



致理科技大學

資訊管理系專題報告

**Cypher Code 圖片加密平台**

**Cypher Code encryption platform**

專題生：

**60810105 吳浩愷**

**60810138 黃子緒**

**60810134 張詠銓**

**60810131 李奕信**

**60810149 馮冠瑋**

**60810129 王睿祺**

**60810150 馮郁婷**

指導教授：黃信博老師

中華民國 112 年 5 月



致  
理  
科  
技  
大  
學

資  
訊  
管  
理  
系

畢  
業  
專  
題

Cypher Code  
圖  
片  
加  
密  
平  
台

—  
—  
學  
年  
度

# 致理科技大學

## 授權書

本授權書所授權之專題報告在致理科技大學

學年度第 學期所撰寫。

**專題名稱：Cypher Code 圖片加密平台**

本人具有著作財產權之論文或專題提要，授予致理科技大學，得重製成電子資料檔後收錄於該單位之網路，並與台灣學術網路及科技網路連線，得不限地域時間與次數以光碟或紙本重製發行。

本人具有著作財產權之論文或專題全文資料，授予教育部指定送繳之圖書館及本人畢業學校圖書館，為學術專題之目的以各種方法重製，或為上述目的再授權他人以各種方法重製，不限時間與地域，惟每人以一份為限。並可為該圖書館館藏之一。

本論文或專題因涉及專利等智慧財產權之申請，請將本論文或專題全文延至民國 年 月 日後再公開。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。

(上述同意與不同意之欄位若未勾選，本人同意視同授權)

同意 不同意

**學生簽名：**

(親筆正楷簽名)

指導老師姓名：

(親筆正楷簽名)

中華民國 年 月 日



# 摘要

專題報告名稱：Cypher Code 加密平台

頁數：34

校系別：致理科技大學資訊管理系

完成時間：111 學年度第 1 學期

專題生：吳浩愷、黃子緒、李奕信、張詠笙、王睿祺、馮冠璋、馮郁婷

指導教授：黃信博

本專題利用 AES 加密算法、LSB 演算方式、LSB 匹配的關係數據庫可逆隱藏技術、JAVA Spring Boot 架構、AES 訊息加密算法+LSB 演算技術以上技術做圖片加密。

首先我們先建置 JAVA Spring Boot 架構的一個環境，在裡面有 AES 訊息加密算法+LSB 演算技術進行圖片加密，利用了 AES 加密算法、LSB 演算方式加密解密的動作，讓使用者能在這個此環境上傳的作品在著作權上獲得足夠的保障。

關鍵詞：AES 加密算法、LSB 演算方式、LSB 匹配的關係數據庫可逆隱藏技術、JAVA Spring Boot 架構、AES 訊息加密算法+LSB 演算技術

# ABSTRACT

Thesis Title: Cypher Code encryption platform

Pages : thirty-four

University : Chihlee University of Technology

Graduate School : Department of Information Management

Date : November , 2022

Degree : Finish

Researcher : Wu Haokai 、 Huang Zixu 、 Yixin Lee 、 Zhang Yongquan 、 Wang Ruiqi 、  
Feng Guanwei 、 Feng Yuting

Advisor : Huang Xinbo

This study uses AES encryption algorithm, LSB calculus method, LSB matching relational database reversible hiding technology, JAVA Spring Boot architecture, AES message encryption algorithm + LSB calculus technology for image encryption.

First of all, we first build an environment of JAVA Spring Boot architecture, in which there are AES message encryption algorithm + LSB algorithm technology for image encryption, using AES encryption algorithm, LSB algorithm method to encrypt and decrypt actions, so that users can use this environment in this environment. The uploaded works have sufficient protection in copyright.

Keywords : AES encryption algorithm 、 LSB calculation method 、 Reversible Hiding Technology for Relational Databases with LSB Matching 、 JAVA Spring Boot Architecture 、 AES message encryption algorithm + LSB calculation technology

## 誌謝

在完成這篇論文的過程中，我們要感謝許多人對我們的協助和支持。首先，我們要感謝我們的指導教授黃信博。他/她不僅在整個研究過程中提供了寶貴的指導和建議，也給我們提供了一個良好的環境和平台，讓我們能夠順利地進行研究和寫作。

我們也要感謝所有參與這個研究項目的同事和夥伴，包括吳浩愷、黃子緒、張詠筌、李奕信、馮冠璋、王睿祺、馮郁婷。他們在整個研究過程中付出了大量的時間和精力，提供了寶貴的意見和建議，並協助我們克服了许多困難和挑戰。

最後，我們要感謝所有支持我們的家人和朋友們。他們總是在我們需要的時候給予了無盡的關愛和支持，讓我們能夠堅定地走完整個研究過程，並完成這篇論文。

在這裡，我們再次向以上所有人致以衷心的感謝和敬意，謝謝你們在我們的論文完成的路上給予的支持和鼓勵。

所有組員姓名：吳浩愷、黃子緒、張詠筌、李奕信、馮冠璋、王睿祺、馮郁婷  
謹致

致理科技大學 資訊管理 學士班

中華民國 年 月

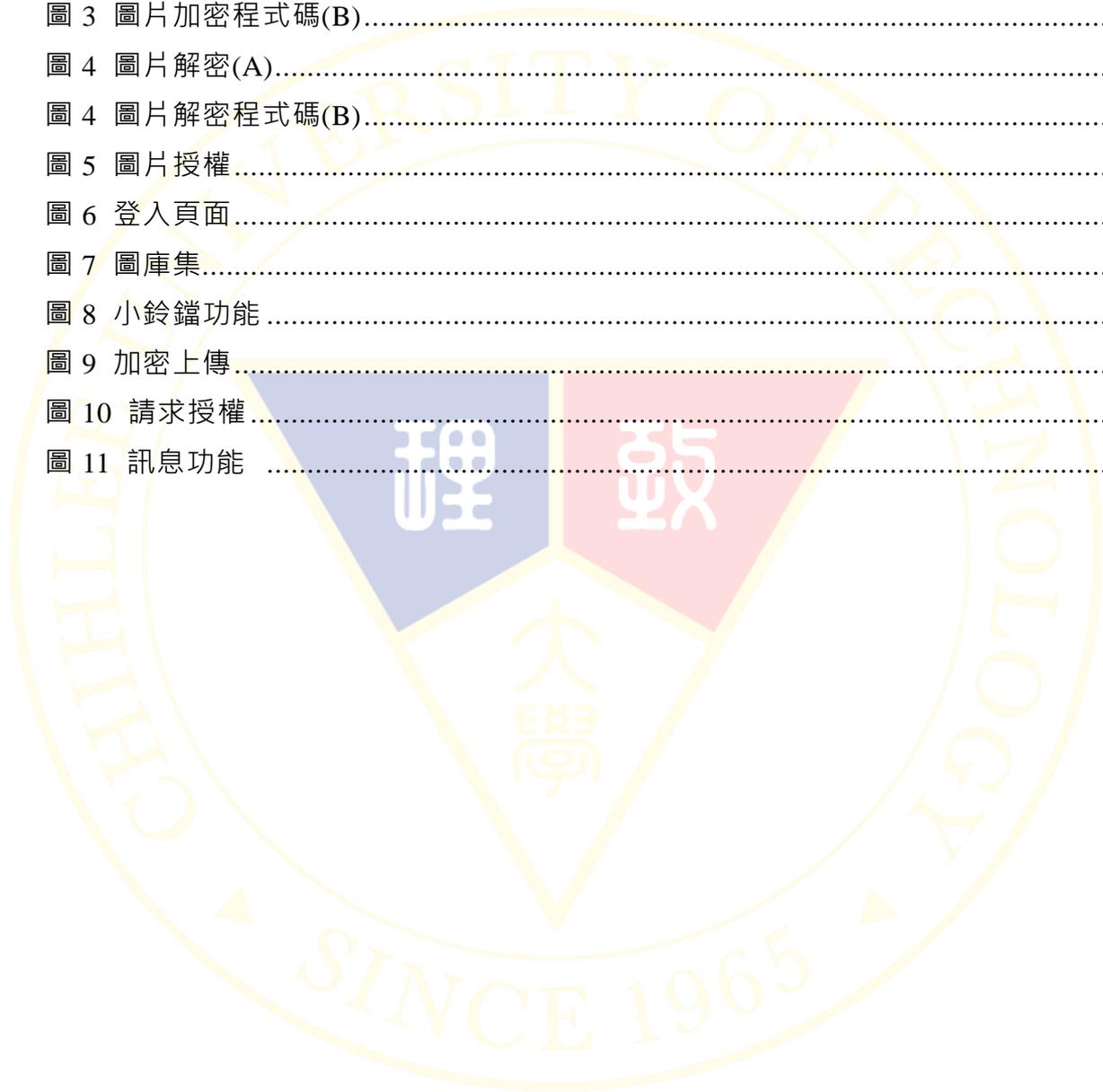
# 目錄

中文摘要 .....	i
ABSTRACT .....	ii
誌謝 .....	iii
目錄 .....	iv
圖目錄 .....	v
第壹章 緒論 .....	1
第一節 專題背景 .....	1
第二節 圖片庫平台的介紹 .....	1
第三節 專題動機及目的 .....	1
第四節 整體架構 .....	1
第貳章 文獻探討 .....	2
第一節 AES 加密算法 .....	2
第二節 LSB 演算方式 .....	2
第三節 LSB 匹配的關係數據庫可逆隱藏技術 .....	2
第四節 JAVA Spring Boot 架構 .....	3
第五節 AES 訊息加密算法+LSB 演算技術 .....	3
第參章 專題內容與方法 .....	5
第肆章 專題結果與設計 .....	7
第伍章 結論與建議 .....	13
第陸章 參考文獻 .....	14
附錄	
附錄一 專題執行計畫表 .....	16
附錄二 專題分配表 .....	17
附錄三 開發工具清單 .....	18
附錄四 需求訪談計畫表 .....	19
附錄五 需求訪談紀錄表 .....	20
附錄六 資料詞彙 .....	21
附錄七 活動圖 .....	27
附錄八 類別圖 .....	28
附錄九 會議記錄 .....	29



# 圖目錄

圖 1 平台結構圖.....	5
圖 2 網站細分圖.....	7
圖 3 圖片加密(A).....	7
圖 3 圖片加密程式碼(B).....	8
圖 4 圖片解密(A).....	8
圖 4 圖片解密程式碼(B).....	8
圖 5 圖片授權.....	9
圖 6 登入頁面.....	9
圖 7 圖庫集.....	10
圖 8 小鈴鐺功能.....	10
圖 9 加密上傳.....	11
圖 10 請求授權.....	11
圖 11 訊息功能.....	12



# 第壹章 緒論

## 1-1 專題背景

目前科技不斷翻新的時代下，越來越多的電子產品及相關硬體設備如桌機、筆電、手機等.....，各種多媒體的訊號如文字、圖片、影片，皆出現了數位化傾向，便廣泛使用，正因如此資訊量流通非常的迅速，如果有重大文件或者機密文件沒有妥善保護好，就容易落入有心人的利用，間接造成使用者的權益受損。

也因如此資訊安全的重要性也漸漸地受到重視，在法律上設立了個人資料保護法保護個子的安全，而科技方面則是有各式各樣的加密演算法用以加密資料，增強資料的安全性。在加密演算法上最主要的效能取決於演算法的複雜度以及執行速度快慢，演算法複雜度越高則文件就會相對的越安全，而執行時間越短則能在相同的時間之下處理越多資料，間接提升加密效率。但越複雜的演算法相對的時間也會較長，所以追求高安全性並且高效能的演算法一直都是資訊安全領域所重視的話題。

在本論文上，為了解決創作者的問題，我們運用 AES 加密算法加 LSB 演算技術幫助創造者進行資料保護，並且聲明說這是創作者的所有物，也能防止第三方非法竊取、擅自分享原作等問題，以保障創作者的權益。

## 1-2 圖片庫平台的介紹

加密圖片庫平台，讓用戶可以傳送自己創作的作品，供給其他人做使用，而使用同時我們也保護用戶專屬的作品，以防自我創作的作品被盜竊等等，有點類似法律所呈現的創用 CC 授權條款，但是用戶跟用戶之間可以有連接，使用加密金鑰互換圖片，在這之間可以只有雙方得知而已，不會讓第三方竊取到此圖的途徑。

## 1-3 專題動機及目的

本專題是製作一個網站平台，讓使用者能在平台上使用（上傳圖片、圖片加密、圖片解密、傳送訊息、授權等）功能，且有開放式圖片庫可以提供此網站會員們之間閱覽，若有需求也可以傳訊息給圖片的所有權者請求授權藉此分享。再來還需要一個後臺管理介面來管理所有使用者及更新資訊。

所以前端畫面主要兩種，第一種是宣傳頁面並提供註冊及登入功能，第二種則是登入後使用者主要操作的管理頁面，後臺的權限部分主要分為兩種權

限，第一種為會員使用者權限，只能使用平台上的功能，第二種為管理者權限，用來管理此平台所有使用者的記錄及更新平台活動資訊內容使用。

為了提高工作效率及分工明確，此專案我們以「JAVA」的開發方式，透過 Spring Boot 架構 MVC 的模式，進行切版畫面、設計模式、流程動線及用戶體驗，後端則利用 Model 層，對數據庫進行存儲和一些業務邏輯上的處理。

#### 1-4 整體架構

在本論文中，我們會在第二、三章介紹我們所使用的方法讓圖文進行加密的動作以及解說，第四章則是呈現我們平台所做的程式展現，第五章是檢討實作過程中的優缺點和結論以及未來展望。



## 第貳章 文獻探討

### (1) AES 加密算法

Advanced Encryption Standard 稱為高級加密於民國 90 年 11 月由美國國家標準與技專題院公布 FIPS PUB 197，經過一年半便成為密碼學標準。[1]由四個步驟組成，SubBytes，ShiftRows，MixColumns 和 AddRoundKey，密鑰大小為 128、192 及 256 位元，取決於需要之安全層級。

在 AES 加密過程中，相同的操作重複 10、12 和 14 次。賦予該算法的密鑰被擴展成長度為 4bytes 的 44、52 或 60 個字元。

首先將沒有加密的文字區塊與初回合金鑰進行 XOR 運算，以產生出相對應的密文，稱之矩陣，接著進行循環式的運算，而在最後一回合省略了 MixColumns 運算，即只執行三個步驟。

每回合加密運算均包含 4 個步驟，第一步驟 SubBytes，是透過一個固定非線性的置換盒(S-BOX)[2]，用查表的方式依序將狀態矩陣中每個元素替換成對應的密文。第二步驟的 ShiftRows，將狀態矩陣中的第  $i$  列做左旋  $i$  位元組， $0 \leq i \leq 3$ 。第三步驟是 MixColumns，這個步驟將狀態矩陣中的每個直行在  $\text{moduloy}8+y4+y3+y+1$  的情況下，和原本固定之的多次項式進行相乘運算。最後一步 AddRoundKey，狀態矩陣中的每一元素都會與該本回合金鑰相對應的位元組做 XOR 運算，從而回合金鑰是經由金鑰擴展程序產生。

由於 AES 加密過程需要 10、12 或 14 回合來加密明文塊，致使其效能不足以滿足 LTE-5G 通信環境的性能要求，此效能不足的缺陷是目前 AES 面臨的首要問題。

在民國 99 年，Orr Dunkelman、Nathan Keller 和 Adi Shamir 提出單鑰攻擊改良法來破解 AES[3]，此法比窮盡搜索更具效率，他們的方法從著名的 Demirci-Selcuk 攻擊中，可以對 7 回合 AES 做到更具效率的破解。由於 AES 使用固定的 S-Box，使得 SubByte 運算輸出的密文呈現線性對應的安全缺陷，因而大大降低 AES 的安全性

### (2) LSB 演算方式

Chan 及 Cheng 學者[4](2004)提出 LSB 藏入法(OPAP)，將機密訊息取代較低位元，達到高藏量及低失真度的資訊隱藏效果。首先將灰階影像中的目標像素轉換成二進制，再從機密訊息串當中取出  $k$  個位元的機密訊息，取代目標像素中後面的  $k$  個位元。例如：目標像素為 110，欲藏入 3 個位元的機密訊息(010)2。

首先，目標像素  $110=(01101110)_2$ ，機密訊息為  $(010)_2$ ，然後將機密訊息取代目標像素的後面 3 個位元，得到偽裝像素值  $106=(01101010)_2$ 。在取出機密訊息的過程中，只要將偽裝像素值轉成二進制並取出最後 3 個位元  $(010)_2$ ，即可得到藏入的機密訊息。

### **(3)LSB 匹配的關係數據庫可逆隱藏技術**

LSB 匹配隱藏法[5-6]的嵌入過程與 LSB 相似，透過替換二進制像素值的最低有效位元來藏入秘密訊息，不過在 LSB 匹配法裡，兩個像素藏入兩個位元時，只需更動到一個位元。以機率來觀察 LSB 對每個像素值的隱藏負擔量是  $1/1$ ，而 LSB 匹配法為  $1/2$ ，可知 LSB 匹配法是可降低原始像素被修改的機率。而用關係數據庫現有的關係型數據庫數據隱藏技術無法在隱藏後恢復原始數據。本文的目的是為關係數據庫提出第一個可逆隱藏技術。在隱藏階段，它通過關係數據庫的 LSB 匹配法將機密訊息隱藏至關係數據庫之中。在提取和恢復階段，它通過關係數據庫的 LSB 和 LSB 匹配方法獲取機密消息。最後，採用平均法恢復原始數據。根據實驗，我們提出的技術滿足數據隱藏要求。它不僅能夠恢復原始數據，而且還保持了很高的遮蓋力。我們算法的複雜性顯示了它們的效率。

### **(4)JAVA Spring Boot 架構**

以 Spring 為核心 Spring Boot[7]只需要用簡化配置就可以直接運行，這樣應用程式可以既簡單的獨立創建並且又有擴展性，而 Spring 提供的第三方函式庫有提供許多的依賴包，也能減少版本衝突問題。

而 Spring Boot 擁有嵌入式 Tomcat 這樣在最後專案打包時就可以直接包成 JAR 檔不用包成 WAR 檔，而 JAR 跟 WAR 的區別在於 Java Archive 檔中是存取專案內的程式碼轉譯而形成的 class 檔案以及專案內所使用的函式庫及所用的靜態資源檔案，而 Web Application Archive 檔則是需要額外包含網頁程式所會用到的資源內容。

### **(5)AES 訊息加密算法+LSB 演算技術**

本專案主軸是利用使用所留下的訊息文字先用 AES 加密進行 Base64 編碼轉換成二進制數據最後再利用 LSB (最低有效位) 將訊息編碼到圖片中。

在 JAVA Spring 的裡面中包含著可以運用在圖像加密的兩個程式碼 AES、LSB 以下會講解如何在圖像加密的部分細說:

AES 區塊加密演算法是由 128 位元進行運算，密鑰會區分 AES-128、

AES-192、AES-256，是使用還沒使用過的加密區塊重複執行進行回合加密則會根據密鑰長度決定會經由以下加密過程四步驟。

1.SubBytes—是利用 S-box 去做替換函式，而 S-box 是個經過設計且能提供非線性的變換，能將區塊內位元替換成對應的元組。

2.ShiftRows—主要是在做位移資料，將數據進行循環位移區塊的動作。

3.MixColumns—是以每行為一個向量通過另一個 4X4 之矩陣做相乘與該回合的運算，乘法用  $GF(2^8)$  算法實現，這樣最後這些數字不管如何計算都會落在  $2^8$  之內。

4.AddRoundKey—將上面所有資料都跟回合密鑰做 XOR 運算，輸出的結果再按列跟原區塊中的狀態位原做互斥加法得到最終結果。至於 AES 有相當致命的弱點就是對於旁道攻擊以及社會工程學攻擊沒辦法預防，因為在定位址系統產生的加密演算法雖然是最佳化，但是產生的表格會因為 XOR 運算時，如有平台記憶體不足時會再進行一次運算時，就會在這當下從而變成旁道攻擊的最佳可能。

結合了 LSB 演算是最底的有效位元隱藏方法是在空間中寫入資料的一種技術[8]，即在原圖中寫入資料於每一個像素中，以此達到寫入秘密資訊於浮水印的目的，並會使影像變化不輕易被肉眼所察覺。首先記錄原圖中每一像素之灰階值，其中灰階值所對應的十進位制值範圍是於 0 到 255 之間，再將其轉換為長度 8 位元且只含 0 和 1 的二進位序列，然後在其取一組是數字又或者是文字的密文，但此內容則依照 ASCII 做對應形成一組二進制位列序，此二進位中抓取 n 個位元隱藏到每單位之中。而寫入方法就是每 8 位元灰階的最後 n 位元是用二進位序列每個 n 位元來做取代，直至所有密文內容皆藏於該圖中。然後接收端在取出密文時，只需要把收到之影像單位畫素值傳回二進位制，接續 pop 出每單位畫素中，導致較後的 n 位元，透過 ASCII 碼解碼完畢，即可變成原密文之資料。

## 第參章 專題內容與方法

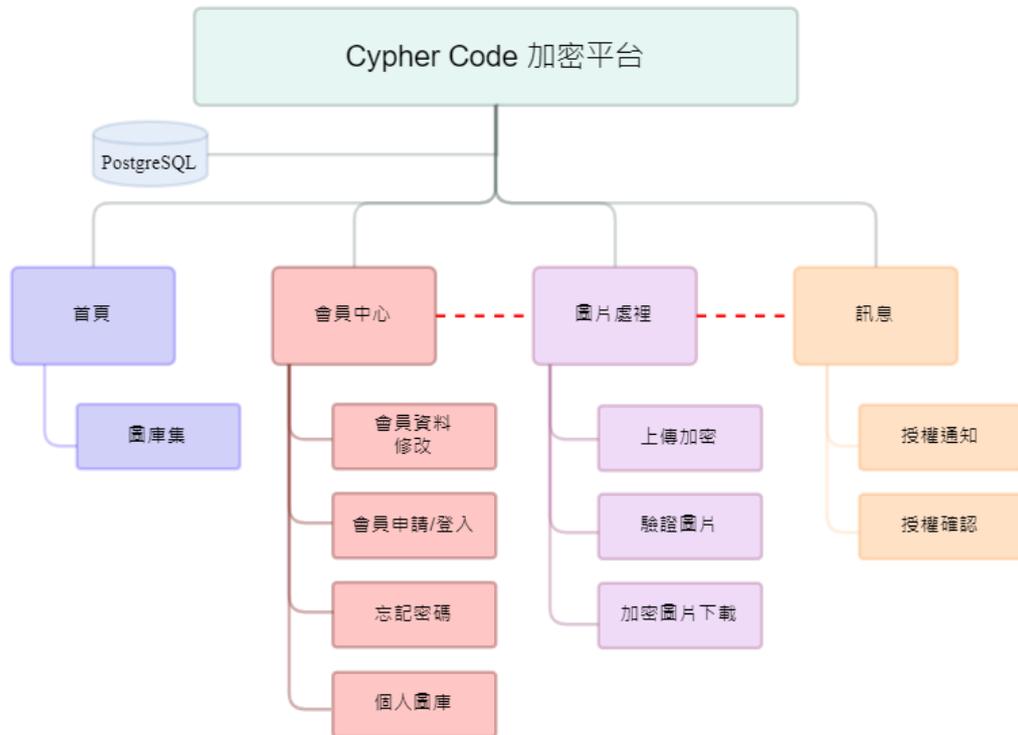


圖 1 平台結構圖

本專題使用 MPA (Multi-Page Application)開發方式：

MPA (Multi-Page Application)一般傳統的 Web Front-End 開發方式，有多少頁面就製作多少 HTML 檔案，每當網站點去另一頁時，網頁瀏覽器會將 CSS、Javascript 網站資源等所有東西，重新刷新讓你讀取新頁面。

優點：

對於 SEO 友好：

瀏覽器的網站爬蟲可以方便讀取你的網站內容，好讓瀏覽器網站分析合適的搜尋結果推薦給消費者，這樣你的網站可以更有機會獲取免費 SEO 流量。開發門檻低。

隨然現主流開方式是 SPA，但是不是所有人都會使用前端框架，所以在開發上使用傳統 MPA 進行開發，容易學習及維護上方便。

前端使用 HTML、CSS 及 Bootstrap 5 框架開發 RWD，後端使用 JAVA 透過 Spring Boot MVC 架構的模式開發。平台系統功能，有七個子系統，分別為：(1)

圖片庫(2)上傳圖片(3)圖片加密(4)圖片解密(5)傳送訊息(6)授權(7)會員中心。

加解密部分首先我們使用與 AESCrypt-ObjC 和 AESCrypt Ruby 兼容的 AES-256 位加密來加密和解密消息。而美國人之公務部門啟用來取代 DES 方法為新穎之加密方法，而 DES 為一種秘密金鑰加密方法，明文以及密文皆為 64 位元，但由於科技進步密碼技術及電腦硬體提升，使得 DES 的安全性產生出嚴重的漏洞。在民國 86 年於國家標準暨技術專題院曾公開徵集更高效與安全的替代 DES 加密演算法，其中有 5 種演算法入圍了決賽，經過 3 年的驗證 AES 演算法最終入選。AES 加密演算法的明文與密文長度皆為 128 位元，金鑰長度可為 128、192 或 256 位元，金鑰演算長度為 128 位元稱為 AES-128，金鑰演算長度為 192 位元稱為 AES-192，金鑰演算長度為 256 位元稱為 AES-256，金鑰長度會影響重複執行加解密的回合運算，回合運算各 10、12、14 次數，當加解密回合運算次數越多，其安全性更高，但是加解密需要的時間更長。AES 加密演算法操作在蓋羅瓦理論[9]中的蓋羅瓦(Galois Field, GF)，它係指有限元素的集合，在這個集合內可執行加、減、乘等運算。在 AES 加密演算法中使用  $GF(2^8)$  有限場的加法和乘法算，達到線性組合的編碼。有限場會因為乘法，使運算結果超出有限場  $GF(2^8)$ ，而運算超出有限場時會模除多項式，取其餘式，稱為 xtime 運算。

AES 也可以是一種可逆的加密算法，對用戶的極度敏感的訊息加密處理將 AES 密鑰和數據保存到圖像中。並針對初始訊息進行 AES 加密演算後，在執行 Base64 的編碼進行轉化動作。使用 256 位 AES 和從密碼生成的密鑰對消息進行加密和編碼然後從圖像中獲取訊息 String text 獲取訊息獲取圖像後解碼，指定圖像中獲取隱藏訊息(BufferedImage 物件的 image)

從圖像中獲取解碼文本，@param password aes secret key.AES 密鑰，@param imagePath image path.圖片路徑@return origin text.獲取訊息後再回傳訊息。

使用保存在圖像中的密碼從圖像中獲取訊息，解密要找出加密時所輸入的特殊符號"|"取出索引值，利用索引值位置取出 password 字串，再利用索引值位置取出訊息後回傳訊息。

而從圖像獲取訊息和路徑，進行圖像長度的演算解碼，像

BufferedImage image = Utils.streamToImage(inputStream);獲取圖像

final int imageLength = image.getHeight() \* image.getWidth();圖像的長度

final int startingOffset = Utils.calculateStartingOffset(null,imageLength);計算

return steganography.decode(image,startingOffset);解碼

在進行回傳訊息的動作。

然後生成用作密鑰的密碼的 SHA-256 hash 通過 final MessageDigest digest = MessageDigest.getInstance(HASH\_ALGORITHM);拿到一個 MD5 轉換器

此 MessageDigest[10]為提供消息摘要的應用程序演算，如本專題使用的 SHA-256。而消息摘要是一種安全且單向散列函數，它採用的數據則是隨意不拘大小並輸出長度固定的散列值。

MessageDigest 使對象進行初始化。可以透過使 updat 來更新數據。不管發生甚麼樣的錯誤都能使用 reset 來重置摘要。一旦全部的數據都更新完畢，就 digest 調用其中一種方法來完成散列計算。

該 digest 方法可以針對給定數量的更新調整一次。在 digest 被調整後，MessageDigest 對象就會被重置為起始化狀態。皆可以實現 Cloneable 接口。

## 第肆章 專題結果與設計

本專題先透過圖 2 去做規劃以下程序:首先進入網站後，有兩個選項，第一個是本就是會員，第二個是新註冊會員；如原本是會員輸入帳號密碼即可登入，但如果忘記密碼就必須輸入先前設定的帳號以及信箱去做找回密碼的動作；而新註冊會員則是輸入帳號密碼以及信箱和電話號碼來做儲存登入，即可進入首頁。

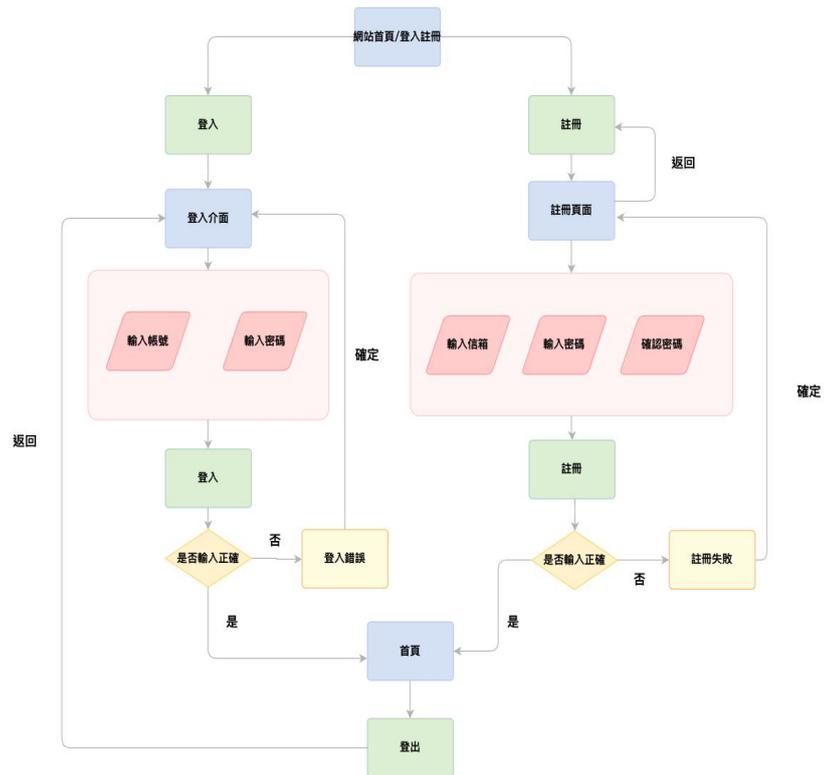
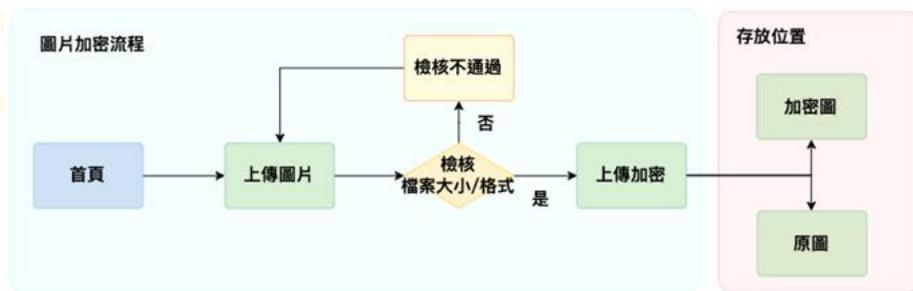


圖 2 網站細分圖

進入首頁後的客戶可以，進行網站的應用，開始創作自我的作品，創作完的作品可以進行上傳圖片動作，系統會檢測出照片的檔案大小以及格式等細部檢查，如果不通過會跳過通知告知客戶需要哪些地方進行修改，才能繼續上傳動作，如上傳成功會跳出如圖 3 這個畫面是否要對作品進行加密動作如圖 4，進行完成後會產出兩種圖檔，原畫質圖檔以及加密圖檔。



(A)

```

155 StringBuilder output = new StringBuilder();
156 for (int i = 0; i < input.length(); i++) {
157     output.append((char) (input.charAt(i) ^ key[i % key.length]));
158 }
159 System.out.println("EncryptService.encryptDecrypt加密解密結果: " + output.toString());
160 return output.toString();
161 }
162
163 public static void main(String[] args) throws GeneralSecurityException {
164     /* 加密所需參數 */
165     String msg = "Test標題內容"; // 要隱藏的內容
166     String userEncrypt = "ellenEncrypt123"; // 使用者加密金鑰
167     String userDecrypt = "ellenDecrypt123"; // 使用者解密金鑰
168     String imagePath = "C:\\Users\\ellen\\Desktop\\test.png"; // 圖片路徑
169     boolean isSuccess = toImgAESWithPW(msg, userEncrypt, imagePath, userDecrypt);
170     System.out.println("加密結果: " + isSuccess);
171 }
172
173 }
174
175

```

```

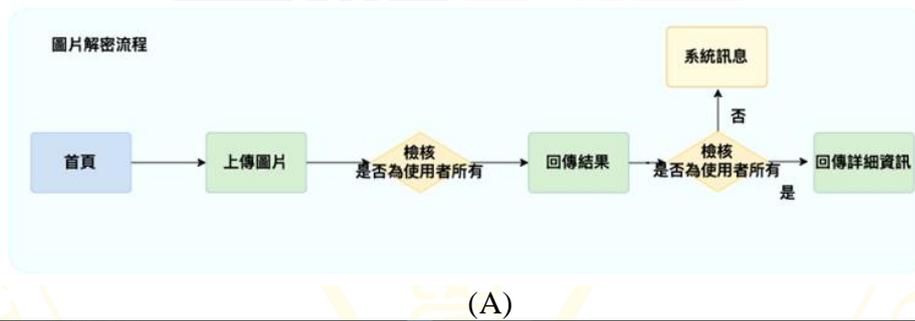
EncryptService.toImgAESWithPW 所接收的參數 msg: Test標題內容 imagePath: C:\Users\ellen\Desktop\test.png userDecrypt: ellenDecrypt123
AesCrypt.encrypt AES加密訊息結果: CCMpHh6SL1P7GCPSP2s1QuD7XkPF8X181bPUCrdDg=
EncryptService.encryptDecrypt 所接收的參數 input: ellenEncrypt123|CCMHh6WSL1P7GCPSP2s1QuD7XkPF8X181bPUCrdDg=
Steganography.encode.addText msg: [86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~
EncryptService.toImg 所接收的參數 msg: +)86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~ imagePath: C:\Users\ellen\Desktop\test.png userDecrypt: ellenDecrypt123
EncryptService.toImg 找到實體檔案
Utils.calculateStartingOffset 所接收的參數 password: ellenDecrypt123 maxValue: 16384
Utils.calculateStartingOffset 提取字串的索引: 1489
Steganography.encode.addText msg: [86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~
EncryptService.fromImgAESWithPW 訊息: +)86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~
EncryptService.encryptDecrypt 所接收的參數 input: +)86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~
EncryptService.encryptDecrypt 加密解密結果: ellenEncrypt123|CCMHh6WSL1P7GCPSP2s1QuD7XkPF8X181bPUCrdDg=
EncryptService.encryptDecrypt 利用 "" 取出索引值前使用者解密金鑰: ellenDecrypt123
EncryptService.encryptDecrypt 利用 "" 取出包含索引值後的訊息: |CCMHh6WSL1P7GCPSP2s1QuD7XkPF8X181bPUCrdDg=
AesCrypt.decrypt AES解密訊息結果 (編碼轉換UTF8): Test標題內容
解密結果: Test標題內容

```

(B)

圖 3 (A) 圖片加密流程 (B) 圖片加密程式碼

相反的有加密就有解密的動作，一樣進入首頁到上傳圖片的位置，檢核是否為使用者所有的動作後，如是就會回傳詳細資訊，如不是就會跳出畫面如圖 4 圖 5。



(A)

```

167 String msg = "Test標題內容"; // 要隱藏的內容
168 String userEncrypt = "ellenEncrypt123"; // 使用者加密金鑰
169 String userDecrypt = "ellenDecrypt123"; // 使用者解密金鑰
170 String imagePath = "C:\\Users\\ellen\\Desktop\\test.png"; // 圖片路徑
171 String text = fromImgAESWithPW(imagePath, userDecrypt); // 提取內容
172 System.out.println("解密結果: " + text);
173 }
174
175

```

```

EncryptService.fromImgAESWithPW 所接收的參數 imagePath: C:\Users\ellen\Desktop\test.png userDecrypt: ellenDecrypt123
EncryptService.fromImg 所接收的參數 imagePath: C:\Users\ellen\Desktop\test.png userDecrypt: ellenDecrypt123
Utils.calculateStartingOffset 所接收的參數 password: ellenDecrypt123 maxValue: 16384
Utils.calculateStartingOffset 提取字串的索引: 1489
Steganography.decode 訊息結果: +)86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~
EncryptService.fromImgAESWithPW 訊息: +)86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~
EncryptService.encryptDecrypt 所接收的參數 input: +)86+2k*875 bwp7
865~u|8"3c000-8f=)8&lt;8"8( :u/)00
702~
EncryptService.encryptDecrypt 加密解密結果: ellenEncrypt123|CCMHh6WSL1P7GCPSP2s1QuD7XkPF8X181bPUCrdDg=
EncryptService.encryptDecrypt 利用 "" 取出索引值前使用者解密金鑰: ellenDecrypt123
EncryptService.encryptDecrypt 利用 "" 取出包含索引值後的訊息: |CCMHh6WSL1P7GCPSP2s1QuD7XkPF8X181bPUCrdDg=
AesCrypt.decrypt AES解密訊息結果 (編碼轉換UTF8): Test標題內容
解密結果: Test標題內容

```

(B)

圖 4 (A) 圖片解密流程 (B) 圖片解密程式碼

當客戶進入自己的圖庫集時，可以請求授權並且發送訊息給所有客戶，如所有的客戶同意就便可同意下載，但如有一人不同意，此創作品不能提供給其他客戶，如圖 5。

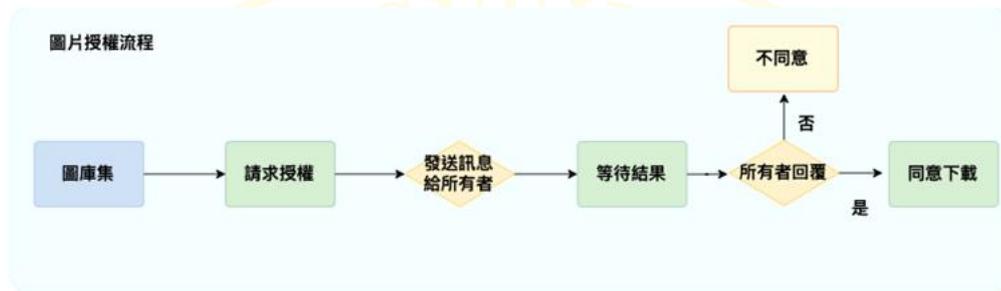


圖 5 圖片授權

### 系統展示

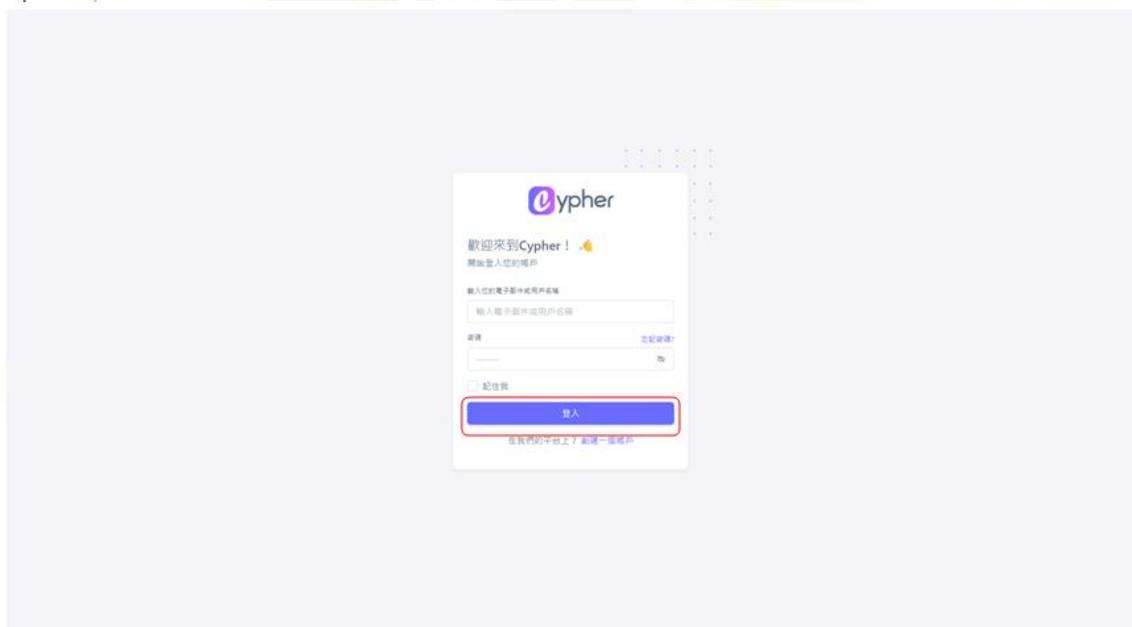


圖 6 登入頁面

登入頁-可以用電子郵件或者用戶名稱來進行登入動作。

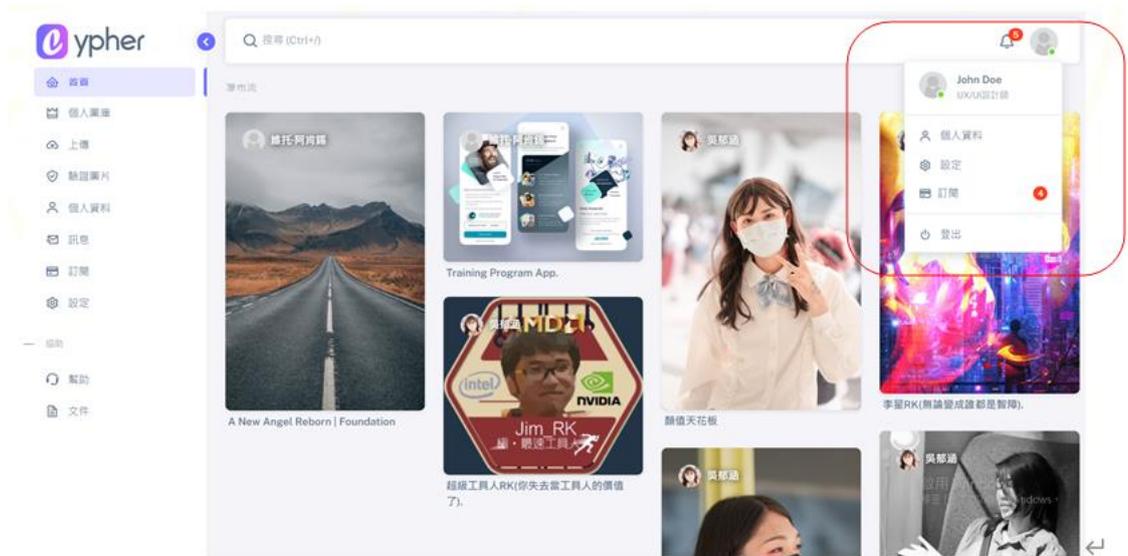


圖 7 圖庫集

首頁-首頁內容為圖庫集，是放置會員們已上傳並且選擇公開的圖片讓會員們進行分享左邊為目錄選單-目錄選單為此平台所有功能集。

右上角為會員功能-會員目錄能看見此會員的頭像及用戶名稱，以及能所能登出或修改的功能項目。

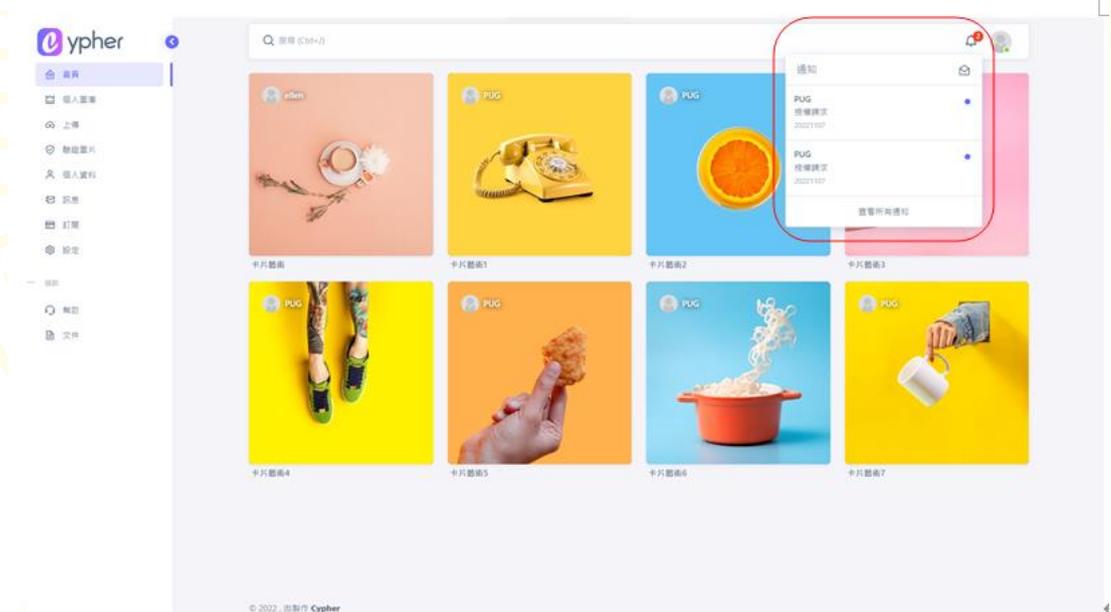


圖 8 小鈴鐺功能

小鈴鐺-能呈現目前會員所未讀的訊息內容，點擊查看所有通知畫面便會導向訊息頁。

例：私人訊息、授權訊息、系統訊息。



圖 9 加密上傳

加密上傳-點擊或拖拉圖片至框內可顯示要上傳的圖片，下方輸入標題填選位置及點擊是否願意公開圖片，點擊上傳便可以進行上傳及加密動作，最後成功或失敗會跳出視窗顯示訊息。

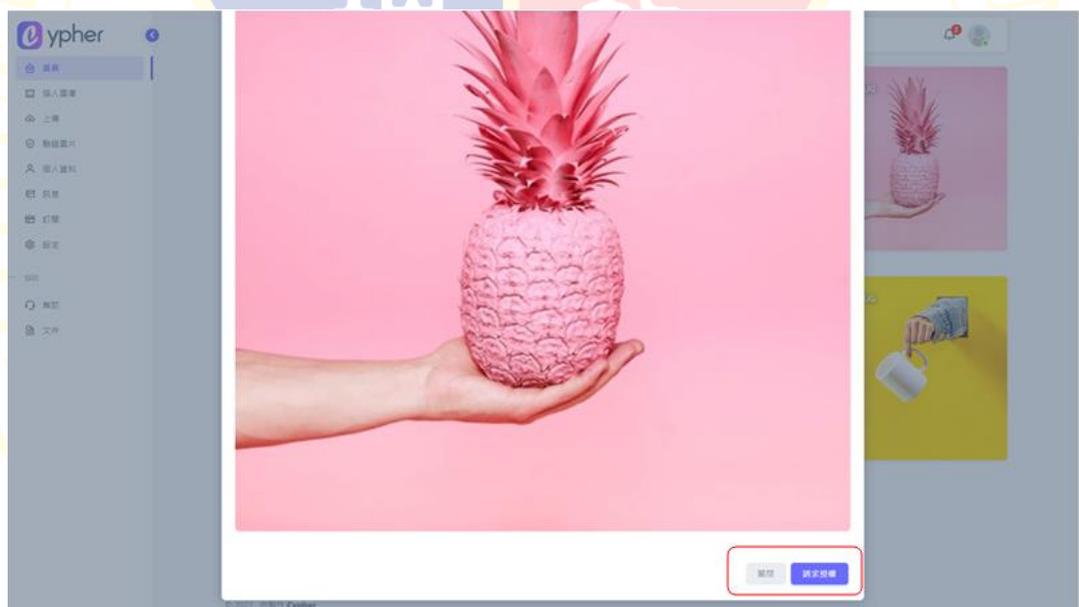


圖 10 請求授權

請求授權-在首頁圖庫及部分點擊每張圖時都會彈跳出視窗放大，如果不是自己的圖片便可在右下角看見請求授權按鈕，點擊請求授權便可發送訊息給圖片所有者的會員請求同意。

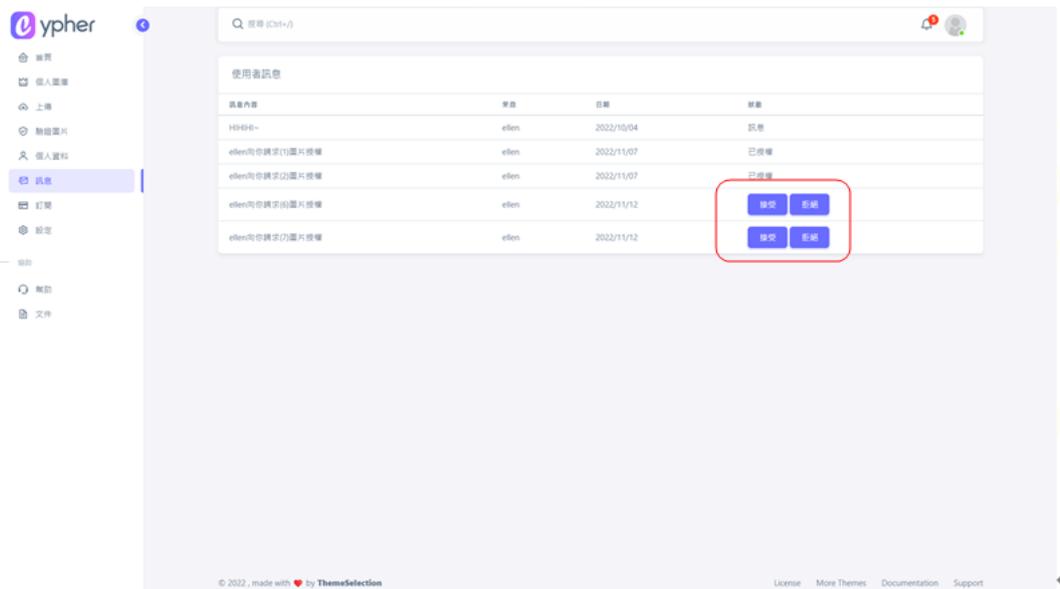


圖 11 訊息功能

訊息功能-此頁為所有訊息展示，裡面可以看見此會員所有的訊息內容，如果是請求授權也可以在訊息頁選擇接受或拒絕，點擊後畫面會自動刷新更新資訊。



## 第五章 結論與建議

### 一、結論

本專題依據研究目的，探討了圖片著作者在智慧財產權的保護以及如何避免私自盜用於未經許可的營利使用上遇見的困難，我們分析了現有社群媒體在相關問題上遇到的弊端，希望加強著作者維護自己的相關權益相關功能，從而開發出本網頁，本專題現階段完成首頁、圖庫集、訊息頁、通知、圖片加密與圖片解密模組的規劃與開發，且進入測試階段，後續擬將剩餘功能完成來達到平台的完整度。

本專題認為所做目前的程式圖片加密無法讓客戶明顯感受到其差異之別，未來希望能夠加強圖片作者的相關權益及網頁的使用流程優化。

根據我們分析現有社群媒體後我們推出：

1. 圖片加密模組
2. 圖片解密模組
3. 圖片的公開與否相關功能

### 二、研究限制及建議

受到現今網路媒體的影響，本專題原先希望能夠依據現網路使用者之使用體驗為目的，而想跟進現今較為流行的訂閱制付費會員的股本與一般使用者作區別，但礙於技術方面以及有金錢上面的相關議題，目前的我們還缺乏在後續製作及完善的相關知識及技術如強硬的塞入恐會造成用戶在使用和管理的不方便性以及本社群網站的安全憂慮，最終本專題暫時捨棄相關的功能從而完善個使用功能。

## 第陸章 參考文獻

- [1] 該演算法為比利時密碼學家 Joan Daemen 和 Vincent Rijmen 所設計，結合兩位作者的名字，以 Rijndael 為名投稿進階加密標準的甄選流程。
- [2] .Federal Information Processing Standards Publication 197, 2001; Barkan and Biham, 2002.
- [3].O. Dunkelman , N. Keller, and A. Shamir “Improved single-key attacks on 8-round AES-192 and AES-256”, pp. 6-24,2010
- [4]C.K. Chan and L.M. Cheng , “Hiding data in images by simple LSB substitution ,” Pattern Recognition , Vol. 37 , Issue 3 , pp.469-474 , 2004.
- [5] J. Mielikainen , “LSB matching revisited ,” IEEE Signal Processing Letters , Vol. 13 , No. 5 , pp. 285-287 , 2006.
- [6] A. D. Ker , “Improved detection of LSB steganography in grayscale images ,” In Proc. Information Hiding Workshop , Vol. 3200 , Springer LNCS , pp. 97-115 , 2004.
- [7] Spring 系列專案於 2003 年啟動，以因應早期 JAVA 開發的複雜性，並提供開發 JAVA 應用程式的支援。
- [8]Z. Wang , C. F. Lin and J. C. Lin , “Image hiding by Optimal LSB substitution and genetic algorithm ,” Pattern Recognit. , vol.34 , no.3 , pp.671-683 , 2000.
- [9] 資料來源:維基百科，網址: <https://reurl.cc/GXpR5G>
- [10] Java™ Platform , Standard Edition 8 API Specification

畢業專題 系統操作手冊

【放置附錄】



**附錄一【專題執行計畫表】**

<b>組名</b>	蛋頭吐司		
<b>組員</b>	<b>班 級</b>	<b>學 號</b>	<b>姓 名</b>
	夜資四 A	60810105	吳浩愷
	夜資四 A	60810138	黃子緒
	夜資四 A	60810131	李奕信
	夜資四 A	60810134	張詠笙
	夜資四 A	60810127	王睿祺
	夜資四 A	60810148	馮郁婷
	夜資四 A	60810149	馮冠璋
<b>專題名稱</b>	<b>Cypher Code 加密平台</b>		
<p><b>專題資訊系統功能描述</b></p> <p>現在科技發達的時代，資訊流通非常便捷，手機、電腦、line、臉書等應用程式都可以隨意截圖或是下載，導致版權意識低落。</p> <p>儘管到了 2022 年，情況雖然有所改善，但還是不夠，下載、截圖沒標註原作者、發佈時間等等對於原創的版權保護無法做到很完善，就算一開始有註明，但經過一次次的傳播，不再有人在乎到底誰才是創作者。</p> <p>不管是圖片還是影片、粉絲專頁都有人盜用他人作品，甚至流量更勝原創，這是對於創作者非常不公平的事。</p> <p>創作者想抓也抓不完，抓了一個還有幾百個，也浪費時間與金錢。</p> <p>雖然說有著作權法上的保護但並不完善，因此我們想架設一個網站讓創作者在這裡的作品能得到保護，不管是截圖、下載都可以讓創作者追蹤到盜用者，這不僅僅是保護創作者也是在提升人們的版權意識，讓社會更進一步。</p>			
<b>指導老師簽名</b>	黃信博	<b>日期</b>	111 年 1 月 20 日
<b>備註</b>			

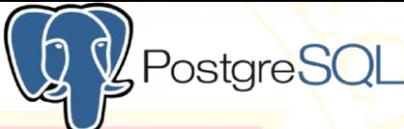
## 附錄二【專題工作分配表】

組名	蛋頭吐司	填寫人	李奕信					
專題名稱	Cypher Code 加密平台	填寫日期	111 年 2 月 20 日					
主要編號	主要與次要工作項目	主要成員姓名				機動成員姓名		
		吳浩愷	張詠笙	李奕信	黃子緒	馮冠璋	王睿祺	馮郁婷
01	蒐集需求		v	v				
02	分析需求		v	v				
03	平台流程規劃	v			v			
04	程式撰寫	v			v			
05	建置環境	v			v			
06	資料庫設計				v			
07	文書撰寫			v			v	v
08	簡報製作					v	v	

活動	計劃開始時間	計劃持續時間	實際開始時間	實際持續時間	期間	圖例	
						% 完成	% 完成 (超出計劃)
					1	計劃持續時間	實際開始時間
						實際 (超出計劃)	
蒐集需求	1	3	1	3	1-3	100%	100%
分析需求	2	4	2	4	2-4	100%	100%
平台流程規劃	3	2	3	2	3-4	100%	100%
程式撰寫	4	3	4	6	4-6	100%	100%
建置環境	4	3	4	6	4-6	100%	100%
資料庫設計	4	3	4	6	4-6	100%	100%
文書撰寫	7	2	9	2	7-9	100%	100%
簡報製作	11	1	11	1	11-11	100%	100%

· 附錄三【開發工具清單】

組名	蛋頭吐司	填寫人	黃子緒
專題名稱	Cypher Code 加密平台	填寫日期	111 年 3 月 27 日
工具名稱	解說	LOGO 圖像	
Eclipse 2022-06	JAVA 後端開發所使用的 IDE		
Visual Studio Code	前端畫面所使用的編輯器		
PostgreSQL	資料庫		
Maven	套件管理		
Git	版本控制		
Bitbucket	版本庫代管平台		
Bootstrap 5	快速設計及自訂響應式網站		
Jquery	JavaScript 的所有函式庫中，簡化與 HTML 間的許多操作步驟		
JavaScript	開發人員用來建立互動式網頁的程式設計語言		
HTML5	可以說 HTML5 廣義包括 CSS、JavaScript 和 HTML 三內容		
CSS	畫面樣式語言		

### 附錄四【需求訪談計畫表】

<b>組名</b>	蛋頭吐司	<b>填寫人</b>	王睿祺
<b>專 題 名稱</b>	Cypher Code 加密平台	<b>填寫日期</b>	111 年 4 月 12 日
<ol style="list-style-type: none"> <li>1. 客戶面臨的問題是什麼?</li> <li>2. 客戶期望達成的目標?</li> <li>3. 是否付費購買圖片庫容量?</li> <li>4. 客戶聽過敘述後覺得哪邊需要改善?</li> <li>5. 客戶願意在此平台更新的頻率?</li> <li>6. 客戶是否能接受訂閱制?</li> <li>7. 客戶是否能同意跟臉書、google 等平台連接帳號?</li> <li>8. 客戶是否希望有行動版，為什麼?</li> </ol>			

附錄五【需求訪談紀錄表】

組名	蛋頭吐司	填寫人	馮冠璋
專 題 名稱	Cypher Code 加密平台	填寫日期	111 年 4 月 20 日



### **1. 客戶面臨的問題是什麼?**

許多創作在不知情的狀況下被他人盜用私自拿去使用，當成自己的作品或是變成商品販賣，使客戶失去原本應有的權利及收入。

### **2. 客戶期望達成的目標?**

不僅僅是只有保障客戶一人，而是要讓整個創作圈都能受到保護及改善人們的版權意識。

### **3. 是否付費購買圖片庫容量?**

客戶認為平台成效好，自然願意付費買更多空間，而價格合理下最好的方式當然是一次買斷，不過客戶也表示可接受訂閱式方案。

### **4. 客戶聽過敘述後覺得哪邊需要改善?**

客戶希望他在別的地方(像 pixiv)的既有的創作可以同步在此平台，不用重新發佈

因為創作很多一個一個重新發佈也很累。

### **5. 客戶願意在此平台更新的頻率?**

客戶表示自己主要是靠接案繪畫維生，若單純產圖更新作品不做商業使用的話，其實是沒辦法有太多的心思能顧及自己創作品的流向，如果此平台可以讓我直接接洽客戶，在平台上能操作購買、匯款、顯示接案量等商業功能，或許能達到定期三日更新。

### **6. 客戶是否能接受訂閱制?**

客戶表示平台流量好、績效佳，就能接受訂閱制，因為現在很多平台也都使用訂閱制，因此不是這麼難以接受。

### **7. 客戶是否能同意跟臉書、google 等平台連接帳號?**

客戶表示可以連接獲同步當然是最好，這樣也不用重新設定很多東西，也不用在記帳號密碼，如果可以同步更佳，就不用重新發文，也希望在一個平台可以同時發文，像臉書跟 IG 一樣。

### **8. 客戶是否希望有行動版，為什麼?**

客戶表示現在每人一台手機，方便又即時，可以隨時發文回訊息，不用受時間地點的限制，所以一定是希望有行動版，但也表示如果沒把握行動版的品質那就不要。

· · 附錄六【資料詞彙】

組名	蛋頭吐司			填寫人	張詠笙		
專 題 名稱	Cypher Code 加密平台			填寫日期	111 年 5 月 2 日		

	A	B	C	D	E	F	G
1	欄位名稱	欄位類型	長度	預設值	允許NULL	說明	備註
2	ROWID	BIGINT	null	X	N	Key	
3	USRID	NVARCHAR	10	X	N	帳號	
4	USRNM	NVARCHAR	10	X	N	使用者名稱	
5	NICKNM	NVARCHAR	10	X	Y	暱稱	
6	ENCRYPT	NVARCHAR	8	X	N	加密	
7	DECRYPT	NVARCHAR	8	X	N	解密	
8	ID	NVARCHAR	2	X	N	權限	
9	PWD	NVARCHAR		X	N		
10	EMAIL	NVARCHAR		X	N		
11							

Query Query History

1 select \* from users

Data output Messages Notifications

	rowid [PK] bigint	usrid character varying	usrnm character varying	nicknm character varying	encrypt character varying	decrypt character varying	id character varying	pwd character varying	email character varying
1	1	ellen	EllenHuang	PUG	[null]	[null]	M	AAA	[null]
2	3	PUG	天天利	nicknm	[null]	[null]	Y	AAA	[null]

【資料詞彙】

組名	蛋頭吐司			填寫人	張詠荃		
專題名稱	Cypher Code 加密平台			填寫日期	111年5月15日		

	A	B	C	D	E	F	G
1	欄位名稱	欄位類型	長度	預設值	允許NULL	說明	備註
2	ROWID	BIGINT	null	X	N	Key	
3	USRID	NVARCHAR	10	X	N	帳號	
4	TITLE	NVARCHAR	20	X	N	標題	
5	PICNAME	NVARCHAR	100	X	N	圖片名稱	
6	OVERT	NVARCHAR	1	X	N	公開	Y=公開 N=非公開
7	ADDDATE	NVARCHAR	12	X	N	新增日期	
8	ID	NVARCHAR	2	X	N	權限	
9	RMK	NVARCHAR	100	X	Y	備註訊息	
10	FILEPH	NVARCHAR		X	N	路徑	
11							

Query Query History

1 select \* from gallery

Data output Messages Notifications

	rowid [PK] bigint	userid character varying	title character varying	picname character varying	overt character varying	addate character varying	id character varying	rmk character varying	fileph character varying
1	1	ellen	卡片藝術	11	Y	[null]	[null]	[null]	/resources/GALL...
2	2	PUG	卡片藝術1	1	Y	[null]	[null]	[null]	/resources/GALL...
3	3	PUG	卡片藝術2	2	Y	[null]	[null]	[null]	/resources/GALL...
4	4	PUG	卡片藝術3	3	Y	[null]	[null]	[null]	/resources/GALL...
5	5	PUG	卡片藝術4	4	Y	[null]	[null]	[null]	/resources/GALL...
6	6	PUG	卡片藝術5	6	Y	[null]	[null]	[null]	/resources/GALL...
7	7	PUG	卡片藝術6	7	Y	[null]	[null]	[null]	/resources/GALL...
8	8	PUG	卡片藝術7	8	Y	[null]	[null]	[null]	/resources/GALL...

【資料詞彙】

組名	蛋頭吐司	填寫人	吳浩愷
專 題 名稱	Cypher Code 加密平台	填寫日期	111 年 5 月 27 日



	A	B	C	D	E	F	G
1	欄位名稱	欄位類型	長度	預設值	允許NULL	說明	備註
2	ROWID	BIGINT	null	X	N	Key	
3	USRID	NVARCHAR	10	X	N	帳號	
4	ID	NVARCHAR	2	X	N	權限	
5	IP	NVARCHAR	20	X	N	IP位置	
6	SEQ	NVARCHAR	3	X	N	排序	
7	PICNAME	NVARCHAR	30	X	N	圖片名稱	
8	UPLOAD	NVARCHAR	12	X	N	上傳日期	
9	LOWER	NVARCHAR	1	X	Y	使用者刪除檔案	X=已刪除
10	FILEPH	NVARCHAR		X	N	路徑	
11	FILENM	NVARCHAR		X	N	檔名	
12	VIEW_PH	NVARCHAR		X	N	加密後檔案完整路徑	
13							

Query Query History

```
1 select * from encrypt
```

Data output Messages Notifications

	rowid	usrid	id	ip	seq	picname	upload	lower	fileph	filenm	view_ph
	[PK] bigint	character varying	character varying	character varying							
1	1	ellen	[null]	127.0.0.1	1	1	1111001	[null]	/resources/original/elements/1...	1.jpg	/resources/GALLERY/ENCRYPT/elements/1...



**【資料詞彙】**

組名	蛋頭吐司	填寫人	吳浩愷
專 題	Cypher Code 加密平台	填寫日期	111 年 6 月 4 日

名稱						
	A	B	C	D	E	F
1	欄位名稱	欄位類型	長度	預設值	允許NULL	說明
2	ROWID	BIGINT	null	X	N	Key
3	USRID	NVARCHAR	10	X	N	帳號
4	ID	NVARCHAR	2	X	N	權限
5	IP	NVARCHAR	20	X	N	IP位置
6	SEQ	NVARCHAR	3	X	N	排序
7	NAME	NVARCHAR	30	X	N	圖片名稱
8	DOWNDT	NVARCHAR	12	X	N	下載日期
9	STATUS	NVARCHAR		X	N	狀態

Query Query History

```
1 select * from decrypt
```

Data output Messages Notifications

	rowid [PK] bigint	userid character varying	id character varying	ip character varying	name character varying	downt character varying	status character varying
1	5	PUG	Y	XXXXXX	11	20221016	[null]
2	6	ellen	M	XXXXXX	1	20221016	[null]

【資料詞彙】

組名	蛋頭吐司	填寫人	吳浩愷
----	------	-----	-----

專題名稱	Cypher Code 加密平台				填寫日期	111 年 6 月 13 日	
欄位名稱	A	B	C	D	E	F	G
1	欄位名稱	欄位類型	長度	預設值	允許NULL	N	備註
2	ROWID	BIGINT	null	X	N	Key	
3	USRID	NVARCHAR	10	X	N	帳號	
4	TOUSR	NVARCHAR	10	X	N	所有者	
5	SEQ	NVARCHAR		X	N	排序	
6	INDATE	NVARCHAR	8	X	N	請求日期	系統西元日期
7	NAME	NVARCHAR	30	X	N	圖片名稱	
8	STATUS	NVARCHAR	1	X	N	狀態	S=等待 Y=成功 N失敗
9	SERIAL_NB	NVARCHAR		X	Y	編號	所有者同意時所給的編號
10	VIEW_PH	NVARCHAR		X	N	加密檔案路徑	

Query Query History

1 select \* from award

Data output Messages Notifications

	rowid [PK] bigint	usrid character varying	touser character varying	seq character varying	indate character varying	name character varying	status character varying	serial_nb character varying	view_ph character varying
1	11	PUG	ellen	1	20221016	11	Y	[null]	/resources/GALL...
2	13	ellen	PUG	1	20221016	2	S	[null]	/resources/GALL...
3	12	ellen	PUG	1	20221016	1	Y	[null]	/resources/GALL...

【資料詞彙】

組名	蛋頭吐司	填寫人	張詠荃
專題名稱	Cypher Code 加密平台	填寫日期	111年6月25日

	A	B	C	D	E	F	G	H
1	ROWID	BIGINT	null	X	N	Key		
2	USRID	NVARCHAR	10	X	N	帳號		
3	STATUS	NVARCHAR	1	X	N	狀態	MSG=訊息 AWARD=授權請求	
4	MSG	NVARCHAR		X	N	訊息內容		
5	INDATE	NVARCHAR	8	X	N	日期	系統西元日期	
6	COMETO	NVARCHAR		X	N	對方帳號		
7	VIEW	NVARCHAR		X	N	顯示狀態	N=未讀 Y=已讀 D=刪除	
8								

Query Query History

1 select \* from message

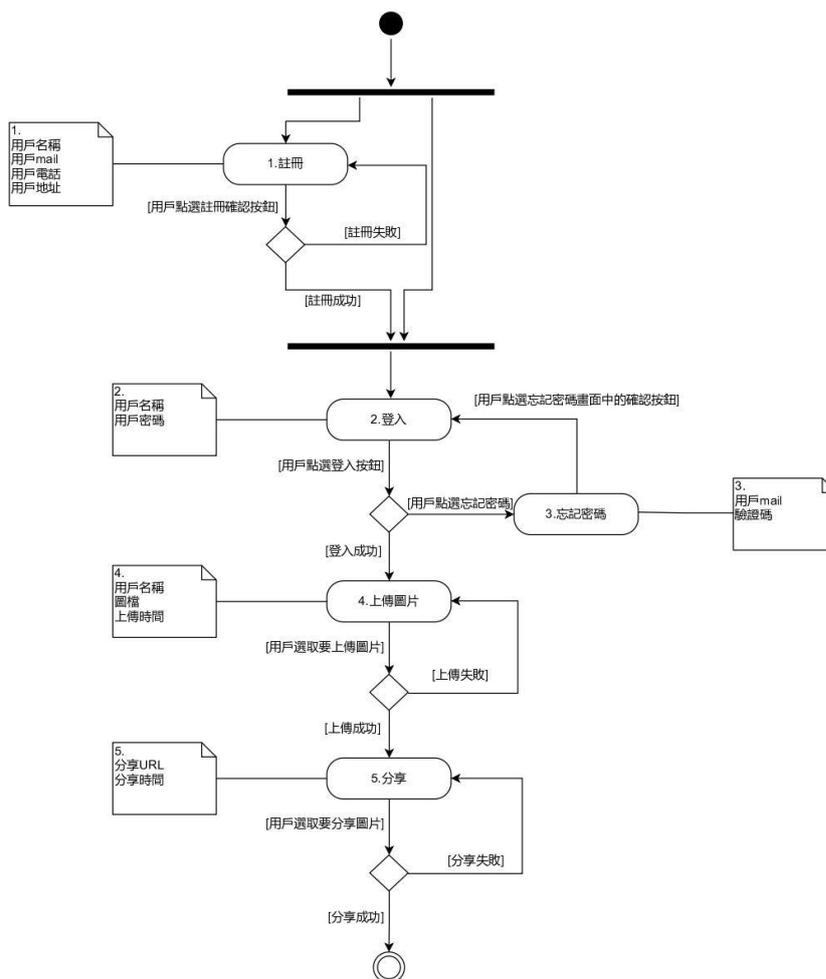
Data output Messages Notifications

	rowid [PK] bigint	usrid character varying	status character varying	msg character varying	indate character varying	cometo character varying	view character varying
1	2	PUG	MSG	HIHIHI~	20221004	ellen	N
2	8	PUG	AWARD	ellen同意你請求(...	20221016	ellen	N
3	9	PUG	AWARD	ellen向你請求(1)...	20221016	ellen	N
4	10	PUG	AWARD	ellen向你請求(2)...	20221016	ellen	N
5	11	ellen	AWARD	PUG同意你請求(...	20221016	PUG	N

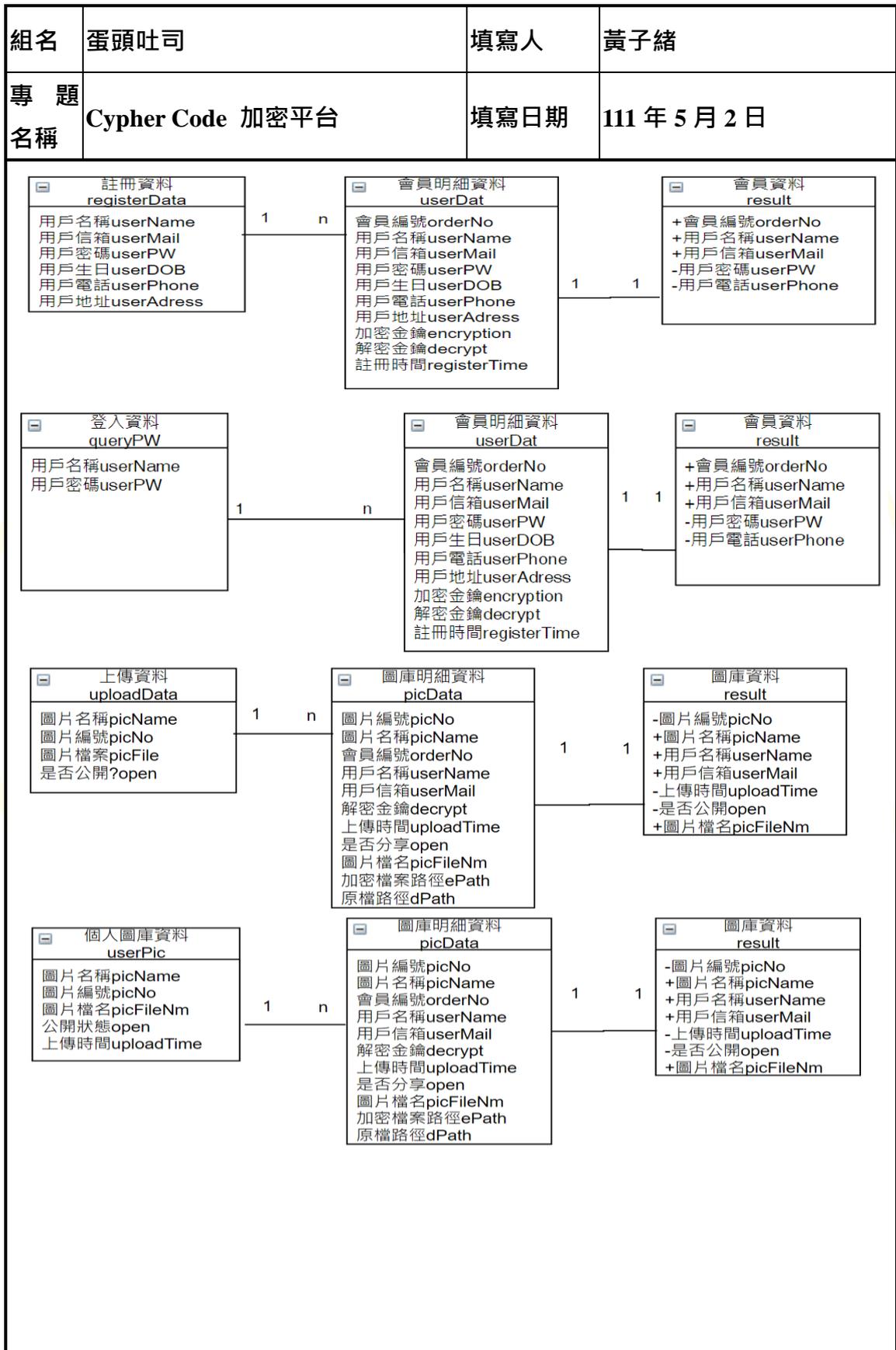


### 附錄七【活動圖】

<b>組名</b>	蛋頭吐司	<b>填寫人</b>	李奕信
<b>專題名稱</b>	Cypher Code 加密平台	<b>填寫日期</b>	111年4月12日



## 附錄八【類別圖】



· 附錄九【會議記錄】

<b>專 題 名稱</b>	Cypher Code 加密平台				
<b>會議 編號</b>	M1	<b>召集人 兼主席</b>	李奕信	<b>紀錄者</b>	馮郁婷
<b>討論 主題</b>	平台系統功能規畫修正			<b>會議 時間</b>	2022/3/27 PM20:00
				<b>會議 地點</b>	學校
<b>上 次 會 議</b>	<b>決議事項</b>		<b>執行狀況</b>		
	平台系統規劃初稿		已完成		
<b>本 次 會 議</b>	<b>本週工作進度</b>		<b>本週工作內容</b>		<b>負責人員</b>
	平台系統功能開發軟件		撰寫平台系統功能目標		馮郁婷
<b>本 次 會 議 內 容</b>	確定平台系統功能的軟件以及設計的功能有哪些，並且開始施行撰寫功能軟件				
<b>決議事項（與主席裁示）</b>					
確定平台畫面按鈕等					
<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>
李奕信	吳浩愷	黃子緒	王睿祺	張詠筌	馮冠璋
<b>請簽名</b>					
馮郁婷					

下次會議	召集人	吳浩愷	紀錄者	馮郁婷	時間	PM20:00
					地點	學校
預定討論主題	撰寫平台系統內容的修改					
指導老師意見	架構雖然有出來，但凡還是希望我們先呈現簡單的畫面給老師查看。					



## 【會議記錄】

<b>專 題 名稱</b>	Cypher Code 加密平台				
<b>會議 編號</b>	M2	<b>召集人 兼主席</b>	吳浩愷	<b>紀錄者</b>	馮郁婷
<b>討論 主題</b>	平台系統架構修改以及撰寫文書			<b>會議 時間</b>	2022/7/5 PM20:00
				<b>會議 地點</b>	學校
<b>上 次 會 議</b>	<b>決議事項</b>		<b>執行狀況</b>		
	平台系統功能開發軟件		已完成		
<b>本 次 會 議</b>	<b>本週工作進度</b>		<b>本週工作內容</b>		<b>負責人員</b>
	平台系統架構修改查找相關 軟件的論文		平台軟件的功能要清楚知道其功 能是做甚麼功用，查找相關軟件的 論文		張詠筌
<b>本 次 會 議 內 容</b>	平台系統軟件清楚列出功能，並且尋找功能對應其他軟件，以及查找相關論文參考，是否可以加以其用在我們的平台系統上，或者做替換功能軟件				
<b>決議事項（與主席裁示）</b>					
查詢論文、平台軟件是否替換					
<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>
李奕信	吳浩愷	黃子緒	王睿祺	張詠筌	馮冠璋
<b>請簽名</b>					
馮郁婷					

下次會議	召 集 人	吳浩愷	紀 錄 者	馮郁婷	時間	PM20:00
					地點	學校
預 定 討論主題	確定軟件的開發以及本組查詢滿意的論文					
指導老師 意 見	找尋關於軟件的文章，並且要組員們挑選出適合本組精選的文章，來加以利用在本組的文書方面					



### 【會議記錄】

<b>專 題 名稱</b>	Cypher Code 加密平台				
<b>會議 編號</b>	M3	<b>召集人 兼主席</b>	吳浩愷	<b>紀錄者</b>	馮郁婷
<b>討論 主題</b>	確定軟件的開發以及本組查詢滿意的論文			<b>會議 時間</b>	2022/8/17 PM20:00
				<b>會議 地點</b>	視訊會議
<b>上 次 會 議</b>	<b>決議事項</b>		<b>執行狀況</b>		
	平台系統架構修改以及撰寫文書		平台系統架構軟件有所變更，找尋相關論文內容有些許不足		
<b>本 次 會 議</b>	<b>本週工作進度</b>		<b>本週工作內容</b>		<b>負責人員</b>
	確定軟件開發，設計藍圖、流程圖		軟件開發、畫藍圖、流程圖		黃子緒
<b>本 次 會 議 內 容</b>	我們從本身的從 vue-js 開始著手寫，但是由於版本過於新穎，再加上時間問題，所以修改成熟悉的 JAVA 開始寫，並且開始設計藍圖、流程圖，找尋相關的論文撰寫				
<b>決議事項（與主席裁示）</b>					
JAVA 撰寫程式、找尋相關論文					
<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>
李奕信	吳浩愷	黃子緒	王睿祺	張詠筌	馮冠瑋
<b>請簽名</b>					
馮郁婷					

下次會議	召集人	李奕信	紀錄者	馮郁婷	時間	PM20:00
					地點	學校
預定討論主題	論文探討、程式的不足					
指導老師意見	因為是在從 JAVA 重新設計，雖然不影響主題，但是比其用 vue 去撰寫程式可能會比較熟悉					



### 【會議記錄】

<b>專 題 名稱</b>	Cypher Code 加密平台				
<b>會議 編號</b>	M4	<b>召集人 兼主席</b>	李奕信	<b>紀錄者</b>	馮郁婷
<b>討論 主題</b>	論文探討、程式的不足			<b>會議 時間</b>	2022/10/3 PM20:00
				<b>會議 地點</b>	學校
<b>上 次 會 議</b>	<b>決議事項</b>		<b>執行狀況</b>		
	確定軟件開發，設計藍圖、流程圖		已完成		
<b>本 次 會 議</b>	<b>本週工作進度</b>		<b>本週工作內容</b>		<b>負責人員</b>
	論文撰寫以及修改程式不足		論文著手撰寫、修改程式不足		張詠筌
<b>本 次 會 議 內 容</b>	我們要找尋程式中所使用的軟件的相關文章，撰寫文書內容，但是要以最淺顯易懂的方式去明白在撰寫文書				
<b>決議事項（與主席裁示）</b>					
讓組員去了解程式的大致意思					
<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>	<b>請簽名</b>
李奕信	吳浩愷	黃子緒	王睿祺	張詠筌	馮冠璋
<b>請簽名</b>					
馮郁婷					

下次會議	召集人	李奕信	紀錄者	馮郁婷	時間	PM20:00
					地點	學校
預定討論主題	文書內容檢討					
指導老師意見	希望我們可以大致明白開發者的程式是如何寫出，並且加以煉化成我自己的東西					

### 【會議記錄】

專題名稱	Cypher Code 加密平台					
會議編號	M5	召集人兼主席	李奕信	紀錄者	馮郁婷	
討論主題	文書內容檢討			會議時間	2022/10/25 PM20:00	
				會議地點	學校	
上次會議	決議事項		執行狀況			
	論文撰寫以及修改程式不足		文書內容太過於複雜需要重新撰寫			
本次會議	本週工作進度		本週工作內容		負責人員	
	撰寫文書內容		撰寫文書內容		李奕信	
本次會議內容	由於上次撰寫文書內容太過於科學數字複雜化，而且無法用言語確切說出，所以要在找尋更加讓所有人以及組員懂得言語去撰寫					
決議事項 (與主席裁示)						

撰寫淺顯易懂的文書					
請簽名 李奕信	請簽名 吳浩愷	請簽名 黃子緒	請簽名 王睿祺	請簽名 張詠笙	請簽名 馮冠瑋
請簽名 馮郁婷					
下次會議	召集人 吳浩愷	紀錄者 馮郁婷	時間 PM20:00	地點 學校	
預定 討論主題	文書完成品				
指導老師 意見	不要太過於去用複雜方式呈現我們所做的程式內容·要用大家比較容易明白方式去撰寫文書以及找尋相關文獻並標明				

**【會議記錄】**

專題 名稱	Cypher Code 加密平台				
會議 編號	M6	召集人 兼主席	李奕信	紀錄者	馮郁婷
討論 主題	文書完成品			會議 時間	2021/11/13 PM20:00
				會議 地點	學校
上 次 會 議	決議事項		執行狀況		
	文書內容檢討		已完成		
本 次 會 議	本週工作進度		本週工作內容		負責人員
	文書完成品		演講文書內容		王睿祺

本次會議內容	由於我們程式跟文書都完成了，所以我們要試著抓時間演講我們所要呈現內容				
<b>決議事項（與主席裁示）</b>					
抓時間演講內容					
請簽名 李奕信	請簽名 吳浩愷	請簽名 黃子緒	請簽名 王睿祺	請簽名 張詠笙	請簽名 馮冠瑋
請簽名 馮郁婷					
指導老師意見	演講內容不要太過於冗長				