

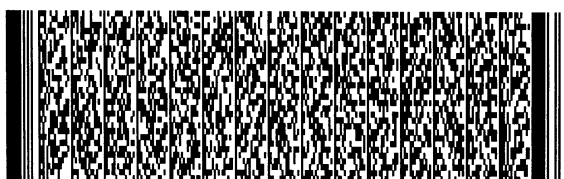
申請日期: 91.4.15	案號: 91107604
類別: 6092 400	

(以上各欄由本局填註)

發明專利說明書

583614

一、 發明名稱	中文	著作權保護系統及其方法
	英文	COPYRIGHT PROTECTION SYSTEM AND METHOD THEREOF
二、 發明人	姓名 (中文)	1. 森下卓也 2. 宮內宏 3. 峯松一彦 4. 尾花賢
	姓名 (英文)	1. Takuya MORISHITA 2. Hiroshi MIYAUCHI 3. Kazuhiko MINEMATSU 4. Satoshi OBANA
	國籍	1. 日本 2. 日本 3. 日本 4. 日本
	住、居所	1. 日本國東京都港區芝五丁目7番1號 日本電氣股份有限公司內 2. 日本國東京都港區芝五丁目7番1號 日本電氣股份有限公司內 3. 日本國東京都港區芝五丁目7番1號 日本電氣股份有限公司內 4. 日本國東京都港區芝五丁目7番1號 日本電氣股份有限公司內
三、 申請人	姓名 (名稱) (中文)	1. 日本電氣股份有限公司
	姓名 (名稱) (英文)	1. NEC Corporation(日本電氣株式会社)
	國籍	1. 日本
	住、居所 (事務所)	1. 日本國東京都港區芝五丁目7番1號
	代表人 姓名 (中文)	1. 西垣浩司
	代表人 姓名 (英文)	1. Koji NISHIGAKI



本案已向

國(地區)申請專利	申請日期	案號	主張優先權
日本 JP	2001/04/19	2001-121061	有

有關微生物已寄存於	寄存日期	寄存號碼
-----------	------	------

無



五、發明說明 (1)

發明之領域

本發明係關於一著作權保護系統及其方法，用來藉由加密以保護一廣播或類似物所提供之作品之著作權。

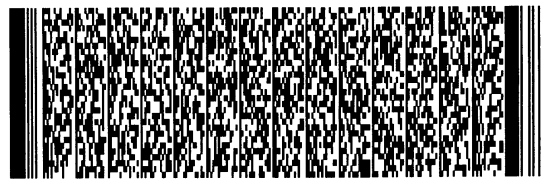
發明之背景

第3圖為一習知著作權保護系統之示意圖。第3圖所顯示之著作權保護系統係用來保護記錄於DVD上之作品之著作權。在販售記錄於DVD上之作品時，為了防止作品被惡意的第三方非法使用，會將作品資料，例如影像和聲音，加密之後，再記錄於DVD中。再者，用來解密所記錄資料之磁碟鑰匙與標題鑰匙係被加密並且記錄於DVD中。

習知著作權保護系統包含一DVD讀取裝置21、一匯流排22、一匯流排認證部分23、一萬用鑰匙24、一磁碟鑰匙解碼部分25，一標題鑰匙解碼部分26、一解變頻部分27，以及一MPEG解碼器28。DVD讀取裝置21、匯流排認證部分23以及解變頻部分27係分別連接至匯流排22，而資料傳輸可以經由匯流排22發生。匯流排認證部分23與解變頻部分27會藉由DVD讀取裝置21，經由匯流排22，取得從DVD讀取出之資料。

以下將說明上述之習知著作權保護系統之操作。

首先，匯流排認證部分23會藉由匯流排22與DVD讀取裝置21進行相互認證，並且係共用一時間-變化鑰匙，用來經由匯流排22傳送一鑰匙。接下來，匯流排認證部分23會藉由DVD讀取裝置21，從DVD讀取並且取得被加密的磁碟鑰匙與標題鑰匙，並且提供磁碟鑰匙至磁碟鑰匙解碼部分



五、發明說明 (2)

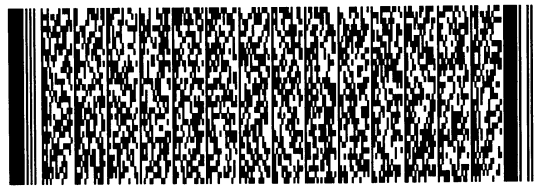
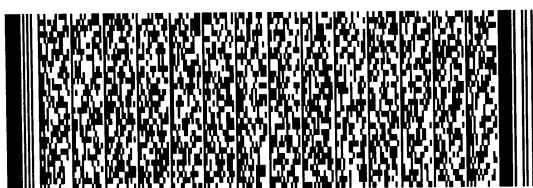
25，並且提供標題鑰匙至標題鑰匙解碼部分26。磁碟鑰匙解碼部分25會藉由萬用鑰匙24，解碼磁碟鑰匙之密碼程式，並且解碼磁碟鑰匙。標題鑰匙解碼部分26會從磁碟鑰匙解碼部25，取得被解碼的磁碟鑰匙，並且解密標題鑰匙之密碼程式，藉由磁碟鑰匙，並且解碼標題鑰匙，並且提供標題鑰匙至解變頻部分27。

再者，藉由標題鑰匙，解變頻部分20會解密來自DVD之作品之被加密資料之密碼編譯程序，藉由DVD讀取裝置21，並且將其輸出至MPEG解碼器28。MPEG解碼器28會再產生影像或聲音，藉由使用密碼編譯程序所解碼之資料。

如上所述，在習知著作權保護系統，會提供記錄於DVD之磁碟鑰匙以及用來解密標題鑰匙之萬用鑰匙，而其構造會造成，在沒有萬用鑰匙的情況下，磁碟鑰匙與標題鑰匙無法被解碼，而記錄於DVD之作品資料之密碼編譯程序也無法被解碼。再者，因為在匯流排22上傳送之資料係被加密，即使資料係從匯流排22取得，從該資料，很難取得作品資料，其可以被再產生。

因此，習知著作權保護系統會防止作品被惡意的第三方非法使用。

再者，上述之著作權保護系統可以提供一處理裝置，能夠執行程式，而此處理裝置可以執行一程式，以分別實現部分23與25至28之各別功能，以建立各別之部分23與25至28。因此，可能提供給第3圖之著作權保護系統一資訊處理裝置，例如一個人電腦。



五、發明說明 (3)

然而，在上述之習知著作權保護系統中，在惡意之第三方藉由分析程式而破解認證方法或加密方法的情況下，難以改變複數個鑰匙(萬用鑰匙)以及相關於正在使用之著作權保護系統密碼編譯程序之程式，而無法防止對作品之非法使用。

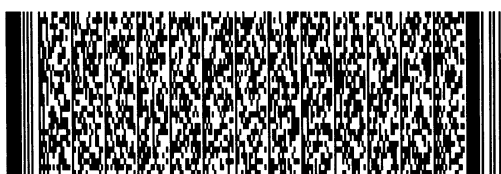
因此，在認證方法或加密方法被破解且作品被非法使用之情況下，必須建立著作權保護系統，其可以使相關於著作權保護系統密碼編譯程序之鑰匙失效，並且防止進一步的非法使用。

此外，關於作品之著作權保護，例如經由廣播來提供之廣播節目之影像與聲音，無法產生對應於記錄與再產生之反測量，而必須建立著作權保護系統，其可以執行關於紀錄與再產生之著作權保護。

發明之概述

因此，經由考量這些情況，本發明之目的在於提供一著作權保護系統及其方法，其可以使相關於系統本身之密碼編譯程序之鑰匙失效。此外，本發明之目的在於提供一著作權保護程式，用來藉由使用電腦來實現著作權保護系統。

此外，本發明之目的在於提供一著作權保護系統及其方法，其可以輕易地改變相關於在複數個著作權保護系統中之密碼編譯程序之鑰匙或程式。此外，本發明之目的在於提供一著作權保護程式，用來藉由使用電腦來實現著作權保護系統。



五、發明說明 (4)

此外，本發明之目的在於提供一著作權保護系統及其方法，其可以執行相關於記錄與再產生之著作權保護。此外，本發明之目的在於提供一著作權保護程式，用來藉由使用電腦來實現著作權保護系統。

為了解決上述之任務，第一發明係為一著作權保護系統，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，而其特徵在於：該系統包含認證裝置，具有關於密碼編譯程序之鑰匙之無效資訊，並且用來否決認證，在認證鑰匙之資訊是包含於該無效資訊中之情況下，其係用來認證，當第一加密裝置與第一解密裝置係共用關於加密之第一密碼鑰匙時；以及無效資訊更新裝置，用來更新該無效資訊之內容，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

第二發明之特徵在於：該系統包含認證鑰匙更新裝置，用來更新該認證鑰匙，當接收到用來更新之認證鑰匙時，其係與該輸入資料一起被提供。

第三發明之特徵在於：該系統包含一處理裝置，用來執行一處理程式，以實現相關於該加密之解密之功能，而該處理裝置會更新該處理程式，當接收到用來更新之程式時，其係與該輸入資料一起被提供。

第四發明之特徵在於：該系統包含第二加密裝置，用來加密該輸入資料，藉由使用一第二密碼鑰匙，並且記錄該第二密碼資料於一記錄媒體。

第五發明之特徵在於：該系統包含第二解密裝置，用



五、發明說明 (5)

來藉由該第二密碼鑰匙，解密該第二密碼資料之密碼編譯程序，而該第二密碼鑰匙係包含於該系統本身。

第六發明係為在一著作權保護系統之一著作權保護方法，用來加密相關於一作品之一輸入資料，進而保護該作品之著作權，其特徵在於該方法包含下列步驟：進行認證，當第一加密裝置和第一解密裝置係共用關於該加密之第一密碼鑰匙時；否決該認證，在用來認證之認證鑰匙之資訊是包含於在關於密碼編譯程序之鑰匙中之無效資訊中之情況下；以及更新該無效資訊之內容，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

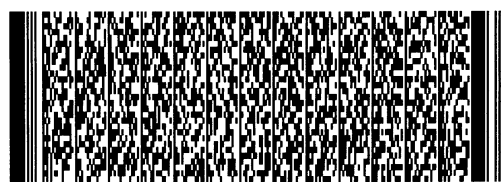
第七發明之特徵在於該方法另包含下列步驟：當接收到用來更新之認證鑰匙時，其係與該輸入資料一起被提供，更新該認證鑰匙。

第八發明之特徵在於該方法另包含下列步驟：接收用來更新之程式，其係與該輸入資料一起被提供，並且更新用來實現相關於該加密之解密功能之處理程式，藉由該用來更新之程式。

第九發明之特徵在於該方法另包含下列步驟：加密該輸入資料，藉由使用一第二密碼鑰匙，並且記錄該第二密碼資料於一記錄媒體中。

第十發明之特徵在於該方法另包含下列步驟：將該第二密碼鑰匙存放於該系統中，並且藉由該第二密碼鑰匙，解密該第二密碼資料之密碼編譯程序。

第十一發明係為一著作權保護程式，用來在一著作權



五、發明說明 (6)

保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，而其特徵在於：該程式使得一電腦執行處理，用來進行認證，當第一加密裝置和第一解密裝置係共用關於該加密之第一密碼鑰匙時；執行處理，用來否決該認證，在用來認證之認證鑰匙之資訊是包含於在關於密碼編譯程序之鑰匙中之無效資訊中之情況下；以及執行處理，用來更新該無效資訊之內容，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

第十二發明之特徵在於：該程式另使得該電腦執行處理，用來加密該輸入資料，利用一第二密碼鑰匙，並且執行處理，用來記錄該第二密碼資料於一記錄媒體中。

第十三發明之特徵在於：該程式另使得該電腦執行處理，用來將該第二密碼鑰匙存放於該系統中，並且執行處理，用來解密該第二密碼資料之密碼編譯程序，藉由該第二密碼鑰匙。

第十四發明係為一著作權保護程式，用來在一著作權保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，而其特徵在於：該程式使得一電腦執行處理，用來接收用於更新之認證鑰匙，其係與該輸入資料一起被提供，並且更新該認證鑰匙。

第十五發明之特徵在於：該程式另使得該電腦執行處理，用來接收用於更新之程式，其係與該輸入資料一起被



五、發明說明 (7)

提供，並且執行處理，用來更新用於實現相關於該加密之解密之功能之處理程式，藉由該用於更新之程式。

第十六發明係為一記錄媒體，其中存放一著作權保護程式，用來在一著作權保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，其特徵在於：該程式使得一電腦執行處理，用來進行認證，當第一加密裝置和第一解密裝置係共用關於該加密之第一密碼鑰匙時；執行處理，用來否決該認證，在用來認證之認證鑰匙之資訊是包含於在關於密碼編譯程序之鑰匙中之無效資訊中之情況下；以及執行處理，用來更新該無效資訊之內容，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

第十七發明之特徵在於：該程式另使得該電腦執行處理，用來加密該輸入資料，利用一第二密碼鑰匙，並且執行處理，用來記錄該第二密碼資料於一記錄媒體中。

第十八發明之特徵在於：該程式另使得該電腦執行處理，用來將該第二密碼鑰匙存放於該系統中，並且執行處理，用來解密該第二密碼資料之密碼編譯程序，藉由該第二密碼鑰匙。

第十九發明係為一著作權保護程式，用來在一著作權保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，其特徵在於：該程式使得一電腦執行處理，用來接收用於更新之認證鑰匙，其係與該輸入資料一起被提供，並且更新該認證鑰



五、發明說明 (8)

匙。

第二十發明之特徵在於：該程式另使得該電腦執行處理，用來接收用於更新之程式，其係與該輸入資料一起被提供，並且執行處理，用來更新用於實現相關於該加密之解密之功能之處理程式，藉由該用於更新之程式。

藉由這些著作權保護程式，上述之著作權保護系統可以藉由使用一電腦來實現。

發明之詳細說明

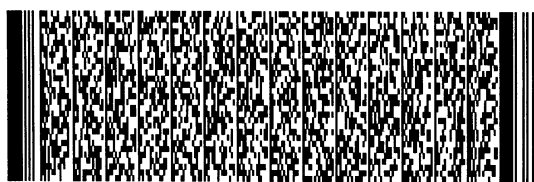
配合下列圖示，以下將說明本發明之實施例。

第1圖為本發明實施例之著作權保護系統之方塊圖。

在此圖中，代碼1是一廣播接收裝置，用來接收一廣播信號。此廣播信號包含一影像資料或一聲音資料，其係經過壓縮與編碼，並且加密(以下將稱為經壓縮之加密資料)。經過加密，只有具有收取權利的人才可以觀看與收聽。此外，上述之廣播信號可以經由一無線電廣播來傳送，例如，電視與收音機，也可為有線廣播，例如，有線電視，或可以經由一通訊網路來傳送，例如，有線電話網路、無線電電話網路和網際網路。

代碼2是一廣播解密裝置，用來解密經壓縮之加密資料之密碼編譯程序，經壓縮之加密資料係由廣播接收裝置來接收，並且輸出一影像資料或一聲音資料，其係經過壓縮與編碼(以下將稱為經壓縮資料)。

代碼3係為一第一加密裝置，用來藉由一第一密碼鑰



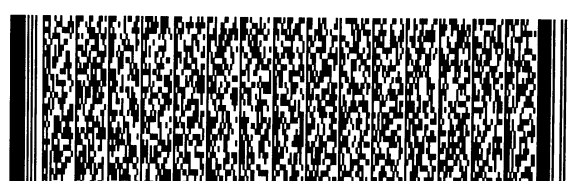
五、發明說明 (9)

匙來加密經壓縮資料，該資料係從廣播解密裝置2輸出，並且輸出一第一密碼資料A1。代碼4係為一認證裝置，用來產生該第一密碼鑰匙，並且將其提供至第一加密裝置3，並且藉由一認證鑰匙，加密第一密碼鑰匙，並且輸出該經加密之第一密碼鑰匙，在根據該認證鑰匙完成相互認證之情況下。此認證裝置4具有一證明撤銷列表D1，其中描述有效認證鑰匙之資訊，並且否決該認證，在用來相互認證之認證鑰匙之資訊是包含於證明撤銷列表D1中之情況下。代碼5係一證明撤銷列表更新裝置，用來更新認證裝置4之證明撤銷列表D1，當從廣播接收裝置1接收到即將無效之物件之認證鑰匙資訊時，其係包含於該廣播信號中。

代碼6係為一處理裝置，其包含一記憶體與中心處理器或相似物，並且用來實現其功能，藉由裝載一程式於記憶體中，並且執行它。此處理裝置6會執行一程式，以實現第一解密部分11、聲音/影像解碼部分12、認證部分13以及認證鑰匙更新部分14之個別功能。

第一解密部分11會接收第一密碼資料A1，並且藉由用來加密之第一密碼鑰匙，解碼密碼編譯程序。聲音/影像解碼部分12會接收經壓縮之資料，其中密碼編譯程序係藉由第一解密部分11來解密，並且應用延伸處理至此資料。藉由此延伸處理，經壓縮之資料會變成可以再產生之影像資料與聲音資料。聲音/影像解碼部分12可以發生被解碼的影像資料和聲音資料之再產生處理。

認證部分13會傳送與接收資料A2至/從認證裝置4，並



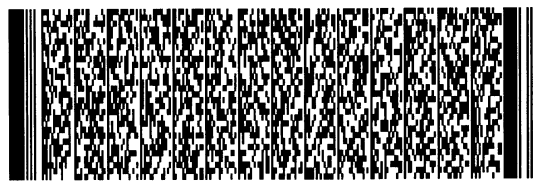
五、發明說明 (10)

且發生相互認證，並且根據認證之完成，從認證裝置4取得第一密碼鑰匙，以被使用於第一解密部分11。此認證部分13具有一認證鑰匙，以被使用於與認證裝置4之相互認證。認證鑰匙更新部分14會更新認證部分13之認證鑰匙，當接收到來自廣播接收裝置1之用來更新之認證鑰匙，其係包含於廣播信號。再者，當接收到來自廣播接收裝置1之用來更新之程式時，此程式係包含於廣播信號中，認證鑰匙更新部分14會更新第一解密部分11、聲音/影像解碼部分12、認證部分13以及部分14之個別程式(第一解密處理程式、聲音/影像解碼處理程式、認證處理程式以及認證鑰匙更新處理程式)。

代碼7係為一第二加密裝置，用來加密來自廣播解密裝置2之經壓縮資料，藉由使用一第二密碼鑰匙，並且輸出一第二密碼資料B1。第二加密裝置7存放有用來加密之第二密碼鑰匙。代碼8係為一第二解密裝置，用來從第二加密裝置7接收用來加密之第二密碼鑰匙，並且解密此密碼編譯程序。

代碼9係為一記錄裝置，當接收到來自第二加密裝置7之第二密碼資料B1時，用來將其記錄於一記錄媒體中。記錄裝置9可為一硬碟機、一光學磁性磁碟裝置，或一讀寫裝置等等。

此外，一輸入裝置、一顯示裝置，以及一擴音機等等(未顯示)係被連接至上述之處理裝置6，以作為週邊裝置。在此，輸入裝置係指一輸入裝置，例如一鍵盤與一滑



五、發明說明 (11)

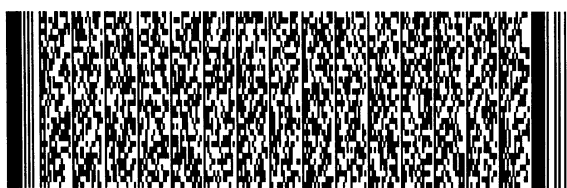
鼠。顯示裝置係指一陰極射線管(CRT)、一液晶顯示裝置或類似物。處理裝置6可為一資訊處理裝置，例如一個人電腦與一行動資訊終端機。

再者，上述之裝置1至5、7與8可以組合成一個裝置。例如，一電子電路，用來實現裝置1至5、7與8之個別功能，其安裝於一基底上，並且係被連接至處理裝置6與記錄裝置9。因此，藉由將基底安裝於資訊處理裝置，例如一個人電腦，可以建立第1圖之著作權保護系統。

此外，上述之裝置3至5、7與8可以藉由一專用硬體。再者，這些裝置3至5、7與8可包含一記憶體與一中心處理器，並且藉由存放一程式於記憶體中並且執行它，以實現裝置3至5、7與8之個別功能。在藉由使用具有中央處理器之電腦來實現各功能之情況下，如果程式係存放於一專用記憶體(ROM)，用來讀取，其可以防止此程式被偽造。否則，這些裝置3至5、7與8可以被建立，藉由一大規模積體電路(一系統大規模積體電路，a system LSI)，其具有一中心處理器與記憶體。

再者，以下將描述第1圖之著作權保護系統之操作。一開始，將先描述接收廣播信號與再產生廣播內容之操作。首先，當接收廣播信號時，廣播接收裝置1會輸出經壓縮之加密資料，而廣播解密裝置會2解密其密碼編譯程序，並且輸出經壓縮之資料。

再者，當接收到來自廣播解密裝置2之經壓縮資料時，第一加密裝置3會進行加密，藉由使用認證裝置4所提



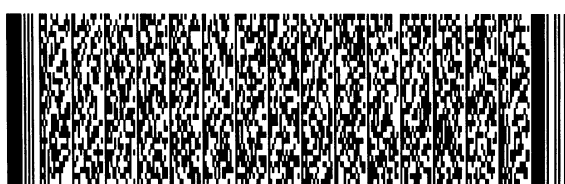
五、發明說明 (12)

供之第一密碼鑰匙，並且輸出第一密碼資料A1。在此所使用的第一密碼鑰匙係為一與處理裝置6共用的鑰匙。此外，以下將描述共用此第一密碼鑰匙之操作。

再者，當接收到來自第一加密裝置3之第一密碼資料A1時，處理裝置6之第一解密部分11會解碼此密碼編譯程序，藉由使用與第一加密裝置3共享之第一密碼鑰匙。當接收到密碼編譯程序係由第一解密部分13來解碼之經壓縮資料時，聲音/影像解碼部分12會進行延伸處理，並且再產生一影像或聲音。

如上所述，在此實施例中，由於從第一加密裝置3輸出至處理裝置6之資料(第一密碼資料A1)係被加密，即使資料係從一傳輸媒體取得(一匯流排或其他可以傳送資料之相似物)，其將第一加密裝置3連接至處理裝置6，也難以取得作品之資料，其可以從資料被再產生。

再者，配合參考第2圖，將說明共用上述之第一密碼鑰匙之操作。雖然，第一密碼鑰匙之共用處理係發生於認證裝置4與認證部分13之間，但是，認證裝置會同時與認證部分13進行相互認證，根據認證鑰匙。第2圖為第一密碼鑰匙之共用處理之流程圖。第2圖亦顯示一範例，其中第一密碼鑰匙係經由相互認證來共用，藉由使用一公共鑰匙密碼方法。如第2圖所示，認證裝置4具有一公共鑰匙p1、一公共鑰匙證明c1、一秘密鑰匙e1、證明撤銷列表D1，以及一公共鑰匙pc。再者，認證部分13具有一公共鑰匙p2、一公共鑰匙證明c2、一秘密鑰匙s2，以及一公共鑰



五、發明說明 (13)

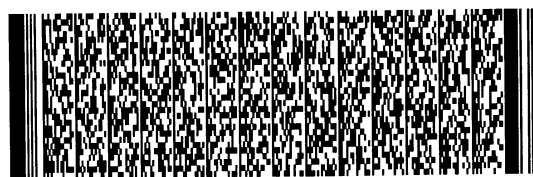
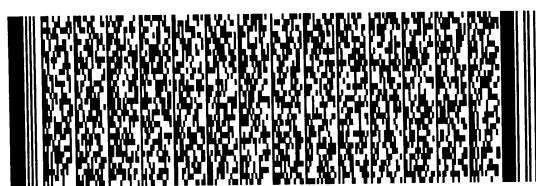
匙pc。

上述之公共鑰匙證明c1係由一第三方組織(認證機關)來發布，其中簽名係預先被加入至公共鑰匙p1中，藉由第三方組織(認證機關)所擁有的一秘密鑰匙sc，而此簽名係由公共鑰匙pc來核對。同樣地，公共鑰匙證明c2係由一第三方組織來發布，其中簽名係預先被加入至公共鑰匙p2中，藉由秘密鑰匙sc，而此簽名係由公共鑰匙pc來核對。藉由這些簽名，可以避免公共鑰匙證明c1與c2遭到偽造。

公共鑰匙p1和秘密鑰匙s1係一對認證鑰匙。同樣地，公共鑰匙p2與秘密鑰匙s2也是一對認證鑰匙。此外，上述之公共鑰匙p2和秘密鑰匙s2是其中一對認證鑰匙，用來在認證裝置4和認證部分13之間的相互認證，並且成為相關於第一密碼鑰匙加密之鑰匙，該加密係由認證裝置4來執行。

再者，在證明撤銷列表D1中，必須具有顯示一無效公共鑰匙證明c2之資訊。再者，對此證明撤銷列表D1而言，為了避免為造，秘密鑰匙sc會加入簽名，此鑰匙係第三方組織所擁有並且發佈。

首先，認證裝置4會產生一隨機號碼R1，並且將其傳送至認證部分13(第2圖中之步驟SP1和SP2)。再者，認證部分13會藉由秘密鑰匙s2產生一簽名Sig(s2, R1 || ID2)至被接收的隨機號碼R1。在產生簽名Sig(s2, R1 || ID2)時，公共鑰匙證明c2之序列號碼可以作為號碼ID2。此外，認證部分13會產生一隨機號碼R2。再者，認證部分



五、發明說明 (14)

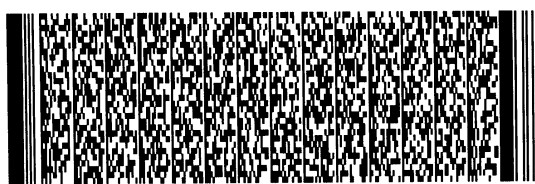
13 會傳送所產生的簽名 $\text{Sig}(s2, R1 \parallel ID2)$ 、公共鑰匙證明 $c2$ 和隨機號碼 $R2$ 至認證裝置4 (第2圖之步驟SP3至SP5)。

此外，上述之符號 " $\parallel$ " 係表示位元的連接。例如，" $R1 \parallel ID2$ " 係表示位元序列，其中隨機號碼 $R1$ 與號碼 $ID2$ 係相互連接之位元，而簽名 $\text{Sig}(s2, R1 \parallel ID2)$ 係位元序列，其中簽名係藉由秘密鑰匙 $s2$ 被加入至位元序列 " $R1 \parallel ID2$ "。

再者，熱量雜訊可以使用於上述之隨機號碼 $R1$ 和 $R2$ ，或一擬似隨機號碼可以被使用。然而，在使用擬似隨機號碼的情況下，雖然，擬似隨機號碼產生器可以分別被提供於認證裝置4和認證部分12，其要求這些擬似隨機產生器彼此不一致。

再者，認證裝置4會核對被接收的公共鑰匙證明 $c2$ 未被描述於證明撤銷列表 $D1$ 中。在此，在被接收的公共鑰匙證明 $c2$ 係被描述於證明撤銷列表 $D1$ 中的情況下，認證裝置4會決定該公共鑰匙 $p2$ 是無效的，並且利用認證部分13否決該認證，並且結束未完成認證的處理。在另一方面，在被接收的公共鑰匙證明 $c2$ 未被描述於證明撤銷列表 $D1$ 中的情況下，認證裝置4會繼續相互認證，並且執行下面的處理(第2圖之步驟SP6)。

再者，認證裝置4會藉由公共鑰匙 p_c 核對公共鑰匙，並且藉由公共鑰匙 $p2$ 與隨機號碼 $R1$ 核對簽名 $\text{Sig}(s2, R1 \parallel ID2)$ 。在此，當核對的結果係反常的，認證裝置4會連



五、發明說明 (15)

同認證部分13否決此認證，並且結束未完成認證的處理（第2圖之步驟SP7和SP8）。

另一方面，如果所有核對結果都是正常的，認證裝置4會藉由秘密鑰匙s1產生一簽名Sig (s1, R2 II ID1)至隨機號碼R2。在產生此簽名Sig (s1, R2 II ID1)時，公共鑰匙證明c1之序列號碼可以用於號碼ID1。

再者，認證裝置4會產生一第一密碼鑰匙K1，並且加密此第一密碼鑰匙K1，藉由公共鑰匙p2，以產生一密碼編譯程序Enc (p2, K1)。再者，認證裝置4會提供所產生的第一密碼鑰匙K1至第一加密裝置3。再者，認證裝置4會傳送簽名Sig (s1, R2 II ID1)，公共鑰匙證明c1與密碼編譯程序Enc(p2, K1)至認證部分1（第2圖之步驟SP10至SP12）。

再者，認證部分13會核對所接收的公共鑰匙證明c1，藉由公共鑰匙pc。再者，它會核對簽名Sig (s1, R2 II ID1)，藉由公共鑰匙p1和隨機號碼R2。在此，當其中一個核對的結果係反常的，認證裝置4會連同認證部分13否決此認證，並且結束未完成認證的處理（第2圖之步驟SP13和SP14）。

另一方面，如果所有核對結果都是正常的，認證部分13會藉由秘密鑰匙s2解碼密碼編譯程序Enc (p2, K1)，並且獲得第一密碼鑰匙K1，並且提供此第一密碼鑰匙K1至第一解密部分11（第2圖之步驟SP15）。因此，第一加密裝置3和第一解密部分11會共用認證裝置4所產生的第一密碼鑰



五、發明說明 (16)

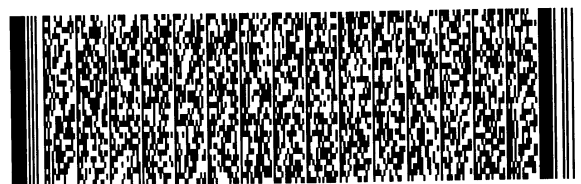
匙K1。

此外，在上述之實施例中，雖然t1 20 在第一密碼鑰匙之共用處理中之認證係透過相互確認來執行，利用公共鑰匙密碼方法，認證方法並不限於此公共鑰匙密碼方法。

再者，以下將說明使認證部分13之認證鑰匙無效之操作。即將無效的物件之認證鑰匙係為其中一個認證鑰匙，用來在認證裝置4和認證部分13之間進行相互認證，並且成為相關於第一密碼鑰匙之加密之鑰匙，此加密係由認證裝置4來執行。在上述藉由公共鑰匙密碼方法來執行之相互認證之範例中，顯示於第2圖中，其係由公共鑰匙p2和秘密鑰匙s2來表示。

有一種情況，其中懷有惡意的第三方會非法取得在第1圖之著作權保護系統中之認證部分13的認證鑰匙，並且利用認證鑰匙，與認證裝置4共用第一密碼鑰匙，並且解密第一密碼資料A1之密碼編譯程序，並且非法使用作品，例如廣播節目的影像和聲音。在這種情況下，為了防止對作品的非法使用，廣播事業經營者會廣播，以包含在廣播信號中即將無效之物件之認證鑰匙資訊以及用於更新之認證鑰匙。以下將說明第1圖之著作權保護系統之操作。

當即將無效之物件之認證鑰匙資訊係包含於被接收的廣播信號中時，廣播接收裝置1會輸出資訊至證明撤銷列表更新裝置5。當從廣播接收裝置1接收到即將無效之物件之認證鑰匙資訊時，證明撤銷列表更新裝置5會更新認證裝置4的證明撤銷列表D1。因此，認證部分13之認證鑰匙



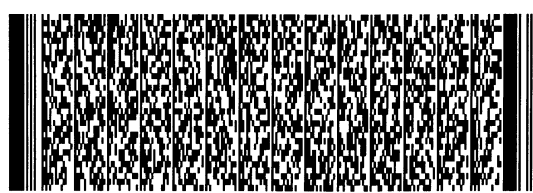
五、發明說明 (17)

會無效。

再者，當用於更新之認證鑰匙係包含於被接收的廣播信號中，廣播接收裝置1會輸出用於更新之認證鑰匙至處理裝置6之認證鑰匙更新部分14。當接收到來自廣播接收裝置1之用於更新之認證鑰匙時，認證鑰匙更新部分14會更新認證部分13的認證鑰匙。因此，認證部分13之認證鑰匙會成為一有效的認證鑰匙。

因此，在懷有惡意的第三方藉由非法取得的認證鑰匙使用一作品之情況下，由於已經無效的認證鑰匙係被使用於在認證裝置4和認證部分13之間共用第一密碼鑰匙，在上述步驟SP6中，確認裝置4會否決與認證部分13的相互認證，並且不提供第一密碼鑰匙至認證部分13。因此，第一解密部分11不會獲得第一密碼鑰匙，其係被第一加密裝置3用來加密，並且變得無法解密第一密碼資料A1的密碼編譯程序。因此，即使認證方法和加密方法係被解密，而作品係被懷有惡意的第三方非法使用，認證鑰匙(關於密碼編譯程序之鑰匙)會無效，而可以避免作品的非法使用。

再者，如上所述，根據此實施例之著作權保護系統，藉由即將無效之物件之認證鑰匙資訊與用於更新之認證鑰匙，其係包含並且被提供於廣播信號中，認證鑰匙之無效與改變會發生。因此，為了防止非法使用作品，如果廣播事業經營者僅是廣播，以包含在廣播信號中即將無效之物件之認證鑰匙資訊以及用於更新之認證鑰匙，認證鑰匙的無效與改變可以簡單地被建立。



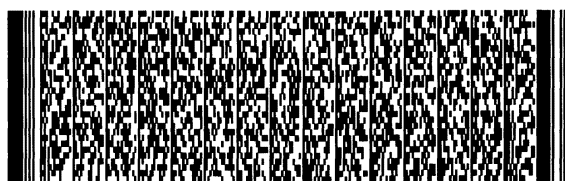
五、發明說明 (18)

如果關於密碼編譯程序之鑰匙（認證鑰匙）之無效與改變會被執行，藉由即將無效之物件之認證鑰匙資訊與用於更新之認證鑰匙，其係與輸入資料一起被提供，此輸入資料係關於一廣播作品，例如一影像資料和聲音資料，其可能使得關於密碼編譯程序之鑰匙之無效與改變，突然發生於複數個著作權保護系統，其中關於該作品之輸入資料會被使用。因此，可以有效地防止作品的非法使用。

再者，廣播事業經營者可以廣播，以包含一用於更新之程式於廣播信號中，其可以更新處理裝置6之第一解密部分11、聲音/影像解碼部分12、認證部分13和認證鑰匙更新部分14之各自的處理程式（第一解密處理程式、聲音/影像解碼處理程式、認證處理程式、一認證鑰匙更新處理程式）。在這種情況下，廣播接收裝置1會輸出用來更新之被接收的程式至認證鑰匙更新部分14，而認證鑰匙更新部分14會更新各自的處理程式，藉由用於更新之程式。如果在處理裝置6中之處理程式係被更新，即使在該處理程式被非法偽造與使用的情況下，其可以進一步防止被偽造的處理程式的非法使用。

再者，將說明一操作，其中第1圖之著作權保護系統會接收廣播信號，並且記錄廣播的內容，並且再產生被記錄的廣播內容。首先，當接收到廣播信號時，廣播接收裝置1會輸出經壓縮的加密資料，而廣播解密裝置2會解密此密碼編譯程序，並且輸出經壓縮資料。

再者，當接收到來自廣播解密裝置2之經壓縮資料，

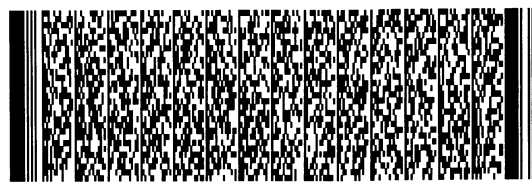
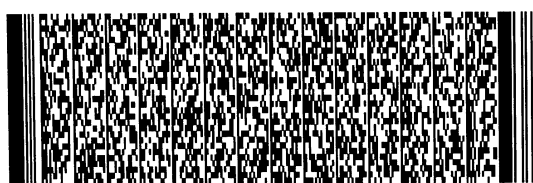


五、發明說明 (19)

第二加密裝置7會執行加密，藉由使用第二密碼鑰匙，並且輸出第二密碼資料B1。每當執行加密時，第二加密裝置7會藉由使用隨機號碼或類似物，產生第二密碼鑰匙，並且將其存放於裝置7中。當接收到來自第二加密裝置7之第二密碼資料B1時，記錄裝置9會將其記錄於一記錄媒體中。

當被記錄的資料被再產生時，首先記錄裝置9會從記錄媒體讀取第二密碼資料B2，並且將其輸出。當接收到第二密碼資料B2時，第二解密裝置8會從第二加密裝置7取得用來加密之第二密碼鑰匙，並且解密第二密碼資料B2之密碼編譯程序，並且將其輸出至第一加密裝置3。再者，在經過關於上述藉由第一密碼鑰匙之加密處理之後，記錄裝置9所記錄的廣播內容會藉由聲音/影像解碼部分12來再產生。

此外，在上述實施例中，作為提供第二密碼鑰匙至第二解密裝置8之方法，雖然每當執行加密時，第二加密裝置7會產生第二密碼鑰匙，藉由使用一隨機號碼或類似物，並且將第二密碼鑰匙存放於裝置7中，而第二密碼鑰匙可以由記錄裝置9來記錄。然而，在這種情況下，其要求被記錄的第二密碼鑰匙可以僅被使用於此系統中。例如，特定於每一第二加密裝置7之不同的辨識號碼 (identification numbers, IDs) 和第二密碼鑰匙之預定計算結果會被加入至第二密碼資料B1並且被記錄。在這種情況下，第二解密裝置8會從第二加密裝置7取得其辨識號



五、發明說明 (20)

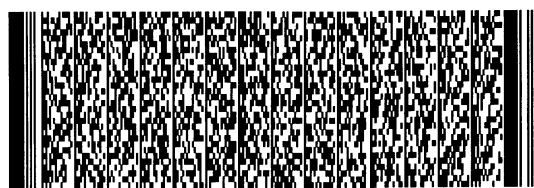
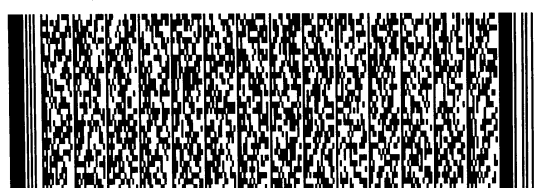
碼，並且恢復與取得第二密碼鑰匙，藉由被加入至第二密碼資料B1之計算結果與被取得的辨識號碼。

如果第二密碼鑰匙係被提供至第二解密裝置8，藉由任何上述提供第二密碼鑰匙之方法，即使記錄裝置9係被從第1圖之著作權保護系統除去，並且被連接至其他具有相同配置之著作權保護系統，也難以取得正確的第二密碼鑰匙，而可以使得再生產僅發生於第二密碼鑰匙記錄於其中之著作權保護系統，而不可能發生於其它系統中。因此，可以防止作品的非法複製。

此外，藉由任何上述提供第二密碼鑰匙之方法，使得再生產僅發生於第二密碼鑰匙記錄於其中之著作權保護系統，而不可能發生於其它系統中。例如，特定於一系統之認證可以用來將其從記錄媒體讀取出來。

再者，根據上述實施例，關於記錄之裝置7至9與關於再產生之裝置3至6係被個別提供，可以執行被稱為時間轉移之處理，其中記錄處理與再生產處理可以同時執行。

如上所述，根據此實施例，由於不同的方法係分別被使用為記錄加密方法(藉由第二密碼鑰匙之方法)，以及再生產加密方法(藉由第一密碼鑰匙之方法)，即使再生產之第一密碼編譯程序係被解密，而會發生作品的非法記錄或再生產，其可以防止記錄的第二密碼編譯程序被直接解密。因此，藉由改變關於再生產之第一密碼編譯程序之鑰匙(認證鑰匙)，其可以防止作品被非法記錄或再生產。再者，關於由第二密碼編譯程序所記錄的資料，其可以與之



五、發明說明 (21)

前相同之方式再產生。因此，關於記錄和再產生之著作權保護可以被執行，而無需損害使用者的方便性。

此外，在上述實施例中，雖然作為一物件之作品，其著作權必須被保護，係為一影像或聲音，而關於此作品之輸入資料，其為即將加密之物件，係為一影像資料或聲音資料，在此係作為範例來說明，但是其可以相同地應用於其它作品。例如，小說之構成係為一物件之作品，其著作權必須被保護，而關於此作品之輸入資料可以應用為一文字資料。

再者，在上述實施例中，雖然已經說明關於一作品之輸入資料係包含於廣播信號中，並且被分佈，但是取得關於此作品之輸入資料之方法並不限於這種情況，其中其係以廣播的形式來分佈。例如，著作權保護系統之使用者可以自己取得關於一作品之輸入資料，經由一通訊網路，例如一網際網路。在這種情況下，一通訊網路連接裝置（一數據機和一撥接路由器或類似物）和一關於其通訊資料之解密裝置會取代第1圖中之裝置1和2而被提供。

否則，關於一作品之輸入資料可以經由一記錄媒體取得。例如，一作品之資料，其係記錄於DVD中，可以作為關於一作品之輸入資料。在這種情況下，一用於DVD之讀取裝置和一關於其所讀取資料之解密裝置會取代第1圖中之裝置1和2而被提供。

此外，在上述實施例中，第1圖之第一加密裝置係對應於第一加密裝置，而第一解密部分11係對應於第一解密



五、發明說明 (22)

裝置。再者，認證裝置4係對應於認證裝置，而認證裝置4之證明撤銷列表D1所描述之內容係對應於關於密碼編譯程序之鑰匙之無效資訊。再者，證明撤銷列表更新裝置5係對應於無效資訊更新裝置。

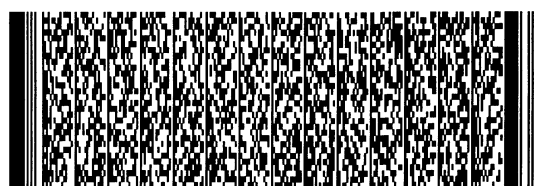
再者，處理裝置6之認證鑰匙更新部分14係對應於認證鑰匙更新裝置。再者，處理裝置6係對應於處理裝置，其執行處理程式以實現關於加密之解密功能。此外，第一解密部分11、聲音/影像解碼部分12、認證部分13和認證鑰匙更新部分14之各自的處理程式(第一解密處理程式、聲音/影像解碼處理程式、認證處理程式、一認證鑰匙更新處理程式)係對應於處理程式，以實現關於加密之解密功能。

再者，第二加密裝置7係對應於第二加密裝置，而第二解密裝置8係對應於第二解密裝置。

此外，著作權保護處理可以藉由記錄程式以實現第1圖之裝置3至8在一電腦可讀取記錄媒體中所執行的各個處理，並且使得一電腦系統讀取和執行記錄在此記錄媒體中之程式來完成。此外，在此所提及之「電腦系統」可包含硬體，例如作業系統和周邊裝置。

再者，如果有使用全球資訊網(World Wide Web)，「電腦系統」應該包含一網頁提供環境(或顯示環境)。

此外，「電腦可讀取記錄媒體」係意指一可攜式媒體，例如一機動式磁碟、一光學磁性磁碟、一ROM、一CD-ROM以及一記憶卡，而一儲存裝置，例如，一硬碟，係



五、發明說明 (23)

安裝於一電腦中。

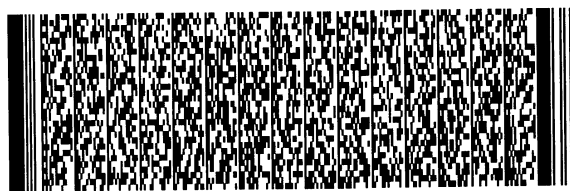
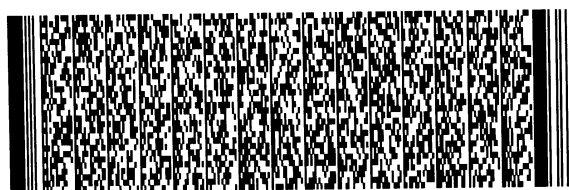
此外，「電腦可讀取記錄媒體」包含一記錄媒體，其存放一程式於一固定時期，例如，一位於電腦系統中之可揮發性記憶體(RAM)，其成為一伺服器或一客戶端，當程式係經由一網路，例如一網際網路，或一通訊電路，例如，一電話電路，來傳送時。

再者，上述之程式可以經由一傳輸媒體或藉由一位於傳輸媒體之傳輸波，從存放有此程式於一儲存裝置或相似物中之電腦系統傳送至其它電腦系統。在此，傳送程式之「傳輸媒體」係意指一具有傳送資訊功能之媒體，像是一網路（一通訊網路），例如一網際網路，或一通訊電路（一通訊線），例如一電話電路。

再者，上述之程式可為一用來實現一部分上述功能之程式。此外，其可為所謂的一微分檔案（一微分程式），其中上述功能可以藉由組合一已經記錄在電腦系統中之程式來實現。

雖然，配合圖示，以上已經詳細描述本發明之實施例，但是特定之配置並不限於此實施例，在一定範圍內的設計變化或修改，並不會偏離本發明之主要精神。

如上所述，根據本發明，關於密碼編譯程序之鑰匙之無效資訊係被提供，而當認證鑰匙的資訊係包含於無效資訊中時，其係用來作為認證，當關於加密之第一密碼鑰匙係共用於第一加密裝置與第一解密裝置之間時，該認證會被否決。此外，當即將無效之物件之鑰匙資訊係與關於一



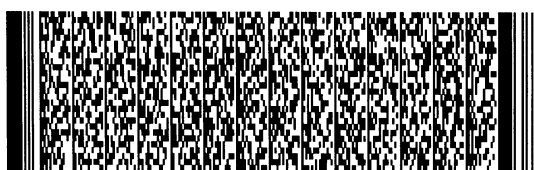
五、發明說明 (24)

作品之輸入資料一起被提供，無效資訊之內容會被更新。因此，可以使在系統中關於密碼編譯程序之鑰匙無效。此外，其可以突然執行使關於密碼編譯程序之鑰匙無效於複數個著作權保護系統，其中關於一作品之輸入資料係被使用。因此，可以有效地防止作品的非法使用。

再者，如果認證鑰匙係藉由用於更新之認證鑰匙來更新，其係與關於一作品之輸入資料一起被提供，其可以僅改變關於密碼編譯程序之鑰匙(認證鑰匙)於複數個著作權保護系統。

再者，如果用於更新之程式，其係與關於一作品之輸入資料一起被提供，係被接收，而藉由用於更新之程式，用於實現關於加密之解密功能之處理程式會被更新，其可以僅改變關於密碼編譯程序之程式於複數個著作權保護系統。

再者，如果關於一作品之輸入資料係藉由使用第二密碼鑰匙係被加密，而該第二密碼資料係記錄於一記錄媒體中，可以使用不同的方法分別作為記錄之加密方法(藉由第二密碼鑰匙之方法)，以及再產生加密方法(藉由第一密碼鑰匙之方法)，即使再產生之第一密碼編譯程序係被解密，而發生作品的非法記錄或再產生，其可以防止記錄的第二密碼編譯程序被直接解密。因此，藉由改變關於再產生之第一密碼編譯程序之鑰匙(認證鑰匙)，其可以防止作品被非法記錄或再產生。再者，關於由第二密碼編譯程序所記錄的資料，其可以與之前相同之方式再產生。

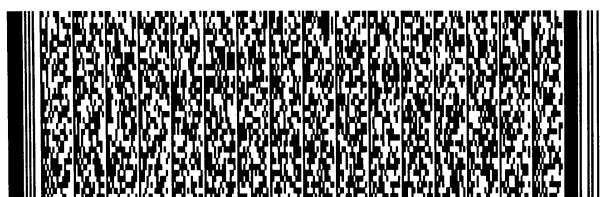


五、發明說明 (25)

因此，關於記錄和再產生之著作權保護可以被執行，而無需損害使用者的方便性。

再者，如果第二密碼鑰匙係存放於系統本身中，而第二密碼資料之密碼編譯程序係藉由存放於系統中之第二密碼鑰匙來解密，則再產生被記錄之資料僅會發生於一作品記錄於其中之著作權保護系統，而不可能發生於其它系統中。因此，可以防止作品本身的非法複製。

綜上所述，雖然本發明已以較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作各種之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

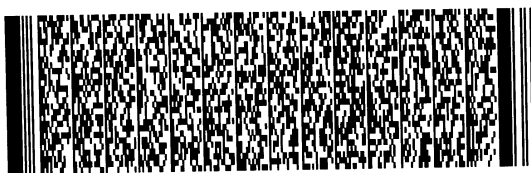


圖式簡單說明

- 第1圖為本發明實施例之著作權保護系統之方塊圖。
第2圖為第一密碼鑰匙之共用處理之流程圖。
第3圖為一習知著作權保護系統之示意圖。

符號說明

- 1 廣播接收裝置
- 2 廣播解密裝置
- 3 第一加密裝置
- 4 認證裝置
- 5 證明撤銷列表更新裝置
- 6 處理裝置
- 7 第二加密裝置
- 8 第二解密裝置
- 9 記錄裝置
- 11 第一解密部分
- 12 聲音/影像解碼部分
- 13 認證部分
- 14 認證鑰匙更新部分



四、中文發明摘要 (發明之名稱：著作權保護系統及其方法)

本發明之特徵在於：包含一認證裝置，具有關於密碼編譯程序之鑰匙之無效資訊，並且用來否決認證，在認證鑰匙之資訊是包含於該無效資訊中之情況下，其係用來認證，當第一加密裝置與第一解密裝置係共用關於加密之第一密碼鑰匙時；以及一證明撤銷列表更新裝置，用來更新在認證裝置中之該無效資訊之內容，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

英文發明摘要 (發明之名稱：COPYRIGHT PROTECTION SYSTEM AND METHOD THEREOF)

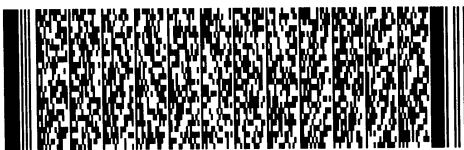
It is characterized to comprise an authentication device 4 having invalid information of a key in relation to cryptology, and for disapproving authentication in case that information of an authentication key is included in the invalid information, which is used for authentication when a first cryptographic key in relation to encrypting is shared between a first encrypting device 3 and a first decryption section 11, and an certificate revocation list updating

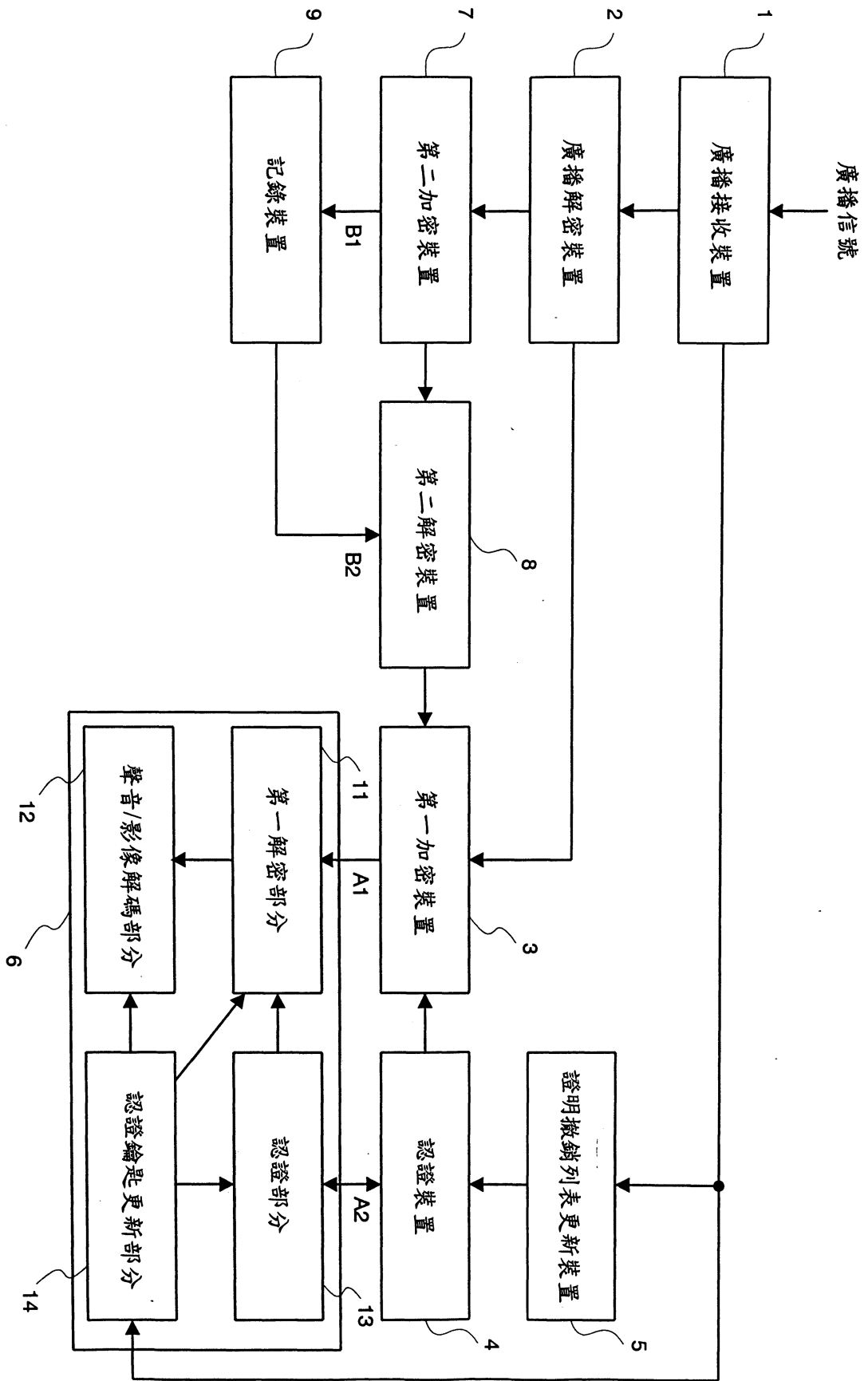


四、中文發明摘要 (發明之名稱：著作權保護系統及其方法)

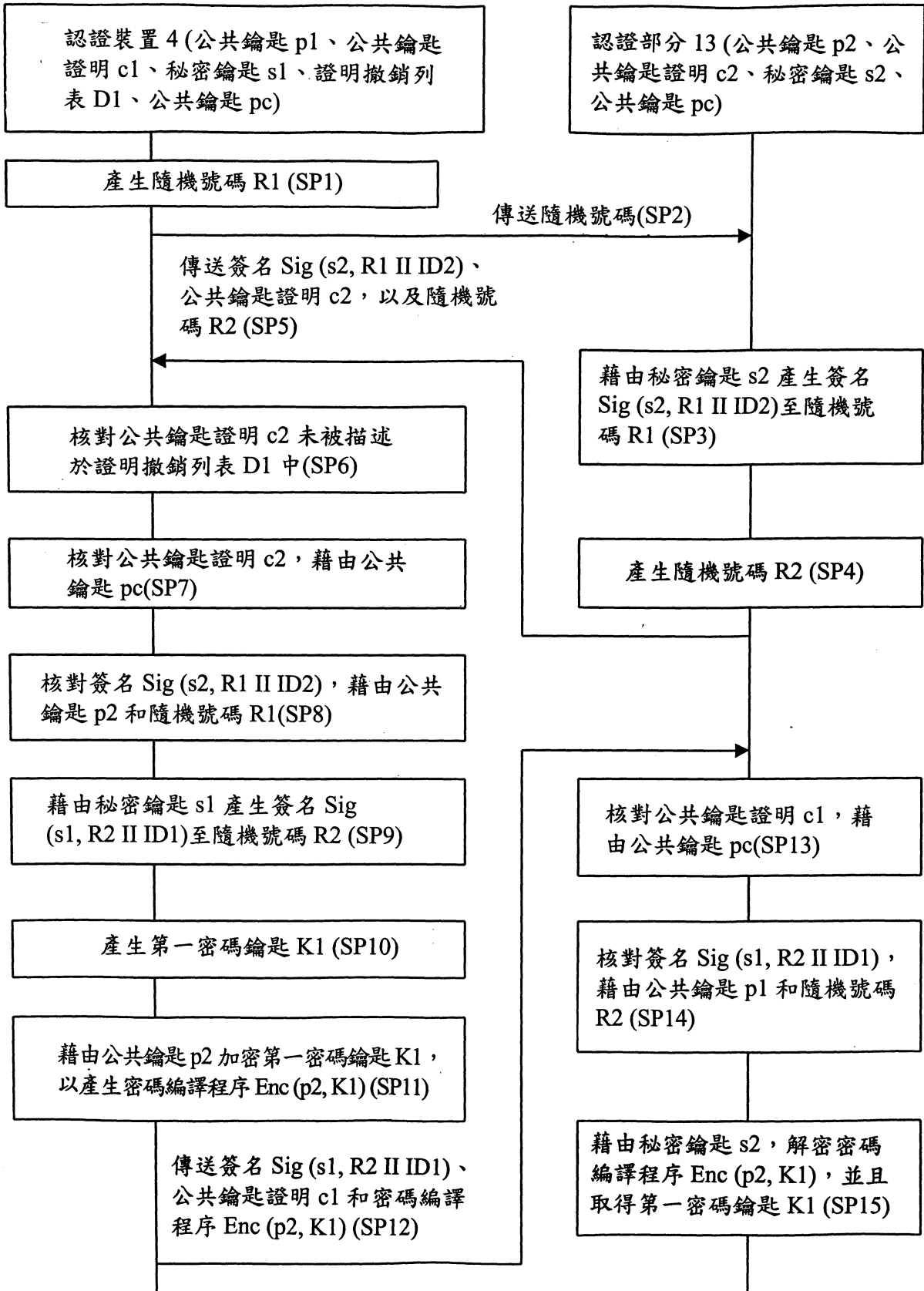
英文發明摘要 (發明之名稱：COPYRIGHT PROTECTION SYSTEM AND METHOD THEREOF)

device 5 for updating contents of the invalid information in the authentication device 4 when receiving information of a key of an object to be invalidated, which is provided together with an input data in relation to a work.

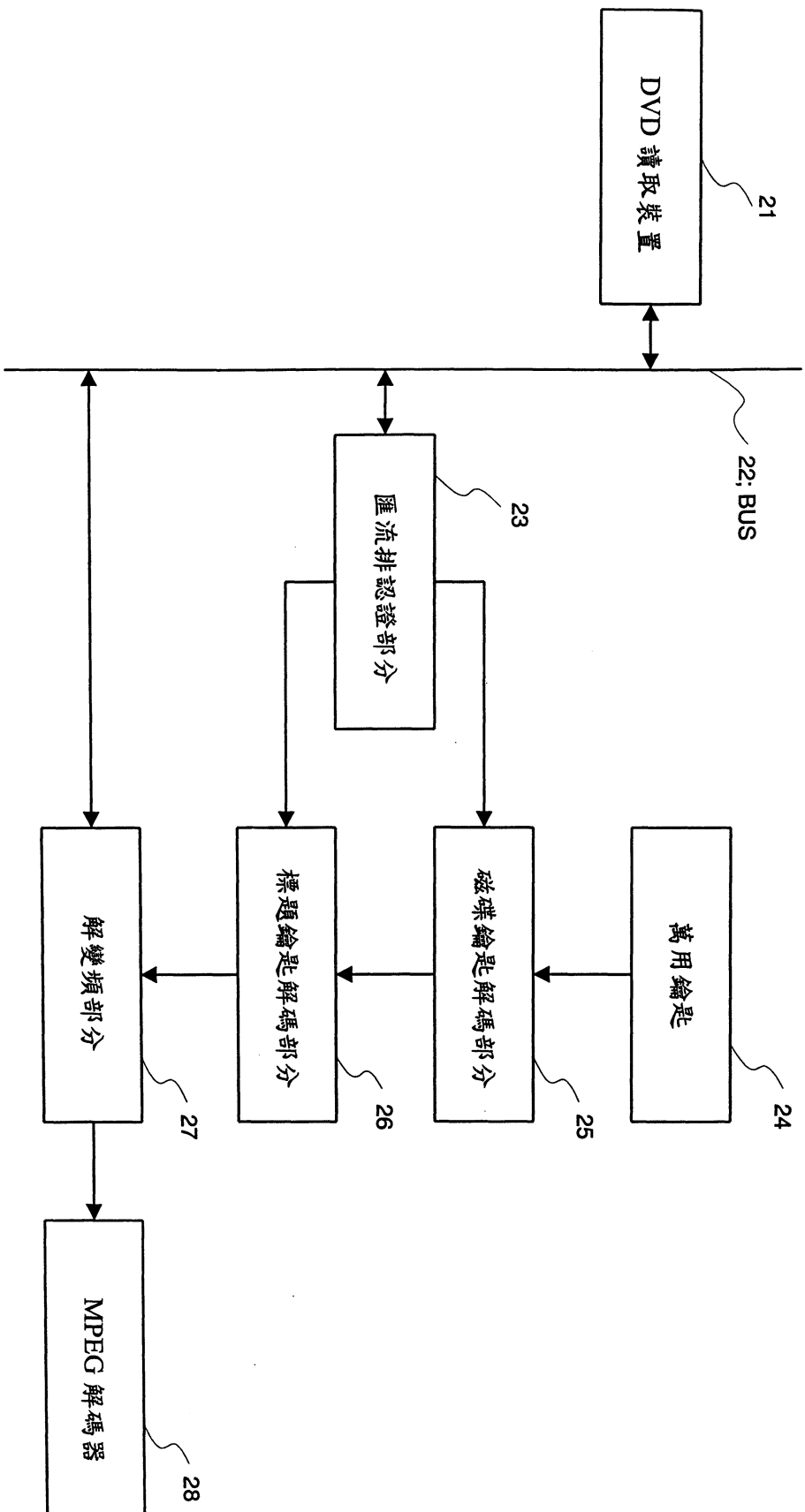




第1圖



第 2 圖



第 3 圖

六、申請專利範圍

1. 一種著作權保護系統，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，該系統包含：

認證裝置，具有關於密碼編譯程序之鑰匙之無效資訊，並且用來否決認證，在認證鑰匙之資訊是包含於該無效資訊中之情況下，其係用來認證，當一第一加密裝置與一第一解密裝置係共用關於該加密之一第一密碼鑰匙時；以及

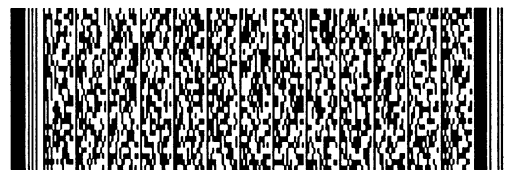
無效資訊更新裝置，用來更新該無效資訊之內容，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

2. 如申請專利範圍第1項之著作權保護系統，其中，該系統包含認證鑰匙更新裝置，用來更新該認證鑰匙，當接收到用來更新之認證鑰匙時，其係與該輸入資料一起被提供。

3. 如申請專利範圍第1項之著作權保護系統，其中，該系統包含一處理裝置，用來執行一處理程式，以實現相關於該加密之解密之功能，而該處理裝置會更新該處理程式，當接收到用來更新之程式時，其係與該輸入資料一起被提供。

4. 如申請專利範圍第1、2或3項之著作權保護系統，其中，該系統包含第二加密裝置，用來加密該輸入資料，藉由使用一第二密碼鑰匙，並且記錄該第二密碼資料於一記錄媒體。

5. 如申請專利範圍第4項之著作權保護系統，其中，



六、申請專利範圍

該系統包含第二解密裝置，用來藉由該第二密碼鑰匙，解密該第二密碼資料之密碼編譯程序，而該第二密碼鑰匙係包含於該系統本身。

6. 一種著作權保護方法，應用於一著作權保護系統中，用來加密相關於一作品之一輸入資料，進而保護該作品之著作權，其特徵在於該方法包含下列步驟：

進行認證，當第一加密裝置和第一解密裝置係共用關於該加密之第一密碼鑰匙時；

否決該認證，在用來認證之認證鑰匙之資訊是包含於在關於密碼編譯程序之鑰匙中之無效資訊中之情況；以及

更新該無效資訊之內容，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

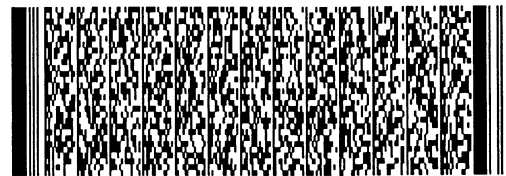
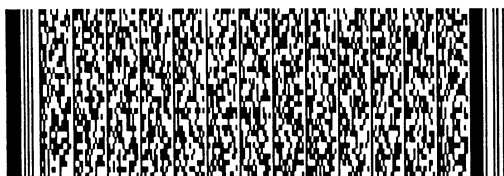
7. 如申請專利範圍第6項之著作權保護方法，其中，該方法另包含下列步驟：當接收到用來更新之認證鑰匙時，其係與該輸入資料一起被提供，更新該認證鑰匙。

8. 如申請專利範圍第6項之著作權保護方法，其中，該方法另包含下列步驟：接收用來更新之程式，其係與該輸入資料一起被提供；以及

更新用來實現相關於該加密之解密功能之處理程式，藉由該用來更新之程式。

9. 如申請專利範圍第6項之著作權保護方法，其中，該方法另包含下列步驟：加密該輸入資料，藉由使用一第二密碼鑰匙，並且記錄該第二密碼資料於一記錄媒體中。

10. 如申請專利範圍第9項之著作權保護方法，其中，



六、申請專利範圍

該方法另包含下列步驟：將該第二密碼鑰匙存放於該系統中，並且藉由該第二密碼鑰匙，解密該第二密碼資料之密碼編譯程序。

11. 一種電腦可讀取之儲存媒體，其儲存一著作權保護程式，用來在一著作權保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，而其特徵在於該程式使得一電腦執行：

用來進行認證的處理，當第一加密裝置和第一解密裝置係共用關於該加密之第一密碼鑰匙時；

用來否決該認證的處理，在用來認證之認證鑰匙之資訊是包含於在關於密碼編譯程序之鑰匙中之無效資訊中之情況下；以及

用來更新該無效資訊之內容的處理，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

12. 如申請專利範圍第11項之儲存媒體，其中，該程式另使得該電腦執行：

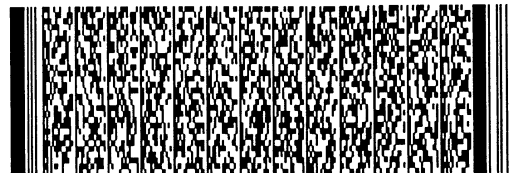
用來加密該輸入資料，利用一第二密碼鑰匙的處理；以及

用來記錄該第二密碼資料於一記錄媒體中的處理。

13. 如申請專利範圍第12項之儲存媒體，其中，該程式另使得該電腦執行：

用來將該第二密碼鑰匙存放於該系統中的處理；以及

用來解密該第二密碼資料之密碼編譯程序，藉由該第二密碼鑰匙的處理。



六、申請專利範圍

14. 一種電腦可讀取之儲存媒體，其儲存一著作權保護程式，用來在一著作權保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，其特徵在於該程式使得一電腦執行：

用來接收用於更新之認證鑰匙的處理，其係與該輸入資料一起被提供，並且更新該認證鑰匙。

15. 如申請專利範圍第14項之儲存媒體，其中，該程式另使得該電腦執行：

用來接收用於更新之程式的處理，其係與該輸入資料一起被提供；以及

用來更新用於實現相關於該加密之解密之功能之處理程式，藉由該用於更新之程式的處理。

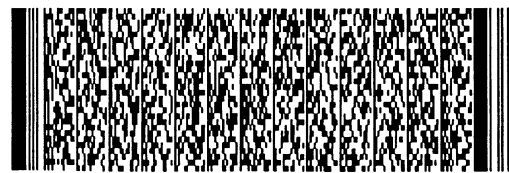
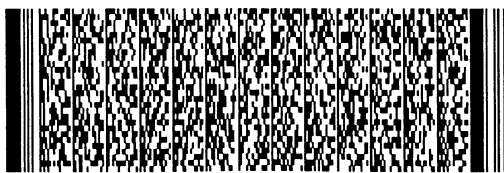
16. 一種記錄媒體，存放一著作權保護程式，用來在一著作權保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，其特徵在於該程式使得一電腦執行：

用來進行認證的處理，當第一加密裝置和第一解密裝置係共用關於該加密之第一密碼鑰匙時；

用來否決該認證的處理，在用來認證之認證鑰匙之資訊是包含於在關於密碼編譯程序之鑰匙中之無效資訊中之情況下；以及

用來更新該無效資訊之內容的處理，當接收到即將無效之物件之鑰匙資訊時，其係與該輸入資料一起被提供。

17. 如申請專利範圍第16項之記錄媒體，其中，該程



六、申請專利範圍

式另使得該電腦執行：

處理，用來加密該輸入資料，利用一第二密碼鑰匙；
以及

處理，用來記錄該第二密碼資料於一記錄媒體中。

18. 如申請專利範圍第17項之記錄媒體，其中，該程式另使得該電腦執行：

用來將該第二密碼鑰匙存放於該系統中的處理；以及
用來解密該第二密碼資料之密碼編譯程序，藉由該第二密碼鑰匙的處理。

19. 一種電腦可讀取之儲存媒體，其儲存一著作權保護程式，用來在一著作權保護系統中執行著作權保護處理，用來加密相關於一作品之輸入資料，進而保護該作品之著作權，其特徵在於該程式使得一電腦執行：

用來接收用於更新之認證鑰匙的處理，其係與該輸入資料一起被提供，並且更新該認證鑰匙。

20. 如申請專利範圍第19項之儲存媒體，其中，該程式另使得該電腦執行：

用來接收用於更新之程式的處理，其係與該輸入資料一起被提供；以及

用來更新用於實現相關於該加密之解密之功能之處理程式，藉由該用於更新之程式的處理。

