機密訊息重編碼技術應用於雙影像無失真資訊隱藏方法

呂慈純
朝陽科技大學 副教授
e-mail:tclu@cyut.edu.tw

劉家維
朝陽科技大學碩士生
j320130@yahoo.com.tw

摘要

隨著數位資訊的普及，網際網路已經成為資訊傳遞不可或缺的重要工具，但是，當資料在透明化的數位環境傳遞時，可能會遭受非法的第三者利用不正當手段竊取、修改，甚至是毀損檔案，因此，什麼方法能夠增加資訊傳遞的安全性，就成為各個學者不斷討論的議題。

資訊隱藏是在原始的媒體中加入機密訊息，產生出的偽裝媒體即可躲過不法第三者的窺視，成功達到秘密訊息交換的目的。媒體包括了文字檔、圖片檔、影音檔或是其他的數位訊號媒體等等，本篇論文以影像做為研究的主要使用物件。

關鍵詞：無失真資訊隱藏、雙影像技術、中間對折策略、重新編碼規則

1. 介紹

資訊隱藏又可分類為可逆式資訊隱藏以及不可逆式的資訊隱藏兩種，而兩者的差異是偽裝影像是否能還原為原始的影像，可逆式資訊隱藏方法簡稱(Reversible Information Hiding，RIH)是能夠將原本所藏入的機密訊息從偽裝影像取出並能夠將原始影像還原的技術，多用於醫學影像或是軍事影像。

早在十年前，可逆式的資訊隱藏方法已經被很多學者所提出，其中像素差異值擴張方法以及直方圖位移法為最先被提及。像素差異值擴張方法是將機密訊息藏入至原始影像擴張數倍後的兩個像素當中，在 2003 年 Tian 學者提出第一個關於像素值差異擴張法的技術，計算兩個像素之間的差異值後，將所計算的差異值擴張至兩倍並同時藏入一個位元的機密訊息。2004 年 Alatter 學者將 Tian 學者的方法做改良，他將原本的像素值差異改成以向量導向的方式計算，利用相鄰的四個像素來算出差異值，並將擴張兩倍的差異值同時藏入三個位元的機密訊息。

Li 等學者在 2011 年時提出了適應性的藏入技術，他們的方法首先要將圖片像素區分成平坦區域以及不平坦區域兩種，再決定像素的預測誤差及計算所藏入的機密訊息數量。2014 年，Gui 等學者改良 Li 等學者在 2011 年所提的方法，利用增加複雜度的類型做為區隔，以利增加像素的預測誤差值的可藏入資訊量。

直方圖位移方法是利用統計預測誤差值次數的方式，產生直方圖圖表進行藏入，該方法將機密訊息藏入至出現頻率最高的數值當中，例如，在 2006 年 Ni 等學者所提出的直方圖位移方法。Tsai 等學者在 2009 年提出利用線性預測的方法，建立正向誤差值及負向誤差值的兩張直方圖圖表，並將機密訊息藏入至誤差值出現次數頻率最高當中。

2013 年 Wang 等學者提出差異預測直方圖方法，利用每兩個像素值產生誤差值的方法，產生出一張以誤差值所組成的二維度直方圖圖表，接著將二維度的圖表切分為一維度的直方圖圖表後再進行藏入。

除了差異值擴張方法及直方圖位移方法兩種方法之外，最近較流行的方法是利用雙影像的技術做藏入，它是當機密訊息要藏入時，將原始影像複製成兩張一樣的偽裝影像，藉此增加資訊藏入量。此外，雙影像的方法能夠有效的增加所藏入機密訊息的安全性，因為若是非法第三者沒有同時得到兩張偽裝影像的話，就不可能完整提取所藏入的機密訊息，因此雙影像的資訊隱藏技術是一種方便用於秘密共用的一種概念。

在 2007 年 Chang 等學者將模數函式藏匿法結合雙影像資訊隱藏技術，此方法一開始會先建立一張 256X256 大小的矩陣，接著以兩個位元的機密訊息為一組的方式做藏入，再由模數函式的矩陣當中取以左上至右下及左下至右上的兩條對角線的交點對應值做為兩張偽裝影像的偽裝像素值。之後，Chang 等學者為了能夠有效的降低影像失真程度，將所對應的左上至右下的對角線改為水平線，左下至右上的對角線改成為垂直線，這樣僅有兩條線所對應的像素值做更動。Lee 等學者在 2009 年提出的

方法認為將像素值設定為中心點，利用其上、下、左及右四個方向的像素值做偽裝影像素值，為了使影像能夠順利的還原回來，必須透過兩張像素值的關聯性得知第二張的偽裝影像是否有做過藏入的動作，若是無法進行藏入則第二張偽裝影像的偽裝像素值，要回復成原來的像素值。

Lee 和 Huang 學者所提出的方法先將機密訊息轉換成以五進制為基底的機密符號，並以兩個單位為一組，透過已經定義過後的藏入演算法取得兩張偽裝影像的偽裝像素值。2013 年 Chang 等學者為了使藏入機密訊息的資訊負載量能夠有效的提升，因此將原本以五進制為基底的機密訊息修改成以十進制為基底的機密訊息，利用由左下至右上的對角線所對應的數值做為偽裝像素值。2014 年 Qin 等學者將第一張偽裝影像以模數函式的藏入方法進行嵌入，再依照第一張影像所藏入的結果進行第二張偽裝影像藏入。2015 年 Lu 等學者提出了利用最低位元匹配法(LSB Matching)藏入機密訊息，首先利用最低位元匹配法取得兩張偽裝影像的偽裝像素值之後，透過像素值兩兩平均的方法來檢查是否能將偽裝像素還原至原始的像素值，不能還原的偽裝像素值，需要利用規則表進行像素值的修改，藉此使影像能夠有效的還原成功。

由以上的方法介紹可得知，雙影像資訊隱藏的技術結合了模數函式藏匿法、最低位元匹配法、藏入規則表的方法將偽裝像素值做修改，可以發現使用的藏入方法不同，所得到的資訊負載量及影像的品質也會有所差異，比如使用 Lee 等學者的方法可以達到較高的影像品質結果，但是缺點是藏入的資訊量僅僅只有 0.75bpp 而已，相較於 Chang 等學者提出利用模數函式藏匿法所得到的高資訊負載量，但是影像品質結果卻不佳。

因此研究後發現影響影像品質效果的關鍵來自於所藏入的機密訊息大小，普遍的資訊隱藏技術中，大多會先將藏入的機密訊息先做進制上的更改，大多為十進制為基底的為主，再將修改後的機密訊息進行像素值的計算，包含相加、相減以及平均法的計算等等，但若是機密訊息過大的話，則所修改後的偽裝像素值會與原始影像像素值相差甚大，導致影像的失真程度增大，影響影像品質。

本研究將針對機密訊息做前處理，利用 Lu 等學者在 2015 年提出的中間對折策略先將機密訊息轉成有正有負的值域範圍，接著統計對折後的機密符號所出現的頻率，將機密符號依出現頻率重新編碼，出現頻率越高的符號其編碼越接近 0，讓高出現頻率的機密符號在與像素值進行相加或相減時其造成的失真度能夠降到最低。

2. 文獻探討

2.1. 基於模數函式藏匿方法之雙影像技術

Zhang 和 Wang 學者於 2006 年提出模數函數藏匿方法，它是將 n 個像素值為一組後進行藏入，並且利用模數函式來計算像素值是否需要被修改。

模數函式的公式如下：

$$F(x_{i,j},x_{i,j+1},\ldots,x_{i,j+n-1})=\left[\sum_{q=1}^{n}(x_{i,j+q-1}\times q)\right] \bmod (2n+1), \quad (1)$$

其中，$x_{i,j}$ 代表原始的像素值，i 和 j 為像素的索引值，利用 $k=\lfloor \log_2(2n+1) \rfloor$ 公式可以計算 n 個像素中可藏入多少個機密訊息，並將 k 個機密訊息為一組轉換成以(2n+1)進制為基底的機密符號 d 值，利用 F()函式公式計算出 F 函式值後，判斷 F 函式值與要藏入的機密訊息 d 值是否相等，兩者相等的話，則像素值不作任何修改，反之，則需要改其中一個像素值，修改像素值的公式如下：

$$u=(d-F) \bmod (2n+1), \quad (2)$$

$$\begin{cases} x'_{i,j+u-1}=x_{i,j+u-1}+1, & \text{if } u\le n, \\ x'_{i,j+2n-u}=x_{i,j+2n-u}-1, & \text{otherwise.} \end{cases} \quad (3)$$

u 代表的是要修改的像素值位置，透過公式(2)可求得 u 值，並依照 u 值算出來的結果利用公式(3)進行像素值的修改，讓 F 函式值與機密訊息 d 值相同。

以圖 1 為例，當 n=4 且機密訊息為 001110101111，代表 4 個像素為一組可藏入 $k=\lfloor \log_2(2\times 4+1) \rfloor=3$ 個機密訊息，並將每 k 個位元為一組，轉成(2×4+1)進制值得到機密訊息 d 為 $(001)_2=(1)_9$、$(110)_2=(6)_9$、$(101)_2=(3)_9$ 和 $(111)_2=(7)_9$。在圖 1 中第一組區塊的 4 個像素值分別為 23、24、22 和 25，代入公式(1)計算出 F 函式值為 F(23,24,22,25)=(23×1+24×2+22×3+25×4) mod (2×4+1)=3，計算後 F 函式值不等於第一個機密訊息 d=$(1)_9$，因此利用公式(2)計算要修改的像素值位置 u=(1-3) mod (2×4+1)=7，並利用公式(3)取得修改後的像素值 $x'_{1,(1+2\times 4-7)}$=24-1=23，即偽裝像素值為 23、23、22 和 25。

	1	2	3	4
1	**23**	**24**	**22**	**25**
2	32	40	35	43
3	36	65	48	50
4	52	46	40	45

圖 1 EMD 之藏入範例

為了改善 EMD 的藏入量，Chang 等學者在 2007 年提出第一個雙影像技術。此方法是將 EMD 的模數函式公式(1)加以改良。改良後公式如下：

$$M(x_{i,j}, x_{i,j+1}) = (x_{i,j} + 2 \times x_{i,j+1}) \bmod 5, \quad (4)$$

M 為模數函式矩陣，在裡面存放像素值 0~255 的所有模數函式值。首先，此方法先利用公式(4)建立一個 256x256 的模數函式矩陣 $M=\{M(0,0), M(0,1),\ldots, M(255,255)\}$，如圖 2 所示。接著以 2 個機密訊息為一組，並轉成 5 進制為基底的機密訊息 d，每次以取 2 個機密訊息 d 為一組進行藏入。利用像素值配對 $x_{i,j}$ 和 $x_{i,j+1}$ 取得模數函式值 $M(x_{i,j}, x_{i,j+1})$ 做為中心，從模數函式矩陣 M 中選取 5x5 區塊。若區塊中的模數函式值等於機密訊息 d 值時，則會將所對應到的像素值 $x_{i,j}$ 和 $x_{i,j+1}$ 作為偽裝像素值。

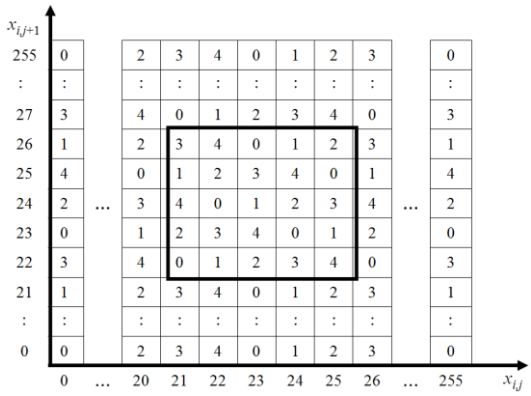

圖 2 256x256 模數函式矩陣

以像素值配對 $x_{1,1}$=23、$x_{1,2}$=24 且機密訊息為 001110 為例，每 2 個機密訊息為一組，轉成 5 進制機密訊息 d 為 $(00)_2=(0)_5$、$(11)_2=(3)_5$ 和 $(10)_2=(2)_5$。以模數函式值 $M(23,24)=1$ 為中心，選取一個 5x5 區塊(如圖 2 所示)，利用該區塊內右對角線 (如圖 3(a) 所示)和左對角線 (如圖 3(b) 所示)藏入機密訊息 $(0)_5$ 和 $(3)_5$。當第 1 個機密訊息 $d=(0)_5$，對應到像素值為 $x'_{1,1}$=24 和 $x'_{1,2}$=23，此即為第 1 張偽裝影像的像素值；第 2 個機密訊息 $d=(3)_5$，對應到像素值為 $x''_{1,1}$=22 和 $x''_{1,2}$=23，此即為第 2 張偽裝影像的像素值，藏入範例如圖 3 所示。

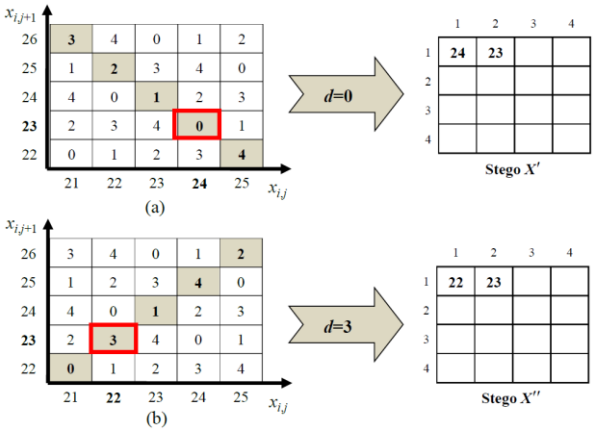

圖 3 Chang 等學者之雙影像範例

然而，為了追求更好的影像品質，Chang 等學者在 2009 年將 EMD 雙影像技術再加以進行改良。此方法是將機密訊息的對應方式由右對角線和左對角線，修改成水平線和垂直線進行藏入，以像素值配對 $x_{1,1}$=23、$x_{1,2}$=24 且機密訊息 d 為 $(0)_5$ 和 $(3)_5$ 為例，將模數函式值 $M(23,24)=1$ 視為中心點，並選取一個 5x5 區塊，以垂直線上的模數函式值(如圖 4(a)所示)和水平線上的模數函式值(如圖 4(b)所示)對機密訊息 $(0)_5$ 和 $(3)_5$ 進行藏入。第 1 個機密訊息 $d=(0)_5$，對應到的像素值為 $x'_{1,1}$=23 和 $x'_{1,2}$=26，此即為第 1 張偽裝影像的像素值；第 2 個機密訊息 $d=(3)_5$，對應到像素值為 $x''_{1,1}$=25 和 $x''_{1,2}$=24，此即為第 2 張偽裝影像的像素值，藏入範例如圖 4 所示。

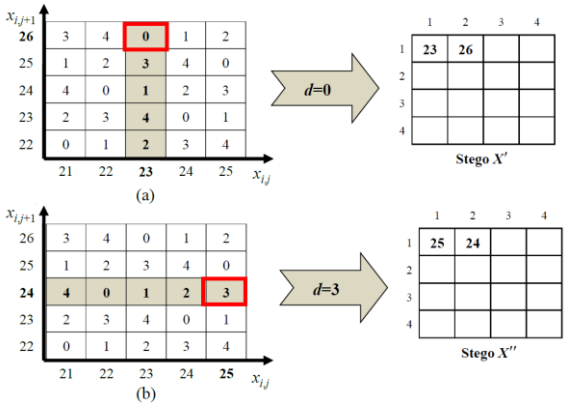

圖 4 Chang 等學者之改良後雙影像範例

Chang 等學者在 2013 年將模數函式矩陣的區塊大小由 5x5 擴增至 9x9，並且以 10 進制為基底的機密訊息 d 進行藏入。為了提升影像品質，該方法將機密訊息的對應方式由左對角線及右對角線，修改為只利用右對角線進行嵌入，並且同時對第 1 張影像的偽裝像素值 $x'_{i,j}$

和第 2 張影像的偽裝像素值 $x''_{i,j}$ 進行修改。此方法將模數函式矩陣公式(5)進行修改，公式如下所示：

$$M(x_{i,j},x_{i,j})=(x_{i,j}+3\times x_{i,j}) \bmod 9. \quad (5)$$

以像素值 $x_{1,1}$=23 且機密訊息為 001110 為例，機密訊息轉成 10 進制機密訊息 d 為 $(001)_2=(1)_{10}$ 和 $(110)_2=(6)_{10}$。接著將像素值 $x_{1,1}$ 代入公式(5)取得模數函式值 $M(23,23)=2$，以模數函式值為中心，選取 9x9 區塊(如圖 5(a)所示)。第 1 個機密訊息 $d=(1)_{10}$，對應到像素值為 $x'_{1,1}$=19(如圖 5(b)所示)和 $x''_{1,1}$=27(如圖 5(c)所示)。

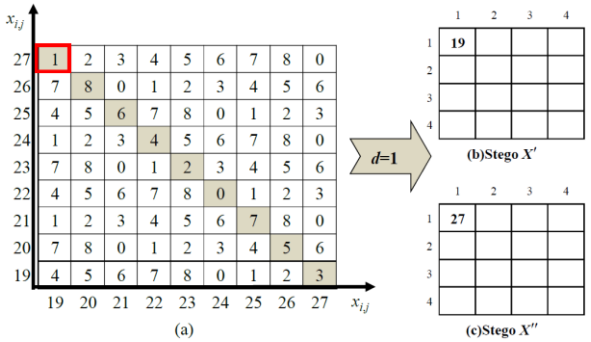

圖 5 Chang 等學者 2013 年改良後之雙影像範例

Qin 等學者在 2014 年將 EMD 與雙影像技術結合，此方法是將機密訊息轉成以 5 進制為基底的機密訊息，並且利用像素值配對 $x_{i,j}$ 和 $x_{i,j+1}$ 將機密符號 d_1 和 d_2 進行藏入。機密符號 d_1 先利用 EMD 藏入影像中，取得第一張偽裝影像像素值配對 $x'_{i,j}$ 和 $x'_{i,j+1}$。為了避免影像無法還原回原始影像，該方法以偽裝像素值配對 $x'_{i,j}$ 和 $x'_{i,j+1}$ 判斷機密符號 d_2 的藏入方法，判斷的條件如下所示：

(1)當 $x'_{i,j}=x_{i,j}$ 且 $x'_{i,j+1}=x_{i,j+1}$，機密符號 d_2 繼續利用 EMD 進行嵌入，產生第 2 張偽裝影像像素值配對 $x''_{i,j}$ 和 $x''_{i,j+1}$。

(2)當 $x'_{i,j}=x_{i,j}$ 且 $x'_{i,j+1}\neq x_{i,j+1}$，對第 2 張偽裝影像的像素值 $x_{i,j+1}$ 進行修改，使 F 函式值等於機密符號 d_2。修改的公式如下所示：

$$l=\begin{cases}1, & \text{if } d_2=F\left[x_{i,j},x_{i,j+1}-1\times\text{sign}(x'_{i,j}-x_{i,j+1})\right],\\ 2, & \text{if } d_2=F\left[x_{i,j},x_{i,j+1}-2\times\text{sign}(x'_{i,j}-x_{i,j+1})\right],\\ 3, & \text{if } d_2=F\left[x_{i,j},x_{i,j+1}-3\times\text{sign}(x'_{i,j}-x_{i,j+1})\right],\\ 4, & \text{if } d_2=F\left[x_{i,j},x_{i,j+1}-4\times\text{sign}(x'_{i,j}-x_{i,j+1})\right],\\ 5, & \text{if } d_2=F\left[x_{i,j},x_{i,j+1}-5\times\text{sign}(x'_{i,j}-x_{i,j+1})\right].\end{cases} \quad (6)$$

$$\begin{cases}x''_{i,j}=x_{i,j},\\ x''_{i,j+1}=x_{i,j+1}-l\times\text{sign}(x'_{i,j+1}-x_{i,j+1}).\end{cases} \quad (7)$$

l 是為介於 1~5 之間的數值，sign()為正負號符號函數，以 1 和-1 表示正數和負數。為了使 F 函式值與機密符號 d_2 相等，利用公式(6)計算並找出數值 l，並將數值 l 代入公式(7)計算出第 2 張影像偽裝像數值配對 $x''_{i,j}$ 和 $x''_{i,j+1}$。

(3)當 $x'_{i,j}\neq x_{i,j}$ 且 $x'_{i,j+1}=x_{i,j+1}$，對第 2 偽裝張影像的像素值 $x_{i,j}$ 進行修改，使 F 函式值等於機密符號 d_2，而修改的公式如下所示：

$$l=\begin{cases}1, & \text{if } d_2=F\left[x_{i,j}-1\times\text{sign}(x'_{i,j}-x_{i,j}),x_{i,j+1}\right],\\ 2, & \text{if } d_2=F\left[x_{i,j}-2\times\text{sign}(x'_{i,j}-x_{i,j}),x_{i,j+1}\right],\\ 3, & \text{if } d_2=F\left[x_{i,j}-3\times\text{sign}(x'_{i,j}-x_{i,j}),x_{i,j+1}\right],\\ 4, & \text{if } d_2=F\left[x_{i,j}-4\times\text{sign}(x'_{i,j}-x_{i,j}),x_{i,j+1}\right],\\ 5, & \text{if } d_2=F\left[x_{i,j}-5\times\text{sign}(x'_{i,j}-x_{i,j}),x_{i,j+1}\right].\end{cases} \quad (8)$$

$$\begin{cases}x''_{i,j}=x_{i,j}-l\times\text{sign}(x'_{i,j}-x_{i,j}),\\ x''_{i,j+1}=x_{i,j+1}.\end{cases} \quad (9)$$

為了使 F 函式值與機密符號 d_2 相等，利用公式(8)來計算並找出數值 l，並將數值 l 代入公式(9)計算出第 2 張影像偽裝像數值配對 $x''_{i,j}$ 和 $x''_{i,j+1}$。

以像素值配對 $x_{1,1}$=23、$x_{1,2}$=24 且機密訊息為 0011 為例，將機密訊息轉成機密符號 $d_1=(00)_2=(0)_5$ 和 $d_2=(11)_2=(3)_5$。透過公式(1)計算出 F 函式值為 $F(23,24)=(23\times1+24\times2) \bmod (2\times2+1)=4$，由於 F 函式值不等於機密符號 d_1，利用公式(2)計算出欲修改像素位置 $u=(0-2) \bmod (2\times2+1)=4$，接著透過公式(3)取得修改後像素值 $x'_{1,2}$=23-1=22，取得第一張影像偽裝像素值 $x'_{1,1}$ 和 $x'_{1,2}$ 為 22、24。因為 $x'_{i,j}=x_{i,j}$ 且 $x'_{i,j+1}\neq x_{i,j+1}$，所以利用公式(6)計算出數值 l=3，並且代入公式(7)取得第 2 張影像偽裝像數值配對 $x''_{i,j}$=23-(3×sign(22-23))=26 和 $x''_{i,j+1}$=24。

2.2.植基於位置性之雙影像技術

Lee 等學者於 2009 年提出一個基於位置性的雙影像技術，此方法利用像素值配對為 $x_{i,j}$ 和 $x_{i,j+1}$ 一組座標，像素值 $x_{i,j}$ 和 $x_{i,j+1}$ 分別代表著 X 軸及 Y 軸的座標，此組像素值配對視為十字座標圖(如圖 6 所示)中心點$(x_{i,j}, x_{i,j+1})$，中心點的上、下、左及右 4 組像素值配對分別對應到機密訊息 s_1 和 s_2 的四種不同組合，其中 s_1 和 s_2 各為 1 位元機密訊息，並將所對應到的像素值配對當作第一張偽裝影像的像素值配對 $x'_{i,j}$ 和 $x'_{i,j+1}$。對應公式如下所示：

$$\left(x'_{i,j}, x'_{i,j+1}\right)=\begin{cases}\left(x_{i,j}+1, x_{i,j+1}\right), & \text{if } s_1s_2=00,\\ \left(x_{i,j}, x_{i,j+1}-1\right), & \text{if } s_1s_2=01,\\ \left(x_{i,j}, x_{i,j+1}+1\right), & \text{if } s_1s_2=10,\\ \left(x_{i,j}-1, x_{i,j+1}\right), & \text{if } s_1s_2=11.\end{cases} \quad (10)$$

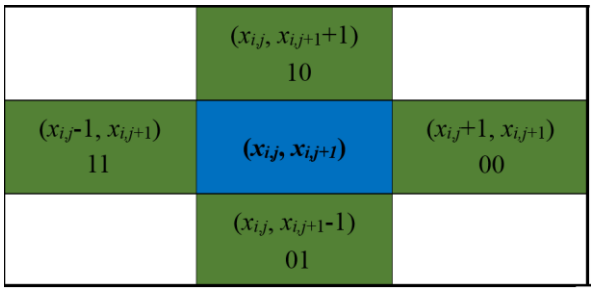

圖 6 十字座標圖

接著利用類似方法來嵌入機密訊息 s_3 和 s_4，取得第 2 張偽裝影像的像素值配對 $x''_{i,j}$ 和 $x''_{i,j+1}$。嵌入的公式如下所示：

$$\left(x''_{i,j}, x''_{i,j+1}\right)=\begin{cases}\left(x_{i,j}+1, x_{i,j+1}\right), & \text{if } s_3s_4=00,\\ \left(x_{i,j}, x_{i,j+1}-1\right), & \text{if } s_3s_4=01,\\ \left(x_{i,j}, x_{i,j+1}+1\right), & \text{if } s_3s_4=10,\\ \left(x_{i,j}-1, x_{i,j+1}\right), & \text{if } s_3s_4=11.\end{cases} \quad (11)$$

利用公式(11)可取得偽裝像素值的配對 $x''_{i,j}$ 和 $x''_{i,j+1}$，為了判斷機密訊息 s_3 和 s_4 是否能嵌入，因此利用偽裝像素值配對 $x'_{i,j}$ 和 $x'_{i,j+1}$ (在圖 7 中以 x' 表示)和偽裝像素值配對 $x''_{i,j}$ 和 $x''_{i,j+1}$ (在圖 7 中以 x'' 表示)，當兩組偽裝像素值配對在十字座標圖上位置呈對向關係(如圖 7 (a)-(d))或是順時針方向(如圖 7 (e)-(h))，則能完成機密訊息的嵌入；反之，若是在其他情況下，則無法嵌入，因此偽裝像素值配對 $x''_{i,j}$ 和 $x''_{i,j+1}$ 還原成像素值配對 $x_{i,j}$ 和 $x_{i,j+1}$。

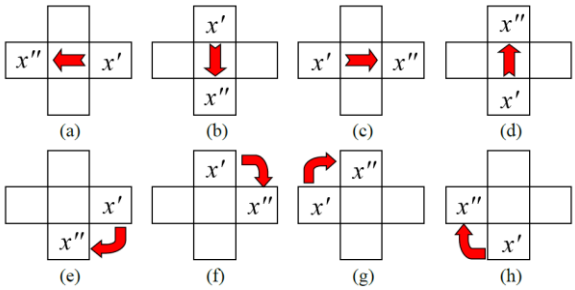

圖 7. Lee 等學者的方向性策略

以像素值配對 $x_{1,1}$=35 和 $x_{1,2}$=36 且機密訊息 s_1 和 s_2 等於 00 為例，利用公式(10)取得偽裝像素值配對為 $x'_{1,1}$=35+1 和 $x'_{1,2}$=36，位於十字座標圖的中心點右方(如圖 8 (a))。假設機密訊息 s_3 和 s_4 為 11，利用公式(11)計算出偽裝像素值配對為 $x''_{1,1}$=35-1=34 和 $x''_{1,2}$=36，位於十字座標圖的中心點左方，和偽裝像素值配對 $x'_{1,1}$=36 和 $x'_{1,2}$=36 呈對向關係(如圖 8(b))，則代表可嵌入機密訊息，完成嵌入的動作。若 s_1 和 s_2 等於 00 的情況下，而 s_3 和 s_4 為 10，代入公式(11)可取得偽裝像素值配對 $x''_{1,1}$=35 和 $x''_{1,2}$=37，位於偽裝像素值配對 $x'_{1,1}$=36 和 $x'_{1,2}$=36 的逆時針位置(如圖 8(c)所示)，則無法進行嵌入，因此將偽裝像素 $x''_{1,1}$ 和 $x''_{1,2}$ 還原成 35 和 36。

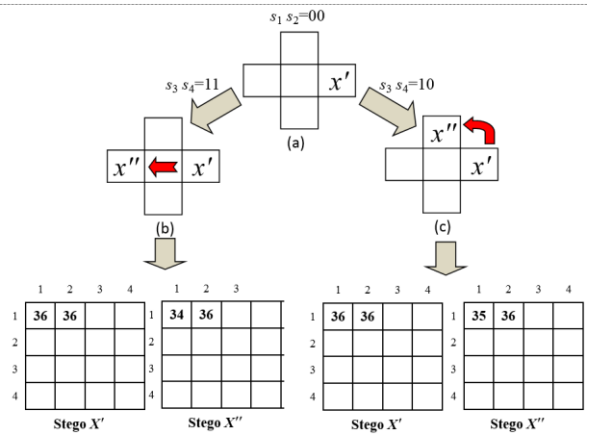

圖 8 Lee 等學者的雙影像技術範例

為了提高藏入量，Lee 和 Huang 學者於 2013 年將機密訊息轉成 5 進制機密符號，並利用定義好的嵌入規則表來進行藏入。此方法首先取 5 個機密位元 $s=\{s_1, s_2, s_3, s_4, s_5\}$，轉換成 10 進制的機密符號 d，若當 $16 \leqq d \leqq 24$，則將機密訊息 s 轉成一組 5 進制機密符號得到 d_1 和 d_2；而當 $d<16$ 或 $d>24$，則從機密訊息 s 中取前 4 位的機密訊息，並轉成 5 進制機密符號得到 d_1 和 d_2。以 s=00110 為例，先將機密訊息轉成 10 進制的機密符號 $d=(00110)_2=(6)_{10}$，因為 $d<16$，則從機密訊息中取 4 個機密訊息 $s=(0011)_2$，轉成 5 進制機密符號 $d_1=(0)_5$ 和 $d_2=(3)_5$。

機密符號 d_1 和 d_2 總共會有 25 種組合方式，此方法針對 25 種組合定義 25 組不同嵌入規則表(如表 1)。每組的機密符號 d_1 和 d_2 都會對應到一組嵌入的規則，將像素值配對 $x_{i,j}$ 和 $x_{i,j+1}$ 代入嵌入規則表，取得第 1 張偽裝影像像素值配對 $x'_{i,j}$ 和 $x'_{i,j+1}$ 和第 2 張偽裝影像像素值配對 $x''_{i,j}$ 和 $x''_{i,j+1}$。以像素值配對 $x_{1,1}$=35、$x_{1,2}$=36 為例，機密符號 $d_1=(0)_5$ 和 $d_2=(3)_5$，所對到的規則為 $x'_{i,j}=x_{i,j}$=35，$x'_{i,j+1}=x'_{i,j+1}$+1=36+1=37，而 $x''_{i,j}=x_{i,j}$+1=35+1=36，$x''_{i,j+1}=x_{i,j+1}$+1=36+1=37。

表 1 Lee 和 Huang 學者之嵌入規則表

d_1	$x'_{i,j}$	$x'_{i,j+1}$	d_2	$x''_{i,j}$	$x''_{i,j+1}$
0	$x_{i,j}$	$x_{i,j+1}$+1	0	$x_{i,j}$	$x_{i,j+1}$
			1	$x_{i,j}$ -1	$x_{i,j+1}$-1
			2	$x_{i,j}$ -1	$x_{i,j+1}$+1
			3	$x_{i,j}$ +1	$x_{i,j+1}$+1
			4	$x_{i,j}$ +1	$x_{i,j+1}$-1
1	$x_{i,j}$-1	$x_{i,j+1}$-1	0	$x_{i,j}$	$x_{i,j+1}$+1
			1	$x_{i,j}$ -1	$x_{i,j+1}$
			2	$x_{i,j}$ +1	$x_{i,j+1}$+1
			3	$x_{i,j}$ +1	$x_{i,j+1}$
			4	$x_{i,j}$ +1	$x_{i,j+1}$-1
2	$x_{i,j}$-1	$x_{i,j+1}$+1	0	$x_{i,j}$ +1	$x_{i,j+1}$
			1	$x_{i,j}$ +1	$x_{i,j+1}$-1
			2	$x_{i,j}$	$x_{i,j+1}$+1
			3	$x_{i,j}$	$x_{i,j+1}$-1
			4	$x_{i,j}$ -1	$x_{i,j+1}$-1
3	$x_{i,j}$+1	$x_{i,j+1}$+1	0	$x_{i,j}$	$x_{i,j+1}$-1
			1	$x_{i,j}$ -1	$x_{i,j+1}$-1
			2	$x_{i,j}$ -1	$x_{i,j+1}$
			3	$x_{i,j}$ +1	$x_{i,j+1}$
			4	$x_{i,j}$ -1	$x_{i,j+1}$+1
4	$x_{i,j}$+1	$x_{i,j+1}$-1	0	$x_{i,j}$ -1	$x_{i,j+1}$
			1	$x_{i,j}$ -1	$x_{i,j+1}$+1
			2	$x_{i,j}$	$x_{i,j+1}$+1
			3	$x_{i,j}$ +1	$x_{i,j+1}$+1
			4	$x_{i,j}$	$x_{i,j+1}$-1

2.3.植基於最低位元取代匹配法的雙影像技術

Mielikainen 學者於 2006 年提出最低位元取代匹配法 (Least-Significant-Bit Matching, LSB Matching)。為了嵌入兩個機密訊息 s_1 和 s_2，此方法利用一個二元函式(Binary Function)來決定如何修改像素值配對 $x_{i,j}$和 $x_{i,j+1}$，嵌入的流程如圖 9 所示，其中 $x'_{i,j}$和 $x'_{i,j+1}$為偽裝像素值。

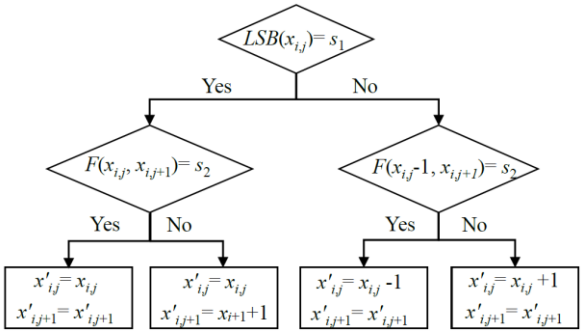

圖 9 LSB 匹配法嵌入流程

嵌入的流程中，透過 LSB 函式計算出像素值 $x_{i,j}$ 的最低位元，並判斷 $x_{i,j}$ 的最低位元是否與機密訊息 s_1 相等，若相等，則像素值配對 $x_{i,j}$和 $x_{i,j+1}$ 直接代入 F 函式；若不相等，則像素值 $x_{i,j}$ 減 1，並代入 F 函式中，F 函式如下：

$$F(x_{i,j}, x_{i,j+1}) = LSB(\left\lfloor \frac{x_{i,j}}{2} \right\rfloor + x_{i,j+1}). \qquad (12)$$

接著利用像素值 $x_{i,j}$ 的最低位元和 F 函式值判斷來修改像素值，當 $LSB(x_{i,j})=s_1$ 且 $F(x_{i,j}, x_{i,j+1})=s_2$，則偽裝像素值配對 $x'_{i,j}$和 $x'_{i,j+1}$ 等於像素值配對 $x_{i,j}$和 $x_{i,j+1}$；當 $LSB(x_{i,j})=s_1$ 且 $F(x_{i,j}, x_{i,j+1})\neq s_2$，則偽裝像素值配對 $x'_{i,j}$和 $x'_{i,j+1}$ 等於 $x_{i,j}$和 $x_{i,j+1}$+1；當 $LSB(x_{i,j})\neq s_1$ 且 $F(x_{i,j}$-1, $x_{i,j+1})=s_2$，則偽裝像素值配對 $x'_{i,j}$和 $x'_{i,j+1}$ 等於 $x_{i,j}$-1 和 $x_{i,j+1}$；當 $LSB(x_{i,j})\neq s_1$ 且 $F(x_{i,j}$-1, $x_{i,j+1})\neq s_2$，則偽裝像素值配對 $x'_{i,j}$和 $x'_{i,j+1}$ 等於 $x_{i,j}$+1 和 $x_{i,j+1}$。

以像素值配對 $x_{1,1}$=35 和 $x_{1,2}$=36 且機密訊息 s_1 和 s_2 為 00 為例，$LSB(35)=1$ 且 $LSB(35)=1\neq s_1$，將 35-1 代入公式(12)計算出 $F(34, 36)$函式值為 1。由於 $LSB(45)=1\neq s_1$ 且 $F(34, 36)=s_2=1\neq s_2$，故偽裝像素值配對 $x'_{1,1}$和 $x'_{1,2}$為 36 和 36。

Lu 等學者將 LSB 匹配方法應用在雙影像的技術中以提高影像品質，此方法每次以像素值配對 $x_{i,j}$和 $x_{i,j+1}$ 為一組，嵌入 4 個機密訊息 s_1、s_2、s_3 及 s_4。首先，利用 LSB 匹配法來將機密訊息 s_1 及 s_2 嵌入至第 1 張偽裝影像當中，取得偽裝像素值配對 $x'_{i,j}$和 $x'_{i,j+1}$，而機密訊息 s_3 和 s_4 同樣利用 LSB 匹配法進行嵌入，取得第 2 張偽裝影像偽裝像素值配對 $x''_{i,j}$和 $x''_{i,j+1}$。接著利用平均法來檢查偽裝像素值是否能還原回到原始的像素值，檢查公式如下：

$$\begin{cases} p_{i,j} = \left\lfloor (x'_{i,j} + x''_{i,j})/2 \right\rfloor, \\ p_{i,j+1} = \left\lfloor (x'_{i,j+1} + x''_{i,j+1})/2 \right\rfloor, \end{cases} \qquad (13)$$

其中 $p_{i,j}$和 $p_{i,j+1}$ 為還原後的像素值。透過公式(13)判斷偽裝像素值是否能還原，當 $x_{i,j}=p_{i,j}$ 且 $x_{i,j+1}=$

$p_{i,j+1}$，代表像素值可以還原，偽裝像素值不需要修改；若當 $x_{i,j} \neq p_{i,j}$ 或 $x_{i,j+1} \neq p_{i,j+1}$，則代表像素值無法順利還原，則須依照規則表來修改偽裝像素值，規則表如表 2 所示。

表 2 Lu 等學者之規則表

Case	像素值修改情形				偽裝像素值			
	$x'_{i,j}$	$x'_{i,j+1}$	$x''_{i,j}$	$x''_{i,j+1}$	$x'_{i,j}$	$x'_{i,j+1}$	$x''_{i,j}$	$x''_{i,j+1}$
1	0	0	-1	0	$x_{i,j}+2$	$x_{i,j+1}+1$	$x_{i,j}-1$	$x_{i,j+1}+1$
2	0	1	0	1	$x_{i,j}$	$x_{i,j+1}+1$	$x_{i,j}$	$x_{i,j+1}-1$
3	0	1	-1	0	$x_{i,j}+2$	$x_{i,j+1}$	$x_{i,j}-1$	$x_{i,j+1}$
4	-1	0	0	0	$x_{i,j}-1$	$x_{i,j+1}$	$x_{i,j}+2$	$x_{i,j+1}+1$
5	-1	0	0	1	$x_{i,j}-1$	$x_{i,j+1}$	$x_{i,j}+2$	$x_{i,j+1}$
6	-1	0	-1	0	$x_{i,j}-1$	$x_{i,j+1}+2$	$x_{i,j}+1$	$x_{i,j+1}-1$
7	1	0	1	0	$x_{i,j}-1$	$x_{i,j+1}-1$	$x_{i,j}+1$	$x_{i,j+1}+2$

以像素值配對 $x_{1,1}$=35 和 $x_{1,2}$=35 為例，利用 LSB 匹配法將機密訊息$(00)_2$和$(10)_2$嵌入 2 張影像當中，嵌入第一組機密訊息$(00)_2$時，因為 $LSB(35)=1 \neq s_1=0$，將像素值 $x_{1,1}$-1 代入公式(12)計算出 F 函式值為 $F(34,35)=0=s_1=0$，故像素值 $x_{1,1}$ 減 1，取得偽裝像素值配對 $x'_{1,1}$ 和 $x'_{1,2}$ 為 35-1=34 和 36；嵌入第二組機密訊息$(10)_2$時，由於 $LSB(35)=1$，透過公式(12)計算出 F 函式值為 $F(35,35)=0=s_2=0$，則偽裝像素值配對 $x''_{1,1}$ 和 $x''_{1,2}$ 為 35 和 36。接著透過公式(13)計算出還原後的像素值$p_{1,1}=\lfloor (34+35)/2 \rfloor = 34$和$p_{1,2}=\lfloor 36+36/2 \rfloor = 36$，其中$p_{1,1}$不等於像素值 $x_{1,1}$，代表影像不可進行還原，因此偽裝像素值需要修改，而該修改情況符合表 2 中的 Case 4，因此，偽裝像素的修改須修正為 $x'_{1,1}=x_{1,1}-1=35-1=34$，$x'_{1,2}=x'_{1,2}=35$；$x''_{1,1}=x_{1,1}+2=35+2=37$，$x''_{1,2}=x_{1,2}+1=35+1=36$。

2.4.植基於中間對折策略的雙影像技術

Lu 等學者在 2015 年提出利用中間對折策略的雙影像技術，此方法將機密訊息先對折，再將對折後的機密訊息分別藏入兩張偽裝影像當中，藏入流程如圖 10。

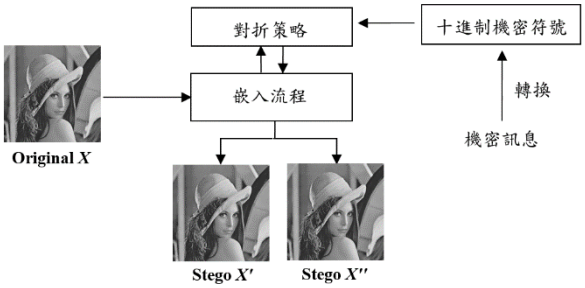

圖 10 中間對折策略藏入流程

首先，將機密訊息(Secret Message)以每 k 個位元為一組，轉成一個機密符號 d，為了避免機密符號 d 過大而造成影像失真，利用中間對折策略對機密符號 d 進行縮減，使得機密符號的值域由 $R=\{0, 1, 2, \ldots, 2^k-1\}$變為 $\bar{R}=\{-2^{k-1}, -2^{k-1}+1, \cdots, -1, 0, 1, \cdots, 2^{k-1}-2, 2^{k-1}-1\}$，公式如下：

$$\bar{d} = d - 2^{k-1}, \tag{14}$$

其中 $\bar{d}$ 為對折後的機密符號，2^{k-1} 為中間值。利用公式(14)將機密符號 d 轉換成對折後機密符號 $\bar{d}$，若當 $d<2^{k-1}$，則對折後機密符號 $\bar{d}$ 以負數表示；若當 $d=2^{k-1}$，則對折後機密符號 $\bar{d}$ 以 0 表示；若當 $d>2^{k-1}$，則對折後機密符號 $\bar{d}$ 以正數表示。圖 11 為 R 與 $\bar{R}$ 的值域示意圖，公式(14)將原本都是正數的機密符號 d 轉成為正、負數的數值。

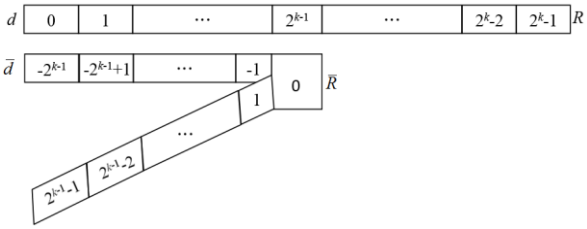

圖 11 R 與 $\bar{R}$ 值域示意圖

為了提升影像品質，此方法是利用平均法將對折後機密符號 $\bar{d}$ 嵌入至兩張偽裝影像當中。嵌入公式如下：

$$\begin{cases} \bar{d}_1 = \left\lfloor \dfrac{\bar{d}}{2} \right\rfloor, \\ \bar{d}_2 = \left\lceil \dfrac{\bar{d}}{2} \right\rceil. \end{cases} \tag{15}$$

$$\begin{cases} x'_{i,j} = x_{i,j} + \bar{d}_1, \\ x''_{i,j} = x_{i,j} - \bar{d}_2, \end{cases} \tag{16}$$

其中 $\bar{d}_1$ 以及 $\bar{d}_2$ 是由 $\bar{d}$ 分割出來的，嵌入像素值 $x_{i,j}$ 中，形成二個偽裝像素值 $x'_{i,j}$ 及 $x''_{i,j}$。

以圖 12 為例，原始影像 $X=\{35, 36, 40, 42\}$。假設每次嵌入位元數為 k=3，當 $x_{1,1}$=35 且機密訊息為 $s=(001)_2$，將機密訊息 s 轉成 10 進制的機密符號 $d=(1)_{10}$，利用公式(14)將機密符號 d 對應至新的值域 $\bar{R}$ 中，取得對折後機密符號 $\bar{d}=1-4=-3$。接著利用公式(15)計算出對折後機密符號 $\bar{d}$ 的兩個數值 $\bar{d}_1=\lfloor -3/2 \rfloor = -2$ 及 $\bar{d}_2=\lceil -3/2 \rceil = -1$，然後將 $\bar{d}_1$ 和 $\bar{d}_2$ 代入公式(16)計算可取得偽裝像素值 $x'_{1,1}$=35+(-2)=33 和 $x''_{1,1}$=35-(-1)=36。

下一個像素值為 $x_{1,2}$=36，假設機密訊息為 $s=(110)_2$。首先將機密訊息 s 轉成機密符號 $d=(6)_{10}$，利用公式(14)將機密符號 d 對應至新值域 $\bar{R}$ 中，取得對折後機密符號 $\bar{d}=6-4=2$。接著利用公式(15)計算對折後機密符號 $\bar{d}$ 的兩個數值 $\bar{d}_1=\lfloor 2/2 \rfloor=1$ 和 $\bar{d}_2=\lceil 2/2 \rceil=1$，接著將數值 $\bar{d}_1$ 和 $\bar{d}_2$ 代入公式(16)計算可取得偽裝像素值 $x'_{1,2}$=36+1=37 和 $x''_{1,2}$=36-1=35。

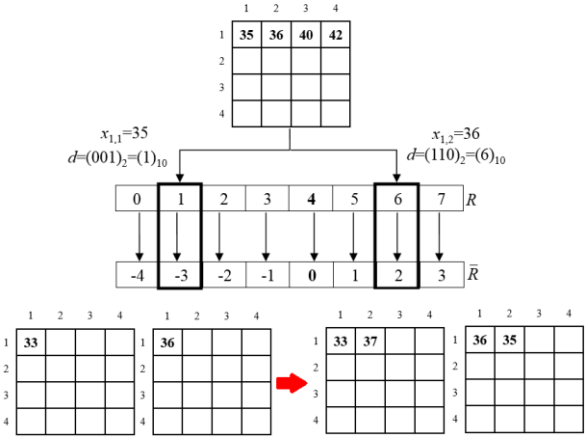

圖 12 嵌入範例

3.研究方法

本研究使用機密訊息重新編碼技術，將機密訊息重新編碼，再透過中間對折策略將機密訊息對折，接著將對折後的機密訊息分別藏入兩張偽裝影像當中，研究設計圖如圖 13 所示。

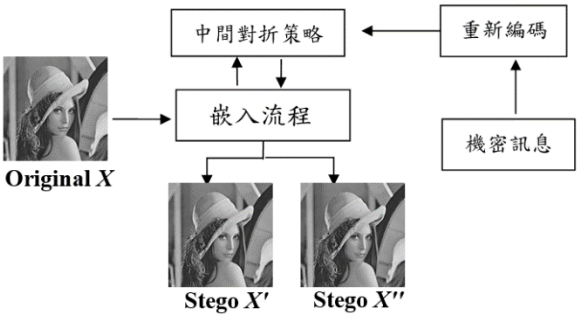

圖 13 研究設計圖

3.1 嵌入階段

令原始影像為 $X=\{x_{1,1}, x_{1,2},\ldots, x_{h,w}\}$，其中 h，w 為影像的高和寬。先將機密訊息(Secret Message)轉換成以二進制為基底，以每 k 個位元為一組，轉成以十進制為基底的機密符號 d，將所有的機密符號依據出現的次數做統計，並利用所出現的次數統計表進行由次數多到次數少的排序，並透過中間對折策略方法使機密符號 d 的值域進行縮減。以表 3 為例，令 k=4，表中 d=15 出現了 $H(d)$=12 次為出現頻率最多的，因此重新編碼為對折後的訊息 $F(d)$=0。

表 3 規則表

d	15	10	12	8	11	9	7	6	4	14	3	13	2	5	0	1
$H(d)$	12	10	9	8	7	6	5	5	4	4	4	3	3	2	1	0
$F(d)$	0	1	-1	2	-2	3	-3	4	-4	5	-5	6	-6	7	-7	8

由表 3 的規則表可以得到原始機密符號 d 值所對應的新機密符號 $F(d)$值，為了有效提升影像品質，本篇論文採用平均法將新機密訊息 $F(d)$嵌入至兩張偽裝影像當中，嵌入的公式如下：

$$\begin{cases} X'_{i,j}=X_{i,j}+\left\lceil \frac{F(d)}{2} \right\rceil \\ X''_{i,j}=X_{i,j}-\left\lceil \frac{F(d)}{2} \right\rceil \end{cases} \quad (17)$$

將 $F(d)$值一分為二嵌入至 $X_{i,j}$ 中，可以得到兩個偽裝像素值 $X'_{i,j}$ 和 $X''_{i,j}$。偽裝像素產生過程中，可能因為機密符號的嵌入產生溢位問題，例如當 $X_{i,j}$=253 且 $\left\lceil \frac{F(d)}{2} \right\rceil$ =5 時，兩者相加就會造成上溢 (Overflow) 問題。由於 $F(d)$的值域為$[-2^{k-1}, 2^{k-1}-1]$，當像素值小於 2^{k-1} 則可能因為加上 -2^{k-1} 而造成下溢，或像素值大於 $255-(2^{k-1}-1)=256-2^{k-1}$，則可能因為加上 $2^{k-1}-1$ 而造成上溢。因此，在進行嵌入時要先判斷偽裝像素值是否介於 2^{k-1} 到 $256-2^{k-1}$ 之間。整體的嵌入流程如下所示：

(1) 令原始影像為 X。

(2) 判斷像素值 $X_{i,j}$ 是否介於$[2^{k-1}, 256-2^{k-1}]$之間，若像素值 $X_{i,j}$ 在範圍內則可進行嵌入；若像素值 $X_{i,j}$ 超出此範圍，代表該像素值可能會發生溢位問題，則像素不能嵌入，令 $X'_{i,j}=X_{i,j}$ 且 $X''_{i,j}=X_{i,j}$，跳到下一個像素。

(3) 取出 k 個機密訊息 $s=\{s_1, s_2, s_3,\ldots, s_k\}$，轉成 10 進制的機密符號 d。統計 d 出現的次數 $H(d)$，依 $H(d)$由大至小排序，$H(d)$越大則 $F(d)$造成的失真越小，$F(d)$的編碼原則為從 0 開始，數值一正一負給值，例如：0，1，-1，2，-2，3，-3，…，$-(2^{k-1}-1)$，2^{k-1}。

(4) 將 $F(d)$值代入公式(17)，將 $F(d)$一分為二，可以得到偽裝像素值 $X'_{i,j}$ 和 $X''_{i,j}$。

(5) 以此類推，重複步驟 (2)-(4)直到所有機密訊息都完成嵌入。

以圖 14 為例，原始影像 $X=\{30, 40, 45, 50\}$。假設每次嵌入位元數為 k=4，機密訊息 0010100100100100 以 4 個位元一組轉成十進制的機密符號 d，利用下方的對照表將機密符號出現的次數由多至少進行排序可得下表：

d	2	9	4
H(d)	2	1	1
F(d)	0	1	-1

當 $X_{1,1}$=30 且機密訊息為 $s=(0010)_2$ 轉成十進制機密符號 d 值為$(2)_{10}$ 透過對照表可得到對折後的機密符號 $F(d)$值為 0，利用公式(17)計算出偽裝像素值$X'_{1,1}=X_{1,1}+\left\lceil\frac{F(d)}{2}\right\rceil$= 30+0=30 和$X''_{1,1}=X_{1,1}-\left\lfloor\frac{F(d)}{2}\right\rfloor$=30-0=30。

下一個像素值是 $X_{1,2}$=40 且機密訊息為 $s=(1001)_2$ 轉成十進制機密符號 d 值為$(9)_{10}$ 透過對照表可得到對折後的機密符號 $F(d)$值為 1，利用公式(17)計算出偽裝像素值$X'_{1,2}=X_{1,2}+\left\lceil\frac{F(d)}{2}\right\rceil$= 40+1=41 和$X''_{1,2}=X_{1,2}-\left\lfloor\frac{F(d)}{2}\right\rfloor$=40-0=40。

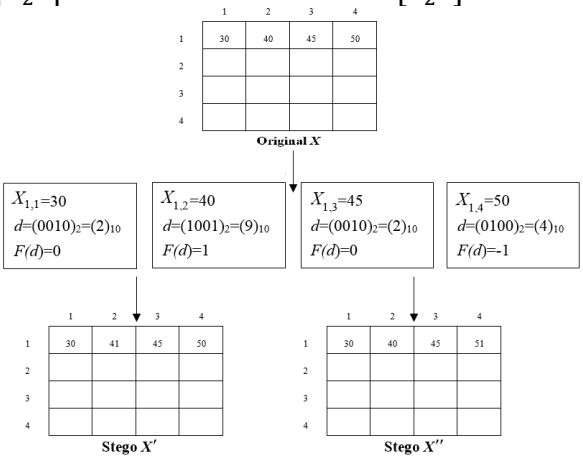

圖 14 嵌入範例

3.2. 資訊取出和影像還原

藏入資訊的取出，首先要判斷偽裝像素值 $X'_{i,j}$ 和 $X''_{i,j}$ 是否相等，若 $X'_{i,j}$= $X''_{i,j}$ 且數值不介於$[2^{k-1}, 256-2^{k-1}]$的範圍內則表示沒有藏入機密訊息，偽裝像素即為原始像素；反之，若偽裝像素值 $X'_{i,j}$ 和 $X''_{i,j}$ 其中一個介於範圍內，表示此像素有藏機密訊息，則將偽裝像素值 $X'_{i,j}$ 和 $X''_{i,j}$ 進行相減，可以取得對折後機密符號$F(d)$，接著透過對照表可得到原始的機密符號 d，機密訊息取出的公式如下：

$$F(d)= X'_{i,j}-X''_{i,j} \quad (18)$$

利用公式(18)取得對折後機密符號 $F(d)$，並且將對折後機密符號$F(d)$代入規則表可以得到機密符號 d。接著將機密符號 d 轉換成以二進制為基底的機密訊息，取得 k 個機密訊息 s。

以偽裝像素值 $X'_{1,1}$=30 和 $X''_{1,1}$=30 為例，每次嵌入位元數為 k=4，透過公式(18)計算出對折後機密符號 $F(d)$=30-30=0，利用規則表取得機密符號 d=2，接著將機密符號 d 轉換成以二進制為基底的機密訊息 $s=(0010)_2$。下一個偽裝像素值 $X'_{1,2}$=41 和 $X''_{1,2}$=40，取得對折後機密符號 $F(d)$=41-40=1，利用規則表取得機密符號 d=9，接著將機密符號 d 轉換成以二進制為基底的機密訊息 $s=(1001)_2$。

影像還原的部分，將偽裝像素值 $X'_{i,j}$ 和 $X''_{i,j}$ 進行平均後，即可取得原始像素值 $X_{i,j}$。還原公式如下：

$$X_{i,j}=\left\lceil\frac{X'_{i,j}+X''_{i,j}}{2}\right\rceil \quad (19)$$

以偽裝像素值 $X'_{1,1}$=30 和 $X''_{1,1}$=30 為例，透過公式(19)計算出原始像素值$X_{i,j}=\lceil(30+30)/2\rceil=30$；偽裝像素值 $X'_{1,2}$=41 和 $X''_{1,2}$=40 代入公式(19) 計算出原始像素值 $X_{i,j}=\lceil(41+40)/2\rceil=40$。資訊取出和影像還原的範例如圖 15 所示。

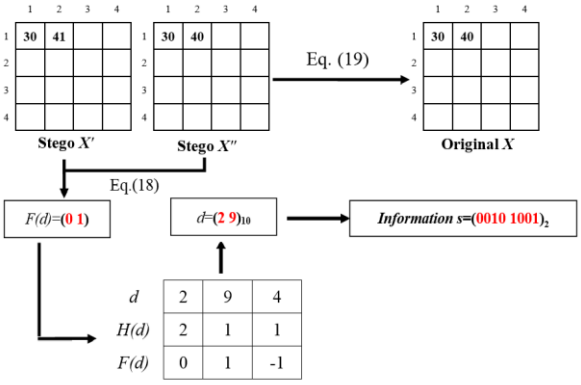

圖 15 資訊取出和影像還原範例

4. 實驗結果

本研究透過 Matlab 7.14.0 (R2012a)實作出所提方法與其他雙影像技術，利用灰階影像進行實驗。灰階影像取自 The Waterloo GreyscaleSet2 (http://links.uwaterloo.ca/Repository.html) 資料庫中 8 張 512×512 大小的標準灰階影像，如圖 16 所示。

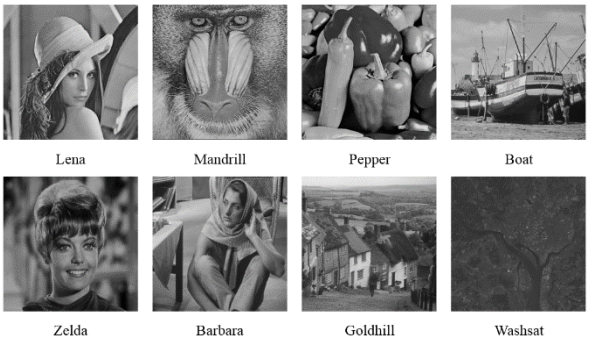

圖 16 標準灰階影像

本篇論文利用影像峰值信號雜訊比（Peak Signal to Noise Ratio, PSNR）評估原始影像和偽裝影像像素之間的差異，PSNR 公式如下所示：

$$\mathrm{PSNR} = 10 \times \log_{10}\left[\frac{255^2}{\frac{1}{h \times w} \times \sum_{i=1}^{h}\sum_{j=1}^{w}(x'_{i,j} - x_{i,j})^2}\right](\mathrm{dB}), \qquad (20)$$

$h \times w$ 為整張影像的大小，$x'_{i,j}$ 和 $x_{i,j}$ 分別代表偽裝影像和原始影像的像素值。若是兩張影像之間的像素值差異較小，則代表會有較好的影像品質，PSNR 值也就越高。反之，兩張影像之間的像素值差異過大，則代表影像品質會較差，PSNR 值也就越低。為了衡量藏入方法的藏入能力，利用每個像素能夠嵌入位元數（Bits Per Pixel, bpp）評估偽裝影像的藏入量大小，bpp 公式如下所示：

$$\mathrm{bpp} = \frac{C}{2 \times h \times w}, \qquad (21)$$

C 為兩張偽裝影像的藏入量的加總。當 bpp 較大時，代表此方法的藏入能力較好，可以藏入的資訊量也就越多，而當 bpp 較小時，代表此方法的藏入能力較差，可以藏入的資訊量也就越少。

表 4 是本篇論文提出方法在不同的機密訊息長度 k 下，影像品質與總藏量之比較，其中 PSNR_1 和 PSNR_2 分別為第一張偽裝影像和第二張偽裝影像的影像品質，PSNR_Avg 代表兩張偽裝影像的影像品質平均值。從表 4 中可以發現當 k 設為 3 時，實驗中的 8 張影像的偽裝影像 PSNR 值皆會大於 59dB，代表原始影像與偽裝影像的像素值差異較小，總藏入量大約可達到 786,000 位元；若當 k=6，實驗中的 8 張影像的總藏量平均為 1,501,778 位元，且平均的 PSNR 值皆在 42 dB 以上。

表 4 不同訊息長度 k 下影像品質及總藏量比較

k		Lena	Mandrill	Pepper	Boat	Zelda	Barbara	Goldhill	Washsat
3	PSNR_1	55.50	55.50	55.62	55.50	55.50	55.50	55.50	55.50
	PSNR_2	62.91	62.91	63.22	62.91	62.91	62.91	62.91	62.91
	PSNR_Avg	59.20	59.20	59.42	59.20	59.20	59.20	59.20	59.2071
	Capacity	786,432	786,042	777,474	786,429	785,973	786,432	786,432	786,432
4	PSNR_1	51.83	51.83	52.38	51.83	51.87	51.83	51.83	51.83
	PSNR_2	54.05	54.05	54.74	54.05	54.11	54.05	54.05	54.05
	PSNR_Avg	52.94	52.94	53.56	52.94	52.99	52.94	52.94	52.94
	Capacity	1,048,576	1,047,636	1,000,924	1,048,568	1,044,800	1,048,576	1,048,576	1,048,576
5	PSNR_1	46.29	46.31	46.83	46.29	46.45	46.29	46.29	46.29
	PSNR_2	46.82	46.83	47.37	46.82	46.99	46.82	46.82	46.82
	PSNR_Avg	46.56	46.57	47.10	46.56	46.72	46.56	46.56	46.56
	Capacity	1,310,700	1,308,560	1,210,070	1,310,290	1,282,500	1,310,715	1,310,720	1,310,720
6	PSNR_1	41.89	41.95	42.07	42.01	42.03	41.99	42.01	41.89
	PSNR_2	42.12	42.17	42.24	42.21	42.21	42.20	42.21	42.11
	PSNR_Avg	42.01	42.06	42.15	42.11	42.12	42.10	42.11	42.00
	Capacity	1,568,766	1,558,368	1,384,650	1,480,476	1,425,852	1,540,872	1,482,390	1,572,852

表 5 為所提方法與 2015 年 Lu 等學者提出的方法 [17] 之總藏入量和影像品質的比較表，當 k=3 時，本篇論文所提方法的第一張偽裝影像 PSNR 值為 55.50dB，較 Lu 等學者於 2015 年所提出的方法高出約 12 dB，而第 2 張偽裝影像 PSNR 值更達到 62.91 dB，比 Lu 等學者的方法高出 20 dB，以平均 PSNR 值來看 Lu 等學者的平均 PSNR 值為 42.45 dB，較本篇所提的方法的 59.20 dB 低了 16.75 dB。當機密訊息 k 的長度越大時，本篇論文所提的方法與 Lu 等學者 2015 年所提出的方法的影像品質差異更為顯著。由表 5 可以發現，雖然本篇所提方法的藏入能力與 Lu 等學者於 2015 年所提的方法相同，但本篇論文所提出的方法在影像品質上有更好的表現。

表 5 和 Lu et al.方法影像品質及總藏量比較

Method	k		Lena	Mandrill	Pepper	Boat	Zelda	Barbara	Goldhill	Washsat
Lu et al. (2015)	3	PSNR_1	42.72	42.73	42.76	42.72	42.72	42.72	42.72	42.73
		PSNR_2	42.18	42.19	42.23	42.18	42.18	42.18	42.18	42.19
		PSNR_Avg	42.45	42.46	42.50	42.45	42.45	42.45	42.45	42.46
		Capacity	786,432	786,042	777,474	786,429	785,973	786,432	786,432	786,432
Proposed Method	3	PSNR_1	55.50	55.50	55.62	55.50	55.50	55.50	55.50	55.50
		PSNR_2	62.91	62.91	63.22	62.91	62.91	62.91	62.91	62.91
		PSNR_Avg	59.20	59.20	59.42	59.20	59.20	59.20	59.20	59.2071
		Capacity	786,432	786,042	777,474	786,429	785,973	786,432	786,432	786,432
Lu et al. (2015)	4	PSNR_1	36.69	36.70	36.86	36.69	36.69	36.69	36.69	36.71
		PSNR_2	36.31	36.31	36.48	36.31	36.31	36.31	36.31	36.32
		PSNR_Avg	36.50	36.50	36.67	36.50	36.50	36.50	36.50	36.51
		Capacity	1,048,576	1,047,636	1,000,924	1,048,568	1,044,800	1,048,576	1,048,576	1,048,576
Proposed Method	4	PSNR_1	51.83	51.83	52.38	51.83	51.87	51.83	51.83	51.83
		PSNR_2	54.05	54.05	54.74	54.05	54.11	54.05	54.05	54.05
		PSNR_Avg	52.94	52.94	53.56	52.94	52.99	52.94	52.94	52.94
		Capacity	1,048,576	1,047,636	1,000,924	1,048,568	1,044,800	1,048,576	1,048,576	1,048,576
Lu et al. (2015)	5	PSNR_1	30.64	30.65	30.95	30.64	30.64	30.64	30.64	30.72
		PSNR_2	30.41	30.42	30.73	30.41	30.42	30.41	30.41	30.50
		PSNR_Avg	30.53	30.53	30.84	30.53	30.53	30.53	30.53	30.61
		Capacity	1,310,700	1,308,560	1,210,070	1,310,290	1,282,500	1,310715	1,310,720	1,310,720
Proposed Method	5	PSNR_1	46.29	46.31	46.83	46.29	46.45	46.29	46.29	46.29
		PSNR_2	46.82	46.83	47.37	46.82	46.99	46.82	46.82	46.82
		PSNR_Avg	46.56	46.57	47.10	46.56	46.72	46.56	46.56	46.56
		Capacity	1,310,700	1,308,560	1,210,070	1,310,290	1,282,500	1,310,715	1,310,720	1,310,720
Lu et al. (2015)	6	PSNR_1	24.51	24.54	25.07	24.59	24.77	24.76	24.52	24.94
		PSNR_2	24.38	24.41	24.95	24.45	24.64	24.63	24.36	24.82
		PSNR_Avg	24.44	24.47	25.01	24.52	24.71	24.70	24.43	24.88
		Capacity	1,568,766	1,558,368	1,384,650	1,480,476	1,425,852	1,540,872	1,482,390	1,572,852
Proposed Method	6	PSNR_1	41.89	41.95	42.07	42.01	42.03	41.99	42.01	41.89
		PSNR_2	42.12	42.17	42.24	42.21	42.21	42.20	42.21	42.11
		PSNR_Avg	42.01	42.06	42.15	42.11	42.12	42.10	42.11	42.00
		Capacity	1,568,766	1,558,368	1,384,650	1,480,476	1,425,852	1,540,872	1,482,390	1,572,852

5. 結論

本篇論文是將機密訊息進行重新編碼後，再使用中間對折策略和雙影像技術提高藏量與降低失真度，為了使影像品質能夠保有良好的效果，將重新編碼後的機密符號利用中間對折策略將機密符號對折縮減，並利用平均法將對折後機密符號嵌入至兩張偽裝影像中。在實驗結果上可以發現，所提方法與近年來的其他方法相比皆表現出很好的結果，不但具有較高的總藏入量和也有較佳影像品質。

參考文獻

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

2004.

[2] C.C. Chang, Y.C. Chou, and T.D. Kieu, "Information Hiding in Dual Images with Reversibility," ***Proceedings of Third International Conference on Multimedia and Ubiquitous Engineering***, pp. 145-152, 2009.

[3] C.C. Chang, T.D. Kieu, and Y.C. Chou, "Reversible Data Hiding Scheme Using Two Steganographic Images," ***Proceedings of IEEE Region 10 International Conference (TENCON)***, pp. 1-4, 2007.

[4] C.C. Chang, T.C. Lu, G. Horng, Y.H. Huang, and Y.M. Hsu, "A High Payload Data Embedding Scheme Using Dual Stego-images with Reversibility," ***Proceedings of Third International Conference on Information, Communications and Signal Processing***, pp. 1-5, 2013.

[5] X. Gui, X. Li, and B. Yang, "A High Capacity Reversible Data Hiding Scheme Based on Generalized Prediction-Error Expansion and Adaptive Embedding," ***Signal Processing***, Vol. 98, pp. 370-380, 2014.

[6] C.F. Lee and Y.L. Huang, "Reversible Data Hiding Scheme Based on Dual Stegano-Images Using Orientation Combinations," ***Telecommunication Systems***, Vol. 52, No. 4, pp. 2237-2247, 2013.

[7] C.F. Lee, K.H. Wang, C.C. Chang, and Y.L. Huang, "A Reversible Data Hiding Scheme Based on Dual Steganographic Images," ***Proceedings of the Third International Conference on Ubiquitous Information Management and Communication***, pp. 228-237, 2009.

[8] X. Li, B. Yang, and T. Zeng, "Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection," ***IEEE Transactions on Image Processing***, Vol. 20, pp. 3524-3533, 2011.

[9] T.C. Lu, C.Y. Tseng, and J.H. Wu, "Dual Imaging-based Reversible Hiding Technique Using LSB Matching," ***Signal Processing***, Vol. 108, pp. 77-89, 2015.

[10] J. Mielikainen, "LSB Matching Revisited," *IEEE Signal Processing Letters*, Vol. 13, No. 5, pp. 285-287, 2006.

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

[1] C. Qin, C.C. Chang, and T.J. Hsu, "Reversible Data Hiding Scheme Based on Exploiting Modification Direction with Two Steganographic Images," ***Multimedia Tools and Applications***, pp. 1-12, 2014.

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

[14] P. Tsai, Y.C. Hu, and H.L. Yeh, "Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting," ***Signal Processing***, Vol. 89, pp. 1129-1143, 2009.

[15] S.Y. Wang, C.Y. Li, and W.C. Kuo, "Reversible Data Hiding Based on Two-dimensional Prediction Errors," ***IET Image Processing***, Vol. 7, pp. 805-816, 2013.

[16] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," ***IEEE Communications Letters***, Vol. 10, No. 11, pp. 781-783, 2006.

[17] T.C. Lu, J.H. Wu, and C.C. Huang, "Dual-Image-Based Reversible Data Hiding Method Using Center Folding Strategy," ***Signal Processing***, Vol. 115, pp. 195-213, 2015.