

圖像驗證碼之設計與實作

程凱* 黃靖栩 王佳萱 楊吳泉

義守大學智慧網路科技學系

摘要

近年來資訊業不斷的進步發展，為人們帶來便利，使用網際網路的時間也越來越長，卻讓一些有心人士利用此便利性將自動化程式，也就是所謂的「機器人」，不當使用於網路上，造成資源的浪費。例如創造大量電子郵件帳號藉此發送垃圾信件，就是一種資安上的風險。2000年時卡內基大學發明驗證碼(CAPTCHA)系統，這是利用電腦去分辨使用者是機器還是人類。系統一開始是由英文和數字去組成進行排列，在經過扭曲變形等輸出驗證碼，後來光學的進步，使得文字驗證碼遭到破解。近年發展出圖片驗證系統，此系統是將許多圖片放在題目中，利用選擇圖片來完成驗證，進而提升其安全性。本研究設計一圖像驗證碼系統，並藉由實際操作與使用回饋，驗證此系統之實用性。

關鍵詞：驗證碼，圖像驗證，資訊安全

一、前言

當一個計算機程序能夠生成一個測試來區分人和計算機時，它被稱為驗證碼。過去，網站常被大量的惡意程式攻擊，這些惡意程式藉由重複註冊來消耗大量的網路資源或在網路上散播不實的謠言。為了解決這個問題，研究人員產生了將驗證碼利用於網路的想法，這樣能阻止機器人大量的攻擊伺服器。驗證碼作為一個安全機制，必須設計只有人類才能回答的問題。過去的文字驗證碼已經能被計算機程式輕鬆的破解，如果想要加深文字驗證碼的難度往往會使得人類也難以辨識。近年來，圖片驗證碼已經成為替代方案，利用視覺方法來挑戰計算機程式。而許多研究人員也開始建立基礎的圖片驗證碼系統。

圖片驗證碼研究的目的主要在於提高網站、應用程式或其他系統的安全性，防止機器人或自動化程式的非法存取。隨著科技的不斷發展，傳統的文字驗證碼漸漸變得容易被破解，因此轉而針對圖片進行驗證碼的研究成為一個重要的方向。首先，圖片驗證碼的研究目的在於提高安全性。在網路世界中，有大量的敏感資訊需要保護，例如個人帳戶、金融交易等。機器人或爬蟲程式可能會利用自動化的方式進行非法存取，對這些資訊進行攻擊。使用圖片驗證碼可以增加辨識的難度，從而提高系統的安全性，減少被非法存取的風險。其次，圖片驗證碼的研究目的在於提高使用者的使用體驗。傳統的文字驗證碼可能對一些使用者造成困擾，因為有時候文字不易閱讀，導致錯誤的輸入或耗費過多的時間。相比之下，圖片驗證碼可以更加直

觀，使用者更容易理解和操作。這樣一來，不僅可以確保安全性，還能提高使用者的使用滿意度，降低因驗證碼而產生的使用障礙。另外，圖片驗證碼的研究目的也在於應對新型的攻擊手段。隨著技術的不斷進步，攻擊者的手段也在不斷演進。傳統的文字驗證碼可能容易受到機器學習或其他高級攻擊的威脅。因此，研究如何使用圖片、圖形或其他更複雜的元素來構建驗證碼，以對抗新型攻擊手段，是圖片驗證碼研究的重要目標之一。最後，圖片驗證碼的研究還可以推動相關領域的發展。圖片處理、模式識別、機器學習等技術在這一領域都有廣泛應用，進一步的研究和發展可以促進這些領域的進步。同時，圖片驗證碼的研究還可以激發更多相關領域的探索，拓寬研究的視野，促使更多新的理念和技術的湧現。整體來說，圖片驗證碼的研究目的是多方面的，包括提高安全性、提升使用體驗、應對新型攻擊手段以及推動相關領域的發展。這些目的共同推動著圖片驗證碼技術的不斷創新和進步。

在本研究中，先進行驗證碼相關文獻探討，從驗證碼的起源、驗證碼類型、驗證碼的破解技術等相關研究，作為本研究的基礎。本研究蒐集各式各樣的圖片，並將圖片經由線上軟體將圖片進行部分馬賽克，以及建立一個簡易的網頁來進行圖片驗證碼。研究圖片如果經由馬賽克來增加圖片辨識的難度是否能增加安全度，以及是否會影響大眾對於圖片驗證碼的接受度。結束測試後，計算整體受試者通過此圖片驗證碼之正確率，以及依據受測者的操作時間，分析不同族群使用的差異性並分析

之間的差異原因。接著本研究將依據「馬賽克圖片驗證碼」去做更進一步的安全性分析。

本論文分為六個部分，以下為各小節的敘述：

第一小節為簡介，敘述研究背景與動機、研究目的、研究限制、研究方法和流程與架構等。第二小節是文獻探討，探索驗證碼的起源、類型及相關研究，並深入探討各種驗證碼可能會被破解的方法。第三小節是研究設計，敘述如何設計一個具有馬賽克圖片的圖片驗證碼的過程，並介紹的相關工具及程式軟體。第四小節為驗證實驗，敘述「馬賽克圖片驗證碼」設計之使用性，並藉由本實驗所架設之網站來做實際的施測。第五小節為驗證結果與分析，驗證結果之分析與討論，說明實測過後的結果。並根據施測的結果來分析「馬賽克圖片驗證碼」之正確率是否會因不同族群、年齡、性別而有所影響。第六小節是結論。

二、文獻探討

2.1 驗證碼理論

驗證碼（CAPTCHA）的起源可以追溯到20世紀90年代中期，當時物聯網的使用逐漸普及，垃圾郵件和自動化攻擊也開始威脅到網站和網路系統的正常運作。為了應對這一挑戰，計算機科學家和研究人員開始思考如何區分人類用戶和自動化程式[1]。1997年，卡內基梅隆大學的 Luis von Ahn 教授和他的團隊開始尋找一種方法，可以在線上區分人類用戶和計算機程式。他們最終提出了 CAPTCHA 的概念，即 “Completely Automated Public Turing test to tell Computers and Humans Apart”

（完全自動的公共圖靈測試，用於區分計算機和人類）[2-4]。

CAPTCHA 的核心思想是通過要求用戶執行一些對人類容易而對計算機難以完成的任務，來確保用戶是真實的人類。最初的 CAPTCHA 版本包括讓用戶辨識扭曲的文字或數字，這樣計算機程序就難以準確地解讀。這種方法的初衷是使用人類的視覺和認知能力，而這對於早期的光學字符識別（OCR）技術來說是一個巨大的挑戰。在進行 CAPTCHA 技術的發展過程中，研究人員逐漸意識到可以同時利用用戶生成的數據來解決其他問題。例如，reCAPTCHA 是一種廣泛使用的 CAPTCHA 變種，它利用用戶輸入的數據來數字化和改進印刷書籍中的文字。這樣的方法使得解決 CAPTCHA 同時具有了區分計算機和人類的功能，同時實現了有價值的數據處理。隨著技術的不斷發展，CAPTCHA 的形式也在不斷變化。除了扭曲的文字，還有圖片辨識、滑動圖片驗證、圖片拼圖等多種形式的 CAPTCHA 應運而生。此外，生物特徵識別技術（如指紋識別、視網膜識別）和行為分析（如滑鼠移動軌跡、點擊模式）也被整合到 CAPTCHA 中，以進一步提高安全性。總體來說，CAPTCHA 的起源是為了應對網路安全威脅，特別是防止自動化攻擊和垃圾郵件。隨著技術的發展，CAPTCHA 的形式和應用領域也在不斷擴展，以確保在線上環境中的安全性和真實性[5]。

2.2 驗證碼的類型

驗證碼大致可分為文本型（text-based schemes）、圖片型（image-based

schemes)、生物特徵型、行為分析型、問答型以及簡訊和信箱型[6]。

1. 文本型

文本型驗證碼有文字驗證碼及數字驗證碼。文字驗證碼(圖1)是一種透過文字形式提供的人機識別驗證工具，旨在確保使用者是真實的人類而不是自動化程序或機器人。這種驗證碼通常以難以識別的形式呈現，要求使用者在註冊、登錄或執行特定操作時輸入驗證碼，從而驗證其真實身份。文字驗證碼在網絡安全和使用身份驗證方面發揮著關鍵作用，有助於防止惡意活動和網絡攻擊。



圖1. 文字驗證碼

文字驗證碼的應用領域非常廣泛，常見於註冊新帳戶、登錄(圖2)、密碼重置、線上調查等場景。此外，許多線上服務和網站採用文字驗證碼來防範惡意爬蟲、垃圾註冊和其他自動化攻擊，以維護網絡平台的整體安全。



圖2. 登入驗證碼

2. 圖片型

圖像驗證碼是一種網站安全機制，用於區分真實使用者和自動化程式，特別是機器人或惡意腳本。這種驗證方式通常要求用戶進行視覺識別或互動操作，確保其是真實的人類。

圖像驗證碼是利用不同的圖片性質去做改變，例如現在流行的 GOOGLE reCAPTCHA(圖3)、拖曳拼圖式驗證碼(圖4)。



圖3. GOOGLE reCAPTCHA

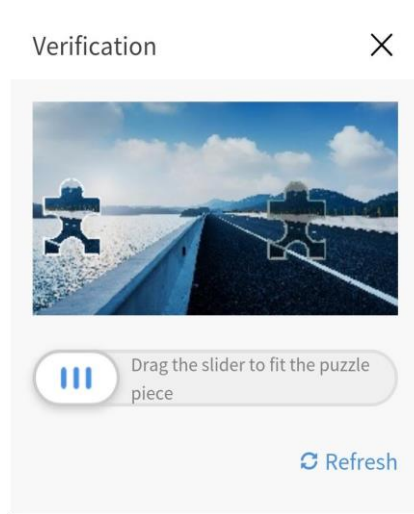


圖4. 拖曳拼圖式驗證碼

3. 生物特徵型

生物特徵型驗證碼是一種透過生物特徵識別技術，將個體獨特的生理或行為特徵應用於身份驗證的安全機制。這種驗證方式利用人體生物特徵的獨一無二性，確保使用者身份的真實性和唯一性，進一步提升安全性和使用便捷性。例如：虹膜辨識、指紋辨識(圖5)、臉部辨識(圖6)以及聲紋辨識。

生物特徵型驗證碼通過運用生物特徵的獨特性，提供了更高層次的身份確認安全性。相較於傳統的密碼或卡片驗證方式，生物特徵型驗證碼更難被模仿或冒用，提高了系統的抗攻擊性。然而，同時也需要關注隱私和個人數據保護的問題，確保這些生物特徵資訊的合法使用和儲存。生物特徵型驗證碼的不斷發展將為我們的生活帶來更安全、更便捷的身份確認體驗。

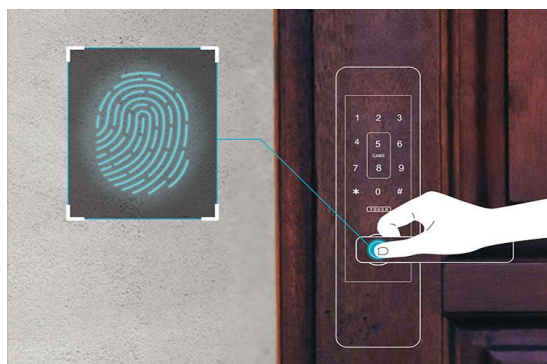


圖5. 指紋辨識



圖6. 臉部辨識

4. 行為分析型

行為分析型驗證碼是一種透過分析使用者行為模式來確認其身份的安全驗證機制。與傳統的密碼或生物特徵辨識不同，行為分析型驗證碼關注的是使用者在互動過程中的行為習慣、操作方式和模式，以此作為身份認證的依據。例如在應用程式、網站或系統中的滑鼠移動、點擊模式(圖7)、鍵盤輸入速度等數據。每個人的操作行為都有一定的獨特性，因此通過分析這些行為特徵，可以建立一個獨特的行為模型，用於身份驗證。

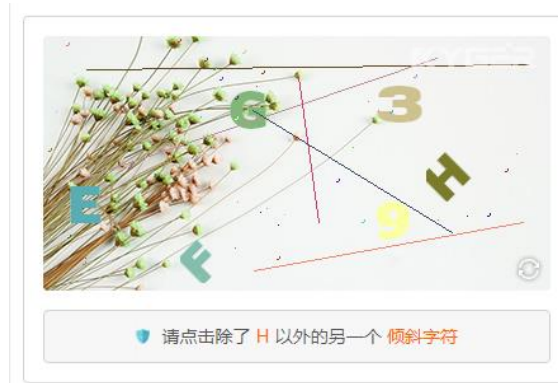


圖7. 點擊模式

行為分析型驗證碼在確保身份安全的同時，避免了一些傳統身份驗證方式可能存在的弱點，如密碼的被盜風險或生物特徵辨識的技術限制。它更加強調用戶的實際操作行為，減少了對用戶的侵擾，提供了更為自然且無縫的身份驗證體驗。然而，同時也需要注意系統的安全性，以防止惡意攻擊者模擬合法用戶的行為進行身份冒用。隨著科技的不斷進步，行為分析型驗證碼將在未來繼續發揮重要作用，為數字安全提供更多層次的保障。

5. 問答型

問答型驗證碼是一種通過提問和回答特定問題來確認使用者身份的身份驗證機制。

這種方式不同於傳統的密碼或生物特徵辨識，而是藉由使用者對預先設定的問題給予正確回答，以達到確保身份合法性的目的(圖8)。

實驗功能：驗證方式 瞭解驗證方式功能

圖8. 問答型驗證碼

問答型驗證碼是一種簡單而直觀的身份確認方式，特別適用於那些不需要高度安全性的應用場景。它不依賴於複雜的技術，易於實施和使用。然而，同時也需要注意問題的合理性和安全性，以免被攻擊者利用漏洞進行非法訪問。在實際應用中，問答型驗證碼常與其他驗證方式結合，形成多層次的安全防護體系。

6. 簡訊和信箱型

簡訊和信箱型驗證碼是一種通過簡訊或電子郵件發送一次性驗證碼，用戶需要輸入這些碼來完成身份驗證的機制。這種方式常見於註冊、登錄、重設密碼等需要驗證身份的應用場景(圖9、10)。



圖9. 簡訊型驗證碼



圖10. 信箱型驗證碼

這兩種方式的優勢在於其簡單易行，無需額外的硬體設備，使用方便。同時，由於驗證碼是一次性的，即使被截獲，也難以被濫用。然而，也有一些潛在的風險，例如 SIM 卡被盜用、郵箱被入侵等，因此在實際應用中，需要綜合考慮安全性和使用便捷性。

2.3 驗證碼的破解技術

根據相關文獻顯示[7,8]，大多數的驗證碼都已經被惡意自動化程式破解，但依照被機器辨識破解的機率來說，圖像驗證碼被破解的機率較低。圖像驗證碼較難被破解的原因是人類處理圖片的能力相較於機器人辨識圖片的能力是較強的，再加上電腦需要先將圖片做分類、進行目標辨識，最後才是理解整個圖片的背景，所以圖像驗證碼被破解的機率比其他驗證碼還要低很多。以下將常見的破解方式介紹：

1. OCR 光學自動辨識法

光學自動辨識 (OCR) 是一種技術，它使用光學、機械和電子手段來將印刷或手寫文本轉換成電子碼，以便計算機可以理解、搜索和處理。OCR 技術在許多領域中都有廣泛的應用，包括文檔數字化、自動化數據輸入、圖書館管理、印刷和出版等。

2.暴力破解法

暴力破解法是一種密碼分析的方法，主要透過軟體逐一測試可能的密碼，直到找出真正的密碼為止。如果一個多位數並且包含以上所有可能字元的密碼，其組合方法一定多的驚人，且每增加一位數，密碼組合數量會以數十倍指數成長（例如：包含數字及字母大小寫，共62個字元的10位數的密碼，共有 62^{10} ，大約 83.9×10^{16} 種組合。因此，暴力破解法對於大量的資料來說可行性並不高，甚至要花很多時間才能成功破解，對於現在的技術而言，暴力破解法是不太會被採用的。

3.資料庫攻擊法

資料庫攻擊法大多都是針對圖像驗證碼的图片資料庫，因為圖像驗證碼需要大量的資料庫空間，而樣本也不容易取得，如果檔案過大的話，會影響傳輸速率。本研究認為 OCR 也不容易破解資料庫，因為現在的資料庫已經變得很先進，也有做相對的保護措施，因此不易進入。

4.人力破解法

人力破解法是雇用廉價的第三世界國家人力，利用大量的人力去辨識驗證碼，以進行不法商業。由於人類能利用自身的視覺能力去輕易辨識出文本驗證碼，所以必須將資料進行加密，否則很難阻擋人力破解驗證碼。

三、研究方法

3.1 研究架構

圖像驗證碼的實現需要一個適當的架構，包括前端設計和後端驗證處理。藉由此設定來達到網頁是由人類進入，而不是機器登入。下面是圖像驗證碼所需的主要

架構組件：

1. 前端介面：這是使用者與圖像驗證碼進行交互的界面。它通常由網頁或應用程式的前端部分實現。前端介面應該清晰地顯示驗證碼圖像和相關的任務，並提供相應的操作元素，例如列出選單或輸入框。
2. 圖像生成：圖像生成模組負責生成馬賽克圖像。它可以使用隨機生成的圖像、變形的圖像、扭曲的圖像等技術來增加驗證碼的複雜度和安全性。生成的圖像應該具有足夠的差異性，以區分人類使用者和機器。
3. 後端驗證：後端驗證處理負責接收使用者提交的圖像馬賽克答案。當它接收使用者提交的答案，並進行比對和驗證，以識別使用者的回答是否正確。
4. 安全性考量：圖像驗證碼架構應該具有一定的安全性措施，以防止惡意攻擊和破解。例如，防止自動化腳本的多重提交和暴力破解攻擊。這可以通過限制提交次數、添加時間限制、使用適當的加密技術等方式實現。

在這個研究中，我們選擇使用 Notepad++ 作為前端網頁的開發工具，其提供了一個簡單且功能豐富的編輯環境，適合快速開發出網頁應用程式。這個前端網頁的主要任務是展示網頁和接收使用者的輸入，並展示隨機選取的馬賽克圖片。為了實現這一目標，Notepad++ 的開發者需要使用 HTML、和 JavaScript 等網頁技術。

Xampp 被選為後端服務的架構，它包括了 Apache 伺服器和 MySQL 資料庫，提供了一個完整的開發環境。Apache 伺

伺服器負責處理前端網頁的請求，並將它們轉發到相應的處理邏輯。而 MySQL 資料庫被用來存儲後台的語言資料庫，其中可能包含了各種答案和相應的比對條件。當使用者打開網頁時，前端網頁會自動連接到圖片資料夾，這是一個存放馬賽克圖片的地方。通過使用 JavaScript，網頁可以從資料夾中隨機挑選一張馬賽克圖片並展示給使用者。這樣的設計使得每次使用者訪問網頁時都能看到不同的圖片，增加了實驗的隨機性和驗證的可靠性。使用者填寫完畢後，前端網頁會將填寫的內容和後台的答案進行比對驗證。這個比對過程可能會利用程式比對，以確保使用者提供的答案是正確的。同時，答案、正確與否的結果和填寫的時間將被記錄下來，這有助於後續的數據分析和評估實驗的有效性。

整個架構的設計使得實驗過程變得方便且快速，前端和後端的相互工作確保了使用者體驗的順暢性，同時後台的數據儲存和處理為實驗結果的評估提供了豐富的資料。這樣的技術結合，不僅實現了實驗的基本目標，還讓我們學習了網頁架構的基礎。(圖11)

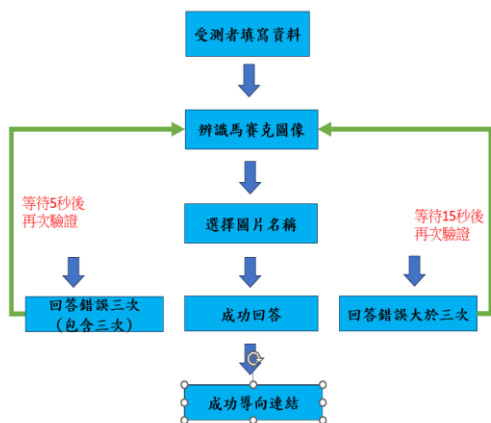


圖11. 研究流程

步驟一：測驗者填寫資料

步驟二：辨識隨機出現的馬賽克圖像

步驟三：會先讓測驗者選擇種類，在選擇圖片正確名稱

步驟四：測驗者如果回答正確，會直接導向網頁連結，而錯誤三次(包含三次)則會等待5秒後再次測驗；三次以上則是等待15秒後再次測驗。

3.1.1 使用的程式工具

Notepad++是一套免費文字編輯器(圖12)，是一套自由且開放原始碼軟體，其操作簡單，十分適合用在編寫電腦程式語言上。內部程式語法有許多不同選擇，使用者在編寫不同語言時能隨時更改，編寫同時相關語法會呈現不同顏色，以方便觀看和降低錯誤率。且在完成編寫後可直接按執行功能，連接到你所想使用的瀏覽器。



圖12. Notepad++內部和封面

XAMPP 是一個可以簡單整合 Apache (網頁伺服器)、PHP (伺服器端語言) 及 MySQL (資料庫) 的軟體包，透過 XAMPP 就可以方便快捷架站。由於 XAMPP 同時包含這些軟體，所以大多數人會直接下載此軟體，利用此方便性去架設網站，且可利用此資料庫去儲存資料，同

時在網頁有所需要時能去顯示你所儲存的資料或圖片。(圖13)

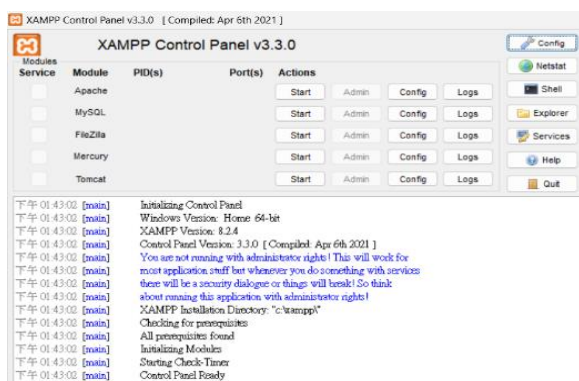


圖13. XAMPP 介面

Apache：是一個開放原始碼網頁伺服器軟體。

MySQL：是一個可以用於儲存的資料庫，經常同時和網站使用。

PHP：是一個伺服器腳本的語言。他可以和 HTML 整合，以實現結合靜、動態網站

phpMyAdmin：用來管理 MySQL 資料庫的工具，使用戶能簡單去操作資料庫，如創建、刪除或修改。

整體來說，建一個動態且功能豐富的網站通常需要不同的技術元件協同工作。會先使用 PHP 腳本語言去編寫 HTML 網頁，因為它可以和 HTML 緊密整合，使開發人員能夠輕鬆創建具有豐富功能的網站，Apache 則用於處理網頁請求並將網頁內容傳送給用戶的瀏覽器，後台資料庫儲存網頁資訊則使用 MySQL，因為它支援多種數據類型和查詢語言，且同時配合使用類似 phpMyAdmin 的工具，以使用戶能夠方便地操作資料庫，例如創建、刪除或修改數據表。

3.1.2 資料庫欄位設計

如圖14作為介紹資料庫種類名稱。

#	名稱	類型	編碼與排序	屬性	空值(Null)	預設值	備註	額外資訊	動作
1	names	varchar(10)	utf8mb4_unicode_ci	KD	非				修改 刪除 更多
2	age	int(10)		KD	非				修改 刪除 更多
3	gender	int(10)		KD	非				修改 刪除 更多
4	question2	int(10)		KD	非				修改 刪除 更多
5	time	int(10)		KD	非				修改 刪除 更多
6	result	int(10)		KD	非				修改 刪除 更多
7	id	int(10)		KD	非			AUTO_INCREMENT	修改 刪除 更多

圖14. 資料庫個欄位名稱

names：代表使用者學號。

age：代表使用者年齡。(1 代表11-20歲；2 代表21-30歲；3 代表31-40歲，以此類推)

gender：代表使用者性別。(1 代表男生；2 代表女生；3 代表不願透露)

question2：代表使用者選擇的答案。

time：代表使用者填寫到送出所花費的時間。

result：代表正確性。(1 代表正確；2代表錯誤小於三次；3代表錯誤大於三次)

id：流水號。

在此資料庫中，欄位的類型設置有許多選擇，可依照你所想儲存的資料去選擇。且也可以設定你所想儲存得長度(INT: -2147483648 ~ 2147483647；VARCHAR :0~65535)。編碼排序的部分是選擇 unicode，因為此實驗需要用於標準來排序，且由於有中文，所以使用 unicode 會比較精準。

3.2 圖像驗證碼之設計

此圖像驗證研究是利用馬賽克去塗鴉照片，讓使用者在進入網頁前會先經過馬賽克驗證，通過者才能進入網頁。由於圖片的部分大小不一，所以我們選擇手動的方式去馬賽克重要部分，讓使用者去選擇正確答案。我們使用的是網頁版的馬賽克，

利用選擇圖片放入，在選擇你所想馬賽克的像素去改變圖片，儲存即可。(圖15)



圖15. 馬賽克的介面

在圖片編輯工具的進階選項中，圖片的馬賽克效果有了更多的控制選項。(圖16)這個特殊的馬賽克選擇模式提供了更靈活的調整，使用戶能夠根據具體需求調整像素畫質、模糊視覺效果以及形狀等多個參數。在這個馬賽克效果的模式中，您可以自由調整像素畫質，從2到100的範圍內選擇。這意味著您可以根據自己的需求，選擇更加細緻或者更加粗糙的馬賽克效果。最後，用戶只需選擇所需的馬賽克大小，點擊打馬賽克，整個過程就完成了。(圖17)

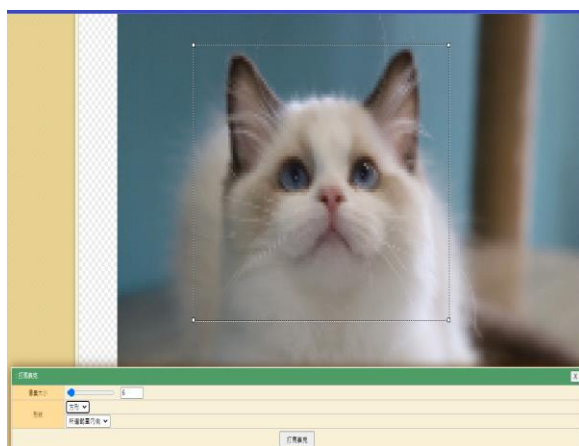


圖16. 馬賽克像素選擇和區域選擇



圖17. 圖片馬賽克後

3.3 網站之設計

本研究是使用 cPanel 去架設網站，它是一種用於管理網站和伺服器的網頁控制面板。它提供了一個直觀的用戶界面，這使得即使對於沒有深入技術知識的用戶來說，管理網站和伺服器也變得相對簡單。主要的功能有網站管理、郵件管理、數據資料庫管理和文件管理等。當使用者在使用它時，工具頁面都會幫你分區分好，這種直覺性的分區設計使得用戶可以輕鬆找到所需的功能，讓用戶可以輕鬆上傳、下載、瀏覽和編輯網站文件。(圖18)

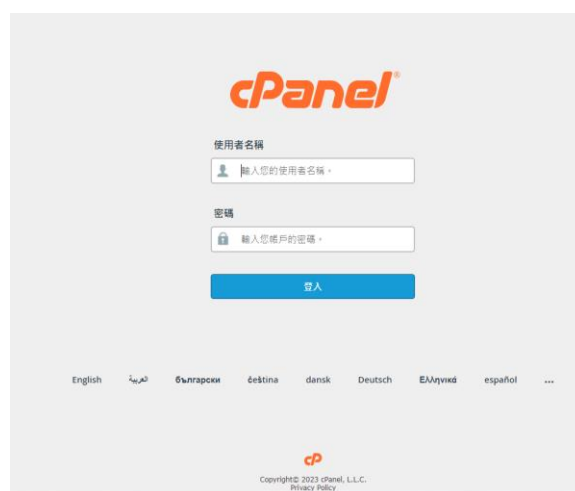


圖18. cPanel 登入介面

本研究使用了 phpMy 管理、MySQL 資料庫、網域建設和檔案管理員。第一步是建設一個資料庫(圖19)，以方便收集所需要資訊，再透過 phpMy 管理去察看所蒐集到的資訊，當這些用完後再將所寫好的程式碼透過檔案管理上傳，最後在建設一個網址。



圖19. 資料庫建立

資料庫建立完成後，透過phpMySQL管理去新增你所需要的欄位和觀看你所蒐集到的資料數據(圖20)。

	names	age	gender	question2	time	result	id
☐	編輯 複製 刪除	10908023	2	1	9	32	1 24
☐	編輯 複製 刪除	10908008a	1	3	10	35	1 27
☐	編輯 複製 刪除	10908008a	4	2	8	13	1 28
☐	編輯 複製 刪除	10908001	2	1	19	31	2 30
☐	編輯 複製 刪除	10908008a	2	2	7	43	1 31
☐	編輯 複製 刪除	10908008a	2	2	7	32	1 32
☐	編輯 複製 刪除	10908008a	4	1	54	21	1 33
☐	編輯 複製 刪除	123	2	2	56	34	1 34
☐	編輯 複製 刪除	11151008a	1	3	3	32	1 35
☐	編輯 複製 刪除	11105037	1	2	60	18	1 36

圖20. 資料數據

這些建立完後再使用檔案管理去上傳網頁架構的程式碼(圖21)。



圖21. 檔案管理上傳

上圖中的1.php 是我們的網頁架設，

pic.php 是顯示隨機照片，back.php 是前端網頁填寫完畢後傳送到後台對比是否正確的。

接下來建立一個網址(圖22)，即可將所展現出來的網頁讓人人都可以連線。

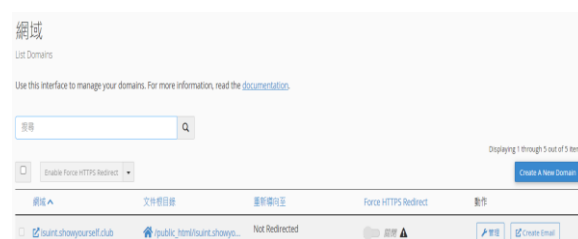


圖22. 網址建置

四、研究驗證

4.1網頁驗證

本研究的網頁架設是建置最基本的網頁驗證的填寫內容。此設計一方面是為了能夠了解此架構是否方便、快速。(圖23)

學號	
性別	男生 v
年齡	11-20 v
照片	
請選擇種類	請選擇類別... v
請選擇名稱	請選擇正確答案... v
送出	

圖23. 驗證碼網頁

為了提升使用者的方便性，由於當初只有一個名稱選項，而且太多不同類型的種類在選項內，所以在原有的名稱選項基礎上，新增了一個種類選項。透過新增的種類選項，使用者現在可以更精確地找到他們所需要選擇的類別，節省了尋找的時

間。

圖24為種類的清單，這個清單將不同的名稱歸納成特定的類別，使得整個選項列更加有秩序。

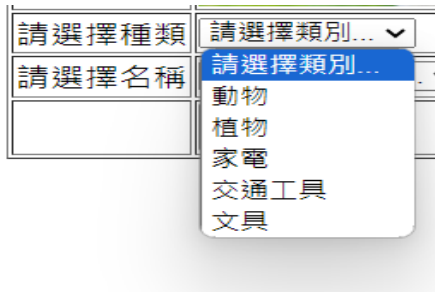


圖24. 種類清單

在使用者看完馬賽克圖片後，選擇相符種類後，名稱選項將會出現相關名稱，再由使用者去選擇相對應答案，圖25為選擇特定種類後名稱會出現相關選項。

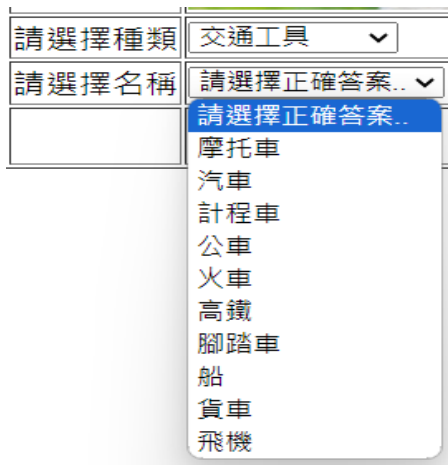


圖25. 特定種類的名稱選項

4.2 操作驗證

在使用者填寫完畢送出後，後台將進行答案驗證，以對照使用者提供的答案和正確答案，以確定驗證的成功與否。本研究制定了一套合理的次數和時間限制，以提供良好的使用者體驗。

具體而言，如果使用者在三次（包含三次）以下未成功通過驗證，系統將在五秒後自動將其導回驗證網頁，給予使用者

機會進行正確的操作(圖26)。這種短時間的重試間隔有助於減少使用者等待時間，提高整體效率。



圖 26. 三次（包含三次）錯誤

然而，若使用者連續失敗驗證達到三次以上，系統會延長重試的時間，將等待時間設定為十五秒(圖27)。這能促使使用者更加謹慎地填寫驗證資訊，提高整體安全性。在成功通過驗證的情況下，失敗次數將重新計數，為使用者提供新的起點(圖28)。

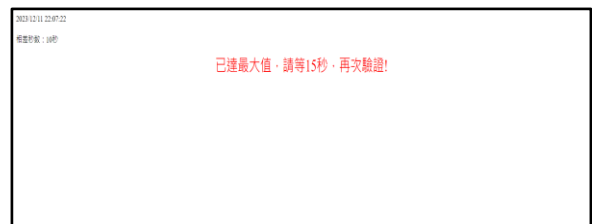


圖27. 錯誤次數大於三次



圖28. 成功畫面

4.3 資料處理驗證

使用 MySQL 資料庫做為後台資料收集，當使用者在網頁輸入完畢後，資料庫就會自動新增資訊(圖29)，方便管理者觀看。

	names	age	gender	question2	time	result	id
☐	編輯 複製 刪除 10908023	2	1	9	32	1	24
☐	編輯 複製 刪除	1	3	10	35	1	27
☐	編輯 複製 刪除 10908008a	4	2	8	13	1	28
☐	編輯 複製 刪除	2	2	18	7	2	29
☐	編輯 複製 刪除 10908001	2	1	19	31	2	30
☐	編輯 複製 刪除 10908008a	2	2	7	43	1	31
☐	編輯 複製 刪除 10908008a	2	2	7	32	1	32
☐	編輯 複製 刪除 10908008a	4	1	54	21	1	33
☐	編輯 複製 刪除 123	2	2	56	34	1	34
☐	編輯 複製 刪除 11151008a	1	3	3	32	1	35
☐	編輯 複製 刪除 11105037	1	2	60	18	1	36
☐	編輯 複製 刪除 isu10923015a	2	2	41	35	1	37
☐	編輯 複製 刪除	2	1	7	15	1	38
☐	編輯 複製 刪除	6	3	29	38	2	39
☐	編輯 複製 刪除	6	3	29	43	2	40
☐	編輯 複製 刪除	2	1	20	20	1	41
☐	編輯 複製 刪除 10806052a	2	1	30	59	1	42
☐	編輯 複製 刪除 10926010A	2	2	22	21	1	43

圖29. 資料收集

五、回饋數據分析

5.1 數據蒐集

以下的數據收集是利用現在大學中人人幾乎都會使用的應用程式，Dcard 和義守大學社群(圖30)。



圖30. 義守大學社群

在此研究中，共收集了61份樣本資料，其中男女比率女性占比較多(圖31)。由於此研究測驗是在學校中請同儕測驗的，所以在這些人數之中，年齡相對是比較年輕的(圖32)。

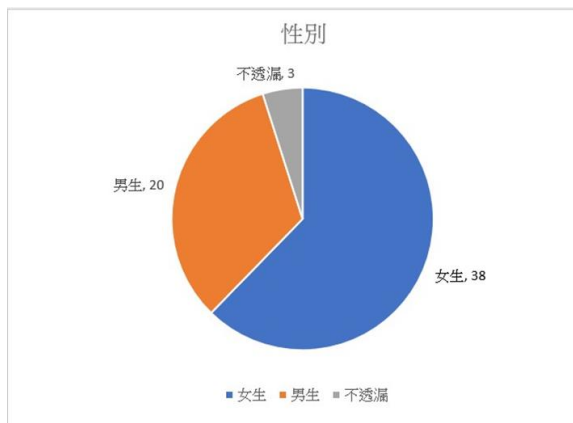


圖30. 男女比例

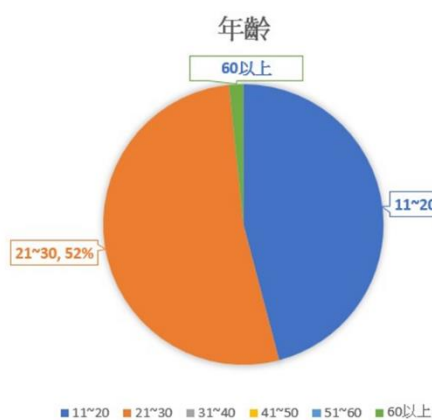


圖31. 年齡比例

在這些測驗中，我們發現大部分的測驗者，一次成功的比率很高(圖32)。

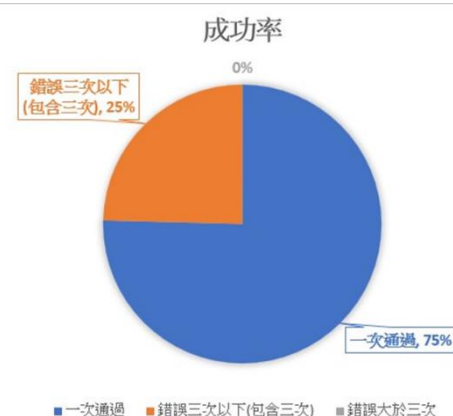


圖32. 成功比例

5.2 差異分析

本研究是和現在網路上常見的九宮格驗證做差異性比較，這兩種都是為了驗證

使用者是否為真人，以下為分析此兩種的差異。

參考文獻中[9,10]有提到Poker圖像驗證有238份資料，而成功有202份，成功率為84.8%，平均33.9秒；影像驗證有200份資料，成功有162份，成功率為81%，平均15.56秒。本研究所提到的馬賽克有61份資料，成功有46份，成功率為75%。由於這次收集樣本數不多，導致成功百分比沒有那麼高。(圖33)

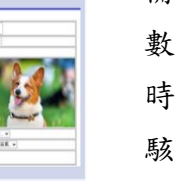
	以Poker圖像驗證碼之設計研究	影像驗證碼應用於行動裝置之研究	圖像驗證碼之設計與實作
圖像範例			
平均秒數	33.9秒	15.86秒	27.81秒
成功率	84.8%	81%	75%

圖33. 驗證碼差異分析

六、結論

圖像驗證碼技術是一種重要的安全機制，用於區分人類使用者和機器人。通過要求使用者完成與圖像相關的任務或回答問題，圖像驗證碼能夠有效地防止機器人的非法訪問和惡意行為。此技術其實比起文字驗證更有效能且更能防禦網路攻擊。馬賽克圖像驗證其實比一般圖像驗證來的更有困難度。

這些驗證碼技術都利用人類與機器在視覺辨識能力上的差異，設計出不同的任務或挑戰，使機器難以準確辨識或完成。例如，要求使用者在一系列圖片中選擇特定物體或識別特定形狀或顏色，或者讓使用者根據提示選擇正確的答案。優點是此技術對於機器人來說往往是困難的，因為

它們需要具備視覺辨識和理解能力。此外，圖像驗證碼技術還採用了一些增加驗證碼複雜度和安全性的技術，如圖像扭曲、變形、分割和拼圖等。這些技術使驗證碼更難以被機器識別，同時保持使用者友好性。

然而，隨著駭客攻擊技術的不斷進步，傳統的圖像驗證碼技術可能會面臨一些挑戰。攻擊者可以使用機器學習和計算機視覺技術來破解某些驗證碼。因此，為了提高圖像驗證碼的安全性，我們需要不斷創新和改進。在設計圖像驗證碼時，需要具備一定的安全性措施，這包括限制提交次數、實施時間限制、使用加密技術等。同時圖像驗證碼需要不斷創新和改進來避免駭客利用蒐集圖庫來破解。此缺點是需要努力更新圖庫以及足夠的資料庫。

參考文獻：

- [1] 陳威翔，基於馬賽克圖像驗證碼之研究，碩士論文，朝陽科技大學資訊管理系，雲林，2019。
- [2] CAPTCHA project website. <http://www.captcha.net>
- [3] J.Thatcher, "CAPTCHAs, CAPTCHAs everywhere," retrieved from: <https://jimthatcher.com/captchas.htm>(2019)
- [4] A. S. Almazayad, Y. Ahmad, and S. A. Kouchay, "Multi-Modal CAPTCHA: A User Verification Scheme," IEEE International Conference on Information Science and Applications, pp. 1-7, 2011.
- [5] 郭環逸，影像驗證碼應用於行動裝置之研究，碩士論文，臺中科技大學多媒體設計系，台中，2015。
- [6] H. S. Baird and J. L. Bentley. Implicit

- CAPTHCAs. SPIE/IS&T Conference on Document Recognition and Retrieval (DRR'05), 2005.
- [7] M. Mehrnejad, A. G. Bafghi and A. Harati, E. Toreini, "SEIMCHA : a new semantic image CAPTCHA using geometric transformations," The ISC International Journal of Information Security, pp.63-76, 2012.
- [8] J. Elson, J. R. Douceur, J. Howell and J. Saul, "Asirra : a CAPTCHA that exploits interest-aligned manual image categorization," In Proceedings of ACM CCS, pp.1-16, 2008.
- [9] 莊凱婷，以 Poker 為圖像驗證碼之設計研究，碩士論文，交通大學應用藝術研究所，新竹，2013。
- [10] 劉晉昇，一個可自動增加驗證圖庫的圖像 CAPTCHA 系統，碩士論文，逢甲大學資訊工程所，台中，2011。

Design and Implementation of Image CAPTCHA

Kai Chain*, Jing-Shiu Huang, Jia-Xuan Wang, Wu-Chuan Yang

Department of Intelligent Network Technology, I-SHOU University

Abstract

In recent years, the ongoing advancements in the information technology industry have provided people with unprecedented convenience, leading to a significant increase in internet usage. Unfortunately, this accessibility has been exploited by some individuals who deploy automated programs, commonly referred to as "bots," for illicit activities online. This misuse, such as generating numerous email accounts to disseminate spam, poses a serious security risk and results in wasteful resource consumption. In the year 2000, Carnegie Mellon University invented the CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) system. This system utilizes computers to distinguish whether users are machines or humans. Initially, the system consisted of arrangements of English letters and numbers, forming a captcha that underwent distortion and deformation. However, with advancements in optical technology, text-based captchas became susceptible to cracking. In recent years, there has been the development of image verification systems. This system involves presenting multiple images in a challenge, requiring users to select specific images to complete the verification process, thereby enhancing its security. This research focuses on designing an image captcha system and validating its practicality through hands-on implementation and user feedback.

Key words : Captcha, Image Captcha, Information Security