

植基於倒傳遞類神經網路之空間域數位影像藏密分析方法

劉興漢 楊顯豪* 周世淵

國防大學資訊管理學系

論文編號：NM-42-02-03

來稿 2022 年 3 月 7 日→第一次修訂 2022 年 3 月 25 日→第二次修訂 2022 年 3 月 30 日→

同意刊登 2022 年 4 月 13 日

摘要

目前藏密分析技術之發展，仍以人為選取藏密特徵為主。但以人為方式選取適當的藏密特徵，並不是件容易的事，同時也可能因為所採用的藏密演算法不同或更動，造成所選取的藏密特徵不再適用，而無法有效偵測。因此，考量人為選取之藏密特徵無法針對個別影像進行調整，本研究探討由演算法自動選取適當特徵並透過機器學習進行藏密偵測之可行性。目標在於利用機器學習將特徵選取及分類整合至同一個架構，並自動從大量的特徵數據中進行訓練與學習。依據此目標，提出了一套植基於倒傳遞類神經網路機器學習架構之空間域數位影像藏密分析方法，能有效偵測以空間域為基礎的藏密技術。並透過繁複實驗測試，證明本分析方法可達到更高之偵測正確率(96.6%)，值得將其應用於資訊安全領域中。

關鍵詞：機器學習、藏密分析、特徵選取

* 聯絡作者：楊顯豪 email: franky051205@gmail.com

A Steganalysis Method Based on the Back Propagation Neural Network for Digital Images in the Spatial Domain

Liu, Hsing-Han Yang, Chuan-Hao* Chou, Shih-Yuan

Department of Information Management, National Defense University, Taiwan, R.O.C.

Abstract

The development of steganalysis techniques nowadays is mainly based on manual stego feature selection. However, selecting appropriate stego features manually is not an easy task. Besides, it is also possible that the selected stego features are no longer applicable because the adopted steganography algorithms have been different or modified. In such a situation, effective detection is not guaranteed. Therefore, considering the fact that the manually-selected stego features are not capable of being adjusted to fit the condition of each individual image, this research investigated the feasibility of utilizing an algorithm to automatically select appropriate features and applying the machine learning technique to performing stego detection. The main objective is to use the machine learning technique to integrate feature collection and classification in the same framework, and to automatically complete the training and learning processes among a massive amount of feature data. To achieve such an objective, this research proposed a spatial domain digital image steganalysis (SDDIS) method base on a machine learning technique, namely, the back propagation neural network, to effectively detect the spatial domain-based stego techniques. Various experimental tests have verified that the proposed method can achieve a higher detection accuracy (96.6%) and is worth applying to the field of information security.

Keywords: Machine Learning, Steganalysis, Feature Selection.

* Corresponding Author Email: franky051205@gmail.com

一、緒論

1.1 前言

電腦科技的發展為生活及工作帶來了便利與效率，但隨之產生更多以往沒有的問題。現今許多資料都在網際網路上傳遞與交流，但使用者的不良習慣或系統的缺陷，將助長有心或不法人士藉此機會，進而竊取個人或組織的機密(敏)資訊，所造成的損失將難以估計。為了避免此類問題肇生及保護重要的機密(敏)資訊，可應用密碼學(Cryptography)的資料加密技術，進而保護其機密性(Confidentiality)(Barr, 2002)。然而加密的過程將會使資料出現亂碼，這也成為有心人士判斷資料重要性的指標之一，並可針對此徵兆來進行破解或破壞，造成另一項資安問題。而資訊隱藏(Information Hiding)技術將可以降低與解決此類問題。

資訊隱藏技術主要可將機密(敏)資訊嵌入特定媒體中，產生出包含機密(敏)資訊的影像或聲音等載體(Carrier)，大幅降低有心人士察覺機密(敏)資料存在的機率，進而防止遭到破壞或竊取。近幾年資訊隱藏領域依運用之目的不同，大致可區分為兩種重要類型的技術。第一種是數位浮水印技術(Watermarking)，是為了確保影像完整性所發展的技術，在不影響原載體完整性的前提下，進而達到確保智慧財產權的目的；第二種是影像藏密技術(Steganography)，是把傳遞的秘密資訊嵌入載體，藉以降低第三者的察覺，而合法接收者取得藏密載體後，可依反藏密程序將秘密資訊恢復。藏密技術須具備不可察覺性(Imperceptibility)及高資訊負載(Payload)等特性。不可察覺性是指被藏密影像不可輕易地被人眼察覺到失真，而高資訊負載是可滿足傳輸大量秘密資訊之需求。前述兩種資訊影藏技術中，影像藏密技術為本研究探討之重點，而後續所開發之藏密分析方法，是用來有效判別影像中是否有運用藏密技術加入秘密資訊。

根據 Boroumand 等 3 位學者於 2018 年的研究發表說明，目前藏密分析技術的發展，主要以人為選取藏密特徵為主，再搭配機器學習的分類器為輔，以建立藏密分析模型進行偵測。但若採取的藏密演算法改變，會對藏密模型的偵測效果造成影響(Boroumand, 2018)。由此可知，人為選取藏密特徵的做法，難以適應個別影像特性的差異，而會影響藏密偵測的正確率。為了改善這個情形，本研究提出一套機制，能自動對不同影像提取適當特徵值，來因應不同偵測目標影像特性的差異，以提供較佳的藏密偵測正確率。

1.2 研究目的

資訊隱藏技術雖可以用來確保資訊於傳遞過程中的安全性，然而，另一方面而言，秘密資訊的傳遞，也很可能被應用在危害國防與國家安全的行動中。因此，如何針對目前利用影像進行藏密之技術來開發分析方法，有效進行藏密偵測，以達到早期預警並進而確保國防與國家的安全，便顯得非常重要。另外，藏密分析方法也可運用於評估現有藏密技術對於偵測攻擊的抵抗力，對於藏密技術的發展也有所助益。目前藏密分析技術之發展，仍以人為選取藏密特徵為主，但以人為方式來選取適當的藏密特徵並不容易，另外也可能因為藏密演算法不同或更動，而造成所選取的特徵不再適用，而無法有效偵測。因此，有鑑於人為選取藏密特徵的偵測效果並不理想，本研究將探討是否能運用一套機制來適時自動調整特徵選取方式，以提升藏密偵測之效能。此外，可運用機器學習

的技術，將特徵選取及分類整合至同一個架構，並自動從大量的特徵數據中進行訓練與學習。

根據上述情形，本研究目的是提出一套植基於機器學習架構之空間域數位影像藏密分析方法，期能跳脫原本以人為固定方式選取特徵值的做法，而將能適應不同影像之特性，達到自動選取適當特徵值之功能，以有效偵測以空間域為基礎的藏密技術。另外，常見的藏密技術還包含頻率域技術，然因領域與特徵值擷取技術均不同，故本研究將僅針對空間域技術做探討。

二、文獻探討

本研究主要著重於開發一套可針對不同影像進行適應性特徵選取的藏密分析方法，可針對空間域影像藏密技術進行偵測。由於灰階影像的資料量較彩色影像低，較適合做為分析之樣本，故本研究將運用灰階影像來進行各種測試，然而所開發之方法同樣可以運用於彩色影像之藏密分析。於藏密技術的使用上，將以兩項性能優異之空間域藏密技術為主，分別為 Khodaei 等 2 位學者(2012)所提出結合「最低有效位元(Least-Significant-Bit, LSB)取代法」與「像素差值(Pixel-Value Differencing, PVD)藏密法」之新式藏密技術(簡稱為新式 LSB/PVD 藏密技術)，以及 Shen 等 2 位學者(2015)所提出結合「改良式修正方向利用法(Improved Exploiting Modification Direction, IEMD)」與「PVD 藏密法」之藏密技術(簡稱 IEMD/PVD 藏密技術)。後續將簡單介紹前述兩項影像藏密技術、藏密分析技術、機器學習理論，以及機器學習理論在藏密分析上之應用。於機器學習理論的介紹中，亦會針對本研究藏密分析所運用的類神經網路結構設計進行說明。

2.1 藏密技術概論

一般而言，為了能夠在影像中藏入大量資訊，並同時能保持影像品質，會利用影像中最低有效位元像素來進行藏密，此種方法稱為最低有效位元(LSB)取代法。但相對的，如果藏密的位元太多則將會使影像失真。Wu 和 Tsai 兩位學者於 2003 年指出，影像中包含了平滑區域(Smooth Areas)與邊緣區域(Edged Areas)，而當邊緣區域(相較於平滑區域)的像素值變化時，將較不容易被人眼察覺。他們並進一步利用此原理，提出了相鄰像素差值(PVD)藏密法(Wu and Tsai, 2003)。

Khodaei 等 2 位學者於 2012 年基於 Wu 與 Tsai 之研究成果，提出了新式 LSB/PVD 藏密技術。此技術之特點在於它的適應性資訊藏密方式，是以 LSB 取代法和 PVD 藏密法兩者結合為基礎。於藏密過程中，它將載體影像(Cover Image)分割為含有 3 個連續像素之區塊，並以每個區塊的中間像素做為基本像素，再藉由 LSB 取代和最佳化像素調整程序(Optimal Pixel Adjustment Process, OPAP)，將資訊隱藏於基本像素中。後續，再藉由計算區塊中基本像素和其他像素間的差值，來確定可藏入之資訊量(針對此部分，可參考事先定義之像素差值範圍區間表來做判斷。該表將顯示不同範圍區間可藏入資訊之位元數)。新式 LSB/PVD 藏密技術的步驟如圖 1 所示。

Shen 與 Huang 兩位學者於 2015 年以修正方向利用法(Exploiting Modification Direction, EMD)與 PVD 藏密法為基礎，提出了一種結合改良式 EMD(Improved EMD，縮寫為 IEMD)與 PVD 藏密法之技術(整體簡稱為 IEMD/PVD 藏密技術)。此藏密技術主

要是藉由希爾伯特曲線(Hilbert Curve)將載體影像轉換成一維，接續將其區分為具有 1×2 個連續像素且互不重疊之區塊，並依 PVD 藏密法計算每個像素區塊之藏密量，像素差值較大的區塊將可藏入較多秘密資訊。此技術可以避免溢位與影像失真問題，並具備較高的峰值訊號雜訊比(Peak Signal-to-Noise Ratio, PSNR)值。(資訊隱藏的關鍵因素定義如表 1 所示)

表 1 資訊隱藏的關鍵因素

關鍵因素	定義
強健性(Robustness)	藏密影像遭受數位訊號處理攻擊後，其品質仍在可接受的範圍內，且其藏密訊息仍可順利取出。
隱蔽性(Imperceptibility)	欲藏入之秘密訊息嵌入後，藏密影像與載體影像的差異性，必須讓人無法使用肉眼進行辨識，也就是對藏密影像品質有基本的要求。
位元錯誤率(Bit Error Rate)	數位傳輸過程中，發生錯誤之位元數除以傳輸位元總數之比率。一般用來評估通訊系統之效能，通常通道雜訊越大，位元錯誤率會越高。
均方差(Mean Square Error)	評估藏密影像常用的方式。所計算的均方差值越小，表示載體影像與藏密影像之間的差異越少，也代表藏密影像的品質越好。
峰值訊號雜訊比(Peak Signal-to-Noise Ratio)	在影像壓縮與影像藏密等相關領域中，影像品質的測量方法。利用影像像素的最大值與影像中雜訊的比值作為評估的標準，當計算出來的比值越大，表示藏密影像與載體影像越接近，也代表藏密影像品質越好。

(資料來源：本研究)

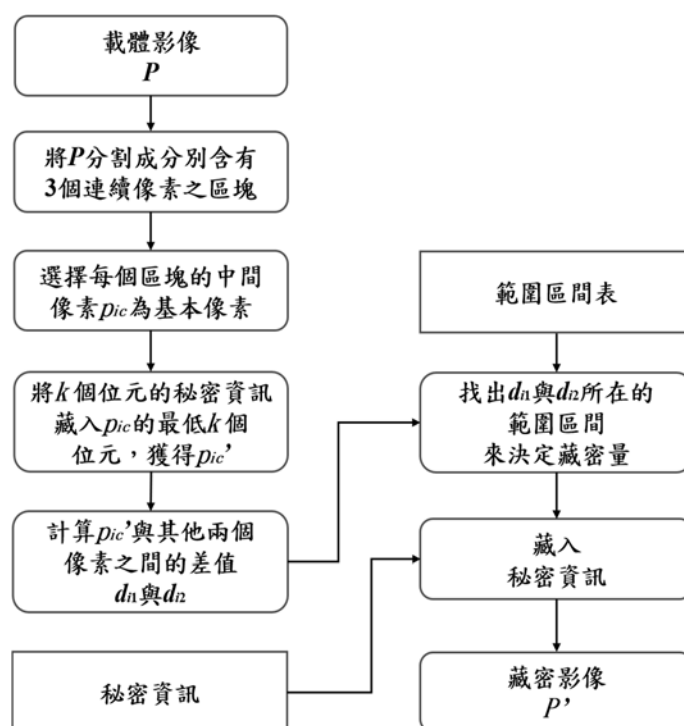


圖 1 新式 LSB/PVD 藏密技術流程圖

(資料來源：Khodaei and Faez., 2012)

2.2 藏密分析技術

2.2.1 藏密分析技術發展

在 1998 年的 IHW(Information Hiding Workshop)會議中，Johnson 與 Jajodia 兩位學者首次提出，可透過觀察影像藏密後所產生的特徵差異，來有效達到分析偵測的目的 (Johnson and Jajodia, 1998)。而隨著各類藏密演算法不同，所產生的特徵也不相同，目前大致可依技術區分為特定嵌入型偵測(Specific Embedding Steganalysis)與通用盲目型偵測(Universal Blind Steganalysis)兩大類。

2.2.2 藏密分析技術種類

a) 特定嵌入型偵測：

此類技術之偵測原理是針對特定藏密技術，藉由分析特徵值方式達到偵測效果。因為此方式有其針對性，故僅能在符合類型之藏密技術上有較佳的偵測正確率，若偵測不同類型藏密技術則無法發揮功效。

b) 通用盲目型偵測：

此類偵測技術不限定偵測特定藏密方式。其原理是透過分類器蒐集大量圖片，將未藏密影像及有藏密影像加以分類並萃取特徵值，接著透過訓練分類器的方式產生特徵值資料庫，再利用這些資料庫的資料來分析判斷影像是否嵌入訊息。其優、缺點正好與特定嵌入型偵測相反。因偵測過程需仰賴特徵值資料庫，因此資料庫的資料量與類型等是否完整，均為偵測率好壞之關鍵因素。

2.3 機器學習

多年來，人工智慧領域礙於電腦運算效能的限制，相關技術與應用一直無法有效發展，直到機器學習的萌芽，才使得它有了突破的可能性。機器學習是透過經驗讓電腦自動學習的一種演算法，首先從資料中分析出規律，再運用這些規律來做預測。現今機器學習也常被應用在各種領域，例如：影像辨識、資料探勘、自然語言處理及證卷市場分析等。

McCulloch 與 Pitts 兩位學者(1943)，提出了結合邏輯數學及神經生理學的神經元模型，並由 Rosenblatt 學者(1958)將其進一步發展，提出了感知器架構，可以模擬生物感知與學習能力，使類神經網路研究開始有不同形態的發展與研究。其中，Rumelhart 等學者(1986)提出倒傳遞類神經網路，其架構屬於多層感知器(Multi-Layer Perception, MLP)或前饋式類神經網路(Feed Forward Neural Network, FFNN)，而所採用的監督式學習，一般是運用誤差倒傳遞演算法(Error Back Propagation, EBP)做為學習演算法，也可簡稱為 BP 演算法。前述兩者結合，則形成倒傳遞類神經網路，具備學習精準度高、可處理複雜樣本識別、處理速度快、輸出可為連續值及高度非線性函數合成等優點，可更快速有效地解決分類問題(其架構如圖 2 所示)。

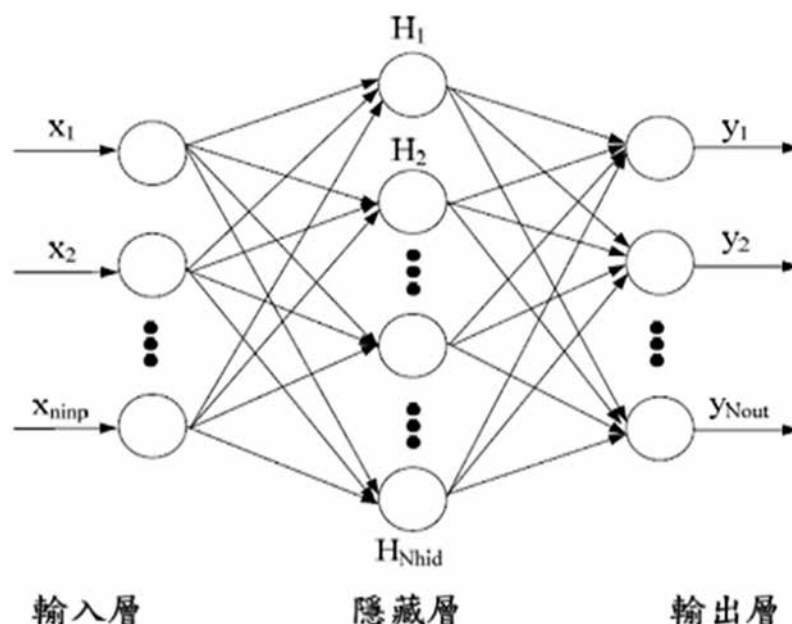


圖 2 倒傳遞類神經網路 BPNN 架構圖
(資料來源：Rumelhart et al., 1986)

2.4 機器學習與藏密分析相關研究

藏密分析，是針對運用藏密技術藏密的媒體進行偵測的分析技術。常見的藏密分析可以區分為：藏密載體偵測、藏密演算法分析、藏密資訊提取、藏密明文獲取等。其中，藏密載體偵測主要是檢測載體影像是否有被藏入秘密資訊，而藏密演算法分析是應用在分析特定藏密技術的藏密方式。最後的藏密資訊提取與藏密明文獲取，則是建立在前兩項分析的基礎之上，當前兩項分析完成之後，即可進行秘密資訊的提取與解密。

近年來，藏密分析技術的發展大多停留在偵測作業，相關研究所提出的應用主要是偵測載體影像是否有藏入秘密資訊，致力於提供更高的偵測正確率。針對這項應用，有許多研究運用機器學習理論，透過提取影像特徵來建立訓練資料集，接著再使用它來訓練分類器，而完成訓練的分類器將可以用來進行藏密分析。目前常見的空間域藏密分析技術，包含差分像素鄰接模型(Subtractive Pixel Adjacency Model, SPAM)、內容選擇殘差(Content-Selective Residuals, CSR)藏密分析技術、基於富模型(Rich Model)的高維特徵分析技術等。其中，CSR 藏密分析技術是由 Denemark 等學者於 2014 年提出，它針對測試影像擷取 1,183 個特徵進行分析，來判斷是否為藏密影像。本研究將採用此分析技術做為對照，透過實驗進行藏密偵測正確率比較，來證明本研究所提出之方法更能有效偵測空間域藏密影像。

Lerch-Hostalot 與 Megías 於 2016 年運用機器學習理論，提出結合人工訓練集與監督式分類方式，來建構一個非監督式學習影像藏密分析方法。可有效針對最低有效位元匹配法(LSB matching)、高度不可偵測藏密方法(Highly Undetectable steGO, HUGO)及小波權重法(Wavelet Obtained Weights, WOW)3 種藏密演算法進行藏密分析。惟此方法需事先確定藏密演算法種類，才能構建訓練模型。Hou 等 3 位學者於 2017 年提出利用 8 個特徵選取指標，並將其運用於 3 種藏密法之分析。此方法透過訓練小型訓練集以進行

藏密偵測作業，標榜僅利用少量的特徵選取即可達到有效的藏密偵測，然而當樣本數量減少，特徵選取反而會降低偵測的效益。

Liu 等 2 位學者於 2019 年提出一套運用於空間域之通用藏密分析方法，它以預測誤差直方圖(Prediction Error Histogram, PEH)特徵擷取為基礎，可針對 12 種空間域藏密方法(100%嵌入)進行偵測。它擷取了 PEH 的 8 個特徵來組成特徵向量，再利用概率神經網路(Probabilistic Neural Network, PNN)就這些特徵來進行分類器訓練。最後運用完成訓練之 PNN 分類器判斷可疑影像是否藏入秘密資訊。根據其實驗結果，顯示此方法優於其他常用之空間域藏密分析技術，如：SPAM、局部極值幅度檢測法(Amplitude of Local Extrema, ALE)等。

綜觀近年來藏密分析結合機器學習之相關文獻，本研究將聚焦於空間域藏密影像之分析，並跳脫以往以人為固定方式進行特徵選取之做法，開發出一套能依個別影像特性來適應性選取特徵之方法，並透過機器學習理論中的倒傳遞類神經網路進行分類訓練，以達到有效偵測空間域藏密影像之目的。

三、研究方法

本研究的主要目的，是開發一套針對空間域數位影像之藏密分析方法。因此，本章將以兩種具代表性之空間域藏密技術為例，來做為本研究方法分析之對象。這兩種技術分別為「新式 LSB/PVD 藏密技術」與「IEMD/PVD 藏密技術」。本研究分析方法以影像藏密前後像素差值直方圖(Pixel Difference Histogram, PDH)產生變異之特徵為探討重點，針對該特徵進行適當抽取後，再交由倒傳遞類神經網路(BPNN)分類器進行訓練與偵測。第一部分先說明前述 2 種空間域藏密技術的藏密過程所造成 PDH 變化之特性，第二部分闡述本研究針對此類藏密技術所開發之特徵值計算機制，而第三部分則說明本研究藏密分析方法的偵測流程。

3.1 本研究分析之藏密技術

Khodaei 及 Faez 兩位學者於 2012 年提出了新式 LSB/PVD 藏密技術。此藏密技術的主要做法，是將載體影像(Cover Image)分割成含有 1×3 個連續像素且互不重疊之區塊，並以每個區塊的中間像素做為基本像素，接續運用 LSB 取代法將秘密資訊藏入基本像素中。另外，計算基本像素與左右相鄰像素間的差值，並依圖 3 範圍區間表來決定可藏入的秘密資訊量。本研究使用其中 Type 2 方法，可藏入大量秘密資訊並同時維持藏密影像(Stego Image)的品質。

Shen 和 Huang 兩位學者於 2015 年提出了 IEMD/PVD 藏密技術。此藏密技術的主要做法，是藉由 Hilbert 曲線將載體影像轉換成一維，接續將其區分為含有 1×2 個連續像素且互不重疊之區塊，並依 PVD 藏密法計算每個像素區塊之藏密量，像素差值較大的區塊將可藏入較多秘密資訊，此技術可以避免溢位與影像失真問題，並可保持藏密影像品質。後續，本研究將針對前述這 2 種具代表性空間域技術之藏密影像，進行藏密分析實驗。

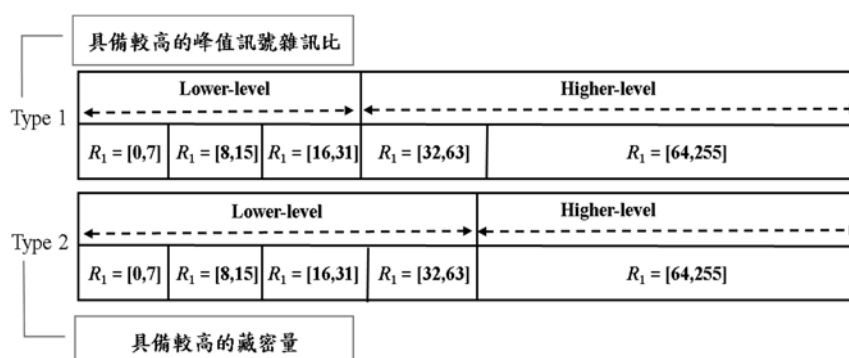


圖 3 新式 LSB/PVD 藏密技術範圍區間表
(資料來源：Khodaei and Faez, 2012)

3.2 本研究藏密分析方法之特徵值計算機制

本節將透過「載體影像與藏密影像像素差值直方圖比較」、「適應性特徵選取基準」及「特徵值計算」，來論述如何計算出適當之特徵值，相關名詞定義如表 2 所示：

表 2 本研究名詞定義說明表

項次	名詞	說明
1	特徵值 基準參考位置	於像素差值直方圖中，經由本研究所提出之公式，所計算出之特殊像素差值，用來做為特徵抽取之參考位置。
2	載體影像 像素差值直方圖	將載體(未藏密)影像轉換成矩陣，再進行掃描計算連續相鄰像素差，最後針對不同像素差值之發生次數進行統計，所描繪成之直方圖。
3	藏密影像 像素差值直方圖	類似前項說明之載體影像像素差值直方圖，惟運用的是藏密後的影像。

(資料來源：本研究)

3.2.1 載體影像與藏密影像像素差值直方圖比較

本研究將載體影像與藏密影像先行轉換成矩陣，再進行行與行間的掃描，來計算連續相鄰像素差(即相鄰像素值相減，如： $(p_2 - p_1)$ 、 $(p_3 - p_2)$ 、 $(p_4 - p_3)$ 、 $\dots$)，獲得載體影像與藏密影像的像素差值直方圖(PDH)(如圖 3-2 與 3-3 所示)。而所採用的藏密技術，為新式 LSB/PVD 與 IEMD/PVD 藏密技術，其藏密量分別設定為 100%、75%、50%及 10%(圖 3-2 與 3-3 所顯示的，分別為新式 LSB/PVD 與 IEMD/PVD 藏密技術 100%藏密量之影像數據)。由於秘密資訊嵌入的緣故，可觀察載體影像與藏密影像的 PDH 差異，利用此差異作為區分載體與藏密影像的基礎。

3.2.2 適應性特徵選取基準

本研究藏密分析方法將藉由下述方式，針對不同影像自動計算適當之特徵值。此方式是透過觀察大量載體與藏密影像 PDH 之差異，由所獲得之經驗所推導出來的。首先，由載體及藏密影像的 PDH，可得知影像之像素差值大致會趨近常態分佈(Normal Distribution)，故在特徵值之基準參考位置(整數 b ，代表某像素差值)的選取上，可採用該分佈標準差的常數倍數($a \cdot \sigma$ ，其中 σ 為標準差，而 a 為常數)，即可有效針對個別影像不同的 PDH 狀態獲得相對應之基準參考位置 b 。接著利用所得位置 b 附近 PDH 曲線斜率的特性，來開發能突顯載體與藏密影像差異之特徵值計算方式。以圖 4 與 5 中載體

影像與藏密影像之 PDH 為例(其中直方圖改以折線圖表示,以利於清楚說明該計算方式之概念),在位置 b 附近(放大部分如圖 6 所示,為突顯藏密前後影像普遍具備之特性,圖中曲線為概略繪製之示意圖,並非使用實際資料值),載體影像之曲線斜率會隨著像素差值增加而降低,相對的,藏密影像之曲線斜率則將會升高。若分別抽取載體影像曲線斜率 m'_1 與 m'_2 及藏密影像 m_1 與 m_2 ,則基於前述特性,載體影像的斜率比值 m'_1/m'_2 會大於 1,而藏密影像的 m_1/m_2 則會小於 1。兩者數值之差異特性將可做為後續輸入 BPNN 進行訓練與偵測之特徵值。斜率計算方式(以藏密影像為例)如公式(1):

$$m_1 = \frac{H_b - H_{b+1}}{1}, \quad m_2 = \frac{H_{b+2} - H_{b+3}}{1} \quad (1)$$

上式中, H_x 代表 PDH 圖中特定位置 x (代表像素差值,為整數值)所對應之數值(代表出現次數,為大於或等於 0 之整數值)。而基準參考位置 $b = a \cdot \sigma$, 其中常數 a 為可依需求調整之值(本研究設定為 0.08,於選取上並未經過最佳化,其目的僅為協助闡述本方法之概念)。

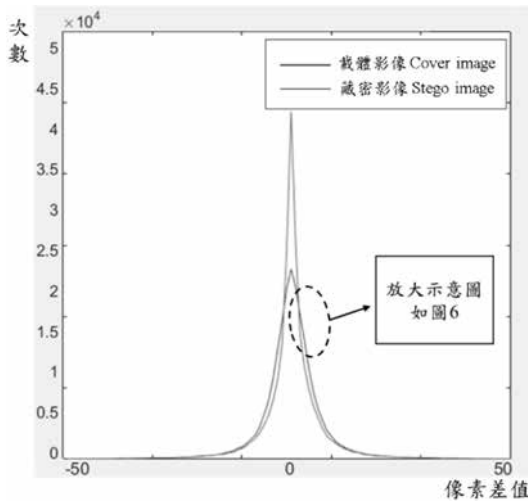


圖 4 新式 LSB/PVD 藏密前後之影像 PDH

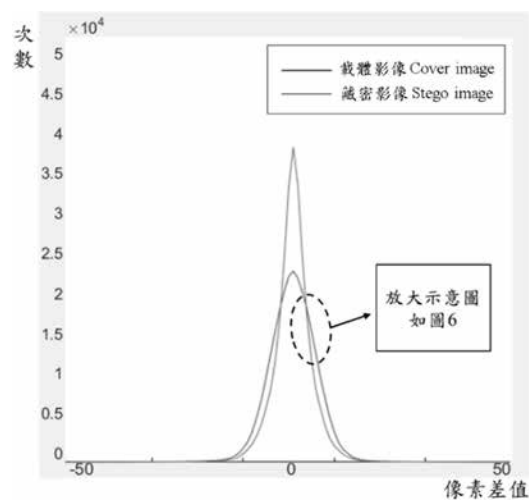


圖 5 IEMD/PVD 藏密前後之影像 PDH

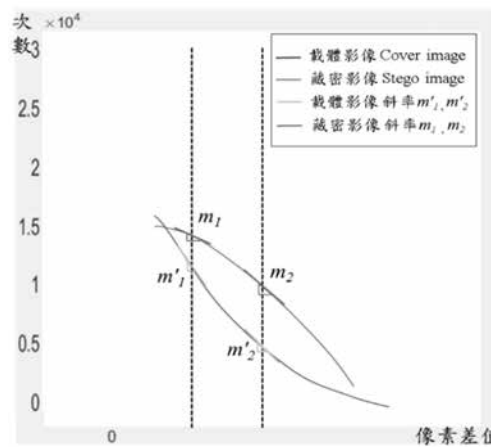


圖 6 藏密前後影像 PDH 曲線斜率示意圖

3.2.3 特徵值

依照前述適應性特徵值選取基準，本研究分別計算每張載體及藏密影像像素差值之標準差，藉以獲得適合之特徵值基準參考位置 b ，並計算出本研究藏密分析方法的 4 項特徵值($F_1 \sim F_4$)，計算方式如表 3 所示(其中 F_1 與 F_3 即為前述斜率比值)。

表 3 本研究藏密分析方法之特徵值計算方式

項次	特徵值符號	特徵值計算方式
1	F_1	$(H_b - H_{b+1}) / (H_{b+2} - H_{b+3})$
2	F_2	H_b / H_{b+1}
3	F_3	$(H_{-b} - H_{-b-1}) / (H_{-b-2} - H_{-b-3})$
4	F_4	H_{-b} / H_{-b-1}

(資料來源：本研究)

本研究實驗針對所使用的 BossBase 影像資料庫中 6,000 張載體影像與相對應的藏密影像進行特徵值擷取，各特徵分佈分別如圖 7~10(新式 LSB/PVD 藏密前後，載體影像與藏密影像之特徵值)與圖 11~14(IEMD/PVD 藏密前後，載體影像與藏密影像之特徵值)所示(其中縱軸為特徵值，橫軸代表個別測試影像。為使讀者更清楚觀察載體與藏密影像特徵值的分佈狀況，圖中之橫軸與縱軸僅顯示一個較小的區間)。就特徵值 F_1 與 F_3 而言，實驗結果顯示載體影像特徵值大部分數值大於 1，且分佈較廣，而藏密影像特徵值則大部分小於 1，集中分佈於 0~1 之間。就 F_2 與 F_4 而言，載體影像特徵值同樣大部分大於 1，且分佈較廣，而藏密影像特徵值則大部分僅微大於 1，集中分佈於 1 附近。

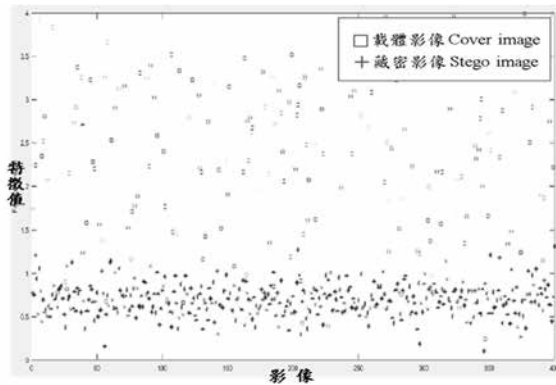


圖 7 新式 LSB/PVD 藏密前後影像特徵值 F_1

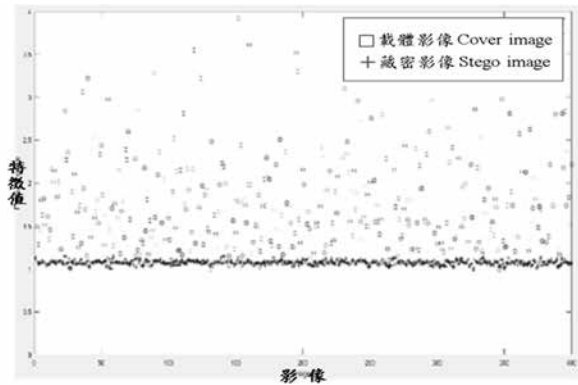


圖 8 新式 LSB/PVD 藏密前後影像特徵值 F_2

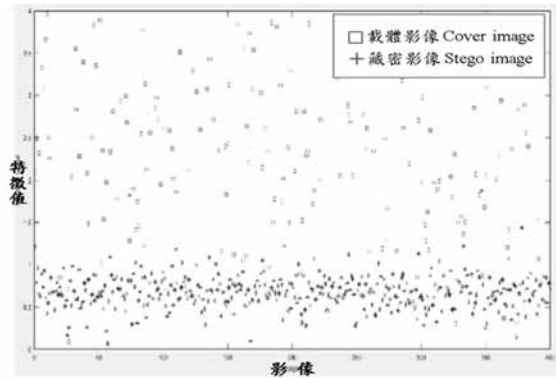


圖 9 新式 LSB/PVD 藏密前後影像特徵值 F_3

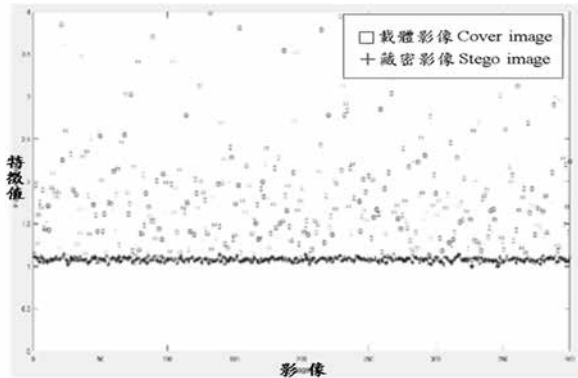


圖 10 新式 LSB/PVD 藏密前後影像特徵值 F_4

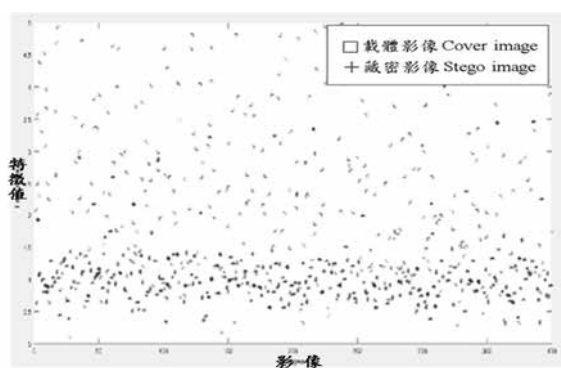


圖 11 IEMD/PVD 藏密前後影像特徵值 F_1

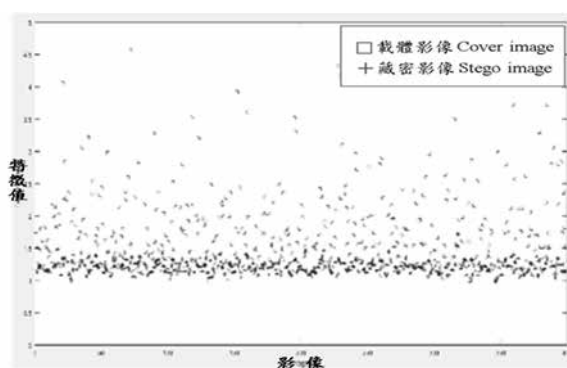


圖 12 IEMD/PVD 藏密前後影像特徵值 F_2

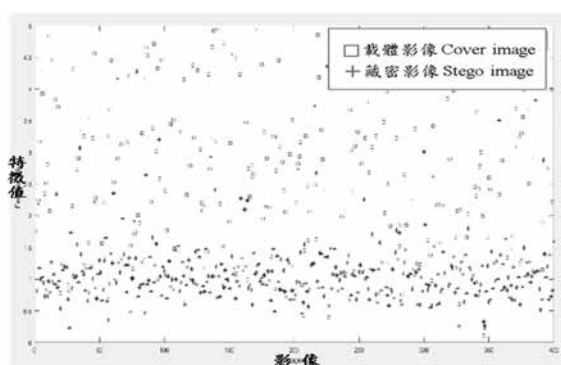


圖 13 IEMD/PVD 藏密前後影像特徵值 F_3

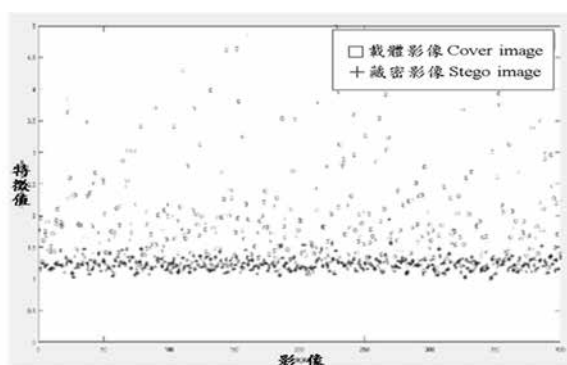


圖 14 IEMD/PVD 藏密前後影像特徵值 F_4

3.3 本研究藏密分析方法流程

本研究藏密分析方法的主要特性，在於輸入個別影像時，可於計算像素差值之後，自動判斷適合之特徵值基準參考位置，並據此計算 4 個特徵值。在訓練階段，將特徵值交由 BPNN 進行訓練，來有效提升偵測正確率。本方法採用 3 層 BPNN 架構，分別為輸入層、單層隱藏層及輸出層。其中輸入層具有 4 個神經元，可將特徵值 F_1 至 F_4 輸入至隱藏層內。而在實驗過程中，發現當隱藏層神經元的個數為 20 時，其偵測正確率最佳，故本方法使用 20 個隱藏層神經元，並將特徵值 F_1 至 F_4 進行非線性轉換後，將結果送至輸出層。輸出層具有 1 個神經元，負責評估測試影像是否藏有秘密訊息。

藏密分析流程如圖 15 所示，區分為 BPNN 分類器訓練過程及影像測試過程 2 階段。

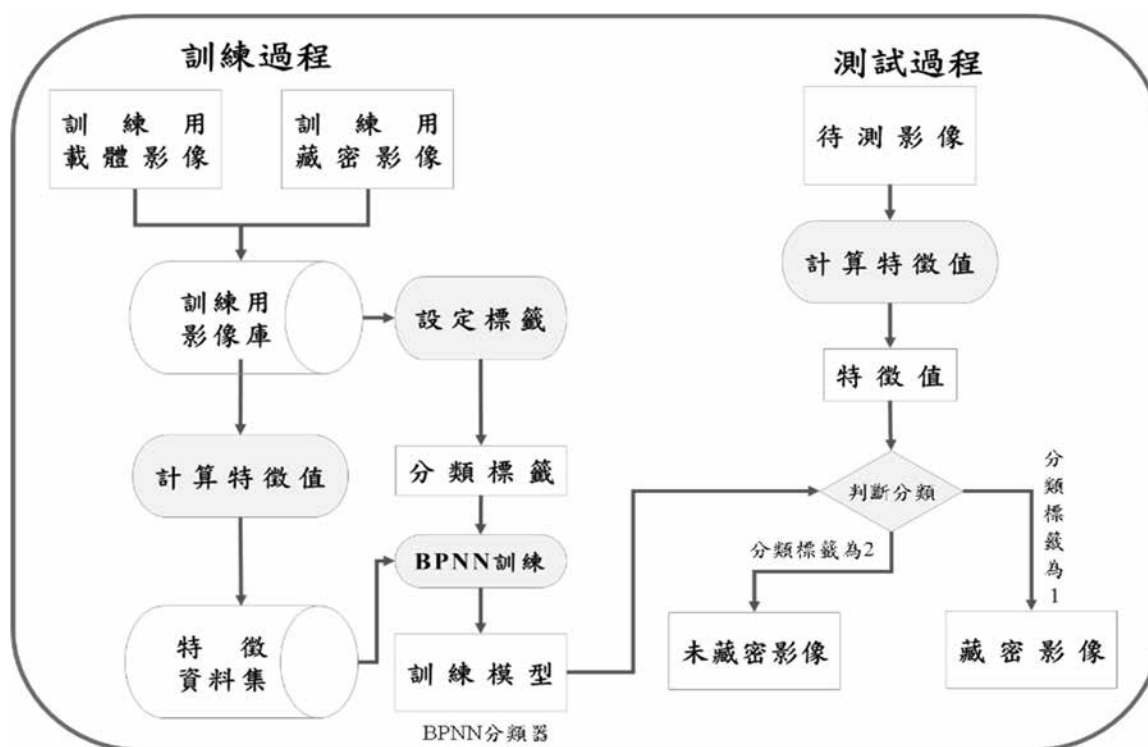


圖 15 本研究藏密分析方法流程圖

(資料來源：本研究)

在 BPNN 分類器訓練過程中，利用載體影像及藏密影像(分別經新式 LSB/PVD 與 IEMD/PVD 藏密技術進行藏密)做為訓練樣本，並以表 2 特徵值計算方式，針對所有樣本進行特徵擷取以完成特徵資料集。另分別設定藏密影像的分類標籤為 1，載體(未藏密)影像的分類標籤為 2，再將分類標籤與特徵資料集輸入 BPNN 進行訓練，以獲得完成訓練的訓練模型(BPNN 分類器)。

在影像測試過程中，是針對未知是否藏密的待測影像進行特徵值擷取，再輸入至已完成訓練的 BPNN 分類器做判斷，則將可得知該測試影像是否有藏密。若輸出的標籤為 1，則判斷為經新式 LSB/PVD 或 IEMD/PVD 藏密技術所藏密的影像，而若輸出標籤為 2，則判斷為一般載體影像。

四、實驗結果

4.1 實驗環境

本研究所採用的實驗平台，是配備 i5-6500 處理器(CPU)與 8G 記憶體之個人電腦，其作業系統為 64 位元的 Windows 10，而實作相關演算法所使用的程式語言為 Python 3.7 及 MATLAB R2016a。另外，實驗中使用的圖片，是來自藏密分析領域中常用的 BOSSbase 自然影像資料庫，於其中隨機選擇 6,000 張大小為 512*512 像素之 8 位元灰階影像(其中 3,000 張做為訓練影像，餘 3,000 張做為測試影像)，並使用 BPNN 進行訓練與測試(範例影像如圖 16 所示)。於藏密技術的使用上，分別採用 Khodaei 與 Faez(2012)的新式 LSB/PVD 藏密技術，以及 Shen 與 Huang(2015)的 IEMD/PVD 藏密技術，來將秘密資訊

藏入影像(分別進行 100%、75%及 50%藏密量之藏密)，接著以 MATLAB 程式完成藏密影像分析。此外，為了突顯適應性特徵選取方式(自動選取適當特徵值基準參考位置)之效益，本實驗亦納入人為選取方式(固定特徵值基準參考位置)之偵測數據進行比較。相關實驗步驟與結果分述如下。



圖 16 BossBase 資料庫灰階影像範例

(資料來源：BOSS Break Our Steganographic System 影像資料庫網站)

4.2 實驗步驟

- 步驟 1：在 BossBase 資料庫 6,000 張影像中，隨機挑選 3,000 張影像做為訓練影像，並運用藏密技術進行藏密，得到 3,000 張藏密影像。
- 步驟 2：分別針對挑選出之 3,000 張藏密前之載體影像與 3,000 張藏密影像，進行特徵值計算，並給予分類標籤，獲得特徵集合。
- 步驟 3：將步驟 2 所得之特徵集合與相對應的分類標籤，輸入 BPNN 進行分類訓練，產生訓練模型(訓練後之分類器)。
- 步驟 4：將扣除訓練用影像後的 3,000 張影像做為測試影像，並運用藏密技術進行藏密，產生 3,000 張藏密影像。
- 步驟 5：運用步驟 3 所產生之訓練模型，對步驟 4 的 6,000 張影像(3,000 張藏密前之載體影像與 3,000 張藏密影像)進行分類測試。
- 步驟 6：將步驟 1 至 5 重複 10 次，計算其偵測分類結果之平均值。

4.3 實驗結果

依前述實驗步驟進行操作所獲得之結果，將以表 4 所列出之各項指標來做為評量依據。相關評量指標包含：正確率(AC)、精確率(Precision)、召回率(Recall)及 F1 分數(F1 Score)。

表 4 實驗數據評量指標表

評量指標	評量指標描述	計算式($\times 100\%$)
正確率 Accuracy	藏密分析效能比率(正確判斷之比率)。	$\frac{TP + TN}{TP + TN + FP + FN}$
精確率 Precision	在所有判斷為藏密影像者中，實際亦為藏密影像之比率。	$\frac{TP}{TP + FP}$
召回率 Recall	在所有實際為藏密影像者中，正確判斷為藏密影像之比率。	$\frac{TP}{TP + FN}$
F1 Score	精確率與召回率的調和平均數。	$\frac{2}{\frac{1}{Precision} + \frac{1}{Recall}}$
備註	藏密分析結果區分四種： 真陽性(True Positive, TP)，正確判別為藏密影像之張數 假陽性(False Positive, FP)，錯誤判別為藏密影像之張數 真陰性(True Negative, TN)，正確判別為載體影像之張數 假陰性(False Negative, FN)，錯誤判別為載體影像之張數	

(資料來源：修訂自 Liu, 2019)

4.3.1 本研究適應性特徵選取方式與人為選取方式比較

本實驗分別採用所提出之適應性特徵選取方式及人為特徵選取方式進行藏密偵測(此處人為選取方式之特徵值基準參考位置 b 設定為 0)，針對兩種藏密技術所藏密之影像，其測試結果如表 5~10 所示(分別針對 100%、75%及 50%藏密量之影像進行偵測)。本研究所提出之適應性特徵值藏密分析方法，針對新式 LSB/PVD 藏密技術 100%藏密量之影像，其偵測正確率平均可達 96.6%，另針對 75%及 50%藏密量之影像，亦可達到 84.4%與 75.7%，皆優於人為特徵選取方式之藏密偵測結果(綜合比較數據，如表 11 所示)。另針對 IEMD/PVD 藏密技術 100%藏密量之影像，其偵測正確率平均可達 85.4%，而針對 75%及 50%藏密量之影像，亦可達到 80%與 74.6%，同樣優於人為特徵選取方式之藏密偵測結果(綜合比較數據，如表 12 所示)，由此驗證本研究藏密分析方法能有效偵測使用新式 LSB/PVD 與 IEMD/PVD 為代表之空間域藏密技術所進行藏密之影像。

表 5 適應性特徵選取方式與人為選取方式比較表(針對 LSB/PVD、100%藏密量)

針 對 新 式 L S B / P V D 藏 密 影 像 (1 0 0 % 藏 密 量) 之 偵 測 結 果										
執行 次數	本 研 究 適 應 性 特 徵 選 取 方 式					人 為 特 徵 選 取 方 式 ($b = 0$)				
	TP	FN	TN	FP	AC 值	TP	FN	TN	FP	AC 值
1	2972	28	2819	181	96.5%	2999	1	2751	249	95.8%
2	2960	40	2834	166	96.6%	2991	9	2751	249	95.7%
3	2965	35	2834	166	96.7%	2988	12	2743	257	95.5%
4	2969	31	2815	185	96.4%	2999	1	2751	249	95.8%
5	2974	26	2825	175	96.7%	2993	7	2757	243	95.8%
6	2966	34	2830	170	96.6%	2999	1	2752	248	95.9%
7	2965	35	2834	166	96.7%	2994	6	2753	247	95.8%
8	2954	46	2848	152	96.7%	3000	0	2739	261	95.7%
9	2965	35	2834	166	96.7%	2999	1	2751	249	95.8%
10	2976	24	2811	189	96.5%	2998	2	2767	233	96.1%
平均	AC(偵測正確率)				96.6%	AC(偵測正確率)				95.8%
	Recall(召回率)				98.9%	Recall(召回率)				99.9%
	Precision(精確率)				94.5%	Precision(精確率)				92.3%
	F1 Score				96.7%	F1 Score				96.0%

表 6 適應性特徵選取方式與人為選取方式比較表(針對 LSB/PVD、75%藏密量)

針 對 新 式 L S B / P V D 藏 密 影 像 (7 5 % 藏 密 量) 之 偵 測 結 果										
執行 次數	本 研 究 適 應 性 特 徵 選 取 方 式					人 為 特 徵 選 取 方 式 ($b = 0$)				
	TP	FN	TN	FP	AC 值	TP	FN	TN	FP	AC 值
1	2836	164	2275	725	85.2%	2600	400	2309	691	81.8%
2	2836	164	2275	725	85.2%	2590	410	2339	661	82.2%
3	2601	399	2384	616	83.1%	2519	481	2343	657	81.0%
4	2788	212	2294	706	84.7%	2572	428	2351	649	82.1%
5	2707	293	2313	667	83.7%	2713	287	2290	710	83.4%
6	2694	306	2382	618	84.6%	2627	373	2337	663	82.7%
7	2812	188	2255	745	84.5%	2570	430	2378	622	82.5%
8	2587	413	2371	629	82.6%	2547	453	2391	609	82.3%
9	2737	263	2375	625	85.2%	2632	368	2171	829	80.1%
10	2836	164	2275	725	85.2%	2595	405	2351	649	82.4%
平均	AC(偵測正確率)				84.4%	AC(偵測正確率)				82.1%
	Recall(召回率)				91.5%	Recall(召回率)				86.6%
	Precision(精確率)				80.2%	Precision(精確率)				79.4%
	F1 Score				85.5%	F1 Score				82.8%

表 7 適應性特徵選取方式與人為選取方式比較表(針對 LSB/PVD、50%藏密量)

針 對 新 式 L S B / P V D 藏 密 影 像 (5 0 % 藏 密 量) 之 偵 測 結 果										
執行 次數	本 研 究 適 應 性 特 徵 選 取 方 式					人 為 特 徵 選 取 方 式 ($b = 0$)				
	TP	FN	TN	FP	AC 值	TP	FN	TN	FP	AC 值
1	2368	632	2177	823	75.8%	2424	576	2080	920	75.1%
2	2368	632	2177	823	75.8%	2472	528	1945	1055	73.6%
3	2380	620	2156	620	75.6%	2358	642	2066	934	73.7%
4	2354	646	2192	808	75.8%	2354	646	2033	967	73.1%
5	2514	486	2077	923	76.5%	2378	622	2144	856	75.4%
6	2368	632	2177	823	75.8%	2333	667	2039	961	72.9%
7	2380	620	2156	844	75.6%	2331	669	2078	922	73.5%
8	2354	646	2192	808	75.8%	2472	528	2094	906	76.1%
9	2514	486	2077	923	76.5%	2466	534	2022	978	74.8%
10	2372	628	2120	880	74.9%	2410	590	2076	924	74.8%
平均	AC(偵測正確率)				75.7%	AC(偵測正確率)				74.3%
	Recall(召回率)				79.9%	Recall(召回率)				80.0%
	Precision(精確率)				74.4%	Precision(精確率)				71.8%
	F1 Score				77.0%	F1 Score				75.7%

表 8 適應性特徵選取方式與人為選取方式比較表(針對 IEMD/PVD、100%藏密量)

針 對 I E M D / P V D 藏 密 影 像 (1 0 0 % 藏 密 量) 之 偵 測 結 果										
執行 次數	本 研 究 適 應 性 特 徵 選 取 方 式					人 為 特 徵 選 取 方 式 ($b = 0$)				
	TP	FN	TN	FP	AC 值	TP	FN	TN	FP	AC 值
1	2692	308	2440	560	85.5%	2857	143	2143	857	83.3%
2	2670	330	2466	534	85.6%	2825	175	2131	869	82.6%
3	2676	324	2408	592	84.7%	2850	150	2124	876	82.9%
4	2685	315	2447	553	85.5%	2848	152	2113	887	82.7%
5	2681	319	2406	594	84.8%	2800	200	2197	803	83.3%
6	2661	339	2433	567	84.9%	2879	121	2105	895	83.1%
7	2673	327	2463	537	85.6%	2833	167	2148	852	83.0%
8	2700	300	2480	520	86.3%	2820	180	2164	836	83.1%
9	2683	317	2410	590	84.8%	2859	141	2140	860	83.3%
10	2699	301	2479	521	86.3%	2862	138	2133	867	83.3%
平均	AC(偵測正確率)				85.4%	AC(偵測正確率)				83.1%
	Recall(召回率)				89.4%	Recall(召回率)				94.8%
	Precision(精確率)				82.8%	Precision(精確率)				76.8%
	F1 Score				86.0%	F1 Score				84.8%

表 9 適應性特徵選取方式與人為選取方式比較表(針對 IEMD/PVD、75%藏密量)

針 對 I E M D / P V D 藏 密 影 像 (7 5 % 藏 密 量) 之 偵 測 結 果										
執行 次數	本 研 究 適 應 性 特 徵 選 取 方 式					人 為 特 徵 選 取 方 式 ($b = 0$)				
	TP	FN	TN	FP	AC 值	TP	FN	TN	FP	AC 值
1	2676	324	2146	854	80.4%	2640	360	1932	1068	76.2%
2	2639	361	2129	871	79.5%	2785	215	1987	1013	79.5%
3	2651	349	2192	808	80.7%	2660	340	1884	1116	75.7%
4	2633	367	2204	796	80.6%	2699	301	2030	970	78.8%
5	2648	352	2190	810	80.6%	2584	416	2042	958	77.1%
6	2621	379	2148	852	79.5%	2655	345	1990	1010	77.4%
7	2668	332	2163	837	80.5%	2766	234	1994	1006	79.3%
8	2659	341	2161	839	80.3%	2684	316	1840	1160	75.4%
9	2663	337	2086	914	79.2%	2704	296	1866	1134	76.2%
10	2662	338	2069	931	78.9%	2598	402	2008	992	76.7%
平均	AC(偵測正確率)				80.0%	AC(偵測正確率)				77.2%
	Recall(召回率)				88.6%	Recall(召回率)				89.3%
	Precision(精確率)				72.3%	Precision(精確率)				72.0%
	F1 Score				79.6%	F1 Score				80.0%

表 10 適應性特徵選取方式與人為選取方式比較表(針對 IEMD/PVD、50%藏密量)

針 對 I E M D / P V D 藏 密 影 像 (5 0 % 藏 密 量) 之 偵 測 結 果										
執行 次數	本 研 究 適 應 性 特 徵 選 取 方 式					人 為 特 徵 選 取 方 式 ($b = 0$)				
	TP	FN	TN	FP	AC 值	TP	FN	TN	FP	AC 值
1	2530	470	1950	1048	74.7%	2602	398	1720	1280	72.0%
2	2517	483	1925	1075	74.0%	2469	531	1812	1188	71.4%
3	2523	477	1957	1043	74.7%	2443	557	1754	1246	70.0%
4	2514	486	1943	1057	74.3%	2641	359	1664	1336	71.8%
5	2497	503	1977	1023	74.6%	2656	344	1703	1297	72.7%
6	2545	455	1935	1065	74.7%	2618	382	1746	1254	73.0%
7	2503	497	2005	995	75.1%	2520	480	1749	1251	71.2%
8	2512	488	2001	999	75.2%	2570	430	1806	1194	72.9%
9	2508	492	1966	1034	74.6%	2574	426	1715	1285	71.5%
10	2499	501	1941	1059	74.0%	2606	394	1700	1300	71.8%
平均	AC(偵測正確率)				74.6%	AC(偵測正確率)				71.8%
	Recall(召回率)				83.8%	Recall(召回率)				85.7%
	Precision(精確率)				70.8%	Precision(精確率)				67.1%
	F1 Score				76.7%	F1 Score				75.2%

4.3.2 本研究藏密分析方法與 CSR 藏密分析技術比較

本研究相較於 2014 年 Denmark 等 3 位學者所提出的內容選擇殘差(Content-Selective Residuals, CSR)藏密分析技術，本研究藏密分析方法之偵測結果廣泛較佳(比較數據如表 11 與 12 所示)，其主要原因在於適應性特徵選取方式較能有效反映多數影像之特性。反之，CSR 所採用的人為選取方式則僅能就已進行人工檢視之影像群組尋求較佳之選項(此處人為選取之特徵值基準參考位置 b 設定為 0)。

表 11 針對新式 LSB/PVD 藏密影像之偵測正確率綜合比較表

偵測率/新式 LSB/PVD 藏密百分比	100%藏密	75%藏密	50%藏密
本 研 究 藏 密 分 析 方 法 偵 測 率	96.6%	84.4%	75.7%
人 為 特 徵 選 取 分 析 方 法 偵 測 率	95.8%	82.1%	74.3%
C S R 藏 密 分 析 技 術 偵 測 率	84.1%	62.7%	53.5%

表 12 針對 IEMD/PVD 藏密影像之偵測正確率綜合比較表

偵測率/IEMD/PVD 藏密百分比	100%藏密	75%藏密	50%藏密
本研究藏密分析方法偵測率	85.4%	80.0%	74.6%
人為特徵選取分析方法偵測率	83.1%	77.2%	71.8%
CSR 藏密分析技術偵測率	77.4%	63.3%	53.9%

本研究透過實驗測試，將所提出之適應性特徵值藏密分析方法，分別與人為固定式特徵選取之藏密分析方法及 CSR 藏密分析技術進行比較，可證實本研究所提出之藏密分析方法有較佳之偵測正確率。其中針對運用新式 LSB/PVD 藏密技術所藏密之影像，當藏密量為 100%、75%及 50%時，其偵測正確率分別可達到 96.6%、84.4%及 75.7%。另外，針對運用 IEMD/PVD 藏密技術所藏密之影像，當藏密量為 100%、75%及 50%時，其偵測正確率亦可分別達到 85.4%、80%及 74.6%。而在特徵值的選取上，本研究藏密分析方法與人為固定式特徵選取之藏密分析方法，均僅選取 4 個特徵值來進行藏密分析，相較於 CSR 藏密分析技術選取 1,183 個特徵值進行分析，可降低分析所需之運算資源。

4.3.3 本研究藏密分析方法運算時間

本研究藏密分析方法各階段運算時間，如表 13 所示。其中，針對影像進行特徵擷取佔較高比率之運算時間(項次 1)，而運用影像特徵集合進行 BPNN 訓練與偵測則較低(項次 2、3)。而整體訓練時間，為特徵擷取時間與 BPNN 訓練時間之和(項次 4)；整體偵測時間，為特徵擷取時間與 BPNN 偵測時間之和(項次 5)。

表 13 本研究藏密分析方法各階段運算時間

項次	運算內容	平均時間(秒)
1	對 6,000 張訓練影像或受測影像(3,000 張藏密前之載體影像、3,000 張藏密影像)進行特徵擷取	198.46
2	將 6,000 張訓練影像(3,000 張藏密前之載體影像、3,000 張藏密影像)之特徵集合，輸入 BPNN 進行分類訓練，產生訓練模型	14.23
3	對 6,000 張受測影像(3,000 張藏密前之載體影像、3,000 張藏密影像)之特徵集合，運用 BPNN 訓練模型(分類器)進行偵測	0.06
4	訓練時間(項次 1、項次 2 加總)	212.69
5	偵測時間(項次 1、項次 3 加總)	198.52

五、結論

本研究所提出之藏密分析方法，主要是透過觀察載體影像與藏密影像之像素差值直方圖，並找出兩者之間的差異，進而推導出偵測影像藏密與否最具關鍵性之特徵值計算機制。其中為了能夠因應個別影像之特性，本研究提出了一套適應性特徵值基準參考位置選取機制，可有效據此計算出適當之特徵值。依照本研究之藏密分析流程，先藉由輸入載體影像及藏密影像的特徵資料集，提供 BPNN 進行訓練以產生完成訓練的模型(分類器)，最後在影像測試階段，再利用已完成訓練的模型對輸入的測試影像進行偵測分

類。本研究利用 PYTHON 與 MATLAB 程式語言實作新式 LSB/PVD 與 IEMD/PVD 藏密技術、適應性特徵選取機制及 BPNN 訓練模型，並使用 BOSSBase 影像資料庫中之影像進行實驗。實驗數據證明本研究所提出之分析方法，針對前述兩種空間域藏密技術之藏密影像，分別可達 96.6%與 85.4%的偵測正確率。於後續的研究中，將進一步針對近年來各種新式空間域藏密技術，進行偵測結果之分析比較。

六、國防相關應用

6.1 秘密資訊傳遞強度檢測與藏密技術開發

本研究之目的是開發一套影像藏密分析方法，可有效針對藏密影像來進行分析偵測。當國防組織與國安單位間有運用空間域藏密技術進行秘密資訊傳遞之需求，則可以運用本方法來評估其藏密強度，以提升機敏訊息傳遞之安全性與隱匿性。同時，對於後續藏密技術的開發也有所助益。

6.2 空間域影像藏密分析

自 2001 年 9 月 11 日發生於美國本土的九一一事件後，國家社會遭受恐怖攻擊與駭客攻擊的威脅與日俱增，無時無刻都在發生。而在有心人士進行不法行動過程中，為了達到秘密通訊的目的，也可能會利用藏密技術來將重要訊息藏入不重要的影像中進行傳遞，這無論對組織或國家社會都會造成莫大的損害。有鑑於此，本研究可提供國防資安領域作為於資訊隱藏與藏密分析之參據，納入國防資安防護網之範疇，將可針對可疑影像實施偵測，避免不法資訊之傳遞。

參考文獻

- Barr, T., 2002. Invitation to cryptology, *Upper Saddle River*, NJ: Prentice Hall.
- Bender, W., Gruhl, D., Morimoto, N. and Lu, A., 1996. Techniques for data hiding, *IBM Systems Journal* (35:3), pp. 313–336.
- Boroumand, M., Chen, M. and Fridrich, J., 2018. Deep residual network for steganalysis of digital images, *IEEE Transactions on Information Forensics and Security* (14:5), pp.1181-1193.
- Denemark, T., Fridrich, J. and Holub, V., 2014. Further study on the security of S-UNIWARD, *SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics* (9028).
- Feng, J.-B., Lin, I.-C., Tsai, C.-S. and Chu, Y.-P., 2006. Reversible watermarking: current status and key issues, *International Journal of Network Security* (2:3), pp. 161-171.
- Hou, X., Zhang, T., Ji, L. and Wu, Y., 2017. Combating highly imbalanced steganalysis with small training samples using feature selection. *Journal of Visual Communication and Image Representation* (49), pp. 243-256.
- Johnson, N. and Jajodia, S., 1998. Exploring steganography: seeing the unseen. *Proceedings of Computer* (31:2), pp. 26-34.
- Khodaei, M. and Faez, K., 2012. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing, *IET Image Process* (6:6), pp. 677-686.
- Lerch-Hostalot, D. and Megías, D., 2016. Unsupervised steganalysis based on artificial training sets, *Engineering Applications of Artificial Intelligence* (50), pp. 45-59.
- Li, X., Li, J., Li, B. and Yang, B., 2013. High fidelity reversible data hiding scheme and prediction-error expansion, *Signal Processing* (93:1), pp. 198-205.
- Liu, H.-H., and Liu, C.-L., 2019. Universal steganalysis method for spatial domain steganography technique based on prediction-error histogram feature, *Journal of Technology* (34:1), pp. 46-47.
- McCulloch, W. S., and Pitts, W., 1943. A logical calculus of the ideas immanent in nervous activity, *The bulletin of mathematical biophysics* (5:4), 115-133.
- Ni, Z., Qing, S., Ansari, N. and Su, W. F., 2006. Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology* (16:3), pp. 354-362.
- Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G., 1999. Information hiding - a survey, *Proceedings of the IEEE* (87:7), pp. 1062-1078.
- Rumelhart, D. E., Hinton, G. E. and Williams, R. J., 1986. Learning representations by back-propagating errors, *Nature* (323:9), 533-536.
- Rosenblatt, F., 1958. The perceptron: a probabilistic model for information storage and organization in the brain. *Psychological Review*, (65:6).
- Shen, S. Y. and Huang, L. H., 2015. A data hiding scheme using pixel value differencing and improving exploiting modification directions, *Computers & Security* (48), pp. 131-141.
- Wu, D.-C. and Tsai, W.-H., 2003. A Steganographic method for images by pixel-value

differencing, *Pattern Recognition Letters* (24:9), pp. 1613-1626.

Wu, H.-C., Wu, N.-I, Tsai, C.-S. and Hwang, M.-S., 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods, *IEEE Proceedings on Vision, Image and Signal Processing* (152:5), pp. 611-615.

Zhang, X. and Wang, S., 2006. Efficient steganographic embedding by exploiting modification direction. *IEEE Communications Letters* (10:11), pp.781-783.

網路參考資料：

BOSS Break Our Steganographic System, BOSSBases (v0.93), <http://agents.fel.cvut.cz/boss/index.php?mode=VIEW&tmpl=materials> [Retrieved on May 8, 2019].