雙偽裝影像的可逆式資訊隱藏技術之探究

李金鳳*
朝陽科技大學
資訊管理學系教授
lcf@cyut.edu.tw

陳思婷
中興大學
資訊管理學系研究生
tingchen319@gmail.com

摘要

資訊隱藏是在不破壞影像的前提下，將重要的機密訊息直接藏入影像中，且不會使影像有明顯的改變。因此，藏入機密訊息後的偽裝影像，在網路傳輸的過程中並不會被察覺，以達到保護機密資料的目的。現今已有許多學者投入資訊隱藏領域進行研究，可逆式資訊隱藏可以使偽裝影像在取出機密訊息後回復為原始影像，在研究之深度與實際應用上扮演著舉足輕重的角色。在可逆式資訊隱藏的影像載體又分為單一影像與多重影像。因為多重影像藏入不僅可增加資訊負載量又保有優良的影像品質，以達到高藏量、高品質與高安全性的特性，因此本文針對目前已發表過有關於多重可逆式偽裝影像資訊隱藏技術的學術論文，從資訊的負載量、視覺影像品質與各學者的研究結果進行比較，並探討未來相關領域可以延伸的部分。

所謂的多重偽裝影像藏匿法，主要是將機密資訊平均藏在多張偽裝影像上，因此像素值進行修改時，並不會產生太多的變化；當要取出機密資訊和恢復原始影像時，只須將數張影像進行重疊或是透過對照表等就能達到還原原始影像與取出機密資訊的目的。2007 年，Chang 學者等人提出一個可逆式雙影像資訊隱藏技術，使用魔術矩陣藏入機密資訊，最後輸出兩張偽裝影像，但影像品質仍有進步的空間。2009 年， Chang 學者等人提出可將對角線魔術矩陣改為十字魔術矩陣的改善方法，如此便能提高影像品質，同時又保有優良的藏量。2009 年，Lee 學者等人提出一個可逆式雙偽裝影像高影像品質資訊隱藏技術，藉由十字座標空間法，讓機密資訊藏入的過程中，使像素值不會有大幅度的調整，以達到高藏量。2011 年，Lee 學者等人提出一個雙偽裝影像差異組合藏匿技術，可進一步改善 5 進制的數字轉換系統，使安全性、影像品質和負載量皆同時提升。2014 年，Lee 學者等人提出一個雙偽裝影像運用直方圖修改與模術運算之可逆式資訊隱藏技術，藉由可逆式直方圖修改技術與可逆式對角魔術矩陣的資訊隱藏技術藏入兩階段的機密資訊，但影像品質仍有進步的空間，因此 2015 年，Lee 學者等人提出改善方法，將第二階段改為使用十字魔術矩陣，提高影像品質的同時又可維持穩定的藏量。

關鍵詞：可逆式資訊隱藏、直方圖修改資訊隱藏技術、雙偽裝影像資訊隱藏技術、對角魔術矩陣、十字魔術矩陣

一、前言

隨著網路科技的進步，檔案傳輸越發快速與便利，在網路傳輸的過程中，藏有機密訊息(Secret Data)的影像極有可能會發生安全問題。因此，如何將機密訊息藏入影像中，並且不被發現，是現今資訊隱藏領域中重要的議題。資訊隱藏(Data Hiding)是將機密訊息直接藏入影像中，因此像素值改變的程度非常細微，並不會影響影像的外觀，進而被肉眼察覺。如此在網路傳輸的過程中，即可避免被第三者發現機密訊息的存在，以達到保護機密訊息及安全傳輸的目的。優良的資訊隱藏技術須滿足三要點：安全性(Security)、不可察覺性(Imperceptivity)以及高資訊附載量(Capacity)。資訊隱藏分為不可逆式(Non-Reversible Data Hiding) [17][1]與可逆式(Reversible Data Hiding, RDH)，其中可逆式資訊隱藏(RDH)可以使偽裝影像(Stego Image)在取出機密訊息後，回復為原始影像(Cover Image)，故其應用的領域更為寬廣，尤其針對不容許資料有所失真的重要領域如醫療或軍事等方面，因此可逆式資訊隱藏也稱為無失真資訊隱藏。可逆式資訊隱藏技術中的影像載體可分為單一影像藏入(Single Image Hiding)與多重影像藏入(Multiple Image Hiding)。單一影像的可逆式資訊隱藏技術(Single Image Reversible Data Hiding, SI-RDH)是將機密資訊藏入單一原始影像中，並輸出單一偽裝影像，而多重影像的可逆式資訊隱藏技術(Multiple Image Reversible Data Hiding, MI-RDH)則可輸出多重偽裝影像，接收方須收到所有偽裝影像才可取出完整的機密資訊，如此便能提高機密資訊的安全性。

在單一影像的可逆式資訊隱藏技術(SI-RDH)中有相當多的研究，可分為二大類型：差異擴張法(Difference Expansion, DE)與直方圖位移修正法(Histogram Shifting and Modification)。所謂的差異擴張法是將像素分群並計在群組間的像素的差異值，或者是計算像素與預測值對間的差異值。然而再將機密訊息藏於擴張後的差異值中。例如，Tian(2003) [12]、Alattar(2004) [1]、Yang(2013)[16]等。然而較大的差異值在擴張又藏入機密訊息後可能會導致嚴重的失真，造成像素值有上溢位或下溢問題 (Overflow or Underflow Problem)，故該類的方法須要一張位置圖(Location Map)的額外資訊需要處理，故差異擴張的 RDH 方法會較為複雜。相反地，利用像素值或像素的差異值進行直方圖統計，再將機密訊息藏於峰值點中。例 如，Ni et al. (2006) [10]Tai et al. (2009) [11], Tsai et al. (2009) [13], Tseng et al. (2009) [14], Luo et al. (2010) [4], Yang et al. (2010) [15], Zhao et al. (2011) [18], 及 Hong(2012) [5]等所提直方圖藏入技術。

2006 年，Ni 學者等人提出一個可逆式直方圖位移修改(Histogram-shifting-and-modification)資訊隱藏技術 [10]。該技術統計像素[0, 255]出現的次數，以形成一張統計直方圖，並從中找出峰值點(Peak Point)和零值點(Zero Point)。峰值點為出現最多次的像素值，零值點為出現次數為 0 的像素值或者是出現最少次的像素值，再根據條件，位移正負一個單位，空出峰值點左或右的位置以藏入機密訊息，但藏入量並不出色。

2007 年，Chang 學者等人提出一個可逆式雙影像資訊隱藏技術 [3]。藉由 EMD(Exploiting Modification Direction) [10]產生擁有像素對組合的 5×5 的魔術矩陣，再藉由魔術矩陣修改像素對，並以對角線的方式進行機密資訊藏入，因此像素對中的兩個像素值有可能同時被加 2 或減 2，會造成失真度提高的現象，影像品質(Peak Signal to Noise Ratio, PSNR)仍有改善的空間。

2009 年，Chang 學者等人提出改善影像品質的方法 [2]。將對角魔術矩陣藏入法改為十字魔術矩陣藏入法，像素對中的兩個像素值只有其中一個最多會被加 2 或減 2，所以能夠大幅提高影像品質同時又能保有穩定的藏入量。同年，Lee 學者等人提出一個可逆式雙偽裝影像高影像品質資訊隱藏技術 [8]。主要方法是藉由十字座標空間法(Cross Pattern)，依照規則進行機密資訊藏入，可讓像素值不被大幅調整，提高影像品質。

2011 年，Lee 學者等人提出一個可逆式雙偽裝影像差異組合資訊隱藏技術 [9]。改善 5 進制的數字轉換系統，使 2 位數 5 進制中的$(31)_5$~$(44)_5$之間的數值也可用以藏入機密資訊。2014 年，Lee 學者等人提出一個可逆式雙偽裝影像運用直方圖修改與模術運算資訊隱藏技術 [7]。使用兩階段藏入過程，第一階段為可逆式直方圖位移修改資訊隱藏技術，第二階段運用差值直方圖位移與修改法(Difference Histogram Shifting and Modification)暨四象限魔術矩陣的模數運算(Modulo Calculation on a Four-quadrant Magic Matrix)之可逆式資訊隱藏技術。第二階段使用的對角魔術矩陣會造成像素對中的兩個像素值同時被改變，進而影響影像品質，因此若將差值的四象限對角魔術矩陣模數運算改為差值的四象限十字魔術矩陣模數運算，將可在影像品質大幅提昇。因為使用十字魔術矩陣進行機密資訊藏入，像素對中只會有其中一個像素值被改變，因此能夠大幅提高影像品質，同時又可保有穩定而極高的藏量。

二、文獻探討

本節為維持一致性與提升可讀性，會定義本論文使用到的所有相關符號，如 2.1 節詳述。 2.2 節接續介紹可逆式直方圖位移修改資訊隱藏技術。

2.1 相關符號定義

為維持一致性與提升可讀性，製表定義本研究使用到的所有相關符號，如**表 2-1** 所示。

表 2-1: 相關符號定義

符號	定義
H 與 W	一張影像的長與寬
$I(p_1, p_2, p_3, \dots, p_{H\times W})$	一張有 $H\times W$ 個介於 0~255 像素值的原始影像
$I_1(p_1^1, p_2^1, p_3^1, \dots, p_{H\times W}^1)$	兩張有 $H\times W$ 個介於 0~255 像素值的第一張原始影像
$I_2(p_1^2, p_2^2, p_3^2, \dots, p_{H\times W}^2)$	兩張有 $H\times W$ 個介於 0~255 像素值的第二張原始影像
$I'(q_1, q_2, q_3, \dots, q_{H\times W})$	一張有 $H\times W$ 個介於 0~255 像素值的偽裝影像
$I_1'(q_1^1, q_2^1, q_3^1, \dots, q_{H\times W}^1)$	兩張有 $H\times W$ 個介於 0~255 像素值的第一張偽裝影像
$I_2'(q_1^2, q_2^2, q_3^2, \dots, q_{H\times W}^2)$	兩張有 $H\times W$ 個介於 0~255 像素值的第二張偽裝影像
$P(v_1, v_2, v_3, \dots, v_{H\times W})$	一張有 $H\times W$ 個介於 0~255 像素值的預測影像
$P'(e_1, e_2, e_3, \dots, e_{H\times W})$	一張有 $H\times W$ 個介於 0~255 像素值的預測誤差影像
$P''(r_1, r_2, r_3, \dots, r_{H\times W})$	將由預測誤差影像P'轉換的預測誤差影像
$S(s_1, s_2, s_3, \dots)$	一組隨機產生 0 與 1 的二進制機密訊息

2.3 可逆式直方圖位移修改資訊隱藏技術

Ni 學者等人於 2006 年提出一個直方圖位移修改技術的可逆式資訊隱藏技術 [10]。主要方法是統計原始影像中所有像素值的出現次數，以產生一張直方圖，再將出現次數最高的像素值設定為峰值點，出現次數最低的像素值設定為零值點。接著位移介於兩點之間的像素值，以空出峰值點左或右的位置並藏入機密訊息。因為像素都只位移一個單位，所以改變幅度並不大，如此即可維持影像品質，但藏入量與峰值點的出現次數成正比，因此整體而言藏入量並不穩定。以下步驟將說明機密訊息的藏入程序：

輸入：一張原始影像I與機密訊息S。

輸出：一張偽裝影像I'、峰值點p與零值點z。

步驟一：統計原始影像 I 像素值$p_i \in \{0, 1, 2, \dots, 255\}$的出現次數，並產生一張直方圖$H$。

步驟二：在直方圖H中，尋找出現次數最多的像素值設定為峰值點p，出現次數最少的像素值設定為零值點z。

步驟三：判斷峰值點p與零值點z的大小，並將兩者之間的像素值p_i根據以下條件進行位移，以產生偽裝像素值q_i：

$$q_i = \begin{cases} p_i - 1, \text{if } z < p_i < p, \\ p_i + 1, \text{if } z > p_i > p. \end{cases} \quad (2\text{-}1)$$

當$z < p_i < p$時，偽裝像素$q_i = p_i - 1$，即為往左位移，使像素值 p-1 的出現次數為零。

當$z > p_i > p$時，偽裝像素$q_i = p_i + 1$，即為往右位移，使像素值 p+1 的出現次數為零。

步驟四： 機密訊息$s_i \in \{0,1\}$會藏入於峰值點p處，其藏入後的偽裝像素值如下：

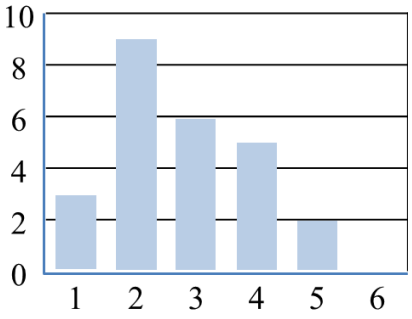
$$q_i = \begin{cases} p, & \text{if } s_i = 0, \\ p-1, & \text{if } s_i = 1 \text{ and } z < p, \\ p+1, & \text{if } s_i = 1 \text{ and } z > p. \end{cases} \quad (2\text{-}2)$$

範例 2-1

假設有一張大小為 5×5 的原始影像 I 如圖 2-1(a)所示。首先，將原始影像 I 中像素出現的次數進行直方圖統計後，從圖 2-1(b)中得知出現次數最高的像素為 2，則表示為尖峰點 p=2;出現次數為零的像素為 6，則為零點 z=6。判斷尖峰點 p 小於零點，將介於尖峰點 p 與零點 z 之間的像素(即 3、4、5)進行向右位移，得到位移後的像素如圖 2-2(a)以及位移後像素直方圖 2-2(b)所示。

1	2	3	2	2
2	4	2	4	3
3	5	3	4	2
4	2	1	3	4
2	5	3	2	1

(a)

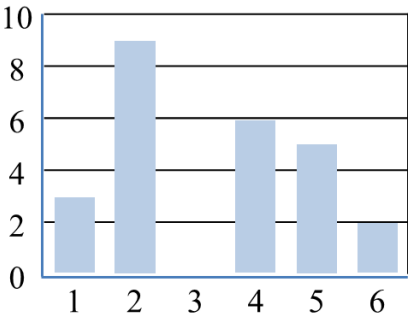


(b)

圖 2-1 原始影像 I(a)與原始影像 I 的直方圖統計(b)

1	2	4	2	2
2	5	2	5	4
4	6	4	5	2
5	2	1	4	5
2	6	4	2	1

(a)



(b)

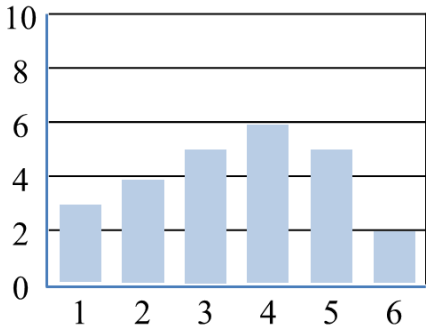
圖 2-2 像素位移後影像(a)與對應的直方圖統計(b)

最後，將一串二進制的機密資訊 S = 010011101 藏入尖峰點 p=2 之處，故當 s = 0 時則該像素維持在像素值 2；然而當 s = 1 時則將像素值 2 加上 1 變成像素值 3。將所有的機密

資訊都藏入尖峰點後，我們就可以得到一張偽裝影像 I'如圖 2-3(a)與偽裝影像直方圖如圖 2-3(b)。

1	2	4	3	2
2	5	3	5	4
4	6	4	5	3
5	3	1	4	5
2	6	4	3	1

(a)



(b)

圖 2-3 藏入機密資訊的影像(a)與對應的直方圖統計(b)

Ni 等學者[10]提出了一個簡單的可逆式資訊隱藏方法，只針對灰階影像的像素值進行稍微修改，就能夠嵌入機密資訊。然而機密資訊只有藏在尖峰點(Peak Point)中，一張影像的尖峰點若是不多，則該影像只能攜帶少量的機密資訊(512×512 的灰階影像約 5–80 K bits)。因此，後續有許多學者進行改良以提高機密資訊藏入數量。

三、Chang 學者等人所提出的可逆式雙影像資訊隱藏技術

3.1 對角魔術矩陣之可逆式雙影像資訊隱藏技術(2007)

Chang 學者等人於 2007 年提出一個可逆式雙影像藏匿技術 [3]。主要方法是利用 EMD (Exploiting Modification Direction) [10]的運算方法，產生像素對組成的五進制對角魔術矩陣如圖 2-4，並透過魔術矩陣修改像素對後，以對角線的方式藏入機密資訊，對角線的範圍是 5×5 區塊。以下步驟將說明機密訊息的藏入程序：

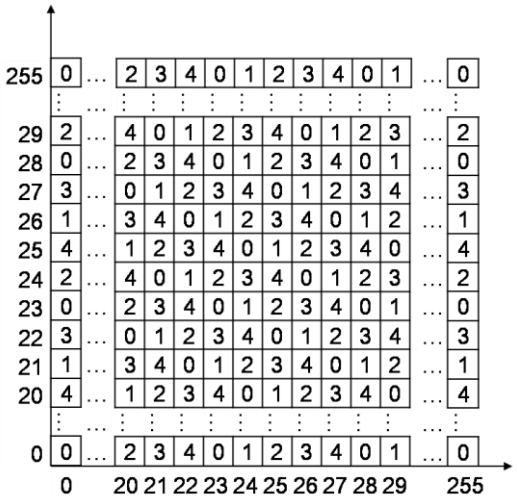


圖 2-4: 五進制對角魔術矩陣

輸入：一張原始影像I與機密訊息S。

輸出：兩張偽裝影像I_1'與I_2'。

步驟一：For i = 1 至$(H\times W)/2$，j = 1 至 k：從原始影像I中由上而下、由左而右，每次取出一組像素對為$(p_i\ ,p_{i+1})$。如果像素值p_i <2, p_{i+1} <2 或p_i >253, p_{i+1} >253 時，表示無法藏入機密資訊，因此直接將偽裝像素對的值設成(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1)與(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2)。

處理外溢問題，將$p_i = 0$與p_i =255 分別修改為 1 與 254，並記錄於位置圖B中。

步驟二：如果 $2\leq p_i, p_{i+1}+1 \leq 253$，則以$(p_i\ ,p_{i+1})$為魔術矩陣$M$的中心座標位置，並且將$(p_i\ ,p_{i+1})$及代入公式(3-1)：

$$f(p_1, p_2, p_3, \dots, p_n) = (\sum_{i=0}^{n} p_i \times i) \bmod (2n+1) \quad \text{(3-1)}$$

步驟三：候選值集合D_1和 D_2分別是 135 度對角線和 45 度對角線的 5 個五進制數值{0, 1, 2, 3, 4}所構成的集合。也就是：

$$D_1 = \{M(p_i+2, p_{i+1}-2),$$
$$M(p_i+1, p_{i+1}-1),$$
$$M(p_i, p_{i+1}),$$
$$M(p_i-1, p_{i+1}+1),$$
$$M(p_i-2, p_{i+1}-1).\}\ \text{與}$$

$$D_2 = \{M(p_i+2, p_{i+1}-2),$$
$$M(p_i+1, p_{i+1}-1),$$
$$M(p_i, p_{i+1}),$$

$$M(p_i - 1, p_{i+1} + 1),$$
$$M(p_i - 2, p_{i+1} - 1).\} \quad (3\text{-}2)$$

而(p_i, p_{i+1})及代入公式(3-2)所得到的五進制數值即為$M(p_i, p_{i+1})$。

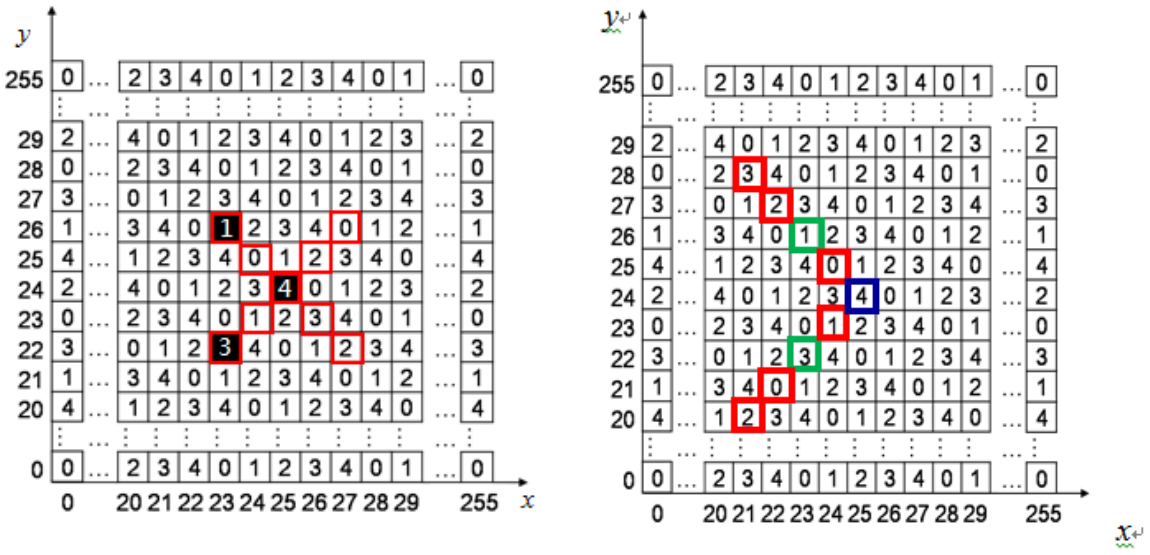
步驟四：在候選值集合D_1中找出和五進制機密數值s_j相等的矩陣元素$M(a', b')$後，並將偽裝像素值設為$(q_i^1, q_{i+1}^1) = (a', b')$即表示機密資訊$s_j$藏到偽裝影像$I_1'$中。

步驟五：在候選值集合D_2中找出和機密數值s_{j+1}相等的矩陣元素$M(a'', b'')$後，並將偽裝像素值設為$(q_i^2, q_{i+1}^2) = (a'', b'')$即表示機密資訊$s_{j+1}$藏到偽裝影像$I_2'$中。

步驟六：令$i = i + 2$及 $j = j + 2$，當原始影像I中的像素對反覆做完步驟二至步驟四的步驟後，就可以得到兩張偽裝影像 I_1'與I_2'。

範例 2-2

假設從原始影像中取出像素對$(p_1, p_2) = (25, 24)$，而預藏入的機密資訊$(s_1\ s_2)_5 = (1\ 3)_5$。透過公式(2-4)計算出兩組候選值集合D_1與D_2，分別 $D_1 = \{M(27, 22)=2, M(26, 23)=3, M(25, 24)=4, M(24, 25)=0, M(23, 26)=1\}$與$D_2 = \{M(27, 26)=0, M(26, 25)=2, M(25, 24)=4, M(24, 23)=1, M(23, 22)=3\}$，接著將機密數值 $s_1 = 1$ 與 D_1 中的候選值進行比對，得到偽裝影像值$(q_1^1, q_2^1) = (23, 26)$；接著將機密數值$s_2 = 3$ 與 D_2 中的候選值進行比對，得到偽裝影像值$(q_1^2, q_2^2) = (23, 22)$，最後可以得到兩張偽裝影像。當接收方收到兩張經過偽裝的影像後，先各取出一組像素對，分別為$(q_1^1, q_2^1) = (23, 26)$與$(q_1^2, q_2^2) = (23, 22)$，並利用公式(2-3)將藏入的機密資訊$(1\ 3)_5$取出。最後再利用取出的像素對，產生兩組候選值集合 D_1'與 D_2'，並從式(2-3)將藏入的機密資訊$(1\ 3)_5$取出。最後再利用取出的像素對，產生兩組候選值集合 D_1'與 D_2'中找出具有相同的像素對$(25, 24)$，便還原回原始的像素對。



(a) (b)

圖 2-5: 五進制對角魔術矩陣的訊息藏匿(a)與取出(b)

Chang 等學者[3]提出的可逆式之雙偽裝影像技術，能夠提升機密資訊在傳送時的安全性與資訊負載量，但此方法為直接針對像素值進行機密資訊的藏入，在最壞的情況下，在一對的像素中每一個像素值皆可能被加 2 或減 2，因此會增加偽裝像素的失真度，對於影像品質影響較大。

3.2 十字魔術矩陣之可逆式雙影像資訊隱藏技術

Chang 學者等人隨後於 2009 年 [2] 提出一個使用十字魔術矩陣代替對角魔術矩陣，由 5×5 區塊改變為 1×5 區塊。以下步驟將說明機密訊息的藏入程序：

輸入：一張原始影像I與機密訊息S。

輸出：兩張偽裝影像I_1'與I_2'。

步驟一：For i = 1 至$(H\times W)/2$，j = 1 至 k：從原始影像I中由上而下、由左而右，每次取出一組像素對為(p_i, p_{i+1})。如果像素值$p_i < 2, p_{i+1} < 2$或$p_i > 253, p_{i+1} > 253$時，表示無法藏入機密資訊，因此直接將偽裝像素對的值設成$(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1)$與$(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2)$。

處理外溢問題，將$p_i = 0$與$p_i = 255$分別修改為 1 與 254，並記錄於位置圖B中。

步驟二：如果$2 \le p_i, p_{i+1} + 1 \le 253$，則以$(p_i, p_{i+1})$為魔術矩陣$M$的中心座標位置，並且將$(p_i, p_{i+1})$及代入公式(3-3)：

$$f(p_1, p_2, p_3, \dots, p_n) = (\sum_{i=0}^{n} p_i \times i) \bmod (2n+1) \quad \text{(3-3)}$$

步驟三：候選值集合D_1和 D_2分別是 135 度對角 線和 45 度對角線的 5 個五進制數值{0, 1, 2, 3, 4}所構成的集合。也就是：

$$D_1 = \{M(p_i, p_{i+1} - 2), M(p_i, p_{i+1} - 1), M(p_i, p_{i+1}), M(p_i, p_{i+1} + 1), M(p_i, p_{i+1} - 1).\} \text{ 與}$$

$$D_2 = \{M(p_i + 2, p_{i+1}), M(p_i + 1, p_{i+1}), M(p_i, p_{i+1}),$$

$$M(p_i - 1, p_{i+1}),$$
$$M(p_i - 2, p_{i+1}).\} \quad (3\text{-}4)$$

而$(p_i\ , p_{i+1})$及代入公式(3-4)所得到的五進制數值即為$M(p_i, p_{i+1})$。

步驟四：在候選值集合D_1中找出和五進制機密數值s_j相等的矩陣元素$M(a', b')$後，並將偽裝像素值設為$(q_i^1, q_{i+1}^1) = (a', b')$即表 示機密資訊$s_j$藏到偽裝影像$I_1'$中。

步驟五：在候選值集合D_2中找出和機密數值s_{j+1}相等的矩陣元素$M(a'', b'')$後，並將偽裝像素值設為$(q_i^2, q_{i+1}^2) = (a'', b'')$即表示機密資訊$s_{j+1}$藏到偽裝影像$I_2'$中。

步驟六：令$i = i + 2$及 $j = j + 2$，當原始影像I中的像素對反覆做完步驟二至步驟四的步驟後，就可以得到兩張偽裝影像 I_1'與I_2'。

為改善對角魔術矩陣失真問題，Chang 等學者[2]使用十字魔術矩陣代替對角魔術矩陣的可逆式之雙偽裝影像技術，不僅能夠提升機密資訊在傳送時的安全性與資訊負載量，在一載體像素對中只會有一個像素可能被加 2 或減 2，如此可顯著減少失真度，提高影像品質，同時保持高藏量。

四、基植於位置性之可逆式雙偽裝影像隱藏技術

Lee 學者等人於 2009 年[8]與 2011 年[9]分別提出基植於位置性的雙影像技術。將像素對視為一組座標，以該像素對為中心點，搭配藏匿策略調整座標位置以藏入機密訊息並將改變過的座標視為偽裝影像的影素對。因為在藏匿訊息位元的過程是環繞著中心點進行微調，故所產生的影像品質極高，其藏入的流程如 0 所示，先以原始影像複製出兩張與原始影像完全相同的影像來做為掩護影像，並以一把私鑰（Private Key）來輔助資訊的嵌入以強化資訊的安全性並輸出兩張偽裝影像，當使用者接收到兩張偽裝影像後需以相同一把私鑰才能正確無誤的取出機密訊息並還原原始影像。Lee 學者等人所提出的基植於位置性之可逆式雙影像技術將分別在 4.1 與 4.2 節說明之。

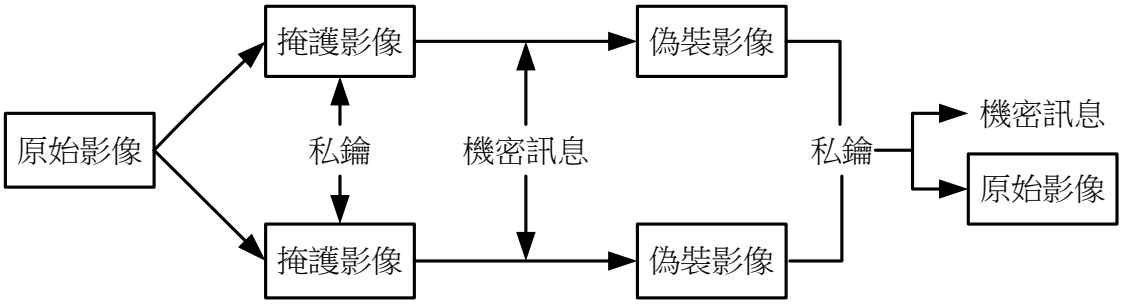


圖 4-1:植基於雙偽裝影像之可逆式資訊隱藏技術流程圖

4.1 十字座標空間位置法可逆式雙偽裝影像高影像品質資訊隱藏技術

Lee 學者等人於 2009 年提出一個可逆式雙偽裝影像高影像品質資訊隱藏技術 [8]。主方法是透過十字座標空間位置法(Cross Position)，讓影像在進行機密資訊藏入時，像素值不會有大幅度的調整，使影像品質高達 52.3dB。

每次從原始影像中取出一個將像素對(p_i, p_{i+1})投射到一個二維的十字座標的位置空間，使得像素值p_i對應 X 軸的座標值，像素值p_{i+1}則對應 Y 軸的座標值；如圖 4-2 的所示，根據(p_i, p_{i+1})的座標可以在座標空間中找到一個點作為中心點(如圖 4-2 中心點*)，此中心點位於十字座標中央，並將機密訊息的四種組合分別定義在十字座標中心點的上、下、左、右四個方位，進行機密訊息嵌入時，偽裝影像的像素值便根據十字座標中的機密訊息組合去修改產生。當嵌入的機密訊息為 “00”時(p_i, p_{i+1})需往右位移，從二維座標 X 軸 Y 軸的觀念來看相當於 X 軸座標值加 1 而 Y 軸座標值保持不變，因此偽裝像素值會等於$(p_i + 1, p_{i+1})$；而當機密訊息為“10”時就如同由中心點向上位移，因此偽裝像素值便等於$(p_i, p_{i+1} + 1)$；透過此概念嵌入機密訊息“01”和“11”時 ，則偽裝像素值分別會等於$(p_i, p_{i+1} - 1)$以及$(p_i - 1, p_{i+1})$。以下步驟將說明機密訊息的藏入程序：

輸入：一張原始影像I與機密訊息S。

輸出：兩張偽裝影像I_1'與I_2'。

步驟一：將輸入的原始影像I另外複製出兩張相同的影像，分別I_1及I_2。

步驟二：透過私鑰PK(private key)決定I_1為主要原始影像，而 I_2為輔助原始影像，分別藏入兩位元的機密資訊。

步驟三：For $i = 1$至$(H \times W)/2$：首先從主要原始影像I_1中，分次取出一組像素對(p_i^1, p_{i+1}^1)。當像素對中有一個像素值$(p_i^1, p_{i+1}^1) \le 0$或$(p_i^1, p_{1+1}^1) \ge 255$時，則表示無法藏入機密資訊，因此直接將偽裝像素對的值設成$(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1)$，並跳至步驟七。

步驟四：可以藏入機密資訊，則主要原始影像的機密資訊組$S = s_j s_{j+1}$會有下列四種模式產生：

模式 1：$s_j s_{j+1} =$ "00"，則$(q_i^1, q_{i+1}^1) = (p_i^1 + 1, p_{i+1}^1)$。

模式 2：$s_j s_{j+1} =$ "10"，則$(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1 + 1)$。

模式 3：$s_j s_{j+1} =$ "11"，則$(q_i^1, q_{i+1}^1) = (p_i^1 - 1, p_{i+1}^1)$。

模式 4：$s_j s_{j+1} =$ "01"，則$(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1 - 1)$。

步驟五：同樣的從輔助原始影像I_2中，取出一組像素對(p_i^2, p_{i+1}^2)。當像素對中有一個像素值$(p_i^2, p_{i+1}^2) \le 0$或$(p_i^2, p_{i+1}^2) \ge 255$ 時， 則表示無法藏入機密資訊，則直接將偽裝像素對的值設成$(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2)$，並跳至步驟七。

步驟六：可以藏入機密資訊，則輔助原始影像的機密資訊組 $S = s_{j+2} s_{j+3}$會有下列八種模式產生：

模式 1：當$s_j s_{J+1}$ = "00"時，且$s_{j+2}s_{j+3}$ = "11"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2)$，如圖 4-3(a)所示。

模式 2：當$s_j s_{J+1}$ = "00"時，且$s_{j+2}s_{j+3}$ = "01"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2 - 1)$，如圖 4-3(b)所示。

模式 3：當$s_j s_{J+1}$ = "10"時，且$s_{j+2}s_{j+3}$ = "01"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2 - 1)$，如圖 4-3(c)所示。

模式 4：當$s_j s_{J+1}$ = "10"時，且$s_{j+2}s_{j+3}$ = "00"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2 + 1, p_{i+1}^2)$，如圖 4-3(d)所示。

模式 5：當$s_j s_{J+1}$ = "11"時，且$s_{j+2}s_{j+3}$ = "00"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2 + 1, p_{i+1}^2)$，如圖 4-3(e)所示。

模式 6：當$s_j s_{J+1}$ = "11"時，且$s_{j+2}s_{j+3}$ = "10"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2 + 1)$，如圖 4-3(f)所示。

模式 7：當$s_j s_{J+1}$ = "01"時，且$s_{j+2}s_{j+3}$ = "10"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2 + 1)$，如圖 4-3(g)所示。

模式 8：當$s_j s_{J+1}$ = "01"時，且$s_{j+2}s_{j+3}$ = "11"，則 $s_{j+2}s_{j+3}$ 可以被藏入，而 $(q_i^2, q_{i+1}^2) = (p_i^2 + 1, p_{i+1}^2)$，如圖 4-3(h)所示。

步驟七：令$i = i + 2; j = j + 4$，直到I_1和 I_2中所有的像素對都進行步驟四到步驟六後，就會得到兩張進行偽裝過的影像I_1'與I_2'。

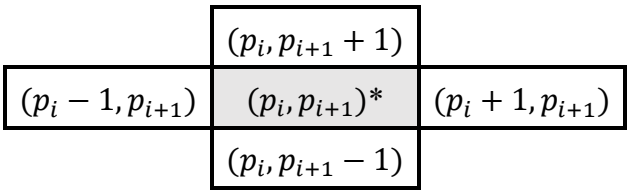


圖 4-2: 十字座標示意圖

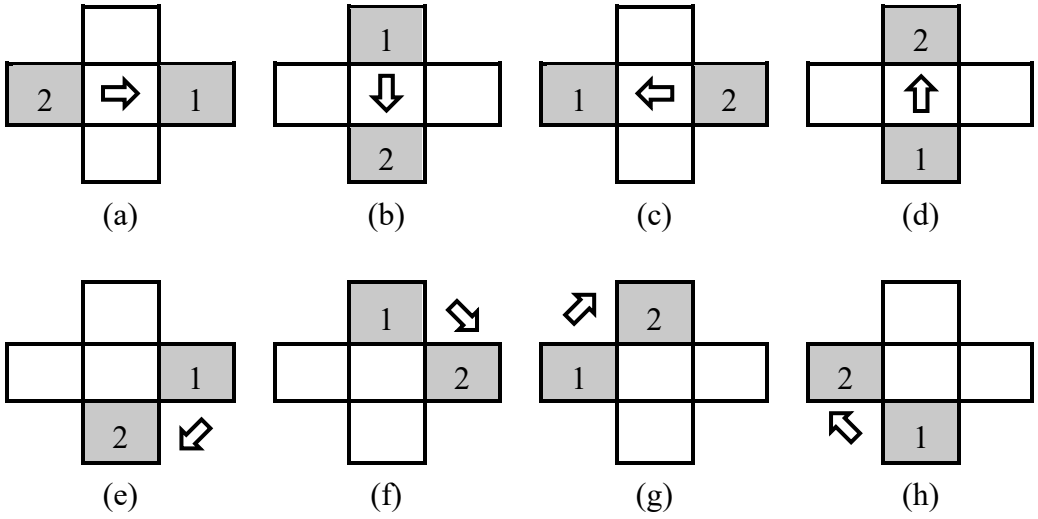


圖 4-3:主要原始影像與輔助原始影像藏入機密資訊組合示意圖；
(a)~(d)為對向位置，(e)~(h)為順時鐘方向位置

4.2 可逆式雙偽裝影像位置組合資訊隱藏技術

Lee 學者等人於 2011 年提出一個可逆式雙偽裝影像位置組合資訊隱藏技術[9]，會將像素值投射至二維的像素值座標空間中，進行修改以產生偽裝影像，如 0 所示，其中*代表以掩護像素值做為座標所投射在二維座標空間中的位置，而機密訊息的嵌入策略依 $s_1 \in \{0, 1, 2, 3, 4\}$分為 5 種型態，每一種型態又各自對應機密訊息 $s_2 \in \{0, 1, 2, 3, 4\}$ 的 5 種數值，因此共有 25 種嵌入策略如表 4-1 整理所示。

就我們所知，以 2 個 5 進制機密數值表示其最大值$(44)_5$，而 10 進制數值則為$(24)_{10}$，但 Chang 等學者[3][2]所提出的方法，每次只能提取最大值僅為$(1111)_2 = (15)_{10} = (30)_5$。因此在 Chang 等學者所提出的方法中，2 個位數的 5 進制訊息中$(31)_5$到$(44)_5$之間的值皆無法用來藏入機密資訊。Lee 學者等人的可逆式雙偽裝影像位置組合資訊隱藏技術 [9]亦提出 5 進制的數字轉換系統的機密訊息的擷取藏匿方式，目的為讓 2 位數的 5 進制數值$(00)_5$~$(44)_5$都能用來藏入機密資訊，使得安全性、影像品質和負載

量皆同時提升。以下步驟將說明機密訊息的藏入程序：

前置作業：從機密資訊S中每次取 5 位元轉換為十進制的數值k，若k小於十進制 24，則將k轉換成 2 個五進制數值$s_j s_{j+1}$； 若k大於十進制 24，僅從機密資訊S中取出 4 位元的機密資訊，並轉換為 2 個五進制數值$s_j s_{j+1}$。

輸入：一張原始影像I與機密訊息S。

輸出：兩張偽裝影像I_1'與I_2'。

步驟一：將輸入的原始影像I，另外再複製出兩張相同的原始影像 I_1 和 I_2，接著分別I_1和I_2中，取出相同的像素對(p_i, p_{i+1})，再利用隨機產生的二元私鑰PK決定主要掩護像素對 (Major)與輔助掩護像素對(Auxiliary)。

步驟二：將機密資訊$s_j s_{j+1}$配置在九宮格的十字空間座標中，並以原始影像對(p_i, p_{i+1})作為九宮格的中央位置，用*符號標示，如圖 4-4 所示。透過藏入策略表 4-1 進行訊息藏入後，最後就能依照座標位置來對像數值進行加減，可分別得到兩張偽裝影像I_1'和I_2'。

當私鑰 PK=1 並嵌入機密訊息 s_1 與 s_2 分別產生主要偽裝像素對(q_i^1, q_{i+1}^1)和輔助偽裝像素對(q_i^2, q_{i+1}^2)之後需檢查是否發生溢位，若偽裝像素值$q_i^1, q_{i+1}^1, q_i^2, q_{i+1}^2$其中有一值發生了小於零或大於 255 的溢位狀況，則不進行嵌入機密訊息 s_1 與 s_2 且依下列規則來調整偽裝像素：

規則 1：當q_i^1或q_{i+1}^1大於 255，則 $(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1)$且$(q_i^2, q_{i+1}^2) = (p_i^2 - 3, p_{i+1}^2)$。

規則 2：當q_i^2或 q_{i+1}^2大於 255，則$(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1)$且$(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2 - 3)$。

規則 3：當q_i^1或q_{i+1}^1小於 0，則$(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1)$且$(q_i^2, q_{i+1}^2) = (p_i^2 + 3, p_{i+1}^2)$。

規則 4：當q_i^2或 q_{i+1}^2小於 0，則$(q_i^1, q_{i+1}^1) = (p_i^1, p_{i+1}^1)$且$(q_i^2, q_{i+1}^2) = (p_i^2, p_{i+1}^2 + 3)$。

範例 4-1

假設原始影像$I = (100, 100)$、私鑰 $PK = 1$且二元機密訊息S=10011。首先，轉換二元機密訊息S成5進制機密訊息S= s_1 s_2=$(34)_5$，並且先以原始影像複製出兩影像I_1和I_2。由於$K = 1$，因此自I_1取出的像素對設為主要掩護像素對(p^1, p^1)、自I_2取出的像素對設為輔助掩護像素對(p^2, p^2)。：嵌入機密訊息 s_1 =3 s_2=4，故套用 0 中的策略 20 可得到，$(q^1, q^1) = (p^1 + 1, p^1 + 1)$ =(100+1, 100+1)=(101, 101); $(q^2, q^2) = (p^2 - 1, p^2 + 1)$=(100-1，100+1)=(99，101)，因此偽裝影像$I_1' = (101, 101)$以及偽裝影像$I_2' = (99, 101)$。

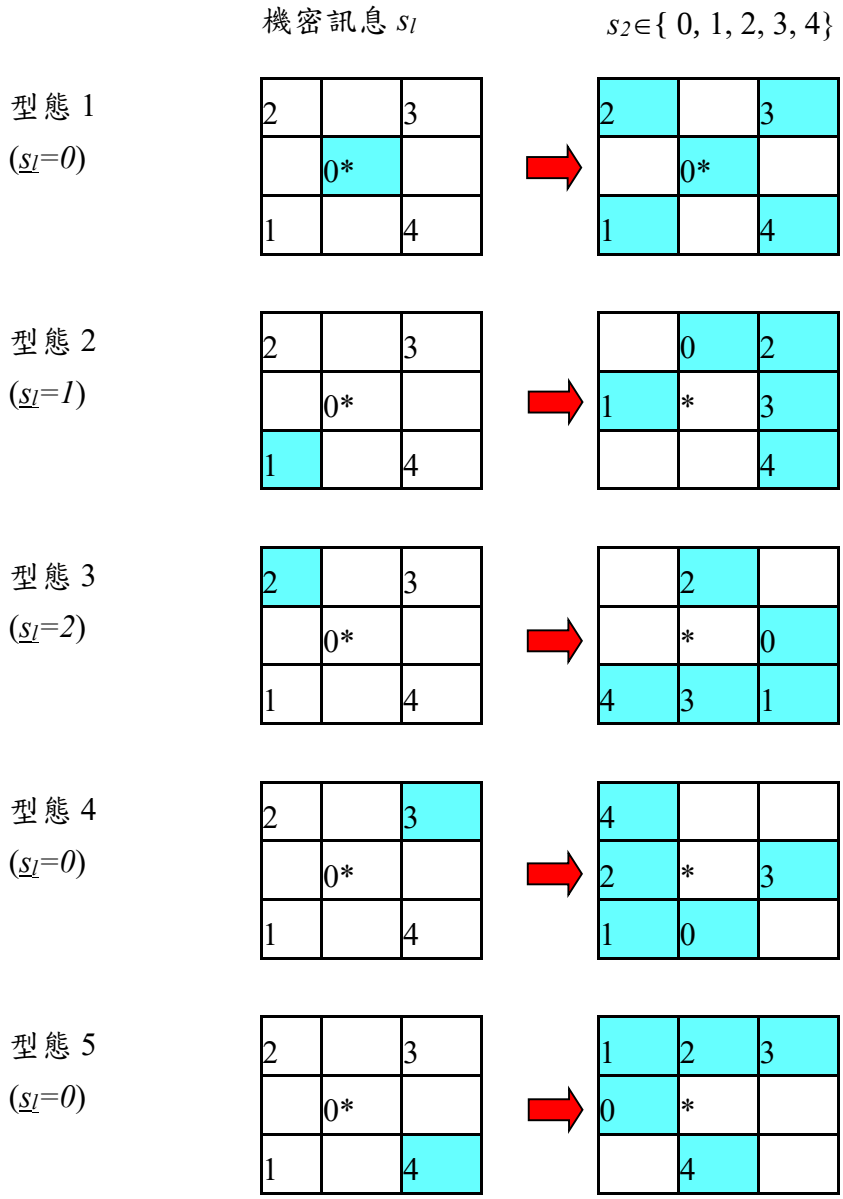


圖 4-4 機密訊息 s_1s_2 的嵌入策略圖；*為掩護像素值之位置

表 4-1 機密資訊 s_1 與 s_2 的嵌入策略(當 PK=1 時)

策略	機密資訊	主要偽裝像素 (q_i^1, q_{i+1}^1)	輔助偽裝像素 (q_i^2, q_{i+1}^2)
1	當 s_1= 0 且 s_2=*0*	(p_i^1, p_{i+1}^1)	(p_i^2, p_{i+1}^2)
2	當 s_1= 0 且 s_2=*1*		$(p_i^2 - 1, p_{i+1}^2 - 1)$
3	當 s_1= 0 且 s_2=*2*		$(p_i^2 - 1, p_{i+1}^2 + 1)$
4	當 s_1= 0 且 s_2=*3*		$(p_i^2 + 1, p_{i+1}^2 + 1)$
5	當 s_1= 0 且 s_2=*4*		$(p_i^2 + 1, p_{i+1}^2 - 1)$
6	當 s_1= 1 且 s_2=*0*	$(p_i^1 - 1, p_{i+1}^1 - 1)$	$(p_i^2, p_{i+1}^2 + 1)$
7	當 s_1= 1 且 s_2=*1*		$(p_i^2 - 1, p_{i+1}^2)$
8	當 s_1= 1 且 s_2=*2*		$(p_i^2 + 1, p_{i+1}^2 + 1)$
9	當 s_1= 1 且 s_2=*3*		$(p_i^2 + 1, p_{i+1}^2)$
10	當 s_1= 1 且 s_2=*4*		$(p_i^2 + 1, p_{i+1}^2 - 1)$
11	當 s_1= 2 且 s_2=*0*	$(p_i^1 - 1, p_{i+1}^1 + 1)$	$(p_i^2 + 1, p_{i+1}^2)$
12	當 s_1= 2 且 s_2=*1*		$(p_i^2 + 1, p_{i+1}^2 - 1)$
13	當 s_1= 2 且 s_2=*2*		$(p_i^2, p_{i+1}^2 + 1)$
14	當 s_1= 2 且 s_2=*3*		$(p_i^2, p_{i+1}^2 - 1)$
15	當 s_1= 2 且 s_2=*4*		$(p_i^2 - 1, p_{i+1}^2 - 1)$
16	當 s_1= 3 且 s_2=*0*	$(p_i^1 + 1, p_{i+1}^1 + 1)$	$(p_i^2, p_{i+1}^2 - 1)$
17	當 s_1= 3 且 s_2=*1*		$(p_i^2 - 1, p_{i+1}^2 - 1)$
18	當 s_1= 3 且 s_2=*2*		$(p_i^2 - 1, p_{i+1}^2)$
19	當 s_1= 3 且 s_2=*3*		$(p_i^2 + 1, p_{i+1}^2)$
20	當 s_1= 3 且 s_2=*4*		$(p_i^2 - 1, p_{i+1}^2 + 1)$
21	當 s_1= 4 且 s_2=*0*	$(p_i^1 + 1, p_{i+1}^1 - 1)$	$(p_i^2 - 1, p_{i+1}^2)$
22	當 s_1= 4 且 s_2=*1*		$(p_i^2 - 1, p_{i+1}^2 + 1)$
23	當 s_1= 4 且 s_2=*2*		$(p_i^2, p_{i+1}^2 + 1)$
24	當 s_1= 4 且 s_2=*3*		$(p_i^2 + 1, p_{i+1}^2 + 1)$
25	當 s_1= 4 且 s_2=*4*		$(p_i^2, p_{i+1}^2 - 1)$

五、可逆式雙偽裝影像運用直方圖修改與模術運算資訊隱藏技術

Lee 學者等人於 2014 年提出一個可逆式雙偽裝影像運用直方圖修改與模數運算之可逆式資訊隱藏技術[7]。主要方法共有 2 階段進行訊息的藏匿，分別運用差值直方圖位移與修改法(Difference Histogram Shifting and Modification)暨四象限魔術矩陣的模數運算(Modulo Calculation on a Four-quadrant Magic Matrix)之可逆式資訊隱藏技術。輸入一張影像 I 來做為預備嵌入機密資訊的掩護影像(Cover Image)，將掩護影像切割成一個個 3×3 大小的掩護影像區塊(cover image block)，每一區塊可產生四個群組G_1、G_2、G_3、G_4，其中$G_1 = \{p_5, p_2, p_1\}$、$G_2 = \{p_5, p_4, p_7\}$、$G_3 = \{p_5, p_8, p_9\}$及$G_4 = \{p_5, p_6, p_3\}$，如圖 5-1 所示，中心位置的 p_5即為參考像素(reference pixel)。計算群組中參考像素(reference pixel)與其相鄰像素(adjacent pixel)間的差值，其中每一群組皆可運用差值的修正每次都能將 2 個五進制的機密資訊嵌入，而產生兩個偽裝影像區塊(stego-image block)。

*p*1	*p*2	*p*3
*p*4	*P*5	*p*6
*p*7	*p*8	*p*9

圖 5-1: 每次取出 3×3 的像素區塊

結合差值直方圖位移修改法與四象限魔術矩陣模數運算方法(本文以 dHw4Q 稱之)的流程如圖 5-2 所示。Phase1 為第一階段機密資訊的嵌入；Phase2 為第二階段機密資訊的嵌入，以及 Phase3 為機密資訊的取出與還原。其說明如下：在第一階段中，計算相鄰像素間的差值，再採用可逆式直方圖位移修改資訊隱藏技術，進行第一階段的機密資訊藏入。為了提升藏量與機密資訊的安全性，第二階段採用在相鄰像素間的差值的模數(Modulo) 運算，提出一個四象限魔術矩陣的可逆式資訊隱藏技術。

在第二階段中所提出的方法中，每一個五進制的機密資訊系統的數字可用 $\log_2 5$bits 表示之， 每一個掩護影像區塊有四個群組可藏 2 個五進制的機密資訊，故每一個區塊可藏入 $4\times(2\times\log_2 5)$ bits，因此計算每一張偽裝影像的資訊嵌入率為 $2\times\frac{4}{9}$ $(2\times\log_2 5)/2$ bits per pixel，也就是第二階段的藏入率為$\frac{4}{9}(\log_2 5)$bpp。以下將分為兩階段說明機密訊息的藏入程序：

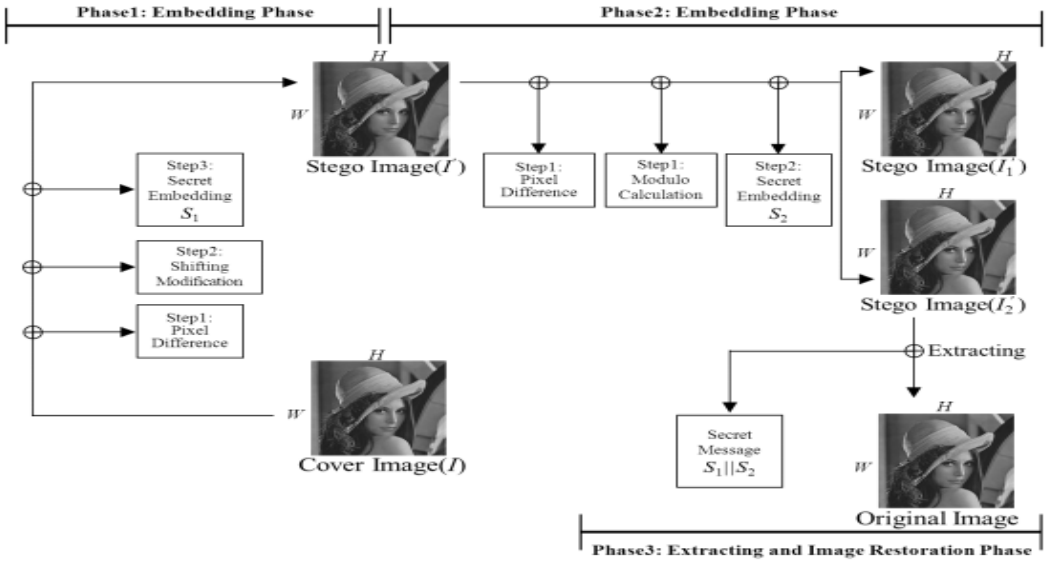


圖 5-2: 結合差值直方圖位移修改法與四象限魔術矩陣模數運算方法之可逆式雙偽裝影像資訊隱藏技術(dHw4QM)流程圖

5.1 第一階段藏入

輸入：一張原始影像I與機密訊息S。

輸出：一張偽裝影像I'、正數峰值點pp、正數零值點pz、負數峰值點np與負數零值點nz。

步驟一： 為了防止溢位(underflow/overflow)問題發生，因此會將所有符合 255 的像素值改為 254 與符合 0 的像素值改為 1 後，每次取出3×3區塊B。

步驟二：將區塊B分成四個群組為G_1 、G_2 、G_3 、G_4 ，其中：

$$\begin{cases} G_1 = \{q_5, q_2, q_1\}, \\ G_2 = \{q_5, q_4, q_7\}, \\ G_3 = \{q_5, q_8, q_9\}, \\ G_4 = \{q_5, q_6, q_3\}. \end{cases}$$

步驟三：計算區塊B中的每個群組G_k $(k = 1,2,3,4)$之兩個差值。

$$\begin{cases} d_{11} = q_5 - q_2 \\ d_{12} = q_5 - q_1 \end{cases}$$
$$\begin{cases} d_{21} = q_5 - q_4 \\ d_{22} = q_5 - q_7 \end{cases}$$
$$\begin{cases} d_{31} = q_5 - q_8 \\ d_{32} = q_5 - q_9 \end{cases}$$
$$\begin{cases} d_{41} = q_5 - q_6 \\ d_{42} = q_5 - q_3 \end{cases} \quad (5\text{-}1)$$

步驟四：運用直方圖統計所有區塊中的差值$d_{k(t)}(k=1,2,3,4)(t=1,2)$，找到正/負差值的峰值點與零值點。分別設定正數峰值點pp、正數零值點pz、負數峰值點np與負數零值點nz，根據差值直方圖位移與修改條件進行位移：

(1) 當$pz > d_{k(t)} > pp$，表示介於$[pp+1, pz-1]$的像素值往右邊位移一個單位，空出$(pp+1)$的位置。

(2) 當$np > d_{k(t)} > nz$，表示介於$[np-1, nz+1]$的像素值皆往左邊位移一個單位，空出$(np+1)$的位置。

步驟五：從S_1中每次提取 1 位元的機密資訊s藏入峰值點pz與np：

(1) 如果$\mathrm{s}=0$，則設定偽裝差值$d'_{k(t)} = d_{k(t)}$。

(2) 如果$\mathrm{s}=1$ 且 $pz > pp$，則設定偽裝差值$d'_{k(t)} = d_{k(t)} + 1$。

(3) 如果$\mathrm{s}=1$ 且 $np > nz$，則設定偽裝差值$d'_{k(t)} = d_{k(t)} - 1$。

5.2 第二階段藏入

輸入：一張由第一階段產生的偽裝影像I'、機密訊息S、正數峰值點pp、正數零值點pz、負數峰值點np與負數零值點nz。

輸出：兩張偽裝影像I'_1與I'_2。

步驟一：讀取影像I'，每次取出3×3區塊並且以符號B'稱之。

步驟二：將B'區塊分成四個群組為G'_1、G'_2、G'_3、G'_4，其中：

$$\begin{cases} G'_1 = \{q_5, q_2, q_1\}, \\ G'_2 = \{q_5, q_4, q_7\}, \\ G'_3 = \{q_5, q_8, q_9\}, \\ G'_4 = \{q_5, q_6, q_3\}. \end{cases}$$

步驟三：將B'區塊的每個群組$G'_k(k=1,2,3,4)$計算差值。

$$\begin{cases} d'_{11} = q_5 - q_2 \\ d'_{12} = q_5 - q_1 \end{cases}$$
$$\begin{cases} d'_{21} = q_5 - q_4 \\ d'_{22} = q_5 - q_7 \end{cases}$$
$$\begin{cases} d'_{31} = q_5 - q_8 \\ d'_{32} = q_5 - q_9 \end{cases}$$
$$\begin{cases} d'_{41} = q_5 - q_6 \\ d'_{42} = q_5 - q_3 \end{cases}$$

(5-2)

步驟四：假若 $G'_k - \{q_5\} \in \{0, 1, 253, 254\}$ 或 $d'_{k(t)} > 253$ 或$d'_{k(t)} < -253$ $(k = 1,2,3,4;\ t=1,2)$時，則會造成溢位(overflow/underflow)問題，因此群組$G'_k(for\ k=1,2,3,4)$無法藏入機密資訊，直接跳至步驟八的(規則 R1)，反之則

進行步驟五將機密訊息藏入差值中。

步驟五：若差值為$-253 < d'_{k(t)} < 253$，則將$d'_{k(t)}$ (where $t = 1,2$)代入公式(5-3)，計算魔術矩陣$M_k(k = 1,2,3,4)$的樞鈕元素值 $M_k\left(d'_{k(1)}, d'_{k(2)}\right)(for\ k = 1,2,3,4)$。

$$M_k\left(d'_{k(1)}, d'_{k(2)}\right) = \left(\sum_{t=1}^{2} d'_{k(t)} \times t\right) \bmod 5 \quad \text{(5-3)}$$

步驟六：再以樞鈕元素值做為魔術矩陣M_k的中心點，產生兩組候選元素集為$dD_{k(1)}$(135度對角候選元素集)與$\mathrm{d}D_{k(2)}$(45 度對角候選元素集)，如下所示：

$$\begin{aligned} d\mathrm{D}_{k(1)} = \{&M_k\left(d'_{k(1)} + 2, d'_{k(2)} - 2\right), \\ &M_k\left(d'_{k(1)} + 1, d'_{k(2)} - 1\right), \\ &M_k\left(d'_{k(1)}, d'_{k(2)}\right), \\ &M_k\left(d'_{k(1)} - 1, d'_{k(2)} + 1\right), \\ &M_k\left(d'_{k(1)} - 2, d'_{k(2)} - 1\right).\} \text{ 與} \\ d\mathrm{D}_{k(2)} = \{&M_k\left(d'_{k(1)} + 2, d'_{k(2)} - 2\right), \\ &M_k\left(d'_{k(1)} + 1, d'_{k(2)} - 1\right), \\ &M_k\left(d'_{k(1)}, d'_{k(2)}\right), \\ &M_k\left(d'_{k(1)} - 1, d'_{k(2)} + 1\right), \\ &M_k\left(d'_{k(1)} - 2, d'_{k(2)} - 1\right).\} \end{aligned} \quad \text{(5-4)}$$

步驟七：以 2 個五進制的機密資訊作為鍵值(key)$s_{k(1)}$與 $s_{k(1)}(for\ k = 1,2,3,4)$在候選集$D_{k(1)}$尋找符合機密資訊$s_{k(1)}$的魔術元素值$M_k\left(a_{k(1)}, b_{k(1)}\right)$，以及在 $D_{k(2)}$中尋找符合機密資訊$s_{k(2)}$的魔術元素值$M_k\left(a_{k(2)}, b_{k(2)}\right)$。並取出魔術元素所在的座標$\left(a_{k(1)}, b_{k(1)}\right)$與$\left(a_{k(2)}, b_{k(2)}\right)$。

步驟八：計算群組$G'_{k(t)}(t = 1,2)(k = 1,2,3,4)$以回儲兩組偽裝區塊$B'_1$與$B'_2$的像素值。

(規則 R1) 如果會造成溢位，則像素差值不藏入機密資訊，計算為$q_i^1 = q_i^2 = q_i$ for i=1, 2, …, 9，亦即$G'_{k(1)} = G'_{k(2)} = G'_k$。

(規則 R2) 計 算$q_5^1 = q_5$、$q_2^1 = q_5 - a_{1(1)}$、$q_1^1 = q_5 - b_{1(1)}$、$q_4^1 = q_5 - a_{2(1)}$、$q_7^1 = q_5 - b_{2(1)}$、$q_8^1 = q_5 - a_{3(1)}$、$q_9^1 = q_5 - b_{3(1)}$、$q_6^1 = q_5 - a_{4(1)}$、$q_3^1 = q_5 - b_{4(1)}$與$q_5^2 = q_5$、$q_2^2 = q_5 - a_{1(2)}$、$q_1^2 = q_5 - b_{1(2)}$、$q_4^2 = q_5 - a_{2(2)}$、$q_7^2 = q_5 - b_{2(2)}$、$q_8^2 = q_5 - a_{3(2)}$、$q_9^2 = q_5 - b_{3(2)}$、$q_6^2 = q_5 - a_{4(2)}$、$q_3^3 = q_5 - b_{4(2)}$。

可分別獲得偽裝影像區塊B'_1的四個群組$G'_{1(1)} = \{q_5^1, q_2^1, q_1^1\}$、$G'_{2(1)} = \{q_5^1, q_4^1, q_7^1\}$、$G'_{3(1)} = \{q_5^1, q_8^1, q_9^1\}$、$G'_{4(1)} = \{q_5^1, q_6^1, q_3^1\}$以及

與偽裝影像區塊B'_2的四個群組$G'_{1(2)} = \{q_5^2, q_2^2, q_1^2\}$、$G'_{2(2)} = \{q_5^2, q_4^2, q_7^2\}$、$G'_{3(2)} =$

$\{q_5^2, q_8^2, q_9^2\}$、$G'_{4(2)} = \{q_5^2, q_6^2, q_3^2\}$。

步驟九：重複步驟一至步驟八直到藏入所有的機密資訊S_2，便能得到兩張偽裝影像I'_1與I'_2。

上述，此步驟六為差值的四象限對角魔術矩陣模數運算，若將該步驟的兩個候選元素集改為下列，即為差值的四象限十字魔術矩陣模數運算。也就是在第六步驟改為樞鈕元素值做為魔術矩陣M_k的中心點，產生兩組候選元素集為$cD_{k(1)}$(90 度線候選元素集)與$cD_{k(2)}$(0 度的候選元素集)，如下所示，其他步驟皆如上述。

$$\begin{aligned} cD_{k(1)} = \{&M_k\left(d'_{k(1)}, d'_{k(2)} - 2\right),\\ &M_k\left(d'_{k(1)}, d'_{k(2)} - 1\right),\\ &M_k\left(d'_{k(1)}, d'_{k(2)}\right),\\ &M_k\left(d'_{k(1)}, d'_{k(2)} + 1\right),\\ &M_k\left(d'_{k(1)}, d'_{k(2)} + 2\right).\} \text{ 與} \end{aligned}$$

$$\begin{aligned} c\mathrm{D}_{k(2)} = \{&M_k\left(d'_{k(1)} - 2, d'_{k(2)}\right),\\ &M_k\left(d'_{k(1)} - 1, d'_{k(2)}\right),\\ &M_k\left(d'_{k(1)}, d'_{k(2)}\right),\\ &M_k\left(d'_{k(1)} + 1, d'_{k(2)}\right),\\ &M_k\left(d'_{k(1)} + 2, d'_{k(2)}\right).\} \end{aligned}$$

在第二階段使用差值的四象限十字魔術矩陣模數運算進行機密資訊藏入，像素差值對中只會有其中一個差值被改變，進而影響到的像素值亦只有一個，且此像素值最大的調幅為加 2 或減 2，因此偽裝影像的品質與原始影像差異不大，同時又可保有穩定而極高的藏量。

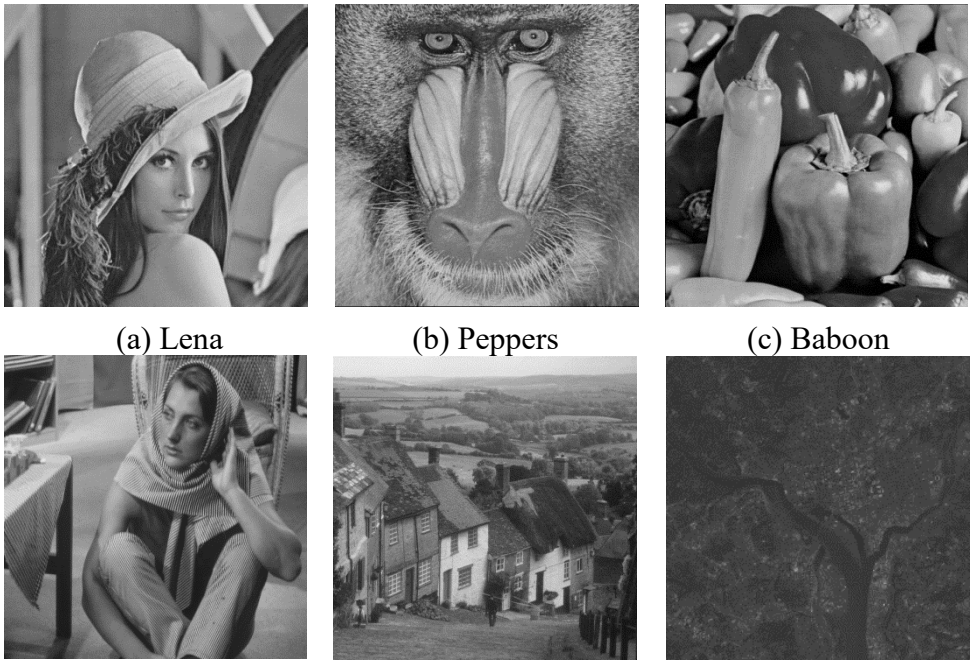
六、實驗結果

本文透過 Matlab R2010b 實作上述所提出的雙影像藏匿技術，並使用四張 512×512 大小的標準灰階影像進行實驗，分別是 Lena、Peppers、Baboon 與 Barbara，如圖 6-1 所示。本文利用資訊負載量以公式(6-1)衡量各方法的藏密能力，並採用 MSE(Mean Squared Error) 和高峰影像信號雜訊比(Peak Signal to Noise Ratio, PSNR) 評估偽裝影像品質與原始影像品質的差異程度，MSE 與 PSNR 值的計算如公式(6-2)。

$$\text{資訊負載量(bpp)} = |S|/(2HW) \tag{6-1}$$

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{MES}\right) \text{ (單位：dB)} \tag{6-2}$$

一般而言，資訊負載量是以一張影像中每一個像素可以承載機密訊息位元數(bit per pixels, bpp)。當 MSE(Mean Squared Error)越小或 PSNR(Peak Signal to Noise Ratio)越大時，代表其原始影像跟偽裝影像之差距越小，所以越不容易被他人識破有藏資訊在裡面，PSNR 的單位為 dB (decibel scale)，通常 PSNR 值在 30dB 以上時以我們人類的肉眼就難以分辨原始影像與偽裝影像的差異性。



(a) Lena (b) Peppers (c) Baboon

(d) Barbara (e) Goldhill (f)Washsat

圖 6-1: 三張 512×512 的灰階實驗影像

表 6-1 為本文所探究的數個雙偽裝影像的可逆式資訊隱藏方法在單張影像的品質、雙影像的平均影像品質及每張影像的最大藏量與資訊負載量的實驗結果比較。在表 6-1 比較 Chang 學者等人的方法[3][2]中，可觀察出兩者的藏量皆在 1 bpp，但是在 2009 年發表的十字魔術藏匿法[2]的影像品質能夠比在 2007 年發表的對角魔術藏匿法[3]的影像品質更好，平均可將 PSNR 提升 3.14dB 左右。以 Lena 影像為例，PSNR 從 48.13 dB 提升至 52.39 dB，且藏量仍能維持在約 1 bpp。

基植於位置性之可逆式雙偽裝影像隱藏技術[8][9]在影像品質方面皆有較高的 PSNR 值，尤其十字座標空間位置法的雙偽裝影像的可逆式資訊隱藏方法[8]在 PSNR 值上的表現平均約高達 52.5dB。因為十字座標空間位置法在藏入訊息的過程中僅讓像素值往上下左右一個方向移位一步。而位置組合做為藏匿策略的雙偽裝影像的可逆式資訊隱

藏方法[9]不僅可達到 49.67 dB 的高偽裝影像品質，在一張影像每個像素值的平均資訊負載量亦達到 1.07bpp。

影像一般在位置相鄰的像素間彼此的像素值具有相同或近似的特徵，因此若能善用鄰似像素值的差異大多集中在零值附近的特性，先行以差值直方圖位移修改法進行第一階段的訊息藏入，再將魔術藏匿法運用於差值數值中，可有效提昇影品質及機密訊息的藏量。由表 6-1 中可觀察到，結合差值直方圖位移修改法與四象限魔術矩陣模數運算，不論是使用對角差值候選集或十字差值候選集，皆可使資訊負載量達到更高的藏量。以 Lena 為例，不僅藏量可維持高水準約 1.12 bpp，而且 PSNR 達到 48.67 dB 的高影像品質之境地。

七、結論

現今有越來越多學者在可逆式多重影像藏匿技術的領域進行探究。所謂的多重影像藏匿法，主要是將機密資訊平均藏在多張偽裝影像上，其目的旨在增加資訊負載量並保有一定的影像品質，又能兼顧機密資訊藏在偽裝影像上的安全性。然而雖然將機密資訊平均藏在多張影像上可以有效增加資訊負載量並保有一定的影像品質，但亦會增加機密資訊的藏入與取出的複雜度。此外，如果一次傳送過多的偽裝影像，亦可能會造成有心人士懷疑，反而導致安全性下降。因此，目前大多數的學者多著墨於兩張影像上進行可逆式雙重影像藏匿技術的研究。

在未來展望方面，有鑑於雙重影像藏匿技術的研究在每次藏密後會造成偽裝影像的數量加倍，因此不若單一影像藏匿技術可反覆在影像上進行多層次的藏入(multiple-layer embedding)。因此，如何改良現有雙重影像藏匿技術的影像擴增囿限，將是可逆式多重影像藏匿技術的重要貢獻。

表 6-1: 雙偽裝影像的可逆式資訊隱藏方法的比較

Methods		Lena	Baboon	Pepper	Barbara	Goldhill	Washsat
Chang et al. [3](2007)	**PSNR-1(**dB)	45.19	45.20	45.21	45.20	45.13	45.58
	PSNR-2(dB)	45.20	45.21	45.21	45.21	45.14	45.13
	PSNR(Avg)	45.20	45.21	45.21	45.21	45.14	45.36
	Capacity(bits)	262,144	261,444	261,678	262,144	262,144	262,144
	Capacity(bpp)	1.00	1.00	1.00	1.00	1.00	1.00
Chang et al. [2] (2009)	**PSNR-1(**dB)	48.13	48.14	48.11	48.13	48.13	48.59
	PSNR-2(dB)	48.14	48.11	48.14	48.12	48.15	48.12
	PSNR(Avg)	48.14	48.13	48.13	48.13	48.14	48.36
	Capacity(bits)	262,144	262,144	262,144	262,144	262,144	262,144
	Capacity(bpp)	1.00	1.00	1.00	1.00	1.00	1.00
Lee et al. [8](2009)	**PSNR-1(**dB)	52.39	52.39	52.39	52.39	51.14	51.14
	PSNR-2(dB)	52.39	52.39	52.39	52.39	54.16	54.14
	PSNR(Avg)	52.39	52.39	52.39	52.39	52.65	52.64
	Capacity(bits)	196,608	193,987	196,608	193,972	196,539	196,771
	Capacity(bpp)	0.75	0.75	0.75	0.75	0.75	0.75
Lee et al. [9](2011)	**PSNR-1(**dB)	49.76	49.77	49.75	49.75	49.77	49.76
	PSNR-2(dB)	49.56	49.56	49.58	49.56	49.57	49.56
	PSNR(Avg)	49.66	49.67	49.67	49.66	49.67	49.66
	Capacity(bits)	280,494	280,494	280,494	280,494	280,494	280,494
	Capacity(bpp)	1.07	1.07	1.07	1.07	1.07	1.07
dHw4QM [7]	**PSNR-1(**dB)	44.02	44.10	44.19	44.14	44.00	44.78
	PSNR-2(dB)	44.04	44.10	44.19	44.14	44.01	45.21
	PSNR(Avg)	44.03	44.10	44.19	44.14	44.01	4500
	Capacity(bits)	294,099	281,138	291,403	290,108	288,667	342,494
	Capacity(bpp)	1.12	1.07	1.11	1.11	1.10	1.31
結合直方圖位移修改法與十字四象限魔術矩陣模數運算	**PSNR-1(**dB)	48.67	48.69	48.70	48.66	48.66	49.41
	PSNR-2(dB)	48.68	48.67	48.71	48.67	48.67	48.48
	PSNR(Avg)	48.68	48.68	48.71	48.67	48.67	48.95
	Capacity(bits)	294,099	281,138	291,403	290,108	274,651	274,651
	Capacity(bpp)	1.12	1.07	1.11	1.11	1.05	1.05

參考文獻

[1] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE transaction on Image Processing*, Vol. 13, 2004.

[2] C.C. Chang, Y.C. Chou, and T.D. Kieu, "Information hiding in dual images with reversibility," P*roceedings 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," I*EEE TENCON 2007*, pp. 1-4, 2007.

[4] L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security*, Vol.5, No.1, pp. 187–193, 2010.

[5] W. Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting," *Optics Communications*, Vol. 285, pp. 101-108, 2012.

[6] T. D. Kieu and C. C. Chang, "A Steganographic scheme by fully exploiting modification directions," *Expert Systems with Applications*, Vol. 38, pp. 10648-10657, 2011.

[7] C. F. Lee, J.Y. Chen, and S.T. Chen, "A high capacity reversible multiple-image hiding scheme", *Proceedings of International Computer Symposium* (ICS), Taichung, Taiwan. December 12-14, 2014.

[8] C. F. Lee 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. 336-341, SKKU, Suwon, Korea, 2009.

[9] C. F. Lee and Y. L. Huang, "Reversible data hiding scheme Based on dual stegano-images using orientation combinations," *Telecommunication System,* Vol.52, No.4, pp. 2237-2247, 2013. (Published online: July 2011)

[10] Z. C. 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.

[11] W.L. Tai, C.M. Yeh, and C.C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transaction on Circuits and Systems for Video Technology*, Vol. 19, No. 6, pp.906–910, 2009.

[12] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890-896, 2003.

[13] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, Vol. 89, No.6, pp.1129-1143, 2009.

[14] H. W. Tseng and C. P. Hsieh, "Prediction-based reversible data hiding," *Information Sciences*, Vol. 179, No.14, pp. 2460-2469, 2009.

[15] C. H. Yang and M.H. Tsai, "Improving histogram-based reversible data hiding by interleaving predictions," *IET Image Processing*, Vol. 4, No. 4, pp. 223-234, 2010.

[16] W.J. Yang, K.L. Chung, H.Y. Liao, and W.K. Yu, "Efficient reversible data hiding algorithm based on gradient-based edge direction prediction," *The Journal of Systems and Software*, Vol. 86, pp. 567-580, 2013.

[17] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, Vol. 10, Issue 11, pp.781–783, 2006.

[18] Z. Zhao, H. Luo, Z. M. Lu and J. S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," *International Journal of Electronics and Communications* (AEÜ), Vol. 65, pp. 814-826, 2011.