LSB+*n*PVD 資訊隱藏方法的探討

冷輝世　　蔣翔能
國立彰化師範大學數學系　國立彰化師範大學數學系
lenghs@cc.ncue.edu.tw　m0322004@mail.ncue.edu.tw

摘要

最低位元藏匿法(以下簡稱 LSB)與像素差值藏匿法(以下簡稱 PVD)是常見的不可逆資訊隱藏法，兩者都具有高藏入量與低失真度的優點。LSB 是利用最低位元藏入機密訊息，缺點是易於被偵測導致安全性不佳。PVD 則是利用相鄰像素差值所屬的量化區間決定藏入機密訊息的長度，在邊緣區嵌入較平坦區更多的機密訊息，缺點是一般影像平坦區居多導致藏入量無法提昇。基於以上的原則，許多學者提出將兩者結合的資訊隱藏方法。本研究提出 LSB+*n* PVD 的資訊隱藏方式。其中 PVD 方法主要是使用 Hsiao 與 Chang 學者改良 PVD 的方法，並比較 Khodaei 與 Faez 學者以及 Gulve 與 Joshi 學者的方法。實驗結果顯示本研究的方法在影像品質符合人類視覺系統敏感度的情況下具有高藏入量。

關鍵詞：不可逆資訊隱藏法、最低位元藏匿法、像素差值藏匿法、人類視覺系統。

Abstract

The LSB(Least-Significant-Bit) substitution method and the PVD(Pixel-Value-Differencing) method are popular irreversible data hiding methods. Both methods have high payload and low distortion. The LSB substitution method embeds the secret message by replacing rightmost LSBs. The disadvantage of the LSB substitution method is that it can be detected by RS-Analysis easily if it uses too many rightmost LSBs. The PVD method determines the length of the embedding secret message by which range table of the difference value of two neighboring pixels is belongs to and it embeds more secret message in the edge area than the smooth area. In general, most part of an image is located in the smooth area, so it can't increase the payload. Many researchers have studied the related works by combining the LSB substitution method and the PVD method.

In this study, we propose a LSB+*n*PVD data hiding method. We use an improved PVD method which is proposed by Shiao and Chang. In addition, we compare with Khodaei and Faez's study and Gulve and Joshi's study. The experimental results show that the proposed method has higher payload with acceptable imperceptibility under the human vision system.

Keywords: Irreversible data hiding, LSB substitution method, PVD method.

1. 前言

資訊隱藏是指傳送方將機密訊息藏匿於掩蔽媒體中，讓非法人士無法察覺機密訊息的存在，以避免被攔截、竄改或破解。資訊隱藏包括了可逆式資訊隱藏與不可逆式資訊隱藏。可逆式資訊隱藏在接收方接收到已藏入機密訊息的偽裝影像後，可以取出機密訊息並還原原始影像；不可逆式資訊隱藏在接收方取出機密訊息後無法還原原始影像。

不可逆式資訊隱藏方法中又以 LSB 與 PVD 方法[5]最著名。LSB 方法的藏入方法是將機密訊息取代最低位元，所以取出時可以直接利用最低位元取出。PVD 方法是將掩蔽影像兩兩像素一組並計算其差值，由量化區間表決定可藏入的機密訊息長度。由於藏入時的變化量將由兩個像素值均攤，所以可以減少失真程度，有助於提昇偽裝影像的品質。

近年來，許多的學者也相繼提出了 PVD 方法的改良 [1,4,6-7]。例如：Wu 等學者(2005)[6]，以及 Yang 等學者(2010) [7]均提出針對 PVD 方法中差值較小的部份利用 LSB 方法(Least-Significant-Bit，以下簡稱 LSB)提高藏入量。Khodaei 與 Faez (2011)[4]將像素改良成 1×3 個為一組，使用 LSB+2PVD 的方法藏匿機密訊息。另外， Gulve 與 Joshi (2015)[1]將像素

改良成 2x3 個像素值為一組，使用 LSB+5 PVD 的方法藏匿機密訊息。Hsiao 和 Chang(2011) [2-3]提出改良 PVD 的方法使 PVD 方法可以藏入更多的機密訊息。

本研究探討LSB+*n*PVD的資訊隱藏方法。藉由 Hsiao 和 Chang 的改良 PVD 方法， 在影像品質符合人類視覺系統敏感度的情況下具有較高的藏入量。

2. 文獻探討

2.1 Wu 和 Tsai 學者的 PVD 方法

Wu 和 Tsai 在 2003 年提出 PVD 藏方法，將掩蔽影像中的像素兩兩一組，每組中有兩個像素值 p_i 與 p_{i+1}，$p_i \in [0,255]$，$p_{i+1} \in [0,255]$，計算其差值 $d=|p_i - p_{i+1}|$，$d \in [0,255]$，則依量化區間 R_n 的定義估計藏入機密訊息的長度。其中量化區間 $R_n=[l_n,u_n]$，l_n 表示該量化區間的下界，u_n 表示為該量化區間的上界。

藏入機密訊息的過程如下：首先計算出一組像素(p_i,p_{i+1})的差值 $d=|p_i - p_{i+1}|$，對照量化區間 R_n，找出 $d \in R_n=[l_n,u_n]$。則藏入機密訊息的長度 $t=\log_2|R_n|$，其中$|R_n|$表示 R_n 區間的長度。取長度為 t 的機密訊息，並將其從二進制轉為十進制 s。舉例來說，若 $t=4$，且機密訊息為 0110…，則取長度為 4 的機密訊息為$(0110)_2=(6)_{10}$，得到 $s=6$。由(1)式計算新的像素差值 d'，以及 $m=d'-(p_{i+1}-p_i)$。

$$d' = \begin{cases} l_n + s & \text{if } p_{i+1} - p_i \geq 0 \\ -(l_n + s) & \text{if } p_{i+1} - p_i < 0 \end{cases} \quad (1)$$

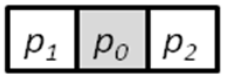
再由(2)式，利用 m 將 d' 平均分攤給(p_i,p_{i+1})，得到偽裝像素值。

$$(p_i', p_{i+1}') = \begin{cases} \left(p_i - \lceil m/2 \rceil, p_{i+1} + \lfloor m/2 \rfloor\right) \\ \quad \text{if } d \text{ is an odd number;} \\ \left(p_i - \lfloor m/2 \rfloor, p_{i+1} + \lceil m/2 \rceil\right) \\ \quad \text{if } d \text{ is an even number} \end{cases} \quad (2)$$

取出機密訊息的過程如下：首先計算出一組偽裝像素(p'_i,p'_{i+1})的差值 $d'=|p'_i - p'_{i+1}|$，再對照量化區間 R_n，找出 $d' \in R_n=[l_n,u_n]$。計算出該區間機密訊息的長度 $t=\log_2|R_n|$，其中$|R_n|$表示 R_n 區間的長度。最後，計算 $s'=d'-l_n$，再將 s' 轉換成長度為 t 的二進制數列 s，則 s 為該區塊所藏入的機密訊息。

2.2 Khodaei 和 Faez 的方法

Khodaei 和 Faez 在 2012 年提出 LSB+2PVD 的方法，將掩蔽影像中的像素依序劃分為 1x3 個像素為一區塊，分別利用 LSB 與 PVD 藏匿法藏入機密訊息。由於藏入時分別有兩種不一樣的藏匿法，且利用 PVD 藏匿法藏入的機密訊息長度是由不同差值與量化區間表所設計，所以透過此藏匿法藏匿的機密訊息也較不容易被偵測與破解。



圖一：每 1x3 個像素為一區塊(藏入前)

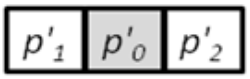
藏入機密訊息的過程如下：首先將原始影像每 1x3 個像素為一區塊，如圖一。像素值 p_0 以 LSB 藏匿法藏入 k 位元的機密訊息 s_0，將機密訊息 s_0 藏入後，將像素值經過最佳化使得差值最小，得到新的像素值 p'_0。接著再以像素值 p_1 與像素值 p_2，分別計算出與新的像素值 p'_0 的差值 $d_1=|p_i - p'_0|$、$d_2=|p_2 - p'_1|$，對照量化區間表，其中 Khodaei 和 Faez 將量化區間表劃分成 $R_1=[0,7]$、$R_2=[8,15]$、$R_3=[16,31]$、$R_4=[32,63]$、$R_5=[64,255]$，並將其分成兩種情況：(1)R_1、R_2、R_3 屬於 lower-level，皆可藏入 3 位元的機密訊息；R_4、R_5 屬於 higher-level，皆可藏入 4 位元的機密訊息；(2)R_1、R_2、R_3、R_4 屬於 lower-level，分別可藏入 3、3、4、5 位元的機密訊息；R_5 屬於 higher-level，可藏入 6 位元的機密訊息。接著利用量化區間表找出 d_1 與 d_2 分別屬於哪個量化區間 R_n、該量化區間的最小值 l_1 與 l_2，以及分別可以藏入 t_1 與 t_2 位元的機密訊息。取出 t_1 與 t_2 位元的機密訊息，並將其轉成十進制 s_{i1} 與 s_{i2}，求得新的像素差值 $d'_1=l_1+s_l$ 與 $d'_2=l_2+s_2$。接著求得 $p''_1=p'_0-d'_1$、$p'''_1=p'_0+d'_1$、$p''_2=p'_0-d'_2$、$p'''_2=p'_0+d'_2$，最後利用(3)式求得新的像素值 p'_1、p'_2。

$$p'_1 = \begin{cases} p''_1, \text{if } |p_1 - p''_1| \leq |p_1 - p'''_1| \\ \quad \text{and } 0 \leq p''_1 \leq 255 \\ p'''_1, \text{otherwise} \end{cases}$$

$$p'_2 = \begin{cases} p''_2, \text{if } |p_2 - p''_2| \leq |p_2 - p'''_2| \\ \quad \text{and } 0 \leq p''_{i+2} \leq 255 \\ p'''_2, \text{otherwise} \end{cases} \quad (3)$$

取出機密訊息的過程如下：首先將一原始影像每 1x3 個像素為一區塊，如圖二。像素值 p'_0 以 LSB 藏匿法取出 k 位元的機密訊息 s_0，接著再以像素值 p'_1 與像素值 p'_2，分別計算出與像素值 p'_0 的差值 $d'_1=|p'_1 - p'_0|$、$d'_2=|p'_2 - p'_0|$，對照量化區間表，找出 d'_1 與 d'_2 分別屬於哪個

量化區間 R_n、該量化區間的最小值 l_1 與 l_2，以及分別可以藏入 t_1 與 t_2 位元的機密訊息，接著計算 $s'_1=d'_1-l_1$、$s'_2=d'_2-l_2$，最後分別將 s'_1、s'_2 由十進制轉成二進制 s_1、s_2，取出機密訊息 s_1、s_2。

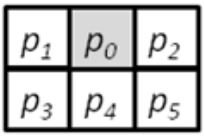


圖二：每 1x3 個像素為一區塊(藏入後)

Khodaei 和 Faez 所提出的方法有效的提升了機密訊息的藏入量與維持影像品質，但其藏入量卻因其量化區間的劃分與藏入時像素差值 d 的計算提升效果卻相當有限。

2.3 Gulve 和 Joshi 的方法

Gulve 和 Joshi 在 2015 年提出 LSB+5PVD 方法，將掩蔽影像中的像素依序劃分為 2x3 個像素為一區塊，並且在 PVD 藏匿法藏入過程中對於藏入的機密訊息長度做調整，使得影像品質有較明顯的提升。



圖三：每 2x3 個像素為一區塊(藏入前)

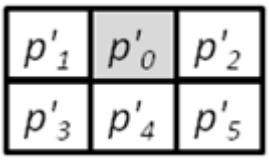
藏入機密訊息的過程如下：首先將原始影像每 2x3 個像素為一區塊，如圖三。像素值 p_0 以 LSB 藏匿法藏入 3 位元的機密訊息 s_0，將機密訊息 s_0 藏入後，將像素值經過最佳化使得差值最小，得到新的像素值 p'_0。接著再計算像素值 p_i 與像素值 p'_0 的差值 $d_i=p_i-p'_0$，求得$|d_i|$所屬的量化區間 $R_{i,n}$ 以及可以藏入的位元 t_i，接著計算該區塊的平均可藏入的長度 $avg=\lfloor(t_1+t_2+t_3+t_4+t_5)/5\rfloor$，計算像素差值 d_i 除以 2^{avg} 的餘數 dl_i，求得$|dl_i|$所屬的量化區間 $R_{i,n}$、其量化區間 $R_{i,n}$ 的最小值 l_i，以及可以藏入的位元 t'_i，分別取 t'_i 位元的機密訊息將其轉乘十進制 s_i，利用(4)式求得新的像素差值 d'_i。

$$d'_i=\begin{cases}|d_i|-|dl_i|+l_i+s_i, \text{if } d_i\geq 0\\ -(|d_i|-|dl_i|+l_i+s_i), \text{if } d_i<0\end{cases} \quad (4)$$

利用(5)式，我們可以分別求出每組像素值(p'_0,p_i)藏入機密訊息後分別改變成(p''_0,p''_i)

$$(p''_0,p''_i)=(p'_0-\lceil m_i/2\rceil, p_i+\lfloor m_i/2\rfloor) \quad \text{where } m_i=d'_i-d_i \quad (5)$$

接著以$|m_i|$最小的該組像素值中的 p''_0 為基礎像素 p，將其他四組像素組的差值保持不變將(p''_0,p''_i)改變為(p,p'_i)，最後檢查 LSB$(p,3)$是否等於 LSB$(p'_0,3)$，其中 LSB(a,b)表示將 a 用二進制表示後的末 b 碼，若相等則得到圖四的結果；若不相等則將 LSB$(p,3)$調整成 LSB$(p'_0,3)$，並保持像素差值 d'_i 維持不變，調整像素值中的 p'_i，得到圖四的結果。



圖四：每 2x3 個像素為一區塊(藏入後)

但若調整後的 6 個像素值 p'_i 當中某個像素值 p'_i，$-8\leq p'_i<0$，則所有像素值 $p'_i=p'_i+8$；若調整後的 6 個像素值 p'_i 當中某個像素值 p'_i，$255<p'_i\leq 263$，則所有像素值 $p'_i=p'_i-8$；若調整後還有像素值 $p'_i\notin[0,255]$，則此張掩蔽影像則不適合用來藏入機密訊息。

取出機密訊息的過程如下：首先將一原始影像每 2x3 個像素為一區塊，如圖四。像素值 p'_0 以 LSB 藏匿法取出 3 位元的機密訊息 s_0。接著再計算像素值 p'_i 與像素值 p'_0 的差值 $d'_i=p_i-p'_0$，求得$|d'_i|$所屬的量化區間 $R_{i,n}$ 以及可以藏入的位元 t_i，接著計算該區塊的平均可藏入的長度 $avg=\lfloor(t_1+t_2+t_3+t_4+t_5)/5\rfloor$，計算像素差值 d'_i 除以 2^{avg} 的餘數 dl'_i，求得$|dl'_i|$所屬的量化區間 $R_{i,n}$、其量化區間 $R_{i,n}$ 的最小值 l_i，以及可以藏入的位元 t'_i，計算 $s'_i=dl'_i-l_i$，最後分別將 s'_i 由十進制轉成二進制 s_i，取出機密訊息 s_i。

Khodaei 和 Faez 所提出的改良方法因為其藏入時的特性，對於任意掩蔽影像藏入機密訊息藏入量都趨近一致，藏入量的提升也是有限的，但也因此影像品值相對來說維持的較好。但是在調整後有可能無法令所有的像素值皆屬於 0 到 255 之間，進而導致該張掩蔽影像不適合用來藏入機密訊息，所以也使得能夠使用該方法藏匿機密訊息的掩蔽影像減少許多。

2.4 Hsiao 和 Chang 的方法

Hsiao 和 Chang 在 2011 年提出改良的 PVD 方法，在每個區塊中機密訊息至少能藏 1 位元，在原本計算像素差值 d，改變為 $d^n=$

$2^n+b(s,n)_{10}-al$，其中 $n=1、2、\cdots、7$；$b(s,n)_{10}$ 表示將 n 位元的機密訊息由二進制轉成十進制的值；al 使得每個區塊中機密訊息長度至少 $\log_2 al$ 位元且 al 必須為 2 的次方數。在從偽裝影像取出機密訊息時，計算像素差值 $|d'|=|d^n|=2^n+b(s,n)_{10}-al$，其中 $n=\lfloor \log_2(|d'|+al)\rfloor=\lfloor \log_2(2^n+b(s,n)_{10})\rfloor$；$b(s,n)_{10}=|d'|+al-2^n$。

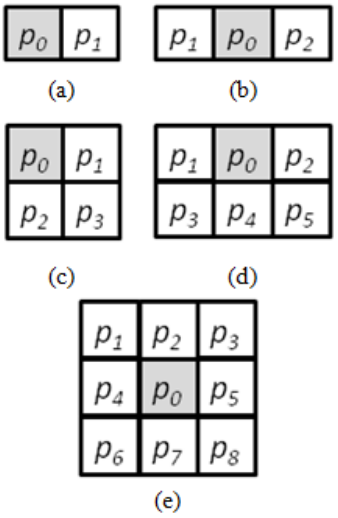
本研究中，n 為當使用像素差值 d^n 時，偽裝影像與掩蔽影像中的像素值的變化是最小，以利增加藏入量與維持影像品質。

3.研究方法

本研究提出 LSB+n PVD 的資訊隱藏方式，在影像品質符合人類視覺系統敏感度的情況下具有高藏入量。主要是使用 Hsiao 和 Chang 的改良的 PVD 方法，並比較 Khodaei 與 Faez 以及 Gulve 與 Joshi 的方法。以下所使用的 PVD 方法皆為 Hsiao 和 Chang 的改良的 PVD 方法。

3.1 區塊劃分

PVD 方法是將掩蔽影像中的像素依序劃分為 1x2 個像素值為一區塊，本研究將分別討論 1x2、1x3、2x2、2x3、3x3 個像素值為一區塊(如圖五所示)，在藏匿機密訊息時，我們會將每個區塊中分為以 LSB 方法藏匿與以 PVD 方法藏匿兩個部份，如圖五中灰色區塊像素值 p_0，我們將以 LSB 藏匿法藏匿 k 位元的機密訊息，其餘白色區塊像素值 p_i 將以 p_0 藏匿機密訊息後的像素值 p'_0 為參考像素值，利用 PVD 方法藏匿機密訊息。



圖五：每 mxn 個像素為一區塊

也就是說在圖五中，(a)是以 1x2 個像素值為一區塊，並且在一區塊中以 1 個 LSB、1 個 PVD 藏匿法做藏匿；(b)是以 1x3 個像素值為一區塊，並且在一區塊中以 1 個 LSB、2 個 PVD 藏匿法做藏匿；(c)是以 2x2 個像素值為一區塊，並且在一區塊中以 1 個 LSB、3 個 PVD 藏匿法做藏匿；(d)是以 2x3 個像素值為一區塊，並且在一區塊中以 1 個 LSB、5 個 PVD 藏匿法做藏匿；(e)是以 3x3 個像素值為一區塊，並且在一區塊中以 1 個 LSB、8 個 PVD 藏匿法做藏匿。

3.2 藏匿過程

首先將原始影像每 mxn 個像素為一區塊，如圖五所示，共有五種討論方案。像素值 p_0 以 LSB 藏匿法藏入 k_1 位元的機密訊息 s_0，將機密訊息 s_0 藏入後，得到像素值 $p''_0=p_0-\mathrm{mod}(p_0,2^{k_1})+s_0$，利用(6)式經過最佳化使得差值最小，得到新的像素值 p'_0。

$$p'_0=\begin{cases} p''_0+2^{k_1} & ,\text{if } p'_0-p_0<-2^{k_1-1} \\ p''_0-2^{k_1} & ,\text{if } p'_0-p_0>2^{k_1-1} \\ p''_0 & ,\text{otherwise} \end{cases} \quad (6)$$

接著取像素值 p_i、像素值 p'_0，以 PVD 藏匿法至少藏 k_2 位元機密訊息藏匿，利用(7)式計算 $P_{i,n,1}$ 與 $P_{i,n,2}$，其中 $n=1、2、\cdots、7$，其中 secret(n)表示取 n 位元的機密訊息轉為十進制。

$$\begin{aligned} P_{i,n,1}&=p'_0+(2^n+\mathrm{secret}(n)-2^{k_2}) \\ P_{i,n,2}&=p'_0-(2^n+\mathrm{secret}(n)-2^{k_2}) \end{aligned} \quad (7)$$

利用(8)式計算 $P_{i,n}$，其中 n=1,2,⋯,7。

$$P_{i,n}=\begin{cases} P_{i,n,1} & ,\text{if } |P_{i,n,1}-p_i|<|P_{i,n,2}-p_i| \\ & \quad \text{and } 0\le P_{i,n,1}\le 255 \\ P_{i,n,2} & ,\text{otherwise} \end{cases} \quad (8)$$

最後計算每個 $P_{i,n}$ 的改變量 $D_{i,n}=|P_{i,n}-p_i|$，找出 $D_{i,n}$ 的最小值 $D_{i,x}=\min\{D_{i,n}|n=1,2,\cdots,7\}$，則新的像素值 $p'_i=P_{i,x}$，且藏入的機密訊息 $s_i=\mathrm{secret}(x)$。

3.3 取出過程

首先將原始影像每 mxn 個像素為一區塊，如(圖五所示，共有五種討論方案)，像素值 p_0 以 LSB 藏匿法取出 k_1 位元的機密訊息 s_0，如(9)式所示。

$$s_0=\left(\mathrm{mod}(p'_0,2^{k_1})\right)_2 \quad (9)$$

接著利用像素值 p'_i、像素值 p'_0，取出機密

訊息 $s_i=(d_i'-2^{t_i})_2$ ，其中 $d_i'=\mid p_i'-p_0'\mid+2^{k_2}$ ，$t_i=\lfloor\log_2(d_i')\rfloor$。

4. 實驗結果

在這個段落，將本研究方法分別使用本研究方法中的以 1x3 個像素值為一區塊(圖五中的(b))與 Khodaei 和 Faez 所提出的方法比較、討論；以及使用本研究方法中的以 2x3 個像素值為一區塊(圖五中的(d))與 Gulve 和 Joshi 所提出的方法做比較。

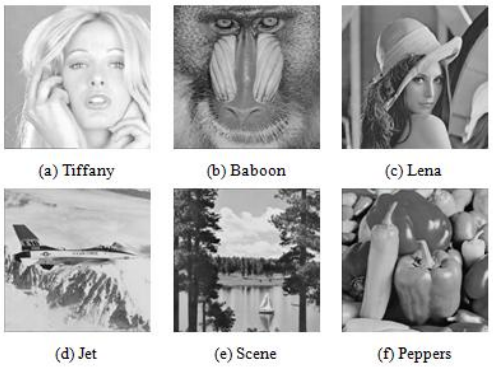
本研究選用 SIPI 影像資料庫的 Tiffany、Baboon、Lena、Jet、Scene、Peppers 六張標準影像作為原始影像(如圖六)並使用(10)式中的 PSNR (Peak Signal to Noise Ratio)做為影像品質評比的依據。

$$\text{PSNR}=10\times\log_{10}\frac{255^2}{\text{MSE}}\ (\text{dB}) \qquad (10)$$

其中 MSE 定義如(11)式。

$$\text{MSE}=\frac{1}{w\times h}\sum_{i=i}^{w}\sum_{j=1}^{h}(x_{i,j}-x_{i,j}')^2 \qquad (11)$$

其中 w 與 h 分別代表影像的長與寬，$x_{i,j}$ 與 $x_{i,j}'$ 分別代表掩蔽影像與偽裝影像第 i 列第 j 行的像素值。

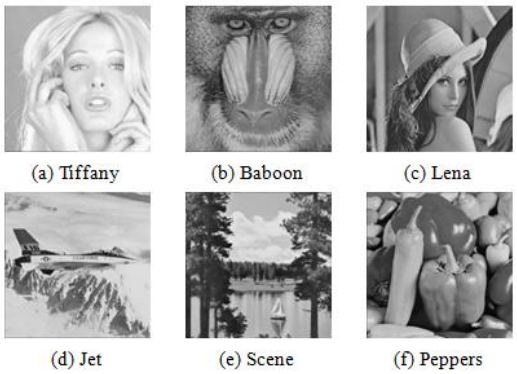


圖六：原始影像

4.1 與 Khodaei 和 Faez 方法的比較

本研究與 Khodaei 和 Faez 方法的主要差異在於使用 PVD 藏匿法藏匿機密訊息時，本研究所藏匿的機密訊息長度是變動的；而 Khodaei 和 Faez 兩位學者的方法則是將量化區間表劃分成 R_1=[0,7]、R_2=[8,15]、R_3=[16,31]、R_4=[32,63]、R_5=[64,255]，並將其分成 Type 1 與 Type 2 兩種情況，Type 1：R_1、R_2、R_3 屬於 lower-level，皆可藏入 3 位元的機密訊息；R_4、R_5 屬於 higher-level，皆可藏入 4 位元的機密訊息；Type 2：R_1、R_2、R_3、R_4 屬於 lower-level，分別可藏入 3、3、4、5 位元的機密訊息；R_5 屬於 higher-level，可藏入 6 位元的機密訊息。

表 I 是由本研究中的以 1x3 個像素值為一區塊(圖五中的(b))且 $k_1=3$，$k_2=3$(簡稱 LSB(3)+2PVD(3))時，與 Khodaei 和 Faez 的方法中 $k=3$ 時 Type 1 與 Type 2 兩種情況的藏入量與影像品質比較表，由表 I 可以發現到本研究方法的藏入量高於 Khodaei 和 Faez 的方法約 16,000~100,000 位元，並且影像品質能與 Khodaei 和 Faez 方法的 Type 2 相差不多，PSNR 值皆能保持在 34dB 以上，圖七為本研究方法藏匿機密訊息後的偽裝影像。



圖七：LSB(3)+2PVD(3)藏匿訊息後的偽裝影像

表 I
本研究與[4]的比較

	[4] k=3，type 1		[4] k=3，type 2		Our LSB(3)+2PVD(3)	
	Capacity(bit)	**PSNR(dB)**	**Capacity(bit)**	**PSNR(dB)**	**Capacity(bit)**	**PSNR(dB)**
Tiffany	790,253	38.33	806,847	37.79	**826,404**	37.55
Baboon	810,126	36.72	886,516	36.29	**913,961**	34.46
Lena	791,253	38.18	809,966	37.63	**835,506**	37.48
Jet	792,617	38.05	809,262	37.53	**825,753**	37.19
Scene	-	-	-	-	**861,770**	36.39
Peppers	789,989	38.35	802,228	37.97	**835,700**	37.12

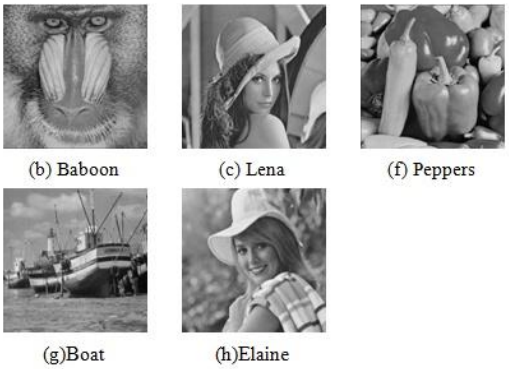
4.2 與 Gulve 和 Joshi 方法的比較

本研究與Gulve和Joshi方法的主要差異在於使用 PVD 藏匿法藏匿機密訊息時，本研究方法所藏匿的機密訊息長度是變動的；而Gulve和Joshi的方法則是由每個區塊中的平均藏入量決定每組像素值利用 PVD 藏匿機密訊息的長度，且 Gulve 和 Joshi 的方法因為藏入機密訊息且調整後有可能導致該張掩蔽影像不適合用來藏入機密訊息，所以本研究方法將挑選 SIPI 影像資料庫中可以與其比較的五張掩蔽影像(Baboon、Lena、Peppers、Boat、Elaine)作為實驗數據的比較。

表 II
本研究與[1]的比較

	[1]		Our LSB(3)+5PVD(3)	
	Capacity (bit)	**PSNR (dB)**	**Capacity (bit)**	**PSNR (dB)**
Baboon	784,216	41.00	**974,432**	32.01
Lena	780,544	41.53	**847,220**	36.88
Peppers	780,608	41.50	**850,289**	36.27
Boat	762,720	41.32	**880,661**	35.39
Elaine	762,000	41.41	**865,758**	37.07

表 II 是由本研究中的以 2x3 個像素值為一區塊(圖五中的(b))且 $k_1=3$，$k_2=3$(簡稱 LSB(3)+5PVD(3))時，與 Gulve 和 Joshi 的方法的藏入量與影像品質比較表，由表 II 可以發現到本研究方法的藏入量高於 Gulve 和 Joshi 兩位學者的方法約 60,000~200,000 位元，但因藏入量提升了許多，所以影像品質皆下降了 4.34~8.99 dB，不過本研究的 PSNR 值依然可以保持在 32dB 以上，仍滿足人類視覺敏感度的要求(大於 30dB)。圖八為本研究藏匿機密訊息後的偽裝影像。



圖八：LSB(3)+5PVD(3)藏匿訊息後的偽裝影像

4.3 五種區塊劃分法比較

在表 I 與表 II 中，本研究方法藏入量皆都高於[1]、[4]16,000~200,000 位元，並且品質仍滿足人類視覺敏感度 (大於 30dB)。

表 III 是由本研究方法中五種情況且 $k_1=3$，$k_2=3$ 時的藏入量與影像品質比較表，由表 III 我們可以發現到，當 n 越來越大時，也就是說當 PVD 藏匿法的比例調高時，藏入量也會越來越多；影像品質也因為藏入量的提升而相對降低。

表 III 本研究的五種情況，k_1=3；k_2=3

	LSB(3)+1PVD(3)		LSB(3)+2PVD(3)		LSB(3)+3PVD(3)		LSB(3)+5PVD(3)		LSB(3)+8PVD(3)	
	Capacity (bit)	**PSNR (dB)**	**Capacity (bit)**	**PSNR (dB)**	**Capacity (bit)**	**PSNR (dB)**	**Capacity (bit)**	**PSNR (dB)**	**Capacity (bit)**	**PSNR (dB)**
Tiffany	819,340	38.07	826,404	37.55	835,278	35.90	837,923	35.76	836,626	36.95
Baboon	885,208	35.38	913,961	34.46	959,889	32.28	974,432	32.01	988,586	31.86
Lena	825,567	38.04	835,506	37.48	842,948	37.15	847,220	36.88	847,831	36.69
Jet	818,503	37.67	825,753	37.19	842,159	36.17	845,847	35.86	847,551	35.85
Scene	845,781	37.14	861,770	36.39	881,070	35.48	889,132	35.03	894,732	34.68
Peppers	826,336	37.85	835,700	37.12	846,943	36.63	850,289	36.27	851,501	36.09

5. 結論

本研究探討在區塊中使用 LSB+*n*PVD 方法藏匿機密訊息，並且使用 Hsiao 和 Chang 的改良 PVD 方法。實驗結果顯示當 k_1＝3 與 k_2＝3 時，藏入量至少都有 810,000 位元以上且藏匿機密訊息後的偽裝影像其 PSNR 值都保持在 31.86～38.07dB。此外，本研究的五種討論方案相較於[4]和[5]皆有較高的藏入量且偽裝影像品質皆滿足人類視覺敏感度 (大於 30dB)。

參考文獻

[1] Gulve, A., & Joshi, M. (2015). A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution. International Journal of Image, Graphics and Signal Processing IJIGSP, 66-74.

[2] Hsiao, J., & Chang, C. (2008). Steganographic scheme for digital images using difference in neighbouring pixels. The Imaging Science Journal, 291-299.

[3] Hsiao, J., & Chang, C. (2011). An adaptive steganographic method based on the measurement of just noticeable distortion profile. Image and Vision Computing, 155-166.

[4] Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image Processing, 677-686.

[5] Wu, D., & Tsai, W. (2002). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 1613-1626.

[6] Wu, H., Wu, N., Tsai, C., & Hwang, M. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings - Vision, Image, and Signal Processing IEE Proc., Vis. Image Process., 611-611.

[7] Yang, C., Weng, C., Wang, S., & Sun, H. (2010). Varied PVD LSB evading detection programs to spatial domain in data embedding systems. Journal of Systems and Software, 1635-1643.