

2020 年第 23 屆資訊管理學術暨
警政資訊實務研討會
——「網路犯罪與跨域資安治理」

論文集

時間：2020 年 11 月 30 日

目 錄

大會組織.....	II
序言.....	III
1 應用可解釋性深度卷積網路於單一樣本的簽名驗證方法 (高信雄、溫哲彥、張凱評).....	01
2 電商退款圖像取證的探討與應用-以 EMD 訊息嵌入法為例 (梁羽涵、楊佩瑜、林鈺烽、洪維恩)	09
3 警車即時影像及定位導航視訊系統在攔截圍捕上的應用 (古淳寶、董正談、鄧少華)	14
4 5G 結合車聯網在交通事故現場重建上的應用(王逸嵐、董正談、鄧少華)..	24
5 現場拍攝取證文字辨識特徵實證研究：以 Google Keep 為例 (郭冠呈、吳國清)	34
6 社群媒體網站鑑識效率之比較分析：以 Facebook 為例(黃蘭萱、王朝煌)..	45
7 治安監錄攝影機畫面偏移異常自動偵測：以桃園市警用監視錄影系統為例 (蕭天佑、顏志平、林曾祥)	53
8 政府組態基準(GCB)推動實務-以彰化縣警察局為例(劉立偉、吳俊德).....	63
9 面對 DeepFake 如何維護機關資訊安全(吳俊德、李瑋晟)	68
10 網路通信紀錄分析於犯罪偵查之應用(劉韻慈、鄧少華、董正談).....	73
11 應用於犯罪現場之帳密取證與特徵分析實證研究(許庭于、吳國清).....	82

**2020 年第 23 屆資訊管理學術暨
警政資訊實務研討會
——「網路犯罪與跨域資安治理」
大會組織**

大會主席：

黎校長文明

大會副主席：

莊副校長德森

籌備及議程委員會主席：

黃主任勝源

廖主任有祿

籌備委員：

黃主任勝源、廖主任有祿、王教授朝煌

吳教授國清、鄧教授少華、王教授旭正

林教授曾祥、高副教授大宇、顏副教授志平

董助理教授正談

執行秘書：

簡助教羚茜

序 言

本校與內政部警政署為促進資訊管理學術與警政資訊實務之交流，結合資訊管理學術與警察資訊實務工作，期經由警察資訊應用技術的開發來提昇警察工作效能，進而促使警察能夠採取更經濟有效的方法來服務社會。為具體落實此項目標，本校定期舉辦資訊管理學術暨警政資訊實務研討會，期能藉由舉辦研討會交流學術研究成果與實務經驗智慧，共同研討尋求解決方案。此外有鑒於資訊科技不斷地創新應用與發展，資訊科技不但已經成為現代化社會、生活與工作的必備利器，更讓我們能夠突破時空的侷限來進行過去無法完成的事項；而社會環境不斷地變遷，對於警察角色的定位也有所轉變，已經從法律與治安的維護者，擴大為社會與民眾的服務者，因此如何整合並運用資通訊科技來維護治安與打擊犯罪，並以創新的思維來面對警察工作的挑戰已成為迫切的課題。本次研討會主題為「網路犯罪與跨域資安治理」，相信在各位作者的熱情參與下，對於警察資訊人員如何以創新的思維跟上時代的脈動並順利完成各項警察工作，將會有更宏觀的認識與啟發。

論文發表部份，本屆研討會因疫情關係，改為線上發表方式，總計刊登 11 篇文章，分別探討「應用可解釋性深度卷積網路於單一樣本的簽名驗證方法」、「電商退款圖像取證的探討與應用-以 EMD 訊息嵌入法為例」、「警車即時影像及定位導航視訊系統在攔截圍捕上的應用」、「5G 結合車聯網在交通事故現場重建上的應用」、「現場拍攝取證文字辨識特徵實證研究：以 Google Keep 為例」、「社群媒體網站鑑識效率之比較分析：以 Facebook 為例」、「治安監錄攝影機畫面偏移異常自動偵測：以桃園市警用監視錄影系統為例」、「政府組態基準(GCB)推動實務-以彰化縣警察局為例」、「面對 DeepFake 如何維護機關資訊安全」、「網路通信紀錄分析於犯罪偵查之應用」、「應用於犯罪現場之帳密取證與特徵分析實證研究」，涵蓋學術與實務領域，契合本研討會之宗旨。

本屆研討會得以順利舉辦，首先要感謝黎校長、莊副校長、林院長以及各級長官的鼎力支持與協助，為資訊管理學系添購各項軟硬體設備，並充實教學與研究環境，其次感謝本系所有教師以及學校各單位同仁通力合作共襄盛舉，並感謝本系簡羚茜助教及所有在幕後任勞任怨付出與幫忙的所有審查委員們，最後感謝各位先進、前輩、校友以及警界同仁的熱情參與，希望藉由大家的參與交流集思廣益，能夠進一步提昇國內資訊管理學術與警政資訊實務的發展與研究水準。

中央警察大學資訊管理學系主任廖有祿敬序

中華民國 109 年 11 月 5 日

應用可解釋性深度卷積網路於單一樣本的簽名驗證方法

高信雄

刑事警察局科技犯罪防制中心 偵查正

k@email.cib.gov.tw

溫哲彥

中央警察大學鑑識科學學系暨研究所 教授

cwen@mail.cpu.edu.tw

張凱評

刑事警察局刑事鑑識中心 技士

fs731235@email.cib.gov.tw

摘要

簽名驗證是最常用的識別技術之一，並廣泛應用於各式法律及商務用途。由於目前在實務上進行簽名驗證的工作是以人工為主，如何應用科技的方式提高驗證的效能，成為重要的課題。近年來，具可解釋性的深度學習研究已成為重要的領域，也應用於生物特徵的輔助比對。本文提出基於深度卷積網路(DCNN)的方法，以中、外文簽名為實驗樣本，透過單一參考樣本進行簽名驗證並提供量化的判斷結果，亦可做為鑑識輔助系統，藉由視覺化的熱點圖協助鑑定人員識別簽名中的筆跡真偽。

關鍵字:手寫簽名驗證、卷積神經網路(CNN)、深度學習、可解釋性AI (XAI)

Abstract

Signature verification is one of important biometric techniques for personal identification, and has been widely used for legal and various commercial purposes. In practice, most signature verification works are processed by visual examination. And, we need a certain number (more than one) signature samples to accomplish our examination. Recently, deep learning based methods have been shown as useful tools for identification. In this paper, we propose a method based on the deep convolutional neural network (DCNN) and single reference sample. We use actual Chinese and foreign signatures to provide quantitative results for handwritten signature verification. The proposed method can also be used as an assistant system for forensics by identifying genuine or suspicious strokes through the visualized saliency maps.

Keywords: handwritten signature verification, convolutional neural network (CNN), deep learning, explainable artificial intelligence (XAI)

一、前言

簽名驗證在人類社會的運用存在已久，至少在數百年來已廣泛應用於商業，法律和其他日常文件中，並且時至今日仍是最常見的生物識別技術之一。隨著資訊技術的發展，為了進一步提升驗證的效率與可靠性，自動化的簽名驗證技術已經發展了數十年，特別是近年崛起的深度學習技術，通過擴展網路層的深度、規模和複雜性，改善了傳統人工神經網路的各種不足，被視為是人工智慧領域最大的突破之一。這使得深度學習成為瞭解影像識別問題(包含簽名驗證)的絕佳方法。

儘管學界對於自動簽名驗證已有廣泛的研究基礎，但大多數基於深度學習的驗證方法，仍需依賴大量的真實簽名樣本來進行特徵擷取或模型訓練，而這勢必降低了其實用性。舉例來說，在許多日常應用場景中：如銀行業務、支票付款等，簽名驗證的流程皆是基於單一已知樣本的人工查核，導致多數的簽名方法無從適用。除了前述的單一樣本問題外，本文另針對以下3個關乎實用性的議題進行探討。

首先，自動化簽名驗證的應用因種種法律或技術因素，至今尚未用於司法鑑定及大多數的金融業務中，實務上主要仍仰賴人類

專家或從業人員的人工識別。而歸結其主要原因，便是由於大多數深度學習的決策結果是不透明的(也可稱為缺乏可解釋性)，並且也幾乎無法與人類專家協作，難以確保用於司法、大額交易等嚴謹用途的可接受度。為此，本研究的主要目的之一是通過視覺化解釋技術來增強自動化簽名驗證方法的可解釋性。

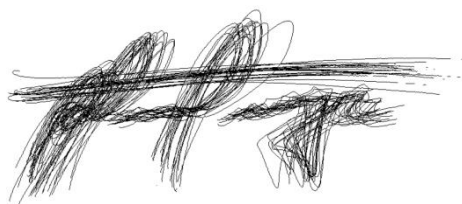
再者，即使僅考量司法用途的簽名鑑識，也並非所有的案件都能直接進入實驗室等級的鑑定程序。以刑事警察局的鑑定流程為例，鑑識人員需要收集足夠的已知樣本，始能準確地執行鑑定工作，其收集來源包括：犯罪現場、調閱日常文書、鑑定對象於法庭書寫的庭書字跡等。然而，這些額外的樣本雖能保障鑑識結果的可靠性，卻也大幅提高了簽名鑑定的門檻與時間成本。在更多的情況下，前線的執法人員很難在第一時間內收集到足夠的樣本數量。此時我們的方法便可用於案件處於初步調查階段時，幫助執法人員快速評估簽名的真實性。

最後，現行以專家為主體的筆跡鑑識方法在相當程度上仍需依賴專家本身的知識及經驗。而本研究的方法可以輔助人類專家或金融從業人員進行鑑定，並同時提供視覺化的輔助及量化結果的建議，以減輕從業人員負擔。

二、相關研究

1. 自動化簽名驗證

相較於其他常見的生物辨識技術，諸如：虹膜、指紋、臉型及DNA等，手寫簽名具有較低的組間變異(inter-class variance)，例如偽造的簽名可能與真實簽名十分相近。同時手寫簽名亦具有較高的組內變異(intra-class variance)，代表即使是同一書寫者的字跡，也可能會存在明顯的差異，這也是為何筆跡鑑識專家會需要收集多個已知簽名樣本，其主要目的便是釐清由組內變異所呈現的筆跡自然變化，如圖一所示。



圖一：簽名的自然變化，摘自[1]

基於以上原因，儘管手寫簽名已廣泛用於個人身分驗證且行之有年，但至今仍然是生物識別技術中最具挑戰性的難題之一。

特徵擷取是自動化簽名驗證技術中最關鍵的環節，依據近年多篇回顧型論文的彙整[2-5]，現行主流的特徵擷取方法大致可分為兩類：「人工定義特徵」和「自動化特徵學習方法」。前者主要基於專家或研究人員的主觀認知來設計特徵擷取器，最常見的方法為透過精心設計的傅立葉轉換(Fourier Transform)或小波轉換(Wavelet Transform)程序，來擷取筆跡特徵。另一方面，後者(特徵學習方法)則是讓系統自主學習特徵，而無需人工干預。此類方法在近年主要以深度學習為主，特別是其中的卷積神經網路(Convolutional Neural Network, CNN)，被視為影像處理領域最有發展潛力的技術之一，因而也被廣泛使用於簽名辨識的研究。例如Khalajzadeh等人[6]以CNN方法直接從簽名圖片的像素中學習特徵，以分類不同作者的簽名。另Hafemann等人[7]更進一步提出了藉由CNN從不同大小的簽名中擷取穩定特徵的方法。

2. 基於單一簽名的鑑定

基於深度學習的方法已在影像辨識、紋理分析等領域取得了重大的突破，但仍需依賴大量(乃至於巨量)的訓練樣本來確保其強大的效能，而這無疑限制了此類方法的實用性。特別是在簽名驗證的應用場景中，更多的樣本需求意味著更高的實施門檻，況且實務上通常難以取得如此大量的真實簽名樣本，例如：在商業使用上，通常僅靠客戶留存的單一樣本進行比對。基於這些原因，近年來，使用小樣本進行深度學習的想法受到了廣泛關注，但大多數方法仍需要多個已知的真實簽名樣本來訓練網路[2-5]。Bouamra等人[8]嘗試通過少量的真實簽名樣本，以單類向量機(One-Class Support Vector Machine, OC-SVM)的方法訓練模型並用以偵測偽造簽名。另Adamskie[9]更是僅採用了單一參考樣本，透過人工定義特徵的方式，先將簽名字跡轉化為1個像素寬的線條型態，並從中擷取向量特徵，可惜該方法僅能做到區分不同姓名的簽名(僅簽名分類)，尚無法做到偵測偽造簽名的地步。

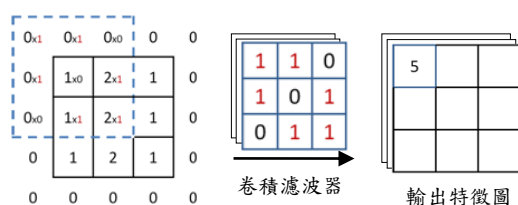
3. CNN

卷積神經網路(CNN) [10]是深度學習網路的一個分支，並且已在許多影像處理及電腦視覺的應用中表現突出。一些研究人員聲稱他們的CNN方法在圖像識別領域已可達到人工等級[11]，甚至超越人類水準的辨識效能[12-14]。

CNN架構通常由三個主要類型的網路元件組成：卷積層(Convolutional layer)、池化層(Pooling layer)和全連接層(Fully-connected layer)。全連接層即是傳統用於分類任務的神經網路，在此不做贅述，以下僅重點介紹卷積層和池化層兩種用於擷取特徵的關鍵結構。

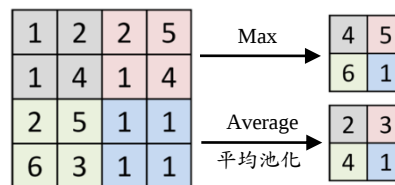
每個卷積層包含多組卷積濾波器(filter) [10]，或稱卷積核(kernel)，用以從底層資訊中擷取更高階(抽象)的紋理特徵。以本研究的簽名驗證工作為例，卷積濾波器可以從原始簽名圖像中逐漸擷取到筆劃的邊緣、轉折、連接點，甚至是其他更抽象的特徵(例如運筆速度、不自然停筆、抖動等)。

卷積濾波器的原理為類似圖片遮罩(Mask)的概念，可以看作是在整體圖像上滑動的窗口。將滑動區域的像素乘以濾波器的數值，藉此輸出新的像素特徵。另外，為了防止濾波器與原始圖片的邊緣覆蓋不完全，常將原圖的邊緣以像素值0填充，稱為zero padding。卷積濾波器的運作舉例如圖二。



圖二: 卷積濾波器示意圖[15]

CNN的另一個重要部分是池化層[16]。由於前述卷積層擔任上一層(輸入層)的特徵產生器，輸出了大量的特徵圖(Feature Map)。而這些輸出特徵又將成為下一層網路的輸入層，如此反覆操作下，造成特徵圖的數量急劇增長，造成極大的運算成本。因此，為了避免系統消耗過多的運算資源，CNN採用池化方法來縮減特徵圖的大小，進而更快的收斂網路訓練結果，並提供更好性能。在本文中，我們使用2種不同類型的池化層：最大池化層(Max-Pooling)和平均池化層(Average-Pooling)，其運作方式如圖三所示



圖三: 池化層(2x2 filter)示意圖

由圖三可以明顯看出最大池化和平均池化之間的差異。理論上最大池化可以減少背景雜訊並擷取到最重要的紋理特徵，但同時對原始資訊的破壞程度較大。相較而言，平均池化擷取的特徵更加平滑，可將較多的原始資訊傳遞到下一層網路，此舉特別有利於較深層的網路，藉此擷取到更高階的抽象特徵。

三、實驗方法

本研究的開發環境使用Python 3.6及Pillow 5.0進行影像處理，並基於深度學習框架TensorFlow 1.7和Keras 2.1來構建我們的網路。硬體配備為Intel Core i7-4790 CPU(8-Core,4 GHz,8M)和12 GB RAM的PC。

1. 單一樣本的簽名驗證策略

如第2.1節所述，手寫簽名驗證最大的困難就是同一位書寫者的簽名間具有較高的組內變異，而通常解決的方法(無論是深度學習或人類專家鑑定)就是添加足夠的參考樣本，透過機器學習或人工歸納的方式，盡可能消除組內變異的不利影響。惟本研究處理的是單一參考樣本這種極端狀況，爰提出以下3種策略來解決樣本不足的問題。

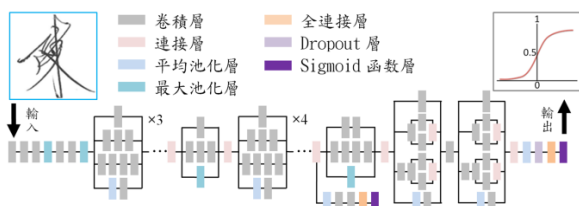
- (1) 首先我們要釐清簽名樣本不足並不等於筆跡特徵不足，這取決於有無足夠的手段從有限樣本中擷取出更多的可用特徵。我們先大膽假設在單一簽名內其實存在許多有用的局部特徵，例如：筆劃線條、起點、頓點、轉折處、運筆品質等特徵，這些局部特徵遍佈在整個簽名圖像上並在簽名驗證中起著重要作用。為此我們設計了特有的局部特徵擷取方法，將單個簽名圖像轉換為多個相互重疊的圖像區塊，讓系統著重於驗證局部圖像區塊(而非其他研究常使用的整體簽名)。此外，再配合一些深度學習常用的數據擴增技術，如此擴展後的樣本數量

基本已能符合CNN的訓練需求，更多細節將在第3.4節中說明。

- (2) 由於我們正在處理的是典型的二元分類問題(辨別真偽)，因此即使真實簽名的特徵不足，亦可採用反向策略，即提供更多的偽造簽名樣本讓CNN系統學習何謂偽造的簽名。幸運的是，偽造簽名的樣本實務上相對容易獲得(可以通過人為模仿或演算法生成)。在往後的章節中，我們將使用實驗數據來證明透過更多偽造簽名樣本訓練後的CNN模型，確實能學到更多普遍存在於「不同簽名」和「不同作者」中的偽造特徵(即與作者無關且通用型的特徵)，例如：筆跡的不自然的顫抖、筆速停滯等。
- (3) 為了更進一步增強本方法的可靠性，我們以視覺化技術呈現CNN模型的決策過程，一方面檢驗辨識的過程是否合理；另一方面，視覺化的呈現結果更容易與人類專家或其他簽名鑑定從業人員協作，並可藉此提供更好的證明力及可接收度。視覺化的細節將在之後的章節中詳細說明。

2. 網路架構

本研究使用Inception V3網路結構[17]。Inception V3是Google研究團隊開發的深度卷積神經網路(DCNN)架構，且已在ImageNet大規模視覺辨識競賽中展現了極為出色的性能[13]。其架構包含卷積層、池化層、dropout層、全連接層和sigmoid函數層，如圖四所示。



圖四: Inception V3網路架構[18]

在圖四中，卷積層和池化層負責特徵擷取工作；連結層合併來自前一層的多組數據；全連接層基本與傳統類神經網路的多層感知器(Multilayer Perceptron, MLP)相同，用於分類任務；在dropout層中，50%的感知器在訓練過程中會被隨機忽略，該技術被廣泛用於防止神經網路過度擬合(overfitting)。

最後，我們使用sigmoid函數作為輸出層來處理二進制分類問題。該函數會生成一條S形曲線，其值介於0到1之間，可以定義如下：

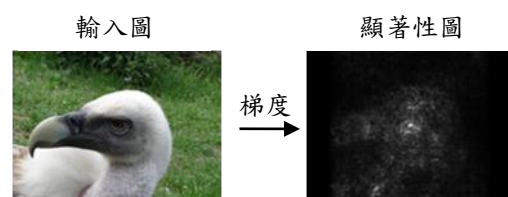
$$\text{Sigmoid}(x) = p = \frac{1}{1 + e^{-x}} \quad (1)$$

在本研究中sigmoid層的輸出值可以表示系統判定輸入資訊為真實簽名的概率 p ，由此類推，偽造簽名的概率即為 $1-p$ 。

3. 可解釋性深度學習

儘管深度學習已在各個領域都表現出了卓越的性能，但由於這些方法普遍缺乏可解釋性，這種被歸類為黑盒子(black box)類型的運作方式，使得它們難以被運用在司法鑑定、財產處分等關乎個人重大權益的領域。因此，近年來可解釋性的深度學習方法(Explainable Deep Learning)或稱可解釋人工智慧(Explainable Artificial Intelligence, XAI)受到了越來越多的關注。

在電腦視覺領域方面，Simonyan等人[19]提出了一種基於梯度(gradient)顯著性的視覺化方法，並特別適合用於可視覺化神經網路的決策過程。其主要概念是對於那些在神經網路預測過程中造成影響的像素，個別標注其梯度上的變化。最後，藉由圖示化這些標記結果產生網路的顯著性圖(saliency map)，如圖五所示，其結果可以檢查網路的決策過程是否合理，或是否符合人類的認知。



圖五: CNN識別鳥類的顯著性圖[19]

4. 資料蒐集與前處理

本研究所使用的英文簽名樣本主要來自ICDAR 2011 SigComp資料集[20]，中文簽名樣本則是實際收集自1位真實作者和4位偽造者，每位偽造者通過模仿真實作者的第1筆簽名(同時也是唯一用於網路訓練的已知真實簽名)產出4筆偽造簽名。所有中文簽名均使用相同的黑色圓珠筆(0.5mm)書寫在A4白紙上，以Canon UFR II掃描器600 dpi的解析度掃描後存成8-bit灰階圖。

接著進行資料前處理的步驟主要包含：

(1)調高圖片亮度(像素RGB值 $\times 1.075$)以除去掃描器背景雜訊及紙張紋理。(2)每格20像素將原簽名切割為 299×299 大小且互相重疊的局部圖像區塊。(3)以10至60度的角度，多次旋轉子圖像區塊，以確保旋轉不變性(rotational invariance)及進一步擴增樣本數。(4)篩選具備足夠筆劃像素(灰階像素)的圖像區塊組成訓練、驗證、測試資料集。相關細節可參照我們之前的研究[21]。

5. 實驗設計及網路訓練

實驗設計和網路訓練的內容主要承接自我們之前的研究[21]。其目在於驗證本文於3.1章提出的假設：即本文提出的訓練策略能在單一已知(真實)樣本的極端情況下，讓系統透過更多的偽造樣本學習到足以分辨簽名真偽的有用特徵。為此，我們以SigComp資料集中偽造簽名數量最多的簽名(編號14及16)做為實驗對象。然後為這2組簽名各安排了3種不同大小的偽造樣本數做為對照實驗共，共進行了6組實驗。

每組實驗都再細分為：訓練、驗證、測試3個階段。訓練階段僅用單一真實樣本訓練網路；驗證階段用相同作者的不同簽名檢驗訓練成果；最後的測試階段則是以全新作者評估網路實際效能(包含正確率、型I及型II錯誤等)。前述每一階段的樣本只在該階段中使用，此外為求慎重，測試階段僅採用全新的偽造作者(未曾出現在網路的訓練及驗證階段)，以確保CNN模型的可靠性，詳如表1所示。

表一：實驗樣本設計

實驗對象	組別	實驗編號	實驗階段	真實簽名編號	偽造簽名編號			
					作者1	作者2	作者3	作者4
簽名14 (實驗1-3) / 簽名16 (實驗4-6)	控制組	1/4	訓練	No.1	No.1,2	No.1,2	No.1,2	
			驗證	No.2-4	No.3,4	No.3,4	No.3,4	
			測試	No.5-8	No. 1-4			
	實驗組	2/5	訓練	No.1	No.1,2	No.1,2		
			驗證	No.2-4	No.3,4	No.3,4		
			測試	No.5-8	No. 1-4			
	實驗組	3/6	訓練	No.1	No.1,2			
			驗證	No.2-4	No.3,4			
			測試	No.5-8	No. 1-4			

四、實驗結果與討論

1. 網路效能

我們使用隨機梯度下降法(Stochastic Gradient Descent, SGD)[22]來優化網路，並依據測試階段的結果評估網路效能如表二。

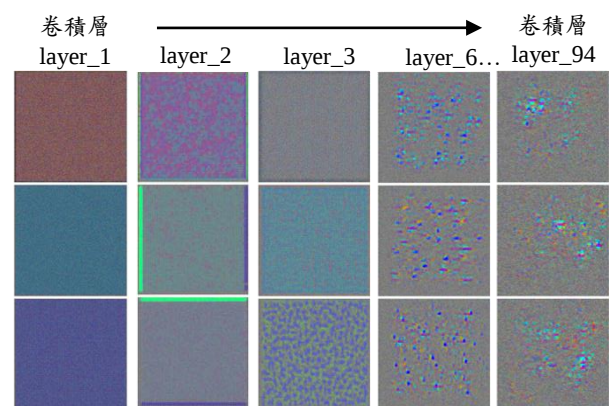
表二：實驗結果

實驗對象	簽名編號14			簽名編號16		
實驗編號	實驗1	實驗2	實驗3	實驗4	實驗5	實驗6
偽造作者數	3	2	1	3	2	1
偽造簽名數	6	4	2	6	4	2
訓練準確率(%)	99.93	100	99.67	100	99.97	100
驗證準確率(%)	100	100	95.66	98.96	97.56	99.98
測試準確率(%)	99.96	99.98	76.93	94.37	90.23	90.85
測試 FRR (%)	0.22	0.07	1.47	5.34	3.66	16.31
測試 FAR (%)	0	0	27.81	5.88	15.16	2.83

其中實驗1、4採用了最多的偽造樣本，可做為評估網路效能的主要實驗。FRR 代表錯誤拒絕率(False Rejected Rate或稱型I錯誤)；FAR 代表錯誤接受率(False Acceptance Rate或稱型II錯誤)。

2. 結果可視化

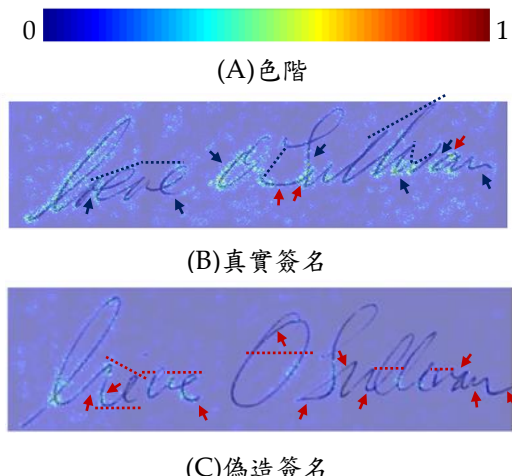
為了使本研究的CNN方法更具解釋性，我們分別針對卷積層的濾波器及全連接層的顯著性圖做可視化處理。首先，由於卷積濾波器本身不可見，我們通過讓濾波器優化我們輸入的隨機灰階雜訊，藉此產生可視化圖形，如下圖六。



圖六：本實驗各卷積層的濾波器

在圖六中，我們可以觀察到第1層的卷積濾波器主要負責色彩資訊處理（在本實驗中，由於我們使用灰階影像作為樣本，因此並無明顯差異），而在之後的第2及第3層中迭代出一些斑點和線條紋理。隨著CNN網路深度的加深，這些濾波器將成為越來越複雜的特徵提取器，並逐層擷取出更高級別的特徵。

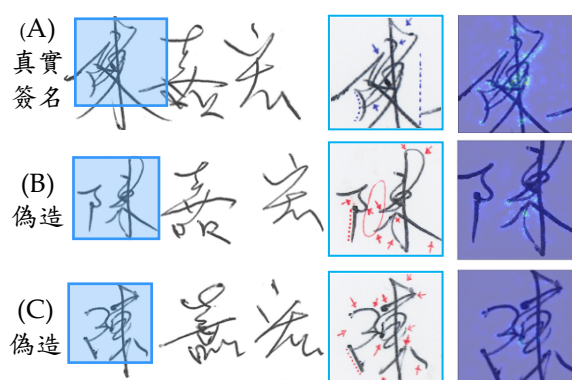
更直觀的方法便是直接可視化網路的決策過程，其結果基於網路架構中最後的全連接層。為了使圖形更清晰，我們使用了Jet色表，由藍、綠、黃、紅等色階代表顯著圖中各像素由0至1的顯著性強度，並將其結果與刑事警察局筆跡鑑定專家的鑑識結果進行比對，如圖七。



圖七: 外文簽名顯著圖與專家鑑定結果[18]

圖中出現的亮點便是對CNN決策結果造成顯著影響的區域(梯度變化較高)，在本研究的二元分類的情境中，亮點區域亦可理解為CNN系統判定該簽名為真實簽名的區域特徵。例如我們可以發現圖(B)的真實簽名中出現大量的顯著性熱區，而圖(C)的偽造簽名中則否。另外，人類鑑識專家的鑑定結果亦在同一張圖片中以虛線及箭頭標注，其中深藍色標記代表該處字跡與真實字跡相近，反之，紅色標記則代表與真實簽名有明顯差異，可視為偽造特徵。

此外我們也做了中文簽名的對照圖，用以探討本研究模型在不同語系中的表現。圖八以臺灣最大宗姓氏「陳」為例，即可明顯看出CNN模型在中文字體的識別效果亦是相當顯著，更多細節將於在下個章節中探討。



圖八: 中文簽名顯著圖與專家鑑定結果

3. 討論

由實驗結果得知，我們的CNN方法可以通過單一已知樣本執行自動簽名驗證，特別是針對我們的控制組實驗(實驗1與實驗4)，

在測試階段中達到了99.6及94.37的準確率。其測試樣本為未曾參與網路訓練的真實簽名搭配全新的偽造作者，且樣本的排序完全依據原始資料集中的檔案編號所排列，以確保實驗的可靠性。另外，我們使用相同的方法，針對中文簽名進行測試，亦達到89.5%的準確率。

觀察表二實驗結果可以發現，CNN預測的準確率隨著參與訓練偽造樣本數的增加而有所提升，證明我們通過提供額外的偽造樣本來提高網路性能的策略是可行的。表示系統確實能從額外的偽造簽名中學習到有用且可供辨識的偽造特徵，並且這些偽造特徵極可能普遍存在於不同的偽造作者之間，因此能用於偵測出其他未知作者的偽造簽名。

接著我們進一步觀察圖七與圖八的CNN決策過程顯著圖，其結果亦符合研究人員的預期。首先，我們發現圖中的顯著區域(亮點)主要集中於字跡輪廓而非無關的背景雜訊，由此可知，由掃描器雜訊及紙張紋理產生的背景干擾對於決策過程的影響有限。另外，這些顯著圖也符合筆跡鑑識專家的認知，藉由觀察亮點在筆跡上的分布，便能有效區分該筆跡的真偽(或運筆品質)。

最後，藉由彙整CNN的可視化顯著圖與人類專家的鑑定結果，我們可為本研究的自動化簽名驗證方法提出以下見解：

- (1) 透過觀察顯著圖，可以歸納哪些筆跡對網路的決策最為重要(亮點熱區)，例如：我們發現轉折處和筆劃的交會處經常被CNN視為簽名驗證的重要特徵。
- (2) CNN系統特別擅長於檢查筆劃的「品質」，例如：偽造簽名字跡大多缺乏流暢性，並經常會出現諸如猶豫、顫抖、刻意潤飾、筆速停滯等相對拙劣的筆觸，而真實字跡則否。
- (3) 比較顯著圖和專家的檢查結果。人類專家更擅長檢查簽名的整體佈局，如筆劃的相對位置、字元間距等。考慮到本文的CNN系統主要致力於局部特徵的分析，很大程度上被迫放棄了整體特徵，因此這種結果亦十分合理。
- (4) 受限於人類有限的注意力及現有的鑑定方式，鑑識專家僅能在有限的作業空間中，為系爭簽名標注真實/偽造特徵，直至標注的特徵足以支持鑑定結果。但相較之下，CNN卻可自動化且無差別的標注所有真實/偽造的特徵，這也為原本無

從「量化」的筆跡鑑定工作，提供了良好的數據基礎。

五、結論與未來展望

在本文中，我們提出了使用單一已知樣本並基於深度CNN網路的手寫簽名驗證方法。實驗過程透過一系列步驟來確保實驗結果的可靠性，包括：資料前處理(消除背景雜訊)、安排對照實驗、測試未知樣本，並最終透過視覺化技術與人類專家協作，以檢驗結果的合理性。由實驗結果可知，即使是在小樣本量的不利條件下，其測試準確率仍可維持在89.5%和99.96%之間。

本文的方法在實用性上具備明顯優勢，不僅可用於自動化簽名驗證，另一個特點便是能更易於與人類專家協作，從而獲得更直接且強大的可靠度與可接受性。亦可做為電腦輔助系統，並協助執行「可量化」的簽名驗證。在後續的研究，我們希望可透過CNN系統的持續學習與反饋，進一步協助筆跡鑑定人員。

六、參考文獻

1. Justino E. J., El Yacoubi A., Bortolozzi F. and Sabourin R., "An off-line signature verification system using HMM and graphometric features," Proc. of the 4th international workshop on document analysis systems, 2000, pp: 211-222.
2. Shah A. S., Khan M. and Shah A., "An appraisal of off-line signature verification techniques," International Journal of Modern Education and Computer Science, (7:4) 2015, pp: 67-75.
3. Impedovo D., Pirlo G. and Plamondon R., "Handwritten signature verification: New advancements and open issues," 2012 International Conference on Frontiers in Handwriting Recognition, 2012 of Conference, pp: 367-372.
4. Hafemann L. G., Sabourin R. and Oliveira L. S., "Offline handwritten signature verification—literature review," 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), 2017 of Conference, pp: 1-8.
5. Diaz M., Ferrer M. A., Impedovo D., Malik M. I., Pirlo G. and Plamondon R., "A perspective analysis of handwritten signature technology," ACM Computing Surveys (CSUR), (51:6) 2019, pp: 1-39.
6. Khalajzadeh H., Mansouri M. and Teshnehlab M., "Persian signature verification using convolutional neural networks," International Journal of Engineering Research and Technology, (1:2) 2012, pp: 7-12.
7. Hafemann L. G., Oliveira L. S. and Sabourin R., "Fixed-sized representation learning from offline handwritten signatures of different sizes," International Journal on Document Analysis and Recognition (IJDAR), (21:3) 2018, pp: 219-232.
8. Bouamra W., Djeddi C., Nini B., Diaz M. and Siddiqi I., "Towards the design of an offline signature verifier based on a small number of genuine samples for training," Expert Systems with Applications, (1072018) pp: 182-195.
9. Adamski M. and Saeed K., "Signature verification by only single genuine sample in offline and online systems," AIP Conference Proceedings, (1738:1) 2016, pp: 180011-180015.
10. LeCun Y., Boser B., Denker J. S., Henderson D., Howard R. E., Hubbard W. and Jackel L. D., "Backpropagation applied to handwritten zip code recognition," Neural computation, (1:4) 1989, pp: 541-551.
11. Taigman Y., Yang M., Ranzato M. A. and Wolf L., "Deepface: Closing the gap to human-level performance in face verification," Proceedings of the IEEE conference on computer vision and pattern recognition, 2014, pp: 1701-1708.
12. Zhong Z., Jin L. and Xie Z., "High performance offline handwritten chinese character recognition using googlenet and directional feature maps," 2015 13th International Conference on Document Analysis and Recognition (ICDAR), 2015, pp: 846-850.
13. Russakovsky O., Deng J., Su H., Krause J., Satheesh S., Ma S., Huang Z., Karpathy A., Khosla A. and Bernstein M., "Imagenet large scale visual recognition challenge," International journal of computer vision, (115:3) 2015, pp: 211-252.
14. He K., Zhang X., Ren S. and Sun J., "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," Proceedings of the IEEE international conference on computer vision, 2015, pp: 1026-1034.
15. Kao H.-H. and Wen C.-Y., "A Deep Learning-Based Offline Signature Verification Method by Single Known Sample," Journal of Chung Cheng Institute of Technology, (49:1) 2020, pp: 23-34.
16. Scherer D., Müller A. and Behnke S., "Evaluation of pooling operations in convolutional architectures for object recognition," International conference on artificial neural networks, 2010, pp: 92-101.
17. Szegedy C., Vanhoucke V., Ioffe S., Shlens J. and Wojna Z., "Rethinking the inception architecture for computer vision," Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp: 2818-2826.
18. Kao H.-H., Wen C.-Y. and Chan K.-P., "An Improvement of the Interpretability for the Deep Learning Based Signature Examination Assistance Method," unpublished.
19. Simonyan K., Vedaldi A. and Zisserman A., "Deep inside convolutional networks: Visualising image classification models and saliency maps," arXiv preprint arXiv:1312.6034, 2013.

20. Liwicki M., Malik M. I., Van Den Heuvel C. E., Chen X., Berger C., Stoel R., Blumenstein M. and Found B., "Signature verification competition for online and offline skilled forgeries (sigcomp2011)," 2011 International Conference on Document Analysis and Recognition, 2011, pp: 1480-1484.
21. Kao H.-H. and Wen C.-Y., "An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach," Applied Sciences, (10:11) 2020, pp: 3716-3731.
22. Bottou L., "Large-scale machine learning with stochastic gradient descent," Proceedings of COMPSTAT'2010, 2010, pp: 177-186.

電商退款圖像取證的探討與應用-以EMD訊息嵌入法為例

梁羽涵¹楊佩瑜²

國立臺中科技大學商業經營系

¹kelly643030@gmail.com ²rachel870621@gmail.com

林鈺烽³洪維恩^{4,*}

國立臺中科技大學資訊工程系

³zhengfeng017@gmail.com ^{4,*}wienhong@nutc.edu.tw

摘要

當今電子商務網購行為盛行，而衍生出許多買賣雙方之糾紛問題，如電子商務之退貨與退款時，由消費者提供之瑕疵商品的圖像，其真實性難以辨別，因而造成許多買家與賣家之間的糾紛。為維護買賣雙方之權益問題，本研究提出一個新的架構，買家方面以電商平台提供的App拍攝瑕疵商品的同時，電商平台提供App將以EMD嵌入法嵌入買家的留言(文字訊息，或是由語音轉成的文字)與圖像的驗證訊息。電商平台在接收到消費者提供的圖像時，首先驗證圖像的真偽，欲確認買家是否使用電商平台提供的App來執行拍攝等問題。如果通過驗證，則將圖像交由賣家，賣家可以從嵌入訊息的圖像中提取出買家的留言，然後進行後續的賠償或退貨處理，達到公平地處理交易之事宜。本研究實作方面欲以Python來實現語音轉文字與EMD訊息嵌入法，實作的平台則是以Android Studio來開發。實驗結果顯示，本研究方法可以方便地驗證買家發送的圖像是否經過修改，同時在買家嵌入訊息後，圖像也可以保有相當良好的品質。

關鍵字:EMD、電子商務、訊息嵌入。

一、緒論

買賣交易已是人們生活中不可或缺的一項活動，因近十幾年來智慧型手機的蓬勃發展，以及受嚴重特殊傳染性肺炎疫情的影響，大多數民眾逐漸偏向在電商平台上購物，以代替實體通路購買各項商品及服務，加速宅經濟的發展，更帶動了電子商務的龐大商機。網路購物固然便利，但相較於實體通路挑選時，難以仔細檢視商品，往往做出非理性消費的決定，而事後後悔當初沒仔細查看店家提供之商品資訊。網路購物所衍生的買賣糾紛，如退貨退款、仿冒品，或是通過修飾圖像假造商品而引起買賣糾紛。

以社群網站平台之案例，有賣家於Facebook買賣社團進行交易，此賣家使用修圖軟體Photoshop將從網路上抓取精品名牌包的商品照片，試圖編輯混入與賣家本人照片中，讓買家誤信賣方真的持有此商品，事實上卻以低價巧克力充當，使買家受騙上當，藉此賺取不法獲利(徐聖倫，2017)。除了買家受騙外，也有賣家遭受欺騙的案例，買賣雙方約定匯款轉帳，再進行面交，買家憑藉修圖過的假匯款單，成功欺騙賣家，賣家誤信買家已完成付款，殊不知已受騙上當(張晏碩、羅執中，2017)。一名網路賣家被客人質疑送達的包裹內皆為

垃圾，並且附上全程開箱錄影作為證據，聲稱不會進行匯款行為。賣家堅信有確實將商品寄出，只是未拍攝包裝影片，因此無法證明清白，由於開箱影片有嚴重的曝光問題，無法看清楚包裹託運單的單號，故而引起買賣雙方議論(趙蔡州，2020)。在資訊科技發達的時代，雖然網路購物方便又快速，可不受時間、地點的影響，但正因無法看到商品實物，僅由網路商場所張貼的產品照片獲取資訊，其產品照可能已經由商家私下地修改或編輯，而產生寄送到達商品實體與圖像不符合的風險，衍生出退換貨與退款問題。然而當顧客要求退換貨時，商家也無從確認商品是否如買家所稱是有瑕疵的；抑或是無法驗證購買者傳送的圖像是否屬實且未經修改。為避免以上可能導致糾紛問題之總述，並基於保障買賣雙方的權益，本研究欲解決消費糾紛之圖像正確性，故提出新的架構，驗證其圖像是否經過後製處理，以利分辨其真偽，以電子商務退貨退款為例。

本研究將實作應用於開發手機App，利用Python內SpeechRecognition套件撰寫語音轉文字程式，App內可使用語音輸入方式以便描述商品狀況，並運用EMD(2006)技術，將訊息嵌入圖像中，在這過程中App會另外嵌入驗證碼，使用者將含有訊息、驗證碼的圖像一併

傳輸給對方，對方可藉由驗證碼以檢驗圖像是否經過處理。

二、文獻探討

語音辨識(Speech recognition)技術，主要是讓電腦依據人類說出的內容自動與電腦資料庫進行比對辨識，並將其結果轉換成相對應的文字。故語音辨識可稱為語音轉文字(Speech to text)、自動語音辨識(Automatic speech recognition)或電腦語音識別(Computer speech recognition)。其應用範圍相當廣泛，可使用於語音輸入文字，生活中常見的有iPhone中的Siri和Google的Google助理，另外還可用於演講稿轉文字、語音控制產品(撥號與導航)、或是語音查詢系統(圖像、影音、檔案或文字)等等。本研究將使用Python提供的SpeechRecognition模組中的recognize_google方法來進行語音辨識，並以EMD(Exploiting modification direction)嵌入技術將語音辨識後生成的文字利用EMD技術嵌入圖像中。

過去有許多嵌入技術相繼被發展出來，其中Mielikainen(2006)的方法可有效的將LSB嵌入法造成的MSE從0.5減少到0.375。Zhang與Wang(2006)的方法則是Mielikainen方法(2006)的改良版，它可以利用像素之間的關係來嵌入一個特定進位的數字。Chao等學者(2009)的方法則提出了Diamond Encoding的技術，可以以兩個像素為一組，嵌入特定進位的數字。Hong與Chen(2012)則改進了Chao等學者的方法，使得兩個像素可以嵌入任意進位的數字。在這些方法中，因為Zhang和Wang(2006)的方法可以在嵌入的資料量較少的情況下獲得較佳的圖像品質，因為本研究採用Zhang與Wang(2006)所提的EMD方法，作為本研究的核心嵌入技術。

EMD訊息嵌入技術是以 n 個像素為一組，只要將一個像素加一或減一，即可嵌入一個 $2n+1$ 進位的數字。由於像素值更動較小，因此嵌入訊息後得到的圖像品質較傳統的最低有效位元替換(Least Significant Bit; LSB)嵌入法由佳，且可以有效的控制嵌入方式以達到較好的效果，因此本研究以EMD作為本研究主要的嵌入技術。

設有 n 個像素 $g_1, g_2, \dots, g_n$ 一組，現欲嵌入一個 $2n+1$ 進位的數字 d ，首先計算提取函數的值 f ：

$$f(g_1, g_2, \dots, g_n) = \left[\sum_{i=1}^n (g_i \times i) \right] \bmod (2n+1) \quad (1)$$

當 $d = f$ ，則嵌入訊息後的像素值不改變；反之，當 $d \neq f$ ，代表某一個像素值要改變，因此須先決定哪一個像素要進行處理。首先計算 $s = (d - f) \bmod (2n+1)$ ，並由計算結果來選擇哪一個像素值必須增加或減少一個灰階值。如果 s 小於等於 n ，則將像素 g_s 加1。如果 s 大於 n ，則將像素 g_{2n+1-s} 減1。

舉例來說，如果三個像素[90,40,30]欲嵌入一個七進位的數字，設 $d=1$ ，則 $n=3$ ，從(1)式可以求得 $f=1$ 。因為 $d=f$ ，故嵌入訊息後，像素的值仍為[90,40,30]，意旨不改變任何像素值。如果欲嵌入九進位的數字，設 $d=8$ ，則必須以四個像素為一組，設原像素組為[183, 80, 90, 100]，且 $n=4$ 。從(1)式可以求得 $f=5$ ，因 $d \neq f$ ，故可求得 $s=3$ 。由於 $s \leq n$ ，因此第三個像素的值要增加1，所以嵌入後的像素組為[183, 80, 91, 100]。

三、語音轉換文字與訊息嵌入

3.1 聲源的取得與轉換

本研究是利用語音轉文字套件SpeechRecognition，將使用者的語音轉換成文字。此外運用PyAudio套件來啟動並使用麥克風。在使用SpeechRecognition時，必須先匯入speech_recognition套件，再利用套件中的Recognizer類別來建立一個識別物件，並以物件的listen()方法來聆聽聲源。最後再以recognize_google()方法將聆聽到的聲源，以指定語系的方式來辨識出文字。

3.2 求得最佳的像素組數

上述的聲源可以是買家對於產品的抱怨、產品瑕疵的描述、購買的時間、以及其它有利於與賣家溝通的訊息等等。一般而言，這些描述應少於三分鐘，一般人平常說話的語速約為160個字。假設中文以Unicode編碼，每個中文字元佔16個位元，因此說話3分鐘轉成文字之後，其資訊量約為 $3 \times 160 \times 16 = 7680$ 個位元。另外需將圖像利用MD5雜湊運算來生成256個位元的驗證碼，因此整張圖像要嵌入的訊息量約為8000個位元。這對於一般擁有千萬

像素的手機而言，資訊的嵌入量較小。因此如果利用較少的像素為一組來嵌入訊息的話，顯然嵌入的區域會集中在圖像的某個區域，如此將造成該區域會有較不自然的統計性質，容易被藏密分析法檢測出來。

因此本研究是依影像的大小與欲藏入的訊息量來推估出最佳像素組的大小，使得圖像的破壞為最少。設 N 為彩色圖像像素的總數，因彩色的像素有3個通道（Channel），可以視為 $3N$ 個灰階像素得以嵌入訊息。如果是以 n 個像素為一組， p 為欲嵌入的訊息量， $3N$ 個灰階像素共有 $3N/n$ 組，每組嵌入的訊息量為 $\log_2(2n+1)$ ，因此總共可嵌入的訊息量為 $\log_2(2n+1) \times 3N/n$ ，這個數字必須大於欲嵌入的訊息量 P ，若要嵌入 P ，必須滿足下面的公式：

$$\log_2(2n+1) \times 3N/n \geq P \quad (2)$$

例如，假設 p 為8000個位元，彩色圖像的大小為 512×512 ，則

$$\log_2(2n+1) \times 3 \times 512 \times 512 / n \geq 8000 \quad (3)$$

必須成立。由上面的不等式中可以解得最大的 n 為8001。也就是取 $8001/3=2667$ 個彩色像素為一組時，方能得到最佳嵌入後圖像的品質。

3.3 進位數的轉換

語音轉文字後，可以取得代表文字的一串二進位的位元流（Bit stream），而MD5雜湊運算的結果也是二進位的位元流，然而EMD需要的是某一個特定進位的數字，必須進行二進位與特定進位的轉換，才能將順利的將訊息嵌入圖像中。一般的程式語言並沒有提供二進位與特定進位的轉換，故Python的整數運算可以有無窮多個位數的精度，這使得在Python的環境裡，能夠容易進行特定位數的轉換。以下為本研究提供的兩個函數，其中 `int2base(integer, base)` 可以將十進位的整數 `integer` 轉換成 `base` 進位的數字，而轉換的結果以Python的List容器來儲存。另一個函數 `base2int(digits, base)` 則是將由 `base` 進位組成的 `digits`（為一個List）轉換成十進位的整數。這兩個函數列表如下：

```
#十進位轉任意進位
#傳入值型態: integer(int)、base(int)
#傳回值型態: digits(list)
def int2base(integer, base):
    digits = []
    while integer:
        digits.append(integer % base)
        integer=integer//base
    digits.reverse()
    return digits
#print(int2base(2482,2))

#任意進位轉十進位
#傳入值型態: digits(list)、base(int)
#傳回值型態: total(int)
def base2int(digits,base):
    r_digits=digits.copy()
    r_digits.reverse()
    p_base=1 # power of base
    total=0
    for d in r_digits[1:]:
        p_base*=base
        total+=d*p_base
    total+=r_digits[0]
    return total
```

3.4 訊息嵌入

設語音轉文字之後的位元流為 P ，長度為 $|P|$ ，圖像 I 的總像素為 $3N$ （一個彩色像素的三個Channel視為3個像素）。MD5雜湊的結果 M 為128個位元，因此利用一個金鑰 k 隨機挑選128個像素，它們的LSB將用來嵌入 M 。這128個像素已經用來承載 M ，因此可以用來承載 P 的像素為 $3N-128$ 個，故找到最大的 n ，使得

$$\log_2(2n+1) \times (3N-128) / n \geq P \quad (4)$$

解得 n 之後，即可利用EMD的方法，以 n 個像素為一組，將 P 嵌入。

嵌入 P 之後，得到 I' 。將 I' 的所有像素，除了用金鑰 k 隨機挑選的128個像素之外，進行MD5的運算，得到 M 。然後再將 M 嵌入到

這128個像素的LSB中，即可得到一張嵌入文字和驗證碼的圖像 I'' 。

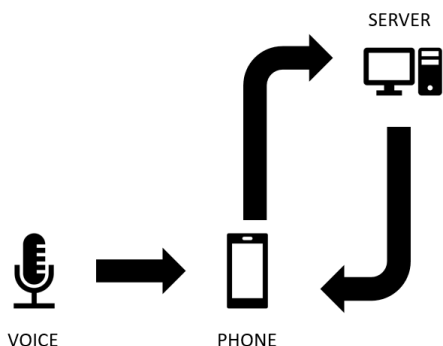
3.5 圖像驗證

在電商平台收到買家提供的圖像之後，可以先利用金鑰 k 取得嵌入128個像素之LSB的 M' 。如果 $M' \neq M$ ，代表圖像已被篡改。如果 $M' = M$ ，代表圖像沒有被修改過，此時可以將圖像傳送給賣家進行後續的處理。賣家接收到圖像之後，可以取得嵌入圖像的訊息 P ，將其轉換成十進位的數字，再轉成中文字元後，便得已知悉買家的訴求，進而與買家溝通，進行後續的處理。

四、系統實作與實驗結果

本研究實作以 Android Studio 來開發 App，Android Studio 是用來撰寫 Android 手機 App 的一個開發環境，裡面整合大量且常用的應用程式介面(API)可供使用，像是藍芽連接、語音辨識、語音轉文字等。本研究欲透過 Google 提供的 RecognizerIntent 套件，使用其中的語音轉文字功能來取得說出的文字內容，並利用 OkHttp 套件來達成連接網路的需求，將圖像與文字傳送到後端進行處理。

在資料嵌入的部分，透過 Python 撰寫文字藏匿的部分，並將這段程式碼放置在後端的伺服器(Server)上。在伺服器的架設上，選擇以 Node.js 框架來進行開發，原因是其輕量且開發快速的優點。當伺服器接收到 App 傳送的文字及圖像後，便會開執行資料藏匿的動作，最後將藏匿完成的圖像傳回手機呈現。本研究系統實作示意圖如圖一所示。



圖一：本系統的實作示意圖

在實驗方面，以四張手機拍攝的圖像作為範例進行測試，將其剪裁成 768×512 的

小，以利檢測。這四張圖像如圖二所示：(a)為泡麵未附上調味包(b)藍芽耳機有污漬(c)袋子圖示印刷已掉色(d)收到手機殼實體與店家提供圖像不符合。



圖二：四張測試圖像

圖像品質的測試是以 PSNR 來衡量，其定義為

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}}, \quad (5)$$

其中 MSE 為原始圖像和嵌入訊息後之圖像的均方差。在每張圖像中，約嵌入 2 分鐘語音轉成文字之後的訊息量，約為 320~400 個字。實驗結果顯示，每張圖的 PSNR 均在 60dB 以上。表示本研究方法實驗結果有相當好的圖像品質，同時也能起到圖像保護的作用，且足以將必要的訊息嵌入於圖像中，為電商平台的交易糾紛提供另一個解決的方案。

六、結論

本研究針對電商退款情境中買賣雙方交易糾紛，提出一種 App 可透過語音轉文字來描述買方欲退貨的瑕疵商品，並且運用 Zhang 與 Wang(2006)所提的 EMD 方法進行圖像驗證，Zhang 與 Wang(2006)的方法可以在嵌入的資

料量較少的情況下獲得較佳的圖像品質。以上總述，本研究結果歸納如下：

通常訊息嵌入圖像會破壞圖像品質，然而本研究依據影像的大小與欲藏入的訊息量來推估出最佳像素組的大小，使得圖像的破壞為最少。實作結果顯示，每張圖像的品質測試PSNR均在60dB以上，達到非常好的圖像品質，也能兼顧圖像保護的作用。因電商購物的普及，電子商務交易糾紛之問題備受關注，故本研究提供新的解決方法，透過App用語音轉文字來方便描述瑕疵商品與提出圖像驗證機制，幫助電商在短時間進行圖像驗證真偽，進行後續退貨退款處理，保障買賣雙方的交易權利，降低其交易糾紛之機會，本研究可供相關電商業者及後續研究人員參考，以達成學術與實務上的貢獻。

本研究因範圍僅侷限於電商領域，建議未來研究可擴大其應用範圍領域，如金融領域、通訊、交友軟體，並可增設影像之功能，不侷限於圖像。

七、參考文獻

1. 丁家群，「語音辨識與VisualBasic」，義守大學電子工程學系碩士論文，2003，第7~8頁。
2. 徐聖倫，〈男手拿LV拍照取信買家 原來都是P上去的〉，自由時報。2017，取自<https://news.ltn.com.tw/news/society/breakingnews/2162355>
3. 張晏碩、羅執中，〈「直播網紅」修圖改匯款單 賣家受騙出貨〉，民視。2017，取自<https://reurl.cc/Y6k49x>
4. 趙蔡州，〈買家收包裹問「為何寄垃圾」！他回一句話掉入陷阱 網曝3大疑點：快報警〉，ETtoday新聞雲。2020，取自<https://www.ettoday.net/news/20200924/1817011.htm>
5. 賴昀琪，「一種新的影像驗證方案於電子商務退款應用」，國立臺中科技大學流通管理系碩士班碩士論文，2020，第1~7頁。
6. Chan C.K. and Cheng L.M., "Hiding Data in Images by Simple LSB Substitution," Pattern Recognition, vol. 37, no. 3, pp. 469-474, 2004.
7. Chao, R.M., Wu, H.C., Lee, C.C., and Chu, Y.P., "A Novel Image Data Hiding Scheme with Diamond Encoding," EURASIP Journal on Information Security, vol. 2009, Article ID 658047. doi:10.1155/2009/658047, 2009.
8. Hong W. and Chen T.S., "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 176-184, 2012.
9. Lin, K.Y., Hong, W., Chen, J., Chen, T.S., and Chiang, W.C., "Data hiding by Exploiting Modification Direction technique using optimal pixel grouping," International Conference on Education Technology and Computer, pp. V3-121-V3-123, 2010.
10. Mielikainen J., "LSB Matching Revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.
11. Zhang X. and Wang S., "Efficient Steganographic Embedding by Exploiting Modification Direction," IEEE Communications Letters, vol. 10, no. 11, pp. 781-783, 2006.

警車即時影像及定位導航視訊系統在攔截圍捕上的應用

古淳寶

中央警察大學資訊管理所研究生

im1093061@mail.cpu.edu.tw

董正談

中央警察大學資訊管理所助理教授

tung@mail.cpu.edu.tw

鄧少華

中央警察大學資訊管理所教授，通訊作者

pdeng@mail.cpu.edu.tw

摘要

警車追逐具高度危險性，強硬的追車行為可能導致追逐員警及逃逸者在追逐的過程中造成意外，因此追逐員警對於逃逸車輛應採取尾隨跟車方式保持安全距離，待支援到達後再以優勢警力進行攔截圍捕。有鑑於此，本研究使用警車行車記錄器即時影像結合M-Police(警用行動電腦)定位導航功能，建構一套整合即時影像、定位導航、推播訊息及群組軟體功能之系統，搭配5G以及車聯網概念，連結勤務指揮中心伺服器及各支援警力，提供警方使用勤務指揮中心電腦、M-Police等終端設備互相聯絡，並顯示警車追逐現場即時狀況及定位導航位置，以利支援警力鎖定逃逸車輛的即時位置，進而順利完成攔截圍捕任務。透過本研究之「警車即時影像及定位導航視訊系統」以尾隨跟車並等待支援警力攔截圍捕的方式取代單一警車追逐，期望減少警車追逐造成之意外，以安全為優先考量，提升員警執勤的安全性。

關鍵字：執勤安全、定位導航、推播系統、車聯網、5G

一、前言

警察於巡邏、臨檢勤務發現民眾有公共危險、攜帶毒品、槍枝等違法情事時，若民眾不願配合而逕自駕駛車輛逃逸，此時警方就必須以警車追逐方式逮捕違法民眾。在只有單一警車進行警車追逐時，常因過於緊張而導致傷亡，因此對於逃逸車輛宜先保持安全距離尾隨在後，待支援到達後再以優勢警力進行攔截圍捕，方可在安全的前提下逮捕逃逸違法民眾。本研究使用警車行車記錄器即時影像結合M-Police定位導航功能，以5G和車聯網概念，建構一套結合即時影像、定位導航、推播訊息及群組軟體功能之系統，讓勤務指揮中心人員及參與攔截圍捕行動的所有警力可以互相聯絡，並透過電腦、手機等終端設備追蹤警車追逐的即時現場狀況及定位導航位置，如此藉由即時影像結合定位導航的方式，輔助警方以更加安全

的方式追捕逃逸違法民眾，改善攔截圍捕的效率及警車追逐的安全性。

二、研究動機

2019年8月28日警員薛定岳騎乘警用機車追捕毒駕(吸食毒品後駕駛車輛)機車騎士王男，在追逐過程中與王男擦撞導致薛員摔車身亡；2016年11月2日警員涂毓修、陳明慧執行取締酒駕(飲酒後駕駛車輛)勤務，自小客車駕駛劉男酒駕拒檢並加速逃逸，在追逐過程中巡邏車失控自撞路樹，導致涂員受傷、陳員傷重不治。

以上兩起事故再次證明警車追逐之高度危險性，在單一警車進行警車追逐時，欲逮捕逃逸人犯只能以強硬的追車手段逼近逃逸車輛並喝令對方停車，但此種方式不僅危險，成效也十分低落。

上述案例如能使用警車即時影像及定位導航視訊系統，以尾隨方式跟車，將

現場的即時影像與定位導航位置傳送給勤務指揮中心及支援警力，並於攔截圍捕群組中互相溝通、協調，將會大幅改善警車追逐的安全性。

三、研究目的

本研究期望提升警車追逐的安全性及強化警車攔截圍捕應用，以降低追捕逃逸車輛造成的損害及傷亡。透過警車行車記錄器即時影像結合M-Police定位導航功能，以警車即時影像及定位導航視訊系統提供第一線執勤員警以尾隨跟車等待支援取代單一警車追逐。在警車即時影像及定位導航視訊系統的輔助下，尾隨跟車員警可以透過M-Police與勤務指揮中心人員及支援警力聯繫，並將警車追逐現場的即時影像及定位導航位置同步於上述人員的終端設備，以利進行攔截圍捕任務。

四、相關文獻及背景知識

本研究使用警車行車記錄器即時影像結合M-Police定位導航功能，將即時影像及位置提供給勤務指揮中心人員及支援警力，以下就相關文獻及背景知識進行探討。

1、員警駕駛能力與對道路熟悉情形

目前國內基層員警的駕駛能力，大多來自於民間駕訓班，對於警車追逐攔查的駕車技巧大都來自員警個人實務經驗的累積，因此警察在警車追逐的先天上條件是趨於劣勢的；再加上，警車追逐一旦進入他轄或逃逸者熟悉的環境道路，執勤員警常囿於對道路環境的陌生以及通訊指揮聯絡的能力，影響警車追逐的攔獲能力[1]。

2、員警因公受傷

依據警察人員因公傷殘死亡殉職慰問金發給辦法第4條，本辦法所稱因公受傷、殘廢、死亡，指因下列情事之一所致者[2]：

(1)執行職務發生意外。

(2)公差遇險。

(3)在辦公場所發生意外。

前條所定人員於非上班時間內執行職務或逮捕現行犯、通緝犯或其他緊急事故之行為，致受傷、殘廢、死亡者，視為執行職務發生意外。第一項第二款所稱公差，指經機關指派執行一定之任務，其時程之計算係自出發以迄完成指派任務返回辦公場所或住（居）所止；第三款所稱辦公場所，指於辦公時間或指派工作之時間內，處理公務之場所。

由於警車追逐時常造成傷亡，因此必須加強員警執勤安全的觀念，以尾隨跟車等待支援取代單一警車追逐，減少員警因公受傷的可能。

3、逃逸者的立即危害性

就危害性而言，車輛交通違規除非是酒後駕車、濫用毒品藥物、疲勞駕車或於道路上飆車、競逐等交通違規者外，一般違規車輛尚不會有帶來立即性危險；而刑事犯罪者在未遇警車追緝前，其行為亦會趨於保守，不致帶來立即性的危害，然而一旦警察發動警車追逐，逃逸者就可能加速逃逸，且當警車越加積極追逐，逃逸者就越易瘋狂加速，相對公眾危害性也會因而提升[10]。因此，警車追逐前，宜評估逃逸者的立即危害程度與進行追逐後可能帶來的危險性。

4、全球衛星定位系統

全球定位系統(Global Positioning System, GPS)，又稱全球衛星定位系統，由美國國防部研製和維護的中距離圓型軌道衛星導航系統。它可以為地球表面絕大部分地區(98%)提供準確的定位、測速和高精度的時間標準。可滿足全球任何地方或近地空間的軍事用戶連續精確的確定三維位置、三維運動和時間的需要。該系統包括大空中的24顆GPS衛星；地面上的1個主控站、3個數據注入站和5個監測站及作為用戶端的GPS接收機。最少只需其中3顆衛星，就能迅速確定用戶端在地球上所處位置及海拔高度；所能接收連接到衛星數越多，解碼出來的位置就越精確。對使用者而言，只需擁有GPS接收

機即可收到 GPS 衛星傳來的信號並利用此資訊去計算用戶的三維位置及時間。

GPS行車導航系統，在雲端化的導航趨勢下，結合動態路況，更可經由用路人分享的資訊，將所有最新路況消息傳送至遠端系統進行整合，再將資訊回饋給導航服務，如此GPS裝置即可讓駕駛人掌握最即時的路況變化。因此在行動裝置日趨普及的今日，借助APP結合行動裝置，能將更多直覺式的行車服務所產生的巨量資料，進行駕駛人行車習慣與旅運行為分析，進而提供個人化的差異服務[6]。

5、Google Maps 電子地圖服務

Google Maps是Google公司向全球提供的電子地圖服務，是利用計算機技術以數位方式儲存和查閱的地圖，同時也是目前全球最被廣泛運用的電子地圖，地圖包含地標、線條、形狀等資訊，也可分成一般向量地圖、街景服務、地形圖等三種視圖[3]。

當駕駛者一邊存取 Google Maps 的地圖資訊時，Google Maps 也會將駕駛者現在的位置上傳，只要數量夠多，就知道哪些地方人多，哪些地方人少。此外 Google Maps 也會根據歷史資料判斷某些時段的汽車駕駛速度。透過 Google Maps 的預測即時路況之功能，其主要是根據用戶過往透過手機回傳的地理位置資訊，從起始點和目的地終止點的資料，可約略計算出每一台手機移動速度，並以此綜合判斷出，這一段路上所有手機在行駛狀況時的資訊，所約略估算分析出這條路是否順暢或回堵的交通量狀況。

7、位置感知技術(Location Awareness)

位置感知技術是能夠檢測其當前位置然後操縱該數據以控制事件和信息的任何技術。通過使用各種傳感器和計算地理位置的方法（例如通過GPS技術）來檢測位置。位置感知設備能夠給出相對於位置的指示，訪問地理上感知的服務和數據，以及廣播設備的位置。

通常通過積體電路模組在設備中啟用位置感知技術，從可安裝在車輛中的完整GPS設備到安裝在諸如電話和平板電腦的移動設備中的小型GPS微晶片。手機設備中的位置感知技術與設備的操作系統連接，以提供位置感知或位置特定的服務。例如，Android和iOS的一些應用程序基於設備的位置具有不同的數據和內容，顯示不同的事件或旅遊目的地，地標甚至餐館。簡單的定義，位置感知可以知道您所處的位置以及您與周圍環境相關的位置。我們將位置感知與可以確定其位置的各種設備相關聯。當我們在自動化和人工智能驅動的應用程序中處於領先地位時，更多設備在需要處於不同位置以執行特定任務的應用程序中運行。設備知道它的位置的能力將是知道執行專用任務所需的第一步。

位置感知的服務是利用具有IP功能的移動設備上的軟體應用程式，其需要關於移動設備位於何處的知識。位置感知的服務可以即時查詢，並提供有用的訊息。

位置感知構成的四個基本條件[11]：

- (1)Positioning technology 定位技術
- (2)Communication network 通訊雲端網路
- (3)Content provider 內容供應商
- (4)Mobile device 移動設備

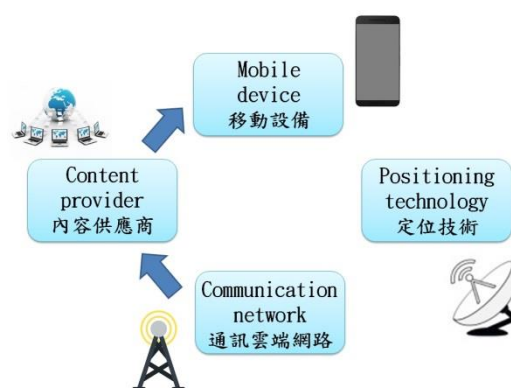


圖1：位置感知構成的四個基本條件

6、智慧型行動裝置推播技術

推播(Push)應用的產生主要是因為

傳統的Pull架構是一個以請求/回應為主的運作方式。使用者只能在有需要的情況下主動提出要求，接著就是等候服務的回應，這是屬於典型的同步互動模式。而Push技術則是允許在非同步的情況下，將符合需求的資訊主動地傳送給使用者，讓使用者即時取得最新的內容。由於具備了這樣的特性，可以將它應用在訊息主動通知的服務上，例如：股票的即時報價、訂票補位的通知、交通路況的提供…等[8]。

想了解何謂推播，首先要知道什麼是Pull，當伺服器端產生網頁後，使用者必須點入該網頁才可能獲得所需要的資訊或服務，Pull的概念就是必須由使用者（客戶端）花時間主動去連接伺服器端。Pull的缺點就是有時候使用者經過漫長的查詢，卻還看到一堆沒有用或不想要的資訊，於是推播技術順勢而生。推播是將資料主動由伺服器端傳送至使用者，伺服器端掌握資料的控制權，而使用者可以選擇是否想要接收伺服器端推播即時資訊給自己，創造雙贏的局面[4]。

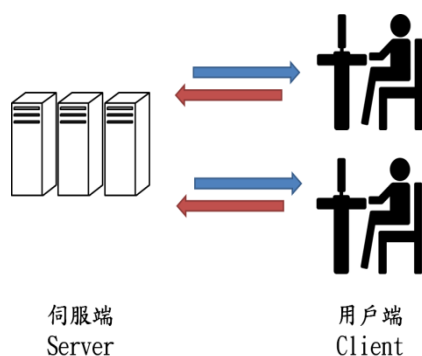


圖2：Pull / Smart Pull示意圖

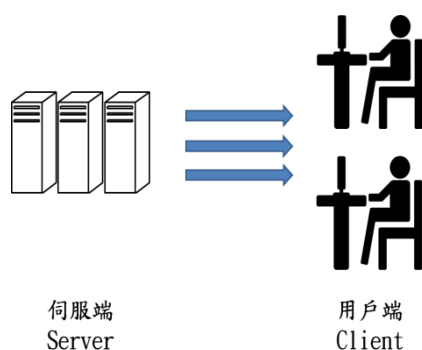


圖3：Push示意圖

7、車聯網

車聯網是物聯網在交通領域的應用，串接車輛資訊與行動網路，運用衛星定位、感測器、電子標籤、無線網路通訊、資料處理等技術對車輛、行人和道路環境三方的靜態和動態訊息進行有效辨識及傳遞，並將資料彙整後端平台進行智慧化管理和服務除提供駕駛者相關資訊外，也普遍應用於交通安全、交通服務、城市管理、物流運輸、智慧收費等(來源：MBA智庫百科、數位時代)。其減少交通擁塞，同時增加行車安全與節能[9]。

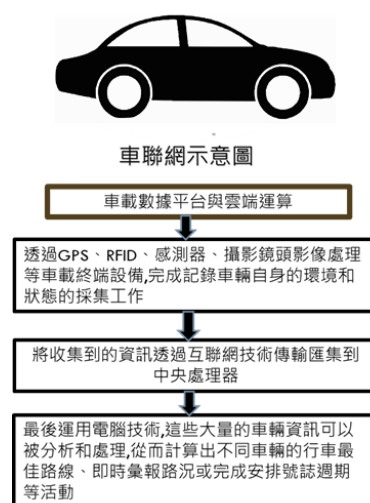


圖4：車聯網示意圖

8、群組軟體(Groupware)

亦稱為協同作業軟體、協同軟體、群件等[12]。群組軟體是「網路軟體」的概念，由一群人透過網路連接使用應用程式，達到共同作業的目的，例如 Line 軟體使用戶間相互通訊和協調活動即是一個很好的例子。傳統上有以下幾個主軸[5]：

- (1) 溝通(Communication)：專注於讓互相合作的人們可以有效交換資訊，目的在避免錯誤認知與假設。
- (2) 協調(Coordination)：主要是讓各樣的工作能夠井然有序的進行，目的在加強效率。
- (3) 合作(Cooperation)：是要讓共同作

業的成員能好好相處，目的在合諧。當然，有效合作需要有效的溝通；很多溝通需求就要用好的協調機制來管理；協調機制會安排有利合作的工作分配。如此複雜的循環，就會讓一群共同工作者想要有個系統來輔助他們。

9、第五代行動通訊技術(5G)

第五代行動通訊技術(5G)具有高速度、低延遲等特性。5G 技術的速度最快可達 4G 技術的 100 倍，其特性能夠運用在行動電信以外的產業服務與產品上，如物聯網(Internet of Things)、人工智慧、大數據等概念，隨著 5G 議題的討論更加興盛，新興的商業模式與競爭策略在 5G 時代也會全然與 4G 時代不同[7]。

針對 5G 的應用，埃森哲(Accenture)指出以 5G 為首的五大科技，將被聚焦在：(一) 5G；(二) AR、VR、MR，甚至是 XR；(三)、人工智慧 (AI)；(四) 智慧駕駛；(五) 數位信任。而透過物聯網 (IoT)、人工智慧 (AI)、大數據等技術，5G 則能運用到智慧交通運輸、智慧城市、健康連結、智慧家居和媒體、無線網路產業等，衍生出無限的商機。

五、解決方案—警車即時影像及定位導航視訊系統

有鑑於警車追逐的危險性，本研究開發警車即時影像及定位導航視訊系統，使第一線執勤員警可以透過建立攔截圍捕群組與勤務指揮中心人員及支援警力進行溝通，並分享現場即時影像及同步定位導航位置，以利支援警力快速掌握目標位置，降低警車追逐造成的危害。以下就警車即時影像及定位導航視訊系統簡介、系統架構與操作頁面設計分別敘述：

1、系統簡介

警車即時影像及定位導航視訊系統結合警車行車紀錄器影像以及M-Police定位導航功能，以建立群組的方式將即時影像及定位導航位置分享給勤務指揮中

心及支援警力，並且能與群組內成員進行語音通話，使勤務指揮中心人員可以快速指揮調度，以及使支援警力可以互相溝通、協調，以便等待最佳時機以優勢警力進行攔截圍捕，降低警車追逐造成的損害及傷亡。

2、系統架構

警車即時影像及定位導航視訊系統結合即時影像、定位導航、推播訊息及群組軟體功能，讓第一線員警使用M-Police的Wi-Fi功能連結警車行車紀錄器影像，加上Google Maps定位導航位置，以車聯網架構使用5G行動通訊將警車即時影像及定位導航位置連結至勤務指揮中心伺服器，再由勤務指揮中心人員將即時影像及位置連結至加入攔截圍捕行動的支援警力。上述人員能夠運用群組語音對話功能互相溝通、聯絡，搭配即時影像及定位導航便能提高攔截圍捕的效率及安全性，相關系統架構如圖5。

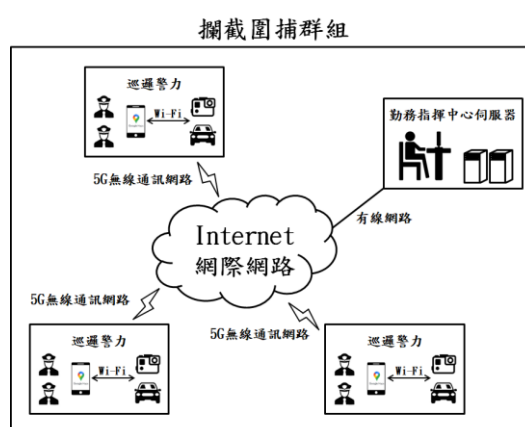


圖5：系統架構圖

3、警車即時影像及定位導航視訊系統之操作頁面設計

以下介紹警車即時影像及定位導航視訊系統之操作頁面設計。

3.1、登入頁面

本系統登入頁面以下拉式選單選取單位名稱，如澄觀派出所、仁武派出所、

大華派出所等單位，並輸入使用車輛之車牌號碼以登入主畫面，如圖6。



圖6：登入頁面

3.2、主選單頁面

主選單頁面分為「即時影像連結」、「顯示定位畫面」及「進行攔截圍捕」三個選項功能，如圖7。

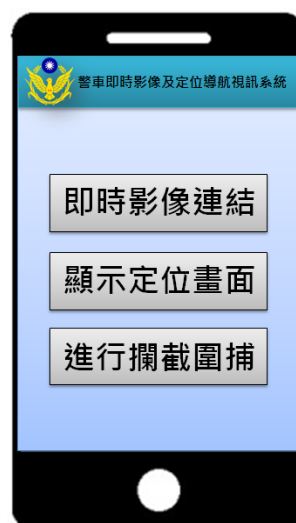


圖7：主選單頁面



圖8：連結警車行車紀錄器頁面

3.2.2、「顯示定位畫面」功能

「顯示定位畫面」功能將使用者的單位名稱、車牌號碼、即時影像連結所同步的行車紀錄器影像及M-Police定位導航位置呈現於螢幕上，讓使用者確認即時影像畫面及自身定位導航位置使否正常，如圖9。



圖9：顯示定位畫面頁面

3.2.1、「即時影像連結」功能

「即時影像連結」功能以Wi-Fi連結警車行車紀錄器，如圖8。

3.2.3、「進行攔截圍捕」功能

「進行攔截圍捕」功能分為「開始攔截圍捕」與「支援攔截圍捕」兩個選項功能。如圖10。

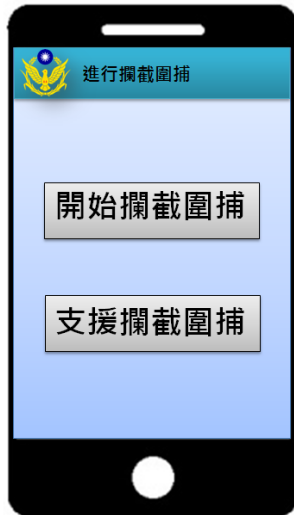


圖10：攔截圍捕頁面



圖12：攔截圍捕之推播訊息

3.2.3.1、「開始攔截圍捕」功能

點擊「開始攔截圍捕」功能，將會顯示開始攔截圍捕畫面，如圖11。使用者發起攔截圍捕的消息會以推播訊息通知所有登入警車即時影像及定位導航視訊系統的警力，如圖12。並由勤務指揮中心人員將即時影像及定位導航位置同步至加入攔截圍捕行動的支援警力所攜帶之M-Police上，如圖13。



圖11：開始攔截圍捕頁面



圖13：支援警力點擊推播訊息後呈現的支援攔截圍捕畫面

3.2.3.2、「支援攔截圍捕」功能

「支援攔截圍捕」功能為自行查看目前是否有正在進行的攔截圍捕行動，若同一時間有多件攔截圍捕行動，該功能頁面將會顯示多筆資料，使用者能夠查看並點擊加入攔截圍捕行動，如圖14。



圖14：於支援攔截圍捕頁面點擊欲加入之攔截圍捕行動

3.3、勤務指揮中心切換畫面功能

勤務指揮中心電腦以分割畫面顯示所有加入攔截圍捕行動之警力的即時影像，如圖15。點擊分割畫面能夠放大單一警力的即時影像畫面，如圖16。定位導航方面則是以位置感知技術整合所有加入攔截圍捕的警力，紅色定位點為目前提供即時影像的警車位置。勤務指揮中心人員可操作切換畫面功能，當其他支援警力追上逃逸車輛時，勤務指揮中心人員能夠點擊左側列表清單，視情況將同步畫面切換成不同警力的即時影像畫面，如圖17。

紅圈表示目前同步的即時影像為該車行車紀錄器畫面
表示由駕駛車牌號碼ABC-1234警車之澄觀派出所員警發起的攔截圍捕行動



圖15：勤務指揮中心畫面分割顯示



圖16：放大單一警力的即時影像畫面



圖17：勤務指揮中心切換同步畫面

3.4、群組軟體功能

使用者參加攔截圍捕行動便是加入攔截圍捕群組，可查看即時影像及定位導

航畫面，並與所有參加攔截圍捕行動之警力對話，以利支援警力互相連絡及勤務指揮中心進行指揮調度。

五、情境模擬

本研究針對警車即時影像及定位導航視訊系統的運用進行情境模擬，狀況如下：2020年10月15日17時45分許，高雄市政府警察局仁武分局澄觀派出所巡邏員警張三、李四於八德西路、八德中路交岔路口攔查駕駛自小客車闖紅燈民眾王五，製單舉發時發現其違法持有一級毒品海洛因(Heroine)，王五見毒品被警方發現便立刻駕車沿八德中路向東逃逸，此時現場員警李四立即拿出M-Police使用警車即時影像及定位導航視訊系統，點選「開始攔截圍捕」功能，由張三駕駛巡邏車、李四於副駕駛座操作M-Police聯絡勤務指揮中心及支援警力，如圖18。並於逃逸車輛後保持安全距離持續尾隨跟車。



圖18：開始攔截圍捕示意圖

仁武分局勤務指揮中心及其他派出所的巡邏警力藉由推播訊息功能得知澄觀派出所警車ABC-1234發起攔截圍捕行動後，立即點選支援攔截圍捕功能加入攔截圍捕群組，由勤務指揮中心人員同步即時影像及位置至各支援警力所攜帶之M-Police上。當仁武派出所支援警力駕駛之ABC-1235巡邏車於八德南路、澄觀路交岔路口靠近逃逸車輛時，勤務指揮中心人員將同步畫面切換為仁武派出所巡邏車ABC-1235的即時影像畫面，如圖19。最後於慈惠一街巷底由三輛警車攔截圍捕逃

逸車輛，如圖20。成功在未發生意外的情況下逮捕違法民眾王五。



圖19：切換同步畫面示意圖



圖20：攔截圍捕成功示意圖

六、結論及後續研究

警車追逐具高度危險性，若只有單一警車追逐逃逸車輛，在孤立無援的情況下難以確保員警自身、追逐對象及其他人的生命、身體安全，因此追捕逃逸車輛應以聯絡支援警力並尾隨在後的方式進行。希望透過本研究之警車即時影像及定位導航視訊系統讓追車員警以攔截圍捕取代單一警車追逐，達到安全逮捕人犯的成果。後續研究方面，可再增加警車即時影像及定位導航視訊系統的功能，以位置感知技術顯示警車追逐現場周圍環境的相關資訊，如即時路況、警察機關位置、道路施工情形等資訊，提供勤務指揮中心人員指揮調度參考；另外在第一線員警方面，若M-Police為螢幕面積較大的平板電腦，也能增加更多顯示於螢幕面板上的資

訊，以提升支援警力攔截圍捕的效率，達到降低警車追逐傷亡的成效。

參考文獻

1. 江建忠，「員警駕駛警車追逐影響因素之研究」，中央警察大學碩士論文，2015，第 33 頁。
2. 考試院，警察人員因公傷殘死亡殉職慰問金發給辦法。全國人事法規釋例資料庫，2013。
3. 安守中，GPS 定位原理及應用，新北市：全華，2005。
4. 林彥伶，「行動車牌辨識與推播技術於犯罪偵查之應用」，中央警察大學碩士論文，2014，第 28~30 頁。
5. 林東清，資訊管理：e 化企業的核心競爭能力，台北市：智勝，2016。
6. 陶冶中，我國發展智慧運輸系統之重要課題：車路協同系統技術發展藍圖與推動策略，國土及公共治理，第三卷，第二期，2015，第 35 頁。
7. 葉俊廷，「行動電信業者之動態競爭策略」，國立政治大學碩士論文，2019，第 5~6 頁。
8. 蔡慶信，「網站伺服器推播技術之架構」，國立中山大學碩士論文，2001，第 1~2 頁。
9. Cheng, Ho Ting; Shan, Hangguan; Zhuang, Weihua, Infotainment and road safety service support in vehicular networking: From a communication perspective. Mechanical Systems and Signal Processing, 2011, pp:2020~2038.
10. Falcone, D. N., Wells, D. N. and Edward, W. L., A study of police vehicle pursuit policy characteristics. Criminal Justice Policy Review, Vol. 9. No. 3-4, 1999.
11. Ferraro, Richard and Aktihanoglu, Murat, Location-Aware Applications, 2011, pp:4-6.
12. Raptis, D. and Skov, M. B., "Continuity in multi-device

interaction: an online study," In proc. of the 9th Nordic Conference on Human-Computer Interaction, ACM, 2016.

5G結合車聯網在交通事故現場重建上的應用

王逸嵐

中央警察大學資訊管理所研究生

im1093062@mail.cpu.edu.tw

董正談

中央警察大學資訊管理所助理教授

tung@mail.cpu.edu.tw

鄧少華

中央警察大學資訊管理所教授，通訊作者

pdeng@mail.cpu.edu.tw

摘要

當發生交通事故時，因現場無路口監視器設備或無相關行車影像畫面，以至於無法順利還原交通事故現場。為了強化影像紀錄在道路交通事故現場重建的運用，車聯網可以收集並處理道路交通網路中每輛汽車的資訊，讓資訊共享，實現人，車，路三位一體互聯，搭配5G行動通訊系統來達成低延遲通訊和大頻寬數據傳輸，即時傳輸行車資訊，如GPS位置、車速、緊急煞車時間點與行車紀錄器之影像…等等資訊傳送至交通雲端資料庫，藉由電腦輔助篩選事故發生周圍車輛之行車影像，加快交通事故之重建。隨著智慧型行動裝置的普及化，幾乎人手一機，可利用推播技術提供使用者更快速的資訊或服務。本研究提出一個雲端電腦輔助交通事故現場重建系統，透過車聯網將每一輛車GPS位置資訊連網上傳，當雲端主機接收到碰撞訊息時，由交通勤務中心操作人員發出指令，要求交通事故現場周遭車輛之行車資訊被動上傳至雲端資料庫，可得知事故車輛及路過車輛之行車資訊，重建交通事故現場，釐清肇事責任歸屬，並提供適地性的交通事故推播訊息服務，提升交通安全及交通事故之鑑識品質。

關鍵字：車聯網、5G、交通事故、現場重建。

一、前言

當交通事故發生後，經第一時間通報，由警察到現場處理，進行現場蒐證、製作筆錄等等，以相機拍攝現場人員倒地位置、車輛停止位置、撞擊點、地面痕跡及散落物位置，並繪製「道路交通事故現場圖」，提供後續行車事故鑑定。但其缺點在於如拍攝角度有限，無法全部延攬入鏡，此外有影像處理偽造的問題，亦無法得知肇事原因及經過。如能搭配行車紀錄器之動態的影像，對於交通事故現場資料蒐集及現場重建還原技術會有相當大的幫助，有助於肇事責任歸屬之判斷，使得鑑定工作更快速，鑑定品質也能提升。

行車紀錄器影像畫面，用於事故現場重建，還原交通行為，釐清事故發生經過與肇事原因。101年至106年間臺灣高等法院及各分院以影像錄影為證據之判決，發現：有 79%是道路交通事故，其中80%屬監視器錄影、16%是行車影像錄影，幾乎全部用於證明碰撞之過程〔3〕。本研究為了強化影像紀錄在道路交通事故現場重建的運用，以5G結合車聯網之

技術，讓行車影像自動上傳至雲端平台，藉由電腦輔助篩選事故發生周圍車輛之行車影像，加快交通事故之重建，以及搭配推播系統建議用路人提早改道。

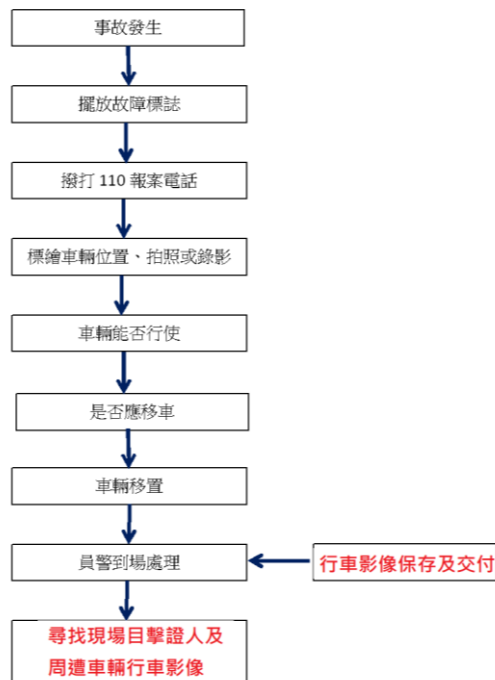
國際研究暨顧問機構Gartner資深研究總監Stephanie Baghdassarian預測，可主動連接5G服務的5G連網汽車，市佔將從2020年的15%增加到2023年的74%，並於2028年達到94%，屆時5G技術將用於蜂巢式車聯網（Cellular-Vehicle to Everything, C-V2X）通訊，使用者不僅可以在汽車內部傳送和接收訊息，亦能在車輛、基礎設施、行人、單車騎士等個體間進行溝通。可主動連線5G服務的聯網汽車，最終有望協助維持交通順暢並提升道路安全〔2〕。

二、研究動機

以109年9月26日於台88線快車道路時，一台黃牌重機遭水產行小貨車從後方高速追上並從右側路肩硬擠側撞，小貨車惡意路肩逼車之行為，導致騎士慘摔重傷。幸好後方車輛

之行車紀錄器錄製到相關影像畫面，有助於交通事故責任歸屬及現場重建。

當發生交通事故時，因現場無路口監視器設備，使當事人可能需要上網尋求目擊證人或相關行車影像畫面，還原交通事故現場案發情形，但並非所有目擊證人皆為熱心人士或是關鍵行車影像畫面因記憶卡容量問題已自動刪除，以至於無法順利還原交通事故現場。交通事故流程圖(圖一)如下。



圖一：交通事故流程圖

如能以車聯網搭配5G通訊系統來達成低延遲通訊和大頻寬數據傳輸，傳輸行車資訊，如GPS位置、車速、緊急煞車時間點與行車紀錄器之影像…等等資訊至交通雲端資料庫，將有助於交通事故之重建，亦能免除當事人尋求其他車輛之影像資訊之困難。

三、研究目的

為提昇道路交通事故處理品質，強化交通事故資料的完整性。交通事故影像資料的取得及其證據性，更是交通事故現場重建的關鍵因素。隨著5G車聯網的發展，使影像能自動上傳至交通雲端系統，具備證據力，自動化交通事故現場之重建，提升交通事故鑑識之品質。本研究的目的在於針對車聯網之行車影像提供一個交通現場重建之自動化架構與方法，來協助第一線交通人員有效地篩選識別事

故影像節省寶貴的現場重建時間，提昇交通事故鑑識之品質。

四、相關文獻與背景知識

1. 車聯網

將車與車連接起來的網絡，就是車聯網，車聯網可收集並處理道路交通網絡中每輛汽車的資訊，讓資訊共享。

車載網路 (Vehicular Ad Hoc Network, VANET) 是建立滿足特定需求或情況的車輛網路，主要目標是在不使用任何集中控制裝置的情況下在車輛之間構建和維持通訊網路。每輛車都成為網路的一部分，管理和控制該網路上的通訊以及自身的通訊要求。近來關於車載網路的研究工作集中在特定領域，例如：路由器，網路流量，服務品質和安全性〔8〕。

車聯網連接近來發展的社交網路車聯網 (Social Internet of Vehicle, SIoV) 系統是 IoV 的現代趨勢，車輛可以共享交通壅塞資訊，道路狀況，天氣狀況，空置停車位和媒體共享等資訊相互交流，需要在車輛實體內建立相互的信任關係，保證車輛駕駛之間的互動安全可靠。在 SIoV 中，車輛可以通過 Wi-Fi，蜂窩網絡或專用的短程通信等傳統通信技術與其他車輛和基礎設施進行通信〔18〕。

車載網路中不同的協議有：

(1) 控制區域網 (Controller Area Network, CAN)

CAN 是車輛中最常見的網路，通常有多種 CAN 網路，如動力總成和舒適。CAN Bus 基本概念，汽車上有 10-20 個電控單元 (Engine Control Unit, ECU)，每個 ECU 與感測器連接，與其他 ECU 交換資訊都需要通訊網路。CAN 匯流排提供 ECU 之間的通訊，構成車載網路系統。每個 ECU 都是網路上的一個節點，藉由 CAN 匯流排的控制器、驅動器，使用二條導線 (不含地線) 連接到下一個節點〔5〕。

(2) 本地互連網路 (Local Interconnect Network, LIN)

LIN 是一種用於非安全關鍵傳感器和執行器系統的低速通訊協議。

(3) 媒體導向的系統傳輸 (Media-Oriented Systems Transport, MOST)

MOST協議允許高寬頻並用於傳輸音頻和視頻數據。環狀架構，環狀連結中斷，就會停止運作，例如音樂位元訊號組依順序撥放，比位元到達準確性重要，所以MOST用在非關鍵性運用，如娛樂系統。

當車禍發生時，車輛會經由自動或手動方式，通報事故位置等相關訊息，以利醫療人員迅速抵達現場並提供適當的醫療服務；在資訊服務部分，電信業者與資通訊業者也以車聯網技術，蒐集即時的交通路況，並提供駕駛動態導航等雲端服務，以避開交通壅塞路段，提升行車效率。隨著智慧型手機的普及，目前車聯網的實作方式之一，是將智慧型手機當作是一個通訊平台與人機介面，透過駕駛人的通訊裝置來收發訊息，可以避免額外通訊服務費用的支出；另一方面，藉由開發智慧型手機的應用程式，可以透過智慧型手機便利的人機介面，來提供各式各樣的新服務〔6〕。

2. 5G

5G是指第五代行動通訊技術，稱之為LTE Advanced (Advanced Long Term Evolution, 進階長期演進技術)，解決目前在4G無法解決的問題與限制。最主要的特徵與特性有三個，分別為：一、速度號稱可比4G最高快到100倍，網路延遲速度不到1毫秒(4G為30~70毫秒)；二、能夠讓往來電信網路承載更多的節點(Node)或是裝置，以應付龐大節點的物聯網(Internet of Things, IoT)應用；三、超可靠度和低延遲通訊(Ultra-reliable and Low Latency Communications, URLLC)，透過超可靠低延遲性，未來可發展出車聯網的應用與遠距即時手術，以降低風險〔7〕。

針對5G所規劃的三大特性與場景，都是由於在無線擷取技術上的突破而有了新的面貌，以下做詳細描述與說明。

(1) 增強型行動寬頻通訊(Enhanced Mobile Broadband, eMBB)

寬頻應用情境可涵蓋不同的傳輸範圍，包括廣域覆蓋和熱點傳輸。對於在廣域覆蓋的情況下，無縫的覆蓋以及較高的移動速度是主要需求。在熱點的應用，主要針對具有高用戶密度的區域，其對於移動性的需求較低，但會需要非常高的數據傳輸量。增強型行動寬頻預期將傳輸速度再提升至下行20G bit/sec、上行10G bit/sec。也就是5G的傳輸速度將是4G傳輸

速度的20倍，或者高於20倍。而這樣的頻寬，將與有線寬頻的頻寬不相上下。

eMBB的用例側重於內容和速度。eMBB有助於增強動態網路配置與管理，按需分配頻寬以滿足訊號接收和速度需求。eMBB的刷新速度更快，而且可以更廣泛地連接各種網路，因此有望改善車間內的無線連接，確保手機或平板電腦上的應用更順暢地運行。

(2) 大規模機器型通訊(Massive Machine Type Communications, mMTC)

為了因應未來5G機器型通訊的各種可能應用情境，mMTC技術的設計必須滿足未來的應用需求。隨著社會的互聯互通程度越來越高，人們需要更多的能量為其提供動力。所謂智慧城市、智慧家庭、智慧能源和公用事業、農業和運輸業都是mMTC的主要5G應用領域，提升邊緣計算和機器對機器應用的規模與速度，同時降低能耗。mMTC的用例有望提高多個領域的機器智能，比如造就智慧農業的拖拉機、為智慧城市帶來互聯交通網的列車等。而在能源和公用事業行業，基於mMTC的監控工具可對更廣泛的實體基礎設施和智慧電網技術進行監控，即時報告並因應不斷變化的情況。

應用於物聯網，藉由嵌入感測器使機器運算能力提升，其所收集的數據即可以傳回雲端並即時運算比對，隨時進行監控，即時反映給使用者，達到更高效能。如NB-IoT智慧停車、智慧城市。

(3) 超可靠度和低延遲通訊

URLLC應用在用戶平面的延遲部分需低至0.5毫秒(ms)以下，錯誤率(Block Error Rate, BLER)在1毫秒的延遲與封包大小為32 bytes的情況下要達到 10^{-5} 以下(3GPP規範：TR 38.913)。URLLC解決了對時間和安全最敏感的訊息傳遞問題，URLLC對自動駕駛汽車遠程設備操控的進一步發展，發揮了至關重要的作用。工廠可能會使用雲計算和網路切片技術以及名為微蜂巢的低功率蜂巢基地台，構建以車間為中心的私有網路，尤其是在IP密集型場所或軍事應用中。除此之外，URLLC還可以幫助自動駕駛車輛相互通訊溝通，以便在接近十字路口或遇到潛在危險時做出明智決策。

以物理特性而言，頻率越高時，訊號就

更易受到干擾或遮蔽，尤其是高頻的毫米波（mmWave），傳輸距離不如低頻頻段。比起4G，5G的使用頻段更高，因此若要提升5G高頻訊號的覆蓋率，勢必要部署更多的基地台。工研院資訊與通訊研究所副所長丁邦安指出，5G時代兩個基地台的距離，是以前4G時代的三分之一至十分之一，未來小基地台布建的密度將大幅提升，保守預估，到了2028年，全球至少有7、800萬台小基站的規模，成為5G時代新的增量市場〔1〕。

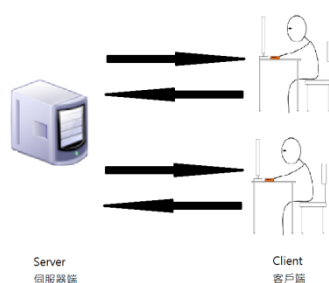
5G扮演重要的角色，支持政府及政策制定者將城市轉化為智能城市，透過5G新的應用和服務提高用戶服務及體驗，GSM協會（Groupe Speciale Mobile Association，GSMA）預計2025年5G連接將達11億個〔16〕。

3. 智慧型行動裝置推播(Push)技術

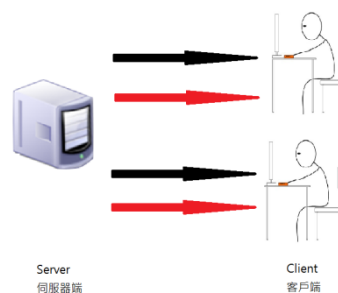
隨著智慧型行動裝置的普及化，可利用推播（Push）技術提供使用者更快速的資訊或服務。

想了解何謂推播，首先要知道什麼是Pull，當伺服器端產生網頁後，使用者必須點入該網頁才可能獲得所需要的資訊或服務，Pull的概念就是必須由使用者（客戶端）花時間主動去連接伺服器端。Pull的缺點就是有時候使用者經過漫長的查詢，卻還看到一堆沒有用或不想要的資訊，於是推播技術順勢而生。推播是將資料主動由伺服器端傳送至使用者，伺服器端掌握資料的控制權，而使用者可以選擇是否想要接收伺服器端推播即時資訊給自己，創造雙贏的局面〔4〕。

Pull與Push的差異以圖二與圖三來說明：



圖二：Pull示意圖



圖三：Push示意圖

以下舉例說明智慧型行動裝置常見的推播技術應用：當有新電子郵件時，電子信箱的應用程式可以在行動裝置的主畫面上跳出訊息，告知使用者有新的電子郵件，有些電子信箱的應用程式甚至提供簡單即時預覽的功能；智慧型行動裝置的推播功能另一種常見的應用，在應用程式有改版時，跳出橫幅提醒使用者更新；也有部分遊戲應用程式利用推播技術提醒使用者有新的關卡可以遊玩。

推播技術是由server端將使用者所需的資料送到使用者的主機上或是使用者指定的地方去，如電子信箱、多點傳送(Multicast)及廣播(Broadcast)等技術。推播技術的優點為：使用者可依自己的喜好，訂閱自己想要得到的資訊；節省使用者到網路上搜尋資料的時間；可在本機上閱讀到最新的資訊，不須讓使用者自己花費時間下載；可大量減輕網路傳輸量；可大量減輕提供資訊之伺服器的負擔〔13〕。

多點傳送是一個技術術語，可以同時將一個封包發送到多個站點，可視為網路的廣播版本。多點傳送的站點在許多方面類似於廣播信號的電視台。單一信號源可以傳送到每個人的信號區域中。在多點傳送網路上，可以從一台電腦發送一個訊息封包到其他數台電腦，取代一次發送一個訊息封包到一台電腦〔17〕。

4. 交通事故現場重建

交通事故現場重建在於描述交通事故中發生的各事件，對人、車在事故發生過程中所有情況合理化描述，如事故發生地點、人與車之行進方向、車速、碰撞之位置。交通事故現場重建指利用已有之資料了解交通事故如何發生，並得知交通事故為何發生。

為了發掘交通事故之真相，重建工作者以事故現場處理資料，經過資料整理、比對與跡證鑑識、重建事故現場；若事故發生過程被監視攝影系統記錄，該視訊影像紀錄就是鑑識

分析的標的，並據以完成現場重建、肇事原因分析與責任鑑定〔9〕。

5. 全球定位系統 (Global Positioning System, GPS) 位置資訊

GPS最初作為美國軍事系統，後來開放給民間使用。透過衛星發射之訊號，接收機接受此訊息，訊息由載波、電碼及導航訊息所組成，解算此訊息可得到使用者之位置、速度等資訊〔14〕。

GPS 行車導航系統，在雲端化的導航趨勢下，結合動態路況，更可經由用路人分享的資訊，將所有最新路況消息傳送至遠端系統進行整合，再將資訊回饋給導航服務，如此 GPS 裝置即可讓駕駛人掌握最即時的路況變化。因此在行動裝置日趨普及的今日，借助 APP 結合行動裝置，能將更多直覺式的行車服務所產生的巨量資料，進行駕駛人行車習慣與旅運行為分析，進而提供個人化的差異服務〔10〕。

當駕駛者一邊存取Google Maps的地圖資訊時，Google Maps也會將駕駛者現在的位置上傳，只要數量夠多，可得知目前的車流量大小。Google Maps會根據政府機關的資料得知行車速限以及歷史資料判斷某些時段的車輛駕駛速度。Google Maps的預測即時路況之功能，其主要是根據駕駛者曾透過手機回傳的地理位置資訊，從出發點和終止點的資料，約略計算出每一台手機移動速度，綜合判斷出路上所有手機在行駛狀態時的資訊，估算分析出這條路是否順暢或回堵的交通量狀況。

五、解決方案—雲端電腦輔助交通事故現場重建系統

國道或快速道路交通事故一直存在事故影像取得困難的現象，長久以來都影響著交通事故現場重建，然而以台灣國內設有密集的107614座基地台設備〔11〕，以及全台手機用戶數為2907.5萬戶〔12〕，故本研究即在探討如何利用現有手機APP(Google Maps) 結合車聯網，打造一個智慧警政交通系統，再將警示的資訊即時推播給線上用路人，來提醒用路人交通現況，提高注意力，以及提早改道通行，降低塞車狀況，維護交通秩序。警方則可利用交通雲端資料庫系統，得知事故之GPS位置，以事故車及事故發生前後一分鐘經過之車輛為調閱行車影像之標的，重建交通事故現場，提升交通事故鑑識之品質，此為本研究題目之



定義。

1. 訊息推播

將交通事故警示畫面及訊息推播給線上用路人知悉，藉由事故駕駛人手機上網使用Google Maps導航功能，得知連接之基地台位置。以方圓三公里之基地台發送交通事故推播訊息給其他用路人，藉此產生提高注意力之效果，並達成交通分流，降低交通壅塞，提升交通安全（圖四）。

圖四：訊息推播

2. 交通雲端資料庫系統

利用Firebase開發交通雲端資料庫系統。Firebase 是一個雲端開發平台，使用者經過申請後便能享有即時雲端服務API，可同時支援 Android、iOS及網頁的App。其中使用Real-time database 能夠即時的將數據存到雲端平台，其他裝置就能立即的存取相同雲端平台的數據，達到即時共享數據的目的，讓開發者可以做到訊息推播系統、即時數據存取等應用。使用 Firebase 的 Real-time database，車輛收到啟動命令便開始動作，並即時發送車載資訊，如GPS、車速、緊急煞車時間點及行車影像紀錄等相關資訊至雲端資料庫系統〔15〕。

以下分為系統簡介、系統架構、系統資料庫設計、系統資料庫主檔設計與系統操作頁面及運作流程，分述如下：

(1) 系統簡介

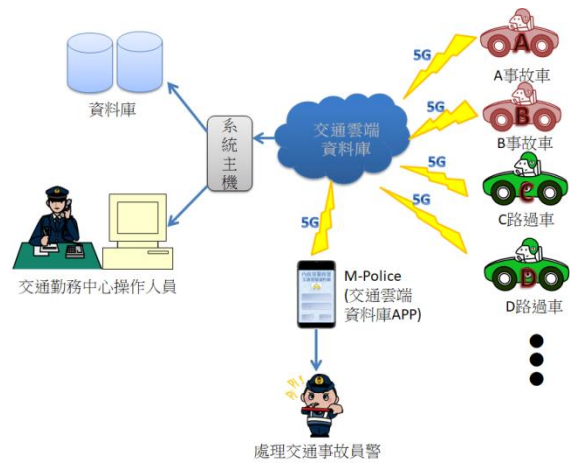
本研究之系統運用車聯網，搭配5G行動通訊、推播技術，當發生交通事故時能將事故車的行車資訊上傳至雲端平台，並以推播技術告知周遭用路人，警示交通路況，且利用電腦輔助功能篩選、編輯相關影片資料，重建交通事故現場狀況，釐清事故發生原因，提升交通

事故鑑識品質，並即時提醒保障其他用路人的安全，更是保障現場執勤同仁之安全。

(2) 系統架構

每輛連網車所產生的行車資料（車輛GPS位置、當時之車速、緊急煞車時間點及行車影像畫面）為非結構性資料，其資料量規模龐大，無法藉由人工方式擷取並處理成對警方有用的資訊，屬於巨量資料。如發生交通事故時將大量行車資料藉由5G行動通訊即時上傳至交通雲端資料庫，這些合法的要求將會癱瘓系統，造成阻斷服務（Denial of Service, DoS）攻擊，使系統無法提供服務或當機。因此，本系統以上傳車輛之GPS位置為原則，被動上傳行車資訊為輔，防止資料量過大而系統無法負荷。當系統主機接收到碰撞訊息時，由交通勤務中心操作人員發出指令，要求事故車及事故前後一分鐘經過之車輛上傳其行車資訊。採用長時間執行的批次作業來處理行車資料，以便蒐集、彙整、處理成警方所需資訊，亦可避免系統資源閒置。批次資料傳輸的順序為優先傳輸事故車行車資訊，再傳輸距離事故車越近之車輛行車資訊，使相關行車資訊接續上傳至交通雲端資料庫。

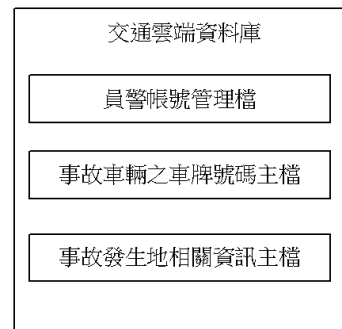
車輛藉由5G行動通訊將行車資料之GPS位置上傳至交通雲端資料庫，當A車與B車發生交通事故時，雲端資料庫會接收到碰撞訊息，並將碰撞訊息傳送至系統主機。系統主機以交通事故發生地方圓三公里為範圍，發出交通事故推播訊息至其他駕駛人手機（C車、D車…），提醒駕駛人注意行車安全並提早改道。交通勤務中心操作人員可操控系統主機，要求交通事故周遭車輛傳輸行車資訊，以電腦輔助方式篩選交通事故關鍵資訊並存放至資料庫中。處理交通事故員警可藉由M-Police登入交通雲端資料庫APP，查詢交通事故相關資訊，重建交通事故現場，釐清肇事責任。系統架構圖以圖五說明：



圖五：系統架構圖

(3) 系統資料庫設計

交通雲端資料庫架構(圖六)由員警帳號管理檔、事故車輛之車牌號碼主檔及事故發生地相關資訊主檔所構成。可記錄員警登入系統之時間，並查詢交通事故之車輛及周遭車輛相關資訊。



圖六：資料庫架構圖

(4) 系統資料庫主檔設計

員警帳號管理檔內容設計（圖七）分為員警帳號、員警密碼、員警個人資訊及員警登入APP的日期及時間，可確認個人資訊是否正確外，登入日期與時間則可作為日後交通勤務中心操作人員查核之紀錄，防止員警將民眾資料外洩或另作他用途。

員警帳號管理檔
員警帳號
員警密碼
員警個人資訊
登入日期與時間

圖七：員警帳號管理檔內容設計

事故車輛之車牌號碼主檔內容(圖八)分為車輛所有人、車輛行照、交通事故發生之GPS位置、事故當時之車速、緊急煞車時間點及行車紀錄器之影像。員警可解由此主檔得知車輛發生事故時之相關訊息，車速是否符合速限，是否有採取緊急煞車行為，並透過行車紀錄器之影像畫面來證明碰撞之過程。

事故車輛之車牌號碼主檔
車輛所有人
車輛行照
事故發生之 GPS 位置
當時之車速
緊急煞車時間點
行車紀錄器之影像

圖八：事故車輛之車牌號碼主檔內容設計

事故發生地相關資訊主檔內容(圖九)所顯示之資料為事故發生時間之前後一分鐘，分為事故發生地及發生時間、周圍之車輛及其車速變化、有急煞行為之車輛及行車影像具事故發生車之車輛。藉由事故發生地及發生時間可確認查詢之資料是否為本身所處理之案件，並可得知周圍車輛有哪些，其車速變化是否有異常，有採取急煞行為之車輛可推論出靠近事故發生地，行車影像具事故車輛之畫面，有助於交通事故責任歸屬及現場重建。

事故發生地相關資訊主檔
事故發生地及發生時間
周圍之車輛及車速變化
有急煞行為之車輛
行車影像具事故發生車之車輛
資料為事故發生時間之前後一分鐘

圖九：事故發生地相關資訊主檔內容設計

(5) 系統操作頁面及運作流程

執勤員警於執勤前，先行領用M-Police並登入警察交通雲端資料庫APP(圖十)，輸入員警帳號密碼登入系統(圖十一)，開始進行查詢事故車輛及相關資訊(圖十二)。由員警帳號管理檔(圖十三)會記錄每次登錄日期及時間，交通勤務中心操作人員可點選登入日期及時間查看哪些車輛被查詢(圖十四)，以免此系統遭非法利用。



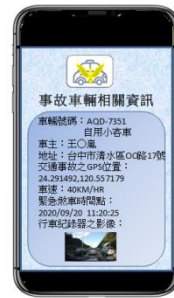
圖十：系統App圖示



圖十一：登入與查詢圖



圖十二：事故相關資訊



圖十六：事故車輛相關資訊查詢內容



圖十三：員警帳號管理



圖十四：登入日期及時間相關資訊圖

點選主檔之事故車輛相關資訊(圖十五)，輸入車牌號碼或車輛所有人即可查詢相關資訊，得知交通事故之GPS位置、當時車速、緊急煞車時間點，以及行車影像畫面(圖十六)。



圖十五：事故車輛相關資訊

點選主檔之事故發生地相關資訊(圖十七)，輸入事故發生時間及發生地或GPS位置即可查詢相關資訊，得知事故發生前後一分鐘之周遭車輛，並可得知車輛相對位置圖，亦能取得其行車影像，有利於現場之重建(圖十八、圖十九)。



圖十七：事故發生地相關資訊



圖十八：事故發生地相關資訊查詢內容



圖十九：事故發生地相關資訊查詢內容之二

五、系統應用與模擬案例探討

1. 模擬案例說明

黃五駕駛自小客車ABC-1234，於2019年10月21日11時20分行駛於國道一號北上204.5公里處擦撞護欄以致車輛翻覆起火燃燒，駕駛人黃五因遭受撞擊當場昏迷，以致逃生不及而身亡，現場交通事故造成車流回堵2公里。

2. 系統應用

黃五駕駛之自小客車ABC-1234搭載車聯網系統，使用5G行動通訊技術連網，將自小客車ABC-1234之GPS位置資訊上傳至交通雲端資料庫。因車聯網車輛感測器接收到碰撞訊息，並傳輸到交通雲端資料庫系統，由交通勤務指揮中心操作人員發出指令，要求事故車ABC-1234及事故當下前後一分鐘路過之車輛傳輸行車資訊至交通雲端資料庫。此外，以駕駛人手機連網之基地台為中心，並結合鄰近基地台發送交通事故推播訊息至方圓三公里之其他用路人，提醒其他用路人改道通行，並保持適當跟車距離，注意行車安全。

自小客車ABC-1234因車輛燃燒，無法現場取得行車紀錄器之畫面，而警方依規定排除事故後，利用M-Police輸入員警帳號及密碼，登入交通雲端資料庫APP，查詢「事故車輛相關資訊」，取得自小客車ABC-1234緊急煞車時間點、車速、行車影像畫面…等等資訊。再藉由「事故發生地相關資訊」查詢事故發生前後一分鐘，周圍可能錄製到關鍵影像之車輛，發現李四駕駛之自小客車ABD-5678有採取緊急煞車行為並且行車影像畫面拍攝到自小客車ABC-1234交通事故發生情形。

經檢驗黃五及李四之行車影像畫面協助重建交通事故現場，釐清肇事責任歸屬為張三駕駛之自小客車XX-0001之惡意逼車行為，導致黃五駕駛之自小客車ABC-1234失控擦撞護欄，以致車輛翻覆燃燒而身亡。

七、結論及後續研究工作

交通與治安為警察工作之核心，面對交通事故時，適當運用資訊科技，可有效提升工作效率、重建交通事故現場。本系統利用5G搭配車聯網，使行車資訊上傳至交通雲端資料庫，提供警方完善的行車資料分析，協助警方有效地篩選識別交通事故影像，節省交通事故現場重建時間，有助於肇事責任歸屬之判斷。後續研究工作，對於交通雲端資料庫系統所獲得的行車相關資料，以區塊鏈方式，使資料上

傳時透過加密方式串連，保障資料的完整性、不可竄改性，加強資料的證明力，提昇交通事故鑑識之品質。

八、參考文獻

1. 工業技術研究院，「攜手臺廠打造5G小基站生態系」，工業技術與資訊，第338期，2020。
2. 王智仁，「Gartner：戶外監視攝影機三年內成為5G物聯網解決方案最大市場」，網管人，第176期，2019。
3. 吳俊良，「影像紀錄運用於事故現場重建之證據力-個案報告」，106年道路交通安全與執法研討會，2017，第20~21頁。
4. 林彥伶，「行動車牌辨識與推播技術於犯罪偵查之應用」，中央警察大學資訊管理研究所碩士論文，2014年，第28~30頁。
5. 邱翊晉，「結合雲端服務與OBD-II之Android車載資訊通平台設計與實作」，樹德科技大學資訊工程系碩士論文，2013，第3~4頁。
6. 莊嶸騰，「前進向雲端的汽車車聯網系統與應用介紹」，彰化：財團法人車輛研究測試中心知識庫，2012。
7. 洪英章，「善用5G三大獨特性生態系結盟創新應用」，網管人，第171期，2020。
8. 連章雄，「車輛鑑識之研究」，執法新知論衡，第15卷，第2期，2019，第77頁。
9. 陳高村、陳祈昇，「視訊影像紀錄之肇事時空關係重建研究」，102年道路交通安全與執法研討會，2013，第235~236頁。
10. 陶冶中，「我國發展智慧運輸系統之重要課題：車路協同系統技術發展藍圖與推動策略」，國土及公共治理，第三卷，第二期，2015，第35頁。
11. 國家通訊委員會，「行動通信業務基地台統計數」，2020。
12. 國家通訊委員會，「2020年第2季行動通訊市場統計資訊」，2020。
13. 黃源龍，「使用行動代理者之互動式推播技術」，成功大學碩士論文，2002，第19~21頁。
14. 蔡亮宇，「使用支持向量機降低GPS定位的多路徑干擾」，國立臺灣海洋大學通訊與導航工程學系碩士學位論文，2018，第1頁。

- 15.薛詩瀚，「小型電動車之可行駛區域搜索與定位」，國立台灣科技大學機械工程系碩士學位論文，2019，第26頁。
- 16.Brahima Sanou, “Setting the Scene for 5G Opportunities and Challenges ” , International Telecommunication Union,2018,pp:3-4.
- 17.Kevin Savetz, Neil Randall and Yves Lepage ,“MBONE: Multicasting Tomorrow's Internet” ,1996 ,chapter3 section1.
- 18.Ricardo Silva and Razi Iqbal, “Ethical Impl-ications of Social Internet of Vehicles Syst-ems”,IEEE10.1109/JIOT.2018.2841969 ,2019, pp:1-3.

現場拍攝取證文字辨識特徵實證研究：以 Google Keep 為例

郭冠呈

中央警察大學資訊管理學系學生

ibaneffiekuo@gmail.com

吳國清

中央警察大學資訊管理學系教授

wkc@mail.cpu.edu.tw

摘要

長久以來，犯罪現場證據保全、扣押證物和設備清冊、現場環境的拍照取證等工作，已經成為警察機關和執法人員在傳統和電腦等犯罪案件的必要程序，其中扣押證物和設備清冊將列入警方移送書的重要一部分。近幾年來，「科技執法」已列入警政署和各級警察機關的警政執法策略。由智慧型手機專用且免費的 Google Keep App 文字辨識功能，將可用於犯罪現場的拍攝證物和證據，並儲存影像和擷取文字。本研究擬透過實證途徑和取得 236 件具代表性的影像（內含文數字和特殊符號）樣本，試圖了解該 OCR 的文字辨識特徵，以供執法人員在使用上的參考依據。研究結果發現：（1）變別字符和偽別字符發生在一個或二個洞同倫等價特徵的文數字上；（2）天氣變化和環境照度等因素對辨識中文字效果影響甚微，它主要來自受照物體的照度，低照度值效果較佳；（3）當兩者距離愈遠、OCR 所需辨識處理時間愈久和字數愈多，會導致中文錯誤字數增加；（4）在 OCR 整體辨識效果上，現場的濕度、目標字數和 OCR 辨識複雜度等為主要影響因素，濕度、字數和複雜度三者愈高，錯誤率愈高；而距離則為次要影響因素。

關鍵字：OCR、拍攝、取證、辨識複雜度。

一、前言

磁條、語音辨識、無線射頻識別、條碼、光學標記識別（Optical Mark Recognition, OMR）和光學字元識別（Optical Character Recognition, OCR）等技術的應用，滿足了電腦自動化的需求[15]。OCR 程序是將掃描過的打字、手寫文字影像轉換為機器可讀的純文字。它是一種將印刷文字轉變成數位化編碼的方法，並可將它電子化儲存、檢索和用於機器處理，如文字到語音、機器翻譯和文字探勘。OCR 技術的應用已經徹底改變了文件管理程序。OCR 技術使掃描過的影像檔案變成完全可尋找或檢索的文字檔案，這些可用來尋找文字內容和可被電腦加以識別[7]。OCR 可以協助人們擷取相關資訊並自動記錄，而且結果很準確，並可在較短時間內處理足夠的資訊。OCR 方法的識別準確度隨著演算法和影像品質的不同而異。文字識別場景有很多的應用，如導航、路標偵測、語言翻譯等。代替條碼

技術的文字標籤可以提供了較為完整的資訊。然而，雜亂的背景和非文字離群值，場景文字識別變得更具挑戰性。此外，字元類型（Character Type）（如英數字或中文字）、字體類型（Font Type）（如細明體、標楷體等）和字體大小等不同的文字態樣（Text Patterns），也增加了它的識別困難度[16]。隨著智慧型手機的高速處理器、記憶體容量的大幅提升、極高畫素的攝影機和 5G 行動資料或 Wifi 的高速網路傳輸速率，並結合雲端硬碟，使得更有利於 OCR 的發展與多元應用的實現。

隨著科技的創新應用愈來愈廣，最熱門的「科技執法」已成為現今警政署和各級警察機關的推動重點。它除了用於提升整體警察執法效能之外，也試圖解決「警政治理」的警力不足問題。另一方面，由於資通訊的快速發展和國人使用手機的高普及率，使得資訊安全威脅事件和電腦犯罪案件，並沒有隨著警方「科技執法」的普遍實施，而有明顯減緩的跡象。因而

如何「善用科技」以提升偵查鑑識能力，使能在短時間內破案，有效嚇阻犯罪發生，成為警方推動與落實「科技執法」所要面對與有待解決的議題。

警方第一線執法人員，如何進行犯罪現場證據保全，並可透過科技執法工具快速取得嫌疑犯或被害人所留下的可疑證據，是極為關鍵的。以偵辦相關電腦犯罪為例，偵查人員實施搜索扣押之法定程序外，對電腦或手機的動態取證（Live Acquisition）和靜態取證（Dead Acquisition）成為必要偵查手段，例如螢幕上出現正在下載違反《兒童及少年性剝削防治條例》規定的情色圖片；還有在犯罪現場所貼張犯罪用的資訊或器物等。基於此，這些犯罪情境都是無法透過電腦或手機數位鑑識工具來進行動態取證，但皆是不利於嫌疑犯的被訴事實。因而，現今偵查人員如何透過攝影或拍照之機器設備，以獲取現場拍攝與擷取有價值的證據和證物，並設法轉換成「足以為表示用意之證明」，已成為警察機關偵查犯罪的必要程序，如我國《警察偵查犯罪手冊》第一百七十一條第二、三項之對扣押物應「照相或錄影，並應加以編號、記載細目」規定。然而，這些細目絕大部分都是印刷在扣押物上，例如，廠牌名稱，一長串的 S/N 序號或品名等資訊。偵查人員可能做法是透過電腦文書編輯軟體，如 Microsoft Word，來逐字敲打與核對它們。但這種做法卻與「善用科技，以提升偵查鑑識能力」有明顯落差，另則增加偵查鑑識人員的工作負荷。鑑此，如何善用科技來減輕工作負荷，以提升偵查鑑識整體效能，是警政署和各級警察機關所要共同面對的難題。

現今，用於各家廠牌和機種的智慧型手機專用且免費 Google Keep App 除了可以記事、編輯、提醒、共用外，還提供一項強大功能，就是光學字元識別（OCR）。持有手機使用者可透過手機極高畫質的鏡頭拍攝具有文字的物體，並立即將剛拍完的影像進行擷取圖片文字，透過網路即可將圖片內文字轉成可被編輯的文字，另還可與使用者帳號的電子郵件取得自動同步或透過電腦 Google Keep 同步存取 Google 雲端硬碟內該影像和文字內容等。

使用這項功能，即可讓使用者很快速「即拍即識」之圖文並存與對照，這對往後將文字複製貼上 Word 編輯區十分方便，可以大幅減少傳統字元識別過程所需時間。因此，偵查鑑識人員可以透過個人手機或警用 M-Police 和 Google Keep 軟體，來完成犯罪現場拍攝和取證等執法工作。不過，由於犯罪現場情境複雜和多樣化，且取證時間又受到法院核發的搜索扣押令狀之時間限制，衍生出因偵查鑑識人員對於 Google Keep OCR 在不同情境下文字辨識特徵的不了解，而導致「事倍功半」問題發生，甚至於不如由人工敲打來得快，反而增加工作負荷，寧願捨棄「科技執法」。

為了解決上述難題，本研究擬以 Google Keep 作為研究工具，透過個人手機在不同之地點、情境（背景）和目標物等情況下，進行當場手機拍攝與立即擷取圖片文字。經過長達七個月時間（考量不同時間之氣候、濕度和地區關係），總計蒐集到 236 件有效樣本。本研究人員透過實證方法、研究設計（各種變數）和撰寫程式碼，來進行資料之洗清、處理、統計分析和結果解釋，希望達到以下之研究目的：

- （1）OCR 文字辨識發生變辨字符（變造）和偽辨字符（偽造）有那些？如何以拓撲學理論來解釋這些誤辨發生的字符共通特徵？
- （2）OCR 文字辨識與那些背景因素有關聯？又有那些背景因素不具關聯？
- （3）試圖了解 OCR 辨識那些錯誤字符具有相關性？
- （4）試圖找出影響 OCR 辨識中文字錯誤數和整體字符錯誤數的因素？

二、文獻綜述

1. OCR 基本原理

OCR 的概念，首先由德國科學家 Tausheck 於 1929 年提出，後來美國科學家 Handel 依其概念為基礎提出了對文字進行辨識的構想，而這個構想直到電腦的問世，並結合光學掃描技術將其轉換為電腦編碼才正式實現。隨著 OCR 技術發展的成熟，其識別對象從印刷字體轉向手寫

字體，到了1974年OCR在西方國家被廣泛應用，如信件分類和生活層面上[3]。

OCR 基本原理就是透過掃描器（或拍照圖）將一份文件的影像輸入給電腦，然後由電腦取出影像內每一個文數字，並將其轉換成編碼的文數字。其具體工作過程是，掃描器將中文字文件透過電荷（感光）耦合元件（Charge Coupled Device, CCD）將文件的光信號轉換為電信號，經過類比數位轉換器轉化為數位訊號傳輸給電腦。電腦接收到文件的數位影像，其影像上的文數字可能是印刷、雕刻或手寫形式，然後對這些影像中的文數字進行識別（Recognition）。對於印刷字體，首先採用光學方式將文件資料轉換成原始黑白點陣的影像檔案，再透過識別軟體將影像中的文字轉換成文字編碼格式，以便供文書處理軟體的進一步人工(Artifact)編輯。因此，文字識別是OCR的重要技術[3]。

2. OCR 文字識別過程

光學文字辨識(OCR)指透過光學技術與電腦技術將影像中的印刷字體或雕刻、手寫字體辨識為電腦能夠識別之電子訊號，其識別過程主要分為下列階段：[2]

- (1) 分割單字階段：OCR 軟體會將影像中之文字、數字與符號分割出來。
- (2) 單字細線化階段：細線化是將不等寬度的字體經過多次的循環取捨，將寬度細化為由一個點素所構成的（輪廓）線，又稱為骨架化（Skeletonizing）。OCR 軟體透過將單字的線條變細，僅針對其骨架進行辨識，藉以排除可能造成誤判的錯誤或無意義資料量。
- (3) 擷取單字特徵點階段：OCR 技術透過各種演算法分析進行文字中最具辨識的圖案特徵(Pattern Features)，並針對精簡化的文字進行編碼，最後將結果儲存於軟體的識別資料庫（Recognition Database）內。
- (4) 比對、校正和輸出階段：OCR 軟體將精簡化與編碼的文字骨架與後台的識別資料庫進行比對，逐一檢視與特徵最相近的文字，而該文字即為最後辨識結果，直到所有文字均

被辨識完成後，再進行語意校正和產出最終結果，即影像所相對應的OCR文字檔。其中語意校正是根據前後文義（Context）的關聯，及統計模型，如隱藏式馬可夫模型（Hidden Markov Model, HMM），來進行語意校正[4]。

3. OCR 與機器學習探討

人工神經網路（Artificial Neural Networks, ANN）也稱為類神經網路或連接模型（Connectionist Model），是對人腦或自然神經網路（Natural Neural Network）基本特性的抽象和模擬。人工神經網路以對大腦的生理研究成果為基礎的，其目的在於模擬大腦的某些機理與機制，實現某個方面的功能。國際著名神經網路研究專家 Hecht Nielsen[1]將人工神經網路定義為：「由人工建立的以有向圖為拓撲結構的動態系統，它透過對連續或斷續的輸入作狀態相應而進行資訊處理。」隨著深度學習（Deep Learning）的興起，OCR 技術便以全新的思路突破了傳統架構所遭遇的瓶頸（如藝術字體、低解析度、分均勻光照、字元型變、多語言混合、檢測框字元殘缺等等）。深度學習為機器學習（Machine Learning）的分支和分散表示（Distributed Representation），其透過模仿生物中樞神經系統的人工神經網路對函式進行運算、估計，以對目標資料反覆進行特徵學習。現今，透過深度學習結合OCR技術的主流實現架構主要有卷積神經網路（Convolutional Neural Network, CNN）、循環神經網路（Recurrent Neural Network, RNN）和連結時間性分類（Connectionist Temporal Classification, CTC）損失演算法等[5]。

4. OCR 與相關研究

在電腦視覺（Computer Vision）中，影像（Image）內文字的擷取是一項具有挑戰性的任務。文字擷取在提供有用和有價值的資訊方面發生重要作用[6]。光學字元辨識是一種技術，它可以將影像形式的文字或符號轉換成電腦中文字編碼格式

(Encoding Format)。OCR 是人工智慧和圖形識別 (Pattern Recognition) 的熱門研究領域之一，帶給人類在日常生活中的高度實用性。利用 OCR 技術已經開發了許多商用應用軟體。包括驗證碼圖像[14]，自動號牌 (車牌) 識別[10]，文件資訊擷取[6]等。

在開發 OCR 系統的過程中會出現幾個問題。首先，電腦在識別與其他數值有相似性的數值時可能會有困難。例如：電腦很難正確判斷英文字母 "l" 和數字 "1"。其次，當擷取有背景雜音的特徵時，比如字體和紙張的對比，字體後面的圖片等等，將會使辨識錯誤率增加。為了提高光學字元辨識 (OCR) 的準確率，許多研究人員已經發展出多種研究方法和不同的演算法，並做出顯著的貢獻。

- (1) 2008 年，Malon 和他的團隊[9]，在「支援向量機的數學符號識別」研究中，使用支援向量機 (Support Vector Machine, SVM) 來識別圖中的數學符號，使用 SVM 以提高 InftyReader 方法在分類數學符號方面的性能，結果發現 SVM 可成功地將錯誤率降低到 41%。
- (2) 2011 年，Ramana Murthy 等人[11]提出一種用基於分區式特徵擷取 (Zoning Based Feature Extraction) 進行字元識別的新技術。做法上，字元影像被劃分為預先定義好的區域 (Zones)，並從每個區域中計算出一個特徵 (Feature)。這個特徵是基於該區域中包含的圖案 (黑色) 畫素 (Pixels)。這些特徵包括平均畫素密度、平方和距離和直方圖 (Histogram) 等。但是平均畫素密度、畫素的不同組合位置等特徵，都會產生相同的平均畫素密度，導致分類上的錯誤。文章提出一種新的技術，就是應考慮圖案畫素位置 (Pattern Pixel Location)，並儘可能去貢獻獨特的特徵。
- (3) 2013 年，Ghai 等人[6]使用了自我調整局部連接圖 (Adaptive Local Connectivity Map, ALCM)、期望值最大化 (Expectation Maximization,

EM)、最大化機率 (Maximization Likelihood, ML)、馬可夫隨機場域 (Markov Random Field, MRF)、螺旋式運行長度塗抹演算法 (Spiral Run Length Smearing Algorithm, SRLSA) 和曲線變換 (Curvelet Transform) 等多種方法，用於從掃描的書籍封面、期刊、多色文件、手寫文件、古文件和報紙檔等影像中擷取文字。文件中的文字取決於各種因素，如語言、風格、字體、大小、顏色、背景、方向、波動的文字線、交叉或接觸的文字線等。從混淆矩陣中獲得召回率 (Recall Rate)、精確率 (Precision Rate)、所需處理時間 (Processing Time) 和準確度 (Accuracy) 等方面，來幾種文字擷取方法進行效能的比較。結果發現，準確率 (98.53%) 以混合 (連接元件和紋理分析) 方法和基於邊緣的文字擷取技術為最佳。精確率 (96%) 和召回率 (93%) 在 EM 演算法和 ML 分割方法的情況下是最好的。處理時間 (1.17 秒) 在使用 Haar 小波的數位濾波器的情況下是最好的。對於手寫文字影圖像，準確度 (99.5%) 以 ALCM 和基於直方圖投影的方法最好。

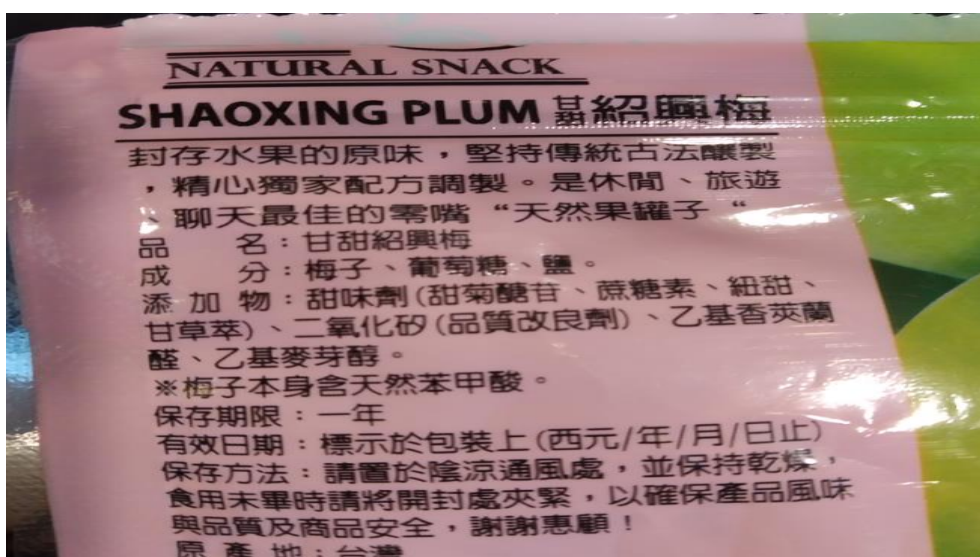
- (4) 2015 年，Mahto 等人[8]提出一種結合水平和垂直投影特徵擷取方法來識別 Gurmukhi 的手寫字元。該實驗使用 SVM (線性和多項式內核) 和 k-NN ($k=1, k=3, k=5, k=7$) 對手寫字元進行分類。結果使用線性 SVM 獲得 98.06% 的極高準確度。
- (5) 2016 年，由 Rao 和他的研究團隊[12]，進行一項名為「光學字元辨識技術演算法」的研究，他們提出一種基於人工神經網路之反向傳播的光學字元辨識方法的修正版，該方法成功計算出錯誤率，並在 OCR 中獲得 100% 的準確度。
- (6) 2017 年，Sahu 等人[13]針對 OCR 技術和模型進行研究，用以解決光學字元辨識的假設和數字模型問題。他們認為光學字元辨識 (OCR) 和

磁性字元識別 (Magnetic Character Recognition, MCR) 技術通常被用來識別圖案或字母。一般來說，字母是以各種影像圖片形式出現，可以是手寫的，也可以是印刷的，或者是任何系列、形狀或方向、角度等。另外，在 MCR 中，字母是用磁性油墨印製的，研究機器根據每個字母所形成的專屬磁場對字母進行分類。MCR 和 OCR 在銀行和不同的貿易設備中都有應用到。

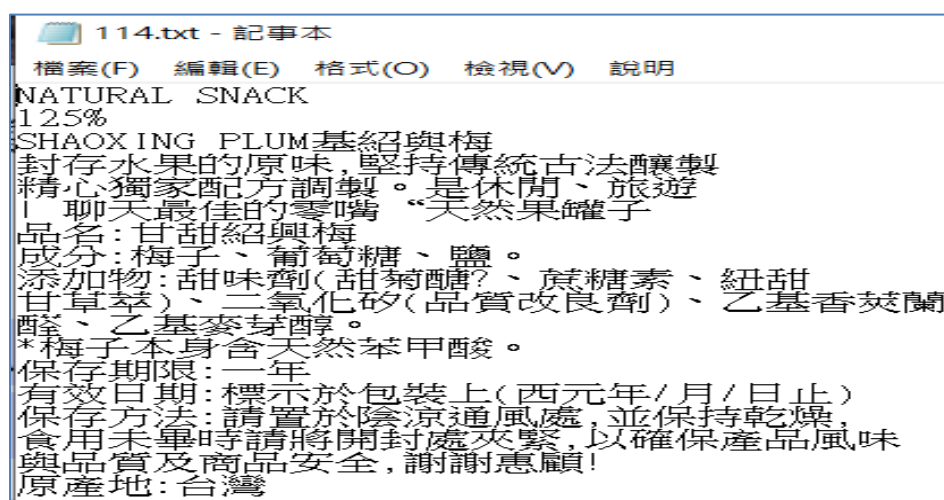
三、研究方法

1. 資料來源

本研究人員透過手機 Google Keep 所提供的拍攝功能，在不同環境因素(如地點、濕度、溫度、空氣汙染等)、人為操作(如距離、角度等)和不同目標物體等，進行實地拍攝，並將 JPEG 影像檔案和 Google Keep OCR 軟體進行擷取文字後，儲存至 Google 雲端內。實地拍攝取樣時間從 2019 年 12 月 14 日至 2020 年 7 月 29 日止，取得有效樣本共 236 件 (影像檔案數)。圖一為數位影像原始 JPEG 檔案範例，其透過 Google Keep OCR 辨識後的相對應文字內容，如圖二所示。



圖一：經手機拍攝的數位影像原始 JPEG_114 檔案範例



圖二：JPEG_114 檔案經由 Google Keep OCR 辨識成文字檔案 114.txt 範例

2. 研究工具

- (1) 攝影設備：本研究以智慧型小米手機針對目標物進行拍攝，手機型號為 Redmi 7，CPU 核心數為 8 核心（最高 1.80GHz）、相機最高畫素為 1200 萬像素。
- (2) OCR 軟體：由於 Google Keep 為免費軟體，內建的 OCR 文字辨識功能亦不需付費即可使用，且其具有簡單操作之使用者圖形介面，十分適合刑事執法人員在犯罪現場取證之用。故本研究採用它，並在 Android 作業系統（版本為 9 PKQ1.181021.001）環境操作之。
- (3) 程式開發：DOS 指令，Excel VBA，R 語言，及 Stata MP-16 ado Script 劇本語言等。

3. 實施步驟

為達成本研究之目的，擬依照下列步驟逐步實施之：

- (1) 數位影像拍攝：透過智慧型手機對目標樣本進行拍攝，依照拍攝次序以阿拉伯數字對影像檔進行命名，並以 JPEG 檔案儲存之，以利檔案管理。
- (2) 記錄數據：現場拍攝時記錄時間、地點、溫度、濕度、氣壓、空氣汙染指數、風速、環境照度、距離、目標物材質（含木頭、塑膠、紙類、金屬、含藝術字的看板、電腦和手機螢幕…）、目標照度等，依照檔案編號將其登錄於 Excel 工作表中。
- (3) 擷取檔案內容：透過 Google Keep 軟體將研究樣本匯入，使用其內建之 OCR 功能擷取文字，並記錄辨識完成所需時間、樣本字數等。過程中若發現辨識時間超過 15 秒或顯示「無法辨識，請稍後再試」，即捨棄該次紀錄，關閉並重新開啟 Google Keep 後再次辨識之。若重複超過 3 次則該資料視為無效。若辨識成功，則將文字複製至記事本當中，採 ANSI 編碼系統儲存。

- (4) 計算影像和文字錯誤字數：這是一項十分費時工作，完全必須仰賴研究人員去處理共計 236 個 JPEG 和 236 個 TXT 檔案，逐檔比較與計算出 OCR 的錯誤字數。
- (5) 處理與分析：研究人員撰寫 DOS 指令（批次檔），Excel VBA，R 程式和 Stata MP-16 ado 程式等，來對 236 個 TXT 檔案和背景數據 Excel 檔案進行處理，然後產出 CSV 檔案供 Stata MP-16 進一步資料處理與統計分析。

四、研究結果與討論

1. 敘述統計

變辨字符（變造）係指在受照目標物內存在的文字或符號，但被 Keep OCR 錯誤辨識變成其他文字或符號。偽辨字符（偽造）係指受照目標物內不存在的文字或符號，但被 Keep OCR 錯誤辨識成是文字或符號。從表一結果顯示，這兩者交集 = {O, o, 6, E, 9, a}。為了解釋此一 OCR 的辨識錯誤結果起見，本文採用拓撲學概念。依拓撲特性，對於特定物件（稱為拓撲空間）在特定變換（稱為連續映像）下具有不變性質。拓撲等價可分成同胚和同倫等價等兩個類型。兩個空間同胚係指若一個空間不須切開或黏合即可變形成另一個空間。若兩者都可由某個較大的物件「壓扁」而成，兩個物件就可被視為同倫等價。例如，O 有一個洞，R 有一個洞及兩個尾巴，故兩者是不同的胚；但因為 R 的尾巴可被壓扁成「洞」的一部分，所以 O 與 R 具有同倫等價關係。從表一可歸納出，變辨字符同倫等價 = {{0, 4, o, 9, R, a, 6}, {8, B, 日}, {E}}；偽辨字符同倫等價 = {{o, 6, 9, D, O, a, e}, {3, E}, {1, -}}。這一研究結果顯示，刑事偵查人員在犯罪現場透過手機拍攝與取得具有文字符號之影像證據時，{O, o, 6, E, 9, a} 是容易被手機 OCR 辨識錯誤的。其誤辨發生的字符共通特徵是具有一個或二個洞的字符。

表一：OCR 誤辨的變辨字符和偽辨字符排序後前 11 個字符統計

變辨字符	發生次數	偽辨字符	發生次數
0	6	o	7
E	6	6	6
4	5	1	5
o	5	9	5
8	4	D	5
9	4	O	5
R	4	a	5
a	3	e	5
6	3	-	4
B	3	3	4
日	3	E	4

此外，本研究人員從拍攝樣本數為 236 件影像檔案，以逐檔開啟和透過人眼去辨識相片內的文字內容和字形組成。大致可歸類成{英數字,中文字,藝術字,特殊字符}等 4 大類型。然後根據這 4 個類型的不同組成，組成數量多寡和外觀輪廓等考量因素，來決定 OCR 辨識的複雜度。

例如，複雜度=1，表示該張相片只存在英數字。從表二結果顯示，在全部 236 張相片中，以英數字的 45 張最多，其次是{特殊字符,中文字,英數字}的 43 張，僅為藝術字者為 24 張，{英數字,中文字}計 23 張；複雜度最高者，即由「其他」所組成的，計 26 張。

表二：OCR 辨識複雜度與其相對應字形組成統計

OCR 辨識複雜度	目標物字形組成	發生次數	所占百分率
1	{英數字}	45	19.07
2	{中文字}	17	7.20
3	{藝術字}	24	10.17
4	{特殊字符}	1	0.42
5	{英數字, 中文字}	23	9.75
6	{英數字, 藝術字}	7	2.97
7	{藝術字, 中文字}	4	1.69
8	{英數字, 特殊字符}	19	8.05
9	{中文字, 特殊字符}	9	3.81
10	{特殊字符, 藝術字, 英數字}	14	5.93
11	{特殊字符, 中文字, 英數字}	43	18.22
12	{特殊字符, 藝術字, 中文字}	4	1.69

13	其他	26	11.02
總計	—	236	100.00

2. OCR 辨識與背景因素關聯檢定

當利用手機鏡頭拍攝目標物時，OCR 辨識效果可能會受到當時情境因素而影響到它的準確度，包括天氣和照度。由表三研究結果顯示，(1) 環境照度 (Illuminance) 與辨識英數字沒有關聯 (卡方值=4.2036；機率值 = 0.649) (未表列呈現)；(2) 環境照度與中文字辨識沒有關聯 (卡方值=11.595；機率值 = 0.237)；(3)

OCR 辨識效果也不會受到當時的天候影響 (卡方值=6.4331；機率值 = 0.376)；(4) 辨識效果與目標物照度強弱有極顯著的關聯 (卡方值=57.873；機率值 = 0.000)，且呈現正向關聯 (Gamma = +0.6685)，這意味著目標物照度超過 20 Lux，太亮就易造成中文辨識效果差。總之，天氣和環境照度等因素對 OCR 辨識效果影響甚微，反而是受照物體的照度大小影響顯著。

表三：天氣、照度與中文字辨識關聯檢定結果 (N = 236)

發生次數		中文錯誤等級					卡方關聯檢定
		0	1	2	3	列總計	
天氣	晴天	107	46	7	6	166	likelihood-ratio chi2(6) = 6.4331; Pr = 0.376; Cramér's V = 0.1195; gamma = -0.0087
	陰天	26	7	5	2	40	
	雨天	21	5	3	1	30	
	行總計	154	58	15	9	236	
目標物 照度 (註)	<= 20	144	54	15	6	219	likelihood-ratio chi2(3) = 57.873; Pr = 0.000; Cramér's V = 0.5960; gamma = 0.6685
	>20	10	4	0	3	17	
	行總計	154	58	15	9	236	
環 境 照 度	小於 100	20	7	1	3	31	likelihood-ratio chi2(9) = 11.595; Pr = 0.237; Cramér's V = 0.1264; gamma = 0.0842
	100-299	81	30	6	2	119	
	300-599	23	11	3	0	37	
	600 以上	30	10	5	4	49	
	行總計	154	58	15	9	236	

註：照度定義為被照物體單位面積所受照光通量 (Luminous Flux, Lux)，即光通量密度。照度太低，易導致眼睛疲勞，太高則刺眼。

3. OCR 辨識字符錯誤數相關分析

從表四皮爾森相關分析結果得知，只有特殊字符辨識錯誤數與中文字誤辨數、英數字誤辨數等具有顯著的正相關。這意

味著 OCR 對特殊字符辨識錯誤數增加時，將會使中文字和英數字誤辨數增加之「共伴效應」。

表四：OCR 對不同字符發生辨識錯誤之字數相關分析 (N = 236)

辨識錯誤相關值	藝術字誤辨數	特殊字符誤辨數	中文字誤辨數	英數字誤辨數
藝術字誤辨數	1.0000	—	—	—
特殊字符誤辨數	-0.0050	1.0000	—	—

中文字誤辨數	-0.0949	0.2826***	1.0000	—
英數字誤辨數	-0.0001	0.1582*	0.0288	1.0000

註：*: prob < .05；***: prob < 0.001。—表示對稱矩陣 $A_{ij}=A_{ji}$ 。

4. 線性迴歸分析

由於刑事執法人員在犯罪現場為了在很短時間內進行取證工作起見，其可行做法是透過個人手機立即拍攝可疑物體（含電腦或手機等設備和畫面內容），試圖去獲取圖片和擷取相對應文字，以作為數位證據之用，因而，執法人員會特別關注在中文字的辨識效果上。由表五線性迴歸結果顯示，中文字錯誤字數（因變數）

顯然受到距離、OCR 辨識所需處理的時間、目標字數等變數的影響（如模型一）。當手機和拍攝物距離愈長、處理時間愈久和所需辨識的字數愈多者，則中文字錯誤字數就會明顯增加。不過當考慮藝術字體字數後，處理時間對中文字錯誤字數的影響明顯降低，取而代之的是藝術字體字數（如模型二）。當目標物的藝術字體字數愈多，會使中文字錯誤字數很顯著降低。

表五：影響中文字錯誤字數因素線性迴歸分析 (N = 236)

參數估計值	線性迴歸模型：中文字錯誤字數（因變數）	
自變數名稱	模型一	模型二
距離	.043759***	.0408993***
處理時間	.323003*	.3039041+
目標字數	.0095048***	.0143185***
藝術字體字數	—	-.0172574***
F 檢定	F(4, 232) = 23.15; Prob > F = 0.0000; R-squared = 0.2853	F(3, 233) = 24.70; Prob > F = 0.0000; R-squared = 0.2413

註：+: prob. < 0.1；*: prob. < 0.05；***: prob. < 0.001。

—表示該變數未列線性迴歸模型內。

如從辨識錯誤字總和（因變數）角度分析之，表六線性迴歸分析顯示，（1）模型一顯示出濕度、溫度、空氣汙染、目標物照度、環境照度、距離、處理時間和目標字數等自變數中，只有濕度和目標字數對辨識錯誤字總和有顯著的影響，尤其是目標字數。當濕度愈高或目標字數愈多，將會造成 OCR 辨識效果愈差。（2）當只考慮濕度、目標字數和 OCR 辨識複雜度

時（模型二），濕度影響度反而增加，辨識複雜度太高很容易增加辨識錯誤。（3）若將距離考慮進來（模型三），它影響辨識錯誤字總和數略為增加（prob. < 0.1），不如它對中文字錯誤字數的很顯著影響（prob. < 0.001）。因此，影響任何辨識錯誤字數因素，主要為現場的濕度、目標字數和 OCR 辨識複雜度等。

表六：影響辨識錯誤字總和因素線性迴歸分析 (N = 236)

參數估計值	線性迴歸模型：辨識錯誤字總和（因變數）		
自變數名稱	模型一	模型二	模型三
濕度	3.821605*	3.571038***	2.805512**

溫度	-.0004178	—	—
空氣汙染	.0090583	—	—
目標物照度	.0040746	—	—
環境照度	.0007564	—	—
距離	.0445672	—	.0451208+
處理時間	.0467823	—	—
目標字數	.018258***	.0118529*	.0117864*
OCR 辨識複雜度	—	.3048968**	.2936831**
F 檢定	F(8, 228) = 22.34; Prob > F=0.0000; R-squared=0.4394	F(3, 233) =63.00; Prob > F=0.0000; R-squared =0.4479	F(4, 232)=48.45; Prob > F= 0.0000; R-squared=0.4552

註：+：prob. < 0.1；*：prob. < 0.05；**：prob. < 0.01；***：prob. < 0.001。

—表示該變數未列線性迴歸模型內。

四、結論

有關本研究結論如下：

- (1) 因 OCR 辨識錯誤所造成的變別字符和偽別字符，發生在一個或二個洞的文數字同倫等價特徵上。
- (2) 就 OCR 辨識中文字效果上，天氣變化和環境照度等因素對影響甚微，主要來自受照物體的照度值影響。低照度值效果較佳。
- (3) 特殊字符辨識錯誤數對中文字誤辨數和英數字誤辨數等有顯著正相關。
- (4) 當手機和拍攝物距離愈遠、OCR 處理時間愈久和所需辨識的字數愈多者，則中文字錯誤字數就會明顯增加。
- (5) 濕度和目標字數對辨識錯誤總字數有顯著影響，尤其是目標字數。當濕度愈高或目標字數愈多，將會造成 OCR 辨識效果愈差。
- (6) 影響 OCR 整體辨識效果，現場的濕度、目標字數和 OCR 辨識複雜度等

為主要影響因素；手機和受照物體之間距離，只為次要影響因素。

參考文獻

1. MBA 智庫百科，「人工神經網路」，<https://wiki.mbalib.com/zh-tw/人工神經網路>，2020/09/01。
2. PLUSTEK 公司，「什麼是 OCR？」，數位蘋果網，<http://www.fuji.com.tw/posts/1889>，2009/09/12。
3. 每日頭條，「淺談 OCR 技術的發展及應用」，<https://kknews.cc/tech/oykk2qm.html>，2017/04/11。
4. 維基百科，「光學字元辨識」，<https://zh.wikipedia.org/zh-tw/光學字元辨識>，2020/09/30。
5. 維基百科，「深度學習」，<https://zh.wikipedia.org/wiki/深度學習>，2020/09/10。
6. Ghai, D., Jain, N., “Text Extraction

- from Document Images- A Review,”
International Journal of Computer
Applications (0975 – 8887) (84: 3) 2013,
pp: 40-48.
7. Kanagarathinam, K., Sekar, K., “Text
Detection and Recognition in Raw
Image Dataset of Seven Segment
Digital Energy Meter Display,” Energy
Reports (5) 2019, pp: 842-852.
 8. Mahto, M. K., Bhatia, K., Sharma, R. K.,
“Combined Horizontal and Vertical
Projection Feature Extraction Technique
for Gurmukhi Handwritten Character
Recognition,” International Conference
on Advances in Computer Engineering
and Applications 2015, pp: 59-65.
 9. Malon, C., Uchida, S., Suzuki, M.,
“Mathematical Symbol Recognition
with Support Vector Machines,” Pattern
Recognition Letter (29: 9) 2008, pp:
1326-1332.
 10. Qadri, M.T., Asif, M., “Automatic
Number Plate Recognition System for
Vehicle Identification Using Optical
Character Recognition,” International
Conference on Education Technology
and Computer 2009, pp: 335-338.
 11. Ramana Murthy, O. V., Hanmandlu, M.,
“Zoning based Devanagari Character
Recognition,” International Journal of
Computer Applications (0975 - 8887)
(27: 4) 2011, pp: 21-25.
 12. Rao, N. V., Sastry, Dr. A.S.C.S.,
Chakravarthy, A.S.N.,
Kalyanchakravarthi, P., “Optical
Character Recognition Technique
Algorithms,” Journal of Theoretical and
Applied Information Technology (83: 2)
2016, pp: 275-282.
 13. Sahu, N., Sonkusare, M., “A Study on
Optical Character Recognition
Techniques,” The International Journal
of Computational Science, Information
Technology and Control Engineering (4:
1) 2017, pp: 1-15.
 14. Sharma, S., Seth, N., “Survey of Text
CAPTCHA Techniques and Attacks,”
International Journal of Engineering
Trends and Technology (22: 6) 2015, pp:
240-245.
 15. Weigelt, K., Hambsch, M., Karacs, G.,
Zillger, T., Hubler, A. C., “Labeling the
World: Tagging Mass Products with
Printing Processes,” IEEE Pervasive
Computing (9: 2) 2010, pp: 59-63.
 16. Yi, C., Tian, Y., “Scene Text
Recognition in Mobile Applications by
Character Descriptor and Structure
Configuration,” IEEE Transaction
Image Process (23: 7) 2014, pp:
2972-2982.

社群媒體網站鑑識效率之比較分析 - 以Facebook為例

黃蘭萱

中央警察大學資訊管理研究所碩士生

im1073087@mail.cpu.edu.tw

王朝煌

中央警察大學資訊管理系教授

jwang@mail.cpu.edu.tw

摘要

社群媒體鑑識為數位鑑識新獨立出的領域，隨著社群媒體的普及，與社群媒體相關的犯罪日漸增加，使社群媒體鑑識也日趨重要。在國外雖已有許多社群媒體鑑識的相關研究，然而國內相關研究偏重於使用者端設備的鑑識，例如：電腦中透過瀏覽器留下的資料、手機應用程式儲存在本機端的資料。本研究主要探討的是社群媒體業者網站系統端資料的鑑識方法，包括「透過應用程式介面擷取資料」、「透過網路爬蟲擷取資料」以及「手動擷取資料」三種鑑識方法。本研究以Facebook為例，實驗三種方法擷取網站系統的使用者資料和貼文內容兩種數位證據，並比較三者時間效率的差異，得到時間效率以「透過應用程式介面擷取資料」為最佳，亦發現「透過網路爬蟲擷取資料」及「手動擷取資料」可取得帳戶中的所有資料。本研究歸納最有效率的社群媒體網站鑑識方式為：先透過應用程式介面擷取數位證據，再根據目標資料的資料量，決定要以「透過網路爬蟲擷取資料」還是「手動擷取資料」的方式來擷取其他相關數位證據。

關鍵字:社群媒體網站鑑識，社群媒體快照，網路爬蟲，應用程式介面。

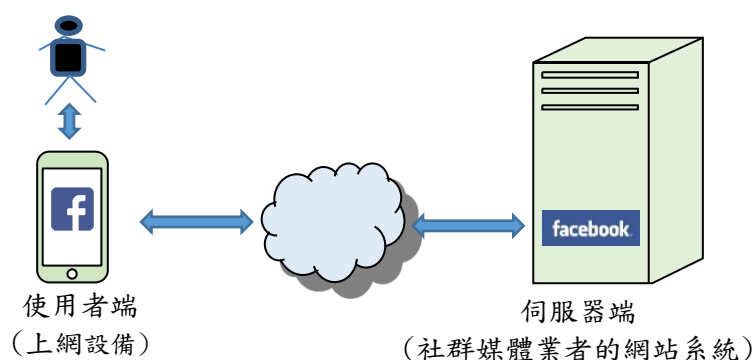
一、前言

隨著資訊科技的進步，電腦科技的應用也越來越貼近人們的日常生活，甚至改變人們交際及互動的型態。最明顯的例子如：Web 2.0 技術的流行，讓使用者與網頁可有雙向的互動，而使用者與使用者之間透過網頁產生的連結，逐漸勾勒出社群網路(Social Network)的雛形，也進一步使得社群媒體被人們廣為應用。

然而，社群媒體的廣為應用，讓人們對於社群媒體的使用越來越依賴，使得與社群媒體有關的犯罪案件也跟著呈現增加的趨勢，且隨著犯罪智慧化，社群媒體已經成為犯罪的重要媒介之一。常見的社群媒體犯罪案件如：社群媒體的使用者對其他使用者進行網路霸凌(Cyberbullying)、網路騷擾(Cyber-Harassment)、網路跟蹤(Cyberstalking)、網路詐騙、網路身分竊用、或散布假新聞(Fake News)製造民眾恐慌

等。為了追訴這類犯罪案件，執法機關須在社群媒體中尋找得以佐證犯罪的資料以作為數位證據，使得社群媒體鑑識顯得越來越重要。

根據社群媒體的架構，儲存在社群媒體的資料主要分為在使用者端與在伺服器端，如圖一所示。使用者端指的是使用者的上網設備，包含行動裝置或桌上型電腦；伺服器端則是指社群媒體業者的網站系統。社群媒體中的數位證據，除了在被告或嫌犯的上網設備外，社群媒體業者的網站系統更是大部份資訊的儲存場所。使用者端及網站系統的資料均需加以蒐集，才能更完整地進行社群媒體鑑識[1]。我國關於社群媒體鑑識的相關研究主要以使用者端的資料蒐集[3]-[5][7]為主。本研究嘗試透過應用程式介面、網路爬蟲或手動方式擷取伺服器端資料，探討社群媒體網站的鑑識方法。



圖一：社群媒體架構圖

由於社群媒體資料具高度動態性，因此本研究除了瞭解社群媒體網站鑑識的方式外，更著重於探討社群媒體網站鑑識的效率。本研究藉由比較分析不同的社群媒體網站鑑識方法在時間效率的差異，藉以歸納較佳的社群媒體網站鑑識方式。本研究以Facebook為例，說明比較社群媒體網站鑑識方法的時間效率差異。本文組織如下：第二節探討社群媒體網站鑑識、應用程式介面及網路爬蟲，第三節說明本研究的研究設計，第四節為實驗結果分析，最後一節為結論與建議。

二、文獻探討

以下分別探討「社群媒體網站鑑識」、「應用程式介面」與「網路爬蟲」之相關文獻。

1. 社群媒體網站鑑識

社群媒體鑑識(Social Media Forensics)，又稱社群網路鑑識(Social Network Forensics; Social Cyber Forensics)，是網路鑑識(Cyber Forensics)中的一環，為近幾年蓬勃發展中的領域。社群媒體鑑識主要在於調查社群媒體中資訊角色之間的關係，可能是個體與個體間的關係，也可能是一個群組或一個組織相互的關係，值得一提的是一個資訊角色可不只擁有一個社群媒體帳戶，另一方面，社群媒體鑑識亦有擷取社群媒體中的數位證據之目的，所包含的資料包括社群媒體中的使用者資料、貼文內容，以及與這些資料相關聯的中繼資料(metadata)等等，例如：地理位置、IP位址、時間戳記[3]。

在社群媒體鑑識時所擷取到的資料，又常以「社群媒體快照(Social Snapshot)」稱之，指的是擷取某一時間點或極短的時間內的網站狀態及其資料內容[12]。這是因為社群媒體鑑

識相較於傳統數位鑑識，在數位證據蒐集上需有更多的時間考量。社群媒體的證據本質為動態的資料，隨時都有可能因為相關使用者的操作而有所變動，擷取網站系統資料的時間越短，資料的變動範圍也相對較少。

社群媒體的數位證據，一部分可能存放在被告或嫌犯的上網的終端設備，大部分則是儲存在社群媒體業者的網站系統(參圖一)[1]。本研究探討擷取後者資料的鑑識方法，即「社群媒體網站」的鑑識方法。

2. 應用程式介面

應用程式介面(Application Programming Interface, API)是一種本地端使用者與遠端系統軟體程式之間銜接的介面，使用者可透過API執行軟體程式所提供的功能，也就是說使用者可直接透過API的連線，來呼叫(call)遠端網站或應用程式的一些功能，即可獲得其相關應用[6]。

API又可分為作業系統級API及非作業系統級API[13]。本研究所使用到的API為Web API。Web API屬於非作業系統級的自訂API。根據維基百科，Web API定義為針對網頁伺服器或網頁瀏覽器的API，基於開發的概念，通常是用以限制網頁應用程式的用戶端，因此透過API大多無法獲得伺服器端或瀏覽器端的詳細資訊[14]。

本研究所使用的API為社群媒體網站Facebook所提供的API—圖形API(Graph API)。根據Facebook的官方文件，Graph API是欲在Facebook上開發應用程式的使用者(開發者)使應用程式得以讀取或寫入Facebook中社交關係資料的主要方法。Graph API以HTTP協定為基礎，讓開發者以程式設計的方式，讓欲開

發的應用程式執行Facebook的多項操作，例如：發文、查詢資料等[11]。

3. 網路爬蟲

網路爬蟲(Web Crawler)指的是可以自動化替使用者蒐集網頁資訊的程式。維基百科的定義為能夠自動瀏覽全球資訊網的網路機器人，透過抓取網頁上的資訊，以達到編纂網路索引的目的[15]。網路爬蟲是透過遞迴拜訪網頁中的連結，有系統地瀏覽目標URL的網站，同時取得快照頁面，以儲存並檢視網頁。因此早期擷取社群媒體網站中的線上資料，皆是使用網路爬蟲的方法[9]。

網路爬蟲的工具不勝枚舉，以程式語言的角度來看，目前網路爬蟲的程式以JAVA和Python這兩種程式語言為大宗。本研究使用的網路爬蟲工具是Selenium工具，該工具可支援Java、C#、Ruby、Python多種語言，為一種自動化瀏覽的工具。本研究以程式模擬成一般的使用者透過瀏覽器使用網頁的行為，向網站伺服器送出請求，取得回應後，再從其中取得所需要的資訊[10][16]。

三、研究設計

以下分別說明「研究方法」與「實驗設計」。

1. 研究方法

為了擷取儲存在社群媒體業者網站系統中的數位證據，本研究使用了三種社群媒體網站鑑識的方法，分別是「透過API擷取資料」、「透過網路爬蟲擷取資料」和「手動擷取資料」。

根據台灣網路資訊中心2019年臺灣社群媒體的市場調查[2]，國內使用率最高的社群媒體為Facebook。因此本研究選擇Facebook進行研究，對該網站「使用者資料」及「貼文內容」兩種資料，比較不同社群媒體網站鑑識方法在時間效率的差異。

2. 實驗設計

以下分別說明「實驗環境」、「實驗項目」與「實驗步驟」。

2.1 實驗環境

本研究的實驗是使用筆記型電腦進行實體機器的社群媒體網站鑑識。電腦的品牌為ASUS華碩，型號是S400C，所安裝的作業系統為Windows 10 家用版64-bit版本，處理器為i5-3317U CPU，記憶體為12G。

實驗選擇的社群媒體為Facebook，該網站為2020版。由於Facebook在各類瀏覽器均可進行API及網路爬蟲的操作，因此本研究選擇Google Chrome瀏覽器進行實驗，瀏覽器版本為86.0.4240.75。

在Facebook透過API擷取資料所需使用到的工具為Graph API，此工具是Facebook開發給使用者取得帳號中的資料，目前線上可用的版本有6.0版、7.0版與8.0版。在Facebook透過網路爬蟲擷取資料所需使用到的工具為Selenium的Python套件，Selenium版本為3.141.59。本研究透過Spyder軟體作Python開發環境，所使用的Spyder版本為3.3.6。

本研究所使用的實驗環境與工具彙整歸類如表一：

表一：實驗環境與工具彙整歸類表

類別	軟／硬體名稱	型號／版本
設備	ASUS 華碩的筆記型電腦	S400C
作業系統	Windows	10 家用版
社群媒體網站	Facebook	V 2020
瀏覽器	Google Chrome	V 86.0.4240.75
API 工具	Graph API	V 7.0/6.0/8.0
網路爬蟲工具	Selenium	V 3.141.59
Python 開發環境	Spyder	V 3.3.6

2.2 實驗項目

本研究以Facebook為例進行社群媒體網站鑑識，分別以三種不同的社群媒體網站鑑識方式：「透過API擷取資料」、「透過網路爬蟲擷取資料」及「手動擷取資料」，針對「使用者資料」及「貼文內容」進行擷取，並記錄下三種社群媒體網站鑑識方法所需時間。本研究實驗可分為兩個部分，分別為：

(1)擷取「使用者資料」數位證據時，三種不同的社群媒體網站鑑識方式（API、網路爬蟲及手動）所需的時間。

(2)擷取「貼文內容」數位證據時，三種不同的社群媒體網站鑑識方式（API、網路爬蟲及手動）所需的時間。

針對兩種資料分別以三種鑑識方式進行實驗，本研究的實驗又可再細分為六項子實驗：

- (1)實驗A1：「透過API」擷取「使用者資料」所需的時間。
- (2)實驗A2：「透過網路爬蟲」擷取「使用者資料」所需的時間。
- (3)實驗A3：「手動」擷取「使用者資料」所需的時間。
- (4)實驗B1：「透過API」擷取「貼文內容」所需的時間。
- (5)實驗B2：「透過網路爬蟲」擷取「貼文內容」所需的時間。
- (6)實驗B3：「手動」擷取「貼文內容」所需的時間。

2.3 實驗步驟

本研究依照社群媒體網站鑑識方式的不同，分別有不同的實驗步驟，以下分為「透過API擷取資料的實驗步驟」、「透過網路爬蟲擷取資料的實驗步驟」以及「手動擷取資料的實驗步驟」。

2.3.1 透過API擷取資料的實驗步驟

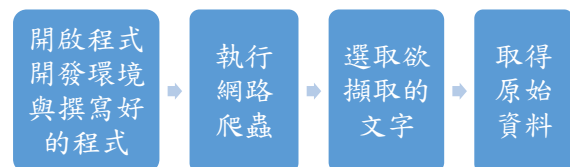
透過API去擷取Facebook中的資料，所採取的流程如圖二所示：



圖二：透過API擷取Facebook資料之流程圖

2.3.2 透過網路爬蟲擷取資料的實驗步驟

透過網路爬蟲去擷取Facebook中的資料，所採取的流程如圖三所示：



圖三：透過網路爬蟲擷取Facebook資料之流程圖

2.3.3 手動擷取資料的實驗步驟

手動去擷取Facebook中的資料，所採取的流程如圖四所示：



圖四：手動擷取Facebook資料之流程圖

四、實驗結果分析

本研究選擇Facebook這個社群媒體網站，對該網站系統中的「使用者資料」以及「貼文內容」數位證據做擷取，以進行社群媒體網站鑑識，比較並分析擷取的效率。即針對「使用者資料」和「貼文內容」兩個數位證據面向，分別進行「透過API擷取資料」、「透過網路爬蟲擷取資料」及「手動擷取資料」三種方式進行鑑識實驗，並進一步比較分析三者擷取的時間差異。

研究者在操作三、研究設計中的2.2實驗項目所述之六項實驗時，每項實驗皆在同一時段進行，以確保實驗環境一致。且各項實驗均操作十次，記錄各次實驗所花費的時間，再予以計算平均及變異數，以作為實驗結果。其中，所需時間的計算，為「從登入系統開始，一直到資料以文字儲存為另一檔案完成為止」所經過的時間。

以下分別為「擷取『使用者資料』數位證據之實驗結果分析」、「擷取『貼文內容』數位證據之實驗結果分析」以及「實驗之其他比較分析」。

1. 擷取「使用者資料」數位證據之實驗結果分析

擷取「使用者資料」數位證據之實驗為三、研究設計中的2.2實驗項目所述的實驗A1、實驗A2及實驗A3，三項實驗均操作十次，又再進一步計算出平均與變異數。三種不同社群媒體網站鑑識方法擷取使用者資料各次所花費的時間及其平均與變異數，如下表二。

表二：三種不同社群媒體網站鑑識方法擷取使用者資料所花費的時間

	透過API擷取使用者資料	透過網路爬蟲擷取使用者資料	手動擷取使用者資料
第一次	41.70秒	58.20秒	2分27.95秒
第二次	42.70秒	57.66秒	2分25.70秒
第三次	40.15秒	58.46秒	2分26.46秒
第四次	38.87秒	58.37秒	2分23.67秒
第五次	43.22秒	59.15秒	2分20.98秒
第六次	41.90秒	57.74秒	2分15.44秒
第七次	42.58秒	58.89秒	2分17.37秒
第八次	43.10秒	59.10秒	2分14.23秒
第九次	40.30秒	58.75秒	2分11.79秒
第十次	42.52秒	59.05秒	2分18.44秒
平均	41.70 秒	58.54秒	2分20.20秒
變異數	1.912844	0.267761	28.228241

其中，三種不同社群媒體網站鑑識方法擷取使用者資料所花費的時間平均分別為：「透過API擷取使用者資料」為41.70秒，「透過網路爬蟲擷取使用者資料」為58.54秒，而「手動擷取使用者資料」為2分20.20秒。

由上可知，「透過API擷取使用者資料」時間效率最佳。研究者認為原因在於Facebook所提供的API工具—Graph API，功能強大且便利，大多功能僅須透過點選按鈕或下拉式選單的欄位即可完成資料的擷取，因此透過API擷取使用者資料時間效率最佳。

值得一提的是，三種不同社群媒體網站鑑識方法擷取使用者資料，十次實驗的操作時間變異數，以「透過網路爬蟲擷取使用者資料」最小，「透過API擷取使用者資料」稍大，「手動擷取使用者資料」最大。代表「透過網路爬蟲擷取使用者資料」所需時間較為接近，但「手動擷取使用者資料」所需時間差異較大。研究者認為這是因為手動擷取數位證據的方式，因全程為人為操作，在操作的過程相較於電腦自動化操作較為不穩定，且人為操作部分越多的社群媒體網站鑑識方式，鑑識所需時間的差異越大。

2. 擷取「貼文內容」數位證據之實驗結果分析

擷取「貼文內容」數位證據之實驗為三、研究設計中的2.2實驗項目所述的實驗B1、實驗B2及實驗B3，三項實驗均操作十次，又再進一步計算出平均與變異數。三種不同社群媒體網站鑑識方法擷取貼文內容各次所花費的時間及其平均與變異數，詳如表三。

表三：三種不同社群媒體網站鑑識方法擷取貼文內容所花費的時間

	透過 API 擷取貼文內容	透過網路爬蟲擷取貼文內容	手動擷取貼文內容
第一次	54.89秒	2分31.47秒	3分57.49秒
第二次	55.25秒	2分33.44秒	3分56.23秒
第三次	48.57秒	2分32.67秒	3分51.68秒
第四次	45.30秒	2分33.52秒	3分52.89秒
第五次	46.79秒	2分33.90秒	3分51.06秒
第六次	46.33秒	2分32.37秒	3分47.98秒
第七次	47.98秒	2分32.56秒	3分49.70秒
第八次	54.68秒	2分32.99秒	3分50.03秒
第九次	53.72秒	2分33.42秒	3分50.15秒
第十次	42.52秒	2分59.05秒	3分18.44秒
平均	50.59秒	2分32.85秒	3分51.64秒
變異數	14.136316	0.501361	8.501881

其中，三種不同社群媒體網站鑑識方法擷取貼文內容所花費的時間平均分別為：「透過API擷取貼文內容」為50.59秒，「透過網路爬蟲擷取貼文內容」為2分32.85秒，而「手動擷取貼文內容」為3分51.64秒。

由上可知，「透過API擷取貼文內容」時間效率最佳。主要因為Facebook所提供的API工具—Graph API功能強大且便利，大多功能僅須透過點選按鈕或下拉式選單的欄位即可完成資料的擷取，因此透過API擷取貼文內容的時間效率最高。

研究者將三種不同社群媒體網站鑑識方法擷取使用者資料所需的時間，分別計算出十次實驗操作時間的變異數，並比較變異數大小，發現以「透過網路爬蟲擷取使用者資料」最小，「透過API擷取貼文內容」稍大，「手

動擷取使用者資料」最大，代表「透過網路爬蟲擷取使用者資料」所需時間較為接近，但「手動擷取使用者資料」所需時間差異較大。主要因為手動擷取數位證據的方式全程為人為操作，在操作的過程相較於電腦自動化操作較為不穩定，而透過網路爬蟲又相較於透過API擷取數位證據又更多自動化的過程，也就是說人為操作部分越多的社群媒體網站鑑識方式，鑑識所需時間差異越大。

3. 實驗之其他比較分析

本研究主要著重在不同社群媒體網站鑑識方式在鑑識時間效率的比較分析，然而研究者發現雖然已有鎖定相同的目標擷取資料，但不同社群媒體網站鑑識方式可取得到的資料量並不一致，研究者為在相同基準上比較時間效率，因此擷取之資料範圍有所限制，以避免基準不同使得比較意義不大。

而在界定限制範圍的過程，研究者發現無論是「擷取使用者資料數位證據」，還是「擷取貼文內容數位證據」，三種社群媒體網站鑑識方法中，都是以「透過API擷取資料」所得的資料量最少，研究者認為在於API可擷取到的資料被社群媒體業者限制許多權限，使得API並無法取得帳戶中的所有資料，而透過網路爬蟲或手動方式皆是以「正常」連線方式瀏覽網站，因此兩者均可取得帳戶中的所有資料。

除此之外，「透過網路爬蟲擷取資料」及「手動擷取資料」兩種社群媒體網路鑑識方式，所取得的資料量也略微不同。研究者認為跟網頁結構與頁面的圖形化配置相關。由於網路爬蟲是事先撰寫好的程式，該程式擷取的資料是根據網頁中HTML的元素去做選擇，因而可能同時會擷取到在同一元素中並非目標資料的名目資料或廣告，例如：確認、贊助等等。同樣地，這也會發生在手動擷取資料的狀況，但因研究者在擷取資料時會再加以判斷是否為所需資料，因此不必要的資料會相較網路爬蟲擷取到的資料少。而手動仍會擷取到非目標資料的原因在於選取時的時間效率，為了節省選取時間，當選取的範圍僅有少部分非目標資料時，研究者仍會直接選取，以避免為了剔除其中的非目標資料而耗時更多，而這正是影響資料量多寡的原因。但是，以使用者資料的項目或貼文內容的貼文數來看，「透過網路爬蟲

擷取資料」及「手動擷取資料」是一致的，因此研究者認為雖然這兩種社群媒體網路鑑識方式所取得的資料量略微不同，但這是合理、可被允許的操作誤差。

五、結論與建議

社群媒體網站鑑識依照擷取數位證據的方式，主要可以分為「透過API擷取資料」、「透過網路爬蟲擷取資料」以及「手動擷取資料」三種社群媒體網站鑑識方式。

本研究以Facebook為例，針對上述三種社群媒體網站鑑識的方式，分別擷取使用者資料及貼文內容兩種數位證據，進行時間效率的比較。在擷取使用者資料數位證據時，時間效率以透過API擷取資料所花費的平均時間41.70秒為最佳，而在擷取貼文內容數位證據時，時間效率也以透過API擷取資料所花費的平均時間50.59秒為最佳。

由上可知，在時間效率皆以透過API擷取資料的效率為最佳，研究者認為這與Facebook所提供的API工具最為相關。由於Graph API功能方便且齊全，大多功能僅須透過點選按鈕或下拉式選單的欄位即可完成所需資料的選擇，因此透過API可快去擷取所需要的數位證據，是社群媒體網站鑑識時間上最有效率的方式。

研究者再進一步進行比較分析，計算出三種不同社群媒體網站鑑識方法在十次實驗操作所花費時間的變異數。無論是擷取「使用者資料」數位證據之實驗結果分析，還是擷取「貼文內容」數位證據之實驗結果分析，變異都是以「透過網路爬蟲擷取使用者資料」最小，「手動擷取使用者資料」最大。研究者認為這是因為手動擷取數位證據的方式，因全程為人為操作，而透過網路爬蟲幾乎都是電腦自動化操作，在操作的過程人為操作相較於電腦自動化操作較為不穩定，也就是說當人為操作部分越多的社群媒體網站鑑識方式，所花費的時間差異就越大。

然而，在實驗過程中，研究者發現透過API擷取資料的資料量最少，研究者認為原因在於API可擷取到的資料被社群媒體業者限制許多權限，使得API並無法取得帳戶中的所有資料，而透過網路爬蟲或手動方式皆是以「正常」連線方式瀏覽網站，因此兩者均可取得帳戶中的所有資料。

綜合而言，研究者認為最有效率的社群媒體網站鑑識方式為：透過API擷取資料的社群媒體網站鑑識方式為最佳。畢竟社群媒體網站資料是隨時變動的，擷取資料的時間越短，網站資料的變動越少，社群媒體網站鑑識的公信力就容易被肯定。透過API擷取資料後，可再用手動或網路爬蟲擷取相關資料。若資料為有限固定欄位，例如：使用者資料，直接透過手動擷取資料即可；但若無法預測資料筆數時，例如：貼文內容，則可透過網路爬蟲擷取資料較有效率。

最後，由於採用不同的鑑識方法，可擷取到的資料範圍亦會有所不同。未來對於社群媒體網站鑑識效率的比較標準可以更廣，例如：從擷取的資料數量或內容，進行更進一步的比較分析。

參考文獻

1. 王朝煌 (2020)，社群媒體鑑識 - 以行動上網為例，明辨雜誌，第十二期，取自 <https://www.hclf.org.tw/issues/eb42>。
2. 台灣網路資訊中心 (2019)，2019台灣網路報告 - 服務應用概況。取自 https://report.twinc.tw/2019/TrendAnalysis_globalCompetitiveness.html。
3. 林靖祐 (2018)，社群網路鑑識之研究：以Dcard與LinkedIn為例 (碩士論文)，取自臺灣博碩士論文系統。(系統編號106CPU05396004)
4. 孫揚展 (2016)，社群網路鑑識-以Google+、Twitter及LinkedIn為例 (碩士論文)，取自臺灣博碩士論文系統。(系統編號104CPU05396004)
5. 陳志達 (2015)，Facebook社群網路服務鑑識—以Windows 10環境為例 (碩士論文)，取自臺灣博碩士論文系統。(系統編號103CPU05396009)
6. 許郁文 (譯) (2017)，圖解雲端技術 | 基礎架構x運作原理x API (原作者：平山毅、中島倫明等)，臺北：碁峰資訊。
7. 賴宥霖 (2017)，社群網路鑑識之研究：以Instagram、Pinterest與Tumblr為例 (碩士論文)，取自臺灣博碩士論文系統。(系統編號105CPU05396016)
8. Al-khateeb, S., & Agarwal, N. (2019), 4.1 – Social Cyber Forensics Analysis (SCF):

- Using Maltego, Deviance in Social Media and Social Cyber Forensics: Uncovering Hidden Relations Using Open Source Information (OSINF), Springer, pp. 67-70.
9. Arshad, H., Jantan, A., & Omolara, E. (2019), "Evidence collection and forensics on social networks: Research challenges and directions," *Digital Investigation*, vol. 28, pp. 126-138.
 10. Bing Guo. "網路爬蟲淺談," Medium.com. <https://reurl.cc/Z7AkAM> (accessed Sep. 9, 2020).
 11. Facebook for Developers. Graph API. Online at <https://developers.facebook.com/docs/graph-api>. Accessed April 13rd, 2020.
 12. Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., & Weippl, E., (2011), "Social snapshots: Digital forensics for online social networks," *Proceedings of the 27th annual computer security applications conference*, pp. 113-122.
 13. Wikipedia. Application programming interface. Online at https://zh.wikipedia.org/wiki/Application_programming_interface. Accessed April 13rd, 2020.
 14. Wikipedia. Web API. Online at https://en.wikipedia.org/wiki/Web_API. Accessed November 2nd, 2020.
 15. Wikipedia. Web crawler. Online at https://en.wikipedia.org/wiki/Web_crawler. Accessed October 21st, 2020.
 16. Zino Lin. "Python Selenium 自動化登入FB 爬首篇貼文-windows 版(附程式碼與教學影片)," Medium.com. <https://reurl.cc/GrxvRA> (accessed Sep. 9, 2020).

治安監錄攝影機畫面偏移異常自動偵測：以桃園市警用監視錄影系統為例

蕭天佑

中央警察大學資訊管理學系研究生

eric_friendex@hotmail.com.tw

顏志平

中央警察大學資訊管理學系助理教授

peter@mail.cpu.edu.tw

林曾祥

中央警察大學資訊管理學系教授

jslin168@mail.cpu.edu.tw

摘要

桃園市政府警察局建置之天羅地網監視錄影系統為國內少數採用影像集中後端儲存之架構，且攝影機數量逐年快速增加中，根據統計，畫面模糊異常與鏡頭偏移異常為兩大主要報修原因，已逐漸造成機關人力檢查的高度負擔。由於近年自動化與智慧化已成為警用監錄系統發展方向，其中攝影機是否能自動自我檢測異常，將直接影響人力維護成本。目前有多項研究針對攝影機偏移異常提出可行作法，但其資料來源多數為室內環境與採用人為加工方式，且其方式有使用情境之限制。我們希望能夠提出符合現行系統架構且具高度可行性之策略，所以我們建議使用基於深度學習的方式，並結合高效率的低階電腦視覺作法，利用監視錄影系統實際擷取之照片進行驗證，提出適合實務上執行自動化偏移異常檢測之解決方案。

關鍵字：深度學習、物件偵測、攝影機偏移、監錄攝影機

一、前言

1. 研究動機

在全國均仰賴監錄系統輔助偵辦案件的情況下，桃園市建置之天羅地網監視錄影系統為國內少數採用影像集中後端儲存之架構，且攝影機數量逐年快速增加中，目前已突破20,000支，然而該局警力數歷年均維持於3,000餘名，經統計桃園市每月須使用6,000人次的警力進行每日查修，其中以2019年全年度攝影機異常報修統計資料顯示，全年度人力報修總件數約為5,700件，其中鏡頭模糊及偏移之比例已超過85%。

我們先前針對鏡頭模糊偵測已提出基於深度學習的解決方案，且能符合實務單位現有監視錄影系統的需求與預算限制、使用高效率、高實現性的架構，在此目標下我們利用具有輕量化、高效率的darknet框架，並普遍獲得超過95%的辨識率，且darknet模組具有輕量化及辨識效率佳的優點[1]。

所以我們將目光轉移到第二大報修主因「偏移異常」，目前桃園市警用監錄系統攝影機日常維護方式，除由系統針對攝影機斷訊具有自動檢測機制外，需仰賴大量員警於每日特

定時段登入系統進行目視檢查，相當耗費人力，且未來攝影機建置數量仍持續增加，人力檢查效率恐日益下降，不利整體監錄系統整體之維護。

2. 研究目的

所有攝影機都須經過安裝、調校後進行攝錄，當攝影機正常供電運作下，攝錄畫面發生與初始設定狀態畫面不同，使人類無法透過其攝影機獲取原預期可取得之資訊時，即視為攝影機異常。程克羽在[2]中認為，攝影機異常事件可分為畫面無法保持清晰和錯誤的拍攝視野兩類，另外Sidnev A.定義的三種攝影機異常態樣中，偏移異常指的是攝影機受到重新定向[3]。偏移異常的成因眾多，也因此有不少研究[2,4]提到受自然或人為影響造成攝影機移動使得拍攝角度改變、大風或地震搖晃後使拍攝畫面改變等，或者風的吹動、輕微的地震或光影變化等造成錯誤的誤判。

我們觀察桃園市政府警察局監錄系統施工方式，每支警用監視器由廠商依據招標規範內之施工預定圖，於施工階段會同機關人員進行確認後安裝，攝影機經調校完成驗收後會先

儲存數張標準照片，作為警察局調閱平台內

「每日檢查」系統之比對基準照片。



(a)



(b)

圖一：車道攝影機正常情形(a)、車道攝影機偏移異常(b)

我們檢視許多偏移異常的攝影機案例，偏移態樣除了往左、右、上及下外，也發現有大量上偏與大量下偏之狀況(如圖一)，我們分析此類異常主因有3種：使用之鎖具設計問題、金屬束帶老化、保養或維修人員操作不當，上述狀況均導致攝影機夾具失去固定能力，造成大角度偏移而拍攝地面或天空等情形(如圖二)。

我們希望持續透過基於深度學習的做法，建構一個能自動檢測各攝影機發生偏移異常之作法，當戶外攝影機偏移超過正常範圍能夠自動偵測為偏移異常，並進行通報機關或廠商人員到場維修，甚至可取代傳統警察同仁須以人力監看，改為以系統自動檢測為主，人力檢測為輔之方式，有效減輕員警工作負荷量。



(a)



(b)



(c)



(d)



(e)



(f)

圖二：鏡頭偏移型態：輕微上偏(a)、大量上偏(b)、輕微下偏(c)、

大量下偏(d)、左偏(e)、右偏(f)。

3. 研究範圍

為有效驗證警用監錄系統拍攝之戶外場域畫面，本研究以桃園市警用監視錄影系統之每日檢查照片為實驗範圍，提出基於深度學習的應用做法，並提出實務上適合警用監錄系統全時段執行偏移異常檢測之解決方案。

「天羅地網監視錄影系統」是桃園市政府警察局布建之治安監錄系統，目前已設置約20,000支攝影機，且桃園市自106年起逐年布建新式200萬畫素數位攝影機，全時傳送視訊檔案至後端機房存錄，本研究使用各攝影機完工時設定之標準照片，並擷取各時段具有各類車輛、行人、施工物件等之即時照片進行分類與運算。

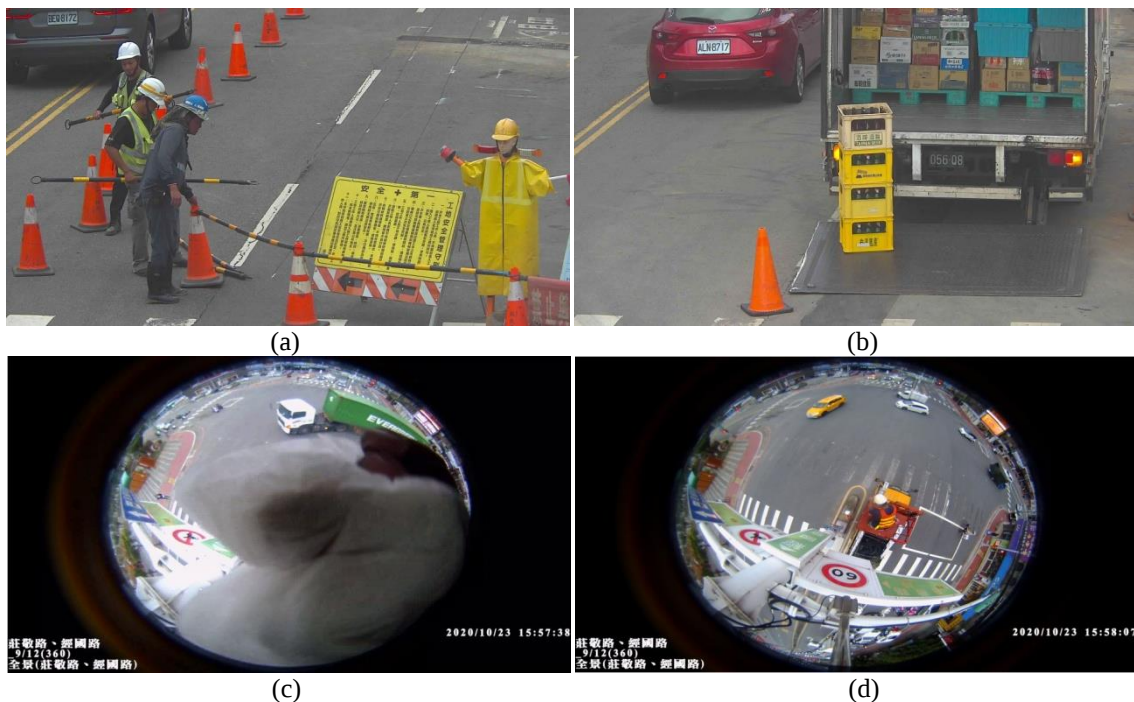
二、文獻探討

在戶外場域的監錄系統應用中，因攝影機偏移造成拍攝範圍非原定區域，被歸類為偏移異常，為解決這類現象所發表的檢測方法眾多，像是基於Block Matching的做法，例如Saglam及Temizel等人[5]認為發生位移之前後幅影像差異明顯大於未發生位移之前後幅影像，因此使用前後影像相異像素計數做偏移判斷，不過此方式容易受前景影像(如車輛、行人等)干擾而造成誤報，另外，也有基於區塊提取特徵並進一步加入線上卡爾曼濾波器之作法[6]；另外像是基於直方圖的分析也被廣

泛用於檢測不同的篡改事件。例如使用直方圖分析，並使用短期和長期紀錄池。每個新的框架都被推送到短期池中；如果短期池已滿，則將最舊的畫面推送到長期池[6,7]。Chen等人利用使用光流演算法研究車道攝影機畫面的動態特性，並且使用將光流方向統計為直方圖[8]，以及同樣使用直方圖與歷史紀錄池，並透過忽略行車方向角度位移的方式進行偏移偵測[3]，但往往在實務上仍可能有多樣性的因素導致判斷失誤。

我們觀察警察局設置戶外型道路監錄系統的實際照片，發現干擾偏移偵測的因素可區分為自然與人為因素，自然因素包含風力造成攝影機附掛之立桿搖晃震動現象，且在風力增強情況下，使立桿頂部因槓桿原理而晃動程度大幅增大。另外日光照射造成強烈光影差異也會造成誤判警報的增加。

人為因素則有車道攝影機遭遇大型車輛(如大貨車、公車等)或塞車占據畫面，或者短、中、長期停放路邊的車輛或物體影響演算法的判讀，以及最常發生的道路施工、道路封閉過程中施工人車的不規則移動，以及攝影機維護廠商至攝影機進行保養維修而導致誤判為偏移，透過傳統區塊提取特徵光流演算法與歷史紀錄池等方式，實務上仍可能因上述各類因素產生誤判警報(如圖三)。



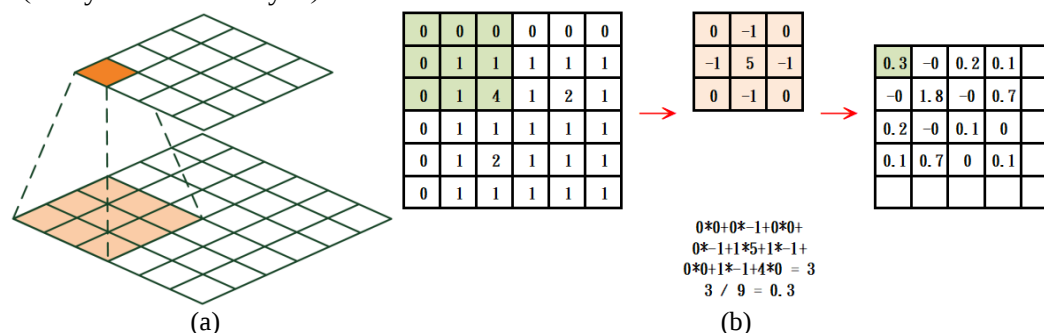
圖三：誤判偏移異常型態：(a)道路施工障礙物、(b)無法預估臨停時間長短之車輛

(c)保養人員擦拭鏡頭、(d)維修人員調校鏡頭時造成之變化

三、背景知識

1.卷積神經網路

卷積神經網路 (Convolutional Neural Network) 簡稱CNN，是一種辨識圖片的方法，基本架構有卷積層 (Convolutional layer)、整流線性單元 (Rectified Linear Unit, ReLU)、池化層 (Pooling layer) 及全連接層 (Fully-connection-layer)。



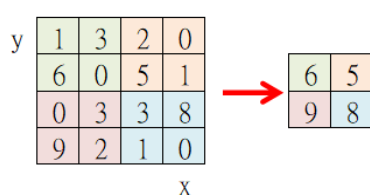
圖四: 卷積層運算範例：完成卷積後維度將減少(a)。卷積完成後將圖像特徵明顯化(b)。

圖片重複執行上述步驟，歸納出圖片中各種特徵，即可完成卷積。可想而知，卷積的過程相當耗運算資源，而圖片中像素數量及每個特徵中的像素數量多寡也將影響到運算量。

整流線性單元 (Rectified Linear Unit, ReLU) 是類神經網路中活化函數(activation function)的一種。活化函數主要目的是用來增加類神經網路模型的非線性，例如當事件值小於0時，則直接輸出0，若事件值大於0時則直接輸出該值，這樣的模式可讓類神經網路模型在學習上更加活化。若以生物神經作為參照，當刺激未達一定的強度時，神經元不會反應而引發神經脈衝；反之如果刺激超過某個臨界值，生物才會引起神經脈衝，Relu在某種程度上正好詮釋了類生物神經的原理。

池化層的作用主要將圖片資料量減少並同時保留重要資訊，把原本的資料做一個最大化或是平均化的降維計算，以圖8為例，以2X2方式採Max Pooling方式，每個區塊選擇最大值，做完池化後，圖片的維度會減半。

池化法除最大化池化法外，還有最小化池化法(取最小值)與平均池化法(取平均值)等。



圖五: 池化層運算範例

全連接層(full connected layer)指的就是一般的神經網路，前面提到的卷積層和池化層，主要作用分別是提取特徵及減少圖像參數，然後將特徵資訊丟到全連接層進行分類，並依模型的分類數量進行輸出。其中全連接層裡的各神經元均與前一層各神經元彼此連結，各連結均有其權重值，這個現象造成全連接層會耗用相當多的運算資源，運算成本(如記憶體、CPU或GPU使用量)極為可觀。

2. You Look Only Once(Yolo)

Yolo系列是Joseph Redmon利用其開發的小眾darknet架構，全名為You Only Look Once[9]，開發針對物件偵測(object detection)的類神經網路演算法，其特色為輕量化、高效率之演算法，故已被廣泛被工商業界廣泛使用在各類應用領域，例如人體圖形偵測、道路車輛偵測等。

Joseph Redmon在後續兩年內接續推出YoloV2及V3，其中YoloV3使用新的基底網路Darknet-53[10]，具有53層神經網路，隨著網路層數不斷加深，作者採取類似ResNet結構之方式，一共加入23個Residual block來解決梯度問題，收到良好的成效(如表1)。

表一: Darknet-53架構圖[10]

Type	Filters	Size	Output
Convolutional	32	3 × 3	256 × 256
Convolutional	64	3 × 3 / 2	128 × 128
Convolutional	32	1 × 1	
Convolutional	64	3 × 3	
Residual			128 × 128
Convolutional	128	3 × 3 / 2	64 × 64
Convolutional	64	1 × 1	
Convolutional	128	3 × 3	
Residual			64 × 64
Convolutional	256	3 × 3 / 2	32 × 32
Convolutional	128	1 × 1	
Convolutional	256	3 × 3	
Residual			32 × 32
Convolutional	512	3 × 3 / 2	16 × 16
Convolutional	256	1 × 1	
Convolutional	512	3 × 3	
Residual			16 × 16
Convolutional	1024	3 × 3 / 2	8 × 8
Convolutional	512	1 × 1	
Convolutional	1024	3 × 3	
Residual			8 × 8
Avgpool		Global	
Connected		1000	
Softmax			

另外Yolo V3為了提升對小物體的偵測能力，採取類似Feature Pyramid Network(多層級預測架構，FPN)的方式，採用不同尺度的feature map對各種尺寸的物體進行偵測，通過下採樣32倍、16倍、8倍得到3個不同尺度的feature map，例如輸入416x416的圖片，則會得到13x13 (416/32)、26x26 (416/16)、52x52 (416/8)，這3個尺度的feature map。這種方式可以讓低階預測較佳的目標位置和高階較佳的語義特徵結合，並且在不同特徵層獨立進行預測，使Yolo V3對小物體檢測較Yolo V2具有更好的效果。

透過表二可以發現，由於網路層數的增加，Darknet-53辨識速度明顯比Darknet-19較慢，但 Darknet-53處理速度仍到78fps，與

ResNet系列相比較Yolo V3仍保持高性能的表現。

表二: 四種框架網路的效能比較[10]

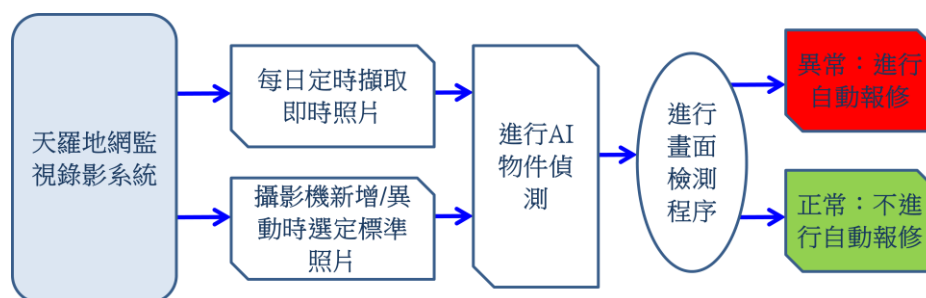
Backbone	Top-1	Top-5	Bn Ops	BFLOP/s	FPS
Darknet-19 [15]	74.1	91.8	7.29	1246	171
ResNet-101[5]	77.1	93.7	19.7	1039	53
ResNet-152 [5]	77.6	93.8	29.4	1090	37
Darknet-53	77.2	93.8	18.7	1457	78

四、解決方案

我們提出一個解決方案，希望利用目前發展普遍的深度學習技術，同時與傳統電腦視覺技術做整合，且需考量符合桃園市政府警察局現行天羅地網監視錄影系統之相容性與可行性，我們利用該系統每支攝影機於完工時設置的標準照片，並與每日檢查時段擷取的即時照片同時進行處理(如圖六)。

我們使用深度學習方式將輸入的兩張照片個別進行物件偵測(Object Detection)，物件偵測方式的選擇上，考量必須能符合桃園市政府警察局現有監視錄影系統的需求與預算限制，必須採用具有效率的架構，在目前主流使用的數種物件偵測中，Yolo系列具有輕量化、高效率的特點，適合作為實務上建置系統的選擇，故我們使用主流之一的YoloV3進行本次試驗。

完成物件偵測後將產生兩張照片內各類人車物件之bounding box，透過OpenCV函式庫功能，我們將兩張照片所偵測得之物件位置進行挖除，然後利用Canny進行邊緣偵測與二值化，可有效將照片後景內之道路標線、背景分離出來，然後透過膨脹(Dilation)與腐蝕(Erosion)等進行雜訊處理與特徵強化。我們將預處理完之兩張圖片進行相減，並進行非黑點數量計算(Count Non Zero)，並嘗試找到適當的閾值進行判別。



圖六: 自動化偵測攝影機位移異常系統之操作流程

五、系統模擬建置與實驗

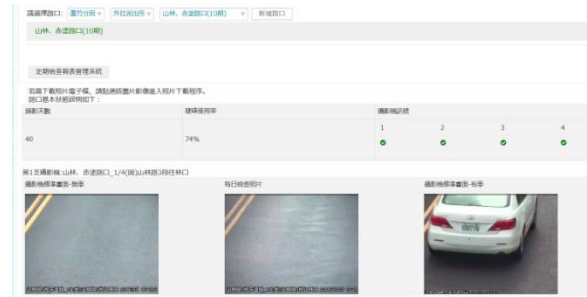
1.攝影機偏移異常自動化流程

我們針對桃園市政府警察局建置之天羅地網監視錄影系統之實務條件，評估建立一套自動化偵測攝影機偏移異常之操作流程，我們之後就其中檢測成效進行實驗與評估。

桃園市政府警察局建置之天羅地網監視錄影系統，目前在各路口設置3種類型數位攝影機，分別為360度超廣角魚眼數位攝影機(非機械式)、固定式廣角數位攝影機及固定式車道數位廣角攝影機，上述這些攝影機在完工時均由人員篩選兩張標準照片於「每日檢查系統」(如圖七)，分別為無車與有車照片，原因是因為當員警登入系統進行目視檢查時，系統當下自動擷取之照片可能為有車或無車之狀態，故系統編排兩張標準照片提供員警進行目視檢查，目前每個派出所員警單一時段須檢測其轄內20至100支攝影機，對警察人力形成極大的負擔。

在我們提出的設計流程中(如圖八)，攝影機僅需於完工階段隨機儲存一張標準照片，因為警用監視系統為封閉式網路，故均透過GSN/VPN或警察局自建之警政光纖骨幹網路傳輸並儲存於後端機房內之VMS主機，且無

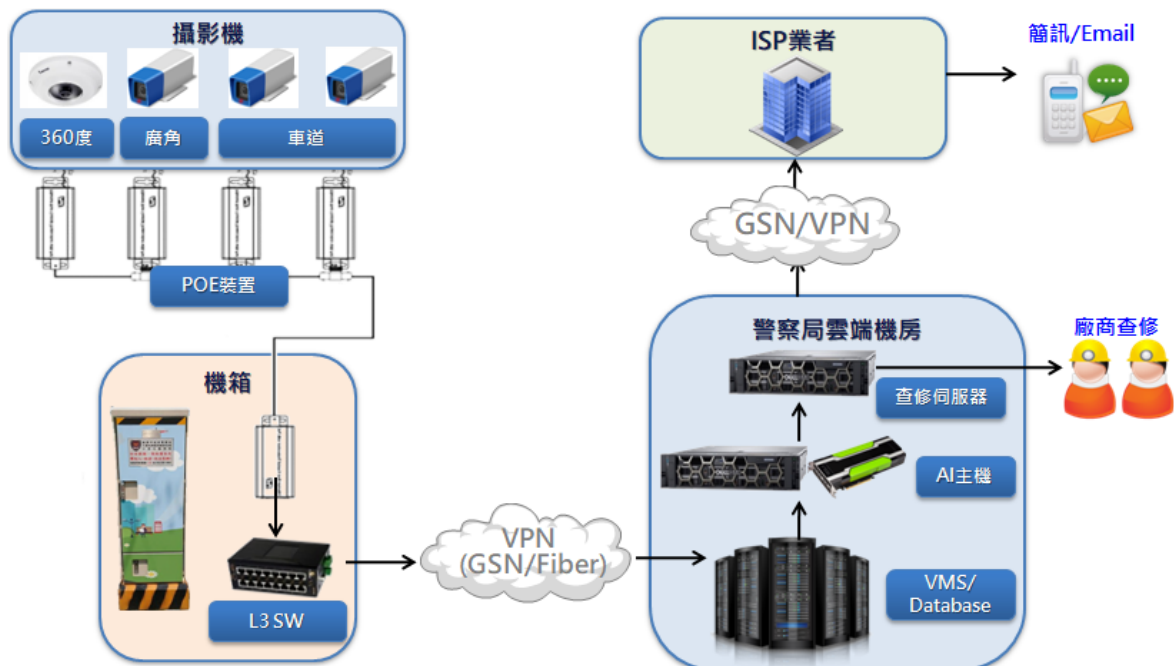
須篩選有車或無車之照片，節省建置施工期人力之耗費，也節省伺服器之儲存空間。



圖七：天羅地網監視系統「每日檢查」介面內可見完工時之標準照片(見圖內左、右)。

在執行每日偏移檢測程序時，由路口前端攝影機回傳即時照片儲存於VMS或資料庫，與VMS已儲存之標準照片同步傳送至AI運算主機進行偏移檢測，檢測結果相關數據傳送至查修伺服器進行紀錄與儲存。

如檢測結果判定為偏移異常，由查修伺服器於天羅地網監視系統平台自動成立報修表單，由廠商專責人員登入系統進行接收與派員查修，或者依廠商需求介接報修資訊至其公司內部查修系統，另外也可透過通信業者傳送簡訊或E-mail進行通報。



圖八：自動化偏移異常檢查告警系統

2. 實驗環境

為驗證上述偏移異常檢測系統的可行性，我們建置了一個電腦環境，使用初階的圖形運算介面，未來實際建置時，可購置針對AI運算專用的圖形運算加速卡與專用伺服器，提升批次處理的運算能力。

本研究使用的訓練硬體環境如下：

CPU：Intel®Core-i7-7500U® 2.70GHz

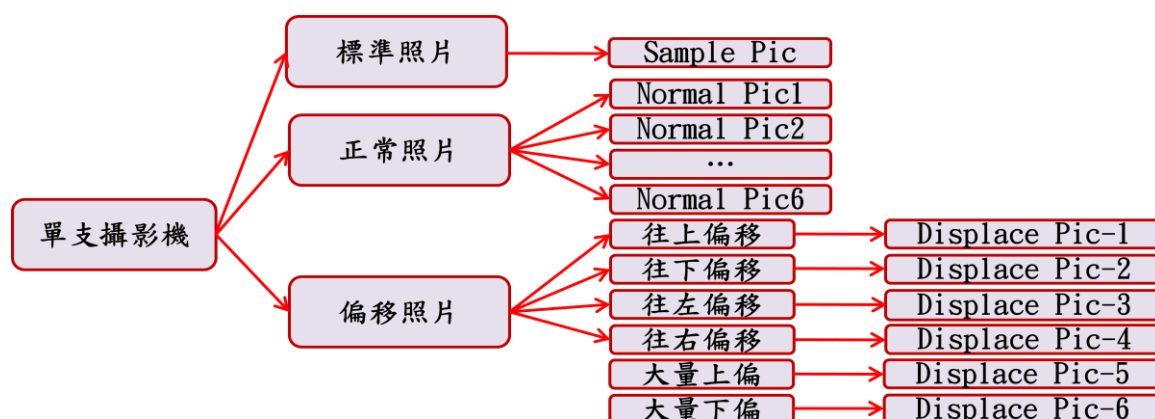
Ram：16G DDR4 2133 DRAM

GPU：NVIDIA Geforce 940MX 2G

OS：Windows10 Home Edition

3. 資料集

依資料處理流程，我們隨機選定天羅地網監視錄影系統戶外場域30支攝影機畫面，每一支攝影機均有完工時儲存之標準照片一張，另外分別擷取偏移(向下、向上、向左、向右)及大量偏移(向上及向下)，合計共180張偏移異常照片，另針對每支攝影機各擷取6張正常角度照片，且包含各類車輛或行人等物件，合計為180張正常照片(如表三)。



圖九：資料集分類方式說明

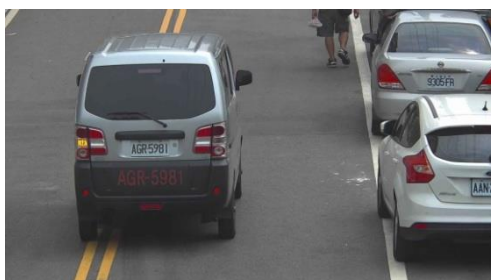
表三：訓練集與驗證集資料數量

項目	標準照片	正常照片 (未偏移)	偏移異常					
			向上	向下	向左	向右	大量上偏	大量下偏
數量	30	180	30	30	30	30	30	30
小計	30	180	180					
總和	390							

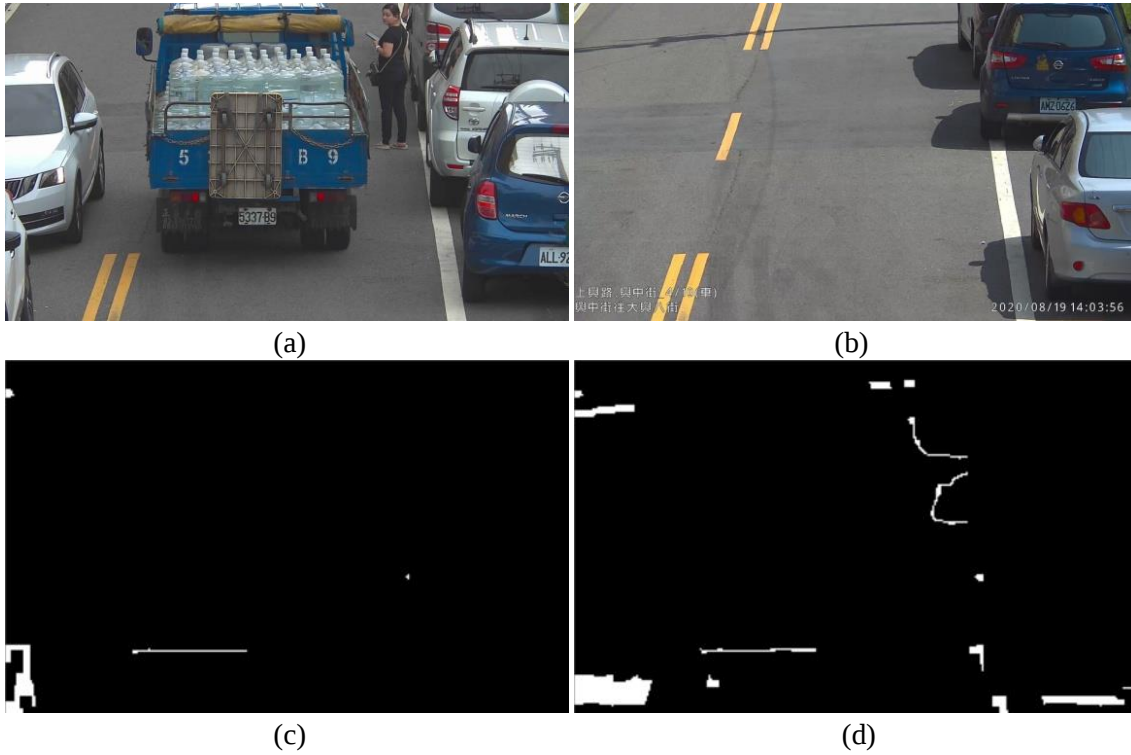
六、實驗結果與討論

我們記錄整個辨識過程的照片與數據，例如蘆竹區上興路、興中路監控點第4支攝影機之影像，我們將標準照片(如圖十)與正常照片(如圖十一)透過AI物件偵測，將兩張照片中影響背景判讀之車輛或行人等進行挖除，再分別

使用標線後進行相減，結果發現正常照片與標準照片之差異度不大，也有效排除車輛與行人等外在因素，另外因日照產生之陰影變化，透過處理後也僅剩下邊緣部分，經過影像清洗後也有效降低影像判讀之可能性。



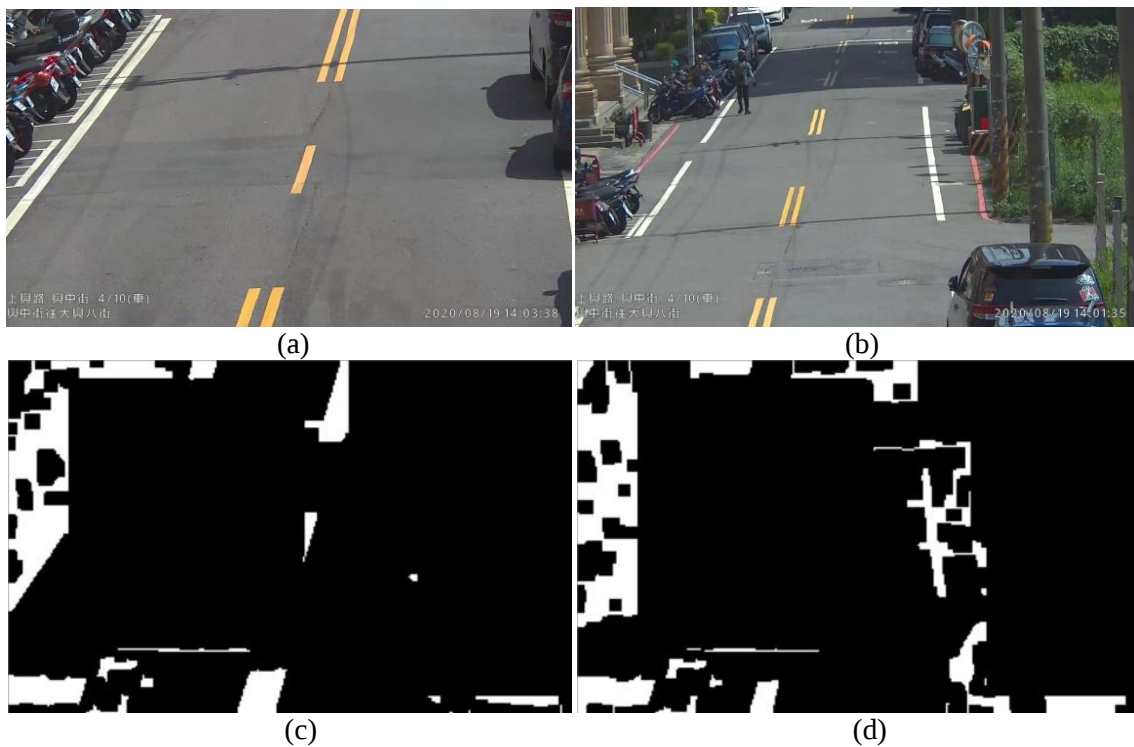
圖十: 標準照片



圖十一: 正常照片與標準照片透過AI物件偵測與電腦視覺處理後之影像，有效將照片內屬於前景部分去除:(a)至(d)。

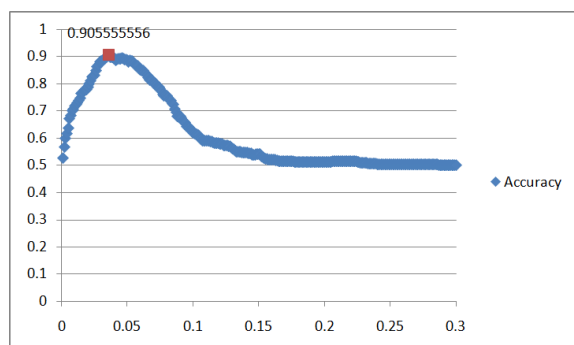
另外我們觀察該攝影機組偏移異常之樣本(如圖十二)，經過物件偵測與影像處理後，有效將前景物件干擾因素去除，並保留道路標

線與背景環境，與標準照片進行差異分析後，可明顯看到差異程度較正常照片明顯。



圖十二: 屬偏移異常之照片經過處理後之結果: (a)(c)異常偏左之影像、(b)(d)大量上偏之影像。

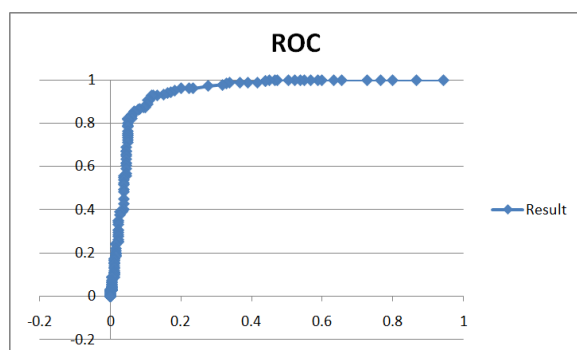
我們將閾值設定0.001至1，並紀錄所有檢測結果，在0.036時可取得最高之正確率90.56%(如圖十二)，其中屬於正常照片之正確率為88.33%，而偏移異常照片之正確率92.77%(如表四)，各閾值所測得之數據繪製成ROC曲線圖(如圖五)。



圖十二: 各閾值測得之準確度

表四: 閾值設定為0.036之檢測結果

	判定正常	判定異常	合計
正常照片	159	21	180
異常照片	13	167	180
正確率	88.33%	92.77%	



圖十三: ROC曲線圖

考量本實驗最後預測出來的結果屬於分類問題，為了評估各模型的表現差異，我們透過Accuracy、Recall、Precision、F1 Score來進行評估，而F1 Score是Precision和Recall加權調和平均總結成單一數字評估的方式，是一般常用的評判標準。

其中Accuracy、Recall、Precision、F1 score的定義如下:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (1)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (2)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (3)$$

$$\text{F1 score} = \frac{2\text{TP}}{2\text{TP} + \text{FN} + \text{FP}} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

其中 TP 為 True Positive，TN 為 True Negative，FP 為 False Positive，FN 為 False Negative。原則上 TP 和 TN 出現愈多而 FP 和 FN 出現愈少，代表模型效果是良好的，把所有正確的情況 (TP 和 TN)，加總後除以所有個數就是 Accuracy，此為常用的評比指標。另外從 Precision 和 Recall 的定義可得知，兩者關注的都是 TP，但 Precision 指的是電腦判斷結果為正確時，其實際的正確率是多少；而 Recall 則是在所有陽性樣本中，能準確預測出的比率。

表五: 各衡量指標結果

TP	167
TN	159
FN	13
FP	21
Accuracy	0.90555

七、結論與後續研究

由於警用監錄系統均設置於戶外，天候、人力或零件等多種因素均導致鏡頭偏移，成為畫面異常之主因之一，在警用監錄系統建置數量逐年大量攀升的情形下，尋找自動偏移偵測以協助人力檢修成為當務之急。本研究提出透過施工設置完成時的標準照片，直接與系統當下即時擷取之照片透過深度學習方式偵測物件位置，同步進行挖除、邊緣偵測及影像處理，計算畫面的整體差異值，解決過去使用逐幅 (frame by frame) 或歷史紀錄池等檢測方式可能造成的使用限制，且能符合實務單位現有監視錄影系統的需求與預算限制。

未來我們將持續加入更多實際案場之照片樣本，並使用其他物件偵測如 SSD、YoloV4

等基於深度學習之方式，以進一步提高智慧偏移監視系統之效率與可用性。

參考文獻

- 1.蕭天佑、顏志平、林曾祥，「治安監錄攝影機畫面模糊自動偵測：以桃園市警用監視錄影系統為例」，「管理思維與實務」暨「應用科學」研討會，2020，第9頁。
- 2.程克羽、王元凱，「使用顯著區域供現實視訊監控使用之即時攝影機異常偵測」，輔仁大學電機工程研究所碩士論文，2012，第2頁。
- 3.Sidnev, A., Nosov, S., Barinova, M., “Efficient Camera Tampering Detection with Automatic Parameter Calibration,” 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2018.
- 4.Wang, Y.K., Fan, C.T., Cheng, K.Y., and Deng, P.S., “Real-time Camera Anomaly Detection for Real-world Video Surveillance,” International Conference on Machine Learning and Cybernetics: 1520-1525, 2011.
- 5.Saglam, A. and Temizel, A., “Real-time adaptive camera tamper detection for video surveillance,” Proc. IEEE International Conference on Advanced Video and Signal Based Surveillance, 2009, pp. 430-435.
- 6.Ribnick, E., Atev, S., Masoud, O., Papanikolopoulos, N. and Voyles, R., “Real-Time Detection of Camera Tampering,” IEEE International Conference on Advanced Video and Signal Based Surveillance, 2006 pp: 10-15.
- 7.Liang, S., Liu, N., Wang, G. and Guo, W., “Camera Sabotage Detection Based on LOG Histogram and Bhattacharyya Distance,” Lecture Notes in Electrical Engineering Future Wireless Networks and Information Systems, 2012, pp: 197-203.
- 8.Chen, J., Fan, C. and Wang, Y., “Traffic Camera Anomaly Detection,” 22nd International Conference on Pattern Recognition, 2013.
- 9.Redmon, J., Divvala, S., Girshick, R. and Farhadi, A., “You Only Look Once: Unified, Real-Time Object Detection,” IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.
- 10.Redmon, J. and Farhadi, A., “YOLOv3: An Incremental Improvement,” IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

政府組態基準(GCB)推動實務-以彰化縣警察局為例

劉立偉

彰化縣警察局巡官

rjhjp2n@ms2.chpb.gov.tw

吳俊德

彰化縣警察局巡官

iamlidan@ms2.chpb.gov.tw

摘要

微軟在今年6月29日發表亞太地區「2019年端點安全防護威脅報告」，針對遭遇惡意軟體、勒索軟體、加密貨幣挖礦和偷渡式下載等四大知名網路攻擊方式的發生做統計分析，其中指出臺灣遭受惡意程式攻擊發生率比全球平均高1.2倍，遭受勒索軟體攻擊高於全球平均1.5倍，而端點安全能降低網路惡意攻擊管道，是有效提升資安防護能量的方法之一。

政府對資安防禦部署態度，已提升成國防備戰準備，從資通安全管理法立法、建立資安治理模式、推動政府組態基準(GCB)，到政府機關資安弱點通報機制系統(VANS)施行，亦清楚認知到端點安全及防護是一切資安部署的起點，彰化縣警察局在彰化縣政府大力支持下，已完成GCB的初期導入強化機關內端點資訊安全的防護能量，分享本局推動GCB的實務經驗，期透過分享能與先進交流相關經驗。

關鍵字：政府組態基準、GCB、端點安全、資安防禦部署、彰化縣警察局

一、引言

為實現國家資通訊安全發展方案(102年至105年)的4大策略目標，該方案共規劃20項執行策略及52個行動方案，其中第2策略目標的第3項執行策略下第2點行動方案「2.3.2推展資安基礎環境安全設定」，明訂要求科技部持續規劃不同系統的政府組態基準(Government Configuration Baseline, GCB)設定(每年至少新增1項資通訊設備)、設計相對應的GCB部署機制(針對服務目錄網域環境與單機作業環境)及每年辦理GCB教育訓練。此3項執行要點，為推動GCB的主要依據。

我國自102年開始推動政府組態基準(GCB)，以「中央部會推動至所屬機關及地方政府」的政策，至105年已逐步推行到各基層政府機關，為持續加強政府組態基準(GCB)推動之深廣度，於國家資通訊安全發展方案(106年至109年)「5.3建構地方政府資安區域聯防體系」，即要求各地方政府機關導入政府組態基準(GCB)，並逐步汰換具高風險資訊軟硬體設備，以完善機關資安縱深防禦的工作項目。

行政院資通安全處更在106年的「強化政府基層機關資安防護及區域聯防計畫」內，規劃藉由汰換基層機關7年以上電腦主機及資安防護設備，順勢將GCB導入基層機關；行政院國家資通安全會報的國家資通訊安全發展

方案(106年至109年)亦要求各地方政府於109年底前導入GCB達95%，以建構地方政府資安區域聯防體系。

二、政府組態基準(GCB)

1. GCB起源

政府組態基準(GCB)是一套由國家提供的資訊安全組態標準，我國GCB是由行政院國家資通安全會報技術服務中心(NCCST)參考美國政府組態基準(United States Government Configuration Baseline, USGCB)內容訂定，目的在於規範資通訊終端設備(如：個人電腦、伺服器主機及網通設備)的一致性安全設定(如：密碼長度、更新期限等)，以降低駭客入侵管道，進而提升政府機關的資安防護能力。

USGCB是從聯邦桌面核心組態(Federal Desktop Core Configuration, FDCC)計劃演變而來，FDCC由美國國家標準技術研究所(National Institute of Standards and Technology, NIST)與微軟公司聯合制定，是一套針對Windows產品的安全指南，由美國國家安全局(NSA)在美國政府機構中推行，其目的是要提高美國聯邦政府所使用的微軟系統安全性，並實現個人電腦安全管理的標準化和自動化。

隨著軟體和作業系統的更新及微軟新產品的發布，FDCC不得不擴充及更新相關標

準，因此在西元2010年創建USGCB，明確說明FDCC的任務及進一步制定各軟體或作業系統的資安防護組態基準。

2.GCB與端點安全

不管政府機關還是企業法人花費多少經費及精神建構資安防線，總是會有筆記型電腦、USB設備、行動載具等漏網之魚，將惡意軟體、勒索軟體、加密貨幣挖礦和偷渡式下載等網路攻擊帶入機關內部。

依行政院國家資通安全會報技術服務中心(NCCST)公布資料，我國政府組態基準(GCB) 以提升端點安全為主要目的，從Windows環境擴及Linux、Firefox、Chrome、行動設備、網通設備，將政府機關共有、常用的資通訊終端設備，逐年規劃訂定一致性的安全組態(configuration)，即是期望透過強化端點安全能降低網路惡意攻擊管道，以有效提升政府機關資安防護能量。

3.GCB發展及推動現況

3.1GCB推動進程

我國國家安全局參考美國國家安全局(NSA)推行的FDCC，於100年率先施行資訊安全共通組態的機制，後由行政院於101年在共用系統(如：主計、人事等)主管機關及院本部進行政府組態基準(GCB)測試，同年開始推動各部會資通訊終端設備(如：個人電腦)部署GCB，並要求各部會在102年底前完成Windows7或IE8環境導入GCB設定，於105年開始推廣至各部會所屬三、四級機關及地方政府，以「中央部會推動至所屬機關及地方政府」及「部署範圍從終端設備擴及伺服器與網通設備」的政策持續推動GCB。

政府組態基基(GCB)的資訊安全共通組態相關安全標準，是由行政院國家資通安全會報技術服務中心(NCCST)自102年能開始持續規劃訂定，至108年共計制訂(109年公布)23項GCB項目，目前有網通設備、作業系統、應用程式、瀏覽器等4類別，表一即為102年至108年制訂的GCB項目及各項目的基準項數。

3.2GCB項目發展現況

表一：102年~108年制訂的GCB項目

項次	類別	制訂年度	GCB項目	規範項數
1	作業系	102年	Windows7	275
2		103年	Windows Server 2008 R2 SP1	332

3		103年	Red Hat Enterprise Linux 5	190
4		104年	Windows8.1	334
5		106年	Windows10	345
6		106年	Windows Server 2012 R2	712
7		107年	Microsoft Windows Server 2016	690
8	瀏覽器	102年	Internet Explorer 8	115
9		104年	Internet Explorer 11	154
10		105年	Google Chrome	30
11		106年	Mozilla Firefox	52
12	網通設備	107年	Microsoft Edge	12
13		104年	無線網路	19
14		105年	Juniper Firewall	49
15		106年	Fortinet FortiGate	47
16	應用程式	107年	Cisco Firewall	44
17		105年	Exchange Server 2013	49
18		107年	Microsoft IIS 8.5	53
19		108年	Word 2016	44
20		108年	Excel 2016	56
21		108年	PowerPoint 2016	39
22		108年	Outlook 2016	91
23		108年	Apache HTTP Server 2.4	64

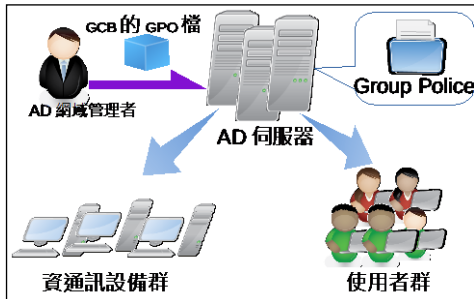
三、推動方式

1.設計GCB部署機制

群組原則(Group Policy)是微軟作業系統內建的系統管理機制，用來管理使用者和電腦的一般性功能與安全性設定，透過群組原則的組態(Configuration)設定，例如個人電腦自動播放、IE/Chrome瀏覽器自動填入等功能是否開啟，或是要求帳戶密碼複雜性策略的組態設定，即可以強制使用者在端電設備上應遵行的行為基準，進而實現統一的資安政府，而這一套組態就被稱群組原則物件(Group Policy Object, GPO)，也就是群組原則組態設定的集合物件。

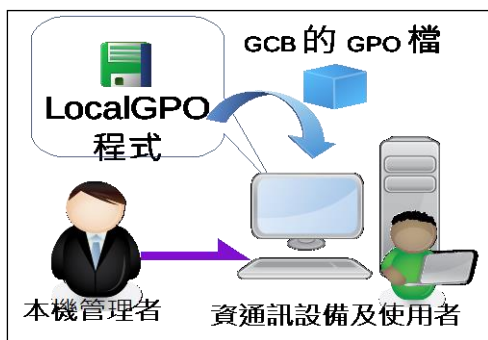
行政院國家資通安全會報技術服務中心(NCCST)就是依據各種資通訊設備的作業系統環境，將GCB各項組態規範打包成「群組原則物件」(GPO)，並依據國家資通訊安全發展方案(102年至105年)「2.3.2推展資安基礎環境安全設定」行動方案的執行要點，分別設計服務目錄(Active Directory, AD)網域環境與單機作業環境的GCB部署機制。

已建有AD網域環境的政府機關，可將打包好的GPO檔，匯入至AD伺服器的群組原則裡，再將GPO連結至組織單位(OU)，當使用者電腦登入網域後，因會自動套用群組原則，即可完成GCB部署，如圖一示意圖。



圖一：AD網域部署GCB示意圖

在獨立且非網域的電腦上，透過安裝本機群組原則(LocalGPO)程式，將打包好的GPO套用在本地群組原則裡，使用者重新開機後，就完成GCB部署，如圖二示意圖。

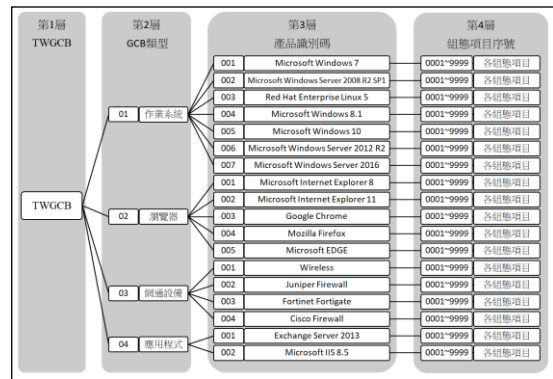


圖二：本機導入GCB示意圖

2. 建立GCB唯一識別碼

NCCST為讓各政府機關於部署及實作過程中，可以快速識別與方便查找GCB規範項目，參考物件識別碼(OID)與Common Configuration Enumeration (CCE) ID 識別碼等編碼方式發展 TWGCB-ID，做為我國政府組態基準專屬編碼方式，為每項組態設定提供唯一識別碼，並於108年9月發佈說明文件。

TWGCB-ID識別碼採用樹狀結構，由4組字元構成，各組字元透過「-」符號進行分隔，格式為「TWGCB-GCB類型-產品識別碼-組態項目序號」，圖三為該識別碼範例圖。



圖四：TWGCB-ID階層樹狀結構圖(資料來源：NCCST)

第1層「TWGCB」為根節點不會改變，第2層「GCB 類型」目前有作業系統、瀏覽器、網路設備及應用程式等4個類型，分別以1~4來代表，第3層「產品識別碼」節點會在第2層的「GCB 類型」節點下，各自依照該GCB類型中GCB項目發布的時間順序，使用001~999的數字依序進行編號。

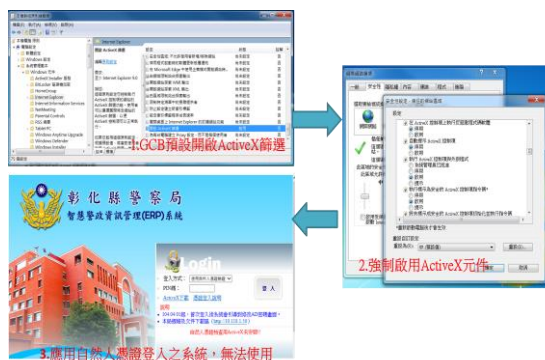
例如105年制訂Exchange Server 2013及107年定 Microsoft IIS 8.5等2GCB項目，皆屬應用程式類別，其產品識別碼分別以時間先後編排001及002的識別碼，詳細可參考圖四TWGCB-ID 階層樹狀結構圖。

四、實務案例

彰化縣警察局建有AD網域環境，在初期導入GCB時，是利用NCCST所提供的GPO透過AD部署GCB，但為了能在套用GCB後即時彙整全機關近2000台個人電腦的套用情形及協助快速有效除錯，後購買商業套裝軟體協助GCB導入工作，以下分享在實務中推動GCB時所遇到的問題案例：

1. 瀏覽器IE11案例：TWGCB-02-002-0020

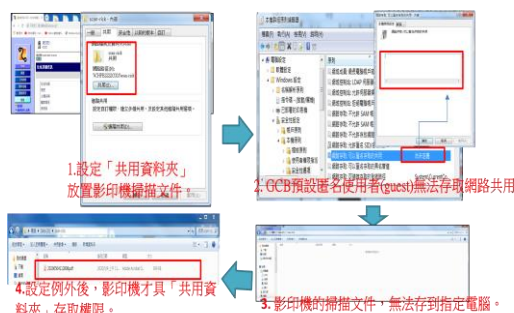
該GCB資訊安全組態會造成資訊系統無法透過IE11瀏覽器使用自然人憑證登入，其原因是該組態預設啟用ActiveX篩選，因此會先執行內建的ActiveX元件，而使用自然人憑證登入之系統，通常需使用內政部憑證管理中心的跨平台網頁元件，當使用者未將該資訊系統的登入網頁新增例外條件，就會因找不到對應的網頁元件，而無法使用自然人憑證登入。圖五為其圖示。



圖五：資訊系統無法使用自然人憑證登入原因圖

2. 個人電腦作業系統 Windows7 案例：TWGCB-01-001-0063

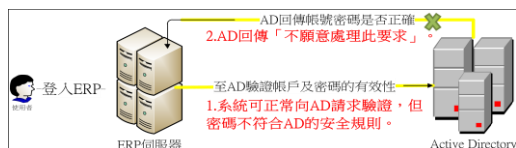
該GCB資訊安全組態會造成影印機掃描文件，無法存到指定的Windows7電腦，其原因是該組態預設匿名使用者(guest)只能存取指定的共同資料夾，而預設值為空白(未定義)，又影印機一般都為匿名使用者，所以沒有「共同資料夾」的存取權限，故而造成無法使用的狀況。圖六為其示意圖。



圖六：解決影印機掃描文件，無法存到指定的Windows7電腦示意圖

3. 伺服器作業系統 Windows server2012 R2 案例：TWGCB-01-006-0003

資訊系統在與AD交接時，因其設定的密碼長度不符合GCB資訊安全組態，造成使用者登入資訊系統時，會出現「不願意處理此要求」的錯誤訊息。圖七為發生示意圖。



圖七：資訊系統無法與AD驗證帳密的原因圖

4. 解決方案

政府機關在導入政府組態基準(GCB)時，通常會依據實務需求修訂基本設定，如上面所提的3個案例，皆有難以直接套用的因素，先透過變更部分設定或暫不套用的方式，在確保資訊系統能正常提供服務後，再逐步調整。

如案例3，看似直接修改資訊系統的密碼長度以符合GCB資訊安全組態，應沒有太大問題，但實務上因直接修改密碼會造成與該資訊系統介接的系統(資料庫系統)無法使用，又該資訊系統須提供24小時不間斷的服務，因此初期會暫不套用該GCB項目，會在清查相關連的系統並確實能同步修改密碼長度後，再套用相關組態設定。

五、結論

由於端點安全及防護是一切資安部署的起點，而政府組態基準(GCB)是實現資通訊終端設備統一資安政策的重要方式之一，又為建構地方政府資安區域聯防體系的重要環節，因此從中央部會到地方政府皆十分重視GCB的推動，而各政府機關承辦人從臨時受命的不知所措，到現今對各GCB項目的應用及如何導入GCB，皆有獨門見解及處理流程。

本文章經由探討GCB起源、推動政策、策略目標、行動方案及執行要點，來闡明推動GCB的重要，本次分享瀏覽器IE11、個人電腦作業系統 Windows7 及伺服器作業系統 Windows server2012 R2作業系統等不同系統遇到的問題案例，在實務上當然不只這3個問題，旨在拋磚引玉為「完備資安防護管理，分享多元資安情報」的目標，做部分努力。

於108年製定，109年9月公布的5項GCB項目說明文件-Microsoft Word 2016、Excel 2016、PowerPoint 2016、Outlook 2016及Apache HTTP Server2.4，相關推動實務經驗，亦需請先進交流分享。

六、參考文獻

1. 行政院國家資通安全會報，國家資通訊安全發展方案(102年至105年)，民國105年2月。
2. 行政院國家資通安全會報，國家資通訊安全發展方案(106年至109年)，民國108年4月修正。
3. 行政院資通安全處，強化政府基層機關資安防護及區域聯防計畫，民國106年7月。
4. 行政院國家資通安全會報技術服務中心，政府組態基準GCB_TWGCB-ID說明文件，民國108年9月。

5. 行政院國家資通安全會報技術服務中心，政府組態基準(GCB)網路教育訓練教材，
<https://www.nccst.nat.gov.tw/GCB>。
6. 楊宸賓，孫嘉明，周芳銘，資訊安全防護基準與安全組態管理之結合應用，電腦稽核，34期，民國105年8月20日，第66~77頁。
7. 楊宸賓，安全組態管理對資訊確保之形式面與實質面的影響，民國104年7月。

面對DeepFake如何維護機關資訊安全

吳俊德

彰化縣警察局巡官

iamlidan@ms2.chpb.gov.tw

李瑋晟

彰化縣警察局警務員

imasaka@ms2.chpb.gov.tw

摘要

因現今硬體技術的飛速進步，深度學習的技術已經逐漸普及化，而深度偽造更是在這波技術中熱門的討論議題，其中所隱含的，是人類善與惡的之間的互搏。善的應用，可以拿來做公共利益宣傳，或是提升娛樂影音享受，而惡的運用，則是拿來製造色情影片以及生產假新聞以獲取利益。在這善惡議題之間，人們應當改變對於影像的傳統認知，「眼見」或不再為憑，應對影片人物真假進行判斷，並加上客觀條件進行判別。而社群媒體也應當對平台內散佈的內容負起責任，制定相關審核規範。政府機關無可避免，也應當在這波潮流中，瞭解相關的技術及議題，制定規範並提升機關內部人員資訊安全意識，以保障人民生命財產安全。

關鍵字：深度學習(Deep Learning)、深度偽造(DeepFake)、機器學習(Machine Learning)、生成對抗網路(Generative Adversarial Network)。

一、前言

2017年12月，一位名為「DeepFakes」的使用者在Reddit(美國社群網站)發布了一段偽造影片，將電影「神力女超人」的女主角蓋兒·加朵(Gal Gadot)的臉孔換到色情影片女演員上，由於太過逼真，影片很快就大肆流傳。沒多久，許多好萊塢明星都成為受害者，甚於美國前後任總統歐巴馬(Obama)、川普(Trump)等也被做為實驗對象，DeepFake也因此廣為人知。

2019年1月7日，一群武裝軍人占領了加彭國家廣播電台，指責現任總統邦戈(Ali Bongo)已無能力繼續領導國家，要發動政變。究其原因，是2018年10月底邦戈在拜訪沙烏地阿拉伯時驚傳就醫，直至2019年新年，邦戈親自出現在電視上向人民拜年，但螢幕上的他看似中風的模樣，卻引發大眾揣測這是一部DeepFake影片，邦戈本人健康狀態已嚴重到不能露面，而實際掌權的，是他身旁貪腐的裙帶集團，政變因此發生。雖然事後該影片其「極可能」並非DeepFake，但造謠容易，澄清卻很困難。

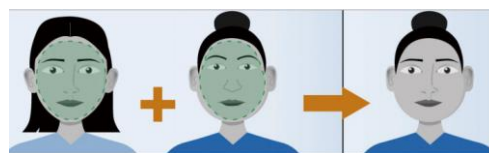
2019年3月，國際間出現了前所未見的網路詐騙行為。一位英國能源公司CEO接到他德國母公司老闆的電話，要求他代墊約730萬新台幣款項，將費用轉給該集團位於匈牙利的一家供應商，並表示之後會再將錢補還給他。由

於聲音與執行長一樣，CEO不疑有它，就依指示匯出，事後卻發現遭到詐騙，警方發現駭客利用AI合成語音，以老闆聲音騙過CEO，達成詐騙目的。這個案件中提到的AI合成語音，背後的技術就是目前最熱門DeepFake。

二、什麼是DeepFake？

DeepFake是英文「Deep Learning(深度學習)」和「Fake(偽造)」兩詞的混合名詞，指的是基於人工智慧的人體圖像合成技術的應用，特別指運用深度學習中的卷積神經網路(Convolutional Neural Network，簡稱CNN)或與生成對抗網路(Generative Adversarial Network，簡稱GAN)技術，將已有的圖像或影片疊加至目標圖像或影片上，進行換臉、偽造語音等工作。Agarwal等人[2]將DeepFake影像分為三種，我們納入人臉生成與聲音合成將分類擴充為五種：

- **臉部替換：**分別取得目標和素材兩個人各種不同的影像，使用素材人臉替換目標人臉，如圖一所示。



圖一：臉部替換範例圖

(Source:GovernmentAccountabilityOffice,
<https://www.gao.gov/products/GAO-20-379SP#summary>)

- **臉部再製**：透過修改目標人物臉部表情，例如移動嘴巴、鼻子或眼睛，這類型的技術並不是取代他們的臉部特徵，而是更改他們的面部細節來使照片傳達的訊息不同，如圖二所示。



圖二：臉部再製範例圖

(Source:GovernmentAccountabilityOffice,
<https://www.gao.gov/products/GAO-20-379SP#summary>)

- **嘴唇同步**：這是通過僅操縱嘴唇區域來創建偽造的視頻，以便目標似乎說出他/她在現實中不會說的話。
- **人臉生成**：利用「GAN」（生成對抗網路）深度學習技術來創造一個不存在的人臉。這種技術使用兩個神經網路互相對抗，其中一個生成影像，另一個負責判斷生成的影像是否夠好。
- **聲音合成**：透過蒐集某些人的聲音，來建立個人聲音的模型，就能透過 DeepFake 的技術來合成那個人的聲音唸出我們指定的文字。

臉部替換的技術在 GitHub 已有不少免費提供的軟體可使用，另外也有商業軟體可使用，例如 FakeApp、faceswap-GAN、faceswap 和 DeepFaceLab 等。還有一些線上服務可以按需生成 DeepFake 影片，如：<https://DeepFakesweb.com>。

三、DeepFake與人工智慧

人工智慧的領域當中，有「深度學習(Deep Learning)」、「機器學習(Machine Learning)」及「類神經網路(Neural Network)」等。而這次的焦點「深度學習」就是機器學習的一門分支，是技術是建立於類神經網路之上，透過模擬人類神經元的運作方式進行建立人工智慧。這樣的演算法最早出現於1980年代，然而受限於當時電腦運算速度緩慢，因此無法呈現出有效的應用成果，也導致這個領域不受重視。受益於近幾年來電腦硬體技術的發展有很大的進步，使得原本難以實現的AI人工智慧演

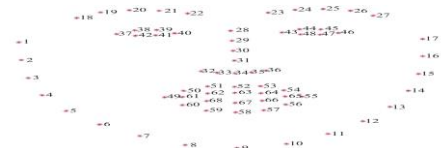
算法得以實現。以前需要耗時數天或數週以上的時間去訓練類神經網路學習，如今可縮短到數小時之內，而這也使得一般使用者也可以透過自己的高階電腦來體驗AI人工智慧，另一面專業研究人員或公司也能運用更多資源進行巨量資料運算，進而取得更多的成果。有了更深層的學習運算，讓電腦在資料的判讀上，可以大幅提高判斷的精準程度，甚至超越了人類的判斷能力。

人工智慧的最大挑戰在於機器不擅長創新事物，但這在2014年時有了改變。蒙特婁大學博士伊恩·古德費洛(Ian Goodfellow)等人在2014年提出生成對抗網路(GAN)的深度學習理論，這是各由一個生成網路與一個判別網路所組成，透過兩個神經網路間不斷地生成回饋迴路、互相學習以及不斷調整相關參數，最終使判別網路無法判斷生成網路的輸出結果是否為真實。所以若是輸入的資料樣本足以讓電腦學習，就能透過GAN來「創造」新的資料，相當於讓電腦擁有「有限的創造」能力。因此，如將GAN的技術用於DeepFake中，就能強化產生「假臉」的能力。

四、DeepFake的技術

DeepFake主要是運用深度學習所建立的技術，其主要運用的技術有三：

- **人臉偵測**：使用 HOG (Histograms of Oriented Gradients)，這是基於人臉特徵的識別演算法，基本的要領在於找出人臉上的眉毛、眼睛、鼻子、嘴巴與臉部線條，用此判斷是否為人臉，總計紀錄 68 個特徵點做為後續的處理依據，如圖三所示。若是需要出現人臉側面的情況，則使用前文所提到 CNN 技術，透過大量的訓練讓電腦來學習判斷。



圖三：人臉 68 個特徵點圖

- **自動編解器(AutoEncoder)**：是一種多層神經網路，架構中可細分為兩部分，分別為 Encoder（編碼器）和 Decoder（解碼器），透過搜集兩張臉的相似之處，藉而

取出影像特徵點進行編碼，接著壓縮成極小的數據，再透過編碼器讀取數據以重建還原，經過重覆多次，電腦就能愈來愈掌握重要的影像特徵。訓練完後只要故意將輸入的人臉用「錯誤」的解碼器重建，就可達成換臉目的。

- **生成對抗網路 (Generative Adversarial Network, GAN)**：分別由生成網路及判別網路這兩種神經網路所構成，藉由兩組模型相互對抗、回饋，經過多輪的訓練，產生更為精準的圖片。但 GAN 不易控制，有時會反而產生出乎意料的結果，如膚色、瞳孔出現異常等。簡單來說，DeepFake並非是自成一格的創新技術，而是在現有技術的基礎下進行偽造工作，因此許多研究者也嘗試透過這些技術反偵測影片是否為偽造。例如 DeepFake 所產生的臉部表情可能與頭部角度不符、部分偽造影片人物的眼睛不會眨眼，以及 DeepFake 目前只能產生畫質較差的影像，因此若將影片放大就可能發現被偽造的區域有模糊的情況。

五、DeepFake的衝擊

然而，在不當運用下，DeepFake也為社會帶來以下層面的問題[1]：

- **社會層面**：如果將 DeepFake 用來偽造女性裸照或色情片就會侵犯女性的隱私，或是某人為了報復，將前任男朋友或女朋友的臉植入色情影片，在社群網站大肆分享。而當越來越多此類的影像或影片在網路中流竄，人們會逐漸失去對社會的信任，轉成冷漠而影響社會的正常運作。
- **政治層面**：DeepFake 如果用來偽造政治人物的發言或行為，將可能損害民主社會，造成民眾對政治人物的不信任。尤其當 DeepFake 被運用在選舉抹黑上，如果在選前一天發布時，儘管受害者指稱影片是偽造的，但因無法即時確認影片的真偽，將足以影響選舉結果。
- **經濟層面**：如果 DeepFake 的受害者為公司，例如偽造公司老闆的影像或聲音，輕則是騙取金錢、重則可能導致公司信譽受損，有心人亦可能會偽造公司老闆對未來經營的悲觀看法，或宣布進行重大投資等，透過影響股市獲取不正常的利益。若

是多家有信譽的公司接連受害，導致民眾對公司領導人有不信任感，進而否定公司的產品或服務，將嚴重影響經濟。

- **科技層面**：在以前時是「眼見為憑」的世代，而現在是「眼見不足以為憑」。為了對抗 DeepFake 的影響，科技上需要持續進步以找出方法協助民眾判斷所收到的多媒體訊息是否為真。此外，為要對抗 DeepFake，人們需要將日常活動記錄下來，未來也可能會有相關的科技產品，或運用科技來提供此類服務的公司出現，這些公司在取得了許多民眾的個人資料後，將可能比現在的 Facebook 更具影響力。

六、打擊DeepFake詐騙與限制

1. 社群平臺：

- **Facebook**

2020年1月宣布，除了刻意用來嘲諷的影片以外，他們會下架所有 DeepFake 影片。Facebook 也與其他科技大廠如微軟、AWS（亞馬遜網路服務）聯手，發起 DeepFake 偵測挑戰賽，投入100萬美元總獎金來激勵偵測技術研發，希望破解更多層出不窮的 DeepFake 手法

- **YouTube**

官方部落格「YouTube 如何支持選舉」文章中，對於會誤導選情的內容採取零容忍態度，例如可能誤導使用者和散播不實資訊的變造過影片（包括 DeepFake）。

- **Twitter**

關於合成和變造媒體資訊的規則更新中包括 DeepFake，單純宣布禁止「可能造成傷害」的合成或變造媒體資訊。

2. 以物理或生理特性分辨：

由於使用網站上的照片作為訓練數據，造成許多 DeepFake 影像人物未有合理的眨眼[4]，如全程未眨眼或僅一眼在眨。另外亦有 DeepFake 影片中出現不連貫的頭部姿勢[9]。另外像是 F. Matern 等人[8]注重於影像被修改後的一些特性，如：整體的一致性（眼瞳虹膜顏色）、亮度（如鼻子的陰影、眼睛的反射）、幾何評估（換臉後造成的變形或破圖）做為特徵來進行偽造影像判斷。

3. 深度學習：

運用深度學習技術找出特定痕跡來進行分辨[3, 6, 10]。如Bappy等人[3]所提出的檢測Deepfake偽造影像的基於Hybrid LSTM演算法,就在於影像經過修改的部分周圍的邊界往往包含著操作過的痕跡,如果一個(偽造)物體被插入,它的邊界區域通常具有不一致的特徵,因此篡改影像的人會刻意讓邊界變得平滑好融入影像,這就導致被篡改的影像部分邊界通常比自然影像更平滑。基於這樣的特性就能找出可能遭受竄改的影片。

4. 限制：

儘管DeepFake影片至今已有相關的技術可進行分辨,並已相當進步,但在運用上還是有些限制存在[7],如：

- 檢測資料庫：DeepFake影片的大量資料集是用來開發DeepFake檢測方法的主要方式。但這些資料未必符合現有的DeepFake影片,有些資料集中的影片品質不佳,所以可以被輕易分辨出來。如此一來,檢測技術於實際運用上的正確率就得存疑了。
- 檢測結果說明：檢測的結果是否夠明確？執法機關進行鑑識後判斷為偽造,是否有足夠的學理依據來證明？深度學習如同黑盒子一樣的特性,使得說明不易,就可能在法庭遭受質疑。

七、DeepFake對政府機關的影響與因應作法

政府機關存放著大量的民眾個資與各類公務機密文件,一直以來都是各類攻擊者的目標,政府機關具備嚴格門禁管制措施,並依各類法規設置資安設備與預算,實體與網路入侵不易,傳統上攻擊者多以電話、電子郵件等方式,進行社交工程或是植入惡意程式來騙取他們想要的資料。

因應2019-Covid疫情,遠距視訊已成為各機關可或缺的工作方式之一,而且重要性與使用率都越來越高,雲端存取、居家辦公、視訊通話、線上會議等,均為遠距工作必要的措施,而這些措施在有效提升機關面對疫情的同時,也衝擊了嚴格的門禁與完善的資安設備所提供的保護。

在遠距工作的環境下,辦理各項業務需透過網路來執行,嚴格的門禁與完善的資安設備無法為在機關以外場所辦公的同仁,提供相同的防護,而此時也是攻擊者使用DeepFake發動攻擊的大好機會,例如,攻擊者可以：

1. 使用DeepFake偽裝成同仁,入侵機關舉辦的視訊會議,竊取公務機關會議內容。
2. 使用DeepFake偽裝成同仁,以視訊通話向機關請求資料查詢,或偽裝成單位主管,以視訊通話向同仁發佈不實命令。

面對這樣的威脅,政府機關可以執行以下的策略：

1. 選擇可靠的視訊產品：在選擇視訊會議軟體產品時,除產品功能外,也應考量資安方面的問題,例如視訊軟體操作時身份驗證機制,會議內容是否會留存,如果有留存,存放的位置是否在線上,以及線上是存放於何處等,選擇擁有良好資安功能的產品,可以為機關線上會議提供最基本的保護措施。

2. 設定線上會議密碼：視訊會議軟體為便利與會者參加會議,提供無密碼、免許可登入會議室功能,但攻擊者利用這個特性,即可任意加入機關的視訊會議,所以機關召開線上會議時,應該為線上會議室設定符合安全規則的密碼,同時開啟與會人員審核功能,指派專人進行審核,非屬本次會議相關人員,即拒絕其與會。

3. 相關人員教育訓練：線上會議操作人員,於會議前應瞭解軟體操作,才能針對各類狀況進行即時應對與處理,例如某大學使用視訊會議進行線上考試時,遭到攻擊者以播放不雅影片方式干擾考試,此時操作人員如熟稔軟體操作,即可利用禁止發言、分享桌面等方式,確保考試繼續進行。

4. 限制會議討論內容：如涉及機密、敏感議題的內容與資料,不宜於線上會議中討論與傳遞,避免發生外洩的可能性。

在手機通訊軟體部分,使用者可以參考所屬機關的相關規定,以內政部警政署訂定的「警察機關使用即時通訊軟體注意事項」為例：

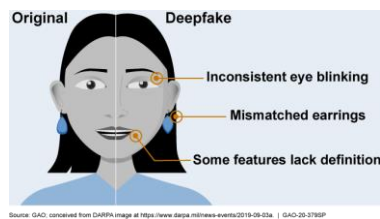
- 以傳送溝通訊息為主。
- 傳遞訊息,內容不得涉及機密性、安全性、隱私性、敏感性或洩漏個人資料。
- 聯絡群組,應指定群組管理人員並定期清查群組成員。
- 機關交付正式文書,應循現有行政程序辦理。

以上關於線上會議與手機通訊軟體的注意事項,可以有效降低攻擊者進入政府機關遠距工

作的環境裡，攻擊者無法進入這個環境，自然無從發動使用DeepFake的攻擊。

除了防止攻擊者進入政府機關遠距工作的環境，我們也需要瞭解DeepFake目前尚且無法完美地進行偽造，對於可能是偽造的影片，我們可參考圖四，並加強注意下列情形：

- **眨眼率：**DeepFake影片中的人眨眼率會低於正常人，或只有一眼在眨。
- **語音嘴唇同步情形：**DeepFake影片中的人講話時容易會有語音與嘴唇不同步的情形。
- **影片情緒吻合情形：**DeepFake影片中的人情緒與表情常會無法相互對應，甚至會出現有雜訊的影像。
- **畫面模糊情形：**DeepFake影片中容易發生畫面模糊、停頓或變色，特別人臉週圍會出現模糊影像。



圖四：判別是否為DeepFake影片範例圖

七、結語

現今2019-Covid全球疫情仍然嚴重，因應疫情所產生的各類遠距辦公將持續是熱門的工作應用方式。未來在相關技術使用與軟、硬體的投資，以及其所帶來的優勢，將會使遠距辦公持續存在，因此我們也難無法擺脫DeepFake威脅。

本文中，我們就DeepFake進行介紹，分析其技術與帶來的影像，以及目前的因應之道。特別是在於公務機關，我們應落實各種標準作業程序，並善盡相關查證工作，且持續加強自己的資通安全觀念，才能有效維護機關安全與公務機密。

參考文獻

1. 柯宏叡, "真假難辨的人工智慧-換臉," 警光雜誌, 第764期, 2020年3月。
2. S. Agarwal, H. Farid, Y. Gu, M. He, K. Nagano and H. Li, "Protecting World

Leaders Against Deep Fakes", CVPRW, 2019.

3. J. H. Bappy, Cody Simons, L. Nataraj, BS Manjunath, and A. K Roy-Chowdhury, "Hybrid lstm and encoder-decoder architecture for detection of image forgeries," IEEE Transactions on Image Processing (TIP), 2019.
4. Y. Li, M. C. Chang, and S. Lyu, "In ictu oculi: Exposing AI generated fake face videos by detecting eye blinking," in IEEE International Workshop on Information Forensics and Security (WIFS), 2018.
5. Y. Li and S. Lyu, "Exposing DeepFake Videos By Detecting Face Warping Artifacts," IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2019.
6. Y. Liu, Q. Guan, X. Zhao, and Yun Cao, "Image forgery localization based on multi-scale convolutional neural networks," in ACM Workshop on Information Hiding and Multimedia Security (IHMMSec), 2018.
7. S. Lyu, "Deepfake Detection: Current Challenges and Next Steps," 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), London, United Kingdom, 2020, pp. 1-6.
8. F. Matern, C. Riess, M. Stamminger, "Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations," IEEE Winter Applications of Computer Vision Workshops, 2019.
9. X. Yang, Y. Li, and S. Lyu, "Exposing deep fakes using inconsistent head poses," in IEEE International Conference on Acoustics, Speech and Signal Processing, 2019.
10. P. Zhou, X. Han, V. Morariu, and Larry S Davis, "Learning rich features for image manipulation detection," in CVPR, 2018.

網路通信紀錄分析於犯罪偵查之應用

劉韻慈

中央警察大學資訊管理所研究生

im1083061@mail.cpu.edu.tw

鄧少華¹

中央警察大學資訊管理所教授

pdeng@mail.cpu.edu.tw

董正談

中央警察大學資訊管理所助理教授

tung@mail.cpu.edu.tw

摘要

隨著網路與資訊不斷整合發展，民眾已鮮少使用傳統語音通話與簡訊互相聯繫，轉而使用免費及含有更多元服務的通訊軟體，只要透過網路連線即可進行語音及視訊通話並傳遞各種多媒體訊息。而警方偵辦刑案原依通訊保障及監察法聲請調取雙向通聯，已無法如以往取得大量通聯受話手機、電話；此外，因網路通化透過封包傳輸與加密特性，通訊監察難以取得通話語音內容，以往案件偵辦手法已不易克服網路這道高牆。不僅如此，犯罪者深諳網路匿名性與無國界性，即使身處台灣也可透過虛擬私有網路等服務，隱身於境外IP的外衣，致使警方束手無策。以往網路犯罪之研討，有關網路通信（連線）紀錄應用之討論均依附在通訊監察一角，本研究將探討相關網路通信（連線）紀錄於法律制定、保存方式、應用刑案偵辦，並提出自動化網路通信紀錄分析概念，以完整最後一塊通信紀錄之拼圖。

關鍵字：網路犯罪、網路通信紀錄、封包分析

¹ 通訊作者

一、前言

1.研究動機

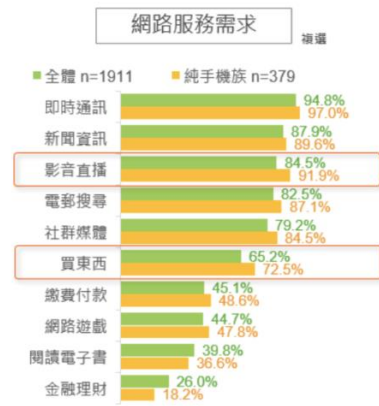
通訊傳播與資訊科技技術之進步與推陳出新，電信、傳播及網際網路基礎建設與網路服務，因寬頻化及數位化之推波助瀾，得以將語音、影像、數據等不同訊息內容，充分整合並快速傳遞；此外，使用者透過行動智慧終端裝置，連線各種連網服務，取得網際網路上所提供之各式服務，更帶動各式資訊應用服務蓬勃發展 [1]。

據TWNIC 2019年台灣網路報告，全體民眾曾經上網率89.6%；「連網方式」以行動上網85.2%最高、使用家中WiFi分享65.2%與公開場所WiFi分享上網約佔4成；「上網裝置」以手機97.9%最高、桌上型電腦與筆記型電腦約佔5成許；「網路服務需求」依序為即時通訊、新聞資訊、影音直播、電郵搜尋、社群媒體、買東西；民眾偏好網路各式服務需求，其中我國使用即時通訊以LINE、FB Messenger與Garena，社群媒體以Facebook、Instagram與Linked為大宗；網民世代從12至54歲上網率近9成6以上，55歲以上之上網率為71.7% [2]。由以上調查數據發現我國網路使用的高普及率，生活需求與網路使用的緊密結合，較高年齡層踏入網路的門檻更低更方便取得，我國已正式邁入全網路數位化生活。

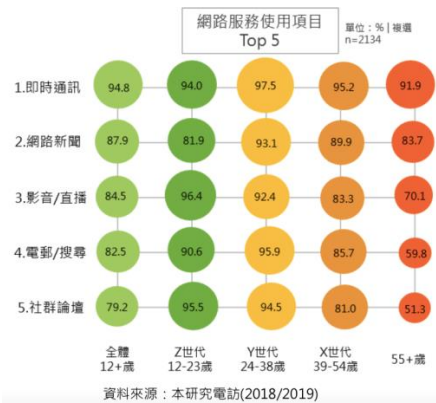
		全體 n=2134	純手機族 n=417
連網方式	行動上網	85.2%	88.6%
	使用家中 WiFi 上網	65.2%	53.1%
	公開場所 WiFi 上網	42.0%	40.3%
		全體 n=1911	純手機族 n=379
上網裝置	手機	97.9%	99.5%
	桌上型電腦	59.6%	53.9%
	筆記型電腦	51.5%	56.9%
		全體 n=使用者人數	純手機族 n=使用者人數
平均每月花費 (元)	行動上網	663	785
	網購	2661	2827
	遊戲	1495	2455

資料來源：本研究電話訪(2019)

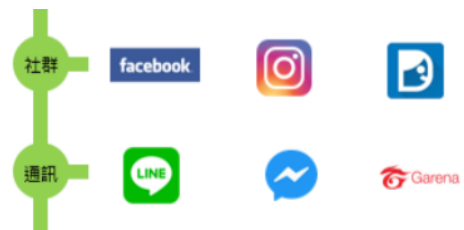
圖一：2019年台灣使用網路方式



圖二：網路服務需求



圖三：台灣各年齡層網路服務使用項目



圖四：台灣常用社群、通訊軟體服務



圖五：2019年網民世代上網率

換言之，我們已完全身處於資通訊的環境，同樣，犯罪者與其行為亦與網路關係緊密，從內政部警政署165全民防騙網公布各式詐欺帳號，其媒介即係透過網路社群媒體與通訊軟體，犯罪者隱身於網際網路背後，

透過虛擬私有網路 (Virtual Private Network)、代理伺服器(Proxy)等用以連線至各電商平台網站，無論用於創設帳號或掌握各項物流快遞資訊，即便網路平台服務業者配合警方資料調閱，涉案帳號卻是使用境外IP因而造成查緝斷點，何況大多應用程式所屬企業幾乎為境外公司，不論是各國司法適用或管轄權等問題皆是調閱資料偵辦上的阻礙。再者，網路封包加密技術是目前資訊安全最重要環節，通訊監察也難以解密取得監察目標通話與訊息內容 [3]，且通訊監察是針對現在、未來的通話語音內容和網路連線做監察，已發生、過去的是無法透過監察取得資料。民眾依賴通訊軟體APP作為日常社交，鮮少使用電話，故警方向司法機關聲請調取通聯，通聯記錄也不會有目標犯嫌通話對象使用門號，致使通聯調取已無法滿足犯罪偵查之需求。

手機電腦網網相連，唯有倚靠網路通信(連線)紀錄，藉由網際網路通訊協定與每個連結節點之IP位址(IP Address)紀錄，記錄與辨識被害者與犯罪集團，作為涉案人之上網動態與識別身分方式。因應大眾使用網路習慣、歹徒深諳網路特性，為解決目前調取(語音)通聯紀錄之不足，提出網路通信(連線)紀錄之保存與應用於犯罪偵查。

2.研究目的

學術界與偵查實務對於網路犯罪、針對通訊軟體App之通訊監察之探討與應對措施，分別在法律面、資安層面及社會賦予之企業責任等各面向多有討論，希望就此在犯罪偵查上給予實質幫助及立法上的建議與修正，強化警方執法的程序與正當性，減少刑案偵查遇到網路案件無法可查之困境。而本次研究提出網路通信紀錄運用於刑案偵辦，以符現行社會實際使用網路於通訊軟體App之VoIP或連線網站等行為模式，填補通訊監察無法溯及過去之網路連線紀錄，與國內法無司法權要求境外網路服務業者提供資料等情況。

故本研究目的：

- 1.網路通信記錄保存必要性之說明與印證。
- 2.規劃電信業者於通訊架構中存取網路連線資料裝置。

3.檢視我國通訊保障及監察法賦予電信業者有關保存與提供網路通信紀錄義務之規範與修訂建議。

4.提出網路通聯紀錄整理之自動化程式，協助偵查人員快速掌握通聯重點，並嘗試將網路通信紀錄套用實務上常見犯罪案類，以強化本研究論點。

3.研究範圍與限制

本研究提出網路通信紀錄，目的就是取得我國第一、二類電信公司提供網路服務之上網IP連線紀錄，藉以找出參與刑案犯嫌身份，為個化其身份與實際窩藏犯罪據點，不論其使用是否為本國網路，犯嫌實際位置必需要在我國境內，如犯嫌位於境外而生之網路連線紀錄，並非本研究要討論之目標。

目前尚無法律明文規定電信業者有提供網路通信紀錄之義務，且絕大部分業者是未建置及紀錄保存，故討論內容與細節可預見與業者實際保留網路通聯紀錄情形會有出入，另儲存網路連紀錄之技術、建置資金與成本並非本研究討論範圍。

二、文獻探討與背景知識

1.通聯紀錄在犯罪偵查上之應用

為我國最早深入研究討論通聯紀錄之文章，時空背景為政府開放電信自由化政策，作者認為通聯紀錄是一重要之偵查工具，為期提高偵查效率，使偵查人員有效率了解通聯紀錄分析流程與方法，將各式分析流程模式化，以減少人工比對可能出現判斷錯誤。提出5類通聯紀錄分析流程如下，「通聯紀錄的來話、受話基本分析流程」：可用以研判對象交往單純或複雜、與通話對象之供需關係、關係密切或疏離；「行動電話持機的動態分析流程」：持機人活動時間與活動地點分析、案發時持機人位置、分析及推測共犯；「行動電話持機人的靜態分析流程」：持機人休息（睡眠）時間、以地址分析法與基地台電話觀察法研判持機人落腳居住地；「基地台通聯紀錄分析流程」；「手機序號通聯紀錄的分析流程」，最後列舉以通聯紀錄分析破案之應用案例。此文章研究標的之通聯紀錄即為電話語音通聯紀錄 [4]。

2.數位資訊在犯罪偵查上之應用——以電話通聯電腦分析系統為例

此文探討數位資訊在犯罪偵查之應用，並以目標軌跡、全球衛星定位系統及電話通聯電腦分析系統為例。電話通聯電腦分析系統，說明如何運用數位資訊於犯罪偵查，以偵查領域知識轉變成專家系統的邏輯規則，據以分析通聯紀錄協助偵查，該研究亦證實，電話通聯偵查技術可以採用專家系統方式予以自動化，並研發一套電話通聯電腦分析系統，該系統具有電話通聯紀錄轉檔、淨化、管理、分析等13項功能，系統以Excel VBA語言撰寫，由7個模組構成，內涵141Sub程式、14個Function程式，已實際應用於犯罪偵查實務，具有輔助犯罪偵查效益，且該程式語言支援模組化程式設計，作業系統功能可擴充，只需附加模組方式即可完成。此作者研究之通聯紀錄亦為電話語音通聯 [5]。

3.行動APP通訊詐欺犯罪手法與被害特性之研究

作者指出犯罪集團透過行動APP加密通訊以規避警方查緝，在通訊監察、執法機關無法向網路服務供應商要求調閱資料等情形下，作者針對LINE詐騙模式包含惡意超連結、取得認證碼、代購點數等，分析犯罪手法及被害原因，建議公部門加強跨境合作、落實犯罪預防宣導、增加行動APP通訊詐騙犯罪阻力等 [6]。

4.網路犯罪

根據109年第9週警政統計通報有關108年網路犯罪概況，其網路犯罪係指附屬發生場所為電腦網路者稱之，按案類別分為詐欺、妨害名譽（信用）、妨害電腦使用、侵害智慧財產權、賭博、妨害自由、毒品、違反兒童及少年性剝削防制條例、一般妨害風化與其他，統計來源為警方受理、破獲案件所填輸之刑案記錄表。可知警政單位統計網路犯罪之標準是以附屬發生場所為電腦網路者，只要案件發生與網路、電腦相關皆屬網路犯罪 [7,8]。

我國刑法第三十六章妨害電腦使用罪，犯罪態樣分為無故入侵他人電腦、無故取得電磁紀錄等，顯見其為狹義之電腦犯

罪，保護法益是電腦使用安全。據本罪章立法理由說明「電腦犯罪有廣義、狹義分別，廣義電腦犯罪指凡犯罪之工具或過程牽涉到電腦或網路，即為電腦犯罪，狹義之電腦犯罪則專指以電腦或網路為攻擊對象之犯罪。我國刑法原本對廣義之電腦犯罪有相關處罰規定，毋庸重複規範，故本章所規範之妨害電腦使用罪為狹義之電腦犯罪。」

5.虛擬私有網路（Virtual Private Network）

虛擬專用網路（VPN）將專用網路擴展到整個公用網路，並使用戶能夠跨共享或公用網路發送和接收數據，就像其計算設備直接連接到專用網路一樣。因此，跨VPN運行的應用程序可能會受益於專用網路的功能，安全性和管理。加密是VPN連接的常見（但不是固有）部分。

開發VPN技術是為了向遠程或移動用戶以及分支機構提供對公司應用程序和資源的訪問。為了安全起見，可以使用加密的分層隧道協議建立專用網路連接，並且可能要求用戶通過各種身份驗證方法來訪問VPN。在其他應用程序中，Internet用戶可以使用VPN保護其連接，以規避地理封鎖和審查，或者連接到代理服務器以保護個人身份和位置，以在Internet上保持匿名。但是，某些網站阻止訪問VPN所使用的已知IP地址，以防止繞過其地理限制。並且許多VPN提供商一直在製定策略來解決這些問題。通過使用專用電路或通過現有網路上的隧道協議建立虛擬的點對點連接來創建VPN。可從公共Internet獲得的VPN可以提供廣域網路（WAN）的某些好處。從用戶的角度來看，可以遠程訪問專用網路中的可用資源 [9]。

三、解決方案

法務部於今(109)年9月公布「科技偵查法」草案，其訂定宗旨因應科技日新月異，為避免犯罪調查之手段落後於科技發展之腳步，故規範偵查機關實施運用科技設備或技術進行必要科技偵查作為之合法性，保障人民基本權、穩定國家安全及社會秩序。該草案即提出通訊軟體逐漸取代傳統固網電話通訊之情形，向地方法院聲請通訊監察核准，實施設備端通訊監察，其定義為侵入受監察人所使用之資訊系統或設備，在通訊尚

未加密前之發出端或已解密後之收取端，紀錄未加密或以解密之通訊內容方式，而實施之通訊監察。立法允許該偵查手段，但實際如何以實體接觸、網路傳輸等方法侵入受監察人所使用之資訊系統或設備，換言之，即為植入木馬程式到受監察人使用之手機、電腦或平板等設備端。該偵查手段無論人權侵害之隱憂與實際執行技術均有很大之討論空間 [10]。

民眾習慣使用網路服務 Google、Amazon、Facebook、IG、Twitter、LINE、WeChat 等提供電子郵件、雲端儲存、電商平台消費、社群通訊軟體應用程式，惟警方即便知悉犯嫌使用何帳號或 ID，因通訊軟體與社群平台所屬公司大部分繫屬國外，不論是司法權、刑事程序與各個國家對於犯罪之認定與容忍度，都無法保證可以成功調閱，也無強制力要求提供，舉例臉書公司以刑事警察局作為調閱窗口管道，惟臉書公司在審核案類也未必允許我方調閱需求而拒絕提供資料。

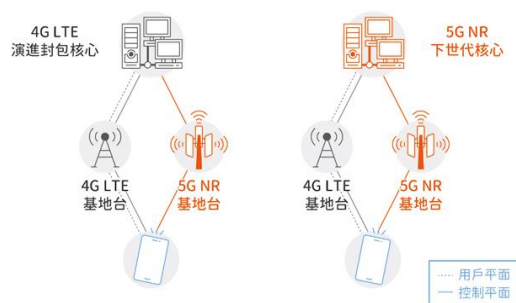
通訊保障及監察法規定通聯調取是指過去已發生結束之通聯紀錄，通訊監察則是以現在及未來之語音作擷錄，惟現在語音使用量大幅減少，警方很難從語音通聯取得曾與偵查目標有過通話及聯繫對象資訊，而往往最關鍵通聯就在案發前後，已經發生、過去之聯絡記錄。綜上目前刑案偵辦面對之困境，若電信業者保留網路連線紀錄，警方可以針對一個涉案行動電話於犯罪時間前後調閱取得連網 IP，或是從網路平台業者提供涉案帳號登入之境外 IP，調閱曾於境內連線該涉案 IP，藉以掌握可疑聯絡對象，又電信業者(第一、二類電信)均受我國相關法律規範之，若有完整網路連線之法律制定，網路通信紀錄確實可以成為警方偵辦刑案用以克服上揭困境。

1. 網路通信紀錄擷取與保存之架構

(1) 行動通訊

我國於今(109)年2月上旬，5G 頻譜位置正式結標，確立五大電信業者分配頻譜，也正式宣告 5G 世代走入你我生活。5G 指第五代行動網路，為 4G LTE 之後新一代行動網路簡稱，相較 4G，其特性具有超高速度(增強行動寬頻上網)、超低延遲(高可靠低延遲通

訊)及超大連結(大量裝置聯網通訊)。目前電信業者將 5G 服務架構在非獨立(non-standalone, NSA)組網上，5G 基地台依附在 4G 的核心網路運作，手機與基地台之間的控制平面(control plane)經由 4G 的基地台傳送，用戶平面(user plane)經由 4G 或 5G 的基地台傳送，5G 的基地台無法獨力作業。未來待 5G 獨立(standalone, SA)技術成熟後，從 NSA 轉至 SA 架構，5G 基地台依附在 5G 的核心網路運作，手機與基地台之間的控制平面與用戶平面經由 5G 基地台傳送，5G 基地台可以完全獨立運作 [11]。

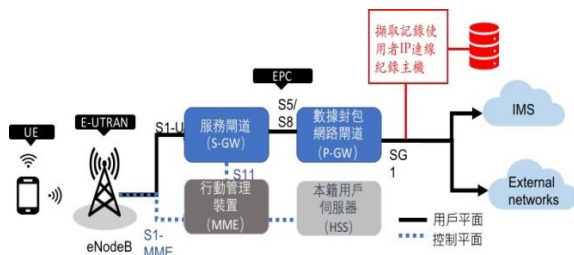


圖六：第五代行動通訊技術之非獨立系統



圖七：第五代行動通訊技術之獨立系統

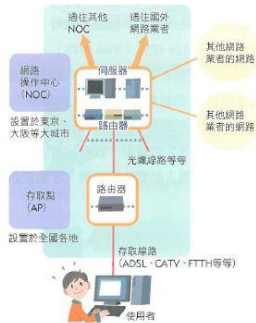
以 4G 行動通訊系統為例，包括演進式數據封包核心網路 (EPC)、骨幹網路 (backbone)、演進無線接取網路 (Evolved Universal Terrestrial Radio Access Network, E-UTRAN) 和用戶設備 (user equipment, UE) 等。「數據封包網路閘道」是 EPC 和外部 IP 網路之間的互連點，並提供手機和外部封包資料網路的連線，其除負責安排與外部 PDN 網路之封包傳輸的路徑，也執行 IP 位址及 IP 字首位址的配置、規則的控制與計費作業。故電信業者紀錄網路連線資料即是建置在數據封包網路閘道 (P-GW) 與外部 IP 網路之間，設立儲存裝置資料庫，並建立與偵查機關連線調閱之機制 [12]。



圖八：4G行動通訊系統建置擷取存取使用者
IP連線紀錄

(2) 固網通訊

網際網路由網際網路服務提供(Internet Service Provider, ISP)建造網路互相連結，網路使用者家中的電腦會以存取線路連結存取點(Access Point, AP)，AP又會透過光纖纜線之類的線路連接網路操作中心(Network Operation Center, NOC)，NOC會透過光纖纜線連結全世界各地網路業者的NOC，所以只要加入一網路業者的服務，就能連接全世界的網路。連結用戶住家與網路據點(例如機房)的線路稱為存取線路，目前有ADSL、有線電視(Cable Television, CATV)與光纖到府FTTH [13]。



圖九：網路業者之網路架構

2.網路通信紀錄保留之法規檢視與修法建議

揆諸通訊保障及監察法規定通信紀錄調取與通訊的監察，科技偵查法草案中更是洋洋灑灑明定有關被歸類為科技設備之法定程序，但卻尚未針對網路通信紀錄作相關修訂與規範，惟網路生活已是趨勢，犯罪者亦深知只要使用VPN跳板服務，警方也莫可奈何。為合法調閱網路通信紀錄，及賦予電信業者儲存與提供紀錄之義務，因此舉係干涉人民自由與權利之措施，須有法律明文規範。

(1)現行通訊保障及監察法規定「通信紀錄」，而未明確定義「網路通信紀錄」

通訊保障及監察法為我國對於通信相關強制處分之特別法，「通信紀錄」定義於第3-1條：謂電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。電信法第2條定義「電信」：指利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息。從文義解釋，網路通信紀錄理應符合使用人使用電信業者提供之網路服務，並以科技產品發送、傳輸文字聲音等訊息，電信系統產出IP位址等規定，惟尚需更明確相關規定以符法律保留原則。

(2)明定「網路通信紀錄」(即網路連線資訊)之定義

連線資訊可由電信事業現有網路設備所產生網路流量紀錄資訊之取得，係使用者於使用期間內之發送方(Source)、接收方(Destination)之網際網路位址(IP Address)與通訊埠(Port)、協定(Protocol)、通信日期、通信起迄時間(Start/End Time)、封包大小、封包數量(Number of Packets)、域名伺服器(Domain Name Serve)查詢(Request)與回應(Response)等欄位資訊，未涉及通訊內容[14]。

(3)明確賦予電信事業儲存建置資料庫與提供調閱網路通信(連線)紀錄之義務

現行通訊保障及監察法施行細則規定
電信事業(包括第二類電信事業)有協助執行
通訊監察之義務，為完整網路通信紀錄之保
存及所需軟硬體設備之建置，應參照電信事
業協助執行通訊監察之義務，配合建置及提
供調閱網路通信紀錄。

四、運用網路通信紀錄之偵查作業程序

以下為偵查人員偵辦刑事案件與聲請調閱網路通信紀錄調取票之流程建議。

1.刑事偵查程序

(1)發動偵査

因告訴、告發、自首或其他情事知有犯罪嫌疑者，應即開始偵查。（刑事訴訟法第228條至第231條）

(2)鎖定犯嫌使用通信電話或IP

犯嫌可能使用之電話、曾上線登入電商平台、網路論壇之IP與使用帳號，匡列犯嫌對外聯繫之電信資料。

(3)依法聲請調取票

依涉案刑法罪章類別，最重本刑三年以上有期徒刑之罪，有事實足認通信紀錄於本案之偵查有必要性及關聯性，以書面聲請管轄法院核發調取票（通訊保障及監察法第11-1條第1、2項）；為偵辦最輕本刑十年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪防制條例等罪，而有需要時，得由檢察官依職權或司法警察官向檢察官聲請同意後，調取通信紀錄（通訊保障及監察法第11-1條第3項）。

(4)向電信業者調閱網路通信紀錄

警方向管轄法院或地檢署聲請調取涉案電話或IP之網路通信紀錄，依各家電信業者收件作業方式，可透過刑事警察局通訊監察科建置投單系統上傳申請，或是使用公文調閱。

(5)使用通聯分析程式過濾分析連線通信標的IP

根據電信業者回復電信標的之網路連線紀錄，篩選、歸納整理曾與調閱目標IP或電話曾經連線IP，再調閱相關申登人資料。

(6)重複程序項目2至項目5，案件破獲、逮捕犯嫌。



圖十：刑事偵查流程圖

2.分析「網路通信紀錄」欄位與自動化程式概念

電信業者提供網路通信紀錄欄位有「編號」、「日期與時間」、「來源IP」、「目的IP」、「協定」、「封包長度與資訊」等

紀錄。根據網路連線方式，來源IP與目的IP會彼此互相連線，故網路通信紀錄的調閱的目標IP，亦會成為source（來源）與destination（目的），目標IP可能是第一筆網路通聯的source IP（連線至其他目的IP）、第二筆網路通聯的destination IP（由其他IP連線至目標IP）。如同語音雙向通聯有發話受話方向，調閱的目標門號可能是通聯第一筆資料中的發話電話、通聯第二筆資料的受話電話。

圖十一：網路通信紀錄示意圖

了解網路通信紀錄的欄位與內容後，由於調閱目標IP可藉由網路傳輸協定判別實際連網活動情形，可分門別類調閱目標上網活動，可預見網路通信紀錄資料量很大，為幫助偵查人員快速整理分析該資料，有必要製作一自動化程式用以整理網路通信紀錄，使偵查人員能有效率檢視資、快速鎖定可疑目標，使偵查資源能最大化運用。

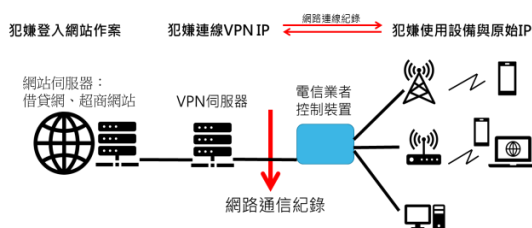
Python是一種廣泛使用的直譯式、進階程式、通用型程式語言。Python支援多種程式範式，包括物件導向、結構化、指令式、函數式和反射式程式。它擁有動態型別系統和垃圾回收功能，能夠自動管理記憶體使用，並且其本身擁有一個巨大而廣泛的標準庫。Python的設計哲學強調代碼的可讀性和簡潔的語法，尤其是使用空格縮排劃分代碼塊。相比於C或Java，Python讓開發者能夠用更少的代碼表達想法。不管是小型還是大型程式，該語言都試圖讓程式的結構清晰明瞭[15]。網路通信紀錄篩選工具會以Python作為本次使用程式，以期符合外勤同仁易於瀏覽閱讀、快速找到與犯罪相連之IP，承辦人不需要先行理解複雜網路知識，透過直覺式篩選鍵即可得出極具案件偵辦價值之資訊。

五、案例應用

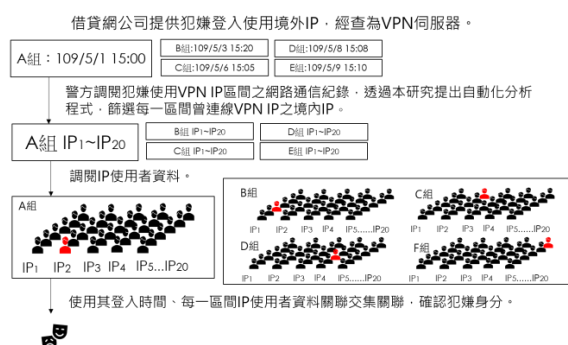
本次案例即是民眾依賴網際網路而生之犯罪型態，無論行為人使用行動網路、無線網路分享或實體網路線路，故本研究所提出之網路通信紀錄可應用在任何網路節點連線情形，作為犯罪偵查使用。

案例模擬：偵辦詐欺集團於借貸網站詐騙人頭金融帳戶，透過超商交貨便掌握包裹寄送進度。

1. 類型：犯嫌透過連線虛擬私有網路(下稱VPN)隱匿原始IP。
2. 案情：詐欺集團透過VPN連線至借貸網與超商交貨便網頁登入帳號，刊登廣告以借錢低息名義吸引被害人，運用話術要求被害人至超商使用店到店寄出金融帳戶存摺與金融卡，犯嫌使用超商交貨便網站服務取得寄貨編號，同時掌握貨運物流進度，再通知收簿手或詐欺取款車手領取包裹，接續等候詐欺集團指示使用人頭戶金融卡提領詐欺贓款。
3. 偵辦方式：警方方向借貸網與超商網站調閱涉案帳號之登入IP歷程，發現犯嫌使用境外IP分別於109年5月(下同)1日15時0分、3日15時20分、6日15時5分、8日15時8分及9日15時10分登入網站，查詢涉案IP於Whois主機伺服器，研判犯嫌透過VPN隱匿原始IP，向電信業者調閱涉案IP於上揭時段區間於我國境內IP連線紀錄，據以找出犯嫌原始使用IP，交集IP使用者資料縮小範圍以確認犯嫌實際使用行動門號、連線WiFi位置或有線區域網路申裝地址。
4. 分析方法：透過網路連線紀錄取得曾經連線VPN之IP，運用時間排序與關聯分析交集，找出詐欺集團使用IP與實際使用門號。



圖十二：犯嫌透過VPN之擷取網路通信紀錄示意圖



圖十三：偵辦犯嫌使用境外IP調取網路通信紀錄與分析示意圖

六、結論及後續研究

民眾取得網路使用較之過往是非常方便又快速，又可不受時間、地點之限制，使民眾更加倚賴網路的方便性，使犯罪者更肆無忌憚透過網路向民眾伸出魔爪，比如透過網路社交平台的一頁式詐騙、接獲詐騙電話猜猜我是誰加入犯嫌的LINE帳號，透過通訊軟體買毒賣毒等犯行，犯罪行為無不躲藏於網路世界並且與之緊密連結，迫使偵查犯罪方法亦隨著民眾生活習慣與犯罪型態變化而有所改變，故本研究提出網路通信紀錄之概念，嘗試解決電話語音通聯之不足、境外網路服務業者因法律問題不願提供涉案帳號註冊資訊、目前技術上無法解密網路語音內容徒增監察辛勞、通訊監察只能保留經法院核准後之網路通信資料等情況，透過網路通信紀錄找出用戶連線網路另一端之使用者資料，俾偵查人員有更多偵辦資料與方向。

為符合民主、法治國原則，首先增修通訊保障及監察法，以明確定義「網路通信紀錄」與聲請調閱之刑事案類門檻，予電信業者建置、擷錄與保存相當期間網路通信紀錄資料庫之責任與義務，以供偵查單位調取資料分析。另提供一分析網路通聯之自動程式，為使該程式結合警察機關之資料庫與使用上便利，選用Python程式編寫，以期協助外勤人員快速整理歸納網路通聯，使偵辦案件更加效率。並舉例實務上發現詐欺集團利用借貸網誘騙不知情民眾騙取其金融存摺與取款卡，如何運用網路通信紀錄追查本案之犯嫌，證明在犯罪偵查上是有偵辦之需求及重要性。現行犯罪之發生、場所及工具很難不與資通網路無關，更是常見因各式型態網路普遍而衍生犯罪態樣，若能調閱「網路

通信紀錄」，試圖從網路連線紀錄找出涉案人使用IP，案件就有很大的機會續行偵辦，也印證「網路通信紀錄」在偵查犯罪面有保存之價值，遑論相關法制化與完整建立儲存資料機制。

當偵查機關透過偵查犯罪取得網路通信紀錄，藉以收集歸納犯罪者使用境外IP(比如詐騙集團使用)，警政機關提供警示IP，整合至電信業者網路通信資料庫內作為犯罪預警及阻擋惡意攻擊之參考，此為未來研究方向及預防犯罪之用。

參考文獻

- 1.電信管理法總說明，民國108年。
- 2.財團法人台灣網路資訊中心，2019台灣網路報告，民國108年。
- 3.朱子函，我國網路通訊監察困境之研析，刑事雙月刊第80期，民國106年，第56-59頁。
- 4.邱紹洲，通聯紀錄在犯罪偵查上之應用，中央警察大學刑事警察研究所碩士論文，民國90年。
- 5.李文章，數位資訊在犯罪偵查上之應用——以目標軌跡、全球衛星定位系統、電話通聯電腦分析系統為例，中央警察大學刑事警察研究所碩士論文，民國93年。
- 6.黃茂穗，行動APP通訊詐欺犯罪手法與被害特性之研究，中央警察大學警政論叢第十四期，民國93年，第109-141頁。
- 7.汪毓瑋等人合著，跨國（境）組織犯罪理論與執法實踐之研究分論，台北：元照出版有限公司，民國101年，第212-225頁。
- 8.警政署統計室，警政統計通報 108年網路犯罪概況，民國109年。
- 9.擷取自維基百科：https://en.wikipedia.org/wiki/Virtual_private_network，2020。
- 10.科技偵查法草案，法務部，民國109年。
- 11.曲建仲，5G技術大補帖，科學月刊第607期，民國109年，第20-23頁。
- 12.胡志男、周傳凱等，4G生活大未來，高雄：財團法人電信技術中心，民國102年，第97-112頁。
- 13.井上伸雄著、李漢庭譯，全彩圖解通信原理，台北：臉譜出版，2017年，第40-41頁、第80-95頁。

14.通訊保障及監察法部分條文修正草案總說明，民國107年。

15.擷取自維基百科：<https://zh.wikipedia.org/wiki/Python>，2020。

應用於犯罪現場之帳密取證與特徵分析實證研究

許庭于

中央警察大學資訊管理學系學生

ch5566444111@gmail.com

吳國清

中央警察大學資訊管理學系教授

wkc@mail.cpu.edu.tw

摘要

長久以來，數位鑑識軟體工具對於手機和電腦等設備之靜態取證、處理、鑑定和分析等進展上，已經取得突出的表現，並對資安事件和電腦犯罪案件等鑑識上，作出顯著的貢獻。然而，受到世界各國對資安的重視和登入應用程式的身分驗證的日趨保護，以及防止隱私或機敏性資料儲存到本機磁碟內，實已讓執法人員在案發現場取證上，造成科技執法的一大挑戰與有待解決的問題。鑑此，本研究擬以實證方法，採用不同登入應用程式和不同地點進行實機與實地試驗，並取得 249 個有效樣本數。研究結果顯示：(1) 有八成機率可在電腦 RAM 內成功找到帳號和密碼，且出現在 RAM 不同位址數量不少；(2) 取得帳號和密碼成功機率排名分別為臉書（最易）、網路購物、電子郵件、LINE（最難），LINE 的失敗率為 57.14%；(3) 不同登入程式和試驗成敗存在關聯性；(4) 以<..密碼..>特徵較為顯著，且可由 RAM 的低位址方向去找到它們。

關鍵字：主記憶體、密碼、數位鑑識、揮發性記憶體

一、前言

私有瀏覽（Private Browsing, PB）設施是許多主流網際網路瀏覽器的一部分。因此，那些從事惡意或非法瀏覽行為的人以私有化方式進行瀏覽的可能性增加了。許多私有瀏覽模式被設計為「本機私有」，提供使用者的瀏覽行為資料不被儲存在他所用的本機硬碟內。例如，Google Chrome 瀏覽器的隱身模式（Incognito Mode），微軟 Edge 瀏覽器的使用私有（InPrivate）選項設定，或者 firefox 瀏覽器的私有視窗（Private Window）等。這樣的行為，雖然將可大為確保資訊的機敏性，但卻也可能損害任何證據資料的可用性和完整性，導致駭客或嫌疑犯可利用這種功能來從事非法活動，實已對調查資安事件或偵辦電腦犯罪帶來挑戰和頭痛的問題 [2]。執法機關司法警察（官）、資安或數位鑑識人員已關注到數位鑑識特點和 PB 所帶來的風險，即防止潛在的數位證據被儲存在本地設備上。雖然 PB 本身並非為反鑑識（Anti-Forensic）而設計的，但它可以用作反鑑識的用途。

揮發性記憶體的使用經常被認為是

私人瀏覽歷史恢復的一個位置[8]，然而這項作用並非在於實體隨機存取記憶體（Random Access Memory, RAM）的抓取和 PB 內容的分析。實體記憶的抓取仍然不是所有犯罪現場的普遍做法，尤其是嫌疑犯已在執法人員抵達犯罪現場之前，就早已關閉電腦電源了。因此，警方必須在偵查不公開下，快速進行搜索扣押動作，有一些關鍵或機敏性資訊高度仰賴現場取證（Live Acquisition），而無法從靜態取證（Static or Dead Acquisition），例如，警方在嫌疑犯正在上網（電腦處於開啟）且他始終保持緘默權之情況下，逕行對 RAM 獲取身分驗證用的帳號和密碼，是件有待克服的挑戰。基於此，本研究擬嘗試透過實證研究途徑，以研究人員持有不同的帳號、密碼，在不同地點和不同登入程式，Wifi 和行動數據，移動中和靜止狀態等不同情境下，利用數位鑑識軟體去抓取 RAM 內的帳號、密碼，並期望達到下列之研究目的：

- (1) 試圖了解是否可找到帳號、密碼；
- (2) 登入程式取得帳號、密碼的難易排名；
- (3) 試圖分析找到的密碼與其相對應配置

RAM 位址的特徵。

二、文獻綜述

1. 名詞解釋

數位證據指儲存媒體中任何足以證明犯罪構成要件或關聯的電子數位資料，亦即在儲存媒體內以電磁紀錄方式儲存可供佐證犯罪之資料，包括有文字、圖片、聲音、影像等型態。數位證據可視為電腦科學與鑑識科學兩個領域之結合，其中電腦科學提供了電腦基本常識及技術來處理數位證據，而鑑識科學則提供了處理傳統證據的方法與步驟，結合這兩項專業知識後，才得以確保數位證據之有效性[1]。

記憶體鑑識 (Memory Forensics) (也稱為記憶體分析) 是指對電腦記憶體傾印中的揮發性資料進行分析。刑事執法 (數位鑑識) 官員或資訊安全專業人員進行記憶體鑑識，以調查和確定不容易在硬碟資料上留下痕跡的攻擊、入侵、竊取或其他惡意等非法行為。記憶體鑑識可視成一種分析電腦記憶體 (RAM) 以解決數位犯罪 (Digital Crimes) 的藝術。

揮發性資料 (Volatile Data) 是指電腦運行時臨時儲存在記憶體中的資料，或是隨著時間的推進而使資料隨之變動。駐留在電腦主記憶體內的揮發性資料，可以包括身分驗證、瀏覽歷史、聊天資訊、編輯文件、剪貼簿……等內容資料，及正在執行中的前景和背景程式名稱。例如，如果我們正在使用 Word 或 Pages 等軟體編輯一份文件內容時，但因尚未儲存到硬碟或其他非揮發性儲存媒體內，卻遭遇到電腦不預警的當機或斷電時，若重新開機後，則原留在主記憶體內的資料就會「幾乎」¹全部丟失掉。

記憶體傾印 (Memory Dump) (也稱為核心傾印或系統傾印) 係指對特定瞬間 (某一個時刻點) 的電腦記憶體 RAM 資料的快照抓取 (Capture)。在電腦發生當機、關機或安全性漏洞等事件發生之前，記憶體傾印可以包含有關係系統狀態和有價值的潛在數位證據資料。記憶體傾印包含 RAM 資料，可用於確定資安事件或犯罪

案件的原因和其他有關發生的關鍵細節，及其犯罪跡證[5]。

雕刻或拼湊過程 (Carving or Salvaging Process) 是指從映像檔案 (Image File) 中，將散落在磁碟或記憶體中的檔案碎片或記憶體的離散分頁內容，使能還原回來的過程[7]。由於這項程序涉及到文字編碼系統和識別表示用意之證明，故可能較耗費人力和較長的工時，而且也只能得到片斷的資訊，即對證據之證明力較薄弱些。基於此，它比較適合在獲取資訊量較少的取證上。例如，身分驗證用的帳號、密碼，或是關鍵詞 (如專案或程式名稱) 等。

2. 文獻探討

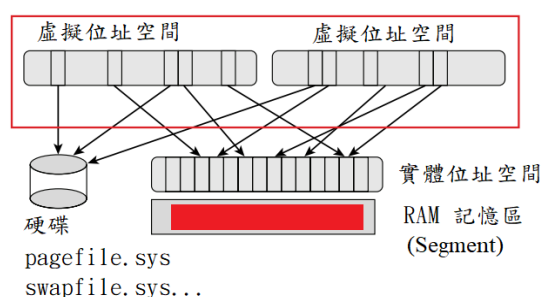
記憶體存取和記憶體管理是現代電腦操作中非常重要的一部分[9]。每條指令在執行之前都必須從記憶體指令碼區 (Code Segment) 中取出 (Fetch)，大多數指令都涉及到從記憶體中檢索資料或在記憶體中儲存資料。

記憶體管理乃是作業系統管理實體記憶體的分配、重分配和組織的演算法。這些演算法通常取決於設備硬體的支援。由於現今電腦已提供了多個並行處理程序、多執行緒，及多個核心數目和邏輯處理器等系統功能，可讓中央虛擬記憶體作業系統 (Virtual Memory Operating Systems) 為每個程序提供了自己私有的虛擬位址空間。這種抽象在過程看到的邏輯記憶體和安裝在機器上的實際實體記憶體之間建立一個分離。因此，使用者可以編寫程式，好像它們可以存取整個實體位址空間，並且所有記憶區 (Memory Segments) 都是常駐的記憶體。但實際運作機制上，位址空間的某些分頁 (Pages) 可能並不常駐在 RAM 內。作業系統透過背景處理，使記憶體管理器負責將記憶體的區域轉移到次級儲存 (如硬碟根目錄內的 pagefile.sys、swapfile.sys、recovery folder……) 中以釋放 (Release) 實體記憶體的空間。在執行過程中，記憶體管理器和記憶體管理單元 (Memory Management Unit, MMU) 一起

¹ 開機後，電腦會主動從 Recovery 資料夾內

的檔案，載入到主記憶體 RAM 內。

工作，將虛擬位址轉化為實體位址。如果一個執行緒存取了一個已經轉移到次級（硬碟）儲存的虛擬位址，那麼該資料就會被載入到實體記憶體中，通常是透過頁面錯誤（Page Fault）而引發例外處理和中斷機制來完成²。這種交互作用的運作機制，如圖一所示[4]。當執法或鑑識人員對記憶體管理運作有了初步了解後，將有助於記憶體鑑識概念的建立與數位證據取證工作的展開。由圖一示意圖中，也說明了為何執法或鑑識人員在抓取記憶體（Capture Memory）的同時，也可能會去獲取 pagefile.sys 檔案的原因。這種作法也出現在現今數位鑑識軟體上，如 FTK Imager 或 Encase Forensic 等產品。



圖一：多個虛擬位址空間共享記憶體和
硬碟示意圖

資料來源：Ligh et al. (2014) [4]

由於電腦的中央處理單元（CPU）存取並處理資料不可以直接存取儲存媒體內的檔案，而是必須透過主記憶體（或稱記憶體）來為之。因而，不論是資料（含錄音、錄影或電磁紀錄）和執行檔案（含.com、.exe、dll）等，都須載入（Load）到記憶體 RAM 內；而 CPU 則須透過已載入到 RAM 內的系統或應用程式執行，方能對資料進行搬移（Move）、處理和運算，並將執行結果暫存到 RAM 內。此外，現今和未來 RAM 記憶容量將高速成長，使得依賴 pagefile.sys 機會將大為減少，以獲得電腦處理效能的提升。

在許多情況下，使用者或駭客的上網活動與攻擊或威脅有關的關鍵資料將僅存在於系統記憶體中，例如網路連接、帳戶身分驗證、電子商務購物、聊天資訊、加密金鑰、正在運行的程序、電子郵件、嵌入的代碼片段，以及網際網路活動歷史紀錄等資料。現今，在資安威脅風險和電腦犯罪案件隨著攻擊或入侵手法趨於更多元且複雜而增加，況且許多基於網路的安全解決方案（如防火牆和防病毒工具）無法即時偵測到隨機載入電腦實體記憶體中的惡意軟體。因而，導致記憶體鑑識工具和技能已成為當今資安和鑑識專業人士的迫切需求和技術水準的強化。資安團隊或執法機關可能尋求記憶體鑑識工具和專家的幫助，以確保可取得無法透過硬碟檔案找到的潛在數位證據。雖然，現在最複雜的企業資安系統都具有初步的記憶體鑑識和行為分析功能，可以識別系統實體記憶體中是否存在惡意軟體（如 rootkits 和零日攻擊），不過離實用功能仍有一段差距，包括普遍缺乏儲存在記憶體中的揮發性資料的分析能力，資料的雕刻與湊合成一段可表示用意之證明內容等。

主記憶體取證與磁碟取證之差別：前者可以被認為是系統的當時快照，可在使用過程中為鑑識人員提供近乎即時的系統映像（Image）；後者則集中於資料恢復和解密，通常是從有關驅動器（Driver）的映像著手進行。因而，可將主記憶體取證視為對當前資安威脅或電腦犯罪的立即回應，而磁碟取證則可視為已發生事件的事後檢驗。鑑識人員應根據調查的性質，於兩種技術中選擇適當的操作來獲取有關該系統的更多資訊。

揮發性資料（Volatile Data）常見於揮發性記憶體（Volatile Memory）。指當電力供給中斷後，所儲存的資料便會消失在電腦記憶體 RAM 內；非揮發性記憶體（Non-Volatile Memory）所儲存之資料，僅需重新供電即可重新和重複讀取記憶體資料。

揮發性數位證據特性包括：（1）易變

² 當作業系統為了讓新的頁面載入到記憶體時，就會將駐留（電子）記憶體的頁面（Page）轉移到（機械運轉）磁碟去，於是就會發生分頁（Paging）。許多作業系統透過分頁來容納量

大而無法常駐在實際記憶體的資料。然而如果系統常發生分頁，將會導致電腦整體效能的降低。

性：揮發性數位證據內容隨時間和電腦運轉而不斷在變動著；(2) 萃取與分析難[10][6]：因為主記憶體傾印後所建立的映像檔案，係與文字編碼系統有關，另也會涉及到記憶體配置位址策略演算法所帶來的內部碎片化 (Internal Fragmentation) 和外部碎片化 (External Fragmentation) 之殘留資料問題。故在雕刻拼湊和語意分析，有其難度；也可能找到的資料內容確為假陽性擊中 (False-Positive Hits)，而造成數位證據的錯誤解讀或誤判。因此，執法人員必須確保正確獲取記憶體的映像檔，並保持其完整性：若沒有清晰地抓取映像檔，則映像檔中將留下很少內容可供進行分析；(3) 不可逆性：揮發性數位證據消逝後即無法再回復[3]，即資料內容不具可重複性。如當電腦關機後，主記憶體內資料就會消失。總之，揮發性數位證據專用鑑識軟體工具的發展和執法人員的取證、鑑定和分析等水準，仍有待努力。

三、研究方法

1. 資料來源

本研究之資料來源，係由研究人員親自到學校、醫院、派出所、住家、大賣場、超商、速食店、火車站、捷運站及圖書館等場所，透過個人所擁有的多組帳號、密碼和筆記型電腦，經由社群軟體、網路購物及電子郵件等登入畫面，輸入帳號、密碼與登入成功後，再登出它。隨後以 FTK Imager 軟體去嘗試取得該組帳號、密碼是否可在筆記型電腦的主記憶體 RAM 內找到它們。最後將結果記錄在 Excel 檔案內。其取樣時間從 2020 年 1 月 9 日起至 2020 年 7 月 27 日止，共得到有效樣本 249 筆。由於本研究必須在嘉義、桃園和台北等三個地方進行取樣，因此，資料取得十分辛苦。

2. 研究工具

- (1) 電腦設備：ASUS 筆記型電腦，作業系統為 Windows 10，CPU 核心數目為 4，邏輯處理器為 8，主記憶體 RAM 為 4GB。
- (2) 軟體設備：AccessData FTK Imager 4.3 版；StataMP-16 專業統計軟

體。

- (3) 開發語言：Word VBA、Excel VBA、R 語言和 StataMP-16 ado script 語言。

3. 實施步驟

- (1) 主記憶體 RAM 的傾印 (Dump)。
- (2) 帳號、密碼的萃取與 RAM 位址的記錄。將原始的帳號密碼換為十六進位(如:將密碼轉換為 630070007500650064007500740077003800370031003100 38003700，見圖 1)，在 FTK Imager 中快速搜尋所得之位址後，如圖二所示，將它們記錄於 Excel 中(如:密碼出現於位址 009c82800 - 009c8280B)，並記錄帳號、密碼出現之次數及其前後內容。
- (3) 去除 RAM 內帳號密碼位址的前後內容亂碼。
- (4) 將以集合表示的密碼 RAM 位址加以展開。
- (5) 進行各種統計分析。

309c82700	88 01 00 00 00 00 00 00 00-5B 00 00 00 00 00 00	[.....
309c82710	00 00 00 00 0E 00 00 00 00-20 00 00 00 00 00 00	
309c82720	80 01 00 00 00 00 00 00 00-00 00 00 01 00 00 00	
309c82730	02 00 00 00 03 00 00 00 00-70 01 00 00 00 00 00	p.....
309c82740	80 01 00 00 00 00 00 00 00-80 01 00 00 00 00 00	
309c82750	10 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	
309c82760	0E 00 00 00 03 00 00 00 00-6E 5B 78 1A FF 00 00	E[we y.....
309c82770	10 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	
309c82780	14 00 00 00 06 00 00 00 00-50 00 41 00 53 00 53 00	P A S S.....
309c82790	57 00 44 00 00 00 00 00 00-10 00 00 00 00 00 00	W D.....
309c827a0	08 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	
309c827b0	10 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	P A S S.....
309c827c0	14 00 00 00 06 00 00 00 00-50 00 41 00 53 00 53 00	P A S S.....
309c827d0	57 00 44 00 00 00 00 00 00-10 00 00 00 00 00 00	W D.....
309c827e0	08 00 00 00 00 00 00 00 00-24 00 00 00 0E 00 00 00	S.....
309c827f0	63 00 70 00 75 00 65 00 64 00 75 00 74 00 77 00	c p u e d u t w.....
309c82800	58 00 37 00 31 00 31 00 38 00 37 00 00 00 00 00	8 7 i i g 7.....
309c82810	10 00 00 00 08 00 00 00 00-70 61 73 73 77 6F 72 64	password.....
309c82820	08 00 00 00 00 00 00 00 00-10 00 00 00 00 00 00	
309c82830	08 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	
309c82840	10 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	
309c82850	1C 00 00 00 0A 00 00 00 00-6C 00 6F 00 67 00 69 00	l o g i.....
309c82860	6E 00 49 00 6E 00 70 00 75 00 74 00 00 00 00 00	n i n p u t.....
309c82870	10 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	
309c82880	08 00 00 00 00 00 00 00 00-10 00 00 00 00 00 00	
309c82890	08 00 00 00 00 00 00 00 00-08 00 00 00 00 00 00	

圖二：已在 RAM 找到密碼範例

四、研究結果與討論

1. 敘述統計

從表一統計結果顯示，在本研究實證總次數為 249 次中，成功次數為 203 次，占整體的 81.53%；失敗次數為 46 次，占整體的 18.47%。其中，獲取帳號密碼失敗者，以 LINE 最多，計 28 次，占全部 LINE 次數的 57.14%，占整體失敗次數的 60.87%；其次是網路購物（如淘寶網、yahoo 超級商城、蝦皮），計 15 次，占全部網路購物次數的 10.49%，占整體失敗次

數的 32.61%；電子郵件失敗次數為 3 次，占全部電子郵件次數的 12.00%，占整體失敗次數的 6.52%；而每次獲取帳密皆成功者為臉書。因此，刑事偵查人員在電腦開機狀態下對嫌疑犯的帳密「現場取證」

(Live Acquisition)成功機率排名分別為：臉書、網路購物、電子郵件、LINE。由此可見，臉書對使用者的身分驗證可被揭露最容易，LINE 最困難。

表一：依登入程式分類統計

登入程式類型		臉書	LINE	網路購物	電子郵件	總計
帳密試驗	次數	32	49	143	25	249
	成功	32	21	128	22	203
	失敗	0	28	15	3	46
所占百分率		12.85	19.68	57.43	10.04	100.00

在網路型態試驗上，Wifi 網路為 177 次（71.08%），行動數據網路為 72 次（28.92%）。在登入地點上，本試驗以火車站（含台北、桃園、嘉義）83 次最多，其

次是速食店（42 次），從甲地到乙地搭車途中上網試驗為 32 次，超商為 25 次，住家為 16 次。

表二：依登入地點分類統計

登入地點類型	試驗次數	所占百分率	累計百分率
火車站	83	33.33	33.33
速食店	42	16.87	50.2
移動中(註)	32	12.85	63.05
超商	25	10.04	73.09
住家	16	6.43	79.52
警大	15	6.02	85.54
圖書館	12	4.82	90.36
大賣場	8	3.21	93.57
派出所	6	2.41	95.98
捷運站	5	2.01	97.99
醫院	5	2.01	100.00
總計	249	100	100

註：移動中表示登入帳號密碼當時，正處於移動狀況，即在搭乘交通工具的途中。

2. 帳號密碼試驗關聯檢定

本研究針對登入程式的類型和試驗成敗，進行卡方關聯檢定：

H_0 ：不同登入程式和試驗成敗無關聯

H_1 ：不同登入程式和試驗成敗有關聯

從表三的卡方關聯檢定結果顯示，卡

方值為 62.6479，機率值小於 0.001，這表示不同登入程式和試驗成敗有關聯存在，其關聯強度高達 0.5016。此外，在登入地點類型和試驗成敗關聯檢定上，卡方統計值為 18.2485，機率值為 0.954，Cramér's $V=0.1785$ ，未達顯著水準，這意味著試驗成敗與否是與不同登入地點無關聯。

表三：登入程式和試驗成敗關聯檢定

登入程式類型	取得失敗	取得成功
臉書	0	32
LINE	28	21
網路購物	15	128
電子郵件	3	22
Pearson chi2(3) = 62.6479 Pr = 0.000 Cramér's V = 0.5016		

3. 帳號密碼試驗相關分析

本研究針對登入程式類型、帳號密碼試驗成功次數、找到密碼數量等級、個人熱點

和使用狀態等變數進行相關分析。從表四皮爾森相關分析結果顯示，(1) 取得帳號密碼試驗成功所需次數多寡與其他變數呈現不相關。(2) 找到密碼數量多寡與臉書呈現正相關，而與 LINE 呈現負相關，這表示當刑事執行人員如果在臉書登入帳號和密碼且找到它們時，就可在出現很多主記憶體 RAM 位址內，但反觀 LINE 即使找到它們，但出現在 RAM 位址內數量很少。(3) 臉書較傾向沒有透過手機上網且在靜止狀態取得帳號密碼資料。(4) 個人熱點和使用狀態兩者呈現正相關，這意味著本研究試驗如處於移動狀態，就會高度依賴手機個人熱點。

表四：帳號密碼試驗皮爾森相關分析結果

	帳號密碼 成功次數	找到密碼 數量等級	臉書	LINE	網路購物	電子郵件	個人熱點	使用狀態
帳號密碼 成功次數	1							
找到密碼 數量等級	-0.0744	1						
臉書	-0.0839	0.1786*	1					
LINE	0.0757	-0.3584*	-0.1901*	1				
網路購物	0.0145	0.0473	-0.4460*	-0.5749*	1			
電子郵件	0.0017	0.0948	-0.1283*	-0.1654*	-0.3880*	1		
個人熱點 (註 1)	-0.0213	-0.0763	-0.1655*	-0.0038	0.1191	-0.0067	1	
使用狀態 (註 2)	-0.0744	-0.0085	-0.1475*	0.0212	0.0879	-0.0085	0.4433*	1

註 1：個人熱點表示使電腦是否透過手機熱點（Hot Spot）連網。

註 2：使用狀態係指連網登入帳號密碼是處於靜止或移動狀態下。

4. 出現密碼特徵分析

本文先前假設在密碼為已知情況去找出密碼出現在 RAM 的那些位址內。問題是執法人員如何判斷所取證到的一串資料就是嫌疑犯的密碼？這是個很有挑戰的議題。為了解決這個問題，本研究嘗試透過 AccessData FTF Imager 軟體來獲取已知的密碼資料，然後再透過人工方式加以記錄其相對應 RAM 位址值。當然這種做法對研究人員十分費時又費工，乃因為 FTF Imager 軟體並未提供 Script Language 來撰寫程式和自動化之故。此外，

位址表示法是採用集合，例如，研究人員找到密碼的 RAM 位址={00aa43ac0 - 00aa43ad0, 046344141 - 046344150, 046344640 - 046344650, 046344c40 - 046344c50, 12727f990 - 12727f9b0, 127bbe990 - 127bbe9b0, 15431d190 - 15431da90}。

從表五密碼特徵與 RAM 位址關聯分析結果顯示，(1) 特徵一係指只要找到密碼即可，但是這有個缺點，刑事執法人員無法確認該組密碼是嫌疑犯真正的密碼，或是為嫌疑犯的資料。(2) 特徵二為在密

碼的前後會存在一個以上 ASCII 控制字元。從表中發現它的卡方統計量機率值為 0.192，未達 0.05 的顯著水準，故執法人員較難確定密碼大概出現在低位址或高位址。(3) 特徵三為在密碼的前後會存在二個以上 ASCII 控制字元。由於它的卡方統計量機率值為 0.000，已達到非常顯著水準，另 $\gamma = -0.1532$ ，這表示執法人員當有找到<..密碼..>特徵時，真正的密碼大概出現在較低位址上。(4) 特徵四為在密碼的前後會存在三個以上 ASCII 控制字元。

其卡方統計檢定也達到非常顯著水準，它的 $\gamma = -0.2018$ 。這證明了特徵四和特徵三是一樣的情況，執法人員在低位址找到的密碼，比在高位址更具證據能力（密碼是否存在）、證據之證明力（密碼數量多寡）。因此，犯罪現場執法人員，只要找出滿足特徵三者，即往 RAM 低位址方向去找有<..密碼..>者，例如，「..\$RT123!az..」，就可去嘗試嫌疑犯的臉書、網路購物商店或電子郵件等。

表五：出現密碼特徵與 RAM 位址關聯分析

RAM 位址首 2 位	特徵一：密碼	特徵二：..密碼.	特徵三：..密碼..	特徵四：...密碼...
00	65(註)	54	41	33
01	84	63	36	31
02	88	65	48	38
03	72	60	46	35
04	98	73	49	37
05	92	73	46	29
06	79	68	44	29
07	110	81	63	42
08	61	41	21	16
10	37	31	21	17
11	64	45	27	18
12	51	39	21	17
13	53	42	27	20
14	54	46	28	17
15	116	90	44	19
16	33	21	3	2
卡方統計量與檢定	Pearson chi2(16) = 136.2139; Pr = 0.000; Cramér's V=0.3351; gamma = 0.6930	Pearson chi2(16) = 20.6578; Pr = 0.192; Cramér's V = 0.1331; gamma = - 0.0248	Pearson chi2(16) = 55.0121; Pr = 0.000 ; Cramér's V = 0.2172; gamma = -0.1532	Pearson chi2(16) = 53.6799; Pr = 0.000; Cramér's V = 0.2146 ; gamma = -0.2018

註：數值表示總計 249 次試驗中，有 65 次密碼出現在 RAM 位址首 2 位為 00 者。

五、結論

本研究透過人為操作取得 249 筆樣本數，然後利用 VBA、R 和 STATAado 等電腦語言，撰寫程式來進行清洗、處理和分析這些樣本，並得到下列結論：

- (1) 在 249 樣本數（即試驗次數）中，成功次數為 203 次，占整體的 81.53%；失敗次數為 46 次，占整體的 18.47%。

這顯示大約有八成機率可獲得暫存在電腦 RAM 內的帳號和密碼。

- (2) 帳號和密碼成功機率排名分別為臉書、網路購物、電子郵件、LINE。由此可見，臉書對使用者的身分驗證可被揭露最容易，LINE 最困難。
- (3) 不同登入程式和試驗成敗有關聯，然與不同登入地點無關聯。

(4) 找到密碼數量多寡與臉書正相關，
與 LINE 負相關，這意味著執行人員
臉書密碼會出現很多主記憶體
RAM 位址內，但 LINE 則出現數量

很少。

(5) 密碼以<..密碼..>特徵較為顯著，且
可由 RAM 低位址方向去找到它們。

參考文獻

1. Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet, Academic Press, Waltham, 2000.
2. Horsman, G., Findlay, B., Edwick, J., Asquith, A., et al., "A Forensic Examination of Web Browser Privacy-Modes," Forensic Science International: Reports 2019, pp:1-7.
3. Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., and Wright, C., The Official CHFI Study Guide (Exam 312-49): for Computer Hacking Forensic Investigator, Syngress, Burlington, 2007.
4. Ligh, M. H., Case, A., Levy, J., Walters, A., The Art of Memory Forensics Detecting Malware and Threats in Windows, Linux, and Mac Memory, John Wiley & Sons, Inc., 2014.
5. Lord, N., "What Are Memory Forensics? A Definition of Memory Forensics," Digital Guardian, <https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics>, 2020/09/24.
6. Maclean, N., "Acquisition and Analysis of Windows Memory," Forensic Informatics, 2006.
7. Nelson, B., Phillips, A., and Steuart, C., Guide to Computer Forensics and Investigations: Processing Digital Evidence, Cengage Learning, 2016.
8. Satvat, K., Forshaw, M., Hao, F., and Toreini, E., "On the Privacy of Private Browsing - A Forensic Approach," Data Privacy Management and Autonomous Spontaneous Security 2014, pp: 380-389.
9. Silberschatz, A., Gagne, G., and Galvin, P. B., Operating System Concepts, Wiley India Pvt. Limited, 2018.
10. Stefan, V., Felix, C. F., "A Survey of Main Memory Acquisition and Analysis Techniques for the Windows Operating System," Digital Investigation, Volume (8:1) 2011, pp:3-22.

國家圖書館出版品預行編目（CIP）資料

2020 年第 23 屆資訊管理學術暨警政資訊實務研討會：「網路犯罪與跨域資安治理」論文集 / 廖有祿編輯. -- 初版. -- 桃園市：中央警察大學資管系, 2020.11

面；公分

ISBN 978-986-98280-5-5 (平裝) NT\$: 150

1.資訊管理 2.數位偵查 3.網路犯罪 4.資安治理

575.807

109017745

2020 年第 23 屆資訊管理學術暨警政資訊實務研討會-「網路犯罪與跨域資安治理」論文集

發行者：黎文明

編輯者：廖有祿

出版者：中央警察大學資訊管理學系

作者：高信雄、溫哲彥、張凱評等著

地址：33304 桃園市龜山區大崗里樹人路 56 號

電話：(03)328-5189

印刷者：尚暉文化事業有限公司

地址：22066 新北市板橋區板新路 103 號 4 樓之 1

電話：(02)2958-6010

定價：新台幣一百五十元

二〇二〇年十一月初版

版權所有，翻印必究