國立勤益科技大學資訊工程系實務專題成果報告

※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ 安全增強型之 QR Code 實作 ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※

執 行 期 間 ： 110 學年度上學期至 110 學年度下學期

專題參與人員：

部別：日間部

組別：第 42 組

班別：四訊四甲 座號:18 姓名：李晉宇
四訊四甲 座號:21 姓名：張名崧

指導老師： 林基源教授

中 華 民 國 110 年 5 月 28 日

目錄

目錄.....2
圖目錄.....3
表目錄.....4
第一章 緒論.....6
1.1 研究動機與目的.....6
1.2 報告架構.....6
第二章 系統軟硬體設備與方法.....7
2.1 Matlab 介紹.....7
2.2 App Designer 介面.....7
2.3 群環體簡介.....9
2.4 伽羅瓦域.....10
2.5 本原多項式.....10
2.6 bch 碼編碼方式.....10
2.7 RS 碼編碼方式.....10
2.8 QR Code 結構.....10
2.9 QR Code 資料存取.....11
2.10 QR Code 資訊格式編碼.....14
2.11 QR Code 秘密分享.....15
2.12 QR Code 非對稱加密.....16
第三章 實驗方法與結果.....17
3.1 秘密分享 QR Code 介面.....17
3.2 非對稱加密 QR Code 介面.....17
3.3 秘密分享 QR Code 操作說明.....18
3.4 非對稱加密 QR Code 操作說明.....20
第四章 結論與未來展望.....22

圖目錄

圖 一 MATLAB 介面 7
圖 二 APP DESIGNER 元件庫 8
圖 三 APP DESIGNER 設計介面 8
圖 四 APP DESIGNER 程式介面 9
圖 五 QR CODE VERSION1 範例 11
圖 六 RS 碼編排順序圖 14
圖 七 基本八種掩碼圖示 14
圖 八 QR CODE BCH 碼圖示(綠色部分) 15
圖 九 秘密分享 QR CODE 合成 15
圖 十 秘密分享 QR CODE 產生 16
圖 十一 對掩碼作 ARNOLD 轉換 16
圖 十二 QR CODE 秘密分享介面 17
圖 十三 QR CODE 非對稱加密介面 18
圖 十四 秘密分享 QR CODE 參數輸入介面 18
圖 十五 秘密分享 QR CODE 生成 19
圖 十六 合成後 QR CODE 與使用掩碼 19
圖 十七 加入錯誤值後修正的 QR CODE 20
圖 十八 非對稱加密 QR CODE 參數輸入介面 20
圖 十九 ARNOLD 矩陣、循環週期、掩碼及原始 QR CODE 21
圖 二十 加密金鑰、加密掩碼及加密後 QR CODE 21
圖 二十一 解密金鑰、解密後掩碼及解密後 QR CODE 22

表目錄

表 四 資料編碼格式 11
表 五 字元總數二進制 BIT 個數對照表 12
表 六 VERSION 1 容錯能力表 12
表 七 SHORTING 後 RS 碼編排格式 13
表 八 BCH 碼編碼格式 14

安全增強型之 QR Code 實作
Security-Enhanced QR Code

專題生：李晉宇, 張名崧　　指導教授：林基源 教授

Student: LI,JIN-YU, ZHANG,MING-SONG
Advisor: ：Dr. Chi-Yuan Lin

國立勤益科技大學資訊工程系
Department of Computer Science and Information Engineering
National Chin-Yi University of Technology

摘要

計劃設計具有兩種功能的 QR Code，一種是使用秘密分享技術去達成 QR Code 分享之應用，當所有秘密分享 QR Code 集合在一起時，即可讀取 QR Code 內部的資料；另一種則是使用 arnold 技術對 QR Code 加密，提升掩碼的亂度，比起基本八種掩碼更增加了保密性及安全性。

We plan to design QR Code with two functions. One is to use secret sharing technology to achieve QR Code sharing application. When all secret sharing QR Codes are assembled together, the information inside the QR Code can be read; the other is to use The arnold technology encrypts the QR Code, increases the chaos of the mask, and increases the confidentiality and security compared to the basic eight masks.

第一章 緒論

1.1 研究動機與目的

現今社會中 QR Code 的應用有很多，像是 Line 新增好友、行動支付、網址連結、火車驗票等皆為 QR code 的應用，但有些 QR code 的應用需要存放個人資料或一些需保密的資料，像是火車驗票、行動支付等，為了防止有心人士盜用或竊取，因此我們針對 QR code 加密的部分做了一些研究，本專題加密技術包含兩個部分，一種是使用秘密分享技術去達成 QR Code 秘密分享之應用，將秘密分享 QR code 分給一些此祕密的擁有者，當這些人集合在一起時才可得知此 QR code 所要表示的資料；另一種則是使用非對稱加密技術，讓 QR code 加密具有不可否認性的效果。

1.2 報告架構

該報告架構分為四個章節，各章節說明如下：

第一章 緒論

說明本研究的研究背景、系統架構。

第二章 系統軟硬體設備與方法

敘述本研究使用到的軟硬體設備及介紹： Matlab、App Designer 及其他相關說明。

第三章 實驗方法與結果

說明實驗的步驟、方法與測試結果。

第四章 結論與未來展望

說明本研究系統之結論與該系統整合應用、未來方向。

第二章 系統軟硬體設備與方法

2.1 Matlab 介紹

MATLAB(Matrix Laboratory)，是一種用於演算法開發、資料視覺化、資料分析及數值計算的進階計算語言和互動式環境。

MATLAB 主要提供以下功能：

・可用於計算的高階語言

・可對代碼、檔案和資料進行管理的開發環境

・可以按疊代的方式查探、設計及求解問題的互動式工具

・可用於線性代數、統計、傅立葉轉換、篩選、最佳化以及數值積分等的數學函式

・可用於視覺化資料的二維及三維圖形函數

・可用於建構自訂的圖形化使用者介面的各種工具

・可將基於 MATLAB 的演算法與外部應用程式和語言整合的各種函數

因為數量眾多的附加工具箱，使得 MATLAB 在不同領域也能應用，如影像處理、深度學習、訊號處理及金融建模等。

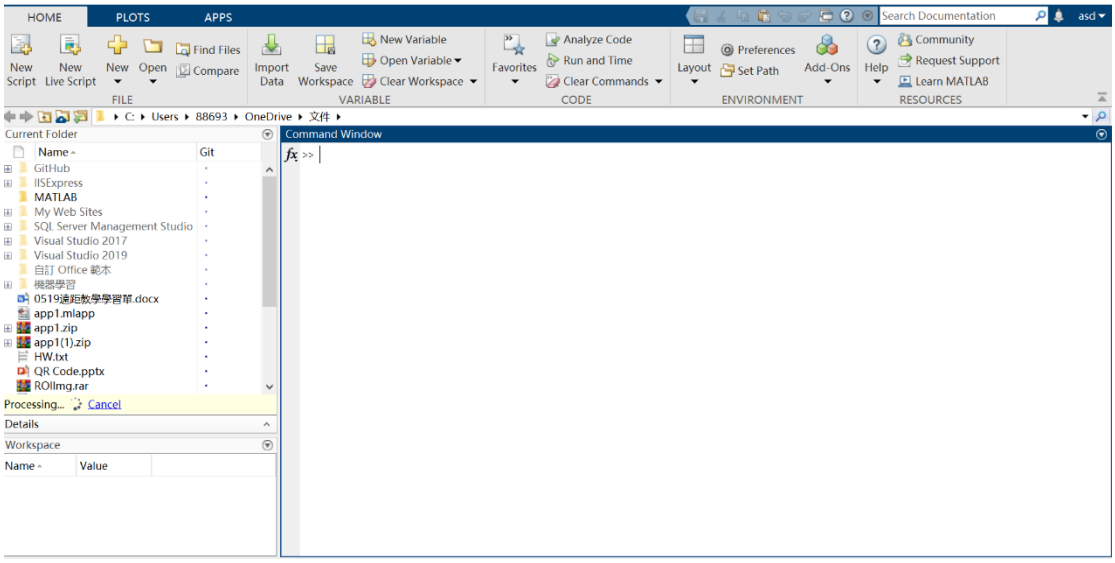

圖 一 MATLAB 介面

2.2 App Designer 介面

在 R2016a 版本中，引入了 App Designer 作為新的應用程式建構平台，主要功能為設定視覺元件與程式設計行為。左邊有元件庫，提供許多元件以拖曳方式去做新增，在介面設計上更加方便。支援一系列標準組件，如編輯欄位、按鈕、文字輸入欄位……等。

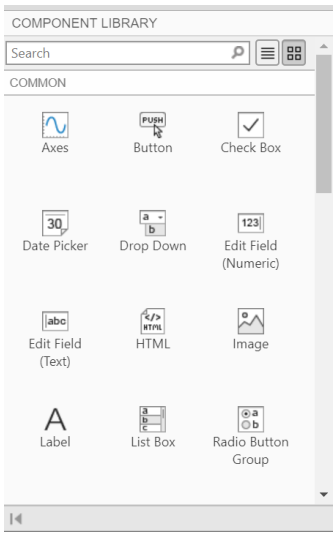

圖 二 App Designer 元件庫

圖 三 App Designer 設計介面

圖 四 App Designer 程式介面

2.3 群環體簡介

1. 群:

   假設(F, +)為一個代數系統

   ∀a, b, c∈ F

   1. 加法封閉性:

      a+b ∈ F

   2. 加法結和性:

      (a+b)+c=a+ (b+c)

   3. 存在加法單位元素:

      $\exists I \in F, a + I = a$ 與 $I + a = a$

   4. 存在加法反元素:

      $a^{-1} \in F, a + a^{-1} = I$ 與 $a^{-1} + a = I$

   只要此代數系統滿足這 4 個條件我稱此代數系統為群。

2. 環:

   假設(F, +, *)為一個代數系統

   1. (F, +)為一個交換群

   2. (F, *)為一個半群

   3. *對+具有分配性

   只要此代數系統滿足這 3 個條件我稱此代數系統為環。

3. 體:

   假設(F, +, *)為一個代數系統

1.(F,+)為一個交換群

2.(F,*)為一個交換群

3.*對+具有分配性

只要此代數系統滿足這 3 個條件我稱此代數系統為體。

2.4 伽羅瓦域

伽羅瓦場為一種有限場，GF(2^p)有 2^p 個元素(0,1,a,a^2,…,a^{2p-2})。

1.加法定義:

$a_1a_2\cdots a_n \oplus b_1b_2\cdots b_n$

2.乘法定義:

$a^a a^b = a^{(a+b) \bmod p}$

3. a^b的反元素:

$a^b a^{-b}=I$ 因此 a^{-b} 為 a^b 的反元素

2.5 本原多項式

除了本身與 1 沒有任何多項式可整除此多項式，此多項式稱為本原多項式。

2.6 bch 碼編碼方式

假設 n 為可糾錯 bits 數，令原訊息為 m(x)，

本原多項式為 $p_1(x), p_3(x), p_5(x), \ldots, p_n(x)$

發送訊息 $r(x)=m(x)/ (p_1(x)p_3(x)p_5(x)\ldots p_n(x))+e(x)$

e(x)為 $m(x)/ (p_1(x)p_3(x)p_5(x)\ldots p_n(x))$的餘式。

2.7 RS 碼編碼方式

假設 t 為可糾錯 bytes 數,令原訊息為 m(x),被除式 $g(x)=(x-2^1)(x-2^2)\cdots(x-2^{2t})$

發送訊息 $r(x)=m(x)/ g(x)+e(x)$

e(x)為 m(x)/g(x)的餘式。

2.8 QR Code 結構

QR code 形狀為正方形，顏色多為黑白兩色，三個像是回字的圖標坐落於 QR code 的三個角落，其功能為幫助解碼軟體定位，使用者不須對準，資料也能被正確讀取。QR code 提供了 40 種版本、8 種掩碼類型，灰色部分為格式資訊與 BCH 糾錯

碼，提供解碼程式版本與掩碼類型，糾錯碼則依 QR code 的容錯等級做錯誤修正。藍色部分為 RS 碼，是資料主要的存放位置。

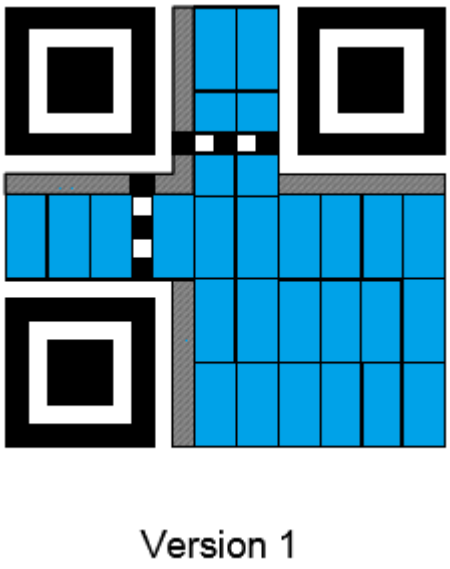

圖 五 QR Code Version1 範例

2.9 QR Code 資料存取

資料編碼模式	資料長度	二元資料串

表 一 資料編碼格式

QR code 資料編碼模式：

1.純數字模式 Numeric mode(編碼模式:0001)

2.英、數組合字元模式 Alphanumeric mode(編碼模式:0010)

3.中文編碼(UTF-8)模式 8-bit byte mode(編碼模式:0100)

4.日文模式 Kanji mode(編碼模式:1000)

以 Numeric mode 的 Version 1 儲存 12345678 為例：

Step1:將數字以三個為一組拆開

123 456 78

Step2:十進制轉為二進制

123=0001111011

456=0111001000

78=1001110

Step3:將轉換後的值做結合

000111101101110010001001110

Step4:將加入編碼模式(Numeric mode:0001)及字元總數(以 **10bits 的二進制**表示)依照編碼格式做排列

0001 000001000 00011110110111001000100111 0

Version	Numeric Mode	Alphanumeric Mode	8-bit byte Mode	Kanji Mode
1 to 9	10	9	8	8
10 to 26	12	11	16	10
27 to 40	14	13	16	12

表 二 字元總數二進制 bit 個數對照表

將結果(0001 0000001000 00011110110111001000100111 0)以 8bits 為一組做排列。其中綠色部分為結束符號，若資料串最後未達 8bits，則補上 0 直到滿足 8bits。黃色部分為補齊符號，若未達到最大 bits 數的限制，則需穿插 11101100(236)和 00010001(17)直到滿足容錯表的長度 K。

00010000
00100000
01111011
01110010
00100111
00000000

11101100
00010001
11101100
00010001
...

容錯能力：QR code 具有糾錯能力，以防 QR code 有髒汙或破損，讀取不到內部的資料，而容錯能力分為四個級別，分別為 L(7%字碼修正)、M(15%字碼修正)、Q(25%字碼修正)、H(30%字碼修正)，等級越高，除錯能力相對較高。

容錯能力表：

Version	Total number of codewords	Error correction level	Number of error correction codewords	Number of error correction blocks	Error correction code per block
1	26	L	7	1	(26,19,2)
		M	10	1	(26,16,4)
		Q	13	1	(26,13,6)
		H	17	1	(26,9,8)

表 三 Version 1 容錯能力表

Error correction code per block：(N,K,c)

N:Codewords 總個數

K:資料碼個數

c:糾錯碼容量

更正能力：$t = \left\lfloor \frac{N-K}{2} \right\rfloor$

容錯百分比計算：$Error\ capapcity = \frac{t}{N} \times 100\%$

一般 RS 碼的編碼長度為$2^m - 1$，*若* RS *碼的長度*無法滿足 QR 碼的格式大小，則可利用 Shortening 的技術做 RS 碼長度的調整。

假設 QR 碼為版本 1，因版本 1 的 RS 碼長為 26，所以選擇長度$2^m - 1 > 26$ *的有限場*產生 RS 碼$(2^m - 1, K')$，以 m=5 形成(31, K')。

因為 QR 碼的長度只能為 26，因此使用 Shortening 技術將 31 縮短 5 個符號為 26，讓資料符號補 5 個零後長度為K'，*則*原始符號資料為$K = K' - 5$，RS 碼為(26, K)。

資料編碼轉成符號未達K，資料符號填滿後不足用補齊符號增長至K，再補 5 個符號 0 形成K'個 RS 碼的資訊符號。

將K'個欲進行 RS 編碼的資訊符號利用系統化編碼方程進行編碼，產生$31 - K'$個同位符號。

X^{30}	X^{29}	X^{28}	X^{27}	X^{26}	X^{25}	X^{24}	X^{23}	X^{22}	. . .				X^2	X	1
同位符號	同位符號	同位符號	同位符號	0	0	0	0	0	. . .	補齊符號	結束位元	. . .	資料串	資料長度	編碼模式

表 四 Shorting 後 RS 碼編排格式

存放依下圖順序存放，1 為資料編碼模式與結束位元，因一個字元需要八個位元組成，所以合併為一個字元，而其餘依照數字順序做編排。

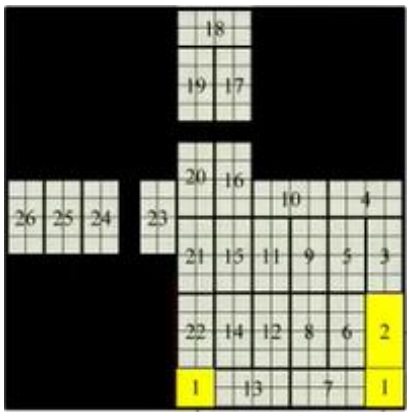

圖 六 RS 碼編排順序圖

2.10 QR Code 資訊格式編碼

QR code 版本	掩碼資訊	BCH 糾錯碼

表 五 BCH 碼編碼格式

QR code 版本目前共有 1~40 個版本，每個版本都有各自的大小與格式，依我們使用的版本 1 為例，提供了21 × 21個 modules，隨版本逐漸增大。掩碼資訊一般分為 8 種，由 3bit 二進制 000~111 來表示，其樣式如圖十四所表示，圖型只掩蓋 RS 碼部分，用於加密不讓人輕易讀取資料內容。而 BCH 糾錯碼則依容錯等級作訂定，當 QR code 出現毀損時，還原其資料。

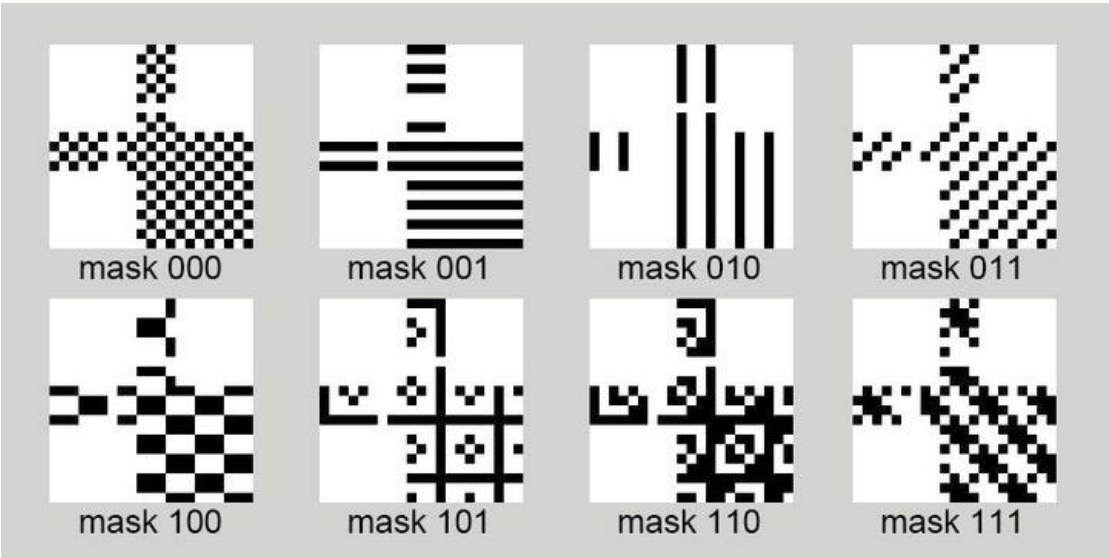

圖 七 基本八種掩碼圖示

將 BCH 碼整理好後，由左至右、由下至上排列，結果如圖十五。

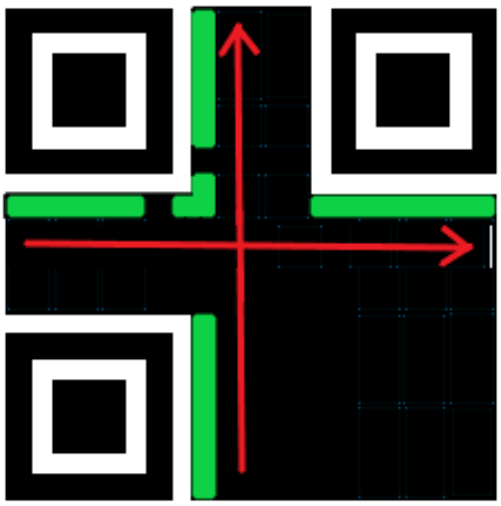

圖 八 QR Code BCH 碼圖示(綠色部分)

2.11 QR Code 秘密分享

秘密分享的用意是將一張 QR Code 分成需要的數量，分發給需使用的人，當其中一位需要使用時，所有秘密分享後的 QR Code 擁有者必須各提供一份 QR Code 作 XOR，才能讀取內部資料。

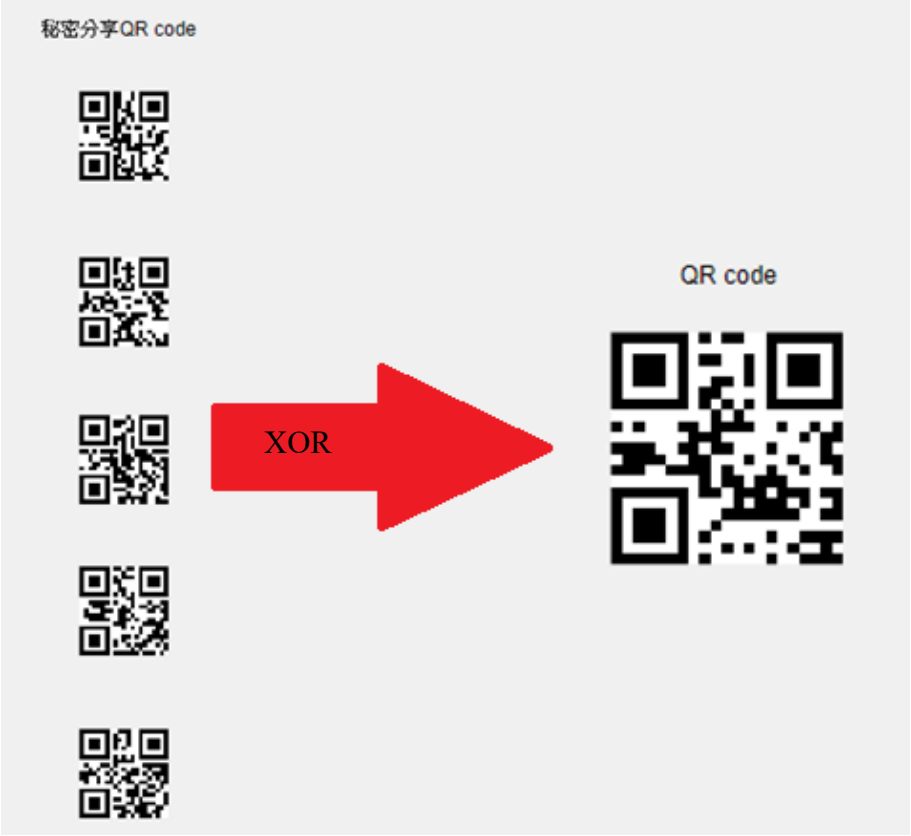

圖 九 秘密分享 QR Code 合成

假設產生五份秘密分享 QR Code，其中第 1~4 份為隨機亂數產生，產生後保留格

式資訊及定位點，第五份由 1~4 張作 XOR 運算後，再對原始 QR Code 作 XOR 運算，即可產生。

圖 十 秘密分享 QR Code 產生

2.12 QR Code 非對稱加密

非對稱加密是密碼學的一種演算法，它需要兩把金鑰，分別為加密金鑰與解密金鑰，加密和解密必須使用不同金鑰，兩個須配對使用，才能解開加密的掩碼，並具有不可否認性特質。

Arnold 轉換具備有非對稱加密特性，因此我們使用它作為 QR Code 的加密，讓 QR Code 的安全性提升。

Arnold 轉換公式：$\begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} X \\ Y \end{bmatrix} mod N$，其中 A、D-B、C=1(行列式為 1)，X 與 Y 為 QR Code 的座標，N 為 QR Code 版本 1 最大值(21)。

假設 Arnold 矩陣為$\begin{bmatrix} 16 & 11 \\ 13 & 9 \end{bmatrix}$，QR Code 為版本 1：

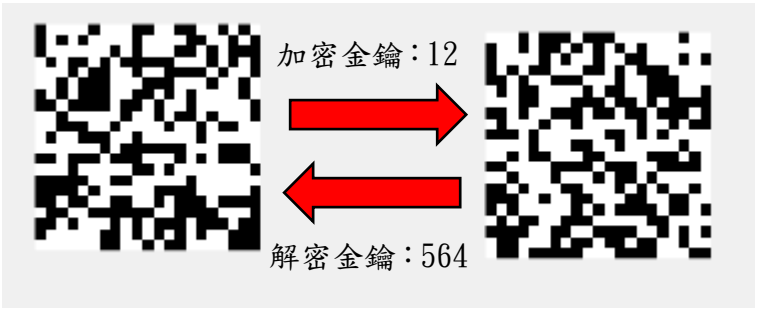

圖 十一 對掩碼作 Arnold 轉換

加密金鑰為 12 代表掩碼經過 12 次 Arnold 的矩陣轉換得到加密的掩碼，而加密金鑰 12 加上解密金鑰 564 為週期 24 的倍數，因此解密金鑰為 564 代表掩碼經過 564 次 Arnold 的矩陣轉換後得到原始的掩碼。

第三章　實驗方法與結果

3.1 秘密分享 QR Code 介面

1:參數輸入區塊
2:秘密分享 QR Code 顯示區塊
3:QR Code 與掩碼顯示區塊
4:錯誤值及加上錯誤值的 QR Code 顯示區塊

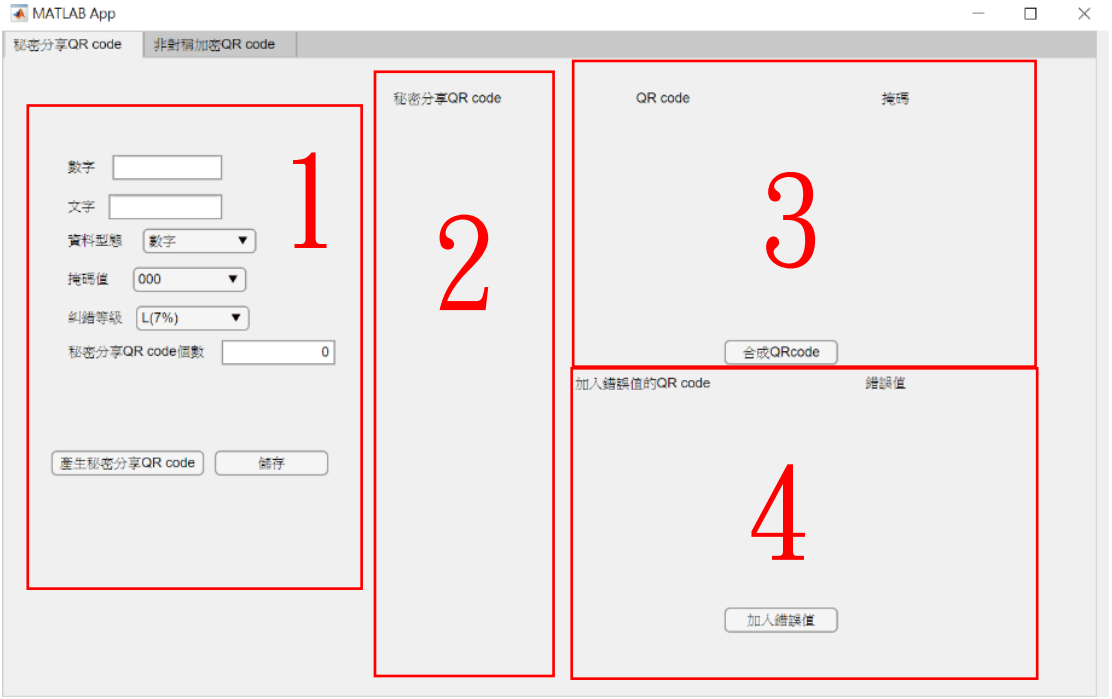

圖 十二 QR Code 秘密分享介面

3.2 非對稱加密 QR Code 介面

1. 參數輸入區塊
2. Arnold 矩陣、循環週期及加解密金鑰顯示區塊
3. 基本掩碼與原始的 QR Code 顯示區塊
4. 經 Arnold 轉換後的掩碼與蓋上加密掩碼後的 QR Code 顯示區塊
5. 解密後掩碼與蓋上解密掩碼後的 QR Code 顯示區塊

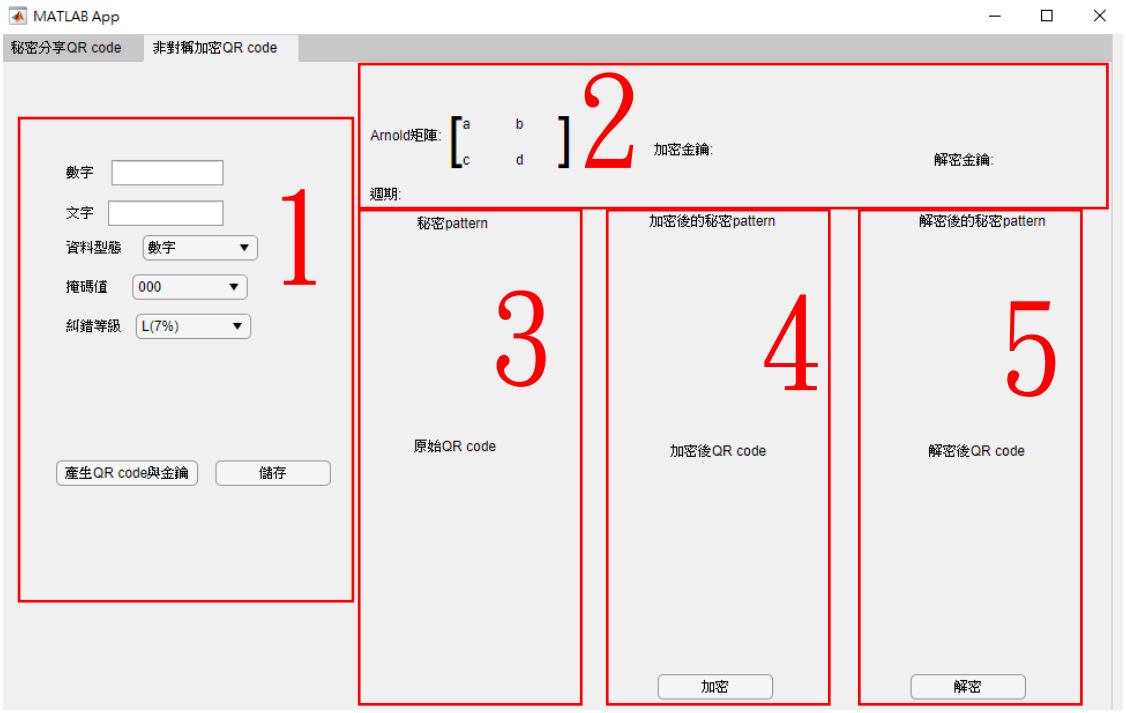

圖 十三 QR Code 非對稱加密介面

3.3 秘密分享 QR Code 操作說明

於數字欄位輸入資料，資料型態可選數字、文字(僅限大寫英文)，掩碼值可使用 000~111 共八種掩碼，糾錯等級有 L、M、Q、H，設定秘密分享 QR Code 個數即可產生 QR Code。

圖 十四 秘密分享 QR Code 參數輸入介面

輸入後即產生下圖結果(五張秘密分享 QR Code)：

圖 十五 秘密分享 QR Code 生成

點擊合成 QR Code 將五張秘密分享 QR Code 進行合成：

圖 十六 合成後 QR Code 與使用掩碼

點擊加入錯誤值後測試 QR Code 是否有除錯能力：

圖 十七 加入錯誤值後修正的 QR Code

3.4 非對稱加密 QR Code 操作說明

於數字欄位輸入資料，資料型態可選數字、文字(僅限大寫英文)，掩碼值可使用 000~111 共八種掩碼，糾錯等級有 L、M、Q、H：

圖 十八 非對稱加密 QR Code 參數輸入介面

點擊產生 QR Code 與金鑰將會產生原始 QR Code 並隨機生成 Arnold 矩陣：

圖 十九 Arnold 矩陣、循環週期、掩碼及原始 QR Code

點擊加密後產生加密金鑰並對掩碼作 Arnold 矩陣轉換，形成加密後的 QR Code：

圖 二十 加密金鑰、加密掩碼及加密後 QR Code

點擊解密後顯示解密金鑰，對加密 QR Code 作解密，並將解密後掩碼及 QR Code 顯示：

圖 二十一 解密金鑰、解密後掩碼及解密後 QR Code

第四章 結論與未來展望

在本實驗的 Arnold 轉換對 QR Code 進行加密，只要掌握住 Arnold 矩陣數值，即可增加竊取者竊取資料的困難度，同時也提升機密資料的安全性，達成保護秘密的目的。

非對稱加密套用在應用上是可行的，主要是因為一般驗證產品真偽，會在印刷上加入雷射標籤，讓消費者來從外觀上判斷產品的真假，但雷射標籤仿冒不容易杜絕。因此採用 QR Code 作為防偽的機制，將防偽的資訊放入 QR Code 條碼內容中，再加上對 QR Code 作非對稱加密後，讓有心人士更難以對 QR Code 作仿冒。

而秘密分享可應用於公司的簽呈上，當一份文件需要各部門的簽署才能被採用，於是我們希望將印章改成 QR Code 的形式作為同意文件的依據，當所有 QR Code 收集在一起，即可合成為一個所有部門同意的 QR Code，也代表文件通過審核。有別於實體印章能再網路上進行傳輸，不須本人到場即可完成簽署，也不再遇到忘記帶印章的窘境，達成數位簽署的作用。