(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5911876号
(P5911876)
(45)発行日　平成28年4月27日(2016.4.27)　(24)登録日　平成28年4月8日(2016.4.8)

(51)Int.Cl.　　F I
G06F 21/44 (2013.01)　　G06F 21/44
H04L 9/32 (2006.01)　　H04L 9/00　673C

請求項の数 14　(全 8 頁)

(21)出願番号　特願2013-536530(P2013-536530)
(86)(22)出願日　平成23年10月28日(2011.10.28)
(65)公表番号　特表2013-544003(P2013-544003A)
(43)公表日　平成25年12月9日(2013.12.9)
(86)国際出願番号　PCT/KR2011/008160
(87)国際公開番号　WO2012/057577
(87)国際公開日　平成24年5月3日(2012.5.3)
審査請求日　平成26年10月28日(2014.10.28)
(31)優先権主張番号　10-2010-0107317
(32)優先日　平成22年10月29日(2010.10.29)
(33)優先権主張国　韓国(KR)

(73)特許権者　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・４４３－７４２・キョンギ－ド・スウォン－シ・ヨントン－ク・サムスン－ロ・１２９
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　ボ－ギョン・カン
大韓民国・キョンギ－ド・４４３－７１４・スウォン－シ・メタン・３－ドン・（番地なし）・リムワン・アパート・＃１－６０７

最終頁に続く

(54)【発明の名称】記憶装置、記憶装置の認証方法及び認証装置

(57)【特許請求の範囲】
【請求項１】
ホスト装置による記憶装置の認証方法であって、
複数の符号化された個別ＩＤを格納した記憶装置から前記複数の符号化された個別ＩＤのうち一つの符号化された個別ＩＤを受信するステップと、
前記符号化された個別ＩＤを復号化するステップと、
個別ＩＤに対応する認証情報を前記記憶装置から受信するステップと、
前記認証情報を用いて前記復号化された個別ＩＤを検証するステップと、を含むことを特徴とする記憶装置の認証方法。
【請求項２】
前記複数の符号化された個別ＩＤは、複数の使用用途に対応することを特徴とする請求項１に記載の記憶装置の認証方法。
【請求項３】
前記認証情報は、前記復号化された個別ＩＤを暗号化アルゴリズムを通して暗号化することで生成されたデータを用いて検証されることを特徴とする請求項１に記載の記憶装置の認証方法。
【請求項４】
前記認証情報は、前記復号化された個別ＩＤを暗号化アルゴリズムを通して暗号化することで生成されたデータとの比較を通して検証されることを特徴とする請求項１に記載の記憶装置の認証方法。

【請求項５】
前記検証が失敗した場合、前記記憶装置の認証を中断するステップをさらに含むことを特徴とする請求項１に記載の記憶装置の認証方法。
【請求項６】
記憶装置を認証するためのホスト装置であって、
複数の符号化された個別ＩＤを格納した記憶装置から前記複数の符号化された個別ＩＤのうち一つの符号化された個別ＩＤを受信し、前記符号化された個別ＩＤを復号化するＩＤデコーダと、
個別ＩＤに対応する認証情報を前記記憶装置から受信し、前記認証情報を用いて前記復号化された個別ＩＤを検証する認証処理部(Authenticator)と、を含むことを特徴とするホスト装置。
【請求項７】
前記複数の符号化された個別ＩＤは、複数の使用用途に対応することを特徴とする請求項６に記載のホスト装置。
【請求項８】
前記認証情報は、前記復号化された個別ＩＤを暗号化アルゴリズムを通して暗号化することで生成されたデータを用いて検証されることを特徴とする請求項６に記載のホスト装置。
【請求項９】
前記認証情報は、前記復号化された個別ＩＤを暗号化アルゴリズムを通して暗号化することで生成されたデータとの比較を通して検証されることを特徴とする請求項６に記載のホスト装置。
【請求項１０】
前記認証処理部は、前記検証が失敗した場合、前記記憶装置の認証を中断することを特徴とする請求項６に記載のホスト装置。
【請求項１１】
ホスト装置で記憶装置を認証するために使用される情報の前記記憶装置からの伝送方法であって、
前記記憶装置に格納された複数の符号化された個別ＩＤのうち一つの符号化された個別ＩＤをホスト装置に伝送するステップと、
個別ＩＤに対応する認証情報を前記ホスト装置に伝送するステップと、を含み、
前記認証情報は、前記個別ＩＤを暗号化アルゴリズムを通して暗号化することで生成されることを特徴とする伝送方法。
【請求項１２】
前記複数の符号化された個別ＩＤは、複数の使用用途に対応することを特徴とする請求項１１に記載の伝送方法。
【請求項１３】
記憶装置であって、
複数の符号化された個別ＩＤを格納するＥＩＤ(Encoded IDentifier)領域と、
前記複数の符号化された個別ＩＤのうち一つの符号化された個別ＩＤをホスト装置に伝送し、個別ＩＤに対応する認証情報を前記ホスト装置に伝送するように構成されたコントローラと、を含み、
前記認証情報は、前記個別ＩＤを暗号化アルゴリズムを通して暗号化することで生成されることを特徴とする記憶装置。
【請求項１４】
前記複数の符号化された個別ＩＤは、複数の使用用途に対応することを特徴とする請求項１３に記載の記憶装置。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、不揮発性記憶装置に関し、特に不揮発性記憶装置の認証方法及び装置に関する。

【背景技術】

【０００２】

デジタル著作権管理(Digital Rights Management:ＤＲＭ)技術、ＳＤ(Secure Digital)カードのためのＣＰＲＭ(Content Protection for Recordable Media)技術及びブルーレイ(Blue-ray)ディスクのためのＡＡＣＳ(Advanced Access Content System)技術では、公開キー基盤(Public Key Infrastructure:ＰＫＩ)のような暗号技術(cryptographic technology）を用いて記憶装置の認証を遂行する。

一般的に記憶装置は、記憶装置自らのセキュリティ(Security)用途に関係なく固有な識別子を使用する。記憶装置が、上記のような認証手順によって適合しない保存媒体であると判別されると、別途の手順を通じて該当記憶装置は廃棄される。

ＳＤカードのＣＰＲＭ技術、ブルーレイディスクのためのＡＡＣＳ等の技術が提案する機器認証方法は、保存媒体の生産当時に、読み取り専用領域(Read-Only Area)として指定された位置に任意の識別子(Identifier)を格納し、暗号スキーム(Cryptographic Scheme）を適用して機器認証及びコンテンツ保護などに使用する方法である。

しかしながら、以後、記憶装置の不正使用により識別子を廃棄する場合、記憶装置(例えば、ＳＤカード、ブルーレイディスク)をいかなる用途としても活用できなくなる問題点が発生する。

これによって、記憶装置の各種用途によって、識別子を提供する方法が要求される。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

本発明の目的は、少なくとも上述した問題点及び／又は不都合に取り組み、少なくとも以下の便宜を提供することにある。すなわち、本発明の目的は、記憶装置の用途によって識別子を多様に提供して、識別子別に個別的に認証を遂行する記憶装置と、その記憶装置の認証方法及び装置を提供することにある。

【課題を解決するための手段】

【０００４】

上記のような目的を達成するために、本発明の実施形態の一態様によれば、記憶装置の認証方法を提供する。上記方法は、上記記憶装置を認証するための認証装置が上記記憶装置にＥＩＤ(Encoded IDentifier)を要請するステップと、上記要請に対応して上記認証装置が上記記憶装置からＥＩＤを受信するステップと、上記受信したＥＩＤを復号化して元来のＩＤ情報を復元するステップと、上記記憶装置から受信したＩＤ認証情報を用いて上記ＩＤ情報に含まれた上記記憶装置の使用用途に対応する個別ＩＤ情報を検証するステップと、を含み、上記ＩＤ情報は、前記記憶装置の使用用途に対応する複数個の個別ＩＤ情報を含むことを特徴とする。

【０００５】

本発明の実施形態の他の態様によれば、記憶装置を認証するための認証装置を提供する。上記認証装置は、記憶装置を認証するための認証装置が上記記憶装置にＥＩＤ(Encoded IDentifier)情報を要請し、上記要請に対応して上記認証装置が上記記憶装置からＥＩＤを受信し、上記受信したＥＩＤを復号化して元来のＩＤ情報を復元するＩＤデコーダと、上記記憶装置から受信したＩＤ認証情報を用いて上記ＩＤ情報に含まれた上記記憶装置の使用用途に対応する個別ＩＤ情報を検証する認証処理部(Authenticator）と、を含み、上記ＩＤ情報は、上記記憶装置の使用用途に対応する複数個の個別ＩＤ情報を含むことを特徴とする。

【０００６】

本発明の実施形態のさらに他の態様によれば、記憶装置を提供する。上記記憶装置は、上記記憶装置の特定領域に位置し、上記記憶装置の固有な識別のためのＥＩＤ(Encoded IDentifier)を格納するＥＩＤ領域と、上記ＩＤ情報を検証するための情報を含むＩＤ認証

情報と、上記ＥＩＤと上記ＩＤ認証情報が上記記憶装置の認証を遂行する認証装置に伝達されるように制御するコントローラと、を含み、上記ＩＤ情報は、上記記憶装置の使用用途に対応する複数の個別ＩＤ情報を含むことを特徴とする。

【発明の効果】

【０００７】

本発明は、記憶装置の用途によって識別子を多様に提供し、識別子別に個別的に認証を遂行する。これによって記憶装置の特定用途の識別子が認証に失敗した場合、該当記憶装置を全体的に使用できなくなる代わりに、認証に失敗した特定用途の機能だけを個別的に廃棄することができる。これによって記憶装置の特定用途の機能が廃棄されても、他の用途で記憶装置を継続使用することができるようにして記憶装置の活用性を高める効果がある。また本発明の記憶装置は、このような多様な識別子に対する認証手順を同じ認証装置(ＩＤデコーダ)を用いて同じ方式で遂行することができる。

本発明による実施形態の上記及び他の態様、特徴、及び利点は、添付の図面と共に述べる以下の詳細な説明から、一層明らかになるはずである。

【図面の簡単な説明】

【０００８】

【図１】本発明の一実施形態による識別子の構造及び記憶装置の構成を示した図である。

【図２】本発明の一実施形態による記憶装置の認証を遂行する認証装置の構成を示した図である

【図３】本発明の一実施形態による記憶装置の認証を遂行する動作の流れを示した図である。

【発明を実施するための形態】

【０００９】

以下、本発明の好適な実施形態について添付図面を参照しながら詳細に説明する。図面における同様な構成要素に対しては、他の図面に表示されても、同様な参照番号及び符号を付けてあることに注意されたい。また、明瞭性及び簡潔性の観点から、本発明に関連した公知の機能や構成に関する具体的な説明が本発明の要旨を不明瞭にすると判断される場合には、その詳細な説明を省略する。

【００１０】

本発明は、不揮発性(Non-volatile)記憶装置の活用性を高めることができる記憶装置の用途に従う個別的な認証方法及び装置を提案する。このために、本発明の記憶装置は、記憶装置のそれぞれの機能に対応する複数のＩＤで構成されたＩＤを符号化して特定領域に含む。上記記憶装置を認証する認証装置は、記憶装置を使用するとき、ＩＤデコーダを用いて元来のＩＤを復元し、使用用途に該当するＩＤを検証して認証を遂行する。本発明は、記憶装置が特定用途で不正に利用されて認証に失敗した場合、認証に失敗したＩＤに該当する用途だけを不正使用を防ぐために廃棄する。これによって該当記憶装置は他の用途で継続活用することができる。

以下、図面を参照して本発明の構成及び動作に対して詳細に説明する。

【００１１】

図１は、本発明の一実施形態による識別子の構造及び記憶装置の構成を示した図である。

【００１２】

図１において、記憶装置１３０を識別するための識別子(ＩＤ)１１０は、複数の個別ＩＤ(ＩＤ_ｉ)とチェックサム(checksum)を含む。識別子の個別ＩＤ(ＩＤ_ｉ)は、記憶装置の各使用用途に従う識別のために使用される。本発明の実施形態で記憶装置は、コンテンツ保存用途他にも個人情報の保存、ＤＲＭのような文書暗号技術を利用したデータ保存、認証書情報保存などのような多様な用途で使用されることができ、本発明は、このようなそれぞれの用途によって個別的にＩＤを生成することができる。

【００１３】

図１を参照すれば、ＩＤエンコーダ１２０は、記憶装置１３０を識別するための識別子

(ＩＤ)１１０を用いて符号化されたＩＤ(Encoded ID:ＥＩＤ)を生成する。

【００１４】

記憶装置１３０は、ＥＩＤ１３１とＩＤ１１０のそれぞれの個別ＩＤに対応する認証書情報(Certificate)１３２を含む。認証書情報１３２は、記憶装置を認証する認証装置が復元したＩＤの適合性を検証するための情報である。

【００１５】

記憶装置１３０を識別するための識別子１１０は、記憶装置１３０の生成またはテスト段階で、ＩＤエンコーダ１２０を通して符号化され、ＥＩＤ１３１に変換され、このようなＥＩＤ１３１は、記憶装置１３０にプログラムされる。

【００１６】

以後、記憶装置１３０のレコーディングまたは再生のとき、レコーディングまたは再生を遂行するホスト装置は、上記ＥＩＤを用いて記憶装置の認証を遂行する。

【００１７】

図２は、本発明の一実施形態による記憶装置の認証を遂行する認証装置の構成を示した図である。

【００１８】

図２を参照すれば、記憶装置１３０は、符号化されたＩＤ情報を格納するＥＩＤ１３１と個別ＩＤを検証するための複数の認証書情報１３２を含み、映画のような映像データ１３３と個人情報１３４等のデータを格納することができる。また記憶装置１３０は、記憶装置の入出力、読み取り書き取りを制御するためのコントローラ(図示せず)をさらに含む。

コントローラは、記憶装置を認証するために、ＩＤ認証情報がＥＩＤに伝達されるように制御する。

【００１９】

図２で、記憶装置１３０を認証する認証装置(ホスト装置)１４０は、ＥＩＤデコーダ１４１と、認証処理部 (Authenticator)１４２と、コンテンツ復号化／再生モジュール１４３を含む。

【００２０】

ＥＩＤデコーダ１４１は、記憶装置１３０からＥＩＤを受信して元来のＩＤを復元する。

【００２１】

認証処理部１４２は、 ＥＩＤデコーダ１４１から出力された記憶装置１３０のＩＤを受信し、暗号学的検証を遂行して記憶装置の認証を遂行する。この場合、認証装置１４０、すなわちホスト装置は、ホスト装置が使用しようとする記憶装置の用途によって、それに対応する記憶装置の個別ＩＤ(ＩＤ_ｉ)及び認証書情報１３２を用いて記憶装置１３０の適合性を判断する。

【００２２】

コンテンツ復号化／再生モジュール１４３は、認証処理部１４２により個別ＩＤの適合性が判断されると、個別ＩＤ値を用いてコンテンツ復号化キーを生成してコンテンツを復号化してコンテンツ再生を遂行する。

【００２３】

ＥＩＤデコーダ１４１は、記憶装置１３０の認証時、記憶装置１３０のＥＩＤ領域１３１からＥＩＤを受信し、認証処理部１４２は記憶装置から認証書情報１３２を受信する。

【００２４】

記憶装置１３０の個別ＩＤを検証するために、認証書情報１３２を利用する公開キー基盤(Public Key Infrastructure：ＰＫＩ)を使用したが、本発明はこれは限定されない。ブロードキャストキー管理技法を使用する時には、認証書情報１３２の代わりに、各用途に従うキー管理の可能なキーの集合が提供されることができる。またＰＫＩ方式とブロードキャストキー管理技法を混合して使用することもできる。このような場合には記憶装置１３０は、認証書情報とキー管理の可能なキーの集合の両方とも含むことができる。

【００２５】
図３は、本発明の一実施形態による記憶装置の認証を遂行する動作の流れを示した図である。
【００２６】
図３を参照すれば、記憶装置１３０をレコーディングあるいは再生するためのホスト装置が記憶装置１３０の特定コンテンツに対するアクセス要請を受信すれば、ステップ３１０でホスト装置に含まれた記憶装置１３０を認証するための認証装置１４０は、ＥＩＤデコーダ１４１を通して記憶装置１３０にＥＩＤを要請し、該当要請によって記憶装置１３０からＥＩＤを受信する。
【００２７】
この場合、ＩＤデコーダ１４１は、記憶装置１３０の使用用途によってＥＩＤの中で記憶装置１３０の使用用途に対応する符号化された個別ＩＤ(ＩＤ_ｉ)だけを記憶装置１３０から受信するように設定することができる。詳細に説明すれば、ＩＤデコーダ１４１が記憶装置１３０にＥＩＤを要請するとき、ＩＤデコーダ１４１は、記憶装置１３０の使用用途に対する情報を共に伝達し、記憶装置１３０はこのような情報に基づいて使用用途に対応する符号化された個別ＩＤだけをＥＩＤ１３１から抽出し、抽出された符号化された個別ＩＤをＩＤデコーダ１４１に伝達する。
【００２８】
一方、ステップ３１０でＩＤデコーダ１４１は、記憶装置１３０の全体ＥＩＤを受信して今後段階で記憶装置１３０の使用用途に該当する個別ＩＤだけを使用するように設定することができる。
【００２９】
ステップ３２０で、ＥＩＤデコーダ１４１は、受信したＥＩＤを用いて元来のＩＤを復元する。
【００３０】
ステップ３３０で、認証処理部１４２は、復元されたＩＤから記憶装置の使用用途(特定コンテンツ)に対応する個別ＩＤ(ＩＤ_ｉ)を確認する。この場合、認証処理部１４２は、記憶装置から個別ＩＤに対応する認証書情報１３２を受信する。
【００３１】
ステップ３４０で、認証処理部１４２は、認証書情報１３２を用いて個別ＩＤ ＩＤ_ｉの有効性を検証する。このような有効性検証には、下記のようなアルゴリズム１が使用されることができる。
[アルゴリズム１]
Hash(ID_i)=?checksum
【００３２】
ステップ３５０で、個別ＩＤの有効性が立証されたか判断する。仮りに個別ＩＤが適合でないと判断されると、プロセスは終了する。一方、このような場合、ホスト装置はコンテンツの再生動作を中止し、予め設定されたライセンス検証サイト(License Authority Site)などに接続して該当記憶装置１３０の該当用途に対する廃棄事由を伝送して廃棄を要請することができる。
【００３３】
ステップ３５０で、個別ＩＤが適合であると判断されると、ステップ３６０に進行してコンテンツ復号化／再生モジュール１４３を呼び出し、個別ＩＤ（ＩＤ_ｉ）をコンテンツ復号化／再生モジュール１４３に伝達する。
【００３４】
次のステップ３７０で、コンテンツ復号化／再生モジュール１４３は、検証された個別ＩＤが映像データ用として定義された場合、個別ＩＤを用いてコンテンツ復号化キーを生成する。この場合、コンテンツ復号化キーを生成するときには、下記のようなアルゴリズム２が使用されることができる。
[アルゴリズム２]

Hash(ID_i、Decryption Key)=ContentsDecryptionKey)

【００３５】

次のステップ３８０でコンテンツの復号化及び再生を遂行する。

【００３６】

本発明は、記憶装置の用途によって識別子を多様に提供して識別子別に個別的に認証を遂行する。これによって記憶装置の特定用途の識別子が認証に失敗した場合、該当記憶装置を全体的に使用できなくなる代わりに、認証に失敗した特定用途の機能だけを個別的に廃棄するようにすることができる。これによって記憶装置の特定用途の機能が廃棄されても他の用途で記憶装置を継続使用することができるようにして記憶装置の活用性を高める効果がある。また本発明の記憶装置はこのような多様な識別子に対する認証手順を同じ認証装置(ＩＤデコーダ)を用いて同じ方式で遂行することができる。

【００３７】

上記のように本発明の一実施形態に従う記憶装置と、記憶装置の認証方法及び装置の構成及び動作がなされることができる。

【００３８】

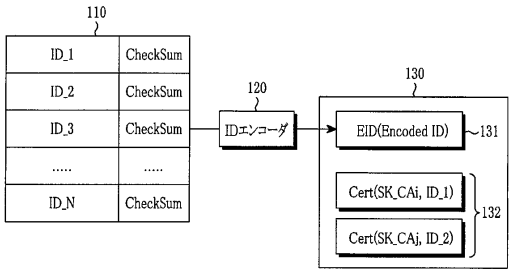
以上、本発明を具体的な実施形態を参照して詳細に説明してきたが、本発明の範囲及び趣旨を逸脱することなく様々な変更が可能であるということは、当業者には明らかであり、本発明の範囲は、上述の実施形態に限定されるべきではなく、特許請求の範囲の記載及びこれと均等なものの範囲内で定められるべきである。

【符号の説明】

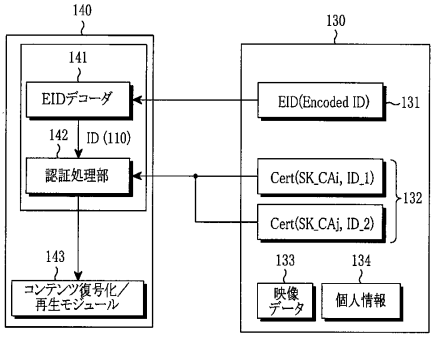
【００３９】

１１０　識別子（ＩＤ）
１２０　ＩＤエンコーダ
１３０　記憶装置
１４０　認証装置

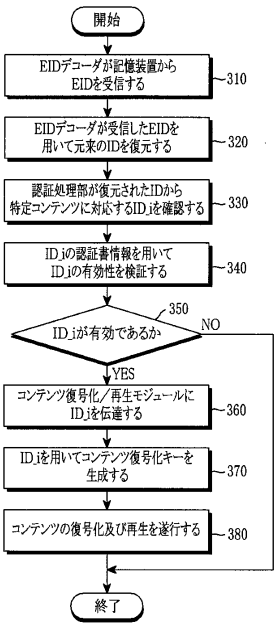
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　ビュンーレ・イ
大韓民国・ソウル・１３７－９１８・ソチョーグ・ソチョ・１－ドン・（番地なし）・レミアン・ソチョ・ユニヴィル・＃１１１５

審査官　中里　裕正

(56)参考文献　特開２００９－１００３９４（ＪＰ，Ａ）
国際公開第２０１０／０３５４４９（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４
Ｈ０４Ｌ　９／３２