國立中興大學　　科學與資訊計　研究所

學術演講

主講人：陳昱圻 教授

講題：

A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms

摘要：

可逆式資訊隱藏於加密影像上(RDHEI)被視為是保有影像隱私且又能實現嵌入資料的重要方法。RDHEI架構通常包含三種單位：影像提供者、資料隱藏者、驗證者。在金鑰設定的安全角度上，可以分為三個種類共享獨立私鑰(SIK)、共享單一金鑰(SOK)以及無共享私鑰(SNK)。在SIK上，影像提供者與資料隱藏者必須分別獨立的與驗證者共享私鑰，而SNK則完全相法不需共享任何私鑰。然而，在過去方法中所提出的SNK方法皆基於計算成本高的同態加密。本研究致力於SOK這樣的設定，唯有影像提供者與驗證者需共享金鑰，而資料隱藏者不需任何秘密資訊即可動作。換言之，任何人皆可以擔任資訊隱藏者。為實現SOK，本研究提出一個新技術利用多私密分享擔任底層加密方式。此方法雖完成構造但卻導　金鑰過長，為克服此問題，本研採用輕量密碼學演算法來做壓縮。最後，我們利用實驗與分析來驗證提出方法的效率與可行性。

13 JAN | **AM 10:30**
資科大樓**U501**

歡迎本系所師生共同參與

Department of Applied Math. & Institute of Statistics