適用於整合像素差值及最低位元取代法之資訊隱藏分析技術

劉興漢[1*] 劉江龍[2]

[1]國防大學管理學院資訊管理學系
[2]國防大學理工學院電機電子工程學系

摘　　要

自從 911 事件發生後，資訊隱藏及偵測技術成為各國國防安全上的熱門研究課題。以像素差值為基礎的藏密法(PVD-Based Steganography)可有效的在影像中藏入大量祕密訊息，但其在像素差值的直方圖上卻有不正常的分佈。本論文提出可有效偵測整合像素差值法與最低位元取代法所產生藏密影像之偵密技術，主要是透過像素差值直方圖的比率關係來進行特徵值的擷取，並利用倒傳遞類神經網路進行分類，以分辨是否為藏密影像。實驗結果證明，本文所提出之偵測技術對整合 PVD 與 LSB 藏密法的偵測正確率達 99%以上，與 2010 年 Pevný 學者提出之偵測方法所提供 76.8%偵測率比較，可有效提升對整合 PVD 與 LSB 藏密法之藏密影像的偵測正確率，適合國防安全上之應用。

關鍵詞：資訊隱藏，藏密學，資訊隱藏分析技術，像素差值直方圖

Specific Steganalysis for Detection Integrating Pixel-Value Differencing and LSB Replacement Schemes

Hsing-Han Liu[1*] and Chiang-Lung Liu[2]

[1] *Department of Information Management, Management College, National Defense University*
[2] *Department of Electrical and Electronic Engineering, Chung-Cheng Institute of Technology, National Defense University*

ABSTRACT

Information hiding and steganalysis have become hot research topics in the field of national defense security after the 911 tragedy. The PVD-Based Steganography (PBS) can effectively hide large amount secret message in an image. However, the histogram of the pixel-value differencing appears abnormal distribution. In this paper, we propose a steganalysis method which can effectively detect the stego images created by integrating PVD and LSB steganography. The proposed method uses the ratio of pixel-vale differencing to extract the image feature. The image feature is then classified by Back-Propagating Neural Network. Experimental results show that the accurate detection rate of the proposed steganalysis method to PBS is above 99% and outperform the performance of 76.8% provided by the method proposed by Pevný et al. in 2010. Therefore, the proposed steganalysis method can effectively improve the detection rate for detecting the stego images created by integrating PVD and LSB steganography and is practical for applications of national defense security.

Keywords: information hiding, steganography, steganalysis, pixel-value differencing

文稿收件日期 104.08.20;文稿修正後接受日期 105.01.13; *通訊作者
Manuscript received August 20, 2015; revised January 13, 2016; * Corresponding author

一、前　言

由於智慧型手機、電腦及相關產業技術的進步，再加上 Wi-Fi 無線區域網路裝置的佈建越來越普及化，使得往常需要藉由人力的資料運送方式，已進步成只需透過網路即可傳遞數位資料。但這如此方便的環境就像雙面刃，若有心人士企圖利用此便利的環境竊取機密或有價值的資訊，對個人或機關所造成的危害將無法估計。為了保護個人或團體的重要資訊，可藉由密碼學(Cryptograghy)的資料加密技術[1]，以確保其機密性(Confidentiality)。但由於資料加密技術的過程會針對原始資料內容進行處理，使其成為不具意義的亂碼，反而成為已加密文件的重要特徵，引導不法人士針對此一部分進行破解或破壞，造成加密後資訊在安全上的另一項隱憂。為了解決此問題，資訊隱藏技術(Information Hiding)因此興起。

資訊隱藏可將機密資訊嵌入於特定媒體內，產生隱含機密的影像或聲音等載體(Carrier)，以避免機密被不法人士所察覺，進而達到保護機密資訊不會遭到破解、破壞或竊取之目的。資訊隱藏技術依其運用目的之差異，可區分為兩種重要類型。第一種是為了確保影像完整性所發展出的數位浮水印技術(Watermarking)，其是在不影響載體完整性(Integrity)下，進行保護訊息的嵌入(Embedding)，達到保護智慧財產權的目的；第二種是為進行祕密通訊所發展出來的藏密技術(Steganography) [2]，其主要作法是將欲傳遞的祕密訊息嵌入掩護載體(Cover Carrier)中，以躲避有心人士的察覺，而合法接收者在取得已藏密的偽裝載體(Stego Carrier)後，則可依取密程序取出祕密訊息。

無線網路的高度普及化與資訊科技的快速發展提供了藏密技術良好的研發環境，而數位影像則因具有大量散佈、容易取得、及有龐大的藏密空間等特性，已成為最普遍使用的掩護載體[3]。一般而言，好的影像藏密技術須能符合不可察覺性(Imperceptibility)與高資訊負載(Payload)的要求[4]。所謂不可察覺性，是指被嵌入祕密訊息之藏密影像(Stego Image)不可顯現出人類視覺系統或統計上可發覺到的人工失真(Artificial Distortion)；而高資訊負載則是為了滿足傳輸大量祕密訊息之需求。密碼學與藏密技術在祕密通訊之實務上屬相輔相成，為增加祕密通訊的安全性，欲傳送的祕密訊息常經過密碼學技術加密後，再嵌入載體影像(Cover Image)後傳送，其關係如圖 1 所示。

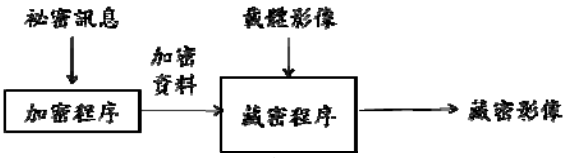

圖 1. 密碼學與藏密技術之關係圖。

藏密技術依據藏密空間的選擇，可區分為轉換域及空間域技術。轉換域技術是先將載體影像透過頻率轉換，在特定的頻帶中進行藏密，一般使用的轉換技術有離散餘弦轉換(Discrete Cosine Transform, DCT) [5, 6]、離散小波轉換(Discrete Wavelet Transform, DWT) [7, 8]及離散傅立葉轉換(Discrete Fourier Transform, DFT) [9]等；空間域藏密技術的作法則是直接針對原始像素值進行修改，以達到藏密的目的。由於在相同失真率要求下，轉換域藏密技術可供嵌入的藏密量較空間域藏密技術為少，因此學者多數致力於空間域藏密技術的研發。

空間域藏密技術最常使用影像像素最不重要的位元(Least Significant Bit, LSB)來進行訊息嵌入，稱為最不重要位元取代藏密法[10]，簡稱為 LSB 藏密法。由於 LSB 藏密法已被 RS 偵測技術[11]或 x^2 攻擊法[12]等統計式的分析技術所破解，因此許多學者提出 LSB 藏密的改進方法[13, 14]。相較於 LSB 藏密法，像素值差異藏密法(Pixel Value Difference, PVD)藏密法[15]的藏密量較高，且可有效避免被 RS 統計分析技術所破解，因此近年來以 PVD 為基礎的藏密技術[16-20]成為熱門的研究領域。

雖然藏密技術可隱藏訊息的存在，進而確保機密資訊的安全，但「水可載舟，亦可覆舟」，恐怖組織亦可能利用各種不同的藏密技術傳遞不法訊息，危害國土安全。根據美國中情局及相關單位的研究，發現發動 911 恐怖攻擊事件的蓋達組織，很有可能透過藏密技術來進行情報的傳送[21-23]；另外德國當局在其所破獲的恐怖分子嫌犯的偽裝色情檔案中，也發現了國際恐怖組織隱藏其中的上百份祕密文件[24]。上述案例不但說明藏密技術已被用於非法應用，更顯示發展藏密分析技術(Steganalysis)之重要性與急迫性。藏密分析技術除了可察覺藏密技術是否遭到不法應用外，其也可用來檢視藏密技術對攻擊的抵抗

力，有助於安全藏密技術之發展，已成為多媒體安全領域的熱門研究課題。

藏密分析技術依偵測藏密法的種類，可分為特定藏密分析(Specific Steganalysis)及通用藏密分析(Universal/Blind Steganalysis)等兩大技術。前者針對特定藏密演算法所引發的特徵進行設計，由於已知藏密演算法於嵌入過程中對載體影像所造成的影響，所以特定藏密分析技術通常具有極佳的偵測正確率；後者在未知所分析的可疑影像所應用的藏密演算法的情形下，將受測影像從空間域轉換至不同領域後，擷取有效之特徵，並經由分類器的訓練與學習，亦可提供可靠的偵測正確率。

由於以 PVD 為基礎的藏密法[16-20]陸續被提出，而針對以 PVD 為基礎的藏密法之偵測技術[25-29]亦陸續發表，但未有學者針對 Yang 等學者[20]提出的整合像素差值法及最低位元取代法之影像藏密技術進行分析。故本研究旨在針對 Yang 等學者提出的藏密技術，藉由擷取其像素差值直方圖(Pixel Difference Histogram, PDH)之特徵，並結合倒傳遞類神經網路 (Back-Propagating Neural Network, BPNN)[30]的分類能力，區分載體影像與整合 PVD 與 LSB 藏密法所產生的藏密影像。由於本研究只針對 Yang 等學者[20]的方法，故屬於特定藏密分析技術，其貢獻在於提出 4 項有效特徵與提供極佳的偵測正確率。

本文其餘章節安排如下：第 2 節概述與本研究有關的相關文獻；第 3 節說明本研究所提出的方法；第 4 節是與本研究所提出偵測技術相關之實驗及討論；最後於第 5 節提出結論。

二、文獻探討

本節探討與本研究相關之文獻。首先探討 Wu 等學者所提出之像素值差異資訊隱藏技術；其次探討其他相關的 PVD 改進技術、針對像素值差異藏密法的特定藏密分析技術的發展；最後探討倒傳遞類神經網路。

2.1 Wu 等學者的方法

Wu 與 Tsai 等學者在 2003 年提出像素值差異藏密技術(PVD)[15]，並成為近期熱門的藏密演算法。PVD 藏密技術是將影像劃分為兩兩相鄰且不重疊的像素對後，再進行其像素差值的計算。假設像素對之像素值分別是 P_i 及 P_{i+1}，而其像素差值 d 即為 $P_{i+1} - P_i$。並定義像素差值的絕對值 R_k，可用來對像素差值進行區分，並可得嵌入祕密訊息的二進位位元數 n 與區間上下限值 u_k 和 l_k，如表 1 所示。

表 1. PVD 嵌入訊息範圍區分表

K	1	2	3	4	5	6
R_k	0~7	8~15	16~31	32~63	64~127	128~255
n	3	3	4	5	6	7
u_k	7	15	31	63	127	255
l_k	0	8	16	32	64	128

PVD 藏密技術依據表 1 所對應之 n 值，計算嵌入訊息 b 之十進位值，並加上區間的下限值 l_k，可得新的像素差值 d'，如式(1)所示：

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

最後，將新舊像素差值之差異(d' - d)，平均分至P_i及P_{i+1}像素，可得藏密後的像素值 P_i' 及 P_{i+1}'，如式(2)所示：

$$(P_i', P_{i+1}') = \begin{cases} (P_i - \left\lfloor \frac{d'-d}{2} \right\rfloor, P_{i+1} + \left\lceil \frac{d'-d}{2} \right\rceil), \text{當} d \text{為偶數} \\ (P_i - \left\lceil \frac{d'-d}{2} \right\rceil, P_{i+1} + \left\lfloor \frac{d'-d}{2} \right\rfloor), \text{當} d \text{為奇數} \end{cases} \quad (2)$$

在祕密訊息擷取部分，PVD藏密技術先將藏密影像切割成兩兩相鄰且不重疊的像素對，再計算像素對內像素值P'_i及P'_{i+1}的差值d'，然後依其差值大小區分藏密區間的上下限值u_k和l_k，再利用像素差值減去(或加上)下限值即可取出祕密訊息b，如式(3)所示：

$$b = \begin{cases} d' - l_k, & \text{當} d \geq 0 \\ d' + l_k, & \text{當} d < 0 \end{cases} \quad (3)$$

2.2 相關的 PVD 改進技術

2005 年，Wu 等學者[16] 基於原始 PVD，發表了結合 LSB 與 PVD 的藏密法(本研究稱為 Enhanced PVD)，透過門檻值(相鄰像素間的差值等於 15)的設定，選擇嵌入祕密訊息的方法。若門檻值小於或等於 15，表示欲嵌入的影像像素屬於較平滑的區域，無法容許較大的失真，使用 LSB 藏密法進行祕密訊息的嵌入；若門檻值大於 15，表示欲嵌入的影像像素為較複雜區域，可容許較大的失真，則使用原始

PVD 藏密法，藉此增加藏密法的嵌入量。

2008 年，Yang 等學者[17] 提出高藏密量的 PVD 藏密法(本研究稱為 Adaptive PVD)，其使用與原始 PVD 藏密法相同的區間表，並將相鄰像素間差值劃分為低級、中級與高級等三個區間，針對位於不同區間的像素，分別使用 LSB 藏密法嵌入 3、4 及 5 個位元的祕密訊息，藉此增加藏密量。

2008 年，Chang 等學者[18]為有效增加藏密量及改善像素值邊界溢出問題，提出改進的 PVD 藏密法，稱為三方 PVD 藏密法(Tri-way PVD, TPVD)。其將用於藏密的像素區塊大小由 1×2 更改成 2×2，並計算 4 組相鄰像素間的差值，藉由 2 組條件式判斷，決定 4 組像素是否符合 TPVD 嵌入狀況。若其中一組條件式成立，使用原始 PVD 藏密法將祕密訊息嵌入第 1 及第 3 像素對；若 2 組條件式均不成立，則用 TPVD 將祕密訊息嵌入前 3 組像素對。

2008 年，Wang 等學者[19]提出使用模數運算的 PVD 藏密法，稱為 Modulus PVD。其仍使用與原始 PVD 藏密法相同的區間表，但利用模數運算修改相鄰像素的餘數，以縮小嵌入訊息後新舊像素值的差異。與原始 PVD 法比較，在相同的藏密量下，其可有效改進藏密影像的品質。

2012 年，Yang 等學者[20]提出整合像素差值法及最低位元取代法之影像藏密技術，稱為整合 PVD 與 LSB 藏密法。其藏密法與 Wu 等學者[15]提出的原始 PVD 方法相同，亦是利用修改兩個相鄰且不重疊的像素 P_i 及 P_{i+1} 之間的像素差值為基礎，計算出新的像素差值後，可得到新像素值 (P_i', P_{i+1}')。然後判斷 P_{i+1}' 像素的 LSB 值(令其為 r)是否與接續要隱藏的 1 位元資料(令其為 u)相同，此時會產生下列 4 組狀態：(r,u)=(0,0)、(0,1)、(1,0)或(1,1)。當 r 與 u 的值相同時，此時可視為已將要接續隱藏 1 位元資料嵌入 P_{i+1}'，完成這組像素的資訊隱藏動作。而當 r 與 u 的值不相同時，可分為以下情況處理。當(r,u)=(0,1)時，r 值將被修正為 1，故將 P_{i+1}'的像素值減 1，此時為了維持新的像素差值，故將 P_i' 的像素值同步減 1。當(r,u)=(1,0)，r 值將被修正為 0，故將 P_{i+1}'的像素值加 1，此時亦為了維持新的像素差值，故同步將 P_i' 的像素值加 1，完成這組像素的資訊隱藏動作。Yang 等學者提出的整合 PVD 與 LSB 藏密法與原始 PVD 法比較，可有效增加藏密的資訊量。

2.3 針對像素值差異藏密法的偵測技術

2003 年 Wu 與 Tsai 學者所提的 PVD 藏密法雖可抵抗 RS 偵密技術的攻擊，但 Zhang 等學者[25]指出，經 PVD 藏密後的影像的像素差值直方圖(PDH)會有階梯狀的不自然分佈現象(如圖 2 所示)，形成明顯的特徵，暴露其藏密的事實，並提出以模數運算為基礎的像素值差異藏密法(Modified PVD)，利用模數運算來修改分類區間的上下限值，有效改善藏密影像的 PDH 之階梯分佈狀況。

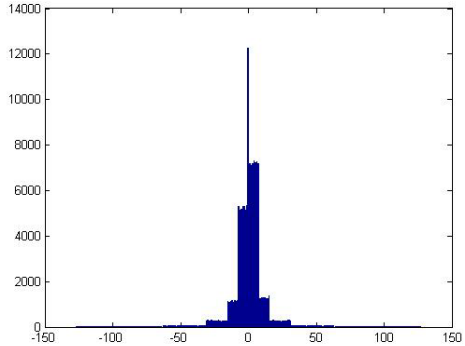

圖 2. PVD 藏密影像的像素差值直方圖。

2005 年 Wu 等學者所發表的 Enhanced PVD 技術，因為結合了 LSB 與 PVD 藏密技術，其 PDH 也會產生不自然階梯狀的分佈現象，因此也無法抵抗相關統計技術的攻擊。2008 年，Joo 等學者[26]提出了針對 Modulus PVD 之偵測技術，其利用藏密前後的 PDH 分佈之差異性進行偵測。2010 年，Sabeti 等學者[27] 將待偵測之影像利用 Modified PVD 藏密法進行二次藏密，取二次藏密前後的 PDH 之差異，提出 21 項明顯之特徵，並利用類神經網路進行藏密偵測。

2010 年，Joo 等學者[28]針對 Modulus PVD 藏密法，使用了曲線擬合法(Curve-fitting Method) 與直方圖逆蹤法 (Histogram Reverse-tracing Method)，定義 3 組特徵值，並針對 3 組特徵值計算個別門檻值，提出改進之偵測方法。2011 年，Zaker 等學者[29]分別利用水平相鄰像素、垂直相鄰像素及對角相鄰像素之像素間的差值進行祕密訊息的嵌入(TPVD)，而從 TPVD 所產生的 PDH 中，發現了屬於不同藏密區間相鄰像素間的差異，可被應用於識別影像是否有藏密，並設計藏密分析演算法。實驗結果顯示，針對 TPVD 藏密影像有不錯的偵測效果。

2.4 倒傳遞類神經網路

McCulloch 及 Pitts 二位學者[31]於 1943 年共同提出結合神經生理學及邏輯數學的神經元模型，開始類神經網路之研究。而更進一步的發展則是由 Rosenblatt[32]於 1958 年所提出的感知器(Perceptron)架構，其成功模擬生物的感知與學習能力，引發了學者對類神經網路的研究風潮。後續因應不同的問題類型，產生出許多不同型態的類神經網路。

Rumelhart 等學者[30]於 1986 年提出倒傳遞類神經網路(BPNN)，其適用於處理複雜的高度非線性函數合成問題。BPNN 是由多層的神經元結構所構成，其中第一層接收輸入變數，稱為輸入層(Input Layer)，中間的神經元稱為隱藏層(Hidden Layer)，而最後產生預測結果的神經元則稱之為輸出層(Output Layer)。隱藏層的功能主要是增加類神經網路的複雜性，以便模擬複雜的非線性關係，BPNN 的架構如圖 3 所示。

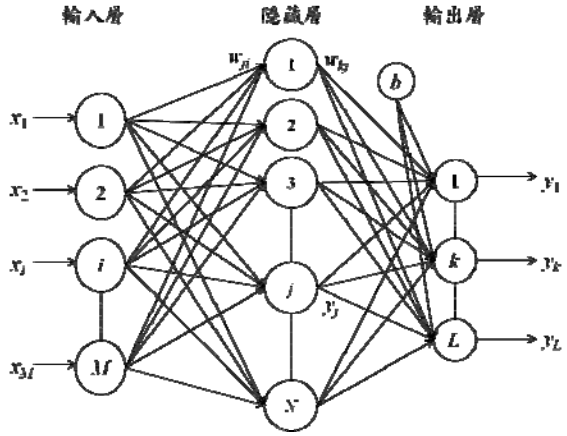

圖 3. 倒傳遞類神經網路架構圖。

BPNN 架構的輸出值為

$$y_k = f\left(\sum_{j=1}^{N} w_{kj} y_j - b_k\right) \tag{4}$$

其中 y_k 為輸出層神經元 k 的輸出值；y_j 為隱藏層神經元 j 的輸出值；$f(\bullet)$為非線性轉移函數；w_{kj} 為隱藏層神經元 j 與輸出層神經元 k 之間的權重值；b_k 為輸出層神經元 k 的偏權值。

由於 BPNN 屬於監督式學習網路，針對每筆輸入資料，都有其相對應的目標輸出值(d_k)可供比對。故在每次迭代的過程中，均會計算網路輸出值(y_k)與目標輸出值(d_k)之間的均方差(Mean Square Error, MSE)

$$e(t) = \frac{1}{2}\sum_{k}\left(d_k(t) - y_k(t)\right)^2 \tag{5}$$

BPNN 調整網路連結權重的學習法則是利用最陡坡降法找尋最小的瞬時目標函數值。假設目標函數值為目標輸出值與 BPNN 網路輸出值的誤差期望值（即 $e(t)$），則對目標函數微分後得

$$\Delta w_{ji} = \eta \delta_j^n y_i^{n-1} \ , \tag{6}$$

其中

$$\delta_j^n = -\frac{\partial e}{\partial net_j^n} \ 。 \tag{7}$$

在每一次學習的過程中，可利用式(6)進行輸入層與隱藏層間或隱藏層與輸出層間的神經元之權重值與偏權值的調整，直到網路輸出值達到容忍誤差值標準或學習迭代的次數達到設定的最大值。

三、本偵測技術

本節提出可偵測 Yang 等學者[20]提出的整合 PVD 與 LSB 藏密法之偵測技術(以下稱為本偵測技術)，其主要是針對藏密後的藏密影像之 PDH 特徵為基礎，結合 BPNN 分類器進行藏密偵測。本節首先分析 Yang 等學者提出的整合 PVD 與 LSB 藏密法在嵌密過程中所產生之 PDH，其次闡述本偵測技術針對 Yang 等學者提出的整合 PVD 與 LSB 藏密方法所提出之特徵值，最後則說明本技術之偵測流程。

3.1 整合 PVD 與 LSB 藏密法之分析

由於 Yang 等學者[20]提出的整合 PVD 與 LSB 藏密技術，其藏密演算法仍是以原始 PVD 法為主，先藉此完成第一階段祕密訊息的嵌入後，再輔以 LSB 藏密法多嵌入 1 個位元的祕密訊息。故其藏密影像的 PDH 與原始 PVD 的 PDH 相同，將會由原本的自然分佈改變成不自然的階梯狀分佈(如圖 4 所示)。

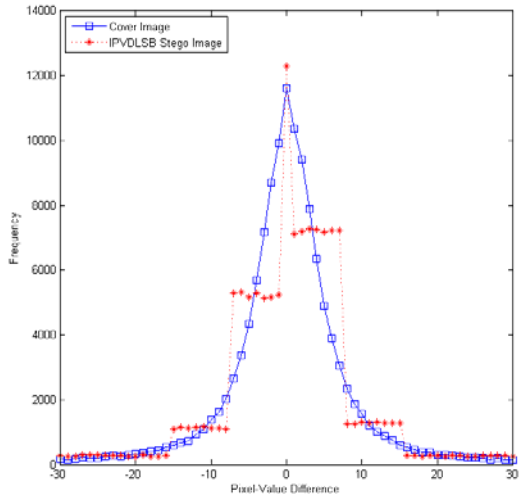

圖 4. 載體影像與藏密影像像素差值直方圖。

為了找出適用於整合 PVD 與 LSB 藏密法的藏密特徵，本偵測技術將載體與藏密影像區分為兩兩相鄰且不重疊的像素對，再進行其像素差值的計算，可得到載體影像與藏密影像之像素差值直方圖(PDH)。再比對載體與藏密影像的 PDH，找出其相異特徵，以作為有效區分載體與藏密影像之基礎，其特徵比對流程如圖 5 所示。

圖 5 為載體與藏密影像差值直方圖比對流程，在此流程中，藉由比對載體與藏密影像差值直方圖的差異，建構本研究所需的 4 項特徵，並經由擷取大量載體影像及其相對應的藏密影像之 4 個特徵值，於 BPNN 分類器進行訓練，可得已完成訓練之模型。而在影像偵測階段，接收端(或偵測者)只要有此訓練模型，針對受測影像擷取出相同的 4 個特徵值，即可進行分類，故在此階段接收端(或偵測者)並不需要事先知道受測影像是載體或藏密影像，亦不需要原本的載體影像。

依圖 5 的流程，可得載體影像與整合 PVD 與 LSB 藏密法所產生的藏密影像之 PDH，如圖 6 與圖 7 所示。從圖 6 與圖 7 可明顯觀察出載體影像與整合 PVD 與 LSB 藏密法所產生的藏密影像之 PDH 有明顯的差異，可藉此建構出有用的特徵。

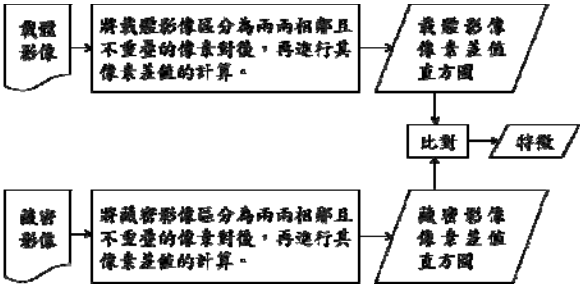

圖 5. 載體與藏密影像差值直方圖比對流程圖。

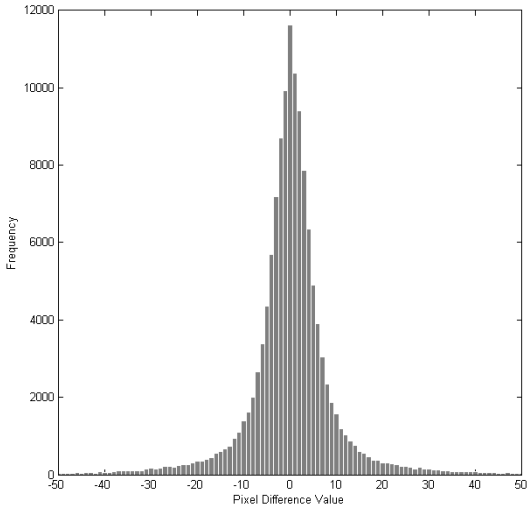

圖 6. 載體影像的像素差值直方圖。

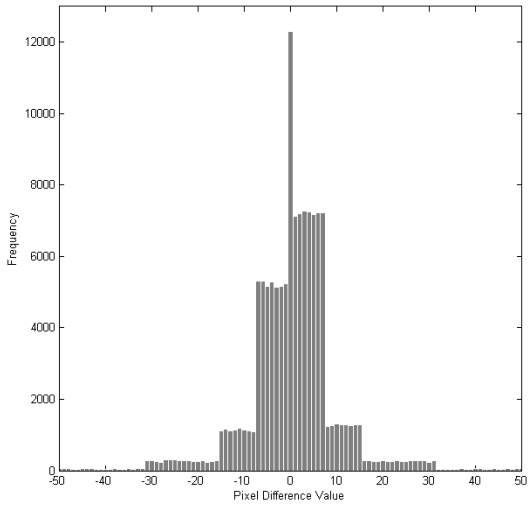

圖 7. 藏密影像的像素差值直方圖。

3.2 本偵測技術使用之特徵值

由於祕密訊息嵌入的緣故，載體影像的 PDH 產生了不正常的階梯狀分布(如圖 7 所示)。而為了便於說明本偵測技術提出的特徵，PD 值為-15 至 15 的 PDH 示意圖如圖 8 所示，其中 P_{peak} 代表 PDH 的峰值；P_x 代表正

的像素差值，本技術提出特徵所計算的範圍為 1 至 7；P_{-x} 代表負的像素差值，本技術提出特徵所計算的範圍為-1 至-7。

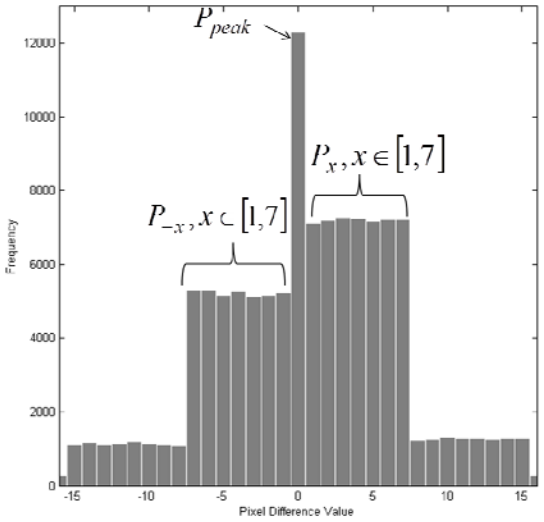

圖 8. PD 值範圍為-15 至 15 的 PDH 示意圖。

本偵測技術以 PDH 之 PD 比率關係作為整合 PVD 與 LSB 藏密法藏密之 4 項特徵，整理如表 2 所示。

以下分別針對 F_1 至 F_4 特徵的特性進行說明。特徵 F_1 主要是擷取受測影像的 PDH 於差值範圍 1 至 7 的正負區間內正負差值(需相同差值)之差除以正差值的總和，當設定 x=1 到 7 時，其總和最大(如表 3 所示)，表示能有效區別載體與藏密影像，故本研究 F_1 設定為 x=1 到 7 的總和。

特徵 F_2 主要是擷取受測影像的 PDH 於差值範圍 1 至 3 的正負區間內正負差值(需相同差值)之和，並計算其與 PDH 峰值之間的差值，再除以 PDH 峰值的總和，當設定 x=1 到 3 或 x=1 到 4 時，其總和最大(如表 4 所示)，表示能有效區別載體與藏密影像，故本研究 F_2 設定為 x=1 到 3 的總和。其與 F_1 特徵差異在於有將 PDH 峰值納入特徵計算之考量。

特徵 F_3 主要是擷取受測影像的 PDH 於正差值區間(其範圍為 1 至 6)的兩兩差值之差，再除以前一差值的總和，當設定 x=1 到 6 時，其總和最大(如表 5 所示)，表示能有效區別載體與藏密影像，故本研究 F_3 設定為 x=1 到 6 的總和。

特徵 F_4 主要是擷取受測影像的 PDH 於負差值區間(其範圍為-1 至-6)的兩兩差值之差，再除以前一差值的總和，當設定 x=-1 到-6 時，其總和最大(如表 6 所示)，表示能有效區別載體與藏密影像，故本研究 F_4 設定為 x=-1 到-6 的總和。

表 2. 本偵測技術所提之特徵值

特徵值符號	特徵值計算
F_1	$\sum_{x=1}^{7}\frac{P_x - P_{-x}}{P_x}$
F_2	$\sum_{x=1}^{3}\frac{\left((P_x + P_{-x}) - P_{peak}\right)}{P_{peak}}$
F_3	$\sum_{x=1}^{6}\frac{\left(P_x - P_{x+1}\right)}{P_x}$
F_4	$\sum_{x=-1}^{-6}\frac{\left(P_x - P_{x-1}\right)}{P_x}$

表 3. 藏密影像與載體影像特徵值 F_1 與其差值

	x=1-1	x=1-2	x=1-3	x=1-4	x=1-5	x=1-6	x=1-7
Stego_F_1	0.2192	0.4161	0.6245	0.8598	1.0692	1.279	1.497
Cover_F_1	0.0045	0.0179	0.0479	0.0855	0.137	0.2331	0.3145
Difference	0.2147	0.3982	0.5766	0.7743	0.9322	1.0459	1.1825

表 4. 藏密影像與載體影像特徵值 F_2 與其差值

	x=1-1	x=1-2	x=1-3	x=1-4	x=1-5	x=1-6	x=1-7
Stego_F_2	0.0058	1.3067	1.6021	1.6389	1.4342	1.0163	0.5536
Cover_F_2	0.7474	0.0116	0.0219	0.0415	0.0444	0.0629	0.0814
Difference	-0.7416	1.2951	1.5802	1.5974	1.3898	0.9984	0.4722

表 5. 藏密影像與載體影像特徵值 F_3 與其差值

	x=1-1	x=1-2	x=1-3	x=1-4	x=1-5	x=1-6
Stego_F_3	-0.0101	-0.0214	-0.0176	-0.0062	-0.0128	-0.0137
Cover_F_3	0.0933	0.2567	0.4497	0.6798	0.8813	1.099
Difference	-0.1034	-0.278	-0.4674	-0.686	-0.8941	-1.1127

表 6. 藏密影像與載體影像特徵值 F_4 與其差值

	x=-1~-1	x=-1~-2	x=-1~-3	x=-1~-4	x=-1~-5	x=-1~-6
Stego_F_4	0.0135	0.0188	-0.0088	0.0142	-0.0138	-0.0123
Cover_F_4	0.1228	0.2983	0.5051	0.7413	0.964	1.1758
Difference	-0.1093	-0.2795	-0.5139	-0.727	-0.9779	-1.1881

為了說明 F_1 至 F_4 特徵值的有效性，本偵測技術針對實驗所使用的 NRCS 影像資料庫[33]中 2724 張載體影像及相對應的整合 PVD 與 LSB 藏密法之藏密影像進行特徵值擷取，其結果如圖 9 至圖 12 所示，其橫軸為測試影像，而縱軸則代表影像之 F_1 至 F_4 的特徵值。

圖 9 至圖 12 之結果顯示，載體影像的特徵值 F_1 至 F_4 呈現隨機的分佈情形；但對於藏密影像而言，因整合 PVD 與 LSB 藏密技術對於像素值的調整，致使特徵值 F_1 至 F_4 的值呈現群聚現象，故載體影像與藏密影像 F_1 至 F_4 特徵值的分佈呈現兩明顯分隔的群組。

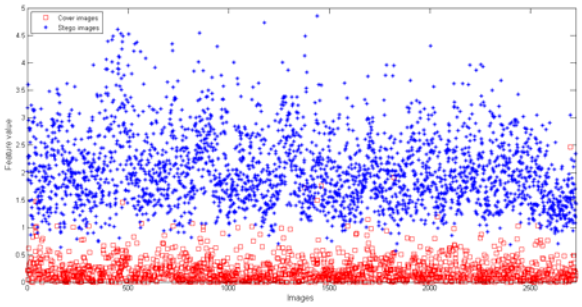

圖 9. 載體影像與藏密影像之 F_1 特徵值分佈圖。

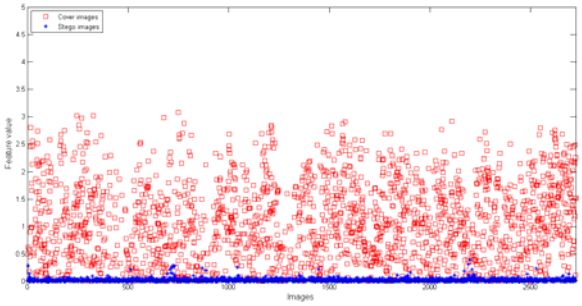

圖 10. 載體影像與藏密影像之 F_2 特徵值分佈圖。

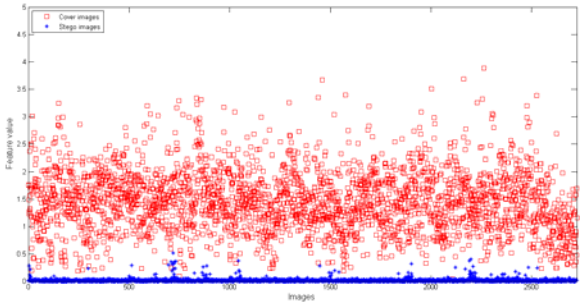

圖 11. 載體影像與藏密影像之 F_3 特徵值分佈圖。

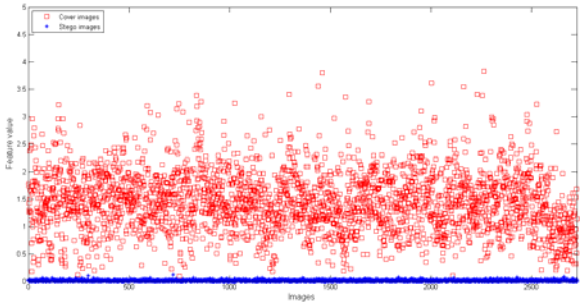

圖 12. 載體影像與藏密影像之 F_4 特徵值分佈圖。

3.3 本研究之偵測流程

本研究主要結合上述之 4 項特徵值與 BPNN 分類器，以偵測受測影像是否為載體影像或為整合 PVD 與 LSB 藏密法之藏密影像，其偵測流程如圖 13 所示。本研究之偵測流程概分為兩大階段，一為分類模型產生階段，一為影像偵測階段，分述如下。

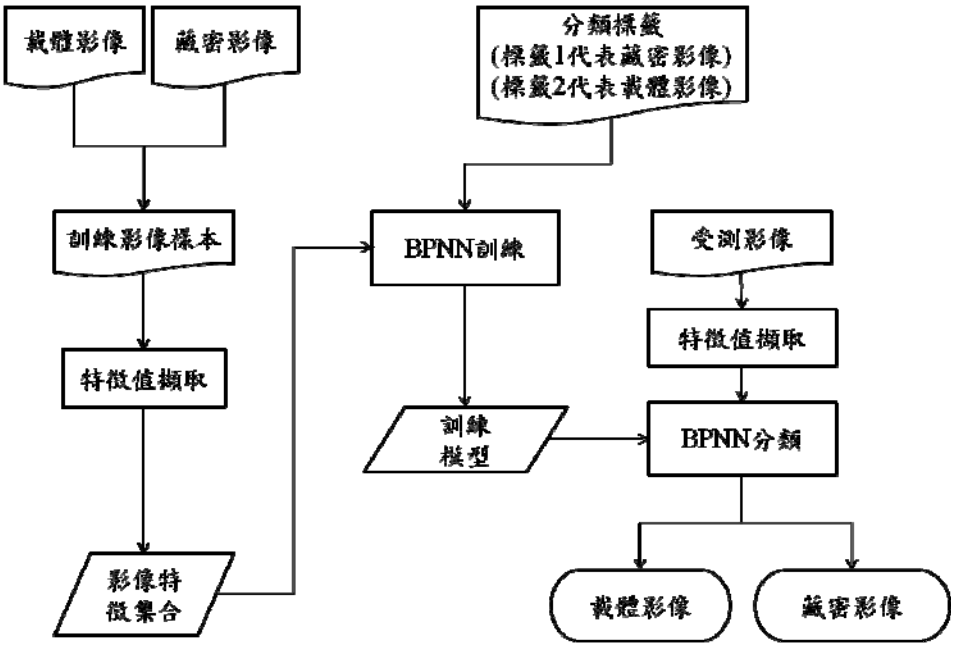

圖 13. 本研究之偵測流程圖。

在分類模型產生階段，本研究利用未藏密的載體影像與經整合 PVD 與 LSB 演算法藏密後的藏密影像作為訓練樣本，並根據本研究所提的 4 項特徵值對所有樣本影像進行特徵值擷取，完成訓練樣本特徵值集合。另外，本研究分別設定藏密影像之分類標籤為 1 而載體影像分類標籤為 2，並將分類標籤與訓練樣本特徵值輸入 BPNN 分類器進行訓練與學習，以產生訓練模型(Trained Model)。

在影像偵測階段，我們亦將受測影像根據本研究所提的 4 項特徵值進行特徵值擷取，並輸入至 BPNN 分類器進行藏密偵測。BPNN 分類器依據已完成訓練的模型對受測影像進行分類，並輸出分類結果。若輸出之標籤為 1，表示為使用整合 PVD 與 LSB 藏密法所產生的藏密影像；若輸出之標籤為 2，表示為載體影像。

四、實驗結果

本節針對本研究所提偵測技術進行實驗，以驗證本研究所提之 4 項整合 PVD 與 LSB 演算法之藏密特徵可以有效偵測整合 PVD 與 LSB 藏密技術。本實驗結果同時與現行的通用偵測技術進行比較，以驗證本偵測技術之效果。相關之實驗環境、步驟、場景及結果分述於以下各節。

4.1 實驗環境

本實驗所採用之軟、硬體實驗環境如下：

(1) 硬體環境：Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz 4GB RAM 桌上型電腦。

(2) 模擬程式：以 MATLAB 實現整合 PVD 與 LSB 藏密技術與特徵值萃取程式。

(3) 祕密訊息：以 MATLAB 內建之亂數產生器產生實驗所需之均勻分佈二位元數值序列，模擬加密後之祕密訊息。

(4) BPNN 分類器：使用 MATLAB 類神經網路工具箱所內建的倒傳遞類神經網路相關指令作為 BPNN 分類器[34]。

(5) 影像資料庫：為驗證本偵測技術提出的 4 項特徵能適用於不同類型的影像資料庫，本研究分別以 NRCS[33]、BOSS[35]及 BOWS2[36]影像資料庫之 2724 張、9074 張及 10000 張 8 位元 512*512 大小之灰階影像做為原始影像，圖 14 顯示其中 BOWS2 影像資料庫其中六張範例影像。並使用整合 PVD 與 LSB 藏密技術，分別針對上述影像資料庫進行藏密，藏生相對應之藏密影像供後續實驗所使用。

圖 14. BOWS2 影像資料庫之範例影像。

4.2 實驗步驟

本研究實驗步驟說明如下：

步驟一：分別輸入受測影像資料庫之載體影像與該受測影像資料庫經整合 PVD 與 LSB 藏密法所產生之藏密影像。

步驟二：從受測影像資料庫之載體影像中，隨機選取半數之載體影像；並從該受測影像資料庫經整合 PVD 與 LSB 藏密法所產生之藏密影像中，選取相對應的藏密影像，組合成訓練影像樣本。

步驟三：利用特徵值擷取程式，分別針對受測影像資料庫所隨機選取的載體影像及相對應的藏密影像進行特徵值擷取。

步驟四：將步驟三所得訓練影像特徵值集合及相對應的分類標籤輸入 BPNN 分類器進行分類訓練，產生訓練模型。

步驟五：從受測影像資料庫之載體影像中，選取剩餘半數載體影像；並從該受測影像資料庫經整合 PVD 與 LSB 藏密法所產生之藏密影像中，選取剩餘相對應的藏密影像，組合成受測影像樣本，並利用特徵值擷取程式進行特徵值的擷取。

步驟六：將步驟四所得之訓練模型及步驟五所得之受測影像的特徵值集合分別輸入 BPNN 分類器進行分類，並記錄其分類結果。

步驟七：重複進行步驟二至六 10 次，並計算分類結果之平均值。

4.3 實驗場景

實驗場景區分為測試不同特徵組合之偵測正確率、相同與不同類型影像資料庫的訓練與測試。

測試不同特徵組合之偵測正確率旨在說明單獨使用某項特徵或是結合 2-3 種特徵與 BPNN 分類器，對於受測影像的偵測正確率是否有影響。本研究以 NRCS 為受測影像資料庫，依不同特徵組合，並依循 4.2 節所述步驟進行實驗。

相同類型影像資料庫的訓練與測試意謂在倒傳遞類神經網路的訓練與測試階段，均使用相同影像資料庫的載體與藏密影像。本研究利用 4.2 節所述實驗步驟，分別針對 NRCS、BOSS 及 BOWS2 影像資料庫之 2724 張、9074 張及 10000 張之灰階影像做為原始影像，並使用整合 PVD 與 LSB 藏密技術產生相對應的 NRCS、BOSS 及 BOWS2 影像資料庫之藏密影像進行藏密偵測。

不同類型影像資料庫的訓練與測試則表示在倒傳遞類神經網路的訓練與測試階段，是使用不同影像資料庫的載體與藏密影像。不同類型影像資料庫之訓練與測試的實驗設定整理如表 7 所示。

表 7. 不同影像資料庫之訓練與測試之實驗設定

訓練影像資料庫	測試影像資料庫
NRCS：分別從 2724 張載體與藏密影像，隨機選擇 2000 張載體與藏密影像，組合成 4000 張訓練影像。	BOSS：分別從 9074 張載體與藏密影像，隨機選擇 5000 張載體與藏密影像，組合成 10000 張測試影像。
	BOWS2：分別從 10000 張載體與藏密影像，隨機選擇 5000 張載體與藏密影像，組合成 10000 張測試影像。
BOSS：分別從 9074 張載體與藏密影像，隨機選擇 5000 張載體與藏密影像，組合成 10000 張訓練影像。	NRCS：分別從 2724 張載體與藏密影像，隨機選擇 2000 張載體與藏密影像，組合成 4000 張測試影像。
	BOWS2：分別從 10000 張載體與藏密影像，隨機選擇 5000 張載體與藏密影像，組合成 10000 張測試影像。
BOWS2：分別從 10000 張載體與張藏密影像，隨機選擇 5000 張載體與藏密影像，組合成 10000 張訓練影像。	NRCS：分別從 2724 張載體與藏密影像，隨機選擇 2000 張載體與藏密影像，組合成 4000 張測試影像。
	BOSS：分別從 9074 張載體與藏密影像，隨機選擇 5000 張載體與藏密影像，組合成 10000 張測試影像。

依表 7 設定好訓練影像樣本後，利用特徵值擷取程式進行特徵值擷取，可得訓練影像特

徵值集合，再與相對應的分類標籤輸入 BPNN 分類器進行分類訓練，產生訓練模型。然後將表 7 所列測試影像樣本，亦利用特徵值擷取程式進行特徵值的擷取，產生測試影像的特徵值集合。將前一步驟所得之訓練模型及測試影像的特徵值集合分別輸入 BPNN 分類器進行分類，並記錄其分類結果。重複進行這些步驟 10 次，並計算分類結果之平均值。

4.4 實驗結果

表 8 至表 12 為依 4.2 節之實驗步驟與 4.3 節之測試不同特徵組合之偵測正確率、相同類型影像資料庫的訓練與測試的實驗場景所得之實驗結果，其中 *AC* 值為偵測正確率，定義如下：

$$AC = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \text{ ，} \quad (8)$$

其中 *TP* 表示受測影像有藏密，而偵測結果有藏密的數目；*TN* 表示受測影像未藏密，而偵測結果未藏密的數目；*FP* 表示受測影像未藏密，而偵測結果卻有藏密的數目；*FN* 表示受測影像有藏密，而偵測結果卻未藏密的數目。

測試不同特徵組合之偵測正確率實驗結果如表 8 所示。從表 8 可明顯看出，單一特徵的偵測正確率略遜於兩個以上特徵組合的偵測正確率，顯示單一特徵仍有其偵測侷限性。而隨著加入特徵組合的特徵數越多，偵測正確率亦隨之穩定成長，顯示特徵之間有互補的效果。

表 8. 不同特徵組合之偵測正確率

特徵組合	F_1	F_2	F_3	F_4	F_1,F_2	F_1,F_3	F_1,F_4	F_2,F_3
AC	0.98904	0.96384	0.99368	0.9934	0.99632	0.99878	0.99914	0.99846
特徵組合	F_2,F_4	F_3,F_4	F_1,F_2,F_3	F_1,F_2,F_4	F_1,F_3,F_4	F_2,F_3,F_4	F_1,F_2,F_3,F_4	
AC	0.99938	0.99946	0.99946	0.99944	0.9996	0.99976	0.99992	

為說明訓練影像集合特徵並結合 BPNN 分類器產生訓練模型時間與以受測影像集合特徵進行 BPNN 分類時間，本研究分別以 NRCS、BOSS 與 BOWS2 為受測影像資料庫，並依循 4.2 節之步驟進行實驗，實驗結果如表 9 所示。從表 9 可看出，隨著受測影像資料庫內含影像張數的不同，擷取特徵的時間亦有所不同；而產生訓練模型的時間是大於以受測影像集合特徵進行 BPNN 分類時間，表示訓練模型產生後，可藉由此訓練模型快速地進行受測影像之偵測。

表 10 至表 12 為依 4.2 節之實驗步驟與 4.3 節之相同類型影像資料庫訓練與測試的實驗場景所得之實驗結果，由表 10 至表 12 可看出，本偵測技術分別針對 NRCS、BOSS 及 BOWS2 影像資料庫的載體影像與相對應的藏密影像，進行訓練與測試，其偵測正確率均可達 99%，此實驗結果表示本偵測技術對整合 PVD 與 LSB 藏密技術所產生之藏密影像，具有極佳之偵測效果，且對各影像資料庫之載體影像之誤判率極低。

表 9. 擷取特徵、特徵結合 BPNN 分類器產生訓練模型時間與進行 BPNN 分類時間

	NRCS	BOSS	BOWS2
擷取訓練與受測影像特徵時間	140.58	678.3	680.62
訓練影像集合特徵結合BPNN分類器產生訓練模型時間	22.34	47.22	50.44
以受測影像集合特徵進行 BPNN 分類時間	0.13	0.31	0.34
			單位：秒

表 13 至表 18 為依 4.3 節之不同類型影像資料庫的訓練與測試的實驗場景所得之實驗結果，本偵測技術依表 7 訓練影像樣本與測試影像樣本的設定，分別進行訓練與測試，其偵測正確率亦均可達 99%。此實驗結果表示，在 BPNN 訓練與測試階段使用不同影像資料庫的載體影像與其相對應之整合 PVD 與 LSB 藏密技術所產生之藏密影像，本偵測技術亦具有極佳之偵測效果。

表 10. 本偵測技術針對 NRCS 影像庫的實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	1362	0	1362	0	1.00000
2	1362	0	1360	2	0.99927
3	1361	1	1362	0	0.99963

4	1362	0	1361	1	0.99963
5	1361	1	1362	0	0.99963
6	1362	0	1361	1	0.99963
7	1362	0	1360	2	0.99927
8	1357	5	1362	0	0.99816
9	1361	1	1362	0	0.99963
10	1359	3	1362	0	0.99890
平均	1360.9	1.1	1361.4	0.6	0.99938

表 11. 本偵測技術針對 BOSS 影像庫的實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	4537	0	4531	6	0.99934
2	4534	3	4532	5	0.99912
3	4537	0	4532	5	0.99945
4	4534	3	4532	5	0.99912
5	4536	1	4535	2	0.99967
6	4537	0	4531	6	0.99934
7	4537	0	4530	7	0.99923
8	4536	1	4533	4	0.99945
9	4536	1	4531	6	0.99923
10	4536	1	4528	9	0.99890
平均	4536	1	4531.5	5.5	0.99928

表 12. 本偵測技術針對 BOWS2 影像庫的實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	5000	0	4999	1	0.99990
2	5000	0	4999	1	0.99990
3	5000	0	4999	1	0.99990
4	5000	0	4999	1	0.99990
5	5000	0	4998	2	0.99980
6	5000	0	4997	3	0.99970
7	4999	1	4998	2	0.99970
8	5000	0	4998	2	0.99980
9	5000	0	4999	1	0.99990
10	4999	1	5000	0	0.99990
平均	4999.8	0.2	4998.6	1.4	0.99984

表 13. 訓練：NRCS、測試：BOSS 之實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	4991	9	4961	39	0.995
2	5000	0	4964	36	0.996
3	4994	6	4967	33	0.996
4	4995	5	4976	24	0.997
5	5000	0	4921	79	0.992
6	4987	13	4980	20	0.997
7	5000	0	4972	28	0.997
8	5000	0	4948	52	0.995
9	4990	10	4979	21	0.997
10	4998	2	4968	32	0.997
平均	4995.5	4.5	4963.6	36.4	0.996

表 14. 訓練：NRCS、測試：BOWS2 之實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	5000	0	4981	19	0.9981
2	4998	2	4989	11	0.9987
3	5000	0	4982	18	0.9982
4	5000	0	4983	17	0.9983
5	4999	1	4986	14	0.9985
6	4993	7	4994	6	0.9987
7	4994	6	4987	13	0.9981
8	4996	4	4989	11	0.9985
9	5000	0	4982	18	0.9982
10	4982	18	4971	29	0.9953
平均	4996.2	3.8	4984.4	15.6	0.9981

表 15. 訓練：BOSS、測試：NRCS 之實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	2000	0	2000	0	1
2	2000	0	2000	0	1
3	2000	0	1999	1	0.99975
4	2000	0	1999	1	0.99975
5	2000	0	2000	0	1
6	2000	0	2000	0	1
7	1999	1	2000	0	0.99975
8	2000	0	1999	1	0.99975
9	1999	1	1999	1	0.9995
10	2000	0	2000	0	1
平均	1999.8	0.2	1999.6	0.4	0.99985

表 16. 訓練：BOSS、測試：BOWS2 之實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	5000	0	4999	1	0.9999
2	4999	1	5000	0	0.9999
3	5000	0	5000	0	1
4	4999	1	5000	0	0.9999
5	5000	0	4999	1	0.9999

6	5000	0	4999	1	0.9999
7	5000	0	5000	0	1
8	5000	0	4999	1	0.9999
9	5000	0	5000	0	1
10	4999	1	5000	0	0.9999
平均	4999.7	0.3	4999.6	0.4	0.99993

表 17. 訓練：BOWS2、測試：NRCS 之實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	2000	0	2000	0	1
2	2000	0	2000	0	1
3	2000	0	1999	1	0.99975
4	2000	0	2000	0	1
5	1999	1	2000	0	0.99975
6	2000	0	2000	0	1
7	2000	0	1998	2	0.9995
8	2000	0	1999	1	0.99975
9	2000	0	2000	0	1
10	1999	1	2000	0	0.99975
平均	1999.8	0.2	1999.6	0.4	0.99985

表 18. 訓練：BOWS2、測試：BOSS 之實驗結果

	TP	*FN*	*TN*	*FP*	*AC*
1	4997	3	4999	1	0.9996
2	4994	6	4996	4	0.999
3	4994	6	5000	0	0.9994
4	4995	5	4997	3	0.9992
5	4990	10	4998	2	0.9988
6	4998	2	4998	2	0.9996
7	4996	4	4997	3	0.9993
8	4996	4	4998	2	0.9994
9	4994	6	4996	4	0.999
10	4995	5	4998	2	0.9993
平均	4994.9	5.1	4997.7	2.3	0.99926

為顯示本偵測技術之效果，本研究與 Pevny 等學者[37]所提使用 2 階馬可夫鏈的 686 個 SPAM 特徵之空間域通用偵測技術進行比較。本研究自美國紐約州立賓漢頓大學電子與計算機工程學系數位資料嵌入實驗室下載實驗所需 SPAM 特徵[38]，且遵循 4.2 節實驗步驟與 4.3 節相同類型影像資料庫訓練與測試之實驗場景來訓練及測試 SPAM 特徵，所用來訓練與測試的資料庫為 NRCS，並依此設定進行實驗，表 19 所列 SPAM 特徵之偵測正確率即為其實驗結果。

由表 19 的結果可看出本技術之偵測正確率優於 Pevny 等學者所提的偵測技術，且所耗費的計算資源與時間亦低於 SPAM，可證明本分析技術之優越性。

表 19. 本偵測技術與 Pevny 的技術之偵測正確率

	本偵測技術	SPAM 特徵
整合 PVD 與 LSB 藏密技術	99%	76.8%

五、結論

藏密技術之濫用可能危害國土與社會安全，也突顯出發展藏密分析技術重要性與急迫性。本研究旨在針對 Yang 等學者提出的整合 PVD 與 LSB 藏密技術，提出有效的特徵，以有效偵測整合 PVD 與 LSB 藏密技術。

本偵測技術將載體與藏密影像區分為兩兩相鄰且不重疊的像素對後，再進行其像素差值的計算，可得到載體影像與藏密影像之像素差值直方圖(PDH)。再比對載體與藏密影像的 PDH，找出其相異特徵，以作為有效區分載體與藏密影像之基礎。本研究之偵測流程區分為訓練模型產生及影像偵測兩個階段。在訓練模型產生階段，先輸入已標記的載體影像與藏密影像樣本至 BPNN 分類器，進行學習與訓練，產生訓練模型。在影像偵測階段，則利用已訓練的模型，對輸入之受測影像進行偵測分類。

為驗證本偵測技術所使用藏密特徵之有效性，本研究使用 MATLAB 實現 Yang 等學者提出的整合 PVD 與 LSB 藏密技術之模擬程式及特徵值擷取程式，並結合了 BPNN 分類器及 NRCS、BOSS 及 BOWS2 影像資料庫以進行相同與不同類型影像資料庫的訓練與測試之實驗。實驗結果證明，本研究所提之 4 項藏密特徵於偵測整合 PVD 與 LSB 藏密法時，可達 99%的偵測正確率。實驗結果同時證明，本偵測技術對整合 PVD 與 LSB 藏密技術之偵測效果優於 SPAM 通用型之偵測技術。

參考文獻

[1] Barr, T., Invitation to Cryptology, Prentice Hall, Upper Saddle River, 2002.
[2] Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G., “Information Hiding-A

Survey," Proceedings of the IEEE, Vol. 87, No. 7, pp. 1062-1078, 1999.
[3] Rabah, K., "Steganography-The Art of Hiding Data," Information Technology Journal, Vol. 3, No. 3, pp. 245-269, 2004.
[4] Cacciaguerra, S. and Ferretti, S., "Data Hiding: Steganography and Copyright Marking," http://www.cs.unibo.it/~scacciag/home_files/teach/datahiding.pdf.
[5] Shih, F. Y. and Wu, Scott. Y. T., "Combinational Image Water Marking in the Spatial and Frequency Domains," Pattern Recognition, Vol. 36, No. 4, pp. 969-975, Apr. 2003.
[6] Chang, C. C., Chen, T. S., and Chung, L. Z., "A Steganographic Method Based upon JPEG and Quantization Table Modification," Information Sciences, Vol. 141, No. 1-2, pp. 123-138, 2002.
[7] Joo, S., Suh, Y., Shin, J., and Kikuchi, H., "A New Robust Watermark Embedding into Wavelet DC Components," ETRI Journal, Vol. 24, No. 5, pp. 401-404, 2002.
[8] Lee, W. B. and Chen, T. H., "A Public Verifiable Copy Protection Technique for Still Images," Journal of Systems and Software, Vol. 62, No. 3, pp. 195-204, 2002.
[9] Alturki, F. and Mersereau, R., "Secure Blind Image Steganographic Technique Using Discrete Fourier Transformation," Proceedings of IEEE International Conference on Image Processing, Thessaloniki, pp. 542-545, 2001.
[10] Bender, W., Gruhl, D., Morimoto, N., and Lu, A., "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, No. 3-4, pp. 313-336, 1996.
[11] Fridrich, J., Goljan, M., and Rui, D., "Detecting LSB Steganography in Color, and Gray-scale Images," Magazine of IEEE Multimedia Special Issue on Security, Vol. 4, No. 4, pp. 22-28, 2001.
[12] Westfeld, A. and Pfitzmann, A., "Attacks on Steganographic Systems," Proceedings of the Third International Workshop on Information Hiding, Dresden, Germany, pp. 61-75, 1999.
[13] Chang, C. C., Hsiao, J. Y., and Chan, C. S., "Finding Optimal Least-Significant-Bit Substitution in Image Hiding by Dynamic Programming Strategy," Pattern Recognition, Vol. 36, No. 7, pp. 1583-1595, 2003.
[14] Mielikeainen, J., "LSB Matching Revisited," IEEE Signal Processing Letters, Vol. 13, No. 5, pp. 285-287, 2006.
[15] Wu, D. C., and Tsai, W. H., "A Steganographic Method for Images by Pixel-Value Differencing," Pattern Recognition Letters, Vol. 24, No. 9-10, pp. 1613-1626, 2003.
[16] 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," IEEE Proceedings on Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.
[17] Yang, C. H., Weng, C. Y., Wang, S. J., and Sun, H. M., "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.
[18] 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, 2008.
[19] 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, 2008.
[20] Yang, S. K. and Huang, P. S., "Image Steganographic Approach by Integrating Pixel-value Differencing and LSB Replacement Schemes," Journal of Chung Cheng Institute of Technology, Vol. 41, No. 2, pp. 89-98, Nov, 2012.
[21] http://www.cnn.com/2001/US/09/20/inv.terrorist.search.
[22] http://www.usatoday.com/life/cyber/ccarch/2001/12/19/maney.htm.
[23] http://www.usatoday.com/life/cyber/tech/2001/10/17/bin-laden-site.htm.
[24] http://news.chinatimes.com/world/110504/112012050200143.html.
[25] Zhang, X. and Wang, S., "Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security," Pattern Recognition Letters, Vol. 25, No. 3, pp. 331-339, 2004.
[26] Joo, J. C., Lee, H. Y., Bui, C. N., Yoo, W. Y., and Lee, H. K., "Steganalytic Measures for the Steganography Using Pixel-Value Differencing and Modulus Function,"

Proceedings of the 9th Pacific Rim Conference on Multimedia: Advances in Multimedia Information Processing, Tainan, Taiwan, pp. 476-485, 2008.
[27] Sabeti, V., Samavi, S., Mahdavi, M., and Shirani, S., "Steganalysis and Payload Estimation of Embedding in Pixel Differences Using Neural Networks," Pattern Recognition, Vol. 43, No. 1, pp. 405-415, 2010.
[28] Joo, J. C., Kim, K. S., and Lee, H. K., "Histogram Estimation Scheme Based Steganalysis Defeating the Steganography Using Pixel-Value Differencing and Modulus Function," Optical Engineering, Vol. 49, No. 7, pp. 1-11, 2010.
[29] Zaker, N. and Hamzeh, A., "A Novel Steganalysis for TPVD Steganographic Method Based on Differences of Pixel Difference Histogram," Multimedia Tools and Applications, Vol. 58, No. 1, pp. 147-166, 2012.
[30] Rumelhart, D. E., Hinton, G. E., and Williams, R. J., "Learning Representations by Back-Propagating Errors," *Nature*, Vol. 323, No. 9, pp. 533-536, 1986.
[31] McCulloch, W. and Pitts, W., "A Logical Calculus of the Ideas Immanent in Nervous Activity," *Bulletin of Mathematical Biology*, Vol. 5, No. 4, pp. 115-133, 1943.
[32] Rosenblatt, F., "The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain," *Psychological Review*, Vol. 65, No. 6, pp. 386-408, 1958.
[33] http://photogallery.nrcs.usda.gov/.
[34] http://www.mathworks.com/products/neural-network/index.html.
[35] http://www.agents.cz/boss/BOSSFinal/index.php?mode=VIEW&tmpl=materials.
[36] http://bows2.ec-lille.fr/BOWS2OrigEp3.tgz.
[37] Pevny, T., Bas, P., and Fridrich, J., "Steganalysis by Subtractive Pixel Adjacency Matrix," IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, pp. 215-224, 2010.
[38] http://dde.binghamton.edu/download/feature_extractors/.