

申請日期	88.10.18
案號	88117981
類別	G66F 12/14

A4
C4

461996

(以上各欄由本局填註)

發明專利說明書

一、發明 名稱	中 文	資料編碼裝置與非法更改防止系統
	英 文	DATA ENCIPHERMENT APPARATUS AND ILLEGAL ALTERATION PREVENTION SYSTEM
二、發明 創作人	姓 名	森下卓也
	國 籍	日本
	住、居所	東京都港區芝五丁目7番1號 日本電氣株式會社內
三、申請人	姓 名 (名稱)	日本電氣股份有限公司 (日本電氣株式會社)
	國 籍	日本
	住、居所 (事務所)	東京都港區芝五丁目7番1號
	代 表 人 姓 名	西垣浩司

裝

訂

線

1996

(由本局填寫)

承辦人代碼：
大 類：
I P C 分類：

A6

B6

本案已向：

日 本 國 (地 區) 申 請 專 利 , 申 請 日 期 : 案 號 : , ☒ 有 ☐ 無 主 張 優 先 權

1998年10月19日特願平10-297081號

有關微生物已寄存於： , 寄存日期： , 寄存號碼：

(請先閱)
面之注意事項再填寫本頁各欄)

經濟部中央標準局員工消費合作社印製

五、發明說明(¹)

(發明背景)

(發明領域)

本發明係關於防止非法使用者企圖非法使用軟體或資料(非法複印等)而更改(alternation)電腦軟體或資料之資料編碼裝置及非法更改防止系統。

(相關技術說明)

用於防止非法複印電腦軟體之技術係為已知，例如，日本專利公報第平9-231137號，名稱"複製辨別方法及讀出裝置"所揭露者。依該裝置具有特定錯誤率K之鍵碼係被證存於部份之CD-ROM(小巧磁碟唯讀記憶體)內。錯誤率K值係被選定為使讀取裝置上錯誤校正編碼-解碼裝置無法對CD-ROM執行完全之錯誤校正。如果CD-ROM被非法地複印時鍵碼之錯誤率則改變。上述之裝置係使用此剛述及之現象辨別載入裝置之CD-ROM是否為一非法複製之CD-ROM，如果是的話則停止讀取裝置之動作。

另外一種廣為人知，採用相似之非法複印防止技術，之系統係增加具有特定鍵之簡單硬體，當執行程式時系統則辨別該鍵之值是否正常，只有當正常時程式才容許被執行。

上述之以往裝置及系統具有下述問題。

第1個問題為難於分種程式碼及藉何種機構辨別非法複印。理由係能藉分析工具，諸如反向組譯程式(disassembler)工具，分析程式碼及根據分析結果改程式，進而非法使用程式。

五、發明說明(²)

第 1 個問題為如果程式碼被更改時則無法阻止其被複印於貯存媒體。其理由係如果程式用於辨別被複印之貯存媒體之程式碼之部份被更改致其經常指示該媒體係為原版，即使其係為複印版，時則無法阻止藉複印之媒體執行軟體。相似之問題不僅會發生在程式上，亦會發生在資料上。

(發明概述)

本發明之目的係提供能防止非法使用者企圖更改及非法使用資料，諸如程式碼之編碼裝置及非法更改防止系統。

為達成上述目的，依本發明之型態，提供資料編碼裝置，其包含將資料分成第 1 至第 $n+1$ 個區塊之裝置， n 係等於或大於 1 之整數；用於分別根據第 1 至第 n 個區塊之資料接續地產生第 1 至第 n 個密碼鍵之密碼鍵產生裝置，分別藉第 1 至第 n 個密碼鍵接續地對第 2 至第 $n+1$ 個區塊進行編碼之編碼裝置；及用於接續地輸出第 1 區塊及編碼之第 2 至第 $n+1$ 個區塊之輸出裝置。

輸出裝置可根據事先決定之第 0 個密碼鍵對第 1 區塊編碼並輸出編碼之第 1 區塊。

依本發明之其它型態，提供資料之非法更改防止系統，其包含資料處理裝置，檔案裝置及用於產生要被寫入檔案裝置之資料之編碼裝置，此編碼裝置含有將資料分成第 1 至第 $n+1$ 個區塊之裝置， n 係等於或大於 1 之整數；用於分別根據第 1 至第 n 個區塊之資料接續地產生

五、發明說明 (3)

第 1 至第 n 個密碼鍵之密碼鍵產生裝置；分別藉第 1 至第 n 個密碼鍵接續地對第 2 至第 $n+1$ 個區塊進行編碼之編碼裝置；及用於接續地輸出第 1 區塊及編碼之第 2 至第 $n+1$ 個區塊之裝置。

依本發明之另外型態，提供資料之非法更改防止系統，其包含資料處理裝置；含有用於貯存頂部區塊資料之第 1 貯存區及用於貯存跟在頂部區塊後之 n 個資料區塊之第 2 個貯存區之檔案裝置， n 係等於或大於 1 之整數；及用於產生要被寫入檔案裝置之資料之編碼裝置，此編碼裝置能動作以根據第 1 貯存區之資料產生第 1 密碼鍵，藉第 1 密碼鍵對 n 個區塊之第 1 個區塊編碼，根據 n 個區塊之 i 個區塊之資料接續地產生 i 個密碼鍵並藉 i 個密碼鍵接續地對 i 個區塊編碼， i 係等於或大於 2 但等於或小於 n 之整數，前述資料處理裝置含有用於讀取第 1 貯存區之資料之第 1 讀取裝置；用於接續地讀取第 2 貯存區之資料之第 2 讀取裝置；用於藉接續地供給之密碼鍵接續地對被第 2 讀取資料讀取之 i 個區塊接續地解碼之解碼裝置；及用於根據第 1 讀取資料之輸出產生第 1 密碼鍵並將第 1 密碼鍵供給至解碼裝置，根據從解碼裝置輸出之 $i-1$ 個區塊之解碼輸出接續地產生 i 個密碼鍵及接續地供給 i 個密碼鍵至解碼裝置之密碼鍵計算裝置。

資料之非法更改防止系統可構成爲第 1 貯存區已存有藉事先決定之第 0 個密碼鍵編碼之頂部區塊資料，及第

五、發明說明(4)

1 讀取裝置藉第 0 個密碼鍵對貯存於第 1 貯存區內之資料編碼並輸出編碼之資料。

密碼鍵計算裝置可使用單向函數產生第 1 至第 n 個密碼鍵。

於資料編碼裝置及非法更改防止系統上，因程式碼大都被編碼，故其本身難於藉分析工具，如反向組譯程式，分析程式碼。另外，因目前執行之程式碼之單向函數係被密碼鍵計算裝置做為解碼鍵計算並用來對次一個要被執行之程式碼解碼，故難於被更改及非法使用程式碼。

本發明之上述及其它目的，特徵及優點將隨著下面參照附圖所作之敘述及申請專利範圍各項之陳述而更形清楚，附圖上相同之部件或元件係用相同之符號表示。

(附圖之簡述)

第 1 圖係實施本發明之非法使用防止系統之方塊圖；

第 2 圖係說明第 1 圖之非法使用防止系統之動作之流程圖；

第 3 圖係說明當非法使用者未執行更改程式碼之企圖時第 1 圖之非法使用防止系統之動作之流程圖；及

第 4 圖係示出用於產生要被寫入第 1 圖之非法使用防止系統之檔案裝置之資料之編碼裝置之構成之方塊圖。

(良好實例之敘述)

第 1 圖示出實施本發明之非法使用防止系統之軟體。所示之非法使用防止系統包括在程式之控制下動作之資料處理裝置 100，檔案裝置 110，及編碼裝置 120。資

五、發明說明 (5)

料處理 100 包含非編碼程式讀取部 101，密碼鍵計算部 102，編碼程式讀取部 103，及解碼部 104。檔案裝置 110 包含非編碼程式貯存部 111 及加編碼程式貯存部 112。

非編碼程式貯存部 111 內存有非編碼程式碼。編碼程式貯存部 112 內存有多數區塊或程式 1，2，---，n 之編碼程式碼。非編碼程式碼及編碼程式碼係以貯存於非編碼程式貯存部 111 內之非編碼程式碼及編碼區塊 1，2，---，n 之順序被讀入資料處理裝置 100。

非編碼程式讀取部 101 從非編碼程式貯存部 111 將非編碼程式碼讀入未圖示之主貯存部。

密碼鍵計算部 102 使用單向函數，諸如存在主貯存部 5 之程式碼之隨機函數，以產生要被用來轉換被讀入其內之編碼程式碼區塊為平面文件 (plaintext) 之密碼鍵。編碼程式讀取部 103 從編碼程式貯存部 112 將次一個要被執行之這些程式碼讀入主貯存部。解碼部 104 使用被密碼鍵計算部 102 算出之密碼鍵對編碼之程式碼進行解碼。

下面將參照第 4 圖敘述用於產生要被寫入檔案裝置 110 之資料之編碼裝置 120，圖上示出編碼裝置 120 之構成。

要被貯存於檔案裝置 110 之程式碼係被送至分岐電路 201。分岐電路 201 將收到之程式碼分割成 $n+1$ 個區塊，並將頂部區塊寫入第 1 圖所示之非編碼程式貯存部 111 並進一步將之供給至密碼鍵計算部 102。在輸出頂部區

五、發明說明 (6)

塊後分歧電路 201，接續地將除了頂部區塊或第 0 個區塊外剩餘之 n 個區塊輸出到遲延電路 203 及密碼鍵計算部 102。

密碼鍵計算部 102 當收到來自分歧電路 201 之頂部區塊時則使用單向函數，如頂部區塊之程式碼之隨機函數，以計算要被用來對次於頂部或第 0 個區塊之區塊（第 1 個區塊）之資料進行編碼之第 1 個密碼鍵。俟第 1 個密碼鍵被輸出後第 1 區塊，第 2 區塊，---，第 n 個區塊則接續地被送到密碼鍵計算部 102，而第 2 個密碼鍵，---，第 n 個密碼鍵也就接續地從密碼鍵計算部 102 輸出至編碼單元 204。

其時，遲延電路 203 接續地對接續地來自分歧電路 201 之第 1 個至第 n 個區塊遲延一個區塊之時間間隔並輸出遲延後之區塊。結果，第 1 個區塊係被藉第 0 個區塊之資料所產生之第 1 個密碼鍵編碼並被貯存於第 1 圖所示之編碼程式貯存部 112 內。第 2 個區塊係被藉第 1 個區塊之資料所產生之第 2 個密碼鍵編碼並被貯存於第 1 圖所示之編碼程式貯存部 112 內。相似地，第 i 個區塊係被藉第 $i-1$ 個區塊之資料所產生之第 i 個密碼鍵並被貯存於第 1 圖所示之編碼程式貯存部 112 內。

以這種方式，非編碼程式碼係被存入非編碼程式貯存部 111，而編碼程式則被分割成多數之區塊 1，2，---， n 存入編碼程式貯存部 112。

下面將參照第 2 圖之方塊圖敘述整體非法使用防止系

五、發明說明 (7)

統之動作。

於編碼程式貯存部 112 上，對應於貯存在非編碼程式貯存部 111 內之程式碼之程式碼係被貯存於多數之區塊內，每個區塊含有使用該區塊之緊鄰之前一區塊之程式碼之隨機值做為密碼鍵而被編碼之程式碼。

首先於步驟 A1 上，非編碼程式讀取部 101 從非編碼程式貯存部 111 將非編碼程式碼讀入主貯存部並開始執行程式編碼。此處理一般係由作業系統之程式執行機構管理。

於步驟 A2 上，密碼鍵計算部 102 藉單向函數，如隨機函數，將非編碼程式讀取部 101 讀進貯存部內之程式碼轉換成密碼鍵。

於步驟 A3 上，編碼程式讀取部 103 係編碼程式貯存部 112 將這些稍後要被執行之編碼程式碼讀進主貯存部。

於步驟 A4 上，解碼部 104 使用密碼鍵計算部 102 算出之密碼鍵對編碼程式碼進行解碼。

於步驟 A5 上，密碼鍵計算部 102 計算要做為下一個解碼用之解碼程式碼之隨機值。

接著於步驟 A6 上，執行目前存在主貯存部上之解碼程式碼。此處理步驟係執行非法複印等之辨別。

於步驟 A7 上，辨別步驟 A3 至 A6 之處理是否已對貯存於編碼程式貯存部 112 上之所有區塊之程式碼執行。如果有區塊之程式碼尚未被執行前述處理時資料處理裝置之控制則返回步驟 A3。

五、發明說明(8)

第3圖示出當企圖更改程式碼未被非法使用者執行時非法使用防止系統之動作流程。如果程式碼未被更改時則藉編碼程式碼解碼用之密碼鍵a, b及c得出正確值。

如果貯存於非編碼程式碼貯存部111之非編碼程式碼被更改時則在步驟A3上算出之密碼鍵之值迥異於原來之密碼鍵a。因此, 在步驟A4上解碼之程式碼2係與其之原來程式碼差異極大, 進而隨後之程式不會正常地執行。另外當編碼之程式碼貯存部112之內之程式碼被更改時跟隨在被更改之程式碼後之區塊當於步驟A4上被解碼後係與它們之原來程式碼差異極大, 進而隨在被更改之程式碼後之程式則不會正常動作。

這種方式, 如果程式碼被更改時則為了使跟在更改程式碼後之程式動作正常, 需藉一些裝置蒐集所有隨後之區塊之密碼鍵並更改隨後之區塊之程式碼俾密碼鍵能做為被解碼部104使用之密碼鍵。這種方法係理想地使非法使用者更改程式碼之困難度隨著區塊數目之增加而增加。

雖然本發明實例之非法使用防止系統偵測對程式碼之更改, 但亦可在產生密碼鍵之際利用資料區之單向函數偵測出對資料之更改。於此例子, 前述之"單一程式"或"多數程式"應讀成"資料"。

另外, 雖然本發明實例之計算部改防止系統之前面敘述曾述及在非編碼程式碼貯存部111內之程式碼或資料係以未被編碼之平面文字貯存, 顯然地在非編碼程式碼貯存

五、發明說明(9)

部 111 內之這種程式碼或資料也可用藉既定之密碼鍵編碼之程式碼或資料貯存。於此例子，第 1 圖之非編碼程式讀取部 101 具有根據既定之密碼鍵對非編碼程式貯存部 111 內之編碼資料解碼之功能。

雖然本發明之良好實例已用特定之名詞敘述如上，但這種敘述僅做為說明用，請瞭者係可對本發明作任何修改及變更而不會逾越申請專利範圍各項陳述之精神及範圍。

符號之說明

100	資料處理裝置
101	非編碼程式讀取部
102	密碼鍵計算部
103	編碼程式讀取部
104	解碼部
110	檔案裝置
111	非編碼程式貯存部
112	編碼程式貯存部
120	編碼裝置
201	分岐電路
203	遲延電路
204	編碼單元

四、中文發明摘要(發明之名稱：

資料編碼裝置與非法更改防止系統)

本發明提供能防止非法使用者企圖更改及非法使用諸如程式碼之資料之編碼(encipherment)裝置及非法更改防止系統。編碼後之程式碼係分區地被貯存在編碼後程式貯存部之多數區塊內。密碼鍵計算部使用單向函數(one-way function), 諸如目前存在於主貯存部上之程式碼之隨機函數(hash function), 算出要被用於解碼(decipherment)這些被貯存於編碼後程式貯存部之編碼後之程式區塊內之編碼程式碼及爾後要被執行之密碼鍵。如果欲非法使用軟體而更改程式碼時程式則停止執行。

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

四、~~英~~文發明摘要(發明之名稱: DATA ENCIPHERMENT APPARATUS AND ILLEGAL)
ALTERNATION PREVENTION SYSTEM

The invention to provide an encipherment apparatus and an illegal alteration prevention system which can prevent an attempt of alteration to and illegal use of data such as program codes by an illegal user. Enciphered program codes are divisionally stored in a plurality of blocks in an enciphered program storage section. A cryptographic key calculation section uses a one-way function such as a hash function of the program codes currently present on a main storage section to calculate a cryptographic key to be used for decipherment of those enciphered program codes of a block stored in the enciphered program storage section and to be executed subsequently. If any of the program codes is altered in order to illegally utilize the software, then correct cryptographic keys are not obtained later, and execution of the program is halted.

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

錄

六、申請專利範圍

1. 一種資料編碼裝置，其包含：

用於分割資料成第 1 至第 $n+1$ 個區塊之裝置， n 係等於或大於 1 之整數；

用於分別根據第 1 至第 n 個區塊之密碼鍵接續地產生第 1 至第 n 個密碼鍵之密碼鍵產生裝置；

用於藉第 1 至第 n 個密碼鍵接續地對第 2 至第 $n+1$ 個區塊編碼之編碼裝置；及

用於接續地輸出第 1 區塊及編碼之第 2 至第 $n+1$ 個區塊之輸出裝置。

2. 如申請專利範圍第 1 項之資料編碼裝置，其中，該輸出裝置根據事先決定之第 0 個密碼鍵對第 1 區塊編碼及輸出編碼之第 1 區塊。

3. 一種資料之非法更改防止系統，其包含：

資料處理裝置；

檔案裝置；及

用於產生要被寫入該檔案裝置之資料之編碼裝置；

該編碼裝置含有：

用於將資料分割成第 1 至第 $n+1$ 個區塊之裝置， n 係等於或大於 1 之整數；

用於分別根據第 1 至第 n 個區塊之資料接續地產生第 1 至第 n 個密碼鍵之密碼鍵產生裝置；

用於分別藉第 1 至第 n 個密碼鍵接續地對第 2 至第 $n+1$ 個區塊編碼之編碼裝置；及

用於接續地輸出第 1 區塊及編碼之第 2 至第 $n+1$ 個

六、申請專利範圍

區塊之輸出裝置。

4. 一種資料之非法更改防止系統，其包含：

資料處理裝置；

含有用於貯存資料之頂部區塊之第1貯存區及用於貯存跟在頂部區塊後面之 n 個資料區塊之第2貯存區之檔案裝置， n 係為等於或大於1之整數；及

用於產生要被寫入該檔案裝置之資料之編碼裝置，該編碼裝置係能根據該第1貯存區之資料以產生第1密碼鍵，藉第1密碼鍵對第 n 區塊之第1區塊編碼，接續地根據第 n 個區塊之 i 個區塊產生 i 個密碼鍵及藉 i 個密碼鍵接續地對 i 個區塊編碼， i 係等於或大於2但等於或小於 n ；

該資料處理裝置包含：

用於讀出該第1貯存區之資料之第1讀出裝置；

用於接續地讀出該第2貯存區之資料之第2讀出裝置；

用於接續地對被該第2讀出裝置接續地讀出之 i 個區塊藉接續地收到 i 個密碼鍵執行解碼之解碼裝置；及

用於根據該第1讀出裝置之輸出產生第1密碼鍵；供給第1密碼鍵至該解碼裝置；根據來自該解碼裝置之 i 個區塊之解碼輸出接續地產生 i 個密碼鍵及接續地供給 i 個密碼鍵至該解碼裝置之密碼鍵計算裝置。

5. 如申請專利範圍第4項之資料之非法更改防止系統，

(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

其中資料係為程式碼。

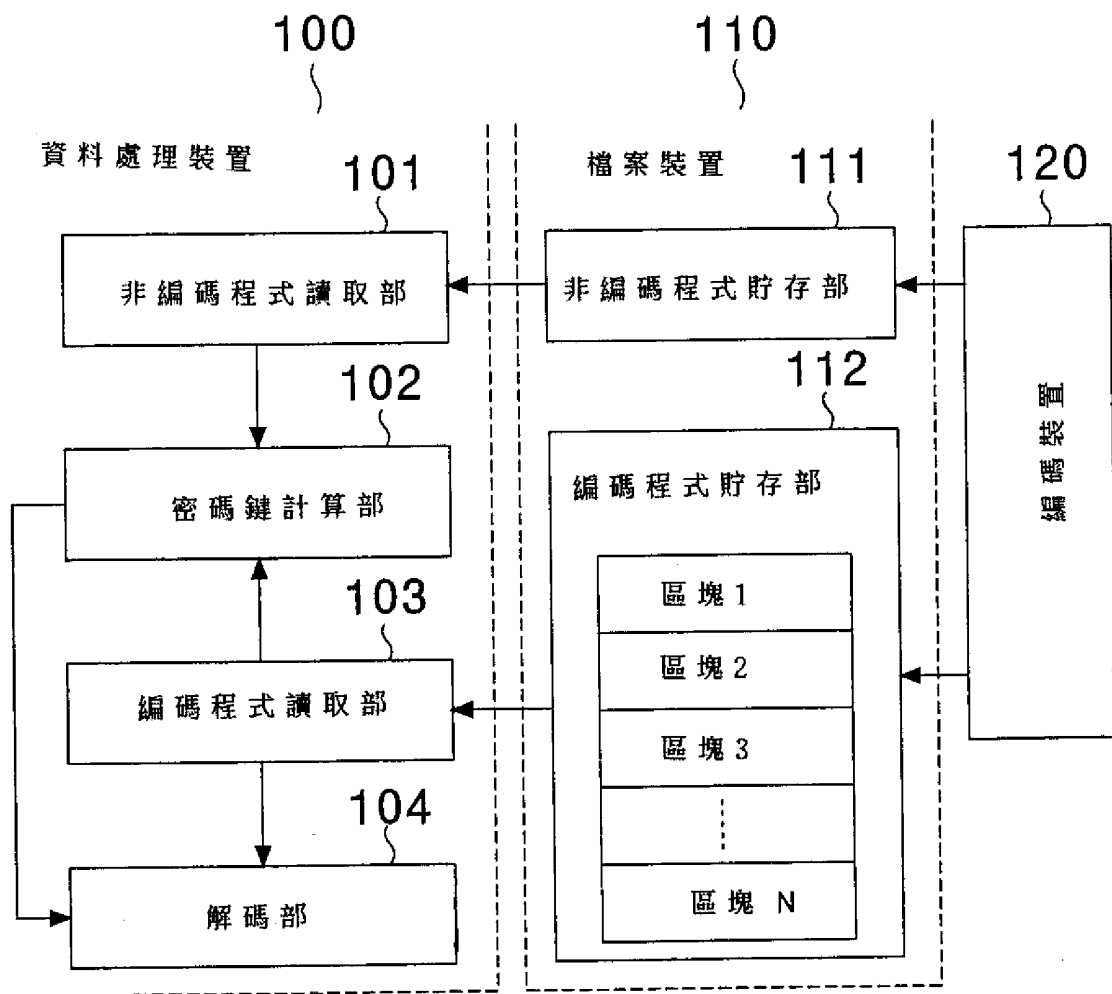
6. 如申請專利範圍第4項之資料之非法更改防止系統，
其中該第1貯存區內存有藉預先決定之第0個密碼鍵
編碼之資料之頂部區塊及該第1讀出裝置藉第0個密
碼鍵對貯存於該第1貯存區內之資料執行編碼。
7. 如申請專利範圍第4項之資料之非法更改防止系統，
其中該編碼程式計算裝置使用單向函數以產生第1至
第n個密碼鍵。

(請先閱讀背面之注意事項再填寫本頁)

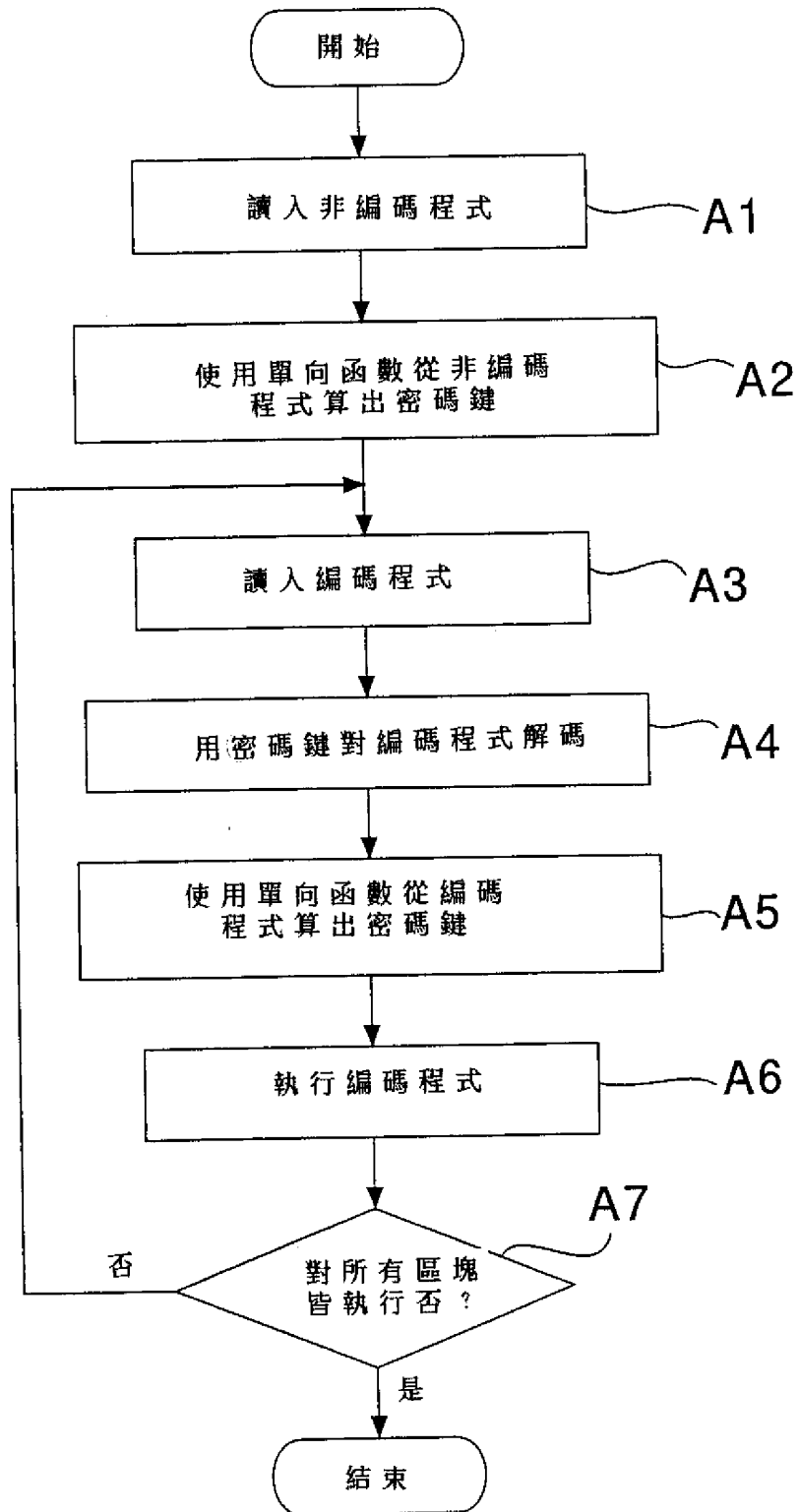
裝

訂

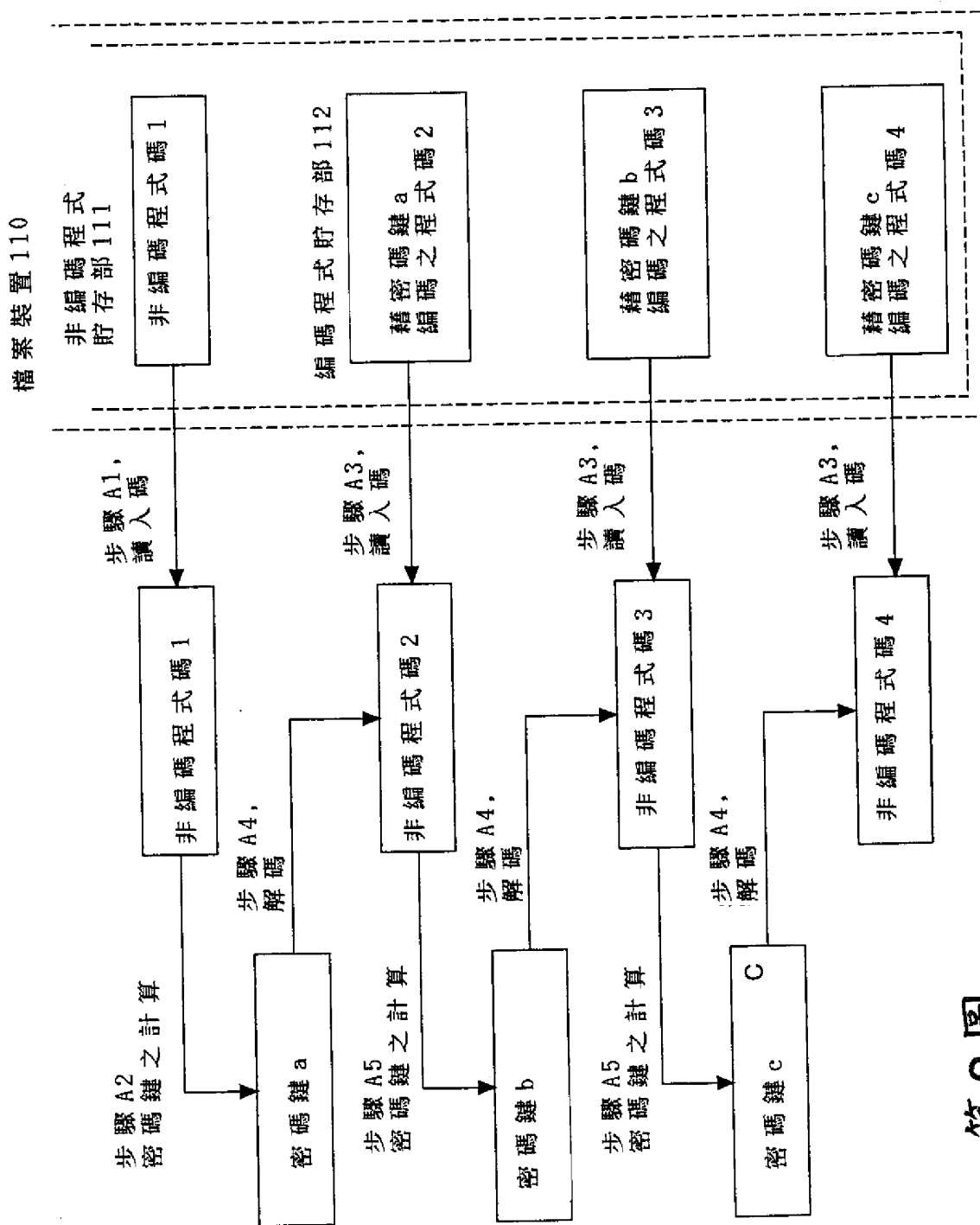
線



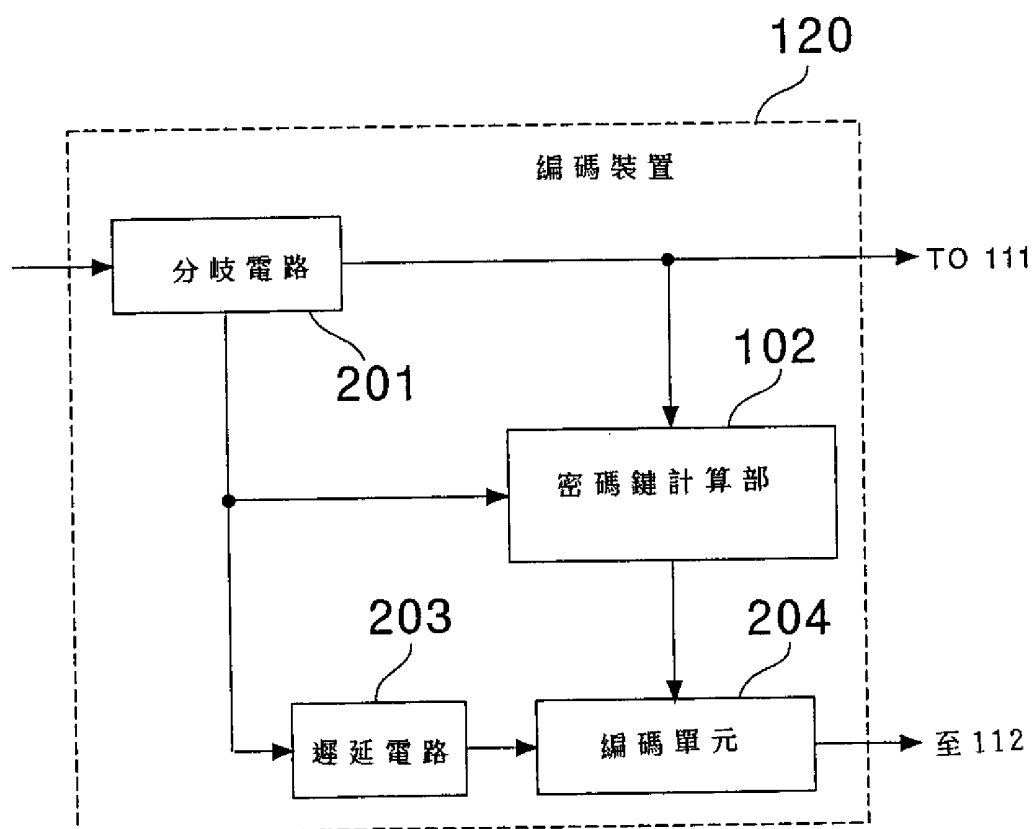
第1圖



第2圖



第3圖



第4圖