(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2009-537029
(P2009-537029A)
(43)公表日　平成21年10月22日(2009.10.22)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 1/00	(2006.01)	G09C	1/00	660D	5B017
H04L 9/08	(2006.01)	H04L	9/00	601B	5C053
G06Q 50/00	(2006.01)	H04L	9/00	601E	5J104
G06F 21/24	(2006.01)	G06F	17/60	142	
H04N 5/91	(2006.01)	G06F	12/14	540A	

審査請求 有　予備審査請求 未請求　（全 15 頁）　最終頁に続く

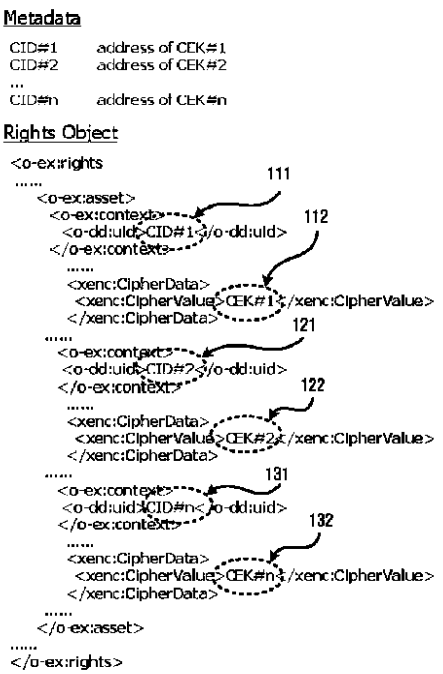
(21)出願番号　特願2009-509432 (P2009-509432)
(86)(22)出願日　平成19年5月10日 (2007.5.10)
(85)翻訳文提出日　平成20年11月11日 (2008.11.11)
(86)国際出願番号　PCT/KR2007/002298
(87)国際公開番号　WO2007/133007
(87)国際公開日　平成19年11月22日 (2007.11.22)
(31)優先権主張番号　60/799,652
(32)優先日　平成18年5月12日 (2006.5.12)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10-2007-0037396
(32)優先日　平成19年4月17日 (2007.4.17)
(33)優先権主張国　韓国 (KR)

(71)出願人　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国キョンギ－ド，スウォン－シ，ヨントン－ク，マエタン－ドン　４１６
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】コンテンツ暗号キーの位置を効率的に提供する方法および装置

(57)【要約】
コンテンツ暗号キーの位置を効率的に提供する方法および装置が提供される。
本発明の一実施形態によるコンテンツ暗号キーの位置を効率的に提供する方法は、権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を含むメタデータを生成する段階と、前記生成されたメタデータおよび前記権利オブジェクトを携帯用保存装置に設置する段階とを含む。



【特許請求の範囲】
【請求項１】
権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を含むメタデータを生成する段階と、
前記生成されたメタデータおよび前記権利オブジェクトを携帯用保存装置に設置する段階と、を含む、コンテンツ暗号キーの位置を効率的に提供する方法。
【請求項２】
前記生成されたメタデータを利用してコンテンツ暗号キーを検索する段階をさらに含む、請求項１に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項３】
前記メタデータは、
前記権利オブジェクトに記述されたコンテンツが２個以上である場合に、前記コンテンツ暗号キーの位置に対する情報に対応されるコンテンツ識別情報をさらに含む、請求項１に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項４】
前記コンテンツ暗号キーの位置に対する情報は、前記権利オブジェクトの開始の部分から前記コンテンツ暗号キーが存在する位置までのバイト数を利用して表示される、請求項１に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項５】
前記生成する段階は、
前記権利オブジェクトに記述された権限によってコンテンツを再生するホスト装置が前記メタデータを生成する段階を含む、請求項１に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項６】
前記設置する段階は、
前記ホスト装置が前記携帯用保存装置に前記メタデータおよび前記権利オブジェクトの設置を要請する段階と、
前記要請に応じて前記携帯用保存装置が前記メタデータおよび前記権利オブジェクトの設置空間の有無を確認して、その結果を前記ホスト装置に応答する段階と、
前記ホスト装置が前記設置空間が存在するという応答を受信する場合、前記メタデータおよび前記権利オブジェクトを前記携帯用保存装置に伝送する段階、および
前記携帯用保存装置が前記メタデータおよび前記権利オブジェクトを設置する段階と、を含む、請求項５に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項７】
前記設置する段階は、
前記携帯用保存装置が前記設置を完了する場合、設置完了メッセージを前記ホスト装置に伝送する段階と、
前記設置完了メッセージに応じて前記ホスト装置が前記携帯用保存装置に設置終了を要請する場合、前記携帯用保存装置が前記設置を終了する段階と、をさらに含む、請求項６に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項８】
前記生成する段階は、
前記権利オブジェクトに記述された権限によってコンテンツを再生するホスト装置が前記携帯用保存装置に前記メタデータおよび前記権利オブジェクトの設置を要請する段階と、
前記要請に応じて前記携帯用保存装置が前記メタデータおよび前記権利オブジェクトの設置空間の有無を確認して、その結果を前記ホスト装置に応答する段階と、
前記ホスト装置が前記設置空間が存在するという応答を受信する場合、前記権利オブジェクトを前記携帯用保存装置に伝送する段階、および
前記携帯用保存装置は、前記伝送された権利オブジェクトに対する前記メタデータを生

成する段階と、を含む、請求項１に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項９】
前記設置する段階は、
前記携帯用保存装置が前記生成されたメタデータおよび前記伝送された権利オブジェクトを設置する段階を含む、請求項８に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項１０】
前記設置する段階は、
前記携帯用保存装置が前記設置を完了する場合、設置完了メッセージを前記ホスト装置に伝送する段階と、
前記設置完了メッセージに応じて前記ホスト装置が前記携帯用保存装置に設置終了を要請する場合、前記携帯用保存装置が前記設置を終了する段階をさらに含む、請求項９に記載のコンテンツ暗号キーの位置を効率的に提供する方法。
【請求項１１】
権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を含むメタデータを生成するメタデータ生成部と、
前記生成されたメタデータおよび前記権利オブジェクトを携帯用保存装置に設置する設置部と、を含む、コンテンツ暗号キーの位置を効率的に提供する装置。
【請求項１２】
前記生成されたメタデータを利用してコンテンツ暗号キーを検索する検索部をさらに含む、請求項１１に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項１３】
前記メタデータは、
前記権利オブジェクトに記述されたコンテンツが２個以上である場合に、前記コンテンツ暗号キーの位置に対する情報に対応されるコンテンツ識別情報をさらに含む、請求項１１に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項１４】
前記コンテンツ暗号キーの位置に対する情報は、前記権利オブジェクトの開始の部分から前記コンテンツ暗号キーが存在する位置までのバイト数を利用して表示される、請求項１１に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項１５】
前記生成部は、
前記権利オブジェクトに記述された権限によってコンテンツを再生するホスト装置に前記メタデータを生成する、請求項１１に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項１６】
前記設置部は、
前記ホスト装置が前記携帯用保存装置に前記メタデータおよび前記権利オブジェクトの設置を要請する場合、前記要請に応じて前記メタデータおよび前記権利オブジェクトを設置する、請求項１５に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項１７】
前記設置空間が存在する場合、前記ホスト装置から前記携帯用保存装置に前記メタデータおよび前記権利オブジェクトを伝送する送受信部をさらに含む、請求項１５に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項１８】
前記設置部は、
前記送受信部が前記ホスト装置から前記携帯用保存装置に設置終了を要請するメッセージを伝送する場合、前記要請に応じて前記設置を終了する、請求項１７に記載のコンテンツ暗号キーの位置を効率的に提供する装置。

【請求項１９】
前記生成部は、
前記権利オブジェクトに記述された権限によってコンテンツを再生するホスト装置が前記携帯用保存装置に前記メタデータおよび前記権利オブジェクトの設置を要請する場合、前記要請に応じて前記携帯用保存装置に前記メタデータを生成する、請求項１１に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項２０】
前記設置空間が存在する場合、前記ホスト装置から前記携帯用保存装置に前記権利オブジェクトを伝送する送受信部をさらに含み、
前記生成部は、前記伝送された権利オブジェクトに対する前記メタデータを前記携帯用保存装置に生成する、請求項１９に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項２１】
前記設置部は、
前記生成されたメタデータおよび前記ホスト装置から伝送された権利オブジェクトを前記携帯用保存装置に設置する、請求項１９に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項２２】
前記設置部は、
前記送受信部が前記ホスト装置から前記携帯用保存装置に設置終了を要請するメッセージを伝送する場合、前記設置を終了する、請求項２１に記載のコンテンツ暗号キーの位置を効率的に提供する装置。
【請求項２３】
コンテンツ暗号キーの位置を効率的に提供する方法を実行するためにコンピュータによって実行されるプログラムコードを含むコンピュータで判読可能な記録媒体であって、前記方法は、
権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を含むメタデータを生成する段階、および
前記生成されたメタデータおよび前記権利オブジェクトを携帯用保存装置に設置する段階と、を含む、コンピュータで判読可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタル著作権管理技術に関するものであって、より詳細には、保安用マルチメディアカード（Ｓｅｃｕｒｅ　Ｍｕｌｔｉｍｅｄｉａ　Ｃａｒｄ）に権利オブジェクトを保存する場合にコンテンツ暗号キーの位置に対するメタデータを別途に添付して保存することによってコンテンツ暗号キーの位置を効率的に提供できるコンテンツ暗号キーの位置を効率的に提供する方法および装置に関するものである。
【背景技術】
【０００２】
最近、デジタル著作権管理（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ：以下「ＤＲＭ」という）を適用した商用サービスが導入されたり導入されつつある。ＤＲＭは、容易に不正コピーおよび配布できるデジタルコンテンツを保護するための技術概念である。
【０００３】
デジタルコンテンツを保護しようとする努力は従来にもあったが、それは主にデジタルコンテンツに対する不正アクセス防止に重点を置いていた。例えば、デジタルコンテンツに対するアクセス（ａｃｃｅｓｓ）は代価を払ったユーザだけに許され、代価を払わないユーザはデジタルコンテンツにアクセスできなかった。しかし、デジタルデータの特性上、デジタルコンテンツは再使用、加工、コピーおよび配布が容易であるため、代価を払っ

てデジタルコンテンツにアクセスしたユーザがこれを不正コピーまたは配布する場合には代価を払わないユーザもデジタルコンテンツを使用することができる。

【０００４】

このような問題点を克服するために、ＤＲＭはデジタルコンテンツを暗号化して配布し、暗号化されたデジタルコンテンツを使用するためには、権利オブジェクト（Ｒｉｇｈｔ Ｏｂｊｅｃｔ：ＲＯ）というライセンスが必要である。

【０００５】

一方、ホスト装置に保存された権利オブジェクトは、携帯用保存装置に移動（ｍｏｖｅ）またはコピー（ｃｏｐｙ）できる。ＸＤカードやマルチメディアカードのような携帯用保存装置は携帯電話、コンピュータ、デジタルカメラなどのようにホスト装置に容易に脱付着できる装置であり、従来のハードディスクやコンパクトディスク（ｃｏｍｐａｃｔ ｄｉｓｋ）が有する限界を超えて、単にデータの保存能力だけではなく、データに対する制御、演算などのようなコンピュータ機能を実行することができる。そして、このような携帯用保存装置に保安機能を追加してデジタルコンテンツの保存および送受信に対する保安により、デジタル著作権を保護できる新概念の携帯用保存装置が開発されている。したがって、携帯用保存装置とホスト装置間との関係に対してもＤＲＭを適用させることができる。すなわち、携帯用保存装置に権利オブジェクトを保存することができ、ホスト装置は携帯用保存装置に保存された権利オブジェクトを使用し暗号化されたコンテンツを再生させるようになる。

【０００６】

図１は、従来技術による権利オブジェクト内でのコンテンツ暗号キーを検索する過程を示す例示図である。前記図１に図示された権利オブジェクトは一つ以上のコンテンツに対する著作権を記述することができる。ユーザの望むコンテンツのコンテンツ暗号キーを獲得するために、先に権利オブジェクト内でコンテンツを記述する技術部を見つけなければならないが、これは図１の中間の部分に表示された＜ｏ－ｅｘ ｃｏｎｔｅｘｔ＞部分から始めて＜ｏ－ｅｘ ｐｅｒｍｉｓｓｉｏｎ＞部分までのボックスの部分（（１）部分）で記述されている。次に、（１）部分のコンテンツ技術部内でユーザの望むコンテンツと一致するコンテンツ識別情報（Ｃｏｎｔｅｎｔｓ ＩＤ）を見つけなければならないが、これは図１で＜ｏ－ｄｄ ｕｉｄ＞ＣｏｎｔｅｎｔＩＤ＜／ｏ－ｄｄ ｕｉｄ＞部分から始めて＜／ｏ－ｅｘ ａｓｓｅｔ＞部分までのボックスの部分（（２）部分）で記述されている。最後に、このように検索されたコンテンツ識別情報を記述した部分内でコンテンツ暗号キーを見つけるようになるが、これはＥｎｃｒｙｐｔｅｄＣＥＫと表示された部分（（３）部分）に示していることが分かる。

【０００７】

しかし、前述した従来技術により権利オブジェクト内でコンテンツ暗号キーを検索する過程は次のような問題がある。

【０００８】

最初に、権利オブジェクト内で特定のコンテンツ暗号キーだけが必要な場合でも該当コンテンツ識別情報のコンテンツ暗号キーを見つける時まで権利オブジェクトをいちいちパーシング（ｐａｒｓｉｎｇ）しなければならないという不便がある。

【０００９】

二つ目、このような権利オブジェクトをパーシングするためには該当権利オブジェクトを記述した言語のパーサー（ｐａｒｓｅｒ）が必要となるという問題がある。

【００１０】

三つ目、コンテンツ再生のようにコンテンツ暗号キーをリアルタイムで抽出しなければならない作業の場合において、必要ではない権利オブジェクトのパーシングにより応答速度を低下させるという問題がある。

【００１１】

四つ目、保安用マルチメディアカードのような低性能装置が権利オブジェクトのコンテンツ暗号キーを獲得するために前述した検索過程に従う場合、権利オブジェクトのパーシ

ング費用が高いため性能が低下するという問題がある。
【発明の開示】
【発明が解決しようとする課題】
【００１２】
本発明は、前記のような問題点を解決するために創案されたものであって、本発明が解決しようとする課題は、デジタル著作権を記述している権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を別途のメタデータで作成して、権利オブジェクトと共に設置することによって権利オブジェクト内でコンテンツ暗号キーをは速く、効率的に検索できるコンテンツ暗号キーの位置を効率的に提供する方法および装置を提供するものである。
【００１３】
本発明の目的は、以上で言及した目的に制限されなく、言及されていないまた他の目的は次の記載から当業者に明確に理解できるであろう。
【課題を解決するための手段】
【００１４】
前述した目的を達成するための本発明の一実施形態によるコンテンツ暗号キーの位置を効率的に提供する方法は、権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を含むメタデータを生成する段階と、前記生成されたメタデータおよび前記権利オブジェクトを携帯用保存装置に設置する段階と、を含む。
【００１５】
好ましくは、前記生成されたメタデータを利用してコンテンツ暗号キーを検索する段階をさらに含む。
【００１６】
また、前述した目的を達成するための本発明の一実施形態によるコンテンツ暗号キーの位置を効率的に提供する装置は、権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を含むメタデータを生成するメタデータ生成部と、前記生成されたメタデータおよび前記権利オブジェクトを携帯用保存装置に設置する設置部と、を含む。
【００１７】
好ましくは、前記生成されたメタデータを利用してコンテンツ暗号キーを検索する検索部をさらに含む。
【００１８】
その他実施形態の具体的な内容は詳細な説明および図に含まれている。
【発明の効果】
【００１９】
前記したような本発明の実施形態によれば次のような効果が一つ以上存在する。
【００２０】
デジタル著作権を記述している権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報を別途のメタデータで作成して権利オブジェクトと共に設置することによって、権利オブジェクト内でコンテンツ暗号キーを速く、効率的に検索することができる。
【００２１】
また、権利オブジェクトを保存した携帯用保存装置が必ず権利オブジェクトを記述した言語のパーサー（ｐａｒｓｅｒ）を有しなくても良いため、携帯用保存装置の要求リソースが節減される。
【００２２】
また、権利オブジェクト内でのコンテンツ暗号キーの抽出速度が速くなるため、コンテンツの再生時に応答速度が増加する。
【００２３】
本発明の効果は、以上で言及した効果に制限されず、言及されていないまた他の効果は請求範囲の記載から当業者に明確に理解できるであろう。
【発明を実施するための最良の形態】

【００２４】
本発明の利点、特徴、およびそれらを達成する方法は、添付される図面と共に詳細に後述される実施形態を参照すれば明確になるであろう。しかし、本発明は、以下で開示される実施形態に限定されるものではなく、互いに異なる多様な形態で具現されることが可能である。本実施形態は、単に本発明の開示が完全なように、本発明が属する技術分野で通常の知識を有する者に対して発明の範疇を完全に知らせるために提供されるものであり、本発明は、請求項の範囲によってのみ定義される。なお、明細書全体にかけて、同一の参照符号は同一の構成要素を指すものとする。
【００２５】
以下、添付された図面を参照して本発明の好ましい実施形態を詳細に説明する。 まず、本明細書で使用する用語の意味を簡略に説明するが、これは、発明の理解を助けるためのものであって、本発明を限定するものではない。したがって、本発明の詳細な説明で特に限定しない限り、以下で説明する用語は、本発明の技術的思想を限定するものとして使っているのではないことに注意しなければならない。
－ ＤＲＭ（Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ）：デジタル著作権管理を意味する。
－権利オブジェクト（Ｒｉｇｈｔｓ Ｏｂｊｅｃｔ ＲＯ）：暗号化されたデジタルコンテンツを使用するための権限と制約を記述した著作権オブジェクトであって一種のライセンスである。暗号化されたコンテンツに対する使用権限では、再生（Ｐｌａｙ）、ディスプレイ（Ｄｉｓｐｌａｙ）、実行（Ｅｘｅｃｕｔｅ）、印刷（Ｐｒｉｎｔ）、伝送（Ｅｘｐｏｒｔ：コピー、移動）あるいは閲覧などがある。本発明で定義する権利オブジェクトに対する好ましい例は、ＯＭＡ ＤＲＭ（Ｏｐｅｎ Ｍｏｂｉｌｅ Ａｌｌｉａｎｃｅ Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ）で定義する権利オブジェクトでありうる。
－ホスト（Ｈｏｓｔ）装置：携帯用保存装置と連結可能で、携帯用保存装置に保存された権利オブジェクトに記述された権限によって暗号化されたＤＲＭコンテンツを実行させることができる装置であって、一般的にカード接続部を有している。ホスト装置は、携帯電話、ＰＤＡ、ＭＰ３プレーヤなどの携帯用マルチメディア機器であり得、携帯用でないコンピュータ、デジタルＴＶのようなマルチメディア機器でありうる。
－携帯用保存装置：フラッシュメモリのようにデータを読み取り、書き込み、削除することができる性質を有する非揮発性メモリを含み、データに対する所定の演算能力を有し、ホスト装置との連結および分離が容易な保存装置を意味する。携帯用保存装置の例では、スマートカード、メモリスティック、ＣＦカード、ＸＤカード、マルチメディアカードなどがある。本発明の好ましい実施形態では、携帯用保存装置は所定の保安機能を有する保安用マルチメディアカード（Ｓｅｃｕｒｅ Ｍｕｌｔｉ－ｍｅｄｉａ Ｃａｒｄ Ｓｅｃｕｒｅ ＭＭＣ）でありうる。
－コンテンツ暗号キー（Ｃｏｎｔｅｎｔｓ Ｅｎｃｒｙｐｔｉｏｎ Ｋｅｙ ＣＥＫ）：暗号化されたコンテンツを復号化するキーであって権利オブジェクト内に暗号化された状態で存在する。
－ ＣＩＤ（Ｃｏｎｔｅｎｔｓ ＩＤ）：ホスト装置によって実行されるコンテンツの識別情報を意味する。
【００２６】
図２は、本発明の一実施形態による権利オブジェクトおよび前記権利オブジェクト内のコンテンツ暗号キーの位置情報を含むメタデータの構成を示す図である。
【００２７】
前記図２で図示した権利オブジェクトは、理解を助けるための例であり、ＯＭＡ ＤＲＭ ２．０のＲｉｇｈｔｓ Ｅｘｐｒｅｓｓｉｏｎ Ｌａｎｇｕａｇｅにより一つ以上のＤＲＭコンテンツに対する著作権を記述しているが、本発明の実施形態で言及している権利オブジェクトがＯＭＡ ＤＲＭ ２．０で限定されるものではない。
【００２８】

前記図２では、権利オブジェクト内に存在するコンテンツ暗号キーの位置に対する情報を別途のメタデータで抽出していることが分かる。権利オブジェクトのシェーマにはコンテンツ識別情報（Ｃｏｎｔｅｎｔｓ　ＩＤ：ＣＩＤ）とコンテンツ暗号キー（Ｃｏｎｔｅｎｔｓ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ：ＣＥＫ）が含まれているが、前記図２では第１コンテンツの識別情報であるＣＩＤ＃１（１１１）およびこれに対するコンテンツ暗号キーであるＣＥＫ＃１（１１２）、第２コンテンツの識別情報であるＣＩＤ＃２（１２１）およびこれに対するコンテンツ暗号キーであるＣＥＫ＃２（１２２）、第ｎコンテンツの識別情報であるＣＩＤ＃ｎ１３１およびこれに対するコンテンツ暗号キーであるＣＥＫ＃ｎ１３２が図示されていることが分かる。

【００２９】

しかし、前述した図１での方式を利用してコンテンツ暗号キーを検索する場合には、望むコンテンツ識別情報のコンテンツ暗号キーを見つける時まで権利オブジェクトをいちいちパーシング（ｐａｒｓｉｎｇ）しなければならず、該当権利オブジェクトを記述した言語のパーサー（ｐａｒｓｅｒ）が必要となるという不便さが存在した。このような不便さを防止するために、前記権利オブジェクト内に存在するコンテンツ暗号キーの位置情報を該当コンテンツ識別情報と対応させて提供するメタデータを権利オブジェクトと別途に添付して設置すれば、コンテンツを再生するコンテンツ暗号キーの位置を簡単で、効率的に検索できるであろう。さらには、権利オブジェクト内に記述されたコンテンツの数が多くなれば多くなるほどさらに効率的に検索できるであろう。前記図２では権利オブジェクトのシェーマと別途に、一つ以上のコンテンツ識別情報およびこれに対応するコンテンツ暗号キーの位置情報がメタデータで生成されていることが分かる。

【００３０】

一方、権利オブジェクトが管理するコンテンツが一つだけ存在して、コンテンツ暗号キーが一つだけ存在する場合、すなわち、区別しなければならない他のコンテンツ暗号キーがない場合においてのメタデータはコンテンツ識別情報を含む必要なく、コンテンツ暗号キーの位置情報だけを独立的に含むこともできる。

【００３１】

ここで、コンテンツ暗号キーの位置に対する情報は様々な方式で表現することができるが、本発明の実施形態では権利オブジェクトの開始の部分から該当コンテンツ暗号キーが存在する位置までのバイト（ｂｙｔｅｓ）数を利用して表示することができる。

【００３２】

以下、このようなメタデータを生成して設置する過程の実施形態を説明する。以下では、高性能装置であるホスト装置と低性能装置である携帯用保存装置を例えて説明するが、本発明の権利範囲が必ずこれに限定されものではない。

【００３３】

図３は、本発明の一実施形態による権利オブジェクトとメタデータの設置過程を示す例示図である。前記図３の実施形態ではホスト装置１００がメタデータを生成する主体であり、携帯用保存装置２００がメタデータおよび権利オブジェクトを設置する主体になる実施形態である。

【００３４】

先に、ホスト装置１００がコンテンツ暗号キーの位置に対する情報を含むメタデータを生成する（Ｓ１０２）。メタデータにはコンテンツ暗号キーの位置に対する情報に対応されるコンテンツ識別情報（ＣＩＤ）も共に含まれていることは前記図２の説明の部分で前述したことがある。

【００３５】

メタデータを生成した以後に、ホスト装置１００は携帯用保存装置２００にメタデータおよび前記権利オブジェクトの設置を要請する（Ｓ１０４）。このような要請を受けた携帯用保存装置２００はメタデータおよび権利オブジェクトの設置空間の有無を確認して（Ｓ１０６）、その結果をホスト装置１００に応答する（Ｓ１０８）。仮に、ホスト装置１００が前記設置空間が存在するという応答を受信する場合、メタデータおよび権利オブジ

ェクトを携帯用保存装置２００に伝送する（Ｓ１１０）。これの伝送を受けた携帯用保存装置２００はメタデータおよび権利オブジェクトを設置する（Ｓ１１２）。このとき、メタデータと権利オブジェクトを共に設置しても良いが、別途の保存空間に設置しても良い。

【００３６】

携帯用保存装置２００が前記設置を完了すると、設置完了メッセージをホスト装置１００に伝送する（Ｓ１１４）。設置完了メッセージを受信したホスト装置１００が携帯用保存装置２００に設置終了を要請すると（Ｓ１１６）、携帯用保存装置２００は設置を終了する（Ｓ１１８）。

【００３７】

メタデータおよび権利オブジェクトの設置が完了すると、携帯用保存装置２００はメタデータに含まれたコンテンツ暗号キーの位置情報を利用してコンテンツ暗号キーを検索できる。

【００３８】

図４は、本発明のまた他の一実施形態による権利オブジェクトとメタデータの設置過程を示す例示図である。前記図４の実施形態ではホスト装置１００がメタデータを生成するのではなく、携帯用保存装置２００がメタデータを生成する主体となり、またメタデータおよび権利オブジェクトを設置する主体となる実施形態である。

【００３９】

先に、ホスト装置１００が携帯用保存装置２００にメタデータおよび権利オブジェクトの設置を要請する（Ｓ２０２）。このような要請を受けた携帯用保存装置２００はメタデータおよび権利オブジェクトの設置空間の有無を確認して（Ｓ２０４）、その結果をホスト装置１００に応答する（Ｓ２０６）。

【００４０】

設置空間が存在するという応答を受信したホスト装置１００は権利オブジェクトを携帯用保存装置２００に伝送する（Ｓ２０８）。前記権利オブジェクトの伝送を受けた携帯用保存装置２００は前記権利オブジェクト内に存在するコンテンツ暗号キーの位置情報を記述しているメタデータを生成する（Ｓ２１０）。メタデータを一度生成した以後には携帯用保存装置２００はこれ以上メタデータを生成する必要がなくなる。次に、携帯用保存装置２００は生成されたメタデータおよび伝送された権利オブジェクトを設置する（Ｓ２１２）。

【００４１】

携帯用保存装置２００が前記設置を完了する場合には、設置完了メッセージをホスト装置１００に伝送して（Ｓ２１４）、前記設置完了メッセージに応じてホスト装置１００が携帯用保存装置２００に設置終了を要請する場合（Ｓ２１６）、携帯用保存装置２００は設置を終了する（Ｓ２１８）。

【００４２】

そして、前記図３の実施形態と同様に、設置が完了すると携帯用保存装置２００はメタデータに含まれたコンテンツ暗号キーの位置情報を利用してコンテンツ暗号キーを検索できる。

【００４３】

図５は、本発明の一実施形態によるコンテンツ暗号キーの位置を効率的に提供する装置の構成図である。

【００４４】

本図面の説明で使用される「～部」という用語、すなわち「～モジュール」または「～テーブル」などはソフトウェア、ＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）または注文型半導体（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ、ＡＳＩＣ）のようなハードウェアの構成要素を意味し、モジュールはある機能を果たす。しかし、モジュールは、ソフトウェアまたはハードウェアに限定される意味ではない。モジュールは、アドレッシングできる保存媒体

にあるように構成されることもでき、一つまたはそれ以上のプロセッサーを再生させるように構成されることもできる。

【００４５】

構成要素とモジュールのうちから提供される機能はさらに小さい数の構成要素およびモジュールに結合されたり追加的な構成要素とモジュールにさらに分離したりすることができる。のみならず、構成要素およびモジュールは、デバイス内の一つまたはそれ以上のＣＰＵを再生させるように具現されることもできる。

【００４６】

前記図５を参照して説明すると、コンテンツ暗号キーの位置を効率的に提供する装置３００は、生成部３１０、設置部３２０、検索部３３０および送受信部３４０を含み構成される。

【００４７】

生成部３１０は、権利オブジェクト内でのコンテンツ暗号キーの位置に対する情報および前記位置に対する情報に対応されるコンテンツ識別情報を含むメタデータを生成する役割を果たす。生成部３１０は、ホスト装置１００にメタデータを生成することもでき、携帯用保存装置２００に生成することもできる。携帯用保存装置２００にホスト装置１００がメタデータおよび権利オブジェクトの設置を要請する場合には、生成部３１０は携帯用保存装置２００にメタデータを生成する。

【００４８】

設置部３２０は、前記生成されたメタデータおよび前記権利オブジェクトを携帯用保存装置２００に設置する役割を果たすが、ホスト装置１００が携帯用保存装置２００にメタデータおよび権利オブジェクトの設置を要請する場合にはメタデータおよび権利オブジェクトを設置する。

【００４９】

検索部３３０は、生成されたメタデータを利用して権利オブジェクト内でコンテンツ暗号キーを検索する役割を果たす。

【００５０】

送受信部３４０は、ホスト装置１００から携帯用保存装置２００に権利オブジェクトを伝送したり、メタデータと権利オブジェクトを共に伝送したりする役割を果たす。また、送受信部３４０がホスト装置１００から携帯用保存装置２００に設置終了を要請するメッセージを伝送する場合、設置部３２０は前記要請に応じて設置を終了する。

【００５１】

一方、本発明の実施形態によるコンテンツ暗号キーの位置を効率的に提供する方法の権利範囲は、前記のような方法をコンピュータで実行するためのプログラムコードを記録したコンピュータで読み取りできる記録媒体にも及ぼすことは当業者に自明である。

【００５２】

以上添付された図面を参照して本発明の実施形態について説明したが、本発明が属する技術分野で通常の知識を有する者は、本発明が、その技術的思想や必須の特徴を変更しない範囲で他の具体的な形態で実施され得るということを理解できるものである。したがって、以上で記述した実施形態はすべての面で例示的なものであり、限定的でないものと理解しなければならない。

【図面の簡単な説明】

【００５３】

【図１】従来技術による権利オブジェクト内でのコンテンツ暗号キーを検索する過程を示す例示図である。

【図２】本発明の一実施形態による権利オブジェクトおよび前記権利オブジェクト内のコンテンツ暗号キーの位置情報を含むメタデータの構成を示す図である。

【図３】本発明の一実施形態による権利オブジェクトとメタデータの設置過程を示す例示図である。

【図４】本発明のまた他の一実施形態による権利オブジェクトとメタデータの設置過程を

示す例示図である。
【図５】本発明の一実施形態によるコンテンツ暗号キーの位置を効率的に提供する装置の構成図である。
【符号の説明】
【００５４】
１００　ホスト装置
２００　携帯用保存装置
３１０　生成部
３２０　設置部
３３０　検索部
３４０　送受信部

【図１】

Rights Object

```
<o-ex:rights
xmlns:o-ex=" http://odrl.net/1.1/ODRL-EX"
xmlns:o-dd=" http://odrl.net/1.1/ODRL-DD"
xmlns:oma-dd=" http://www.openmobilealliance.com/oma-dd"
xmlns:ds=" http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc=" http://www.w3.org/2001/04/xmlenc#"
o-ex:id=" C.1">
 <o-ex:context>
  <o-dd:version>2.0</o-dd:version>
  <o-dd:uid>RightsObjectID</o-dd:uid>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset>
   <o-ex:context>
    <o-dd:uid>ContentID</o-dd:uid>
   </o-ex:context>
   <o-ex:digest>
    <ds:DigestMethod Algorithm=" http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>DCFHash</ds:DigestValue>
   </o-ex:digest>
   <ds:KeyInfo>
    <xenc:EncryptedKey>
     <xenc:EncryptionMethod Algorithm=" http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
     <ds:KeyInfo>
      <ds:RetrievalMethod URI=" REKReference" />
     </ds:KeyInfo>
     <xenc:CipherData> (3)
      <xenc:CipherValue>EncryptedCEK</xenc:CipherValue>
     </xenc:CipherData>
    </xenc:EncryptedKey>
   </ds:KeyInfo>
  </o-ex:asset>
  <o-ex:permission>
   <o-dd:play/>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>
```

【図２】

[Fig. 2]

Metadata

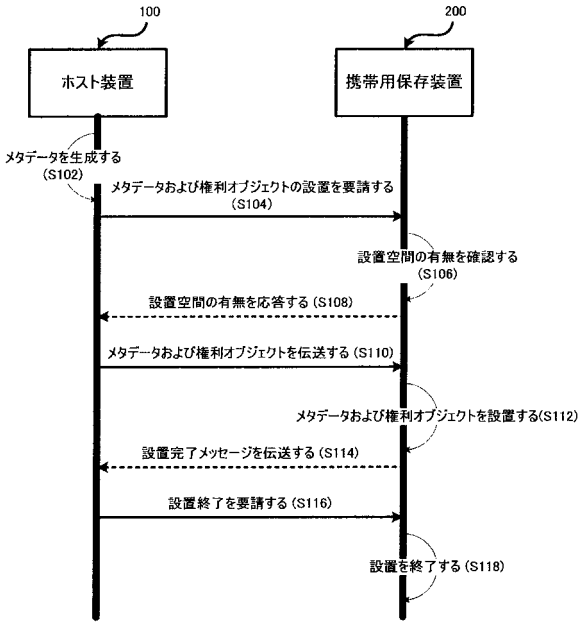
CID#1　address of CEK#1
CID#2　address of CEK#2
...
CID#n　address of CEK#n

Rights Object

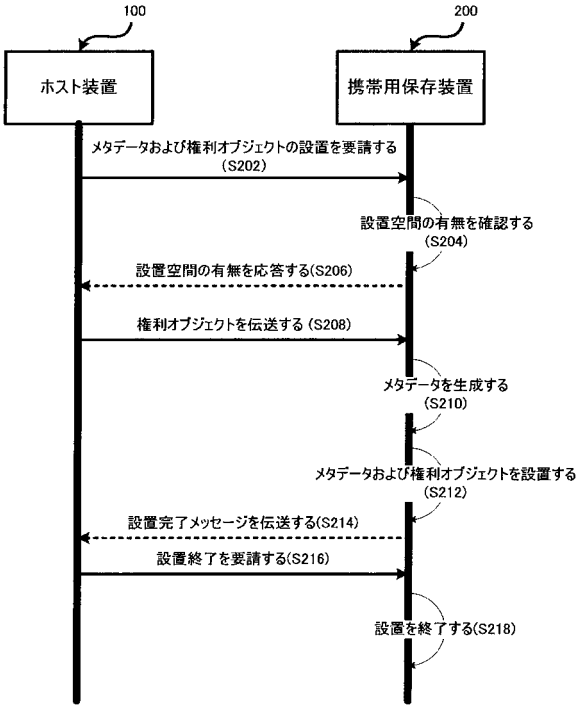
```
<o-ex:rights
 ......
   <o-ex:asset>
    <o-ex:context>
     <o-dd:uid>CID#1</o-dd:uid>
    </o-ex:context>
     ......
     <xenc:CipherData>
      <xenc:CipherValue>CEK#1</xenc:CipherValue>
     </xenc:CipherData>
 ......
    <o-ex:context>
     <o-dd:uid>CID#2</o-dd:uid>
    </o-ex:context>
     ......
     <xenc:CipherData>
      <xenc:CipherValue>CEK#2</xenc:CipherValue>
     </xenc:CipherData>
 ......
    <o-ex:context>
     <o-dd:uid>CID#n</o-dd:uid>
    </o-ex:context>
     ......
     <xenc:CipherData>
      <xenc:CipherValue>CEK#n</xenc:CipherValue>
     </xenc:CipherData>
 ......
   </o-ex:asset>
 ......
</o-ex:rights>
```

111
112
121
122
131
132

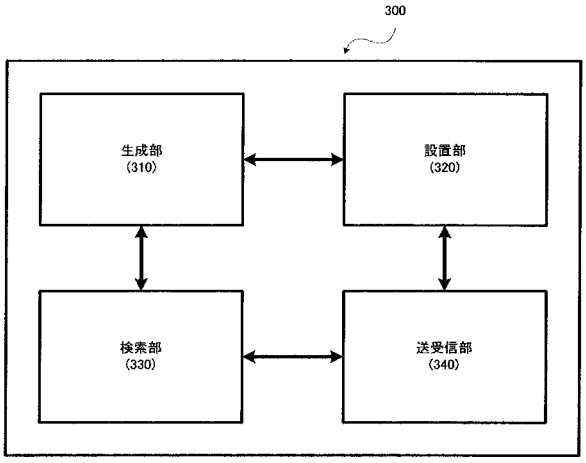
【図３】


100
200
ホスト装置
携帯用保存装置
メタデータを生成する
(S102)
メタデータおよび権利オブジェクトの設置を要請する
(S104)
設置空間の有無を確認する
(S106)
設置空間の有無を応答する (S108)
メタデータおよび権利オブジェクトを伝送する (S110)
メタデータおよび権利オブジェクトを設置する(S112)
設置完了メッセージを伝送する (S114)
設置終了を要請する (S116)
設置を終了する (S118)

【図４】


100
200
ホスト装置
携帯用保存装置
メタデータおよび権利オブジェクトの設置を要請する
(S202)
設置空間の有無を確認する
(S204)
設置空間の有無を応答する(S206)
権利オブジェクトを伝送する (S208)
メタデータを生成する
(S210)
メタデータおよび権利オブジェクトを設置する
(S212)
設置完了メッセージを伝送する(S214)
設置終了を要請する(S216)
設置を終了する(S218)

【図５】


300
生成部
(310)
設置部
(320)
検索部
(330)
送受信部
(340)

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/002298

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/00(2006.01)i

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)
IPC8 G06F 17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models since 1975
Japanese Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
ekipass "contents, encryption key, location, metadata, host, DRM, storage"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 20010050111 A (INTERNATIONAL BUSINESS MACHINES CO., LTD.) 15 JUN. 2001 See abstract; figures 1a~1d, 3. claims 1~3,6.	1-23
A	KR 20040072256 A (SAMSUNG ELECTRONICS CO., LTD.) 18 AUG. 2004 See abstract; figures 2~4. claims 1,4,8.	1-23
A	KR 20050066522 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 30 JUN. 2005 See abstract; figures 2,4,7. claims 1,4,7,9,15.	1-23
A	KR 20030055702 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 04 JUL. 2003 See abstract; figures 1,2,5. claims 1,2,4,14.	1-23

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
14 AUGUST 2007 (14.08.2007)	**14 AUGUST 2007 (14.08.2007)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer KIM, Jung Jin Telephone No. 82-42-481-5962

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2007/002298

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR20010050111A	15.06.2001	DE60030814C0	02.11.2006
		EP01077398A1	21.02.2001
		EP01077398B1	20.09.2006
		IL137880A0	31.10.2001
		US2002002468A1	03.01.2002
		US2002107803A1	08.08.2002
		US20030105718A1	05.06.2003
		US2006085343AA	20.04.2006
		US20060899912AA	27.04.2006
		US2006095792AA	04.05.2006
		US6611812BB	26.08.2003
		US6983371BA	03.01.2006
		US7110984BA	19.09.2006
		US7228437BB	05.06.2007
KR20040072256A	18.08.2004	US2004158707A1	12.08.2004
KR20050066522A	30.06.2005	US2005144439A1	30.06.2005
KR20030055702A	04.07.2003	US20030126434A1	03.07.2003

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	H04N 5/91	Z

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

(72)発明者 キム，ヨーージン
大韓民国 ４４２－８３５ キョンギード スウォンーシ パルダルーグ インゲードン １１１９ チャーマント・オフィステル ５０７号
(72)発明者 オー，ユンーサン
大韓民国 １３５－８５５ ソウル カンナムーグ ドゴック ２－ドン ケポ・ハンシン・アパート ８－７０３号（番地なし）
(72)発明者 シム，サンーギュー
大韓民国 ４４３－８２３ キョンギード スウォンーシ ヨントンーグ ウォンチョンードン ４１９－１７ ホサン・ヴィレッジ １０３－２０２号
(72)発明者 ジョン，キョンーイム
大韓民国 ４６３－７２８ キョンギード ソンナムーシ ブンダンーグ スネードン パークタウン・ロッテ・アパート １２８－９０３号（番地なし）
(72)発明者 キム，ジースー
大韓民国 ４４８－７５０ キョンギード ヨンインーシ スジーグ サンヒョンードン プンサン・アパート １０２－７０１号（番地なし）

Ｆターム(参考) 5B017 AA03 BA07 CA16
5C053 FA27 GB06 GB11 JA21 LA15
5J104 AA15 AA16 EA16 PA07 PA10