321764 公告本

321764

申請日期	85 年 6 月 4 日
案號	85106682
類別	Int. Cl6 G11B 20/18

A4
C4

（以上各欄由本局填註）

321764

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中文	資料記錄方法及裝置、資料記錄媒體、及資料再生方法及裝置
	英文	
二、發明 ~~創作~~ 人	姓名	(1) 佐古曜一郎 (2) 川嶋功 (3) 栗原章
	國籍	(1) 日本 (2) 日本 (3) 日本
	住、居所	(1) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
		(2) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
		(3) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
三、申請人	姓名（名稱）	(1) 蘇妮股份有限公司 ソニー株式会社
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國東京都品川區北品川六丁目七番三五號
	代表人姓名	(1) 出井伸之

裝 訂 線

經濟部中央標準局員工消費合作社印製

321764

申請日期	85 年 6 月 4 日
案號	85106682
類別	

A4
C4

（以上各欄由本局填註）

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中文	
	英文	
二、發明 ~~創作~~ 人	姓名	⑷ 大澤義知 ⑸ 応和英男
	國籍	⑷ 日本　　⑸ 日本
	住、居所	⑷ 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社 ⑸ 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
三、申請人	姓名（名稱）	
	國籍	
	住、居所（事務所）	
	代表人姓名	

裝 訂 線

經濟部中央標準局員工消費合作社印製

321764

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

國（地區）　申請專利，申請日期：　　案號：　　，□有　□無主張優先權

日本　　1995 年　6 月 30 日　　P07-166698　　☑無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

經濟部中央標準局員工消費合作社印製

五、發明說明（1）

〔發明所屬之技術領域〕

本發明係關於：能夠防止複製（copy）及不正使用，或是可適用於課金系統的資料記錄方法及裝置，資料記錄媒體、以及，資料再生方法及裝置。

〔先行技術〕

近年來，由於光碟等的數位記錄媒體的大容量化及普及，而使防止複製及不正使用變的很重要。即是，在數位音聲資料及數位影像資料的場合，可以很容易的由複製或傾卸複製（dumping）而產生無劣化的複製物，再者，在電腦資料的場合，因爲很容易使可複製出與原有的資料相同的資料，所以實際上不法複製已經產生了弊害。

〔發明所欲解決之課題〕

雖然爲了避免數位音聲資料及數位影像資料的不法複製，已有了所謂的ＳＣＭＳ（系列複製管理系統）及ＣＧＭＳ（複製世代管理系統）的規格，但是因爲這些方式均是在記錄資料的特定部份設置禁止複製旗標（flag），所以對將數位２值信號全部複製的所謂傾卸複製等的方法，會產生將資料挑出的問題。

再者，譬如說，在特開昭６０－１１６０３０號公報所示的，在電腦資料的場合，係將檔案內容本身暗號化，並僅對正式登記的使用者允許其使用。此對資訊流通的形態而言，係將資訊暗號化並使記錄了的數位記錄媒體廣爲

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（2）

流傳，而使用者對所要的內容付出金錢而得到關鍵資訊並破解暗號而能夠使用的系統，但是最好是能夠確立簡單而有用的暗號化手法。

本發明係有鑑於上述的情形，而提供：以簡單的構成來進行暗號化，而可以簡單的結構便可實現以資料的暗號化來防止複製及不正使用，並使暗號的解讀不易，且可容易的控制暗號的難易變成深度的控制的資料記錄方法及裝置、資料記錄媒體，以及，資料再生方法及裝置，爲目的。

〔用以解決課題之手段〕

爲了解決上述之課題，本發明的資料記錄方法的特徵係：在以所定資料量單位對輸入數位資料做磁區化的磁區化過程、及、附加上頭的頭附加過程、及、錯誤訂正過程、及、以所定的調變方式做調變的調變過程、及、附加同步樣式（pattern）的同步附加過程中的至少其中之一的過程中，對輸入進行暗號化處理而解決上述的課題。也可以使進行這些暗號化處理的過程之一包含：進行用以附去同步樣式的隨機（random）化處理的拌碼處理過程。

此資料記錄方法可適用於資料記錄裝置。

本發明也可提供記錄了：以上述記錄方法所得的信號，的資料記錄媒體。

本發明的資料再生方法係在將以上述資料記錄方法所記錄的資料記錄媒體再生時，在同步分離過程，解調過程

（請先閱讀背面之注意事項再填寫本頁）

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（ 3 ）

、錯誤訂正解碼過程，磁區化分解過程，以及、頭分離過程之中，至少對對應一個過程的記錄時的過程進行了暗號化處理，並在對應此記錄時進行了暗號化處理的過程的再生時的過程，藉由對輸入進行暗號的解碼處理而解決上述的課題。也可以使可進行這些暗號解碼處理的過程之一包含：進行解除記錄時的拌碼的解碼器（descranble）處理，的解拌處理過程。

此資料再生方法也可適用於資料再生裝置。

再者，本發明的資料記錄方法的特徵係：對錯誤訂正編碼處理時所處理的資料，依據暗號化的關鍵資訊而對至少一部份的資料進行資料變換。此資料變換可以是：資料及上述關鍵資訊的邏輯運算、及、轉置、置換等。

再者，本發明的資料記錄方法係藉由：使用所定的關鍵資訊而對資料進行暗號化處理，且係使用寫入於與記錄媒體的資料記錄區域不同區域的資訊來做爲此暗號化的關鍵資訊的至少一部份，來解決上述的課題。並使其他可適用於資料記錄裝置、資料記錄媒體。

再者，本發明的資料再生方法係藉由：在進行用以使對記錄時進行了暗號化處理的數位信號再生的信號處理時，使寫入於與資料記錄媒體的資料記錄區域不同的區域的資訊係使用至少一部份爲關鍵資訊，來進行暗號解碼處理；而解決上述的課題。並使其也可適用於資料再生裝置。

而且，本發明的資料記錄方法係藉由：依照暗號化的關鍵資訊而使拌碼處理過程的初期值及生成多項式的至少

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（ 4 ）

一方改變，而解決上述的課題。

再者，本發明的資料再生方法係藉由：依照記錄時的暗號化的關鍵資訊而使初期值及生成多項式的至少一方改變並進行解除拌碼的解拌碼處理，而解決上述的課題。

以所定資料量單位來將輸入數位資料做磁區化，附加上頭，並進行錯誤訂正編碼處理，以所定的調變方式做調變，並附加上同步樣式，而記錄到記錄媒體。在這些過程中的至少一個過程中，藉由對輸入進行暗號化處理並輸出，而使在那一個過程進行了暗號化處理成爲暗號的關鍵，而使暗號的難易度變高。

將暗號化的關鍵資訊的至少一部份寫入與記錄媒體的資料記錄區域不同的區域，在再生時，讀取此關鍵資訊的至少一部份的資訊、以使用於暗號解碼。因爲暗號解碼的關鍵資訊並不僅是記錄媒體的資料記錄區域內的資訊，所以可使暗號的難易度變高。

在進行以用以除去資料列的同一樣式的隨機化爲主目的的拌碼處理時，使生成多項式及初期值的至少一方會依照暗號化的關鍵而變化。而可將即存的拌碼處理也使用於暗號化。

〔發明之實施形態〕

以下，參照附圖來說明本發明的數個最佳實施形態。

圖 1 係概略的顯示本發明的第 1 實施形態的區塊圖。

在此圖 1 中，將，譬如說，數比的音聲信號及影像信

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部中央標準局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（5）

號做數位變換所得的資料及電腦資料等的數位資料供應到輸入端點１１。此輸入的數位資料則經由界面電路１２而送到磁區化電路１３，並以所定資料量單位，譬如說２０４８位元組（byte）單位來做磁區化。磁區化了的資料則被送到拌碼處理電路１４來進行拌碼處理。此場合的拌碼處理係將輸入資料隨機化而使同一樣式不會連續出現，即是除去同一樣式，進行以使信號能夠適當的讀寫爲主有的隨機化處理。做了拌碼處理或隨機處理的資料則被送到頭附加電路１５，並在對各磁區的前頭附加了配置的頭資料之後，送到錯誤訂正編碼電路１６。在錯誤訂正編碼電路１６則進行資料遲延及同位（parity）計算並附加上同位。而在其次的調變電路１７依照所定的調變方式而，譬如說，將８位元資料調變爲１６頻道（channel）位元的調變資料，並送到同步附加電路１８。在同步附加電路１８則打破上述所定的調變方式的調變規則，而以所定的資料量單位附加上所謂的超出規定（out-of-rule）的樣式的同步信號，並經由驅動電路即是驅動器１９而送到記錄頭２０。記錄頭２０係用以，譬如說，進行光學或磁性光學的記錄，係將上述調變了的記錄信號記錄到碟片狀的記錄媒體２１。此碟片狀記錄媒體２１則由軸馬達（spindle motor）２２所旋轉驅動。

再者，上述拌碼處理電路１４並非必需，再者，也可以將其插入到頭附加電路１５的後段，並在對頭加了的數位資料進行拌碼處理，將其送到錯誤訂正編碼電路１６。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（ 6 ）

此處，在磁區化電路１３、拌碼處理電路１４、頭附加電路１５、錯誤訂正編碼電路１６、調變電路１７、以及、同步附加電路１８中的至少１個的電路係：對輸入進行暗號化處理並輸出。最好是在２個以上的電路進行暗號化處理。此暗號化處理的關鍵資訊係使用：寫入到記錄媒體２１的資料記錄區域不同的區域的識別資訊，如，媒體固有的識別資訊，製造商識別資訊，販賣商識別資訊，或是，記錄裝置及編碼器的固有有識別資訊、切割機（cutting machine）及打印機（stamper）等的媒體製造裝置的固有的識別資訊、國別碼等的地域資訊，供應自外部的識別資訊等，至少做爲其一部份。如此，寫入到媒體的資料區域以外的識別資訊係，譬如說，從上述界面電路１２經由ＴＯＣ（table of contents）生成電路２３而送到端點２４的資訊，或是從界面電路１２直接的送到端點２５的資訊。來自這些端點２４，２５的識別資訊係使用爲暗號化時的關鍵資訊的一部份，並在電路１３～１８中的至少１個，最好是２個以上對使用此關鍵資訊的輸入資料進行暗號化處理。

在此場合，在電路１３～１８的那一個電路的暗號化處理的進行即成爲選擇分枝之一，且係爲在再生時用以獲得再生信號所必要的關鍵。即是，若在１個電路進行暗號化處理則必需要選擇６個選擇分枝之一，若在２個電路進行暗號化處理則必需要從相當於２個電路的組合數目的１５個選擇分枝之中選擇其一。在能夠在６個電路１３～

（請先閱讀背面之注意事項再填寫本頁）

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（ 7 ）

１８之中的１～６個電路進行暗號化處理的場合，選擇分枝變更多，很難以嘗試錯誤來找出此組合，而可充份達到暗號的作用。

再者，暗號化的關鍵資訊的所定定時（timing），譬如說，可以是以磁區化周期做切換。在以此所定定時來做關鍵資訊的切換的場合，也可以使用：是否進行切換、切換周期、複數的關鍵資訊的切換順序等的資訊來做爲關鍵；而更加提高暗號化的程度（level）或暗號的難易度、難解度、解讀的困難度。

其次，說明各電路１３～１８的構成及暗號化處理的具體例。

首先，在磁區化電路１３中可以是，譬如說，進行如圖２所示的偶數、奇數位元組的交錯（interleave）處理。即是，在圖２中，將上述圖１的界面電路１２的輸出送到２輸出的切換開關３１，並使此切換開關３１的一方的輸出經由偶奇交錯器３３而送到磁區化器３４，並將切換開關３１的另一方的輸出不改變的送到磁區化器３４。在磁區化器３４以，譬如說，輸入資料的２０４８位元組單位來做爲１磁區。並以關鍵的１位元的控制信號來控制：此磁區化電路１３的切換開關３２的切換動作。偶奇交錯器３３則將如圖３Ａ所示的以偶數位元組３６ａ及奇數位元組３６ｂ交互配置了的輸入資料的１磁區份，如圖３Ｂ所示的，分配爲偶數資料部３７ａ及奇數資料部３７ｂ並輸出。而且也可以是，如圖３Ｃ所示的，以關鍵資訊來特

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（8）

定１磁區內的所定的區域３９，而僅將此區域３９內的資料分配爲偶數資料部３９ａ及奇數資料部３９ｂ。在此場合，也可以將區域３９的特定方法設定爲能夠做複數種的選擇，而可更增加關鍵資訊的選擇分枝而能夠更提高暗號化的程度。

其次，在拌碼處理電路１４，譬如說如圖４所示的，可以使用１５位元的移位暫存器（stift register）的所謂平行區塊（parallel block）同步形的拌碼器。並以ＬＳＢ（最下位位元）在時間上優先的順序，即所謂ＬＳＢ先（ＬＳＢ first），將來自上述磁區化電路１３的電路輸入到此拌碼器的資料輸入用的端點３５。拌碼器用的１５位元的移位暫存器１４ａ則依據使用互斥邏輯合（ＥＸＯＲ）電路１４ｂ而產生的多項式$X^{15}+X+1$而加上回授（feedback），而在１５位元的移位暫存器１４ａ上則設定了如圖５所示的預置（pre-set）值（或初期值），圖５的預置值的選擇號碼則對應，譬如說，磁區位址的下位側４位元的值，並以磁區單位來切換預置值。以ＥＸＯＲ電路１４Ｃ來取得來自移位暫存器１４ａ的輸出資料與來自端點３５的輸入資料的互斥邏輯和，並從端點１４ｄ取出，並送到圖１的頭附加電路１５。

此處，可依據所定的識別號碼等的關鍵資訊而改變上述生成多項式及預置值（初期值）。即是，可以使用，譬如說，如圖６所示的構成而改變上述生成多項式。在此圖６中，將來自１５位元的移位暫存器１４ａ的各位元的輸

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（9）

出送到切換開關１４ｆ的各被選擇端點，並以，來自控制端點１４ｇ的，譬如說，４位元的控制資料來切換控制此切換開關，並將來自切換開關１４ｆ的輸出送到ＥＸＯＲ電路１４ｂ。並藉由改變此種構成的控制端點１４ｇ的控制資料便能夠改變生成多項式$X^{15}+X^{n}+1$的ｎ。再者，爲了改變上述預置值可以使上述圖５的預置值表的各預置值與，譬如說，１６位元組的識別資訊的各位元組值做邏輯運算。在此場合的識別資訊可以是使用：如上所述的媒體固有的識別資訊、製造商的識別資訊，販賣商識別資訊、及、記錄裝置及編碼器的固有的識別資訊、媒體製造裝置固有的識別資訊，地域資訊、外部所供應的識別資訊、或是其組合及與其它資訊的組合等；再者上述邏輯運算可以是使用：互斥邏輯和（ＥＸＯＲ）、及、邏輯積（ＡＮＤ）、邏輯和（ＯＲ）、移位運算等。再者，用以改變生成多項式的構成並不限於圖６的構造，也可以任意的改變位移暫存器的段數及取出的分枝（ｔａｐ）數。

其次，說明頭附加電路１５。

首先，圖７係顯示磁區格式（sector format）的具體例，１磁區係對２０４８位元組的使用者資料區域４１附加４位元組的同步區域４２、及、１６位元組的頭區域４３、及，４位元的錯誤檢出符號（ＥＰＣ）區域４４而構成。錯誤檢出區域４４的錯誤檢出符號係由對使用者資料區域４１及頭區域４３所產生的３２位元的ＣＲＣ符號所構成。在頭附加電路１５的暗號化處理可以是：對同期

（請先閱讀背面之注意事項再填寫本頁）
訂

經濟部中央標準局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（10）

所謂資料接收（data sink），對頭的位址及ＣＲＣ而進行。

以對磁區的同步即是資料接收進行暗號化處理的一例可以是：在將分配爲４位元組的同步區域４２的各位元組的位元組樣式分別表示於圖８的「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」時，可使用２位元的關鍵資訊，並以位元組單位將此４位元組的內容做移位或旋轉（rotate）。即是，藉由使其切換爲在２位元的關鍵爲「０」時爲「ＡＢＣＤ」、「１」時爲「ＢＣＤＡ」、「２」時爲「ＣＤＡＢ」、「３」時爲「ＤＡＢＣ」，而在此鍵不吻合時使其無法做磁區的同步，而無法正常的再生。再者，上述位元樣式「Ａ」～「Ｄ」可以是使用，譬如說，ＩＳ０６４６的字元碼（character code）等。

在頭區域４３內，如圖９所示的，設置了：所謂巡回符號的ＣＲＣ４５，用以做複製的許可／不許可及複製世代管理等的複製資訊４６，顯示多層碟片的某一層的層４７、位址４８、予備４９的各區域。在這其中，對位址４８的３２位元做位元拌碼，在此場合，藉由進行以位元單位的轉置處理而進行暗號化。再者，ＣＲＣ４５的生成多項式在使用$X^{16}+X^{15}+X^{2}+1$的場合，可以是依照其關鍵而改變對應X^{15}～Ｘ的１５位元來取代第２、第３項的X^{15}、X^{2}。再者，也可以是使ＣＲＣ１５的１６位元與關鍵資訊做邏輯運算。

再者，上述關鍵資訊，如上所述的，可以是使用：媒

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

五、發明說明（11）

體固有的識別資訊、製造商識別資訊、販賣商識別資訊、及、記錄裝置及編碼，或是媒體製造裝置的固有的識別資訊，地域資訊，供應自外部的識別資訊等，或是這些的組合或是與其它資訊的組合。

其次，在圖１０、圖１１中，在輸出端點５１，將來自上述圖１的頭附加電路１５的資料供應到第１符號化器的Ｃ１編碼器５２。在此具體例中，錯誤訂正符號化的一框架（frame）係設定爲由１４８位元組成１４８字元的資料所構成，並將來自輸入端點５１的數位資料每１４８位元組匯集一次而供應到第１符號化器的Ｃ１編碼器５２。在Ｃ１編碼器５２則附加上８位元組的Ｐ同位，再經由用以交錯的遲延電路５３而送到第２符號化器的Ｃ２編碼器５４。在Ｃ２編碼器５４附加上１４位元組的Ｑ同位，此Ｑ同位則經由遲延電路５５而掃還到Ｃ１編碼器５２。取出包含來自此Ｃ１編碼器５２的Ｐ、Ｑ相位的１７０位元組，並經由遲延電路５６，經由具有反相器（inventer）部５７ａ的再配列電路５７而從輸出端點５８取出，再送到圖１的調變電路１７。

在這種錯誤訂正編碼電路中，在進行暗號化處理的場合，譬如說，可以依據暗號的關鍵資訊而對再配列電路５７內的反相器部５７ａ的每一位元組選擇是否包括反相器。即是，在基準構成中，雖是對２２位元組的Ｐ、Ｑ同位由再配列電路５７的反相部器５７ａ的反相器的反相並輸出，但是，也可以去掉這些反相器中的數個，或是使

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

五、發明說明（12）

C1資料側包括數個的反相器並使其反相而輸出。

在進行這種資料變換的場合，錯誤訂正不能的比率會因爲基準構程的不同的程度而改變，而相對於在不同較少時再後的再生輸出的錯誤發生機率會稍微變高，在不同很多時，會無法對全體進行錯誤訂正而幾乎無法再生。即是，譬如說，以C1編碼器而言，因爲做爲顯示錯誤訂正能力的指標的所謂距離（distance）爲9，所以可進行最多4位元組的錯誤檢出訂正，而因爲若是有消失（erase）指示器則最多可做8位元的訂正，所以若是不同有5個以上則以C1碼便無法訂正或產生錯誤的訂正。而在不同爲4個的場合，若其它再有1位元組的錯誤產生便會成爲訂正不可的微妙狀態。而隨著不同爲3、2、1個的減少，可錯誤訂正的機率便會增加。若利用此點，在提供音聲及影像的軟體的場合，雖然在某些程度上可做再生但並不完全而有時會產生錯誤，而可積極的作出此種再生狀態，而可使用於僅告知該軟體的用途等。

在此場合，可以有：預先將進行反相器的變更的場所規定爲，譬如說，約2個左右的方法，及，依照關鍵資訊而隨機的選擇變更場所，而將最低個數限制爲2個地方左右的方法、及、複合這些方法等方法。

而且，以反相器的插入或變更位置而言，並不限定於圖10、圖11的再配列電路57內的位置，而，譬如說，也可以是C1編碼器52的前段及後段等的其它位置及這些位置的組合。在複數的位置的場合也可以是使用不同

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部中央標準局員工消費合作社印製

五、發明說明（13）

的關鍵。再者，以上述的資料變換而言，除了使用反相器之外，也可以是使用位元的加算及各種的邏輯運算、依據暗號化的關鍵資訊而將資料轉置，或是依據暗號化的關鍵資訊而將資料置換。再者，當然也可以是：使用移位暫存器來做變換，以各種函數運算而做變換等，而能夠適用各種的暗號化手法，而且也可以是將這些方法組合而使用。

此處，圖１２係以上述錯誤訂正編碼電路１６的其它的具體例而言，顯示：將互斥邏輯和（ＥＸＯＲ）電路群６１插入到再配列電路５７內的反相器部５７ａ的後段的位置，並將ＥＸＯＲ電路群６６也插入到Ｃ１編碼器５２的前段即是輸入側的位置，的例子。

具體而言，ＥＸＯＲ電路群６１係使用互斥邏輯和（ＥＸＯＲ）電路而對從Ｃ１編碼器５２並經過遲延電路５６及上述再述列電路５７的反相器部５７ａ而取出的１７０位元組的資料，即是，資訊資料$C1_{170n+169}$～$C1_{170n+22}$及同位資料$P1_{170n+21}$～$P1_{170n+14}$，$Q1_{170n+13}$～$Q1_{170n}$的資料進行資料變換，ＥＸＯＲ電路群６６則使用互斥邏輯和（ＥＸＯＲ）電路而對１４８位元組的輸入資料B_{148n}～$B_{148n+147}$進行資料變換。使用於這些ＥＸＯＲ電路群６１，６６的ＥＸＯＲ電路係分別取得１位元組即８位元的輸入資料，及、以１位元的控制資料所指示的所定的８位元資料，的互斥邏輯和（ＥＸＯＲ）的８位元ＥＸＯＲ電路；這種８位元ＥＸＯＲ電路（所定的８位元資料在均爲１的場合相當於

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（14）

反相器電路）在ＥＸＯＲ電路群６１使用１７０個，而在ＥＸＯＲ電路群６６則使用１４８個。

在此圖１２中，將１７０位元的關鍵資訊供應到端點６２，並經由所謂的Ｄ閂鎖（latch）電路６３而分別供應到ＥＸＯＲ電路群６１內的１７０個的各ＥＸＯＲ電路。Ｄ閂鎖電路６３則依照供應到置能（enable）端點６４的１位元的暗號化控制信號而做切換控制，使來自端點６２的１７０位元的關鍵資訊來改變的送到ＥＸＯＲ電路群６１，或是，全部設爲〝０〞，即是將１７０位元全部設爲〝０〞。在ＥＸＯＲ電路群６１的１７０個的各ＥＸＯＲ電路之中，從Ｄ閂鎖電路６３送來〝０〞的ＥＸＯＲ電路會將來自再配列電路５７內的反相器部５７ａ的資料不做改變的輸出，而從Ｄ閂鎖電路６３送來〝１〞的ＥＸＯＲ電路則屬將來自再配列電路５７內的反相器部５７ａ的資料反相再輸出。在全爲〝０〞的時候，會將來自再配列電路５７內的反相器部５７ａ的資料不做改變的輸出。再者，對ＥＸＯＲ電路６６而言，具有１４８個的ＥＸＯＲ電路，除了關鍵資訊爲１４８位元之外，均與上述ＥＸＯＲ電路群６１的場合相同，供應到端點６７的１４８位元的關鍵資訊會經由Ｄ閂鎖電路６８而分別送到ＥＸＯＲ電路群６６內的１４８個的ＥＸＯＲ電路，而且，Ｄ閂鎖電路６８則依據置能端點６９的暗號化控制信號而切換控制爲１４８位元的關鍵資訊，或是，全部爲〝０〞。

（請先閱讀背面之注意事項再填寫本頁）

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（15）

在此圖１２的例中，ＥＸＯＲ電路群６１係使用互斥邏輯和（ＥＸＯＲ）電路而對從Ｃ１編碼器５２並經由遲延電路５６、反相器部５７ａ所取得的１７０位元組的資料的資訊資料$C1_{170n+169}$～$C1_{170n+22}$、及、同位資料$P1_{170n+21}$～$P1_{170n+14}$、$Q1_{170n+13}$～$Q1_{170n}$的資料進行資料變換，但是，也可以是不對同位資料進行資料變換，而對剩餘的１４８位元組的資訊資料$C1_{170n+169}$～$C1_{171n+22}$使其依據１４８位元的關鍵資訊而進行資料變換。

在此圖１２的電路中，當然也可以得到與在上述圖１０、圖１１的場合的場合同樣的效果。再者，也可以是僅使用ＥＸＯＲ電路群６１，６６其中之一，及，使用其中一方或雙方的選擇來做爲暗號化的關鍵。

上述關鍵資訊係，如上所述的，可以是使用：媒體固有的識別資訊、製造商識別資訊、販賣商識別資訊、及、記錄裝置及編碼器或是媒體製造裝置的固有的識別資訊，地域資訊，供應自外部的識別資訊等，或是這些資訊的組合及與其它資訊的組合。

再者，以上述資料變換手段而言，也可以是使用ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ、反相器電路群等以取代ＥＸＯＲ電路群６１、６６。再者，除了以８位元單位來進行１位元的關鍵資訊或關鍵資料的邏輯運算之外，也可以是對８位元的資訊資料以８位元的關鍵資料來進行羅輯運算，而且；對相當於資訊資料的１字元的８位元之中

（請先閱讀背面之注意事項再填寫本頁）
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（16）

的各位元而言，也可以是分別使用ＡＮＤ、ＯＲ、ＥＸＯＲ、ＮＡＮＤ、ＮＯＲ、反相器電路的組合。在此場合，譬如說，對１４８位元組即是１４８×８位元的資料而言，會是使用１４８×８位元的關鍵資料，而且，在使用組合ＡＮＤ、ＯＲ、ＥＸＯＲ、ＮＡＮＤ、ＮＯＲ、反相器電路的場合，也可以使用這些的組合本身來做爲關鍵。再者，除了邏輯運算之外，也可以使用改變資料的位置的轉置，及、置換資料的值的置換來做爲上述的資料變換。再者，當然，使用移位暫存器做變換、以各種函數做變換等，各種暗號化手法也都可適用，也可以使用這些方法的組合。

而且，在此第１實施形態中，雖然是以交互交錯（cross interleave）型的錯誤訂正碼的例子來做說明，但是也可適用於積碼的場合，此點將後述爲本發明的第２實施形態。

其次，參照圖１３來說明圖１的調變電路１７的暗號化處理。在此圖１３中，將來自上述錯誤訂正編碼電路１６的資料每次供應８位元（１位元組）到輸入端點７１，並供應８位元的關鍵資訊到輸入端點７２，這些８位元資料則被送到做爲邏輯運算電路的１例的ＥＸＯＲ電路７３，並求出其互斥邏輯和。來自此ＥＸＯＲ電路７３的８位元輸出則被送到所定的調變方式的調變器，譬如說，８－１６變換電路７４，而轉變成１６頻道位元（channelbit）。以此８－１６變換電路７４的８－１６調變方

（請先閱讀背面之注意事項再填寫本頁）

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（17）

式的一例而言，如所謂的ＥＦＭ加（plus）調變方式。

在此圖１３的例中，雖然在資料調變之前使用８位元的關鍵資訊而進行了暗號化處理，但是關鍵資訊的位元數並不限定爲８位元，再者，也可以是依照關鍵資訊而改變在做８－１６調變時的變換表的輸出入的對應關係。而關鍵資訊則當然可以使用上述的媒體固有的識別資訊等。

其次，說明同步附加電路１８。

在同步附加電路１８中，譬如說，使用如圖１４所示的４種類的同步字元Ｓ０～Ｓ３，並以上述８－１６調變的框架（frame）單位取得同步。此８－１６調變框架（譬如說，ＥＦＭ加框架）係由８５資料碼（data symbal）的１３６０通道位元所構成，並對每１個此１框架１３６０頻道位元附加上３２通道位元的同步字元，而且，對此框架對應上述Ｃ１碼及Ｃ２碼而做構造化，並使Ｃ１碼系列的前頭框架的同步字元與其它的框架的同步字元不同等，而分別使用上述４種類的同步字元Ｓ０～Ｓ３。這些同步字元Ｓ０～Ｓ３則依據前面的字元的〝１〞，〝０〞的狀態及所謂的數位和（digital sum）或直流值等而分別具有２個的同步樣式ａ、ｂ。

譬如說，使用如圖１５所示的電路，並藉由依２位元的關鍵資訊７５來改變此種４種類的同步字元Ｓ０～Ｓ３的選擇而進行暗號化。即是，使指定４種類的同步字元Ｓ０～Ｓ３的２位元資料７６的各位元、及、上述２位元的關鍵資訊７５的各位元分別由２個的ＥＸＯＲ電路７７

（請先閱讀背面之注意事項再填寫本頁）

訂

經濟部中央標準局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（18）

、７８而做互斥邏輯和，而形成新的同步字元指定資料７９。由此，在上述框架構造中，使同步字元的使用方法或是框架構造內的各種同步字元的使用位置做改變，而進行暗號化。

再者，也可以再增加同步字元的種類數目，而由暗化號的關鍵來決定從這其中取出４種類的同步字元的取出方法。此種關鍵資訊則可以使用上述的媒體固有的識別資訊等。

其次，圖１６顯示做爲記錄媒體的一例的光碟等的碟片狀記錄媒體１０１。此碟片狀記錄媒體１０１在中央有中央孔１０２，並從此碟片狀記錄媒體１０１的內側向著外側形成：做爲程式管理區域的ＴＯＣ（table of contents）區域的導入（lead in）區域１０３、及、記錄了程式資料的程式區域１０４、及、程式結束區域，所謂的導出（lead out）區域１０５。在音聲信號及影像信號再生用光碟中，在上述程式區域１０４記錄了音聲及影像資料，此音聲及影像資料的時間資訊則在上述導入區域１０３做管理。

以上述關鍵資訊而言，可以使用寫入到做爲資料記錄區域的程式區域１０４以外的區域的識別資訊等。具體而言，在做爲ＴＯＣ區域的導入區域１０３及導出區域１０５寫入：識別資訊、譬如說媒體固有的製造號碼等的識別資訊、製造商識別資訊、販賣商識別資訊，或是，記錄裝置及編碼器的固有的識別資訊，切割機及打印機等的

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（19）

媒體製造裝置的固有的識別資訊，而且，以這些資訊做爲關鍵資訊，而將以上述6個電路13～18的至少1個，最好是2個以上進行暗號化處理而得到的信號記錄到做爲資料記錄區域的程式區域104。在再生時，只要使用上述識別資訊來做爲用以將暗號解碼的關鍵資訊即可。再者，也可以在導入區域103的內側以物理的或化學的寫入識別資訊，並在再生時將其讀取出，而使用爲用以將暗號解碼的關鍵資訊。

其次，參照圖17來說明本發明的資料再生方法，資料再生裝置的實施形態。

在圖17中，做爲記錄媒體的一例的碟片狀記錄媒體101則由軸馬達108而做旋轉驅動，並由光學拾取（pickup）裝置等的再生頭裝置109而讀取媒體記錄內容。

由再生頭裝置109所讀取的數位信號則被送到TOC解碼器111及放大器112。從TOC解碼器（decoder）111則讀取記錄於碟片狀記錄媒體101的上述導入區域103以做爲TOC資訊的一部份的上述識別資訊，譬如說，媒體固有的製造號碼等的識別資訊，製造商識別資訊，販賣商識別資訊，或是，記錄裝置及編碼器的固有的識別資訊，切割機及打印機等的媒體製造裝置的固有的識別資訊，而此識別資訊則被使用爲用以將暗號解碼的關鍵資訊的至少一部份。此外，也可以是從再生裝置內部的CPU122輸出再生裝置固有的識別資訊，及

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

五、發明說明（20）

，來自外部的資訊，並將此識別資訊做爲關鍵資訊的至少一部份。再者，以來自外部的識別資訊而言，可以是：經由通信電路及傳送路等而受信的識別資訊、及、讀取所謂ＩＣ卡、ＲＯＭ卡、磁卡、光卡等所得的識別資訊等。

從再生頭裝置１０９經由放大器１１２、ＰＬＬ（相鎖迴路）電路１１３所取得的數位信號則被送到同步分離電路１１４，並對在上述圖１的同步附加電路１８所附加的同步信號進行分離。來自同步分離電路１１４的數位信號則被送到解調電路１１５，並對上述圖１的調變電路１７的調變進行解調處理。具體而言，進行將１６頻道位元轉換爲８位元的資料的處理。來自解調電路１１５的數位資料則被送到錯誤訂正解碼電路１１６，並進行做爲在圖１的錯誤訂正編碼電路１６的編碼的逆處理的解碼處理。以下，在磁區分解電路１１７分解爲磁區，並在頭分解電路１１８將各磁區的前頭部份的頭分離。而此磁區分解電路１１７及頭分解電路１１８則係對應上述圖１的磁區化電路１３及頭附加電路１５。其次，由解拌碼（de-scramble）處理電路１１９進行做爲上述圖１的拌碼處理路１４的拌碼處理的逆處理的解拌碼處理，並經由界面電路１２０而從輸出端點１２１取出再生資料。

此處，如上所述的，在記錄時，在上述圖１的磁區化電路１３，拌碼處理電路１４、頭附加電路１５、錯誤訂正編碼電路１６、調變電路１７、以及、同步附加電路１８的至少其中之一的電路中進行暗號化處理，而在對應

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（21）

此進行了此暗號化處理的電路的再生側的電路１１４～１１９，必需進行將暗號解碼。即是，在上述圖１的磁區化電路１３進行暗號化處理的場合，在磁區分解電路１１７必需對在暗號化時使用的關鍵資訊的暗號進行解碼處理。以下，相同的，對應在圖１的拌碼處理電路１４的暗號化處理必需要在解拌碼處理電路１１９進行暗號解碼處理；而對應在圖１的頭附加電路１５的暗號化處理必需要在頭分解電路１１８進行暗號解碼處理；對應在圖１的錯誤訂正編碼電路１６的暗號化處理必需在錯誤訂正解碼電路１１６進行暗號解碼處理；對應在圖１的調變電路１７的暗號化處理必需在解調電路１１５進行暗號化解碼處理，而且，對應在圖１的同步附加電路１８的暗號化處理必需在同步分離電路１１４進行暗號化解碼處理。

在同步分離電路１１４進行的暗號化處理係，如上述圖１４及１５所共同說明的，複數種類、譬如說，４種類的同步字元的使用方法或框架構造內的各種同步字元的使用位置會依照關鍵資訊而變更，並依據關鍵資訊而讀出被暗號化了的地方。

其次，在解調電路１１５所進行的暗號解碼處理係，如圖１８所示的，將來自同步分離電路１１４並被送到１６－８變換電路１３１的１６頻道位元轉變爲８位元資料者，送到對應於上述圖１３的ＥＸＯＲ電路７３的ＥＸＯＲ電路１３２，並藉由取得其與來自端點１３３的８位元的關鍵資訊的互斥邏輯和，而使相當於被供應到圖

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（22）

１３的輸入端點７１的８位元資料的資料復元，並將其送到錯誤訂正解碼電路１１６。

其次，在錯誤解碼電路１１６由圖１９，圖２０的構成來進行如上述圖１０、圖１１的錯誤訂正編碼處理的逆處理。

在此圖１９、圖２０中，將在上述解調電路１１５所解調的資料的１７０位元組成１７０碼（synbol）整合爲１，並經由具有反相器部１４２a的再配列電路１４２，經由遲延電路１４３而送到做爲第１解碼器的Ｃ１解碼器１４４。在被供應到此Ｃ１解碼器１４４的１７０位元組的資料之中，２２位元組係Ｐ，Ｑ同位，而在Ｃ１解碼器１４４則使用此同位資料而進行錯誤訂正解碼。從Ｃ１解碼器１４４輸出１７０位元組的資料並經由遲延電路１４５而送到做爲第２解碼器的Ｃ２解碼器１４６，並使用同位資料來進行錯誤訂正解碼。將輸出自Ｃ２解碼器１４６的資料送到圖１９的遲延・Ｃ１解碼電路１４０。這１點係與上述遲延電路１４３及Ｃ１解碼器１４４相同，係藉由重覆的進行與此遲延電路１４３及Ｃ１解碼器１４４相同的處理而進行錯誤訂正解碼。在圖８的例中，係以遲延電路１４７及做爲第３解碼器的Ｃ３解碼器１４８所表示。在此遲延電路１４７及Ｃ３解碼器１４８，或是、遲延。Ｃ１解碼器電路１４０進行最後的錯誤訂正解碼，並經由輸出端點１４９而取出無同位的１４８位元組的資料。此１４８位元組的資料係相當於被輸入到上

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（23）

述圖１０、圖１１的Ｃ１編碼器５２的１４８位元組的資料。

而且，在圖１０、圖１１的錯誤訂正編碼電路的再配列電路５７內的反相器部５７ａ，在以是否有反相器而進行暗號化的場合，在圖１９，圖２０的錯誤訂正解碼電路的再配列電路１４２內的反相器部１４２ａ，必需進行對應的暗號解碼。此外，當然，也需要進行，用以解除對應說明於圖１０、圖１１的各種暗號化處理的暗號化的逆處理的暗號解碼。

此處，圖２１係顯示對應上述圖１２的錯誤訂正編碼電路的具體構成的錯誤訂正解碼電路的具體構成的圖。

在此圖２１中，對應於插入到上述圖１２的再配列電路５７內的反相器部５７ａ的輸出側的ＥＸＯＲ電路群６１，而將ＥＸＯＲ電路群１５１插入到再配列電路１４２的反相器部１４２ａ的輸入側及遲延電路１４３的輸入側的位置；並對應插入到圖１２的ｃ１編碼器５２的輸入側的ＥＸＯＲ電路群６６，而將ＥＸＯＲ電路群１５６插入到Ｃ３解碼器１４８的輸出側。

這些ＥＸＯＲ電路群１５１、１５６係，如上所述的，進行：用以將圖１２的ＥＸＯＲ電路群６１、６２的資料變換分別解碼的資料變換；ＥＸＯＲ電路群１５１則係，譬如說，由１７０個的８位元ＥＸＯＲ電路所構成，而ＥＸＯＲ電路群１５６則係由１４８個的８位元ＥＸＯＲ電路所構成，再者，在記錄側的圖１２的錯誤訂正編碼電

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（24）

路ＥＸＯＲ電路群６１，在依據關鍵資訊而對除了同位資料以外的１４８位元組的資訊資料進行資料變換的場合，當然，ＥＸＯＲ電路群１５１係由１４８個的8位元ＥＸＯＲ電路所構成。

將相當於被供應到圖１２的端點６２的關鍵資訊的１７０位元的關鍵資訊供應到此圖２１的端點１５２，並經由所謂的Ｄ閂鎖（latch）電路１５３而分別供應到ＥＸＯＲ電路群１５１內的１７０個的各ＥＸＯＲ電路。Ｄ閂鎖電路１５３則依據供應到置能端點１５４的1位元的暗號化控制信號，而將來自端點１５２的１７０位元的關鍵資訊未改變的送到ＥＸＯＲ電路群１５１，或是，將其設爲全零，即是將１７０位元均設爲〝０〞。再者，對ＥＸＯＲ電路群１５６而言，除了具有１４８個ＥＸＯＲ電路，且其關鍵資訊係與供應到圖１２的端點６７的關鍵資訊同樣爲１４８位元之外，係與上述ＥＸＯＲ電路群１５１的場合同樣的，係經由Ｄ閂鎖電路１５８而將被供到端點

１５７的１４８位元的關鍵資訊分別送到ＥＸＯＲ電路群１５６內的１４８個的ＥＸＯＲ電路，而且，Ｄ閂鎖電路係依據置能端點１５９的暗號化控制信號而切換控制爲：１４８位元的關鍵資訊或全零。

如此，藉由使用錯誤訂正電路的反相器及ＥＸＯＲ電路等以做爲暗號化的關鍵，便可很容易的實現大的暗號化。再者，藉由控制此反相器等的數目，便可依據安全位準

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（25）

（security level）而對應爲：即時平時也是無法再生的暗號位準的資料，或是，在錯誤（error）狀態變差時爲無法再生的資料。即是，藉由控制反相器及ＥＸＯＲ電路等的個數，便可控制爲：在錯誤狀態良好時能夠再生而變壞時便無法再生，再者，也能夠形成爲僅靠錯誤訂正無法回復的無法再生狀態。再者，因爲暗號化的關鍵係如上述圖示的例一般的，在一個地方會具有一百多位元而能夠使暗號化的關鍵的位元數目變大，因此也可以改善資料安全性。而且，藉由將這種錯誤訂正編碼電路及錯誤訂正解碼電路實現於所謂的ＬＳＩ及ＩＣ晶片（chip）的硬體內，便使一般使明者很難獲得而以此點而言也可提高其資料安全性。

其次，在磁區分解電路１３中，如上述圖２，圖３所說明的，在記錄時在上述磁區化電路１３以偶數、奇數位元組的交錯而進行暗號化的場合，則進行可解除此偶奇交錯的逆處理，即所謂的解交錯處理。

再者，在頭分解電路１１８中，在記錄時，在上述頭附加電路１５中，在進行了上述圖７～圖９所說明的暗號化處理，即使磁區同步的資料接收的位元組樣式（byte pattern）的轉置、及、位址、ＣＲＣ的變更的場合，則進行暗號解碼處理以使其復元。

其次，圖２２顯示解拌碼處理電路１１９的具體例，係將來自圖１７的頭分解電路１１８的數位資料供應到端點１６１。並，譬如說，在具有如上述圖４所示的構成的

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（26）

解拌碼１６３對來自此端點１６１的數位資料進行解拌碼處理，並由輸出端點１６４取出。並藉由使此解拌碼１６３的上述圖４所說明的生成多項式１６５及預置值（或初期值）１６６會依照來自認證機構１７１的暗號的關鍵資訊而產生變化，而能夠進行暗號解碼。在此認證機構１７１，則由上述頭資訊１６７的複製資訊４６的內容，及，媒體固有的或再生裝置固有的固有識別資訊１７２，及，製造商、販賣商等的共通識別資訊１７３、及，供應自外部的外部識別資訊１７４等，而產生暗號的關鍵資訊；並依據此關鍵資訊而控制生成多項式１６５及預置值１６６。

在這些各電路１１４～１１９中是否需要進行暗號解碼處理的資訊，也如前述的，使其成爲暗號的關鍵資訊。再者，也能夠以所定周期，譬如說磁區周期，來切換暗號的關鍵資訊，並藉由使是否進行此切換，及，切換周期等也設爲關鍵，便可提高暗號化的困難度。

如以上所說明的，藉由組合製造商識別資訊，販賣商識別資訊，裝置識別資訊等，與別外設定的複製防止資訊、課金資訊來將資料暗號化並做記錄，便能夠以物理方式來實現複製防止、海盜盤防止、不正使用的防止等。再者，也能夠將資料安全功能的資訊、如複製允許／不允許資訊，有償／無償資訊實現（implement）爲記錄媒體及記錄／再生系統的物理樣式。

即是，藉由將安全／收費資訊預先記錄於媒體，使用

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（27）

記錄或未記錄於媒體的識別資訊並使其與資料暗號化組合，便能夠以簡單的裝置來防止複製及不正使用。再者，藉由使其係內在於物理樣式便可使其難以解讀。再者，因爲即使被傾卸複製也仍然是暗號化了所以很安全。而且，可以以磁區單位及檔案單位及區（zone）單位及層（layer）單位等來做改變。而且，也可以以通信及ＩＣ卡及遙控等方式來控制。而且，對海盜盤會留下記號。

其次，說明本發明的第２實施形態。

此第２實施形態係將上述第１實施形態的構成做部份變更，其全體構成係如前述圖１所示。以下說明此圖１的構成的各電路１３～１８內的變更部份。

圖１的磁區化電路１３係與前述的第１實施形態具有相同即可，但是拌碼處理電路１４則是使用圖２３所示的構成。

在此圖２３所示的拌碼處理電路１４中，在時間上以ＬＳＢ（最下位位元）先的順序，即所謂ＬＳＢ先而將來自圖１的磁區化電路１３的資料輸入到資料輸入用的端點３５。拌碼用的１５位元的移位暫存器１４ａ則連到依據使用互斥邏輯和（ＥＸＯＲ）電路１４ｂ的生成多項式 $X^{15}+X^{4}+1$ 的回授（feedback），並在１５位元的移位暫存器１４ａ設定如圖２４所示的預置值（或初期值）。圖２４的預置值的選擇號碼則對應，譬如說，磁區位址的下位側４位元的值，而以磁區爲單位切換預置值。在ＥＸＯＲ電路１４Ｃ則求得來自移位暫存器１４ａ的輸出

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

五、發明說明（28）

資料、及，來自端點35的輸入資料的互斥邏輯和，端點14d取出並送到圖1的頭附加電路15。

此處，可依照所定的識別號碼等的關鍵資訊而改變上述預置值（初期值）。即是，可以是上述圖24的預置值表的各預置值與，譬如說，16位元組的識別資訊的各位元組值的邏輯運算。在此場合的識別資訊可以是使用：如上所述的媒體固有的識別資訊，製造商識別資訊、販賣商識別資訊、及、記錄裝置及編碼器的固有的識別資訊、媒體製造裝置固有的識別資訊、地域資訊，供應自外部的識別資訊等，或是其組合及與其它資訊的組合；而上述邏輯運算則可以使是：互斥邏輯和（EXOR）、及、邏輯積（AND）、邏輯和（OR）、移位運算等。

其次，此第2實施形態的磁區格式（sector format）可以是使用如圖25所示者。

如此圖25所示的，1磁區係由：1行172位元組的12行，即是2064位元組所構成；其中包括主資料2048位元組。在12行的最初的行的前頭位置依序配置了：4位元組的ID（識別資料）、及、2位元組的IED（ID錯誤檢出碼）、及、6位元組的RSV（予備）；而在最後1行的終端位置配置了：4位元組的EDC（錯誤檢出碼）。

上述ID（識別資料）的4位元組係；如圖26所示的，MSB側的最初的位元組（位元b31～b24）係由磁區資訊所構成，剩餘的3位元組（位元b23～b0

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

五、發明說明（29）

）則係由磁區號碼所構成。磁區資訊係從ＭＳＢ側依序由：１位元的磁區格式形態、１位元的磁軌（tracking）方法、１位元的反射率、１位元的預備、２位元的區域形態（area type）、２位元的層號碼，的各資訊所構成。

在圖１的頭附加電路１５，在這種磁區格式中，係藉由依據上述關鍵資訊而對如上述ＩＤ（識別資料）內的磁區號碼的２４位元進行以位元單位的拌碼處理的轉置處理，而可進行暗號化。再者，依據上述關鍵資訊而改變上述２位元組的ＩＥＤ（ＩＤ錯誤檢出碼）的生成多項式及４位元組的ＥＤＣ（錯誤檢出碼）的生成多項式，或是，由對這些資訊與關鍵資訊做邏輯運算，也可以來進行暗號化。

其次，使用如圖２７所示構造的電路來做爲圖１的錯誤訂正編碼電路１６。此編碼係使用如圖２８所示的積碼或區塊碼。

在圖２７中，供應來自前述圖１的頭附加電路１５的資料到輸入端點２１０，此輸入資料則被送到做爲第１編碼器的ＰＯ編碼器２１１。送到此ＰＯ編碼器２１１的輸入資料係如圖２８所示的，爲B_{00}～$B_{191,171}$的１７２位元×１９２行的資料；在ＰＯ編碼器２１１則對１７２列的各列１９２位元組的資料則附加上分別各做爲１６位元的リードソワモニ（ＲＳ）碼的ＲＳ（２０８，１９２，１７）的外碼（ＰＯ）。來自ＰＯ編碼器２１１的輸出資料係經由用以如前述的暗號化的資料變

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（30）

換電路２１２而被送到交錯電路２１３並進行交錯處理，再生到ＰＩ編碼器２１４。在此ＰＩ編碼器２１４，如圖２８所示的，對附加了上述ＰＯ同位的１７２位元組×２０８行的資料的各行的１７２位元組的資料分別加上各爲１０位元組的ＲＳ（１８２，１７２，１１）的內碼（ＰＩ）。因此，從此ＰＩ編碼器２１４會輸出１８２位元組×２０８行的資料。此輸出資料則經由用以如前述的暗號化的資料變換電路２１５而從輸出端點２１６取出。

此處，對資料變換電路２１２而言，因爲ＰＯ編碼器２１１會對每一列的１９２位元組的輸入資料附加１６位元組的ＰＯ同位，並輸出２０８位元組的資料，因此，對此１６位元組的同位，或對２０８位元組的資料全體，可以藉由進行如前述的資料變換而進行暗號化。此資料變換，如前所述的，也可以是依據經由端點２１８而輸入的關鍵資訊而進行。再者，對資料變換電路２１５而言，因爲ＰＩ編碼器２１４會對各行的１７２位元組的資料分別附加１０位元組的ＰＩ同位而輸出１８２位元組的資料，因此，可以藉由對此１０位元組的同位，或是對１８２位元組的資料全體進行資料變換而進行暗號化。此暗號化也是，如前所述的，可依據經由端點２１９的輸入的關鍵資訊而進行。

上述資料變換，具體而言，係如前述圖１０、圖１１、圖１２所說明的，在所定位置配設樣式（pattern），依據關鍵資訊而由ＥＸＯＲ電路群選擇性的使資料反相，

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

五、發明說明（31）

也可以是使用其它的ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ電路群等。再者，除了以８位元爲單位進行１位元的關鍵資訊或關鍵資料的邏輯運算之外，也可以是對８位元的資訊資料及８位元的關鍵資料進行邏輯運算。而且，也可以是對相當於資訊資料的１字元的８位元內的各位元分別以ＡＮＤ、ＯＲ、ＥＸＯＲ、ＮＡＮＤ、ＮＯＲ、反相電路的組合而使用。再者，當然，使用移位暫存器來做變換，以各種函數運算做變換等，也可以適用各種的暗號化手法。在者，在係使用ＡＮＤ、ＯＲ、ＥＸＯＲ、ＮＡＮＤ、ＮＯＲ、反相器電路的組合的場合，也可以使用其組合本身來做爲關鍵。再者，除了邏輯運算之外，也可以使用：改變資料的位置的轉置、置換資料的值的置換等，以做爲上述的資料變換。再者，當然也可以適用以移暫存器來變換、以各種函數運算來變換等各種暗號化手法，而且也可以使用其組合。

被錯誤訂正編碼了的上述１８２位元組×２０８行的資料對行做交錯，並分割爲各爲１３行的１６群（group），並使各群對應記錄磁區。１磁區則成爲１８２位元組×１３行的２３６６位元組，並對此做調變，而如圖２９所示的，對每１行附加上２個同步碼ＳＹ。雖然調變係使用與前述的第１實施形態相同的８－１６變換，但是將１行分割爲２個單框架（single frame），而１單框架係由３２頻道位元的同步碼ＳＹ及１４５６頻道位元的資料部所構成。圖２９顯示被調變且附加了的１磁區份的

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（32）

構造，此圖２９所示的１磁區份的３８６８８頻道位元係相當於調變前的２４１８位元組。

在圖２９的調變輸出信號中使用８種類的同步碼ＳＹ０～ＳＹ７，這些同步碼ＳＹ０～ＳＹ７則依據上述８－１６變換的狀態，而在狀態１及２時成爲圖３０的（ａ）的同步樣式，而在狀態３及４時成爲圖３０的（ｂ）的同步樣式。

藉由，譬如說，使用如圖３１所示的電路並依據３位元的關鍵資訊而將如此的８種類的同步碼ＳＹ０～ＳＹ７的選擇做變更，便可進行暗號化。即是，由３個的ＥＸＯＲ電路２２３、２２４、２２５而分別取得指定上述８種類的同步碼ＳＹ０～ＳＹ７的３位元資料２２１的各位元、及、上述３位元的關鍵資訊２２２的各位元的互斥邏輯和，便可得到新同步碼指定資料２２６。由此，在上述框架構造中可改變同步碼的使用方法或框架構造內的各種同步碼的使用位置，而成爲暗號化。當然，對此３位元也可以依據關鍵資訊而將資料轉置、置換、或由移位暫存器變換。再者，也可以做函數變換。

其次，相對於上述的本發明的第２實施形態的記錄側的構成，再生側的基本構成係與前述圖１７相同，係對應顯示於上述第２實施形態的各部的變更。處而分別進行變更了的逆處理。譬如說，對於上述圖２７所示的錯誤訂正編碼的逆處理可由如圖３２的構成的錯誤訂正解碼電路而實現。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（33）

即是，在此圖３２中，在輸入端點２３０爲來自前述圖１７的解調電路１１５的輸出信號，且供應了相當於來自上述圖２７的輸出端點２１６的輸出的上述圖２８的積碼的１８２位元組×２０８行的資料。將來自此輸入端點２３０的資料送到資料逆變換電路２３１，並進行上述圖２７的資料變換電路２１５的逆處理。將來自資料逆變換電路２３１的輸出資料送到ＰＩ（內碼）解碼器２３２；並進行做爲上述圖２７的ＰＩ編碼器２１４的逆處理的解碼處理，即是，使用ＰＩ碼的錯誤訂正處理；而成爲上述圖２８的１７２位元組×２０８行的資料。來自ＰＩ解碼器２３２的輸出資料則在解交錯電路２３３進行上述交錯電路２１３的逆處理，並將其送到資料逆變換電路２３４並在進行上述圖２７的資料變換電路２１２的逆處理之後，送到ＰＯ（外碼）解碼器２３５。在ＰＯ解碼器２３５，進行做爲上述圖２７的ＰＯ編碼器２１１的逆處理的解碼處理，即是使用ＰＯ碼的錯誤訂正處理，並經由輸出端點２３６取出圖２８的原來的１７２位元組×１９２行的資料。在在上述圖２７的資料變換電路２１２，２１５的資料變換時使用關鍵資訊的場合，將分別供應到各端點２１８，２１９的關鍵資訊分別供應到圖３２的資料逆變換電路２３４，２３１的各端點２３９，２３８；並依據這些關鍵資訊來進行資料逆變換即可。

以上所說明的本發明的第２實施形態的效果也是與在前述第１實施形態的場合相同。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（34）

再者，本發明並不僅限定於上述的實施形態，譬如說，以資料變換而言，雖是以反相器及ＥＸＯＲ爲例，但是當然也是可以使用其它的，位元相加，各種邏輯運算來進行資料變換。再者，當然，依照暗號化的關鍵資訊而將資料置換、轉置、使用移位暫存器來變換，以各種函數運算來變換等，也可適用各種暗號化手法，也可以使用其組合。此外，在未超出本發明的要旨的範圍，也可以使用各種的變更。

〔發明之效果〕

在本發明的資料記錄方法中，因爲在以所定資料量將輸入數位資料做磁區化的磁區化過程、及、附加頭的頭附加過程，及、錯誤訂正編碼過程，及，以所定的調變方式做調變的調變過程，及，附加同步樣式的同步附加過程之中的至少一項過程中，對輸入進行暗號化處理並輸出，所以在那一個過程進行了暗號化處理也成爲暗號的關鍵，而可提高暗號的困難度。而也可以使這些可進行暗號化處理的過程之一包含進行用以除去同一樣式的隨機化處理的拌碼處理過程。再者，也具有僅變更即存的構成的一部份便可簡單的實現暗號化的優點。此爲在資料記錄裝置、記錄媒體、再生方法及裝置的場合也可獲得的效果。

再者，在本發明中，因爲對在錯誤訂正編碼處理時所處理的資料進行了將對應暗號化的關鍵資訊的至少一部份的資料做資料變換，所以在錯誤訂正處理從某種程度的資

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（35）

料爲可以復元的狀態，到不進行資料復元的狀態爲止的任意程度均可進行暗號化。由此，可以將其控制爲：在錯誤狀態好時可再生而在不好時無法再生，而能夠依照資料提供的用途或依照安全程度而可做各種對應。

再者，因爲在錯誤訂正處理中可使其成爲關鍵的位元數目很大的暗號化，可在錯誤訂正編碼及解碼ＩＣ或ＬＳＩ的巨大黑盒（black box）之中實現暗號化，所以一般使用者很難解讀，而能夠大幅的改善資料的安全性。

而且，在本發明中，係使用所定的關鍵資訊來對資料進行暗號化處理，而且將此暗號化的關鍵資訊的至少一部份寫入與記錄媒體的資料記錄區域不同的區域，而在再生時讀取此關鍵資訊的至少一部份的資訊，並使用於暗號解碼。而固爲暗號解碼的關鍵資訊不會僅爲記錄媒體的資料記錄區域內的資訊而已，所以可提高暗號化的困難度。

而且，在本發明中，在進行以除去資料列的同一樣式的隨機化爲主目的的拌碼處理時，藉由依照暗號化的關鍵來改變生成多項式及初期值的至少一方，便能夠以既存的拌碼處理來做暗號化，而以簡單的構成便可實現暗號化。

藉由這種資料的暗號化便可以以簡單的構造來防止複製及不正使用，也很容易適用於安全及收費裝置。

〔圖面之簡單說明〕

第1圖係顯示本發明的資料記錄裝置的第1實施形態的概略構成的區塊圖。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（ 36 ）

第 2 圖係顯示用以實現磁區化電路的偶數，奇數位元組的交錯的構成例的區塊圖。

第 3 圖係用以說明偶數，奇數位元組的交錯的圖。

第 4 圖係顯示拌碼器的一例。

第 5 圖係顯示拌碼器的預置值的一例的圖。

第 6 圖係顯示生成多項式爲可變的拌碼器的一例的圖。

第 7 圖係顯示磁區格式的一例的圖。

第 8 圖係用以說明磁區內的同步區域的暗號化的一例的圖。

第 9 圖係顯示磁區內的頭區域的一例的圖。

第 1 0 圖係顯示錯誤訂正編碼電路的一例的概略構成的圖。

第 1 1 圖係顯示錯誤訂正編碼電路的一例的具體的構成的圖。

第 1 2 圖係顯示錯誤訂正編碼電路的其它例的圖。

第 1 3 圖係用以說明調變電路的暗號化處理的一例的圖。

第 1 4 圖係顯示附加於調變信號的同步字元的具體例的圖。

第 1 5 圖係用以說明同步附加電路的暗號化的一例的圖。

第 1 6 圖係顯示資料記錄媒體的一例的圖。

第 1 7 圖係顯示本發明的資料再生裝置的第 1 實施形

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（37）

態的概略構成的區塊圖。

第１８圖係用以說明解調電路的暗號化處理的一例的圖。

第１９圖係顯示錯誤訂正解碼電路的一例的概略構成的圖。

第２０圖係顯示錯誤訂正解碼電路的一例的具體的構成的圖。

第２１圖係顯示錯誤訂正解碼電路的其它例的圖。

第２２圖係顯示解拌碼處理電路的一例的圖。

第２３圖係顯示拌碼器的其它例的圖。

第２４圖係顯示圖２３的拌碼器的預置值的一例的圖。

第２５圖係顯示磁區格式的其它例的圖。

第２６圖係顯示圖２５的磁區格式的磁區內的頭區域的一例的圖。

第２７圖係顯示錯誤訂正編碼電路的其它例的區塊圖。

第２８圖係顯示做爲錯誤訂正碼的具體例的積碼的圖。

第２９圖係顯示磁區的信號格式的一例的圖。

第３０圖係顯示附加於調變信號的同步字元的其它的具體例的圖。

第３１圖係用以說明同步附加電路的暗號化的其它例的圖。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

五、發明說明（38）

第３２圖係顯示錯誤訂正解碼電路的其它例的區塊圖。

〔圖號說明〕

１３：磁區化電路

１４：拌碼處理電路

１５：頭附加電路

１６：錯誤訂正編碼電路

１７：調變電路

１８：同步附加電路

５７、１４２：再配列電路

６１、６６、１５１、１５６：ＥＸＯＲ電路群

１１４：同步分離電路

１１５：解調電路

１１６：錯誤訂正解碼電路

１１７：磁區分解電路

１１８：頭分解電路

１１９：解拌碼處理電路

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

A5
B5

四、中文發明摘要（發明之名稱：　　）

資料記錄方法及裝置、資料記錄媒體、及資料再生方法及裝置

本發明以簡單的構成來進行不易解讀的暗號化。

本發明係在：用以處理輸入資料並做爲記錄信號的磁區（sector）化電路13、拌碼（scramble）處理電路14、頭（head）附加電路15、錯誤訂正編碼電路16、調變電路17、以及、同步附加電路18之中的至少其中之一的電路中，對輸入進行暗號化處理並將其輸出。在電路內進行暗號化處理本身並不僅是關鍵，而在那一個電路進行暗號化處理更是關鍵。

英文發明摘要（發明之名稱：　　）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

經濟部中央標準局員工消費合作社印製

A8
B8
C8
D8

86年1月14日 修正補充

六、申請專利範圍

第８５１０６６８２號專利申請案

中文申請專利範圍修正本

民國８６年５月修正

１．一種資料記錄方法，其特徵係具有：

以所定資料量單位將輸入的數位資料做磁區化的磁區化過程，及

將頭附加到此被磁區化了的數位資料的頭附加過程，及

將錯誤訂正碼附加到此附加了頭的數位資料的錯誤訂正編碼過程，及

以所定的調變方式將此錯誤訂正編碼了的數位資料做調變的調變過程，及

對此調變了的數位信號附加上同步樣式的同步附加過程，及

將附加了此同步樣式的數位信號記錄到記錄媒體的記錄過程；

並在上述磁區化過程、頭附加過程、錯誤訂正編碼過程、調變過程、以及同步附加過程中之至少一個過程中，對輸入進行暗號化處理，然後輸出。

２．如申請專利範圍第１項之資料記錄方法，其中：

設置：對在上述磁區化過程被磁區化了的數位資料，或是，在上述頭附加過程被頭附加了的數位資料，進行用以除去同一樣式的隨機化處理的拌碼處理過程；

並在上述磁區化過程、頭附加過程、錯誤訂正編碼過

煩請委員明示本案是否變更實質內容

經濟部中央標準局員工消費合作社印製

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

程、調變過程、同步附加過程、以及拌碼處理過程中的至少其中之一的過程中，對輸入進行暗號化處理，然後輸出。

3．如申請專利範圍第1項之資料記錄方法，其中：

設定複數的使用於上述暗號化處理的關鍵資訊，並以所定定時來切換這些關鍵資訊。

4．如申請專利範圍第1項之資料記錄方法，其中：

係以在上述磁區化過程、頭附加過程、錯誤訂正編碼過程、調變過程、以及同步附加過程中的任何一項過程中進行的暗號化，來做爲關鍵資訊。

5．如申請專利範圍第1項之資料記錄方法，其中：

依照暗號化的關鍵資訊而對在上述錯誤訂正編碼過程的錯誤編碼處理時所處理的資料的至少一部份，進行資料變換。

6．如申請專利範圍第1項之資料記錄方法，其中：

上述錯誤訂正碼係積碼。

7．一種資料記錄裝置，其特徵係具有：

以所定資料量單位將輸入的數位資料做磁區化的磁區化手段，及

將頭附加到輸出自此磁區化手段的數位資料的頭附加手段，及

將錯誤訂正碼附加到輸出自此頭附加手段的數位資料的錯誤訂正編碼手段，及

以所定的調變方式對輸出自此錯誤訂正編碼手段的數

（請先閱讀背面之注意事項再填寫本頁）

裝 訂

經濟部中央標準局員工消費合作社印製

六、申請專利範圍

位資料做調變的調變手段，及

將同期樣式附加到輸出自此調變手段的數位信號的同步附加手段，及

將輸出自此同步附加手段的數位信號記錄到記錄媒體的記錄手段；

並在上述磁區化手段、頭附加過程、錯誤訂正編碼手段、調變手段、以及同步附加手段中的至少一個手段對輸入進行暗號化處理，然後輸出。

8．如申請專利範圍第7項之資料記錄裝置，其中；

設置：對在上述磁區化手段被磁區化了的數位資料，或是，在上述頭附加手段被頭附加了的數位資料，進行用以除去同一樣式的隨機化處理的拌碼處理手段；

並在上述磁區化手段、頭附加手段、錯誤訂正編碼手段、調變手段、同步附加手段、以及拌碼處理手段中的至少一個手段對輸入進行暗號化處理，然後輸出。

9．如申請專利範圍第7項之資料記錄裝置，其中：

上述錯誤訂正編碼手段係：依照暗號化的關鍵資訊而對在錯誤訂正編碼處理時所處理的資料的至少一部份，進行資料變換。

10．一種資料記錄媒體，其特徵係：

以所定資料量單位將輸入數位資料磁區化，附加上頭，做錯誤訂正編碼，以所定的調變方式做調變，附加上同步樣式，而且，在此磁區化頭附加、錯誤訂正編碼、調變、以及同步附加之中之任何一者時，將對輸入進行暗號化

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

六、申請專利範圍

了的信號做記錄。

１１．一種資料再生方法，其特徵係具有：

從讀取自資料記錄媒體的數位信號分離出同步信號的同步分離過程，及

依據所定的調變方法，對此同步分離了的數位信號進行解調的解調過程，及

對此解調而得的數位資料進行錯誤訂正解碼處理的錯誤訂正解碼過程，及

將進行了此錯誤訂正解碼處理的數位資料分離爲所定的磁區的磁區分解過程，及

將此磁區分解了的數位資料的磁區構造的頭部份分離的頭分離過程；

而且，在對應上述同步分離過程、解調過程、錯誤訂正解碼過程、磁區分解過程、以及頭分離過程之中，至少一個過程的記錄時的過程，已進行了暗號化處理，而在對應此記錄時進行了暗號化處理的過程的再生時的過程，對輸入進行暗號的解碼處理，並輸出。

１２．如申請專利範圍第１１項之資料再生方法，其中：

設置：對在上述磁區分解過程被磁區分解了的數位資料，或是，在上述頭分離過程被頭分離了的數位資料，解讀記錄時的拌碼的解拌碼過程，

而且，在對應上述同步分離過程、解調過程、錯誤訂正解碼過程、磁區分解過程、頭分離過程，以及解拌碼處

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

六、申請專利範圍

理過程之中，至少一個過程的記錄時的過程，已進行了暗號化處理，而在對應此記錄時進行了暗號化處理的過程的再生時的過程，對輸入進行暗號的解碼處理，並輸出。

１３．一種資料再生裝置，其特徵係具有：

從讀取自記錄媒體的數位信號分離出同步信號的同步分離手段，及

依據所定的調變方式，對此輸出自同步分離手段的數位信號進行解調的解調手段，及

對得自此解調手段的數位資料進行錯誤訂正解碼處理的錯誤訂正解碼手段，及

將輸出自此錯誤訂正解碼手段的數位資料分離爲所定的磁區的磁區分解手段，及

將輸出自此磁區分解手段的數位資料的磁區構造的頭部份分離的頭分離手段；

而且，在對應上述同步分離手段、解調手段、錯誤訂正解碼手段、磁區分離手段、以及頭分離手段之中，至少一個過程的記錄時的過程，已進行了暗號化處理，而在對應此記錄時進行了暗號化處理的過程的再生時的手段，對輸入進行暗號的解碼處理，然後輸出。

１４．如申請專利範圍第１３項之資料再生裝置，其中：

設置：對輸出自上述磁區分解手段的數位資料，或是，輸出自上述頭分離手段的數位資料，進行解讀記錄時的拌碼的解拌碼處理的解拌碼處理手段；

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部中央標準局員工消費合作社印製

六、申請專利範圍

而且，在對應上述同步分離手段、解調手段、錯誤訂正解碼手段、磁區分解手段、頭分離手段、以及解拌碼處理過程之中，至少一個手段的記錄時的手段，已進行了暗號化處理，而在對應此記錄時進行了暗號化處理的手段的再生時的手段，對輸入進行暗號的解碼處理，然後輸出。

１５．一種資料記錄方法，係對輸入的數位資料進行錯誤訂正編碼處理並記錄到記錄媒體的資料記錄方法，其特徵係：

依據暗號化的關鍵資訊，而對在上述錯誤訂正編碼處理時所處理的資料的至少一部份，進行資料變換。

１６．如申請專利範圍第１５項之資料記錄方法，其中：

係以：資料及上述關鍵資訊的邏輯運算，使用關鍵資訊的置換，轉置，或是函數運算的至少其中之一來進行上述資料變換。

１７．如申請專利範圍第１５項之資料記錄方法，其中：

係依暗號化的難易度來改變進行上述資料變換的資料的個數。

１８．一種資料記錄裝置，係對輸入的數位資料進行錯誤訂正編碼處理並記錄到記錄媒體的資料記錄裝置，其特徵係具有：

暗號化的關鍵資訊的輸入手段；及

依據來自此輸入手段的關鍵資訊，而對在上述錯誤訂

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

六、申請專利範圍

正編碼處理時所處理的資料的至少一部份進行資料變換的手段。

１９．一種資料記錄媒體，其特徵係：

依據暗號化的關鍵資訊，而對在對輸入的數位資料進行錯誤訂正編碼處理時所處理的資料的至少一部份進行資料變換，而將所得到的信號記錄而構成。

２０．一種資料再生方法，係進行錯誤訂正編碼，並將記錄於記錄媒體的信號再生的資料再生方法，其特徵係：

依據暗號化的關鍵資訊而對在上述錯誤訂正編碼處理時所處理的資料的至少一部份進行資料變換；

並依據對應上述錯誤訂正編碼處理的錯誤解碼處理時所處理的資料中的上述暗號化的關鍵資訊而對資料進行上述資料變換的逆變換。

２１．一種資料再生裝置，係進行錯誤訂正編碼處理並將記錄於記錄媒體的信號再生的資料再生裝置，其特徵係具有：

將顯示在上述錯誤訂正編碼處理時所處理的資料中進行了資料變換的資料的暗號化的關鍵資訊輸入的關鍵資訊輸入手段；及

除了進行對應於上述錯誤訂正編碼處理的錯誤訂正解碼處理之外，也依據來自上述關鍵資訊輸入手段的暗號化的關鍵資訊，而對資料進行上述資料變換的逆變換，的錯誤訂正解碼手段。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂

經濟部中央標準局員工消費合作社印製

六、申請專利範圍

２２．一種資料記錄方法，係對輸入資料進行用以記錄的信號處理，並記錄於記錄媒體的所定的資料記錄區域的資料記錄方法，其特徵係：

除了使用所定的關鍵資訊而對資料進行暗號化處理之外，也使用寫入到與上述記錄媒體的資料記錄區域不同的區域的資訊來做爲此暗號化的關鍵資訊的至少一部份。

２３．如申請專利範圍第２２項之資料記錄方法，其中：

係使用：媒體固有的識別資訊、記錄裝置固有的識別資訊、媒體製造裝置固有的識別資訊，製造商／販賣商的識別資訊，地域資訊，供應自外部的識別資訊，的至少其中之一，以做爲上述的關鍵資訊。

２４．一種資料記錄裝置，係對輸入資料進行用以記錄的信號處理，並記錄到記錄媒體的所定的資料記錄區域，的資料記錄裝置，其特徵爲：

除了使用所定的關鍵資訊來對資料進行暗號化處理之外，也使用寫入於與上述記錄媒體的資料記錄區域不同區域的資訊來做爲此暗號化的關鍵資訊的至少一部份。

２５．一種資料媒體，其特徵係：

將使用關鍵資訊的至少一部份，而對寫入於與資料記錄區域不同的區域的資訊進行暗號化處理的資料，記錄到上述資料記錄區域。

２６．一種資料再生方法，其特徵係：

對於讀取自資料記錄媒體的資料記錄區域，且在記錄

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部中央標準局員工消費合作社印製

六、申請專利範圍

時進行了暗號化處理的數位信號，在進行用以再生的信號處理時，使用關鍵資訊的至少一部份，而對寫入於與上述資料記錄媒體的上述資料區域不同的區域的資訊進行錯誤解碼處理。

２７．如申請專利範圍第２６項之資料再生方法，其中：

係使用：媒體固有的識別資訊，記錄裝置固有的識別資訊，媒體製造裝置固有的識別資訊，製造商／販賣商的識別資訊、再生裝置固有的識別資訊、地域資訊、供應自外部的識別資訊、以做爲上述關鍵資訊。

２８．一種資料再生裝置，係對於讀取自資料記錄媒體的資料記錄區域並在記錄時進行了暗號化處理的數位信號，進行用以再生的信號處理，的資料再生裝置，其特徵係：

使用關鍵資訊的至少一部份，而對寫入於與上述資料記錄媒體的上述資料區域不同的區域的資訊進行暗號解碼處理。

２９．一種資料記錄方法，其特徵係具有：

以所定資料量單位來對輸入的數位資料進行磁區化的磁區化過程，及

對此磁區化了的數位資料進行拌碼處理的拌碼處理過程，及

將頭附加到此拌碼處理了的數位資料的頭附加過程，及

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部中央標準局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

將錯誤訂正碼附加到此頭附加了的數位資料的錯誤訂正編碼過程，及

以所定的調變方式對此錯誤訂正編碼了的數位資料做調變的調變過程，及

將同步樣式附加到此調變了的數位信號的同步附加過程，及

將此同步樣式附加了的數位信號記錄到記錄媒體的記錄過程；

而且，依據暗號化的關鍵資訊，而改變上述拌碼處理過程的初期值及生成多項式的至少一方。

３０．一種資料記錄裝置，其特徵係具有：

以所定資料量爲單位將輸入的數位資料做磁區化的磁區化手段，及

依據暗號化的關鍵資訊而對輸出自此磁區化手段的數位資料進行改變其初期值及生成多項式的至少一方的拌碼處理的拌碼處理手段，及

將頭附加到輸出自此拌碼處理手段的數位資料，的頭附加手段，及

將錯誤訂正碼附加到輸出自此頭附加手段的數位資料，的錯誤訂正編碼手段，及

以所定的調變方式來對輸出自此錯誤訂正編碼手段的數位資料做調變的調變手段，及

將同步樣式附加到輸出自此調變手段的數位信號的同步附加手段，及

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製

六、申請專利範圍

將輸出自此同步附加手段的數位信號記錄到記錄媒體的記錄手段。

３１．一種資料記錄媒體，其特徵係：

以所定資料量單位將輸入的數位資料做磁區化，並進行依據暗號化的關鍵資訊來改變初期值及生成多項式的至少一方的拌碼處理，附加上頭，做錯誤訂正編碼，以所定的調變方式來調變，而將信號記錄。

３２．一種資料再生方法，其特徵係具有：

係讀取自資料記錄媒體的數位信號分離出同步信號的同步分離過程，及

依據所定的調變方式，對此同步分離了的數位信號進行解調的解調過程，及

對此解調而得的數位資料進行錯誤訂正解碼處理的錯誤訂正解碼過程，及

將進行了此錯誤訂正解碼處理的數位資料分解爲所定的磁區的磁區分解過程，及

將此磁區分解了的數位資料的磁區構造的頭部份分離的頭分離過程，及

依據記錄時的暗號化的關鍵資訊，而對此頭分離了的數位資料改變初期值及生成多項式的至少一方，而進行解除拌碼的解拌碼處理的解拌碼處理過程。

３３．一種資料再生裝置，其特徵係具有：

從讀取自記錄媒體的數位信號分離出同步信號的同步分離手段，及

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

經濟部中央標準局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

依據所定的調變方式，對此輸出自同步分離手段的數位信號進行解調的解調手段，及

對得自此解調手段的數位資料進行錯誤訂正解碼處理的錯誤訂正解碼手段，及

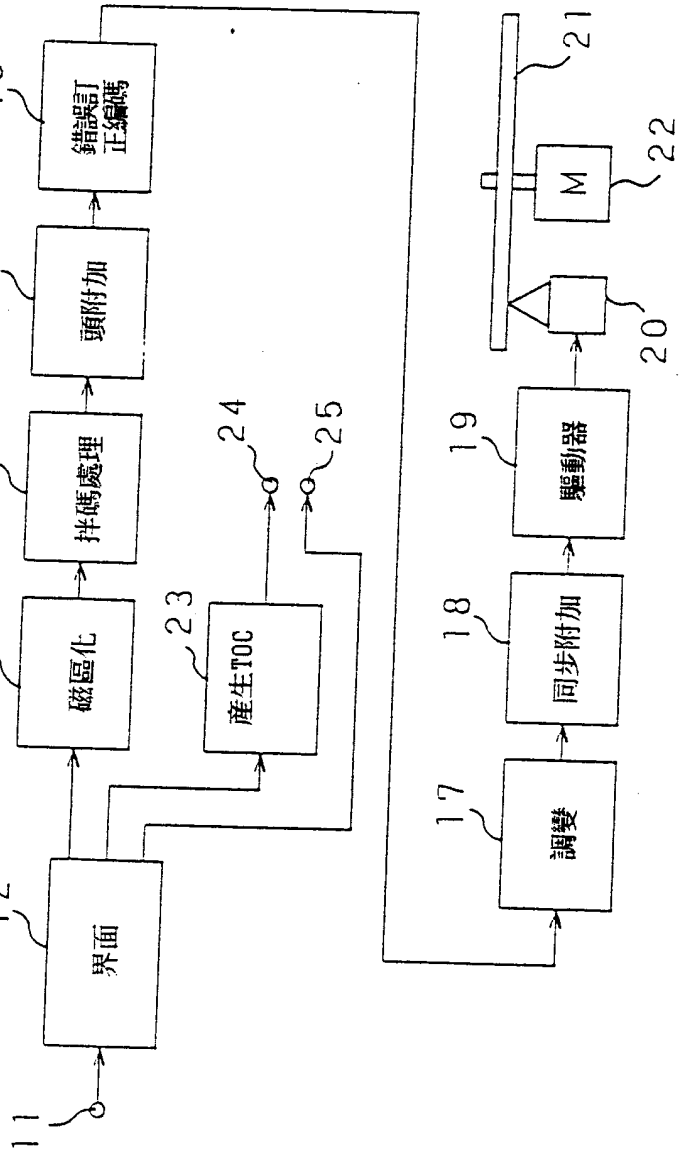
將輸出自此錯誤訂正解碼手段的數位資料分解爲所定的磁區的磁區分解手段，及

將輸出自此磁區分解手段的數位資料的磁區構造的頭部份分離的頭分離手段，及

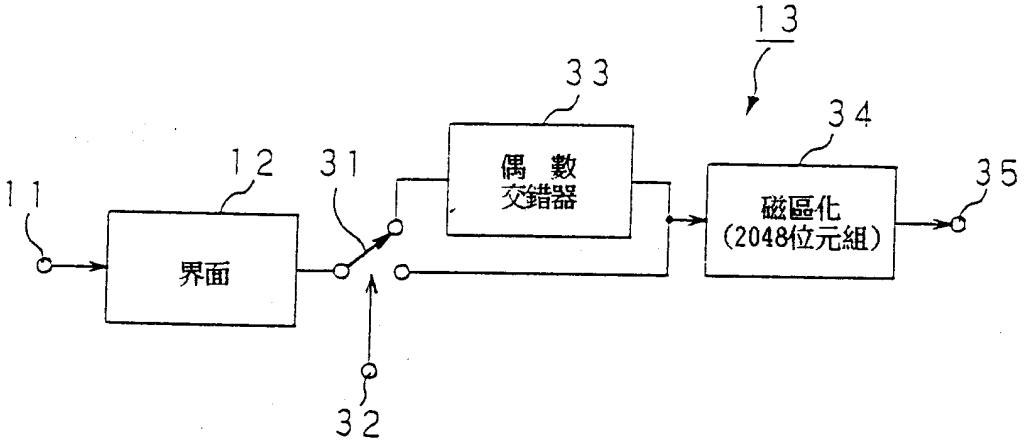
依據記錄時的暗號化的關鍵資訊，而對輸出自此頭分離手段的數位資料改變初期值及生成多項式的至少一方，而進行解除拌碼的解拌碼處理的解拌碼手段。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製

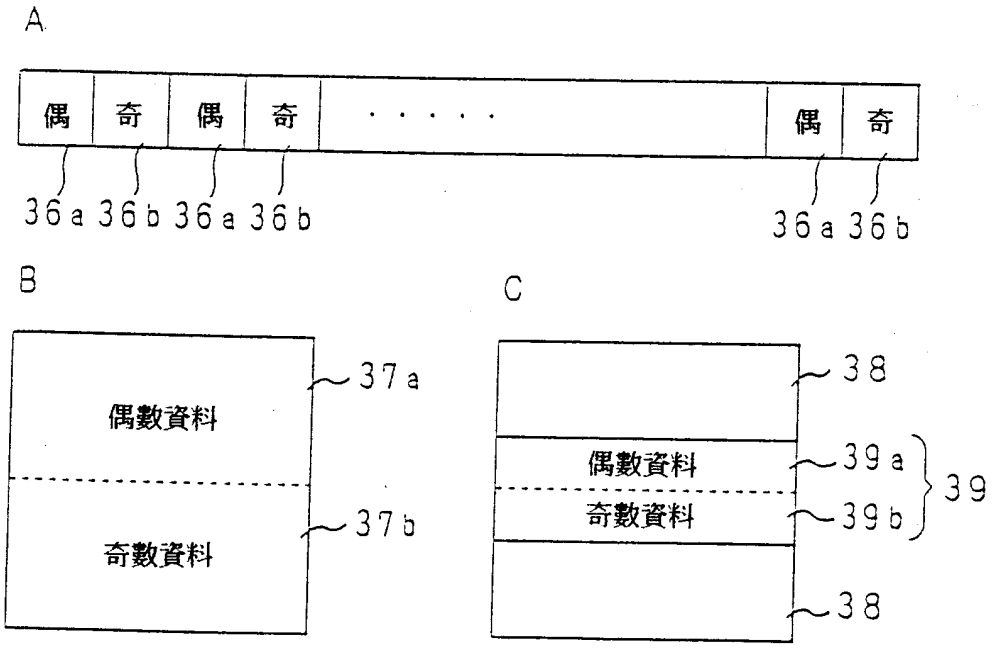
第1圖


11
12
界面
13
磁區化
14
拌碼處理
15
頭附加
16
錯誤訂正編碼
17
調變
18
同步附加
19
驅動器
20
21
22
M
23
產生TOC
24
25

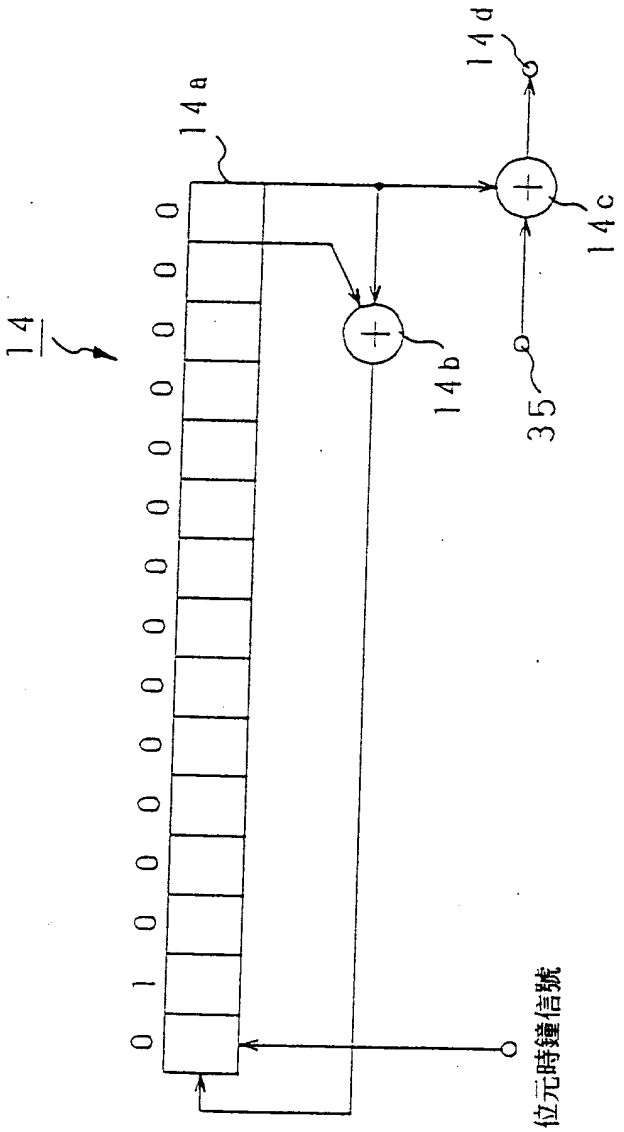
第2圖


13
33
34
12
31
偶 數
交錯器
磁區化
(2048位元組)
35
11
界面
32

第3圖


A
偶
奇
偶
奇
偶
奇
36a 36b 36a 36b
36a 36b
B
偶數資料
37a
奇數資料
37b
C
38
偶數資料
39a
奇數資料
39b
39
38

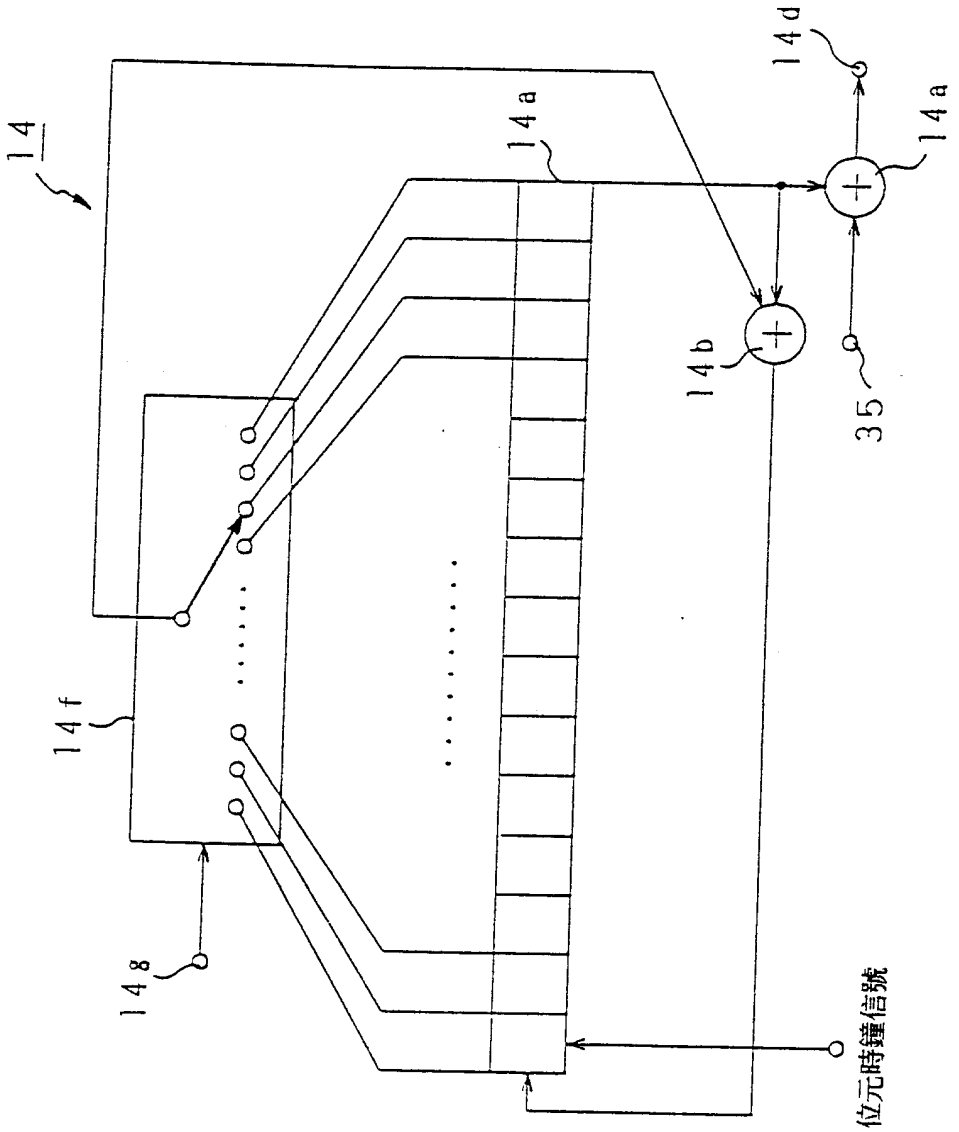
第4圖



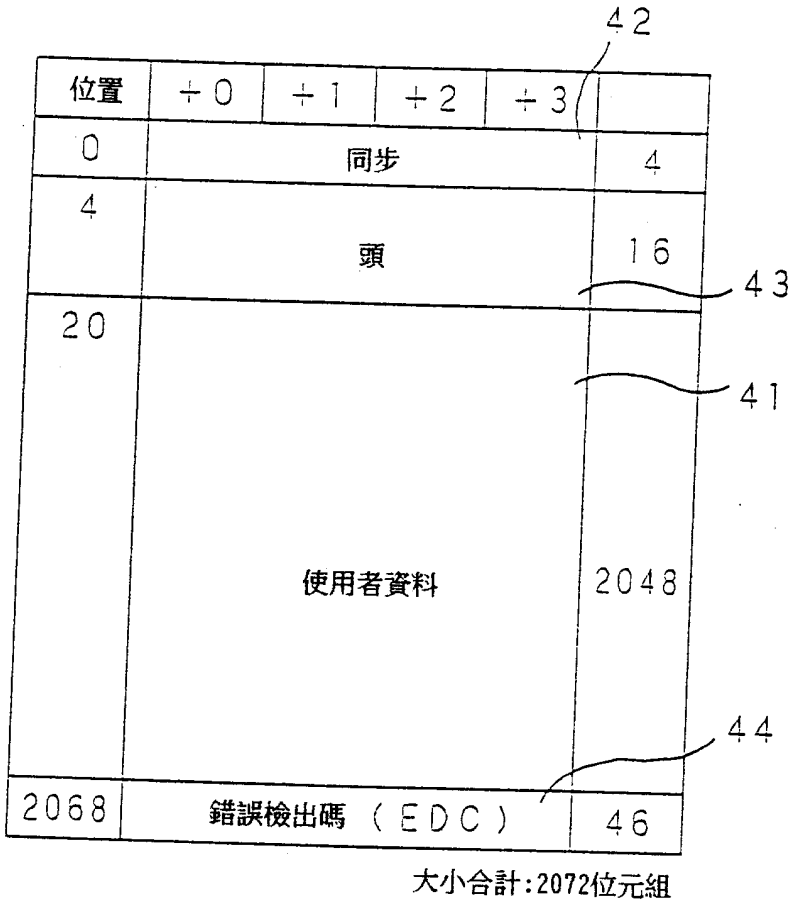
第 5 圖

選擇號碼	預置值	選擇號碼	預置值
0	$0001	8	$4080
1	$4000	9	$2040
2	$2000	10	$1020
3	$1000	11	$0810
4	$0800	12	$0408
5	$0400	13	$0204
6	$0200	14	$0102
7	$0100	15	$4081

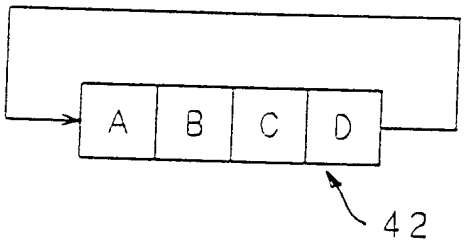
第 6 圖



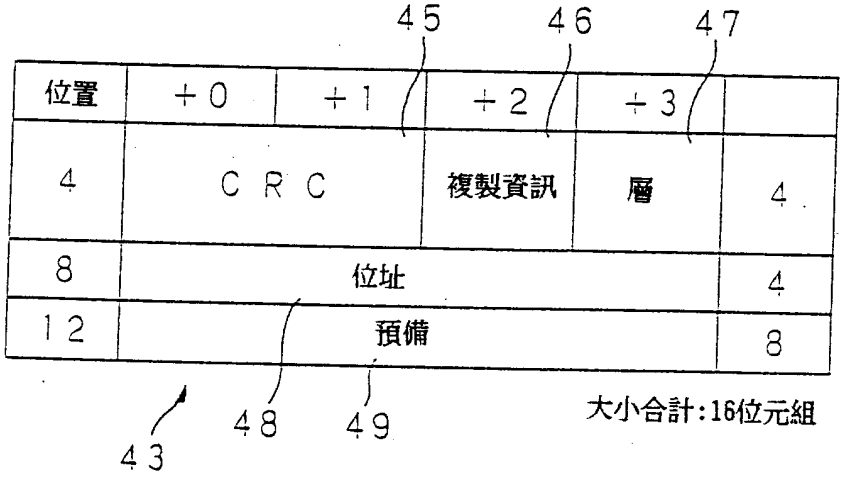
第7圖


42
位置
+0
+1
+2
+3
0
同步
4
4
頭
16
43
20
41
使用者資料
2048
44
2068
錯誤檢出碼（EDC）
46
大小合計:2072位元組

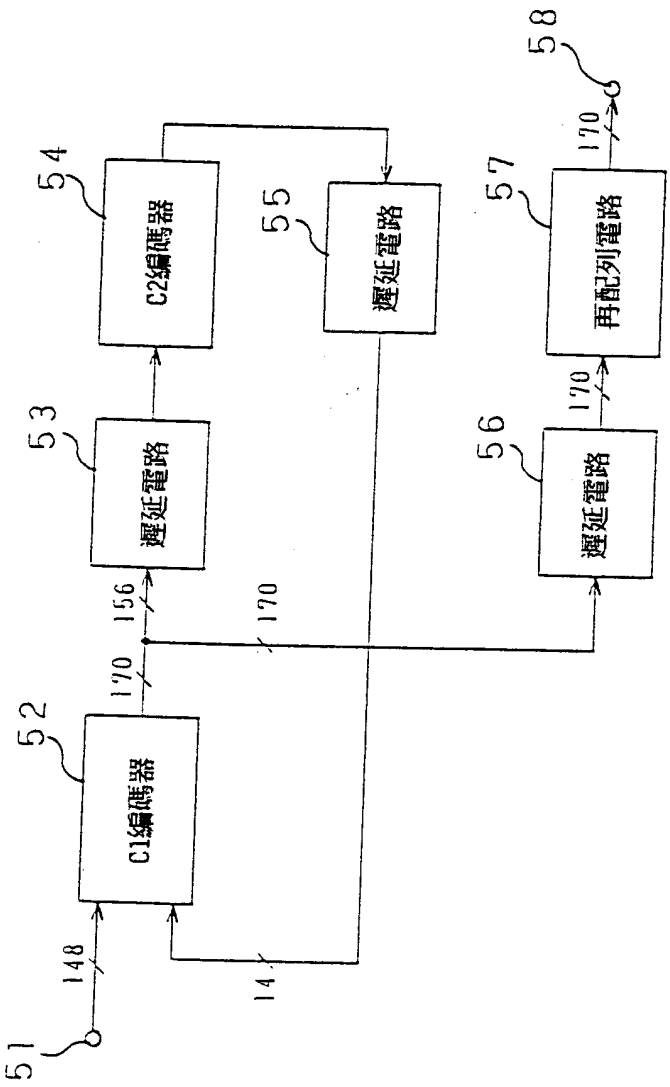
第8圖


A
B
C
D
42

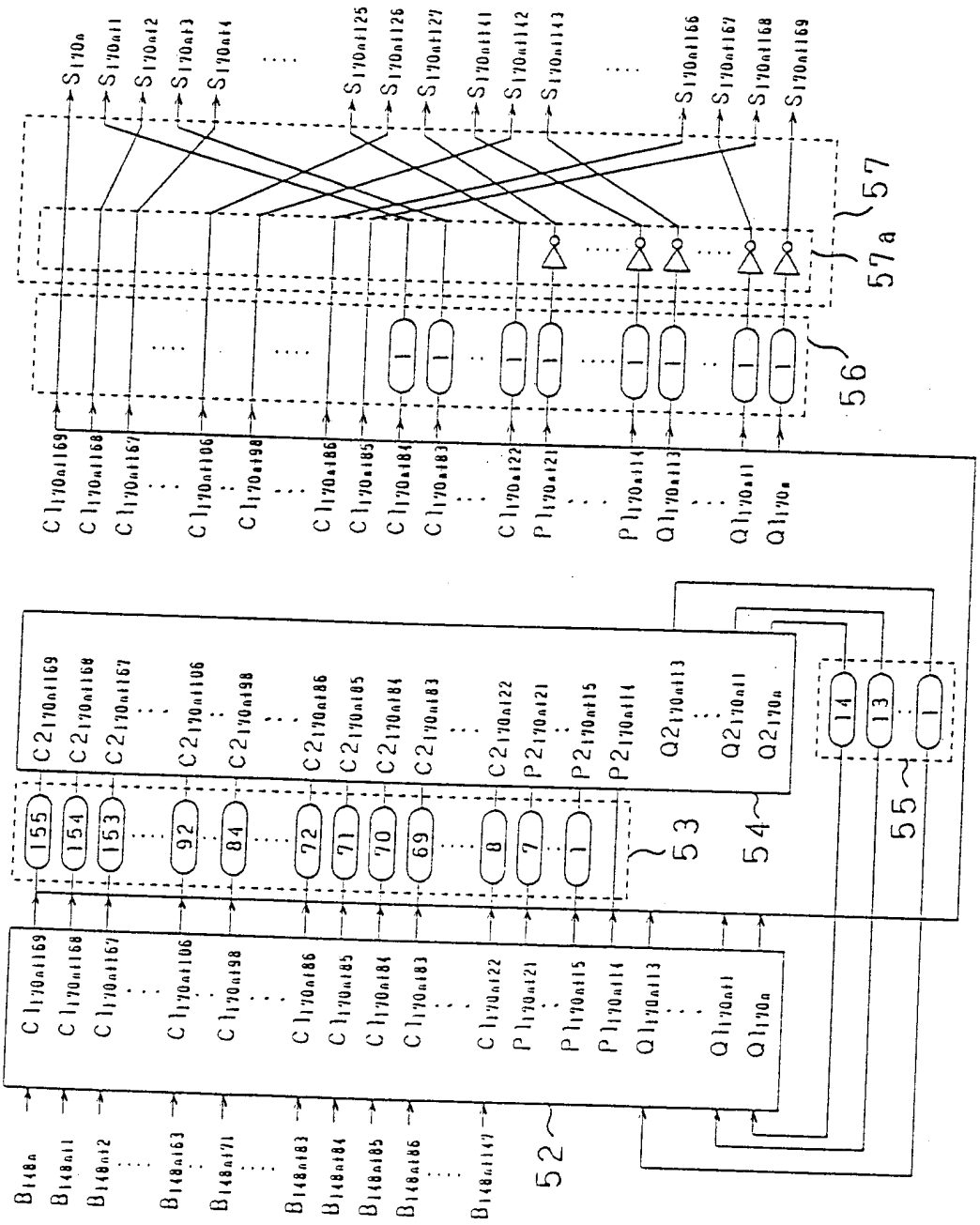
第 9 圖



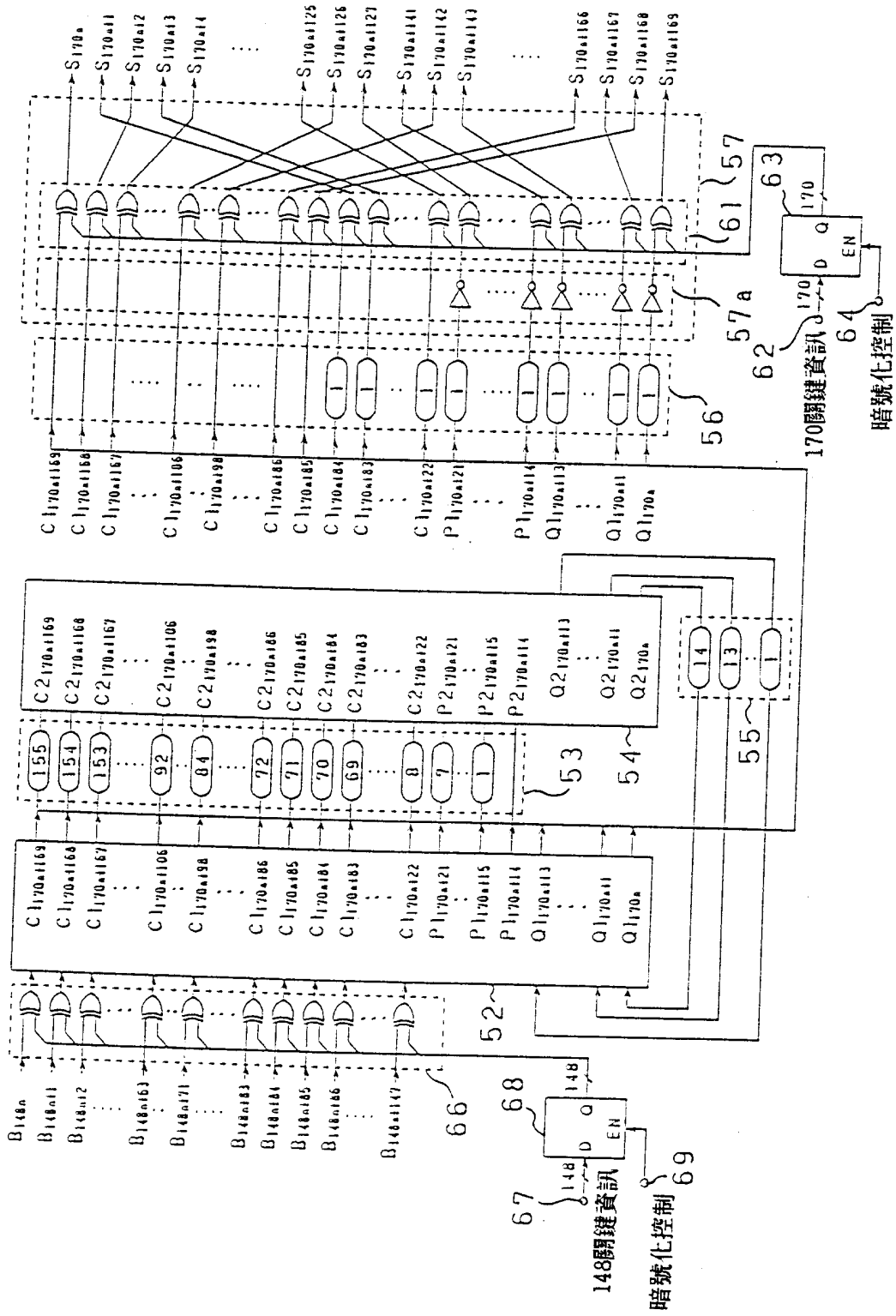
第10圖


51
148
52
C1編碼器
170
156
53
遲延電路
54
C2編碼器
55
遲延電路
170
56
遲延電路
57
再配列電路
170
58
170
14

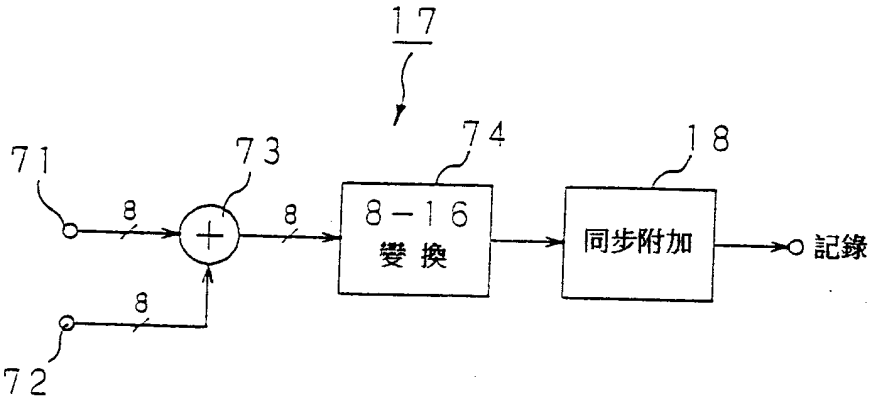
第11圖



第12圖


148關鍵資訊
暗號化控制
170關鍵資訊
暗號化控制
52
53
54
55
56
57
57a
61
62
63
64
66
67
68
69
D
Q
EN

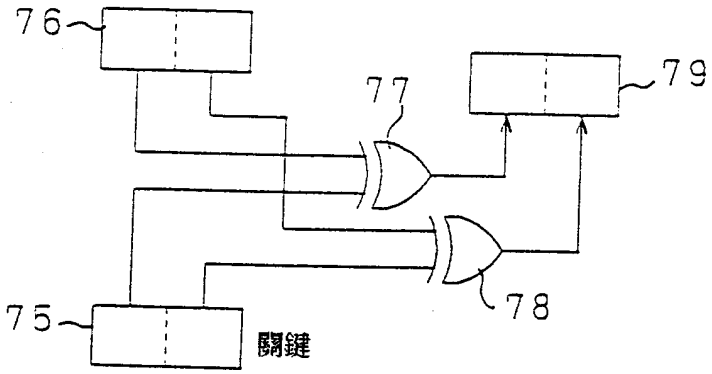
第13圖



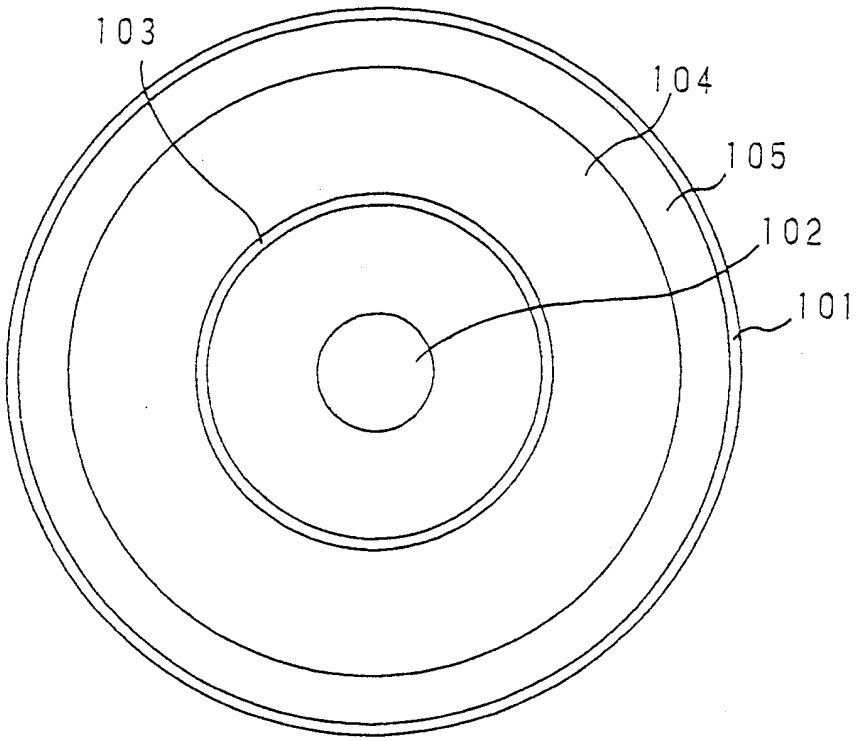
第14圖

同步字元	碼字元			
	msb 同步樣式a lsb		msb 同步樣式b lsb	
S0	0001001001000000000100000000001		1001001001000000000100000000001	
S1	0001000001000000000100000000001		1001000001000000000100000000001	
S2	0000100010000000001000000000001		1000100010000000001000000000001	
S3	0000100001000000000100000000001		1000100001000000000100000000001	

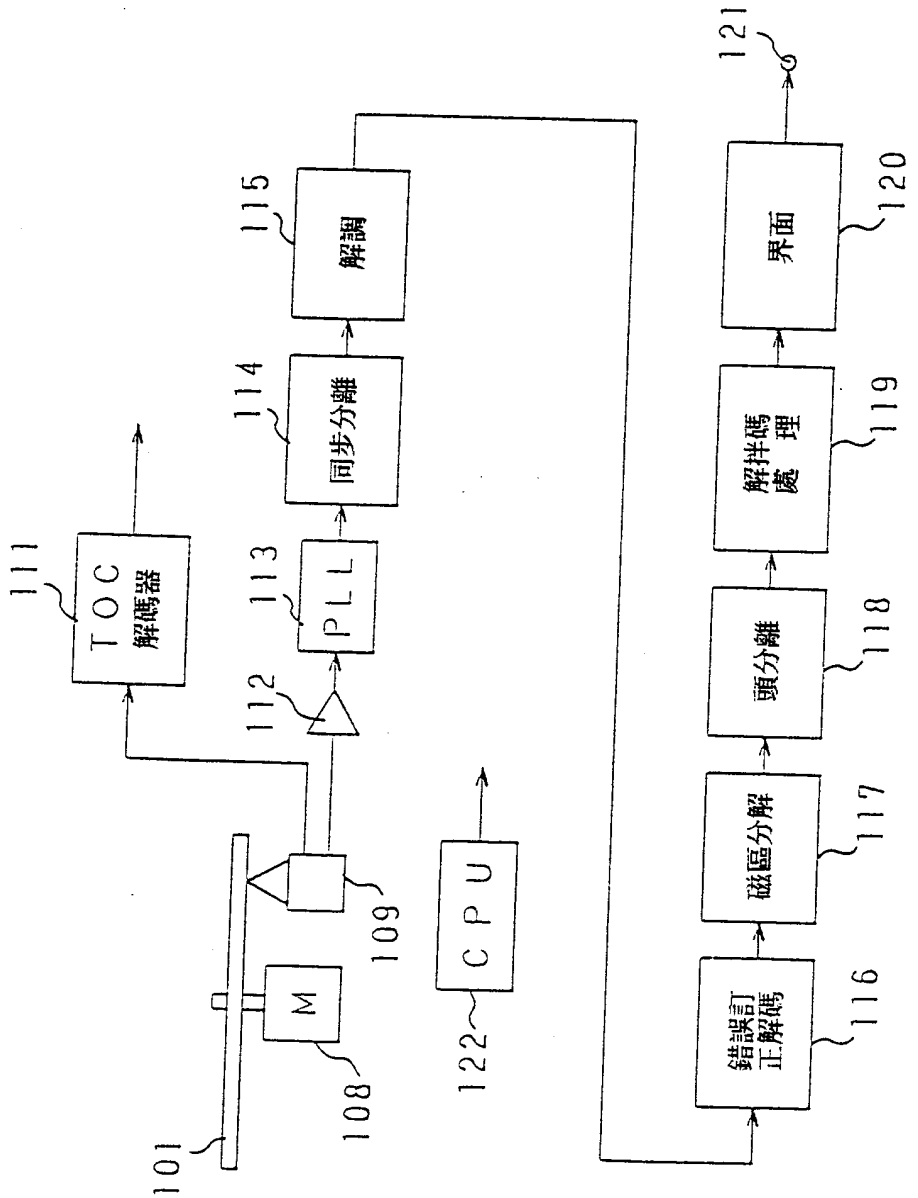
第15圖



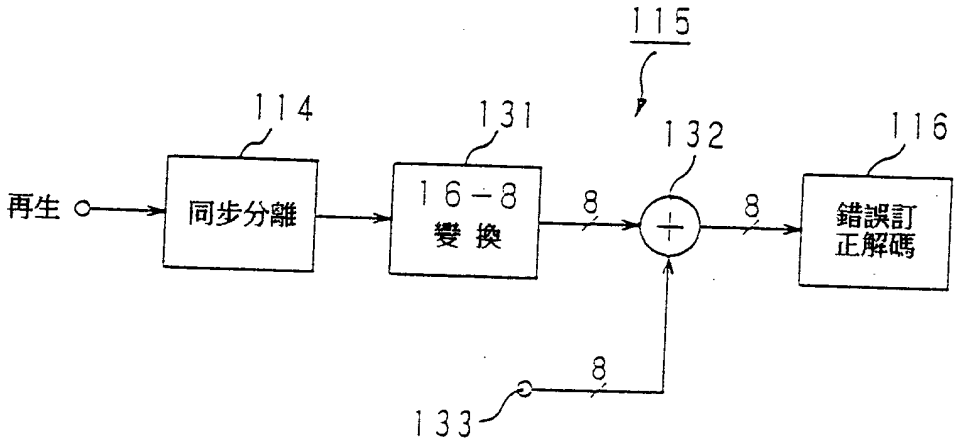
第16圖



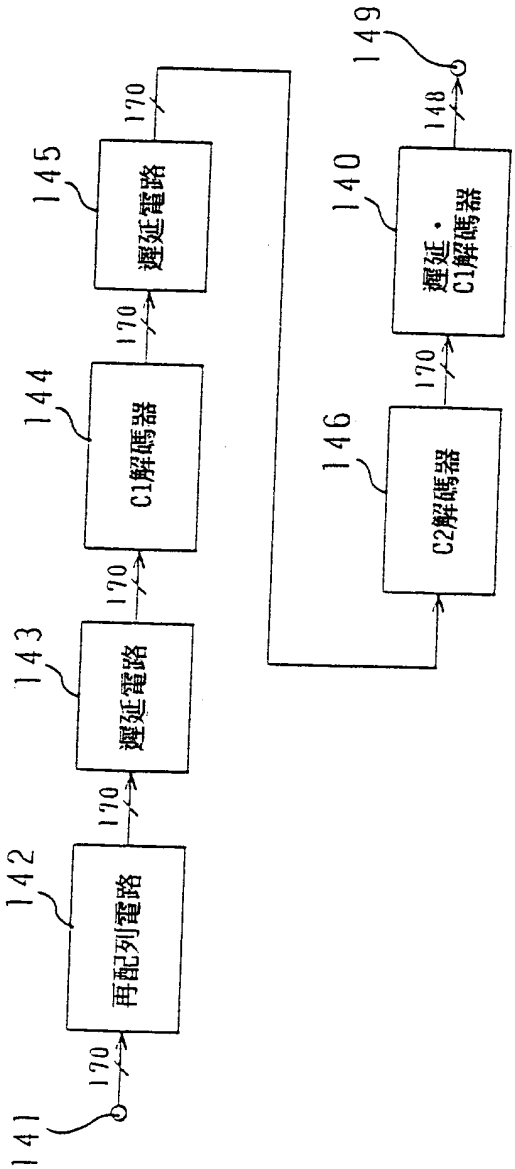
第17圖


101
M
108
109
112
111
TOC
解碼器
113
PLL
114
同步分離
115
解調
CPU
122
錯誤訂正解碼
116
磁區分解
117
頭分離
118
解拌碼處理
119
界面
120
121

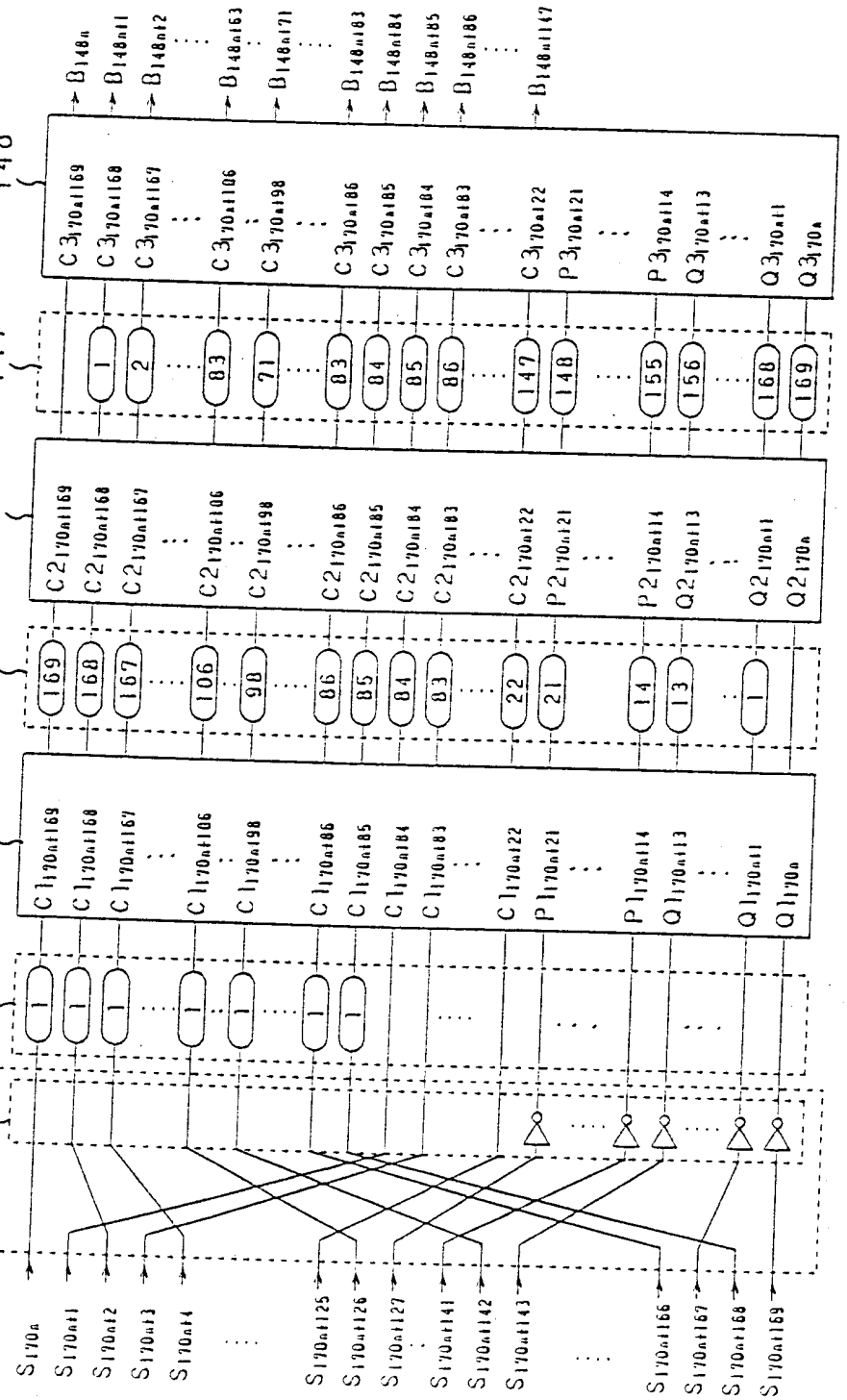
第18圖



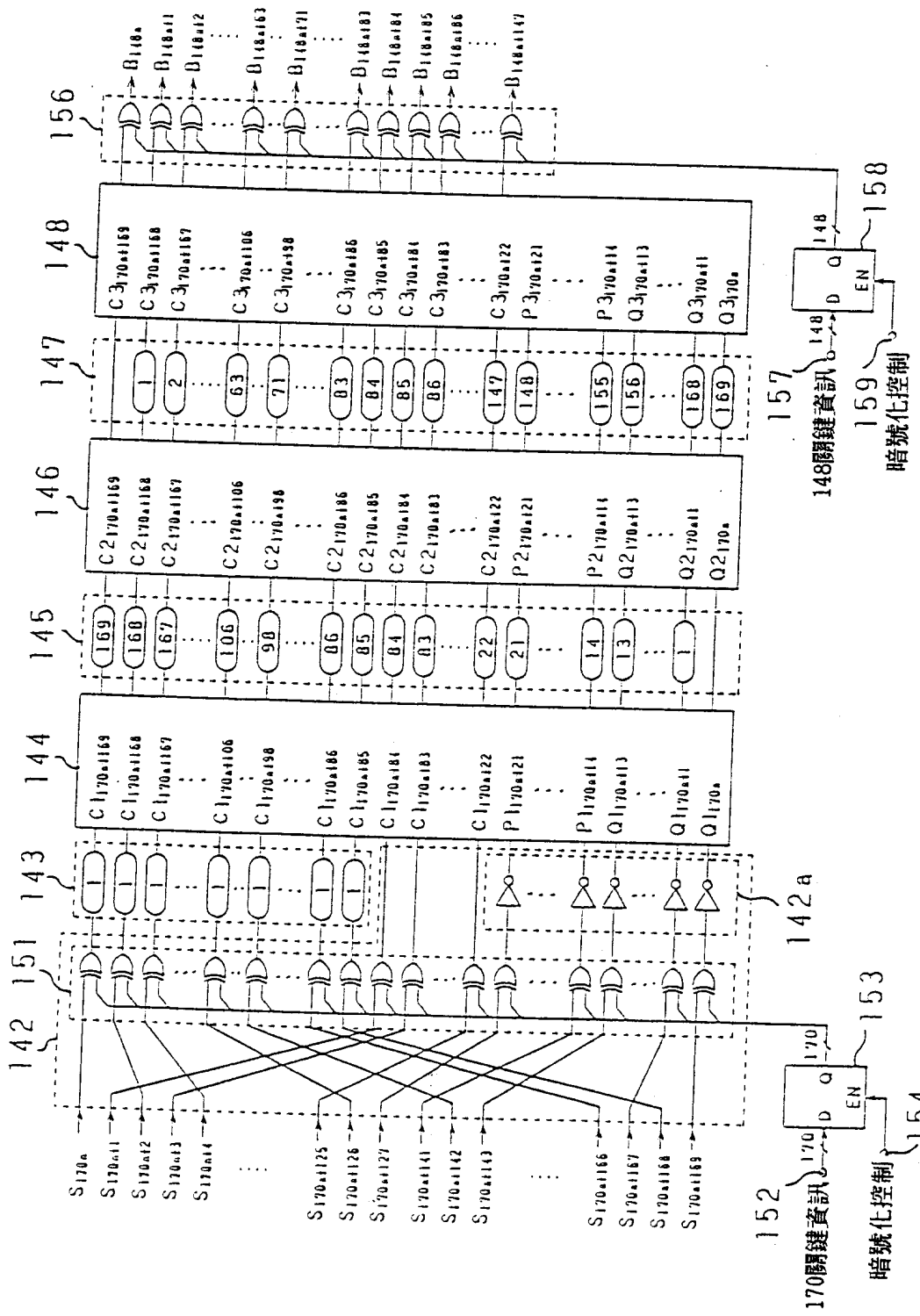
第19圖


141
170
142
再配列電路
170
143
遲延電路
170
144
C1解碼器
170
145
遲延電路
170
146
C2解碼器
170
140
遲延・
C1解碼器
148
149

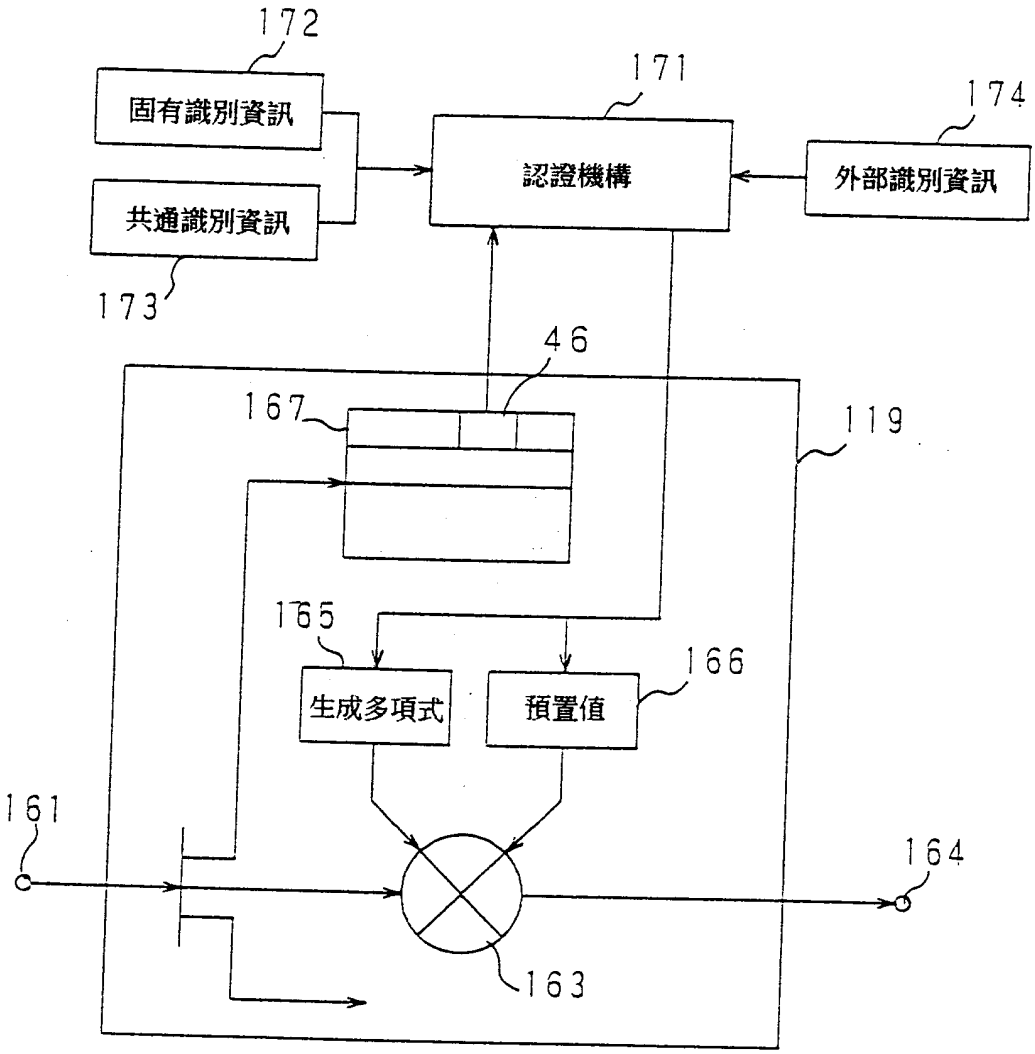
第20圖



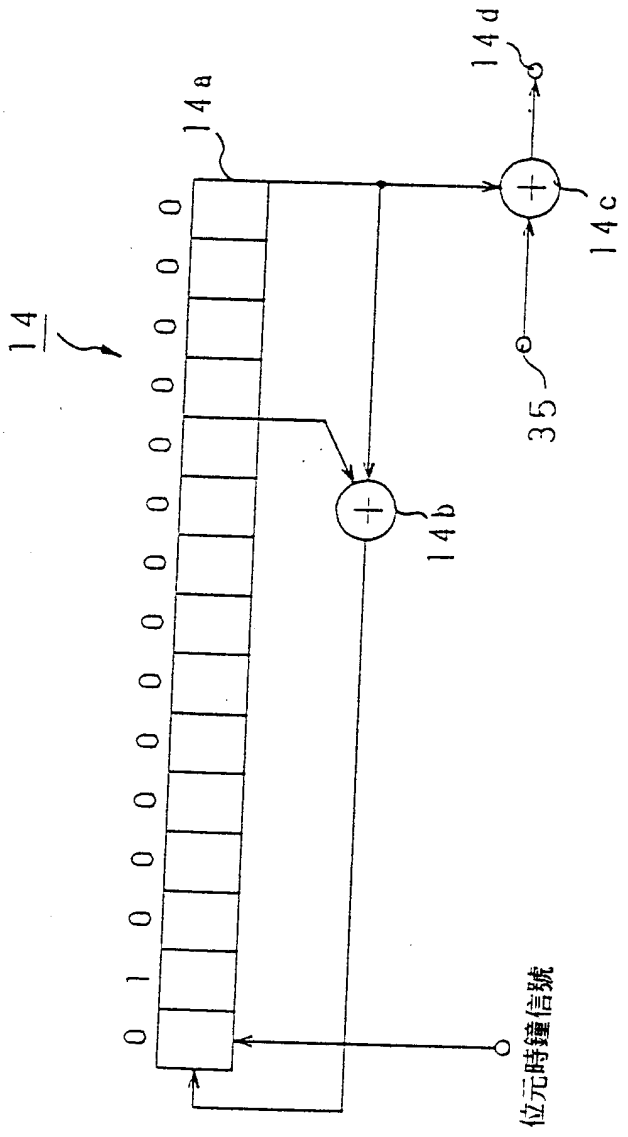
第21圖


142
151
143
144
145
146
147
148
156
142a
152
153
154
157
158
159
170關鍵資訊
暗號化控制
148關鍵資訊
暗號化控制

第22圖


172
固有識別資訊
171
174
認證機構
外部識別資訊
共通識別資訊
173
46
167
119
165
166
生成多項式
預置值
161
164
163

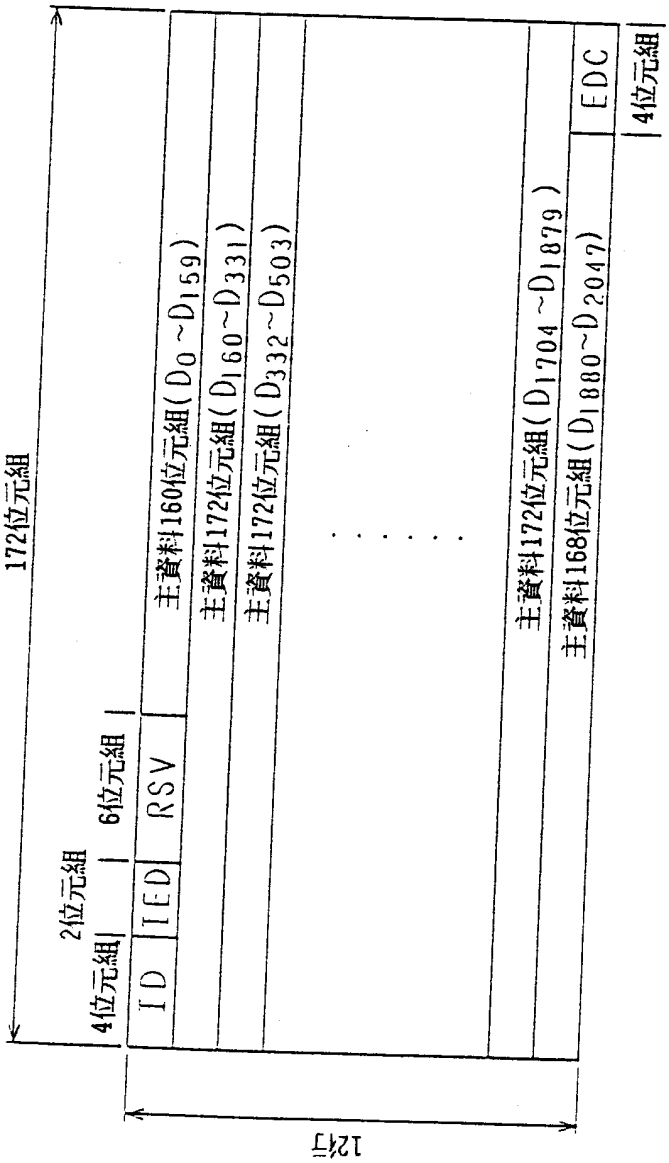
第23圖



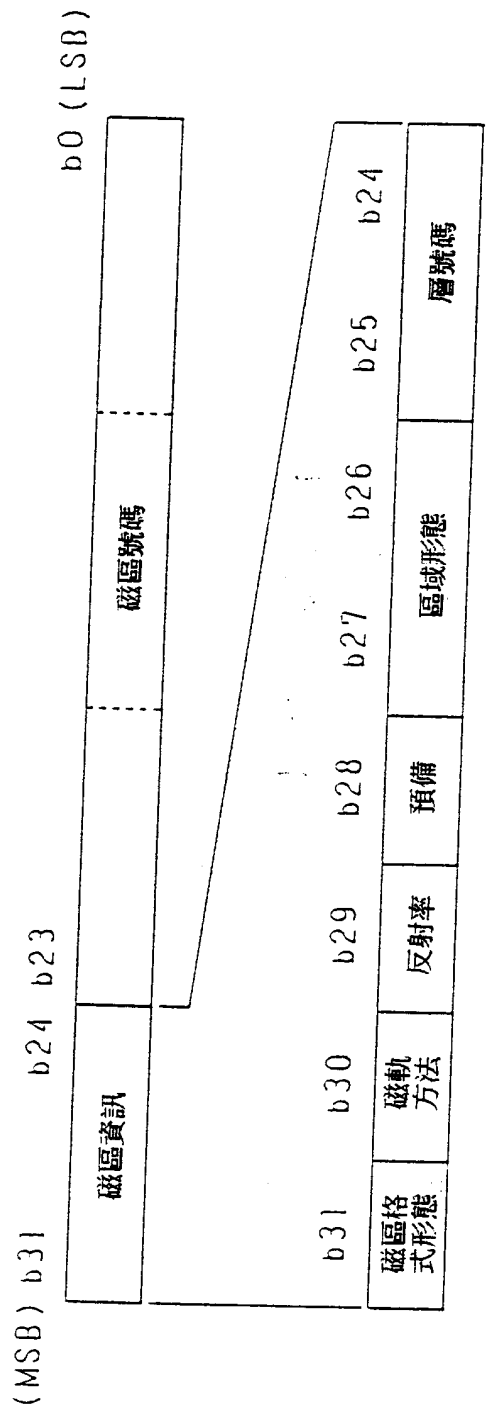
第24圖

選擇號碼	預置值	選擇號碼	預置值
0	$0001	8	$0010
1	$5500	9	$5000
2	$0002	10	$0020
3	$2A00	11	$2001
4	$0004	12	$0040
5	$5400	13	$4002
6	$0008	14	$0080
7	$2800	15	$0005

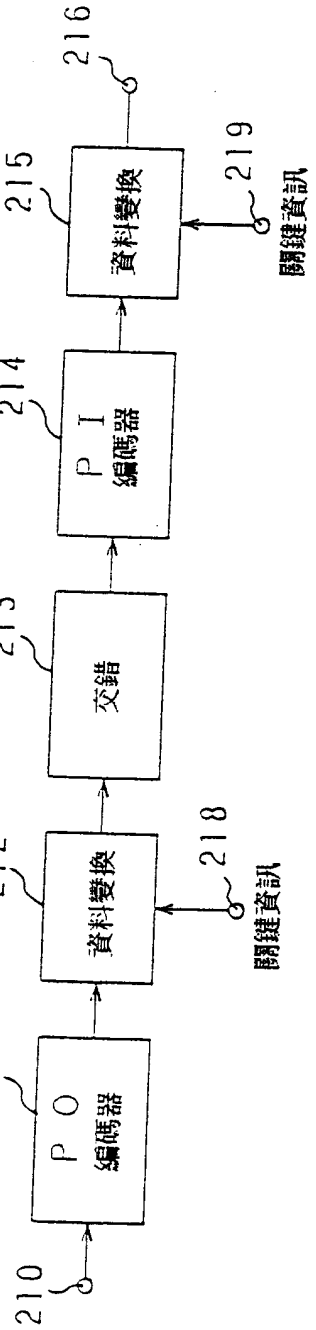
第25圖


172位元組
2位元組
4位元組
6位元組
ID
IED
RSV
主資料160位元組(D0~D159)
主資料172位元組(D160~D331)
主資料172位元組(D332~D503)
主資料172位元組(D1704~D1879)
主資料168位元組(D1880~D2047)
EDC
4位元組
124行

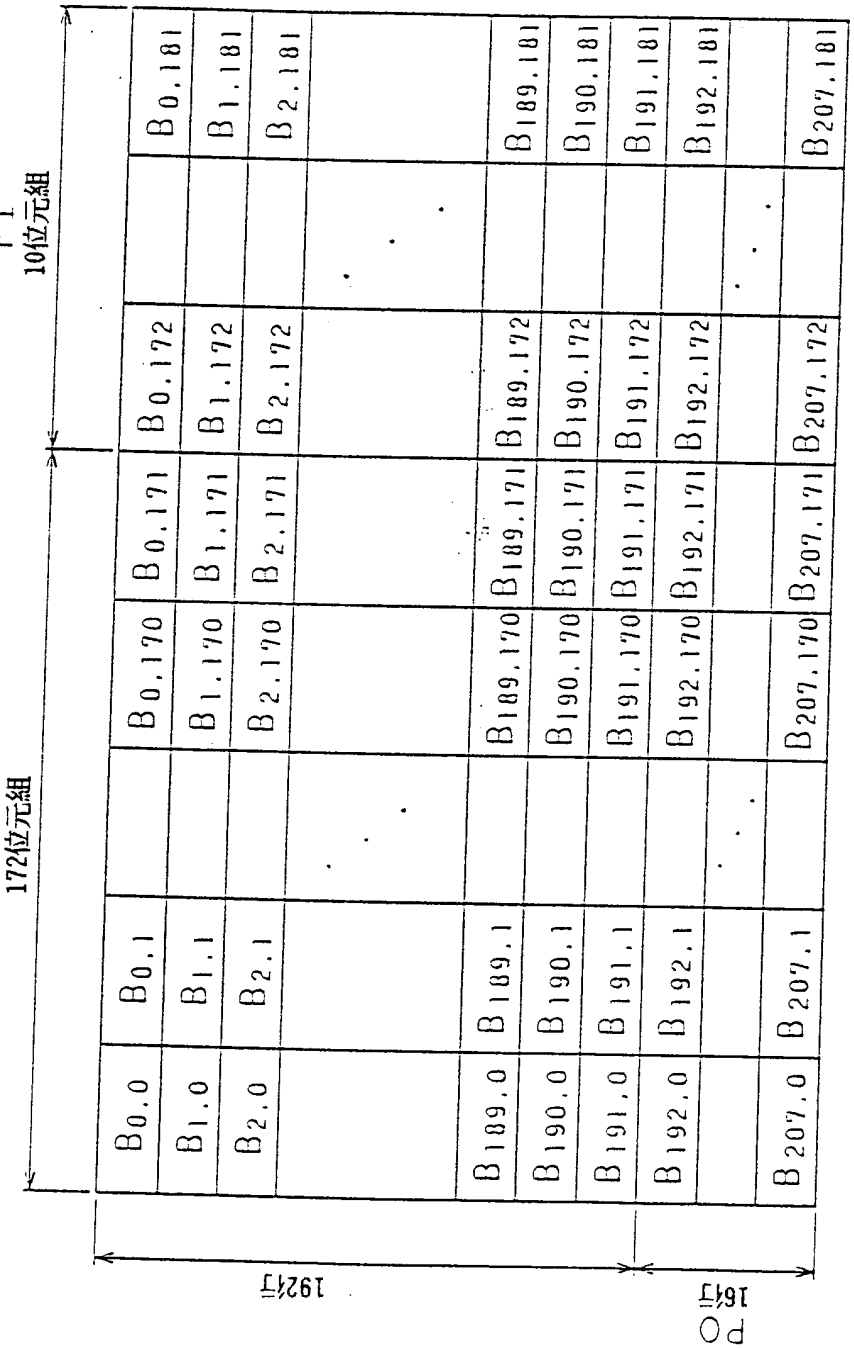
第26圖


(MSB) b31
b24 b23
b0 (LSB)
磁區資訊
磁區號碼
b31
b30
b29
b28
b27
b26
b25
b24
磁區格式形態
磁軌方法
反射率
預備
區域形態
層號碼

第27圖


210
211
PO
編碼器
212
資料變換
218
關鍵資訊
213
交錯
214
PI
編碼器
215
資料變換
219
關鍵資訊
216

第28圖


172位元組
PI
10位元組
192行
164行
PO
B0,0 B0,1 B0,170 B0,171 B0,172 B0,181
B1,0 B1,1 B1,170 B1,171 B1,172 B1,181
B2,0 B2,1 B2,170 B2,171 B2,172 B2,181
B189,0 B189,1 B189,170 B189,171 B189,172 B189,181
B190,0 B190,1 B190,170 B190,171 B190,172 B190,181
B191,0 B191,1 B191,170 B191,171 B191,172 B191,181
B192,0 B192,1 B192,170 B192,171 B192,172 B192,181
B207,0 B207,1 B207,170 B207,171 B207,172 B207,181

第29圖


32
1456
32
1456
SY0
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY5
SY5
SY5
SY5
SY5
SY6
SY6
SY6
SY6
SY7
SY7
SY7
SY7
13行
單框架
單框架

第30圖

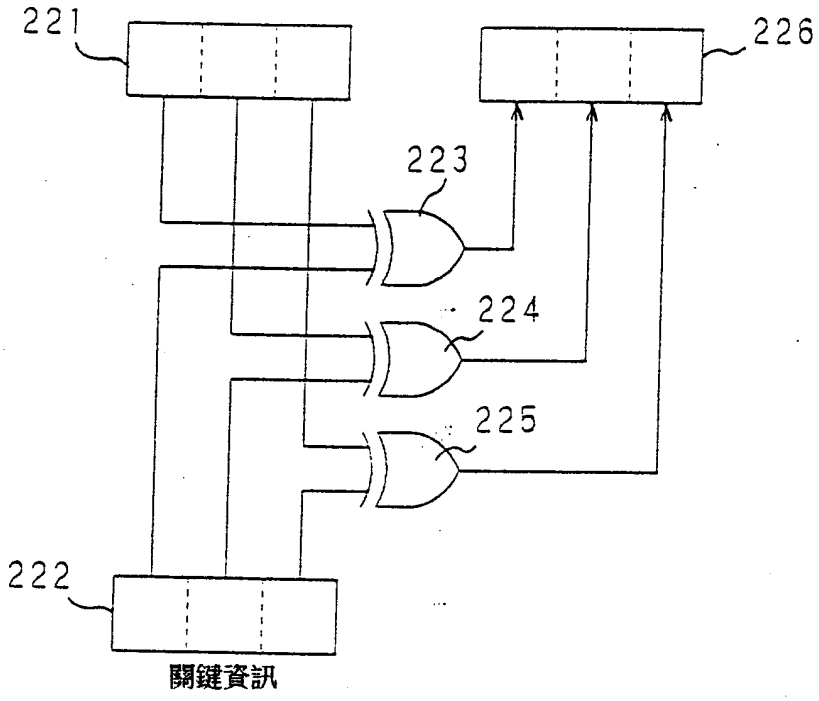
(a)狀態1及2

	(MSB)	(LSB)	(MSB)	(LSB)
SY0=	0001001001000100	0000000000010001	0001001000000100	0000000000010001
SY1=	0000010000000100	0000000000010001	0000010001000100	0000000000010001
SY2=	0001000000000100	0000000000010001	0001000001000100	0000000000010001
SY3=	0000100000000100	0000000000010001	0000100001000100	0000000000010001
SY4=	0010000000000100	0000000000010001	0010000001000100	0000000000010001
SY5=	0010001001000100	0000000000010001	0010001000000100	0000000000010001
SY6=	0010010010000100	0000000000010001	0010000010000100	0000000000010001
SY7=	0010010001000100	0000000000010001	0010010000000100	0000000000010001

(b)狀態3及4

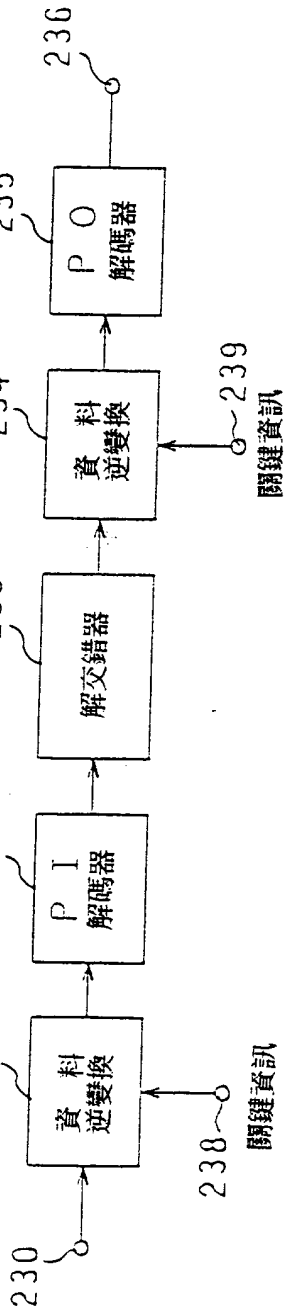
	(MSB)	(LSB)	(MSB)	(LSB)
SY0=	1001001000000100	0000000000010001	1001001001000100	0000000000010001
SY1=	1000010001000100	0000000000010001	1000010000000100	0000000000010001
SY2=	1001000001000100	0000000000010001	1001000000000100	0000000000010001
SY3=	1000001001000100	0000000000010001	1000001000000100	0000000000010001
SY4=	1000100001000100	0000000000010001	1000100000000100	0000000000010001
SY5=	1000100100000100	0000000000010001	1000000100000100	0000000000010001
SY6=	1001000010000100	0000000000010001	1000000001000100	0000000000010001
SY7=	1000100010000100	0000000000010001	1000000010000100	0000000000010001

第31圖



321764

第32圖


230
231
資料逆變換
238
關鍵資訊
232
PI解碼器
233
解交錯器
234
資料逆變換
239
關鍵資訊
235
PO解碼器
236