國立台北大學資訊工程學系專題報告

基於資訊隱藏與串流密碼實現多媒體加解密應用程式

專題編號: PRJ-NTPUCSIE-110-002

執行期間 : 2021 年 9 月至 2022 年 5 月

1. 摘要

資訊隱藏技術做為資訊安全領域中較為新興的一個分支，近幾年來基於各種載體及不同隱寫術的不斷研究與精進，已發展出諸如數位浮水印等等許多成熟的實際應用。在此次的專題研究中，我們以 LSB 隱寫術為基礎原理，開發新的圖片資訊隱藏隱寫術算法，將可藏資訊量擴增三倍，並控制圖片失真在人體肉眼可察覺的範圍之下。除此之外，為提高對機密訊息的保護層級，我們加入了串流密碼的加密系統，使得機密訊息更難以被破解。

最後，為提升本專題研究所開發出的應用程式之實用性，我們利用 google 所提供的語音辨識套件，為應用程式增加可將使用者語音輸入的訊息轉換為文字的功能，我們同時實踐了可將文字透過 google 語音助理執行語音合成後輸出的功能，使得程式實用性更加提升。

關鍵字 : 圖片資訊隱藏、LSB Steganography、串流密碼、語音辨識、語音合成

2. 簡介

結合資訊隱藏技術及串流加密系統，打造容易使用的應用程式，供使用者將不限類型的機密檔案藏入圖片或影片中，達到保護機密檔案且安全性高的目的。

3. 專題進行方式

3.1 資訊隱藏

作為資訊安全領域的一部分，旨於保護目標檔案或特定訊息不被攻擊者破譯、解讀，但與加、解密系統不同，除了要被保護的機密檔案外，尚需要一個載體檔案，透過演算法將機密檔案嵌入載體檔案，且嵌入後載體檔案必須保證難以被察覺，方為資訊隱藏技術的應用。

3.1.1 圖片資訊隱藏

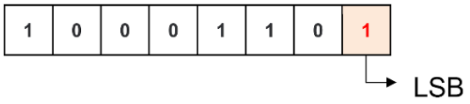
本專題研究所研製出的應用程式，即利用圖片作為載體，將機密檔案嵌入圖片中，且保證圖片在嵌入機密訊息後，不會產生嚴重的質變，使攻擊者得以輕易察覺該圖片中暗藏玄機而嘗試攻擊之。

影像經過資訊隱藏演算法後，不可察覺性可透過與原圖對比是否能夠察覺異樣主觀判斷，然而人體眼睛對色彩的靈敏度因人而易，因此學術上多以計算 PSNR 數值作為評量標準，PSNR 數值低於 30 時，表示影像的失真已可為大多數人所見。

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (1)$$

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (2)$$

3.1.2 Least Significant Bit Steganography



最低有效位元(Least Significiant Bit，簡稱 LSB)，代表二進制數字中最小的位元，即最低位元。

LSB 隱寫術(Least Significant Bit Steganography)是一種將圖像的 LSB 進行替換的技術。在此隱寫術中，可以抹去原先 LSB 的資料並嵌入訊息，能夠儲存訊息並達到資訊隱藏的效果，同時對圖像本身的影響最小，提升其不易查覺性。提取機密訊息時，我們可以通過提取像素的 LSB 來獲得不失真秘密訊息。

3.1.3 Modified LSB Steganography

我們以 LSB 隱寫術的原理做為基礎，設計實驗研究若每個像素點中各個通道數值轉成二進位表示後，用以嵌入機密訊息的位元不只一位，而分別嘗試將最低一到四位元都用以嵌入訊息，對嵌入後的影像品質有多大程度的影響，及是否仍能滿足不可察覺性。

實驗選擇七張照片，檔案類型皆為 .png 檔案，總像素介於 13 萬至 647 萬。為確保位元經過置換後，能盡可能計算出最小的 PSNR 數值，置換後所得實驗結果如下表 1，再將表 1 資料可視化為圖 3。

表 1

	a	b	c	d	e	f	g
總 pixel 數	278,419	2,711,880	360,000	137,641	6,471,936	426,400	565,692
嵌入最低一位元後 PSNR 值	48.1308	48.1308	48.1308	48.1308	48.1308	48.1308	48.1308
嵌入最低兩位元後 PSNR 值	39.9994	38.9551	39.9856	41.5410	39.9957	40.0282	39.9229
嵌入最低三位元後 PSNR 值	33.1493	31.7207	33.1267	32.9929	33.1370	33.2131	32.8213
嵌入最低四位元後 PSNR 值	26.7343	25.1297	26.7309	27.0841	26.7629	26.5290	26.8542

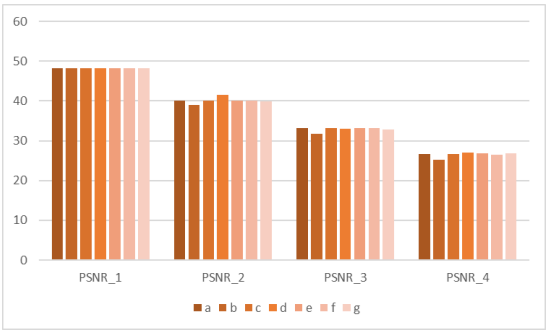


圖 1

根據以上實驗，我們得出結論：置換至最低三位元時，PSNR 數值大多介於 30 至 35 之間，且可滿足不可察覺性。故在容量與不可察覺性兩者間取出平衡點，取用最低三位元用以嵌入機密檔案的位元流，是為 Modified LSB 隱寫術。

3.2 Stream Cipher

一種對稱加密演算法，加密和解密雙方使用相同偽隨機加密資料流(pseudo-random stream)作為金鑰，明文資料每次與金鑰資料流順次對應加密，得到密文資料流。

3.2.1 pseudo random bit generator

簡稱 PRBG，用於產生偽隨機亂數。為提高加密強度，使用者輸入之密碼做為 PRBG 的初始值，利用 PRBG 產生出的偽隨機數列再當作加密用的金鑰。

3.2.2 Linear feedback shift register

線性反饋移位暫存器(LFSR)。給定初始狀態，由每一組的 LFSR 在同一個時序下產生的輸出組合為 Key Stream，透過 LFSR 極大的循環周期，可以產生安全性非常高的偽隨機亂數數列。3.2.1 小節的 PRBG 即由許多組 LFSR 組合而成以實踐。

3.2.3 Nonlinear Combining Function

由於各組 LFSR 產生出的亂數數列都有周期限制，透過此函數將各組 LFSR 產生出的結果組合，以獲得一個週期更大的偽隨機亂數數列。

3.2.4 XOR Stream Cipher

XOR 加密流程如下圖 2，使用者所輸入的金鑰會做為亂數種子放進 PRBG，再由其產出加密用的金鑰位元流(Key stream)，接著將金鑰位元流與機密檔案的位元流做 XOR 運算，得到加密後的機密檔案位元流。解密時只需要將加密後的機密檔案位元流與金鑰位元流再做一輪 XOR，即可得到機密檔案的位元流。

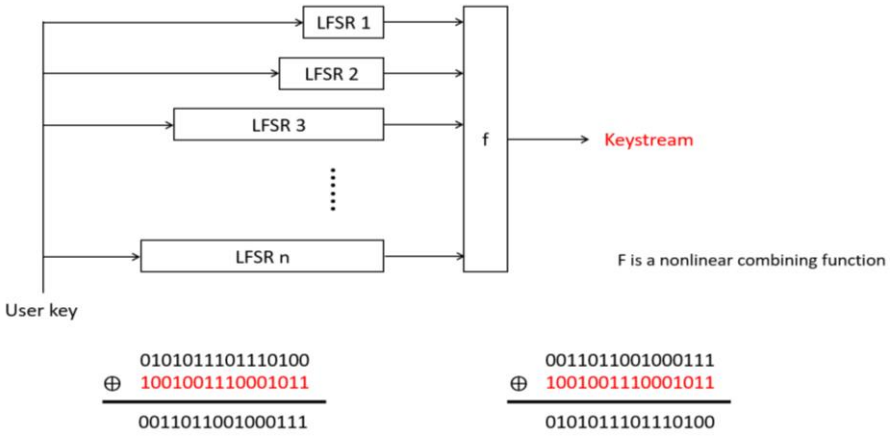


圖 2

3.3 Programming & Data Structure

File amount (4 bits)	File name length (8 bits)
File data length (28 bits)	
File name bitstream	File data bitstream

圖 3

如上圖 3，透過圖片的總 pixel 數、檔案名稱與內容的位元流總長度，來控制要在影像的最低第幾位元中正確地解出機密訊息的內容。

考量到可以藏入多份檔案，因此在檔頭的部分，用 4 bits 紀錄該份載體中藏入的檔案數量。藏入的每份檔案，檔頭皆僅保留 8 bits 紀錄該份檔案檔名位元流的長度、28 bits 紀錄該份檔案內容的位元流長度，緊跟著檔頭分別是檔名位元流與檔案內容位元流。

3.4 使用者操作介面

在應用程式設計上，我們將藏入與解出的功能整合於同一個應用程式中，使用者可點選按鈕進入不同功能的介面。

圖 4. 應用程式主介面

藏入功能的使用者介面如下圖 5。

Step1 ：Select Media 讓使用者可選擇本機的一張照片或影片當作載體，Take Photo 則是開啟相機讓使用者可以直接拍照當作載體。

Step2 ：Select File 讓使用者選擇本機中要藏入的機密檔案，Create File 讓使用者可以透過我們的應用程式撰寫要隱藏的機密檔案，按下 Create File 後將開啟分頁如下圖 6：使用者按下 Record 按鈕，程式會開啟麥克風收音，再將使用者的語音翻譯為文字顯示。

使用者開啟或編輯出的多份待隱藏檔案，會顯示於右邊的列表中，列表下的 Delete 按鈕則可用以移除已上傳至應用程式中的待隱藏檔案。在 Preview 預覽框下方的進度條，會顯示使用者目前上傳的所有待隱藏檔案，佔載體可藏容量的百分比。

Step3 ：使用者可自行定義 16 位不限英、數字、符號的密碼，或是按下右邊的 Random 按鈕由應用程式提供一組隨機產生出的密碼。

START：使用者完成前三步驟後，按下並選擇存檔路徑即可得到一份藏有機密訊息的影像檔案。

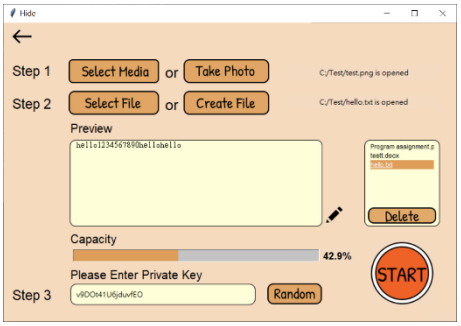


圖 5

圖 6

解出功能的使用者介面如下圖 7。

Step1：Select Media：供使用者選擇藏有機密檔案的照片或影片。

Step2：請使用者輸入密碼。

Step3：使用者完成 Step1、2 後，按下 Start 鈕會跳出對話視窗供其選擇解出的機密檔案所要存放的位置。解出的所有機密檔案，各檔案名稱都會顯示於右邊的列表之中，使用者可點選列表中的檔案，若檔案為文字檔則會顯示於左側的 Preview 視窗，此時按下視窗旁的撥放鍵，應用程式會將視窗中的內容交予 google 語音助理執行語音合成後，語音輸出該份文字檔，再按下暫停鍵即可暫停或繼續撥放，按下停止鍵結束撥放。

圖 7

3.5 困難與解決方式

3.5.1 照片載體的容量限制

由於以圖片作為載體的可藏入資訊的容量有限，所以設計能夠處理影片作為載體輸入的應用程式，便不再受限於一張圖片的限制，增加可藏入資訊的容量。

將影片逐幀切為照片存放，按照順序嵌入機密檔案位元流，當該張照片放滿即開啟下一張照片繼續嵌入，直到機密檔案位元流完全被嵌入。

對於一般使用者來說，一部 10 秒鐘的影片即足以藏入論文或是其他照片檔案等等，因此也是我們的應用程式中非常重要的一項功能。

4. 主要成果與評估

我們研製出的這份應用程式具有幾項特點：第一點，結合資訊隱藏與串流密碼兩項技術，機密檔案的安全性非常高。攻擊者若想要發起攻擊，首先需要知道圖片或影片是否有藏入機密檔案，並且知悉將機密檔案的位元流嵌入載體照片或影片的規則，最後還需要金鑰將

加密過後的機密訊息位元流還原為正確的機密訊息位元流，因此，我們的應用程式確實可達到保護機密訊息的目的。

第二點，應用程式功能齊全，介面採步驟式設計，讓使用者容易操作，且藏入的機密檔案沒有檔案類型限制，不論是文字檔、pdf 檔、csv 檔…等都沒有問題，滿足使用者在各種情境下有保護機密檔案的需求，在兼顧不可察覺性的條件下載體容量也達到最高，約為載體檔案的 3/8。

5. 結語與展望

這次的專題研究中，我們鑽研了資訊隱藏與串流密碼兩個資訊安全的重要分支，並將兩原理吸收後，組合出我們的作品。除了掌握基本理論以外，我們也不斷嘗試擴充應用程式所包含的功能，利用 Google 提供的開發套件，實作語音轉文字的輸入與文字轉語音的輸出，提供更便捷的使用方式，最後從使用者的角度出發，將應用程式的使用者介面設計為流程式的操作。

未來我們期盼能夠在掌握更多理論基礎後，精進演算法使容量提升。

6. 銘謝

非常感謝指導教授提供資源與研究經驗分享及建議，讓我們在進行專題的路上更加順利，也感謝組員們的合作才能使我們的專題能如期完成。

7. 參考文獻

[1]

Chi-Kwong Chan∗, L.M. Cheng, Hiding data in images by simple LSB substitution, 2003

[2]

D. Neeta, K. Snehal and D. Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits," 2006 1st International Conference on Digital Information Management, 2007, pp. 173-178, doi: 10.1109/ICDIM.2007.369349.

[3]

http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf

[4]

https://art.csu.edu.tw/e-book/data/1041118-1041204/mobile/index.html#p=1

[5]

V. Agham and T. Pattewar, "Data hiding technique by using RGB-LSB mechanism," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-5, doi: 10.1109/ICICES.2014.7033981.