(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2007-528561
(P2007-528561A)
(43)公表日　平成19年10月11日(2007.10.11)

(51)Int.Cl.		F I			テーマコード（参考）
G11B 20/10	(2006.01)	G11B	20/10	H	5B017
H04N 5/91	(2006.01)	H04N	5/91	P	5C052
H04N 5/85	(2006.01)	H04N	5/85	Z	5C053
H04L 9/08	(2006.01)	H04L	9/00	601B	5D044
G06F 21/24	(2006.01)	H04L	9/00	601E	5J104

審査請求 有　予備審査請求 未請求　（全 12 頁）　最終頁に続く

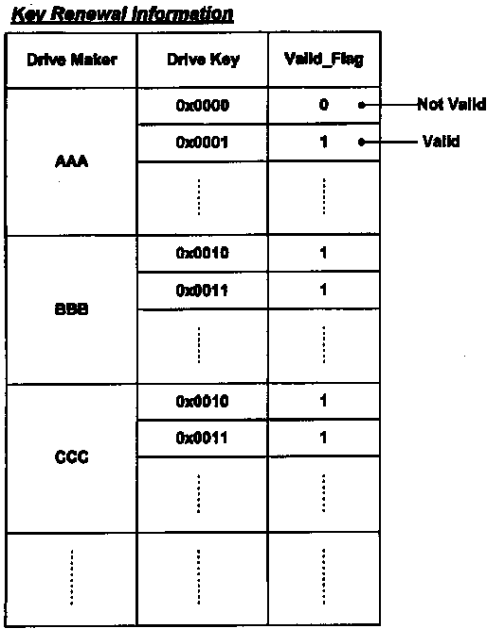
(21)出願番号　特願2006-507821 (P2006-507821)
(86)(22)出願日　平成16年4月24日 (2004.4.24)
(85)翻訳文提出日　平成17年12月21日 (2005.12.21)
(86)国際出願番号　PCT/KR2004/000951
(87)国際公開番号　WO2004/095161
(87)国際公開日　平成16年11月4日 (2004.11.4)
(31)優先権主張番号　10-2003-0026149
(32)優先日　平成15年4月24日 (2003.4.24)
(33)優先権主張国　韓国 (KR)

(71)出願人　502210921
エルジー　エレクトロニクス　インコーポレイテッド
大韓民国、１５０－７２１、ソウル　シティ、ヤンドュンポ－ク、ヨイド－ドン、２０
(74)代理人　100094318
弁理士　山田　行一
(74)代理人　100123995
弁理士　野田　雅一

最終頁に続く

(54)【発明の名称】記録媒体の複写防止情報管理方法

(57)【要約】
記録媒体の複写防止情報管理方法に関する。光ディスクのデータ領域に暗号化して記録されたA／Vデータを復号化するための複写防止情報が記録されるキーロッカー内に、光ディスクドライブを製造したメーカー情報、各メーカー別ドライブキー、そしてドライブキーの有効可否を示すためのフラッグが連係するキー更新情報を付加記録する。光ディスクのA／Vデータを再生する場合、光ディスクドライブ内で管理されるドライブキーと光ディスクに記録されたキー更新情報を比較して、キーロッカー内に記録された複写防止情報を読み出して復号化する。従って、不法複製された光ディスクドライブが正常的な再生動作をこれ以上遂行することができないようにして、光ディスクドライブの不法複製を効率的に抑制することができる。また、全てのメーカーの光ディスクドライブが一度に不法複製されることを未然に防止できる。
【選択図】図７



【特許請求の範囲】
【請求項１】
記録媒体の複写防止情報管理方法において、
記録媒体のデータ領域に暗号化して記録されたデータを復号化するための複写防止情報を第１特定領域に記録して；
前記複写防止情報を復号化するための第１キーを前記記録媒体の第２特定領域に記録して；そして
前記複写防止情報を復号化するために必要な第２キーの有効可否を示すキー更新情報を前記第１特定領域に記録することで構成されて、
ここで、前記第２キーは記録媒体を再生するドライブまたはアプリケーション内で管理されることを特徴とする記録媒体の複写防止情報管理方法。
【請求項２】
前記第１キーはビット対ビット複写方式により複製されない低周波成分を有するウォーブル形状のヒドン・コードであって、前記第２キーは前記ドライブを製造したメーカー別固有のＩＤによって区分される固有のキーであって、前記複写防止情報は暗号化して記録される記録媒体キーであることを特徴とする、請求項１に記載の記録媒体の複写防止情報管理方法。
【請求項３】
前記キー更新情報には、前記ドライブを製造したメーカー情報、各メーカー別第２キー、そして第２キーの有効可否を示すフラッグが連係記録されることを特徴とする、請求項３に記載の記録媒体の複写防止情報管理方法。
【請求項４】
複写防止情報により暗号化したデータが記録されるデータ領域と；
前記複写防止情報と、前記複写防止情報を復号化するために必要な第２キーの有効可否を示すキー更新情報が記録される第１特定領域；及び
前記複写防止情報を復号化するための第１キーが記録される第２特定領域で構成されることを特徴とする記録媒体。
【請求項５】
前記複写防止情報は暗号化して記録されたディスクキーであって、前記第１キーと前記記録媒体を再生するドライブにより管理される第２キーの組合により復号化されることを特徴とする、請求項４に記載の記録媒体。
【請求項６】
前記第２キーはドライブキーまたはアプリケーションキーであることを特徴とする、請求項５に記載の記録媒体。
【請求項７】
前記第１キーはビット対ビット複写方式により複製されない低周波成分を有するウォーブル形状のヒドン・コードであることを特徴とする、請求項４に記載の記録媒体。
【請求項８】
前記キー更新情報には、記録媒体を再生するドライブまたはアプリケーションを製造したメーカー情報、各メーカー別第２キー、そして第２キーの有効可否を示すフラッグが連係記録されることを特徴とする、請求項４に記載の記録媒体。
【請求項９】
記録媒体の第２特定領域から読み出される第１キーと前記記録媒体を再生するドライブまたはアプリケーション内で管理される第２キーを利用して、前記記録媒体の第１特定領域のキー更新情報を読み出す段階；及び
前記読み出されたキー更新情報を根拠にして、前記第２キーの有効可否を判断する段階；及び
前記判断結果によって、前記第１キーと第２キーを利用して、前記第１特定領域に記録された複写防止情報を復号化する段階を含んで構成されることを特徴とする記録媒体の複写防止情報管理方法。

【請求項１０】
前記第１キーはビット対ビット複写方式により複製されない低周波成分を有するウォーブル形状のヒドン・コードであって、前記第２キーはドライブキーまたはアプリケーションキーであって、前記キー更新情報はキーロッカー内に記録されたことを特徴とする、請求項９に記載の記録媒体の複写防止情報管理方法。
【請求項１１】
前記キー更新情報には、記録媒体を再生するドライブまたはアプリケーションを製造したメーカー情報、各メーカー別第２キー、そして第２キーの有効可否を示すフラッグが連係記録されることを特徴とする、請求項９に記載の記録媒体の複写防止情報管理方法。
【請求項１２】
前記キー更新情報に含まれた情報のうちで、前記ドライブまたはアプリケーション内で管理される第２キーに該当するフラッグにより前記第２キーが有効だと判断する場合、前記第１キーと第２キーを利用して前記第１特定領域に記録された複写防止情報を復号化することを特徴とする、請求項１１に記載の記録媒体の複写防止情報管理方法。
【請求項１３】
前記キー更新情報に含まれた情報のうちで、前記ドライブまたはアプリケーション内で管理される第２キーに該当するフラッグにより前記第２キーが有効でないと判断する場合、前記第１特定領域に記録された複写防止情報を復号化しないことを特徴とする、請求項１１に記載の記録媒体の複写防止情報管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は記録媒体の複写防止情報管理方法に係り、さらに詳細にはＣＤ（Ｃｏｍｐａｃｔ Ｄｉｓｃ）、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ）またはＢＤ（Ｂｌｕ－ｒａｙ Ｄｉｓｃ）等のような光ディスクのデータ領域に暗号化して記録されたＡ／Ｖデータを復号化するための複写防止情報（Ｃｏｐｙ Ｐｒｏｔｅｃｔｉｏｎ Ｉｎｆｏｒｍａｔｉｏｎ）の保安性を向上させるための方法に関する。
【背景技術】
【０００２】
一般的にデジタルビデオ及びオーディオデータを記録することができる光ディスク、例えばＣＤとＤＶＤが広く普及されて商用化されており、またＢＤ等のような高密度光ディスクの規格化作業が急速に進展するによって、関連製品が商用化されることと期待されている。
【０００３】
一方、前記のような光ディスクに記録されたデジタルビデオ及びオーディオデータのコンテンツ（Ｃｏｎｔｅｎｔｓ）を無断で不法複製することができないようにするために、複写防止情報により暗号化したＡ／Ｖデータを光ディスクのデータ領域に記録して、前記複写防止情報を光ディスクのリードイン領域等のような特定領域に記録して管理する方法が提案されているが、これに対して詳細に説明すると次のようである。
【０００４】
図１は一般的なＤＶＤの複写防止情報管理方法が適用される光ディスクドライブとアプリケーションに対する構成を示したものである。前記光ディスクドライブ２００には、認証部（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｂｌｏｃｋ）２０、キー分配部（Ｋｅｙ Ｓｈａｒｉｎｇ Ｂｌｏｃｋ）２１、そして暗号化部（ＥｎｃｒｙｐｔｉｏｎＢｌｏｃｋ）２２、２３等で構成されることができる。
【０００５】
個人用コンピューター（ＰＣ）等のようなアプリケーション３００には、認証部３０、キー分配部３１、復号化部（Ｄｅｃｒｙｐｔｉｏｎ Ｂｌｏｃｋ）３２、３３、ディスクランブル部（Ｄｅｓｃｒａｍｂｌｅ Ｂｌｏｃｋ）３４、デコンプレッション部（Ｄｅｃｏｍｐｒｅｓｓｉｏｎ Ｂｌｏｃｋ）３８、ディスクキー復号化部３６、そしてタイトル

キー復号化部３７等で構成されることができる。
【０００６】
そして、前記光ディスクドライブ２００に挿入されるＤＶＤ　１００には、認証コントロールキー（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｎｔｒｏｌ　Ｋｅｙ）、セキュアドディスクキー（Ｓｅｃｕｒｅｄ　Ｄｉｓｃ　Ｋｅｙ）、エンクリプティッドタイトルキー（Ｅｎｃｒｙｐｔｅｄ　Ｔｉｔｌｅ　Ｋｅｙ）、そしてスクランブルドＡ／Ｖデータ（Ｓｃｒａｍｂｌｅｄ　Ａ／Ｖ　Ｄａｔａ）が保存されることができる。
【０００７】
一方、前記光ディスクドライブの認証部２０では、前記ＤＶＤ　１００から読み出される認証コントロールキーを利用して、前記アプリケーションの認証部３０とのデータ送受信のための一連の認証過程を遂行するようになる。前記暗号化部２２、２３では、前記キー分配部２１から提供する所定の暗号化キーを利用して、前記ＤＶＤ　１００から読み出されるセキュアドディスクキーとエンクリプティッドタイトルキーをデータ送受信に適合なデータで再び暗号化して伝送するようになる。
【０００８】
そして、前記アプリケーションの復号化部３２、３３では、前記キー分配部３１から提供する所定の復号化キーを利用して、前記光ディスクドライブ２００から受信されるセキュアドディスクキーとエンクリプティッドタイトルキーを復号化する一連の動作を遂行するようになる。
【０００９】
一方、前記ディスクキーは前記アプリケーション３００内で管理されるマスターキー３５により復号化されて、前記タイトルキーは前記復号化されたディスクキーにより復号化されて、前記ディスクランブル部３４では、前記タイトルキーを利用して、ＤＶＤから読み出されるスクランブルドＡ／Ｖデータをディスクランブル処理するようになって、前記デコンプレッション部３８では、ディスクランブル処理されたＡ／Ｖデータを非圧縮処理して、本来のＡ／Ｖデータで出力するようになる。このような過程を介して、前記ＤＶＤにスクランブル処理されて記録されたオーディオ及びビデオデータのコンテンツが無断で不法複製されることを防止することができるようになる。
【００１０】
しかし、前記ＤＶＤに記録されたセキュアドディスクキーとエンクリプティッドタイトルキーのような複写防止情報がハッカー（Ｈａｃｋｅｒ）等のような第３者により不法的にハッキングされて流出される場合、前記ＤＶＤのデータ領域に暗号化して記録されたＡ／Ｖデータの不法複製が可能になる。したがって、複写防止情報の保安性をより強化させることができる効率的な解決方案の用意が急に要求されている実情である。
【発明の概要】
【００１１】
本発明は前記のような実情を勘案して創作されたものであって、本発明の目的は、複写防止情報の保安性をより強化する、記録媒体の複写防止情報を管理する方法を提供することにある。
【００１２】
本発明の他の目的は、記録媒体の複写防止情報を管理し、それによって、不法複製された光ディスクドライブが正常的な再生動作をこれ以上遂行することができないようにする管理方法を提供することにある。
【００１３】
前記のような目的を達成するための本発明による記録媒体の複写防止情報管理方法は、記録媒体のデータ領域に暗号化して記録されたデータを復号化するための複写防止情報を第１特定領域に記録して；前記複写防止情報を復号化するための第１キーを前記記録媒体の第２特定領域に記録して；そして前記複写防止情報を復号化するために必要な第２キーの有効可否を示すキー更新情報を前記第１特定領域に記録することで構成されて、ここで、前記第２キーは記録媒体を再生するドライブまたはアプリケーション内で管理されるこ

とを特徴とする。

【００１４】

また、本発明による記録媒体は、複写防止情報により暗号化したデータが記録されるデータ領域と；前記複写防止情報と、前記複写防止情報を復号化するために必要な第２キーの有効可否を示すキー更新情報が記録される第１特定領域；及び前記複写防止情報を復号化するための第１キーが記録される第２特定領域で構成されることを特徴とする。

【００１５】

また、本発明の他の実施形態による記録媒体の複写防止情報管理方法は、記録媒体の第２特定領域から読み出される第１キーと前記記録媒体を再生するドライブまたはアプリケーション内で管理される第２キーを利用して、前記記録媒体の第１特定領域のキー更新情報を読み出す段階；及び前記読み出されたキー更新情報を根拠にして、前記第２キーの有効可否を判断する段階；及び前記判断結果によって、前記第１キーと第２キーを利用して、前記第１特定領域に記録された複写防止情報を復号化する段階を含んで構成されることを特徴とする。

【発明を実施するための最良の形態】

【００１６】

以下、本発明による記録媒体の複写防止情報管理方法に対する望ましい実施形態に対して、添付した図面を参照しながら詳細に説明する。

【００１７】

図２は本発明による記録媒体の複写防止情報管理方法が適用される光ディスクドライブに対する構成を示したものである。前記光ディスクドライブ５００には、復号化部（Ｄｅｃｒｙｐｔｉｏｎ　Ｂｌｏｃｋ）５０とキー計算部（Ｋｅｙ　Ｃａｌｃｕｌａｔｉｏｎ）５１が含まれて、本発明により新しく定義されたドライブキー（Ｄｒｉｖｅ　Ｋｅｙ）５２が管理されることができる。

【００１８】

また、前記光ディスクドライブ５００に挿入される光ディスク４００には、複写防止情報、例えば暗号化したディスクキー（Ｄｉｓｃ　Ｋｅｙ）がキーロッカー（Ｋｅｙ　Ｌｏｃｋｅｒ）内に記録されると共に、前記光ディスク４００の特定領域、例えば光ディスクのリードイン領域（Ｌｅａｄ－Ｉｎ　Ａｒｅａ）のＰｒｅ－ｒｅｃｏｒｄｅｄ（またはＥｍｂｏｓｓｅｄ）Ａｒｅａには前記ディスクキーを読み出すための第１キー値のヒドン・コード（Ｈｉｄｄｅｎ　Ｃｏｄｅ）がＰｒｅ－ｒｅｃｏｒｄｅｄ　ｔｙｐｅで記録される。

【００１９】

前記キーロッカー内に記録されたディスクキーは、前記第１キー値のヒドン・コードと前記光ディスクドライブ内で管理される第２キー値のドライブキーの組合により計算される有効なキー（Ｖａｌｉｄ　Ｋｅｙ）値により、読み出されて復号化される。したがって、複写防止情報の保安性が向上する。

【００２０】

また、前記光ディスクドライブのキー計算部５１は、図３に示したように、前記ヒドン・コードとドライブキーの組合によりキーロッカーを解除することができる有効なキーを計算する計算部（Ｃａｌｃｕｌａｔｉｏｎ）（未符号）と、前記計算された有効キーを利用して前記キーロッカー内に暗号化して記録されたディスクキーを復号化する復号化部（Ｄｅｃｒｙｐｔｉｏｎ）（未符号）で構成されることができる。

【００２１】

前記ドライブキー（Ｄｒｉｖｅ　Ｋｅｙ）は、光ディスクドライブによって相異なるキー値で管理されることができることであって、例えば光ディスクドライブを製造したメーカー別ＩＤ（Ｄｒｉｖｅ　Ｍａｋｅｒ_ＩＤ）にしたがって区分される固有のキー値で管理されることができる。

【００２２】

一方、前記光ディスクドライブ５００は、図４に示したように、保安認証チャネル（Ｓ

ＡＣ：Ｓｅｃｕｒｅ Ａｕｔｈｅｎｔｉｃａｔｅｄ Ｃｈａｎｎｅｌ）７０を介してデータを送受信するようになるアプリケーション６００、例えば個人用コンピューター等と連結されて使われることができる。前記アプリケーション６００には、前記保安認証チャネルを介して受信されたＡ／Ｖデータをデコーディングするための Ａ／Ｖデコーダー６０が含まれる。

【００２３】

また、前記アプリケーション６００内にはアプリケーションキー６１が管理されて、前記光ディスクドライブ５００内にはアプリケーションキーモジュール５３が含まれることができる。この場合、前記アプリケーションキーモジュール５３では、前記アプリケーション内で管理されるアプリケーションキー６１を前記保安認証チャネル７０を介して受信した後、前記キー計算部５１に提供するようになる。

【００２４】

前記光ディスクドライブのキー計算部５１では、光ディスク４００から読み出される第１キー値のヒドン・コードと光ディスクドライブまたはアプリケーション内で管理される第２キー値のドライブキーまたはアプリケーションキーを組み合わせて、前記光ディスクに記録されたキーロッカー内のディスクキーを読み出して復号化するようになる。

【００２５】

そして、前記復号化部５０では、前記ディスクキーを利用して、光ディスクのデータ領域に暗号化して記録されたオーディオ及びビデオデータを復号化する一連の動作を遂行した後、前記保安認証チャネル（ＳＡＣ）７０を介してオーディオ及びビデオデータをアプリケーション６００で出力するようになる。

【００２６】

前記アプリケーションに含まれたＡ／Ｖデコーダー６０では、前記のような過程を介して受信されるオーディオ及びビデオデータをデコーディングしてオーディオ及びビデオで復元するようになる。このような過程を介して、光ディスクに記録されたオーディオ及びビデオデータが正常的に再生される。

【００２７】

一方、前記アプリケーション内に含まれるＡ／Ｖデコーダー６０は、図５に示したように、光ディスクドライブ５００内に含まれることができる。この場合、前記光ディスクドライブでは、前記保安認証チャネル７０を介して、アプリケーション６００でデコーディングが完了したオーディオ及びビデオデータを出力するようになるので、図４に示したように、オーディオ及びビデオのビットストリームをアプリケーションで直接伝送する場合に比べて、複写防止情報のハッキング危険性を減少させることができるようになる。

【００２８】

そして、前記のような場合、光ディスクドライブ５００内には、図５に示したように、アプリケーションキーモジュール５３ではないドライブキー５２が管理される。

【００２９】

参考に、前記ヒドン・コードは、光ディスク上に低周波成分を有する物理的なウォーブル（Ｗｏｂｂｌｅ）形状またはＷｏｂｂｌｅ ｐｒｅ－ｐｉｔ ｔｙｐｅ等で記録されて、ビット対ビット（Ｂｉｔ ｔｏ Ｂｉｔ）複写により不法複製されない。また、前記ドライブキー、キーロッカーに含まれるディスクキー等も前記ヒドン・コードのようにリードイン領域上に低周波成分を有する物理的なウォーブル形状またはＷｏｂｂｌｅ ｐｒｅ－ｐｉｔ ｔｙｐｅで記録されることができる。一方、前記ヒドン・コードとドライバーキーにより暗号化するキーロッカー内には、ディスクキーのような複写防止情報以外にも、多様な付加情報が暗号化して記録されることができる。

【００３０】

例えば、図６に示したように、前記光ディスクのキーロッカーには、複写防止情報以外にも、キー更新情報（Ｋｅｙ Ｒｅｎｅｗａｌ Ｉｎｆｏｒｍａｔｉｏｎ）が付加的に暗号化して記録されることができる。前記キー更新情報には、図７及び図８に示したように、光ディスクドライブを製造したメーカー情報（Ｄｒｉｖｅ Ｍａｋｅｒ）、各メーカー

別ドライブキー（Ｄｒｉｖｅ　Ｋｅｙ）、そしてドライブキーの有効可否を示すためのフラッグ（Ｖａｌｉｄ　Ｆｌａｇ）が連係記録されたり、またはアプリケーションを製造したメーカー情報（Ａｐｐｌｉｃａｔｉｏｎ　Ｍａｋｅｒ）、各メーカー別アプリケーションキー（Ａｐｐｌｉｃａｔｉｏｎ　Ｋｅｙ）、そしてアプリケーションキーの有効可否を示すためのフラッグ（Ｖａｌｉｄ　Ｆｌａｇ）が連係記録されることができる。

【００３１】

そして、特定メーカーで製造した光ディスクドライブ５００またはアプリケーション６００が無断で不法複製された場合、特に前記複写防止システムに従わなければならないドライブ製造業者が権利者（Ｌｉｃｅｎｓｏｒ）からライセンス契約を結ばないでドライブを生産する場合、前記不法複製されたまたはライセンスがない光ディスクドライブまたはアプリケーションのドライブキーまたはアプリケーションキーがこれ以上有効に作用することができないように、その以後から新しく製作される光ディスクには新しいキー更新情報を記録するようになる。

【００３２】

例えば、‘ＡＡＡ’メーカーで製造した光ディスクドライブに‘０ｘ００００’ドライブキーが記録されている状態で前記光ディスクドライブが不法複製された場合、光ディスクを製作するコンテンツ提供業者は、図７に示したように、新しく製作される光ディスク内に記録されるキー更新情報のうち、‘ＡＡＡ’メーカーの‘０ｘ００００’ドライブキーが有効でないことを示すために、そのフラッグビット値を‘０’に設定して、前記ＡＡＡメーカー及び‘０ｘ００００’ドライブキー情報に連係記録するようになる。

【００３３】

そして、新しく製作された光ディスクドライブで管理されるドライブキー、例えば‘０ｘ０００１’と前記ドライブキーが有効であるということを示すために‘１’に設定したフラッグビットを前記キー更新情報内に‘ＡＡＡ’メーカー情報に連係記録するようになる。

【００３４】

一方、前記新しく製作された光ディスクドライブのキー計算部５１では、光ディスク４００から読み出されるヒドン・コードと光ディスクドライブまたはアプリケーション内で管理されるドライブキーまたはアプリケーションキーを組み合わせて、前記キーロッカー内のキー更新情報を読み出すようになる。

【００３５】

そして、前記読み出されたキー更新情報に含まれたメーカー情報、各メーカー別ドライブキーまたはアプリケーションキー、そしてドライブキーまたはアプリケーションキーの有効可否を示すフラッグビットを参照して、前記キーロッカー内に記録された複写防止情報を読み出し及び復号化するようになる。

【００３６】

前記光ディスクドライブまたはアプリケーション内で管理されるドライブキーまたはアプリケーションキーが‘０ｘ０００１’の場合、前記読み出されたキー更新情報に含まれたフラッグビットが‘１’であるので、光ディスクドライブまたはアプリケーション内で管理されるドライブキーまたはアプリケーションキーが有効だと判断する。したがって、前記複写防止情報を正常的に読み出し及び復号化して、光ディスクのデータ領域に暗号化して記録されたオーディオ及びビデオデータの再生動作を正常的に遂行する。

【００３７】

反面、前記光ディスクドライブまたはアプリケーション内で管理されるドライブキーまたはアプリケーションキーが‘０ｘ００００’の場合には、前記読み出されたキー更新情報に含まれたフラッグビットが‘０’であるので、前記ドライブキーまたはアプリケーションキーが有効でないと判断する。したがって、前記複写防止情報を正常的に読み出し及び復号化しなくなって、光ディスクのデータ領域に暗号化して記録されたオーディオ及びビデオデータの再生動作が正常的に遂行されなくなる。

【００３８】

この場合、前記複写防止情報も、ヒドン・コードと前記ドライブキーまたはアプリケーションの組合により、復号化される。しかし、前記キー更新情報に含まれたフラッグビットにより光ディスクドライブまたはアプリケーション内で管理されるドライブキーまたはアプリケーションキーが有効だと判断した場合、前記復号化なしに前記複写防止情報を得るようにすることができる。

【００３９】

前記のように構成される本発明は、複写防止情報に対する保安性をさらに向上させて、光ディスクドライブの不法複製を効率的に抑制して、不法複製された光ディスクドライブを無力化する効果がある。特にライセンスなしに生産されたドライブに対して光ディスクを再生することができないようにする。また、本発明はすべてのメーカーの光ディスクドライブが一度に複製されることを未然に防止することができる。

【００４０】

以上前述した本発明の望ましい実施形態は例示の目的のために開示されたものであって、当業者ならば添付された特許請求範囲に開示された本発明の技術的思想とその技術的範囲内でまた他の多様な実施形態を改良、変更、代替または付加などが可能であることである。

【図面の簡単な説明】

【００４１】

【図１】一般的なＤＶＤの複写防止情報管理方法が適用される光ディスクドライブとアプリケーションに対する構成を示したものである。

【図２】本発明による記録媒体の複写防止情報管理方法が適用される光ディスクドライブに対する構成を示したものである。

【図３】本発明による記録媒体の複写防止情報管理方法が適用される光ディスクドライブに対する構成を示したものである。

【図４】本発明による記録媒体の複写防止情報管理方法が適用される光ディスクドライブとアプリケーションに対する他の実施形態の構成を示したものである。

【図５】本発明による記録媒体の複写防止情報管理方法が適用される光ディスクドライブとアプリケーションに対する他の実施形態の構成を示したものである。

【図６】本発明による光ディスクのキーロッカー内に付加記録されたキー更新情報に対する実施形態を示したものである。

【図７】本発明による光ディスクのキーロッカー内に付加記録されたキー更新情報に対する実施形態を示したものである。

【図８】本発明による光ディスクのキーロッカー内に付加記録されたキー更新情報に対する実施形態を示したものである。

【図１】

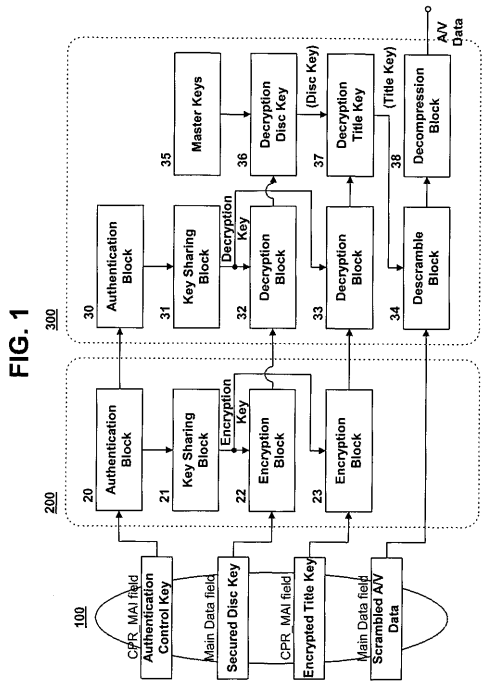


FIG. 1
A/V Data
Master Keys
Decryption Disc Key
(Disc Key)
Decryption Title Key
(Title Key)
Decompression Block
35
36
37
38
Authentication Block
Key Sharing Block
Decryption Key
Decryption Block
Decryption Block
Descramble Block
30
31
32
33
34
300
Authentication Block
Key Sharing Block
Encryption Key
Encryption Block
Encryption Block
20
21
22
23
200
100
CPR_MAI field
Authentication Control Key
Main Data field
Secured Disc Key
CPR_MAI field
Encrypted Title Key
Main Data field
Scrambled A/V Data

【図２】

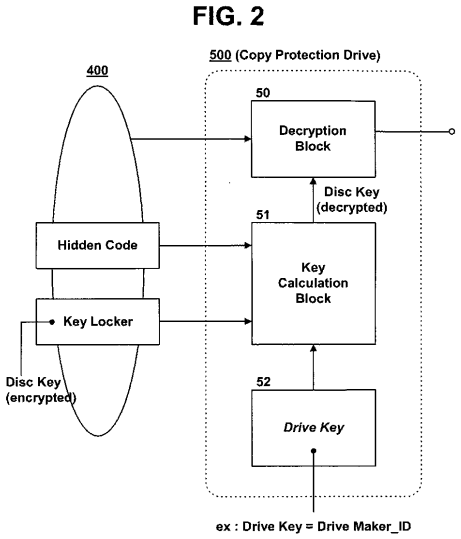


FIG. 2
500 (Copy Protection Drive)
400
50
Decryption Block
Disc Key (decrypted)
51
Hidden Code
Key Calculation Block
Key Locker
52
Drive Key
Disc Key (encrypted)
ex : Drive Key = Drive Maker_ID

【図３】

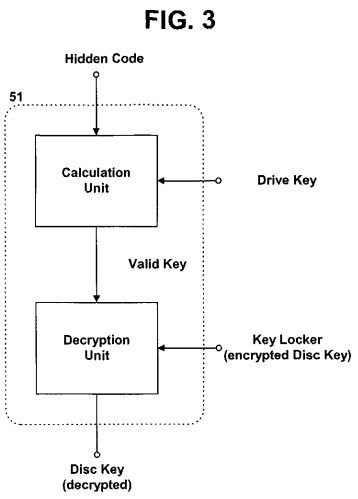


FIG. 3
Hidden Code
51
Calculation Unit
Drive Key
Valid Key
Decryption Unit
Key Locker (encrypted Disc Key)
Disc Key (decrypted)

【図４】

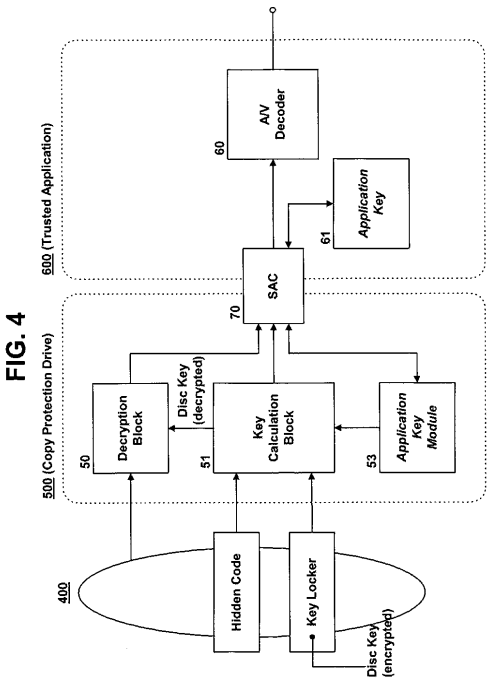
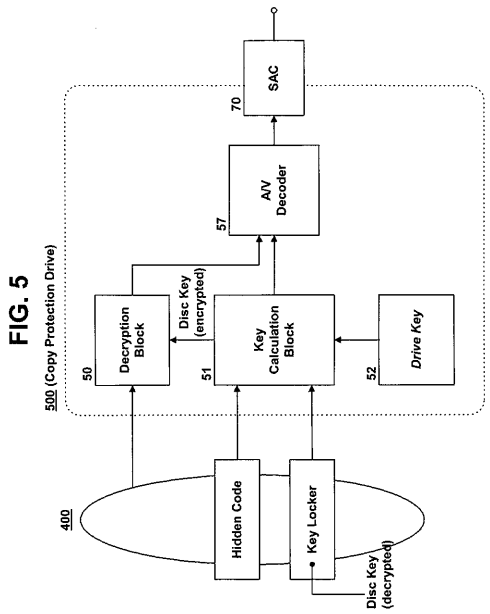


FIG. 4
600 (Trusted Application)
A/V Decoder
60
Application Key
61
SAC
70
500 (Copy Protection Drive)
Decryption Block
50
Disc Key (decrypted)
Key Calculation Block
51
Application Key Module
53
400
Hidden Code
Key Locker
Disc Key (encrypted)

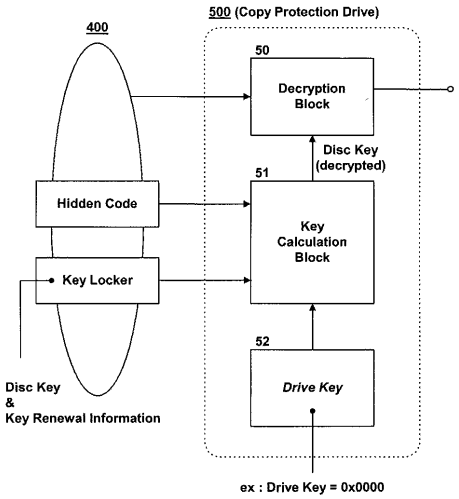
【図５】

FIG. 5



【図６】

FIG. 6



【図７】

FIG. 7

Key Renewal Information

Drive Maker	Drive Key	Valid_Flag	
AAA	0x0000	0	Not Valid
	0x0001	1	Valid
	⋮	⋮	
BBB	0x0010	1	
	0x0011	1	
	⋮	⋮	
CCC	0x0010	1	
	0x0011	1	
	⋮	⋮	
⋮	⋮	⋮	

【図８】

FIG. 8

Key Renewal Information

Application Maker	*Application Key*	Valid_Flag	
AAA	0x0000	0	Not Valid
	0x0001	1	Valid
	⋮	⋮	
BBB	0x0010	1	
	0x0011	1	
	⋮	⋮	
CCC	0x0010	1	
	0x0011	1	
	⋮	⋮	
⋮	⋮	⋮	

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2004/000951

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G11B 7/0045

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G11B, G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, PAJ"copy protection""encrypt""decrypt"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6289102 B1(Matsushita Electric Industrial Co. Ltd.) 11 September 2001 See abstract and claims 28.	1-13
Y	US 6134201 A(Sony Corp.) 17 October 2000. See claims 5-7 and 14-19.	1-13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 AUGUST 2004 (10.08.2004)	12 AUGUST 2004 (12.08.2004)

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	SONG, Jin Suk Telephone No. 82-42-481-5694

Form PCT/ISA/210 (second sheet) (January 2004)

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	G06F 12/14 550B	

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 キム, ビュン, ジン
大韓民国, ４６３－０１０, キュンギード, サンナム, ブンダン－ギュ, ジェオンジャドン, １１０, ハンソル チェング アパートメント, １１１－２０４
(72)発明者 キム, ヒュン, サン
大韓民国, ソウル １３０－８７８, ドンダエモン－ギュ, ヒュイギュン ２－ドン, ２８６－２６６

Ｆターム(参考) 5B017 AA06 CA09
5C052 AA02 CC01 DD04
5C053 FA13 FA24 GB06
5D044 AB05 AB07 BC02 CC06 DE17 FG18 GK12 GK17
5J104 EA09 EA16 EA20 PA14