I445323

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I445323 B**

(45)公告日： 中華民國 103 (2014) 年 07 月 11 日

(21)申請案號：099145027 (22)申請日： 中華民國 99 (2010) 年 12 月 21 日

(51)Int. Cl.： ***H03M7/20 (2006.01)***

(71)申請人：財團法人工業技術研究院 (中華民國) INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE (TW)

新竹縣竹東鎮中興路 4 段 195 號

國立交通大學 (中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)

新竹市大學路 1001 號

(72)發明人：易志偉 YI, CHIH WEI (TW) ；劉炳傳 LIU, PIN CHUAN (TW) ；呂孝恆 LU, HSIAO HENG (TW)

(74)代理人：洪堯順

(56)參考文獻：

EP 1055287B1 US 2006/0153315A1

Svetla Nikova, Vincent Rijmen, Martin Schläffer, "Using Normal Bases for Compact Hardware Implementations of the AES S-box" Security and Cryptography for Networks Lecture Notes in Computer Science, Volume 5229, 2008, pp. 236-245.

審查人員：陳臆聰

申請專利範圍項數：17 項 圖式數：14 共 0 頁

(54)名稱

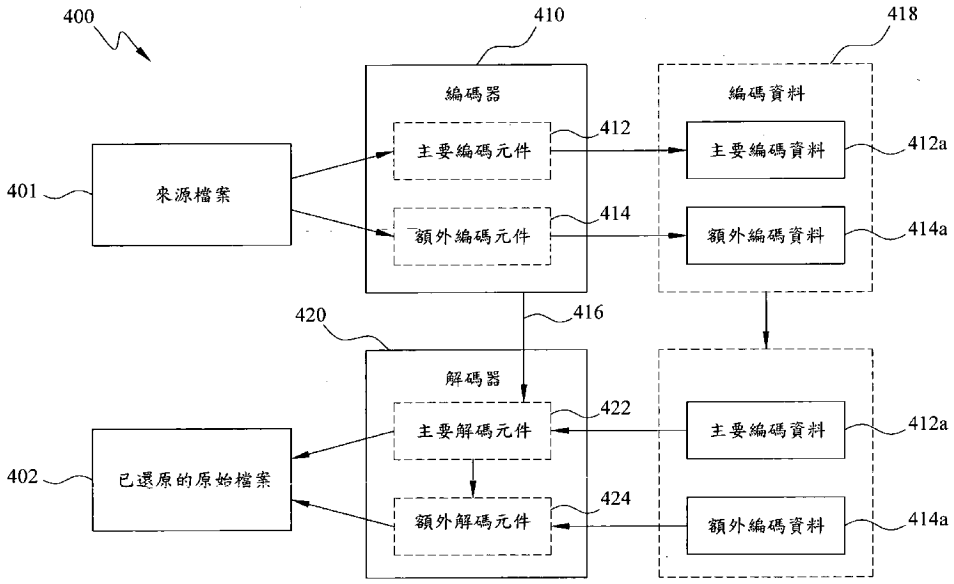
資料傳送的混合式編解碼裝置與方法

HYBRID CODEC APPARATUS AND METHOD FOR DATA TRANSFERRING

(57)摘要

在一種資料廣播的混合式編解碼裝置中，使用一個編碼器將來源檔案切割成 N 個子區段，並在第一有限場編碼產生 N 筆主要編碼資料，且將此 N 個子區段在第二有限場編碼產生 k 筆額外編碼資料後，輸出一組編碼係數及 N +k 筆編碼資料至解碼器。解碼器接收到此組編碼係數及此 N +k 筆編碼資料後，將其中 N 筆主要編碼資料在第一有限場進行解碼，若無法解碼出 N 個子區段時，再利用剩餘 k 筆額外編碼資料在第二有限場輔助資料的解碼運算。依此，解碼出一已還原的來源檔案。

In a hybrid codec apparatus for data transferring, an encoder divides a source file intoN sections, generatesN principle encoded data after coding on a first finite field an dk additional encoded data after coding on a second finite field, then transmits a group of coefficient encoded data and theN +k encoded data to a decoder. The decoder merges the group of coefficient encoded data and theN +k encoded data, and decodes the N principle encoded data on the first finite field. When the decoder fails to decode theN principle encoded data, it uses thek additional encoded data to assist the data decoding on the second finite field. After the decoding, a recovered source file is produced.



第四圖

400・・・混合式編解碼裝置

401・・・來源檔案

410・・・編碼器

412・・・主要編碼元件

412a・・・主要編碼資料

414・・・額外編碼元件

414a・・・額外編碼資料

416・・・一組編碼係數資料

418・・・編碼資料

420・・・解碼器

422・・・主要解碼元件

424・・・額外解碼元件

402・・・已還原的來源檔案

I445323

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：99146027

※申請日：99.12.21　※IPC 分類：H03M 7/20 (2006.01)

一、發明名稱：（中文/英文）

資料傳送的混合式編解碼裝置與方法/

HYBRID CODEC APPARATUS AND METHOD FOR DATA TRANSFERRING

二、中文發明摘要：

在一種資料廣播的混合式編解碼裝置中，使用一個編碼器將來源檔案切割成N個子區段，並在第一有限場編碼產生N筆主要編碼資料，且將此N個子區段在第二有限場編碼產生k筆額外編碼資料後，輸出一組編碼係數及$N+k$筆編碼資料至解碼器。解碼器接收到此組編碼係數及此$N+k$筆編碼資料後，將其中N筆主要編碼資料在第一有限場進行解碼，若無法解碼出N個子區段時，再利用剩餘k筆額外編碼資料在第二有限場輔助資料的解碼運算。依此，解碼出一已還原的來源檔案。

三、英文發明摘要：

In a hybrid codec apparatus for data transferring, an encoder divides a source file into N sections, generates N principle encoded data after coding on a first finite field and k additional encoded data after coding on a second finite field, then transmits a group of coefficient encoded data and the $N+k$ encoded data to a decoder. The decoder merges the group of coefficient encoded data and the $N+k$ encoded data, and decodes the N principle encoded data on the first finite field. When the decoder fails to decode the N principle encoded data, it uses the k additional encoded data to assist the data decoding on the second finite field. After the decoding, a recovered source file is produced.

四、指定代表圖：

(一)本案指定代表圖為：第（四）圖。

(二)本代表圖之元件符號簡單說明：

400 混合式編解碼裝置

401 來源檔案

410 編碼器

412 主要編碼元件

412a 主要編碼資料

414 額外編碼元件

414a 額外編碼資料

416 一組編碼係數資料

418 編碼資料

420 解碼器

422 主要解碼元件

424 額外解碼元件

402 已還原的來源檔案

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本揭露係關於一種資料傳送的混合式(hybrid)編解碼方法與裝置。

【先前技術】

資料在傳輸時，為了讓接收端可以正確地判斷出傳送端送出的資料，一般會進行資料的編碼(encode)。由傳送端將需傳送的資料經過編碼後，再將編碼後的資料經由實體通道傳送出去。而接收端接收到經過編碼的資料後，它會做相對應的解碼(decode)動作，一方面取出原始資料，另一方面確保原始資料的正確性。

目前已發展出許多的編解碼技術，例如：在原始資料後面加入同位元檢查(parity check)，讓接收端可以判斷前面的原始資料是否正確。或是更進一步在原始資料後面加入循環冗餘檢查(Cyclic Redundancy Check，CRC)部份，使得接收端除了可以判斷原始資料是否正確接收外，還可以修正一部份的錯誤。

為了使編碼後的資料分散在電腦網路(computer network)上時，具有高延展性(scalable)與容錯能力(fault-tolerant)，由 Luby 發展出一種新類型的編碼，稱為 LT 碼。第一圖是 LT 碼之編碼的一個範例示意圖。第一圖中，此 LT 編碼使用特殊的機率分佈來決定編碼

時，多筆原始符元(source symbol)110 之每一筆原始符元所使用的分支度(degree)。此 LT 編碼將一來源檔案視為由多個相等大小的區段所組成之組合，從其中取出數個(分支度)區段進行 XOR 運算以產生編碼資料。LT 編碼後的符元 120 是經由重複進行此編碼動作，直到解碼器能夠將來源檔案完全還原為止。

另一種編碼類型稱為 Raptor 碼。Raptor 碼是 LT 編碼的延伸，Raptor 碼使編碼與解碼的工作能在線性時間內完成(with linear time encoding and decoding)。第二圖是 Raptor 碼之編碼的一個範例示意圖。第二圖中，Raptor 碼的編碼過程可分為兩階段，先以低計算複雜度的編碼技術對數個來源檔案區段，即多筆原始符元 210，進行一對一編碼，再將所產生的先編碼符元(Pre-coded symbol)220 使用第一圖之 LT 碼進行二度編碼，然後，Raptor 編碼後的符元 230 被傳送至解碼器。

在節點對節點(Peer To Peer，P2P)系統的應用中，編碼資料會在節點(Peer)間彼此傳遞(Relay)，每一節點會將所收到的編碼資料再次編碼(Re-Code)後，才傳遞給其他節點。因此，若以 Raptor 編碼，則在解碼時需要花費多層次的步驟。

網路編碼是一項在含有多重路徑(multi-path)網路中傳遞檔案的技術。第三圖是將網路編碼技術應用在分散

式(distributed)網路的一個範例示意圖。第三圖中，接收端的網路節點，例如網路節點 R1~R4，會收到來自一或多個其他節點，例如節點 C1~C8 中的節點，的編碼封包，透過多層次的路由傳遞到所指定的目的節點，即網路節點 R1~R4 中的節點，使得目的節點能夠將原始資料還原。每透過一層次的路由傳遞，這些編碼封包就會被編碼一次。例如，透過兩層次的路由傳遞，網路節點 R1 收到來自節點 C1 與 C5 的編碼封包，以及來自節點 C2 與 C6 的編碼封包。也就是說，這些編碼封包透過一層次的路由傳遞，就會被編碼一次。此技術於資料編碼與解碼時，所使用的亂數係數皆位於相同的有限場(Finite Field)中。

網路編碼技術可以用來保護資料傳輸外，也可以有效的利用網路中的連線頻寬。經過多通道傳送的資料，可以彼此的引用，藉由編碼後資料的運算，進一步解碼出原始的資料。在網路編碼技術中，其中一種為亂數線性網路編碼(Random Linear Network Coding，RLNC)技術。此 RLNC 技術使用多位元的有限場(Finite Field)計算做為編解碼的基底，產生複雜的運算，會降低所成就的資料傳輸量與解碼率。

另一種稱為二位元網路編碼(Binary Network coding，BNC)技術，使用 XOR 計算做為編解碼基底。相較於 RLNC 技術，BNC 技術的計算量大幅的減少，

且有較低的資料傳輸經費(overhead)和有效率的編碼運算。當使用 BNC 編碼技術時，一旦發生資料在傳輸時遺失，傳送端需要補充傳送更多的資料。

在網路編碼技術中，編碼器將來源檔案分割成N個子區段，再分別計算所有子區段的線性組合N次來產生不同的主要編碼資料。解碼器可透過矩陣運算將N筆主要編碼資料還原成來源檔案。然而，各別的編碼資料可能形成彼此線性相依的現象，造成無效的編碼資料。因此，編碼器須額外傳送k筆額外編碼資料使得解碼器能夠從收到的$N+k$筆編碼資料中找出N筆彼此線性獨立的編碼資料，並進一步將來源檔案還原。

若N筆主要編碼和k筆額外編碼皆採用空間較小的有限場，例如加邏瓦場(Galois Field) $GF(2)$，則能夠有效率的完成編碼與解碼工作，惟，因為空間小容易導致編碼資料彼此線性相依，因此需要較大的k值來保證N筆線性獨立編碼資料的存在，故其需要較高的資料傳送成本。反之，若N筆主要編碼和k筆額外編碼皆採用空間較大的有限場，例如$GF(2^8)$，因為編碼資料相依不易，所以所需的資料傳送成本也低，但用於編碼與解碼工作的計算量也隨之提高。

【發明內容】

本揭露實施的範例可提供一種資料傳送的混合式編

解碼裝置與方法。

在一實施範例中，所揭露者是關於一種資料傳送的混合式編解碼裝置。此裝置包含: 一編碼器，將一來源檔案(source file)切割成N個子區段並在第一有限場編碼產生N筆主要編碼資料(encoded data)，且將此N個子區段在第二有限場編碼產生k筆額外編碼資料(additional encoded data)。然後，編碼器輸出一組編碼係數資料及$N+k$筆編碼資料，其中N與k皆為非負整數; 以及一解碼器，合併此組編碼係數資料及此$N+k$筆編碼資料後，將其中N筆主要編碼資料在第一有限場進行解碼，若N個子區段無法被順利解碼時，利用剩餘k筆額外編碼資料來輔助資料的解碼，並在此第二有限場進行解碼。依此，解碼器可將來源檔案還原。

在另一實施範例中，所揭露者是關於一種資料廣播的混合式編解碼方法。此方法包含: 將一來源檔案切割成N個子區段，分別以兩種編碼方式來編碼此N個子區段，並分別產生N筆主要編碼資料及k筆額外編碼資料; 將一組編碼係數資料及此$N+k$筆編碼資料傳送至解碼器; 並由此解碼器以一相對應的解碼方式來解碼此N筆主要編碼資料; 以及當此解碼器無法解碼出此N個子區段時，補上此k筆額外編碼資料，並以另一相對應的解碼方式來輔助資料的解碼，依此，此解碼器解碼出一已還原的來源檔案。其中此兩種編碼方式是採用兩種不同

空間大小的有限場來進行資料編碼。

茲配合下列圖示、實施範例之詳細說明及申請專利範圍，將上述及本揭露之其他目的與優點詳述於後。

【實施方式】

本揭露實施的範例在資料廣播的傳送與接收兩方間進行混合式編解碼傳輸。於資料傳輸機制中，在編碼時使用不同空間大小的有限場來產生編碼資料。若來源檔案被切割成N個子區段，則編碼器先以空間較小的有限場產生N筆主要編碼資料並傳送至解碼器，再附以k筆空間較大的有限場額外編碼資料。如此，編碼器能夠有效率的先從N筆主要編碼資料中透過矩陣運算去除線性相依者，再合併k筆額外編碼資料來將來源檔案還原。

第四圖是資料廣播的混合式編解碼裝置的一範例示意圖，與所揭露的某些實施範例一致。參考第四圖，混合式編解碼裝置 400 包含一編碼器 410 以及一解碼器 420。編碼器 410 可包括一主要編碼元件 412 以及一額外編碼元件 414。解碼器 420 可包括一主要解碼元件 422 以及一額外解碼元件 424。

編碼器 410 先將來源檔案 401 切割成N個子區段後，可藉由主要編碼元件 412 將此N個子區段在一第一有限場進行編碼，並產生 N 筆主要編碼資料 412a;再以

額外編碼元件414將此N個子區段在一第二有限場進行編碼，並產生k筆額外編碼資料414a;然後，編碼器410將一組編碼係數資料416及$N+k$筆編碼資料418，輸出至解碼器420，N與k皆為非負整數。

解碼器420先合併此組編碼係數資料416及$N+k$筆編碼資料，例如先將此組編碼係數資料安排成一矩陣後，與該$N+k$筆編碼資料合併成一增廣矩陣(augmented matrix)，然後藉由主要解碼元件422利用一種矩陣化簡(matrix reduce)法，例如利用高斯消去法(Gaussian Elimination)來化簡該增廣矩陣，將N筆主要編碼資料412a先在第一有限場進行解碼;當主要解碼元件422無法解碼出此N個子區段時，再藉由額外解碼元件424利用k筆額外編碼資料414a，來輔助資料的解碼，並在第二有限場進行解碼;依此，解碼器420解碼出一已還原的來源檔案402。

承上述，在本揭露實施的範例中，於資料傳輸機制中，可混合不同空間大小的有限場來產生編碼資料，而該組編碼係數資料416是由兩部份的係數資料所組成，其中一部份的係數資料屬於第一有限場，另一部份的係數資料屬於第二有限場。也就是說，第一有限場與第二有限場可以是不同空間大小的有限場。例如，第一有限場可採用空間較小的有限場，例如$GF(2)$;而第二有限場可採用空間較大的有限場，例如$GF(2^8)$。如此，可混合

BNC 及 LNC 編碼方式來進行編解碼。傳送端在傳輸資料時，可先使用 BNC 進行編碼傳輸，再補上數筆 RLNC 編碼資料。接收端在解碼時，則先使用 BNC 方式對主要編碼資料進行解碼，若無法正確解碼出來源檔案的資料，則採用 RLNC 進行輔助運算。

以下使用兩個工作範例來說明混合 BNC 及 RLNC 編碼方式來進行編解碼。其中，此兩工作範例使用不同的編碼係數矩陣，並且以 N 等於 8 為例，也就是說來源檔案被切割成 8 個子區段，以 D_0~D_7 表示，如第五圖的範例所示。

在第一工作範例中，編碼過程說明如下。來源檔案被切割成 8 等份後，在 $GF(2)$ 空間中進行編碼，產生 $N=8$ 筆主要編碼資料，以 E_0~E_7 表示，再以 $GF(2^8)$ 空間中產生 $k=2$ 筆額外編碼資料，以 E_8~E_9 表示，並將用於編碼的編碼係數矩陣及編碼資料 E_0~E_9 一併傳送至解碼器。此編碼過程可用第六圖的矩陣關係來表示。在第六圖中，若將編碼係數矩陣分成係數矩陣 A1 與係數矩陣 A2 共兩部份、D_0~D_7 以矩陣 D 表示、E_0~E_7 以矩陣 E1 表示、以及 E_0~E_9 以矩陣 E2 表示，則這些矩陣有如下的關係:E1 = A1×D，而 E2 = A2×D。並且，可以看出係數矩陣 A1 裡的元素屬於 $GF(2)$ 空間，其值可為 0 或 1，而係數矩陣 A2 裡的元素屬於 $GF(2^8)$ 空間，其值可為 0~255 之任意整數。

上述編碼係數矩陣及編碼資料 E_0~E_9 一併傳送至解碼器後，解碼過程說明如下。解碼器將編碼係數矩陣及編碼資料合併成一增廣矩陣，此增廣矩陣如第七 A 圖所示;先在*GF*(2) 空間中，採用 BNC 方式來進行解碼，利用高斯消去法將此大小為 8×9 的增廣矩陣化簡，已化簡的矩陣如第七 B 圖所示。從第七 B 圖可以得知，在*GF*(2) 空間中，已化簡的矩陣有一階數(Rank)為 8，亦即等於 *N*。換句話說，在*GF*(2) 空間中，利用基本列運算化簡線性方程組的增廣矩陣，找出 8 筆彼此線性獨立的編碼資料，可求得一組解且恰有一組解。因此，在第一工作範例中，無須使用到額外編碼資料就能夠將資料子區段 D_0~D_7 還原，並重組成來源檔案。

在第二工作範例中，其編碼步驟與第一工作範例相同，但編碼係數矩陣中，原係數矩陣 A1 的元素有所改變，從第八圖之編碼過程中係數矩陣 810 可以看出。類似地，第八圖之編碼係數矩陣及編碼資料 E_0~E_9 一併傳送至解碼器後，解碼器將此編碼係數矩陣及編碼資料合併成一增廣矩陣，此增廣矩陣如第九 A 圖所示; 類似地，先在*GF*(2) 空間中，採用 BNC 方式來進行解碼，並利用高斯消去法將此大小為8×9的增廣矩陣化簡，第九 B 圖是已化簡的矩陣。從第九 B 圖可以發現，已化簡的矩陣有兩筆線性相依的編碼資料 920，也就是說，在*GF*(2) 空間中，此已化簡的矩陣中沒有 8 筆彼此線性獨立的編碼資料。此時可利用另外在$GF(2^8)$ 空間中的兩筆

額外編碼資料，即 E_8~E_9，來輔助資料的解碼。

因此，對於第九 B 圖之已化簡的矩陣，除了可利用 $GF(2^8)$ 空間中的兩筆額外編碼資料 E_8~E_9，並且在 $GF(2^8)$ 空間中採用 RLNC 方式來進行解碼，以高斯消去法將此大小為10×9的增廣矩陣化簡成矩陣 1000，並且找出 8 筆彼此線性獨立的編碼資料，如第十圖的範例所示。此時，已化簡之編碼係數矩陣的階數為 8，因此，在第二工作範例中，當在 $GF(2)$ 空間中進行解碼，無法解碼出此 8 個子區段時，則可使用 $GF(2^8)$ 空間中的兩筆額外編碼資料，來將資料子區段 D_0~D_7 還原，並重組成來源檔案。

從第二工作範例中，可知本揭露之實施範例的編碼器先以空間較小的有限場產生 N 筆主要編碼資料並傳送至解碼器，再附以空間較大的有限場額外編碼資料 k 筆。如此，編碼器能夠有效率地先從 N 筆主要編碼資料中透過矩陣運算去除相依者，再合併 k 筆額外編碼資料來還原來源檔案。

承上述，在本揭露實施的範例中，資料廣播的混合式編解碼方法可如第十一圖的範例流程所載述。在第十一圖的範例流程中，先將來源檔案 401 切割成 N 個子區段，分別以兩種編碼方式來編碼此 N 個子區段，並分別產生 N 筆主要編碼資料及 k 筆額外編碼資料，如步驟

1110 所示。然後，將一組編碼係數資料及此$N+k$筆編碼資料傳送至一解碼器，如步驟 1120 所示。並由此解碼器以一相對應的解碼方式來解碼此N筆主要編碼資料，如步驟 1130 所示。當此解碼器無法解碼出此N個子區段時，補上此k筆額外編碼資料，並以另一相對應的解碼方式來輔助資料的解碼，如步驟 1140 所示。依此，此解碼器解碼出已還原的來源檔案 402。其中此兩種編碼方式是採用兩種不同空間大小的有限場來進行資料編碼。

在步驟 1110 中，兩種編碼方式是分別在第一及第二有限場中進行資料編碼。此兩種編碼方式例如可以是 BNC 及 RLNC，或是線性網路編碼(linear network coding)等。在資料傳輸機制中，混合空間較小的有限場中 BNC 編碼方式及空間較大的有限場中 RLNC，可使得透過較少的運算量及資料傳輸量即可達到相同的效果。在步驟 1120 中，解碼器可在空間較小的有限場中，先採用 BNC 相對應的解碼方式解碼此N筆主要編碼資料，先從N筆主要編碼資料中透過矩陣運算去除相依者，例如利用前述的高斯消去法將增廣矩陣化簡。在步驟 1130 中，當此解碼器無法解碼出此N個子區段時，再附以空間較大的有限場額外編碼資料k筆，以 RLNC 相對應的解碼方式來輔助資料的解碼。

在本揭露實施的範例中，還可提供 BNC 混合 RLNC

之最佳k值的數量表。以採用有限場$GF(2^n)$為例，第十二圖是一範例圖表，說明在不同n值時，增加傳輸額外編碼資料筆數k與可達到之成功解碼機率，與所揭露的某些實施範例一致。第十二圖的範例圖表中，$GF(2^n)$是以RLNC方式來增加傳輸k筆額外編碼資料時所使用的有限場。

例如，當使用的有限場是$GF(2^4)$時，若可達到之成功解碼機率是$1-10^{-6}$的話，則需要增加傳輸 6 筆$(k=6)$額外編碼資料。以上述第二工作範例來說，所使用的有限場是$GF(2^8)$並且增加兩筆$(k=2)$額外編碼資料，則可達到之成功解碼機率是$1-10^{-2}$。從第十二圖的範例圖表還可以看出，當$n\geq 3$時，也就是說，所使用的有限場的空間大小是大於等於$GF(2^8)$的空間大小時，並且當增加k筆額外編碼資料，k=2、3、4、5 時，則可達到之成功解碼機率分別都是$1-10^{-2}$或$1-10^{-4}$或$1-10^{-6}$或$1-10^{-8}$。若要達到之成功解碼機率是$1-10^{-10}$的話，則可使用有限場$GF(2^2)$及額外編碼資料 17 筆、或是有限場$GF(2^4)$及額外編碼資料 9 筆、或是有限場$GF(2^8)$及額外編碼資料 6 筆、或是有限場$GF(2^{16})$及額外編碼資料 5 筆。因此，參考第十二圖的範例圖表，還可使得透過較少的運算量及資料傳輸量即可達到相同的效果。

第十二圖之範例圖表中k值的數量可從下列兩關係式而得到支持，說明如下。令$f(m,n,r,t)$是在$GF(t)$中，一個$m\times n$的亂數矩陣(random matrix)其階數為r之事件

發生的機率，其中 m 與 n 皆大於 1 且 $r \le \min(m,n)$。則下列關係式成立:

$f(m,n,r,t)=\frac{1}{t^{mxn}}$，若 $r=0$;

$= (1-\frac{1}{t^{n-r+1}})(1-\frac{1}{t^{n-r+2}})...(1-\frac{1}{t^{n}})$，若 $m=r\ge 1$;

$=(1-\frac{1}{t^{n-r}})f(m-1,n,r,t)+(1-\frac{1}{t^{n-r+1}})f(m-1,n,r-1,t)$,若 $m>r\ge 1$。

另一關係式說明如下。令 S 為 $GF(t)^n$ 中的 $n-r$ 維的一個子空間(subspace)，A 是一個 $m\times n$ 的亂數矩陣，其中 $m\ge r$。令 $g(m,n,r,t)$ 是 S 及 A 的列空間(row space)能夠展開 $GF(t)^n$ 之事件發生的機率，則下列關係式成立:

$g(m,n,r,t)=1$，若 $r=0$;

$= (1-\frac{1}{t^{1}})(1-\frac{1}{t^{2}})...(1-\frac{1}{t^{r}})$，若 $m=r\ge 1$;

$=(1-\frac{1}{t^{r}})g(m-1,n,r,t)+(1-\frac{1}{t^{r}})g(m-1,n,r-1,t)$，若 $m>r\ge 1$。

綜上所述，本揭露實施的範例在資料傳輸機制中混合兩種編碼方式，此兩種編碼方式採用兩種不同空間大小的有限場來進行資料編碼。在資料傳輸時，先採用空間較小的有限場進行一種編碼傳輸，再採用空間較大的有限場並補上數筆額外編碼資料來進行另一種編碼傳輸。在解碼時，先採用該空間較小的有限場來進行解碼，若無法正確解碼出，則採用該空間較大的有限場來輔助資料的解碼。使得透過較少的運算量及資料傳輸量

即可達到相同的效果。

以上所述者僅為本揭露實施之範例，當不能依此限定本揭露實施之範圍。即大凡本揭露申請專利範圍所作之均等變化與修飾，皆應仍屬本發明專利涵蓋之範圍。

【圖式簡單說明】

第一圖是LT碼之編碼的一個範例示意圖。

第二圖是Raptor碼之編碼的一個範例示意圖。

第三圖是將網路編碼技術應用在分散式網路的一個範例示意圖。

第四圖是資料廣播的混合式編解碼裝置的一範例示意圖，與所揭露的某些實施範例一致。

第五圖是將來源檔案切割成數個子區段的一範例示意圖，與所揭露的某些實施範例一致。

第六圖是第一工作範例之編碼過程的一範例示意圖，與所揭露的某些實施範例一致。

第七A圖是第一工作範例之解碼過程中的增廣矩陣的一範例示意圖，與所揭露的某些實施範例一致。

第七B圖是第七A圖之增廣矩陣化簡後的一範例示意圖，與所揭露的某些實施範例一致。

第八圖是第二工作範例之編碼過程的一範例示意圖，與所揭露的某些實施範例一致。

第九A圖是第二工作範例之解碼過程中的增廣矩陣的一範例示意圖，與所揭露的某些實施範例一致。

第九B圖是第九A圖之增廣矩陣化簡後的一範例示意圖，與所揭露的某些實施範例一致。

第十圖是對於第九B圖之化簡後的矩陣，再利用$GF(2^8)$空間中的兩筆額外編碼資料來化簡矩陣的一範例示意圖，與所揭露的某些實施範例一致。

第十一圖是一資料廣播的混合式編解碼方法的一範例流

程圖，與所揭露的某些實施範例一致。

第十二圖是一範例圖表，以有限場$GF(2^n)$為例，說明在不同的n值下，增加傳輸額外編碼資料筆數k與可達到之成功解碼機率，與所揭露的某些實施範例一致。

【主要元件符號說明】

110 原始符元

120 LT 編碼後的符元

210 原始符元

220 先編碼符元

230 Raptor 編碼後的符元

R1~R4 網路節點

C1~C8 其他節點

400 混合式編解碼裝置

401 來源檔案

410 編碼器

412 主要編碼元件

412a 主要編碼資料

414 額外編碼元件

414a 額外編碼資料

416 一組編碼係數資料

418 編碼資料

420 解碼器

422 主要解碼元件

424 額外解碼元件

402 已還原的來源檔案

D_0~D_7 8 個子區段

E_0~E_7 8 筆主要編碼資料

E_8~E_9 2 筆額外編碼資料

A1、A2 係數矩陣

810 係數矩陣

920 兩筆線性相依的編碼資料

1000 矩陣

1110 將來源檔案切割成N個子區段，分別以兩種編碼方式來編碼此N個子區段，並分別產生N筆主要編碼資料及k筆額外編碼資料

1120 將一組編碼係數資料及此$N+k$筆編碼資料傳送至一解碼器

1130 由此解碼器以一相對應的解碼方式來解碼此N筆主要編碼資料

1140 補上此k筆額外編碼資料，並以另一相對應的解碼方式來輔助資料的解碼

103年4月14日 修正頁

七、申請專利範圍：

1. 一種資料傳送的混合式編解碼裝置，該裝置包含:

一編碼器，將一來源檔案切割成N個子區段並在一第一有限場進行編碼後，產生N筆主要編碼資料，且將該N個子區段在一第二有限場進行編碼，並產生k筆額外編碼資料，然後，該編碼器輸出一組編碼係數資料及該$N+k$筆編碼資料，N與k皆為非負整數;以及

一解碼器，合併該組編碼係數資料及該$N+k$筆編碼資料後，將該N筆主要編碼資料在該第一有限場進行解碼，當無法解碼出該N個子區段時，利用該k筆額外編碼資料來輔助資料的解碼，並在該第二有限場進行解碼，依此，該解碼器解碼出一已還原的來源檔案。

2. 如申請專利範圍第 1 項所述之混合式編解碼裝置，其中該編碼器還包括:

一主要編碼元件，將該N個子區段在該第一有限場進行編碼，並產生該N筆主要編碼資料;以及

一額外編碼元件，將該N個子區段在該第二有限場進行編碼，並產生該k筆額外編碼資料。

3. 如申請專利範圍第 1 項所述之混合式編解碼裝置，其中該解碼器還包括:

一主要解碼元件，將該N筆主要編碼資料在該第一有限場進行解碼;以及

一額外解碼元件，利用該k筆額外編碼資料來輔助資料的解碼，並在該第二有限場進行解碼。

4. 如申請專利範圍第 1 項所述之混合式編解碼裝置，其中

該第一有限場與該第二有限場是不同空間大小的有限場。

5. 如申請專利範圍第 1 項所述之混合式編解碼裝置，其中該第一有限場的空間大小比該第二有限場的空間大小還要小。

6. 如申請專利範圍第 1 項所述之混合式編解碼裝置，其中在該第一有限場係使用二位元網路編碼來進行編解碼。

7. 如申請專利範圍第 1 項所述之 1 項所述之混合式編解碼裝置，其中在該第二有限場係使用亂數線性網路編碼來進行編解碼。

8. 如申請專利範圍第 1 項所述之混合式編解碼裝置，其中該組編碼係數資料是由兩部份的係數資料所組成，其中一部份的係數資料屬於該第一有限場，另一部份的係數資料屬於該第二有限場。

9. 如申請專利範圍第 1 項所述之混合式編解碼裝置，該裝置還提供採用二位元網路編碼混合亂數線性網路編碼的一最佳 k 值的數量表。

10. 一種資料廣播的混合式編解碼方法，實現在一編解碼裝置上，該方法包括:

將一來源檔案切割成 N 個子區段，分別以兩種編碼方式來編碼該 N 個子區段，並分別產生 N 筆主要編碼資料及 k 筆額外編碼資料，N 與 k 皆為非負整數;

傳送一組編碼係數資料及該 $N+k$ 筆編碼資料至一解碼器，並由該解碼器以一相對應的解碼方式來解碼該 N 筆主要編碼資料;以及

當該解碼器無法解碼出該N個子區段時，補上該k筆額外編碼資料，以另一相對應的解碼方式來輔助資料的解碼，依此，解碼出一已還原的來源檔案;

其中該兩種編碼方式是採用兩種不同空間大小的有限場來進行資料編碼。

11. 如申請專利範圍第 10 項所述之混合式編解碼方法，其中該兩種編碼方式分別為二位元網路編碼及亂數線性網路編碼。

12. 如申請專利範圍第 11 項所述之混合式編解碼方法，其中該解碼器以該二位元網路編碼相對應的解碼方式來解碼該N筆主要編碼資料。

13. 如申請專利範圍第 12 項所述之混合式編解碼方法，其中當該解碼器無法解碼出該N個子區段時，該解碼器以該亂數線性網路編碼相對應的解碼方式來進行解碼資料。

14. 如申請專利範圍第 11 項所述混合式編解碼方法，其中該二位元網路編碼所採用的有限場的空間大小比該亂數線性網路編碼採用的有限場的空間還要小。

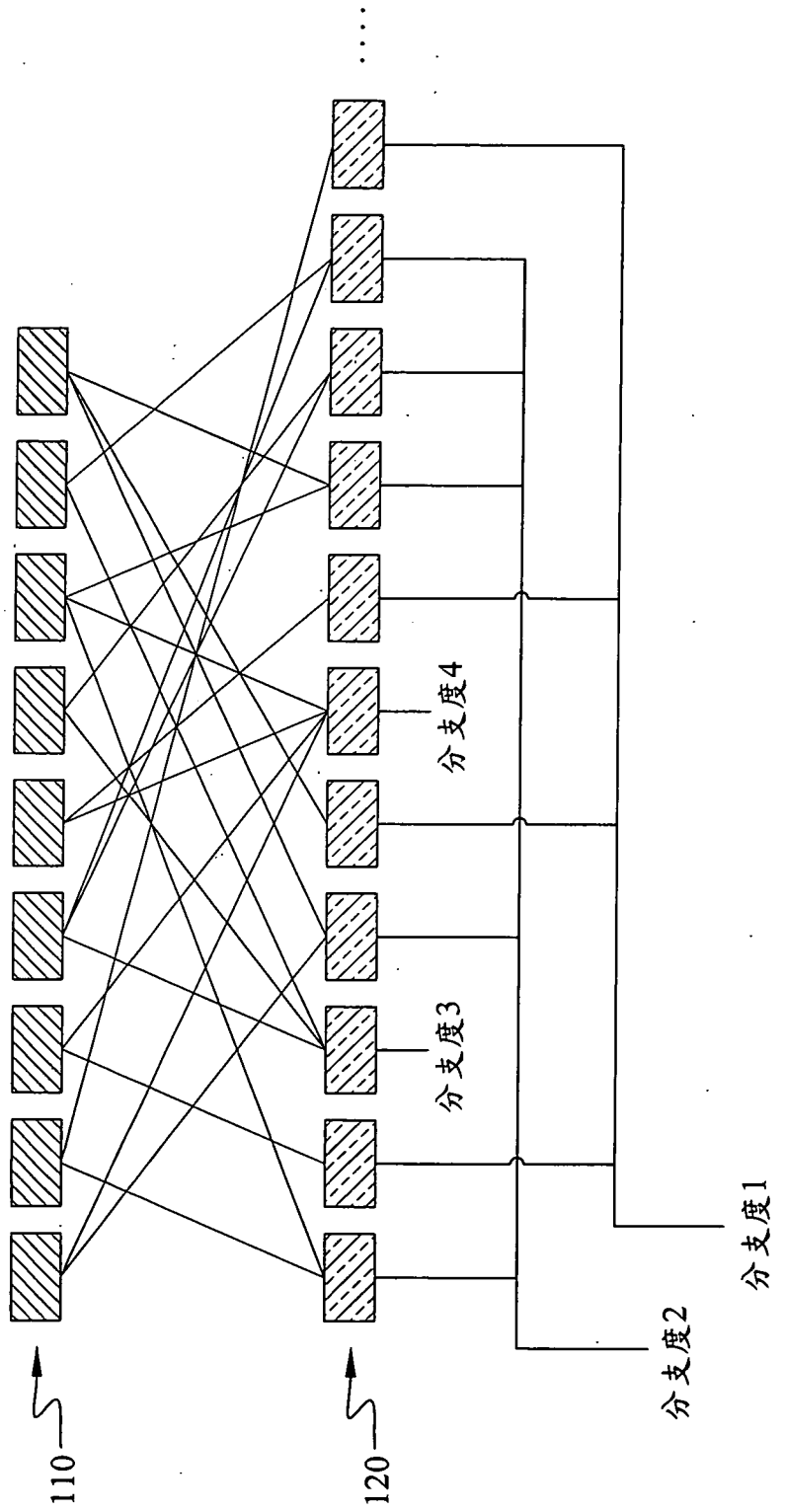
15. 如申請專利範圍第 14 項所述混合式編解碼方法，其中該亂數線性網路編碼採用的有限場為一加邏瓦場$GF(2^n)$，$n \geq 2$。

16. 如申請專利範圍第 15 項所述混合式編解碼方法，該方法還提供採用二位元網路編碼混合亂數線性網路編碼的一最佳k值的數量表。

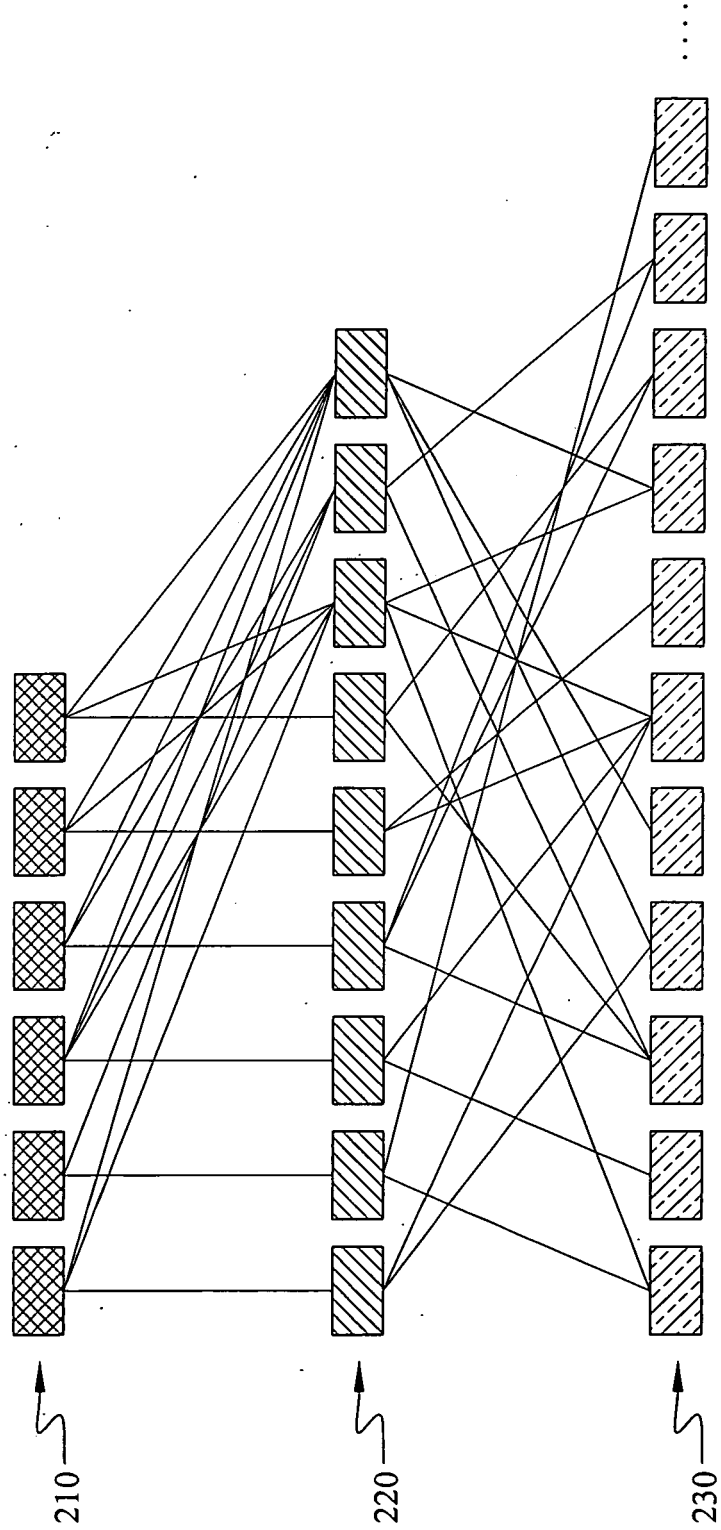
17. 如申請專利範圍第 16 項所述混合式編解碼方法，其中

當$n \geq 8$時，並且當增加k筆額外編碼資料，$k=2$、3、4、5時，則可達到之成功解碼機率分別都是$1-10^{-2}$或$1-10^{-4}$或$1-10^{-6}$或$1-10^{-8}$。

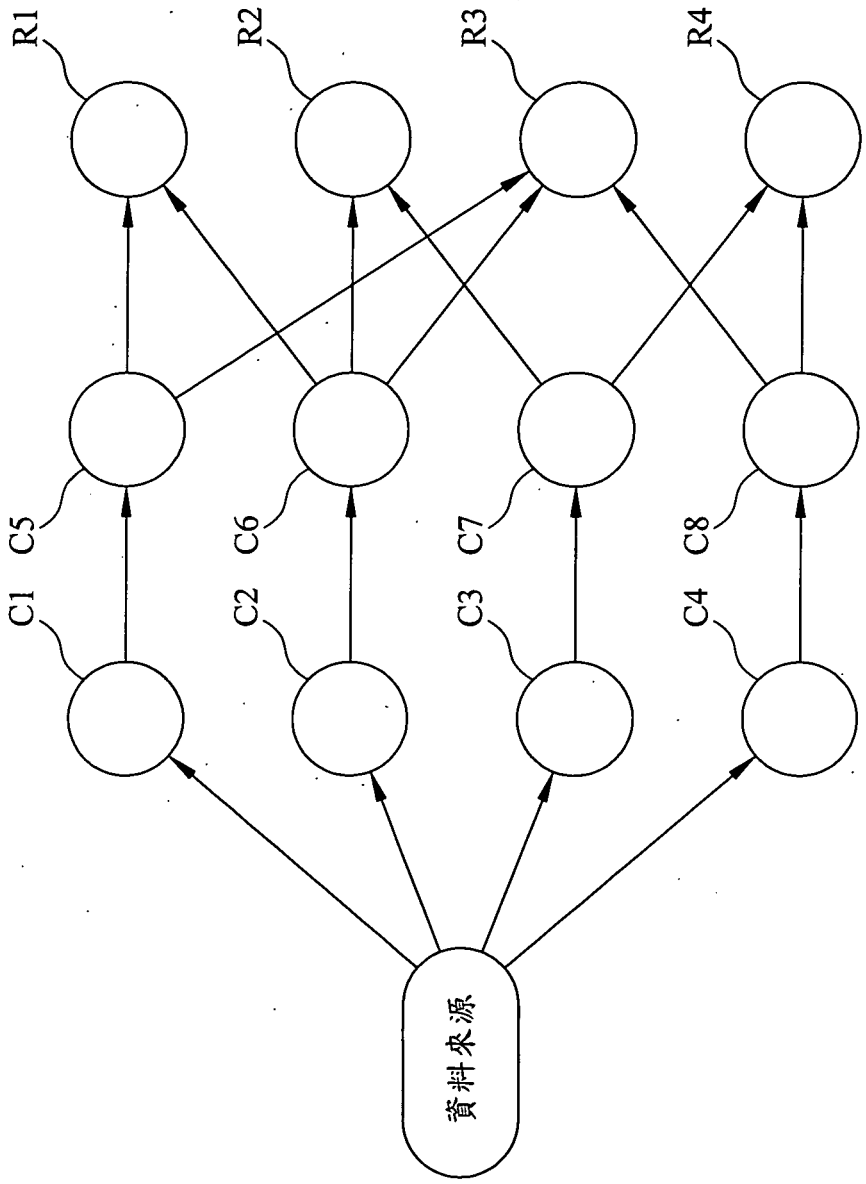
八、圖式



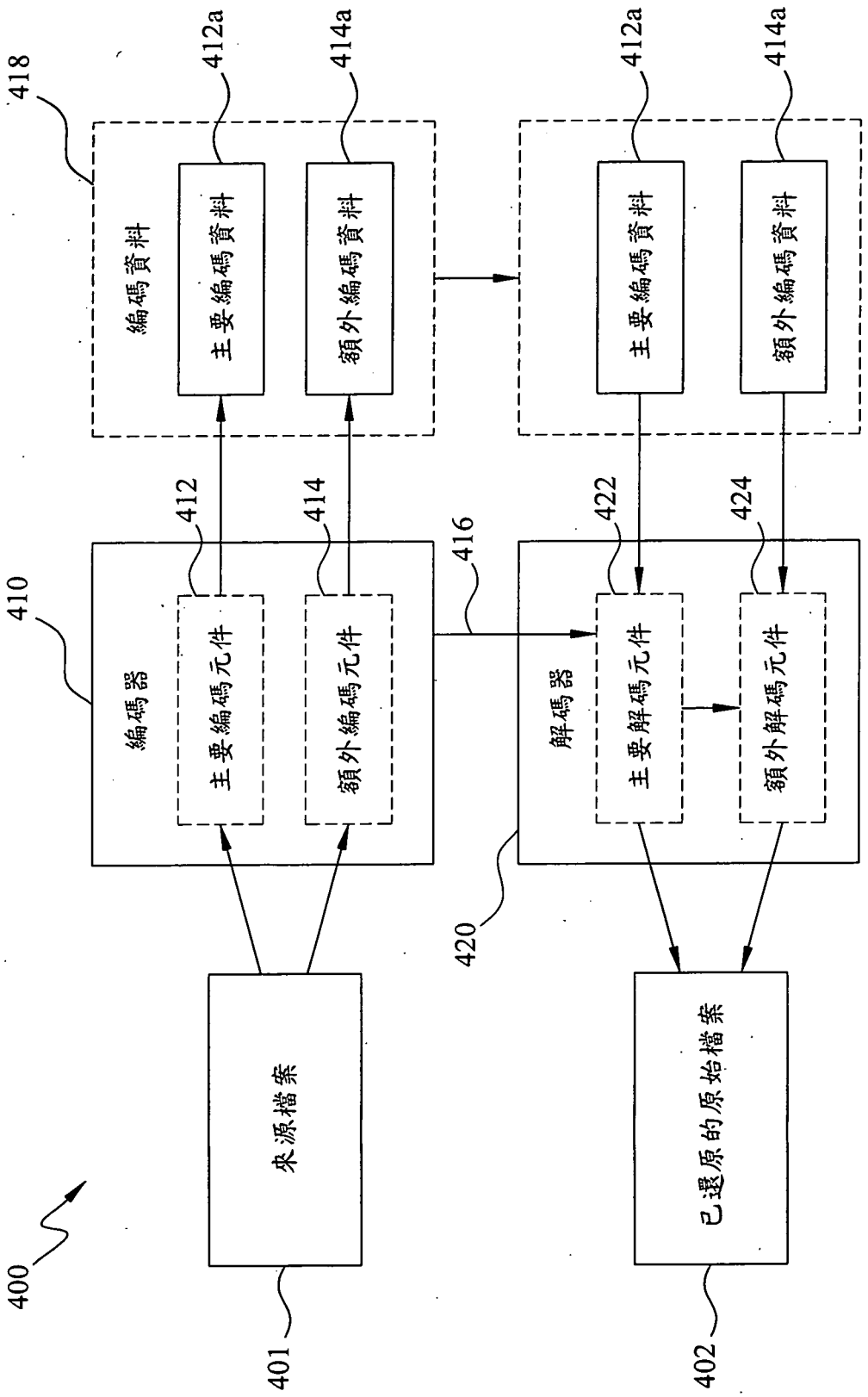
第一圖



第二圖



第三圖


400
401
402
410
412
414
416
418
420
422
424
412a
414a
412a
414a
來源檔案
已還原的原始檔案
編碼器
主要編碼元件
額外編碼元件
解碼器
主要解碼元件
額外解碼元件
編碼資料
主要編碼資料
額外編碼資料
主要編碼資料
額外編碼資料

第四圖

D_0	D_1	D_2	D_3	D_4	D_5	D_6	D_7

第五圖

A1

1	0	1	1	0	1	1	0
1	1	0	1	1	1	0	1
0	1	1	0	1	0	1	0
1	0	1	0	1	0	0	1
0	0	0	1	0	1	1	0
0	1	1	0	1	0	1	1
1	0	1	0	1	0	1	1
1	1	0	0	0	1	0	0

A2

5	48	124	19	250	116	94	37
91	55	18	210	165	47	47	15

$\times$

$$\begin{bmatrix} D_0 \\ D_1 \\ D_2 \\ D_3 \\ D_4 \\ D_5 \\ D_6 \\ D_7 \end{bmatrix} = \begin{bmatrix} E_0 \\ E_1 \\ E_2 \\ E_3 \\ E_4 \\ E_5 \\ E_6 \\ E_7 \\ E_8 \\ E_9 \end{bmatrix}$$

第六圖

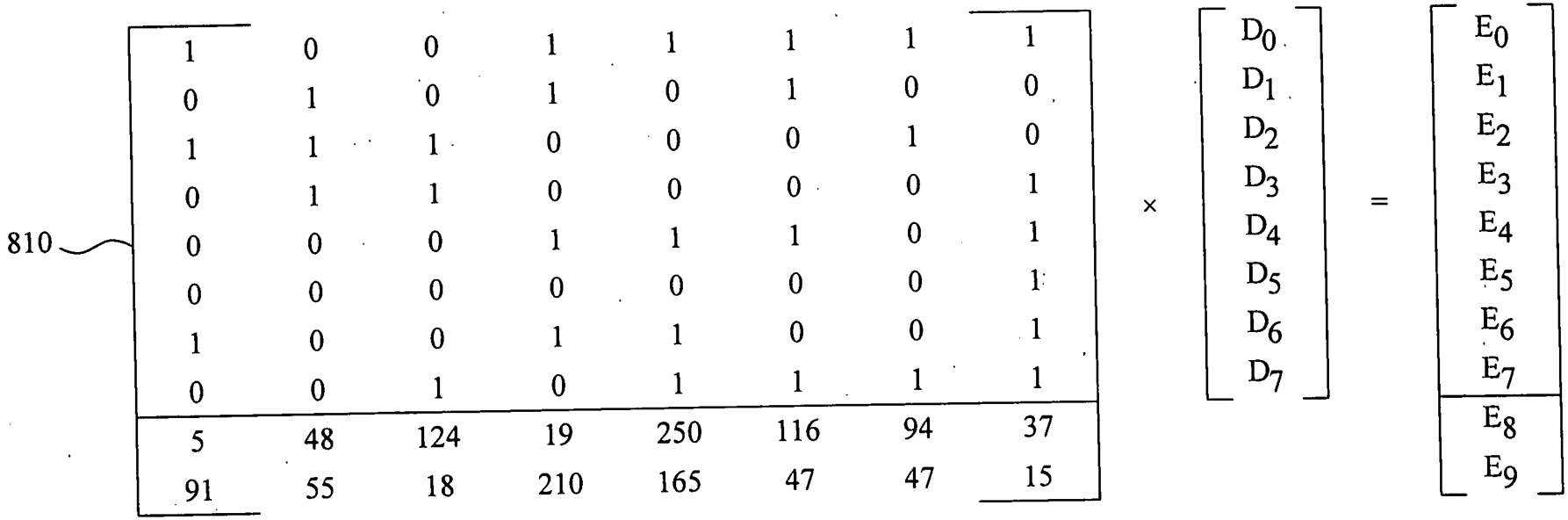
107年4月14日修正替換頁

1	0	1	1	0	1	1	0	E_0
1	1	0	1	1	1	0	1	E_1
0	1	1	0	1	0	1	0	E_2
1	0	1	0	1	0	0	1	E_3
0	0	0	1	0	1	1	0	E_4
0	1	1	0	1	0	1	1	E_5
1	0	1	0	1	0	1	1	E_6
1	1	0	0	0	1	0	0	E_7
5	48	124	19	250	116	94	37	E_8
91	55	18	210	165	47	47	15	E_9

第七A圖

1	0	0	0	0	0	0	0	D_0
0	1	0	0	0	0	0	0	D_1
0	0	1	0	0	0	0	0	D_2
0	0	0	1	0	0	0	0	D_3
0	0	0	0	1	0	0	0	D_4
0	0	0	0	0	1	0	0	D_5
0	0	0	0	0	0	1	0	D_6
0	0	0	0	0	0	0	1	D_7
5	48	124	19	250	116	94	37	E_8
91	55	18	210	165	47	47	15	E_9

第七B圖


810
1 0 0 1 1 1 1 1
0 1 0 1 0 1 0 0
1 1 1 0 0 0 1 0
0 1 1 0 0 0 0 1
0 0 0 1 1 1 0 1
0 0 0 0 0 0 0 1
1 0 0 1 1 0 0 1
0 0 1 0 1 1 1 1
5 48 124 19 250 116 94 37
91 55 18 210 165 47 47 15
×
D0 D1 D2 D3 D4 D5 D6 D7
=
E0 E1 E2 E3 E4 E5 E6 E7
E8 E9

第八圖

1	0	0	1	1	1	1	1	E_0
0	1	0	1	0	1	0	0	E_1
1	1	1	0	0	0	1	0	E_2
0	1	1	0	0	0	0	1	E_3
0	0	0	1	1	1	0	1	E_4
0	0	0	0	0	0	0	1	E_5
1	0	0	1	1	0	0	1	E_6
0	0	1	0	1	1	1	1	E_7
5	48	124	19	250	116	94	37	E_8
91	55	18	210	165	47	47	15	E_9

第九A圖

900

1	0	0	1	1	0	0	0	$D_1+D_4+D_5$
0	1	0	0	1	0	0	0	D_2+D_5
1	0	1	0	1	0	0	0	D_3+D_5
0	0	0	1	1	0	1	0	$D_4+D_5+D_7$
0	0	0	0	0	1	1	0	D_6+D_7
0	0	0	0	0	0	0	1	D_7
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
5	48	124	19	250	116	94	37	E_8
91	55	18	210	165	47	47	15	E_9

920

第九B圖

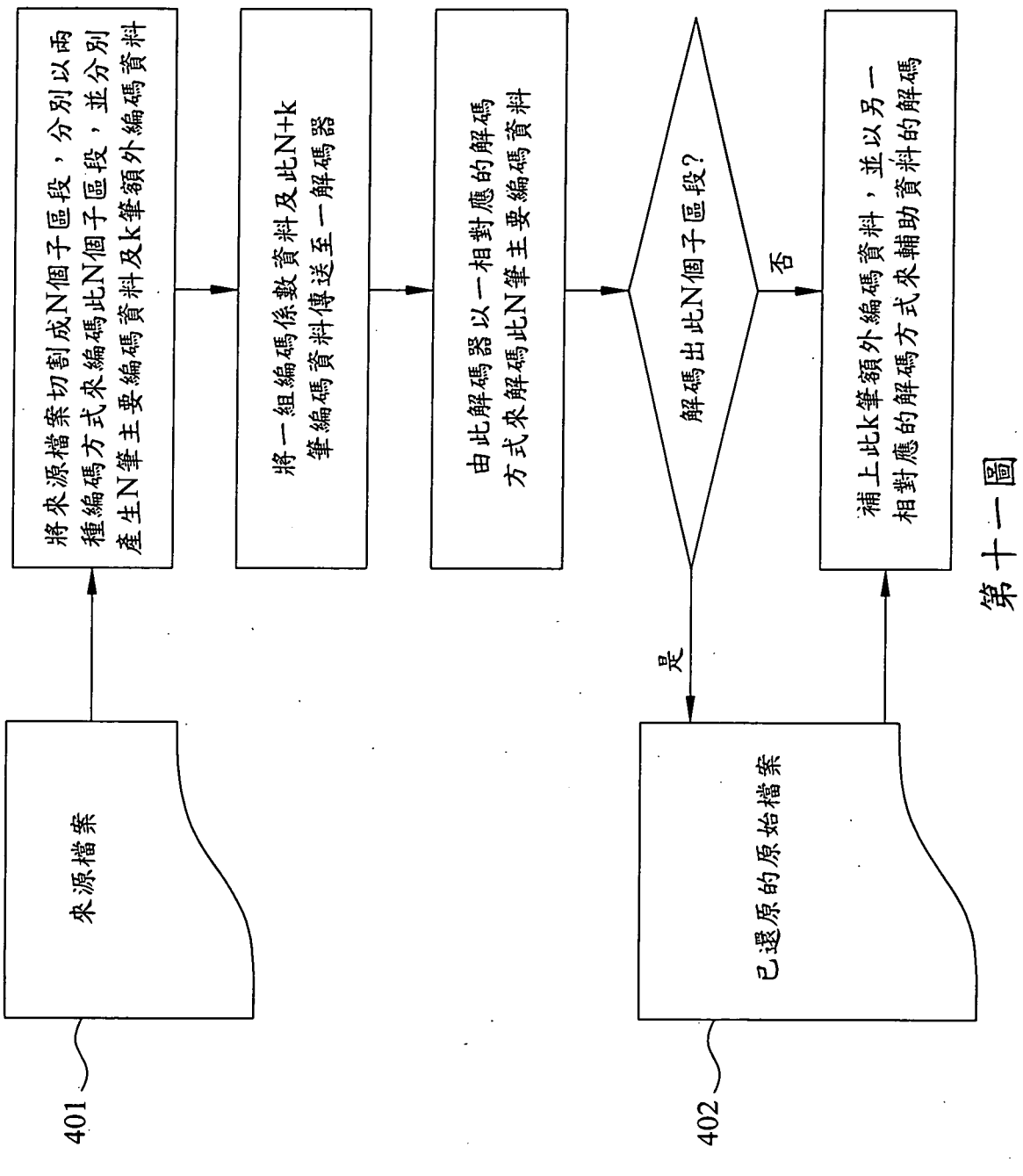
900

1	0	0	1	1	0	0	0	$D_1+D_4+D_5$
0	1	0	0	1	0	0	0	D_2+D_5
1	0	1	0	1	0	0	0	D_3+D_5
0	0	0	1	1	0	1	0	$D_4+D_5+D_7$
0	0	0	0	0	1	1	0	D_6+D_7
0	0	0	0	0	0	0	1	D_7
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
5	48	124	19	250	116	94	37	E_8
91	55	18	210	165	47	47	15	E_9

1000

1	0	0	0	0	0	0	0	D_0
0	1	0	0	0	0	0	0	D_1
0	0	1	0	0	0	0	0	D_2
0	0	0	1	0	0	0	0	D_3
0	0	0	0	1	0	0	0	D_4
0	0	0	0	0	1	0	0	D_5
0	0	0	0	0	0	1	0	D_6
0	0	0	0	0	0	0	1	D_7
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

第十圖


來源檔案
401
將來源檔案切割成N個子區段，分別以兩種編碼方式來編碼此N個子區段，並分別產生N筆主要編碼資料及k筆額外編碼資料
將一組編碼係數資料及此N+k筆編碼資料傳送至一解碼器
由此解碼器以一相對應的解碼方式來解碼此N筆主要編碼資料
解碼出此N個子區段?
是
否
已還原的原始檔案
402
補上此k筆額外編碼資料，並以另一相對應的解碼方式來輔助資料的解碼

第十一圖

成功解碼機率 / $GF(2^n)$	$1-10^{-2}$	$1-10^{-4}$	$1-10^{-6}$	$1-10^{-8}$	$1-10^{-10}$
GF(2)	7	15	20	27	-
$GF(2^2)$	4	7	11	14	17
$GF(2^4)$	3	4	6	8	9
$GF(2^8)$	2	3	4	5	6
$GF(2^{16})$	2	3	4	5	5
$GF(2^{32})$	2	3	4	5	5

第十二圖