段としてのExOR回路群６１、６６の代わりに、ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路群等を使用してもよい。また、８ビット単位で１ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、８ビットの情報データに対して８ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの１ワードに相当する８ビットの内の各ビットに対してそれぞれＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路を組み合わせて使用してもよい。この場合には、例えば１４８バイトすなわち１４８×８ビットのデータに対して、１４８×８ビットの鍵データが用いられることになり、さらにＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【００４７】

次に、図１の変調回路１７での暗号化処理について、図１２を参照しながら説明する。この図１２において、入力端子７１には、上記誤り訂正符号化回路１６からのデータが８ビット（１バイト）毎に供給され、入力端子７２には８ビットの鍵情報が供給されており、これらの８ビットデータは、論理演算回路の一例としてのExOR回路７３に送られて排他的論理和がとられる。このExOR回路７３からの８ビット出力が、所定の変調方式の変調器、例えば８－１６変換回路７４に送られて、１６チャンネルビットに変換される。この８－１６変換回路７４での８－１６変調方式の一例としてはいわゆるＥＦＭプラス変調方式が挙げられる。

【００４８】

この図１２の例では、データ変調の前に８ビットの鍵情報を用いた暗号化処理を施しているが、鍵情報のビット数は８ビットに限定されず、また、８－１６変調の際の変換テーブルの入出力の対応関係を鍵情報に応じて変化させるようにしてもよい。鍵情報には、上述した媒体固有の識別情報等を使用できることは勿論である。

【００４９】

次に、同期付加回路１８について説明する。

同期付加回路１８では、例えば図１３に示すような４種類の同期ワードＳ０～Ｓ３を用いて、上記８－１６変調のフレーム単位で同期をとっている。この８－１６変調フレーム（例えばＥＦＭプラスフレーム）は、例えば８５データシンボルである１３６０チャンネルビットから成り、この１フレーム１３６０チャンネルビット毎に３２チャンネルビットの同期ワードが付加されると共に、このフレームを上記Ｃ１符号やＣ２符号に対応させて構造化し、Ｃ１符号系列の先頭フレームの同期ワードと他のフレームの同期ワードを異ならせる等して、上記４種類の同期ワードＳ０～Ｓ３を使い分けている。これらの同期ワードＳ０～Ｓ３は、直前のワードの“１”、“０”の状態やいわゆるデジタルサムあるいは直流値等に応じてそれぞれ２つの同期パターンａ、ｂを有している。

【００５０】

このような４種類の同期ワードＳ０～Ｓ３の選択を、例えば図１４に示すような回路を用いて、２ビットの鍵情報７５に応じて変更することにより、暗号化が行える。すなわち、上記４種類の同期ワードＳ０～Ｓ３を指定する２ビットデータ７６の各ビットと、上記２ビットの鍵情報７５の各ビットとが、２つのExOR回路７７、７８によりそれぞれ排他的論理和され、新たな同期ワード指定データ７９となる。これにより、上記フレーム構造における同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が変更され、暗号化がなされることになる。

【００５１】

なお、同期ワードの種類数をさらに増やしてそれらの内から４種類の同期ワードを取り出す取り出し方を暗号化の鍵により決定するようにしてもよい。この鍵情報としては、上述した媒体固有の識別情報等が使用できる。

【００５２】

次に図１５は、記録媒体の一例としての光ディスク等のディスク状記録媒体１０１を示している。このディスク状記録媒体１０１は、中央にセンタ孔１０２を有しており、このディスク状記録媒体１０１の内周から外周に向かって、プログラム管理領域であるＴＯＣ（table of contents ）領域となるリードイン（lead in ）領域１０３と、プログラムデータが記録されたプログラム領域１０４と、プログラム終了領域、いわゆるリードアウト（lead out）領域１０５とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域１０４にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域１０３で管理される。

【００５３】

当該図１５の記録媒体１０１において、前記鍵格納場所情報は、リードイン領域１０３に、ＴＯＣ情報の一部として記録される。再生時には、上記鍵格納場所情報を読み出し、この読み出した鍵格納場所情報に基づいて、前記暗号化を復号するための鍵情報を取り出すようにする。

【００５４】

なお、上記鍵格納場所情報にて格納場所が指示される鍵情報の当該格納場所については後述する。

【００５５】

次に、上記ディスク状記録媒体１０１からデータを再生する再生装置について、図１６を用いて説明する。

【００５６】

図１６において、上記ディスク状記録媒体１０１は、スピンドルモータ２１１により回転駆動され、光学ピックアップ装置等の再生ヘッド装置２１２により当該記録媒体１０１の

記録内容が読み取られる。

【００５７】

再生ヘッド装置２１２により読み取られた信号は、２値化回路２１３にて２値のディジタルデータに変換され、ディジタル信号処理回路２２０に送られる。また、上記２値化回路２１３にて２値に変換されたディジタルデータのうち、ＴＯＣ領域から読み出されたデータは、ＴＯＣデコーダ２１９に送られてデコード処理され、このデコード処理により得られるＴＯＣ情報がＣＰＵ２２４に送られる。

【００５８】

当該ＣＰＵ２２４は、上記ＴＯＣデコーダ２１９からのデータより、前記鍵格納場所情報を取り出す。ＣＰＵ２２４は、当該鍵格納場所情報に基づいて、鍵情報を後述するようにして取り出し、この鍵情報をディジタル信号処理回路２２０の複数の暗号鍵情報蓄積回路２２２_{1}～２２２_{N}に蓄積させる。

【００５９】

ディジタル信号処理回路２２０は、複数の復号器２２１_{1}～２２１_{N}と複数の暗号鍵情報蓄積回路２２２_{1}～２２２_{N}を有してなるものであり、各復号器２２１_{1}～２２１_{N}は、上記図１の構成のセクタ化回路１３～同期付加回路１８までの構成に対応する逆処理を行うものである。すなわち、前述したように、これら回路１３～１８の少なくとも１つ、好ましくは２以上で、鍵情報を用いた暗号化処理が施されたときに、当該ディジタル信号処理回路２２０では、これら回路１３～１８のうち暗号化処理に関わった回路に対応する復号器に対して、それぞれ暗号鍵情報蓄積回路２２２_{1}～２２２_{N}に蓄積した鍵情報を用いて当該暗号化を解くようにする。

【００６０】

より具体的に説明すると、ディジタル信号処理回路２２０は、図１７に示すような構成を復号器２２１_{1}～２２１_{N}に対応して設けてなるものであり、この図１７の端子１１３に上記２値化回路２１３からの出力データが供給される。この図１７において、同期分離回路１１４では、上記図１の同期付加回路１８で付加された同期信号の分離が行われる。同期分離回路１１４からのディジタル信号は、復調回路１１５に送られて、上記図１の変調回路１７の変調を復調する処理が行われる。具体的には、１６チャンネルビットを８ビットのデータに変換するような処理である。復調回路１１５からのディジタルデータは、誤り訂正復号化回路１１６に送られて、図１の誤り訂正符号化回路１６での符号化の逆処理としての復号化処理が施される。以下、セクタ分解回路１１７によりセクタに分解され、ヘッダ分離回路１１８により各セクタの先頭部分のヘッダが分離される。これらのセクタ分解回路１１７及びヘッダ分離回路１１８は、上記図１のセクタ化回路１３及びヘッダ付加回路１５に対応するものである。次に、デスクランブル処理回路１１９により、上記図１のスクランブル処理回路１４におけるスクランブル処理の逆処理としてのデスクランブル処理が施され、この出力データが端子１２０から出力されて、図１６の出力端子２２３に送られる。

【００６１】

ここで、前述したように、記録時に図１のセクタ化回路１３にて暗号化処理が施されている場合には、セクタ分解回路１１７にて暗号化の際の鍵情報を用いた暗号の復号化処理が行われ、以下同様に、図１のスクランブル処理回路１４での暗号化処理に対応してデスクランブル処理回路１１９での暗号復号化処理が、図１のヘッダ付加回路１５での暗号化処理に対応してヘッダ分離回路１１８での暗号復号化処理が、図１の誤り訂正符号化回路１６での暗号化処理に対応して誤り訂正復号化回路１１６での暗号復号化処理が、図１の変調回路１７での暗号化処理に対応して復調回路１１５での暗号復号化処理が、さらに図１の同期付加回路１８での暗号化処理に対応して同期分離回路１１４での暗号復号化処理が、それぞれ行われるようになっている。

【００６２】

ところで、本発明の再生装置のＣＰＵ２２４は、上述したように、上記ＴＯＣデコーダ２１９から供給された鍵格納場所情報に基づいて、実際に鍵情報が格納されている位置を求

め、当該鍵格納場所情報に対応する場所に格納されている鍵情報を取り出し、当該取り出した鍵情報を、上記各復号器２２１$_1$～２２１$_N$に対応する暗号鍵情報蓄積回路２２２$_1$～２２２$_N$に蓄積させ、当該蓄積した鍵情報を用いて上記復号処理を行うようにしている。

【００６３】

このようなことを行うため、本発明では、図１８に示すようなデータ構造の鍵格納場所情報ＫＰ$_1$～ＫＰ$_N$を、ディジタル信号処理回路２２０内のそれぞれの復号器２１$_1$～２２１$_N$毎に用意し、当該鍵格納場所情報ＫＰ$_1$～ＫＰ$_N$が前記記録媒体１０１のＴＯＣ領域に配置されている。

【００６４】

ここで、上記各鍵格納場所情報ＫＰ$_1$～ＫＰ$_N$は、この図１８に示すように、セクタアドレス情報とオフセット情報とバイト数情報と属性情報とからなるものである。すなわち、これら各鍵格納場所情報ＫＰ$_1$～ＫＰ$_N$は、ある復号器で暗号化を解くために必要な暗号鍵情報ＣＫが、セクタアドレス情報にて示されるセクタ内において、オフセット情報にて示される位置（先頭バイトからオフセット情報にて示される位置のバイト）からバイト数情報にて示される長さのバイト分に納められていることを示している。なお、属性情報としては、復号器２２１$_1$～２２１$_N$の使用の有無や、その他の情報を納めることができる。

【００６５】

次に、上記鍵格納場所情報テーブルを用いた場合の図１６の再生装置における復号処理の流れを以下に説明する。

【００６６】

図１６の再生装置は、ディスク状記録媒体１０１が交換される度に、全ての復号器２２１$_1$～２２１$_N$，暗号化鍵情報蓄積装置２２２$_1$～２２２$_N$をリセットすると共に、ディスク状記録媒体１０１の全セクタアドレスをアクセス可能なモードに設定する。

【００６７】

次に、再生装置は、ディスク状記録媒体１０１のＴＯＣ領域から上記鍵格納場所情報ＫＰ$_1$～ＫＰ$_N$を読み出し、これら鍵格納場所情報ＫＰ$_1$～ＫＰ$_N$において各々の復号器２２１$_1$～２２１$_N$のエントリに示された属性情報により、該当する復号器の使用の有無を判断する。ここで、もしもその復号器が使用される場合には、鍵格納場所としてセクタアドレス情報に示されているセクタの内容を読み出して（特殊なアドレスが書かれている場合については後述する）、さらにこのセクタから上記オフセット情報とバイト数情報にて示される範囲の情報を読み出して暗号鍵情報を取り出した後、その暗号鍵情報を暗号鍵情報蓄積手段２２２に蓄積すると共に復号器２２１にセットして暗号化を解く（すなわち平文化する）ための準備を完了する。これをすべての復号器２２１$_1$～２２１$_N$について繰り返す。

【００６８】

その後、再生装置は、ユーザのアクセス領域制限モードに移行する。

【００６９】

次に、再生装置はユーザのコマンドを受け付け、これに応じてユーザデータを読み出し、当該ユーザデータに施されている暗号化を上記暗号鍵情報蓄積手段２２２に蓄積した暗号鍵情報に基づいて解く。

【００７０】

以下に、上記鍵情報とその格納場所、及び鍵格納場所情報について説明する。

【００７１】

ここで、セクタアドレス情報にて示されるセクタアドレスとしては、ディスク状記録媒体１０１上の全てのセクタを対象にできるので、例えばセクタアドレス情報が４バイトの２の補数形式で表されているとし、例えばＴＯＣ領域のようなシステムで使用する領域が（０ｆｆｆｆｆｆｆｆｈ）にあるとしたとき、その中に収められている本来は別の目的、例えば製造履歴の記録などに利用するために書き込まれている認識情報を暗号鍵情報として指定することができることになる。例えば、製造履歴情報がＴＯＣ領域のセクタ内の先頭から１６０バイト目の１６バイト分に記録されているとしたとき、オフセット情報＝１６０バイト目とし、バイト数情報＝１６バイトとすれば、これらにより上記製造履歴の認識

情報を指定することができる。

【００７２】

また、例えば、セクタアドレスとして（０ｆｆｆｆｆｆｆ０ｈ）のような負の値を設定して、ユーザがアクセス不可能な領域（この場合、例えばリードインエリア等）に書かれた暗号鍵情報を指定することで、暗号鍵をユーザから隠すことができるようになる。

【００７３】

さらに例えば上記ディスク状記録媒体１０１が複数の記録層を持つものであるとしたとき、当該記録媒体１０１上のデータ記録層とは別の記録層のセクタアドレスが例えば（７ｆｆｆｆｆｆｆｈ）から減少していくように定められているような場合において、セクタアドレス情報として（７ｆｆｆｆｆｆｆｈ）を指定することで、当該記録媒体１０１上のデータ記録層とは別の記録層の最初のセクタに収められた暗号鍵情報を指定することができる。

【００７４】

また、セクタアドレス情報に特殊なアドレスが書かれている例として、ディスク状記録媒体１０１上に存在しないセクタアドレスの番号、例えば（９０００００００ｈ）から（０ｅｆｆｆｆｆｆｈ）等を下記に挙げるような情報それぞれに割り当てることにより、セクタアドレスという統一的な表現で種々の情報を暗号鍵情報として取り扱うことができる。

【００７５】

この場合は、通常のセクタから鍵情報を読み出す構成の代わりに、媒体上の別の記録形式、例えはバーコード，ウォブリング，紫外線等で書かれた情報や、図１６に示す装置内のＥＥＰＲＯＭ２２５などに記録されている記録／再生装置固有の識別情報や装置の出荷先の地域を表す仕向け情報（Regional Code） や、装置に接続若しくは内蔵されているＩＣカードやいわゆるＰＣＭＣＩＡ(Personal Computer Memory Card International Association) などの情報蓄積装置２２６に蓄積された情報や、通信インターフェイス２２７を介するモデム／ＬＡＮなどの通信装置から供給される情報や、キーボード２２８やリモコン送信装置２３２からリモコン受信手段２２９により受信した外部装置から供給される情報等を、識別情報として取り出すようにする。

【００７６】

ここで、例えば鍵格納場所情報を読み出したとき、例えばディスク状記録媒体１０１の盤面上に記録されたバーコードＢＣに収められた情報を鍵情報とすることが、上記特殊なセクタアドレス（９０００００００ｈ）としてセクタアドレス情報に指定されていた場合、通常の読み出し装置とは独立に設けられているバーコード読み取り装置２１０を動作させ、この読み取り装置２１０からの情報をバーコード解読装置２３３にて解読し、この解読した情報をＣＰＵ２２４に送るようにすれば、上述同様に鍵情報を復号器に設定することができる。

【００７７】

なお、キーボード２２８やリモコン送信装置２３２及びリモコン受信手段２２９のような人と対話的に入力を行うような装置が、暗号鍵格納場所として指定されたときには、装置に内蔵または接続された表示回路２３０及びディスプレイ装置２３１などを使って、上記操作する人に対して暗号鍵の入力を促す工程が、鍵情報の読み取り工程の手前に必要となる。

【００７８】

このような特殊セクタアドレスを使う場合には、鍵格納場所情報のオフセット情報やバイト数情報に対しては、それぞれの情報や装置固有の意味を持たせることにより、装置間の相違点を吸収することができる。例えば、暗号鍵情報をモデムから読み込むような指定が行われた場合、暗号鍵情報の配布会社の電話番号の指定に、オフセット情報を使う例が考えられる。

【００７９】

また、暗号鍵情報を用いて暗号化を解く場合の他の例としては、セクタ単位で復号できる復号器Ａと、媒体単位で復号できる復号器Ｂがあった場合、例えば上記セクタ単位の復号

器Ａにて暗号鍵を読み出した後、当該復号器Ａに暗号鍵を設定する動作を復号器Ｂの暗号鍵を取り出す動作の前に行うことにより、復号器Ｂの暗号鍵の隠匿性をより増すことができる。

【００８０】

なお、上述の説明では、記録装置で複数の暗号化処理を行い、それに対応して再生装置に複数の復号器を設ける例を挙げているが、本発明は基本的には一つの暗号化処理とそれに対応する一つの復号器を設けるものであっても適用できることは言うまでもない。

【００８１】

上述したように、本発明の上記構成例によれば、暗号鍵情報の配置場所をその装置の持つ復号器に応じて用意（必要ならば複数用意）し、それぞれに配置場所を指し示すポインタ（鍵格納場所情報）を媒体上に記録することにより、暗号鍵情報の配置場所を媒体上の任意の位置に柔軟に指定することが可能となり、例えばユーザアクセス不能な場所を指定することにより暗号鍵情報の隠匿性を高めることができる。また、すでに物理フォーマットで規定されている任意の認識情報を指定したり、媒体の物理的特徴（例えば記録面を複数もつ媒体の別の記録層）を指定することにより、不法な複製に対する抑止力を高めたり、複数の暗号鍵を一つのセクタ内に一まとめにしておけるので、多数の暗号鍵に対して高速アクセスが可能となる。

【００８２】

また、鍵格納場所情報の指す鍵情報は、媒体上の通常の読み出し手段で読み出されるデータ領域のみならず、別の記録方法で媒体上に記録された情報を指定することも可能である。さらに、鍵格納場所情報が指す鍵情報は、媒体上のみならず、記録再生装置に付随する論理デバイスも指定できるので、記録再生装置の内部情報（認識番号など）を指定したり外部装置からの暗号鍵の入力にも対応できる。

【００８３】

また、鍵情報の組み合わせは、媒体の原盤毎に変更可能なので、再生装置におけるそれぞれの復号器の特性を生かして、鍵情報の一部分しか使わないなど、原盤作製者の意向にそった媒体の作製が容易に行える。

【００８４】

もちろんこの配置方法は、一般的な暗号化手法の鍵情報配置においても応用可能であることは言うまでもない。

【００８５】

次に、図１７の各構成要素における暗号復号化処理について、説明する。

【００８６】

先ず、図１７の同期分離回路１１４での暗号復号化処理は、上記図１３や図１４と共に説明したように、複数種類、例えば４種類の同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が鍵情報に応じて変更され、暗号化がなされたものを、鍵情報に応じて検出することで行われる。

【００８７】

次に、復調回路１１５での暗号復号化処理は、図１９に示すように、同期分離回路１１４から１６－８変換回路１３１に送られて１６チャンネルビットが８ビットデータに変換されたものを、上記図１２のExOR回路７３に対応するExOR回路１３２に送り、端子１３３からの８ビットの鍵情報との排他的論理和をとることで、図１２の入力端子７１に供給された８ビットデータに相当するデータが復元され、これが誤り訂正復号化回路１１６に送られる。

【００８８】

次に、誤り訂正復号化回路１１６では、例えば上記図１０の誤り訂正符号化処理の逆処理が、図２０の構成により行われる。

【００８９】

この図２０において、上記復調回路１１５にて復調されたデータの１７０バイトあるいは１７０シンボルを１まとまりとして、インバータ部１７２ａを有する再配列回路１４２を

介し、遅延回路１４３を介して第１の復号器であるＣ１デコーダ１４４に送られている。このＣ１デコーダ１４４に供給される１７０バイトのデータの内２２バイトがＰ，Ｑパリティであり、Ｃ１デコーダ１４４では、これらのパリティデータを用いた誤り訂正復号化が施される。Ｃ１デコーダ１４４からは、１７０バイトのデータが出力されて、遅延回路１４５を介して第２の復号器であるＣ２デコーダ１４６に送られ、パリティデータを用いた誤り訂正復号化が施された後、さらに遅延回路１４７を介して第３の復号器であるＣ３デコーダ１４８に送られる。ここで、遅延回路１４７及びＣ３デコーダ１４８は、上記遅延回路１４３及びＣ１デコーダ１４４と同様のものであり、この遅延回路とＣ１デコーダの組を複数組設けるようにしてもよい。このＣ３デコーダ１４８で最終的な誤り訂正復号化が施され、パリティ無しの１４８バイトのデータが取り出される。この１４８バイトのデータは、上記図１０のＣ１エンコーダ５２に入力される１４８バイトのデータに相当するものである。

【００９０】

そして、図１０の誤り訂正符号化回路の再配列回路５７内のインバータ部５７ａで、インバータの有無による暗号化が施されている場合には、図２０の誤り訂正復号化回路の再配列回路１４２内のインバータ部１４２ａにて、対応する暗号復号化を行うことが必要とされる。この他、図１０と共に説明した各種暗号化処理に対応して、その暗号化を解くための逆処理となる暗号復号化が必要とされることは勿論である。

【００９１】

ここで、図２１は、上記図１１の誤り訂正符号化回路の具体的構成に対応する誤り訂正復号化回路の具体的な構成を示す図である。

【００９２】

この図２１において、上記図１１の再配列回路５７内のインバータ部５７ａの出力側に挿入されたExOR回路群６１に対応して、再配列回路１４２のインバータ部１４２ａの入力側及び遅延回路１４３の入力側の位置に、ExOR回路群１５１が挿入され、図１１のＣ１エンコーダ５２の入力側に挿入されたExOR回路群６６に対応して、Ｃ３デコーダ１４８の出力側にExOR回路群１５６が挿入されている。

【００９３】

これらのExOR回路群１５１、１５６は、上述したように、図１１のExOR回路群６１、６６によるデータ変換をそれぞれ復号化するためのデータ変換を施すものであり、ExOR回路群１５１は、例えば１７０個の８ビットExOR回路により、またExOR回路群１５６は、１４８個の８ビットExOR回路によりそれぞれ構成されている。なお、記録側の図１１の誤り訂正符号化回路のExOR回路群６１で、パリティデータを除く１４８バイトの情報データに対して鍵情報に応じたデータ変換が施されている場合には、ExOR回路群１５１は１４８個の８ビットExOR回路により構成されることは勿論である。

【００９４】

この図２１の端子１５２には、図１１の端子６２に供給される鍵情報に相当する１７０ビットの鍵情報が供給され、いわゆるＤラッチ回路１５３を介してExOR回路群１５１内の１７０個の各ExOR回路にそれぞれ供給されている。Ｄラッチ回路１５３は、イネーブル端子１５４に供給された１ビットの暗号化制御信号に応じて、端子１５２からの１７０ビットの鍵情報をそのままExOR回路群１５１に送るか、オールゼロ、すなわち１７０ビットの全てを“０”とするかが切換制御される。また、ExOR回路群１５６については、１４８個のExOR回路を有し、鍵情報が図１１の端子６７に供給される鍵情報と同様の１４８ビットであること以外は、上記ExOR回路群１５１の場合と同様であり、端子１５７に供給された１４８ビットの鍵情報がＤラッチ回路１５８を介してExOR回路群１５６内の１４８個のExOR回路にそれぞれ送られると共に、Ｄラッチ回路１５８はイネーブル端子１５９の暗号化制御信号により１４８ビットの鍵情報かオールゼロとするかが切換制御される。

【００９５】

このように、誤り訂正回路のインバータやExOR回路等を暗号化の鍵として使うことにより、簡易で大きな暗号化が実現できる。また、このインバータ等の数を制御することにより

、絶対再生不可能な暗号化レベルのデータとか、エラー状態が悪くなると再生不可能となるデータとか、セキュリティレベルの要求に応じて対応できる。すなわち、インバータやExOR回路等の個数をコントロールすることにより、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、また、エラー訂正のみでは回復不可能な絶対再生不可能状態を形成することもできる。また、暗号化の鍵としては、上記図示の例のように１箇所当たり百数十ビットもの大きなビット数となり、鍵のビット数の大きな暗号化ができるため、データセキュリティが向上する。しかも、このようなエラー訂正符号化回路やエラー訂正復号化回路を、いわゆるＬＳＩやＩＣチップのハードウェア内で実現することにより、一般ユーザからはアクセスが困難であり、この点でもデータセキュリティが高いものとなっている。

【００９６】

次に、セクタ分解回路１１７においては、上記図２、図３と共に説明したように、記録時に上記セクタ化回路１３で偶数・奇数バイトのインターリーブによる暗号化が施されている場合に、この偶奇インターリーブを解くような逆の処理、いわゆるデインターリーブ処理を施すものである。

【００９７】

また、ヘッダ分離回路１１８においては、記録時に、上記ヘッダ付加回路１５において、上記図７～図９と共に説明したような暗号化処理、すなわちセクタ同期となるデータシンクのバイトパターンの転置や、アドレス、ＣＲＣの変更がなされている場合に、これを復元するような暗号復号化処理を施すものである。

【００９８】

次に、図２２は、デスクランブル処理回路１１９の具体例を示しており、端子１６１には、図１７のヘッダ分離回路１１８からのディジタルデータが供給されている。この端子１６１からのディジタルデータは、例えば上記図４に示すような構成を有するスクランブラ１６３でデスクランブル処理され、出力端子１６４より取り出される。このスクランブラ１６３についての、上記図４と共に説明したような生成多項式１６５及びプリセット値（あるいは初期値）１６６を、認証機構１７１からの暗号の鍵情報に応じて変化させることにより、暗号復号化を行うことができる。この認証機構１７１では、上記ヘッダ情報１６７のコピー情報４６の内容や、媒体固有のあるいは再生装置固有の固有識別情報１７２や、製造者、販売者等の共通識別情報１７３や、外部から与えられる外部識別情報１７４等により、暗号の鍵情報を生成し、この鍵情報に応じて生成多項式１６５やプリセット値１６６を制御する。

【００９９】

これらの各回路１１４～１１９のいずれで暗号復号化処理が必要とされるかの情報も、暗号の鍵情報となることは前述した通りである。また、暗号の鍵情報を所定周期、例えばセクタ周期で切り換えることができ、この切換を行うか否かや、切換周期等も鍵とすることにより、暗号化の難易度が高められる。

【０１００】

次に、本発明の第２の実施の形態について説明する。

この第２の実施の形態は、上述した第１の実施の形態の構成を部分的に変更したものであり、全体の基本構成は、前述した図１に示す通りである。この図１の構成の各回路１３～１８の内の変更部分について以下説明する。

【０１０１】

図１のセクタ化回路１３は前述した第１の実施の形態と同様に構成すればよいが、スクランブル処理回路１４については、図２３に示す構成を用いている。

【０１０２】

この図２３に示すスクランブル処理回路１４において、データ入力用の端子３５には、ＬＳＢ（最下位ビット）が時間的に先となる順序、いわゆるＬＳＢファーストで、図１のセクタ化回路１３からのデータが入力される。スクランブル用の１５ビットのシフトレジスタ１４ａは、排他的論理和（ExOR）回路１４ｂを用いて生成多項式$x^{15}+x^{4}+1$ に従っ

たフィードバックがかけられ、１５ビットのシフトレジスタ１４ａには、図２４に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図２４のプリセット値の選択番号は、例えばセクタアドレスの下位側４ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ１４ａからの出力データと端子３５からの入力データとは、ExOR回路１４ｃにより排他的論理和がとられて、端子１４ｄより取り出され、図１のヘッダ付加回路１５に送られる。

【０１０３】

ここで、上記プリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記図２４のプリセット値テーブルの各プリセット値を、例えば１６バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND）、論理和（OR）、シフト演算等を使用できる。

【０１０４】

次に、この第２の実施の形態のセクタフォーマットとしては、例えば、図２５に示すようなものを用いている。

【０１０５】

この図２５に示すように、１セクタは、１行１７２バイトの１２行、すなわち２０６４バイトから成り、この中にメインデータ２０４８バイトを含んでいる。１２行の最初の行の先頭位置には、４バイトのＩＤ（識別データ）と、２バイトのＩＥＤ（ＩＤエラー検出符号）と、６バイトのＲＳＶ（予備）とがこの順に配置されており、最後の行の終端位置には、４バイトのＥＤＣ（エラー検出符号）が配置されている。

【０１０６】

上記ＩＤ（識別データ）の４バイトは、図２６に示すように、ＭＳＢ側の最初のバイト（ビットｂ３１～ｂ２４）はセクタ情報から成り、残りの３バイト（ビットｂ２３～ｂ０）はセクタ番号から成っている。セクタ情報は、ＭＳＢ側から順に、１ビットのセクタフォーマットタイプ、１ビットのトラッキング方法、１ビットの反射率、１ビットの予備、２ビットのエリアタイプ、２ビットの層番号の各情報から成っている。

【０１０７】

図１のヘッダ付加回路１５では、このようなセクタフォーマットにおいて、例えば上記ＩＤ（識別データ）の内のセクタ番号の２４ビットに対して、上記鍵情報に応じて例えばビット単位でのスクランブル処理である転置処理を施すことにより、暗号化を施すことができる。また、上記２バイトのＩＥＤ（ＩＤエラー検出符号）の生成多項式や、４バイトのＥＤＣ（エラー検出符号）の生成多項式等を上記鍵情報に応じて変更することによっても、あるいはこれらの情報と鍵情報とを論理演算することによっても、暗号化を施すことができる。

【０１０８】

次に、図１の誤り訂正符号化回路１６としては、図２７に示すような構成の回路が用いられる。この符号化は、図２８に示すような積符号あるいはブロック符号が用いられる。

図２７において、入力端子３１０には、前記図１のヘッダ付加回路１５からのデータが供給され、この入力データは、第１の符号化器であるＰＯエンコーダ３１１に送られる。このＰＯエンコーダ３１１への入力データは、図２８に示すように、$B_{0,0}$～$B_{191,171}$の１７２バイト×１９２行のデータであり、ＰＯエンコーダ３１１では、１７２列の各列１９２バイトのデータに対して、それぞれ１６バイトずつのリード・ソロモン（ＲＳ）符号としてのＲＳ（208,192,17）の外符号（ＰＯ）を付加している。ＰＯエンコーダ３１１からの出力データは、前述したような暗号化のためのデータ変換回路３１２を介して、インターリーブ回路３１３に送られてインターリーブ処理され、ＰＩエンコーダ３１４に送られる。このＰＩエンコーダ３１４では、図２８に示すように、上記ＰＯパリティが付加され

た１７２バイト×２０８行のデータの各行の１７２バイトのデータに対して、それぞれ１０バイトずつのＲＳ（182,172,11）の内符号（ＰＩ）を付加している。従って、このＰＩエンコーダ３１４からは、１８２バイト×２０８行のデータが出力されることになる。この出力データは、前述したような暗号化のためのデータ変換回路３１５を介して、出力端子３１６より取り出される。

【０１０９】

ここで、データ変換回路３１２については、ＰＯエンコーダ３１１が各列毎の１９２バイトの入力データに対して１６バイトのＰＯパリティを付加して２０８バイトのデータを出力することから、この１６バイトのパリティに対して、あるいは２０８バイトのデータ全体に対して、前述したようなデータ変換を行うことにより暗号化を施すことができる。このデータ変換は、前述したように、入力される鍵情報に応じて施すようにしてもよい。また、データ変換回路３１５については、ＰＩエンコーダ３１４が各行の１７２バイトのデータに対して、それぞれ１０バイトずつのＰＩパリティを付加して１８２バイトのデータを出力することから、この１０バイトのパリティに対して、あるいは１８２バイトのデータ全体に対してデータ変換を行うことにより暗号化を施すことができる。

【０１１０】

上記データ変換は、具体的には、前記図１０、図１１と共に説明したように、インバータを所定位置に配設したり、ExOR回路群により鍵情報に応じて選択的にデータを反転させたり、その他、ＡＮＤ、ＯＲ、NAND、NOR 回路群等を使用してもよい。また、８ビット単位で１ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、８ビットの情報データに対して８ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの１ワードに相当する８ビットの内の各ビットに対してそれぞれＡＮＤ、ＯＲ、ExOR、NAND、NOR 、インバート回路を組み合わせて使用してもよい。また、ＡＮＤ、ＯＲ、ExOR、NAND、NOR 、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【０１１１】

誤り訂正符号化された上記１８２バイト×２０８行のデータは、行についてインターリーブされ、１３行ずつ１６のグループに分けられて、各グループが記録セクタに対応付けられる。１セクタは、１８２バイト×１３行の２３６６バイトとなるが、これらが変調されて、図２９に示すように１行当たり２つの同期コードＳＹが付加される。変調には、前述した第１の実施の形態と同様に８－１６変換が用いられるが、１行は２つのシンクフレームに分けられ、１シンクフレームは、３２チャネルビットの同期コードＳＹと１４５６チャネルビットのデータ部とから成っている。図２９は、変調され同期付加されて得られた１セクタ分の構造を示し、この図２９に示す１セクタ分の３８６８８チャネルビットは、変調前の２４１８バイトに相当する。

【０１１２】

図２９の変調出力信号には、８種類の同期コードＳＹ０～ＳＹ７が用いられており、これらの同期コードＳＹ０～ＳＹ７は、上記８－１６変換の状態（ステート）に応じて、ステート１及び２のときが図３０の（ａ）、ステート３及び４のときが図３０の（ｂ）の同期パターンとなっている。

【０１１３】

このような８種類の同期コードＳＹ０～ＳＹ７の選択を、例えば図３１に示すような回路を用いて、３ビットの鍵情報に応じて変更することにより、暗号化が行える。すなわち、上記８種類の同期コードＳＹ０～ＳＹ７を指定する３ビットデータ３２１の各ビットと、上記３ビットの鍵情報３２２の各ビットとを、３つのExOR回路３２３，３２４，３２５によりそれぞれ排他的論理和をとることにより、新たな同期コード指定データ３２６とする。これにより、上記フレーム構造における同期コードの使い方あるいはフレーム構造内で

の各種同期コードの使用位置が変更され、暗号化がなされることになる。勿論、その３ビットに対して鍵情報に応じてデータを転置したり、置換したり、シフトレジスタにより変換したりできる。また、これは関数変換でもかまわない。

【０１１４】

以上説明した本発明の第２の実施の形態における効果も、前述した第１の実施の形態の場合と同様である。

【０１１５】

次に、上述した本発明の第２の実施の形態の記録側の構成に対して、再生側の基本構成は、前記図１７と同様であり、上記第２の実施の形態に示した各部の変更箇所に対応して変更された逆処理がそれぞれ施される。例えば、上記図２７に示す誤り訂正符号化に対する逆処理は、図３２のような構成の誤り訂正復号化回路により実現できる。

【０１１６】

すなわち、この図３２において、入力端子３３０には前記図１７の復調回路１１５からの出力信号であり、上記図２７の出力端子３１６からの出力に相当する上記図２８の積符号の１８２バイト×２０８行のデータが供給されている。この入力端子３３０からのデータは、データ逆変換回路３３１に送られて、上記図２７のデータ変換回路３１５の逆処理が行われる。データ逆変換回路３３１からの出力データは、ＰＩ（内符号）デコーダ３３２に送られて、上記図２７のＰＩエンコーダ３１４の逆処理としての復号化処理すなわちＰＩ符号を用いた誤り訂正処理が施され、上記図２８の１７２バイト×２０８行のデータとなる。ＰＩデコーダ３３２からの出力データは、デインターリーブ回路３３３で上記インターリーブ回路３１３での逆処理が施され、データ逆変換回路３３４に送られて上記図２７のデータ変換回路３１２の逆処理が行われた後、ＰＯ（外符号）デコーダ３３５に送られる。ＰＯデコーダ３３５では、上記図２７のＰＯエンコーダ３１１の逆処理としての復号化処理すなわちＰＯ符号を用いた誤り訂正処理が施され、図２８の元の１７２バイト×１９２行のデータが出力端子３３６を介して取り出される。上記図２７のデータ変換回路３１２、３１５でのデータ変換の際に鍵情報を用いる場合には、各端子３１８、３１９にそれぞれ供給した鍵情報を、図３２のデータ逆変換回路３３４、３３１の各端子３３９、３３８にそれぞれ供給して、これらの鍵情報に応じてデータ逆変換を行わせればよい。

【０１１７】

以上説明した本発明の第２の実施の形態における効果も、前述した第１の実施の形態の場合と同様である。

【０１１８】

なお、本発明は、上述した実施の形態のみに限定されるものではなく、例えば、データ変換としては、インバータやExORの例を示しているが、この他、ビット加算や、各種論理演算等によりデータ変換を行わせてもよいことは勿論である。また、暗号化の鍵情報に応じてデータを置換したり、転置したり、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

【０１１９】

【発明の効果】

本発明においては、信号記録媒体には鍵情報の場所を指示する鍵格納場所情報を記録し、信号再生の際には当該鍵格納場所情報に基づいて鍵情報を取り出すようにすることにより、鍵情報を容易に取り出せないようにしているため、不法解読や不法コピーを防止することができる。

【図面の簡単な説明】

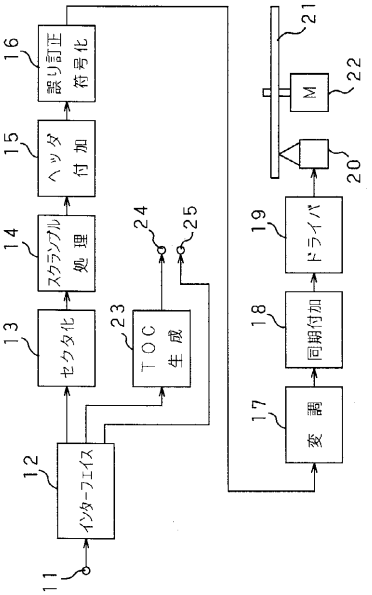
【図１】本発明の信号記録装置の一構成例を示すブロック回路図である。

【図２】セクタ化回路における偶数・奇数バイトのインターリーブを実現するための構成例を示すブロック回路図である。

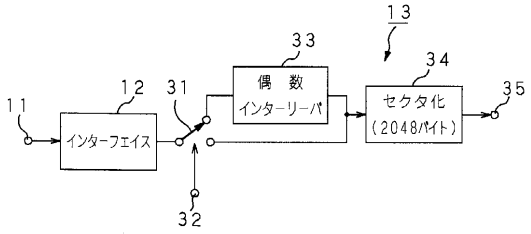
【図３】偶数・奇数バイトのインターリーブを説明するための図である。

【図４】スクランブラの一例を示す回路図である。
【図５】スクランブラのプリセット値を示す図である。
【図６】生成多項式が可変のスクランブラの一例を示す図である。
【図７】セクタフォーマットの一例を示す図である。
【図８】セクタ内の同期領域での暗号化の一例を説明するための図である。
【図９】セクタ内のヘッダ領域の一例を示す図である。
【図１０】誤り訂正符号化回路の一例を示す図である。
【図１１】誤り訂正符号化回路の他の例を示す図である。
【図１２】変調回路での暗号化処理の一例を説明するための図である。
【図１３】変調信号に付加される同期ワードの具体例を示す図である。
【図１４】同期付加回路での暗号化の一例を説明するための図である。
【図１５】データ記録媒体の一例を示す図である。
【図１６】本発明の信号再生装置の一構成例を示すブロック回路図である。
【図１７】信号再生装置のディジタル信号処理回路の具体的構成を示すブロック回路図である。
【図１８】鍵格納場所情報テーブルについて説明するための図である。
【図１９】復調回路での暗号化処理の一例を説明するための図である。
【図２０】誤り訂正復号化回路の一例を示す図である。
【図２１】誤り訂正復号化回路の他の例を示す図である。
【図２２】デスクランブル処理回路の一例を示す図である。
【図２３】スクランブラの他の例を示す図である。
【図２４】図２１のスクランブラのプリセット値の一例を示す図である。
【図２５】セクタフォーマットの他の例を示す図である。
【図２６】図２３のセクタフォーマットにおけるセクタ内のヘッダ領域の一例を示す図である。
【図２７】誤り訂正符号化回路の他の例を示すブロック図である。
【図２８】誤り訂正符号の具体例としての積符号を示す図である。
【図２９】セクタの信号フォーマットの一例を示す図である。
【図３０】変調信号に付加される同期ワードの他の具体例を示す図である。
【図３１】同期付加回路での暗号化の他の例を説明するための図である。
【図３２】誤り訂正復号化回路の他の例を示すブロック図である。
【符号の説明】
１３　セクタ化回路、　１４　スクランブル処理回路、　１５　ヘッダ付加回路、　１６　誤り訂正符号化回路、　１７　変調回路、　１８　同期付加回路、５７，１４２　再配列回路、　６１，６６，１５１，１５６　ExOR回路群、　１１４　同期分離回路、　１１５　復調回路、　１１６　誤り訂正復号化回路、１１７　セクタ分解回路、　１１８　ヘッダ分離回路、　１１９　デスクランブル処理回路、　２２０　ディジタル信号処理回路、　221_1～221_N　復号器、　222_1～222_N　暗号鍵情報蓄積回路、　２２４　ＣＰＵ

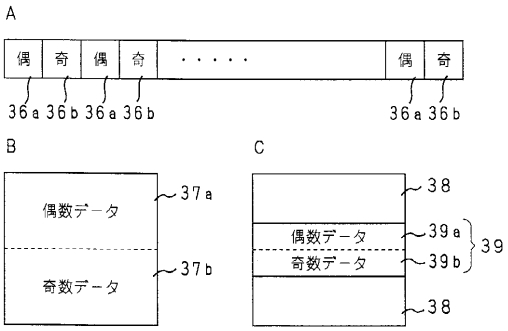
【図１】



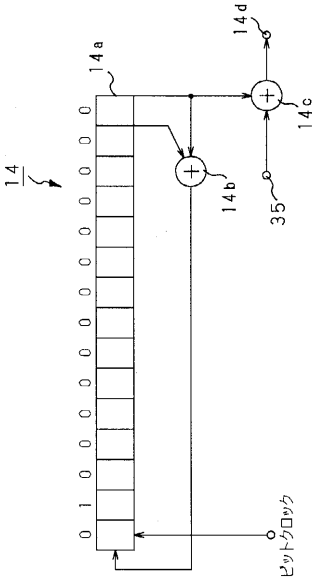
【図２】



【図３】



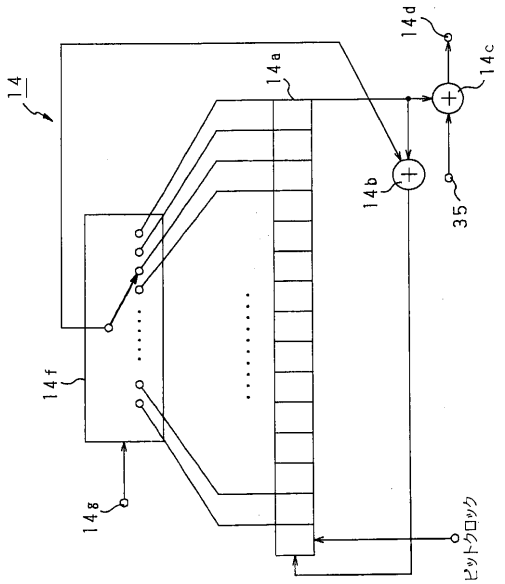
【図４】



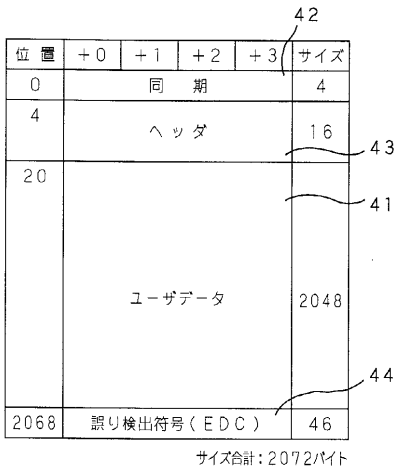
【図５】

選択番号	プリセット値	選択番号	プリセット値
0	0001h	8	4080h
1	4000h	9	2040h
2	2000h	10	1020h
3	1000h	11	0810h
4	0800h	12	0408h
5	0400h	13	0204h
6	0200h	14	0102h
7	0100h	15	4081h

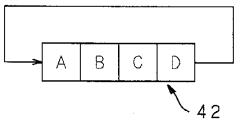
【図６】



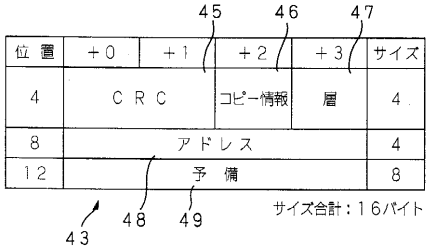
【図７】



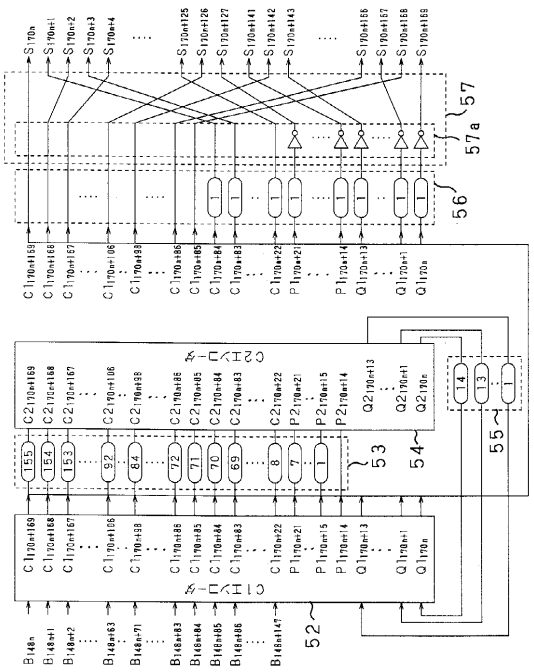
【図８】



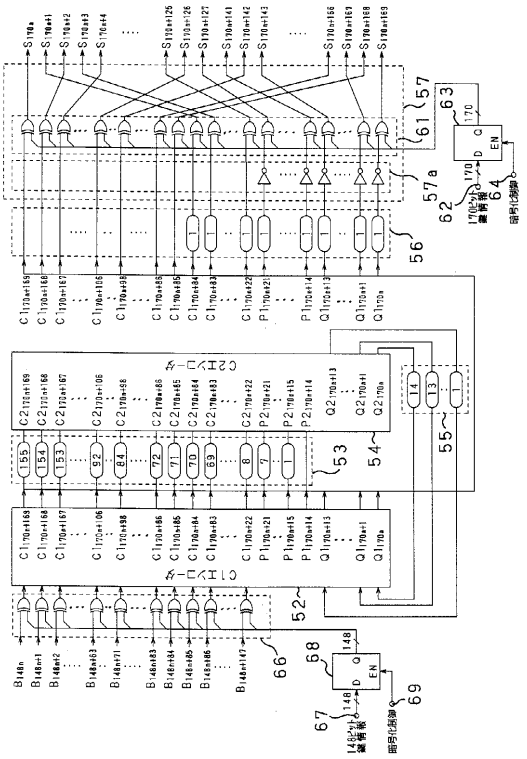
【図９】



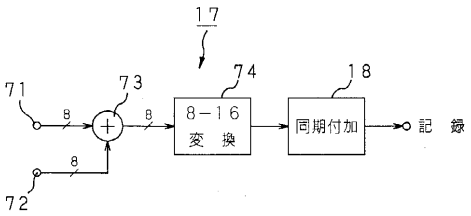
【図１０】



【図１１】



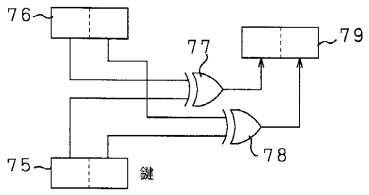
【図１２】



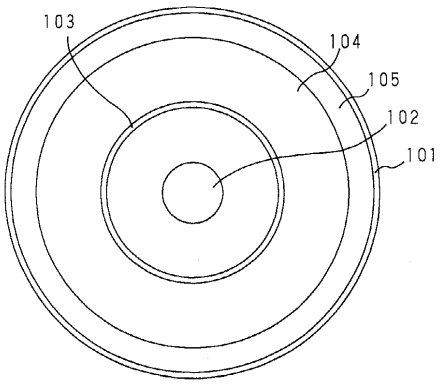
【図１３】

同期ワード	符号ワード			
	msb	同期パターンa	lsb	msb	同期パターンb	lsb
S0	00010010010000000000100000000001			10010010010000000000100000000001		
S1	00010000010000000000100000000001			10010000010000000000100000000001		
S2	00000100010000000000100000000001			10000100010000000000100000000001		
S3	00001000010000000000100000000001			10001000010000000000100000000001		

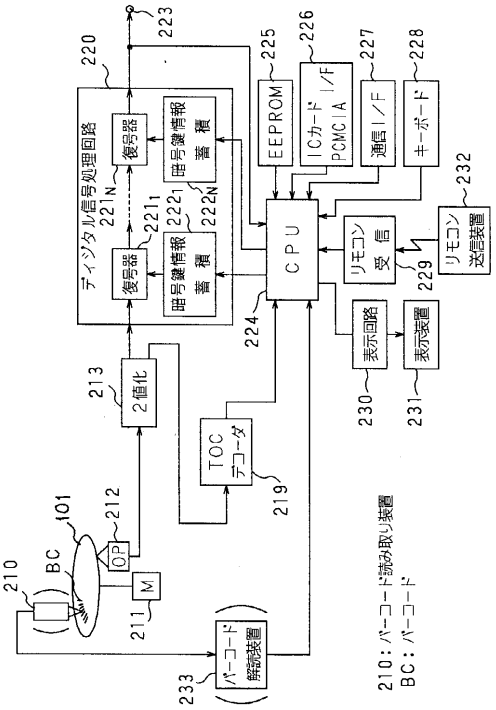
【図１４】



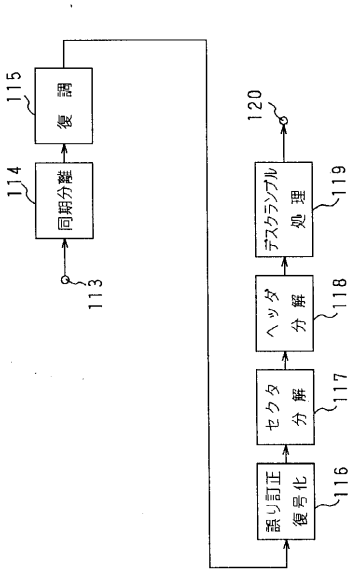
【図１５】



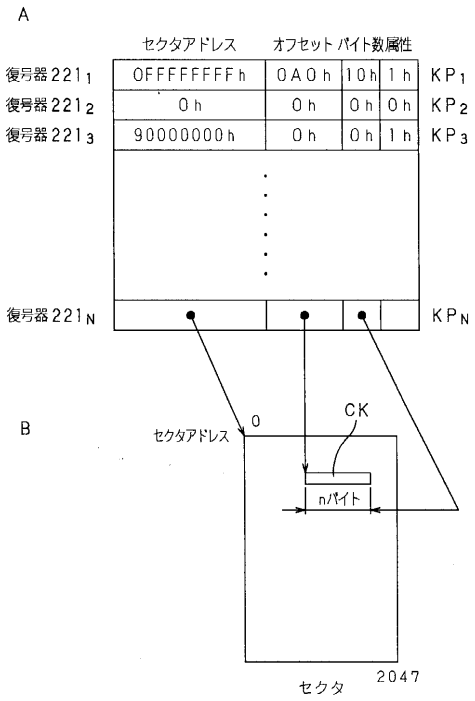
【図１６】



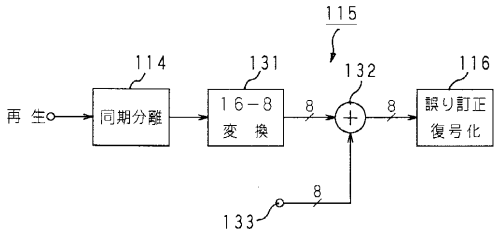
【図１７】



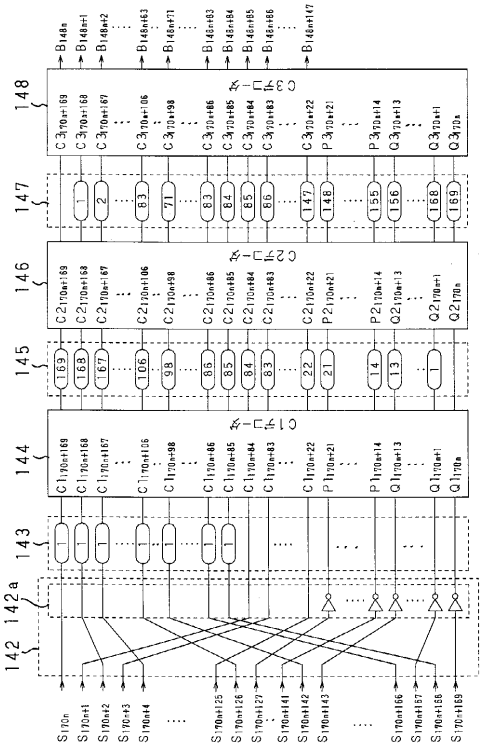
【図１８】



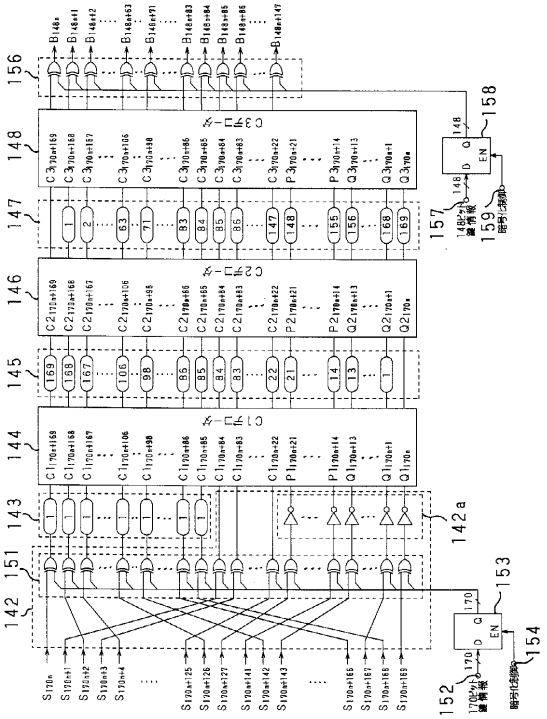
【図１９】



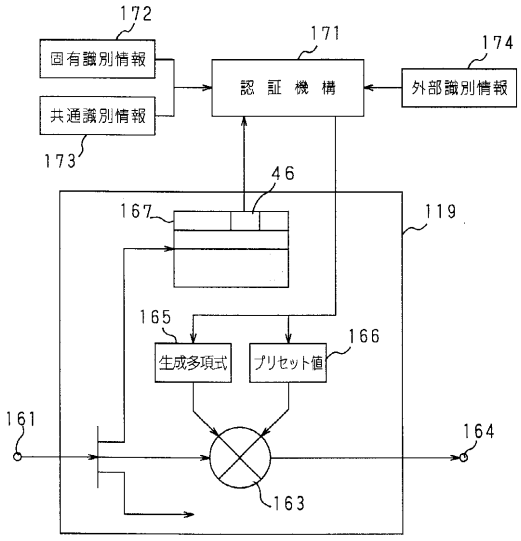
【図２０】



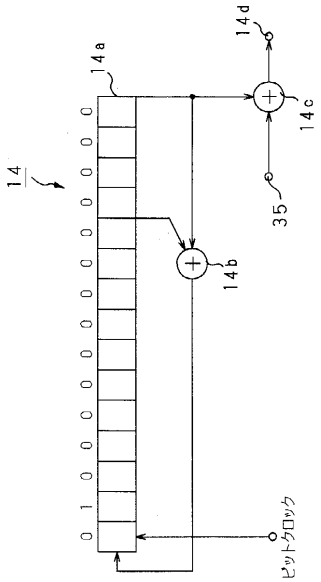
【図２１】



【図２２】



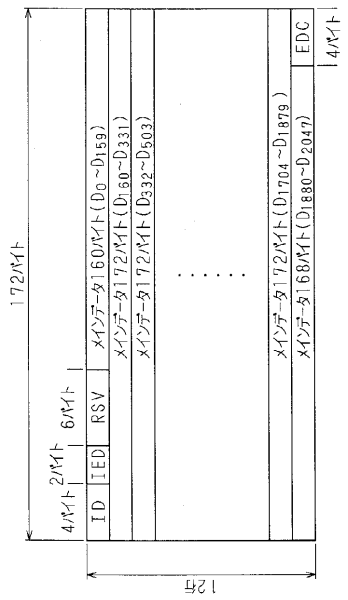
【図２３】



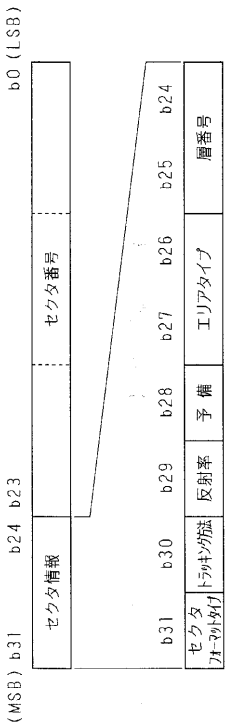
【図２４】

選択番号	プリセット値	選択番号	プリセット値
0	0001h	8	0010h
1	5500h	9	5000h
2	0002h	10	0020h
3	2A00h	11	2001h
4	0004h	12	0040h
5	5400h	13	4002h
6	0008h	14	0080h
7	2800h	15	0005h

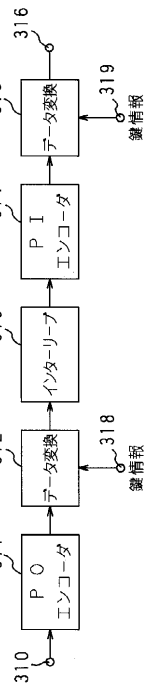
【図２５】



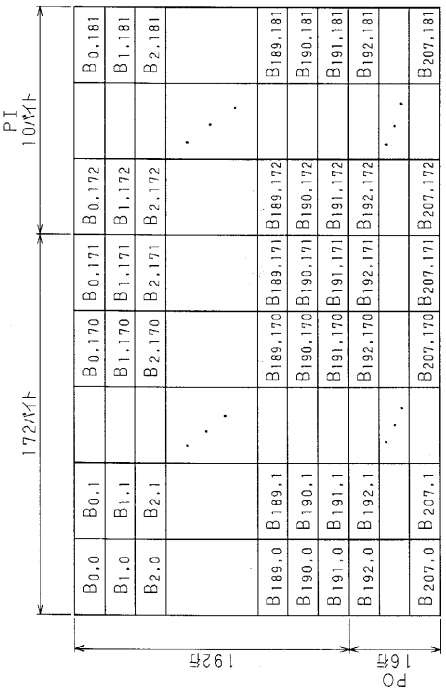
【図２６】



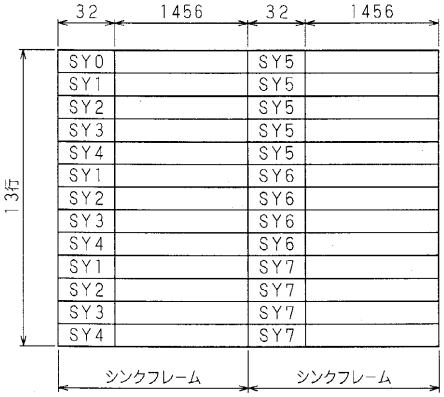
【図２７】



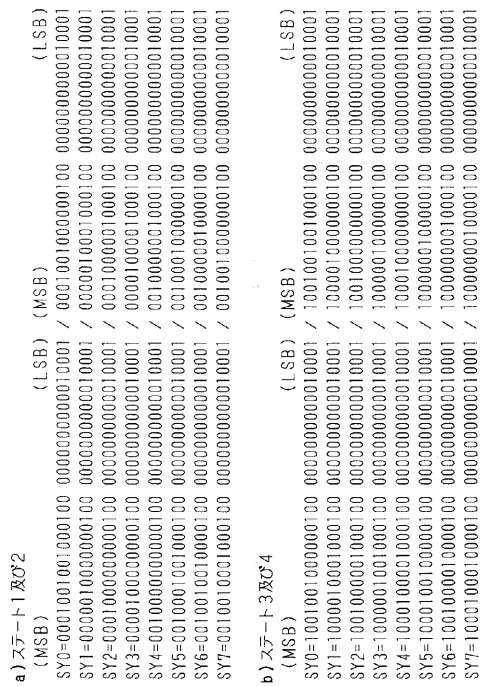
【図２８】



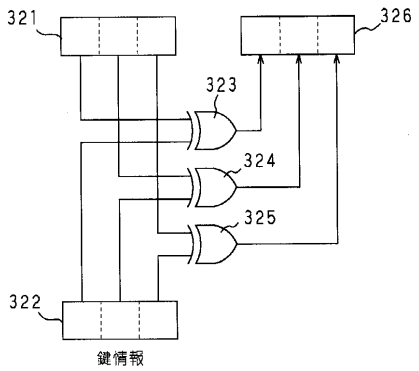
【図２９】



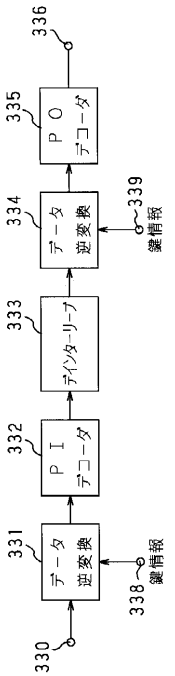
【図３０】



【図３１】



【図３２】


330
331
データ逆変換
338
鍵情報
332
PIデコーダ
333
デインターリーブ
334
データ逆変換
339
鍵情報
335
POデコーダ
336

フロントページの続き

(72)発明者　栗原　章
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　川嶋　功
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　高橋　克

(56)参考文献　特開平０７－０２１６８８（ＪＰ，Ａ）
特開平０７－０８５５７４（ＪＰ，Ａ）
特開平０７－０２１６８７（ＪＰ，Ａ）
特開平０７－０６５０３６（ＪＰ，Ａ）
特開昭６３－２５３４５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 12/14
G09C　1/00
G11B 20/10
H04L　9/08