

畫中有話

基於資訊隱藏與串流密碼實現多媒體加解密應用程式

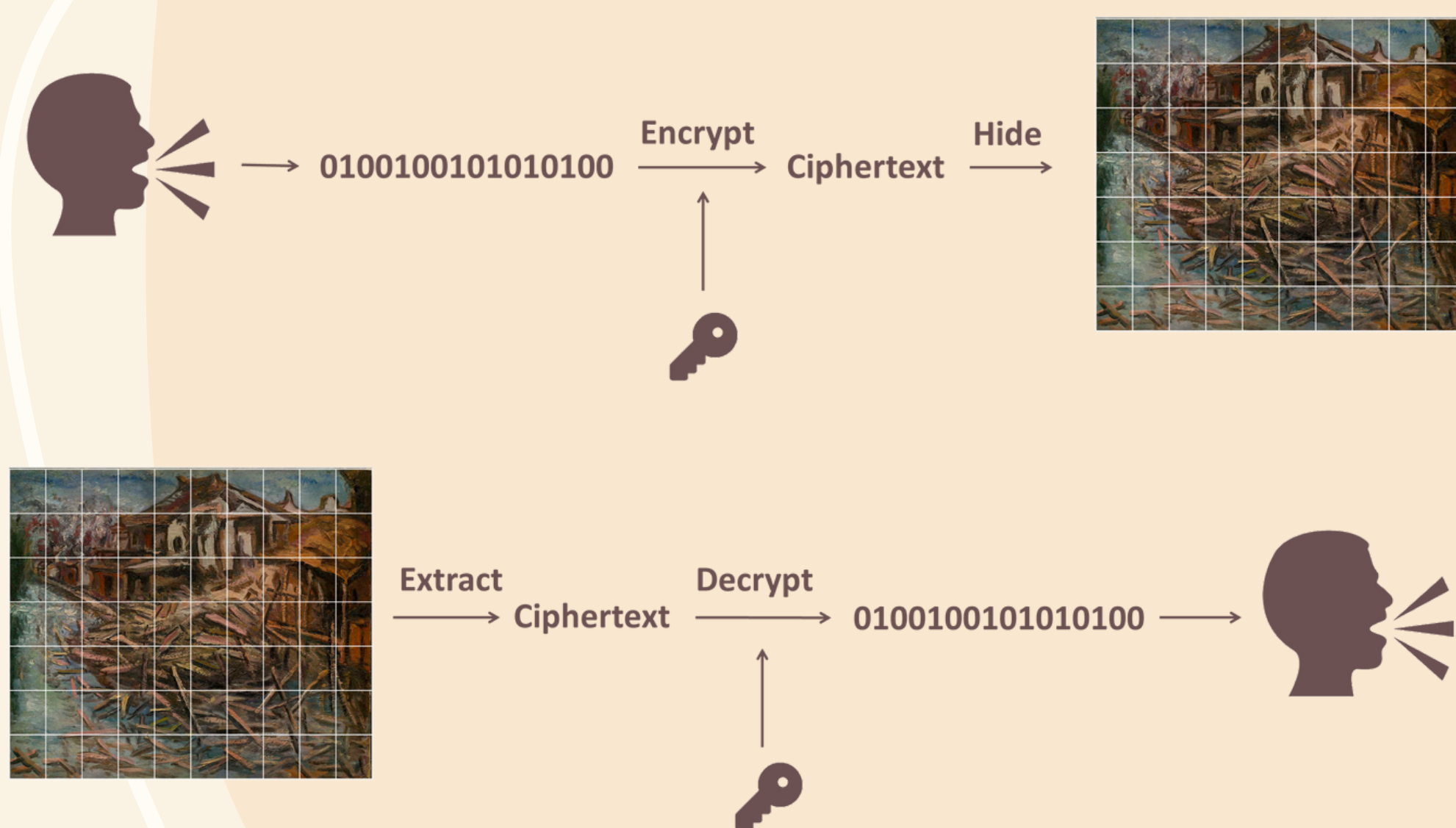
張維哲、劉政彥、蔡依霖、田翊辰

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，我們以 LSB Steganography 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。

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，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。

系統流程



系統介紹

1. Modified LSB Steganography

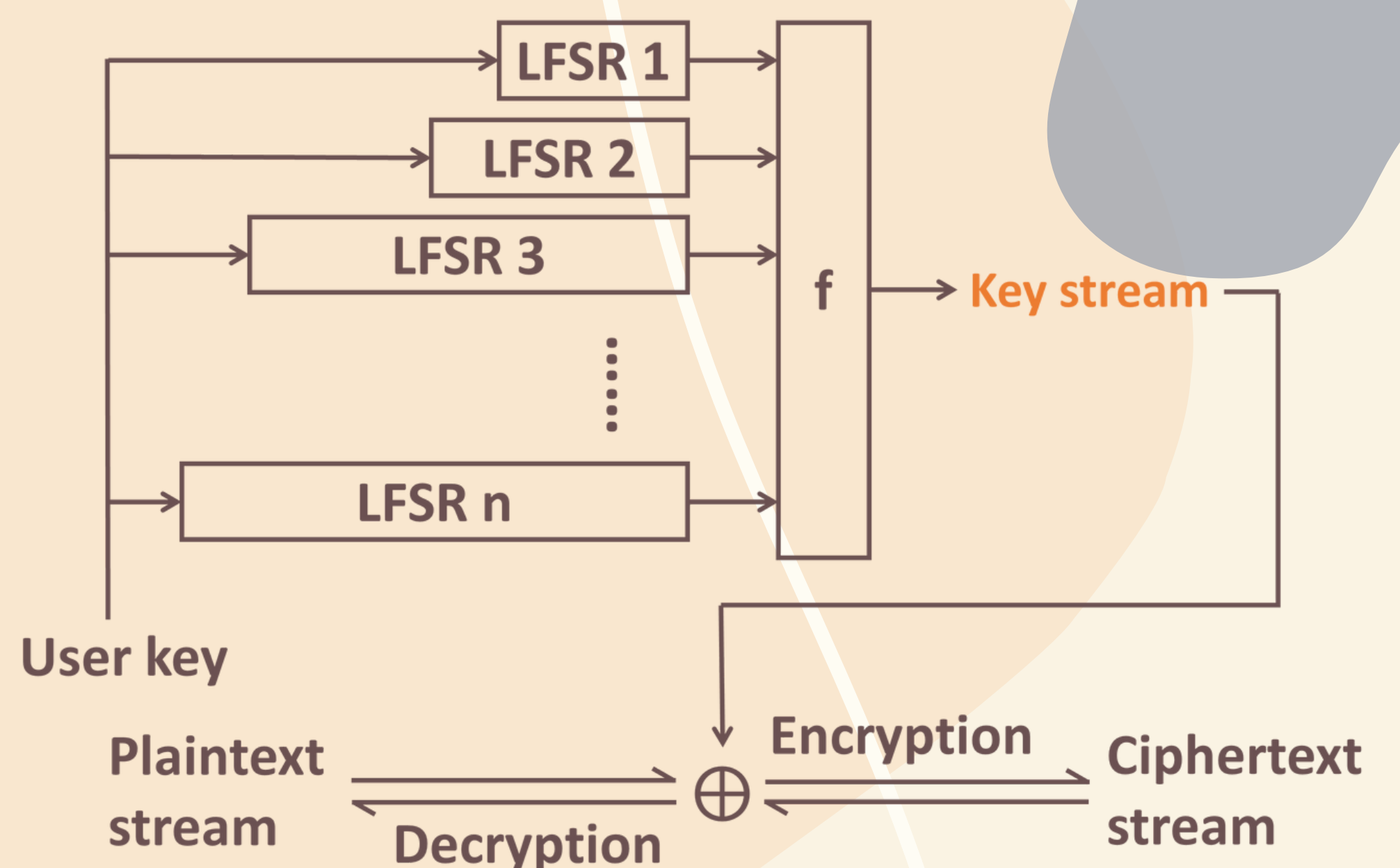
以 LSB Steganography 的原理做為基礎，在容量與不可察覺性兩者間取出平衡點，使用最低三位元嵌入機密訊息後，仍可滿足不可察覺性。

2. Data Structure



3. Stream Cipher

將Key stream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流。pseudo random bit generator 簡稱 PRBG，用於隨機產生亂數。為提高加密強度，使用者輸入之密碼並不會直接拿來當作加密金鑰，而是做為 PRBG 的輸入，利用 PRBG 產生出的隨機數列再當作加密用的金鑰。



結語與展望

這次的專題研究中，我們專研了資訊隱藏與串流密碼兩個資訊安全的重要分支，並將兩者原理吸收後，組合出我們最後研製出的作品。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，並且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，提高程式的穩健性。

考量本應用程式在實際應用上，使用者為保護機密訊息，必須用一份足夠大的照片或影片作為載體將訊息嵌入，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昇。