四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 日本；2004.04.02；特願 2004-110069
2. 日本；2004.05.17；特願 2004-146963
3. 日本；2004.05.21；特願 2004-151621
4. 日本；2004.06.01；特願 2004-163734
5. 日本；2004.07.02；特願 2004-196531
6. 日本；2004.07.07；特願 2004-201009
7. 日本；2004.07.13；特願 2004-206335

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

發明的技術領域

本發明係有關一種用以驗證內容之有效性的技術，且更確切來說，本發明係有關一種用以降低包含在該種驗證動作之處理負載的技術。

【先前技術】

發明的技術背景

用以避免包含非法複製、竄改、以及置換內容等欺騙行為的方法包括應用表示該等內容已由合法權所有者發佈的簽章資訊，並且與該等內容一同分散用以驗證該等內容是否包含可能受到竄改等行為之未授權內容的驗證資訊。

專利參考文案1，其為該等方法的一實例，揭露了一種藉著透過網路分散簽章資訊、驗證資訊以及內容來驗證內容有效性的技術。根據此種技術，在傳輸內容之前，將把包括傳輸來源之簽章資訊以及用以檢查構成該等內容之個別部份內容一致性之驗證資訊的鑑認資訊傳送到一執行裝置。當接收到該鑑認資訊時，執行裝置將驗證包含在其中的簽章資訊。如果驗證該簽章資訊的動作成功的話，該執行裝置將接收並且播放該等內容。與播放動作同時進行的是，該執行裝置將藉著利用該驗證資訊來重複驗證該等個別部份內容的一致性，並且當驗證動作失敗時，停止播放動作。

即使該執行裝置已接收到包括未授權內容的內容，此種

技術將令該執行裝置無法開始播放該等內容或中途停止該播放動作。

[專利參考案 1]美國專利公開案號 6480961；

[專利參考案 2]日本早期公開專利申請公開案號 2002-281013；

[非專利參考案 1] http://positron.jfet.org/dvdvideo.html (2004 年 5 月 17 日存取)

[非專利參考案 2] http://www.pioneer.co.jp/crdl/tech/mpeg/1.html (2004 年 5 月 17 日存取)；

[非專利參考案 3]由 Donald E. Knuth 所著之"電腦編程化技術第 2 集，半數字演算法"，ISBN：0-201-03822-6；以及

[非專利參考案4]由Atsuko Miyaji與Hiroaki Kikuchi二人所著而由日本資訊處理協會彙編之"Joho安全(資訊安全)"。

【發明內容】

發明的概要說明

[本發明欲解決的問題]

然而，根據上述的習知技術，執行裝置必須要持續與播放動作並行地來驗證驗證資訊，且因此在內容播放動作進行中，會產生執行裝置的處理負載問題。

再者，以安全性的觀點來看，受到分散的往往是已編碼內容，而不是一般內容。如此一來，執行裝置亦必須要並

行地進行解密處理，且因此處理負載便增加更多。

因此，執行裝置必須要配備有可運作以並行地處理該等程序的高度有效率處理器。

本發明可解決該等問題，且本發明的目的在於提供能夠達成無障礙內容播放動作的一種資料處理裝置、一種資料處理方法、一種資料處理程式，以及一種記錄媒體，其即便在所配備的處理器並不具有效率時，能在內容播放的過程中降低執行裝置的處理負載。

[用以解決問題的方法]

為了達成上述目的，本發明的資料處理裝置使用一種記錄在記錄媒體上的數位工作，該記錄媒體亦記錄有(i)從構成該數位工作之多個資料區塊產生的多個記錄摘要值；以及(ii)根據其上之某些或所有該等多個記錄摘要值而產生的記錄簽章資料。該資料處理裝置包含：一使用單元，其可運作以使用該數位工作；一選擇單元，其可運作以從該等多個資料區塊中隨機地選出一預定數量的資料區塊；一計算單元，其可運作以針對各個該等選出資料區塊計算一計算摘要值；一讀取單元，其可運作以讀取剩餘記錄摘要值，各個該等剩餘記錄摘要值對應於並未從該等多個記錄摘要值中選出資料區塊中之一；一簽章驗證單元，其可運作以藉著使用該記錄簽章資料、該等計算摘要值、以及該等剩餘記錄摘要值來驗證是否該數位工作為有效的；以及一使用控制單元，其可運作以當該簽章驗證單元判斷出該

數位工作並不有效時，使該使用單元停止使用該數位工作。

[本發明的較佳效應]

根據上述結構，本發明之資料處理裝置的選擇單元可從該等多個資料區塊中選出一預定數量的資料區塊。該計算單元從該等選出資料區塊中計算出計算摘要值，而該簽章驗證單元藉著利用該已計算計算摘要值、從該記錄媒體讀取的記錄簽章資料、以及該剩餘記錄簽章資料來驗證該數位工作的有效性。據此，可以藉著把計算摘要值限制在新計算出來的一預定數量而降低包含在驗證記錄簽章資料中的一連串處理負載。

此外，該選擇單元進行的選出動作是隨機的。因此，每當進行驗證動作時，不同的資料區塊可為驗證目標，且因此可以某種程度地補充因為把用於驗證動作之資料區塊數量限制在一預定數量中而產生驗證動作正確性下降的問題。再者，第三者難以預測欲選出的是哪些資料區塊，這可因此防止包含僅把未用於驗證之數位工作部份竄改或置換為未授權資訊的欺騙行為。

在本發明的資料處理裝置中，該等多個記錄摘要值可包括多個主要記錄摘要值，各個主要記錄摘要值係針對該等多個資料區塊之一而產生，且多個次要記錄摘要值係從該等多個主要記錄摘要值中的二或數個產生，並且可藉著對該等多個次要記錄摘要值進行數位簽章來產生記錄簽章資料。該讀取單元可從該等多個主要記錄摘要值中讀取該等

剩餘記錄摘要值。該簽章驗證單元可藉著根據該等計算摘要值以及剩餘記錄摘要值來計算一或數個次要計算摘要值來驗證該數位工作的有效性，並且藉著使用該記錄簽章資料、該等多個次要記錄摘要值、以及該等次要計算摘要值來進行一項數位簽章驗證。

根據上述結構，該等記錄摘要值包括第一記錄摘要值以及第二記錄摘要值。該簽章驗證單元根據該等計算摘要值以及剩餘記錄摘要值來計算一或數個第二計算摘要值。因此，該讀取單元僅讀取用以計算該等第二計算摘要值所需的該等第一記錄摘要值以及未對應於該等選出資料區塊的該等第二摘要值。因此，可以降低從該記錄媒體讀取的記錄摘要值總數。

在本發明的資料處理裝置中，該數位工作可包括多個檔案，各個檔案對應於該等多個次要記錄摘要值中之一，且係由該等多個資料區塊中的二或數個構成。可藉著利用主要記錄摘要值來產生各個該等多個次要記錄摘要值，該主要記錄摘要值係一對一對應於構成對應於該等次要記錄摘要值之一檔案的該等多個資料區塊中的二或數個。該簽章驗證單元可包括：一主要讀取子單元，其可運作以從該記錄媒體讀取該記錄簽章資料；一計算子單元，其可運作以藉著使用對應於包括在該檔案中之該等未選出資料區塊的主要記錄摘要值以及對應於該等選出資料區塊的該等計算摘要值而參照包括該等選出資料區塊之至少一個的各個檔案來計算一次要計算摘要值；一次要讀取子單元，其可運

作以參照並未包括任何該等選出資料區塊的各個檔案讀取對應於該檔案的一次要記錄摘要值；一簽章子單元，其可運作以藉著使用該等計算出的次要計算摘要值以及該等已讀取次要記錄摘要值來進行該數位簽章而產生計算簽章資料；以及一比較子單元，其可運作以比較該計算簽章資料與該記錄簽章資料。當該計算簽章資料與該記錄簽章資料彼此相符時，該簽章驗證單元便驗證該數位工作為有效的，且當該計算簽章資料與該記錄簽章資料彼此並不相符時，該簽章驗證單元便判斷該數位工作並不有效。

根據上述結構，該讀取單元可針對包含該等選出資料區塊之至少一個的各個檔案來讀取對應於該檔案包含之該等未選出資料區塊的第一記錄摘要值。另一方面，該簽章驗證單元中的該第二讀取子單元將針對並不包含任何該等選出資料區塊的各個檔案從該記錄媒體讀取對應於該檔案的第二記錄摘要值。因此，可以降低從該記錄媒體讀取的摘要值總數。再者，可以藉著根據該第二記錄摘要值以及該第二計算摘要值來產生計算簽章資料並且比較已產生的計算簽章資料以及該記錄簽章資料而容易地進行驗證數位工作之有效性的動作。

在本發明的資料處理裝置中，該等多個記錄摘要值為各利用雜湊函數而產生的雜湊值。由該計算單元計算出的該等計算摘要值為藉著對各個該等選出資料區塊套用雜湊函數而計算出的雜湊值。由該計算子單元計算出的該等次要計算摘要值為藉著對對應於該等未選出資料區塊的該等主

要記錄摘要值以及該等計算摘要值套用雜湊函數而計算出的雜湊值。

根據上述結構，該等記錄摘要值係利用雜湊函數而產生。該計算單元以及該計算子單元則利用雜湊函數來計算該等計算摘要值以及該等計算摘要值。

因為雜湊函數是一種單向功能，如果用來計算對應於該等選出資料區塊之第一記錄摘要值的該等資料區塊部分地不同於該等選出資料區塊的話，該等第一記錄摘要值以及該等第一計算摘要值彼此並不相符。因此，當該等選出資料區塊已受到竄改時，該等計算摘要值以及第二計算摘要值並不與該記錄媒體上記錄的對應第一摘要值以及第二摘要值相符。藉此，可以正確地檢測出該等選出資料區塊受到竄改的狀況。

在本發明的資料處理裝置中，該數位工作可為數位內容，且該使用單元可藉著重播該數位內容來使用該數位內容。

根據上述結構，該使用控制單元將停止播放已遭到竄改的數位內容。據此，可以降低已受竄改之內容的流通性。

在本發明的資料處理裝置中，該數位工作為一種電腦程式，且該使用單元可藉著解密構成該電腦程式且根據該已解密程式碼運作的指令程式碼來使用該電腦程式。

根據上述結構，該使用控制單元將停止執行已遭到竄改的電腦程式。據此，可以避免因為執行未授權程式而造成的負面影響，例如毀壞使用者的資料以及應用不應該被使

用的資料。

除了該使用控制單元之外，本發明的資料處理裝置另包含：一警告顯示單元，其可運作以當判斷出該數位工作並不有效時顯示出該數位工作之無效性的一通知。

根據上述結構，當驗證出該數位工作不為有效時，該警告顯示單元將因此顯示出來，且該資料處理裝置能夠通知該使用者記錄在該記錄媒體的數位工作是未經授權的。藉此，該使用者便可知悉記錄在該記錄媒體的數位工作是未經授權，並且套用保護措施，例如從該時點起不把該記錄媒體載入到該資料處理裝置上。因此，可以避免因為使用該數位工作而造成的負面影響。

在本發明的資料處理裝置中，該記錄媒體已另記錄有(i)具有已調整資料大小的填充內容，以使該記錄媒體上閒置空間的容量成為一預定值或較低；以及(ii)根據該數位工作與該等填充內容的部分或全部而產生的簽章資料。該資料處理裝置另包含：一驗證單元，其可運作以藉著使用該數位工作、該等填充內容與該簽章資料來驗證該數位工作與該等填充內容為有效的。該使用控制單元可運作以當該驗證單元判斷出該數位工作與該等填充內容中至少一個並不有效時，使該使用單元停止使用該數位工作。

根據上述結構，該等填充內容係記錄在該記錄媒體中。如果該閒置空間容量為一預定值的話，其夠小或者甚至小於該預定值，一未授權第三者便無法把未授權資訊加入到該記錄媒體中。再者，該資料處理裝置不只驗證該數位工

作的有效性，同時也驗證該填充內容的有效性。因此，即使該填充內容的部分或全部遭到竄改，該資料處理裝置可停止使用該數位工作。因此，就算是利用此種方式來分散未授權資訊，亦可避免使用未授權資訊。

在本發明的資料處理裝置中，該記錄媒體已另記錄有(i)指出一外部裝置得到允許可存取該記錄媒體上之一存取允許區域的區域資訊；以及(ii)根據該數位工作與該區域資訊的部分或全部而產生的簽章資料。該資料處理裝置可另包含：一存取禁止單元，其可運作以根據該區域資訊禁止存取該存取允許區域之外的區域；以及一驗證單元，其可運作以藉著利用該數位工作、該區域資訊與該簽章資料來驗證是否該數位工作與該區域資訊為有效的。該使用控制單元可運作以當該驗證單元判斷出該數位工作與該區域資訊中至少一個並不有效時，使該使用單元停止使用該數位工作。

大致上來說，除了數位工作之外，在記錄媒體中有時亦包括顯示出用以使用該數工作之程序的程序檔案。根據上述結構，該資料處理裝置並不存取除了該區域資訊所指示之該存取允許區域之外的區域。

因此，即使一未授權第三者已把未授權資訊加入到該記錄媒體的閒置空間中，且已進一步竄改該程序檔案以便使用該未授權資訊，該資料處理裝置並不會讀取該未授權資訊。

此外，因為該簽章資料係根據該數位工作以及該區域資

訊而產生，該使用控制單元能夠停止使用該數位工作，即使是未授權人士已竄改該區域資訊。因此，可以避免使用該未授權資訊。

在此，本發明申請專利範圍中的資料處理裝置為下列實施例中的一種執行裝置。本發明申請專利範圍中的該等資料區塊對應於第一、第五以及第六實施例中的已加密單元，並且對應於第二至第四實施例中的部份內容。

圖式簡要說明

第 1 圖為一結構圖，其展示出第一實施例中一種未授權內容檢測系統的結構；

第 2 圖為一方塊圖，其展示出第一實施例中一種分散裝置 1100 的結構；

第 3 圖展示出欲輸入到分散裝置 1100 之內容 1120 的結構；

第 4 圖展示出由執行裝置資訊儲存單元 1104 儲存之裝置識別表 1130 的結構；

第 5 圖展示出由金鑰區塊產生單元 1103 產生之金鑰區塊 1150 的細節；

第 6 圖展示出由單元產生單元 1105 進行之分離內容產生程序的大致概要；

第 7 圖展示出由單元產生單元 1105 產生之單元檢選資訊 1200 的結構；

第 8 圖展示出由加密處理單元 1106 進行之加密處理動作的部分；

第 9 圖展示出加密處理單元 1106 產生之已加密內容 1330 的結構；

第 10 圖展示出由頭標資訊產生單元 1107 進行之頭標資訊 1260 產生程序的大致概要；

第 11 圖展示出由頭標資訊產生單元 1107 進行的第一雜湊表產生程序；

第 12 圖展示出由頭標資訊產生單元 1107 產生之第二雜湊表的細節；

第 13 圖展示出由簽章資訊產生單元 1111 進行的處理動作；

第 14 圖展示出由第一實施例中的 DVD 1500 儲存的資訊；

第 15 圖為一方塊圖，其展示出第一實施例中一種執行裝置 1600 的結構；

第 16 圖展示出由簽章資訊驗證單元 1611 進行之簽章資訊驗證處理動作的大致概要；

第 17 圖展示出由簽章資訊驗證單元 1611 進行之處理動作的部分；

第 18 圖展示出由簽章資訊驗證單元 1611 進行之第一已置換雜湊表的產生程序；

第 19 圖展示出由簽章資訊驗證單元 1611 進行之第二已置換雜湊表的產生程序；

第 20 圖展示出由簽章資訊驗證單元 1611 進行的簽章資訊驗證動作；

第 21 圖為一流程圖，其展示出分散裝置 1100 的運作性行為；

第 22 圖為一流程圖，其展示出分散裝置 1100 的運作性行為(續接第 21 圖)；

第 23 圖展示出由執行裝置 1600 進行的簽章資訊驗證程序；

第 24 圖為一流程圖，其展示出執行裝置 1600 的運作性行為；

第 25 圖為一流程圖，其展示出執行裝置 1600 的運作性行為(續接第 24 圖)；

第 26 圖為一方塊圖，其根據第一實施例的修改方案展示出執行裝置 1100b 的結構；

第 27 圖為一方塊圖，其根據第二實施例展示出一種分散裝置 2100 的結構；

第 28 圖展示出內容 2120 以及欲輸入到分散裝置 2100 中的識別資訊部分；

第 29 圖展示出由選擇單元 2105 進行之處理動作的大致概要；

第 30 圖展示出由頭標資訊產生單元 2107 產生之選擇位置資訊 2160 的結構；

第 31 圖展示出由頭標資訊產生單元 2107 產生之頭標資訊 2200 的結構；

第 32 圖展示出由加密處理單元 2109 產生之已加密內容的結構；

第 33 圖展示出記錄在第二實施例中之 DVD 2500 上的資訊；

第 34 圖為一方塊圖，其展示出第二實施例中一種執行裝置 2600 的結構；

第 35 圖為一流程圖，其展示出分散裝置 2100 的運作性行為；

第 36 圖為一流程圖，其展示出執行裝置 2600 的運作性行為；

第 37 圖為一方塊圖，其展示出第三實施例中一種分散裝置 3100 的結構；

第 38 圖展示出由頭標資訊產生單元 3107 產生之頭標選擇資訊 3130 的結構；

第 39 圖展示出記錄在第三實施例中之 DVD 3500 上的資訊；

第 40 圖為一方塊圖，其展示出第三實施例中一種執行裝置 3600 的結構；

第 41 圖為一方塊圖，其展示出第四實施例中一種分散裝置 4100 的結構；

第 42 圖展示出由部份內容產生單元 4105 產生的分離內容以及識別資訊部分；

第 43 圖展示出由頭標資訊產生單元 4107 產生之內容位置資訊 4140 的結構；

第 44 圖展示出由頭標資訊產生單元 4107 產生之頭標資訊 4160 的結構；

第 45 圖展示出記錄在第四實施例中之 DVD 4500 上的資訊；

第 46 圖為一方塊圖，其展示出第四實施例中一種執行裝置 4600 的結構；

第 47 圖展示出由選擇單元 4611 進行之選擇位置資訊 4620 產生程序的大致概要；

第 48 圖展示出由選擇單元 4611 進行之選出頭標資訊 4630 產生程序的大致概要；

第 49 圖展示出由部份內容解密單元 4616 進行之解密處理動作的大致概要；

第 50 圖為一流程圖，其展示出分散裝置 4100 的運作性行為；

第 51 圖展示出由分散裝置 4100 進行之簽章資訊 4170 的產生程序；

第 52 圖為一流程圖，其展示出執行裝置 4600 的運作性行為；

第 53 圖為一流程圖，其展示出執行裝置 4600 的運作性行為(續接第 52 圖)；

第 54 圖展示出由執行裝置 4600 進行之簽章資訊以及頭標資訊的驗證程序；

第 55 圖為一方塊圖，其展示出第五實施例中一種分散裝置 5100 的結構；

第 56 圖展示出由填充內容產生單元 5108 產生之分離填充內容 5120 的結構；

第 57 圖展示出從填充內容產生單元 5108 輸出之單元檢選資訊 5140 的結構；

第 58 圖展示出由頭標資訊產生單元 5107 進行之頭標資訊 5109 產生程序的大致概要；

第 59 圖展示出由頭標資訊產生單元 5107 產生之第二雜湊表 5180 的結構；

第 60 圖展示出記錄在第五實施例中之 DVD 5500 上的資訊；

第 61 圖為一方塊圖，其展示出第五實施例中一種執行裝置 5600 的結構；

第 62 圖為一流程圖，其展示出分散裝置 5100 的運作性行為；

第 63 圖為一流程圖，其展示出分散裝置 5100 的運作性行為(續接第 62 圖)；

第 64 圖為一流程圖，其展示出執行裝置 5600 的運作性行為；

第 65 圖展示出一種想像未授權 DVD 5500b；

第 66 圖展示出一種想像未授權 DVD 5500c；

第 67 圖為一方塊圖，其展示出第六實施例中一種分散裝置 6100 的結構；

第 68 圖展示出由配置產生單元 6108 產生之寫入配置資訊 6120；

第 69 圖展示出記錄在第六實施例中之 DVD 6500 上的資訊；

第 70 圖為一方塊圖，其展示出第六實施例中一種執行裝置 6600 的結構；以及

第71圖展示出DVD 1500的組態以及取得單元1601的結構。

【實施方式】

較佳實施例的詳細說明

1.第一實施例

以下將藉由圖式的輔助把未授權內容檢測系統 1 解說為本發明實施例的一實例。

1.1 未授權內容檢測系統 1

如第 1 圖所示，未授權內容檢測系統 1 包含分散裝置 1100、執行裝置 1600 以及監視器 1620。

舉例來說，分散裝置 1100 為包括視訊以及音訊內容之合法著作權所有者擁有的裝置。根據操作者進行的運作，分散裝置 1100 將取得內容，並且藉著加密取得內容來產生已加密內容。此外，分散裝置 1100 將藉著利用該內容而產生各種不同類型的資訊。例如，由分散裝置 1100 產生的資訊包括在執行裝置 1600 中用來驗證是否未授權內容包括在該內容中的頭標資訊。再者，分散裝置 1100 將藉著使用其本身特定的一簽章金鑰來產生簽章資訊，並且把所產生的已加密內容、簽章資訊、頭標資訊等寫入到 DVD(數位多功能碟片)1500 中。

將透過分散通路把該 DVD 1500 販售或分散給使用者。

當載入 DVD 1500 時，執行裝置 1600 將從已載入 DVD 1500 讀取簽章資訊、頭標資訊等、進行讀取簽章資訊的驗證動作，並且根據從 DVD 1500 讀取的資訊來驗證是否包括未授權內容。

只有在驗證簽章資訊的動作成功時，執行裝置 1600 將開始播放內容。

以下將詳細說明包含未授權內容檢測系統 1 以及 DVD 1500 的個別裝置。

1.2 分散裝置 1100

如第 2 圖所示，分散裝置 1100 包含輸入單元 1101、內容金鑰產生單元 1102、金鑰區塊產生單元 1103、執行裝置資訊儲存單元 1104、單元產生單元 1105、加密處理單元 1106、頭標資訊產生單元 1107、簽章資訊產生單元 1111、簽章金鑰儲存單元 1112 以及記錄單元 1114。

1.2.1 輸入單元 1101

輸入單元 1101 將根據操作者的運作接收來自外部裝置或外部記錄媒體的內容。在此將藉著第 3 圖的輔助來說明輸入單元 1101 接收到的內容結構。

如第 3 圖所示，輸入單元 1101 所接收的內容 1120 係由 c 個檔案"CNT1"1121、"CNT2"1122、"CNT3"1123 至"CNTc"1124 組成(c 為整數 1 或者更大)。在此，輸入單元 1101 取得的內容 1120 為執行裝置 1600 可播放的格式

(如以下將詳細說明地)，且 DVD-視訊格式以及 MPEG-2(移動圖象專家組格式 2)格式為該等可播放格式的實例。本實施例係假設內容 1120 為 DVD-視訊格式且各個該等檔案為一 VOB(視訊物件)檔案來進行說明。

當取得內容 1120 時，輸入單元 1101 將指示內容金鑰產生單元 1102 要產生內容金鑰，並且輸出已取得內容 1120 到單元產生單元 1105。

1.2.2 內容金鑰產生單元 1102

輸入單元 1101 將指示內容金鑰產生單元 1102 要產生該內容金鑰。響應於該指令，內容金鑰產生單元 1102 將產生一擬隨機數，且隨後藉著使用已產生的擬隨機數來產生一個 128 位元長度的內容金鑰"CK"。並非為一個擬隨機數，可例如藉著使用信號中的雜音來產生一真實隨機數。非專利參考案 3 提供了一種用以產生隨機數之方法的相關細節。此外，可使用一種不同方法來產生該內容金鑰。

隨後，內容金鑰產生單元 1102 將輸出已產生的內容金鑰"CK"到金鑰區塊產生單元 1103 以及加密處理單元 1106。

1.2.3 金鑰區塊產生單元 1103 以及執行裝置資訊儲存單元 1104

例如，執行裝置資訊儲存單元 1104 係由 ROM 或 EEPROM 組成，並且如第 4 圖所示地儲存裝置識別表 1130。

裝置識別表 1130 係由 n 個裝置識別符以及 n 個裝置金

鑰(n 為一自然數)組成。該等裝置識別符為識別資訊的部分，而各個部分對允許讀取分散裝置 1100 寫入到 DVD 1500 上的資訊並且播放已讀取資訊的裝置來說為特定的。一對一的對應於該等裝置識別符的該等裝置金鑰為對應裝置識別符表示之個別裝置的分別特定金鑰資訊部分。例如，裝置識別符"AID_1"1131 對應於裝置金鑰"DK_1"1136。

金鑰區塊產生單元 1103 將接收來自內容金鑰產生單元 1102 的內容金鑰"CK"，並且產生一金鑰區塊。

第 5 圖展示出在此時點中產生的金鑰區塊 1150 結構實例。金鑰區塊 1150 係由 n 個裝置識別符以及 n 個已加密內容金鑰組成。該等裝置識別符與包括在裝置識別表 1130 中的該等裝置識別符相同。該等裝置識別符係一對一的對應於已加密內容金鑰，且該等已加密內容金鑰係藉著使用對應裝置金鑰而對內容金鑰"CK"套用加密演算法 E1 來產生。例如，裝置識別符"AID_1"1141 與包含在裝置識別表 1130 中的裝置識別符"AID_1"1131 相同，且對應於已加密內容金鑰"Enc(DK_1、CK)"1142。已加密內容金鑰"Enc(DK_1、CK)"1142 係利用包括在裝置識別表 1130 中的裝置金鑰"DK_1"1136 來加密內容金鑰"CK"而產生。在以下的說明中，藉著使用金鑰 A 來加密一純文本(plain text)B 而產生的已加密文本係表示為"Enc(A、B)"。

接下來將說明一種用以產生金鑰區塊 1150 的程序。

當接收到內容金鑰"CK"時，金鑰區塊產生單元 1103 將

從執行裝置資訊儲存單元 1104 的裝置識別表 1130 中讀取位於第一行中的裝置識別符"AID_1"1131 以及裝置金鑰"DK_1"1136。金鑰區塊產生單元 1103 將藉著使用讀取裝置金鑰"DK_1"1136 而對內容金鑰"CK"套用加密演算法 E1 來產生已加密內容金鑰"Enc(DK_1、CK)"。在此，將使用 AES(高階加密標準)作為加密演算法 E1 的一實例。非專利參考案 4 提供了有關 AES 的細節。要注意的是，本文中使用的加密系統並不限於 AES，且亦可使用一種不同的系統。

金鑰區塊產生單元 1103 將儲存讀取裝置識別符"AID_1"1131 以及已產生的已加密內容金鑰"Enc(DK_1、CK)"，並且把該等二者連結在一起。

金鑰區塊產生單元 1103 將針對所有 n 對的裝置識別符以及裝置金鑰重複進行相同類型的處理動作、產生 n 對的裝置識別符以及已加密內容金鑰，並且把該等識別符放置在一起以形成金鑰區塊 1150。

隨後，金鑰區塊產生單元 1103 將把已產生的金鑰區塊 1150 輸出到記錄單元 1114。

在此，舉最簡單的實例來說，將說明針對可運作以播放寫入到 DVD 1500 之資訊的各個裝置分派的一特定金鑰。然而，專利參考 2 中揭露的技術包括用以降低已加密內容金鑰數量的技術以及用以避免特定裝置播放該等內容的技術。

1.2.4 單元產生單元 1105

單元產生單元 1105 將接收來自輸入單元 1102 的內容 1120。當接收到內容 1120 時，單元產生單元 1105 將在下列的一程序中產生分離內容以及單元檢選資訊。

以下將說明的是：分離內容產生動作(a)；以及單元檢選資訊產生動作(b)。

(a)分離內容產生

如第 6 圖所示，單元產生單元 1105 將從內容 1120 中產生分離內容 1160。以下將藉由第 6 圖的輔助來說明一種用以產生分離內容 1160 的程序。

當接收到內容 1120 時，單元產生單元 1105 將產生檔案識別符"FID1"1161 以及對應於已接收內容 1120 中包括之檔案"CNT1"1121 的一份檔案識別資訊"AD1"。檔案識別符"FID1"1161 為獨特地指出檔案"CNT1"1121 的識別資訊，且為指出內容 1120 中檔案"CNT1"1121 順序或者該檔案名稱的一自然數。該檔案識別資訊"AD1"為用以識別檔案"CNT1"1121 的資訊，且為內容 1120 標題的一差距值、一區段編號、或一位址。

接下來，單元產生單元 1105 將針對各個 VOBU(視訊物件單元)來劃分檔案"CNT1"1121 以產生 m 個單元"U1_1"、"U1_2"至"U1_m"(m 為任何自然數)。隨後，單元產生單元 1105 將產生指出已產生單元數量的一單元編號"N1"(在此，N1=m)。

接下來，單元產生單元 1105 將產生由檔案識別符

"FID1"1161、檔案識別資訊"AD1"、以及單元編號"N1"組成的檔案資訊，並且儲存已產生的檔案資訊。

隨後，單元產生單元 1105 將針對該等個別單元產生單元識別符。該等單元識別符為各獨特地識別出 m 個單元中之一的識別資訊、可例如為從標題單元開始的序數，例如 1、2、3 以及 m，且可為標題單元的位元累積數。在本實施例中，將假設單元識別符為從該標題單元開始的序數。在下列的說明中，一對對應單元識別符以及一單元係被稱為一份單元資訊，而 m 個單元資訊則整體地被稱為一分離檔案。因此，如第 6 圖所示，從檔案"CNT1"1121 產生的分離檔案"splCNT1"1171 係由 m 個單元資訊 1191、1192、1193 以及 1194 組成。各個單元資訊係由一對應單元識別符以及一單元組成。舉一實例來說，一個單元資訊 1191 包括一單元識別符"UID1_1"1181 以及一單元"U1_1"1186。

接下來，單元產生單元 1105 將產生包括檔案識別符"FID1"1161 以及分離檔案"splCNT1"1171 的分離檔案資訊 1176。

單元產生單元 1105 將針對所有檔案重複進行相同類型的處理動作，以產生 c 個檔案資訊以及 c 個分離檔案資訊 1176、1177、1178 以及 1179。在此，所產生的 c 個分離檔案資訊係整體地被稱為分離內容 1160。要注意的是，已產生單元的數量 m 可因著檔案而不同。

接下來，單元產生單元 1105 將把已產生分離內容 1160 輸出到加密處理單元 1106。

在此，要注意的是，單元產生單元 1105 係產生檔案識別符以及檔案識別資訊，然而，該等物件可隨著內容 1120 一同從外部輸入。

此外，係針對各個 VOBU 來劃分該等個別檔案，然而該分離單元並不限於此。例如，可依據每個千位元組劃分各個該等檔案，或者依據對應於二分之一播放時間的每個部分。替代地，可設計為令操作者能輸入指出該分離單元的資訊。

(b)單元檢選資訊產生

在完成輸出分離內容 1160 的動作之後，單元產生單元 1105 將產生由 c 個檔案資訊組成的單元檢選資訊。第 7 圖展示出在此時點中產生之單元檢選資訊 1200 的結構。

單元檢選資訊 1200 由 c 個檔案資訊 1201、1202 至 1204 組成。各個檔案資訊係由一檔案識別符、一檔案識別資訊以及一單元編號組成。

舉例來說，一檔案資訊 1201 包括一檔案識別符"FID1"1211、一檔案識別資訊"AD1"1216、以及一單元編號"N1"1221。

單元產生單元 1105 將輸出已產生單元檢選資訊 1200 到簽章資訊產生單元 1111 以及記錄單元 1114。

1.2.5 加密處理單元 1106

加密處理單元 1106 將接收來自內容金鑰產生單元

1102 的內容金鑰"CK"，並且接收來自單元產生單元 1105 的分離內容 1160。

第 8 圖展示出加密處理單元 1106 進行的處理動作部分。以下將藉由第 8 圖的輔助來說明加密處理單元 1106 進行的處理動作。

當接收到分離內容 1160 時，加密處理單元 1106 將選出包含在組成已接收分離內容 1160 之分離檔案資訊 1176 中的分離檔案"splCNT1"1171。加密處理單元 1106 將從選出分離檔案"splCNT1"1171 之單元資訊 1191 的標題部分摘取出單元"U1_1"，並且藉著使用內容金鑰"CK"對該已摘取單元"U1_1"1186 套用加密演算法 E1 來產生已加密單元"EU1_1"1231。在此，EU1_1=Enc(CK、U1_1)。

加密處理單元 1106 將產生由包括在單元資訊 1191 中的已產生已加密單元"EU1_1"1231 以及單元識別符"UID1_1"組成的已加密單元資訊 1241。在以下的說明中，一對對應單元識別符以及已加密單元係稱為一份已加密單元資訊。

加密處理單元 1106 將針對單元資訊 1192、1193 以及 1194 的剩餘部份重複進行相同類型的處理動作，以產生對應的已加密單元資訊 1242、1243 以及 1244。在此，從一分離檔案產生的 m 個已加密單元資訊係整體地稱為一已加密分離檔案。

如第 8 圖所示，在上述程序中從分離檔案"splCNT1"1171 產生的已加密分離檔案"EsplCNT1"1251 係

由 m 個已加密單元資訊 1241、1242、1243 以及 1244 組成。各個已加密單元資訊係根據組成分離檔案 1171 的單元資訊而產生，且包括一單元識別符以及一已加密單元。例如，已加密單元資訊 1241 係根據單元資訊 1191 而產生，且包括單元識別符"UID1_1"1181 以及已加密單元"EU1_1"1231。

接下來，加密處理單元 1106 將從組成已產生已加密分離檔案"EsplCNT1"1251 的各個已加密單元資訊中摘取出一已加密單元。在此，m 個已摘取已加密單元係整體地稱為一已加密檔案"ECNT1"。

隨後，加密處理單元 1106 將藉著把包括在分離檔案資訊 1176 中的分離檔案"splCNT1"1171 置換為已產生已加密分離檔案"EsplCNT1"1251 來產生已加密分離檔案資訊。

加密處理單元 1106 將對分離檔案資訊 1177、1178 以及 1179 進行相同動作以產生已加密分離檔案資訊以及已加密檔案。

在此時點產生的 c 個已加密分離檔案資訊係整體地稱為一已加密分離內容。隨後，加密處理單元 1106 將輸出該已產生已加密分離內容到頭標資訊產生單元 1107。第 10 圖展示出在此輸出之已加密分離內容 1210 的結構。

接下來，加密處理單元 1106 將把 c 個已加密檔案作為已加密內容輸出到記錄單元 1114。第 9 圖展示出在此時點產生的已加密內容 1330 結構。已加密內容 1330 係由 c 個已加密檔案"ECNT1"1331、"ECNT2"1332、"ECNT3"1333

以及"ECNTc"1334 組成。各個該等已加密檔案係根據已加密分離內容中包含的已加密分離檔案而產生，且包括多個已加密單元。舉一實例來說，該已加密檔案"ECNT1"1331包括已加密單元"EU1_1"、"EU1_2"等等。

1.2.6 頭標資訊產生單元 1107

頭標資訊產生單元 1107 將從加密處理單元 1106 接收到已加密分離內容 1210。當接收到已加密分離內容 1210 時，頭標資訊產生單元 1107 將藉著使用接收到的已加密分離內容來產生頭標資訊 1260，如第 10 圖所示。

第 10 圖展示出由頭標資訊產生單元 1107 進行之頭標資訊 1260 產生程序的大致概要。頭標資訊產生單元 1107 接收到的已加密分離內容 1210 係由 C 個已加密分離檔案資訊 1246、1247、1248 以及 1249 組成。各個已加密分離檔案資訊包括一檔案識別符以及一已加密分離檔案。例如，一已加密分離檔案資訊 1246 包括一檔案識別符"FID1"1161 以及一已加密分離檔案"EsplCNT1"1251。

頭標資訊產生單元 1107 將根據已加密分離檔案資訊 1246 中包括的各個分離檔案來產生第一雜湊表。例如，頭標資訊產生單元 1107 將根據已加密分離檔案"EsplCNT1"1251 來產生第一雜湊表"HA1TBL1"1261。頭標資訊產生單元 1107 將從已產生的 C 個第一雜湊表來產生第二雜湊表"HA2TBL"1269。

以下將詳細地說明上述第一以及第二雜湊表的產生程

序。

1.2.6.1 第一雜湊表產生

第 11 圖展示出由頭標資訊產生單元 1107 進行的第一雜湊表"HA1TBL1"1261 產生程序的大致概要。

以下將藉由第 11 圖的輔助來說明第一雜湊表"HA1TBL1"1261 的產生程序。所有第一雜湊表"HA1TBL2"、"HA1TBL3"以及"HA1TBLc"的產生程序與第一雜湊表"HA1TBL1"1261 的產生程序相同。

首先，頭標資訊產生單元 1107 將從組成已加密分離檔案"EsplCNT1"1251 的標題已加密單元資訊 1241 摘取出一已加密單元"EU1_1"1231，並且藉著把已摘取已加密單元"EU1_1"1231 指派給一雜湊函數來產生一單元雜湊值"UHA1_1"1271。

在此，將針對該雜湊函數套用利用區塊密碼的 SHA-1(安全雜湊演算法-1)或 CBC-MAC(密碼區塊鏈-訊息鑑認程式碼)。

在此，頭標資訊產生單元 1107 將藉著把已加密單元資訊 1241 的已加密單元"EU1_1"1231 置換為已產生單元雜湊值"UHA1_1"1271 來產生單元雜湊資訊 1281。

頭標資訊產生單元 1107 將針對已加密單元資訊 1242、1243 以及 1244 的剩餘部份重複進行相同類型的處理動作，以產生對應的單元雜湊資訊 1282、1283 以及 1284。在此時點產生的 m 個單元雜湊資訊係整體地稱為第

一雜湊表"HA1TBL1"1261。第 11 圖展示出在此時點中產生之第一雜湊表"HA1TBL1"1261 的結構。

1.2.6.2 第二雜湊表產生

頭標資訊產生單元 1107 將重複上述程序。在完成從已加密分離內容 1210 產生 c 個第一雜湊表的動作之後，頭標資訊產生單元 1107 將從該等已產生的 c 個第一雜湊表產生第二雜湊表 1269，如第 12 圖所示。第二雜湊表"HA2TBL"1269 係由 c 個檔案雜湊資訊 1301、1302、1303 以及 1304 組成，且各個檔案雜湊資訊包括一檔案識別符以及一檔案雜湊值。舉一實例來說，一檔案雜湊資訊 1301 包括檔案識別符"FID1"1161 以及一檔案雜湊值"FHA1"1291。

以下將說明第二雜湊表 1269 的產生程序。

頭標資訊產生單元 1107 將藉著對該雜湊函數分派由組成已產生第一雜湊表"HA1TBL1"1261 之所有單元識別符以及單元雜湊值結合而形成的一項已合併結果來產生檔案雜湊值"FHA1"1291。

隨後，頭標資訊產生單元 1107 將從對應於第一雜湊表"HA1TBL1"1261 的已加密分離檔案資訊 1246 中摘取出檔案識別符"FID1"1161，並且產生由已摘取檔案識別符"FID1"1161 以及已產生檔案雜湊值"FHA1"1291 組成的檔案雜湊資訊 1301。

頭標資訊產生單元 1107 將針對第一雜湊表 1262、1263

以及 1264 重複進行相同類型的處理動作，以分別地產生檔案雜湊資訊 1302、1303 以及 1304。

接下來，頭標資訊產生單元 1107 將把該等已產生的 c 個第一檔案雜湊資訊湊在一起以形成第二雜湊表"HA2TBL"1269。

於此得到了第一雜湊表(1.2.6.1)以及第二雜湊表(1.2.6.2)產生程序的結論。頭標資訊產生單元 1107 將產生在上述程序中產生而包括 c 個第一雜湊表以及單一個第二雜湊表"HA2TBL"1269 的頭標資訊 1260，並且把已產生頭標資訊 1260 輸出到記錄單元 1114。

再者，頭標資訊產生單元 1107 將把已產生第二雜湊表"HA2TBL"1269 輸出到簽章資訊產生單元 1111。

1.2.7 簽章資訊產生單元 1111 以及簽章金鑰儲存單元 1112

由 ROM 組成的簽章金鑰儲存單元 1112 將儲存分散裝置 1100 特定的一簽章金鑰 1113。

第 13 圖展示出簽章資訊產生單元 1111 之運作性行為的大致概要。以下將藉由第 13 圖的輔助來說明簽章資訊產生單元 1111 進行的簽章資訊產生動作。

簽章資訊產生單元 1111 將從單元產生單元 1105 接收單元檢選資訊 1200，而從頭標資訊產生單元 1107 接收第二雜湊表"HA2TBL"1269。當接收到單元檢選資訊 1200 以及第二雜湊表 1269 時，簽章資訊產生單元 1111 將從簽章金鑰儲存單元 1112 讀取簽章金鑰 1113。

隨後，簽章資訊產生單元 1111 將藉著使用讀取簽章金鑰 1113 而從已接收單元檢選資訊 1200 以及第二雜湊表 1269 產生簽章資訊 1310。更確切來說，藉著使用讀取簽章金鑰 1113，簽章資訊產生單元 1111 將對藉著合併包括在已接收第二雜湊表 1269 中的 c 個檔案雜湊值以及包含在單元檢選資訊 1200 中的 c 個檔案資訊而得到的一已合併結果套用簽章產生演算法 S。

舉一實例來說，DSA(數位簽章演算法)係用於簽章產生演算法 S。

隨後，簽章資訊產生單元 1111 將把已產生簽章資訊 1310 輸出到記錄單元 1114。

1.2.8 記錄單元 1114

將把記錄單元 1114 載入到 DVD 1500 中。

記錄單元 1114 將接收來自金鑰區塊產生單元 1103 的金鑰區塊 1150、來自單元產生單元 1105 的單元檢選資訊 1200、來自加密處理單元 1106 的已加密內容 1330、來自頭標資訊產生單元 1107 的頭標資訊 1260、以及來自簽章資訊產生單元 1111 的簽章資訊 1310。

當接收到上述資訊時，記錄單元 1114 將把已接收金鑰區塊 1150、單元檢選資訊 1200、頭標資訊 1260、簽章資訊 1310 以及已加密內容 1330 寫入到 DVD 1500 中。

1.3 DVD 1500

DVD 1500 為載入到執行裝置 1600 上的一種可攜帶式光碟媒體。

如第 14 圖所示，DVD 1500 儲存金鑰區塊 1510、單元檢選資訊 1530、頭標資訊 1550、簽章資訊 1570、以及已加密內容 1580。該等項目係由分散裝置 1100 寫入，且分別地與分散裝置 1100 產生的金鑰區塊 1150、單元檢選資訊 1200、頭標資訊 1260、簽章資訊 1310、以及已加密內容 1330 相同。因此，僅針對該等項目進行簡單的說明。

1.3.1 金鑰區塊 1510

金鑰區塊 1510 係由 n 個裝置識別符"AID_1"、"AID_2"、"AID_3"、與"AID_n"以及分別地對應於該等 n 個裝置識別符的 n 個已加密內容金鑰"Enc(DK_1、CK)"、"Enc(DK_2、CK)"、"Enc(DK_3、CK)"與"Enc(DK_n、CK)"組成。

1.3.2 單元檢選資訊 1530

單元檢選資訊 1530 係由 c 個檔案資訊 1541、1542 等組成，且各個檔案資訊包括一檔案識別符、檔案識別資訊、以及一單元編號。個別檔案資訊對應於包括在已加密內容 1580 中的已加密檔案。此外，各個該等檔案對應於包括在頭標資訊 1550 中的第一雜湊表。

1.3.3 已加密內容 1580

已加密內容 1580 係由 C 個已加密檔案 1581、1582、1583 至 1587 組成。各個該等已加密檔案包括多個已加密單元。

1.3.4 頭標資訊 1550

頭標資訊 1550 係由 C 個第一雜湊表 1551、1552 至 1557 以及第二雜湊表 1556 組成。

各個該等第一雜湊表係由多個單元雜湊資訊組成，且各個單元雜湊資訊包括一單元識別符以及一單元雜湊值。

第二雜湊表 1556 係由 C 個檔案雜湊資訊 1561、1562、1563 至 1567 組成，且各個檔案雜湊資訊包括一檔案識別符以及一檔案雜湊值。

1.3.5 簽章資訊 1570

將藉著對合併包括在第二雜湊表 1556 中的 C 個檔案雜湊值以及包括在單元檢選資訊 1530 中的 C 個檔案資訊所得的一已合併結果套用簽章產生演算法 S 來產生簽章資訊 1570。

1.4 執行裝置 1600

如第 15 圖所示，執行裝置 1600 係由取得單元 1601、內容金鑰取得單元 1602、裝置金鑰儲存單元 1604、執行單元 1606、簽章資訊驗證單元 1611、以及驗證金鑰儲存單元 1612 組成。

1.4.1 取得單元 1601

將把取得單元 1601 載入到 DVD 1500 中。當檢測到已經載入到 DVD 1500 中時，取得單元 1601 將從 DVD 1500 讀取金鑰區塊 1510、單元檢選資訊 1530 以及簽章資訊 1570，並且輸出已讀取金鑰區塊 1510 到內容金鑰取得單元 1602，而同時輸出已讀取單元檢選資訊 1530 以及簽章資訊 1570 到簽章資訊驗證單元 1611。

此外，取得單元 1601 將根據來自執行單元 1606 以及簽章資訊驗證單元 1611 的指令從 DVD 1500 讀取頭標資訊 1550 以及已加密內容 1580 的全部或部分。

1.4.2 內容金鑰取得單元 1602 以及裝置金鑰儲存單元 1604

由 ROM 組成的裝置金鑰儲存單元 1604 將儲存一裝置識別符"AID_p"1608 以及一裝置金鑰"DK_p"1609(p 為 n 或者較小數字的一自然數)，如第 15 圖所示。

裝置識別符"AID_p"1608 為獨特地指出執行裝置 1600 的識別資訊，而裝置金鑰"DK_p"1609 為執行裝置 1600 特定的金鑰資訊。

內容金鑰取得單元 1602 將從取得單元 1601 接收金鑰區塊 1510。當接收到金鑰區塊 1510 時，內容金鑰取得單元 1602 將從裝置金鑰儲存單元 1604 讀取裝置識別符"AID_p"1608。隨後，內容金鑰取得單元 1602 將檢測對應於從已接收金鑰區塊 1510 讀取之裝置識別

符"AID_p"1608 的一裝置識別符，並且摘取出對應於已檢測裝置識別符的一已加密內容金鑰。

隨後，內容金鑰取得單元 1602 將從裝置金鑰儲存單元 1604 讀取裝置金鑰"DK_p"1609。內容金鑰取得單元 1602 將藉著使用讀取裝置金鑰"DK_p"1609 而對已摘取的已加密內容金鑰套用解密演算法 D1 來產生內容金鑰"CK"，並且隨後輸出已產生內容金鑰"CK"到執行單元 1606。

在此，解密演算法 D1 為一種用以解密針對利用加密演算法 E1 而產生之已加密文本的演算法。

1.4.3 簽章資訊驗證單元 1611 以及驗證金鑰儲存單元 1612

由 ROM 組成的驗證金鑰儲存單元 1612 將儲存驗證金鑰 1613。驗證金鑰 1613 為對應於分散裝置 1100 所儲存之簽章金鑰 1113 的金鑰資訊。

簽章資訊驗證單元 1611 將從取得單元 1601 接收單元檢選資訊 1530 以及簽章資訊 1570。

第 16 圖展示出由簽章資訊驗證單元 1611 進行之簽章資訊驗證處理動作的大致概要。當接收到單元檢選資訊 1530 以及簽章資訊 1570 時，簽章資訊驗證單元 1611 將從已接收的單元檢選資訊 1530 選出 i 個檔案識別符(i 為 c 或更小數字的一自然數)，如第 16 圖所示。在此，以下的說明係假設簽章資訊驗證單元 1611 已選出檔案識別符"FID1"1531、"FID3"1533 等。

簽章資訊驗證單元 1611 將根據對應於選出檔案識別

符"FID1"1531 的第一雜湊表"HA1TBL1"1551 以及已加密檔案 "ECNT1"1581 產生第一已置換雜湊表"REPHA1TBL1"1631。簽章資訊驗證單元 1611 將對其他選出檔案識別符"FID3"等進行相同動作，以產生第一已置換雜湊表 1633 等。簽章資訊驗證單元 1611 將根據儲存在 DVD 1500 中的已產生第一已置換雜湊表 1631、1633 等以及第二雜湊表"HA2TBL"1556 來產生第二已置換雜湊表"REPHA2TBL"1639，並且藉著利用已產生第二已置換雜湊表"REPHA2TBL"1639 來驗證簽章資訊 1570。

因此得到了第 16 圖展示之大致概要的結論。以下的詳細說明係藉由圖式的輔助且根據產生第一已置換雜湊表(1.4.3.1)的動作、產生第二已置換雜湊表(1.4.3.2)的動作、以及簽章資訊(1.4.3.3)的驗證程序。

1.4.3.1 產生第一已置換雜湊表的的動作

將藉由第 17 圖與第 18 圖的輔助來說明一種用以產生第一已置換雜湊表的程序。

如第 17 圖所示，簽章資訊驗證單元 1611 將從包括在已接收單元檢選資訊 1530 的 c 個檔案資訊中選出 i 個檔案資訊(i 為 c 或更小數字的一自然數)。如何選出 i 個檔案資訊的方式為例如產生 i 個擬隨機數(r1、r2、至 ri)，其各為 1 或較大數字但為 c 或較小，且選出 r1st、r2nd 至檔案識別符。此選擇方法並不限於此，且任何方法均適用，只要難以預測哪些檔案識別符為選出識別符即可。例如，可使

用電子信號的溫度、溼度、噪音等。

在本實施例中，以下的說明係根據 i=7 且選出 7 個檔案資訊 1541、1543 等的假設而進行。

隨後，簽章資訊驗證單元 1611 將選出對應於包括在選出檔案資訊 1541 中檔案識別符"FID1"的已加密檔案"ECNT1"1581 中任何一個已加密單元，並且從 DVD 1500 讀取所選出已加密單元，如第 18 圖所示。更確切來說，簽章資訊驗證單元 1611 將讀取包括在選出檔案資訊 1541 中的單元編號"N1"，並且產生一擬隨機數 t (在此，t=3)，其為"N1"或較小。隨後，簽章資訊驗證單元 1611 將透過取得單元 1601 且根據包括在選出檔案資訊 1541 中的檔案識別資訊"AD1"從 DVD 1500 讀取已加密單元"EU1_3"，其為已加密檔案"ENCT1"1581 中的第三已加密單元。

接下來，簽章資訊驗證單元 1611 將藉著對一雜湊函數分派讀取已加密單元"EU1_3"來產生一置換單元雜湊值"H3"。在此，簽章資訊驗證單元 1611 將使用分散裝置 1100 之頭標資訊產生單元 1107 所使用的相同雜湊函數。

接下來，簽章資訊驗證單元 1611 將透過取得單元 1601 讀取包括在頭標資訊 1550 中的第一雜湊表"HA1TBL1"1551。

隨後，簽章資訊驗證單元 1611 將利用從組成已讀取第一雜湊表"HA1TBL1"1551 之 m 個單元雜湊資訊計算出的置換單元雜湊值"H3"來置換單元雜湊值"UHA1_3"，其對應於符合 t=3 的單元識別符"UID1_3"。此項結果為第一已置換

雜湊表"REPHA1TBL1"1631。

簽章資訊驗證單元 1611 將針對其他選出的檔案資訊 1542 等重複進行相同類型的處理動作，以分別地產生第一已置換雜湊表"REPHATBL3"1633 等。

1.4.3.2 產生第二已置換雜湊表的動作

以下將藉由第 19 圖的輔助來說明一種用以產生第二已置換雜湊表的程序。

在完成根據該等選出的 7 個檔案資訊來產生第一已置換雜湊表之後，簽章資訊驗證單元 1611 將合併所有的單元識別符、所有的單元雜湊值、以及組成已產生第一已置換雜湊表"REPHA1TBL1"1631 的已置換雜湊值，並且藉著對雜湊函數分派該合併結果來產生一置換檔案雜湊值"fha1"。相似地，簽章資訊驗證單元 1611 將分別地根據第一已置換雜湊表"REPHA1TBL3"1633 等來產生置換檔案雜湊值"fha3"等。

接下來，簽章資訊驗證單元 1611 將從 DVD 1500 讀取包括在頭標資訊 1550 中的第二雜湊表"HA2TBL"1556。從包括在讀取第二雜湊表"HA2TBL"1556 中的 c 個檔案雜湊資訊，簽章資訊驗證單元 1611 將置換包括檔案識別符"FID1"、"FID3"等檔案雜湊資訊的檔案雜湊值，其係分別地與已產生置換檔案雜湊值"fha1"、"fha3"等一同包括在該等選出的 7 個檔案資訊中。以對其進行此種置換動作的第二雜湊表 "HA2TBL"1556 為已置換的第二雜湊

表"REPHA2TBL"1639。

1.4.3.3 簽章資訊驗證動作

以下將藉由第 20 圖的輔助來說明簽章資訊驗證動作。

在產生第二已置換雜湊表"REPHA2TBL"1639 之後，簽章資訊驗證單元 1611 將從驗證金鑰儲存單元 1612 讀取驗證金鑰 1613。

隨後，簽章資訊驗證單元 1611 將產生一項合併結果，其係藉著合併包括在第二已置換雜湊表"REPHA2TBL"1639 中的所有檔案雜湊值與置換檔案雜湊值以及包括在單元檢選資訊 1530 中的 c 個檔案資訊而形成，並且藉著使用驗證金鑰 1613 而對已產生合併結果套用簽章驗證演算法 V 來產生簽章驗證資訊。隨後，簽章資訊驗證單元 1611 將比較該已產生簽章驗證資訊以及從取得單元 1601 接收到的簽章資訊 1570。當該等資訊不相符時，簽章資訊驗證單元 1611 便判斷出此簽章驗證動作並不成功，並且輸出指出禁止進行內容播放的播放禁止資訊到執行單元 1606。在此，簽章驗證演算法 V 為一種用以驗證利用簽章產生演算法 S 產生之簽章的演算法。

當該等資訊相符時，簽章資訊驗證單元 1611 便結束驗證處理動作。

1.4.4 執行單元 1606

執行單元 1606 將接收來自內容金鑰取得單元 1602 的

內容金鑰"CK"。

此外，執行單元 1606 可接收來自簽章資訊驗證單元 1611 的播放禁止資訊。

當接收到內容金鑰"CK"時，執行單元 1606 將透過取得單元 1601 從 DVD 1500 讀取構成已加密內容 1580 的已加密檔案"ECNT1"。執行單元 1606 將藉著使用已接收的內容金鑰"CK"依序地對構成已讀取已加密檔案 1581 的已加密單元"EU1_1"、"EU1_2"等套用解密演算法 D1，以產生由單元"U1_1"、"U1_2"等構成的檔案"CNT1"。

隨後，執行單元 1606 將擴展已產生檔案"CNT1"以產生視訊與音訊資料。執行單元 1606 將根據已產生的視訊與音訊資料來產生視訊與音訊信號，並且把已產生視訊與音訊信號輸出到監視器 1620。

有關已加密檔案"ECNT2"至"ECNTc"，執行單元 1606 將重複讀出動作、解密動作、以及擴張動作，並且相似地輸出視訊以及音訊信號。

如果在重複動作中，接收到來自簽章資訊驗證單元 1611 的播放禁止資訊的話，執行單元 1606 將中止該重複動作，且通知使用者在執行裝置 1600 上播放 DVD 的不可實行性，藉著例如開啟一指示燈或者使監視器 1620 顯示出通知一項錯誤的一螢幕。

1.4.5 監視器 1620

監視器 1620 具有藉著一條電線與執行裝置 1600 連接

的一內建揚聲器。

監視器1620將從執行裝置1600的執行單元1606接收視訊與音訊信號、從已接收影像信號產生螢幕，並且顯示該等螢幕。再者，監視器1620將從音訊信號產生音訊，且從揚聲器輸出已產生的音訊。

1.5 運作性行為

以下將說明分散裝置1100以及執行裝置1600的運作性行為。

1.5.1 分散裝置1100的運作性行為

將藉由展示於第21圖與第22圖中之流程圖的輔助來說明分散裝置1100。

輸入單元1101將根據操作者進行的運作取得由c個檔案組成的內容1120(步驟S1011)，並且指示內容金鑰產生單元1102要產生內容金鑰。

內容金鑰產生單元1102將利用一隨機數來產生內容金鑰"CK"，並且輸出該已產生內容金鑰"CK"到金鑰區塊產生單元1103(步驟S1012)。

金鑰區塊產生單元1103將接收內容金鑰"CK"，並且從執行裝置資訊儲存單元1104讀取裝置識別表1130(步驟S1013)。金鑰區塊產生單元1103將產生金鑰區塊1150，利用已接收的內容金鑰"CK"以及讀取裝置識別表1130(步驟S1016)。

在步驟 S1017 至 S1023 中，分散裝置 1100 的單元產生單元 1105 將針對組成內容 1120 的各個檔案重複進行步驟 S1018 至 S1022。

單元產生單元 1105 將產生一檔案識別符以及對應於一檔案的檔案識別資訊(步驟 S1018)。隨後，單元產生單元 1105 將藉著劃分該檔案來產生 m 個單元(步驟 S1019)、產生指出該已產生單元之數量的一單元編號、並且產生由已產生檔案識別符、檔案識別資訊以及單元編號組成的檔案資訊(步驟 S1020)。

接下來，單元產生單元 1105 將產生一對一的對應於已產生單元的單元識別符(步驟 S1021)。隨後，單元產生單元 1105 將產生各包括一對應單元識別符以及一單元的 m 個單元資訊，且把該等單元資訊置放在一起以形成一分離檔案。隨後，單元產生單元 1105 將產生由分離檔案與檔案識別符組成的分離檔案資訊(步驟 S1022)。

在針對所有該等檔案重複完成步驟 S1017 至 S1023，並且產生 c 個分離檔案資訊與檔案資訊之後，單元產生單元 1105 將產生由該等 c 個檔案資訊組成的單元檢選資訊 1200(步驟 S1024)，並且輸出已產生單元檢選資訊 1200 到簽章資訊產生單元 1111 以及記錄單元 1114。此外，單元產生單元 1105 將輸出由該等 c 個分離檔案資訊組成的分離內容 1160 到加密處理單元 1106。

加密處理單元 1106 將從單元產生單元 1105 接收分離內容 1160，並且藉著使用內容金鑰"CK"加密組成已接收分

離內容 1160 之個別分離檔案的各個單元來產生已加密分離內容 1210(步驟 S1026)。

接下來，加密處理單元 1106 將藉著從各個已加密分離檔案中摘取出已加密單元來產生 c 個已加密檔案，並且把該等已加密檔案結合在一起以形成已加密內容 1330(步驟 S1027)。接下來，加密處理單元 1106 將對頭標資訊產生單元 1107 輸出已加密分離內容 1210，而同時對記錄單元 1114 輸出已加密內容 1330。

頭標資訊產生單元 1107 將從加密處理單元 1106 接收已加密分離內容 1210。頭標資訊產生單元 1107 將藉著對雜湊函數分派組成已加密分離內容 1210 之各個已加密分離檔案中包括的已加密單元來計算單元雜湊值，並且產生 c 個第一雜湊表(步驟 S1028)。

接下來，頭標資訊產生單元 1107 將針對各個該等第一雜湊表且根據該第一雜湊表來計算一檔案雜湊值，並且產生包括 c 個已計算檔案雜湊值的第二雜湊表 1269(步驟 S1029)。

接下來，頭標資訊產生單元 1107 將產生包括已產生第二雜湊表 1269 以及該等 c 個第一雜湊表的頭標資訊 1260(步驟 S1031)。

簽章資訊產生單元 1111 將從簽章金鑰儲存單元 1112 讀取簽章金鑰 1113(步驟 S1032)，並且藉著使用讀取簽章金鑰 1113 而對第二雜湊表 1269 以及單元檢選資訊套用簽章產生演算法來產生簽章資訊(步驟 S1033)。

記錄單元 1114 將把金鑰區塊 1150、單元資訊 1200、頭標資訊 1260、簽章資訊 1310 以及已加密內容 1330 寫入到 DVD 1500 中(步驟 S1034)。

1.5.2 執行裝置 1600 的運作性行為

第 23 圖展示出一種包含在驗證簽章資訊之資訊組建的程序。為了方便說明，針對頭標資訊 1550，僅在圖中說明包括在第一雜湊表中的單元雜湊值以及包括在第二雜湊表中的檔案雜湊值。第 24 圖以及第 25 圖為展示出執行裝置 1600 之運作性行為的流程圖。要注意的是，第 23 圖至第 25 圖中的相同步驟編號係表示相同的處理動作。

以下將藉由第 23 圖至第 25 圖的輔助來說明執行裝置 1600 的運作性行為。

當載入到 DVD 1500 中時，取得單元 1601 將從 DVD 1500 讀取金鑰區塊 1510、單元檢選資訊 1530 以及簽章資訊 1570，並且輸出金鑰區塊 1510 到內容金鑰取得單元 1602 而同時輸出單元檢選資訊 1530 以及簽章資訊 1570 到簽章資訊驗證單元 1611(步驟 S1041)。

簽章資訊驗證單元 1611 將接收單元檢選資訊 1530 以及簽章資訊 1570，並且藉著使用一隨機數來從包括在單元檢選資訊 1530 中的 c 個檔案識別符選出 i 個檔案識別符(步驟 S1046)。

在步驟 S1047 至 S1057，簽章資訊驗證單元 1611 將針對各個該等選出的 i 個檔案識別符重複進行步驟 S1048 至

S1056，以產生 i 個第一已置換雜湊表。

簽章資訊驗證單元 1611 將從單元資訊中摘取出對應於該等選出檔案識別符中之一的一單元編號(步驟 S1048)。隨後，簽章資訊驗證單元 1611 將產生一隨機數 t(步驟 S1049)，t 為 1 或較大但為該讀取單元編號或較小。簽章資訊驗證單元 1611 將從單元資訊中摘取出對應於選出檔案識別符的一檔案識別資訊，並且根據已摘取單元識別資訊從 DVD 1500 讀取對應於選出檔案識別符之已加密檔案中的第 t 個已加密單元(步驟 S1051)。在第 23 圖中，每當重複上述處理動作時，簽章資訊驗證單元 1161 將依序地讀取：包括在已加密檔案 1581 中的已加密單元 1511、包括在已加密檔案 1583 中的已加密單元 1512、以及包括在已加密檔案 1587 中的已加密單元 1513 等等。

簽章資訊驗證單元 1611 將藉著對雜湊函數分派所讀取的已加密單元來計算置換單元雜湊值(步驟 S1052)。

接下來，簽章資訊驗證單元 1611 將從 DVD 1500 讀取對應於選出檔案識別符的第一雜湊表(步驟 S1054)，並且藉著以已計算置換單元雜湊值置換對應於已計算置換單元雜湊值的一單元雜湊值來產生第一已置換雜湊表(步驟 S1056)。在第 23 圖中，每當重複上述處理動作時，簽章資訊驗證單元 1611 將從已加密單元 1511 以及第一雜湊表 1551 產生第一已置換雜湊表 1631、從已加密單元 1512 以及第一雜湊表 1553 產生第一已置換雜湊表 1633、以及從已加密單元 1513 以及第一雜湊表 1557 產生第一已置換雜

湊表 1637 等。

在針對所有該等 i 個檔案識別符完成重複步驟 S1047 至 S1057 的動作後，簽章資訊驗證單元 1611 將藉著個別地對雜湊函數分派第一已置換雜湊表來計算 i 個置換檔案雜湊值(步驟 S1059)。

接下來，簽章資訊驗證單元 1611 將從 DVD 1500 讀取第二雜湊表 1556(步驟 S1061)，並且藉著以已計算 i 個置換檔案雜湊值來置換對應選出 i 個檔案識別符的檔案雜湊值來產生產生第二已置換雜湊表 1639(步驟 S1063)。在第 23 圖中，已產生第二已置換雜湊表 1639 包括：從第一已置換雜湊表 1631 計算出的一置換檔案雜湊值 1641、從 DVD 1500 讀取的一檔案雜湊值 1572、從第一已置換雜湊表 1633 計算出的一置換檔案雜湊值 1643、以及從第一已置換雜湊表 1637 計算出的一置換檔案雜湊值 1647 等。

接下來，簽章資訊驗證單元 1611 將從驗證金鑰儲存單元 1612 讀取驗證金鑰 1613(步驟 S1064)，並且藉著利用單元檢選資訊 1530、已產生第二已置換雜湊表、以及讀取驗證金鑰 1613 來進行簽章資訊 1570 的驗證動作(步驟 S1066)。

當簽章資訊的驗證動作成功時(步驟 S1067：是)，簽章資訊驗證單元 1611 將隨後結束簽章資訊 1570 的驗證動作。

如果簽章驗證動作不成功的話(步驟 S1067：否)，簽章資訊驗證單元 1611 將對執行單元 1606 輸出播放禁止資訊

(步驟 S1073)。

內容金鑰取得單元 1602 將接收金鑰區塊 1510，並且從裝置金鑰儲存單元 1604 讀取裝置識別符 1608 以及裝置金鑰 1609(步驟 S1071)。隨後，內容金鑰取得單元 1602 將從讀取裝置識別符 1608、裝置金鑰 1609 以及金鑰區塊 1510 產生內容金鑰"CK"，並且輸出已產生內容金鑰"CK"到執行單元 1606(步驟 S1072)。

執行單元 1606 將接收內容金鑰"CK"。在此，如果已從簽章資訊驗證單元 1611 接收到播放禁止資訊的話(步驟 S1074：是)，執行單元 1606 將通知使用者播放儲存在 DVD 1500 上之內容的不可實行性(步驟 S1076)，並且結束播放動作。

如果並未接收到播放禁止資訊的話(步驟 S1074：否)，執行單元 1606 將從 DVD 1500 讀取組成已加密內容 1580 的已加密檔案(步驟 S1077)。執行單元 1606 將首先藉著使用內容金鑰"CK"解密已讀取已加密檔案來產生檔案(步驟 S1079)，並且隨後藉著擴展已產生檔案來產生視訊與音訊資料(步驟 S1081)。隨後，執行單元 1606 將分別地從已產生視訊與音訊資料產生視訊與音訊信號、輸出該等信號到監視器 1400，並且使監視器 1400 播放視訊與音訊(步驟 S1082)。當已完成讀取所有該等已加密檔案或已經受到使用者所進行之運作的指示而要完成播放動作時(步驟 S1084：是)，執行單元 1606 便結束播放動作。

如果仍有尚未讀取的已加密檔案的話且執行單元 1606

尚未從使用者接收到要完成播放的一項指令的話，執行單元 1606 將返回到步驟 S1074 且重複進行步驟 S1074 至 S1084 的處理動作。

1.6 總結以及較佳效應

如以上說明地，在本實施例中，DVD 1500 將儲存：包括 c 個已加密檔案的已加密內容，其各包括多個已加密單元；包括根據該等多個已加密單元而產生之 c 個第一雜湊表以及一第二雜湊表的頭標資訊；以及根據該第二雜湊表產生的簽章資訊。

在開始進行讀出、解密以及播放已加密內容等動作的同時，執行裝置 1600 將藉著使用隨機數來隨機地選擇 i 個已加密單元，並且根據該等選出的 i 個已加密單元來計算置換單元雜湊值以及置換檔案雜湊值。

接下來，執行裝置 1600 將從 DVD 讀取第二雜湊表，並且藉著從包括在已讀取第二雜湊表中的檔案雜湊值把對應於已計算置換檔案雜湊值的檔案雜湊值置換為已計算置換檔案雜湊值來產生已置換第二雜湊表。隨後，執行裝置 1600 將藉著使用已置換第二雜湊表來進行簽章資訊的驗證動作。如果驗證動作並不成功的話，執行裝置 1600 便中止播放內容。

因此，藉著把針對簽章資訊驗證動作而新計算出的單元雜湊值數量限制在 i 個，便可降低包含在簽章資訊驗證動作的計算數量，這可降低內容播放動作中處理的負載。

再者，藉著使用包含第一與第二雜湊表的一種二層結構來進行簽章資訊驗證動作，執行裝置 1600 能夠降低從 DVD 1500 讀取到的資訊數量。更確切來說，在本發明的第一實施例中，不需要讀取對應於未選出之檔案資訊的第一雜湊表。因此，可以縮短讀取資訊所需的時間。

此外，在第一實施例中將讀取對應於選出檔案資訊的第一雜湊表。然而，從構成對應於選出檔案資訊之第一雜湊表的部件中，僅讀取除了對應於已計算置換單元雜湊值之單元雜湊值之外的部件。這同樣地適用於讀取第二雜湊表的動作。據此，可以進一步的減少從 DVD 1500 讀取的資訊量。

藉著使用從已加密單元產生的已置換雜湊值來進行簽章資訊驗證動作，可以一次完成驗證是否包括未授權內容以及驗證是否簽章資訊係利用合法權所有者所擁有的簽章金鑰來產生的二項動作。

在驗證處理中，如果以未授權內容來置換 DVD 1500 的部分或所有已加密內容的話，此第一實施例便很有可能可以檢測未授權內容，因為只有 i 個已加密單元係隨機地選出以供使用。

在此，一項特定說明係根據假設已把一半已加密內容寫入到未授權內容中來提出。選出單一已加密單元為分散裝置 1100 產生的一有效已加密單元的可能性為 1/2。例如，如果選擇 7 個已加密單元且進行驗證動作的話，該等選出 7 個已加密單元全部為有效的可能性是$(1/2)^7=1/128$。即，

於此，無法檢測出未授權內容的可能性為小於 1%。據此，此第一實施例將作為避免詐欺行為的一種防止方法，其包含以未授權內容來置換合法權所有者所分散之內容的部分。

1.7 第一實施例的修改方案

在第一實施例中，分散裝置 1100 將把組成已取得內容的各個檔案劃分為單元，且隨後針對各個單元進行加密動作。然而，分散裝置 1100 可針對各個檔案進行加密動作以產生已加密檔案，並且藉著劃分各個該等已產生已加密檔案來產生已加密單元。於此，執行裝置 1600 的執行單元 1606 將從 DVD 1500 讀取已加密內容、針對各個已加密檔案解密已讀取已加密內容，並且播放已解密內容。

將藉由第 26 圖的輔助來說明本修改方案的分散裝置 1100b。

分散裝置 1100b 係由輸入單元 1101b、內容金鑰產生單元 1102、金鑰區塊產生單元 1103、執行裝置資訊儲存單元 1104、單元產生單元 1105b、加密處理單元 1106b、頭標資訊產生單元 1107、簽章資訊產生單元 1111、簽章金鑰儲存單元 1112、以及記錄單元 1114 組成。

因為內容金鑰產生單元 1102、金鑰區塊產生單元 1103、執行裝置資訊儲存單元 1104、頭標資訊產生單元 1107、簽章資訊產生單元 1111、簽章金鑰儲存單元 1112 以及記錄單元 1114 與第一實施例中的相同，在此將省略說

明該等部件。

此外，因為輸入單元 1101b 與第一實施例的輸入單元 1101 相同，除了係對加密處理單元輸出內容而不是對單元產生單元之外，在此亦省略其說明。

1.7.1 加密處理單元 1106b

加密處理單元 1106b 將從內容金鑰產生單元 1102 接收內容金鑰"CK"。

加密處理單元 1106 將從輸入單元 1101b 接收內容。在此，該等內容係由檔案"CNT1"、"CNT2"、至"CNTc"組成，如展示於第 3 圖中的內容 1120 一般。

當接收到內容時，加密處理單元 1106 將藉著使用內容金鑰"CK"而對包括在已接收內容中的檔案"CNT1"套用加密演算法 E1 來產生已加密檔案"ECT1"。

加密處理單元 1106 將對檔案"CNT2"至"CNTc"進行相同動作以產生已加密檔案"ECNT2"至"ECNTc"。

接下來，加密處理單元 1106 將把由已產生已加密檔案"ECNT1"、"ECNT2"、"ECNT3"至"ECNTc"構成的已加密內容輸出到單元產生單元 1105b 以及記錄單元 1114b。

1.7.2 單元產生單元 1105b

單元產生單元 1105b 將從加密處理單元 1106b 接收已加密內容。當接收到已加密內容時，單元產生單元 1105b 將產生檔案識別符"FID1"以及對應於包括在已接收已加密

內容中之已加密檔案"ECNT1"的檔案識別資訊"AD1"。

接下來，單元產生單元 1105b 將依據每 64 千位元組來劃分已加密檔案"ECNT1"以產生 m 個已加密單元。此時，如果最後已加密單元小於 64 千位元組的話，將以例如"000...000"的資料來填補已加密單元。

接下來，單元產生單元 1105b 將產生表示已產生已加密單元之數量的一數字"N1"，並且隨後產生由已產生檔案識別符"FID1"、檔案識別資訊"AD1"、以及單元編號"N1"組成的檔案資訊。

接下來，單元產生單元 1105b 將產生分別地對應於已產生 m 個已加密單元"EU1_1"、"EU1_2"、"EU1_3"至"EU1_m"的單元識別符"UID1_1"、"UID1_2"、"UID1_3"至"UID1_m"。隨後，單元產生單元 1105b 將藉著使對應已加密單元以及單元識別符配對來形成 m 個已加密單元資訊。

接下來，單元產生單元 1105b 將把 m 個已加密單元資訊結合在一起以形成已加密分離檔案"SplECNT1"。

單元產生單元 1105b 將針對包括在已加密內容中已加密檔案"ECNT2"、"ECNT3"至"ECNTc"的剩餘部份重複進行相同類型的處理動作，以產生已加密分離檔案"SplECNT2"、"SplECNT3"至"SplECNTc"以及檔案資訊的剩餘部份。隨後，單元產生單元 1105b 將把已產生的 c 個已加密分離檔案"SplECNT1"、"SplECNT2"、"SplECNT3"至"SplECNTc"輸出到頭標資訊產生單元 1107b 作為已加密

分離內容。

此外，單元產生單元 1105b 將產生由 c 個檔案資訊組成的單元檢選資訊，並且把已產生單元檢選資訊輸出到記錄單元 1114 以及簽章資訊產生單元 1111b。

2.第二實施例

以下將藉由圖式輔助且根據本發明來說明第二實施例。

2.1 未授權內容檢測系統

第二實施例的未授權內容檢測系統係由一分散裝置、一執行裝置、以及一監視器組成，如第一實施例的未授權內容檢測系統 1 一般。

分散裝置將根據操作者所進行的運作取得內容，並且加密取得內容來產生已加密內容。此外，分散裝置將摘取出該內容的部分，並且根據該等內容的已摘取部分(以下係稱為"代表性部份內容")來產生資訊，例如用以檢測未授權內容是否包括在該內容中的頭標資訊、用以證明該等內容係由合法權所有者發布的簽章資訊等等。分散裝置將把已產生已加密內容、簽章資訊等寫入到一 DVD 中。

將透過分散通路把該 DVD 販售或分散給使用者。

當載入該 DVD 時，執行裝置將從儲存在已載入 DVD 中的已加密內容產生代表性部份內容，並且根據已產生代表性部份內容來進行簽章資訊以及頭標資訊的驗證動作。如果驗證動作成功的話，執行裝置便開始播放該等內容。當

驗證動作並不成功時，執行裝置便禁止內容播放動作。

以下將詳細說明組成本實施例之未授權內容檢測系統的個別裝置以及 DVD。

2.2 分散裝置 2100

第 27 圖展示出構成本實施例之未授權內容檢測系統的分散裝置結構。如第 27 圖所示，分散裝置 2100 係由輸入單元 2101、內容金鑰產生單元 2102、金鑰區塊產生單元 2103、執行裝置資訊儲存單元 1104、選擇單元 2105、頭標資訊產生單元 2107、簽章資訊產生單元 2108、簽章金鑰儲存單元 1112、加密處理單元 2109、以及記錄單元 2114 組成。

以下將詳細說明組成分散裝置 2100 的個別裝置。要注意的是，因為執行裝置資訊儲存單元 1104 以及簽章金鑰儲存單元 1112 與第一實施例中的相同，在此便省略該等部件的說明。

2.2.1 輸入單元 2101

輸入單元 2101 將根據操作者的運作從外部裝置或外部記錄媒體取得內容以及多份識別資訊。

第 28 圖展示出內容以及輸入單元 2101 取得的識別資訊。

內容 2120 係由 c 個部份內容"CNT1"2121、"CNT2"2122、"CNT3"2123 至"CNTc"2127

組成。在此，輸入單元 2101 所取得的內容 2120 為執行裝置 2600 可播放的格式(如以下將詳細說明地)，且 DVD-視訊格式以及 MPEG-2(移動圖象專家組格式 2)格式為該等可播放格式的實例。

各個識別資訊為獨特地指出構成內容 2120 部份內容中之一的資訊，且可例如為來自該等內容標題之一對應部份內容的一差距值、一區段編號、或參照該等內容標題指定之部份內容的一播放開始點。例如，識別資訊"AD1"2131 對應於部份內容"CNT1"2121，且部份內容"CNT1"2121 的標題係位於內容 2120 標題的"AD1"上。

該輸入單元 2101 將輸出已取得內容 2120 以及 c 個識別資訊到內容金鑰產生單元 2102。

2.2.2 內容金鑰產生單元 2102

內容金鑰產生單元 2102 將接收來自輸入單元 2101 的內容 2120 以及 c 個識別資訊。當接收到內容 2120 以及 c 個識別資訊時，內容金鑰產生單元 2102 將產生一擬隨機數，且藉著使用已產生擬隨機數來產生一個 128 位元長度的內容金鑰"CK"。並非為一個擬隨機數，可產生一真實隨機數，例如藉著使用信號中的雜音。

接下來，內容金鑰產生單元 2102 將輸出已產生的內容金鑰"CK"、已接收內容 2120、以及 c 個識別資訊到金鑰區塊產生單元 2103 以及加密處理單元 2109。

2.2.3 金鑰區塊產生單元 2103

金鑰區塊產生單元 2103 將從內容金鑰產生單元 2102 接收內容金鑰"CK"、內容 2120、以及 c 個識別資訊。當接收到內容金鑰"CK"時，金鑰區塊產生單元 2103 將藉著使用儲存在執行裝置資訊儲存單元 1104 中的裝置識別表 1130 以及已接收內容金鑰"CK"來產生一金鑰區塊。因為用以產生金鑰區塊的程序與第一實施例中的相同，在此便省略其說明。此外，在此產生的金鑰區塊具有與第 5 圖之金鑰區塊 1150 相同的結構。

接下來，金鑰區塊產生單元 2103 將把已產生金鑰區塊、已接收內容金鑰"CK"、內容 2120、以及 c 個識別資訊輸出到選擇單元 2105。

2.2.4 選擇單元 2105

第 29 圖展示出由選擇單元 2105 進行之處理動作的大致概要。以下將藉由第 29 圖的輔助來說明選擇單元 2105。

選擇單元 2105 將接收來自金鑰區塊產生單元 2103 的金鑰區塊、內容金鑰"CK"、內容 2120、以及 c 個識別資訊。當接收到該等資訊時，選擇單元 2105 將從已接收的 c 個識別資訊中選出 k 個。在此，將假設 k=3 來進行說明。

有關選擇方法，可例如使用隨機數、或從日期、或從溫度等中選出 k 個識別資訊。替代地，可設計為能接受操作者的選擇。如果內容 2120 為 MPEG 格式的話，可選出指出內部圖像的識別資訊。此外，選擇單元 2105 可預儲存識別

出 k 個欲選出識別資訊的資訊，且響應於操作者的指令來進行選擇動作。

如第 29 圖所示，選擇單元 2105 在此將選擇數份識別資訊"AD3"2133、"AD7"2134、以及"ADc"2137。

接下來，選擇單元 2105 將摘取出對應於識別資訊"AD3"2133 的一部份內容"CNT3"(其係從已接收內容 2120 中選出)，並且產生一代表性資訊 2141(其由已選出的識別資訊"AD3"2133 以及已摘取的部份內容"CNT3"組成)。在此，選出的部份內容係稱為"代表性部份內容"。

選擇單元 2105 將針對識別資訊"AD7"2134 以及"ADc"2137 重複進行相同的處理動作，以產生代表性資訊 2142 以及 2143。

接下來，選擇單元 2105 將對頭標資訊產生單元 2107 輸出：已產生代表性資訊 2141、2142 與 2143、已接收金鑰區塊、內容金鑰"CK"、以及內容 2120。

2.2.5 頭標資訊產生單元 2107

頭標資訊產生單元 2107 將接收來自選擇單元 2105 的三份代表性資訊 2141、2142 以及 2143、金鑰區塊、內容金鑰"CK"以及內容 2120。

當接收該等項目時，頭標資訊產生單元 2107 將產生獨特地識別已接收代表性資訊 2141 的一識別資訊識別符"ADID1"。 例如，用以產生識別資訊識別符的方法包括一種自然數的序列配置以及一種利用隨機數的隨機配置。

接下來，頭標資訊產生單元 2107 將從已接收代表性資訊 2141 中摘取出識別資訊"AD3"，並且產生由已產生識別資訊識別符"ADID1"以及識別資訊"AD3"構成的代表性檢測資訊。

隨後，頭標資訊產生單元 2107 將從已接收代表性資訊 2141 摘取出代表性部份內容"CNT3"，並且藉著把已摘取代表性部份內容"CNT3"指派給雜湊函數來產生一部份雜湊值"HA3"。頭標資訊產生單元 2107 將產生由已產生識別資訊識別符"ADID1"以及部份雜湊值"HA3"構成的代表性雜湊資訊。

頭標資訊產生單元 2107 將針對代表性資訊 2142 與 2143 重複進行相同的處理動作，並且產生代表性檢測資訊以及代表性雜湊資訊。頭標資訊產生單元 2107 將產生由三份已產生代表性檢測資訊組成的選擇位置資訊。

第 30 圖展示出在此時點產生之選擇位置資訊的結構。選擇位置資訊 2160 係由代表性檢測資訊 2161、2162 與 2163 組成，其分別地對應於代表性資訊 2141、2142 與 2143。各個代表性檢測資訊係由一識別資訊識別符以及一識別資訊組成。舉一實例來說，代表性檢測資訊 2161 對應於代表性資訊 2141，且包括識別資訊識別符"ADID1"2171 以及識別資訊"AD3"2176。

此外，頭標資訊產生單元 2107 將產生由三份已產生代表性雜湊資訊組成的頭標資訊。

第 31 圖展示出在此時點產生之頭標資訊的結構。如第

31圖所示，頭標資訊2200係由代表性雜湊資訊2201、2202與2203構成，其分別地對應於代表性檢測資訊2161、2162與2163。

各個代表性雜湊資訊包括一識別資訊識別符以及一部份雜湊值。例如，代表性雜湊資訊2201係根據代表性資訊2141而產生，且包括一識別資訊識別符"ADID1"2211以及一部份雜湊值"HA3"。

接下來，頭標資訊產生單元2107將把已產生選擇位置資訊2160、頭標資訊220、已接收金鑰區塊、內容金鑰"CK"以及內容2120輸出到簽章資訊產生單元2108。

2.2.6 簽章資訊產生單元2108

簽章資訊產生單元2108接收來自頭標資訊產生單元2107的選擇位置資訊2160、頭標資訊2200、金鑰區塊、內容金鑰"CK"以及內容2120。當接收到該等資訊時，簽章資訊產生單元2108將摘取出包括在已接收頭標資訊2200中的部份雜湊值"HA3"、"HA5"以及"HAc"。

接下來，簽章資訊產生單元2108將從簽章金鑰儲存單元1112讀取簽章金鑰1113。簽章資訊產生單元2108將藉著對一合併結果分派簽章產生演算法S來產生簽章資訊，該合併結果係藉著利用讀取簽章金鑰1113的動作而合併已摘取部份雜湊值"HA3"、"HA5"與"HAc"。

接下來，簽章資訊產生單元2108將把已產生簽章資訊、已接收選擇位置資訊2160、頭標資訊2200、金鑰區

塊、內容金鑰"CK"以及內容 2120 輸出到加密處理單元 2109。

2.2.7 加密處理單元 2109

加密處理單元 2109 將接收來自簽章資訊產生單元 2108 的簽章資訊、選擇位置資訊 2160、頭標資訊 2200、金鑰區塊、內容金鑰"CK"以及內容 2120。

當接收到該等資訊時，加密處理單元 2109 將藉著分別地對構成已接收內容 2120 的部份內容"CNT1"、"CNT2"、"CNT3"至"CNTc"套用加密演算法 E1 且藉著使用已接收內容金鑰"CK"來產生已加密部份內容"ECNT1"、"ECNT2"、"ECNT3"至"ECNTc"。已產生已加密部份內容"ECNT1"、"ECNT2"、"ECNT3"至"ECNTc"係整體地稱為已加密內容。在此，加密內容可表示為 ECNTb=Enc(CK、CNTb)，其中 b 為 c 或更小的自然數。第 32 圖展示出在此時點產生之已加密內容 2220 的結構。

隨後，加密處理單元 2109 將藉著對已接收選擇位置資訊套用加密演算法 E1 且使用已接收內容金鑰"CK"來產生已加密選擇位置資訊。

接下來，加密處理單元 2109 將對記錄單元 2114 輸出已產生已加密內容 2220、已加密選擇位置資訊、已接收簽章資訊、頭標資訊 2200、以及金鑰區塊。

2.2.8 記錄單元 2114

記錄單元 2114 能夠被載入到 DVD 中。

記錄單元 2114 將從加密處理單元 2109 接收已加密內容 2220、已加密選擇位置資訊、簽章資訊、頭標資訊 2200 以及金鑰區塊，並且把已接收已加密內容 2220、已加密選擇位置資訊、簽章資訊、頭標資訊 2200 與金鑰區塊寫入到 DVD。

2.3 DVD 2500

如第 33 圖所示，DVD 2500 將儲存金鑰區塊 2510、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580。

已經由分散裝置 2100 寫入金鑰區塊 2510、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580，且該等部件的結構均如上所述。

2.4 執行裝置 2600

如第 34 圖所示，執行裝置 2600 係由取得單元 2601、內容金鑰取得單元 2602、裝置金鑰儲存單元 1604、位置資訊解密單元 2606、簽章資訊驗證單元 2611、驗證金鑰儲存單元 1612、代表性部份內容解密單元 2616、頭標資訊驗證單元 2617 以及執行單元 2618 組成。

以下將詳細說明組成執行裝置 2600 的個別部件。要注意的是，因為裝置金鑰儲存單元 1604 以及驗證金鑰儲存單元 1612 與構成第一實施例之執行裝置 1600 的單元相同，

在此便省略該等部件的說明。

2.4.1 取得單元 2601

將把取得單元 2601 載入到 DVD 2500 中。當檢測到已載入到 DVD 2500 中時，取得單元 2601 將從 DVD 2500 讀取金鑰區塊 2510、加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580。取得單元 2601 將輸出已讀取金鑰區塊 2510、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580 到內容金鑰取得單元 2602。

2.4.2 內容金鑰取得單元 2602

內容金鑰取得單元 2602 將從取得單元 2601 接收金鑰區塊 2510、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580。

當接收到該等資訊時，內容金鑰取得單元 2602 將藉著利用由裝置金鑰儲存單元 1604 以及已接收金鑰區塊儲存的裝置識別符"AID_p"以及裝置金鑰"DK_p"來產生內容金鑰"CK"。因為用以產生內容金鑰"CK"的程序與構成第一實施例之執行裝置 1600 之內容金鑰取得單元 1602 所進行的內容金鑰"CK"產生程序相同，在此便省略其說明。

接下來，內容金鑰取得單元 2602 將對位置資訊解密單元 2606 輸出已產生內容金鑰"CK"、已接收已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570、以及已加密

內容 2580。

2.4.3 位置資訊解密單元 2606

位置資訊解密單元 2606 將接收來自內容金鑰取得單元 2602 的內容金鑰"CK"、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580。

當接收到該等資訊時，位置資訊解密單元 2606 將藉著對已接收已加密選擇位置資訊 2530 套用解密演算法 D1 且使用已接收內容金鑰"CK"來產生選擇位置資訊。在此時點產生的選擇位置資訊具有與第 30 圖之選擇位置資訊 2160 相同的結構。

接下來，位置資訊解密單元 2606 將對簽章資訊驗證單元 2611 輸出已產生選擇位置資訊、已接收內容金鑰"CK"、頭標資訊 2550、簽章資訊 2570、以及已加密內容 2580。

2.4.4 簽章資訊驗證單元 2611

簽章資訊驗證單元 2611 將接收來自位置資訊解密單元 2606 的選擇位置資訊、內容金鑰"CK"、頭標資訊 2550、簽章資訊 2570、以及已加密內容 2580。

當接收到該等資訊時，簽章資訊驗證單元 2611 將從驗證金鑰儲存單元 1612 讀取驗證金鑰。接下來，簽章資訊驗證單元 2611 將分別地從構成已接收頭標資訊 2550 的三份代表性雜湊資訊中摘取出部份雜湊值"HA3"、"HA7"、以及"HAc"，並且藉著使用讀取驗證金鑰而由合併已摘取部份

雜湊值"HA3"、"HA7"以及"HAc"形成的合併結果套用簽章驗證演算法 V 來產生簽章驗證資訊。簽章資訊驗證單元 2611 將比較已產生簽章驗證資訊以及已接收簽章資訊。當該等二項資訊部相符時，簽章資訊驗證單元 2611 便判斷出簽章驗證動作並不成功，且中止後續處理動作。

當該等二項資訊部相符時，簽章資訊驗證單元 2611 便判斷出簽章驗證動作成功，且對代表性部份內容解密單元 2616 輸出已接收選擇位置資訊、內容金鑰"CK"、頭標資訊 2550 以及已加密內容 2580。

2.4.5 代表性部份內容解密單元 2616

代表性部份內容解密單元 2616 將接收來自簽章資訊驗證單元 2611 的選擇位置資訊、內容金鑰"CK"、頭標資訊 2550、以及已加密內容 2580。

當接收到該等資訊時，代表性部份內容解密單元 2616 將摘取出包括在構成已接收選擇位置資訊之第一代表性檢測資訊中的識別資訊識別符"ADID1"以及對應識別資訊"AD3"，並且根據已摘取識別資訊"AD3"進一步地從已接收已加密內容 2580 摘取出已加密部份內容"ECNT3"。接下來，代表性部份內容解密單元 2616 將藉著對已摘取已加密部份內容"ECNT3"套用解密演算法 D1 而使用已接收內容金鑰"CK"來產生代表性部份內容"CNT3"。在此，一對已產生代表性部份內容"CNT3"以及已摘取識別資訊識別符"ADID1"將被稱為"一對驗證代表性資訊"。

接下來，代表性部份內容解密單元 2616 將針對剩餘的代表性檢測資訊重複進行相同類型的處理動作，以產生由識別資訊識別符"ADID2"以及代表性部份內容"CNT7"組成的一份驗證代表性資訊以及由識別資訊識別符"ADID3"以及代表性部份內容"CNTc"組成的一份驗證代表性資訊。

接下來，代表性部份內容解密單元 2616 將對頭標資訊驗證單元 2617 輸出三份已產生驗證代表性資訊、已接收內容金鑰"CK"、頭標資訊 2550 以及已加密內容 2580。

2.4.6 頭標資訊驗證單元 2617

頭標資訊驗證單元 2617 將接收來自代表性部份內容解密單元 2616 的三份驗證代表性資訊、內容金鑰"CK"、頭標資訊 2550、以及已加密內容 2580。

當接收到該等資訊時，頭標資訊驗證單元 2617 將藉著分別地把包括在三份已接收驗證代表性資訊中的代表性部份內容"CNT3"、"CNT7"以及"CNTc"指派給雜湊函數來產生驗證雜湊值"H3"、"H7"與"Hc"。在此使用的雜湊函數與用於分散裝置 2100 之頭標資訊產生單元 2107 中的相同。

接下來，頭標資訊驗證單元 2617 將在頭標資訊 2550 中搜尋與包括在對應驗證代表性資訊中之識別資訊識別符"ADID1"相符的識別資訊識別符，並且摘取出對應於已檢測識別資訊識別符的部份雜湊值"HA3"。隨後，頭標資訊驗證單元 2617 將比較已摘取部份雜湊值"HA3"以及已產生驗證雜湊值"H3"。

此外，頭標資訊驗證單元 2617 將根據包括在對應驗證代表性資訊中的識別資訊識別符"ADID2"從頭標資訊 2550 中摘取出部份雜湊值"HA7"，並且比較已摘取部份雜湊值"HA7"以及已產生驗證雜湊值"H7"。

頭標資訊驗證單元 2617 將根據包括在對應驗證代表性資訊中的識別資訊識別符"ADIDc"從頭標資訊 2550 中摘取出部份雜湊值"HAc"，並且比較已摘取部分值"HAc"以及已產生驗證雜湊值"Hc"。

當比較各個該等三對且其中有偶數對彼此並不相符時，頭標資訊驗證單元 2617 便中止後續處理動作。

當比較各個該等三對時所有三對均相符時，頭標資訊驗證單元 2617 便判斷出驗證頭標資訊 2550 的動作是成功的，且輸出已接收內容金鑰"CK"以及已加密內容 2580 到執行單元 2618。

2.4.7 執行單元 2618

執行單元 2618 將從頭標資訊驗證單元 2617 接收內容金鑰"CK"以及已加密內容 2580。

當接收到該等資訊時，執行單元 2618 將藉著對構成已接收已加密內容 2580 的各個已加密部份內容"ECNT1"、"ECNT2"、"ECNT3"至"ECNTc"套用解密演算法 D1 且使用已接收內容金鑰"CK"來產生由部份內容"CNT1"、"CNT2"、"CNT3"至"CNTc"組成的內容。

接下來，執行單元 2618 將擴展已產生內容以產生視訊

與音訊資料，並且從所產生的視訊與音訊資料中產生視訊與音訊信號。執行單元 2618 將把已產生的視訊與音訊信號輸出到監視器。

2.5 分散裝置 2100 與執行裝置 2600 的運作性行為

以下將說明分散裝置 2100 以及執行裝置 2600 的運作性行為。

2.5.1 分散裝置 2100 的運作性行為

以下將藉由第 35 圖中展示之流程圖的輔助來說明分散裝置 2100 的運作性行為。

輸入單元 2101 將接收由 C 個部份內容以及 C 個識別資訊組成的內容 2120(步驟 S2011)，並且輸出已接收內容 2120 以及識別資訊到內容金鑰產生單元 2102。

內容金鑰產生單元 2102 將接收內容 2120 以及 C 個識別資訊，並且產生內容金鑰(步驟 S2012)。

金鑰區塊產生單元 2103 將從內容金鑰產生單元 2102 接收內容金鑰、內容 2120、以及 C 個識別資訊，並且從執行裝置資訊儲存單元 1104 讀取裝置識別符以及裝置金鑰(步驟 S2013)。金鑰區塊產生單元 2103 將產生金鑰區塊，利用讀取裝置識別符以及裝置金鑰(步驟 S2014)，並且輸出已產生金鑰區塊、已接收內容金鑰、內容 2120 以及 C 個識別資訊到選擇單元 2105。

選擇單元 2105 將接收金鑰區塊、內容金鑰、內容 2120

以及識別資訊，並且藉著從已接收內容 2120 中選出 k 個代表性部份內容來產生 k 個代表性資訊(步驟 S2016)。隨後，選擇單元 2105 將對頭標資訊產生單元 2107 輸出已產生的 k 個代表性資訊、已接收內容金鑰以及內容 2120。

頭標資訊產生單元 2107 將從選擇單元 2105 接收 k 個代表性資訊、內容金鑰、以及內容 2120，並且從已接收的 k 個代表性資訊產生選擇位置資訊 2160 以及頭標資訊 2200(步驟 S2018)。接下來，頭標資訊產生單元 2107 將對簽章資訊產生單元 2108 輸出已產生選擇位置資訊 2160、頭標資訊 2200、已接收金鑰區塊、內容金鑰以及內容 2120。

隨後，簽章資訊產生單元 2108 將從頭標資訊產生單元 2107 接收選擇位置資訊 2160、頭標資訊 2200、金鑰區塊、內容金鑰以及內容 2120。當接收到該等資訊時，簽章資訊產生單元 2108 將從簽章金鑰儲存單元 1112 讀取簽章金鑰 1113(步驟 S2019)，並且從讀取簽章金鑰 1113 以及頭標資訊 2200 產生簽章資訊(步驟 S2021)。接下來，簽章資訊產生單元 2108 將對加密處理單元 2109 輸出已產生簽章資訊、已接收金鑰區塊、選擇位置資訊 2160、頭標資訊 2200、內容金鑰以及內容 2120。

加密處理單元 2109 將從簽章資訊產生單元 2108 接收簽章資訊、金鑰區塊、選擇位置資訊 2160、頭標資訊 2200、內容金鑰以及內容 2120，並且藉著使用已接收內容金鑰加密選擇位置資訊 2160 來產生已加密選擇位置資訊(步驟 S2022)。隨後，加密處理單元 2109 將藉著使用內容金鑰

加密內容 2120 來產生已加密內容 (步驟 S2023)，且隨後對記錄單元 2114 輸出已產生已加密選擇位置資訊、已加密內容、已接收金鑰區塊、簽章資訊以及頭標資訊 2200。

記錄單元 2114 將把從加密處理單元 2109 接收到的金鑰區塊、已加密選擇位置資訊、頭標資訊 2200、簽章資訊以及已加密內容寫入到 DVD 2500 中(步驟 S2024)。

2.5.2 執行裝置 2600 的運作性行為

以下將藉由第 36 圖流程圖的輔助來說明執行裝置 2600 的運作性行為。

當載入到 DVD 2500 中時，取得單元 2601 將從 DVD 2500 讀取金鑰區塊 2510、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570、以及已加密內容 2580(步驟 S2041)。隨後，取得單元 2601 將輸出金鑰區塊 2510、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580 到內容金鑰取得單元 2602。

當從取得單元 2601 接收到金鑰區塊 2510、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570 以及已加密內容 2580 時，內容金鑰取得單元 2602 將從裝置金鑰儲存單元 1604 讀取裝置識別符以及裝置金鑰(步驟 S2042)。內容金鑰取得單元 2602 將從讀取裝置識別符、裝置金鑰、以及已接收金鑰區塊 2510 產生一內容金鑰(步驟 S2043)。內容金鑰取得單元 2602 將對位置資訊解密單元 2606 輸出已產生內容金鑰、已接收已加密選擇位置資訊 2530、頭標

資訊 2550、簽章資訊 2570、以及已加密內容 2580。

位置資訊解密單元 2606 將從內容金鑰取得單元 2602 接收內容金鑰、已加密選擇位置資訊 2530、頭標資訊 2550、簽章資訊 2570、以及已加密內容 2580，並且藉著使用已接收內容金鑰解密已加密選擇位置資訊 2530 來產生選擇位置資訊 (步驟 S2044)。接下來，位置資訊解密單元 2606 將對簽章資訊驗證單元 2611 輸出已產生選擇位置資訊、已接收內容金鑰、頭標資訊 2550、簽章資訊 2570、以及已加密內容 2580。

簽章資訊驗證單元 2611 將從位置資訊解密單元 2606 接收選擇位置資訊、內容金鑰、頭標資訊 2550、簽章資訊 2570、以及已加密內容 2580，並且從驗證金鑰儲存單元 1612 讀取一驗證金鑰(步驟 S2046)。隨後，簽章資訊驗證單元 2611 將藉著使用讀取驗證金鑰以及已接收頭標資訊 2550 來驗證簽章資訊 2570(步驟 S2048)。當驗證簽章資訊 2570 的動作不成功時(步驟 S2049：否)，簽章資訊驗證單元 2611 便中止執行裝置 2600 的後續處理動作。

當驗證簽章資訊 2570 的動作成功時(步驟 S2049：是)，簽章資訊驗證單元 2611 便對代表性部份內容解密單元 2616 輸出已接收選擇位置資訊、內容金鑰、頭標資訊 2550、以及已加密內容 2580。

代表性部份內容解密單元 2616 將從簽章資訊驗證單元 2611 接收選擇位置資訊、內容金鑰、頭標資訊 2550、以及已加密內容 2580，並且根據已接收選擇位置資訊、已加

密內容 2580 與內容金鑰來產生 k 個代表性部份內容(步驟 S2051)。隨後，代表性部份內容解密單元 2616 將產生由對應代表性部份內容以及識別資訊識別符構成的 k 個驗證代表性資訊(步驟 S2052)，並且把已產生 k 個驗證代表性資訊、已接收內容金鑰、頭標資訊 2550 以及已加密內容 2580 輸出到頭標資訊驗證單元 2617。

頭標資訊驗證單元 2617 將接收來自代表性部份內容解密單元 2616 的 k 個驗證代表性資訊、內容金鑰、頭標資訊 2550、以及已加密內容 2580，並且藉著使用已接收的 k 個驗證代表性資訊來進行驗證頭標資訊 2550 的動作(步驟 S2054)。如果驗證動作不成功的話(步驟 S2056：否)，頭標資訊驗證單元 2617 便中止後續處理動作。

如果驗證動作成功的話(步驟 S2056：是)，頭標資訊驗證單元 2617 將對執行單元 2618 輸出已接收內容金鑰以及已加密內容 2580。

當接收到來自頭標資訊驗證單元 2617 的內容金鑰以及已加密內容 2580 時，執行單元 2618 將藉著使用已接收內容金鑰解密已加密內容 2580 來產生該等內容(步驟 S2057)、擴展已產生內容(步驟 S2058)，並且使監視器播放該等內容(步驟 S2059)。

2.6 總結以及較佳效應

如以上所述，在第二實施例中，分散裝置 2100 將藉著僅使用構成該等內容之 c 個部份內容中的 k 個代表性部份

內容來產生頭標資訊，並且藉著對頭標資訊套用簽章產生演算法來進一步產生簽章資訊。

執行裝置 2600 將根據選擇位置資訊產生 k 個代表性部份內容來驗證是否包括未授權內容，並且藉著使用已產生的 k 個代表性部份內容來驗證頭標資訊。當驗證動作成功時，執行裝置 2600 便開始內容播放動作、判斷出並未包括未授權內容。

因此，藉著僅使用構成該等內容之 c 個部份內容中的 k 個部分內容來驗證頭標資訊，便可使執行裝置 2600 之用以進行驗證動作的處理負載降低。

再者，亦可以降低分散裝置 2100 之頭標資訊產生過程中包括的處理負載。

3.第三實施例

以下將根據本發明的第三實施例來說明一種未授權內容檢測系統。

3.1 未授權內容檢測系統

第三實施例的未授權內容檢測系統係由一分散裝置、一執行裝置、以及一監視器組成，如第一實施例的未授權內容檢測系統一般。

分散裝置將根據操作者所進行的運作取得內容，並且加密所取得的內容來產生已加密內容。

此外，分散裝置將摘取出該內容的部分，並且根據該等

內容的已摘取部分(以下係稱為"一份代表性部份內容")來產生資訊，例如用以檢測未授權內容是否包括在該內容中的頭標資訊、用以證明該等內容係由合法權所有者發布的簽章資訊等等。分散裝置將重複摘取一份代表性部份內容的動作、產生一份頭標資訊、產生一份簽章資訊以產生多份頭標以及簽章資訊，並且把已產生已加密內容以及多份頭標與簽章資訊寫入到 DVD 中。

將透過分散通路把該 DVD 販售或分散給使用者。

執行裝置將從錄製在 DVD 上的多份簽章資訊以及多份頭標資訊中選擇一份資訊，並且驗證選出的簽章以及頭標資訊。

以下將詳細說明組成本實施例之未授權內容檢測系統的個別裝置以及 DVD。

3.2 分散裝置 3100

第 37 圖展示出本實施例中分散裝置的結構。如第 37 圖所示，分散裝置 3100 係由輸入單元 2101、內容金鑰產生單元 2102、金鑰區塊產生單元 2103、執行裝置資訊儲存單元 1104、選擇單元 3105、頭標資訊產生單元 3107、簽章資訊產生單元 3108、簽章金鑰儲存單元 1112、加密處理單元 3109、以及記錄單元 3114 組成。

輸入單元 2101、內容金鑰產生單元 2102、金鑰區塊產生單元 2103、執行裝置資訊儲存單元 1104、以及簽章金鑰儲存單元 1112 均與第二實施例中的相同，因此在此便省

略該等部件的說明。

3.2.1 選擇單元 3105

選擇單元3105將預儲存"x"重複的次數(x為2或更大的整數)。

選擇單元 3105 將接收來自金鑰區塊產生單元 2103 的金鑰區塊、內容金鑰"CK"、內容、以及 c 個識別資訊。當接收到金鑰區塊、內容金鑰"CK"、內容、c 個識別資訊時，選擇單元 3105 將以相同於第二實施例之選擇單元 2105 的方式來產生 k 個代表性資訊。

選擇單元 3105 將重複相同的處理動作 x 次，以產生 x 個群組的 k 個代表性資訊。在此，第一組的代表性資訊係稱為"第一代表性群組"，而第二組至第 x 組的代表性資訊則分別地稱為"第二代表性群組"至"第 x 代表性群組"。此處的一特定實例是所有第一至第 x 代表性群組係分別地由 k 個代表性資訊所組成，然而，代表性資訊的數量可依據群組而不同。

接下來，選擇單元 3105 將把已產生第一、第二至第 x 代表性群組、已接收金鑰區塊、內容金鑰"CK"以及內容輸出到頭標資訊產生單元 3107。

3.2.2 頭標資訊產生單元 3105

頭標資訊產生單元 3107 將接收來自選擇單元 3105 的第一、第二至第 x 代表性群組、金鑰區塊、內容金鑰"CK"

以及內容。

當接收到該等資訊時，頭標資訊產生單元 3107 將根據包括在已接收第一代表性群組以及內容中的 k 個代表性資訊來產生選擇位置資訊"POS1"以及頭標資訊"HEAD1"。用以產生選擇位置資訊以及頭標資訊的特定程序與第二實施例之頭標資訊產生單元 2107 執行的選擇位置資訊 2160 與頭標資訊 2200 產生程序相同，因此在此便省略其說明。選擇位置資訊"POS1"的結構與第 30 圖之選擇位置資訊 2160 的結構相同，而頭標資訊"HEAD1"的結構與第 31 圖之頭標資訊 2200 的結構相同。

接下來，頭標資訊產生單元 3107 將產生對一對已產生選擇位置資訊"POS1"以及頭標資訊"HEAD1"特定的頭標識別符"HEADID1"。在此，一組已產生頭標識別符"HEADID1"、一份選擇位置資訊"POS1"、以及一份頭標資訊"HEAD1"將稱為"第一頭標群組"。

頭標資訊產生單元 3107 將針對第二、第三至第 x 代表性群組重複進行相同的處理動作，以產生第二、第三至第 x 頭標群組。

接下來，頭標資訊產生單元 3107 將從第一至第 x 頭標群組中摘取出頭標識別符，並且產生由已摘取之 x 份的頭標識別符所構成的頭標選擇資訊。

第 38 圖展示出在此時點產生之頭標選擇資訊的結構。頭標選擇資訊 3130 係由 x 份頭標識別符所組成，且頭標識別符分別地對應於第一至第 x 頭標群組。

接下來，頭標資訊產生單元 3107 將對簽章資訊產生單元 3108 輸出已產生頭標選擇資訊 3130、第一、第二至第 x 頭標群組、已接收金鑰區塊、內容金鑰"CK"、以及內容。

3.2.3 簽章資訊產生單元 3108

簽章資訊產生單元 3108 將接收來自頭標資訊產生單元 3107 的頭標選擇資訊 3130、第一、第二至第 x 頭標群組、金鑰區塊、內容金鑰"CK"、以及內容。

當接收到該等資訊時，簽章資訊產生單元 3108 將從簽章金鑰儲存單元 1112 讀取簽章金鑰 1113。

接下來，簽章資訊產生單元 3108 將藉著使用包括在第一頭標群組中的頭標資訊"HEAD1"以及讀取簽章金鑰 1113 來產生一份簽章資訊"Sign1"。用以產生簽章資訊的一特定程序與簽章資訊產生單元 2108 進行的相同。

在此，將對"第一頭標群組"重新分派一結果，其係藉著把已產生的簽章資訊"Sign1"加到頭標識別符"HEADID1"、選擇位置資訊"POS1"以及頭標資訊"HEAD1"中而形成。

簽章資訊產生單元 3108 將針對第二至第 x 頭標群組重複進行相同類型的處理動作，以產生簽章資訊，且藉著把已產生簽章資訊分別地加到對應頭標識別符、選擇位置資訊、以及頭標資訊中而新近地形成第二至第 x 頭標群組。

接下來，簽章資訊產生單元 3108 將對加密處理單元 3109 輸出第一、第二至第 x 頭標群組、已接收頭標選擇資訊 3130、金鑰區塊、內容金鑰"CK"、以及內容。

3.2.4 加密處理單元 3109

加密處理單元 3109 將接收來自簽章資訊產生單元 3108 的第一、第二至第 x 頭標群組、頭標選擇資訊 3130、金鑰區塊、內容金鑰"CK"、以及內容。

加密處理單元 3109 將藉著使用已接收內容金鑰"CK"而對構成已接收內容的個別部份內容套用加密演算法 E1 來產生 c 個已加密部份內容，並且把已產生的 c 個已加密部份內容置放在一起而形成加密內容。在此時點產生的已加密內容的結構與第 32 圖中的已加密內容 2220 相同。

接下來，加密處理單元 3109 將從第一頭標群組摘取出選擇位置資訊"POS1"，並且藉著使用內容金鑰"CK"而對已摘取的選擇位置資訊"POS1"套用加密演算法 E1 來產生一份已加密選擇位置資訊"EPOS1"。接下來，加密處理單元 3109 將把包括在第一頭標群組中的選擇位置資訊"POS1"置換為已產生的已加密選擇位置資訊"EPOS1"。在此，EPOS1=Enc(CK、POS1)。

加密處理單元 3109 將第二至第 x 頭標群組進行相同動作，以產生已加密選擇位置資訊，並且把對應選擇位置資訊置換為已加密選擇位置資訊。

接下來，加密處理單元 3109 將對記錄單元 3114 輸出第一、第二至第 x 頭標群組、已產生已加密內容、已接收頭標選擇資訊 3130 以及金鑰區塊。

3.2.5 記錄單元 3114

記錄單元 3114 將接收來自加密處理單元 3109 的第一、第二至第 x 頭標群組、已加密內容、頭標選擇資訊 3130、以及金鑰區塊，並且把已接收第一、第二至第 x 頭標群組、已加密內容、頭標選擇資訊 3130、以及金鑰區塊寫入到 DVD 中。

3.3 DVD 3500

第 39 圖展示出本實施例中由 DVD 記錄的資訊。

如第 39 圖所示，DVD 3500 將儲存金鑰區塊 3510、頭標選擇資訊 3520、第一頭標群組 3530、第二頭標群組 3540 至第 x 頭標群組 3560、以及已加密內容 3580。

各個第一頭標群組 3530、第二頭標群組 3540 至第 x 頭標群組 3560 係由一頭標識別符、一已加密選擇位置資訊、一頭標資訊、以及一簽章資訊組成。

例如，第一頭標群組 3530 係由頭標識別符"HEAD1"3531、已加密選擇位置資訊"EPOS1"3532、頭標資訊"HEAD1"、以及簽章資訊"Sign1"3534 組成。

已由分散裝置 3100 把該等資訊寫入到 DVD3500 中。各個該等資訊的結構均如前所述，且因此在此將省略其說明。

3.4 執行裝置 3600

如第 40 圖所示，執行裝置 3600 係由取得單元 3601、

內容金鑰取得單元 2602、裝置金鑰儲存單元 1604、位置資訊解密單元 2606、簽章資訊驗證單元 2611、驗證金鑰儲存單元 1612、代表性部份內容解密單元 2616、頭標資訊驗證單元 2617 以及執行單元 2618 組成。

除了取得單元 3601 以外的部件均與構成第二實施例之執行裝置 2600 的內容金鑰取得單元 2602、裝置金鑰儲存單元 1604、位置資訊解密單元 2606、簽章資訊驗證單元 2611、驗證金鑰儲存單元 1612、代表性部份內容解密單元 2616、頭標資訊驗證單元 2617、以及執行單元 2618 具有相同的結構以及運作性行為，因此在此僅說明取得單元 3601。

3.4.1 取得單元 3601

當檢測到已載入到 DVD 3500 中時，取得單元 3601 將從 DVD 3500 讀取頭標選擇資訊 3520。隨後，取得單元 3601 將使用隨機數來選擇包括在讀取頭標資訊 3520 中的頭標識別符 "HEADID1"、"HEADID2"、"HEADID3" 至 "HEADIDx"。選擇方法並不限於此，且任何方法均適用，只要難以由第三者猜測出選出的識別符為何便可。

接下來，取得單元 3601 將從錄製在 DVD 3500 上的第一、第二至第 x 頭標群組中取回包括選出頭標識別符的一頭標群組，並且從該頭標群組中讀取一已加密選擇位置資訊、一頭標資訊、以及一簽章資訊。

隨後，取得單元 3601 將從 DVD 3500 讀取金鑰區塊

3510與已加密內容3580，並且對內容金鑰取得單元2602輸出讀取金鑰區塊3510、已加密內容、已加密選擇位置資訊、頭標資訊以及簽章資訊。

3.5 總結以及較佳效應

如以上所述，第三實施例的分散裝置3100將產生x個群組，其各由一已加密選擇位置資訊、一頭標資訊、以及一簽章資訊組成，且執行裝置將選擇該等x群組中之一，並且藉著利用選出群組的一已加密選擇位置資訊、一頭標資訊、以及一簽章資訊來驗證是否包括未授權內容。

因此，藉著增加用於驗證之代表性部份內容的份數，可以增加檢測未授權內容的準確度。再者，難以預測出在執行裝置3600中於該等第一至第x頭標群組中所選出的頭標群組，且因此可以避免包含把一份未用於驗證之部份內容置換置換為未授權內容的詐欺行為。

4.第四實施例

以下將根據本發明的第四實施例來說明一種未授權內容檢測系統。

4.1 未授權內容檢測系統

第四實施例的未授權內容檢測系統係由一分散裝置、一執行裝置、以及一監視器組成，如第一實施例一般。

分散裝置將根據操作者進行的運作取得內容，並且加密

取得的內容來產生已加密內容。

此外，分散裝置將把內容劃分為多份部份內容，並且根據該等部份內容的所有部分產生用以檢測未授權內容是否包括該內容中的資訊，以及用以證明該等內容係由合法權所有者發布的簽章資訊等等。分散裝置將把已產生已加密內容、簽章資訊等寫入到 DVD 中。

將透過分散通路把該 DVD 販售或分散給使用者。

當載入到 DVD 中時，執行裝置將從組成該等內容的多份部份內容中選出某些，並且僅利用選出部份內容來驗證頭標資訊。

以下將詳細說明組成本實施例之未授權內容檢測系統的個別裝置以及 DVD。

4.2 分散裝置 4100

第 41 圖展示出第四實施例中分散裝置的結構。如第 41 圖所示，分散裝置 4100 係由輸入單元 4101、內容金鑰產生單元 4102、金鑰區塊產生單元 4103、執行裝置資訊儲存單元 4104、部份內容產生單元 4105、頭標資訊產生單元 4107、簽章資訊產生單元 4108、簽章金鑰儲存單元 1112、加密處理單元 4109、以及記錄單元 4114 組成。

以下將說明構成分散裝置 4100 的個別部件。要注意的是，因為執行裝置資訊儲存單元 1104 與簽章金鑰儲存單元 1112 與第一實施例中的相同，在此將省略該等部件的說明。

4.2.1 輸入單元 4101

輸入單元 4101 將根據分散裝置 4100 之操作者的運作從外部裝置或外部記錄媒體取得內容。在此取得的內容為執行裝置 4600 可播放的格式(如以下將詳細說明地)，且 DVD-視訊格式以及 MPEG-2(移動圖象專家組格式 2)格式為該等可播放格式的實例。

輸入單元 4101 將對內容金鑰產生單元 4102 輸出所取得的內容。

4.2.2 內容金鑰產生單元 4102

內容金鑰產生單元 4102 將接收來自輸入單元 4101 的內容。當接收到該等內容時，內容金鑰產生單元 4102 將產生一擬隨機數，且藉著使用該已產生的擬隨機數產生一個 128 位元長度的內容金鑰"CK"。並非為一個擬隨機數，可產生一真實隨機數，例如藉著使用信號中的雜音。

接下來，內容金鑰產生單元 4102 將輸出已產生的內容金鑰"CK"以及已接收內容 2120 到金鑰區塊產生單元 4103。

4.2.3 金鑰區塊產生單元 4103

金鑰區塊產生單元 4103 將從內容金鑰產生單元 4102 接收內容金鑰"CK"以及內容。當接收到內容金鑰"CK"以及內容時，金鑰區塊產生單元 4103 將藉著使用已接收內容金鑰"CK"以及儲存在執行裝置資訊儲存單元 1104 中的裝置

識別表來產生一金鑰區塊。因為用以產生金鑰區塊的特定程序與第一實施例中金鑰區塊產生單元 1103 所進行的相同，在此便省略其說明。

接下來，金鑰區塊產生單元 4103 將把已產生金鑰區塊、已接收內容金鑰"CK"以及內容輸出到部份內容產生單元 4105。

4.2.4 部份內容產生單元 4105

部份內容產生單元 4105 將接收來自金鑰區塊產生單元 4103 的金鑰區塊、內容金鑰"CK"、以及內容。

當接收該等資訊時，部份內容產生單元 4105 將把已接收內容劃分為 c 個部份內容"CNT1"、"CNT2"、"CNT3"至"CNTc"。例如，當該等內容為 DVD-視訊格式時，VOB 或 VOBU 可作為分離單元。另一方面，當該等內容為 MPEG-2 格式時，GOP(圖像群組)、欄位、訊框、或內部圖像可用來作為分離單元。替代地，不管內容格式為何，可依據每 64 千位元組來劃分該等內容，或者依據對應於二分之一播放時間的每個部分。此時點產生的 c 個部份內容整體地稱為一分離內容。

接下來，部份內容產生單元 4105 將產生數個識別資訊"AD1"、"AD2"、"AD3"至"ADc"，其分別地對應於已產生的 n 個部份內容。各個識別資訊為獨特地識別出一對應部份內容的資訊，且例如為來自該等內容標題的一差距值、或者參照該等內容標題指定之部份內容的一播放開始點。

第 42 圖展示出在此時點產生的分離內容以及識別資訊部分。分離內容 4120 係由 c 個部份內容"CNT1"4121、"CNT2"4122、"CNT3"4123、至"CNTc"4127 組成。各個部份內容對應於一份識別資訊。例如，一份識別資訊"AD1"4131 為用以識別部份內容"CNT1"4121 的資訊。

接下來，部份內容產生單元 4105 將輸出已產生的 c 個識別資訊、分離內容 4120、已接收金鑰區塊以及內容金鑰"CK"到頭標資訊產生單元 4107。

4.2.5 頭標資訊產生單元 4107

頭標資訊產生單元 4107 將接收來自部份內容產生單元 4105 的 c 個識別資訊"AD1"、"AD2"、"AD3"至"ADc"、分離內容 4120、金鑰區塊、以及內容金鑰"CK"。

當接收該等資訊時，頭標資訊產生單元 4107 將使用一隨機數來產生獨特地識別出識別資訊"AD1"的一識別資訊識別符"ADID1"。

在此，一對已產生識別資訊識別符"ADID1"與已接收識別資訊"AD1"係稱為"一份內容檢測資訊"。

接下來，頭標資訊產生單元 4107 將根據已接收的識別資訊"AD1"從分離內容 4120 中摘取出部份內容"CNT1"4121，並且藉著把已摘取部份內容"CNT1"4121 指派給雜湊函數來計算一部份雜湊值"HA1"。在此，一對已產生識別資訊識別符"ADID1"與已計算雜湊值"HA1"係稱

為"一份部分雜湊資訊"。

頭標資訊產生單元 4107 將針對剩餘的識別資訊"AD2"、"AD3"至"ADc"重複進行相同類型的處理動作，以產生數份內容檢測資訊以及數份部分雜湊資訊。

接下來，頭標資訊產生單元 4107 將產生由已產生的 c 個內容檢測資訊構成的內容位置資訊。第 43 圖展示出在此時點產生之內容位置資訊的結構。內容位置資訊 4140 係由 c 個內容檢測資訊 4141、4142、4143 至 4146 組成。各個內容檢測資訊包括一識別資訊識別符以及一識別資訊。舉一實例來說，內容檢測資訊 4141 包括識別資訊識別符"ADID1"4151 以及識別資訊"AD1"4131。

隨後，頭標資訊產生單元 4107 將產生由已產生的 c 個部分雜湊資訊構成的頭標資訊。第 44 圖展示出在此時點產生之頭標資訊的結構。頭標資訊係由 c 個部分雜湊資訊 4161、4162、4163 至 4166 構成。各個部分雜湊資訊包括一識別資訊識別符以及一部份雜湊值，且對應於構成內容位置資訊 4140 的一份內容檢測資訊。例如，部分雜湊資訊 4161 包括識別資訊識別符"ADID1"4171 以及部份雜湊值"HA1"4172。

接下來，頭標資訊產生單元 4107 將對簽章資訊產生單元 4108 輸出已產生內容位置資訊 4140、頭標資訊 4160、已接收分離內容 4120、金鑰區塊以及內容金鑰"CK"。

4.2.6 簽章資訊產生單元 4108

簽章資訊產生單元 4108 將接收來自頭標資訊產生單元 4107 的內容位置資訊 4140、頭標資訊 4160、分離內容 4120、金鑰區塊以及內容金鑰"CK"。

當接收該等資訊時，簽章資訊產生單元 4108 將摘取出包括在構成已接收頭標資訊 4160 之個別部分雜湊資訊中的雜湊值。簽章資訊產生單元 4108 將藉著對雜湊函數分派由合併已摘取 c 個部份雜湊值"HA1"、"HA2"、"HA3"至"HAc"形成的一已合併結果來產生一合併雜湊值。

接下來，簽章資訊產生單元 4108 將從簽章金鑰儲存單元 1112 讀取簽章金鑰 1113，並且藉著使用讀取簽章金鑰 1113 而對已產生合併雜湊值套用簽章產生演算法 S 來產生簽章資訊。

當已產生簽章資訊時，簽章資訊產生單元 4108 將對加密處理單元 4109 輸出已產生簽章資訊、已接收內容位置資訊 4140、頭標資訊 4160、分離內容 4120、金鑰區塊、以及內容金鑰"CK"。

4.2.7 加密處理單元 4109

加密處理單元 4109 將從簽章資訊產生單元 4108 接收簽章資訊、內容位置資訊 4140、頭標資訊 4160、分離內容 4120、金鑰區塊、以及內容金鑰"CK"。

當接收該等資訊時，加密處理單元 4109 將藉著對構成已接收分離內容 4120 的部份內容"CNT1"4121 套用加密演算法來產生已加密部份內容"ECNT1"。加密處理單元 4109

將針對部份內容"CNT2"4122、"CNT3"4123、至"CNTc"4127重複進行相同類型的處理動作，以產生已加密部份內容"ECNT2"、"ECNT3"至"ECNTc"。

接下來，加密處理單元 4109 將產生由已產生的 C 個已加密部份內容"ECNT1"、"ECNT2"、"ECNT3"至"ECNTc"構成的已加密內容。在此時點產生的已加密內容具有相同於第二實施例之已加密內容 2220(第 32 圖)的結構。

接下來，加密處理單元 4109 將對記錄單元 4114 輸出已產生已加密內容、已接收簽章資訊、內容位置資訊 4140、頭標資訊 4160、以及金鑰區塊。

4.2.8 記錄單元 4114

記錄單元 4114 係載入到一 DVD 中。

記錄單元 4114 將從加密處理單元 4109 接收已加密內容、簽章資訊、內容位置資訊 4140、頭標資訊 4160 以及金鑰區塊。

當接收該等資訊時，記錄單元 4114 將把已接收已加密內容、簽章資訊、內容位置資訊 4140、頭標資訊 4160、以及金鑰區塊寫入到 DVD 中。

4.3 DVD 4500

第 45 圖展示出第四實施例中儲存在 DVD 上的資訊。如第 45 圖所示，DVD 4500 將儲存金鑰區塊 4510、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 以及已加密內

容 4580。

已經由分散裝置 4100 寫入該等資訊。該等資訊的結構均如上所述，且因此在此省略其說明。

4.4 執行裝置 4600

第 46 圖展示出第四實施例中執行裝置的結構。如第 46 圖所示，執行裝置 4600 係由取得單元 4601、內容金鑰取得單元 4602、裝置金鑰儲存單元 1604、簽章資訊驗證單元 4606、驗證金鑰儲存單元 1612、選擇單元 4611、部份內容解密單元 4616、頭標資訊驗證單元 4617、以及執行單元 2618 組成。

以下將詳細說明組成執行裝置 4600 的個別部件。要注意的是，因為裝置金鑰儲存單元 1604 以及驗證金鑰儲存單元 1612 與構成第一實施例之執行裝置 1600 的單元相同，且執行單元 2618 與第二實施例中的相同，在此便省略該等部件的說明。

4.4.1 取得單元 4601

將把取得單元 4601 載入到 DVD 4500 中。當檢測到已載入到 DVD 4500 中時，取得單元 4601 將讀取金鑰區塊 4510、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 以及已加密內容 4580，並且輸出已讀取金鑰區塊 4510、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 以及已加密內容 4580 到內容金鑰取得單元 4602。

4.4.2 內容金鑰取得單元 4602

內容金鑰取得單元 4602 將從取得單元 4601 接收金鑰區塊 4510、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 以及已加密內容 4580。

當接收到該等資訊時，內容金鑰取得單元 4602 將藉著利用已接收金鑰區塊 4510 以及裝置金鑰儲存單元 1604 儲存的裝置識別符"AID_p"與裝置金鑰"DK_p"來產生內容金鑰"CK"。因為用以產生內容金鑰"CK"的程序與構成第一實施例之執行裝置 1600 之內容金鑰取得單元 1602 所進行的內容金鑰"CK"產生程序相同，在此便省略其說明。

接下來，內容金鑰取得單元 4602 將對簽章資訊驗證單元 4606 輸出已產生內容金鑰"CK"、已接收內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570、以及已加密內容 4580。

4.4.3 簽章資訊驗證單元 4606

簽章資訊驗證單元 4606 將接收來自內容金鑰取得單元 4602 的內容金鑰"CK"、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 以及已加密內容 4580。

當接收到該等資訊時，簽章資訊驗證單元 4606 將在下列程序中驗證簽章資訊 4570。

首先，簽章資訊驗證單元 4606 將從構成已接收頭標資訊的個別部分雜湊資訊摘取出部份雜湊值，並且藉著對雜

湊函數指派一合併結果來計算簽章驗證合併雜湊值，其係藉著合併已摘取部份雜湊值"HA1"、"HA2"、"HA3"至"HAc"而形成。

接下來，簽章資訊驗證單元 4606 將從驗證金鑰儲存單元 1612 讀取驗證金鑰 1613，並且藉著對計算出的簽章驗證合併雜湊值套用簽章驗證演算法來產生簽章驗證資訊。隨後，簽章資訊驗證單元 4606 將比較已產生簽章驗證資訊以及已接收簽章資訊。當該等二者並不相符時，簽章資訊驗證單元 4606 便判斷出驗證簽章資訊 4570 的動作並不成功，並且中止執行裝置 4600 的後續處理動作。

當該等二者相符時，簽章資訊驗證單元 4606 便判斷出驗證簽章資訊 4570 的動作成功，且對選擇單元 4611 輸出已接收內容金鑰"CK"、內容位置資訊 4530、頭標資訊 4550 以及已加密內容 4580。

4.4.4 選擇單元 4611

選擇單元 4611 將從簽章資訊驗證單元 4606 接收內容金鑰"CK"、內容位置資訊 4530、頭標資訊 4550、以及已加密內容 4580。

當接收到該等資訊時，選擇單元 4611 將從下列程序中從已接收內容位置資訊 4530 產生選擇位置資訊。第 47 圖展示出選擇單元 4611 進行之選擇位置資訊 4620 產生程序的大致概要以及在此時點產生之選擇位置資訊的結構。以下將藉由第 47 圖的輔助來說明選擇位置資訊的產生程序。

選擇單元 4611 將使用隨機數從構成已接收內容位置資訊 4530 的 c 個內容檢測資訊 4531、4532、4533 至 4536 選擇 k 個。選擇方法並不限於此，且任何方法均適用，只要難以預測哪些檔案識別符為選出識別符即可。

第 47 圖展示出當中已經選出包括數個內容檢測資訊 4531、4533 與 4536 的 k 個資訊。

接下來，選擇單元 4611 將產生由選出的 k 個內容檢測資訊 4531、4533 至 4536 組成的選擇位置資訊 4620。

接下來，選擇單元 4611 將根據已接收頭標資訊 4550 在下列程序中產生選擇頭標資訊。第 48 圖展示出一種用以產生選擇頭標資訊之程序的大致概要，以及選擇頭標資訊的結構。以下將藉由第 48 圖的輔助來說明選擇頭標資訊的產生程序。

首先，選擇單元 4611 將從構成已產生選擇位置資訊 4620 的各個內容檢測資訊 4531、4532 至 4536 中摘取出一識別資訊識別符，並且進一步摘取出數個部分雜湊資訊 4551、4553 至 4556，其包括與已摘取識別資訊識別符"ADID1"、"ADID3"至"ADIDc"相同的識別資訊識別符。

接下來，選擇單元 4611 將產生由已摘取部分雜湊資訊 4551、4553 至 4556 組成的選擇頭標資訊 4630。

接下來，選擇單元 4611 將對部份內容解密單元 4616 輸出已產生選擇位置資訊 4620、選擇頭標資訊 4630、已接收內容金鑰"CK"、以及已加密內容 4580。

4.4.5 部份內容解密單元 4616

部份內容解密單元 4616 將接收來自選擇單元 4611 的選擇位置資訊 4620、選擇頭標資訊 4630、內容金鑰"CK"、以及已加密內容 4580。

當接收到該等資訊時，部份內容解密單元 4616 將於下列程序中產生驗證內容。第 49 圖展示出一種用以產生驗證內容之程序的大致概要，以及在此時點產生之驗證內容 4650 的結構。以下將藉由第 49 圖的輔助來說明用以產生驗證內容的程序。

首先，部份內容解密單元 4616 將從組成已接收選擇位置資訊 4620 的內容檢測資訊 4531 中摘取出識別資訊"AD1"，並且根據已摘取識別資訊"AD1"進一步地從已接收已加密內容 4580 中摘取出已加密部份內容"ECNT1"。

部份內容解密單元 4616 將藉著把解密演算法 D1 套用到已摘取部份內容"ECNT1"來產生部份內容"CNT1"。隨後，部份內容解密單元 4616 將產生包括在內容檢測資訊 4531 中識別資訊識別符"ADID1"以及已產生部份內容"CNT1"組成的驗證部份內容資訊 4651。

部份內容解密單元 4616 將針對剩下的內容檢測資訊 4532 至 4536 重複進行相同類型的處理動作，以產生驗證部份內容資訊 4652 至 4656。接下來，部份內容解密單元 4616 將產生由已產生 k 個驗證部份內容資訊構成的驗證內容 4650。

當已產生驗證內容 4650 時，部份內容解密單元 4616

將對頭標資訊驗證單元 4617 輸出已產生驗證內容 4650、已接收選擇頭標資訊 4630、內容金鑰"CK"、以及已加密內容 4580。

4.4.6 頭標資訊驗證單元 4617

頭標資訊驗證單元 4617 將接收來自部份內容解密單元 4616 的驗證內容 4650、選擇頭標資訊 4630、內容金鑰"CK"、以及已加密內容 4580。

當接收到該等資訊時，頭標資訊驗證單元 4617 將藉著把構成已接收驗證內容 4650 第一份驗證部份內容資訊 4651 中包括的部份內容"CNT1"4624 指派給雜湊函數來產生一驗證雜湊值"H1"。

接下來，頭標資訊驗證單元 4617 將摘取出包括在驗證部份內容資訊 4651 中的識別資訊識別符"ADID1"4621。隨後，頭標資訊驗證單元 4617 將檢測部分雜湊資訊 4551，其包括從已接收選擇頭標資訊 4630 中摘取出之識別資訊識別符"ADID1"4621 的相同識別資訊識別符，並且摘取出包括在已檢測部分雜湊資訊 4551 中的一部份雜湊值"HA1"4632。接下來，頭標資訊驗證單元 4617 將比較已摘取部份雜湊值"HA1"4632 以及已計算驗證雜湊值"H1"。

頭標資訊驗證單元 4617 將針對剩餘的驗證部份內容資訊 4652 至 4656 重複進行相同類型的處理動作，並且比較一部份雜湊值以及一驗證雜湊值達 k 次。

當比較一部份雜湊值以及一驗證雜湊值 k 次而即使有

一次彼此並不相符時，頭標資訊驗證單元 4617 便中止執行裝置 4600 中的後續處理動作。

當所有部份雜湊值與驗證雜湊值在 k 次比較中相符時，頭標資訊驗證單元 4617 將輸出已接收內容金鑰"CK"以及已加密內容 4580 到執行單元 4618。

4.5 運作性行為

以下將說明分散裝置 4100 以及執行裝置 4600 的運作性行為。

4.5.1 分散裝置 4100 的運作性行為

第 50 圖為一流程圖，其展示出分散裝置 4100 的運作性行為，而第 51 圖展示出由分散裝置 4100 之運作性行為中的處理內容流程。

以下將藉由第 50 圖以及第 51 的輔助來說明分散裝置 4100 的運作性行為。

輸入單元 4101 將取得內容(步驟 S4012)，並且輸出已取得內容到內容金鑰產生單元 4102。

內容金鑰產生單元 4102 將接收內容、藉著使用一隨機數來產生內容金鑰(步驟 S4013)、並且輸出已產生內容金鑰以及已接收內容到金鑰區塊產生單元 4103。

當接收到該等內容金鑰與內容時，金鑰區塊產生單元 4103 將產生一金鑰區塊，並且輸出已產生金鑰區塊、已接收內容金鑰以及內容到部份內容產生單元 4105(步驟

S4014)。

部份內容產生單元 4105 將接收來自金鑰區塊產生單元 4103 的金鑰區塊、內容金鑰與內容。接下來，部份內容產生單元 4105 將把已接收內容 4119(如第 51 圖所示)劃分為產生 C 個部份內容(步驟 S4016)，並且把已產生的 C 個部份內容置放在一起以形成分離內容 4120。接下來，部份內容產生單元 4105 將產生分別地對應於已產生 C 個部份內容的數份識別資訊(步驟 S4018)，並且輸出已產生分離內容 4120、C 個識別資訊、已接收金鑰區塊、內容金鑰以及內容到頭標資訊產生單元 4107。

頭標資訊產生單元 4107 將接收來自部份內容產生單元 4105 的分離內容、C 個識別資訊、金鑰區塊以及內容金鑰，產生分別地對應於已接收識別資訊的識別資訊識別符，並且進一步產生包括已產生識別資訊識別符以及數份識別資訊的內容位置資訊 4140。再者，如第 51 圖所示，頭標資訊產生單元 4107 將藉著個別地把構成已接收分離內容 4120 的 C 個部份內容指派給雜湊函數來計算 C 個部份雜湊值，並且產生包括已計算 C 個部份雜湊值的頭標資訊 4160(步驟 S4019)。接下來，頭標資訊產生單元 4107 將對簽章資訊產生單元 4108 輸出已產生內容位置資訊 4140、頭標資訊 4160、已接收金鑰區塊以及內容金鑰。

簽章資訊產生單元 4108 將接收來自頭標資訊產生單元 4107 的內容位置資訊 4140、頭標資訊 4160、金鑰區塊以及內容金鑰。如第 51 圖所示，簽章資訊產生單元 4108 將

摘取已接收頭標資訊中包括的 c 個部份雜湊值、合併所摘取出的 c 個部份雜湊值，並且藉著把已合併結果指派給雜湊函數來計算一已合併雜湊值(步驟 S4021)。

接下來，簽章資訊產生單元 4108 將從簽章金鑰儲存單元 1112 讀取簽章金鑰 1113(步驟 S4022)。如第 51 圖所示，簽章資訊產生單元 4108 將藉著讀取簽章金鑰 1113 而對已產生合併雜湊值套用簽章產生演算法來產生簽章資訊 4170(步驟 S4023)。

接下來，簽章資訊產生單元 4108 將對加密處理單元 4109 輸出已產生簽章資訊、已接收內容位置資訊 4140、頭標資訊 4160、分離內容 4120 以及內容金鑰。

加密處理單元 4109 將接收簽章資訊、內容位置資訊 4140、頭標資訊 4160、分離內容 4120 以及內容金鑰，並且藉著使用已接收內容金鑰來加密構成分離內容 4120 的個別部份內容來產生已加密內容(步驟 S4024)。加密處理單元 4109 將對記錄單元 4114 輸出已產生已加密內容、已接收簽章資訊、內容位置資訊 4140、頭標資訊 4160、以及金鑰區塊。

記錄單元 4114 將接收已加密內容、簽章資訊、內容位置資訊 4140、頭標資訊 4160 與金鑰區塊，並且把已接收金鑰區塊、內容位置資訊 4140、頭標資訊 4160、簽章資訊、已加密內容寫入到 DVD 4500(步驟 S4026)。

4.5.2 執行裝置 4600 的運作性行為

第 52 圖與第 53 圖為展示出執行裝置 4600 之運作性行為的流程圖。第 54 圖展示出構成執行裝置 4600 之個別部件處理的資訊。要注意的是，第 52 圖至第 54 圖中的相同參考步驟編號係表示相同的處理動作。

以下將藉由第 52 圖至第 54 的輔助來說明執行裝置 4600 的運作性行為。

當載入到 DVD 4500 中時，取得單元 4601 將從 DVD 4500 讀取金鑰區塊 4510、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570、以及已加密內容 4580(步驟 S4041)，並且輸出該等已讀取的資訊到內容金鑰取得單元 4602。

內容金鑰取得單元 4602 將接收金鑰區塊 4510、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 與已加密內容 4580，並且藉著利用裝置金鑰儲存單元 1604 儲存的已接收金鑰區塊 4510、裝置識別符與裝置金鑰來產生內容金鑰(步驟 S4042)。接下來，內容金鑰取得單元 4602 將對簽章資訊驗證單元 4606 輸出已產生內容金鑰、已接收內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 以及已加密內容 4580。

簽章資訊驗證單元 4606 將接收內容金鑰、內容位置資訊 4530、頭標資訊 4550、簽章資訊 4570 與已加密內容 4580，合併包括在已接收頭標資訊 4550 中的 c 個部份雜湊值，並且藉著把合併結果指派給雜湊函數來產生一簽章驗證合併雜湊值(步驟 S4043)。接下來，簽章資訊驗證單元

4606 將從驗證金鑰儲存單元 1612 讀取驗證金鑰 1613(步驟 S4044)，並且藉著利用讀取驗證金鑰 1613 以及已產生簽章驗證合併雜湊值來驗證已接收簽章資訊 4570(步驟 S4046)。

如果驗證簽章資訊 4570 的動作不成功的話(步驟 S4048：否)，簽章資訊驗證單元 4606 便中止執行裝置 4600 的後續處理動作。

如果驗證簽章資訊 4570 的動作成功的話(步驟 S4048：是)，簽章資訊驗證單元 4606 便對選擇單元 4611 輸出已接收內容金鑰、內容位置資訊 4530、頭標資訊 4550 與已加密內容 4580。

當接收到內容金鑰、內容位置資訊 4530、頭標資訊 4550 以及已加密內容 4580 時，選擇單元 4611 將從包括在內容位置資訊 4530 中的 c 個內容檢測資訊選出 k 個(步驟 S4049)。接下來，選擇單元 4611 將產生由選出內容檢測資訊構成的選擇位置資訊 4620(步驟 S4051)。隨後，選擇單元 4611 將根據構成已產生選擇位置資訊 4620 之 k 個內容檢測資訊中包括的識別資訊識別符從已接收頭標資訊 4550 中選出 k 個部分雜湊資訊(步驟 S4053)，並且產生由選出 k 個部分雜湊資訊構成的選擇頭標資訊 4630(步驟 S4056)。接下來，選擇單元 4611 將對部份內容解密單元 4616 輸出已產生選擇位置資訊 4620、選擇頭標資訊 4630、已接收內容金鑰以及已加密內容 4580。

部份內容解密單元 4616 將接收選擇位置資訊 4620、選

擇頭標資訊 4630、內容金鑰與已加密內容 4580，並且根據已接收選擇位置資訊 4620 中包括的數份識別資訊從已加密內容 4580 中摘取出 k 個已加密部份內容 4581、4582、4583 至 4586(步驟 S4057)，如第 54 圖所示。接下來，部份內容解密單元 4616 將藉著解密所摘取出的 k 個已加密部份內容 4581、4582、4583 至 4586 來產生數份部份內容(步驟 S4059)。接下來，部份內容解密單元 4616 將產生含有包括在已接收選擇位置資訊 4620 與已產生 k 個部份內容中之 k 個識別資訊識別符的驗證內容 4650(步驟 S4061)。部份內容解密單元 4616 將對頭標資訊驗證單元 4617 輸出已產生驗證內容 4650、已接收選擇頭標資訊 4630、內容金鑰與已加密內容 4650。

頭標資訊驗證單元 4617 將接收驗證內容 4650、選擇頭標資訊 4530、內容金鑰以及已加密內容 4580。當接收到該等資訊時，頭標資訊驗證單元 4617 將藉著個別地把已接收驗證內容 4650 中包括的 k 個部份內容 4591、4592、4593 至 4596 指派給雜湊函數來產生 k 個驗證雜湊值(步驟 S4062)，並且個別地比較包括在已接收頭標資訊與對應已產生驗證雜湊值中的 k 個部份雜湊值(步驟 S4064：是)。

在比較各由一驗證雜湊值以及一對應部份雜湊值組成的 k 對部份雜湊值時，當任一對彼此並不相符時(步驟 S4066：否)，頭標資訊驗證單元 4617 便中止執行裝置 4600 的後續處理動作。

在比較 k 對部份雜湊值時，當所有 K 對均相符時(步驟

S4066：是)，頭標資訊驗證單元 4617 便對執行單元 2618 輸出已接收內容金鑰以及已加密內容 4580。

執行單元 2618 將接收來自頭標資訊驗證單元 4617 的內容金鑰與已加密內容 4580、藉著使用已接收內容金鑰來解密構成已接收已加密內容 4580 的個別已加密部份內容來產生由 c 個部份內容構成的內容(步驟 S4067)、擴展已產生內容(步驟 S4068)，並且使監視器播放已擴展內容(步驟 S4071)。

4.6 總結以及較佳效應

如以上所述，第四實施例的未授權內容檢測系統係由分散裝置 4100 以及執行裝置 4600 組成，且分散裝置 4100 將藉著劃分該等內容來產生 c 個部份內容，並且進一步藉著使用所有已產生的 c 個部份內容來產生頭標資訊與驗證資訊。

執行裝置 4600 將從構成已加密內容的 c 個已加密部份內容中選出 k 個，並且從包括在頭標資訊中的 c 個部份雜湊值中摘取出對應於選出 k 個部份內容的 k 個部份雜湊值。執行裝置 4600 僅藉著使用已摘取的 k 個部份雜湊值來驗證選出的 k 個已加密部份內容。只有在驗證動作成功時，執行裝置 4600 才藉著解密已加密內容來產生內容並且播放已解密內容。

因此，藉著把用以驗證是否包括未授權內容之已加密部份內容數量限制在 k 個，便可以降低驗證動作中包含的處

理負載。

藉著使用隨機數來選擇一份不同已加密部份內容，每當執行裝置 4600 進行驗證動作時，便可以補充檢測未授權內容準確度的降低，因為僅把用以驗證已加密部份內容數量限制在 k 個。

此外，難以預測哪些已加密部份內容欲用來進行驗證動作，且因此可以避免把構成已加密內容的數份已加密部份內容置換為未授權內容的詐欺行為，尤其是並不會用來進行驗證的已加密部份內容。

5.第五實施例

以下將根據本發明的第五實施例來說明一種未授權內容檢測系統。

5.1 未授權內容檢測系統

第五實施例的未授權內容檢測系統係由一分散裝置、一執行裝置、以及一監視器組成，如第一實施例一般。

分散裝置將根據操作者進行的運作取得內容，並且加密取得內容來產生已加密內容。此外，分散裝置將產生用以在執行裝置中驗證內容有效性的單元檢選資訊、頭標資訊與簽章資訊。

分散裝置將取得 DVD 上可寫入區域的儲存容量以及已產生各種不同資訊的資料大小。

分散裝置將藉著從已取得儲存容量減去各種不同資訊

之已取得資料大小的總合來計算一填充容量、產生具有對應於已計算填充容量之資料大小的填充內容，並且把已產生填充內容以及各種不同資訊一同寫入到 DVD 中。

5.2 分散裝置 5100

第 55 圖展示出第五實施例中分散裝置的結構。如第 55 圖所示，分散裝置 5100 係由輸入單元 1101、內容金鑰產生單元 1102、金鑰區塊產生單元 1103、執行裝置資訊儲存單元 1104、單元產生單元 5105、加密處理單元 5106、頭標資訊產生單元 5107、填充內容產生單元 5108、簽章資訊產生單元 5111、簽章金鑰儲存單元 1112、以及記錄單元 5114 組成。

以下將說明構成分散裝置 5100 的個別部件。要注意的是，因為輸入單元 1101、內容金鑰產生單元 1102、金鑰區塊產生單元 1103、執行裝置資訊儲存單元 1104 以及簽章金鑰儲存單元 1112 與第一實施例中的分散裝置 1100 相同，在此將省略該等部件的說明。

5.2.1 單元產生單元 5105

如第一實施例中說明的單元產生單元 1105，單元產生單元 5105 將從輸入單元 1101 接收由 c 個檔案"CNT1"、"CNT2"、"CNT3"等構成的內容，並且藉著使用已接收內容來產生單元檢選資訊與分離內容。用以產生單元檢選資訊與分離內容的程序與第一實施例之單元產生單

元 1105 進行的相同，且在此產生之單元檢選資訊與分離內容的結構即如分別於第 6 圖與第 7 圖中的一般，且因此省略其說明。

接下來，單元產生單元 5105 將對加密處理單元 5106 輸出已產生分離內容，而且填充內容產生單元 5108 輸出已產生單元檢選資訊。

5.2.2 加密處理單元 5106

加密處理單元 5106 接收來自單元產生單元 5105 的分離內容，並且根據已接收分離內容來產生已加密分離內容與已加密內容。用以產生該等已加密分離內容與已加密內容的程序與第一實施例之加密處理單元 1106 進行的相同，且此處已產生已加密內容與已加密分離內容的結構即如分別於第 9 圖與第 10 圖中的一般，且因此省略其說明。

接下來，加密處理單元 5106 將對頭標資訊產生單元 5107 輸出已產生已加密分離內容，而對記錄單元 5114 以及填充內容產生單元 5108 輸出已產生已加密內容。

5.2.3 填充內容產生單元 5108

填充內容產生單元 5108 將預存金鑰區塊大小"KBSIZE"、檔案資訊大小"FISIZE"、單元雜湊大小"USIZE"、檔案雜湊大小"FSIZE"、比率"RT"、以及一差別數"j"。

單元雜湊大小"USIZE"展示出構成頭標資訊產生單元

5107 產生之第一雜湊表之數個單元雜湊資訊的資料大小。確切來說，此處的單元雜湊資訊與第一實施例之頭標資訊產生單元 1107 產生的單元雜湊資訊相同。

檔案雜湊大小"FSIZE"展示出由頭標資訊產生單元 5107 產生之第二雜湊表構成之數個檔案雜湊資訊的位元長度。確切來說，此處的檔案雜湊資訊與第一實施例之頭標資訊產生單元 1107 產生的檔案雜湊資訊相同。

當簽章資訊產生單元 5111 藉著對資訊 A 套用簽章產生演算法 S 來產生簽章 SignA 時，比率"RT"展示出資訊 A 以及簽章 SignA 之間的位元長度比率。

差別數"j"為劃分填充內容之填充內容產生單元 5108 產生的單元數量(如以下詳細說明地)。

此外，填充內容產生單元 5108 將預儲存 56 位元長度播放不能實行資訊"DAMY"，其指出該等填充內容並無法被播放。

填充內容產生單元 5108 將接收來自單元產生單元 5105 的單元檢選資訊，而同時接收來自加密處理單元 5106 的已加密內容。

當接收到單元檢選資訊與已加密內容時，填充內容產生單元 5108 將藉著下列程序中使用已接收單元檢選資訊與已加密內容來計算一填充容量、根據計算出的填充容量來產生填充內容，並且更新單元檢選資訊。

以下將說明計算填充容量的動作(a)、產生填充內容的動作(b)、以及更新單元檢選資訊的動作(c)。

(a)填充容量計算動作

填充容量指出在已經對 DVD 寫入金鑰區塊、單元檢選資訊、頭標資訊、簽章資訊與已加密內容之後，該 DVD 上的閒置空間。以下將說明一種用以產生填充容量的程序。

首先，填充內容產生單元 5108 將透過記錄單元 5114 來測量載入到記錄單元 5114 中之 DVD 上可寫入區域的儲存容量，並且產生指出可用以寫入資訊到其中之容量的最大儲存容量"MSIZE"。在此，並不透過記錄單元 5114 來測量可寫入區域的儲存容量，而是藉著操作者的輸入來取得最大儲存容量"MSIZE"。

接下來，填充內容產生單元 5108 將測量已接收已加密內容的資料大小，並且產生內容大小"CNTSIZE"。

接下來，填充內容產生單元 5108 將計算包括在已接收內容檢選資訊中的檔案資訊數量"c"，並且在利用下列的方程式進行更新之後(將在以下的單元檢選資訊更新動作(c)中詳細說明)，計算單元檢選資訊的資料大小"UCSIZE"：

UCSIZE = FISIZE x (c+1)。

接下來，填充內容產生單元 5108 將摘取出包括在已接收單元檢選資訊中的 c 個單元編號"N1"、"N2"、"N3"至"Nc"，並且藉著使用已摘取的單元編號"N1"、"N2"、"N3"至"Nc"以及已儲存的差別數"j"而利用下列方程式來計算頭標資訊產生單元 5107 產生之(c+1)個第一雜湊表之資料大小的總和"HA1SIZE"(如以下詳細說明的)：

HA1SIZE = [N1 + N2 + N3 + ... + Nc + j] x USIZE。

後續地，填充內容產生單元 5108 將產生由頭標資訊單元 5107 利用下列方程式產生之第二雜湊表的資料大小"HA2SIZE"(如以下詳細說明的)：

HA2SIZE = FSIZE x (c+1)，

並且藉著利用下列方程式從第一雜湊表之資料大小"HA1SIZE"以及第二雜湊表之資料大小"HA2SIZE"的已產生總和來計算頭標資訊產生單元 5107 產生之頭標資訊的資料大小"HEADSIZE"：

HEADSIZE = HA1SIZE + HA2SIZE。

接下來，填充內容產生單元 5108 將藉著下列方程式而使用比率"RT"來計算"SigSIZE"，其指出簽章資訊產生單元 5111 產生之簽章資訊的資料大小：

SigSIZE = (UCSIZE + HA2SIZE) x RT。

接下來，填充內容產生單元 5108 將藉著利用下列方程式來計算填充容量"FilSIZE"：

FilSIZE = MSIZE - [KBSIZE + UCSIZE + HEADSIZE + SigSIZE]。

(b)填充內容產生動作

當已經計算出填充容量"FilSIZE"時，填充內容產生單元 5108 將產生一隨機數，並且把已產生隨機數與播放不可實行資訊"DAMY"合併以產生資料大小為"FilSIZE"的填充內容。

接下來，填充內容產生單元 5108 將產生用以特別指出已產生填充內容的檔案識別符"FIDf"以及用以識別已產生填充內容的檔案識別資訊"ADf"。接下來，填充內容產生單元 5108 將根據已儲存的差別數"j"把已產生分離內容劃分為 j 個單元"Uf_1"、"Uf_2"、"Uf_3"至"Uf_j"，並且產生單元識別符"UIDf_1"、"UIDf_2"、"UIDf_3"至"UIDf_j"，其各對應於該等單元中之一。在此，一單元以及一對應單元識別符係稱為"一份單元資訊"。此外，填充內容產生單元 5108 將產生由 j 個單元資訊組成的分離填充內容。第 56 圖展示在此時點產生之分離填充內容的結構。如第 56 圖所示，分離填充內容 5120 係由多個單元資訊 5121、5122、5123 至 5126 組成，且各個單元資訊包括一單元識別符以及一單元。例如，單元資訊 5121 包括單元識別符"UIDf_1"5131 以及單元"Uf_1"5132。用以從填充內容中產生分離填充內容的程序與用以從一檔案產生分離檔案的程序相同，且因此在此僅提供簡單的說明。

在此，一對已產生檔案識別符"FIDf"以及分離填充內容 5120 係稱為"填充檔案資訊"。

(c)單元檢選資訊更新動作

在已產生填充內容以及分離填充內容 5120 之後，填充內容產生單元 5108 將產生由已產生檔案識別符"FIDf"構成的一份檔案資訊、已產生的檔案識別資訊"ADf"、以及指出已產生單元數量的單元編號"Nf"，並且把已產生檔案資訊

加入到已接收單元檢選資訊中。第 57 圖展示出已對其加入已產生檔案資訊後的單元檢選資訊 5140。單元檢選資訊 5140 係由(c+1)份檔案資訊 5141、5142、5143、至 5146 與 5147 組成，且各個檔案資訊包括一檔案識別符、一檔案識別資訊、以及一單元編號。數份檔案資訊 5141、5142、5143 至 5146 係由單元產生單元 5105 根據該等內容而產生，且與展示於第 7 圖中之構成單元檢選資訊 1200 的數份檔案資訊 1201、1202、1203 至 1204 相同。檔案資訊 5147 係由填充內容產生單元 5108 根據該等填充內容而產生，且包括對應於填充內容的一檔案識別符"FIDf"5151、一檔案識別資訊"AD1"5152、以及一單元編號"Nf"5153。

接下來，填充內容產生單元 5108 將對記錄單元 5114 輸出已產生填充內容以及單元檢選資訊 5140、對頭標資訊產生單元 5107 輸出已產生填充檔案資訊、並且對簽章資訊產生單元 5111 輸出單元檢選資訊 5140。

5.2.4 頭標資訊產生單元 5107

頭標資訊產生單元 5107 將接收來自加密處理單元 5106 的已加密分離內容，而同時從填充內容產生單元 5108 接收包括檔案識別符"FIDf"以及分離填充內容 5120 的填充檔案資訊 5156。

當接收到填充檔案資訊 5156 以及已加密分離內容 5160 時，頭標資訊產生單元 5107 將從已接收資訊中產生頭標資訊 5190，如第 58 圖所示。第 58 圖展示出頭標資訊

產生單元 5107 進行之頭標資訊 5109 產生程序的大致概要。以下將藉由第 58 圖的輔助來說明頭標資訊 5190 的產生程序。

頭標資訊產生單元 5107 將從已接收已加密分離內容 5160 產生第一雜湊表"HA1TBL1" 5171、"HA1TBL2" 5172、"HA1TBL3" 5173 至"HA1TBLc" 5176。在此產生的第一雜湊表"HA1TBL1"5171、"HA1TBL2" 5172、"HA1TBL3" 5173 至"HA1TBLc" 5176 與第一雜湊表"HA1TBL1" 1261、"HA1TBL2" 1262、"HA1TBL3" 1263 至"HA1TBLc" 1264 相同，且產生程序亦相同。因此，將省略第一雜湊表的說明。

接下來，頭標資訊產生單元 5107 將根據已接收填充檔案資訊 5156 中包括的填充內容來產生第一雜湊表"HA1TBLf"5177。此產生程序與用以從已加密分離檔案產生第一雜湊表的程序相同，且因此將省略其說明。

接下來，頭標資訊產生單元 5107 將分別地根據(c+1)個第一雜湊表來計算檔案雜湊值、產生數個檔案雜湊資訊，其各包括已計算的(c+1)個檔案雜湊值之一以及對應於檔案雜湊值的檔案識別符，並且進一步產生由已產生(c+1)個檔案資訊的第二雜湊表"HA2TBL"5180。用以產生第二雜湊表的特定程序與第一實施例中用以產生第二雜湊表 1269 的程序相同，除了係用檔案識別符"FIDf"5157 以及從填充內容產生單元 5108 接收到的分離填充內容 5120 以外，且因此將省略其詳細說明。

第 59 圖展示出在此時點產生之第二雜湊表"HA2TBL"5180 的結構。第二雜湊表"HA2TBL"5180 係由(c+1)個檔案雜湊資訊 5181、5182、5183 至 5186 與 5187 構成。各個檔案雜湊資訊包括一檔案識別符以及一檔案雜湊值。該等檔案雜湊資訊 5181 至 5186 係從已加密分離內容 5160 產生，且與構成第一實施例中之第二雜湊表"HA2TBL"1269 的數個檔案雜湊資訊 1301 至 1304 相同。檔案雜湊資訊 5187 係根據填充檔案資訊 5156 而產生。

頭標資訊產生單元 5107 將對簽章資訊產生單元 5111 輸出已產生第二雜湊表 5180，而同時對記錄單元 5114 輸出包括已產生的(c+1)個第一雜湊表以及第二雜湊表"HA2TBL"5180 的頭標資訊 5190。

5.2.5 簽章資訊產生單元 5111

簽章資訊產生單元 5111 將接收來自填充內容產生單元 5108 的單元檢選資訊 5140，而同時接收來自頭標資訊產生單元 5107 的第二雜湊表"HA2TBL"5180。

當接收到單元檢選資訊 5140 以及第二雜湊表"HA2TBL"5180 時，簽章資訊產生單元 5111 將讀取由簽章金鑰儲存單元 1112 記錄的簽章金鑰 1113。

接下來，簽章資訊產生單元 5111 將藉著對由合併構成已接收第二雜湊表"HA2TBL"5180 之(c+1)個檔案雜湊值以及構成已接收單元檢選資訊 5140 之(c+1)個檔案資訊所形成的一合併結果套用簽章產生演算法 S 且使用讀取簽章金

鑰 1113 來產生簽章資訊。

接下來，簽章資訊產生單元 5111 將對記錄單元 5114 輸出已產生簽章資訊。

5.2.6 記錄單元 5114

記錄單元 5114 係載入到 DVD 中。

記錄單元 5114 將從響應於填充內容產生單元 5108 的一項指令來測量已載入 DVD 上可寫入區域的儲存容量。

記錄單元 5114 將接收來自金鑰區塊產生單元 1103 的金鑰區塊、接收來自加密處理單元 5106 的已加密內容、以及接收來自填充內容產生單元 5108 的填充內容與單元檢選資訊 5140。此外，記錄單元 5114 將接收來自頭標資訊產生單元 5107 的頭標資訊 5190，而同時接收來自簽章資訊產生單元 5111 的簽章資訊。

當接收該等資訊時，記錄單元 5114 將把已接收金鑰區塊、已加密內容、填充內容、單元檢選資訊 5140、頭標資訊 5190 以及簽章資訊寫入到 DVD 中。

5.3 DVD 5500

第 60 圖展示出第五實施例中儲存在 DVD 上的資訊。如第 60 圖所示，DVD 5500 將儲存金鑰區塊 5510、單元檢選資訊 5530、頭標資訊 5550、簽章資訊 2570、已加密內容 5580 以及填充內容 5590。

已經由分散裝置 5100 寫入該等資訊。各個該等資訊的

結構均如上所述，且因此在此省略其說明。

5.4 執行裝置 5600

如第 61 圖所示，執行裝置 5600 係由取得單元 1601、內容金鑰取得單元 1602、裝置金鑰儲存單元 1604、執行單元 5606、簽章資訊驗證單元 5611 以及驗證金鑰儲存單元 1612 組成。

以下將詳細說明組成執行裝置 5600 的個別部件。要注意的是，因為取得單元 1601、內容金鑰取得單元 1602 以及驗證金鑰儲存單元 1612 與構成第一實施例中的相同，在此便省略該等部件的說明。

5.4.1 簽章資訊驗證單元 5611

簽章資訊驗證單元 5611 將接收來自取得單元 1601 的單元檢選資訊 5530 以及簽章資訊 5570。

當接收該等資訊時，簽章資訊驗證單元 5611 將藉著使用已接收單元檢選資訊 5530 以及儲存在 DVD 5500 中的頭標資訊 5550、已加密內容 5580 與填充內容 5590 來驗證已接收簽章資訊 5570。將省略說明用以進行驗證的特定程序，因為它與構成第一實施例之執行裝置 1600 的簽章資訊驗證單元 1611 所進行的簽章資訊驗證動作相同，除了利用已加密內容 5580 外還利用填充內容 5590 以外。

5.4.2 執行單元 5606

執行單元 5606 預儲存 56 位元長度播放不可實行資訊"DAMY"。

執行單元 5606 將接收來自內容金鑰取得單元 1602 的內容金鑰"CK"。此外，執行單元 5606 可接收來自簽章資訊驗證單元 5611 的播放禁止資訊。

當接收到內容金鑰"CK"時，執行單元 5606 將透過取得單元 1601 逐一讀取構成已加密內容 5580 或填充內容 5590 的已加密檔案"ECNT1"、"ECNT2"、"ECNT3"至"ECNTc"。

執行單元 5606 將比較已讀取已加密檔案的前面 56 位元或已讀取填充內容的前面 56 位元以及已儲存的播放不可實行資訊"DAMY"。當該等二個彼此並不相符時，讀取資訊為已加密檔案且為可播放的，且因此執行單元 5606 將利用已接收內容金鑰"CK"而藉著參照各個單元來解密讀取已加密檔案以產生一檔案。接下來，執行單元 5606 將擴展已產生檔案以產生視訊與音訊資料、從已產生視訊與音訊資料來產生視訊與音訊信號、並且藉著對監視器輸出已產生視訊與音訊信號來播放該等內容。

當該等前面 56 位元以及已儲存的播放不可實行資訊"DAMY"彼此相符時，該讀取資訊便為填充內容且並無法被播放，且因此執行單元 5606 便中止上述解密、擴展以及播放動作，並且移動到處理下一個已加密檔案的動作。

直到已完成讀取所有的已加密檔案以及填充內容，執行單元 5606 將於相似程序中重複讀出、解密、擴展以及播放動作，相較於播放不可實行資訊"DAMY"。

如果在上述的重複動作中從簽章資訊驗證單元 5611 接收到播放禁止資訊的話，執行單元 5606 便中止該重複動作。

5.5 運作性行為

以下將說明第五實施例之分散裝置 5100 以及執行裝置 5600 的運作性行為。

5.5.1 分散裝置 5100 的運作性行為

以下將藉由第 62 圖與第 63 圖中展示之流程圖的輔助來說明分散裝置 5100 的運作性行為。

分散裝置 5100 的輸入單元 5101 將接受內容的一項輸入(步驟 S5011)、輸出已接受內容到單元產生單元 5105，並且指示內容金鑰產生單元 1102 要產生一內容金鑰。

內容金鑰產生單元 1102 將根據輸入單元 1101 的指令來產生內容金鑰(步驟 S5012)，並且對金鑰區塊產生單元 1103 與加密處理單元 5106 輸出已產生內容金鑰。

金鑰區塊產生單元 1103 將接收內容金鑰。當接收到內容金鑰時，金鑰區塊產生單元 1103 將從執行裝置資訊儲存單元 1104 讀取一裝置識別表(步驟 S5013)，並且根據已接收內容金鑰與已讀取裝置識別表來產生一金鑰區塊(步驟 S5016)。接下來，金鑰區塊產生單元 1103 將對記錄單元 5114 輸出已產生金鑰區塊。

當接收該等內容時，單元產生單元 5105 將把構成已接

收內容的各個檔案劃分為數個單元以產生分離內容(步驟S5017)。當已產生分離內容時，單元產生單元 5105 將產生由數個檔案資訊構成而分別地對應於該等分離檔案的單元檢選資訊 (步驟 S5018)，並且對填充內容產生單元 5108 輸出已產生單元檢選資訊而同時對加密處理單元 5106 輸出分離內容。

當接收內容金鑰以及分離內容時，加密處理單元 5106 將藉著使用內容金鑰加密包括在已接收分離內容中該等內容的各個單元來產生已加密分離內容 (步驟 S5019)。加密處理單元 5106 將摘取包括在已產生已加密分離內容中的已加密單元、產生已加密內容(步驟 S5021)，並且對記錄單元 5114 與填充內容產生單元 5108 輸出已產生已加密內容而同時對頭標資訊產生單元 5107 輸出已產生已加密分離內容。

當接收到單元檢選資訊與已加密內容時，填充內容產生單元 5108 將透過記錄單元 5114 取得 DVD 5500 的最大儲存容量(步驟 S5022)，並且測量已接收已加密內容的資料大小(步驟 S5023)。

接下來，填充內容產生單元 5108 將根據已接收單元檢選資訊來計算頭標資訊的資料大小以及簽章資訊的資料大小(步驟 S5026)，且進一步根據已取得的最大儲存容量、頭標資訊與簽章資訊的資料大小等來計算一填充容量(步驟 S5028)。

接下來，填充內容產生單元 5108 將藉著合併播放不可

實行資訊與一隨機數來產生具有已計算填充容量之資料大小的填充內容(步驟 S5029)，並且產生對應於填充內容的一檔案識別符與檔案識別資訊(步驟 S5031)。

填充內容產生單元 5108 將根據已儲存的差別數"j"把已產生填充內容劃分為 j 個單元來產生分離填充內容(步驟 S5032)。

接下來，填充內容產生單元 5108 將產生包括已產生檔案識別符與識別資訊的檔案資訊、指出已產生單元數量的單元編號，並且把已產生檔案資訊加入到已接收單元檢選資訊中(步驟 S5033)。填充內容產生單元 5108 將對記錄單元 5114 輸出已產生填充內容與單元檢選資訊 5140、對頭標資訊產生單元 5107 輸出由已產生檔案識別符與分離填充內容 5120 所組成的填充檔案資訊 5156、以及對簽章資訊產生單元 5111 輸出單元檢選資訊 5140。

當接收已加密分離內容以及填充檔案資訊 5156 時，頭標資訊產生單元 5107 將從包括在已接收已加密分離內容中的 c 個已加密分離檔案中產生 c 個第一雜湊表(步驟 S5034)。後續地，頭標資訊產生單元 5107 將從包括在已接收填充檔案資訊 5156 中的分離填充內容中產生第一雜湊表(步驟 S5036)。

頭標資訊產生單元 5107 將根據已產生的(c+1)個第一雜湊表來產生第二雜湊表(步驟 S5037)、產生包括(c+1)個第一雜湊表與第二雜湊表的頭標資訊(步驟 S5039)，並且對記錄單元 5114 輸出已產生頭標資訊而同時對簽章資訊產

生單元 5111 輸出已產生第二雜湊表。

當接收到單元檢選資訊 5140 與第二雜湊表時，簽章資訊產生單元 5111 將藉著對已接收單元檢選資訊與第二雜湊表套用簽章產生演算法來產生簽章資訊(步驟 S5041)，並且對記錄單元 5114 輸出已產生簽章資訊。

當接收到金鑰區塊、已加密內容、填充內容、單元檢選資訊、頭標資訊、章資訊時，記錄單元 5114 將把已接收金鑰區塊、已加密內容、填充內容、單元檢選資訊、頭標資訊與簽章資訊寫入到 DVD 5500 中(步驟 S5042)。

5.5.2 執行裝置 5600 的運作性行為

以下將藉由第 64 圖以及第 65 圖中展示之流程圖的輔助來說明執行裝置 5600 的運作性行為。

當載入到 DVD 5500 中時，取得單元 1601 將從 DVD 5500 讀取金鑰區塊 5510、單元檢選資訊 5530 與簽章資訊 2570，並且對內容金鑰取得單元 1602 輸出金鑰區塊 5510 而同時對簽章資訊驗證單元 1611 輸出單元檢選資訊 5530 與簽章資訊 5570(步驟 S5061)。

簽章資訊驗證單元 5611 將藉著使用隨機數與單元檢選資訊 5530 且使用選出 i 個以及頭標資訊來產生 i 個已置換第一雜湊表，從包括在已加密內容 5580 中的多個已加密單元以及包括在填充內容 5590 中的 j 個單元中選出 i 個來接收單元檢選資訊 5530 與簽章資訊 5570 (步驟 S5063)。

簽章資訊驗證單元 5611 將從各個已產生 i 個置換雜湊

表中計算出一置換檔案雜湊值(步驟 S5064)。

接下來，簽章資訊驗證單元 5611 將從 DVD 5500 讀取第二雜湊表(步驟 S5066)，並且藉著以置換雜湊值來置換對應於已產生 i 個置換檔案雜湊值的檔案雜湊值來產生一已置換第二雜湊表 (步驟 S5068)。簽章資訊驗證單元 5611 將藉著使用已產生置換第二雜湊表、已接收單元檢選資訊 5530、以及儲存在驗證金鑰儲存單元 1612 中的驗證金鑰 1613 來驗證簽章資訊 5570(步驟 S5069)。如果驗證簽章資訊 5570 的動作不成功的話(步驟 S5071：否)，簽章資訊驗證單元 5611 便對執行單元 5606 輸出播放禁止資訊(步驟 S5073)。

當驗證簽章資訊 5570 的動作成功時(步驟 S5071：是)，簽章資訊驗證單元 5611 隨後便結束該驗證動作。

內容金鑰取得單元 1602 將接收金鑰區塊 5510，並且從裝置金鑰儲存單元 1604 讀取一裝置識別符以及一裝置金鑰(步驟 S5074)。內容金鑰取得單元 1602 將從讀取裝置識別符、裝置金鑰與金鑰區塊 5510 產生內容金鑰"CK"，並且對執行單元 5606 輸出已產生內容金鑰"CK"(步驟 S5076)。

執行單元 5606 將從內容金鑰取得單元 1602 接收內容金鑰。在此，如果接收到來自簽章資訊驗證單元 5611 的播放禁止資訊的話(步驟 S5077：是)，執行單元 5606 將通知使用者儲存在 DVD 5500 中該等內容的播放不可實行性(步驟 S5079)，並且中止後續的播放動作。

如果並沒有接收播放禁止資訊的話(步驟 S5077：否)，

執行單元5606將讀取構成已加密內容與填充內容之c個已加密檔案中之一(步驟S5081)。執行單元5606將比較讀取已加密檔案或填充內容的前面 56 位元以及預儲存的播放不可實行資訊(步驟 S5082)。當該等二者彼此相符時(步驟 S5084：是)，執行單元5606便返回到步驟S5077。

當該等二者彼此並不相符時(步驟S5084：否)，該已讀取檔案便是已加密檔案且為可播放的。因此，執行單元5606 將藉著使用已接收內容金鑰來解密已加密檔案而產生一檔案(步驟S5086)、擴展已產生檔案(步驟S5087)，並且使監視器播放已擴展檔案(步驟S5089)。當已完成讀取構成已加密內容與填充內容的所有已加密檔案或者受到指示要由使用者完成該播放動作時(步驟S5091：是)，執行單元5606便結束該播放動作。如果尚未完成讀取構成已加密內容與填充內容的所有已加密檔案的話且執行單元 5606 尚未接收到要由使用者完成該項播放動作的一指令的話(步驟S5091：否)，執行單元5606便返回到步驟S5077並且重複步驟5077至S5091的處理動作。

5.6 總結以及較佳效應

如以上所述，在本實施例中，除了包括已加密內容的各種不同資訊之外，DVD 5500亦將儲存具有適當資料大小的填充內容，以便不會在 DVD 5500 中遺留一個可寫入儲存區域。再者，不僅根據已加密內容亦同時根據填充內容來產生頭標資訊與簽章資訊。

組成執行裝置 5600 的執行單元 5606 將依序地讀取寫在 DVD 5500 上的檔案，並且比較個別讀取檔案的前面 56 位元以及預儲存的播放不可實行資訊。當該等二者彼此相符時，執行單元 5606 便判斷該讀取檔案為填充內容，且避免播放檔案。

當 DVD 5500 並未儲存該等填充內容時，可假設下列包括詐欺行為的二種狀況。

第 65 圖展示出 DVD 5500b 的結構，其係藉著把包含未授權內容的一檔案加入到已由合法權所有者產生的 DVD 5500a 中而產生。

DVD 5500a 將把頭標資訊、單元檢選資訊、簽章資訊儲存在區域 5703 中，而同時把構成已加密內容的個別已加密檔案儲存在區域 5704、5705 至 5707 中。除了該等資訊之外，DVD 5500a 亦將分別地在區域 5701 以及區域 5702 中儲存一檔案表與一播放順序檔案。

儲存在區域 5701 中的檔案表包括儲存在 DVD 5500 中所有檔案的檔案識別符、該等檔案的開始位址、該 DVD 上個別檔案佔用的區段編號，其與檔案識別符、開始位址、以及個別檔案區段編號相關聯。例如，具有檔案識別符"FID1"的檔案係儲存在於位址"0XAA1"開始的 70 個區段。

儲存在區域 5702 中的播放順序檔案展示出儲存在 DVD 中之檔案的播放順序。在此一實例中，檔案係呈從具有檔案識別符"FIF1"的檔案到具有檔案識別符"FIDc"的檔案的

順序來播放。

此外，DVD 5500a 上並沒有東西已儲存在區域 5711 中。

在此狀況中，假設未授權第三者已在 DVD 5500a 的區域 5711 中寫入包括未授權內容的一檔案，且已藉著竄改檔案表以及播放順序檔案來產生 DVD 5500b。

在 DVD 5500b 的區域 5701 中，對應於未授權檔案的檔案識別符"FIDx"、未授權檔案的開始位址"0XAAx"、以及區段編號"200"均已被加入。此外，儲存在區域 5702 中的一播放順序檔案已遭到竄改，因此播放動作將以具有檔案識別符"FIDx"的檔案來開始。

此外，亦將考量一種狀況，其中展示於第 66 圖中的 DVD 5500c 係藉著把未授權內容加入到儲存在 DVD 5500a 中的有效檔案中而產生。

DVD 5500c 將把未授權內容儲存在區域 5711 中，其即刻跟在有效地儲存在區域 5707 中的一檔案後面。對應於儲存在檔案表之區域 5707 中的檔案區段編號已被竄改為"320"，其係藉著把當中原始儲存有檔案的區段編號加入到當中已儲存有已加入未授權內容的一區段編號。已改變播放順序檔案，因此播放動作將以該等檔案中具有檔案識別符"FIDc"的第 51 個區段開始，即已加入的未授權內容。

因此，當已進行未授權竄改時，因為頭標資訊、單元檢選資訊、簽章資訊與已加密內容根本未受到竄改，一旦已正常地完成驗證簽章資訊的動作時，執行裝置便可根據順序檔案所指出的順序讀取未授權檔案並且開始進行播放。

在本實施例中，並不會在 DVD 5500 上留存一可寫入儲存區域，因為填充內容出現的關係。此外，填充內容亦可用來產生簽章資訊。因此，如果以未授權檔案來置換填充內容的話，執行裝置 5600 中的驗證簽章資訊動作將不會成功，且因此播放動作將受到中止。

6.第六實施例

以下將說明本發明的第六實施例。

6.1 未授權內容檢測系統

第六實施例的未授權內容檢測系統係由一分散裝置、一執行裝置、以及一監視器組成，如第一實施例中的未授權內容檢測系統一般。

除了第一實施例中說明的金鑰區塊、單元檢選資訊、已加密內容、頭標資訊以及簽章資訊之外，分散裝置亦將產生用以指出 DVD 上之一儲存區域的區域資訊，其中係儲存有由分散裝置有效地寫入的資訊，分散裝置並將在該 DVD 上寫入已產生區域資訊。

執行裝置將從 DVD 讀取區域資訊，並且僅讀取由讀取區域資訊指出而儲存在儲存區域中的資訊。

6.2 分散裝置 6100

第 67 圖展示出構成第六實施例之未授權內容檢測系統的分散裝置結構。如第 67 圖所示，分散裝置 6100 係由輸

入單元 1101、內容金鑰產生單元 1102、金鑰區塊產生單元 6103、執行裝置資訊儲存單元 1104、單元產生單元 6105、加密處理單元 6106、頭標資訊產生單元 6107、配置產生單元 6108、區域資訊產生單元 6109、簽章資訊產生單元 6111、簽章金鑰儲存單元 1112、以及記錄單元 6114 組成。

以下將說明構成分散裝置 6100 的個別部件。要注意的是，因為輸入單元 1101、內容金鑰產生單元 1102、執行裝置資訊儲存單元 1104 以及簽章金鑰儲存單元 1112 與第一實施例中的分散裝置 1100 相同，在此將省略該等部件的說明。

在此，並不是輸出金鑰區塊、單元檢選資訊、已加密內容以及頭標資訊的記錄單元，金鑰區塊產生單元 6103、單元產生單元 6105、加密處理單元 6106 以及頭標資訊產生單元 6107 將個別地輸出其本身產生的資訊到配置產生單元 6108。除此之外，金鑰區塊產生單元 6103、單元產生單元 6105、加密處理單元 6106 與頭標資訊產生單元 6107 均分別地與第一實施例的金鑰區塊產生單元 1103、單元產生單元 1105、加密處理單元 1106 與頭標資訊產生單元 1107 相同，且因此在此將省略該等部件的說明。

6.2.1 配置產生單元 6108

配置產生單元 6108 將預儲存簽章資訊產生單元 6111 產生之簽章資訊的最大資料大小。此外，配置產生單元

6108 將儲存區域資訊產生單元 6109 產生之區域資訊的資料大小。

配置產生單元 6108 將接收來自金鑰區塊產生單元 6103 的金鑰區塊、接收來自單元產生單元 6105 的單元檢選資訊、接收來自加密處理單元 6106 的已加密內容、以及接收來自頭標資訊產生單元 6107 的頭標資訊。

當接收到該等資訊時，配置產生單元 6108 將產生寫入配置資訊 6120，如第 68 圖所示。將藉著以與 DVD 組態相同方式配置已接收資訊來產生寫入配置資訊 6120，並且把已配置的資訊寫入到記憶體上。以下藉由第 68 圖的輔助來說明用以產生寫入配置資訊 6120 的程序。

配置產生單元 6108 將把金鑰區塊寫入到記憶體的區域 6121 中、把單元資訊寫入到區域 6122 中，且把頭標資訊寫入到區域 6123 中。

接下來，配置產生單元 6108 將取得分別地對應於已儲存區域資訊與簽章資訊之最大資料大小的區域 6124 與 6125。隨後，配置產生單元 6108 將把已加密內容寫入到區域 6125 之後的區域 6126 中。

配置產生單元 6108 將對區域資訊產生單元 6109 與記錄單元 6114 輸出已產生寫入配置資訊 6120。

要注意的是，展示於第 68 圖中該等資訊的配置順序僅為實例，且本發明並不限於此。

在此，配置產生單元 6108 將儲存簽章資訊的最大資料大小。然而，配置產生單元 6108 可利用與第五實施例填充

內容產生單元 5108 相同的方式來計算出簽章資訊的資料大小。

6.2.2 區域資訊產生單元 6109

區域資訊產生單元 6109 將接收來自配置產生單元 6108 的寫入配置資訊 6120。當接收到寫入配置資訊 6120 時，區域資訊產生單元 6109 將從已接收寫入配置資訊 6120 產生區域資訊。區域資訊為用以指出 DVD 上一區域的資訊，其中係儲存有分散裝置 6100 寫入的有效資訊。該區域資訊例如為用以把配置資訊 6120 寫入到 DVD 上開始位置(以下稱為開始位址)以及結束位置(結束位址)的一對位址。

區域資訊並不限於此實例，且任何資訊均適用，例如一對開始位址以及儲存有有效資訊的區段編號，只要儲存有能識別除有效資訊之處的資訊即可。

區域資訊產生單元 6109 將對簽章資訊產生單元 6111 與記錄單元 6114 輸出已產生區域資訊。

6.2.3 簽章資訊產生單元 6111

簽章資訊產生單元 6111 將接收來自單元產生單元 6105 的單元檢選資訊、接收來自頭標資訊產生單元 6107 的第二雜湊表、並且接收來自區域資訊產生單元 6109 的區域資訊。

當接收到該等資訊時，簽章資訊產生單元 6111 將從簽章金鑰儲存單元 1112 讀取簽章金鑰 1113。

接下來，簽章資訊產生單元 6111 將藉著使用讀取簽章金鑰 1113 而對由合併已接收第二雜湊表中包括的 c 個檔案雜湊值、組成單元檢選資訊的 c 個檔案資訊、以及已接收區域資訊所形成的合併結果套用簽章產生演算法 S 來產生簽章資訊。

接下來，簽章資訊產生單元 6111 將對記錄單元 6114 輸出已產生簽章資訊。

6.2.4 記錄單元 6114

記錄單元 6114 係載入到 DVD 中。

記錄單元 6114 將接收來自配置產生單元 6108 的寫入配置資訊 6120、接收來自區域資訊產生單元 6109 的區域資訊、並且接收來自簽章資訊產生單元 6111 的簽章資訊。

當接收到該等資訊時，記錄單元 6114 將把已接收區域資訊插入到寫入配置資訊 6120 的區域 6124 中，而同時把簽章資訊插入到區域 6125 中。

當已把區域資訊與簽章資訊插入到寫入配置資訊 6120 中時，記錄單元 6114 將把寫入配置資訊 6120 寫入到一 DVD 中。

6.3 DVD 6500

第 69 圖展示出第六實施例中儲存在 DVD 上的資訊。如第 69 圖所示，DVD 6500 將儲存金鑰區塊 6510、單元檢選資訊 6530、頭標資訊 6550、區域資訊 6560、簽章資訊 6570

與已加密內容 6580。已經由分散裝置 6100 寫入該等資訊，且因此在此省略其說明。

6.4 執行裝置 6600

第 70 圖展示出第六實施例之執行裝置的結構。如第 70 圖所示，執行裝置 6600 係由驅動機單元 6620 以及內容執行單元 6625 組成。

驅動機單元 6620 係由取得單元 6601、區域資訊儲存單元 6603、加密傳遞單元 6604 以及加密金鑰儲存單元 6605 組成。

內容執行單元 6625 則由內容金鑰取得單元 1602、裝置金鑰儲存單元 1604、解密傳遞單元 6607、解密金鑰儲存單元 6608、簽章資訊驗證單元 6611、驗證金鑰儲存單元 1612 與執行單元 6606 組成。

以下將詳細說明組成執行裝置 6600 的個別部件。要注意的是，因為內容金鑰取得單元 1602、裝置金鑰儲存單元 1604 以及驗證金鑰儲存單元 1612 與構成第一實施例中的執行裝置 1600 相同，在此便省略該等部件的說明。

6.4.1 取得單元 6601

取得單元 6601 係載入到 DVD 6500 中。當載入到 DVD 6500 中時，取得單元 6601 將首先讀取區域資訊 6560、隨後把讀取區域資訊 6560 寫入到區域資訊儲存單元 6603 中，並且對加密傳遞單元 6604 輸出讀取區域資訊 6560。

接下來，取得單元 6601 將從 DVD 6500 讀取金鑰區塊 6510、單元檢選資訊 6530 與簽章資訊 6570，並且對內容金鑰取得單元 1602 輸出讀取金鑰區塊 6510，而同時對簽章資訊驗證單元 6611 輸出讀取單元檢選資訊 6530 與簽章資訊 6570。

此外，取得單元 6601 將接收用以從簽章資訊驗證單元 6611 與執行單元 1606 讀取各種不同資訊的請求。當接收到讀出請求時，簽章資訊驗證單元 6611 將從區域資訊儲存單元 6603 讀取區域資訊。當一組要求資訊儲存在由區域資訊指出的一區域中時，取得單元 6601 將從 DVD 6500 讀取該要求資訊，並且對一請求來源(即簽章資訊驗證單元 6611 或執行單元 1606)輸出讀取資訊。

當一組要求資訊並未儲存在由讀取區域資訊指出的該區域中時，取得單元 6601 將輸出指出無法讀取要求資訊組的一錯誤通知信號。

6.4.2 區域資訊儲存單元 6603

區域資訊儲存單元 6603 係例如由 RAM 組成，且將儲存取得單元 6601 寫入的區域資訊。

6.4.3 加密傳遞單元 6604 與加密金鑰儲存單元 6605

例如，加密金鑰儲存單元 6605 係由 ROM 組成，且將儲存一個 56 位元長度的加密金鑰。

加密傳遞單元 6604 將接收來自取得單元 6601 的區域

資訊6560。當接收到區域資訊6560時，加密傳遞單元6604將從加密金鑰儲存單元6605讀取一加密金鑰，並且藉著對讀取加密金鑰套用加密演算法 E2 來產生已加密區域資訊。在此，係使用 DES(資料加密標準)作為加密演算法 E2 的一實例。

接下來，加密傳遞單元 6604 將對解密傳遞單元 6607 輸出已產生已加密區域資訊。

6.4.4 解密傳遞單元 6607 與解密金鑰儲存單元 6608

例如，解密金鑰儲存單元 6608 係由 ROM 組成，且將儲存一個 56 位元長度的解密金鑰。在此，解密金鑰係與加密金鑰儲存單元 6605 儲存的加密金鑰相同。

解密傳遞單元 6607 將接收來自加密傳遞單元 6604 的已加密區域資訊。當接收到已加密區域資訊時，解密傳遞單元 6607 將從解密金鑰儲存單元 6608 讀取解密金鑰，並且藉著使用讀取解密金鑰而對已接收已加密區域資訊套用解密演算法 D2 來產生區域資訊。在此，解密演算法 D2 為用以解密利用加密演算法 E2 產生之加密文本的一種演算法。

接下來，解密傳遞單元 6607 將對簽章資訊驗證單元 6611 輸出已產生區域資訊。

上述說明係假設加密金鑰與解密金鑰為相同的，且解密傳遞單元 6607 係使用一種對稱金鑰密碼系統。然而，本發明並不限於此，且可反之使用一種公開金鑰密碼系統。替

代地，每當進行通訊時，可把一公開金鑰密碼系統與一對稱金鑰密碼系統合併在一起以產生一不同金鑰，且可使用已產生金鑰來進行密碼式通訊。

此外，在此僅有區域資訊為加密的，且隨後對內容執行單元 6625 輸出，然而，可加密所有在內容執行單元 6625 與驅動機單元 6620 之間傳送且接收的資訊。

6.4.5 簽章資訊驗證單元 6611

簽章資訊驗證單元 6611 將接收來自取得單元 6601 的單元檢選資訊 6530 與簽章資訊 6570，以及來自解密傳遞單元 6607 的區域資訊。

當接收到單元檢選資訊 6530 與簽章資訊 6570 時，簽章資訊驗證單元 6611 將根據已接收單元檢選資訊 6530 以及儲存在 DVD 6500 中的已加密內容 6580 與頭標資訊 6550 來產生已置換第二雜湊表。用以產生已置換第二雜湊表的程序與第一實施例中簽章資訊驗證單元 1611 產生已置換第二雜湊表的程序相同，且因此在此將省略其說明。

接下來，簽章資訊驗證單元 6611 將從驗證金鑰儲存單元 1612 讀取驗證金鑰 1613。隨後，簽章資訊驗證單元 6611 將藉著使用讀取驗證金鑰 1613 而對合併所有檔案雜湊值以及已產生置換第二雜湊表中包括的置換檔案雜湊值、所有包括在已接收單元檢選資訊 6530 中的檔案資訊、以及區域資訊而形成的一合併結果套用簽章驗證演算法 V 來產生簽章驗證資訊。簽章資訊驗證單元 6611 將比較已產生簽章

驗證資訊以及已接收簽章資訊 6570。

當該等二者彼此並不相符時，簽章資訊驗證單元 6611 便判斷出驗證簽章資訊的動作並不成功，且對執行單元 1606 輸出播放禁止資訊。

當該等二者彼此相符時，簽章資訊驗證單元 6611 便判斷驗證已接收簽章資訊 6570 的動作是成功的，且結束驗證處理動作。

在上述處理動作中，簽章資訊驗證單元 6611 將指示取得單元 6601 要讀取部分的已加密內容與頭標資訊。然而，在此時點中，簽章資訊驗證單元 6611 可接收指出不可能進行讀出動作的一錯誤通知信號。

當接收到錯誤通知信號時，簽章資訊驗證單元 6611 將中止簽章資訊的驗證處理動作，並且對執行單元 1606 輸出播放禁止資訊。

6.4.6 執行單元 6606

執行單元 6606 將接收來自內容金鑰取得單元 1602 的一內容金鑰，並且開始重複進行已加密檔案的讀出、解密與播放動作，如構成第一實施例之執行裝置 1600 的執行單元 1606 一般。

在重複動作中，執行單元 6606 可接收來自簽章資訊驗證單元 6611 的播放禁止資訊。

此外，在重複動作中，執行單元 6606 將要求取得單元 6601 要讀取組成已加密內容 6580 的已加密檔案。然而，

在此時點中，執行單元 6606 可從取得單元 6601 接收指出不可能進行讀出動作的一錯誤通知信號。

當接收到播放禁止資訊或一錯誤通知信號時。執行單元 6606 將中止播放處理動作，並且通知使用者已載入 DVD 的播放不可實行性。

6.5 總結以及較佳效應

如以上所述，構成本實施例未授權內容檢測系統的分散裝置 6100 將產生指出由分散裝置 6100 有效寫入資訊所儲存之區域的區域資訊，並且寫入已產生區域資訊到 DVD 中。再者，分散裝置 6100 將從第二雜湊表、單元檢選資訊與區域資訊產生簽章資訊，並且寫入資訊到 DVD 中。

當載入到 DVD 6500 中時，執行裝置 6600 的取得單元 6601 將首先從 DVD 6500 讀取區域資訊，並且僅讀取由讀取區域資訊指出之一區域中的資訊，但並不讀取寫入在其他區域中的資訊。

據此，即使當把未授權內容寫入到 DVD 6500 上的閒置空間等詐欺行為發生時，如第五實施例中所述，並無法在執行裝置 6600 中播放未授權內容。

此外，係利用區域資訊來產生儲存在 DVD 6500 中的簽章資訊，且執行裝置 6600 的簽章資訊驗證單元 6611 將使用從 DVD 6500 讀取的區域資訊來驗證簽章資訊。因此，即使是未授權第三者竄改區域資訊且插入未授權內容，簽章資訊驗證單元 6611 進行的簽章資訊驗證動作並不會成

功，且因此無法播放未授權內容。

當 DVD 上並沒有閒置空間時，可能會有詐欺行為發生，例如把儲存在有效 DVD 中的所有資料複製到其儲存容量大於該有效 DVD 的另一個媒體並且把未授權內容加入到該媒體的閒置空間中。即使在此種狀況中，本實施例之未授權內容檢測系統中的執行裝置 6600 並不會讀取由區域資訊指出之區域以外之儲存區域中的資訊。因此，本實施例能夠避免詐欺行為的發生。

6.6 第六實施例的修改方案

在第六實施例中，分散裝置 6100 所產生的區域資訊為指出儲存有分散裝置有效寫入之資訊的區域資訊。替代地，該區域資訊可為分散裝置 6100 有效寫入之資訊的總體資料大小。

於此，執行裝置 6600 的取得單元 6601 將首先從 DVD 6500 讀取總體資料大小，並且隨後測量儲存在 DVD 6500 中之資訊的總體資料大小。當測量出的資料大小大於讀取資料大小時，取得單元 6601 便中止從 DVD 6500 讀取資料，並且對執行單元 6606 輸出一錯誤通知信號。

7.其他修改方案

雖然已根據上述實施例來說明本發明，本發明當然並不限於該等實施例。本發明亦包括以下事例。

[1]在上述第一、第五與第六實施例中，分散裝置將藉

著把已加密單元指派給雜湊函數來計算單元雜湊值，並且根據計算出的單元雜湊值來產生頭標資訊與簽章資訊，而執行裝置同時將利用選出的 i 個已加密單元來驗證簽章資訊。然而，分散裝置可藉著在加密之前使用單元來計算單元雜湊值，且執行裝置可藉著解密選出的i個已加密單元來產生i個單元，並且藉著使用已產生的i個單元來驗證簽章資訊。

[2]另一方面，在第二至第四實施例中，分散裝置將藉著把數個部份內容指派給雜湊函數來計算部份雜湊值，並且根據計算出的部份雜湊值來產生頭標資訊簽章資訊。然而，分散裝置可藉著對雜湊函數指派加密個別部份內容而產生的已加密部份內容來計算部份雜湊值，並且根據計算出的部份雜湊值來產生頭標資訊簽章資訊。

於此，執行裝置將使用已加密部份內容來驗證頭標資訊。此動作可降低配置代表性部份內容解密單元與部份內容解密單元的需要，而降低檢測系統的電路大小。

[3]在第二至第四實施例中，在已成功驗證簽章資訊與頭標資訊之後，執行單元便開始已加密內容的解密、擴展與播放動作。然而，執行單元可開始並行地與驗證動作一同進行有關播放的處理動作。於此，當分別由簽章資訊驗證單元與頭標資訊驗證單元進行的個別驗證不成功時，簽章資訊驗證單元與頭標資訊驗證單元將指示執行單元要中止播放動作。

[4]在第一、第五與第六實施例中，簽章資訊驗證單元

可具有用以測量經過時間的一計時器，並且如果並未在一段預定時間中完成驗證簽章資訊動作的話，便判斷驗證並不成功。

當並行地與驗證動作一同進行驗證簽章資訊動作時，如果內容、簽章資訊或頭標資訊已受到竄改的話，將播放未授權內容直到完成驗證動作為止。

因此，設定用以驗證簽章資訊的一段時間限制將因為進行竄改而對延長未授權內容播放時間的詐欺行為起反作用，因而使完成驗證簽章資訊的動作延誤。

此外，修改方案[3]中的簽章資訊驗證單元與頭標資訊驗證單元可相似地具有一計時器。

[5]在上述第一至第六實施例中，分散裝置具有一簽章金鑰，而執行裝置具有一對應驗證金鑰，且該等裝置係藉著使用例如 DSA 的一種簽章產生演算法來產生並且驗證簽章資訊。

大致上來說，許多簽章產生演算法係根據公開金鑰密碼系統，如以 DSA 與 RSA(Rivest-Shamir-Adleman)代表。然而在本發明中，任何簽章產生演算法均為適用的，例如根據對稱金鑰密碼系統的一種演算法，只要它能夠證明 DVD 上記錄的簽章資訊為合法權所有者產生的資訊。

舉另一實例來說，可使用單向功能而當中隱藏處理動作。於此，分散裝置與執行裝置分別地在一儲存區域中儲存相同的單向功能，該區域並無法由外部裝置來讀取。分散裝置藉著使用單向功能來產生簽章資訊，而執行裝置藉

著使用相同的單向功能來產生簽章驗證資訊。

[6]在產生簽章資訊時，套用簽章產生演算法的資訊並不限於上述實施例中說明的資訊。例如，在第一實施例中，可把簽章產生演算法套用至第二雜湊表與單元檢選資訊，然而，僅可把簽章產生演算法套用到第二雜湊表，或者除了第二雜湊表之外可把其套用到內容金鑰"CK"以及已加密內容的資料大小。在第二實施例中，可把簽章產生演算法套用到數個代表性部份內容本身中，而不是對從該等代表性部份內容產生的部份雜湊值套用簽章產生演算法。

尤其地，在第二實施例中，當從該等代表性部份內容產生簽章資訊時，可藉著分別地對 k 個代表性部份內容套用簽章產生演算法來產生 k 個簽章資訊。

於此，執行裝置將根據選擇位置資訊來產生 k 個代表性部份內容，且藉著使用已產生 k 個代表性部份內容來驗證 k 個簽章資訊。

替代地，分散裝置可藉著對合併 k 個代表性部份內容而形成的合併結果套用簽章產生演算法來產生簽章資訊，而同時執行裝置將藉著使用該合併結果來驗證簽章資訊。

在此狀況中，如果驗證簽章資訊動作成功的話，將一次確認下列二項事項：簽章資訊是否由合法權所有者產生；以及該等代表性部份內容是否免於受到竄改。此動作可降低產生頭標資訊以及寫入頭標資訊到 DVD 的需要，因而使寫入到 DVD 中的資料大小變小。

[7]在第二與第三實施例中，執行裝置可預儲存選擇位

置資訊，且已加密選擇位置資訊可能不會記錄在 DVD 上。據此，有效執行裝置便能夠藉著使用預儲存的選擇位置資訊來驗證頭標資訊。

[8]在第三實施例中，將把頭標選擇資訊與 x 個頭標群組寫入到 DVD 中。然而，在修改方案[7]中，分散裝置可選出第一頭標至第 x 頭標群組中之一、摘取出一頭標識別符、頭標資訊與包括在選出頭標群組中的簽章資訊，並且把該等資訊寫入到 DVD 中。

執行裝置可預儲存 x 對的選擇位置資訊以及頭標識別符、根據寫入到 DVD 的頭標識別符來選擇一份選擇位置資訊，並且在後續處理動作中選出選擇位置資訊。

[9]上述第一至第七實施例係假設該執行裝置為一單一裝置。然而，可使用多個裝置來達到執行裝置的功能。

[10]在第三實施例中，執行裝置的取得單元將選出 x 個頭標識別符中之一。然而，本發明並不限於此，且可反之選出二或數個識別符，且可重複驗證簽章資訊與頭標資訊二次或更多次。據此，可以較可靠地檢測未授權內容。

[11]在上述實施例與修改方案中，分散裝置的簽章金鑰儲存單元以及執行裝置的驗證金鑰儲存單元將分別地儲存一份金鑰資訊，然而，本發明並不限於此。

[11-1]例如，簽章金鑰儲存單元可儲存一簽章金鑰以及對應於該簽章金鑰的一金鑰識別符，且該記錄單元將把金鑰識別符連同簽章資訊一同寫入到 DVD 中。

執行裝置的驗證金鑰儲存單元將儲存多個驗證金鑰以

及一對一地對應於該等驗證金鑰的金鑰識別符。簽章資訊驗證單元將接收金鑰識別符以及簽章資訊、從驗證金鑰儲存單元儲存的多個金鑰識別符中取回符合已接收金鑰識別符的一金鑰識別符、讀出對應於已取回驗證金鑰識別符的驗證金鑰，並且使用已讀取驗證金鑰來驗證簽章資訊。

據此，本發明亦可適用於有多個不同分散裝置的狀況。

[11-2]執行裝置可能不具備驗證金鑰儲存單元，可把一簽章金鑰與對應於該簽章金鑰的一驗證金鑰儲存在分散裝置的簽章金鑰儲存單元中。在此狀況中，記錄單元將把驗證金鑰連同簽章資訊一同寫入到 DVD 中。

[11-3]除了簽章金鑰與驗證金鑰之外，分散裝置可儲存由公正第三者產生之驗證金鑰的鑑認資訊。在此，係假設鑑認資訊為藉著使用第三者的私密金鑰而對驗證金鑰套用簽章產生演算法而產生的一金鑰簽章。

記錄單元將把驗證金鑰與金鑰簽章連同簽章資訊一同寫入到 DVD。

執行裝置的驗證金鑰儲存單元將儲存金鑰驗證資訊，而不是驗證金鑰。金鑰驗證資訊為用以驗證金鑰簽章的資訊，於此，一公開金鑰將與產生金鑰簽章之公正第三者的私密金鑰配對。

簽章資訊驗證單元將接收金鑰簽章與驗證金鑰，並藉著在驗證簽章資訊之前使用已接收金鑰與金鑰驗證資訊來驗證金鑰簽章。只有在驗證動作成功時，簽章資訊驗證單元才會如以上實施例所述地開始驗證簽章資訊。

據此，即使當有多個分散裝置時，執行裝置僅需要保有第三者的金鑰驗證資訊，而不必具有多個驗證金鑰。

[12]在修改方案[11]中，執行裝置可儲存指出無效驗證金鑰的一取消列表。該簽章資訊驗證單元將判斷是否已把已接收金鑰識別符或驗證金鑰登錄到該取消列表中，且當已登錄時，中止驗證簽章資訊的動作。

[13]執行裝置可從外部來源取得取消列表，如修改方案[12]中所述。例如，可透過 DVD 的記錄媒體來取得取消列表，或者可透過網際網路、廣播等方式來取回取消列表。替代地，執行裝置可週期性地取得一更新取消列表。

據此，本發明能夠處理當中新發現到需要使驗證金鑰無效的一種狀況。

[14]分散裝置可透過 DVD 把各種不同資訊(例如已加密內容與簽章資訊)分散到執行裝置。然而，本發明並不限於 DVD，且該資訊可透過下列項目來分散：例如 CD-ROM 與 DVD-ROM 的光碟；例如 CD-R、DVD-R 與 DVD-RAM 的可寫入光碟；磁性光碟；以及記憶卡。替代地，可把例如快閃記憶體的半導體記憶體以及硬碟整合到執行裝置中。

再者，本發明並不限於該等記錄媒體，且可透過例如網際網路的通訊系統來分散資訊，或者可透過廣播來分散資訊。

[15]雖然上述實施例與修改方案係假設內容為由影像與音訊組成的視訊內容，且該等內容可為一電腦程式。例如，假設執行裝置為一遊戲控制台；該等內容為儲存在合

併到遊戲控制台之快閃記憶體中的一電腦程式。在此，電腦程式為一種用以判斷載入到遊戲控制台中的遊戲軟體(例如光碟與記憶卡)是否為有效軟體的判斷程式。在此狀況中，即使未授權使用者竄改判斷程式以執行未授權遊戲軟體，本發明能夠藉著使用簽章資訊與頭標資訊來驗證是否包括未授權內容來檢測該竄改動作，且因此可避免或者中止執行判斷程式的動作。因此，藉著停止執行動作本身，可以避免上面已進行未授權竄改動作之判斷程式實現的未授權運作，即避免執行未授權遊戲軟體。

[16]如上述修改方案中所述，在該等內容為儲存在包含於執行裝置中微電腦上載入之快閃記憶體的一電腦程式時，可能會發生第五實施例中所述的詐欺行為。確切來說，首先將把一未授權程式加入到快閃記憶體的閒置空間中，而不會竄改儲存在快閃記憶體中的有效電腦程式。隨後，將引發因為使用有效電腦程式之程式錯誤而導致的緩衝器過速問題，因此程式的開始點將跳到已加入未授權程式的前面，且開始執行未授權程式的動作。

在此，可藉著把填充內容寫入到快閃記憶體中而避免上述的詐欺行為，因此不會在快閃記憶體中遺留閒置空間，如第五實施例般，因為無法加入未授權內容。

替代地，如第六實施例中所述，可事先把指出儲存有分散裝置寫入有效資訊一區域的區域資訊寫入到快閃記憶體中，且執行裝置係設計為無法在區域資訊指出之區域以外的區域中讀取資訊。藉此，即使當加入了未授權程式，執

行裝置並不會執行未授權程式。

[17]上述第一至第六實施例以及修改方案係假設執行單元為播放由視訊與音訊構成內容的一部件，然而，執行單元可為對外部記錄媒體輸出內容的一部件，或為具有列印功能且可把影像資料列印在紙張上的一部件。

[18]在上述實施例中，每當把一組內容輸入到分散裝置中時，內容金鑰產生單元將產生一內容金鑰。然而，內容金鑰產生單元可預儲存多個內容金鑰，並且選擇且輸出已儲存內容金鑰中之一。

[19]在上述實施例中，執行裝置係設計為在載入 DVD 時，開始驗證頭標資訊、簽章資訊等，然而本發明並不限於此。

例如，當受到指示要根據使用者的按鈕運作來進行播放時，執行裝置可開始該等驗證動作，或者可從載入 DVD 時以規則間隔時間來進行該等驗證動作。

[20]在第二與第三實施例中，並不需要把頭標資訊寫入到 DVD 中。

當並未把頭標資訊寫入到 DVD 中時，執行裝置將根據選擇位置資訊摘取出 k 個代表性部份內容，並且藉著分別地把摘取出的代表性部份內容指派給雜湊函數來計算驗證雜湊值。

隨後，執行裝置將藉著對使用驗證金鑰合併已計算驗證雜湊值而形成的合併結果套用簽章驗證演算法 V 來產生簽章驗證資訊。該執行裝置將藉著比較已產生簽章驗證資訊

來驗證簽章資訊。

於此，執行裝置不再需要頭標資訊驗證單元，這可縮小檢測系統的電路大小。此外，可在驗證簽章資訊的同時，完成驗證是否包括未授權內容的動作。

[21]在第四實施例中，在簽章資訊驗證單元 4606 已經成功地進行驗證簽章資訊的動作之後，執行裝置 4600 僅驗證包括在頭標資訊中 c 個部份雜湊值中的 k 個。然而，可藉著使用 k 個已加密部份內容與頭標資訊而以單一驗證動作來驗證簽章資訊與頭標資訊二者。

更確切來說，執行裝置將根據內容位置資訊從已加密內容中摘取出 k 個已加密部份內容，並且藉著解密已摘取出的 k 個已加密部份內容來產生 k 個部份內容。隨後，執行裝置將藉著分別地把已產生 k 個部份內容指派給雜湊函數來計算置換部份雜湊值。

接下來，執行裝置將從包括在頭標資訊中的 c 個部份雜湊值把對應於選出 k 個已加密部份內容的部份雜湊值置換為已計算出的置換部份雜湊值。

執行裝置將藉著使用驗證金鑰以及藉著合併置換部份雜湊值以及包括在已置換頭標資訊中的部份雜湊值所形成的一項合併結果來驗證簽章資訊。

於此，執行裝置不再需要頭標資訊驗證單元，這將縮小檢測系統的電路大小。此外，可在驗證簽章資訊的同時，完成驗證是否包括未授權內容的動作。

[22]在上述第一至第六實施例中，寫入到 DVD 中僅為

一組已加密內容，以及對應於該組已加密內容的各個簽章資訊與頭標資訊。然而，可儲存分別地對應於該等資訊組的數個不同已加密內容組以及數個頭標語簽章資訊。

此外，DVD 僅可包括根據所有頭標資訊產生的一份簽章資訊。再者，除了該等已加密內容之外，DVD 可包括並不需要著作權保護的內容，例如廣告、開啟螢幕、選單等等。可播放該等不需要著作權保護的內容，而同時進行驗證簽章資訊與頭標資訊的動作。

[23]在第一至第六實施例與修改方案中，當驗證簽章資訊與驗證頭標資訊的動作中至少有一個不成功時，執行裝置可儲存用以識別載入到取得單元上 DVD 的一碟片識別符以及用以識別正在播放內容的一內容識別符。

當載入具有相同於受記錄識別符之碟片識別符的 DVD 時，執行裝置便中止播放內容。替代地，當受到指示要播放具有相同於受記錄識別符之識別符的內容時，執行裝置便中止播放該內容。

[24]在上述實施例與修改方案中，當驗證簽章資訊與驗證頭標資訊的動作中至少有一個不成功時，執行裝置便中止播放內容，並且通知使用者內容並未得到授權，例如藉著在監視器上顯示出一錯誤通知螢幕。在驗證錯誤時，執行裝置採取的運作性行為並不限於此，且亦可考量下列事例。再者，可合併下列三種修改方案。

[24-1]分散裝置與執行裝置二者均連接至網際網路。當驗證簽章資訊與驗證頭標資訊的動作中至少有一個不成功

時，執行裝置將透過網際網路通知分散裝置驗證失敗。在此時點，執行裝置亦將傳送指出未成功驗證該等內容的一內容識別符。

分散裝置將預儲存內容識別符以及由內容識別符指出的內容產生日期，把該等二者連結在一起。

分散裝置將透過網際網路從執行裝置接收到驗證失敗的通知與內容識別符。分散裝置將根據對應於已接收內容識別符的一產生日期來產生允許內容播放的播放允許資訊，或禁止內容播放的播放禁止資訊。例如，當內容識別符指出新內容不到產生日期起算的半年時，分散裝置將產生播放禁止資訊。另一方面，當內容識別符指出從產生日期起算已經大約半年或更長時間的舊內容時，分散裝置將產生播放允許資訊。

接下來，分散裝置將透過網際網路對執行裝置傳送已產生播放允許資訊或播放禁止資訊，且只要在接收播放允許資訊時，執行裝置將解密並且播放儲存在 DVD 中的已加密內容。

假設內容已從發行時存在達一段預定期間且已某種程度地符合內容的要求時，預測內容的未來銷售量並不是十分重要。於此，上述修改方案藉著允許使用者觀看該內容而優先考量把已購買 DVD 之使用者的利益。另一方面，當最近已發行內容且內容的未來銷售量是很重要的議題時，此修改方案將藉著禁止播放動作而優先考量著作權所有者的權利。即，此修改方案能夠調整使用者以及著作權所有

者的權益。

要注意的是，用以決定要傳送播放允許資訊以及播放禁止資訊中之何者的方法並不限於此，且分散裝置可參照各組內容來儲存反映出意圖的條件，例如，內容的著作權所有者以及代理經銷商。

[24-2]如前所述，記錄內容的媒體並不限於 DVD，且可為一種可重複寫入的記錄媒體。在此，配備有快閃記憶體的記憶卡係作為一實例。

當驗證簽章資訊或頭標資訊不成功時，執行裝置將刪除記錄在記憶卡中的部分或全部已加密內容。

據此，可以可靠地避免未授權內容於未來受到使用。

[24-3]當內容為 HD(高清晰度)視訊資料時，執行裝置將在把其轉換為 SD(標準清晰度)之後播放視訊資料，如果驗證不成功的話。

當內容為高品質聲音的(5.1 頻道)的音訊資料時，執行裝置將在把其轉換為標準品質聲音(2 頻道)的音訊資料之後播放音訊資料，如果驗證不成功的話。

因此，藉著在降低播放品質時進行播放，可以某種程度地調整使用者的便利以及著作權所有者的權益。

[25]在第二與第三實施例中，當把 DVD 載入到其上時，執行裝置將讀出金鑰區塊、已加密選擇位置資訊、頭標資訊簽章資訊以及已加密內容。然而，執行裝置可根據各個部件的處理進度且透過取得單元而僅讀出所需資訊。

例如，執行裝置可因此在載入 DVD 時僅讀出金鑰區塊、

在完成產生內容金鑰時僅讀出已加密選擇位置資訊、且在完成解密已加密選擇位置資訊時僅讀出簽章資訊與頭標資訊，並且隨後驗證簽章資訊。一旦完成驗證簽章資訊後，執行裝置將讀取由選擇位置資訊指出的 k 個已加密區塊。

相似地在第四實施例中，可僅視需要地讀取所需資訊。

[26]在第一實施例中，當讀取選出的 i 個已加密單元時，可增加讀出速度，藉著如下所述地配置讀出順序。

為了說明方便，在此將假設 i=4，且考量當中欲讀出 4 個已加密單元的事例。

在例如 DVD 的一光碟上，用以記錄資料的一區域將劃分為數個部分，且呈年輪型樣的區域係分別地稱為磁軌。數個區段係包括在各個磁軌中，且係逐區段地讀取且寫入資料。區段大小可例如為 512 位元組。於此，可利用磁軌識別碼、區段識別碼或區段大小來識別用以在 DVD 上讀出的數份資料。

第 71 圖展示出 DVD 1500 的組態以及取得單元 1601 的結構。圖中的同心圓區域為磁磁軌。

如第 71 圖所示，取得單元 1601 具有讀取頭部分(亦稱為"拾取器")1628 與旋轉軸 1629。將藉著旋轉旋轉軸 1629 來呈逆時鐘方向來旋轉 DVD 1500。圖中以虛線表示的箭頭係指出旋轉方向。藉著指定磁軌識別碼、區段識別碼或區段大小，取得單元 1601 可移動讀取頭部分 1628 並且取得供讀出的一份資料。

大致上來說，已知的是把讀取頭部分 1628 移動到儲存

有讀出目標資料之一磁軌可能需要花費時間。換言之，因為在DVD上從內部圓周移向外部圓周或者從外部圓周移向內部圓周的距離會增加，將花費較長時間來讀出資料。

在此，四個已加密單元"EU1_3"、"EU3_1"、"EU8_7"與"EU9_2"為讀出目標，且係分別地儲存在DVD 1500上的部分1591、1592、1593與1594中。

在DVD 1500中，係假設讀取頭部分1628係位於第71圖展示的位置中。

於此，根據第一實施例中說明的程序，取得單元1601將首先把讀取頭部分1628移動到部分1591存在的磁軌1501上，並且讀出記錄在部分1591中的已加密單元"EU1_3"。隨後，取得單元1601將把讀取頭部分1628移動到磁軌1504，並且從部分1592讀出已加密單元"EU3_1"。隨後，取得單元1601將以相似方式把讀取頭部分1628移動到磁軌1502以讀出部分1593中的已加密單元"EU8_7"，且後續地移動到磁軌1503以讀出部分1594中的已加密單元"EU9_2"。

因此，當採用第一實施例中所述的程序時，讀取頭部分1628的移動距離將變長，且因此要讀出所有的已加密單元便需要花費一段長時間。

在此，可改變讀出4個已加密單元的順序，以使讀取頭部分1628能永遠從其開始所在的一磁軌移動到最靠近的磁軌。即，取得單元1601將比較指出讀取頭部分1628之位置的磁軌編號以及儲存有該等4個已加密單元之部分

1591、1592、1593 與 1594 之位置的區段編號與磁軌編號。隨後，取得單元 1601 將重新配置已取得該等四個部分之區段編號與磁軌編號的順序，以使讀取頭部分 1628 能採用最短的移動距離以重新配置順序進行讀出與存取各個部分的動作。

據此，可縮短用以讀出資料所需的時間。此外，當欲讀出的已加密單元位於相同磁軌或鄰近磁軌上時，可根據讀取頭部分 1628 的目前位置以及指出當中儲存有個別已加密單元部分的區段編號來改變讀出順序。

要注意的是，用以最佳化讀出順序的一種方法係依據取得單元 1601 之旋轉軸與讀取頭部分的操作屬性，且因此在此說明的最佳化程序僅為一實例。例如，光碟的旋轉控制方法包括恆定角速度(CAV)方法以及恆定線速度(CLV)方法，且可考量該種方法的特徵。此外，當使用一硬碟而不是使用例如 DVD 的光碟時，可相似地達成讀出順序的配置。

同樣在第五與第六實施例中，可相似地改善讀出速度。根據第二至第四實施例的修改方案[20]亦是如此。

[27]在第一、第五與第六實施例中，執行裝置將隨機地選出 i 個已加密檔案，且從各個選出已加密檔案中進一步選出一個已加密單元。然而，選擇程序並不限於此，且可從一個已加密檔案中選出多個已加密單元，只要選出數量的總數為 i 即可。

[28]在第一、第五與第六實施例中，可在執行裝置中預設執行裝置選出的"i"的已加密單元，或者可寫入到 DVD 中。

隨著選出已加密單元的數量"I"變大，可增加驗證是否包括未授權內容的準確度，而亦會增加驗證簽章資訊動作的處理負載。

因此，欲選出的"I"個已加密單元係記錄在 DVD 中，且隨後執行裝置將根據從 DVD 取得的"I"來驗證簽章資訊。據此，可以在驗證動作中反映出 DVD 製造者的意圖。

此外，此項技術亦可適用於在第四實施例中選出 k 個已加密部份內容的動作。

[29]在第一、第五與第六實施例中，將藉著對合併 c 個檔案雜湊值而形成的合併結果套用簽章產生演算法來產生簽章資訊。然而，可藉著對計算一合併雜湊值、進一步把合併結果指派給雜湊函數且對所計算出的合併雜湊值套用簽章產生演算法來產生簽章資訊。

[30]在第一、第五與第六實施例中，頭標資訊係由具有二層式結構的雜湊值組成。換言之，該二層式結構係有下列組成：從個別已加密單元產生的單元雜湊值；以及從根據相同檔案產生之 m 個單元雜湊值中產生的檔案雜湊值。另一方面，簽章資訊係由 c 個檔案雜湊值組成。

反之，頭標資訊可包括具有三層式結構的雜湊值。確切來說，頭標資訊包括 y 個合併檔案雜湊值。該等 y 個合併檔案雜湊值係藉著首先把 c 個檔案雜湊值劃分為 y 個群組且個別地把合併結果(其係針對各個群組而合併檔案雜湊值)指派給雜湊函數而產生。於此，可藉著使用該等 y 個合併檔案雜湊值來產生簽章資訊。

因此，藉著增加結構中層體的數量，可以減少欲從 DVD 讀取的資訊。

[31]如第五實施例中所述，有時顯示出內容播放順序的播放順序檔案係儲存在 DVD 中。於此，DVD 可包括播放順序檔案的簽章資訊。

據此，如第五實施例中所述，即使未授權第三者進行加入或置換未授權內容的動作並且竄改播放順序檔案，可藉著驗證播放順序檔案的簽章資訊來檢測到該竄改動作，並且不會因此顯示出未授權內容。

[32]在第三實施例中，分散裝置 3100 之選擇單元 3105 從一組內容中選出的代表性部份內容總數量為(k 乘以 x)個。

於此，所有該等 c 個部份內容係至少被選出一次而作為一份代表性部份內容。據此，當儲存在 DVD 中的部分已加密內容受到置換時，可以增加檢測未授權內容的準確度。

[33]在第一、第五與第六實施例中，分散裝置係把單元檢選資訊寫入到 DVD 中。反之，分散裝置可對 DVD 寫入藉著使用內容金鑰來加密單元檢選資訊所產生的已加密單元檢選資訊。

此外，在第四實施例中，分散裝置將把內容位置資訊寫入到 DVD 中。反之，分散裝置可對 DVD 寫入藉著使用內容金鑰加密內容位置資訊所產生的已加密內容位置資訊。

[34]在第一至第六實施例與修改方案中，可藉著分別地把已加密單元指派給雜湊函數來計算單元雜湊值，而同時

可藉著分別地把數個部份內容指派給雜湊函數來計算部份雜湊值。然而，可從合併對應於已加密單元之一識別符、一份識別資訊以及已加密單元所形成的一合併結果來計算各個單元雜湊值。相似地，可從合併對應於部份內容之一識別符、一份識別資訊以及部份內容所形成的一合併結果來計算各個部份雜湊值。

[35]在第五實施例中，欲產生填充內容的資料大小與填充容量相同。然而，該資料大小並不限於此，只要該資料大小可使 DVD 上的剩餘閒置空間夠小即可。

[36]在第一至第六實施例中，執行裝置可藉著對外部監視器輸出視訊與音訊信號來播放該等內容。然而，執行裝置可具有內建的監視器。

[37]可把構成上述個別裝置的部分或全部部件組構成一單一系統 LSI(大型積體電路)。系統 LSI 為藉著把多個部件整合在一晶片上而產生的一種超多重功能的 LSI，且更確切來說，系統 LSI 為一種由微處理器、ROM、RAM 等構成的電腦系統。一電腦程式係儲存在 RAM 中。微處理器將根據該電腦程式來運作，且藉此該系統 LSI 可完成其功能。替代地，可在個別積體電路上建構各個部件。

雖然在此稱為系統 LSI，亦可稱為 IC、LSI、超級 LSI 以及超 LSI，依據整合的程度而定。此外，用以組構積體電路的方法並不限於 LSI，且可使用一種專屬的通訊電路或一般用途的處理器來達成。可使用在產生 LSI 之後進行編程的 FPGA(現場可編程閘陣列)，或者允許重新組態連結且設

定 LSI 中電路晶胞的可再組構處理器。

[38]本發明可為一種用以實現上述未授權內容檢測系統的方法。本發明可為由電腦實現該方法的一種電腦程式，或可為代表該電腦程式的一數位信號。

亦可由電腦可讀記錄媒體來實現本發明，例如軟碟片、硬碟、CD-ROM(光碟唯讀記憶體)、MO(磁性光學)碟片、DVD、DVD-ROM(數位多用途碟片唯讀記憶體)、DVD-RAM(數位多用途碟片隨機存取記憶體)、BD(Blu-ray 藍光碟片)、或上面記錄有上述電腦程式或數位信號的半導體記憶體。本發明亦可為記錄在該種儲存媒體上的電腦程式或數位信號。

本發明亦可為透過網路傳輸的電腦程式或數位信號，如由通信、有線/無線通訊以及網際網路表示，或透過資料傳播。

本發明亦可為一種具有微處理器與記憶體的電腦系統，其中該記憶體儲存該電腦程式而該微處理器則根據該電腦程式來運作。

電腦程式或數位信號可記錄在上述儲存媒體上，且傳輸到一獨立電腦系統，或者可替代地透過上述網路傳輸到獨立電腦系統。隨後，獨立電腦系統可執行該電腦程式或數位信號。

[39]本發明包括一種結構，其中可結合上述二或數個實施例以及修改方案。

產業應用性

本發明可運作性地、連續性地且重複地應用於產生、銷售、傳輸並且使用內容的產業中，且亦可應用於製造、銷售且使用用以顯示、編輯且處理該等內容之各種不同電子裝置的產業中。

【圖式簡單說明】

第 1 圖為一結構圖，其展示出第一實施例中一種未授權內容檢測系統的結構；

第 2 圖為一方塊圖，其展示出第一實施例中一種分散裝置 1100 的結構；

第 3 圖展示出欲輸入到分散裝置 1100 之內容 1120 的結構；

第 4 圖展示出由執行裝置資訊儲存單元 1104 儲存之裝置識別表 1130 的結構；

第 5 圖展示出由金鑰區塊產生單元 1103 產生之金鑰區塊 1150 的細節；

第 6 圖展示出由單元產生單元 1105 進行之分離內容產生程序的大致概要；

第 7 圖展示出由單元產生單元 1105 產生之單元檢選資訊 1200 的結構；

第 8 圖展示出由加密處理單元 1106 進行之加密處理動作的部分；

第 9 圖展示出加密處理單元 1106 產生之已加密內容 1330 的結構；

第 10 圖展示出由頭標資訊產生單元 1107 進行之頭標資訊 1260 產生程序的大致概要；

第 11 圖展示出由頭標資訊產生單元 1107 進行的第一雜湊表產生程序；

第 12 圖展示出由頭標資訊產生單元 1107 產生之第二雜湊表的細節；

第 13 圖展示出由簽章資訊產生單元 1111 進行的處理動作；

第 14 圖展示出由第一實施例中的 DVD 1500 儲存的資訊；

第 15 圖為一方塊圖，其展示出第一實施例中一種執行裝置 1600 的結構；

第 16 圖展示出由簽章資訊驗證單元 1611 進行之簽章資訊驗證處理動作的大致概要；

第 17 圖展示出由簽章資訊驗證單元 1611 進行之處理動作的部分；

第 18 圖展示出由簽章資訊驗證單元 1611 進行之第一已置換雜湊表的產生程序；

第 19 圖展示出由簽章資訊驗證單元 1611 進行之第二已置換雜湊表的產生程序；

第 20 圖展示出由簽章資訊驗證單元 1611 進行的簽章資訊驗證動作；

第 21 圖為一流程圖，其展示出分散裝置 1100 的運作性行為；

第 22 圖為一流程圖，其展示出分散裝置 1100 的運作性行為(續接第 21 圖)；

第 23 圖展示出由執行裝置 1600 進行的簽章資訊驗證程序；

第 24 圖為一流程圖，其展示出執行裝置 1600 的運作性行為；

第 25 圖為一流程圖，其展示出執行裝置 1600 的運作性行為(續接第 24 圖)；

第 26 圖為一方塊圖，其根據第一實施例的修改方案展示出執行裝置 1100b 的結構；

第 27 圖為一方塊圖，其根據第二實施例展示出一種分散裝置 2100 的結構；

第 28 圖展示出內容 2120 以及欲輸入到分散裝置 2100 中的識別資訊部分；

第 29 圖展示出由選擇單元 2105 進行之處理動作的大致概要；

第 30 圖展示出由頭標資訊產生單元 2107 產生之選擇位置資訊 2160 的結構；

第 31 圖展示出由頭標資訊產生單元 2107 產生之頭標資訊 2200 的結構；

第 32 圖展示出由加密處理單元 2109 產生之已加密內容的結構；

第 33 圖展示出記錄在第二實施例中之 DVD 2500 上的資訊；

第 34 圖為一方塊圖，其展示出第二實施例中一種執行裝置 2600 的結構；

第 35 圖為一流程圖，其展示出分散裝置 2100 的運作性行為；

第 36 圖為一流程圖，其展示出執行裝置 2600 的運作性行為；

第 37 圖為一方塊圖，其展示出第三實施例中一種分散裝置 3100 的結構；

第 38 圖展示出由頭標資訊產生單元 3107 產生之頭標選擇資訊 3130 的結構；

第 39 圖展示出記錄在第三實施例中之 DVD 3500 上的資訊；

第 40 圖為一方塊圖，其展示出第三實施例中一種執行裝置 3600 的結構；

第 41 圖為一方塊圖，其展示出第四實施例中一種分散裝置 4100 的結構；

第 42 圖展示出由部份內容產生單元 4105 產生的分離內容以及識別資訊部分；

第 43 圖展示出由頭標資訊產生單元 4107 產生之內容位置資訊 4140 的結構；

第 44 圖展示出由頭標資訊產生單元 4107 產生之頭標資訊 4160 的結構；

第 45 圖展示出記錄在第四實施例中之 DVD 4500 上的資訊；

第 46 圖為一方塊圖，其展示出第四實施例中一種執行裝置 4600 的結構；

第 47 圖展示出由選擇單元 4611 進行之選擇位置資訊 4620 產生程序的大致概要；

第 48 圖展示出由選擇單元 4611 進行之選出頭標資訊 4630 產生程序的大致概要；

第 49 圖展示出由部份內容解密單元 4616 進行之解密處理動作的大致概要；

第 50 圖為一流程圖，其展示出分散裝置 4100 的運作性行為；

第 51 圖展示出由分散裝置 4100 進行之簽章資訊 4170 的產生程序；

第 52 圖為一流程圖，其展示出執行裝置 4600 的運作性行為；

第 53 圖為一流程圖，其展示出執行裝置 4600 的運作性行為(續接第 52 圖)；

第 54 圖展示出由執行裝置 4600 進行之簽章資訊以及頭標資訊的驗證程序；

第 55 圖為一方塊圖，其展示出第五實施例中一種分散裝置 5100 的結構；

第 56 圖展示出由填充內容產生單元 5108 產生之分離填充內容 5120 的結構；

第 57 圖展示出從填充內容產生單元 5108 輸出之單元檢選資訊 5140 的結構；

第 58 圖展示出由頭標資訊產生單元 5107 進行之頭標資訊 5109 產生程序的大致概要；

第 59 圖展示出由頭標資訊產生單元 5107 產生之第二雜湊表 5180 的結構；

第 60 圖展示出記錄在第五實施例中之 DVD 5500 上的資訊；

第 61 圖為一方塊圖，其展示出第五實施例中一種執行裝置 5600 的結構；

第 62 圖為一流程圖，其展示出分散裝置 5100 的運作性行為；

第 63 圖為一流程圖，其展示出分散裝置 5100 的運作性行為(續接第 62 圖)；

第 64 圖為一流程圖，其展示出執行裝置 5600 的運作性行為；

第 65 圖展示出一種想像未授權 DVD 5500b；

第 66 圖展示出一種想像未授權 DVD 5500c；

第 67 圖為一方塊圖，其展示出第六實施例中一種分散裝置 6100 的結構；

第 68 圖展示出由配置產生單元 6108 產生之寫入配置資訊 6120；

第 69 圖展示出記錄在第六實施例中之 DVD 6500 上的資訊；

第 70 圖為一方塊圖，其展示出第六實施例中一種執行裝置 6600 的結構；以及

第71圖展示出DVD 1500的組態以及取得單元1601的結構。

【主要元件符號說明】

1	未授權內容檢測系統	1122	檔案
1100	分散裝置	1123	檔案
1100b	分散裝置	1124	檔案
1101b	輸入單元	1130	裝置識別表
1101	輸入單元	1131	裝置識別符
1102	內容金鑰產生單元	1136	裝置金鑰
1103	金鑰區塊產生單元	1141	裝置識別符
1104	執行裝置資訊儲存單元	1142	已加密內容金鑰
		1150	金鑰區塊
1105	單元產生單元	1160	分離內容
1105b	單元產生單元	1161	檔案識別符
1106	加密處理單元	1171	分離檔案
1106b	加密處理單元	1176	分離檔案資訊
1107	頭標資訊產生單元	1177	分離檔案資訊
1111	簽章資訊產生單元	1178	分離檔案資訊
1112	簽章金鑰儲存單元	1179	分離檔案資訊
1113	簽章金鑰	1181	單元識別符
1114	記錄單元	1186	單元
1114b	記錄單元	1191	單元資訊
1120	內容	1192	單元資訊
1121	檔案	1193	單元資訊

1194	單元資訊	1282	單元雜湊資訊
1200	單元檢選資訊	1283	單元雜湊資訊
1201	檔案資訊	1284	單元雜湊資訊
1202	檔案資訊	1291	檔案雜湊值
1203	檔案資訊	1301	檔案雜湊資訊
1204	檔案資訊	1302	檔案雜湊資訊
1211	檔案識別符	1303	檔案雜湊資訊
1216	檔案識別資訊	1304	檔案雜湊資訊
1221	單元編號	1310	簽章資訊
1231	已加密單元	1330	已加密內容
1241	已加密單元資訊	1331	已加密檔案
1242	已加密單元資訊	1332	已加密檔案
1243	已加密單元資訊	1333	已加密檔案
1244	已加密單元資訊	1334	已加密檔案
1246	已加密分離檔案資訊	1500	DVD
1247	已加密分離檔案資訊	1501	磁軌
1248	已加密分離檔案資訊	1502	磁軌
1249	已加密分離檔案資訊	1503	磁軌
1251	已加密分離檔案	1504	磁軌
1260	頭標資訊	1510	金鑰區塊
1261	第一雜湊表	1511	已加密單元
1269	第二雜湊表	1512	已加密單元
1271	單元雜湊值	1513	已加密單元
1281	單元雜湊資訊	1530	單元檢選資訊

1531 檔案識別符
1533 檔案識別符
1541 檔案資訊
1542 檔案資訊
1543 檔案資訊
1550 頭標資訊
1551 第一雜湊表
1552 第一雜湊表
1553 第一雜湊表
1556 第二雜湊表
1557 第一雜湊表
1561 檔案雜湊資訊
1562 檔案雜湊資訊
1563 檔案雜湊資訊
1567 檔案雜湊資訊
1570 簽章資訊
1571 檔案雜湊值
1572 檔案雜湊值
1573 檔案雜湊值
1574 檔案雜湊值
1580 已加密內容
1581 已加密檔案
1582 已加密檔案
1583 已加密檔案
1587 已加密檔案
1591 DVD上的部分
1592 DVD上的部分
1593 DVD上的部分
1594 DVD上的部分
1600 執行裝置
1601 取得單元
1602 內容金鑰取得單元
1604 裝置金鑰儲存單元
1606 執行單元
1608 裝置識別符
1609 裝置金鑰
1611 簽章資訊驗證單元
1612 驗證金鑰儲存單元
1613 驗證金鑰
1620 監視器
1628 讀取頭部分
1631 第一已置換雜湊表
1633 第一已置換雜湊表
1637 第一已置換雜湊表
1639 第二已置換雜湊表
1641 置換檔案雜湊值
1643 置換檔案雜湊值
1647 置換檔案雜湊值

2100	分散裝置
2101	輸入單元
2102	內容金鑰產生單元
2103	金鑰區塊產生單元
2105	選擇單元
2107	頭標資訊產生單元
2108	簽章資訊產生單元
2109	加密處理單元
2114	記錄單元
2120	內容
2121	部份內容
2122	部份內容
2123	部份內容
2127	部份內容
2131	識別資訊
2132	識別資訊
2133	識別資訊
2134	識別資訊
2137	識別資訊
2141	代表性資訊
2142	代表性資訊
2143	代表性資訊
2160	選擇位置資訊
2161	代表性檢測資訊
2162	代表性檢測資訊
2163	代表性檢測資訊
2171	識別資訊識別符
2176	識別資訊
2200	頭標資訊
2201	代表性雜湊資訊
2202	代表性雜湊資訊
2203	代表性雜湊資訊
2211	識別資訊識別符
2212	識別資訊識別符
2213	識別資訊識別符
2216	部分雜湊值
2217	部分雜湊值
2218	部分雜湊值
2220	已加密內容
2500	DVD
2510	金鑰區塊
2530	已加密選擇位置資訊
2550	頭標資訊
2570	簽章資訊
2580	已加密內容
2600	執行裝置
2601	取得單元
2602	內容金鑰取得單元

2606	位置資訊解密單元	3600	執行裝置
2611	簽章資訊驗證單元	3601	取得單元
2616	代表性部份內容解密單元	4100	分散裝置
		4101	輸入單元
2617	頭標資訊驗證單元	4102	內容金鑰產生單元
2618	執行單元	4103	金鑰區塊產生單元
3100	分散裝置	4104	執行裝置資訊儲存單元
3105	選擇單元		
3107	頭標資訊產生單元	4105	部份內容產生單元
3108	簽章資訊產生單元	4107	頭標資訊產生單元
3109	加密處理單元	4108	簽章資訊產生單元
3114	記錄單元	4109	加密處理單元
3130	已產生頭標選擇資訊	4114	記錄單元
3500	DVD	4119	已接收內容
3510	金鑰區塊	4120	分離內容
3520	頭標選擇資訊	4121	部份內容
3530	第一頭標群組	4122	部份內容
3531	頭標識別符	4123	部份內容
3532	已加密選擇位置資訊	4127	部份內容
3533	頭標資訊	4131	識別資訊
3534	簽章資訊	4140	內容位置資訊
3540	第二頭標群組	4141	內容檢測資訊
3560	第x頭標群組	4142	內容檢測資訊
3580	已加密內容	4143	內容檢測資訊

4146	內容檢測資訊	4582	已加密部份內容
4151	識別資訊識別符	4583	已加密部份內容
4160	頭標資訊	4584	已加密部份內容
4161	部分雜湊資訊	4586	已加密部份內容
4162	部分雜湊資訊	4591	部份內容
4163	部分雜湊資訊	4592	部份內容
4166	部分雜湊資訊	4593	部份內容
4170	簽章資訊	4594	部份內容
4171	識別資訊識別符	4596	部份內容
4172	部份雜湊值	4600	執行裝置
4500	DVD	4601	取得單元
4510	金鑰區塊	4602	內容金鑰取得單元
4530	內容位置資訊	4606	簽章資訊驗證單元
4531	內容檢測資訊	4611	選擇單元
4532	內容檢測資訊	4616	部份內容解密單元
4533	內容檢測資訊	4617	頭標資訊驗證單元
4536	內容檢測資訊	4620	已產生選擇位置資訊
4550	頭標資訊	4621	識別資訊識別符
4551	部分雜湊資訊	4622	識別資訊識別符
4553	部分雜湊資訊	4623	識別資訊識別符
4556	部分雜湊資訊	4624	部份內容
4570	簽章資訊	4630	選擇頭標資訊
4580	已加密內容	4631	識別資訊識別符
4581	已加密部份內容	4632	部份雜湊值

4650	驗證內容	5151	檔案識別符
4651	驗證部份內容資訊	5152	檔案識別資訊
4652	驗證部份內容資訊	5153	單元編號
4656	驗證部份內容資訊	5156	填充檔案資訊
5100	分散裝置	5157	檔案識別符
5105	單元產生單元	5160	已加密分離內容
5106	加密處理單元	5171	第一雜湊表
5107	頭標資訊產生單元	5172	第一雜湊表
5108	填充內容產生單元	5173	第一雜湊表
5111	簽章資訊產生單元	5176	第一雜湊表
5114	記錄單元	5177	第一雜湊表
5120	分離填充內容	5180	第二雜湊表
5121	單元資訊	5181	檔案雜湊資訊
5122	單元資訊	5182	檔案雜湊資訊
5123	單元資訊	5183	檔案雜湊資訊
5126	單元資訊	5186	檔案雜湊資訊
5131	單元識別符	5187	檔案雜湊資訊
5132	單元	5190	頭標資訊
5140	單元檢選資訊	5500	DVD
5141	檔案資訊	5500a	DVD
5142	檔案資訊	5510	金鑰區塊
5143	檔案資訊	5530	單元檢選資訊
5146	檔案資訊	5550	頭標資訊
5147	檔案資訊	5550a	頭標資訊

5550b	頭標資訊	6120	配置資訊
5550c	頭標資訊	6121	區域
5570	已接收簽章資訊	6122	區域
5580	已加密內容	6123	區域
5590	填充內容	6124	區域
5600	執行裝置	6125	區域
5606	執行單元	6126	區域
5611	簽章資訊驗證單元	6500	DVD
5701	區域	6510	金鑰區塊
5702	區域	6530	單元檢選資訊
5703	區域	6550	頭標資訊
5704	區域	6560	區域資訊
5705	區域	6570	簽章資訊
5707	區域	6580	已加密內容
5711	區域	6600	執行裝置
6100	分散裝置	6601	取得單元
6103	金鑰區塊產生單元	6603	區域資訊儲存單元
6105	單元產生單元	6604	加密傳遞單元
6106	加密處理單元	6605	加密金鑰儲存單元
6107	頭標資訊產生單元	6606	執行單元
6108	配置產生單元	6607	解密傳遞單元
6109	區域資訊產生單元	6608	解密金鑰儲存單元
6111	簽章資訊產生單元	6611	簽章資訊驗證單元
6114	記錄單元	6620	驅動機單元

6625 內容執行單元

S1011~S1028 步驟

S1029~S1034 步驟

S1041~S1084 步驟

S1059~S1069 步驟

S2011~S2024 步驟

S2041~S2059 步驟

S4012~S4026 步驟

S4041~S4062 步驟

S4064~S4071 步驟

S5011~S5032 步驟

S5033~S5042 步驟

S5061~S5091 步驟

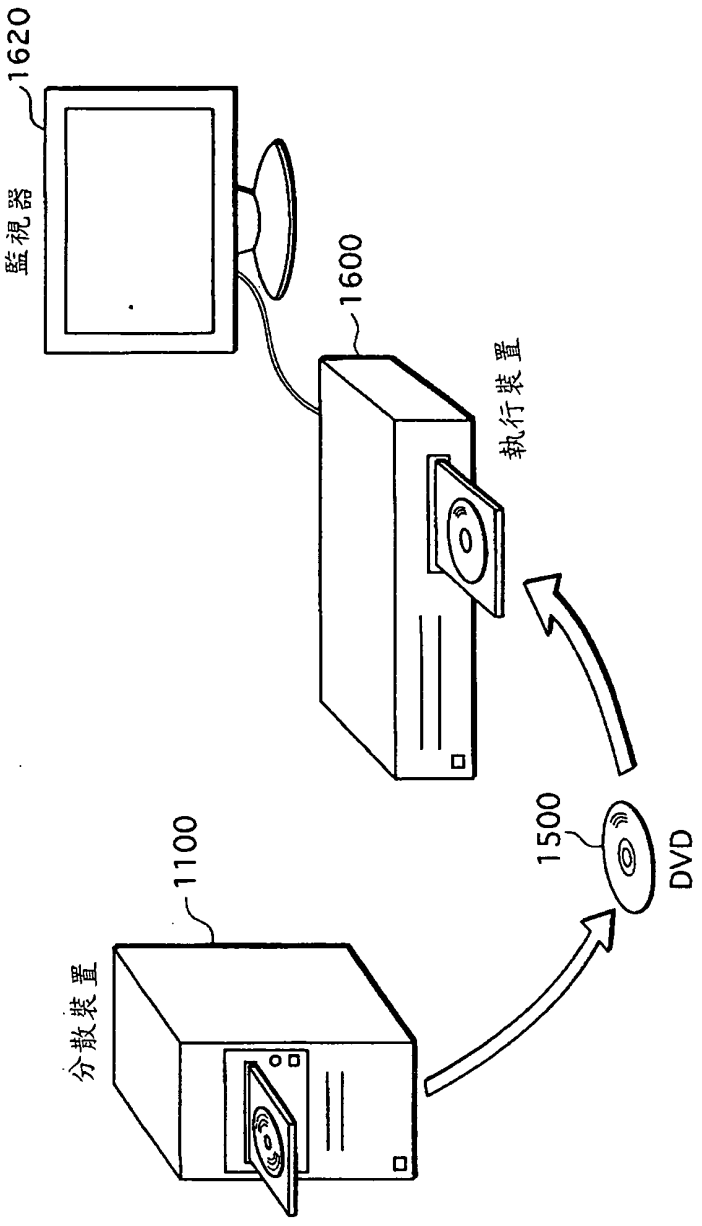
五、中文發明摘要：

在播放內容的過程中，執行裝置上用以進行播放動作的處理負載是很高的，因為該執行裝置係並行地與內容播放動作進行驗證內容有效性的動作，且因此該執行裝置必須配備有高度有效率的處理器。本發明可藉著針對驗證動作使用從錄製在DVD上而構成已加密內容之多個已加密單元中隨機地選出一預定數量的已加密單元來降低驗證動作中的處理負載。此外，本發明能夠藉著在每每進行驗證動作時隨機地選出一預定數量的已加密單元而相當程度地改進檢測未授權內容的準確度。

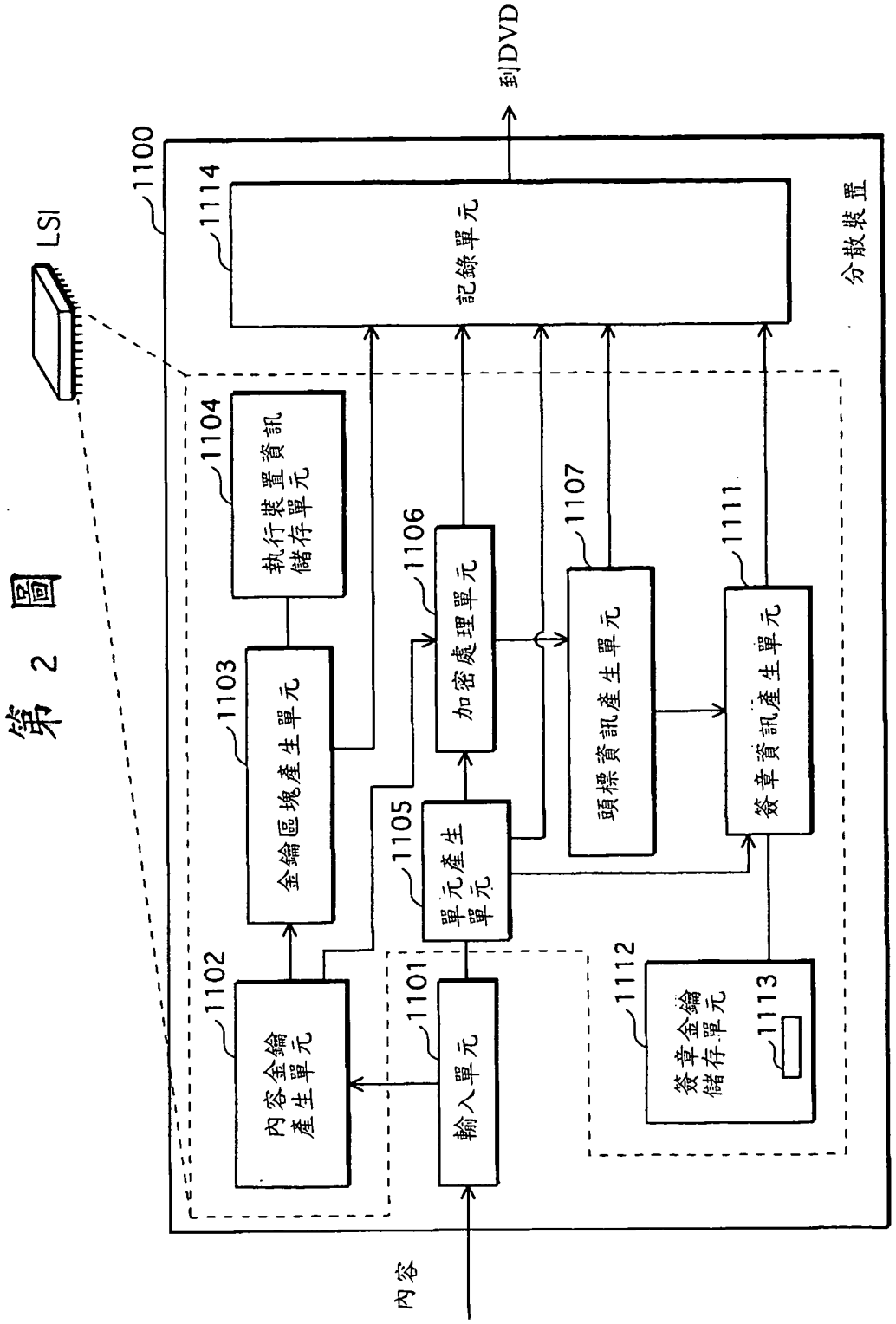
六、英文發明摘要：

Processing load on an executing device for conducting playback is high during the playback of contents since the executing device performs verification of the contents validity in parallel with the contents playback, and therefore the executing device has to be equipped with a highly efficient processor. The present invention reduces the processing load involved in the verification by using, for the verification, only a predetermined number of encrypted units selected randomly from multiple encrypted units constituting encrypted contents recorded on the DVD. In addition, the present invention is capable of improving the accuracy of detecting unauthorized contents to some extent by randomly selecting a predetermined number of encrypted units every time the verification is performed.

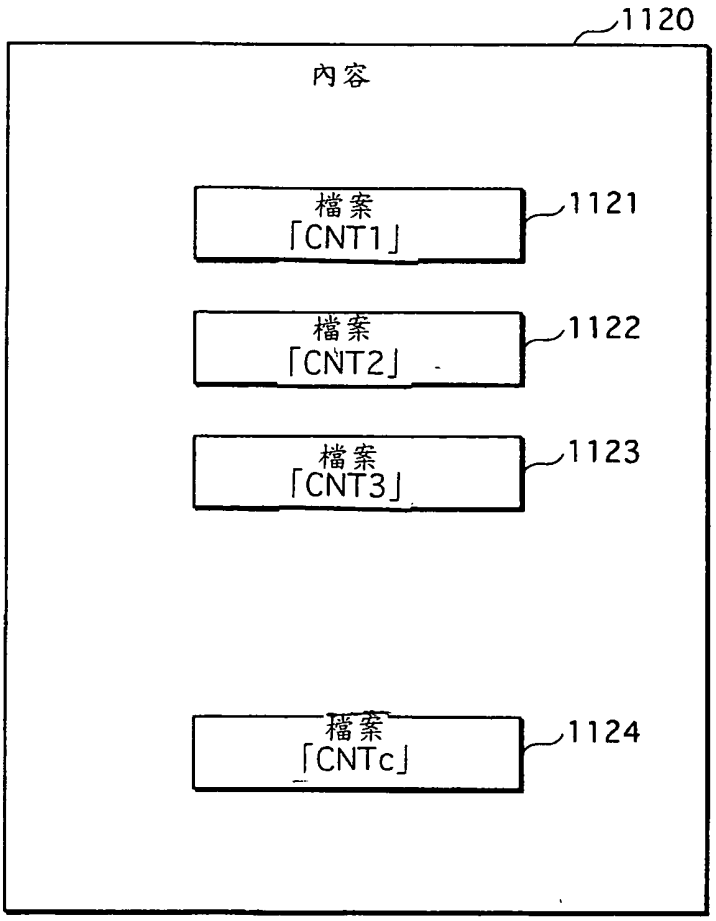
第 1 圖



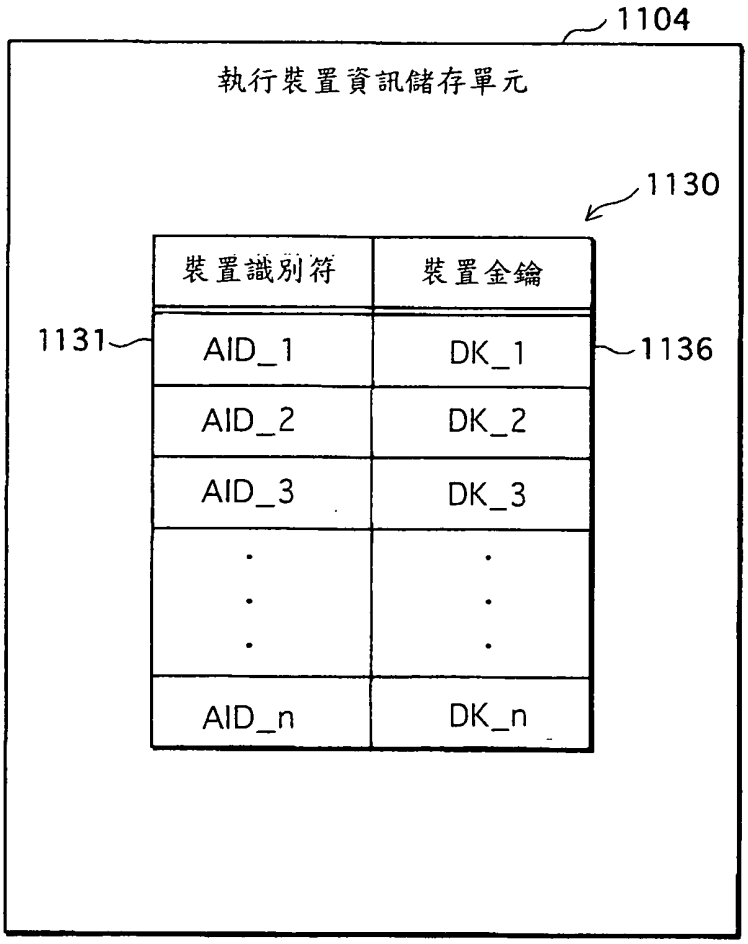
第 2 圖


LSI
1100
分散裝置
到DVD
內容
1101
輸入單元
1102
內容金鑰產生單元
1103
金鑰區塊產生單元
1104
執行裝置資訊儲存單元
1105
單元產生單元
1106
加密處理單元
1107
頭標資訊產生單元
1111
簽章資訊產生單元
1112
簽章金鑰儲存單元
1113
1114
記錄單元

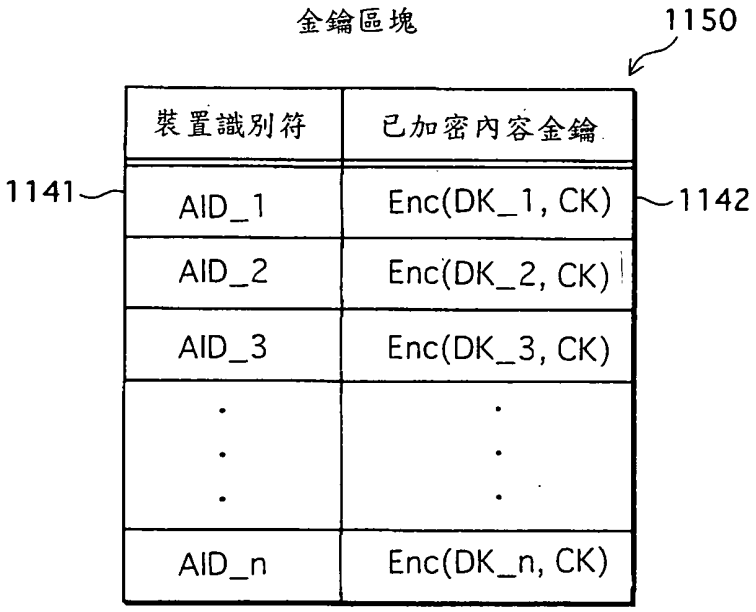
第 3 圖



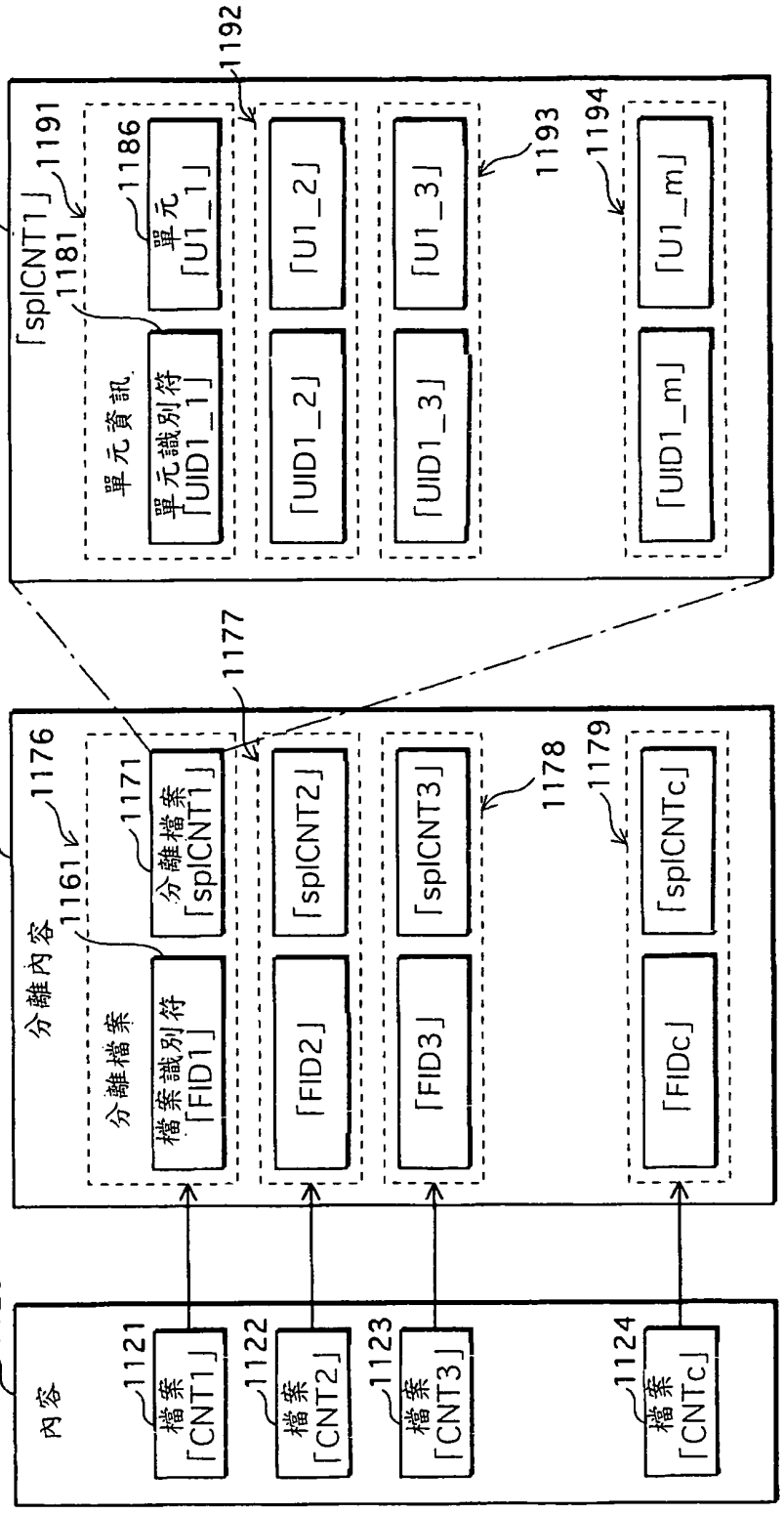
第 4 圖


1104
執行裝置資訊儲存單元
1130
裝置識別符
裝置金鑰
1131
AID_1
DK_1
1136
AID_2
DK_2
AID_3
DK_3
AID_n
DK_n

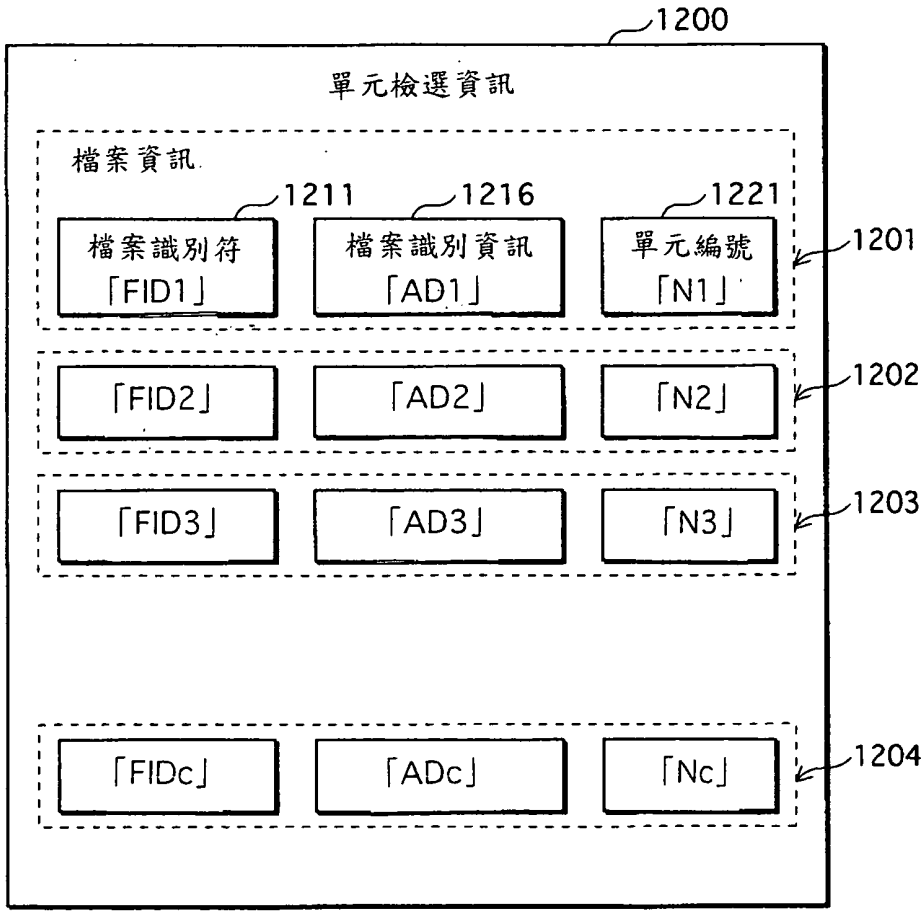
第 5 圖


金鑰區塊
1150
裝置識別符
已加密內容金鑰
1141
1142
AID_1
Enc(DK_1, CK)
AID_2
Enc(DK_2, CK)
AID_3
Enc(DK_3, CK)
AID_n
Enc(DK_n, CK)

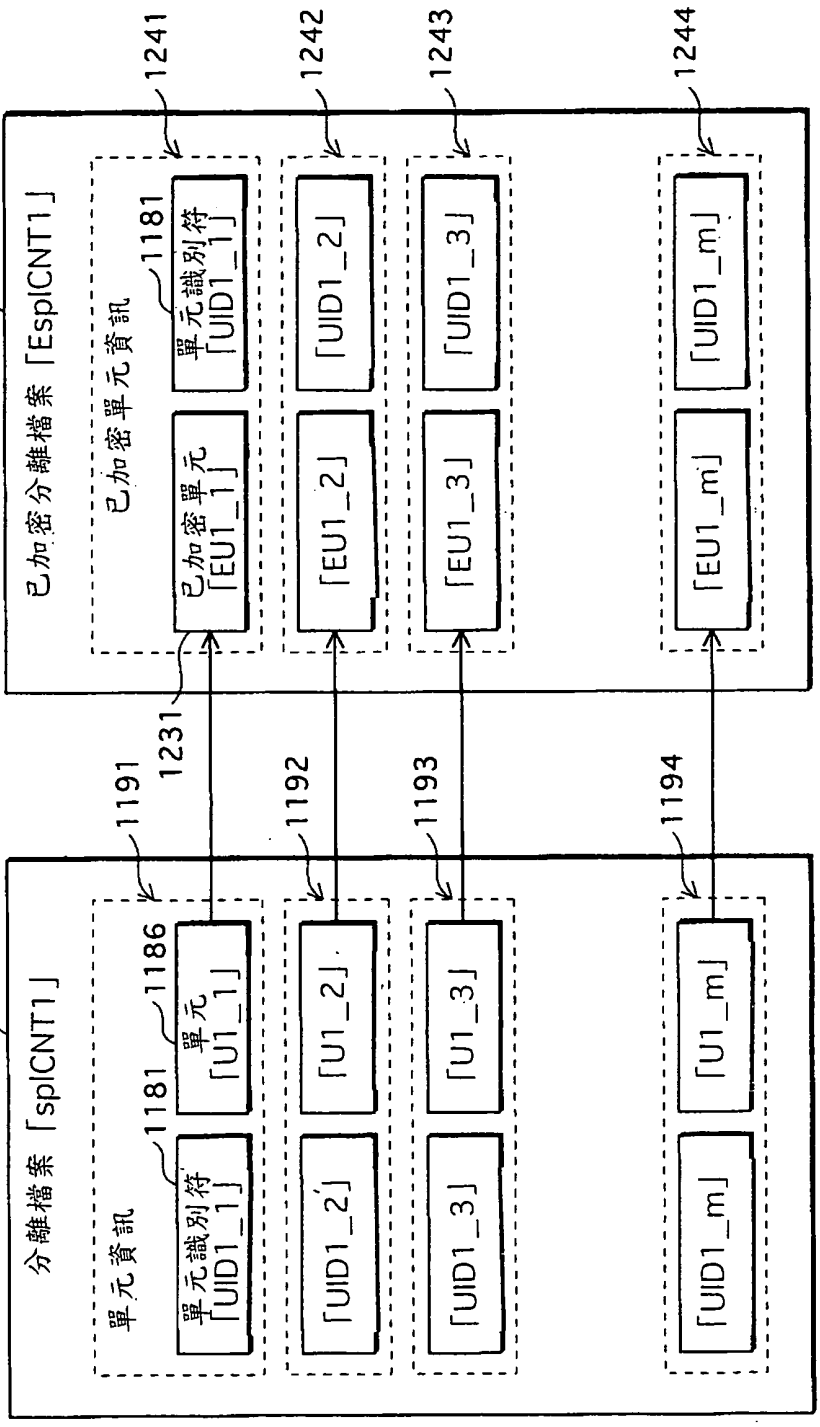
第 6 圖


1171
「splCNT1」
1191
1181
單元資訊
單元識別符
「UID1_1」
1186
單元
「U1_1」
1192
「UID1_2」
「U1_2」
「UID1_3」
「U1_3」
1193
「UID1_m」
「U1_m」
1194
1160
1176
分離內容
1161
分離檔案
檔案識別符
「FID1」
1171
分離檔案
「splCNT1」
1177
「FID2」
「splCNT2」
「FID3」
「splCNT3」
1178
「FIDc」
「splCNTc」
1179
1120
內容
1121
檔案
「CNT1」
1122
檔案
「CNT2」
1123
檔案
「CNT3」
1124
檔案
「CNTc」

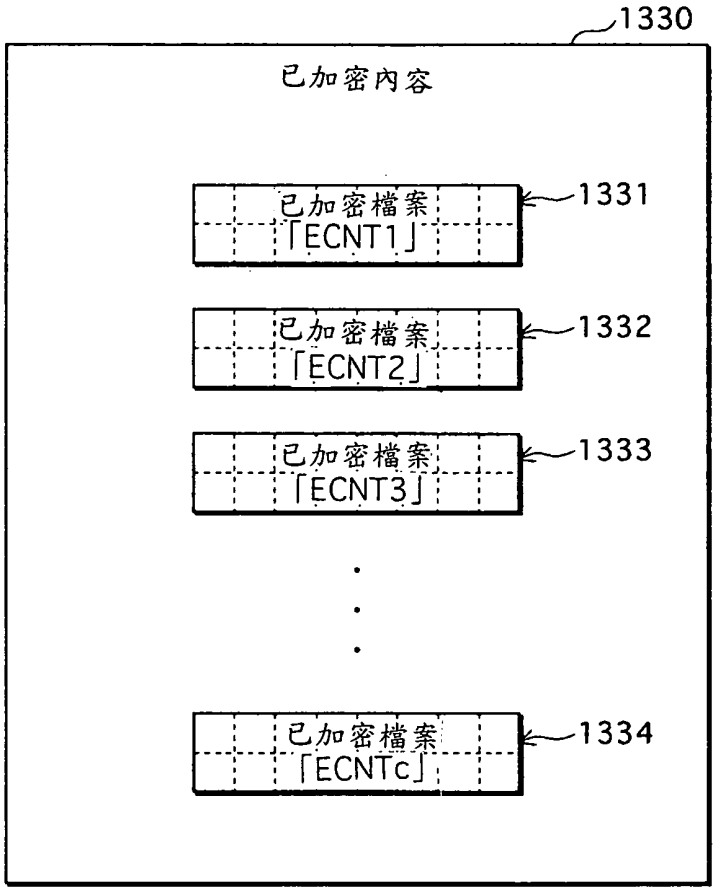
第 7 圖


1200
單元檢選資訊
檔案資訊
1211
1216
1221
檔案識別符
「FID1」
檔案識別資訊
「AD1」
單元編號
「N1」
1201
「FID2」
「AD2」
「N2」
1202
「FID3」
「AD3」
「N3」
1203
「FIDc」
「ADc」
「Nc」
1204

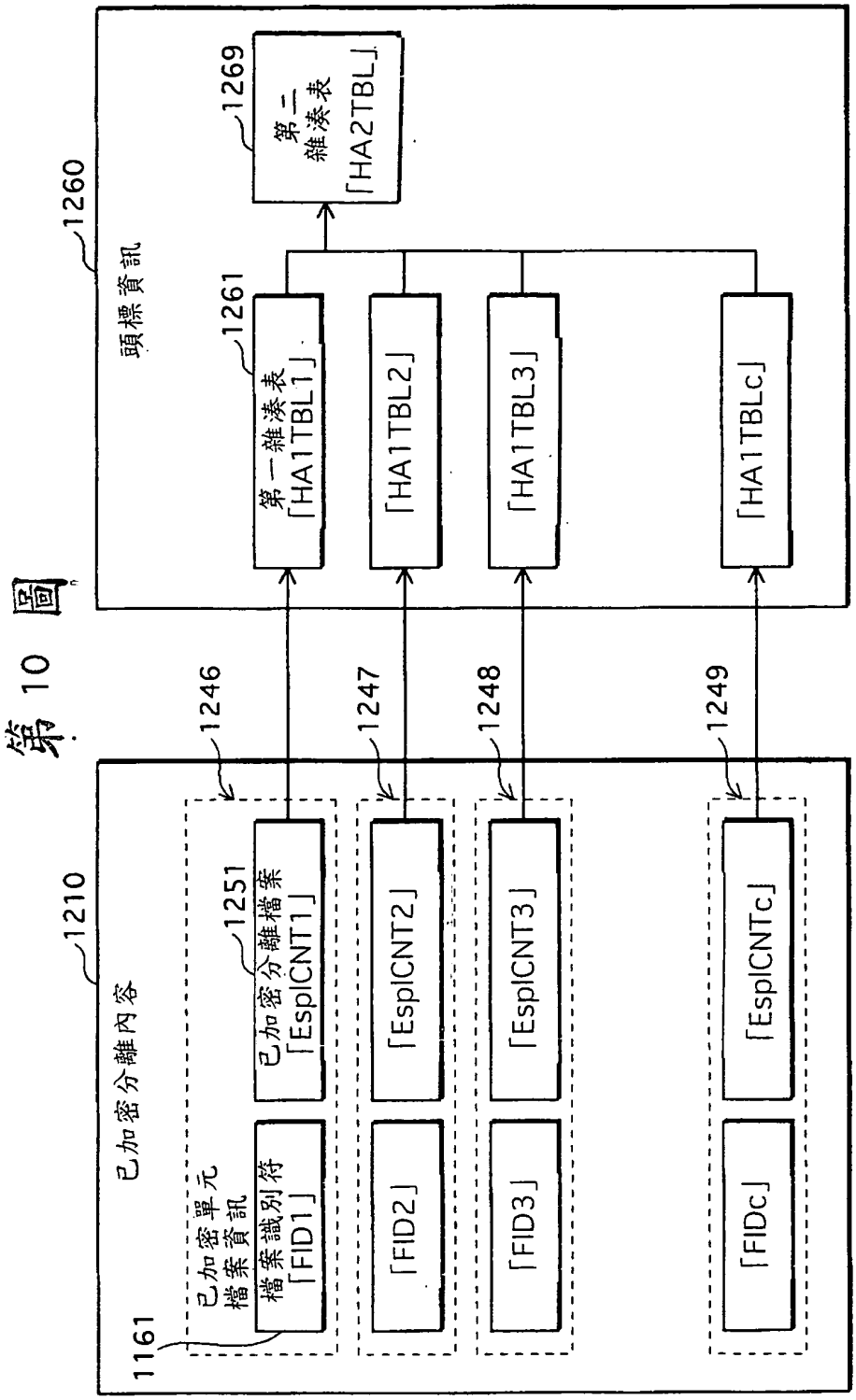
第 8 圖


1171
分離檔案「splCNT1」
單元資訊
1181
單元識別符「UID1_1」
1186
單元「U1_1」
「UID1_2」
「U1_2」
「UID1_3」
「U1_3」
「UID1_m」
「U1_m」
1191
1192
1193
1194
1231
1251
已加密分離檔案「EsplCNT1」
已加密單元資訊
1181
單元識別符「UID1_1」
已加密單元「EU1_1」
「UID1_2」
「EU1_2」
「UID1_3」
「EU1_3」
「UID1_m」
「EU1_m」
1241
1242
1243
1244

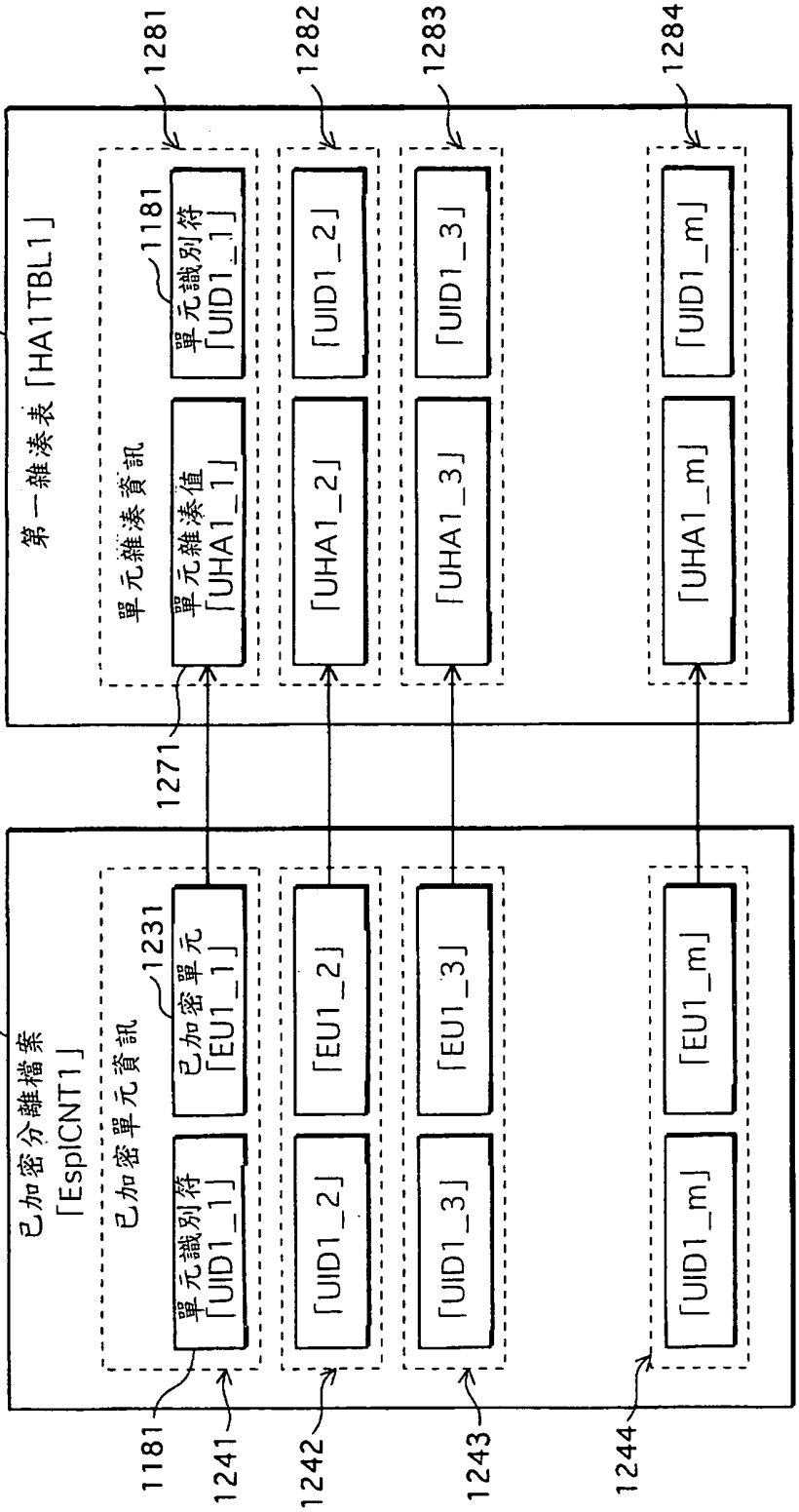
第 9 圖


1330
已加密內容
已加密檔案「ECNT1」
1331
已加密檔案「ECNT2」
1332
已加密檔案「ECNT3」
1333
已加密檔案「ECNTc」
1334

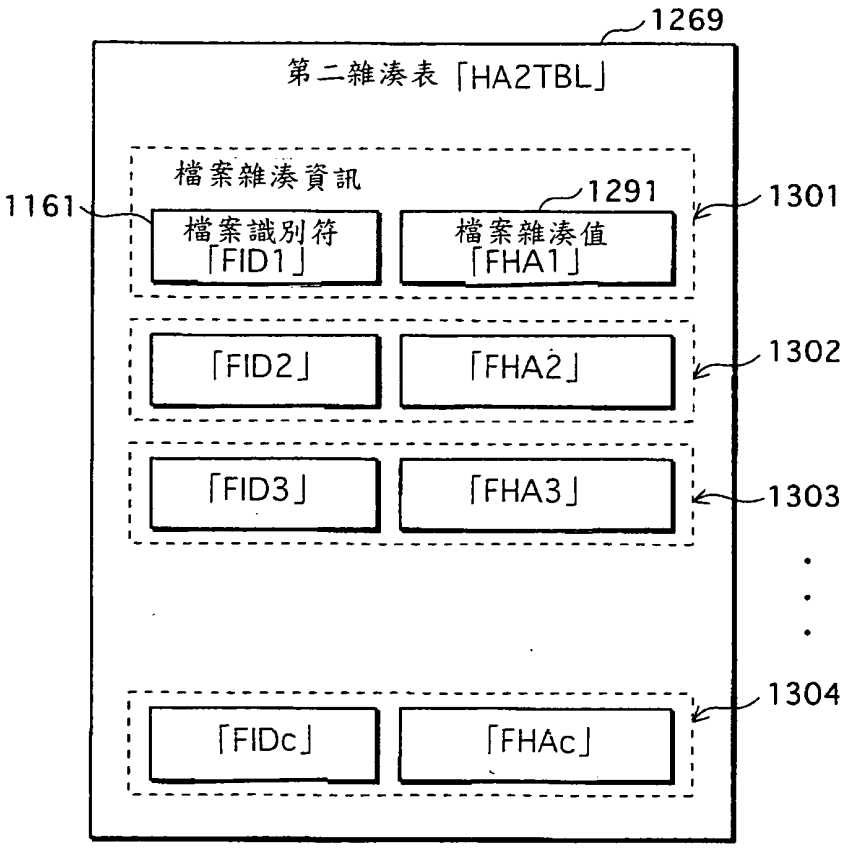
第10圖


1260
頭標資訊
1269
第二雜湊表
「HA2TBL」
1261
第一雜湊表
「HA1TBL1」
「HA1TBL2」
「HA1TBL3」
「HA1TBLc」
1246
1247
1248
1249
1210
已加密分離內容
1251
已加密分離檔案
「EsplCNT1」
「EsplCNT2」
「EsplCNT3」
「EsplCNTc」
已加密單元
檔案資訊
檔案識別符
「FID1」
「FID2」
「FID3」
「FIDc」
1161

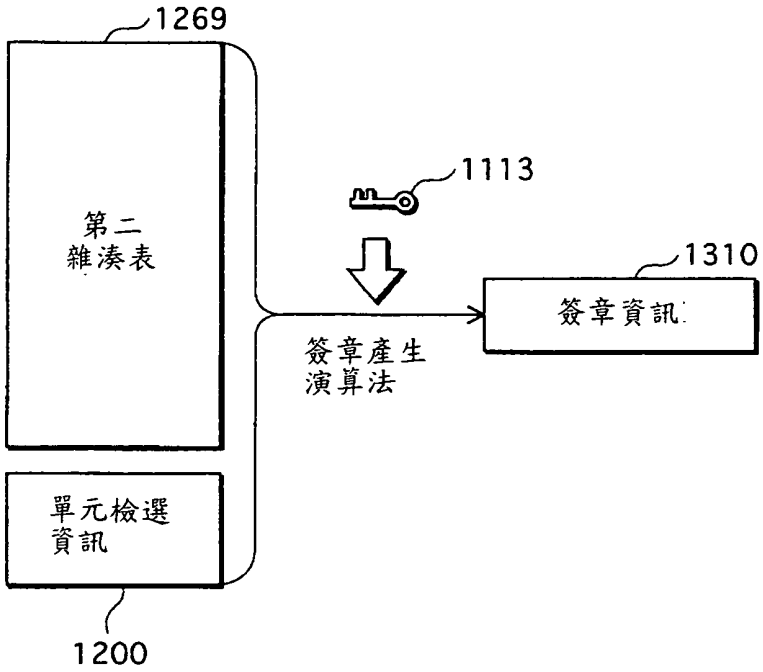
第 11 圖


1261
第一雜湊表「HA1TBL1」
1281
1282
1283
1284
單元雜湊資訊
1181
單元識別符「UID1_1」
單元雜湊值「UHA1_1」
「UID1_2」
「UHA1_2」
「UID1_3」
「UHA1_3」
「UID1_m」
「UHA1_m」
1271
1251
已加密分離檔案「EsplCNT1」
已加密單元資訊
1231
已加密單元「EU1_1」
「EU1_2」
「EU1_3」
「EU1_m」
「UID1_2」
「UID1_3」
「UID1_m」
1181
1241
1242
1243
1244

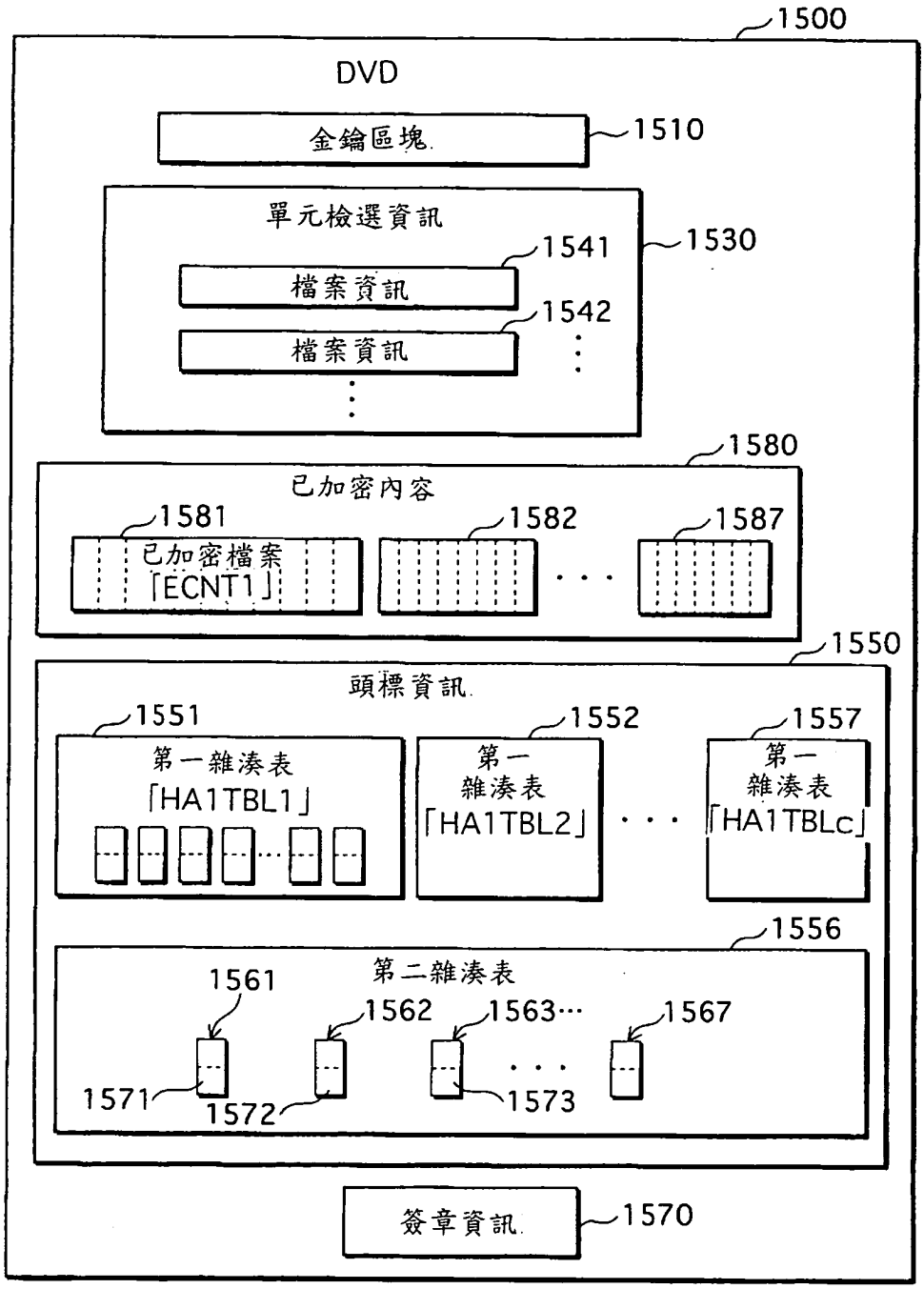
第 12 圖


1269
第二雜湊表「HA2TBL」
檔案雜湊資訊
1161
1291
1301
檔案識別符
「FID1」
檔案雜湊值
「FHA1」
「FID2」
「FHA2」
1302
「FID3」
「FHA3」
1303
1304
「FIDc」
「FHAc」

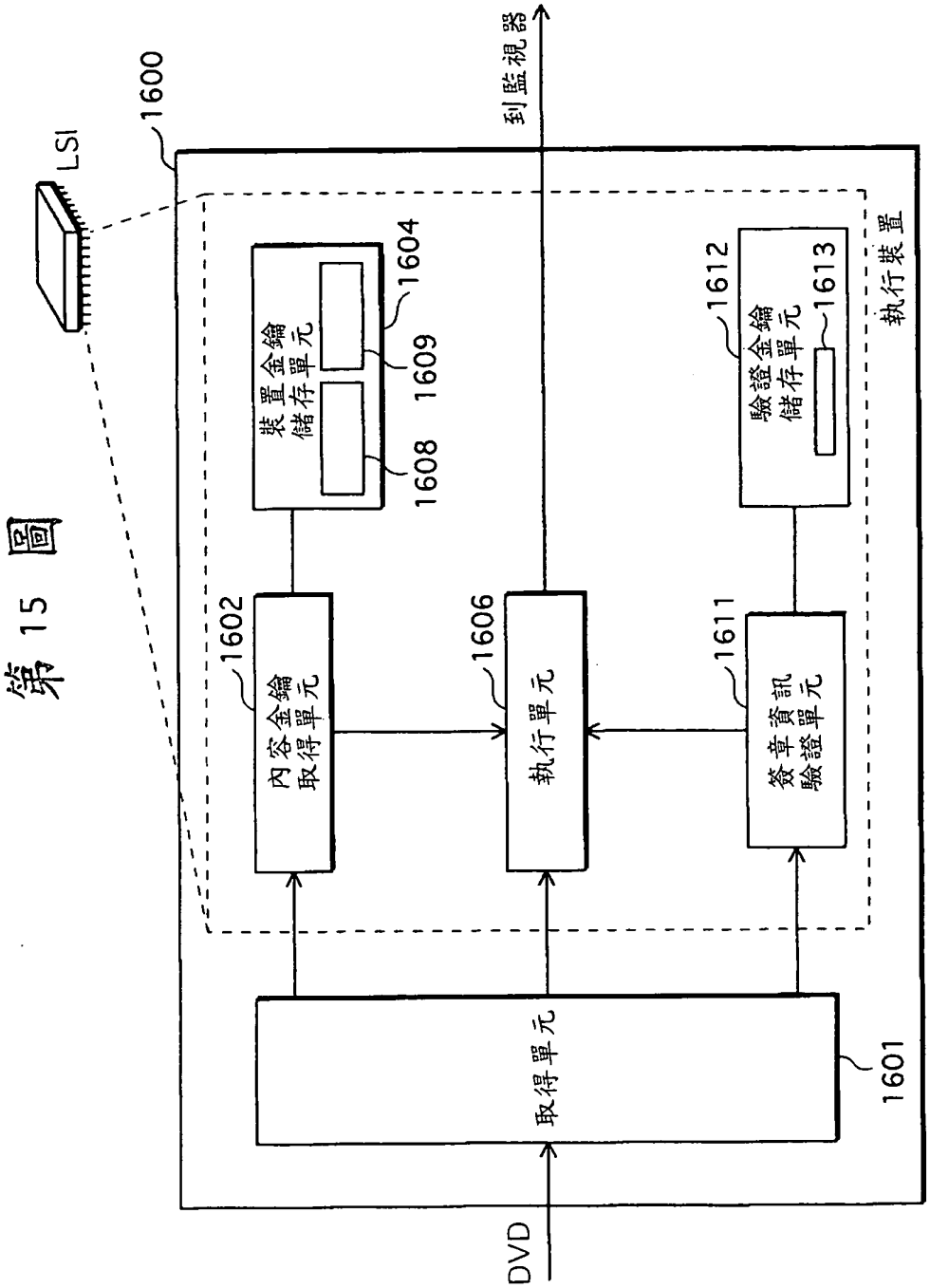
第 13 圖



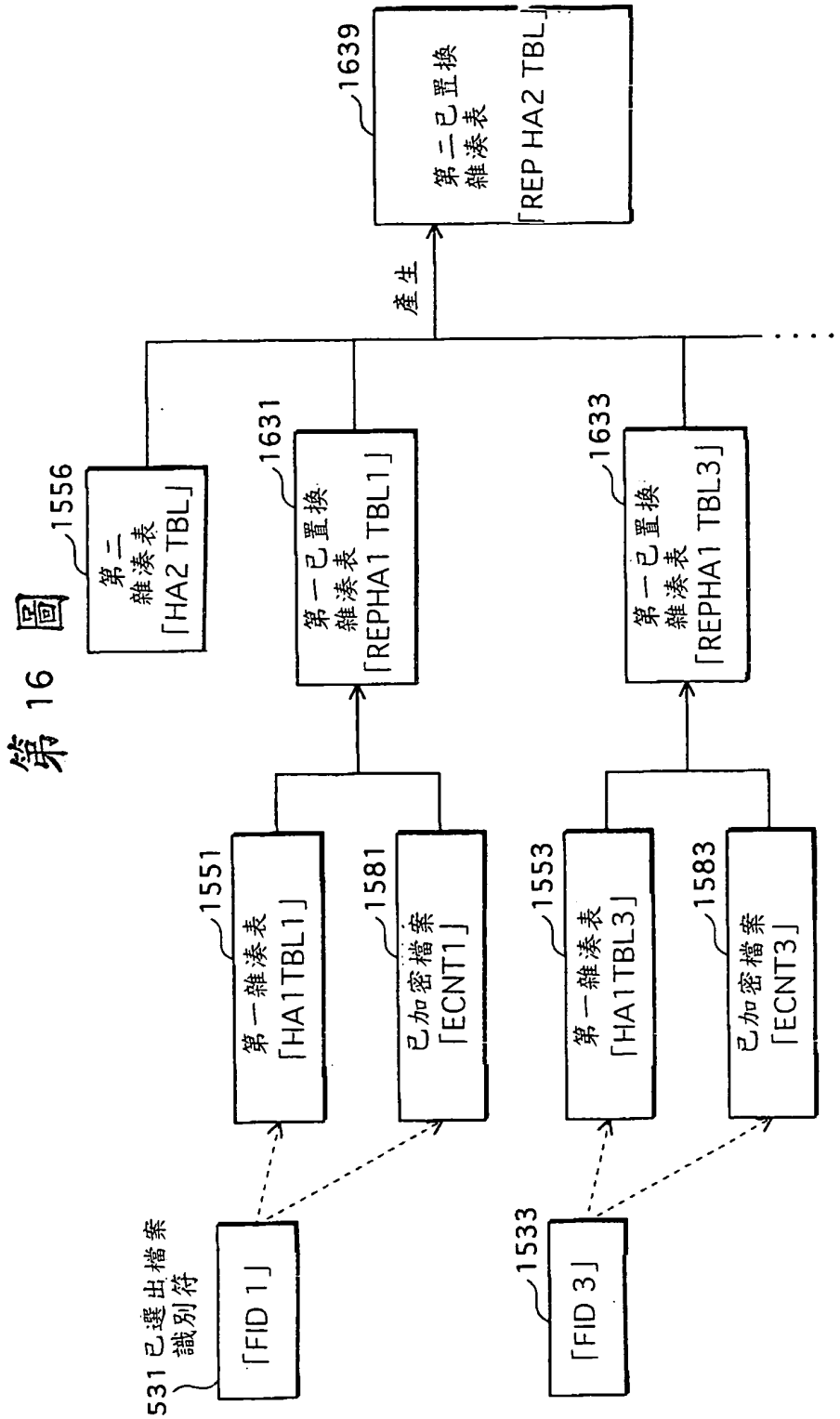
第 14 圖


1500
DVD
金鑰區塊
1510
單元檢選資訊
1530
1541
檔案資訊
1542
檔案資訊
1580
已加密內容
1581
已加密檔案
「ECNT1」
1582
1587
1550
頭標資訊
1551
第一雜湊表
「HA1TBL1」
1552
第一
雜湊表
「HA1TBL2」
1557
第一
雜湊表
「HA1TBLc」
1556
第二雜湊表
1561
1562
1563…
1567
1571
1572
1573
簽章資訊
1570

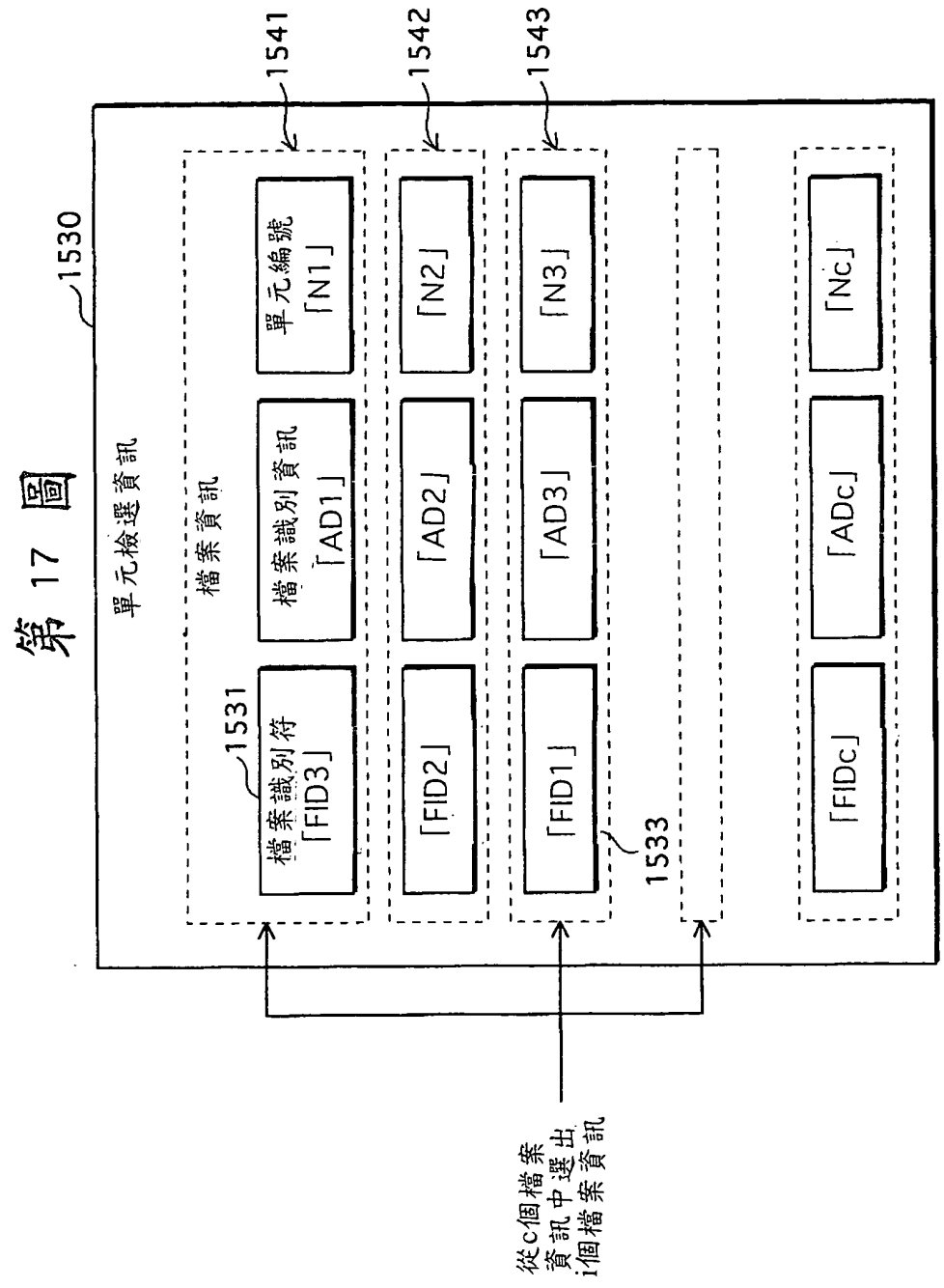
第 15 圖


LSI
1600
到監視器
裝置金鑰儲存單元
1604
1609
1608
驗證金鑰儲存單元
1612
1613
執行裝置
內容金鑰取得單元
1602
執行單元
1606
簽章資訊驗證單元
1611
取得單元
1601
DVD

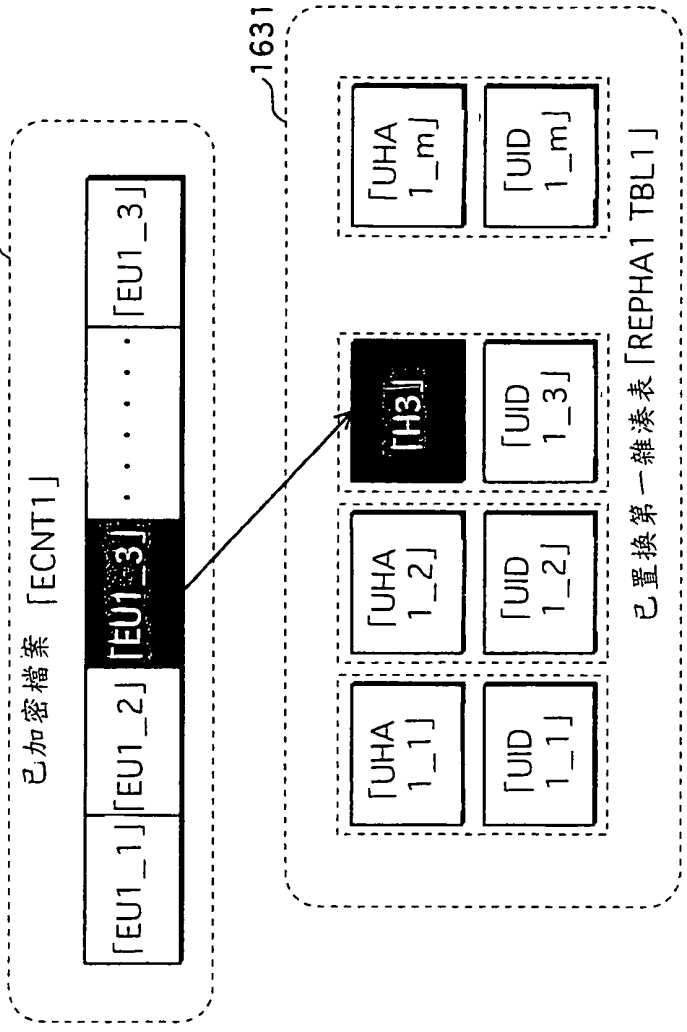
第16圖


1639
第二已置換
雜湊表
「REP HA2 TBL」
產生
1556
第二
雜湊表
「HA2 TBL」
1631
第一已置換
雜湊表
「REPHA1 TBL1」
1633
第一已置換
雜湊表
「REPHA1 TBL3」
1551
第一雜湊表
「HA1TBL1」
1581
已加密檔案
「ECNT1」
1553
第一雜湊表
「HA1TBL3」
1583
已加密檔案
「ECNT3」
1531已選出檔案
識別符
「FID 1」
1533
「FID 3」

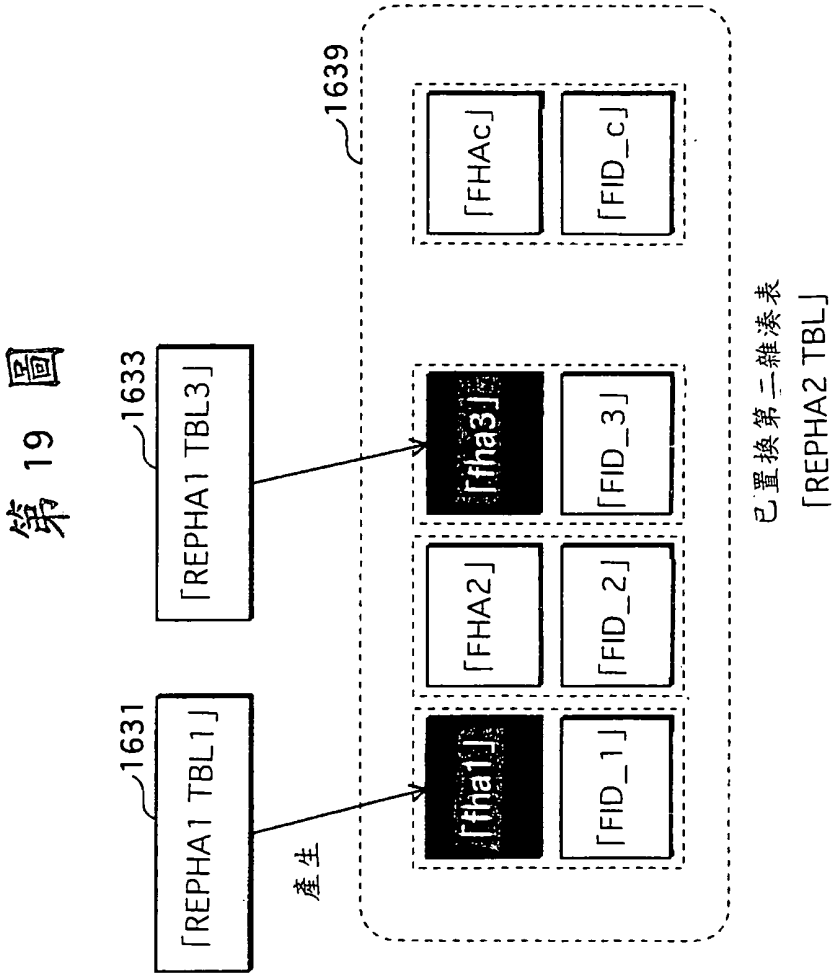
第 17 圖


單元檢選資訊
1530
檔案資訊
1541
1542
1543
單元編號
「N1」
檔案識別資訊
「AD1」
檔案識別符
「FID3」
1531
「N2」
「AD2」
「FID2」
「N3」
「AD3」
「FID1」
1533
「Nc」
「ADc」
「FIDc」
從c個檔案
資訊中選出
i個檔案資訊

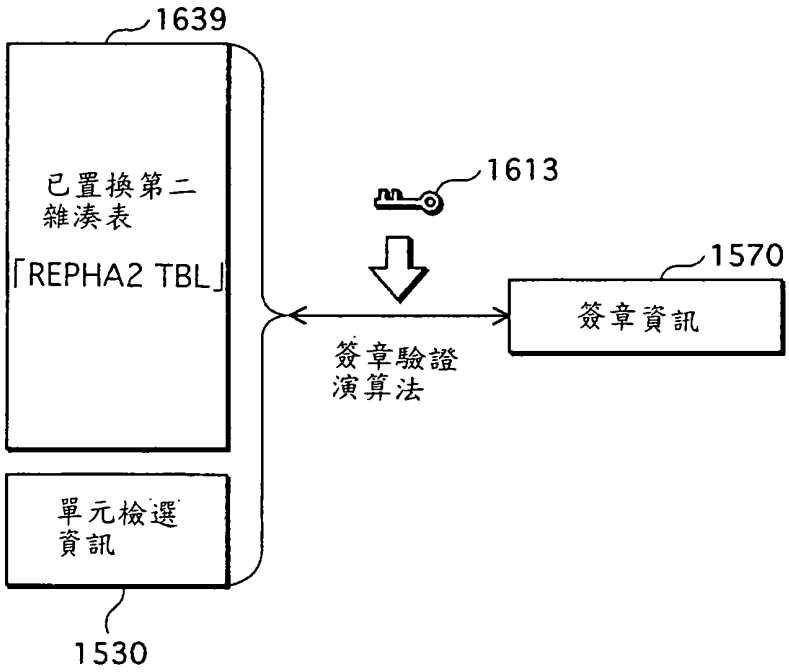
第 18 圖


1581
已加密檔案「ECNT1」
「EU1_1」
「EU1_2」
「EU1_3」
「EU1_3」
1631
「UHA 1_1」
「UID 1_1」
「UHA 1_2」
「UID 1_2」
「H3」
「UID 1_3」
「UHA 1_m」
「UID 1_m」
已置換第一雜湊表「REPHA1 TBL1」

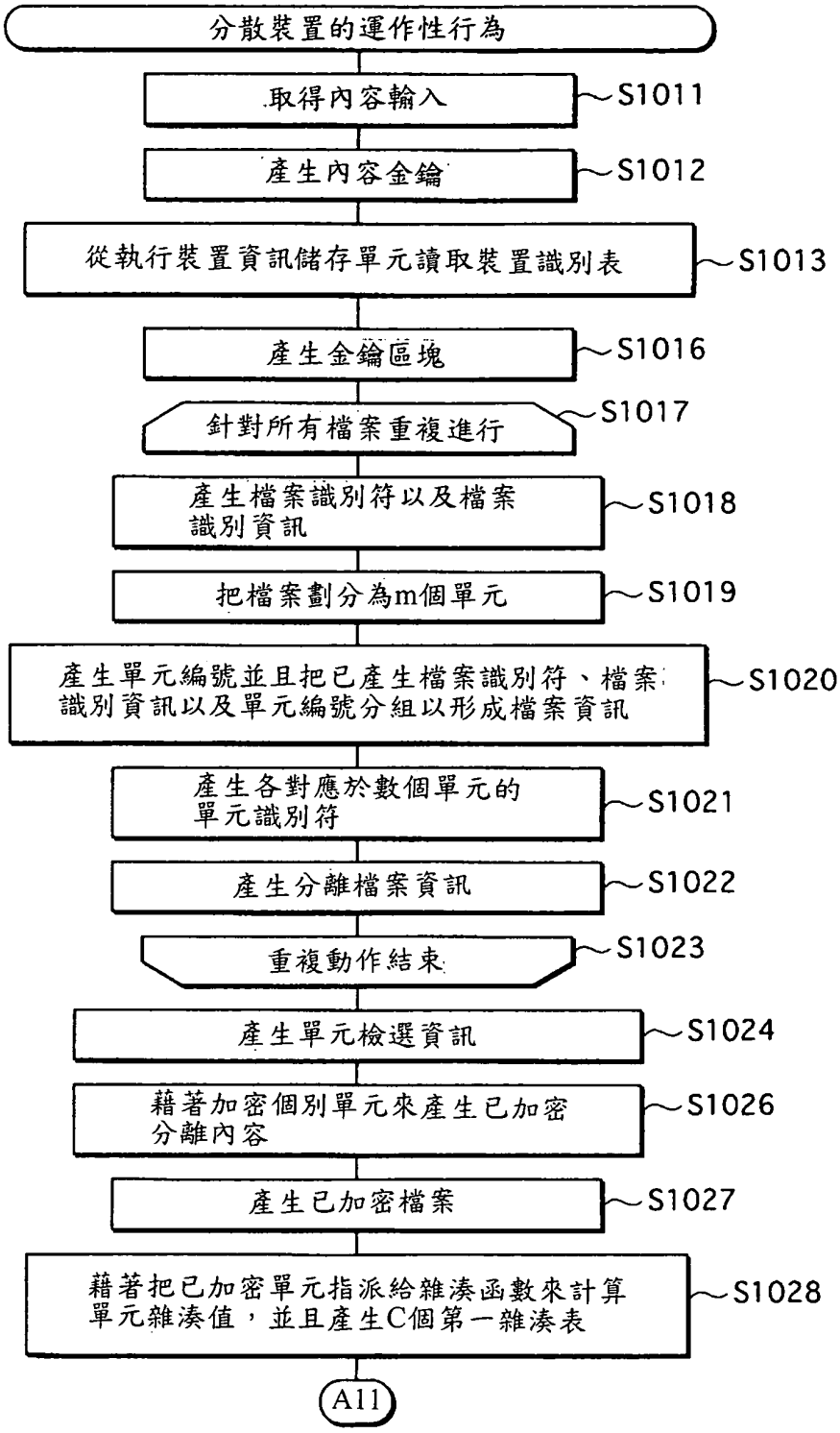
第 19 圖


1631
「REPHA1 TBL1」
1633
「REPHA1 TBL3」
產生
1639
「fha1」
「FID_1」
「FHA2」
「FID_2」
「fha3」
「FID_3」
「FHAc」
「FID_c」
已置換第二雜湊表
「REPHA2 TBL」

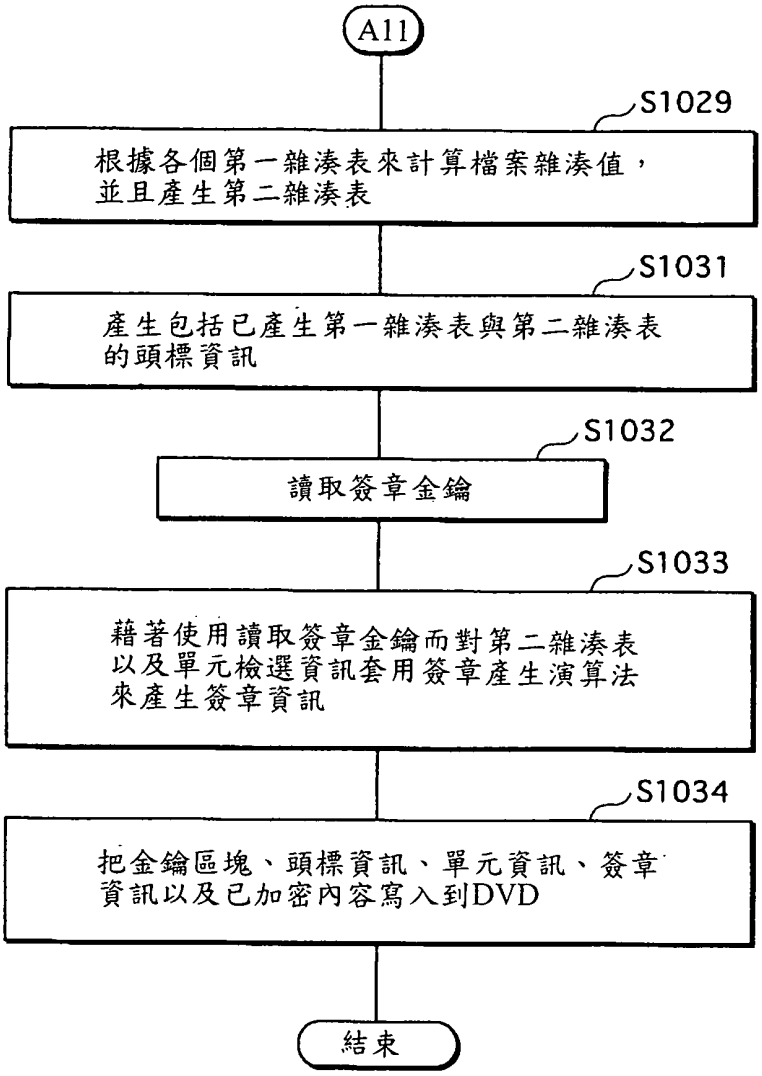
第 20 圖


1639
已置換第二
雜湊表
「REPHA2 TBL」
1613
1570
簽章資訊
簽章驗證
演算法
單元檢選
資訊
1530

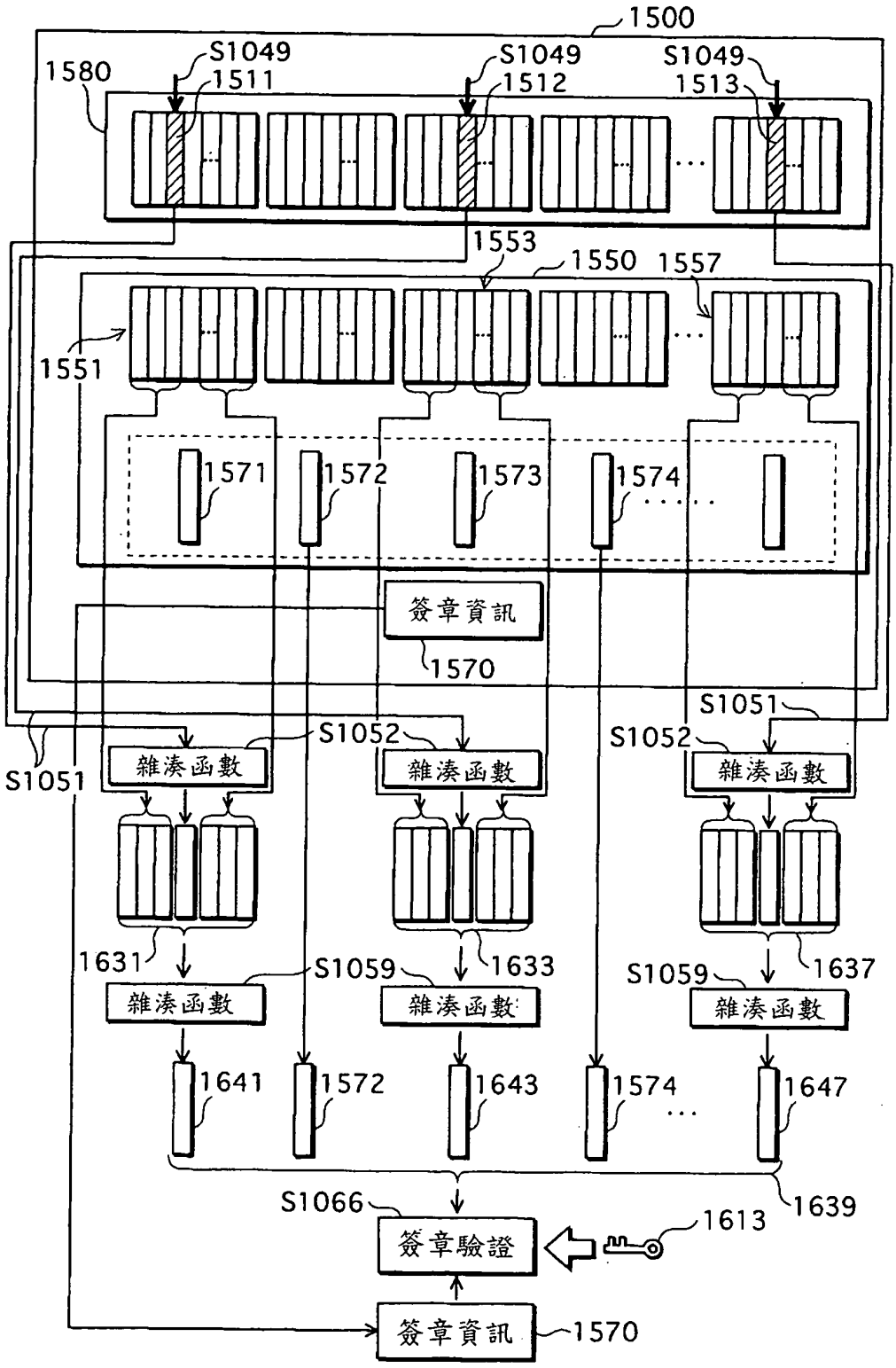
第 21 圖


分散裝置的運作性行為
取得內容輸入
S1011
產生內容金鑰
S1012
從執行裝置資訊儲存單元讀取裝置識別表
S1013
產生金鑰區塊
S1016
針對所有檔案重複進行
S1017
產生檔案識別符以及檔案識別資訊
S1018
把檔案劃分為m個單元
S1019
產生單元編號並且把已產生檔案識別符、檔案識別資訊以及單元編號分組以形成檔案資訊
S1020
產生各對應於數個單元的單元識別符
S1021
產生分離檔案資訊
S1022
重複動作結束
S1023
產生單元檢選資訊
S1024
藉著加密個別單元來產生已加密分離內容
S1026
產生已加密檔案
S1027
藉著把已加密單元指派給雜湊函數來計算單元雜湊值，並且產生C個第一雜湊表
S1028
A11

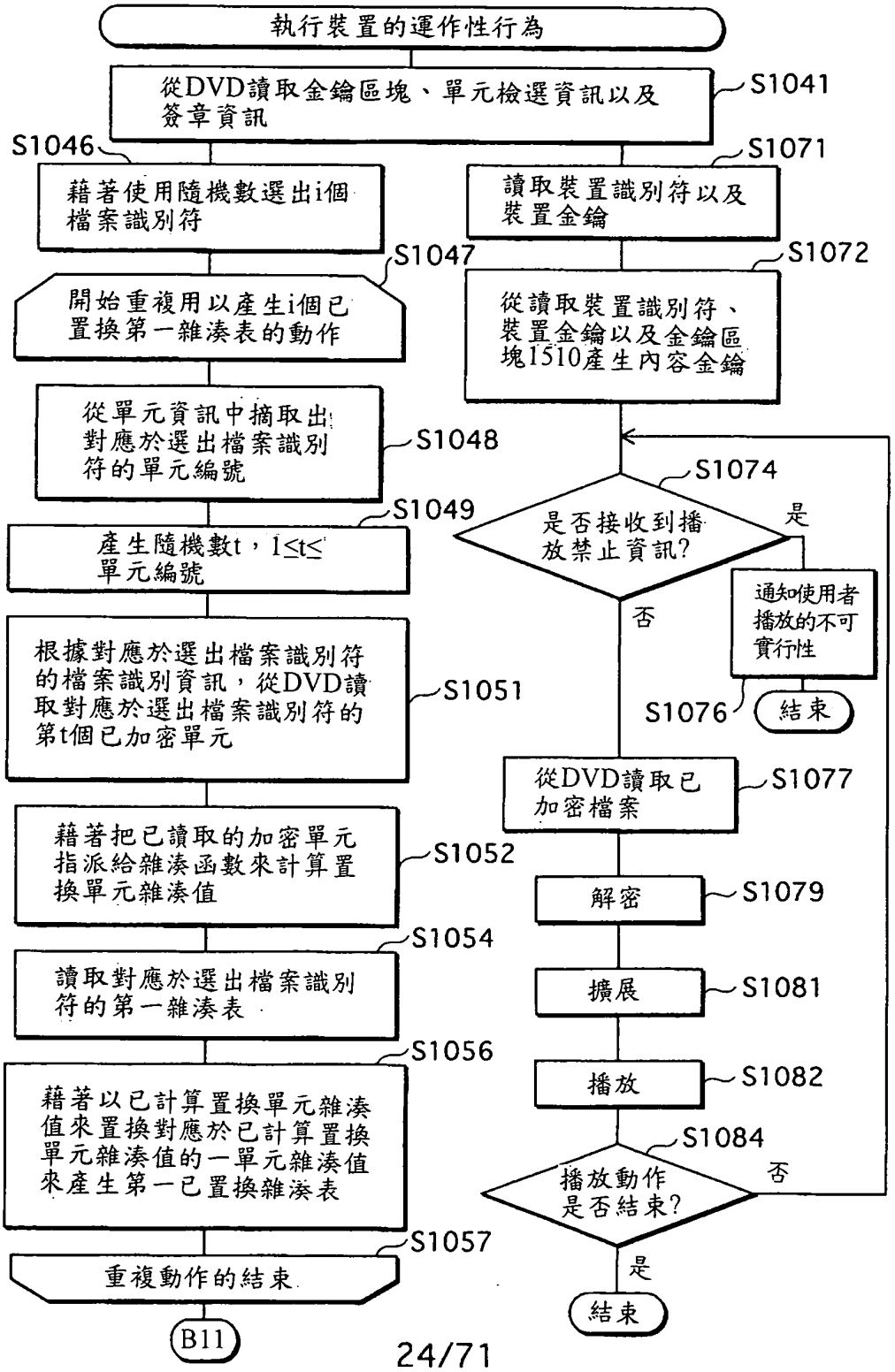
第 22 圖


A11
S1029
根據各個第一雜湊表來計算檔案雜湊值，並且產生第二雜湊表
S1031
產生包括已產生第一雜湊表與第二雜湊表的頭標資訊
S1032
讀取簽章金鑰
S1033
藉著使用讀取簽章金鑰而對第二雜湊表以及單元檢選資訊套用簽章產生演算法來產生簽章資訊
S1034
把金鑰區塊、頭標資訊、單元資訊、簽章資訊以及已加密內容寫入到DVD
結束

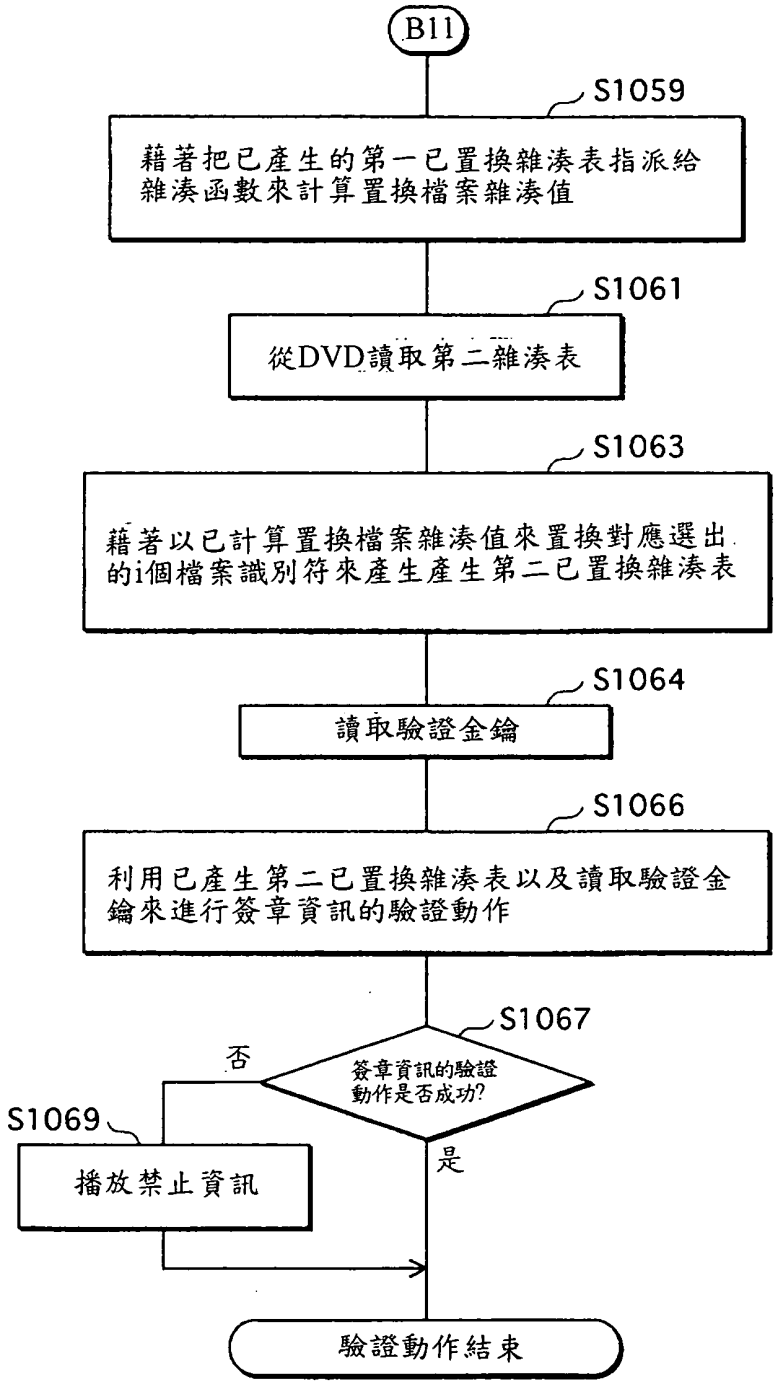
第 23 圖


1500
1580
S1049
1511
S1049
1512
S1049
1513
1553
1550
1557
1551
1571
1572
1573
1574
簽章資訊
1570
S1051
S1052
S1052
S1051
雜湊函數
雜湊函數
雜湊函數
1631
S1059
1633
S1059
1637
雜湊函數
雜湊函數
雜湊函數
1641
1572
1643
1574
1647
1639
S1066
1613
簽章驗證
簽章資訊
1570

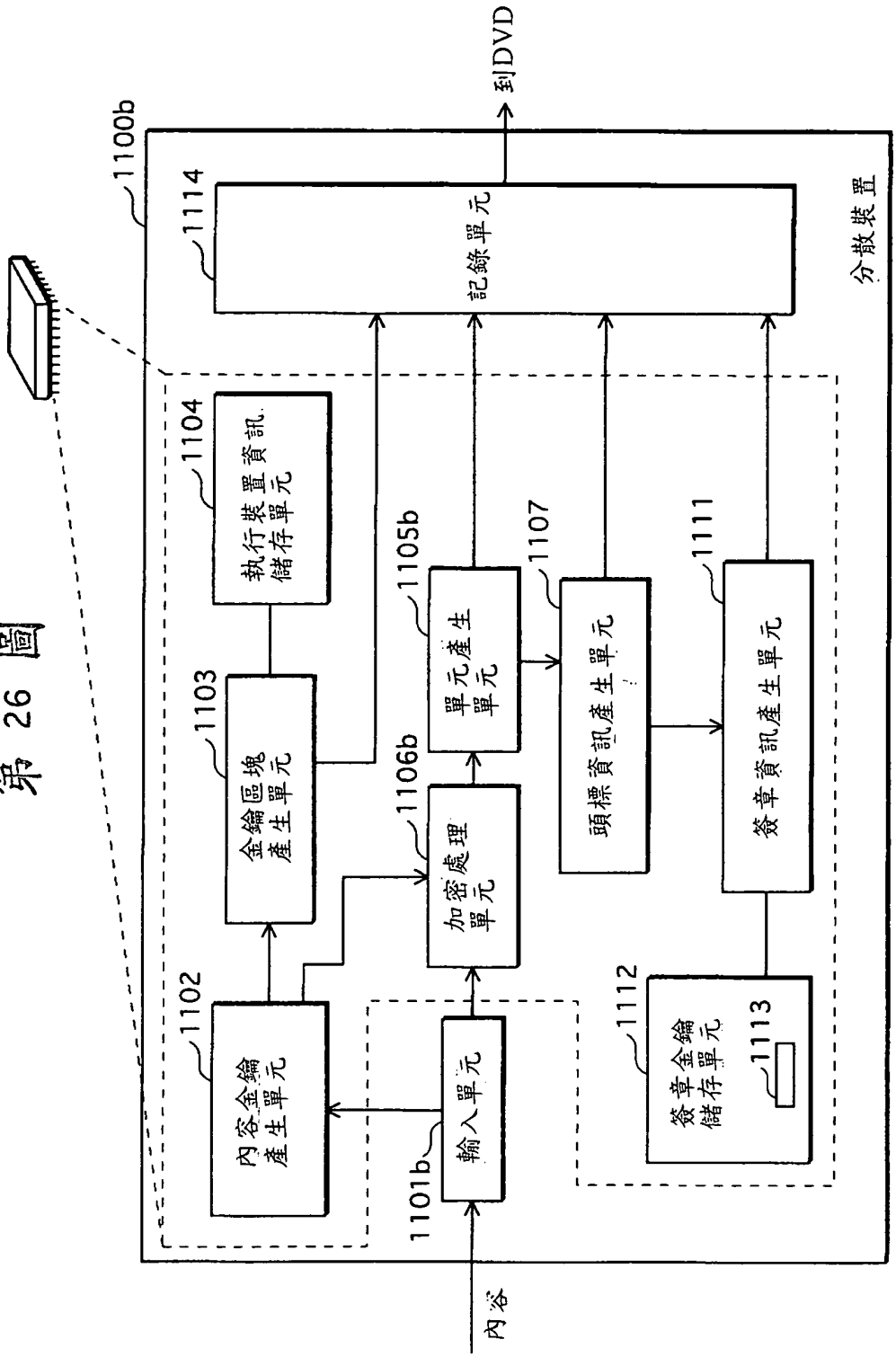
第 24 圖


執行裝置的運作性行為
從DVD讀取金鑰區塊、單元檢選資訊以及簽章資訊
S1041
S1046
藉著使用隨機數選出i個檔案識別符
S1071
讀取裝置識別符以及裝置金鑰
S1047
開始重複用以產生i個已置換第一雜湊表的動作
S1072
從讀取裝置識別符、裝置金鑰以及金鑰區塊1510產生內容金鑰
從單元資訊中摘取出對應於選出檔案識別符的單元編號
S1048
S1074
是否接收到播放禁止資訊?
是
否
通知使用者播放的不可實行性
S1076
結束
S1049
產生隨機數t，1≤t≤單元編號
根據對應於選出檔案識別符的檔案識別資訊，從DVD讀取對應於選出檔案識別符的第t個已加密單元
S1051
從DVD讀取已加密檔案
S1077
藉著把已讀取的加密單元指派給雜湊函數來計算置換單元雜湊值
S1052
解密
S1079
S1054
讀取對應於選出檔案識別符的第一雜湊表
擴展
S1081
S1056
藉著以已計算置換單元雜湊值來置換對應於已計算置換單元雜湊值的一單元雜湊值來產生第一已置換雜湊表
播放
S1082
S1084
播放動作是否結束?
否
是
S1057
重複動作的結束
結束
B11

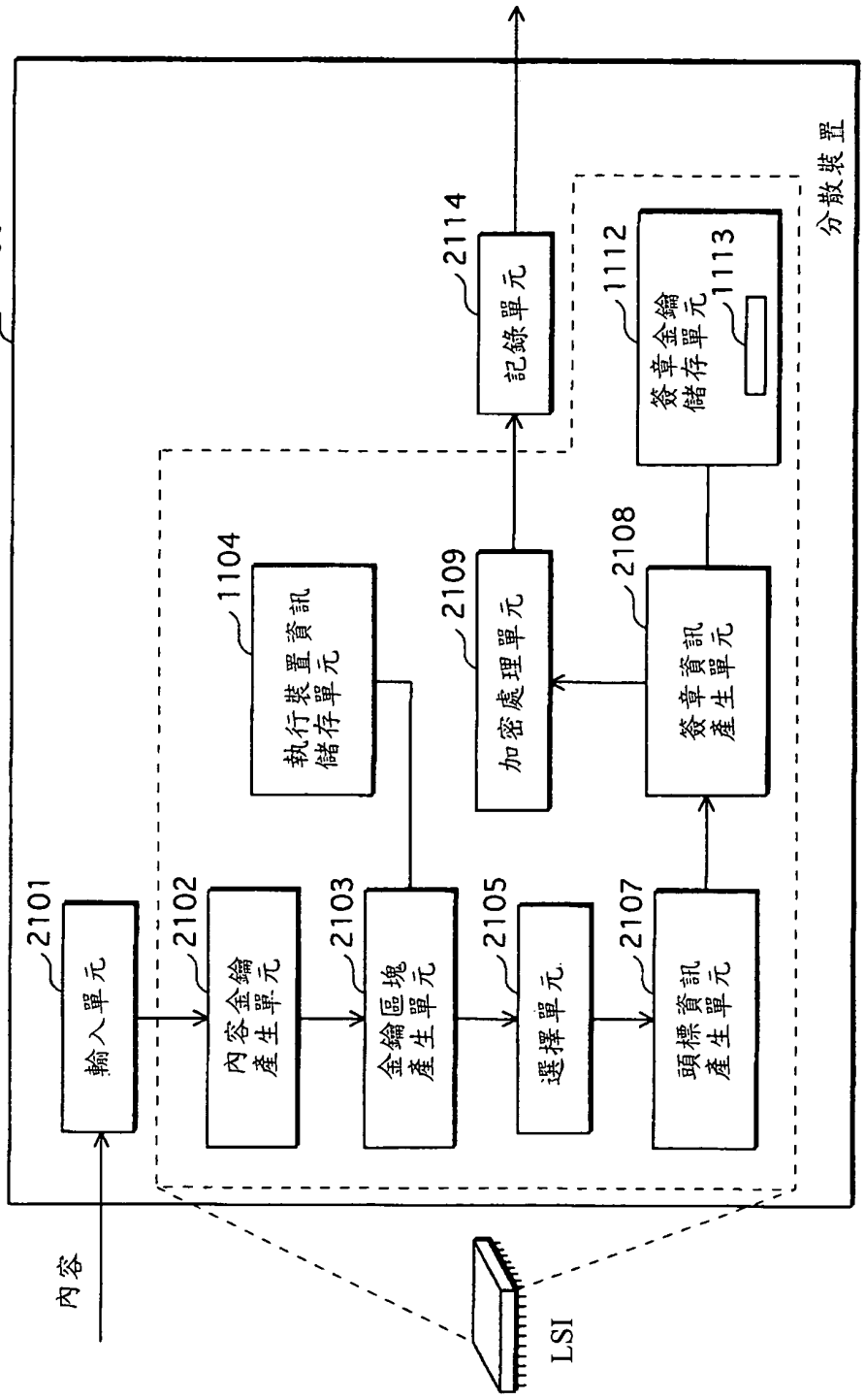
第 25 圖


B11
S1059
藉著把已產生的第一已置換雜湊表指派給雜湊函數來計算置換檔案雜湊值
S1061
從DVD讀取第二雜湊表
S1063
藉著以已計算置換檔案雜湊值來置換對應選出的i個檔案識別符來產生產生第二已置換雜湊表
S1064
讀取驗證金鑰
S1066
利用已產生第二已置換雜湊表以及讀取驗證金鑰來進行簽章資訊的驗證動作
S1067
簽章資訊的驗證動作是否成功?
否
是
S1069
播放禁止資訊
驗證動作結束

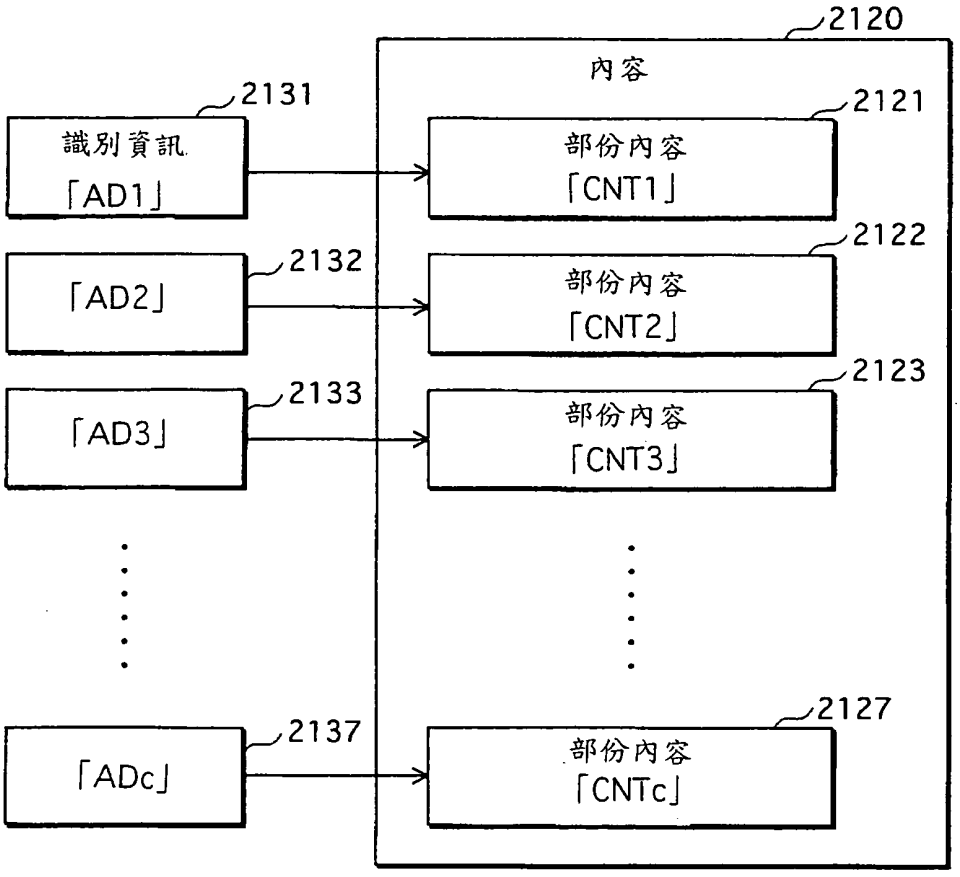
第 26 圖


1100b
到DVD
1114
記錄單元
分散裝置
1104
執行裝置資訊儲存單元
1103
金鑰區塊產生單元
1105b
單元產生單元
1107
頭標資訊產生單元
1111
簽章資訊產生單元
1106b
加密處理單元
1102
內容金鑰產生單元
1101b
輸入單元
1112
簽章金鑰儲存單元
1113
內容

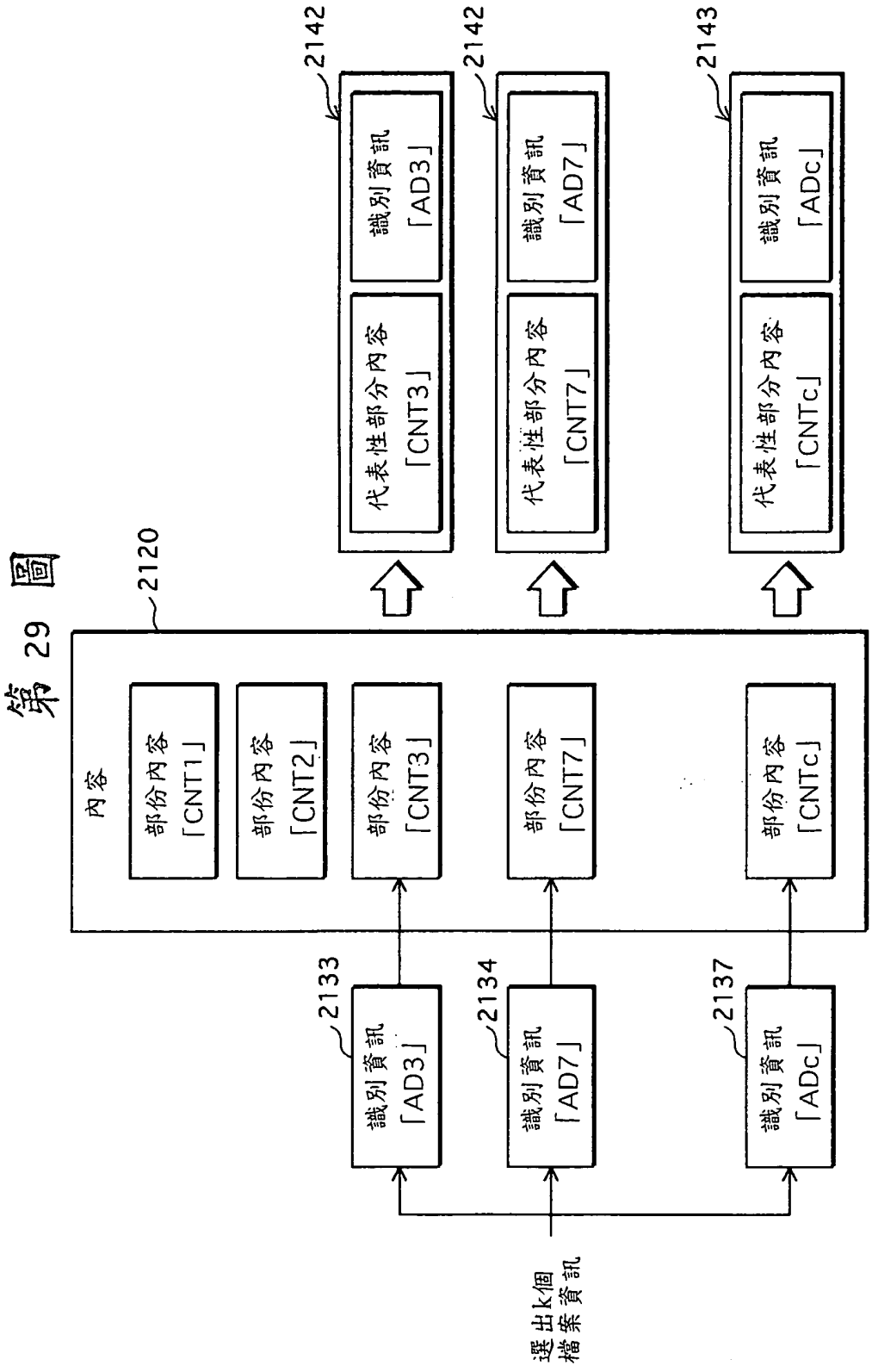
第 27 圖


2100
分散裝置
2101
輸入單元
2102
內容金鑰產生單元
2103
金鑰區塊產生單元
2105
選擇單元
2107
頭標資訊產生單元
1104
執行裝置資訊儲存單元
2109
加密處理單元
2108
簽章資訊產生單元
2114
記錄單元
1112
簽章金鑰儲存單元
1113
內容
LSI

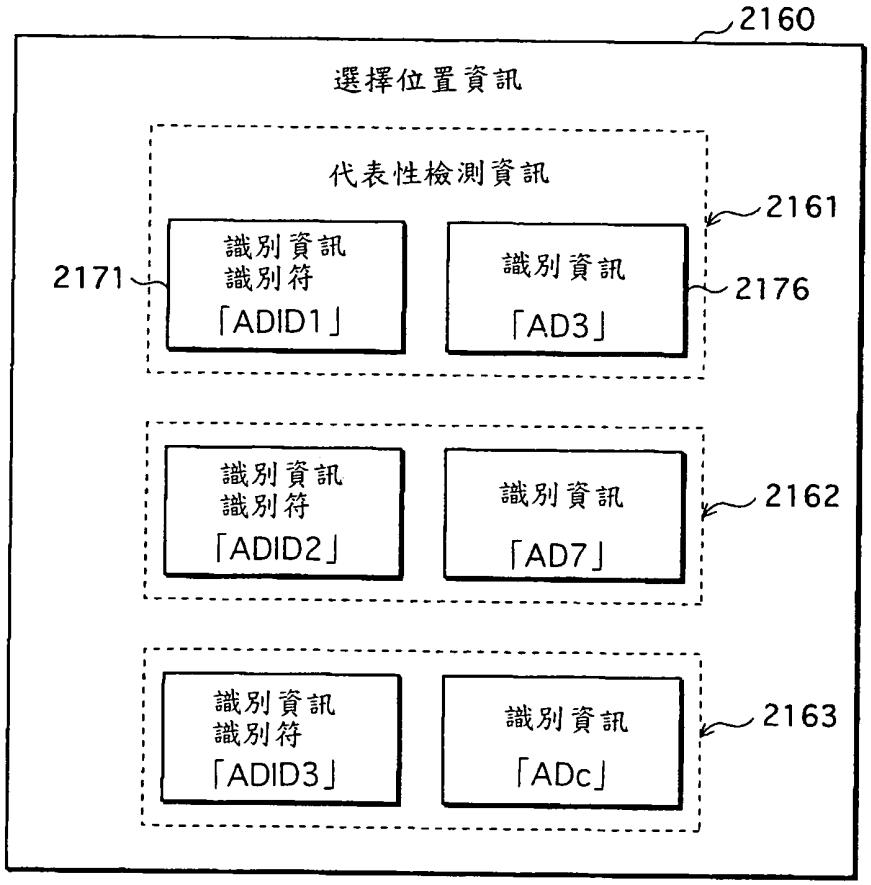
第 28 圖


2120
內容
2131
識別資訊
「AD1」
2121
部份內容
「CNT1」
2122
「AD2」
2132
部份內容
「CNT2」
2123
「AD3」
2133
部份內容
「CNT3」
2127
「ADc」
2137
部份內容
「CNTc」

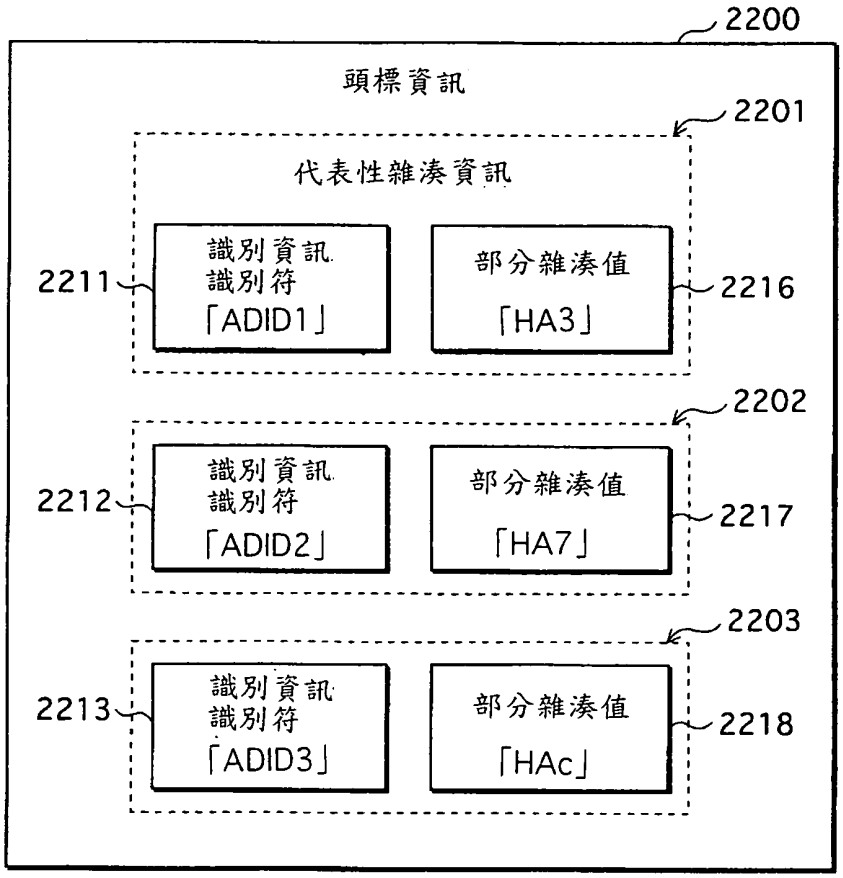
第 29 圖


2142
2142
2143
識別資訊「AD3」
識別資訊「AD7」
識別資訊「ADc」
代表性部分內容「CNT3」
代表性部分內容「CNT7」
代表性部分內容「CNTc」
2120
內容
部份內容「CNT1」
部份內容「CNT2」
部份內容「CNT3」
部份內容「CNT7」
部份內容「CNTc」
2133
2134
2137
識別資訊「AD3」
識別資訊「AD7」
識別資訊「ADc」
選出k個檔案資訊

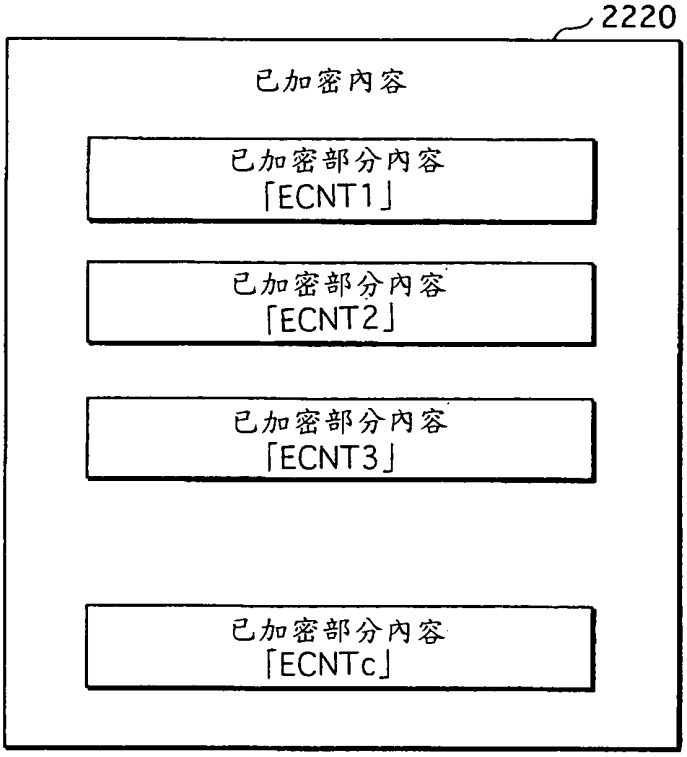
第 30 圖


2160
選擇位置資訊
代表性檢測資訊
2161
2171
識別資訊
識別符
「ADID1」
識別資訊
「AD3」
2176
識別資訊
識別符
「ADID2」
識別資訊
「AD7」
2162
識別資訊
識別符
「ADID3」
識別資訊
「ADc」
2163

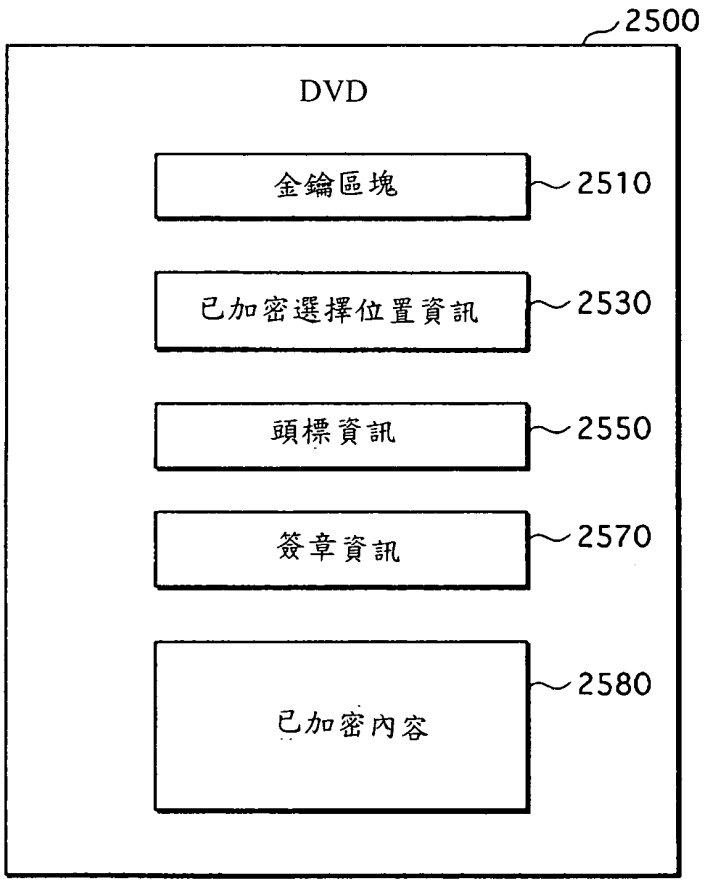
第 31 圖


2200
頭標資訊
2201
代表性雜湊資訊
2211
識別資訊
識別符
「ADID1」
部分雜湊值
「HA3」
2216
2202
2212
識別資訊
識別符
「ADID2」
部分雜湊值
「HA7」
2217
2203
2213
識別資訊
識別符
「ADID3」
部分雜湊值
「HAc」
2218

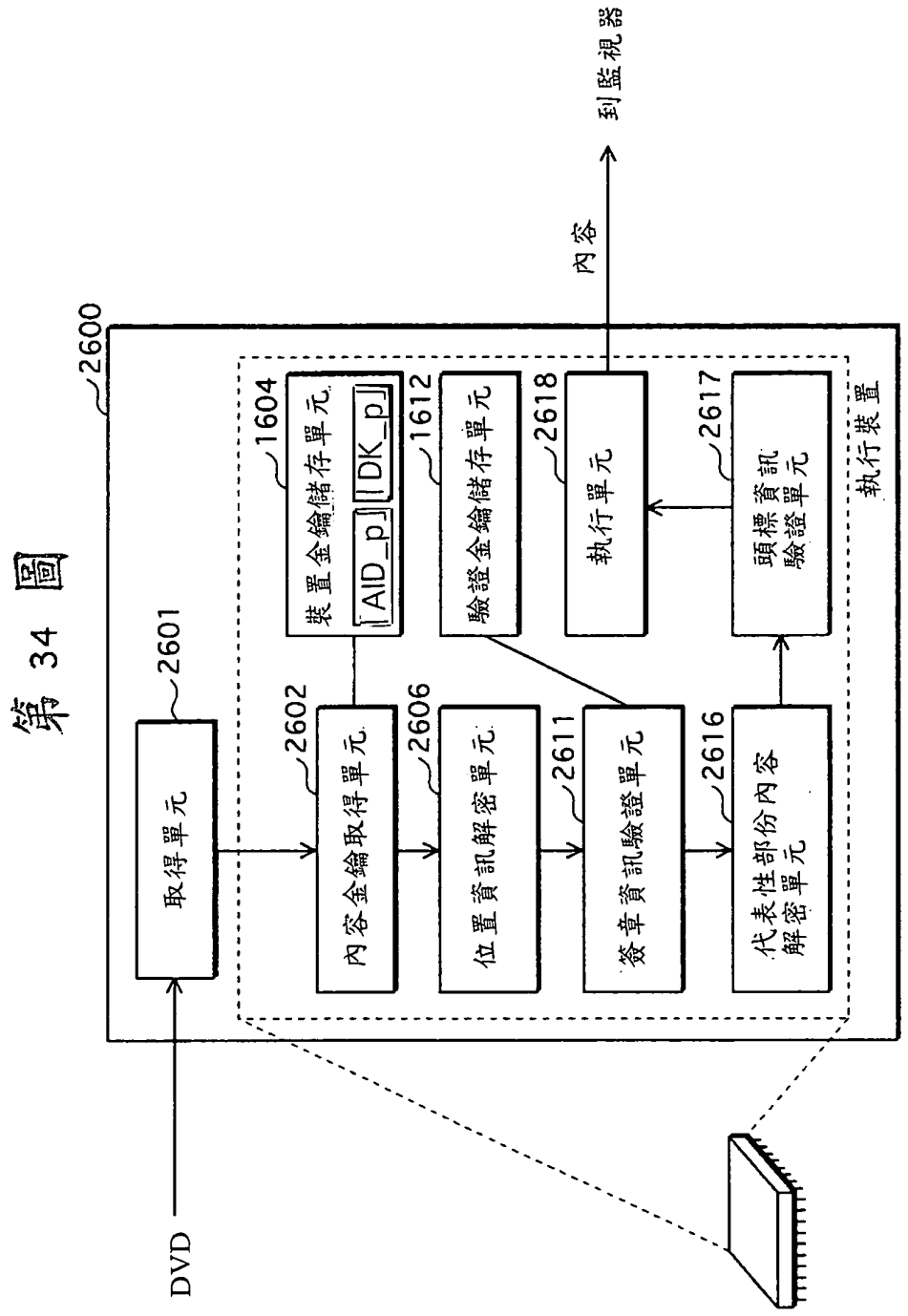
第 32 圖


2220
已加密內容
已加密部分內容
「ECNT1」
已加密部分內容
「ECNT2」
已加密部分內容
「ECNT3」
已加密部分內容
「ECNTc」

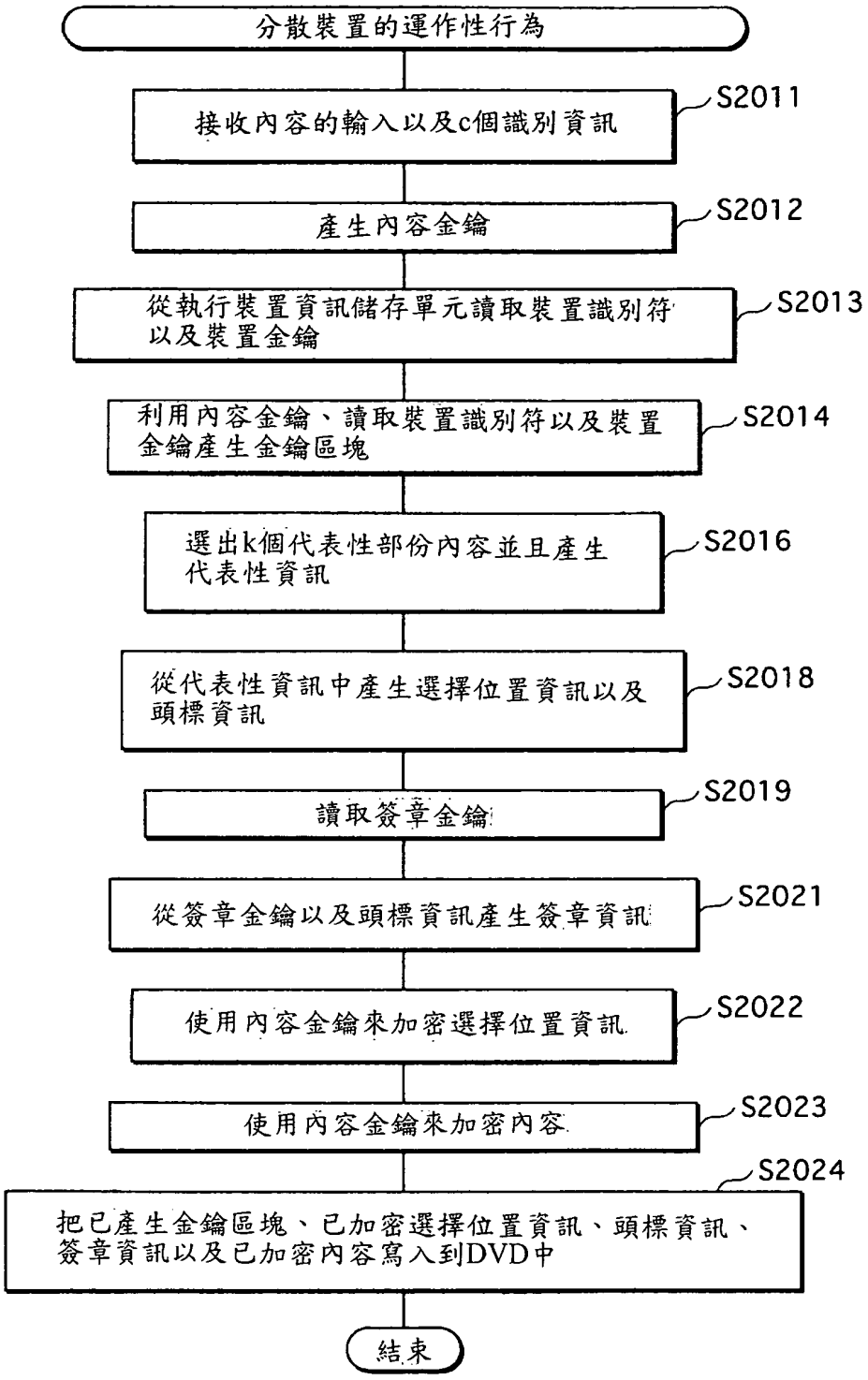
第 33 圖


2500
DVD
金鑰區塊
2510
已加密選擇位置資訊
2530
頭標資訊
2550
簽章資訊
2570
已加密內容
2580

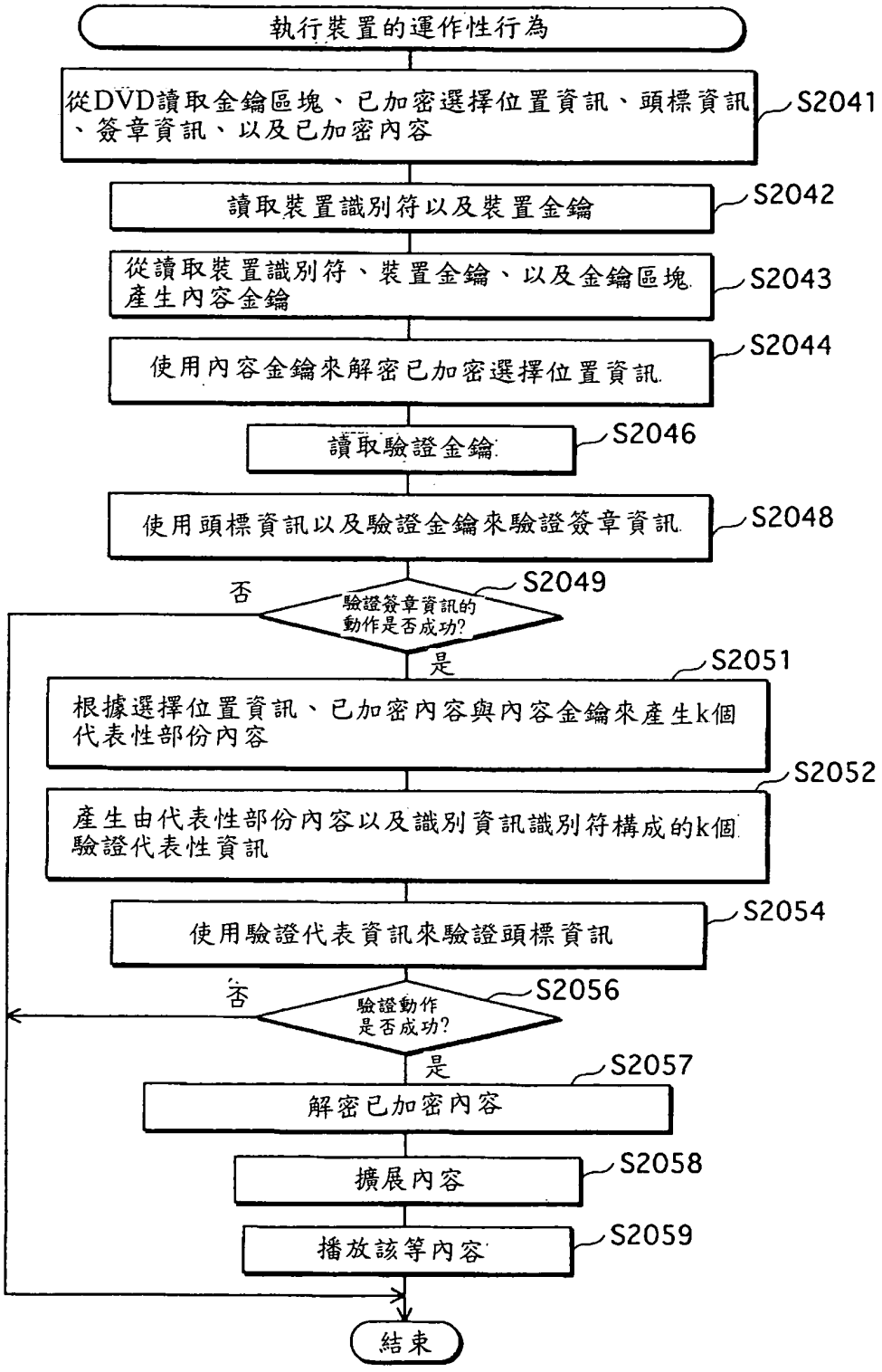
第 34 圖


DVD
2600
2601
取得單元
2602
內容金鑰取得單元
2606
位置資訊解密單元
2611
簽章資訊驗證單元
2616
代表性部份內容解密單元
1604
裝置金鑰儲存單元
AID_p
DK_p
1612
2618
驗證金鑰儲存單元
執行單元
2617
頭標資訊驗證單元
執行裝置
內容
到監視器

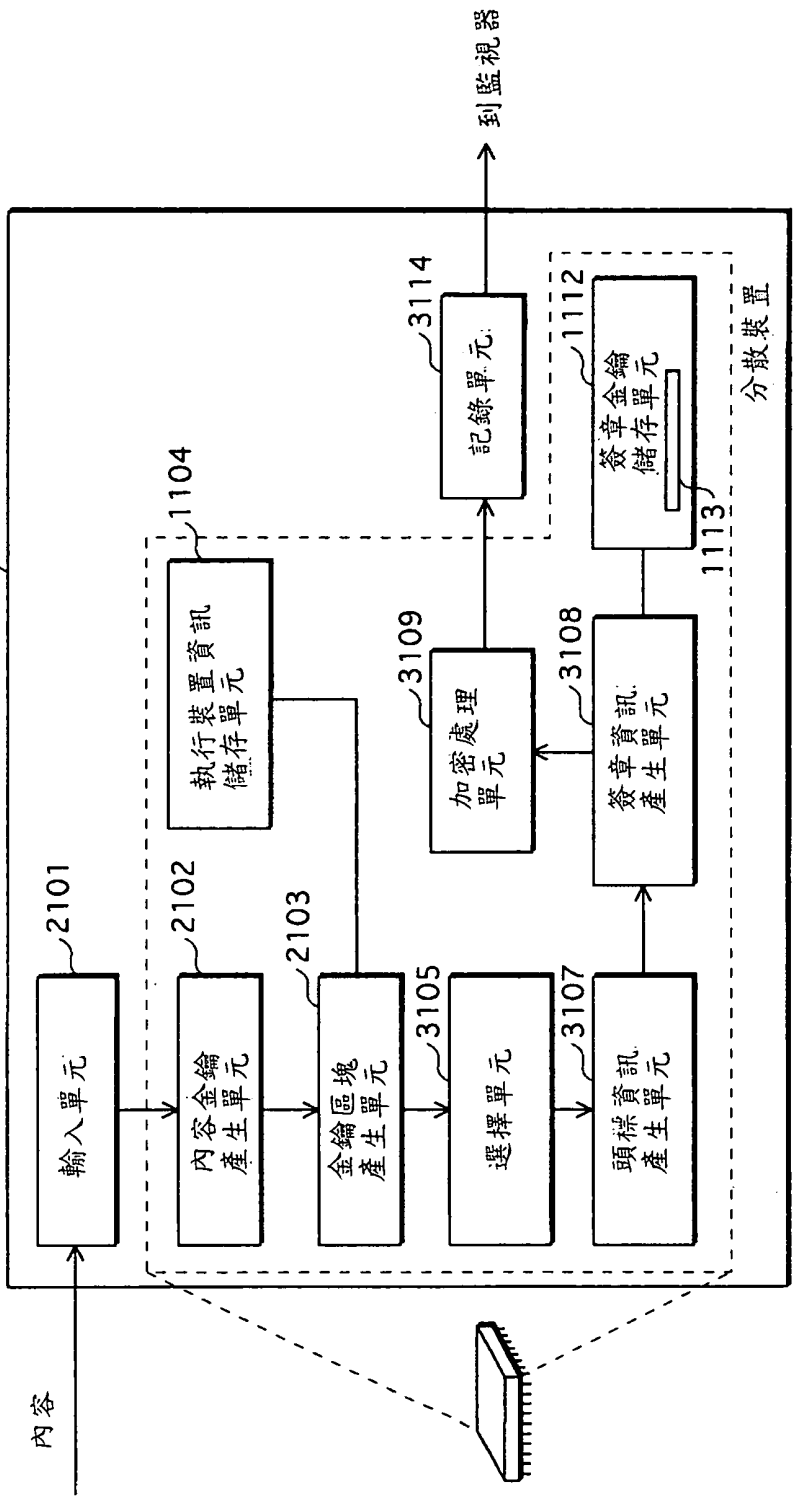
第 35 圖


分散裝置的運作性行為
接收內容的輸入以及c個識別資訊
S2011
產生內容金鑰
S2012
從執行裝置資訊儲存單元讀取裝置識別符以及裝置金鑰
S2013
利用內容金鑰、讀取裝置識別符以及裝置金鑰產生金鑰區塊
S2014
選出k個代表性部份內容並且產生代表性資訊
S2016
從代表性資訊中產生選擇位置資訊以及頭標資訊
S2018
讀取簽章金鑰
S2019
從簽章金鑰以及頭標資訊產生簽章資訊
S2021
使用內容金鑰來加密選擇位置資訊
S2022
使用內容金鑰來加密內容
S2023
把已產生金鑰區塊、已加密選擇位置資訊、頭標資訊、簽章資訊以及已加密內容寫入到DVD中
S2024
結束

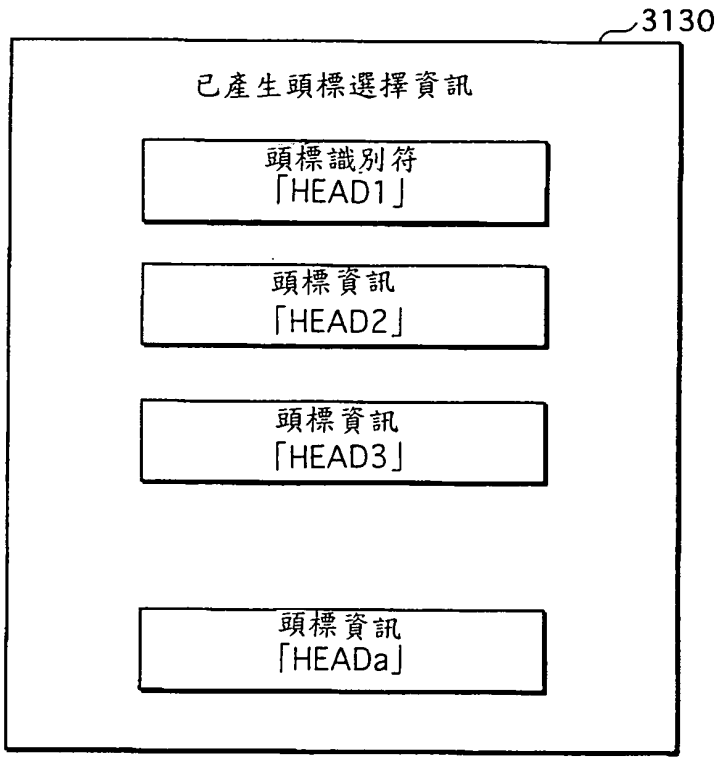
第 36 圖


執行裝置的運作性行為
從DVD讀取金鑰區塊、已加密選擇位置資訊、頭標資訊、簽章資訊、以及已加密內容
S2041
讀取裝置識別符以及裝置金鑰
S2042
從讀取裝置識別符、裝置金鑰、以及金鑰區塊產生內容金鑰
S2043
使用內容金鑰來解密已加密選擇位置資訊
S2044
讀取驗證金鑰
S2046
使用頭標資訊以及驗證金鑰來驗證簽章資訊
S2048
否
驗證簽章資訊的動作是否成功?
S2049
是
根據選擇位置資訊、已加密內容與內容金鑰來產生k個代表性部份內容
S2051
產生由代表性部份內容以及識別資訊識別符構成的k個驗證代表性資訊
S2052
使用驗證代表資訊來驗證頭標資訊
S2054
否
驗證動作是否成功?
S2056
是
解密已加密內容
S2057
擴展內容
S2058
播放該等內容
S2059
結束

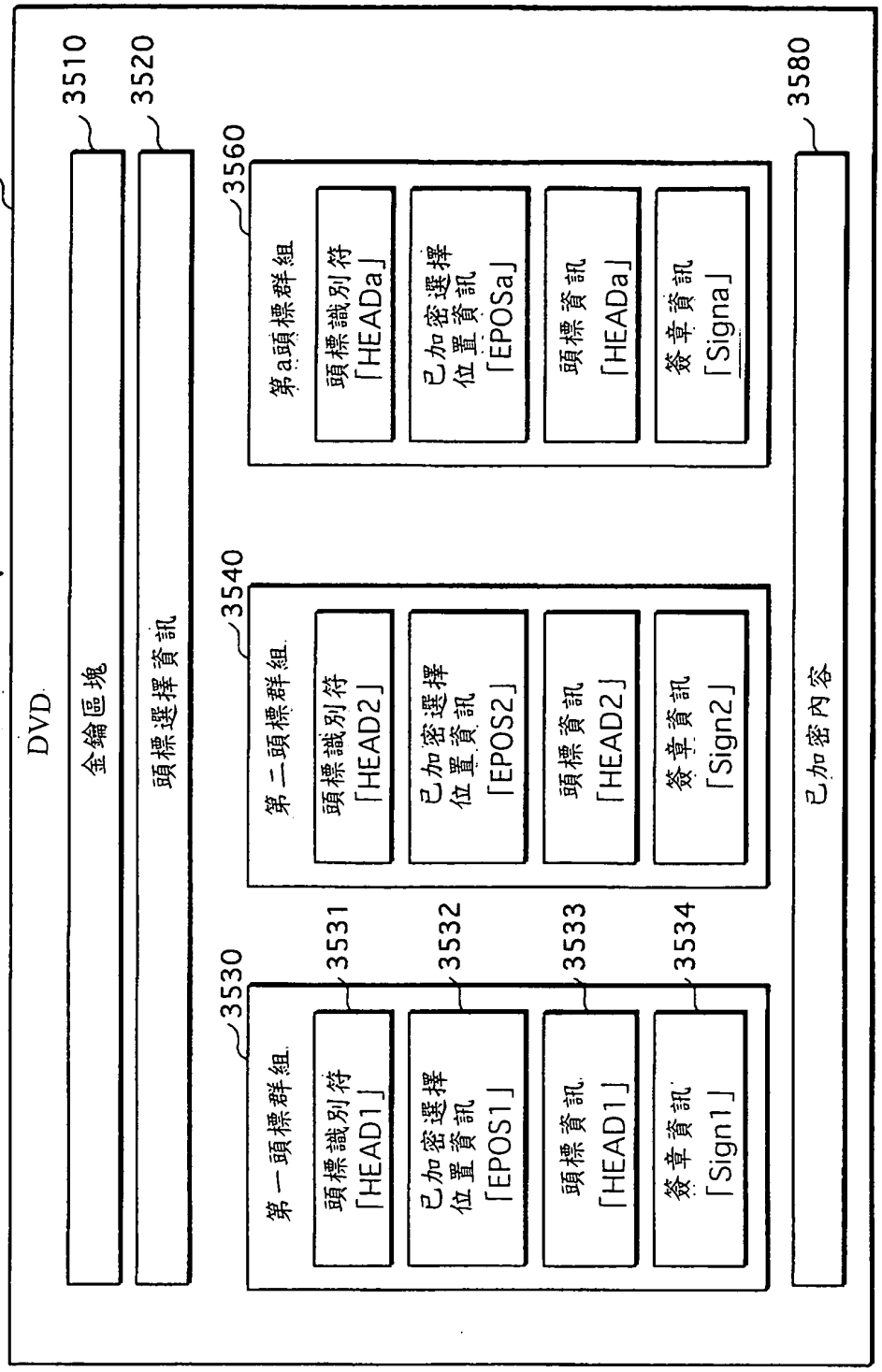
第 37 圖


內容
輸入單元
2101
內容金鑰產生單元
2102
金鑰區塊產生單元
2103
選擇單元
3105
頭標資訊產生單元
3107
簽章資訊產生單元
3108
加密處理單元
3109
執行裝置資訊儲存單元
1104
記錄單元
3114
簽章金鑰儲存單元
1112
1113
分散裝置
3100
到監視器

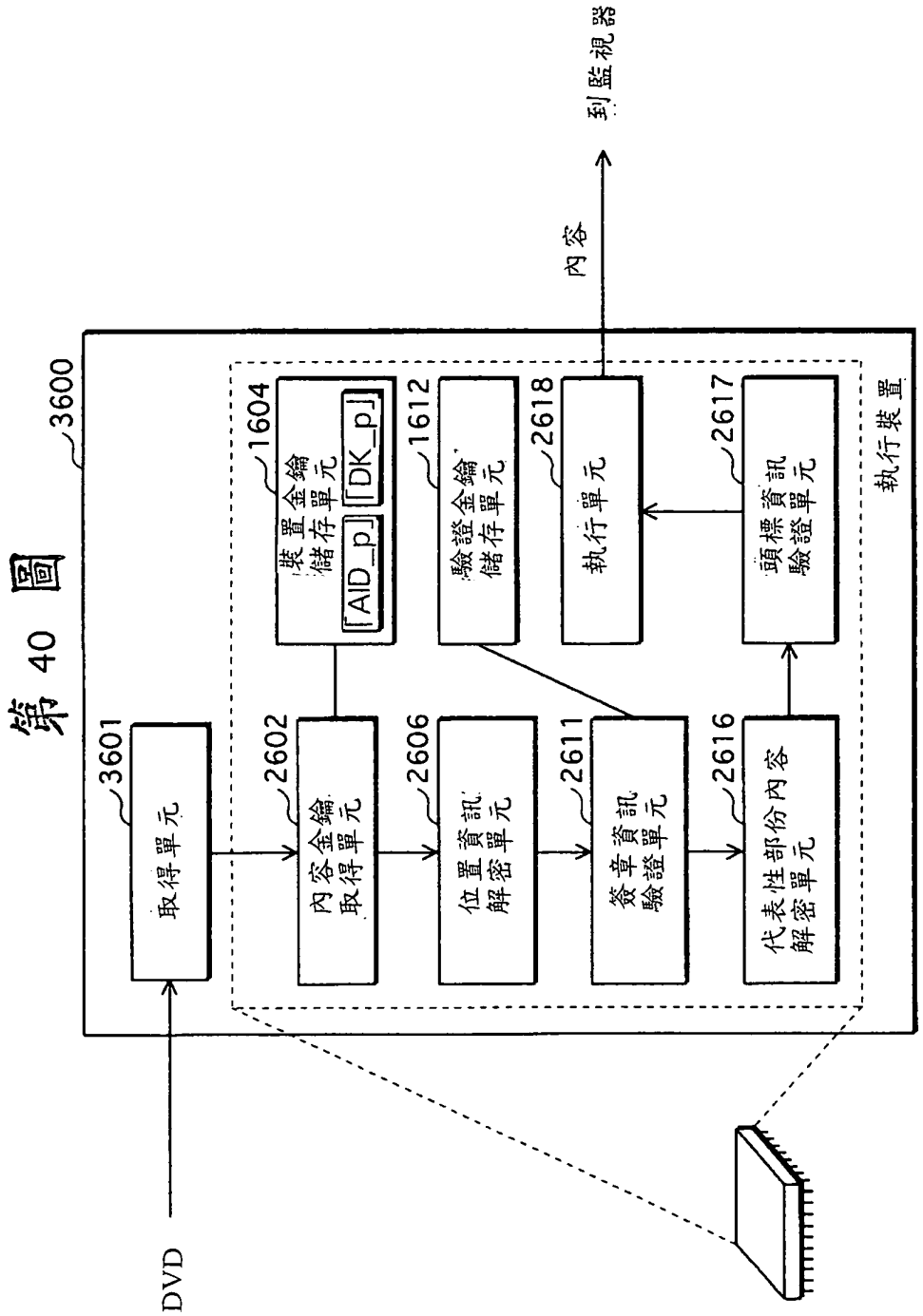
第 38 圖


3130
已產生頭標選擇資訊
頭標識別符
「HEAD1」
頭標資訊
「HEAD2」
頭標資訊
「HEAD3」
頭標資訊
「HEADa」

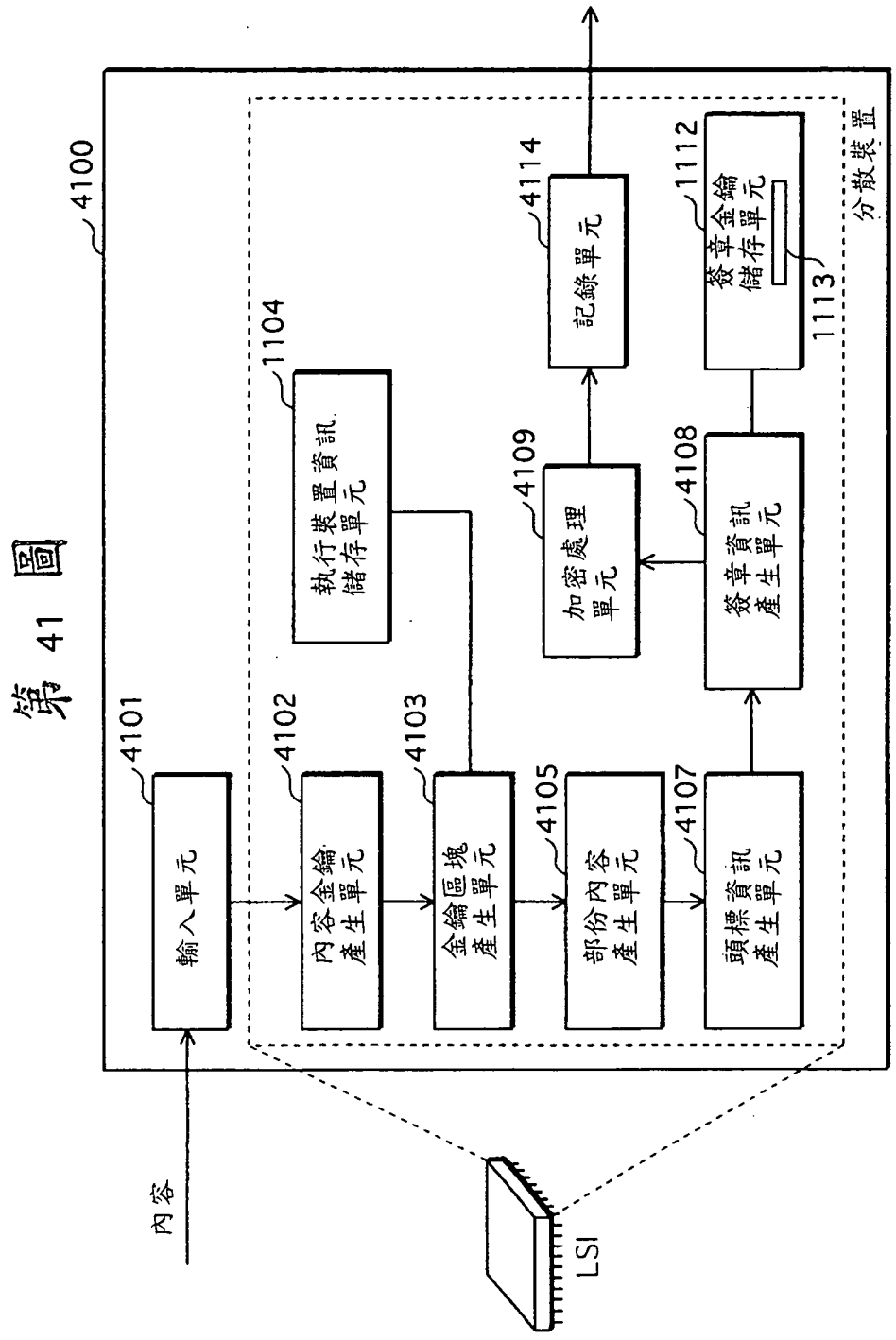
第 39 圖


DVD
3500
金鑰區塊
3510
頭標選擇資訊
3520
第一頭標群組
3530
頭標識別符「HEAD1」
3531
已加密選擇位置資訊「EPOS1」
3532
頭標資訊「HEAD1」
3533
簽章資訊「Sign1」
3534
第二頭標群組
3540
頭標識別符「HEAD2」
已加密選擇位置資訊「EPOS2」
頭標資訊「HEAD2」
簽章資訊「Sign2」
第a頭標群組
3560
頭標識別符「HEADa」
已加密選擇位置資訊「EPOSa」
頭標資訊「HEADa」
簽章資訊「Signa」
已加密內容
3580

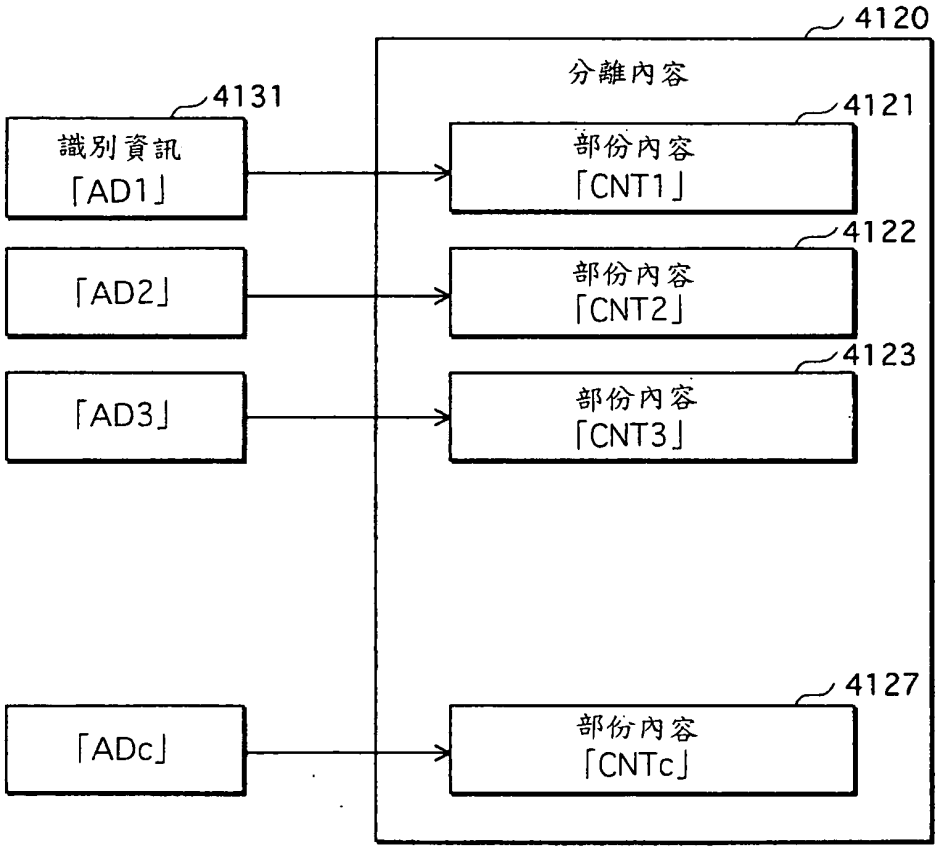
第 40 圖


3600
執行裝置
3601
取得單元
2602
內容金鑰取得單元
2606
位置資訊解密單元
2611
簽章資訊驗證單元
2616
代表性部份內容解密單元
1604
裝置金鑰儲存單元
「AID_p」
「DK_p」
1612
驗證金鑰儲存單元
2618
執行單元
2617
頭標資訊驗證單元
內容
到監視器
DVD

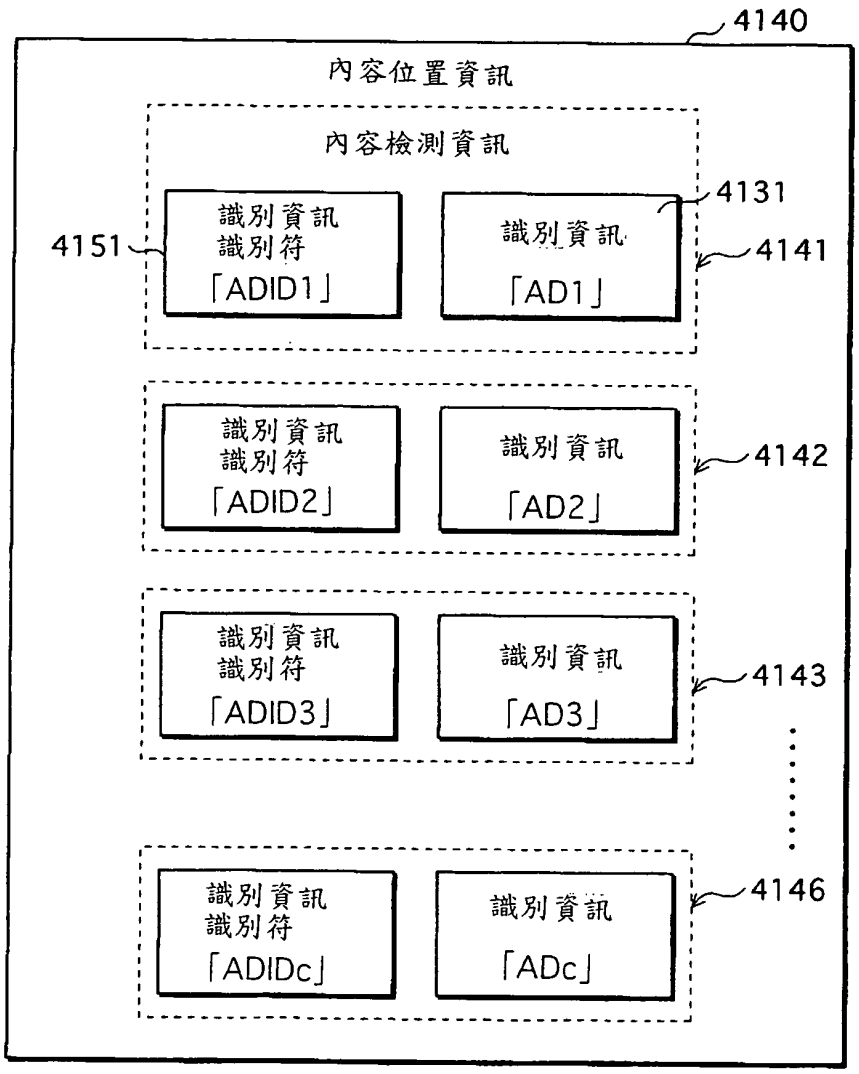
第 41 圖


4100
分散裝置
4101
輸入單元
4102
內容金鑰產生單元
4103
金鑰區塊產生單元
4104
執行裝置資訊儲存單元
4105
部份內容產生單元
4107
頭標資訊產生單元
4108
簽章資訊產生單元
4109
加密處理單元
4112
簽章金鑰儲存單元
4113
4114
記錄單元
內容
LSI

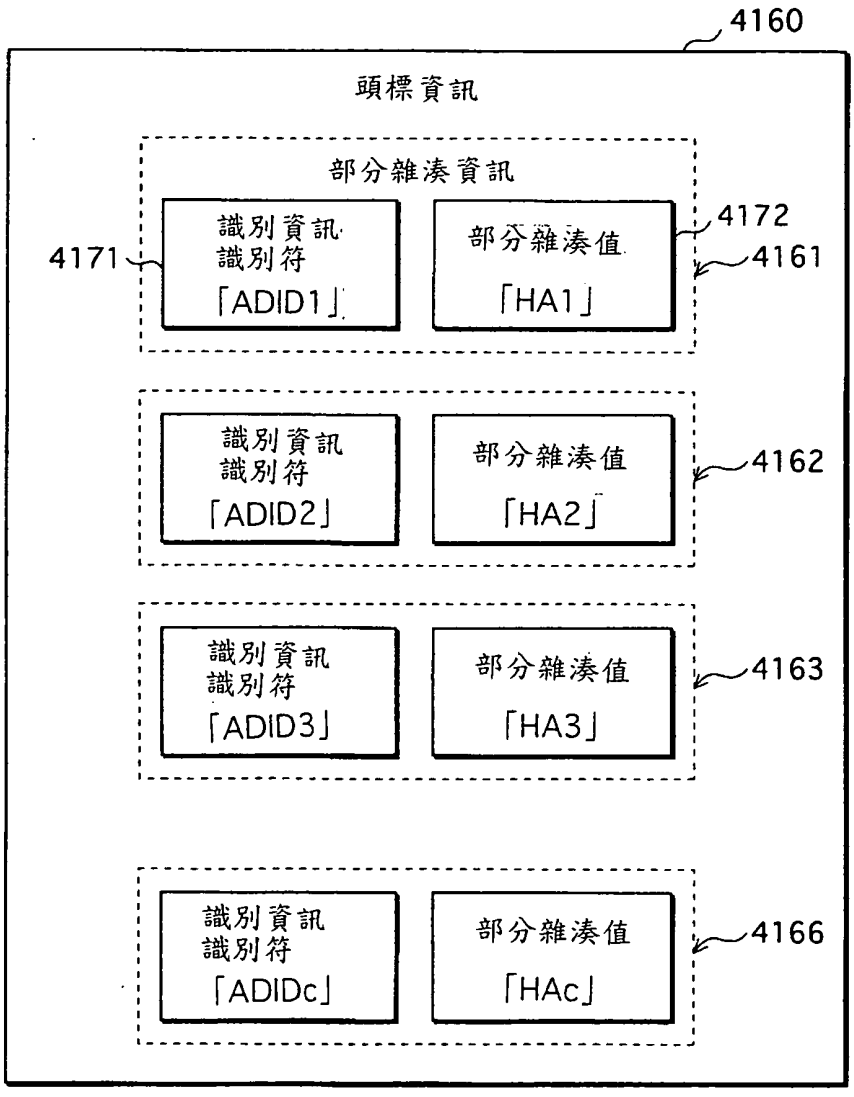
第 42 圖


4120
分離內容
4131
識別資訊
「AD1」
4121
部份內容
「CNT1」
「AD2」
4122
部份內容
「CNT2」
「AD3」
4123
部份內容
「CNT3」
4127
「ADc」
部份內容
「CNTc」

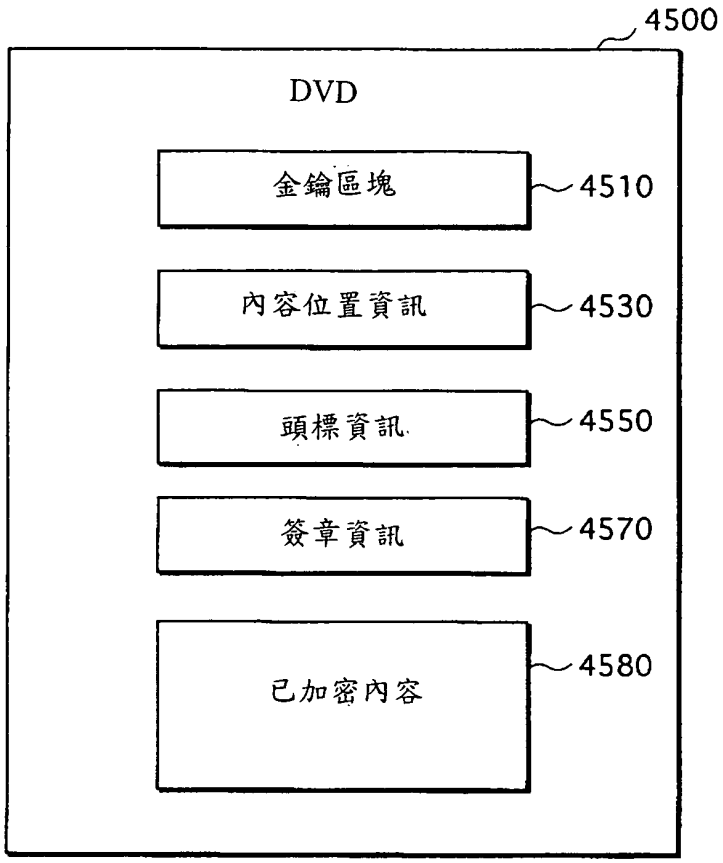
第 43 圖


4140
內容位置資訊
內容檢測資訊
識別資訊
識別符
「ADID1」
識別資訊
「AD1」
4131
4151
4141
識別資訊
識別符
「ADID2」
識別資訊
「AD2」
4142
識別資訊
識別符
「ADID3」
識別資訊
「AD3」
4143
識別資訊
識別符
「ADIDc」
識別資訊
「ADc」
4146

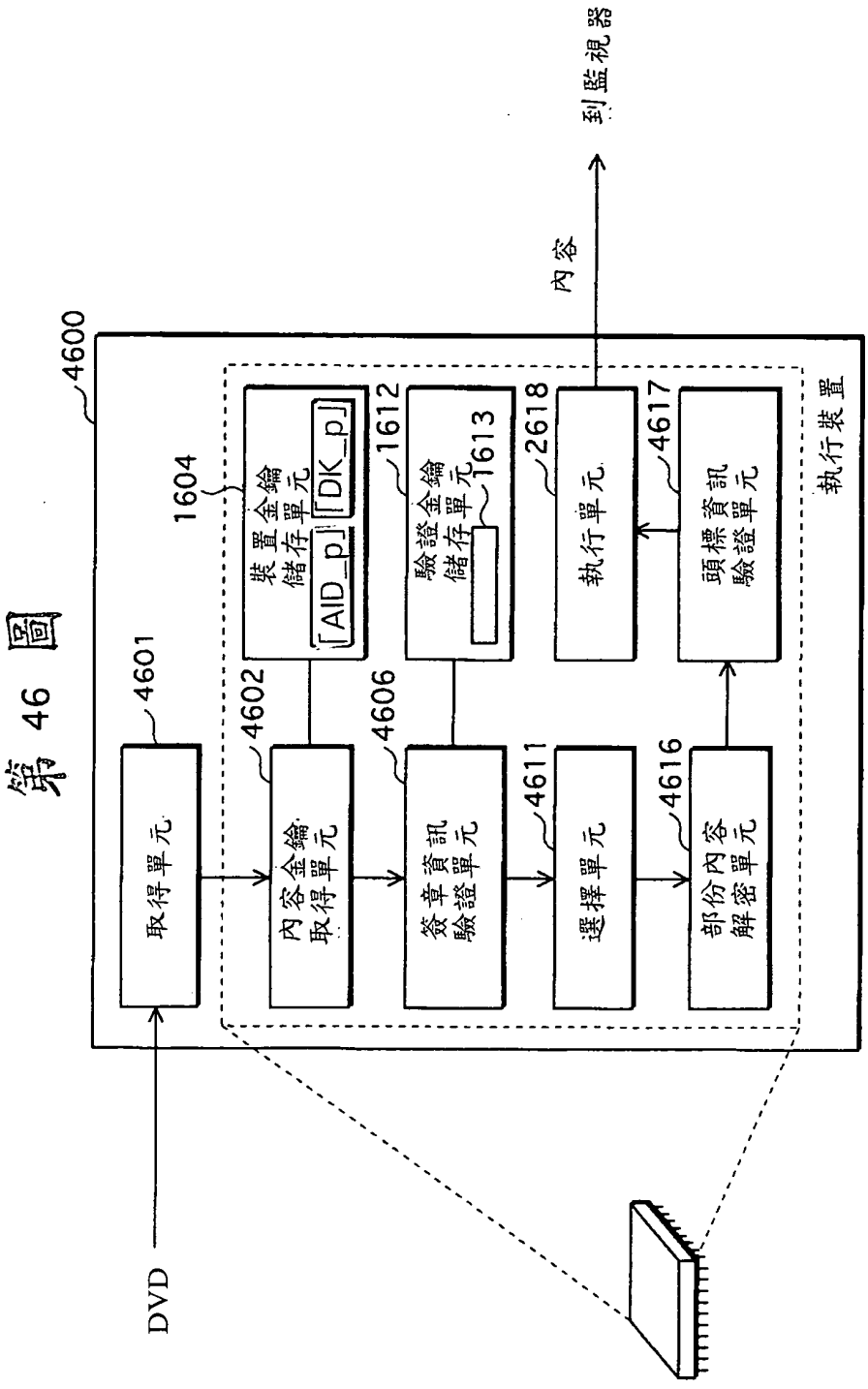
第 44 圖


4160
頭標資訊
部分雜湊資訊
識別資訊
識別符
「ADID1」
部分雜湊值
「HA1」
4171
4172
4161
識別資訊
識別符
「ADID2」
部分雜湊值
「HA2」
4162
識別資訊
識別符
「ADID3」
部分雜湊值
「HA3」
4163
識別資訊
識別符
「ADIDc」
部分雜湊值
「HAc」
4166

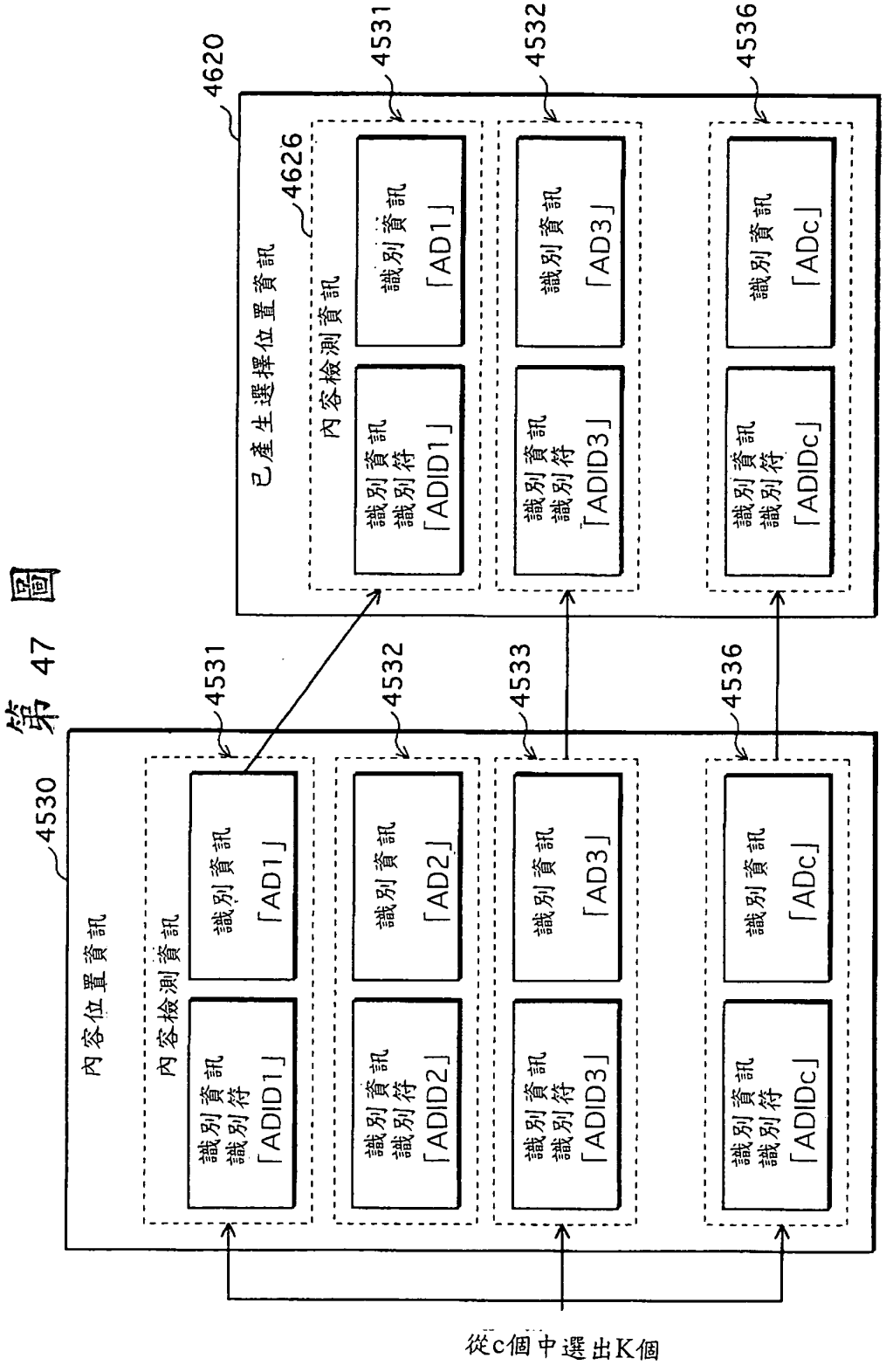
第 45 圖


4500
DVD
金鑰區塊
4510
內容位置資訊
4530
頭標資訊
4550
簽章資訊
4570
已加密內容
4580

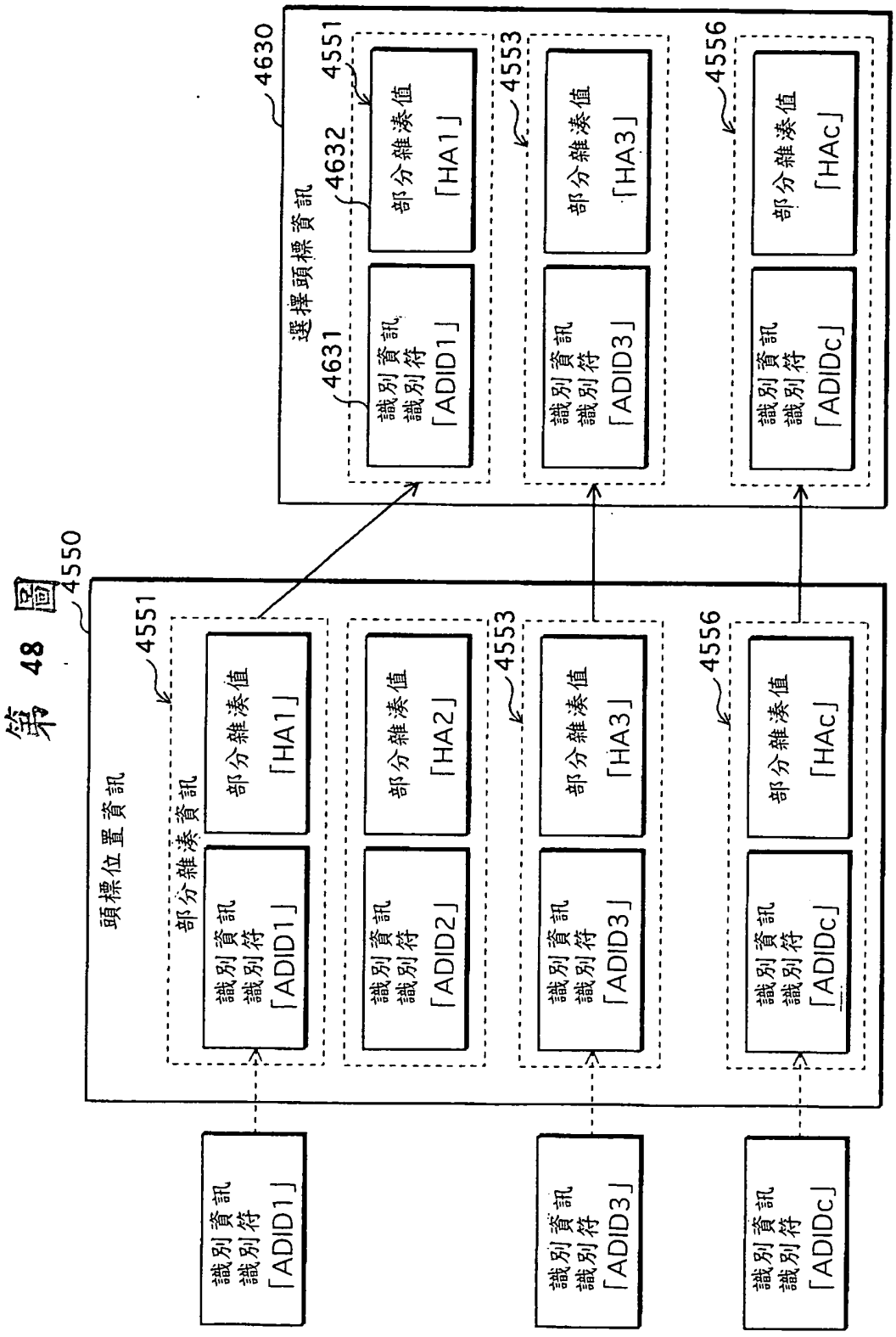
第 46 圖


4600
1604
4601
4602
4606
4611
4616
2618
4617
1612
1613
取得單元
內容金鑰取得單元
簽章資訊驗證單元
選擇單元
部份內容解密單元
執行單元
頭標資訊驗證單元
裝置金鑰儲存單元
「AID_p」
「DK_p」
驗證金鑰儲存單元
執行裝置
內容
到監視器
DVD

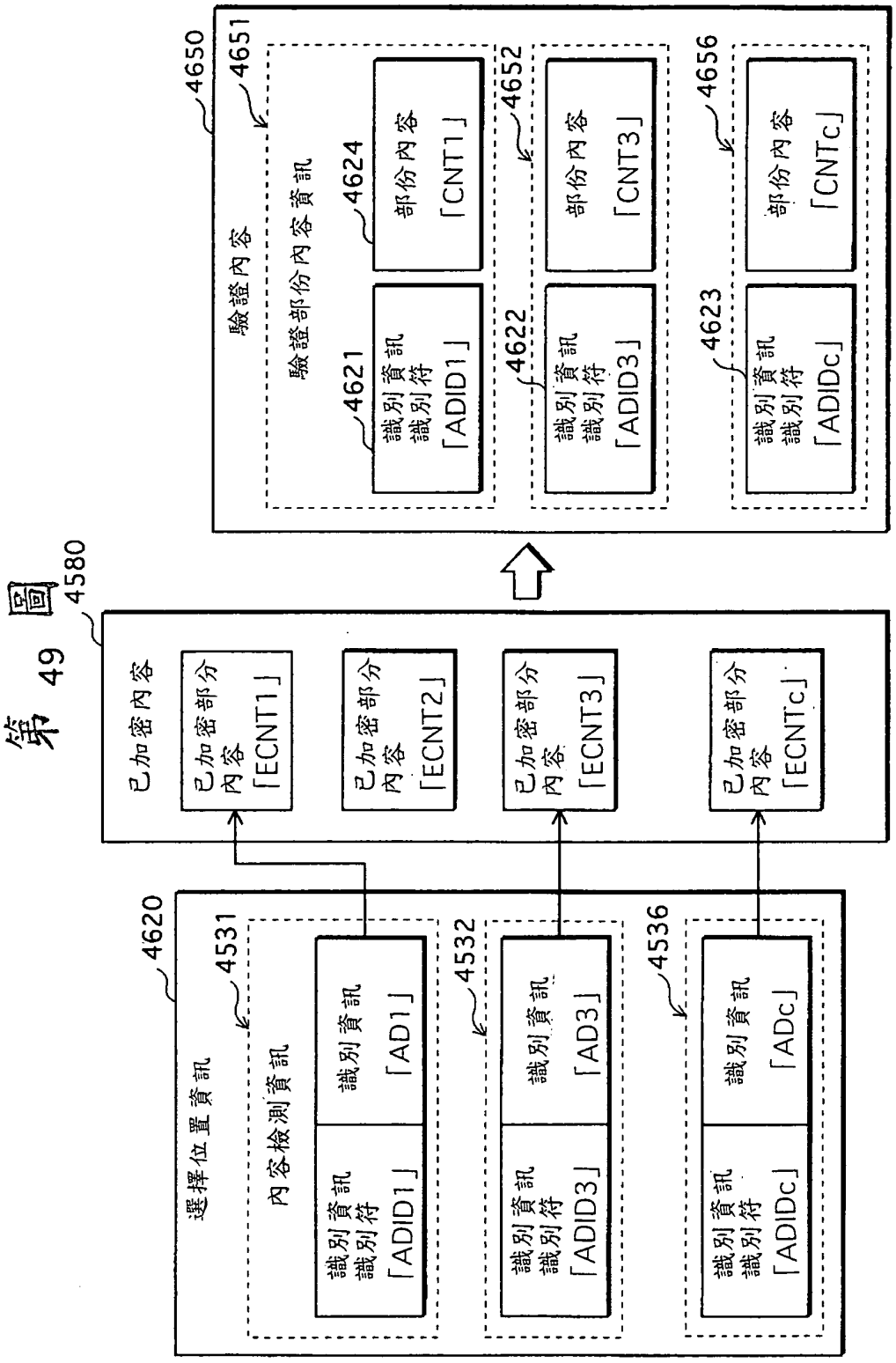
第47圖


4620
已產生選擇位置資訊
4626
內容檢測資訊
4531
識別資訊
識別符
「ADID1」
識別資訊
「AD1」
4532
識別資訊
識別符
「ADID3」
識別資訊
「AD3」
4536
識別資訊
識別符
「ADIDc」
識別資訊
「ADc」
4530
內容位置資訊
內容檢測資訊
4531
識別資訊
識別符
「ADID1」
識別資訊
「AD1」
4532
識別資訊
識別符
「ADID2」
識別資訊
「AD2」
4533
識別資訊
識別符
「ADID3」
識別資訊
「AD3」
4536
識別資訊
識別符
「ADIDc」
識別資訊
「ADc」
從c個中選出K個

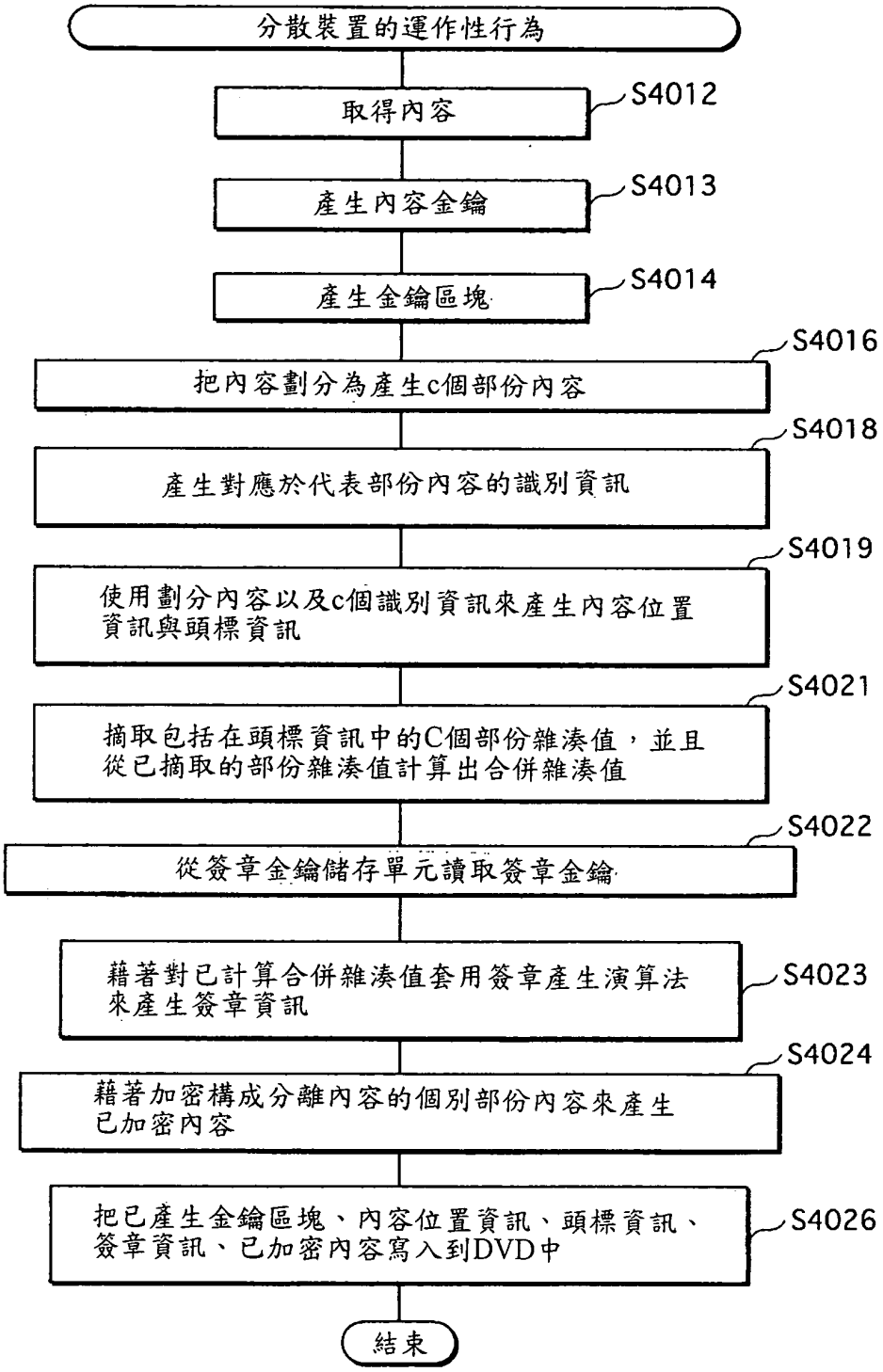
第 48 圖


4550
頭標位置資訊
4551
部分雜湊資訊
識別資訊
識別符
「ADID1」
部分雜湊值
「HA1」
識別資訊
識別符
「ADID2」
部分雜湊值
「HA2」
4553
識別資訊
識別符
「ADID3」
部分雜湊值
「HA3」
4556
識別資訊
識別符
「ADIDc」
部分雜湊值
「HAc」
4630
選擇頭標資訊
4551
4631
4632
識別資訊
識別符
「ADID1」
部分雜湊值
「HA1」
4553
識別資訊
識別符
「ADID3」
部分雜湊值
「HA3」
4556
識別資訊
識別符
「ADIDc」
部分雜湊值
「HAc」
識別資訊
識別符
「ADID1」
識別資訊
識別符
「ADID3」
識別資訊
識別符
「ADIDc」

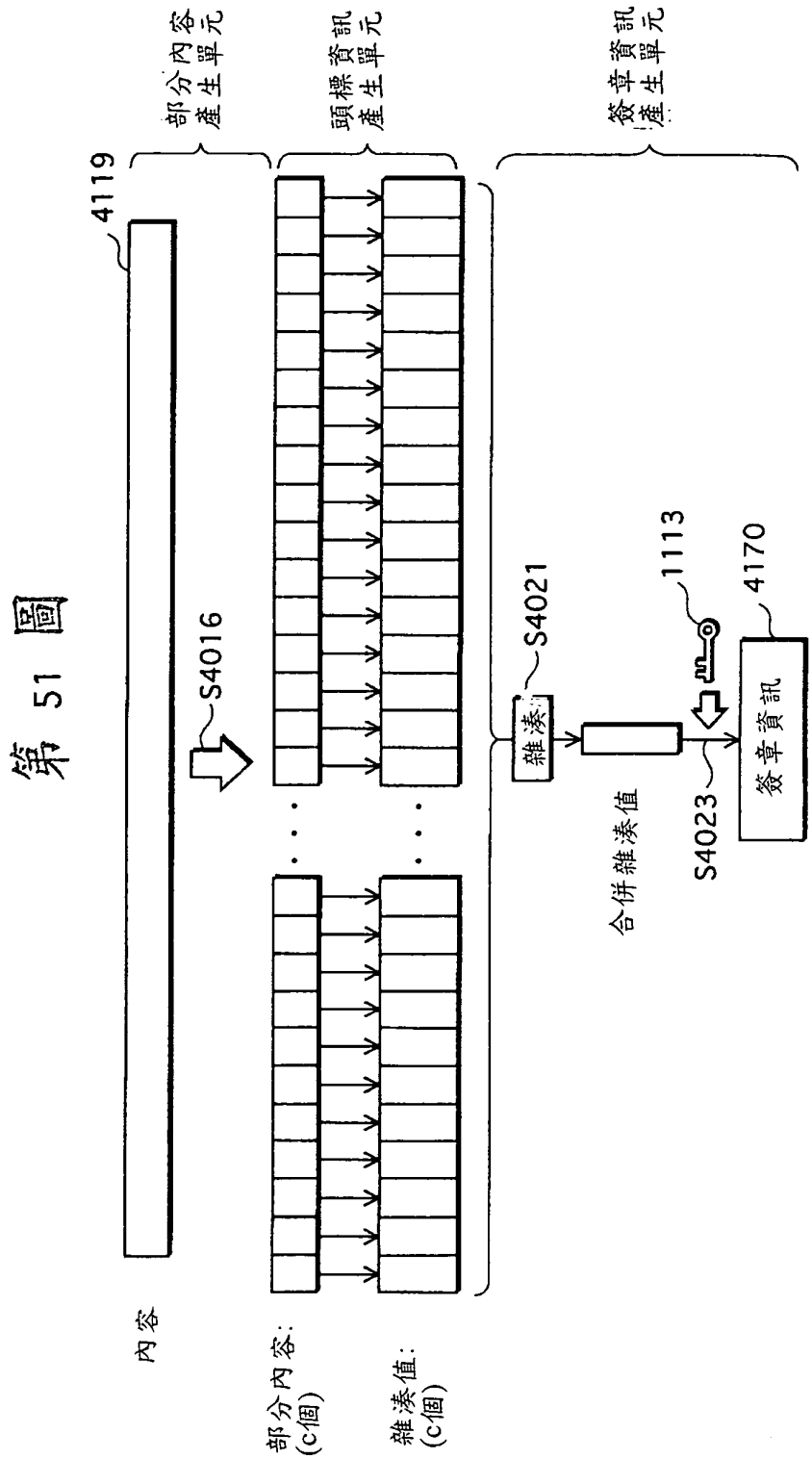
第 49 圖


4650
4651
驗證內容
驗證部份內容資訊
4621
識別資訊
識別符
「ADID1」
4624
部份內容
「CNT1」
4622
識別資訊
識別符
「ADID3」
4652
部份內容
「CNT3」
4623
識別資訊
識別符
「ADIDc」
4656
部份內容
「CNTc」
4580
已加密內容
已加密部分
內容
「ECNT1」
已加密部分
內容
「ECNT2」
已加密部分
內容
「ECNT3」
已加密部分
內容
「ECNTc」
4620
選擇位置資訊
4531
內容檢測資訊
識別資訊
識別符
「ADID1」
識別資訊
「AD1」
4532
識別資訊
識別符
「ADID3」
識別資訊
「AD3」
4536
識別資訊
識別符
「ADIDc」
識別資訊
「ADc」

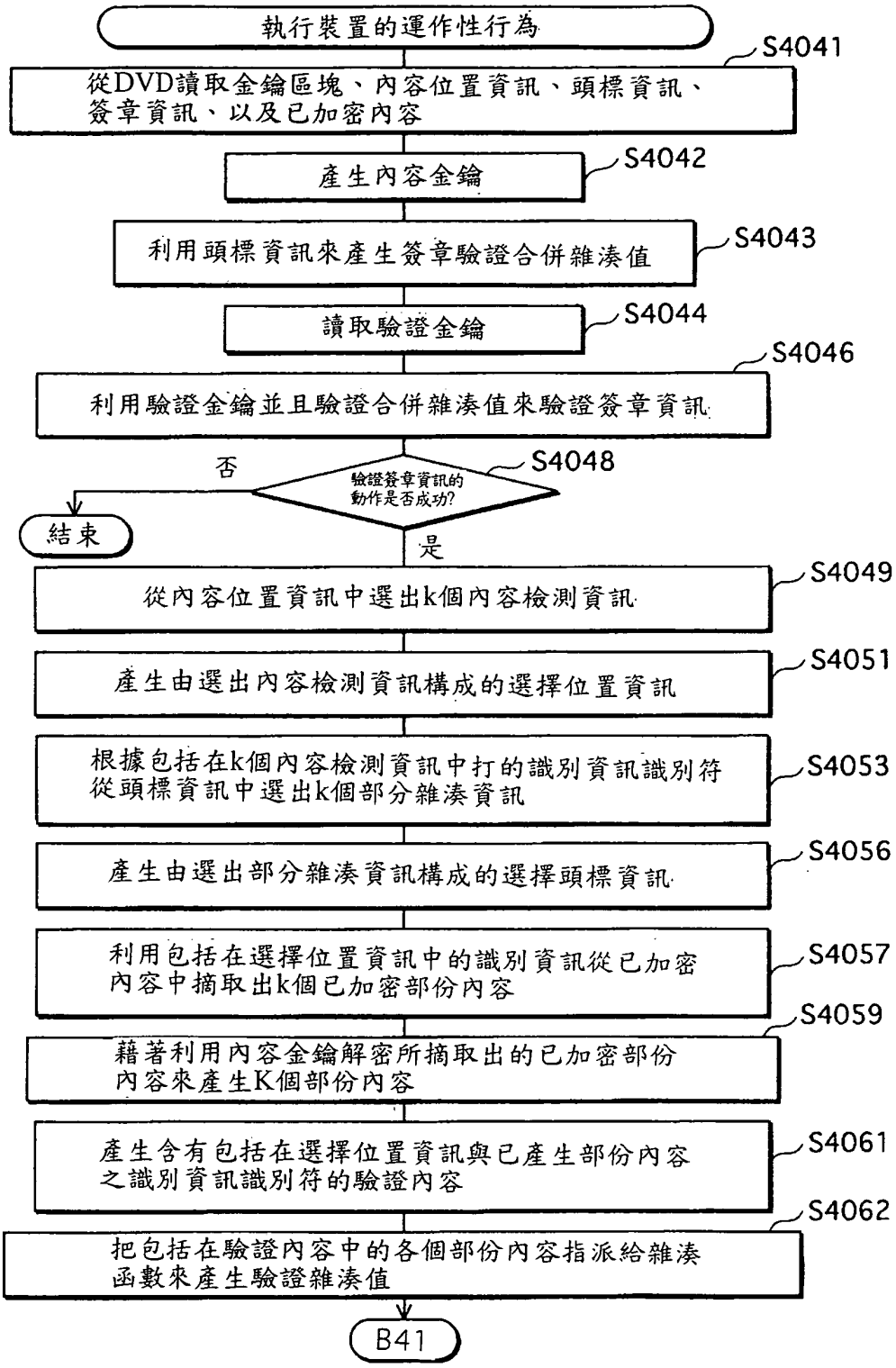
第 50 圖


分散裝置的運作性行為
取得內容
S4012
產生內容金鑰
S4013
產生金鑰區塊
S4014
把內容劃分為產生c個部份內容
S4016
產生對應於代表部份內容的識別資訊
S4018
使用劃分內容以及c個識別資訊來產生內容位置資訊與頭標資訊
S4019
摘取包括在頭標資訊中的C個部份雜湊值，並且從已摘取的部份雜湊值計算出合併雜湊值
S4021
從簽章金鑰儲存單元讀取簽章金鑰
S4022
藉著對已計算合併雜湊值套用簽章產生演算法來產生簽章資訊
S4023
藉著加密構成分離內容的個別部份內容來產生已加密內容
S4024
把已產生金鑰區塊、內容位置資訊、頭標資訊、簽章資訊、已加密內容寫入到DVD中
S4026
結束

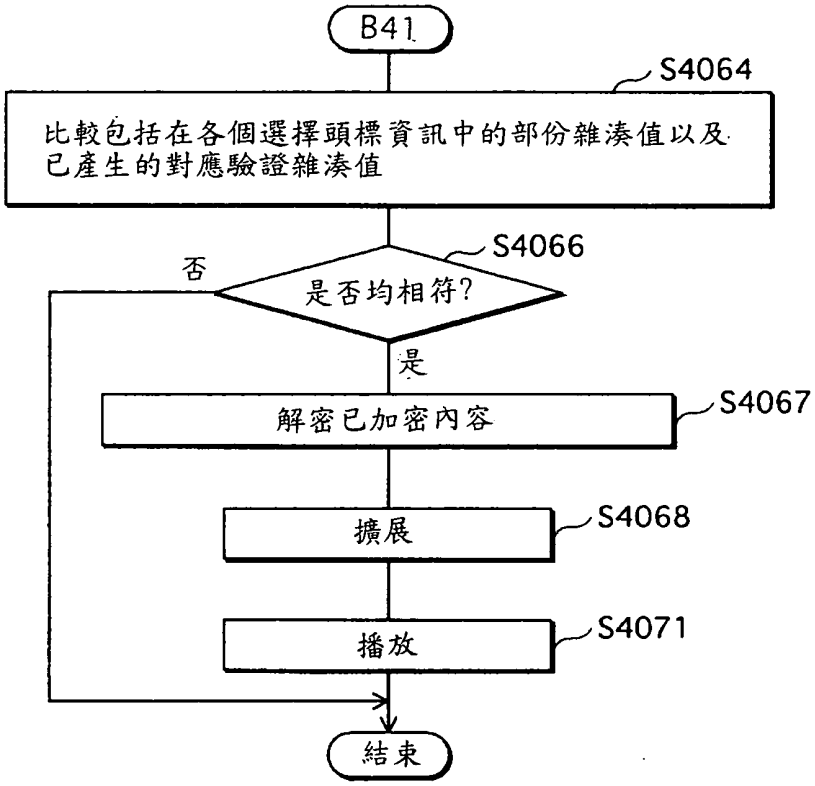
第 51 圖


部分內容產生單元
頭標資訊產生單元
簽章資訊產生單元
4119
S4016
S4021
雜湊
1113
4170
簽章資訊
S4023
合併雜湊值
內容
部分內容:
(c個)
雜湊值:
(c個)

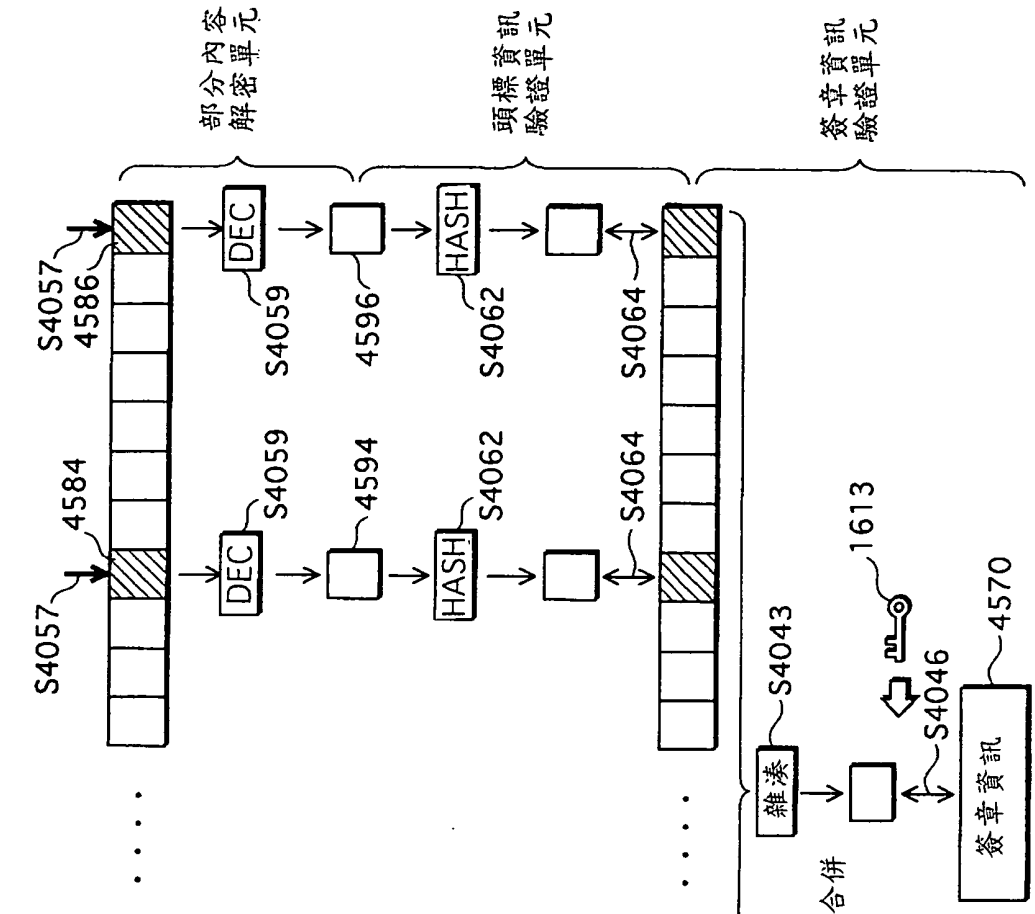
第 52 圖


執行裝置的運作性行為
S4041
從DVD讀取金鑰區塊、內容位置資訊、頭標資訊、簽章資訊、以及已加密內容
S4042
產生內容金鑰
S4043
利用頭標資訊來產生簽章驗證合併雜湊值
S4044
讀取驗證金鑰
S4046
利用驗證金鑰並且驗證合併雜湊值來驗證簽章資訊
S4048
驗證簽章資訊的動作是否成功?
否
結束
是
S4049
從內容位置資訊中選出k個內容檢測資訊
S4051
產生由選出內容檢測資訊構成的選擇位置資訊
S4053
根據包括在k個內容檢測資訊中打的識別資訊識別符從頭標資訊中選出k個部分雜湊資訊
S4056
產生由選出部分雜湊資訊構成的選擇頭標資訊
S4057
利用包括在選擇位置資訊中的識別資訊從已加密內容中摘取出k個已加密部份內容
S4059
藉著利用內容金鑰解密所摘取出的已加密部份內容來產生K個部份內容
S4061
產生含有包括在選擇位置資訊與已產生部份內容之識別資訊識別符的驗證內容
S4062
把包括在驗證內容中的各個部份內容指派給雜湊函數來產生驗證雜湊值
B41

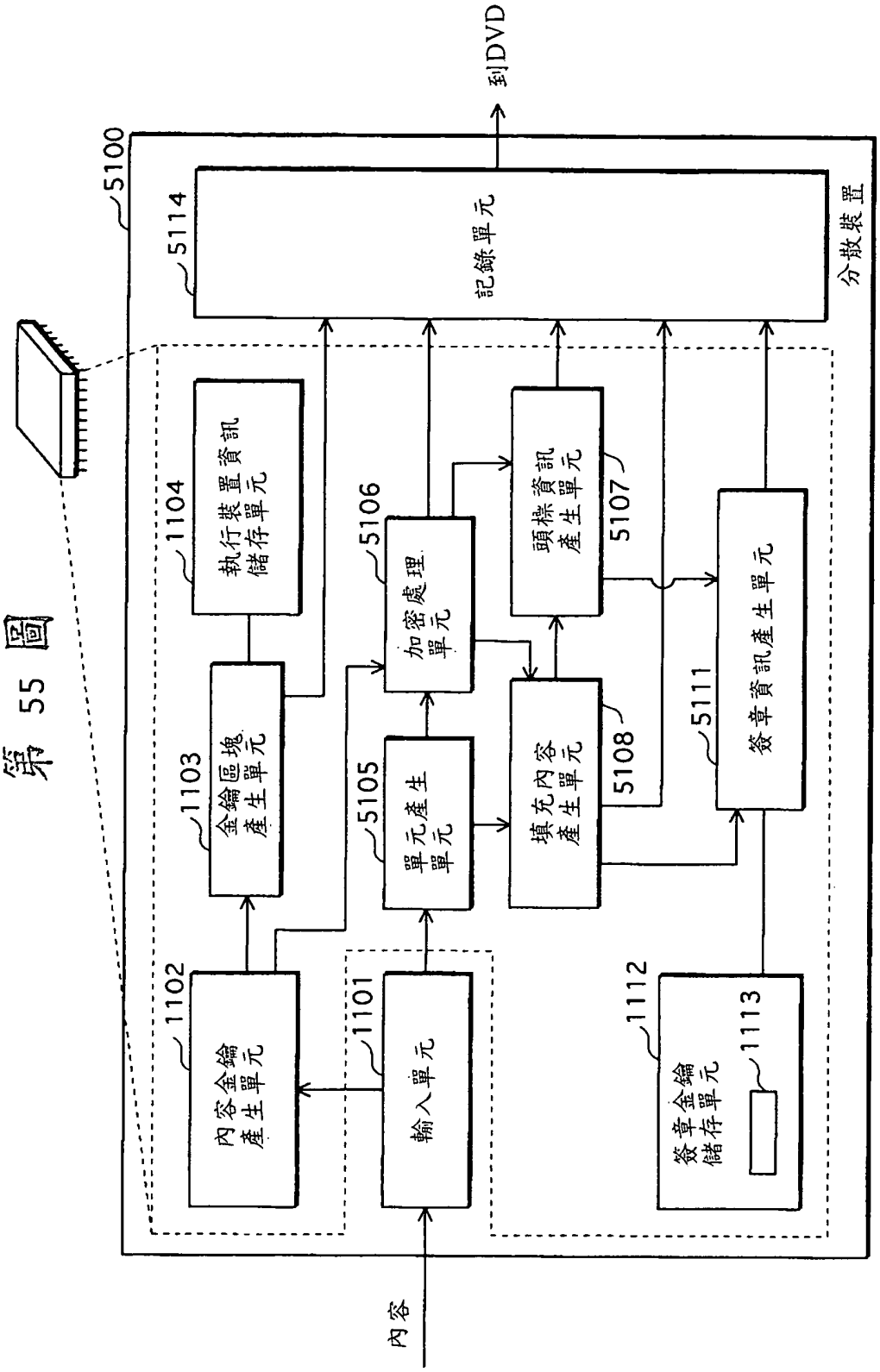
第 53 圖


B41
S4064
比較包括在各個選擇頭標資訊中的部份雜湊值以及已產生的對應驗證雜湊值
S4066
否
是否均相符?
是
解密已加密內容
S4067
擴展
S4068
播放
S4071
結束

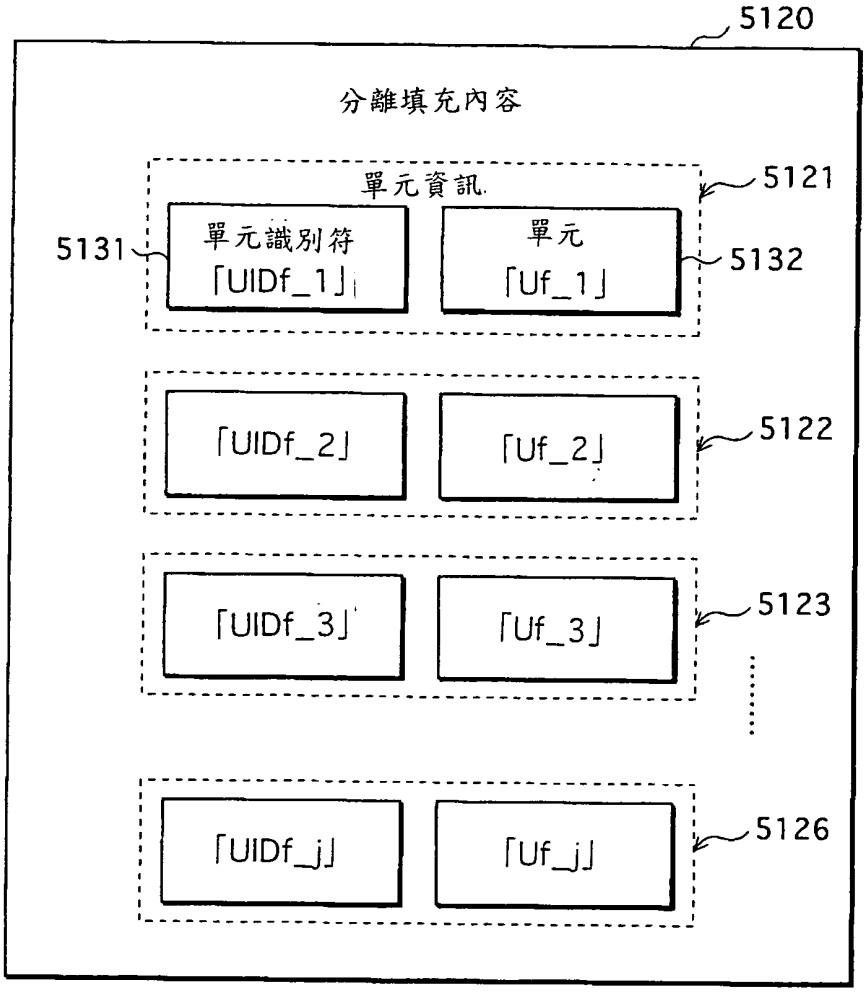
第 54 圖


部分內容解密單元
頭標資訊驗證單元
簽章資訊驗證單元
S4057
4581
4582
4583
4584
4586
DEC
S4059
4591
4592
4593
4594
4596
HASH
S4062
S4064
已加密部分內容(c個)
部分內容(k個)
驗證雜湊值
部分雜湊值(c個)
雜湊
S4043
簽章驗證合併雜湊值
1613
S4046
簽章資訊
4570

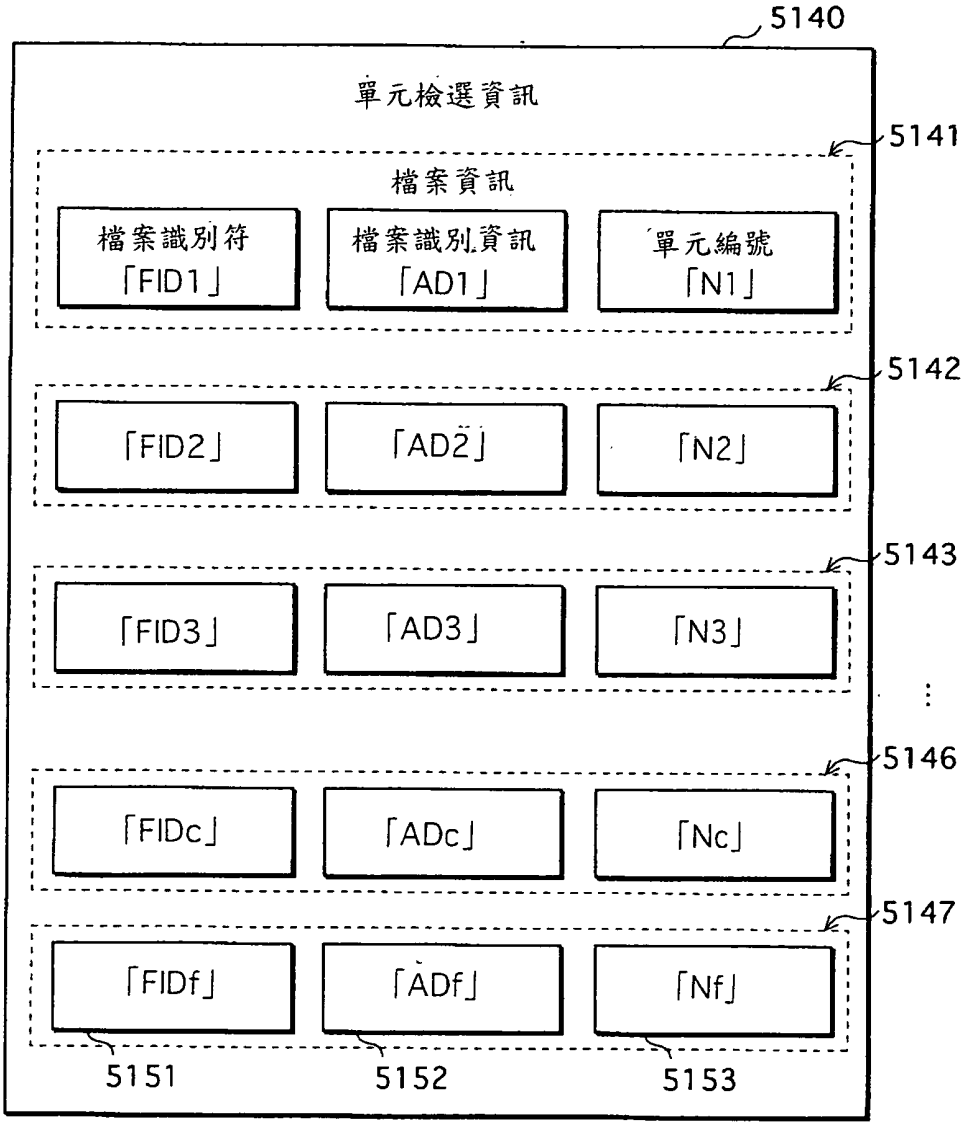
第 55 圖


5100
到DVD
5114
記錄單元
分散裝置
1104
執行裝置資訊儲存單元
5106
加密處理單元
5107
頭標資訊產生單元
1103
金鑰區塊產生單元
5105
單元產生單元
5108
填充內容產生單元
5111
簽章資訊產生單元
1102
內容金鑰產生單元
1101
輸入單元
1112
簽章金鑰儲存單元
1113
內容

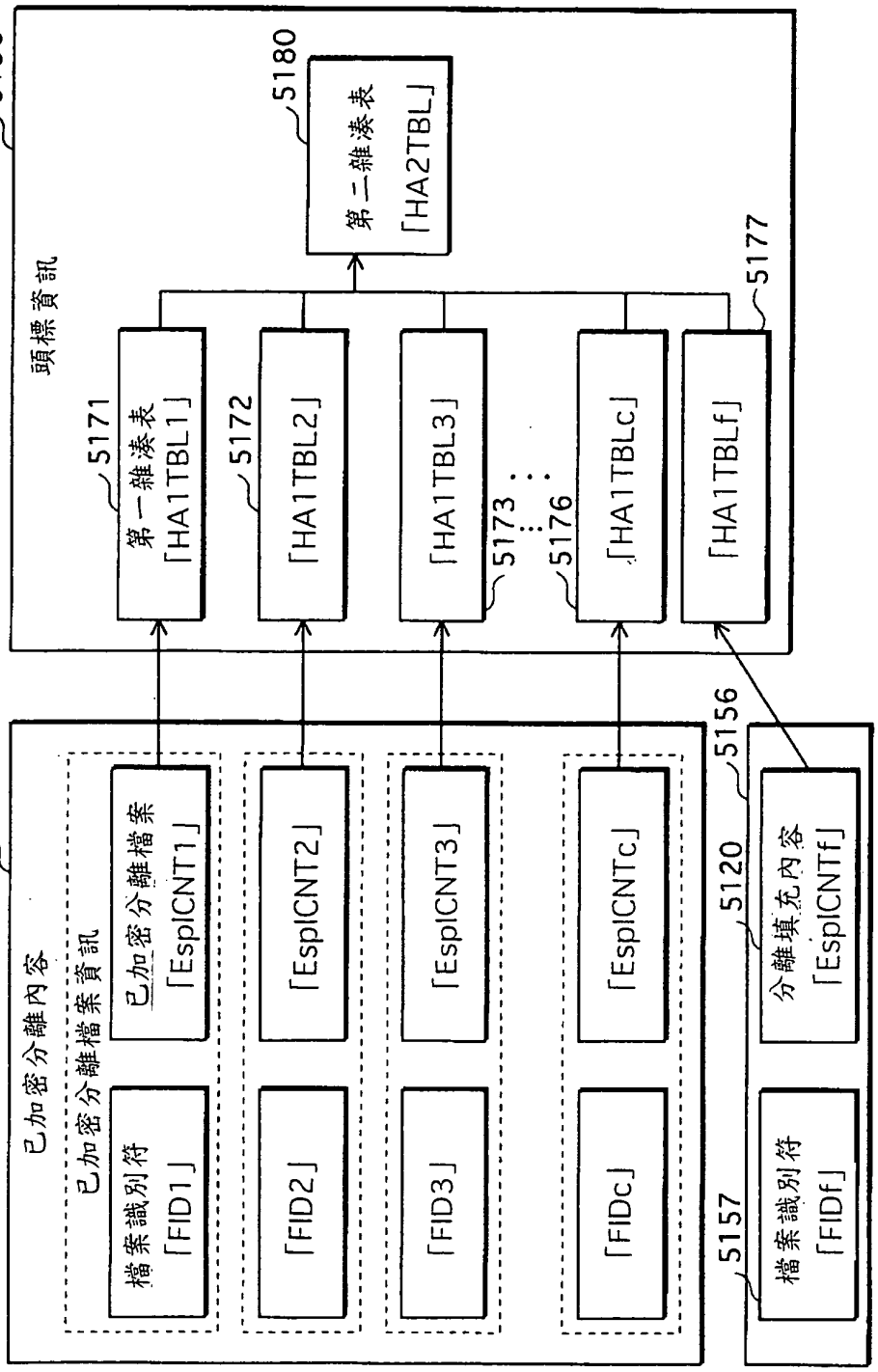
第 56 圖


5120
分離填充內容
單元資訊
5121
5131
單元識別符
「UIDf_1」
單元
「Uf_1」
5132
「UIDf_2」
「Uf_2」
5122
「UIDf_3」
「Uf_3」
5123
「UIDf_j」
「Uf_j」
5126

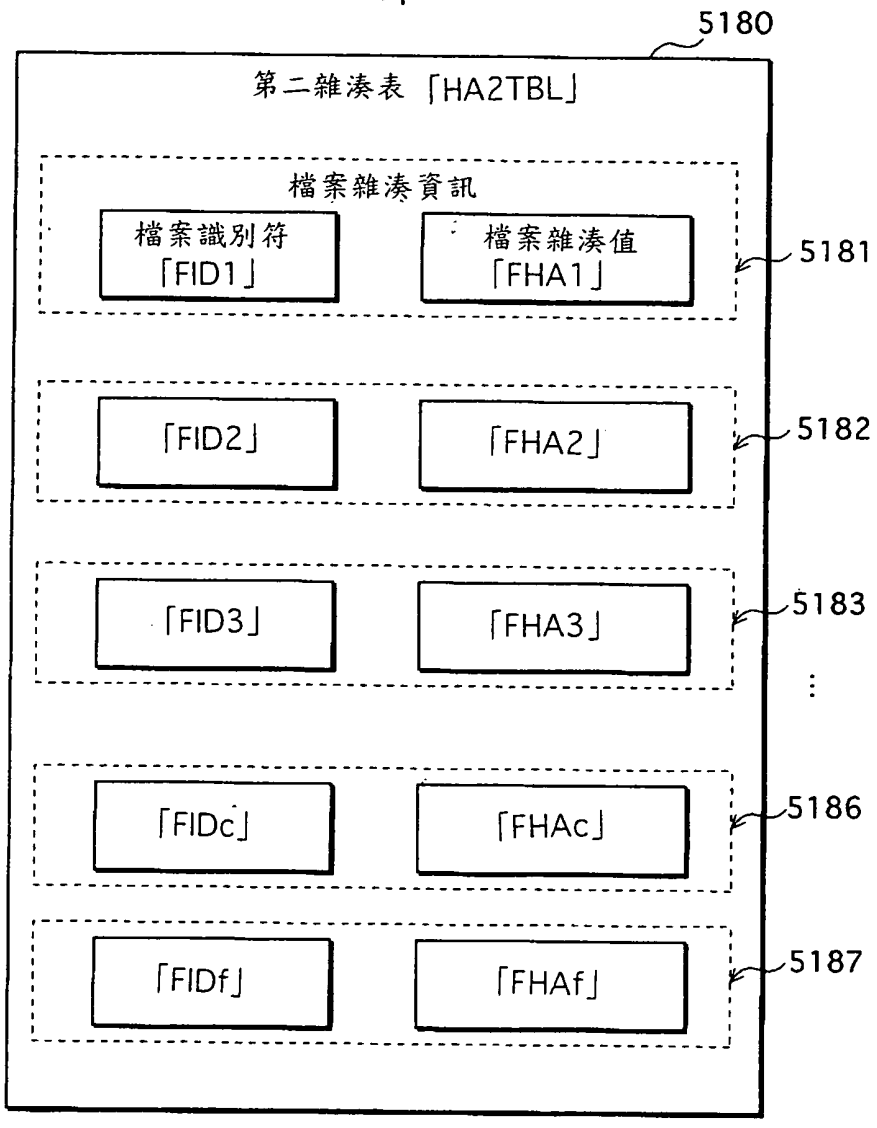
第 57 圖


5140
單元檢選資訊
5141
檔案資訊
檔案識別符
「FID1」
檔案識別資訊
「AD1」
單元編號
「N1」
5142
「FID2」
「AD2」
「N2」
5143
「FID3」
「AD3」
「N3」
5146
「FIDc」
「ADc」
「Nc」
5147
「FIDf」
「ADf」
「Nf」
5151
5152
5153

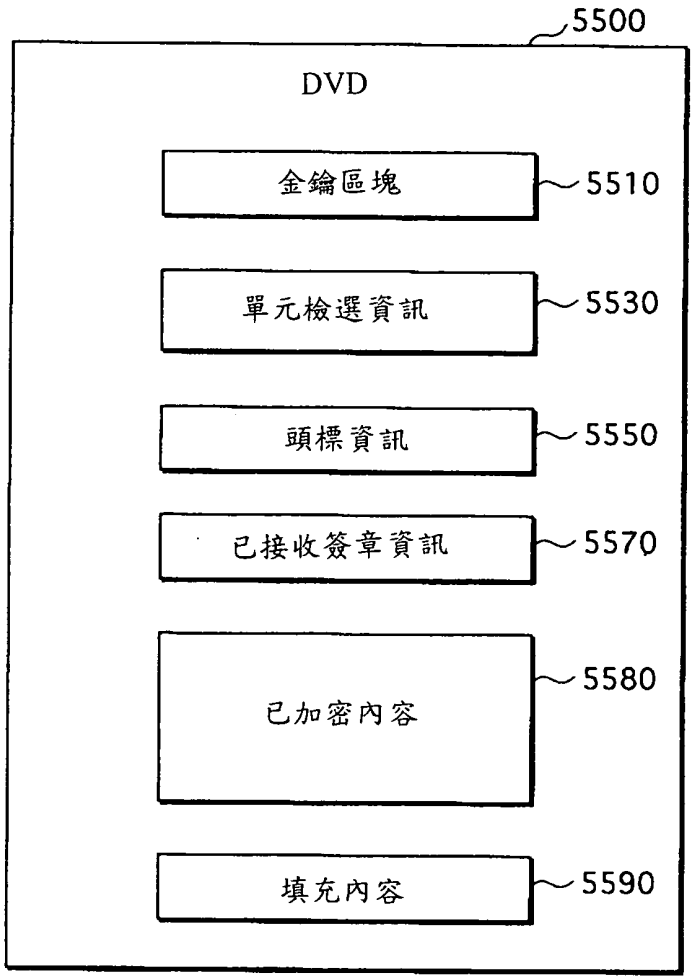
第 58 圖


5190
頭標資訊
5180
第二雜湊表
「HA2TBL」
5171
第一雜湊表
「HA1TBL1」
5172
「HA1TBL2」
「HA1TBL3」
5173
5176
「HA1TBLc」
「HA1TBLf」
5177
5160
已加密分離內容
已加密分離檔案資訊
檔案識別符
「FID1」
已加密分離檔案
「EsplCNT1」
「FID2」
「EsplCNT2」
「FID3」
「EsplCNT3」
「FIDc」
「EsplCNTc」
5156
5120
分離填充內容
「EsplCNTf」
5157
檔案識別符
「FIDf」

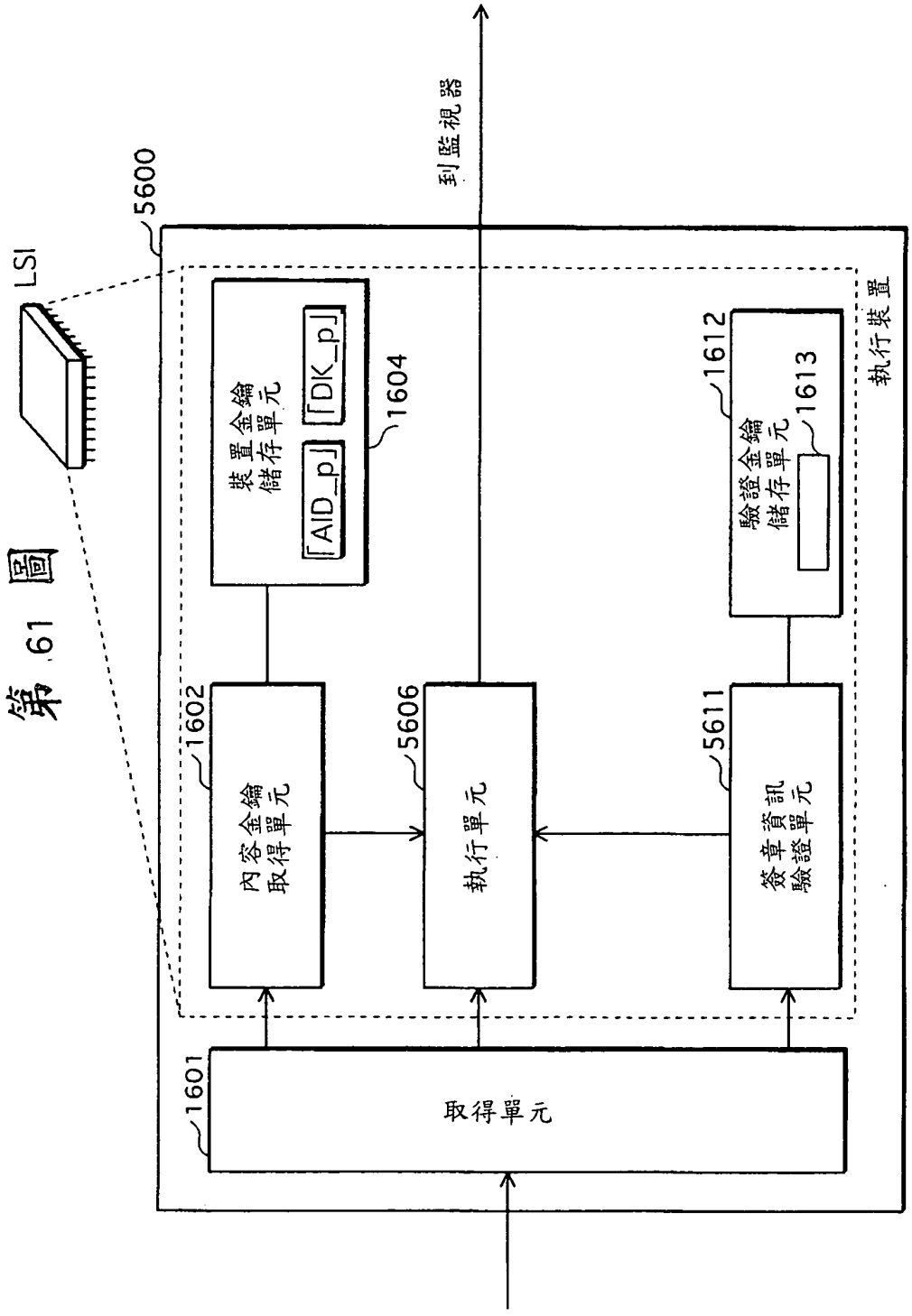
第 59 圖


5180
第二雜湊表「HA2TBL」
檔案雜湊資訊
檔案識別符
「FID1」
檔案雜湊值
「FHA1」
5181
「FID2」
「FHA2」
5182
「FID3」
「FHA3」
5183
「FIDc」
「FHAc」
5186
「FIDf」
「FHAf」
5187

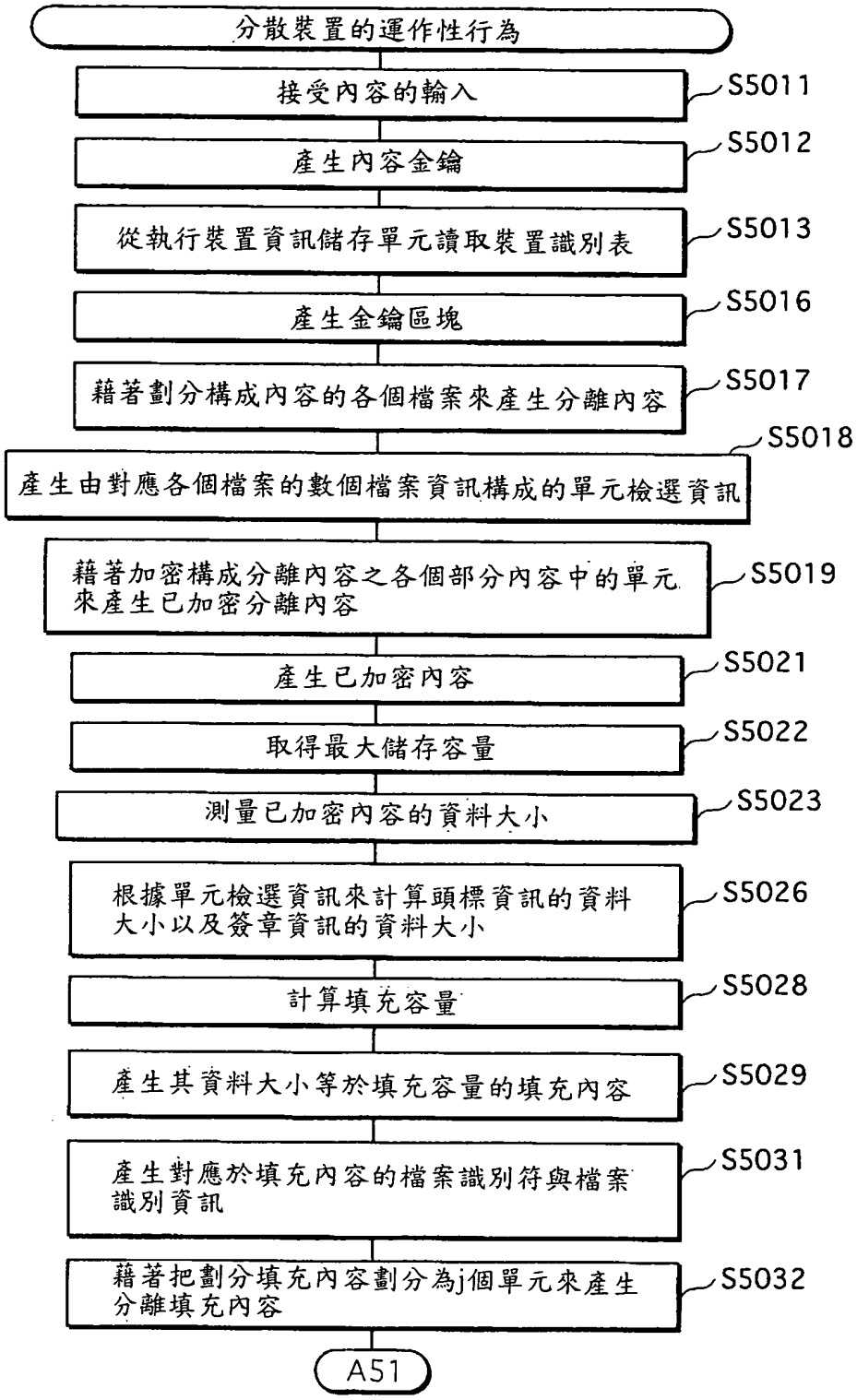
第 60 圖


5500
DVD
金鑰區塊
5510
單元檢選資訊
5530
頭標資訊
5550
已接收簽章資訊
5570
已加密內容
5580
填充內容
5590

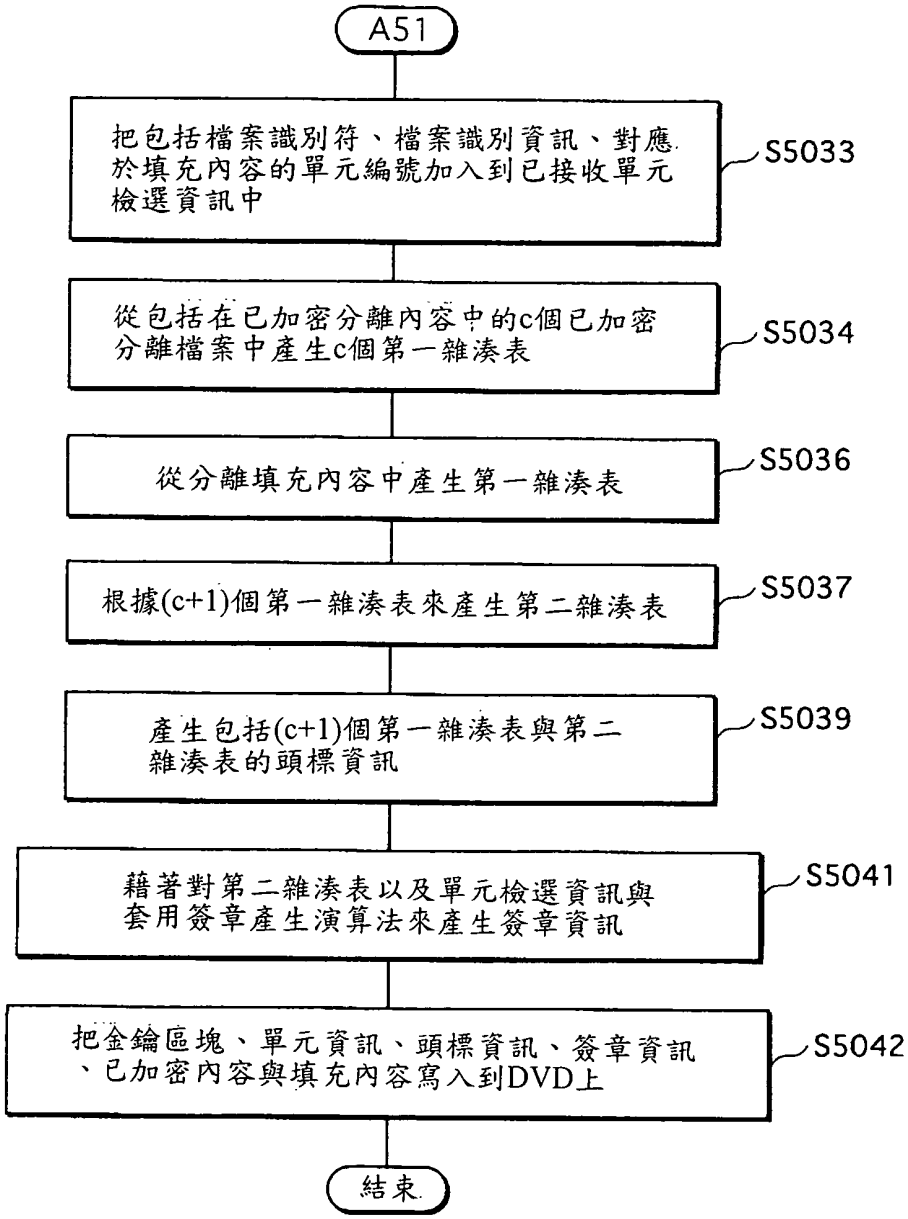
第 61 圖


LSI
5600
到監視器
執行裝置
裝置金鑰
儲存單元
「AID_pJ」
「DK_pJ」
1604
1602
內容金鑰
取得單元
5606
執行單元
1612
驗證金鑰
儲存單元
1613
5611
簽章資訊
驗證單元
1601
取得單元

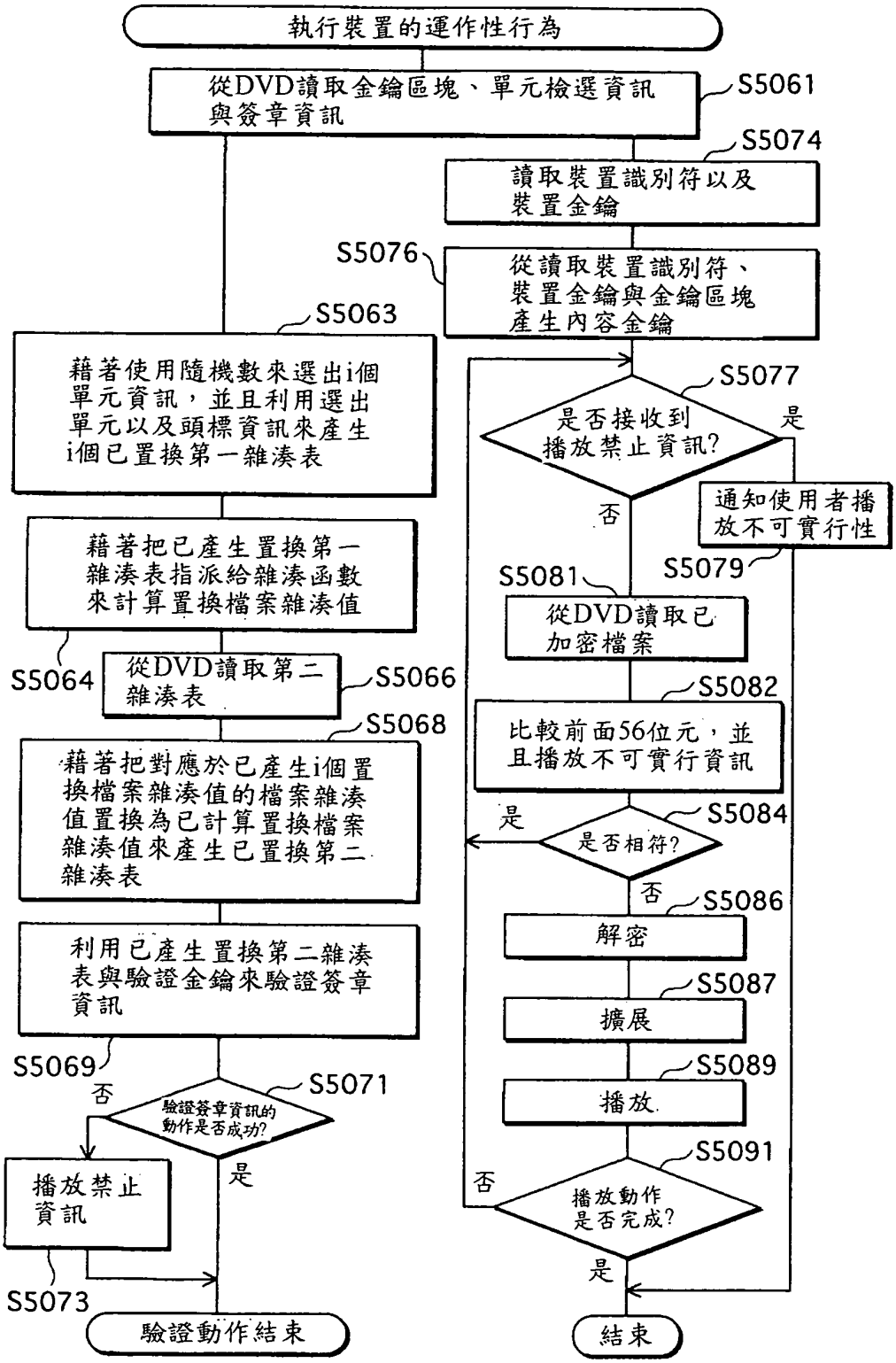
第 62 圖


分散裝置的運作性行為
接受內容的輸入
S5011
產生內容金鑰
S5012
從執行裝置資訊儲存單元讀取裝置識別表
S5013
產生金鑰區塊
S5016
藉著劃分構成內容的各個檔案來產生分離內容
S5017
產生由對應各個檔案的數個檔案資訊構成的單元檢選資訊
S5018
藉著加密構成分離內容之各個部分內容中的單元來產生已加密分離內容
S5019
產生已加密內容
S5021
取得最大儲存容量
S5022
測量已加密內容的資料大小
S5023
根據單元檢選資訊來計算頭標資訊的資料大小以及簽章資訊的資料大小
S5026
計算填充容量
S5028
產生其資料大小等於填充容量的填充內容
S5029
產生對應於填充內容的檔案識別符與檔案識別資訊
S5031
藉著把劃分填充內容劃分為j個單元來產生分離填充內容
S5032
A51

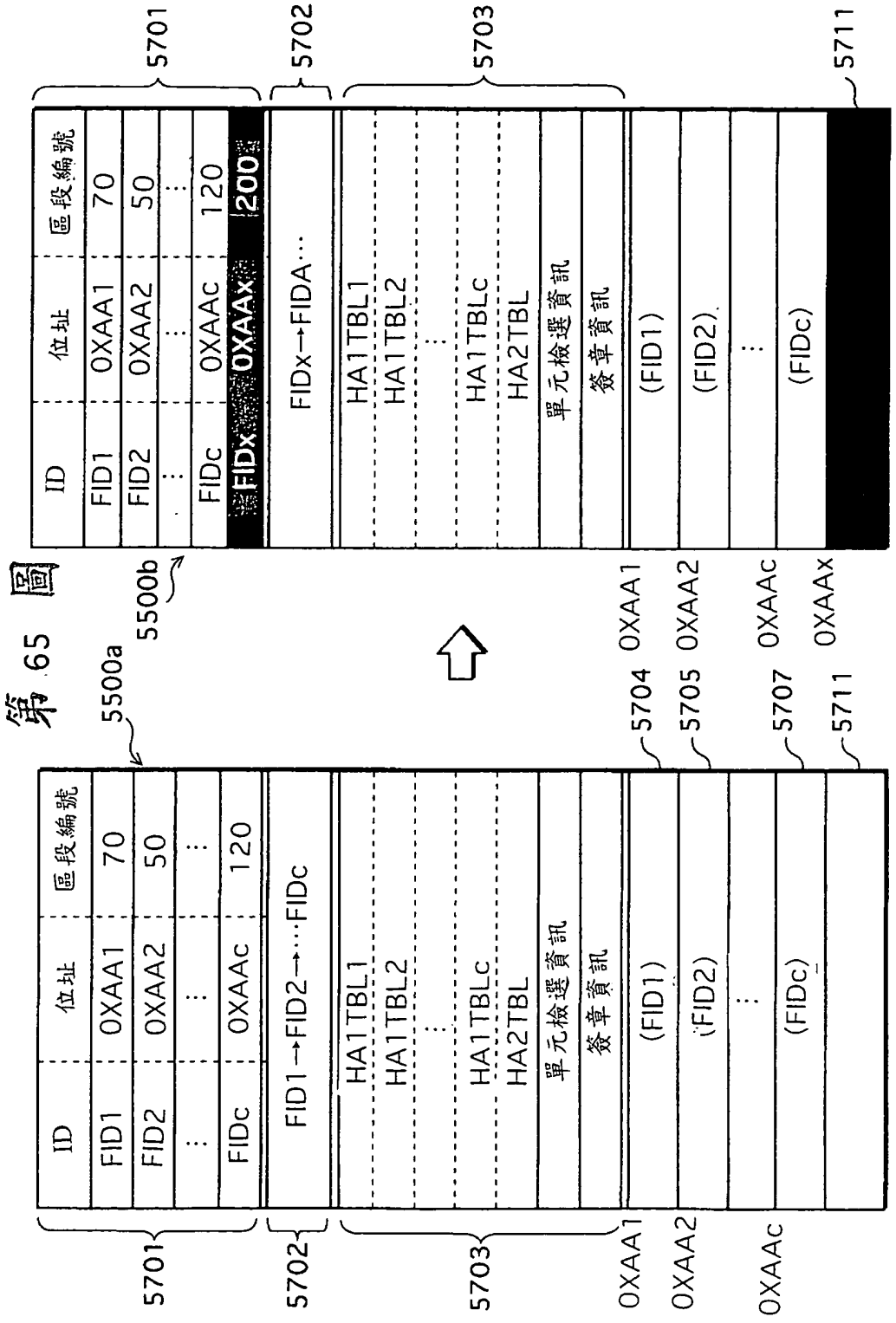
第 63 圖


A51
把包括檔案識別符、檔案識別資訊、對應於填充內容的單元編號加入到已接收單元檢選資訊中
S5033
從包括在已加密分離內容中的c個已加密分離檔案中產生c個第一雜湊表
S5034
從分離填充內容中產生第一雜湊表
S5036
根據(c+1)個第一雜湊表來產生第二雜湊表
S5037
產生包括(c+1)個第一雜湊表與第二雜湊表的頭標資訊
S5039
藉著對第二雜湊表以及單元檢選資訊與套用簽章產生演算法來產生簽章資訊
S5041
把金鑰區塊、單元資訊、頭標資訊、簽章資訊、已加密內容與填充內容寫入到DVD上
S5042
結束

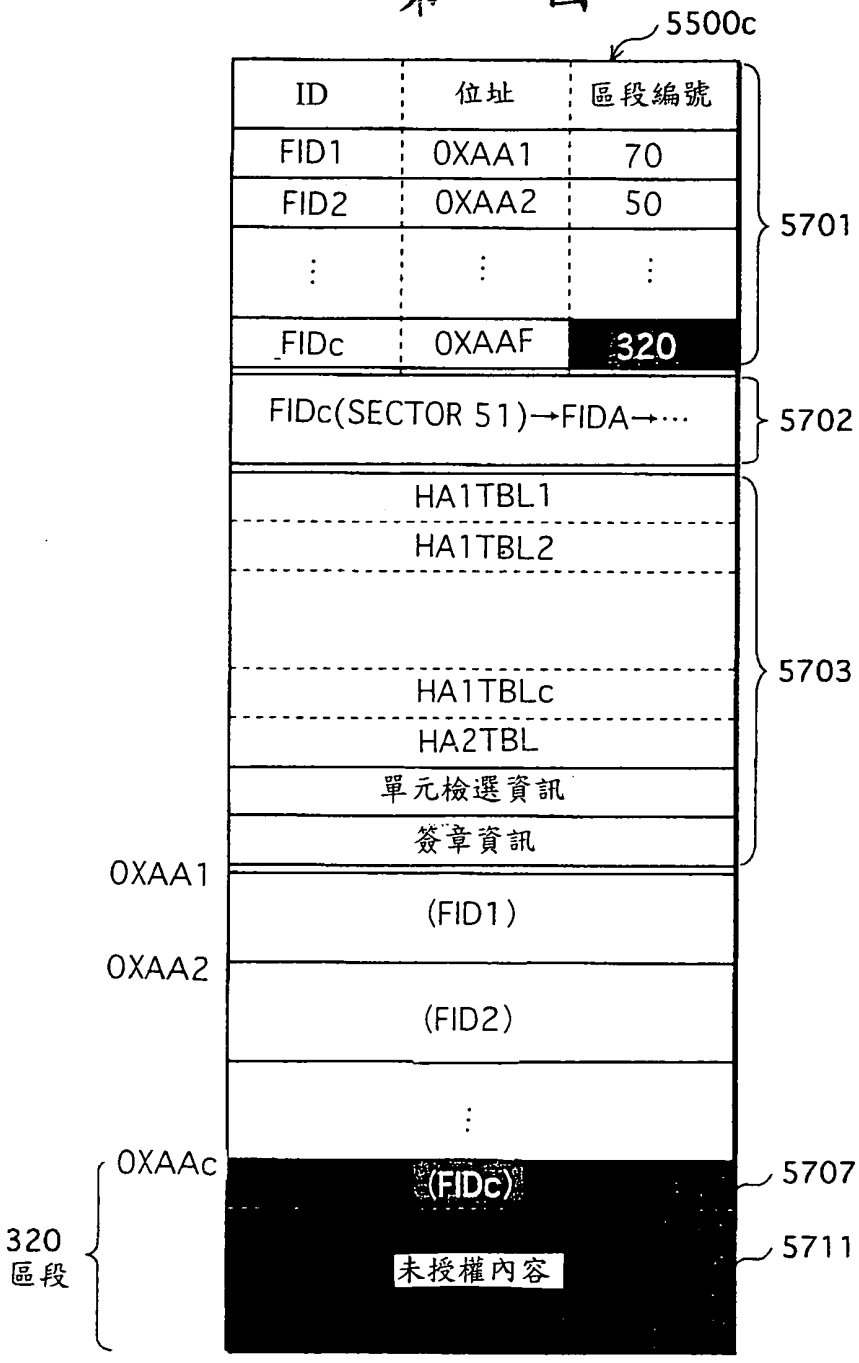
第 64 圖


執行裝置的運作性行為
從DVD讀取金鑰區塊、單元檢選資訊與簽章資訊
S5061
S5074
讀取裝置識別符以及裝置金鑰
S5076
從讀取裝置識別符、裝置金鑰與金鑰區塊產生內容金鑰
S5063
藉著使用隨機數來選出i個單元資訊，並且利用選出單元以及頭標資訊來產生i個已置換第一雜湊表
藉著把已產生置換第一雜湊表指派給雜湊函數來計算置換檔案雜湊值
S5064
從DVD讀取第二雜湊表
S5066
S5068
藉著把對應於已產生i個置換檔案雜湊值的檔案雜湊值置換為已計算置換檔案雜湊值來產生已置換第二雜湊表
利用已產生置換第二雜湊表與驗證金鑰來驗證簽章資訊
S5069
否
驗證簽章資訊的動作是否成功?
S5071
是
播放禁止資訊
S5073
驗證動作結束
S5077
是否接收到播放禁止資訊?
是
否
通知使用者播放不可實行性
S5079
S5081
從DVD讀取已加密檔案
S5082
比較前面56位元，並且播放不可實行資訊
是
是否相符?
S5084
否
S5086
解密
S5087
擴展
S5089
播放
S5091
否
播放動作是否完成?
是
結束

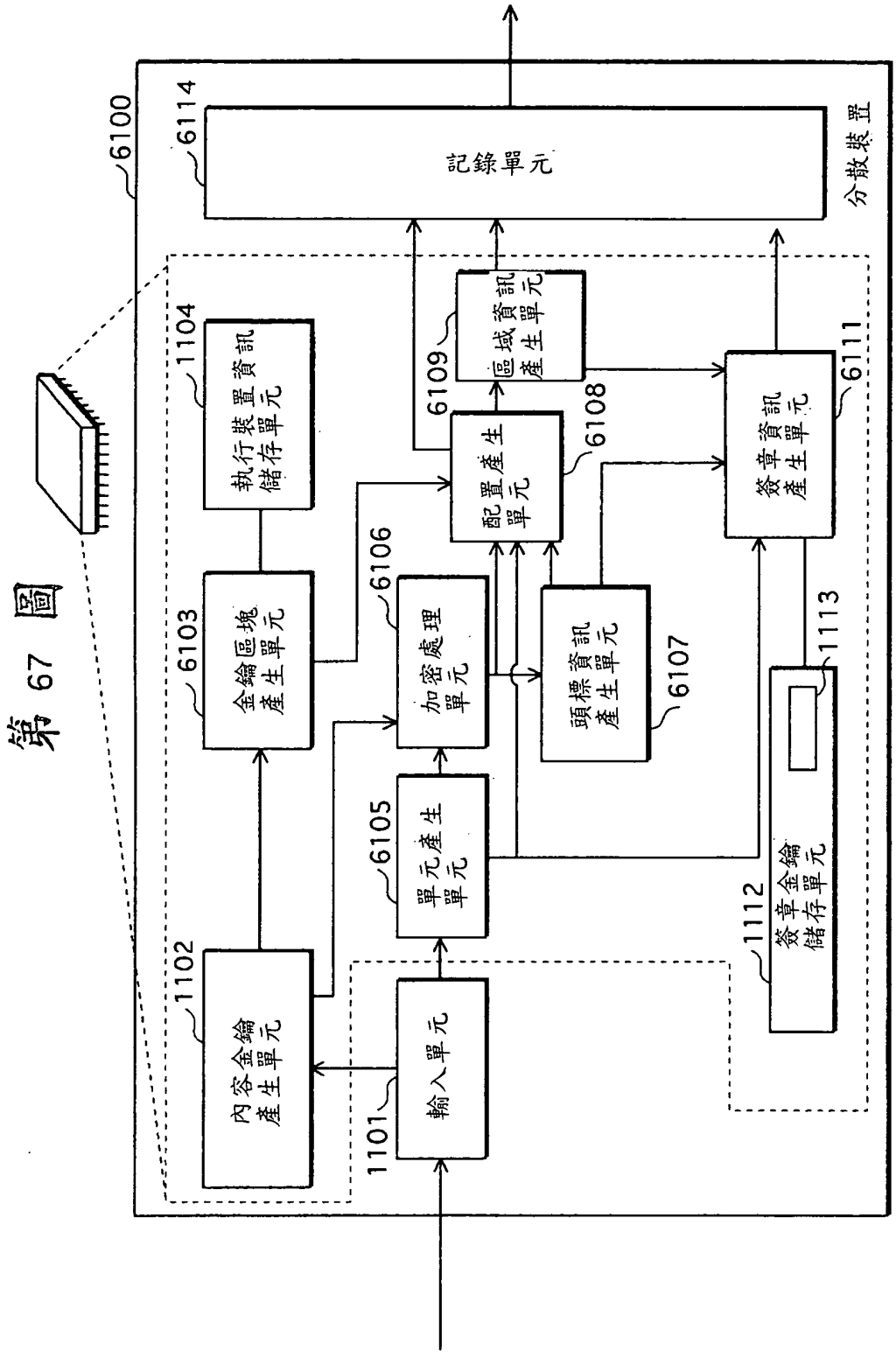
第 65 圖


5500a
5500b
ID
位址
區段編號
FID1
FID2
FIDc
0XAA1
0XAA2
0XAAc
0XAAx
70
50
120
200
FID1→FID2→…FIDc
FIDx→FIDA…
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
單元檢選資訊
簽章資訊
(FID1)
(FID2)
(FIDc)
5701
5702
5703
5704
5705
5707
5711
0XAA1
0XAA2
0XAAc
0XAAx

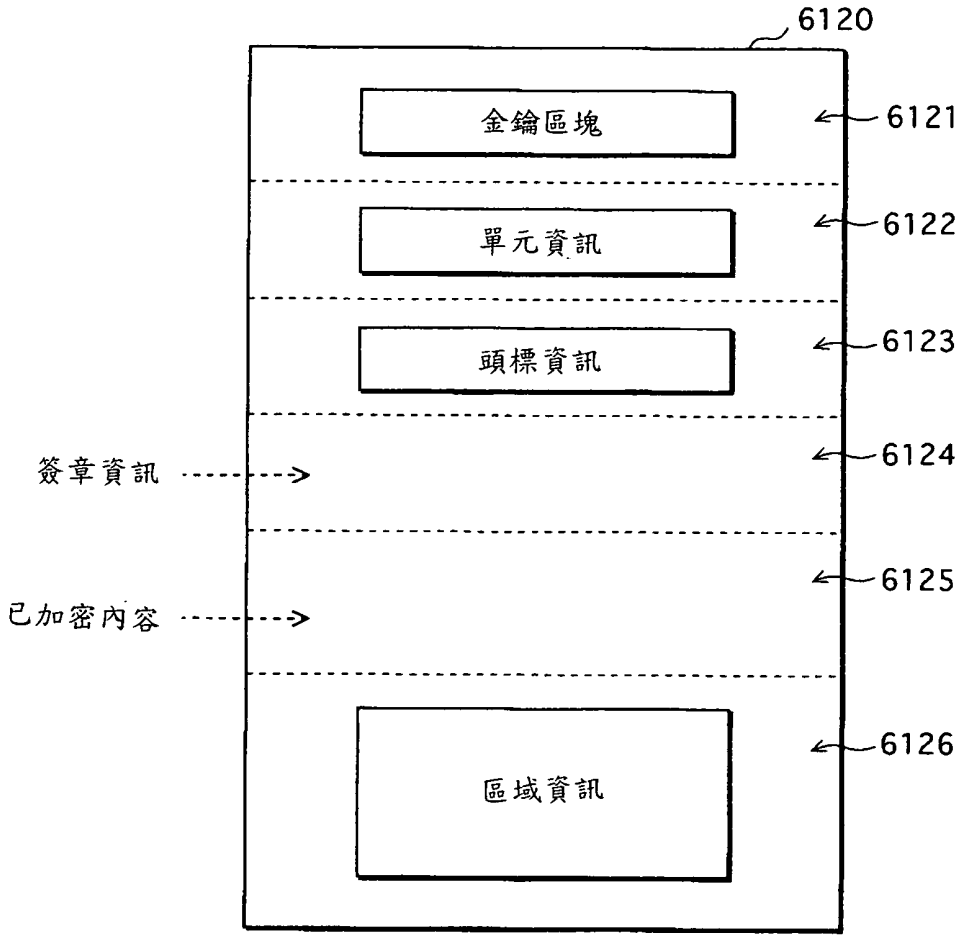
第 66 圖


5500c
ID
位址
區段編號
FID1
0XAA1
70
FID2
0XAA2
50
FIDc
0XAAF
320
5701
FIDc(SECTOR 51)→FIDA→…
5702
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
單元檢選資訊
簽章資訊
5703
0XAA1
(FID1)
0XAA2
(FID2)
0XAAc
(FIDc)
5707
未授權內容
5711
320
區段

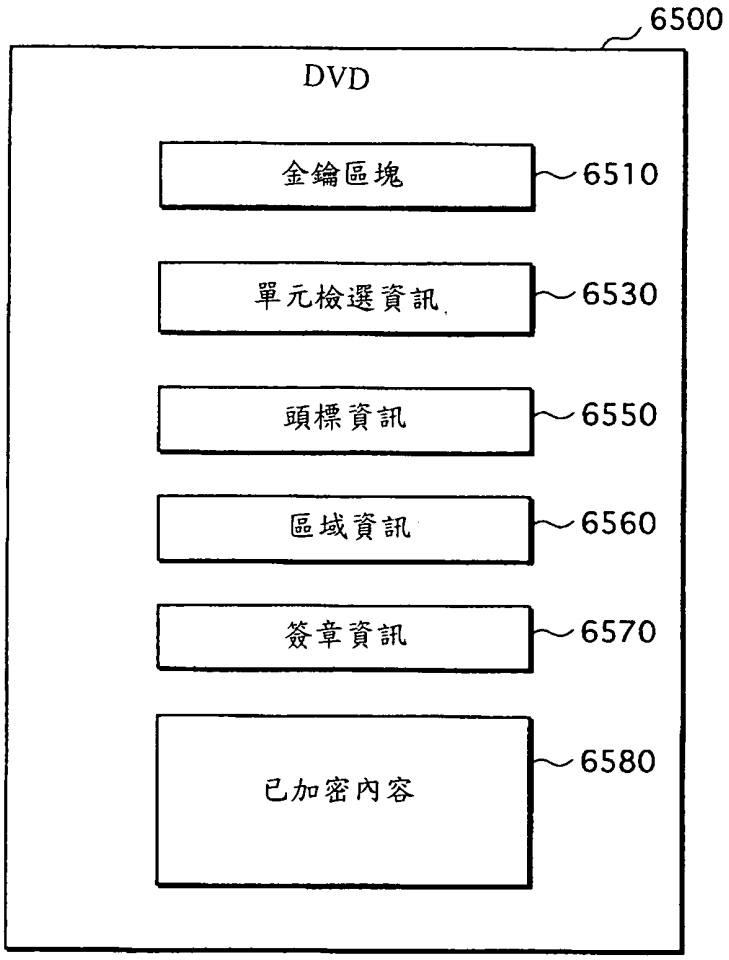
第 67 圖


6100
6114
記錄單元
分散裝置
1104
執行裝置資訊儲存單元
6109
區域資訊產生單元
6108
配置產生單元
6111
簽章資訊產生單元
6103
金鑰區塊產生單元
6106
加密處理單元
頭標資訊產生單元
6107
1113
6105
單元產生單元
1102
內容金鑰產生單元
1112
簽章金鑰儲存單元
1101
輸入單元

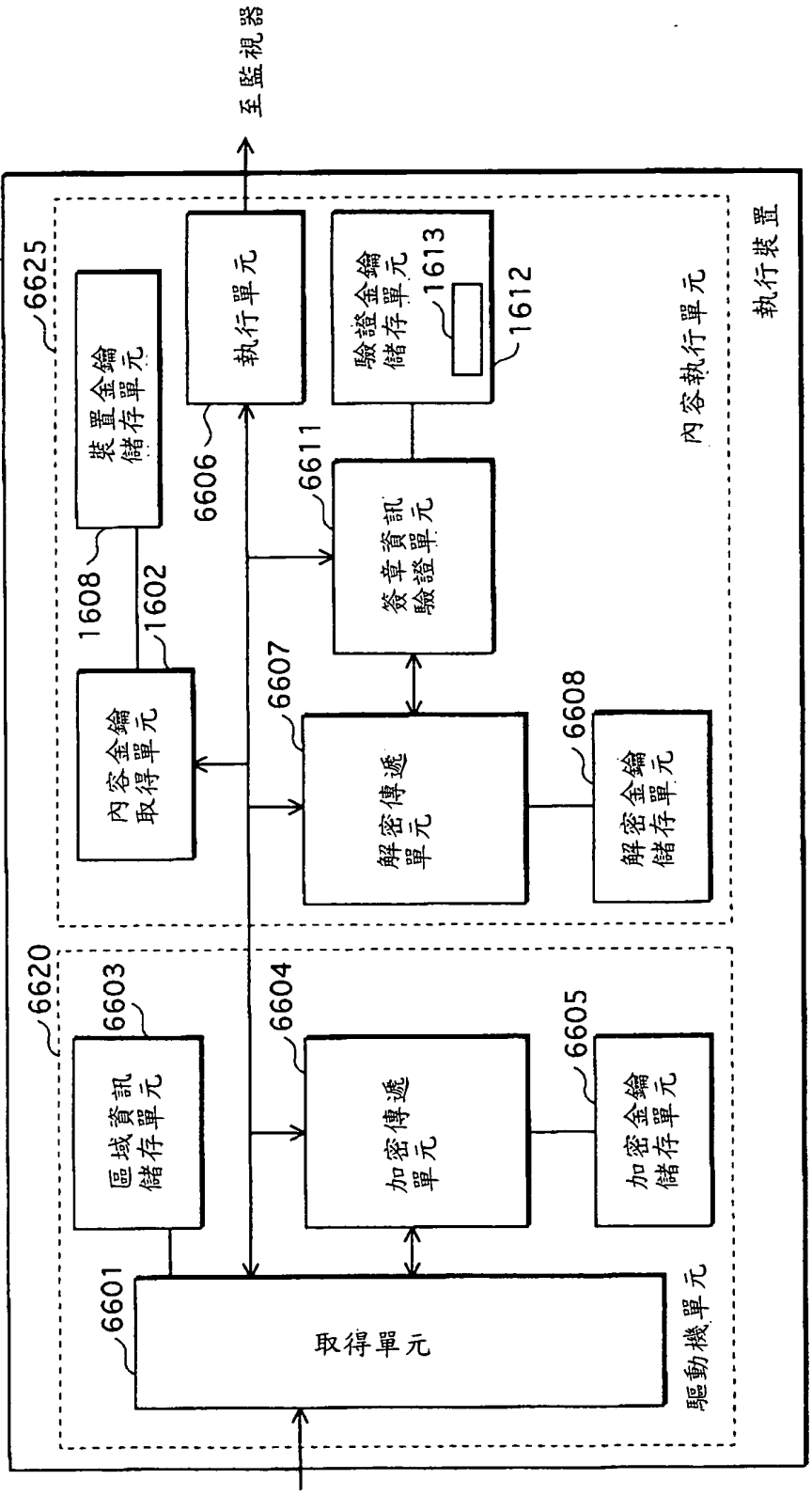
第 68 圖


6120
金鑰區塊
6121
單元資訊
6122
頭標資訊
6123
簽章資訊
6124
已加密內容
6125
區域資訊
6126

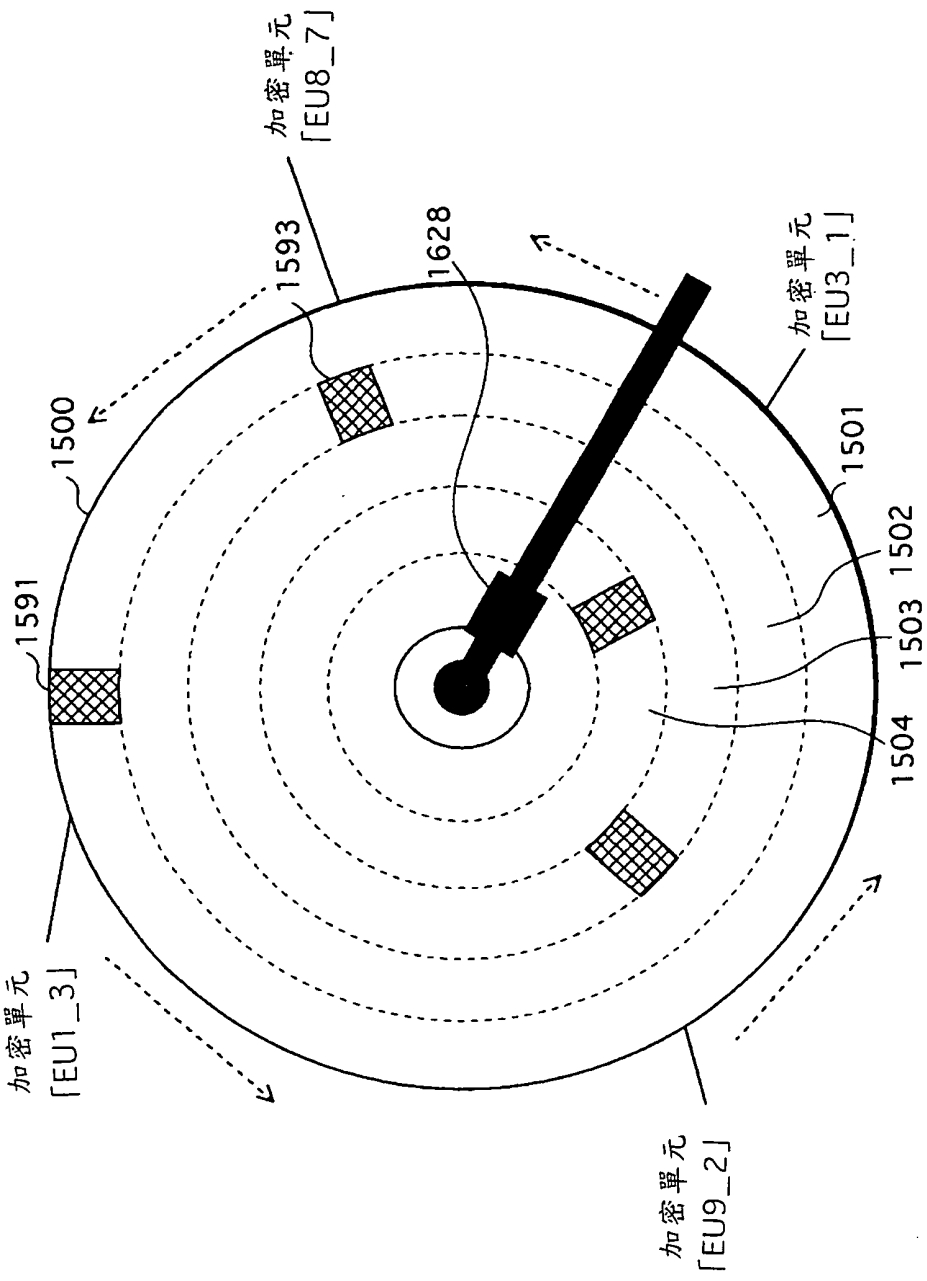
第 69 圖


6500
DVD
金鑰區塊
6510
單元檢選資訊
6530
頭標資訊
6550
區域資訊
6560
簽章資訊
6570
已加密內容
6580

第 70 圖


至監視器
6600
6625
裝置金鑰儲存單元
執行單元
驗證金鑰儲存單元
1613
1612
1608
1602
6606
6611
簽章資訊驗證單元
內容金鑰取得單元
6607
解密傳遞單元
6608
解密金鑰儲存單元
內容執行單元
執行裝置
6620
6603
6604
6605
區域資訊儲存單元
加密傳遞單元
加密金鑰儲存單元
6601
取得單元
驅動機單元

第 71 圖


加密單元
「EU8_7」
1593
1628
加密單元
「EU3_1」
1500
1501
1591
1502
1503
1504
加密單元
「EU1_3」
加密單元
「EU9_2」

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

1 未授權內容檢測系統

1100 分散裝置

1500 DVD

1600 執行裝置

1620 監視器

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

I364683

公告本

97年12月31日修正替換頁

發明專利分割說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96128187

※ 申請日期：94.3.29　　※IPC 分類：G06F 21/00 (2006.01)

原申請案號：94109886　　H04N 7/16 (2006.01)

一、發明名稱：（中文/英文）

未授權內容檢測系統(三) / Unauthorized Contents Detection System

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

松下電器產業股份有限公司 / PANASONIC CORPORATION

代表人：（中文/英文）

大坪文雄 / OHTSUBO, FUMIO

住居所或營業所地址：（中文/英文）

日本國大阪府門真市大字門真1006番地 / 1006, Oaza Kadoma, Kadoma-Shi, Osaka, 571-8501 Japan

國　籍：（中文/英文）

日本 / Japan

三、發明人：（共 9 人）

姓　名：（中文/英文）

1. 野仲　真佐男 / NONAKA, Masao
2. 布田　裕一 / FUTA, Yuichi
3. 中野　稔久 / NAKANO, Toshihisa
4. 横田　薫 / YOKOTA, Kaoru
5. 大森　基司 / OHMORI, Motoji
6. 宮崎　雅也 / MIYAZAKI, Masaya
7. 山本　雅哉 / YAMAMOTO, Masaya
8. 村瀬　薫 / MURASE, Kaoru
9. 小野田　仙一 / ONODA, Senichi

國　籍：（中文/英文）

日　本 / Japan

第 096128187 號申請案
100 年 12 月 16 日修正替換

十、申請專利範圍：

1. 一種資料產生裝置，其用於產生欲與一數位作品一同被寫入一記錄媒體之資料，該資料產生裝置包含：

一取得單元，其可運作以取得該數位作品；

一填充內容產生單元，其可運作以產生欲與該數位作品一同被寫入該記錄媒體之填充內容，該填充內容具有一資料大小，該記錄媒體上閒置空間的容量會因為該資料大小而變成小於或等於一預定量；

一頭標資訊產生單元，其可運作以產生記錄摘要值，該等記錄摘要值係由構成該數位作品之多個資料區塊與由構成該填充內容之多個資料區塊所產生；

一簽章資訊產生單元，其可運作以根據部份或全部該等多個記錄摘要值來產生簽章資料；以及

一寫入單元，其可運作以至少將該數位作品、該填充內容、該部份或全部之記錄摘要值、及該簽章資料寫入該記錄媒體。

2. 如申請專利範圍第1項之資料產生裝置，

其中，該填充內容產生單元產生不可由使用該數位作品之播放裝置所使用的填充內容。

3. 如申請專利範圍第1項之資料產生裝置，

其中該填充內容產生單元具有隨機數產生功能，並且產生包括有一所產生隨機數之該填充內容。

4. 如申請專利範圍第1項之資料產生裝置，其更包含：

一容量資訊取得單元，其可運作以取得有關指示可寫入

該記錄媒體的資料量之一最大記錄容量之資訊，

其中該填充內容產生單元至少根據該最大記錄容量及該數位作品之一資料大小來判定該填充內容之該資料大小。

5. 如申請專利範圍第4項之資料產生裝置，

其中該容量資訊取得單元經由該寫入單元取得已安裝記錄媒體之該最大記錄容量。

6. 如申請專利範圍第 1 項之資料產生裝置，其中前述取得單元、前述填充內容產生單元、前述頭標資訊產生單元、前述簽章資訊產生單元、及前述寫入單元形成於一積體電路上。

7. 一種用以利用錄製在記錄媒體上之數位作品的資料處理裝置，其中該記錄媒體同時錄製有：(i)具有一資料大小之填充內容，該記錄媒體上閒置空間的容量會因該資料大小而變為小於或等於一預定量；(ii)記錄摘要值，該等記錄摘要值係由構成該數位作品與該填充內容之多個資料區塊所產生；以及(iii)根據部分或全部的該等多個記錄摘要值產生的簽章資料，該資料處理裝置包含：

一使用單元，其可運作以使用該數位作品；

一選擇單元，其可運作以從該等多個資料區塊中隨機地選出一預定數量的資料區塊；

一計算單元，其可運作以由該等選出的資料區塊來計算一或多個計算摘要值；

一讀取單元，其可運作以讀取剩餘記錄摘要值，前述剩

餘記錄摘要值係在該等多個記錄摘要值中不包括與該計算出之計算摘要值對應之記錄摘要值；

一驗證單元，其可運作以藉著使用該簽章資料、該等計算摘要值與該等剩餘記錄摘要值，來驗證該數位作品與該填充內容之有效性；以及

一使用控制單元，其可運作以在該驗證單元判定出該數位作品與該填充內容中至少一種並不有效時，使該使用單元停止使用該數位作品。

8. 如申請專利範圍第7項之資料處理裝置，

其中該填充內容包括指示禁止播放資料之播放不可實行資訊，以及

該使用單元不會使用該數位作品中由該播放不可實行資訊所指示之部份。

9. 一種記錄媒體，其上記錄有：

一數位作品，

具有一資料大小之填充內容，該記錄媒體上閒置空間的容量會因該資料大小而變為小於或等於一預定量；

多個記錄摘要值，該等記錄摘要值係由構成該數位作品之多個資料區塊與由構成該填充內容之多個資料區塊所產生；以及

根據部分或全部的該等多個記錄摘要值而產生的簽章資料。

10. 一種使用於資料產生裝置之資料產生方法，該資料產生裝置產生欲與一數位作品一同被寫入一記錄媒體的資料，

該方法包含下列步驟：

取得步驟，係取得該數位作品；

填充內容產生步驟，係產生欲與該數位作品一同被寫入該記錄媒體的填充內容，該填充內容具有一資料大小，該記錄媒體上閒置空間的容量會因為該資料大小而變成小於或等於一預定量；

頭標資訊產生步驟，係產生記錄摘要值，該等記錄摘要值係由構成該數位作品之多個資料區塊與由構成該填充內容之多個資料區塊所產生；

簽章資訊產生步驟，係根據部份或全部之該等多個記錄摘要值來產生簽章資料；以及

寫入步驟，其用以至少將該數位作品、該填充內容、該部份或全部之記錄摘要值、及該簽章資料寫入該記錄媒體。

11. 一種電腦可讀取記錄媒體，其記錄有使用於資料產生裝置之資料產生程式，該資料產生裝置產生欲與一數位作品一同被寫入一記錄媒體的資料，該資料產生程式會使該資料產生裝置執行下列步驟：

取得步驟，係取得該數位作品；

填充內容產生步驟，係產生欲與該數位作品一同被寫入該記錄媒體的填充內容，該填充內容具有一資料大小，該記錄媒體上閒置空間的容量會因為該資料大小而變成小於或等於一預定量；

頭標資訊產生步驟，係產生記錄摘要值，該等記錄摘要值係由構成該數位作品之多個資料區塊與由構成該填充內

容之多個資料區塊所產生；

簽章資訊產生步驟，係根據部份或全部之該等多個記錄摘要值來產生簽章資料；以及

寫入步驟，其用以至少將該數位作品、該填充內容、該部份或全部之記錄摘要值、及該簽章資料寫入該記錄媒體。