(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2005-502975

(P2005-502975A)

(43)公表日　平成17年1月27日(2005.1.27)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11B 20/10	G11B 20/10	H	5B017
G06F 12/14	G06F 12/14	320E	5D044
G11B 7/004	G11B 7/004	C	5D090
G11B 7/005	G11B 7/005	Z	
G11B 7/007	G11B 7/007		

審査請求 未請求　予備審査請求 有　（全 67 頁）　最終頁に続く

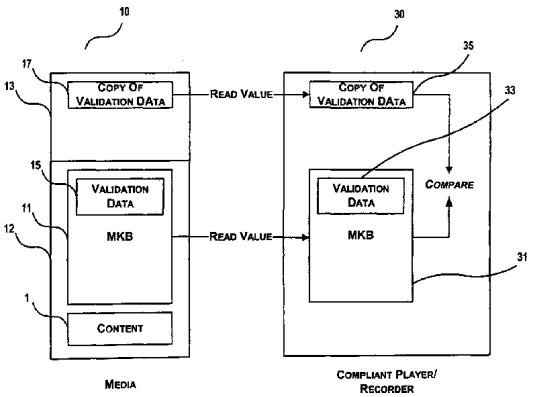
(21)出願番号　特願2002-555413(P2002-555413)
(86)(22)出願日　平成13年12月21日(2001.12.21)
(85)翻訳文提出日　平成15年6月30日(2003.6.30)
(86)国際出願番号　PCT/US2001/049784
(87)国際公開番号　WO2002/054401
(87)国際公開日　平成14年7月11日(2002.7.11)
(31)優先権主張番号　09/750,642
(32)優先日　平成12年12月28日(2000.12.28)
(33)優先権主張国　米国(US)
(31)優先権主張番号　09/823,718
(32)優先日　平成13年3月30日(2001.3.30)
(33)優先権主張国　米国(US)
(31)優先権主張番号　09/973,547
(32)優先日　平成13年10月9日(2001.10.9)
(33)優先権主張国　米国(US)

(71)出願人　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　100064621
弁理士　山川　政樹
(72)発明者　リプリー，マイク
アメリカ合衆国・９７１２４・オレゴン州・ヒルズボロ・ノースイースト　５６ティエイチ　コート・１２２２
(72)発明者　カトウ，タク
〒２４８－０００３神奈川県鎌倉市浄明寺３－１２－２０

最終頁に続く

(54)【発明の名称】媒体のカッティング領域に妥当性検査データを格納することによるメディア・キー・ブロックの保全性の検証

(57)【要約】
ＤＶＤ－ＲまたはＤＶＤ－ＲＷなどの媒体のカッティング領域に妥当性検査データを格納することにより、メディア・キー・ブロック（ＭＫＢ）の保全性を検証するための方法。一実施形態では、妥当性検査データはメディア・キー・ブロック上にハッシュ関数を含む。他の実施形態では、ＭＫＢのメディア・キー検証レコードの妥当性検査データ・フィールドである。



【特許請求の範囲】
【請求項１】
媒体の第１の部分からメディア・キー・ブロックを読み取ること、
媒体の第２の部分からメディア・ブロックに関する妥当性検査データを読み取ること、および
妥当性検査データを使用してメディア・キー・ブロックの妥当性を検査すること
を含む方法。
【請求項２】
前記妥当性検査データを使用するメディア・キー・ブロックの妥当性検査が、
メディア・キー・ブロックと妥当性検査データとを比較すること、および
メディア・キー・ブロックが妥当性検査データに対応する場合は、コンテンツへのアクセスを許可することを含む請求項１に記載の方法。
【請求項３】
メディア・キー・ブロックが妥当性検査データと一致する場合、メディア・キー・ブロックは妥当性検査データに対応するものである請求項２に記載の方法。
【請求項４】
メディア・キー・ブロックを介したハッシュ関数が妥当性検査データと一致する場合、メディア・キー・ブロックは妥当性検査データに対応するものである請求項２に記載の方法。
【請求項５】
妥当性検査データがメディア・キー・ブロックのハッシュ関数を含み、前記メディア・キー・ブロックの妥当性検査が、
妥当性検査データを介したメッセージ認証コード（ＭＡＣ）を使用して第１のＭＡＣを算出すること、
媒体の読取り専用領域から読み取ったメディア・キー・ブロックを介したハッシュ関数を使用することによって、読取り器ＭＫＢを算出すること、
読取り器ＭＫＢを介したＭＡＣアルゴリズムを使用して第２のＭＡＣを算出すること、
第１のＭＡＣと第２のＭＡＣとを比較すること、および
第１のＭＡＣが第２のＭＡＣと一致する場合、ＭＫＢの真正性を検証することを含む請求項４に記載の方法。
【請求項６】
媒体がＤＶＤ－ＲＡＭ（デジタル汎用ディスク－ランダム・アクセス・メモリ）を含み、第２の部分が媒体の制御データ領域を含む請求項１に記載の方法。
【請求項７】
媒体がＤＶＤ－Ｒ（デジタル汎用ディスク－記録可能）を含み、第２の部分が媒体のナロー・バースト・カッティング領域を含む請求項１に記載の方法。
【請求項８】
媒体がＤＶＤ－ＲＷ（デジタル汎用ディスク－再書込み可能）を含み、第２の部分が媒体のナロー・バースト・カッティング領域を含む請求項１に記載の方法。
【請求項９】
第１のデバイスで、
媒体の読取り専用領域に格納されたメディア・キー・ブロックを読み取ること、および
メディア・キー・ブロックのハッシュ関数に等しい第１の妥当性検査データを読み取ることを含み、妥当性検査データは媒体の読取り専用領域のカッティング領域に格納されており、
さらに第１のＭＡＣを形成するために、第１の妥当性検査データを介して媒体認証コード（ＭＡＣ）アルゴリズムを算出することを含み、
第２のデバイスで、
媒体の読取り専用領域から読み取られたメディア・キー・ブロックのハッシュ関数に等しい第２の妥当性検査データを算出すること、

第２のＭＡＣを形成するために、第２の妥当性検査データを介して媒体認証コード（ＭＡＣ）アルゴリズムを算出すること、
第１のＭＡＣと第２のＭＡＣとを比較すること、および
第１のＭＡＣが第２のＭＡＣと等しい場合、媒体の読取り専用領域から読み取られたメディア・キー・ブロックの真正性を検証すること
を含む方法。
【請求項１０】
媒体がＤＶＤ－Ｒ（デジタル汎用ディスク－記録可能）を含み、第２の部分が媒体のナロー・バースト・カッティング領域を含む請求項９に記載の方法。
【請求項１１】
媒体がＤＶＤ－ＲＷ（デジタル汎用ディスク－再書込み可能）を含み、第２の部分が媒体のナロー・バースト・カッティング領域を含む請求項９に記載の方法。
【請求項１２】
媒体の読取り専用領域の第１の部分からメディア・キー・ブロックを読み取ること、
メディア・キー・ブロックからメディア・キーを生成すること、
媒体の読取り専用領域の第２の部分からメディア・キー・ブロックに関する妥当性検査データを読み取ること、
メディア・キーを使用して妥当性検査データを復号すること、および
妥当性検査データが事前に定義された値に復号した場合、メディア・キー・ブロックの真正性を検証すること
を含む方法。
【請求項１３】
妥当性検査データが、メディア・キー・ブロックのメディア・キー検証レコードの検証データ・フィールドを含む請求項１２に記載の方法。
【請求項１４】
事前に定義された値が、ＤＥＡＤＢＥＥＦに等しい１６進値を含む請求項１２に記載の方法。
【請求項１５】
読取り専用領域の第２の部分が媒体のカッティング領域を含む請求項１２に記載の方法。
【請求項１６】
媒体が、記録可能媒体用コンテンツ保護（ＣＰＲＭ）フォーマットを使用して保護される請求項１５に記載の方法。
【請求項１７】
カッティング領域がバースト・カッティング領域を含み、媒体が、
ＤＶＤ－Ｒ（デジタル汎用ディスク－記録可能）と、
ＤＶＤ－ＲＷ（デジタル汎用ディスク－再書込み可能）のうちの１つである請求項１６に記載の方法。
【請求項１８】
読み取られる媒体に関連付けられた媒体タイプを決定すること、
媒体の第１の部分からメディア・キー・ブロックを読み取ること、
決定された媒体タイプに基づいた媒体の第２の領域からメディア・ブロックに関する妥当性検査データを読み取ること、および
妥当性検査データを使用してメディア・キー・ブロックを妥当性検査すること
を含む方法。
【請求項１９】
前記妥当性検査データを使用したメディア・キー・ブロックの妥当性検査が、
メディア・キー・ブロックと妥当性検査データを比較すること、および
メディア・キー・ブロックが妥当性検査データに対応する場合は、コンテンツへのアクセスを許可することを含む請求項１８に記載の方法。
【請求項２０】

媒体のタイプが、
ＤＶＤ－Ｒ（デジタル汎用ディスク－記録可能）と、
ＤＶＤ－ＲＷ（デジタル汎用ディスク－再書込み可能）のうちの１つを含み、
第２の部分が媒体の読取り専用領域のバースト・カッティング領域部分を含む請求項１８に記載の方法。
【請求項２１】
媒体のタイプがＤＶＤ－ＲＡＭ（デジタル汎用ディスク－ランダム・アクセス・メモリ）を含み、第２の部分が媒体の読取り専用領域の制御データ領域を含む請求項１８に記載の方法。
【請求項２２】
命令のシーケンスを表すデータを格納したマシン読取り可能媒体であって、命令のシーケンスが処理装置によって実行されると、処理装置に、
媒体の第１の部分からメディア・キー・ブロックを読み取ること、
媒体の第２の部分からメディア・キー・ブロックに関する妥当性検査データを読み取ること、および
妥当性検査データを使用してメディア・キー・ブロックを妥当性評価すること
を実行させるマシン読取り可能媒体。
【請求項２３】
前記妥当性検査データを使用するメディア・キー・ブロックの妥当性評価が、
メディア・キー・ブロックと妥当性検査データとを比較すること、および
メディア・キー・ブロックが妥当性検査データに対応する場合は、コンテンツへのアクセスを許可することを含む請求項２２に記載のマシン読取り可能媒体。
【請求項２４】
メディア・キー・ブロックが妥当性検査データと一致する場合、メディア・キー・ブロックは妥当性検査データに対応するものである請求項２３に記載のマシン読取り可能媒体。
【請求項２５】
メディア・キー・ブロックを介したハッシュ関数が妥当性検査データと一致する場合、メディア・キー・ブロックは妥当性検査データに対応するものである請求項２３に記載のマシン読取り可能媒体。
【請求項２６】
命令のシーケンスを表すデータを格納したマシン読取り可能媒体であって、命令のシーケンスが処理装置によって実行されると、処理装置に、
媒体の読取り専用領域の第１の部分からメディア・キー・ブロックを読み取ること、
メディア・キー・ブロックからメディア・キーを生成すること、
媒体の読取り専用領域の第２の部分からメディア・キー・ブロックに関する妥当性検査データを読み取ること、
メディア・キーを使用して妥当性検査データを復号すること、および
妥当性検査データが事前に定義された値に復号した場合、メディア・キー・ブロックの真正性を検証すること
を実行させるマシン読取り可能媒体。
【請求項２７】
妥当性検査データが、メディア・キー・ブロックのメディア・キー検証レコードの検証データ・フィールドを含む請求項２６に記載のマシン読取り可能媒体。
【請求項２８】
読取り専用領域の第２の部分が媒体のカッティング領域を含む請求項２６に記載のマシン読取り可能媒体。
【請求項２９】
媒体の書込み可能領域と、
媒体の書込み可能領域に格納されたコンテンツと、
カッティング領域部分と非カッティング領域部分とを有する媒体の読取り専用領域と、

非カッティング領域部分に格納されたメディア・キー・ブロックと、
カッティング領域部分に格納されたメディア・キー・ブロックの真正性を検証するための妥当性検査データと
を含むマシン読取り可能媒体。
【請求項３０】
妥当性検査データが暗号化された事前に選択された値を含む請求項２９に記載のマシン読取り可能媒体。
【請求項３１】
暗号化された事前に選択された値が、メディア・キー・ブロックのメディア・キー検証レコードを含む請求項３０に記載のマシン読取り可能媒体。
【請求項３２】
妥当性検査データが、メディア・キー・ブロックを介したハッシュ関数を含む請求項２９に記載のマシン読取り可能媒体。
【請求項３３】
妥当性検査データが、メディア・キー・ブロックのメディア・キー検証レコードの検証データ・フィールドのコピーを含む請求項２９に記載のマシン読取り可能媒体。
【請求項３４】
媒体がデジタル汎用ディスク（ＤＶＤ）を含む請求項２９に記載のマシン読取り可能媒体。
【請求項３５】
書込み可能領域と、
書込み可能領域に格納されたコンテンツと、
カッティング領域部分と非カッティング領域部分とを有する読取り専用領域と、
非カッティング領域部分に格納されたメディア・キー・ブロックと、
カッティング領域部分に格納されたメディア・キー・ブロックの真正性を検証するためのメディア・キー・ブロックのハッシュ関数に等しい第１の妥当性検査データとを有する、媒体と、
媒体の読取り専用領域に格納されたメディア・キー・ブロックを読み取るため、
カッティング領域部分から第１の妥当性検査データを読み取るため、および
第１のＭＡＣを形成するために、第１の妥当性検査データを介して媒体認証コード（ＭＡＣ）アルゴリズムを算出するための、
ドライブと、
媒体の読取り専用領域から読み取られたメディア・キー・ブロックのハッシュ関数に等しい第２の妥当性検査データを算出するため、
第２のＭＡＣを形成するために、第２の妥当性検査データを介して媒体認証コード（ＭＡＣ）アルゴリズムを算出するため、
第１のＭＡＣと第２のＭＡＣとを比較するため、および
第１のＭＡＣが第２のＭＡＣと等しい場合、媒体の読取り専用領域から読み取られたメディア・キー・ブロックの真正性を検証するための、
ホストとを含むシステム。
【請求項３６】
媒体が、
ＤＶＤ－Ｒ（デジタル汎用ディスク－記録可能）と、
ＤＶＤ－ＲＷ（デジタル汎用ディスク－再書込み可能）のうちの１つを含む請求項３５に記載のシステム。
【請求項３７】
カッティング領域部分が媒体の読取り専用領域のナロー・バースト・カッティング領域部分を含む請求項３６に記載のシステム。
【請求項３８】
書込み可能領域と、

書込み可能領域に格納されたコンテンツと、
カッティング領域部分と非カッティング領域部分とを有する読取り専用領域と、
非カッティング領域部分に格納されたメディア・キー・ブロックと、
カッティング領域部分に格納されたメディア・キー・ブロックの真正性を検証するための妥当性検査データとを有する、
媒体と、
媒体の読取り専用領域の第１の部分からメディア・キー・ブロックを読み取るため、
メディア・キー・ブロックからメディア・キーを生成するため、
媒体の読取り専用領域の第２の部分からメディア・キー・ブロックに関する妥当性検査データを読み取るため、
メディア・キーを使用して妥当性検査データを復号するため、および
妥当性検査データが事前に定義された値に復号した場合、メディア・キー・ブロックの真正性を検証するための、
デバイスとを含むシステム。
【請求項３９】
デバイスが大衆消費電子デバイスを含む請求項３８に記載のシステム。
【請求項４０】
媒体がＤＶＤ－Ｒ（デジタル汎用ディスク－記録可能）を含み、第２の部分が媒体のナロー・バースト・カッティング領域を含む請求項３８に記載のシステム。
【請求項４１】
媒体がＤＶＤ－ＲＷ（デジタル汎用ディスク－再書込み可能）を含み、第２の部分が媒体のナロー・バースト・カッティング領域を含む請求項３８に記載のシステム。
【請求項４２】
媒体の読取り専用領域の第１の部分からメディア・キー・ブロックを読み取る手段と、
メディア・キー・ブロックからメディア・キーを生成する手段と、
媒体の読取り専用領域の第２の部分からメディア・キー・ブロックに関する妥当性検査データを読み取る手段と、
メディア・キーを使用して妥当性検査データを復号する手段と、
妥当性検査データが事前に定義された値に復号した場合、メディア・キー・ブロックの真正性を検証する手段と
を含む装置。
【請求項４３】
妥当性検査データが、メディア・キー・ブロックのメディア・キー検証レコードの検証データ・フィールドを含む請求項４２に記載の装置。
【請求項４４】
読取り専用領域の第２の部分が媒体のカッティング領域を含む請求項４２に記載の装置。
【発明の詳細な説明】
【関連技術】
【０００１】
本明細書は、２０００年１２月２８日付出願の「ＭＥＴＨＯＤ　ＡＮＤ　ＡＰＰＡＲＡＴＵＳ　ＦＯＲ　ＶＥＲＩＦＹＩＮＧ　ＴＨＥ　ＩＮＴＥＧＲＩＴＹ　ＯＦ　Ａ　ＭＥＤＩＡ　ＫＥＹ　ＢＬＯＣＫ」と題する現在同時係属中の米国特許出願第０９／７５０６４２号の一部継続出願である。
【０００２】
（著作権通知）
本明細書の内容は、著作権保護を対象とする資料である。著作権所有者は、特許商標庁の特許ファイルまたは記録に記載されている場合は、何人による特許開示の複製に対しても意義を唱えるものではないが、そうでない場合はいかなる無断転載も禁ずる。
【技術分野】
【０００３】

本発明は、静的および動的な情報の格納および取出しに関する。より詳細に言えば、本発明は格納された情報への未許可のアクセスを防止するための方法、装置、およびシステムに関する。

【背景技術】

【０００４】

情報またはコンテンツは、様々な媒体に格納することができる。格納された情報へのアクセスおよびこれらのコピーの速度および利便性が上がるに従って、情報が未許可でコピーされるおそれが増えてきた。格納された情報への未許可のアクセスを防止するために、これまで様々な方式が採られてきた。たとえば、媒体に格納されたコンテンツは、媒体へのアクセスが許可されたデバイスだけが知る１つまたは複数の秘密鍵で暗号化することである。鍵が１つだけの場合の欠点は、鍵を変えることによって特定のデバイスの許可を無効にするには、媒体を読み取るすべてのデバイスへの許可を無効にしなければならないという点である。複数の鍵を使用する場合のいくつかの欠点の中には、特定のデバイスそれぞれが鍵を伝送および格納するために潜在的に大きな負担を強いられるという点が含まれる。

【０００５】

コンテンツの未許可のコピーを防止するために開発された代替方法は、４Ｃ　Ｅｎｔｉｔｙ，ＬＬＣの「ＣＯＮＴＥＮＴ　ＰＲＯＴＥＣＴＩＯＮ　ＦＯＲ　ＲＥＣＯＲＤＡＢＬＥ　ＭＥＤＩＡ　ＳＰＥＣＩＦＩＣＡＴＩＯＮ」Ｒｅｖｉｓｉｏｎ　０．９４（２０００年１０月１８日）という名称の出版物に記載されているように、コンテンツのコピーを許可するためにメディア・キー・ブロック（ＭＫＢ）を使用する。許可されたデバイスは、以下で部分的に記載するように、許可されたデバイスがコンテンツをコピーできるようにするメディア・キーを算出するためにＭＫＢを処理する。ＭＫＢ方法とは、メディア・ユニーク・キーを使用して、暗号化されたコンテンツを再生元となる媒体に結びつけるものである。

【０００６】

鍵が損傷したり無効にされたりすると、ＭＫＢは非常に大規模になり、数メガバイトにのぼるものも珍しくない。媒体には読取り専用スペースが限られているタイプのものが多いため、ＭＫＢを媒体の書込み可能領域に格納する必要が生じる。ＭＫＢを書込み可能領域に格納すると、悪意による不正変更をさそうため脆弱性が生じる。こうした直接攻撃の場合、不正変更者の意図は、媒体に格納された現在のＭＫＢを古いＭＫＢに置き換えようとするものであることが多い。あるいは不正変更者は、媒体に格納された現在のＭＫＢの一部を古いＭＫＢの一部に置き換える場合がある。古いＭＫＢには現在のＭＫＢによって無効にされた鍵が依然として含まれているので、こうして置き換えることにより、現在のＭＫＢが提供するコンテンツ保護を場合によっては損傷させることになる。

【０００７】

たとえＭＫＢが媒体の読取り可能領域に格納されている場合でも、ＭＫＢ方法のもう１つの弱点は、現在のＭＫＢの処理試行中に現在のＭＫＢを古いＭＫＢに置き換えるマン・イン・ザ・ミドル攻撃ができる点である。あるいはマン・イン・ザ・ミドル攻撃者は、現在のＭＫＢの処理試行中に現在のＭＫＢの一部を古いＭＫＢの一部に置き換える場合がある。したがって、マン・イン・ザ・ミドル攻撃は、現在のＭＫＢが提供するコンテンツ保護を場合によっては損傷させる。

【０００８】

有効なＭＫＢのない媒体を読み取ることが可能性であり、未許可の読取り者は保護された媒体に格納されたコンテンツを読み取ることが可能である。ＭＫＢ方法の変形例では、ＭＫＢについてのハッシュ値が算出され、媒体の読取り専用領域に格納される。読取り者はＭＫＢを読み取り、媒体から読み取ったＭＫＢのハッシュ値を算出し、そのハッシュ値と読取り専用領域から読み取ったハッシュ値とを比較する。ただし、ハッシュ値の算出は、許可プロセスに望ましくない遅延を負わせる。したがって、この従来技術を改善することが望ましい。

【０００９】
本発明は、添付の図面において限定的なものとしてではなく例示的なものとして示されており、同じ参照番号は同じ要素を示すものである。
【発明の開示】
【００１０】
発明の一態様では、ＤＶＤ－ＲまたはＤＶＤ－ＲＷなどの媒体のカッティング領域に妥当性検査データを格納することにより、メディア・キー・ブロック（ＭＫＢ）の保全性を検証する方法が開示される。
【００１１】
一実施態様では、妥当性検査データは、ドライブ・ホスト構成内でメディア・キー・ブロック（ＭＫＢ）が検証されるときに、ＤＶＤ－ＲＡＭとの互換性を達成するために、ＭＫＢにハッシュ関数を含むことができる。この実施態様では、ドライブが、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、またはＤＶＤ－ＲＷのいずれかのディスクの制御データ領域（ＣＤＡ）からＭＫＢを読み取る。ドライブを微調整することによって、ドライブはＤＶＤ－ＲＡＭのＣＤＡから、あるいはＤＶＤ－ＲまたはＤＶＤ－ＲＷのナロー・バースト・カッティング領域（ｎａｒｒｏｗ　ｂｕｒｓｔ　ｃｕｔｔｉｎｇ　ａｒｅａ／ＮＢＣＡ）から、ハッシュ値を読み取ることができるようになり、そのためドライブは、以前に確立された手順を使用してＭＫＢの真正性を検証することができるようになる。
【００１２】
他の実施態様では、妥当性検査データは、大衆消費電子製品プレーヤ／レコーダ（以下「ＣＥデバイス」と呼ぶ）によってＭＫＢが検証されるときに、ＤＶＤ－ＲＡＭとの互換性を達成するために、ＭＫＢのメディア・キー検証レコードの検証データ・フィールドを含むことができる。この実施態様では、ＣＥデバイスはディスクのＣＤＡからＭＫＢを読み取る。ドライブを微調整することによって、ドライブはＤＶＤ－ＲＡＭのＣＤＡから、あるいはＤＶＤ－ＲまたはＤＶＤ－ＲＷのナロー・バースト・カッティング領域（ＮＢＣＡ）から、妥当性検査データ・フィールドを読み取ることができ、そのためドライブは、以前に確立された手順を使用してＭＫＢの真正性を検証することができるようになる。
【００１３】
本発明は様々なオペレーションを含むものであり、次にこれらについて説明する。本発明のオペレーションはハードウェア構成要素によって実行可能であるか、または、汎用または特定用途向けの処理装置あるいは命令を使用してプログラムされた論理回路にオペレーションを実行させる際に使用可能なマシン実行可能命令で実施可能である。あるいは、オペレーションは、ハードウェアとソフトウェアの組合せによって実行可能である。
【００１４】
本発明は、本発明に従ってプロセスを実行するために、コンピュータ（または他の電子デバイス）をプログラミングする際に使用可能な命令を格納したマシン読取り可能媒体を含むコンピュータ・プログラム製品として提供することができる。マシン読取り可能媒体は、フロッピー（登録商標）・ディスク、光ディスク、ＣＤ－ＲＯＭ（コンパクト・ディスク読取り専用メモリ）、および光磁気ディスク、ＲＯＭ（読取り専用メモリ）、ＲＡＭ（ランダム・アクセス・メモリ）、ＥＰＲＯＭ（消去可能プログラム可能読取り専用メモリ）、ＥＥＰＲＯＭ（電磁的消去可能プログラム可能読取り専用メモリ）、磁気または光カード、フラッシュ・メモリ、あるいは電子命令の格納に好適な他のタイプの媒体／マシン読取り可能媒体を含むことができるが、これらに限定されるものではない。
【００１５】
さらに本発明は、コンピュータ・プログラム製品としてもダウンロード可能であり、このプログラムは、搬送波または他の伝播媒体で具体化されたデータ信号により、通信リンク（たとえばモデムまたはネットワーク接続）を介して、リモート・コンピュータ（たとえばサーバ）から要求側コンピュータ（たとえばクライアント）に転送することができる。したがって本明細書では、搬送波はマシン読取り可能媒体を含むとみなされる。
【００１６】

本発明の以下の詳細な説明では、本発明を完全に理解するために数多くの特定の細部について述べる。ただし当分野の技術者であれば、本発明がこれらの特定の細部なしに実施可能であることが明らかであろう。他の場合では、本発明の態様を不必要に曖昧なものにしないために、よく知られた方法、手順、構成要素、および回路については詳細に説明しない。

【発明を実施するための最良の形態】

【００１７】

概説

本明細書では、本発明の特徴について論じるために、ある一定の用語が使用される。たとえばコンテンツとは、同報通信またはケーブル・ネットワークなどの、所有者または免許保有者によってプログラミングされた情報のことである。「コンテンツ」は、ビジネス・データ、ニュース、スポーツ、芸術的パフォーマンス、エンターテイメント、広告、ドキュメンタリ、談話、映画、ビデオ、漫画、テキスト、音楽、およびグラフィックスを含む、どんな形のオーディオまたはビジュアル情報であってもよい。

【００１８】

（媒体）

媒体には、マシン（たとえばコンピュータ）が読取り可能な形でコンテンツを提供（すなわち格納および／または伝送）する任意のメカニズムが含まれる。たとえば、マシン読取り可能媒体には、読取り専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、磁気ディスク記憶媒体、光記憶媒体、フラッシュ・メモリ・デバイス、電気、光、音波、または他の形式の伝播信号（たとえば搬送波、赤外線信号、デジタル信号など）などが含まれる。コンテンツは、通常、ＤＶＤ、ＣＤ、フロッピー・ディスク、フラッシュ・メモリ・アレイなどの媒体に暗号化形式で格納することができる。未許可のデバイスまたは無効になった鍵を有するデバイスは、ＭＫＢを首尾よく処理し、ＭＫＢの妥当性を検査し、コンテンツを復号することができないことからアクセス制御が生じる。

【００１９】

（媒体読取り器）

媒体読取り器は、媒体からのコンテンツを読み取る電子デバイスである。媒体読取り器は、媒体からのコンテンツ以外のデータも読み取ることができる。たとえば媒体読取り器は、ＤＶＤドライブまたはプレーヤ、ＣＤドライブまたはプレーヤ、フロッピー・ドライブ、デジタル・テレビジョン、デジタルＶＣＲ、パーソナル・コンピュータのＣＰＵ、フラッシュ・メモリ・セルに結合された処理装置または回路、あるいは媒体に格納されたコンテンツにアクセスすることのできる任意の他の大衆消費電子製品であってよい。ＣＤ－ＲＷドライブなどの媒体への書込みまたは記録も行うデバイスも、媒体読取り器とみなされる。

【００２０】

（記録可能媒体用コンテンツ保護（ＣＰＲＭ））

本発明の実施形態では、媒体読取り器は、コンテンツを保護するための記録可能媒体用コンテンツ保護（ＣＰＲＭ）フォーマットを実装することができる。ＣＰＲＭは、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、およびＤＶＤ－ＲＷを含むがこれらに限定されることのない、いくつかのタイプの物理媒体に格納されたコンテンツを保護するための方法を定義する。デバイス要件については、以下の「メディア・キー・ブロック」と題された項で、より詳細に説明する。

【００２１】

メディア・キー・ブロック

ＭＫＢは一連の連続するレコードとしてフォーマット化される。各レコードはレコード・タイプ・フィールドで始まり、その後にレコード長さフィールドが続く。ＭＫＢとは、データを有するｎ個のＭＫＢパックから構築されるＭＫＢフレームの一部である。各ＭＫＢフレームは、第１のＭＫＢパックすなわちＭＫＢパック＃０の一部であるＭＫＢ記述子で始まる。第１のｎ－１個のＭＫＢパックは、それぞれ完全に充填される。ｎ番目のＭＫＢ

パックは、ゼロ充填された未使用のバイトで終わることができる。

【００２２】

ＭＫＢを処理するために、許可された各デバイスは「ｎ」個のデバイス・キー・セットを受け取る。「ｎ」個のデバイス・キーはＫｄ＿ｉ（ｉ＝０、１、．．．、ｎ－１）と称される。各デバイス・キーについて、ＭＫＢ内に、関連付けられた列と行の値があり、それぞれ列の値（ｉ＝０、１、．．．、ｎ－１の場合のＣｄ＿ｉ）および行の値（ｉ＝０、１、．．．、ｎ－１の場合のＲｄ＿ｉ）と称される。許可されたデバイスは、ＭＫＢの各列については多くても１つのデバイス・キーを有するが、許可されたデバイスは１行あたり複数のデバイスを有することができる。

【００２３】

デバイス・キーならびに関連付けられた行と列の値は秘密が保たれる。デバイス・キーのセットが損傷すると、更新されたＭＫＢが解放され、損傷したデバイス・キーのセットを有するデバイスに、残りの適合デバイスによって算出されるものとは異なるメディア・キーを算出させる。この方法では、損傷したデバイス・キーは新しいＭＫＢによって「無効」とされる。

【００２４】

デバイスは、そのデバイス・キーを使用し、最初から最後まで１つずつＭＫＢのレコードを処理することによって、メディア・キーを算出する。ＭＫＢの処理が完了した後、デバイスは一番新しく算出されたメディア・キーの値をメディア・キーの最終値として使用する。デバイスがＭＫＢによって無効となったデバイス・キーを使用してＭＫＢを正しく処理すると、結果として生じる最終メディア・キーは特殊値０Ｈを有することになる。ここでＨは１６進数を指定する。この特殊値がＭＫＢの正しい最終メディア・キー値であることは決してないため、常にデバイス・キーが無効にされたことを示すものとみなすことができる。デバイスがこの特殊メディア・キー値を算出すると、進行中の認証、再生、またはレコーディング・セッションを停止し、その後のどんな計算においても、そのメディア・キー値は使用しない。

【００２５】

適切にフォーマット化されたＭＫＢは、第１のレコードとして厳密に１つのメディア・キー検証レコード（ＶＭＫＲ）を有する。ＶＭＫＲには、正しい最終メディア・キーで暗号化された１６進値ＤＥＡＤＢＥＥＦが含まれる。ＶＭＫＲの存在は必須であるが、デバイスによるＶＭＫＲの仕様は必須ではない。デバイスは、後続のレコードの処理中に、１６進値ＤＥＡＤＢＥＥＦを毎回チェックしながら、その現在のメディア・キー値を使用してＶＭＫＲの復号を試みることができる。デバイスがＶＭＫＲを首尾よく復号した場合は、デバイスはすでに正しい最終メディア・キー値を算出したことになるため、ＭＫＢの処理を停止する。

【００２６】

適切にフォーマット化されたＭＫＢは、厳密に１つのメディア・キー計算レコード（ＣＭＫＲ）を有する。デバイスは、ＭＫＢの第１のＣＭＫＲ以降に遭遇するＣＭＫＲはどれも無視しなければならない。ＣＭＫＲには列フィールドが含まれる。列フィールドは、以下で説明するように、このレコードで使用されるデバイス・キーに関連する列値を示す。ＣＭＫＲは、各デバイス・キー行に対応する各列に、暗号化されたキー・データも含む。ＣＭＫＲを処理する前に、デバイスは、デバイスが関連付けられた列値Ｃｄ＿ｉ＝＝ｃｏｌｕｍｎ（ｉは何らかの値）を備えたデバイス・キーを有することを確認する。

【００２７】

デバイスが関連付けられた列値を備えたデバイス・キーを有していない場合、デバイスはＣＭＫＲの残りを無視する。そうでなければ、上記の条件からの値ｉ、デバイス・キー、およびｒ＝Ｒｄ＿ｉ、ｃ＝Ｃｄ＿ｉを使用して、デバイスは、行ｒ＝Ｒｄ＿ｉについて暗号化されたキー・データからメディア・キー値を復号する。結果として生じるメディア・キー値が現在のメディア・キー値となる。

【００２８】

適切にフォーマット化されたＭＫＢは、ゼロまたはそれ以上の条件付きメディア・キー計算レコード（Ｃ－ＣＭＫＲ）を有する。Ｃ－ＣＭＫＲには暗号化された条件付きデータが含まれる。列では、Ｃ－ＣＭＫＲには二重に暗号化されたキー・データが含まれる。首尾よく復号されると、以下に示すように、暗号化された条件付きデータには、１６進値ＤＥＡＤＢＥＥＦ、およびこのＣ－ＣＭＫＲで使用されるデバイス・キーの関連する列値が含まれる。デバイスはこの現在のメディア・キー値を使用して、暗号化された条件付きデータから条件付きデータを復号する。

【００２９】

レコード・プロセスを続行する前に、デバイスは、復号された条件付きデータが１６進値ＤＥＡＤＢＥＥＦを含むこと、およびデバイスが条件付きデータから復号された新しく関連付けられた列値（ｉ）を備えたデバイス・キーを有すること、という条件に当てはまるかどうかをチェックする。これらの条件のうちいずれかに当てはまらない場合、デバイスはＣ－ＣＭＫＲの残りを無視する。そうでなければ、上記の条件からの値ｉ、現在のメディア・キー値、およびｒ＝Ｒｄ＿ｉ、ｃ＝Ｃｄ＿ｉを使用して、デバイスは、Ｃ－ＣＭＫＲの関連付けられた列で二重に暗号化されたキー・データを復号する。次にデバイスは、デバイスのｉ番目のデバイス・キーを使用して、二重に暗号化されたデータの第１の復号の結果を復号する。その結果生じるメディア・キーが現在のメディア・キー値となる。

【００３０】

妥当性検査データの読取り専用領域への格納

次に図１を参照すると、媒体読取り器（３０）にロードされた媒体（１０）の一実施形態例が示されている。媒体読取り器（３０）は、媒体（１０）からコンテンツ（１）を読み取る。媒体（１０）が書込み可能領域（１２）を含む場合、媒体読取り器（３０）が媒体（１０）の書込み可能領域（１２）にデータを書き込むこともできる。前述のように、媒体読取り器（３０）は、媒体に格納された情報を読み取ることができるどんなデバイスであってもよい。媒体読取り器（３０）には、マイクロプロセッサまたは復号、計算、および本明細書で論じる他の処理を実行するための他の回路が含まれる。媒体（１０）は、情報を格納するためのどんな媒体であってもよい。

【００３１】

媒体（１０）は、読取り専用領域（１３）および媒体（１０）に格納されたメディア・キー・ブロック（ＭＫＢ）（１１）を含む。図１は、媒体（１０）の書込み可能領域（１２）に格納されたＭＫＢ（１１）を示す図である。ただし別法として、本発明の精神および範囲を逸脱することなく、ＭＫＢ（１１）を媒体（１０）の読取り専用領域（１３）に格納することもできる。

【００３２】

ＭＫＢ（１１）は一部を暗号化することが可能であり、メディア・キー検証レコード（１５）を含む。本発明の一実施形態では、メディア・キー検証レコード（１５）は「妥当性検査データ」と呼ばれることもあり、暗号化され、事前に選択された値を含む。媒体読取り器（３０）は、ＭＫＢ（１１）の処理中に妥当性検査データ（１５）を復号するものもあることに留意されたい。このような場合、本発明は、妥当性検査データ（１５）を取り出すために、従来技術を上回る追加の読取りオペレーションを必要としない。

【００３３】

妥当性検査データのコピー（１７）は、媒体（１０）の読取り専用領域（１３）に格納される。読取り専用領域（１３）には、たとえばＤＶＤのエンボス・データ・ゾーンまたはカッティング領域が含まれている。妥当性検査データのコピー（１７）がカッティング領域に格納される一実施形態例について、以下で説明する。妥当性検査データのコピー（１７）は、妥当性検査データ（１５）が暗号化されるときと同じ方法で暗号化される。したがって、妥当性検査データのコピー（１７）と妥当性検査データ（１５）が復号されるときには、悪意のある不正変更がなければ、同じ値が得られるはずである。

【００３４】

再度図１を参照すると、媒体読取り器（３０）は媒体（１０）から情報を読み取る。媒体

読取り器（３０）が媒体（１０）から読み取る情報には、コンテンツ（１）（アクセスが許可された後）、ＭＫＢ（３１）、読取り器妥当性検査データ（３３）、および読取り器妥当性検査データのコピー（３５）が含まれる。媒体読取り器（３０）は、ＭＫＢの処理によって事前に取得されたメディア・キーを使用して、読取り器妥当性検査データ（３３）、読取り器妥当性検査データのコピー（３５）、またはその両方を復号する。いずれかの復号の結果、事前に選択された値に等しくない復号値が得られた場合、媒体読取り器（３０）は、媒体（１０）に格納されたコンテンツ（１）へのアクセス許可を拒否する。復号されたすべての値が事前に選択された値と一致する場合、媒体読取り器（３０）は許可プロセスを続行する。

【００３５】

コンテンツ（１）が著作権侵害、直接攻撃、マン・イン・ザ・ミドル攻撃、および他の悪意のある不正変更を受ける環境では、媒体（１０）に格納されたときのデータ・アイテムの値と媒体読取り器（３０）によって読み取られたときのデータ・アイテムの値とが異なる場合がある。したがって、媒体（１０）に格納された妥当性検査データ（１５）と媒体読取り器（３０）によって媒体（１０）から読み取られた妥当性検査データ（３３）とを区別するために、妥当性検査データ（１５）を媒体妥当性検査データ（１５）と呼び、妥当性検査データ（３３）を読取り器妥当性検査データ（３３）と呼ぶことがある。同様に、媒体（１０）に格納された他のデータ・アイテムと媒体読取り器（３０）によって読み取られたときのデータ・アイテムの値とを区別することができる。

【００３６】

媒体読取り器（３０）は、読取り器妥当性検査データ（３３）と読取り器妥当性検査データのコピー（３５）とを比較する。この比較は、暗号化された値または復号された値のどちらでもよい。両方の比較を行うこともできる。読取り器妥当性検査データ（３３）の値と読取り器妥当性検査データのコピー（３５）の値とが等しければ、媒体読取り器（３０）は媒体（１０）に格納されたコンテンツ（１）へのアクセスを許可する。これらの値が等しくなければ、媒体読取り器（３０）は媒体（１０）上のコンテンツ（１）へのアクセス許可を拒否する。

【００３７】

したがって、アクセス許可に関連して、読取り器妥当性検査データ（３３）と読取り器妥当性検査データのコピー（３５）とを比較することによって、媒体（１０）と媒体読取り器（３０）との間に挿入されたマン・イン・ザ・ミドル・デバイスを検出することができる。妥当性検査データの２つのコピーを比較することに関連して使用されるコンテンツへのアクセスを許可する方法は、たとえばＭＫＢからメディア・キーを復号することを含み、当分野でよく知られた方法から選択することができる。媒体妥当性検査データのどちらかのコピー（１５または１７）のマン・イン・ザ・ミドル改変は、読取り器妥当性検査データのコピー（３３および３５）の暗号化または復号された値を比較することによって検出できる。両方の媒体妥当性検査データのコピーのマン・イン・ザ・ミドル改変は、読取り器妥当性検査データのどちらかの復号コピー、または両方の復号された値で、事前に選択された値をチェックすることによって検出される。

【００３８】

次に図２を参照すると、本発明の媒体（１０）と媒体読取り器（３０）の他の実施形態例が示されている。この実施形態では、ＭＫＢ（５１）は、媒体（１０）に読取り専用領域（１３）と書込み可能領域（１２）との間の境界にまたがるように格納され、媒体妥当性検査データ（５５）は読取り専用領域（１３）に格納される。この実施形態では、媒体（１０）の読取り専用領域（１３）の読取り専用という性質によって、妥当性検査データが未許可で不正変更されるのを防ぐことから、妥当性検査データのコピーは不要である。

【００３９】

次に図３を参照すると、本発明の媒体（１０）および媒体読取り器（３０）の他の実施形態例が示されている。この実施形態では、媒体（１０）は、コンテンツが格納された物理媒体と、処理装置または他の論理回路（７２）の両方を含む。たとえば、媒体（１０）は

処理装置を含むフラッシュ・メモリ・アレイであってよい。処理装置を備えた他の媒体例は、ドライバを管理するためのＣＰＵを備えたＤＶＤドライブである。当分野の技術者であれば、処理装置を備えた媒体の他の組合せが明らかであることを理解されよう。他の実施形態の場合も、媒体は書込み可能領域（１２）を含むことができる。

【００４０】

本発明の他の実施形態には、処理装置およびＤＶＤドライブなどの入出力デバイスを備えたパーソナル・コンピュータが含まれる。コンテンツ（１）を格納している媒体（１０）が入出力デバイスにロードされる。媒体（１０）の存在を感知するかまたはユーザ・コマンドを受け取ると、処理装置は、媒体（１０）に格納されたコンテンツへのアクセスを試みる。したがって、パーソナル・コンピュータの処理装置は媒体読取り器（３０）として動作し、入出力デバイスは媒体（１０）として動作する。処理装置は、本明細書で前述したように、媒体妥当性検査データ（１５）および媒体妥当性検査データのコピー（１７）を処理するように構成することができる。当分野の技術者であれば明らかなように、媒体（１０）および媒体読取り器（３０）の組合せによって、コンテンツ（１）を保護し、これにアクセスするためのシステムが形成される。

【００４１】

（メッセージ認証コード（ＭＡＣ）の使用）

前述の妥当性検査データに加えて、メッセージ認証コードを使用することができる。本実施形態でメッセージ認証コード（ＭＡＣ）を含めるために、媒体（７０）は、媒体（７０）と媒体読取り器（３０）との間で認証およびキー交換を介して確立されたランタイム・セッション・キーを使用して、媒体妥当性検査データのコピー（１７）を介して媒体ＭＡＣ（７３）を算出する。実際には、媒体（１０）は媒体ＭＡＣ（７３）を使用して媒体ＭＫＢ（１１）に電子的に署名する。

【００４２】

媒体読取り器（３０）は、媒体（１０）から媒体ＭＡＣ（７３）を読み取る。さらに媒体読取り器（３０）は、媒体妥当性検査データのコピー（１７）も読み取り、媒体ＭＡＣ（７３）の算出に使用したものと同じアルゴリズムを使用して、読取り器妥当性検査データのコピー（３５）を介して読取り器ＭＡＣ（７５）を算出する。

【００４３】

読取り器ＭＡＣ（７５）と媒体ＭＡＣ（７３）とを比較することにより、媒体読取り器（３０）は、媒体（７０）のコンテンツ（１）へのアクセスを許可すべきかどうかの第２の決定を行う。読取り器ＭＡＣ（７５）と媒体ＭＡＣ（７３）とが異なる場合、媒体読取り器（３０）は媒体（７０）のコンテンツ（１）へのアクセスを拒否する。２つのＭＡＣが同一であれば、媒体読取り器（３０）は媒体（７０）のコンテンツ（１）へのアクセスを許可する。したがって、媒体読取り器（３０）は、媒体の電子署名をチェックする。読取り器ＭＡＣと媒体ＭＡＣの計算および比較は、妥当性検査データの保全性チェックが実行される前または実行された後を含む、許可プロセス中のいつでも行うことができる。

【００４４】

そこでＭＡＣは、ＭＫＢ（１１）へのマン・イン・ザ・ミドル改変に対する他のレベルの保護を提供する。媒体妥当性検査データのコピー（１７）が媒体（１０）から読み取られるときに、マン・イン・ザ・ミドル・デバイスが媒体妥当性検査データのコピー（１７）を改変すると、媒体ＭＡＣ（７３）と読取り器ＭＡＣ（７５）とが異なることになる。

【００４５】

次に図４を参照すると、本発明の媒体に格納されたコンテンツへのアクセスを許可するためのプロセス（４００）の一実施形態が示されている。媒体が配布される前に、媒体妥当性検査データを含むＭＫＢが媒体に格納される（ブロック４０１）。媒体妥当性検査データは、媒体の読取り専用領域に格納するか、または媒体の書込み可能領域に格納することができる。媒体妥当性検査データが書込み可能領域に格納されると、次に媒体妥当性検査データのコピーが読取り専用領域に格納される（ブロック４０３）。コンテンツは正しいメディア・キーを使用して暗号化され、媒体に格納された後に、ブロック４０５で媒体が

配布される。ブロック４０７では、使用される媒体の形式によって決まるように、ユーザが媒体を媒体読取り器に挿入するか、または媒体と媒体読取り器を接続する。

【００４６】

他の実施形態には、コンテンツを暗号化して格納する媒体が含まれる。言い換えれば、この実施形態の媒体は、ＣＤ－ＲＷドライブなどのコンテンツ・レコーダであってよい。したがって、媒体はブロック４０４を実行することができる。

【００４７】

媒体の存在を感知するか、あるいはユーザまたは他のデバイスからのコマンドまたは要求を受け取ると、ブロック４０９で、媒体読取り器は媒体からの媒体妥当性検査データを含む媒体ＭＫＢを読み取る。媒体妥当性検査データのコピーが媒体の読取り専用領域に事前に格納されている場合、ブロック４１１で、媒体読取り器は媒体から媒体妥当性検査データのコピーも読み取る。

【００４８】

その後媒体読取り器は、ブロック４１３で、媒体から読み取られた読取り器妥当性検査データの暗号化された値と、媒体から読み取られた読取り器妥当性検査データのコピーの暗号化された値とを比較することができる。２つの値が異なる場合、媒体読取り器はブロック４１４でコンテンツへのアクセス許可を否定する。そうでなければ、ブロック４１５で、許可プロセスを続行することができる。

【００４９】

ブロック４１５および４１７では、媒体読取り器が、媒体から読み取られた読取り器妥当性検査データと、媒体から読み取られた読取り器妥当性検査データのコピーとを復号する。次に媒体読取り器は、ブロック４１９にあるように、ＭＫＢの処理によって得られたメディア・キーを使用して、読取り器妥当性検査データの復号された値と、妥当性検査データの読取り器コピーの復号された値とを比較する。２つの値が異なる場合、媒体読取り器はコンテンツへのアクセス許可を拒否する。そうでなければ許可プロセスはブロック４２０へと進む。

【００５０】

ブロック４２０では、媒体読取り器が、読取り器妥当性検査データの復号された値、または読取り器妥当性検査データのコピーの復号された値のいずれかを、事前に選択された値と比較する。あるいは、読取り器は、復号された読取り器妥当性検査データと復号された読取り器妥当性検査データのコピーの両方を、事前に選択された値と比較することができる。比較のうちいずれか１つでも一致しないと、媒体読取り器はコンテンツへのアクセス許可を拒否する。

【００５１】

ブロック４２１および４２３では、媒体および媒体読取り器が、当分野で知られたいずれかの方法で共用セッション・キーを確立する。ブロック４２５では、媒体から読み取られた読取り器ＭＫＢの読取り器ハッシュ値を介して、媒体読取り器が読取り器ＭＡＣを算出する。ブロック４２７では、媒体が同様に媒体ＭＫＢの媒体ハッシュ値を介して媒体ＭＡＣを算出する。ブロック４２６および４２９では、ドライバが媒体から媒体ＭＡＣを読み取り、それを読取り器ＭＡＣと比較する。２つの値が異なる場合、媒体読取り器は、ブロック４１４でコンテンツへのアクセス許可を拒否する。そうでなければドライバは、ブロック４３１に示されるように、コンテンツへのアクセスを許可するか、またはＭＫＢを処理することができる。

【００５２】

他の実施形態例には、正しいメディア・キーを取得するためのＭＫＢの処理、メディア・キーを使用した妥当性検査データの復号、妥当性検査データが事前に選択された正しい値を含むかどうかの検証、および、ＭＫＢにある妥当性検査データの暗号化された値とデバイスおよび読取り器によってＭＡＣが首尾よく算出されたときに使用した暗号化された妥当性検査データとの比較が含まれる。

【００５３】

他の実施形態例には、妥当性検査データを介してＭＡＣを首尾よく算出すること、媒体の読取り専用領域に格納された妥当性検査データの復号、および妥当性検査データが事前に選択された正しい値を含むかどうかの検証が含まれる。

【００５４】

他の実施形態には、妥当性検査データの２つのコピーを読み取る前にＭＡＣを算出および比較することが含まれる。したがって、読取り器が妥当性検査データのいずれかのコピーを読み取るときに、ＭＡＣは妥当性検査データを伴うことができる。

【００５５】

読取り専用領域のＣＡ（カッティング領域）部分への妥当性検査データの格納

一実施形態例では、図５に示されるように、カッティング領域（１９）と呼ばれる（ＣＡまたはＣＡ部分とも呼ばれる）読取り専用領域（１３）の特殊部分に、妥当性検査データ（１５）を格納することができる。ＣＡ部分とは、通常の大衆消費レコーディング機器／媒体を使用して模倣することを困難にする、物理的特性を有するある種の媒体タイプの一部のことである。ＣＡ部分には書き込むための特殊な製造機器が必要であり、これによってコンテンツをコピーしにくくしている。さらにＣＡは、媒体の他の部分を読み取るのに使用されるプロセスとは物理的に異なるプロセスを使用して読み取られるため、デバイスは、ＣＡに書き込まれたコンテンツと、通常の記録可能媒体に通常のレコーダによって書き込まれたコンテンツとを、物理的に区別することができる。

【００５６】

当分野の通常の技術者であれば、「ＣＡ」または「ＣＡ部分」という用語が、本明細書に記載された一般的な特性を有する領域とみなされること、および「ＣＡ」または「ＣＡ部分」という用語が、本明細書に記載されたＣＡの特性を有する他の領域がＣＡの等価物とみなされるのを妨げるものでないことを理解されたい。

【００５７】

ＣＡの例には、ＤＶＤ－ＲＯＭ（デジタル汎用ディスク－読取り専用メモリ）およびＤＶＤ－ＲＡＭ（デジタル汎用ディスク－ランダム・アクセス・メモリ）のバースト・カッティング領域（ＢＣＡ）、ＤＶＤ－Ｒ（デジタル汎用ディスク－記録可能）およびＤＶＤ－Ｒ／Ｗ（デジタル汎用ディスク－再書込み可能）のナロー・バースト・カッティング領域（ＮＢＣＡ）が含まれる。（ＤＶＤ－ＲおよびＤＶＤ－ＲＷは、まとめてＤＶＤ－Ｒ／Ｗと呼ぶものとする。）

【００５８】

前述のように、妥当性検査データは、メディア・キー検証レコード（１５）のコピーを含むことができる。他の実施形態では、妥当性検査データはメディア・キー検証レコードの検証データ・フィールドのコピー、および／またはＭＫＢ＿Ｈａｓｈとしても知られるＭＫＢのハッシュ関数を含むことができる。

【００５９】

（ＭＫＢ＿Ｈａｓｈを含む妥当性検査データ）

妥当性検査データはＭＫＢ＿Ｈａｓｈを含むことができる。これによって、たとえば、ＤＶＤ－ＲＡＭとの互換性を維持するのに役立ち、ＭＫＢ＿Ｈａｓｈは、ＣＰＲＭコンテンツ保護が使用されるドライブ・ホスト構成を有するＰＣベースシステムのＤＶＤ－ＲＡＭ読取り専用領域のＣＤＡに格納される。こうしたシステムでは、ＤＶＤドライブおよびＰＣホストが協働して、ＣＰＲＭ保護コンテンツ用の記録デバイスおよび／または再生デバイスとして動作する。ドライブ・ホスト構成では、ホストはドライブから受け取ったＭＫＢの保全性を検証する。これは、メッセージ認証コード（ＭＡＣ）計算アルゴリズムを使用して実行される。

【００６０】

ＤＶＤ－Ｒ／Ｗフォーマットでは、たとえば製造業者はＭＫＢ＿Ｈａｓｈを算出し、その結果をＮＢＣＡに格納する。たとえば、ＭＫＢ＿ＨａｓｈはＣ２＿Ｈ（ＭＫＢ）として算出される場合があり、ここでＣ２＿ＨはＣＰＲＭ技術で使用されるＣ２暗号化アルゴリズムに基づいたハッシュ手順であり、ＭＫＢはＭＫＢフレーム全体からＭＫＢ記述子を除い

た部分を含む。ドライブ・ホスト構成では、妥当性検査データはＭＫＢ＿Ｈａｓｈを含み、これは図６に示されるように、ＤＶＤ－ＲＡＭおよびＤＶＤ－Ｒ／Ｗの両方でのＭＫＢの保全性を検証するために使用される。

【００６１】

ホスト（６１）からの要求があると、ドライブ（６０）はＤＶＤ－Ｒ／Ｗに第１のＭＫＢパック（ＭＫＢパック＃０）を要求し、ＮＢＣＡ（１９）からＭＫＢ＿Ｈａｓｈ（１５）を読み取る。ＭＡＣ計算アルゴリズム（６２）を使用して、ＭＫＢ＿Ｈａｓｈ（１５）値を介してドライブＭＡＣすなわちｍ１（６３）が算出され、ＭＫＢパック＃０のＭＫＢ記述子の一部がｍ１（６３）に置き換えられる。その後、修正されたＭＫＢ記述子はホスト（６１）に戻される。より多くの使用可能なＭＫＢパックがある場合、ホスト（６１）はドライブ（６０）からそれらを読み取る。次に、ＭＫＢとＭＫＢフレーム内でその後に続く任意の未使用（ゼロ値）バイトとを使用して、ホスト（６１）は以下のように値ｈを算出するが、この式で、Ｃ２＿Ｈ（６５）はＭＫＢ＿Ｈａｓｈ（１５）の算出に使用されるハッシュ関数を表す。

ｈ＝Ｃ２＿Ｈ（ＭＫＢおよび後続のゼロ）

【００６２】

次にホストは、結果として生じるｈ値を使用して、ＭＡＣアルゴリズム（６２）を使用してホストＭＡＣ、すなわちｍ２（６６）を以下のように算出する。

ｍ２＝ＤＶＤ－ＭＡＣ（ｈ）

【００６３】

ホスト（６１）の比較機能（６７）は、ｍ１＝ｍ２であるかどうかを判定することによって、受け取られたＭＫＢ（１１）の保全性を検証する。検証が失敗した場合、ホスト（６１）は進行中の再生または記録セッションを打ち切る。そうでなければ、メディア・ユニーク・キー（K_{mu}）を算出する。メディア・キー（K_m）の計算前または後にＭＫＢ（１３）の保全性が実現定義済み(implementation-defined)であることをホスト（６１）が検証するかどうかに留意されたい。

【００６４】

図７では、ブロック７００から始まるドライブ・ホスト構成でのＭＫＢ妥当性検査の方法が示されている。ブロック７０２で、ドライブは媒体からＭＫＢ＿Ｈａｓｈを読み取り、ブロック７０４でＭＫＢ＿Ｈａｓｈを介してＭＡＣアルゴリズムを算出する。ブロック７０６でドライブＭＡＣ、すなわちｍ１が生成され、ブロック７０８でＭＫＢのＭＫＢ記述子の一部が交換される。修正されたＭＫＢ記述子は、ブロック７１０でホストに送られる。次にホストは、ブロック７１２で媒体にＭＫＢを要求し、ブロック７１４でＭＫＢを介してＭＡＣアルゴリズムを算出する。ブロック７１６では、ホストＭＡＣ、すなわちｍ２が生成される。ブロック７１８でｍ１とｍ２が比較され、ｍ１がｍ２に等しくない場合はブロック７２０でアクセスが拒否され、ｍ１とｍ２が等しい場合はブロック７２２でアクセスが許可される。方法はブロック７２４で終了する。

【００６５】

（検証データを含む妥当性検査）

妥当性検査データは、メディア・キー検証レコードの検証データ・フィールドのコピーを含む。これによってたとえば、ＤＶＤ－ＲＡＭとの互換性を維持するのに役立ち、メディア・キー検証レコードの検証データ・フィールドのコピーは、ＣＰＲＭコンテンツ保護が使用される、大衆消費電子デバイス（以下「ＣＥデバイス」と呼ぶ）のＤＶＤ－ＲＡＭ読取り専用領域のＣＤＡに格納される。

【００６６】

これを実現するには、ＭＫＢのメディア・キー検証レコードの検証データ・フィールドのコピーがＮＢＣＡに格納される。図８に示されるように、ＣＥデバイス（８０）は、前述のようにＤＶＤ－Ｒ／Ｗディスクからの ＭＫＢ（１１）を処理すること（８１）によって、ＤＶＤ－Ｒ／ＷにあるＭＫＢ（１１）を認証する。ＣＥデバイス（８０）は、結果として生じるメディア・キー（K_m）（８３）を使用して、ＤＶＤ－Ｒ／ＷのＮＢＣＡに格納

された検証データ・フィールドのコピー（１７）を復号し（８２）、必ず次へ進む前に１６進値ＤＥＡＤＢＥＥＦ（８４）に復号する。

【００６７】

図９では、ブロック９００で始まるドライブ・ホスト構成でのＭＫＢの妥当性検査の方法が示されている。ブロック９０２では、メディア・キーを生成するためにＭＫＢが処理される。次にＣＥデバイスは、ブロック９０４で検証データを読み取る。復号器はブロック９０６で、メディア・キーを使用して検証データを復号する。ブロック９０８で調べられるように、検証データが所定の値（すなわちＤＥＡＤＢＥＥＦ用の１６進値）に復号した場合、ＣＥデバイスはブロック９１０でコンテンツへのアクセスを許可する。そうでなければ、ＣＥデバイスはブロック９１２でコンテンツへのアクセスを拒否する。方法はブロック９１４で終了する。

【００６８】

（ＤＶＤ－ＲＡＭとの互換性の維持）

一実施形態例では、たとえば使用されるデバイスに関係なく、ＤＶＤ－ＲＡＭとＤＶＤ－Ｒ／Ｗとの間の完全な互換性が達成される。したがって、ＭＫＢ＿Ｈａｓｈと検証データの両方が、ＤＶＤ－Ｒ／ＷのＮＢＣＡに格納される。両方のタイプの検証データをディスクのカッティング領域に格納することによって、媒体読取り器をわずかにまたはまったく修正することなく、ＤＶＤ－ＲＡＭとＤＶＤ－Ｒ／ＲＷの両方でのＭＫＢの保全性を検証することができる。

【００６９】

ＭＫＢ＿Ｈａｓｈ（１５）を媒体のＣＡ（１９）に配置することによって、ＭＫＢ（１１）の妥当性検査にＭＫＢ＿Ｈａｓｈ（１５）を使用する現存の媒体タイプとの互換性を維持することができる。デバイスは、ＤＶＤ－ＲＡＭの制御データ領域（ＣＤＡ）からＭＫＢ＿Ｈａｓｈを読み取るため、またはＤＶＤ－Ｒ／ＲＷのＮＢＣＡからＭＫＢ＿Ｈａｓｈを読み取るためのどちらかを判定するために、微調整するだけである。ＣＰＲＭフォーマットでは、媒体読取り器は媒体のＭＫＢを読み取ることによって、媒体のタイプを区別することができる。さらに、ドライブ・インターフェース・コマンドや戻されるデータがＤＶＤ－Ｒ／ＷとＤＶＤ－ＲＡＭとでは同じであり、ホストはＣＰＲＭ仕様によって事前に決められた同一の手順を使用して、ＭＫＢの真正性を検証する。

【００７０】

ＤＶＤ－ＲＡＭとＤＶＤ－Ｒ／ＲＷの両方でのＭＫＢの保全性は、大衆消費電子プレーヤ／レコーダ（以下「ＣＥデバイス」と呼ぶ）でＣＥデバイスを微調整することで検証できる。媒体の読取り専用領域から妥当性検査データを読み取るための前述の方法で、ＣＥデバイスはＭＫＢの真正性を検証するために、ＤＶＤ－ＲＡＭの制御データ領域から検証データを読み取るのに対して、ＣＥデバイスは、ＭＫＢの真正性を検証するためにＤＶＤ－Ｒ／ＷのＮＢＣＡからＭＫＢ＿Ｈａｓｈを読み取る。ここでも媒体読取り器は、ＣＰＲＭフォーマットで媒体のＭＫＢを読み取ることによって、媒体タイプを区別することができる。

【００７１】

結論

したがって本発明の実施形態は、ＤＶＤ－Ｒ／Ｗ媒体のＣＰＲＭコンテンツなどのコンテンツを未許可のコピーから保護するために、メディア・キー・ブロックの妥当性を検査する堅固な手段を提供する。改良された保護は、本発明を使用する新しいディスクおよび新しいデバイスによって実行可能である。同時に、媒体読取り器をわずかにまたはまったく修正することなく、新しいデバイスと古いデバイスとの間および新しい媒体と古い媒体との間の完全な相互運用性が維持される。

【００７２】

以上、本発明についてその特有の実施形態を参照しながら述べてきた。ただし、本発明の広範な精神および範囲から逸脱することなく、様々な修正および変更が可能であることは明らかであろう。したがって本明細書および図面は、限定的なものではなく例示的なもの

であるとみなされる。

【００７３】

たとえば、例示的な実施形態について説明してきたが、当分野の通常の技術者であれば、本発明の概念が他のタイプのコンテンツ、コンテンツ保護システム、および媒体フォーマットにも適用可能であることを理解されたい。たとえば、本明細書に記載された例示的実施形態は、現在の保護形式（すなわちＣＰＲＭ）に関するＤＶＤ媒体に特有のものであるが、当分野の通常の技術者であれば、現存のまたは今後開発される他の保護形式も同様に適用可能であることを理解されよう。

【００７４】

さらに、本明細書に記載された本発明の実施形態は、カッティング領域と呼ばれる領域に関するものであるが、カッティング領域は本明細書に記載された特徴を備える領域のことであり、こうした領域はカッティング領域と呼ばれるかまたはカッティング領域という用語を含む領域に限定されるものでないことを理解されたい。一例として、ＤＶＤ－ＲＯＭおよびＤＶＤ－ＲＡＭはバースト・カッティング領域と呼ばれるカッティング領域を含むが、ＤＶＤ－ＲおよびＤＶＤ－ＲＷはナロー・バースト・カッティング領域と呼ばれるカッティング領域を含む。

【図面の簡単な説明】

【００７５】

【図１】本発明の一実施形態を示す簡易構成図である。

【図２】本発明の他の実施形態を示す簡易構成図である。

【図３】本発明の他の実施形態を示す簡易構成図である。

【図４】本発明の一方法を示す簡易流れ図である。

【図５】読取り専用領域が媒体のカッティング領域部分を含む一実施形態を示す図である。

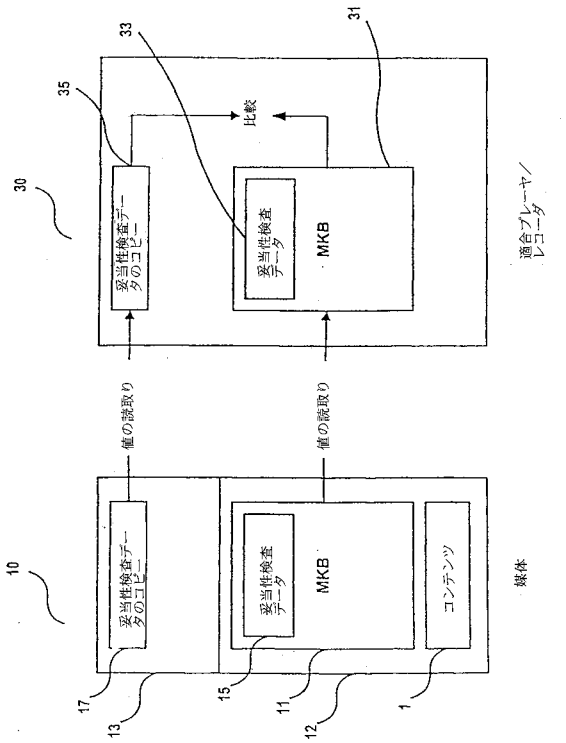
【図６】データの妥当性を検査するために媒体のカッティング領域部分を使用する一システム例を示す図である。

【図７】図６の一方法を示す図である。

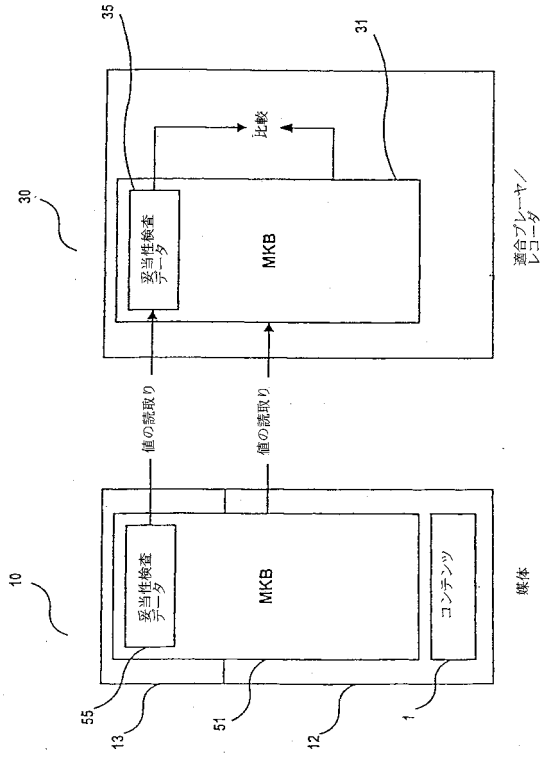
【図８】データの妥当性を検査するために媒体のカッティング領域部分を使用する他のシステム例を示す図である。

【図９】図８の一方法を示す図である。

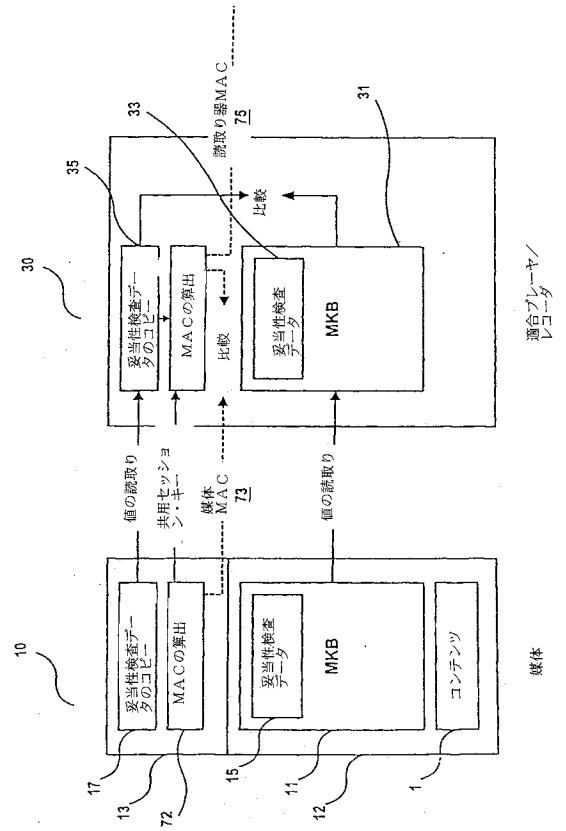
【図１】


適合プレーヤ／レコーダ
媒体
妥当性検査データのコピー
妥当性検査データ
MKB
コンテンツ
比較
値の読取り

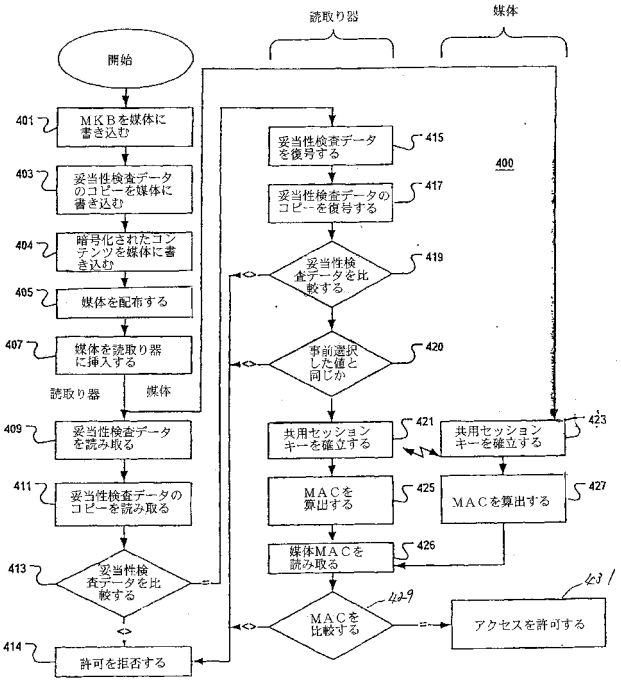
【図２】


適合プレーヤ／レコーダ
媒体
妥当性検査データ
MKB
コンテンツ
比較
値の読取り

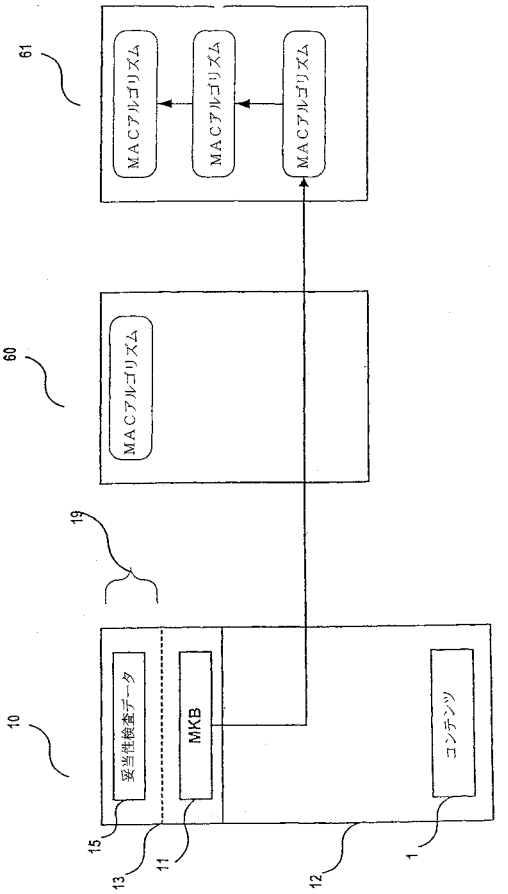
【図３】


適合プレーヤ／レコーダ
媒体
読取り器MAC
妥当性検査データのコピー
MACの算出
妥当性検査データ
MKB
コンテンツ
比較
値の読取り
共用セッション・キー
媒体MAC

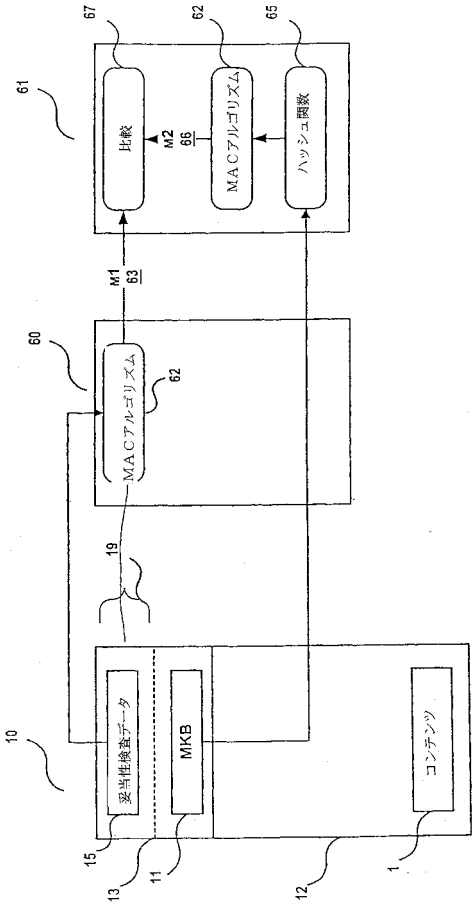
【図４】


読取り器
媒体
開始
MKBを媒体に書き込む
妥当性検査データのコピーを媒体に書き込む
暗号化されたコンテンツを媒体に書き込む
媒体を配布する
媒体を読取り器に挿入する
妥当性検査データを読み取る
妥当性検査データのコピーを読み取る
妥当性検査データを比較する
許可を拒否する
妥当性検査データを復号する
妥当性検査データのコピーを復号する
妥当性検査データを比較する
事前選択した値と同じか
共用セッションキーを確立する
MACを算出する
媒体MACを読み取る
MACを比較する
アクセスを許可する

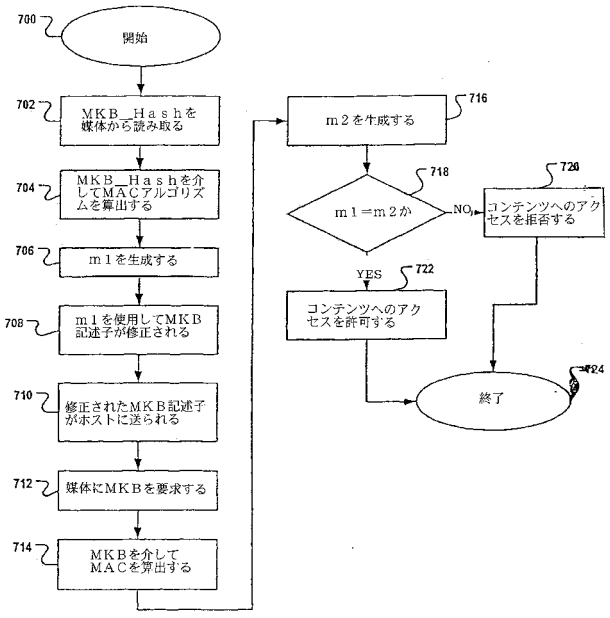
【図５】


61
MACアルゴリズム
MACアルゴリズム
MACアルゴリズム
60
MACアルゴリズム
19
10
妥当性検査データ
MKB
コンテンツ
15
13
11
12
1

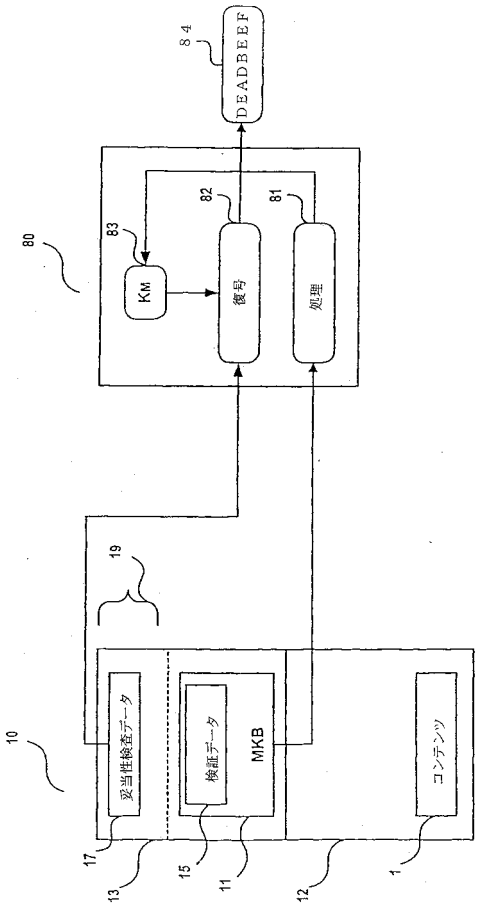
【図６】


67
62
65
61
比較
M2
66
MACアルゴリズム
ハッシュ関数
M1
63
60
MACアルゴリズム
62
19
10
妥当性検査データ
MKB
コンテンツ
15
13
11
12
1

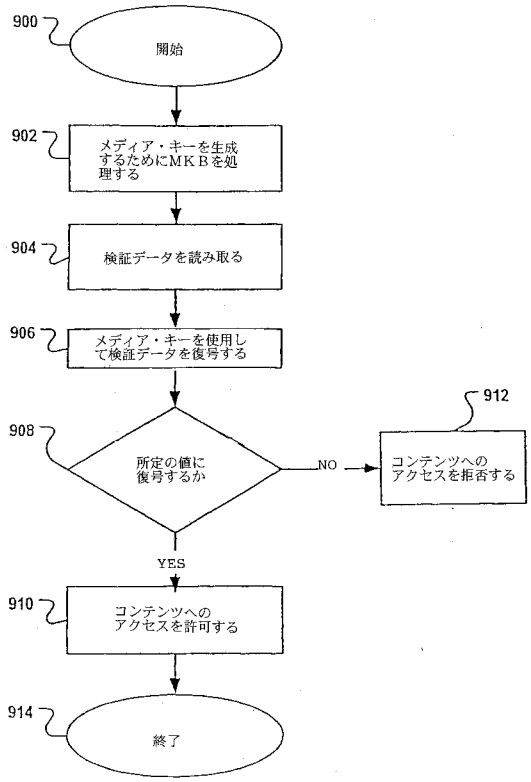
【図７】


700
開始
702
MKB_Hashを媒体から読み取る
704
MKB_Hashを介してMACアルゴリズムを算出する
706
m1を生成する
708
m1を使用してMKB記述子が修正される
710
修正されたMKB記述子がホストに送られる
712
媒体にMKBを要求する
714
MKBを介してMACを算出する
716
m2を生成する
718
m1=m2か
NO
720
コンテンツへのアクセスを拒否する
YES
722
コンテンツへのアクセスを許可する
724
終了

【図８】


84
DEADBEEF
80
83
82
81
Km
復号
処理
19
10
妥当性検査データ
検証データ
MKB
コンテンツ
17
13
15
11
12
1

【図９】


900
開始
902
メディア・キーを生成するためにＭＫＢを処理する
904
検証データを読み取る
906
メディア・キーを使用して検証データを復号する
908
所定の値に復号するか
NO
912
コンテンツへのアクセスを拒否する
YES
910
コンテンツへのアクセスを許可する
914
終了

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 July 2002 (11.07.2002)

PCT

(10) International Publication Number
WO 02/054401 A1

(51) International Patent Classification[7]: G11B 20/00

(21) International Application Number: PCT/US01/49784

(22) International Filing Date:
21 December 2001 (21.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/750,642	28 December 2000 (28.12.2000)	US
09/823,718	30 March 2001 (30.03.2001)	US
09/973,547	9 October 2001 (09.10.2001)	US

(71) Applicant: **INTEL CORPORATION** [US/US]; (a Delaware Corporation), 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: **RIPLEY, Mike**; 1222 NE 56th Court, Hillsboro, OR 97124 (US). **KATOH, Taku**; 3-12-20, Jyomyoji, Kamakura, Kanagawa 248-0003 (JP). **LOTSPIECH, Jeffrey**; 992 Foothill Drive, San Jose, CA 95123 (US). **ISHIHARA, Atsushi**; 21-11 Tsutsujigaoka, Aoba-ku, Yokohama 227-005 (JP). **FUKUSHIMA, Yoshihisa**; 6-14-C-508, Sekime, Jyouto-ku, Osaka-shi, Osaka 536-0008 (JP).

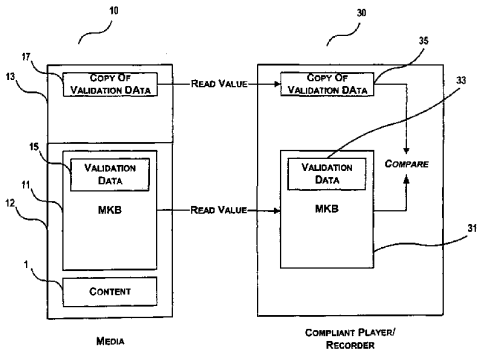
(74) Agents: **MALLIE, Michael, J.** et al.; Blakely Sokoloff Taylor & Zafman, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent

[Continued on next page]

(54) Title: VERIFYING THE INTEGRITY OF A MEDIA KEY BLOCK BY STORING VALIDATION DATA IN THE CUTTING AREA OF MEDIA



(57) Abstract: A method for verifying the integrity of a media key block (MKB) by storing validation data in a cutting area of a medium, such as a DVD-R or a DVD-RW. In one embodiment, validation data comprises a hash function on a media key block. In another embodiment, validation data field of an MKB's Verify Media Key Record.

WO 02/054401 A1

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

VERIFYING THE INTEGRITY OF A MEDIA KEY BLOCK BY STORING VALIDATION DATA IN A CUTTING AREA OF MEDIA

[0001] This application is a continuation-in-part of presently co-pending U.S. patent application, Serial No. 09/750,642 filed on December 28, 2000, entitled "METHOD AND APPARATUS FOR VERIFYING THE INTEGRITY OF A MEDIA KEY BLOCK".

COPYRIGHT NOTICE

[0002] Contained herein is material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever.

FIELD

[0003] This invention relates to static and dynamic information storage and retrieval. More particularly, this invention relates to methods, apparatus and systems for the protection of stored information from unauthorized access.

BACKGROUND

[0004] Information or content may be stored on a wide variety of media. As the speed and convenience of accessing and copying stored information have increased, the threat of unauthorized coping of the information has increased correspondingly. Various schemes have been employed to protect the stored information from unauthorized access. For instance, the content stored on the media may be encrypted with a secret key, or keys, known only to devices authorized to access the media. A disadvantage of only one key is the inability to revoke the authorization of a particular device, by changing the key, without revoking the authority of all devices to read the media. Some of the disadvantages of using multiple keys include the potentially large burden of transmitting and storing the keys for each particular device.

[0005] An alternative method developed to protect content from unauthorized copying uses a media key block (MKB) to authorize copying of the content, as described by a publication from 4C Entity, LLC, entitled "CONTENT PROTECTION FOR RECORDABLE MEDIA SPECIFICATION," Revision 0.94 (October 18, 2000). Authorized devices process the MKB to calculate, as described in part below, a media key allowing an authorized device to copy the content. The MKB method uses a media unique key to bind encrypted content to the media from which it will be played back.

[0006] As keys are compromised and revoked, the MKB can become quite large, with a size of several megabytes not being unusual. Since many types of media have limited read-only space, it becomes necessary to store the MKB on writeable areas of the media. Storing the MKB on the writeable area creates a vulnerability of the MKB to direct malicious tampering. In such a direct attack, the intent of the tamperer will likely be to substitute an older MKB for the current MKB stored on the media. In the alternative, the tamperer may substitute a portion of an older MKB for a portion of the current MKB stored on the media. Since the older MKB will still contain keys that are revoked by the current MKB, the substitution will potentially compromise the content protection provided by the current MKB.

[0007] Even if the MKB is stored on the readable area of the media, another weakness of the MKB approach is the ability for a man-in-the-middle attack to substitute an older MKB for the current MKB during the attempted processing of the current MKB. In the alternative, the man-in-the-middle attacker may substitute a portion of an older MKB for a portion of the current MKB during the attempted processing of the current MKB. Thus, a man-in-the-middle attack also potentially compromises the content protection provided by the current MKB.

[0008] Thus, media without a valid MKB could be read and readers without authorization could read content stored on protected media. In a variation on the MKB approach, a hash value is calculated over the MKB and stored on the read-only area of the media. The reader reads the MKB, calculates a hash value of the MKB as read from the media and compares that hash value to the hash value as

read from the read-only area. Calculating the hash value however imposes an undesirable delay upon the authorization process. Therefore, it is desirable to improve upon the prior art.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[0010] FIG. 1 is a simplified block diagram of an embodiment of the present invention.

[0011] FIG. 2 is a simplified block diagram of another embodiment of the present invention.

[0012] FIG. 3 is a simplified block diagram of another embodiment of the present invention.

[0013] FIG. 4 is a simplified flowchart of a method of the present invention.

[0014] FIG. 5 illustrates an embodiment in which the read-only area comprises a cutting area region of a medium.

[0015] FIG. 6 illustrates one exemplary system which utilizes the cutting area region of a medium to validate data.

[0016] FIG. 7 illustrates a method of FIG. 6.

[0017] FIG. 8 illustrates another exemplary system which utilizes the cutting area region of a medium to validate data.

[0018] FIG. 9 illustrates a method of FIG. 8.

DETAILED DESCRIPTION OF THE INVENTION

[0019] In one aspect of the invention, a method for verifying the integrity of a media key block (MKB) by storing validation data in a cutting area of a medium, such as a DVD-R or a DVD-RW, is disclosed.

[0020] In one embodiment, validation data may comprise a hash function on a media key block (MKB) to achieve compatibility with DVD-RAMs when the MKB is being verified in a drive-host configuration. In this embodiment, the drive reads the MKB from the control data area (CDA) of a disc, whether it is a DVD-RAM, a DVD-R, or a DVD-RW. A minor adjustment to the drive allows the drive to read the hash value from the CDA of a DVD-RAM or a narrow burst cutting area (NBCA) of a DVD-R or a DVD-RW, thus allowing the drive to verify the authenticity of the MKB using previously established procedures.

[0021] In another embodiment, validation data may comprise a Verification Data field of an MKB's Verify Media Key Record to achieve compatibility with DVD-RAMs when the MKB is being verified by a consumer electronics player/recorder (hereinafter a "CE device"). In this embodiment, a CE device reads the MKB from the CDA of a disc. A minor adjustment to the drive allows the drive to read the Verification Data field from the CDA of a DVD-RAM or a narrow burst cutting area (NBCA) of a DVD-R or a DVD-RW, thus allowing the drive to verify the authenticity of the MKB using previously established procedures.

[0022] The present invention includes various operations, which will be described below. The operations of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the operations. Alternatively, the operations may be performed by a combination of hardware and software.

[0023] The present invention may be provided as a computer program product which may include a machine-readable medium having stored thereon instructions which may be used to program a computer (or other electronic

devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs (Compact Disc-Read-only Memories), and magneto-optical disks, ROMs (Read-only Memories), RAMs (Random Access Memories), EPROMs (Erasable Programmable Read-only Memories), EEPROMs (Electromagnetic Erasable Programmable Read-only Memories), magnetic or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions.

[0024] Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer (e.g., a server) to a requesting computer (e.g., a client) by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection). Accordingly, herein, a carrier wave shall be regarded as comprising a machine-readable medium.

[0025] In the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one skilled in the art that the present invention may be practiced without these specific details. In other instances well known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

Introduction

[0026] Herein, certain terminology is used to discuss features of the present invention. For example, content is information programmed by owners or licensees, such as broadcast or cable networks. "Content" can by any form of audible or visual information including business data, news, sports, artistic performances, entertainment, advertising, documentaries, talk, films, videos, cartoons, text, music and graphics.

Media

[0027] Media includes any mechanism that provides (i.e., stores and/or transmits) content in a form readable by a machine (e.g., a computer). For example, a machine readable medium includes read-only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); etc. Typically, content may be stored in encrypted form on media such as DVDs, CDs, floppy discs, flash memory arrays. Access control comes from the inability of an unauthorized device, or a device having revoked keys, to successfully process the MKB, validate the MKB and then decrypt the content.

Media Reader

[0028] A media reader is an electronic device that reads the content from the media. A media reader may also read data other than the content from the media. For instance, media reader may be a DVD drive or player, a CD drive or player, a floppy drive, a digital television, a digital VCR, a CPU of a personal computer, a processor or a circuit coupled to flash memory cells, or any other consumer electronics device capable of accessing content stored on the media. Devices which also write or record to the media, such as CD-RW drives, are also considered media readers.

Content Protection For Recordable Media (CPRM)

[0029] In embodiments of the invention, media readers may implement Content Protection for Recordable Media (CPRM) format for protecting content. CPRM defines a method for protecting content stored on a number of physical media types, including, but not limited to, DVD-RAM, DVD-R, and DVD-RW. The device requirements are explained in further detail in the section below entitled "Media Key Block".

Media Key Block

[0030] An MKB is formatted as a sequence of contiguous records, where each record begins with a record type field, followed by a record length field. An

MKB is part of an MKB Frame that is constructed from n MKB Packs having data. Each MKB Frame begins with an MKB Descriptor, which is part of the first MKB Pack, or MKB Pack #0. Each of the first n-1 MKB Packs are filled completely. The nth MKB Pack may end up with unused bytes, which are zero-filled.

[0031] In order to process the MKB, each authorized device receives a set of "n" device keys. The "n" device keys are referred to as Kd_i (i=0,1,...,n-1). For each device key there is an associated column and row value in the MKB, referred to as column value (Cd_i for i=0,1,...,n-1) and row value (Rd_i for i=0,1,...,n-1), respectively. An authorized device will have at most one device key for each column of the MKB, alhough, an authorized device may have more than one device key per row.

[0032] The device keys and associated row and column values are kept secret. If a set of device keys is compromised, an updated MKB can be released that causes a device with the compromised set of device keys to calculate a different media key than is computed by the remaining compliant devices. In this way, the compromised device keys are "revoked" by the new MKB.

[0033] Using its device keys, a device calculates the media key by processing records of the MKB one-by-one from first to last. After processing of the MKB is completed, the device uses the most recently calculated media key value as the final value for the media key. If a device correctly processes an MKB using device keys that are revoked by that MKB, the resulting final media key will have the special value 0H, where H designates a hexadecimal number. This special value will never be an MKB's correct final media key value, and can therefore always be taken as an indication that the device's keys are revoked. If a device calculates this special media key value, it stops the authentication, playback, or recording session in progress, and will not use that media key value in any subsequent calculations.

[0034] A properly formatted MKB will have exactly one Verify Media Key Record (VMKR) as its first record. The VMKR contains the hexadecimal value DEADBEEF encrypted with the correct, final media key. The presence of the

VMKR is mandatory, but the use of the VMKR by a device is not mandatory. A device may attempt to decrypt the VMKR using its current media key value during the processing of subsequent Records, checking each time for the hexadecimal value DEADBEEF. If the device successfully decrypts the VMKR, the device has already calculated the correct final media key value, and may therefore stop processing the MKB.

[0035] A properly formatted MKB will have exactly one calculate media key record (CMKR). Devices must ignore any CMKRs encountered after the first one in an MKB. The CMKR includes a column field. The column field indicates the associated column value for the device key to be used with this record, as described below. The CMKR also contains encrypted key data in each column corresponding to each of the device key rows. Before processing the CMKR, the device checks that the device has a device key with associated column value Cd_i == column, for some i.

[0036] If the device does not have a device key with the associated column value, the device ignores the rest of the CMKR. Otherwise, using the value i from the condition above, the device key and r = Rd_i, c = Cd_i, the device decrypts a media key value from the encrypted key data for row r = Rd_i. The resulting media key value becomes the current media key value.

[0037] A properly formatted MKB may have zero or more conditionally calculate media key records (C-CMKR). The C-CMKR contains encrypted conditional data. In the columns, the C-CMKR contains doubly encrypted key data. If decrypted successfully, as described below, the encrypted conditional data contains the hexadecimal value DEADBEEF and the associated column value for the device key to be used with this C-CMKR. Using its current media key value, the device decrypts conditional data from the encrypted conditional data.

[0038] Before continuing to process the Record, the device checks that the following conditions are true: the decrypted conditional data contains the hexadecimal value DEADBEEF and the device has a device key with a newly

associated column value (i) decrypted from the conditional data. If any of these conditions is false, the device ignores the rest of the C-CMKR. Otherwise, using the value i from the condition above, the current media key value, and r = Rd_i, c = Cd_i, the device decrypts the doubly encrypted key data at the associated column in the C-CMKR. The device then decrypts the result of the first decryption of the doubly encrypted data using the device's i-th device key. The resulting media key becomes the current media key value.

Storing Validation Data in Read-Only Area

[0039] Referring now to Figure 1, an exemplary embodiment of a media (10) loaded into a media reader (30) is shown. The media reader (30) reads content (1) from the media (10). If the media (10) includes a writeable area (12), the media reader (30) may also write data to the writeable area (12) of media (10). As described above, the media reader (30) may be any device capable of reading information stored on a media. The media reader (30) includes microprocessors or other circuits to perform the decryptions, calculations and other processing discussed herein. The media (10) may be any media for storing information.

[0040] Media (10) includes a read-only area (13) and a media key block (MKB) (11) stored on the media (10). FIG. 1 illustrates the MKB (11) being stored on the writeable area (12) of the media (10). However, the MKB (11) may alternatively be stored on the read-only area (13) of the media (10) without departing from the spirit and scope of the invention.

[0041] Parts of the MKB (11) may be encrypted and includes a Verify Media Key Record (15). In one embodiment of the invention, the Verify Media Key Record (15) may also be referred to as "validation data", which is encrypted and contains a pre-selected value. It should be noted that some media readers (30) decrypt the validation data (15) during the processing of the MKB (11). In such cases, the present invention does not require an additional read operation over the prior art to retrieve the validation data (15).

[0042] A copy of the validation data (17) is stored on the read-only area (13) of the media (10). The read-only area (13) may comprise, for example, an embossed data zone or a cutting area of a DVD. An exemplary embodiment in which the validation data (17) is stored in the cutting area is described below. The copy of the validation data (17) is encrypted in the same manner as the validation data (15) is encrypted. Thus, when the copy of the validation data (17) and the validation data (15) are decrypted, the same value should be obtained if no malicious tampering has occurred.

[0043] Referring still to Figure 1, the media reader (30) reads information from the media (10). The information that the media reader (30) reads from the media (10) includes the content (1) (after access is authorized), the MKB (31), the reader validation data (33), and a copy of the reader validation data (35). The media reader (30) decrypts the reader validation data (33), the reader copy of the validation data (35), or both using the media key obtained previously by processing the MKB. If the result of either decryption yields a decrypted value not equal to the preselected value, the media reader (30) refuses to authorize access to the content (1) stored on the media (10). If all of the decrypted values match the preselected value, the media reader (30) continues the authorization process.

[0044] It should be noted that the value of a data item as stored on the media (10) and the value of the data item as read by the media reader (30) may differ in an environment in which the content (1) is subject to piracy, direct attacks, man-in-the-middle attacks and other malicious tampering. Therefore, to distinguish between the validation data (15) stored on the media (10) and the validation data (33) read from the media (10) by the media reader (30), the validation data (15) may be referred to as the media validation data (15) and the validation data (33) may be referred to as the reader validation data (33). Similar distinctions can be made between other data items stored on the media (10) and the value of that data item as read by the media reader (30).

[0045] The media reader (30) compares the reader validation data (33) and the copy of the reader validation data (35). The comparison may be of either the encrypted values or the decrypted values. Both comparisons may also be made.

If the value of the reader validation data (33) and the value of the copy of the reader validation data (35) are equal then the media reader (30) authorizes access to the content (1) stored on the media (10). If these values are not equal, the media reader (30) refuses to authorize access to the content (1) on the media (10).

[0046] Thus, by comparing the reader validation data (33) and the copy of the reader validation data (35) in conjunction with authorizing access, man-in-the-middle devices inserted between the media (10) and the media reader (30) may be detected. The method of authorizing access to the content used in conjunction with the comparison of the two copies of the validation data may be chosen from those methods well known to the art, including for example decrypting a media key from an MKB. A man-in-the-middle alteration of either copy of the media validation data (15 or 17) may be detected by the comparison of the encrypted or decrypted values of the copies of the reader validation data (33 and 35). A man-in-the-middle alteration of both copies of the media validation data will be detected by checking for the pre-selected value in either decrypted copy of the reader validation data, or in both decrypted values.

[0047] Referring now to Figure 2, another exemplary embodiment of a media (10) and a media reader (30) of the present invention is shown. In this embodiment, the MKB (51) is stored on the media (10) so as to straddle the boundary between the read-only area (13) and the writeable area (12), with the media validation data (55) being stored on the read-only area (13). No copy of the validation data is required in this embodiment because the read-only nature of the read-only area (13) of the media (10) protects the validation data from unauthorized tampering.

[0048] Referring now to Figure 3, yet another exemplary embodiment of a media (70) and a media reader (30) of the present invention is shown. In this embodiment, the media (70) includes both the physical media on which the content is stored and a processor or other logic circuit (72). For instance, the media (70) may be a flash memory array including a processor. Another example of a media with a processor is a DVD drive with a CPU to manage the driver.

Though, those skilled in the art will recognize that other combinations of media with a processor are obvious. As with other embodiments, the media may also contain a writeable area (12).

[0049] Another embodiment of the present invention includes a personal computer having a processor and an input/output device such as a DVD drive. A media (10) having a content (1) stored on it is loaded into the input/output device. Upon sensing the presence of the media (10), or upon user command, the processor attempts to access the content stored on the media (10). Thus, the processor of the personal computer acts as a media reader (30) and the input/output device acts as a media (10). The processor may be configured to process the media validation data (15) and the copy of the media validation data (17), as set forth herein. As will be obvious to those skilled in the art, the combination of a media (10) and a media reader (30) form a system for protecting and accessing the content (1).

Using a Message Authentication Code (MAC)

[0050] A message authentication code may be employed in addition to the validation data discussed previously. To include a message authentication code (MAC) in the present embodiment, the media (70) calculates a media MAC (73) over the copy of the media validation data (17) using a run-time session key established via authentication and key exchange between the media (70) and a media reader (30). In effect, the media (70) electronically signs the media MKB (11) with the media MAC (73).

[0051] The media reader (30) reads the media MAC (73) from the media (70). The media reader (30) also reads the copy of the media validation data (17) and calculates a reader MAC (75) over the copy of the reader validation data (35) using the same algorithm as was used to calculate the media MAC (73).

[0052] By comparing the reader MAC (75) and the media MAC (73), the media reader (30) makes a second determination of whether authorization for

access to the contents (1) of the media (70) should be granted. Should the reader MAC (75) and the media MAC (73) differ, the media reader (30) refuses access to the contents (1) of the media (70). If the two MACs are identical, the media reader (30) allows access to the contents (1) of the media (70). Thus, the media reader (30) checks the electronic signature of the media. The calculation and comparison of the reader and media MACs may occur at any time during the authorization process, including before or after the validation data integrity check is executed.

[0053] Thus, a MAC provides another level of protection against man-in-the-middle alterations to the MKB (11). If the man-in-the-middle device alters the copy of the media validation data (17) as the copy of the media validation data (17) is being read from the media (10), the media MAC (73) and the reader MAC (75) will differ.

[0054] Referring now to Figure 4, an embodiment of a process (400) for authorizing access to content stored on media of the present invention is shown. Before the media is distributed, the MKB including the media validation data is stored on the media (block 401). The media validation data may be stored on the read-only area of the media or it may be stored on the writeable area of the media. If the media validation data is stored on the writeable area then a copy of the media validation data is stored on the read-only area (block 403). The content is encrypted using the correct media key and then stored on the media before the media is distributed in block 405. In block 407 the user inserts the media into a media reader or connects the media and media reader as dictated by the form of media employed.

[0055] Another embodiment includes a media which encrypts and stores content. In other words, the media of this embodiment may be a content recorder such as a CD-RW drive. Thus, the media may execute block 404.

[0056] Upon sensing the presence of the media or upon a command or request from the user or other device, the media reader reads the media MKB including the media validation data from the media in block 409. If a copy of the

media validation data has been previously stored on the read-only area of the media, the media reader also reads the copy of the media validation data from the media in block 411.

[0057] The media reader may then compare the encrypted value of the reader validation data read from the media with the encrypted value of the copy of the reader validation data read from the media at block 413. If the two values are different the media reader denies authorization to access the content in block 414. Otherwise, the authorization process may continue with block 415.

[0058] In blocks 415 and 417, the media reader decrypts the reader validation data read from the media and the copy of the reader validation data read from the media. The media reader may then compare the decrypted values of the reader validation data and of the reader copy of the validation data, as in block 419 using the media key obtained by processing the MKB. If the two values are different the media reader denies authorization to access the content. Otherwise, the authorization process continues with block 420.

[0059] In block 420, the media reader compares either the decrypted value of the reader validation data or the decrypted value of the copy of the reader validation data to the pre-selected value. In the alternative, the reader may compare both the decrypted reader validation data and the decrypted copy of the reader validation data to the pre-selected value. If any one of the comparisons fails, then the media reader denies authorization to access the content.

[0060] In blocks 421 and 423, the media and media reader establish a shared session key in any manner known to the art. The media reader, in block 425, calculates a reader MAC over a reader hash value of the reader MKB read from the media. The media, in block 427, likewise calculates a media MAC over a media hash value of the media MKB. In blocks 426 and 429, the driver then reads the media MAC from the media and compares it to the reader MAC. If the two values are different the media reader denies authorization to access the content at block 414. Otherwise, the driver may authorize access to the content or may process the MKB, as shown in block 431.

[0061] Another exemplary embodiment includes processing the MKB to obtain the correct media key; decrypting the validation data with the media key; verifying that the validation data contains the correct preselected value; and comparing the encrypted value of the validation data in the MKB with the encrypted validation data over which a MAC has been successfully calculated by the device and reader.

[0062] Another exemplary embodiment includes successfully calculating a MAC over the validation data; decrypting the validation data stored on the read-only area of the media; and verifying that the validation data contains the correct preselected value.

[0063] Yet another embodiment includes calculating and comparing the MACs before reading the two copies of the validation data. Thus, when the reader reads either copy of the validation data the MAC may accompany the validation data.

Storing Validation Data in a CA (Cutting Area) Region of a Read-Only Area

[0064] In one exemplary embodiment, as illustrated in FIG. 5, validation data (15) may be stored in a special region of the read-only area (13) called a cutting area (19) (also referred to as a CA, or a CA region). A CA region is a portion of certain media types that has physical properties that make it difficult to mimic using ordinary consumer recording equipment/media. A CA region requires special manufacturing equipment to write, making its contents difficult to copy. Furthermore, since the CA is read using a physically different process from that used to read the other areas of a medium, a device can physically distinguish contents written to a CA from contents that may have been written by an ordinary recorder on ordinary recordable media.

[0065] It should be understood by one of ordinary skill in the art that the term "CA" or "CA region" is to be construed as an area having the general properties described herein, and that the term "CA" or "CA region" shall not

preclude other areas having the properties of a CA described herein from being construed as an equivalent of a CA.

[0066] Examples of CAs include a burst cutting area (BCA) of a DVD-ROM (Digital Versatile Disc - Read-Only Memory) and a DVD-RAM (Digital Versatile Disc - Random Access Memory); and a narrow burst cutting area (NBCA) of a DVD-R (Digital Versatile Disc - Recordable) and DVD-R/W (Digital Versatile Disc - Rewriteable). (DVD-Rs and DVD-RWs shall together be referred to as DVD-R/Ws.)

[0067] Validation data may comprise a copy of the verify media key record (15), as discussed above. In other embodiments, validation data may comprise a copy of the Verification Data field of the Verify Media Key Record, and/or a hash function on the MKB, also known as the MKB_Hash.

Validation Data Comprising MKB_Hash

[0068] Validation data may comprise `MKB_Hash`. This can, for example, help to maintain compatibility with DVD-RAMs, where `MKB_Hash` is stored in a CDA of a DVD-RAMs read-only area in a PC based system having a drive-host configuration where CPRM content protection is used. In such a system, a DVD drive and PC host act together as a recording device and/or playback device for CPRM protected content. In a drive-host configuration, the host verifies the integrity of the MKB it receives from the drive. It does this by using a message authentication code (MAC) calculation algorithm.

[0069] In DVD-R/W formats, for instance, the manufacturer calculates `MKB_Hash`, and stores the result in the NBCA. For example, `MKB_Hash` may be calculated as `C2_H(MKB)`, where `C2_H` is a hashing procedure based on a C2 encryption algorithm used in CPRM technology, and where MKB includes the entire MKB Frame minus the MKB Descriptor. In a drive-host configuration, validation data comprises `MKB_Hash`, which is used to verify the integrity of the MKB on both a DVD-RAM and a DVD-R/W, as illustrated in FIG. 6.

[0070] Upon request from the host (61), the drive (60) requests the first MKB Pack (MKB Pack #0) from a DVD-R/W, and reads an MKB_Hash (15) from the NBCA (19). Using a MAC calculation algorithm (62), a drive MAC, m1 (63), is calculated over the MKB_Hash (15) value, and part of the MKB Descriptor of MKB Pack #0 is replaced with m1 (63). The modified MKB Descriptor is then returned to the host (61). If there are more MKB Packs available, the host (61) reads them from the drive (60). Then, using the MKB and any unused (zero-valued) bytes that follow it in the MKB Frame, the host (61) calculates a value, h, as:

[0071] h = C2_H(MKB and trailing zeros), where C2_H (65) represents the hash function used to calculate MKB_Hash (15).

[0072] Using the resulting h value, the host then uses the MAC algorithm (62) to calculate a host MAC, m2 (66) as:

[0073] m2 = DVD-MAC(h).

[0074] A compare function (67) of the host (61) verifies the integrity of the received MKB (11) by determining if m1 = m2. If verification fails, then the host (61) aborts the playback or recording session in progress. Otherwise, it calculates a media unique key (K_{mu}). Note that whether the host (61) verifies the MKB's (13) integrity before or after the calculation of the media key (K_m) is implementation-defined.

[0075] A method for MKB validation in a drive-host configuration is shown in FIG. 7, starting at block 700. At block 702, the drive reads the MKB_Hash from the media, and calculates a MAC algorithm over the MKB_Hash at block 704. A drive MAC, m1, is generated at block 706, and parts of the MKB Descriptor of the MKB are replaced at block 708. The modified MKB Descriptor is sent to the host at block 710. The host then requests the MKB from the media at block 712, and calculates the MAC algorithm over the MKB at block 714. At block 716, a host MAC, m2, is generated at block 716. At block 718, m1 is compared to m2, and access is denied at block 720 if m1 does not equal m2, or granted at block 722 if m1 equals m2. The method ends at block 724.

Validation Comprising Verification Data

[0076] Validation data may comprise a copy of the Verification Data field of the Verify Media Key Record. This can, for example, help to maintain compatibility with DVD-RAMs, where a copy of the Verification Data field of the Verify Media Key Record is stored in a CDA of a DVD-RAMs read-only area in an consumer electronics device (hereinafter referred to as "CE device") where CPRM content protection is used.

[0077] To implement this, a copy of the Verification Data field of the MKB's Verify Media Key record is stored in the NBCA. As shown in FIG. 8, a CE device (80) authenticates the MKB (11) on a DVD-R/W by processing (81) the MKB (11) from the DVD-R/W disc, as described above. The CE device (80) uses the resulting Media Key (K_m) (83) to decrypt (82) the copy of the Verification Data field (17) stored in the NBCA of the DVD-R/W, ensuring that it decrypts to the hexadecimal value DEADBEEF (84) before proceeding.

[0078] A method for MKB validation in a drive-host configuration is shown in FIG. 9, starting at block 900. At block 902, the MKB is processed to produce a media key. The CE device then reads the verification data at block 904. Using the media key, a decryptor decrypts the verification data at block 906. If the verification data decrypts to a pre-determined value (i.e., hexadecimal value for DEADBEEF) as checked at block 908, then the CE device grants access to the contents at block 910. Otherwise, the CE device denies access to the contents at block 912. The method ends at block 914.

Maintaining Compatibility With DVD-RAMs

[0079] In an exemplary embodiment, full compatibility between DVD-RAMs and DVD-R/Ws, for example, is achieved without regard to the device being used. Thus, both an MKB_Hash and Verification Data are stored in the NBCA of DVD-R/Ws. By storing both types of validation data in the cutting area of a disc, the integrity of an MKB may be verified on both DVD-RAMs and DVD-R/RWs with little or no modification to media readers.

[0080] By placing the MKB_Hash (15) in the CA (19) of a medium, compatibility with currently existing media types using MKB_Hash (15) to validate MKBs (11) can be maintained. The device is merely subject to a minor adjustment for determining whether to read the MKB_Hash from the control data area (CDA) of a DVD-RAM or to read the MKB_Hash from the NBCA of a DVD-R/RW. In CPRM format, a media reader can differentiate between media types by reading the MKB of the media. Furthermore, the drive interface command and returned data are the same for DVD-R/W and DVD-RAM, and the host verifies the authenticity of the MKB using the identical procedures previously defined by the CPRM specification.

[0081] The integrity of an MKB on both DVD-RAMs and DVD-R/RWs may be verified in consumer electronics players/recorders (hereinafter referred to as "CE devices") with minor adjustments to the CE device. Whereas a CE device reads verification data from the Control Data Area of a DVD-RAM to verify the MKBs authenticity, in a manner described above for reading validation data from the read-only area of a medium, a CE device reads the MKB_Hash from the NBCA of a DVD-R/W to verify the MKBs authenticity. Again, a media reader can differentiate between media types by reading the MKB of the media in CPRM format.

Conclusion

[0082] Thus, embodiments of the invention provide a robust means of validating a media key block to protect content, such as CPRM content on DVD-R/W media, against unauthorized copying. The enhanced protection is enabled by new discs and new devices that use the invention. At the same time, full interoperability among new and old devices, and new and old media is maintained with little or no modifications to media readers.

[0083] In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from

the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

[0084] For example, while exemplary embodiments have been described, it should be understood by one of ordinary skill in the art that concepts of this invention can be applied to other types of content, content protection systems, and media formats. For example, while the exemplary embodiments described herein are specific to DVD media as they relate to a current form of protection (i.e. CPRM), one of ordinary skill in the art would understand that other forms of protection currently existing or to be developed in the future may apply as well.

[0085] Furthermore, while embodiments of the invention described herein refer to an area called the cutting area, it should be understood that the cutting area is an area having characteristics described herein, and that such an area is not limited to areas that are called, or that contain the term, cutting area. As an example, DVD-ROMs and DVD-RAMs comprise a cutting area called a burst cutting area, while DVD-Rs and DVD-RWs comprise a cutting area called a narrow burst cutting area.

CLAIMS

WHAT IS CLAIMED IS:

1. A method, comprising:

reading a media key block from a first region on a medium;

reading validation data related to the media block from a second region on the medium; and

validating the media key block using the validation data.

2. The method of claim 1, wherein said validating the media key block using the validation data comprises:

comparing the media key block to the validation data; and

granting authorization to access the content if the media key block corresponds to the validation data.

3. The method of claim 2, wherein the media key block corresponds to the validation data if the media key block matches the validation data.

4. The method of claim 2, wherein the media key block corresponds to the validation data if a hash function over the media key block matches the validation data.

5. The method of claim 4, wherein the validation data comprises a hash function of the media key block, and said validating the media key block comprises:

calculating a first MAC using a message authentication code (MAC) algorithm over the validation data;

calculating a reader MKB by using the hash function over the media key block read from the read-only area of the medium;

calculating a second MAC using the MAC algorithm over the reader MKB;

comparing the first MAC to the second MAC; and

verifying the authenticity of the MKB if the first MAC matches the second MAC.

6. The method of claim 1, wherein the medium comprises a DVD-RAM (Digital Versatile Disc - Random Access Memory), and the second region comprises a control data area of the medium.

7. The method of claim 1, wherein the medium comprises a DVD-R (Digital Versatile Disc - Recordable), and the second region comprises a narrow burst cutting area of the medium.

8. The method of claim 1, wherein the medium comprises a DVD-RW (Digital Versatile Disc - Rewriteable), and the second region comprises a narrow burst cutting area of the medium.

9. A method, comprising:

on a first device:

reading a media key block stored on a read-only area of a medium;

reading a first validation data equal to a hash function of the media key block, the validation data being stored on a cutting area of the read-only area of the medium; and

calculating a media authentication code (MAC) algorithm over the first validation data to form a first MAC; and

on a second device:

calculating a second validation data equal to the hash function of the media key block that is read from the read-only area of the medium;

calculating the media authentication code (MAC) algorithm over the second validation data to form a second MAC;

comparing the first MAC and the second MAC; and

verifying the authenticity of the media key block read from the read-only area of the medium if the first MAC equals the second MAC.

10. The method of claim 9, wherein the medium comprises a DVD-R (Digital Versatile Disc - Recordable), and the second region comprises a narrow burst cutting area of the medium.

11. The method of claim 9, wherein the medium comprises a DVD-RW (Digital Versatile Disc - Rewriteable), and the second region comprises a narrow burst cutting area of the medium.

12. A method comprising:

reading a media key block from a first region of a read-only area of a medium;

generating a media key from the media key block;

reading validation data related to the media key block from a second region of a read-only area of the medium;

decrypting the validation data using the media key; and

verifying the authenticity of the media key block if the validation data decrypts to a predefined value.

13. The method of claim 12, wherein the validation data comprises a verification data field of the media key block's verify media key record.

14. The method of claim 12, wherein the predefined value comprises a hexadecimal value equal to DEADBEEF.

15. The method of claim 12, wherein the second region of the read-only area comprises a cutting area of the medium.

16. The method of claim 15, wherein the medium is protected using Content Protection For Recordable Media (CPRM) format.

17. The method of claim 16, wherein the cutting area comprises a burst cutting area, and the medium is one of:

a DVD-R (Digital Versatile Disc - Recordable); and

a DVD-RW (Digital Versatile Disc - Rewriteable).

18. A method comprising:

determining a media type associated with a medium to be read;

reading a media key block from a first region on a medium;

reading validation data related to the media block from a second region on the medium, the second region based on the determined media type; and

validating the media key block using the validation data.

19. The method of claim 18, wherein said validating the media key block using the validation data comprises:

comparing the media key block to the validation data; and

granting authorization to access the content if the media key block corresponds to the validation data.

20. The method of claim 18, wherein the media type comprises one of:

DVD-R (Digital Versatile Disc - Recordable); and

DVD-RW (Digital Versatile Disc - Rewriteable);

and the second region comprises the burst cutting area region of the read-only area of the medium.

21. The method of claim 18, wherein the media type comprises DVD-RAM (Digital Versatile Disc - Random Access Memory), and the second region comprises the control data area of the read-only area of the medium.

22. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

read a media key block from a first region on a medium;

read validation data related to the media block from a second region on the medium; and

validate the media key block using the validation data.

23. The machine-readable medium of claim 22, wherein said validating the media key block using the validation data comprises:

comparing the media key block to the validation data; and

granting authorization to access the content if the media key block corresponds to the validation data.

24. The machine-readable medium of claim 23, wherein the media key block corresponds to the validation data if the media key block matches the validation data.

25. The machine-readable medium of claim 23, wherein the media key block corresponds to the validation data if a hash function over the media key block matches the validation data.

26. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

read a media key block from a first region of a read-only area of a medium;

generate a media key from the media key block;

read validation data related to the media key block from a second region of a read-only area of the medium;

decrypt the validation data using the media key; and

verify the authenticity of the media key block if the validation data decrypts to a predefined value.

27. The machine-readable medium of claim 26, wherein the validation data comprises a verification data field of the media key block's verify media key record.

28. The machine-readable medium of claim 26, wherein the second region of the read-only area comprises a cutting area of the medium.

29. A machine readable medium, comprising:

a writeable area of the medium;

a content stored on the writeable area of the medium;

a read-only area of the medium having a cutting area region, and a non-cutting area region;

a media key block being stored on the non-cutting area region; and

validation data for verifying the authenticity of the media key block being stored on the cutting area region.

30. The machine-readable medium of claim 29, wherein the validation data comprises a preselected value that is encrypted.

31. The machine-readable medium of claim 30, wherein the encrypted, preselected value comprises a verify media key record of the media key block.

32. The machine-readable medium of claim 29, wherein the validation data comprises a hash function over the media key block.

33. The machine-readable medium of claim 29, wherein the validation data comprises a copy of a verification data field of a verify media key record of the media key block.

34. The machine-readable medium of claim 29, wherein the media comprises a digital versatile disc (DVD).

35. A system comprising:

a medium having:

a writeable area;

a content stored on the writeable area;

a read-only area having a cutting area region, and a non-cutting area region;

a media key block being stored on the non-cutting area region; and

a first validation data equal to a hash function of the media key block for verifying the authenticity of the media key block being stored on the cutting area region;

a drive to:

read a media key block stored on a read-only area of a medium;

read the first validation data from the cutting area region; and

calculate a media authentication code (MAC) algorithm over the first validation data to form a first MAC; and

a host to:

calculate a second validation data equal to the hash function of the media key block that is read from the read-only area of the medium;

calculate the media authentication code (MAC) algorithm over the second validation data to form a second MAC;

compare the first MAC and the second MAC; and

verify the authenticity of the media key block read from the read-only area of the medium if the first MAC equals the second MAC.

36. The system of claim 35, wherein the media comprises one of:

a DVD-R (Digital Versatile Disc - Recordable); and

a DVD-RW (Digital Versatile Disc - Rewriteable).

37. The system of claim 36, wherein the cutting area region comprises a narrow burst cutting area region of the read-only area of the medium.

38. A system comprising:

a medium having;

a writeable area;

a content stored on the writeable area;

a read-only area having a cutting area region, and a non-cutting area region;

a media key block being stored on the non-cutting area region; and

validation data for verifying the authenticity of the media key block being stored on the cutting area region; and

a device to;

read a media key block from a first region of a read-only area of a medium;

generate a media key from the media key block;

read validation data related to the media key block from a second region of a read-only area of the medium;

decrypt the validation data using the media key; and

verify the authenticity of the media key block if the validation data decrypts to a predefined value.

39. The system of claim 38, wherein the device comprises a consumer electronics device.

40. The system of claim 38, wherein the medium comprises a DVD-R (Digital Versatile Disc - Recordable), and the second region comprises a narrow burst cutting area of the medium.

41. The system of claim 38, wherein the medium comprises a DVD-RW (Digital Versatile Disc - Rewriteable), and the second region comprises a narrow burst cutting area of the medium.

42. An apparatus comprising:

means for reading a media key block from a first region of a read-only area of a medium;

means for generating a media key from the media key block;

means for reading validation data related to the media key block from a second region of a read-only area of the medium;

means for decrypting the validation data using the media key; and

means for verifying the authenticity of the media key block if the validation data decrypts to a predefined value.

43. The apparatus of claim 42, wherein the validation data comprises a verification data field of the media key block's verify media key record.

44. The apparatus of claim 42, wherein the second region of the read-only area comprises a cutting area of the medium.

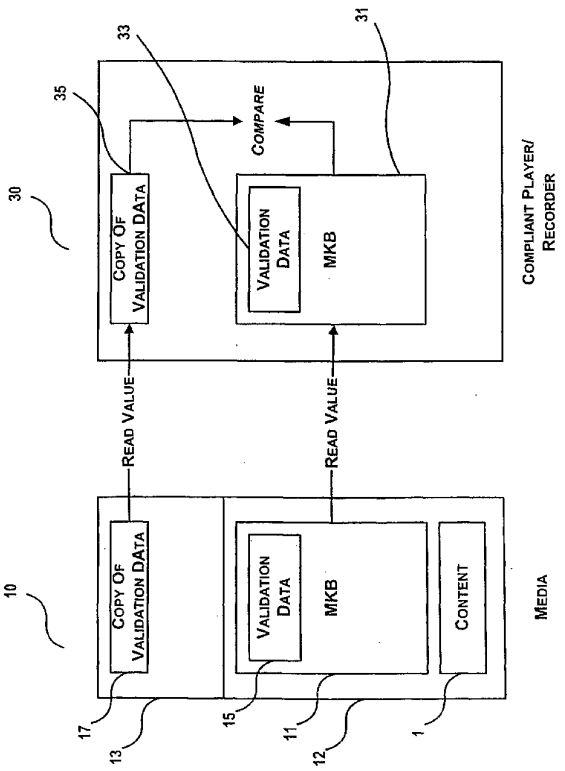

33
31
35
COMPARE
30
COPY OF VALIDATION DATA
VALIDATION DATA
MKB
COMPLIANT PLAYER/ RECORDER
READ VALUE
READ VALUE
10
COPY OF VALIDATION DATA
VALIDATION DATA
MKB
CONTENT
MEDIA
17
13
15
11
12
1

Fig. 1

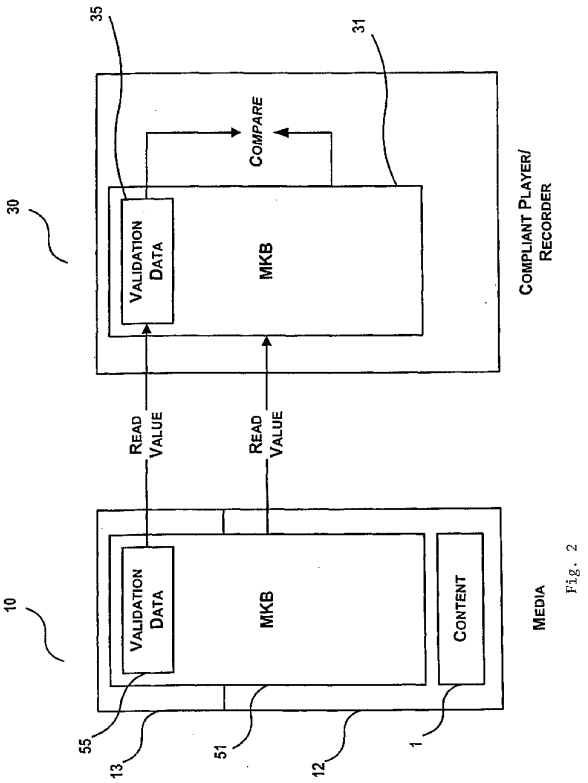

35
31
30
COMPARE
VALIDATION DATA
MKB
COMPLIANT PLAYER/ RECORDER
READ VALUE
READ VALUE
10
VALIDATION DATA
MKB
CONTENT
MEDIA
55
13
51
12
1

Fig. 2

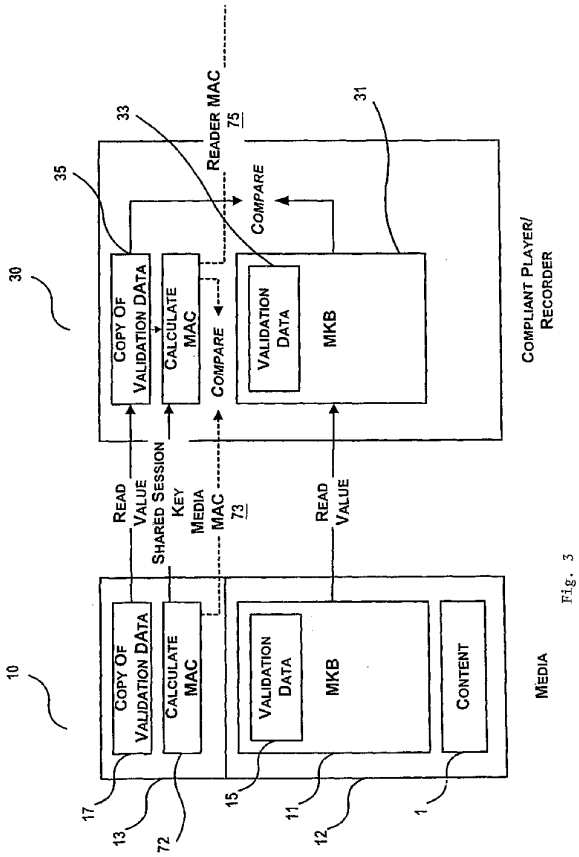

READER MAC
75
33
31
35
30
COMPARE
COPY OF VALIDATION DATA
CALCULATE MAC
COMPARE
VALIDATION DATA
MKB
COMPLIANT PLAYER/ RECORDER
READ VALUE
SHARED SESSION KEY
MEDIA MAC
73
READ VALUE
10
COPY OF VALIDATION DATA
CALCULATE MAC
VALIDATION DATA
MKB
CONTENT
MEDIA
17
13
72
15
11
12
1

Fig. 3

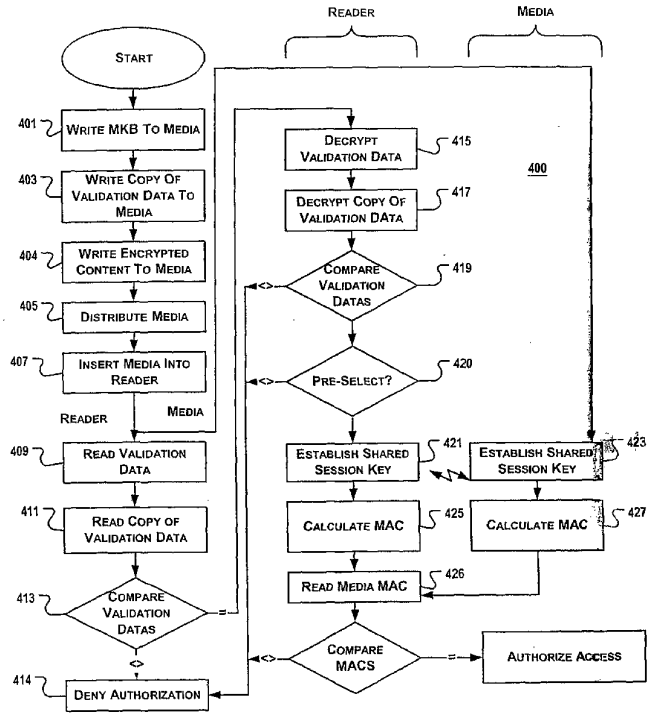

READER
MEDIA
START
401
WRITE MKB TO MEDIA
403
WRITE COPY OF VALIDATION DATA TO MEDIA
404
WRITE ENCRYPTED CONTENT TO MEDIA
405
DISTRIBUTE MEDIA
407
INSERT MEDIA INTO READER
READER
MEDIA
409
READ VALIDATION DATA
411
READ COPY OF VALIDATION DATA
413
COMPARE VALIDATION DATAS
=
<>
414
DENY AUTHORIZATION
DECRYPT VALIDATION DATA
415
400
DECRYPT COPY OF VALIDATION DATA
417
COMPARE VALIDATION DATAS
419
<>
PRE-SELECT?
420
<>
ESTABLISH SHARED SESSION KEY
421
ESTABLISH SHARED SESSION KEY
423
CALCULATE MAC
425
CALCULATE MAC
427
READ MEDIA MAC
426
COMPARE MACS
<>
=
AUTHORIZE ACCESS

FIG. 4

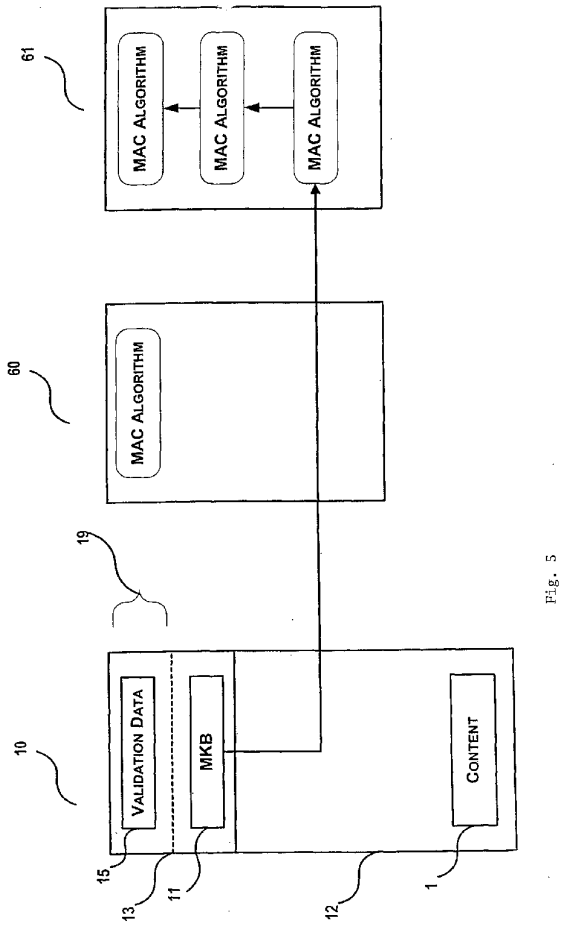

61
MAC ALGORITHM
MAC ALGORITHM
MAC ALGORITHM
60
MAC ALGORITHM
19
10
VALIDATION DATA
MKB
CONTENT
15
13
11
12
1

Fig. 5

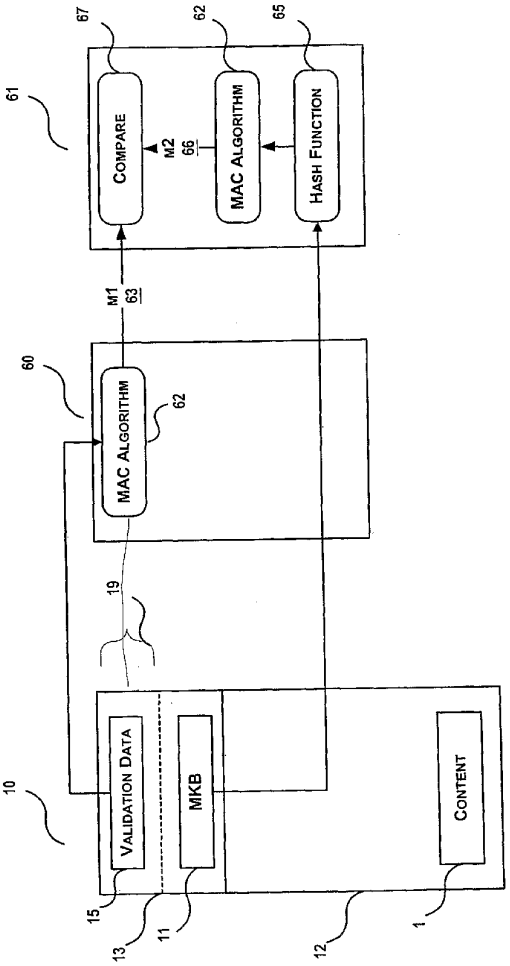

67
62
65
61
COMPARE
M2
66
MAC ALGORITHM
HASH FUNCTION
M1
63
60
MAC ALGORITHM
62
19
10
VALIDATION DATA
MKB
CONTENT
15
13
11
12
1

Fig. 6

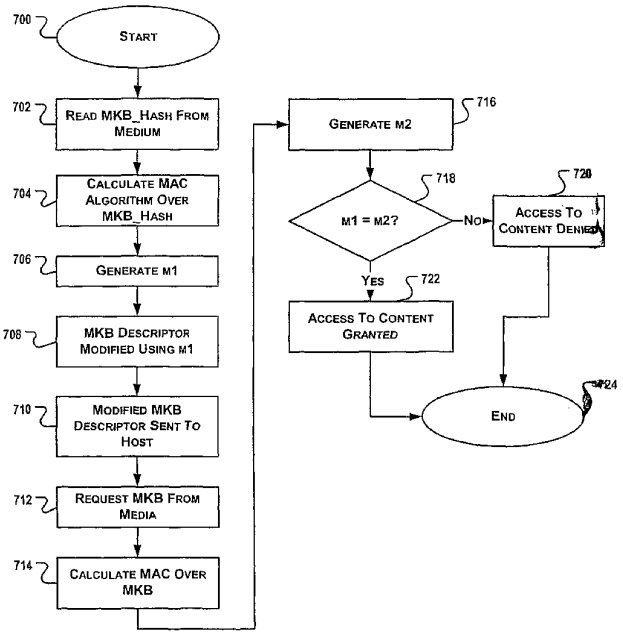

700
START
702
READ MKB_HASH FROM MEDIUM
704
CALCULATE MAC ALGORITHM OVER MKB_HASH
706
GENERATE m1
708
MKB DESCRIPTOR MODIFIED USING m1
710
MODIFIED MKB DESCRIPTOR SENT TO HOST
712
REQUEST MKB FROM MEDIA
714
CALCULATE MAC OVER MKB
716
GENERATE m2
718
m1 = m2?
No
720
ACCESS TO CONTENT DENIED
Yes
722
ACCESS TO CONTENT GRANTED
724
END

FIG. 7

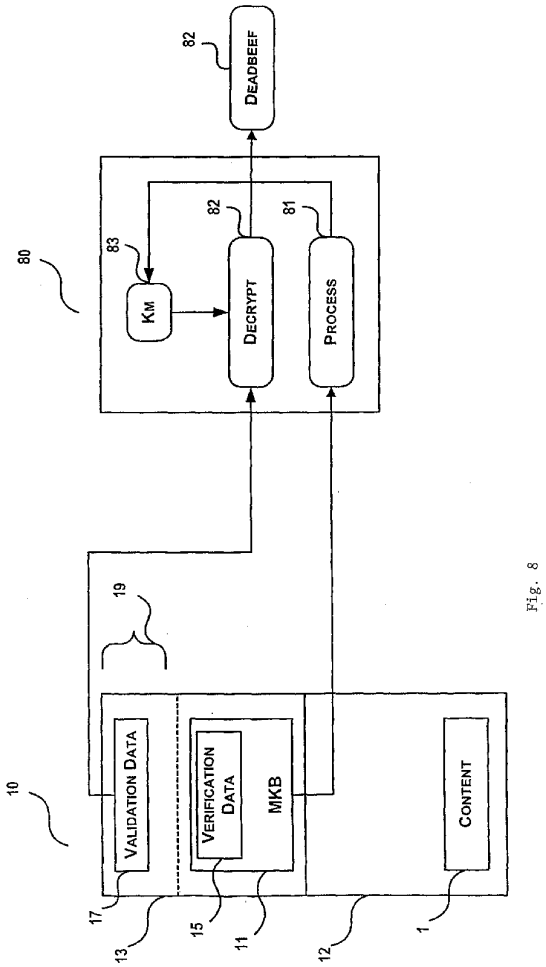

82
DEADBEEF
80
83
82
81
KM
DECRYPT
PROCESS
19
10
VALIDATION DATA
VERIFICATION DATA
MKB
CONTENT
17
13
15
11
12
1

Fig. 8

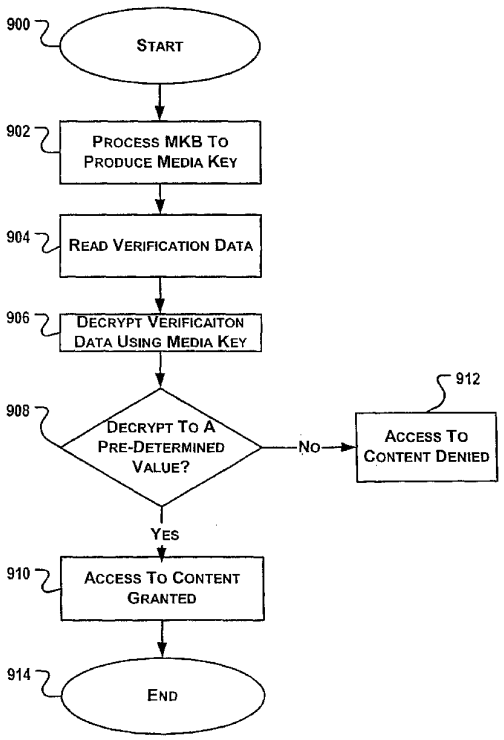

900
START
902
PROCESS MKB TO PRODUCE MEDIA KEY
904
READ VERIFICATION DATA
906
DECRYPT VERIFICAITON DATA USING MEDIA KEY
908
DECRYPT TO A PRE-DETERMINED VALUE?
No
912
ACCESS TO CONTENT DENIED
YES
910
ACCESS TO CONTENT GRANTED
914
END

FIG. 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int onal Application No
PCT/US 01/49784

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B 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 practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	INTEL CORPORATION ET AL: "Content Protection for Recordable Media Specification: DVD Book, Revision 0.94" 4C ENTITY, 18 October 2000 (2000-10-18), XP002167964 cited in the application	1,2,4,5, 7-17, 22-32, 34-44
A	page 3.1 -page 6.10	3,6,8, 18-21,33
P,X	WO 01 95327 A (KONINKL PHILIPS ELECTRONICS NV) 13 December 2001 (2001-12-13)	1,2,4,6, 22,23, 25,29, 30,32,34
P,A	the whole document	5,9,12, 18,21, 26,35, 38,39,42

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

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

Date of the actual completion of the international search	Date of mailing of the international search report
5 June 2002	12/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 01/49784

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 984 346 A (HITACHI EUROP LTD) 8 March 2000 (2000-03-08) column 2, line 29 - line 43 column 4, line 22 - line 44 column 5, line 1 - line 11 column 5, line 33 -column 6, line 42	1-3,6,7, 22-24, 29,34
A	column 8, line 35 -column 9, line 37	4,25,32

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/US 01/49784

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0195327 A	13-12-2001	AU 6391701 A	17-12-2001
		WO 0195327 A2	13-12-2001
		NO 20020528 A	21-03-2002
		US 2001049662 A1	06-12-2001
EP 0984346 A	08-03-2000	EP 0984346 A1	08-03-2000
		JP 2000076141 A	14-03-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51)Int.Cl.[7]	ＦＩ	テーマコード（参考）
Ｇ１１Ｂ 20/12	Ｇ１１Ｂ 20/12	

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,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,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZM,ZW

(72)発明者 ロッツピーチ，ジェフリー
アメリカ合衆国・９５１２３・カリフォルニア州・サン ノゼ・フットヒル ドライブ・９９２
(72)発明者 イシハラ，アツシ
〒２２７－００５横浜市青葉区つつじが丘２１－１１
(72)発明者 フクシマ，ヨシヒサ
〒５３６－０００８大阪府大阪市城東区関目６－１４－シイ－５０８

Ｆターム(参考) 5B017 AA06 CA09
5D044 BC04 CC04 DE17 DE50 GK12 GK18
5D090 AA01 CC04 CC18 DD03 FF09 GG36