

## 整合像素差值法及最低位元取代法之影像藏密法

楊勝凱<sup>1</sup> 黃炳森<sup>2\*</sup>

<sup>1</sup> 嘉南藥理科技大學資訊管理系

<sup>2</sup> 銘傳大學電子工程系

### 摘 要

資料隱藏技術主要是設法把重要資訊隱藏於數位化媒體(如圖像、聲音、視訊)之中。利用像素值之調整可達到藏密之目的，倘若能同時整合像素差值法與最低位元法，則更可以提升藏密資料量。本論文所提出的演算法，先使用像素差值法藏入資料，再利用最低位元取代法來調整已隱藏資料的像素值，以增加藏密容量，並同時降低對圖像品質之影響，抽取隱藏資料的方式則可以反方向進行之。實驗結果顯示，當藏密容量需求增加時，本論文所提方法與像素差值法及像素差值和最低位元取代合併法比較後，本論文所提方法之優點是可以同時增加藏密容量，並保持圖像品質的。

**關鍵詞：**資料隱藏，加密，像素差值，最低位元取代法。

## Image Steganographic Approach by Integrating Pixel-value Differencing and LSB Replacement Schemes

Sheng-Kai Yang<sup>1</sup> and Ping S. Huang<sup>2\*</sup>

<sup>1</sup>Department of Information Management, Chia Nan University of Pharmacy&Science

<sup>2</sup>Department of Electronic Engineering, Ming Chuan University

### ABSTRACT

The purpose of information hiding is to embed important message into digital media, such as images, voice, and video. Information hiding can be achieved by adjusting the pixel values inside the image and the hiding capacity can be increased by integrating the methods of pixel-value differencing (PVD) and LSB replacement (LSBR). To increase hiding capacity and reduce image degradation, this paper presents a hiding algorithm by firstly embedding information into the image using PVD and then adjusting the altered pixel values using LSBR to hide more information. The information extraction can be done along the reverse direction. Experimental results demonstrate that the proposed approach can increase the hiding capacity and keep the image quality simultaneously, while compared with the method of pixel-value differencing (PVD) and the combined version of PVD and LSBR.

**Keywords:** information hiding, steganography, pixel-value differencing, LSB replacement.

## 一、前言

近年來由於電腦與資訊科技的不斷進展，在這多媒體技術發達的時代中，文字、圖像、聲音及視訊皆可被轉換為數位資料來進行快速地傳遞。所以，如此也間接地增加了機密資料曝光而被竊取的危險，人們傳遞訊息及儲存資訊過程的安全性往往也大受挑戰。

傳統以密碼來進行設定權限的方式，並不太能完全有效地保證機密資料之保存，此法無疑是此地無銀三百兩，更增加了有心攔截竊取者想進一步破解密碼以得到資料的欲望。密碼學技術為保護資料的一種方法，處理方式乃將文件或各項資料轉變為亂碼以進行加密[1]，然後在網路上進行傳遞，以避免他人在竊取訊息後，能直接得知機密資料的內容。但是亂碼容易引起非法者起疑，而且現在電腦運算的速度越來越快，大大降低了破解秘密訊息所需的成本，相對地也增加了資料洩密的危險性。舉例來說，若要傳遞一個最普通不起眼的桌面圖像或網路圖像，如果我們能將欲傳遞的資料先行加密後，再儲存於偽裝圖像裡進行雙重保護，有心的攔截竊取者想達到其破解的目的就更難了。所以，為確保資料的安全性和機密性，資料隱藏(data hiding)[2-7]技術已成為當今數位資訊時代重要的課題。

資料隱藏在過去幾年來已被廣泛討論著，它是一種在公開場合傳送數位化資料，而不被發現其傳送資料裡頭有隱藏秘密資料的方法。顧名思義，就是當機密資料被隱藏進入載體圖像後，使得一般人單從載體外觀並不容易察覺到該資料的存在，並且可以在需要時能完整無缺地將秘密資料抽取出來。資料隱藏技術已被廣泛的使用於軍事[8]、商業和與反犯罪等相關應用中，其中最常用方式的是把資料隱藏於圖像當中，而圖像就是所謂載體。在藏入秘密資料之前的圖像稱為掩護圖像(cover image)，而藏入資料後的圖像稱為偽裝圖像(stego image)[9]。一個秘密的資料隱藏流程是發送方先將秘密資料藏入掩護圖像後成為偽裝圖像，然後透過網路傳遞方式將偽裝圖像送給接收方，接收方在接收後再從偽裝圖像中把秘密資料抽取出來。

秘密資料可分為二種，第一種是用在秘密通訊與資料管理。第二種是用來隱藏一個版權資訊如公司的商標、特別的註記等等，當圖像

遭受破壞時，仍然保有聲明版權的浮水印[10]。浮水印技術強調在萃取出浮水印之完整度與強健性[11]，而第一種主要著重在可藏入資料之最大容量及影像品質。

資料隱藏的藏密技術，依照處理方式的不同，大致可分為空間域(spatial domain)藏密技術及頻率域(frequency domain)藏密技術二種[6]。空間域的藏密技術主要是直接以小幅度改變掩護圖像的像素值來達成隱藏秘密資訊的目的，此類藏密法可以在不破壞影像的視覺品質下達成隱藏高容量資訊之目的。較常見的空間域藏密技術有像素差值法、補丁法、紋理區塊編碼法[12]、向量量化編碼法及最低位元取代法[6]等。本文所要探討的就是空間域的藏密技術，期望能在藏入最大容量的資料時[13]，同時顧全影像的品質。頻率域技術主要是把空間域中各影像的像素值關係轉換成頻率域的係數，再將秘密訊息隱藏在所選定的係數中。它是利用人類眼睛對於高頻訊號不易感知的原理，所以我們可以對高頻訊號加以改變，並且仍使眼睛不易看出改變之處，而達到資料隱藏的目標[14]。以網際網路上流傳最廣的 JPEG 圖像為例，部份學者是將秘密訊息嵌入在 JPEG 圖像量化後的離散餘弦轉換(Discrete Cosine Transform, DCT) 頻率係數中。

許多資訊隱藏方法已陸續被提出，其中的最低位元(Least Significant Bit, LSB)法[7,15]是把資料隱藏於圖像中最常用的一種方法，其原理是利用人類視覺系統對於圖像中像素的少量改變並沒有非常敏感，故針對像素的最低位元值做有限度調整是不會被發現的。另外，Da-Chun Wu 等[2]進一步提出了像素差值(Pixel-Value Differencing, PVD)的資料隱藏法，主要作法是以改變兩個相鄰且不重疊像素之間的像素差值為基礎，並將資料隱藏其中，它的偽裝圖像影像品質非常好。H.-C. Wu 等[3]提出了像素差值和最低位元取代合併法，主要以像素差值(Pixel-Value Differencing, PVD)的資料隱藏法為基礎，當像素差值小於某一分界值時，直接以最低位元法修改像素值來隱藏資料；若高於此分界值時，則以像素差值法來藏密。此舉雖然增加了隱藏的資料[16]，但也同時降低了偽裝圖像的品質[17]。Ko-Chin Chang 等[4]所提的三方向像素差值法帶動了另一方面的思考，它是以四個像素為一組，並以一對

三的方式區分出三個像素差值組，此方法比原始的像素差值(PVD)法多出了一對像素差值以供藏密，所以它能大大地提升可隱藏的資料容量，但相對的偽裝圖像影像品質也降低了不少。

本篇論文主要是針對灰階影像，提出一個可同時整合像素差值法和最低位元取代法的影像藏密法。不同於 H.-C. Wu 等[3]所提出的方法，必須在不同的量化區域分別使用像素差值法或最低位元取代法，我們的方法是在像素差值法所改變的像素值上，繼續使用改良的最低位元取代法來做第二次的像素值更改。第二次更改的結果除了可增加藏密量外，另可同時保持更改前的影像品質，不致於像傳統的低位元取代法會使影像品質惡化。因此，本論文的方法大大地改善了 H.-C. Wu 等[3]所提出的方法，不論在資料藏密量或圖像品質方面，都有較佳之效能。

## 二、圖像藏密法回顧

### 2.1 像素差值(PVD)法

Da-Chun Wu 等[2]所提出的像素差值(PVD)資料隱藏法，主要是藉著改變兩個相鄰且不重疊像素之間的像素差值為基礎[18]，其方法首先利用兩像素之差值大小所對應的量化表，決定出可隱藏資料的位元數，然後再進一步依據可隱藏的資料值來調整兩像素之差值，並進而改變其像素值以達到藏入資料的目的。

假設存在一個灰階影像，其高度與寬度分別為  $M$  個與  $N$  個像素，則此影像總共包含了  $M \times N$  個像素。其中的每一個像素可視為一個亮度的分量，各分量強度位元組的大小為 8 個位元。假設兩相鄰像素的位置分別為  $(i, j)$  及  $(i, j+1)$ ，而其所對應的像素值為  $f(i, j)$  及  $f(i, j+1)$ 。如果我們定義  $d$  為兩像素之差值  $|f(i, j+1) - f(i, j)|$ ，則  $d$  值應介於 0 與 255 之間。把  $d$  值的可能範圍分成 6 個區域，分別為 0 至 7、8 至 15、16 至 31、32 至 63、64 至 127 及 128 至 255(詳如表 1)。其中每塊區域所對應的可隱藏資料位元數分別為 3、3、4、5、6 與 7， $k$  為可藏入之位元量。當我們從隱藏資料中取出  $k$  位數，將其換算為 10 進位後的值

為  $w$ ，接著將  $w$  加上該區域的最小值  $g$  後得到  $p$ ，其中  $w + g = p$ 。此時利用  $p$  與  $d$  來調整  $f(i, j)$  及  $f(i, j+1)$  的像素值，以達到資訊隱藏之目的。

表 1. 差值範圍區間表

區域	差值範圍	可隱藏位元數(k)	區域最小值(g)
1	0至7	3	0
2	8至15	3	8
3	16至31	4	16
4	32至63	5	32
5	64至127	6	64
6	128至255	7	128

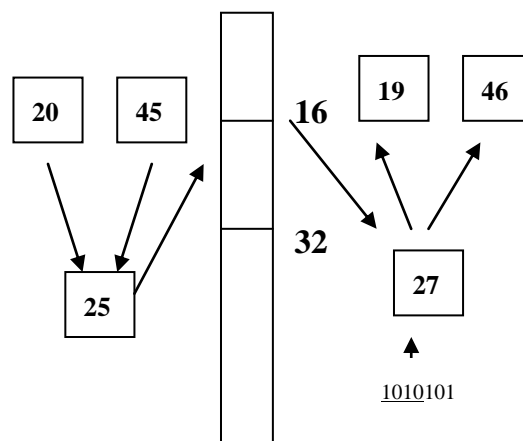


圖 1. PVD 方法示意圖

在此舉一例來說明像素差值法的運作方式。首先我們將整張影像以不重疊的兩個相鄰像素為單位來分組，此處以  $f(i, j) = 45$  及  $f(i, j+1) = 20$  為例，圖 1 為利用 PVD 方法進行資料隱藏的示意圖。假設  $d$  為兩相鄰像素之差值，在此例中的  $d = 45 - 20 = 25$ 。由表 1 得知 25 所對應的可隱藏資料位元數為  $k = 4$ ，此即表示可藏入的資料量為 4 個位元，若所隱藏資料的二進位值為  $(1011)_2$ ，將其換算為 10 進位後的值為  $(11)_{10}$ ，接著將其加上該區域的最小值 16 後得到  $p = 11 + 16 = 27$ 。接下來我們可以根據此值來調整  $f(i, j)$  及

$f(i, j+1)$  的像素值，得到新像素值  $f'(i, j)$  及  $f'(i, j+1)$ 。調整的算式如下所示：

$$p-d = 27-25 = 2 \quad d' = \left\lfloor \frac{2}{2} \right\rfloor = 1$$

$$f'(i, j) = 45+1 = 46$$

$$f'(i, j+1) = 20-1 = 19 \quad (1)$$

對於所隱藏資料的萃取方式則可利用反方向來進行。

## 2.2 H.-C. Wu 方法

H.-C. Wu 等[3]所提出的像素差值和最低位元取代合併法，主要是先計算兩個相鄰且不重疊像素之間的像素差值，然後根據此差值大小來決定藏密法。若差值小於預設之分界值時，則使用最低位元取代法來改變像素值；不然，則利用像素差值法來進行藏密。舉例來說，假設事先決定的分界值為 15，而最低取代的位元數為 3。當像素差值大於分界值時，則依像素差值法[2]進行藏密；若小於分界值時，則從隱藏資料位元序列中取出 6 位元數值（取代位元數  $3 \times 2 = 6$ ），並分別置入兩個相鄰且不重疊像素值的最低 3 位元，此時所得到的新像素值為  $f'(i, j)$  及  $f'(i, j+1)$ 。最後，再將此兩像素值分別進行數值 8 ( $2^3 = 8$ ) 的調整，得到最終的像素值  $f''(i, j)$  及  $f''(i, j+1)$ ，其算式如下：

if  $f'(i, j+1) \geq f'(i, j)$  then

$$f''(i, j+1) = f'(i, j+1) - 8 \quad \text{and}$$

$$f''(i, j) = f'(i, j) + 8$$

else  $f''(i, j+1) = f'(i, j+1) + 8$  and

$$f''(i, j) = f'(i, j) - 8 \quad (2)$$

由 H.-C. Wu 論文的實驗數據可知，當資訊隱藏量增加時，其影像品質就會大大地降低了。有鑑於此，在本論文中我們主要考慮如何在隱藏量增加時，同時降低對圖像品質的影響。

## 三、研究方法

在本文所提出的方法中，我們一樣是利

用修改兩個相鄰且不重疊像素  $f(i, j)$  及  $f(i, j+1)$  之間的像素差值為基礎。首先將整張影像以不重疊的兩個相鄰像素為單位來分組。對於每一組的兩個像素，仍舊先使用像素差值法[2]來改變兩像素值，當完成新像素值  $f'(i, j)$  及  $f'(i, j+1)$  的計算後，我們可再於  $f'(i, j+1)$  中多藏入 1 位元的隱藏資料。詳細之判斷方法說明如下。

假設現在正處理的分組像素差值大於 128 且欲藏入的資料值為  $(1111111)_2$  時，亦即新像素差值將被調整為 255，則略過增藏 1 位元資料的步驟，並繼續處理下一組兩個相鄰且不重疊像素。

令  $r$  為  $f'(i, j+1)$  以二進位表示時之最小位元，故  $r$  不是 '0' 就是 '1'。另外令接續要隱藏的 1 位元資料為  $u$ ，此時將  $r$  與  $u$  兩相比對，因為要隱藏的資料不是 '0' 就是 '1'，所以會產生以下 4 個情況： $(r, u) = (0,0)$ 、 $(0,1)$ 、 $(1,0)$  或  $(1,1)$ 。

當  $(r, u) = (0,0)$  或  $(1,1)$  時，代表  $r$  與  $u$  兩個值是相同的，所以就將  $r$  視為  $u$ ，也就是已經把要增加的 1 位元資料藏入於  $f'(i, j+1)$  當中了。現在，這組資料之隱藏動作已結束，接下來繼續處理下一組的兩個相鄰且不重疊像素。

當  $(r, u) = (0,1)$  時， $r$  值將被改變為 '1'，所以我們將  $f'(i, j+1)$  減 1，而  $f'(i, j+1)$  之二進位表示的最後 1 位元就成為 '1'，使得  $(r, u) = (1,1)$ 。此時的  $f(i, j)$  也需同步減 1，以維持固定的新像素差值，使影像品質不變。

當  $(r, u) = (1,0)$  時， $r$  值將被改變為 '0'，所以我們將  $f'(i, j+1)$  加 1，而  $f'(i, j+1)$  之二進位表示的最後 1 位元就成為 '0'，使得  $(r, u) = (0,0)$ 。此時的  $f(i, j)$  也需同步加 1，以維持固定新像素差值，使影像品質不變。

這裡要特別注意的是，若一開始執行完 PVD 法後的新像素差值被調整為 255，則略過增藏 1 位元資料的步驟。因為當新像素差值為 255，也就是兩像素為  $(0,255)$  或  $(255,0)$  時，如果  $f'(i, j+1) = 255$  而接續隱藏位元值為 '0' 時，則需將  $f'(i, j+1)$  加 1 而使得像素值超過 255，這是不允許的。同樣的，當  $f'(i, j+1) = 0$  而接續 1 位元值為 '1' 時，則需將  $f'(i, j+1)$  減 1 而使得像素值小於 0。所以當我們遇到 PVD 調整完的新像素差值為 255 時，就略過不增藏

1 位元資料。在抽取隱藏資料時，只要加入判斷式，當像素差值為 255 時，則不多讀取 1 位元隱藏資料，即可跳過此像素分組的步驟。

當完成多藏入 1 位元的隱藏資料後，我們也需顧及調整完的新像素值可能大於 255 或小於 0 的狀況。如果新像素值大於 255，則兩新像素值必需同時減 2，以使兩像素值皆小於或等於 255。另若新像素值小於 0 時，則兩像素值必需同時加 2，以使得兩像素值皆大於等於 0 為止。圖 2 為本研究方法之資料隱藏流程圖，請注意此方法一開始仍以像素差值(PVD)法來執行。

根據上述針對所提方法之解釋，茲將詳細的演算法步驟詳述如下：

Step 1) 輸入一張灰階影像，將整張影像的所有像素以不重疊的兩個相鄰像素為單位來分組。

Step 2) 若已藏完所有欲隱藏之資料位元，則演算法結束；否則，從尚未藏資料之分組取出一個，假設此組的兩個像素值為  $f(i, j)$  及  $f(i, j+1)$ 。利用 PVD 法[2]計算出  $f(i, j)$  及  $f(i, j+1)$  之差值  $d$ ：

$$d = |f(i, j) - f(i, j+1)| \quad (3)$$

參考表 1，找出差值  $d$  之對應區域可隱藏之位元數  $k$ ，並從藏密資料序列取出  $k$  位數後轉為 10 進位值  $w$ ，再將  $w$  加上該區域的最小值  $g$ ，其中  $p = w + g$ ，新像素差值  $d'$  可由下式算出：

$$d' = \left\lfloor \frac{|p-d|}{2} \right\rfloor \quad (4)$$

根據上述針對所提方法之解釋，茲將詳細的演算法步驟詳述如下：

Step 1) 輸入一張灰階影像，將整張影像的所有像素以不重疊的兩個相鄰像素為單位來分組。

Step 2) 若已藏完所有欲隱藏之資料位元，則演算法結束；否則，從尚未藏資料之分組取出一個，假設此組的兩個像素值為  $f(i, j)$  及  $f(i, j+1)$ 。利用 PVD 法[2]計算出  $f(i, j)$  及  $f(i, j+1)$  之差值  $d$ ：

$$d = |f(i, j) - f(i, j+1)|$$

參考表 1，找出差值  $d$  之對應區域可隱藏之位元數  $k$ ，並從藏密資料序列取出

$k$  位數後轉為 10 進位值  $w$ ，再將  $w$  加上該區域的最小值  $g$ ，其中  $p = w + g$ ，新像素差值  $d'$  可由下式算出：

$$d' = \left\lfloor \frac{|p-d|}{2} \right\rfloor$$

接下來參考差值  $d$  與  $d'$ ，使用 PVD 法[2]分成下列四種判斷之情況，來改變兩相鄰像素值，以完成  $k$  位數的隱藏，修改後的新像素值為  $f'(i, j)$  及  $f'(i, j+1)$ 。

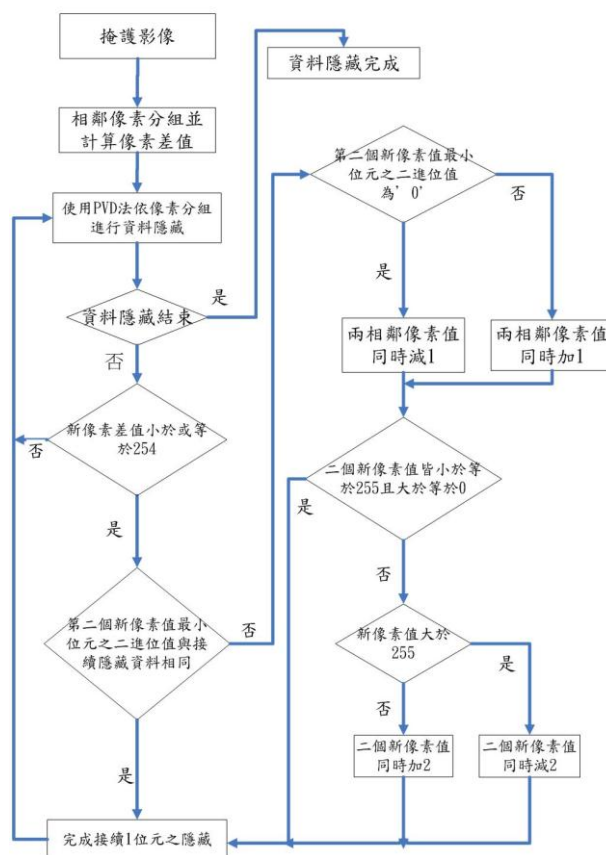


圖 2. 資料隱藏流程圖

**Case 1:** 假如第一個像素值大於或等於第二個像素值，且新像素差值大於或等於原來像素差值則處理如下：

if  $f(i, j) \geq f(i, j+1)$  and  $p \geq d$ ,  
 then  $f'(i, j) = f(i, j) + d'$ ,

$$f'(i, j+1) = f(i, j+1) - d'. \quad (5)$$

**Case 2:** 假如第一個像素值大於或等於第二個像素值，且新像素差值小於原來像素差值則處理如下：

$$\begin{aligned} \text{if } f(i, j) \geq f(i, j+1) \text{ and } p < d, \\ \text{then } f'(i, j) = f(i, j) - d', \\ f'(i, j+1) = f(i, j+1) + d'. \end{aligned} \quad (6)$$

**Case 3:** 假如第一個像素值小於第二個像素值，且新像素差值大於或等於原來像素差值則處理如下：

$$\begin{aligned} \text{if } f(i, j) < f(i, j+1) \text{ and } p \geq d, \\ \text{then } f'(i, j) = f(i, j) - d', \\ f'(i, j+1) = f(i, j+1) + d'. \end{aligned} \quad (7)$$

**Case 4:** 假如第一個像素值小於第二個像素值，且新像素差值小於原來像素差值則處理如下：

$$\begin{aligned} \text{if } f(i, j) < f(i, j+1) \text{ and } p < d, \\ \text{then } f'(i, j) = f(i, j) + d', \\ f'(i, j+1) = f(i, j+1) - d'. \end{aligned} \quad (8)$$

以 PVD 法[2]完成兩相鄰像素差值之資料隱藏後，我們可使用所提出之方法，於接下來的步驟在  $f'(i, j+1)$  中再多藏入 1 位元的資料。

Step 3)

**Case 1:** if  $p > 254$ ，就略過不增藏 1 位元資料，並接續下一組的兩相鄰像素之資料隱藏，回到 Step 2。

**Case 2:**

(1) 如果  $f'(i, j+1)$  最小位元之二進位值與接續隱藏之資料位元相同時，則已自動完成增加隱藏 1 位元資料，即  $f''(i, j) = f'(i, j)$  與  $f''(i, j+1) = f'(i, j+1)$ ，回到 Step 2。

(2) 如果  $f'(i, j+1)$  最小位元之二進位值與接續隱藏之資料位元不同時，則需依照下列兩種情況分別處理：

(a) 若  $f'(i, j+1)$  最小位元之二進位值為 '1'，且接續隱藏的 1 位元資料為 '0' 時：

$$\begin{aligned} f''(i, j) &= f'(i, j) + 1, \\ f''(i, j+1) &= f'(i, j+1) + 1 \end{aligned} \quad (9)$$

(b) 若  $f'(i, j+1)$  最小位元之二進位值為 '0'，且接續隱藏 1 位元資料為 '1' 時：

$$\begin{aligned} f''(i, j) &= f'(i, j) - 1 \\ f''(i, j+1) &= f'(i, j+1) - 1 \end{aligned} \quad (10)$$

Step 4) 假如調整完分組的兩新像素值皆小於等於 255 及大於等於 0 時，則回到 Step 2。否則依照下列兩種狀況處理：

**Case 1:** 假如調整完分組任一新像素值大於 255 時，則兩個新像素值同時減 2：

$$\begin{aligned} \text{if } f''(i, j) > 255 \text{ 或 } f''(i, j+1) > 255, \\ \text{then } f''(i, j) &= f''(i, j) - 2, \\ f''(i, j+1) &= f''(i, j+1) - 2. \end{aligned} \quad (11)$$

直到  $f''(i, j) \leq 255$  且  $f''(i, j+1) \leq 255$ ，回到 Step 2。

**Case 2:** 假如調整完分組任一新像素值小於 0 時，則兩個新像素值同時加 2：

$$\begin{aligned} \text{if } f''(i, j) < 0 \text{ 或 } f''(i, j+1) < 0, \\ \text{then } f''(i, j) &= f''(i, j) + 2, \\ f''(i, j+1) &= f''(i, j+1) + 2. \end{aligned} \quad (12)$$

直到  $f''(i, j) \geq 0$  且  $f''(i, j+1) \geq 0$

回到 Step 2。

演算至此，我們的方法已經比 PVD 多隱藏了一個位元。

圖 3 為本研究方法之抽取隱藏資料流程圖，首先將偽裝影像以不重疊的兩個相鄰像素為單位來分組，然後計算像素差值，以 PVD 抽取法抽取隱藏資料。完成後再判斷原像素差值是否小於等於 254，如原像素差值小於等於 254 則可再抽取一位元隱藏資料。當第二像素值為奇數時，則抽取一位元隱藏資料為 '1'；當第二像素值為偶數時，則抽取一位元隱藏資料為 '0'。如原像素差值大於 254，則本組無續抽取之隱藏資料，並移至下一分組進行隱藏資料抽取。

舉一個範例來說明，假設一組兩個相鄰且不重疊之像素值分別為 28 及 50，接續隱藏的資料序列為 1010101101...。圖 4 為此範例資料隱藏之示意圖。

在 Step 2 中，由運算式(3)計算出  $d=50-28=22$ ，從表 1 得知 25 所對應的可隱藏資料位元數為  $k=4$ ，即表示可藏的資料量為 4 bits；將隱藏資料 1010 轉為 10 進位值後為 10，接著由運算式(4)計算出  $p=10+16=26$ ， $d'=2$ 。因為第一個像素值小於第二個像素值，且新像素差值大於原來像素差值，由運算式(7)計算出

$$f'(i, j) = f(i, j) - d' = 28 - 2 = 26$$

$$f'(i, j + 1) = f(i, j + 1) + d' = 50 + 2 = 52$$

在 Step 3 中，因  $f'(i, j + 1)$  之值為 52，其二進位值最小 1 位元值為 '0'，而接續要隱藏的 1 位元資料為 '1'，由運算式(10)可算出

$$f''(i, j) = f'(i, j) - 1 = 26 - 1 = 25$$

$$f''(i, j + 1) = f'(i, j + 1) - 1 = 52 - 1 = 51$$

在 Step 4 中，因此時兩新像素值皆介於 0 與 255 之間，所以結束了一組像素之資料隱藏，接下來回到 Step 2，進行下一組兩相鄰像素的資料隱藏，此時剩下的接續隱藏資料為 011101...。請注意此時的像素差值與 PVD 法調整完的差值相同，但已比 PVD 法多藏入了一位元。故我們的方法可同時保持影像品質與增加資料隱藏容量。

另針對此範例之隱藏資料抽取動作說明如下。延續前段敘述的資料隱藏結果，偽裝影像一組兩個相鄰且不重疊之像素值分別為 25 及 51。首先所計算出的像素差值為  $51-25=26$ ，因為 26 介於 16 與 31 之間，從表 1 得知此差值落於第 3 區域。接下來將 26 減去第 3 區域之最小值 16 即可得到  $26-16=10$ 。10 以二進位制表示為 '1010'，所以 '1010' 為先經由 PVD 法抽取出之隱藏資料。

因適才計算出來的像素差值為 26，而 26 的數值小於 254，所以根據我們的方法，可再多抽出一位元的隱藏資料。由於此時的第二像素值為 51，而 51 為一奇數，故所抽取出來的一位元隱藏資料為 '1'。最後由此像素分組總共抽取出來的隱藏資料為五個位元，即為 '1010' 與 '1'，所以這個分組的隱藏資料

為 '10101'。依照圖 3 所示的資料抽取流程圖，我們可其餘分組的資料抽取工作。

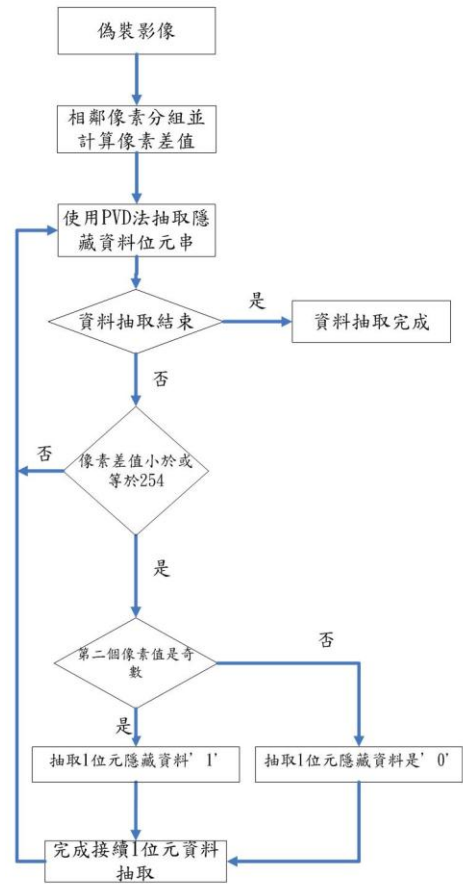


圖 3. 資料抽取流程圖

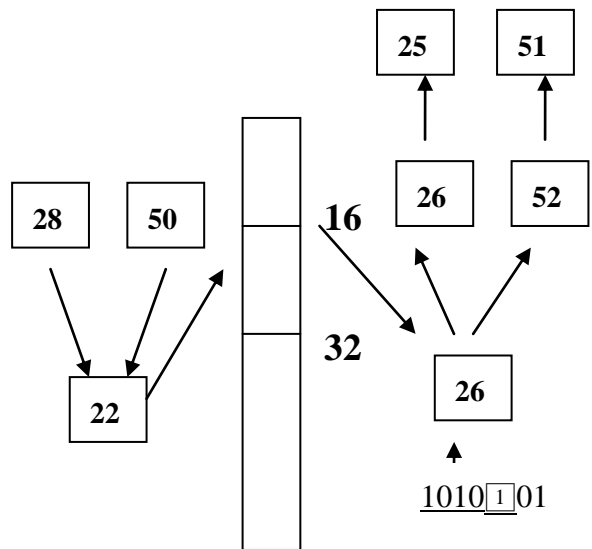


圖 4. 範例演算示意圖

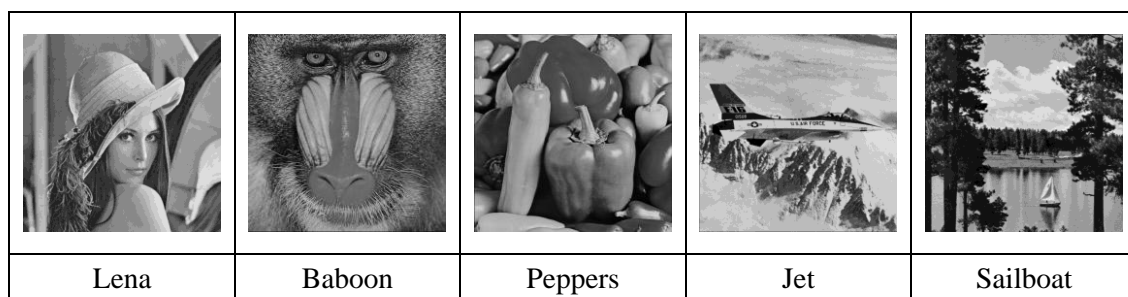


圖 5. 灰階 512x512

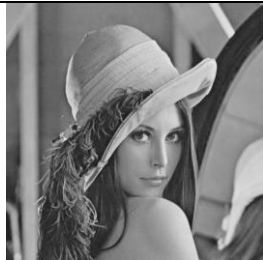
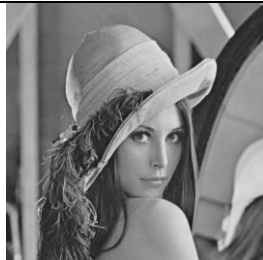
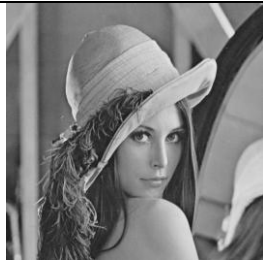

			
Lena(灰階)原圖	PVD 方法	H.-C. Wu 方法(2bits)	我們的方法(1bit)
與原圖比較 PSNR 值 (db)	41.0675	40.9384	40.7183
隱藏容量(Bytes)	51219	63654	67603

圖 6. 相同影像品質的隱藏容量比較

表 2. PVD 方法與本方法比較

Cover images (512*512)	Da-Chun Wu's PVD 方法		本方法	
	Capacity (bytes)	PSNR (db)	Capacity (bytes)	PSNR (db)
Lena	51219	41.0927	67603	40.6813
Baboon	57521	36.5592	73905	36.4093
Peppers	50916	40.5583	67300	40.1805
F-16	51550	39.9838	67934	39.6634
Sailboat	52779	39.3369	69163	39.0543

表 3. H-C Wu 方法與本方法比較

Cover images (512*512)	H.-C. Wu 方法		本方法	
	Capacity (bytes)	PSNR (db)	Capacity (bytes)	PSNR (db)
Lena	95754	37.1131	100371	37.8962
Baboon	89750	35.0103	106672	35.1468
Peppers	96187	36.8186	100065	37.5932
F-16	96197	36.6526	100702	37.3295
Sailboat	94184	36.3920	101930	36.9577

#### 四、實驗結果及討論

在演算法測試之實驗階段，我們使用 MATLAB 軟體為工具[19]，電腦硬體為 Intel(R) Core(TM)2 Quad CPU Q8400，1.75GB 的 RAM。如圖 5 所示，測試圖像為五張尺寸為 512×512 的灰階影像 (Lena、Baboon、Peppers、Jet、sailboat)。我們所提方法的目標是提高資料隱藏量及同時保持影像的品質不變，所採用的隱藏資料為亂數序列，所有實驗結果的數值都是在執行 1000 次後所取的平均值。使用 PVD 方法[2]時，我們採用寬度為 8、8、16、32、64 及 128 的分區表。藏密影像品質的評估標準以 PSNR(Peak Signal to Noise Ratio)值來計算，單位為 dB。PSNR 值以 30 以上為容許範圍，40 以上的值則幾乎與原圖無視覺差異。

如圖 6 所示，在維持幾近相同的影像品質 (40<PSNR<41)前提下，實驗結果顯示我們所提的方法比 PVD 法[2]能多藏入 16384 bytes，比 H.-C. Wu 方法[3]多藏入 3949 bytes，請注意此處的 H.-C. Wu 方法已使用了兩個 LSB 位元。

將我們前述增藏 LSB 1 bit 的方法稍加修



改,即可延伸至增藏 2 bit 或 3 bit。因增藏 4 bit 以上之影像品質已無法接受,故不在本論文中討論。如前面所述,增加 1bit 新像素差值需小於等於 254,如引用相同邏輯再提高資料隱藏量時我們可改良為增加 2 bits,但此時新像素差值需小於等於 252,同理亦可改良為增加 3 bits,但新像素差值需小於等於 248。如新像素差值不屬於此範圍,則不在此分組新增隱藏資料,只完成 PVD 法即可。

經過 5 張圖像各 1000 次亂數資料的隱藏,可得知每次對同一張圖片所隱藏的資料量幾乎是相同的。所不同的是 PSNR 值,因為每次執行的隱藏資料是亂數序列,所以對圖像的品質影響就有些微不同。我們在實驗中的比較皆是使用同樣的亂數資料去做不同方法的計算。

因為我們所提方法的目標是在改良 PVD 方法[2],希望在進行資料隱藏後,能保持相同影像品質並增加藏密容量。所以接下來我們就針對 PVD 方法[2]與我們的方法(增加 1bit)來比較。如表 2 所示,可以很清楚的看出,我們的方法之平均隱藏容量比 PVD 方法多增加約 30%,但 PSNR 值只降低約 0.4 dB,人的視覺對圖像 PSNR 值降低 0.4 dB 幾乎是感覺不到它的差異性。

最後,我們要進行的實驗是使用與表 2 同樣的亂數資料,將 H.-C. Wu 方法(代位元數為 3 位元)[3]與我們的方法(增加 3bits)進行比較。整理的實驗結果如表 3 所示,針對 5 張圖像個別所執行的實驗結果來看,不管是在資料隱藏容量或是 PSNR 值方面,我們的方法所表現之效能皆優於 H.-C. Wu 方法[3]。

## 五、結 論

資料隱藏技術所要考量的兩項重要因素,第一是資料隱藏容量,另一是偽裝影像的完整性及品質,通常這兩項是互相矛盾且無法同時達成的。空間域的藏密技術主要是直接以小幅度改變掩護影像的像素值來達成隱藏秘密資訊的目的。本論文主要在討論空間域藏密技術的像素差值法及最低位元取代法,期望能在藏入最大容量的資料時,同時顧全影像的品質。

Da-Chun Wu 等[2]所提出的 PVD[20]資料隱藏法係利用像素之間的差值量化方式來隱

藏資料。H.-C. Wu 等[3]開發的像素差值和最低位元取代合併法,可以增加資料隱藏容量,但同時也把影像品質降低了。本文所提出的方法係將 PVD 法及最低有效位元替換方法整合在一起,不但可隱藏更多的資料,同時保留了影像品質,這個優點已透過本文的實驗結果得到驗證。未來的研究方向將以本研究成果為基礎,朝向與其他空間域的藏密技術進行整合。

## 參考文獻

- [1] Anderson, R. J. and Petitcolas, F. A. P., "On the Limit of Steganography," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 474-481, May 1998.
- [2] Wu, D. C. and Tsai, W. H., "A Steganographic Method for Images by Pixel-value Differencing," Pattern Recognition Letters, 24(9-10), pp. 1613-1626, June 2003.
- [3] 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, Vol. 152, No. 5, pp. 611-615, 2005.
- [4] Chang, K. C., Chang, C. P., Huang P. S., and Tu, T. M., "A Novel Image Steganographic Method Using Tri-way Pixel-value Differencing," Journal of Multimedia, Vol. 3, No. 2, pp. 37-44, June 2008.
- [5] 連國珍, "數位影像處理 MATLAB" 儒林圖書, 第四章, 4-1 - 4-57, 2009。
- [6] 鐘國亮, "影像處理與電腦視覺導論" 東華書局, 第二章, 2009。
- [7] Chan, C. K. and Cheng, L. M., "Hiding Data in Images by Simple LSB Substitution," Pattern Recognition, 37(3), pp. 469-474, 2004.
- [8] 婁德權, "藏密學發展現況", 國防大學中正理工學院電機工程系, 資通安全專論 T95010, 2006 年 09 月 06 日。
- [9] Westfeld, A., "F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis," Proc. 4th Int'l Workshop Information Hiding, Springer-Verlag, 2001, Vol. 2137, pp. 289-302.

- [10] Huang, P. S., Chiang, C. S., Chang, C. P., and Tu, T. M., "Robust Spatial Watermarking Technique for Colour Images Via Direct Saturation Adjustment," *IEE Proc.-Vis. Image Signal Process.*, Vol. 152, No. 5, pp. 561-574, October 2005.
- [11] Wang, Y. and Pearmain, A., "Blind Image Data Hiding Based on Self Reference," *Pattern Recognition Letters*, 25(15), pp. 1681-1689, 2004.
- [12] 蔡耀德, "利用最佳區塊配對的高容量影像隱藏法", 銘傳大學資訊傳播工程學系, 碩士學位論文, 2005年6月。
- [13] Wang, R. Z. and Tsai, Y. D., "An Image-hiding Method with High Hiding Capacity Based on Best-Block Matching and K-means Clustering," *Pattern Recognition Letters*, 40(2), pp. 398-409, February 2007.
- [14] Lou, D. C., Wu, N. I., Wang, C. M., Lin, Z. H., and Tsai, C. S., "A Novel Adaptive Steganography Based on Local Complexity and Human Vision Sensitivity," *Journal of Systems and Software*, Vol. 83, No. 7, pp.1236-1248, 2010.
- [15] Yang, C. H., Weng, C. Y., and Wang, S. J., "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain systems," *IEEE Transactions on Information Forensic and Security*, Vol. 3, No. 3, September, pp. 488-497, 2008.
- [16] 施明宏、劉震昌, "對 Pixel Value Differencing 影像中資料隱藏法的改進", 民生電子暨信號處理研討會, 2005。
- [17] Yang, C. H., Wang, S. J., and Weng, C. Y., "Analyses of Pixel-Value-Differencing Schemes with LSB Replacement in Stegonagraphy," *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSp 2007*, Vol. 1, pp. 445-448, November 2007.
- [18] Chang, C. C. and Tseng, H. W., "A Steganographic Method for Digital Images Using Side Match," *Pattern Recognition Letters*, 25(12), pp. 1431-1437, September, 2004.
- [19] 張智星, "MATLAB 程式設計與應用" 清蔚科技, 2000。
- [20] Wang, C. M., Wu, N. I., Tsai, C. S. and Hwang, M. S., "A High Quality Steganographic Method with Pixel-value Differencing and Modulus Function," *Journal of Systems and Software*, Vol. 81, No. 1, pp.150-158, 2010.