200529196
755519

（此處由本局於收文時黏貼條碼）

發明專利說明書

200529196

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：93140825

※申請日期：93 年 12 月 27 日　　※IPC 分類：G11B20/10

一、發明名稱：

(中) 記錄媒體、記錄媒體寫入裝置、記錄媒體讀取裝置、記錄媒體寫入方法、及記錄媒體讀取方法

(英) Recording medium, recording medium writing device, recording medium reading device, recording medium writing method, and recording medium reading method

二、申請人：(共 1 人)

1.姓　名：（中）東芝股份有限公司
（英）KABUSHIKI KAISHA TOSHIBA
代表人：（中）1.岡村正
（英）1.OKAMURA, TADASHI
地　址：（中）日本國東京都港區芝浦一丁目一番一號
（英）
國籍：（中英）日本　　JAPAN

三、發明人：(共 7 人)

1.姓　名：（中）小島正
（英）KOJIMA, TADASHI
國　籍：（中）日本
（英）JAPAN

2.姓　名：（中）山田尚志
（英）YAMADA, HISASHI
國　籍：（中）日本
（英）JAPAN

3.姓　名：（中）石原淳
（英）ISHIHARA, ATSUSHI
國　籍：（中）日本
（英）JAPAN

4.姓　名：（中）加藤拓
（英）KATO, TAKU
國　籍：（中）日本
（英）JAPAN

5.姓　名：（中）磯崎宏
（英）ISOZAKI, HIROSHI
國　籍：（中）日本
（英）JAPAN

6.姓　名：（中）松下達之
（英）MATSUSHITA, TATSUYUKI
國　籍：（中）日本
（英）JAPAN

7.姓　名：（中）松川伸一
（英）MATSUKAWA, SHINICHI
國　籍：（中）日本
（英）JAPAN

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　　；2004/01/09；2004-004710 ☑有主張優先權

4.姓　名：（中）加藤拓
（英）KATO, TAKU
國　籍：（中）日本
（英）JAPAN

5.姓　名：（中）磯崎宏
（英）ISOZAKI, HIROSHI
國　籍：（中）日本
（英）JAPAN

6.姓　名：（中）松下達之
（英）MATSUSHITA, TATSUYUKI
國　籍：（中）日本
（英）JAPAN

7.姓　名：（中）松川伸一
（英）MATSUKAWA, SHINICHI
國　籍：（中）日本
（英）JAPAN

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　　；2004/01/09；2004-004710 ☑有主張優先權

九、發明說明

【發明所屬之技術領域】

本發明係關於記錄著影像及聲音等各種內容之記錄媒體、記錄媒體寫入裝置、記錄媒體讀取裝置、記錄媒體寫入方法、以及記錄媒體讀取方法。

【先前技術】

CD（Compact Disk）及DVD（Digital Versatile Disk）等之記錄媒體，係使用於影像、聲音、以及文章等各種內容之儲存及分發等。亦即，可將內容記錄儲存於記錄媒體並進行分發。

此處之內容係一般之著作物，因爲必須防止違法複製，故會採用著作權保護技術。

因此，一般係將經過加密之內容記錄於記錄媒體。再生內容時，使用密碼金鑰對經過加密之內容進行解密。如此，只要密碼金鑰處於保密狀態，即無法實施內容之再生。爲了使密碼金鑰處於保密狀態，只要對密碼金鑰本身實施加密後再記錄於記錄媒體即可。

然而，此種手法無法對應將記錄於記錄媒體之資料全體（包含加密內容及經過加密之密碼金鑰之雙方）複製至其他記錄媒體時。

因此，出現以下之技術，亦即，在記錄型光碟之不同於通常之資料記錄再生區域之區域，以除去光碟上之反射膜而形成條狀之方式，配設用以記錄碟片識別資訊之再生

（2）

專用碟片識別資訊區域（參照日本特開 2001-189015 號公報）。

【發明內容】

將用以識別記錄媒體之資訊記錄於記錄媒體時，若複製記錄媒體本身，則無法防止著作物之違法複製。

有鑑於此，本發明之目的係在提供記錄媒體、記錄媒體寫入裝置、記錄媒體讀取裝置、記錄媒體寫入方法、以及記錄媒體讀取方法，在實施記錄媒體之資料全體、甚至於記錄媒體本身之複製時，亦可保護內容。

A.爲了達成上述目的，本發明之記錄媒體含有填埋完成所有資料，該填埋完成所有資料係在附加著錯誤校正碼之所有權對象之所有資料之附加校正碼所有資料填滿著以實施加密內容之解密爲目的之解密金鑰資料。

因爲所有資料填埋著解密金鑰資料，故無法取得解密金鑰資料。無法從填埋完成所有資料取得解密金鑰資料而想進行內容複製等時，必須針對包含所有資料在內之資料進行複製等。此時，可以針對所有資料之複製等進行法律追究，例如，很容易即可針對記錄於記錄媒體之資料全體及記錄媒體本身之非法複製進行追究。

（1）前述所有權之實例如著作權、商標權、以及眾所皆知之名稱。

所有資料具有著作物性，例如，以影像及聲音之資料爲例，可以侵害著作權之法律責任來追究所有資料之複製

（3）

等。

此外，所有資料具有商標機能時，可以侵害商標權或依違反不正競爭防止法之非法行爲來追究法律責任。具有商標機能時，例如，將記錄媒體裝設於再生裝置（磁片驅動器等）時，再生記錄媒體之製造業者之商標圖案。在販賣店展示時，可讓顧客認識到該所有資料爲商標。此時，若販賣複製了包括所有資料在內之資料全體之記錄媒體時，即會侵害到商標權。

（2）使用前述錯誤校正碼實施前述填埋完成所有資料之錯誤校正處理，會破壞前述解密金鑰資料。

亦即，利用無法從經過錯誤校正處理之填埋完成所有資料取得解密金鑰資料，故可確保解密金鑰資料之秘密性。只利用所有資料建立錯誤校正碼並利用該錯誤校正碼實施錯誤校正時，可從填埋完成所有資料重現原有之所有資料，解密金鑰資料則會消失。結果，可使再生裝置之通常輸出不含有解密金鑰資料之資訊。

解密金鑰資料之分離可以利用錯誤校正處理。亦即，錯誤校正處理步驟中，可從檢測到之錯誤型樣重現解密金鑰資料。此外，利用校正前後之填埋完成所有資料之比較，亦可再生解密金鑰資料。

（3）前述填埋完成所有資料亦可以利用以前述解密金鑰資料置換前述附加校正碼所有資料中之部份所有資料之方式而產生。

以前述解密金鑰資料置換部份所有資料，可以埋入解

（4）

密金鑰資料。

此處，亦可在前述置換之前，先以第 1 調變方式實施前述附加校正碼所有資料之調變，並以不同於第 1 調變方式之第 2 調變方式實施前述解密金鑰資料之調變。

亦即，以對應前述第 1 調變方式之第 1 解調方式實施前述填埋完成所有資料之解調，可破壞前述解密金鑰資料。結果，難以從用以實施所有資料及內容等主資訊之解密之主資訊用解密器輸出之解調資料析出解密金鑰資料。

此外，亦可以對應第 2 調變方式之第 2 解調方式來實施填埋完成所有資料之解調而得到解密金鑰資料。

（4）前述填埋完成所有資料亦可含有利用前述附加校正碼所有資料中之部份所有資料及前述解密金鑰資料進行運算處理所得到之運算資料。

利用資料間之運算來埋入解密金鑰資料。

該運算可以使用例如前述所有資料之一部份及前述解密金鑰資料間之加法運算。此外，運算亦可以使用乘法運算等之其他運算。

如上面所述，利用資料間之運算可以強化解密金鑰資料之隱密性。亦即，第 3 者難以直接從填埋完成所有資料中分離出解密金鑰資料本身。

（5）前述解密金鑰資料亦可分散配置於前述填埋完成所有資料中。

分散配置解密金鑰資料，可使第 3 者更難以取得解密金鑰資料。

（5）

此處，前述填埋完成所有資料亦可含有用以代表前述填埋完成所有資料中之解密金鑰資料之配置之資料。利用該資料可確認以分離解密金鑰資料爲目的之位置。

（6）記錄媒體亦可進一步記錄著以校正前述解密金鑰資料之錯誤爲目的之金鑰資料錯誤校正碼。

可對應因某種原因而使記錄之解密金鑰資料發生錯誤時。

此處，前述填埋完成所有資料亦可包含前述金鑰資料錯誤校正碼在內。

因爲填埋之解密金鑰資料本身並未附加錯誤校正碼，可以減少填埋於附加校正碼所有資料之資料量。因爲在附加校正碼所有資料填埋資料，會導致附加校正碼所有資料出現錯誤（Error），故不應填埋大量資料量。

（7）前述所有資料亦可含有前述記錄媒體再生時不會被確認之無法確認資料。

此處，「無法確認」係指視聽利用記錄媒體之再生所得到之影像或聲音時，不會以影像或聲音呈現出來、或即使被呈現出來亦爲會被辨識成不具意義之雜訊。亦即，該無法確認資料係具有所謂不可見之水印（Water Mark）之機能。

利用此種無法確認資料，在非法複製記錄媒體時，很容易進行追蹤。亦即，複製記錄媒體時，會連無法確認資料一起複製，很容易確認原來之資料的來源。

前述無法確認資料亦可具有以實施前述加密內容之解

密爲目的之第 2 解密金鑰資料之機能。組合解密金鑰資料來實施加密內容之解密，可以使第 3 者更難以解除加密。

如上所示，可將無法確認資料利用於資料來源之確認及內容之加密・解密。

B.本發明之記錄媒體寫入裝置具有用以產生在所有權對象之所有資料填埋以實施加密內容之解密爲目的之解密金鑰資料所得到之填埋完成所有資料之手段、及用以將前述產生之填埋完成所有資料寫入記錄媒體之手段。

利用記錄媒體寫入裝置，可以製作記錄著在所有資料填埋解密金鑰資料所得到之填埋完成所有資料之記錄媒體。結果，可有效對記錄於記錄媒體之資料全體及記錄媒體本身之非法複製進行追究。

C.本發明之記錄媒體讀取裝置具有用以從記錄媒體讀取加密內容之手段、用以從前述記錄媒體讀取在所有權對象之所有資料填埋以實施加密內容之解密爲目的之解密金鑰資料所得到之填埋完成所有資料之手段、用以從前述讀取之填埋完成所有資料分離出前述解密金鑰資料之手段、以及用以利用前述分離出之解密金鑰資料實施前述讀取之加密內容之解密之手段。

利用記錄媒體讀取裝置，可從記錄著在所有資料填埋解密金鑰資料所得到之填埋完成所有資料之記錄媒體再生內容。結果，可有效對記錄於記錄媒體之資料全體及記錄媒體本身之非法複製進行追究。

D.本發明之記錄媒體寫入方法具有以下之步驟，亦即

，用以產生在所有權對象之所有資料填埋以實施加密內容之解密爲目的之解密金鑰資料所得到之填埋完成所有資料，並將前述產生之填埋完成所有資料寫入記錄媒體。

利用記錄媒體寫入方法，可以製作記錄著在所有資料填埋解密金鑰資料所得到之填埋完成所有資料之記錄媒體。結果，可有效對記錄於記錄媒體之資料全體及記錄媒體本身之非法複製進行追究。

E.本發明之記錄媒體讀取方法具有以下之步驟，亦即，從記錄媒體讀取加密內容，從前述記錄媒體讀取在所有權對象之所有資料填埋以實施加密內容之解密爲目的之解密金鑰資料所得到之填埋完成所有資料，從前述讀取之填埋完成所有資料分離出前述解密金鑰資料，利用前述分離出之解密金鑰資料實施前述讀取之加密內容之解密。

利用記錄媒體讀取方法，可從記錄著在所有資料填埋解密金鑰資料所得到之填埋完成所有資料之記錄媒體再生內容。結果，可有效對記錄於記錄媒體之資料全體及記錄媒體本身之非法複製進行追究。

【實施方式】

以下，參照圖面，針對本發明之實施形態進行詳細說明。

（第1實施形態）

A.記錄媒體

第 1 圖係本發明第 1 實施形態之記錄媒體之再生專用光碟 10 之平面圖。

再生專用光碟 10 之內周 11 及外周 12 之間配置著抓持區域 13、BCA（Burst Cutting Area）14、引入（Lead-IN）區域 15、資料區域 16、以及引出（Lead-OUT）區域 17。

抓持（Clamping）區域 13 係以利用夾頭等固定光碟 10 爲目的之區域。

利用 BCA14、YAG 雷射等高輸出雷射光源照射脈衝狀雷射光，除去光碟 10 之部份反射層，用以記錄一種條狀條碼資料之區域。因爲針對該區域之寫入需要高輸出雷射光源，一般使用者難以對寫入於該區域之資訊進行複製（至少一般磁片驅動器無法進行寫入）。

此外，再生專用光碟 10 亦可以浮雕凹洞來構成 BCA14。

很容易即可利用母片來大量生產再生專用光碟 10。

本實施形態時，BCA14 記錄著標記識別碼（Volume-ID）。標記識別碼（Volume-ID）係以本單位（例如，1 部電影、1 首音樂）來表示記錄於光碟 10 之內容。亦即，亦可以將標記識別碼（Volume-ID）稱爲專題識別碼（Album-ID）。

如後面所述，標記識別碼（Volume-ID）係以對加密內容（Enc-contents）實施解密爲目的之解密金鑰之一。將標記識別碼（Volume-ID）記錄於一般使用者難以建立

及寫入之 BCA14，可以防止光碟 10 之非法複製。亦即，即使將光碟 10 之其他資料複製至其他記錄媒體，亦無法從該記錄媒體再生內容。

此外，本實施形態將標記識別碼（Volume-ID）記錄於 BCA14，其目的在於可以很容易地大量生產記錄著同一內容（content）之光碟 10（其他實施形態說明之記錄型記錄媒體係將用以識別記錄媒體之媒體識別碼（Media-ID）記錄於 BCA14）。

引入區域 15 係用以記錄光碟 10 之管理資訊之區域。此外，後述之可記錄型光碟 10a 時，該區域會區分成由浮雕凹洞所構成之再生專用區域（浮雕區域）、及以後可進行記錄之可記錄區域。

引入區域 15 之再生專用區域記錄著媒體金鑰區塊（MKB：Media Key Block）。媒體金鑰區塊（MKB）係以對加密內容（Enc-contents）實施解密爲目的之解密金鑰之一，與記錄於再生裝置側等之後述之裝置金鑰（Device Key）進行組合即可產生媒體金鑰（Km）。

媒體金鑰區塊（MKB）係多數金鑰之集合體，由以防止內容被非法複製爲目的而設立之 CP（Copy Protection）管理機構提供。該媒體金鑰區塊（MKB）會因爲原本爲秘密之裝置金鑰（Device Key）之呈現等，反映該時點爲無效對象之磁片驅動器等資訊而產生。因此，無效對象之磁片驅動器等無法再生記錄著媒體金鑰區塊（MKB）之光碟 10，前述媒體金鑰區塊係對應該磁片驅動器之無效。

此外，引入區域 15 記錄著最適合光碟 10 之記錄條件（參數）、及其他光碟 10 製造廠商之特有資訊。

資料區域 16 係記錄著內容之區域。該內容係包含電影等圖像資料（含靜畫及動畫在內）、音樂等聲音資料、以及電腦軟體等必須保護著作權之一般資料。

資料區域 16 記錄著填埋完成所有資料（RP-Data+MM）及加密標題金鑰（Enc-Kt）。但是，若引入區域 15 尚有空間，亦可將填埋完成所有資料（RP-Data+MM）及加密標題金鑰（Enc-Kt）記錄於該區域。

加密標題金鑰（Enc-Kt）係用以對以加密內容（Enc-contents）之解密爲目的之標題金鑰（Kt）進行加密。

填埋完成所有資料（RP-Data+MM）係在所有資料（RP-Data：Replicator Proprietary Data）以如電子穿透之保密資訊記錄再生方式填埋媒體記號（MM：Media Mark）所形成。

該所有資料（RP-Data）係著作權、商標權、以及眾所皆知之名稱等所有權對象之資料。所有資料（RP-Data）若爲影像及聲音資料等具有著作物性之資料，即爲著作權之對象。此外，所有資料（RP-Data）具有商標機能時，即爲商標權之對象。具有商標機能之實例，例如，將光碟 10 裝設於碟片驅動器（再生裝置）而再生商標之圖案時。在販賣店展示時，可讓顧客該所有資料爲商標。

因爲所有資料（RP-Data）係光碟 10 製造業者之所有物，故可保護製造業者。例如，引入區域 15 等記錄著光

碟 10 製造業者之特有資料時，不一定能以法律禁示將該資料複製至其他記錄媒體之行爲（該資料不具著作物性時，無法獲得保護）。相對於此，所有資料（RP-Data）之複製等可依據侵害著作權、侵害商標權、或不正競爭防止法來追究非法行爲之法律責任，進而保護記錄媒體製造業者。

媒體記號（MM）係以實施加密內容（Enc-contents）之解密爲目的之解密金鑰之一。因爲媒體記號（MM）填埋於所有資料（RP-Data），第 3 者難以從填埋完成所有資料（RP-Data+MM）進行分離，故可防止內容之複製。

引出區域 17 係用以記錄用以表示資料區域 16 之結束等資訊之區域。

B.將內容記錄於記錄媒體

第 2 圖係將內容記錄於光碟 10 之步驟圖。

利用著作權者 20 及 CP 管理機構 30 所提供之資料，碟片寫入裝置 40 對內容（contents）進行加密並將加密內容（Enc-contents）寫入光碟 10。

此外，著作權者 20 及 CP 管理機構 30 係個人或団體，其本身並非物。

著作權者 20 對記錄媒體製造業者提供標題金鑰（Kt）及內容（content）。

CP 管理機構 30 對碟片製造業者提供媒體金鑰（Km）及媒體金鑰區塊（MKB）。媒體金鑰區塊（MKB）係由

MKB 產生處理部 31 利用裝置金鑰（Device key）群及媒體金鑰（Km）所產生。

標記識別碼（Volume-ID）、所有資料（RP-Data）、以及媒體記號（MM）係由碟片製造業者自行決定，儲存於碟片寫入裝置 40。

媒體金鑰區塊（MKB）係由碟片寫入裝置 40 記錄於光碟 10 之引入區域 15。

標記識別碼（Volume-ID）係由碟片寫入裝置 40 記錄於 BCA14。

第 1 金鑰產生處理部 41 利用媒體金鑰（Km）及標記識別碼（Volume-ID）產生第 1 特有媒體金鑰（Kume1）。產生之第 1 特有媒體金鑰（Kume1）及媒體記號（MM）信號被傳送至第 2 金鑰產生處理部 42 並產生第 2 特有媒體金鑰（Kum2）。

加密處理部 44 利用該第 2 特有媒體金鑰（Kum2）產生標題金鑰（Kt）經過加密之加密標題金鑰（Enc-Kt）。利用碟片寫入裝置 40 將產生之加密標題金鑰（Enc-Kt）記錄於資料區域 16。

加密處理部 45 產生利用對內容（content）進行加密前之標題金鑰（Kt）實施加密之加密內容（Enc-contents）。利用碟片寫入裝置 40 將產生之加密內容（Enc-contents）記錄於資料區域 16。

媒體記號填埋處理部 43 將媒體記號（MM）填埋至所有資料（RP-Data）而產生填埋完成所有資料（RP-

Data+MM）。利用碟片寫入裝置 40 將產生之填埋完成所有資料（RP-Data+MM）記錄於資料區域 16。

此外，將媒體記號（MM）填埋於所有資料（RP-Data）之詳細方法如後面所述。

C.從記錄媒體再生內容

第 3 圖係再生光碟 10 並實施加密內容（Enc-contents）之解密之步驟圖。此處之構成上，係利用如電腦之系統來再生光碟 10。亦即，利用光碟讀取裝置 50 讀取資料，並利用 AV（Audio Visual）解碼器模組 60 實施加密內容（Enc-contents）之解密。

光碟讀取裝置 50 係用以從光碟 10 讀取資料之例如 DVD 驅動器。AV 解碼器模組 60 係例如連結於電腦之 AV 解碼器基板，用以輸出再生之內容（content）。

光碟讀取裝置 50 及 AV 解碼器模組 60 之各認證處理部 51、61 間會相互實施認證。該認證之目的係在決定後述之加密處理部 52～54 及解密處理部 62～64 之加密、解密方式。

在光碟讀取裝置 50 及 AV 解碼器模組 60 之間實施金鑰資訊之加密並進行傳送及接收，可防止金鑰資訊等之流出。

該加密、解密方式可分別由認證處理部 51、61 相互交換亂數而決定。決定之加密、解密方式分別由認證處理部 51、61 傳送至加密處理部 52～54 及解密處理部 62～64

，光碟讀取裝置 50 對金鑰資訊進行加密並傳送，AV 解碼器模組 60 可進行解密。

此外，若將利用認證決定之加密・解密方式限定成特定時間內使用，則可更有效地防止金鑰資訊等之流出。此外，該認證若使用儲存於 AV 解碼器模組 60 之裝置金鑰組（Device Key Set）等，可有效地防止非法之機器使用。

認證後，光碟讀取裝置 50 分別從光碟 10 之引入區域 15 及 BCA14 讀取媒體金鑰區塊（MKB）及標記識別碼（Volume-ID），並傳送至 AV 解碼器模組 60。該傳送時，媒體金鑰區塊（MKB）及標記識別碼（Volume-ID）會在加密處理部 52、53 被進行加密並輸出，且在解密處理部 62、63 進行解密。其目的係在防止光碟讀取裝置 50 之輸出洩漏媒體金鑰區塊(MKB)及標記識別碼(Volume-ID)。

此外，光碟讀取裝置 50 從資料區域 16 讀取填埋完成所有資料（RP-Data+MM），並以媒體記號分離處理部 55 分離出媒體記號（MM）。此外，該分離之詳細情形如後面所述。

分離出之所有資料（RP-Data）及媒體記號（MM）從光碟讀取裝置 50 傳送至 AV 解碼器模組 60。此時，媒體記號（MM）在加密處理部 54 經過加密並輸出，並在解密處理部 64 實施解密。其目的係在防止光碟讀取裝置 50 之輸出洩漏媒體記號（MM）。

此外，光碟讀取裝置 50 從資料區域 16 讀取加密標題

金鑰（Enc-Kt）及加密內容（Enc-contents），並傳送至AV解碼器模組60。

AV解碼器模組60則執行以下之處理。亦即，媒體金鑰區塊處理部65利用媒體金鑰區塊（MKB）及儲存於AV解碼器模組60之裝置金鑰（Device Keys）產生媒體金鑰（Km）。此外，第1金鑰產生部66利用媒體金鑰（Km）及標記識別碼（Volume-ID）產生第1特有媒體金鑰（Kum1）。第2金鑰產生部67則利用媒體記號（MM）將第1特有媒體金鑰（Kum1）變換成第2特有媒體金鑰（Kum2）。

解密處理部68利用第2特有媒體金鑰（Kum2）實施讀取之加密標題金鑰（Enc-Kt）之解密，產生標題金鑰（Kt）。解密處理部69使用標題金鑰（Kt）做爲用以對加密內容（Enc-contents）實施解密之解密金鑰，再生內文之內容（content）。

AV解碼器模組60輸出之所有資料（RP-Data）可應用於電腦等，例如，可利用其在視聽內容本身之前顯示碟片製造業者之商標。

D.針對所有資料（RP-Data）之媒體記號（MM）之填埋・分離

針對所有資料（RP-Data）之媒體記號（MM）之填埋及分離詳細說明如下。如後面所述，被填埋之媒體記號（MM）在光碟10之通常之再生處理時會被消除，而不易被

光碟讀取裝置 50 讀取。換言之，被填埋之媒體記號（MM）可稱爲「可消除電子穿透」。

第 4 圖係利用錯誤型樣填埋媒體記號（MM）之步驟圖。

此外，第 5 圖～第 8 圖係第 4 圖之步驟中之資料狀態模式圖。

媒體金鑰區塊（MKB）、內容（content）、以及所有資料（RP-Data）被視爲主資訊（M-Data），與扇區 ID 及其他補助資料 RSB（Reserv）等一起被傳送至 EDC（Error Detection Code）產生部 R02，用以產生 EDC。此時，資料被會實施扇區化而成爲資料扇區。

第 5 圖係資料扇區之構成模式圖。

資料扇區由 12 行（1 行=172 位元組）所構成。前頭行配置著由扇區號碼及扇區資訊所構成之扇區識別碼（ID），其次，爲 ID 錯誤檢測符號（IED）及補助資料（RSB），其後則爲 2K 位元組之主資料區域。最後行之最後附加著以主資料爲目的之錯誤檢測碼（EDC）。

拌碼部 R03 實施主資訊（M-Data）之拌碼。爲了避免記錄資料成爲相同圖案之重複，該資料拌碼在主資訊（M-Data）爲「全“0”」時亦會實施。係防止因爲光碟 10 之鄰接磁軌之串音等導致無法正確檢測出尋軌伺服錯誤信號等問題。

16 資料框集合部 D031 係由 16 組資料框集合而成，由 PO/PI 產生部 R05 產生錯誤校正碼 PO（外符號）/PI（

內符號）。結果，主資訊（M-Data）被以 16 扇區單位實施 ECC（錯誤校正碼）塊化。亦即，所有資料（RP-Data）成爲附加著錯誤校正碼之 ECC 塊。

媒體記號用錯誤校正碼產生部 R11 利用媒體記號（MM）產生媒體記號用錯誤校正碼（MM-Pa）。

媒體記號加法運算部 R12 對 ECC 塊中之所有資料（RP-Data）之一部份實施媒體記號（MM）及媒體記號用錯誤校正碼（MM-Pa）之重　加法運算。亦即，實施所有資料（RP-Data）之一部份及媒體記號（MM）之加法運算，可在所有資料（RP-Data）中填埋媒體記號（MM），而產生填埋完成所有資料（RP-Data+MM）。此外，此時之加法運算係互斥或，爲「1+0=1」、「1+1=0」。

如此，利用資料間之運算，可使解密金鑰資料更爲隱密。亦即，第 3 者難以直接從填埋完成所有資料中分離出解密金鑰資料本身（比以媒體記號（MM）置換部份所有資料（RP-Data）時更爲隱密）。

第 6 圖係填埋著媒體記號（MM）之 ECC 塊之模式圖。

針對 ECC 塊之各列（縱向）產生 16 位元組（1 位元組=1 行）之外符號 PO，針對各行（橫方向）產生 10 位元組之內符號 PI。16 行（16 位元組）之外符號 PO 係以每 12 行（各扇區）配置 1 行（位元組）之方式來進行分散配置。

此處，係以分散填埋媒體記號（MM）之方式來提高

媒體記號（MM）之保密性。此外，以配置於所有資料（RP-Data）之特定位置之填埋位置資訊表示媒體記號（MM）信號填埋位置。

此時，以某函數決定媒體記號（MM）之填埋位置，填埋位置資訊可以當做用以輸入該函數之資料使用。利用此方式，媒體記號（MM）信號之填埋位置會因爲所有資料（RP-Data）之內容而不同，故可提高安全性。

其後，PO 交插部 R06 實施外符號 PO 之交插處理，SYNC 附加&調變處理部 R07 實施 SYNC（同步信號）之附加及調變處理，記錄媒體寫入部 R08 將資料記錄於光碟 10。

第 7 圖係 PO 交插後之 ECC 塊構成之模式圖。

16 行（16 位元組）之外符號 PO 會被以每 12 行（各扇區）配置 1 行（位元組）之方式進行分散配置。因爲外符號 PO 之一部份（1 行）附加於第 5 圖所示之扇區（12 行）而成爲 12 行+1 行，對其實施交插。

第 8 圖係以何種方式將所有資料（RP-Data）及媒體記號（MM）信號配置於 ECC 塊之模式圖。

所有資料（RP-Data）會被分割且配置於複數 ECC 塊。

媒體記號（MM）配置於 1 個 ECC 塊內。但是，以分散於複數實體扇區之方式進行配置。此外，媒體記號用錯誤校正碼（MM-Pa）配置於最後之實體扇區。

如此，將媒體記號（MM）配置於 1 個 ECC 塊內，很

容易將媒體記號（MM）填埋於複數 ECC 塊（媒體記號（MM）之多重寫入），而提高媒體記號（MM）之信賴度。

其次，針對從填埋完成所有資料（RP-Data+MM）分離出媒體記號（MM）進行說明。

如前面所述，利用媒體記號分離處理部 55 從填埋完成所有資料（RP-Data+MM）分離出媒體記號（MM）。

該分離係利用錯誤校正處理。亦即，對填埋完成所有資料（RP-Data+MM）實施錯誤校正處理，在該步驟中檢測出錯誤型樣。因爲該錯誤型樣對應媒體記號（MM），故可以利用錯誤型樣再生媒體記號（MM）。

此外，將錯誤校正處理前後之填埋完成所有資料（RP-Data+MM）進行比較，亦可再生媒體記號（MM）。

本實施形態係以分散方式配置媒體記號（MM），利用第 6 圖之填埋位置資訊，可以從錯誤型樣等再生媒體記號（MM）。

（第 2 實施形態）

其次，針對本發明第 2 實施形態進行說明。本實施形態使用與第 1 實施形態相同之光碟 10，故省略光碟 10 本身之說明。

A.將內容記錄於記錄媒體

第 9 圖係將內容記錄於光碟 10 之步驟圖。本圖係對應第 2 圖。

此處，係配置著金鑰產生處理部 411，用以取代第 2 圖之第 1、第 2 金鑰產生處理部 41、42。此外，配置著第 1、第 2 加密處理部 441、442，用以取代第 2 圖之加密處理部 44。

金鑰產生處理部 411 利用媒體金鑰（Km）及標記識別碼（Volume-ID）產生特有媒體金鑰（Kum）。

第 1 加密處理部 441 利用該特有媒體金鑰（Kum）對標題金鑰（Kt）實施加密而得到加密標題金鑰（Enc-Kt）。此外，第 2 加密處理部 442 利用媒體記號（MM）將加密標題金鑰（Enc-Kt）加密成級聯而產生多重加密標題金鑰（Enc.Enc-Kt）。將產生之多重加密標題金鑰（Enc.Enc-Kt）記錄於光碟 10。

此外，以電子穿透技術將媒體記號（MM）填埋於所有資料（RP-Data）並進行記錄之手段，與第 1 實施形態相同。

利用此構成，可將媒體記號（MM）信號密封於磁片驅動器（光碟讀取裝置 50a）內。後面會進行說明。

B.從記錄媒體再生內容

第 10 圖係再生以第 9 圖所示之方式進行記錄之光碟 10 並對加密內容（Enc-contents）實施解密之步驟圖，對應第 3 圖。

此處，配置著金鑰產生處理部 661，用以取代第 3 圖之第 1、第 2 金鑰產生處理部 66、67。此外，配置著第 1

、第 2 解密處理部 541、681，用以取代第 3 圖之解密處理部 68。

利用光碟讀取裝置 50a 從光碟 10 讀取填埋完成所有資料（RP-Data+MM），並利用媒體記號分離處理部 55 分離出媒體記號（MM）。

利用光碟讀取裝置 50a 從光碟 10 讀取之多重加密標題金鑰（Enc.Enc-Kt）在第 1 解密處理部 541 進行解密並產生加密標題金鑰（Enc-Kt），且被傳送至 AV 解碼器模組 60a。

AV 解碼器模組 60a 之金鑰產生處理部 661 利用媒體金鑰（Km）及標記識別碼（Volume-ID）產生特有媒體金鑰（Kum）。第 2 解密處理部 681 利用該特有媒體金鑰（Kum）實施加密標題金鑰（Enc-Kt）之解密而產生標題金鑰（Kt）。

加密內容（Enc-contents）利用該標題金鑰（Kt）實施解密，再生內文之內容（contents）。

由以上可知，從填埋完成所有資料（RP-Data+MM）分離出之媒體記號（MM），只使用於光碟讀取裝置 50a 內，而不必輸出至 AV 解碼器模組 60a。亦即，因爲光碟讀取裝置 50a 讀取之資料不含媒體記號（MM），可以防止第 3 者讀取媒體記號（MM）並利用其實施加密內容（Enc-contents）之解密。

（第 3 實施形態）

其次，針對本發明第 3 實施形態進行說明。本實施形態使用使用者可對光碟執行記錄之記錄再生媒體。

A.記錄媒體

第 11 圖係本發明第 3 實施形態之記錄媒體之可記錄光碟 10a 之平面圖，對應第 1 圖。

光碟 10a 之內周 11 及外周 12 之間配置著抓持區域 13、BCA 區域（Burst Cutting Area）14、引入（Lead-IN）區域 15、已記錄區域 161、未記錄區域 162、以及引出（Lead-OUT）區域 17。亦即，配置已記錄區域 161 及未記錄區域 162，用以取代第 1 圖之資料區域 16。此外，已記錄區域 161 及未記錄區域 162 之雙方被稱爲記錄區域。

BCA14 配置著以識別各光碟 10a 爲目的之媒體識別碼（Media-ID），用以取代第 1 圖之標記識別碼（Volume-ID）。

引入區域 15 除了記錄著媒體金鑰區塊（MKB）以外，尙記錄著填埋完成所有資料（RP-Data+MM）。填埋完成所有資料（RP-Data+MM）之記錄部位與第 1 圖不同，係光碟 10a 之已記錄區域 161 及未記錄區域 162 已預定使用者用以記錄之區域。

填埋完成所有資料（RP-Data+MM）所含有之所有資料（RP-Data）使用記錄媒體製造廠商具有所有權之商標圖案等檔案，很容易追究光碟 10a 之非法複製。亦即，對於利用複製填埋完成所有資料（RP-Data+MM）或所有資

料（RP-Data）、或直接複製光碟 10a 本身來製造相同記錄再生媒體之行爲，很容易適用著作權法、商標權法、或不正競爭防止法等。

B.記錄媒體之製造

光碟 10a 之由記錄媒體之製造業者進行製造，然而，資料之記錄上，則預定成由一般使用者實施。因此，將其分成光碟 10a 之製造時及內容之記錄時來進行說明。

第 12 圖係製造時之將資料記錄於光碟 10a 之步驟圖。

CP 管理機構 30 將媒體金鑰區塊（MKB）提供給碟片製造業者。媒體金鑰區塊（MKB）係由 MKB 產生處理部 31 利用裝置金鑰（Device key）群及媒體金鑰（Km）所產生。

媒體識別碼（Media-ID）、所有資料（RP-Data）、以及媒體記號（MM）可由碟片製造業者自行決定，記錄於碟片寫入裝置 40b。

媒體金鑰區塊（MKB）利用碟片寫入裝置 40b 記錄於光碟 10 之引入區域 15。

媒體識別碼（Media-ID）利用碟片寫入裝置 40b 記錄於 BCA14。

媒體記號填埋處理部 43 以碟片寫入裝置 40b 將利用所有資料（RP-Data）及媒體記號（MM）所產生之填埋完成所有記號（RP-Data+MM）記錄於引入區域 15。

C.將內容記錄於記錄媒體

第 13 圖係將內容記錄於光碟 10a 之步驟圖。

利用光碟寫入裝置 70a 及 AV 編碼器模組 80a 實施內容（contents）之加密並記錄於光碟 10a。

光碟寫入裝置 70a 及 AV 編碼器模組 80a 之各認證處理部 71a、81a 間會相互實施認證。該認證之目的係在決定後述之加密處理部 72a～74a 及解密處理部 82a～84a 之加密、解密方式。

在光碟寫入裝置 70a 及 AV 編碼器模組 80a 之間實施金鑰資訊之加密並進行傳送及接收，可防止金鑰資訊等之流出。

認證後，光碟寫入裝置 70a 分別從光碟 10a 之引入區域 15 及 BCA14 讀取媒體金鑰區塊（MKB）及媒體識別碼（Media-ID），並傳送至 AV 編碼器模組 80a。該傳送時，媒體金鑰區塊（MKB）及媒體識別碼（Media-ID）會在加密處理部 72a、73a 被進行加密並輸出，且在解密處理部 82a、83a 進行解密。其目的係在防止媒體金鑰區塊（MKB）及媒體識別碼（Media-ID）之洩漏。

此外，光碟寫入裝置 70a 從引入區域 15 讀取填埋完成所有資料（RP-Data+MM），並以媒體記號（MM）分離部 75a 分離出媒體記號（MM）。分離出之所有資料（RP-Data）及媒體記號（MM）從光碟寫入裝置 70a 傳送至 AV 編碼器模組 80a。此時，媒體記號（MM）在加密處理部

71a 經過加密並輸出，並在解密處理部 84a 實施解密。其目的係在防止光碟寫入裝置 70a 之輸出洩漏媒體記號（MM）。

AV 編碼器模組 80a 執行以下之處理。亦即，媒體金鑰區塊（MKB）處理部 85a 利用媒體金鑰區塊（MKB）及記錄於 AV 編碼器模組 80a 之裝置金鑰（Device Keys）產生媒體金鑰（Km）。此外，第 1 金鑰產生部 86a 利用媒體金鑰（Km）及媒體識別碼（Media-ID）產生第 1 特有媒體金鑰（Kum1）。第 2 金鑰產生部 87a 利用媒體記號（MM）將第 1 特有媒體金鑰（Kum1）變換成第 2 特有媒體金鑰（Kum2）。

標題金鑰產生部 90a 產生標題金鑰（Kt）並輸出。該標題金鑰產生部 90a 係使用亂數產生器。

加密處理部 88a 利用標題金鑰（Kt）對第 2 特有媒體金鑰（Kum2）進行加密，產生加密標題金鑰（Enc-Kt），利用光碟寫入裝置 70a 將其寫入光碟 10a 之記錄區域。

另一方面，加密處理部 89a 利用標題金鑰（Kt）實施內容（content）之加密，產生加密內容（Enc-contents），利用光碟寫入裝置 70a 將其寫入光碟 10a 之記錄區域。

所有資料（RP-Data）可應用於電腦等，例如，可利用其在裝設光碟 10a 時顯示碟片製造業者之商標。

D.從記錄媒體再生內容

第 14 圖係再生光碟 10a 並實施加密內容（Enc-

contents）之解密之步驟圖。此處之構成上，係利用如電腦之系統來再生光碟 10。亦即，利用光碟讀取裝置 50b 讀取資料，並利用 AV（Audio Visual）解碼器模組 60b 實施加密內容（Enc-contents）之解密。

第 14 圖所示之處理內容係以媒體識別碼（Media-ID）取代標記識別碼（Volume-ID），與第 3 圖及處理內容十分類似。因此，省略第 14 圖之詳細說明。

（第 4 實施形態）

其次，針對本發明第 4 實施形態進行說明。本實施形態所使用之光碟 10a 之構成、及其製造步驟與第 3 實施形態相同。因此，只針對記錄媒體之內容記錄及再生進行說明。

A.將內容記錄於記錄媒體

第 15 圖係對內容（contents）進行加密並記錄於光碟 10a 之步驟圖，對應第 13 圖。

此處，配置著金鑰產生處理部 86b，用以取代第 13 圖之第 1、第 2 金鑰產生處理部 86a、87a。此外，配置著第 1、第 2 加密處理部 88b、76b，用以取代第 13 圖之加密處理部 88a。

金鑰產生處理部 86b 利用媒體金鑰（Km）及媒體識別碼（Media-ID）產生特有媒體金鑰（Kum）。

第 1 加密處理部 88b 利用該特有媒體金鑰（Kum）實

施標題金鑰（Kt）之加密而成爲加密標題金鑰（Enc-Kt）。此外，第 2 加密處理部 76b 利用媒體記號（MM）實施加密標題金鑰（Enc-Kt）之加密而產生多重加密標題金鑰（Enc.Enc-Kt）。產生之多重加密標題金鑰（Enc.Enc-Kt）被記錄於光碟 10a。

利用此構成，可將媒體記號（MM）信號密封於驅動器內。其說明如後面所述。

B.從記錄媒體再生內容

第 16 圖係再生以第 15 圖所示之方式進行記錄之光碟 10 並對加密內容（Enc-contents）實施解密之步驟圖，對應第 14 圖。

此處，配置著金鑰產生處理部 66c，用以取代第 14 圖之第 1、第 2 金鑰產生處理部 66b、67b。此外，配置著第 1、第 2 解密處理部 56c、68c，用以取代第 14 圖之解密處理部 68b。

利用光碟讀取裝置 50c 從光碟 10a 讀取填埋完成所有資料（RP-Data+mm），並利用媒體記號分離處理部 55c 分離出媒體記號（MM）。

利用光碟讀取裝置 50c 從光碟 10a 讀取之多重加密標題金鑰（Enc.Enc-Kt）在第 1 解密處理部 56c 進行解密並產生加密標題金鑰（Enc-Kt），且被傳送至 AV 解碼器模組 60c。

AV 解碼器模組 60c 之金鑰產生處理部 66c 利用媒體

金鑰（Km）及標記識別碼（Volume-ID）產生特有媒體金鑰（Kum）。第 2 解密處理部 68c 利用該特有媒體金鑰（Kum）實施加密標題金鑰（Enc-Kt）之解密而產生標題金鑰（Kt）。

利用該標題金鑰（Kt）實施加密內容（Enc-contents）之解密，再生內文之內容（contents）。

由以上可知，從填埋完成所有資料（RP-Data+MM）分離出之媒體記號（MM），只使用於光碟讀取裝置 50c 內，而不必輸出至 AV 解碼器模組 60c。亦即，因爲光碟讀取裝置 50c 讀取之資料不含媒體記號（MM），可以防止第 3 者讀取媒體記號（MM）並利用其實施加密內容（Enc-contents）之解密。

（第 5 實施形態）

其次，針對本發明第 5 實施形態進行說明。本實施形態只有媒體記號（MM）之填埋方式不同於其他實施形態。此外，本實方面形態係以對光碟 10 執行記錄爲例，然而，亦適用於光碟 10a。

第 17 圖係採用特殊調變方式做爲媒體記號（MM）之填埋方式時之步驟，對應第 4 圖。

PO/PI 產生部 R05 產生錯誤校正碼 PO（外符號）/PI（內符號），至將該錯誤校正碼附加於 ECC 塊爲止，與第 4 圖相同。此處，PO/PI 產生部 R05 輸出之 ECC 塊會直接在 PO 交插部 R06 實施 PO 之交插處理，SWC 附加&調

變處理部 R07 實施 SYNC（同步信號）之附加及調變處理。

媒體記號用錯誤校正碼產生部 R11 利用媒體記號（MM）產生媒體記號用錯誤校正碼（MM-Pa），其後，利用調變部 R13 實施調變處理。

如以上所示，分別對所有資料（RP-Data）及媒體記號（MM）實施調變。亦即，媒體記號（MM）係與不同於主資訊（M-Data）之調變方式來進行調變。

其後，媒體記號置換部 R14 以媒體記號（MM）及媒體記號用錯誤校正碼（MM-Pa）之調變記錄信號置換所有資料（RP-Data）之調變記錄信號之一部份，產生記錄信號並記錄於光碟 10。

使媒體記號（MM）之調變方式不同於主資訊（M-Data），即使知道媒體記號（MM）之填埋位置時，亦可防止第 3 者取得媒體記號（MM）。

第 18 圖係利用第 17 圖所示之特殊調變方式填埋媒體記號（MM）信號時之實體扇區（Physical sector）之模式圖。

以 2 組 32+1456 通道位元之「SYNC 框」構成 1 行。例如，第 18 圖之第 1 行之 SY0 及 SY5 爲槽框。以 26 個此種類之行之集合構成實體扇區。

此處，媒體記號（MM）係填埋於 SY3 之框。

（第 6 實施形態）

其次，針對本發明第 6 實施形態進行說明。本實施形態與第 5 實施形態相同，係以不同於主資訊（M-Data）之調變方式來實施媒體記號（MM）之調變。

第 19 圖係採用特殊調變方式做爲媒體記號（MM）之填埋方式時之步驟，對應第 17 圖。此外，第 20 圖係第 19 圖之步驟之詳細圖，除了主資訊（M-data）含有控制資料（Control-Da）及明示資料框 DO2 等以外，執行之處理內容爲實質相同。

此處，係追加媒體記號用錯誤校正碼（MM-Pa）做爲主資訊（M-data）所有資料（RP-Data）之一部份。如此，可獲得以下之優點。

亦即，以填埋媒體記號（MM）使主資訊側產生某種錯誤。因此，對主資訊側追加媒體記號用錯誤校正碼（MM-Pa），可減少填埋於主資訊之媒體記號（MM）之填埋量。

此外，對含有媒體記號用錯誤校正碼（MM-Pa）之主資訊附加錯誤校正碼，可提高媒體記號用錯誤校正碼（MM-Pa）本身之信賴度。

亦即，再生時，可對主資訊實施錯誤校正處理，校正媒體記號用錯誤校正碼（MM-Pa）本身之錯誤。此外，使用該媒體記號用錯誤校正碼（MM-Pa）執行媒體記號（MM）之錯誤校正處理。

如以上所示，在主資訊側追加媒體記號用錯誤校正碼（MM-Pa），與填埋媒體記號（MM）及媒體記號用錯誤

校正碼（MM-Pa）之雙方時相比，可提高媒體記號（MM）之信賴度。

此外，媒體記號用錯誤校正碼（MM-Pa）組合於主資訊並洩漏至外部時，只有媒體記號用錯誤校正碼（MM-Pa）仍然難以重現媒體記號（MM），故保密性不會大幅降低。

（第 7 實施形態）

其次，針對本發明第 7 實施形態進行說明。

本實施形態係在所有資料（RP-Data）內之圖案資訊內填埋水印（WM：Water Mark）。到目前爲止所說明之媒體記號（MM），基本上，不會被從光碟讀取裝置輸出，亦即，係無法複製之電子穿透資訊。此處之水印（WM）會被從光碟讀取裝置輸出，故可謂是與光碟 10 內之通常資料相同之可複製之電子穿透資訊。

第 21 圖係在所有資料（RP-Data）內之圖案資訊內填埋水印（WM）來產生填埋完成所有資料（RP-Data+WM）之步驟。

該水印（WM）雖然可複製，然而，卻是視聽光碟 10 時不易辨認之物。亦即，基本上，此處之水印（WM）係不可見，不會以第 21 圖之填埋完成所有資料（RP-Data+WM）之圖樣可辨識出水印（WM）之圖案之形式呈現出來。

如此，填埋不可見之水印（WM），在複製所有資料

（RP-Data）時，會在不知情之狀況下連水印（WM）一起複製。結果，複製所有資料（RP-Data）時，很容易進行追蹤調查。

第 22 及 23 圖係同時使用媒體記號（MM）及水印（WM）來進行內容之加密、解密之步驟圖，分別對應第 2 及 3 圖。此時，水印（WM）被視爲密碼金鑰而非第 21 圖之圖像資訊。

利用媒體金鑰塊（MKB）、標記識別碼（Volume-ID）、以及媒體記號（MM）產生第 2 特有媒體金鑰（Kum2）與第 2 圖相同。

第 22 圖係針對第 2 圖追加了第 3 金鑰產生處理部 46 及水印填埋處理部 47。

利用水印（WM）將第 2 特有媒體金鑰（Kum2）變換成第 3 特有媒體金鑰（Kum3），並利用其實施標題金鑰（Kt）之加密。此外，進一步在填埋完成所有資料（RP-Data+MM）填埋水印（WM），並將其視爲多重填埋完成所有資料（RP-Data+MM 十 WM）記錄於光碟 10。

第 23 圖係在第 3 圖追加了水印分離處理部 691 及第 3 金鑰產生處理部 692。利用媒體記號分離處理部 55 從多重填埋完成所有資料（RP-Data+MM+WM）分離出媒體記號（MM），產生填埋完成所有資料（RP-Data+WM）。此外，利用水印分離處理部 691 從填埋完成所有資料（RP-Data+WM）分離出水印（WM）。此外，利用水印（WM）將第 2 特有媒體金鑰（Kum2）變換成第 3 特有媒體金鑰

（Kum3），利用其實施標題金鑰（Kt）之解密。

此外，使媒體記號（MM）及水印（WM）相同、或具有某種關係式成立之關係時，利用比較兩者可檢測到違法複製。

亦即，使媒體記號（MM）及水印（WM）之間具有某種關連，可以判斷缺少其中任一方（或其中之一部份）之光碟 10 爲複製品。如前面所述，因爲通常難以複製媒體記號（MM），從光碟 10 複製資料時，會複製水印（WM）而沒有媒體記號（MM）。如此，對以互相對應之方式記錄著媒體記號（MM）及水印（WM）之光碟 10 進行複製時，該對應關係很難維持。

（其他實施形態）

如以上所示，上述實施形態係在例如代表記錄媒體製造者之所有權之標章等資料檔案之所有資料（RP-Data）填埋可消除之電子穿透（媒體記號（MM））或不可消除之電子穿透（水印（WM）），可保護記錄於記錄媒體之內容及記錄媒體本身。

本發明之實施形態未受限於上述實施形態，可進行擴充及變更，擴充及變更之實施形態亦屬於本發明之技術範圍。

【圖式簡單說明】

第 1 圖係本發明第 1 實施形態之光碟之平面圖。

第 2 圖係將內容記錄於本發明第 1 實施形態之光碟之步驟圖。

第 3 圖係從本發明第 1 實施形態之光碟再生內容之步驟圖。

第 4 圖係利用錯誤型樣填埋媒體記號之步驟圖。

第 5 圖係第 4 圖之步驟中之資料狀態模式圖。

第 6 圖係第 4 圖之步驟中之資料狀態模式圖。

第 7 圖係第 4 圖之步驟中之資料狀態模式圖。

第 8 圖係第 4 圖之步驟中之資料狀態模式圖。

第 9 圖係本發明第 2 實施形態之將內容記錄於光碟之步驟圖。

第 10 圖係本發明第 2 實施形態之從光碟再生內容之步驟圖。

第 11 圖係本發明第 3 實施形態之光碟之平面圖。

第 12 圖係製造本發明第 3 實施形態之光碟時之記錄資料之步驟圖。

第 13 圖係將內容記錄於本發明第 3 實施形態之光碟之步驟圖。

第 14 圖係本發明第 3 實施形態之從光碟再生內容之步驟圖。

第 15 圖係本發明第 4 實施形態之將內容記錄於光碟之步驟圖。

第 16 圖係本發明第 4 實施形態之從光碟從內容再生之步驟圖。

第 17 圖係本發明第 5 實施形態之利用特殊調變方式填埋媒體記號之步驟圖。

第 18 圖係本發明第 5 實施形態之利用特殊調變方式填埋著媒體記號（MM）信號時之實體扇區之模式圖。

第 19 圖係本發明第 6 實施形態之利用特殊調變方式填埋媒體記號（MM）信號之步驟圖。

第 20 圖係本發明第 6 實施形態之第 19 圖之詳細模式圖。

第 21 圖係利用在所有資料內之圖案資訊內填埋水印來產生填埋完成所有資料之步驟。

第 22 圖係同時使用媒體記號及水印實施內容之加密之步驟圖。

第 23 圖係同時使用媒體記號及水印實施內容之解密之步驟圖。

【主要元件之符號說明】

10、10a：光碟

11：內周

12：外周

13：抓持區域

14：BCA 區域（Burst Cutting Area）

15：引入（Lead-In）區域

16：資料區域

161：已記錄區域

162：未記錄區域

17：引出（Lead-0UT）區域

20：著作權者

30：CP管理機構

31：MKB產生處理部

40、40a、40b：碟片寫入裝置

411：金鑰產生處理部

41：第1金鑰產生處理部

42：第2金鑰產生處理部

43：媒體記號填埋處理部

44：加密處理部

441：第1加密處理部

442：第2加密處理部

45：加密處理部

46：第3金鑰產生處理部

47：水印填埋處理部

50、50a、50b、50c：光碟讀取裝置

51、51b、51c：認證處理部

52、52b、52c：加密處理部

53、53b、53c：加密處理部

54、54b：加密後處理部

55、55b、55c：媒體記號分離處理部

56c：第1解密處理部

541：第1解密處理部

60、60a、60b、60c：AV解碼器模組

61、61b、61c：認證處理部

62、62b、62c：解密處理部

63、63b、63c：解密處理部

64、64b：解密處理部

65、65b、65c：媒體金鑰區塊處理部

66、66b：第1金鑰產生部

66c：金鑰產生處理部

661：金鑰產生處理部

67、67b：第2金鑰產生部

68、68b：解密處理部

68c：第2解密處理部

681：第2解密處理部

69、69b、69c：解密處理部

691：水印分離處理部

692：第3金鑰產生處理部

70a：光碟寫入裝置

71a、71b：認證處理部

72a、72b：加密處理部

73a、73b：加密處理部

74a、74b：加密處理部

75a：媒體記號（MM）分離部

76b：第2加密處理部

80a、80b：AV編碼器模組

81a、81b：認證處理部

82a、82b：解密處理部

83a、83b：解密處理部

84a：解密處理部

85a、85b：媒體金鑰區塊（MKB）處理部

86a：第 1 金鑰產生部

86b：金鑰產生處理部

87a：第 2 金鑰產生部

88a：加密處理部

88b：第 1 加密處理部

89a、89b：加密處理部

90a、90b：標題金鑰產生部

五、中文發明摘要

發明之名稱：記錄媒體、記錄媒體寫入裝置、記錄媒體讀取裝置、記錄媒體寫入方法、及記錄媒體讀取方法

將在所有權對象之所有資料填埋解密金鑰資料而成之填埋完成所有資料記錄至記錄媒體，該解密金鑰資料係用以實施加密內容之解密者。因爲所有資料填埋著解密金鑰資料，難以從所有資料分離並取出解密金鑰資料。對於包含所有資料在內之複製等行爲時，可針對所有資料之複製等進行法律追訴。

六、英文發明摘要

發明之名稱：RECORDING MEDIUM, RECORDING MEDIUM WRITING DEVICE, RECORDING MEDIUM READING DEVICE, RECORDING MEDIUM WRITING METHOD, AND RECORDING MEDIUM READING METHOD

Embedded proprietary data, which is configured by embedding decoding key data for decoding encoded contents into proprietary data that is a subject of ownership, is recorded on a recording medium. Since the decoding key data is embedded into the proprietary data, it is difficult to separate and take out the decoding key data from the proprietary data. When copying or the like including the proprietary data is performed, it becomes possible to legally pursue a copy or the like of the proprietary data.

(1)

十、申請專利範圍

1. 一種記錄媒體，其特徵爲包含：

在所有權對象之所有資料被附加有錯誤校正碼的附加校正碼所有資料上，被填埋解密金鑰資料而成的填埋完成所有資料，該解密金鑰資料爲用於對加密內容進行解密者。

2. 如申請專利範圍第 1 項之記錄媒體，其中

前述所有權，係包含著作權、商標權、及眾所皆知之名稱之至少其中任一。

3. 如申請專利範圍第 1 項之記錄媒體，其中

利用前述錯誤校正碼執行前述填埋完成所有資料之錯誤校正處理來破壞前述解密金鑰資料。

4. 如申請專利範圍第 1 項之記錄媒體，其中

前述填埋完成所有資料，係利用前述解密金鑰資料置換前述附加校正碼所有資料中之所有資料之一部份而產生。

5. 如申請專利範圍第 4 項之記錄媒體，其中

在前述置換之前，先以第 1 調變方式實施前述附加校正碼所有資料之調變，並以不同於第 1 調變方式之第 2 調變方式實施前述解密金鑰資料之調變。

6. 如申請專利範圍第 5 項之記錄媒體，其中

以對應於前述第 1 調變方式之第 1 解調方式實施前述填埋完成所有資料之解調來破壞前述解密金鑰資料。

7. 如申請專利範圍第 1 項之記錄媒體，其中

(2)

前述填埋完成所有資料，係包含針對前述附加校正碼所有資料中之所有資料之一部份及前述解密金鑰資料執行運算處理所得到之運算資料。

8. 如申請專利範圍第 7 項之記錄媒體，其中

前述運算係前述所有資料之一部份與前述解密金鑰資料間之加法運算。

9. 如申請專利範圍第 1 項之記錄媒體，其中

前述解密金鑰資料，係分散配置於前述填埋完成所有資料中。

10. 如申請專利範圍第 9 項之記錄媒體，其中

前述填埋完成所有資料，係含有資料用以表示前述填埋完成所有資料中之解密金鑰資料之配置。

11. 如申請專利範圍第 1 項之記錄媒體，其中

進一步具有金鑰資料錯誤校正碼，用以校正前述解密金鑰資料之錯誤。

12. 如申請專利範圍第 11 項之記錄媒體，其中

前述金鑰資料錯誤校正碼包含於前述填埋完成所有資料之內。

13. 如申請專利範圍第 1 項之記錄媒體，其中

前述所有資料含有前述記錄媒體之再生時無法進行確認之無法確認資料。

14. 如申請專利範圍第 13 項之記錄媒體，其中

前述無法確認資料，係作爲第 2 解密金鑰資料之機能，用以實施前述加密內容之解密。

(3)

15. 一種記錄媒體寫入裝置，其特徵爲包含有：

填埋完成所有資料產生單元，用以在所有權對象之所有資料填埋解密金鑰資料而產生填埋完成所有資料，該解密金鑰資料係用以實施加密內容之解密；及

寫入單元，用以將前述產生之填埋完成所有資料寫入記錄媒體。

16. 一種記錄媒體讀取裝置，其特徵爲包含有：

內容讀取單元，用以從記錄媒體讀取加密內容；

所有資料讀取單元，用以從前述記錄媒體讀取在所有權對象之所有資料上填埋解密金鑰資料而成之填埋完成所有資料，該解密金鑰資料係實施加密內容之解密者；

分離單元，用以從前述讀取之填埋完成所有資料分離出前述解密金鑰資料；以及

解密單元，利用前述分離出之解密金鑰資料實施前述讀取之加密內容之解密。

17. 一種記錄媒體寫入方法，其特徵爲包含：

在所有權對象之所有資料填埋解密金鑰資料而產生填埋完成所有資料，該解密金鑰資料係用以實施加密內容之解密者，

並將前述產生之填埋完成所有資料寫入記錄媒體。

18. 一種記錄媒體讀取方法，其特徵爲包含：

從記錄媒體讀取加密內容，

從前述記錄媒體讀取在所有權對象之所有資料填埋解密金鑰資料而成之填埋完成所有資料，該解密金鑰資料係

(4)

用以實施加密內容之解密，

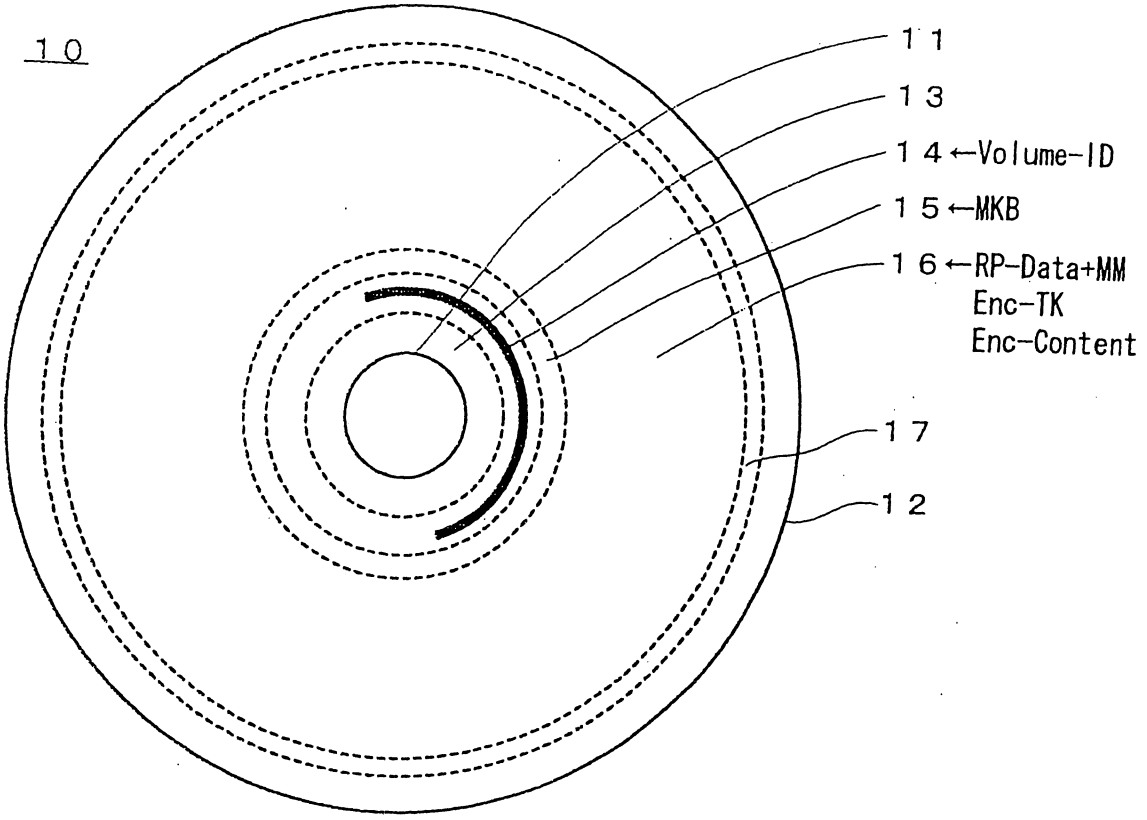
從前述讀取之填埋完成所有資料分離出前述解密金鑰資料，

利用前述分離出之解密金鑰資料，實施前述讀取之加密內容之解密。

200529196

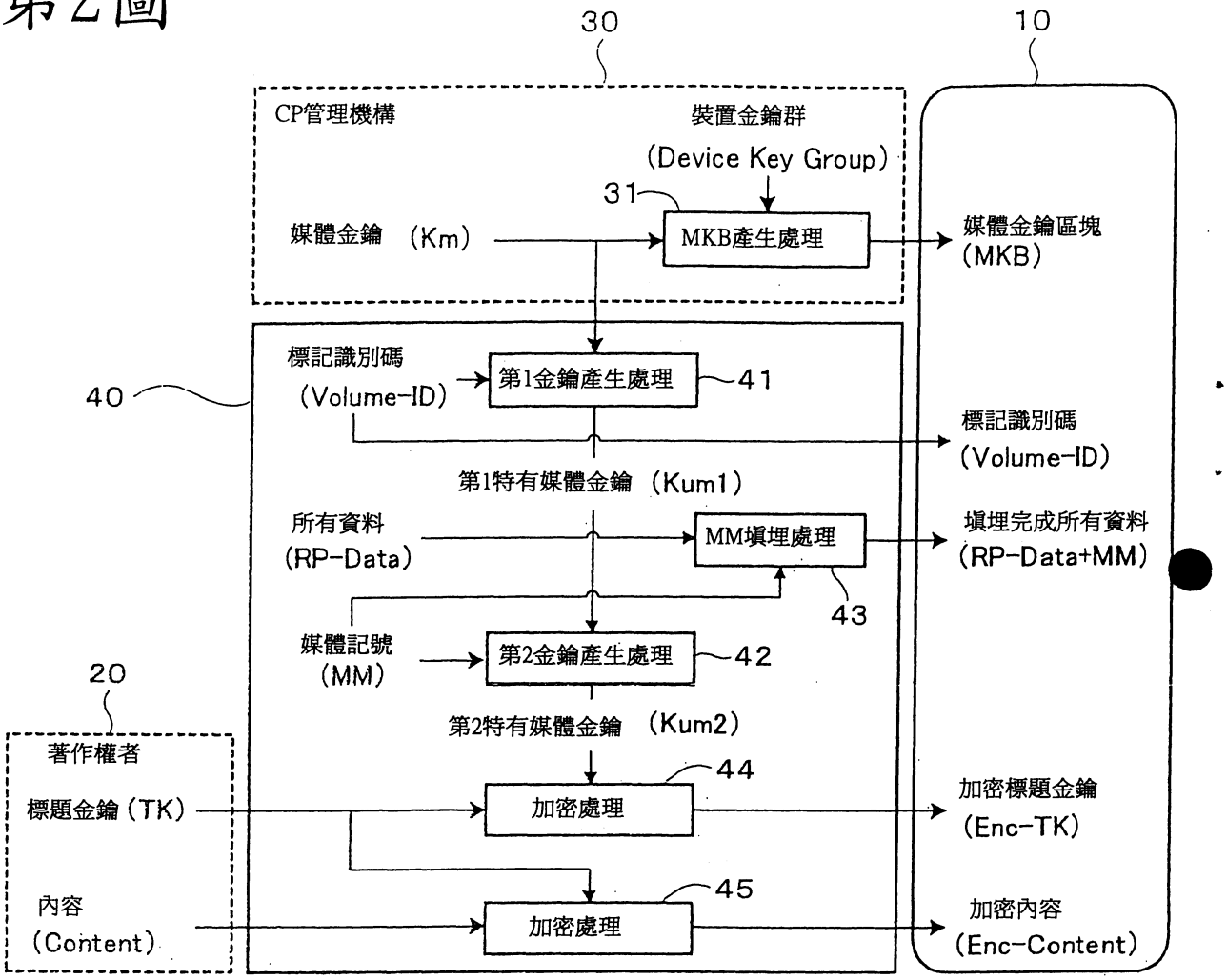
755519

第1圖

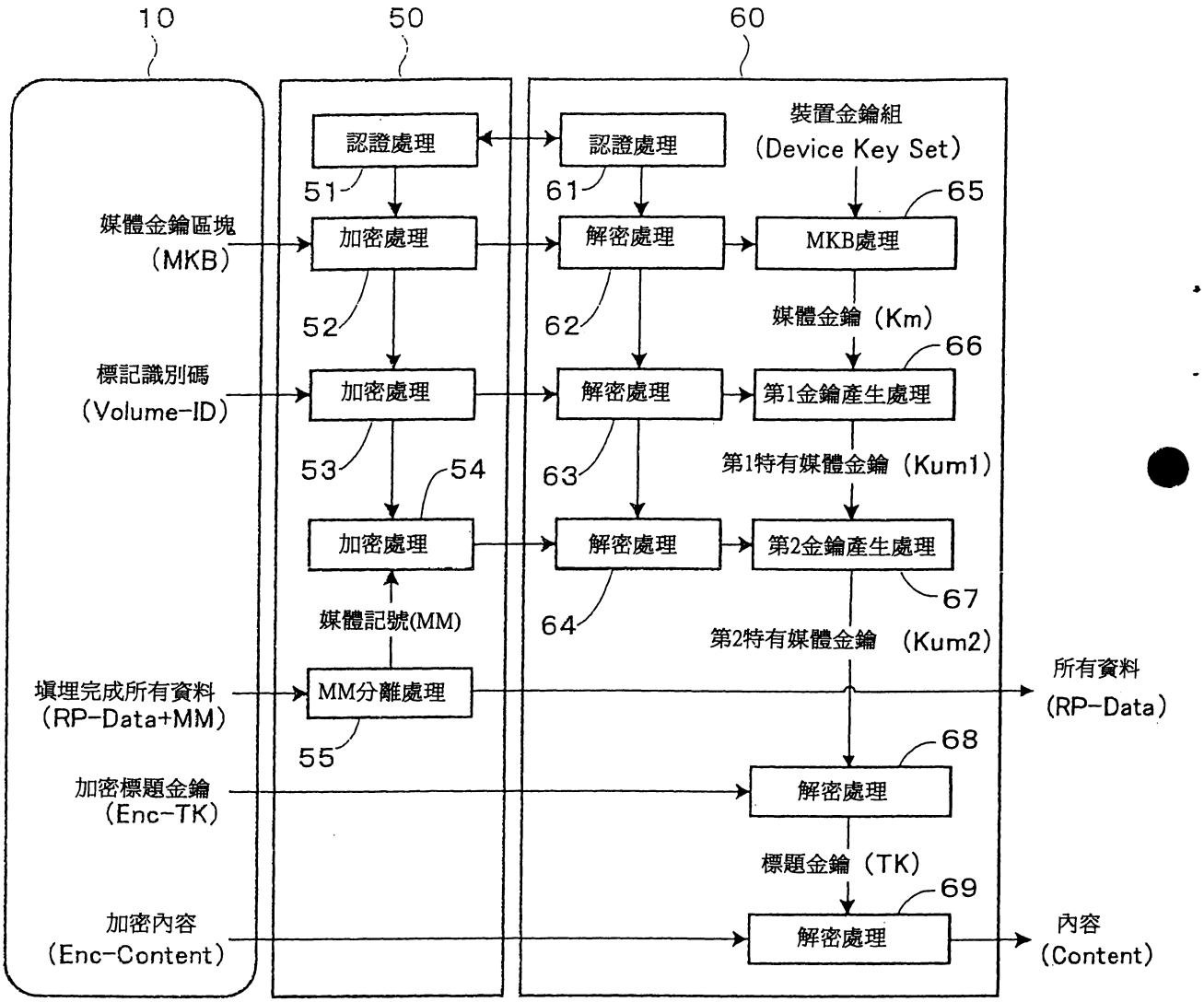


200529196

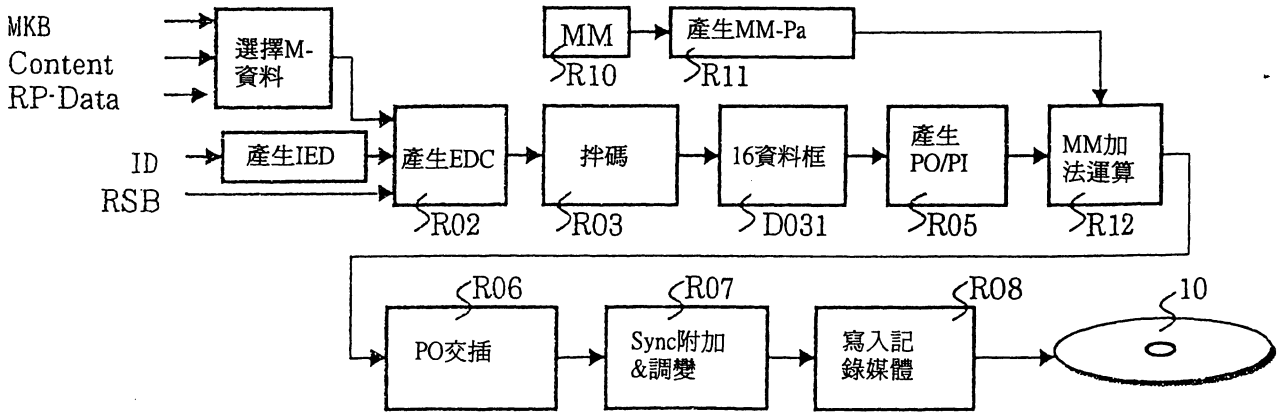
第2圖



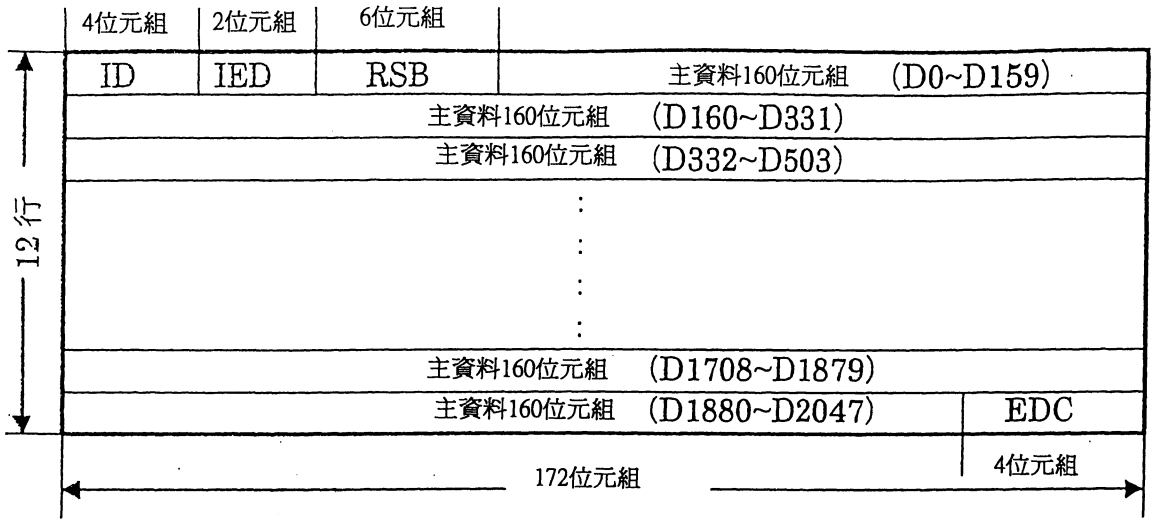
第3圖


10
50
60
認證處理
認證處理
裝置金鑰組
(Device Key Set)
51
61
65
媒體金鑰區塊
(MKB)
加密處理
解密處理
MKB處理
52
62
媒體金鑰 (Km)
66
標記識別碼
(Volume-ID)
加密處理
解密處理
第1金鑰產生處理
53
54
63
第1特有媒體金鑰 (Kum1)
加密處理
解密處理
第2金鑰產生處理
67
媒體記號(MM)
64
第2特有媒體金鑰 (Kum2)
所有資料
(RP-Data)
填埋完成所有資料
(RP-Data+MM)
MM分離處理
55
68
加密標題金鑰
(Enc-TK)
解密處理
標題金鑰 (TK)
69
加密內容
(Enc-Content)
解密處理
內容
(Content)

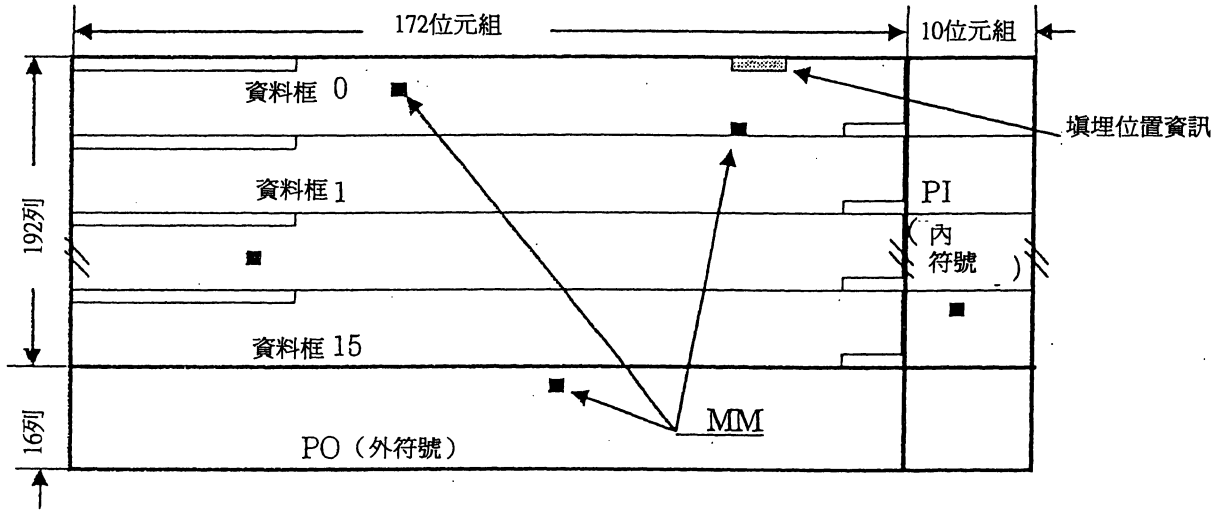
第4圖


MKB
Content
RP-Data
選擇M-資料
ID
RSB
產生IED
產生EDC
R02
拌碼
R03
16資料框
D031
產生PO/PI
R05
MM加法運算
R12
MM
R10
產生MM-Pa
R11
R06
PO交插
R07
Sync附加&調變
R08
寫入記錄媒體
10

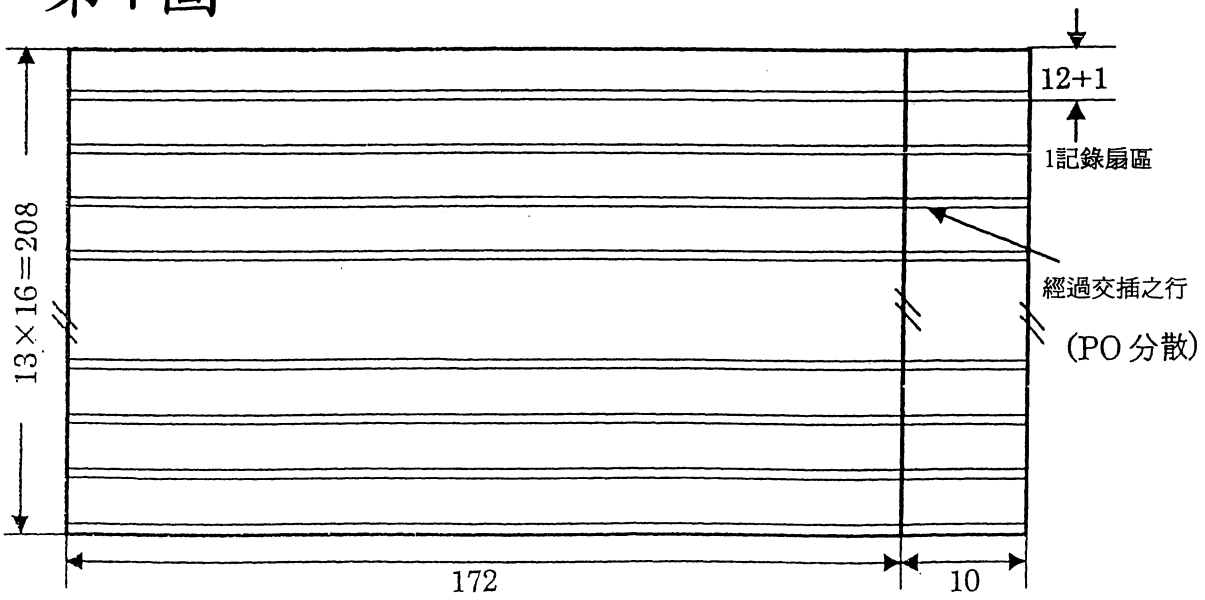
第5圖


4位元組
2位元組
6位元組
ID
IED
RSB
主資料160位元組 (D0~D159)
主資料160位元組 (D160~D331)
主資料160位元組 (D332~D503)
主資料160位元組 (D1708~D1879)
主資料160位元組 (D1880~D2047)
EDC
4位元組
12行
172位元組

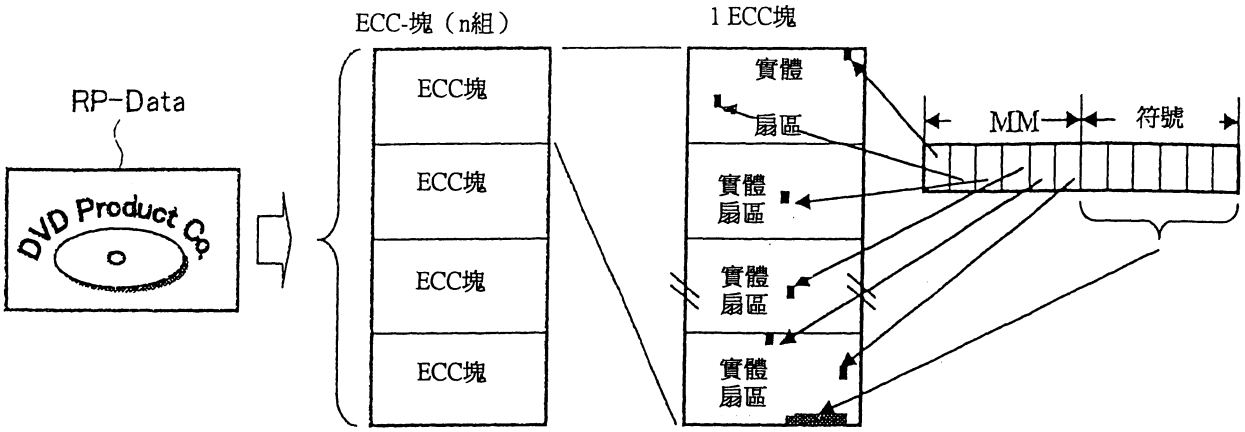
第6圖


172位元組
10位元組
資料框 0
資料框 1
資料框 15
填埋位置資訊
PI
內符號
192列
16列
MM
PO（外符號）

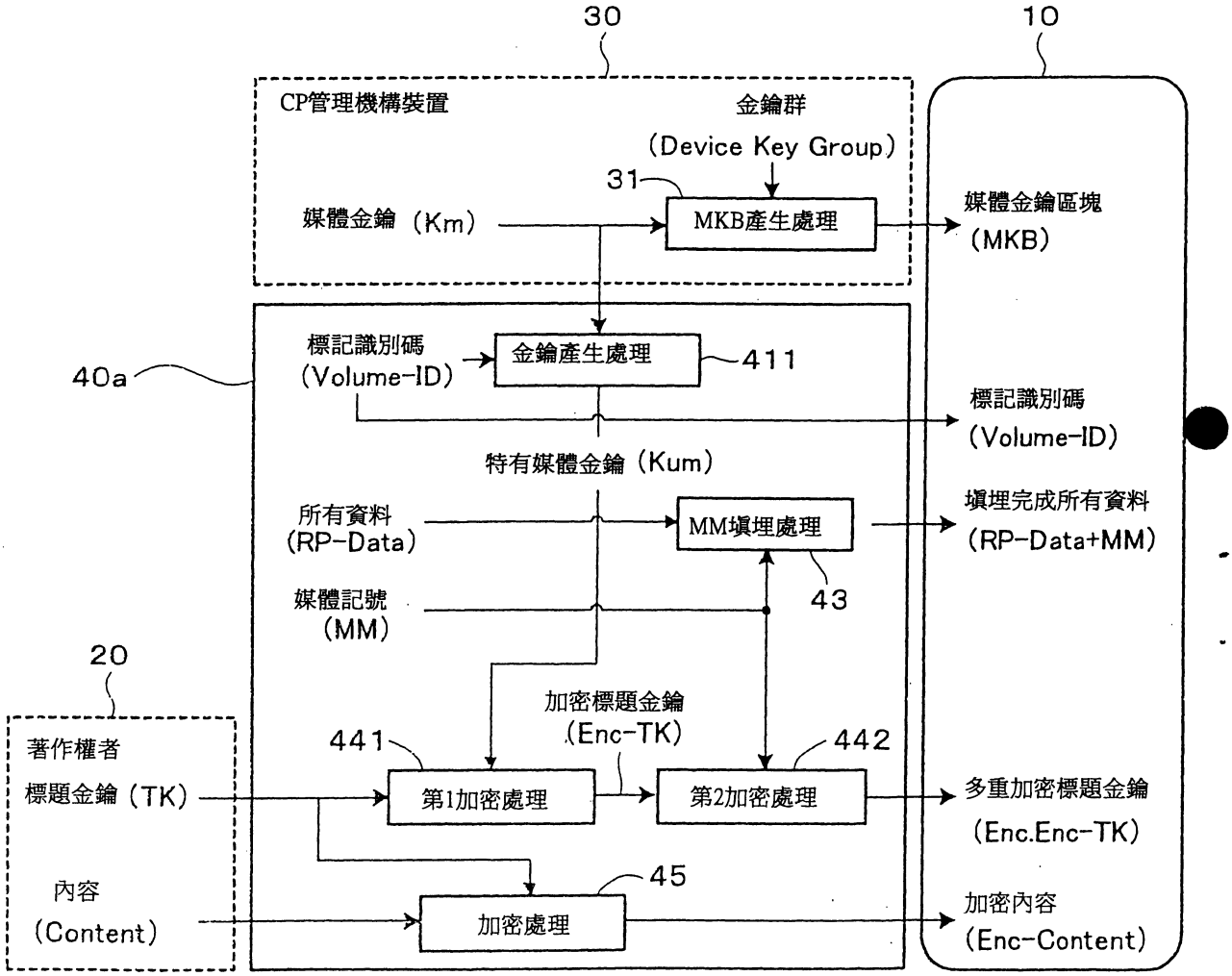
第7圖


12+1
1記錄扇區
經過交插之行
(PO 分散)
13×16=208
172
10

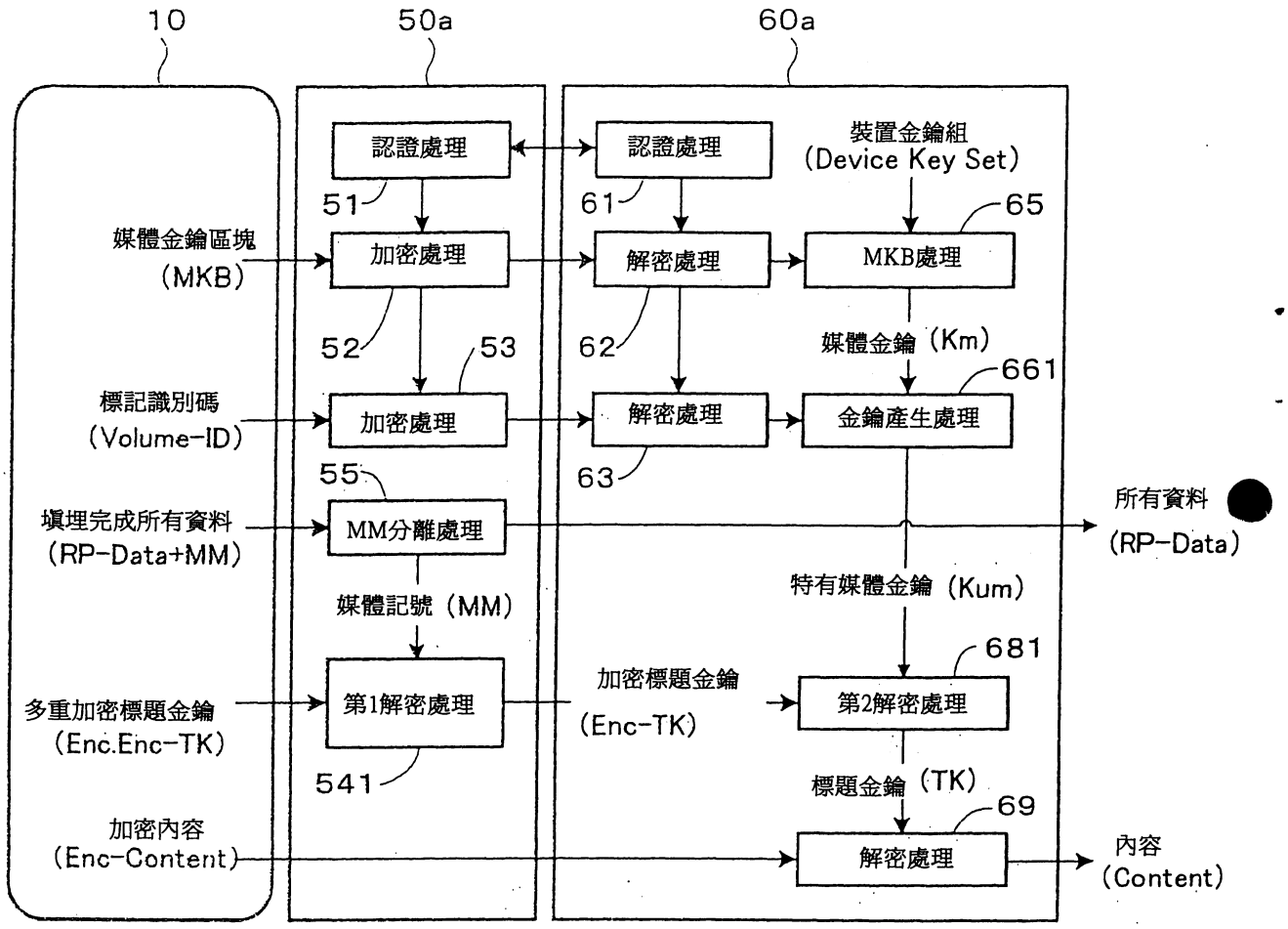
第8圖


ECC-塊（n組）
1 ECC塊
RP-Data
DVD Product Cp
ECC塊
ECC塊
ECC塊
ECC塊
實體
扇區
實體
扇區
實體
扇區
實體
扇區
MM
符號

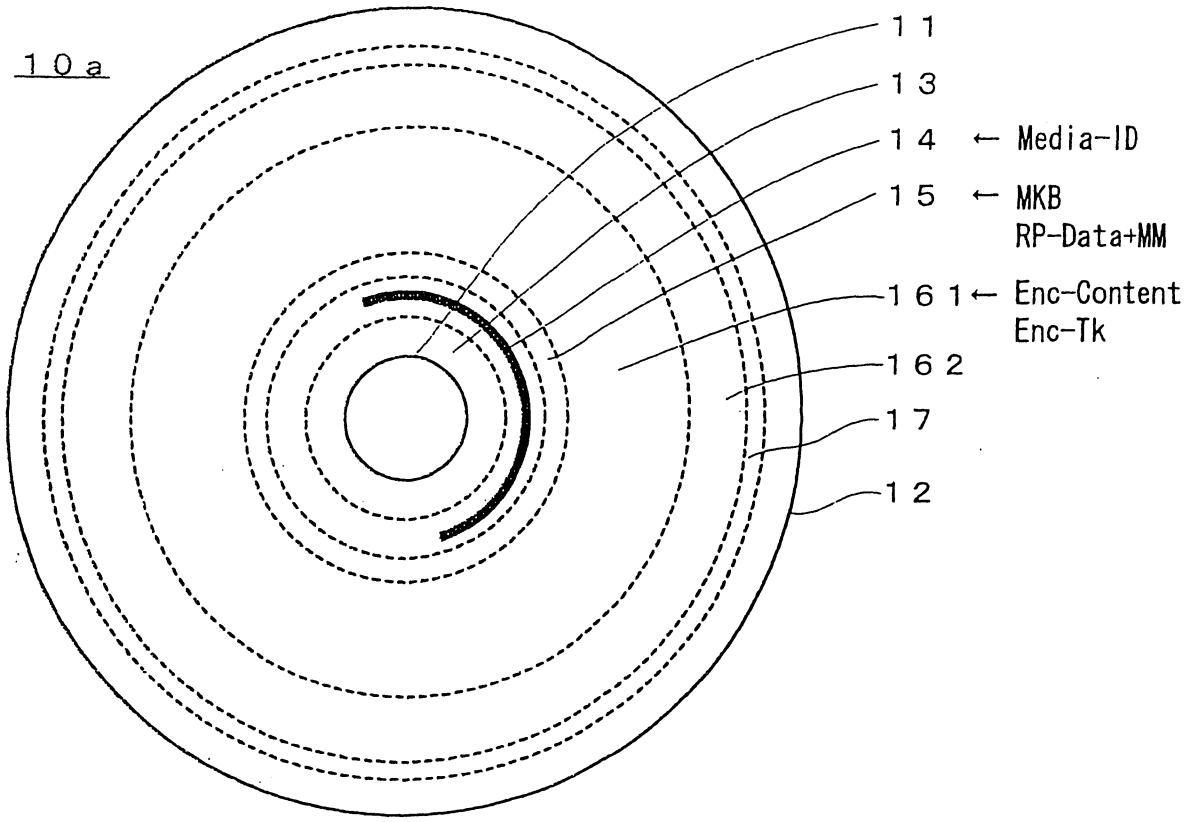
第9圖


30
10
CP管理機構裝置
金鑰群
(Device Key Group)
31
媒體金鑰（Km）
MKB產生處理
媒體金鑰區塊
(MKB)
40a
標記識別碼
(Volume-ID)
金鑰產生處理
411
標記識別碼
(Volume-ID)
特有媒體金鑰（Kum）
所有資料
(RP-Data)
MM填埋處理
填埋完成所有資料
(RP-Data+MM)
媒體記號
(MM)
43
20
加密標題金鑰
(Enc-TK)
441
442
著作權者
標題金鑰（TK）
第1加密處理
第2加密處理
多重加密標題金鑰
(Enc.Enc-TK)
45
內容
(Content)
加密處理
加密內容
(Enc-Content)

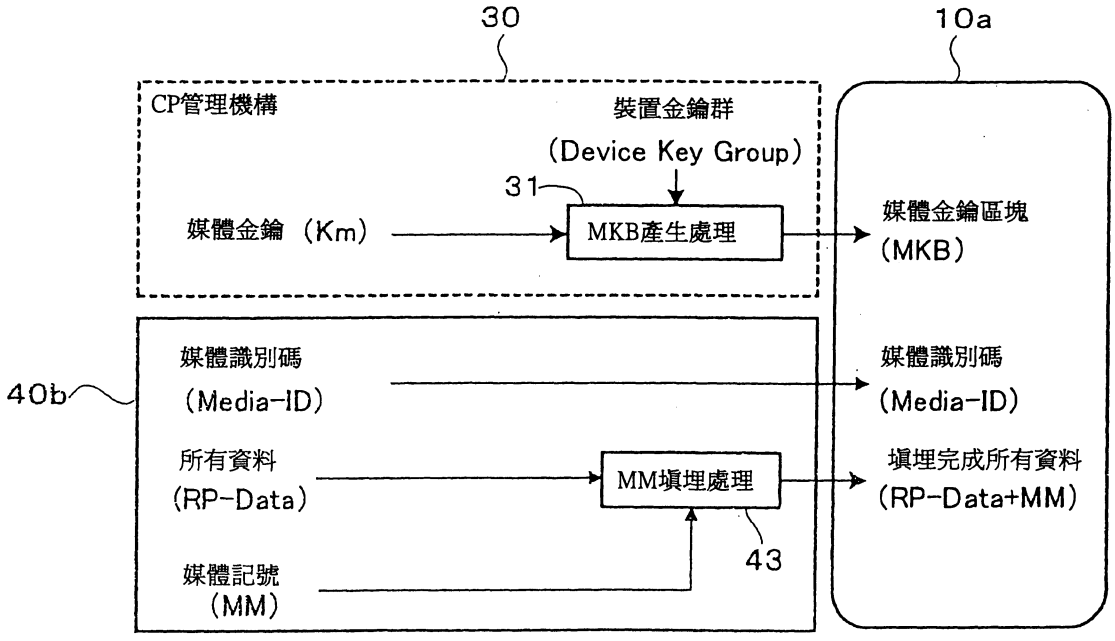
第10圖


10
50a
60a
認證處理
認證處理
裝置金鑰組
(Device Key Set)
51
61
65
媒體金鑰區塊
(MKB)
加密處理
解密處理
MKB處理
52
62
媒體金鑰 (Km)
53
661
標記識別碼
(Volume-ID)
加密處理
解密處理
金鑰產生處理
55
63
填埋完成所有資料
(RP-Data+MM)
MM分離處理
所有資料
(RP-Data)
特有媒體金鑰 (Kum)
媒體記號 (MM)
681
加密標題金鑰
(Enc-TK)
多重加密標題金鑰
(Enc.Enc-TK)
第1解密處理
第2解密處理
541
標題金鑰 (TK)
69
加密內容
(Enc-Content)
解密處理
內容
(Content)

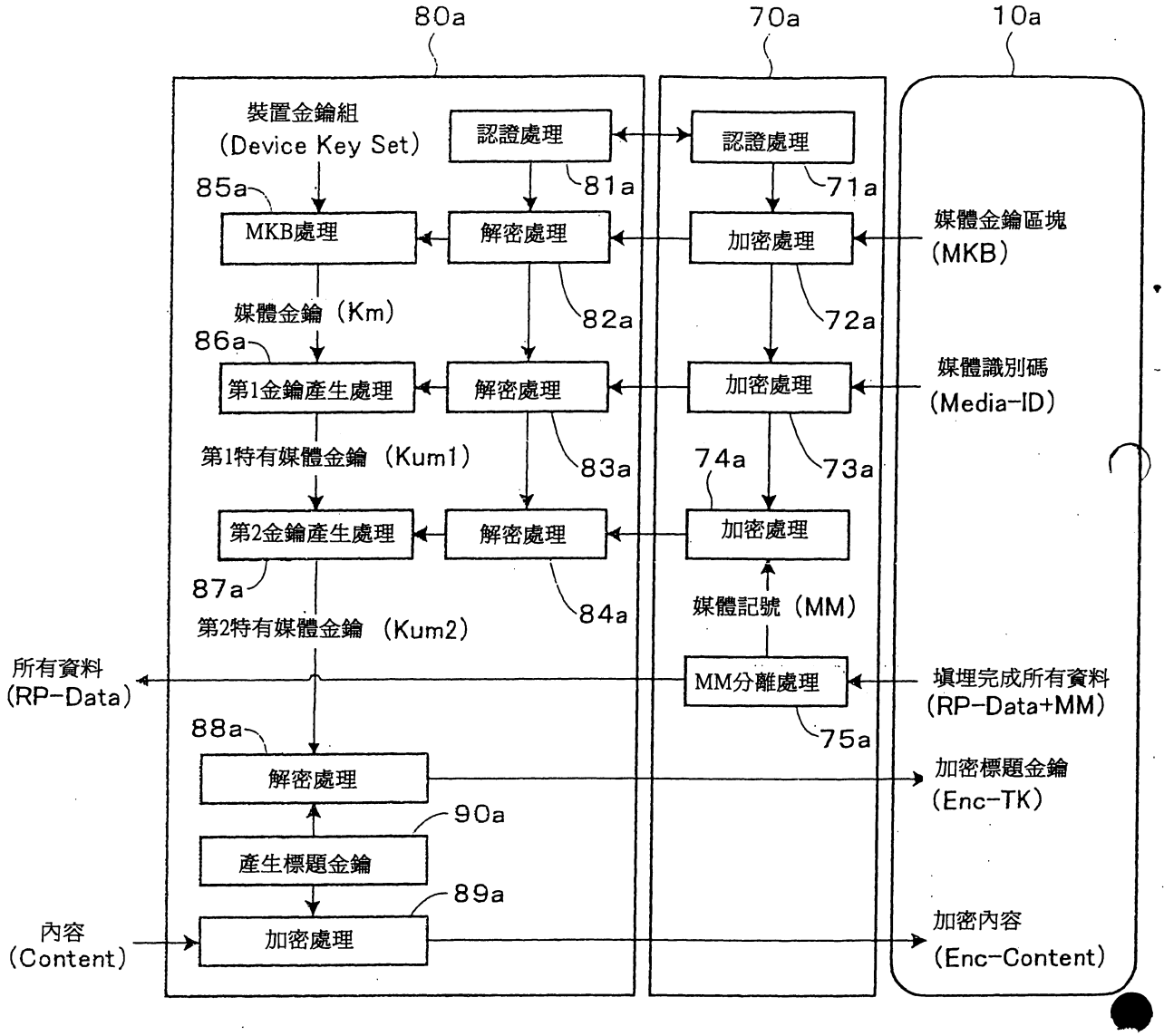
第11圖


10a
11
13
14 ← Media-ID
15 ← MKB
RP-Data+MM
161 ← Enc-Content
Enc-Tk
162
17
12

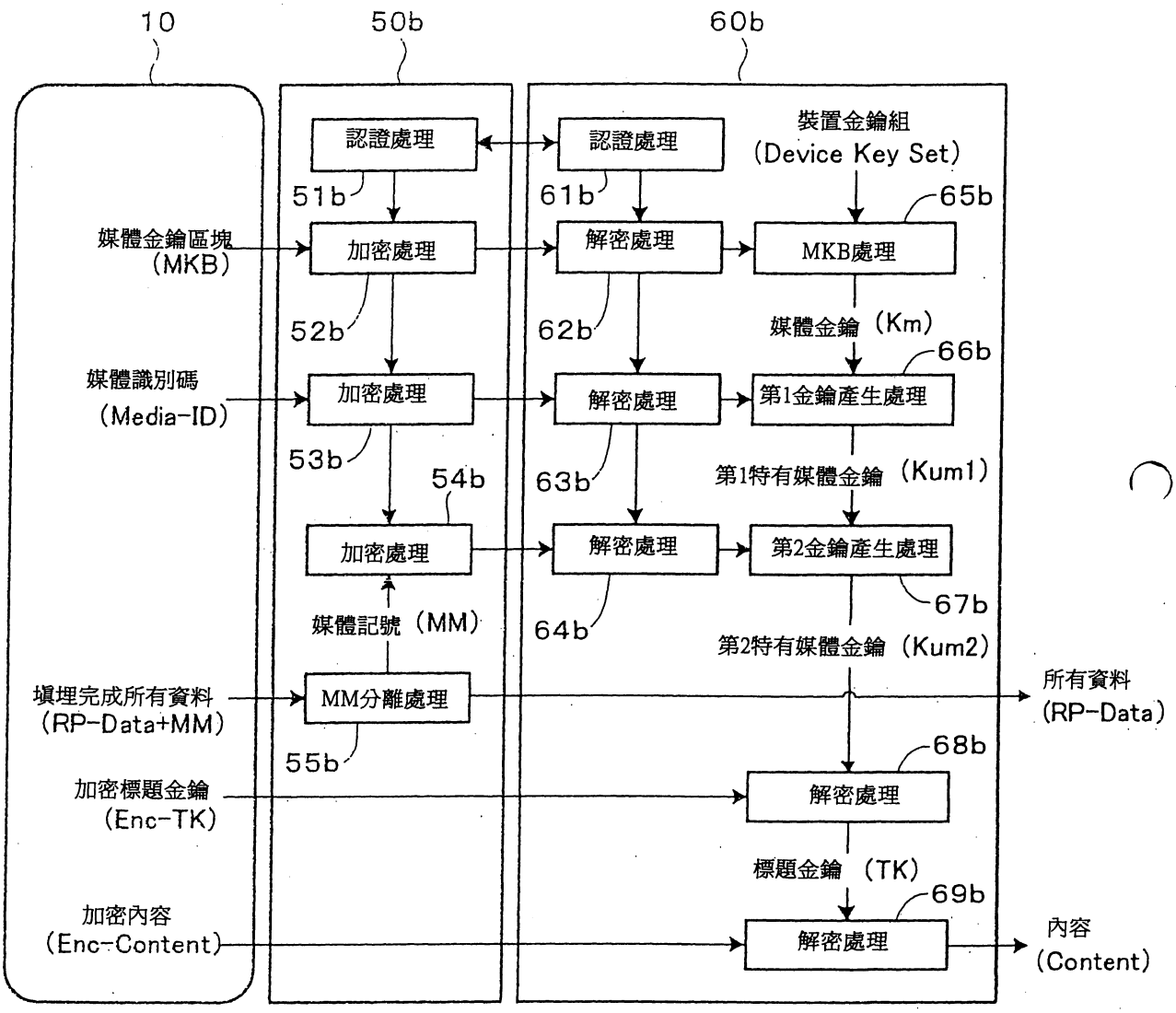
第12圖


30
10a
CP管理機構
裝置金鑰群
(Device Key Group)
31
媒體金鑰 (Km)
MKB產生處理
媒體金鑰區塊
(MKB)
媒體識別碼
(Media-ID)
媒體識別碼
(Media-ID)
40b
所有資料
(RP-Data)
MM填埋處理
填埋完成所有資料
(RP-Data+MM)
43
媒體記號
(MM)

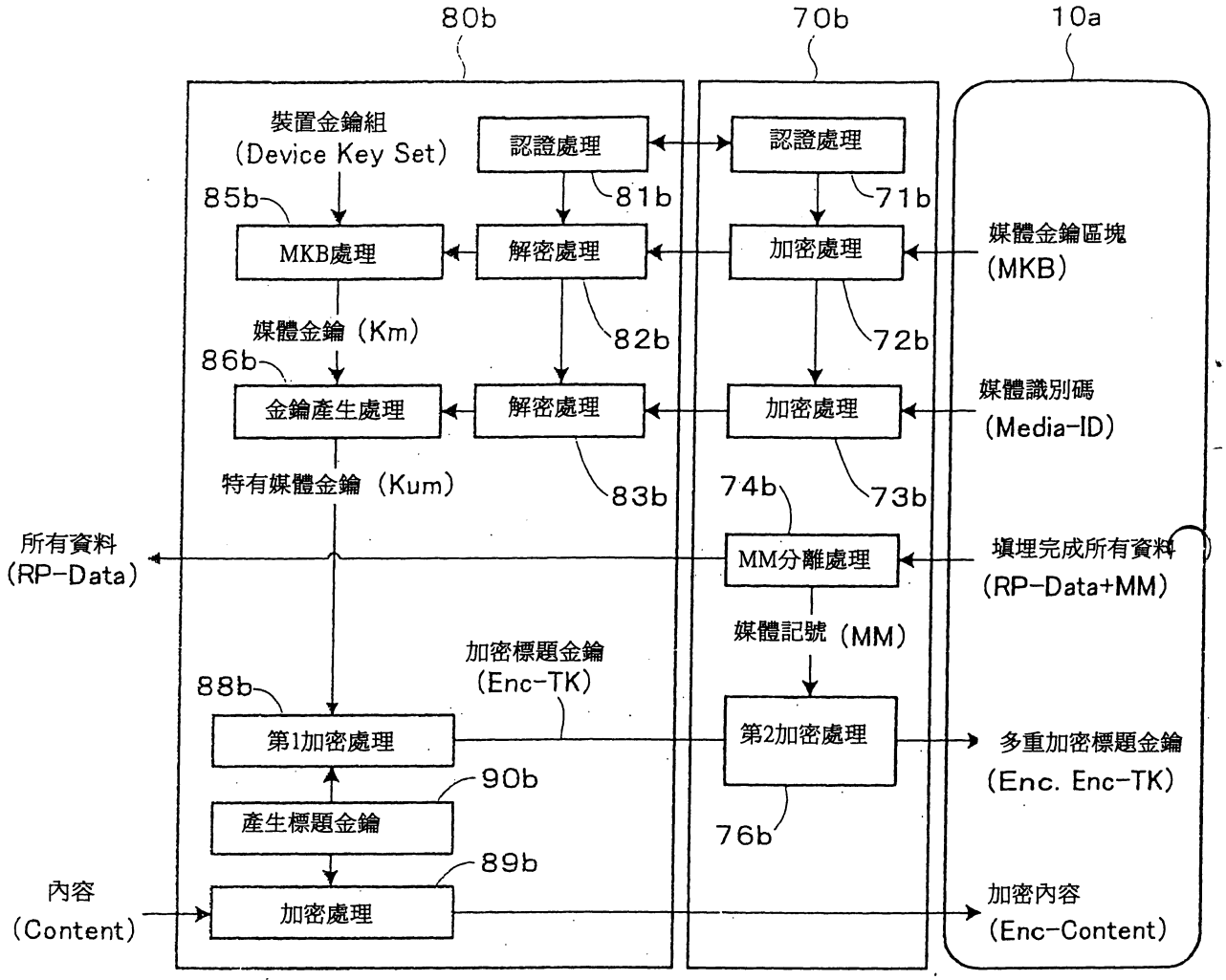
第13圖


80a
70a
10a
裝置金鑰組
(Device Key Set)
認證處理
認證處理
81a
71a
85a
MKB處理
解密處理
加密處理
媒體金鑰區塊
(MKB)
媒體金鑰 (Km)
82a
72a
86a
第1金鑰產生處理
解密處理
加密處理
媒體識別碼
(Media-ID)
第1特有媒體金鑰 (Kum1)
83a
74a
73a
第2金鑰產生處理
解密處理
加密處理
87a
84a
媒體記號 (MM)
第2特有媒體金鑰 (Kum2)
所有資料
(RP-Data)
MM分離處理
填埋完成所有資料
(RP-Data+MM)
75a
88a
解密處理
加密標題金鑰
(Enc-TK)
90a
產生標題金鑰
89a
內容
(Content)
加密處理
加密內容
(Enc-Content)

第14圖

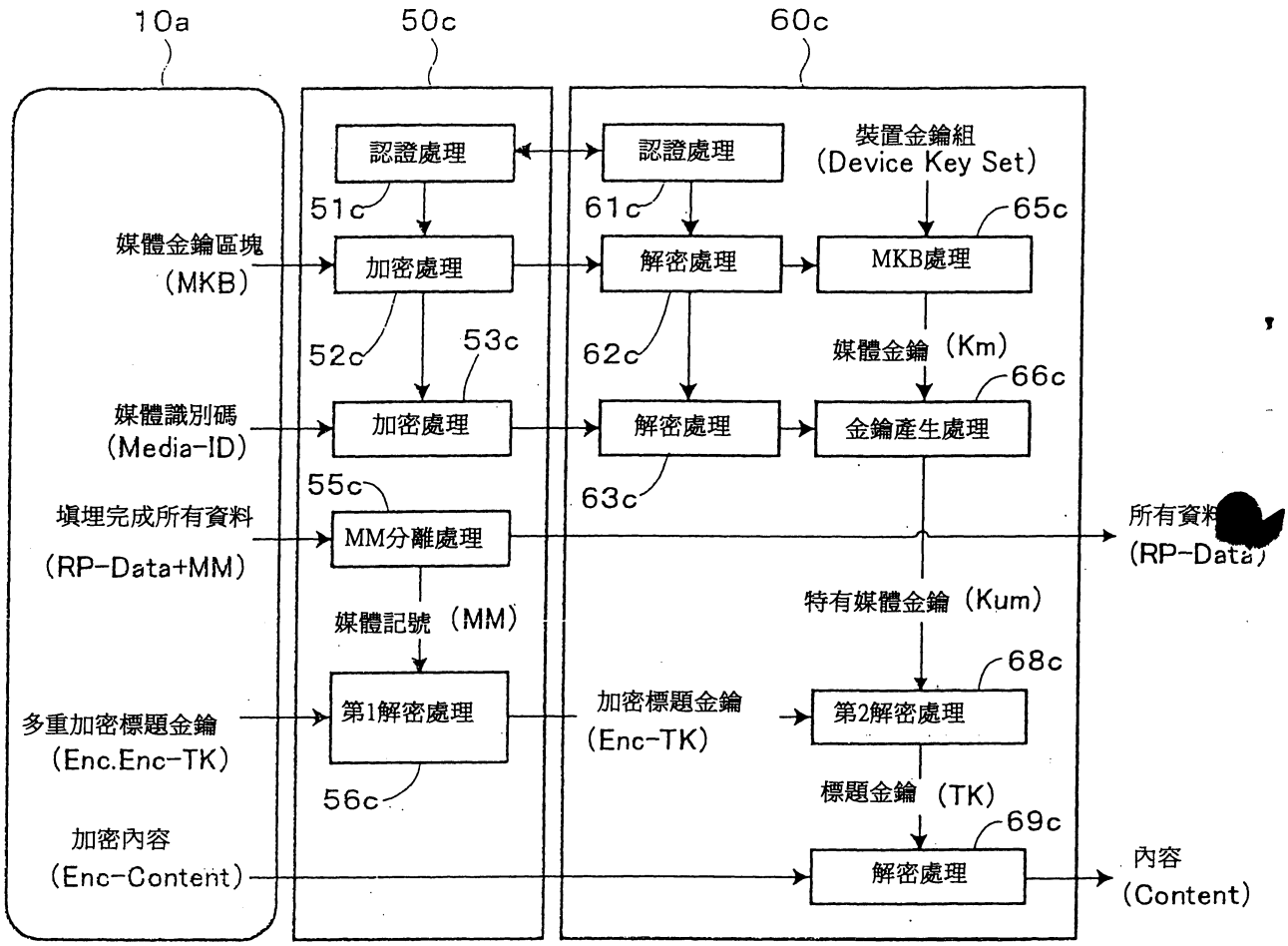

10
50b
60b
認證處理
認證處理
裝置金鑰組
(Device Key Set)
51b
61b
65b
媒體金鑰區塊
(MKB)
加密處理
解密處理
MKB處理
52b
62b
媒體金鑰 (Km)
66b
媒體識別碼
(Media-ID)
加密處理
解密處理
第1金鑰產生處理
53b
63b
第1特有媒體金鑰 (Kum1)
54b
加密處理
解密處理
第2金鑰產生處理
67b
媒體記號 (MM)
64b
第2特有媒體金鑰 (Kum2)
填埋完成所有資料
(RP-Data+MM)
MM分離處理
所有資料
(RP-Data)
55b
68b
加密標題金鑰
(Enc-TK)
解密處理
標題金鑰 (TK)
69b
加密內容
(Enc-Content)
解密處理
內容
(Content)

第15圖

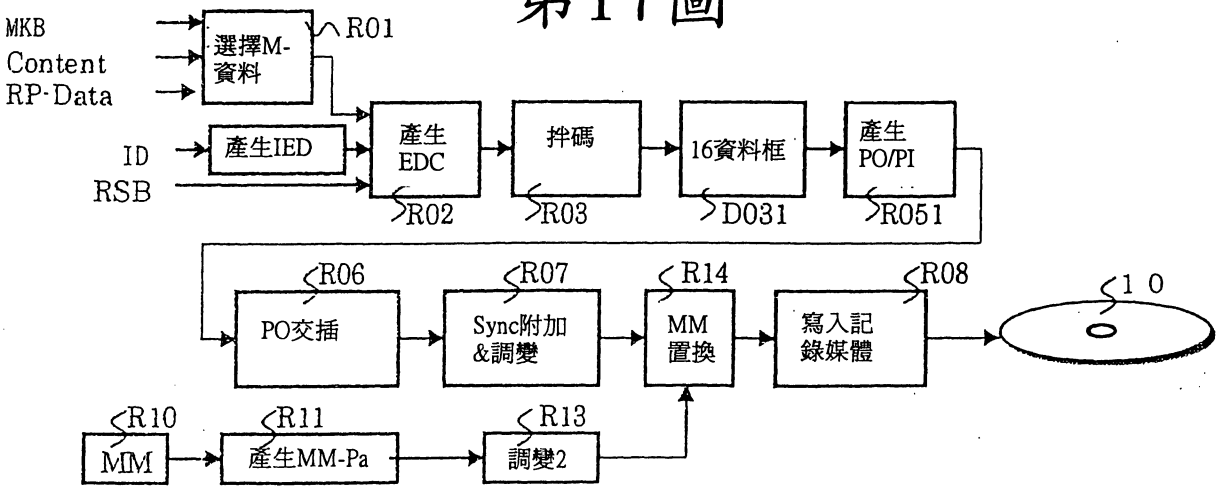

80b
70b
10a
裝置金鑰組
(Device Key Set)
認證處理
認證處理
85b
81b
71b
MKB處理
解密處理
加密處理
媒體金鑰區塊
(MKB)
媒體金鑰 (Km)
82b
72b
86b
金鑰產生處理
解密處理
加密處理
媒體識別碼
(Media-ID)
特有媒體金鑰 (Kum)
83b
74b
73b
所有資料
(RP-Data)
MM分離處理
填埋完成所有資料
(RP-Data+MM)
媒體記號 (MM)
加密標題金鑰
(Enc-TK)
88b
第1加密處理
第2加密處理
多重加密標題金鑰
(Enc. Enc-TK)
90b
產生標題金鑰
76b
89b
內容
(Content)
加密處理
加密內容
(Enc-Content)

200529196

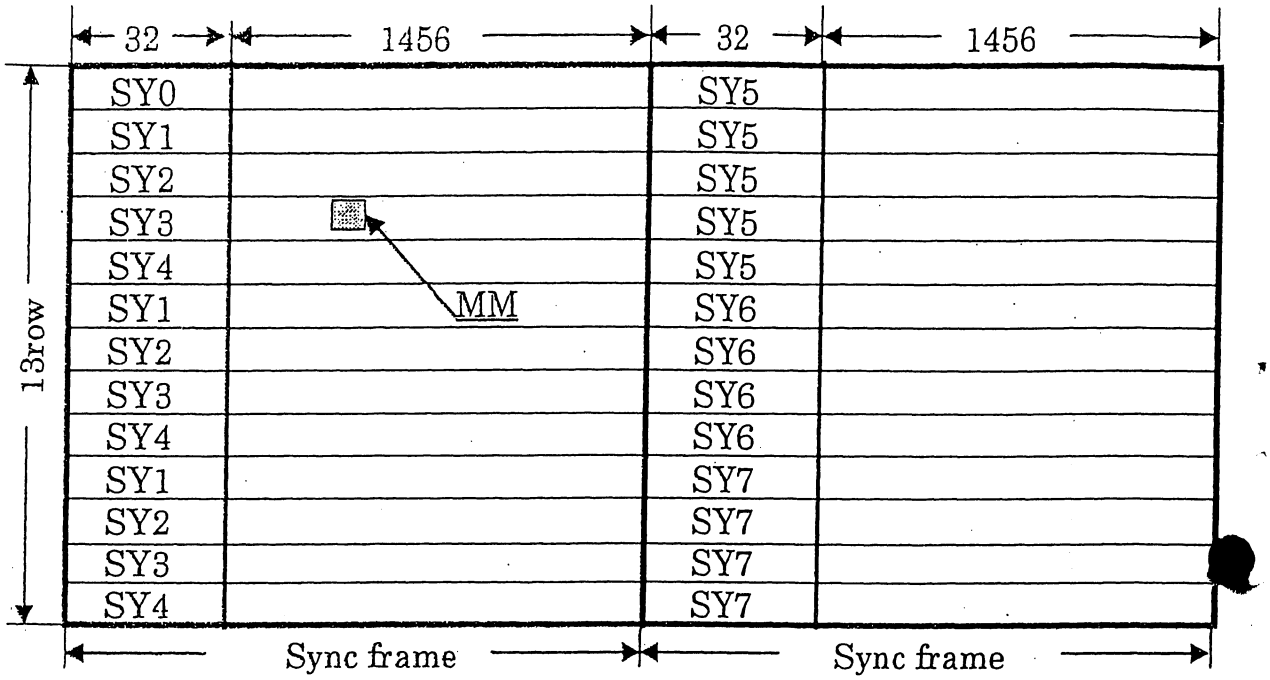
第16圖



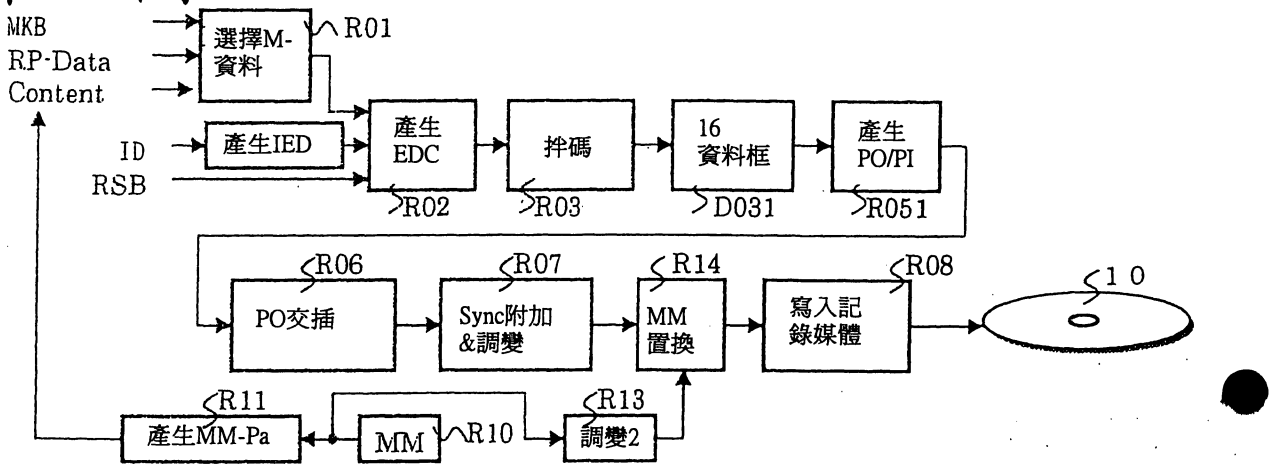
第17圖



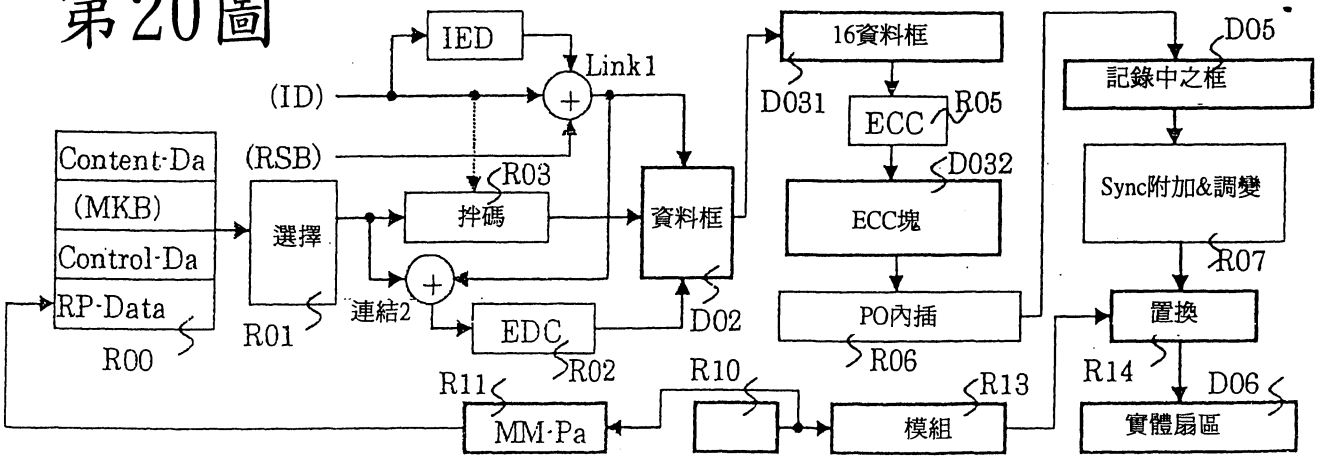
第18圖



第19圖

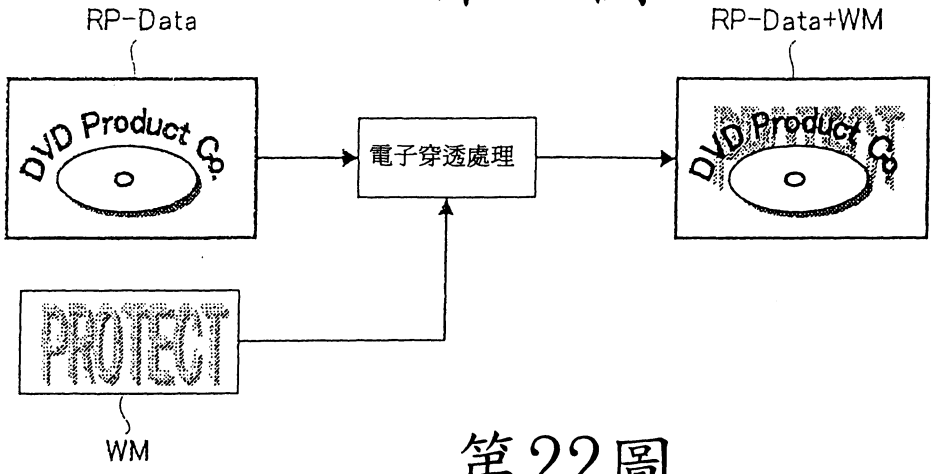


第20圖

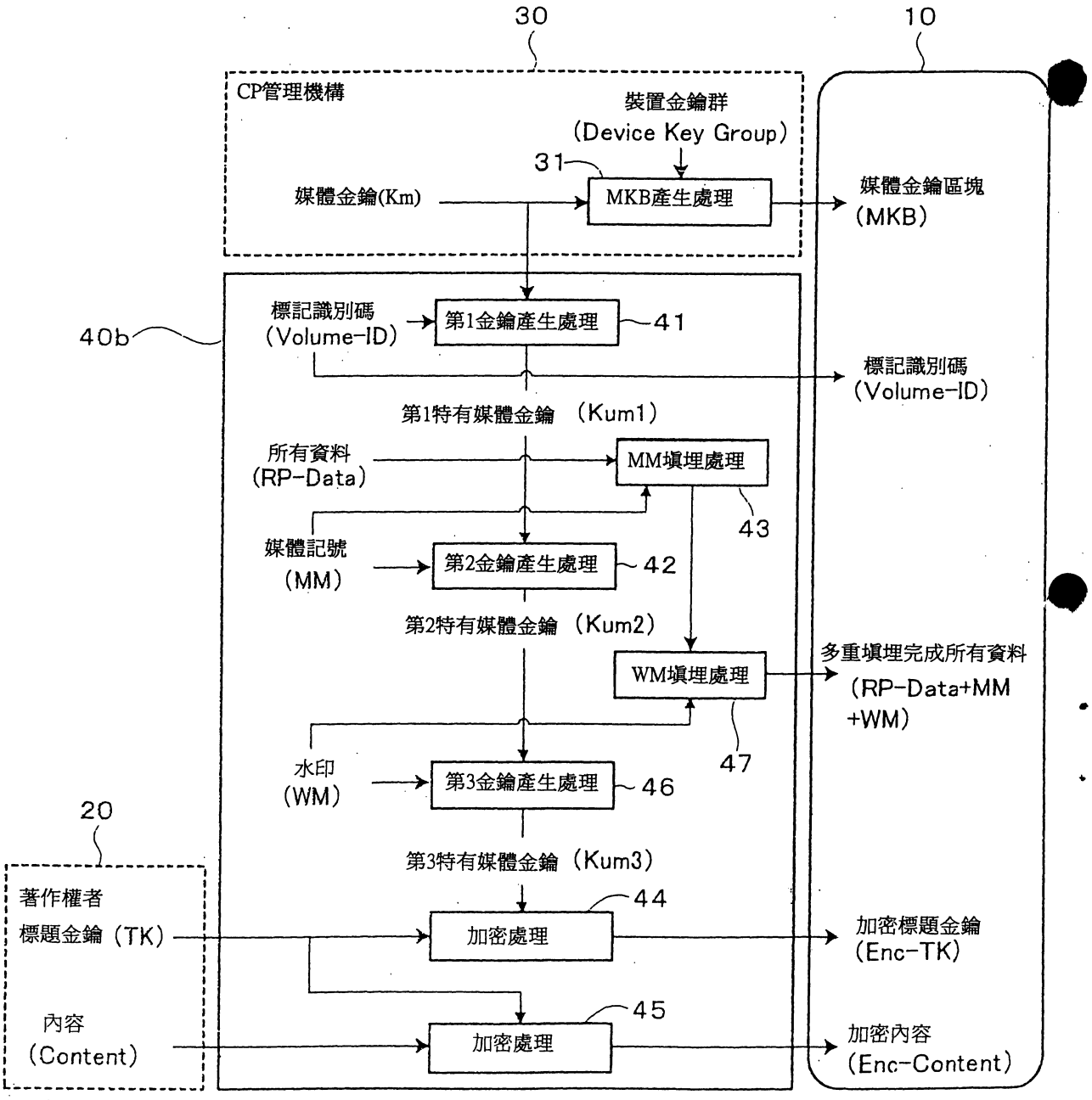


200529196

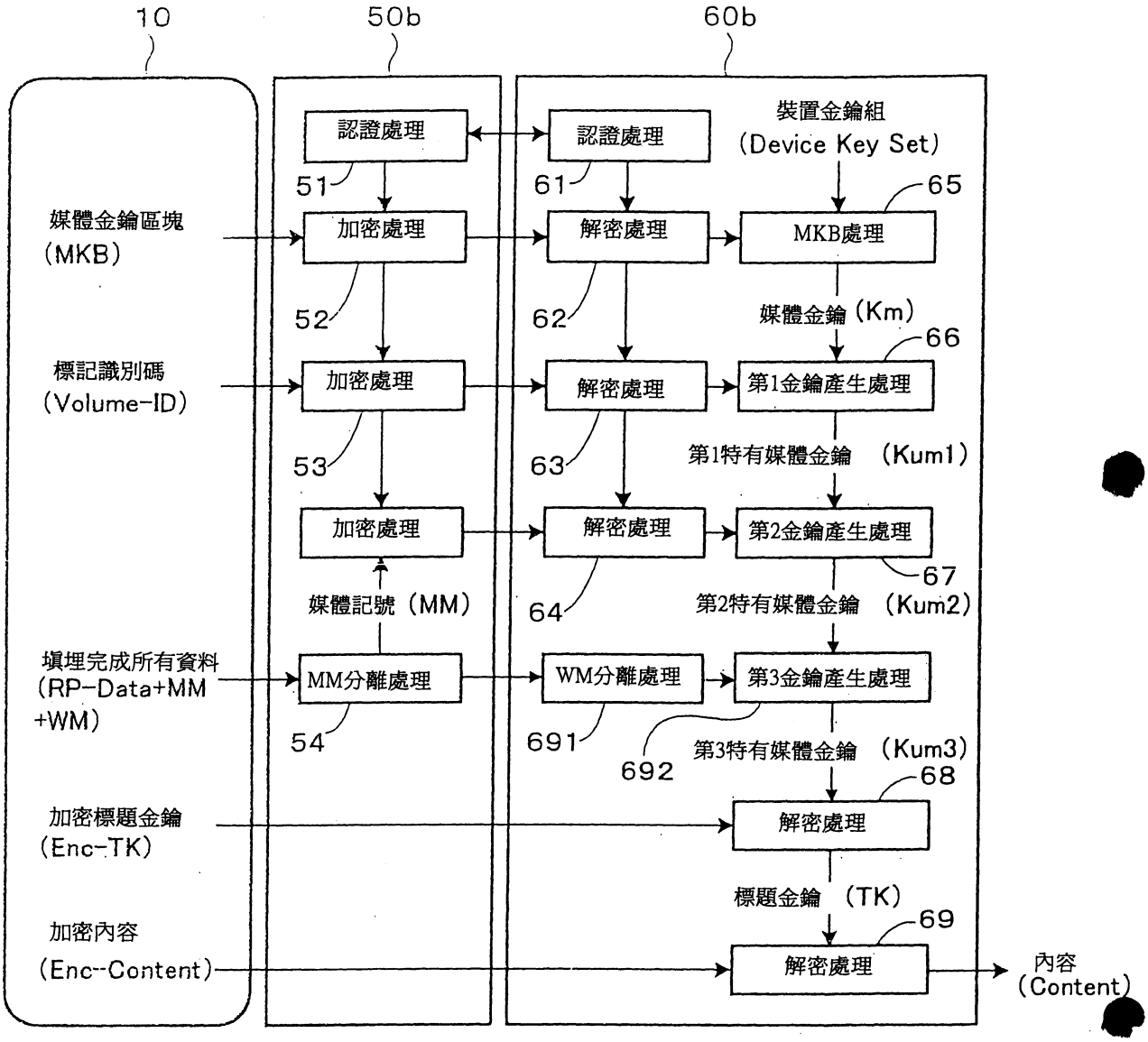
第21圖



第22圖



第23圖


10
50b
60b
認證處理
認證處理
裝置金鑰組
(Device Key Set)
51
61
65
媒體金鑰區塊
(MKB)
加密處理
解密處理
MKB處理
52
62
媒體金鑰 (Km)
66
標記識別碼
(Volume-ID)
加密處理
解密處理
第1金鑰產生處理
53
63
第1特有媒體金鑰 (Kum1)
加密處理
解密處理
第2金鑰產生處理
67
媒體記號 (MM)
64
第2特有媒體金鑰 (Kum2)
填埋完成所有資料
(RP-Data+MM
+WM)
MM分離處理
WM分離處理
第3金鑰產生處理
54
691
692
第3特有媒體金鑰 (Kum3)
68
加密標題金鑰
(Enc-TK)
解密處理
標題金鑰 (TK)
69
加密內容
(Enc-Content)
解密處理
內容
(Content)

七、指定代表圖：

（一）、本案指定代表圖為：第（1）圖

（二）、本代表圖之元件代表符號簡單說明：

10：光碟

11：內周

12：外周

13：抓持區域

14：Burst Cutting Area（叢發切割區域）

15：引入（Lead-In）區域

16：資料區域

17：引出（Lead-0UT）區域

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：