

研究計畫

隨著科技的進步，人們上網的時間越來越長，網路已經是生活中不可或缺的一部分，這也使得網路傳輸的安全顯得格外重要。我在大四暑假，研究 secret sharing 中，發現原來不是只有 Shamir's Secret Sharing，還有 Blakley's Secret Sharing、Counting-based Secret Sharing 或 Matrix-based Secret Sharing。其中也有針對圖片的 Visual Secret Sharing 或是針對聲音的 Audio Secret Sharing。我有意往這方面研究，發掘其在網路上的應用場景。

在我研究的「Secret Sharing with Multi-cover Steganographic Audio Files」題目，探討了 secret sharing 與隱寫術。在研究過程中，曾瀏覽到有篇論文提到在圖片中使用 LSB 的藏法會相當危險，因為圖片鄰近 pixel 的值通常會連續，他們的 LSB 值也會連續，但事實是否如此，如果圖片雜訊較多或是經過壓縮，那結果是否還會一樣呢？而聲音的 LSB 是否真的沒有連續性？我也有意往這方面探索。

同時我也對資訊安全相關領域想多嘗試。這學期我修習了「C 語言安全程式設計」，目前學到許多相關知識，像是 Buffer Overflow 會造成的問題，也期待自己能在這堂課收穫滿滿。而我也會在大四剩餘的時間裡，學習資安相關的知識。