

本案已向

國(地區)申請專利
英國 GB

申請日期
2001/07/03 GB 0116278.3

案號

主張優先權
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)

發明背景

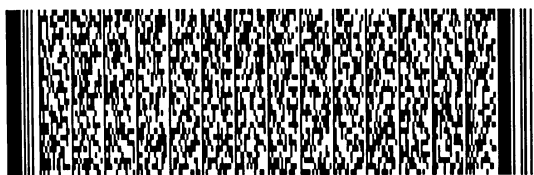
本發明係有關一種數位資料複製的保護方法，及一儲存有數位資料之媒體的保護方法。

儲存有音樂或其它聲音的數位音樂光碟片(CD-DA)可以藉由更複雜的裝置，如光碟機(CD-ROM)來播放或讀取。這表示，使用者可藉由個人電腦中的光碟機將數位音樂光碟片內的資料讀進電腦內，並可以將資料複製到另一個光碟片或其它的記錄媒體。因此，可將資料寫入光碟片內的燒錄器，其與日俱增的能力已經嚴重威脅了音樂工業。

在一較早公布的方法中，一數位音樂光碟可藉由不正確和/或不準確的在光碟片中加入編碼過的控制資料來加以保護。此不正確的資料編碼至光碟片內後，將無法被數位音樂光碟播放器所承認或是被正常的使用。因此，使用者所購買的合法音樂光碟片可以正常的在音樂光碟器上播放。然而，上述不正確的資料可令光碟片無法被光碟機播放。

可是，雖然上述的音樂光碟片令光碟機無法播放它，卻也阻礙了使用者合法地、單純地藉由光碟機來播放光碟片上的音樂或其它聲音。

因此，需要一種防止數位音樂光碟片被複製的方法，



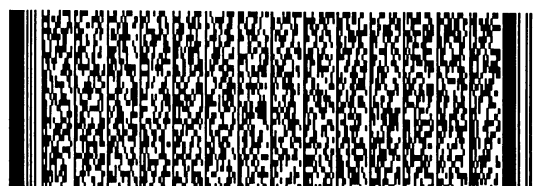
五、發明說明 (2)

在阻止製造出可使用的複製光碟時，卻不會在所有具有播放功能的光碟機上阻止或降低具有保護機制的聲音光碟片的播放。

WO 01/15028 揭露了一種防止數位音樂光碟片被複製的方法，其錯誤的資料係被導入至聲音資料本體內。這些錯誤的資料將被辨識為"不可修正"，藉由一般在聲音播放器或資料讀取裝置內的錯誤修正解決機制。因此，一聲音播放器會隱藏上述的錯誤，例如，藉由以一插入值取代被辨識為錯誤的聲音資料，反之，一資料讀取裝置將會無法讀取上述的錯誤資料，或是只能讀到錯誤的數值。上述在數位音樂光碟片內不正確的錯誤資料將令被保護的數位音樂光碟片無法被複製，或是當播放一個被保護的數位音樂光碟片時，會加入令人無法接受的雜音。

因此，很清楚的，在WO 01/15028 的中並不能可靠地製造出會被辨識成"無法修正"的錯誤。它只提到當一聲音播放器辨識出在聲音資料內的錯誤時，其利用錯誤隱藏的方法，如插入一數值。然而那些錯誤，除了插入一數值或是其它的錯誤隱藏的方法，並不被使用，因為無法辯認它是否存在，上述的聲音資料在再重製時會包含上述加入的錯誤。很清楚地，這是無法被接受的。

本發明係尋求改進如WO 01/15028 中所揭露的複製保



五、發明說明 (3)

護的方法。

根據本發明之第一個目的，係提供一種編碼過之數位資料複製的保護方法，此編碼過的數位資料在解碼後可被成功地插入一數值或隱藏錯誤以用於播放用途，此方法至少包括下列的步驟：

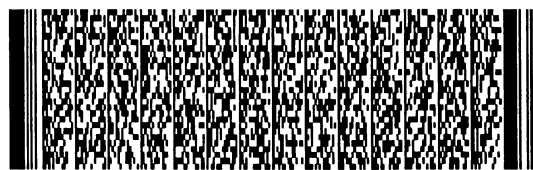
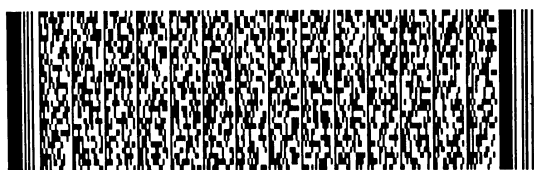
導入改變過的數值至數位資料中；以及

改變包含有上述導入的改變數值的所有代號，使得在解碼時上述的代號將被辯認為無法修正的；

其中，每一個代號藉由加入至少其中數值的一部份，一無法修正的錯誤的典型數值被定義為集合。

使用此典型數值集合 (syndrome representative value) 來改變每一個代號，提供了在解碼時的可靠性，每一個代號的改變將會使得其被定義為無法修正的。

在一較佳具體例中，每一個代號中的4個位元藉由以4個位元中的典型數值集合來加入。較佳地，所有被改變的4個位元皆為同位值。換句話說，也可以加入典型數值集合到只有3或2個位元的代號中。對數位音樂光碟片而言，只要一個修正碼大致上至少有兩個位元，則典型數值集合



五、發明說明 (4)

通常至少有兩個位元。

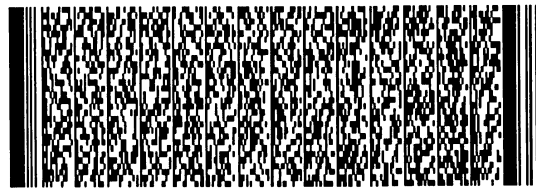
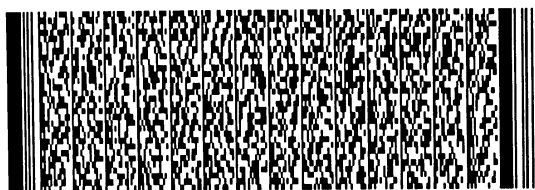
較佳地，上述的典型數值集合是一個集合的主陪集 (coset leader) 代表。

在一較佳具體例中，此集合是被產生的，其中，一解碼器中產生的錯誤定位多項式 (error locator polynomial) 是沒有根值的 (has no roots)。

既然本發明的目的係提供一種數位音樂光碟複製的保護方法，本發明很清楚的對任何數位資料具有保護的功用，其中在數位資料中的錯誤將被辨認或修正，當讀取此資料的時候；且任何被辨識為無法修正的錯誤通常會被插入一數值，或是被隱藏，在播放期間。

本發明之數位資料複製的保護方法係準備用來辨識具有改變過數值的代號，其中，該代號為無法修正的。只要上述的數位資料被播放，例如，聲音、虛擬圖像或影像，則撥放器會讀取隱藏的錯誤機制，例如，一插入值。因此，此被視做無法修正的代號被用來強制上述改變過的資料值成為一插入值或其它隱藏的機制，當播放此資料時。

然而，當讀取資料時，一資料讀取裝置不會使用此錯誤隱藏機制，雖然其可以使用進一步的解碼和錯誤修正機



五、發明說明 (5)

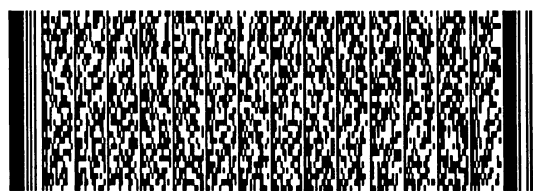
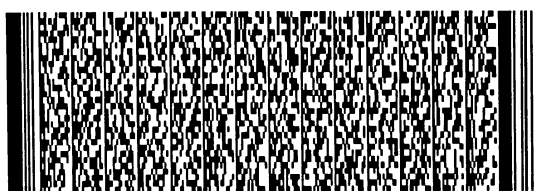
制來試著進一步更正資料。因此，假如經由本發明所產生的此編碼過的、防止複製的數位資料被一數位讀取裝置解碼，且被標記為無法更正的話，此資料可能經由其它的方法來更正，然後此數位資料結合一改變過的數值，被視做未曾改變。假如此資料讀取裝置被當做一複製機的輸入端，例如，此改變過的數值將被編碼至複製的介面，如數位音樂光碟片（CD-DA）。藉由此方法，產生的複製品的品質會劣化。

在本發明之一較佳具體例中，此改變過的數值將被製造造成數位音軌資料。它可能為聲音資料，例如，被編碼至一數位音樂光碟片內。

較佳地，此改變過的數值藉由增加大量的數值至聲音資料數值內而被導入。以上可在二元集合（binary domain）內完成，例如，藉由增加一介於128至143間之數值到聲音資料數值內的最高有效位元（MSB）。

藉由XORing，對此數值提供一大量的樣品，它不需要知道聲音資料原來的數值是多少，因為計算學可以確保在聲音資料上會有一可聽見的尖銳聲音被產生。

本發明亦可擴展至一媒體，此媒體複製了被保護的，編碼過的數位資料，在解碼以後，其可成功的插入一數



五、發明說明 (6)

值，或進行一錯誤隱藏，以供播放使用。其中，此媒體記載了導入有改變過的數值的數位資料，且代號，已經被更改過使其在解碼時被辨識為無法修正，此代號包括一改變過的數值，且此代號藉由至少加入數值的其中一部份而被改變，一無法修正的錯誤的典型數值被定義為集合。

本發明發現了可用於防止複製的特別應用，例如，應用於數位音樂光碟片，本發明能可靠地產生一錯誤標幟，其可應用於其它方面，例如，用於浮水印，或提供一個特徵。

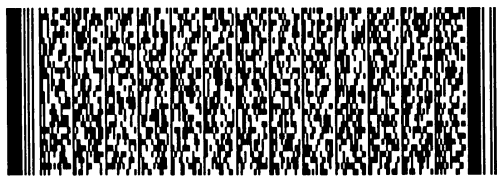
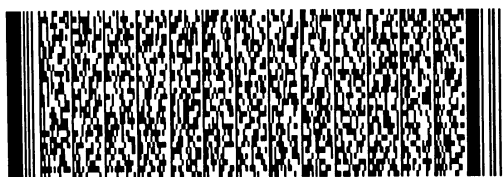
本發明亦可擴展至一數位資料的編碼方法，此方法至少包括下列步驟：

改變預先決定好的、從數位資料中產生的代號，使得在解碼時，此代號能被辨識為無法修正，

其中每一個代號藉由至少加入數值的其中一部份而被改變，一無法修正的錯誤的典型數值被定義為集合。

本發明亦可延伸引用至一防止複製的檔案，此檔案係用來改變數位資料，且由此產生代號，藉由上述的定義。

本發明之目的及諸多優點將藉由下列具體實施例之詳



五、發明說明 (7)

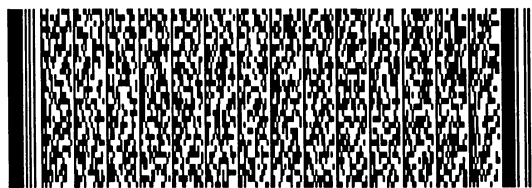
細說明，及參照所附圖示，而被完全揭露。

發明詳細說明：

本發明的一些實施例會詳細描述如下。然而，除了下列應用外，本發明還可以廣泛應用在其它需要編碼的領域。因此本發明的範圍不受此限定，其以之後的申請專利範圍為準。

數位資料的編碼在實務上已經被發展出來以確保在整個較早期的溝通頻道上，不管有無雜訊，資料能被正確的接收，例如，電報。然而，現今數位資料被例行性的編碼以容許資料中將被偵測出的錯誤並將其更正。以此觀點來看，本發明中所描述的基本方法係特別關於在數位音樂光碟片上資料的編碼和解碼。然而，吾人可以察覺到這些方法也相同的適用在其它領域，只要有數位資料需要被編碼，例如，當播放時，為了可靠性，以及數位資料中將要被隱藏的錯誤的緣故，藉由插入一值或其它的隱藏錯誤技巧來達成。

上述錯誤修正碼的理論將被熟悉此領域的技藝人士所瞭解，因此不再這裡說明。然而，某些基本的概念將在此被解釋，藉由下列的例子以幫助瞭解。



五、發明說明 (8)

數位音樂光碟片，及光碟機和相似的構造，利用 Reed-Solomon 編碼學來編碼和偵測錯誤。Reed-Solomon 密碼學係為 BCH 碼的一個子集合；雖然 BCH 碼是漢明碼 (Hamming codes) 的一般化。漢明碼是單一修正碼，且被歸納於 BCH 碼，其允許大量錯誤的修正。

首先，先檢視一簡單線性的，單一錯誤的修正碼 (Hamming)。

一訊號 u ，具有一符號 k ，被編碼進入一代號或向量 x ，具有 n 個符號，以產生一線性碼。代號的第一部份包含函數 (message) 本身，隨之而來的是 $n-k$ 檢查符號或同位元值 (parity value)。

因此，若函數為：

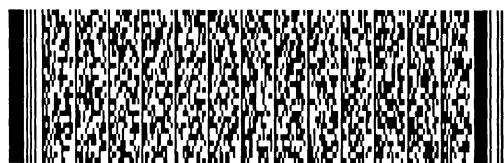
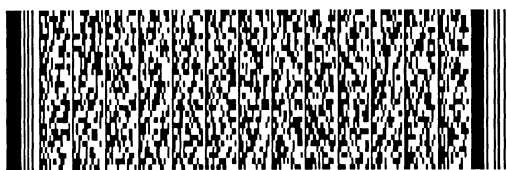
$$u = u_1 \ u_2 \ \cdots u_k$$

則代號為

$$x = x_1 \ x_2 \ \cdots x_k \ \cdots x_n$$

其中 $n > k$ ，且 $u_1 = x_1$ ， $u_2 = x_2$ ， $\cdots$ ， $u_k = x_k$

此檢查符號被選擇出，所以



五、發明說明 (9)

$$Hx^{tr} = H \quad = 0$$

其中H係為密碼的同位元矩陣。

此計算係執行模2(modulo 2)，或XOR，例如 $0+1=1$ ， $1+1=0$ ， $-1=+1$ 。

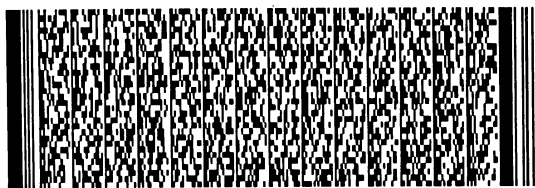
為了從函數產生一碼，此函數u被生成元矩陣G(generator matrix G)操作而產生代號x，例如，

$$x = uG$$

此生成元矩陣G(generator matrix G)係與同位元檢查矩陣H和一組獨立代號有關，此係從一可做為生成元矩陣列的密碼獲得。

因此，如上所述，一函數需要

$u = u_1 \ u_2 \ \cdots u_k$ 轉換成



五、發明說明 (10)

代號 $x = x_1 \ x_2 \ \cdots x_k \ \cdots \ x_n$

當解譯時，系統接收到了

接收向量 (received vector) $y = y_1 \ y_2 \ \cdots y_k \ \cdots \ y_n$

此系統需要決定接收向量 y 中的那一個字元被修正，因此，假如代號存在有錯誤，則系統會將其修正。

線性密碼有效的解碼方法係利用陪集 (cosets)。如上面所舉的例子來說，對一線性代號 C ，其將以 q 元素填滿一個區域 (field)，此方程式為

$$a + C = \{ a + x : x \in C \}$$

其中 a 為密碼 C 中的任一向量，是代號 C 中的一個陪集。每一個陪集具有一個向量 q^k 。

第1a圖係顯示對於 $[4, 2]$ 密碼的一生成元矩陣 G ，例如，一密碼其中 $k=2$ ， $n=4$ ；第1b圖係顯示表現出一函數的標準陣列，藉由操作生成元矩陣 G ，可從此函數產生一代號 C 。此三個位於陣列中左手邊欄位的陪集字元 (coset words) 具有向量中最小的非零數值，在每一個陪集中；



五、發明說明 (11)

因此，具有最小重量 (minimum weight) 。這些最小重量向量係為主陪集 (coset leaders) 。

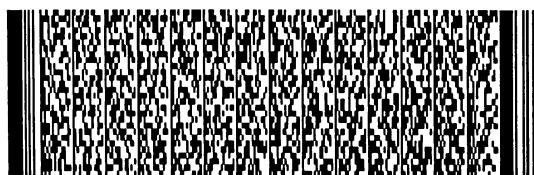
當一接收向量 y 收到一字元時，其在標準陣列中的位置就被定義了。假如它在其中的陪集之一被發現，一個適當的主陪集 (coset leader) 被確認為可能的錯誤，藉此，字元就能被解碼。

因此，舉例來說，若 y 值是 1111 (示於圖示中元件符號 14 的位置)，且此位置決定了適當的主陪集 (coset leader) 為 0100，如元件符號 16 所示。第 1b 圖所示的陣列顯示出正確的代號 18 是 1011。在解碼過程中，此代號 18 可被解釋為 $1111 - 0100 = 1011$ 。此解碼的方法係為最大可能解碼 (likelihood decoding)。

第 1b 圖中所示的陣列中的最後一個欄位顯示了對陣列中每一列的集合 (syndrome) S ，其被定義為

$$S = Hy^{\text{tr}}$$

並且說明了錯誤的位置。假如沒有錯誤存在， y 的集合則為 0。再者，兩向量係為相同的陪集假如它們具有相同的集合。基本上，集合包括了接受者所有關於錯誤的資訊。



五、發明說明 (12)

當然，在實務系統上，超過一個以上的錯誤可能會發生且需要更正。藉由增加檢查符號，及藉由增加密碼中同位元檢查矩陣 H 內及生成元矩陣 G 內的向量數目，則有可能來進行複製。然而，為了使計算更容易被管理，每一個矩陣中 m 二元向量的欄位，一個 m 元組為一適當的多項式 α 。此生成元矩陣被一生成元多項式所置換：

$$g(x) = (x - \alpha^b) (x - \alpha^{b+1}) \cdots (x - \alpha^{b+d-1})$$

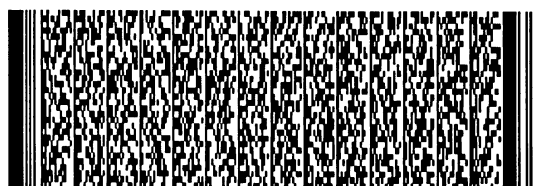
其中 b 為一整數 (number)，通常是 1。

然後，此標準陣列包括了多項式以代表代號，更勝於用密碼本身來代表。然而，其仍然安排有陪集，與主陪集 (coset leaders)，及具有集合確認錯誤的位置。

因此，參見第 1b 圖，解碼工作如上面所述，除了 m 元組需要被映對以提供密碼，且用於 m 元組的多項式必須被解決當其為根值時，其中，根值定義了錯誤定位。

在此，大略地翻閱一下 WO 01/15028 中，在數位音樂光碟片上數位資料的編碼及防止複製的方案。

一數位音樂光碟片，其被製造且錄製成一已知的標準



五、發明說明 (13)

資料格式（紅皮書標準），其上紀錄有音樂資料且將在聲音播放器上播放，例如一傳統光碟機播放器。如同定義光碟片的物理性質一樣，例如，它的尺寸大小，光學特性，及雷射波長，此紅皮書亦定義了訊號格式和將被使用的解碼資料。

眾所周知的，依照紅皮書的標準使用可以確保任何依照標準所生產的數位音樂光碟片可以在任何依照標準所生產的聲音播放器播放。

第2圖係概要的顯示在光碟片6上的突起（spike）音軌4。此在數位音樂光碟片上的尖銳音軌4被分隔進入導入區8，一連續的音樂或聲音音軌10，和一導出區12。此導入軌8包括一音樂內容目錄（Table of Contents, TOC），其定義了在播放機上光碟片可被播放的軌數，當導出區12提示了尖銳（spike）音軌4將被結束。

一聲音播放器總是在開始時讀取導入軌8。然後，音樂軌可被連續的播放當讀取頭隨著軌道4從導入到導出。另一方面，如果有需要，播放器可控制讀取頭到每一個音軌10的起始處。

以肉眼來看，一光碟片看起來就像一數位音樂光碟片且具有一樣的尖銳音軌4被區分成各區段。然而，資料讀



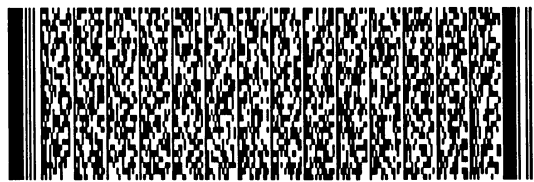
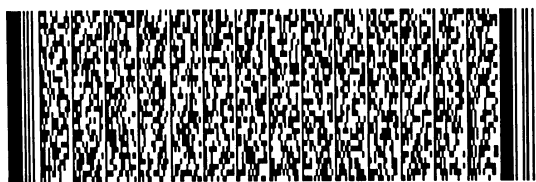
五、發明說明 (14)

取裝置，例如一光碟機，可以讀取數據，處理資料，從光碟片上的每一個區段，依據光碟的資料或數據的屬性而定。一資料讀取裝置從每一個區段讀取資料，藉此，當有需要時，讀取頭能被驅動以讀取尖銳音軌 4 中任何適合適當的部份。

為了確保資料讀取裝置可讀取任何的光碟片，光碟片和讀取裝置皆以已知的標準來製造，在此為標準黃皮書。這些標準黃皮書規範併入，且延伸為標準紅皮書規範。因此，一資料讀取裝置，例如一光碟機，能被控制以播放一數位音樂光碟片。

資料讀取裝置讀取、壓縮的能力，或是讀取在數位音樂光碟片上資料的能力對音樂工業造成了一個問題。一使用者可使用它的光碟機從一音樂光碟片上讀取資料，例如，變成一電腦檔案，然後使資料就可以被複製。具有將資料記載到光碟片上的燒錄裝置越來越容易得到，代表著個人和組織現在可以很容易的利用此科技來完美的複製音樂光碟片。因此，音樂工業界很關心這個問題。

因為在光碟機內的數位音樂光碟片上的資料根據適當的標準被編碼的過程已經是習知的技術，因此在這裡就不再詳細的描述。



五、發明說明 (15)

簡單的來說，在光碟片上的資料藉由EFM (eight to fourteen modulation 8至14調幅) 被編碼進入一無形的框架 (frame)。圖三顯示出此框架的格式，從那裡明顯的看得出來，每一個框架具有一個同位資料 (syn data)，次密碼字元 (sub-code bits) 提供了控制和顯示符號，資料字元 (data bits) 和同位元字元 (parity bits)。每一個框架包括有一24個位元組的資料，此資料對數位音樂光碟片來說為一聲音資料。

在每個框架中包含有8個次密碼，分別為P、Q、R、S、T、U、V和W。一般說來，只有P和Q次密碼字元被以聲音格式使用。標準規範需要圖三框架中的98被組合成一個區段，且98框架中的次密碼字元被收集至形成次密碼區塊。亦即，每一個次密碼字元區塊被構築成一位元，以此種方式，8個不同的次頻道 (subchannels)，P到W被形成。這些次頻道包含有可應用於光碟上的控制資料。此P-和Q-次頻道併入了用於光碟軌道上的時間資料和控制資料，且通常是音樂光碟上唯一被使用的次頻道。

在光碟上的資料被進行EFM編碼且被形成為框框結構前 (如第三圖所示)，其先進行錯誤修正編碼。更特別地說，儲存在光碟上的資料被交錯以傳送錯誤，且具有同位元值併入於錯誤修正當中。此Reed-Solomon Code (CIRC) 及CIRC編碼圖的例子被顯示於第四圖中。我們可



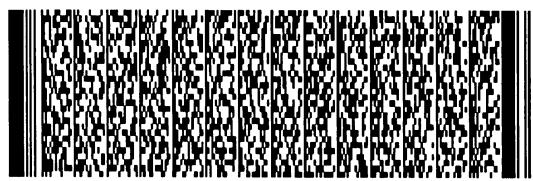
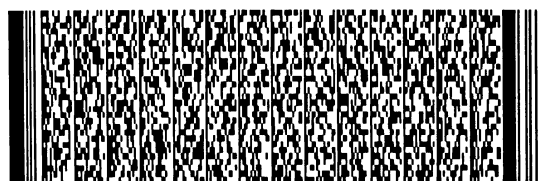
五、發明說明 (16)

以看到，一C2編碼器20接受了24個位元組的聲音資料，使某些位元組延遲，且產生4個位元組的Q同位元值。穿越交錯藉由一遵守C2編碼器20的交錯器22，藉此28個位元組經由不同的間隔被延遲。在交錯動作後，每一個字元C2被儲存在28個不同的C1代號。

一C1編碼器24接受了28個位元組的向量，此向量包含有從28個不同的C2代號得來的資料，且產生出4個更多位元組的P同位元值。因此而產生的32個位元組代號留下了第四圖中的CIRC編碼器並且被提供給EMF編碼器。

第四圖中，藉由一CIRC編碼器產生的區塊資料被顯示在第五圖中，其中每一個S值代表4個位元組的資料，每一個Q值代表4個位元組的Q同位元值，且每一個P值代表代表4個位元組的P同位元值。此外，第五圖顯示出資料列，如26所示，其係藉由C2解碼器來解碼；且資料列，如28所示，係藉由C1解碼器來解碼。

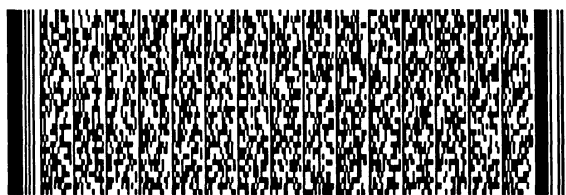
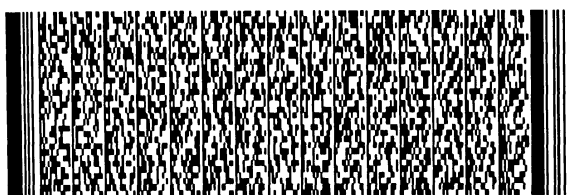
第六圖係概略顯示出一用於解碼光碟上區塊資料的CIRC解碼器。因此，如我們所知道的，光碟上的凹洞和平面(land)被讀取且被進行一EFM解調器，然後被提供給用於去交錯、錯誤偵測和錯誤修正的CIRC編碼器。然後，資料被輸入進如第五圖所示的區塊中的解碼器，且輸出成一24個位元組的聲音資料。



五、發明說明 (17)

因此，第六圖中顯示了元件符號32之8個位元字元 (bit words) 的框架提供至解碼器。具有32個位元組的框架的包括有24個位元組的聲音資料和8個位元組的同位元值。在C1解碼器30中，藉由4P同位元值來偵測錯誤且短時間內持續的錯誤得以被更正。較大的錯誤，例如，大量激增的錯誤，將會使得C1列中的某一些列的值無法被修正或具有兩個可修正的錯誤。這些列將會被適當的標識起來。例如，在C2階段中的被期望為還可以修正的錯誤，高階解碼器利用刪除標幟可標識起每一個錯誤的列。所有被認為有效的字元皆跳過而未被處理。因此，C1解碼器30標識了任何被辨識出來的錯誤，但未將其修正，如元件符號32所示。當沒有錯誤時，C2解碼器34傳送了所有的字元而不帶有標幟，假若其在C2解碼過程中也沒有出現錯誤的話。C2解碼器34傾向於修正任何殘留的錯誤，藉由Q同位元值和任何的錯誤標幟。

如上所述，在解碼中，首先檢查C1列以偵測單獨的錯誤並給予修正。C1解碼器通常被修正以一大部份為明顯錯誤的記號，且因此，可在超過其準確度的極限下偵測出錯誤的情況，並且以記上標幟的方式傳送出錯誤偵測的資訊，到C2解碼器34。在C2解碼器中，一在錯誤修正範圍內被偵測到的錯誤將會被修正。然而，超過錯誤修正範圍而被偵測出來的錯誤會產生如C2中所標示出來的標幟。一C2



五、發明說明 (18)

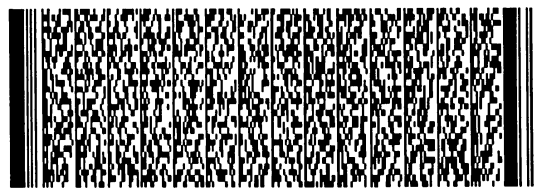
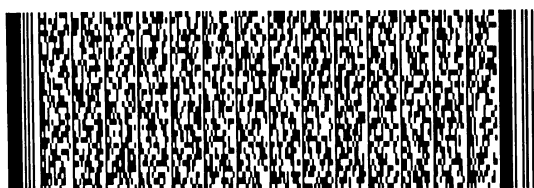
標幟代表著偵測到一無法被修正的錯誤。

第七圖係概略地顯示出一聲音播放器。如圖所示，從數位音樂光碟片6上讀取的資料被傳送到一紅皮書解碼器，元件符號為36，然後可能被直接送入聲音重製裝置38。然而，當偵測到一無法修正的錯誤且產生一C2標幟時，資料藉由一錯誤隱藏單元40被傳送到聲音重製裝置38。

在一聲音播放器內的錯誤隱藏單元40的屬性是可以改變的，例如，併入聲音靜音電路。在如下說明的具體例中，錯誤隱藏單元40被顯示為一插入裝置40。

一聲音音譜通常是連續的，假若一錯誤在音譜中產生不連續，則缺少的數值，在大部份的案例中可被快速地及相當準確的被插入。然而，例如，當一資料讀取裝置被用來讀取數位資料時，插入值無法被使用做為一符號的值，因為其與將被救回、拯救的值沒有任何關聯性。此提供了一個防止數位音樂光碟片被複製的方法，此防止複製計劃允許光碟片在聲音播放器上播放，但阻止了利用一資料讀取裝置從光碟片上產生一可使用的複製資料。

基本上，對於防止複製這方面，非期望的的噪音被併入聲音資料內一起錄製到碟片上，並與錯誤修正字元相聯



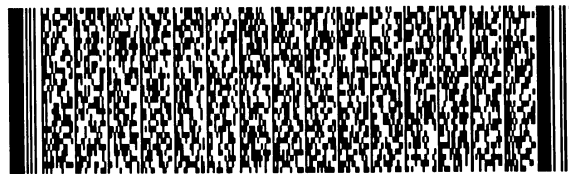
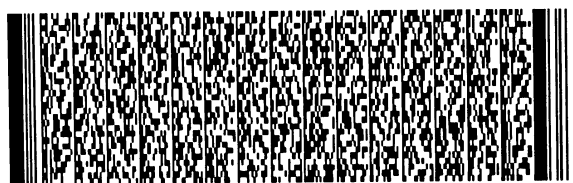
五、發明說明 (19)

結，其定義非期望的噪音為無法修正的，並藉此產生如上述所說的標幟C2。這樣的資料將藉由一聲音播放器傳送至一插入裝置40，此插入裝置可以移除非期望的噪音並置換一更適合的聲音數值。然而，一資料讀取裝置只單純的讀取聲音資料，標識為無法修正，所以此非期望的噪音被寫入碟片中，例如，在複製的過程中。因此，此複製的碟片係相當的劣質。

在W0 01/15028中一防止數位音樂光碟片被複製的方法係藉由引入一標幟，對於碟片上非期望的噪音標識為無法修正。此份報告藉由增加"尖銳(spikes)"來改變聲音資料，然後改變聯結於C1列和C2列的同位元字元，其包含有改變過的聲音資料，使得變更過的聲音資料被辨識出來，然後標識為無法修正。一般來說，W0 01/15028中提出的報告係以未使用的符號來置換C2 同位元位元組，且以零來置換C1 同位元位元組。

然而，不同的解碼器使用不同的演算法，在錯誤修正上也有不同的表現。我們已經發現有些解碼器錯誤地更正了原本的錯誤，更勝於將其標識為無法修正。對C1 同位元位元組來說，理論上也有可能為零，因此，將其設定為零將不會改變C1 列。

如上所述的防止複製方案，其係加入尖銳到數位音樂

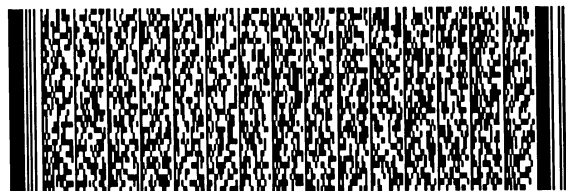
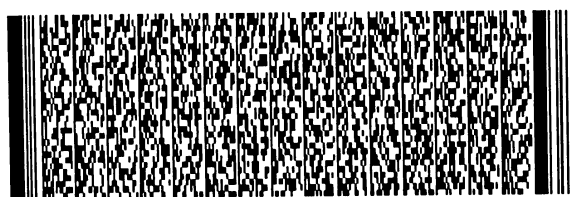


五、發明說明 (20)

光碟片上的聲音資料以產生喀喀聲，這是為了完全確保所有的聲音播放器能被觸發去使用它門的插入器以移除尖銳，不論解碼器提供的資料是多麼的複雜或是用什麼樣的錯誤修正方法。因此，很清楚地，音樂工業非常不願意採用一防止複製的技術，假若實務上有可能使非期望的添加的噪音被聽見，當消費者播放一正版的數位音樂光碟片在一典型的聲音播放器上。

由上述解碼的過程中可以看到，一集合能從一接收向量中的符號 (symbols) 中被計算出來。由此點來看，計算能被安排以使得每一個集合只包含有關於其如何從一個正確的列中聯結另一列。如果集合皆為0，這代表了此列沒有錯誤，於是，接收向量為一代號。因此，在接收向量中不需要任何的錯誤修正。對本發明之防止複製資料的方法來說，一解碼器會根據其集合來處理一系列的資料，而不是根據一系列中資料符號的值來處理，這是很重要的一點。因此，如上所述，假如集合所顯示的列的資料是正確的，則資料將未經改變被傳送。同樣地，假如集合所顯示的列的資料是不正確的，則解碼器會傳送包含有一錯誤標幟組的列的資料。

因此，在本發明的方法中，列的資料將未經修正被傳送，但伴隨著一錯誤標幟組，假如與列聯結的集合告訴解碼器在列中的資料是不可修正的。因此，不論是從實務上



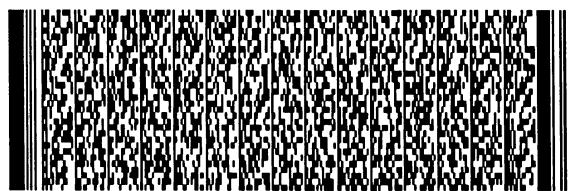
五、發明說明 (21)

或數學上，都有必要找出一個集合，其將總是阻止解碼器修正相關的列。

有很多的方法可使得一解碼演算法失效而產生一錯誤標幟。使解碼演算法失效最普通的方法係為不具有根值，且與列聯結的錯誤定位多項式。在本發明的一較佳具體例中，選擇一集合來代表一不具有根值的錯誤定位多項式。

當然，藉由解碼器產生一集合是很困難的，因此，資料在碟片上必需被編碼，以便可以穩定的對於C1或C2列的資料產生集合，其中該資料包含有改變過的聲音數值。再者，此"集合產生的資料 (syndrome generating data)"將不會單獨被編碼到碟片上，會與聲音資料一起被編碼，且控制和解讀資料。

在編碼和解碼的過程中，向量被加入模2(modulo 2)計算，其中，數位組是與XORed一起。依照本發明，一個或一個以上的在代號中的符號係XORed，而與一個或一個以上的符號一起。這些符號被選擇使得解碼一包含有被選擇的符號的代號能產生決定性的集合。特別地，被選擇的符號的向量是陪集中的主陪集(coset leader)，它提供了所需的集合。我們已經發現XORing資料的數值和所需集合的典型會穩定地使一解碼器去標識在代號中一不小心的錯誤。



五、發明說明 (22)

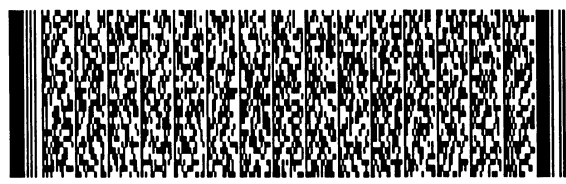
當然，使用此穩定地，從解碼器中獲得一錯誤標幟的方法以對一碟片打上浮水印是有可能的，或是藉由額外增加的記號來保護。在浮水印的過程中，特定描述的資料被加入碟片中以區別複製過的碟片和原本的碟片。

然而，本發明發現了防止複製的特別的使用方法，其中特定的聲音樣品將被改變以引起尖銳，此尖銳可以被聽見為一種喀喀聲，當它在播放時。舉個例子，例如，在W001/15028中，脈衝被堆疊在修正過的聲音資料中的特定的樣品上以在其內產生尖銳。

因此，依照本發明，一個或更多的聲音的樣本若需要的話，可被改變以劣化聲音的內容。例如，藉由W001/15208中所揭露脈衝堆疊的方法 (superimposition of impulses)。於是，所有包涵了那些改變過的樣品的代號被定義，且每一個代號中的資料藉由XORing位元組而改變，且其中包括有主陪集(coset leader)的值。

大致上，每一個代號的4個位元組藉由XORing和4個位元組的主陪集(coset leader)而被改變。

在較佳具體例中，如第九圖所示，4個位元組相對於同位元值被改變。因此，在被選擇的主陪集(coset



五、發明說明 (23)

leader) 70 中的所有的值，將表現得如同一損壞的列，其值將為零，除了相對於同位元位元組72中的數值。這是已經預先決定的，如果所有4個同位元位元組被給與非零的數值，則由其中而產生的列將會可靠地被標識為無法修正。能不能找到一個主陪集(coset leader)具有三個、兩個或一個非零的元素，得視陪集本身來決定。

第九圖概略地描述了本發明之方法，其中一聲音列74並入一可聽見的喀喀聲76，其係與一錯誤修正字元70相聯結，此字元定義了列74為無法修正的。併入有可聽見的喀喀聲76的列74係XORed78 與主陪集(coset leader)70一起以產生列80，列80併入了喀喀聲76及損壞的同位元位元組72。因此，雖然列80係一包含有正確聲音資料的代號，其被定義為無法修正的，藉由損壞的同位元位元組 72 的存在。

當然，是有可能去決定一個單一的主陪集(coset leader)，如元件符號70，並且使用它以改變在數位音樂光碟片上的所有的代號，其中，此數位音樂光碟片包含有劣化的聲音資料。然而，雖然目前集合和它的主陪集(coset leader)將不在對一整個碟片來使用，但是各種不同的集合仍會被利用。

如WO 01/15028中所揭露，既然聲音資料可以被改



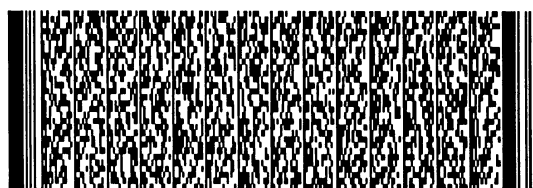
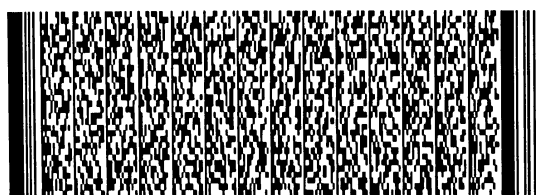
五、發明說明 (24)

變，則也有可能只改變樣本中大部份有意義的位元組 (MSB) 為無法修正。

因此，在一較佳具體例中，範圍在128到143端點中的一數值被XORed 與聲音資料中最有意義的位元組以產生一變更的資料樣本76，如第九圖中所示。這些變更過的資料樣本將以喀喀聲的形態被聽見假如被播放的話。然而，對這些樣本來說，在聲音播放器對列80解碼的過程中，錯誤的標幟將可靠地利用插入來解決，或其它的錯誤隱藏方法。然而，一資料讀取裝置將不改變資料而將其傳送或是修正它。假如資料被讀取裝置讀取，然後被複製到一碟片上，則喀喀聲聲在播放時將會被聽見藉此劣化此複製碟片的音質。

當聲音符號被XORing改變時，其相對的變得容易去改變位元組的數值，且此值被加入最有意義的位元組內。假若此數值是假性的隨機取樣的話，例如，則每一個樣本的MSB皆能非預期地以一個位元組被XORed，例如，具有一範圍在128到143內的一數值。

這代表一強制發生的尖銳的強度不一致，使得想要淨化複製碟片以便於被承認和移除外加的尖銳變得非常不容易。

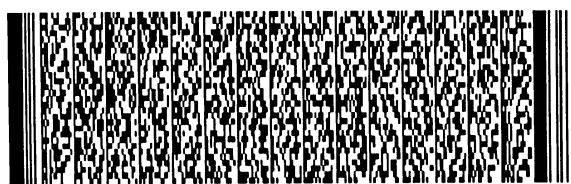


五、發明說明 (25)

第九圖揭露了一聯結代號 74 的方法，以一改變過的聲音數值和一主陪集(coset leader)70，藉此產生一被標識為無法修正的代號80。然而，在實務上確保代號74和主陪集(coset leader)70之間可靠地聯結關係是很困難的。藉由圖十中概括性所描述的方法可以避免掉上述所提及的困難。

如第十圖所示，一具有損壞的同位元位元組72的主陪集(coset leader)70被以一創造的代號84 XORed。此創造的代號84已經從一個向量中被創造，此向量包括有所有為零的數值，除了一個在關聯區的MSB。代號84中的同位元組82確認了被創造出來的代號中的聲音資料是正確的。藉由XORing 70產生主陪集(coset leader)90且84從代號84中併入了喀喀聲76及從主陪集(coset leader)70中併入了損壞的同位元位元組。因此，主陪集(coset leader)90顯示出喀喀聲76是無法修正的。假如在一聲音來源中，主陪集(coset leader)90以一個代號94被XORed，其中此聲音來源需要併入一喀喀聲，則產生的列100將包含所需要的聲音資料，亦即從列94中而來的、伴隨有喀喀聲76的聲音資料，但其藉由同位元位元組 72的存在以被標識為無法修正。

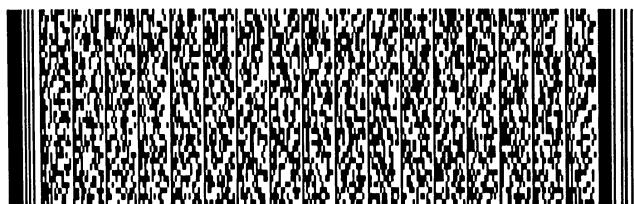
第八圖顯示一用於防止複製一音樂光碟的系統。如習知所示，一紅皮書編碼器50接受一進入的資料便於編碼和



五、發明說明 (26)

應用，藉由一雷射控制器52和一燒錄雷射54，到一母片碟片60。一般來說，進入紅皮書編碼器50的資料會是從來源62中的聲音資料。然而，依照本發明，如上所述，對聲音資料所做的改變係由於防止複製的軟體所引起的，其係從一防止複製的檔案來源係與聲音資料62縱向排列地被引入到紅皮書編碼器50。此系統用於第十圖中所描述的方法特別有用，當從來源62中讀取聲音資料62中被選擇的列94時，其能以創造出的主陪集(coset leaders)90被XORed。

以上僅為本創作之較佳具體例而已，並非用以限定本創作之申請專利範圍；凡其它未脫離本創作所揭示之精神下所完成之等效改變或修飾，均應包含在下述之申請專利範圍內。



圖式簡單說明

第1a圖係顯示一用於生成元矩陣的碼，第1b圖係顯示一藉由操作生成元矩陣而產生的標準陣列；

第二圖係顯示一光碟片的概略示意圖；

第三圖係顯示一光碟片上資料欄的格式；

第四圖係概略地顯示一CIRC編碼器，用於將被編碼至光碟片上的資料；

第五圖係顯示一編碼後的資料區塊；

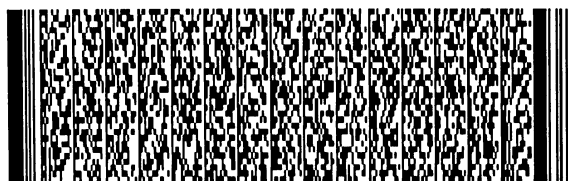
第六圖係顯示一CIRC解碼器；

第七圖係顯示一聲音播放器的概略示意圖；

第八圖係顯示一電路，用於提供本發明之防止複製的方法至一光碟片上；

第九圖係概略地顯示一方法，一聯結有同位元值（parity values）的聲音資料列，其定義該列為無法修正的；及

第十圖係概略地顯示一進一步的方法，一聯結有同位

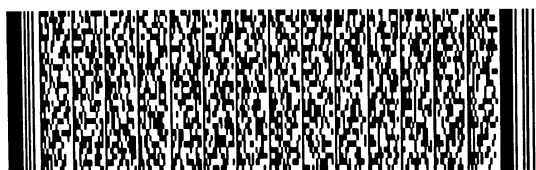


圖式簡單說明

元值 (parity values) 的聲音資料列，其定義該列為無法修正的。

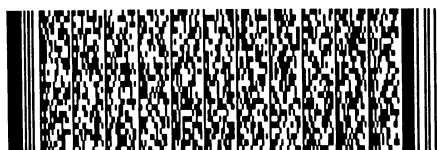
主要部份之代表符號

4	尖銳音軌
6	光碟片
8	導入區
10	音軌
12	導出區
14	1111
16	0100
18	1011
20	C2 編碼器
22	交錯器
24	C1 編碼器
26	資料列
28	資料列
30	C1 解碼器
32	8 個位元字元
34	C2 解碼器
36	紅皮書解碼器
38	聲音重製裝置
40	錯誤隱藏單元(插入裝置)
50	紅皮書編碼器



圖式簡單說明

- 52 雷射控制器
- 54 燒錄雷射
- 60 母碟片
- 62 聲音資料來源
- 70 主陪集(coset leader)
- 72、82 同位元位元組
- 74 列
- 76 喀喀聲
- 78 X0red
- 80 列
- 84 代號
- 90 主陪集(coset leader)
- 94 代號
- 100 列

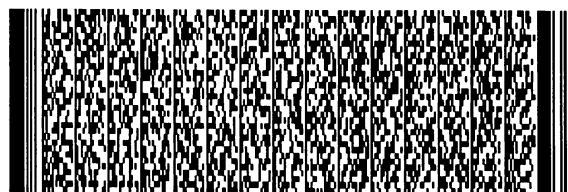
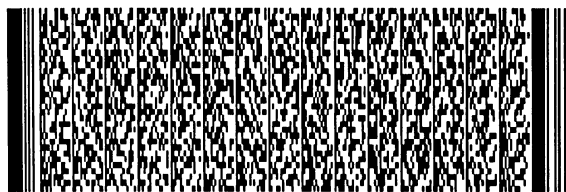


四、中文發明摘要 (發明之名稱：數位資料的複製保護方法)

在一保護編碼過之數位資料的系統中，例如：在一數位音樂光碟片(CD-DA)中，特定的聲音樣品被改變以引起尖銳，使得其播放時聽起來有喀喀的聲響。然後，在編碼資料中，包含有被改變過的樣品的所有代號被確認，且每一個代號中的資料將被改變使得在解碼時，這些代號能被定義為無法修正。因此，假如解碼出來的資料藉由聲音播放器播放時，錯誤的標幟便會可靠的出現，因為運用了隱藏性的錯誤，例如"中斷"，且將不會聽見尖銳聲。然而，一資料讀取裝置將可略過此不正確、未更改過的資料，或是試著修正它。因此，假如一聲音資料被複製，則在播放過程中將會聽見上述喀喀的聲響。

英文發明摘要 (發明之名稱：The Copy Protection of Digital Data)

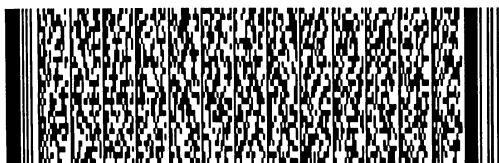
In a system for protecting encoded digital data, for example, on a digital audio compact disc (CD-DA), specific audio samples are altered to cause spikes which are audible as clicks if played. All of the codewords in the encoded data which contain those altered samples are then identified, and data in each codeword is changed such that on decoding, the codewords will be identified as uncorrectable. Thus, if the decoded data is played by an audio player, error flags are



四、中文發明摘要 (發明之名稱：數位資料的複製保護方法)

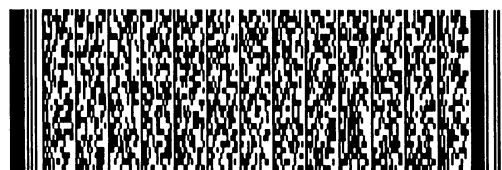
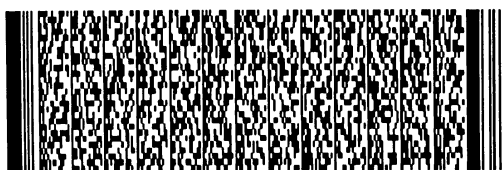
英文發明摘要 (發明之名稱：The Copy Protection of Digital Data)

reliably set so that error concealment, such as interpolation, is invoked and the spikes are inaudible. However, a data reader will either pass the uncorrectable data unchanged or will attempt to correct it. Therefore if a copy of the audio data is made, the clicks will be audible on playback.



六、申請專利範圍

1. 一種數位資料複製的保護方法，其可以在解碼後成功的插入或進行錯誤隱藏以並於播放，該方法包含下列步驟：
引入改變過的數值進入數位資料；
改變所有包含有引入的改變數值的所有代號，例如，在解碼過程中，該代號將被辨識為無法修正；且
其中，每一個代號藉由加入至少部份的其中的數值，一無法修正的錯誤的典型數值被定義為集合。
2. 如申請專利範圍第1項所述之數位資料複製的保護方法，其中每一個代號的4個位元組藉由加入4個位元組的集合代表數 (syndrome representative value) 。
3. 如申請專利範圍第2項所述之數位資料複製的保護方法，其中，所有被改變的4個位元組皆為同位元數值。
4. 如申請專利範圍第1項所述之數位資料複製的保護方法，其中，集合代表數至少為2個位元組。
5. 如申請專利範圍第1、2、3或4項所述之數位資料複製的保護方法，其中，集合代表數係為一集合的主陪集(coset leader)代表。
6. 如申請專利範圍第1、2、3或4項所述之數位資料複製的保護方法，其中，該集合係被製造的，在那裡，一錯誤定



六、申請專利範圍

位多項式在一解碼器中產生且不具有根值。

7. 如申請專利範圍第1、2、3或4項所述之數位資料複製的保護方法，被安排來保護將被播放的數位資料，例如一聲音、一虛擬圖像或一影像，其中，提供有一具有錯誤隱藏裝置的數位資料播放器，該方法包括有：

使用辨識為無法修正的代號以強制的讓改變過的資料數值在播放資料的期間內被一錯誤隱藏裝置處理。

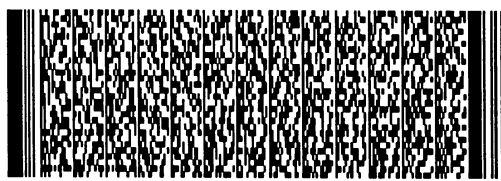
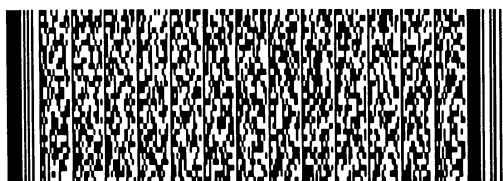
8. 如申請專利範圍第1項所述之數位資料複製的保護方法，其中，該改變過的數值係被製作為數位聲音資料。

9. 如申請專利範圍第8項所述之數位資料複製的保護方法，其中，該改變過的數值係藉由加入一大的數值到聲音資料數值而被引入。

10. 如申請專利範圍第9項所述之數位資料複製的保護方法，其中，加入到該聲音資料數值的該大的數值係為一2位元範圍(binary domain)，藉由加入一介於128至143間的數值到該聲音資料數值中的最高有效位元(MSB)。

11. 一種編碼數位資料的方法，該方法包括下列步驟：

改變從數位資料中產生的預先決定的代號，使得再解碼過程中，該代號能被定義為無法修正的，其中，每一個

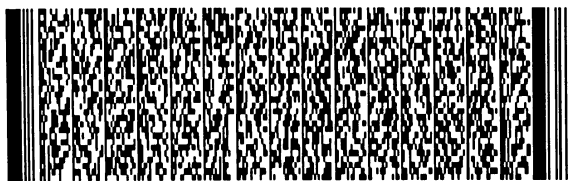


六、申請專利範圍

該代號藉由至少加入其中的一部份的數值而被改變，一無法修正的錯誤的典型數值被定義為集合。

12. 如申請專利範圍第1項所述之方法，用來改變數位資料的防止複製檔案，和由其中產生的代號。

13. 一儲存有防止複製的編碼過的數位資料的媒體，其可在播放時的解碼中被成功地被插入或進行錯誤隱藏，其中，該媒體記錄了包含有改變過的導入的數值的數位資料，且包含有改變過的導入的數值的代號，其已經被改變使得在解碼時會被定義為無法修正，其中，每一個代號藉由一至少加入其中的一部份的數值而被改變，一無法修正的錯誤的典型數值被定義為集合。



$$G = \begin{bmatrix} 1011 \\ 1101 \end{bmatrix}$$

圖 1a

函數 :	00	10	01	11	集合
碼 :	0000	1011	0101	1110	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
陪集 :	1000	0011	1101	0110	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
陪集 :	0100	1111	0001	1010	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
陪集 :	0010	1001	0111	1100	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

主陪集

圖 1b

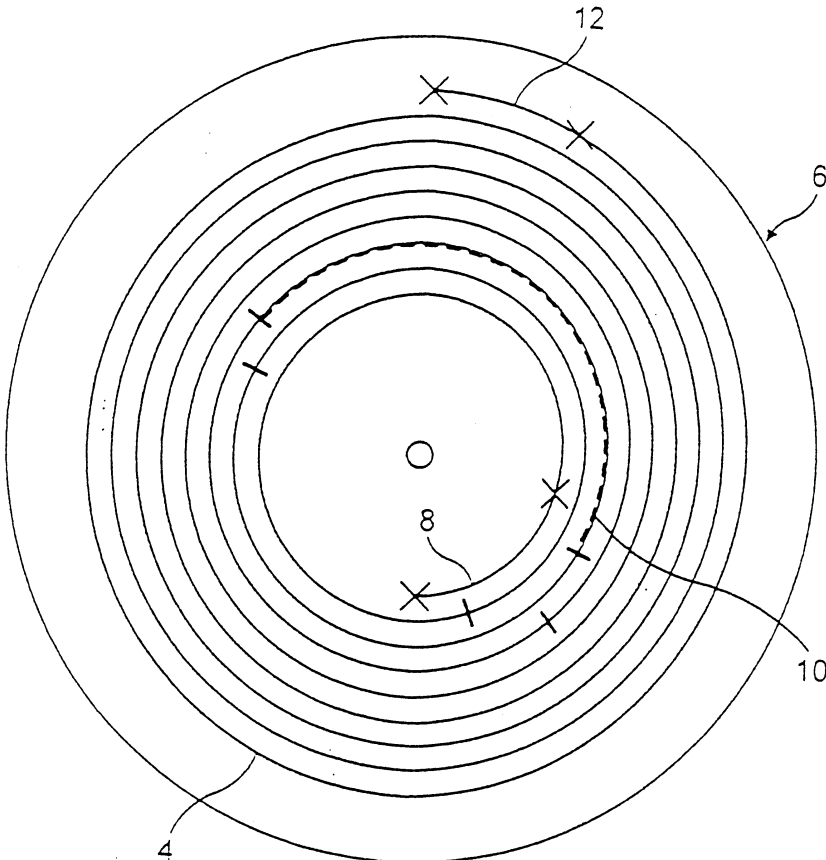


圖 2

8 / 8



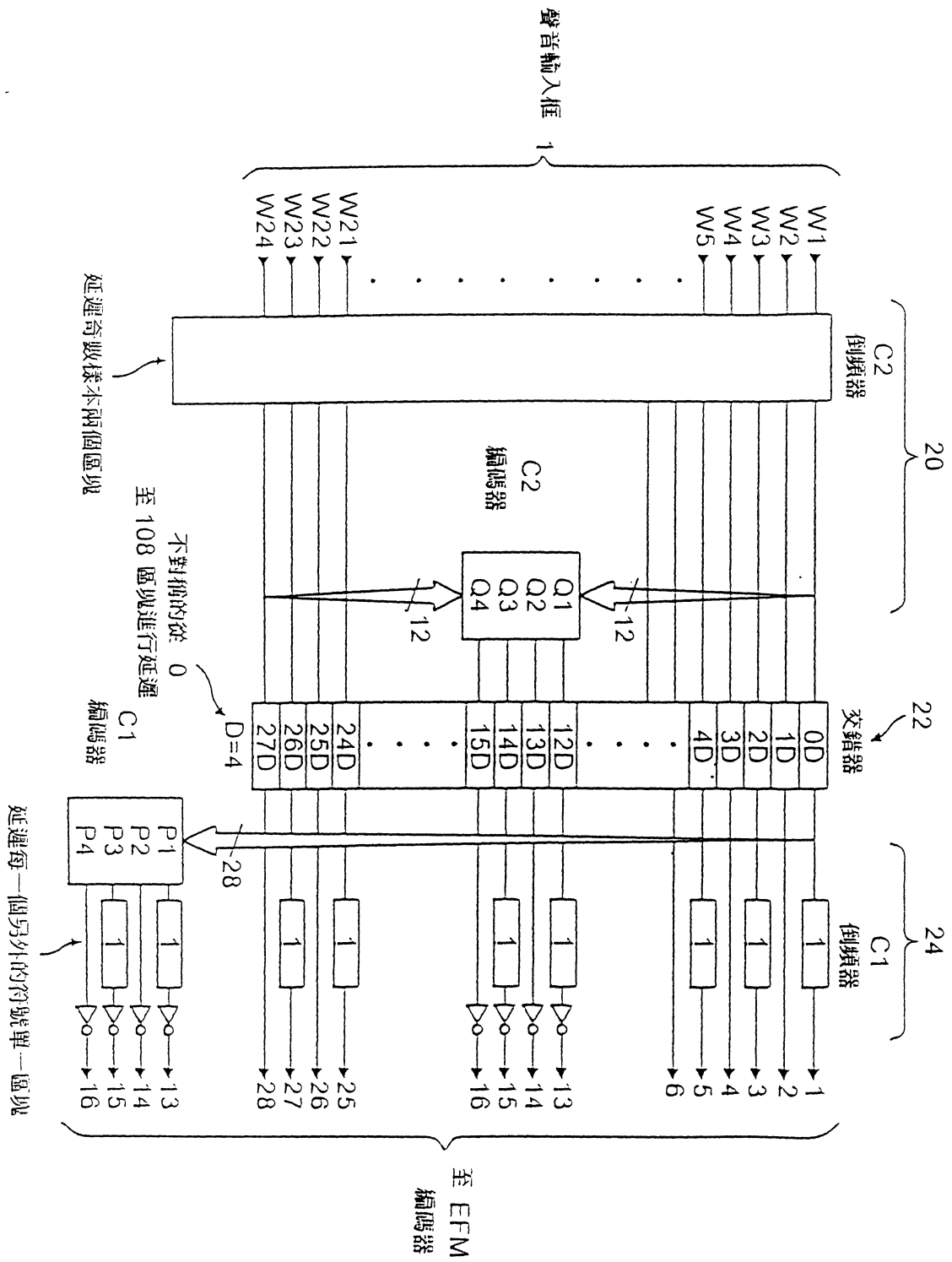
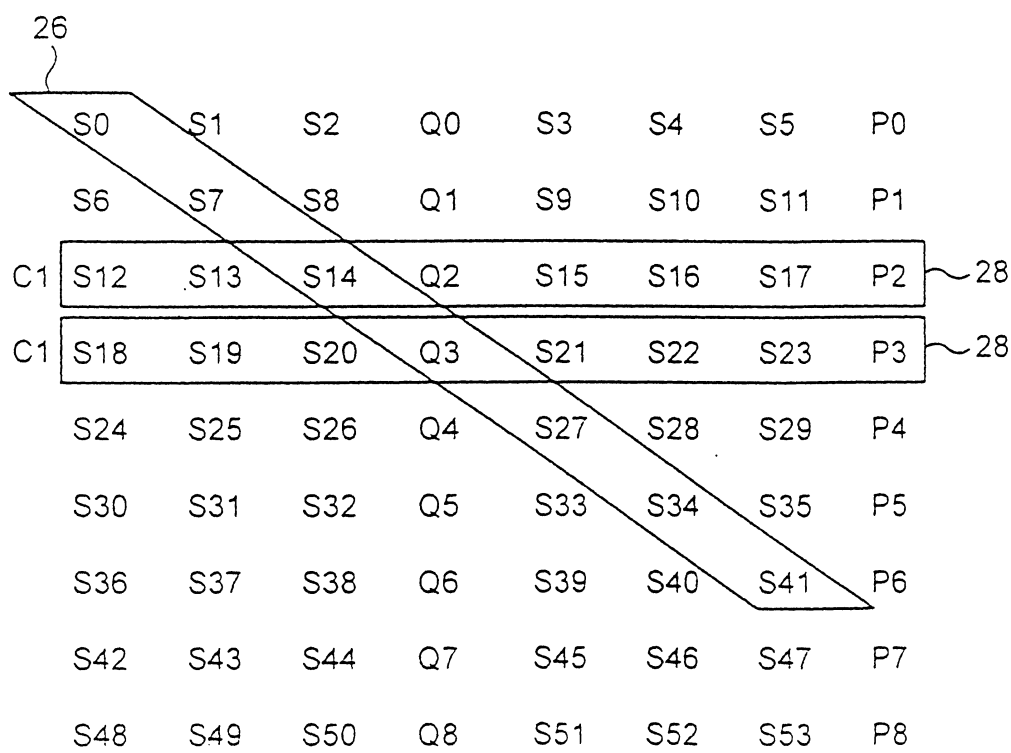
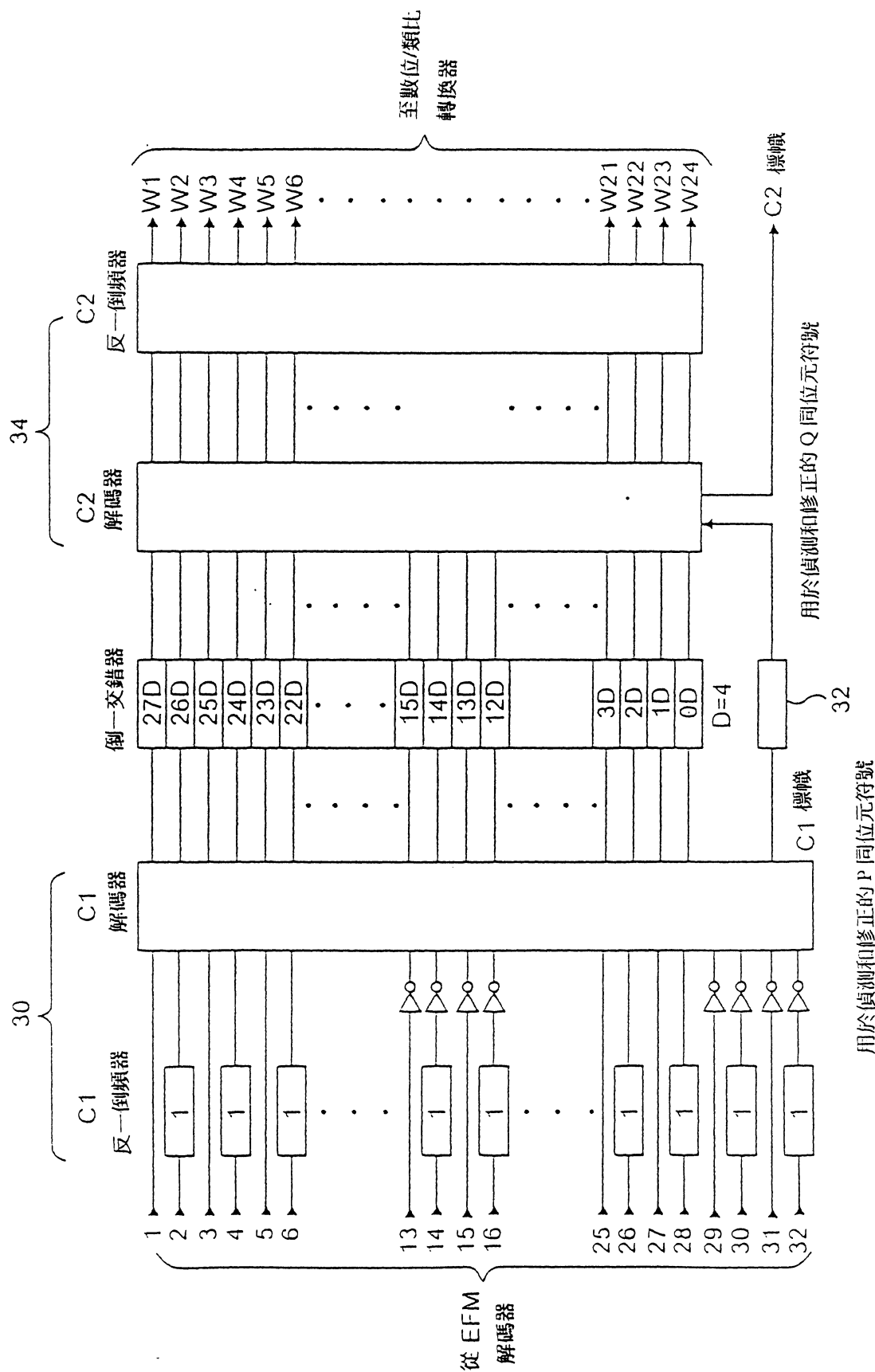
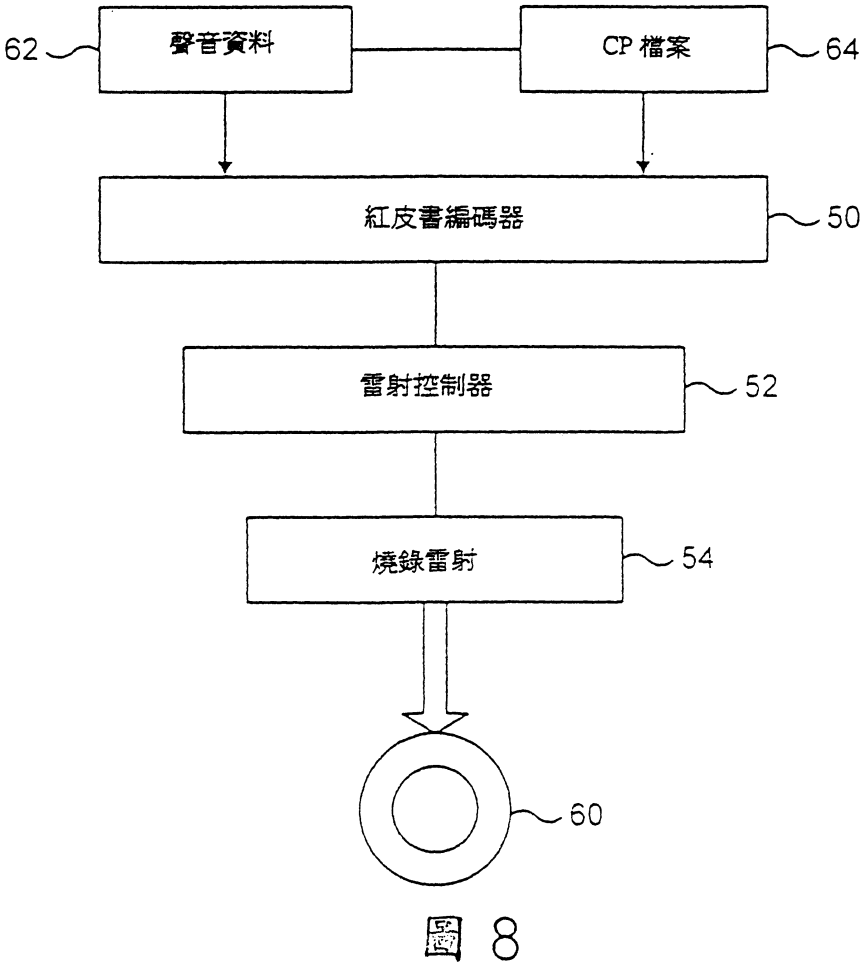
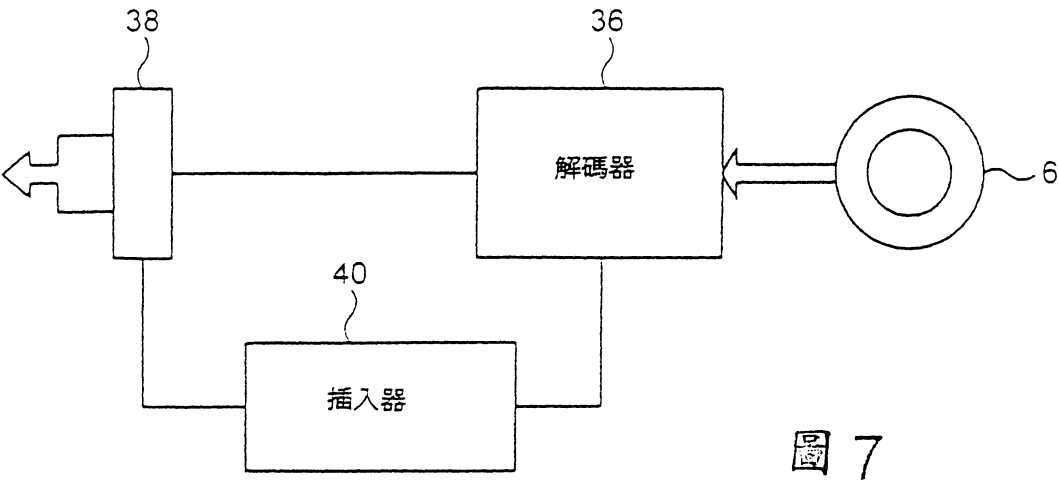


圖 4



5





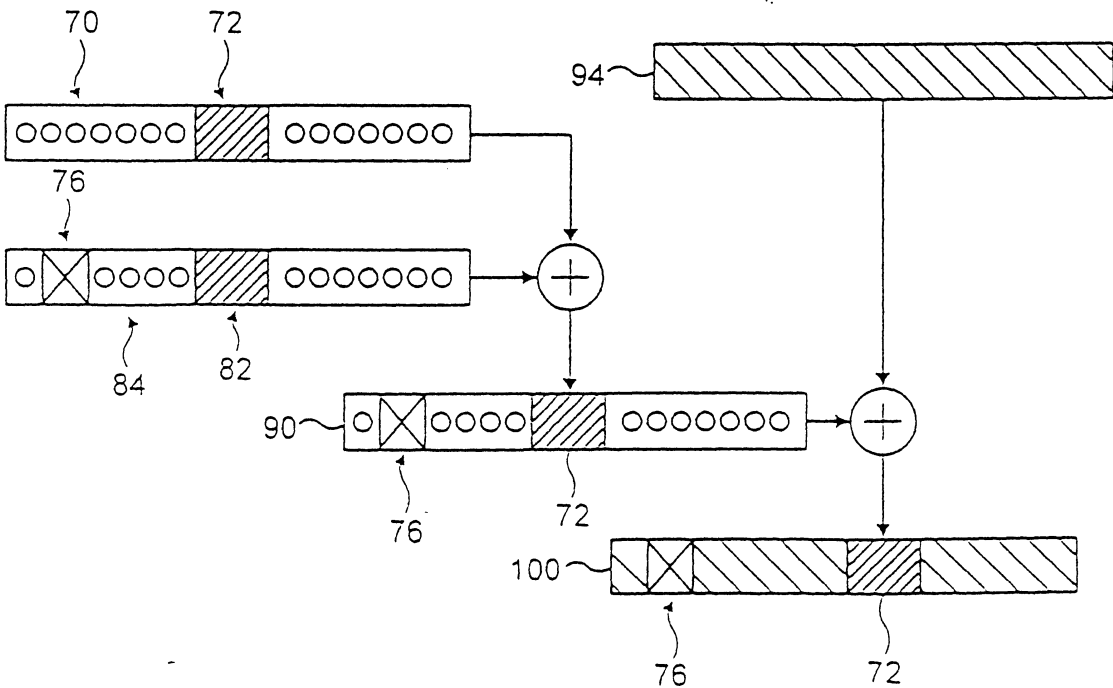
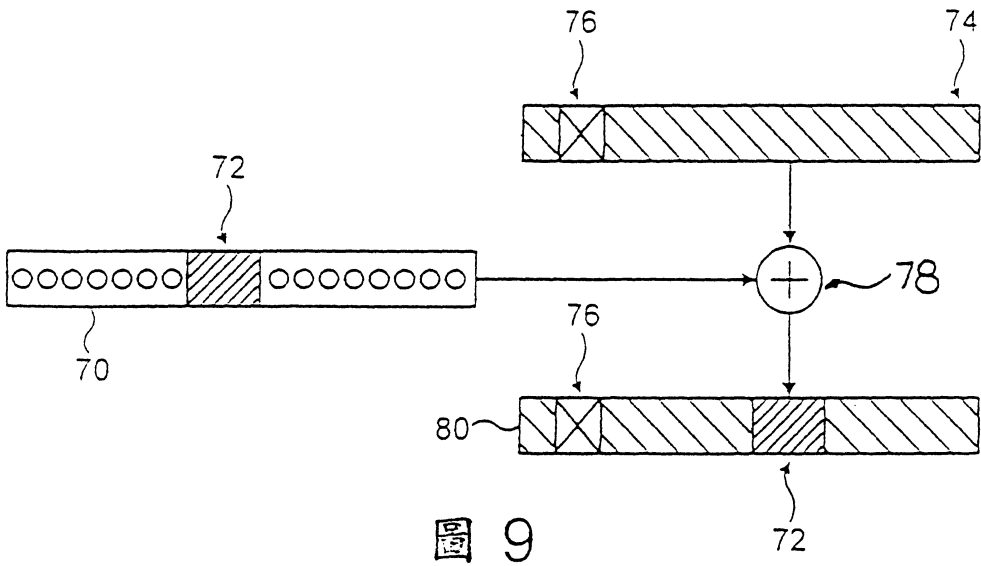


图 10

申請日期： 91.6.18

案號： 91113232

公告本

類別： G06F12/14, G11B20/00, H03M13/15

(以上各欄由本局填註)

92年10月2日 修正

發明專利說明書

565765

一、 發明名稱	中 文	數位資料的複製保護方法
	英 文	The Copy Protection of Digital Data
二、 發明人	姓 名 (中文)	1. 黑恩理查
	姓 名 (英文)	1. HEYLEN, Richard A. A.
	國 籍	1. 英國
	住、居所	1. 英國西約克夏郡里德市西公園歐特列227號
三、 申請人	姓 名 (名稱) (中文)	1. 寬視股份有限公司
	姓 名 (名稱) (英文)	1. Macrovision Corporation
	國 籍	1. 美國
	住、居所 (事務所)	1. 美國加州聖卡拉市酷茲道2830號
	代表人 姓 名 (中文)	1. 依凡羅伯特 哈里佛斯
	代表人 姓 名 (英文)	1. Ian Robert Halifax

