

Editorial

新的出刊，在 2020 的年初，綜合 2019 年，本期 2019-JITAS，<http://jitas.im.cpu.edu.tw/>，共刊載五篇論文，分列三個領域：資訊應用、資訊犯罪、資訊安全。

I. 資訊應用

- 植基於 QoE 之網路電話系統語音品質監測機制之研究
- 資訊用光碟機產業發展策略

第一篇論文，“植基於 QoE 之網路電話系統語音品質監測機制之研究，”作者為陳建誠、劉興華、傅振華。本研究植基於改良簡易式 E 模型中的 QoE(Quality of Experience) 演算法，建置一個網路電話系統架構上量測語音品質 QoE 的雛型系統，提供管理者有效且即時監控網路電話服務通話品質的量測工具；透過此一雛型系統，網路電話管理者可以省略複雜的主動式音頻評估方式，即可及時獲得端點對端點的用戶通話數據，精準量測語音品質的平均意見得分(Mean Opinion Scores, MOS)。第二篇論文，“資訊用光碟機產業發展策略，”作者為劉靖華。本研究發現由於光碟片及光碟機相關技術仍持續演進，強化光儲存設備本身的特性之外，同時增強較其他儲存媒體不足之處，讓光碟機更適用於新需求領域。

II. 資訊犯罪

- Image Recognition in New and Emerging Drugs (NEDs) Package with Convolutional Neural Network
- 無痕瀏覽模式調查惡意攻擊跡證

第三篇論文，“Image Recognition in New and Emerging Drugs (NEDs) Package with Convolutional Neural Network,” the author is Chih-Ping Yen. Based on deep learning, this paper proposes a Multi-channel convolutional neural network (MCCNN) architecture to check the suspected packaging by taking photos with smart phones。第四篇論文，“無痕瀏覽模式調查惡意攻擊跡證，”作者為莊禾暘、左瑞麟、柯宏叡、洪國寶、王旭正。目前物聯網 (Internet of Thing, IoT) 發展已來到第四階段，也就是透過既有的Web標準來達成設備間互相通訊，稱之為WoT (Web of Things)。本研究著重於Web應用程式在無痕瀏覽模式下的SQL Injection與Cross-Site Scripting (XSS) 的攻擊手法進行分析，藉由記憶體鑑識技術找出攻擊端及受駭端之證據關聯性，建立完整鑑識程序。

III. 資訊安全

- 運用可位移嵌入策略以提高圖像品質之可逆式資訊隱藏技術

第五篇論文，“運用可位移嵌入策略以提高圖像品質之可逆式資訊隱藏技術，”作者為沈肇基、李金鳳、吳宜蓁。資訊隱藏是將特定的資訊嵌入媒體，例如文本、圖像、視頻等。目的在於保護隱藏的資訊不引起監控者的注意，而減少被攻擊的可能性。本研究使用圖像作為嵌入媒體，並選擇可逆式資訊隱藏(Reversible Data Hiding, RDH)作為嵌入方法，在取出機密資訊後，能還原至原始影像。本篇論文提出了一種使用可位移區塊嵌入的策略應用在 PVO 及 DE 系列，來提升偽裝影像的影像品質。

EiC, JITAS

王旭正/Shiuh-Jeng WANG

<http://www.secforensics.org/>