基植區塊式像素值差異法之多媒體隱藏研究

楊政興
屏東教育大學資訊科學系

王旭正
中央警察大學資訊管理系

翁麒耀
清華大學資訊工程系

孫宏民
清華大學資訊工程系

摘要

一個良好的藏密學技術必須是高容量以及偽裝後的影像不易被察覺。在2003年學者Wu et al.提出利用二個相鄰像素之間的像素值差異來隱藏資訊。本研究以四個相鄰的像素為一個區塊，利用像素的差異值來衡量區塊屬於邊緣區域或是平滑區域。如果區塊屬於邊緣區域，則可以容忍隱藏大量的資訊；反之，區塊屬於平滑區城，則可容忍隱藏較少的資訊量。區塊式像素值差異(Blocked Pixel-Value Differencing; Blocked PVD)的觀念為擴展學者Wu et al.提出的像素值差異(PVD)，將四個相鄰像素的差異值整體做考量，然後再劃分為二個群組，分別利用像素值差異法來隱藏資訊。另外，我們提出像素值移位的技術，讓嵌入的方法更具彈性。由實驗數據顯示，我們所提出的Blocked PVD方法，其資訊隱藏量比PVD方法還要多。

關鍵字：藏密學、資訊隱藏、像素值移位、像素值差異

聯絡人：王旭正
E-mail: sjwang@mail.cpu.edu.tw

Blocked Pixel-Value Differencing to Secret Embedding in Multimedia Image Systems

Cheng-Hsing Yang
Department of Computer Science, National Pingtung University of Education

Shiuh-Jeng Wang
Department of Information Management, Central Police University

Chi-Yao Weng
Department of Computer Science, National Tsing-Hua University

Hung-Ming Sun
Department of Computer Science, National Tsing-Hua University

Abstract

An efficient steganographic method usually provides a large embedding capacity and a small distortion for the stego-images. In 2003, Wu et al. proposed the pixel-value differencing (PVD) approach which applies the difference value of two consecutive pixels to data hiding. In this paper, we process a four-pixel block at a time, and use its difference value to judge that it is located in edged areas or smooth areas. If a block is located in edged areas, it may tolerate larger embedded information than those in smooth areas. Our blocked PVD approach is based on the PVD approach of Wu and Tsai. Each four-pixel block is divided into two two-pixel groups elaborately and each group is processed by the PVD approach. Moreover, an idea of pixel-value shifting is proposed in order to embed data more flexibly. Experimental results show that our method provides a larger embedding capacity than that of Wu and Tsai.

Key words: Steganography, information hiding, pixel-value shifting, pixel-value differencing

Correspondence: Shiuh-Jeng Wang
E-mail: sjwang@mail.cpu.edu.tw

壹、前言

近年來資訊科技的發展迅速，網路愈來愈普及化，至今已成為一種公開與不可缺少的溝通途徑。相對的，在一個公開的溝通管道中，將會面臨到許多的問題，如：資料安全、著作財產權的防護等。為了達成資訊安全與防護，資料加密是眾所皆知的技術(Highland 1997；Chu & Chang 1999)，此技術可以有效的達到安全的資訊傳輸，但經過加密的資料會呈現亂碼的情形，也特別容易引起有心人士的注意。因此，藏密學(Steganography) (Bender et al. 1996；Anderson & Peticolas 1998；Katzenbeisser & Petitcolas 2000；Lee & Chen 2000；Artz 2001；Yu et al. 2005)的出現，又開闢另一種新的機密傳輸之里程埤。

最不重要位元(Least Significant Bit; LSB)的應用是藏密學中眾所皆知的方法(Wang et al. 2000；Chang et al. 2002)。簡單LSB取代方法(Simple LSB Substitution Method)是一種最容易且經常被使用的方法，它直接將欲隱藏的資訊取代每個像素值的固定位元的LSB部份，這種方法雖然迅速且簡單，但是很容易被人類的視覺或是程式檢測出資訊隱藏的事實(Lee & Chen 2000；Fridrich et al. 2001)。 於是，許多學者陸陸續續的提出改良方式，來減少LSB方法所造成的影像失真(Wang et al. 2000；Chan & Chen 2004；Yang & Wang 2006)。另一方面，也有一些學者運用人類視覺系統(Human Visual System; HVS)之概念，開發避免被程式所檢測出來的資訊隱藏技術(Wu & Tsai 2003；Chang & Tseng 2004)，其中，學者Wu et al.提出像素值差異(Pixel-Value Differencing；PVD)法，利用兩個像素的差異值來決定隱藏多少個秘密資訊。此隱藏秘密訊息的方法是依據像素差異值屬於那個區間(Range)，利用此區間的大小來判斷隱藏多少位元。藏入位元後會產生新的差異值，再將此新的差異值反應給原始的兩個像素，產生新的像素值。另外，亦有學者針對LSB和PVD，提出結合的方法(Wu et al. 2005)。

在本論文中，我們提出一個有效率且不易被察覺的資訊隱藏技術。人類視覺系統的觀念指出，在邊緣區域(Edged Area)所能容忍的改變程度比平滑區域(Smooth Area)還要大(Lee & Chen 2000；Wu & Tsai 2003；Chang & Tseng 2004)，應用此觀念，我們以四個鄰近的像素為一個區塊(Block)，而機密資訊的隱藏量是依據區塊屬於平滑區域或是邊緣區域來決定。每一個區塊被劃分成二組，分別利用像素值的差異來做資訊隱藏。為了能正確的萃取出機密資訊，必須限制隱藏後的像素差異值與隱藏前的像素差異值要屬於同一個區間(Range)內。學者Wu et al.所提出的PVD方法，有可能會造成某些區塊無法隱藏訊息，針對此問題，我們提出了像素值移位(Pixel-Value Shifting)的技術來減少此情形的發生。經由實驗數據顯示，我們所提出的Blocked PVD方法，其隱藏的資訊量比學者Wu et al.提出的PVD方法還要多，而且也能通過Fridrich et al. (2001)方法的檢測。本篇論文的組成如下：第二節介紹學者Wu et al. (2003)所提出的像素值差異法，以及Wu et al. (2005)提出的結合PVD方法與LSB取代法；第三節提出我們的區塊式像素值差異法；實驗結果顯示在第四節；最後，在第五節中提出結論。

貳、文獻探討

在本節中我們將簡要的描述目前Wu et al. (2003)提出的像素值差異法(Pixel-Value Differencing)與Wu et al. (2005)提出的結合像素值差異法(Pixel-Value Differencing)與LSB取代法。

一、 像素值差異法(Pixel-Value Differencing)

在此小節中，我們將介紹學者Wu et al. (2003)提出的像素值差異法(Pixel-Value Differencing)，其方法是基於修正兩個相鄰像素的像素值來達到資訊隱藏的目的。在給定用來嵌入機密資訊的掩護影像(Cover Image)後，首先，掩護影像利用Z字型的順序，將兩個相鄰像素當作一個區塊，如此劃分成多個不重疊的區塊。然後，再去計算每一個區塊的像素差異值。假設一個區塊內有二個灰階的像素p_i與p_i+1，其像素值分別為g_i和g_i+1，則此區塊的差異值d為g_i+1– g_i。差異值的可能範圍為—255到255，取其絕對值為0～255，再將此範圍切割成多個連續的區間R_i (i = 1, 2, 3, ⋯, r)。區間R_i的上限定義為u_i，下限定義為l_i，R_i的寬度(Width)為$u_i - l_i + 1$，當區塊的差異值落在較前面的區間，表示此區塊位於平滑區域，相同的道理，當區塊的差異值落在較後面的區間，表示此區塊位於邊緣區域。

在資訊隱藏的階段中，我們要先去計算區塊B中的二個像素之差異值d。假設像素差異值d屬於第k個區間內，則可以計算出此一區塊 B 可以藏入n = log2 ($uk - lk + 1$)個位元，從機密訊息S中取出n個位元，則可從下面的運算式中得到新的像素差異值d'。

$$d' = \begin{cases} l_k + b & for\ d \geq 0 \\ -(l_k + b) & for\ d < 0 \end{cases} \tag{1}$$

其中，b是此n個位元所換算出的數值，而b被隱藏在新的像素差異值d'中，並用d'來取代舊的像素差異值d。最後，再從d'去做反向計算產生新的像素值g'_i和g'_i+1。當所有的資訊皆隱藏完畢，即代表已經結束了資訊隱藏階段。

反向計算的目的是利用原來的二個像素值(g_i, $g_i + 1$) ，以及新的像素差異值d'，算出新的像素值(g'_i, g'_i +1)，其反向計算的函數定義如下：

$$f((g_i, g_{i+1}), m) = (g'_i, g'_{i+1}) = \begin{cases} (g_i - ceiling_m, g_{i+1} + floor_m) \\ \quad \text{if } d \text{ is an odd number;} \\ (g_i - floor_m, g_{i+1} + ceiling_m) \\ \quad \text{if } d \text{ is an even number;} \end{cases} \tag{2}$$

其中$m = d' - d$, $ceiling_m = \lceil m/2 \rceil$, and $floor_m = \lfloor m/2 \rfloor$。上述的方程式中，所產生的新像素值$g'_i$和$g'_i$+1，其差異值與$d'$相等，當新的像素值超出了[0, 255]的範圍，反向計算後的結果是無效的，此時像素 p_i 與 p_i +1不可用來隱藏資訊。因此，為了要檢驗像素值(g_i, g_i + 1) 是否可以用來隱藏資訊，必須利用函數f(g_i, g_i +1), $u_k - d$)去檢查所產生的新像素值

$(\hat{g}_i, \hat{g}_{i+1})$是否在[0, 255]的範圍之內，其中$u_k$為$d$所落入的區間$R_k$之上界，如果超出了此範圍，就必須放棄利用此區塊來隱藏秘密訊息。

二、結合像素值差異法(Pixel-Value Differencing)與LSB取代法(LSB Replacement)

在此小節中，我們將介紹學者Wu et al. (2005)提出的結合像素值差異法(Pixel-Value Differencing)與LSB取代法，其方法是基於兩個相鄰像素的像素值差異來達到資訊隱藏的目的。首先，要先設定Div門檻值，所謂Div門檻值是劃分二個像素值(g_i與g_i+1)的差異值為高頻區域與低頻區域，而高頻區塊的劃分方式與PVD的範圍切割方法相同。然後，再將掩護影像劃分多個不重疊的區塊，而每一個區塊為二個相鄰的像素。再去計算每一個區塊的差異值。假設一個區塊內有二個灰階的像素p_i與p_i+1，則此區塊的差異值$d = |g_i - g_{i+1}|$。當區塊的差異值落在較低頻區間，表示此區塊位於平滑區域，相同的道理，當區塊的差異值落在較後面的區間，表示此區塊位於邊緣區域。

在資訊隱藏的階段中，假設Div =15，並且先去計算區塊B中的二個像素值(g_i與g_i+1)之差異值$d = |g_i - g_{i+1}|$。假設像素差異值d屬於低頻區域，則利用3-bit LSB來隱藏機密資訊，嵌入後得到了新像素值(g'_i與g'_i+1)。然後，再去計算新像素差異值$d' = |g'_i - g'_{i+1}|$，如果新像素差異值d'屬於低頻區域，則完成此區塊的資訊隱藏。相對的，如果新像素差異值d'屬於高頻區域，則必須針對新的像素值(g'_i和g'_i+1)進行調整，其調整的函數如方程式(3)所示。相對的，假設像素差異值d屬於高頻區域，則利用PVD來隱藏機密資訊。

$$(g'_i, g'_{i+1}) = \begin{cases} (g'_i - 8,\ g'_{i+1} + 8), & if\ \ g'_i \geq g'_{i+1} \\ (g'_i + 8,\ g'_{i+1} - 8), & if\ \ g'_i < g'_{i+1} \end{cases} \tag{3}$$

例如，有二個像素值g_i = 160和 g_i+1 = 150，機密訊息為$111000_{(2)}$, 高頻與低頻的門檻值 Div =15，則兩個像素的差異值d = | 160 – 150 | = 10，屬於低頻區域，則利用3-bit LSB做資訊隱藏，經過隱藏後得到新的像素值g'_i = 167和 g'_i+1 = 144。但是，新的像素差異值為 d'_i = 23 (167-144) > Div = 15，則必須要利用方程式(3)進行調整，得到調整後g'_i = 159和 g'_i+1 = 152，而且調整後的像素值差異d'_i = 7 (159 – 152)，仍然與原始像素差值值落於相同的低頻區域。

參、研究方法

在本節中，將介紹我們所提出的Blocked PVD 資訊隱藏技術，以四個像素為一個Block來做考量。我們的方法主要是擴展學者Wu et al.的PVD方法，其方法每次只考慮二個像素所組成的區塊。在圖1(a)中，顯示出學者Wu et al.提出的像素值差異法，四個相鄰像素的分群方式。而四個相鄰像素為一個區塊的所有可能的分群方式表示在圖1(b)。考量分群的方式愈周延，可以促使資訊隱藏的方法愈有效率，提高資訊隱藏的容量。所

以，我們一次考量含有四個像素之區塊，以整體區塊的像素值差異為依據，調和出二對像素值，分別用PVD方式來嵌入資訊，以便增加嵌入的效率。在下面小節中，會詳細的介紹資訊隱藏與萃取的步驟。

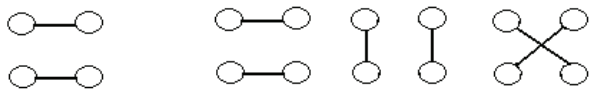


圖1：以四個相鄰像素為一個區塊的分群情形。 (a) 學者 Wu et al.提出的像素值差異法的分群結果。 (b) 在一個區塊中所有可能的分群情形。

一、區塊劃分和群組建立

從掩護影像中，將四個相鄰的像素($p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$, $p_{i+1,j+1}$)劃分為一個區塊，利用雷射掃描的順序由左到右由上到下，把整張圖形做完整的劃分，成為多個不重疊的區塊，如圖2所示。將此四個相鄰像素($p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$, $p_{i+1,j+1}$)重新命名為p_1、p_2、p_3和p_4，其對應的灰階值g_1、g_2、g_3和g_4符合$g_1 \le g_2 \le g_3 \le g_4$的限制。將此四個像素值分為($g_1$, g_4)和 (g_2 , g_3)二個群組(Groups)，其中像素$p_{i,j}$所屬的群組定義為*group*1，另外一個群組定義為*group*2。接著，計算整個區塊的差異值d，其計算方式為$(g_4 + g_3) - (g_2 + g_1)$。另外，分別計算二個群組各自的像素差異值$(g_4 - g_1)$ 和 $(g_3 - g_2)$，並將*group*1的差異值定義為d_1，*group*2的差異值定義為d_2。整個區塊的差異值最大範圍為0～511，將此範圍劃分為數個連續的區間R_i ($_i = 1, 2, 3, \cdots, r$)，其中i稱為區間R_i的索引值。區間R_i的上界定義為u_i，下界定義為l_i，其寬度w_i為$u_i - l_i + 1$。每一個區間的寬度必須限制為2的次方，方便隱藏二進制(Binary)的機密資訊。

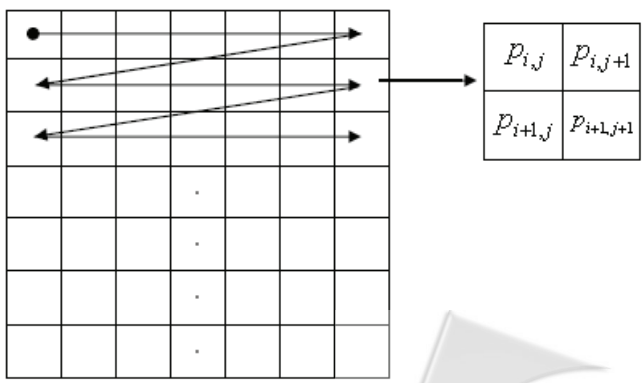


圖 2：以雷射掃描的順序來劃分掩護影像成為不重疊的區塊，其中每個區塊包含四個相鄰像素。

二、嵌入資訊的方法

在嵌入資訊的階段中，我們可以把欲藏入的秘密訊息當成是一個很長的二元字串

(Bit String)，藏入區塊中。整個區塊的差異值屬於某個區間內，就可依照此區間的寬度得知此區塊可以藏入多少個位元。假設有四個相鄰像素的區塊B，其區塊差異值d落在區間R_k內，則可以計算區間R_k的寬度$w_k=u_k-l_k+1$，並將寬度w_k平均分配給二個群組$group1$和$group2$，各自用來嵌入資訊，所以每個群組可以藏入$\log_2 \frac{w_k}{2}$個位元。群組藏入資訊的方式，依照方程式(4)來運算，可以產生兩群組的新差異值d'_1和d'_2：

$$\begin{aligned}
&\text{Case 1: } |d_1 - d_2| \le (u_k - l_k + 1)/2 \\
&\qquad d_1' = (l_k/2) + b_1,\ d_2' = (l_k/2) + b_2; \\
&\text{Case 2: } |d_1 - d_2| > (u_k - l_k + 1)/2 \\
&\qquad \text{If } d_1 > d_2 \\
&\qquad\quad d_1' = l_k + b_1,\ d_2' = b_2 \\
&\qquad \text{Else} \\
&\qquad\quad d_1' = b_1,\ d_2' = l_k + b_2;
\end{aligned} \tag{4}$$

其中，b_1和b_2為欲藏入的位元所換算出來的數值，並分別藏入群組group1和group2中。最後，利用新差異值g'_1和g'_2，經由反向計算產生新的四個像素值g'_1、g'_2、g'_3和g'_4。整個嵌入方法的步驟如下：

（一）利用雷射掃描的順序，把掩護影像的四個相鄰像素($p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$, $p_{i+1,j+1}$)視為一個區塊，劃分成多個不重疊的區塊。

（二）在每一個區塊中必須執行下列的步驟：

1. 將區塊中的像素重新命名為p_1、p_2、p_3和p_4。
2. 將p_1、p_2、p_3和p_4區分為二個群組$group1$和$group2$。
3. 計算區塊的差異值d，並且找出d所落入的區間R_k。如果R_k為最後一個區間，即$k = r$，則放棄在此一區塊的嵌入過程(其證明在附錄中的Lemma 3)。
4. 計算群組$group1$和$group2$的像素差異值d_1和d_2。
5. 利用方程式(4)計算新的差異值d'_1和d'_2。
6. 利用下面的反向計算產生新的像素值g'_1、g'_2、g'_3和g'_4。

群組$group1$的反向計算：

If $group1$包含 p_1 和 p_4

$$g_1' = g_1 - \lceil (d_1' - d_1)/2 \rceil$$
$$g_4' = g_4 + \lfloor (d_1' - d_1)/2 \rfloor$$

Else

$$g_2' = g_2 - \lceil (d_1' - d_1)/2 \rceil$$
$$g_3' = g_3 + \lfloor (d_1' - d_1)/2 \rfloor$$

群組$group2$的反向計算：

If group2包含 p_1 和 p_4

$$g_1' = g_1 - \lceil (d_2' - d_2)/2 \rceil$$
$$g_4' = g_4 + \lfloor (d_2' - d_2)/2 \rfloor$$

Else

$$g_2' = g_2 - \lceil (d_2' - d_2)/2 \rceil$$
$$g_3' = g_3 + \lfloor (d_2' - d_2)/2 \rfloor$$

1. 運用像素值移位(Pixel-Value Shifting)的技術移動像素值，使得像素值符合$g_1' \le g_2' \le g_3' \le g_4'$或$g_2' \le g_1' \le g_4' \le g_3'$的情況。而且，使得$(g_1-g_1')^2+(g_2-g_2')^2+(g_3-g_3')^2+(g_4-g_4')^2$的數值最小化。
2. 依據圖3和圖4的分類，利用像素值移位方式，微調區塊中的像素值，使得$p_{i,j}$可以辨視出它的夥伴。

上述的演算法中，所謂像素值移位技術，是對同一群組的像素值同時加上或減去某個數值，達到平行移動的效果，如此可以維持其差異值不變。另外，為了能夠正確的萃取出秘密資訊，必須能夠判斷出$p_{i,j}$的夥伴(Partner)，以便區別出*group*1和*group*2的各自成員。故我們必須去考量經過隱藏後$p_{i,j}$及其他三個像素值的所有變動情形。圖3與圖4顯示出所有可能的情形，其中，圖3顯示出經過隱藏後$p_{i,j}$的像素值與其他三個像素值不相等的所有情形。在圖3的狀況下，$p_{i,j}$可以輕易的找出它的夥伴，以區分出*group*1和*group*2的成員(成員以像素值做區別即可，不需用像素本身來區分)。相對的，經過隱藏後也有可能造成$p_{i,j}$的像素值與其他三個像素值有相等的情形，此時辨別$p_{i,j}$的夥伴，必須運用像素值移位的技術來進一步處理。圖4顯示$p_{i,j}$的像素值與其他的三個像素值至少有一個相同的所有情形。部份情形會造成$p_{i,j}$無法辨別出它的夥伴。例如，圖4(a)之 $p_{i,j}$就無法辨別出其夥伴，此時須利用像素值移位操作，進一步的處理，圖4(a)右半部顯示處理後的可能情形，經由移位後$p_{i,j}$就可以辨視出其夥伴。最後，比較特的是圖4(g)之右半部第二種情形，這是唯一經過像素值移位操作後，$p_{i,j}$仍無法辨視出其夥伴的案例，但我們可以將$p_{i,j}$的夥伴視為與$p_{i,j}$有相同像素值者即可解決。

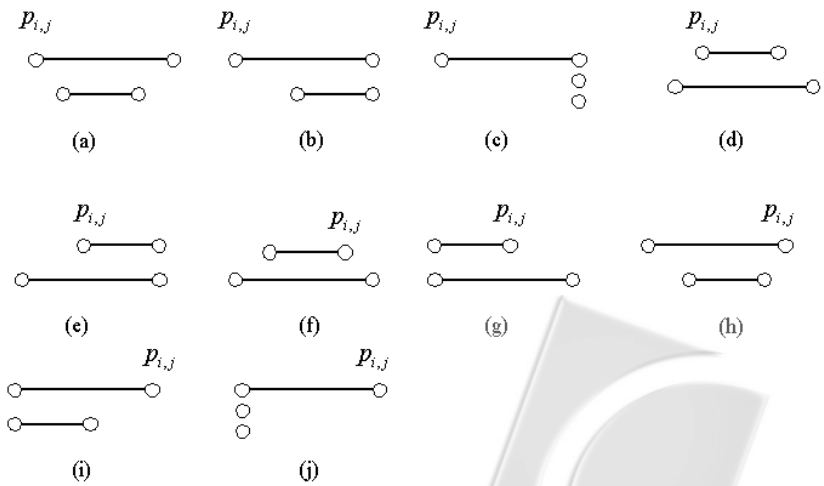


圖3：一個區塊中，$p_{i,j}$的像素值與其三個像素值不相等的所有情形。

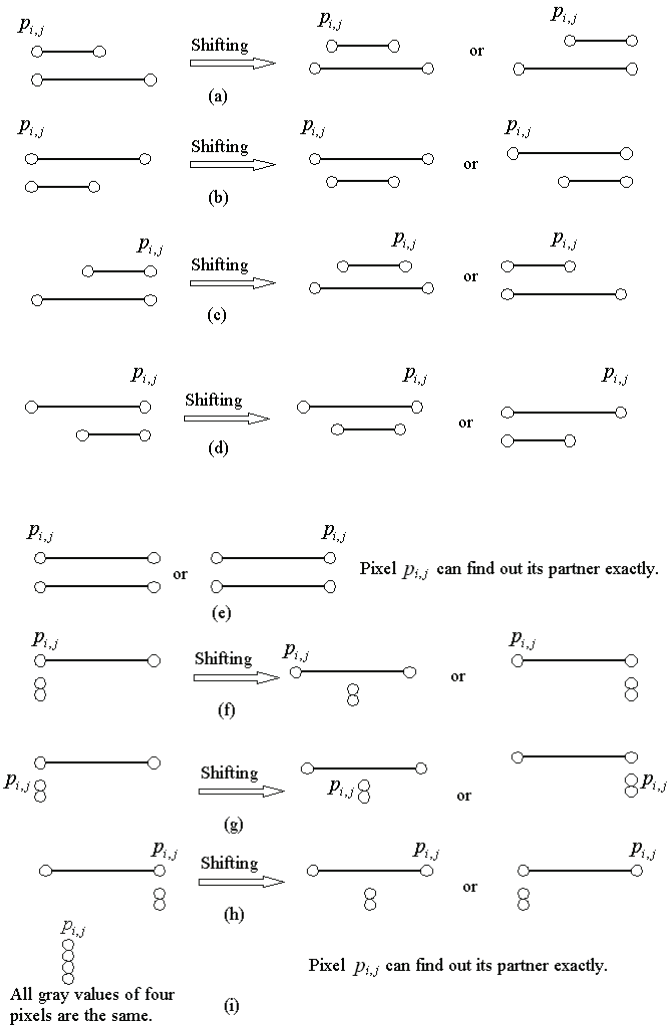


圖4：一個區塊中，至少有一個像素值與 $p_{i,j}$ 的像素值相等的所有情形，其中，部份情形須經由像素值移位方式來處理。

在圖5中，我們以一個區塊範例來說明。首先，先將四個像素值重新命名為$(g_1, g_2, g_3, g_4) = (137, 140, 150, 153)$，因為$p_{i,j}$的像素值為$g_4 = 153$，所以，*group*1為 $(g_1, g_4) = (137, 153)$，*group*2 為 $(g_2, g_3) = (140, 150)$。接著計算區塊差異值 d 為 $(153 + 150) – (140 + 137) = 26$，差異值$d$落於$R_k[16, 31]$內，此區間的寬度$w_k = 31–16+1=16$，表示每一個群組可以藏入$\log_2 \frac{16}{2} = 3$位元的資料量。群組之差異值$d_1=16$和$d_2=10$。假設有秘密訊息110011011，依序由左至右被嵌入，則*group*1被嵌入的訊息為110，*group*2被嵌入的訊息為011。因為$|d_1 – d_2| = 6 \le 8\ (= 16 / 2)$，由方程式(4)的Case 1 可以得到$d'_1$與$d'_2$的值，$d'_1=8+(110)_2=14$與$d'_2=8+(011)_2=11$ 。最後，利用嵌入演算法中步驟二(6)來進行像素的反向計算，得到新的像素值$(g'_1, g'_4) = (138, 152)$ 與 $(g'_2, g'_3) = (139, 150)$。因為經過反向計算後所得到的新像素

值已經滿足了$g_1' \le g_2' \le g_3' \le g_4'$的限制，所以，就省略了步驟二(7)的動作。目前$p_{i,j}$的像素值$g'_4 = 152$，與其他三個像素值形成圖3(h)的狀況，所以步驟二(8)不會進一步微調區塊中的像素值。嵌入資訊後新的區塊差異值為d' (152 + 150) – (139 + 138) =25， 仍然與嵌入前的區塊差異值屬於相同的區間[16, 31]，這一點我們在附錄中的Lemma 1提出證明。另外因為$|d_1 - d_2| \le 8$，所以d'_1和 d'_2亦會滿足$|d'_1 - d'_2| \le 8$的關係式，這一點我們在附錄中的Lemma 2提出證明。

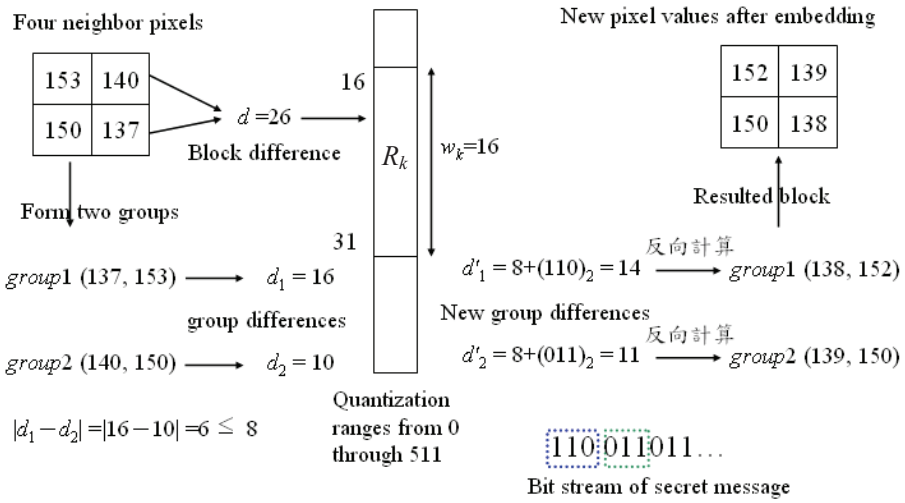


圖5：以一個區塊範例來做資訊隱藏

三、萃取資訊的方法

在萃取的過程中，其區塊劃分的方式與嵌入時完全相同。從每一個區塊中取得d, k, *group*1, *group*2, d_1,和d_2數值，若$k = r$代表此區塊沒有藏入資訊，否則利用方程式(5)計算出所藏入的數值b_1和b_2。最後，利用w_k算出藏入各個群組的位元數，再將b_1和b_2轉換成藏入的位元。

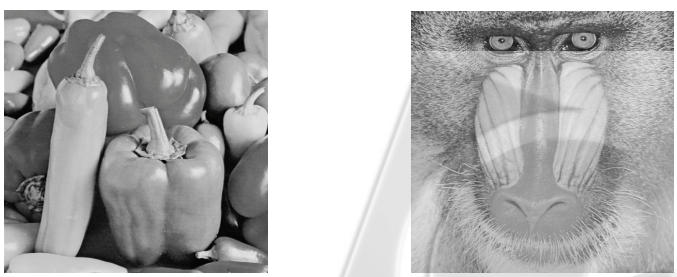
$$
\begin{aligned}
&\text{Case 1: } |d_1 - d_2| \le (u_k - l_k + 1)/2 \\
&\qquad b_1 = d_1 - (l_k / 2), b_2 = d_2 - (l_k / 2); \\
&\text{Case 2: } |d_1 - d_2| > (u_k - l_k + 1)/2 \\
&\qquad \text{If } d_1 > d_2 \\
&\qquad\quad b_1 = d_1 - l_k, b_2 = d_2 \\
&\qquad \text{Else} \\
&\qquad\quad b_1 = d_1, b_2 = d_2 - l_k;
\end{aligned}
\tag{5}
$$

我們以圖5範例來說明萃取的過程。由圖5藏入資訊後的區塊，可以得到$p_{i,j}$的像素值$g'_4 = 152$，所以*group*1=(g_1, g_4) = (138, 152) ，(g_2, g_3) = (139, 150)。計算區塊的差異值d = (152 + 150) (139 + 138) = 25。差異值d落於R_k[16, 31]內，此區間的寬度w_k = 31 – 16 + 1= 16，表示每一個群組可以藏入3位元的資料量。群組之差異值d_1 = 14 和 d_2 = 11。因為$|d_1 -$

$d_2| = 3 \le 8\ (= 16 / 2)$，由方程式(5)的Case 1 可以得到$b_1$和$b_2$的值，$b_1 = 14 - 8 = (110)_2$和$b_2 = 11 - 8 = (110)_2$。

肆、實驗結果

在此節我們使用了十張512×512的灰階掩護影像來做實驗分析，其中二張掩護影像如圖6所顯示的‘Peppers’和‘Baboon’；在此實驗中，我們設定了二組區間寬度，將[0, 511]範圍切割成多個連續的區間。在第一組實驗中我們將[0, 511]切割成為[0, 15]，[16, 31]，[32, 63]，[64, 127]，[128, 255]，[256, 511]。第二組實驗將[0, 511]切割成為[0, 31]，[32, 63]，[64, 127]，[128, 255]，[256, 511]。在此實驗中，我們使用了Random Bits、影像‘Boat’和‘Airplane’做為機密資訊，圖7所顯示大小為256×256 的灰階機密影像。當以Random Bits為機密資訊時，其資訊隱藏量與PSNR值的計算，是經過100次的實驗取其平均值的結果。由表1可以看出我們所設定的二組區間寬度的資訊隱藏量與PSNR值的結果，其中，在第二組的實驗中，我們將實驗的區間寬度拉大了，所以會有較大的資訊隱藏量。相對的，因為隱藏了較多的訊息，所以PSNR值會比第一組的還要差，但仍在人類視覺可以接受的PSNR範圍內。圖8為使用‘Peppers’和‘Baboon’為掩護影像的執行結果。圖8(a)為藏入Random Bits為機密資訊所產生之偽裝影像。圖8(b)為偽裝影像與掩護影像之間的差異圖形(每一個像素差異數值乘以8，再取反相)。同樣的實驗方法，圖9中則顯示了，利用另一組區間寬度的實驗結果。從圖8(b)與 圖9(b)中，可以看出我們將大量的資訊藏在邊緣區域。表2呈現的是我們所提出的方法與學者Wu et al.所提出方法之資訊隱藏量與PSNR值之比較。從表2中可以明顯的看出，我們所提出的方法有較大的資訊隱藏量，也能維持偽裝影像的一定品質。而且，我們也引用了Fridrich et al. (2001)所提出的統計檢測方法來檢測，檢測我們所提出的方法是否符合機密嵌入之安全性，其結果如圖10所示。從圖10(a)(b)所示，利用Simple 2-bit LSB取代法，以及和結合像素值差異法與3-bit LSB取代法，其嵌入資訊後後，無法使得$R_m \cong R_{-m}$與$S_m \cong S_{-m}$，由此可知，此資訊嵌入的方法容易被RS-diagrams 所檢測。相對的，可知我們所提出的Blocked PVD方法與學者Wu et al.所提出的PVD方法皆能使得$R_m \cong R_{-m}$與$S_m \cong S_{-m}$，通過RS-diagrams 所檢測，使得嵌入的資訊更具有安全性。

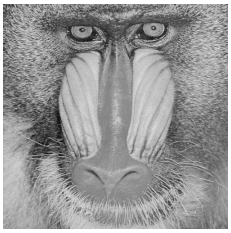


(a) (b)

圖6 ：實驗中的二張51 2 × 512大小的灰階掩護影像: (a) Peppers; (b) Baboon


(a) (b)

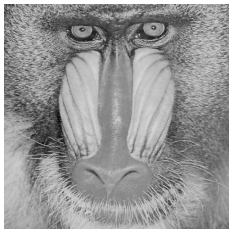
圖7 ：實驗中的256×256大小的灰階機密影像: (a) Boat; (b) Airplane。

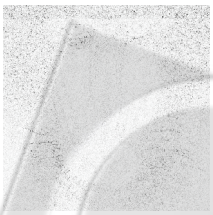
(a)


(b)

圖8：利用16、16、32、64、128和256的區間寬度之執行結果：
(a)偽裝影像；(b) 偽裝影像與掩護影像之差異圖形。

(a)

(b)

圖9：利用32、32、64、128和256的區間寬度之執行結果：
(a)偽裝影像； (b) 偽裝影像與掩護影像之差異圖形。

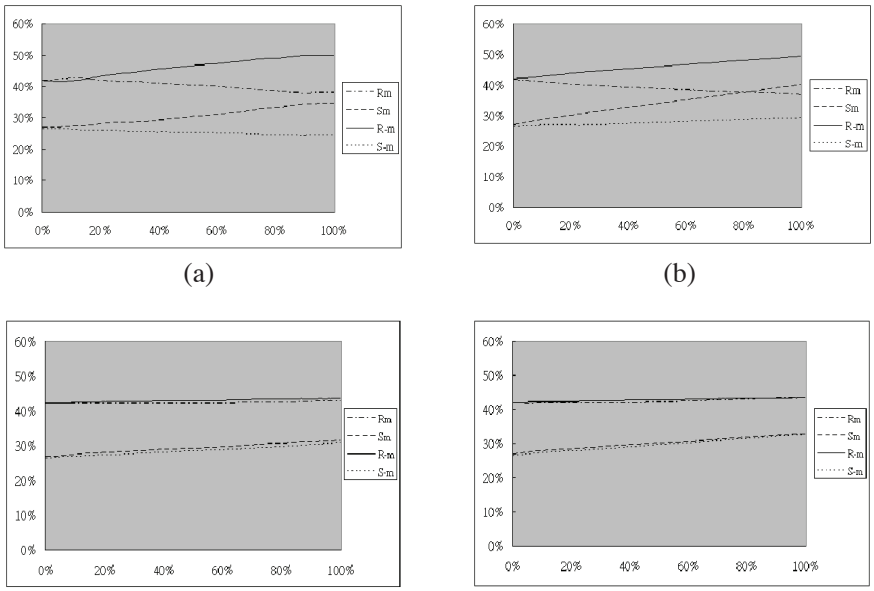


圖10：利用學者Fridrich et al. (2001)所提出的RS-diagrams 檢測法，來檢測四種以Random為機密訊息嵌入至Lean的圖形中: (a) Simple 2-bit LSB (b) 結合像素值差異法與3-bit LSB取代法 (c) 像素值差異法 (d) 利用16、16、32、64、128和256的區間寬度之區塊式方法。

表1：我們的Blocked PVD方法利用Random bits 、Boat和Airplane為機密資訊，嵌入至掩護影像後的資料隱藏量及PSNR值。

掩護影像 (512×512)		第一組區間寬度 16, 16, 32, 64, 128 , 256			第二組區間寬度 32, 32, 64, 128 , 256		
		Random bits	Boat	Airplane	Random bits	Boat	Airplane
Lena	Capacity PSNR	408,828 39.31	408,828 40.25	408,828 40.05	527,626 35.94	527,626 36.81	527,626 36.42
Baboon	Capacity PSNR	481,288 33.37	481,288 33.99	481,288 33.71	553,994 32.48	553,994 32.99	553,994 32.76
Peppers	Capacity PSNR	406,688 39.20	406,688 40.12	406,688 39.87	527,924 36.53	527,924 36.86	527,924 36.48
Toys	Capacity PSNR	418,274 38.07	418,274 38.72	418,274 38.44	532,460 35.65	532,460 36.25	532,460 35.81
Sailboat	Capacity PSNR	426,396 36.96	426,396 37.49	426,396 37.35	533,496 34.60	533,496 35.39	533,496 35.12
Girl	Capacity PSNR	406,254 39.59	406,254 39.74	406,254 39.46	526,810 36.41	526,810 36.49	526,810 36.10
Gold	Capacity PSNR	414,528 38.82	414,528 39.67	414,528 39.49	528,042 35.91	528,042 36.75	528,042 36.44

Zelda	Capacity PSNR	400,698 40.86	400,698 41.40	400,698 41.35	525,674 37.20	525,674 37.39	525,674 36.91
Barb	Capacity PSNR	456,800 34.90	456,800 35.53	456,800 35.31	545,072 33.52	545,072 34.25	545,072 33.93
Tiffany	Capacity PSNR	406,144 39.53	406,144 40.01	406,144 39.83	527,776 35.87	527,776 36.58	527,776 36.13

表2：比較學者Wu et al. (2003)提出的PVD方法與我們提出的Blocked PVD方法，利用Random Bits為機密訊息，嵌入至掩護影像後的資料隱藏量及PSNR值。

掩護影像 (512×512)	PVD方法		Blocked PVD方法	
	區間寬度8, 8, 16, 32, 64, 128		區間寬度16, 16, 32, 64,128, 256	
	Capacity	PSNR	Capacity	PSNR
Lena	406,632	41.71	408,828	39.31
Baboon	437,806	39.14	481,288	33.37
Peppers	401,980	40.39	406,688	39.20
Toys	406,656	39.93	418,274	38.07
Sailboat	415,554	37.36	426,396	36.96
Girl	402,965	42.54	406,254	39.59
Gold	405,634	42.20	414,528	38.82
Zelda	398,584	42.66	400,698	40.86
Barb	442,529	36.24	456,800	34.90
Tiffany	403,764	41.47	406,144	39.53
Average	412,210	40.36	422,590	38.06

伍、結論

在本篇論文中，我們提出一個新的藏密技術，可擁有更高容量、不易被察覺，且不可被程式檢測的特性。我們稱之為Blocked PVD的資訊隱藏技術。我們的方法延伸了學者Wu et al.所提出的像素值差異的方法，一次以四個相鄰像素的差異值來做資訊隱藏，我也提出了像素值移位的方式，促使我們的資訊隱藏技術更具有彈性且更具有周延性。實驗數據顯示，我們所提出的Blocked PVD方法比學者Wu et al.所提出的PVD方法，擁有較多的資訊隱藏量，且其偽裝影像品質都還在適當的PSNR值之內。雖然，目前學者Wu et al.所提出結合像素值差異法與LSB取代法，擁有較高的資訊隱藏量與擁有較佳的偽裝影像品質，但是其方法很容易被Fridrich et al.學者的程式檢測，不符合資訊嵌入之安全性；相對的，我們的所提出的Blocked PVD 方法與PVD方法，都可以通過Fridrich et al.學者的程式檢測。藉此，我們的研究為藏密學的技術發展提供一個具體可行的策略，以為研發的需求。

致謝

This research was partially supported by the National Science Council of the Republic of China under the Grants NSC 96-2221-E-153-001 and the TWISC@NCKU under the Grants NSC 96-2219-E-006-009.

參考文獻

1. Anderson, R. J., and Peticolas, F. A. P. "On the Limits of Steganography," *IEEE Journal of Selected Areas in Communications* (16:4), 1998, pp. 474-481.
2. Artz, D. "Digital Steganographic: Hiding Data within Data," *IEEE Internet Computing* (5:3), 2001, pp. 75-80.
3. Bender, W., Gruhl, D., Morimoto, N., and Lu, A. "Techniques for Data Hiding," *IBM Systems Journal* (35) 1996, pp. 313-316.
4. Chan, C. K., and Chen, L. M. "Hiding Data in Images by Simple LSB Substitution," *Pattern Recognition* (37:3), 2004, pp. 469-474.
5. Chang, C. C., and Tseng, H. W. "A Steganographic Method for Digital Images Using Side Match," *Pattern Recognition Letters* (25:12), 2004, pp. 1431-1437.
6. Chang, C. C., Chen, T. S., and Chung, L. Z. "A Steganographic Method Based upon JPEG and Quantization Table Modification," *Information Sciences* (141:1), 2002, pp. 123-138.
7. Chu, Y. H., and Chang, S. "Dynamical Cryptography Based on Synchronized Chaotic Systems," *IEE Electronics Letters* (35:12), 1999, pp. 974-975.
8. Fridrich, J., Goljan, M., and Du, R. "Reliable Detection of LSB Stegnography in Grayscale and Color Images," *Proceedings of ACM Workshop on Multimedia and Security*, 2001, pp. 27-30.
9. Highland, H. J. "Data Encryption: a non-Mathematical Approach," *Computers and Security* (16:5), 1997, pp. 369-386.
10. Katzenbeisser, S., and Petitcolas, F. A. P. *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Inc., Boston, 2000.
11. Lee, Y. K, and Chen, L. H. "High Capacity Image Steganography," *IEE Proceedings on Vision Image and Signal Processing* (147:3), 2000, pp. 288-294.
12. Wang, R. Z., Lin, C. F., and Lin, J. C. "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," *Pattern Recognition* (141:1), 2000, pp. 671-683.
13. Wu, D. C., and Tsai, W. H. "A Steganographic Method for Images by Pixel-Value Differencing," *Pattern Recognition Letters* (24:9-10), 2003, pp. 1613-1626.
14. Wu, H. C., Wu, N. I., Tsai, C. S., and Hwang, M. S. "Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods," *IEE Proceedings on*

Vision Image and Signal Processing (152:5), 2005, pp. 611-615.

15. Yang, C. H., and Wang, S. J. "Weighted Bipartite Graph for Locating Optimal LSB Substitution for Secret Embedding," *Journal of Discrete Mathematical Sciences & Cryptography* (9:1), 2006, pp. 153-164.
16. Yu, Y. H., Chang, C. C., and Hu, Y. C. "Hiding Secret Data in Images via Predictive Coding," *Pattern Recognition* (38:5), 2005, pp. 691-705.

附錄

在我們的Blocked PVD方法中，其區間分割方式需要受到一點限制，其描述如下：

限制：Blocked PVD的區間的分割方式，必須限制$l_k \geq w_k$，其中l_k為區間R_k的下界，w_k為區間R_k的寬度，但$k \neq 1$。

對於區間[0, 511]的分割，滿足上述限制的分割範例如實驗中所使用的二組，第一組是[0, 15]，[16, 31]，[32, 63]，[64, 127]，[128, 255]，[256, 511]。第二組是[0, 31]，[32, 63]，[64, 127]，[128, 255]，[256, 511]。

為了進一步論述我們的Blocked PVD的演算法的正確性，我們證明下面的定理：

Lemma 1. 嵌入資訊前的區塊差異值d，與嵌入資訊後的區塊差異值d'，會落在同一個區間內。

證明：

假設區塊差異值d是落於區間R_k內，u_k和l_k分別為R_k的上界與下界。另外，d_1和d_2分別是*group*1與*group*2的像素差異值。嵌入資訊後，d'_1和 d'_2分別是*group*1與*group*2新的像素差異值。

$d \in [l_k, u_k]$, *let* $w_k = u_k - l_k + 1$

if $|d_1 - d_2| \leq \frac{w_k}{2}$

$\Rightarrow$ 由公式(4)得知，$[l_k, u_k]$被化分成$[\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$和$[\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$，分別給 *group*1 與 *group*2 來嵌入資訊。

$\Rightarrow d'_1 \in [\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$， $d'_2 \in [\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$

$\Rightarrow d' = d'_1 + d'_2 \in [\frac{l_k}{2} + \frac{l_k}{2}, (\frac{l_k}{2} + \frac{w_k}{2} - 1) + (\frac{l_k}{2} + \frac{w_k}{2} - 1)]$

$\Rightarrow d' \in [l_k, l_k + w_k - 2]$

$\Rightarrow d' \in [l_k, u_k]$

if $|d_1 - d_2| > \frac{w_k}{2}$ and $d_1 > d_2$

(我們只證明 $d_1 > d_2$ 的情形，另一種 $d_1 < d_2$ 的情形，其證明過程類似)

$\Rightarrow [l_k, u_k]$被化分成$[l_k, l_k + \frac{w_k}{2} - 1]$和$[0, 0 + \frac{w_k}{2} - 1]$，分別給 *group*1 和

*group*2 來嵌入資訊。

$\Rightarrow d'_1 \in [l_k, l_k + \frac{w_k}{2} - 1]$ ， $d'_2 \in [0, 0 + \frac{w_k}{2} - 1]$

$\Rightarrow d' = d'_1 + d'_2 \in [l_k + 0, (l_k + \frac{w_k}{2} - 1) + (0 + \frac{w_k}{2} - 1)]$

$\Rightarrow d' \in [l_k, l_k + w_k - 2]$

$\Rightarrow d' \in [l_k, u_k]$ Q.E.D.

Lemma 2. 假設區塊差異值d落於區間$R_k = [l_k \geq u_k]$內，其中u_k和l_k分別是R_k的上界和下界。令$w_k = u_k - l_k + 1$為區間R_k的寬度。另外，*group*1與*group*2嵌入資訊前後的像素差異值分別為d_1, d_2與d'_1, d'_2。則$k \neq 1$時，下列關係式存在：

if $|d_1 - d_2| \leq \frac{w_k}{2}$, *then* $|d'_1 - d'_2| \leq \frac{w_k}{2}$

if $|d_1 - d_2| > \frac{w_k}{2}$, *then* $|d'_1 - d'_2| > \frac{w_k}{2}$

證明：

if $|d_1 - d_2| \leq \frac{w_k}{2}$

$\Rightarrow$ 由公式(4)得知，$[l_k, u_k]$被化分成$[\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$和$[\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$，分別給 *group*1 與 *group*2 來嵌入資訊。

$\Rightarrow d'_1 \in [\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$ ， $d'_2 \in [\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$

$\Rightarrow \frac{l_k}{2} - (\frac{l_k}{2} + \frac{w_k}{2} - 1) \leq d'_1 - d'_2 \leq (\frac{l_k}{2} + \frac{w_k}{2} - 1) - \frac{l_k}{2}$

$\Rightarrow |d'_1 - d'_2| \leq \frac{w_k}{2} - 1$

$\Rightarrow |d'_1 - d'_2| \leq \frac{w_k}{2}$

if $|d_1 - d_2| > \frac{w_k}{2}$ and $d_1 > d_2$

(我們只證明 $d_1 > d_2$ 的情形，另一種 $d_1 < d_2$ 的情形，其證明過程類似)

$\Rightarrow [l_k, u_k]$被化分成$[l_k, l_k + \frac{w_k}{2} - 1]$和$[0, 0 + \frac{w_k}{2} - 1]$，分別給 *group*1 與 *group*2 來嵌入資訊。

$\Rightarrow d'_1 \in [l_k, l_k + \frac{w_k}{2} - 1]$ ， $d'_2 \in [0, 0 + \frac{w_k}{2} - 1]$

由 Blocked PVD 的區間分割限制：當 $k \neq 1$ 時， $l_k \geq w_k$

$\Rightarrow l_k - (0 + \frac{w_k}{2} - 1) \leq d'_1 - d'_2 \leq (l_k + \frac{w_k}{2} - 1) - 0$

$\Rightarrow l_k - \frac{w_k}{2} + 1 \leq d'_1 - d'_2 \leq l_k + \frac{w_k}{2} - 1$

（只考慮左半部）

$$\Rightarrow |d'_1 - d'_2| \geq l_k - \frac{w_k}{2} + 1 \geq w_k - \frac{w_k}{2} + 1$$

$$\Rightarrow |d'_1 - d'_2| \geq \frac{w_k}{2} + 1$$

$$\Rightarrow |d'_1 - d'_2| > \frac{w_k}{2}$$

Q.E.D.

在Lemma 2中，只考慮$k \neq 1$的情況。當時，在嵌入資訊後的過程，不管是$|d_1 - d_2| \leq \frac{w_k}{2}$，或是$|d_1 - d_2| > \frac{w_k}{2}$，公式(4)都是將區間$R_1$=[$l_1$, u_1]化分成$[0, \frac{w_1}{2} - 1]$和$[0, \frac{w_1}{2} - 1]$，分別給*group*1和*group*2來嵌入資訊。因此，嵌入資訊後，$d'_1 \in [0, \frac{w_1}{2} - 1]$且$d'_2 \in [0, \frac{w_1}{2} - 1]$。所以，$|d'_1 - d'_2| \leq \frac{w_1}{2}$。此時，其所對應的萃取資訊的過程，公式(5)會利用Case 1來萃取出正確的機密訊息。

Lemma 3. 一個區塊不能用來隱藏資訊的情況，只有當區塊的差異值d，落在最後一個區間R_r時。

證明：

因為我們運用了Pixel-Value Shifting 的技術，所以當嵌入資訊後$d_1' \leq 255$或$d_2' \leq 255$，則表示*group*1與*group*2可以被用來嵌入資訊。所以，只有在$d_1' > 255$或$d_2' > 255$時，必須要放棄整個區塊的資訊隱藏。

由公式(4)得知，

if $|d_1 - d_2| \leq \frac{w_k}{2}$，[$l_k$, u_k]則被化分成$[\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$和$[\frac{l_k}{2}, \frac{l_k}{2} + \frac{w_k}{2} - 1]$，分別給*group*1與*group*2來嵌入資訊。

if $|d_1 - d_2| > \frac{w_k}{2}$ and $d_1 > d_2$(我們只證明$d_1 > d_2$的情形，另一種$d_1 < d_2$的情形，其證明過程類似)，則[l_k, u_k]被化分成$[l_k, l_k + \frac{w_k}{2} - 1]$和$[0, 0 + \frac{w_k}{2} - 1]$，分別給*group*1與*group*2來嵌入資訊。

所以，嵌入資訊後，

$$\frac{l_k}{2} \leq d'_1 \leq \frac{l_k}{2} + \frac{w_k}{2} - 1，\ \frac{l_k}{2} \leq d'_2 \leq \frac{l_k}{2} + \frac{w_k}{2} - 1$$

或$l_k \leq d'_1 \leq l_k + \frac{w_k}{2} - 1$，$0 \leq d'_2 \leq w_k - 1$

由Blocked PVD 區間分割之限制，我們可以得知R_r = [256, 511]。因此，唯根據上列d'_1和d'_2的可能範圍，有當$k = r$時，會造$l_k + \frac{w_k}{2} - 1 = 256 + \frac{256}{2} - 1 = 383 > 255$，即造成$d_1'$>255。所以，當區塊差異值$d$落在最後一個區間$R_r$時，此區塊不能用來隱藏資訊。

Q.E.D.

由Lemma 3的證明過程中得知，我們的嵌入演算法之所以不能使用$k = r$的區塊來

嵌入資訊時，主要是因為此時公式(4)之Case 2，會分割出區間$[l_k, l_k + \frac{w_k}{2} - 1]$給*group*1或*group*2來嵌入資訊。所以，我們只要稍微調整公式(4)和公式(5)，就可以避開$k = r$時不能嵌入資的情形。其調整如下：

公式(4)之調整：

If $k \neq r$

Case 1: $|d_1 - d_2| \leq (u_k - l_k + 1)/2$

$d_1' = (l_k / 2) + b_1,\ d_2' = (l_k / 2) + b_2$;

Case 2: $|d_1 - d_2| > (u_k - l_k + 1)/2$

If $d_1 > d_2$

$d_1' = l_k + b_1,\ d_2' = b_2$

Else

$d_1' = b_1,\ d_2' = l_k + b_2$

Else

$d_1' = (l_k/2) + b_1,\ d_2' = (l_k/2) b_2$

公式(5)之調整：

If $k \neq r$

Case 1: $|d_1 - d_2| \leq (u_k - l_k + 1)/2$

$b_1 = d_1 - (l_k / 2), b_2 = d_2 - (l_k / 2)$;

Case 2: $|d_1 - d_2| > (u_k - l_k + 1)/2$

If $d_1 > d_2$

$b_1 = d_1 - l_k, b_2 = d_2$

Else

$b_1 = d_1, b_2 = d_2 - l_k$

Else

$b_1 = d_1 - (l_k/2), b_2 = d_2 - (l_k/2)$