# 中間對折變動藏入位元內插技術

呂慈純 林美辰 呂侑靜
朝陽科技大學副教授 朝陽科技大學研究生 朝陽科技大學研究生
tclu@cyut.edu.tw s10214608@gm.cyut.edu.tw yuching1120@gmail.com

## 摘要

Jung 和 Yoo 學者於 2009 年提出影像放大技術，該方法使用相鄰像素將影像預測放大至原始大小的 2 倍大，再將影像切割成 2x2 的區塊，每個區塊依左上角的像素計算差值，再依據差值將機密訊息嵌入於放大後產生的像素之中。Jung 和 Yoo 的方法每個像素的藏入位元數是固定的，該方法並沒有充分利用影像鄰近像素非常相似，可以藏入較多位元的特性，因此本研究擬利用鄰近像素的變異程度來判斷每個像素可以藏入的位元數。本研究首先使用影像放大技術，計算每個影像區塊的變異程度，統計變異數後，區分區塊級別，再依據區塊級別將不同位元數機密訊息切割並嵌入於預測像素中。針對機密訊息部份，本研究使用中間對折策略，該策略將機密訊息從中間對折，成為有正有負的數值，使其在嵌入時減少對影像品質的破壞程度。

**關鍵字**：可逆式資訊隱藏、影像內插技術、中間對折策略、變異數

## Abstract

Jung and Yao proposed a image interpolation technique in 2009 which uses the neighboring pixel values and expands a prediction image for two times and then divided the image into 2*2 blocks, non-overlapping , Before hiding secret message can be calculated the difference on the upper left in each block and hide the secret message into the predicted pixel. However , in their method each pixel can embed secret bits is regular, and their method have the advantage in similar pixels so that can hiding secret message more but they don't use this feature so this study use the neighboring pixel of variance level to judge the payload. At first ,this study use the image interpolation technique and compute the variance degree in each block and then statistics the variance and separate the block level Last, according to the block level hiding the secret message into the predicted pixel for different bits. Focus on the part of secret message, we use the center folding strategy to folding the secret message from center so that let the secret message have positive and negative values and increase the quality when hiding.

**Keywords**: reversible data hiding、neighbor mean Interpolation、center folding strategy、variance

## 1. 前言

隨著網際網路的發展，許多人透過網路將資訊傳送給不同的人，比如文宣、照片、病歷、公司資料等等。但在網路上傳送資料並非是安全的，資料有可能被不法第三者從中攔截竊取並竄改破壞，使得較為私密的資料因此洩密。為了確保傳送資料的安全性，有學者提出資訊隱藏概念，將訊息嵌入於媒體之中，產生出偽裝媒體，因偽裝媒體與原始媒體並無太大差異，故可躲過不法第三者攻擊，將較為私密的訊息安全地傳送至對方手中。

在使用資訊隱藏技術時須滿足三個條件：安全性、不可察覺性、高資訊負載量。安全性指得是傳送方將訊息嵌入於影像之中，產生出的偽裝影像必須只有接受方可以將訊息取出；不可察覺性指得是當訊息嵌入於影像之中，產生的偽裝影像不可有扭曲、變形與失真的狀況，使得不法第三者察覺進而攔截訊息；高資訊負載量則是指在相同的影像品質之下，嵌入最多的機密訊息。但此條件又與不可察覺性互相抵觸，故如何在兩者兼顧的情況下尋找平衡點，是當今學者研究的重點。

資訊隱藏依偽裝影像是否可還原成原始影像分為可逆式與不可逆式兩種類別。可逆式資訊隱藏是指訊息嵌入於偽裝影像之後，可再取出訊息後將偽裝影像還原成原始型態；反之，不可還原的稱之為不可逆式資訊隱藏。在可逆式資訊隱藏研究方面，有許多較為著名的技術，像是直方圖位移技術、差異擴張技術、影像內插技術[7][9][13]等等。

直方圖位移技術是較為常見的技術， Ni 學者於 2006 年首先提出此技術[11]，該方法先統計影像中的所有像素值，從中找到出現頻率最高和最低的兩個像素值，分別作為峰值點與零值點，將峰值至零值間的像素往零值點進行直方圖位移，以挪出可嵌入訊息的空間，並將機密訊息嵌入於峰值點中。該方法雖然執行簡單，但資訊負載量卻不高。針對此問題，學者們提出利用預測值與原始像素的差值進行的直方圖位移技術，藉此提高峰值點的數量以提升資訊負載量[2][3][5][6][11] [16]。另一種常見技術為差異擴張技術，該技術是利用像素與像素間的差異進行擴張，並將機密訊息嵌入於差異之中。Tian 學者於 2003 年首先提出此技術，他將兩個相鄰像素擴張成兩倍，再將一個位元的機密訊息嵌入[15]；為了增加該方法的嵌入量，Alatter 學者於 2004 年提出修改方法，他延伸 Tian 學者的方法，將四個鄰近的像素的差異擴張成兩倍之後，將三個位元的的機密訊息嵌入其中[1]。該技術由於將差異倍數擴張，在平滑影像因差異值不大，擴張後受破壞程度不大，但在複雜影像因差異值大，在數倍擴張後則會造成嚴重的失真。因此針對該問題，學者們也做了許多的改良[8][12][14] 。

另一項新興技術為影像內插技術。該技術將影像放大成原始的 2 倍大小，並將機密訊息嵌入於放大後產生的虛構像素中。Jung 和 Yoo 學者於 2009 年首先提出了影像插值法（Neighbor Mean Interpolation, NMI）[7]；Lee 和 Huang 學者於 2012 年提出相鄰像素插值法（Interpolation by Neighboring Pixels, INP）[9]；以及 Tang 等學者於 2014 年提出的的高藏量可逆式隱寫術（High Capacity Reversible Steganography，CRS）[13]。該類方法產生的偽裝影像為原始影像的兩倍大，在取出機密訊息時只需從虛構像素中提取，再將影像縮小即可還原成原始影像。但該類方法所產生的偽裝影像較易有鋸齒狀殘影的問題，且嵌入量也較少，因此本研究擬改良先前影像放大技術，針對只能嵌入固定位元，限制藏量的問題進行改善，採用的方式是利用像素變異數分析區塊複雜度。

所提方法使用影像放大技術，利用 Jung 和 Yoo 學者提出的 NMI 技術放大影像，並切割可重疊的區塊計算變異數，統計整體影像變異數再將區塊分級，依據區塊級別將不同位元的機密訊息切割，再嵌入於虛擬預測值中。而針對機密訊息的部份，本研究使用 Lu 等學者於 2015 年提出的中間對折策略壓縮機密訊息[10]，藉此提升影像品質。

本研究架構如下，第二章為文獻探討，詳細介紹 NMI 技術（第 2.1 節）、INP 技術（第 2.2 節）、CRS 技術（第 2.3 節）以及中間對折策略（第 2.4 節）；第三章將說明本研究的嵌入、取出流程與範例；第四章將會探討實驗結果；第五章將對研究進行結論與分析。

## 2. 文獻探討

### 2.1 影像插值法(NMI)

Jung 和 Yoo 學者於 2009 年提出影像插值法(Neighbor Mean Interpolation, NMI)[7]。影像插值法流程如圖 1 所示，圖 1(a)為影像大小 H×W 的原始影像。Jung 和 Yoo 學者將原始影像縮小為縮小影像(圖 1(b))，其大小為原始影像的四分之一($\frac{H}{2}\times\frac{W}{2}$)。縮小影像的水平與垂直的任兩個像素中會插入一個預測像素，完成後可得到如圖 1(c)影像大小 H×W 的預測影像。將機密訊息嵌入於預測像素中形成圖 1(d)偽裝影像。接收方在取得偽裝影像後，將影像縮小，透過取出流程即可取得機密訊息和一張縮小影像。

像素放大示意圖如圖 2 所示，圖 2(a)為 4 × 4 影像區塊，縮小時使用四個角落像素做為基準將影像縮小為 2 × 2 區塊，此區塊亦做為原始區塊使用(圖 2(b))。每兩個像素之間插入一個預測像素得到 $P^{NMI}$ 預測區塊(圖 2(c))。計算每個預測像素 $P^{NMI}$ 的差異值，將機密訊息嵌入於每個預測像素之中以獲得圖 2(d)偽裝影像。

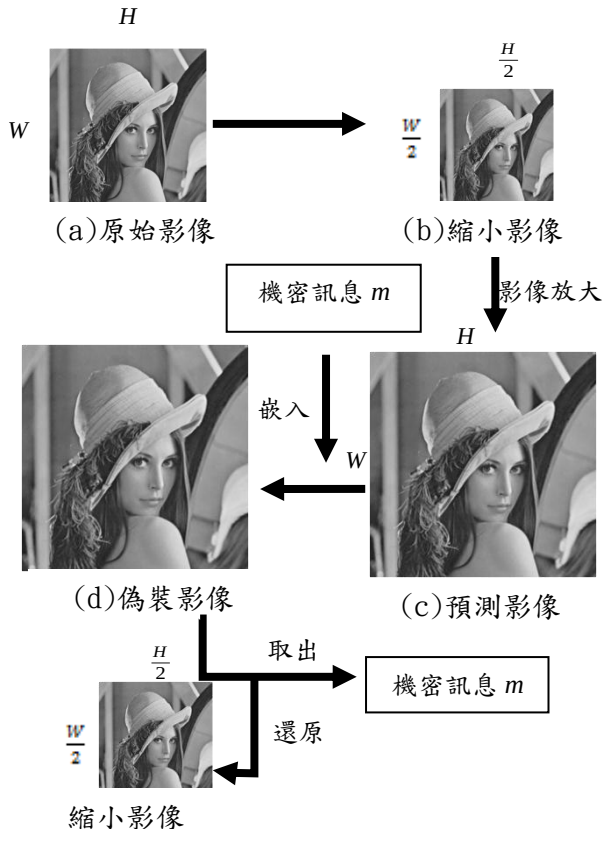



**圖 1 影像插值法流程圖**

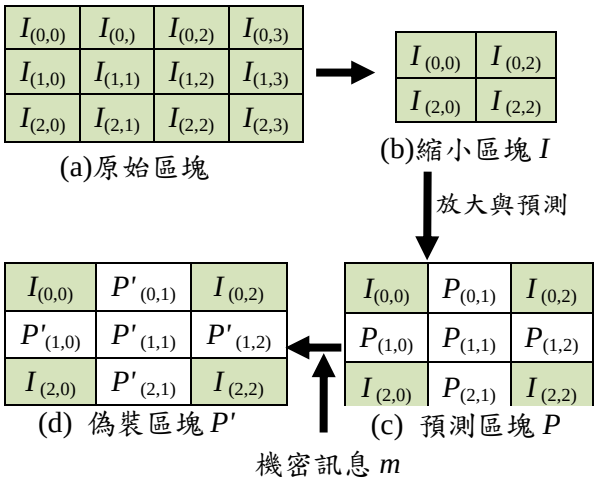



**圖 2 影像放大與嵌入示意圖**

$P^{\mathrm{NMI}}$ 的計算方式是透過使用影像插值法公式，該公式是將鄰近像素進行平均，以作像素預測值，其公式如下：

$$P^{\mathrm{NMI}}_{(i,j)}=\begin{cases}\left\lfloor\dfrac{\left(I_{(i,j-1)}+I_{(i,j+1)}\right)}{2}\right\rfloor, & \text{if } i=2h,\ j=2w+1,\\ \left\lfloor\dfrac{\left(I_{(i-1,j)}+I_{(i+1,j)}\right)}{2}\right\rfloor, & \text{if } i=2h+1,\ j=2w,\\ \left\lfloor\dfrac{\left(I_{(i-1,j-1)}+P^{\mathrm{NMI}}_{(i-1,j)}+P^{\mathrm{NMI}}_{(i,j-1)}\right)}{3}\right\rfloor, & \text{otherwise.}\end{cases} \quad (1)$$

公式(1)中，h 與 w 為影像區塊內的高與寬，i 與 j 為像素的位置。當預測值 符合第一個條件 i=2h, j=2w+1 時，將相鄰左右兩個像素相加平均取下限；當預測值 符合第二個條件 i=2h+1, j=2w 時，則將相鄰上下兩個像素相加平均取下限；若預測值符合第三個條件，則將當前預測值位置的上方與左方兩個像素與左上角原始像素相加平均取下限。舉例來說，假設 I（0,0）=156、I（0,2）=160、I（2,0）=159 及 I（2,2）=161，如圖 3(a)所示；假設機密訊息 M = (110010)2；透過公式(1)計算預測值 $P^{\mathrm{NMI}}_{(0,1)}$ 、 $P^{\mathrm{NMI}}_{(1,0)}$ 和 $P^{\mathrm{NMI}}_{(1,1)}$ 可得到 $P^{\mathrm{NMI}}_{(0,1)}=\lfloor(156+160)/2\rfloor=158$ ；$P^{\mathrm{NMI}}_{(1,0)}=\lfloor(156+159)/2\rfloor=157$ ；中間預測值 $P^{\mathrm{NMI}}_{(1,1)}\lfloor(158+157+156)/3\rfloor=157$ 。重覆以上動作直到計算出所有預測值即可得到一張預測影像，如圖 3(b)所示。將三個預測值 $P^{\mathrm{NMI}}_{(0,1)}$ 、$P^{\mathrm{NMI}}_{(1,0)}$ 和 $P^{\mathrm{NMI}}_{(1,1)}$ 與左上角的原始像素 I（0,0）相減，得到 $d_1^{\mathrm{NMI}}$ 、$d_2^{\mathrm{NMI}}$ 與 $d_3^{\mathrm{NMI}}$ 三個差異值，其公式如下所示：

$$\begin{aligned} d_1^{\mathrm{NMI}} &= \left|P^{\mathrm{NMI}}_{(0,1)} - I_{(0,0)}\right|,\\ d_2^{\mathrm{NMI}} &= \left|P^{\mathrm{NMI}}_{(1,0)} - I_{(0,0)}\right|,\\ d_3^{\mathrm{NMI}} &= \left|P^{\mathrm{NMI}}_{(1,1)} - I_{(0,0)}\right|. \end{aligned} \quad (2)$$

延續上面的例子可得 $d_1^{\mathrm{NMI}}$ =|158-156|=2，$d_2^{\mathrm{NMI}}$ =|157-156|=1，$d_3^{\mathrm{NMI}}$ =|157-156|=1。再將差異值 $d^{\mathrm{NMI}}$ 進行 log 運算，其結果為機密訊息長度 $n^{\mathrm{NMI}}$ ，公式如下所示：

$$\begin{aligned} n_1^{\mathrm{NMI}} &= \left\lfloor \log_2\left(d_1^{\mathrm{NMI}}\right)\right\rfloor,\\ n_2^{\mathrm{NMI}} &= \left\lfloor \log_2\left(d_2^{\mathrm{NMI}}\right)\right\rfloor,\\ n_3^{\mathrm{NMI}} &= \left\lfloor \log_2\left(d_3^{\mathrm{NMI}}\right)\right\rfloor. \end{aligned} \quad (3)$$

將上方的例子 $d^{NMI}$ 帶入公式(3)，得到 $n_1^{NMI}=\lfloor \log_2(2) \rfloor=1$，$n_2^{NMI}=\lfloor \log_2(1) \rfloor=0$ 和 $n_3^{NMI}=\lfloor \log 2(1) \rfloor=0$。其中 $n_2^{NMI}$=0 與 $n_3^{NMI}$=0，表示該對應預測值 $P_{(1,0)}^{NMI}$ 與 $P_{(1,1)}^{NMI}$ 不嵌入機密訊息。而 $n_1^{NMI}$=1 則表示其對應預測值 $P_{(0,1)}^{NMI}$ 將嵌入 1 個位元的機密訊息。從機密訊息 M 切割 1 個位元的機密訊息並轉置成十進制，得到 m=(1)10，再將 m 嵌入於 $P_{(0,1)}^{NMI}$ 中得到 $P'^{NMI}_{(0,1)}$：$P_{(0,1)}^{NMI}$ = +m=158+1=159。以此類推，嵌入所有的機密訊息，最後可得到如圖 3(c)結果。

| | |
|---|---|
| 156 | 160 |
| 159 | 161 |

(a) 縮小像素

| | | |
|---|---|---|
| 156 | 158 | 160 |
| 157 | 157 | |
| 159 | | 161 |

(b) NMI 預測結果

| | | |
|---|---|---|
| 156 | 159 | 160 |
| 157 | 157 | |
| 159 | | 161 |

(c) 偽裝像素

**圖 3　Jung 和 Yoo 藏入範例**

## 2.2 相鄰像素插值法(INP)

Lee 和 Huang 學者於 2012 年相鄰像素插值法（Interpolation by Neighboring Pixels, INP）[9]。該方法如同 NMI 一樣，先將縮小影像放大得到預測影像，再藏入機密訊息以得到偽裝影像。但預測值 的計算則略為不同，該值利用相鄰像素插值法計算，將相鄰的 2 個像素相加取平均後，加上縮小像素 I（0,0），再重取得平均值作為像素預測值，公式如下所示：

$$P_{(i,j)}^{INP}=\begin{cases}\left\lfloor \dfrac{\left(I_{(i,j-1)}+\left(I_{(i,j-1)}+I_{(i,j+1)}\right)/2\right)}{2} \right\rfloor, & \text{if } i=2h, j=2w+1,\\ \left\lfloor \dfrac{\left(I_{(i-1,j)}+\left(I_{(i-1,j)}+I_{(i+1,j)}\right)/2\right)}{2} \right\rfloor, & \text{if } i=2h+1, j=2w,\\ \left\lfloor \dfrac{\left(P_{(i-1,j)}^{INP}+P_{(i,j-1)}^{INP}\right)}{2} \right\rfloor, & \text{otherwise.}\end{cases} \quad (4)$$

使用章節 2.1 的範例舉例，假設 I（0,0）=156、I（0,2）=160、I（2,0）=159 及 I（2,2）=161，透過公式(4)計算出預測值 $P_{(0,1)}^{INP}$、$P_{(1,0)}^{INP}$ 以及 $P_{(1,1)}^{INP}$ 以及 $P_{(1,1)}^{INP}$ 。

$$P_{(0,1)}^{INP}=\left\lfloor \left(I_{(0,0)}+\left(I_{(0,0)}+I_{(0,1)}\right)/2\right)/2 \right\rfloor=\left\lfloor \left(156+\left(156+160\right)/2\right)/2 \right\rfloor=157$$

$$P_{(1,0)}^{INP}=\left\lfloor \left(I_{(0,0)}+\left(I_{(0,0)}+I_{(1,0)}\right)/2\right)/2 \right\rfloor=\left\lfloor \left(156+\left(156+159\right)/2\right)/2 \right\rfloor=156$$

中間像素預測值計算只需將 $P_{(0,1)}^{INP}$ 與 $P_{(1,0)}^{INP}$ 相加平均，其計算方法為：$P_{(1,1)}^{INP}=\lfloor (157+156)/2 \rfloor=156$ ，其結果如圖 4(a)所示。

得到預測影像後，計算差異值 $d_1^{INP}$ 、$d_2^{INP}$ 與 $d_3^{INP}$。在計算差異值之前，需先計算不會隨意更動的固定值 B，該值使用四個角落像素中的最大值，做為與預測值相減的基礎，藉此提高嵌入量，其公式如下所示：

$$B=\max\left(I_{(0,0)},I_{(0,2)},I_{(2,0)},I_{(2,2)}\right). \quad (5)$$

透過公式(5)選擇最大值做為與預測值相減的依據，延續本節例子：B=max（156,157,160,162）=162，將 B 值與預測值相減，得到差距，公式如下所示：

$$\begin{aligned} d_1^{INP}&=\left|B-P_{(0,1)}^{INP}\right|,\\ d_2^{INP}&=\left|B-P_{(1,0)}^{INP}\right|,\\ d_3^{INP}&=\left|B-P_{(1,1)}^{INP}\right|. \end{aligned} \quad (6)$$

使用公式(6)，套入例子中，可得到 $d_1^{INP}$=|162-157|=5，$d_2^{INP}$=|162-156|=7，$d_3^{INP}$=|162-156|=6。再將差異值 $d^{INP}$ 進行 log 運算以取得機密訊息長度 $n^{INP}$，得到 $n_1^{INP}=\lfloor \log_2(5) \rfloor=2$，$n_2^{INP}=\lfloor \log_2(7) \rfloor=2$ 以及 $n_3^{INP}=\lfloor \log_2(6) \rfloor=1$。由於 $n_1^{INP}$、$n_2^{INP}$、$n_3^{INP}$ 皆等於 2，所以將機密訊息 M 各自切割 2 個位元並轉置成十進制 m 機密符號後，嵌入於相對應預測值 $P_{(0,1)}^{INP}$、$P_{(1,0)}^{INP}$ 以及 $P_{(1,1)}^{INP}$ 之中，得到 $P'^{INP}_{(0,1)}=P_{(0,1)}^{INP}+m_1=157+3=160$ 、$P'^{INP}_{(1,0)}=156$ 、$P'^{INP}_{(1,1)}=158$ ，結果如圖 4(b)所示。

| | | |
|---|---|---|
| 156 | 157 | 160 |
| 156 | 156 | |
| 159 | | 161 |

(a) INP 預測結果

| | | |
|---|---|---|
| 156 | 160 | 160 |
| 156 | 158 | |
| 159 | | 161 |

(b) 嵌入後結果

**圖 4　INP 嵌入範例**

## 2.3 高藏量可逆式隱寫術(CRS)

Tang 等學者於 2014 年提出高藏量可逆式

隱寫術（High Capacity Reversible Steganography，CRS）[13]。該方法在計算預測值前，需先從四個角落像素中選擇最大值 Imax 與最小值 Imin，其公式如下所示：

$$I_{\max} = \max\left(I_{(0,0)}, I_{(0,2)}, I_{(2,0)}, I_{(2,2)}\right),$$
$$I_{\min} = \min\left(I_{(0,0)}, I_{(0,2)}, I_{(2,0)}, I_{(2,2)}\right). \quad (7)$$

使用章節 2.1 例子，根據公式(7)計算得到該區塊 Imax=max(156, 160, 159, 161)=161；Imin=min(156, 160, 159, 161)=156。依據 Imax 與 Imin 計算參考值 AD，AD 值使用該區塊四個角落像素的最大值與最小值，因此計算出該區塊的預測值也較為準確，公式如下所示：

$$AD = \left(3 \times I_{\min} + I_{\max}\right) / 4. \quad (8)$$

使用公式(8)得到 AD=(3x156+161)/4=157.25。依參考值 AD 與相鄰像素取平均後計算預測值，其公式如下所示：

$$P_{(i,j)}^{CRS} = \begin{cases} \left\lfloor \frac{\left(AD + \left(I_{(i,j-1)} + I_{(i,j+1)}\right)/2\right)}{2} \right\rfloor, & \text{if } i = 2h, j = 2w+1, \\ \left\lfloor \frac{\left(AD + \left(I_{(i-1,j)} + I_{(i+1,j)}\right)/2\right)}{2} \right\rfloor, & \text{if } i = 2h+1, j = 2w, \\ \left\lfloor \frac{\left(I_{(i+1,j-1)} + P_{(i-1,j)}^{CRS} + P_{(i,j-1)}^{CRS}\right)}{3} \right\rfloor, & \text{otherwise.} \end{cases} \quad (9)$$

將上面例子代入公式(9)，得到 $P_{(0,1)}^{CRS} = \left\lfloor \left(157.25 + (156+160)/2\right)/2 \right\rfloor = 157$，$P_{(1,0)}^{CRS} = \left\lfloor \left(157.25 + (156+159)/2\right)/2 \right\rfloor = 157$。$P_{(1,1)}^{CRS}$ 計算方式則同 NMI 算法，使用上方與左方預測值加上左上縮小像素平均取下限得到：$P_{(0,1)}^{CRS} = \left\lfloor (157+157+156)/3 \right\rfloor = 156$。其預測結果如圖 5(a)所示。該方法同樣也是依據差異值 $d^{\text{CRS}}$ 將機密訊息嵌入於預測值 $P^{CRS}$ 之中，但該方法差異值 $d^{\text{CRS}}$ 會依據預測值 $P^{CRS}$、最大值 *Imax* 以及最小值 *Imin* 平均數決定其計算方式，公式如下所示：

$$d_1^{\text{CRS}} = \begin{cases} I_{\max} - P_{(0,1)}^{\text{CRS}}, & \text{if } P_{(0,1)}^{\text{CRS}} < \left(I_{\min} + I_{\max}\right)/2, \\ P_{(0,1)}^{\text{CRS}} - I_{\min}, & \text{if } P_{(0,1)}^{\text{CRS}} \geq \left(I_{\min} + I_{\max}\right)/2. \end{cases}$$
$$d_2^{\text{CRS}} = \begin{cases} I_{\max} - P_{(1,0)}^{\text{CRS}}, & \text{if } P_{(1,0)}^{\text{CRS}} < \left(I_{\min} + I_{\max}\right)/2, \\ P_{(1,0)}^{\text{CRS}} - I_{\min}, & \text{if } P_{(1,0)}^{\text{CRS}} \geq \left(I_{\min} + I_{\max}\right)/2. \end{cases}$$
$$d_3^{\text{CRS}} = \begin{cases} I_{\max} - P_{(1,1)}^{\text{CRS}}, & \text{if } P_{(1,1)}^{\text{CRS}} < \left(I_{\min} + I_{\max}\right)/2, \\ P_{(1,1)}^{\text{CRS}} - I_{\min}, & \text{if } P_{(1,1)}^{\text{CRS}} \geq \left(I_{\min} + I_{\max}\right)/2. \end{cases} \quad (10)$$

延續上方例子代入公式(10)，得到 $d_1^{\text{CRS}}$=161-157=4，$d_2^{\text{CRS}}$=161-157=4 以及 $d_3^{\text{CRS}}$=161-156=5 再將三個差異值分別進行 log 運算，求各自預測值預計嵌入的機密訊息位元長度，$n_1^{CRS} = \left\lfloor \log_2(4) \right\rfloor = 2$，$n_2^{CRS} = \left\lfloor \log_2(4) \right\rfloor = 2$ 以及 $n_3^{CRS} = \left\lfloor \log_2(5) \right\rfloor = 2$。切割機密訊息長度並轉至成十進制後，使用減法方式嵌入於預測值之中，即可完成嵌入程序，結果如圖 5(b)所示。

| | | |
|---|---|---|
| 156 | 157 | 160 |
| 157 | 156 | |
| 159 | | 161 |

(a) CRS 預測結果

| | | |
|---|---|---|
| 156 | 160 | 160 |
| 157 | 158 | |
| 159 | | 161 |

(b) 嵌入後結果

**圖 5　CRS 嵌入範例**

### 2.4 中間對折策略

Lu 等學者於 2015 年提出了中間對折策略(Center Folding Strategy)[10]。該策略是針對機密訊息部份進行對折處理。假設一個像素將被嵌入 k 個位元的機密訊息，其值域變化將是 0 至 2k-1。嵌入時位元數 k 越大，像素的變動程度越大，影像破壞程度也越嚴重。Lu 等學者提出了中間對折策略將機密訊息從中對折，使訊息變成一個有正有負的數值，在相同值域下嵌入訊息最大變化量縮減一半，使影像品質破壞程度降低。其概念如圖 6 所示。*m* 為原始機密訊息，在減去中間值 2k-1 後，轉成對折後機密訊息 $\tilde{m}$。

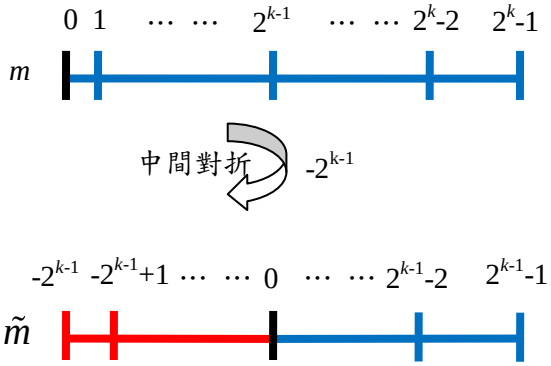



**圖 6　機密訊息對折示意圖**

本研究結合影像放大技術與中間對折策略，並評估區塊特性嵌入適量的機密訊息長度。在預測與放大流程，於章節 2.1、2.2、2.3 介紹的三個方法，預測方法略有不同。Jung 和 Yoo 學者提出的 NMI 在預測放大時參考像素僅以左右相鄰像素平均計算；Lee 和 Huang 學者所提出的 INP 為求更精準，以每個區塊左上角的像素為基準進行預測放大；Tang 等學者

提出的 CRS 則依每個區塊最大值與大小值設置一個基準值以進行放大預測。

本研究擬用其中一個方法執行放大程序，比較三種預測方法產生的預測影像影像品質，選擇品質破壞程度最低的方案。影像品質比較方面，本研究使用高峰影像訊號雜訊比（Peak Signal to Noise Ratio, PSNR）進行實驗測量。其公式如下所示：

$$\mathrm{PSNR} = 10 \times \log_{10}\left[\frac{\left(2^{\mathrm{bit}}-1\right)^2}{\frac{1}{w \times h} \times \sum_{i=0}^{w-1}\sum_{j=0}^{h-1}\left(x_{(i,j)} - x'_{(i,j)}\right)^2}\right](\mathrm{dB}), \quad (11)$$

假設將一張 512x512 影像使用三個方法預測放大成三張 1024x1024 影像，則沒有可以比較影像品質的標準。為解決此難題，本研究將一張 512x512 縮小為 256x256 的影像，再將之預測放大成 512x512 的預測影像，依預測影像與原始影像進行 PSNR 比較。實驗圖使用平滑影像 Lena 與複雜影像 Mandrill 進行測試，其結果如表 1 所示：

表 1 NMI、INP、CRS 預測影像與原始影像 PSNR 比較 (單位：dB )

| Image | NMI[7] | INP[9] | CRS[13] |
|---|---|---|---|
| Lena | 32.55 | 30.69 | 30.59 |
| Mandrill | 22.88 | 22.10 | 22.36 |

由表 1 可知，影像不管屬於平滑或複雜，NMI 在影像品質上都優於另外兩個方法，且越平滑的影像效果越明顯。故本研究使用 NMI 為影像放大策略。

## 3. 研究方法

本研究透過章節 2.1 NMI 預測方法進行影像放大與預測，將影像切割成重複的 3x3 區塊，計算每個區域的變異數，並統計變異數決定每個區域需嵌入一至四個位元的機密訊息至預測值 P(i,j)之中，同時使用中間對折策略儘可能縮小影像失真程度，以下將詳細說明嵌入流程。

### 3.1 嵌入階段

將影像依章節 2.1 方法預測放大，產生一張預測影像。再將影像切割成重複的 3x3 區塊 B，計算該區堆的變異數，如圖 7 所示。

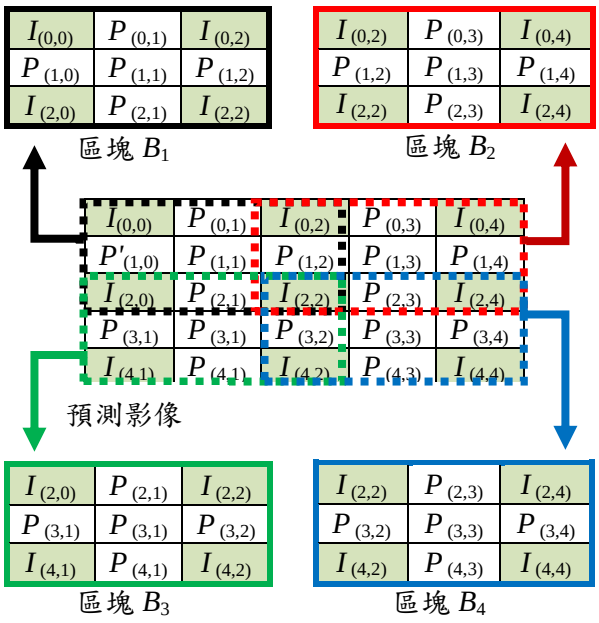



**圖 7　切割影像示意圖**

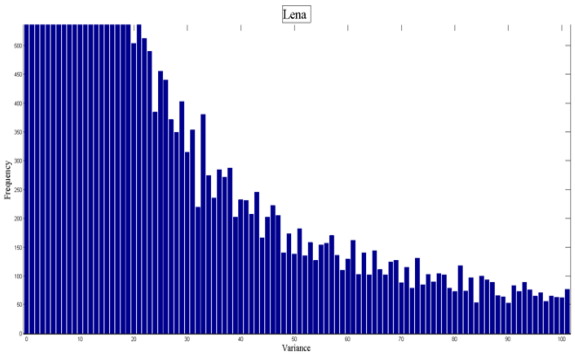
依序計算每一個區塊 B 變異數，其計算方式如下所示：

$$B_n^{avg} = \left\lfloor \frac{I_{lu} + I_{ru} + I_{ld} + I_{rd}}{4} \right\rfloor, \quad (12)$$

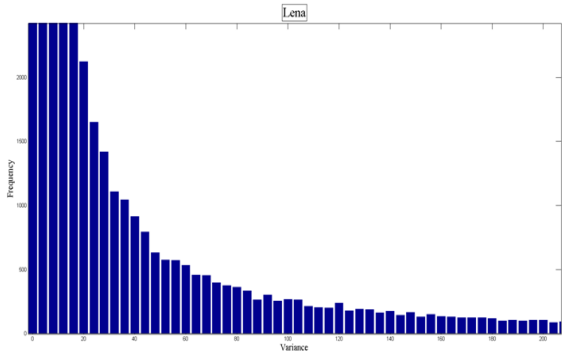
$$B_n^{var} = \left\lfloor \frac{\left(I_{lu} - B_n^{avg}\right) + \left(I_{ru} - B_n^{avg}\right) + \left(I_{ld} - B_n^{avg}\right) + \left(I_{rd} - B_n^{avg}\right)}{4} \right\rfloor. \quad (13)$$

22.88　22.10

公式中 *Ilu*、*Iru*、*Ild*、*Ird* 分別代表區塊 B 中左上、右上、左下、右下四個角落像素值，n 為區域編號。首先依公式(12)計算區塊平均值 $B_n^{avg}$，再依據公式(13)計算區域變異數 $B_n^{\mathrm{var}}$。變異數越小，代表區塊特性越平坦；反之當變異數越大時，區塊特性則越複雜。依序將整張影像區塊計算變異數。再統計所有變異數，彙整影像各區塊變異數出現的次數。由於變異數可能產生 0、1、2…∞種可能，進行門檻值設置不易。因此本研究藉由簡化統計表，透過將數值相近的變異數 4 個為一組，如變異數 0~3 設為群組 0、4~7 設為群組 4…等等，以減少門檻值設定的困難度，如圖 8 所示。




(a)未簡化變異數直方圖




(b)簡化後變異數直方圖

**圖 8　未簡化變異數直方圖與簡化變異數直方圖**

由圖 8(a)可知，未簡化變異數直方圖參差不齊，簡化後變異數直方圖 8(b)則較為平順。依據簡化後的變異數直方圖設置三個門檻植，分別是：T1、T2、T3。變異數群組數最多者設置為 T1，群組數最少且數值最小者設置 T3，T2 則為 T1 與 T3 的平均。若區域變異數 $B_n^{\text{var}}$ 小於等於 T1，該區域嵌入機密訊息長度 k 為 1 位元；若區域變異數 $B_n^{\text{var}}$ 介於 T1 與 T2 之間，機密訊息長度 k 為 2 位元；介於 T2 與 T3 之間，機密訊息長度 k 為 3 位元；大於 T3 則嵌入 4 個位元的機密訊息。如公式(14)所示：

$$k=\begin{cases}1, & \text{if } B_n^{\text{var}} \le T_1,\\ 2, & \text{if } T_1 < B_n^{\text{var}} \le T_2,\\ 3, & \text{if } T_2 < B_n^{\text{var}} \le T_3,\\ 4, & \text{if } B_n^{\text{var}} > T_3.\end{cases} \tag{14}$$

機密訊息嵌入於各個區塊的預測值 P 之中，依據公式(14)決定機密訊息 m 的位元長度。在嵌入流程方面，本研究結合機密訊息對折策略，將機密訊息折半以減少影像失真程度。而在嵌入時，難免會產生溢位的發生，為防止溢位的發生，本研究改變機密訊息嵌入的方向，公式如下所示：

$$P'=\begin{cases}P+m, & \text{if } P \le 2^{k-1}-1,\\ P+(m-2^{k-1}), & \text{if } 2^{k-1}-1 < P \le 255-2^{k-1}+1,\\ P-m, & \text{if } P > 255-2^{k-1}+1.\end{cases} \tag{15}$$

若是預測值 P 小於 $2^{k-1}-1$，機密訊息不進行中間對折策略，因為機密訊息對折後會產生有正負的數值，反而會造成下溢位（underflow）的發生；當預測值 P 介於 2k-1-1 到 $255-2^{k-1}+1$ 之間，則將機密訊息做中間對折再嵌入；當預測值 P 小於時，因為可能會產生上溢位（overflow）不將機密訊息進行對折，再反方向嵌入於預測值之中。以此類推將機密訊息嵌入於所有預測值中即可產生偽裝影像。

### 3.2 取出流程

接收方會收到一張偽裝影像，只需透過這張偽裝影像即可取出機密訊息。因為在影像放大、預測、嵌入時，每個區塊的角落像素是沒有變動的，所以仍然是原始像素。因此可以透過這個特性，將偽裝影像縮小後，再使用相同的方式將影像放大與預測，再統計變異數分析當初設定門檻值，以得知每個區塊嵌入的機密訊息長度 k，以此取出機密訊息，流程圖如圖(9)所示。

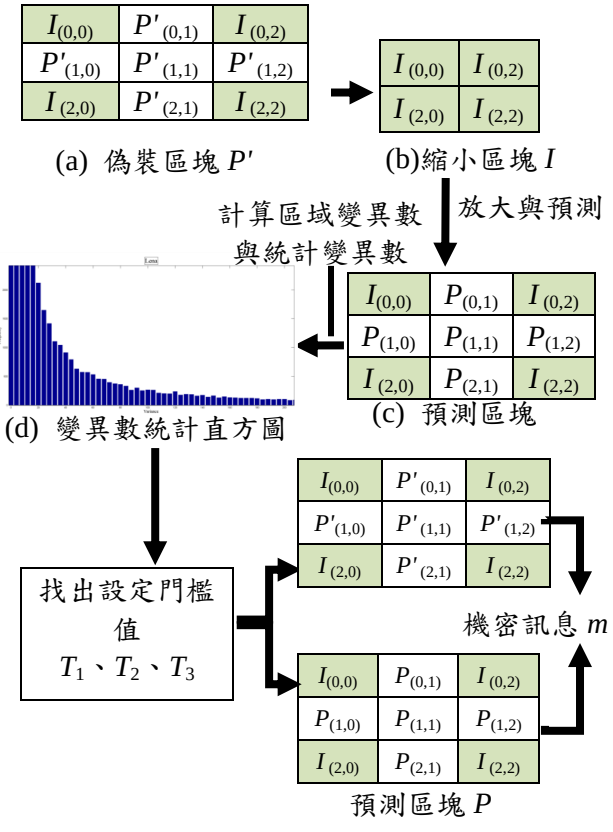



**圖 9 影像還原與取出機密訊息示意圖**

首先將影像縮小，並透過章節 2.1NMI 預測方式獲得預測影像。切割重複的區塊，再使用公式(12)與公式(13)計算出每個區塊的變異數，加以統計以及簡化變異數直方圖，使用相同的條件找到門檻值 T1、T2、T3，再透過公式(14)可取得每個區塊嵌入的機密訊息位元長度 k。獲得門檻值之後即可取出隱藏於偽裝預測值 P'的機密訊息。取出公式如下：

$$m=\begin{cases} P'-P, & \text{if } P\le 2^{k-1}-1, \\ P'-P+2^{k-1}, & \text{if } 2^{k-1}-1<P\le 255-2^{k-1}+1, \\ P-P', & \text{if } P>255-2^{k-1}+1. \end{cases} \quad (16)$$

依序使用公式(16)從偽裝像素值取出機密訊息。將影像縮小即可還原成原始影像。

## 4.實驗結果

本研究與 Jung 等學者於 2009 年提出之影像插值法（NMI）、Lee 等學者於 2012 年提出之相鄰像素插值法（INP）與 Tang 等學者於 2014 年提出之高藏量可逆式隱寫術（CRS）比較。本研究使用六張灰階影像進行測試，如圖 10 所示。

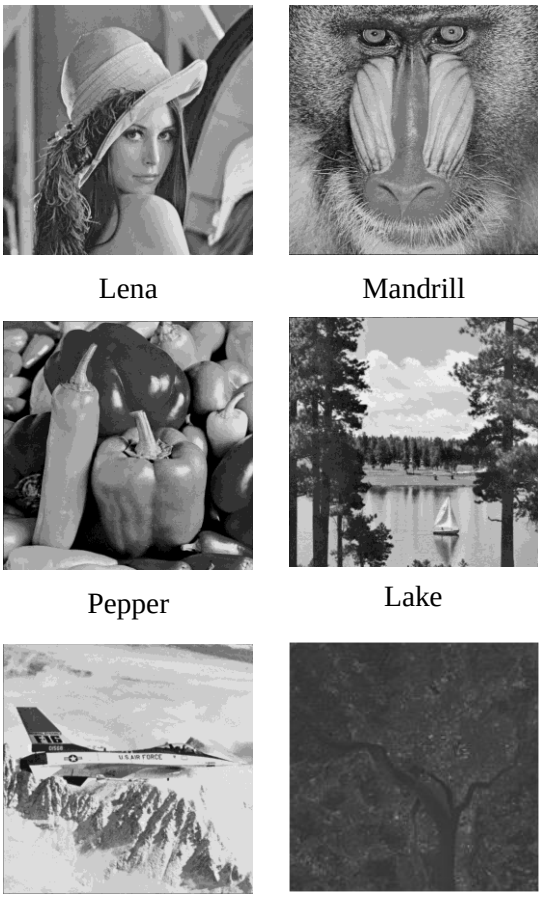



**圖 10 實驗測試影像**

本實驗使用 8 位元 256 色灰階影像進行實驗比較，套入公式(11)以計算影像失真程度。若偽裝影像與原始影像差異越大，計算出的 PSNR 值越低。反之，若差異越小則失真程度越低，PSNR 值也越高。

本研究採用 NMI 影像插值法進行影像擴張，因直接將原始影像 512x512 的影像放大將無基準可以比較 PSNR，故本研究先將影像縮小至 256x256，再將縮小影像使用 NMI 插值法、INP 插值法、CRS 插值法放大與原始 512x512 影像進行實驗比較。

原始影像、縮小影像、預測影像、偽裝影像關係如圖 11 所示。

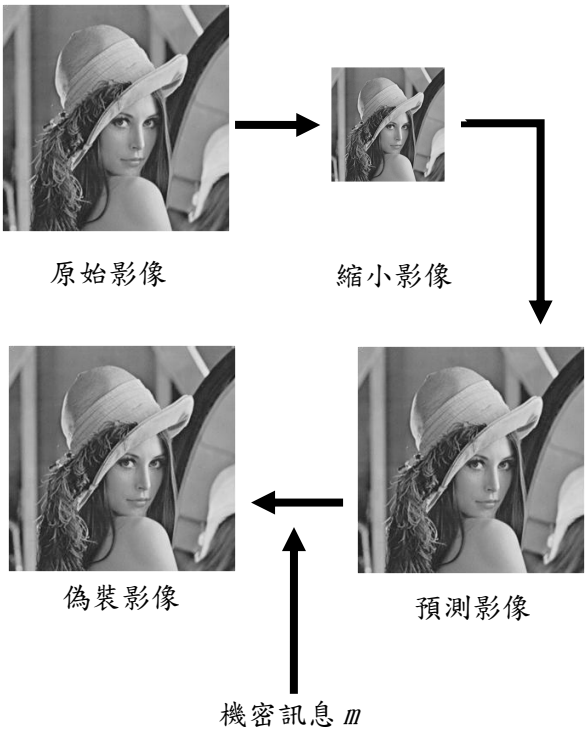



**圖 11 影像關係示意圖**

表 2 為三個方法與本研究原始影像與偽裝影像 PSNR 值比較，表 3 為三個方法與本研究 BPP 比較。以 Lena 為例，雖然本研究嵌入量比 CRS 少 0.09bpp，但 PSNR 卻比 CRS 多 4 db。犧牲少量的嵌入量換取較高的影像品質。以 Mandrill 為例，雖然嵌入量少於 CRS 0.51bpp，影像品質高 2.61 db。與 NMI 方法相比，嵌入量雖然只多 0.01 bpp，但影像品質卻多 0.8 db 之多。因為配合機密訊息對折策略的關係，使得嵌入相同機密訊息的情況下可以減少影像失真程度。

表 4 為三個方法與本研究預測影像與偽裝影像 PSNR 值比較。與表 2 有同的的狀況，其影像品質皆比其他方法好。

表 2 NMI、INP、CRS 與本研究原始影像與偽裝影像 PNSR 比較表

| | Lena | Mandrill | Peppers | Lake | Aireplane | Washsat |
|---|---|---|---|---|---|---|
| Jung & Yoo's NMI | 30.00 | 21.74 | 29.04 | 26.37 | 28.51 | 33.04 |
| Lee & Huang's INP | 29.62 | 21.55 | 28.67 | 26.03 | 28.14 | 32.85 |
| Tang & Song's CRS | 27.06 | 19.93 | 25.88 | 23.56 | 25.24 | 30.99 |
| Proposed Method | 31.36 | 22.54 | 29.87 | 27.61 | 29.87 | 34.26 |

**表 3 NMI、INP、CRS 與本研究 bpp 比較表**

| | Lena | Mandrill | Peppers | Lake | Aireplane | Washsat |
|---|---|---|---|---|---|---|
| Jung & Yoo's NMI | 1.30 | 2.40 | 1.31 | 1.69 | 1.68 | 1.26 |
| Lee & Huang's INP | 1.47 | 2.43 | 1.48 | 1.81 | 1.31 | 1.43 |
| Tang & Song's CRS | 1.84 | 2.92 | 1.86 | 2.23 | 1.13 | 1.75 |
| Proposed Method | 1.75 | 2.41 | 1.60 | 1.94 | 1.57 | 1.02 |

**表 4 NMI、INP、CRS 與本研究預測影像與裝影像 PNSR 比較表**

| | Lena | Mandrill | Peppers | Lake | Aireplane | Washsat |
|---|---|---|---|---|---|---|
| Jung & Yoo's NMI | 33.50 | 27.43 | 32.46 | 29.86 | 30.23 | 37.72 |
| Lee & Huang's INP | 33.03 | 26.96 | 31.96 | 29.35 | 31.28 | 37.02 |
| Tang & Song's CRS | 31.86 | 25.84 | 31.22 | 28.55 | 31.62 | 33.81 |
| Proposed Method | 41.19 | 38.15 | 42.76 | 40.23 | 41.87 | 49.03 |

## 5.結論

本研究提出一個植基於 NMI 插值法之可逆式資訊隱藏方法，分析區塊特性，並設定三個門檻值決定每個區塊應嵌入機密訊息位元長度。並且在嵌入時使用機密訊息對折策略再次降低機密訊息對影像的破壞程度。針對溢位的處理，也透過不同的嵌入方向避免溢位的發生。因為偽裝影像每區塊的四個角落像素，在整個嵌入流程之後並沒有變動，接收方在知道隱藏方法的前提之下，可以只用偽裝影像得知當初設定的門檻值並取出正確的機密訊息。

從實驗結果顯示，不管影像屬於平滑或是複雜，雖然機密訊息嵌入量都不比 CRS 還高，PSNR 值卻相對與其他三個方法還高。本研究也因為沒有溢位問題，不需要記錄額外訊息。

## 參考文獻


[1]A. M. Alattar (2004), "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," ***IEEE Transactions on Image Processing***, Vol. 13, pp. 1147-1156.

[2]L. An, X. Gao, Y. Yuan and D. Tao (2012), "Robust Lossless Data Hiding using Clustering and Statistical Quantity Histogram," ***Neurocomputing***, Vol. 77, No. 1, pp. 1-11.

[3]X. Chen, X. Sun, H. Sun, Z. Zhou, and J. Zhang (2013), "Reversible Watermarking Method Based on Asymmetric-Histogram Shifting of Prediction Errors," ***Journal of Systems and Software***, Vol. 86, No. 10, pp. 2620-2626.

[4]Y. F. Chang and W. L. Tai (2012), "Histogram-based Reversible Data Hiding Based on Pixel Differences with Prediction and Sorting," ***KSII Transactions on Internet and Information Systems***, Vol. 6, No. 12, pp. 3100-3116.

[5]M. Fallahpour (2008), "Reversible Image Data Hiding based on Gradient Adjusted Prediction," ***IEICE Electron Express***, Vol. 5, No. 20, pp. 870 -876.

[6]F. H. Hsu, M. H. Wu and S. J. Wang (2013), "Reversible Data Hiding Using Side-match Predictions on Steganographic Images," ***Multimedia Tools and Applications***, Vol. 67, No. 3, pp. 571-591.

[7]K. H. Jung and K. Y. Yoo (2009), "Data Hiding Method Using Image Interpolation," ***Computer Standards & Interfaces***, Vol. 31, No. 2, pp. 465-470.

[8]C. F. Lee and H. L. Chen (2012), "Adjustable Prediction-Based Reversible Data Hiding, "***Digital Signal Processing***, Vol. 22, No. 6, pp. 941-953.

[9]C. F. Lee, and Y. L. Huang (2012), "An Efficient Image Interpolation Increasing Payload in Reversible Data Hiding," ***Expert***

***Systems with Applications,*** Vol. 39, No. 8, pp. 6712-6719.

[10]T. C. Lu, J. H. Wu, C. C. Huang (2015), "Dual-image-based Reversible Data Hiding Method Using Center Folding Strategy, " ***Signal Processing***, Vol. 115, pp. 195-213.

[11]Z. C. Ni, Y. Q. Shi, N. Ansari and W. Su (2006), "Reversible Data Hiding," ***IEEE Transactions on Circuits and Systems for Video Technology***, Vol. 16, No. 3, pp. 354-362.

[12]V. Sachnev, H.J. Kim, J. Nam, S. Suresh, and Y.Q. Shi (2009)"Reversible Watermarking Algorithm Using Sorting and Prediction," ***IEEE Transactions on Circuits and Systems for Video Technology***, Vol. 19, pp. 989-999.

[13]M. W. Tang, J. Hu, W. Song (2014), "A High Capacity Image Steganography using Multi-layer Embedding," ***Optik***, Vol. 125, pp 3972-3976.

[14]D. M. Thodi and J. J. Rodriguez (2007),"Expansion embedding techniques for reversible watermarking, " ***IEEE Transactions on Image Processing.***, Vol. 16 , No. 3, pp.721 -730 .

[15]J. Tian (2003), "Reversible Data Embedding Using a Difference Expansion," ***IEEE Transactions on Circuits and Systems for Video Technology***, Vol. 13, No. 8, pp. 890-896.

[16]Z. H. Wang, C. F. Lee and C. Y. Chang (2013), "Histogram-Shifting-Imitated Reversible Data Hiding," J***ournal of Systems and Software***, Vol. 86, pp. 315-323.