國防管理學報

第四十五卷　第一期

JOURNAL OF NATIONAL DEFENSE MANAGEMENT

Volume 45, No. 1

副總編輯：劉興漢　國防大學管理學院資訊管理學系
臺北市北投區中央北路 2 段 70 號
(02)23116117#604410
liu.hansh@gmail.com

副總編輯：林杰彬　國防大學管理學院資訊管理學系
臺北市北投區中央北路 2 段 70 號
(02)23116117#604976
cplin.ndu@gmail.com

編輯助理：陳正忠　國防大學管理學院教學支援中心
臺北市北投區中央北路 2 段 70 號
(02)28948714
journalofndm@gmail.com

【發行宗旨】

為因應學術期刊專業化導向之發展趨勢，並提升學術界對「國防管理」專業學術領域之認定與重視，形成專業特色與重點，樹立「國防管理」專業學術權威，並配合國防管理教育訓練與研究發展需要，提升國軍學術水準與研究風氣，增進軍事院校與民間院校及研究機構學術交流，以「國防管理」相關議題為範疇，對外公開徵稿與發行。

國防管理學報第 45 卷第 1 期「編輯的話」

本人於今(2024)年受發行人的委任，擔任《國防管理學報》的新任總編輯，接任之初深感任重道遠，期許能夠延續前人的編輯智慧，彙整領域專家及學者們的見解立論，提供國防及軍事管理在人力、財務、運籌、資訊、決策、法律等領域的專業研究與實務案例，以期出版具品質且專業的學術論文。因此，本人很榮幸邀請劉興漢及林杰彬兩位老師擔任學報副編輯，期望新團隊能夠在共同的努力下，協同維持學報的品質與推展學報的創新，以利學報持續的成長與精進。

一、本期刊出之論文

本次的順利出刊感謝前任的總編輯及所有編輯團隊的超前部署，在去(2023)年的編審會議中完成年度出刊文章的審定作業，感謝所有編審團隊的辛勞，本人致上深深的感激之意。本期共計刊出四篇文章。

第一篇〈*國軍油料補給點前支能力探討-以陸航航空燃油需求為例*〉一文，作者以從事油料彈補業務之經驗為基礎，透過產、官、學等面向的整合，蒐集包括官方文件、美軍報告、國際學術期刊、軍事幕僚運用研究論文、報章雜誌及網路資源等資料進行文獻分析；同時以供應鏈概念探討人力不變的原則下，建構國軍油料補給單位與航空燃油裝備能量協同發展的最佳作業模式，以提供各級長官參考運用，並協助油料部隊建立符合國軍戰備演訓基本能力。

第二篇〈*植基於邊緣偵測及最佳像素調整之資訊隱藏方法*〉一文，作者認為現代戰爭將以資訊戰、不對稱作戰模式為主，故在情報資訊的傳遞中，除快速、準確外，亦應提供情資隱匿或偽裝的方法，以達國防作戰資訊安全管理之效。該篇文章提出植基於邊緣偵測及最佳像素調整之資訊隱藏技術，達到高藏密量且不失真的資訊隱藏方式，且能避免以統計分析技術為基礎的影像偵測攻擊。同時透過與多位學者研究之間的效益評估比較，驗證作者提出演算機制的優勢。

第三篇〈*基於區塊鏈技術建構多銀行數位交易機制之芻議*〉一文，作者運用區塊鏈技術結合智能合約與密碼學原理，設計一個具安全性數位交易支付機制，並嘗試導入多銀行數位交易支付流程，以解決目前電子商務在跨銀行及第三方支付中可能存在的安全性與信任問題，以提升消費者對於電子支付之信心。因該機制具有的安全特性，作者建議可導入於國軍福利站、國軍副食供應中心、國軍服裝供售站等各項商品採購作業中，以提供多元安全之電子支付機制。

第四篇〈*視訊與現場面談情況下應徵者專業及外表吸引力對面試官評分的交互作用影響*〉一文，作者認為具備勝任能力與特質的優秀人力資源是組織競爭優勢的重

要來源，故組織甄選作業的有效性攸關組織績效甚鉅。該研究以類實驗設計方式，探討在視訊與現場面談的不同情境下，應徵者專業能力及外表吸引力對面試官給予應徵者評分的交互作用影響。研究成果除驗證注意力容量理論的觀點外，也補足過去文獻有關視訊面談與現場面談比較的實證缺口。相關成果可以提供國軍在人才招募、考績評鑑、派職任用等各項需要以面談方式進行人力徵選時使用。

二、未來展望

近年由於地緣政治的緊張，許多國家因為不同的原因而爆發出各面向的衝突事件。因此，對於國防戰略規劃、作戰決策、後勤運籌、科技運用、資通威脅及國際法制等各項議題都突顯出其重要性；特別是新興議題對於國防管理面向的威脅與挑戰，將是學報未來持續邀(徵)稿件的重點方向。例如：低軌衛星與無人機在戰爭衝突中對於通訊支援及後勤補給的規劃運用方式、生成式 AI 在國防管理及部隊業務上的威脅或創新、灰色地帶衝突引起的法制規範及現場決策作為等，均是研究人員在快速變化的環境中需要積極探索的國防管理議題。此外，少子化的趨勢對於國軍維持備戰員額也是充滿挑戰，對於軍事人才斷層及國防維持缺口等問題，造成了嚴重的威脅。因此，人力資源及運用的重新規劃、人才招募及培育的創新機制、國防教育與訓練的彈性設計、新興科技於部隊的整合運用等議題，也都是需要持續投入研究的重要方向。

《國防管理學報》有今日的成績，都是歷屆總編輯、副編輯、期刊編輯委員、論文審查委員、行政助理及所有投稿作者的共同參與，在此深深感謝大家的付出。未來冀望學報能夠兼顧學術與實務雙重面向，來連結產業及國防應用的發展趨勢，同時能夠創造出新興議題對於國防管理面向的重要支持。希望大家能夠持續灌溉這個屬於國防管理學界的交流平台，所有作者的來稿就是對我們最大的鼓勵與認同，而所有關注國防管理議題的軍民讀者群的支持與回饋，也是支持學報持續茁壯發展的重要力量，期待未來與大家的互動激盪出學術的火花。

總編輯 陳良駒
國防大學管理學院資訊管理學系 專任教授
113 年 5 月

國防管理學報

第四十五卷　第一期

目　錄

中華民國一一三年五月

國軍油料補給點前支能力探討-以陸航航空燃油需求為例

彭天宏[1]　張林安[2*]

[1] 國防大學管理學院國防管理教育訓練中心

[2] 國防大學管理學院國防管理戰略班

論文編號：NM-43-02-02
DOI：10.29496/JNDM.202405_45(1).0001
來稿2022年4月8日→**第一次修訂**2022年5月16日→**第二次修訂**2023年1月16日→
同意刊登 2023 年 4 月 10 日

摘要

有鑑於陸軍航空部隊 AH-64E、UH-60M 直升機的成軍及未來主戰部隊新式武器裝備的持續獲得，後勤部隊油料補給主要裝備油罐車建案遭受排擠十餘年未能籌獲，亟須結合主戰部隊油料需求，補強國軍油料整補能力，基此，本研究藉探討美軍前方油彈補給點現役加油裝備、多領域作戰後勤支援關鍵能力及國軍油料補給點前支能力現況等產官學文獻分析，獲得優先籌補 M978 油罐車、妥適運用 AAFARS 及擴大徵用航空燃油油罐車等結論，以強化陸航部隊油料整補能力。

關鍵詞：油料補給點、前支點、前方油彈補給點

* 聯絡作者：張林安 email: rock520jojo@gmail.com

On the Frontline Support Capability of the National Army Fuel Supply Points-Take the Air Fuel Requirement of Army Aviation as an Example

Peng, Tien-Hung[1]　**Chang, Lin-An**[2*]

[1] **National Defense Management Education and Training Center, Management College, National Defense University,** ***Taiwan, R.O.C.***

[2] **National Defense Management Strategy Class, Management College, National Defense University,** ***Taiwan, R.O.C.***

Abstract

So far, Taiwan Army aviation troops have received AH-64Es and UH-60Ms. In future, major operational troops will acquire more new weapons and equipment. In order to acquire new fuel tanker truckers which can support warfighters to fight, logistics troops have built cases for budget. However, those cases haven't been approved yet. In fact, it's urgent to integrate various requirements from major operational troops and to improve Armed Forces' fuel supply capability. After reviewing literatures about the current measures of U.S. fuel & munition supply, U.S. critical logistic support capabilities on multi-domain operations and the military fuel servicing capability in Taiwan, this research reaches a conclusion that Army aviation troops' fuel servicing capability can be reinforced through some methods which are putting M978 fuel tanker trucks acquisition on higher priority, utilizing Advanced Aviation Forward Area Refueling System (AAFARS) and expanding the requisition toward civil aeronautical fuel tanker trucks.

Keywords: Fuel Supply Point, Forward Supply Point, Forward Arming and Refueling Point

[*] Corresponding Author: Chang, Lin-An email: rock520jojo@gmail.com

一、前言

作者曾服務於陸軍航空旅油彈補給連，連隊傳承著「飛機沒有彈，只是會飛的鐵；沒有油，就是不會動的鐵」原則與精神，彰顯航空旅油料與彈藥補給的重要性，藉以訓勉全連持續戮力與精進油彈整補作為，俾肆應各種作戰後勤補給需求；續於各地區補給油料庫從事地區油料補給任務，支援著陸、海、空三軍部隊各式裝備各類油料補給作業(國防部後次室，2019)，掌握地區後勤資源分配能量，深感適時適地適量滿足部隊戰備演訓油料需求，為油料補給幹部的重中之重。

經上述航空旅部隊後勤及補給油料庫地區補給的基層歷練，作者發現各級油料部隊油料裝備建軍整備，僅航空旅於 2010 年接裝美軍先進航空前方地區加油系統 AAFARS (Advanced Aviation Forward Area Refueling System)三套，餘單位油料裝備均未獲得新品或新裝，造成各級油料部隊整補能力原地踏步；因此，藉航空旅 2018 年及 2019 年阿帕契及黑鷹直升機全戰力成軍後，主戰載具世代交替背景下，油料部隊面臨打擊部隊各種新式裝備持續接裝與汰換，部隊油料需求逐次加大之挑戰，油料部隊如何因勢制宜滿足部隊油料需求，為當前建軍備戰的重大要務。另就各油料部隊現行油料裝備編現率及妥善率(可靠度)問題而言，單位間緊急調借油料裝備支援戰演訓任務情況，徒增油料部隊裝備挪用困擾與任務執行窒礙，油料裝備建軍整備刻不容緩。

作者以充實油料部隊合宜裝備為著眼，發現油料部隊文獻多以戰術戰法運用為主要著墨，未見檢討油料裝備基本實務之文獻，基此，本研究探討地區補給(油料分庫)與部隊後勤(航空旅油彈連)油料裝備能量與發展，提供各級長官參考運用，並協助油料部隊建立符合國軍戰備演訓基本能力，期達成本研究目的，研析各階層油料補給單位現在優劣與未來建軍發展方向。

二、文獻探討

2.1 供應鏈管理

供應鏈及物流管理的概念演進，可源起於西元 1950 年代開始，當時的物流名詞原為「後勤補給」(Logistics)之意，主要用於軍隊對前線戰士作戰或備戰時，提供物資運輸與軍備支援供應之相關後勤作業；然而當時企業中並無「物流」或「後勤補給」的稱謂，僅以行銷、製造、倉儲、會計…等功能區分的方式，來界定部門及人員之工作歸屬。

就企業而言「供應鏈」與「供應鏈管理」定義是完全不同。Handfield and Nichols (1999)針對供應鏈的定義(SC)是「許多實體程序的結合，由一連串企業產銷價值鏈與交易行為所編織構成，而在不同的產業結構與市場競爭下，不同的企業也可能串連起許多不同的 SC 運作體系」(Dornier, 1998)。然而相比 SC 實體程序的辦法，供應鏈管理(Supply Chain Management, SCM)是「著重於強調 SC 成員相互關係發展與企業互動程序整合，以達到同業競爭的優勢能力 ex：企業聯盟合作的同步化(Scott, 1999)。SCM 不僅僅只是產銷供貨合作與企業聯盟策略，更是深化合作與提升信任的改善作法，促使 SCM 合作程序進一步合理化、彈性化，以換取產業競爭環境下無可取代的合作優勢(Dornier, 1998; Collins, 1999)。

Douncan and Cayway(1996)指出供應鏈管理運作時，若組織內部沒有完善的整合與協調，會使其組織運作不順暢而無法達到預期的績效。因此組織內的個人、部門，甚至每個組織有其工作運行或管理的規則。執行供應鏈管理活動時，組織內部的整合佔有決定性的影響 Vickery et al.(2003)認為供應鏈整合應包括企業內部及企業間的整合，因為外部成員及公司內部功能應被視為供應鏈的一部分，主要分為上游(供應商)整合、內部(跨功能)整合及下游(客戶)整合。

Thomas and Griffin(1996)認為供應鏈管理是供應商、製造商、組裝工廠與物流中心間之物料流與資訊流的管理。Poirier and Reiter(1996)提出通路的成員須延申至供應商(及其供應商)和客戶(及其客戶)，並整合組織的設計、行銷、採購、配銷等活動。由此可以看出供應鏈的管理從每一家公司為出發點，都可以列出相同的前後對應架構，每一家供應鏈中的公司都可視為獨立之個體。

Simchi(2001)則認為供應鏈管理是運用有效率的方式，整合供應商、製造商、倉儲、銷售通路及顧客間，使商品能在對的時間以對的數量配送到對的地點，在達到令人滿意的服務品質，亦能同時使整體系統之成本最小化。且現代企業管理中最重要的是企業間競爭不同是單獨一家企業，而是供應鏈在競爭(Lambert and Cooper, 2000)。供應鏈管理係針對整個供應鏈系統全面進行計畫、操作、控制、協調與優化的各種活動及過程，主要目標係將顧客要求的正確產品(Right Product)能在正確時間(Right Time)、按正確數量(Right Quantity)、有正確質量(Right Quality)和正確狀態(Right Status)等目標下，送到正確地點(Right Place)，並讓系統總成本最小。

Jack Neele(2021)認為「最後一哩路」的宅配服務為何如此重要？宅配為貨品運送過程最後的步驟，係貨物送達最終顧客的住家或取貨點。所以最後一哩路的配送服務對提高顧客滿意度是非常重要的。可是宅配作業耗時且成本高昂，佔運輸成本 53%，約佔供應鏈總成本 41%。

2.2 油料供應商

台灣中油股份有限公司為我國油品主要生產製造廠商，由於國內自產原油極少，台灣中油公司煉製之原油幾乎全數仰賴進口。2020 年進口原油總量達 12,840 萬桶，其中中東原油約占 50.39%，美國約占 41.33%，非洲約占 8.28%，如圖 1。為進口油料，在

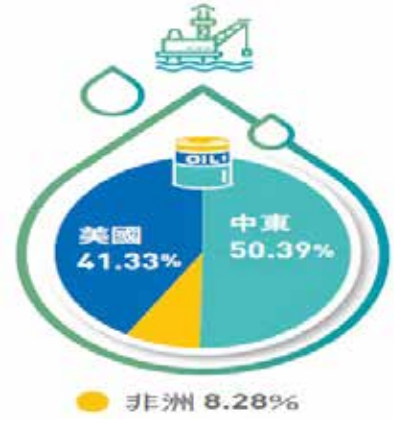


圖 1　中油進口原油比例

資料來源：2021 台灣中油業務簡介

桃園沙崙及高雄大林蒲外海設有卸泊大型油輪的浮筒，並在高雄、台中及深澳港設有油輪專用碼頭。並由桃園(20 萬桶)及大林(40 萬桶)煉油廠，日煉 60 萬桶原油。 2020 年油品產量總計汽油 8,256 千公秉、航空燃油 1,715 千公秉、柴油 5,558 千公秉、燃料油 2,245 千公秉、液化石油氣 367 千公噸。

車用汽油、柴油、燃料油及航空燃油為台灣中油公司於國內油品銷售之大宗。2020 年，國內油品總銷量 16,982 千公秉，以車用汽油占銷貨收入比例最大(約 58.1%)，其次為柴油(約 26.0%)，再其次為燃料油(約 10.1%)以及航空燃油(約 5.8%)。台灣油品市場，由台灣中油與台塑二強供應，台灣中油汽油、柴油、燃料油及航空燃油市場銷量占有率分別達到 79.5%、77.4%、94.9%及 63.6%，總市占率為 78.9%。

在儲運方面，為滿足台灣各地用油需求，除自營加油站之外，在松山、桃園、高雄、台中、花蓮、台東、金門及澎湖等主要機場設有航空加油站；並在基隆、蘇澳、台中、高雄及花蓮等國際商港設有海運加油站。截至 2020 年底止，計有基隆、石門、新竹、台中、臺中港、王田、民雄、台南、豐德、橋頭、蘇澳、花蓮及湖西、金馬行銷中心(供油中心部分)等 14 座供油中心，負責供應各地加油站所需油料，全年發油量共計 19,826 千公秉。台灣中油公司每天大概有 500 部油罐車在全台執行油品配送，平均每日行駛里程 11 萬公里，每部油罐車行駛 220 公里，就石門供油中心而言油罐車 115 部，每日配送車輛約 63 部 行駛 1 萬 3,860 公里。設有基隆、台中、高雄 3 處化驗中心及 6 處化驗室，負責油料化驗及品質控制。 另台灣中油公司執行代儲政府儲油 156 萬 KL，其中航空燃油 10 萬 KL。

綜上，2020 年台灣中油公司自中東、美國及非洲進口原油 12,840 萬桶，分於桃園及高雄接收原油並提煉各式油品 33,574 千公秉，其中航空燃油 1,715 千公秉，透過各地供油中心地下油料管線或管制油罐車配送至各地區油料分庫，另配合演訓任務驗證直供受補單位油彈連。

2.3 油料補給點

2.3.1 任務與編組

陸軍各補給油料庫、油料分庫為補給階層，戰時依作戰命令，開設油料機動補給點。野戰油料補給支援係以滿足三軍用兵需求為目的，為有效達成後勤支援任務，依前支作業標準程序與行動準據，針對支援區之幅員及對狀況開設油料補給勤務設施，整合軍、民能量，執行前支補給支援任務。

平時陸軍後勤指揮部轄地支部，依作戰區分於現駐地開設油料補給後勤設施，遂行三軍通用油料前支任務，戰時各地支部運用既有設施，實施油料支援外並依作戰區固安作戰計畫及作戰需求，開設野戰油料勤務設施支援部隊作戰。

依據「濱海決勝、灘岸殲敵」與「不分階段、立即作戰」的戰略指導，前支點作業納入作戰區年度演習驗證項目，油料整備採「前推預置」及「分區屯儲」原則，配合作戰部隊進入戰術位置，即補給 1/3 戰耗量，以提升整補時效，後續戰耗量(第 2 個 1/3)以「連」為單位完成戰備包裝，並結合作戰區既有戰車堡、掩體、庫房等堅固設施預置分屯，俾達「分散風險」、「就近支援」、「縮短整補時效」等目的，以符戰場實需。

「油料前進支援點」(以下簡稱：油料前支點)為綿密作戰部隊與後方龐大供應網路

之關鍵節點(Key Node)，選址決策對於作戰油料輸補具有重大影響，不僅關係到油料供補是否順遂，更影響主戰部隊作戰全程及勝負關鍵，經地區油料分庫現地踏勘並依後勤設施開設要領，選定營區等 10 處交通便利且條件符合之地點，規劃為戰時油料前支點，以滿足作戰區 19 個連級單位 12 處輜重開設需求，續於年度演習驗證。惟經實況驗證，每處油料前支點作業人力須 5 員(1 員帶班幹部，4 員作業手)，惟作戰區油料分庫陸用油料編制人員僅 21 員，作業能量不足開設 10 處以上之上級指導。經研究結論指出前支點 1 至 10 處，在油料分庫不同開設能力取捨方案，以開設 7 個前支點為最適方案；另現行油料配送路線因高科技武器大量投入使用，配送方式是複雜的網路結構，因應大規模聯合作戰動態環境下，更應研析有效支撐主戰部隊戰鬥持續力之油料配送模式，使可周全完備。

2.3.2 開設指導與原則

支援區運用既有堅固建築開設勤務設施，並依「地區後勤、聯合供補」之指導及考量運補經濟效益，以達「就近支援、就地提領、主動運補」之地區支援要求。設施開設原則如次：

1.運用所屬分庫現有庫儲設施開設三類補給點，並採「預置分屯、前進支援」方式開設，以滿足第一線部隊需求。

2.完成現有補給機(裝)具檢整、油料設施搶修等作業，以迅速恢復補給勤務設施作業能量。

3.設施仍應有主補給路線及預備主補給路線，以保持運補彈性支援作戰，確保補給支援遂行。

4.應於主戰部隊預定補給地區，預先屯儲軍品並實施主動運補，同步全盤掌握補給資訊，以利執行整補作業。在得知預定補給位置後，配合主戰部隊先行預屯各類補給品項量。地區補給油料庫針對軍、民運輸能量應有效運用，適時、適量、適地的運送主戰部隊所需補給軍品，以利作戰任務之遂行。

5.打擊部隊戰鬥間各營、獨立連可在預設之整補位置適宜空投及著陸場開設之油料補給點(前支點)實施整補。

6.對守備旅須於其前進軸線上選擇適當位置，預屯補給品項，使其補給不虞匱乏，同時地區補給庫對守備部隊後續補給須掌握戰況，主動對守備部隊實施運補。

7.戰備分屯各類補給品，於淺山地區分屯混儲時，應依第一線部隊部署，同步完成戰備包裝，預置分屯，以應戰時持續補給。

2.3.3 野戰供補模式

依前述開設指導與原則，我軍之油料供補模式敘述如下：

1.油料供補須保持高度之韌性，設施及補給品採縱深配置與分區屯儲，以增加支援彈性；另油料供補設施應注意疏散、掩蔽與損害管制，以保持作戰持續力。

2.油料部隊結合各現駐地或民間設施開設油料補給點，運用現有支援能量，以建制輸具或運用動員之油罐車等，採主動運補方式實施供補作業，直送至營，滿足作戰需求。亦可運用地區內合約商之直營加油站，以補給點分配法，對受支援單位輪型車輛實施供補作業。

3.當油料供補係以桶裝油料運送、油罐車對車灌補或實車換空車等作為時，應採穿梭運輸方式對受支援單位實施供補作業；另受支援單位於營輜重地區，以油罐車優先對機甲車輛實施油料供補作業。

4.若我軍對敵攻擊時，油料之供補模式係應於集結地區完成一切補給支援準備，供補作業須採統一管制集中運用。油料補給勤務設施需向前配置，惟應於敵砲兵射程外，並隨我軍攻擊進展，適切變換位置，密切補給支援攻擊部隊作戰。

5.接敵運動與擴張戰果時，則應特別加強油料供補作為；當採迂迴攻擊時，則應對迂迴部隊適時、適地追補油料，並可妥適運用陸航實施空中運補。

綜上，油料前支點係運用建制輸具(中型戰術輪車、油罐車)或動員油罐車，以桶裝運送、油罐車對車灌補或實車換空車等方式主動運補至營輜重支援機甲(主戰裝備)車輛為主，或運用合約加油站，以補給點分配法支援輪型車輛為主。另開設 7 個前支點為最適油料輸補方案，油料輸補具對於前支點配送網路與主戰部隊作戰持續力具有關鍵影響。

2.4 FARP 前進油彈補給點

2.4.1 運用原則

Forward Arming and Refuelling Point(FARP，如圖 2)前方油彈補給點是美軍一種組織、裝備和部署在最前線或通用的臨時設施，在戰術上可提供作戰中的航空部隊維持所需的燃料和彈藥。建立 FARP 讓指揮官擴大飛機的航程並減少飛機返回基地整補油彈的必要，可顯著增加在空執行任務的時間。因此 FARP 為航空部隊執行作戰任務的必備能力，並視需求提供空中交通管制(ATC)服務。當航空部隊快速前推，地面機動能力無法及時建立 FARP 時，可透過空中機動完成部署，主要透過先進航空前方區域加油系統(AAFARS)、500 加侖油囊、彈藥(當任務要求時)實施空中機動建立 FARP。

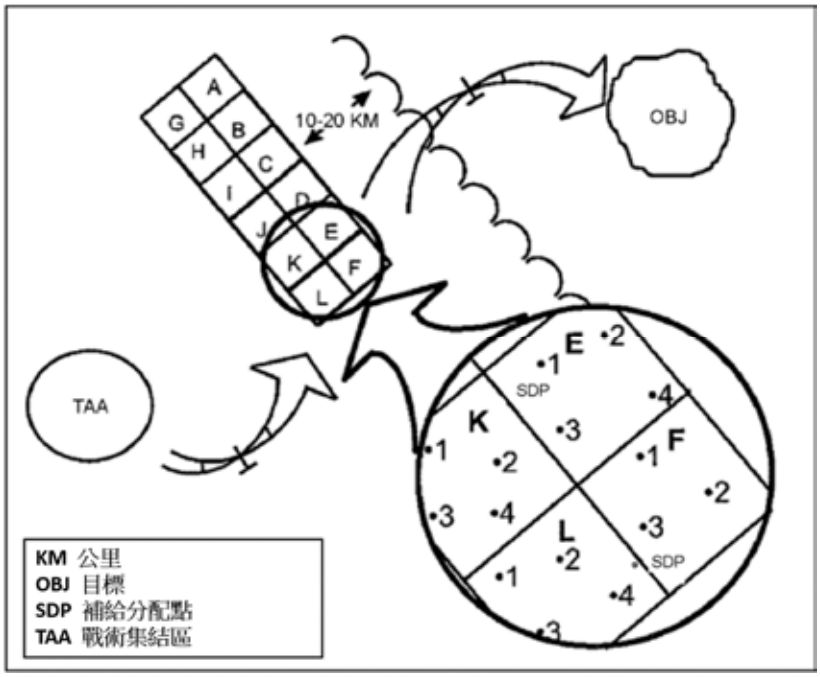


圖 2　FARP 油彈補給點配置範例

資料來源：Techniques for Forward Arming and Refueling Points, ATP 3-04.17

FARP 作業場地的轉移指導方針計有：

1.根據定義，FARP 應該是臨時的，不要在任何地方停留超過三到六個小時(除非確認已位於安全的區域，例如後方基地)。

2.當威脅程度快速變化或當區域威脅確認時，FARP 必須經常移動，位置選定採取備多用少，視敵情調整設置 FARP 場地，如圖 2 配置 A 至 L12 處 FARP，僅使用 E、F、K、L 等 4 處。

3.在安全情況下，FARP 的頻繁移動可能沒有必要。

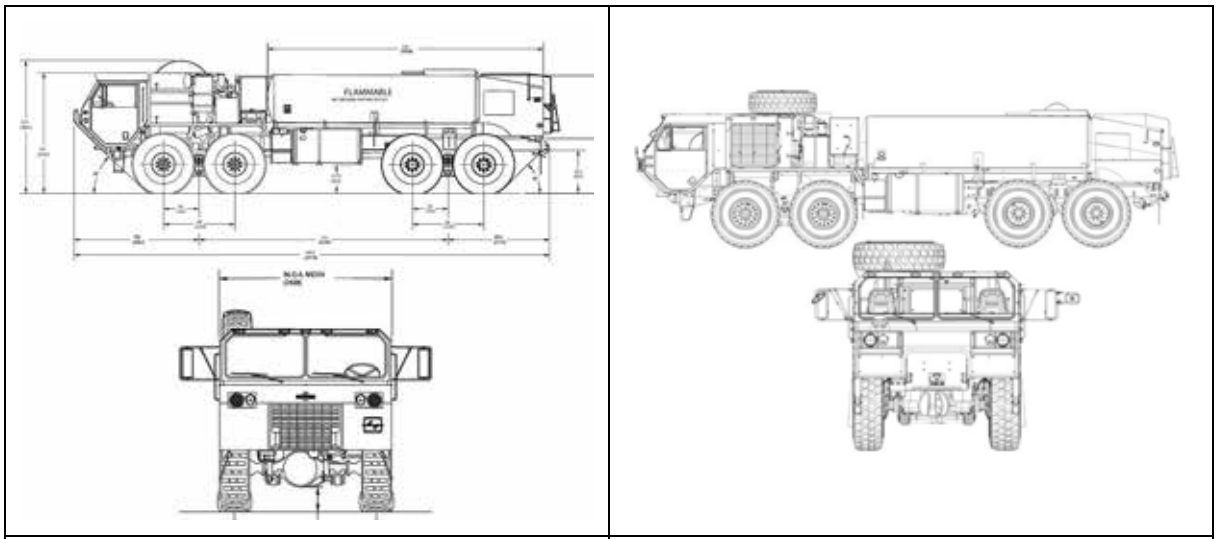
4.在確認敵我空優概等或敵方空中優勢的情況下，FARP 必須經常移動。這只有在滿足任務飛機的補給要求後才能移動 FARP。

2.4.2 加油設備

FARP 可運用的加油設備主要區分為 M978 油罐車、AAFARS 先進航空前方區域加油系統及 HTARS 重型擴展機動戰術加油系統，分述如次：

2.4.2.1 M978 油罐車

M978 油罐車係為美國奧什科甚公司(Oshkosh Defense)製造之 HEMTT 重型擴展機動戰術卡車系列，設計酬載 2,500 加侖油料運輸到 FARP，無論是為地面車輛或飛機加油，M978 油罐車具備八輪越野機動能力，車輛使用柴油油箱 155 加侖可行駛 483 公里，最高速度 100 公里/小時，涉水高度達 1,219 公厘，提供後勤人員可靠的油料運補及一對二加油作業能力；加油系統主要包括每分鐘 300 加侖(GPM)泵浦、標準油水分離器、兩側 50 呎油管、開放式與密閉式油槍。最新 M978 油罐車 A4 構型(圖 3)，改善引擎散熱系統並增加 55 馬力達 500 馬力及加裝駕駛室模組化防護裝甲，提供後勤人員安全操作環境。



A2 構型	A4 構型

圖 3　HEMTT 重型擴展機動戰術卡車 M978 油罐車

資料來源：https://www.oshkoshcorp.com

2.4.2.2 AAFARS 先進航空前方區域加油系統

AAFARS 是一種機動式加油系統，如圖 4，主要組件包括每分鐘 220 加侖(GPM)的柴油發動機泵、標準油水分離器、輕型軟式油管和密閉式油槍。

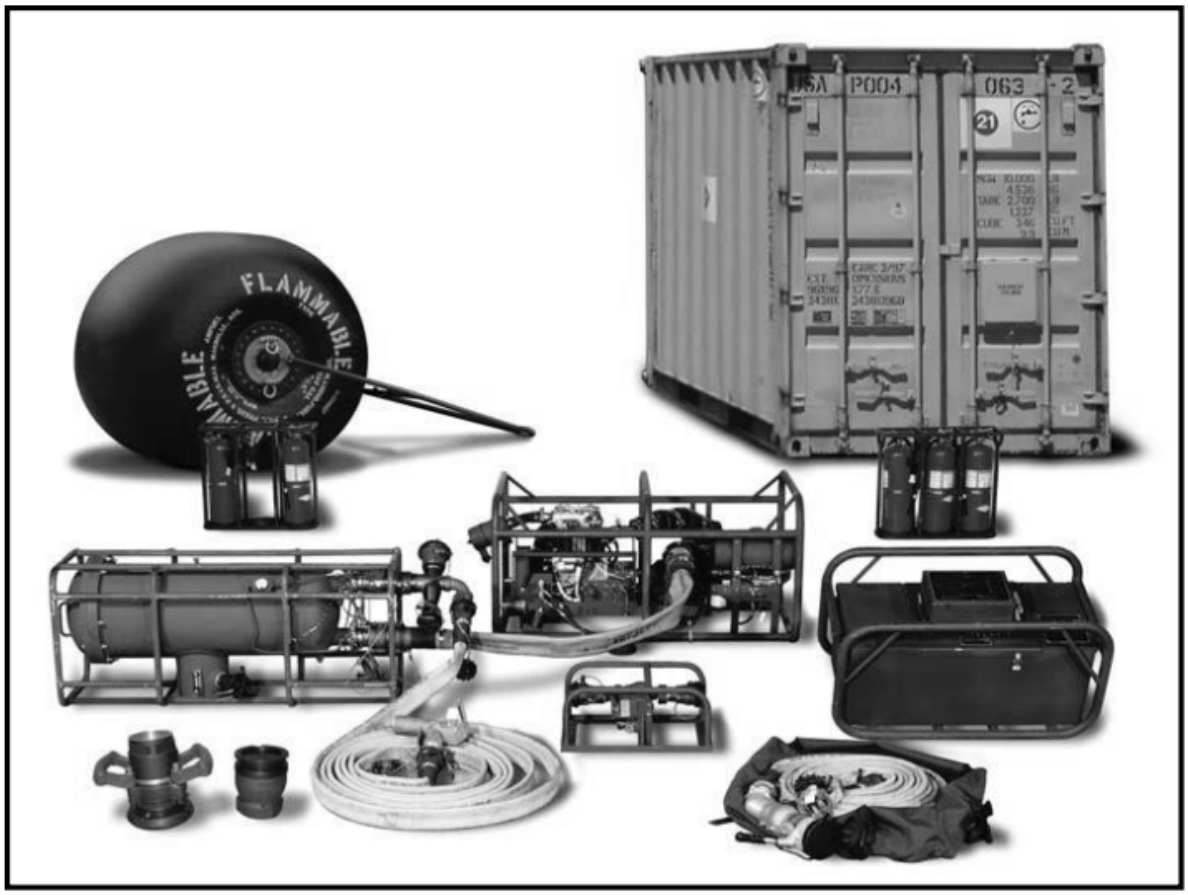


圖 4　AAFARS 先進航空前方區域加油系統

資料來源：Techniques for Forward Arming and Refueling Points, ATP 3-04.17

AAFARS 具備同時一對四加油能力(視機種使用 D1、CCR 密閉油槍或開放式油槍)如圖 5，在每個加油點提供至少 55 GPM，每個加油點間須有 100 英尺的安全距離，主要燃料來源是 500 加侖的可折疊桶。AAFARS 為美軍與與北大西洋公約組織等多國現役加油裝備。

AAFARS 加油系統的設置應利用地形特徵，從而實現最大分散和避障。在規劃 AAFARS 系統的佈局時，人員必須考慮加油期間飛機之間所需的最小間距，間距取決於飛機類型及其旋翼尺寸，兩倍旋翼長度是標準間距。另加油系統開設須注意風向，使直升機能夠按照風向著陸、加油和起飛。

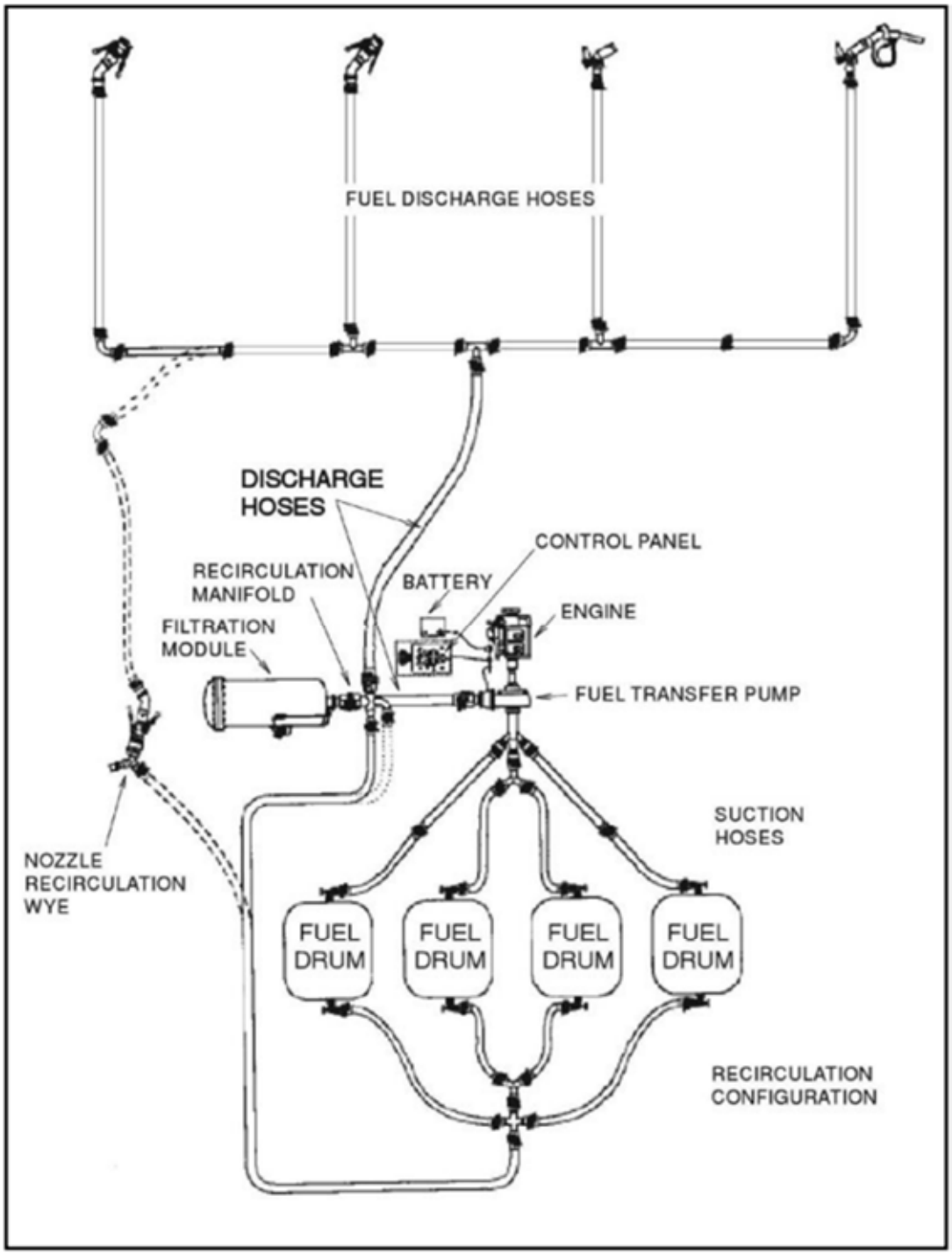


圖 5　AAFARS 先進航空前方區域加油系統開設

資料來源：Techniques for Forward Arming and Refueling Points, ATP 3-04.17

2.4.2.3 HTARS 重型擴展機動戰術加油系統

HTARS 重型擴展機動戰術加油系統是一個專用裝備，包括輸油軟管、接頭、各式油槍和配件來擴充 M978 油罐車的熱加油(或快速加油)能力，使 M978 油罐車具備同時一對四加油能力，HTARS 設備優點為重量輕，具有手動控制功能，並配備閥門和各式加油接頭(油槍)，詳如圖 6。

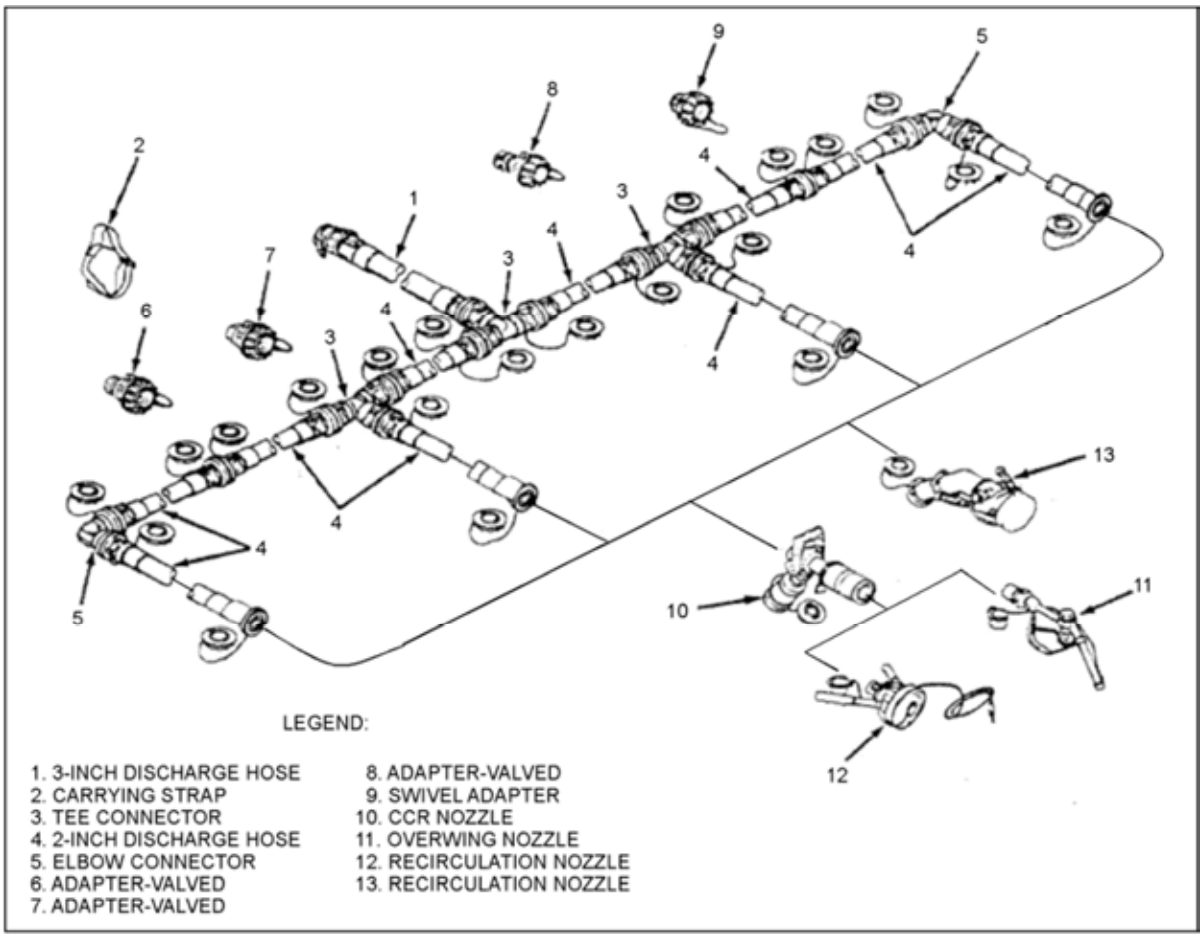


圖 6　HTARS 重型擴展機動戰術加油系統開設

資料來源：Techniques for Forward Arming and Refueling Points, ATP 3-04.17

綜上，FARP 通常以地面車輛運載大量油料與彈藥的進行部署為主要手段。M978 油罐車可攜帶 2,500 加侖油料，可透過兩輛 M978 油罐車與兩套 HTARS 或兩套 AAFARS 組合運用時，該 FARP 可以同時進行八點加油作業。惟單一加油點執行加油作業時需要三個人：第一個操作油槍，第二個操作緊急燃油控制閥，第三人站在飛機飛行員和加油泵浦操作員都可見的地方，負責安全維護。這第三人可由 FARP 或其中一名飛機機組成員。

FARP 加油作業可以在飛機發動機運行(熱或快速加油)的情況下完成，即飛機發動機僅關閉輔助動力裝置執行熱加油作業或關閉發動機冷加油作業。 在一個野戰環境下，機組通常會採用「熱」加油方式。 熱加油作業須運用 CCR 或 D-1 油槍執行各機種燃油補給作業。

2.5 小結

供應商臺灣中油公司地區供油中心、補給單位地區油料分庫油料補給點與受補單位油彈連前進油彈補給點，分為現行國軍航空燃油 JP-8 上、中、下流供應鏈執行單位(如圖 7)，分別運用中油油罐車、M978 油罐車及 AAFARS 等編制裝備對所屬客戶實施油料

供補作業，相關航油作業能量大小與能力強弱，受制於油料裝備編現率而產生先天上的限制，續納本研究前支能力探討與建議。

圖 7　國軍航空燃油 JP-8 供應鏈

三、研究方法

文獻分析係透過文獻之蒐集、分析、歸納、研究而提取所需資料，並針對文獻作客觀且有系統的描述之研究方法。文獻分析運用方法注重客觀、系統與量化的研究方法；在範圍上，不僅分析文獻內容，並研析整個文獻之學術傳播過程；在價值上，不僅針對文獻內容作敘述性解說，並推論文獻內容對整個學術傳播過程之影響(胡龍騰等，2000)。意即文獻分析可以幫助研究者釐清研究背景事實、理論發展狀況、研究具體方向、適當研究設計的方式與研究工具的使用。以幫助我們了解過去、重建過去、解釋現在或推測將來(葉至誠與葉立誠，1999)。

承上，本研究運用文獻分析法，藉蒐集官方文件、軍事論文、國際期刊、學術期刊、國內外學者研究、軍事幕僚運用研究、報章雜誌及網路資料等產官學公開文獻(如圖 8)，擷取本研究「國軍油料補給點前支能力」運用於陸航航空燃油需求相關文獻，並以供應鏈概念探討人力不變的原則下，分析歸納國軍油料裝備與航空燃油補給作業最佳方式，獲得最佳效益的運用當前能量與能力，以推測未來油料部隊油料裝備之建軍備戰需求(如圖 9)。

圖 8　研究方法

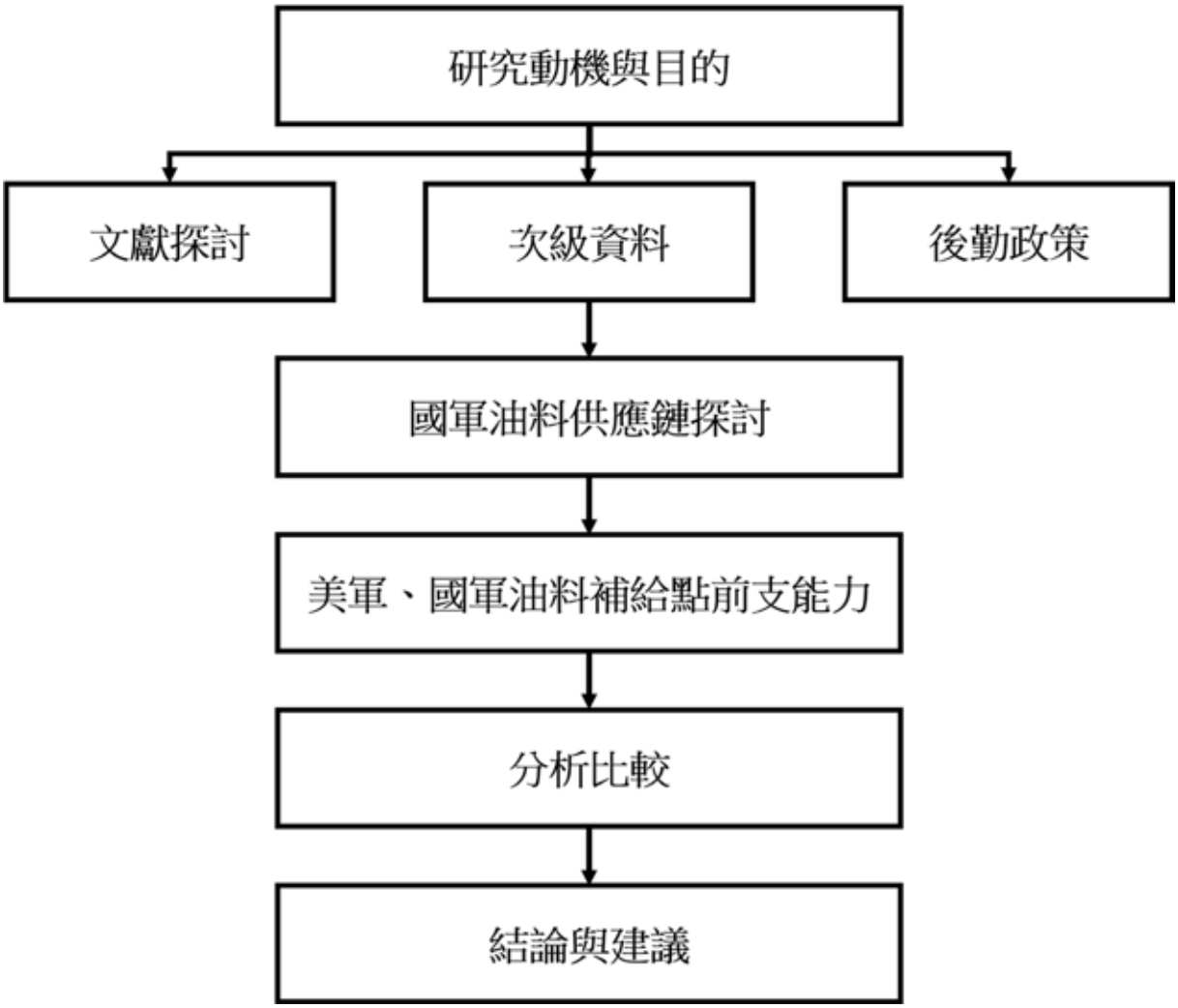


圖 9　研究架構

四、油料前支能力探討

4.1 美軍

因應中共逐漸壯大之海、空軍與俄羅斯、北韓等區域核武強權，美軍認為制衡力量亟須建立，遂發展「反介入／區域拒止」(A2/AD)、「空海一體戰」、「全球公域介入與聯合機動」等新的作戰概念與法規，以肆應未來可能衝突的行動需求。基此，「多領域作戰」為美國陸軍於 2016 年底，依據未來敵情威脅、戰場環境、作戰態勢、預想需求所提出之作戰概念，美軍主張應致力於地面、水域、空中、太空、網路等領域戰場中，提升各軍種聯合作戰效能，藉相互協同合作以主導戰場優勢，執行特定任務。在「關鍵需求能力與支援行動要項」中，以「後勤支援」要項條目數量最多達 26 條，除顯示後勤支援功能所涵蓋範圍之廣泛外，亦可彰顯其支援美軍「多領域作戰」概念之重要性，俾達「行動自由、擴張戰果、延續戰力」目的。

為達到美陸軍對「多領域作戰」中「後勤支援」功能所需具備「關鍵需求能力」之標準與需求，案內「支援行動要項」提出建立後勤基地、預儲物資以支援作戰行動所需、

提升以不同方式配送物資之接收能力、以新裝備精準供應物資等、就地支援整備，改進目前美軍前進支援僅能依賴空投或車隊，而無法精確投送物資或補給線過長，易遭攻擊之缺點。

寓後勤於民力，除上述所提過的就地支援整備外，尚包含保存後勤關鍵能量與運用民間產業能量以創新發展，並以演訓驗證多元聯合後勤供補之能力。

從現代戰爭的發展趨勢來看，未來戰爭的多變性決定了供補的多樣性。因此，美軍針對快速推進的地面部隊，認為應採取直升機直達投送，以充分發揮直升機機動性強的特性，然後使油料或其它補給品能在準確的時間、地點，滿足作戰部隊的需求，此亦為美軍「彈弓式」的供補能力。

圖 10　美國海軍太平洋閃電戰演習 FARP 開設

2019 年 3 月 15 日，太平洋閃電戰演習期間，美國海軍陸戰隊在南加州海岸的一個島嶼上，運用 LCAC 100 級氣墊船及 CH-53 直升機海空立體運送 M969 油罐車、野戰加油系統、油囊與作業人員，跳躍式的建立一個前方地區油料補給點 JFARP(Jump FARP, 如圖 10)，並實施定、旋翼機熱加油作業，即驗證了美軍「彈弓式」的油料供補能力。

美軍 JFARP(Jump FARP) 可以通過多種方式進行，這些方式都取決於任務需求狀況，有三種主要方法 ：

1.從 CH-47SD 直升機掛載 500 加侖油囊，飛往預定的 JFARP 位置，並使用 AAFARS 加油系統建立 FARP。

2.地面車隊運用重型擴展機動戰術卡車(HEMTT)和 M978 油罐車攜帶 2,500 加侖前往 JFARP 地點，並使用 HTARS 加油系統建立 FARP。

3.運用 CH-47SD 直升機內裝載特製「Fat Cow」加油系統，配備 800 加侖油箱和相關加油軟管，建立 FARP。

綜上，美國蘭德公司研究預測在 2025 年後，面對與中國的可能衝突，因為南海和東海地區直接靠近中國大陸，隨著中共軍事能力的增強，美國空軍和海上力量投射將變得越來越困難(John Gordon IV., 2019)。基此，美軍認為未來後勤作業區域的安全維護，將不像面對波斯灣、伊拉克或阿富汗作戰一般容易，能讓後勤部隊在無敵火威脅下安全的作業，遂構思「多領域作戰」下，後勤支援亟須加強關鍵能力，諸如機動、隱密、持續、載具與民力運用等，以降低後勤部隊可能的敵火威脅與負擔，俾符未來防衛作戰需求；美軍多領域作戰下的後勤支援能力，係依中共軍事能力所提出的後勤必備能力，極具國軍油料前支能力探討參據之價值。

4.2 國軍

依據國防部參謀本部後勤參謀次長室後勤政策指導(109 年修訂版)及國軍油料作業手冊規範，國軍後勤油料補給前支作業，係由陸軍後勤指揮部及其他軍種後勤保修指揮部，運用「國軍用兵後勤管理資訊系統」指揮、協調、管制各地區支援指揮部實施前支作業，以滿足三軍部隊油料需求，基此，國軍各油料分庫依循台澎防衛作戰構想，配合年度各項演訓時機，結合各受補單位驗證油料前支補給能力(如圖 11)。

圖 11　國軍油料整補演練

陸軍主戰部隊油料整補係由各油料分庫結合現駐地或民間設施開設油料補給點，運用建制油罐車、大貨車或委商油罐車等輸具，擇一或多元方式實施主動運補油料或油桶

至前支點或直供營輜重位置，據此通用油料作業供應原則，針對陸航部隊航空燃油 JP-8 前支作業能力，分依中油公司、油料分庫與油彈連等油料補給執行單位對下補給能力，簡述如次：

1.中油公司：

中油公司對補給分庫油料補給點係採地下管線輸補或油罐汽車運補方式擇一實施，地下管線具有建置成本高、輸補成本低及固定設施不可移動之特性，油罐汽車特性反之建置成本低、運補成本高及機動載具移動方便，因此，平時採地下管線輸補優先，戰演訓時多採油灌汽車運補效益為佳。

有鑑於管輸若遭敵破壞不易及時修復，僅能採取汽運方式補足油料需求，依前述作戰區假定開設 7 處油料前支點，各點油罐車採輪帶式運補最低須 3 部，以中油公司石門供油中心油罐車 115 部(不含新竹)，可滿足作戰區油料前支點 21 部油罐車之需求。

2.油料分庫：

油料分庫對油彈連油彈補給點係由油彈連編制油罐車自行提領或採委商油罐汽車運補方式擇一實施，油料分庫主要受限於油罐車編現率不足，上述前支點僅能支援陸用油料為宜，航空燃油 JP-8 前支作業均委由中油公司油罐車執行運補作業，若航空旅攻擊 2、戰搜 1、突擊 1 等 4 個大隊，開設油彈補給點 4 處伴隨支援(比照營錙重)，各點油罐車採輪帶式運補最低須 3 部，中油公司允可滿足油彈補給點 12 部油罐車之需求。

3.油彈連：

油彈連油彈補給點對各大隊係以 M978 油罐車及 AAFARS 先進航空前方區域加油系統支援航空燃油需求，M978 油罐車具機動性高、人力需求低及操作簡單之特性，AAFARS 特性反之機動性低、人力需求高及操作複雜，因此，平時均以 M978 油罐車整補航油，戰演訓始驗證 AAFARS 加油系統。

油彈連同樣面臨油罐車編現率不足問題，各油彈補給點雖有中油油罐車提供 JP-8 航空燃油補給作業，中油油罐車卻無法對 AH-64E 等型直升機執行加油作業，各型直升機仍須倚賴 M978 油罐車或 AAFARS 加油系統，尤從陸航部隊 AH-64E 與 UH-60M 直升機接裝成軍以來，近十年 JP-8 航空燃油使用比例(如圖 12)，601 旅及 602 旅油料使用分別成長 2.2 倍與 1.6 倍，即若 101 年度耗油量為 100 萬加侖，601 旅及 602 旅 110 年度耗油量分別成長至 220 萬及 160 萬加侖，油料補給作業十年間負擔巨幅增長，而各航空旅仍只能以 M978 油罐車完成 JP-8 航空油料供應鏈最後一哩路「油箱加滿」。

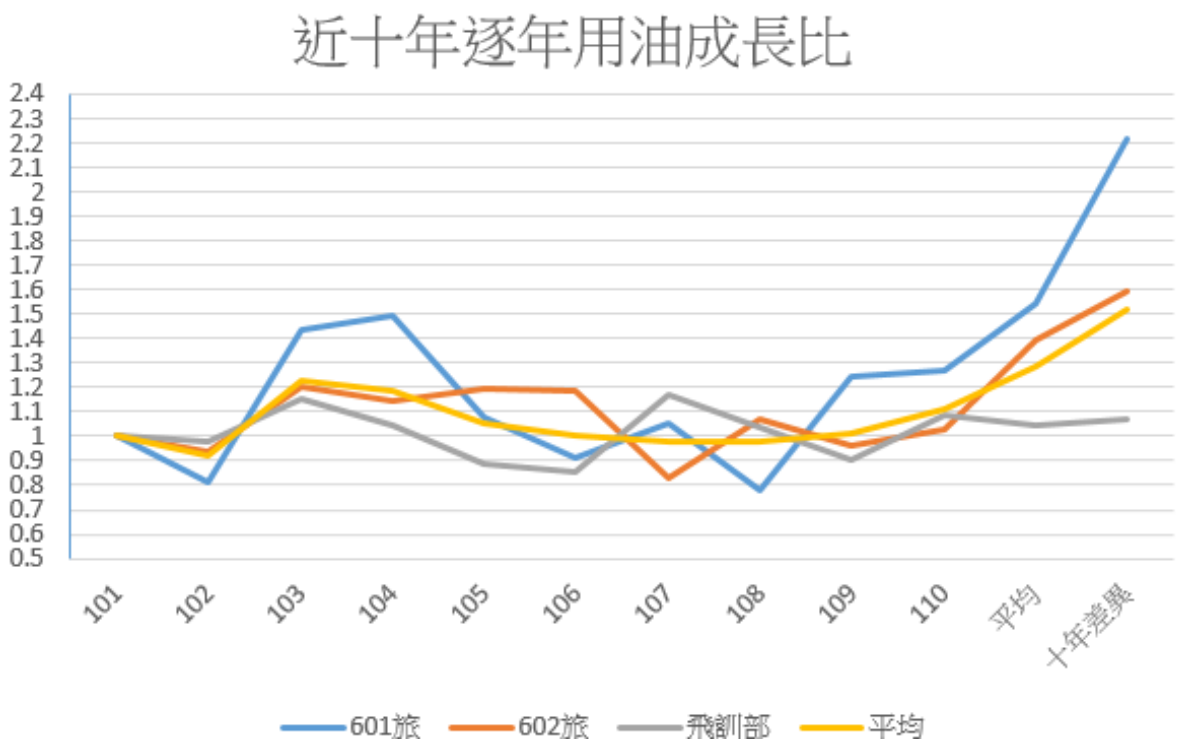


圖 12　陸軍航空部隊近十年 JP-8 航空燃油使用比例趨勢圖

依據美軍 ATP 3-04.17 FARP 技令規範，兩個因素決定 FARP 所需的燃料量：要支持的飛機數量和任務的持續時間。任務燃料需求計算方式為「任務持續時間乘以飛機數量(表 1)乘以每小時加侖的燃料消耗量(表 2)。」

以 601 旅攻擊大隊需求為例，假設每日執行 4 小時任務乘以飛機數量 15 架乘以每小時平均耗油量 179 加侖，得到 JP-8 航空燃油 10,740 加侖需求量，須 2,500 加侖 M978 油罐車整補 5 車次 12,500 加侖，即 5,000 加侖中油油罐車運輸 3 車次，惟整補時間與速度，得視油彈補給點裝備數量而定，採單車多批次或多車單批次整補方式，為當前油料部隊亟需克服的補給難處所在；另允可運用 AAFARS 加油系統連結中油油罐車(待驗證)直接執行加油作業，可大幅提升整補時效。

表 1　陸航各型機單位分配表

直升機型號	601 旅	602 旅	飛訓部	航特部
AH-64E	15、15	-	-	29
AH-1W	-	20、20	21	61
OH-58D	15	15	7	37
UH-60M	15	15	-	30
CH-47SD	-	-	8	8

表 2　陸航各型機油箱容量和平均耗油量

直升機型號	油箱容量(加侖)	平均耗油量(加侖/小時)
		JP-8
AH-64E	370	179
AH-1W	304	113
OH-58D	112	49
UH-60M	362	181
CH-47SD	1,030	522

資料來源：美軍技令 FM3-04.104 FARP(2006)

4.3 小結

美軍因應東、南海近距離面臨中共軍事威脅，構思「多領域作戰」後勤支援關鍵能力計有機動力、隱密性、持續供補、多元載具與民力運用等，以降低後勤部隊可能的敵火威脅與負擔，亦正是國軍面臨的敵情威脅。基此，油料部隊面臨日益嚴重的敵情威脅與主戰部隊逐年增加的油料需求，油料裝備的籌獲亟需加速解決，須符合多領域作戰的後勤支援關鍵能力要求，本研究分以油罐車及加油系統分析關鍵能力優劣，如表 3，獲優先籌補油罐車建議，以肆應臺海軍事威脅。分析如次：

1.機動力：

M978 油罐車底盤具備 8X8 越野能力，行駛範圍達 644KM，行駛速度達 100 公里/小時；AAFARS 加油系統無機動能力。綜上研判 M978 油罐車機動力較優。

2.隱密性：

M978 油罐車可直接運用後方 300GPM 泵浦兩側 50 呎油管，對各型直升機實施加油作業，曝光時間短；AAFARS 加油系統須經組裝後，始可實施加油作業，並須經拆卸後，始可運用載具實施機動，曝光時間長。綜上研判 M978 油罐車曝光時間短隱密性較優。

3.持續供補：

M978 油罐車配賦 2500 加侖罐體乙具，運用動員中油油罐車實施再整補油料；AAFARS 加油系統配賦 500 加侖油囊 12 具，合計 6000 加侖，每次組裝採梯次循環使用，乙次使用 2000 加侖計 4 具油囊，惟油囊須運用油罐車透過低壓泵浦補充油料，導致作業耗時。綜上研判 M978 油罐車持續供補快速較優。

4.多元載具：

M978 油罐車除自主實施地面機動外，可運用 C-130 運輸機實施空中運動；AAFARS 加油系統可藉由中型戰術輪車、CH-47 直升機及 C-130 運輸機實施地空聯合運輸。綜上研判 AAFARS 加油系統藉由 CH-47 直升機靈活運用於交通中斷地區，AAFARS 多元載具運用較優。

5.民力運用：

M978 油罐車及 AAFARS 加油系統均可透過中油公司油罐車實施直供運補。綜合研判民力運用能力概等。

6.綜合建議：

M978 油罐車在機動力、隱密性及持續供補等三項能力較優，同步考量臺灣南北狹長、東西腹地短窄，易受敵軍各式砲火威脅環境下，油罐車允較符合本研究 2.3 輸補具支持與建立前支點配送網路及 2.4FARP 作業時間短經常移動等特性，建議油罐車納入未來油料部隊建軍規畫優先籌購裝備，以符未來作戰環境與部隊需求。

表 3　陸航現行加油裝備多領域作戰後勤能力分析

區分	M978 油罐車	AAFARS 加油系統
機動力	644KM	無
隱密性	免組裝，FARP 開設速度快	須組裝，FARP 開設速度慢
持續供補	獨力供補 2500 加侖	油囊供補 2000 加侖
多元載具	地面自力機動	地空載具機動
民力運用	中油公司油罐車直供運補	
綜合建議	優先籌補	配合戰術運用

五、結論

國軍組織自精實、精進、精粹案編制調整及兵力縮減迄今，油料補給人力嚴重流失，恐將導致戰時油料運補不及，進而影響我全軍戰力發揮；另舒先勝等(2014)歸納裝備完善率對油料保障作業影響為最大。基此，本研究藉供應鏈概念及人力不再改變原則下，以美軍多領域作戰後勤能力要求及油料保障評估指標，檢視陸航部隊現行油料裝備能量，研析以下建軍發展建議：

5.1 優先籌補油罐車

宜購置現役油罐車或延伸構型，除具備上述機動力等優勢外，並可降低教育訓練門檻、裝備熟捻容易上手以及沿用現行整體後勤支援規劃。

5.2 評估 AAFARS 戰術價值

AAFARS 具備強大的 1 對 4 熱加油能力，惟鈍重性高不易機動、場地要求寬闊不易設置等問題，造成目標顯著恐易成為共軍精準武器優先打擊目標，宜納入我掌握(局部)空優之淺山疏散後勤區域使用或參照美軍 CH-47SD 直升機內裝載特製「Fat Cow」加油系統靈活運用。

5.3 擴大徵用航空燃油專用油罐車

平時中油地區供油中心支援 JP-8 航空燃油專用油罐車運補任務不足五部，平戰轉換後中油油罐車僅能運載 2 萬 5,000 加侖執行航油分屯作業，為避免俄烏戰爭油庫設施遭受精準武器攻擊情事發生，宜納入中油公司油料輸補協議書，律定各地供油中心油罐車分屯航空燃油車輛數，俾利航空燃油戰力保存無虞。

5.4 運用指名申請機制

平時即藉指名申請航空燃油補給中高專長人員，並藉教育召集時機考核人員能力，俾利戰時有效增加航空燃油補給人力。

六、國防領域相關應用

有自主的國防，才有自主的國家，「國防自主」是政府一貫的政策，近年來從新式高教機的國機國造，高效能艦艇的國艦國造，均顯示國防自主的決心，本研究建議優先籌補油罐車，除短期從美國軍、商購 M978 油罐車外，另可中、長期採取國車國造方式，全面補充營、連錙重油料補給能力。

航空燃油戰力保存採取擴大徵用油罐車分屯方式行之，陸用油料戰力保存得採中油加油站滿儲為軍事用途，餘台塑等加油站為民生使用，將戰略物資妥善分流使用，俾先安內於民心後壤外於敵軍；另參考 AAFARS 運作方式，預擬加油站停電狀況下切換為發電機供電，並透過延長油管對輪、履帶軍事裝備實施油料整補，將加油站運用最大效益化。

參考文獻

台灣中油股份有限公司（2021）。台灣中油業務簡介中文版。

台灣中油全球資訊網，代儲政府儲油公告，下載於 https://new.cpc.com.tw/News.aspx?n=1493&sms=8976（2022 年 1 月 18 日）。

利杰克 Jack Neele（2021）。「最後一哩路」成為電商必爭之地，工商時報，https://readers.ctee.com.tw/cm/20211101/a39ac3/1153000/share(2022 年 1 月 18 日)。

林國華（2018）。因應敵非線性作戰時我軍陸用油料供補模式之研究。*陸軍後勤季刊*，113-114。

林俊安（2018）。美國陸軍多領域作戰關鍵需求能力與支援行動要項。*陸軍後勤季刊*，61-113。

青年日報（2021）。【勁旅榮光】陸軍航特部飛行訓練指揮部陸航搖籃維保育才。下載於 https://www.ydn.com.tw/news/newsInsidePage?chapterID=1374368&type=military(2022 年 1 月 18 日)。

胡仲適（2002）。特種作戰在台海戰爭中之研究。國防大學國防管理學院決策科學研究所碩士論文。

孫贊凱（2004）。供應鏈全球運籌之建構與分析。國立臺灣大學碩士論文。

張心馨、詹進勝（2000）。企業國際化在全球運籌與供應鏈管理之整合發展研究。*中華管理評論*，3（4），93-110。

黃明弘（2008）。建立供應鏈之策略性供應商選擇模式。中原大學碩士論文。

陳家妤（2013）。供應鏈風險管理之個案研究-以國內童裝業為例。國立成功大學碩士論文。

國防部陸軍司令部（2018）。國軍油料補給作業手冊。

舒先勝、丁澤中、夏亦寒、顏青、詹啟東（2014）。基於主成分分析法的油料保障能力評估。*四川兵工學報*，35（3），85-87。

林珮萱。員工平均 50 歲也做得到！台灣中油如何轉型把「油罐車變聰明」？，下載於 https://www.gvm.com.tw/article/83120(2022 年 2 月 15 日)。

劉培林、劉達生、李廷峯（2017）。運用系統動態學探討人力政策對空用油料供補及空戰影響之研究。*國防管理學報*，38（2），39-57。

羅裕耀、石穎浩（2019）。軍用油料前進支援點開設選址之最佳化研究—以 F 作戰區為例。*陸軍後勤季刊*，69-82。

Charles Q. Brown, Jr., Bradley D. Spacy, Charles G. Glover III. (2015). Rapid mobility and forward basing are keys to airpower's success in the antiaccess/area-denial environment, *Air & Space Power Journal*, 17-28.

Edmund Lee, Ryan Riemer (2020). Maximizing FARP efficiency in large scale combat operations. ARMYAVIATION MAGAZINE.COM, http://www.armyaviationmagazine.com/index.php/archive/not-so-current/1947-maximizing-farp-efficiency-in-large-scale-combat-operations (retrieved on February 20,

2022)。

Handfield, R. B., & Nichols, E. L. (1999). Introduction to. *Supply Chain Management*, Prentice Hall, Englewood Cliffs, NJ, 1-29.

Headquarters, Department of the Army, 2006, Forward Arming and Refueling Point, FM 3-04.104。

Headquarters, Department of the Army (2018). Techniques for Forward Arming and Refueling Points, ATP 3-04.17.

John Gordon IV. (2019). Army Fires Capabilities for 2025 and Beyond, RAND ARMY RESEARC DIVISION.

Lance Cpl. (2019). Forward Air Refueling Point (FARP) Setup. Pacific Blitz 2019, Video by YouTube, https://www.youtube.com/watch?v=46afv-ZpxCs (retrieved on February 20, 2022).

U.S. Department of Defense (2021). Military and security developments involving the People's Republic of China.

Davis, R. D. (2014). Forward Arming and Refueling Points for Fighter Aircraft. *Air and Space Power Journal*, *28*(5), 5-28.

植基於邊緣偵測及最佳像素調整之資訊隱藏方法

劉興漢 [1*]　賀盛志 [2]　鄭岳原 [1]

[1] 國防大學資訊管理學系

[2] 德明財經科技大學資訊管理系

論文編號：NM-44-01-05
DOI：10.29496/JNDM.202405_45(1).0002
來稿2022年9月22日→**第一次修訂**2022年10月3日→**第二次修訂**2023年3月13日→
同意刊登 2023 年 4 月 10 日

摘要

本研究提出植基於邊緣偵測及最佳像素調整之資訊隱藏方法，首先利用中間邊緣偵測法用來區分目標像素是位於邊緣或是平滑區，據以判定秘密訊息的藏入量，基於人類視覺系統，若目標像素位於邊緣則以最低有效位元取代與最佳像素調整法嵌入較多的秘密訊息，若在平滑區則以相同方法嵌入較少的秘密訊息。實驗中，我們使用 Lena 等 8 張灰階影像進行測試，得到高藏密量且偽裝影像品質良好的效果。此項方法不需複雜的演算過程，透過現行基本的軟硬體設備，即可將機密資訊藏入影像中，並從偽裝影像取出隱藏訊息。此研究可提供國防資訊安全管理研究領域參考應用。

關鍵詞：中間邊緣偵測法、最低有效位元取代法、最佳像素調整法

[*]聯絡作者：劉興漢 email: liu.hansh@gmail.com

An Improved Steganographic Method Based on Median Edge Detection and Optimal Pixel Adjustment Process

Liu, Hsing-Han[1*]　Ho, Sheng-Chih[2]　Cheng, Yue-Yuan[1]

[1]Department of Information Management, National Defense University, *Taiwan, R.O.C*
[2]Department of Management Information System, Takming University of Science and Technology, *Taiwan, R.O.C*

Abstract

In this study, we propose an improved steganographic method based on median edge detection and optimal pixel adjustment process. At first, the median edge detection predictor distinguishes the target pixels located at the edge or those in the non-edge area, which determines the number of secret embedded data for each target pixel. According to the concept of human vision system, if the target pixel is located at the edge, the predicted value of the target pixel embeds more secret bits via the least-significant-bit substitution and optimal pixel adjustment process method. Contrarily, if the target pixel is located in the non-edge area, it embeds fewer secret bits via the same method. In this experiment, the modified method achieves a high capacity with better stego-image quality by using 8 grayscale images such as Lena, etc. This method does not require complex computational processes, but uses existing basic hardware and software to hide confidential information in the image and retrieve the hidden information from the stego-image. This study can provide reference applications in the field of defense information security management research.

Keywords: Median Edge Detection, Least-Significant-Bit Substitution, Optimal Pixel Adjustment Process

[*]Corresponding author: Liu, Hsing-Han email: liu.hansh@gmail.com

一、前言

通訊技術與生活便利性息息相關，愈新的通訊技術，在相同的時間內可以傳送愈多的資料量。若有適當的軟硬體配合，時間與空間對通訊終端方在事物的受用上，造成的限制亦隨之降低，學習、工作與生活的整體效率會隨之增加，相較過往通訊不便，現行通訊技術提升及行動網路普及，人們傳遞訊息所使用之文字、圖片、聲音、影片等傳輸媒介亦都數位化，數位資料的傳遞需求也隨之提高，然而當數位資料用來傳遞訊息愈便利，卻也增加了訊息內容遭惡意人士偽造、竊取的風險。因此，將傳遞之訊息「加密」或「隱藏」以確保數位資料傳遞之正確性、安全性，成為了值得探討研究之議題。訊息之「加密」或「隱藏」最大的不同：訊息「加密」是將要傳遞的原始資料「明文」，透過加密轉變為「密文」，將傳遞的訊息隱藏起來；而訊息「隱藏」則是將要傳遞的原始資料，運用方法或技術，儘可能使人無法察覺傳遞出去的訊息中，藏有真正要傳達的隱藏訊息(王旭正與柯宏叡，2006)。資料加密，如欲破解一份密文則必須去破解出其原始加密時所用之金鑰，才能取得原始之明文；但是對於資訊隱藏，其功能或原始意義不需被完全理解，只要隱藏之訊息被察覺，且被證明其存在，便是被破解(張凱崴，2013)。

資訊隱藏技術或可稱之為藏密學，於歷史上可說是五花八門，主要表達訊息中還有著「隱藏訊息」(王旭正等，2012)。歷史上，最早記載是在西元前五世紀，古希臘作家希羅多德(Herodotus)的著作史書(Histories)中提到，古希臘的統治者希斯提奧斯(Histiaus)，其將信任的奴隸頭髮剃光後，在奴隸頭皮上刻印祕密訊息，等到奴隸頭髮長出來，才派遣奴隸至目的地，此時對方只要把奴隸的頭髮剃光，即可得到被隱藏的秘密訊息，藉此傳達軍事訊息(婁德權，2006)。其他在軍事領域上運用資訊隱藏的案例，如傳送方使用隱形墨水，將軍隊動向、攻擊標的等重要軍事訊息，寫在信紙上，在不被敵人發現的狀況進行訊息傳遞，接收方透過將信紙加熱後，就能取得秘密訊息，隱形墨水是利用果汁、醋、牛奶等成分的化學變化來完成資訊隱藏目的；第二次世界大戰時，德國人將作工精細的微縮照片藏匿在普通訊息字句的標點符號內，藉此多次成功傳達軍事機密訊息。資訊隱藏應用方法多而廣泛，全取決於使用者的智慧及變化，隨著數位化時代到來，數位資料普及後，資訊隱藏技術亦被運用在確保數位資料傳輸之安全性。

資訊隱藏藉由通訊載體以達成嵌密之目的，其透由文字、影像、音訊、影片等數位傳輸媒介進行嵌密，現有研究提出嵌密於網路協定(network protocol)、DNA 等載體進行資料傳輸，但其中影像是最受歡迎也最常被使用的載體(Hussain et al., 2018)。數位影像具有下列優點：(一) 常見且取得容易；(二) 結構簡單易懂，可塑性極高；(三) 影像具成熟分析檢查技術，在數位影像上評估影像失真性是很容易的事情(吳南益等，2010)。資訊隱藏技術把秘密訊息嵌入掩護影像(cover image)之中，產生隱含機密訊息的偽裝影像(stego-image)，藉此避免秘密訊息被惡意者發現，以完成秘密通訊，其原理在於透過調整掩護影像的像素，將秘密訊息嵌入影像像素中，因為人類的視覺系統(Human Vision System; HVS)對影像微小的差異，幾乎無法察覺，藉此達到在不被惡意人士注意下，傳遞秘密訊息。

資訊隱藏的初衷不同於傳統密碼學，目標在於不被竊取者發現數位載體上藏有秘密

訊息，並根據資訊隱藏目的、技術，有以下特性：不可察覺性(imperceptibility)、強韌性(robustness)、安全性(security)、不可偵測性(undetectability)、效率性(efficiency)、高隱藏容量(high capacity)。一個安全又可靠的資訊隱藏技術，主要特性為以下三點：(一)不可察覺性：藏密過的數位資料不產生明顯之品質變化，符合人類視覺系統的特性狀態下，難以被人類感官所察覺。(二)高隱藏容量：資訊隱藏之目的，就是要在數位資料中藏入愈多秘密訊息。(三)強韌性：經過資訊隱藏的數位資料，須能被常見之非惡意方法處理後，隱藏資訊仍存在數位資料中，不會遭移除。(左豪官等，2007；陸哲明，2014)在各種特性間取得最佳平衡，儘可能發展同時滿足上述特性之資訊隱藏方法，是學者們持續努力的方向，也是最大的挑戰。

本研究將運用中間邊緣偵測法(Median Edge Detection; MED)預測掩護影像像素是否為邊緣，再以最低位元取代法(Least Significant Bit Substitution; LSB Substitution)結合最佳像素調整法(Optimal Pixel Adjustment Process; OPAP)的方式，將秘密訊息藏入掩護影像，本文之研究貢獻條列如下：

1. 軍事情資能在無人察覺的狀況下，安全地進行傳輸。
2. 實現一種具安全性、高藏密量、藏密過程不需複雜運算，並維持人類視覺可接受的影像品質之數位影像資訊隱藏技術。

本研究藏密方法最大可藏入 4.6bpp，且 PSNR 與 SSIM 值均位於人類視覺無法察覺之範圍，證明本研究藏密方法能有效提升藏密量，並維持一定的影像品質。

二、文獻探討

2.1 最低有效位元取代法

Bender et al.(1996)提出最低有效位元取代法，這個方法通常是研究空間域的資訊隱藏技術時，最先接觸到的一種方法。此概念是利用單個像素值當中最低的位元訊息，如圖 1 所示，直接嵌入秘密訊息，此作法對影像品質影響最小，因為人眼對微小差異無法察覺，此藏密法除操作容易外，也能滿足低處理效率的設備。但其缺點在於若欲增加藏密量，用來隱藏資料的位元數就必須增加，嵌入過多的秘密訊息時，會造成影像的失真，進而引起竊取者的注意。

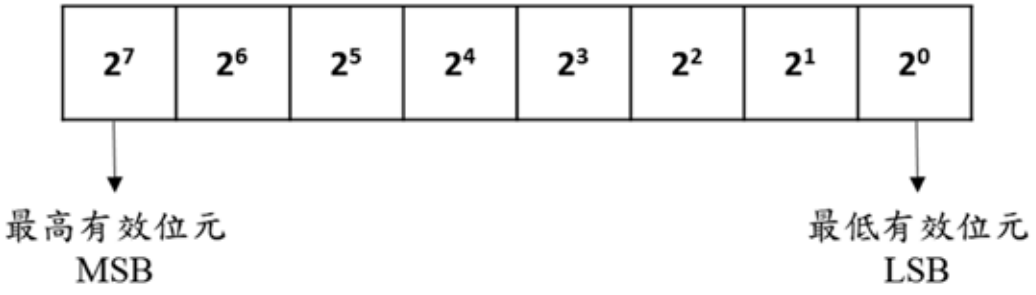


圖 1　像素值的二進位表示圖
資料來源：Chan and Cheng(2004)

以實際範例說明最低有效位元取代法，如圖 2 所示，掩護影像 C 為 2×2 之灰階影像，欲在 C 內嵌入$(11100100)_2$ 共計 8 個位元的秘密訊息 S，因為掩護影像 C 總共有 4 個像素，第一步先將 S 平均分割成 4 等份為 $s_1=(11)_2$、$s_2=(10)_2$、$s_3=(01)_2$、$s_4=(00)_2$，接續分別將 s_1、s_2、s_3、s_4 與掩護影像 C 中 4 個像素內的最低 2 個位元進行替換，完成取代程序後，原本掩護影像 C 的像素(128, 207, 227, 241)，調整成偽裝影像 C'的像素值為(131, 206, 225, 240)，即完成藏密程序，並得到已嵌入秘密訊息 S 的偽裝影像 C'。

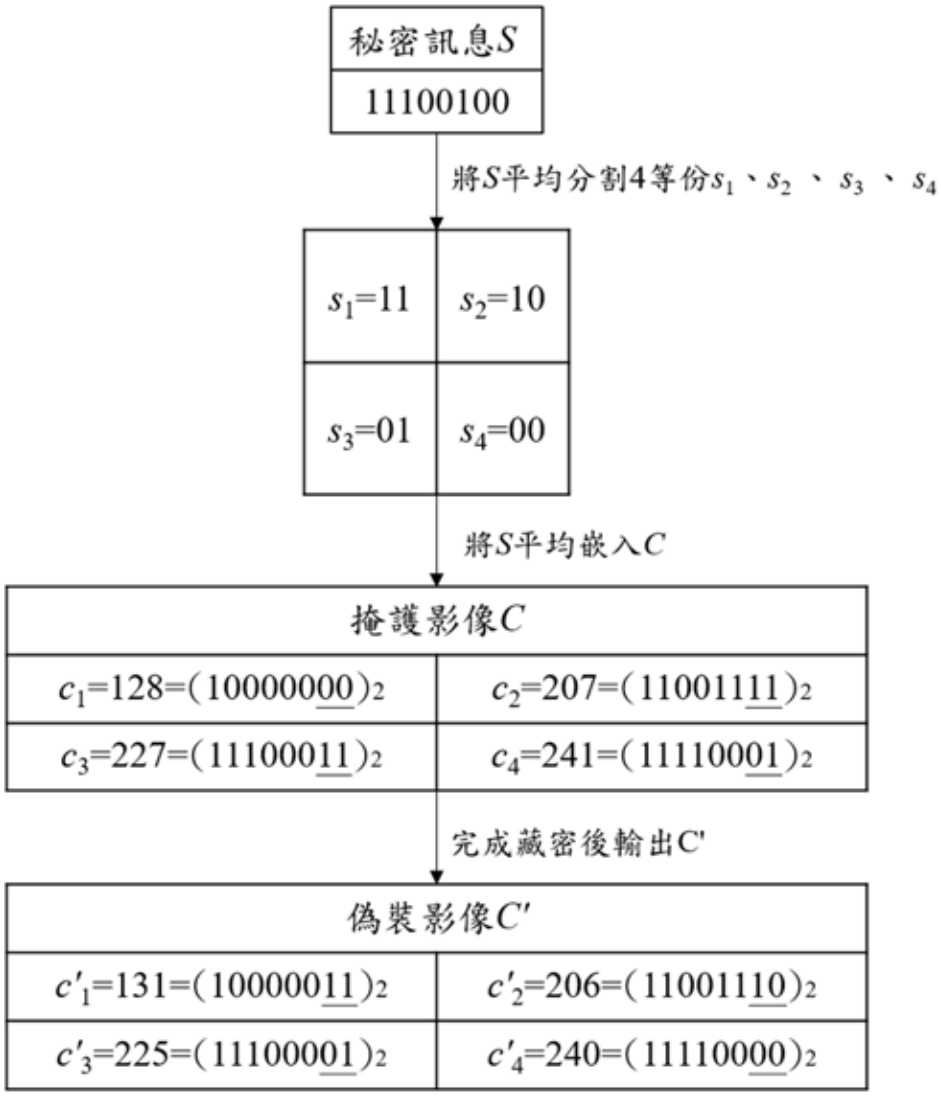


圖 2　最低有效位元取代法藏密步驟示意圖

將上述最低有效位元取代法以方程式來表示，假設 c_i 為掩護影像中其中一個像素值，s_i 為 S 之中一小段 k 位元的祕密訊息，此時要將 k 位元來嵌入 c_i 中，嵌入 k 位元後新像素值為 c'_i，上述嵌密的過程可以用公式(1)來表示：

$$c'_i = c_i - (c_i \ mod \ 2^k) + s_i \tag{1}$$

相反地，取密前只要知道嵌入的位元長度 k 為何，即可從 c'_i 取出秘密訊息 s_i，以公式(2)來表示如下：

$$s_i = c'_i \ mod \ 2^k \tag{2}$$

2.2 最佳像素調整法

Chan and Cheng(2004)提出基於 LSB 的改良方法，最佳像素調整技術，運用在影像經過 LSB 取代法後進行修正，藉由位元置換階層的調整，使像素差值最佳化，在嵌入相同藏密量的狀況下，獲得較佳影像品質，改善偽裝影像失真度。

假設秘密訊息 S，要將 k 位元嵌入掩護影像 C，嵌入後得到偽裝影像為 C'。而 c_i 為掩護影像 C 之像素值，c'_i 為利用 LSB 取代法嵌入秘密訊息後的像素值。另假設 d 為 c'_i 與 c_i 的差值，計算出 d 後，依據 d 的值可以區分三個區間，每個區間符合的條件都不相同，經過調整後得到 c''為經過最佳化調整後之像素值，三個區間分別如下：

區間一：$2^{k-1} < d < 2^k$，若$c'_i \geqq 2^k$則$c''_i = c'_i - 2^k$，否則$c''_i = c'_i$。

區間二：$-2^{k-1} \leq d \leq 2^{k-1}$，$c''_i = c'_i$。

區間三：$-2^k < d < -2^{k-1}$，若$c'_i < 256 - 2^k$則$c''_i = c'_i + 2^k$，否則$c''_i = c'_i$。

以實例說明 OPAP 的調整技術，如圖 3 所示，假設掩護影像 C 中某一像素值 c=168，轉換為二進位為 c=$(10101000)_2$，在這個像素中嵌入 k 為 3 位元之秘密訊息 S=$(111)_2$，得到新像素值 c'=$(10101111)_2$=175，此時計算兩個像素差值 d= c'-c=175-168=7，從上述 OPAP 調整區間可以判斷適用於區間一，且因為 c'=175≥2^3，得到經過最佳調整化過後的像素值 c''= $c' - 2^k$=175-8=167=$(10100111)_2$。原本 c'與 c 像素差值 d 為 7，經 OPAP 方法調整後 c'與 c 像素差值 d'減少為 1，進而提升偽裝影像品質。

反之，OPAP 方法的取密過程，只要藉由公式(2)之 LSB 取密方法即可完成。例如，調整後新像素值 c''為 167，利用公式(2)可以得到秘密訊息 S=167 mod 2^3＝7＝$(111)_2$，即為原本欲藏入 k=3 之秘密訊息 S。

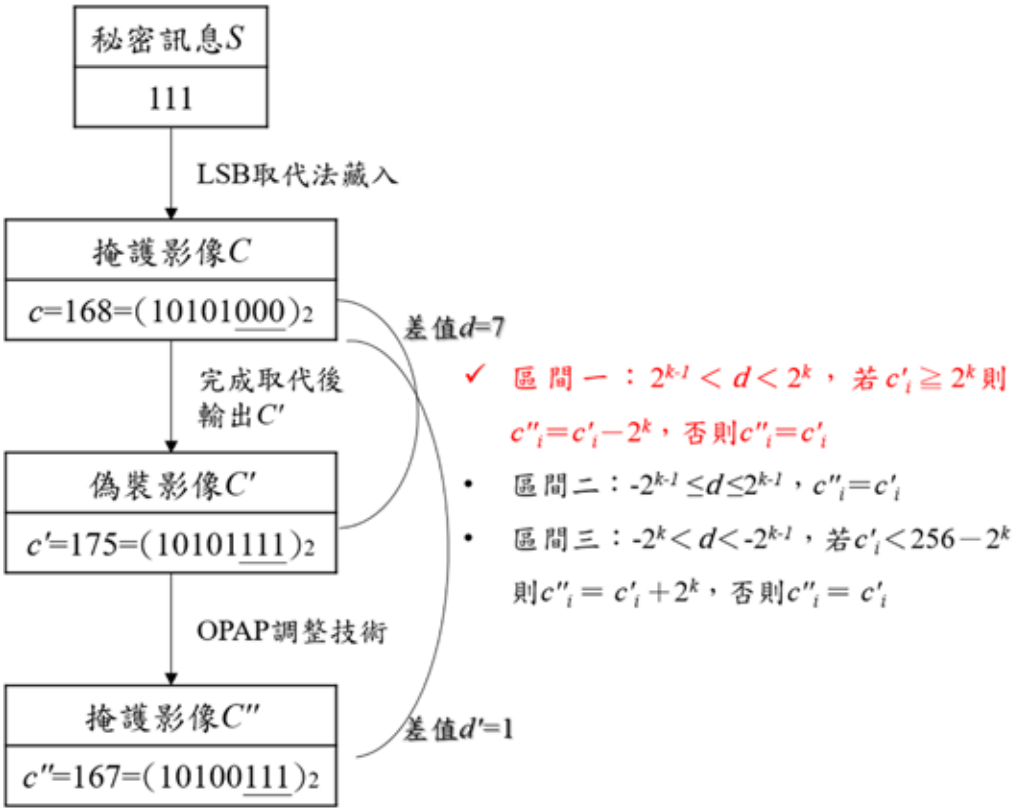


圖 3　最低有效位元取代法藏密步驟示意圖

2.3 中間邊緣偵測法

Martucci(1990)提出中間邊緣偵測法來預測像素的預測方法，該方法在邊緣明顯的影像中有較好的預測效果(Weinberger et al., 1996)。MED 每次進行預測時皆以 2×2 之區塊進行預測，假設預測像素值為 x，與 x 之相鄰像素值分別為 a 以及 b，非相鄰之像素值為 c，如圖 4 所示，預測值的計算如公式(3)說明，其中 $p(x)$為像素值之預測計算式，依像素值 c 符合判斷之狀況，選擇適合的運算式。

c	b
a	x

圖 4　預測像素 x 與其相鄰像素示意圖
資料來源：Weinberger et al.（1996）

$$p(x)=\begin{cases} min(a,b), if & c \geq max(a,b) \\ max(a,b), if & c \leq min(a,b) \\ a+b-c, & otherwise \end{cases} \quad (3)$$

Martucci 的方法預測效果很好，因此有許多研究都是以它為基礎(呂慈純等，2014)，本研究在預測部分亦採用 Martucci 提出的方法，判斷目標像素是否位於邊緣：若 $c \geq \max(a,b)$或 $c \leq \min(a,b)$，則 x 屬邊緣，否則為非邊緣，並稱之為平滑區。

2.4 改良後的中間邊緣偵測法

冷輝世等學者於 2013 年提出保留邊緣特性之改良後的中間邊緣偵測法(MMED)，假設在原始影像中 a、b、c 為目標像素 x 的鄰近像素(如圖 4 所示)，對於個別的影像特徵可找到一個門檻值 T，使其預測值在非邊緣區時更為準確，其預測值計算如公式(4)之說明。

$$p(x)=\begin{cases}\min(a,b), if\ \ c\geq\max(a,b)\\ \max(a,b), if\ \ c\leq\min(a,b)\\ \dfrac{a+b+c}{3}, \quad c\in(a,b), \left|c-\dfrac{a+b}{2}\right|<T, \quad T\in N\\ a+b-c, \quad otherwise\end{cases} \tag{4}$$

在公式(4)的計算過程中，先判斷目標像素是否位於邊緣或非邊緣區，如果 c 與 $(a+b)/2$ 的差小於個別影像特徵找到的門檻值 T，則預測值可設為 $(a+b+c)/3$，其餘預測值的設定與原始 MED 方法相同。修改後的 MMED 預測值經實驗證明，可準確判斷目標像素的特性，進而增加其資訊隱藏的容量。

2.5 藏密技術衡量標準

好的資訊隱藏技術通常需滿足安全性、不可察覺性、高藏密量等特性，但藏密影像品質與藏密量通常難以兼顧，當影像藏密量越大對其品質破壞也越大，因此在藏密影像品質與藏密量尋求最佳平衡點，成為資訊隱藏領域重要的研究議題，其中藏密量 bpp(Bit Per Pixel)表示每一像素值可藏入多少位元數，如公式(5)說明。接續將就峰值訊號雜訊比(Peak Signal to Noise Ratio, PSNR)與結構相似性指標(Structural Similarity Index Measure, SSIM) 2 種量化之衡量標準進行介紹。

$$bpp=\frac{Maximal\ \ Embedding\ \ bits}{m\ \times\ \ n} \tag{5}$$

公式(5)中的 m 與 n 分別代表受測影像的長與寬(單位為 pixel)。

2.5.1 峰值訊號雜訊比

Zhouc and Bovik(2002)提出一種對於影像品質的客觀判斷標準，以均方差(Mean Square Error, MSE)及峰值訊號雜訊比作為判定工具，均方差計算如公式(6)。

$$MSE=\frac{\sum_{i=1}^{m\times n}(C_i-C'_i)^2}{m\times n} \tag{6}$$

m 及 n 分別為影像之長、寬，於公式中相乘的分母表示影像之總像素值；C_i為掩護影像中的一個像素值、C'_i為掩護影像嵌密後的像素值，C_i與C'_i如果相差愈大，得到的均方差就愈大，表示掩護影像與嵌密後的影像差異愈大，愈容易被發現；反之，MSE 愈小、愈趨近於零，代表嵌密後的影像品質愈好、不可察覺性愈高。然而 MSE 將影響 PSNR 的值，其計算如公式(7)所示。

$$\mathrm{PSNR} = 10 \times \log\left(\frac{255^2}{MSE}\right) \tag{7}$$

一般灰階影像像素值以 8 位元表示，公式(7)中的 255 為灰階影像中最大的像素，倘若上述 MSE 的值愈小，PSNR(單位為 dB)就愈高，通常來說，人類的視覺在影像 PSNR 超過 30dB 時，就看不出藏密前後之差異性(陸哲明，2014)；PSNR 值小於 30dB 時，表示人類視覺看起來不能忍受的範圍，因此大部分 PSNR 值皆要大於 30dB，但 PSNR 值越高，不代表影像品質一定好，仍必須靠人的肉眼輔助來判斷影像的品質(王旭正等，2016)。

以圖 5 實例說明 PSNR 值大小與影像品質關係，圖 5(a)為 Lena 影像原圖、圖 5(b)為 Lena 影像 PSNR 值為 54.6dB 圖、圖 5(c)為 Lena 影像 PSNR 值為 31.02dB 圖、圖 5(d)為 Lena 影像 PSNR 值為 22.16dB 圖，圖 5(a)Lena 原圖與圖 5(b) Lena 影像 PSNR 值為 54.6dB 之圖相較之下，難以察覺差異，但當影像由左至右、PSNR 值愈來愈低，圖 5(c)及圖 5(d)影像以人眼即可察覺愈來愈顯粗糙。

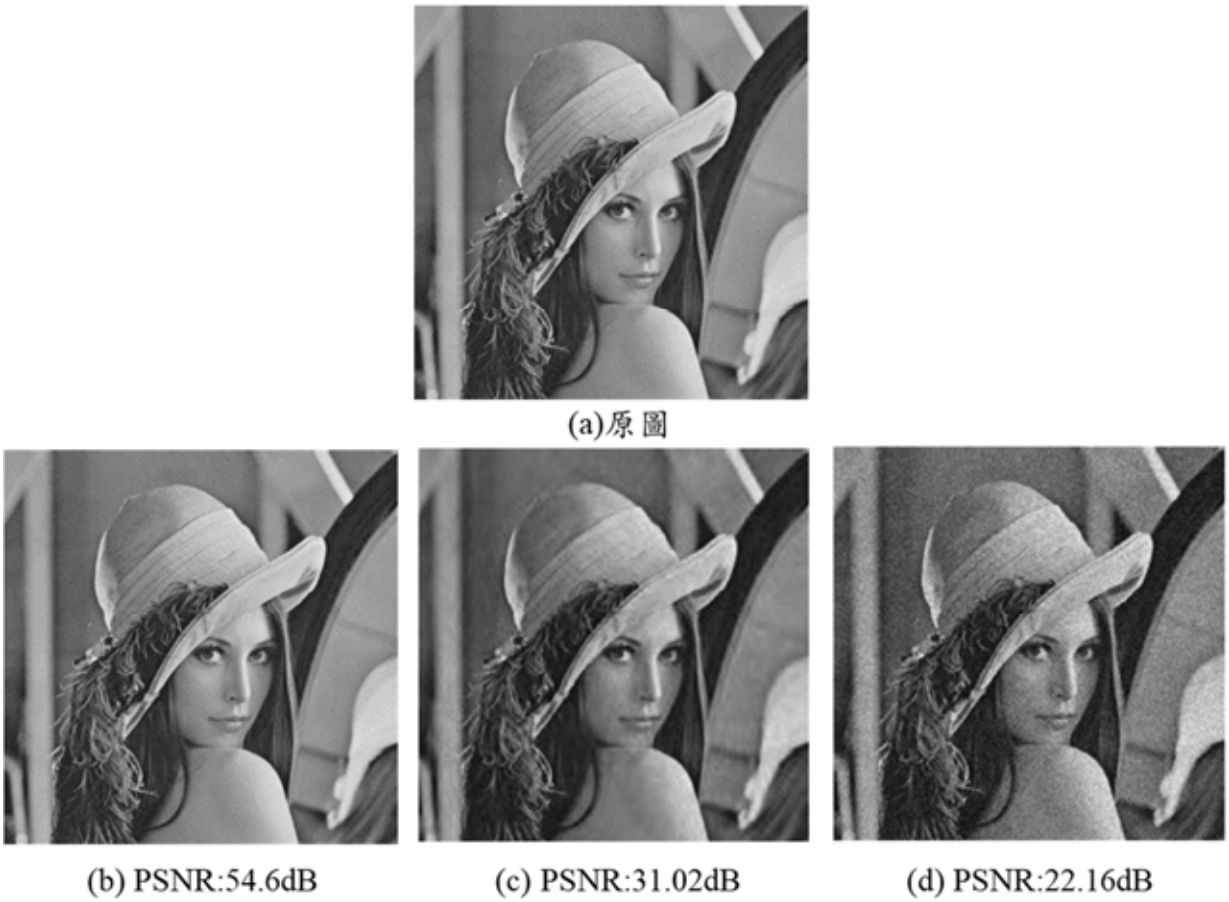


圖 5　PSNR 值實例影像圖

2.5.2 結構相似性指標

PSNR 值判定未列入人眼視覺特性，人眼對空間、亮度、區域對比度敏感度亦會影響感受，對空間頻率較低的敏感度較高、對亮度比對色度差異更敏感、對一個區域的感

知會受其周圍鄰近區域所影響等因素，因此常出現 PSNR 值判定結果與人眼主觀感受分歧的情況，自然影像是高度結構化的，亦即在自然影像相鄰像素之間有很強之關聯性。

因此 Zhou Wang et al.(2004)提出另一種符合人體直覺的影像質量評價標準，用以衡量 2 張數位影像相似程度之量化標準，稱結構相似性指標，主要測量掩護影像和偽裝影像之間結構相似大小，其值介於 0 到 1 之間，值愈大表示兩張影像的相似度愈高，SSIM 為 1 時，表示 2 張數位影像完全一致，SSIM 大於或等於 0.98 時，表示 2 張數位影像難以分辨，而 SSIM 為 0.95 時，表示大多數人對畫面看起來滿意，此數值可以視為及格的畫面，SSIM 為 0.9 時，表示瑕疵可能較 SSIM 為 0.95 時多一倍，人眼可察覺到明顯的畫面劣化。分別從公式(8)之影像亮度、公式(9)之對比度、公式(10)之結構等三方面度量影像相似性，而 SSIM 值計算方式如公式(11)所示。

$$l(x,y)=\frac{2\mu_x\mu_y+c_1}{\mu_x^2+\mu_y^2+c_1} \tag{8}$$

$$c(x,y)=\frac{2\sigma_x\sigma_y+c_2}{\sigma_x^2+\sigma_y^2+c_2} \tag{9}$$

$$s(x,y)=\frac{\sigma_{xy}+c_3}{\sigma_x\sigma_y+c_3} \tag{10}$$

$$SSIM=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{11}$$

其中，μ_x 及 μ_y、σ_x 及 σ_y 分別為 x 和 y 的平均值和標準差，σ_{xy} 為 x 和 y 的共變異數，c_1、c_2、c_3 皆為常數，用以維持$l(x,y)$、$c(x,y)$、$s(x,y)$的穩定。

三、研究方法

本研究利用 Martucci 學者提出的 MED 概念進行影像像素預測，每次預測以 2×2 個像素單位區塊進行預測，直接依照像素目標位置預測為邊緣或平滑區決定藏入量，若像素目標位置預測為邊緣，則藏入較多秘密訊息，若像素目標位置預測為平滑區，則藏入較少的秘密訊息，期藉以提升藏密效率，另為避免單純使用 LSB 取代法藏密後之偽裝影像具明顯特徵，可被現今許多藏密分析方法有效偵破，為了保有安全性，藉由 LSB 取代法結合 OPAP 調整法，調整像素差值，提高影像品質並改善偽裝影像失真度，進而取得偽裝影像，並能具有良好的抵抗藏密偵測之能力，本研究方法設計傳送概念圖如圖 6。

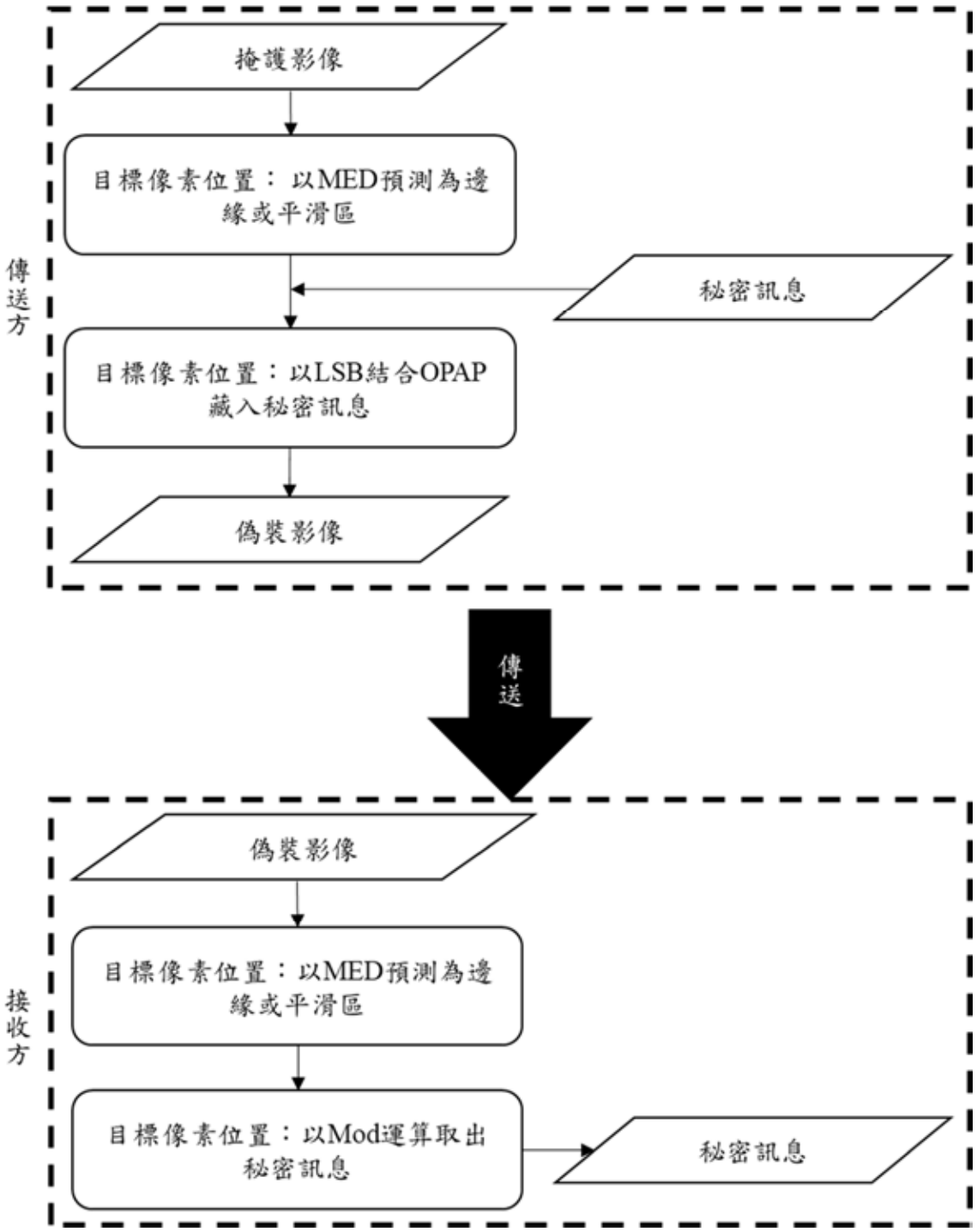


圖 6　本研究方法設計傳送概念圖

3.1 本研究方法之藏密程序

步驟一：以 512×512 大小之灰階影像 *C* 作為掩護影像，第一行與第一列中各 512 個像素作為參考值，均不藏入秘密訊息(如圖 7 斜線部分)。

圖 7　掩護影像目標像素值位置示意圖

步驟二：除了步驟一之斜線部分作為參考值，如圖 7 所示，針對每一像素值，每次以 2×2 像素作為單位區塊進行邊緣預測，如圖 7 黑色粗體虛線框所示，以公式(12)判斷目標像素位置 x_i 屬邊緣或是平滑區，a_i 為目標像素位置 x_i 相鄰左側，b_i 為目標像素位置 x_i 相鄰上側，c_i 為目標像素位置 x_i 左上角相鄰位置。若 c_i 值大於或等於 a_i 與 b_i 的最大值，或 c_i 值小於或等於 a_i 與 b_i 的最小值，則目標像素位置 x_i 為邊緣，若 c_i 值介於 a_i 或 b_i 值之間，則目標像素位置 x_i 為平滑區。

$$c_i \geq max(a_i, b_i) \text{ or } c_i \leq \min(a_i, b_i) \tag{12}$$

步驟三：若目標像素位置 x_i 判定為邊緣(平滑)區塊，以公式(13)分別將目標像素位置 x_i 以 LSB 取代法藏入 k 位元秘密訊息(判定為邊緣區塊)或 k-1 位元秘密訊息(判定為平滑區塊)，而 s_i 為藏入秘密訊息之十進位值，亦會隨邊緣(平滑)區塊進行調整。

$$x'_i = x_i - (x_i \ mod \ 2^k) + s_i \tag{13}$$

步驟四：目標像素 x_i 以 LSB 取代法藏入後，以公式(14)計算目標像素 x'_i 與原本像素之差值d_i。

$$d_i = x'_i - x_i \tag{14}$$

步驟五：使用公式(15) 進行 OPAP 調整，針對 LSB 取代法藏入後目標像素位置 x'_i，得到目標像素位置 x''_i 。

$$x''_i = \begin{cases} x'_i + 2^k, if\ -2^{k-1} > d_i > -2^k \ and \ x'_i < 256 - 2^k \\ x'_i - 2^k, if\ 2^k > d_i > 2^{k-1} \ and \ x'_i \geq 2^k \\ x'_i \ , otherwise \end{cases} \quad (15)$$

步驟六：當單位區塊完成邊緣預測及秘密訊息嵌入後，整個黑色粗體虛線框向右位移 1 個像素，如圖 8 所示，進行下一個新的目標像素位置的邊緣預測及祕密訊息嵌入，以此類推，第一列執行完畢後，以 Z 字型方式換第二列類推，依序藏入秘密訊息，直至沒有下一個新的目標像素位置為止，即可獲得偽裝影像。

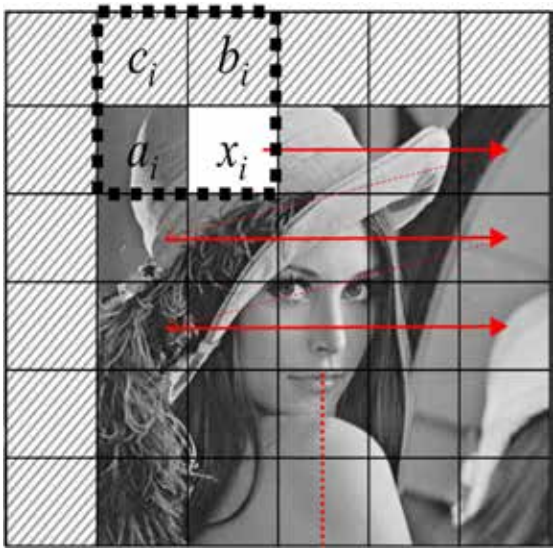


圖 8　掩護影像目標像素值位置位移示意圖

本研究方法藏密流程圖如圖 9 所示，因掩護影像為 512×512 之二維陣列，本研究提出之演算法須利用 2 層 for 迴圈控制其列與行之索引值，且第一列與第一行像素為 MED 預測保留區，故不列入計算，故其藏密演算法時間複雜度為 O(n^2)，其中 n 為影像之列(行)數。

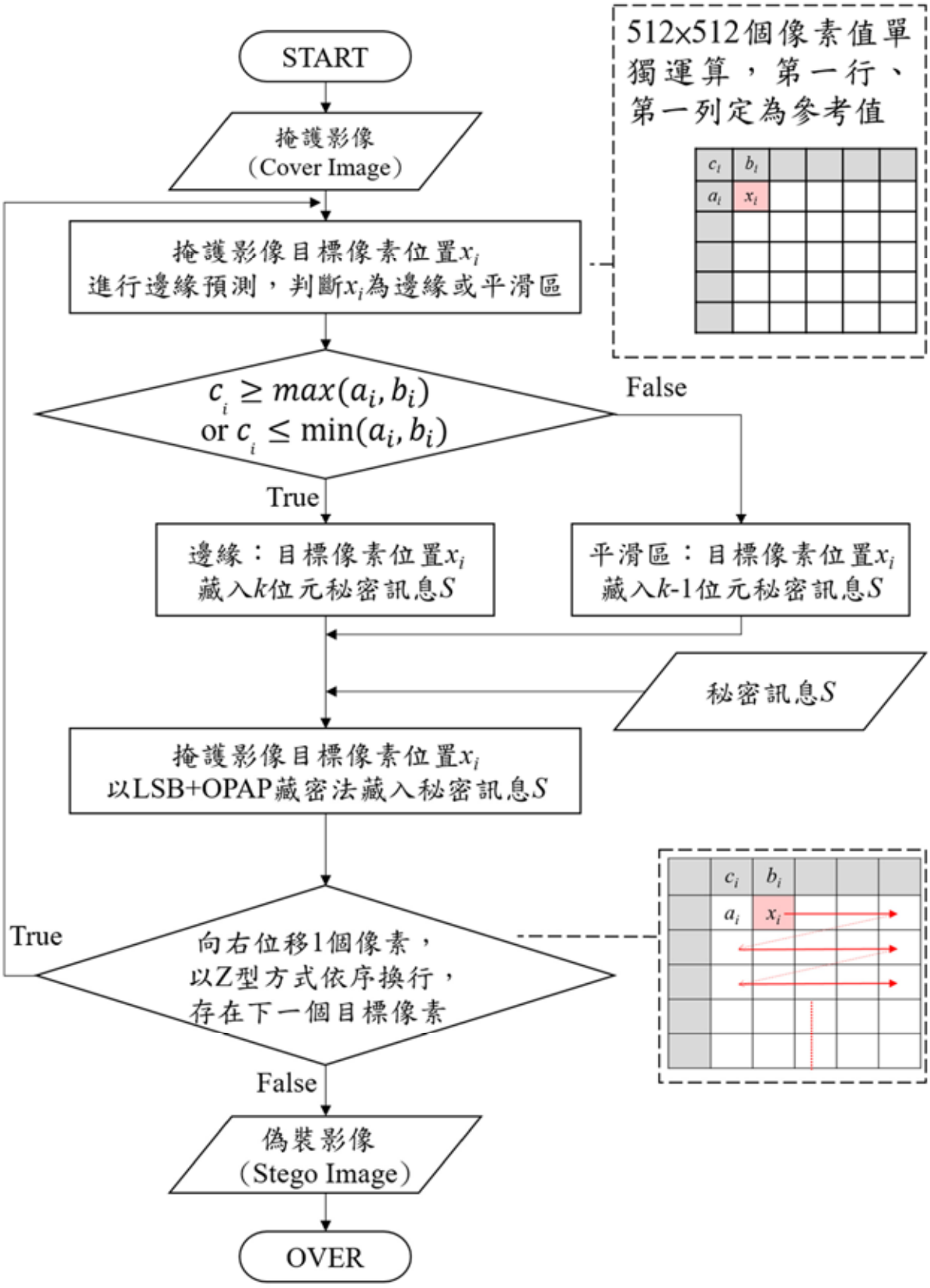
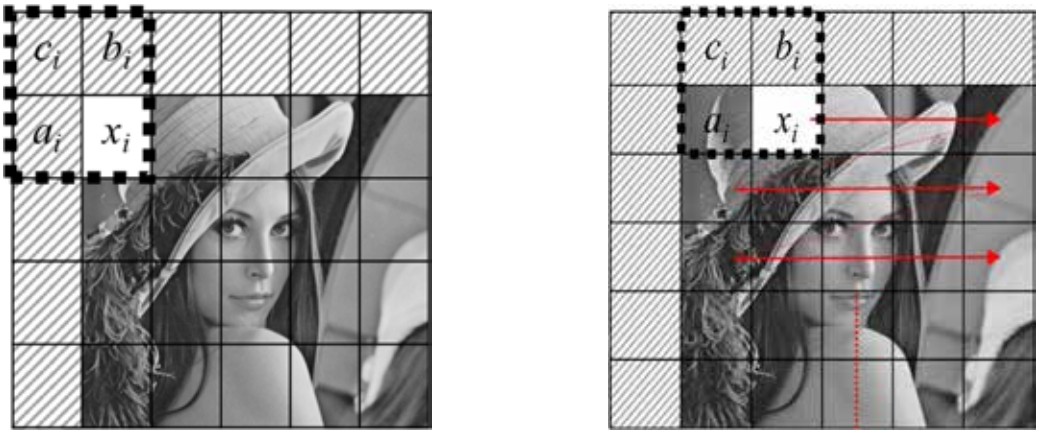

START
掩護影像
（Cover Image）
掩護影像目標像素位置x_i
進行邊緣預測，判斷x_i為邊緣或平滑區
512x512個像素值單獨運算，第一行、第一列定為參考值
c_i
b_i
a_i
x_i
$c_i \geq max(a_i, b_i)$
or $c_i \leq \min(a_i, b_i)$
False
True
邊緣：目標像素位置x_i
藏入k位元秘密訊息S
平滑區：目標像素位置x_i
藏入k-1位元秘密訊息S
秘密訊息S
掩護影像目標像素位置x_i
以LSB+OPAP藏密法藏入秘密訊息S
True
向右位移1個像素，
以Z型方式依序換行，
存在下一個目標像素
False
偽裝影像
（Stego Image）
OVER

圖 9　本研究藏密流程圖

3.2 本研究方法之取密程序

步驟一：藏密後之偽裝影像中，第一行與第一列中之各 512 個像素作為參考值，均不取出秘密訊息(如圖 10(a)斜線部分)。



(a) (b)

圖 10　偽裝影像目標像素值位置與位移示意圖

步驟二：除了步驟一之斜線部分作為參考值，如圖 10(a)所示，針對每一像素值，每次以 2×2 像素作為單位區塊進行邊緣預測，如圖 10(a)黑色粗體虛線框所示，以公式(12)判斷目標像素位置 x_i 屬邊緣區或是平滑區，a_i 為目標像素位置 x_i 相鄰左側，b_i 為目標像素位置 x_i 相鄰上側，c_i 為目標像素位置 x_i 左上角位置。若 c_i 值大於或等於 a_i 或 b_i 的最大值，或 c_i 值小於或等於 a_i 或 b_i 的最小值，則目標像素位置 x_i 為邊緣區，若 c_i 值介於 a_i 或 b_i 值之間，則目標像素位置 x_i 為平滑區。

步驟三：若目標像素位置 x'_i 判定為邊緣(平滑)區塊，以公式(16)分別將目標像素位置x'_i以模運算取出 k 位元秘密訊息(判定為邊緣區塊) 或 k-1 位元秘密訊息(判定為平滑區塊) ，而取出之 s_i 為藏入秘密訊息之十進位值。

$$s_i = \begin{cases} x'_i \bmod 2^k, & if\ x'_i\ is\ located\ at\ the\ edge \\ x'_i \bmod 2^{k-1}, & if\ x'_i\ is\ located\ in\ the\ non-edge\ area \end{cases} \quad (16)$$

步驟四：當單位區塊完成邊緣預測及秘密訊息取出後，整個黑色粗體虛線框向右位移 1 個像素，如圖 10(b)所示，進行下一個新的目標像素位置的邊緣預測及祕密訊息取出，以此類推，第一列執行完畢後，以 Z 字型方式換第二列類推，依序取出秘密訊息，直至沒有下一個新的目標像素位置為止，即可獲完整秘密訊息 S。

本研究方法之取密流程圖如圖 11 所示，因藏密影像為 512x512 之二維陣列，本研究提出之取密演算法須利用 2 層 for 迴圈控制其列與行之索引值，且第一列與第一行像素為 MED 預測保留區，故不列入計算，故其藏密演算法時間複雜度為 O(n^2)，其中 n 為藏密影像之列(行)數。

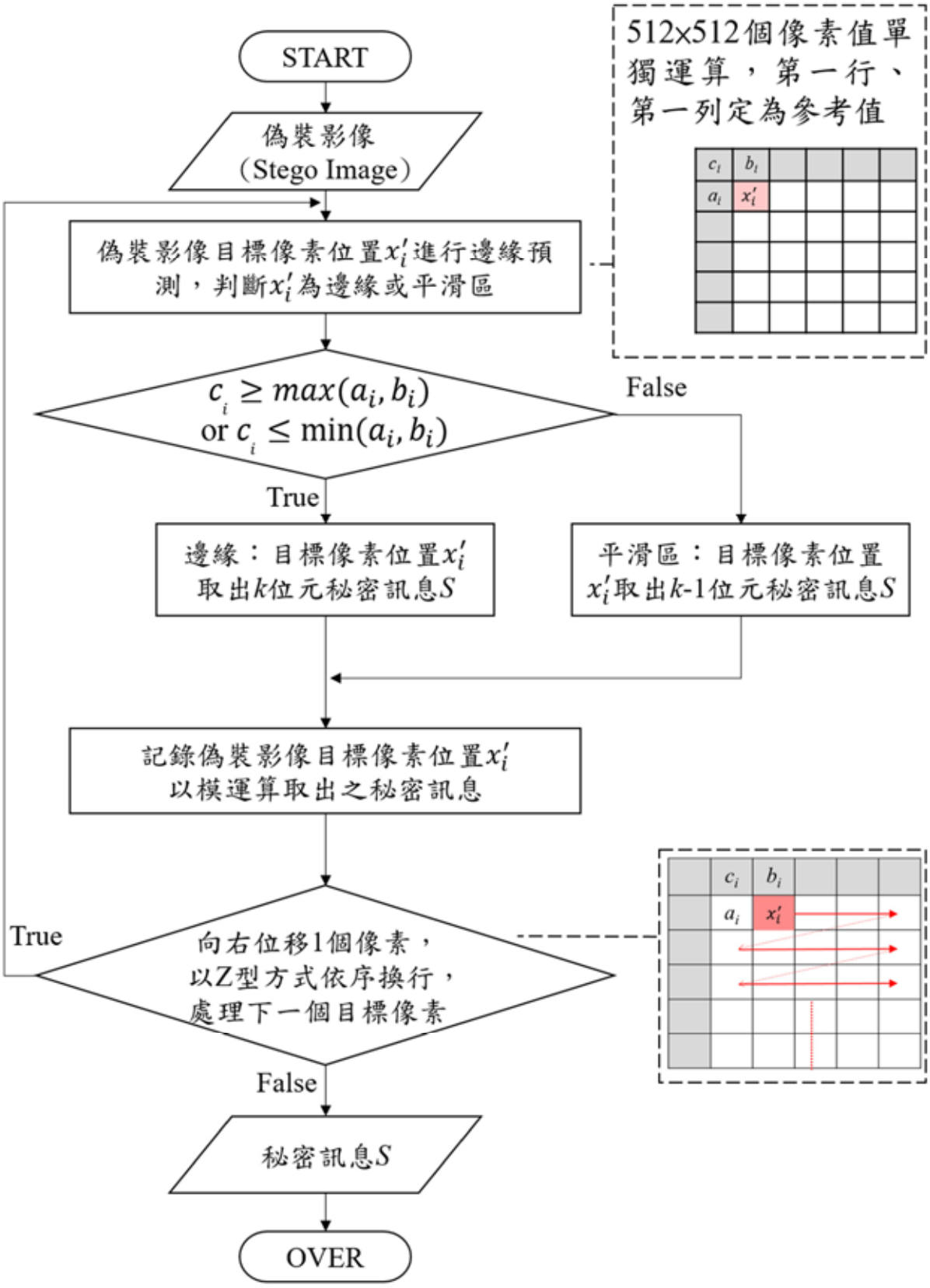


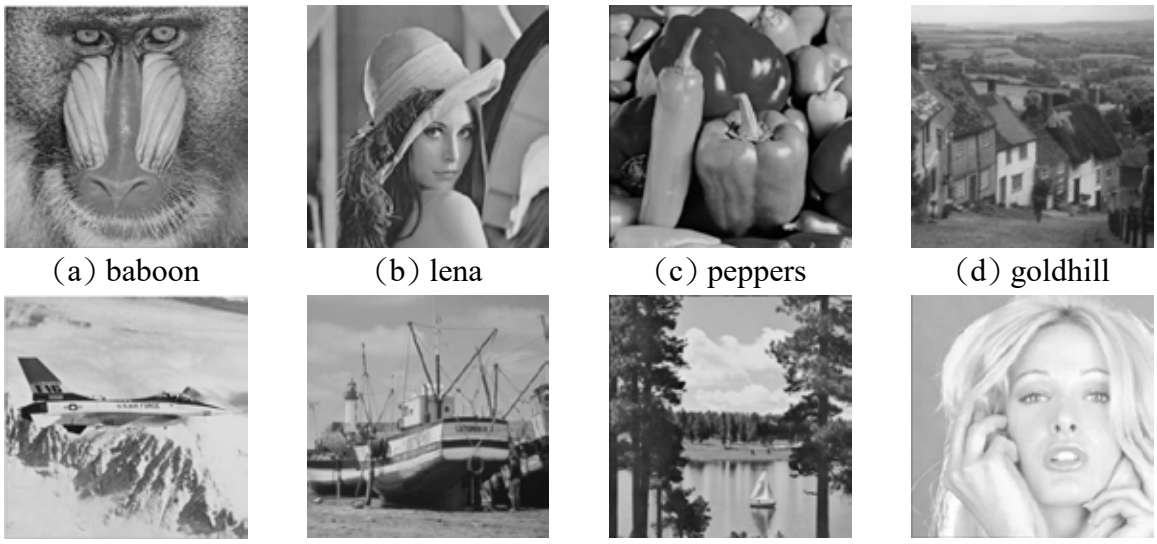
圖 11　本研究之取密流程圖

四、實驗結果與討論

4.1 實驗環境與素材

本研究使用筆記型電腦，作業系統為 MacOS 12.2.1、CPU Intel Core i5 2.0 GHZ，記憶體 16GB，以 Python 程式語言運用 Anaconda 中 Jupyter 進行程式撰寫，以驗證本研究提出的藏密及取密過程之正確性；並使用桌上型電腦，作業系統為 Windows 10、CPU Intel Core I5-6500 3.2 GHz，記憶體 16GB，採用 Matlab 進行安全性測試。

實驗過程運用資訊隱藏領域經常被廣泛使用之 Baboon 等 8 張 512×512 灰階測試影像為掩護影像(如圖 12)；其中包含紋理複雜影像及平滑影像，亦包含人像、風景照、物品及交通工具等影像，可用以代表大部分數位影像之內容。本研究嵌入的機密訊息以隨機亂數 0 或 1 的字串組成，實驗結果以藏密量、峰值訊號雜訊比(PSNR)及結構相似性指標(SSIM)作為衡量標準。



(a) baboon (b) lena (c) peppers (d) goldhill

(e) airplane (f) boat (g) lake (h) tiffany

圖 12　本研究使用之測試影像圖

4.2 實驗結果分析

實驗結果如表 1 所示，經對比 OPAP 藏密法及本研究所提出之藏密方法，在相同的圖片狀況下，OPAP 法僅能藏入 4bpp，本研究藏密方法最大可藏入 4.6bpp，且 PSNR 值均在人類視覺能夠忍受的範圍，證明本研究藏密方法能有效提升藏密量，並維持一定的影像品質。與近年 Liu 等學者於國際期刊所發表之高藏入量藏密法進行比較中，PVD 藏密法平均藏入量為 1.6bpp、平均 PSNR 值為 40.30dB，本研究藏密方法中，在 PSNR 值相當的狀況下，可藏入 2.7bpp(藏入值 k 為 3)；新式 LSB/PVD 藏密法平均藏入量為 3.1bpp、平均 PSNR 值為 37.16dB，本研究藏密方法中，在 PSNR 值相當的狀況下，可藏入 3.7bpp(藏入值 k 為 4)；以及 LSB/MPVD 藏密法平均藏入量為 3.7bpp、平均 PSNR 值為 34.84dB，本研究藏密方法中，在藏入量相當的狀況，平均 PSNR 值為 36.02(藏入值 k 為 4)。本研究所提之藏密方法產生之實驗結果與各方法比較值均較優，證明本研究藏密方法不只能維持較高的藏密量，同時能擁有較佳的影像品質。

表 1　本研究與其他方法之偽裝影像藏密量、PSNR 值比較表

測試影像	OPAP		PVD		New LSB/PVD		LSB/MPVD		本研究之方法					
	Chan and Cheng（2004）		Wu and Tsai（2003）		Khodaei and Faez（2012）		Liu et al.（2020）		*k*=5		*k*=4		*k*=3	
	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR
baboon	4	34.79	1.7	36.96	3.4	36.29	3.7	33.93	4.6	30.2	3.6	36.2	2.6	42.09
lena	4	34.84	1.6	41.18	3.1	37.63	3.7	35.35	4.7	30.03	3.7	35.98	2.7	41.85
peppers	-	-	1.6	40.61	3.1	37.97	3.7	34.89	4.7	29.72	3.7	35.86	2.7	41.78
goldhill	-	-	1.6	41.00	3.1	37.55	3.7	35.31	4.6	30.1	3.6	36.14	2.6	42.05
airplane	4	34.83	1.6	40.20	3.1	37.53	3.7	35.33	4.6	30.08	3.7	36.06	2.7	41.89
boat	-	-	-	-	-	-	-	-	4.6	30.1	3.7	36.07	2.7	41.9
lake	4	34.8	1.6	39.71	3.1	36.53	3.7	34.91	4.6	30.1	3.7	36.07	2.7	41.9
tiffany	-	-	1.6	40.89	3.1	37.79	3.7	34.76	4.7	29.57	3.7	35.78	2.7	41.72
average	4	34.81	1.6	40.30	3.1	37.16	3.7	34.84	4.6	29.99	3.7	36.02	2.7	41.9

本研究亦使用結構相似性指標(SSIM)作為衡量標準，SSIM 數值介於 0 至 1，越接近 1，兩影像越像似；如表 2 所示，本研究 k 值為 2,3,4 時，SSIM 值均接近 1，說明本研究藏密方法具有適應性強的特點，因此，偽裝影像和掩護影像之間的差異是微不足道的，雖然 SSIM 值在 k 值為 5 時差異較大，但在比較簡單的 Lena 圖和複雜的 Baboon 影像中，仍可存入穩定的藏密值，因此無論簡單或是複雜的影像，本藏密方法均能提供良好的藏密效果。

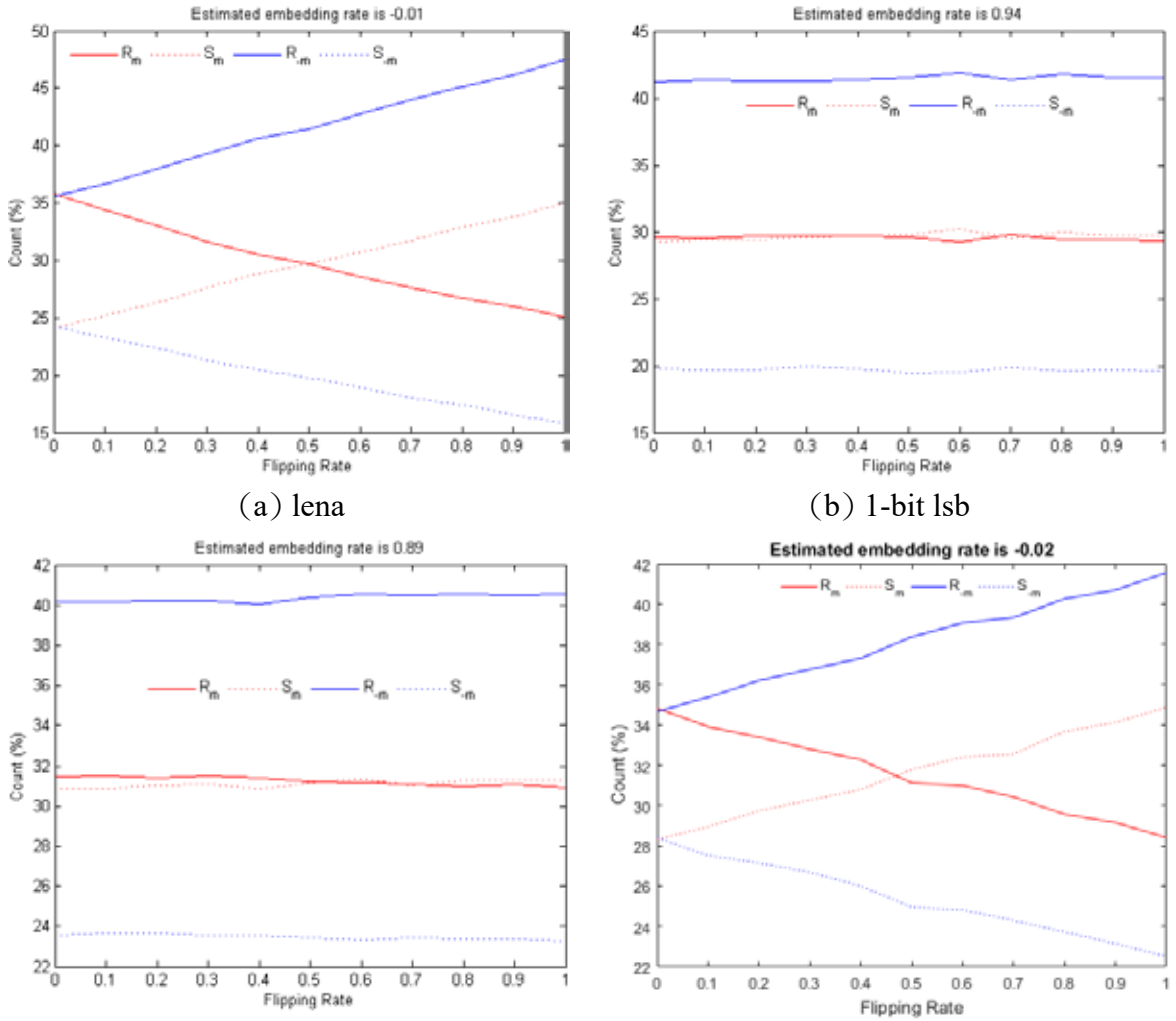
表 2　本研究偽裝影像與掩護影像 SSIM 值統計表

測試影像	*k*=5	*k*=4	*k*=3	*k*=2
	SSIM	SSIM	SSIM	SSIM
baboon	0.8774	0.9627	0.9901	0.9976
lena	0.6944	0.8893	0.9687	0.9923
peppers	0.6841	0.8885	0.9690	0.9922
goldhill	0.7684	0.9238	0.9795	0.9976
airplane	0.6764	0.8780	0.9647	0.9912
boat	0.7215	0.8973	0.9703	0.9925
lake	0.7590	0.9154	0.9759	0.9940
tiffany	0.6471	0.8732	0.9643	0.9912
average	0.7285	0.9035	0.9728	0.9936

4.3 安全性分析

資訊隱藏與密碼學研究，在秘密通訊應用上相輔相成，均是為了保障傳輸資料的安全，而密碼學之於破密，就如同資訊隱藏之於藏密偵知的關係，藏密偵知是利用偵測或分析技術，發現掩護媒體藏有秘密資訊就算成功。在藏密偵知的領域中，已有針對 LSB 取代法的影像隱藏偵測技術，經由統計方法計算影像像素對的特徵資料，即可有效偵測出藏密訊息長度的 RS 偵測技術(Fridrich, 2001)及卡方檢定法(Westfeld, 1999)。

本研究藏密方法是以 LSB 取代法為基礎將秘密訊息藏入掩護影像，為驗證本研究藏密方法之安全性，本研究採用 RS 偵測技術進行影像分析，獲得分析結果如圖 13 所示，圖 13(a)為 RS 偵測技術針對 Lena 原始影像之分析結果，圖 13 (b)與(c)分別針對使用 1-bit LSB 及 3-bits LSB 的 Lena 偽裝影像之分析結果，圖 13(d)為針對本研究藏密方法(k=4)所產生 Lena 偽裝影像之分析結果。從圖 13(a)-(d)之 RS 偵測結果可看出其所評估的藏密比率(embedding rate)分別為-0.01、0.94、0.89 及-0.02，表示 RS 偵測技術可有效偵測 LSB 藏密法，但無法有效偵測本研究藏密方法產生之偽裝影像，說明本研究所提植基於邊緣偵測及最佳像素調整的藏密法可有效抵抗 RS 偵測技術。



(a) lena　　(b) 1-bit lsb

(c) 3-bit lsb　　(d) 本研究偽裝影像(k=4)

圖 13　Lena 原圖、LSB 及本研究藏密產生偽裝影像之 RS 偵測分析圖

五、結論

本研究藉由簡化適性的高藏入量隱藏法，應用 MED 偵測法判定邊緣，並運用 LSB 與 OPAP 藏密法在平滑區嵌入較少秘密訊息、邊緣嵌入較多秘密訊息，藏密及取密演算過程簡易，能藏入高藏密量、維持一定的影像品質，與近年國際期刊所發表之高藏入量藏密法，在同樣的測試影像條件比較下，本研究提出之藏密方法，不只能維持較多的藏密量，產生之偽裝影像 PSNR 值亦較高，影像品質較佳，並通過 RS 偵測技術之安全性驗證，符合資訊隱藏技術特性中，效率性、不可察覺性、高隱藏容量、不可偵測性、安全性等目標。

資訊隱藏技術中重要之考量因素，其一是藏密量，其二為影像品質，此兩項往往是無法同時達成的。本研究尋求高藏密量的方法，並讓影像品質維持基本水準不失真的狀態，未來希望能夠依本研究成果為基礎，研究不同的邊緣偵測技術、調整藏入數量、更佳的像素調整方式，或可整合其他空間域之藏密技術，獲取更佳的藏密量或影像品質。

現代戰爭，將以資訊戰、不對稱作戰模式為主，在情報資訊掌握及傳達上，必需快速且準確，本研究提出透過簡單的邊緣偵測方法，達到高藏密量且不失真的資訊隱藏方式，且能避免運用統計分析技術，針對 LSB 取代法的影像偵測攻擊。此項藏密方法不需複雜的演算過程，透過國軍現行基本的軟硬體設備，即可將傳遞資訊藏入影像中，並從偽裝影像取出隱藏訊息，可提供國軍資訊安全管理技術研究領域參考應用。

參考文獻

王旭正、柯宏叡（2006）。資訊與網路安全－秘密通訊與數位鑑識新技法。新北：博碩文化。

王旭正、翁麒耀、林家禎（2012）。數位影像處理與應用。新北：博碩文化。

王旭正、翁麒耀、黃正達（2016）。數位資訊@多媒體安全與應用。新北：博碩文化。

左豪官、戴鑑廷、盧嘉鴻、婁德權、劉江龍、吳嘉龍（2007）。資訊隱藏技術之研究。*黃埔學報*，52，9-16。

冷輝世、張維剛、曾顯文（2013）。基於預測值與鄰近像素差值的標準差的可逆式資訊隱藏。TANET2013 臺灣網際網路研討會論文集，1-6。

吳南益、傅國欽、王宗銘（2010）。植基於像素差值與模數函數之新型灰階影像資料隱藏技術。*網際網路技術學刊*，11（7），1071-1081。

呂慈純、冷輝世、黃俊智（2014）。植基於邊緣偵測法及鏡射三角定位概念之資訊隱藏技術。*資訊科技國際期刊*，8（2），35-41。

陸哲明（2014）。信息隱藏概論。北京：電子工業。

張凱崴（2013）。資訊隱藏技術於軍事運用之研究。*陸軍通資半年刊*，119，95-119。

婁德權（2006）。藏密學發展現況。資通安全專論，T95010。

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for Data Hiding. *IBM System Journal*, *35*(3.4), 313-336.

Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, *37*(3), 469-474.

Fridrich, J., Goljan, M., & Rui, D. (2001). Detecting LSB steganography in color and gray-scale images. *Magazine of IEEE Multimedia Special Issue on Security*, *4*(4), 22-28.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46-66.

Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. *IET Image Processing*, *6*(6), 677-686.

Liu, H., Su, P., & Hsu, M. (2020). An improved steganography method based on least-significant-bit substitution and pixel-value differencing. *KSII Transactions on Internet and Information Systems*, *14*(11), 4537-4556.

Martucci, S. A. (1990). Reversible compression of HDTV images using median adaptive prediction and arithmetic coding. *IEEE International Symposium on Circuits and Systems*, *8*(2), 1310-1313.

Weinberger, M., Seroussi, G., & Sapiro, G. (1996). LOCO-I: A low complexity, context-based, lossless image compression algorithm. *Proceedings of Data Compression Conference - DCC 96*, 140-149.

Westfeld, A., & Pfitzmann, A. (1999). Attacks on Steganographic Systems. *Proceedings of the Third International Workshop on Information Hiding*, Dresden, Germany, 61-75.

Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, *24*, 1613-1626.

Zhou, W., & Bovik, A. C. (2002). A universal image quality index. *IEEE Signal Processing Letters*, *9*(3), 81-84.

Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, & Eero P. Simoncelli. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, *13*(4), 600−612.

基於區塊鏈技術建構多銀行數位交易機制之芻議

蘇品長 黃琬玲*

國防大學資訊管理學系

論文編號：NM-44-01-06
DOI：10.29496/JNDM.202405_45(1).0003
來稿2022年9月22日→**第一次修訂**2023年2月3日→**第二次修訂**2023年4月10日→
同意刊登 2023 年 4 月 19 日

摘要

近年來網際網路及資訊科技日益發展，區塊鏈已成為全球新興科技趨勢，一旦成功應用於軍事事務，將有助於提高部隊戰鬥力，並促成軍隊轉型發展。其中區塊鏈技術已在金融行業進行了廣泛的實驗、研究和應用，本研究透過區塊鏈分散式帳本、去中心化、資料難以竄改、匿名性等技術及密碼學理論基礎，並運用智能合約導入多銀行數位交易支付機制，解決目前電子商務中跨銀行及第三方來進行支付存在之安全性及信任問題，透過去中心化的系統，降低第三方參與，免除實體貨幣兌換程序並避免電子現金重複消費之問題，有效提升買賣雙方信任度，增強支付機制安全性，可適時導入國軍數位電子現金發行構想，強化數位交易安全機制，提升整體國防財務及後勤管理戰力。

關鍵詞：區塊鏈、智能合約、多銀行數位交易、金融服務、電子支付

*聯絡作者：黃琬玲 email: florence9839@gmail.com

Discussion on the Construction of Multi-Bank Digital Transaction Mechanism Based on Blockchain Technology

Su, Pin-Chang　Huang, Wan-Ling*

Department of Information Management, National Defense University,
Taiwan, R.O.C

Abstract

In recent years, the Internet and information technology have developed rapidly, blockchain has become a global emerging technology trend. Once it is successfully applied to military affairs, it will help to improve the combat effectiveness of the troops and facilitate the transformation and development of the military. Blockchain technology has been extensively experimented, researched and applied in the financial industry. This research uses the technology and cryptography theoretical foundation of the blockchain, such as distributed ledger, decentralization, data hard to tamper, anonymity, and uses smart contracts to import multi-bank digital transaction payment mechanism. It can solve the security and trust problems existing in the current e-commerce for payment across banks and third parties. Through a decentralized system, it can reduce third-party participation, eliminate physical currency exchange procedures, and avoid the problem of double consumption of electronic cash. It can effectively improve the trust between buyers and sellers, and enhance the security of the current payment mechanism. Introduce it into the ROC Armed Forces digital electronic cash issuance concept can strengthen the digital transaction security mechanism and improve the overall defense financial and logistics management capabilities.

Keywords: Blockchain, Smart Contracts, Multi-bank Digital Transactions, Financial Services, Electronic Payments

*Corresponding author: Huang, Wan-Ling email: florence9839@gmail.com

一、前言

因應數位時代的變革，我國傳統金融體系已於 2019 年逐步朝向「開放銀行」(Open Banking)及「開放應用程式介面」(Open Application Programming Interface; Open API)方向轉型，使金融服務的使用者可以取得資料的自主權，而未來趨勢將很有可能結合區塊鏈(Blockchain)技術，實現去中心化的金融服務(彭思遠，2021)，國際研究暨顧問機構 Gartner 也發表，預估於 2030 年，區塊鏈可能帶來高達 3.1 萬億美元的新商業價值，並估計在 2025 年時，其中一半金額所帶動的附加商業價值是為了改善現行營運作業流程而產生的(Gartner, 2022)；另分析師 Avivah Litan 表示區塊鏈將成為未來金融體系的主流，讓交易變得更加安全。

在區塊鏈技術興起之前，網路交易大部分都必須仰賴金融機構作為可信賴的第三方，然而在這種基於信用的模式下，消費者所有交易資訊、機敏資料均儲存及掌控在第三方手上，消費者對於第三方必須完全信任，並且無法參與驗證（李宛蓁與黃杭浔，2016)。近年來，區塊鏈技術不斷發展，利用其去中心化、分散式帳本、不易竄改、智能合約(Smart contract)及共識機制等特性，逐漸影響到各行各業，其中在金融服務領域中，最令人關注和期待(黃敬翔，2019)，主要是因為透過區塊鏈技術可以有效降低交易及營運成本，提高監管能力並消除不必要的中介，建立分散式信任，並促進銀行間交易支付過程(Ramchandra et al., 2022)，而去中心化金融服務和商業模式，使的金融體系得以跨國界、交易自由，並更加透明化及創新發展(Chen and Bellavitis, 2020)。

在傳統支付過程中，多以實體貨幣(現金、紙鈔、硬幣)作為支付工具，隨著數位產業及電子商務發展，我國消費型態逐漸改變，電子支付日益普及，根據金融監督管理委員會(金管會)統計，截至 111 年 6 月底止，使用人數已多達 1 千 7 百餘萬人(金管會，2022)，未來電子支付將會成為支付工具的主流；常見的電子支付機制包含信用卡型、帳戶型與電子現金型三種方式，其中電子現金的概念與傳統貨幣較為接近，使用上的風險與交易成本相對較低，因此深受消費者喜愛，另在向金融機構申購時會留下申請開戶紀錄，在使用上具有匿名性，可保障消費者的隱私與帳戶的安全（郭木興，2003)。然而在眾多發行電子現金的銀行中，各個機構彼此為封閉體系，電子支付系統亦屬於封閉體系，無法進行跨機構間款項轉移(楊金龍，2019)；集中式的數據儲存具有單點故障、傳輸中斷、資料遺失的風險(Liao et al., 2022)，商家在收到不同銀行所發行之電子現金須有發行銀行之公開金鑰或是驗證資訊，才能驗證所收到電子現金的合法性(曹偉駿與蔡欣潔，2010)，在管理上造成不便；跨銀行進行電子現金款項轉移時，因系統無法互通，需透過存放在中央銀行的準備金，負擔交易清算成本，進行跨銀行清算(楊金龍，2019)；另在電子商務中，為了確保消費者與商家雙方交易的安全性、完整性、不可否認性及驗證用戶身分，必須透過公開金鑰基礎建設(Public Key Infrastructure; PKI)來實現，由憑證中心(Certificate Authority; CA)確認身分資訊，使用公鑰來簽發憑證，然而當憑證中心系統遭受駭客攻擊入侵竄改時，將對用戶身分資料保密性、完整性、不可否認性及真實性等造成極大的危害(蘇品長等，2014)。

因此本研究規劃將運用區塊鏈技術結合智能合約與密碼學原理，設計一個具安全性數位交易支付機制，由多銀行組成聯盟鏈，共同維護帳本，透過區塊鏈即時完成跨銀行清算，達到金流互通、資訊流同步一致與資料長時保存的效益，改善銀行之間系統介接及系統維運的成本，提升商家與消費者便利性；而在區塊鏈架構下之多銀行共同參與支付機制需考慮在區塊鏈上匿名監管問題，建立完善的信任機制，因此導入自我認證機制，解決憑證中心可能無法信任導致資訊安全的問題，使銀行、消費者、商家等電子商務中的參與人員身分資料達到完整性、不可否認性及真實性，有效提升交易安全；透過部份盲簽章方式實施電子交易支付，於交易過程確保電子現金有效性，

避免交易內容遭洩漏，亦可解決已簽署之電子現金難以辨識其額度或時效的問題，進而達成電子商務交易安全性，促進電子支付的發展，具備以下優點：

（一）透過區塊鏈結合智能合約設計，達成多銀行金流互通、資訊帳本同步一致及系統自動化，避免資料偽冒及遭竄改之風險。

（二）應用橢圓曲線部份盲簽章技術於電子支付過程，避免交易資訊在傳送過程遭有心人士非法竊取，並可確保電子現金有效性。

（三）運用橢圓曲線特殊點加法運算及其在與 RSA 相同的安全複雜度之下，僅需較小的密鑰長度，可以避免大量的指數運算，有效降低系統負荷，並達到機密性(Confidentiality)、完整性(Integrity)、不可竄改(Immutability)及不可否認性(Non-repudiability)等資安特性，強化電子商務交易安全度。

二、文獻探討

本章節分類整理、歸納分析與本研究相關聯之文獻，並針對區塊鏈、金融服務、電子支付及密碼學等與本研究相關的技術，加以彙整作為本研究的基礎，分述如后：

2.1 區塊鏈介紹

區塊鏈技術日新月異，隨著比特幣問世後，持續不斷演進，如今已成為一項具前瞻性和獨立研究的技術領域，目前在金融、能源、物聯網、健康、供應鏈、保險、媒體等不同領域中快速發展與應用(Chen et al., 2020)，本章節彙整區塊鏈緣起與發展、區塊鏈技術與架構、區塊鏈特性與類型實施介紹，分述如后：

2.1.1 區塊鏈緣起與發展

在 2008 年爆發全球金融風暴，中心化的機構已無法被完全相信，而由中本聰於是年所發表的論文，一篇名為「比特幣：一種點對點的電子現金系統」的白皮書，內容描述比特幣及相關演算法，提出一種新的電子現金系統，採用點對點網路(Peer-to-Peer; P2P)，不須倚賴可信任的第三方執行交易(Nakamoto, 2008)，於 2009 年比特幣誕生，成為一種新型態的數位貨幣；而比特幣即是採用區塊鏈技術為底層架構的加密貨幣，區塊鏈在本質上是一種去中心化的分散式帳本資料庫，透過密碼學演算法，由一串鏈接的區塊所組成，確保區塊內的交易數據不可竄改，在沒有中心的節點控制下，保證資料一致性(鄒均等，2018)。而區塊鏈系統的三個重要屬性，去中心化、安全性和可擴展性，需達成平衡與兼顧，因此在區塊鏈去中心化架構下，尚需考慮安全及效率之問題，如區塊交易速度、智能合約安全性等問題等，目前針對學術界的發展現況和研究，和將區塊鏈的演進區分為區塊鏈 1.0、2.0 及 3.0 三種層次，摘述如后：

(一)區塊鏈 1.0

區塊鏈 1.0 為數位貨幣應用，它指的是透過區塊鏈分散式帳本技術為基礎，利用共識和挖掘機制來交換數位貨幣的概念，打造一個不需仰賴第三方的金流系統，如匯款、轉帳及數位支付系統等，將交易從一個用戶直接轉移到另一個用戶，其中最具代表性為比特幣，自 2009 年比特幣推出以來，相較傳統貨幣它證明了其可靠性、獨立性和安全性(Lee et al., 2021)，而在區塊鏈支付系統中，Hu 等學者(2019)提出一種基於以太坊區塊鏈的支付方案，在偏鄉地區實際驗證金融交易是可以穩定運行，確認區塊鏈在交易支付上具可擴展性。

(二)區塊鏈 2.0

區塊鏈 2.0 是數位經濟，被稱為是在數位貨幣之外的金融應用，利用智能合約，依照預先指定的概念和規則，可以自動執行各種業務流程，徹底改變傳統金

融交易和支付系統，此類應用包含去中心化金融(DeFi)、證券交易、供應鏈金融等，是更廣泛的經濟和更金融應用(Cheng et al., 2021)，由於智能合約程式碼是開源的，因此在開發時需透過相關工具(如 FSolidM、KEVM、MAIAN、Securify、Mythril)，進行漏洞和安全性檢測，避免遭受惡意攻擊(Di Angelo, 2019)。

(三)區塊鏈 3.0

區塊鏈 3.0 是在數位貨幣和金融以外，一種以信任為核心價值的新型經濟形式，推廣至政府、健康、科學、文化和藝術等各領域的應用，並側重於對社會去中心化的監管和治理(Swan, 2015)，各領域可透過區塊鏈技術改善原有的業務模式及生活，區塊鏈最具未來性的前景應用是智慧城市，包含智慧治理、智慧生活、自然資源智慧利用、智慧市民、智慧經濟等要素(Sun et al., 2016)。

2.1.2 區塊鏈技術與架構

一個完整的區塊鏈系統並非單一技術，其中包含儲存數據的區塊、數位簽章、時間戳、點對點網路架構及共識演算法等，而區塊鏈的核心技術是在沒有中心化的控制及無信任基礎的情況下，透過共識機制達成共識，並由節點之間共同維護分散式資料庫(鄒均等，2018)，每個區塊包含多筆交易，而每個區塊中包含前一個區塊的雜湊值、此次區塊的雜湊值、隨機數、當前困難度、區塊產生的時間戳、交易紀錄、挖掘礦工及礦工獎勵(李耕銘，2021)，區塊鏈架構如圖 1 所示。

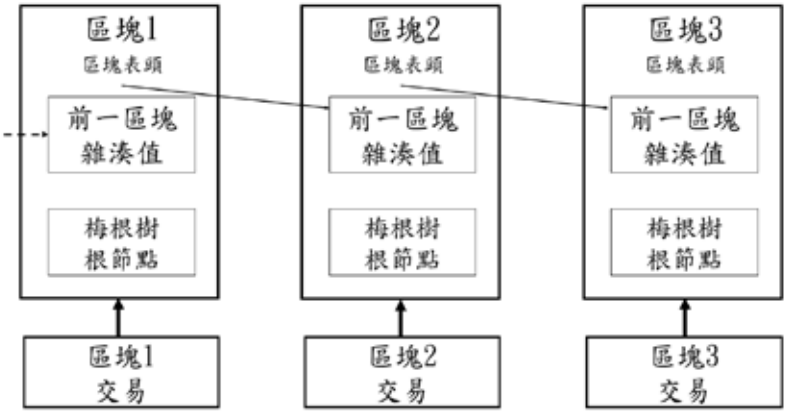


圖 1　區塊鏈架構示意圖
資料來源：鄒均等(2018)

2.1.3 區塊鏈特性與類型:

區塊鏈是由數學、密碼學原理及演算法所組成，其主要具備五大特性，其一為匿名性，各節點在區塊鏈上以不具名方式參與，使用代碼作為名稱，各節點之間是基於交易錢包與交易地址而非個人身分進行資料交換。其二為不可竄改性，當交易紀錄打包成區塊，並同步至各節點，當節點欲竄改區塊鏈資料，則需具備 51%全節點算力，因此任一節點無法任意竄改資料，交易資料具備高可信度。其三為去中心化，無第三方驗證機構單位，採用點對點分散式儲存機制，資料由節點與節點之間共同維護，並驗證訊息真實性。其四為可追溯性，區塊鏈上資料環環相扣並，資料上區塊鏈後都會被記錄，交易紀錄時間序列無法更動，具備可追溯性。其五為共識機制，當新的區塊被廣播到整個區塊鏈網路，節點將交易打包成一個區塊，並加入區塊鏈中，交易紀錄被鏈上的其他參與者確認並接受。

依據區塊鏈的參與者、去中心化程度及應用規模，可分區為「公有鏈」、「私有

鏈」及「聯盟鏈」，其特性如表 1 所示。

(一)公有鏈

公有鏈是高度去中心化的，帳本完全公開透明，參與節點無需經過授權，任何人都可以參與，並在公有鏈上進行資料發送、接收、存取及交易認證，其中比特幣和以太坊是兩個發展最著名的公有區塊鏈。

(二)聯盟鏈

聯盟鏈即是兩種區塊鏈的混合，由聯盟與多個組織共同構建，是需要經過授權的，可以滿足私有鏈的隱私性，又能達到公有鏈共識機制的特性，每個組織都是區塊鏈的一個節點，如果其他組織想要加入聯盟區塊鏈，需要聯盟的授權。

(三)私有鏈

私有鏈僅由一個組織控制，該組織建立並規範授權規則，控制誰可以參與、執行共識和維護共享帳本，參與私有鏈的節點受到嚴格的控制，資料發送、接收、存取及交易權限均受到限制，因此私有鏈交易速度較快，性能較佳。

表 1　區塊鏈特性

類別	公有鏈	聯盟鏈	私有鏈
公開程度	高	中	低
權限	不須授權	須經授權	須經授權
交易速度	低	中	高
可擴展性	低	中	高
去中心化程度	高	中	低
成本	低	中	高
典型代表	Bitcoin、Ethereum	Hyperledger Fabric、Corda	Quorum

資料來源：Zhang and Huang (2022)

2.2 區塊鏈導入金融服務介紹

在金融領域中，透過區塊鏈架構作為一種新的交易底層技術，有效整合金融資訊，提升系統的運行效率和服務質量(Zhang et al., 2020)，本章節介紹區塊鏈導入我國金融服務之發展潛力與效益，摘述如后：

2.2.1 貿易/供應鏈融資

中國信託銀行於 2016 年加入全球區塊鏈組織，發展數位金融，於 2019 年 10 月奇美實業出貨給波蘭的進口商，透過開發的「國際區塊鏈信用狀平臺」，擔任交易過程中的押匯行，完成我國首筆真實交易，利用區塊鏈去中心化、即時傳輸、無法竄改、公開透明及可溯源的特色，將作業流程從 5 天縮短至 1 天，並簡化實體文件傳遞流程，有效提升交易安全性及國際貿易效率(魏喬怡，2019)。

國泰世華銀行於 2021 年與 7 大銀行(上海商銀、台中銀行、新光銀行、陽信銀行、遠東商銀、元大銀行、永豐銀行)、2 大航運商(陽明海運、長榮海運）組成「環球貿易共享區塊鏈」，透過安全雜湊演算法技術，運用於現行進出口貿易融資，如圖 2 所示，將銀行貿易融資的資訊公開化，提高可信度，使各銀行可防範企業重複融資，並達成在保護雙方隱私的前提下，於區塊鏈上驗證供應商提供之交易文件及航運業者的貨運文件，比對各聯盟銀行傳送之交易資訊，增強風險控管作為(國泰金控，2021)。

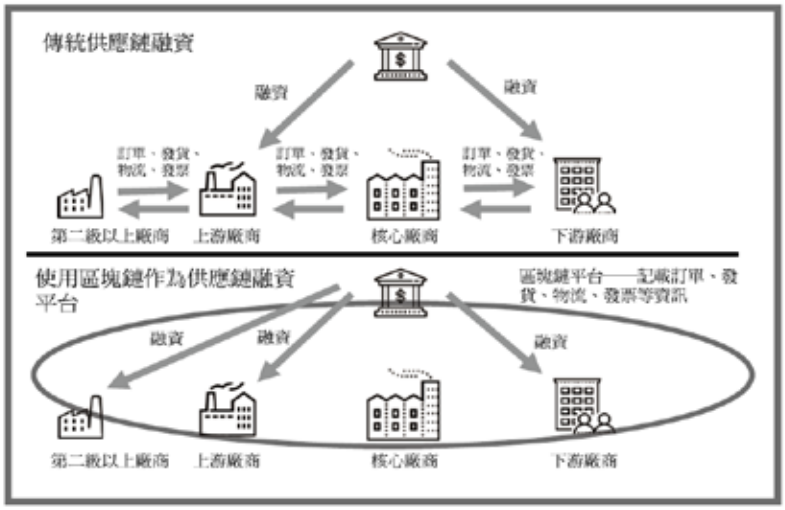


圖 2　區塊鏈供應鏈融資架構

資料來源：黃敬翔(2019)

2.2.2 函證

函證(Confirmation)是指會計師事務所在稽查企業財務報表時，向金融業者發詢證函，並取得相關查核證據的審核程序，為了提高資訊透明化並以企業永續經營為目的，財金公司、財團法人中華民國會計研究發展基金會、金融機構及四大會計師事務所，共同制定統一資訊標準，於 107 年合力建置「區塊鏈函證服務平臺」(李于宏，2021)。透過區塊鏈函證平臺將銀行函證自動化及資訊化，將原本紙本郵寄方式改為透過區塊鏈平臺加密傳送，解決人工填寫易發生誤填、遺失、竄改及舞弊的問題，確保資料來源正確性及安全性；另於區塊鏈上記錄函證資料，相關紀錄均無法修改或遭竄改，解決傳統企業及銀行可能偽冒資料之風險，相關業管單位可隨時掌握執行狀況，提高審核作業時效(財金資訊股份有限公司，2021)，函證作業流程如圖 3 所示。

圖 3　金融區塊鏈函證作業流程

資料來源：財金資訊股份有限公司(2020)

2.3 電子現金相關研究

電子現金即是將傳統的紙本現金以電子數位的方式存在，並透過密碼學技術產生一序列的編碼資料，與傳統的貨幣一樣具有唯一性及不可偽造的特性，在交易階段利

用電子設備以網路連線傳送給商家完成支付作業，提供安全便利之資金移轉服務，現行貨幣比較如表 2。而在典型的電子現金系統包含客戶、銀行（發行方或收單方）和商家三個角色，交易內容包含開戶、提款、支付和存款協議，主要流程為客戶從銀行提取電子現金，使用電子現金交易支付給商家，最後商家將其電子現金存入銀行的過程(Chen et al., 2011)，以下描述 Wang、Tsaur 和 Li 等學者所提出之電子現金支付之研究。

表 2　貨幣比較表

項目	傳統現金	電子現金	虛擬貨幣
來源	中央銀行貨幣	電子貨幣	虛擬貨幣
發行機構	中央銀行	金融機構	任一機構
存在形式	實體	數位	數位
轉移模式	硬幣/紙張	帳戶基礎	代幣基礎
耐久度	易損毀	永久保存	永久保存
攜帶便利性	不易攜帶	易攜帶	易攜帶
發行量	由中央銀行決定	限量發行	限量發行
法償效力	具備	具備	不具備

2.3.1 Wang 等學者電子現金支付機制

2007 年 Wang 等學者提出了一個基於群簽章的公平和可轉移的多銀行離線電子現金系統，由可信任的第三方擔任憑證中心，達成用戶的身分識別，防止舞弊勒索行為，確保電子現金公平交易，並由多個銀合組成一個群體，由中央銀行擔任群組管理者，透過群盲簽章達成聯合發行電子現金的目標，使消費者可以匿名消費，當商家取得群體之公開金鑰後，即可驗證由不同銀行發行之電子現金合法性，系統交易流程如圖 4 所示(Wang et al., 2007)。

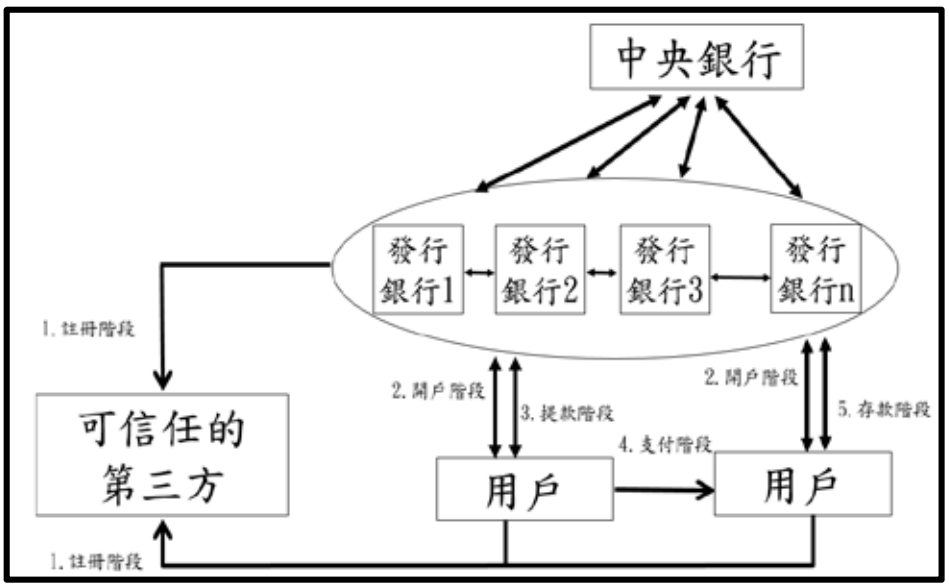


圖 4　多銀行發行離線電子現金系統交易流程
資料來源：Wang et al.（2007）

2.3.2 Tsaur 等學者電子現金支付機制

2018 年 Tsaur 等學者於提出的一種基於橢圓曲線的部份盲簽章電子現金系統，該研究方案由多銀行共同發行的行動電子現金系統，利用橢圓曲線設計之部份盲簽章技

術，解決已簽署之電子現金難以辨識額度與時效的問題，並可改善銀行資料庫迅速成長的情形，提高執行效率並降低計算和通信的成本，並透過自我認證公開金鑰密碼系統，使用者能自行驗算系統中心傳送的公鑰正確性，使得系統中心無法掌握公開金鑰的產生與驗證，系統交易流程如圖 5 所示(Tsaur et al., 2018)。

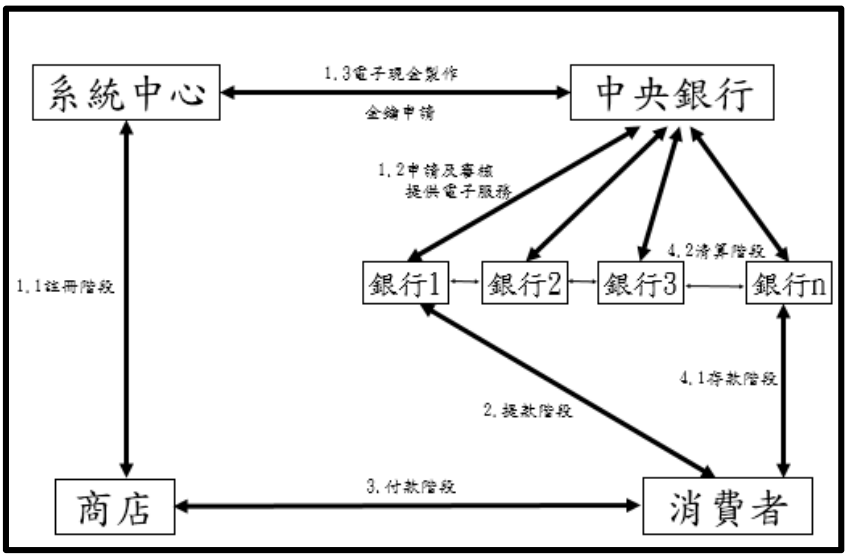


圖 5　多銀行發行電子現金系統交易流程
資料來源：Tsaur et al.（2018）

2.3.3 Li 等學者電子現金支付機制

2019 年 Li 等學者提出的一個高效的公平離線電子現金方案，該研究方案中由中央銀行擔任一個可信任的中央金融機構擔任憑證中心，負責發佈憑證，利用非交互式零知識證明技術，在不公開資訊的情況下，驗證身分及電子現金之合法性，可達成多個銀行發行電子現金之目的，在不受電子現金發行銀行的限制下，驗證電子現金合法性，並合乎電子現金匿名性、不可重複消費、不可偽造性和可追溯性相關的安全屬性，系統交易流程如圖 6 所示(Li et al., 2019)。

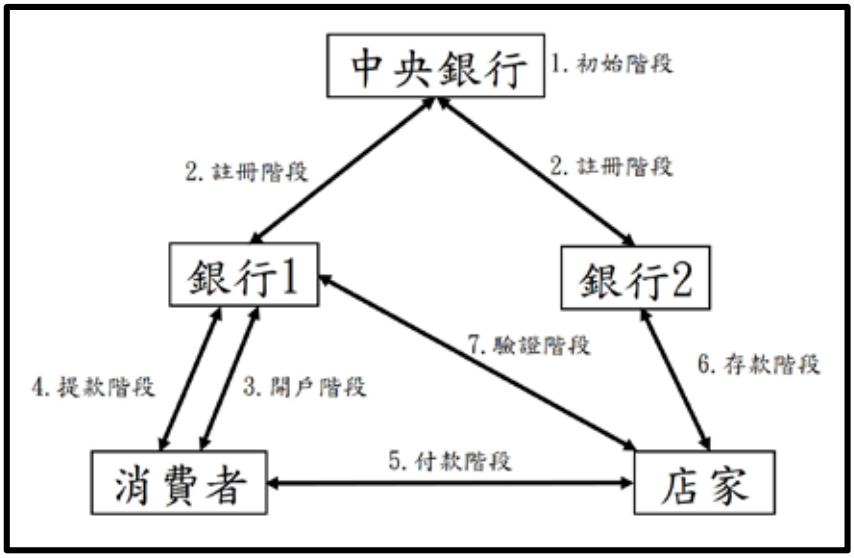


圖 6　標準模型下多銀行的公平離線電子現金流程圖
資料來源：Li et al.（2019）

2.4 密碼學理論

本章節彙整本研究應用之密碼學理論。

2.4.1 橢圓曲線密碼系統

由 Miller(1985)及 Koblitz(1987)兩位學者分別提出將橢圓曲線應用在密碼學上，主要是利用橢圓曲線特殊點加法及反元素的特性，將其運用在公開金鑰加密系統上，一般方程式為：$y^2+axy+by=x^3+cx^2+dx+e$，其中 a、b、c、d、e 為實數，通常以$y^2=x^3+ax+b$方程式來表示，其優點是運用點加法運算，解密者必須窮舉所有可能的點才能破解密鑰，而此問題至今尚無法於多項式時間內求得解答，另在相同安全複雜度下，加密金鑰的長度較 RSA 短，現行依美國國家標準暨技術研究院(National Institute of Standards and Technology; NIST)所制定之國際標準，橢圓曲線簽章及驗證要求之金鑰長度皆大於或等於 224 位元(Barker and Roginsky, 2019)，金鑰比較如表 3 所示。

在 Galois Field 有限域 $GF(p)$ 中，取質數 p （p>3）同餘的橢圓曲線群，以$E: y^2=x^3+ax+b(modp)$來表示，其中 a、b 為小於 p 之正整數，且$4a^3+27b^2\neq 0(modp)$，假設$M(x_1,y_1)$與$N(x_2,y_2)$為 $GF(p)$ 上的點，在橢圓曲線上點加法其具有以下規則：

(一) $M+O=O+M=M$。

(二) 當$M=-N$，表式N為$(x_2,-y_1)$，則$M+N=(x_1,y_1)+(x_1,-y_1)=O$。

(三) 當$M\neq -N$，則$M+N=(x_3,y_3)$，且$x_3=(\lambda^2-x_1-x_2)$，$y_3=\lambda(x_1-x_3)-y_3$，此處：

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & if\ M\neq N\\ \dfrac{3x^2+a}{2y_1} & if\ M=N\end{cases}$$

(四) 為了加速運算，橢圓曲線中利用加法運算達成乘法運算，如：$4M=2M+2M$，再計算$2M=M+M$即可。

(五) 反元素運算：當點$N=(x,y)$的反元素為$-N=-(x,y)=(x,-y)$。（因$N+(-N)=O$，O即為乘法單位元素）

表 3　橢圓曲線密碼系統與 RSA 在相同安全複雜度下金鑰長度之比較表

橢圓曲線密碼系統與 RSA 金鑰長度在相同安全複雜度下之比較					
長度 / 項目	金鑰長度				
橢圓曲線密碼系統	112	163	224	256	384
RSA	512	1024	2048	3072	7680
金鑰長度比	1：5	1：6	1：9	1：12	1：20

資料來源：蘇品長(2007)

2.4.2 部份盲簽章

盲簽章是 1982 年由 Chaum 所提出的一種基於 RSA 的電子簽章，其概念為使用者將訊息利用盲因子盲化後，傳送給簽章者進行簽名，而簽章者收到盲化過的訊息，故無法得知其訊息內容，最後驗證者可利用簽章者的公鑰，驗證簽章的正確性，具有保護使用者隱私的特性，所以可被應用於網際網路環境下的電子現金系統及投票場景保護用戶隱私的安全性問題。

然而，盲簽章後續在電子現金的應用上出現兩個問題，其一為銀行必需留存已使用的電子現金防止雙重支出，導致資料庫無限增長，其二為簽章者必須在無法確認電子現金面額之情況下，完全相信所簽署內容；為了解決上述問題，Abe 和 Fujisaki 於 1996 年提出植基於 RSA 部份盲簽章的概念(Abe and Fujisaki, 1996)，簽章者在簽章時，

可得知部份簽章內容，其餘隱私之內容簽章者無從得知，演算法區分 5 個階段：

(一) 初始階段：

銀行隨機選擇兩個大質數p,q，然後接著計算：

$$n = p \cdot q 及 \emptyset(n) = (p-1)(q-1)$$

決定一公開金鑰及私密金鑰對為e,d，滿足：

$$ed \equiv 1(mod\emptyset(n))及gcd(e,\emptyset(n)) = 1，且e,d < \emptyset(n)$$

銀行對外公佈公開金鑰(e,n)及單向雜湊函數$H()$，對內自行保有私密金鑰(d,p,q)，並且讓每筆發出的電子現金都價值w元。

(二) 盲化階段：

假若消費者決定向銀行提領電子現金，他隨機選擇隨機選取一盲因子r和亂數m，$m,r \in Z$，並計算：

$$\alpha \equiv r^{ev}H(m)modn$$

v為事先與銀行定義好的公開訊息，包含電子現金的面額和有效期限，並將部分盲訊息(α,v)傳給銀行。

(三) 簽章階段：

銀行收到(α,v)之後，先確認v是否正確，假如正確無誤，計算：

$$\beta \equiv \alpha^{(ev)^{-1}}modn$$

從消費者在銀行的帳戶內扣除w元，並傳送β給消費者。

(四) 去盲階段：

消費者收到β後，消除盲因子r，計算：

$$s = r^{-1}\beta modn$$

消費者即得到自己購買的電子現金(m,s,v)。

(五) 交易階段：

當消費者使用電子現金(m,s,v)時，商家獲得電子現金後，商家首先先確認v是否正確，商家使用銀行的公開金鑰e驗證電子現金是否滿足，若滿足則表示電子現金合法：

$$s^{ev}modn \equiv H(m)modn?$$

要求銀行檢驗電子現金(m,s,v)是否有重負支付，若無則銀行將該電子現金(m,s,v)儲存於資料庫中，以便對往後付費時的電子現金可執行重複付費檢查，並在商家帳戶內加入消費者實際消費總額。

2.4.3 自我認證

在安全的電子商務中，PKI 技術的建設是一項重要的系統工程，Girault 於 1991 年提出植基於 RSA 之自我認證公開金鑰密碼系統，不同於一般 ID-Based 由憑證中心製發憑證的作法，在授權階段由憑證中心與用戶雙方共同參與公開金鑰的計算，在驗證階段可以進行自我驗證的演算法，並可透過雙方傳送公開資訊，達成身分的確認，由於憑證中心的憑證內嵌於公鑰中，其他使用者可以驗證該使用者公鑰的正確性(蘇品長等，2014)，Girault 提出三種層次的安全等級如表 4 所示。

表4　Girault 提出之安全等級表

安全等級	說明	應用案例
初等	憑證中心因為擁有所有使用者的私密金鑰與公開金鑰，因此可以在任何時候偽冒任一個使用者而不被發現。	以身分為基礎的認證系統
中等	憑證中心在不知道使用者的私密金鑰的情況下，卻能偽造出一個未授權的使用者而不被發現。	電子憑證之認證系統
高等	1.授權中心透過使用者傳送之參數才能計算其公鑰，在授權階段，憑證中心不知道使用者的私鑰，所以無法自行產生或偽冒使用者的公鑰。 2.使用者可以自行驗算憑證中心傳送之公鑰，並驗證其正確性，故憑證中心無法主導使用者公鑰的產生與驗證。	自我認證公開金鑰密碼系統

資料來源：蘇品長等(2014)

2.5 小節

根據前述文獻探討得知區塊鏈技術具有不可竄改、可追溯及去中心化等特性，已在金融領域中快速發展與應用，可以解決交易雙方信任之問題，對比文獻中專家學者提出之多銀行數位交易機制，仍有電子現金難以辨識額度及資訊不對稱、資料遭竄改及身分偽冒之風險，故本研究提出運用區塊鏈技術結合智能合約與密碼學原理之多銀行數位交易機制，以區塊鏈技術為底層架構，利用分散式帳本技術結合智能合約，改善中心化伺服器最高者管理者權限及資料可能遭竄改之問題，達到金流、資訊流同步一致與資料可追溯性；透過橢圓曲線部份盲簽章方式實施電子交易支付，確保電子現金有效性，解決已簽署之電子現金難以辨識其額度或時效的問題；以自我認證為設計進行身分認證，不需透由第三方認證中心保證，使銀行、消費者、商家等電子商務中的參與人員身分資料達到完整性、不可否認性及真實性，進而達成電子商務交易安全。

三、電子交易機制設計

在本研究構想中，提出一個以區塊鏈為底層架構，利用智能合約建構安全電子交易機制，主要運用部份盲簽章和自我認證這兩種技術，首先，由服務開發者部署智能合約，由多個銀行業者組成聯盟鏈，可達成不同銀行金流互通及共享帳本之目的，接著利用植基於橢圓曲線離散對數難題之部份盲簽章技術，確保於交易階段銀行無法得知交易內容為何，確保交易內容及消費習慣隱蔽性，並達成電子現金驗證性，最後系統導入 Girault 所提出之公開金鑰密碼系統中安全等級 3 的自我認證機制，避免憑證中心在憑證製發的過程中產生偽冒消費者身分進行交易之問題，同時也可減輕憑證伺服器對所有參與人員在公鑰儲存、計算與管理的負擔，以下將說明本研究所提出之電子現金交易系統架構及其運作流程。

3.1 系統架構

本研究設計電子交易參與者計系統服務開發者、多銀行、消費者及商家，首先由服務開發者將智能合約部署至區塊鏈上，所有參與者向憑證中心實施身分註冊，並取得公、私鑰及簽章憑證，接著由消費者與商家各自向銀行完成開戶作業，接續由消費者與商家實施電子交易（商品瀏覽及訂購），由消費者向商家完成付款，商家將款項存

入，最後由商家進行出貨，寄出交易商品，系統整體運作架構如圖 7 所示。

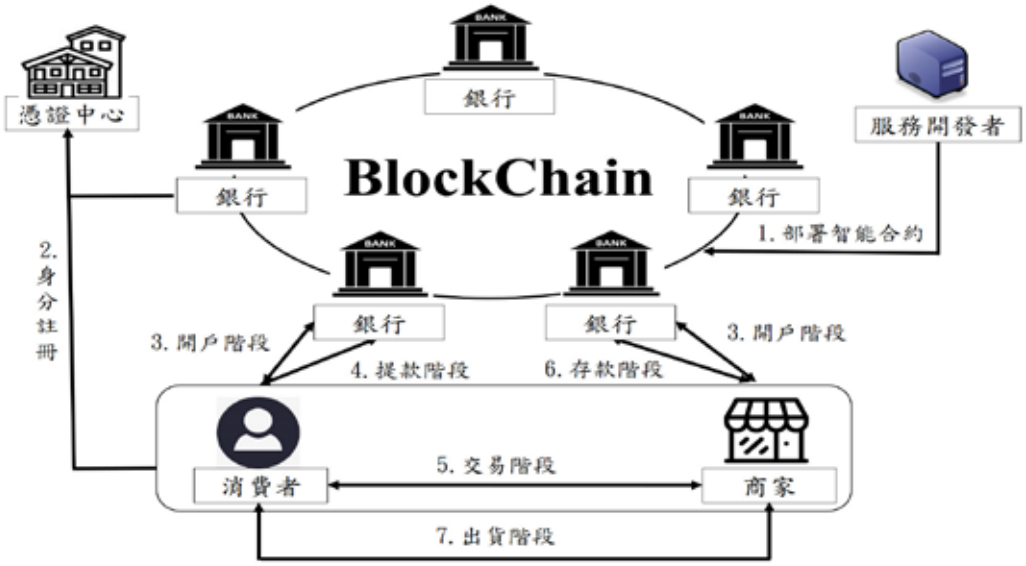


圖 7　系統整體運作架構圖

3.2 系統運作流程

本研究提出之系統作業流程區分系統初始、註冊、開戶、提款、交易、存款、出貨等七階段，參數說明如表 5 所示，首先由服務開發者設計智能合約並部屬至區塊鏈網路，參與者藉由憑證中心完成身分註冊，透過該電子憑證相互進行身分確認，確保為合法之用戶，消費者於後續提款、支付及商家進行存款階段中，將訂單及付款資訊透過部份盲簽章及加密技術傳送，確保資訊安全性。

表 5　系統各參數說明

項目	符號	說明
1	G	為橢圓曲線內之基點
2	$E(F_q)$	有限域F_q中之橢圓曲線
3	n	橢圓曲線上基點的階數(order)
4	q	$q > 2^{256}$之質數
5	$\|\|$	訊息連結符號
6	$CA、SD、EP、CS、SH$	憑證中心、服務開發者、銀行機構、消費者及商家
7	SC	服務開發者設計之智能合約
8	BC	區塊鏈網路
9	DG_{gid}	商品名稱，gid為其專屬的商品代號
10	Num	訂單編號，每筆交易自動產生的編號
11	$Price$	訂單上的金額
12	Key_{gid}	進行數位商品DG_{gid}加解密的對稱式金鑰。
13	ID_i	參與者身分 ID，i∈ $\{CA、SD、EP、CS、SH\}$
14	id_i	參與者匿名身分 id，i∈ $\{CA、SD、EP、CS、SH\}$
15	V_i	參與者簽名檔，i∈ $\{CA、SD、EP、CS、SH\}$
16	Add_i	參與者位址，i∈ $\{CA、SD、EP、CS、SH\}$
17	W_i	參與者計算之驗證值 i∈ $\{CA、SD、EP、CS、SH\}$

表 5　系統各參數說明(續)

項目	符號	說明
18	Ac_i	參與者帳戶，i∈ $\{CA、SD、EP、CS、SH\}$
19	d_i、k_i	隨機秘密參數值，i∈ $\{CA、SD、EP、CS、SH\}$
20	Pk_i、Sk_i	參與者獲得之公鑰及私鑰 i∈ $\{SD、EP、CS、SH\}$
21	Wk_i	CA 計算的參與者簽章 i∈ $\{SD、EP、CS、SH\}$
22	$Key_{i/j}$	雙方經過身分驗證後，建立之共享金鑰 i, j∈ $\{SD、EP、CS、SH\}$
23	ec	交易內容，包含訂單編號、訂單金額及商品名稱
24	t	電子現金之公開資訊，包含電子現金之面額與時限
25	Er	電子發票
26	ts_{ij}	由使用者i所選取之時間戳記，j為傳遞次數，$j = 1,2,\dots,n$
27	$Deploy()$	部署智慧合約，把合約儲存在區塊鏈上，並取得一個專屬的位址
28	$Oac()$	參與者透過智能合約向銀行開戶的過程
29	$Reg()$	參與者向憑證中心註冊的過程
30	$Cer()$	雙方互向認證的過程
31	$Check()$	檢查資料正確性
32	$CheckAc()$	檢查帳戶餘額

3.2.1 初始階段

在初始階段，服務開發者向憑證中心CA取得橢圓曲線公開參數寫入智能合約 SC，服務開發者將其智能合約部屬至區塊鏈上。

$$SD \rightarrow BC：Deploy(SC) \quad (1)$$

3.2.2 註冊階段

參與者$(EP、CS、SH)$各自向憑證中心註冊身分資料，由憑證中心驗證並產出公私鑰Pk_i及簽章Wk_i，憑證中心傳回給參與者$(EP、CS、SH)$，並由參與者各自計算其驗證值V_i，後續於交易可獨立進行身分自我認證。

$$EP \rightarrow CA: Reg(ID_{EP}, V_{EP}, Add_{EP}) \quad (2)$$
$$CA \rightarrow EP: (Pk_{EP}, Wk_{EP}) \quad (3)$$
$$CS \rightarrow CA: Reg(ID_{CS}, V_{CS}, Add_{CS}) \quad (4)$$
$$CA \rightarrow CS: (Pk_{CS}, Wk_{CS}) \quad (5)$$
$$SH \rightarrow CA: Reg(ID_{SH}, V_{SH}, Add_{SH}) \quad (6)$$
$$CA \rightarrow SH: (Pk_{SH}, Wk_{SH}) \quad (7)$$

3.2.3 開戶階段

銀行、消費者與商家完成身分認證後，確認雙方均為合法身分，消費者與商家透過智能合約分別向銀行申請開戶。

$$CS \rightarrow EP: Cer(ID_{CS/EP}, Pk_{CS/EP}, V_{CS/EP}) \quad (8)$$
$$CS \rightarrow EP: Oac(id_{CS}) \quad (9)$$
$$EP \rightarrow CS: Ac_{CS} \quad (10)$$
$$SH \rightarrow EP: Cer(ID_{SH/EP}, Pk_{SH/EP}, V_{SH/EP}) \quad (11)$$
$$SH \rightarrow EP: Oac(id_{SH}) \quad (12)$$

$$EP \rightarrow SH: Ac_{SH} \quad (13)$$

3.2.4 交易階段

消費者與商家完成身分認證後，確認雙方均為合法身分，消費者以 SSL 與商家建立彼此之間的安全通道，會議金鑰為$Key_{CS/SH}$；消費者瀏覽網站上的數位商品，選擇欲購買的數位商品，並發起電子交易。

$$CS \rightarrow SH: Cer(ID_{CS/SH}, Pk_{CS/SH}, V_{CS/SH}) \quad (14)$$

$$CS \rightarrow SH: (DG_{gid} \| ts_{CS1}) \quad (15)$$

$$SH \rightarrow CS: (Num, DG_{gid}, price \| ts_{CS1}, ts_{SH1}) \quad (16)$$

3.2.5 付款階段

在付款階段中，消費者與商家及銀行完成身分認證後，確認雙方均為合法身分，消費者將提款公開訊息 t(包含欲提款的電子現金之面額與時限）與帳戶資訊id，加密傳送給銀行，於雙方進行身分驗證後，銀行檢查公開資訊t之格式及帳號內是否有足夠餘額。接著，消費者將電子現金申請資訊進行盲化α，並由銀行於部分盲訊息上完成簽章S_α，並從消費者帳戶扣除與電子現金面額相等的金額，再將簽章傳回給消費者，消費者可在銀行機構無法獲得完整資訊的情況下取得其部份盲簽章之電子現金。最後，消費者以 SSL 與商家建立彼此之間的安全通道，會議金鑰為$Key_{CS/SH}$，並將訂單編號及電子現金加密傳送商家，商家收到加密訊息，解密後檢驗電子現金是否符合時限，如不符則拒絕。

$$CS \rightarrow EP: Cer(ID_{CS/EP}, Pk_{CS/EP}, V_{CS/EP}) \quad (17)$$

$$CS \rightarrow SH: Cer(ID_{CS/SH}, Pk_{CS/SH}, V_{CS/SH}) \quad (18)$$

$$CS \rightarrow EP: (id_{CS}, t \| ts_{CS1}) \quad (19)$$

$$EP: Check(t) \quad (20)$$

$$EP: CheckAc(id_{CS}) \quad (21)$$

$$CS \rightarrow EP: (\alpha \| ts_{CS2}) \quad (22)$$

$$EP \rightarrow CS: (S_\alpha \| ts_{EP1}) \quad (23)$$

$$CS: S'_\alpha \quad (24)$$

$$CS \rightarrow SH: (Num, (S'_\alpha, t) \| ts_{CS1}) \quad (25)$$

3.2.6 撥款階段

在撥款階段中，商家與電子機構完成身分認證後，確認雙方均為合法身分，商家以 SSL 建立與電子支付機構之間的安全通道，共同會議金鑰$Key_{SH/EP}$，可在傳輸資料時執行加/解密使用，商家將加密後的帳戶及電子現金資訊傳送給電子支付機構，電子支付機構解密並核對電子現金是否重複存款；如檢查正確，則傳給商家一個電子現金為合法的回應 Msg（$legal$），並將錢存入商家的帳戶中。

$$SH \rightarrow EP: Cer(ID_{SH/EP}, Pk_{SH/EP}, V_{SH/EP}) \quad (26)$$

$$SH \rightarrow EP: (id_{SH}, (S'_\alpha, t)) \quad (27)$$

$$EP: Check(S'_\alpha, t) \quad (28)$$

$$EP \rightarrow SH: Msg(legal) \quad (29)$$

3.2.7 出貨階段

在出貨階段中，商家與消費者完成身分認證後，確認雙方均為合法身分，商家以 SSL 建立與消費者之間的安全通道，共同會議金鑰為$Key_{CS/SH}$，商家傳送數位商品DG_{gid}之解密金鑰K_{gid}及電子發票Er給消費者，消費者透過解開Dg_{gid}，獲得數位商品。

$$CS \rightarrow SH: Cer(ID_{CS/SH}, Pk_{CS/SH}, V_{CS/SH}) \quad (30)$$

$$SH \rightarrow CS:(DG_{gid}, K_{gid}, Er) \quad (31)$$

3.3 系統演算法設計

考量文章篇幅，摘述身分註冊及電子現金核心技術，演算法如下。

3.3.1 身分註冊

憑證中心CA在有限域$E(F_q)$上選擇一個安全的橢圓曲線$E(F_q)$：$y^2 = x^3 + ax + b(modq)$且$4a^3 + 27b^2 \neq 0(modq)$，q 為一個 256 位元以上之大質數，並在橢圓曲線$E(F_q)$上選一階數（order）為 n 的基點 G，使$n \cdot G = O$，接續由CA選擇一個單向無碰撞雜湊函數$h(\ )$，選擇私密金鑰並計算公鑰，$Pk_{CA} = Sk_{CA} \cdot G$，最後由$CA$公開參數$E$、$G$、$q$、$h(\ )$、$Pk_{CA}$。

參與者註冊：參與者$(EP、CS、SH)$首先選擇一隨機秘密參數值$d_i \in [2, n-2]$，以參與者位址Add_i與秘密參數值d_i計算產生簽名檔V_i，完成簽名檔計算後將V_i、Add_i傳送至憑證中心CA，計算如下:

$$V_i = h(d_i \parallel Add_i) \cdot G \quad (32)$$

憑證中心CA驗證回傳：憑證中心 CA 接收參與者之註冊資訊後，選擇一隨機秘密參數$k_i \in [2, n-2]$，與註冊資訊計算參與者的驗證公鑰W_i及簽章值Wk_i，憑證中心 CA 完成計算後將W_i及Wk_i回傳給參與者，計算如下:

$$W_i = V_i + \left(k_i - h(Add_i)\right) \cdot G = \left(q_{ix}, q_{iy}\right) \quad (33)$$

$$Wk_i = k_i + Sk_{CA}\left(q_{ix} + h(Add_i)\right) \quad (34)$$

參與者產生公、私鑰階段:參與者接收憑證中心CA回傳之驗證公鑰W_i及簽章值Wk_i，計算自己的公、私鑰(Pk_i, Sk_i)，並驗證公鑰W_i的正確性，計算如下:

$$Sk_i = Wk_i + h(d_i \parallel Add_i) \quad (35)$$

$$Pk_i = Sk_i \cdot G \quad (36)$$

$$Pk_i = [Wk_i + h(d_i \parallel Add_i)] \cdot G \quad (37)$$

$$Pk_i = Sk_i \cdot G = k_i \cdot G + h(d_i \parallel Add_i) \cdot G + [q_{ix} + h(Add_i)]Pk_{CA} \quad (38)$$

3.3.2 電子現金

申請階段：消費者將提款資訊t與帳戶資訊id加密傳送給銀行，銀行檢查確認消費者帳戶金額足夠，隨機選取橢圓曲線上一點P_1和隨機數$af \in [2, n-2]$，並加密隨機數P_a和計算電子現金序號密文摘要 P_Q，將加密隨機數P_a，電子現金序號密文摘要P_Q傳送給消費者。

$$P_a = af \cdot G \quad (39)$$

$$P_Q = P_1 + af \cdot Pk_{EC} \quad (40)$$

盲化階段：消費者收到P_a及P_Q後，隨機選取橢圓取上一點P_2，盲因子$br \in [2, n-2]$和隨機數$bf \in [2, n-2]$，用自身的公開金鑰Pk_{CS}針對電子現金申請資訊進行盲化α，並傳送給銀行。

$$P_R = P_2 + bf \cdot Pk_{CS} \quad (41)$$

$$\alpha = x_{P_2} \cdot br^{-1} \cdot h\left(ec \| x_{P_Q} \cdot x_{P_R}\right) \quad (42)$$

簽章階段：銀行收到α之後，隨機選擇亂數$cf \in [2, n-2]$，並使用電子現金私鑰Sk_{EC}進行簽章，計算S_1, S_2，接著把α、S_1, S_2、P_1傳給消費者。

$$S_1 = t \cdot Sk_{EC} \cdot x_{p1} \cdot \alpha + cf \quad (43)$$

$$S_2 = cf \cdot G \quad (44)$$

解盲階段：消費者收到α、S_1, S_2、P_1之後，進行解盲化，並可在銀行無法得知ec之情形下，取得部份盲簽章(K, J, a, b, t)。

$$a = x_{P1} \cdot x_{P2} \quad (45)$$

$$b = x_{P_Q} \cdot x_{P_R} \quad (46)$$

$$K = br \cdot S_2 \quad (47)$$

$$J = br \cdot S_1 \quad (48)$$

驗證階段：商家收到其電子現金後，可驗證電子現金之有效性。

$$J \cdot \mathrm{G} \stackrel{?}{=} t \cdot Pk_{EC} \cdot a \cdot h \quad (49)$$

驗證說明如后：

$$J \cdot \mathrm{G} = br \cdot S_1 \cdot \mathrm{G} \quad (50)$$

$$= br \cdot [t \cdot Sk_{EC} \cdot x_{p1} \cdot \alpha + cf\,] \cdot \mathrm{G} \quad (51)$$

$$= br \cdot t \cdot Sk_{EC} \cdot x_{p1} \cdot x_{P_2} \cdot br^{-1} \cdot h\left(ec \| x_{P_{Q1}} \cdot x_{P_{Q2}}\right) \cdot \mathrm{G} + br \cdot cf \cdot \mathrm{G} \quad (52)$$

$$= t \cdot Pk_{EC} \cdot a \cdot h \quad (53)$$

四、安全及效益分析

4.1 安全性分析

理想的電子現金系統都應具備基本的安全屬性：不可偽造性-任何使用者都不能偽造或修改電子現金的價值；不可追蹤性-任何使用者都不能從電子現金中得知交易細節或使用者身分細節；防止雙花-任何使用者都不能多次花費同一筆電子現金(Barguil and Barreto, 2015)，本研究除滿足上述基本安全性外，另達到機密性等額外安全要求。

4.1.1 機密性

機密性是指在交易或傳輸期間，資料都是被保密的，無法遭未經授權的人員或程序所取得或透露的特性，只有經過核可的人或程序才能獲得相關數據資料，避免資料外洩(蘇品長等，2022)；在本研究交易中，使用非固定式交談金鑰$Key_{i/j}$，若資訊遭有心人士竊取，因無相對應的交談金鑰，須暴力破解橢圓曲線離散對數之難題，故在實際安全上可確保電子現金機密性。

4.1.2 完整性

完整性是資料在傳遞過程中，確保內容保持完整且正確一致，不會遭任意竄改，在本研究中由於區塊鏈上每個區塊之間以雜湊函數值鏈結，在傳遞過程中內容不能被任意增減或修改(Guo and Yu, 2022)，另銀行簽章之電子現金是由消費者利用雜湊函數演算法所得$\alpha = x_{P_2} \cdot br^{-1} \cdot h\left(ec \| x_{P_Q} \cdot x_{P_R}\right)$，若途中遭攔截並修改後發送給商家，產出之密文摘要不一致，可以確保電子現金內容之完整性。

4.1.3 匿名性

匿名性是在交易階段中，不想透露真實身分的一種不具名行為，本研究基於區塊鏈技術為基礎，在區塊鏈中的參與者，皆是以「英文+數字」的代碼為名稱，採匿名身分進行交易，於鏈上參與者僅能確認該筆交易存在(Rajasekaran et al., 2022)，無法知悉其交易內容，消費者在提領電子現金交易行為，銀行皆無法取得使用者之交易明細ec，因此無法調查消費者之習慣。

4.1.4 防止雙花

消費者在傳送電子現金給商家進行付款時，商家可先行檢查電子現金合法性$J \cdot \mathrm{G} \stackrel{?}{=} t \cdot Pk_{EC} \cdot a \cdot h$，驗證通過後，銀行於收到銀行存入該筆電子現金時，可檢查是否已被使用，若發生重複消費可進行追蹤。

4.1.5 不可否認性

不可否認性是指對已經產生的交易或事件的證明，無法否認其交易行為，在本研究中，參與交易各方之公、私鑰對皆是向憑證中心註冊所得，在電子現金提款階段，已由銀行完成簽章，故接收方能以驗證方式確認其簽章的有效性，各參與者皆無法否認所簽署之資訊，另在交易傳送訊息過程中，加入時戳ts_{ij}，可以達成電子交易時間證明，達到不可否認性。

4.1.6 不可偽造性

不可偽造性是指只有授權方銀行才能發行電子現金，在本研究中，第三方若想偽造發行電子現金，必須得到授權之金鑰，然而想獲得密鑰將會面臨橢圓曲線離散對數的問題；另在付款階段，商家可驗證消費者所支付的電子現金合法性，不需透過發行銀行，可達到電子現金之不可偽造性。

4.1.7 不可竄改性

不可竄改性是指資料及數據不可被任何人任意竄改，在本研究中利用區塊鏈技術建構電子現金系統，參與者均須透過區塊鏈上執行電子現金提款、存款等交易行為，而在區塊鏈上，每個區塊之間以雜湊函數值鏈結，而雜湊函數據不可逆且為單向性，因此存在於鏈中產生的數據是不可被任意竄改的(Rajasekaran et al., 2022)，故具有不可竄改性。

4.1.8 資料可追溯性

可追溯性是指電子現金交易申請資訊可以溯源，在本研究中，每一筆電子現金從銀行傳送至消費者，並由商家存入銀行，區塊鏈上都可以透過智能合約完整追溯其過程(Li et al., 2020)，銀行亦可透過區塊鏈共享帳本確認電子現金合法性，完整記錄溯源。

4.1.9 抗中間人攻擊

中間人攻擊指的是當攻擊者偽冒身分或偽造數據，在不被他人識破的情形下，破壞整體系統運作流程，大多數沒有良好身分驗證安全性的加密系統都面臨中間人攻擊的威脅(Mallik, 2019)，在本研究中以自我認證方式實施身分註冊，使用者可自行驗算憑證中心傳送之公鑰正確性$Pk_i = Sk_i \cdot G = k_i \cdot G + h(d_i \| Add_i) \cdot G + [q_{ix} + h(Add_i)]Pk_{CA}$，並於後續交易過程中，雙方先行完成身分驗證後，始可進行交易，確保參與者合法身分，可有效抵抗中間人攻擊。

4.2 方案比較

本研究設計基於區塊鏈建構多銀行數位交易機制，針對理論基礎與第二章文獻探討中所列學者提出之多銀行電子現金系統進行比較，並依據區塊鏈技術之優勢及特性，參酌相關文獻進行安全性分析與時間複雜度計算(Wang et al. 2007; Tsaur et al., 2018; Li et al., 2019; Tsai and Su, 2021)，可發現電子現金交易時所花費時間成本相對較低，並可滿足安全性要求，安全性比較結果如表 6，運算成本參考如表 7，時間複雜度比較如表 8。

4.2.1 Wang 等學者提出電子現金系統方案

該研究提出透過群盲簽章雖然能達到聯合發行電子現金的目標，惟未能解決銀行資料庫成長快速與已完成簽署之電子現金難以辨識額度及使用效期的問題，在設計中先決條件為可信任之第三方擔任憑證中心，無法避免憑證中心偽冒使用者問題，在計算量與傳輸量方面植基於 RSA 機制，相對需要大量的指數運算，導致系統運算負荷，另針對銀行集中式伺服器管理無法解決資料可能遭受竄改及清算系統故障導致金流及資訊流不對稱之問題及問題。

4.2.2 Tsaur 等學者提出電子現金系統方案

該研究方案設計基於部份盲簽章之多銀行聯合發行的行動電子現金系統，利用部份盲簽章之技術應用於多銀行聯合發行的行動電子現金系統雖可改善銀行資料庫大量成長的衝擊，解決已簽署之電子現金難以辨識其額度與時效的問題，然而針對銀行集中式伺服器管理無法解決資料可能遭受竄改及清算系統故障導致金流及資訊流不對稱之問題。

4.2.3 Li 等學者提出電子現金系統方案

該研究方案中由中央銀行擔任一個可信任的中央金融機構擔任憑證中心，負責發佈憑證，然而未提及中央銀行可能無法信任之解決方案，銀行集中式伺服器管理無法解決資料可能遭受竄改及清算系統故障導致金流及資訊流不對稱之問題，另設計中未提出改善銀行資料庫大量成長的衝擊，解決已簽署之電子現金難以辨識其額度與時效的問題。

表 6　安全性比較表

項目	Wang 等學者提出之電子現金系統(2007)	Tsaur 等學者提出之電子現金系統(2018)	Li 等學者提出之電子現金系統(2019)	本研究機制
機密性	○	○	○	○
完整性	○	○	○	○
匿名性	○	○	○	○
防止雙花	○	○	○	○
不可否認性	○	○	○	○
不可偽造性	○	○	○	○
不可竄改性	Δ	Δ	Δ	○
資料可追溯性	Δ	○	○	○
抗中間人攻擊	X	○	X	○
系統便利性	X	Δ	Δ	○
多銀行發行	○	○	○	○
註：○：符合、Δ：部分符合、X：不符				

表 7　運算成本參考表

符號	定義
T_{ECMUL}	進行一次 ECC 乘法運算所需時間≈29 T_{MUL}。
T_{ECADD}	進行一次 ECC 加法運算所需時間≈5 T_{MUL}。
T_{BP}	進行一次雙線性對運算所需時間≈120 T_{MUL}。
T_{EXP}	進行一次模式指數運算所需時間≈240 T_{MUL}。
T_{INVS}	進行一次模式乘法反元素所需時間≈240 T_{MUL}。
T_{MUL}	進行一次模式乘法所需時間。
T_c	進行一次對稱式加密所需時間。
T_{ADD}	進行一次模式加法所需時間（可忽略不計）。
t_h	進行一次單向雜湊函數所需時間≈0.4 T_{MUL}。

資料來源：Tsai and Su（2021）

表 8　電子現金交易複雜度比較表

項目	Wang 等學者提出之電子現金系統(2007)	Tsaur 等學者提出之電子現金系統(2018)	Li 等學者提出之電子現金系統(2019)	本研究機制
時間複雜度	$1207.44T_{MUL}+6t_h+5T_c$	$409.92T_{MUL}+5t_h+7T_c$	$12T_{EXP}+14T_{ECMUL}$ $2T_{ECADD}+6T_{BP}$	$10T_{ECMUL}+3T_{ECADD}$ $+5T_{ADD}+12T_{MUL}+$ $1T_{INVS}+5t_h+5T_c$
合計	$\approx 1210T_{MUL}+5T_c$	$\approx 412T_{MUL}+7T_c$	$\approx 4016T_{MUL}$	$\approx 559T_{MUL}+5T_c$

五、結論

本研究設計基於區塊鏈建構具安全性數位交易機制，透過區塊鏈可達成各銀行業者共同維護帳本，即時完成跨銀行清算，達成金流互通、資訊流同步一致的目標，提高合作商家與消費者便利性，進而提升電子支付普及率，在本研究機制中，透過銀行帳本同步一致及資料長時保存，可解決現行電子現金易遭惡意竄改，易被複製及重複付款的安全性威脅；利用區塊鏈能監管溯源及匿名之特性，使電子支付能被商家及消費者信任；運用部份盲簽章技術解決電子支付中，電子現金難以辨識其額度或時效的問題，使商家可驗證其有效性，並能保障消費者隱私性；另在電子商務環境中，利用自我認證方式提高系統安全性，在使用者申請註冊及開立電子現金帳戶時，解決憑證中心可能偽冒使用者身分進行註冊及開立電子現金帳戶之情形，達到參與人員身分資料完整性、不可否認性及真實性，並可有效減輕憑證中心公鑰儲存的成本，始能兼顧使用者便利性及交易安全性之外，避免電子支付機構淪為金融犯罪的缺陷。

本研究在安全性上除滿足電子現金基本要求不可偽造性、不可追蹤性及防止雙重花費外，另外達到匿名性、機密性、不可否認、不可竄改、數據可追溯、抗中間人攻擊等特點，並運用智能合約使系統更加自動化，當電子現金出現重複消費爭議及問題時，可快速掌握並釐清責任歸屬，解決資訊不對稱及信任問題，有效提升電子商務中消費者對於電子支付之信心。

5.1 國防領域之應用

本研究可應用於國防採購及財務領域，在採購方面，可將此電子支付機制導入國軍福利站、國軍副食供應中心、國軍文具部、國軍服裝供售站等各項商品銷售支付，隨著電子化購物的消費型態改變，使國軍官兵弟兄姊妹在採購方式上，除了既有的現金支付外，提供更多樣性的選擇，強化國軍電子商務便利性，達成網路商店交易安全，符合現代科技多元支付服務範疇，另可使電子現金支付更具安全性。在財務方面，現行人員獎勵多採用發放獎金（現金）、禮卷等方式，惟紙本不易保存，且承辦單位常無法有效掌握核發對象，如未來可將其實體獎金改為發行電子現金構想，可避免紙本現金、禮卷丟失及重複領用等問題，並達到去中心化（第三方）之目的，同時強化交易之安全性，提升整體國防戰力。

5.2 未來運用方向

經過多年努力，我國電子支付的基礎建設已臻完備，隨著金融科技如大數據、區塊鏈、雲端運算及人工智慧等創新技術發展，各銀行及相關企業企圖透過資訊技術提高執行效率、增加交易安全性及降低成本，亦期望能帶來嶄新的機會，目前國內電子支付比率占消費支出比率仍低於鄰近亞洲國家，如日本、韓國、新加坡等，行政院已訂立目標，在本研究設計中，運用區塊鏈系統達成帳本同步一致，於電子現金開戶、

交易、付款與撥款之金流、資訊流皆不可竄改，可有效解決電子商務中電子現金安全性、雙重花費及信任等問題，並利用密碼學原理、植基於橢圓曲線部份盲簽章技術及自我認證公開金鑰系統技術，提高交易之安全性及提高執行效率，期望透過本機制可提升電子現金使用率，並達成 2025 年行動支付的普及率 90%之目標，達成無現金之數位化生活。

近年來國際間中央銀行正投入研究發展數位貨幣(Central Bank Digital Currency; CBDC)，而我國也正積極投入研究，於「111 年度金融資訊系統年會」中，中央銀行總裁楊金龍表示，央行數位貨幣(CBDC)跟現行電子支付是互補關係，未來俟 CBDC 發展成熟、完善系統營運安全機制，並於我國政府對於區塊鏈發展金融服務之監管與法規體制明確，完成相關系統建設後，可結合本研究支付機制，使支付整體機制更加完整，有利未來金融業者及相關企業金融服務之應用，另在雲端運算環境中存在各式網路攻擊，如側通道攻擊、分散式阻斷服務攻擊及區塊鏈技術上存在智能合約漏洞等安全威脅，可能導致網路服務中斷、私密訊息遭竊及鏈上資訊亦有被竄改之可能性，因此於系統建置後可結合流量分析及封包檢測等設備，監測相關數據，提早發現異狀進行修正，降低系統服務中斷或資料遭竊取之威脅。

六、國防相關應用

本研究可應用於國防採購、財務領域，並導入國軍各式支付機制，如國軍福利站、國軍副食供應中心、國軍文具部、國軍服裝供售站等，提供多元安全之電子支付方案。

參考文獻

李于宏（2021）。解構區塊鏈本質，*財金資訊*，99。

李宛蓁、黃杭浔（2016）。區塊鏈及數位貨幣在金融業的影響與應用研究計畫，台灣金融研訓院。

李耕銘（2021）。區塊鏈生存指南：帶你用 Python 寫出區塊鏈！，臺北：博碩文化。

金融監督管理委員會（2022/8/11）。111 年 6 月份信用卡、現金卡及電子支付機構業務資訊，下載於 https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202208110001&dtable=News（2022 年 8 月 30 日）。

財金資訊股份有限公司（2020/12/11)。財會主管看「金融監理與銀行函證」研討會，下載於 https://www.ardf.org.tw/downloads/ppt/3.pdf（2022 年 9 月 3 日）。

財金資訊股份有限公司，金融區塊鏈函證服務，財金資訊股份有限公司資訊網，下載於 https://www.fisc.com.tw/TC/Business?Caid=7c31a87d-2b5f-42bf-aafd-3c2405f64e8b&CaStyleId=4（111 年 4 月 8 日）。

國泰金控（2021/9/23）。國泰世華銀行「環球貿易共享區塊鏈」獲金管會核准試辦攜手 7 銀行以區塊鏈打造台灣首例企業金融資料交換平臺，國泰金控，下載於 https://www.cathayholdings.com/holdings/information-centre/intro/latest-news/detail?news=aK1nGyfMkECqFdgCC-4kPQ&page=4（2022 年 4 月 2 日）

曹偉駿、蔡欣潔（2010）。基於部分盲簽章之多銀行聯合發行的行動電子現金系統，全國資訊安全會議，第 20 屆，145-150。

郭木興（2003）。*電子商務：觀念、策略與案例實作*，臺北：學貫行銷出版。

彭思遠（2021）。去中心化金融與區塊鏈的發展，*臺灣經濟研究月刊*，44（1），49-55。

黃敬翔（2019）。區塊鏈技術對金融發展之衝擊，*臺灣經濟研究月刊*，42（11），55-61。

楊金龍（2019）。「中央銀行貨幣與零售支付系統-兼論財金公司扮演之角色」，下載於 https://www.cbc.gov.tw/tw/cp-302-104572-883b0-1.html（2023 年 3 月 13 日）。

鄒均、張海寧、唐屹、李磊、劉天喜、陳暉、曲列、鄭曉明(2018)。*區塊鏈技術指南*，北京：機械工業出版社。

魏喬怡（2019/10/23）。中信奇美實創區塊鏈交易首例，中時新聞網，下載於 https://www.chinatimes.com/newspapers/20191023000292-260205?chdtv（2022 年 4 月 10 日）

蘇品長（2007）。植基於 LSK 和 ECC 技術之公開金鑰密碼系統，長庚大學電機工程研究所博士論文。

蘇品長、夏君和、蘇泰昌（2022）。建構具安全性的智慧合約共享方案-以房屋共享為例，*資訊管理學報*，29（3），253-275。

蘇品長、張鈞富、黃棠建（2014）。適用於電子商務之自我認證公開金鑰架構之設計與實作。*電子商務研究*，12（1），73-92。

Abe, M., & Fujisaki, E. (1996). How to date blind signatures. *In International Conference on*

the Theory and Application of Cryptology and Information Security, 244-251. doi:10.1007/BFb0034851

Barguil, J. M., & Barreto, P. S. (2015). Security issues in Sarkar's e-cash protocol. *Information Processing Letters*, *115*(11), 801-803. doi:10.1016/j.ipl.2015.06.007

Barker, E., & Roginsky, A. (2018). Transitioning the use of cryptographic algorithms and key lengths (No. NIST Special Publication (SP) 800-131A Rev. 2). National Institute of Standards and Technology.

Chaum, D. (1983). Blind signatures for untraceable payments. *In Advances in cryptology*, 199-203. Springer, Boston, MA. doi:10.1007/978-1-4757-0602-4_18

Chen, Q., Srivastava, G., Parizi, R. M., Aloqaily, M., & Al Ridhawi, I. (2020). An incentive-aware blockchain-based solution for internet of fake media things. *Information Processing & Management*, *57*(6), 102370.

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13, e00151. doi: 10.1016/j.jbvi.2019.e00151

Chen, Y., Chou, J. S., Sun, H. M., & Cho, M. H. (2011). A novel electronic cash system with trustee-based anonymity revocation from pairing. *Electronic Commerce Research and Applications*, *10*(6), 673-682. doi:10.1016/j.elerap.2011.06.002

Cheng, H. K., Hu, D., Puschmann, T., & Zhao, J. L. (2021). The landscape of blockchain research: impacts and opportunities. *Information Systems and e-Business Management*, *19*(3), 749-755.

Di Angelo, M., & Salzer, G. (2019, April). A survey of tools for analyzing ethereum smart contracts. *In 2019 IEEE International Conference on Decentralized Applications and Infrastructures*, 69-78. doi: 10.1109/DAPPCON.2019.00018

Gartner., “Blockchain Technology: What’s Ahead?”, From https://www.gartner.com/en/information-technology/insights/blockchain（retrieved on April 11, 2022）.

Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: Research and Applications*, *3*(2), 100067.

Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2019). A delay-tolerant payment scheme based on the ethereum blockchain. *IEEE Access*, 7, 33159-33172.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203-209. doi:10.1090/S0025-5718-1987-0866109-5

Lee, S. W., Singh, I., & Mohammadian, M. (2021). Blockchain Technology for IoT Applications. Singapore: *Springer*.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems*, 107, 841-853.

Li, Y., Zhou, F., & Xu, Z. (2019). A fair offline electronic cash scheme with multiple-bank in standard model. *Journal of the Chinese Institute of Engineers*, *42*(1), 87-96.

Liao, C. H., Guan, X. Q., Cheng, J. H., & Yuan, S. M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems*, *135*, 450-466.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Journal Pendidikan Teknologi Informasi*, *2*(2), 109-134.

Miller, V. S. (1985). Use of Elliptic Curve in Cryptography, *In Conference on the Theory and Application of Cryptographic Techniques*, 417-426. doi:10.1007/3-540-39799-X_31

Nakamoto Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System [Online forum comment]. From https://bitcoin.org/bitcoin.pdf（retrieved on April 3, 2022）

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039.

Ramchandra, M. V., Kumar, K., Sarkar, A., Mukherjee, S. K., & Agarwal, K. (2022). Assessment of the impact of blockchain technology in the banking industry. *Materials Today: Proceedings*, *56*, 2221-2226.

Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1), 1-9. doi: 10.1186/s40854-016-0040-y

Swan, M. (2015). *Blockchain Blue print for a New Economy*, O'Reilly Media Publishing, United States.

Tsai, C. H., & Su, P. C. (2021). A robust secure self-certified concurrent signature scheme from bilinear pairings. *The International Arab Journal of Information Technology*, *18*(4), 541-553.

Tsaur, W. J., Tsao, J. H., & Tsao, Y. H. (2018). An efficient and secure ECC-based partially blind signature scheme with multiple banks issuing E-cash payment applications. *In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE)*, 94-100.

Wang, C., Li, Q., & Yang, X. (2007). A fair and transferable off-line electronic cash system with multiple banks. *In IEEE International Conference on e-Business Engineering*, 189-194. doi:10.1109/ICEBE.2007.45

Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X., & Xu, X. (2020). The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science*, *37*(4), 691-698. doi:10.1002/sres.2710

Zhang, T., & Huang, Z. (2022). Blockchain and central bank digital currency. *ICT Express*, *8*(2), 264-270.

視訊與現場面談情況下應徵者專業及外表吸引力對面試官評分的交互作用影響

羅新興[1*] 林美琪[1] 羅景文[2]

[1]健行科技大學企業管理學系
[2]健行科技大學行銷與流通管理系

論文編號：NM-44-01-03
DOI：10.29496/JNDM.202405_45(1).0004
來稿2022年9月5日→**第一次修訂**2023年1月6日→**第二次修訂**2023年4月13日→
同意刊登 2023 年 5 月 3 日

摘要

本研究目的在探討視訊與現場面談情況下，應徵者專業能力及外表吸引力對面試官給予應徵者評分的交互作用影響。本研究分別進行模擬現場面談與視訊面談的受試者間之類實驗設計，研究助理扮演應徵者，研究者模擬擔任發問問題的面試官，受試者模擬擔任未發問問題的面試官。分析 320 份有效樣本資料獲得以下發現：在視訊面談情況下，應徵者專業能力與外表吸引力對面試官給予應徵者評分具加乘效果；在現場面談情況下，應徵者專業能力與外表吸引力對面試官給予應徵者評分具微幅的替代效果。本研究補足視訊面談與現場面談差異的實證缺口。

關鍵詞：應徵者專業、外表吸引力、應徵者表現評價、視訊面談、現場面談

*聯絡作者：羅新興 email: hhlo@uch.edu.tw

The Interaction Effects of Job Applicants' Profession and Physical Attractiveness on Rating in a Video Interview and Face to Face Interview

Lo, Hsin-Hsin[1*]　Lin, Mei-Chi[1]　Lo, Ching-Wen[2]

[1]Department of Business Administration, Chien Hsin University of Science and Technology
[2]Department of Marketing and Distribution Management,
Chien Hsin University of Science and Technology

Abstract

The objective of this study is to explore the interaction effect of job applicants' profession and their physical attractiveness on the score they receive from interviewers in the setting of a video interview and face-to-face interview. This study conducted a quasi-experimental design for face to face and video interviews. Research assistants played the role of job applicants, the researcher of this study served as the interviewer who asked questions, and the participants were undergraduate students and master's students of the continuing education department, who served as interviewers who did not ask questions. A total of 320 valid samples were analyzed, and the following findings were obtained. In video interviews, applicants' profession and physical attractiveness exhibited a multiplier effect on interviewers' rating of the applicants' performance. By contrast, in face-to-face interviews, applicants' profession and physical attractiveness exhibited slightly substitution effect. The contribution of this study that fill the empirical gap of the differences between video and face-to-face interview.

Keywords: Applicant Profession, Physical Attractiveness, Applicant Performance Rating, Video Interview, Face to Face Interview

[*] Corresponding Author: Lo, Hsin-Hsin email: hhlo@uch.edu.tw

一、緒論

在技術變化快速的現代社會，擁有優秀的人力資源是組織競爭優勢的重要來源，組織甄選的目的就是在替組織挑選具備勝任能力與特質的優秀人才，因此甄選作業的有效性攸關組織績效甚鉅。人才甄選的工具很多，例如：筆試測驗、心理測驗、實作測驗及面談等，其中面談的應用相當普遍。雖然有文獻對面談的信度與效度有疑慮（Anderson & Shackleton, 1993），但是，由於面談的便利性與低成本，始終是許多組織經常採用的甄選方式（Barclay, 1999; Campion et al., 1997; Mast et al., 2011）。影響面試官評分的因素包括應徵者因素、面試官因素及面談情境因素等三大類（Dipboye, 1992），面談相關實證研究相當豐富（例如：陳建丞與蔡維奇，2005；陳建丞，2007；羅新興與李幸穗，2004；Anderson et al., 1994; Arvey and Campion, 1982; Baker et al., 2020; Campion et al., 1997; Ellemers et al., 2004; Langer et al., 2019; Podratz and Dipboye, 2002）。應徵者特性例如應徵者的專業能力（例：羅新興等，2022）；面談者特性例如面試官的調節焦點類型（例：羅新興等，2021）；情境因素例如面談結構性（陳建丞，2007）或面談媒介（Blacksmith, 2016）。然而，這些因素可能會對於面試官的評分產生交互作用影響，例如：研究發現女性面試官在視訊面談給予高低專業能力應徵者評分的差距程度大於現場面談，男性面試官在視訊面談給予高低專業能力應徵者評分的差距程度與現場面談無顯著差異（羅新興等，2022）。那麼，應徵者外表吸引力對於面試官評分的影響程度，在專業表現佳或不佳的應徵者身上哪個比較明顯呢？再者：上述應徵者專業與容貌的交互作用影響的態樣是否會因為視訊或現場面談而有不同呢？本研究嘗試釐清這些問題的疑惑。

就應徵者因素而言，應徵者對於職務所需的專業能力確實是影響面試官評分的重要因素，應徵者專業能力愈高則面試官給予的評分愈高（羅新興與李幸穗，2004；Anderson et al., 1994）。除了應徵者的專業能力外，實證研究也指出應徵者的外表吸引力也會影響面試官的評分（羅新興與李幸穗，2004；Beehr and Gilmore, 1982; Anderson and Shackleton, 1990; Podratz and Dipboye, 2002）。此外，也有文獻指出應徵者的外表吸引力會調節專業能力對面試官評分的正向影響，例如：羅新興與李幸穗（2004）指出，在應徵者的外表吸引力低的情況下，專業能力對於面試官評分的正向影響程度強，但是在應徵者的外表吸引力高的情況下，專業能力對於面試官評分的正向影響程度減弱，這表示應徵者的專業與外表吸引力二者具有 1+1 小於 2 的替代效果。此外，研究顯示應徵者的外表吸引力會對面試官給予應徵者的能力評分產生月暈效果（Halo Effect），意即應徵者外表吸引力對於面試官給予應徵者的能力評分具有正向影響（羅新興等，2009），意即應徵者外表吸引力應該會與專業能力產生 1+1 大於 2 的加乘效果。應徵者專業能力與外表吸引力對面試官給予應徵者的評分，究竟是加乘效果或替代效果尚未有充分證據可以定論。

新冠病毒的疫情瀰漫全球，不僅影響了人們的健康以及社會的經濟發展，也改變了人們的工作與生活模式，企業基於防疫需要，愈來愈多居家上班、異地辦公、分流上班等不同的彈性上班型態，視訊會議、視訊教學成為疫情期間的常態，組織面談採用視訊面談也愈來愈普及。過去許多面談實證文獻在探討現場面談情況，目前視訊面談在近年來的日漸普遍。許多文獻開始比較現場面談與視訊面談情況下面試官給予應徵者評分的

差異，許多實證結果顯示現場面談與視訊面談的不同情況下，面試官給予應徵者的評分具有差異性(羅新興等，2013；羅新興等，2021；Chapman and Rowe, 2001, 2002; Langer et al., 2019; Sears et al, 2013; Susan et al., 2001; Weller, 2017)。如果面試官在現場面談與視訊面談給予應徵者評分會有差異性，那麼，應徵者的專業能力與外表吸引力對面試官給予應徵者評分的交互作用影響是否也會因為面談媒介而有差異呢？換言之，應徵者專業能力、外表吸引力以及面談媒介對於面試官給予應徵者的評分是否會產生三階的交互作用呢？本研究的目的在釐清應徵者的專業能力與外表吸引力對於面試官評分的影響，究竟是加乘效果或者替代效果？二者的加乘效果或替代效果是否會因為現場面談或視訊面談而有差異？本研究的主要貢獻在補足面試官評分的影響因素之實證缺口。

二、文獻探討與假說推論

2.1 應徵者專業能力與外表吸引力對面試官評分的影響

企業希望為公司徵選優秀人才來創造更高價值，通常面試官會給予專業能力愈佳的應徵者之評價愈高(Anderson et al., 1994)。然而，多數面試官與應徵者都未曾謀面，外表吸引力是造成第一印象的重要因素(McArthur and Baron, 1983)，實證結果顯示：應徵者的外表吸引力愈高則可以獲得面試官給予愈高的評分(Marlowe et al., 1996)。多數文獻都證實應徵者專業能力與外表吸引力均會正向影響面試官的評分，那麼二者是加乘效果或者替代效果呢？加乘效果表示外表吸引力愈高則專業能力對面談官評分的正向影響會增強；替代效果表示外表吸引力愈高則專業能力對面試官評分的正向影響會減弱。羅新興與李幸穗(2004)利用拍攝面談影片進行應徵者變項的操弄，受試者模擬擔任面試官觀看面談影片的應徵者表現，該研究指出：應徵者的外表吸引力低的情況下，專業能力對於面試官評分的正向影響程度強，應徵者的外表吸引力高的情況下，專業能力對於面試官評分的正向影響程度減弱。換言之，該研究結果顯示應徵者專業能力與外表吸引力對於面試官的評分是替代效果。羅新興與李幸穗(2004)當時認為應徵者專業能力是屬於影響決策的診斷性訊息(Diagnostic Message)，面試官採中央路徑而仔細推敲訊息；外表吸引力則是無關績效的非診斷性訊息，面試官採周邊路徑的訊息處理流程，所以主張非診斷性訊息(外表吸引力)不會與診斷性訊息(專業能力)產生加乘效果，僅會產生彌補性的替代效果。然而，另一項研究顯示：無論高專業能力或者低專業能力的應徵者，外表吸引力對於應徵者獲得的能力評價都具有月暈效果(羅新興等，2009)，意即外表吸引力對於高專業能力的應徵者也可能會有加分效果。

2.2 面談媒介的調節效果

遠距視訊在科技發達的現代社會，早已廣泛地被使用在不同領域上。資訊網路打破了時間與空間的限制，尤其在不利於直接面對面的新冠疫情之下，更大幅提升企業對視訊面談的使用率。視訊面談的特性是溝通雙方透過網路在電子媒介上面互動，彼此可以聽見對方聲音且看見彼此的影像，但是相對於面對面的現場面談，雙方在視訊面談互動過程中較少出現眼神對焦，因為人們通常會目視自己的螢幕(看對方)而非鏡頭，導致眼神互動的親近感相對較低(羅新興等，2021)。近年來，比較視訊面談與現場面談的實證文獻陸續出現(例如：羅新興等，2013；羅新興等，2021；Chapman and Rowe, 2001, 2002;

Susan et al., 2001; Sears et al., 2013; Weller, 2017; Langer et al., 2019），其中，Chapman and Rowe（2001）早期研究發現，在視訊面談的情況下面試官給予應徵者的評分高於現場面談；然而，晚近實證研究結果大都顯示現場面談情況下面試官給予應徵者的評分高於視訊面談情況（例如：羅新興等，2013；羅新興等，2021；Sears et al., 2013），歸納性研究（Meta-analysis）結果顯示：面試官在現場面談情況下給予應徵者的評分高於視訊面談（Blacksmith, 2016），可能是在電腦媒介的溝通模式中，因視覺線索的減少而降低社會臨場感（Sia et al., 2002），由於視訊面談所提供的社會線索較少，面試官可能出現保守心態而在視訊面談給予應徵者評分相對較低（羅新興等，2013；羅新興等，2021；Baker et al., 2020）。上述文獻推測面談媒介可能是應徵者因素影響面試官評分的調節變數，如果是，那麼應徵者專業能力與外表吸引力對面試官評分的替代效果或加乘效果，也可能因為現場或視訊面談而有不同。

診斷性訊息是指個體判斷決策所參照的高關聯性訊息，非診斷性訊息則是對於判斷決策影響較低的訊息（羅新興與李幸穗，2004）。依據經驗法則，應徵者的專業能力應該是面談決策的診斷性訊息，然而，應徵者的外表吸引力是面談決策的診斷性訊息或非診斷性訊息呢？羅新興與李幸穗（2004）指出，面試官在接收應徵者所呈現出的各種訊息時，專業能力是判斷應徵者工作績效具直接關聯性的診斷性訊息，但外表吸引力則是判斷應徵者工作績效無直接關係的非診斷性訊息，只能對專業能力有彌補作用。雖然當時的實證資料驗證了這個論點，但該實證文獻的模擬面談是採用拍攝面談影片進行專業與容貌吸引力的操弄，如果在現場互動面談或者視訊互動面談的情況下，應徵者的外表吸引力對於面試官是否依然是非診斷性訊息呢？依據注意力容量模型（A Capacity Model）的觀點，個體的注意力是一個處理有限的容量，當處理的資訊愈多則注意力愈分散，處理的資訊量愈少則注意力愈集中（Kahnemen, 1973）。注意力容量模型認為注意力是分類和辨識刺激的認知資源（Cognitive Resources），這些認知資源不是無限的，當個體面對越複雜的刺激（例如需同時執行多項任務），就需要越多資源；如果同時出現許多複雜的刺激，認知資源就會很快被用盡（Kahneman, 1973）。當周遭環境同時呈現大量刺激時，人類有限的認知資源就只能處理部分最重要刺激，其它刺激則無法處理；若個體所接受的刺激與訊息沒有超過認知資源之容量限制時，所有訊息皆可得到適度且完善之處理（Kahneman, 1973）。本研究推測：面試官在視訊面試過程中要處理的資訊量可能低於現場面談，在視訊面談過程中，面試官要處理的資訊包括應徵者的語言訊息、非語言訊息（肢體行為、外表吸引力），相對於現場面談，除了聲音及影像以外的其他訊息相對較少，可能導致面試官對於外表吸引力的注意力提高，從而導致外表吸引力提升為視訊面談的診斷性訊息。依據上述推論研究假說如下：

假說：現場面談情況下，應徵者專業能力與外表吸引力對面試官評分的影響是替代效果；視訊面談情況下，應徵者專業能力與外表吸引力對面試官評分的影響是加乘效果。

三、研究方法

3.1 研究對象與有效樣本分布

本研究以企業組織人員為實證對象，資料蒐集方法採便利抽樣，受試者為臺灣北部

某科技大學白天工作的進修部大學生及碩士研究生，在教室進行集體施測。16 個施測班級分配八種實驗情境中(每種情境兩個班級，人數不等)，受試者模擬擔任未發問問題的面試官，每班最多施測人數為 30 人。本研究共發出 395 份問卷，回收問卷後以目測檢視問卷，針對所有題項均回應相同者、填答明顯規律性者、漏答者以及面談媒介檢測題答錯者，均視為無效問卷而予以刪除。例如 Likert 尺度衡量的第 5 題是衡量面試官給予應徵者評價的反向題，如果受試者所有題目填答相同者尺度者視為無效問卷。刪除的 75 份無效問卷中，多數屬於面談媒介檢測題答錯刪除，原因可能是部分受試者誤認為發問問題的研究者在現場，所以回答視訊面談為現場面談。有效問卷 320 份，其中，男性 175 人(54.7%)、女性 145 人(45.3%)；年齡 25 歲以下者 234 人(73.1%)、25-30 歲者 38 人(11.9%)、31-35 歲者 15 人(4.7%)、36-40 歲者 9 人(2.8%)、41 歲以上者 24 人(7.5%)；學歷為大學專科者 290 人(90.6%)、碩士者 30 人(9.4%)；組織身分為基層員工者 282 人(88.1%)、公司主管者 38 人(11.9%)；參與視訊面談者 173 人(54.1%)、參與現場面談者 147 人(45.9%)；參與應徵者專業不佳情境者 154 人(48.1%)、參與應徵者專業佳情境者 166 人(51.9%)；參與應徵者外表吸引力低情境者 163 人(50.9%)、參與應徵者外表吸引力高情境者 157 人(49.1%)。

3.2 實驗設計與流程

本研究採用 2(專業能力佳、專業能力不佳)×2(外表吸引力高、外表吸引力低)×2(現場面談、視訊面談)的全受試者間的類實驗設計，每位受試者會接受八種模擬面談情境的其中一種。本研究遴選英文口說能力佳的助理扮演應徵者，受試者模擬擔任未發問問題的面試官，為了控制模擬面談的實驗情境，面談問題都是事先設計好的結構性問題，並由研究者代表所有面試官發問問題，應徵者(研究助理)依據事先撰寫好的腳本回答問題內容、穿著裝扮及肢體語言。受試者觀看面談全程後填寫問卷，評量應徵者的面談表現。研究者事先在某科技大學應用外語系遴選英語口說流利的二位研究助理(一位稍胖、一位正常)，外表吸引力的操弄採用身材(胖瘦)容貌、化妝技巧以及穿著打扮。在專業能力的操弄方面，本研究利用指導語告知面試官(受試者)任務是代表貿易公司甄選具有英語溝通能力的行政助理，二位原本英語口語能力佳的助理，依據事先設計的面談對話腳本(英語口說能力高低差異)呈現出應徵者的專業高低，英文專業能力高低操弄項目包括使用英文的詞彙、語法文法以及流暢度等，低專業者英語結結巴巴表現，高專業能力者英語流利流場。在面談媒介的操弄方面，模擬面談分別在現場與視訊情況進行，現場面談由應徵者(研究助理)親自到教室內與面試官(研究者)進行現場對話，受試者在現場看到應徵者的表現；視訊面談則是面試官(研究者)使用 Google Meet 視訊會議軟體，連線在另一地的應徵者(研究助理)，受試者在教室投影布幕上看到應徵者的表現。

本實驗流程首先由研究者事先以電子郵件徵詢部分授課老師同意，然後排定施測時間，實驗當天由研究者向受試者說明實驗流程及指導語約 4 分鐘，確保受試者在知情同意情況下自主參與實驗；接著，進行視訊(或現場)的模擬面談約 4 分鐘；最後，發下問卷與禮品，讓受試者依據應徵者的模擬面談表現進行約 5 分鐘的問卷填寫，填寫完畢後由研究者現場收回問卷。

3.3 實驗操弄檢測

本研究針對面談媒介、應徵者專業能力以及外表吸引力進行實驗操弄，問卷中詢問受試者三個實驗操弄檢測的問題，分別 1.我覺得剛剛這位應徵者的專業表現：□專業佳□ 專業普通；2.我覺得剛剛這位應徵者的容貌吸引力：□吸引力佳□吸引力普通；3.我剛剛面談的媒介是：□現場□視訊。然後分別進行卡方檢定以確認實驗操弄是否成功，意即檢定受試者回答情境與研究者操弄情境是否有關，其中，因面談媒介是客觀事實，如果受試者填答不正確即視為無效問卷而刪除，專業能力高低以及外表吸引力高低則是主觀知覺，採卡方檢定檢測操弄是否成功。實驗操弄檢測結果如表 1。由表 1 的檢定結果得知，無論是面談媒介、專業能力或外表吸引力，三項的卡方檢定結果均達統計顯著，受試者確實知覺視訊與現場兩種不同面談媒介(回答錯誤者視為無效問卷，已刪除)；接受操弄專業不佳應徵者的模擬面談情境的受試者中，有 123 人知覺應徵者為專業不佳，有 31 人知覺應徵者為專業佳；接受操弄專業佳應徵者的模擬面談情境的受試者中，有 115 人知覺應徵者專業佳，有 51 人知覺應徵者專業不佳，卡方檢定結果顯著(X^2=77.78，p<.001)；接受操弄低外表吸引力應徵者的模擬面談情境的受試者中，有 149 人知覺應徵者外表吸引力低，有 14 人知覺應徵者外表吸引力高；接受操弄高外表吸引力應徵者的模擬面談情境的受試者中，有 97 人知覺應徵者外表吸引力高，有 60 人知覺應徵者外表吸引力低，卡方檢定結果顯著(X^2=99.89，p<.001)。上述資料分析結果顯示：本研究對面談媒介、應徵者專業高低以及應徵者外表吸引力高低的實驗操弄是成功的。

表1　實驗操弄檢測分析結果

受試者回答面談媒介						
		視訊		現場		卡方值
		人數	比例	人數	比例	
面談媒介	視訊	173	54.1%	0	0%	320.00***
	現場	0	0%	147	45.9%	
受試者回答專業高低						
		專業低		專業高		卡方值
		人數	比例	人數	比例	
專業高低	專業低	123	38.4%	31	9.7%	77.78***
	專業高	51	15.9%	115	35.9%	
受試者回答吸引力高低						
		吸引低		吸引高		卡方值
		人數	比例	人數	比例	
吸引力高低	吸引低	149	46.6%	14	4.4%	99.89***
	吸引高	60	18.8%	97	30.3%	

3.4 變項衡量工具

在本研究問卷內容中，「應徵者表現評價」採用陳建丞與蔡維奇(2005)的 5 題中文量表，正向題例如：「這位應徵者的表現很好」，負向題例如：「我絕對不會讓這位應徵者進入我的公司任職」。受試者參加實驗對模擬應徵者進行評分，可能會考慮應徵者是研究助理，給予模擬應徵者的評分可能產生社會期許偏誤，故，本研究衡量受試者社會期許納入統計模型控制，社會期許量表採用 Hays et al.(1989)所發展的三題負向題量表，例如：「我偶爾會佔別人的便宜」，均採 Likert 6 點尺度衡量。此外，本研究採受試者間設計，意即相同班級的人集體施測的便利抽樣，每位受試者並非隨機分配到不同情境。本研究擔心受試者的個體變項可能混淆研究結果，故將受試者變項納入統計控制，包括受試者的性別、年齡、學歷、組織身分(主管、員工)。由於本研究對於量表文字進行潤飾，故，採用最大變異轉軸法進行探索性因素分析，以檢視兩個不同衡量的構念效度。分析結果如表 2。表 2 顯示每個題目在歸類因子上的因素負荷量均達 0.5 以上，8 個題目萃取二個因素的變異解釋量分別為 47.04%與 24.97%，累積解釋變異量達 72.01%。其中，第 5 題為應徵者表現評價的負向衡量題目，第 6 題至第 8 題是社會期許的負向衡量題目，表 2 的資料分析前已經先將其轉向編碼為正向題，後續的相關分析以及變異數分析亦均採正向編碼所呈現結果。

表 2　探索性因素分析結果

衡量題項	因素	
	應徵者表現評價	社會期許
1、整體而言，這位應徵者的表現很好。	**.88**	.00
2、整體而言，我願意錄取這位應徵者。	**.91**	-.03
3、整體而言，我願意給這位應徵者進一步面談的機會。	**.88**	.07
4、整體而言，我會希望這位應徵者成為我的同事。	**.89**	-.02
5、整體而言，我絕對不會讓這位應徵者進入我的公司任職。	**.73**	-.21
6、我偶爾會佔別人的便宜。	-.05	**.84**
7、我有時候會嘗試報復，而不是原諒別人。	-.15	**.82**
8、我有時候會因為不能隨心所欲而感到生氣。	.09	**.78**
解釋變異量	47.04%	24.97%
累積解釋變異量		72.01%

註：*N*=320。

四、資料分析結果

4.1 簡單相關分析

本研究主要變項的平均數、標準差、變項間相關係數與量表內部一致性的統計分析結果如表 3。表 3 的資料分析結果顯示，社會期許的內部一致性係數為.74，面談表現評價的內部一致性係數為.91，兩者信度均尚可。依據編碼規則解讀類平均數，專業高低的

平均數(*M*=.52)表示 52%受試者參與應徵者專業高的情境，吸引高低平均數(*M*=.49)表示 49%受試者參與應徵者外表吸引力高的情境，面談媒介平均數(*M*=.46)表示 46%受試者參與現場面談情境。觀察表 3 的相關係數可以發現，應徵者專業能力與面試官給予應徵者評分之間具有顯著正相關(r=.31，p<.001)，表示應徵者專業能力愈高則面試官會給予愈高的評分。應徵者外表吸引力與面試官給予應徵者評分之間具有顯著正相關(r=.36，p<.001)，表示應徵者外表吸引力愈高則面試官會給予愈高的評分。簡單相關係數並未發現面談媒介與面試官給予應徵者評分具有顯著的關聯性(r=.03， p>.10)，但後續控制相關變數後的變異數分析結果則呈現邊際關聯性(F=3.6, p<.10)。

表 3　平均數、標準差、相關係數與量表內部一致性

變項	Mean	S.D.	1	2	3	4	5	6	7	8	9
1.性別	.55	.50									
2.年齡	1.60	1.19	-.12*								
3.學歷	2.09	.29	-.14*	.49***							
4.組織身分	.12	.32	.10+	.30***	.05						
5.社會期許	3.03	1.09	.21***	-.05	.07	-.11*	(.74)				
6.專業高低	.52	.50	.13*	.01	.10	-.09+	.11*				
7.吸引高低	.49	.50	-.07	-.15**	-.32***	-.03	-.12*	-.03			
8.面談媒介	.46	.50	-.06	.30***	.35**	.11+	-.02	.01	-.04		
9.面試評分	4.33	.97	.04	-.18***	-.17**	-.10+	-.09	.31***	.36***	.03	(.91)

註 1：編碼規則：男性 1，女性 0；25 歲以下 1，26~30 歲 2，31~35 歲 3，36~40 歲 4，41 歲以上 5；高中職(含)以下 1，大學專科(含就讀中)2，碩士(含就讀中)以上 3；公司主管 1，基層員工 0；專業高 1，專業低 0；吸引力高 1，吸引力低 0；現場面談 1，視訊面談 0。

註 2：括弧數字為內部一致性係數； +表 p<.10, *p<.05, **p<.01, ***p<.001; N=320。

4.2 不同面談媒介下應徵者專業能力與外表吸引力對面試官評分的影響

觀察表 3 的簡單相關分析結果發現：受試者的年齡、學歷、組織身分會影響面試官給予應徵者的評分，此外，研究發現受試者的性別、年齡與職級身分會影響面試官給予應徵者的評分(羅新興等，2014；羅新興等，2022)，因此後續假說檢定的迴歸分析模型，將性別、年齡、學歷、組織身分及社會期許納入統計控制，應徵者專業能力、應徵者外表吸引力及面談媒介三個主要變數，以一般線性模型(GLM)針對面試官給予應徵者的評分進行多因子變異數分析，分析結果如表 4，平均數列聯表如表 5，交互作用示意圖如圖 1 及圖 2。

表 4 分析結果呈現專業高低、吸引力高低、面談媒介的三階交互作用結果顯著(F=6.93，p<.01)。觀察表 5 的平均數發現，在**視訊面談**情境下，面試官給予外表吸引力低但專業能力高應徵者的評分(M=3.86)僅稍高於外表吸引力低且專業能力低應徵者(M=3.71)；但是，面試官給予外表吸引力高且專業能力高應徵者的評分(M=5.19)明顯高於外表吸引力高但專業能力低應徵者(M=4.17)，換句話說，應徵者的外表吸引力會使得專業能力對於面試官評分的影響力提高。在**現場面談**情境下，面試官給予外表吸引力低但專業能力高應徵者的評分(M=4.61)高於外表吸引力低且專業能力低應徵者(M=

3.93)；面試官給予外表吸引力高且專業能力高應徵者的評分(M＝4.86)也高於外表吸引力高但專業能力低應徵者(M＝4.30)，易言之，應徵者的外表吸引力反而使得專業能力對於面試官評分的正向影響力微幅降低。觀察圖 1 及圖 2 的交互作用示意圖可以發現，在視訊面談與情況下，應徵者專業能力與外表吸引力對面試官給予應徵者評分是 1+1>2 的加乘效果，在現場面談情況下，專業能力與外表吸引力對面試官評分的二階交互作用不顯著(微幅替代效果)。故，本研究提出之「現場面談情況下，應徵者專業能力與外表吸引力對於面試官評分是替代效果；視訊面談情況下，應徵者專業能力與外表吸引力對於面試官評分具有加乘效果。」的研究假說獲得實證資料的部分支持。

表 4　面試官評分的變異數分析結果

變異來源	SS	DF	MS	F檢定
校正後的模式	93.95	12	7.83	11.63***
截距	92.04	1	92.04	136.70***
性別	.13	1	.13	.19
年齡	1.03	1	1.03	1.53
學歷	.75	1	.75	1.11
組織身分	.84	1	.84	1.25
專業高低	27.76	1	27.76	41.23***
吸引力高低	24.22	1	24.22	35.98***
面談媒介	2.43	1	2.43	3.60+
面談媒介×專業高低	6.74	1	6.74	10.01**
吸引力高低×面談媒介	.03	1	.03	.04
吸引力高低×專業高低	2.74	1	2.74	4.07*
專業高低×吸引力高低×面談媒介	4.67	1	4.67	6.93**
社會期許	3.11	1	3.11	4.62*
誤差	206.71	307	.67	
總和	6302.04	320		
校正後的總數	300.66	319		

註：+ p<.10, *p<.05, **p<.01, ***p<.001; N=320。

表 5　不同面談媒介下專業能力高低與外表吸引力高低之面試官評分

		應徵者專業					
		低		高		合計	
		平均數	標準差	平均數	標準差	平均數	標準差
視訊	吸引力低	3.71	.13	3.86	.13	4.23	.07
	吸引力高	4.17	.13	5.19	.12		
現場	吸引力低	3.93	.15	4.61	.14	4.42	.07
	吸引力高	4.30	.14	4.86	.15		
合計		4.02	.07	4.63	.07		

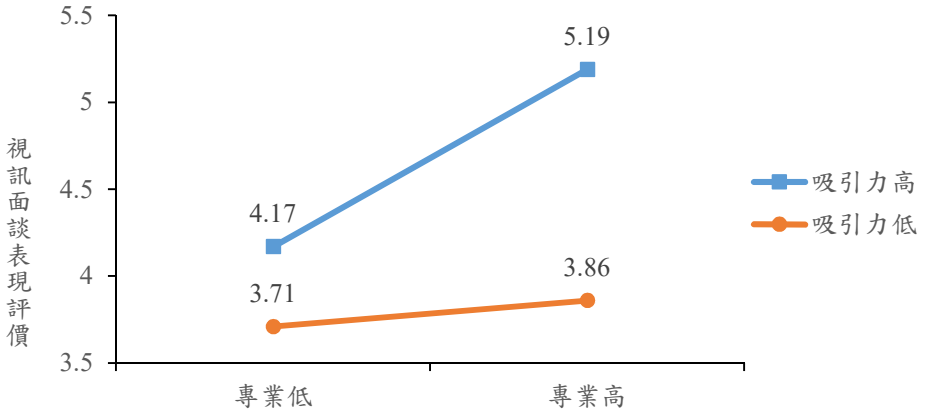


圖 1　視訊面談下專業高低與吸引力高低對面試官評分的交互作用示意圖

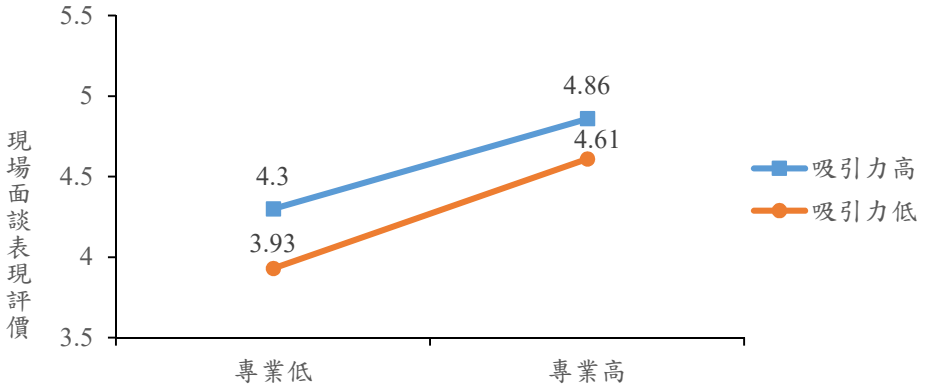


圖 2　現場面談下專業高低與吸引力高低對面試官評分的交互作用示意圖

五、討論與國防管理實務意涵

5.1 綜合討論

專業能力是指能有效執行工作任務的知識與技能，擁有專業能力的員工可以提高對組織的貢獻，故應徵者的專業能力是面試官評分所依據的重要因素。外表吸引力為應徵者給人的第一印象，雖然外表吸引力與工作能力是兩回事，但應徵者外表吸引力仍會影響面試官給予應徵者的面談表現評價。本研究的資料分析結果發現了面談媒介、應徵者專業能力及應徵者外表吸引力對於面試官評分具有顯著的三階交互作用，結果顯示：在現場面談情況下，應徵者專業能力與外表吸引力對面試官給予應徵者評分僅微幅替代效果，研究發現和羅新興與李幸穗(2004)的資料分析結果態樣相似；但是，在視訊面談情況下，應徵者專業能力與外表吸引力對面試官給予應徵者評分具有顯著加乘效果。依據Kahnemen(1973)的注意力容量理論觀點，資訊處理量的提高會降低對特定資訊的注意力，資訊量的減少可以提高注意力，在視訊面談情況下，面試官對應徵者的訊息關注層面較少，透過遠距的視訊畫面互動，原本屬於非診斷性訊息的外表吸引力，提升為對面談表現評分具支配性的診斷性訊息，因而大幅度的提高了專業能力佳且外表吸引力高應徵者的評分。

本研究的模擬面談實驗發現，除了驗證注意力容量理論(Kahnemen, 1973)的觀點外，最主要的價值在於補足過去文獻有關視訊面談與現場面談比較的實證缺口。過去因為視訊面談尚未普及運用，許多探討應徵者因素或面試官因素對面談評分的實證文獻，是在現場面談情境下完成的研究報告，本研究發現不同的面談媒介(視訊面談、現場面談)，

可能會使得某些應徵者因素對面試官給予應徵者評分的影響改變。陳建丞(2007)研究發現面談結構性可以減緩應徵者外表吸引力對面試官評分的影響，那麼，在視訊面談情況下，面談結構性對於減緩外表吸引力對面試官評分影響的程度，是否不同現場面談的情況下呢？類似問題有待後續研究持續驗證，以補足視訊面談情況下的實證缺口。

5.2 國防人力資源管理的應用意涵

無論遠距工作型態、視訊面議，或是遠距甄選面談，視訊的使用已經日益普遍。本研究的發現可以應用在國防人力資源管理實務，包括國軍人才招募面談、考績評鑑面談以及派職任用面談，建議面試官需要準備充足的結構性面談問題清單，專注於面談過程待釐清的問題重點(例如：專業證照、態度特質、工作經驗等)，尤其是在視訊面談的情況下，提醒自己避免受到應徵者非診斷性訊息(例如：外表吸引力、印象管理策略)的支配性影響，才能更精準地替國軍甄選具真正專業的人才。依據本研究發現，建議應徵者(或：被評估者)在視訊面談過程想要獲得更正面的評價，除了要呈現出自己最好的專業表現外，千萬不要忽視呈現外表吸引力，建議要適度的妝扮、親切的笑容以及專注的眼神等，例如：視訊面談時的眼神應該專注鏡頭，而非專注螢幕，透過彼此眼神交會而產生吸引力，如此可能讓面試官感到備受尊重，因而獲得更佳的評價。

5.3 研究限制與未來研究方向

本研究採用模擬面談實驗進行研究，具有以下若干限制，提醒讀者謹慎解讀研究結果。首先，本研究受試者年齡偏低，工作年資及經驗相對較少，並且多數受試者的組織身分為基層人員，實際擔任面試官的經驗相對缺乏，同時為了控制情境變數，模擬面談過程未提供面試官自由發問問題，缺乏真實面談的臨場感，建議後續研究以職場曾經擔任面試官者為受試者，並且提供問題清單輪流發問，以提高研究結果應用的外部效度。雖然本研究對外表吸引力的操弄檢測是成功的，不過，由妝扮不同的兩位助理分別扮演高低外表吸引力的應徵者，其聲音、語調等細節仍可能因人而異，可能會影響實驗控制的穩定度，建議後續研究者純粹運用化妝技巧操弄外表吸引力，以提高實驗的內部效度。此外，可以預見未來將呈現科技發展大幅躍進，建議後續研究方向可以結合影像科技，更精緻分析應徵者面談過程的語言及非語言訊息對於面試官評分的影響。

參考文獻

陳建丞、蔡維奇（2005）。面談前印象對面試官評量效應之影響：以面談結構性為干擾變數。*臺大管理論叢*，16（1），155-170。

陳建丞（2007）。甄選面談中外表與性別偏誤之探討：結構式面談能消除它們嗎？*臺大管理論叢*，18（2），183-208。

羅新興、李幸穗（2004）。應徵者面談過程所呈現的訊息對面談表現評價的影響：以企業員工的招募甄選為實驗情境。*人力資源管理學報*，4（3），55-72。

羅新興、林韶姿、劉佩玲（2014）。面試官與應徵者的性別組合對面談評價之影響：大學教師徵選面談的實證。*臺大管理論叢*，25（1），215-232。

羅新興、高婷鈺、羅景文（2021）。視訊面談與現場面談情況下面試官給予應徵者表現評價的比較：面試官調節焦點之干擾效果。*人力資源管理學報*，21（2），55-72。

羅新興、梁成明、王彥蓁（2022）。專業能力對面談表現評分的影響—男性與女性面試官在視訊與現場面談之差異。*中原企管評論*，20（3），83-104。

羅新興、梁成明、諸承明（2009）。相同能力應徵者的禮貌與容貌對能力評價的影響-探討面談者年齡與性別組合的干擾效果。*人力資源管理學報*，9（1），69-85。

羅新興、蕭金蘭、羅右杰（2013）。視訊面談與臨場面談的面談表現評價之比較-職務-履歷適配之干擾作用。*組織與管理*，6（1），121-140。

Anderson, J. C., Johnson, E. N., & Kaplan, S. E. (1994). Perceived effects of gender, family structure, and physical appearance on career progression in public accounting: A research note. *Accounting, Organizations and Society*, *19*(6), 483-491.

Anderson, J. C., & Shackleton, V. (1990). Decision making in the graduate selection interview: A field study. *Journal of Occupational Psychology*, *63*, 63-76.

Anderson, J. C., & Shackleton, V. (1993). *Successful Selection Interviewing*. Blackwell: Oxford.

Arvey, R. D., & Campion, J. E. (1982). The employment interview: A summary and review recent research. *Personnel Psychology*, *35*, 281-322.

Baker, D. A., Burns, D. M., & Kueny, C. R. (2020). Just Sit Back and Watch: Large Disparities between Video and Face-to-face Interview Observers in Applicant Ratings. *International Journal of Human-computer Interaction*, *36*(20), 1968-1979.

Barclay, J. M. (1999). Employee selection: A question of structure. *Personnel Review*, *28*(1/2), 134-151.

Beehr, T. A., & Gilmore, D. C. (1982). Applicant attractiveness as a perceived job-relevant variable in selection of management trainees. *Academy of Management Journal*, *25*(3), 607-617.

Blacksmith, N., Willford, J. C., & Behrend, T. S. (2016). Technology in the employment interview: A meta-analysis and future research agenda. *Personnel Assessment and Decisions*, *2*(1), 12-20.

Campion, M. A., Palmar, D. K., & Campion, J. E. (1997). A review of structure in the selection interview. *Personnel Psychology*, *50(*3), 655-702.

Chapman, D. S., & Rowe, P. M. (2001). The impact of videoconference technology, interview structure, and interviewer gender on interviewer evaluations in the employment interview: A filed experiment. *Journal of Occupational & Organizational Psychology*, *74*(3), 279-298.

Chapman, D. S., & Rowe, P. M. (2002). The influence of videoconference technology and interview structure on the recruiting function of the employment interview: A filed experiment. *International Journal of Selection and Assessment*, *10*(3), 185-197.

Dipboye, R. L. (1992). Social Interaction in the Interview. In R. L. Dipboye (Ed.). *Selection Interview: Process Perspectives*, Cincinnati, OH: South-Western, 75-100.

Ellemers, N., van den Heuvel, H., de Gilder, D., Maass, A., & Bonvini, A. (2004). The underrepresentation of women in science: Differential commitment or the queen bee syndrome? *British Journal of Social Psychology*, *43*, 315-388.

Hays, R. D., Hayashi, T., & Stewart, A. L. (1989). A five-item measure of socially desirable response set. *Educational and Psychological Measurement*, *49*(3), 629-636.

Kahnemen, D. (1973). *Attention and Effort*, Englewood Cliffs, NJ: Prentice-Hall.

Langer, M., Konig, C., & Papathanasiou, M. (2019). Highly automated job interviews: Acceptance under the influence of stakes. *International Journal of Selection and Assessment*, *27*(3), 217-234.

Marlowe, C. M., Schneider, S. L., & Nelson, C. E. (1996). Gender and attractiveness biases in hiring decisions: Are more experienced managers less biased? *Journal of Applied Psychology*, *81*(1), 11-21.

Mast, M. S., Bangerter, A., Bulliard, C., & Aerni, G. (2011). How accurate are recruiters' first impressions of applicants in employment interviews? *International Journal of Selection & Assessment*, *19*(2), 198-208.

McArthur, L. Z., & Baron, R. M. (1983). Toward an ecological theory of social perception. *Psychological Review*, *90*(3), 215-238.

Podratz, K. E., & Dipboye, R. L. (2002). In search of the "beauty is beastly" effect. In *17th Annual Conference of the Society for Industrial and Organizational Psychology*. Toronto, Canada.

Sears, G. J., Zhang, H., Wiesner, W. H., Hackett, R. D., & Yuan, Y. (2013). A comparative assessment of videoconference and face-to-face employment interviews. *Management Decision*, *51*, 1733-1752.

Sia, C. L., Tan, B. C. Y., & Wei, K. K. (2002). Group polarization and computer mediated communication: Effects of communication cues, social presence, and anonymity. *Information Systems Research*, *13*(1), 70-90.

Susan, S. G., Milesb, J. A., & Levesquec, L. L. (2001). The effect of videoconference, telephone, and face-to-face media on interviewer and applicant judgments in employment interviews. *Journal of Management*, *27*(3), 363-381.

Weller, S. (2017). Using internet video calls in qualitative (longitudinal) interviews: some implications for rapport. *International Journal of Social Research Methodology*, *20*(6), 613-625.

「國防管理學報」徵稿與評審辦法

壹、目的與範圍

「國防管理學報」係為國防大學管理學院發行之學術期刊，凡舉人力資源、財務管理、物流管理、科技管理、資訊管理、資源決策、國防法制、採購管理、戰場管理等學術領域，尤為與軍事結合之論述，或能闡明其軍事管理意涵之稿件，竭誠歡迎專家學者投稿。凡來函稿件以原創性及回顧性論文為主，已發表在其他期刊或審稿中的文章將不接受刊登，稿件文章力求精簡嚴謹，本學報支付稿酬，不收取刊登費用，贈送作者當期學報乙冊，來稿採隨到隨審方式全年徵稿。

稿件篇幅不得超過 20 頁（約 2 萬字）。本學報不收取刊登費用，來稿採隨到隨審、雙向匿名方式進行審查，全年徵稿；自第四十卷第一期起，來稿一經刊載，即依本刊規定奉致稿酬。

貳、投稿方式與格式

本學報為半年刊，每年五、十一月出刊，為便利本學報編審及出版作業，採系統投稿與信箱投稿之雙軌制，來稿敬請將 word 檔逕寄「國防管理學報信箱」journalofndm@gmail.com，並同時於國防大學網站報名（步驟：國防大學首頁左下角→雜誌期刊專區內之雜誌期刊投、審稿作業→報名投稿→送出），以利加速審稿時效。

若有相關問題請洽詢國防大學管理學報　承辦人(陳正忠先生　電話 02-28948714)。

參、評審辦法

評審作業方式由主編推薦兩位相關領域審查人員擔任稿件審查工作，審查意見共分四級，分別為拒絕、修改後再審、修改後主編審閱(原審者不須過目)、刊登，凡經審查接受者始得刊登本學報，審查結果處理方式如下表：

		第二位評審意見			
		拒絕	修改後再審	修改後主編審閱(原審者不需過目)	刊登
第一位評審意見	拒絕	不宜刊登	不宜刊登	送第三人審	送第三人審
	修改後再審	不宜刊登	修改後再審	修改後送第一位原審者再審	修改後送第一位原審者再審
	修改後主編審閱(原審者不需過目)	送第三人審	修改後送第二位原審者再審	修改後刊登	修改後刊登
	刊登	送第三人審	修改後送第二位原審者再審	修改後刊登	刊登

作者須自負文責，並請注意不得違反國軍保密與著作權等相關規定，對審查人員所建議刊登之文章，將隨即進行保密安全查核，凡經查核有疑慮者仍將無法刊登，且編審委員對來稿有刪改或建議修正權，不願刪改時應於稿件上預先註明，不適合刊登之稿件則退還原作者，並附專家學者審查意見供投稿人參考，如有未盡事宜，得經本校編輯委員會補充訂定之。

國防管理學報論文格式範例

王曉明[1]　李大華[2*]

[1] 國防大學資源管理及決策研究所

[2] 國防大學財務管理學系

摘要

本文舉例說明國防管理學報所採用之排版格式，供投稿人編排論文參考之用。首先稿件全文中文部分皆使用標楷體，全形符號，英數的部分則使用 Times New Roman 字型，論文可以中(英)文方式書寫，中(英)文論文必須加附英(中)文題目、作者姓名、單位、摘要及關鍵詞於中(英)關鍵詞(Keywords)之後。英文姓名依護照外文姓名書寫方式，姓在前，名在後，姓之後加逗點，名與名之間加短劃「-」連結。中文關鍵詞分隔符號以頓號「、」進行分隔，英文關鍵詞字首大寫，以半形逗號「,」分隔，關鍵詞後均不加句號。中(英)題目為粗體 16 點字，作者姓名粗體 14 點，單位粗體 11 點，摘要標題粗體 12 點，摘要本文 12 點，關鍵詞標題粗體 12 點。當題目過長無法以一行表示時，必須以倒三角的方式排列。題目、作者姓名、單位、摘要標題與摘要本文之間必須間隔一行來表示。

關鍵詞：國防大學、管理學院、國防管理學報(3-5 個為宜)

English Title

Wang, Siao-Ming[1]　Li, Da-Hua[2*]

[1] **Graduate School of Resources Management and Decision Science, National Defense University, *Taiwan*, *R.O.C.***

[2] **Department of Financial Management, National Defense University, *Taiwan*, *R.O.C.***

Abstract

Please provide the English abstract in 300 words and keywords.

Keywords: National Defense University, Management College, Journal of National Defense Management (3-5 keywords)

---

[*] 聯絡作者：李大華 email: wsf@gmail.com　聯絡作者之 email 請以[*]註腳方式列示於首頁

[1] 註腳不論中英文，請附註在當頁下方，且儘可能少用並以參考文獻代之。任何編排上的問題請電 02-28986600-604813　軍線：604813　E-mail：journalofndm@gmail.com 陳先生。

一、內容格式(大段落標題一律置中)

文章用 A4 大小的紙張，每頁上下緣及左右側各留 2.5 公分，文章以單欄方式打字且左右對齊，採單行間距。

文章內容依序包含中(英)文標題、中(英)文作者、中(英)文摘要、中(英)文關鍵詞、英(中)文題目，英(中)作者姓名、英(中)服務單位、英(中)摘要、英(中)關鍵詞，本文、誌謝、參考文獻、附錄等順序書寫。文稿以不超過 20 頁為原則，應能以印表機清晰列印，且避免使用有保密標號之浮水印影本，減少影響文稿內容之呈現。

1.1 段落編碼方式(中小段落標題靠左對齊)

段落編碼區分中文與英文兩種文稿。中文段落編排分別依一、1.1、1.1.1 順序排列(如圖 1 所示)，英文段落編排則依 1.、1.1、1.1.1 順序排列(如圖 2 所示)。

一、前言(14 級粗黑標楷體，置中)

1.1 設計量度(12 級粗黑標楷體)

1.1.1 可信度(12 級標楷體)

圖 1　中文段落編碼範例

2. Literature Review (14-pt bold Times New Roman, centered)

2.1 Corporate Governance (12-pt bold Times New Roman)

2.1.1 Board structure (12-pt Times New Roman)

圖 2　英文段落編碼範例

1.2 段落

每一段落開始，縮排兩字元，文內所出現之英數使用 Times New Roman 字型，中文稿中之英文詞及括號內之英文對照，除專有名詞外一律小寫表示，文稿經審查被接受時，作者不得擅自於校稿過程中增減內容，僅能就審查委員建議及排版錯誤修正。

二、圖表及方程式格式

2.1 圖片

不論是圖或表必須註明圖(表)號、圖(表)稱以及資料來源，來源格式請參考內文引用格式，若資料來源自研究者本身時則不需註明，文中所用之圖表、照片力求能以雷射列表機清晰印出，其圖標題必須置於圖片下方。若圖標題僅使用一行，則必須置中，否則應靠左對齊。圖(表)必須用阿拉伯數字加以編號，之後不需要加任何標點符號如「：」，直接註明圖(表)稱即可。如文中引用時應指出圖號與表號來指引讀者，避免使用「如下圖所示」來表示。

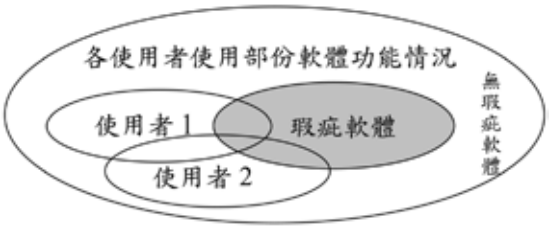


圖 3　軟體使用模式

資料來源：王曉明與李大華(2004)

2.2 表格

表標題必須置於表格上方且置中。如表 1：

表 1　模組轉換機率表

資料來源：Wang and Li(2004)

2.3 方程式

方程式應於上下各留一行空白，方程式應編號，編號靠右對齊並從(1)開始。如下例：

$$Q_{ij} = R_i p_{m_{ij}} \qquad (1)$$

三、內文引述格式

3.1 內文引述文獻

內文引述文獻應依中、英文稿之不同，遵循不同的格式要求。請同時注意以下範例之字體、斜體、底線、標點符號等規定。

3.1.1

內文中引用文獻需含作者及出版年份，出版年份置於標楷體半形括號中，引用英文文獻時，除了少數情形例如同姓的英文作者外，只需列出作者姓氏，中文引用文獻要列出作者全名。例如：A(年度)。若引用文獻有兩位作者，請用「與」或「and」字連接，例如：A 與 B(年度)或 A and B(年度)。若引用文獻有三人以上時，中文為 A 等(年度)而英文為 A et al.(年度)。

3.1.2

引述文獻的括號內包含參考文獻之作者與出版年份時，請以「逗號」連接，例如：中文為(A 與 B，年度)而英文為(A and B, 年度)。若文獻有三人或以上時，中文為(A 等，年度)而英文為(A et al., 年度)。

3.1.3

英文專有名詞字首以大寫書寫並與縮寫之間用半形分號隔開。例如資料包絡分析法(Data Envelopment Analysis; DEA)。

3.1.4

括號內同時有多筆文獻時，中文引述文獻不同作者之間請用全形分號隔開，相同作

者不同年代之文獻請用全形逗號隔開；英文引述文獻不同作者之間用半形分號加空格隔開，相同作者不同年代之文獻用半形逗號加空格隔開。

四、國防領域之應用

本段乃鼓勵作者以 500 字以內簡述本論文於國防相關事務之可能性應用；舉凡人力資源、財務管理、物流管理、資訊管理、資源決策、軍事法律、採購管理、戰場管理等皆可。特別是鼓勵無法直接以軍事單位或國防事務為研究對象之專家學者，依其專業，提出於國防事務應用之價值與可能性，以拓展學刊之多元性，也讓實務工作者可以明瞭此論文於實務之應用與價值。

誌謝

若需要於本文末段簡短表達無則可免。

五、參考文獻

參考文獻須於本文引用才能列出，內文引用的文獻也必須列於參考文獻中。參考文獻不須編碼，區分中文與英文，先列出中文的參考文獻再列出英文的參考文獻，中文文獻依姓氏筆劃順序排列，筆劃較少的排優先，英文文獻則依字母順序排列。當不同文獻出自同一作者時，依年代排序，年代較早的文獻先列出。不論中文與英文參考文獻均採西元年代，中文期卷、頁數均採阿拉伯數字，勿用國字表示。英文參考文獻須列出姓氏以及名字（字首），中文參考文獻要列出所有作者全名。出版地以總公司所在之城市為準，出版地與出版者之間須以冒號隔開，英文書籍出版地須以城市名或州名方式處理，在出版公司之後不需加上「書局」或「出版社」等字，英文則如 Publishing Co.或 Book Company 等字，並請注意英文的標點符號全部為半形，而且在標點符號之後需空一格半形，中文則全部為全形，標點符號之後則不需空格。頁數部分則直接註明頁碼不須以「p.」或「pp.」方式，但英文報紙則須加註以表明版頁。參考文獻以凸排方式編排。所有中英文之期刊、書籍、研討會議、論文集、報告、學位論文、編輯書、翻譯書、報紙與網路之編排格式範例，請參照參考文獻部份範例，若有不足部分，請參考 APA 第六版格式相關規範。

參考文獻

王文義（1983）。談國內百貨公司專櫃制度，經濟日報，1983 年 4 月 12 日，第 16 版。

毛宣棠、傅敬群（1999）。決策理論在軟體使用模式上之應用，陸軍官校七十五年週年校慶綜合學術研討會論文集，33-38。

林彩梅（1986）。多國籍企業，台北：五南。

留忠賢譯（1997）。軟體工程，第 3 版，台北：松崗，譯自 Ian Sommerville。

張文貴（1997）。從產品使用型態談軟體品質的認證，品質學報，3（2），26-29。

許牧彥（2001）。從知識經濟的特質談台灣專利，收錄自吳思華編，知識資本在台灣，台北：遠流，297-352。

楊國隆（1997）。模糊多屬性決策分析評估武器系統，國防管理員院資源管理研究所碩士論文。

經濟部投資業務處編印（1993）。泰國投資環境簡介，20-30。

楊國隆（1999）。模糊統計之可靠度分析模式，陸軍官校八十一週年校慶綜合學術研討會，鳳山。

楊國隆（2000）。模糊多屬性決策分析評估武器系統，下載於 http://www.ndu.edu.tw/artilcles.htm（2003 年 8 月 23 日）。

楊壽仁，動態決策理論之研究，國科會補助研究報告，NSC86-2417-H-224-001。

Baron, R. A. (1993). Affect and Organizational Behavior: When and Feeling Good Matter. In J. K. Murnighan (Ed.) Social Psychology in Organization (66-68) Chichester, England: John Wiley & Sons.

Hock, D. W. (2004). Method for Measuring Intangible Asserts. From http://www.sveiby.com./articles/Inangiblemethods.htm (retrieved on May 18, 2005)

Kao, C., & Yang, Y. C. (1992). Reorganization of forest districts via efficiency measurement, *European Journal of Operational Research*, *58* (2), 356-362.

Kotler, P. (1991). *Marketing Management*, trans. John Glueck, 1993.

Kurtenbach, E. (1995). *Housing Crisis is Real Life Drama*, The China Post, July 11 1995, 12.

Liang, S. K., Yang, K. L., & Chu, P. (2003). Fuzzy multi-object programming application for time-cost trade-off of CPM in project management, *Portland International Conference on Management of Engineering and Technology'03*. U.S.A.

Mills, H. D. (1992). *Software Productivity*, 10th ed, NJ: Prentice Hall.

Rosenwein, M., 1986. Design and Application of Solution Methodologies to Optimize Problems in Transportation Logistics, Ph. D. Dissertation, Department of Decision Sciences, University of Pennsylvania, Philadelphia.

Shih, Y. C., Wang, M. J., & Chang, C. H. (1996). The effects of handle angle on maximum acceptable weight of lifting, *Proceedings of the 4th Pan-Pacific Conference on Occupational Ergonomics*, 260-263.

Simpson, B. H. (1975). Improving the Measurement of Chassis Dynamometer Fuel, Society of Automotive Engineers Technical Paper Series 750002.

附錄

和本文無直接關係或太過冗長內容請放置附錄，其內容以單欄方式放置文章之最後。

國防管理學報

JOURNAL OF NATIONAL DEFENSE MANAGEMENT

創 辦 人：果　芸
發 行 人：林振裕
出 版 者：國防大學管理學院
網　　址：https://www.mnd.gov.tw/PublishMPPeriodical.aspx?title=軍事刊物&id=22
　　(連結軍事出版品／軍事刊物／國防管理學報)
地　　址：臺北市北投區中央北路 2 段 70 號
電　　話：(02)28948714
登記證字號：行政院新聞局局版台誌第 3853 號
　　中華郵政台字第 1112 號執照登記為雜誌交寄
創刊日期：73 年元月
承 印 者：國防部軍備局生產製造中心第 401 廠北部印製室
　　TEL：(03)4801145，4801456
發 行 量：450 本
展 售 處：五南文化廣場　網址：http://www.wunanbooks.com.tw
地　　址：403 臺中市西區臺灣大道二段 85 號　電話(04)22260330
國家書店：網址：http://www.govbooks.com.tw
　　地址：104 臺北市松江路 209 號 1F　電話(02)25180207
定　　價：新台幣 350 元／本

GPN：2007300059
ISSN：1022-4858
DOI：10.29496/JNDM
中華民國一一三年五月