改良五像素配對差異擴張技術之資訊隱藏方法

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

摘要

Avinash 及 Madhuri 學者於 2015 年提出一個以像素差異擴張法為基礎的資訊隱藏技術，作者將影像切割成 2×3 大小且不重疊的區塊，以中間像素作為基礎像素，並與其他相鄰的 5 個像素進行差值運算，結合 LSB 位元取代法進行機密訊息的嵌入。兩位學者的方法之中，固定使用 2×3 大小的區塊進行機密訊息的嵌入，以至於藏量受到限制。因此，本論文調整其區塊大小以提高其藏量，並且能有效的保持其影像品質。實驗結果顯示將影像區塊大小改為 2×2，藏量效果能優於兩位學者的方法。

關鍵詞：資訊隱藏、像素差異擴張法、最低位元取代藏入法。

Abstract

In 2015, Avinash and Madhuri proposed a Five Pixel Pair Differencing and LSB Substitution (FPPD) hiding scheme to improve pixel-value differencing technique. In their scheme a cover image is divided into several non-overlapping blocks sized 2×3 pixels. Center pixel in each block is a basic pixel and used to compute differences with other five pixels. The differences are used to conceal the secret message by using pixel value differencing hiding method. In their scheme, the embedding capacity is limited by the size of the block. Thus, in this paper, we readjust the size of the block to increase the embedding capacity and keep image quality of the stego-image. Experimental results show that the embedding capacity is higher than that of Avinash and Madhuri's scheme especially with block size 2×2.

Keywords: Data hiding, Least-significant-bit substitution, Pixel value differencing.

1. 前言

隨著網路科技的蓬勃發展，許多人使用網際網路進行資料的傳遞及交換，使得數位資料在網路的空間裡被廣泛的散佈及應用。然而在網路上進行資料的傳輸是不安全的，資料有可能被不法的第三者竊取並恣意竄改或破壞。因此，為了確保機密資料傳遞的安全性，學者發展出資訊隱藏的概念，將機密資料嵌入於多媒體中，例如:影像、聲音、文字等等，進而產生出偽裝媒體，以偽裝媒體進行傳遞，來躲避不法第三者的攻擊，將機密資料安全地傳送出去。

資訊隱藏依其偽裝影像是否可以還原成原始影像可分為可逆式與不可逆式兩種方法，當嵌入的機密資料取出後，可以恢復至原始的影像狀態，即為可逆式的資訊隱藏技(Reversible Data Hiding Techniques)；相反的，不可恢復至原始影像狀態者，即為不可逆式的資訊隱藏技術(Irreversible Data Hiding Techniques)。

此外，資訊隱藏技術依照其處理方式的不同，分為空間域、頻率域與壓縮域這三種方式。空間域為最常見的隱藏方式，直接在原始媒體的像素上進行嵌入動作，像是差異擴張法[10]，該方法是將相鄰像素間進行差值的擴張，並將機密資料嵌入於差值之中；另外一種最為廣泛應用的方法為直方圖位移法，Ni 學者於 2006 首先提出此方法[7]，該方法是將影像的像素進行統計並產生直方圖，從中找到出現頻率最高(峰值點)及頻率最低(零值點)的像素值，進行像素值的修改達到隱藏的效果。

頻率域的嵌入方式是將空間域的像素透過轉換公式，將其轉換成頻率域係數，並將機密資料嵌入於頻率係數中。在壓縮域的技術，則是根據區塊特性來採取不同的編碼策略，較平滑的區塊利用該區塊平均值來編碼，較複雜的區塊使用查表來編碼；Lema 與 Mitchell 於 1984 年提出的動量絕對值區塊截短編碼（Absolute Moment BTC, AMBTC）[5]，針對位元圖的取樣來進行編碼，以原有的 16 位元的位元圖（區塊大小為 4×4）取其中 8 個位元當作樣本做編碼，位元圖以類似向量量化（Vector Quantization, VQ）[4, 6, 8] 的編碼簿（Codebook）的概念，找出最具有代表性的位元圖來編碼，並將機密資料嵌入其中。

空間域的資訊隱藏技術為大多數研究學者，研究的目標，因此，有大量的空間域資訊隱藏技術被提出，例如 Wu 及 Tsai 所提出的像素差異擴張法（Pixel Value Differencing, PVD）[12]為空間域著名的研究技術之一，有許多的專家學者以該方法為基礎提出了許多不同的改良方法。如 2015 年，Tyagi 等學者提出一個以像素差異擴張法為基礎的資訊隱藏技術(Pixel Value Differencing and Pixel Value Sum, PVS)[11]，作者將影像切割成 2×2 大小且不重疊的區塊，並將兩個連續的像素進行運算，取得兩像素之總和，接著利用這兩像素總和的特徵，使用不同的演算步驟將機密訊息嵌入；如果像素總和小於 255，則使用原始 PVD 方法進行機密訊息的嵌入，反之，像素總和大於 255，將像素修正後再進行嵌入的動作。除此之外，還有許多學者將影像切割成不同的區塊大小，來提高藏量[6] [8]，並根據每個區塊的影像特性，結合不同的技術進行嵌入。如果該區塊位於影像的平滑區可以結合最低位元取代(Least Significant Bit Replacement, LSB)技術[9] [13]。然而 PVD 技術，很容易被第三者竊取出機密訊息，為了躲避不法第三者的攻擊，因此，有學者利用隨機產生的序列作為金鑰，以加密的方式進行嵌入，藉此提高資訊隱藏技術的安全性[2] [4]。

2015 年，Avinash 及 Madhuri 學者提出一個以 PVD 為基礎的五像素配對差異擴張技術(Five Pixel Pair Differencing and LSB Substitution, FPPD)[3]，作者將影像切割成 2×3 大小且不重疊的區塊，接著以中間像素作為基礎像素，與其他相鄰的 5 個像素進行差值運算，作者結合最低位元取代技術（Least Significant Bit, LSB）進行機密訊息的嵌入。兩位學者的方法之中，固定使用 2×3 大小的區塊進行機密訊息的嵌入，以至於藏量受到限制。

因此，本論文改良 FPPD 技術，修改其原始方法的區塊大小，分析不同區塊大小，例如 1×3、2×2 和 3×3 三種區塊大小，其藏入效能，藉以觀察影像位於不同區塊的變化，並根據影像的特性，歸納出區塊的分割方法。

本研究架構如下，第二章為文獻探討，詳細介紹像素差異擴張技術（第 2.1 節）、LSB 最低位元取代技術（第 2.2 節）以及 FFPD（第 2.3 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 像素差異擴張法 (Pixel Value Differencing, PVD)

Wu 及 Tsai 學者於 2003 年提出像素差異擴張方法 (Pixel Value Differencing, PVD) [12]，該方法是將兩個相鄰的像素視為一個區塊，將影像分成多組 1×2 不重疊的區塊，接著利用公式(1)計算該區塊的像素差異值d_i，誤差值越大代表該區塊越趨近邊緣區域或複雜區域；反之，誤差值越小代表該區塊趨近平滑區域。

$$d_i = |px_i - px_{i+1}| \tag{1}$$

接著依照誤差值d_i所對應到區間量表(如圖 1)，決定像素可嵌入的機密訊息位元數。區間量表根據誤差值大小分為六個區間，每一個區間都有其對應的上界u_i與下界l_i，利用上下界的值求得對應的藏量。

[0,7]	[8,15]	[16,31]	[32,63]	[64,127]	[128,255]
$log_2 8 = 3$	$log_2 8 = 3$	$log_2 16 = 4$	$log_2 32 = 5$	$log_2 64 = 6$	$log_2 128 = 7$
R_1	R_2	R_3	R_4	R_5	R_6

圖 1 誤差值與藏量區間量表

例如，區塊誤差值為d_i =9∈[8,15]，對應到 R_2 的區間，透過公式(2)計算其藏量，表示該區塊可以嵌入 3 個位元的機密訊息。接著從機密訊息取出 k 個位元進行嵌入，並將機密訊息轉換成十進制表示得到機密符號b_i。將b_i加上對應區間的下界值l_i，即可得修正的新誤差值$d_i' = l_i + b_i$。為了將機密訊息適當的分配在該區塊的兩個像素中，作者利用公式(3)，將像素值進行修正，如此一來，嵌入機密訊息前的像素值，與嵌入機密訊息後的像素值，差異會最小，其中 z= $|d_i - d_i'|$。

$$k=\lfloor log_2(u - l + 1) \rfloor \tag{2}$$

$$(px_i', px_{i+1}') = \begin{cases} \left(px_i + \left\lceil \frac{z}{2} \right\rceil, px_{i+1} - \left\lfloor \frac{z}{2} \right\rfloor\right) \ if\ px_i \geq px_{i+1}\ and\ d_i' > d_i, \\ \left(px_i - \left\lceil \frac{z}{2} \right\rceil, px_{i+1} + \left\lfloor \frac{z}{2} \right\rfloor\right) \ if\ px_i < px_{i+1}\ and\ d_i' > d_i, \\ \left(px_i - \left\lceil \frac{z}{2} \right\rceil, px_{i+1} + \left\lfloor \frac{z}{2} \right\rfloor\right) \ if\ px_i \geq px_{i+1}\ and\ d_i' \leq d_i, \\ \left(px_i + \left\lceil \frac{z}{2} \right\rceil, px_{i+1} - \left\lfloor \frac{z}{2} \right\rfloor\right) \ if\ px_i < px_{i+1}\ and\ d_i' \leq d_i. \end{cases} \tag{3}$$

取出機密訊息時，先求出偽裝影像區塊中的像素誤差值d_i'並與區間量表進行對照，找尋其對應的區間，利用d_i'減去相對應的區間下界值l_i，即可取得十進位制的機密訊息，最後，將機密訊息轉為二進制，即完成取出流程。

2.2 最低位元取代法(Least Significant Bit Replacement)

Chan 等學者於 2004 所提出的 LSB 最低位元取代法[1]是空間域裡著名的不可逆式資訊隱藏技術，將機密訊息嵌入於影像最不重要的位元之中，而此位元的改變對像素的影響並不大，藉此達到資訊隱藏的目的，其優點是擁有很高的藏量且低失真。

將機密訊息嵌入在像素值最後的 t 個位元，t 可依照需要藏入的位元數自行調整，當然藏入的位元數越多，影像品質也會跟著降低。在進行嵌入的過程中，像素值與機密訊息都以二進制的方式表示，根據機密訊息的長度直接在原始像素值做取代的動作，以完成嵌入流程。以像素值 $px_i = 152$ 為例，首先，將像素值轉為二進制 $px_i = (10011\underline{000})_2$，並藏入 3 位元的機密訊息為 $(011)_2$，機密訊息嵌入後得到偽裝像素值為 $px_i' = (10011011)_2 = 155$。

取出流程，只需要將偽裝影像轉為二進制後，再根據該像素值所嵌入的機密訊息位元數 n 進行取出，即可取出得機密訊息。

2.3 五像素配對差異擴張技術（Five Pixel Pair Differencing and LSB Substitution, FPPD)

Avinash 及 Madhuri 學者於 2015 年提出五像素配對差異擴張技術及 LSB 取代法（Five Pixel Pair Differencing and LSB Substitution, FPPD) [3]，該方法是將影像分成多組 2×3 不重疊的區塊，圖 2 為在 2×3 大小的區塊像素排列的情形。

px_1 $P_{(x,y)}$	px_0 $P_{(x,y+1)}$	px_2 $P_{(x,y+2)}$
px_3 $P_{(x+1,y)}$	px_4 $P_{(x+1,y+1)}$	px_5 $P_{(x+1,y+2)}$

圖 2 像素分布(2×3 區塊)

其中(x, y)為像素的位置。以px_0作為基礎像素(Common Pixel)，並以 LSB 位元取代法嵌入 3 位元的機密訊息，其他剩餘的五個像素與基礎像素兩兩為一組分別組成 (px_0, px_1)、(px_0, px_2)、(px_0, px_3)、(px_0, px_4)、(px_0, px_5)，共五組像素配對，以 Wu 和 Tsai 學者的 PVD 方法為基礎，計算每一組像素對的誤差值$|d_i|$，接著依照所得之誤差值對應 Wu 和 Tsai 學者的區間量表(如圖 1)，找出該組像素對嵌入的位元數k_i，為了避免機密訊息嵌入量的懸殊且必須維持影像品質，因此，將機密訊息平均分配至每一個像素，利用公式(4)計算該區塊的平均藏量。

$$avg = \left\lfloor \frac{\sum k_i}{5} \right\rfloor. \tag{4}$$

公式(4)所得之平均藏量，透過公式(5)修改誤差值得到dl_i，並計算原始誤差值d_i與修改後的誤差值dl_i的位移量。修改及計算位移量公式如下：

$$dl_i = d_i \bmod 2^{avg}, \tag{5}$$

$$\mathrm{OD}_i = |d_i| - |dl_i|. \tag{6}$$

再以新誤差值對應 Wu 和 Tsai 學者的區間量表(如圖 1)，來決定該組像素的嵌入的位元數，找出該區間的下界值l_i，並由機密訊息串列中取出與該區間相同的機密訊息位元數，透過公式(7)將轉為十進制的機密符號b_i嵌入。

$$d_i' = \begin{cases} OD_i + l_i + b_i, & if\ d_i \geq 0, \\ -(OD_i + l_i + b_i), & if\ d_i < 0. \end{cases} \tag{7}$$

為了找出與原始像素最為相近的偽裝像素值，作者透過公式(8)，計算新的誤差值d_i'與原始的誤差值d_i兩者之間的差異m_i，利用m_i的絕對值選擇出最小的誤差值，以該誤差值的原始像素作為基準，再利用這個基準像素與其他像素利用公式(9)做修正，以保持每一個像素修改後的誤差值區間會與修改前是一致的。其中p_c為已經藏入 3 位元機密訊息的基礎像素，px_i為原始像素。

$$m_i = d_i' - d_i, \tag{8}$$

$$(p_C', p_i') = \left(p_c - \left\lceil \frac{m}{2} \right\rceil, p_i + \left\lfloor \frac{m}{2} \right\rfloor\right). \tag{9}$$

接著將像素進行修正，以基準像素p_C'與嵌入 3 位元機密訊息的基礎像素做誤差值的運算，將剩餘的 5 個像素減去該誤差值，即可得到偽裝影像，完成嵌入流程。

取出機密訊息時，先將px'_0基礎像素轉為二進制，取出最後 3 位元的機密訊息。為了尋找該區塊的平均藏量，因此，將基礎像素與剩餘的 5 個像素進行誤差值的運算，再對照區間量表(圖 1)，找尋位於該區間之像素所對應的藏量k_i，並利用公式(4)，計算出其平均藏量，接著透過公式(5)，計算出其修改後的誤差值dl_i。

根據取得的誤差值dl_i對照 Wu 及 Tsai 學者的區間量表(如圖 1)，可以取得該對像素位於

該區間能藏入及區間的下界值l_i，利用(10)取出機密訊息，並轉為二進制，即完成取出流程。

$$b_i = |dl_i| - l_i \quad (10)$$

3.研究方法

Avinash 及 Madhuri 學者的 FPPD 方法藏入區塊大小固定為 2×3，再以中間像素作為基礎像素與其他像素進行 PVD 運算，將機密訊息藏入差異值中。該方法能有效將訊息藏入任二組差異值中，然而，像素配對的差異值是影響藏入效能很重要因素。以複雜影像而言，像素間的差異值會很大，雖然差異大代表所能藏入的機密位元數較大，但相對的影像差異也會跟著變大，導致影像品質變差。因此，本論文擬改變 FPPD 的區塊大小，利用不同區塊大小，找出符合影像特徵的最佳藏入設定。本研究將影像切割成不重疊的 1×3、2×2、3×3 區塊，根據不同的區塊大小及不同的影像特性進行分析，觀察其藏量及影像品質的變化。以下將以 2×2 的區塊大小為範例並詳細說明嵌入及取出流程。

3.1 嵌入階段

首先將影像切割成$m \times n$不重疊的區塊，本研究的區塊切割方式有三種，分別為 1×3、2×2 和 3×3，區塊示意圖如圖 3。所示。

px_1 $P_{(x,y)}$	px_0 $P_{(x,y+1)}$	px_2 $P_{(x,y+2)}$

(a) 1×3 區塊

px_1 $P_{(x,y)}$	px_0 $P_{(x,y+1)}$
px_2 $P_{(x+1,y)}$	px_3 $P_{(x+1,y+1)}$

(b) 2×2 區塊

px_1 $P_{(x,y)}$	px_0 $P_{(x,y+1)}$	px_2 $P_{(x,y+2)}$
px_3 $P_{(x+1,y)}$	px_4 $P_{(x+1,y+1)}$	px_5 $P_{(x+1,y+2)}$

(c) 2×3 區塊

圖 3 不同區塊大小像素分布

以圖 4 區塊大小 2×2 為例，($m = 2$且$n = 2$)，每一個 2×2 的區塊由 4 個像素px_0、px_1、px_2、px_3共同組成，其中(x, y)為像素的位置。

86	150
53	156

圖 4 像素範例

所有區塊皆以px_0作為基礎像素(Common Pixel)，先使用 LSB 位元取代法，將 3 個位元的機密訊息藏入到基礎像素中。以像素值$px_0 = 150$為例，假設機密訊息為$(111)_2$；嵌入後的基礎像素更改為$px_{\text{base}} = 151$，將剩餘的三個像素，分別與基礎像素px_{base}，組成以下三組像素對：

$$(px_{\text{base}}, px_1) = (151,86)$$
$$(px_{\text{base}}, px_2) = (151,53)$$
$$(px_{\text{base}}, px_3) = (151,156)$$

利用每一組像素對的誤差值，來決定藏量；計算方法為像素值減去px_{base}，產生三組像素的誤差值d_i，分別為$d_1 = px_1 - px_{\text{base}} = 86 - 151 = -65$、$d_2 = px_2 - px_{\text{base}} = 53 - 151 = -98$、$d_3 = px_3 - px_{\text{base}} = 156 - 151 = 5$，根據其誤差值對照 Wu 和 Tsai 學者的區間量表(如圖 1)，利用公式(2)計算出該區間的藏量k_i，為了將機密訊息平均的分攤到每一個像素上；因此，透過公式(11)計算該區塊的平均藏量

$$avg = \left\lfloor \frac{\sum k_i}{3} \right\rfloor. \quad (11)$$

接著利用平均藏量avg修正每個像素配對的差異值，即利用公式(5)分別計算修改後的誤差值dl_i。延續上述的例子，$k_1 = 6$、$k_2 = 6$、$k_3 = 3$則$avg = \left\lfloor \frac{\sum k_i}{3} \right\rfloor = 5$，利用$avg$修正差異值得到$dl_1 = d_1 \; mod \; 2^{avg} = -65 \bmod 2^5 = -1$、$dl_2 = -2$和$dl_3 = 5$。

接著利用公式(6)計算原始誤差值d_i與修改後的誤差值dl_i的位移量，依照所得之新誤差值$|dl_i|$，對照 Wu 及 Tsai 學者的區間量表(如圖 1)，來決定該組像素的嵌入的位元數，找出該區間的下界值l_i，並由機密訊息串列中取出與該區間相同的機密訊息位元數，接著計算原始差異和新差異間的距離$\text{OD}_i = |d_i| - |dl_i|$，再透過公式(7)將轉為十進制的機密訊息$b_i$嵌入。

上例中$|dl_1| = 1$其藏入量為$k_1 = 3$，假設對應的機密訊息為$b_1 = (110)_2 = 6$；$|dl_2| = 2$其藏入量為$k_2 = 3$，對應的機密訊息為$b_2 = (101)_2 = 5$；$|dl_3| = 5$其藏入量為$k_3 = 3$，

對應的機密訊息為$b_3 = (000)_2 = 0$。接著計算原始差異和新差異間的距離$\mathrm{OD}_1 = |d_1| - |dl_1| = 65 - 1 = 64$ 、 $\mathrm{OD}_2 = |d_2| - |dl_2| = 98 - 2 = 96$、$\mathrm{OD}_3 = |d_3| - |dl_3| = 5 - 5 = 0$。再透過公式(7)將轉為十進制的機密訊息$b_i$嵌入，如原始誤差值為負數，利用公式(7)須加上負號，以維持其原始的區間的誤差值，因此，可以利用其修正後的誤差值及區間下界值，算出嵌入機密訊息後的像素值分別為$d'_1 = -(OD_1 + l_1 + b_1) = -(64 + 0 + 6) = -70$ 、$d'_2 = -(OD_2 + l_2 + b_2) = -(96 + 0 + 5) = 101$、$d'_3 = (OD_3 + l_3 + b_3) = 0 + 0 + 0 = 0$。

為了找出一個與原始像素最為相近的偽裝像素值，透過公式(8)，計算新的誤差值d'_i與原始的誤差值d_i兩者之間的差異m_i，分別為$m_1 = d'_1 - d_1 = -70 - (-65) = -5$ 、$m_2 = d'_2 - d_2 = -101 - (-98) = -3$ 、$m_3 = d'_3 - d_3 = 0 - 5 = -5$。根據$m_i$計算每個像素配對修正後的數值為何，其中$px_{\text{base}}$為嵌入 3 位元機密訊息的基礎像素，$px_i$為原始像素值，計算過程如下：

$$(pu_i, pd_i) = (px_{\text{base}} - \left\lceil \frac{m_i}{2} \right\rceil, px_i + \left\lfloor \frac{m_i}{2} \right\rfloor). \quad (12)$$

接續上面的例子，

$pu_1 = 151 - \left\lceil \frac{-5}{2} \right\rceil = 153, pd_1 = 86 + \left\lfloor \frac{-5}{2} \right\rfloor = 83$；

$pu_2 = 151 - \left\lceil \frac{-3}{2} \right\rceil = 152, pd_2 = 53 + \left\lfloor \frac{-3}{2} \right\rfloor = 51$；

$pu_3 = 151 - \left\lceil \frac{-5}{2} \right\rceil = 153, pd_3 = 156 + \left\lfloor \frac{-5}{2} \right\rfloor = 153$。

上面的步驟是計算任一配對與基礎像素px_{base}進行藏入位移時，基礎像素需移動到那一個地方，pu_1、pu_2和pu_3即是候選像素值。為了讓基礎像素移動量最小，選一個移動量最小的pu_i做為標的。m_i是造成px_{base}移動的因素，因此，最小的m_i就會是最小的pu_i。利用最小的誤差值$min = min\,(|m_1|, |m_2|, \ldots, |m_i|)$，以該誤差值的對應的$pu_i$數值作為標的$pu_{min}$以修正其他像素。

上例中，$min = min\,(|-5|, |-3|, |-5|)$=3，其中$m_1$的值最小，因此以$m_2$對應的$pu_2 = 152$數值作為標的 pu_{min}=152 修正其他像素。修正公式如下：

$$pc_i = pd_i + pu_{min} - pu_i. \quad (13)$$

修正後像素為 $pc_1 = 83 + 152 - 153 = 82$, $pc_2 = 51 + 152 - 152 = 51$, $pc_3 = 153 + 152 - 153 = 152$。

截至目前為止，我們已經將機密訊息分別藏入到所有像素配對中，但是pu_{min}=152 與px_{base}=151 不相等，若直接以pu_{min}取代px_{base}則無法從中取出原先藏入的 3 個 LSB 位元。因此，要利用pu_{min}與px_{base}的差異，再對其他像素pc_i進行微調，微調公式如下：

$$px'_i = pc_i + (px_{\text{base}} - pu_{min}). \quad (14)$$

微調後像素為 $px'_1 = 82 + (151 - 152) = 81$, $px'_2 = 51 + (151 - 152) = 50$, $px'_3 = 152 + (151 - 152) = 151$，即可得到偽裝影像，如圖 5。所示，完成嵌入流程。

81	151
50	151

圖 5 偽裝像素範例

3.2 取出流程

在嵌入階段是利用像素的誤差值決定該組像素對的藏量；因此，我們可以透過這個特性取出相對應的機密訊息。首先，先將影像分成多組$m \times n$大小的區塊，利用其他鄰近的像素與基礎像素px_0進行相減，得到誤差值，再從誤差值中取出機密訊息。

延續上面圖 5 的例子，$m \times n$=2×2，基礎像素px_{base}=151，鄰近像素分別為px'_1=81、px'_2=50、px'_3=151，分別計算 px'_1 與 px'_0 誤差為$d_1 = 81 - 151 = -70$、px'_2 與 px'_0 誤差為$d_2 = 50 - 151 = -101$、px'_3 與 px'_0 誤差為$d_3 = 151 - 151 = 0$。根據誤差值的絕對值來對照 Wu 及 Tsai 學者的區間量表(如圖 1)，可以得知 $|d_1|$位於 R_5 區間藏量為 6 位元、$|d_2|$位於 R_5 區間藏量為 6 位元、$|d_3|$位於 R_1 區間藏量為 3 位元。

透過公式(11)計算其平均藏量為$avg = \left\lfloor \frac{(6+6+3)}{3} \right\rfloor$ = 5 位元，利用公式(5)修正差異值得到$dl_1 = d_1 \; mod \; 2^{avg} = -70 \bmod 2^5 = -6$、$dl_2 = -5$和$dl_3 = 0$。以修正後誤差值$dl_i$來對照 Wu 和 Tsai 學者的區間量表(如圖 1)，可以取得該像素的藏入量及區間的下界值l_i，透過公式(10)取出機密訊息並將其轉為二進制，機密訊息分別為$b_1 = |-6| - 0 = 6 = (110)_2$、$b_2 = |-5| - 0 = 5 = (101)_2$ 、 $b_3 = |0| - 0 = 5 = (000)_2$。基礎像素$px_{\text{base}}$利用 LSB 取代法將機密訊息嵌入，因此，只需要將基礎像素$px_{\text{base}} = 151$ 轉為二進制

$px_{\text{base}} = (10010111)_2$，並取出 3 位元的機密訊息為 111。根據以上步驟，即可從偽裝影像依序將每一個區塊的機密訊息依序取出。

4. 實驗結果

本研究與 2015 年 FPPD 方法進行比較，利用六張 512×512 大小的灰階影像進行測試，測試影像如圖 6 所示。

圖 6 實驗測試影像

本論文利用高峰影像信號雜訊比（Peak Signal to Noise Ratio, PSNR）針對原始影像和偽裝影像之間的差異進行評估。PSNR 公式如下所示：

$$\text{PSNR} = 10 \times log_{10}\left[\frac{255^2}{\frac{1}{h\times w}\times\sum_{i=1}^{h}\sum_{j=1}^{w}(px'_{i,j}-px_{i,j})}\right] \quad (15)$$

其中 $h \times w$為影像大小，$px'_{i,j}$ 和 $px_{i,j}$ 分別為偽裝影像和原始影像的像素值。兩張影像之間的差異越小，代表影像品質較好，PSNR 則越高；反之，兩張影像之間差異越大，代表影像品質較差，PSNR 值越低。

為了評估所提出方法的嵌入能力，利用每一個像素能嵌入位元數(Bits Per Pixel, bpp)評估偽裝影像的藏量。bpp 公式如下所示：

$$\text{bpp} = \frac{Capacity}{h\times w} \quad (16)$$

其中 Capacity 為偽裝影像的總藏入量。當 bpp 越大，代表藏入能力較好；反之，而 bpp 越小，代表藏入能力較差。

表 1 為所提的方法在不同的區塊大小下，影像品質與總藏量之比較，本研究分別實驗了 1×3、2×2、3×3 三種區塊大小。從表 3 中可以發現當區塊設為 2×2 的區塊大小時，6 張影像的 bpp 值皆高於 3 bpp 以上，區塊大小 2×2 其單位藏量較設為其他區塊大小來得高，且影像品質落在 37-38 db 左右。相較於 Avinash 及 Madhuri 學者使用了 2×3 區塊大小，本論文所提的方法，在 1×3 及 2×2 區塊都藏量都明顯比原始的 2×3 區塊來得高，且 PSNR 都高於 37 db 以上。

經實驗結果發現，2×2 區塊其藏入量較高，不管是使用較平滑或是複雜的影像，其單位藏量都大於 3 bpp 以上；因此，如需要嵌入大量的機密訊息或影像為複雜影像時，建議可以使用 2×2 區塊來進行嵌入。

表 1 不同區塊大小下之單位藏量與影像品質比較表

區塊大小		Lena	Baboon	Jet	Sailboat	Peppers	Zelda
1×3	PSNR	38.569	37.819	38.596	37.935	38.004	37.997
	BPP	2.9911	3.0013	2.9920	2.9940	2.9909	2.9893
2×2	PSNR	38.050	37.584	38.014	37.914	38.004	37.930
	BPP	**3.0021**	**3.0281**	**3.0070**	**3.0072**	**3.0037**	**3.0025**
2×3	PSNR	38.094	37.770	38.105	37.982	38.033	38.056
	BPP	2.9896	3.0049	2.9906	2.9923	2.9901	2.9896
3×3	PSNR	38.099	37.858	38.153	38.028	38.082	38.004
	BPP	2.9774	2.9893	2.9782	2.9786	2.9778	2.9780

5. 結論與未來工作

本論文改良 Avinash 及 Madhuri 學者於 2015 年所提出的 FPPD 方法，所提的方法透過設置區塊大小控制其藏入量以及影像品質，嵌入方法是利用每一組像素對的誤差值，對照 Wu 和 Tsai 學者的區間量表，來決定該組像素對的藏量；因此，在複雜或是邊緣區的影像部分，使用 2×2 區塊進行嵌入，其藏入的效果會比較好。在較平滑的影像部分，可以使用 1×3 區塊進行嵌入，其藏入的效果會比原始 2×3 區塊效果較來得好。

未來工作主要是以利用影像的特性去區分

區塊的切割的大小，從實驗結果我們可以發現，複雜區或邊緣區其藏入量較高；因此，位於複雜區及邊緣區的影像，我們可以將影像分割為 2×2 的區塊進行嵌入，平滑區域則利用 1×3 的區塊進行嵌入，以達到最佳的藏量，並維持其影像品質。未來將利用分析影像特性的方法，自動切割影像成不一樣的區塊大小進行嵌入。

參考文獻

[1] C.K. Chan, and L.M. Cheng, "Hiding Data in Images by Simple LSB Substitution," ***Pattern Recognition,*** vol. 37, no. 03, pp. 469-474, 2004.

[2] J. Chen, "A PVD-based Data Hiding Method with Histogram Preserving using Pixel Pair Matching," Image Communication, vo1. 29, no.3, pp. 375-384, 2014.

[3] A.K. Gulve, and M.S. Joshi, "A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution," ***Graphics and Signal Processing,*** vol. 7, no. 5, pp. 64-74, 2015.

[4] A.K. Gulve, and M.S. Joshi, "An Image Steganography Algorithm with Five Pixel Pair Differencing and Gray Code Conversion," ***Graphics and Signal Processing,*** vol. 6, no. 3, pp. 488-493, 2014.

[5] M. D. Lema, and O. R. Mitchell, "Absolute Moment Block Truncation Coding and its Application to Color Image," ***IEEE Transactions on Communications,*** vol. 32, no. 10, pp. 1148-1157, 1984.

[6] Y.P. Lee, L.C. Lee, W.K. Chen, K.C. Chang, I.J. Su, and C.P. Chang, "High Payload Image Hiding with Quality Recovery using Tri-way Pixel-Value Differencing," ***Information Sciences***, vol. 191, pp.214-225, 2012.

[7] Z.C. Ni, Y.Q. Shi, N. Ansari, and Wei Su, "Reversible Data Hiding," ***IEEE Transactions on Circuits and Systems for Video Technology***, vol. 16, no. 3, pp. 354-362, 2003.

[8] G. Swain, and S.K. Lenka, "Pixel value differencing steganography using correlation of target pixel with neighboring pixels," ***Electrical, Computer and Communication Technologies***, Coimbatore, pp. 1-6, 2015.

[9] G. Swain, "Digital image steganography using nine-pixel differencing and modified LSB substitution," ***Science and Technology,*** Vol. 7, No. 9, pp. 1444-1450, 2014.

[10] 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.

[11] A. Tyagi, S. Changder, and R. Roy, "High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum," ***Advances in Computing and Communication Engineering,*** Dehradun, pp. 488-493, 2015.

[12] D.C. Wu, and W.H. Tsai, "A Steganographic Method for Images by Pixel-Value Differencing," ***Pattern Recognition Letters,*** vol. 24, no. 9-10, pp. 1613-1626, 2003.

[13] H.C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, "Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods," ***Image and Signal Processing,*** vol. 152, no. 5, pp. 611-615, 2005.