Communications of the CCISA
Vol. 31 No. 2 May 2025

基於像素預測與空間保留在可逆式加密影像之資訊隱藏技術

楊政興[1]、翁麒耀[2*]、洪嘉伶[3]、吳胤霆[4]、王旭正[5]
[1]屏東大學電腦科學與人工智慧學系、[2,4]嘉義大學資訊工程系、
[3]陽明交通大學智能系統研究所、[5]中央警察大學資訊管理系
[1]chyang@mail.nptu.edu.tw, [2]cyweng@mail.ncyu.edu.tw, [3]vivian1728390@gmail.com,
[4]a31258114@gmail.com, [5]dopwang@gmail.com

摘要

可逆式資訊隱藏技術結合加密影像，不僅可以完整的還原原始影像且能保護掩護影像的安全性。Wang 等學者在 2022 年提出區塊預測的方式來保留空間。本篇論文改良 Wang 等學者所提出的方法，利用像素間的群組編碼及壓縮法來保留空間，以提高資訊隱藏的嵌入量。本研究先產生一張預測影像，並將影像分成多個不重疊群組，根據預測誤差的範圍使用霍夫曼編碼技術來標記每種群組類型。預測誤差範圍較小的群組使用較少的位元來表示，可產生較多空間。接著，再利用影像金鑰來加密影像，並將加密後的秘密訊息嵌入加密影像中的預留空間。在實驗數據的模擬中，我設定了不同的群組大小，並實驗了不處理特殊群組的實驗與處理特殊群組的實驗。由實驗結果可知，增加特殊群組的處理，即使多了需要紀錄 L 及 S 的代價，但 L 及 S 的長度小於多產生的空間，因此增加特殊群組處理可以產生更多空間。此外，我們也和相關研究做了實驗數據的比較，從比較的數據來看，本篇論文都有很好的效能。

關鍵詞：加密影像、群組編碼、霍夫曼編碼、預測誤差

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 31 No. 2 May 2025

Reversible data hiding in encrypted image using pixel prediction and room reservation

Cheng-Hsing Yang[1], Chi-Yao Weng[2*], Chia-Ling Hung[3], Yin-Ting Wu[4], Shiuh-Jeng WANG [5]

[1] Department of Computer Science and Artificial Intelligence, National Pingtung University, Pingtung 900, Taiwan,

[2,4] Department of Computer Science and Information Engineering, National Chiayi University, Chiayi 600, Taiwan,

[3]Institute of Artificial Intelligence Innovation, National Yang Ming Chiao Tung University, Hsinchu City 300, Taiwan

[5]Department of Information Management, Central Police University, Taoyuan City 333, Taiwan

[1]chyang@mail.nptu.edu.tw, [2]cyweng@mail.ncyu.edu.tw, [3]vivian1728390@gmail.com, [4]a31258114@gmail.com, [5]dopwang@gmail.com

Abstract

Reversible Data Hiding in Encrypted Images (RDHEI) not only enables complete restoration of the original image but also ensures the security of the stego image. Wang et al. proposed a block prediction method to preserve space in 2022. This paper improves upon Wang et al.'s approach by employing inter-pixel group coding and compression techniques to reserve more space for data hiding. The proposed method first generates a prediction image and divides it into non-overlapping groups. Based on the range of prediction errors, Huffman coding is used to label each group type. Groups with smaller prediction error ranges require fewer bits for representation, resulting in increased space for data hiding. Subsequently, the image is encrypted using a secret key, and the encrypted secret message is embedded into the reserved space within the encrypted image. In the experiments, various group sizes were tested for both special and regular groups. The results show that incorporating special group processing, even with the need to record identifiers L and S, can still yield more space overall while the combined size of L and S is smaller than the additional space generated. Furthermore, comparisons with related methods indicate that the proposed approach achieves superior performance.

Keywords: Encrypted Image, Grouping Encode, Huffman Encode, Prediction Error

壹、前言

隨著數位科技的蓬勃發展，資訊成為 21 世紀最關鍵的資產之一。無論是在電子商務、金融交易、智慧醫療或政府治理中，資訊的安全性都直接影響系統運作與信任機制。然而，隨著資通環境的複雜化，資訊安全面臨來自駭客攻擊、惡意程式與社交工程等多樣威脅。因此，深入瞭解資訊安全的核心概念、發展現況與保護措施，成為現代社會不可或缺的課題。於是有學者開始去研究資訊隱藏 (Data Hiding) 的技術，將機密資料嵌入於其他無害資訊之中，使其在不引人注意的情況下傳遞，是資訊安全領域中一種兼具隱密性與保密性的關鍵方法。與加密不同，資訊隱藏強調的是資料「不可察覺性」而非僅僅的「不可解讀性」。目前，資訊隱藏的應用已遍及數位浮水印 (Digital Watermarking)、隱寫術 (Steganography)、影像與音訊標記等多個領域，並在智慧財產權保護、軍事通訊與數位取證等方面發揮重要作用。隨著深度學習與多媒體處理技術的進步，資訊隱藏的演算法也日益精密與高效，對抗偵測技術與破壞攻擊的能力持續提升，成為資安防護體系中不可或缺的一環。

可逆式資訊隱藏 (Reversible Data Hiding, RDH) 是一種能將訊息嵌入到影像中，並能完全提取出訊息的技術。其目的是為了要保護訊息不被竊取，通常這項技術會用在醫療或軍事領域上。嵌入的方式大致可以分為以下幾種:直方圖移位 (Histogram Shifting)[6, 7]、差值擴張 (Difference Expansion,DE) [1,3,15]、預測誤差擴張 [8, 14] (Prediction Error Expansion,PEE)。直方圖移位是利用影像像素值的直方圖，選擇高頻出現的像素值作為嵌入點，透過移動相鄰像素值來騰出空間嵌入資訊。此方法具備良好的影像品質與低失真特性。差值擴張是透過計算相鄰像素間的差值，將差值進行擴張來嵌入資訊。該方法可提供較大的嵌入容量，但可能對影像品質造成較大影響。Tian 學者在 2003 年時提出差值擴張法的可逆式資訊隱藏技術 [15]，舉例來說，假設相鄰兩個像素值分別為 $x=106$ 及 $y=101$，計算其平均值 $l=\left\lfloor\frac{106+101}{2}\right\rfloor=103$ 與差值 $h=|106-101|=5$。將 h 擴展為 2 倍，再加上秘密位元 0 或 1，得到嵌入後的差值h'。假設秘密位元 $b=1$，則$h'=h\times 2+b=11$。最後，將差值h'分配給相鄰的兩個像素，$x'=103+\left\lfloor\frac{11+1}{2}\right\rfloor=109$，$y'=103-\left\lfloor\frac{11}{2}\right\rfloor=98$。由於此方法差異值在擴展後又嵌入訊息，因此嵌入後影像會造成較大的失真。預測誤差擴張是利用預測演算法估算像素值，再以實際值與預測值的差值為基礎進行嵌入，此技術可有效提升影像品質並保有較高的嵌入效率。

影像加密 (Image Encryption) 是一種將影像透過加密演算法處理後，使其變成無法用肉眼辨識的影像。目的是為了要保護影像的資料和特徵，通常這項技術會用在醫療或軍事領域上。影像加密的原理為影像持有者將要加密的影像用金鑰加密，然後傳給接收端。接收端在收到加密影像後，利用加密金鑰解密加密影像，即可將加密影像還原成原始影像。

在加密影像中執行可逆式資訊隱藏 (Reversible Data Hiding in Encrypted Image, RDHEI) 是一種將影像透過加密演算法處理後，將訊息嵌入到加密影像中的技術，目的

是為了保護訊息和影像的資訊 [2, 4, 5, 8-20]。其中嵌入的方式又分為加密前預留空間[8-10] (Reserving Room Before Encryption, RRBE) 和加密後騰出空間 [4, 16, 20] (Vacating Room After Encryption, VRAE)。加密前預留空間的做法是在影像加密前，先對影像進行處理，然後將訊息嵌入後，再進行影像加密。加密後騰出空間是先進行影像加密，然後在加密影像上騰出空間，讓訊息有空間嵌入。

本論文中，我們參考 Wang 等學者的方法 [17]，針對區塊內的所有像素的預測值，並依據此數值分類編碼及壓縮處理。為改善嵌入量效能，我們採取 RRBE 的方式，並且提出預測誤差編碼法的全新策略。我們的方法利用預測誤差範圍較小的群組使用較少的位元來表示，可產生較多空間。本論文其餘內容安排如下：第二節介紹相關方法，第三節介紹我們所提出的方法，第四節呈現我們的實驗數據和實驗成果，第五節為本文結論。

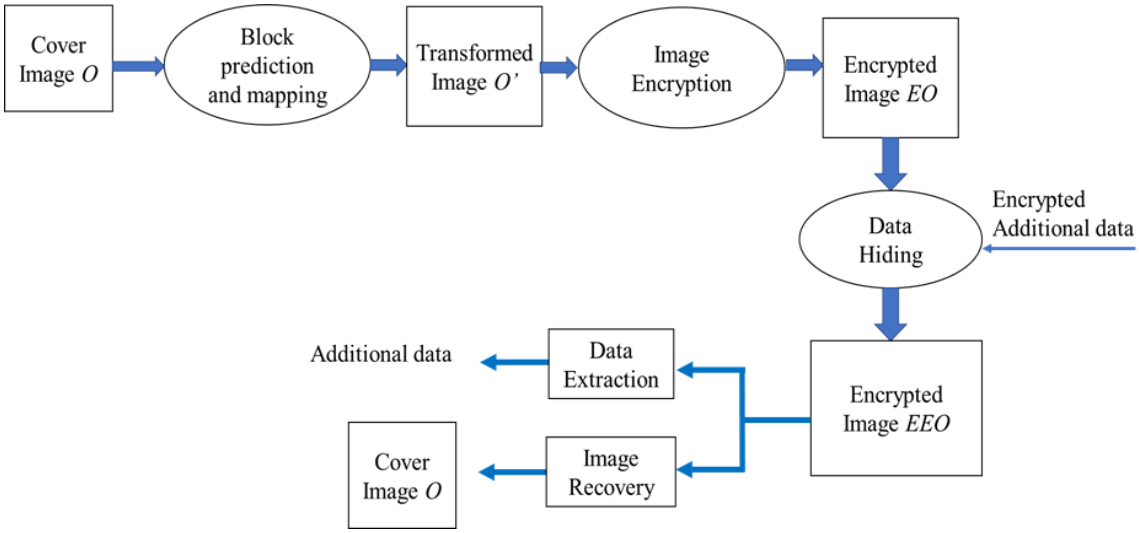
貳、文獻探討

本節中將介紹 Wang 等學者的方法 [17]，圖一為其方法的流程圖。首先，將原始影像 O 分成不重疊塊，如: 3×3 或 4×4。之後，將所有區塊內的像素值使用 MED 預測方式來計算預測誤差值，其中，每個區塊內會指定一個像素作為參考像素。所有區塊內的像素值皆計算完預測誤差值後，即可獲得區塊誤差值。

當相鄰像素值非常接近時，表示像素為有意義的影像，且預測誤差的值域分佈會趨近於拉普拉斯分佈，且數值愈接近 0。當區塊為平滑區時時，就可以用較少的位元來表示誤差值的範圍。接著，將區塊的誤差值分成 8 種不同的型態 (Type 1 ~ Type 8)，每一個型態有各自的規則。例如: Type 1:即表示誤差值為 0，且不需要額外的資訊來記錄誤差值；Type 2~ Type 7:每一位誤差值需要用ρ_n位元來記錄，因此可以保留$8-\rho_n$位元的空間；Type 8:即誤差值範圍為 $[-64,-127]$ 或 $[65,128]$，可用 8 個位元來記錄，但沒有剩餘空間可保留。最後，再利用霍夫曼編碼來記錄區塊的型態。

影像加密的方法則利用 Stream Cipher 加密方法來加密影像，如:用位元的方式和影像金鑰執行 XOR 運算，可獲得加密影像 EO。

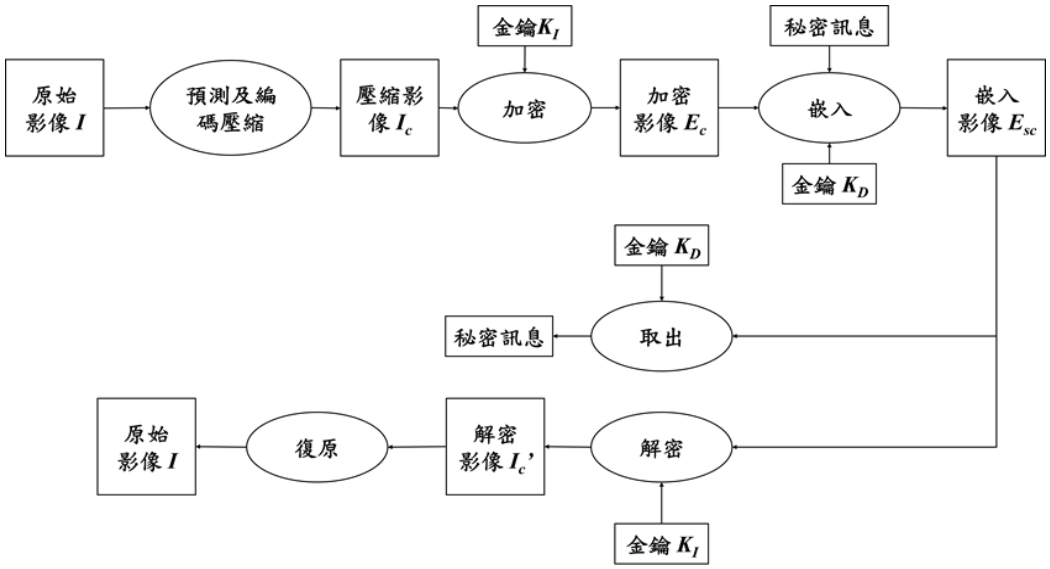
在資訊隱藏階段，為了增加訊息的安全性，在執行資訊隱藏前，先將機密訊息 (Additional Data) 加密，再將加密後的訊息，直接取代執行 Type 1 ~ Type7 所保留的空間。



圖一：整體方法流程圖

參、本篇方法

本節中我們提出一種加密影像中的可逆式資訊隱藏技術，圖二為本方法流程圖。首先，產生一張預測影像，並將影像分成多個不重疊群組，根據預測誤差的範圍，可以將所有群組分為八種類型，並使用霍夫曼編碼技術來標記每種群組類型。預測誤差範圍較小的群組使用較少的位元來表示，可產生較多空間，將編碼後的資訊產生影像復原的復原序列，然後使用影像金鑰 (Image Key) K_I 將影像加密，使用資料金鑰 (Data Key) K_D 將秘密訊息加密，並將加密後的秘密訊息嵌入加密影像中的空閒空間。圖二下半部為取出秘密訊息及復原影像的流程，根據擁有的金鑰分別可以復原影像及獲得秘密訊息。以下將詳細介紹我們的方法。



圖二：整體方法流程圖

3.1 預測及編碼壓縮

此小節針對圖二中的預測及編碼壓縮進行說明。給定一個大小為 $M \times N$ 的影像 I，其中 M 為影像高度、N 為影像寬度。第一列的所有像素，用其左邊的像素來預測，如公式 (1)、第一行的所有像素，用其上面的像素來預測，如公式 (2)、第一行及第一列以外的像素，用其上面的像素、左邊的像素及左上方的像素來預測，如公式 (3)。

$$\hat{P}(x,y) = P(x,y-1), \text{ if x = 1 and y > 1} \tag{1}$$

$$\hat{P}(x,y) = P(x-1,y), \text{ if x > 1 and y = 1} \tag{2}$$

$$\hat{P}(x,y) = \begin{cases} \min\big(P(x,y-1), P(x-1,y)\big), if P(x-1,y-1) \geq max\big(P(x,y-1), P(x-1,y)\big), \\ \max\big(P(x,y-1), P(x-1,y)\big), if P(x-1,y-1) \leq min\big(P(x,y-1), P(x-1,y)\big) \\ P(x,y-1) + P(x-1,y) - P(x-1,y-1), otherwise \end{cases} \tag{3}$$

上述公式中，$P(x,y)$代表座標位置 (x,y) 的像素值，$1 \leq x \leq M,\ 1 \leq y \leq N$，$\hat{P}(x,y)$代表$P(x,y)$的預測值。上述公式中，只有左上角的像素$P(1,1)$沒有被預測，我們設定 $\hat{P}(1,1)$ = 128。完成預測後，產生預測影像$\hat{I}$。

針對大小為 M×N 的原始影像 I 和預測影像$\hat{I}$，預測誤差 D 可以透過公式 (4) 計算。

$$D(x,y) = P(x,y) - \hat{P}(x,y) \tag{4}$$

其中$D(x,y)$代表座標位置 (x,y) 的預測誤差值，$P(x,y)$ 代表座標位置 (x,y) 的原始像素值，$\hat{P}(x,y)$ 代表 $P(x,y)$ 的預測值。

由左而右、由上而下，將預測誤差D分成大小為 $m \times m$ 的不重疊群組，假設總共分成k個群組，每個群組依序使用D_n，$n = 1, 2, \dots, k$，來表示。由於影像中鄰近像素值非常接近，因此預測誤差值常常接近 0，所以可以使用少於 8 位元來表示。我們以 0 為中心來劃分差值的範圍，若一個群組的所有差值落在範圍$\left(-2^{\lambda}, 2^{\lambda}\right]$內，$\lambda = -1, 0, 1, \dots, 8$，代表可以使用$\lambda + 1$個位元來表示此群組的所有差值；若一個群組的所有差值皆為 0，此時已確認所有差值為 0，所以無需紀錄。對於一個群組D_n，我們可以使用λ_n個位元來表示此群組的所有差值，公式 (5) 為λ_n的定義。表一為不同的λ值的預測誤差值範圍，以及其所包含的差值。

$$\lambda_n = min\{\lambda + 1 \mid \forall D_n(i,j) \in \left(-2^{\lambda}, 2^{\lambda}\right], 1 \leq i,j \leq m, \lambda = -1, 0, \dots, 8\} \tag{5}$$

其中$D_n(i,j)$ 表示群組D_n的座標位置 (i,j) 的預測誤差值。

根據每個群組D_n所需的位元長度λ_n，利用公式 (6) 將群組分為八種類型，$\mathcal{T}_n$代表群組D_n的類型。針對每個群組的類型，可以生成預測誤差編碼規則，如表二所示。

$$\mathcal{T}_n = \begin{cases} 1, & \lambda_n = 0 \\ 2, & \lambda_n = 1,2 \\ \lambda_n, & \lambda_n = 3,4,\dots,7 \\ 8, & otherwise \end{cases} \tag{6}$$

表一：預測誤差值的範圍與包含的差值

$\boldsymbol{\lambda}$	差值範圍	包含的預測誤差值
$\lambda = -1$	$(-2^{-1}, 2^{-1}]$	0
$\lambda = 0$	$(-2^{0}, 2^{0}]$	0,1
$\lambda = 1$	$(-2^{1}, 2^{1}]$	-1,0,1,2
$\lambda = 2$	$(-2^{2}, 2^{2}]$	-3,-2,...,3,4
$\lambda = 3$	$(-2^{3}, 2^{3}]$	-7,-6,...,7,8
$\lambda = 4$	$(-2^{4}, 2^{4}]$	-15,-14,...,15,16
$\lambda = 5$	$(-2^{5}, 2^{5}]$	-31,-30,...,31,32
$\lambda = 6$	$(-2^{6}, 2^{6}]$	-63,-62,...,63,64
$\lambda = 7$	$(-2^{7}, 2^{7}]$	-127,-126,...,127,128
$\lambda = 8$	$(-2^{8}, 2^{8}]$	-255,-254,...,255,256

表二：八種群組類型的預測誤差編碼規則

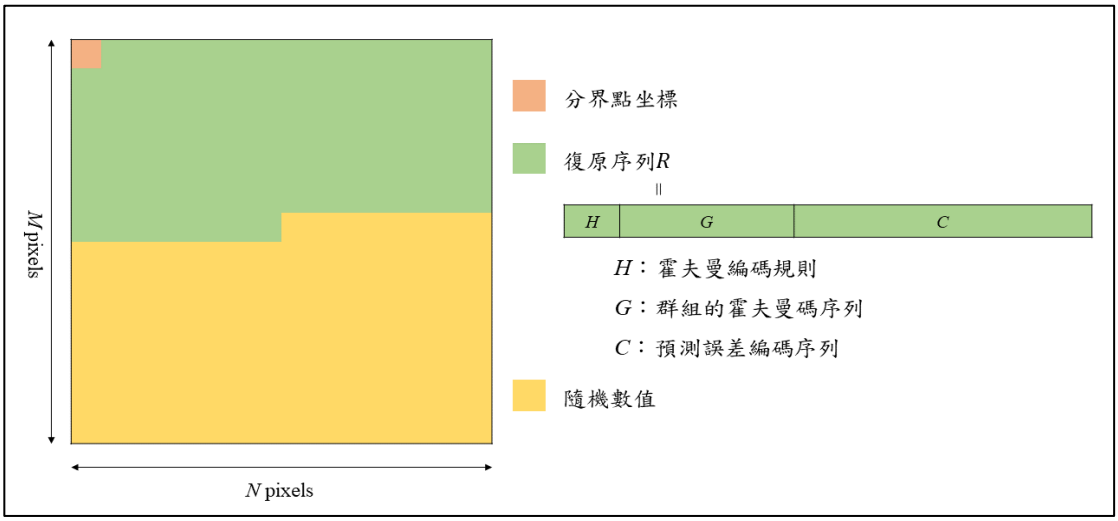
Group types	Prediction errors	Corresponding codes
$\mathcal{T}_n = 1$	0	–
$\mathcal{T}_n = 2$	-1,0,1,2	00,01,10,11
$\mathcal{T}_n = 3$	-3,-2,-1,...,4	000,001,010,...,111
$\mathcal{T}_n = 4$	-7,-6,-5,...,8	0000,0001,0010,...,1111
$\mathcal{T}_n = 5$	-15,-14,-13,...,16	00000,00001,00010,...,11111
$\mathcal{T}_n = 6$	-31,-30,-29,...,32	000000,000001,000010,...,111111
$\mathcal{T}_n = 7$	-63,-62,-61,...,64	0000000,0000001,0000010,...,1111111
$\mathcal{T}_n = 8$	otherwise	–

由於群組類型 1 的群組中所有預測誤差皆為 0，因此不需要進行編碼。針對群組類型 l 的群組，$2 \le l \le 7$，每個預測誤差需要 l 位元表示，以 $\mathcal{T}_n = 2$為例，預測誤差範圍為 [-2, 2]，使用 00,01,10,11 分別表示預測誤差-1, 0, 1, 2，其餘的$8 - 2 = 6$ 個位元可以被騰出。群組類型 8 的群組預測誤差需要使用 8 位元以上紀錄，因此針對類型 8 我們保留原始像素，使用 8 個位元記錄。假設群組D_n的預測誤差編碼序列為C_n，將所有C_n形成序列 $\mathrm{C} = C_1, C_2, \dots, C_n, \dots, C_k$。

我們採用霍夫曼編碼技術來記錄群組類型。針對影像中 8 種類型的群組之出現次數，產生霍夫曼的編碼，令 8 種群組類型的霍夫曼碼分別為h_τ，$\tau = 1,2,\ldots,8$，每個霍夫曼碼的長度為$|h_\tau|$。假設第 n 個群組D_n的群組類型之霍夫曼碼為G_n，影像中所有群組的霍夫曼碼序列為$G = G_1, G_2, \ldots, G_n, \ldots, G_k$。另外使用 3 位元紀錄$|h_\tau|$，並連接相應的$h_\tau$形成霍夫曼編碼規則$H$。

接著，將霍夫曼編碼規則H、霍夫曼碼序列G，以及預測誤差編碼序列C，依序連接形成復原序列 R ($R = H \| G \| C$)，根據復原序列R，我們可以無損的恢復原始影像。

我們將復原序列R放在影像最前面，其餘空閒的空間可以作為嵌入秘密訊息的空間。為了方便秘密訊息的嵌入和提取，必須知道從哪一個像素位置開始進行嵌入，所以必須知道影像中復原序列及秘密訊息之間的分界點，因此在大小為$M \times N$的影像中，我們使用$\log_2(M \times N)$個位元記錄分界點。圖三顯示原始影像I轉換為壓縮影像Ic的結果，其中壓縮影像 Ic 的前$\log_2(M \times N)$個位元用來存放分界點坐標，其後為復原序列R，並隨機使用 0 或 1 來填充其餘空閒的空間。



圖三：壓縮影像 *Ic* 組成圖

由於群組D_n可能發生只有一個預測誤差值 v 在範圍$(-2^\lambda, 2^\lambda]$中，其餘的預測誤差值均在範圍$(-2^{\lambda-1}, 2^{\lambda-1}]$中，我們稱此預測誤差值 v 為特殊的預測誤差值。此時，若將預測誤差值 v 修改為$v - 2^{\lambda-1}$或$v + 2^{\lambda-1}$，則所有的預測誤差值均在範圍$(-2^{\lambda-1}, 2^{\lambda-1}]$中。上述修改，在$\mathcal{T}_n = 3,4,\ldots,8$時，群組$D_n$的群組類型可以從$\mathcal{T}_n$變成$\mathcal{T}_n - 1$。因此，若我們對上述群組$D_n$的特殊預測誤差值做處理，可以更有效的壓縮$D_n$，增加更多空間。參照 Wang 等學者 [17] 的方法，我們稱具有上述特性的群組為特殊群組，其餘群組為一般群組。針對影像上的所有群組，我們使用"0"和"1"分別紀錄該群組為一般群組或特殊群組，這些紀錄形成 location map 稱為L。針對一個大小為$m \times m$的特殊群組D_n，$\mathcal{T}_n = 3,4,\ldots,8$，我們進行下面特殊處理：設定新的群組類型 $\mathcal{T}_n = \mathcal{T}_n - 1$，使用$m$位元表示該群組的哪個

像素值具有特殊預測誤差。當$m = 3$時，m位元只能表示 8 種情況，但是此時群組共有 9 個像素，因此若具有特殊預測誤差值的像素剛好為第 9 個像素時，我們將此群組視為一般群組。我們將所有特殊群組的m位元做串接，稱為資料S。接著，針對此特殊群組D_n，使用公式 (7) 計算新的特殊預測誤差值，其中 (x, y) 代表群組D_n中特殊預測誤差值的座標位置。

$$new\ D_n(x,y) = \begin{cases} D_n(x,y) + 2^{\mathcal{T}_n - 1}, if\ D_n(x,y) < 0 \\ D_n(x,y) - 2^{\mathcal{T}_n - 1}, if\ D_n(x,y) > 0 \end{cases} \quad (7)$$

，其中$\mathcal{T}_n = 2, 3, \dots, 7$為新的群組類型。

舉例來說，假設群組D_n的大小為 2 x 2，其預測誤差值由左而右由上而下依序為[v0, v1, v2, v3] = [-1, 0, 0, -3]，所有的預測誤差值都在範圍$(-2^2, 2^2]$內，此時$\mathcal{T}_n = 3$。由於只有一個誤差值 v3 $\in (-2^2, 2^2]$，其餘的誤差值 v0, v1, v2 $\in (-2^1, 2^1]$，所以D_n為一個特殊群組。我們進行特殊群組的處理，重新設定$\mathcal{T}_n = 3 - 1 = 2$，利用$m = 2$個位元紀錄特殊預測誤差值 v3 的位置，即位置 3，接著利用公式 (7) 計算新的特殊預測誤差值，new v3 = -3 + 22-1 = -1。所以D_n修改後的資訊，預測誤差值序列為[v0, v1, v2, v3] = [-1, 0, 0, -1]、$\mathcal{T}_n = 2$、修改位置為 3。回復時，因為$\mathcal{T}_n = 2$且修改位置的預測誤差值 v3 ≤ 0，所以回復的 v3 = -1 − 22-1 = -3。D_n回復後的資訊，預測誤差值序列為[v0, v1, v2, v3] = [-1, 0, 0, -3]。

上述所定義的特殊群組，只有針對$\mathcal{T}_n = 3, 4, \dots, 8$的群組$D_n$。然而，當$\mathcal{T}_n = 2$時，還是有機會修改一個誤差值，使得變成$\mathcal{T}_n = 1$。舉例說明，假設群組$D_n$的大小為 2 x 2，其預測誤差值序列為[v0, v1, v2, v3] = [0, 0, 0, 1]，此時$\mathcal{T}_n = 2$。然而，我們可以修改 v3，使得新的群組類型$\mathcal{T}_n = 2 - 1 = 1$，修改方式為 new v3 = 1 − 21-1 = 0，修改後的預測誤差值序列為[v0, v1, v2, v3] = [0, 0, 0, 0]。所以，我們增加$\mathcal{T}_n = 2$時的特殊群組之定義：若D_n的群組類型$\mathcal{T}_n = 2$，且存在唯一的特殊預測誤差值 v = 1，則D_n是一個特殊群組。此時，處理此特殊群組D_n的方式：設定新的群組類型 $\mathcal{T}_n = \mathcal{T}_n - 1$，使用$m$位元表示該群組的哪個像素值具有特殊預測誤差，接著，使用公式 (8) 計算新的特殊預測誤差值，其中 (x, y) 代表群組D_n中特殊預測誤差值的座標位置。

$$new\ D_n(x,y) = D_n(x,y) - 2^{\mathcal{T}_n - 1} \quad (8)$$

，其中$\mathcal{T}_n = 1$為新的群組類型。

特殊群組處理後可以產生更多空間嵌入訊息，復原序列R需增加L及S兩個序列，此時$R = H \parallel G \parallel L \parallel S \parallel C$。

3.2 影像加密與秘密訊息嵌入

此小節針對圖二中的加密與嵌入進行介紹，原始影像 I 預測及編碼壓縮後，產生壓縮影像 I_c，透過影像 I_c 前$\log_2(M \times N)$個位元可知嵌入秘密訊息的空間起點與秘密訊息嵌入量。我們使用加密金鑰 K_I 產生一組偽隨機亂數 X，使用公式 (9) 將壓縮影像 I_c 與 X

的數值透過 XOR 運算加密影像，生成一個加密影像 E_c。壓縮影像 I_c 的加密過程如下：

$$E_c(x, y) = I_c(x, y) \oplus X(x, y) \quad (9)$$

其中，$I_c(x, y)$是影像 I_c 的像素值，$X(x, y)$是偽隨機亂數，⊕代表 XOR 運算，$E_c(x, y)$為加密影像的像素值，(x, y) 代表座標。

若我們利用金鑰 K_I 產生一組與加密時相同的偽隨機亂數 X，並透過加密影像 E_c 與 X 的數值做 XOR 運算，可以將影像解密得到影像 I_c，解密過程如公式 (10)：

$$I_c(x, y) = E_c(x, y) \oplus X(x, y) \quad (10)$$

其中，$E_c(x, y)$為加密影像的像素值，$X(x, y)$是偽隨機亂數，$I_c(x, y)$是解密後的影像像素值，(x, y) 代表座標。

影像 I_c 前$\log_2(M \times N)$個位元紀錄復原序列及秘密訊息之間的分界點座標，當秘密訊息嵌入時可以得知從哪裡開始嵌入秘密訊息及可以嵌入多少位元的秘密訊息，因此影像加密時不加密影像 I_c 前$\log_2(M \times N)$個位元的訊息。

透過加密影像 E_c 的前$\log_2(M \times N)$個位元可以得知秘密訊息嵌入起點，接著開始由左而右、由上而下，依序將秘密訊息嵌入於加密影像 E_c 中，秘密訊息透過金鑰 K_D 加密，將所有秘密訊息嵌入後，生成一張已嵌入秘密訊息之加密影像 E_{sc}。

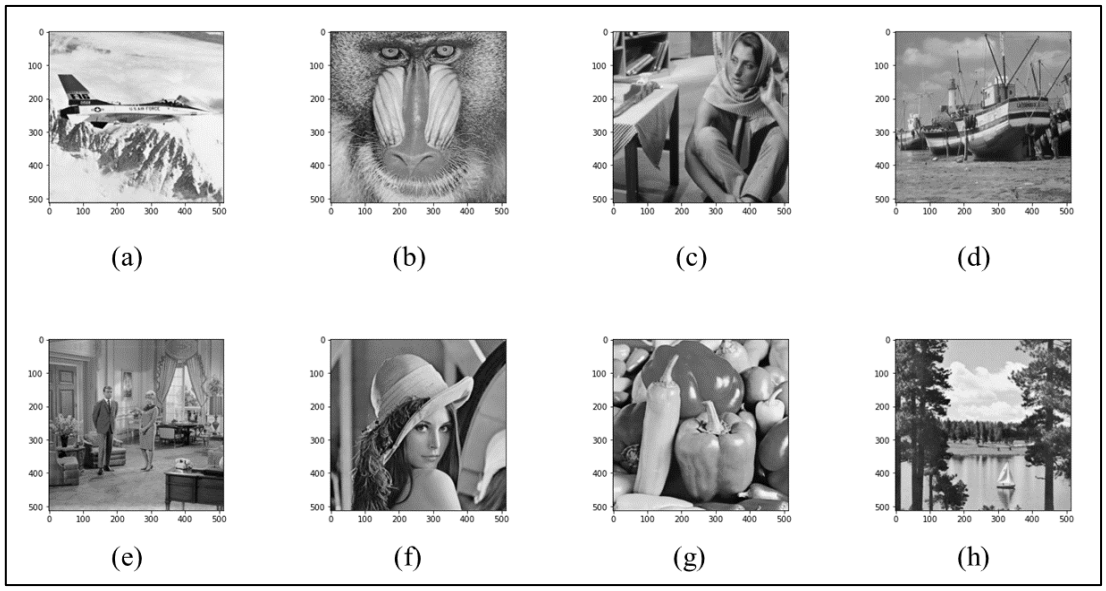
3.3 取出秘密訊息、解密、復原影像

此小節針對圖二中取出、解密、復原進行說明，影像接收者根據是否擁有資料金鑰 (Data Key) K_D 和影像金鑰 (Image Key) K_I，可以將分為三種類型。

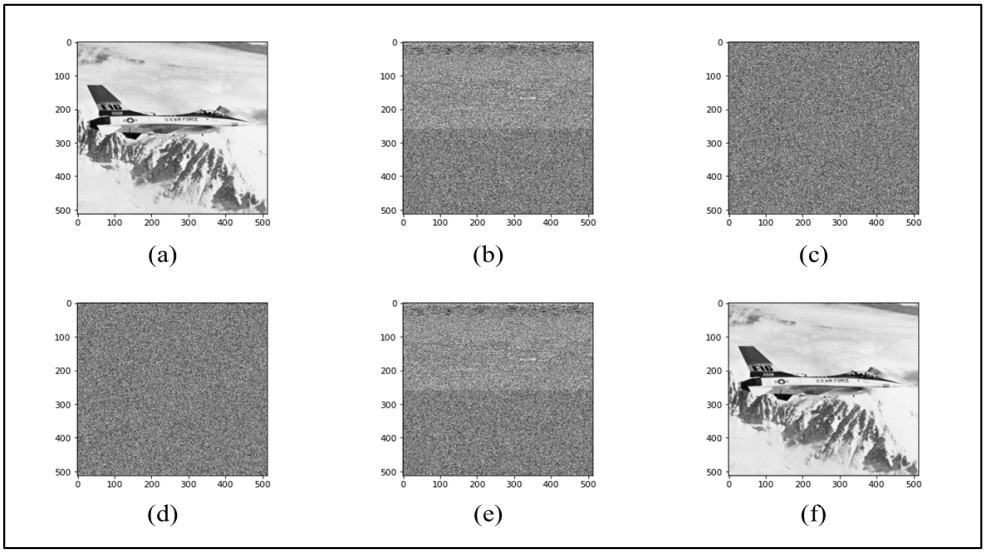
- 第一種接收者只擁有資料金鑰 K_D，可透過影像 E_{sc} 的前$\log_2(M \times N)$ 個位元得知秘密訊息嵌入起點，並由左至右、由上至下，從復原序列及秘密訊息之間的分界點座標開始，提取加密後的秘密訊息，再將提取出的秘密訊息透過資料金鑰 K_D 進行解密，獲得完整的秘密訊息。
- 第二種接受者只擁有影像金鑰 K_I，利用影像金鑰 K_I 透過公式 (9) 對嵌入秘密訊息的加密影像 E_{sc} 進行解密，獲得影像 I_c'，並由影像 E_{sc} 的前$\log_2(M \times N)$ 個位元得知復原序列ℝ及秘密訊息之間的分界點，透過復原序列 R 資訊將影像回復為原始影像 I。
- 第三種接受者同時擁有資料金鑰 K_D 與影像金鑰 K_I，可以取出秘密訊息和回復原始影像 I。

肆、實驗成果與數據分析

本節中我們將進行實驗數據分析，圖四為本次使用的 8 張實驗影像，並針對 8 張實驗影像，將原始影像分為 2×2、3×3、4×4 大小的群組，分別做了不處理特殊群組的實驗與處理特殊群組的實驗。



圖四：8 張實驗原始影像；(a) Airplane、(b) Baboon、(c) Barbara、(d) Boat、(e) Couple、(f) Lena、(g) Peppers、(h) Sailboat



圖五：Airplane 的實驗結果：(a)原始影像、(b)壓縮影像、(c)加密影像、(d)嵌入秘密訊息之加密影像、(e)解密影像、(f)復原後的影像

圖五為 Airplane 的實驗結果，我們將影像群組大小設為 2x2，圖五(a)為原始影像 I，圖五 (b)為壓縮後的影像 I_c，圖五(c)為加密後的影像 E_c，圖五(d)為已嵌入秘密訊息之加密影像 E_{sc}，圖五(e)為解密後的影像 I_c'，圖五(f)為復原的影像 I，其中圖五(a)及圖五(f)完全相同。由實驗結果可知，我們的方法可以完整提取出藏於影像的秘密訊息，並且將影像復原為原始影像。

表二為群組大小設為 2×2 時，影像 Airplane 的群組類型數目、類型指標。表三為群

組大小設為 2×2 時，經過特殊群組處理後，影像 Airplane 的群組類型數目、類型指標。表四為影像 Airplane 在群組大小設為 2×2、3×3、4×4 時，分別做了不處理特殊群組的實驗與處理特殊群組的實驗數據。由於實驗影像大小為 512×512，當群組大小為 3×3 時，無法整數切割整個影像，此時最右邊和最下面剩餘的影像，使用群組大小為 2×2 來切割。

表二：群組大小設為 2×2 時，影像 Airplane 的群組類型數目、類型指標

Image		**Type1**	**Type2**	**Type3**	**Type4**	**Type5**	**Type6**	**Type7**	**Type8**
Airplane	Amount	428	13080	19951	16682	8990	4846	1496	63
	h_τ	010001	00	11	10	011	0101	01001	010000
	$\|h_\tau\|$	6	2	2	2	3	4	5	6

表三：群組大小設為 2×2 時，經過特殊群組處理後，影像 Airplane 的群組類型數目、類型指標

Image		**Type1**	**Type2**	**Type3**	**Type4**	**Type5**	**Type6**	**Type7**	**Type8**
Airplane	Amount	1332	23595	19391	11889	6233	2705	383	8
	h_τ	110001	0	10	111	1101	11001	1100001	1100000
	$\|h_\tau\|$	6	1	2	3	4	5	7	7

表四：不同方法中 Airplane 的實驗相關數據

Approaches	$\|H\|$	$\|G\|$	**特殊群組數量**	$\|L\|$	$\|S\|$	$\|C\|$	$\|R\|$	**嵌入率 (bpp)**
2x2	54	156,206	0	0	0	950,980	1,107,240	**3.7762**
2x2-特殊群組處理	59	147,230	33,782	65,536	67,564	812,244	1,092,633	**3.8319**
3x3	54	71,224	0	0	0	1,055,465	1,126,743	**3.7018**
3x3-特殊群組處理	54	69,353	10,509	29,241	31,363	961,466	1,091,477	**3.8363**
4x4	54	39,855	0	0	0	1,126,600	1,166,509	**3.5501**
4x4-特殊群組處理	54	39,532	5,649	16,384	22,596	1,036,232	1,114,798	**3.7474**

表五為針對 8 張實驗影像的嵌入率比較，我們將群組大小設為 2x2、3x3 及 4x4，並做了不處理特殊群組的實驗與處理特殊群組的實驗。由實驗結果可知，增加特殊群組的處理，即使多了需要紀錄L及S的代價，但L及S的長度小於多產生的空間，因此增加特殊

群組處理可以產生更多空間。

表五：8 張實驗影像在不同方法下的嵌入率比較

	4×4	4×4-特殊群組處理	3×3	3×3-特殊群組處理	2×2	2×2-特殊群組處理
Airplane	3.5501	3.7474	3.7018	3.8363	3.7762	3.8319
Baboon	1.4503	1.6244	1.5808	1.7035	1.6373	1.6693
Barbara	2.5532	2.7088	2.6544	2.7940	2.6320	2.6535
Boat	2.5337	2.7036	2.6943	2.8011	2.7882	2.8047
Couple	2.7450	2.9580	2.9304	3.0653	3.0402	3.0807
Lena	3.1450	3.3213	3.2868	3.3997	3.3635	3.3979
Peppers	2.7114	2.8668	2.8641	2.9607	2.9432	2.9548
Sailboat	2.2924	2.4623	2.4132	2.5442	2.4936	2.5191
Average	2.6227	2.7991	2.7657	2.8881	2.8343	2.8565

表六為我們的方法將群組大小設為 3×3 並處理特殊群組時，與文獻 [2,9,11-13,18,19] 的嵌入率比較，根據實驗結果，我們的方法平均相較之前的方法擁有更多嵌入空間，具有更好的結果。在表六中的文獻 [17] 之數據，為了增加嵌入量，Wang 等學者將 location map L 進行壓縮。但是在我們的數據中，為了單純顯示方法的效能，我們並沒有壓縮 L 來增加嵌入空間。

表六：我們的方法與文獻[2,9,11-13,18,19]的嵌入率比較

	[9]	[2]	[12]	[18]	[19]	[13]	[11]	[19]	**我們的方法**
Airplane	1.2577	1.3672	0.9831	2.2524	3.0045	2.1543	2.7871	3.5719	3.8363
Baboon	0.3865	0.4523	0.8383	1.3406	1.0679	0.8623	1.1973	1.7349	1.7035
Barbara	0.6713	0.8453	0.9734	1.8435	1.8064	1.1853	1.9895	2.5979	2.7940
Boat	0.6586	0.9108	0.9632	1.7423	2.1323	1.6751	2.1617	2.7945	2.8011
Couple	0.6673	0.9594	0.9768	1.6284	2.3851	1.6018	2.0454	2.7507	3.0653
Lena	0.9507	0.7421	0.9774	2.0864	2.5771	1.8533	2.5968	3.3557	3.3997
Peppers	0.6603	0.7248	0.9762	2.1471	2.1774	1.8909	2.5463	3.2045	2.9607
Sailboat	0.6386	0.8011	0.979	1.9716	2.0551	1.7375	2.2598	2.8830	2.5442
Average	0.7032	0.8527	0.9621	1.8996	2.1131	1.5933	2.1916	2.8534	2.8881

伍、結論

本篇論文改良 Wang 等學者在 2022 年所提出區塊預測法，利用計算預誤差值的方式來保留空間。本論文將預測誤差 D 分成不重疊群組，將每個群組D_n分為八種類型的編碼規則，再針對影像中 8 種類型的群組之出現次數，產生霍夫曼的編碼。接著，將霍夫曼編碼規則、霍夫曼碼序列，以及預測誤差編碼序列，依序連接形成復原序列，根據復原序列，就可以無損的恢復原始影像。在實驗的數據呈現，本篇方法平均相較之前的方法擁有更多嵌入空間，具有更好的結果。在表六中的相關研究的比較數據，為了增加嵌入量，Wang 等學者將 location map L 進行壓縮。但是在我們的數據中，為了單純顯示方法的效能，我們並沒有壓縮 L 來增加嵌入空間。因此，本篇論文所預先保留的嵌入空間皆高於先前的研究。

[誌謝]
本研究成果承蒙國家科學及技術委員會計畫補助，計畫編號 :NSTC 112-2221-E-153-003 和 NSTC 113-2221-E-324-017-MY2，特此感謝。

參考文獻

[1] A. Arham and H.A. Nugroho, “Enhanced reversible data hiding using difference expansion and modulus function with selective bit blocks in images”. *Cybersecurity*, vol. 7, pp. 61, 2024.

[2] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” *IEEE Transactions on Cybernetics*, vol. 46, pp. 1132-1143, 2016.

[3] C. Dragoi and D.Coltuc, “Local-prediction-based difference expansion reversible watermarking”, *IEEE Trans. Image Process*., vol. 23, no. 4, pp. 1779-1790, 2014.

[4] I.C. Dragoi and D. Coltuc, “Reversible Data Hiding in Encrypted Images Based on Reserving Room After Encryption and Multiple Predictors,” *2018 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2018.

[5] P.S. Gomathi, S. Sindumathi, and B. Kalaavathi, “Reserving room before encryption for reversible data hiding with scan encryption,” *International Journal of Applied Engineering Research*, vol. 10, no. 3, pp. 8231-8239, 2015.

[6] W. Hong; C.W. Shiu; and T.S. Chen, “A high quality histogram shifting based embedding technique for reversible data hiding,” *2008 Eighth International Conference on Intelligent Systems Design and Applications*,2008.

[7] Y. Jia, Z. Yin, X. Zhang, and Y. Luo, “Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting,” *Signal Processing* 163, pp. 238-246,2019.

[8] Z. Li, L. Lu, G. Fan, P. Li, and Z. Pan, “Prediction-error expansion based reversible data

hiding via diamond search fusion and pairing," *Signal Processing*, vol. 230, pp. 109858, 2025.

[9] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 553-562, 2013.

[10] A. Mohammadi, "A general framework for reversible data hiding in encrypted images by reserving room before encryption," *Journal of Visual Communication and Image Representation*, vol. 85, pp. 103478, 2022.

[11] A. Mohammadi, M. Nakhkash, and M.A. Akhaee, "A high-capacity reversible data hiding in encrypted images employing local difference predictor," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, pp. 2366-2376, 2020.

[12] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security*, vol.13, pp. 1670-1681, 2018.

[13] P. Puteaux and W. Puech, "A recursive reversible data hiding in encrypted images method with a very high payload," *IEEE Transactions on Multimedia*, vol. 23, pp. 636-650, 2021.

[14] W. Qi, T. Zhang, X. Li, B. Ma, and Z. Guo, "Reversible data hiding based on prediction-error value ordering and multiple-embedding," *Signal Processing*, vol. 207, pp. 108956, 2023.

[15] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technology*, vol. 13, pp. 890-896, 2003.

[16] V. Venkatesh, R. Anushiadevi, P. V. Meikandan, H. Mahalingam, and R. Amirtharajan,, "Separable reversible data hiding by vacating room after encryption using encrypted pixel difference," *Scientific Reports*,vol. 15, pp. 11916, 2025.

[17] [8]. X. Wang , C.C. Chang , C.C. Lin , and C.C. Chang, "On the multi-level embedding of crypto-image reversible data hiding," *Journal of Visual Communication and Image Representation*, vol. 87, pp. 103556 , 2022.

[18] S. Yi and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Transactions on Multimedia*, vol. 21, pp. 51-64, 2019.

[19] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Transactions on Multimedia*, vol. 22, pp. 874-884, 2020.

[20] C. Yu, X. Zhang, G. Li, S. Zhan, and Z. Tang, "Reversible data hiding with adaptive difference recovery for encrypted images," *Information Sciences*, vol. 584, pp. 89-110, 2022.