中正嶺學報 第五十三卷 第一期 民國 113. 05
JOURNAL OF C.C.I.T., VOL. 53, NO. 1, MAY, 2024
DOI：10.30188/JCCIT.202405_53(1).0002

適用於混合像素差值與最低位元取代藏密法之資訊隱藏分析技術

劉興漢*

國防大學管理學院資訊管理學系

摘　　要

本研究針對 Jung 學者提出的混合像素差值與最低位元取代藏密技術，提出 4 項有用的藏密分析特徵，並結合機率類神經網路及 BaseCover 影像資料庫進行實驗，以達到有效偵測的目標。實驗結果證明，本研究提出的 4 項特徵在偵測 Jung 學者的藏密技術產生之不同藏密量的偽裝影像時，最高可達到 98.3%的偵測正確率。而本方法與其它偵測技術相比較之實驗結果顯示，本研究對 Jung 學者的藏密技術之偵測正確率最佳，可證明本研究提出的 4 項特徵之有效性。

關鍵詞：像素差值、最低位元取代、藏密分析特徵、機率類神經網路

Specific Steganalysis for Data Hiding Scheme Using Hybrid PVD and LSB on Bit Plane

Hsing-Han Liu*

Department of Information Management, Management College, National Defense University

ABSTRACT

This research focuses on the hybrid steganography technique proposed by Jung, which combines pixel-value differencing and least significant bit methods. Four useful steganalysis features are proposed and combined with a probabilistic neural network and the BaseCover image database for experimentation, aiming to achieve effective detection. The experimental results demonstrate that the four features proposed in this research achieve a maximum detection accuracy of 98.3% when detecting differently steganography images with varying steganographic payloads using Jung's method. Comparing with other detection techniques, the results show that this research provides the best detection accuracy for Jung's method, which validates the effectiveness of the four proposed steganalysis features.

Keywords: pixel-value differencing, least significant bit, steganalysis feature, probabilistic neural network

文稿收件日期 112.07.26; 文稿修正後接受日期 113.01.08; *通訊作者
Manuscript received July 07, 2023; revised Jan 08, 2024; * Corresponding author

一、前　言

根據 2023 年台灣最新網路使用報告[1]指出，全國網路使用者人數已達 2,168 萬人，等同於全國 90.7% 人口，相較 2022 年多了 16 萬人。這也代表行動裝置越來越普及，其可運用的網速亦明顯提升，相比與 2022 年的網速成長 26%，來到 68.04 Mbps[1]。然而，處處可連網的便利環境相對帶來了潛在風險，有心人士可利用此便利性，竊取個人、企業或軍事單位的機敏訊息，造成個人隱私與著作權及單位運作上無法估量的危害。為確保個人、企業或軍事單位的機敏訊息，密碼學(Cryptograghy)的資料加密技術常用來維持訊息之機密性[2]。但加密演算法會對原始資料進行擾亂、混淆及替換，故加密後的文件會呈現毫無意義之內容，成為已加密文件的明顯表徵。而有心人士即能針對具有此特徵的訊息，進行中間人攻擊，故加密後訊息於網路上進行傳送時的安全性有所不足。為克服此問題，資訊隱藏技術(Information Hiding)應運而生。

資訊隱藏技術可將機敏訊息嵌入特定的載體影像(Cover Image)，例如圖片、影像或聲音，產生隱含機密的偽裝影像(Stego Image)。如此可避免有心人士察覺機敏訊息的存在，藉以保護機密資訊不被竊取，進而被破解或破壞。根據資訊隱藏技術應用的差異，可分為兩種主要發展方向。其一是數位浮水印技術，旨在保護智慧財產權，其可在不影響載體完整性的情況下嵌入著作權訊息。其二是藏密技術[3]，可進行秘密通訊。其主要方法是將密文嵌入於載體影像中，以避免有心人士的察覺。合法接收者在獲得偽裝影像後，可以根據取密程序提取密文。

由於 4G 行動網路的普及與各大電信公司持續地推廣 5G 行動網路，且幾乎人手一台行動上網設備[1]，快速滋養了藏密技術研發的環境。而數位影像由於其分佈廣泛、易於取得和具有大量的藏密空間等特點，已成為最常用的載體影像[4]。而良好的影像藏密技術需滿足不可察覺性(Imperceptibility)和高資訊負載(Payload)的要求[5]。不可察覺性指的是嵌入密文後的偽裝影像，人類視覺或統計上不會察覺影像產生失真情況。而高資訊負載則是藏密技術可嵌入大量密文。在實際的秘密通訊運用上，密碼學和藏密技術互相輔助。為提高通訊的安全性，傳送的訊息會先經密碼學技術加密，然後將密文嵌入載體影像，產生偽裝影像後於網路上傳送。

藏密技術可以根據所選擇的藏密空間分為轉換域和空間域技術。轉換域技術是先對載體影像進行頻率轉換，然後將密文嵌入至特定的頻帶。常用的轉換技術包括離散餘弦、小波和傅立葉轉換。而空間域藏密技術則直接修改原始像素值，完成隱藏訊息的目的。若要求相同失真率的情況下，轉換域藏密技術可嵌入的密文較空間域藏密技術少，因此學者更專注於空間域藏密技術的研究。

空間域藏密技術中，最常使用的方法是最不重要位元取代(Least Significant Bit, LSB)藏密法[6]，也被稱為 LSB 藏密法。然而，由於 LSB 藏密法改變了像素分佈的均勻性，容易被 RS 偵測技術[7]或 x^2 攻擊法[8]等統計分析技術攻擊，故許多學者提出了改進 LSB 藏密法的方法[9-11]。與上述 LSB 藏密法相比較，像素值差異藏密法(Pixel Value Difference, PVD)[12]的藏密量更高，且可躲避 RS 統計分析技術之偵測。故最近基於 PVD 的藏密技術[13-18]成為學者聚焦的資訊隱藏研究領域。

雖然藏密技術可以確保機密資訊的安全並隱藏訊息的存在，但若有心人士利用各種藏密技術來傳遞非法訊息，會對社會安全造成不良的影響。故發展藏密分析(Steganalysis)之相關技術，使其能夠檢測藏密技術是否受到濫用，亦可評估藏密技術對攻擊的抵抗能力，對確保人們生命財產安全與發展良好的藏密技術至關重要，而藏密分析技術可區分為特定藏密分析和通用藏密分析兩種技術。

特定藏密分析由於針對已知藏密法所產生的特徵進行設計，由於瞭解已知藏密演算法，於嵌入過程中會對載體影像產生特定影響，故特定藏密分析技術通常具有很高的偵測正確率。而通用藏密分析技術（亦稱為盲藏密分析）則在未知所分析的可疑影像應用何種藏密演算法的情況下，將受測影像從空間域轉換到不同的領域，尋找並擷取有效的特徵，並將特徵經由分類器進行訓練和學習，故通用藏密分析技術可以提供可靠的偵測正確率。特定藏密分析技術對於已知的藏密演算法效果較好，而通用藏密分析技術則更具彈性，可以應對未知的藏密演算法。這兩種技術在藏密分析領域扮演著重要的角色，旨在提高對非法藏密活動的檢測能力，確保數位資訊的安全性。

研究資訊隱藏的學者陸續發表以 PVD 為

DOI：10.30188/JCCIT.202405_53(1).0002

基礎的藏密法[12-18]，其中以 Jung 學者[16]提出將影像像素區分為像高位元與低位元，應用 PVD 於像素高位元部分嵌入密文，而像素低位元的部分，則利用 LSB 藏密。Jung 學者[16]的方法充分利用像素空間，藏密量優於其餘學者的方法[12-17]。然而對於 Jung 學者[16]提出的混合像素差值和最低位元取代藏密技術，尚未有學者進行藏密分析。因此，本研究的目標在於分析 Jung 學者的藏密技術，藉由擷取像素差值直方圖(Pixel Difference Histogram, PDH)的特徵，並結合機率類神經網路(Probabilistic Neural Network, PNN)的分類能力，以區分載體影像與混合 PVD 與 LSB 藏密法所產生的偽裝影像。由於本研究僅針對 Jung 學者的方法進行藏密分析，故屬於特定藏密分析技術。其貢獻在於提出了 4 項可辨別出受測影像是否藏密的有效特徵，實驗證明提供了極佳的偵測正確率。透過本研究對 Jung 學者藏密技術的分析，瞭解 Jung 學者藏密方法對載體影像的改變，能夠對其藏密技術進行有效偵測。

本研究剩餘章節說明如下：第 2 節探討與本研究有關的文獻；第 3 節說明本研究提出的特徵與偵測流程；第 4 節為本研究之實驗結果及討論；第 5 節為本研究之結論。

二、文獻探討

2.1 Jung 學者之混合像素差值與最低位元取代藏密法之藏密技術

在先前學者[12-15, 17]的研究過程中，像素差值（PVD）和最低位元取代法（LSB）通常於不同的像素區塊內單獨或組合使用。Jung 學者[16]於 2018 年提出混合像素差值(PVD）和最低位元取代法（LSB）的資訊隱藏技術，此方法將載體影像切割成連續且不重疊的 1×2 像素區塊後，將區塊內十進位的像素值轉為二進位數值，分為高位元組（二進位數值的前 6 個位元）和低位元組（二進位數值的後 2 個位元），並分別應用 2-bit LSB 藏密法在低位元組以及 PVD 藏密法在高位元組。藉由這兩種藏密法的結合，影像嵌入容量得以提高，同時也保持著低失真的視覺影像品質，以下是 Jung 學者[16]所提方法(以下稱為混和 PVD 與 LSB）的藏密流程說明：

步驟 1：將載體影像依序分割為 1×2 個連續且不重疊的區塊。

步驟 2：計算區塊內個別像素值商數(高位元)及餘數(低位元)，並設定低位元最低位元取代法之置換量為 2 位元($k = 2$)。

$$(P_i^m, P_{i+1}^m) = \left(P_i \ div \ 2^k, P_{i+1} \ div \ 2^k\right)$$
$$\left(P_i^l, P_{i+1}^l\right) = \left(P_i mod \ 2^k, P_{i+1} mod \ 2^k\right) \quad (1)$$

步驟 3：接著依公式(2)計算兩像素商值之差值 d_i^m。

$$d_i^m = |P_{i+1}^m - P_i^m| \quad (2)$$

步驟 4：設定藏密過程所需之藏密區間範圍表，如表 1 所示。

表 1. Jung 學者藏密法之差值區間範圍表

Range(R_i)	R_1	R_2	R_3	R_4
範圍$[l_i, u_i]$	[0,7]	[8,15]	[16,31]	[32,63]
可藏位元數(n)	3	3	4	5

步驟 5：依表 1 之藏密區間範圍表，得可藏位元數 n，並從二進位秘密訊息取 n 位元，並轉換十進位為b_i^m，計算新差值$d_i'^m$。

$$d_i'^m = l_i + b_i^m \quad (3)$$

步驟 6：利用公式(4)計算像素新舊差值m，並依公式(5)計算藏密後之偽裝像素值$(p_i'^m, p_{i+1}'^m)$。

$$m = |d_i'^m - d_i^m| \quad (4)$$

$$(P_i'^m, P_{i+1}'^m) = \begin{cases} (P_i^m - \lceil m/2 \rceil, P_{i+1}^m + \lfloor m/2 \rfloor) & \text{, if } d_i^m \text{ is odd} \\ (P_i^m - \lfloor m/2 \rfloor, P_{i+1}^m + \lceil m/2 \rceil), & \text{if } d_i^m \text{ is even} \end{cases} \quad (5)$$

步驟 7：區塊像素值各嵌入 k 位元 LSB，從二進位秘密訊息取 k 位元，並轉換成十進位b_i^{l1}及b_i^{l2}，依公式(6)可得偽裝像素值(P_i', P_{i+1}')。

$$(P_i', P_{i+1}') = \left(P_i'^m \times 2^k\right) + \sum_{i=0}^{n-1} b_i^{l1}, \left(P_{i+1}'^m \times 2^k\right) + \sum_{i=n}^{2n-1} b_i^{l2} \quad (6)$$

Jung 學者藏密法取密過程說明如下：

步驟 1：將偽裝影像區分成 1×2 個連續相鄰且不重疊的區塊，並將偽裝像素(P_i', P_{i+1}')分別提取 k 位元，並依公式(7)計算新的像素值$(p_i'^m, p_{i+1}'^m)$。

$$(p_i'^m, p_{i+1}'^m) = \begin{cases} (P_i' - (P_i' \ \ mod \ \ 2^k))\text{div } 2^k \\ (P_{i+1}' - (P_{i+1}' \ \ mod \ 2^k))\text{div } 2^k \end{cases} \quad (7)$$

步驟 2：依公式(8)計算像素差值，並對照表 1 之藏密區間範圍表，得知可藏密區間R_i及區間範圍最小值l_i、藏密位元數n，計算秘密訊息b_i^m，並將十進位b_i^m轉換二進位取出密文。

$$\begin{aligned} d_i'^m &= |p_{i+1}'^m - p_i'^m| \\ b_i^m &= |d_i'^m - l_i| \end{aligned} \tag{8}$$

2.2 SPAM 特徵

Pevny 等學者[19]於 2010 年提出以 Subtractive Pixel Adjacency Matrix(SPAM) 特徵為基礎的通用藏密分析技術。由於影像相鄰像素間的相關性極高，故 SPAM 擷取相鄰像素間的特徵值。而得到 SPAM 特徵後，需搭配機器學習相關分類演算法，始能完成藏密偵測之效果。以下說明如何從影像擷取 SPAM 特徵。

因為未藏密的影像(即載體或自然影像)相鄰像素間之關聯性極高，故 SPAM 特徵的計算方式，分別針對左、右、下、上、右上、右下、左上及左下 8 個方向，計算其差值，而相對應差值的有效範圍，則利用門檻值(T)指定。

SPAM 特徵可分為一階特徵值及二階特徵值。SPAM 的一階特徵值是藉由一階馬可夫程序，利用公式(9)計算。

$$\mathbf{M}_{u,v}^{\rightarrow} = \Pr\left(\mathbf{D}_{i,j+1}^{\rightarrow} = u \mid \mathbf{D}_{i,j}^{\rightarrow} = v\right) \tag{9}$$

而 SPAM 的二階特徵值則依二階馬可夫程序，並利用公式(10)計算。

$$\mathbf{M}_{u,v,w}^{\rightarrow} = \Pr\left(\mathbf{D}_{i,j+2}^{\rightarrow} = u \middle| \mathbf{D}_{i,j+1}^{\rightarrow} = v \middle| \mathbf{D}_{i,j}^{\rightarrow} = w\right) \tag{10}$$

依指定門檻值(T)的不同，SPAM 的一階特徵值分別為 162 個(T=4)及 578 個(T=4)，而 SPAM 的二階特徵值則為 686 個(T=4)。

2.3 CSR 特徵

Denemark 等學者[20]於 2014 年提出基於內容選擇性殘差(Content-Selective Residuals, CSR)特徵，提出針對 S-UNIWARD 藏密法進行偵測的藏密分析技術。而 CSR 特徵亦可對其餘空間域藏密技術進行偵測。

為擷取 CSR 特徵，首先須將影像分成互不交集的像素類別，分別為那些在藏密過程中可能會改變的像素與那些藏密過程中不太可能會改變的像素。然後，從這兩個類別計算噪聲殘差(noise residuals)，也就是所謂的內容選擇性殘差(CSR)。最後，特徵向量由 CSR 的一階、二階和三階統計數據組成，如公式(11)至公式(13)所示。

$$R_{i,j}^{(1)} = X_{i,j+1} - X_{i,j} \tag{11}$$

$$R_{i,j}^{(2)} = X_{i,j+1} - 2X_{i,j} + X_{i,j-1} \tag{12}$$

$$R_{i,j}^{(3)} = -X_{i,j+2} + 3X_{i,j+1} - 3X_{i,j} + X_{i,j-1} \tag{13}$$

公式(11)至公式(13)是經水平方向計算殘差值，Denemark 等學者為了增強 CSR 特徵的強韌性，將受測影像轉置後，再以公式(11)至公式(13)運算，亦即針對垂直方向計算殘差值。最後，整合水平與垂直方向的殘差值，得到 CSR 的 1183 個特徵。

2.4 基於 PEH 之通用藏密分析技術

2019 年 Liu 等學者[21]基於預測誤差直方圖（Prediction Error Histogram, PEH）的 8 項特徵(如表 2 所示)，提出可偵測空間域藏密法之通用藏密分析技術。主要利用載體影像與偽裝影像於預測差值直方圖(PEH)之間的差異，作為可供藏密分析的有效特徵，並使用機率類神經網路(PNN)進行分類，以辨別受測影像為載體影像或為偽裝影像。

表 2. Liu 等學者基於 PEH 的 8 項特徵

編號	特徵
1	$F_1=(H_0-H_1)/(H_1-H_2)$
2	$F_2=(H_0-H_{-1})/(H_{-1}-H_{-2})$
3	$F_3=(H_1-H_2)/(H_2-H_3)$
4	$F_4=(H_{-1}-H_{-2})/(H_{-2}-H_{-3})$
5	$F_5=H_1/H_2$
6	$F_6=H_{-1}/H_{-2}$
7	$F_7=H_1/H_3$
8	$F_8=H_{-1}/H_{-3}$

Liu 等學者針對現行常用的 12 種空間域藏密技術(如表 3 所示)進行分析，其藏密法所設定的藏密量為 100%。實驗結果顯示，Liu 等學者提出的藏密分析技術對於使用 100%藏密量之不同空間域藏密技術，可提供 98.2%以上之偵測正確率，且與現行之通用藏密分析技術相比較下，可提供較佳的偵測正確率。

DOI：10.30188/JCCIT.202405_53(1).0002

表 3. Liu 等學者偵測空間域藏密法列表

類別	藏密法(藏密容量均最大藏密量)
LSB Based	*k*-bit LSB (*k*=1,2,3)
PVD Based	PVD, Modified PVD, Enhanced PVD, Tri-way PVD, Modulus PVD and Adaptive PVD
PEHS Based	Kim's PEHS method, Hong's PEHS method, and Tsai's PEHS method
PVO Based	Li's PVO, Chen's PVO

2.5 機率類神經網路

1990 年 Specht 學者[22]提出機率類神經網路(PNN)，其架構屬於四層神經元架構的網路模型(如圖 1 所示)，PNN 理論架構在貝氏決策(Bayesian Decision)的基礎上。PNN 的優勢在於學習速度快，對於錯誤的資訊具有相當的容忍性，並且在樣本不足的情況下，可以根據問題直接調整參數，快速有效地解決任意維度輸出的分類問題，因此受到學者高度重視。

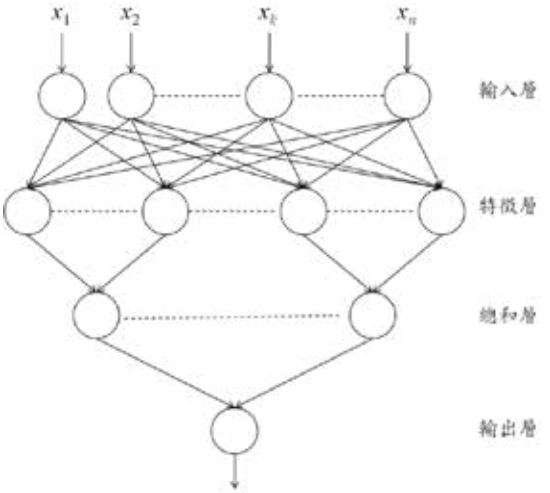

圖 1. 機率類神經網路架構圖

圖 1 為機率類神經網路架構圖，包含輸入層、特徵層、總和層及輸出層。其特徵層內的每組特徵單元，接收來自輸入層相同的資料。

圖 2 說明了每組特徵單元，使用輸入特徵向量 $\mathbf{X}$ 與權重向量 $\mathbf{W}_i$ 進行運算，利用公式(14)求出其內積值。

$$z_i = \mathbf{X} \cdot \mathbf{W}_i \text{，} \qquad (14)$$

其中 $\mathbf{X}=(x_1, x_2, \ldots, x_n)$，$\mathbf{W}_i=(w_{i1}, w_{i2}, \ldots, w_{in})$，$i$ 代表特徵單元的索引值。

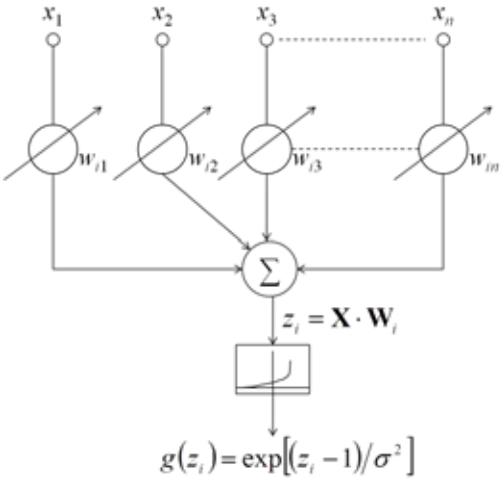

圖 2. 機率類神經網路的特徵單元

而 PNN 的特徵單元則使用 $\exp[(z_i-1)/\sigma^2]$ 對 z_i 執行非線性運算後，將運算值傳送至總和層。z_i 的輸出值可分成 m 個群組 G，而群組 G 的數量需與總和層神經元的個數相符，而且要與分類類別的個數相同。利用公式(15)，總和層內的神經元計算來自特徵層的輸入總和：

$$S_j = \sum_{i \in G_j} \exp[-(\mathbf{W}_i - \mathbf{X})^T (\mathbf{W}_i - \mathbf{X})/2\sigma^2] \quad (15)$$

其中，S_j 為總和層第 j 個神經元的輸出，$j \in \{1, 2, \ldots, m\}$。最後，輸出層得到總和層全部的輸出值，並輸出具有最大 S_j 的類別值，此值代表PNN之分類結果。

三、本偵測技術

可用於偵測 Jung 學者[16]提出的混合 PVD 與 LSB 藏密法的技術（以下稱為本偵測技術）於本節提出，其主要基於偽裝影像的 PDH 特徵，並結合 PNN 分類器來進行藏密偵測。首先，對 Jung 學者的混合 PVD 與 LSB 藏密法，完成載體影像嵌密程序後，所得偽裝影像的 PDH 進行分析。其次，說明本偵測技術針對 Jung 學者的混合 PVD 與 LSB 藏密法，分析擷取相關特徵值的過程。最後，描述本偵測技術判定受測影像是否是偽裝影像的流程。

3.1 混合像素差值與最低位元取代藏密法之分析

因 Jung 學者[16]提出的混合 PVD 與 LSB 藏密技術，主要將像素區分為高位元及低位

元，並以 PVD 法進行高位元部分的藏密，而低位元部分則使用 LSB 嵌入密文。為找出 Jung 學者的方法於藏密前後異常的情形，本研究以像素差值直方圖(PDH)進行分析(如圖 3 所示)。圖 3 中藍色實線為載體影像之 PDH，而紅色虛線為 Jung 學者所提方法之偽裝影像的 PDH，由於其方法高藏密量的緣故，導致載體與偽裝影像的 PDH 有顯著的差異。後續比對載體與偽裝影像的 PDH，定義有偵測成效之特徵，可作為區分載體與偽裝影像之基礎。

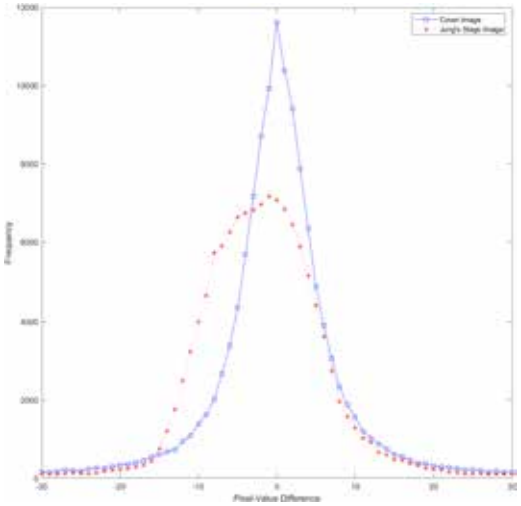

圖 3. 載體影像與偽裝影像像素差值直方圖

進一步地觀察圖4與圖5，可發現載體影像與「混合PVD與LSB藏密法」所產生的偽裝影像之PDH，於像素差值為0之左側部分(請看圖4與圖5紅色引號標示之處)，各差值的分佈有顯著的不同，本研究即以此建構出可偵測 Jung 學者方法之資訊隱藏分析特徵。

3.2 本偵測技術使用之特徵值

因 Jung 學者的藏密法具有可嵌入大量密文之特性，使得偽裝影像的PDH呈現了不正常的分布(如圖5所示)。為利於解釋本偵測技術之特徵，圖6示意了PD值為-15至15的PDH，其中P_0為PDH的峰值；P_{-x}為負的像素差值，而本文所提特徵參考的像素差值區間為-1至-3。

由於載體影像與 Jung 學者藏密法之偽裝影像之PDH，於其各自PD區間為-1至-3有顯著差異，為了將上述的差異特徵化，將像素差值為0的統計值分別除以像素差值為-1與-2的統計值，及將像素差值為-1的統計值分別除以像素差值為-2與-3的統計值，得到其比率值。故本偵測技術使用PDH之PD間經除法運算後所的比率值，作為混合PVD與LSB藏密法藏密之4項特徵，整理如表4所示。

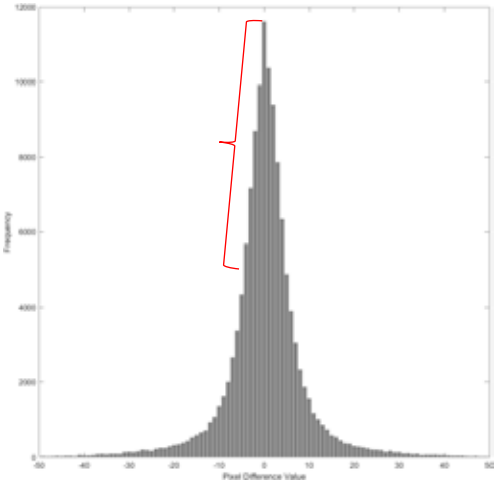

圖 4. 載體影像的像素差值直方圖

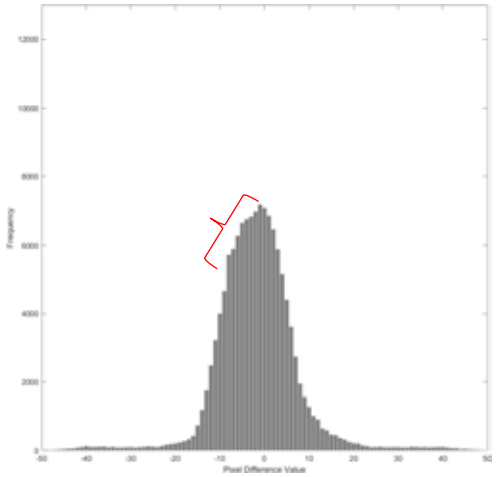

圖 5. 偽裝影像的像素差值直方圖

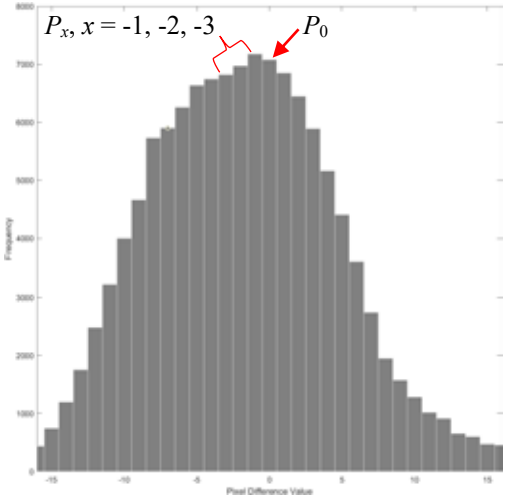

圖 6. PD 值從-15 至 15 之 PDH 示意圖

DOI：10.30188/JCCIT.202405_53(1).0002

表4. 本偵測技術之4項特徵值

特徵值符號	特徵值計算
F_1	P_0/P_{-1}
F_2	P_0/P_{-2}
F_3	P_{-1}/P_{-2}
F_4	P_{-1}/P_{-3}

為驗證F_1至F_4特徵值的區別度，本研究針對實驗使用的BaseCover影像資料庫[23]中10,000張載體影像及相對應的混合PVD與LSB藏密法之偽裝影像擷取4項特徵值，其結果如圖7至圖10所示，其橫軸與縱軸分別標註測試影像及影像擷取之F_1至F_4的特徵值。

觀察圖7至圖10之特徵值分佈結果，可發現載體影像的特徵值F_1至F_4呈現隨機的分佈態樣；但因混合PVD與LSB藏密技術已將密文嵌入於像素，故偽裝影像F_1至F_4的特徵值呈現聚集現象，故載體與偽裝影像F_1至F_4特徵值的分佈呈現兩顯著不同的群組。

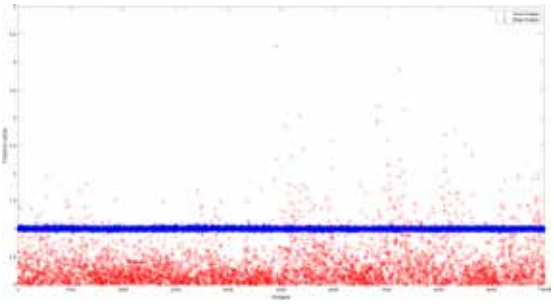

圖 7. 載體影像與偽裝影像之 F_1 特徵值分佈圖

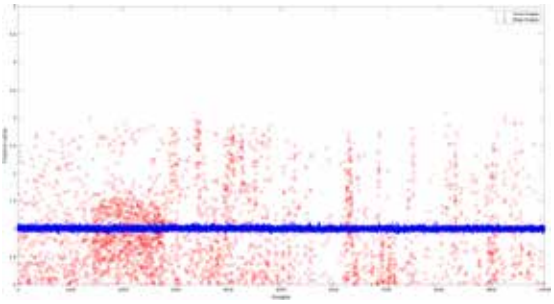

圖 8. 載體影像與偽裝影像之 F_2 特徵值分佈圖

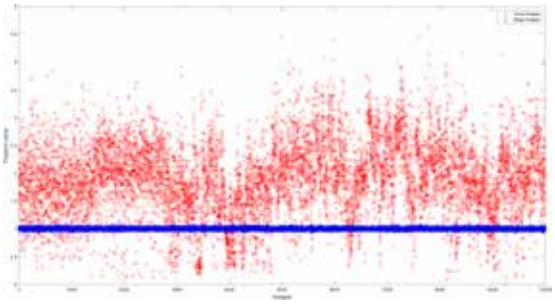

圖 9. 載體影像與偽裝影像之 F_3 特徵值分佈圖

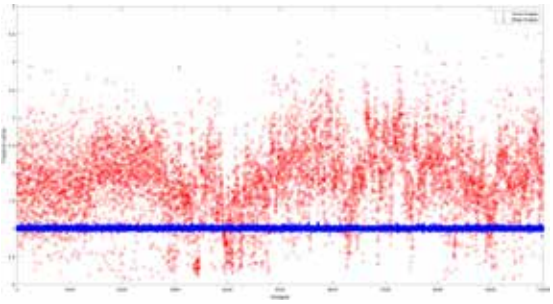

圖 10. 載體影像與偽裝影像之 F_4 特徵值分佈圖

3.3 本研究之偵測流程

本研究之偵測流程結合表 4 之 4 項特徵值與機率類神經網路(PNN)分類器，並分為兩個階段。其一為 PNN 分類模型生成階段、其二為受測影像偵測階段，藉以判斷受測影像為載體影像或為「混合 PVD 與 LSB 藏密法」之偽裝影像，本研究之詳細偵測流程圖如圖 11 所示。

在分類模型生成階段，利用 BaseCover 影像資料庫之 10,000 張 8 位元 512*512 大小之載體影像與相對應的偽裝影像作為訓練影像，並根據表 4 之 4 項特徵值對訓練影像擷取特徵值，產生訓練影像樣本之特徵值集合。由於 PNN 屬監督式學習，故分別設定偽裝影像之分類標籤為 1 而載體影像分類標籤為 2 後，將訓練樣本特徵集合與相對應之分類標籤，輸入 PNN 分類器執行訓練後，生成訓練模型(Trained Model)。

在受測影像偵測階段，亦針對受測影像樣本擷取其 4 項特徵值，並輸入至 PNN 分類器偵測。PNN 分類器根據訓練模型對受測影像樣本進行判斷，並輸出相對應之分類結果。若輸出之標籤為 1，即是偽裝影像；若輸出之標籤為 2，即是載體影像。

四、實驗結果

本節進行相關實驗，藉此檢驗所提之 4 項針對「混和 PVD 與 LSB」演算法之藏密分析特徵，可以有效偵測「混合 PVD 與 LSB」藏密技術。本研究各項實驗結果同時與現行的通用藏密分析技術進行比較，以證明本偵測技術之快速及有效性。以下各節說明本研究相關實驗使用的軟硬體環境、實驗執行的步驟、實驗使用的影像資料庫、不同實驗場景的設計及實驗結果。

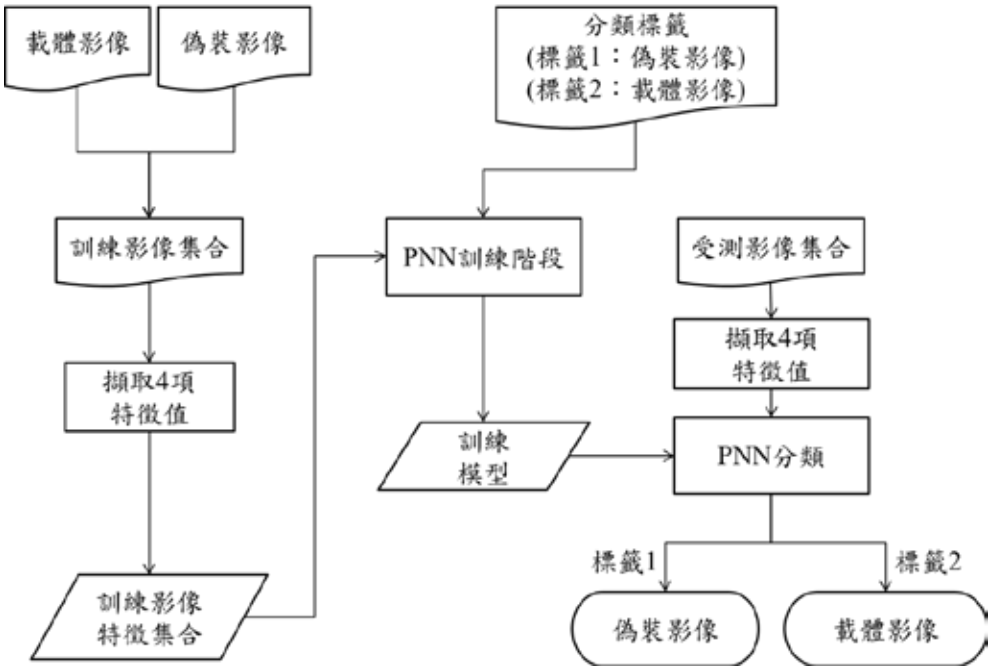

圖 11. 本研究之偵測流程圖

4.1 實驗環境

本研究實驗過程使用之硬體與軟體環境及實驗影像資料庫如下說明：

(1) 硬體環境：使用 Intel(R) Core(TM) i5-6300HQ CPU @ 2.30GHz 16GB RAM 筆記型電腦。

(2) 軟體環境：主要以 MATLAB R2023a 進行以下實驗程序，包含撰寫「混合 PVD 與 LSB 藏密技術」與四項特徵值萃取程式、使用內建之亂數產生器模擬加密後之祕密訊息，最後採用類神經網路工具箱所內建的機率類神經網路相關指令作為 PNN 分類器。

(3) 影像資料庫：本研究使用 BaseCover 影像資料庫[23]，包含了 10,000 張 8 位元 512*512 大小之灰階影像，圖 12 顯示 BaseCover 影像資料庫其中 6 張範例影像。為證明本偵測技術提出的 4 項特徵能適用於不同藏密量(100%、75%及 50%)之偽裝影像，本研究利用「混合 PVD 與 LSB 藏密技術」，以 BaseCover 影像資料庫為載體影像，分別產生了各 10,000 張 100%、75%及 50%藏密量之偽裝影像，進行後續的實驗。

圖 12. BaseCover 影像資料庫之範例影像

4.2 實驗步驟

本研究之實驗步驟如下所述：

步驟一：分別輸入 BaseCover 影像資料庫的載體影像和「混合 PVD 與 LSB 藏密技術」產生的偽裝影像。

步驟二：從 BaseCover 影像資料庫中隨機選取 50%(30%、10%)的載體影像，並從相對應的偽裝影像中選取相同的 50%(30%、10%)偽裝影像，組合成訓練影像樣本。因受測的 BaseCover 影像資料庫共有 10,000 張 512*512 大小之載體影像，故從影像資料庫隨機選取 50%的載體影像，即表示隨機選取 5,000 張影像。而 30%及 10%，即表示分別隨機選取 3,000 及 1,000 張影像。

步驟三：使用本研究提出之 4 項特徵值擷取程式，對隨機選取的載體影像和對應的偽裝影像進行特徵值擷取。

DOI：10.30188/JCCIT.202405_53(1).0002

步驟四：將步驟三中獲得的訓練影像特徵值集合和相對應的分類標籤輸入 PNN 分類器進行分類訓練，生成訓練模型。
步驟五：從受測影像資料庫中選取剩餘 50%(70%、90%)的載體影像，並從對應的偽裝影像中選取剩餘相對應的偽裝影像，組合成受測影像樣本，並使用本研究提出之 4 項特徵值擷取程式進行特徵值的擷取。
步驟六：將步驟四中獲得的訓練模型和步驟五中獲得的受測影像的特徵值集合分別輸入 PNN 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共 10 次，並計算分類結果的平均值。

4.3 實驗場景

本研究使用「混合 PVD 與 LSB 藏密技術」，分別產生了各 10,000 張藏密量為 100%、75%及 50%之偽裝影像。本研究第一項實驗場景是在偽裝影像相同藏密量的情況下，訓練影像與測試影像的選取影像張數不同，其實驗細節如表 5 說明。而本研究第二項實驗場景是使用不同藏密量之偽裝影像進行訓練，並產生已完成訓練的模組，藉以偵測不同藏密量之測試影像，訓練影像與測試影像各為隨機選取之 5,000 張載體影像和與其相對應之 5,000 張偽裝影像，其實驗細節如表 6 說明。

表 5. 相同藏密量之偽裝影像，訓練影像與測試影像的選取比例

偽裝影像之藏密量	訓練影像與測試影像的選取比例
10,000 張藏密量分別為 ● 100%之偽裝影像 ● 75%之偽裝影像 ● 50%之偽裝影像	訓練影像為 50%(各 5,000 張載體與偽裝影像)與測試影像為 50%(另外 5,000 張載體與偽裝影像)
	訓練影像為 30%(各 3,000 張載體與偽裝影像)與測試影像為 70%(另外 7,000 張載體與偽裝影像)
	訓練影像為 10%(各 1,000 張載體與偽裝影像)與測試影像為 90%(另外 9,000 張載體與偽裝影像)

表 6. 使用不同藏密量之偽裝影像進行訓練，偵測不同藏密量之測試影像

訓練模組 (隨機選取各 5,000 張之載體與偽裝影像)	不同藏密量之測試影像 (隨機選取其餘各 5,000 張之載體與偽裝影像)
使用藏密量為 100%之偽裝影像進行訓練	偵測 75%藏密量之偽裝影像
	偵測 50%藏密量之偽裝影像
使用藏密量為 75%之偽裝影像進行訓練	偵測 100%藏密量之偽裝影像
	偵測 50%藏密量之偽裝影像
使用藏密量為 50%之偽裝影像進行訓練	偵測 100%藏密量之偽裝影像
	偵測 75%藏密量之偽裝影像

根據表 5 和表 6 所選定的訓練影像，使用本研究提出之 4 項特徵值擷取程式取出特徵值，獲得訓練影像的特徵值集合。接著將這些特徵值集合與相對應的分類標籤輸入 PNN 分類器進行分類訓練，生成訓練模型。然後，使用相同的特徵值擷取程式對表 5 和表 6 中列出的測試影像樣本進行特徵值擷取，生成測試影像的特徵值集合。將前一步驟所得的訓練模型和測試影像的特徵值集合分別輸入 PNN 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，並計算分類結果的平均值。

4.4 實驗結果

表 7 至表 9 為依 4.2 節實驗步驟與 4.3 節第一項實驗場景之實驗結果，而表 10 至表 12 為依 4.2 節實驗步驟與 4.3 節第二項實驗場景之實驗結果，其中 AC 值為偵測正確率，定義如下：

$$AC = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \qquad (16)$$

其中，*TP*（True Positive）表示受測影像被正確偵測出藏密的數目；*TN*（True Negative）表示受測影像被正確偵測出未藏密的數目；*FP*（False Positive）表示受測影像被錯誤地偵測出藏密的數目；*FN*（False Negative）表示受測影像被錯誤地偵測出未藏密的數目。以上變數可用於評估藏密分析的性能，以衡量其對於偽裝影像的識別準確度。

表 7. 藏密量 100%偽裝影像，分別使用 5000、3000 及 1000 張影像訓練模組之偵測正確率

偽裝影像藏密量	訓練與測試影像選取比例	執行 10 次的平均值				
		TP	*FN*	*TN*	*FP*	*AC*
藏密量為 100%	訓練與測試各為為 50%	5000	0	4829.2	170.8	0.983
	訓練為 30%、測試為 70%	7000	0	6745	255	0.982
	訓練為 10%、測試為 90%	9000	0	8601.7	398.3	0.978

表 8. 藏密量 75%偽裝影像，分別使用 5000、3000 及 1000 張影像訓練模組之偵測正確率

偽裝影像藏密量	訓練與測試影像選取比例	執行 10 次的平均值				
		TP	*FN*	*TN*	*FP*	*AC*
藏密量為 75%	訓練與測試各為為 50%	4949.6	50.4	4281.5	718.5	0.923
	訓練為 30%、測試為 70%	6921.3	78.7	5963.4	1036.6	0.920
	訓練為 10%、測試為 90%	8869.7	130.3	7563.8	1436.2	0.913

表 9. 藏密量 50%偽裝影像，分別使用 5000、3000 及 1000 張影像訓練模組之偵測正確率

偽裝影像藏密量	訓練與測試影像選取比例	執行 10 次的平均值				
		TP	*FN*	*TN*	*FP*	*AC*
藏密量為 50%	訓練與測試各為為 50%	4540.4	459.6	3659.7	1340.3	0.820
	訓練為 30%、測試為 70%	6329.5	670.5	5085.5	1914.5	0.815
	訓練為 10%、測試為 90%	7977.8	1022.2	6406.2	2593.8	0.799

表 10. 以藏密量為 100%偽裝影像產生訓練模組之偵測正確率

產生訓練模組的影像藏密量	測試影像的藏密量	執行 10 次的平均值				
		TP	*FN*	*TN*	*FP*	*AC*
藏密量為 100%	藏密量為 75%	1579.8	3420.2	4828	172	0.641
	藏密量為 50%	621.2	4378.8	4830	170	0.545

表 11. 以藏密量為 75%偽裝影像產生訓練模組之偵測正確率

產生訓練模組的影像藏密量	測試影像的藏密量	執行 10 次的平均值				
		TP	*FN*	*TN*	*FP*	*AC*
藏密量為 75%	藏密量為 100%	5000	0	4280.4	719.6	0.928
	藏密量為 50%	3211.6	1788.4	4282.4	717.6	0.749

DOI：10.30188/JCCIT.202405_53(1).0002

表 12. 以藏密量為 50%偽裝影像產生訓練模組之偵測正確率

產生訓練模組的影像藏密量	測試影像的藏密量	執行 10 次的平均值				
		TP	*FN*	*TN*	*FP*	*AC*
藏密量為 50%	藏密量為 100%	5000	0	3672.3	1327.7	0.867
	藏密量為 75%	4915.4	84.6	3665.6	1334.4	0.858

表 13. SPAM、CSR 及 PEH 特徵與本偵測技術之偵測正確率比較

Jung 方法	SPAM 特徵	CSR 特徵	PEH 特徵	本偵測技術
藏密量為 100%之偽裝影像	94.1%	95.9%	97%	98.3%
藏密量為 75%之偽裝影像	90.9%	86.9%	87.9%	92.3%
藏密量為 50%之偽裝影像	76.3%	74.6%	74%	82%

表 14. SPAM、CSR 及 PEH 特徵與本偵測技術之執行時間比較 (單位：秒)

Jung 方法	SPAM 特徵	CSR 特徵	PEH 特徵	本偵測技術
藏密量為 100%之偽裝影像	7191.46	21972.86	928.16	690.35
藏密量為 75%之偽裝影像	6936.32	22862.85	920.11	672.44
藏密量為 50%之偽裝影像	6745.18	19909.15	941.29	697.38

從表 7 至表 9 第一項實驗場景之實驗結果，可得在偽裝影像相同藏密量的前提下，選取不同張數之訓練與測試影像，其偵測正確率無太大差異。表示本研究提出的 4 項特徵，具有其顯著代表性。即便於不同藏密量，以 1,000 張訓練影像生成訓練模組，偵測 9,000 張測試影像的情況，其偵測正確率分別為 97.8%、91.3%與 79.9%。

從表 10 至表 12 第二項實驗場景之實驗結果，可看出若以不同藏密量產生訓練模組，其偵測正確率有顯著的不同。表 10 的偵測正確率分別為 64.1%與 54.5%，其偵測率不佳的原因，在於是以藏密量為 100%之偽裝影像產生訓練模組，所擷取之 4 項特徵明顯不適用於藏密量為 75%與 50%之偽裝影像。表 11 的偵測正確率分別為 92.8%與 74.9%，表示使用藏密量為 75%之偽裝影像產生訓練模組擷取之 4 項特徵，能有效偵測藏密量為 100%之偽裝影像，而偵測藏密量為 50%之偽裝影像，其偵測結果尚可接受。表 12 的偵測正確率分別為 86.7%與 85.8%，表示使用藏密量為 50%之偽裝影像產生訓練模組擷取之 4 項特徵，偵測藏密量為 100%與 75%之偽裝影像，均能達到 85%以上的偵測正確率。

為證明本偵測方法之可用性，本研究分別與 2010 年 Pevny 等學者[19]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、2014 年 Denemark 等 3 位學者[20]所提出的內容選擇殘差（CSR）藏密分析技術及 2019 年 Liu 等學者[21]基於預測誤差直方圖（PEH）的 8 項特徵，適用於空間域之通用藏密分析方法進行比較。SPAM 與 CSR 之特徵擷取程式於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[24]下載。本研究使用 BaseCover 影像資料庫，並依 4.2 節實驗步驟訓練及測試 SPAM、CSR 及 PEH 特徵，並依此設定進行實驗，所列 SPAM、CSR 及 PEH 特徵之偵測正確率即為其實驗結果。

由表 13 的結果可看出本偵測技術之正確率優於 Pevny 等學者[19]、Denemark 等 3 位學者[20]及 Liu 等 2 位學者[21]所提的偵測技術。且相較於 SPAM 的 686 項特徵、CSR 的 1183 項特徵及 PEH 的 8 項特徵，本偵測技術只需 4 項特徵，故所耗費的計算資源與時間亦低於 SPAM、CSR 及 PEH，如表 14 所示。觀察表 13 及表 14 的比較結果，可證明本分析技術之有用性。

五、結論

由於藏密技術可能被濫用，對國土和社會安全構成威脅，此狀況凸顯了發展藏密分析技術的重要與迫切性。本研究旨在針對 Jung 學

者提出的混合 PVD 與 LSB 藏密技術，提出有效的特徵，以有效偵測混合 PVD 與 LSB 藏密技術。

實驗過程將載體與偽裝影像區分為 1×2 相鄰且不重疊的像素區塊，並計算其像素差值，可得到載體與偽裝影像之 PDH，並比對這 2 組 PDH 之相異特徵，作為藏密分析的基礎。其藏密分析的流程可分為產生訓練模型及判斷受測影像兩階段。首先將載體與偽裝影像樣本與相對應的標籤輸入 PNN 分類器進行訓練後，產生完成訓練之模型。而判斷受測影像階段，則利用已訓練的模型分類受測影像。

為證明本研究使用 4 項藏密分析特徵之辨別性，實驗使用 MATLAB 實作 Jung 學者提出的混合 PVD 與 LSB 藏密技術及 4 項特徵值擷取程式，並結合了 PNN 分類器及 BaseCover 影像資料庫進行實驗。實驗部分可區分 2 類，其一是針對相同藏密量之偽裝影像，訓練影像與測試影像的選取比例不同之實驗；其二為使用不同藏密量之偽裝影像，進行訓練並產生訓練模型後，偵測不同藏密量之測試影像的實驗。實驗結果證明，本研究提出的 4 項特徵在偵測混合 PVD 與 LSB 藏密法產生之不同藏密量的偽裝影像時，最高可達到 98.3%的偵測正確率。而本方法與 SPAM、CSR 及 PEH 等通用型的偵測技術相比較之實驗結果顯示，本研究對混合 PVD 與 LSB 藏密法的偵測正確率最佳，證明本研究提出的 4 項特徵之有效性。

參考文獻

[1] TenMax，“2023 台灣最新網路使用報告，”https://www.tenmax.io/tw/archives/72881?utm_source=media&utm_medium=gvm&utm_campaign=pov. [Retrieved on July 10, 2023]

[2] Barr, T., Invitation to Cryptology, Prentice Hall, Upper Saddle River Press, Chap. 2, pp. 56-89, 2002.

[3] 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.

[4] Rabah, K., “Steganography-The Art of Hiding Data,” Information Technology Journal, Vol. 3, No. 3, pp. 245-269, 2004.

[5] Cacciaguerra, S. and Ferretti, S., “Data Hiding: Steganography and Copyright Marking,” http://www.cs.unibo.it/~scacciag/home_files/teach/datahiding.pdf.

[6] 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.

[7] 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.

[8] Westfeld, A. and Pfitzmann, A., “Attacks on Steganographic Systems,” Proceedings of the Third International Workshop on Information Hiding, Dresden, Germany, pp. 61-75, 1999.

[9] Lou, D. C. and Hu, C. H., “LSB Steganographic Method based on Reversible Histogram Transformation Function for Resisting Statistical Steganalysis,” Information Sciences, Vol. 188, pp. 346-358, 2012.

[10] Rustad, S., Setiadi, D. R. I. M., Syukur, A., and Andono, P. N., “Inverted LSB Image Steganography using Adaptive Pattern to Improve Imperceptibility,” Journal of King Saud University - Computer and Information Sciences, Vol. 34, No. 6, Part B, pp. 3559-3568, 2022.

[11] Setiadi, D. R. I. M., “Improved Payload Capacity in LSB Image Steganography uses Dilated Hybrid Edge Detection,” Journal of King Saud University - Computer and Information Sciences, Vol. 34, No. 2, pp. 104-114, 2022.

[12] 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.

[13] 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.

[14] Khodaei, M. and Faez, K., “New Adaptive Steganographic Method using Least-Significant-Bit Substitution and Pixel-Value Differencing,” IET Image Process, Vol. 6, No. 6, pp. 677-686. 2012.

[15] Shen, S. Y. and Huang, L. H., “A Data Hiding Scheme using Pixel Value Differencing and Improving Exploiting

DOI：10.30188/JCCIT.202405_53(1).0002

Modification Directions," Computers & Security, Vol. 48, pp. 131-141, 2015.
[16] Jung, K. H., "Data Hiding Scheme Improving Embedding Capacity using Mixed PVD and LSB on Bit Plane," Journal of Real-Time Image Processing, Vol. 14, No. 1, pp. 127-136, January, 2018.
[17] Liu, H. H., Su, P. C., and Hsu, M. H., "An Improved Steganography Method based on Least-Significant-Bit Substitution and Pixel-Value Differencing," KSII Transactions on Internet and Information Systems, Vol. 14, No. 11, pp. 4537-4556, Nov. 2020.
[18] Liu, H. H. and Lo, Y. F., "An Improved Steganographic Method based on Least-Significant-Bit Substitution and Modulus Pixel-Value Difference," Journal of Internet Technology, Vol. 22, No. 7, pp. 1609-1620, Dec. 2021.
[19] 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.
[20] Denemark, T., Fridrich, J., and Holub, V., "Further Study on the Security of S–UNIWARD," SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics (9028), 2014.
[21] Liu, H. H. and Liu, C. L., "Universal Steganalysis Method for Spatial Domain Steganography Technique based on Prediction-Error Histogram Feature," Journal of Technology, Vol. 34, No. 1, pp. 46-47, 2019.
[22] Specht, D. F., "Probabilistic Neural Networks," Neural Network, Vol. 3, No. 1 pp. 109-118, 1990.
[23] 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]
[24] Binghamton University, "Download Section of Digital Data Embedding Laboratory," http://dde.binghamton.edu/download/feature_extractors/. [Retrieved on May 15, 2021]