

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2007 年 12 月 27 日 (27.12.2007)

PCT

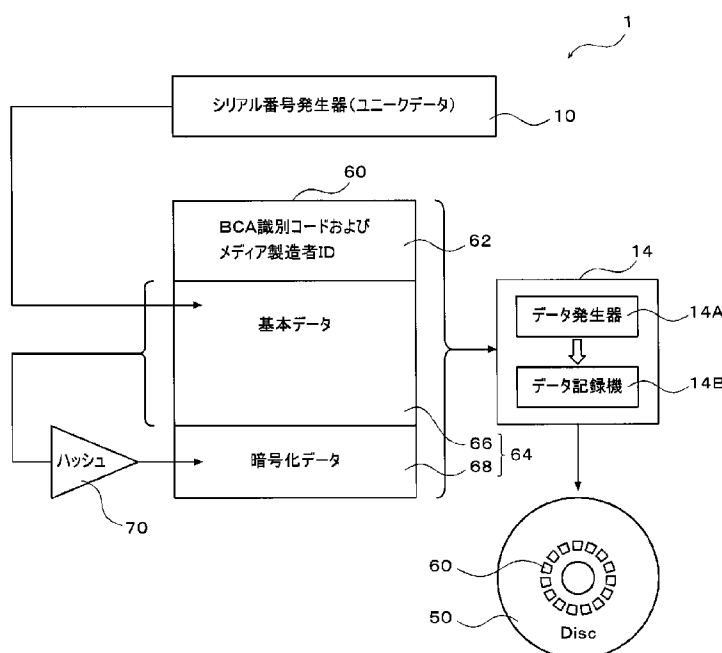
(10) 国際公開番号
WO 2007/148433 A1

- (51) 国際特許分類:
G11B 7/007 (2006.01) G11B 20/12 (2006.01)
G11B 20/10 (2006.01)
- (21) 国際出願番号: PCT/JP2007/000643
- (22) 国際出願日: 2007 年 6 月 18 日 (18.06.2007)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2006-168479 2006 年 6 月 19 日 (19.06.2006) JP
- (71) 出願人 (米国を除く全ての指定国について): TDK 株式会社 (TDK CORPORATION) [JP/JP]; 〒1038272 東京都中央区日本橋一丁目 1 3 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 青井利樹 (AOI, Toshiki) [JP/JP]; 〒1038272 東京都中央区日本橋一丁目 1 3 番 1 号 TDK 株式会社内 Tokyo (JP). 中山陽一
- (74) 代理人: 佐原雅史, 外 (SAHARA, Masashi et al.); 〒3380013 埼玉県さいたま市中央区鈴谷 2 丁目 7 9 4 番 彩都総合特許事務所 Saitama (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): 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, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, 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, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,

[続葉有]

(54) Title: RECORDING MEDIUM FIXED-DATA AREA FORMING METHOD

(54) 発明の名称: 記録媒体の固定データ領域形成方法



- 10 SERIAL NUMBER GENERATOR (UNIQUE DATA)
62 BCA IDENTIFICATION CODE AND MEDIUM MANUFACTURER ID
66 BASIC DATA
68 ENCRYPTED DATA
70 HASH
14A DATA GENERATOR
14B DATA RECORDER

(57) Abstract: A method for forming a fixed-data area in a writable recording medium having a read-only fixed-data area. Basic data including identification information varying among individual recording media is created, and encrypted data is created according to the basic data. The basic data and the encrypted data are nonrewritably stored in the fixed-data area. With this, the recording medium itself can be authenticated by using the fixed-data area of the recording medium, and manufacture of recording media by another arrogating medium manufacturer can be prevented.

(57) 要約: 読み取り専用の固定データ領域を有する書き込み可能な記録媒体における固定データ領域の形成方法であって、記録媒体の個体毎に異なる識別情報を含む基本データを生成すると共に、この基本データに基づいて暗号化データを生成し、固定データ領域に対して、基本データ及び暗号化データを書き換え不能な状態で格納するようにした。これにより、記録媒体の固定データ領域を利用して、記録媒体自体の認証を可能にし、他のメディア製造者になりすました記録媒体の製造を抑制することが可能になる。



SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

記録媒体の固定データ領域形成方法

技術分野

[0001] 本発明は、書込み可能な記録媒体の固定データ領域を形成すると共に、この固定データ領域を利用して記録媒体の認証を行う技術に関する。

背景技術

[0002] 従来、書き込み可能な記録媒体において、コピー回数の制限等を付与しながらコンテンツを記録可能なものが提供されている。この記録媒体によれば、著作権が保護されるべき映像等の記録が実現できる。なお、映像等のコンテンツが著作権保有者の許可なく無制限にコピーされることを防止するために、この種の記録媒体の構造や記録媒体に対する記録手法等、様々な著作権保護技術が提案されている。

[0003] 例えば、書き込み可能な記録媒体において、書き替え不能（読み出し専用）となる固定データ領域が形成されており、この固定データ領域に、記録媒体毎に異なるシリアル番号等のユニークコードが記録されるものがある。著作権保護対象のコンテンツをこの記録媒体にコピーする際には、記録機が、著作権保護技術の管理組織から提供された認証済みの鍵（キー）コードを利用して、記録媒体の上記ユニークコードを暗号化し、この暗号化データを記録可能領域にコンテンツと共に記録しておくようにする。

[0004] 再生時には、固定データ領域のユニークコードと、記録可能領域の暗号化データを読み出して、この暗号化データを復号処理して元に戻す。復号化データとユニークコード一致した場合には、暗号化データと共に記録されたコンテンツが正規コピーであると判断し、再生を行うようにする。

[0005] 一方、記録媒体の記録可能領域に正規に記録された暗号化データ及びコンテンツを、ユニークコードの異なる他の記録媒体にそのままデットコピーした場合、暗号化データを解読して得られた復号化データと、記録媒体のユニークコードが不一致となる。従って、このようなコピーは無許可コピーと判

断し、コンテンツの再生が中止される。このように、コンテンツと共に記録される暗号化データと、記録媒体のユニークコードを1対1で結び付けることで、認証を受けた正規の記録機によるコピーに限って再生を許可することで、未許可コピーを防止する。

- [0006] ところで、記録媒体の固定データ領域には、ユニークコード以外にも、記録媒体のメディア製造者IDや、認証が取り消された記録機のシリアル番号リスト等が記録される場合があり、この固定データ領域の容量不足が懸念されている。特表2003-536193号公報には、固定データ領域の容量不足を補うために、記録可能領域の一部をシステム側領域として利用し、本来、固定データ領域に記録されるべき情報の一部をこのシステム側領域に記録する技術が開示されている。この際、システム側領域に記録された情報が改竄されてしまうことを防止するために、システム側領域に記録された情報に基づいてハッシュ値等を生成し、このハッシュ値を固定データ領域側に記録しておく。この結果、システム側領域の情報を利用する際には、固定データ領域側に記録されたハッシュ値を利用して、改ざんの有無を検証可能とし、改ざんされていない場合に限って記録媒体の利用を許可するようにする。

発明の開示

発明が解決しようとする課題

- [0007] しかしながら、これらの技術は、ユーザがコピーする映像等のコンテンツの無許可コピーを防止するものであり、書き込み可能な記録媒体そのものの模造品を防止することができないという問題があった。
- [0008] 例えば、記録媒体の製造者を判別するものとして、固定データ領域に記録されるメディア製造者IDがある。このメディア製造者IDは、正規の製造者に対して各規格団体等から割り当てられたIDコードであり、例えばDVD-Rの場合には、原盤製造時にスタンパの中にウォブル信号形態で書き込まれる。従って、当該製造者が生産する全てのDVD-Rディスクには、統一されたメディア製造者IDが記録されている。記録機側では、このメディア製造者IDを読み出して、その製造者のDVD-Rの記録特性に合わせた

記録再生条件を選定して、記録・再生を実行する。なお、これらのメディア製造者 I D は、アルファベットや数字等の A S C I I コードを用いて製造者名称を表現したものや、単にバイナリ番号を用いたものがあり、通常数バイト程度が割り当てられる。

[0009] しかし、このメディア製造者 I D は、固定データ領域内に格納する位置が規格で定められているため、記録媒体の製造者が、他社の記録媒体からメディア製造者 I D を不正に入手することが極めて容易であった。従って、記録媒体の製造者が、他の製造者のメディア製造者 I D を無断で利用して記録媒体を大量生産するという問題があった。具体的には、他社のメディア製造者 I D と、自身で生成したユニークデータを組み合わせて固定データ領域の所定位置に記録しておく事で、他社のメディア製造者になりすましたブランク記録媒体が量産されてしまうという問題があった。

[0010] このような模造品の製造行為は、商慣行上は許されるべきではないが、この行為を防止できないのは、メディア製造者 I D 自体が著作物として著作権上の保護対象となっておらず、法的な保護がなされないことが一つの要因であると考えられる。

[0011] 模造品の製造を防ぐ手段として、記録媒体の外表面に製造者を示す模様やロゴ等を施すようにし、外観によって記録媒体の製造者をユーザに識別させて、なりすましを防止することが考えられる。この場合は、模様における著作権や、ロゴの商標権によって法的な保護が受けられる可能性もある。

[0012] しかし、ユーザが独自にプリントを可能とする白紙表面の記録媒体の場合は、そのような対応がとれない。また、記録機側では、記録媒体の外表面の図柄を識別する事は行われておらず、メディア製造者 I D を読み出す事でメディア製造者を判別している。つまり、記録機に対するメディア製造者の不正なりすましは、現状では回避することが困難であるという問題があった。

[0013] また、コンテンツの無許可コピーがなされた記録媒体が市場に流通した場合、記録媒体のメディア製造者 I D を利用して、その流通経路を特定する必要が出てくる。しかし、上述のような不正なりすましの記録媒体が流通して

いる状況では、メディア製造者IDから真の製造者を一義的に特定することができない。同様に、当初から無許可コピーに利用させる目的の記録媒体を製造する場合、特に他社のメディア製造者IDを積極的に利用して、製造者自らの存在を隠滅するような行為が発生してしまうという問題があった。

[0014] 本発明は、上記問題に鑑みてなされたものであり、製造者の不正なりすましを防止し、記録媒体の適正な利用を促す手法を提供しようとするものである。

課題を解決するための手段

[0015] 本発明者らは、鋭意研究の結果、記録媒体の固定データ領域自体で認証を可能にすることで、簡便な構成によって記録媒体の模造品を低減できることを見出した。即ち、上記目的は以下の手段によって達成される。

[0016] 上記目的を達成する本発明は、読み取り専用の固定データ領域を有する書き込み可能な記録媒体における前記固定データ領域の形成方法であって、前記記録媒体の個体毎に異なる識別情報を含む基本データを生成すると共に、前記基本データに基づいて暗号化データを生成し、前記固定データ領域に対して、前記基本データ及び前記暗号化データを書き換え不能な状態で格納することを特徴とする記録媒体の固定データ領域形成方法である。

[0017] 上記目的を達成する固定データ領域形成方法は、上記発明において、前記基本データに含まれる前記識別情報として、前記記録媒体毎に異なるシリアル番号が用いられることを特徴とする。

[0018] 上記目的を達成する固定データ領域形成方法は、上記発明において、前記暗号化データが、ハッシュ関数を用いて生成されることを特徴とする。

[0019] 上記目的を達成する固定データ領域形成方法は、上記発明において、前記暗号化データが、公開キーアルゴリズムを用いて生成されることを特徴とする。

[0020] 上記目的を達成する固定データ領域形成方法は、上記発明において、前記暗号化データが、エラー訂正コードを用いて生成されることを特徴とする。

[0021] 上記目的を達成する固定データ領域形成方法は、上記発明において、前記

記録媒体の製造者を特定するメディア製造者IDが、前記固定データ領域に格納されることを特徴とする。

[0022] 上記目的を達成する固定データ領域形成方法は、上記発明において、前記基本データ及び前記暗号化データが、前記固定データ領域に設定されたユニークデータエリアに連続的に格納されていることを特徴とする。

[0023] 上記目的を達成する本発明は、上記発明に記載の固定データ領域形成方法によって、読み取り専用の前記固定データ領域が形成されていることを特徴とする書き込み可能な記録媒体である。

[0024] 上記目的を達成する本発明は、読み取り専用の固定データ領域を有する書き込み可能な記録媒体であって、前記固定データ領域には、該固定データ領域に保持させるべき基本データ、及び前記基本データに基づいて生成された暗号化データが格納されていることを特徴とする書き込み可能な記録媒体である。

[0025] 上記目的を達成する記録媒体は、上記発明において、CD規格、DVD規格、HD-DVD規格、Blu-ray Disc規格のいずれかであることを特徴とする。

[0026] 上記目的を達成する本発明は、読み取り専用の固定データ領域を有する書き込み可能な記録媒体における前記固定データ領域の形成装置であって、前記記録媒体の個体毎に異なる識別情報を含む基本データを生成する基本データ生成手段と、前記基本データに基づいて暗号化データを生成する暗号化データ生成手段と、前記固定データ領域に対して、前記基本データ及び前記暗号化データを書き換え不能な状態で記録する記録手段と、を備えることを特徴とする記録媒体の固定データ領域形成装置である。

[0027] 上記目的を達成する本発明は、書き込み可能な記録媒体の認証方法であって、前記記録媒体における読み取り専用の固定データ領域を読み出すことで、前記記録媒体の個体を識別可能な基本データ及び前記基本データを暗号化した暗号化データを抽出し、予め設定された暗号化手法によって、前記基本データを暗号化して検証用暗号化データを生成し、前記検証用暗号化データ

と、前記固定データ領域に格納されている前記暗号化データが一致するか否かを判定し、一致する場合には前記記録媒体の使用を許可すると共に、不一致の場合は前記記録媒体の使用を拒否することを特徴とする記録媒体の認証方法である。

[0028] 上記目的を達成する本発明は、書き込み可能な記録媒体の認証方法であって、前記記録媒体における読み取り専用の固定データ領域を読み出すことで、前記記録媒体の個体を識別可能な基本データ及び前記基本データを暗号化した暗号化データを抽出し、予め設定された復号化手法によって、前記暗号化データを復号化して検証用基本データを生成し、前記検証用基本データと、前記固定データ領域に格納されている前記基本データが一致するか否かを判定し、一致する場合には前記記録媒体の使用を許可すると共に、不一致の場合は前記記録媒体の使用を拒否することを特徴とする記録媒体の認証方法である。

[0029] 上記目的を達成する記録媒体の認証方法は、上記発明において、認証で利用した前記暗号化データを所定のメモリ手段に蓄積すると共に、新たに認証する前記記録媒体の前記暗号化データと、過去に認証で利用した前記暗号化データとを比較して、同一の暗号化データが過去に存在したか否かを判定することを特徴とする。

[0030] 上記目的を達成する記録媒体の認証方法は、上記発明において、新たに認証する前記記録媒体の前記暗号化データと同一の暗号化データが、前記メモリ手段に所定の基準数以上存在する場合に、前記記録媒体の使用を拒否することを特徴とする。

[0031] 上記目的を達成する本発明は、書き込み可能な記録媒体の認証装置であって、前記記録媒体における読み取り専用の固定データ領域を読み出すことで、前記記録媒体の個体を識別可能な基本データ及び前記基本データを暗号化した暗号化データを抽出する固定データ領域読み出し手段と、予め設定された暗号化手法によって、前記基本データを暗号化する再暗号化手段と、前記再暗号化手段によって生成された検証用暗号化データと、前記固定データ領

域に格納されている前記暗号化データが一致するか否かを判定する検証手段と、を備えることを特徴とする記録媒体の認証装置である。

発明の効果

- [0032] 本発明によれば、固定データ領域によって記録媒体の認証が可能となり、固定データ領域をコピーした模造品の記録媒体の製造を抑制できるという優れた効果を奏し得る。

図面の簡単な説明

- [0033] [図1] 本発明の第1実施形態にかかる固定データ領域形成装置の構成を示すブロック図
[図2] 同形成装置を用いた固定データ領域の形成プロセスを示すブロック図
[図3] 本発明の第1実施形態にかかる記録再生機の構成を示すブロック図
[図4] 同記録再生機を用いた記録媒体の認証プロセスを示すブロック図
[図5] 本発明の第2実施形態にかかる固定データ領域形成装置の構成を示すブロック図
[図6] 同形成装置を用いた固定データ領域の形成プロセスを示すブロック図
[図7] 本発明の第2実施形態にかかる記録再生機の構成を示すブロック図
[図8] 同記録再生機を用いた記録媒体の認証プロセスを示すブロック図
[図9] 本発明の第3実施形態にかかる記録再生機の構成を示すブロック図
[図10] 同記録再生機を用いた記録媒体の認証プロセスを示すブロック図

発明を実施するための最良の形態

- [0034] 以下、本発明の実施の形態を図面を参照して説明する。
- [0035] 図1には、本発明の第1実施形態にかかる記録媒体50の固定データ領域形成装置（以下、形成装置）1の概略構成が示されている。この形成装置1は、基本データ生成手段10と、暗号化データ生成手段12と、不可逆記録手段14と、を備える。基本データ生成手段10は、記録媒体50の個体毎に異なる識別情報を含む基本データを生成するものであり、ここでは識別情報として記録媒体50毎に異なるシリアル番号を発生する。このシリアル番号によって個体識別が可能となる。

- [0036] 暗号化データ生成手段 12 は、基本データとなるシリアル番号に基づいて、暗号化データを生成する。ここでは、ハッシュ関数を利用してシリアル番号から得たハッシュ値を暗号化データとして利用する。
- [0037] 不可逆記録手段 14 はいわゆる B C A レジスターであり、記録媒体 50 の固定データ領域に対して、基本データ（シリアル番号）及び暗号化データ（ハッシュ値）を書き換え不能な状態で記録する。ここでは、記録媒体 50 の製造工程において、記録媒体 50 の最内周付近に対して高パワーレーザーを照射し、記録層を焼き切るようにして情報を記録する。なお、記録態様としては、バーコード様式を利用した低密度データを採用する。このようにして記録された固定データ領域は B C A（B u r s t C u t t i n g A r e a）と呼ばれ、記録媒体 50 の記録・再生前に自動的に読み出される。この B C A の容量には制限があり 300 バイト以内に設定される場合が多い。
- [0038] 図 2 には、この形成装置 1 による固定データ領域 60 の形成プロセスが示されている。固定データ領域 60 は既に述べた B C A であり、通常、基礎情報エリア 62 とユニークデータエリア 64 から構成されている。基礎情報エリア 62 には、固定データ領域 60 が B C A であることを意味する B C A 識別情報や、記録媒体 50 の製造者を意味するメディア製造者 I D 等が記録される。つまり、この基礎情報エリア 62 は、大量生産する複数の記録媒体 50 間で共通の情報となる。一方、ユニークデータエリア 64 には、著作権保護技術に利用されることを目的に、記録媒体 50 毎に異なる情報を記録しなければならない。識別可能数は無限ではないが、ユニークデータエリア 64 に仮に 35 ビットの容量を割り当てれば、340 億以上のシリアル番号を割り当てることができるので、実用上十分である。
- [0039] この形成プロセスでは、ユニークデータエリア 64 を、形式的に 2 つの領域に分けており、一方を基本エリア 66 とし、他方を暗号化エリア 68 としている。基本エリア 66 には、基本データ生成手段 10 によって生成された基本データが記録される。又暗号化エリア 68 には、暗号化データ生成手段 12 のハッシュ関数 70 を用いて生成された暗号化データが記録される。な

お、基本データが異なると、この基本データに基づいて生成される暗号化データも必ず異なるので、ユニークデータエリア 64 の全体がユニーク情報となることに変わりはない。

[0040] 基礎情報エリア 62 に記録される B C A 識別情報やメディア製造者 I D、ユニークデータエリア 64 に記録される基本データや暗号化データは、一旦、不可逆記録手段 14 のデータ発生器 14 A で合成されて 1 つの B C A 固定情報となる。その後、記録機 14 B によって、B C A 固定情報をまとめて記録することで固定データ領域 60 が形成される。

[0041] なお、上記ハッシュ関数の種別やユニークデータエリア 64 の内部構成（暗号化エリア 69 のデータ位置とビット数）等は、後述する記録再生機の暗号化手段の設計者以外には秘密にされる必要がある。

[0042] 図 3 には、この記録媒体 1 の認証を行った後に記録媒体 1 の記録再生を実行する記録再生機 80 が示されている。つまり、この記録再生機 80 は記録媒体 1 の認証装置を兼ねている。

[0043] 記録再生機 80 は、固定データ領域読み出し手段 82、再暗号化手段 84、検証手段 86、記録再生手段 90 を備える。固定データ領域読み出し手段 82 は、記録媒体 50 の固定データ領域 60 を読み出して、各エリアに記録された情報を個別に抽出可能となっている。従って、固定データ領域読み出し手段 82 には、固定データ領域 60 のデータ配置構成に関する情報（各エリアの開始位置とビット数）が予め設定されており、ユニークデータエリア 64 における基本エリア 66 と暗号化エリア 68 についても個別に読み出すことが可能となっている。

[0044] 再暗号化手段 84 は、形成装置 1 の暗号化データ生成手段 12 で利用したハッシュ関数と同じ関数を備えており、基本エリア 66 の基本データ（シリアル番号）からハッシュ値を算出する。このハッシュ値は検証用の暗号化データとして利用する。検証手段 86 は、暗号化エリア 68 の暗号化データと、再暗号化手段 84 で暗号化された検証用の暗号化データを比較し、両者が一致する場合は適正に認証されたと判断して、記録再生手段 90 による記録

・再生の許可を与え、両者が不一致の場合は認証不可と判断して、記録又は再生を禁止する。

[0045] 図4には、この記録再生機80の認証プロセスがブロックで示されている。まず、記録再生機80では、記録媒体50の固定データ領域60を読み出す。更に記録再生機80では、固定データ領域60における基礎情報エリア62、ユニークデータエリア64の基本エリア66、暗号化エリア68を識別して、各エリアに格納されている情報を個別に抽出する。その後、基本エリア66に記録されているシリアル番号に基づいて、ハッシュ関数92を利用してハッシュ値を生成し、検証用の暗号化データとする。検証手段86では、この検証用の暗号化データ（ハッシュ値）と暗号化エリア68に記録されている暗号化データとを比較し、一致する場合は正規に認証する。認証後は、基礎情報エリア62に記録されたメディア製造者ID等の情報を利用して、所定の記録ストラテジや記録パワー、再生パワー等を選定し、ユーザーデータの記録又は再生を実行する。一方、認証ができなかった場合は記録又は再生が中止される。

[0046] 本第1実施形態の形成装置1や記録再生装置80等によれば、固定データ領域60の暗号化データを利用した認証がなされない限り、この記録媒体の利用を中止することが可能になる。従って、他のメディア製造者IDを利用して記録媒体50を製造するような、なりすまし行為が防止される。

[0047] 例えば、正規に製造された他社の記録媒体50を入手し、この記録媒体50からメディア製造者IDを解読し、自社のシリアル番号を単純に組み合わせて固定データ領域を形成した場合、この記録媒体50には暗号化データが含まれていないので、本実施形態の記録再生装置80では認証されない。

[0048] 従って、他のメディア製造者IDを利用しながらも、この記録再生装置80の認証を得るには、メディア製造者IDに対応する正規メディア製造者が製造時に用いた暗号化手段（ここでは特定のハッシュ関数）、このメディア製造者が設定したユニークデータエリア64内の暗号化エリア68の先頭位置及びデータ容量等入手し、これらの条件に基づいて形成装置1で記録媒

体50を製造しなければならない。しかし、これらの情報は、管理組織において秘密に管理されているので、入手することができないことから、この種のなりすまし行為が防止される。

[0049] また、上記手法以外に、他社のメディア製造者IDを利用したなりすまし行為を実現するには、正規の記録媒体50の固定データ領域60全体をそのままコピーする必要がある。このコピー手法によって、この記録媒体50を大量生産する場合、ユニークデータエリア64が全て同一となる記録媒体50を大量に製造するか、又は、他社の正規の記録媒体50を大量に入手して、1対1の関係で新たな記録媒体50に固定データ領域60をそれぞれコピーしていく必要がある。前者の場合、ユニークデータエリア64がユニークとならない記録媒体を製造することになるので、規則違反で警告処分の対象となる。また、後者の場合は、正規の記録媒体50の入手コストや、固定データ領域のコピーの手間を考えると現実的でない。従って、本実施形態によれば、他のメディア製造者IDを不正利用した記録媒体50の模倣品の量産が抑制され、記録媒体50が認証される限り、正しい製造者から提供された正規の記録媒体であると判断できる。

[0050] 次に、図5等を参照して、本発明の第2実施形態にかかる固定データ領域形成装置101について説明する。なお、この形成装置101において、第1実施形態の形成装置1と同一又は類似する部分については、図中の符号の下二桁を一致させることで、ここでの説明を省略するものとし、第1実施形態と異なる部分を中心に説明する。

[0051] この形成装置101では、暗号化データ生成手段112の内部構成として、ハッシュ値生成部112Aと、公開キーアルゴリズム生成部112Bを備えている。ハッシュ値生成部112Aは、基本データからハッシュ関数を用いてハッシュ値を算出する。また、公開キーアルゴリズム生成部112Bは、公開キーアルゴリズムを利用して、ハッシュ値生成部112Aで生成されたハッシュ値を、秘密キーを利用して暗号化（電子署名）する。このようにして生成された暗号化データは、他のデータと共に固定データ領域160に

記録される。

[0052] 図6には、この形成装置101による固定データ領域160の形成プロセスがブロックで示されている。固定データ領域160は既に述べたBCAであり、基礎情報エリア162と、ユニークデータエリア164から構成されている。基本データに基づいて、ハッシュ関数170及び秘密キー K_s による暗号化処理172を経て生成された暗号化データは、ユニークデータエリア164における暗号化エリア168に記録される。基礎情報エリア162に記録されるBCA識別情報およびメディア製造者ID、ユニークデータエリア164に対応する基本データ及び暗号化データは、不可逆記録手段114のデータ発生器114Aで合成されて1つのBCA固定情報となり、記録機114Bによって記録媒体150に記録されて、固定データ領域160が形成される。

[0053] なお、この形成装置101で利用されるハッシュ関数170は、メディア製造者毎に秘密裏に設定される必要は無く、複数のメディア製造者の間で共有するようにしてもよく、広く公開しても良い。一方、公開キーアルゴリズムにおける秘密キー K_s は、メディア製造者が独自に保有するものであり、完全に非公開の情報とする。

[0054] 図7には、この記録媒体101を認証し、記録再生を実行する記録再生機180が示されている。この記録再生機180は、固定データ領域読み出し手段182と、ハッシュ値生成手段183と、復号化手段185と、検証手段186と、記録再生手段190を備える。固定データ領域読み出し手段182は、記録媒体150の固定データ領域160を読み出して、各エリアから情報を抽出する。

[0055] ハッシュ値生成手段183は、形成装置101におけるハッシュ値生成部112Aと同じハッシュ関数を有しており、基本エリア166に記録されているシリアル番号からハッシュ値を算出する。一方、復号化手段185は、複数のメディア製造者から提供された複数の公開キー K_p を保有しており、固定データ領域160から読み出されたメディア製造者IDに基づいて、そ

のメディア製造者が配布した公開キー K_p を選択し、この公開キー K_p を利用して、暗号化エリア168に記録された暗号化データを復号化する。検証手段186は、復号化手段185によって復号化された検証用のハッシュ値と、ハッシュ値生成手段184によって新たに生成されたハッシュ値を比較し、両者が一致する場合は適正に認証されたと判断して、記録媒体150の利用を許可し、両者が不一致の場合は認証不可と判断して、記録媒体150の利用を禁止する。

[0056] 図8には、この記録再生機180による認証及び記録再生プロセスがブロックで示されている。まず、記録再生機180では、記録媒体150の固定データ領域160が読み出される。具体的に記録再生機180は、固定データ領域160における基礎情報エリア162と、ユニークデータエリア164を識別し、更にユニークデータエリア164における基本エリア166と暗号化エリア168を識別して、個々のデータを抽出する。次いで、基本エリア166の基本データ（シリアル番号）に基づいて、ハッシュ関数192によってハッシュ値が生成される。一方、復号化手段185では、基礎情報エリア162に格納されているメディア製造者IDを利用して、この製造者から配布された公開キー K_p を選定し、この公開キー K_p によって、暗号化エリア168の暗号化データを復号化する。検証手段186では、この復号化データと、ハッシュ値生成手段183で生成されたハッシュ値を比較し、両者が一致する場合は、認証が正しくなされたと判断して、記録媒体150の利用を許可する。一方、両者が不一致の場合は、認証が正しくなされなかったと判断して、記録媒体150の利用を禁止する。

[0057] 本第2実施形態によれば、公開キーアルゴリズムを利用することで、復号化手段185が複数の公開キーを保持するようになっているので、複数の正規メディア製造者が製造した記録媒体150を、それぞれ認証することが可能になる。例えば、第1実施形態で示したように、ハッシュ関数自体をメディア製造者IDに対応させて秘密状態で記録再生装置に組み込む場合、仮に複数のメディア製造者の認証を可能にするには、各メディア製造者が採用し

た異なるハッシュ関数を記録再生装置に組み込む必要がある。しかし、民生用の記録再生機 180 に複数のハッシュ関数のアルゴリズムを搭載するのは負担であり、また、新たな正規メディア製造者の認証を可能にするために、ハッシュ関数を更新することは大変手間がかかる。従って、公開キーアルゴリズムを採用すれば、記録再生機 180 において複数の公開キーを格納することも容易であり、通信手段や記録媒体 150 を利用して、新しい公開キーリストを更新していくことも容易である。更に、本第 2 実施形態では、メディア製造者が秘密キー K_s を秘密に保管しておくことが可能であり、記録再生機 180 の設計者等との間で秘密キー K_s を共有する必要が無いため、安全性が高い。

[0058] 次に、図 9 等を参照して、本発明の第 3 実施形態に係る記録再生機 280 を説明する。なお、この記録再生機 280 において、第 1 実施形態で示した記録再生機 80 と同一又は類似する部分については、符号の下二桁を一致させることで説明を省略する。

[0059] この記録再生機 280 は、固定データ領域読み出し手段 282、再暗号化手段 284、検証手段 286、記録再生手段 290 に加えて、暗号化データ蓄積手段 288 及び暗号化データ履歴照合手段 289 を備える。図 10 に示されるように、暗号化データ蓄積手段 288 は、この記録再生機 280 で利用された記録媒体 250 の暗号化データ (N 、 $N-1$ 、 $N-2 \cdots N-X$) を所定のメモリに蓄積している。また、暗号化データ履歴照合手段 289 は、新たに認証を行う記録媒体 250 の暗号化データ ($N+1$) と、暗号化データ蓄積手段 288 で蓄積した過去の暗号化データを順次照合していき、一致するものが過去に存在するか判定する。この判定の結果、現在読み込まれた暗号化データと同一の暗号化データが、過去に 100 件以上存在していた場合、固定データ領域を不正コピーした記録媒体 250 が数多く流通している疑義が生じたと判断して、この記録媒体 250 の利用を禁止する。一方、新たに認証する記録媒体 250 の暗号化データと同一の暗号化データが過去に 100 件未満しか存在しない場合には、まだ、適正な状態であると判断して

、既に述べた固定データ領域 260 の認証プロセスに移行する。なお、ここでは 100 件の存在を不の判定の基準値に利用したが、本発明はそれに限定されず、他の基準によって判定するようにしても良い。

[0060] 本第 3 実施形態の記録再生機 280 によれば、固定データ領域をそのままコピーした記録媒体を大量生産するというなりすまし行為を検出することが可能になる。従って、ブランクの記録媒体 250 にデジタルコンテンツを正規にコピーするようなメディア出版会社が、この記録再生機 280 を利用すれば、購入したブランク記録媒体が適正なものであるか否かを自動的に判別し、不正な記録媒体の利用を未然に防止することが可能となる。

[0061] また、この記録再生機 280 では、ハッシュ値等の暗号化データを利用して、過去の読み込み履歴と照合するようにしているため、データ量を大幅に低減することができ、照合スピードを高めることができる。例えば、100 ビット以上の容量のユニークデータも存在することから、ユニークデータエリアをそのまま履歴保存しようとするると 100 万枚の履歴で 10 メガバイトになってしまう。これでは、一致・不一致の検証に長時間を要してしまい作業効率が悪化する。一方、本実施形態のように、暗号化データを有効利用して照合を行う場合、ハッシュ値等を 16 ビット程度に設定することも可能であるため、大量の記録媒体の暗号化データを履歴保存しても、短時間で照合できるようになる。

[0062] 以上、本実施形態では、ユニークデータエリアにおいて暗号化データが基本データの後に配置される場合に限って示したが、本発明はそれに限定されない。例えば、基本データの前や中間に暗号化データを配置するようにしてもよい。また、暗号化データを所定の基準で分割して、基本データの中に所定規則で割り込ませるようにしても良い。このようにすると、メディア製造者が、他社のメディア製造者のユニークデータエリアの内部構造を解析することが一層困難になるため、固定データ領域が不正利用される事態を低減できる。また、本実施形態では、シリアル番号となる基本データを利用して暗号化データを生成する場合を示したが、基本データに加えてメディア製造者

I D等の他の情報を含めたデータに基づいて暗号化データを生成しても良い。つまり、基本データに個体識別可能なユニーク情報が含まれていれば十分であり、他の情報を追加して基本データにすることは自由である。

[0063] また、上記実施形態では、基本データの暗号化に関して、ハッシュ関数又は公開キーアルゴリズムを利用する場合に限って示したが、本発明はそれに限定されない。例えば、エラー検出コード（CRCコード）やエラー訂正コード（ECCコード）を暗号化手法として採用することもできる。

[0064] 更に上記実施形態では、記録媒体の規格については特に限定されないが、例えばCD規格、DVD規格、HD-DVD規格、Blu-ray Disc規格等に利用することが可能である。また、本実施形態では、記録媒体の認証に記録再生機を利用した場合を示したが、本発明はそれに限定されず、記録専用機又は再生専用機に採用することも可能であり、認証装置を単独で利用することもできる。

産業上の利用可能性

[0065] 本発明の固定データ領域形成方法等によれば、メディア製造者I Dを不正に利用するような、なりすまし行為を防止することができ、記録媒体の適正な利用が促進されることになる。

請求の範囲

- [1] 読み取り専用の固定データ領域を有する書き込み可能な記録媒体における前記固定データ領域の形成方法であって、
- 前記記録媒体の個体毎に異なる識別情報を含む基本データを生成すると共に、前記基本データに基づいて暗号化データを生成し、
- 前記固定データ領域に対して、前記基本データ及び前記暗号化データを書き換え不能な状態で格納することを特徴とする記録媒体の固定データ領域形成方法。
- [2] 前記基本データに含まれる前記識別情報として、前記記録媒体毎に異なるシリアル番号が用いられることを特徴とする請求の範囲 1 に記載の記録媒体の固定データ領域形成方法。
- [3] 前記暗号化データが、ハッシュ関数を用いて生成されることを特徴とする請求の範囲 1 又は 2 に記載の記録媒体の固定データ領域形成方法。
- [4] 前記暗号化データが、公開キーアルゴリズムを用いて生成されることを特徴とする請求の範囲 1、2 又は 3 に記載の記録媒体の固定データ領域形成方法。
- [5] 前記暗号化データが、エラー訂正コードを用いて生成されることを特徴とする請求の範囲 1 乃至 4 のいずれかに記載の記録媒体の固定データ領域形成方法。
- [6] 前記記録媒体の製造者を特定するメディア製造者 ID が、前記固定データ領域に格納されることを特徴とする請求の範囲 1 乃至 5 のいずれかに記載の記録媒体の固定データ領域形成方法。
- [7] 前記基本データ及び前記暗号化データが、前記固定データ領域に設定されたユニークデータエリアに連続的に格納されていることを特徴とする請求の範囲 1 乃至 6 のいずれかに記載の記録媒体の固定データ領域形成方法。
- [8] 請求の範囲 1 乃至 7 のいずれかに記載の固定データ領域形成方法によって、読み取り専用の前記固定データ領域が形成されていることを特徴とする書き込み可能な記録媒体。

- [9] 読み取り専用の固定データ領域を有する書き込み可能な記録媒体であって、前記固定データ領域には、該固定データ領域に保持させるべき基本データ、及び前記基本データに基づいて生成された暗号化データが格納されていることを特徴とする書き込み可能な記録媒体。
- [10] 前記記録媒体が、CD規格、DVD規格、HD-DVD規格、Blu-ray Disc規格のいずれかであることを特徴とする請求の範囲8又は9に記載に書き込み可能な記録媒体。
- [11] 読み取り専用の固定データ領域を有する書き込み可能な記録媒体における前記固定データ領域の形成装置であって、
前記記録媒体の個体毎に異なる識別情報を含む基本データを生成する基本データ生成手段と、
前記基本データに基づいて暗号化データを生成する暗号化データ生成手段と、
前記固定データ領域に対して、前記基本データ及び前記暗号化データを書き換え不能な状態で記録する記録手段と、
を備えることを特徴とする記録媒体の固定データ領域形成装置。
- [12] 書き込み可能な記録媒体の認証方法であって、
前記記録媒体における読み取り専用の固定データ領域を読み出すことで、前記記録媒体の個体を識別可能な基本データ及び前記基本データを暗号化した暗号化データを抽出し、
予め設定された暗号化手法によって、前記基本データを暗号化して検証用暗号化データを生成し、
前記検証用暗号化データと、前記固定データ領域に格納されている前記暗号化データが一致するか否かを判定し、一致する場合には前記記録媒体の使用を許可すると共に、不一致の場合は前記記録媒体の使用を拒否することを特徴とする記録媒体の認証方法。
- [13] 書き込み可能な記録媒体の認証方法であって、
前記記録媒体における読み取り専用の固定データ領域を読み出すことで、

前記記録媒体の個体を識別可能な基本データ及び前記基本データを暗号化した暗号化データを抽出し、

予め設定された復号化手法によって、前記暗号化データを復号化して検証用基本データを生成し、

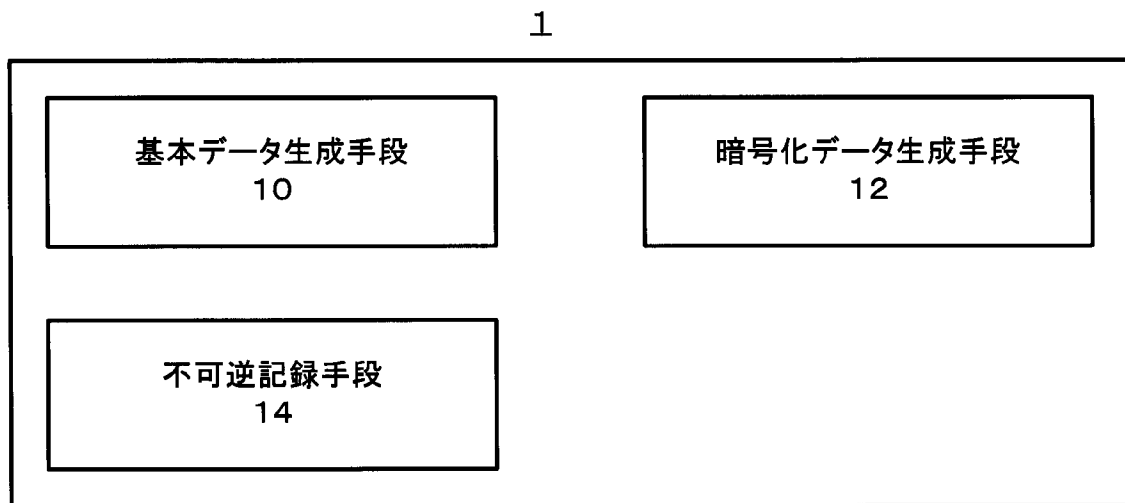
前記検証用基本データと、前記固定データ領域に格納されている前記基本データが一致するか否かを判定し、一致する場合には前記記録媒体の使用を許可すると共に、不一致の場合は前記記録媒体の使用を拒否することを特徴とする記録媒体の認証方法。

- [14] 認証で利用した前記暗号化データを所定のメモリ手段に蓄積すると共に、新たに認証する前記記録媒体の前記暗号化データと、過去に認証で利用した前記暗号化データとを比較して、同一の暗号化データが過去に存在したか否かを判定することを特徴とする請求の範囲 1 2 又は 1 3 記載の記録媒体の認証方法。

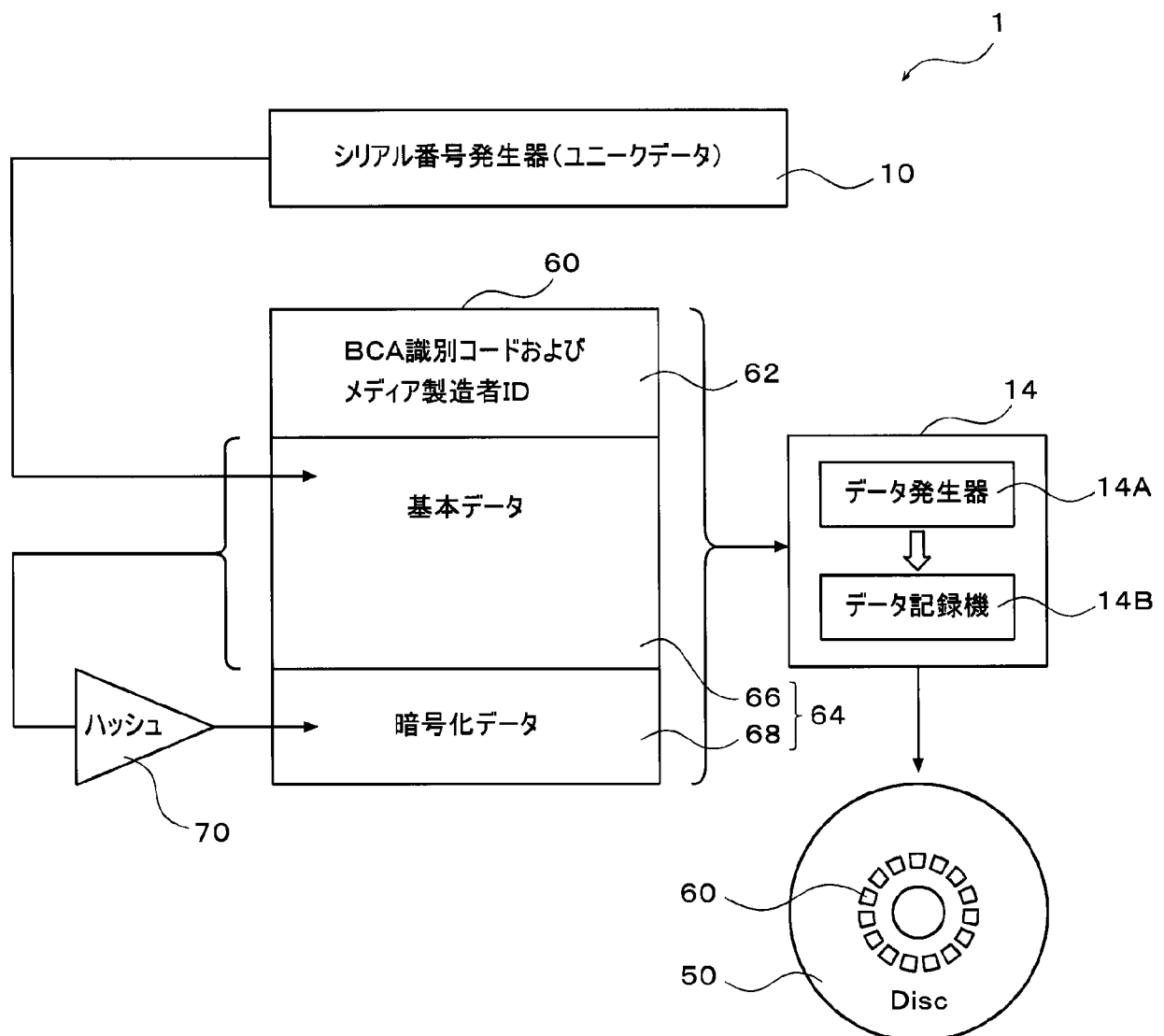
- [15] 新たに認証する前記記録媒体の前記暗号化データと同一の暗号化データが、前記メモリ手段に所定の基準数以上存在する場合に、前記記録媒体の使用を拒否することを特徴とする請求の範囲 1 4 記載の記録媒体の認証方法。

- [16] 書き込み可能な記録媒体の認証装置であって、
前記記録媒体における読み取り専用の固定データ領域を読み出すことで、前記記録媒体の個体を識別可能な基本データ及び前記基本データを暗号化した暗号化データを抽出する固定データ領域読み出し手段と、
予め設定された暗号化手法によって、前記基本データを暗号化する再暗号化手段と、
前記再暗号化手段によって生成された検証用暗号化データと、前記固定データ領域に格納されている前記暗号化データが一致するか否かを判定する検証手段と、
を備えることを特徴とする記録媒体の認証装置。

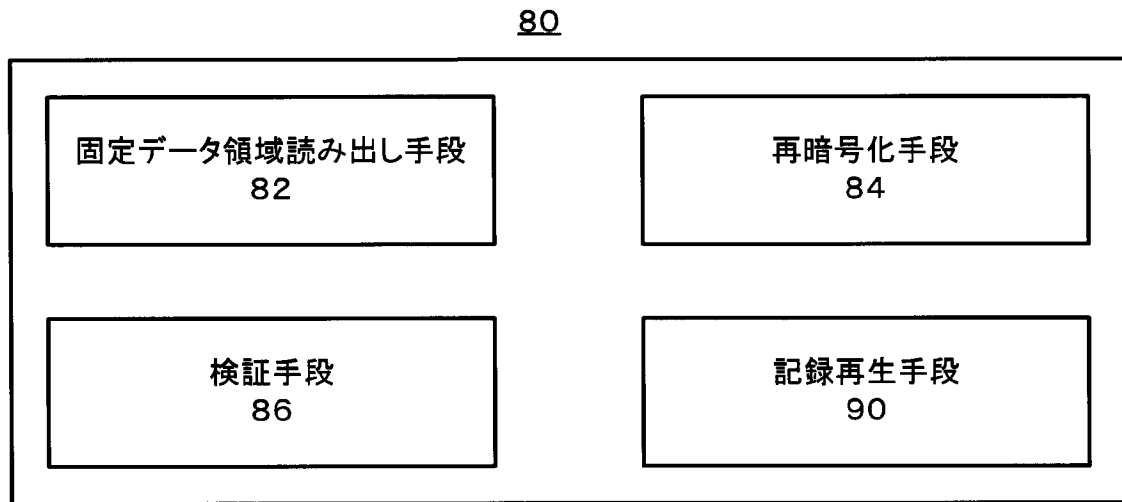
[図1]



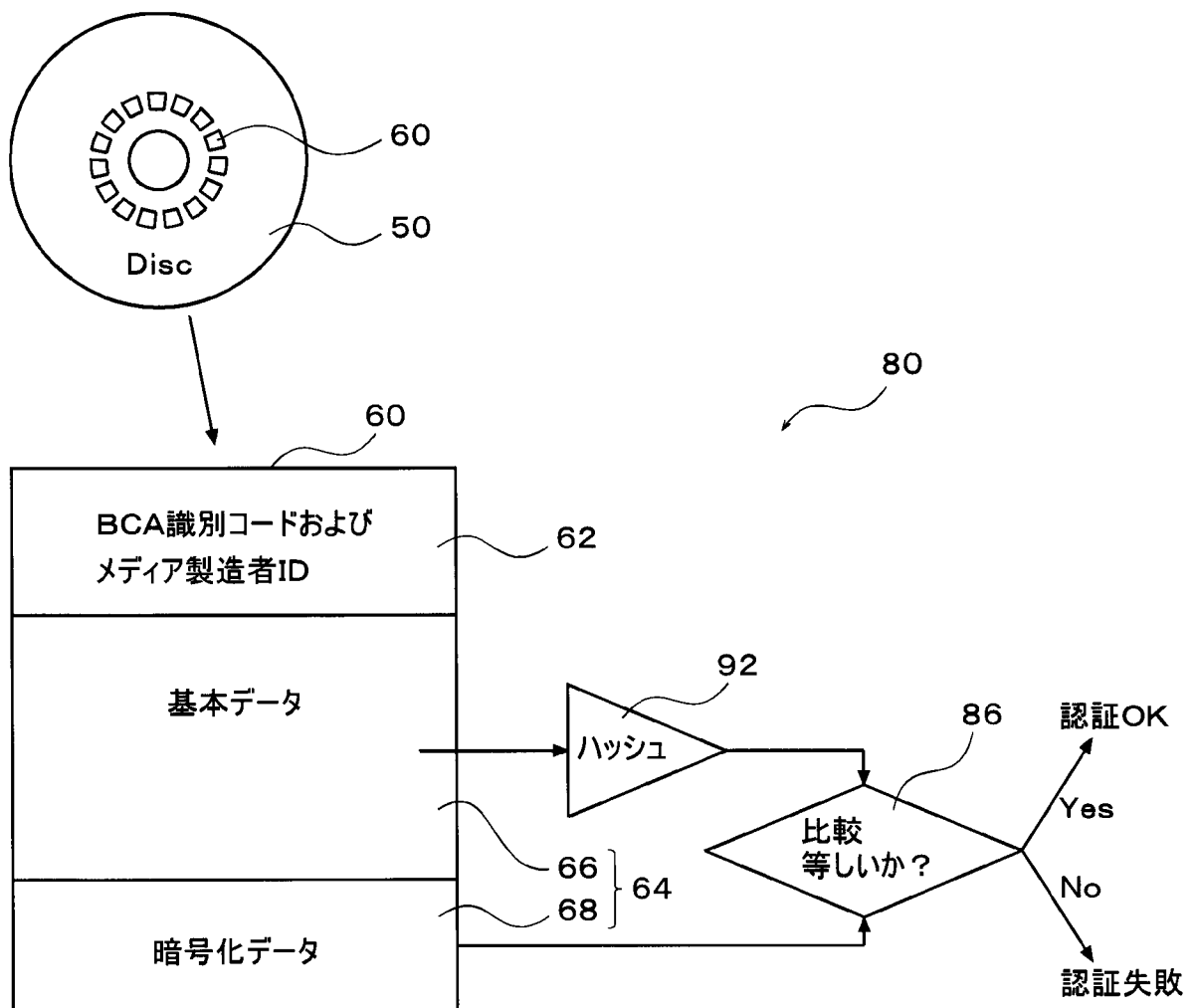
[図2]



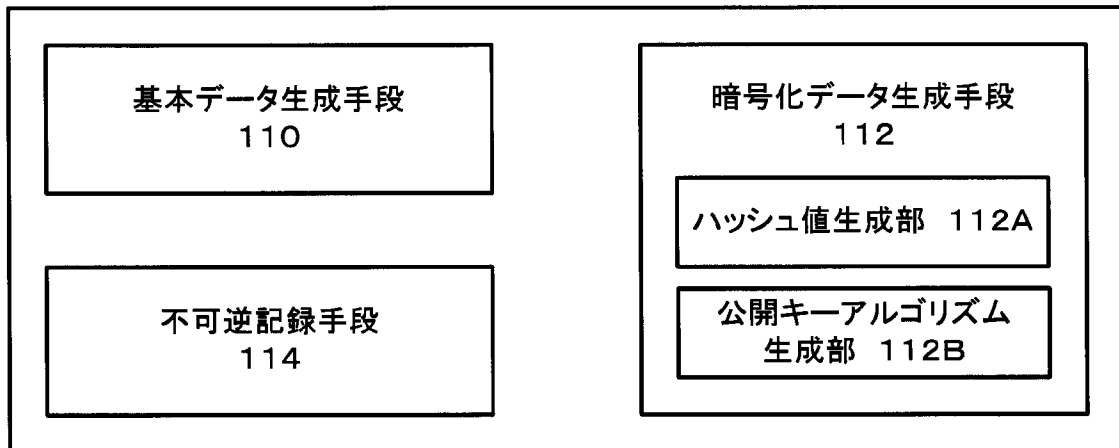
[図3]



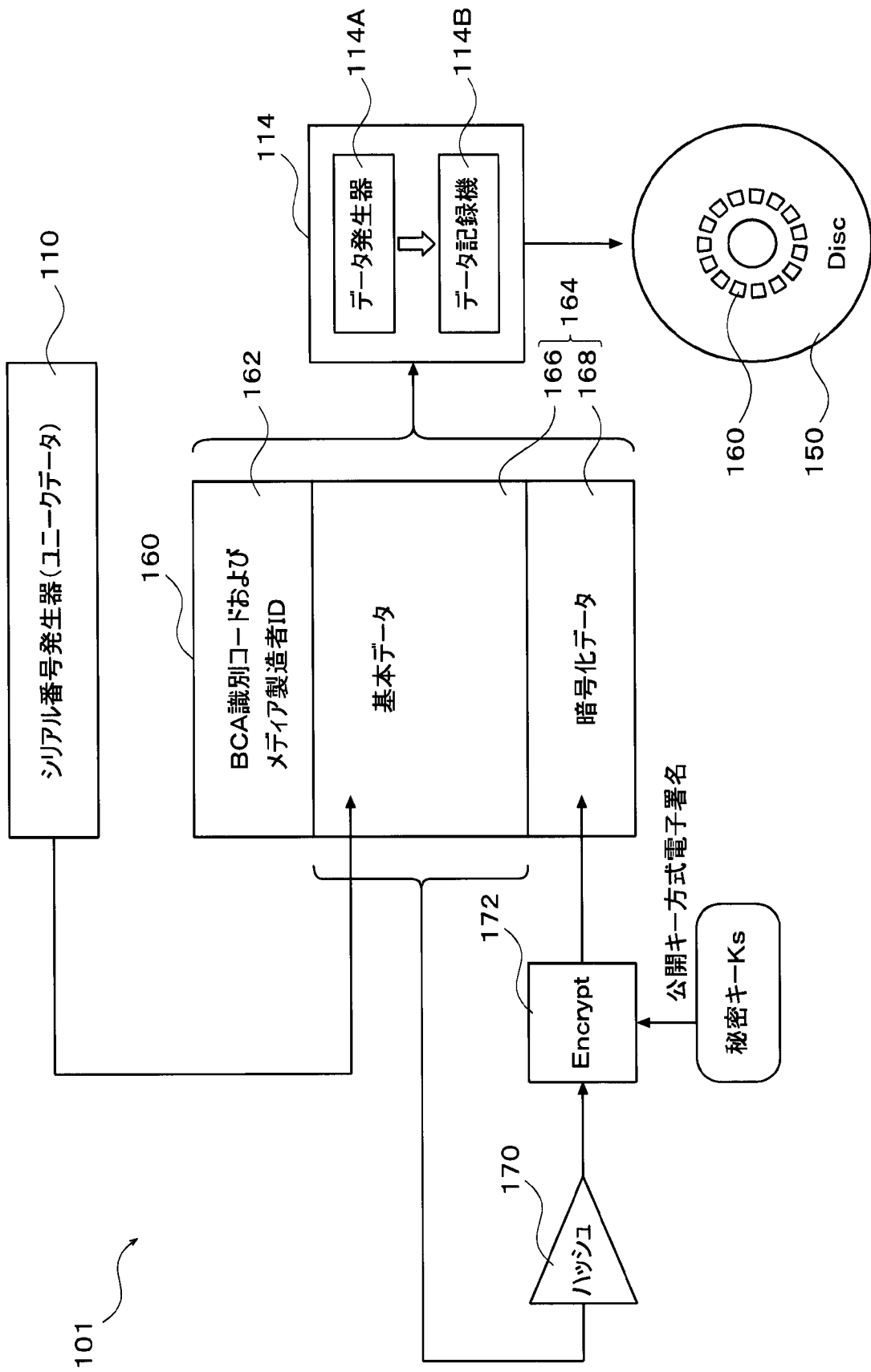
[図4]



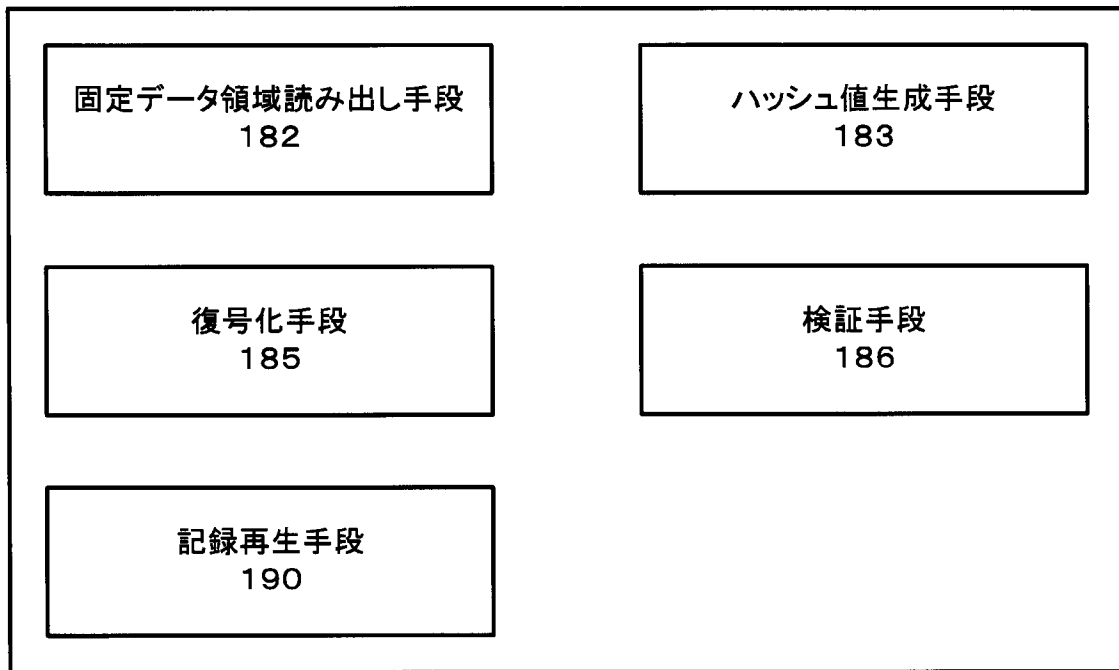
[図5]

101

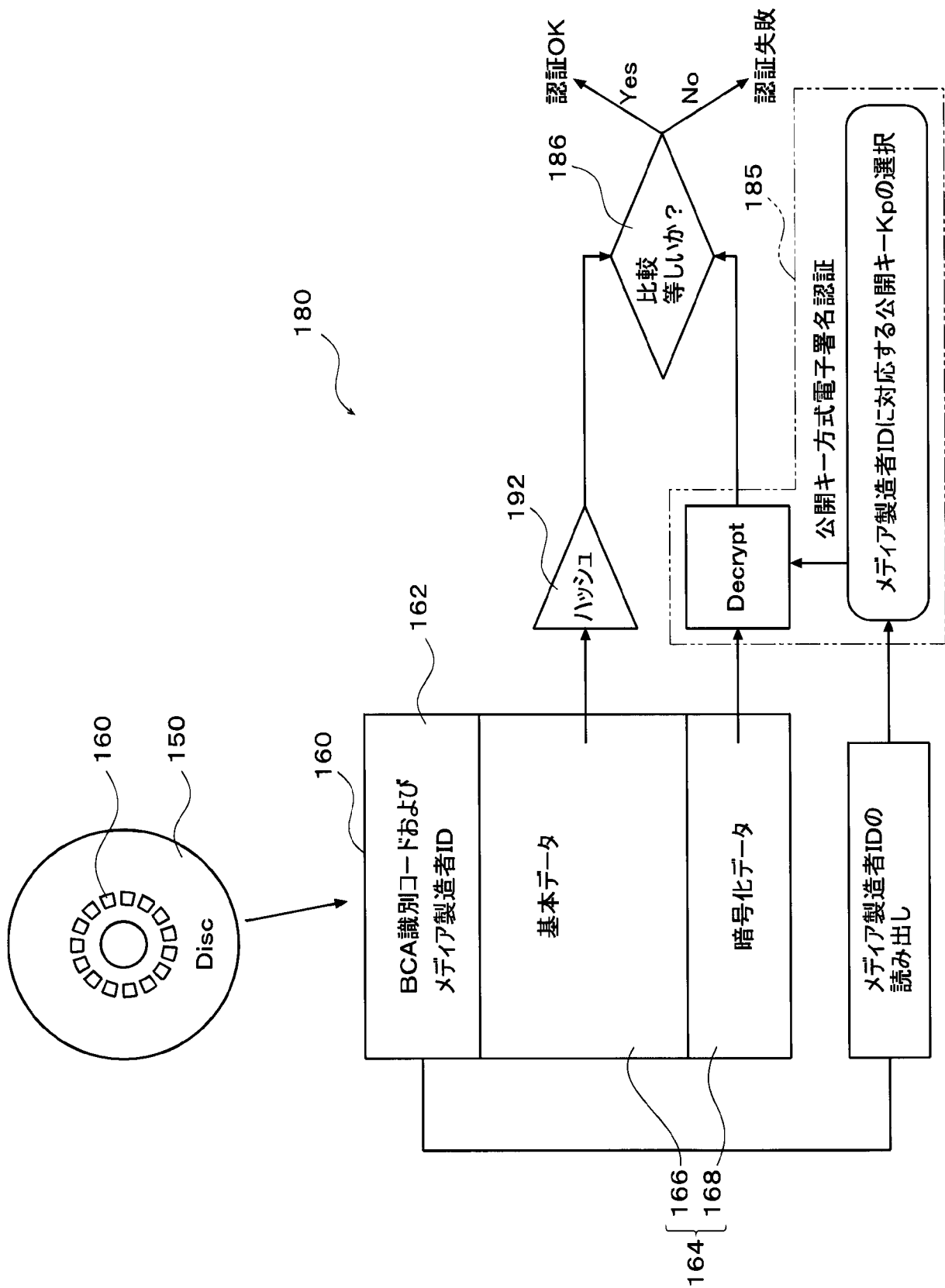
[図6]



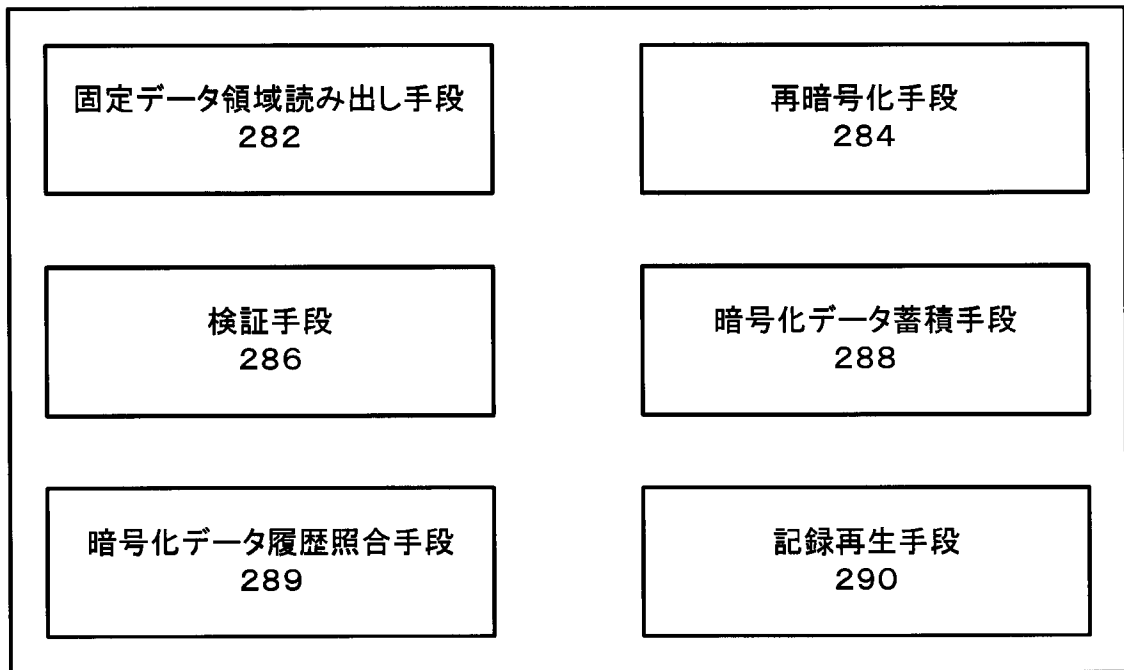
[図7]

180

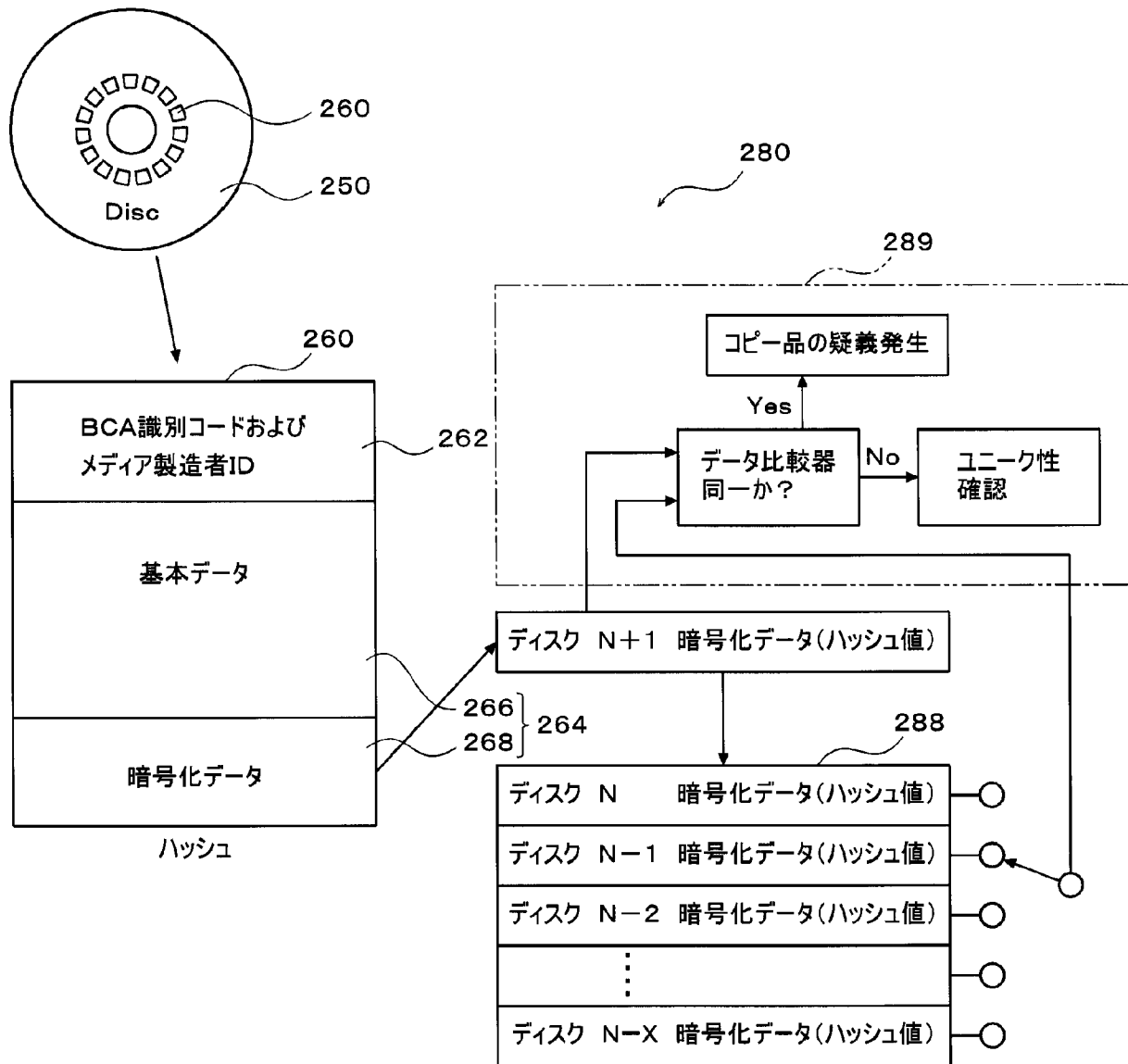
[図8]



[図9]

280

[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/000643

A. CLASSIFICATION OF SUBJECT MATTER

G11B7/007(2006.01)i, G11B20/10(2006.01)i, G11B20/12(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)

G09C1/00-5/00, G11B7/00-7/013, 7/24-7/258, 7/28-7/30, 20/10-20/16, H04K1/00-3/00, H04L9/00-9/38

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2007
Kokai Jitsuyo Shinan Koho	1971-2007	Toroku Jitsuyo Shinan Koho	1994-2007

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/59894 A1 (Sony Computer Entertainment Inc.), 01 August, 2002 (01.08.02), Full text; all drawings & EP 1355309 A1 & JP 2002-319230 A & US 2002/169972 A1	1-16

☐ 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 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
27 August, 2007 (27.08.07)

Date of mailing of the international search report
04 September, 2007 (04.09.07)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G11B7/007(2006.01)i, G11B20/10(2006.01)i, G11B20/12(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G09C1/00-5/00, G11B7/00-7/013, 7/24-7/258, 7/28-7/30, 20/10-20/16, H04K1/00-3/00, H04L9/00-9/38

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 7 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 7 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 7 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO 02/59894 A1（株式会社ソニー・コンピュータエンタテインメント）2002.08.01, 全文, 全図 & EP 1355309 A1 & JP 2002-319230 A & US 2002/169972 A1	1-16

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

2 7 . 0 8 . 2 0 0 7

国際調査報告の発送日

0 4 . 0 9 . 2 0 0 7

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）
郵便番号 1 0 0 - 8 9 1 5
東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官（権限のある職員）

松尾 淳一

5 D

8 8 4 2

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 5 1