編輯序

資訊安全通訊期刊本季Vol. 26 No. 2以電子刊物與印刷的刊物形式並行發行，本會會員將以電子刊物的形式發放，紙本印刷期刊發行予團體及機關訂戶。線上審稿功能系統將於本年度啟用。

本期卷公開徵稿部分收錄了三篇文章，分別為義守大學資訊工程學系陳延華教授及其研究團隊撰寫之「Efficient schemes with diverse of a pair of circulant matrices for AES MixColumns-InvMixcolumns transformation」、崑山科技大學資訊管理學系王平教授及其研究團隊撰寫之「LeNet-5卷積神經網路應用於勒索病毒分類」以及國立宜蘭大學資訊工程系吳信德教授及其研究團隊撰寫之「具有網路安全性保護之智慧藥盒」。

「Efficient schemes with diverse of a pair of circulant matrices for AES MixColumns-InvMixcolumns transformation」一文針對AES加密演算法的混行轉換(MixColumns-InvMixColumns)提出循環矩陣(Circulant matrix)的改善方法，透過在STM32L476VG MCU的實驗數據顯示，能夠減少約60%的加密與解密時間。「LeNet-5卷積神經網路應用於勒索病毒分類」透過沙盒及正規化概念分析法建立勒索病毒之行為特徵矩陣以提供模式預訓練(Pre-training)，再透過深度學習網路(Deep Learning Networks)之LeNet-5卷積神經網路(Convolutional Neural Networks)進行病毒行為的學習及特徵影像識別，提高病電腦病毒分類與偵測的正確性。「具有網路安全性保護之智慧藥盒」提出智慧藥盒結合APP與實際藥盒的應用系統，改善病患時常忘記服藥與服錯藥的困境，並且利用Bilinear Pairing技術進行身分驗證以及資料加密，確保資料的安全性以及身分驗證的合法性。

在本期 Quarterly 部分收錄了團體會員簡介，提供各位會員參閱。本刊將持續朝落實期刊國際化工作方向邁進，陸續著手國際知名研究索引資料庫的申請工作，感謝所有讀者長期的支持，並歡迎各位先進提供最新的研究成果至本刊進行分享與交流。

國立宜蘭大學
資訊工程學系
陳 麒 元