楊政興、翁麒耀、江佳峻、李俊達 (2022)，「機密分享機制在加密影像中實現高容量可逆式隱藏技術」，*資訊管理學報*，第 29 卷，第 2 期，頁 181-197。

機密分享機制在加密影像中實現高容量可逆式資訊隱藏技術

楊政興
國立屏東大學資訊科學系

翁麒耀*
國立屏東大學資訊科學系

江佳峻
國立屏東大學資訊科學系

李俊達
台南應用科技大學資訊管理系

摘要

近年來，因雲端計算和隱私保護技術的逢勃發展，讓人們開始關注在加密影像上實現可逆資訊隱藏(RDHEI)技術的發展。RDHEI 是一種在加密影像中嵌入秘密資訊的技術，不但可以正確的取出秘密資訊，並且無損地解密和重建原始影像。本論文提出了一種基於 Shamir 學者所提出的機密分享(Secret Sharing)技術和多項式建構技巧之 RDHEI 技術。我們的方法透過建構多項式的方式將秘密資訊與像素值一起藏到多項式的係數中，再透過機密分享技術，產生加密的分享影像。從實驗結果中，足以證明我們的方法與其他學者的方法相比，擁有較高的嵌入能力。

關鍵詞：加密影像、可逆式資訊隱藏、機密分享、多媒體安全

* 本文通訊作者。電子郵件信箱：cyweng@mail.nptu.edu.tw
2021/07/09 投稿；2021/10/26 修訂；2022/02/11 接受

Yang, C.H., Weng, C.Y., Chiang, C.C. & Li, C.T. (2022). High-capacity reversible data hiding in encrypted images by secret sharing approach. *Journal of Information Management*, 29(2), 181-197.

High-Capacity Reversible Data Hiding in Encrypted Images by Secret Sharing Approach

Cheng-Hsing Yang
Department of Computer Science, National Pingtung University

Chi-Yao Weng*
Department of Computer Science, National Pingtung University

Chia-Chun Chiang
Department of Computer Science, National Pingtung University

Chun-Ta Li
Department of Information Management, Tainan University of Technology

Abstract

Recently, the cloud computing technology and privacy protection have been rapidly developed, resulting in a reversible data hiding scheme in the encrypted image (RDHEI) that attracts people's eyes. RDHEI is a novel scheme that can hide the secret data in an encrypted image. The encrypted image can be successfully extracted from the secret data and be completely recovered back to the original image. This study proposes a novel RDHEI scheme based on Shamir's secret sharing scheme and a constructed polynomial. In the data hiding algorithm, a polynomial function to conceal the secret data and pixels into the coefficients of the constructed polynomial is proposed. Then, the secret sharing scheme is applied to generate the encrypted sharing images. Experimental results demonstrate that the proposed scheme has outperformance in terms of embedding capacity than that of other state-of-the-art methods.

Keywords: Image encryption, Reversible Data Hiding, Secret Sharing, Multimedia Security

* Corresponding author. Email: cyweng@mail.nptu.edu.tw

2021/07/09 received; 2021/10/26 revised; 2022/02/11 accepted

壹、簡介

由於高速計算設備和通信技術的發達，網路已成為通信上重要的工具。在網路上的通訊，常包含大量的多媒體內容，但是多媒體內容可能遭遇到未經授權的複製、共享、刪除、修改等安全問題，因此多媒體安全(Multimedia Security)已成為實現機密防護(Secret Protection)與內容驗證(Context Authentication)之重要議題。

為了解決多媒體安全的問題，加密技術(Encryption)和資訊隱藏技術(Information Hiding)是兩個經常被使用的方法。就資訊隱藏技術的發展，傳統的資訊隱藏技術可能會造成掩護影像(Cover Image)的損壞，由於軍事影像，醫學影像和法律影像等特殊影像，對於細微的失真都是無法被接受的，因此是否可以完全恢復這些影像十分重要。可逆式資訊隱藏技術(Reversible Data Hiding; RDH)可以滿足此項需求，它通過略為改變掩護媒體(Cover Media)，將秘密資訊嵌入至掩護媒體中，並在提取秘密資訊後可以完全恢復掩護媒體。另一方面，RDHEI(Reversible Data Hiding in Encrypted Images)技術可以將加密技術與 RDH 技術相結合，不但可以將秘密資訊藏入影像中，還可以將影像進行加密，藉此保護影像內容。

RDH 技術大致上可以分成三種類型：(1)差異擴張法(Difference Expansion; DE) (Luo et al. 2010; Tian 2003; Wu &Huang 2012)：透過擴展相鄰像素之間的差異來進行差異擴張，再將秘密資訊嵌入至該差異中，由於秘密資訊嵌入後，差異會擴大，因此，差異擴張法無法避免會產生較大的失真情形; (2)直方圖位移法(Histogram Shift; HS) (Xuan et al. 2006; Tai et al. 2009; Ni et al. 2006)：透過原始影像或預測差異的直方圖，將直方圖進行位移，並將位移後空下來的位置用於嵌入秘密資訊。(3)無損壓縮法(Lossless Compression) (Celik et al. 2005; Fridrich et al. 2002)：將秘密資訊隱藏在壓縮原始影像後所多出的空間中，而由於無損壓縮可能會導致視覺品質顯著的下降，因此受到較少的關注。大致上，RDH 方法都是以上述的為基礎，然後再增加一些其他的策略。例如，在 2020 年 Peng 等學者提出了一種直方圖位移的方法 (Peng et al. 2020)，首先透過編碼方式將秘密資訊轉成只有-1,0,1 的訊息，然後在直方圖位移的策略上，選擇中間一個區段(Segment)的 bin 來嵌入，將這些 bin 向左和向右移位，這些 bin 都可以用來嵌入一個-1,0,1 的訊息。其中區段的 bin 大小則是利用閥值(Threshold)來調整，直方圖則是用棋盤式預測法 (Chess Board Prediction; CBP)所產生的預測誤差值來建立。在 2021 年 Gao 等學者提出了一種直方圖位移的方法(Gao et al. 2021)，其方法針對醫學影像來進行嵌入，透過將醫學影像分為 ROI (Regions of Interest)和 NROI (Regions of Non-Interest)，嵌入過程會先將 ROI 的像素值所建立的直方圖向左和向右延伸，如此可以擴大 ROI 的嵌入能力並增強影像的對比度。

RDHEI 技術可以分為兩類：(1)加密前先騰出空間(Ma et al. 2013; Cao et al. 2016; Puteaux & Puech 2018; Wu et al. 2019; Yi & Zhou 2017; Hong et al. 2012; Qin et al. 2019; Yin et al. 2021) (Vacating Room Before Encryption; VRBE)：先對原始影像騰出空間，再進行加密；(2)加密後騰出空間(Vacating Room After Encryption; VRAE) (Qin et al. 2019; Wang et al. 2019; Wu et al. 2018; Chen et al. 2019)：先對影像進行加密，由於加密後的影像保留某些性質，使得加密後的影像可以進行資訊隱藏。VRBE 技術主要是針對原始影像進行可逆式資訊隱藏或壓縮來空出空間，然後再進行影像加密，如此在加密後的影像中存在一塊空間可以用來藏入資訊。

例如，在 2013 年 Ma 等學者提出一種 RDHEI 方法(Ma et al. 2013)，此方法屬於加密前空出空間的技術。他們的方法事先對原始影像進行可逆式資訊隱藏，將某一塊區塊的 LSB 部分嵌入影像中，因此加密後的影像可以使用此區塊的 LSB 部分來藏入資料。在 2018 年，Puteaux 等學者在原始影像上進行 MSB 的預測和壓縮(Puteaux & Puech 2018)，如此一來，MSB 部分則可以空出大部分的空間，加密後的影像可以利用此 MSB 的部分來嵌入資料。

在 2021 年，Yin 等學者提出了一種基於像素預測和 multi-MSB 平面的方法(Yin et al. 2021)，此方法則屬於加密前騰出空間。他們的方法先使用 Median edge detector (MED)預測器來計算預測值，並計算預測誤差值(Prediction Error; PE)。接下來，將 PE 的符號位元存放在位元平面 8 (bit-plane 8)，PE 的絕對值表示於位元平面 7 (bit-plane 7)到位元平面 1 (bit-plane 1)。然後將位元平面劃分為均勻區塊(Uniform Blocks)和非均勻區塊(Non-Uniform Blocks)，並重新排列這些區塊。由於 PE 值通常集中在零附近，因此這些位元平面，存在大量的均勻區塊，可以進行編碼和壓縮，以便空出空間。另一方面，VRAE 技術主要是使用特定的加密技術，使得加密後的影像中，鄰近的像素維持相依性，可以利用此特性對加密後的影像進行資訊隱藏。常用的特定加密技術包括在影像區塊間內進行攪亂(Block-Level Scrambling) (Qin et al. 2019)或者在同一個區塊內的像素使用同一個亂數值進行 XOR 的加密運算(Block-Level Encryption) (Wang et al. 2019)。例如，在 2019 年，Qin 等學者提出一種 VRAE 的方法(Qin et al. 2019)，首先對影像進行加密，其加密方式為對影像進行 bit-plane 間的攪亂(Disordering of bit planes)、區塊間的攪亂(Scrambling of blocks)和區塊內的攪亂(Scrambling of pixels within a block)，如此區塊內的像素保留相依性。接著，進行資訊嵌入的動作時，採用區塊分類和編碼壓縮的方式，以產生嵌入的空間。在 2019 年，Wang 等學者提出一種 VRAE 的方法(Wang et al. 2019)，他們的加密方式採用 Block-Level Encryption 和 Block-Level Scrambling，因此區塊內的像素仍保留相依性。接著，他們利用翻轉(Flip)區塊中的所有像素的 3-LSB 來進行資訊嵌入的動作。區塊則分為 EB (Embeddable Block)和 NEB (Non-Embeddable Block)二種，僅有 EB 區塊才能被使用於秘密訊息嵌入的動作。位置地圖(Location Map)則是用來記錄區塊是屬於 EB 或 NEB，並將位置地圖利用 RDH 方法藏入所有像素的 5-MSB。

傳統的 RDHEI(Reversible Data Hiding in Encrypted Images)技術通常使用 bit-wise (XOR operation)或 byte-wise (stream-cipher-based)的影像加密方式，這些加密方式在安全上仍存在有弱點的疑慮(Khelifi 2018)。為了解決這些疑慮，以機密分享(secret sharing)為基礎的加密技術(Chen et al. 2019; Chen et al. 2020)因此孕育而生。

近年來，有些學者提出基於秘密分享(Secret Sharing)機制(Shamir 1979)的 RDHEI 方法(Wu et al. 2018; Chen et al. 2019; Chen et al. 2020)。所謂秘密分享機制是將一張秘密影像分解成 n 張具雜訊的分享影像，並設定一個門檻植 $k(2 \leq k \leq n)$，稱(k, n)門檻植。當擁有 k 張或 k 張以上的分享影像，就可組成秘密影像。在 2018 年，Wu 等學者提出了一種以秘密分享為基礎之 RDHEI 方法(Wu et al. 2018)，然而他們的加密影像大小會是原始影像大小的兩倍以上。在 2019 年，Chen 等學者提出了一種基於祕密共享的 RDHEI 方法(Chen et al. 2019)，他們的方法利用秘密分享技術將原始影像轉換為加密影像，並將加密影像分發給資訊隱藏者(Data-hider)進行資訊隱藏。雖然是使用 secret sharing 的加密方式，但實際上只產生一張加密影像。由於生成的加密影像的大小與原始影像的大小相同，因此不會

發生資訊膨脹(Data Expansion)的情形。上述方法，都只針對單一的資訊隱藏者(single data-hider)。在2020年，Chen等學者提出新的祕密共享的RDHEI方法(Chen et al. 2020)，將原本單一資訊隱藏者，擴展成多位資訊隱藏者(multiple data-hiders)，且可以產生多張分享影像，但是越多張分享影像，平均嵌入量會下降。

在本論文中，我們提出一種新的RDHEI技術，我們的方式採用Shamir學者所提出的機密分享技術和多項式建構技巧，對影像進行機密分享和資訊隱藏，透過散佈分享影像的方式，若接收者想要對影像進行解密和取出隱藏的資訊，接收者最少需要獲得門檻值(Threshold)以上的影像才可以對原始影像進行復原。我們先透過建構多項式的方式將秘密資訊與像素值隱藏至多項式的係數中，再透過祕密共享方法，將機密訊息和掩護影像一起進行機密分享。本論文所提出的技術可以產生多張分享影像，越多張分享影像，平均嵌入量會略顯下降。

本文的其餘部分安排如下，在第 2 節中介紹相關文獻；在第 3 節中提出我們的方法；在第 4 節中顯示我們的實驗數據，並與其他學者的方法比較；第 5 節提出本文的結論。

貳、文獻探討

因本研究改善 Chen 等學者的方法(Chen et al. 2020)，故在本節只介紹他們的方法，圖 1 為他們的加密、嵌入、取出和解密流程圖。本篇論文將資訊嵌入的過程中，分為影像擁有者(Context-owner)、資訊隱藏者(Data-hider)及接收者(Receiver)等三種角色。首先影像擁有者對影像進行加密，利用金鑰 ke 將原始影像加密成 n 張加密影像(Encrypted image)，每一張加密影像的大小和原始影像相同；接著將每張加密影像分配給不同的資訊隱藏者，每位資訊隱藏者 t 透過金鑰 kh_t 將資料嵌入其加密影像 t 中，$1 \le t \le n$。接收者只有收集任意 k 張有嵌入資訊的加密影像，以及相關的金鑰，就可以取出被嵌入的資訊並且解密得到原始影像。

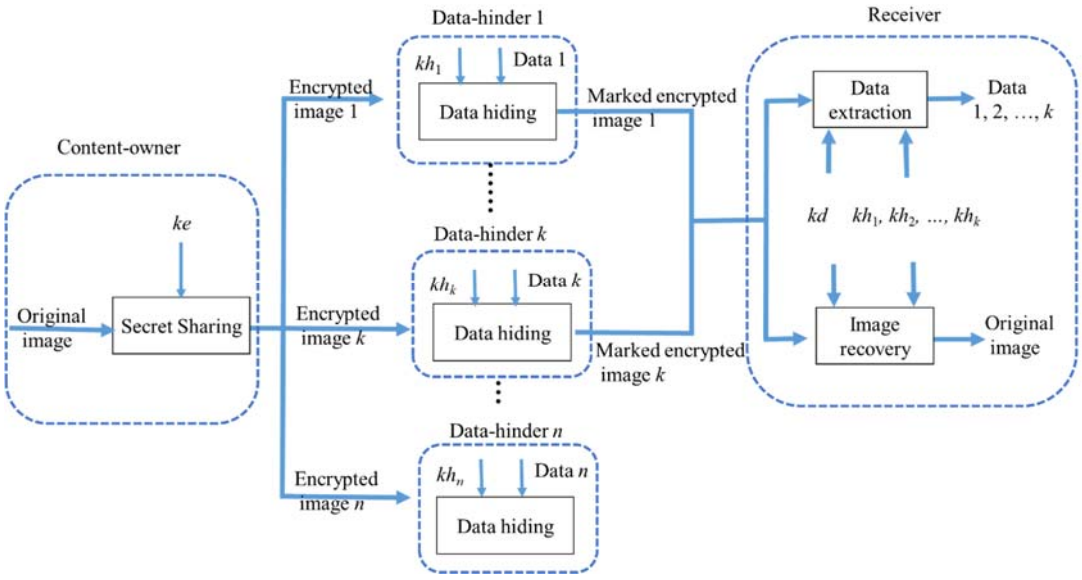


圖1：Chen等學者的加密、嵌入、取出和解密流程圖(Chen et al. 2020)

影像加密的動作是由影像擁有者來執行，先將影像 I 分為 A 部分與 B 部分，A 部分為影像前 10 個 pixel，而剩下的部分則為 B 部分，圖 2 為影像分割表示方式。A 部份用來存放資訊隱藏的參數與直方圖位移過程的參數。首先，從 A 部分提取下面位元，以便挪出空間來存放參數：前兩個像素(pixel)中的所有位元(bit)，以及後面 8 個像素的 3 個 LSB，將所有提取的 bit 定義為 AP。接著對 B 部分進行掃描，用 Location map(LM)記錄像素值≥ 250的位置，並將這些像素值修改為 249。接著，建立 B 部分的直方圖。從直方圖中尋找最適合用於嵌入 Location map 和 AP 的嵌入點，定義為 PP。在直方圖中，將PP + 1和 249 之間的所有值向右移動一個單位，如此可以利用 PP 表示 0；PP + 1表示 1 來將 Location map 和 AP 嵌入，如圖 3 所示。最後，將 PP 值嵌入至 A 部分的後面 8 個像素之 3-LSB 部分。經過上述前置處理後，影像 I 修改成影像I'。

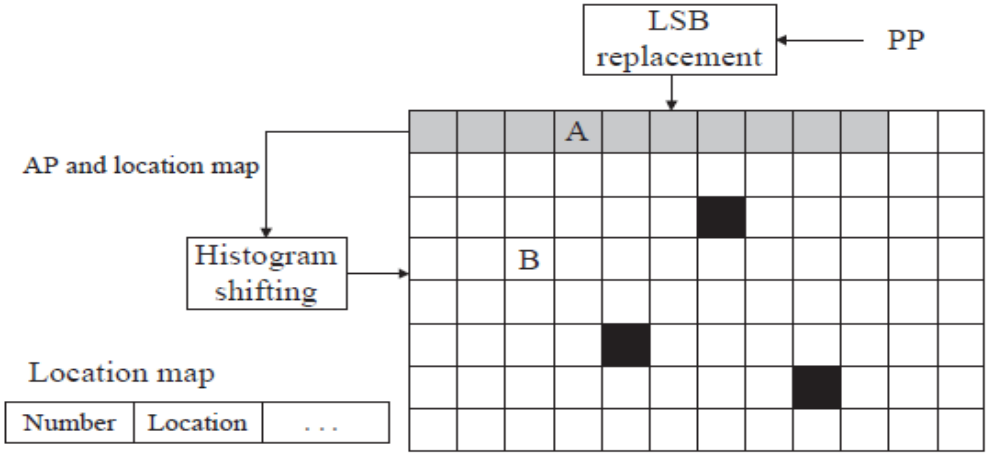


圖2：影像分割成A部分與B部分，其中黑色像素表示其像素值≥ 250

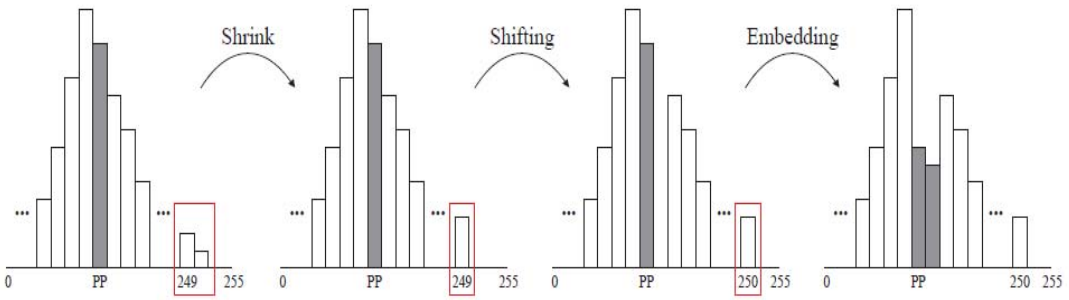


圖 3：像素值縮小與參數嵌入的示意圖

影像I'的 B 部分透過公式(1)進行加密，其中 $T_{i,j}^{(0)}$為一個常數，$a_{i,j}^{(\alpha)}$為一個整數亂數，$I'_{(i,j)}$為位置(i, j)的像素值，pr 為一個質數，若以灰階影像而言，pr 會設定成 251。影像擁有者利用金鑰 ke 產生 n 個非 0 隨機整數值 $x_{i,j}^{(t)}$，$t = 1, 2, \ldots, n$，將非 0 隨機整數值 $x_{i,j}^{(t)}$帶入公式(1)內的 x，並得到加密的結果 $F_{i,j}(x_{i,j}^{(t)})$，$t = 1, 2, \ldots, n$。將參數 t 與 n 藏入至 A 部分的前兩個像素。由此我們可以獲得 n 個加密影像 $E^{(t)}$，$t = 1, 2, \ldots, n$。

$$F_{i,j}(x)=\begin{cases}\left(T_{i,j}^{(0)}+I'_{i,j}x\right) mod\ pr, & if\ k=2\\ \left(T_{i,j}^{(0)}+I'_{i,j}x+\sum_{a=2}^{k-1} a_{i,j}^{(a)}x^a\right) mod\ pr, & if\ 2<k\le n\end{cases} \quad (1)$$

資料嵌入的部分由 n 位資訊隱藏者分別執行，第 t 位資訊隱藏者取得分享的加密影像 $E^{(t)}$可以透過掃描前 2 個像素後所獲得 t、n 值，並將像素以組進行區分，每組包含 n 個像素。再將每組中第 t 個像素的 l 個$(1 \le l \le 7)$LSB 替換為秘密資訊，如此即可獲得 n 張已將秘密資訊嵌入的加密影像 $Em^{(t)}, t = 1, 2, \dots, n$。此方法的嵌入率為 $\frac{\lfloor \frac{WH-2}{n} \rfloor \cdot l}{WH} \approx \frac{l}{n}$ bpp (bits per pixel)，其中 W 和 H 分別是影像的寬和高。

影像取出與解密的部分，假設取得前 k 張分享影像 $Em^{(t)}, t = 1, 2, \dots, k$以及金鑰 ke。在取出藏入的秘密資訊上，針對任一個分享影像 $Em^{(t)}, t = 1, 2, \dots, k$，透過分享影像的前 2 個像素，可以獲得 t 與 n 值。接著，將 $Em^{(t)}$的 B 部分的所有像素，每 n 個分為一組，將每組中第 t 個像素的 l 個 LSB 提取出來，即可獲得分享影像 $Em^{(t)}$的秘密資訊。在影像解密上，針對座標(i, j)的像素 $Em^{(t)}{}_{i,j}, t = 1, 2, \dots, k$，以及金鑰 ke 產生的非 0 隨機整數 $x_{i,j}{}^{(t)}, t = 1, 2, \dots, k$，經由 Lagrange 多項式可以求得公式(1)的 $F_{i,j}(x) = \sum_{t=1}^{k}\left(Em_{i,j}^{(t)} \prod_{a=1, a\ne t}^{k} \frac{x-X_a}{X_t-X_a}\right) mod\ 251$，其中 X_a 使用 $X_{i,j}{}^{(a)}$代入。然而 $Em^{(t)}{}_{i,j}, t = 1, 2, \dots, k$，可能有一個因為藏入 l 個 bit 到 l-LSB，因此無法求得正確的 $F_{i,j}(x)$。不失一般性，假設第 1 個分享影像的像素被藏入 l 個 bit，也就是說 $Em^{(1)}{}_{i,j}$ 被藏入 l 個 bit，則將 $Em^{(1)}{}_{i,j}$ 的 l-LSB 修改成 0 , 1 , 2, …, 2^l-1，必定有一個是嵌入 l-LSB 之前的 $Em^{(1)}{}_{i,j}$，稱為正確的 $Em^{(1)}{}_{i,j}$。利用 $F_{i,j}(0) = T_{i,j}{}^{(0)}$可以辨別出正確的 $Em^{(1)}{}_{i,j}$，其中 $T_{i,j}{}^{(0)}$為加密步驟時所使用的常數。建構出 $F_{i,j}(x)$後，由公式(1)可以得到座標(i, j)的像素$I'_{(i,j)}$，因此可以求得影像I'。最後，利用 A 部分的資訊，將影像I'回復成原始影像 I。

參、本研究所提出之方法

本節中，我們提出一種新的機密影像分享與資訊隱藏相互結合的方法，我們的方法也是引用 Shamir 學者所提出的秘密分享技術（Shamir 1979）。我們改良 Chen 等學者們(Chen et al. 2020)的方法，大幅提升嵌入率，而且提出技巧性的嵌入方式，解決 Overflow 的問題，相較之下 Chen 等學者們的方法需要進行影像預處理以避免 Overflow 的問題，而我們的方法不需要進行預處理，可以直接進行加密與嵌入的動作。圖 4 顯示我們方法在加密、嵌入、取出、解密的操作流程，以 Shamir 學者所提出之秘密分享機制$(3, n)$門檻值為範例，其中 n 代表產生 n 張分享影像，3 代表取得 3 張分享影像就能解密得到原始影像。原始影像 M 經由機密分享後，可以產生 n 張分享影像 $C^{(1)}, C^{(2)}, \dots, C^{(n)}$，同時我們將機密資料 S 嵌入於 n 張分享影像中，金鑰$X_1, \dots, X_n$ 則是對應產生$C^{(1)}, C^{(2)}, \dots, C^{(n)}$所需的金鑰。只要任意 3 張分享影像，就可以進行解密和取出。假設此 3 張分享影像為 C_1, C_2, C_3，則利用金鑰X_1, X_2, X_3可以解密出原始影像 M 和取出機密資料 S。圖 5 是以影像的方式來說明我們的方式之影像變化的流程圖，在影像加密與嵌入後，產生 n 張分享影像，每一張分享影像都呈現加密影像的效果；任意取出 3 張分享影像，可以完全回復原始影像，也能取出嵌入的資訊。

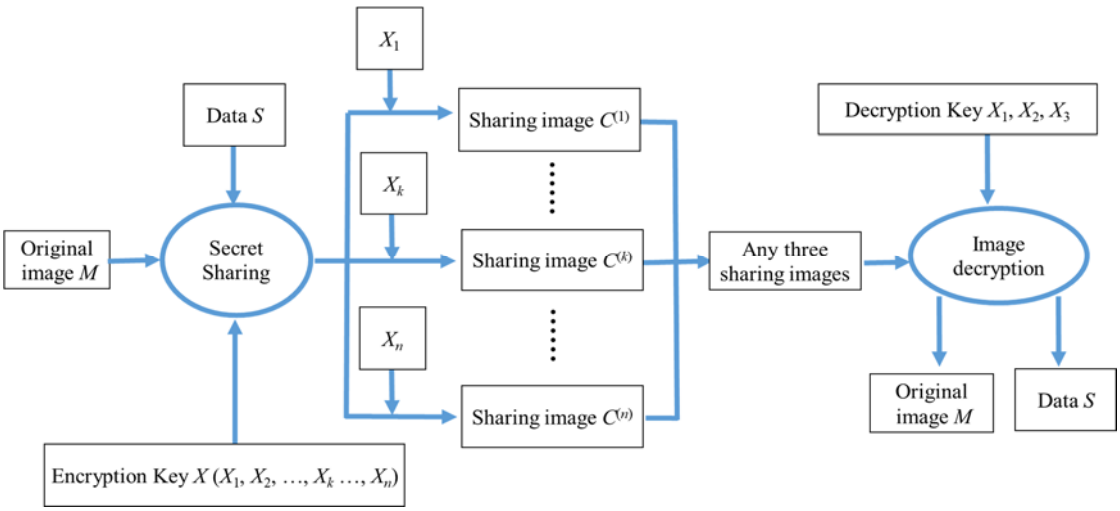


圖4：本研究之加密、嵌入、取出、解密的流程圖

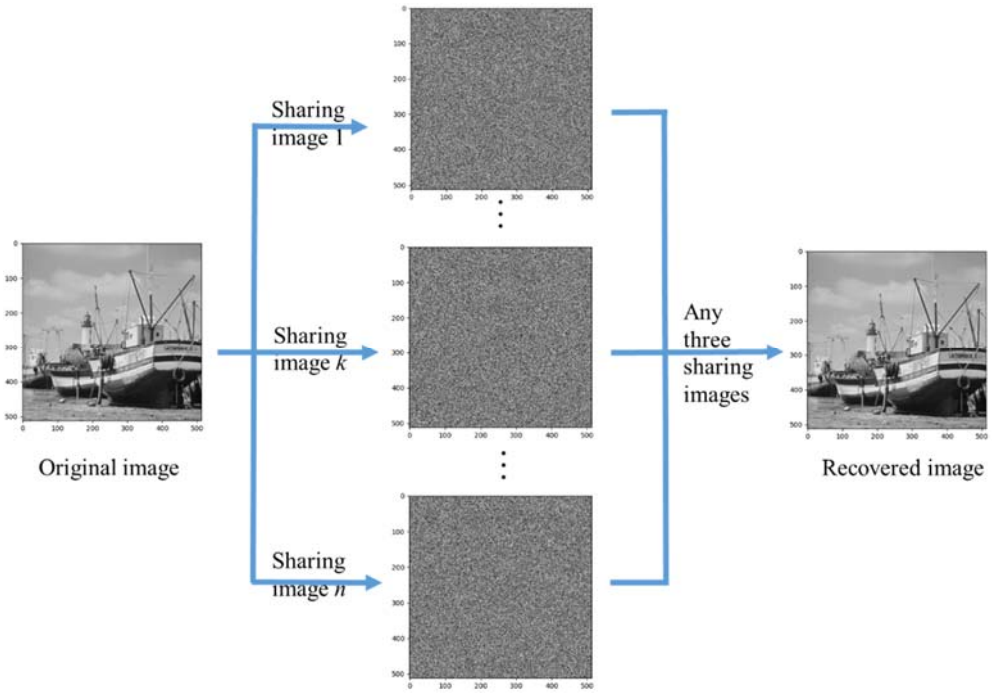


圖5：本研究之流程圖預覽

一、加密與嵌入

在影像加密與嵌入的部分，針對每一張原始影像的像素值與欲隱藏的秘密資訊，產生一個多項式來表示，再透過代入n個機密數值到多項式中，產生n個加密的數值，分別是n個分享像素。以下是本研究所提出的加密與嵌入演算法，我們將以秘密分享機制$(3, n)$門檻值來說明整個演算法，因此多項式為 2 次多項式。

加密與嵌入演算法：

Input: 原始影像 M 、機密資料 S、加密金鑰 X_t，$t = 1, 2, \dots, n$

Output: 分享影像$C^{(t)}$，$t = 1, 2, \dots, n$

Step1. 從原始影像M中提取像素值$P_{i,j}$與欲隱藏資料S，透過建構二項式的方式，產生多項式：$ax^2 + bx + c \mod 251$。

Step2. 將加密金鑰$X_t(t = 1, 2, \dots, n)$代入多項式$ax^2 + bx + c$，獲得n個加密後的像素值$y^{(t)}_{i,j}$，其中$y^{(t)}_{i,j} = aX_t^2 + bX_t + c, t = 1, 2, \dots, n$。

Step3. 重複Step2，直到所有$P_{i,j}$皆已加密。

Step4. 將加密後的像素值以代入的加密金鑰X_i加以區分，並將其合併，以獲得n個加密後的分享影像$C^{(t)}$，$t = 1, 2, \dots, n$。

（一）二次多項式的建構方法：

對一個像素 $P_{i,j}$ 與秘密資訊 S，我們建構出一個二次多項式$ax^2 + bx + c$，將 $P_{i,j}$ 與 S 藏入此二次多項式中，其中 $P_{i,j}$ 可以完整藏入，S 可以藏入的位元數可能為 11 位元、14 位元或 15 位元。假設 $P_{i,j}$ 的像素值為 p，共 8 個位元，由左而右使用$(p_7, p_6, \dots, p_0)_{(2)}$來表示。$S$ 最多可以被嵌入 15 位元，我們以$(S_1, S_2, \dots, S_{15})_{(2)}$表示。此外，$a, b, c$ 必須是小於 251 的數值，我們利用 8 位元來表示，例如，$a = (a_7 a_6 \dots a_0)_{(2)}$、$b = (b_7 b_6 \dots b_0)_{(2)}$、$c = (c_7 c_6 \dots c_0)_{(2)}$。嵌入方式有兩種情況，一種是像素值$p \geq 251$的情況，另一種是$p < 251$的情況，如圖 6 所示。其中，圖 6(a)的圖示中，係數 a 和係數 c 都只有用到 7 個 LSB 位元來做直接嵌入。也就是說，MSB_a = 0 且 MSB_c = 0。

(CASE I) 若 $p < 251$：

(a)將 $p_{7\sim0}$ 和 $S_{1\sim14}$ 藏入$ax^2 + bx + c \mod 251$ 中，其中，$a = (S_{1\sim7})_{(2)}$、$b = (p_{7\sim0})_{(2)}$、$c = (S_{8\sim14})_{(2)}$。

(b)若$(a + 128) < 251$且$(c + 128) < 251$，利用公式(2)和公式(3)將 $S_{15(2)}$ 藏入$ax^2 + bx + c$中。

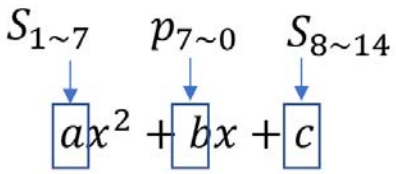
$$a = \begin{cases} a + 128 & \text{if } S_{15} = 1 \\ a & \text{if } S_{15} = 0 \end{cases} \tag{2}$$

$$c = \begin{cases} c + 128 & \text{if } S_{15} = 0 \\ c & \text{if } S_{15} = 1 \end{cases} \tag{3}$$

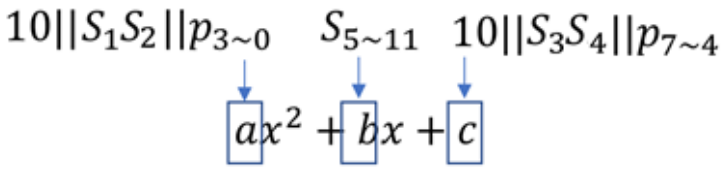
(CASE II) 若 $p \geq 251$：

將 $(p_{7\sim0})_{(2)}$和$(S_{1\sim11})_{(2)}$藏入$ax^2 + bx + c \mod 251$ 中：

$a = 10_{(2)} || (S_1 S_2)_{(2)} || (p_{7\sim4})_{(2)}$、$b = (S_{5\sim11})_{(2)}$、$c = 10_{(2)} || (S_3 S_4)_{(2)} || (p_{3\sim0})_{(2)}$，其中 a 和 c 的首兩個位元被設定成 10，其目的是為了保證 $a < 251$ 和 $c < 251$。



(a)



(b)

圖 6：二次多項式建構方法：(a)當像素值$p < 251$; (b)當像素值$p \geq 251$

二、解密與取出

在資訊取出和影像解密的部分，本研究需收集門檻值(Threshold)以上的分享影像與解密金鑰，才能計算出每個像素所使用的多項式。再透過此多項式將原始影像與秘密資訊取出，便能獲得秘密資訊和原始影像。下面是我們的解密和取出演算法，為了方便說明，假設在秘密分享機制$(3, n)$門檻值中，我們已取得前 3 張分享影像 $C^{(1)}$、$C^{(2)}$、$C^{(3)}$和解密金鑰 X_1、X_2、X_3。

解密和取出演算法：

Input: 三張分享影像 $C^{(1)}$、$C^{(2)}$、$C^{(3)}$、解密金鑰 X_1、X_2、X_3

Output: 機密訊息 S、原始影像 M

Step1. 將三張分享影像的像素值$C^{(1)}_{i,j}$、$C^{(2)}_{i,j}$、$C^{(3)}_{i,j}$與解密金鑰 X_1、X_2、X_3，帶入公式(4)的Lagrange多項式，建立多項式$ax^2 + bx + c$ 。

Step2. 利用多項式$ax^2 + bx + c \mod 251$中的係數值a、b、c，來獲得原始像素值$P_{i,j}$與秘密資訊S_i。

Step3. 重複Step1、Step2直到獲取所有原始像素值$P_{i,j}$與秘密資訊S_i，及合併所有像素值$P_{i,j}$與秘密資訊S_i成為原始影像M和秘密資訊S。

在影像解密的階段，以前三張分享影像 $C^{(1)}$、$C^{(2)}$、$C^{(3)}$為例，在座標位置(i, j)的像素值 $C^{(1)}_{i,j}$、$C^{(2)}_{i,j}$、$C^{(3)}_{i,j}$ 和解密金鑰 X_1、X_2、X_3，利用公式(4)的 Lagrange 多項式，可以建構原始的二次多項式$ax^2 + bx + c \mod 251$：

$$F_{i,j}(x) = \sum_{t=1}^{3}\left(C^{(t)}_{i,j} \prod_{a=1,a\neq t}^{3} \frac{x - X_a}{X_t - X_a}\right) \bmod 251 \quad (4)$$

獲得原始二次多項式$F_{i,j}(x) = ax^2 + bx + c \mod 251$ 後，透過公式(5)和公式(6)來取得原始像素 $P_{i,j}$和機密資訊 S：

$$P_{i,j} = \begin{cases} a_{3\sim0} \,||\, c_{3\sim0} & \text{if MSB\_}a = 1, \text{MSB\_}c = 1 \\ b_{7\sim0} & \text{others} \end{cases} \quad (5)$$

$$S = \begin{cases} a_{6\sim0} \,||\, c_{6\sim0} & \text{if MSB\_}a = 0,\ \text{MSB\_}c = 0 \\ a_{6\sim0} \,||\, c_{6\sim0} \,||\, 1_2 & \text{if MSB\_}a = 1,\ \text{MSB\_}c = 0 \\ a_{6\sim0} \,||\, c_{6\sim0} \,||\, 0_2 & \text{if MSB\_}a = 0,\ \text{MSB\_}c = 1 \\ a_{5\sim4} \,||\, c_{5\sim4} \,||\, b_{6\sim0} & \text{if MSB\_}a = 1,\ \text{MSB\_}c = 1 \end{cases} \quad (6)$$

其中 MSB_a 為 $a_{7(2)}$、MSB_c 為 $c_{7(2)}$。

三、 範例

以下我們使用兩個範例，分別是$p < 251$ 和 $p \geq 251$等二種情況，來說明本研究所提出之加密與嵌入過程。

(一)範例一

假設有一連串的秘密資訊 S = 000 0001 0000 001 $0_{(2)}$，及嵌入秘密訊息的像素值 p = $200_{(10)}$，並使用秘密分享技術的門檻值(k, n) = (3, 4)。

1.嵌入與加密

由於像素值$200 < 251$，因此使用 p < 251 的方式，將像素值與秘密資訊以多項式$ax^2 + bx + c$表示，其中 a = 0000 $0001_{(2)}$ = $1_{(10)}$、b = $200_{(10)}$、c = 0000 $0001_{(2)}$ = $1_{(10)}$，得到多項式：$ax^2 + bx + c$ = x^2 + 200x + 1。由於$(a + 128) < 251$ and $(c + 128) < 251$，因此可以嵌入 S_{15}。因為 S_{15}=0 $_{(2)}$，根據公式(2)和公式(3)，我們修改$c = c + 128 = (1 + 128) = 129$，因此修改過後的多項式為 x^2 + 200x + 129。

接著開始進行加密，此時我們假定由亂數隨機產生的加密金鑰 X_t 分別為 X_1 = 60，X_2 = 80，X_3 = 100，X_4 = 40，將其值代入 $(x^2 + 200x + 129) \bmod 251$，獲得 4 個加密過後的分享像素，分別為 $y^{(1)}$=167 (=(60^2+200×60+129) mod 251)，$y^{(2)}$ = 190 (=(80^2+200×80+129) mod 251)，$y^{(3)}$ = 9 (=(100^2+200×100+129) mod 251)，$y^{(4)}$ = 191 (=(40^2+200×40+129) mod 251)。

2.解密與取出

對上述加密的結果作解密操作。從接收端接收到 3 張分享影像的像素 $y^{(1)}$、$y^{(2)}$、$y^{(3)}$、解密金鑰 X_1、X_2、X_3，將 X_1、X_2、X_3和 $y^{(1)}$、$y^{(2)}$、$y^{(3)}$代入公式(4)，以獲得原始多項式，如下：$167 \times \frac{x-80}{60-80} \times \frac{x-100}{60-100} + 190 \times \frac{x-60}{80-60} \times \frac{x-100}{80-100} + 9 \times \frac{x-60}{100-60} \times \frac{x-80}{100-80} = \frac{-51x^2+7370x-225200}{200} (\bmod 251) = x^2 + 200x + 129 (\bmod 251)$。將獲得的原始多項式透過公式(5)和公式(6)計算像素值 p 與秘密資訊 S。從多項式的係數值中可得知，a= $1_{(10)}$ = $\underline{0}$ 0000001$_{(2)}$、b = $200_{(10)}$、c = $129_{(10)}$= $\underline{1}$ 0000001$_{(2)}$，由於 MSB_a = 0, MSB_c = 1，表示 S_{15} 有藏入秘密資訊，且其值為 0，故機密訊息為 $S_{1\sim15} = a_{6\sim0} \,||\, c_{6\sim0} \,||\, 0$ = 0000001 0000001 $0_{(2)}$。因為 b = 200，所以原始像素值 p 為 200。

(二)範例二

假定秘密資訊 $S = 0000\ 0010\ 0001\ 111_{(2)}$，欲隱藏訊息的像素值 $p = 255_{(10)} = 1111\ 1111_{(2)}$。

1.嵌入與加密

由於像素值$255 \geq 251$，因此使用$p \geq 251$的方式，即 $a = 10_{(2)} \| S_{1\sim2} \| p_{7\sim4} = 10_{(2)} \| 00_{(2)} \| 1111_{(2)}$，$c = 10_{(2)} \| S_{3\sim4} \| p_{3\sim0} = 10 \| 00 \| 1111$，$b = S_{5\sim11} = 0010000_{(2)}$，將像素值與秘密資訊以多項式的方式表示，如下：$a = 10001111_{(2)} = 143_{(10)}$、$c = 10001111_{(2)} = 143_{(10)}$、$b = 0010000_{(2)} = 16_{(10)}$，得到多項式：$ax^2 + bx + c = 143x^2 + 16x + 143$。

接著開始進行加密，此時我們假定由亂數隨機產生的加密金鑰 X_i 分別為 $X_1 = 60$，$X_2 = 80$，$X_3 = 100$，$X_4 = 40$，將這些值代入 $143x^2 + 16x + 143 \bmod 251$，獲得 4 個加密過後的分享像素，分別為 $y^{(1)} = 98$ $(=(143\times60^2+16\times60+143) \bmod 251)$，$y^{(2)} = 222$ $(=(143\times80^2+16\times80+143) \bmod 251)$，$y^{(3)} = 39$ $(=(143\times100^2+16\times100+143) \bmod 251)$，$y^{(4)} = 169$ $(=(143\times40^2+16\times40+143) \bmod 251)$。

2. 解密與取出

對範例二加密結果作解密動作。從接收端收到 3 張分享影像之像素 $y^{(1)}$、$y^{(2)}$、$y^{(3)}$、及解密金鑰 X_1、X_2、X_3。將解密金鑰 X_1、X_2、X_3 和像素 $y^{(1)}$、$y^{(2)}$、$y^{(3)}$ 代入公式(4)，以獲得原始的多項式，多項式計算如下：$98 \times \frac{x-80}{60-80} \times \frac{x-100}{60-100} + 222 \times \frac{x-60}{80-60} \times \frac{x-100}{80-100} + 39 \times \frac{x-60}{100-60} \times \frac{x-80}{100-80} = \frac{-307x^2+47940x-1692800}{800} \pmod{251} = 143x^2 + 16x + 143 \pmod{251}$。將獲得的原始多項式透過公式(5)公式(6)計算像素值 p 與秘密資訊 S，由於 MSB_a = 1, MSB_c = 1，故 $a = 10_{(2)} \| S_{1\sim2} \| p_{7\sim4} = 10_{(2)} \| 00_{(2)} \| 1111_{(2)}$，$c = 10_{(2)} \| S_{3\sim4} \| p_{3\sim0} = 10_{(2)} \| 00_{(2)} \| 1111_{(2)}$，$b = S_{5\sim11} = 0010000_{(2)}$，所以秘密資訊為 $S_{1\sim11} = 0000\ 0010000_{(2)}$，而隱藏訊息的像素值為 $p_{7\sim0} = 11111111_{(2)} = 255$。

肆、實驗模擬與數據分析

在此節中，我們進行實驗模擬與數據分析，本研究使用 8 張標準實驗影像，其大小為 512×512，影像如圖 7 所示。圖 8 為影像 Boat 的實驗結果，我們採用 Shamir 學者(3, 4)門檻值機密分享的方式，將原始影像加密成 4 張分享影像，只要取得任意 3 張分享影像，就可以建構出原始影像，並且取得嵌入的機密訊息。圖 8(a)為原始影像，而圖 8(b)~(e)分別為不同的分享影像，而圖 8(f)為解密且資訊取出後的影像，由影像可知我們的方法可以完全復原。同樣的我們也對 Couple 影像進行一樣的動作，其結果顯示於圖 9。

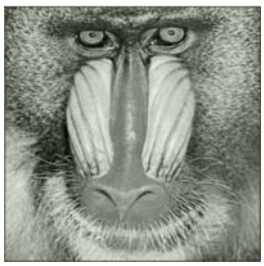
圖 10 為本研究與其他學者之最大嵌入量的比較數據。我們採用 Shamir 學者(3, 3)門檻值機密分享的方式來進行比較。平均而言，我們可以利用一個二次方程式的係數，嵌入大約 15 位元的機密資訊，因此 3 張分享影像的嵌入率接近 5 bpp (bit per pixel)。在 Chen et al. 的方法中(Chen et al. 2020)，他們的嵌入率為 $\frac{\lfloor \frac{WH-2}{n} \rfloor \cdot l}{WH} \approx \frac{l}{n}$ bpp。假設 $n = 3$，$l = 7$，嵌入率大約 2.3 bpp。由圖 9 可得知本研究的方法其嵌入率遠遠的大於其它方法。

(a) Lena

(b) Peppers

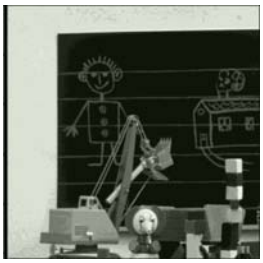
(c) Boat

(d) Sailboat



(e) Baboon

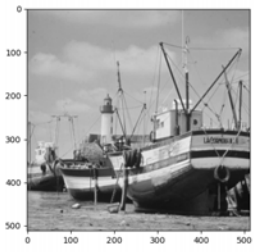
(f) Couple



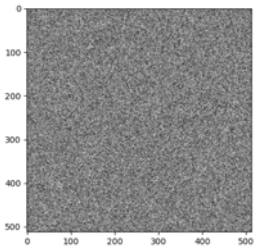
(g) Toys

(h) Girl

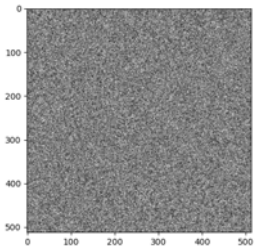
圖7 ： 8張512×512實驗影像



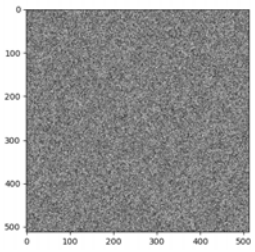
(a)原始影像



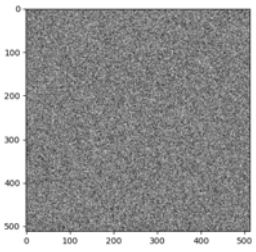
(b) 分享影像1



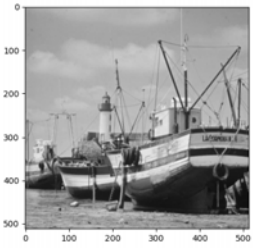
(c) 分享影像2



(d) 分享影像3

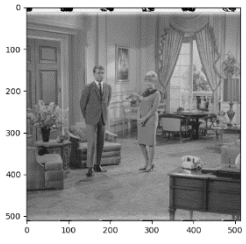


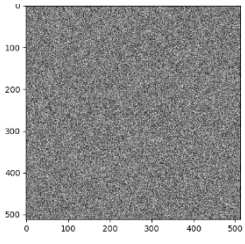
(e) 分享影像4

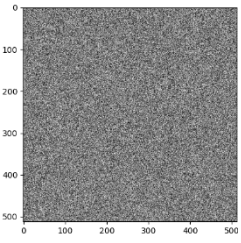


(f) 復原影像

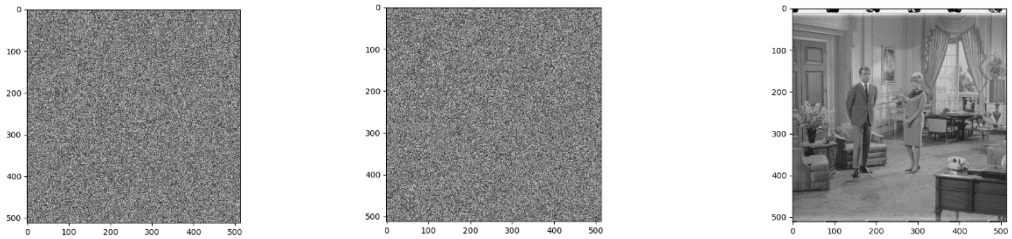
圖 8： Boat 影像的加密結果與影像復原







(a) 原始影像 (b) 分享影像 1 (c) 分享影像 2



(d) 分享影像 3 (e) 分享影像 4 (f) 復原影像

圖 9：Couple 影像的加密結果與影像復原

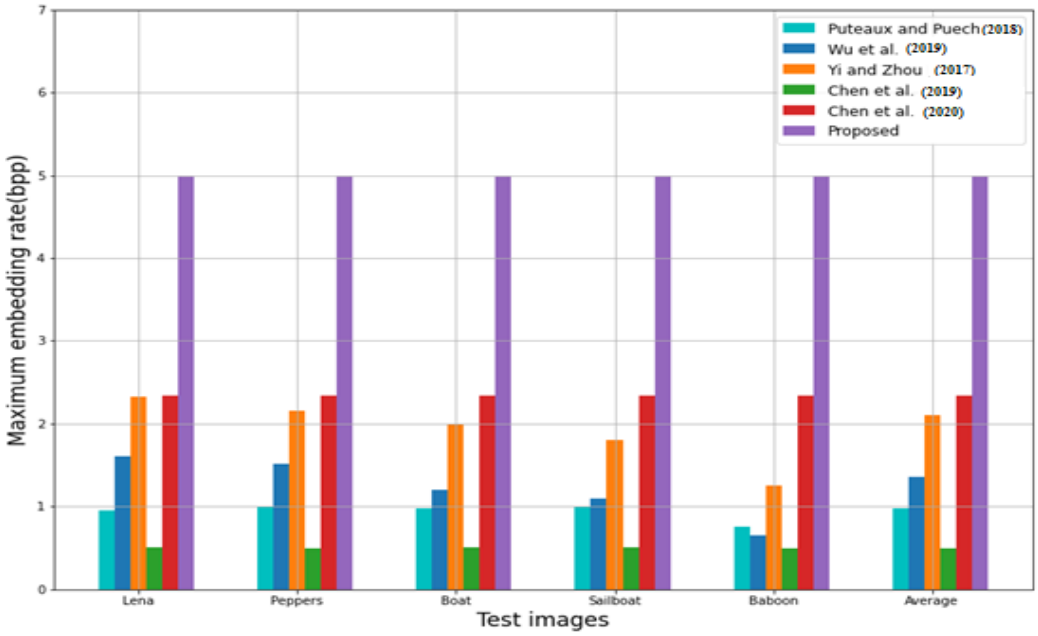


圖 10：最大嵌入率的比較結果

表 1 為本研究與其他學者之特徵比較，由此表中顯示我們的方法富有彈性，不需預先保留空間來嵌入機密訊息；而其他學者的方法，在執行嵌入機密訊息前需預先處理空間保留。一般而言，在資訊嵌入的過程中，分為影像擁有者、資訊隱藏者及接收者等三種角色。而在表 1 中的參與者為 Single，即表示影像擁有者和資訊隱藏者二者為同一個角色；而參與者為 Multiple，則表示影像擁有者和資訊隱藏者二者是不同的角色。

表 2 為嵌入量(bits)與嵌入率(bpp)的比較結果。在我們的方法中，由於實驗數據採用是 Shamir 學者(3, 3)門檻值機密分享的方式，一個二次方程式的係數最多可以嵌入 15 位元的機密資訊，因此一個影像最多可以嵌入$512 \times 512 \times 15 = 3{,}932{,}160$位元。此嵌入量會受到是否嵌入秘密資訊 S_{15} 或像素值是否≥ 251 而有些微影響。由於實驗圖形 Lena、Peppers、Boat、Sailboat、Baboon、Girl 其像素值皆< 251，所以其嵌入量達到 3,922,020 位元，而實驗圖形 Couple 和 Toys 因為有部分像素值≥ 251，因此其嵌入量稍微減少，圖 10 為表 2 所使用的顯示影像。我們可以用一個簡單的方式來評估我們的嵌入率，對一個 Shamir 學者(n, n)門檻值機密分享的方式，針對$n-1$次方程式的係數或常數項來嵌入像素值和機密資

訊，總共有 n 個係數或常數項。若像素值可以用一個係數來表示，其餘$n-1$個數值可以嵌入大約$7(n-1)$位元，因此嵌入率大約$\frac{7(n-1)}{n}$ bpp。此外，本研究利用秘密分享機制中的 Lagrange 運算來獲得多項式，並運用多項式中的係數值來回覆影像及秘密資訊。因為係數值完整的獲得，讓影像可以不失真和無錯誤的還原原始影像，故 PSNR=∞及錯誤率(error rate; ER)ER=0。

表 1：功能性比較表

方法	Separable	加密前是否預先保留空間	加密方式	參與者 (Data-hider)
方法 A (Puteaux and Puech 2018)	Yes	Yes	Stream cipher	Single
方法 B (Wu et al.et al. 2019)	Yes	Yes	Stream cipher	Single
方法 C (Yi and Zhou 2017)	Yes	Yes	Block permutation and modulation	Single
方法 D (Chen et al.et al. 2019)	No	Yes	Secret sharing	Single
方法 E (Chen et al.et al. 2020)	Yes	No	Secret sharing	Multiple
本研究方法	No	No	Secret sharing	Single

表 2：嵌入與影像還原的比較

實驗圖形	嵌入量(bits)	嵌入率 (bpp)	PSNR	ER
Lena	3,922,020	4.986	∞	0
Peppers	3,922,020	4.986	∞	0
Boat	3,922,020	4.986	∞	0
Sailboat	3,922,020	4.986	∞	0
Baboon	3,922,020	4.986	∞	0
Couple1	3,919,833	4.984	∞	0
Toys	3,922,014	4.986	∞	0
Girl	3,922,020	4.986	∞	0

伍、結論

本論文提出了一種基於 Shamir 學者所提出機密分享技術與多項式建構技巧的 RDHEI 技術，該技術將秘密資訊與原始像素以多項式的方式表示，並利用多項式來產生多個分享的像素，因此可以產生多張與原始影像相同大小的分享影像，每一張分享影像都呈現加密型態。以這種方式，即使一部分加密影像受到潛在的破壞，仍然可以透過從未損壞的加密影像中收集足夠的內容來重建原始影像與秘

密資訊。在現今 RDH 和 RDHEI 的技術十分多元的情況下，我們的方法也擁有相較之下較高的嵌入量且較富有彈性。

致謝

本研究承蒙科技部專題研究計畫（編號：MOST 108-2221-E-153-006, 108-2221-E-153-004-MY2, MOST 109-2221-E-153-004, 110-2221-E-153-002-MY2）與中山大學 TWISC(TWISC@NSYSU) 經費補助，以及評審寶貴意見，特此致謝。

參考文獻

Cao, X., Du, L., Wei, X., Meng, D. & Guo, X. (2016). High capacity reversible data hiding in encrypted image by patch-level sparse representation, *IEEE Transaction on Cybernetics*, 46(5), 1132-1143.

Celik, M.U., Sharma, G., Tekalp, A.M. & Saber, E. (2005). Lossless generalized-LSB data embedding, *IEEE Transactions on Image Processing*, 14(2), 253-266.

Chen, B., Lu, W., Huang, J., Weng, J. & Zhou, Y. (2020). Secret sharing based reversible data hiding in encrypted images with multiple data-hiders, *IEEE Transactions on Dependable and Secure Computing*, DOI: 10.1109/TDSC.2020.3011923.

Chen, Y.C., Hung, T.H., Hsieh, S.H. & Shiu, C.W. (2019). A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms, *IEEE Transactions on Information Forensics and Security*, 14(12), 3332-3343.

Fridrich, J., Goljan, M. & Du, R. (2002). Lossless data embedding for all image formats, *Proceedings of the International Society for Optical Engineering,* Vol. 4675, SPIE, 572-583.

Gao, G., Tonga, S., Xiaa, Z., Wu, B., Xu, L. & Zhao, Z. (2021). Reversible data hiding with automatic contrast enhancement for medical images, *Signal Processing*, 178, 107817.

Hong, W., Chen, T.S. & Wu, H.Y. (2012). An improved reversible data hiding in encrypted images using side match, *IEEE Signal Processing Letter*, 19(4), 199-202.

Khelifi, F. (2018). On the security of a stream cipher in reversible data hiding schemes operation in the encrypted domain, Signal Processing, 143, 336-345.

Luo, L., Chen, Z., Chen, M., Zeng, X. & Xiong, Z. (2010). Reversible image watermarking using interpolation technique, *IEEE Transactions on Information Forensics and Security*, 5(1), 187-193.

Ma, K., Zhang, W., Zhao, X., Yu, N. & Li, F. (2013). Reversible data hiding in encrypted images by reserving room before encryption, *IEEE Transaction on Information Forensics and Security*, 8(3), 553-562.

Ni, Z., Shi, Y., Ansari, N. & Su, W. (2006). Reversible data hiding, *IEEE Transaction on Circuits and Systems for Video Technology*, 16(3), 354-362.

Peng, F., Zhao, Y., Zhang, X., Long, M. & Pan, W.-Q. (2020). Reversible data hiding based on RSBEMD coding and adaptive multi-segment left and right histogram shifting, *Signal Processing: Image Communication*, 81(8), 115715.

Puteaux, P. & Puech, W. (2018). An efficient MSB prediction-based method for high -capacity reversible data hiding in encrypted images, *IEEE Transactions on Information Forensics and Security*, 13(7), 1670-1681.

Qin, C., Qian, X., Hong, W., & Zhang, X. (2019). An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer, *Information Sciences*, 487, 176-192.

Shamir, A. (1979). How to share a secret, *Communications of the ACM*, 22(11), 612–613.

Tai, W.L., Yeh, C.M. & Chang, C.C. (2009). Reversible data hiding based on histogram modification of pixel differences, *IEEE Transactions on Circuits and Systems for Video Technology*, 19(6), 906-910.

Tian, J. (2003). "Reversible Data Embedding Using a Difference Expansion, *IEEE Transaction on Circuits and System for Video Technology*, 13(8), 890-896.

Wang, Y., Cal, Z. & He, W. (2019). A New High Capacity Separable Reversible Data Hiding in Encrypted Images Based on Block Selection and Block-Level Encryption, *IEEE Access*, 7, 175671-175680.

Wu, H.T. & Huang, J. (2012). Reversible image watermarking on prediction errors by efficient histogram modification, *Signal Processing*, 92(12), 3000-3009.

Wu, H.T., Yang, Z., Cheung, Y.M., Xu, L. & Tang, S. (2019). High-capacity reversible data hiding in encrypted images by bit plane partition and MSB prediction, *IEEE Access*, 7, 62361-62371.

Wu, X., Weng, J. & Yan, W. (2018). Adopting secret sharing for reversible data hiding in encrypted images, *Signal Processing*, 143, 269–281.

Xuan, G., Yao, Q., Yang, C., Gao, J., Chai, Yun, P., Shi, Q. & Ni, Z. (2006). Lossless Data Hiding Using Histogram Shifting Method Base on Integer Wavelets, *Proceedings of International Workshop on Digital Watermarking,* Lecture Notes in Computer Science, Vol. 4283, Springer, 323-332.

Yi, S. & Zhou, Y. (2017). Adaptive code embedding for reversible data hiding in encrypted images, *Proceedings of IEEE International Conference on Image Processing (ICIP)*, IEEE, 4322-4326.

Yin, Z., She, X., Tang, J. & Luo, B. (2021). Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement, *Signal Processing*, 187, 108146.