第三章　研究方法

本章介紹系統、架構演算法的描述、加密演算法及解密演算法。根據過去(Lee and Lee, 2010)研究的作法為基礎，本研究提出的加解密演算法將在下面幾節介紹。

第一節　系統架構

本節介紹本研究的系統架構，如圖 3-1 所示。本研究的目的在於新聞資料在電腦系統中的儲藏安全，截取下來的新聞資料，需要經過加密保護再儲存，以避免惡意第三方的竄改。經過加密可以達成初部保護作用。而藉由本研究可以在解密之前驗證出資料是否遭到竄改，可以避免再發佈之後才造成不必要的損失。

把要儲藏的新聞資料，經過加密保護之後，儲存在電腦之中，而當需要解密發佈之前，可以先透過檢驗系統來確認資料有沒有遭到竄改，如果沒有被竄改才透過解密器解密發佈。

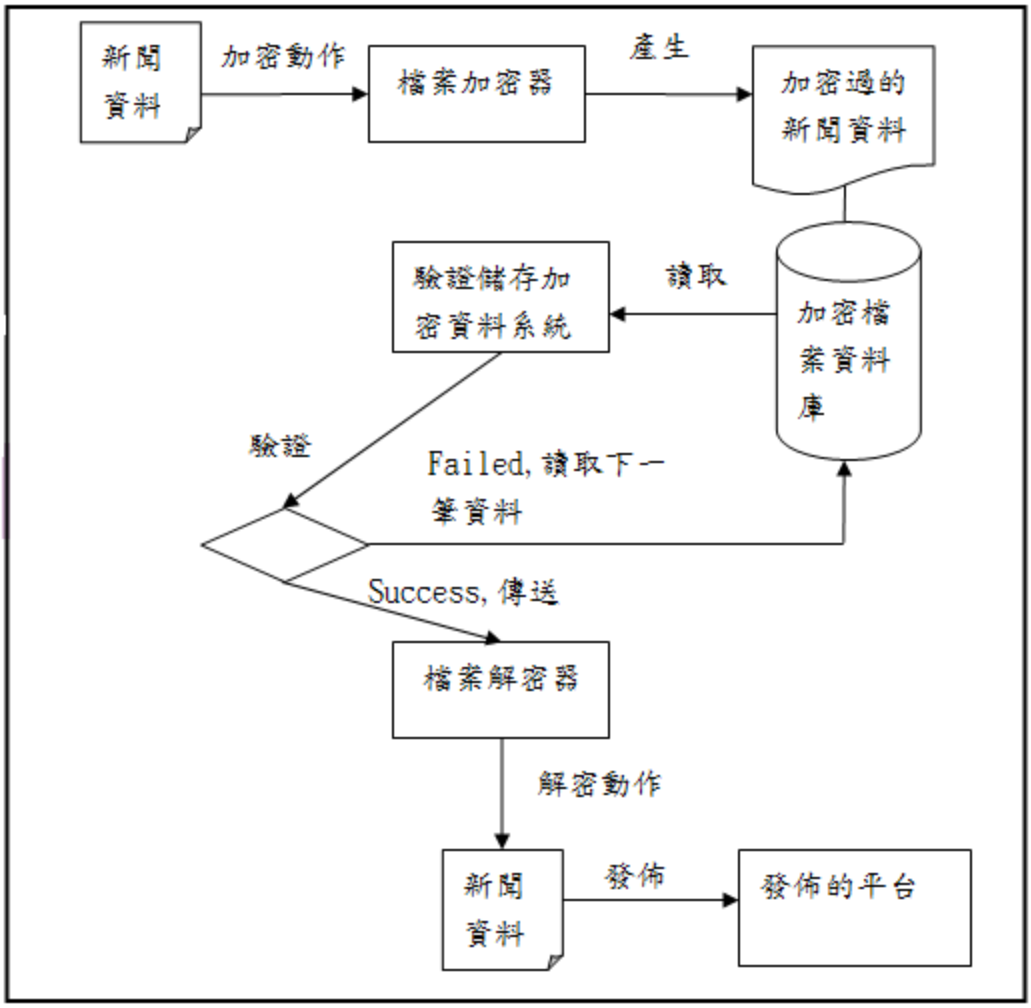

圖 3-1 系統架構

第二節　演算法設計

將明文加密成密文，我們提出的演算法主要使用下列三種方法：

一、確保資料不確定性。

二、明文內容的改變。

三、位置的交換。

這些方法成為我們加密演算法的步驟，加密時我們先將明文

讀入陣列之符號表中，然後經過簡單的電腦基本計算操作，如位移、插入、插入運算元來處理。

一、資料的不確定性：

改變明文，設置旋轉位元組(RB)，將符號表向左或向右旋轉 RB 次數，旋轉之後產生旋轉後符號表。

二、明文內容的改變：

明文內容可能被改變，故建立左移表並左移旋轉後符號表每個位元組，產生轉移後符號表。

三、位置的交換：

經由建立位置表，將轉移後符號表的位置改變，產生密文。

第三節　加密演算法

Lee and Lee (2007)，提出了一個加密演算法介紹如下：

一、獲取新聞資料。

獲得要加密的新聞資料，然後把他存放在符號表。

二、設定加密資料表(EDT)。

把要加密的新聞資料設定加密資料表，如圖 3-2。

加密資料表

格式碼	左移表長度	驗證碼	旋轉量	分割欄位數	偏移量	方向標誌
1byte	1byte	4byte	1byte	1byte	1byte	1byte

圖 3-2　加密資料表

加密資料表的欄位說明如下 ：

(一)格式碼：

格式碼是固定第一位置。根據格式碼的不同，加密的其他鍵值排列順序也跟著改變，如圖 3-3。舉例說明：格式碼 0 為左移表長度，驗證碼，旋轉量，分割欄位數，偏移量，方向標誌。

加密的鍵值排列方式＝左移表長度,驗證碼,旋轉量,分割欄位數，偏移量，方向標誌來輸出。

格式碼由六個項目進行排列組合，操控加密鍵值的輸出順序，有 6 階乘種變化。

格式碼表

格式碼	格式
0	左移表長度，驗證碼，旋轉量，分割欄位數，偏移量，方向標誌
1	左移表長度，驗證碼，旋轉量，分割欄位數，方向標誌，偏移量
2	左移表長度，驗證碼，旋轉量，方向標誌，分割欄位數，偏移量
3	左移表長度，旋轉量，驗證碼，方向標誌，分割欄位數，偏移量
…	…

圖 3-3　格式碼

(二)左移表長度：

左移表長度，另建立左移表。左移表是設定為左移 1~7 個位元。

舉例說明：371 代表左移表長度為 3，第一個字元左移 3 個位元，第二個字元左移 7 個位元，第三個字元左移

第一個字元，循環處理到檔案結尾。

(三)驗證碼：

驗證碼是用來驗證儲存的資料，我們將只有我們知道的驗證碼加插到加密後的檔案中，如圖 3-4。

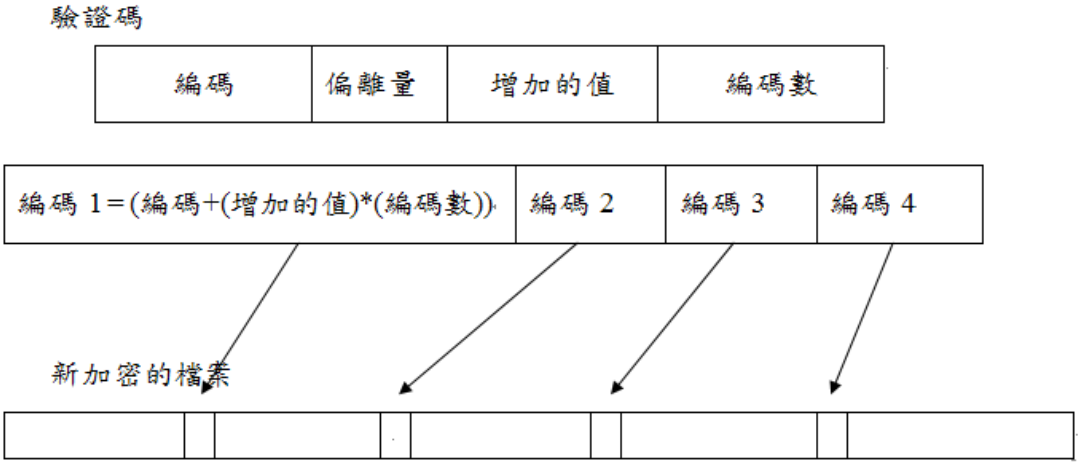

圖 3-4 驗證碼

(四)旋轉量：

設置旋轉位元組(RB)，將區塊向左或向右旋轉 RB 次數。

(五)分割欄位數：

從加密資料表獲得分割欄位數。把明文讀入符號表之後，再按照分割欄位數將符號表分割成區塊。

(六)偏移量：

加密的資料偏移的數量。偏移量 10 就是距離每隔偏移 10 個字元取出。

(七)方向標誌：

資料最後加密完成後輸出的方向，如設定則將資料反轉。

三、我們使用加密資料表的加密演算法的加密步驟如下：

(一)分割欄位：

先將明文讀入符號表中，再按照我們設定的加密資料表的分割欄位數將其分割成區塊，最後區塊不足時加入多餘符號，產生多餘符號表。

(二)旋轉：

取得加密資料表中旋轉量(RB)，將多餘符號表中區塊向左或向右旋轉 RB 次數。

從加密資料表獲得旋轉量。從起始的區塊重複向左或向右旋轉。

從加密資料表獲得旋轉量。從起始的區塊重複向左或向右旋轉。

(三)左移：

取得加密資料表中左移表長度及左移表的值，根據設定的值，把每個位元左移 n 個位元。

從加密資料表獲得左移表長度及獲得左移表。

隨著左移表上的每個位元，順序將旋轉後符號表左移(一個位元值)位元。

最後獲得左移後符號表。

(四)位置交換：

從加密資料表獲得偏移量。

建立位移後符號表。

將左移後符號表，順序每隔偏移量取出，加到位移後符號表後面，一直到左移後符號表結束。

把偏移量減少 1，重複做上一個步驟。

重複做步驟 3、4 直到偏移量等於 0，得到位移後符號表。

(五)輸出方向改變：

從加密資料表獲得方向標誌。如果方向標誌已經設定了，就把位移後符號表反轉，獲得反轉後的符號表。

(六)建立驗證碼表：

從加密資料表獲得驗證碼。

建立驗證碼表，儲存方法如圖 3-5：

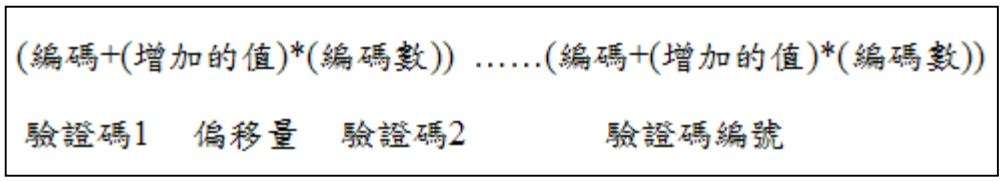

圖 3-5 儲存驗證碼表

(七)創建加密後的檔案：

透過關鍵代碼和檔案長度，我們計算新聞資料位置 1 並且插入左移表到轉後的符號表。

我們計算新聞資料位置 2，並且加入驗證碼表到轉後的符號表。

我們計算新聞資料位置 3，並且把加密資料表加入到轉後的符號表，就創建了加密新聞資料。

第(二)、(三)、(四)、(五)這四個步驟是可變動的，依照加密順序的不同，加密出來的密文也會有所不同。

第四節 解密演算法

解密演算法就是把加密演算法反轉過來，解密的步驟如下：

一、獲得加密資料表：

獲得加密新聞資料。

從新聞資訊資料庫獲得檔案的長度及關鍵代碼。

從檔案長度和關鍵代碼，計算新聞資料位置 3。

提取加密資料表之驗證碼，從加密新聞資料位置 2，摘取檢驗碼表。

利用關鍵代碼和檔案長度計算出新聞資料位置 1，得到左移表。

剩餘加密新聞資料存入加密符號表。

二、進行檔案驗證：

從加密資料表獲取驗證碼建立驗證碼。

上述從加密新聞資料位置 2，摘取檢驗碼表。

當提取出來的檢驗碼表和驗證碼相符合，如圖 3-6，就是驗證成功。

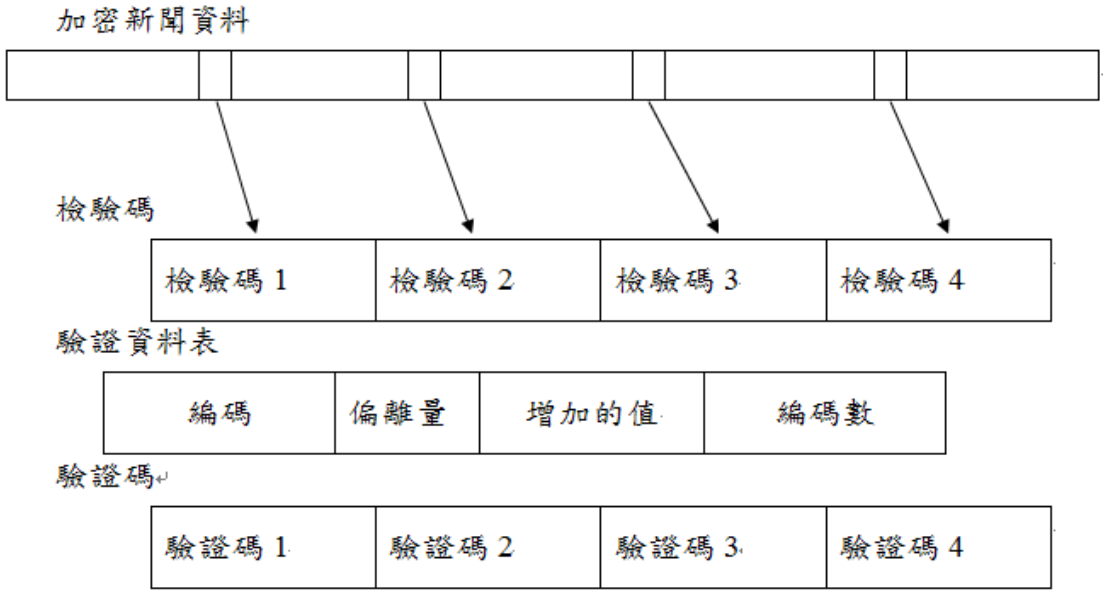

圖 3-6　比對驗證碼

三、還原輸出方向改變：

從加密資料表獲取格式碼。

從格式碼設定值得加密資料表中各欄位值。

從加密資料表獲得方向標誌，如果方向標誌設定，就把加密符號表反轉，獲得反轉後符號表。

四、還原位置交換：

從加密資料表獲得偏移量。

建立位移後符號表。

將反轉後符號表，順序每隔偏移量取出，加到位移後符號表後面，一直到反轉後符號表結束。

把偏移量減少 1，重複做上一個步驟。

重複做步驟 3、4 直到偏移量等於 0，得到位移後符號表。

五、還原左移：

取得加密資料表中左移表長度及左移表的值，根據設定的值，把每個位元左移 n 個位元。

從加密資料表獲得左移表長度及左移表。

隨著左移表上的每個位元值，順序將位移後符號表左移(一個位元值)位元。

最後獲得左移後符號表。

六、還原旋轉：

從加密資料表中獲得分割欄位數。

把左移後符號表照分割欄位數將其分割成區塊。

從加密資料表獲得旋轉量。

從起始的區塊重複向右或向左旋轉旋轉量。

我們獲得旋轉後符號表。

七、獲得加密前的檔案：

獲得新聞資訊資料庫的檔案長度。

從旋轉後符號表獲得前檔案長度之符號。

獲得加密前的資料。

第三、四、五、六，這四個步驟依照加密時所選擇的加密順序不同，解密時也必須讀取加密表單，依照該順序解密。

第五節　研究背景

本研究提出一個方法來驗證加密的資料，我們設定不同的加密資料表，使用這個加密資料表來加密新聞資料，每筆檔案都有不同的關鍵代碼，並且將關鍵代碼儲存在新聞資訊資料庫中。我們把加密資料表加進需要加密的檔案的關鍵代碼中，我們把加密過的檔案儲存在電腦之中，當我們要提取加密的檔案時，我們會同時得到加密過的檔案跟關鍵代碼，透過關鍵代碼，我們可以從加密的檔案中得到加密資料表，我們用加密資料表來解密加密過的新聞資料，在發佈之前，我們必須知道加密的新聞資料是否有遭到竄改。以下介紹本研究使用的檔案、資料庫、資料表。

一、使用者資訊資料庫

系統創建使用者帳號和密碼的時候，就會儲存到使用者資訊資料庫來做為驗證用，如圖 3-7。

使用者帳號	密碼

圖 3-7　使用者資訊資料庫

二、新聞資訊資料庫

新聞資訊資料庫包含新聞內容，新聞分類，關鍵代碼，

檔案長度，如圖 3-8。

新聞內容	新聞分類	關鍵代碼	檔案長度

圖 3-8　新聞資料表

三、加密資料表

加密資料表包含格式碼、左移表長度、旋轉量、驗證碼、偏移量、左移表、偏移量和方向標誌，如圖 3-9，加密資料表的長度為 10 位元。

加密資料表

格式碼	左移表長度	驗證碼	旋轉量	分割欄位數	偏移量	方向標誌
1byte	1byte	4byte	1byte	1byte	1byte	1byte

圖 3-9 加密資料表

四、左移表

左移表的每一個位元，對應加密的檔案的關係如圖 3-10 . LH 是左邊的一個位元，RH 是右邊的一個位元。

位元1		位元2		…		位元 (左移表長度)	
L H	R H	L H	R H			LH	RH

圖 3-10 左移表

五、驗證碼

驗證碼是用來驗證儲存的資料. 他包含編碼、偏離量、增

加的值、驗證碼數量如圖 3-11。

編碼	偏離量	增加的值	編碼數

圖 3-11 驗證碼

六、儲存驗證碼

儲存驗證碼的方法如同圖 3-12。

編碼 (編碼 + 增加的字元).....(編碼 + 增加的字元)
驗證碼1 偏移量 驗證碼2 驗證碼編號

圖 3-12 驗證碼儲存規則

七、檢驗碼表

我們把圖 3-12 組合起來產生檢驗碼表如圖 3-13，我們利用這個表格來驗證儲存中的加密資料。

驗證碼1	驗證碼2	…	驗證碼編號

圖 3-13 檢驗碼表

驗證步驟如下：

(一)獲得加密資料表

1. 獲得加密新聞資料。
2. 從新聞資訊資料庫獲得檔案長度和關鍵代碼。

3. 從檔案長度、關鍵碼來計算新聞資料位置 3。

4. 獲得加密資料表。

(二)獲得驗證碼表

1. 從加密資料表獲得驗證碼，建立驗證碼表。

2. 從檔案長度和驗證碼，我們計算出新聞資料位置 2。

3. 從新聞資料位置 2 和驗證碼，我們得到檢驗碼表。

4. 如果檢驗碼表和存放驗證碼表相同，儲存的資料就是原始沒有被更動過的資料。

八、計算新聞資料位置

透過檔案的關鍵代碼(key code)，檔案長度(length of file)，驗證碼(Verification code)、偏移量(offset number)、左移表長度、和加密資料表長度，我們設計算新聞資料位置 Lp1、Lp2、Lp3 規則如下：

如果(檔案長度+左移表長度)≧關鍵代碼，則新聞資料位置 1 = 關鍵代碼。

如果(檔案長度+左移表長度)<關鍵代碼，則新聞資料位置 1 = mod(關鍵代碼/(檔案長度+左移表長度)。

新聞資料位置 1 用來插入左移表和左移表長度。

D1 = 1+(偏移個數-1)*偏移量

如果(檔案長度+左移表長度+偏移個數)≧(關鍵代碼+D1)，則新聞資料位置 2 = 關鍵代碼。

如果(檔案長度+左移表長度+偏移個數) < (關鍵代碼+D1)，則新聞資料位置 2 = mod(關鍵代碼/(檔案長度+左移表長度+偏移個數))。

如果新聞資料位置 2+D1 > 檔案長度+左移表長度，則重置偏移量和偏移個數。

如果(檔案長度+左移表長度+偏移個數+加密資料表長度) ≧ 關鍵代碼，則新聞資料位置 3＝ 關鍵代碼。

如果(檔案長度+左移表長度+偏移個數+加密資料表長度) ＜ 關鍵代碼，則新聞資料位置 3 ＝ mod(關鍵代碼/(檔案長度+左移表長度+偏移個數+加密資料表長度))。新聞資料位置 3 用來插入加密資料表和加密資料表長度。