出國報告（出國類別：會議）

參加 2011 年第 45 屆
卡拉漢國際會議年會

服務機關：法務部調查局
姓名職稱：蕭調查官志濱
翁調查官逸群
林調查官育梨

派赴國家：西班牙
出國期間：100 年 10 月 16 日至 10 月 23 日
報告日期：101 年 1 月 6 日

摘　要

2011 年第 45 屆卡拉漢國際會議年會（45th IEEE International Carnahan Conference on Security Technology）於 100 年 10 月 18 日至 10 月 21 日於西班牙巴塞隆納 Tecnocampus Mataro 舉行，本次研討會共有 58 篇論文發表及 3 場邀請演講。主辦單位將會議之議程依照其研究主題、技術領域不同設置 16 個發表場次，會場主要可分為以下四大類：biometrics、airport security、physical security、information security 及 applications。

卡拉漢會議創立於 1967 年，至今已有 44 年的歷史，是科技安全方面具權威且歷史攸久的國際性會議。與安全的相關議題是每個國家都熱烈探討的話題，各國為了維護國家安全都會投入大量人力、財力及資源。安全的議題隨著科技的進步、時代的演變，其觀念會有所調整，而其形式會變得多元化及多變化。本次藉由論文的發表參與卡拉漢會議，聆聽各國對於聲紋辨識（鑑定）、影像辨識（鑑定）及資訊安全等議題之研究成果，了解到面對科技日新月異，鑑識人員除了要有熟練的技術外，仍須不斷的充實知識，發掘問題並從不斷地試驗找出有效的解決方法，以強化鑑識（或鑑定）能力，再者，藉由參與國際會議以吸取各國菁英之經驗及技術，有助於提升本局鑑識能量。

目　　次

壹、 會議目的

一、藉由參與國際會議或實習以吸取數位鑑識相關實務經驗，並建立國際交流管道。

二、了解國外數位鑑識科學（或技術）之最新發展趨勢，以適時地運用得知之新技術或知識，提昇本局數位鑑識工作之品質。

三、透過學術論文發表，促進國際之間學術交流，提升研究水準。

貳、 會議過程

2011 年第 45 屆卡拉漢國際會議年會（45th IEEE International Carnahan Conference on Security Technology）於 100 年 10 月 18 日至 10 月 21 日於西班牙巴塞隆納 Tecnocampus Mataro 舉行，本次研討會共有 58 篇論文發表及 3 場邀請演講。主辦單位將會議之議程依照其研究主題、技術領域不同設置 16 個發表場次，會場主要可分為以下四大類：biometrics、airport security、physical security、information security 及 applications。

大會於 10 月 19 日上午 9:00 首先由本次會議執行團隊作開場，並於會中表示非常誠摯地歡迎每位人員來參加一年一度之卡拉漢會議;隨後則熱烈地歡迎會議主席 Gordon Thomas 至會場發表「Security: historical review from Carnahan perspective」。

此次會議共有 16 個場次(含 3 場邀請演講),每個場次約有 4-6 篇論文發表,卡拉漢會議議題涵蓋層面較廣，大多為實體安全（機場安全及管理）、指紋辨識（或鑑定）、聲紋辨識（或鑑定）、生物辨識、影像辨識（或鑑定）及應用，另有少數資訊安全議題。與會人員大多為學術界之教授、學生，藉由參與此會議發表其研究成果，並與此領域之專家、學者共同探討研究方法及分享其心得。會議期間我們就本局業務相關之場次分別聆聽有關於聲紋、影像辨識（或鑑定）以及資訊安全，以下為相關論文之概述：

一、Physical and logical security management organization model based on ISO 31000 and ISO 27001

此篇論文在探討大多數的通訊安全部門皆以不同的形式或組織架構存在企業或管理組織裡,使得推動實體及邏輯安全防護整合及其實施有其困難度。此篇論文提出一個方法論（規範），可以結合 ISO 31000 (實體安全)標準及 ISO 27001 標準並同時分析組織之資訊資產及營運資產。同時,在論文中亦提出一份安全管理制度文件以及在西班牙使用此規範的成功案件。

二、Physical and logical security risk analysis model

此篇論文主要是延續上一篇論文所提出的安全管理制度（規範）,探討實施該規範的同時,企業如何建構一個完整且能符合組織本身的風險管理系統。本篇論文發表一個風險分析方法論，使其能夠達到 ISO 31000 (實體安全)標準及 ISO 27001 標準，並說明如何針對組織的資訊資產及營運資產進行辨識、分析、評價其風險，該方法論在西班牙地區的公司已廣泛被使用。

三、Speaker verification based on comparing normalized spectrograms

此論文為本局與台北大學共同研究之成果,該成果為將錄音內容各字音的音量、字音長度、頻率響應...等進行標準化調整，使得比對的錄音資料得以有相同的位準，對錄音內容優先做統一標準的處理，可使比對結果更理想。在比對方法上使用圖譜直接比對，頻率一階導數變化、二階導數的負值比對等方式。

四、Preventing replay attacks on speaker verification systems

為防止在電話線路中,假冒者以揚聲器重播真實身份者的錄音內容去欺騙語者辨識系統；及將真實身份者的錄音內容關鍵字句剪貼成新的語音，去欺騙含語句密碼的語句相關(text dependent)語者辨識系統。該實驗設計條件多，結果錯誤率在 10%以下。

五、Glottal parameter estimation by wavelet transform for voice biometry

聲門參數估計領域，由肺部送出氣體，經過聲帶(vocal cords)的閉合，通常男生閉合頻率較慢，女生次之，小孩閉合頻率最快，所以男生聲音比較低。閉合產生氣的流動，流經口腔也流經鼻腔等，經由唇、齒、舌、顎的各種位置變化共振發出各種聲音。語音中有聲字音的不同，除在口腔形狀上產生差異外，在共振峰的位置上也有差別，如國語”一”音在第一個共振峰低而第二個共振峰較高的區域，而國語”ㄨ”音在第一個共振峰低而第二個共振峰亦低的區域等，經由共振峰位置可應用於簡單的語音識別及圖譜分析使用。結合聲學、語音學、信號處理學、甚至流體力學，約略模擬出人發音的模式，使人類對於語音的產生更清楚。

六、Increase of digital CCTVs makes it difficult to analyze record images

安全監控數位錄影普及卻衍生畫質降低主要是因為使用者為使硬碟容納最長時間錄影畫面，借由調降解析度、多分割畫面儲存、廣角鏡頭及過度壓縮等方式，導致畫質降低。再者，部份監控業者採用特殊錄影格式壓縮動態影像，重播時，造成畫面失真。針對上述之問題，可使用以下方式強化影像：1、利用同一圖格偏移相疊以獲得較清晰之影像輪廓。2、增加影像三原色色階，突顯畫面之明暗變化。3、二張連續模糊圖格相疊獲得較清晰之影像。

七、Scan documents secure authentication based on simple watermarking

此篇論文主要是提出一個掃瞄文件認證機制，提出的動機為簡化及方便民眾向政府機關申請文件之作業流程。一般民眾向政府機關申請官方文件時，須檢附個人之證件、學位證書、出生證明等文件資料，此類型的文件資料皆無法在網路上取得，必須本人複製後送交至申請機關，才算是完成申辦手續。有鑑於網路資料傳遞快速，應用此機制可使申請人將需提供之文件利用特定之掃瞄器掃瞄成為電子文件後，傳遞至申請機關之收件窗口，該收件窗口亦可驗證文件的完整性及有效性。此機制是利

用雜湊演算法、加密、簽章及浮水印技術，以達到文件資料的機密性、完整性、有效性及不可否認性。

八、Ghost key patterns with equidistant chosen message attack on RSA-CRT

RSA 演算法是應用非常廣泛的公開金鑰演算法之一，為增進其運算元之效率亦可採用其變形－RSA-CRT。現今， IC 智慧卡、可攜式個人裝置等內儲資訊愈來愈豐富且多樣，此類型裝置大多會使用上述之演算法加以保護內存的資料，然而使用此類型裝置的過程中，其側漏的資訊如電力消耗、運算時間與電磁散射等，很容易為攻擊者量測取得。在 2002 年，Boer et al.提出一個新的差分能量攻擊分析方法。此攻擊方法主要目標中間值是依存在 $r = x \bmod p$ ，即從 r 可計算出秘密參數 p 。不同於一般的能量攻擊法，這個方法是建構在相同等式的訊息上，而這些相同等式的訊息通常存在一些隱藏性關鍵資訊，此篇論文則是在發掘、探討及分析這些隱藏性關鍵資訊，並且提出相對應的防禦方法。

九、A digital evidence protection method with hierarchical access control mechanisms

此論文為本局與長庚大學共同研究之成果，主要探討依據階層組織管理原則，鑑識人員受到上層主管之監控，主管擁有加密／解密下屬文件之能力。然而，主管擁有可任意存取下屬文件之權限時，卻可能發生上司舞弊、濫權或破壞下屬隱私等情形，因而破壞數位證據之完整性與正確性，故必須強化數位鑑定報告管理平台之權限控管機制。針對上述情形，提出二種具監控機制之數位證據保全架構－全部監督及部分監督。全部監督意指上司具有存取下屬所有加密文件的能力；部分監督則是指上司只可存取下屬特定加密文件的能力。

十、The color identification of automobiles for video surveillance

此論文提出一個運用車燈偵測模組及樣本配對模組之車輛顏色辨識方法。利用車燈偵測找出有用的 ROI 之色彩來做色彩辨識，並運用 CIELab

方法將攝影機拍攝下來的車輛顏色自動分類，實驗後的結果發現：紅、黃、藍、綠、黑、白及灰色能成功的辨識，且平均正確率達到 81.71%。

參、心得與建議

一、 本次卡拉漢國際會議發表論文數約 58 篇，與語音類相關論文約計 8 篇,國內除發表 1 篇外，餘皆為西班牙及其巴斯克地區發表之論文，由此可看出，西班牙在語音類專業研究的重視。此會議發表之論文大多是傳統鑑識（鑑定）領域的研究成果，從聆聽主講者的報告內容及與會學者提問的問題可得知，參與此會議的學者、專家對於此領域鑽研的非常深入，且對於該領域應用的方法也有著不同的見解。再者，更有些論文的研究成果，已在該國相關組織或學界使用且成效良好。

二、 在語者識別領域，本局與國立台北大學共同合作發表乙篇，題目為正規化聲紋圖譜的語者識別(Speaker verification based on comparing normalized spectrograms)，由此項研究發現，以 69 個人相隔 2 個月的語音資料實驗，在 7 個短語句(每句約 6 至 10 字)中可得出約 99%的準確率。綜觀語者識別的實務應用，最關鍵的地方在於如何決定門檻，使得系統能保有最佳的辨別率。

三、 在錄音偽造判別領域，西班牙 Zaragoza 大學提出之語者識別系統中防止重播方式的攻擊(Preventing replay attacks on speaker verification systems)，根據了解，數位剪接或偽造判別一直是困難的領域，此項研究是一個創新開始。

四、 語音辨別的應用，幾乎由西班牙巴斯克地區的 University of the Basque Country 所發表，包括有語音情緒識別、巴斯克語文識別、強健型語音識別、多特徵模組語音識別安全系統、語意識別等。巴斯克地區位處西班牙、法國交界處，人口數在 2006 年時約 300 多萬人，有自己的巴斯

克語及方言。巴斯克語使用人口約 100 多萬人，語言的發展受法文、西班牙文影響，由此類論文發表可看出巴斯克地區對語言分析的重視。語音識別多數採用 MFCC 方式擷取特徵，再以 HMM 方式經過編譯字典、訓練、模組化等步驟，最後做成 ASR(Automatic speech recognition)自動語音識別系統。而在錄音語料過程，需要求最好的品質，訊雜比 SNR 高，如此經過系統訓練後，語音識別正確率才會提高。當然，在編譯字典上亦要建立更豐富的語料音，使得系統能有最佳的語音解析能力。

五、 從日本學者所發表的論文可以瞭解當前日本有關影像處理、軟體發展，及證據證明力認定法則，對提昇國內鑑識科學量能具參考價值。對於該論文所介紹之影像鑑識軟體其內建功能，均有明確理論說明，由此可知，鑑識工具除要有操作步驟說明外，針對每項功能亦需要附加理論說明，將有助於提昇科學證據之證明力。再者，該論文提到若圖片有使用鑑識工具加工（例如：強化影像），應在報告內加註效果說明，以使法官或檢察官瞭解原圖及修正過後之圖像的差異，並描述使用之鑑定技術其合理性。

六、 卡拉漢國際會議創辦於 1967 年，是歷史攸久的重要年會，今年為第 45 屆。1991 年及 2003 年曾在台北舉辦，對我國在安全專業領域表現重視。在 19 名會議執行委員中，我國列名 3 位，本局蒲副處長長恩，是其中的 1 位執行委員。參與本次會議，更感受到我國在國際專業會議上的努力耕耘，及我國在科技上穩定進步受歐美先進國家重視所帶來的成果。

七、 本局聲紋鑑定以說話人辨識(speaker verification)為主，而目前市場主流，則是以語音識別(speech identification)居多。但兩者僅是應用層面的不同，在專業知識上仍有許多相通之處，故本局應拓展更多機會，與國內外相關學術、研究單位及機關部門，建立溝通管道，甚至合作平臺。

八、 語音或語者自動識別能力，需要依靠數位信號處理背景及相關訓練，

且語音變異數多，分析及研判過程複雜。因此亟需廣納具語音分析的專業人才來從事此工作，使研究及實務均能加以提昇。

九、 建議可參考國內外科學證據判例，以提昇鑑識能力。根據美國證據法則，專家證言應以下列四種方法來檢驗其可採性和可靠性：(1) 專家證言內容是否通過科學方法加以檢測；(2) 作爲專家證言基礎理論或技術是否已發表，並且經得起同行嚴格複查檢驗。(3) 作爲專家證言基礎的研究方法或技術的出錯概率為何；(4) 在特定的科學領域中，有多少學者能加以認同和接受，該專家證言的技術、方法和理論。由此可知，科學證據在法庭上必被嚴格檢驗，因此透過實際的案例，可瞭解那些技術、方法及理論為法庭所接受或排除，並充實相關原理及方法，將有助於提昇鑑識能力。

十、 成立鑑識技術審議機構，制定相關技術準則：科學鑑識目的主要協助法官釐清事實，尤其刑事訴訟改為「改良式當事人進行主義」後，科學證據更突顯其重要性，但也產生許多科學證據證明力上的疑義，如測謊結果的參考性及槍械殺傷力的判定等，有鑑於此，應成立鑑識技術審議機構，針對現行常態性鑑識技術，分析其方法及理論，以確認科學證據之可採性及可靠性，並進一步訂定相關標準及技術說明，以杜絕日益增多的鑑識爭議。

十一、 本次能論文投稿及參與會議，係因國科會、法務部支持本局研究成果，期待未來在工作上發現新的問題或議題，並研究其可行方案，一方面除使本局鑑定實務能量不斷精進提昇，豐富專業人員知識，另一方面可透過論文的發表，了解國際間語音領域、影像鑑識、資訊安全發展情形，增進與國際專家學者互動交流關係，對於本局專業領域極具實質幫助。

附件：ICCST 會場之相關照片

圖 1　ICCST 會場

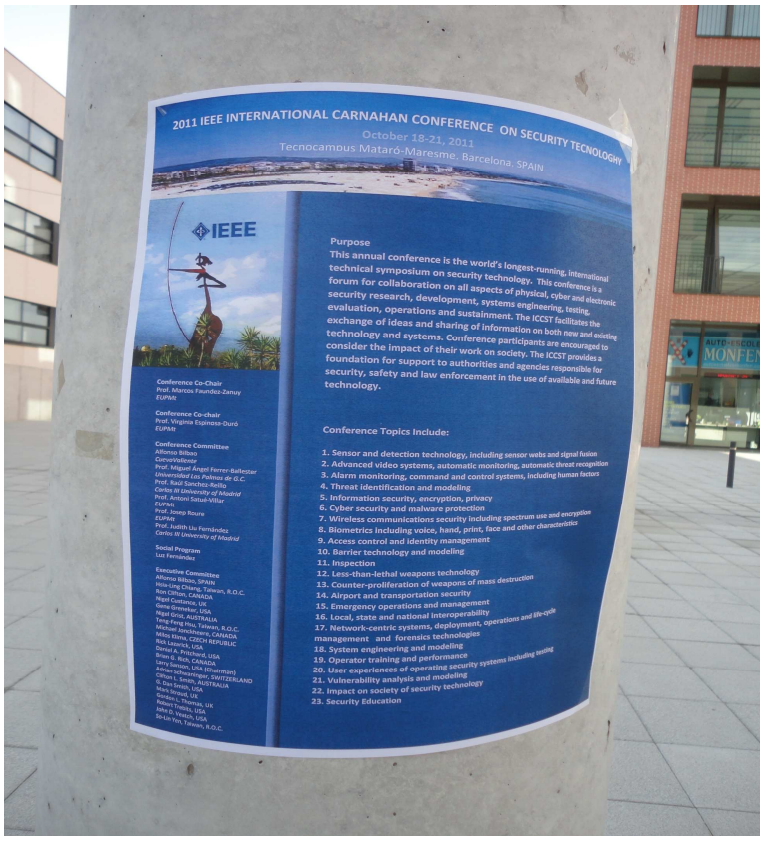

圖 2　2011 ICCST 會議海報

圖 3　ICCST 會議開場

圖 3　邀請演講- Gordon Thomas

圖 4　ICCST 會議之論文發表會場

圖 5　台北大學呂嘉穀教授發表論文

圖 6　中央大學王宇晨同學發表論文

圖 7　晚宴-Gordon Thomas

圖 8　與會之聯合大學韓欽銓教授及中央大學王宇晨同學