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

特許第4672645号
(P4672645)

(45)発行日　平成23年4月20日(2011.4.20)　(24)登録日　平成23年1月28日(2011.1.28)

(51)Int.Cl.		F I		
G11B 20/10	(2006.01)	G11B	20/10	H
G06F 21/24	(2006.01)	G06F	12/14	540A
G11B 20/12	(2006.01)	G11B	20/12	

請求項の数 14　(全 13 頁)

(21)出願番号	特願2006-502564 (P2006-502564)
(86)(22)出願日	平成16年2月5日(2004.2.5)
(65)公表番号	特表2006-518525 (P2006-518525A)
(43)公表日	平成18年8月10日(2006.8.10)
(86)国際出願番号	PCT/IB2004/050079
(87)国際公開番号	WO2004/075187
(87)国際公開日	平成16年9月2日(2004.9.2)
審査請求日	平成19年2月2日(2007.2.2)
審判番号	不服2009-14200 (P2009-14200/J1)
審判請求日	平成21年8月7日(2009.8.7)
(31)優先権主張番号	1022743
(32)優先日	平成15年2月20日(2003.2.20)
(33)優先権主張国	オランダ(NL)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100122769
弁理士　笛田　秀仙
(72)発明者　ステク　アールベルト
オランダ国　５６５６　アーアー　アインドーフェン　プロフ　ホルストラーン　６

最終頁に続く

(54)【発明の名称】アクセス情報を有する情報担体

(57)【特許請求の範囲】

【請求項１】

ユーザ情報を保持するための情報担体であって、前記情報担体はユーザ情報にアクセスするためのアクセス情報ビットの形態のアクセス情報を有し、前記アクセス情報ビットはウォブルチャネルに保存され、前記ウォブルチャネルのウォブルの振幅は積分検出によって検出可能な小ささである情報担体において、前記アクセス情報ビットはキーフレームにあり、前記アクセス情報ビットは、所定のスクランブル方法に従ってスクランブルをかけられ、前記スクランブル方法は前記アクセス情報ビットのシーケンスの入れ替えを有し、前記入れ替えは前記キーフレームごとに異なることを特徴とする情報担体。

【請求項２】

前記アクセス情報ビットは、該アクセス情報ビットの所定のビットを反転させることによりスクランブルをかけられることを特徴とする、請求項１に記載の情報担体。

【請求項３】

前記アクセス情報ビットは、所定の方法で前記ビットのシーケンスを変更することによりスクランブルをかけられることを特徴とする、請求項１に記載の情報担体。

【請求項４】

前記ウォブルチャネルはウォブル状にされたプリグルーブであることを特徴とする、請求項１乃至３のいずれか一項に記載の情報担体。

【請求項５】

前記スクランブル方法が前記情報担体に保存されることを特徴とする、請求項１に記載

の情報担体。
【請求項６】
前記スクランブル方法は、前記ウォブルチャネルに保存されることを特徴とする、請求項５に記載の情報担体。
【請求項７】
前記情報担体は更に、前記所定のスクランブル方法を示すスクランブル方法ビットを有するエリアを有し、前記方法に従って前記アクセス情報ビットがスクランブルされることを特徴とする、請求項５又は６に記載の情報担体。
【請求項８】
前記スクランブル方法ビットは、前記ウォブルチャネルに保存されることを特徴とする、請求項７に記載の情報担体。
【請求項９】
前記エリアは８ビットのスクランブル方法ビットを有することを特徴とする、請求項７又は８に記載の情報担体。
【請求項１０】
前記情報担体はＰＩＣ(Permanent Information & Control data)ゾーンを有し、前記アクセス情報は前記ＰＩＣゾーンにおけるアドレスユニットに保存され、スクランブルのシードが前記ＰＩＣゾーンにおけるアドレスユニットのアドレス番号から導出されることを特徴とする、請求項１乃至９のいずれか一項に記載の情報担体。
【請求項１１】
前記アクセス情報は、予め記録されたピット及びランドの形で、又は予め記録された高周波変調されたグルーブの形で、前記ＰＩＣゾーンに保存されることを特徴とする、請求項１０に記載の情報担体。
【請求項１２】
請求項１乃至１１のいずれか一項に記載の情報担体から情報を読み出す装置において、前記装置は、前記情報担体からユーザ情報を読み出すための読み取りユニットと、積分検出によって前記ウォブルチャネルのウォブルを検出し、前記情報担体から前記アクセス情報を取得するためのアクセス制御手段とを有し、前記アクセス制御手段は、前記キーフレームにある前記アクセス情報ビットの前記異なる入れ替えに基づくデスクランブル及び積分をし、デスクランブルされたアクセス情報を利用して前記ユーザ情報へのアクセスを提供することを特徴とする装置。
【請求項１３】
前記ウォブルチャネルがウォブル状にされたプリグルーブである情報担体から情報を読み出す請求項１２に記載の装置において、前記読み取りユニットは、前記ウォブル状にされたプリグルーブのウォブルから前記アクセス情報ビットを読み出すことを特徴とする装置。
【請求項１４】
前記スクランブル方法が前記ウォブルチャネルに保存される情報担体であって、前記所定のスクランブル方法を示すスクランブル方法ビットを有するエリアを有し、前記方法に従って前記アクセス情報ビットがスクランブルされる情報担体から情報を読み出す請求項１２に記載の装置において、前記アクセス制御手段は、前記スクランブル方法ビットに依存して前記アクセス情報ビットをデスクランブルすることを特徴とする装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザ情報を保持するための情報担体であって、前記情報担体はユーザ情報にアクセスするためのアクセス情報ビットの形をとるアクセス情報を有し、前記アクセス情報ビットはパラメータの変化の形で前記情報担体に保存され、前記変化は積分検出によって検出可能な情報担体に関する。本発明は更に、前記情報担体から情報を読み出す装置に関する。

【背景技術】
【０００２】
ユーザ情報を保持するための情報担体においてアクセス情報を隠蔽する方法は、人（ハッカー）の注意を隠蔽したいアクセス情報から逸らすという事実に存する。該アクセス情報を利用して、前記情報担体上のユーザ情報がアクセスされることができる。コピー保護の目的のため、時として該アクセス情報を、保護したいユーザ情報に隠蔽すること又は前記情報担体に存在するサイドチャネル（side channel）に隠蔽することが望ましい。例えば、ＣＤ又はＤＶＤのような光情報担体から、該アクセス情報は所謂「ウォブルチャネル（wobble channel）」（時としてラジアルエラーチャネルとも呼ばれる）に書き込まれることが知られている。前記アクセス情報は、セキュアな方法でスペクトル拡散手法を利用して、パラメータの変化の形で情報担体に保存され得ることが知られている。該変化は積分によって検出可能であり、前記アクセス情報はウォブル状にされたプリグルーブの径方向の変位の形で保存される。当該変位の振幅は小さく、典型的にはピーク間で約５乃至１０ｎｍである。このようにして、該チャネルを読み出すことにより得られるウォブル信号は非常にノイズが多く、直接コピーすることが不可能である。スペクトル拡散手法においては、前記隠蔽されたアクセス情報は、特殊な方法により読み出し信号を積分することにより検出される。スペクトル拡散手法は、例えば「Digital Modulation and Coding」（Wilson、247－256頁）及び該文献の中の参考文献より知られている。積分検出は、例えば「Digital Baseband Transmission and Recording」（Jan W. M. Bergmans、122－129頁）より知られている。スペクトル拡散手法においては、信号の帯域幅が、スペクトル拡散変調を利用して意図的に大きくされる。前記変調された信号は、例えば仮定的な最尤受信器を利用して積分検出法を利用して検出されることができる。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
本発明の目的は、ユーザ情報の不正な取得が更に防止されるようなアクセス情報を有する情報担体を実現することにある。
【課題を解決するための手段】
【０００４】
本発明によれば本目的は、前記アクセス情報ビットが、所定のスクランブル方法に従ってスクランブルをかけられることを特徴とする情報担体により達成される。所定のスクランブル方法により前記アクセス情報ビットにスクランブルをかけることにより、前記アクセス情報の検出は前記スクランブル方法が未知である限り不可能である。前記アクセス情報ビットを有するエリアの読み出しの後に得られる信号がどのように処理される必要があるかが知られている場合にのみ、積分検出手法を利用することが前記アクセス情報に帰着する。
【０００５】
本発明による情報担体の他の実施例においては、前記アクセス情報ビットは、特定の反転された所定のアクセス情報ビットを前記情報担体に保存することによりスクランブルをかけられる。本発明による情報担体の他の実施例においては、前記アクセス情報ビットは、所定の疑似ランダムな方法で前記ビットのシーケンスを変更することによりスクランブルをかけられる。これらの実施例においては、前記アクセス情報ビットを有するエリアの読み出しにより得られる信号が、利用されたスクランブル方法に従って先に修正されなければ、積分検出手法がアクセス情報に帰着しない。
【０００６】
本発明によるシステムの他の実施例においては、前記情報担体は更にウォブル状にされたプリグルーブを有し、前記アクセス情報ビットは、前記ウォブル状にされたプリグルーブの径方向の変位の変化の形で保存される。
【０００７】
本発明による情報担体の他の実施例においては、前記スクランブル方法は前記情報担体

において隠蔽される。本発明による情報担体の他の実施例においては、前記スクランブル方法は、前記ウォブル状にされたプリグルーブの径方向の変位に隠蔽される。前記スクランブル方法は、可能な限り秘密にされることが好ましい。前記スクランブル方法を前記情報担体に隠蔽することにより、本発明による情報担体を再生するための装置において利用されるＩＣを作成する半導体企業に前記スクランブル方法を明らかにすることを防止できる。このとき、利用されるスクランブル方法についての情報は、十分に定義されたインタフェースを持つＶＥＲＩＬＯＧコードによって前記半導体企業に供給されても良い。前記コードは、前記半導体企業のＩＣ設計に付加されることができ、利用されるスクランブル方法の検出を処理する。このことは、本発明による情報担体を記述する規格の規定において、前記アクセス情報の位置が言及される必要がないという更なる利点を持つ。

【０００８】

或る方法がハッキングされた場合、利用されるスクランブル方法を変更することが可能であることが好ましい。この目的のため、他の実施例においては、前記情報担体は更に、前記所定のスクランブル方法を示すスクランブル方法ビットを有する特別なエリアを有し、前記方法に従って前記アクセス情報ビットがスクランブルされる。好ましくは、前記スクランブル方法ビットは、パラメータの変化の形で前記情報担体に保存され、前記変化は積分検出によって検出可能である。好ましくは、前記特別なエリアは８つのスクランブル方法ビットを有する。

【０００９】

前記スクランブル方法ビットは、種々のスクランブル方法を示すために利用され得る。例えば、８個のスクランブル方法ビットは、とり得る２５６（2^8）個のビットシーケンスを示すことができる。これらのビットシーケンスのそれぞれが、スクランブル方法を表す。前記所定のスクランブル方法がハッキングされた場合、将来の情報担体のために利用されるスクランブル方法を、他の方法のうちの１つに変更することができる。これらのスクランブル方法ビットは例えば、パラメータの変化の形で前記情報担体に保存されても良い。前記変化は積分検出により検出可能であり、それによりこれらのビットは積分検出を利用して検出されることができる。このことは、前記ビットがハッカーによって容易に検出されないという利点を持つ。

【００１０】

他の実施例においては、前記情報担体は不変情報及び制御データ（ＰＩＣ）ゾーンを有し、前記アクセス情報は前記ＰＩＣゾーンに保存される。前記アクセス情報は例えば、予め記録されたピット／ランド（又はマーク／ランド）の形でＰＩＣゾーンに保存されても良いが、該情報は、かなり高い帯域幅の信号で径方向に変調された、予め記録された高周波数変調（ＨＦＭ）されたグルーブの形で保存されても良い。該ＰＩＣゾーンは、ＢｌｕＲａｙディスクと呼ばれる新しい光情報担体において利用される。

【００１１】

本発明は更に、本発明による情報担体から情報を読み出す装置に関する。前記装置は、前記情報担体からユーザ情報及びアクセス情報を読み出すための読み取りユニットと、前記所定のスクランブル方法に従ってスクランブルをかけられたアクセス情報ビットをデスクランブルし、前記デスクランブルされたアクセス情報に依存して前記ユーザ情報へのアクセスを提供するアクセス制御手段とを有する。実施例においては、前記アクセス制御手段はＶＥＲＩＬＯＧブロックに組み込まれる。他の実施例においては、前記装置は更に、所定のスクランブル方法のリストを有するルックアップテーブルを有する。該テーブルを利用することにより、前記スクランブル方法がハッキングされた場合、利用される前記スクランブル方法は、別のスクランブル方法によって置き換えられることができる。

【００１２】

本発明のこれらの及び他の態様は、以下に記載される実施例を参照しながら説明され明らかとなるであろう。

【発明を実施するための最良の形態】

【００１３】

暗号化鍵のみならず、前記鍵又はＩＤ番号を保存するための幾つかの信号処理又は変調方法のような、コピー保護方式の幾つかの部分が秘密に保たれることが必要である。このとき、マスタリング機器に対してフォーマッタとして「ブラックボックス」を供給し、デコーダのＩＣ開発者に対してＶＥＲＩＬＯＧ記述を供給することが必要である。従って、検出に特殊なハードウェアを必要とするような秘密が、デコーダ部分又はサイドチャネルに存在する。かような場合においては、アプリケーションソフトウェア又はドライブのファームウェアを変更するだけでは、ハッカーは成功することができない。この秘密に対する必要性の一方で、製造において媒体をテストする必要性がある。１つの方法は、信号処理経路における１以上のフェーズにおいてスクランブルを利用し、幾つかの指定されたテストエリアにおいて前記スクランブルをスイッチオフすることである。スクランブルをかけられていないエリアにおいては、前記秘密の情報を再生するためのマージンをテストするために「テスト鍵」が読み取られ、幾つかのディジタル信号（例えばビットエラーレート）又は幾つかのアナログ信号（例えばジッタ又は信号対ノイズ比）を測定する必要がある。前記テスト鍵は、幾つかの機密扱いでないディスク情報であっても良い。

【００１４】

ＢＤ－ＲＯＭについては、コピー保護システムは、例えば暗号化鍵の形で前記アクセス情報を含む、ウォブル状にされたピット構造を含む。前記ウォブルの変調は、前記鍵のビットを表す。前記ビットは、秘密のスクランブル方法によってスクランブルをかけられる。前記スクランブル方法が知られていない限り、前記暗号化鍵を形成するビットを検出することはできない。前記スクランブル方法を可能な限り秘密に保つことが可能であることが望ましい。更には、或る方法がハッキングされた場合に、ことによると前記スクランブル方法を変更するバックアップのシナリオを持つことが望ましい。これらのバックアップは、可能な限り単純である必要がある。実施例による情報担体においては、（スクランブルをかけられていない）ウォブルキー（wobble key）の一部に前記スクランブル方法が書き込まれる。

【００１５】

図１に示された情報担体の実施例においては、前記アクセス情報が、前記情報担体のＰＩＣゾーンに保存される。本実施例においては、前記情報担体は所謂ＰＩＣ（Permanent Information & Control data、不変情報及び制御データ）ゾーンを有する。該ＰＩＣゾーンにおいては、前記情報担体についての一般情報及び種々の他の情報が保存されている。このようにして、十分な容量とデータレートを持つ予め記録された情報用のデータチャネルが生成される。本実施例においては、ＰＩＣ情報は予め記録されたピット／ランド（又はマーク／ランド）に保存される。しかしながら該情報は、かなり高い帯域幅の信号で径方向に変調された、予め記録された高周波変調（ＨＦＭ）されたグルーブに保存されても良い。前記情報はウォブルチャネルに保存されるという事実のため、埋め込まれたチャネルが生成される。図１において、ＰＩＣゾーンを有する前記情報担体のレイアウトが示される。前記情報担体上の担体中心に最も近いエリアは、内部エリア（ＩＡ）６と呼ばれる。該エリアの隣にはクランピングエリア（ＣＡ）７があり、該クランピングエリア７は、安定した回転が実現されるように前記情報担体を締着するために再生装置によって利用される。該クランピングエリア７の隣には移行エリア（ＴＡ）８がある。該移行エリア８の後に、情報エリア（ＩＡ）が配置される。該情報エリアは、情報ゾーン（ＩＺ）とバースト・カッティング・エリア（ＢＣＡ）９とを有する。前記バースト・カッティング・エリアは、製造工程の完了後に、前記情報担体に情報を追加するために利用される。ＢＣＡコードが、高いパワーのレーザシステムによって、又は再書き込み可能なディスクの場合にはイニシャライザによって書き込まれる。情報ゾーン（ＩＺ）は、リードインゾーン（ＬＩ）、データエリア１２及びリードアウトゾーン（ＬＯ）１３を有する。前記リードインゾーンは、ＰＩＣゾーン１０と、リードインゾーン１１の残りとを有する。本実施例においては、前記アクセス情報は、ＰＩＣゾーンの所定の領域に保存される。

【００１６】

前記アクセス情報を読み出せるようにするため、ＰＩＣゾーン中の前記アクセス情報の

位置へのリファレンスが、特定の方法によって取得されることができる。本実施例においては、該方法は以下のとおりである。ＰＩＣゾーンは、アドレスユニット番号（ＡＵＮ）を持つ主データチャネルを有する。これらのＡＵＮは、ＰＩＣゾーン中の前記アクセス情報の開始位置を示すために利用される。このことは、前記ウォブルチャネル信号がデータ信号（ＨＦチャネル）に固定されているため可能である。１つのアドレスは４バイトである（ＥＣＣバイトを除く）。ＰＩＣゾーンは前記情報担体の小さな部分に配置されているのみであるため、３２ビットのうちの限られた数だけの最下位ビット（ｌｓｂ）のみが、ＰＩＣゾーン内で変化する（一般に最初の１６個のｌｓｂのみ）。これら１６ビットは、ＰＩＣゾーン内の位置を決定するのに十分である。前記アクセス情報が２０個の連続するトラックのみに存在すると仮定すると、ＰＩＣゾーンは約２０００トラックに亘って延在する。該アクセス情報の開始位置は、前記ユーザ情報からＡＵＮによって決定される。該ＡＵＮの最初の１６個のｌｓｂはこのとき、例えばアンスクランブルド変調（unscrambled modulation）を利用して、ＰＩＣゾーン全体に亘って配置される。これにより、ＰＩＣゾーンのランダムな位置に到達したときにも、ＡＵＮの最初の１６ビットを読み出し、前記アクセス情報の開始位置にジャンプして、前記アクセス情報を読み出すことが可能となる。このようにして、前記アクセス情報の正確な位置はＰＩＣゾーンに更に隠蔽され、該帯域中の特定の位置にのみ配置され、帯域全体に亘って配置されない。

【００１７】

本実施例においては、前記アクセス情報は、ウォブル状にされたピット構造を利用してＢＤ－ＲＯＭのＰＩＣゾーンに書き込まれる。前記ピット構造に含まれる主データは、通常のＰＩＣ情報（ドライブ取り消し情報、ディスク情報）から成る。前記アクセス情報は、前記ディスク上のユーザ情報を復号化するために必要とされる鍵の一部であっても良い。前記ウォブルの振幅は小さく、例えばピーク間で５乃至１０ｎｍである。このように、ウォブル信号は非常にノイズを含むものであり、直接コピーすることが不可能である。

【００１８】

消費者向けドライブについては、大きな振幅のウォブルさえもコピーが不可能である。なぜなら、ドライブがアクチュエータをウォブルさせる（wobble）ことができないからである。従って、前記鍵を含ませるために前記情報担体においてウォブルを利用することは、消費者向けドライブが内容のビット毎のコピーをすることを不可能にする（アクチュエータをウォブルさせることができる高度な消費者向けドライブが将来利用可能となるという仮定の下では、前記ウォブルの実際のコピーを防ぐことはできない）。しかしながら、ＢＤ－ＲＯＭ６９ＴにおけるＣＰＳウォブルの周期を選択する場合、コピーされるＢＤ－ＲＥ上のＣＰＳウォブルは、同じ６９個のチャネルビットの周波数を持つ該ディスク上のプリグルーブと干渉するであろう。それ故、コピーされたディスク上のＣＰＳウォブルの読み出しは不可能である。このことは、ＣＤの場合についてPhilips社の米国特許US5,724,327においても言及されている。しかしながら、マスタリング機器にアクセスできる熟練した侵害者は、次の違法に作成されたスタンパに前記ウォブルをマスタリングするためディフレクタ（deflector）信号を駆動するために、この大きなウォブル振幅を利用し得る。それ故、この方法がこれら侵害者にも不可能となるのに十分なほど、前記ウォブル振幅は小さいべきである。前記ウォブル信号はこのとき、前記ウォブルをコピーするためにマスタリング機器におけるディフレクタを正常に駆動することができない程、ノイズの大きいものとなる。該ウォブル中のデータの検出は、積分検出によってのみ可能である。勿論ハッカーは、前記ウォブルからデータを得るためにこの方法さえも利用し得る。しかしながら、このことを防止するために他の方法、即ちスクランブルが利用される。この実施例は、図２を参照しながら説明される。

【００１９】

データのスクランブルは幾つかの方法で為され得る。１つの可能性は、所定の秘密の方法で、前記鍵のビットを反転させることである。他の可能性は、積分の間に変化する所定の方法で、ビットのシーケンスを入れ替えることである。第３の可能性として、これら方法の両方の組み合わせを利用することができる。スクランブル方法が知られない限り、信

号を積分することはできない。前記信号を適切に積分するためには、検出されたビットに対して前記秘密のスクランブル方法の逆を適用することにより、二極性の信号から単極性の信号を作成する必要がある。これにより初めて、軟判定情報が前記ノイズから取り出されることができる。

【００２０】

図２の実施例においては、ステップ２２において、アクセス情報を有する１６８個のビット、ＣＲＣビット及び予備ビットが、１６８個のランダム的なビットとＸＯＲ演算される。これらのランダム的なビットは例えば、前記情報担体から取得されても良いし、又は前記情報担体を読み出す装置に存在しても良い。結果のビットに対して、ステップ２３においてランダム的な入れ替えが実行される。該入れ替えられたビットは次いで、情報担体１に書き込まれる。これらのビットは、図３において説明されるような、キーフレームに書き込まれても良い。利用される前記ランダム的なビット及び前記ランダム的な入れ替えは、キーフレーム毎に変更されても良い。前記入れ替えは、全てのＥＣＣブロックに繰り返されても良く、スクランブルのシード（seed）は例えばＡＵＮ、即ちＰＩＣゾーンにおいて利用されるアドレス番号から導出されても良い。

【００２１】

図３は、情報担体の他の実施例を示す。本実施例においては、スクランブルをかけられたアクセス情報を有する１６８個のビットが、キーフレーム５１中に存在するウォブルチャネルに保存される。本実施例においては、５つのキーフレームに加え予備のシンク（sync）フレームが、１つの物理セクタを形成する。前記５つのキーフレームは、それ自体で１つのアドレスユニットを形成する（８０個のキーフレームがあるため、各ＥＣＣセクタには１６個のアドレスユニットが存在する）。前記ウォブルチャネルに保存されたアクセス情報に対して利用される秘密の入れ替えの知識があって初めて、前記ビットの適切な積分が実行されることができる。実施例においては、該秘密の入れ替えは、ＶＥＲＩＬＯＧブロック（ＬＳＩパッケージとも呼ばれる）中に留まる。このことは、該情報担体を記述する規格の規定において、前記アクセス情報の位置が言及される必要がないという利点を持つ。本実施例は、スクランブル方法を変更するためのバックアップのオプションが必要とされない場合に利用されることができる。

【００２２】

前記スクランブル方法を可能な限り秘密に保つことが可能であることが望ましい。更には、或る方法がハッキングされた場合に、ことによると前記スクランブル方法を変更するバックアップのシナリオを持つことが望ましい。これらのバックアップは、可能な限り単純である必要がある。前記スクランブル方法を変更することが可能な本発明による情報担体の他の実施例が、図４に示される。本実施例においては、前記情報担体は４つのキーフレーム１４を有する。これらのキーフレームにおいて、３１個のシンクフレームが存在し、０乃至３０の番号が付されている。シンクフレーム番号３、７、１１、１５、１９、２３及び２７（参照番号１５によって示されている）において、前記アクセス情報の正確な位置を示す８ビットの数が保存されている。前記アクセス情報が或るパラメータの変化の形で前記情報担体に保存され、該変化は積分検出により検出可能なものである場合には、前記アクセス情報の正確な位置は、該８ビットの数を利用して変化させられることができる。このとき該８ビットの数は例えば、前記アクセス情報を形成するビットを検出するためどのシード及び入れ替えが利用されるべきかを示しても良い。

【００２３】

スクランブルをかけられない方法で、例えば８個のビットのようなビットのシーケンスを、ＰＩＣゾーン中のウォブルの形で特別なエリアに書き込むことも可能である。スクランブルをかけられていないため、これらの８ビットは、積分検出を利用してノイズから非常に容易に積分されることができる（代替としてスクランブルを使用しても良いが、ドライブに知られた一定の方法であるべきである）。前記ビットのシーケンスは、$2^8 = 256$個のとり得るビットシーケンスを与える。これらのシーケンスのそれぞれはこのとき、秘密のスクランブル方法を表す。これら２５６個の方法のリストを含むルックアップテー

ブルが、秘密のウォブル鍵検出回路において、前記ドライブに含まれても良い。該シーケンスは容易に読み取られることができ、前記スクランブル方法が知られ、前記ウォブル鍵が検出されることができる。前記スクランブル方法がハッキングされた場合は、単に将来のディスク用に他の２５６方法のうちの１つに変更する。勿論、前記ドライブ中のウォブル検出回路は、２５６個のスクランブル方法全てを知っている必要がある。典型的に、前記ウォブル検出回路はＶＥＲＩＬＯＧコード中に配置され、前記回路の製造者に供給される。このように、２５６個のスクランブル方法が何であるかを見出すためには、ＶＥＲＩＬＯＧコードをハッキングする必要がある。このことは複雑であり、全てのひとが該ＶＥＲＩＬＯＧコードにアクセスできるわけでもない。前記スクランブル方法が知られている必要がある他の場所は、マスタリング機器である。しかしながら本例に場合には、２５６個のスクランブル方法全てではなく、現在装備されているスクランブル方法のみが実装される必要がある。１つのスクランブル方法がハッキングされた場合には、前記マスタリング機器のフォーマット生成器における特別なウォブルエンコーダが、（２５６個のとり得る方法のうちの）別のスクランブル方法を備える他のエンコーダと置き換えられることができる。このことは該秘密の情報へのアクセスをかなり制限する。

【００２４】

図５は、情報担体からアクセス情報を読み出す装置の実施例を示す。前記装置は、ユーザ情報及びアクセス情報を記録担体１から読み出すための読み取りユニットを有する。前記読み取りユニットは、トラックを走査し、前記記録担体上の物理的なマークに対応する読み取り信号を生成する読み取りヘッド４１を有する。前記読み取りユニットはまた、例えばＣＤシステムにおけるデコードのためのＥＦＭデコーダのような、前記読み取り信号をビットシーケンスに変換する変換ユニット４２を有する。前記ビットシーケンスは、例えばＣＤシステムにおけるＣＩＲＣ訂正器のような、エラー訂正ユニット４３に結合される。該エラー訂正ユニット４３は、情報を復元し、想定されるエラーを訂正する。前記復元された情報は、前記情報へのアクセスを制御するアクセス制御手段４７に結合される。前記読み出されたアクセス情報は、アクセス制御手段４７の出力４８に対して更に処理をするために利用可能である。読み取りの間、読み取りヘッド４１は通常のタイプのサーボユニット４４によって前記トラック上に配置され、この間前記記録担体はモータユニット４５によって回転させられている。前記情報の読み取りはコントローラ４６によって制御される。該コントローラは、モータユニット４５、サーボユニット４４及びエラー訂正ユニット４３を制御し、例えばアクセス制御手段４７へのインタフェースを介して、読み取りコマンドを受信するように構成される。

【００２５】

前記アクセス情報の読み出しは、以下のように実行される。前記アクセス制御手段は、スクランブルをかけられたアクセス情報ビットをＰＩＣゾーンから読み出す。積分検出手法と、これらビットに用いられたスクランブル（デスクランブル）方法を利用して、前記アクセス制御手段が前記アクセス情報を取得することが可能である。前記アクセス情報は例えば、暗号化されたユーザ情報を復号化するための復号化鍵であっても良い。該アクセス情報を利用して、前記ユーザ情報へアクセスができるようになる。前記情報担体が前記アクセス情報を有さない場合には、又は前記装置が前記アクセス情報を読み出すことができない場合には、前記情報担体は拒絶され、前記ユーザ情報へのアクセスは禁止される。

【００２６】

図６は、前記ユーザ情報にアクセスができるようにするアクセス情報の利用の実施例を示す。例えば図４に示されたような装置を利用して、ユーザ情報１６が情報担体１から読み出されることが示されている。アクセス情報１７は、検出モジュール１８において検出される。前記検出モジュールは、前記アクセス情報ビットにスクランブルをかけるために利用されたスクランブル方法についての知識を持つ。前記スクランブルをかけられたアクセス情報ビットは、最初に積分検出を利用して検出され、次いでデスクランブルされる。該検出されたアクセス情報を利用して、モジュール１９において復号化鍵が算出される。このスクランブル（デスクランブル）方法のための更なる入力として、乱数２０が利用さ

れても良い。該数は、図２を参照しながら説明されたようなビットを入れ替えるために利用された乱数であっても良い。該数は前記情報担体上に隠蔽された数であっても良いし、前記装置のユーザによって入力される数であっても良い。前記算出された鍵は、前記ユーザ情報を復号化するために復号化モジュール２１において利用される。前記ユーザ情報の復号化の後、該情報は更に処理され又は出力される。このことは、正しいアクセス情報の検出を条件とされる。モジュール１８、１９及び２１は、ＶＥＲＩＬＯＧコードの形でＩＣ製造業者に供給されても良い。このため、前記アクセス情報又は鍵算出についての情報は開示される必要はない。なぜならこのことは、ＶＥＲＩＬＯＧブロック２２の内部で実行されるからである。

【００２７】

図７は、前記装置において利用される検出モジュールの実施例を示す。本実施例においては、検出モジュール１８はＶＥＲＩＬＯＧコードとして供給される。フレームシンク及びセクタ先頭が、該検出モジュールに入力される。なぜならこれらは、前記アクセス情報ビットを有するウォブル鍵ビット位置を見出すために必要とされるからである。ＥＣＣブロック先頭が入力されるが、これは前記スクランブルをかけられたアクセス情報ビットの入れ替えシーケンスについての知識のために必要とされるからである。ＡＵＮが入力されるが、これは前記スクランブル方法におけるシード生成において必要とされるからである。全ての信号は、前記ユーザ情報中のフレームシンクと同時に供給され、Ａ／Ｄ変換の後に前記検出モジュールに入力される。前記アクセス情報ビットをデスクランブルした後、前記検出モジュールは、例えば前記ユーザ情報を復号化するための鍵として、前記アクセス情報を出力する。

【００２８】

本発明は上述した実施例を参照しながら説明されたが、同じ目的を達成するため他の実施例が代替として利用されても良いことは明らかであろう。本発明の範囲はそれ故、上述した実施例に限定されるものではなく、読み取り専用、１度書き込み可能又は再書き込み可能なタイプの担体といった、全ての種類の情報担体に適用され得る。本発明の範囲は更に、特定の種類のアクセス情報に限定されるものではない。アクセス情報、即ち本発明による情報担体に保存された又は保存されるべきユーザ情報へのアクセスを可能とするために用いられる情報として利用される又は利用され得る全ての情報は、本発明の範囲内である。本発明の範囲は更に、特定の埋め込まれたチャネル手法又は特定の（隠蔽された）サイドチャネルに限定されるものではない。情報を保存するために利用され得る全ての手法及びチャネルは、本発明の範囲内である。更に、本発明は、前記アクセス情報がウォブル状にされたプリグルーブの小さな径方向の変位の形で保存されるスペクトル拡散手法に限定されるものではない。情報担体に積分検出可能な情報を保存するために、検出可能な特性の小さな変化を導入するため、全ての物理的なパラメータが利用され得る。

【００２９】

「有する（comprise/comprising）」なる語は、請求項を含む本明細書において利用される場合には、言及された特徴、整数、ステップ又は構成要素の存在を規定するものと解釈され、１以上の他の特徴、整数、ステップ、構成要素又はこれらの群の存在又は付加を除外するものではないことは、更に留意されるべきである。また請求項において要素に先行する「１つの（a又はan）」なる語は、複数のかような要素の存在を除外するものではないことも留意されるべきである。更に、いずれの参照記号も請求の範囲を限定するものではなく、本発明はハードウェア及びソフトウェアの両方によって実装されても良く、幾つかの「手段」は同一のハードウェアのアイテムによって表されても良い。更に、本発明はそれぞれの及び全ての新規な特徴又はこれら特徴の組み合わせに存する。

【００３０】

本発明は以下のように要約されることができる。本発明は、ユーザ情報を保持するための情報担体に関し、前記ユーザ情報にアクセスするためのアクセス情報ビットの形をとるアクセス情報を有し、前記アクセス情報ビットがパラメータの変化の形で前記情報担体に保存され、前記変化が積分検出により検出可能である情報担体に関する。前記アクセス情

報ビットは、所定のスクランブル方法に従ってスクランブルをかけられる。所定のスクランブル方法に従って前記アクセス情報ビットにスクランブルをかけることにより、前記スクランブル方法が知られていない限り、前記アクセス情報の検出が不可能となる。前記アクセス情報ビットを有するエリアの読み出しの後に得られる信号がどのように処理される必要があるかが知られている場合にのみ、積分検出手法を利用することが前記アクセス情報に帰着する。このようにして、ユーザ情報の不正な取得が更に防止される。

【図面の簡単な説明】

【００３１】

【図１】本発明による情報担体の第１の実施例を示す。

【図２】本発明による情報担体の第２の実施例を示す。

【図３】本発明による情報担体の他の実施例を示す。

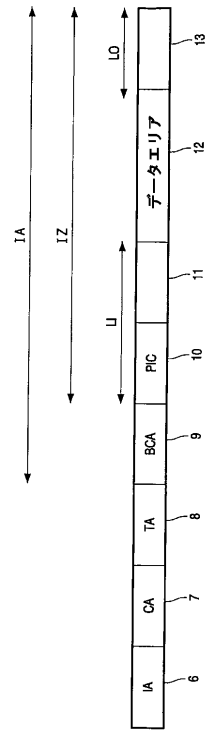
【図４】本発明による情報担体の他の実施例を示す。

【図５】情報担体からアクセス情報を読み出す装置の実施例を示す。

【図６】ユーザ情報にアクセスできるようにするためのアクセス情報の使用の実施例を示す。

【図７】装置において利用される検出モジュールの実施例を示す。

【図１】



【図２】

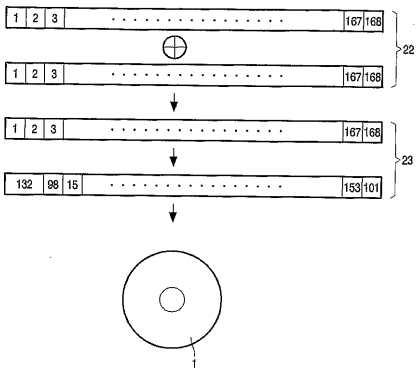
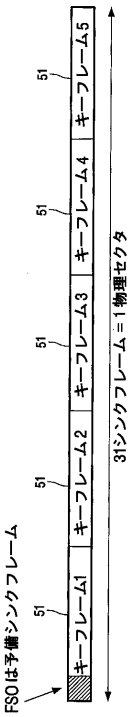
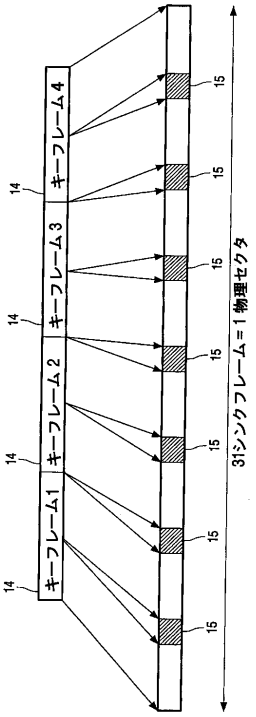


FIG.2

【図３】



【図４】



【図５】

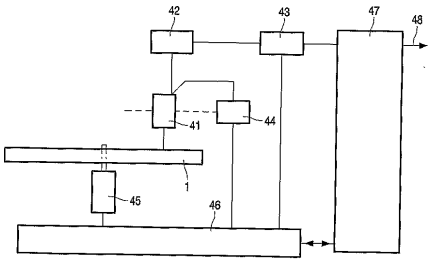


FIG.5

【図６】

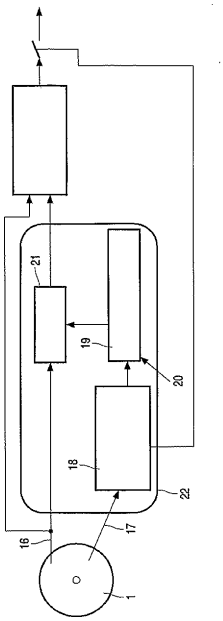
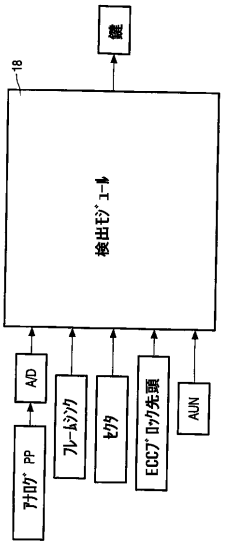


FIG.6

【図７】



フロントページの続き

(72)発明者 ブラム マルティヌス ダヴリュ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６
(72)発明者 ファン ロムパエイ バルト
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６
(72)発明者 ヘームスケルク ヤコブス ピー ジェイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６

合議体
審判長 小松 正
審判官 石川 正二
審判官 石丸 昌平

(58)調査した分野(Int.Cl., ＤＢ名)
G11B20/10
G11B20/12