

出國報告（出國類別：會議）

參加 2018 年 IEEE 資訊理論與應用年度會議（ISITA）

服務機關：中央警察大學、彰化縣警察局

姓名職稱：副教授高大宇、助理教授蔡馥璟、科長柯宏勸

派赴國家：新加坡

出國期間：中華民國 107 年 10 月 27 日至 11 月 1 日

報告日期：中華民國 107 年 12 月 14 日

摘要

2018年資訊理論與應用年度會議（2018 The International Symposium on Information Theory and Its Applications, ISITA）於2018年10月28日至31日在新加坡舉行，本研討會係由IEEE協會和IEICE協會共同主辦。本次大會主題為「量子計算」、「訊號編碼」及「機器學習」等，議程涵蓋領域非常多元，各議程報告子主題包括無線通訊、人工智慧與深度學習在巨量資料之應用、資訊與網路安全及分散式與雲端計算等。此次，來自23個國家，超過230個專家學者參與，從眾多稿件中選出186篇論文進行報告，報告分成39個議程討論。中央警察大學及警政署所屬的警政資安團隊於「安全模式與協定（Security Models and Protocols）」議程中向與會人員發表「Mobile Forensics for Cloud Storage Service on iOS Systems（適用於iOS系統的雲端行動鑑識研究）」論文。

本研討會的主要目的係藉由舉辦國際會議，交流最新通訊技術與研究成果，加速各領域國際間的創新、變革與融合，在科技發展議題上扮演重要角色。與會專家學者的論文發表，可瞭解世界各國目前在電腦科學之學術研究方向，藉由與各國專家分享學術及實務經驗，可建立國際交流管道，提升我國資安犯罪偵查與鑑識之專業知識與相關技能。透過本次參加於新加坡舉辦的國際資訊通訊盛會，對於本校資訊通訊領域的學術發展，激盪出許多的心得。除本次會議中廣泛學習研討內容，適當引進國內發展外，作為警察學術研究的一員，更期許自己能夠不斷學習應用，尋求科技建警的執法因應之道。本校近年來非常重視警政科技之理論與應用，除逐年建立並維護專業且設備充實之科技建警相關實驗室外，亦從理論及實務雙管齊下，發展屬於執法領域的諸多研究能量，強化產（官）學之國際交流。期盼經由更多的國際交流，培育出優秀的專業人才，另建構警察專業人才之長期培養及經驗傳承制度，以利發展理論與實務兼顧的完整培訓體系。

目錄

壹、前言.....	- 4 -
一、會議介紹.....	- 4 -
二、出席目的.....	- 4 -
貳、研討會主題.....	- 5 -
一、機器學習.....	- 5 -
二、圖論與網路模型編碼.....	- 6 -
三、雲端鑑識.....	- 8 -
四、區塊鏈.....	- 10 -
(一) 公有鏈.....	- 11 -
(二) 私有鏈.....	- 11 -
(三) 聯盟鏈.....	- 11 -
五、數位浮水印.....	- 13 -
(一) 透明性.....	- 14 -
(二) 強韌性.....	- 14 -
(三) 安全性.....	- 14 -
(四) 忘卻性.....	- 15 -
(五) 明確性.....	- 15 -
六、視覺密碼學.....	- 16 -
參、與會心得及建議.....	- 19 -
一、與會心得.....	- 19 -
(一) 反思研究方向.....	- 19 -
(二) 持續推廣英文學習環境.....	- 19 -
二、建議事項.....	- 20 -
(一) 強化校際交流，持續鼓勵或經費支持學生參加國際研討會.....	- 20 -
(二) 熟悉工具軟體的應用，持續維護警政相關之專業資通訊實驗室.....	- 20 -

壹、前言

一、會議介紹

本年度資訊理論與應用研討會（2018 IEEE The International Symposium on Information Theory and Its Applications, ISITA）於2018年11月28日至31日（4天）在新加坡的國敦河畔大酒店（Hotel Grand Copthorne Waterfront）會場舉行，係由新加坡大學、IEEE和IEICE所共同主辦，會議內容廣泛包括各項資訊科技，包含「量子計算」、「訊號編碼」及「機器學習」等，細部報告主題包括資訊安全、通訊編碼、人工智慧與深度學習在巨量資料之應用等，對於資通訊領域具有重要的影響力。

本研討會自1990年舉辦至今，至今已有28年的歷史，各年度所發表的論文品質皆非常高，研討會發表的出版論文會收錄在IEEE Xplore學術文獻資料庫。本次研討會特別邀請來自美國聖地牙哥大學的Alexander Vardy學者，以「極化碼的過去、現在、未來（Past, Present, and Future of Polar Coding）」為題，發表專題演講。極化碼為目前訊號編碼的重要理論基礎，主要用於訊號傳遞的品質提升，藉由前向錯誤更正的方式，降低訊號傳遞中所產生的干擾。從2008年ISITA研討會開始，開啟了一連串的討論，在專利、晶片設計等佔有非常重要的地位，在5G訊號編碼的規格會議中，極化碼方案亦成為全球5G編碼的標準之一。本校及警政署團隊希望藉由參與研討會，與全球產官學之專家學者，互相交流最新通訊技術與研究成果，加速各領域國際間的創新、變革與融合，在社會科技發展議題上扮演重要角色。

二、出席目的

ISITA是通訊編碼、資訊安全及雲端運算的年度國際會議，所有來自國內外的專家學者們，藉由本研討會展示他們的最新研究成果，分享未來電信時代新想法和願景。本校及彰化縣警察局的研究團隊，有幸參與本國際會議，吸取世界各國在偵辦網路犯罪案件之心得與調查實務技巧；同時

瞭解世界各國目前在電腦科學之學術研究方向，分享學術及實務經驗，建立國際交流管道，以提昇我國通資警察之專業知識與相關技能。

貳、研討會主題

本次研討會所包含的主題非常廣泛，與會的學者專家發表的研究成果亦非常豐富且深入，以下簡要針對6項主題，摘要重點及分析報告內容。

一、機器學習

目前Web 2.0時代，使用者產生且上傳的資料量非常龐大，過去藉由人工方式建立資料處理模型的方法已無法處理大量資料。機器學習為因應大數據時代而發展的理論，以機器自動學習的觀點，讓資料來訓練機器的學習模式，成為最新的學術研究方向。

本場次共有4篇文章發表，4位發表者皆為日本學者，第1篇文章為 Yasuo Tabei 學者所發表的「Scalable Machine Learning on Compact Data Representations」，研究主題主要因應工業界不斷增長的大量高維度數據，必須提出相對應可擴展的數據計算技術，進行有效率的計算，將處理過的結果用於發現知識。Tabei學者提出運算這些數據的關鍵能力，就是統計模型是否具有自動學習的能力。目前學習統計的方法模型，大部分方法無法產生可解釋的結果，其餘皆會產生過高的計算成本。該文提出以偏最小平方迴歸演算法（Partial Least Squares Regression, PLS）為基礎，在PLS的基礎上，發展出壓縮偏最小平方迴歸演算法（Compression-based PLS），用以學習具有高可解釋性的預測線性模型。實驗結果亦說明該研究提出之方法，在預測準確性方面表現較佳，在計算效率及可解釋性方向，亦獲得較佳的結果。

第2篇文章為Mohammad Emtiyaz Khan 和 Didrik Nielsen學者所發表的「Fast yet Simple Natural-Gradient Descent for Variational Inference in Complex Models」。該文主要使用貝氏網路（Bayesian Network）優化梯度最佳化的問題。貝氏推理網路在機器學習方面發揮著重要作用，應用於深度神經網

路的複雜模型。該研究以自然梯度法，提高最佳化問題的收斂性，並展示如何在指數機率分佈中，以對偶生推導快速而簡單的自然梯度更新，以獲得較佳的學習成果。

第3篇文章為Wataru Kumagai學者所發表的「Introduction to Bandit Convex Optimization Algorithms」，Bandit Convex Optimization (BCO) 是不確定性下決策的基本框架，它概括資訊和統計學習領域的許多問題。雖然該理論可有效理解線性成本函數的特殊情況，但對於具有非線性損失的BCO而言，仍未獲得有效的解決。該文基於連續空間上的成本函數，解決一個凸集合的問題。作者提出隨機鏡像下降計算法，說明該算法可重新約束成本函數的強凸性和平滑性假設，再說明Bandit Convex最小化與成本函數的凸優化之間的等價性。

第4篇文章為Kohei Hatano學者所發表的「Combinatorial Online Prediction」，該文提出一種線上預測演算法，藉由考慮組合概念的線上預測問題，包含s-t路徑、置換、真值分配、集合覆蓋等。線上預測算法的目標係使用事後結果，結合最佳固定組合概念競爭。在離線逼近算法保證完整性差距的情況下，該文提出一種更有效的線上預測算法，實驗結果亦證實該文提出方法具有較佳的預測結果。

二、圖論與網路模型編碼

圖論係指經由分析每個節點 (Node) 與邊 (Edge) 的關係，及節點與網路路徑的關係，如此可獲得該節點在網路中的重要程度及特性，判斷某一節點在網路的重要性主要係藉由計算其中心程度 (Centrality)，其中最常使用的幾項指標為度中心性 (Degree Centrality)、緊密中心性 (Closeness Centrality) 及連接中心性 (Betweenness Centrality)，節點間最短路徑的判別也被經常應用於網路傳輸之路徑選擇，本場次共發表4篇論文，學者分別來自印度、新加坡、日本等地。

第1篇文章為印度學者Niladri Das 及 Brijesh Kumar Rai所發表的「On

the Power of Vector Linear Network Coding」，文章中針對多個單傳播網路，當有限域的特徵屬於給定的有限或共有限的質數集時，具有速率1線性網路編碼解。該研究提出上述情形下的網路編碼一般解，可用於任何速率的線性網路編碼。具體的來說，作者證明對於任何非零正有理數 k/n ，若且唯若有限域的特徵給定時，存在具有速率 k/n 分數線性網路編碼解的多點傳送網路。

第2篇文章為新加坡學者Frederique Oggier、Silivanxay Phetsouvanh及Anwitaman Datta所發表的「Entropy-based Graph Clustering - A Simulated Annealing Approach」，文中主要針對複雜網路，提出以熵值（Entropy）為主的群體偵測方法，目的為預測彼此緊密通信的群組。群組形成主要具有相同主題或具有相同功能，文中所提出的方法可有效從複雜的大型網路中，判別形成群體的節點。

第3篇文章為日本學者Takafumi Nakano及Tadashi Wadayama所發表的「Analysis on Probabilistic Construction of Connected Dominating Sets over Regular Graph Ensembles」，文中係探討在資訊快速傳遞的社會中，通訊網路的穩定性是非常重要的，網路任一節點發生故障，均不能影響整個網路的訊息傳遞路徑。該篇文章利用機率模式，建構完整連線的網路結構，並將其應用於現今網路通訊的情境中。

第4篇文章為日本學者Satoshi Takabe及Tadashi Wadayama所發表的「k-connectivity of Random Graphs and Random Geometric Graphs in Node Fault Model」，文章中探討隨機圖的k-連通性的可靠度，為多結點的無線通訊網路（WSN）的基本屬性。WSN係由小功率電力且妥善度不佳的無線網路節點所組成，作者以k-連通隨機網路模型，模擬節點發生故障時，對通訊網路產生的影響，這被稱為節點故障模型。該研究通過評估網路故障概率，即特定節點移除後隨機圖的斷開概率，研究節點故障模型中隨機圖的k-連通性。

三、雲端鑑識

由警政署警政資安團隊成員，同時也是彰化縣警察局資訊科科長柯宏叡所報告的「Mobile Forensics for Cloud Storage Service on iOS Systems (適用於iOS系統的雲端行動鑑識研究)」為此場研討會少數獲錄取有關電腦鑑識的論文。雲端儲存服務已廣泛於全世界中被許多使用者所使用。雲端儲存服務可以虛擬化、去中心化，並能透過桌上型電腦或手機進行存取，為許多人所愛用。然而，雲端儲存服務對於傳統的電腦鑑識卻是一大挑戰，許多電腦鑑識的採證原則，在雲端儲存服務上就難以使用，例如為達精確的複製所需採用的字元串流拷貝 (bit stream copy)，要在雲端儲存服務上使用，就會有實際上難以執行的問題。後續的搜尋與分析，雲端儲存服務可提供的儲存空間遠遠高過一般個人電腦，若是採用傳統的搜尋方式，會相當曠日廢時。這篇論文就著眼於最受歡迎的三項雲端儲存服務：Google硬碟、Microsoft One Drive與Dropbox進行分析，並在目前知名的手機系統iOS上進行分析。試圖找出哪些殘餘資料可以被找出來，以及建議數位偵查人員可從哪些路徑與檔案下手找出重要的證據。

由於iOS擁有相當高的安全性，要直接在該系統進行採證有相當大的難度。在iOS系統上，有時會需要先使用「越獄」(Jailbreaking)軟體，如Pangu、Electra等來取得系統最高權限 (Root)，這麼一來就可在Cydia (類似Apple App store) 上取得可操作系統的工具軟體。在此篇論文中，主要針對Google硬碟進行實驗，找出相關的重要路徑 (如表1)，以及檔案在經過檢視、離線存取、檢視後刪除、共同編輯、分享等設定後是否能回復進行分析 (如表2)，其結果摘要如下。

表 1：Google 硬碟的重要路徑

路徑	說明
<i>Library/Caches/drivekit/users/ (number code) /images/</i>	JPD、PNG 縮圖 (Thumbnail)
<i>Documents/drivekit/users/ (number code) /files</i>	影像縮圖與檔案離線存取
<i>Documents/drivekit/users/ (number code) / thumbnails</i>	文件與影音縮圖
<i>Documents/drivekit/users/ (number code) /cello</i>	Metadata 檔
<i>Documents/drivekit/users/ (number code) /contacts</i>	Gmail 連絡人資料
<i>Documents/drivekit/users/ (number code) /logs</i>	系統紀錄
<i>tmp/drivekit/GDKGenoaContentProvider</i>	影像暫存檔

表 2：Google 硬碟中檔案的回復表

Google Drive																								
操作	JPG				PNG				DOCX				PDF				MP3				MP4			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
File viewed	○	○	-	-	○	○	-	-	-	○	○	○	○	○	○	○	○	-	○	○	-	-	-	-
No manipulation	○	○	-	-	○	○	-	-	T	-	T	T	T	T	T	T	-	-	-	-	-	-	-	-
File viewed and saved for offline accessed	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	-	○	○	○	○	○	○
File viewed and then deleted	○	○	-	-	○	○	-	-	T	-	T	-	T	T	T	T	-	-	-	-	-	-	-	-
File co-editor	○	○	-	-	○	○	-	-	T	T	-	T	T	T	T	T	-	-	-	-	-	-	-	-
File shared	○	○	-	-	○	○	-	-	T	T	-	T	T	T	T	T	-	-	-	-	-	-	-	-

圖示說明：1: 行動裝置啟動中；2: 行動裝置關機；3: 清除快取檔；4: Cache清除快取檔並關機；○: 有發現；T: 縮圖；- :未發現跡證

實驗中，可以見到影像有最佳的復原率（檔案復原的可能性最高），其次是PDF檔案。以檔案的狀態來看，將檔案以離線方式儲存時會有最佳的復原率，因為離線存取即將雲端上的檔案存到行動裝置上。現今常見的分享檔案進行編輯、分享檔案僅供檢視的功能，由實驗結果可發現若是這些檔案從未被檢視的話，幾乎難以回復。而若是這些檔案有先被使用者於行動裝置上檢視過，那麼就可能產生縮圖（Thumbnail）檔，由於縮圖檔為原檔案的精簡版本，故進行數位偵查時就可以此得到原檔案的部分相關訊息。

此外，在實驗中可發現不論行動裝置是否為關機狀態，對於取證並不會產生太大差異，這與一般電腦的取證就有很大的不同。然而若是清除快取（Cache）檔案則會嚴重影響資料的回復。此篇論文可以見到除電腦鑑識、手機鑑識外，還要能就雲端鑑識去加強，並針對iOS的系統深入了解，方能因應雲端運算與雲端儲存服務所帶來的挑戰。

四、區塊鏈

近幾年來，比特幣（Bitcoin）等虛擬加密貨幣（Cryptocurrency）獲得極大的關注，其價值的暴漲暴跌也吸引了許多投資者或投機者。所謂比特幣，是由化名為中本聰（Satoshi Nakamoto）的一位研究團隊於 2008 年提出的概念，目的在於提出一種電子貨幣，其發行不透過國家銀行，而是運用電腦系統資源去進行大量運算來產生，稱之為工作量證明（POW，Proof of Work），俗稱挖礦。而這種電子貨幣的交易，就必須依靠P2P網路來進行，另外為了確認雙方的交易，運用時戳與雜湊（Hashing）密碼建構出一套交易系統，也就是現今所稱的區塊鏈。

區塊鏈藉由運用密碼學技術來保護交易內容的串聯紀錄（又稱為區塊），每一區塊又包含前一個區塊的雜湊值、時間戳記及交易資料等等，這樣的設計使得區塊內容（交易紀錄）難以竄改，透過區塊鏈所串接起來的分散式帳本能讓交易雙方都有永久有效的交易紀錄，分散式帳本更可達到

去中心化，無需另外建置如憑證中心等系統亦可運作，也因此，想要竄改帳本的難度也會隨著使用者數而增加。雖然有不少人認為加密貨幣很可能是曇花一現，但是區塊鏈的產生，卻是被許多人視為是未來網路中最重要應用方式，因此就產生數種區塊鏈的應用：公有鏈、私有鏈與聯盟鏈。

(一) 公有鏈

公有鏈是比特幣的交易方式，所有人皆可參與，具去中心化的特質，所有參與者亦參與帳本紀錄，但是如此一來的交易效率也相當差。

(二) 私有鏈

相對於公有鏈，不具去中心化，著重於交易的安全性及效率，適用於大型組織的內部使用。

(三) 聯盟鏈

為了能兼顧與多方交易的效率，所以有了聯盟鏈。聯盟成員間建立起互信，協商交易所用密碼演算法與記帳方式，可適用於物流、銀行等產業。

透過不同的應用方式，可使得區塊鏈不只適用於加密貨幣的交易，更可延伸發展出如重要訊息的傳遞與防偽、數位產品如音樂的交易平臺等。原本的比特幣有交易效率差、匿名性不佳的問題，但隨著區塊鏈的應用日漸受到重視，愈來愈多人投入相關研究。為了能更好的應用區塊鏈的去中心化技術，2013年Vitalik Buterin提出以太坊（Ethereum），讓想要建立分散式應用的開發者，可以直接運用以太坊既有的資源來開發，而不需要自己從頭建立區塊鏈。以太坊最大的貢獻在於建立智慧型合約（Smart Contract）功能，這項功能可以協助雙方就合約進行談判和執行。銀行業有數十家組成了R3聯盟，參考區塊鏈的運作方式，另推出Corda分散式帳本系統，打算逐步建立起跨行清算系統。

2015年，LINUX基金會推出Hyperledger專案，以開放原始碼的方式加

強原有區塊鏈的安全性與擴展性，讓各個產業可以透過此一專案建立自己的區塊鏈系統。在Hyperledger專案中，Hyperledger Fabric是最為受到重視的項目，這是一個模組化的架構，可以進行類似以太坊智慧型合約的功能，在此稱為Chaincode，以及提供了建立 channel 的功能，可讓參與者為交易新建一個獨立的帳本。

由Yuto Ehara等人所發表的「How to generate transparent random numbers using blockchain」論文，討論網路遊戲、博奕娛樂網路應用程式，多是基於某些既定規則所產生的亂數結果。然而，我們無法檢驗這些既定的亂數是否正確，即我們無法相信這些亂數是否的確是依照既定規則所產生，還是會有人為的因素在內，導致產生的亂數無法給予公平的結果。該文認為亂數產生應具「透明性」。為了要能讓我們相信亂數是正確的產生，透明性是相當重要的。之前有Sako等人提出一種應用於遊戲「Backgammon」中的隨機亂數產生法，可以在遊戲結束後透過區塊鏈去檢驗亂數產生是否正確。然而這種方式，必須要先確認伺服器是可以信任的，不然若是該伺服器早已被入侵，亂數產生的正確性也會受到影響。在Yuto Ehara等人的論文中，他們提出一種透明隨機亂數產生方法，只要由少數可信任參與者透過公開區塊鏈操作，就可以取得隨機亂數。然而這個方式雖然解決可信任使用者的問題，但是在效能上卻是相當欠缺，因為這種方法使用的是POW與公開鏈技術，因此就會遇到這種技術的缺點，就是隨著參與者愈多，要產生隨機亂數的時間就愈久，若像是線上彩券則還可以適用，但若是線上博奕或是遊戲則可能難以使用。

在公用的區塊鏈上，POW需要大量的電腦資源進行運算，而在私有或聯盟區塊鏈則無需使用POW，因此可以加快交易速度，而且在聯盟鏈中的參與者不用擔心自己資料存在何處，自己產生的資料自己就可以看到，而唯有通過對方授權的密鑰才能看到其他參與者的資料，以此解決隱私和安全性問題，並同時能夠實現部分去中心化。而在Ken Naganuma等人的論文

「Decentralized Netting Protocol over Consortium Blockchain」中，Ken Naganuma等人提出一種基於聯盟方式的區塊鏈去中心化網路協定。作者宣稱透過此協定可以P2P方式進行雙方的金融交易，計算淨額，且無須建立中心組織來運行。

在Ken Naganuma等人的論文中，作者提出使用Hyperledger Fabric的channel功能來達到去中心化的結算協定，這就是一種聯盟鏈的運用。運用channel的功能，交易訊息的發送端與接受端，就可以隱藏交易金額的部分。另外，這篇論文中所提出的協定可以無須建立集中的系統，可以直接透過P2P來運行。然而，這篇論文所提到的協定尚無法排除聯盟鏈中惡意節點的存在。區塊鏈近來在國內快速發展，不少單位已將區塊鏈視為未來交易方式之一，然而由此次研究會研究者所提的論文中，我們也可以發現安全機制尚不完備，未來若要偵辦相關的案件，需要進一步投注相關資源於區塊鏈的研究上。

五、數位浮水印

在往畫家或出版公司要保護自己作品的智慧財產權時，便會在作品上加上簽名象徵其出處，若是要去除其簽名，會很容易損傷到作品本身。數位媒體如電子書、電子影像、聲音等的特性就在於易於複製，修改、變造還能與原件差異極小。這是數位媒體在運用上的優點，使得我們容易藉由操作相關工具程式來編輯數位媒體以達到我們的需求，但這卻也是在保護數位媒體上所必須面臨的問題。因此，要如何保護數位媒體的難度比以往的保護方法要來得高。這不僅是要求加上簽名後不能影響作品本身，還要能達到所嵌入的所有權的資訊在移轉的過程中還要能鑑定出正確的擁有者；經過一般通訊過濾處理仍不遭受破壞的影響，並能避免惡意攻擊者嵌入不同的所有權資訊所引發的爭議，此乃一大挑戰。3D物件與其他的多媒體如聲音、影像等最大的不同在於：其他的多媒體資料是屬於規則排列，而3D物件的資料則多是不規則排列。如影像是屬於二維的規則排列資

料，但是3D物件則是三維的不規則排列資料，因此要嵌入浮水印到3D物件中的方法也會相當不同。

一個強健的浮水印隱藏技術的要求包含透明性 (Transparency)、強韌性 (Robustness)、安全性 (Security)、忘卻性 (Oblivious)、多浮水印 (Multiple Watermarking)、明確性 (Unambiguity) 等條件，以下將針對使用影像圖來製作含浮水印圖樣保護的影像圖 (以下簡稱保護圖)，分別敘述如下：

(一) 透明性

透明性是製作浮水印最基本的要求就是當透過人眼視覺檢視時，無法辨別區分出有何不同。換句話說，保護圖讓人感覺其與原圖幾乎是一模一樣的圖，不會引起任何的懷疑，即無法察覺 (imperceptible)。

(二) 強韌性

多媒體檔案常常會為了傳輸或儲存等目的而進行轉換、壓縮等處理。所以受保護的檔案必須要有足夠強韌度來抵抗格式轉換、壓縮等，還要能萃取出所隱藏的資訊。然而相對於強韌性浮水印，尚有脆弱型 (Fragile) 浮水印，用以偵測多媒體檔案是否曾遭受攻擊，就可以知道該檔案是否完整。

(三) 安全性

浮水印技術的安全性考量，通常著重在原圖的特定區域。在實際的運作上，亦是經由這些所選取的特定區域來找到嵌入隱藏其中的浮水印資料。在此種模式中，被攻擊者推測出浮水印資料所嵌入的區域的可能性必須要低。同時也不允許沒有權限的人任意移除或竄改嵌在其中的浮水印資料。一般來說，安全性是常藉由使用虛擬隨機亂數產生器 (Pseudo-random Generator)，透過一個種子金鑰 (Seed Key) 產生一堆的隨機亂數來完成。當然，在浮水印系統中，只有合法擁有者才知道種子金鑰，也唯有使用正確的種子金鑰，才能真正獲得嵌入的機密訊息。

(四) 忘卻性

所謂非忘卻 (Non-Oblivious) 的浮水印技術是當針對已含有浮水印保護的媒體做萃取浮水印的動作時，需要參考到原始媒體，透過原始媒體的協助，才能順利的萃取出浮水印，但如此一來就需另外空間保留原圖，反而不便。

(五) 明確性

萃取出來的訊息必須具備明確性 (Unambiguity)。浮水印技術應用的主要目的是針對多媒體所有權的鑑別、為所有者的權益提供保障，因此萃取出來的訊息必須要能被識別，常見的評估方式為NC (Normalized Correlation) 或BER (Bit Error Rate)。

由Hiroshi Yamamoto等人所發表的「A Watermarking Method for Embedding into the External Shapes of Objects」論文中提到，近年來低成本3D列印快速發展，使得一般使用者也能負擔。攻擊者要進行3D物件的複製也變得相對容易，只要攻擊者取得圖形資料如設計圖或藍圖，就能透過3D列印技術快速重製相同的產品出來。因此也有愈來愈多的研究著眼於如何在3D的物件中嵌入數位浮水印來防偽。在3D物件中，若是直接將訊息嵌入於物件內部的話，攻擊者將會很容易的進行去除，且不會造成物件變形，或是僅就外形進行複製即可。因此較常用的方法是將訊息嵌入於3D物件的端點 (Vertices)，透過建立軸線與計算頂點座標相對位置來將浮水印或訊息嵌入，以達到防偽的目的。由Hiroshi Yamamoto等人提出的論文中，作者提出一種方法可將訊息嵌入物件的外型。意圖複製的攻擊者無法在不改變外型下來改變嵌入的訊息。所使用的方法在於建立3D物件的偽旋轉軸與切割平面，將訊息藏在與軸線交錯的區域半徑內。經由實驗，可知道這種方法能在不明顯改變3D物件的外形下將訊息嵌入。不過這項技術在於抵抗壓縮等攻擊手法上並未有著墨之處，嵌入與萃取出來的浮水印也未有進一步說明，有不足之處。

六、視覺密碼學

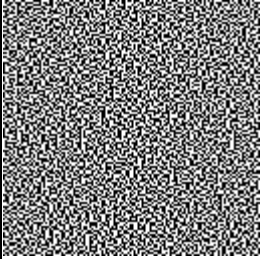
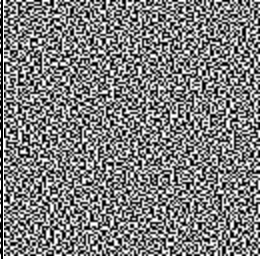
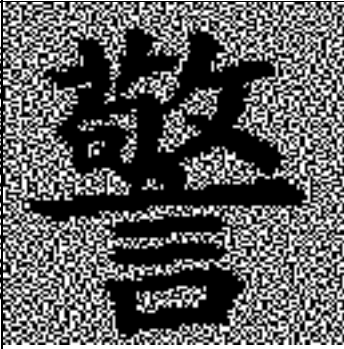
視覺密碼學主要是依據人類視覺系統對於影像色差的反應，賦予影像意義。類似於進行色盲檢測時所用的卡片，即為以人眼視覺的反應來判斷是否有具有意義的訊息包含在雜色點中。視覺密碼學解決了傳統密碼學在解密過程中需要大量複雜的計算過程，在安全性上，同樣可以確保竊取資料者無法從這些個別的分享影像（或稱為子圖）中，察覺出機密影像的輪廓，如圖所示，因此這種機制在密碼學上又可稱之為「秘密分享（Secret Sharing）」。使用視覺密碼學方法的優點就在於，可使得電腦系統與使用者雙方所持有的資訊都是無意義的圖形，但唯有在正確的組合之下，才會是有意義的訊息。這樣的方式就會使得有意進行攻擊或入侵者必須同時取得雙方的資訊方可成功，便能有效提高系統的安全程度。但是此法的缺點就是因為影像所佔的磁碟儲存空間遠比文字來得大，所以需要更多的儲存空間來容納。如果真要達到完全秘密分享的機制的話，日後管理者就不易取消特定單一使用者的權限。

視覺密碼學由要隱藏的原圖中產生兩張黑白交錯的圖，稱之為子圖（share），兩張子圖單獨看是沒意義的，唯有疊在一起才可見到原本隱藏的原圖為何。然而為了將原圖的每個像素進行編碼隱藏，就得使用擴展的方式來進行，如表3與表4。

表 3 子圖編碼重疊示意圖

影像	機密影像（白）	機密影像（黑）
子圖一		
子圖二		
疊合結果		

表 4 子圖資訊隱藏範例

原圖	子圖一	子圖二	疊合結果
警言			

視覺密碼學的進一步發展就是 (t, n) 秘密分享，意即產生 n 張子圖，要取得 t 張以上的子圖才能得知原圖。在 Koutaro Okada 與 Hiroki Koga 所發表的“A Construction of the $(4, n)$ -Threshold Visual Cryptography Scheme Using a 3-Design”這篇論文中，是以 θ 代替 t ，以 (θ, n) -VCS 表示此種視覺密碼學。

Okada & Koga 所發表的這篇論文中，主要是透過建立基本的矩陣，也就是由 0 與 1 組成的子圖，以及設計出 t -Design 的架構進行驗證，因而得到在 $(4, n)$ -VCS 使用 3-design 的話，可以減少像素的擴展。其想法來自同一作者於 2017 年於 IEEE ITW 2017 研討會上所發表的“A Construction of the Progressive $(3, n)$ Threshold Visual Cryptography Using a BIBD and Analysis of Its Optimality”的研究，Okada & Koga 等人已就 $(2, n)$ -VCS 與 $(3, n)$ VCS 運用 Hadamard 矩陣來設計出 BIBD (balanced incomplete block design)，以此推算出最少需要的像素擴展，不過根據作者的評估，這樣的推算還沒辦法證明已為最佳解，不過已能推估出相對最小所需像素擴展的值，使未來在評估圖像所需空間上可以更加明確。



圖 1 議程報告者合影



圖 2 議事會場提問



圖 3 論文發表



圖 4 議事會場提問



圖 5 作者與議程主席合影



圖 6 作者與國際學者研討

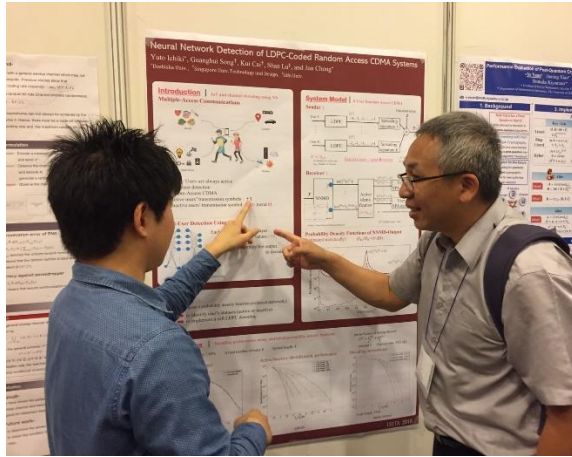


圖 7 作者與日本學者研討



圖 8 參加主辦單位晚宴與國際學者交流

參、與會心得及建議

一、與會心得

(一) 反思研究方向

藉由與全球相同領域的專家學者們密集的研討，可反思自身研發方向，瞭解目前該領域中的主流研究方法，以提升研究實力。國際研討會是各國專家學者相互交流的平臺，除能接觸多元廣泛的議程，在與各國專家學者交流與討論中，可增進資訊通訊技術交流，更能擴展本身研究的廣度，讓與會的國際學者認識國內的研究發展方向。透過本次研討會與國際接軌，有助於本校培育資通訊人才，透過人際網路的連結，將國外先進、優秀的資訊通訊技術，列為為我國未來科技交流之參考，後續更可進一步擴展為國際性的發展合作，為本校研究奠定良好的發展方向。

(二) 持續推廣英文學習環境

本次研討會上臺以英文口頭報告，加上議程中與外籍學者專家溝通的經驗，讓作者深深體會國際化語文的重要性。鑑於近年來警政學術研究蓬勃發展，世界各國均投注大量資源，找尋最新的勤務運作或犯罪偵查策略，所以與其它國家的警務交流，也日趨重要。藉由參考他單位的做法，不僅可作為自身規劃政策的依據，更可在現有的研究之上，針對國內的環境，發展屬於自己的警政策略。然而這一切皆必須具備與全世界溝通的語言

能力。本校學生採集中式管理，於校內生活的時間，相較於其它大專院校明顯較多，目前校內已有多項強化英文生活教育的措施，可在現有機制的良好基礎下，持續塑造良好英文學習環境，以提升全體師生之國際競爭力。

二、建議事項

(一) 強化校際交流，持續鼓勵或經費支持學生參加國際研討會

本次與會的專家學者多來自全球頂尖的大專院校，顯示各國對於資通訊人才培育，均投入相當程度的資源。為厚植本校研究發展實力，利用各項機會與全球優秀人才交流，實為創造本校能見度的重要管道。建議本校持續鼓勵或經費支持校內優秀學生參加類似國際研討會，不僅能開拓國際視野，更能與各大專院校建立友誼。本校目前已與許多國內外研究機構簽訂合作備忘錄，期望能藉由不斷參加國際聚會所累積的能量，幫助學校擴展更多元的校際交流。在資訊高度流通的時代趨勢下，不積極參與國際活動，亦將被世界遺忘。本校為國內唯一培養警察幹部的學術單位，建議持續把握代表國家參與國際警務交流的機會，經由不斷學習與成長，激發不同想法，進而培養各項創新知識，最後將實務與理論層面相互結合運用，達到深化警學研究的目標。

(二) 熟悉工具軟體的應用，持續維護警政相關之專業資通訊實驗室

中央警察大學面對此一資通訊挑戰，已逐步調整課程架構，建置數位鑑識研究中心，普設電腦犯罪偵查實驗室、治安與情報資訊分析實驗室、多媒體鑑識實驗室、情資安全與鑑識科學實驗室運作計畫、資通安全與網路鑑識實驗室、雲端計算實驗室、警政資訊與科學決策實驗室及數位鑑識實驗室等不同類型實驗室，增購諸多鑑識器材，配置專業師資，從事網路犯罪調查及數位證據蒐集分析之相關教學演練，期具備必要軟硬體設備，方便管理、運用、研究及教學，已有相當成效。使本校學生畢業前在學期間能透過實驗室軟硬體設備，了解電腦犯罪原理、犯罪手法，熟悉實務機

關所使用之偵查工具，畢業後即能運用此科技偵查工具投入電腦犯罪偵查工作，縮短摸索與適應期。在習得相關工具應用技術之後，也著墨於工具背後的原理原則，使本校學生不僅僅能夠使用工具，也得以增進將來自行編撰程式碼研發自動化程式工具的可能。未來，亦須持續更新購置網路犯罪偵查或鑑識的工具軟體，於教學課程使用，解決人員與未來實務遭遇相關案件時，對偵查軟體使用上的不熟悉。作為執法人員，為求證據的合法性及完整性，寄望未來於犯罪現場取證時，得以保有事實真相，更進一步推演犯罪模式及犯罪手法，將犯嫌繩之以法，保衛司法的公平正義。