第六章　結論與討論

在此研究中，我們有以下幾點結論：

一、本研究可以解決當系統遭到入侵時，新聞資料會遭人輕易竄改的問題，加入驗證步驟，可以得知密文是否遭到修改。如果密文遭到修改，儲存加密表單及驗證碼的位置就會有所變動，提取出的驗證碼就會不正確，除非攻擊者同時獲得計算位置的公式以及破解出加密表單，否則就算攻擊者將修改後的明文重新加密也可以被發覺，進而防範因資料遭到竄改而蒙受損失。

二、本研究所使用的加密法著重於加密表單的保護措施，即使密文在傳輸過程被人攔截，由於我們加密的鍵值刻意選擇數字，攻擊者並無法有效分辨他擷取到的鍵值是屬於加密表單的哪一個欄位，每一筆新聞資料他都必須要嚐試最多6階乘種變化去排列組合，才能分析出可能的明文，遠比以往的只使用一種加密順序來的安全，就算攻擊者事先獲得部分明文和密文去比對，也很難在訊息有效期間內將密文解密，達到他所想要入侵的目的。

三、透過計算將加密表單隱藏於加密檔案之中，可以比將加密表單另外儲存的傳統做法更為安全。

四、改變加密順序，可以得到不同的密文，除了格式碼和驗證碼的順序不能改動之外，其他步驟都可以任意調配順序、配合加密表單鍵值的排列組合，可以提升破密的難度。

本研究之未來研究方向有下面幾點：

一、針對效能的提升，若是檔案過於龐大時，我們可以考慮將明文分割成多段，加快讀取符號表的效率。

二、程式可發展成不侷限於單一台個人電腦備份，可以考慮區域網路間的加密應用，透過一個執行節點來進行加密動作，而加密檔案儲存於其他節點中，可以更加提升安全性。