

台灣網路智能學會

104 學年度博碩士論文得獎名單

博士論文獎1名

論文題目：資訊隱藏技術於數位內容保護之研究

學校：國立交通大學 資訊科學與工程研究所

研究生：柳曉龍

指導教授：袁賢銘、林家禎

摘要：

網際網路的蓬勃發展，徹底顛覆了人類傳輸資訊的方式，越來越多的數位化內容已通過公開渠道傳播。由於合法和非法用戶可以方便地訪問數位內容，網路上傳輸的數位內容很容易遭受惡意的攻擊，因此數位內容的安全和保護問題應該得到更多的關注。為了保障數位內容的安全傳輸，資訊隱藏技術已經成為近幾年研究的一個重要議題。在本文中，為保護不同的數位內容，我們分別針對機密資訊傳輸和數位圖像保護方面提出了相應的資訊隱藏方案。每種我們提出的方法都會與一些其他現存方法比較，用以證明我們所提方法的優越性。

對於機密資訊傳輸的主題，我們首先提出了一種整合資訊隱藏和圖像壓縮的方法。在壓縮和資訊隱藏步驟，利用MBTC來嵌入機密資訊，並同時壓縮複雜的區塊。對於平滑的區塊，根據當前欲嵌入的機密資訊，圖像修復或BSOC技術將被用於機密資訊嵌入和壓縮。為了提高壓縮效果與資訊藏量，我們接著結合更豐富的圖像壓縮技術提出了一個可回復式的資訊隱藏方法。主要運用於將大量的機密資訊隱藏於經過向量量化 (VQ) 壓縮後的圖像。而搜索順序編碼 (SOC) 和狀態碼本映射器 (SCM) 技術則用於減小輸出碼流的大小。

對於數位圖像保護的主題，我們提出了一個雙重的數位浮水印機制用於保護彩色圖像。其中，不可見的強韌性浮水印和脆弱性浮水印將被同時藏入圖像分別用於版權保護和圖像認證。為了版權保護的目的，第一重強韌的浮水印將利用離散小波變換 (DWT) 嵌入於圖像的YCbCr色彩空間。另一方面，第二重脆弱的浮水印是利用改進後的LSB方法藏入於RGB色彩空間。強韌和脆弱的浮水印結合的機制，將更加適用於寶貴的數位圖像的保護。

關鍵字：資訊隱藏、秘密通訊、浮水印、區塊截短編碼、向量量化編碼、離散小波轉換、版權保護、圖像認證

碩士論文獎 5 名

論文題目：根據區間直覺模糊值及線性規畫法以作多屬性決策之新方法

學校：國立臺灣科技大學 資訊工程系

研究生：黃智呈

指導教授：陳錫明

摘要：

近幾年來，有許多學者專家根據區間直覺模糊集合提出一些方法以作多屬性決策。在本論文

中，我們提出一個根據區間直覺模糊值及線性規劃法以作多屬性決策之新方法，其中每一個屬性的權重值及各方案的評估值均以區間直覺模糊值表示。本論文所提的方法具有比目前已存在的方法更簡單之優點，以在區間直覺模糊的環境中作多屬性決策。本論文提出一個很有用的方法以在區間直覺模糊的環境中作多屬性決策。

關鍵字：直覺模糊集合、區間直覺模糊集合、區間直覺模糊值、線性規劃法、多屬性決策

論文題目：不同階層式架構下之多族群遺傳演算法設計

學校：國立中山大學 資訊工程學系

研究生：彭元慶

指導教授：洪宗貝

摘要：

啟發式演算法近年來常被應用於解決實際生活中的各種複雜問題，其也相當容易使用且得出較好的解。在過去許多各式各樣不同類型的啟發式演算法被提出及應用，而一些學者也提出使用多個族群的啟發式演算法來縮短得到更好近似解所需的代數。因此在本論文中，我們首先回顧多族群基因演算法中的處理機制，並且針對其設計數個階層式執行架構。我們的貢獻分為三個主要部分，在第一部分中，我們首先探討多族群計算的特性，從而設計出不同階層式之多族群基因演算架構。在第二部分中，我們結合遷徙機制於上述多族群階層式架構中，並且比較遷徙機制所帶來的效能。而在第三部分中，我們將進一步考慮對階層式架構的多族群加入外來個體以增加搜尋多樣性並保有菁英個體。最後我們也藉由實驗驗證上述所提方法之有效性及執行效率。從實驗結果中可發現所提的階層式多族群架構可避免陷入區域最佳解，遷徙機制可以改善解的品質，及加入外來個體能增加整體搜尋最佳解的可變性。

關鍵字：基因演算法，啟發式演算法，階層執行架構，遷徙策略，多子群

論文題目：一個結合貪婪法與二元優化法之創新技術用以解決旅行銷售者問題

學校：國立屏東科技大學 資訊管理系

研究生：江耀

指導教授：蔡正發

摘要：

本論文提出一個結合了貪婪法與二元優化法的創新性啟發式演算法用以解決旅行銷售者問題。本技術首先運用二元優化演算法產生一組不錯的初始路徑，再透過隨機選取與貪婪選取兩個改良策略，用以不斷的改善舊有路徑直到完成所設定之終止條件。

本論文之實驗結果顯示，所提之GR-2OPT啟發式演算法在求解旅行銷售者問題方面的表現，比其他知名演算法更具效能與效率，並可能是目前現有之同性質演算法中表現最好的一個。

關鍵字：組合優化問題，旅行銷售者問題，啟發式演算法，二元優化演算法

論文題目：在人體區域網路中一個具有金鑰重建之彈性認證協定

學校：國立中山大學 資訊工程學系

研究生：王建升

指導教授：范俊逸

摘要：

人體區域網路(WBAN)在行動醫療照護之中扮演一個很重要的角色，我們可以將WBAN想像成圍繞在人體周圍的一個小型區域網路。在WBAN之中存在著三個主要的角色：感測器、閘道器、醫療中心。然而，感測器與閘道器的通訊距離僅有1-2公尺，如果閘道器遺失或是離開了由感測器所組成的WBAN之範圍，我們必須額外提供一個備用閘道器來持續地匯整與轉送感測資料。除此之外，由於預設閘道器擁有與醫療中心共享的對稱式金鑰，所以預設閘道器能夠與醫療中心建立安全通訊，但未來將作為備用閘道器的使用者裝置並不具有該把對稱式金鑰。為了解決備用閘道器沒有對稱式金鑰的問題，我們為WBAN此環境提出一個金鑰重建協定，在此協定中，預設閘道器具有賦予備用閘道器重建暫時性權杖(token)的能力，並且備用閘道器能夠透過該暫時性權杖與醫療中心建立安全通訊。

關鍵字：人體區域網路，醫療照護，認證，金鑰重建，同態機密分享

論文題目：多重巨量資料處理平台之排程優化

學校：國立高雄大學 資訊工程學系

研究生：張譯升

指導教授：張保榮

摘要：

本研究透過整合Hive、Impala和Spark SQL等三個平台，建立一套具有高效能、高可用性、高擴展性的多重平台資料處理系統，可以支援SQL命令以執行巨量資料檢索。本研究的目的是設計排成優化及最佳化平台選擇，並讓使用者透過單一介面進行操作，對於輸入的工作命令先進行排成優化，而即將執行的工作經最佳化平台選擇自動挑選效能最佳的巨量資料處理平台來進行。另外，利用Memcached分散式記憶體儲存系統以及Hadoop HDFS分散式檔案系統對SQL查詢結果實施快取機制，因此對重複的SQL命令可以最快速的檢索。雖然最佳化平台選擇可以顯著地降低系統執行SQL命令的查詢時間，但是加入排成優化更進一步地大幅提升系統的效能。

關鍵字：巨量資料處理、多重平台資料處理系統、排成優化、最佳化平台選擇、分散式記憶體快取、分散式檔案系統快取