

輔仁大學資訊管理學系

專題計劃書



臉書實名制
Facebook Identifier

指導教授：葉承達教授

專題成員：

吳柏緯408402066(組長)

黃品綺408402212(組員)

盛慧欣408402327(組員)

張哲維408402377(組員)

吳承翰408402432(組員)

目錄

第一章 系統描述

一、發展背景與動機-----	1
二、系統發展目的-----	2
三、系統範圍-----	4
四、背景知識-----	10
五、系統限制-----	20

第二章 軟體需求規格

一、功能需求-----	21
-------------	----

第三章 軟體設計功能

一、介面設計-----	29
二、資源需求-----	32

第四章 專題實作討論

一、模型訓練結果-----	33
二、發展中遭遇到的問題、困難與解決辦法-----	36
三、系統優缺點 (SWOT) 評估-----	36
四、發展心得-----	36
五、未來展望-----	36

附錄

一、分工及貢獻度說明-----	37
二、參考資料-----	38

第一章 系統描述

一、發展背景與動機

隨著網路的發展，越來越多人使用社交軟體，以線上的方式與他人交換訊息，除了聯絡好友感情，也有人使用這種軟體替自己的商品作宣傳促銷，直接使用社交軟體進行販賣通路的賣家也不在少數，為了因應此種風氣，許多社交軟體也都已經內建了賣場功能。

然而科技帶給人們的不只是便利性，也替有不良意圖的人們增加了更多接觸民眾的通道，除了詐騙以外，也有廣告主會利用假帳號，發布大量的留言，來營造「假的」品牌形象，其所造成的結果小至謠言遠播，大至損失生命財產，我們也可以由此看出假帳號對於資訊安全的嚴重性，也有立即解決之必要性。



圖1-1 買讚廣告【Smile網路行銷暴紅工作室。
取自：<https://smilegood.cyberbiz.co/>】



圖1-2 露天商品介紹圖【取自：<http://www.ruten.com.tw/item/show?21935651715836>】

如圖可看到，社群媒體上的買粉/讚風氣非常興盛，甚至已經有許多專門販售這些服務的網站出現，這讓所謂的「熱門貼文」變成可以人為塑造的產物，許多擁有特定立場的文章也可能會用這種手段，來改變人們對某些議題的看點，也就是所謂的「帶風向」。

2009年臉書 (Facebook) 在台灣興起，不管是個人、企業、政府，大家爭相註冊了臉書帳號，可以說是一人一帳號的廣布程度，然而由於廣告、假帳號的猖獗，近期臉書的使用者有明顯萎縮的現象。

比起原先的社交功能，臉書在大眾 (尤其是年輕人) 心裡的定位已經逐漸轉換為「一個得到商品優惠資訊的通道」，大多數民眾使用臉書的原因為「想要得到關注商品的最新優惠消息」，以及「觸及更多相關的商品品牌」，大多使用者選擇商品時常會受其他使用者的評價影響，在大量使用假帳號洗評論下，好評價與高滿意度都可以用買的得到，可信度也因此大大降低。

除了身為消費方的民眾恐怕會受假的品牌形象所騙以外，身為廣告方的企業也可能受到財務上的影響。廣告商可通過購買臉書的廣告增加觸及率，假設廣告商花了一筆錢買了20萬的觸及率，但因為假帳號太多，這20萬的觸及用戶可能有一大半都不是真人，那麼，廣告

商的錢便付之東流了。

虛假帳戶會隨機點擊廣告或「點讚」頁面，來躲過反欺詐算法的監測。這些行為也欺騙了廣告商，但卻給公司帶來巨大收益。虛假帳戶還經常通過詐騙、假新聞、勒索或其他欺騙手段，欺詐其他的用戶。

因此我們決定以臉書為目標，開發一款能即時辨識臉書假帳號的系統，讓大家能在社交網路上更快的辨識正確訊息，並透過臉書檢舉功能使該假帳號停權，以避免更多人受到假帳號的威脅。

二、系統發展目的

在現在的社群網站上只有少數有提供辨識假帳號的功能，大部分都以檢舉機制為主，比如PTT就有能夠免費查詢特定帳號資料的網站——「發現 PTT Uncovered」，使用者可以直接在網頁填入帳號，就能查詢發回文記錄還有 IP 位址，甚至是同 IP 關聯帳號都能一目了然，就可以知道針對某些政治議題或是特定產品，是否有網軍或公關在批踢踢試圖帶風向情況，算是相當完善又直覺的帳號分析平台。

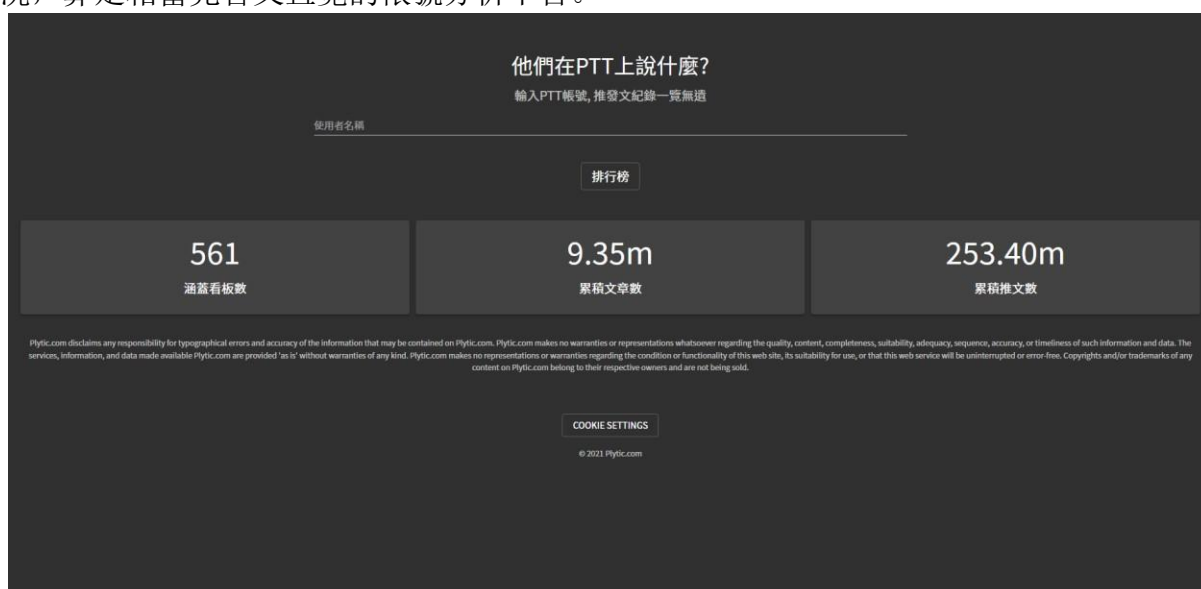


圖1-3 【發現 PTT Uncovered。取自:<https://www.plytic.com/>】

隨著網路的蓬勃發展，社交平台的假帳號、假消息也成為大家注重的議題，不少學者都做過類似的研究，不過大多是以文字去做分析而得的結果。Adikari and Dutta (2014)也透過國外著名社交平台 LinkedIn 建立異常帳號分類器，將帳號公開資訊爬蟲取得後，首先透過主成分分析進行降維，並找出其中有意義的特徵，最後使用神經網路(Neural Network)與支援向量機(Support Vector Machine, SVM)訓練辨識模型，實驗結果顯示不論透過何種方法，正確率都高於 80%。

由此結果可以顯示，深度學習方法擁有一定的能力去區分真假帳號，然而除了Adikari and Dutta (2014)有使用多種資料進行分析，其他的多以文字分析為主，臉書的資料除了文字，圖片也是很重要的一環，假帳號也常以盜圖或是發布大量廣告文來博取一般大眾的信任，因此本研究的辨識系統，不只包含文字，圖片也是模型的重點之一。

雖然臉書的官方也有讓使用者可使用系統內建的檢舉功能，舉報虛假帳號。可是當官方還在檢驗的同時，此帳號卻能繼續在社交網路當中流竄。因此我們想開發一套即使辨識的系統來讓一般民眾能夠使用科技的方法快速得辨識假帳號，希望大家能更舒服得使用社交軟體，也能增加網路言論的可信度。

- Logo設計



圖1-4 LOGO設計圖。

以上為我們針對這次專題所設計的Logo，我們將這個系統命名為臉書實名制，英文名為Facebook Identifier，我們用圓形來代表一個臉書上的帳號，實心為真，空心為假，在社交軟體當中，真假帳號常常相伴出現，將實心的圓放在Logo左上方意味著真實帳號才是人們真的想要的，為了忠實此款APP的核心理念，配色使用與臉書原Logo一樣的藍白配色，方便使用者辨識。

三、系統範圍

我們將以Facebook(臉書)作為我們的辨識範圍，使用臉書的客群範圍較廣，從剛開始接觸網路社會的10歲到60歲當中有多數的人都有註冊臉書帳號，雖然近期有不少其他的社交軟體出現，但臉書的使用率還是維持在一定水平。

■ 以下為市上台灣在2019年~2021年1月對Facebook使用人口統計、普查所做調查：



圖1-5 因為近期出現許多新興社群軟體，導致FB與IG的使用人數，都有些許的減少。【臺灣FB、IG人口普查（2020年1月）。取自：<https://tech.azuremedia.net/2020/01/30/8042/>】

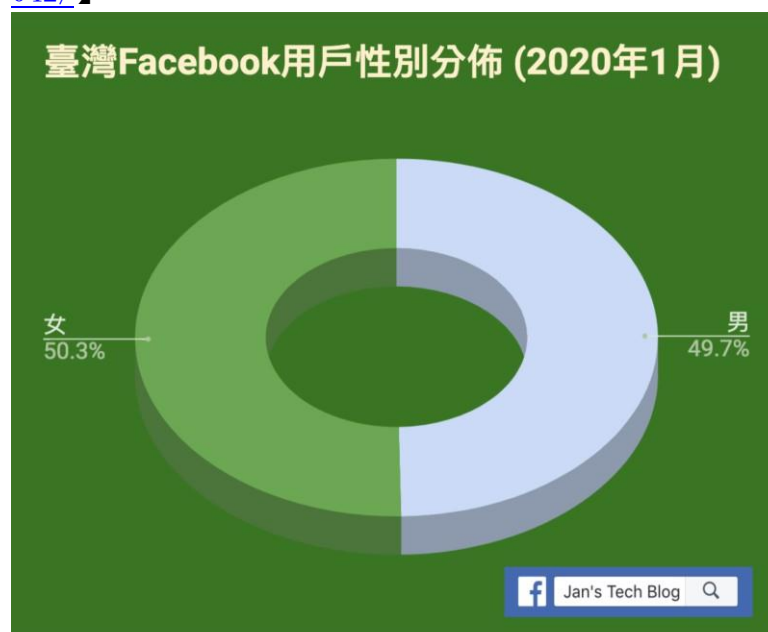


圖1-6 整體人口分布，男女比例是差不多的，890萬vs 900萬。【臺灣FB、IG人口普查（2020年1月）。取自：<https://tech.azuremedia.net/2020/01/30/8042/>】

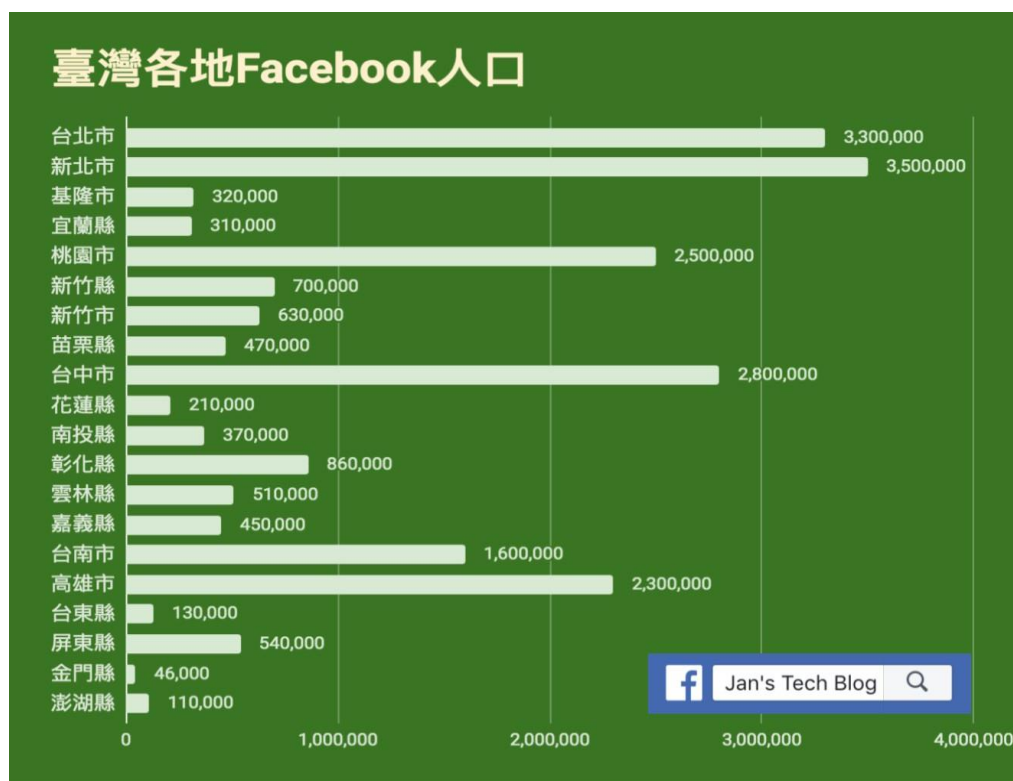


圖1-7 FB使用者在台灣地理區分布如圖所示，以台灣六都:台北市、新北市、桃園市、台中市、台南市、和高雄市所佔使用人口最多。這是根據Facebook廣告管理員的數據統計而來。【臺灣FB、IG人口普查（2020年1月）。取自:<https://tech.azuremedia.net/2020/01/30/8042/>】

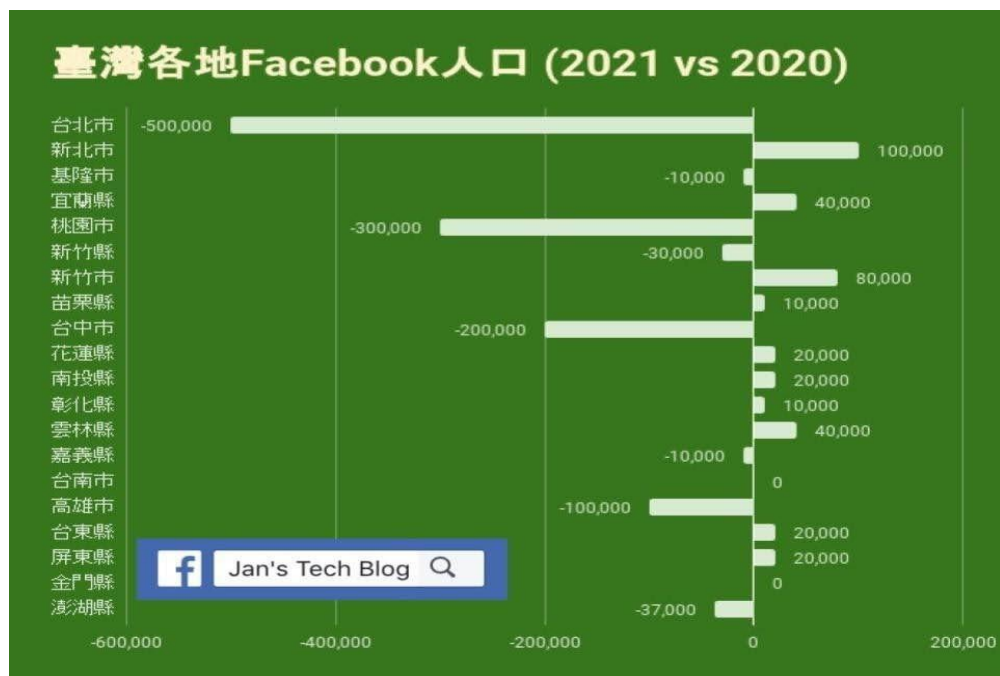


圖1-8 圖為台灣FB使用者在2020年與2021年人口數的差異，其中台北一口氣跌了50萬，桃園、台中和高雄也有減少的現象，六個直轄市裡，只有新北市上升了10萬戶，此現象非常有趣。【臺灣FB、IG人口普查（2021年1月）。取自:<https://tech.azuremedia.net/2021/02/15/8460/>】

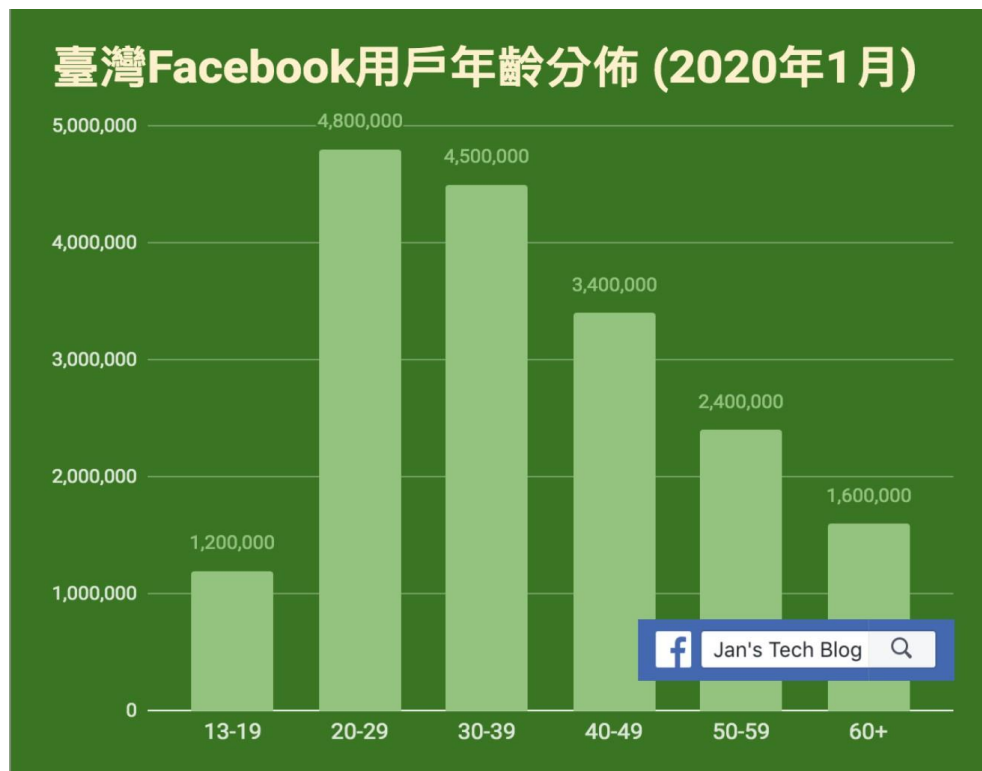


圖1-9 【臺灣FB、IG人口普查 (2020年1月)】。取自:<https://tech.azuremedia.net/2020/01/30/8042/>】

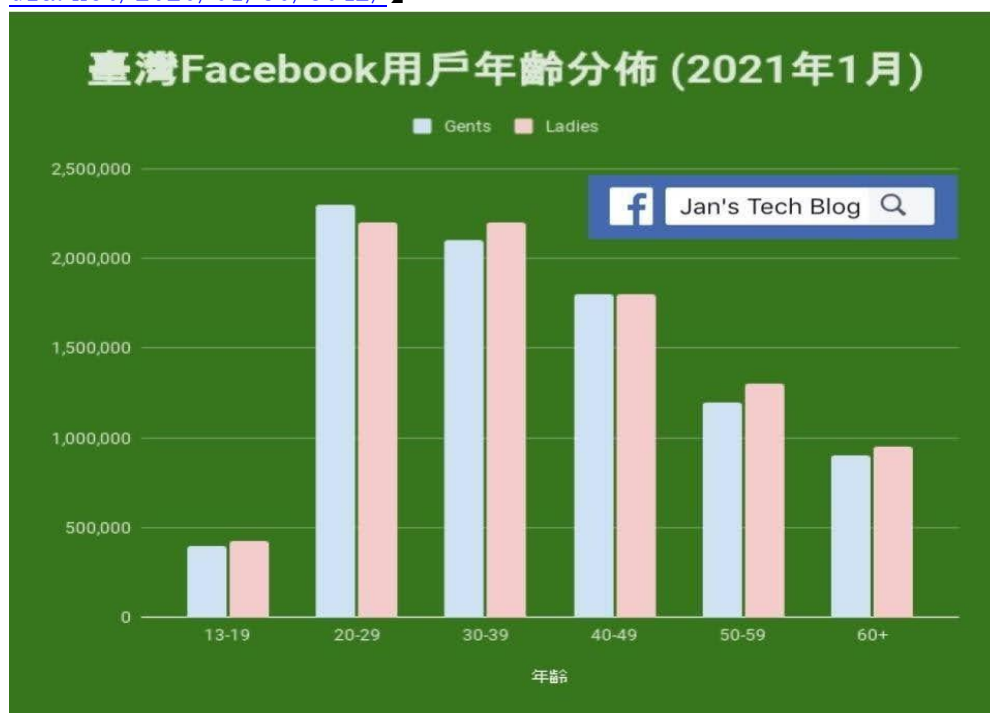


圖1-10 【臺灣FB、IG人口普查 (2021年1月)】。取自:<https://tech.azuremedia.net/2021/02/15/8460/>】

- 對比一下2020年與2021年的用戶年齡分布，我們可以發現：
 - 20-29和30-39這兩個區間用戶數最多。
 - 在13-19歲以及20-29歲的用戶數都有減少。
 - 50歲以上的用戶數卻增加，說明臉書用戶族群逐漸高齡化現象。
- 透過真假帳號的資料集，我們利用網路爬蟲蒐集該使用者在臉書上的各式活動軌跡，並將這些資料作為機器學習的input，讓系統能自動模擬判斷真假帳號。

● 系統流程設計



圖1-11 系統流程圖。

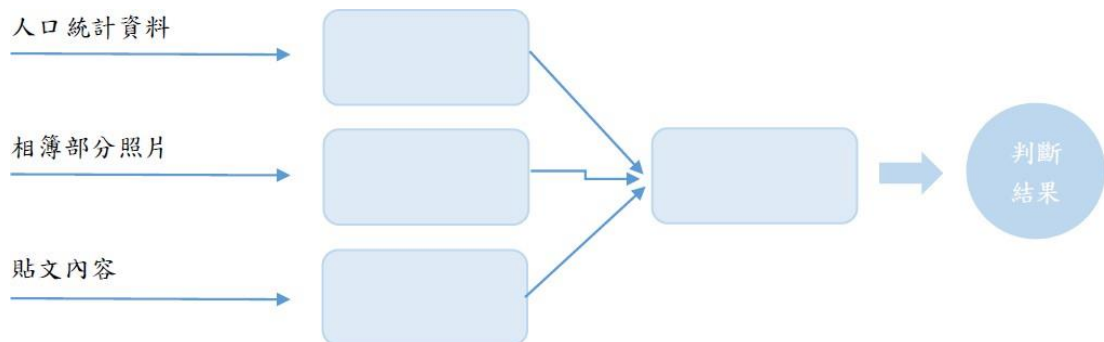


圖1-12 系統架構流程圖。

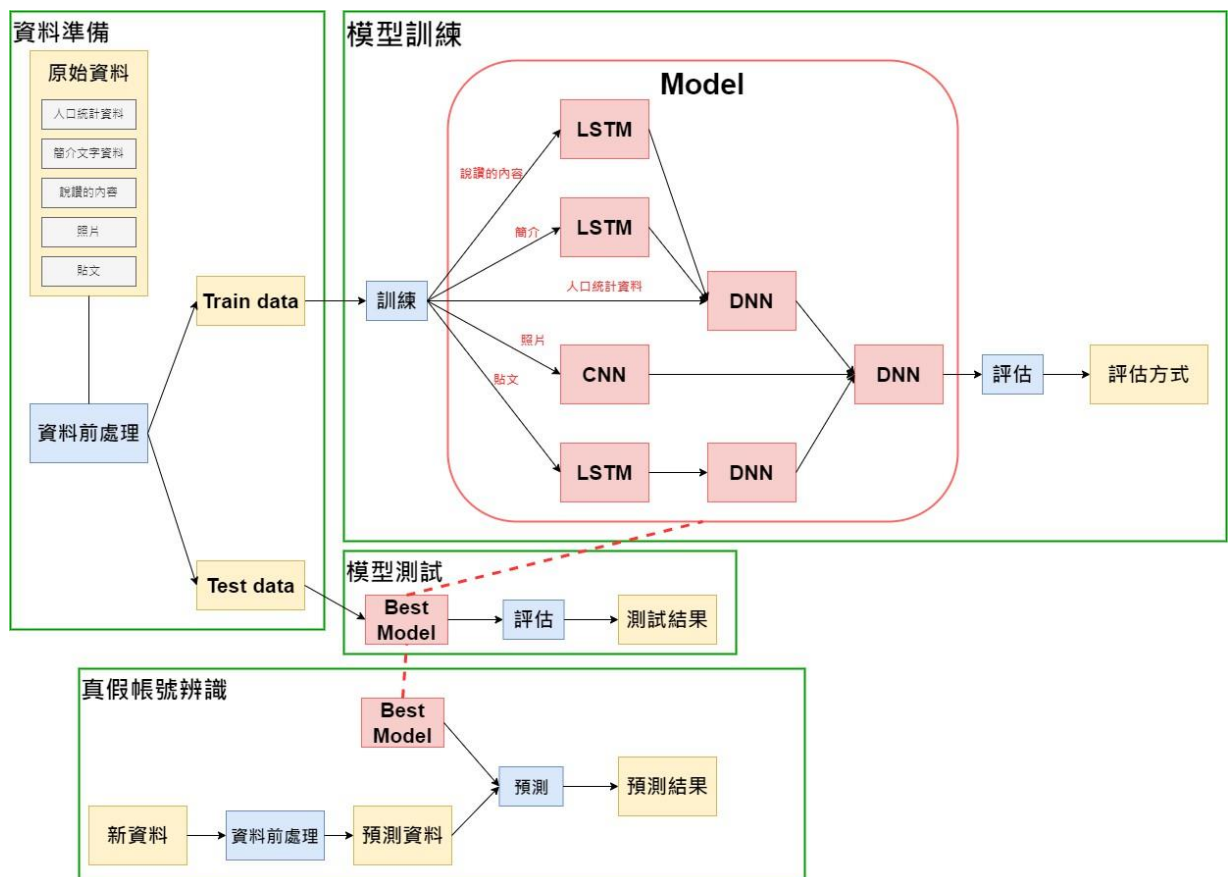


圖1-13 辨識模型架構。

● 系統研究步驟

1. 資料準備

由於臉書官方並未釋出之前受使用者檢舉成功的假帳號資料，因此本研究之資料集僅能以模擬展示。由於無相關論文探討何為臉書假帳號擁有之條件，在擁有 2.3 萬粉絲的臉書社團「臉書詐騙去死團」，吳嘉增(2021)在社團發布了一篇判別假帳號的參考標準，截至 2022 年 2 月 14 日得到 82 個按讚數、38 則留言數、65 次的分享，有許多網友留言表示認同，除此之外，該作者也會不定時更新內文，使其更有參考意義。參考以上該篇文章後，對比真實使用情況，本研究認為其準確性頗高，因此當帳號符合以下多個判斷標準時，本研究將會視為假帳號。本研究就所蒐集到之帳號，將根據以下幾點來決定是否為假帳號。

1-1. 圖片內容

- 只有一張個人圖片：
無論該使用者的個性、人脈等等，只要是真實帳號，除了基本的大頭貼及封面圖片外，有極大的機會被標註進他人的圖文當中，一旦有被標註過的紀錄，該貼文之照片也會同步顯示在自己的主頁，因此正常使用的帳號有極少的機率僅有一張個人圖片。
- 頭貼與年齡不符或頭貼性別與實際性別不符：
該行有較高的機會為盜圖之情況。

1-2. 用戶個人訊息

- 新帳號：
除了年紀較小的用戶以外，新註冊的帳號通常為假帳號。
- 簡介：
假帳號用戶並不會花多餘的時間填寫個人簡介。
- 居住地：
居住地若於國外，有較高的可能為假帳號。

1-3. 好友互動

- 好友組成：
當好友名單大多數皆為同性別或外國人時，有較高的可能為假帳號。
- 加入社團：
假帳號用戶通常會加入大量的免費打廣告、網路直播、直銷等等的社團，以便宣傳此假帳號的創建目的，例如：浮誇新產品功效、增加新產品的好評等等。
- 標記好友：
假帳號用戶通常會發布大量的衣服、鞋子、精品等等的商品貼文，或轉發相關內容，並標記大量的好友以增加曝光度。
- 貼文：
貼文發布時間集中，且缺少好友互動。

以人工決定是否為真假帳號時，並非符合上述一條件即認定為假帳號，須採綜合性判斷。

2. 網路爬蟲與量化資料

透過 Selenium 自動化爬取臉書網頁內容，開啟瀏覽器後，先登入一個為此系統創辦的空帳號，再連結進使用者想搜尋的使用者頁面，爬取其帳號首頁資料(如圖1-14所示)。由於直接從網頁上爬取下來的值不一定適合深度學習使用，所以有些值必須經過適當地預處理方能進行機器學習，表 1-1即描述本研究爬取資料後所獲得的資料型態和量化方式。

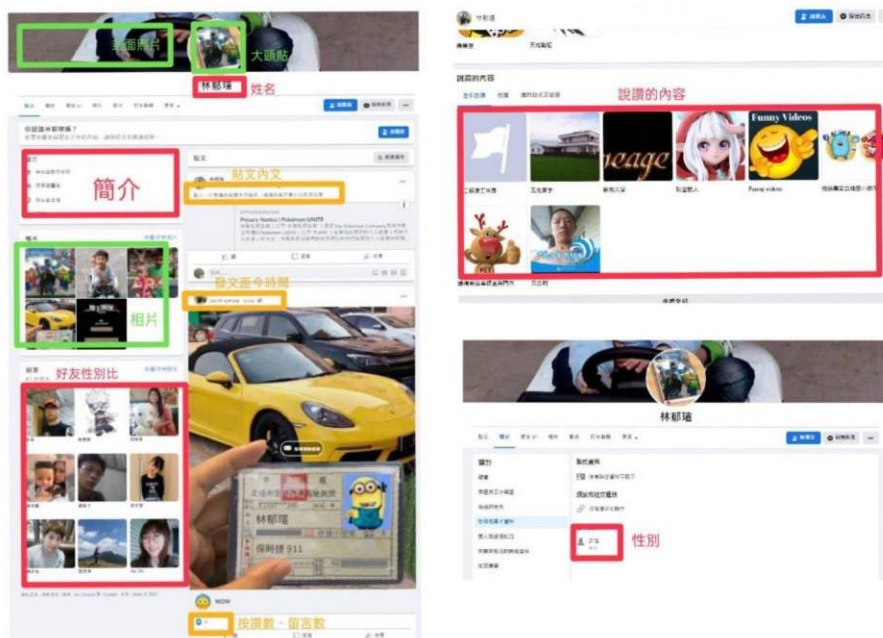


圖1-14 資料爬取的實際位置(紅框代表人口統計資料，綠框代表圖片，黃框代表貼圖內容。)

表1-1為資料型態與量化說明

項目類別	內容類別	資料型態	說明
人口統計資料	簡介	文字	使用Word2vec轉換為詞向量。
	性別	文字	男性編碼1，女性編碼-1，空值為0。
	好友性別比 (男/女)	數值	男女數量相除得到結果。
	說讚的內容	文字	使用Word2vec轉換為詞向量。
發文內容	內文	文字	使用Word2vec轉換為詞向量。
	發文距今 相差時間	數值	貼文發布時間與爬取資料當天相減，單位為天數。
	按讚數	數值	爬取貼文的按讚數。
	留言數	數值	爬取貼文的留言數。
照片	相片	圖檔	爬取個人檔案之11張照片，合併為大小48*64 px的圖檔。

- **模型訓練與測試**

如圖 1-13所示，本模型的大架構為透過人口統計資料、圖片資料、貼文資料，三個面向來分析此帳號是否為假帳號。在人口統計資料中，說讚的內容、簡介這兩個項目由於有多筆資料，且為文字資料，因此階段一將先個別進行 LSTM，將結果併入其他人口統計資料，最後階段二會進行這個類別的DNN。圖片資料中，階段一每一張圖片將進行一次 CNN，將每次整流線性單位函式(Rectified Linear Unit, ReLU)輸出的結果合併，最後於階段二進行 DNN。貼文資料中，階段一每一篇的內文將進行一次LSTM，將 ReLU 輸出的結果與該貼文之發文距今時間、留言數、按讚數合併，視為一筆資料，最後於階段二進行 DNN。三個面向的 DNN 都透過 ReLU 輸出後，最後統整於階段三再進行一次 DNN，透過 Sigmoid 函式輸出得到它為真假帳號的機率。

階段一與階段二的激活函式(Activation Function)均採用 ReLU，此種激活函式是仿照生物學所設計的，且計算速度快，因此使用上可以達到比較好的結果(Glorot et al., 2011)；而階段三除隱藏層採用 ReLU 外，輸出層的激活函式採用 Sigmoid，由於 Sigmoid的輸出值會介於 0~1 之間，因此適合用於二元分類當中(Krohn et al., 2019)。

模型訓練採用交叉熵(Cross Entropy)作為損失函式(Loss Function)，並以 AUC (Area under the ROC Curve)驗證模型之成效。為方便評估模型，本研究將使用混淆矩陣(Confusion Matrix)著重計算精確度(Precision)，因為不希望將假帳號視為真帳號。

- **系統內容**

1. **即時辨識**

透過AI深度學習及網路爬蟲，當使用者輸入臉書個人網頁之連結，系統將會即時回應是否為假帳號，提供使用者即時資訊。

2. **刊登廣告**

在使用功能前，會播放幾秒的廣告，有興趣之廣告主能跟我們購買定時廣告版面，投資我們繼續完善此系統。

3. **使用者回報**

當辨識結果出現嚴重錯誤，使用者能即時回報給我們，方便我們進行系統修繕，並持續增進我們的系統功能。

第二章 軟體需求規格

一、使用者角色說明

角色	說明
臉書使用者	希望可以判別其他用戶是否為假帳號。
開發者	改善和優化系統，排除系統問題

二、使用者故事對應

User Activity	User Task	User Story	優先順序
1 發現可疑帳號	1.1 想確認帳號真偽	1.1.1 發現疑似假用戶之帳號	1
		1.1.2 取得個人網頁網址	2
2 識別假帳號	2.1 辨識假帳號	2.1.1 查看隱私條款	1
		2.1.2 輸入個人網頁網址	2
		2.1.3 取得查詢結果	3
3 確認查詢結果	3.1 分享查詢結果	3.1.1 分享至臉書	1
		3.1.2 分享至LINE	2
		3.1.3 分享至Twitter	3

三、使用者故事卡

名稱	1 發現可疑帳號	類別	User Activity
角色：身為臉書使用者 需求：想確認某使用者是否為假帳號 價值：發現臉書可疑假帳號 接受條件： Given 使用者在使用臉書 Then 使用者想要確認其帳號真偽(1. 1)			

名稱	1. 1 想確認帳號真偽	類別	User Task
角色：身為臉書使用者 需求：可以查詢臉書使用者帳號的真偽 價值：我要檢驗帳號是否為假帳號 接受條件： Given 使用者在使用臉書 When 使用者發現疑似假用戶之帳號(1. 1. 1) Then 使用者取得個人網頁網址(1. 1. 2)			

名稱	1. 1. 1 發現疑似假用戶之帳號	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：可以發現假帳號</p> <p>價值：可以發現可疑的用戶帳號</p> <p>接受條件：</p> <p>Given 使用者已有臉書帳號</p> <p>When 使用者使用臉書</p> <p>Then 使用者可以發現疑似假用戶之帳號(1. 1. 1)</p>			
優先順序	1		

名稱	1. 1. 2 取得個人網頁網址	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：可以取得個人網頁的網址</p> <p>價值：可以找到疑似假帳號的個人網頁</p> <p>接受條件：</p> <p>Given 使用者使用臉書</p> <p>When 使用者發現疑似假用戶的帳號(1. 1. 1)</p> <p>Then 使用者可以取得其個人網頁的網址(1. 1. 2)</p>			
優先順序	2		

名稱	2 識別假帳號	類別	User Activity
<p>角色：身為臉書使用者</p> <p>需求：可以查詢臉書使用者帳號的真偽</p> <p>價值：我要知道檢驗帳號是否為假帳號</p> <p>接受條件：</p> <p>Given 使用者已確定想檢驗之帳號</p> <p>When 使用者輸入個人網頁網址 (2. 1. 2)</p> <p>Then 使用者能查看查詢結果 (2. 1. 3)</p>			

名稱	2. 1. 1 查看隱私條款	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：可以查看本系統之隱私條款</p> <p>價值：可以了解本系統之隱私條款</p> <p>接受條件：</p> <p>Given 使用者已確定想檢驗之帳號</p> <p>When 使用者點擊隱私條款之超連結 (2. 1. 1)</p> <p>Then 使用者查看本系統之詳細隱私條款，決定是否要繼續使用此系統</p>			
優先順序	1		

名稱	2.1.2 輸入個人網頁網址	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：可以輸入可疑帳號之網頁網址</p> <p>價值：我要查詢該帳號是否為假帳號</p> <p>接受條件：</p> <p>Given 使用者使用臉書</p> <p>AND 使用者發現疑似假用戶之帳號(1.1.1)</p> <p>AND 使用者取得個人網頁網址(1.1.2)</p> <p>When 使用者輸入個人網頁的網址(2.1.2)</p> <p>Then 使用者可以查詢其真偽(2.1.3)</p>			
優先順序	2		

名稱	2.1.3 取得查詢結果	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：可以得到該帳號的真偽資訊</p> <p>價值：我要查詢該帳號是否為假帳號</p> <p>接受條件：</p> <p>Given 使用者使用臉書</p> <p>When 使用者發現疑似假用戶之帳號(1.1.1)</p> <p>AND 使用者輸入個人網頁網址(2.1.2)</p> <p>Then 使用者可以取得查詢結果(2.1.3)</p>			
優先順序	3		

名稱	3 確認查詢結果	類別	User Activity
<p>角色：身為臉書使用者</p> <p>需求：可以確認查詢臉書使用者帳號的真偽</p> <p>價值：我要知道檢驗帳號是否為假帳號</p> <p>接受條件：</p> <p>Scenario 1：使用者想分享查詢結果</p> <p>Given 使用者已取得查詢結果(2.1.3)</p> <p>When 使用者分享查詢結果(3.1)</p> <p>Then 使用者可以回報相關意見(3.2)</p> <p>Scenario 2：使用者不想分享查詢結果</p> <p>Given 使用者已取得查詢結果(2.1.3)</p> <p>When 使用者已知查詢結果</p> <p>Then 使用者可以回報相關意見(3.2)</p>			

名稱	3.1 分享查詢結果	類別	User Task
<p>角色：身為臉書使用者</p> <p>需求：我可以分享查詢結果</p> <p>價值：我要將已知的查詢結果分享到其他媒體</p> <p>接受條件：</p> <p>Given 使用者已取得查詢結果(2.1.3)</p> <p>When 使用者已知查詢結果</p> <p>Then 使用者可以分享查詢結果(3.1)</p>			

名稱	3.1.1 分享至臉書	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：我可以將查詢結果分享至臉書</p> <p>價值：我要將已知的查詢結果分享到臉書</p> <p>接受條件：</p> <p>Given 使用者已取得查詢結果 (2.1.3)</p> <p>When 使用者想分享查詢結果 (3.1)</p> <p>Then 使用者可以選擇分享至臉書 (3.1.1)</p>			
優先順序	1		

名稱	3.1.2 分享至LINE	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：我可以將查詢結果分享至LINE</p> <p>價值：我要將已知的查詢結果分享到LINE</p> <p>接受條件：</p> <p>Given 使用者已取得查詢結果 (2.1.3)</p> <p>When 使用者想分享查詢結果 (3.1)</p> <p>Then Then 使用者可以選擇分享至LINE (3.1.2)</p>			
優先順序	2		

名稱	3.1.3 複製連結	類別	User Story
<p>角色：身為臉書使用者</p> <p>需求：我可以將查詢結果的連結複製並分享至Twitter</p> <p>價值：我要將已知的查詢結果分享到Twitter</p> <p>接受條件：</p> <p>Given 使用者已取得查詢結果(2.1.3)</p> <p>When 使用者想分享查詢結果(3.1)</p> <p>Then 使用者可以選擇分享至Twitter(3.1.3)</p>			
優先順序	3		

第三章 軟體設計功能

一、介面設計

1. 介面藍圖一覽表

編號	名稱	對應使用者故事
1	辨識假帳號	
1.1	查看隱私權條款	2.1.1 查看隱私權條款
1.2	查詢結果	2.1.2 取得查詢結果

2. 介面藍圖畫面

1 辨識假帳號

說明

開啟網頁連結，即進入網站首頁。
進入首頁後，點擊隱私條款的文字可以查看隱私權條款(1.1)。

2.1 查看隱私權條款



隱私條款

非常歡迎您光臨「臉書實名制 Facebook Identifier」(以下簡稱本網站)，為了讓您能夠安心的使用本網站的各項服務與資訊，特此向您說明本網站的隱私權保護政策，以保障您的權益，請您詳閱下列內容：

一、隱私權保護政策的適用範圍

隱私權保護政策內容，包括本網站如何處理在您使用網站服務時收集到的個人識別資料。隱私權保護政策不適用於本網站以外的相關連結網站，也不適用於非本網站所委託或參與管理的人員。

二、個人資料的蒐集、處理及利用方式

* 當您造訪本網站或使用本網站所提供之功能服務時，我們將視該服務功能性質，請您提供必要的個人資料，並在該特定目的範圍內處理及利用您的個人資料；非經您書面同意，本網站不會將個人資料用於其他用途。

* 本網站在您使用服務信箱、問卷調查等互動性功能時，會保留您所提供的姓名、電子郵件地址、聯絡方式及使用時間等。

* 於一般瀏覽時，伺服器會自行記錄相關行徑，包括您使用連線設備的IP位址、使用時間、使用的瀏覽器、瀏覽及點選資料記錄等，做為我們增進網站服務的參考依據，此記錄為內部應用，決不對外公佈。

* 為提供精確的服務，我們會將收集的問卷調查內容進行統計與分析，分析結果之統計數據或說明文字呈

說明

點選上方圖示可返回辨識假帳號(2)的搜尋頁面。

2.3 查詢結果



說明

從辨識假帳號(2)的搜尋頁面，可輸入網址進行搜尋。

點選搜尋後將會載入查詢結果(2.2)。

查詢結果頁面會顯示基本個人資料以及經辨識後的回傳的帳號真實度。

可選擇分享查詢結果。若選擇再測一次，則畫面會跳轉回辨識假帳號(2)的搜尋頁面。

二、資源需求

表3-1為開發系統所需要的人力、軟體、硬體及對應的經費評估。

資源項目	資源名稱	需要金額	說明
硬體需求	Window 伺服器 規格：i9-10900HQ NVIDIA Geforce RTX 2080Ti 64位元作業系統 x64型處理器 RAM 128GB	0	開發期間所需硬體設備
	使用開發者已有之電腦	0	開發期間所需硬體設備
軟體需求	資料庫：MySQL	0	開發所使用的資料庫語言
	網頁伺服器:Linux server	0	開發期間所使用的網頁伺服器
	開發環境： Visual Studio Code	0	開發時使用的開發環境
	開發語言：Python、HTML、Javascript	0	主要使用的程式語言
人力需求	開發人力：5人		組員全體

表3-2為營運系統所需要的人力、軟體、硬體及對應的經費評估。

資源項目	資源名稱	需要金額	說明
硬體需求	Window 伺服器 規格：i9-10900HQ NVIDIA Geforce RTX 2080Ti 64位元作業系統 x64型處理器 RAM 128GB	0	營運期間需要的硬體設備
軟體需求	資料庫：MySQL	0	營運時所使用的資料庫語言
	網頁伺服器:Linux server	0	營運期間所使用的網頁伺服器
	開發環境： Visual Studio Code	0	營運時使用的開發環境
	開發語言：Python、HTML、Javascript	0	主要使用的程式語言
人力需求	開發人力：5人	0	組員全體

附錄

一、文件分工及貢獻度說明

列出文件章節並標示參與者之實際工時，貢獻度請以百分比展現。

	組長	組員	組員	組員	組員
	吳柏緯	黃品綺	盛慧欣	吳承翰	張哲維
第一章 系統描述					
一、發展背景與動機		0.4	3		0.1
二、系統發展目的	2	0.9	3.7		0.1
三、系統範圍		0.4	3.1	2	
四、背景知識		0.4	3.2	13	
五、系統限制		0.4	0.5		0.1
第二章 軟體需求規格					
一、功能需求		1.7	4		1.5
第三章 軟體設計功能					
一、資料庫設計		2.5			
二、介面設計	2.25		4.2	0.5	
三、資源需求			1		1.0
第四章 專題實作討論					
一、發展遇到的問題和解決方法					0.5
二、SWOT					0.2
三、發展心得					0.5
四、未來展望					0.5
五、模型訓練結果				5	
附錄:參考資料					2
總工時	4.25	6.7	22.7	22.5	6.5
整體貢獻度	10	25	30	25	10

二、程式分工及貢獻度說明

列出系統程式分工項目並標示參與者之實際工時，貢獻度請以百分比展現。

	組長	組員	組員	組員	組員
	吳柏緯	黃品綺	盛慧欣	吳承翰	張哲維
資料集	1	2	4.2	6	5
爬蟲	24	40	2		15
網頁前端	2		7		
網頁後端	2		25		
模型訓練	5	15		43	
總工時	34	57	38.2	49	20
整體貢獻度	30	25	10	30	5

三、參考資料

1. 買讚的網頁參考(<https://smilegood.cyberbiz.co/>)、(<https://www.ruten.com.tw/item/show?21935651715836>)
2. 發現 PTT Uncovered(<https://www.plytic.com/>)。
3. 臺灣FB、IG人口普查 (2020年1月) (<https://tech.azuremedia.net/2020/01/30/8042/>)。
4. 臺灣FB、IG人口統計 (2020年1月) (<https://tech.azuremedia.net/2021/02/15/8460/>)。
5. Sandy(無日期)。別讓那些人騙走你的財富-揭穿FB假帳號的秘訣(Part 1)。民110年1月26日, 取自:<https://fin.masscloudbiz.com/fake-facebook-accounts/>。
6. GIGABYTE(June 24, 2019)。深度學習這檔事絕對不是運算效能夠大就能搞定。民110年11月26日, 取自:<https://www.gigabyte.com/tw/Article/why-do-you-need-deep-learning-part-i>。
7. 刘建平(無日期)。博客园的学习笔记。民110年11月26日, 取自:<https://info.todoealth.com/37263704>。
8. 王柏鈞(FEB 14, 2020)。DNN(深度神經網路)的全面認識。民110年11月26日, 取自:<https://medium.com/%E6%A9%9F%E5%99%A8%E5%AD%B8%E7%BF%92%E7%9F%A5%E8%AD%98%E6%AD%B7%E7%A8%8B/dnn-%E6%B7%B1%E5%BA%A6%E7%A5%9E%E7%B6%93%E7%B6%B2%E8%B7%AF-%E7%9A%84%E5%85%A8%E9%9D%A2%E8%AA%8D%E8%AD%98-ad50aa531205>。
9. 水面上的小草(FEB 11, 2019)。深度學習激勵函數介紹。民110年11月26日, 取自:<https://cvfiasd.pixnet.net/blog/post/275774124-%E6%B7%B1%E5%BA%A6%E5%AD%B8%E7%BF%92%E6%BF%80%E5%8B%B5%E5%87%BD%E6%95%B8%E4%BB%8B%E7%B4%B9>。
10. Sukanya Bag(FEB 24, 2021)。深度学习领域最常用的10个激活函数, 一文详解数学原理及优缺点。民110年11月26日, 取自:<https://www.jiqizhixin.com/articles/2021-02-24-7>。
11. 機器之心(MAR 30, 2017)。深度神经网络概述: 从基本概念到实际模型和硬件基础。民110年11月26日, 取自:<https://zhuanlan.zhihu.com/p/26091067>。
12. 周秉誼(SEP 20, 2016)。淺談Deep Learning原理及應用。民110年11月26日, 取自:https://www.cc.ntu.edu.tw/chinese/epaper/0038/20160920_3805.html。
13. Cinnamon AI Taiwan(Jun 5, 2019)。深度學習: CNN原理。民110年11月26日, 取自:<https://cinnamonaitaiwan.medium.com/%E6%B7%B1%E5%BA%A6%E5%AD%B8%E7%BF%92-cnn%E5%8E%9F%E7%90%86-keras%E5%AF%A6%E7%8F%BE-432fd9ea4935>。
14. Brandon(AUG 18, 2016)。卷積神經網路的運作原理。民110年11月26日, 取自:<https://brohrer.mcknote.com/zh-Hant/how-machine-learning-works/how-convolutional-neural-networks-work.html>。
15. 曾厚強, 陳柏琳, &宋曜廷(2018)。The 2018 Conference on Computational Linguistics and Speech Processing ROCLING 2018, pp.116-125. <https://aclanthology.org/O18-1012.pdf>。
16. 周秉誼(SEP 20, 2016)。淺談Deep Learning原理及應用。民110年11月26日, 取自:https://www.cc.ntu.edu.tw/chinese/epaper/0038/20160920_3805.html。
17. 陈诚(JAN 2, 2018)。人人都能看懂的LSTM。民110年11月26日, 取自:<https://zhuanlan.zhihu.com/p/32085405>。
18. 打不死的小強(JAN 3, 2019)。長短期記憶網路 - Long short-term memory | LSTM。民國110年11月27日, 取自:<https://easyai.tech/ai-definition/lstm/>。

19. 靜悟生慧 (NOV 11, 2020)。RNN、LSTM、GRU。民國110年11月27日，取自：<https://www.cnblogs.com/Allen-rg/p/13957848.html>。
20. 機器學習\統計方法：模型評估－驗證指標(validation index)。民國110年12月11日，取自：<https://chih-sheng-huang821.medium.com/%E6%A9%9F%E5%99%A8%E5%AD%B8%E7%BF%92-%E7%B5%B1%E8%A8%88%E6%96%B9%E6%B3%95-%E6%A8%A1%E5%9E%8B%E8%A9%95%E4%BC%B0-%E9%A9%97%E8%AD%89%E6%8C%87%E6%A8%99-b03825ff0814>。
21. 吳嘉增 (2021)。如何分辨臉書假帳號。取自 <https://www.facebook.com/groups/891552070994790/posts/1871761532973834/>。
22. Glorot, X., Bordes, A., and Bengio, Y. (2011). Deep sparse rectifier neural networks. *Proceedings of Machine Learning Research*, 15, 315-323.
23. Krohn, J., Beyleveld, G., and Bassens, A. (2019). *Deep Learning Illustrated: A Visual*,
24. *Interactive Guide to Artificial Intelligence*. Addison Wesley, USA.
25. Adikari, S. and Dutta, K. (2014). Identifying fake profiles in LinkedIn. *Pacific Asia Conference on Information Systems (PACIS)*.