淡江大學資訊管理學系碩士班

碩士論文

指導教授：張昭憲 博士

以模型融合為基礎之線上拍賣詐騙偵測

Online Auction Fraud Detection based on Model Fusion

研究生：陳世軒 撰

中華民國 108 年 1 月

論文名稱：以模型融合為基礎之線上拍賣詐騙偵測　　頁數：40

校系所組別：淡江大學資訊管理學系碩士班

畢業時間及提要別：107 學年度第 1 學期碩士學位論文提要

研究生：陳世軒　　指導教授：張昭憲博士

論文提要內容：

隨著金流與物流等基礎建設的成熟，電子商務的蓬勃發展有目共睹，不但已成為現代人生活一部分，交易金額也年年攀高。在 2017 年，全球電子商務總銷售額已高達 2.29 兆美元，其興盛程度可見一斑。但面對如此龐大的交易金額，也引起不肖人士的覬覦，在電子商務平台中進行詐騙，而線上拍賣詐騙更佔其中的大宗。有關線上拍賣詐騙偵測，已有許多方法被提出，但對於日新月異的詐騙手法，其準確率仍有待提升。為解決此問題，本研究將配合模型融合概念，發展有效的詐騙偵測方法。首先，我們以線性迴歸組合數種傳統的分類模型，以產生更有效的融合模型，並比較傳統單一分類模型與融合模型之間的差異。之後，以不同訓練資料配比，將產生各種不同特性之模型，以多階連續過濾以及平衡過濾方式加以整合，以提升詐騙偵測的準確性。此外，由於偵測屬性集與偵測效能息息相關，本研究也探討屬性篩選對於偵測準確率之影響。為驗證提出方法之有效性，本研究採用 Yahoo!奇摩實際交易資料進行實驗。與四種單一偵測模型相比較，結果顯示融合模型確實能提高偵測準確率。當使用連續過濾與平衡過濾流程時，除能獲得高準確率外，也能分段獲得較高之偵測精度。此外，結果亦顯示，使用 Principle Component Analysis 或 Wrapper 法進行屬性篩選，並無助於結果的改善。由上述結果可知，本研究提出方法確有助於改善詐騙偵測準確率，提供消費者更周全的購物安全防護機制。

關鍵字：詐騙偵測(Fraud Detection)、模型融合(Model Fusion)、分類(Classification)、線上拍賣(Online Auctions)、電子商務(e-Commerce)

表單編號：ATRX-Q03-001-FM030-03

Title of Thesis: Online Auction Fraud Detection based on Model Fusion **Total pages:** 40

Key Words: Fraud Detection, Model Fusion, Classification, Online Auctions, e-Commerce.

Name of Institute: MASTER PROGRAM, DEPARTMENT OF INFORMATION MANAGEMENT

Graduate date: January, 2019 **Degree conferred:** Master

Name of Student: Shih-Hsuan Chen **Advisor:** Jau-Shien Chang PhD

陳世軒 張昭憲 博士

Abstract:

With the maturity of infrastructure such as cash flow and logistics, the booming development of e-commerce is obvious to all. Not only has it become a part of modern life, but the transaction amount has also increased year by year. In 2017, global e-commerce total sales have reached 2.29 trillion US dollars, and its prosperity can be seen. However, in the face of such a large transaction amount, it also attracts a lot of fraudsters to join the e-commerce platform. Among the reported cases, online auction fraud undoubtedly forms a large proportion. There have been many methods for online auction fraud detection, but the accuracy of the ever-changing fraud scheme still needs to be improved. In order to solve this problem, this study adopts the model fusion concept to develop effective fraud detection methods to improve the accuracy of detection. First, we combine several traditional classification models with linear regression to produce a more efficient fusion model and compare the differences between the traditional single classification model and the fusion model. After that, training sets with different fraud/non-fraud ratio are used to build detection models of different characteristics. Based on these models, a multi-level continuous filtering and a balanced filtering method are developed to integrate these models and improve the accuracy of fraud detection. In addition, since the detection attribute set is closely related to the detection performance, this study also explores the impact of attribute screening on detection accuracy. In order to verify the validity of the proposed method, the study used Yahoo!Kimo actual transaction data for experiments. Compared with the four single detection models, the results show that the fusion model can improve the detection accuracy. When using continuous filtering and balanced filtering processes, in addition to high accuracy, segmentation can achieve higher detection accuracy. In addition, the results also show that feature selection does not contribute to the improvement of the results. From the above results, the proposed method does help to improve the accuracy of fraud detection and provide consumers with a more comprehensive shopping security protection mechanism.

目錄

表目錄

圖目錄

第一章 緒論

隨著網路與行動裝置的普及，配合金流與物流等基礎建設的成熟，造就電子商務的蓬勃發展。近年來，更由於年輕世代購物習慣的改變，讓電子商務的交易金額年年攀升。在 2014 年，美國全年的網路線上零售總金額已高達 2,940 億美元，同時期中國電子商務交易亦達 2,730 億美元。發展至今，全球電子商務銷售額在 2017 年成長至 2.29 兆美元，更預計在 2021 年達到 4.8 兆美元(eMarketer, 2017)，假以時日有可能超越實體銷售通路。以中國最大的電子商務集團阿里巴巴為例，交易量從 2005 年成立時的每日 10,000 筆，暴增至 2013 年時的每日超過 1 億筆，發展之快速可見一斑(Chen et al., 2015)。隨著線上消費行為的普及，全球電子商務呈現高速成長，進入真正數位經濟的時代。

面對如此龐大的交易金額，也引起不肖人士的覬覦，在電子商務平台中進行詐騙。常見的詐騙行為有收到貨款不出貨、進行假交易、商品敘述不實、販賣偽劣貨等 (NW3C, 2017; Tseng, et al., 2014; Gavish & Tucci, 2008)。但詐騙者亦可扮演買方，以進行付款詐欺、異常退款，甚至洗錢等不法行為(Chen et al., 2015)。為避免消費者懷疑，更有詐騙者以略低於市價販售商品，但巧妙隱藏商品規格細節(例如相機是否附原廠鏡頭)，售出後再以各種藉口規避退貨(Kim et al., 2013)。由於網路的隱蔽性與便利性，讓這些不法行為在短期內便快速成長，若不加以抑制，將嚴重影響線上拍賣未來發展。

為降低詐騙的發生，拍賣網站當局經常以簡單的二元名聲系統(binary reputation system)來協助評估使用者的信用。當買賣雙方交易完成時，可互相給予正評(+1)、普評(+0)、負評(-1)等三種評價，評價的給予可能受到貨時間、價格、售後服務等因素影響。此種評分機制雖然簡單，但累積的分數(名聲)卻足以影響

他人是否願意與你進行交易的意願。例如，有經驗的消費者往往會在購買商品前，花費大量的時間查閱賣家的信用評價，以避免不必要的交易糾紛(Goes et al.,2009)。然而，因二元名聲系統過於簡單，許多不肖份子開始找尋機制的漏洞，讓消費者難以分辨。例如，詐騙者會先建立多個新帳戶，並進行大量商品的買賣，以快速累積正評。待等取得消費者信任後，再開始進行詐騙。面對類似的取巧行為，拍賣網站管理當局只能藉由停權來達到嚇阻效果。然而，受害者仍須自行報案，藉由警方進行偵查，才有可能追回損失。期間可能花費大量的時間金錢，更讓許多求償的受害者心懷畏懼、裹足不前。凡此種種，均嚴重影響線上拍賣的長遠發展。

面對線上拍賣詐騙偵測，學界與業界莫不給予高度關注，並以積極方式來因應 (West & Bhattacharya, 2016)。Alford (2013)更認為現代企業都應發展智慧型詐騙偵測系統，檢視每日進行的所有交易，以維護電子商務之交易安全。為避免消費者受損失，學者也紛紛提出各種詐騙偵測方法。例如，Chau 等人(2006)利用價格異常做為偵測基礎，以分類樹方式建立偵測模型，藉以分辨詐騙者。Chang&Chang(2011, 2012)則提出詐騙預警概念，以階段切割法(phased-profiling)切割交易者生命週期，產生具有潛伏期詐騙者偵測能力之模型。Pandit 等人(2007)則提出二階段偵測概念，利用分類樹與 Markov Random Field 標示詐騙正犯與共犯，希望能找出詐騙者及其所屬共犯集團。Tsang 等人(2014)持續改進 Pandit 等人之方法，以 Markov 方法計算帳號詐騙機率，以更精確方式標示出詐騙共犯集團。除了學界外，業界對於詐騙偵測的投入也不遺餘力。例如，為有效遏止詐騙，阿里巴巴集團即發展了一套即時的詐騙防範與監控系統，監控的行為涵蓋不正常退款、多重帳號、盜取帳號，甚至洗錢等複雜的犯罪行為(Chen et al., 2015)。

線上拍賣詐騙偵測雖已獲得學界與業界的高度關注，亦有許多方法被提出，但仍面臨諸多挑戰(Ahmed et al., 2016; West & Bhattacharya, 2016)。其中，傳統分類技術(classification)雖然有效，但均具有效能瓶頸，需要進一步突破。為降低上述問題的影響，模型融合(Model Fusion)便成為可行的解決之道。各種詐騙偵測模型均有其特質，偵測效能也有所差異。模型融合(Model Fusion)是一種從多種模型中擷取有利於預測效能的流程。模型融合概念已應用在各種不同領域，例如，Li 等人(2012)同時使用貝式分類法與關聯規則探勘，歸納觀察詐騙者行為樣式，除自動偵測外，也能透過專家判讀提升準確率。Chen 等人(2013)則利用貝氏方法進行模型融合，提升網路媒體語意擷取的正確性。Huang 等人(2015)則透過加權平均法整合各模型之預測結果，並藉由機器學習調整模型權重，以產生更精確的商品推薦名單。面對電子商務詐騙，Chen 等人(2015)則利用 logistic regression 組合各種模型產生的可疑分數，以提升詐騙偵測效能，並發現決策樹與 Random Forest 能獲得較佳的偵測效能。根據上述文獻顯示，若能有效整合各種模型的特點，對於偵測的即時性與準確性將有很大助益。

根據上述討論，本研究將運用模型融合概念，發展有效的詐騙偵測方法，以提升偵測之準確性。首先，我們以線性迴歸組合數種傳統的分類模型，期能結合各種模型優點，以產生更有效的融合模型。其次，本研究利用不同訓練資料配比，產生各種不同特性之模型，再以多階連續過濾以及平衡過濾方式加以整合，以提升詐騙偵測的準確性。此外，由於偵測屬性集與偵測效能息息相關，論文中也探討屬性篩選對於偵測準確率之影響。為驗證提出方法之有效性，我們採用 Yahoo! 奇摩實際交易資料進行實驗。與四種單一偵測模型相比較，本研究提出之融合模型確能提高偵測準確率，並提供更穩定的偵測結果。此外，結果亦顯示使用 Principle Component Analysis 或 Wrapper 法進行屬性篩選，對準確率並無明顯改善。當使用連續過濾與平衡過濾流程時，除準確率優於單一模型外，更能獲得較高之分段偵測精度。由上述結果可知，本研究提出方法確有助於改善詐騙偵測準

確率，提供消費者更周全的購物安全防護機制。

本論文後續章節如下: 第二章介紹相關背景知識、術語及技術，第三章為本研究提出過濾式模型融合方法與偵測流程，第四章為實驗結果及討論，第五章為結論與未來工作。

第二章 知識背景與技術介紹

本章將探討相關知識背景、術語以及技術。

2.1 線上拍賣詐騙

線上拍賣帶來的經濟效益有目共睹，但也引起了許多不肖份子的覬覦。根據內政部警政署統計通報的資料顯示，2017 年 1 至 9 月政府受理的詐騙申訴案件高達 1 萬 6,311 筆，網路購物相關案件排名第 3，高達 14.67%(內政部警政署, 2017)。上述數據顯示網路詐騙行為並沒有隨著政府宣導而降低，反而與日俱增。探究其原因，除了電子商務的便利性讓民眾戒心降低，與詐騙者不斷翻新的詐騙手法也有關。表 2.1 所示為數種常見的詐騙類型，第一、二種為傳統常見手法；第三種可能源於賣家資訊洩漏；第四種則最為惡劣，將詐騙責任轉移給不知情的第三者。

表 2.1 常見詐騙類型

詐騙類型	說明
收款不出貨	收款不出貨，累積足夠的受害者後，最後捲款潛逃。
圖文不符，矇騙消費者	消費者所購買之商品與賣家刊登於交易平臺上所見不同。
寄發假得標信，攔截貨款	詐騙者從非法管道取得受害者之電子信箱，寄發假得標信，要求匯款至指定帳戶
偽裝賣家回收貨品	詐騙者要求賣家商品必須指定寄貨地點以及收件人姓名，之後假裝寄件者，到指定地點要求取回貨品。

2.2 模型融合(Model Fusion)

如前所述，單一偵測模型有其效能瓶頸，因此模型融合的要點為擷取各種模型長處，以產生更精確的偵測結果。此外，為避免產生過適(overfitting)現象，模型融合流程對於訓練資料集的運用亦需更加精細。為使後續討論更為順暢，以下將介紹各種可行的融合流程：

(1) 多階段模型融合

參考圖 2.1(a)，此種作法通常會建立多個分類模型($Model_1$~$Model_n$)，而後將將待測資料逐一輸入各種模型，每個模型 $Model_i$ 會將上一階段模型($Model_{i-1}$)之偵測結果做為額外輸入，最後再整合產出偵測結果。應用類似概念，前人研究中亦提出出連續過濾式(successive filtering)的線上拍賣詐騙偵測方法(圖 2.1(b))，差異點為偵測過程中若有決定性的結果，偵測步驟便可中斷。此種作法雖然合理，但模型的排列次序需有更精細的安排，不同待測樣本可能需使用不同的模型排序，而非均採用同一種順序。如此一來，當使用 n 個模型進行連續過濾時，若需針對不同類型樣本進行流程設計，則可能需嘗試 n!組合，這在實務上相當困難，也限制此種作法效能。

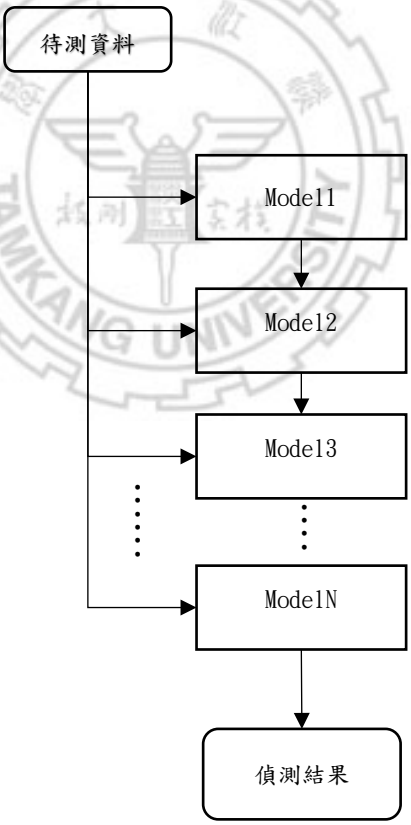


圖 2.1(a) 運用多模型進行多層偵測

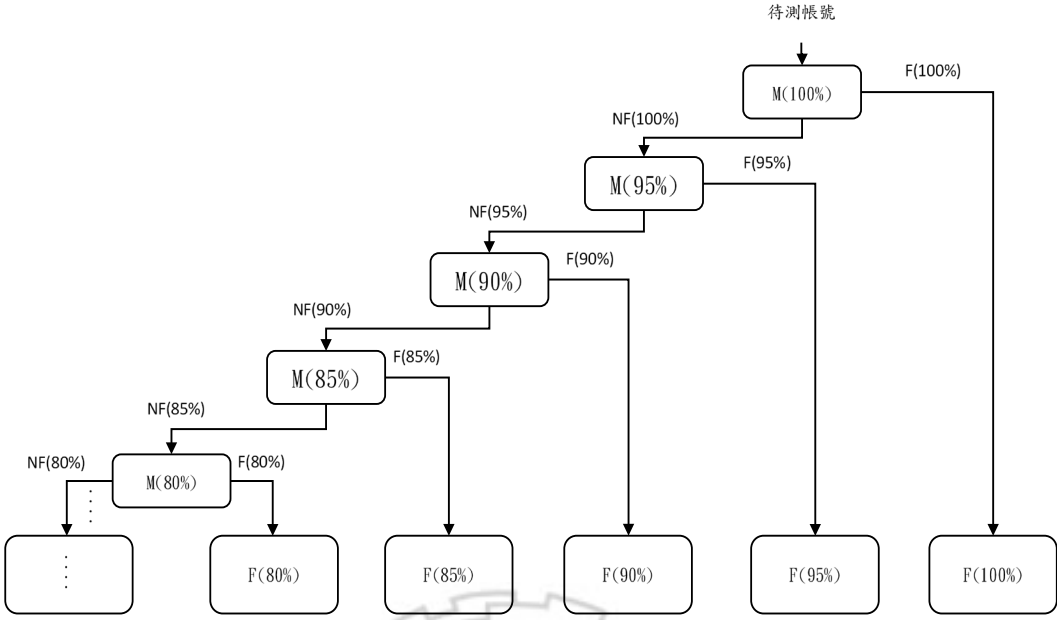


圖 2.1(b) 運用多模型進行練績過濾(Chang & Chang, 2012)

(2) 互補式模型融合

此類型的基本形式由一個主模型(main model)配合一個輔助模型(Aux Model)而組成。參考圖 2.2(a)，主模型提供主要的偵測結果，輔助模型則估計主模型的偵測誤差，再產生最後的偵測結果。圖 2.2(b)為利用此概念所建構的線上拍賣詐騙偵測流程(劉祐宏，2011)，其中 M1 擅長偵測詐騙者，M2 擅長偵測正常者，相互互補。當 M1, M2 無法決定時，再將待測帳號以第三個模型 M3 進行偵測。互補式模型融合雖然較複雜，但理論上可產生更精確的偵測結果。然而，此種作法的效能瓶頸在於最後階段的綜合模型之偵測能力。以上例而言，若 M3 無法對這些難以偵測之帳號進行有效分類，則之前 M1, M2 之準確性可能被抵銷(Chang&Chang, 2012)。有鑑於此， 運用此種融合流程時，可分別考慮以 easiest-first 或 hardest-first 方式來安排待測樣本，以確實提升總體準確率。

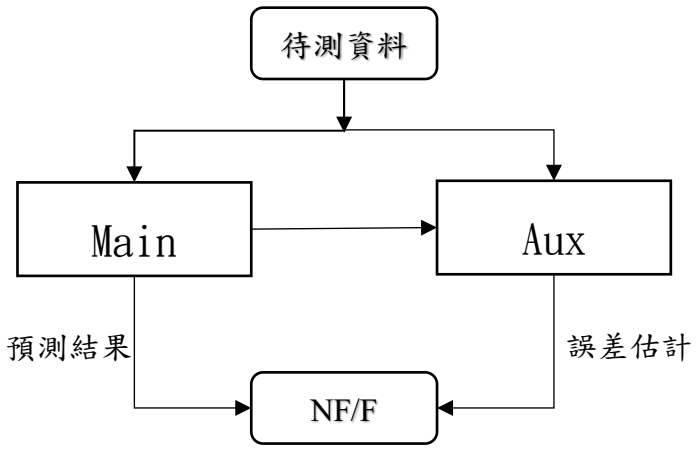


圖 2.2(a) 基本互補式融合流程

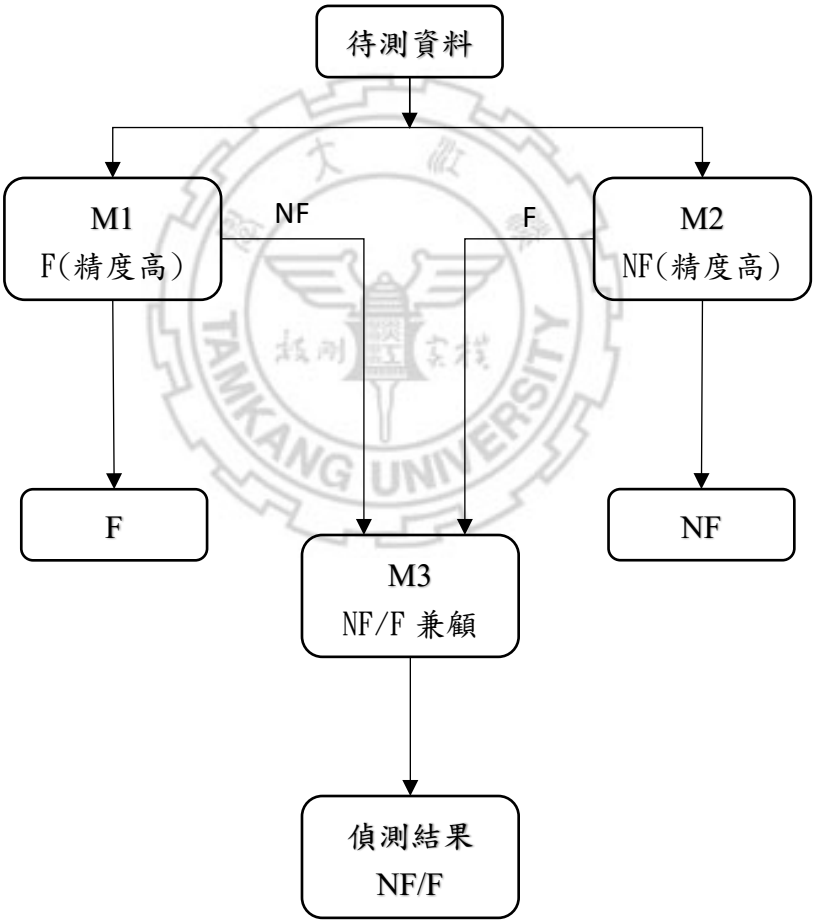


圖 2.2(b) 應用互補融合流程之研究

(3) 演算法融合(Fusion by Algorithm)

此種融合流程為利用特定演算法(如線性加權公式)將所有偵測模型($Model_1$~$Model_n$)之偵測結果加以整合，以產生最後的輸出。參考圖 2.3，其中的 Fusion Algorithm 的類型可根據被融合的模型特性而定，可為線性或非線性。

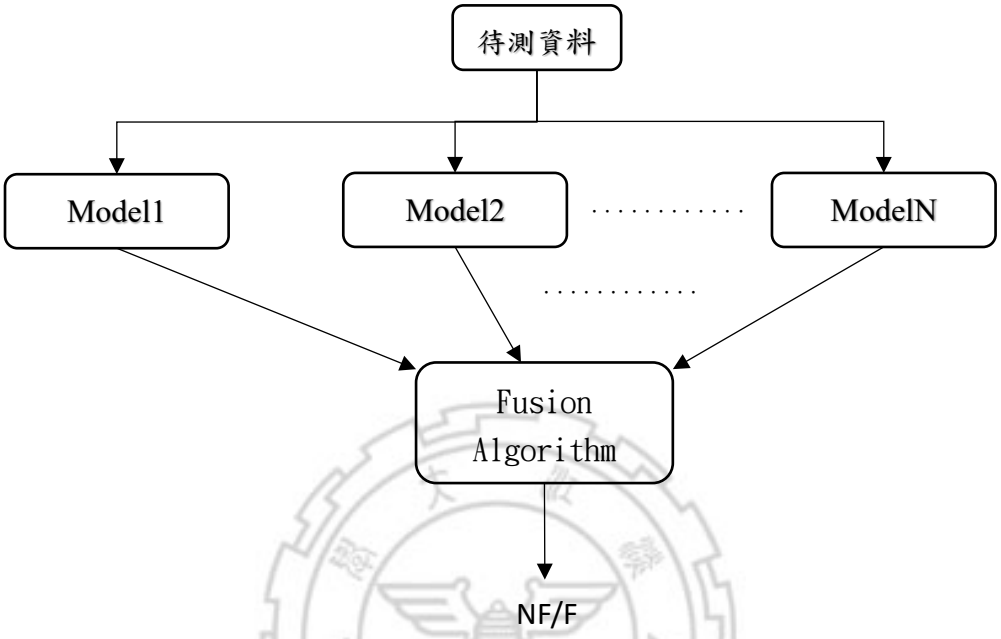


圖 2.3: 使用融合演算法進行模型融合

2.3 分類方法與屬性篩選

本研究的偵測模型是使用多種分類器融合而成，因此本節將介紹各種用於塑模的學習演算法。此外，也將介紹研究中使用之二種屬性篩選方法，以利後續之討論。

(1) 決策樹

C4.5(Quinlan,1993)是 ID3 演算法的改良版，它將 ID3 演算法的缺點進行彌補，能夠處理連續型以及離散型屬性的資料，具有遺漏值的資料也能夠進一步處理，並使用資訊增益率(Gain Ratio)作為決策樹屬性選擇的標準，而所謂的資訊增益率則是觀看一個特徵，分別觀察整顆決策樹有此特徵與無此特徵時的信息量差別，這就是資訊增益率。決策樹為一由節點及有向邊組成之樹狀結構，將其分為

根節點、內部節點和葉節點，前兩項均屬於屬性測試條件，最後一項則為類編號(Miao & Zhang,2015)。從樹的根節點經有向邊連接直到葉子節點的一條路則代表一條分類規則。

(2) 多層感知器(Multilayer Perceptron)

人工神經網路是一種計算模型，之前受限於運算設備導致塑模過程相當耗時，但近幾年因圖形處理器(GPU)的普及，使人工神經網路也得以快速發展。多層感知器(Multilayer Perceptron)是人工神經網路的一種，網路中的節點(node)為基本計算單元，運算方式為從外部接受輸入，節點將所有輸入的值加權計算後再輸出。除了輸入層與輸出層外，多層感知器至少包含一個隱藏層(Hidden Layer)，此層介於輸入層與輸出層間，作用在於將信息從輸入節點再次進行權重加總運算，再傳遞到輸出節點。面對非線性的分類任務，多層感知器可以擁有良好的分類準確率，而單層神經網路只能做線性分類任務，也因此往後的學者研究多以多層感知器為研究方向(詹佳憲、陳嘉平, 2016)。

(3) 貝氏網路(Bayesian Network)

貝氏分類法是一種或然率的學習方法(Probabilistic learning)，也就是一種以機率，統計學為基礎的分類方法，此分類法最大的優點在於具有漸增性(incremental)，當有新樣本出現時不需要將分類器整個拆散重新組合。這是決策樹所沒有的優點，也因此貝氏分類法適用於當有資料必須不斷加入的應用。理論上，貝氏網路是一個有向的非循環圖(Directed Acyclic Graphs)，每個節點代表一個隨機變數，每條連結(有向邊)表示兩個變數間的條件機率關係，因此便可藉由這些關係進行推論。若有新事件產生時，便可透過此網路推論目標事件發生的機率(謝金育, 2013)。

(4) 隨機森林(Random Forests)

隨機森林的基本原理是結合多棵 Gini 索引法(Gini index)的決策樹(參考圖 2-4(a)及 2-4(b))，並加入隨機分配的訓練資料，大幅度提高運算的準確率，也因此它擁有諸多優點例如:對於多種資料隨機森林擁有很好的分類精準度、對於資料的遺失它仍然可以擁有高準確度、對於不平衡的分類資料集來說，隨機森林可以自動平衡其誤差，綜觀上述所講隨機森林也可以被延伸應用在未標記的資料上，使其也擁有高度的分類準確率。以下將說明隨機森林運作原理:「令 N 為訓練樣本個數，M 表示特徵數目，並輸入特徵數目 m，用於確定決策樹上一個節點的決策結果(m 必須遠小於 M)。接著，從 N 個訓練樣本中以抽取並放回的方式取樣 N 次，形成一個訓練集(Bootstrap 取樣)，將未抽中的樣本做為測試集，以評估模型誤差。對每一節點，隨機選擇 m 個特徵，且決策樹上的每個節點其決定都是基於此 m 個特徵，最後計算其最佳的分支方式，而每棵樹成長過程並不進行修剪（Pruning)」（Leo Breiman,2001)。

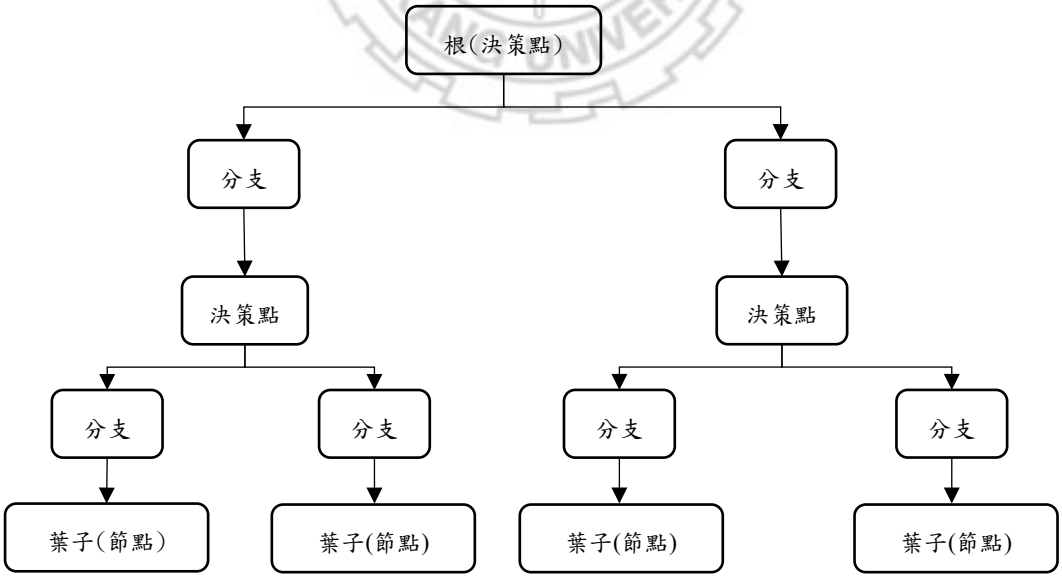


圖 2-4(a) 決策樹

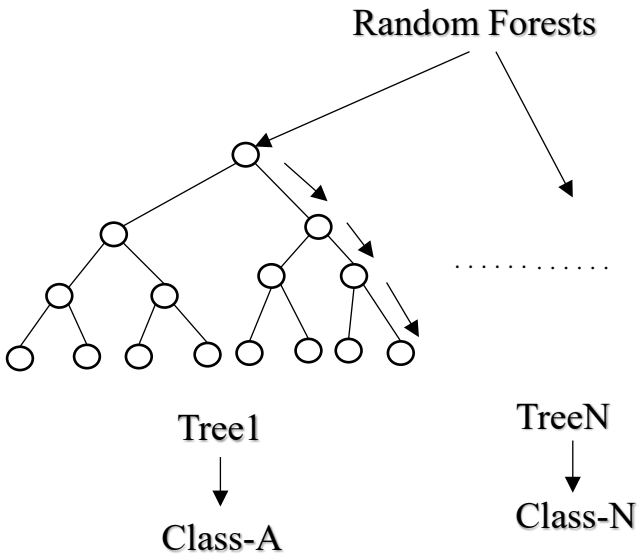


圖 2-4(b) 隨機森林

(5) AdaBoost(Adaptive Boosting)

Adaptive Boosting 中文名稱為自適應增強，其核心主旨在於將數個由同一個訓練集所訓練出來的弱分類器重新集合組裝變成一個強分類器。運作原理為給予初始訓練數據一個權值，假使第一個分類器（弱分類器）被錯誤分類的樣本其權值會增大，反之若是正確分類的樣本其權值則會減少，並用予訓練下一個分類器（弱分類器），並且根據偵測錯誤率的高低，其分類器（弱分類器）在整個集合分類器中佔的權重也會有所不同，錯誤率低的分類器佔的比例高，反之亦然，同時在每一次運行過程中都將加入新的分類器(弱分類器)，直到能夠符合使用者接受範圍的錯誤率或者最大疊代次數時即完成最終分類器(強分類器) (Guo & Li & Li,2008)。

(6) Principal Components Analysis

Principal Component Analysis (PCA)稱為主成分分析，是一種常用的屬性篩選(feature selection)方法，其作用在於降維(Dimension reduction)。當資料維度數(自變數)過於龐大時，常會考慮降低維度以節省資料集建構成本，但希望資料集品質不會因此而受影響。在理想狀況下，PCA 能降低資料的複雜度，並維持原有的

分類準確率(甚至更好)。

(7) Wrapper Subset Evaluation

Wrapper Subset Evaluation 稱為包裝器屬性選取，其作用在於使用一個目標學習演算法去估計屬性子集的值，並使用交叉驗證(cross-validation)來評估分類器對於全新資料之分類準確率。與主成分分析相較，由於 Wrapper Subset Evaluation 需實際建模並評估效果，所耗費時間。

第三章 以多模型融合為基礎之詐騙偵測方法

有關線上拍賣詐騙偵測，相關研究多使用單一模型進行預測，亦有學者採用階段性偵測，但效能仍有其限制。有鑑於此，以下將介紹本研究提出之多模型融合方法，透過線性組合 J48、多層感知器、貝氏網路和隨機森林等四種分類器，以產生更準確之模型。接著，我們針對詐騙者以及正常者不同資料配比對於分類器擁有不同精度(Precision)之特性，進行多模型融合，並提出多階連續過濾偵測以及平衡過濾偵測流程。希望能透過各種模型融合方法，進一步提升詐騙偵測的效能。

3.1 詐騙偵測屬性集

偵測模型的效能與所使用之屬性集息息相關，合適的屬性集能有效表示資料的特質，產生高準確率的偵測模型。根據前人研究，拍賣詐騙偵測屬性大致可分為以下三類: 評價相關屬性(feedback-related features)、價格相關屬性(price-related features)與物品相關屬性(item-related features)。為使偵測結果更為準確，本研究綜合前人所提出之 52 種偵測屬性(Chang & Chang, 2014; Chau et al., 2006; 林敬堯, 103)，並去除其中過於針對性之屬性(與特定機制相關，如 Yahoo 的安全賣家)，最後共得到 37 種偵測屬性(如表 3.1 所示)。其中，與價格相關屬性主要為驗證賣家的交易行為是否改變。例如，原本販賣低價產品，突然改賣高價產品，或者買入商品平均價格與賣出商品平均價格差異過大，均屬於異常交易常見徵兆。此外，與評價相關屬性則用以檢驗評價累積的方式，若出現過於密集或正評來源可疑，亦有異常交易嫌疑。

表 3.1 本研究使用之 37 種詐騙偵測屬性

No	屬性名稱	說明
1	EndCloseToPos	得到正評的結標評平均時間
2	RatioOfPos	正評比率
3	RatioOfSToS	評價來自賣家的比例

4	DensityOfPos	正評密度
5	RatioOfNeg	負評比率
6	RatioOfBuyingRate	買東西比率
7	MeanBuying	平均買價
8	MeanSelling	平均賣價
9	GiveManRating	給評價者平均評價
10	Rating	正評百分比
11	BuyingNumber	買東西數
12	MeanBuyingLast30	後 30 天平均買價
13	StdSellingFirst30	前 30 天賣價標準差
14	BuyingNumberOfPos	買東西正評數
15	SellingNumber	賣東西數
16	SellingNumberOfPos	賣東西正評數
17	MeanBuyingLast15	後 15 天平均買價
18	StdBuyingFirst30	前 30 天買價標準差
19	StdBuyingLast30	後 30 天買價標準差
20	StdSellingFirst15	前 15 天賣價標準差
21	StdBuyingFirst15	前 15 天買價標準差
22	StdBuyingLast15	後 15 天買價標準差
23	(SellingPrice/SellingTime)_LastOneTwo	最後兩筆交易之價格差/交易時間差
24	SellingNumberLast30	後 30 天賣東西數
25	NumberOfPostive	正評數
26	SellingNegtiveNumberLast30	後 30 天賣東西負評數
27	StdSellingLast15-StdSelling	後 15 天賣價標準差-賣價標準差
28	StdSellingLast15- StdSellingLast30	後 15 天賣價標準差-過去 30 天賣價標準差
29	SellingLast15MeanTimeInterval	後 15 天平均交易時間間隔
30	MeanSellingLast15-MeanSelling	後 15 天平均賣價-平均賣價
31	MeanSellingLast15-MeanSellingLast30	後 15 天平均賣價-過去 30 天平均賣價
32	StdSellingLast30-StdSelling	後 30 天賣價標準差-賣價標準差
33	SellingLast30MeanTimeInterval	後 30 天平均交易時間間隔
34	SellingMeanTimeLastOneTwo	最後兩筆交易之間的時間間隔
35	MAXSellingPrice	最大賣價
36	SellingMeanTimeInterval	平均交易時間間隔
37	AllRating	所有評價

3.2 以模型融合建立詐騙偵測模型

為產生更有效的分類模型，以下先討論單一分類模型的效能瓶頸，再說明本研究提出之線性融合模型與過濾式偵測流程。

3.2.1 單一分類模型之效能

為了解各種單一分類模型效能，我們使用 Yahoo 拍賣交易資料進行實驗，分別針對 J48, MLP(Multiple-Layer Perception), BN(Bayes Network)與 RF(Random Forest)進行塑模與驗證。資料集共有 1500 筆紀錄，其中正常者與詐騙者比例為 2:1，實驗結果如表 3.2 所示。由表中可知，表現最佳的為 RF 模型，準確率為 86.66%，次佳的為 J48 之 84.79%，最差的則為 BN，準確率為 80.09%。當再考慮詐騙者(F)與正常者(NF)之偵測精度(Precision)與召回率(Recall)，可看出更多差異。參考表 3.2，各種 分類器對於 NF 之精度普遍高於 F，BN 甚至只有 69.80%。而召回率雖有類似傾向，但低精度的項目，可能具有高召回率(例如 MLP 之 NF 與 J48 之 F)。由上述結果可知，各種分類器各有特色，但對詐騙者類別(F)之偵測，則仍有進一步改善空間。

表 3.2 各種分類器對於詐騙偵測之效能比較

分類器	Accuracy	prec_NF	recall_NF	prec_F	recall_F
J48	84.79%	88.50%	87.14%	77.81%	80.05%
MLP	82.24%	84.53%	90.41%	80.15%	67.91%
BN	80.09%	86.01%	82.23%	69.80%	75.82%
RF	86.66%	88.90%	91.30%	81.60%	77.20%

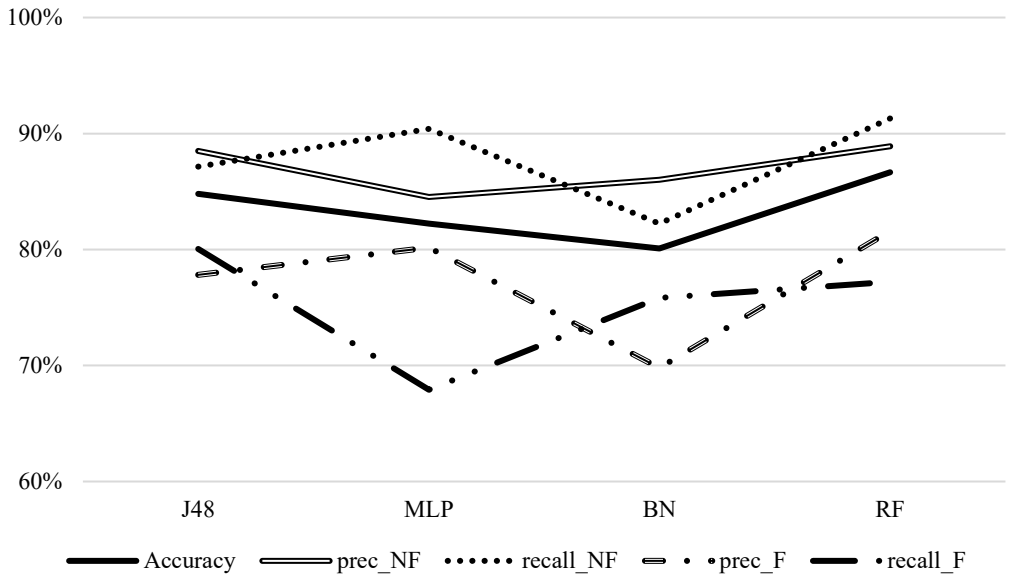


圖 3.1: 各種分類器在各種效能指標之比較

為進一步了解上述效能是否受屬性特質影響，我們再使用二種屬性挑選方法，對屬性集進行過濾。第一種為 Principal Components Analysis(PCA)，其特質為屬性篩選與後續使用之分類器無關，搜尋方式設定為 Ranker。另一種則為 Wrapper Subset Evaluation (Wrapper)，此種方法會依照目標學習演算法進行屬性篩選。實驗時，PCA 之搜尋方式設定為 Ranker，Wrapper 則是為 Best First，結果如表 3.3 所示。由表中可知，以特定分類器效能為目標進行屬性挑選的 Wrapper 法均優於 PCA。然而，以準確率而言，與表 3.2 相較，仍無法提供明顯的改進。

表 3.3 使用 PCA 與 Wrapper 法進行屬性挑選之偵測結果*

Accuracy	J48	MLP	BN	RF
PCA	83.88%	82.03%	80.36%	86.61%
Wrapper_J48	82.64%	80.58%	78.36%	86.76%
Wrapper_MLP	84.64%	82.21%	79.06%	85.91%
Wrapper_BN	82.45%	79.94%	80.73%	85.76%
Wrapper_RF	84.21%	81.52%	80.48%	87.12%

*本表實驗採用 Weka API 之套件來進行

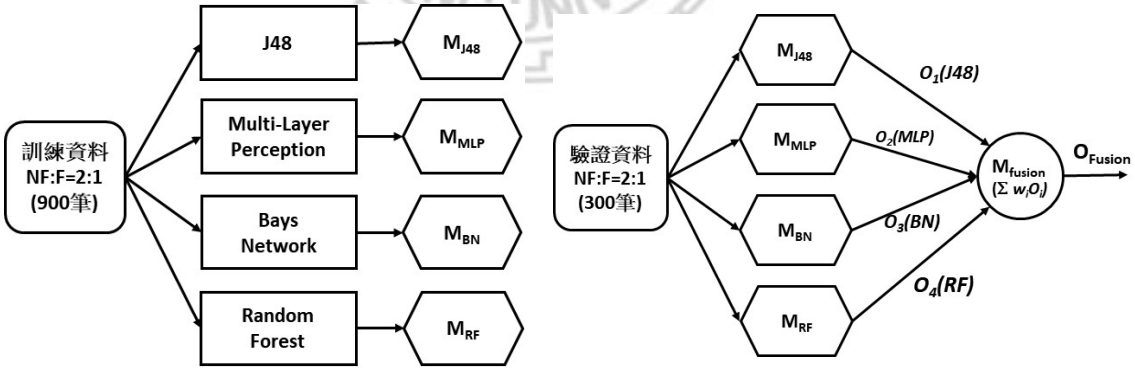
由上述實驗可知，使用各種單一模型配合不同屬性挑選方法，所建立之偵測模型效能有其瓶頸。為改善此狀況，本研究將使用模型融合方式，進一步提升準確率。

3.2.2 以線性方式進行模型融合

根據上述討論，本節將介紹研究所提出之模型融合方法。首先，根據訓練集資料，建立多種單一偵測模型 $M_1, M_2, \ldots, M_n$。之後，再利用線性回歸配合驗證資料集(validation set)，產生融合模型 M_{fusion}，其輸出 O_{Fusion} 公式如下:

$$O_{Fusion} = \sum_{i=1}^{n} w_i O_i + c \qquad \text{(3-2(a))}$$

其中 Oi 為 Mi 對於特定待測帳號的輸出值， c 則為線性公式之常數項。以下說明本研究融合模型產生方式(參考圖 3.2)。首先，利用訓練資料集(900 筆記錄，NF:F=2:1)產生各種單一模型，此處為 J48, MLP, BN 與 RF(參考圖 3.2(b))。之後，再利用驗證集(300 筆記錄，NF:F=2:1)配合回歸分析，導出公式 3.2(a)所需之 *wi* 與 *c*。融合模型建立後，便可對測試資料進行測試(參考圖 3.2(c))。



(b) 建立單一模型　　(c) 建立融合模型

圖 3.2: 詐騙偵測模型融合方法

為瞭解融合模型之準確率，我們使用 300 筆記錄(NF:F=2:1)進行測試，結果如表 3.4 所示，其中 Wrapper 的指定分類器選擇偵測效果最好的 RF(Random Forest)進行比較。此外，Ofusion 為一介於[0,1]之間實數，將其門檻值設定為 0.5，當

Ofusion>0.5 時，令其輸出判讀為 Fraud，否則為 Non-Fraud。參考表 3.4 可知以線性回歸方式融合多種單一模型確實能有效提升整體詐騙偵測之準確率。此外，為驗證屬性篩選是否有助於準確率的提升，本研究採用 PCA(Principal Components Analysis)與 Wrapper(Wrapper Subset Evaluation)進行屬性篩選，結果如表 3.4 所示，並無進一步改善(參考 Accuracy(PCA)與 Accuracy(Wrapper_RF)欄)。總結上述說明，單純以線性方式融合模型，並無法產生穩定領先 Random Forest 之結果(準確率 86.66%)。因此，以下將進一步使用多階連續過濾偵測以及平衡過濾偵測流程之概念，產生更有效的融合模型。

表 3.4 以線性方式融合 4 種分類器之偵測準確率

模型/準確率	Accuracy	Accuracy(PCA)	Accuracy(Wrapper_RF)
線性模型	87.52%	86.94%	87.15%

3.3 多階連續過濾之詐騙偵測流程

以線性組合方式融合各種模型為常見方式，但若能進一步考慮詐騙者與正常者不同訓練資料配比和各分類器效能之間的關係，將有機會產生更加精確的偵測結果。因此，本節首先將探討以不同比例(NF:F)訓練集產生之模型的效能，之後再介紹如何透過這些模型，以多階連續過濾與平衡式過濾流程加以組合。

3.3.1 不同訓練資料集之偵測效能

之前實驗中，訓練集與測試集之 NF:F 比例均為 2:1。以下我們將測試以不同配比進行模型訓練，以瞭解這些模型之偵測效能改變。以下實驗仍採用與表 3.2 相同之 1500 筆交易記錄，訓練集與測試集之 NF:F=2:1，訓練集與測試集資料大小比值 2:1。首先，我們挑選單一模型中表現最佳之 Random Forest，分別針對訓練集之 NF:F=1:5, 1:3, 1:2, 1:1, 2:1, 3:1, 5:1 進行實驗。參考表 3.5 之結果，有表中可看出，偵測準確率仍以 2:1 之模型最高(0.869)，但對於 NF 與 F 之偵測，則可

看出不同資料配比產生之差異。以 NF 之精度而言，當 NF:F=1:5 時，雖然總體準確率只有 0.768，產生之模型具有極高之精度(0.977)。同樣地，當 NF:F 由 1:2 調整至 5:1 時，詐騙者(F)之偵測精度可達 0.900，與 NF:F=2:1 相較，具有明顯提升。圖 3.3 顯示各項偵測效能之趨勢，由圖中可看出其詐騙者的偵測精度(prec_F)隨著 NF 的比例增加而增加，而正常者之精度(prec_NF)則相反，隨著 F 之比例增加而提升。根據上述觀察，串接這些具有不同效能的模型，有機會改善整體的偵測效能。

表 3.5 在不同 NF:F 配比下塑模之偵測結果(Random Forest)

RandomForest	Accuracy	prec_NF	recall_NF	prec_F	recall_F
NF:F=1:5	0.768	0.977	0.669	0.594	0.969
NF:F=1:3	0.806	0.959	0.743	0.644	0.935
NF:F=1:2	0.829	0.943	0.793	0.686	0.903
NF:F=1:1	0.862	0.910	0.881	0.775	0.825
NF:F=2:1	0.869	0.877	0.934	0.848	0.739
NF:F=3:1	0.867	0.862	0.954	0.882	0.693
NF:F=5:1	0.849	0.834	0.966	0.900	0.614

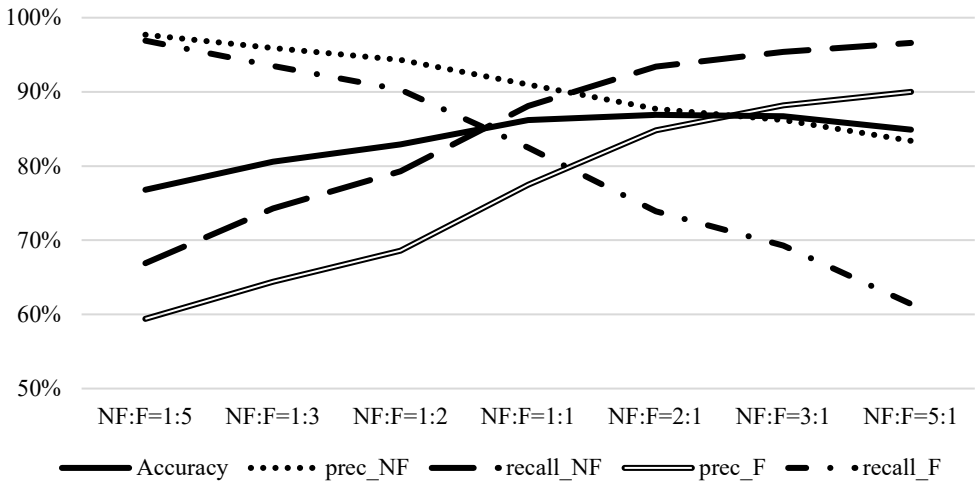


圖 3.3: 使用 Random Forest 配合不同 NF:F 配比之偵測效能變化圖

根據上述方式，我們得知詐騙者(F)與正常者(NF)之偵測精度與召回率，確實會因塑模訓練集與測試集配比改變而改變，為了使融合模型能達到最大效能，我們採用集合弱分類器組成強分類器的 AdaBoost 作為塑模方法進行實驗，並比較不同訓練資料配比下是否如 Random Forests 一樣擁有其特性。實驗結果如表 3.6 所示，我們可以發現其趨勢與 Random Forests 類似(參考表 3.5)。雖是如此，但可發現 AdaBoost 之 NF 比例越來越高時，詐騙者偵測精度(prec_F)不如 Random Forest，但具有較高的召回率。以 NF:F=5:1 為例，其詐騙者偵測精度(prec_F)為 0.878，不如 Random Forest 之 0.900，但其召回率 0.679 卻明顯高於 Random Forest 之 0.614。由上述觀察可知，各種分類器在不同訓練資料配比下，有不同表現。下一節將探討如何加以組合，以產生準確度更高偵測結果。

表 3.6 在不同 NF:F 配比下塑模之偵測結果(AdaBoost)

AdaBoost	Accuracy	prec_NF	recall_NF	prec_F	recall_F
NF:F=1:5	0.757	0.972	0.656	0.583	0.962
NF:F=1:3	0.792	0.954	0.723	0.627	0.930
NF:F=1:2	0.823	0.944	0.782	0.675	0.906
F:NF=1:1	0.854	0.919	0.857	0.747	0.849
NF:F=2:1	0.866	0.889	0.913	0.816	0.772
NF:F=3:1	0.864	0.879	0.925	0.831	0.744
NF:F=5:1	0.862	0.856	0.953	0.878	0.679

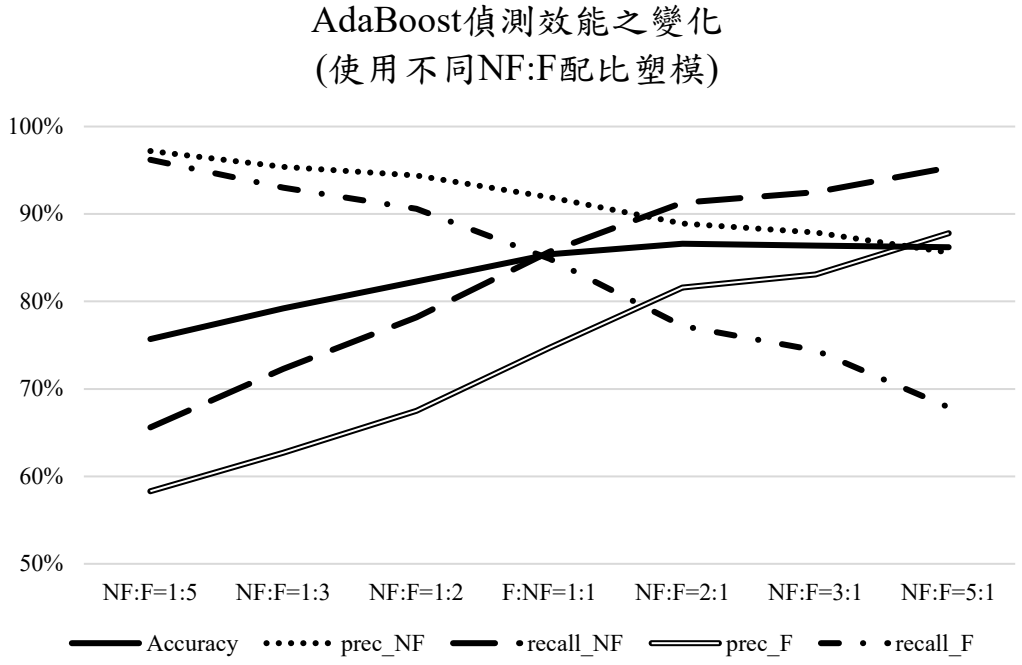


圖 3.4: 使用 AdaBoost 配合不同 NF:F 配比之偵測效能變化圖

3.3.2 多模型詐騙偵測架構

根據上述觀察，本研究發現在不同訓練資料配比下確實會對分類器造成顯著的預測精度影響，因此本研究利用此特性，建構出更有效的融合模型。

(1)多階連續過濾

為進行連續過濾，本研究將先建置以下模型(M1~M5):

模型	塑模方法	訓練資料配比	模型特點
M1	Random Forest	NF:F=1:5	對 NF 具有高偵測精度
M2	Random Forest	NF:F=5:1	對 F 具有高偵測精度
M3	AdaBoost	NF:F=1:3	對 NF 具有較高偵測精度
M4	AdaBoost	NF:F=3:1	對 F 具有較高偵測精度
M5	Random Forest	NF:F=2:1	對 F,NF 具有均衡偵測能力

有關連續過濾流程，請參考圖 3.5 的虛擬碼(SuccessiveFiltering)。對每一待測帳號 acc，進行 M_1~M_5 的偵測，在 M_1 建構對於正常者(NF)擁有高精度預測的模型，因此只要待測帳號 acc 於 M_1 被檢測出為正常者即以正常者結束偵測，假使

不是正常者則流往下一階段 M_2，M_2 則是對於詐騙者(F)擁有高精度預測所建構之模型，因此只要於 M_2 被檢測為詐騙者即以詐騙者結束偵測，M_3 以及 M_4 亦是如此，分別對應正常者以及詐騙者擁有高精度的預測，待到最後如果都無法檢測出其性質，則交給最後的 M_5 進行最後判定。

```
1   procedure SuccessiveFiltering
2   input   M1~M5: 模型集合
3           TestSet: 待測帳號集合
4   output  F 與 NF: 儲存 TestSet 與 M1~M5 之比對結果
5       for each account acc in TestSet do
6           if (!M1.isF(acc)){NF.add(acc)}//如果 M1 判斷為 NF 即是 NF
7           else {
8             if (M2.isF(acc)){F.add(acc)}//如果 M2 判斷為 F 即是 F
9             else {
10               if(!M3.isF(acc)){NF.add(acc)}
11               else {
12                   if(M4.isF(acc)){F.add(acc)}
13                   else {
14                     if(M5.isF(acc))F.add(acc)
15                     else NF.add(acc)
16                 }
17               }
18            }
19      end for
20  end procedure
```

圖 3.5: 運用多階連續過濾進行詐騙偵測

(2) 平衡式過濾

上述連續過濾之優點為逐步運用高精度的模型，過濾出較確定之帳號分類(F 或 NF)。然而，當 M1 與 M2 或者 M3 與 M4 之判斷不同時，可能導致誤判。因此，本研究再提出平衡式過濾流程，希望能將具有爭議的帳號，留待後續模型進行偵測，詳細偵測流程如圖 3.6 所示。當待測帳號 acc 進入平衡式偵測流程時，仍先由 M1 進行偵測(對於正常者擁有高偵測精度)，但與連續過濾模型最大不同之處，其 M2 並不是等 M1 過濾後再進行偵測，而是同時進行偵測。當 M1 與 M2 判斷結果相左，都無法分辨時，便將此帳號流至下一階段。當帳號流至 M3 與 M4

時，其流程亦與 M1, M2 之運用相同。最後，才將 M1~M4 無法分辨之帳號交由 M5 進行最後判定。由上述流程可看出，此種作法具有雙重優點，既能有效運用高精度模型進行偵測，也能避免過早決爭議性帳號，有效提升偵測準確率。有關上述二種提出方法之效能，將在第四章進行討論。

```
1   procedure BalancedFiltering
2   input   M1~M5: 模型集合
3           TestSet: 待測帳號集合
4   output  F 與 NF: 儲存 TestSet 與 M1~M5 之比對結果
5       for each account acc in TestSet do
6           if (!M1.isF(acc)&&(M2.isF(acc)){如果 M1=MF 且 M2=F 則往下一階
7              if (!M3.isF(acc)&&(M4.isF(acc)){
8                   (M5.isF(acc))?F.add(acc):NF.add(acc)
9               } else if (!M3.isF(acc)){NF.add(acc)
10              }else if (M4.isF(acc)){F.add(acc)
11              }
12          }else if (!M1.isF(acc)){NF.add(acc)//M1=F 則確定是 F
13          }else if (M2.isF(acc)){F.add(acc)
14          }
15  end procedure
```

圖 3.6: 平衡式過濾偵測流程

3.4 偵測流程

本研究採用的資料集為 Yahoo!奇摩拍賣 2009~2012 年 1500 筆真實的交易資料，並配合 37 種各類型詐騙偵測屬性進行塑模(參閱 3-1 節)。

整體流程如下：

(1) 資料切割: 將資料集以亂數分割為訓練集(Training)，驗證集(Validation)以及測試集(Test)，各 900 筆、300 筆、300 筆，並將正常者以及詐騙者數量控制在 1:5、5:1、1:3、3:1 以及 2:1，seed(種子數)則設定 10~20，擴大實驗範圍，證明其偵測有效之程度。

(2) 屬性篩選: 使用 Principal Components 與 Wrapper Subset Evaluation 對 37 項各類型偵測指標進行篩選，經由屬性之篩選能否提高模型偵測之準確率。

(3) 建構線性融合模型: 使用 4 種分類器(J48、多層感知器、貝氏網路、隨機森林)做線性回歸模型。

(4) 建構多階連續過濾以及平衡過濾偵測模型: 利用不同訓練資料配比的詐騙者以及正常者對於分類器擁有不同精度之結果，建立預測模型。

(5) 偵測順序: 連續過濾以及平衡過濾偵測模型中之 M1 與 M2 模型，採用單一分類器中擁有最高準確率的 Random Forest (RF)，M3 以及 M4 則是使用 AdaBoost (Ad)，它能組合數個弱分類器將其重新組裝變成強分類器。最後一層之 M5 模型，則改回使用分類效果最佳的 RF 分類器。

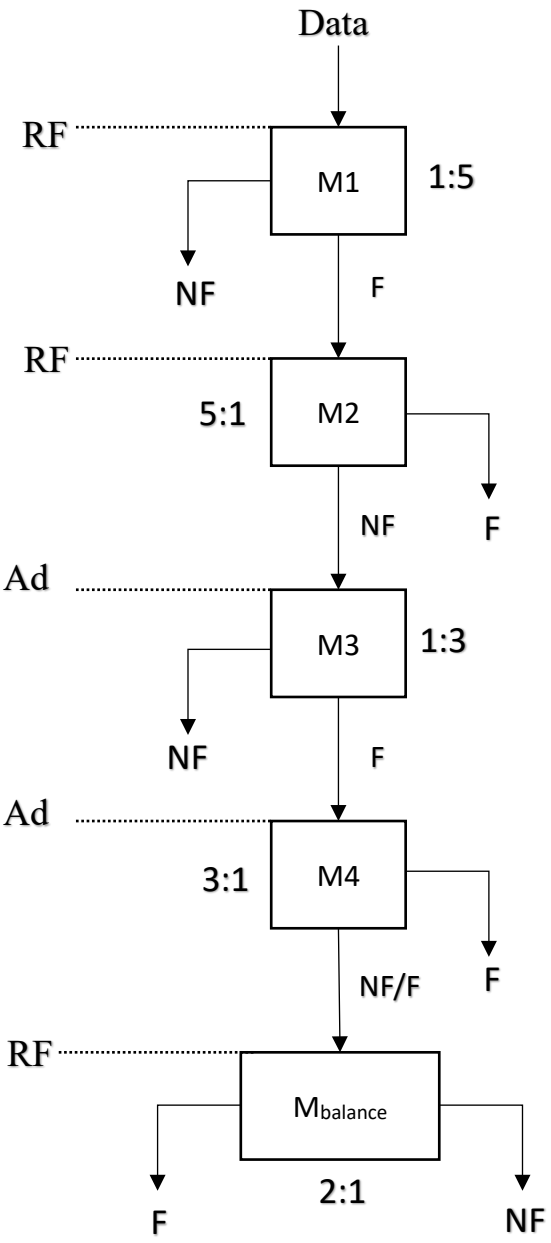


圖 3.7: 多階連續過濾詐騙偵測流程

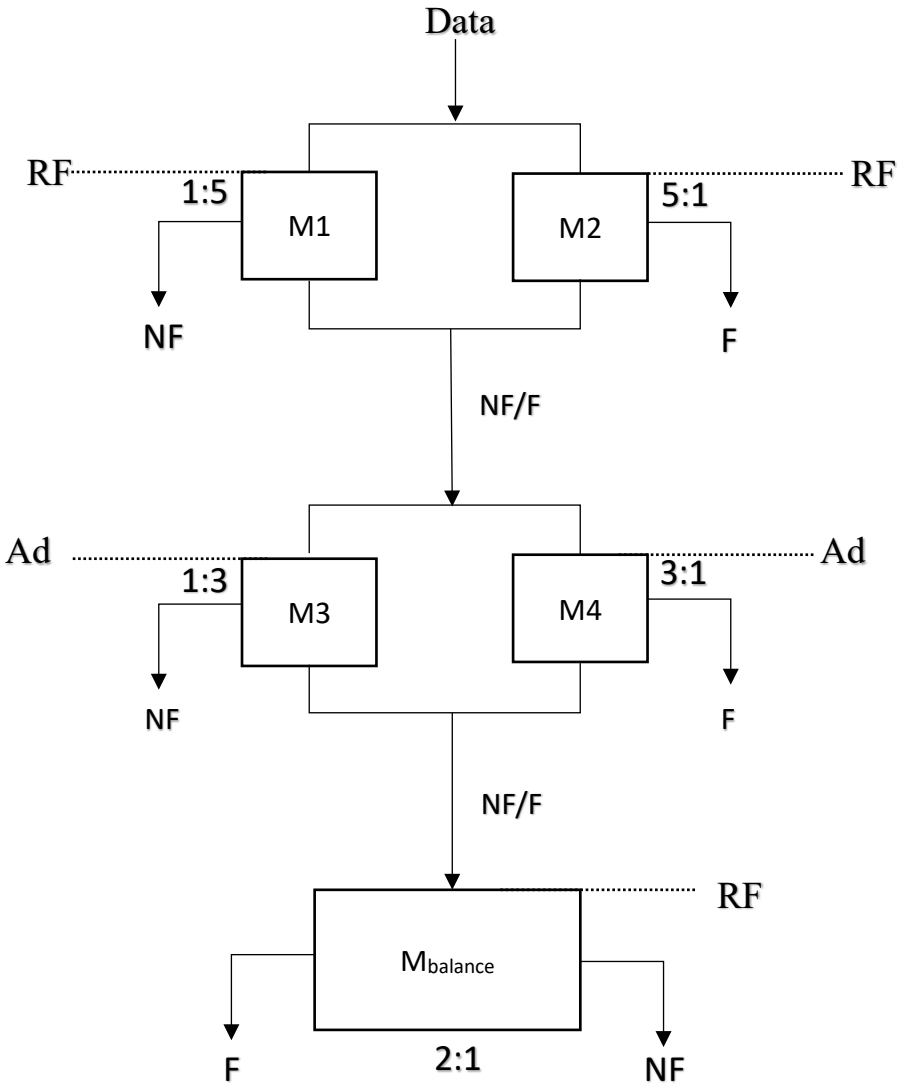


圖 3.8: 平衡過濾詐騙偵測流程

第四章 實驗結果與討論

為驗證本研究提出方法之有效性，我們以 Yahoo!奇摩拍賣網站蒐集之實際交易資料進行測試，以比較融合模型與傳統偵測模型的差異。此外，並探討屬性篩選與否對於偵測準確率產生影響。

4.1 實驗設定

本研究採用 Yahoo!奇摩拍賣 2009 年至 2012 年間，共 1500 筆真實交易做為資料集。實驗時，將其亂數分為訓練集(Training)900 筆、驗證集(Validation)300 筆、與測試集(Test)300 筆，各資料集中正常者與詐騙者比例均為 2:1。模型建立與測試均使用 Weka API 來進行實作，先以 Training Set 建立 J48、多層感知器、貝氏網路和隨機森林偵測模型，在以 Validation Set 進行線性回歸分析，以產生線性融合模型。多階連續過濾以及平衡過濾偵測模型其 M1~M5 分別對應如下，RandomForst(NF:F=1:5)、RandomForst(NF:F=5:1)、AdaBoost(NF:F1:3)、AdaBoost (NF:F=3:1)和 RandomForest(NF:F=2:1)之不同訓練配比所建立，最後使用測試集(NF:F=2:1)驗證其效能。

表 4.1 Confusion Matrix

預測/實際	Positive	Negative
Positive	True Positive (TP)	False Positive(FP)
Negative	False Negative(FN)	True Negative(TN)

爲比較實驗結果優劣，需有合適的評量指標。參考表 4.1 的混淆矩陣(Confusion Matrix)，其中的 TP, TN, FP, NN 分別代表真陽性、真陰性、偽陽性、偽陰性。據此，本研究使用以下文獻中常用的評量指標。其中，Success Rate (Accuracy)為總體預測準確率，由”(TP+TN)/受測樣本數”計算而得。類別 C 之精度(Precison)為預測類別為 C 之所有樣本中，實際為 C 類別之比率；召回率(Recall)

則為受測資料集中實際為類別 C 的樣本數，與預測為 C 之數量之比例。例如，若正常者樣本有 120 個，預測報告顯示有 100 個正常者，但其中僅有 85 位確實為正常者，則其召回率為 85/100=0.85，精度(precision)則為 85/120=0.708。

TP rate = TP/(TP+FN)

FP rate = FP/(FP+TN)

Precision=TP/(TP+FP)

Recall= TP/(TP+FN)　(與 TP rate 相同)

F-Measure = (2 × Recall × Precision)/(Recall + Precision)

Success Rate = (TP+TN) / (TP+FP+TN+FN)

4.2 線性融合模型之效能測試

表 4.2 為單一模型與線性融合模型之準確率比較，由於實驗共進行 10 次，表中結果為使用不同亂數種子所產生之資料集。實驗結果顯示，本研究提出之線性回歸模型，確實可獲得高於其他單一模型偵測準確率(87.52%)，但仍與 Random Forest(RF)相差無幾。然而，參考圖 4.1 偵測準確率比較折線圖，更可看出本研究提出方法之準確性穩定領先其他各種方法。上述結果說明線性融合模型確實有助於提升詐騙偵測準確率，提供更穩定的偵測結果。

表 4.2 單一模型與線性融合模型之偵測準確率比較

Accuracy	J48	MLP	BN	RF	線性融合模型
Seed10	83.00%	83.00%	82.67%	86.67%	87.67%
Seed11	87.33%	82.33%	83.33%	87.67%	87.00%
Seed12	83.33%	81.15%	81.33%	85.00%	86.67%
Seed13	85.30%	81.27%	82.67%	86.67%	87.67%
Seed14	84.33%	81.33%	73.67%	87.00%	87.20%
Seed15	84.33%	82.67%	81.00%	86.75%	88.67%
Seed16	84.75%	81.67%	78.67%	83.45%	86.67%
Seed17	80.67%	81.00%	80.00%	85.75%	86.67%
Seed18	86.67%	83.56%	80.67%	88.60%	89.00%
Seed19	85.33%	84.00%	80.00%	88.67%	88.50%
Seed20	87.67%	82.67%	77.00%	87.00%	87.00%
平均	84.79%	82.24%	80.09%	86.66%	87.52%

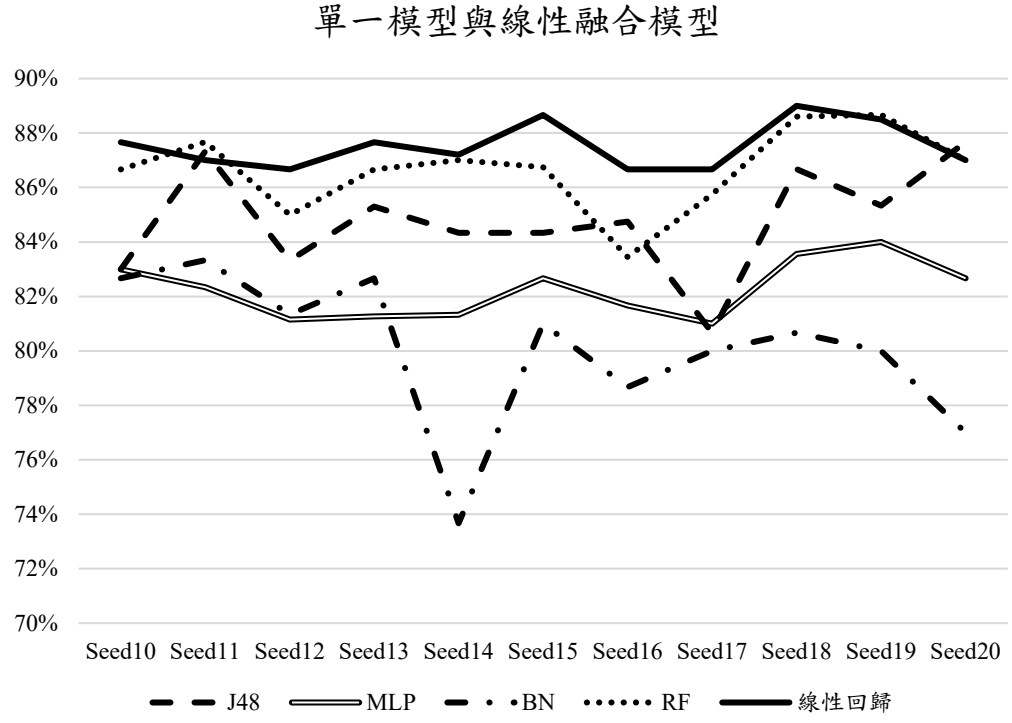


圖 4.1: 單一模型與線性融合模型之偵測準確率比較圖

為驗證屬性篩選是否有助於改善偵測準確率，我們分別以 Principal Components 與 Wrapper Subset Evaluation 對原 37 項偵測指標進行篩選，分別選出 22 項及 14 項屬性。參考圖 4.2 之實驗結果，屬性篩選對於融合偵測模型並無

明顯幫助。因此，如欲以屬性篩選進一步提升總體效能，可能需發展與傳統方式不同之篩選方法。

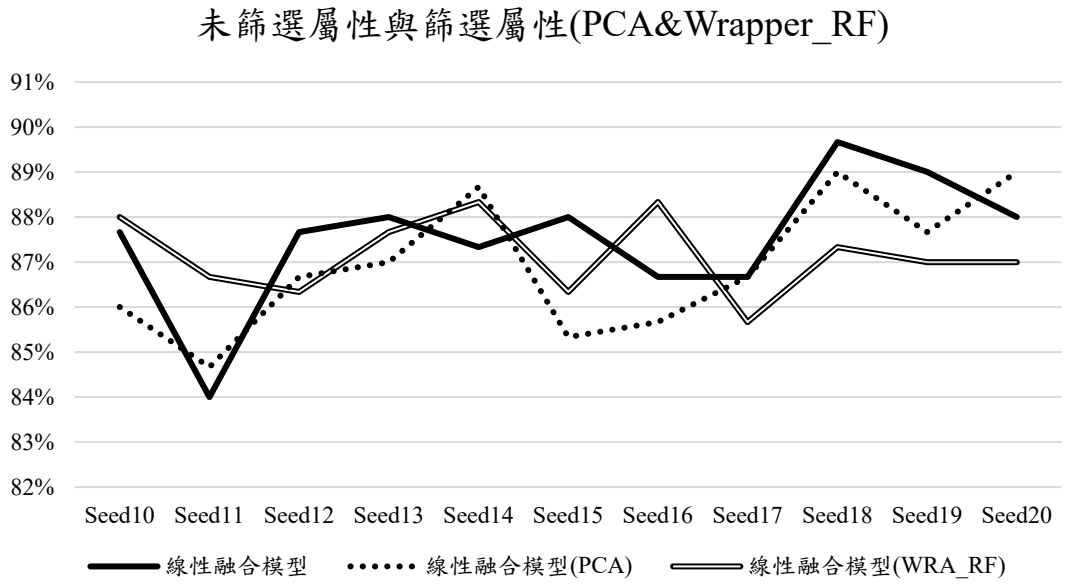


圖 4.2: 線性融合模型偵測結果：屬性篩選與未篩選之比較

4.3 連續過濾偵測流程效能測試

本節將對論文中所提出之多階連續過濾式與平衡過濾偵測流程進行測試，並與單一模型中表現最好之 Random Forest 進行比較(實驗設定採 Test set 正常者與詐騙者 2:1)。實驗結果如表 4.3 所示，由表中可發現，本研究提出之多階連續過濾以及平衡式偵測流程，確實能提高偵測準確率，驗證提出方法之有效性。因此，接下來我們將探討屬性篩選對於兩種融合模型是否一樣擁有提升偵測準確率之效能。

表 4.3 過濾式以及平衡式融合模型與 RF 之準確率比較

準確率/模型	過濾式	平衡式	RF
Accuracy	88.45%	88.36%	86.66%

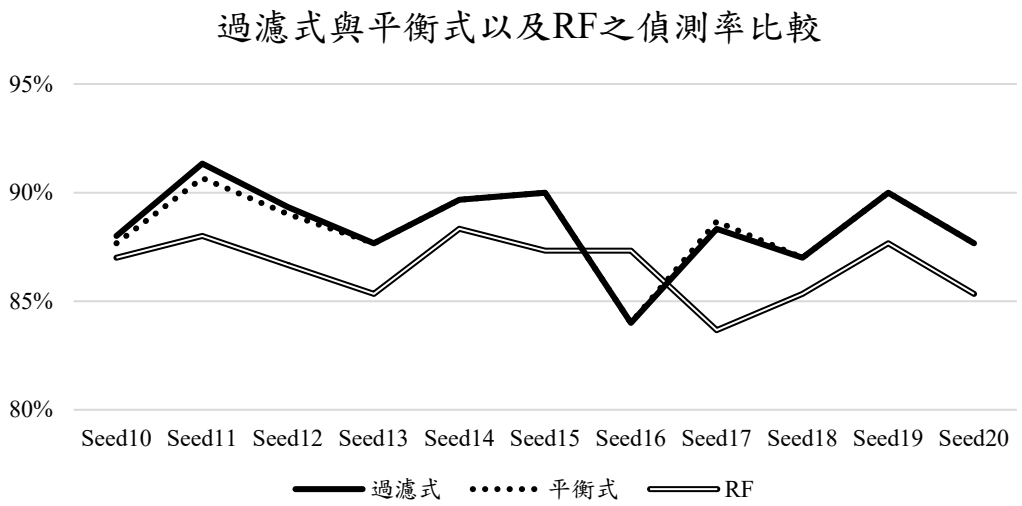


圖 4.3: 多階連續過濾及平衡過濾偵測流程與 Random Forest 之準確率比較

經由表 4.4 實驗結果可得知，即使運用 PCA 事先進行屬性篩選，本研究提出之兩種融合方法均能穩定領先單一分類器(參考表 4.2)。但也可看出，屬性的篩選對於本研究提出之融合模型，並無法有效提升之偵測效能(參考圖 4.4)，因此，如欲以屬性篩選進一步提升總體效能，可能需發展與傳統方式不同之篩選方法。

表 4.4 多階連續過濾以及平衡過濾融合模型與 RF 之準確率比較(PCA 篩選)

準確率/模型	過濾式(PCA)	平衡式(PCA)	RF(PCA)
Accuracy(PCA)	87.30%	87.03%	86.55%

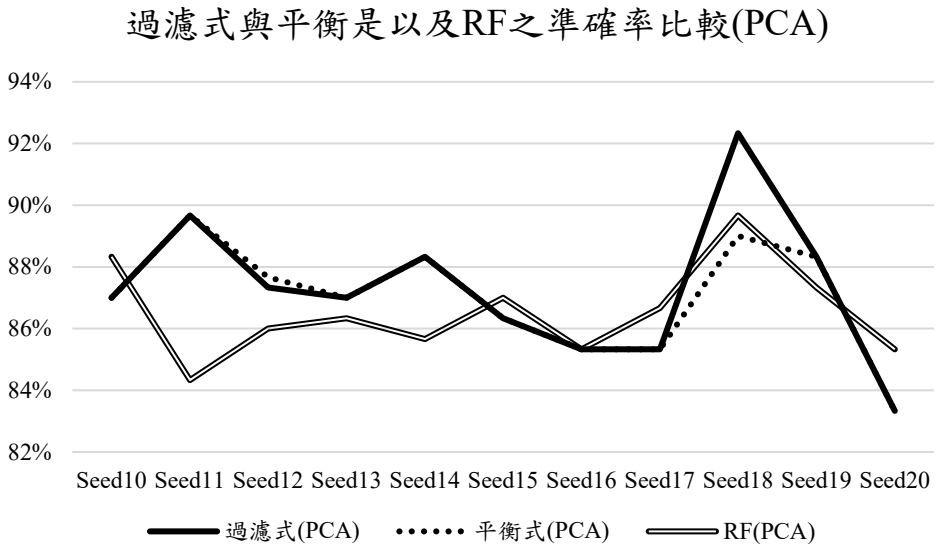


圖 4.4: 多階連續過濾及平衡過濾偵測流程與 Random Forest 之準確率比較(PCA)

連續過濾的優點除能獲得高偵測準確率外，更可在不同階段，提供不同的偵測精度。表 4.5 為使用連續過濾之各模型偵測結果，其中透過 M1 過濾出的正常者共有 120 位(118+2)，其中 118 位確實為 NF，精度高達 95.52%。換言之，若有待測帳號在此階段被判斷為 NF，則將具有很高的可信度。同樣地，M2 對詐騙者(F 類別)的偵測精度高達 95.59%，在此階段被判斷為詐騙地帳號，同樣具有很高的可信度。偵測精度隨著過濾步驟增加，漸漸下降，最後的平衡模型之 NF 精度僅剩 72.29%。縱使如此，流程之總體偵測準確率(Accuracy)仍高達 87.1%。綜合上述結果，明白顯示本研究提出方法與單一模型具有重大差異。同樣具有 87.1%之單一模型，當有帳號被判定為 F 或 NF 時，並無法對此結果提供可信度資料。若以訓練集塑模結果來斷定，其精度大多接近 100%，實無參考價值。但對於多模型連續過濾而言，卻可因待測帳號在哪一階段被偵測出來，斷定其偵測結果之可信度。

表 4.5 連續過濾偵測流程之各階段偵測精度

分類/模型	M1	M2	M3	M4	M5
NF(true)	118	0	108	0	60
F(true)	0	65	0	41	0
NF(false)	2	0	10	0	23
F(false)	0	3	0	19	1
NF_Prec	97.52%		91.52%		72.29%
F_Prec		95.59%		68.33	0%

第五章 結論與未來工作

近年來，電子商務已成為現代人生活得一部分，讓電子商務的交易金額年年攀升。在 2014 年，美國全年的網路線上零售總金額即已高達 2,940 億美元。發展至今，全球電子商務銷售額在 2017 年成長至 2.29 兆美元，更預計在 2021 年達到 4.8 兆美元(eMarketer, 2017)。隨著線上消費行為的普及，全球將真正進入數位經濟時代。面對如此龐大的交易金額，也引起不肖人士的覬覦，在電子商務平台中進行詐騙，其中又以線上拍賣詐騙為大宗。若不加以抑制，將不利於電子商務的長遠發展。有關線上拍賣詐騙偵測，已有許多方法已被提出，但對於日新月異的詐騙手法，其準確率仍有待提升。

為解決此問題，本研究提出一套過濾式模型融合方法，以提升線上拍賣詐騙偵測之準確性。首先，我們以線性回歸組合數種傳統的分類模型，以產生更有效的融合模型，並比較傳統單一分類模型與融合模型之間的差異。之後，根據各種模型對於正常者與詐騙者之偵測精度(Precision)差異，以多階連續過濾以及平衡過濾的方式產生另外兩種更加精確的融合模型。由於偵測屬性集與偵測效能息息相關，本研究也探討屬性篩選對於偵測準確率之影響。為驗證提出方法之有效性，本研究採用 Yahoo!奇摩實際交易資料進行實驗。實驗結果顯示，與四種單一偵測模型相比較，融合模型確實能提高偵測準確率。此外，結果亦顯示，使用 Principle Component Analysis 或 Wrapper 法進行屬性篩選，對本研究之實驗並無助於結果的改善。由上述結果可知，本研究提出方法確有助於改善詐騙偵測準確率，提供消費者更周全的購物安全防護機制。

本研究可能之未來工作如下: 雖然使用 37 種偵測屬性，但對於稀有詐騙類型仍有其瓶頸，因此若能發展新的詐騙屬性或者針對特定詐騙類型擁有特定偵測屬性，將有助於提升整體詐騙偵測準確率。有關此主題，可考慮使用 Convolutional Neural Network 來進行屬性轉換與縮減。其次，本研究均採用傳統如分類樹之學習模型，未來可嘗試使用深度學習慣用之 RNN 或 LSTM，驗證是否能進一步提升偵測準確性。最後，若能將發展之方法應用拍賣網站之實際交易流程中，將有助於管理當局早期發現詐騙情事，儘早進行監控，避免影響電子商務之健全發展。

參考文獻

[1] Alford M. (2013), "Intelligent fraud detection: a comparison of neural and Bayesian methods," Computer Fraud & Security, pp. 14-16

[2] J.-S. Chang, W.-H. Chang/Electronic Commerce Research and Applications 13 (2014) 79–97

[3] Chau, D.H., and Faloutsos,C. (2005). Fraud detection in electronic auction. European Web Mining Forum at ECML/PKDD

[4] Chau, D.H., Pandit,S., and Faloutsos,C. (2006). Detecting fraudulent personalities in networks of online auctioneers. Proceedings of PKDD 2006, pp.103-144.

[5] Chau, D.H., Pandit,S., Faloutsos,C., and Wang,S..:NetProbe:A fast and scalable system for fraud detection in online auction networks. Proceeding of the 16th International Conference on World Wide Web, pp. 201-210.(2007)

[6] Chen C., et al. (2013), "Web Media Semantic Concept Retrieval via Tag Removal and Model Fusion," ACM Trans. on Intelligent Systems and Technology, Vol. 4, No. 4, Sep. 2013.

[7] Chen, J., et al. (2015), "Big Data based fraud risk management at Alibaba," The Journal of Finance and Data Science 1 (2015) 1-10.

[8] eMarketer，Global Ecommerce Platforms 2017:A Country-by-Country Review of the Top Retail Ecommerce Sites(July 13,2017)，https://www.emarketer.com

[9] Huang, S., et al. (2015), "A Hybrid Multigroup Coclustering Recommendation Framework Based on Information Fusion," ACM Trans. on Intelligent Systems and Technology, Vol. 6, No. 2, Mar. 2015.

[10] Gavish, B., and Tucci, C. (2008), 'Reducing Internet Auction Fraud', Communications of the ACM, vo. 51, no. 5 , pp. 89-97.

[11] Goes, UP., Tu, Y. and Tung, A.,:Online Auctions Hidden Metrics, Communications of the ACM, vol.52, No.4, pp.147-149.(2009)

[12] Kim, K., Choi Y., and Park J. (2013), "Price fraud detection in online shopping malls using a finite mixture model," Electronic Commerce Research and Applications 12 (2013) 195-207.

[13] National White Collar Crime Center(NW3C). 2017 Internet Crime Report. Retrieved on Oct. 1, 2017, from Internet Crime Complaint Center: http://www.ic3.gov/media/annualreport/2017_IC3Report.pdf

[14] Mitchell,T. and McGraw-Hill, “Machine Learning”, 1997, pp.52-81

[15] Pandit, S. et al., (2007). Netprobe: a fast and scalable system for fraud detection in online auction networks. Proceedings of the 16th international conference on

World Wide Web (pp. 201-210). ACM.
[16] Tsang, S., et al. (2014), "SPAN: Finding collaborative frauds in online auctions" Knowledge-based systems 71 (2014) 389-408.
[17] Leo Breiman(2001), "Machine Learning",Volume 45,Issue 1,pp.5-32
[18] Miao Yufei & Zhang Xiaohong(2015), "Improvement and application of C4.5 decision tree algorithm",2015,51(13):255-258
[19] Guo Qiao-jin & Li Li-bim & Li Nig,"modified AdaBoost algorithm for imbalanced data classification",2008,44(21):217-221
[20] 詹佳憲、陳嘉平，「以多層感知器辨識情緒於國台客語資料庫」，The Association for Computational Linguistics and Chinese Language Processing, ROCLING 2016, pp. 10-21
[21] 劉祐宏，「線上拍賣詐騙偵測之屬性挑選與流程設計」，淡江大學資訊管理學系，碩士論文，民 101
[22] 洪儀玶，「具早期預警能力之線上拍賣詐騙偵測」，淡江大學資訊管理學系，碩士論文，民 96
[23] 鄭孝儒，「線上拍賣潛伏期詐騙者之有效偵測」，淡江大學資訊管理學系，碩士論文，民 100
[24] 梁賀翔，「一套線上拍賣詐騙即時偵測系統」，淡江大學資訊管理學系，碩士論文，民 99
[25] 林敬堯，「一套有效率的複合式線上拍賣詐騙偵測系統」，淡江大學資訊管理學系，碩士論文，民 103
[26] 謝金育，「結合貝氏網路與激勵理論之推薦機制-電影推薦系統設計」，碩士論文，民 102
[27] 內政部警政署，警政署統計室，警政統計通報(106 年 10 月 28 日)，取自 https://www.npa.gov.tw

附錄 A: 屬性篩選結果

表 A-1: Principal Component Analysis 篩選之 22 項屬性

得到正評的結標評平均時間	EndCloseToPos
正評比率	RatioOfPos
評價來自賣家的比例	RatioOfSToS
正評密度	DensityOfPos
負評比率	RatioOfNeg
買東西比率	RatioOfBuyingRate
平均買價	MeanBuying
平均賣價	MeanSelling
給評價者平均評價	GiveManRating
評價	Rating
買東西數	BuyingNumber
後 30 天平均買價	MeanBuyingLast30
前 30 天賣價標準差	StdSellingFirst30
買東西正評數	BuyingNumberOfPos
賣東西數	SellingNumber
賣東西正評數	SellingNumberOfPos
後 15 天平均買價	MeanBuyingLast15
前 30 天買價標準差	StdBuyingFirst30
後 30 天買價標準差	StdBuyingLast30
前 15 天賣價標準差	StdSellingFirst15
前 15 天買價標準差	StdBuyingFirst15
後 15 天買價標準差	StdBuyingLast15

表 A-2: Wrapper Subset Evaluation 篩選之 14 項屬性(隨機森林)

RatioOfSToS	評價來自賣家的比例
MeanBuyingLast15	後 15 天平均買價
StdBuyingLast15	後 15 天買價標準差
StdSellingFirst30	前 30 天賣價標準差
MeanSelling	平均賣價
SellingNumberOfPos	賣東西正評數
SellingNumberLast30	後 30 天賣東西數
SellingNegtiveNumberLast30	後 30 天賣東西負評數

MeanSellingLast15-MeanSellingLast30	後 15 天平均賣價-過去 30 天平均賣價
StdSellingLast15-StdSelling	後 15 天賣價標準差-賣價標準差
StdSellingLast30-StdSelling	後 30 天賣價標準差-賣價標準差
StdSellingLast15-StdSellingLast30	後 15 天賣價標準差-過去 30 天賣價標準差
SellingLast30MeanTimeInterval	後 30 天平均交易時間間隔
MAXSellingPrice	最大賣價

表 A-3: Wrapper Subset Evaluation 篩選之 8 項屬性(J48)

MeanBuyingLast15	後 15 天平均買價
StdBuyingLast30	後 30 天買價標準差
StdSellingFirst15	前 15 天賣價標準差
MeanSelling	平均賣價
Rating	正評百分比
BuyingNumberOfPos	買東西正評數
SellingNumberOfPos	賣東西正評數
SellingMeanTimeInterval	平均交易時間間隔

表 A-4: Wrapper Subset Evaluation 篩選之 12 項屬性(多層感知器)

DensityOfPos	正評密度
EndCloseToPos	得到正評的結標評平均時間
RatioOfPos	正評比率
RatioOfSToS	評價來自賣家的比例
StdSellingFirst15	前 15 天賣價標準差
SellingNumber	賣東西數
SellingNumberLast30	後 30 天賣東西數
SellingNegtiveNumberLast30	後 30 天賣東西負評數
StdSellingLast15-StdSelling	後 15 天賣價標準差-賣價標準差
StdSellingLast30-StdSelling	後 30 天賣價標準差-賣價標準差
SellingLast15MeanTimeInterval	後 15 天平均交易時間間隔
SellingLast30MeanTimeInterval	後 30 天平均交易時間間隔

表 A-5: Wrapper Subset Evaluation 篩選之 3 項屬性(貝氏網路)

RatioOfSToS	評價來自賣家的比例
MeanBuyingLast15	後 15 天平均買價
SellingNumber	賣東西數