# QR code 上的視覺密碼之研究

蔡秉翰
s110321006@mail1.ncnu.edu.tw

*Abstract*— 本文研究了將視覺密碼系統（Visual Cryptography Scheme, VCS）應用於 QR code 加密的方法。與傳統的安全加密方法如密鑰交換驗證、浮水印技術和資訊隱藏等相比，VCS 更適合用於 QR code 加密。該方法通過將 QR code 拆解成多張分享圖片來實現加密，並通過收集這些圖片來完成解密。我們的研究改進了前人的方法，使得分享圖片的張數可以增加。此外，本文還探討了一種基於偽裝圖像的 QR code 加密方法，該方法使用一張偽裝圖片進行加密，生成兩張與偽裝圖像相似的分享圖片，在保障安全性的同時，使分享圖片變得具有意義，將能降低被攻擊的風險。

## I. INTRODUCTION

隨著資訊技術的快速發展，數據傳輸和儲存的安全性問題變得越來越重要。QR code 因其快速讀取和容易儲存的特性，被廣泛應用於各種場合。然而，QR code 在公開環境中的應用也帶來了資訊安全的隱患。為了提高 QR code 的安全性，研究者提出了多種加密技術，包括密鑰交換驗證、浮水印技術和資訊隱藏等。

視覺密碼系統（VCS）是一種簡單而有效的圖像加密技術。VCS 通過將圖像分割成多張分享圖片，使得單獨一張圖片無法透露任何有用，只有在收集到足夠多的分享圖片後才能還原原始圖像。這種特性使得 VCS 在圖像加密和資訊隱藏領域具有廣泛的應用前景。

本文提出了一種基於 VCS 的 QR code 加密方法。該方法利用 QR code 的錯誤校正能力（ECC），在犧牲部分 ECC 容量的情況下，增加可分享圖片的數量，從而提高加密的安全性和靈活性。具體而言，我們研究了在固定條件下的 QR code 中，文獻[1]是如何在不犧牲 ECC 容量的情況下實現超過 20 張圖片的分享，以及在犧牲部分 ECC 容量的情況下，我是如何實現超過 50 張圖片的分享。

除此之外，本文還探討了一種偽裝圖片的 QR code 加密方法。該方法使用一張偽裝圖片進行加密，生成兩張分享圖片，通過這種方式，既保證了資訊的安全性，又使得分享過程變得更加有意義和便捷。

## II.RELATED WORK

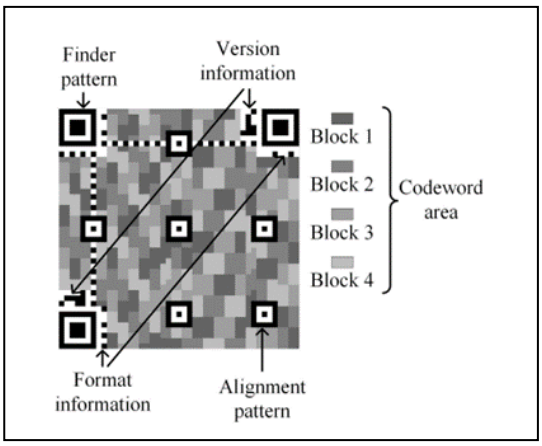
### *A. Definitions*

#### 1. VCS 基本原理

視覺密碼學是一種不需要計算的圖像加密技術，由 Naor 和 Shamir 於 1994 年提出[2]。基本的（$k$, $n$）VCS 方案將一張秘密圖片分割成 $n$ 張分享圖片，只有當至少 $k$ 張分享圖片疊加時，才能還原出原始圖片。這些分享圖片本身不包含有用的資訊，即使獲得少於 $k$ 張圖片，也無法提取任何秘密資訊。

#### 2. QR Code 結構

QR code 由 finder pattern（定位圖案）、version and format information（版本和格式資訊）、alignment pattern（對齊圖案）和 codeword area（資料區域）組成。資料區域進一步分為 data codewords（資料數據）和 error-correction codewords（錯誤校正）。每一個 codewords 由 8 個小方塊組成，小方塊的可能範圍是黑色或白色。如圖一所示。




圖一. QR Code 的結構

#### 3. QR Code 的錯誤校正能力（ECC）

QR code 的錯誤校正能力（ECC）有四個級別：L、M、Q 和 H，分別可以修正約 7%、15%、25%和 30%的錯誤。ECC 的作用是在 QR code 損壞或有部分資訊丟失的情況下，仍然能夠正確解碼。不同的 QR code 版本和 ECC 級別決定了可修正錯誤的數量。圖二列舉出不同級別的錯誤糾正能力。

| 版本 | 錯誤更正等級 | 總Codeword數 (c) | 數據Codeword數 (a) | 糾錯能力 (r) |
|---|---|---|---|---|
| 4 | L | 100 | 80 | 10 |
| | M | 50 | 32 | 9 |
| | Q | 50 | 24 | 13 |
| | H | 25 | 9 | 8 |
| 5 | L | 134 | 108 | 13 |
| | M | 67 | 43 | 12 |
| | Q | 33 | 16 | 9 |
| | H | 33 | 11 | 11 |

圖二. 不同級別 QR Code 的錯誤糾正能力

*B. Related Algorithms*

1. 基於 VCS 的 QR Code 加密方法--無損恢復秘密分發方案

文獻[1]提出了一種基於（$n$ , $n$）VCS 的加密方案，將 QR code 分割成多張秘密圖片。該方案設計了一種將 QR code 劃分為 $n$ 個區域的方法，並將這些區域分配為 $n$ 份分享。當所有分享圖片疊加時，可以無損重建 QR code；如果缺少任意一張圖片，錯誤數量將超過 ECC 的修正能力，導致 QR code 無法正確解碼。

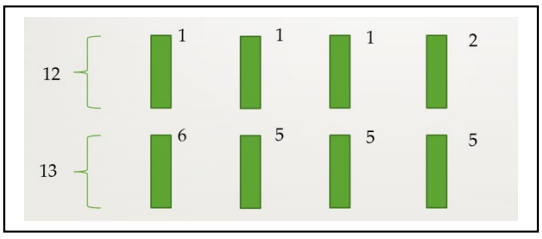
加密方法以版本 4 和錯誤校正等級 H 的 QR code 為例(並非圖一而是類似)，block 的數量為 4 (= $n_b$(H))，每一個 block 有 25 個 codewords，其中分為 9 個 data codewords 和 16 個 error-correction codewords，由圖二得知 ECC 的可修正容量為 8 個 codewords，這代表錯 9 個 codewords，QR code 將無法被正確解碼，在前半部分本文使用 Zxing 解碼器進行解碼。

文獻[1]對不同數量的分享（$n$）的情況提出了三種加密算法：

$n$ = 2 ~ 4：QR code 的一個 block 分配到一張圖片，未使用的 blocks 統一放到最後一張圖片。這樣在重疊時，缺少一張圖片將至少導致一個 block 錯誤為 25 個 codewords 超過 ECC 容量（8 個 codewords），從而達到加密效果。

$n$ = 5 ~ 8：隨機選擇 2*($n_b$(H)) – $n$ 個 blocks 分配到一張圖片，剩餘的每張圖片從剩餘的 blocks 中隨機選取 12 個 codewords（約為 25 的一半）。最後將剩餘的 codewords 放到最後一張圖片。缺少一張圖片將至少導致一個 block 錯誤 12 個以上的 codewords，超出 ECC 容量。

$n$ > 9：將 4 個 block 內的 25 個 codewords 按照黑色方塊數量由小到大排列，切割成 12 和 13 個 codewords，先將劃分好的 8 個區塊分成八張圖片，具體如圖三所示，然後隨機選取一個區塊並確保其第一個 codeword 至少有 2 個黑色像素，移除該區塊中每一個 codeword 的 1 個黑色方塊，放入新的圖片中，直到達到 $n$ 張圖片。因為任何具有錯誤的方塊都會使 codeword 出錯，缺少一張圖片將導致一個 block 錯誤 12 個以上的 codewords，超出 ECC 容量。




圖三. 假設範例示意圖一

文獻[1]對 QR code 的 ECC 進行了分析，設計了一種將 QR code 劃分為 $n$ 個區域的方法。這些區域被分配為 $n$ 份的分享。當所有分享堆疊起來時，QR code 被無損重建，如果堆疊的數為 $n$ − 1 或者堆疊的數較少，恢復的 QR code 就會出現很多錯誤，因為錯誤的數量將超過 ECC 的容量，所以標準解碼器無法對其進行解碼。文獻[1]的方法是不可像素擴展的。所有版本的 QR code 都可以用它加密，但不能加密其他二進位影像。

這方法有效利用了 QR code 的 ECC 特性來實現加密，但在某些情況下並未充分利用 ECC 的容量。為了進一步改進，本文提出了一種新方法，通過犧牲部分 ECC 容量來增加可分享圖片的數量，從而更好地平衡加密和分享功能之間的權衡。

## III. PROPOSED SCHEME

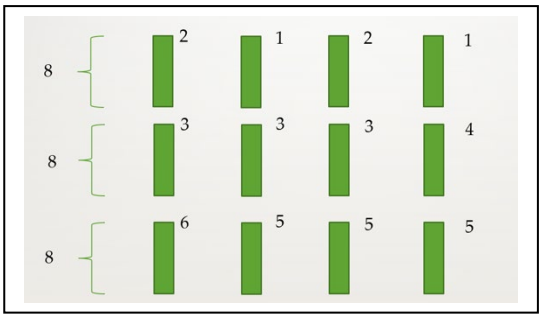
本節分為兩大部分，首先是改進[1]的方法，使得分享圖像的數量可以增加。這部分又細分為四個方法，其增加的數量越來越大。第二部分則是加入偽裝功能，使得 QR Code 的分享圖像可以具有意義，並且疊合後還是可以順利以手機掃描出原密碼。

*A. Improvement*

在這個部分將介紹我們改良前人的演算法，當所有分享圖片疊加時，可以重建 QR code 使 QR code 被 Zxing 掃描解碼，其中包含了四種不同的分配方式。

a.) 移除第一個最少黑色方塊數量的 codeword:

當需求為 $n$ 張圖片時，先將 4 個 blocks 內的 25 個 codewords 按照黑色方塊數量由小到大排列，然後移除第一個最少黑色方塊數量的 codeword，只保留 24 個 codewords，然後將切割成三份每份有 8 個 codeword 如圖四所示 。




圖四. 假設範例示意圖二

先將劃分好的 12 個區塊分成 12 張圖片，然後每次都從劃分好的 12 個區塊中隨機選一個，首先確保該區塊第一個(最少的)codeword 至少有 2 個黑色像素，然後將選到的區塊其中 8 個 codewords 中的每一個 codeword 都拿出 1 個黑色方塊填充到新圖片，這動作會將原圖片的 8 個 codewords 的 1 個黑色方塊移除，共移除 8 個黑色方塊，該區塊第一個(最少的) codeword 值減 1(因為被移除)，直到做到 $n$，因為任何具有錯誤

的方塊都會使 codeword 出錯，所以在重疊時缺少一張圖片，會導致一個 block 錯了 8 個 codewords 再加上最開始移除的第一個最少黑色方塊數量的 codeword，總共會導致一個 block 錯誤 9 個 codewords，超出 ECC 容量(8 個)。

b.) 移除前 4 個最少黑色方塊數量的 codeword:

依照方法 a 延伸，當需求為 *n* 張圖片時，先將 4 個 blocks 內的 25 個 codewords 按照黑色方塊數量由小到大排列，然後移除前 4 個最少黑色方塊數量的 codeword，只保留 21 個 codewords，然後切割成三份每份有 7 個 codeword 。

在重疊時缺少一張圖片，會導致一個 block 錯了 7 個 codewords 再加上最開始移除的 4 個最少黑色方塊數量的 codeword，總共會導致一個 block 錯誤 11 個 codewords，超出 ECC 容量。

此方法可以延伸到移除前 7 個最少黑色方塊數量的 codeword，只保留 18 個 codewords，然後切割成三份每份有 6 個 codeword，重疊時缺少一張圖片，會導致一個 block 錯了 6 個 codewords 再加上最開始移除的 7 個最少黑色方塊數量的 codeword，總共會導致一個 block 錯誤 13 個 codewords，超出 ECC 容量。

c.) 移除前 7 個最少黑色方塊數量的 codeword 並切割成 6 份:

以方法 b 最後的延伸內容為基礎，當需求為 *n* 張圖片時，先將 4 個 blocks 內的 25 個 codewords 按照黑色方塊數量由小到大排列，然後移除前 7 個最少黑色方塊數量的 codeword，只保留 18 個 codewords，然後切割成六份每份有 3 個 codeword 。

在重疊時缺少一張圖片，會導致一個 block 錯了 3 個 codewords 再加上最開始移除的 7 個最少黑色方塊數量的 codeword，總共會導致一個 block 錯誤 10 個 codewords，超出 ECC 容量。

d.) 按照 a、b、c 規律延伸:

依照方法 a、b、c 延伸，當需求為 *n* 張圖片時，我們最終先將 4 個 blocks 內的 25 個 codewords 按照黑色方塊數量由小到大排列，然後移除前 8 個最少黑色方塊數量的 codeword，只保留 17 個 codewords，然後切割成 17 份每份有 1 個 codeword 。

在重疊時缺少一張圖片，會導致一個 block 錯了 1 個 codewords 再加上最開始移除的 8 個最少黑色方塊數量的 codeword，總共會導致一個 block 錯誤 9 個 codewords，超出 ECC 容量。

*B. Meaningful Shares*

在這個部分將提出一個新的演算法$MQ$，使得分享圖像具有偽裝的功能並且當所有分享圖片疊加時，可以重建 QR code 使 QR code 被手機掃描解碼。這個演算法分為四個步驟。首先，我們將要作為偽裝的圖像做檢測再將 QR code、偽裝圖像做處理，接下來，我們將為偽裝圖像和 QR code 做加密。

a.) 偽裝圖像和 QR code 的檢測:

偽裝圖片需要符合兩個特定條件:

1.其大小要跟用來加密的 QR code 一樣為固定的長寬。

2.其黑色和白色部分要和 QR code 的任意其中一個 block 做比較，黑色(或白色)部分需要佔據一個 block 中的 9 個 codewords 以上。

在重疊時缺少一張圖片，會導致一個 block 錯了 9 個 codewords 以上，超出 ECC 容量。

QR code 需要符合一個特定條件:

1.每一個 QR code 的小方塊大小為 1 × 1 的像素。

b.) QR code、偽裝圖像的處裡:

1.將 QR code、偽裝圖像放大一倍，經過放大後，原本 QR code 和偽裝圖像對應位置的像素由 1 × 1 像素變為 2 × 2。

2.將偽裝圖像做反白處理，得到另一張和偽裝圖像相反的圖像。第一張分享將對應到偽裝圖像，第二張分享將對應到反白處理後的偽裝圖像。

c.) 對偽裝圖像的加密:

這裡分為四個部分，分別考慮到偽裝圖像黑色部分和 QR code 黑色部分、偽裝圖像黑色部分和 QR code 白色部分、偽裝圖像白色部分和 QR code 黑色部分、偽裝圖像白色部分和 QR code 白色部分，分別作處理。

1. 偽裝圖像黑色部分和 QR code 黑色部分:

我們將第一張分享對應位置像素左上、左下、右上、右下皆設為黑色，第二張分享對應位置像素左上、左下、右上、右下皆設為白色

2. 偽裝圖像黑色部分和 QR code 白色部分:

我們將第一張分享對應位置像素隨機在左上、左下、右上、右下四個位置中選擇一個設置為黑色其他三個為白色(四分之一的偽裝)，第二張分享對應位置像素設為左上、左下、右上、右下皆設為白色。

3. 偽裝圖像白色部分和 QR code 黑色部分:

我們將第一張分享對應位置像素左上、左下、右上、右下皆設為白色，第二張分享對應位置像素左上、左下、右上、右下皆設為黑色

4. 偽裝圖像白色部分和 QR code 白色部分:

我們將第一張分享對應位置像素設為左上、左下、右上、右下皆設為白色，第二張分享對應位置像素隨機在左上、左下、右上、右下四個位置中選擇一個設置為黑色其他三個為白色(四分之一的偽裝)。

## IV. EXPERIMENTAL RESULTS

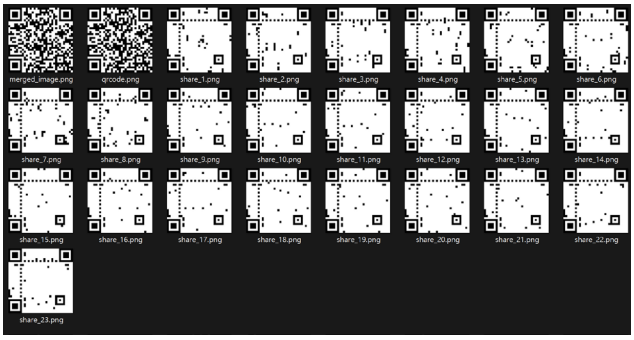
本節依據上節，分為三大部分的實驗。首先將使用圖五的 QR code 為例（330 × 330 像素），先將文獻[1]的演算法實作出來，接著在實作 *Improvement* 的方

法 *a*, *b*, *c*, 和 *d*。接著將修改圖五的 QR code 大小（後面將修改為 33 × 33 像素），並將 *Meaningful Shares* 的演算法$MQ$實作出來。

*A. 對文獻[1]的方法做確認（使用圖五為例）*

圖五. 本實驗所用 QR Code

根據文獻內的方法，計算後得知圖片分享數量最高為 4 + 4 + 4 + 4 + 2 + 2 + 1 + 2 = 23 張分享圖片，如圖六所示。




圖六. 文獻[1]的演算法實驗結果

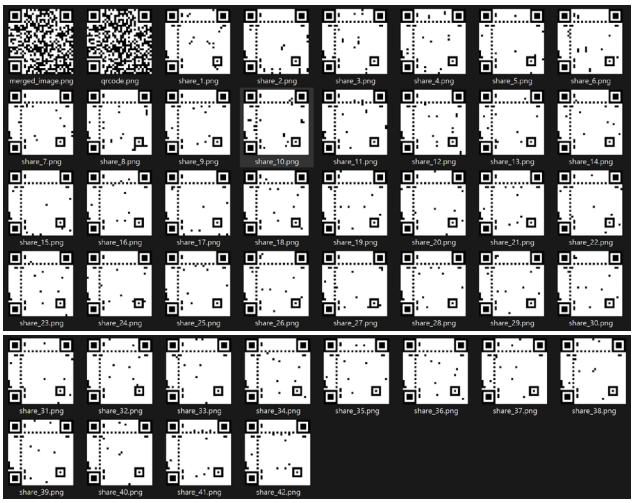
將第 23 張圖片移除並疊合其餘 22 張圖片，結果如圖七所示，缺少一張圖片的疊合結果確實無法解碼。完整疊合 23 張圖片則可以完全還原原本的 QR Code，如圖八所示。

圖七. 疊合 22 張分享圖片的結果

圖八. 疊合全部 23 張分享圖片的結果

*B. 對方法 a, b, c, d 做實驗（使用圖五為例）*

1. 首先對方法 *a* 做驗證，根據我們所提出的方法，圖五的實驗結果最多將可產生 42 張分享圖片：移除第一個最少黑色方塊數量的 codeword 切割成三份每份有 8 個，計算後得知圖片分享數量最高為 2 + 3 + 5 + 2 + 4 + 5 + 2 + 3 + 5 + 2 + 4 + 5 = 42 張分享圖片，如圖九所示。



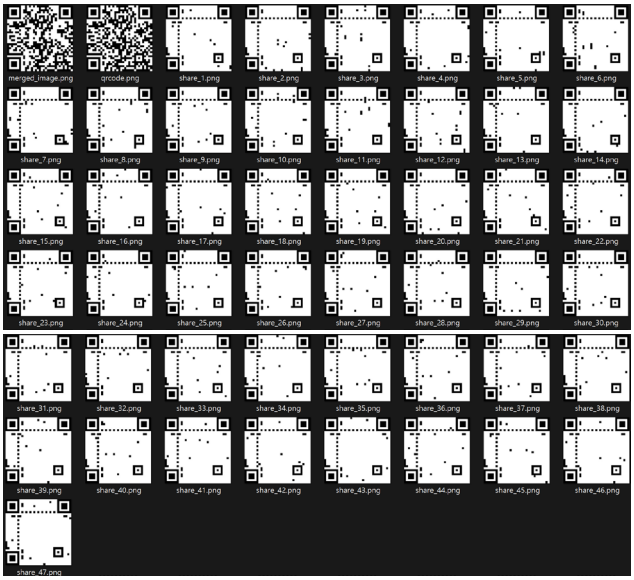

圖九. 方法 *a* 的實驗結果

將第 42 張圖片移除並疊合其餘 41 張圖片，結果如圖十所示，缺少一張圖片的疊合結果確實無法解碼。完整疊合 42 張圖片則可以還原原本的 QR Code 內容，如圖十一所示。

圖十. 疊合 22 張分享圖片的結果

圖十一. 疊合全部 23 張分享圖片的結果

2. 對方法 b 做驗證，根據我們所提出的方法，圖五的實驗結果最多將可產生 47 張分享圖片：移除前 4 個最少黑色方塊數量的 codeword，切割成三份每份有 7 個 codeword，計算後得知圖片分享數量最高為 3 + 4 + 5 + 3 + 4 + 5 + 2 + 4 + 5 + 3 + 4 + 5 = 47 張圖片，如圖十二所示。



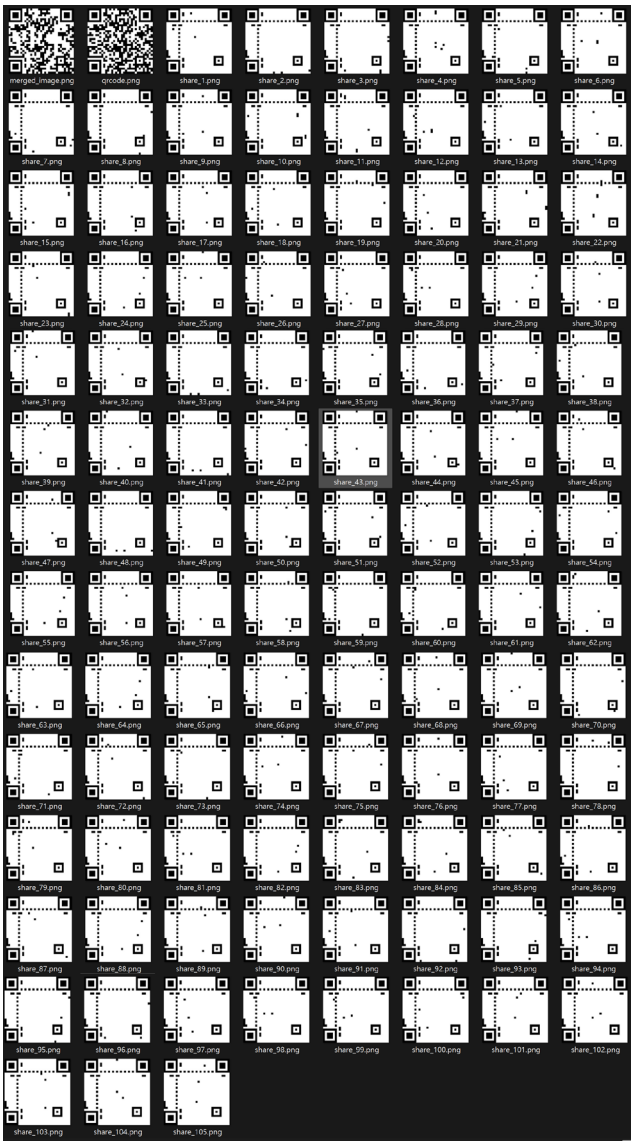
圖十二. 方法 *b* 的實驗結果

將第 47 張圖片移除並疊合其餘 46 張圖片，結果如圖十三所示，缺少一張圖片的疊合結果確實無法解碼。完整疊合 47 張圖片則可以還原原本的 QR Code 內容，如圖十四所示。

圖十三. 疊合 46 張分享圖片的結果

圖十四. 疊合全部 47 張分享圖片的結果

3. 對方法 c 做驗證，根據我們所提出的方法，圖五的實驗結果最多將可產生 107 張分享圖片：移除前 7 個最少黑色方塊數量的 codeword，切割成 6 份每份有 3 個 codeword，計算後得知圖片分享數量最高為 3 + 4 + 4 + 5 + 5 + 6 + 3 + 4 + 4 + 4 + 5 + 6 + 3 + 4 + 4 + 5 + 5 + 5 + 4 + 4 + 4 + 5 + 5 + 6 = 107 張圖片，如圖十五所示。



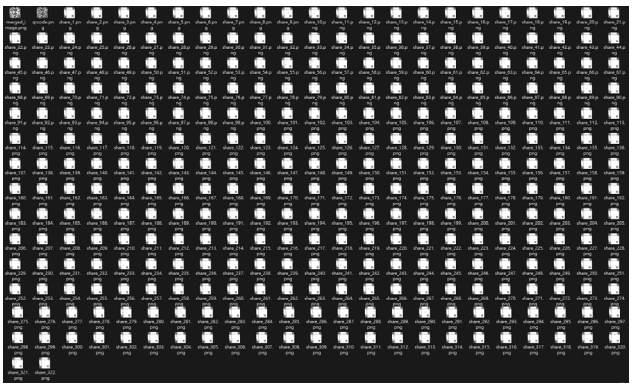
圖十五. 方法 *c* 的實驗結果

將第 105 張圖片移除並疊合其餘 104 張圖片，結果如圖十六所示，缺少一張圖片的疊合結果確實無法解碼。完整疊合 105 張圖片則可以還原原本的 QR Code 內容，如圖十七所示。

圖十六. 疊合 104 張分享圖片的結果

圖十七. 完整疊合 105 張分享圖片的結果

4. 對方法 d 做驗證，移除前 7 個最少黑色方塊數量的 codeword，切割成 6 份每份有 3 個 codeword，使用程式計算得知圖片分享數量最高為 3 + 3 + 4 + 4 + 4 + 4 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 6 + 6 + 6 + 7 + 3 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 5 + 5 + 5 + 6 + 6 + 6 + 6 + 7 +3 + 3 + 4 + 4 + 4 + 4 + 4 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 4 + 4 + 4 + 4 + 4 + 4 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 6 + 6 + 6 + 6 = 322 張圖片



圖十八. 方法 *d* 的實驗結果

將第 322 張圖片移除並疊合其餘 321 張圖片，結果如圖十九所示，缺少一張圖片的疊合結果確實無法解碼。完整疊合 322 張圖片則可以還原原本的 QR Code 內容，如圖二十所示。

圖十九. 疊合 321 張分享圖片的結果

圖二十. 完整疊合 322 張分享圖片的結果

*C. 對演算法MQ做實驗（使用圖二十一為例）*

圖二十一. 本節實驗所用 QR Code 前面圖五的縮小版（33 × 33 像素）

準備好符合兩個特定條件的偽裝圖片，如圖二十二所示，準備好符合小方塊大小為 1 * 1 像素的 QR Code 並將 QR code、偽裝圖像放大一倍。

依照演算法$MQ$對偽裝圖像的加密輸出兩張分享第一張分享將對應到偽裝圖像，如圖二十二所示，第二張分享將對應到反白處理後的偽裝圖像如圖二十三所示。

圖二十二. 本節實驗所用偽裝圖片（33 × 33 像素）

圖二十三. 本節實驗所用反白後的偽裝圖片
( 33 × 33 像素 )

加密輸出的第一張分享將會如圖二十四所示、第二張分享將會如圖二十五所示。

圖二十四. 第一張分享( 66 × 66 像素 )

圖二十五. 第二張分享( 66 × 66 像素 )

將兩張分享重疊後，如圖二十六所示，可以使用手機輕鬆解碼，同時加密輸出的兩張分享仍然保有安全性(無法被破解)，並使得分享過程變得更加有意義。經過實驗驗證，當偽裝圖像黑色部分和 QR code 白色部分、偽裝圖像白色部分和 QR code 白色部分採用二分之一的偽裝，重疊後將無法掃描。

圖二十六. 將兩張分享重疊( 66 × 66 像素 )

## V. Conclusion

本文研究了將視覺密碼系統應用於 QR code 加密的方法。文獻[1]中提出了一種基於 (n, n) VCS 的加密方案，將 QR code 分割成多張分享圖片，最多可分為 23 張分享圖片。我們的研究改進了 [1] 的方法，使得分享圖片的張數可以大幅增加。實驗結果顯示，我們提出的方法最多可將 QR code 分為 322 張分享圖片，大幅提高了加密的安全性和靈活性。

此外，本文還給出一種基於偽裝圖像的 QR code 加密方法，該方法使用一張偽裝圖片進行加密，生成兩張與偽裝圖像相似的分享圖片。實驗證明，在保障安全性的同時，使分享圖片變得具有意義，將能降低被攻擊的風險。通過重疊這兩張分享圖片，可以輕鬆地使用手機掃描出原始的 QR code 內容。

## VI. References

[1] Pan, J.-S., Liu, T., Yan, B., Yang, H.-M., & Chu, S.-C. (2023). A Lossless-Recovery Secret Distribution Scheme Based on QR Codes. Entropy, 25, 653.
[2] Moni Naor and Adi Shamir, Visual Cryptography, EUROCRYPT 1994, pp1–12