國 立 交 通 大 學

應用藝術研究所 工業設計組

碩 士 論 文

以 Poker 為圖像驗證碼之設計研究

The innovative design of

“Poker image-based schemes CAPTCHA”

指導教授：莊明振 教授

研 究 生：莊凱婷

中華民國一０二年七月

摘要

本研究結合網頁驗證碼概念與撲克牌的國際大眾化使用特性，設計一套具雙層驗證功能的「Poker 圖像驗證碼」，供網站使用者提交個資之安全驗證使用。

本「Poker 圖像驗證碼」充分運用了撲克牌具有數字、英文字母、色彩及圖樣等多種特性。不但無地域性限制且資料庫成本低。本研究為驗證此「Poker 圖像驗證碼」設計的使用性，以國際大眾化的 52 張傳統圖樣撲克牌做為圖片資料庫，發展了一套實驗網頁，供不同族群上網實驗。實驗第一層驗證設計：先由程式隨機從 52 張牌抽出 5 張撲克牌，並請使用者依序填寫此 5 張牌所顯示之數字(例如 2、3、...10)或英文字母(例如 J、Q、K、A)，接續進入第二層驗證設計，再請使用者在此五張牌中，辨識 spades、hearts、diamonds 及 clubs 各有幾張。若使用者填寫的雙層驗證答案均正確，則通過驗證。

實驗結果，正確通過雙層驗證之人數有 202 人，正確率為 84.88%，平均驗證操作時間 33.9 秒。 從實驗數據中發現，不同性別與教育程度在操作 (受測) 時間上並無顯著差異，然而不同年齡及職業別則有顯著差異。

在「Poker 圖像驗證碼」雙層驗證中，兩層驗證全被猜中而遭受侵襲機率為 6.11×10^{-8}，與現有網站常用之四個文、數字驗證碼被惡意自動化程式侵襲成功機率 6.77×10^{-8} 相近。實務上若採用撲克牌面之複雜圖像或多樣花色的創新設計，應不易被 OCR 破解。為深入了解本研究設計之安全性問題，特邀集自動化光學檢測、資訊工程及網路軟體等專家召開專家座談會，為本研究提供安全性之改善建議。

後續研究可運用撲克牌的多符號特性、牌面圖樣設計之複雜度增加，將之融入於「Poker 圖像驗證碼」的設計，使本驗證碼設計在使用性與安全性，能更符合網站業主及使用者之需求。

關鍵字：國際大眾化、圖像驗證碼、撲克牌、安全性、使用性。

ABSTRACT

This study combines both concepts of web page CAPTCHA and poker general using to design a new system which called poker image-based schemes CAPTCHA. It could refer transaction or interaction for website security verification.

"Poker image-based schemes CAPTCHA" takes general poker cards as database. In the first layer, it will make a random choosing and five cards will be showed. The user should fill in those numbers in order to continue the second layer. In the second layer, the user should identify how many cards in spades, hearts, diamonds or clubs. Users can get pass when they make right answers in these two layers.

"Poker image-based schemes CAPTCHA" is easy to use and has no area-restriction. And, it costs less and has no problem with expanding cards drawing. What's more, it presents the features of poker cards with numbers, letters, colors, patterns and others. By using complex images, "Poker image-based schemes CAPTCHA" is hard to be cracked by OCR.

To verify the workability of "Poker image-based schemes CAPTCHA", researcher designed an experiment web page. This page could offer different groups to examine it. The correct rate is 84.88%, and an average time is 33.9 seconds for each to operate.

The study found there has no significant difference in operating time by different gender, and different education background. However, different age and career could cause the dissimilarity.

The following studies may use poker cards' multiple symbol characteristics to increase the pattern design complexity and connect the "Poker image-based schemes CAPTCHA" design to meet website owners and users' qualifications.

Keywords: Internationalization and popularization, Image-based schemes, Poker, Security, Usability.

誌謝

本畢業論文之完成，首先感謝指導教授莊博士明振、鄧博士怡莘，才能使本論文得以完整呈現。也感謝自動光學檢測專家黃卯生博士與楊富程副理、資訊工程專家楊文昇老師、網路軟體專家林怡園技術總監，為本研究設計之安全性問題提供寶貴意見，以及感謝龍彥先、陳意婷先進在實驗統計上的協助，讓本研究實測部分得以順利完成。

也由衷感謝願意接受施測的民眾、主管、同事、朋友、同學的幫忙以及鼓勵。您們願意抽出時間為我完成這巨大的挑戰，無形的義氣相挺，點滴在心頭!

謝謝侯博士君昊、鄧博士怡莘、莊博士明振，在炙熱的六月天，百忙之中願意擔任本人口試委員，心中除了感謝還是只能用「無限感謝」這四個字來形容。

求學期間，真心感受到 IAA 眾師長們的真心關懷與幫助，並從中獲取了許多為人處世的道理，實銘感於心；而同學之間的互相提攜學習，也令我難忘。尤其是出了社會之後，更加體會到在交大所遇過的教授們，不但除了有專業的學識與充沛的熱情外，對於學生的尊重與呵護，相信我這輩子會永生難忘並引以為傲。

最後，最感激親人的支持，若沒有父親莊柏年先生與母親廖麗卿女士一直以來對我無私的奉獻，這一篇碩士論文就沒有任何存在的價值。

謹將這份得來不易的碩士論文獻給他們兩位!

莊凱婷 2013.06

交通大學 應用藝術研究所

工業設計組

目次

圖目錄

表目錄

第一章 緒論

第一節 研究背景與動機

電子商務龐大的商機，讓不少企業單位願意投入大量資金在網路平台上提供資訊與服務，希冀藉由網路無遠弗屆的媒介力，吸引全世界目光，以提升企業品牌在市場上的競爭力與能見度。

同時，不法人士也企圖從中謀取商業利益。藉由惡意自動化程式，散播垃圾廣告至網路使用者的電子郵件收件夾中、在網頁上不當留言或註冊、產生連結以提高搜尋排名、進行灌票或散播不實消息等干擾網站活動運行；甚者，有心人士更利用網路，散佈不利於企業的負面報導，以導致股價下跌。McWilliams 指出，2004 年約有五兆封的垃圾郵件，被寄到網路使用者的電子郵件收件夾中，估計社會光是用來過濾垃圾郵件，所耗費的生產值就高達一百億美元〔01〕。為了防止專業垃圾郵件駭客利用這種商業手段謀取利益，美國 FBI 電腦安全系統研究局，不惜在網路犯罪的防止措施上，投入數十億美元的經費。

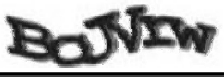
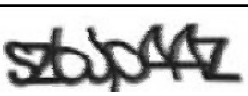
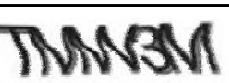
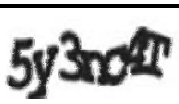
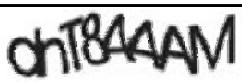
雖然坊間的網站業主並不須要像美國 FBI 一樣，砸下數十億美元來保護網站的安全性。但是為了防止網站資源被過度濫用，還是都會做些安全防護機制。最常見的安全防護機制，是請使用者端在網頁表單輸入「驗證碼」: 一種能夠區分真實人類與惡意自動化程式的工具，以阻擋惡意自動化程式的攻擊〔02〕。驗證碼，英文為 Completely Automated Public Turing Test to tell Computers and Humans Apart，簡稱為 CAPTCHA；中文意為「全自動區分電腦與人類的圖靈測試」。實作的方式很簡單，就是程式問一個電腦答不出來，但人類答得出來的問題。

目前實際應用於網頁安全驗證的驗證碼種類，有數字、文字、語音、邏輯、益智、圖像等。其中最常見到的是阿拉伯數字或英文字母之驗證碼，兩者亦有合併之設計模式，謂之為文本型(text-based schemes)驗證碼。

由於文、數字本身的造形特性，一旦相連結在一起，就會產生其他類似的英文字母或數字，而導致使用者無法辨識，像是字母 o 與數字 0、字

母 I 與數字 1、兩個字母 vv 與一個字母 w、一個字母 d 與兩個字母 cl 等等，(如圖 1.1 及表 1.1 所示)〔03〕〔04〕。這些都容易讓使用者在視覺認知上產生誤判，而導致驗證失敗。而近年來，由於文本型驗證碼被惡意自動化程式的破解率提升，使得驗證碼設計者不得不設計出更扭曲、更變形的文本型驗證碼，最後卻導致使用者無法清楚辨識這些過度扭曲與變形的文、數字驗證碼；這已完全違背了當初驗證碼設計的初衷與良好的使用者經驗原則。

表 1.1 YAHOO 使用之易混淆驗證碼

CAPTCHA	Confusing characters
	最後兩個字為cp或qp或qo？
	第二個字為a或c或o？
	最後兩個字為cl3或cB或d3？
	第三個字為s或b ？
	第三個字為vv或w ？
	第三個字為V或M ？
	倒數第二個字為A或4 ？
	第三個字為b或q？ 倒數第二個字為p或d？
	第五到第八個字為 4還是A？
	第二個字為V還是M？

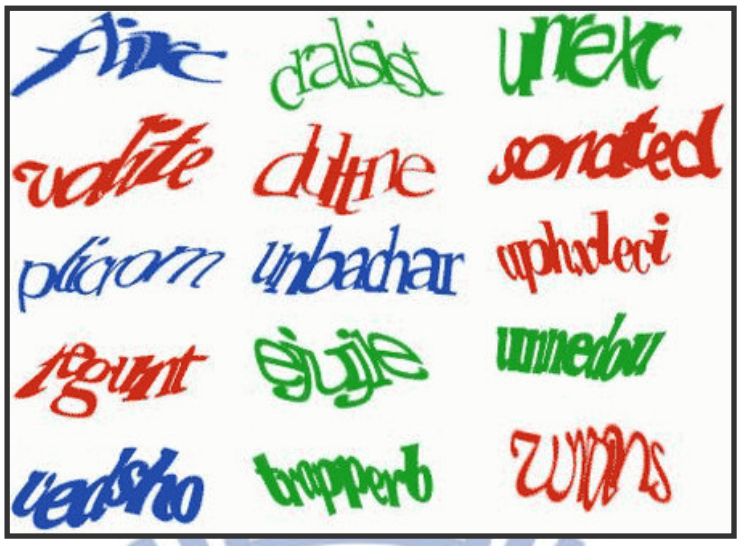


圖 1.1 文、數字相連在一起驗證碼

其他形式驗證碼，如語音型(audio schemes)驗證碼則是因應有視覺障礙的族群所設計，但其答覆驗證的時間較長；邏輯型驗證碼(logical-based schemes)則要求使用者解答程式提問之問題，但這種驗證碼在題目理解上會因使用者的學習背景、文化習俗、個人認知不同，而有不同答案；益智型（instructive schemes）驗證碼則是考驗人類對題目理解力；圖像型驗證碼(image-based schemes)是基於人類對於圖像形狀認知辨識上較電腦卓越，所設計之圖形驗證碼。由於圖像型驗證碼的圖像背景、顏色等複雜特性，較難被電腦機器辨識，相較其它驗證碼，較能區分出人類與惡意自動化程式，是目前惡意自動化程式侵襲成功機率較低的類型，也逐漸成為網路採用之驗證方式。惟現有的圖像型驗證碼仍有下列缺點或使用瓶頸，需要克服或改善：

1. 需要龐大數量的圖片來建置圖像資料庫，儲存成本高，無法大規模產生。
2. 比起文本型驗證碼，使用者需要花較多的時間來解讀驗證題目。
3. 不同國家對於圖片中物體所表達的意義之認知有所不同。
4. 圖片一旦固定樣式與背景，容易被 OCR (Optical Character Recognition)機器破解[05]。

本研究針對文本型及圖像型驗證碼的缺點與使用限制等問題，期望在圖像型驗證碼的設計研究上，結合文本型及圖像型驗證碼的優異特性，並

改善其缺點與使用瓶頸，提出創新圖像驗證碼設計，以對網頁驗證之使用提供實質貢獻。

如何激盪出一個新的圖像型驗證碼，不但需要有豐富經驗，更須能綜合分析現行圖像型驗證碼之特性，並提出優異概念來補強現有之缺點與使用限制，實屬不易。本研究為本人在國外求學期間，發覺日常普通的物品亦能藉由創意思考，而發揮出巨大的設計靈感與效益。在人人熟悉的休閒娛樂遊戲之中，撲克牌（英譯 Poker），不但國際化且大眾化。每份撲克牌共有 52 張牌(不包含 2 張 Joker 鬼牌)，每張皆具數字(2、3、4~10)或英文字母(A、J、Q、K)、圖樣(spades、hearts、diamonds、clubs)以及色彩(黑、紅)之多樣特性。因此，本研究擬以撲克牌為新圖像型驗證碼之設計要素，企圖設計出一個具多變化、多層驗證模式之驗證碼。

第二節 研究目的

綜合上述研究背景與動機，本研究目的在於結合文本型與圖像型驗證碼之使用特性，及撲克牌國際大眾化之優點，嘗試設計一套具使用性與安全性，且淺顯易懂的「Poker 圖像驗證碼」，以供網頁個資內容交易之安全驗證使用。其具體目標為：

1. 運用 52 張撲克牌面傳統圖樣中含有數字、英文字、圖樣及色彩等多符號特性，完成設計一套具雙重驗證功能之「Poker 圖像驗證碼」。

2. 建置實驗網頁，請受測者以自己熟悉操作的電子設備上網，實際進行本「Poker 圖像驗證碼」的驗證操作實驗。探索整體使用者通過「Poker 圖像驗證碼」之正確率及平均驗證操作時間，以及探索不同背景之使用者在驗證操作時間是否有顯著差異，深入了解「Poker 圖像驗證碼」之使用性與大眾化性。

3. 與文本型驗證碼之安全性比較，探索「Poker 圖像驗證碼」被惡意自動化程式破解成功之機率，及以撲克牌之牌面圖樣設計降低被 OCR 機器成功辨識之機率。

第三節 研究限制

本研究為了驗證「Poker 圖像驗證碼」的使用性，而設計一個實驗網頁供受測者上網測試，所獲得之正確率、平均操作時間及不同族群間之平均操作時間差異情形，顯示略有差異，在普及於一般使用者上可能會略有限制。

第四節 研究方法與流程

為達成本研究目的，本研究先採用文獻探討，探討驗證碼的起源、驗證碼的類型、驗證碼的破解技術及其相關研究等，作為本研究在驗證碼之探索基礎。本研究同時蒐集市面上現有之撲克牌種類，並分析各種撲克牌之牌面圖樣設計，並且運用牌面同時具有數字、英文字、圖樣及色彩之多符號特性，研究是否能被設計為圖像型驗證碼之可行性。並據以設計一套，需要辨識牌面文數字與圖樣之雙層驗證「Poker 圖像驗證碼」。

為驗證所設計之「Poker 圖像驗證碼」的實際使用效果，本研究建置一個簡易實驗用網頁，以撲克牌之牌面文數字及圖樣設計驗證碼，進行線上實際測試。由不同背景之受測者，用自己熟悉的電子設備上網進行實測，並由系統程式自動記錄使用者端操作「Poker 圖像驗證碼」之操作時間。

結束測試後，計算整體受測者通過此驗證碼之正確率，以及依據受測者操作時間，計算不同族群之使用差異並分析其差異原因。接著本研究依據此「Poker 圖像驗證碼」被破解成功機率，進行安全性分析。同時也召開專家座談會，邀請光學檢測專家、資訊工程專家及網路軟體專家，進行座談，以提供安全設計之改善建議。最後提出本研究結論與建議。

第五節 論文架構

本研究論文內容分為五大部分，每章節分別敘述如下：

第一章 緒論：闡述研究背景與動機、研究目的、研究限制與研究流程。

第二章 文獻探討：探索網頁驗證碼起源、類型及其相關研究，並了解有關撲克牌牌面圖樣設計及其多符號特性，及了解將撲克牌作為設計圖像驗證碼之可行性。

第三章 驗證碼設計：闡述如何設計一套具雙層驗證之「Poker 圖像驗證碼」的流程。

第四章 驗證實驗：闡述為驗證「Poker 圖像驗證碼」設計的使用性，所進行之實驗網頁設計及實際施測。

第五章 驗證結果之分析與討論，說明實際施測之結果。並根據統計結果，分析「Poker 圖像驗證碼」正確率、平均操作時間、不同族群操作時間之差異性比較，並召開專家座談探索其安全性。

第六章 結論：最後提出研究結論及建議。

第二章 文獻探討

第一節 驗證碼理論及其相關研究之探討

第一項 驗證碼的起源

最早有驗證碼的概念是 Alta-Vista 網路搜尋引擎公司在 1997 年，為防止其註冊網址的服務遭到濫用所開發出來。其由電腦系統亂數產生英文字母及阿拉伯數字後，並將其轉為圖片檔，要求使用者按照圖片中字元的排列順序，輸入所看到的字元，符合即可通過驗證。此方法當時已經為 Alta-Vista 阻擋掉百分之九十五的不當使用〔06〕。

驗證碼，是一種區分用戶是電腦和人的公共全自動程序，中文正式名稱為「全自動區分計算機和人類的圖靈測試」，英語為 Completely Automated Public Turing test to tell Computers and Humans Apart，簡稱 CAPTCHA，是 2000 年由美國卡內基梅隆大學(Carnegie Mellon University)研究人員 Luisvon Ahn、Manuel Blum、Nicholas Hopper 等人及 IBM 的 John Langford 所提出。

在 CAPTCHA 測試中，作為伺服器的計算機會自動生成一個問題，由使用者來解答，並由伺服器計算機來判斷答案是否正確。由於一開始理想化的設定是，只有「人類」才能解答出答案，而自動化程式無法答出伺服器端所問的問題；所以能夠正確回答出該項問題的使用者，就被伺服器計算機定義為「人類」。由於這個測試是由電腦來考人類，而不是由人類來考電腦，人們有時稱 CAPTCHA 是一種反圖靈測試〔07〕。

第二項 驗證碼的類型

本研究依照各個驗證碼的性質作為區分，大致將驗證碼分為文本型（text-based schemes）、語音型（audio schemes）、視頻型(video

schemes)、邏輯型(logical schemes)、圖像型(image-based schemes)及益智型(instructive schemes)等六種類型〔08〕。而隨著網路技術的發展，每種類型驗證碼又大都有衍生類型之驗證模式產生。本研究將目前常見的驗證碼整理如下:

1. 文本型

文本型驗證碼為英文大、小寫字母與阿拉伯數字隨機合成的字串圖片，使用者必須根據所看到圖片中所顯示的字元，輸入正確的對應文、數字，才能通過驗證。為防止被惡意自動化程式侵襲，驗證碼設計者會將文、數字元做扭曲、相連、旋轉、切割或重疊等方式，來防止 OCR 辨識。但這也造成使用者在驗證碼視覺辨識上的混淆和誤判，而導致驗證失敗 (如圖 2.1 所示)。

圖 2.1 更加扭曲與變形的文、數字驗證碼

在文本型驗證碼的發展過程中，reCAPTCHA(如圖 2.2 所示)算是簡易型 CAPTCHA 的一種衍生變形模式。reCAPTCHA 首先從電腦系統挑出兩組英文詞彙，然後將字串作扭曲並從中加上一條切割曲線後，呈現給使用者端。系統只知道兩組英文詞彙其中一組的答案，當使用者端答對了系統本身知道的英文詞彙，那 reCAPTCHA 就會假設使用者端是人類無誤〔09〕，同時也得到另一組的答案。

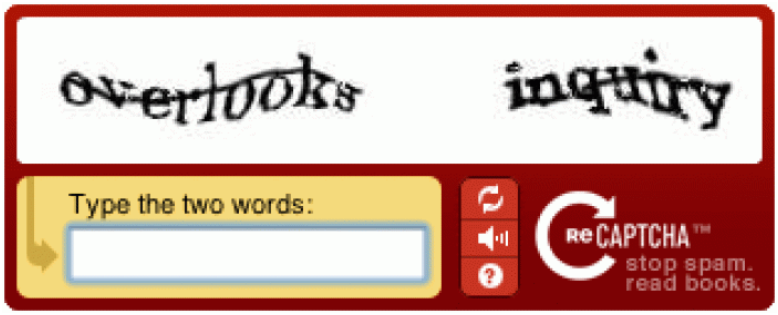


圖 2.2 reCAPTCHA

圖 2.3 所示的驗證碼，是帶有濃厚商業氣息的廣告驗證碼。廣告商讓使用者端輸入圖片中產品名稱，藉此加強或宣傳使用者對此產品的熟稔度。使用者「輸入」驗證碼時，的確是一項驗證的步驟，但其實也是一個宣傳商品廣告的過程。

根據文獻資料顯示，第一個出現在網際網路上的驗證碼廣告平台是 2008 年開始由 Boris Veldhuijzen van Zanten 創辦的 captchatising.com，不過該網址目前已經被移除了〔10〕。雖然 captchatising.com 這平台並沒有能夠持續到今日，但這種藉由輸入產品名稱作為驗證碼以增加網站營收的概念，已經被廣泛在網路平台上使用〔11〕。

圖 2.3 商業氣息濃厚的廣告驗證碼

2. 語音型

在語音型驗證碼未出現時，視覺障礙族群只能請視力正常的朋友告知驗證碼內容或是利用導讀軟體來識別文、數字驗證碼。但在網路越來越普及，驗證碼已經無所不在的時代裡，這確實有許多不便之處。因此語音型驗證碼的出現，的確為視覺障礙族群帶來許多便利性。

語音型驗證碼是在添加背景雜訊的數位字母音訊中，以一人或多人播放的方式，讓使用者輸入所聽到的資訊。如圖 2.4 所示，使用者先聽一段語音，然後再輸入所聽到的四個數字來完成〔12〕。

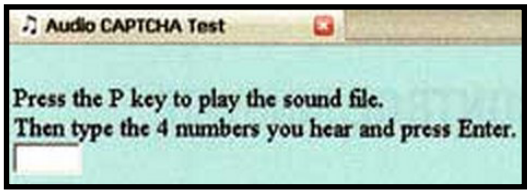


圖 2.4 語音型 CAPTCHA

語音型驗證碼容易受到機器學習演算法的攻擊，僅用分析聲音波形就能知道語音播報的數字。。另外，偏遠地區的少數使用族群會因為對於字母的發音、口音、語速、語調不熟悉，而無法理解問題，導致使用者無法通過測試。

3. 視頻型驗證碼

視頻型驗證碼主要是將驗證碼字串，以旋轉、閃爍、移動等 2D 動畫的方式呈現（如圖 2.5 所示）。

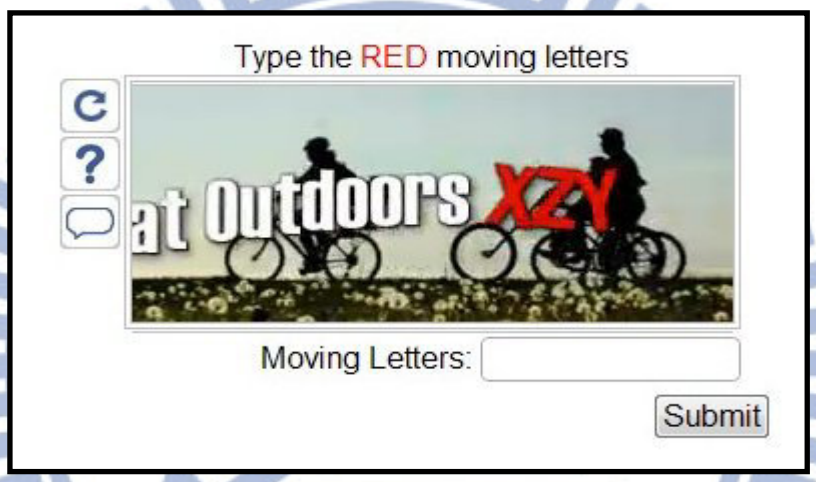


圖 2.5 擷取 NuCaptcha 動態畫面之一

Nucaptcha 使用動態影像旋轉技術來播放影片，然後要求使用者端輸入影片中出現的某顏色字元為何？因為屬於影像動態格式，所以此視頻型驗證碼在網路伺服器速度會變得較慢。圖 2.5 是擷取 NuCaptcha 驗證碼在影片之中所出現 XYZ 之三個紅色字體畫面之一，使用者需依序正確填入此三個字元，方能通過驗證。

儘管是創新的視頻型驗證碼，史丹福大學研究員藉由機器視覺技術，已經破解了 NuCaptcha 驗證碼；破解成功率高達百分之九十〔13〕，這意味著沒有攻不破的驗證碼，只是被破解時間的早晚與機率性而已。

4. 邏輯型驗證碼

亦稱為問答型驗證碼。系統所問的問題，通常讓使用者端無法立即直覺性地回答出答案，需要特別經過大腦判斷、學習及回溯。例如：系統要使用者答出台灣第一名美女是誰？_____。

對於惡意自動化程式而言，邏輯型驗證碼除了要判讀問題，還要進行邏輯判斷，之後還要進行計算後，才能得到驗證碼。相較於文本型驗證碼而言，惡意自動化程式要能夠正確判讀驗證碼的機會的確變低。但在文化習俗、生活習慣及語言差異甚大的世界各國裡，使用者端對正確答案可能也因此有不同見解，因而與電腦預設的答案不同，而無法通過驗證。因此邏輯性驗證碼在趣味價值性較高，但卻不實用〔14〕。

5. 圖像型驗證碼

圖像型驗證碼因為圖像背景複雜、色彩種類多、光線角度反射與陰影等多樣特性，所以相較其它類型驗證碼，惡意自動化程式不容易辨識，因而較能區分出人類與惡意自動化程式，逐漸成為網路採用之驗證方式。圖像型驗證碼資料庫之圖片類型，可謂包羅萬象，諸如：交通工具、材質顏色、花草樹木、昆蟲飛禽、運動物品、科技產品等等。圖片資料庫內容越多，越能有多種圖像型驗證型態可以應用。但現有的圖像型驗證碼仍有下列缺點或使用瓶頸，需要克服或改善：

①. 需要龐大數量的圖片來建置圖像資料庫，儲存成本高，無法大規模產生。

②. 比起文本型驗證碼，使用者需要花較多的時間來解讀驗證題目。

③. 不同國家對於圖片中物體所表達的意義之認知有所不同。

④. 圖片一旦固定樣式與背景，容易被 OCR 機器破解。

⑤.

美國 ASIRRA (Animal Species Image Recognition for Restricting Access)系統是由微軟公司和動物收容平台 Petfinder.com 在 2007 年所開

發的圖像型驗證碼，使用者必須從 12 張不同的狗或貓圖片中，利用點擊圖片方式點選出所有貓或是所有狗的圖片來進行驗證，如圖 2.6 所示〔14〕。

圖 2.6 ASIRRA CAPTCHA

通過驗證後，使用者可以按下圖片下方 Adopt me 選項，網頁就會提供認養平台的網址，如圖 2.7 所示〔15〕，讓使用者自行選擇是否要開啟該網頁進行瀏覽的動作。2008 年 Golle〔16〕使用(Support Vector Machine 簡稱 SVM)方法，藉由顏色、紋理去分類貓與狗的圖片，以破解此驗證碼，破解成功率高達 82.7%〔17〕。

圖 2.7 Petfinder 認養平台

另一較特殊的圖像型驗證碼，就是中文驗證碼(如圖 2.8 所示)。中文驗證碼是以中文部首作為基礎的驗證碼，故稱為「Chinese CAPTCHA」。其透過中文字的拆解組合，即便使用者沒有中文語言能力的背景，也可進行驗證行為。

系統出題方式是隨機從中國古漢字資料庫挑出一個字出題，接著根據漢字解構的部件進行拆解〔18〕，這些部件多是另外一個字形或部首。如圖 2.8 所示，系統先將左方之漢字拆解成三個主要可分辨的部件，再請使用者從右方挑選正確的三個部件。此方法雖兼顧了非漢字使用者，但對漢字熟悉者能更快速地進行驗證〔19〕。

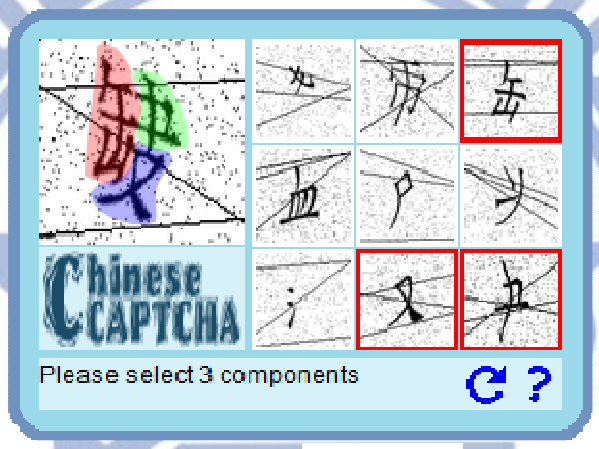


圖 2.8 中文驗證碼

圖 2.9 稱為 Puzzle CAPTCHA。此驗證碼利用影像切割技術，將圖片隨機切割成幾個正方形區塊，並將區塊隨機旋轉 0 度、90 度、180 度、270 度，然後讓使用者在驗證碼圖像區塊中作點擊的動作，使被切割的方塊能夠以 90 度順時針旋轉的動作，來將所有的區塊拼回完整的原圖，以通過驗證碼測試。

圖 2.9 Puzzle CAPTCHA

惟此方式在驗證操作時，使用者萬一不小心多點擊一下而導致旋轉過頭，則又需要再多花費時間重新點擊轉為正確畫面〔20〕。

圖 2.10 PlayThru 屬於一種迷你遊戲之驗證碼，使用者須將左方人臉上之各器官拖曳至右方空白人像正確位置上，方能驗證通過〔21〕。

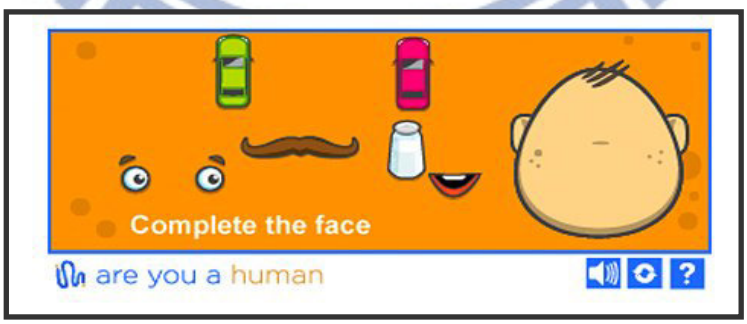


圖 2.10 PlayThru 驗證碼

6. 益智型驗證碼

圖 2.11 為 Rapidshare CAPTCHA Cat 驗證碼，是提供一些含有貓或狗圖案的文、數字。解答方式則是要使用者要先區別貓跟狗，再把含有貓的字母輸入。狗跟貓的區別方式是，狗的頭比較小以及脖子有項圈，使用者需經過學習才能推斷出答案〔22〕。

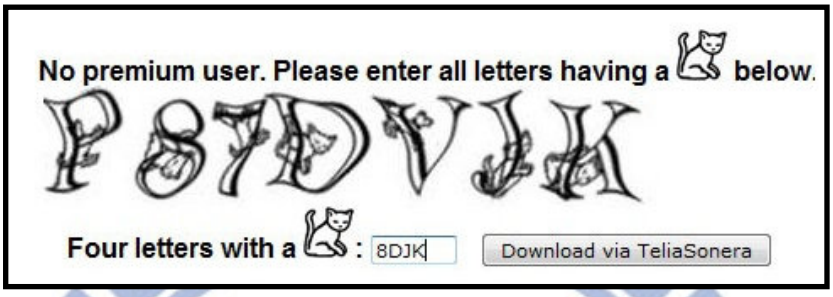


圖 2.11 Rapidshare CAPTCHA Cat

圖 2.12 為 Captcha madness，使用者必須根據框格中的圖形和下方的文、數字對應表，輸入圖形所對應的英、數字，以通過驗證〔23〕。

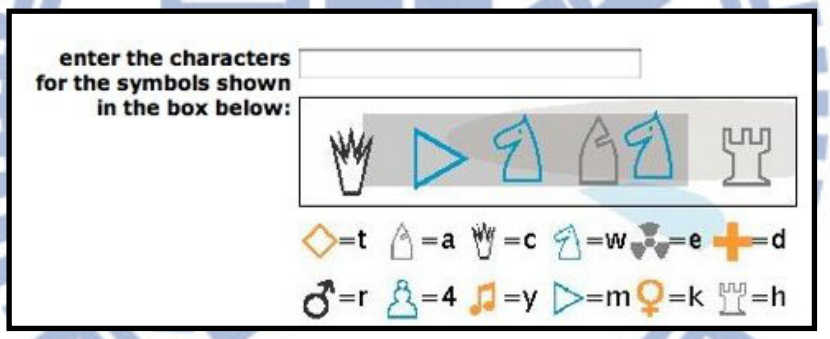


圖 2.12 Captcha madness

圖 2.13 為 Ajax Fancy Captcha，此驗證碼要求使用者將正確的物品，以點選拖曳的方式，放置在特定的位置內〔24〕。此驗證方式若在螢幕較小的電子行動設備上，使用者的手指很容易碰處到原本不想選之圖片；若能直接用點擊的功能來代替拖曳的動作，使用性會較佳。

圖 2.13 Ajax Fancy Captcha

圖 2.14 為 Dice CAPTCHA 驗證碼，其利用骰子的點數特性，由使用者辨識顯示之四顆骰子的點數，填入然後送出驗證，或是要求使用者填入骰子出現點數的總和(如圖 2.15 所示)。這種的任務對大部分使用者並不是項困難的事，然而，每一骰子之六面點數皆只有 1、2、3、4、5、6 點，其被惡意自動化程式破解機率很高。因此 Dice CAPTCHA 驗證碼的安全機制，仍須再加強〔25〕。

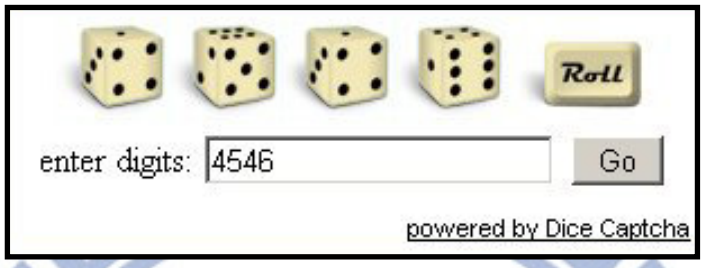


圖 2.14 Dice CAPTCHA 單純填入骰子個別點數

圖 2.15 Dice CAPTCHA 填入骰子出現點數的總和

圖 2.16 為眾人皆知的九宮格遊戲，大多數使用者不需多看題目的說明，就可以直覺性地知道，此驗證碼需要進行何種動作才能通過驗證。把這種國際大眾化的益智遊戲拿來當作驗證碼，算是非常不錯的點子。

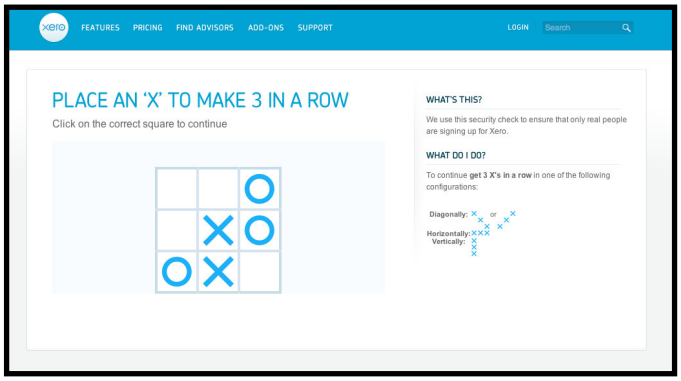


圖 2.16 XERO〔26〕

第二節 驗證碼的破解技術

根據文獻資料探討，上述六種驗證碼類型，大都已遭惡意自動化程式破解，只是依照被機器辨識破解的比例來說，圖像型驗證碼機率較低。

圖像型驗證碼較難被破解的原因，主要是人類視覺比電腦更會處理圖像中的訊息，再加上電腦在圖像分類、目標識別、場景理解等方面的能力較弱。所以在一般情況下，圖像型驗證碼比其他類型的驗證碼更加難以被惡意自動化程式給攻擊。

目前驗證碼破解技術，大致可分下列四大類：

1. OCR 光學自動辨識法

OCR(optical character recognition) 對於不扭曲的文字，擁有良好的處理效能，辨識速度每秒 1000 字，就算是輕度的扭曲文字，辨識率也可以達到 95%。

OCR 主要是透過(一)消去背景，(二)切割元素，(三)辨認元素等三個步驟進行處理。如圖 2.17 所示即為 OCR 破解程序。

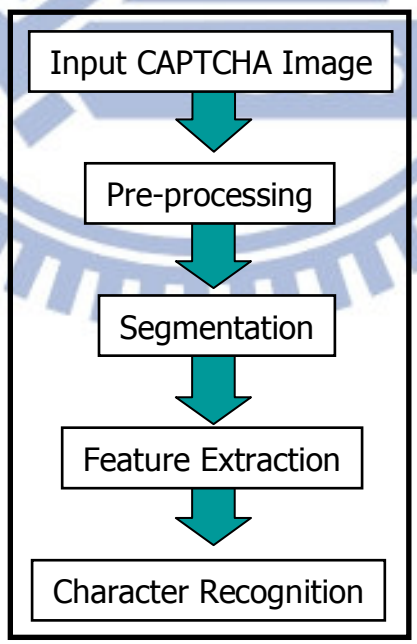


圖 2.17 OCR 辨識驗證碼之破解程序

以破解圖 2.18 所示，由 EM-Gimpy 所產生的驗證碼為例，OCR 破解程式的第一步驟：消去背景上的漸層顏色與雜點。第二步驟：將可辨識的文字 SMWM 切割成單一元素(S/M/W/M)。這些單一有意義的元素易為人類使用者端快速辨識，惟惡意自動化程式卻可能因其扭曲，需花費較多時間辨識。第三步驟：根據每單一元素，也許是文字或數字，進行 OCR 辨識。

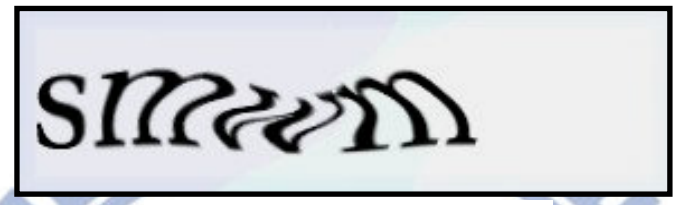


圖 2.18 EZ-Gimpy 產生的 CAPTCHA〔27〕

2. 暴力破解法

暴力破解是將一堆文、數字組合的字串逐一測試。只要有足夠的嘗試機會與時間，透過無數次的測試，就有機會試出正確的答案〔28〕。如圖 2.19 所示，「X5Tb」有 4 個字母組成，被猜中的機率只有(1/62)之四次方，但惡意自動化程式只要不計時間，嘗試所有可能的字母組合，即 62×62×62×62=1477633 種，就一定可以找到正確的驗證碼。

圖 2.19 文數字驗證碼範例「X5Tb」

3. 資料庫攻擊法

資料庫攻擊法大多是針對圖像型驗證碼的圖片資料庫，因為這類驗證碼需要龐大的空間儲存樣本，而樣本又不容易得到或產生，且樣本檔案過大的話，則會影響傳輸速度，因此資料庫所含的圖像樣本數不會太多。相對而言，本研究認為 OCR 也不容易進行資料庫攻擊，因為先進的資料庫一般都會有保護措施，不易進入。而 OCR 系統本身也需要建立龐大之對照樣本資料庫圖片，才能進行與驗證碼資料庫圖片比對，當兩者相符合方能進行攻擊。所以圖像驗證碼不易被 OCR 破解。

4. 人力破解法

人力破解法則是雇用廉價的第三世界國家人力，利用大量人力去辨識驗證碼，以進行不法商業行為。用人力破解法相對等於使用人類的視覺辨識能力，所以是很容易成功破解任何文本型驗證碼。本研究認為除非使用加密型方式進行驗證行為，否則短期內要發展出有效阻擋人力破解法的驗證碼，並不容易。

而 Polisetti (2000) 研究指出，使用者在選擇圖像時，比起輸入文、數字時的當下經驗，是較令人感到愉悅的。因此圖像型驗證碼較能鼓勵使用者，進行提交表單或是註冊會員等網路行為。另外，圖像識別對於人類來說非常容易，但是對於惡意自動化程式卻相對困難。因此圖像識別相較於文、數字組合來說，在安全性上會更高一點。

綜合上述，本研究認為圖像型驗證碼系統較不易被破解，只要改善圖片資料庫過大，以及降低使用複雜度等問題，便會是個使用性佳又具安全性的驗證碼設計。

第三章 研究設計

第一節 設計架構

本研究認為普通的日常物品，能藉由創意思考會激盪出設計靈感，故選擇人人熟悉，人人會玩的休閒娛樂遊戲：撲克牌(英譯 Poker)，做為驗證碼設計要素。擬以撲克牌多符號之特性，設計出一個具國際化、大眾化、多重驗證之「Poker 圖像驗證碼」模式。

為此設計構思的完成，需要有嚴謹的設計架構支持。此架構須先了解網頁驗證碼及撲克牌特性，方能設計出驗證模式。同時也需要架設實際的網頁驗證系統來驗證「Poker 圖像驗證碼」之正確率、驗證操作時間，及不同背景族群在此驗證碼下操作時間的差異性。探索此驗證碼的實證效果，才能確認所設計「Poker 圖像驗證碼」之使用性。圖 3.1 即為本研究之設計架構。

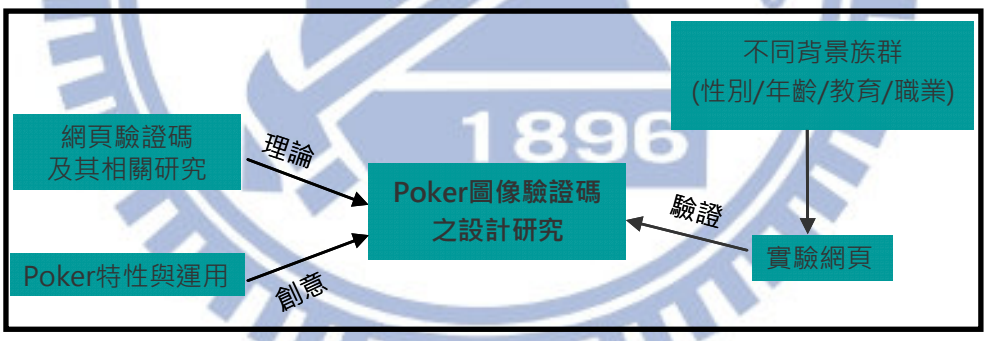


圖 3.1 設計架構

第二節 撲克牌及其運用於圖像驗證碼之設計

撲克牌又稱為英美牌（Anglo-American playing card）、法國牌。是美國商人引進法國塔羅牌後，再另外加入 2 張鬼牌，成為 54 張之全球通用形式，是世界各地最常看到的國際大眾化遊戲工具。

其 52 張基本圖樣之撲克牌中，計分為四類群組圖樣：♣黑梅花(clubs)、♦紅磚(diamonds)、♥紅心(hearts)、♠黑桃（spades）等黑、紅兩種顏色；而每一類群組，又皆由數字 2、3、4、5、6、7、8、9、10 及圖樣 Ace、Jack、Queen、King 組成(如圖 3.2 所示)。

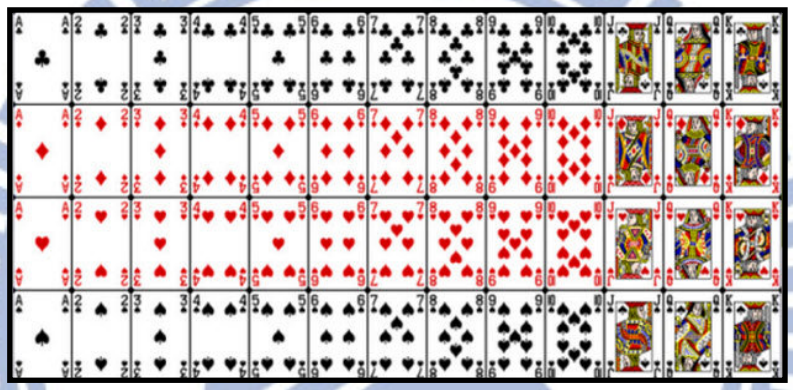


圖 3.2 全球通用的 52 張基本圖樣之撲克牌

撲克牌是一種國際化、大眾化的娛樂遊戲，其牌面圖樣也隨不同區域的使用者，為了增進遊戲樂趣而做了許多的修改與創意設計。但其不變的原則是仍能讓所有使用者理解且辨識出 52 張牌的數字、英文字與四種花色圖樣(spades、hearts、diamonds、clubs)，否則將無法進行各種撲克牌遊戲。

坊間撲克牌的圖樣創意設計很多，包括學校學生、公司行號、政府機關等，都為了各種不同用途，而將 52 張傳統圖樣的撲克牌牌面，做了設計變化。本研究整理撲克牌的創意設計如下：

1. 傳統歷史作為牌面圖樣

以歷史人物肖像、描繪生活風俗民情、或傳統民俗文物，取代原來四種花色圖樣(如圖 3.3 所示)，主要用途在於紀念或作為學習教材。

圖 3.3 以歷史人和物作為牌面圖樣

2. 現代真實人和物作為牌面圖樣

以當代的話題新聞人物、產品或風景照等作為牌面圖樣(如圖 3.4 所示)，其文字、數字及花色圖樣仍可以被使用者辨識，但圖面背景相當複雜，已不容易被 OCR 辨識了。

圖 3.4 以真實人和物作為牌面圖樣

3. 虛擬人物作為牌面圖樣

以虛擬的卡通、漫畫、動畫遊戲人物作為牌面圖樣(如圖 3.5 所示)，其文字、數字及圖樣均做了變化，不容易被 OCR 辨識，但人仍能清楚辨識文數字及四種圖樣。

圖 3.5 以虛擬人物作為牌面圖樣

4. 圖中圖設計作為牌面圖樣

以圖中又有圖樣變化之特殊設計作為牌面圖樣，如圖 3.6 所示之兩張牌均為紅磚 9，使用者或許一時之間還無法立即辨識其點數；OCR 當然也同樣不易辨識。

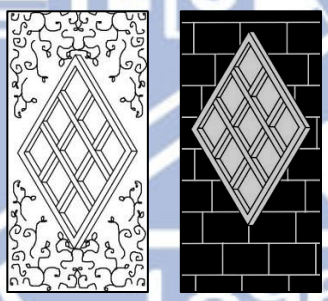


圖 3.6 紅磚 9 之創新設計

5. 將點數圖樣變化做為牌面圖樣

如圖 3.7 所示，設計者利用巧思在♣、♦、♥以及♠之圖樣上，作了設計變化，且中間的梅花 6，數字不但以溫度單位呈現，點數也以樹和小鳥之圖像表現，非常有趣味性。使用者可猜出其圖樣的代表意義，但對 OCR 來說則會稍許困難些。

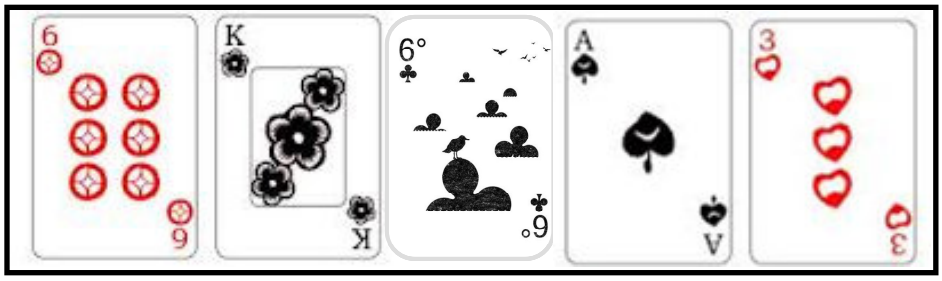


圖 3.7 點數圖樣之創新設計

6. 紋理、色澤與對比顏色作為牌面圖樣

如圖 3.8 所示，在原本只有紅與黑，兩種純色的花色圖樣中，加了紋理、材質、與多種顏色變化，豐富整體視覺感。

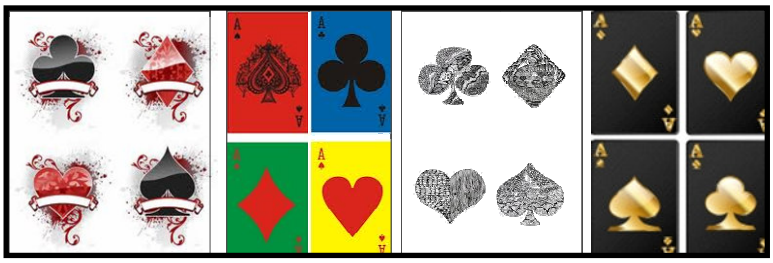


圖 3.8 花俏的花色圖樣

上述各種牌面創意設計，大都可讓使用者辨識出其文、數字與圖樣，但不易被 OCR 破解。所以本研究設計之「Poker 圖像驗證碼」，若要防範 OCR 的攻擊，可在實務上選用較複雜圖片或具設計變化之撲克牌做為圖像型驗證碼的圖片資料庫，以大幅提高安全性。

而本研究以傳統 52 張圖樣撲克牌作為設計要素之理由如下：

1. 傳統 52 張圖樣撲克牌作為圖片資料庫之基本圖片，不需再擴充任何圖片，資料庫容量不必很大，故成本相對較低。

2. 每一張撲克牌可視為一張圖片，但其內容具有多元化特色，包含了九個數字(2、3、4、5、6、7、8、9、10)及四個英文字(A、J、Q、K)、四種圖樣：♣黑梅花(clubs)、♦紅磚(diamonds)、♥紅心(hearts)、♠黑桃（spades）及紅、黑兩種顏色。

3. 運用每一張牌之特色，本「Poker 圖像驗證碼」設計為雙層驗證碼，先以撲克牌出現之文、數字部分為第一層驗證，再以四種圖樣(spades、hearts、diamonds、clubs)出現之張數為第二層驗證。相較於僅做一層驗證之其他方法，具有較高之安全機制考量，但同時也會有拉長驗證操作時間之缺點。

4 傳統圖樣樸克牌具有國際性及大眾化性，無地域區隔之虞。

5 為提高本驗證碼之安全性，本研究召開專家座談會，邀請自動光學辨識專家、資訊工程與網路軟體專家，就本研究設計進行討論，提供改善意見以增加本研究設計之安全性。

本研究運用傳統圖樣之 52 張撲克牌之原有特性，做為網頁驗證碼設計使用，所考慮之另一項理由為，傳統圖樣之撲克牌，使用性上最容易；相反地，在安全性部分，無論是被破解成功的機率，或是被 OCR 辨識成功的程度上，都是較差的。但從安全性表現最差的傳統圖樣撲克牌來做為「Poker 圖像驗證碼」實驗工具，可以從研究結果，了解本研究設計之安全性底線。

第四章　驗證實驗

第一節　　驗證網頁建置

本研究為驗證所設計之「Poker 圖像驗證碼」的實際使用性，發展一個實驗網頁，網址為 http://210.65.11.29/web/form.jsp，網頁驗證畫面及提問之雙層驗證內容如圖 4.1 所示。

圖 4.1「Poker 圖像驗證碼」實驗網頁

本實驗網頁驗證之操作流程，可參考表 4.1 之內容：

表 4.1 網頁驗證畫面及提問之雙層驗證內容

各位好:

本實驗為進行**驗證碼研究**，特設計下列簡要題目，敬請協助填寫，

並送出驗證。您填寫的資料均保密並於研究之後銷毀。謝謝您。

交通大學應用藝術研究所 / 研究生　莊凱婷 敬上

.....

一、.請點選您的背景資料：

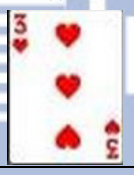
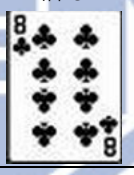
1.○男　○女

2.○20 歲以下　○21~45 歲　○46~60 歲　○61 歲以上

3.○高中以下　○大學專科　○碩博士

4.○服務業　○製造業　○公家單位　○學生　○其他

二、驗證：

牌 1	牌 2	牌 3	牌 4	牌 5
				

1.請依上面所顯示的 5 張撲克牌。由左而右依序輸入 5 張撲克牌之數字或英文字:

[ ] - [ ] - [ ] - [ ] - [ ]

2.上面所顯示的 5 張撲克牌中，

♠類的有[ ]張，♥類的有[ ]張，♦類的有[ ]張，♣類的有[ ]張。

送出

1. 受測者打開網頁，依據網頁指令要求填完相關資料之後，網頁自動隨機從基本圖樣之 52 張撲克牌之中，抽出 5 張撲克牌，如圖 4.2 所示。

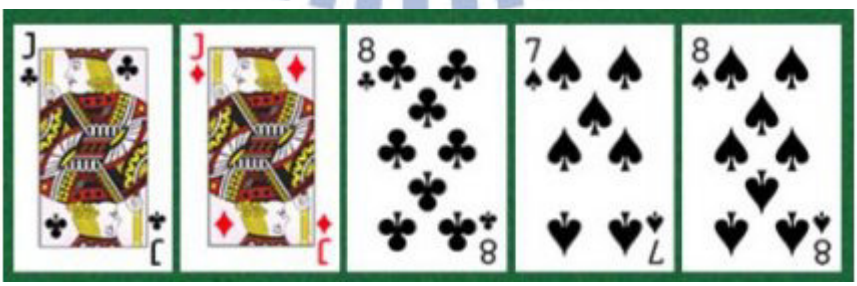


圖 4.2 系統隨機抽取的 5 張撲克牌

2. 驗證碼系統提問:請使用者依螢幕顯示出 5 張撲克牌面上之數字或英文字，由左至右依序填在下列方格之中

3. 系統會續提問：請就螢幕顯示出 5 張撲克牌面之中，填入有幾張黑桃？有幾張紅心？有幾張黑梅花？有幾張紅磚？

4. 使用者填完上述雙重驗證碼之後，按「送出」鍵之按鈕，網頁系統會判別兩道驗證答案是否均正確，並記錄使用者操作時間。

本網頁的功能設計中，具有計時功能，可以計算每一受測樣本之操作時間。而驗證碼操作時間之定義為：受測者填完最後一筆背景資料之後，開始計時，直至受測者填完兩道驗證碼後，按「送出」鍵為止的使用累計時間。

因此，受測者填寫最後一項背景資料之後，即進入本研究之受測實驗程序。依照網頁隨機顯示 5 張基本圖樣之撲克牌，開始進行兩道驗證碼之答題，驗證答案填寫完畢後，受測者按出「送出」鍵按鈕，實驗即為結束。而後，網頁伺服端系統確定收到驗證訊號，並判別兩道驗證問題之答案均是否正確或是有誤。

第二節 驗證實施

本研究之實驗網頁程式在初期完成時，先由本研究者及數位同事，進行試測，並就測試語意作些許調整，完成網頁內容最後測試版本。

隨後，由本研究者聯絡友人、同事、長官、長輩、同學等，請其協助上網填寫背景資料並進行實驗驗證。總計受測者樣本數有 238 人，其中 36 位發生驗證錯誤，因此，兩道驗證碼都正確通過者有 202 人。

通過本實驗受測者之詳細背景與人數統計，如表 4.2 所示：

表 4.2 整體受測族群通過驗證之有效樣本分佈

項目	類別	人數(位)	百分比(%)	合計
性別	男	114	56.4	202 人
	女	88	43.6	
年齡	20 歲以下	24	11.9	202 人
	21~45 歲	133	65.8	
	46~60 歲	22	10.9	
	61 歲以上	23	11.4	
教育程度	高中以下	27	13.4	202 人
	大學大專	102	50.5	
	碩、博士	73	36.1	
職業	服務業	54	26.6	202 人
	製造業	52	25.8	
	公家單位	22	10.9	
	學生	47	23.3	
	其他	27	13.4	

本研究在驗證實施之後，訪談約二十名受訪者，意見綜合如下：

1.受訪者皆表示在第一層驗證碼題目時，毋須看問題即可知道要填選；反觀之，在第二層驗證碼的問題理解上，容易造成受測者混淆。

2.受訪者因為知道此為實驗網頁，並不同一般真實情況急著提交表單進入某網頁，對於在時間上的急迫性與反應速度就沒有如平日一般來得快。

3.受訪者皆主觀認為自己填寫完本驗證碼只花到十秒至十五秒的時間，甚至是十秒以內；但驗證結果的平均值卻都為三十幾秒以上。這代表受測者對時間的主觀與客觀上認知有大落差，此可為日後繼續研究之議題。

4.受訪者反應空格欄位太多，以致每次要輸入文、數字時，都需要再度移動滑鼠游標，感到非常麻煩。若改為點擊或拖曳的方式，就比較能增進使用上的方便性與降低操作時間。

受訪者之意見可做為後續研究問題設計之改善參考。

第三節 資料處理

本研究運用實驗網頁設計之程式，依實驗網頁所得之原始資料紀錄，計算出每一族群受測樣本人數 N、通過驗證之正確率、操作時間之平均值 M、標準差 SD。

接著採用 t 檢定及 One-way ANOVA 來解析其差異性。若 One-way ANOVA 有顯著差異發生，則進行 scheffe 事後檢定。

本研究之各項統計檢定水準α為 0.05。

第五章　驗證結果與分析

第一節　驗證發現

本研究經過驗證實施以及回收樣本，並分析原始數據，發現受測者通過驗證之正確率為 202/238=84.88%，平均之驗證操作時間為 33.9 秒。

而在不同性別族群中，受測者在實驗網頁平均驗證操作時間(mean)、標準差(SD)及 t 檢定，整理如表 5.1 所示：

表 5.1 不同性別受測族群在驗證操作時間之平均數、標準差及 t 檢定

	男性	**女性**
人數(N)	114	88
平均時間(M)	34.2	33.6
標準差(SD)	14.2	14.3
t 值=0.297，自由度＝201		

P=0.766

表 5.1 顯示，本驗證以 t 檢定統計不同性別在驗證碼操作時間之差異性，得到 t 值為 0.297，自由度為 201，P 值為 0.766，這代表男女性族群在本驗證操作時間未達顯著性差異。這也意味著本驗證碼對性別具通用性。

另在不同年齡族群中，可由數據分析發現，受測者在平均驗證操作時間上，存在顯著性差異，其不同年齡族群之平均操作時間(mean)、標準差(SD)、變異數分析及 scheffe 事後檢定分析表，整理如表 5.2 及表 5.3 所示：

表 5.2 不同年齡受測族群在本實驗操作時間之變異數分析

變異來源	平方和	自由度	均方和	F 值	P 值
組間	3808.3	3	1269.4	68	0.00021
組內	36776.7	198	185.7		
總和	40585.0	201			

表 5.3 不同年齡受測族群在本實驗操作時間之事後檢定

年齡	平均值	同質性子集合	
21-45	31.6	A	
20 以下	31.8	A	
46-50	41.4		B
60 以上	42.6		B

由表 5.2 與表 5.3 可知，45 歲以下之受測族群在本驗證碼操作時間，顯著地快於 46 歲以上之受測族群。

另在不同教育程度受測族群之中，本驗證發現受測族群在實驗網頁之平均驗證操作時間不存有顯著性差異，其不同教育程度受測族群之平均操作時間(mean)、標準差(SD)與變異數分析整理如表 5.4 所示：

表 5.4 不同教育程度受測族群在驗證操作時間之變異數分析

變異來源	平方和	自由度	均方和	F 值	P 值
組間	622.6	2	311.3	1.5	0.215
組內	39962.4	199	200.8		
總和	40585.0	201			

另在不同職業別受測族群中，本驗證發現受測族群在平均驗證操作時間存在顯著性差異，其不同職業別受測族群之平均操作時間(mean)、標準差(SD)、變異數分析以及 scheffe 事後檢定分析表，整理如表 5.5 與表 5.6 所示：

表 5.5 不同職業受測族群在驗證碼操作時間之變異數分析

變異來源	平方和	自由度	均方和	F 值	P 值
組間	2237.3	4	559.3	29	0.0241
組內	3347.7	197	194.7		
總和	40585.0	201			

表 5.6 不同職業受測族群在本實驗操作時間之事後檢定

職業	平均值	同質性子集合	
學生	29.6	A	
公家	29.8	A	B
其他	32.7	A	B
製造	36.4	A	B
服務	37.4		B

由表 5.6 可知，學生族群在驗證操作時間顯著快於服務業族群，其他不同職業別受測族群之間，則無顯著差異存在。

第二節 差異分析

綜合上述驗證結果得知，整體受測者 238 名之中，回答正確通過驗證者計有 202 名，正確率達 84.88%，顯見大部分受測者均能容易理解並且懂得如何使用「Poker 圖像驗證碼」。而平均驗證操作時間 33.9 秒則稍偏高，此可能本驗證碼為雙層驗證設計，而造成使用者需花費較多時間辨識與填答。此點在未來實務設計時，可再考慮詳加改善。

針對各個不同族群在「Poker 圖像驗證碼」實驗網頁上，平均驗證操作時間差異情形，闡述如下：

1. 由表 5.1 所示，不同性別族群在實驗網頁上之平均操作時間，分別

為男性 34.2 秒，女性 33.6 秒。女性受測族群雖略快於男性受測族群，但經由 t 檢定結果，並未達顯著差異。

2. 由表 5.3 所示，不同年齡族群在實驗網頁上之平均驗證操作時間，20 歲以下為 31.8 秒；21~45 歲之間為 31.6 秒；46~60 歲之間為 41.4 秒；61 歲以上為 42.6 秒。其中以 21~45 歲之受測族群操作時間最快；61 歲以上受測族群操作時間最慢。經由單因子變異數分析，得知 p 值為 0.00021，已達到顯著差異。經進一步作 scheffe 事後檢定，發現 45 歲以下受測族群在驗證操作時間顯著快於 46 歲以上族群的受測族群。

此種差異現象，可以解釋為 45 歲以下之族群多為上班族或是學生代表的年齡層，長期處於在辦公室或學校環境，對於電腦軟硬體設備之操作經驗較豐富。相對地，46 歲以上年齡的族群，年齡層較大，使用電腦軟硬體設備經驗較不足，其不論在虛擬觸控、鍵盤或滑鼠操作之熟稔度，遠不及正處於巔峰的 45 歲以下年齡層人員，故 45 歲以下年齡族群在驗證操作時間顯著快於 46 歲以上族群，當屬合理的解釋。

3. 由表 5.5 所示，不同教育程度族群在實驗網頁上之驗證碼平均操作時間，高中以下族群為 33.1 秒；大學專科族群為 32.5 秒；碩博士族群為 36.2 秒。其中以大學專科族群操作時間最快；碩博士族群操作時間最慢，三個不同教育程度之族群在平均驗證操作時間雖有快慢，但經由單因子變異數分析，則未達顯著差異。

4. 由表 5.6 所示，本研究發現不同職業族群平均驗證操作時間，服務業為 37.4 秒；製造業為 36.4 秒；公家單位族群 29.8 秒；學生族群為 29.6 秒；其他族群則為 32.7 秒。經由單因子變異數分析，得知 p 值為 0.024，已達到顯著差異，經進一步作 scheffe 事後檢定，發現學生族群在受測操作時間顯著快於服務業族群，此種現象可以解釋為現在的學生族群多以電腦處理文書、學習專業電腦技巧或上網娛樂，自然在網頁上活動頻繁，也較熟悉驗證碼之操作；而服務業，諸如美髮業、餐飲業、交通運輸業等，相比之下，花較少的時間在電腦上，進行網路休閒娛樂活動，故驗證操作時間相對較慢。

綜合上述，本研究設計之「Poker 圖像驗證碼」驗證操作時間，在性別與教育程度上並無顯著性差異存在。而在不同年齡層以及不同職業族群上，雖有顯著差異情形產生。但都可以合理解釋其差異原因。

第三節 安全性分析

常見破解網頁驗證碼的方式有光學辨識法、暴力攻擊法、資料庫攻擊法以及人力破解法等。每一次的破解都導致驗證碼設計更趨向複雜，以致最後造成連使用者也越來越難了解驗證碼真正的初衷為何。

其中資料庫攻擊是透過每一次驗證資訊，再重新組合新的攻擊，此方式在圖像型驗證碼最常見。大量的圖片資料庫是降低此一攻擊的辦法〔29〕。但是大量圖片資料庫建置，不但不容易且建置成本高。本研究之52 張傳統圖樣「Poker 圖像驗證碼」具有圖片數量少之優點，但相對地在安全性也容易會受到惡意自動化程式的攻擊。有關本研究運用 52 張傳統圖樣撲克牌牌面之多符號特性，所設計之「Poker 圖像驗證碼」的安全性，探討如下：

1. 與英文字、數字的文本型驗證碼比較：

   ①. 英文字母包括大小寫共 52 個字母及 0~9 共 10 個數字，共有 62 種，常用驗證碼以四個文數字為驗證碼最多，隨機獨立抽取四個的英文字數字，而被暴力侵襲成功的機率為 $1/(62\times62\times62\times62)=1/14776336=6.77\times10^{-8}$。

   ②. 本研究設計之「Poker 圖像驗證碼」，第一層驗證設計為從圖片資料庫隨機獨立取出之 5 張撲克牌，請使用者辨識並輸入 5 張撲克牌之數字或英文，此第一層驗證設計被暴力侵襲成功的機率為 $(1/13)\times(1/13)\times(1/13)\times(1/13)\times(1/13)=1/371293=2.69\times10^{-6}$。

   ③. 本研究之第二層驗證，請使用者辨識並輸入在此 5 張撲克牌牌之中，四種圖樣（spades、hearts、diamonds、clubs）之出現張數，此第二層驗證設計被暴力攻擊方式猜中侵襲的機率為 $1/44=2.27\times10^{-2}$。兩層驗證同時被暴力侵襲方式猜中侵襲的機率為$(2.69\times10^{-6})\times(2.27\times10^{-2})=6.11\times10^{-8}$。因此，與常見的四個文、數字之驗證碼組合被暴力攻擊成功機

率 6.77×10^{-8} 相近。

④. 本研究若為再提高安全性，則可以將撲克牌之色彩因素考慮進去，降低被暴力侵襲成功的機率。

2. 易被 OCR 辨識的安全性問題

本研究用傳統圖樣之撲克牌來做為實驗網頁之圖片依據，係考量其使用方便性。然而雖使用雙層驗證設計來提高安全性，但此傳統圖樣「Poker 圖像驗證碼」仍易遭受 OCR 的侵襲；OCR 只要簡單建立 52 張基本圖樣之撲克牌圖片作為辨識配對標準，並掃描待測之撲克牌牌面內容，則立即完成高機率之正確辨識，網站自然容易被侵襲了。然而，撲克牌牌面圖樣之設計是千變萬化，有些設計既可以讓人類依然容易視覺辨識，但是對 OCR 則需要花費極多的時間來辨識，例如圖 5.1 所創新設計之撲克牌牌面圖樣，就具有此種效果。

圖 5.1 各種創新設計之撲克牌圖樣

綜合上述，最理想之「Poker 圖像驗證碼」安全性，即是選定或設計具有圖像功能，又兼具容易辨識其 52 張撲克牌牌面的方式為最佳。

本研究為更廣泛了解專家對本研究所設計驗證碼之安全性的意見，特邀集兩位自動光學檢測專家、一位資訊工程專家及一位網路軟體專家，進行一場專家座談會。

座談中，請諸位專家就本研究設計之「Poker 圖像驗證碼」，從 OCR 及資訊網路的技術角度，以及本研究設計內涵，提供寶貴意見。座談會之會議紀錄整理如下：

「以 POKER 為圖像驗證碼之設計研究」安全性分析專家座談會 會議記錄

一、時間：2013 年 6 月 25 日 14：00~15：00

二、地點：新竹市光復路 2 段 321 號工研院光復院區 3 館 205 會議室

三、會議主席：黃卯生博士(工研院量測中心儀器與感測技術組/組長)

四、與會專家：

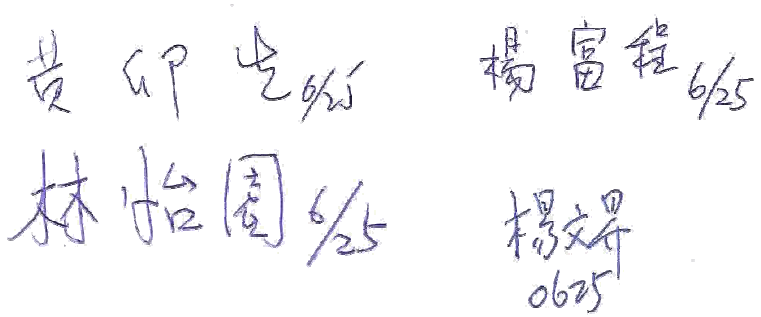
專家 1.自動光學檢測 AOI：楊富程副經理 (工研院量測中心/資深工程師)

專家 2.資訊工程：楊文昇(逢甲大學資訊工程系兼任講師/曾任職威達雲端電訊股份有限公司資訊處經理)

專家 3.網路軟體：林怡園技術總監(云霖科技有限公司)

五、紀錄：莊凱婷

六、會議出席簽到：



七、會議發言紀錄及重點摘要

主席：謝謝各位專家出席今天討論會議，今天會議主要是協助莊凱婷同學，就其研究所碩士論文題目：「以 POKER 為圖像驗證碼之設計研究」中，有關以 POKER 為圖像驗證碼之安全性問題。請以各位之實務經驗，提供寶貴意見，供莊凱婷同學研究參考。

專家 1：本人先就 OCR 之發展與實際運作做一簡單描述，OCR 是 AOI(Automatic Optical Inspection)技術的一環。OCR 的發展從 1960 年代開始，主要針對英文數字之辨識，1990 年隨著 OCR 光學軟硬體技術精進，而增加了漢字的辨識功能。OCR 機構包含了機器視覺、電路控制及訊號處理等，來執行掃描辨識。OCR 最大功用是在協助文書資料單據的儲存與調閱；企業機構運用 OCR 來掃描文件，使之以數位格式存入資料庫待日後引用，是文書資訊自動化的關鍵技術。而 OCR 因光學功能及資訊儲存容量不斷地增強，而能辨識儲存更多東西，包括圖樣與色彩等。這也是 OCR 辨識能力被惡意用來破解圖像型驗證碼的基本概念；OCR 利用已儲存在對比資料庫的圖像，來逐一比對掃描所得之圖像(驗證碼)，若兩者圖像相符即成功侵襲了該網站。但此辨識過程卻是複雜不易的，OCR 辨識圖像比辨識文數字複雜也比較困難，原因是辨識圖像時需要執行：

1.圖像輸入與前處理，包括彩色圖像二值化及背景去除；2.圖像特徵萃取；3.對比識別。圖像特徵被萃取後，必須與對比資料庫內容來比對，而此對比資料庫存放著欲識別(或稱欲用來侵襲)之圖像特徵。另比對方法也是一門學問，眾多比對法之中，常被提出之專家系統(Expert system)也是其中之一種。

要運用 OCR 來正確辨識圖像驗證碼是有一定的難度，只要圖形、顏色、字體做了變化或連接，對 OCR 辨識功能都是挑戰；或是對比資料庫無充分圖像，OCR 很難成功辨識圖像。另外 OCR 光學掃描軟硬體的成本都很高，沒有更高誘因的話，運用 OCR 技術來侵襲任何圖像驗證碼，都是高成本代價的。莊凱婷同學上網驗證之傳統樣式 Poker 牌面雖無多樣花樣，基本上也是屬於圖像之一種，雖然用隨機猜測方式總能猜測成功，但用 OCR 辨識也不容易破解，更何況經過牌面花樣設計之 Poker，被 OCR 辨識破解更不容易了。

專家 2：威達雲端電訊公司是從事 WIMAX 業務之大型企業集團，主要業務是從事寬頻上網、數位有線電視、WIMAX(行動網路、多媒體通訊、行動定位服務、行動 IPTV、行動數位家庭..等等)。所以網頁上之驗證碼設計對本公司也相當重要，一旦網頁交易驗證碼被破解，則將造成網路交易停頓，企業損失極大。網頁上驗證碼之取得與破解是有一定的程序，通常要進入網頁站主之伺服端，此需要高深資訊工程技術與熟練經驗，方能突破

防火牆，繼而需要分析資料格式與位置並讀出資料，轉換為 OCR 掃描儀軟硬體能辨識之格式。要進行 OCR 辨識需要比網頁站主擁有之資訊系統要強大的能力，更何況網頁站主使用之資訊系統品牌或格式雜多。所以補充前位專家所言，OCR 是不容易進行圖像驗證碼的破解，因其投資太大且很容易被偵測出的。有關莊凱婷同學研究設計之 Poker 圖樣驗證碼，充分運用撲克牌之英文字數字及圖樣特性，在第一層驗證過程中，惡意自動化程式成功破解之機率(1/52)的 5 次方不能算高，若再把 2 張鬼牌也加入，則成功破解的機率將更大幅降低，因為鬼牌的辨識可能要用到 OCR，而惡意自動化程式不能只採用隨機猜測方式了。第二層驗證是否也會因鬼牌的加入有變化，則須再請統計專家計算，相信應該不只是 1/44 而已，整體二層驗證的安全性可能會更好。

專家 3：本人從事網路軟體之設計撰寫，有網路驗證碼之設計經驗。圖像驗證之資料庫結構及防衛機制一般都相當嚴謹的，伺服端防火牆、資料格式及儲存位置變化，都是可以提高安全性，而也可利用 time-delay 方式來阻絕惡意自動化程式的隨機猜測攻擊。在莊凱婷同學的研究設計中，可以在系統上限定驗證錯誤(猜錯)三次即停止其驗證功能，必需要等數分鐘之後才可以再行驗證。如此，惡意自動化方程式需要花費多時間來破解。此 time-delay 方式是可以提高傳統 Poker 做圖像驗證碼之安全性。

主席：謝謝今天各位專家的踴躍發言，莊凱婷同學應有完整紀錄，希望今

天針對「以 POKER 為圖像驗證碼之設計研究」安全性問題的探討與分析，

就實務層面，能補強莊凱婷同學之研究內容。

感謝各位今天的撥冗參加，再見。

<以下空白>

由上述專家座談會之專家意見，可以了解 OCR 在破解圖像驗證碼上，確實不易，需要大容量空間儲存對比圖片資料庫，也需要有作業速度快之資訊系統，這些投資均須高成本，若非有高誘因存在，否則使用 OCR 來破解網路驗證碼都是極具挑戰性的。又專家建議本研究設計之「Poker 圖像驗碼」，可以在第一層及第二層驗證時，均將兩張鬼牌一併列入，使之成為 54 張牌，由於鬼牌的牌面圖樣與數字(2~9)及英文(A,J,Q,R,K)不同，因此惡意自動化程式侵襲成功破解之機率會再大幅降低。另專家建議以 time-delay 方式來設計驗證程序，即設定驗證三次仍無法正確通過時，則系統會中止使用者驗證權數分鐘；此 time-delay 方式也有助於提高本「Poker 圖像驗證碼」之安全性。

第六章 結論

第一節 研究成果

綜合上述之研究設計，本研究完成之「Poker 圖像驗證碼」結合了文本型、圖像型驗證碼之特性，以及撲克牌的國際大眾化、易使用及多符號特性，完成一套具雙層驗證功能的「Poker 圖像驗證碼」設計，供網頁個資內容交易或互動之安全驗證使用。經由驗證實驗之結果整理，本研究發展之「Poker 圖像驗證碼」特性如下所述：

第一項 使用性

1. 本設計運用了 52 張傳統圖樣撲克牌面之數字、英文字、圖樣等多符號特性，完成一套具雙層驗證功能之「Poker 圖像驗證碼」。為驗證此圖像型驗證碼及深入了解其使用性，本研究建置實驗性質之網頁網址，由不同背景族群民眾實際上網，進行實驗驗證操作。238 名受測者之中，正確通過雙層驗證共有 202 人，整體正確率達 84.88%，顯見本設計尚能符合大部分使用者的辨識，其簡易程度亦能為大部分使用者接受。另外整體平均驗證操作時間為 33.9 秒稍偏高，此雖係雙層驗證設計造成的，但仍可能會讓使用者感覺不便利。另一方面，操作時間較長也可能是本驗證實驗研究並沒有讓受測者進入一般的網站驗證碼的情境之中，所以受測者在當下就並沒有急著想進入某網站進行其他交易，故純粹抱著慢慢欣賞的心態完成此項實驗。此為日後驗證實驗可再改善之處。

2. 本研究上網實測的不同背景受測者之中

   ①. 不同性別族群在實驗網頁上之驗證碼平均操作時間，分別為男性 34.2 秒及女性 33.6 秒，女性族群雖略快於男性族群，但仍未達顯著差異。

   ②. 不同年齡族群在實驗網頁上之驗證碼平均操作時間，20 歲以

下為 31.8 秒；21~45 歲之間為 31.6 秒；46~60 歲之間為 41.4 秒；61 歲以上為 42.6 秒。變異數分析顯示已達顯著差異，再經事後檢定，發現其中以 45 歲以下之族群操作時間最顯著快於 46 歲以上之族群。此現象可以解釋年輕族群的上班族或學生對電腦之操作熟稔度，均可能優於年齡較長者。

③. 不同教育程度族群在實驗網頁上之驗證碼平均操作時間，高中以下族群為 33.1 秒；大學專科族群為 32.5 秒；碩博士族群為 36.2 秒。但經由單因子變異數分析得知，各族群之間並未達顯著差異。

④. 不同職業族群在實驗網頁上之驗證碼平均操作時間，服務業為 37.4 秒；製造業為 36.4 秒；公家單位族群 29.6 秒；學生族群為 29.8 秒；其他族群為 32.7 秒。變異數分析顯示已達顯著差異，再經事後檢定，其中以學生族群操作時間顯著快於服務業者。此現象可能因學生族群常以電腦為學習工具或進行休閒娛樂活動，亦或是其有較佳之視覺感受或反應能力，故在驗證操作時間均快於服務業者。

第二項 安全性

有關本研究設計之「Poker 圖像驗證碼」安全性

1. 本設計具備雙層驗證功能，而兩層驗證同時被惡意自動化程式侵襲成功機率為 6.11×10^{-8}。相較於常用四個英文字與數字之驗證組合，被暴力攻擊成功的機率 6.77×10^{-8} 相近。

2. 本研究設計採用傳統圖樣之 52 張撲克牌圖樣，可能易被 OCR 辨識侵襲。為避免此現象發生，本研究在實務應用上，或可採用牌面具有複雜圖像，但使用者仍可辨識之撲克牌牌面來運用，則可以降低被 OCR 侵襲成功的機率。

本研究也邀請自動光學檢測專家、資訊工程專家及網路軟體專家，進行專家座談會，就本研究之「Poker 圖像驗證碼」，從 OCR 及資訊網路的技術角度，對本研究設計安全內涵提供寶貴意見。專家一致認同利用 OCR 破

解圖像驗證碼確實不易。專家亦建議本研究設計之「Poker 圖像驗碼」，可以將兩張鬼牌一併列入第一層及第二層驗證，使之成為 54 張牌，則惡意自動化程式侵襲成功破解之機率大幅降低。專家也建議以 time-delay 方式來設計驗證程序，限定使用者驗證次數，若無法正確通過驗證，則系統會中止使用者驗證權數分鐘。此 time-delay 方式也有助於提高「本 Poker 圖像驗證碼」之安全性。

綜合上述及依專家意見來改善本驗證碼設計，則本研究設計之「Poker 圖像驗證碼」確實能符合大眾使用者之使用，並能提供便利性及兼顧安全性。

第二節 建議

本研究運用傳統圖樣 52 張撲克牌面之數字、英文、圖樣等多符號特性，設計此套具備雙層驗證功能的「Poker 圖像驗證碼」。根據驗證結果，其使用性應能為使用者接受，而安全性則可藉由創意設計之牌面複雜圖樣來避免 OCR 侵襲。整體而言，本驗證碼應適宜作為網頁個資內容交易或互動之安全驗證使用。

有關後續研究，建議繼續運用撲克牌之多符號特性，例如增加兩張鬼牌、紅與黑兩種色彩驗證，或是增加 time-delay 驗證設計，甚是將撲克牌之大眾遊戲，融入「Poker 圖像驗證碼」設計之中，讓本「Poker 圖像驗證碼」的設計，在使用性與安全性，能更符合網站業主及使用者之需求。

參考文獻

英文：

〔01〕Brain McWilliams.(2005), Spam Kings.

〔06〕A.M.Turing.(1995), “Computing machinery and intelligence,” *Computers & thought*, pp.11-35.

〔08〕Jeff Yang, Ahmad Salah, E1 Ahmad(2008) , “Usability of CAPTCHAs or usability issues in CAPTCHA design,” *Proceedings of the 4th symposium on privacy and security*.

〔12〕David Summer.(2008), “Implementing Audio CAPTCHA,” *Dr. Dobb’s Journal*, pp.31-38.

〔14〕Jeremy Elson, John R. Douceur, Jon Howell, Jared Saul.(2007), “ Asirra:A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization,” Microsoft Research & Pet□nder, Inc.

〔16〕Philippe Golle(2008), “ Machine learning attacks against the Asirra CAPTCHA,” *Proceedings of the 15th ACM conference on Computer and communications security*.

〔34〕Elson,Douceur..R., Howell & Saul (1974), “A User authentications of the ACM,” Vol.17, No. 8 , pp.437- 442.

〔35〕Elie Bursztein, Steven Bethard, Celine Fabry, John C. Mitchell, Dan Jurafsky.(2010), “How Good are Humans at Solving CAPTCHAs ?” A Large Scale Evaluation. Stanford University.

中文：

〔03〕巫愛雯，民國 100 年，「影像驗證碼技術之研究」。台中技術學院多媒體設計研究所碩士論文(未出版)。

〔19〕陳福維，陳伶志，民國 98 年，「人機辨識碼之中文化研究」，國

立臺灣師範大學資訊工程研究所碩士論文。

〔20〕林明慧，民國 98 年，「應用於行動設備上 CAPTCHA 技術之研究」，銘傳大學資訊工程學系碩士論文(未出版)。

〔29〕曾勝淵，民國 100 年，「網頁驗證碼安全性及效能改善」，東吳大學商學院資訊管理學系碩士論文(未出版)。

〔30〕劉晉昇，民國 100 年，「一個可以自動增加驗證圖庫的圖像 CAPTCHA 系統」，逢甲大學資訊工程學系碩士論文。

〔31〕張紹勳，１９９４，「SPSS For Windows 多變量統計分析」，台北，松崗電腦圖書資料股份有限公司，二版。

〔32〕李金泉，１９９４，「SPSS/PC+實務與應用統計分析」，台北，松崗電腦圖書資料股份有限公司，四版。

〔33〕莊柏年，民國８２年，「科技研究發展人員組織溝通與組織承諾關係之研究 －「以工業技術研究院為例」，國立彰化師範大學工業教育研究所碩士論文。

網路：

〔02〕最新線上檢索日期: 2012 年 2 月 21 日。
http://en.wikipedia.org/wiki/CAPTCHA

〔04〕最新線上檢索日期: 2012 年 5 月 30 日。
http://blog.xuite.net/ppopp33/blog/BCCAPTCHA

〔05〕最新線上檢索日期: 2013 年 4 月 28 日。
http://en.wikipedia.org/wiki/Optical_character_recognition

〔07〕最新線上檢索日期: 2012 年 2 月 21 日。
http://en.wikipedia.org/wiki/CAPTCHA

〔09〕最新線上檢索日期: 2013 年 1 月 8 日。
http://www.google.com/recaptcha

〔10〕最新線上檢索日期: 2012 年 5 月 30 日。
http://thenextweb.com/media/2011/10/06/solve-medias-sma

rt-captcha-ads-improve-brand-recall-by-67/

〔11〕最新線上檢索日期: 2012 年 5 月 16 日。
http://yingxiao.baidu.com/support/topic/94/

〔13〕最新線上檢索日期: 2012 年 5 月 16 日。
http://news.cnet.com/8301-31921_3-57376332-281/stanford-university-researchers-break-nucaptcha-video-security/

〔14〕最新線上檢索日期: 2012 年 5 月 16 日。
http://community.websense.com/blogs/securitylabs/archive/2011/05/02/a-weekend-of-click-jacking-on-facebook.aspx

〔15〕最新線上檢索日期: 2012 年 12 月 12 日。
http://www.petfinder.com/

〔17〕最新線上檢索日期:2013 年 5 月 14 日。
http://www.csie.ntu.edu.tw/~cjlin/

〔21〕最新線上檢索日期:2013 年 5 月 15 日。
http://technabob.com/blog/2012/04/30/playthru-captcha-alternative/

〔22〕最新線上檢索日期: 2013 年 1 月 8 日。
http://www.neebar.com/2008/04/rapidshare-captcha-cat/

〔23〕最新線上檢索日期: 2013 年 1 月 8 日。
http://aralbalkan.com/871/

〔24〕最新線上檢索日期: 2013 年 1 月 8 日。
http://captcha.tw/node/442

〔25〕最新線上檢索日期: 2013 年 4 月 23 日。
http://dice-captcha.com/

〔26〕最新線上檢索日期: 2012 年 12 月 1 日。
http://crecaptcha.org/index.php?page=home&lang=cht

〔27〕最新線上檢索日期: 2012 年 12 月 1 日。
http://chinese.engadget.com/2009/03/30/on-captcha/

〔28〕最新線上檢索日期: 2012 年 12 月 1 日。
http://newsletter.teldap.tw/news/NewsContent.php?nid=5761&lid=658