# 結合 LSB 和改良式 PVD 藏入法的資訊隱藏

曾顯文 [1]　　冷輝世 [12]　　劉信甫 [1]
[1] 朝陽科技大學資訊管理系　[2] 國立彰化師範大學數學系　[1] 朝陽科技大學資訊管理系
hwtseng@cyut.edu.tw　lenghs@cc.ncue.edu.tw　s10314615@cyut.edu.tw

## 摘要

本研究提出結合 LSB 和改良式 PVD 藏入法的資訊隱藏。首先將原始影像分成5×5不重疊的區塊，並選擇中央的像素作為基礎像素；然後將區塊內其它像素分成相對於基礎像素的內層像素及外層像素。根據像素與像素之間的距離作為分類的依據，分別針對內層像素與外層像素使用 LSB 或改良式 PVD 藏入法，藏入法取決於藏入機密訊息後選擇均方差較小的方法進行藏入。實驗結果顯示本研究方法能夠在高藏入量的情況下同時保有良好的偽裝影像品質。

**關鍵詞**：LSB 藏入法、改良式 PVD 藏入法、資訊隱藏

## Abstract

This paper presents a data-hiding method based on least-significant-bit (LSB) substitution and An adaptive steganographic method for grayscale images. The proposed method partitions the cover image into 5 × 5 non-overlapping blocks and select the central pixel as the base pixel. Next, the other pixels in the block are classified into inner pixels and outer pixels. Then, the secret information is embedded into the inner pixels and outer pixels by using LSB or An adaptive steganographic with the minimum MSE. The experimental results show the proposed method can embed the secret information into the cover image while preserving the image quality.

**Keywords**: Data hiding, Steganography, Least-significant-bit (LSB) substitution, Adaptive steganographic

## 1.前言

由於網路科技的迅速發展，許多人透過網際網路進行資料的傳遞及交換，因此大量的數位資料在網路空間被廣泛地散佈及應用。然而在網路上進行資料的傳遞並非是安全的，使得數位資料容易遭到不法的第三者隨意竄改及竊取。因此為了避免這類的問題發生，有學者提出資訊隱藏的概念，將機密訊息藏匿於影像、聲音、文字…等等的多媒體中，接著將藏有機密訊息的偽裝媒體透過網際網路進行傳遞，以躲避不法第三者的攻擊。

一個好的資訊隱藏資訊技術必須滿足安全性、不可察覺性及高資訊負載量三個條件[1]。安全性是指除了合法的參與者之外，其他人沒有辦法從偽裝媒體中取出隱藏的機密訊息，不可察覺性是指偽裝媒體的品質必需在一定的水準之上，而高資訊負載量則是指在一定的偽裝媒體品質要求前提下，盡可能提高資訊的隱藏量，以提高資料傳送的利用率。資訊隱藏可依照處理方式的不同，分為空間域、頻率域與壓縮域三種方式，其中空間域為最常見的隱藏方式。本研究主要是針對空間域裡的最低位元(Least-Significant-Bit，以下簡稱 LSB)藏入法[3]及改良式PVD藏入法[4]加以延伸應用，根據像素與像素之間的距離作為分類的依據，分別針對內層像素與外層像素使用 LSB 或改良式 PVD 藏入法並選擇均方差較小的方法進行藏入，因此可以在高藏入量的情況下同時保有良好的偽裝影像品質。

## 2.文獻探討

本章將分別介紹 LSB 藏入法、改良式 PVD 藏入法及其他兩個結合 LSB 藏入法與 PVD 藏入法的資訊隱藏法。

### 2.1 LSB藏入法

Chan及Cheng學者[3](2004)提出LSB藏入法(OPAP)，將機密訊息取代較低位元，達到高藏量及低失真度的資訊隱藏效果。首先將灰階影像中的目標像素轉換成二進制，再從機密訊息串當中取出*k*個位元的機密訊息，取代目標像素中後面的*k*個位元。例如：目標像素為110，欲藏入3個位元的機密訊息$(010)_2$。首先，目標像素$110 = (01101\underline{110})_2$，機密訊息為$(010)_2$；然後將機密訊息取代目標像素的後面3個位元，得到偽裝像素值$106 = (01101\underline{010})_2$。在取出機密訊息的過程中，只要將偽裝像素值轉成二進制並取出最後3個位元$(010)_2$，即可得到

藏入的機密訊息。

### 2.2 改良式PVD藏入法

Wu及Tsai學者[8](2003)提出PVD藏入法，利用相鄰像素差值參照區間量表決定欲藏入的機密訊息長度。Hsiao及Chang學者[4](2011)提出改良式的PVD藏入法，該方法使用預測像素與目標像素的差值計算出多個不同長度的候選偽裝像素值，並將這些偽裝像素值減去原始像素值再取絕對值得到誤差值，並選擇誤差值最小的偽裝像素值作為最後的結果。本研究則是以這個方法為基礎加以延伸應用。以下介紹使用的變數的定義：

$x_{i,j}$ 為原始影像中第$i$列第$j$行的像素值

$x'_{i,j}$ 為偽裝影像中第$i$列第$j$行的像素值

$p_{i,j}$ 為第$i$列第$j$行的預測像素值

$p_{i,j} = (x'_{i-1,j} + x'_{i,j-1})/2$

$b$為機密訊息字串$b = b_0b_1b_2...b_k$

$b(s,n)$為機密位元串中第$s$個位元到第$(n-1)$個位元所形成的位元串，也就是說$b(s,n) = b_sb_{s+1}...b_{n-1}$

$b(s,n)_{10}$ 為$b(s,n)$的十進制表示法

$al$為用來規定機密訊息所藏的最小位元量為log2 $al$個位元，$al$須為2的正整數次方。

藏入機密訊息串的步驟如下：

1. 使用Chang與Tseng學者[9]的邊緣吻合法預測，可以得到預測像素值$p_{i,j} = (x'_{i-1,j} + x'_{i,j-1})/2$。
2. 令$d' = 2^n + b(s,n)_{10} - al$ 。
3. 取不同的$n$值，$n$ = 1,2,3…去計算$x'_{i,j}$：若$p_{i,j} < x_{i,j}$，則$x'_{i,j} = p_{i,j} + d' = p_{i,j} + 2^n + b(s,n)_{10} - al$；若 $p_{i,j} \geq x_{i,j}$，則$x'_{i,j} = p_{i,j} - d' = p_{i,j} - 2^n - b(s,n)_{10} + al$。接著算出 $d = |x_{i,j} - x'_{i,j}|$，並找出能使$d$為最小值的$n$值，且令此$n$值為$N$，此$N$值即是我們要藏入的機密訊息長度。
4. 利用$N$值計算出的$x'_{i,j}$即為最後的偽裝像素值若 $p_{i,j} < x_{i,j}$，$x'_{i,j} = p_{i,j} + d' = p_{i,j} + 2^N + b(s,N)_{10} - al$；若 $p_{i,j} \geq x_{i,j}$，$x'_{i,j} = p_{i,j} - d' = p_{i,j} - 2^N - b(s,N)_{10} + al$。

取出機密訊息串的步驟如下：

1. 首先我們可以從偽裝影像得知 $x'_{i,j}$ ，並利用 $p_{i,j} = (x'_{i-1,j} + x'_{i,j-1})/2$ 計算出 $p_{i,j}$，於是可以算出 $d' = |x'_{i,j} - p_{i,j}|$。
2. 根據藏入步驟 2.：$d' = 2^N + b(s,N)_{10} - al$ $\Rightarrow d' + al = 2^N + b(s,N)_{10}$。
3. 因為 $2^N + b(s,N)_{10} < 2^{N+1}$，因此 $N = \lfloor \log2(d' + al) \rfloor$。
4. $b(s,N)_{10} = d' + al - 2^N$，且已知 $N$，則可計算出 $b(s,N)$

舉例如下：

| | |
|---|---|
| 120 | 130 |
| 140 | 155 |

**圖 1 原始影像部分區塊**

假設機密訊息串$b = (01101011)_2$，令最少藏一個位元，所以$al = 2^1 = 2$，$p_{i,j} = (130+140)/2 = 135$，且 $p_{i,j} < x_{i,j}$。

**表 1 不同$n$值對應的表格**

| $n$ | $d'$ | $x'_{i,j}$ | $d$ |
|---|---|---|---|
| 1 | 0 | 135 | 20 |
| 2 | 3 | 138 | 17 |
| 3 | 9 | 144 | 11 |
| 4 | 20 | 155 | 0 |

由表 1可知當$n = 4$的時候，$d$會有最小值0，因此取$N = 4$為所藏入機密訊息的長度。$x'_{i,j} = p_{i,j} + d' = p_{i,j} + 2^N + b(0,N-1)_{10} - 2 = 135 + 16 + 6 - 2 = 155$。155即為最後的偽裝像素值。

取出機密訊息串的步驟：

當得知偽裝像素值$x'_{i,j} = 155$與預測像素值$p_{i,j} = 135$之後，$d' = |x'_{i,j} - p_{i,j}| = |155 - 135| = 20$，$N = \lfloor \log2(d' + al) \rfloor = \lfloor \log2(20 + 2) \rfloor = 4$，$b(s,N-1)_{10} = d' + al - 2^N = 20 + 2 - 2^4 = 6$。因此得到機密訊息$b(s,N-1) = (0110)_2$。

### 2.3 其他兩個結合 LSB 藏入法與 PVD 藏入法的資訊隱藏法

M.Khodaei 與 K.Faez 學者[5](2012)提出的相關的研究。首先定義兩種區間量表如圖 2，圖 2 的上方重視影像品質，每個區間分別能藏入 3、3、3、4、4 位元的機密訊息。圖 2 的下方重視機密訊息藏入量，每個區間分別能藏入 3、3、4、5、6 位元的機密訊息。該方法是先將影像分成 1×3 不重疊的區塊，並將每個區塊中間的像素作為基礎像素，利用 LSB 藏入法藏入 $k$ 個位元的機密訊息後，與左右相鄰像素組成兩個像素對，接著計算每一個像素對的像素誤差值，對照區間量表修改像素值進行藏入。

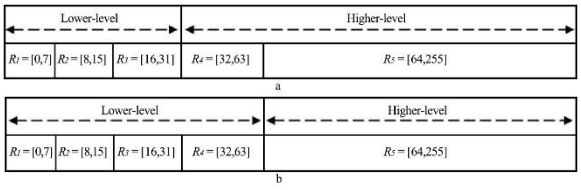



**圖 2 [5]的區間量表**

Avinash K.Gulve 與 Madhuri S. Joshi 學者[6](2015)年亦提出相關的研究。首先將影像分成 2×3 不重疊的區塊，並將區塊第一列中央的像素定義為基礎像素 $P_c$。利用 LSB 藏入法將 3 個位元的機密訊息藏入基礎像素之後，計算基礎像素與其他 5 個像素的誤差值。假設這些誤差值分別為 $d_0$、$d_1$、$d_2$、$d_3$、$d_4$，將這些誤差值取絕對值之後，對照[7] 所提出的區間量表，獲得每個誤差值能藏入的機密訊息位元數 $t_i$。為了平均分配每個誤差值的藏入量，將每個誤差值能藏入的機密訊息位元數加總後取平均值，計算公式如下：

$$avg = \left\lfloor \left( \frac{\sum_{i=0}^{4} t_i}{5} \right) \right\rfloor \quad (1)$$

接著利用下列公式計算出修改後的誤差值：

$$dl_i = d_i \bmod 2^{avg} \quad (2)$$

再計算原始誤差值與修改後誤差值的位移量：

$$OD_i = |d_i| - |dl_i| \quad (3)$$

以修改後的誤差值對應區間量表，找出所屬區間的最小值 $li$ 及可藏入的機密訊息位元數，並取出相同位元數的機密訊息 $bi$，將其轉換成十進制後藏入得到新的誤差值$\mathrm{d}'_i$：

$$\begin{cases} d'_i = OD_i + \mathrm{l}_i + \mathrm{b}_i & if\ \mathrm{d}'_i \geq 0 \\ d'_i = -(OD_i + \mathrm{l}_i + \mathrm{b}_i) & if\ \mathrm{d}'_i < 0 \end{cases} \quad (4)$$

將新的誤差值減去原始的誤差值計算出 $m_i$：

$$m_i = d'_i - d_i \quad (5)$$

利用下列公式算出 5 組像素對的值：

$$(P'_c, P'_i) = \left( P_c - \left\lceil \frac{m_i}{2} \right\rceil, P_i + \left\lfloor \frac{m_i}{2} \right\rfloor \right) \quad (6)$$

因為基礎像素值只能有一個，所以取 $|m_i|$ 最小的值所算出來的基礎像素為基準，而其他像素值再以這個基礎像素作修改，確保每個像素對修改前後的誤差值是相同的。最後將算出來的基礎像素減去一開始利用 LSB 藏入法藏入 3 個位元機密訊息的基礎像素值，計算出誤差值，並將其他 5 個像素減去此誤差值，得到最後的偽裝像素值。

## 3.研究方法

本研究所提出的方法是藉由影像內各像素間的距離不相同的特性，選擇合適的方法進行機密訊息的藏入。將灰階影像分成 5×5 不重疊的區塊(如圖 3)。將位於每個區塊中央的像素作為基礎像素，並將基礎像素外第一層的像素分類為內層像素，而將基礎像素外第二層的像素分類為外層像素。


**圖 3 影像像素部分區塊圖**

### 3.1 藏入機密訊息串的步驟

藏入機密訊息串的步驟如下：

1. 將基礎像素 $x_{i,j}$ 轉成二進制，取出前面 $8-k$ 個位元，再將其轉成十進制，得到修改後的基礎像素值 $x'_{i,j}$。$k$ 為預設要使用 LSB 藏入法藏入的位元數。
2. 從機密訊息串中取出 $k$ 個位元，使用 LSB 藏入法藏入至內層的所有像素，並將藏入後的偽裝像素值記錄下來。
3. 使用改良式 PVD 藏入法，設定 $al$ 值，並以 $x'_{i,j}$ 作為預測像素，分別將機密訊息藏入至內層的所有像素，並將藏入後的偽裝像素值記錄下來。
4. 分別計算偽裝像素值與原始像素值的均方差 $MSE_{LSB\_i}$、偽裝像素值與原始像素值的均方差 $MSE_{JND\_i}$，若 $MSE_{LSB\_i} < MSE_{JND\_i}$，內層像素均以 LSB 藏入法藏入機密訊息；若 $MSE_{LSB\_i} \geq MSE_{JND\_i}$，則內層像素均以改良式 PVD 藏入法藏入機密訊息。

$$MSE = \left(\frac{1}{x}\right) \sum_{i=1}^{x} (CI_i - SI_i)^2$$

其中 x 為像素個數，$\mathrm{CI_i}$及$\mathrm{SI_i}$為原始影像像素值及偽裝影像像素值。

5. 接著重複 2.和 3.，將機密訊息藏入至外層的所有像素，並將使用兩種方法藏入後的偽裝像素值記錄下來。
6. 分別計算使用兩種方法藏入外層像素後的均方差 $MSE_{LSB\_o}$、$MSE_{JND\_o}$，若 $MSE_{LSB\_o} < MSE_{JND\_o}$，外層像素均以 LSB 藏入法藏入機密訊息；若 $MSE_{LSB\_o} \geq MSE_{JND\_o}$，則外層像素均以改良式 PVD 藏入法藏入機密訊息。
7. 從機密訊息串中取出 $k-2$ 個位元，並使用 LSB 藏入法取代二進制 $x'_{i,j}$ 中後面的 $k-2$ 個位元(除了最後 2 個位元之外)，並依照此區塊中內層像素及外層像素所使用的資訊隱藏法，修改二進制 $x'_{i,j}$ 的最後

2 個位元，得到最後的偽裝基礎像素 $x''_{i,j}$ ，如表 2 所示：

**表 2 使用不同資訊隱藏法組合的對應表格**

| 修改結果 | 內層像素 | 外層像素 |
|---|---|---|
| 00 | LSB | LSB |
| 01 | LSB | 改良式 PVD |
| 10 | 改良式 PVD | LSB |
| 11 | 改良式 PVD | 改良式 PVD |

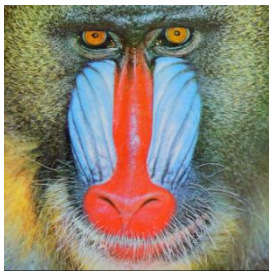
### 3.2 取出機密訊息串的步驟

1. 將偽裝基礎像素 $x''_{i,j}$ 轉成二進制，其中後面的 $k-2$ 個位元(除了最後 2 個位元之外)即是當初藏入基礎像素中的機密訊息，並從最後 2 個位元及表 2 得知，此區塊的內層像素及外層像素分別是用何種資訊隱藏法藏入機密訊息，另取出前面 $8-k$ 個位元，再將其轉成十進制，得到修改後的偽裝基礎像素 $x'_{i,j}$ 。
2. 將內層偽裝像素依當初所使用的資訊隱藏法取出機密訊息。若是使用 LSB 藏入法，則將內層偽裝像素轉成二進制，最後 $k$ 個位元即是機密訊息；若是使用改良式 PVD 藏入法，則使用 $x'_{i,j}$ 作為預測像素值，以及藏入時所設定的 $al$ 值，取出機密訊息。
3. 重複 2.，取出外層偽裝像素中的機密訊息。

## 4.實驗結果

本研究在實驗中使用的原始影像包含 Lena、Baboon、Pepper、Jet 四張彩色影像，並將這四張影像轉換成灰階影像進行藏入，其影像大小為 512×512，如圖 3 所示：


Lena


Baboon


Peppers


Jet

**圖 4 實驗所使用影像**

一般最常用來評估偽裝影像品質的指標為 MSE(Mean Square Error)與 PSNR(Peak Signal to Noise Ratio)，其公式定義如下：

$$MSE = \left(\frac{1}{h \times w}\right)\sum_{i=1}^{h}\sum_{j=1}^{w}\left(x_{i,j} - x'_{i,j}\right)^2 \quad (7)$$

$$PSNR = 10 \times log_{10}\frac{255^2}{MSE} \quad (8)$$

其中 $h$ 與 $w$ 分別代表原始影像中的高與寬，$x_{i,j}$ 與 $x'_{i,j}$ 分別代表原始影像與偽裝影像中第 $i$ 列第 $j$ 行的像素值。

在進行機密訊息藏入時將內層像素分為一組，外層像素分為一組，目的是為了將這些像素依照與基礎像素的距離分類。而當預設 $k$ 值等於 4 時，代表我們欲使用 LSB 藏入法藏入 4 個位元的機密訊息，此時若將 $al$ 值設定為 8，代表我們欲使用改良式 PVD 藏入法至少藏入 3 個位元的機密訊息，而之後會根據算出來偽裝像素值與原始像素值的誤差值，選擇最小的當作偽裝像素值，因此平均可藏入 3 至 5 個位元的機密訊息。再透過計算使用兩種資訊隱藏方法藏入後的均方差，選擇均方差較小的方法進行藏入，以確保所使用的資訊隱藏方法造成的失真度較低，藉以保持良好的影像品質。

從表 3 的實驗結果中顯示，我們所提出的方法平均藏量高出[5]所提出的方法 41447 個位元，而在影像品質部分平均則高出 2.17dB，這是因為[5]所提出的方法是使用原始 PVD 藏入法進行藏入，並沒有根據機密訊息的長度做最佳化的調整，所以在影像品質及藏入量的部分沒有比改良式 PVD 藏入法來的好。在與[6]所提出的方法比較時，雖然影像品質的部分平均少了 2.51dB，但是在藏量部分平均卻高出了 166993 個位元，由此可看出本篇研究所提出的方法能在藏入大量的機密訊息之後，還能使偽裝影像的品質保持一定的水準之上。而我們也發現由於[6]所提出的方法會根據 LSB 藏入後的結果調整最後的偽裝像素值，所以在一些較複雜的影像(例如 Baboon)會有溢位的情況發生。另外本研究方法另外應用在分成 3×3

區塊的原始影像上，而與分成 5×5 區塊的實驗數據比較，可以看出若是只使用 3×3 的區塊進行藏入，效果沒有使用 5×5 的區塊來得好，這也說明了根據像素間的距離來做分類，並選擇合適方法進行藏入的效果是較佳的。

## 5.結論

本篇研究所提出的方法，是先將原始影像分成 5×5 不重疊的區塊大小，選定中央的像素作為基礎像素，並將區塊內的像素依照與基礎像素的距離，分為內層像素及外層像素。之後分別將內層像素及外層像素使用兩種不同的資訊隱藏方法進行機密訊息的藏入，計算藏入後的均方差，選擇對影像失真度較小的方法進行藏入。為了能在取出機密訊息時，能夠辨別內層像素及外層像素分別使用何種方法藏入，我們會利用基礎像素的最後兩個位元進行記錄，確保能夠使用相對應的資訊隱藏方法取出機密訊息。雖然這樣會犧牲掉基礎像素些許的藏入量，但也因此能夠在藏入大量機密訊息的同時，保持良好的影像品質。

**參考文獻**


[1] 呂慈純、陸哲明、張真誠，***多媒體安全技術***，全華圖書股份有限公司，2007。

[2] 冷輝世、張維剛，"鄰近像素標準差與 JND 值關係的研究"，***2013 第七屆資訊國際科技研討會論文集***，2013。

[3] C.K. Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution," ***Pattern Recognition***, Vol. 37, Issue 3, pp.469-474, 2004.

[4] J.Y. Hsiao, "An adaptive steganographic method based on the measurement of just noticeable distortion profile," ***Image and Vision Computing***, Vol. 29, pp.155-166, 2011.

[5] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," ***IET Image Processing***, Vol. 6, pp.677-686, 2012.

[6] Avinash K. Gulve and Madhuri S. Joshi, "A high capacity secured image steganography method with five pixel pair differencing and LSB substitution," ***International Journal of Image, Graphics and Signal Processing***, Vol. 5, pp.66-74, 2015.

[7] Y.Y. Tsai, J.T. Chen, and C.S. Chan, "Exploring LSB substitution and pixel-value differencing for block-based adaptive data hiding," ***International Journal of Network Security***, Vol. 16, pp.363-368, 2014.

[8] D.C. Wu and W.H. Tsai, "A steganographic method for images by pixel-value differencing," ***Pattern Recognition Letters***, Vol. 24, pp.1613-1626, 2003.

[9] C.C. Chang and H.W. Tseng, "A steganographic method for digital images using side-match," ***Pattern Recognition Letters***, Vol. 25, pp.1431-1437, 2004.


**表 3 實驗結果比較**

| 方法 / 影像 | | [5](*k*=4) | [6] | 本研究(5×5) (*k*=4,*al*=8) | 本研究(3×3) (*k*=4,*al*=8) |
|---|---|---|---|---|---|
| Lena | Capacity | 895593 | 783714 | **937308** | 929304 |
| | PSNR | 34.4101 | 38.0842 | 35.6580 | 35.4458 |
| Baboon | Capacity | 959621 | 787726 | **996092** | 984615 |
| | PSNR | 31.4811 | 37.7593 | 34.9978 | 34.8091 |
| Pepper | Capacity | 892394 | 783833 | **934998** | 928834 |
| | PSNR | 33.0093 | 38.0477 | 35.6630 | 35.4409 |
| Jet | Capacity | 893821 | 783972 | **938820** | 932345 |
| | PSNR | 34.3684 | 38.1117 | 35.6412 | 35.4089 |