混合式的高容量空間域資訊藏密法

A Hybrid High-Capacity Steganography Method in Spatial Domain

婁德權

長庚大學資訊工程學系

Email: dclouprof@gmail.com

賀盛志

國防大學理工學院電機電子工程學系

Email: hsz1028@hotmail.com

***摘要*—在此篇文章中，我們提出了一種混合式的空間域資料藏密方法。此方法能夠在人類視覺系統無法察覺情況下在灰階影像中嵌入祕密訊息。本方法結合了像素差（Pixel-Value Differencing；PVD）藏密法與模數函數（Modulus function）藏密法。像素差藏密法能針對影像的特性調整藏密區塊的藏密量，影像邊緣區域可有較多的藏密量，平滑區域則較少；模數函數藏密法有簡單、容易實現及可維持高影像品質的優點。我們所提出的方法可解決上述兩種方法相容性的問題，實驗結果顯示在影像品質維持相同水準下，可比像素差藏密法增加大量藏密的容量。另在安全性方面，經實驗證明本方法可成功抵擋RS攻擊法。**

***關鍵詞*—像素差藏密法、模數函數藏密法、資訊隱藏、空間域。**

abstract— In this article, we propose a hybrid high-capacity steganography method in spatial domain. This method capable of embedding secret data in gray-scale image that is undetectable by human eye. This method is a combination of Pixel-Value Differencing (PVD) steganography method and Modulus function steganography method. The hiding capacity of PVD method depends on the difference value of the two consecutive pixels. It can adjust the volume of embedding data by the characteristics of image block. The advantage of Modulus function steganography method is simply, easy to implement and can maintain high quality of stego-image. In our scheme, we propose a method to resolve the compatibility issues of the above two steganography methods. The experimental results have also demonstrated that the proposed method can increase the embedding capacity and maintain the same level of stego-image quality with PVD steganography method. In security issues, experiments prove that this method can be successfully withstand RS-diagram attacks.

Keywords: PVD, Modulus function, Data hiding, Spatial domain.

一、前言

近年來有許多有關資訊隱藏(Information Hiding)的研究，藏密學是資訊隱藏研究中的一個類別，有別於密碼學的目的是隱藏資訊的涵義，而藏密學則是隱藏資訊的存在。故藏密的目的並不在於讓敵人難以破解，而在於讓人難以察覺。例如傳送秘密訊息時，先將訊息的明文利用密碼學加密成為密文，使敵人即使攔截也難以破解，但仍有被解密的風險；若能再將密文嵌入到掩護載體中(例如影像、音訊、視訊)，使秘密訊息的傳送不容易引起敵人的注意，以減低被敵人攔截的風險。基於上述藏密學的目的，研究的方向則不外乎為：

（一）藏密容量的最大化。

（二）藏密後掩護載體影像品質的最佳化。

（三）藏密方法如何能有效抵抗藏密偵測及分析。

藏密容量的最大化，就是在相同大小的影像中並維持相當的影像品質條件下，研究嵌入祕密訊息的最大值，最有名且簡單有效的方法就是最低位元平面取代藏密法（Least-Significant-Bit；LSB）[4][9][10]，此方

法就是直接將 k bit 的訊息密文，藏在影像每個像素的最後 k bit 的位置，在適當的藏密量下人類視覺並無法察覺藏密圖像的變化。但目前已有許多方法對 LSB 取代藏密法有良好的偵測效果，如 x^2 偵測法[1]、RS 偵測法[8]等。

除了安全性的問題，LSB 替代藏密法針對影像中每個像素的藏密量都是一致的，但由於人類視覺對影像平滑部份的的變動較為敏銳，對邊緣部份的變化較不敏感，基於以上概念，Wu 和 Tsai 在 2003 年提出一個依據相鄰像素差(Pixel-value Differencing；PVD)值決定藏密量大小的藏密方法[6]，以相鄰的兩像素為一區塊，若區塊中兩像素的差值愈大則愈可能屬於影像中的邊緣部份，即可嵌入較多的秘密訊息，若差值越小，則可能屬於影像中的平滑區域，則嵌入較少的秘密訊息。決定每個區塊的藏密量後則調整兩像素之間的差值來嵌入祕密訊息，並實驗證明其可抵抗 RS 偵測法[8]。

Wu 等學者在 2005 年基於 PVD 藏密法與 LSB 替代藏密法提出了一種混合式的高容量藏密法[8]，他們認為 PVD 藏密法雖可依據影像的特徵做到藏密量的差異化，但卻浪費了部分潛在的藏密量，以他們所提出的方法，在人類視覺可容忍的情況下，可較 PVD 藏密法增加約一倍的藏密量，而且在藏密後影像品質約略相等的狀況下，此方法藏密量的也較 PVD 藏密法為多。

Wang 等學者在 2008 年提出了一個利用 PVD 藏密法與模數函式結合的高品質藏密方法[5]，改善原 PVD 藏密法調整相鄰兩像素差的程序，運用模數函式以減少像素值的變化，可在與 PVD 藏密法相同的藏密容量下，有效的提升藏密後的影像品質，並以實驗證明可抵抗 RS 偵測法[7]。

Yang 等學者在 2008 年提出了一種依據影像邊緣調整的高容量 LSB 替代藏密法[3]，先利用 PVD 方法中每區塊兩相鄰像素差值作為 LSB 替代藏密法藏密量的依據，若區塊中兩相鄰像素值越低，屬平滑區域，則利用較少位元數 LSB 替代藏密，反之則用較多位元數的 LSB 替代藏密，此方法可達到較 Wu 等學者[8]更好的影像品質與更高的藏密量。

前述的藏密方法針對同一目標區塊，均僅能實現單一的藏密方法，我們所提出的方法，乃是結合 PVD 藏密方法[2]與以模數函數藏密法[4]的概念，並在每個相鄰兩像素區塊中，能同時存在上述的兩種藏密方法，以增加藏密量。且偽裝影像維持可接受的的品質。

本篇文章的架構如下，第二節中我們先會回顧 PVD 藏密方法[6]與以模數函數藏密法[4]，第三節則是敘述我們所提出方法，第四節是實驗結果與分析，第五節為本論文的結論。

二、相關文獻

（一）Wu 和 Tsai 的方法

Wu 和 Tasi 在 2003 年提出藉由調整相鄰像素間的差值嵌入祕密訊息的方法，藏密後影像仍具有良好的影像品質，且可抵抗 RS 偵測法。在藏密前必須先根據兩相鄰像素差來律定嵌密量對照表，作為嵌入祕密訊息及後續取出秘密訊息的依據。差距越小越可能屬於影像平滑部分則嵌密量較少，反之差距越大就越可能是影像邊緣部分，則可嵌入較多的秘密訊息。假設我們要嵌入密文為 2 進位的連續串流，藏密與取密程序如後：

（1）藏密程序

步驟1：假設掩護影像F的大小為 $m \times n$ 個像素，F_i 為影像F的子區塊，每個子區塊由F中不重複的兩相鄰像素所組成，其順序表示為F={ $F_i \mid i$=1, 2, 3,…., $m \times n / 2$ }，F_i 的左右兩邊的像素值分別為 $P_{(i,x)}$、$P_{(i,y)}$，兩像素差值為 d_i，d_i 可由下式計算得出：

$$d_i = \left| P_{(i,x)} - P_{(i,y)} \right| \quad (1)$$

步驟2：律定範圍表R，其中包含n各連續的子範圍R_j，表示為R=$\{R_j \mid j=1, 2, 3,\ldots, n\}$，範圍表R的功能為訂定每個子區塊$F_i$所能嵌入的秘密訊息量，每個$R_j$有其上下邊界值，記為$u_j$與$l_j$使得$R_j$=$[u_j, l_j]$，$R_j$的寬度為$w_j$，$w_j$是藉由2的乘冪來組成，其值為：

$$w_j = u_j - l_j + 1 \quad (2)$$

步驟3：選擇出F_i最適當的藏密量，$R_i = \min(u_i, d_i)$，其中$u_i \geq d_i$，且R_i=$[l_i, u_i]$，所選擇出的R_i為$1 \leq i \leq n$中的最佳選擇。

步驟4：計算F_i可嵌入的位元數t，以下式求出：

$$t = \lfloor \log_2 w_i \rfloor \quad (3)$$

其中，w_j為R_i的寬度。

步驟5：將t位元的密文轉換成10進位數值b，$b' = l_i + b$，$d_i' = \left| b' - d_i \right|$下列條件式（4）調整$P_{(i,x)}$、$P_{(i,y)}$為新的像素差$d'$：

$$\left(p'_{(i,x)}, p'_{(i,y)}\right) = \begin{cases} (p_{(i,x)} + \lceil m/2 \rceil, p_{(i,y)} - \lfloor m/2 \rfloor), \text{if } p_{(i,x)} \geq p_{(i,y)} \text{ and } d_i' > d_i; \\ (p_{(i,x)} - \lfloor m/2 \rfloor, p_{(i,y)} + \lceil m/2 \rceil), \text{if } p_{(i,x)} < p_{(i,y)} \text{ and } d_i' > d_i; \\ (p_{(i,x)} - \lceil m/2 \rceil, p_{(i,y)} + \lfloor m/2 \rfloor), \text{if } p_{(i,x)} \geq p_{(i,y)} \text{ and } d_i' \leq d_i; \\ (p_{(i,x)} + \lceil m/2 \rceil, p_{(i,y)} - \lfloor m/2 \rfloor), \text{if } p_{(i,x)} < p_{(i,y)} \text{ and } d_i' \leq d_i; \end{cases} \quad (4)$$

其中$m = \left| d_i' - d_i \right|$，然後將新的像素值$(p'_{(i,x)}, p'_{(i,y)})$替換原有的像素值，就完成了區塊$F_i$的嵌密動作。

步驟6：重複前述步驟1至步驟5，直到所有密文都嵌入為止。

（2）取密程序

不需原圖，本方法就可以快速取出嵌入的密文。

步驟1：利用與嵌密時相同的掃描方式組成子區塊，計算子區塊的像素差值d_i，對照表R求出此區塊藏密量，藏密量為k位元。

步驟2：則將d_i轉為2進位值後，取其最後k位元的值，即為之前嵌入的密文。

步驟3：重複前述程序步驟1及步驟2，直到所有密文都取出為止。

（二）Thien 和 Lin 的方法

Thien 和 Lin 於 2003 年提出一種利用模數函式(Modulus Founction)可將及時的數字訊息嵌入圖像中的方法，其方法可達到與 LSB 藏密方法相同的藏密量，嵌入密文後的影像品質亦較高。

（1）嵌密程序：

設P_i為圖像中的任一像素，預藏入 m 位元的秘密訊息，P_i的值為x_i；若以灰階影像為例則$0 \leq x_i \leq 255$，$1 \leq m \leq 8$，但通常若每像素嵌入超過 4 位元，其嵌入後的影像品質就會變的很差。

步驟1：將m位元的密文轉換成10進位值b_i，$b_i \in [0,1,\ldots.,2^m - 1]$；

$$P_{rem(i)} = x_i \bmod 2^m \quad (5)$$

$$d_i = x_i - P_{rem(i)} \quad (6)$$

步驟2：調整d_i的值為d'_i，調整方法如下：

$$d'_i = \begin{cases} d_i, \text{ if } (-\lfloor (m-1)/2 \rfloor) \leq d_i \leq \lceil (m-1)/2 \rceil \\ d_i + 2^m, \text{ if } (-m+1) \leq d_i < (-\lceil (m-1)/2 \rceil) \\ d_i - 2^m, \text{ if } (-\lceil (m-1)/2 \rceil) < d_i < m \end{cases} \quad (7)$$

產生x'_i值如下式：

$$x'_i = x_i + d'_i \quad (8)$$

步驟3：如果經過(8)使得 $x'_i > 255$ 或 $x'_i < 0$，超過灰階影像像素值的範圍，則依下式（9）將 x'_i 調回正常範圍。

$$x'_i = \begin{cases} x_i + d'_i + m \text{ , if } x_i + d'_i < 0 \\ x_i + d'_i - m \text{ , if } x_i + d'_i > 255 \end{cases} \quad (9)$$

最後以 x'_i 代替 x_i 成為 P_i 的像素值，即完成嵌密動作。

（2）取密程序

取密程序非常容易，假設 P_i 所藏的秘密訊息為 s_i，則依下式（10）即可求出 s_i：

$$s_i = x'_i \bmod 2^m \quad (10)$$

再將 s_i 值轉換成 m 位元的 2 進位值即為先前所藏入的秘密訊息。

三、本文所提的方法

我們所提出的方法，是綜合前述兩種藏密方法，並於每個藏密區塊中均同時存在這兩種方法。藏密與取密的程序分述如後。

（一）藏密程序

假設掩護影像F的大小為 $m \times n$ 個像素，F_i 為影像F的子區塊，由相鄰兩像素 Px、Py 所組成。

步驟 1：利用前節 Wu 和 Tsai 的方法藏入祕密訊息，而嵌入密文後所像素值為 $p'_{(i,x)}$ 與 $p'_{(i,y)}$。

步驟 2：對 F_i 的左像素 Px，再利用前述 Thien and Lin 的方法嵌入 m bits 密文，嵌入密文後 Px 的像素值為 $p''_{(i,x)}$。

步驟 3：令 $s = \left| p'_{(i,x)} - p''_{(i,x)} \right|$，利用下列關係式（11）調整 $p'_{(i,y)}$ 為 $p''_{(i,y)}$。

$$p''_{(i,y)} = \begin{cases} p'_{(i,y)} + s \text{ , } if \;\; p'_{(i,x)} < p''_{(i,x)} \\ p'_{(i,y)} - s \text{ , } if \;\; p'_{(i,x)} > p''_{(i,x)} \\ p'_{(i,y)} \text{ , } if \;\; p'_{(i,x)} = p''_{(i,x)} \end{cases} \quad (11)$$

若 $0 \le p''_{(i,y)} \le 255$，則將 $(p''_{(i,x)}, p''_{(i,y)})$ 取代 $(p_{(i,x)}, p_{(i,y)})$ 成為 (Px, Py) 新的像素值，即完成嵌密程序。若 $p''_{(i,y)} < 0$ 或 $p''_{(i,y)} > 255$ 則進入步驟 4。

步驟 4：將 $(p''_{(i,x)}, p''_{(i,y)})$ 依下列條件式（12），調整成 $(p'''_{(i,x)}, p'''_{(i,y)})$，再將 $(p'''_{(i,x)}, p'''_{(i,y)})$ 取代 $(p_{(i,x)}, p_{(i,y)})$ 成為 (Px, Py) 新的像素值，即完成嵌密程序。

$$(p'''_{(i,x)}, p'''_{(i,y)}) = \begin{cases} (p'''_{(i,x)} + 2^m, p'''_{(i,y)} + 2^m), \; if \;\; p''_{(i,y)} < 0 \\ (p'''_{(i,x)} - 2^m, p'''_{(i,y)} - 2^m), \; if \;\; p''_{(i,y)} > 255 \end{cases} \quad (12)$$

（二）取密程序：

假設預取密之子區塊為 F_i，先利用Wu和Tsai的方法將秘密訊息取出，再利用Thien and Lin的方法對 F_i 的左像素 Px 取密，最後將兩組2進位字串結合，即完成此子區塊取密動作。將所有藏密子區塊依以上方法將密文取出後，將所有取出的2進位字串密文相結合即完成全部的取密程序。

（三）實例說明：

本文所使用PVD藏密法對照表設計為六個像素差值域，範圍依序為 $R_1 \in [0, 7]$、$R_2 \in [8, 15]$、$R_3 \in [16, 31]$、$R_4 \in [32, 63]$、$R_5 \in [63, 127]$、$R_6 \in [128, 255]$，每個區域寬度 w 為8、8、16、32、64、128，其藏密量 t 分別為3位元、3位元、4位元、5位元、6位元、7位元。假設F中某一藏密區塊，其 Px 與 Py 之像素值分別為60、120，兩像素值差值 d_i=60，屬 R_4，可藏5個位元之密文，另模數函式藏密法我們藏入4個位元之密文，假設密文為$100011011_{(2)}$，取出前

5個位元為$10001_{(2)}$，等於$17_{(10)}$，此時d_i'=49，經（4）調整後，Px與Py之新像素值分別為66、115，此時完成第一部份藏密。

密文的後4個位元為$1011_{(2)}$，等於$11_{(10)}$，2^4=16依（5），66 mod 2^4 =2，經（6）（7）（8）調整後，Px之新像素值為66−7=59，s值為7，此時依（11）將Py像素值調整為115−7=108，即完成藏密程序。

取密時，先計算藏密區塊內兩像素值差|59−108|=49，屬於R_4的範圍，藏密量為5位元，$49_{(10)}=110001_{(2)}$，取最後5位元為$10001_{(2)}$，再將59 mod 2^4 =11，將11轉換為4位元的2進位數值，$11_{(10)}=1011_{(2)}$，再將$10001_{(2)}$與$1011_{(2)}$合併，即為之前所藏之密文$100011011_{(2)}$。

故取密者只要事先與藏密者協調PVD藏密法對照表與模數函式藏密法在每個藏密區塊的藏密量，即可將密文取出。

四、實驗結果與討論

在本章中我們將顯示本文所提出的方法，在約略相同的影像品質下，可較 PVD 藏密法增加 1/4 以上的藏密容量；在人類視覺可接受的範圍內，其藏密容量可達到 PVD 藏密法的一倍多。我們用 MATLAB 程式語言來實現我們所提的方法及 PVD 藏密法，四個掩護影像為 Lena、Baboon、Couple 與 Pepper（如圖一），PVD 藏密方法的對照表設計為六個像素差值域，範圍依序為$R_1 \in [0, 7]$、$R_2 \in [8, 15]$、$R_3 \in [16, 31]$、$R_4 \in [32, 63]$、$R_5 \in [63, 127]$、$R_6 \in [128, 255]$，每個區域寬度w為 8、8、16、32、64、128，其藏密量t分別為 3 位元、3 位元、4 位元、5 位元、6 位元、7 位元。秘密訊息是由隨機亂數所組成的 2 進位串流，藉由嵌入位元數的多寡及計算 Peak Signal-to-Noise Ratio (PSNR)值作為兩方法比較的基準，PSNR 值的計算方法如後：

$$\text{PSNR}=10\log_{10}\frac{255^2}{\text{MSE}}\text{dB}，$$

$$\text{MSE}=(\frac{1}{m\times n})\sum_{p=0}^{m-1}\sum_{q=0}^{n-1}(a_{pq}-b_{pq})^2 。$$

其中a_{pq}是掩護影像中的一個像素值，b_{pq}是嵌密後影像的像素值，（p, q）是其座標，$m\times n$表示影像的大小。PSNR 值越小表示藏密前後影像的差距越大，越容易被人類視覺系統發現。

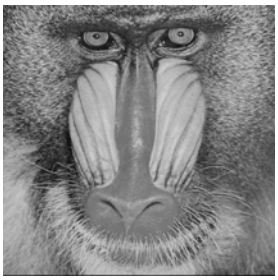
（一）藏密效能實驗

圖一為本次實驗所使用之掩護影像，圖二中（a）（c）（e）（g）為使用 PVD 藏密法嵌入訊息後所產生的影像；（b）（d）（f）（h）為使用本文方法(PVD 藏密法與 1 位元的模數函式藏密法，簡稱為 P-M-1 法)嵌入祕密訊息後所產生的影像。本文方法 P-M-1 法與 PVD 方法的比較如表一。

表一：本文方法 P-M-1 法與 PVD[6]方法比較表

	PVD法[6]		**P-M-1法**	
掩護影像	藏密容量 (bits)	PSNR值 (dB)	藏密容量 (bits)	PSNR值 (dB)
Lena	409810	41.11	540882	40.55
Baboon	457105	36.99	588177	36.69
Couple	421723	39.55	552735	39.17
Peppers	407643	40.93	538715	40.32

（a）Lena



（b）Baboon

（c）Couple

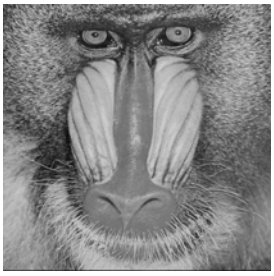
（d）Peppers

圖一：本文實驗所用的原圖

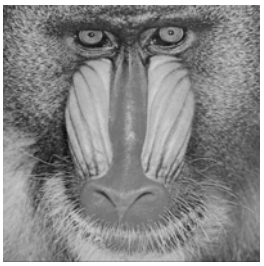
表一的實驗結果中，因為 PVD 藏密法是依據每個子區塊內，相鄰像素差值來決定藏密量的多寡；故針對每張掩護影像特性的不同，藏密量亦有所出入。本文的方法因混合 PVD 藏密法及模數函式藏密法，所以也會隨著不同的掩護影像，有不同的藏密量。但藏密量始終會與 PVD 藏密法保持一定位元數的差距。以本方法中 P-M-1 法為例，在第一階段以 PVD 藏密法嵌入祕密訊息時，共可分為 512*512/2 個子區塊。在第二階段以模數函式藏密法嵌入祕密訊息時，每個子區塊會再嵌入 1 位元的密文；故表一的實驗結果中顯示，在相同的掩護影像下，P-M-1 法可比 PVD 藏密法多嵌入 131,072 位元的密文。

（a）PSNR=41.11

（b）PSNR=40.55



（c）PSNR=36.99



（d）PSNR=36.69

（e）PSNR=39.55

（f）PSNR=39.17

（g）PSNR=40.93

（h）PSNR=40.32

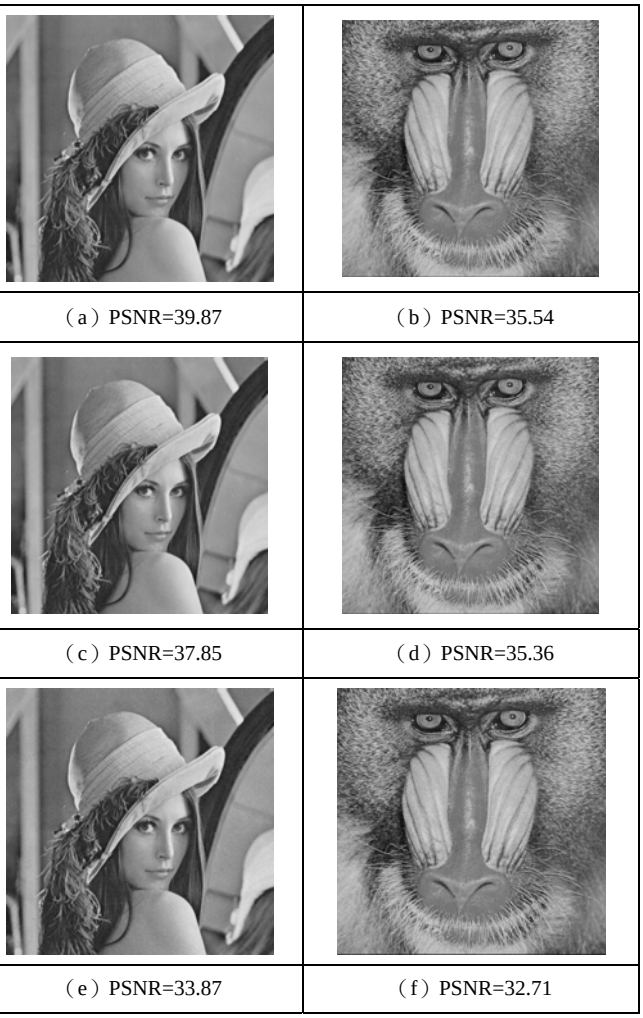
圖二：（a）（c）（e）（g）使用PVD藏密法嵌入訊息，（b）（d）（f）（h）為使用本文P-M-1方法嵌入秘密訊息

表二：本文所提方法藏密後結果

	P-M-2法		**P-M-3法**	
掩護影像	藏密容量 (bits)	PSNR值 (dB)	藏密容量 (bits)	PSNR值 (dB)
Lena	671954	39.87	803026	37.85
Baboon	719249	36.45	850321	35.36
Couple	683867	38.65	814939	36.98
Peppers	669787	39.6	800859	37.55

	P-M-4法	
掩護影像	藏密容量 (bits)	PSNR值 (dB)
Lena	934089	33.87
Baboon	981393	32.71
Couple	933337	33.48
Peppers	931931	33.56

圖三中（a）（b）使用 P-M-2 法，（c）（d）使用使用 P-M-3 法，（e）（f）使用使用 P-M-4 法，藏密後之結果如表二。



（a）PSNR=39.87　（b）PSNR=35.54

（c）PSNR=37.85　（d）PSNR=35.36

（e）PSNR=33.87　（f）PSNR=32.71

圖三：運用本文P-M-2法、P-M-3法、P-M-4法藏密後之影像

(二)安全性實驗

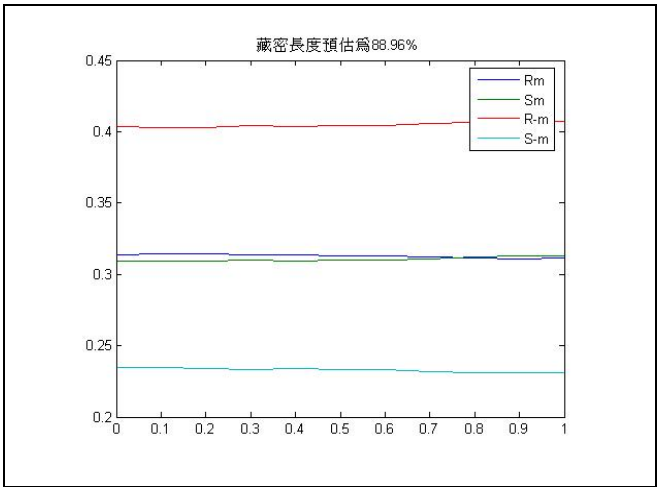
PVD法除了有針對影像特徵來決定藏密量多寡針的特性外，另在安全性方面提出其可抵抗RS偵測法[7]，並有實驗數據證明。針對安全性方面，我們嘗試將本方法所產出的偽裝影像利用RS偵測法加以攻擊。RS 偵測法為Fridrich等學者於2001 年提出的藏密分析法，對LSB 取代藏密法均有良好的偵測效果。假設一張藏密影像其嵌入的秘密訊息長度為p(嵌入的百分比值表示)，RS 偵測法可經由其方法內的藏密量關係式及藏密量計算式估測出其藏密的長度，一般自然影像的藏密預估值約小於正負5%，若預估值大於正負5%則被歸類為可疑的影像。

Wu等學者在2005年基於PVD法與LSB替代藏密法提出新藏密法[8]，以下稱為PVDLSB，其藏密數量優於PVD法，但文章中對安全性方面並無探討。在本節中我們將PVDLSB法實現，因其藏密量與偽裝影像品質與本方法所提之P-M-3法相當，故將本法中P-M-3法與PVDLSB法在藏密效能上做比較，並利用RS偵測法[7]對上述兩種方法的偽裝影像做攻擊，表三為本方法P-M-3法與PVDLSB法的比較表。

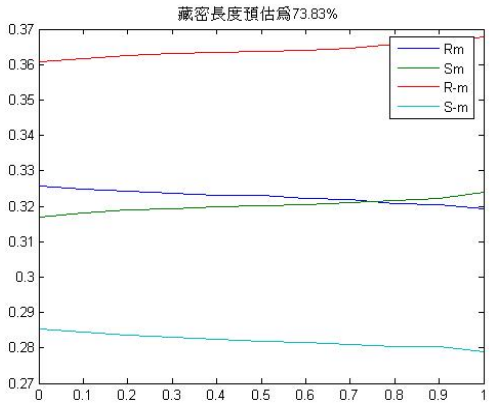
表三：本文方法 P-M-3 法與 PVDLSB[8]方法比較表

	PVDLSB法[8]		**P-M-3法**	
掩護影像	藏密容量 (bits)	PSNR值 (dB)	藏密容量 (bits)	PSNR值 (dB)
Lena	765985	37.13	803026	37.85
Baboon	717946	35.26	850321	35.36
Couple	776160	36.60	814939	36.98
Peppers	775569	36.82	800859	37.55

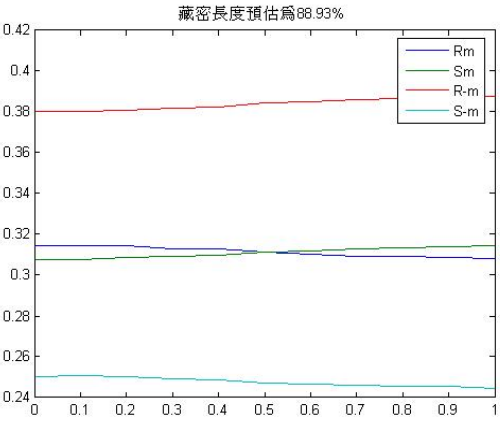
表三中顯示，本方法的P-M-3法，無論在藏密量與偽裝影像的品質上都優於PVDLSB法。對PVDLSB法與本方法實施RS偵測法攻擊結果如圖四。



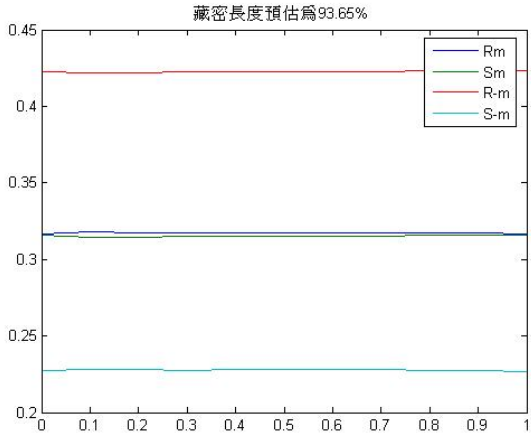
（a）Lean影像藏密後預估藏密量為88.98%



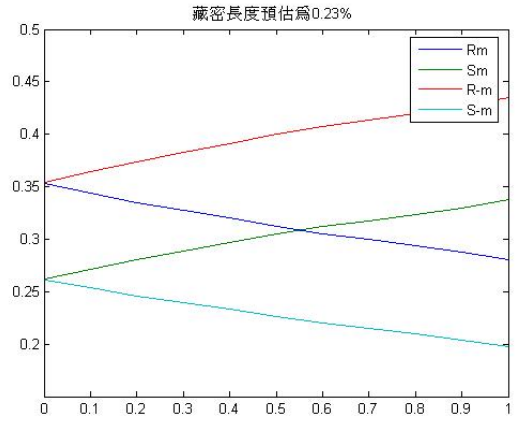
（b）baboon影像藏密後預估藏密量為73.83%



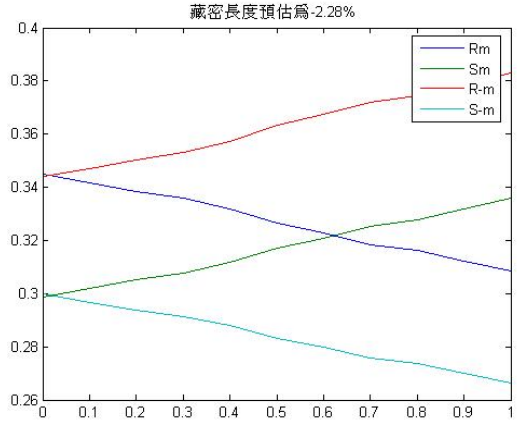
（c）couple影像藏密後預估藏密量為88.93%



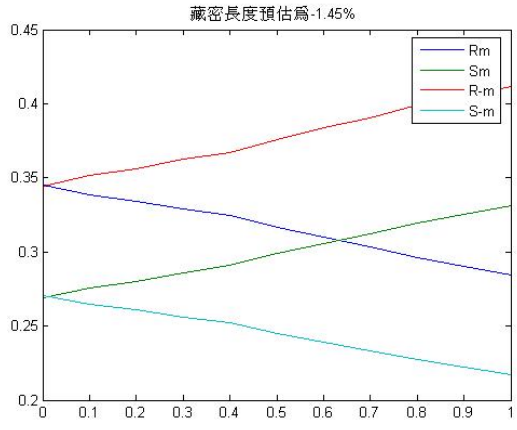
（d）peppers影像藏密後預估藏密量為93.65%



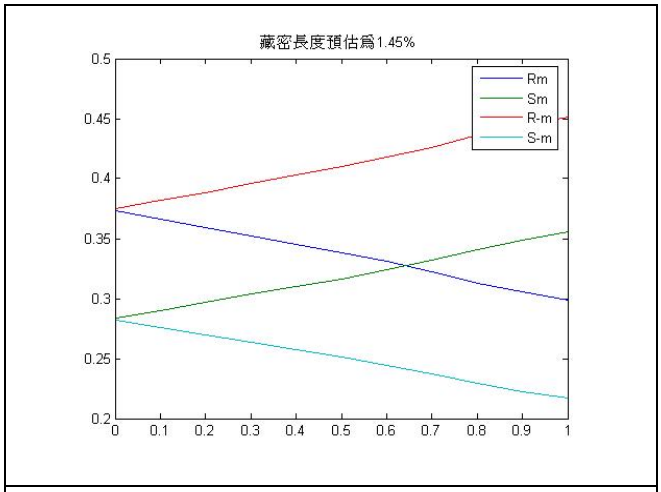
（e）Lean影像藏密後預估藏密量為0.238%



（f）baboon影像藏密後預估藏密量為-2.26%



（g）couple影像藏密後預估藏密量為-1.45%



（h）peppers影像藏密後預估藏密量為1.45%

圖四：運用RS偵測法攻擊PVDLSB法偽裝影像之結果為（a）（b）（c）（d），攻擊P-M-3法偽裝影像之結果為（e）（f）（g）（h）

（三）實驗結果分析

由表一中的實驗結果可得， P-M-1法藏密後的影像品質約略與PVD方法藏密後影像相等，但藏密容量卻多可出4分之1以上。依實驗結果分析，以Lena影像為例，PVD方法在每個子區塊，平均藏密量為3.12位元，而使用P-M-1法，因為本方法混合兩種不同的藏密方法，且讓其可同時於存在於同一子區塊中而不互相干擾，故每個子區塊可較PVD方法多1位元的藏密量。PVD藏密法的藏密容量會隨著影像的複雜度而增減，但不論PVD藏密法針對本文中掩護圖像藏密量為多少，本方法P-M-1法均會比其多出131,072位元的藏密容量。

表二的實驗結果分別顯示P-M-2法、P-M-3法、P-M-4法，每個藏密子區塊分別可比PVD藏密法多2、3、4位元的藏密容量。在人類視覺可容許的範圍內，可持續增加藏密容量。在表二中P-M-4法的實驗結果顯示較PVD方法多出1倍以上的藏密容量且其影像品質仍維持在32至34 dB之間。

就安全性方面，由圖四可看出PVDLSB法雖然在藏密量與偽裝影像的品質上均有不錯的表現，但由於其較PVD方法增加的藏密量，係由LSB藏密法而得，故無法抵擋RS偵測法的攻擊，4個偽裝影像在RS偵測法的預估下，其預估藏密量均遠超過正負5%。而本文所提之P-M-3方法，其4個偽裝影像在RS偵測法的預估下，其藏密量均未超過正負5%，可成功抵擋RS偵測法的分析攻擊。

(四)應用模式討論

本方法除在藏密量、影像品質與安全性有不錯的表現外，其結合兩種完全不同的藏密法之特性，或許亦可衍生出相關應用。舉例來說：潛伏在敵後的情報人員，情資的傳送不易，欲將加密後的兩份情報資訊傳送回國，而其中一份的資訊為機密、另一份為極機密，即可利用此本文方法將兩份情報資訊利用不同之藏密法嵌入一張影像內，掩護影像傳送回國後，權限較高的單位可以擷取兩份密文，權限較低者則只能擷取出一份密文，讓一張影像所嵌入的密文以階層式分享。

五、結論

在這篇文章中，我們提出了一個新的混合式藏密方法，相較於PVD藏密法，新方法在相同的影像品質下可藏入更多的秘密訊息。利用藏密區塊內兩像素值的位移，使PVD藏密法與模數函數藏密法兩種方法間可以同時使用，讓同一影像區塊中存在兩種藏密方法而不相衝突。另在安全性方面，相較於PVDLSB法，本方法之P-M-3法不僅在藏密效能上優於PVDLSB法，亦可成功的抵擋RS偵測法的分析攻擊。

未來將針對本方法的安全性及是否有其他應用做進一步研究，在安全性方面，將實驗證明是否可以抵擋其他已發表的藏密偵測法。在其他應用方面，將探討是否可利用本方法的混合式的特性發展出其他的應用模式。

六、誌謝

本研究為中華民國行政院國家科學委員會專題研究計畫部分成果，計畫編號：NSC 98-2221-E-182-066-MY2。

七、參考文獻

[1] A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” *Proceedings of the 3rd International Workshop on Information Hiding*, Dresden, Germany, Sep. 28 - Oct. 1, 1999, pp. 61-76.

[2] C.-C. Thien and J.-C. Lin, “A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function,” *Pattern Recognition*, vol. 36, pp. 2875-2881, Dec. 2003.

[3] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, “Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488-497, Sep. 2008.

[4] C.-K. Chan and L.-M. Cheng, “Hiding data in images by simple LSB substitution,” *Pattern Recognition*, vol. 37, pp. 469-474, March 2004.

[5] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, “A high quality steganography method with pixel-value differencing and modulus function,” *Journal of Systems and Software*, vol. 81, no. 1, pp. 150-158, 2008.

[6] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letters*, vol. 24, pp. 1613-1626, June 2003.

[7] 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,” *IEE Proceedings – Vision Image and Signal Processing*, vol. 152, pp. 611-615, Oct. 2005.

[8] J. Fridrich, M. Goljan, and R. Du, “Reliable detection of LSB steganography in grayscaleand color images,” *Proceedings of ACM, Special Session on Multimedia Security and Watermarking*, Ottawa, Canada, Oct. 5, 2001, pp. 27-30.

[9] R-.Z. Wang, C.-F. Lin, and J.-C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” *Pattern Recognition*, vol. 34, pp. 671-683, March 2001.

[10] S. Walton., “Image authentication for a slippery new age,” *Dr. Dobb’s Journal of Software Tools for Professional Programmers*, vol. 20, pp. 18-26, 1995.