第一章　緒論

第一節　研究背景與動機

過往所使用的資料加密法，是將檔案進行加密之後，再使用不同的加密法額外加密鍵值來加以保護。就好像是將寶藏鎖在厚重的金庫中，然後再層層保護開啟金庫的那把金鑰，但是這種加密法，只要鑰匙被竊取，那無論金庫的門有多厚重，都形同虛設。為了防止因為鑰匙被竊取使得想要保護的資料遭到破解，因此有了反向思考：如果鑰匙被竊取而使得防盜措施失效，那乾脆把鑰匙和鎖合而為一。直接透過計算把加密表單隱藏至加密檔案之中，再透過驗證的手法來雙重防護，即使鑰匙遭到竊取，檔案也不至於那麼快遭到破解。

將這種加密法應用於有時效限制的新聞資料，新聞網站是一個單位對外發表消息的管道，是由保存用伺服器跟發佈用伺服器所組成，保存用伺服器負責保護新聞資料，發佈用伺服器則用來發佈新聞，過往新聞資料在發佈的途中都是以明文的方式直接傳輸，極容易遭到有心人士攔截及修改，為了避免遭到不正當手段的攻擊造成企業形象受損，我們必須要對資料加密保護，傳輸的時候以密文的方式進行，需要的時候才加以解密驗證，經過特殊的驗證演算法來進行驗證，當資料遭受異動我們可以馬上得知，進而選擇不發佈該則新聞，如此就可以加強我們對新聞資料的保護措施，減少因為被竄改的新聞資料發佈的損失。

第二節　研究目的

本研究的目的是對重要新聞資料提出保護機制，該機制為把新聞資料加密儲存之後，透過加密驗證機制，有效的預防加密資料遭到高明的駭客解密之後竄改內容，在解密發佈之前，提出一個新的資料驗證模組，藉此加以達到資訊隱藏，防範資料遭受竄改的效果。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檔案資訊資料庫中。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。如此就可以避免因被竄改過的新聞資訊造成的有形和無形的損失。

由於現在科技日新月異，不管多完美的加密法如果沒有跟著演進推陳出新，到最後還是會淪為被破解一途，因此本研究企圖多提出一個新的資料驗證方法，搭配加密步驟來達成更高的防護效果。

第三節　研究範圍與限制

本研究主要是將預先處理好的新聞資料加密及驗證，對要加密的新聞內容要預先處理好，加密之前必須以人工的方式先行分類以及判別新聞資料的真偽。

本研究使用的程式設計軟體為 Visual basic 2007，加密和驗證的檔案為.txt 檔，加密和驗證測試皆在單一個人電腦上。

第四節　研究架構與流程

以下將研究流程以圖示表現，請參見圖 1-1。

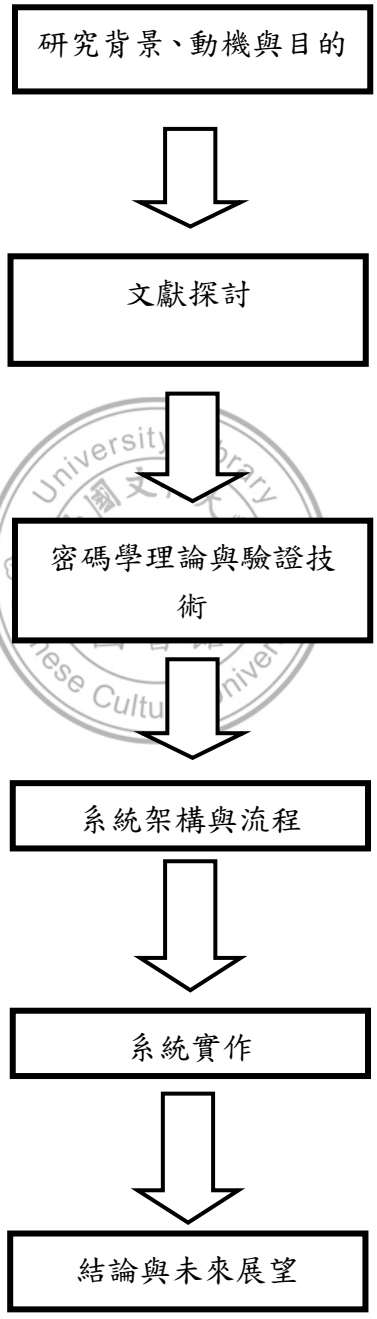

圖 1-1　研究流程圖