植基於最低位元取代與像素差值之資訊隱藏技術

劉興漢* 賀盛志 羅玉芬

國防大學資訊管理學系

論文編號：NM-42-02-02

來稿2021年3月7日→第一次修訂2021年9月15日→第二次修訂2022年4月1日→

同意刊登2022年5月17日

摘要

本研究提出空間域的最低位元取代法與像素差值之資訊隱藏技術，利用人體視覺系統觀察能力有限的情況下於灰階影像中隱藏秘密訊息。本研究是以 Jung 學者於 2018 年所提出混合 LSB/PVD 藏密法為基礎而改良的資訊隱藏方法，其方法是將掩護影像切割成 1×3 個像素區塊進行運算，選定區塊中間像素為基底像素。其次，基底像素採用採用 LSB 及 OPAP 藏密法嵌入 4 位元的秘密訊息，其餘像素與藏密後的基底像素作差值計算，採用改良混合 LSB/PVD 法進行藏密，以 LSB 藏密法為基礎將像素區分高位元組及低位元組，在低位元採用 2-bit LSB 藏密法及高位元中 6 位元採用新式 PVD 藏密法。二種藏密法結合以提高影像嵌入容量，並保持低失真的影像品質。

實驗以 Lena 等 8 張灰階影像進行測試，實驗結果本研究的平均藏密量為 1,075,071 位元，與混合 LSB/PVD 藏密法相較，藏密量可提升約略 2.3%（約 24,219 位元），本研究因具有較高的藏密量，當嵌入率達 4.1 bpp，影像品質可維持約 30.82 dB，證明本研究藏密法可有效提升藏密量，同時能維持人眼難以察覺的範圍內。

關鍵字：資訊隱藏、最低位元取代法、像素差值藏密法。

*通訊作者：劉興漢 email: liu.hansh@gmail.com

An Improved Steganographic Method Based on Least-Significant-Bit Substitution and Pixel-Value Difference

Liu, Hsing-Han* Ho, Sheng-Chih Lo, Yu-Fen

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

Abstract

This research proposes the least-significant-bit（LSB）substitution combined with the pixel-value differencing（PVD）steganography in the spatial domain, which hides secret information in grayscale images when the observation ability of the human visual system is limited. This research is an improved information hiding method based on the hybrid LSB/PVD method proposed by Jung et al. in 2018, which divides the original cover image into three consecutive non-overlapping blocks and selects the second pixel in each block as a base pixel. Next, the 4-bits secret data are embedded into the base pixels through LSB substitution and the Optimal Pixel Adjustment Process（OPAP）.The difference values between the base pixels and their left and right counterparts will then indicate the quantity of information that can be embedded. The improved hybrid LSB/PVD method is used to embed the secret data, and the pixels are divided into high-byte and low-byte groups based on the LSB method. The 2 bits LSB method is used in the low-byte area and the new PVD method is used in the 6 bits in the high-byte area. The least-significant-bit（LSB）substitution combined with the new pixel-value differencing（PVD）steganography increases the image embedding capacity and maintains a low-distortion image quality.

The experiments are tested with 8 grayscale images such as Lena. The experimental results show that the average embedded capacity is 1,075,071 bits. Compared with the original hybrid LSB/PVD method, it can be increased by about 2.3%（about 24,219 bits）.When the embedded capacity is up to 4.1 bpp, the image quality can be maintained at about 30.82 dB. The experimental results show that the proposed method not only increases the embedded capacity, but also maintains the acceptable of the human eye image quality.

Keywords: Steganography, Least-Significant-Bit Substitution, Pixel-Value Differencing.

---

* Corresponding Author Email: liu.hansh@gmail.com

一、緒論

1.1 前言

隨著電腦及網際網路迅速發展，人們利用資訊傳遞管道與方式亦有極大的轉變，因為只要透過一隻智慧型手機，就能連結上網路可以挖掘到數不清的資料，閱覽來自四面八方的各種資訊，涵蓋新聞、股市、理財、購物、旅遊等各方面的資訊，正所謂「大千世界，盡收眼底」。由於科技的進步，使用者能以最短的時間與成本達到互相通訊，只要透過手機幾個按鈕，即可完成曠日廢時才能完成的傳送郵件工作，為日常生活帶來許多便利，當網際網路成為資訊大量流通時，資安問題也隨之而來，讓大家不得不重視這議題。秘密通訊發展為迎合人性及人類生活的需求孕育而生，密碼系統運作方式是將機密文件經由加密運算處理成密文後，成為無法辨識的亂碼，經加密的資料在網路傳輸中即使遭到攔截亦無法解密，進而達到資訊保密的目的。而藏密學是一種在非機密文件中隱藏秘密資訊以避免被發現的技術，其目的是讓有心人士難以察覺。

密碼學（Cryptography），即希臘語「藏匿」之意，密碼系統運作方式是將機密文件經由加密程序處理後，轉譯成為無法辨識的文字或符號，在網路傳送過程中容易引起中間者的好奇，訊息容易受偵測或監視，使資訊傳輸的安全性備受考驗。我國早在中國周朝的兵書六韜中，便已運用密碼作為軍事通訊的方法與策略，例如陰書與陰符。古羅馬時期，凱薩也將密碼運用於軍事通訊中。第二次世界大戰期間，英格瑪密碼機的破解，成為最後聯軍勝利的關鍵。藏密學（Steganography）一詞源自希臘語「隱藏」、「書寫」之意，為雙方建立一個秘密通訊的掩護下傳遞秘密訊息，其目的是避開第三方的懷疑將秘密訊傳遞出去。早期傳遞訊息的媒介如岩石、竹片、銅片等做掩護，十六世紀義大利科學家喬凡尼、波塔，利用煮熟的蛋傳遞訊息，其原理使用明礬和醋酸混合而成的液體作為墨汁，將秘密訊息寫在蛋殼上，此液體會穿透蛋殼，在蛋白表層留下秘密訊息，利用化學變化的效果來達到隱藏目的。由上述案例發現，資訊隱藏的概念從以前就開始建立，藏密學與密碼學存在的目的皆在保護秘密資訊，於 1999 年 Petitcolas 等學者對資訊隱藏技術分類，見圖 1 所示。

現今的資訊隱藏技術，主要由傳輸方利用數位多媒體掩護藏匿秘密訊息，透過微幅修改多媒體的原始內容，將有意義資訊嵌入無意義的數位多媒體內容資訊中。本研究主要利用一張數位影像作為掩護影像（Cover Image）來藏匿資訊，藉由傳送者使用藏密程序把影像像素改變，將秘密訊息藏入影像，已藏訊息的載體稱偽裝影像（Stego Image）使人類視覺系統（Human Vision System, HVS）觀察的細緻程度有限，不易察覺數位影像中像素值細微變化，讓偽裝影像能發送出去給接收者，而接收者必須知道對方所使用藏密方法才能將訊息提取出。

基本的資訊隱藏流程是發送方先將秘密資料嵌入載體影像後成為藏密影像，然後透過網路方式將藏密影像傳遞給接收方，接收方在接收後再從藏密影像中把秘密資料抽取出來，如圖 2 所示。

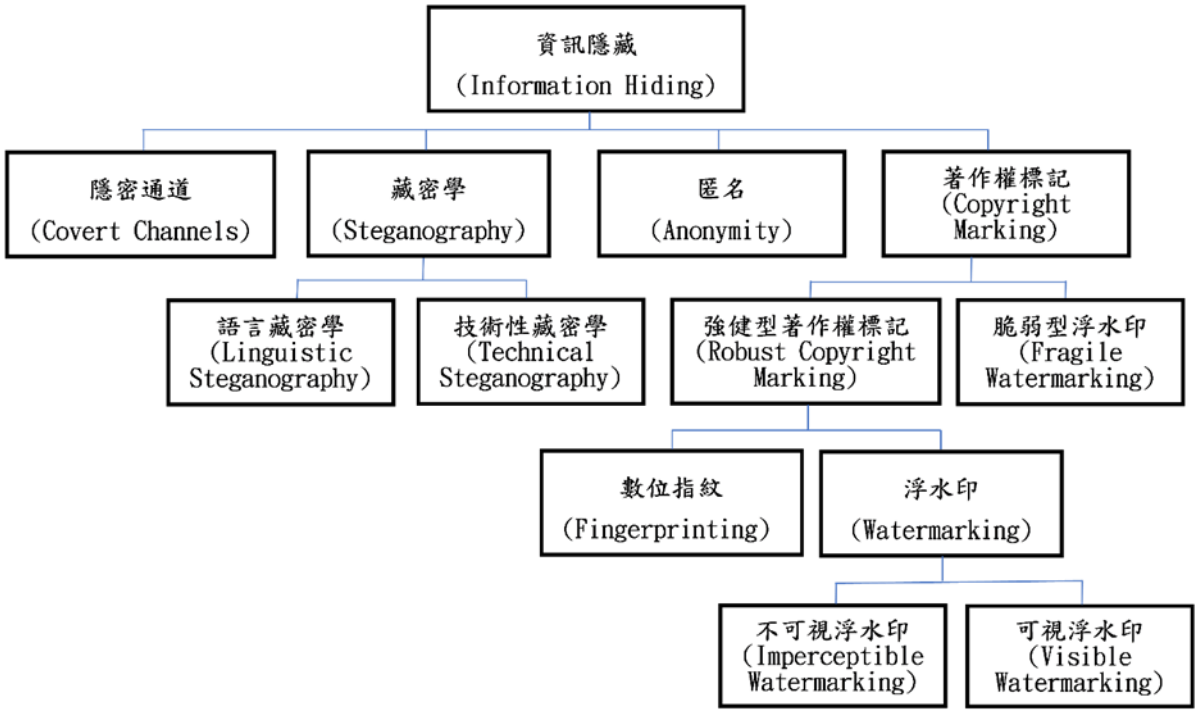


圖 1　資訊隱藏技術分類圖

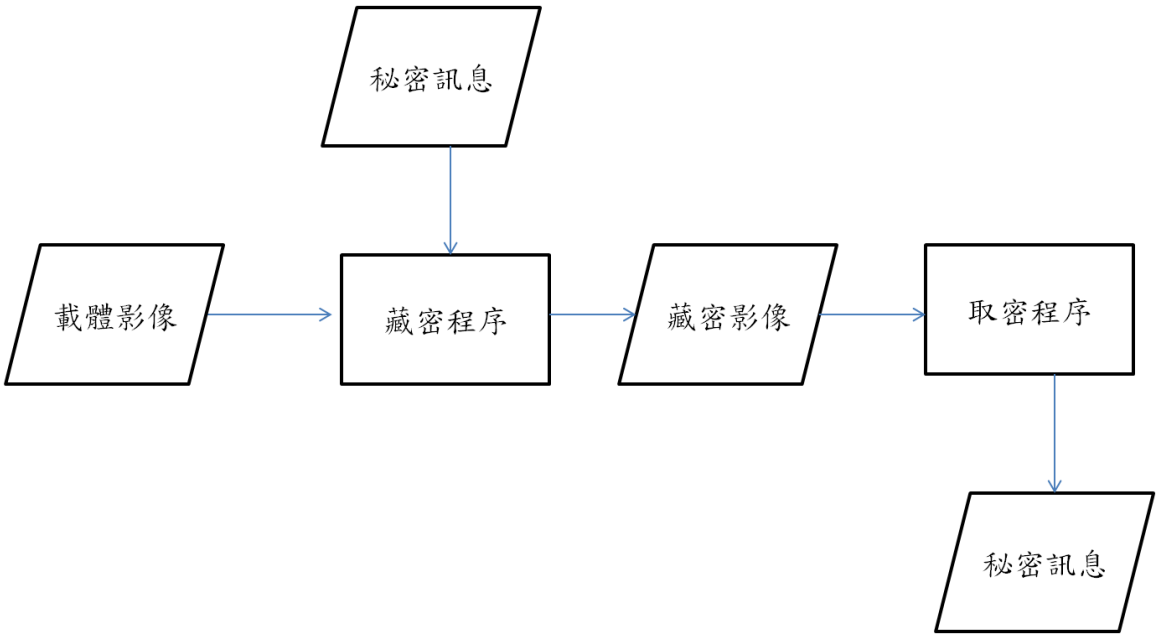


圖 2　資訊隱藏基本流程

目前資訊隱藏技術可區分二種方向，分別為空間域（Spatial Domain）及頻率域（Frequency Domain）技術（Johnson & Jajodia, 1998）。應用在空間域者，主要藉由直接改變影像像素值達到隱藏目的，通常以不破壞原始影像的視覺效果下達成高容量的資訊隱藏，是最常見的隱藏方式，基礎空間域資訊隱藏技術包括最低有效位元取代法（Least-Significant-Bit, LSB）、像素差值藏密法（Pixel-Value Differencing, PVD）。而頻率域的技術則是先將影像由空間域的像素值轉換成頻率域的係數值，再藉由改變頻率域

的係數值嵌入秘密訊息。其中空間域最常用的方法最低位元取代法（LSB），最初由 Bender 等 4 位學者於 1996 年提出使用影像像素最低位元進行訊息藏密，其利用人類視覺對影像輕微調整不易察覺的特性達到隱藏目的，當使用過多的位元數來隱藏機密訊息時，將使偽裝後影像品質降低，甚至會讓偽裝影像造成嚴重的失真，缺點在於藏密量大小受到限制。因此後來學者相繼以 LSB 技術為基礎做改良，提出有效率又不會使影像失真的方法，而 Chan and Cheng 兩位學者於 2004 年提出像素值調整最佳化方法（Optimal Pixel Adjustment Process, OPAP），此方法是以 LSB 藏密法為基礎，在嵌密完後藉由調整其他位元，來比較是否與原影像像素值差距更小，以提升偽裝影像的品質。為了有效增加藏密量，Wu and Tsai 學者於 2003 年提出像素差值藏密法（Pixel Value Differencing, PVD），計算兩像素間的差值，依預先設定固定區間決定嵌入秘密訊息長度，所以藏密量較低，將使偽裝影像產生特定特徵，易遭統計分析的攻擊。後續 Wu 等學者於 2005 年提出基於 PVD 藏密法與 LSB 替代藏密法提出一種高容量藏量法, 透由像素差值門檻值設定，分別採用 LSB 與 PVD 的藏密法。Wang 等學者於 2008 年提出植基於模運算之像素差值藏密法（Modulus PVD, MPVD），利用模數運算修改相鄰像素的餘數來隱藏訊息，並選擇最少失真度的像素值，以降低藏密影像失真，後續由劉江龍等三位學者於 2012 年提出改良 MPVD 藏密法，改善秘密訊息提取不正確問題。Khodaei and Faez 兩位學者於 2012 年提出新式 LSB 和 PVD 藏密法，將掩護影像切割成 3 個連續且不重疊的區塊，針對區塊中間像素嵌入時採用最低位元取代藏密法，最後區塊兩側像素與中間像素分別計算差值，運用改良 PVD 藏密法嵌入秘密訊息。Liu 等學者於 2018 年提出結合邊緣吻合（Side match）和像素差值藏密技術，將掩護影像切割成 3×3 個連續且不重疊的區塊，使用中間像素作為基底，對基底像素的上、左、右、下的像素採用原始 PVD 藏密法，區塊剩餘的四個像素使用 Side match 藏密方法，產生八對像素差值來達到最大藏量，藏密後的影像品質雖然比原始 PVD 方法低，仍在容許影像品質範圍之上。Jung 學者於 2018 年提出混合最低位元取代藏密法和像素差值藏密技術二種藏密法結合以提高影像嵌入容量，並保持低失真視覺影像質量，其缺點藏密後像素值容易產生溢位及藏密前後像素差值在不同區間範圍問題。本研究所提出的方法是結合上述方法優點，改良混合最低位元取代藏密法和像素差值藏密技術及調整像素差值區間表範圍，以提升藏密量情況下，並維持人類視覺可接受的偽裝影像品質。

因應資訊全球化的來臨，國家安全威脅已不再侷限於實體，全球駭客持續入侵網路系統，竊取個資、智慧財產及各類機密資訊，對人權、經濟甚至國家安全都會造成莫大威脅，故資訊隱藏技術的發展仍有其必要。

1.2 研究目的

本研究提出結合空間域資訊隱藏技術中最低位元取代法（LSB）及像素差值（PVD）藏密法，以 Jung 學者於 2018 年提出混合最低位元取代和像素差值藏密法為基礎，改良其藏密後會產生溢位狀況，導致無法正確提取秘密訊息問題。研究過程中運用 Python 程式語言進行程式撰寫，以驗證本研究提出的藏密及取密程序之正確性。本論文主要目的在能維持人類視覺可接受的影像品質下提高藏密量，以提升資訊傳送的利用率。

二、文獻探討

2.1 混合最低位元取代法和像素差值藏密法

Jung 學者於 2018 年提出混合最低位元取代藏密法和像素差值藏密技術，以往都是兩種藏密法單獨或組合使用，而這個藏密方法是以 LSB 藏密法為基礎將像素區分高位元組及低位元組，低位元組採用 2-bit LSB 藏密法和在高位元組中 6 個位元採用 PVD 藏密法，二種藏密法結合以提高圖像嵌入容量，並保持低失真視覺圖像質量。本文後續稱此藏密法為混合 LSB/PVD 藏密法，藏密流程如下：

步驟 1：將掩護影像切割 1×2 個連續不重疊的區塊。

步驟 2：計算像素值商數（高位元）及餘數（低位元），設定低位元最低有效位元取代法之置換量為 2 位元（$k=2$），公式（1）之(P_i^m, P_{i+1}^m)與(p_i^l, p_{i+1}^l)分別代表像素值二進位之高位元與低位元的部分。

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

步驟3：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：設定藏密區間範圍表，如表1所示。

表 1　混合 LSB/PVD 藏密法差值區間範圍表

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：對照藏密區間範圍表，得知可藏密位元數 n，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)計算新舊差值，及下列公式(5)計算嵌密後的像素值$(p_i'^m, p_{i+1}'^m)$。

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

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

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}，最後計算偽裝像素值(P_i', P_{i+1}')。

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

Jung 學者所提方法密文取出程序說明如下：

步驟 1：將偽裝影像切割成兩個連續相鄰且不重疊的區塊，偽裝像素(P_i', P_{i+1}')分別提取 k 位元，並計算新的像素值$(p_i'^m, p_{i+1}'^m)$。

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

步驟 2：計算相鄰兩像素差值，並對照表 3 藏密差值區間範圍表，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，將十進位b_i^m轉換二進位提取密文。

$$d_i'^m = |p_{i+1}'^m - p_i'^m|$$
$$b_i^m = |d_i'^m - l_k| \quad (8)$$

Jung 學者所提方法藏密時會產生溢位問題的範例說明如圖 3 所示，將掩護影像切割成 1× 2個連續且不重疊像素之區塊，假設原始像素區塊的像素值為（0, 255），欲藏入秘密訊息為$(11110\ \ 00\ \ 11)_2$。首先，將 0 與 255 分別轉換成二進位後，分別取出高位元（2 進位之前 6 個位元）與低位元（2 進位之後 2 個位元）。將高位元轉換成十進位後，分別得到 0 與 63，依公式（2）計算其差值d_i^m為 63，對照步驟 5 之藏密區間範圍表，計算出可藏入之密文數量為 5，故將前 5 個密文 11110 轉成 10 進位後的值b_i^m為 30。並依公式（3）計算其新差值為 62，續依公式（4）計算出 m 值為 1。再依公式（5）計算出 PVD 藏密後高位元像素值為（-1, 63）。最後分別將高位元像素與低位元像素相結合後，可得藏密後的像素值（-4, 255），此時-4 已小於灰階影像最低像素值 0，故產生溢位問題。

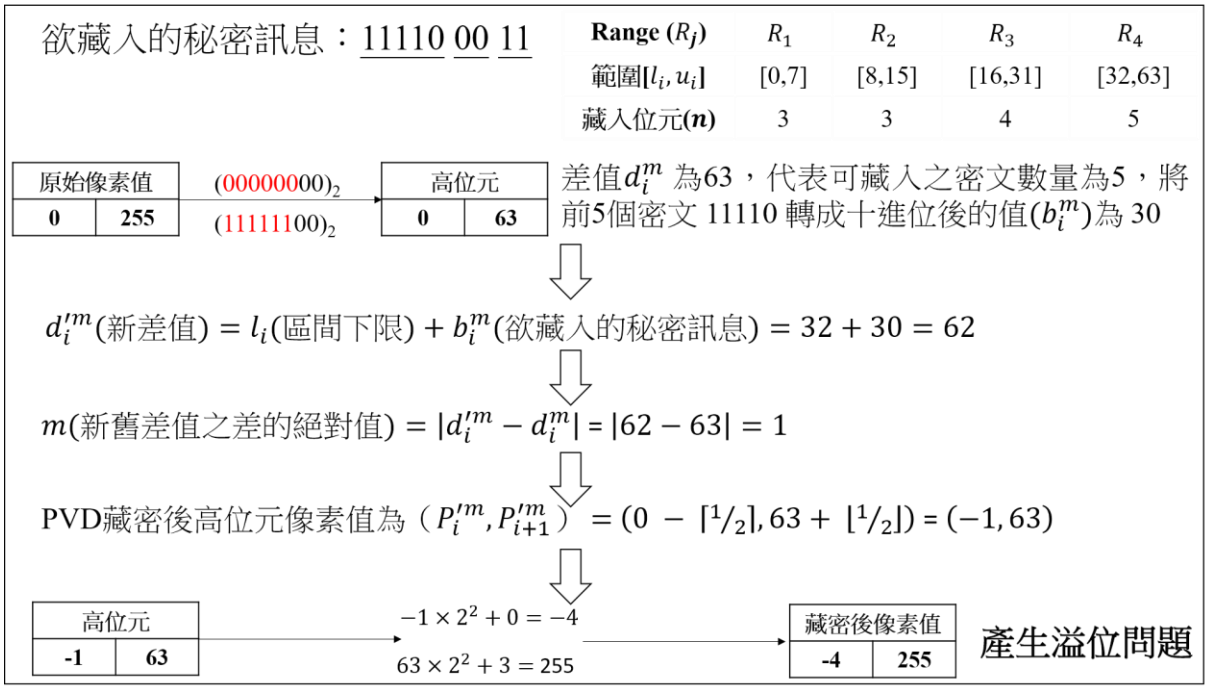


圖 3　Jung 學者所提方法藏密時會產生溢位問題的範例說明

2.2 藏密技術衡量標準

在藏密過程中，影像品質與藏密量通常是一個難以取捨問題，當藏密量愈高時，其藏密後影像品質失真就愈大，而藏密影像技術中失真性評估最常利用峰值信號雜訊比（Peak Signal-to-Noise Ratio, PSNR）來做衡量，其單位為分貝（Decibels, dB），如公式（9）所定義，為 Zhou 和 Bovik 學者於 2002 年提出的一個計算影像的失真量化數據的方法。在計算 PSNR 前，必需先計算出掩護影像與偽裝影像像素間的均方差（Mean Square Error, MSE），計算平均每個像素變動的幅度，公式中均方差值分子計算影像藏密前後的誤差程度，均方差值愈大表示誤差程度大，愈小表示誤差程度小。

$$MSE = \sum_{i=1}^{W \times H} \frac{(x'_{ij} - x_{ij})^2}{W \times H}$$

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right) \quad (9)$$

一般灰階影像像素值以 8 位元表示，其值介於 0 到 255 之間，在 MSE 公式中，W、H表示掩護影像長與寬，而 x'_{ij}、x_{ij}分別代表於 i、j位置的偽裝像素與原始像素的值，當 PSNR 值越大，就代表掩護影像跟偽裝影像的差異度越小，一般而言，PSNR 值小於 30 dB 時，表示人類視覺看起來不能容忍的範圍，因此大部份 PSNR 值皆要大於 30 dB（王旭正等，2016）。

由於 PSNR 未考慮到人眼視覺的特性，而人眼對空間頻率較低的敏感度較高、對亮度比對色度差異更敏感、對一個區域的感知會受其周圍鄰近區域所影響等因素，因此常出現 PSNR 評價結果與人的主觀感受不同的情況。因此，另一種符合人類直覺的影像品質評量標準，稱結構相似性（Structural Similarity, SSIM），由 Zhou Wang 等人在 2004 年發表的論文中提出，主要測量掩護影像和偽裝影像之間結構相似大小，其值藉於 0 到 1 之間，值愈大表示兩張影像的相似度越高，分別從公式（10）計算影像亮度、公式（11）計算對比度、公式（12）計算影像相似性，而結構相似性（SSIM）計算如公式（13）所示。

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (10)$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (11)$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (12)$$

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (13)$$

三、研究方法

本研究將探討在偽裝影像品質可接受的情況下，儘可能提高秘密訊息的藏密量。在文獻收集的過程中，發現混合 LSB/PVD 藏密技術有改進的空間，本研究以混合 LSB/PVD 藏密法為基礎而提出改良的資訊隱藏方法。本節首先探討研究設計架構，其次為藏密與取密程序介紹，並針對藏密方法實施範例說明。

3.1 研究設計

在 2018 年 Jung 學者所提出的混合 LSB/PVD 藏密技術中，以 LSB 藏密法的概念，將像素值區分為高位元及低位元，在高位元組以相鄰像素間的差值來決定藏密量，而低位元組利用人類視覺對低像素修改不易察覺的特性來隱藏訊息，而得到較高的藏密量，但此藏密演算法在藏密後容易造成像素值溢位問題，導致在提取秘密訊息時，無法正確完整復原秘密訊息。

本研究設計將掩護影像切割成 1×3 個連續且不重疊的區塊，採用 LSB 及 OPAP 藏密法對中間像素嵌入 4 位元的秘密訊息，中間像素藏密後就不再變動，分別計算藏密後中間像素與區塊兩側相鄰像素的差值，本研究將採用混合 LSB/PVD 藏密法，針對其演算法進行改良，其技術是以 LSB 藏密法為基礎，將像素值區分高位元組及低位元組，有別於該技術高位元組 6 個位元結合原始 PVD 藏密法，本研究高位元像素組改採用改良新式 PVD 藏密法（Khodaei & Faez, 2012），實驗中試著改良新式 PVD 藏密法運算式，讓每個機密資訊位元都能從偽裝影像中正確完整的取出，使得秘密訊息能夠完整的復原，並試著調整像素差值區間數量及嵌入秘密訊息的位元數，以提升藏密量為目的，同時能維持可接受的偽裝影像品質。

3.2 藏密及取密程序

藏密相關詳細的流程為以下步驟：

步驟 1：將掩護影像（Cover Image）進行劃分，形成分別含有 1×3 個連續且不重疊的像素區塊。

步驟 2：區塊的中間像素P_{ic}表示為第 i 個區塊之基底像素（圖 4），基底像素使用 4-bit LSB 藏密法，基底像素P_{ic} 採用 4-bit LSB 轉換成十進位的值稱為LSB_i，預藏入的 4 位元密文轉換十進位稱為s_i，計算LSB_i與s_i差值如公式（14）所示。

$$d_{ic} = LSB_i - s_i \tag{14}$$

P_{i1}	P_{ic}	P_{i2}

圖 4　基底像素選定示意圖

步驟 3：基底像素P_{ic}採用 4 位元 LSB 嵌密後的像素值P'_{ic}。

$$P'_{ic} = P_{ic} - (P_{ic} \mod 2^4) + s_i \tag{15}$$

步驟 4：使用最佳化像素調整程序調整基底像素P'_{ic}。

$$P'_{ic}=\begin{cases}P'_{ic}+2^4,\ if\ \ d_{ic}>2^3 and\ \ 0\le P'_{ic}+2^4\le 255\\ P'_{ic}-2^4,\ if\ \ d_{ic}<-2^3 and\ \ 0\le P'_{ic}-2^4\le 255\\ P'_{ic}\ ,\ otherwise\end{cases} \quad (16)$$

步驟 5：分別計算像素P_{i1}、P'_{ic}、P_{i2}的商數（高位元）和餘數（低位元），設定低位元最低有效位元取代法之置換量為 2 位元（$k=2$）。

$$Q'_{ic}=P'_{ic}\ \ div\ \ 2^k, and\ \ Q_{iv}=P_{iv}\ \ div\ \ 2^k\ ,\ v=1,2$$
$$R'_{ic}=P'_{ic}\ \ mod\ \ 2^k, and\ \ R_{iv}=P_{iv}\ \ mod\ \ 2^k\ ,\ v=1,2 \quad (17)$$

步驟 6：分別計算Q'_{ic}與Q_{i1}與Q_{i2}差值。

$$d_{iv}=|Q'_{ic}-Q_{iv}| \qquad v=1,2 \quad (18)$$

步驟 7：定義藏密區間範圍表，見表 2 所示。

表 2　本研究區間範圍表

Range（R_j）	R_1	R_2	R_3	R_4
區間範圍$[l_i,u_i]$	[0,3]	[4,11]	[12,19]	[20,63]
可藏位元數（n）	2	3	3	4

步驟 8：依差值d_{i1}、d_{i2}對照表 2，判斷差值的範圍區間R_j，即可得知區間的最低範圍l_i及嵌入秘密訊息的位元數 n，從二進位秘密訊息取 n 位元，並轉換十進位為b_{iv}，計算新差值d'^m_{iv}。

$$d'^m_{iv}=l_i+b_{iv}, v=1,2 \quad (19)$$

步驟 9：計算像素Q_{iv}嵌密後可能之值Q''_{iv}及Q'''_{iv}。

$$Q''_{iv}=Q'_{ic}-d'^m_{iv}\ \text{ and }\ Q'''_{iv}=Q'_{ic}+d'^m_{iv}, v=1,2 \quad (20)$$

步驟 10：以下列公式重新調整藏密後的值。

$$Q'_{iv}=\begin{cases}Q''_{iv}\ ,\ if(Q'''_{iv}>63)\ \ or\ \ |Q_{iv}-Q''_{iv}|<|Q_{iv}-Q'''_{iv}|\\ \qquad and\ \ 0\le Q''_{iv}\le 63\ \ and\ \ 0\le Q'''_{iv}\le 63\\ Q'''_{iv}\ ,\ if\ \ (Q''_{iv}<0)\ \ or\ \ \ |Q_{iv}-Q'''_{iv}|<|Q_{iv}-Q''_{iv}|\\ \qquad and\ \ 0\le Q''_{iv}\le 63\ \ and\ \ 0\le Q'''_{iv}\le 63\end{cases}, v=1,2 \quad (21)$$

步驟 11：從二進位秘密訊息取 k 位元像素值，分別嵌入像素值P_{i1}、P_{i2}之k位元 LSB，並轉換成十進位R'_{i1}及R'_{i2}，最後計算偽裝像素值P'_{i1}與P'_{i2}。

$$P'_{iv}=Q'_{iv}\times 2^k+R'_{iv}\ , v=1,2 \quad (22)$$

取密方法較藏密流程簡易，詳細說明如以下步驟：

步驟 1：將偽裝影像（Stego Image）切割成1×3像素為單位之區塊。

步驟 2：首先將P'_{ic}轉二進位提取最低 4 個位元及P'_{i1}、P'_{i2}轉二進位提取最低 2 位元，並依下列公式分別計算Q'_{ic}及Q'_{i1}、Q'_{i2}。

$$Q'_{iv}=P'_{iv}\ \ div\ \ 2^k\ \ ,\ v=1,\ 2$$
$$Q'_{ic}=P'_{ic}\ \ div\ \ 2^k \quad (23)$$

步驟 3：計算Q'_{i1}、Q'_{ic}差值d'_{i1}與Q'_{i2}、Q'_{ic}差值d'_{i2}。

$$d'_{iv} = |Q'_{ic} - Q'_{iv}|, v=1, 2 \quad (24)$$

步驟 4：對照差值區間表 2，得知d'_{iv}是屬於區間R_j，此區間像素最低範圍l_{iv}，藏密量為 n 位元，依下列公式計算秘密訊息b_{iv}，將十進位b_{iv}轉換二進位提取秘密訊息。

$$b_{iv} = |d'_{iv} - l_{iv}|, v=1, 2 \quad (25)$$

3.3 藏密及取密過程範例說明

本研究藏密過程範例說明見圖 5 所示，將掩護影像切割成 1×3 個連續且不重疊像素之區塊，假設一像素區塊的像素值（P_{i1}, P_{ic}, P_{i2}）=（132,122,80），預藏入秘密訊息$s = (0101\ 010\ 100\ 01\ 11)_2$，若定義$k = 2$，首先進行依據公式（14）計算$LSB_i$與$s_{ic}$之間差值$d_i$，$LSB_i = (1010)_2$=10，取 4 位元密文$s_{ic} = (0101)_2 = 5$，$d_i = 10 - 5 = 5$，將基底像素轉二進位$P_{ic} = 122 = (01111010)_2$，基底像素使用 4-bit LSB 嵌密，並依公式（15）計算最低位元取代法置換$P'_{ic} = 122 - (122\ mod\ 2^4) + 5 = 117$，並依公式（16）調整基底像素後，$P'_{ic}$仍為 117。依據公式（17）計算區塊像素值的商數分別為$Q_{i1} = 33$、$Q'_{ic} = 29$、$Q_{i2} = 20$，餘數分別為$R_{i1} = 0$、R'_{ic} =1、$R_{i2} = 0$，分別計算Q_{ic}與Q_{i1}、Q_{i2}差值$d_{i1} = |29 - 33| = 4$與$d_{i2} = |29 - 20| = 9$，依其值對照區間範圍表 2 判定d_{i1}及d_{i2}屬於區間 2，且得知嵌入秘密訊息位元數分別為$n_{i1} = 3$位元、$n_{i2} = 3$位元，依照所決定的位元數，將預藏入之二進位秘密訊息轉換十進位值，獲得$b^m_{i1} = (010)_2 = 2$與$b^m_{i2} = (100)_2 = 4$，再依據公式（19）計算新差值$d'^m_{i1} = l_{i1} + b^m_{i1} = 4 + 2 = 6$、$d'^m_{i2} = 4 + 4 = 8$，計算像素$Q_i$嵌密後可能的值$Q''_{i1} = Q'_{ic} - d'^m_{i1} = 29 - 6 = 23$與$Q'''_{i1} = Q'_{ic} + d'^m_{i1} = 29 + 6 = 35$，並計算$Q''_{i2} = 29 - 8 = 21$、$Q'''_{i2} = 29 + 8 = 37$，依據公式（21）重新調整藏密後的值獲得$Q'_{i1} = 35$、$Q'_{i2} = 21$，接續，像素低位元嵌入 2 位元，並轉換成十進位$R'_{i1}$=（01）$_2$=1、$R'_{i2}$=（11）$_2$=3，最後依據公式（22）計算偽裝像素值$P'_{i1} = Q'_{i1} \times 2^2 + R'_{i1} = 35 \times 4 + 1 = 141$、$P'_{i2} = 21 \times 4 + 3 = 87$，最終的偽裝像素為（$P'_{i1}, P'_{ic}, P'_{i2}$）=（141, 117, 87）。

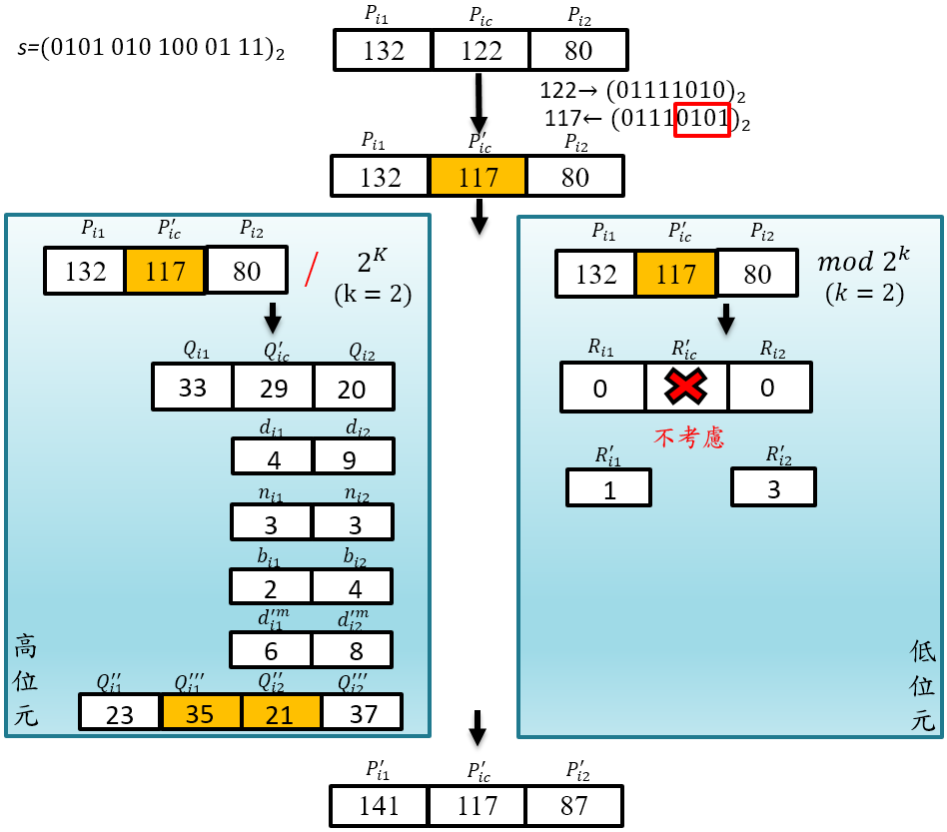


圖 5　本研究藏密過程示意圖

本研究取密過程範例說明見圖 6 所示，假設藏密像素區塊為（$P'_{i1}, P'_{ic}, P'_{i2}$）=（141, 117, 87），首先將基底像素$P'_{ic}$轉二進位 117=（01110101）$_2$，提取基底像素$P'_{ic}$最低 4 位元，其值為 0101。依公式(23)計算藏密像素值商數分別為$Q'_{i1} = 141 \ div \ 4 = 35$、$Q'_{ic} = 117 \ div \ 4 = 29$、$Q'_{i2} = 87 \ div \ 4 = 21$，並計算$Q'_{ic}$與$Q'_{i1}$、$Q'_{i2}$差值 d'_{i1}=$|29 - 35| = 6$，對照差值區間表 2 得知$d'_{i1} \in R_2$，藏密量為 3 位元，此區間最低範圍$l_{i1} = 4$，另$d'_{i2} = |29 - 21| = 8$ 得知 $d'_{i2} \in R_2$，藏密量為 3 位元，此區間最低範圍$l_{i2} = 4$，依公式（25）計算$b'_{iv} = |d'_{iv} - l_{iv}|$, v=1, 2，$b'_{i1} = 6 - 4 = 2$，將b'_{i1}轉二進位其值為（010）$_2$，另$b'_{i2} = 8 - 4 = 4$，將b'_{i2}轉二進位其值為（100）$_2$，再將P'_{i1}、P'_{i2}像素值轉二進位並提取最低 2 位元，獲得（01）$_2$ 及（11）$_2$，最後，依序結合所提取的訊息，即獲得完整秘密訊息 s =（0101 010 100 01 11）$_2$。

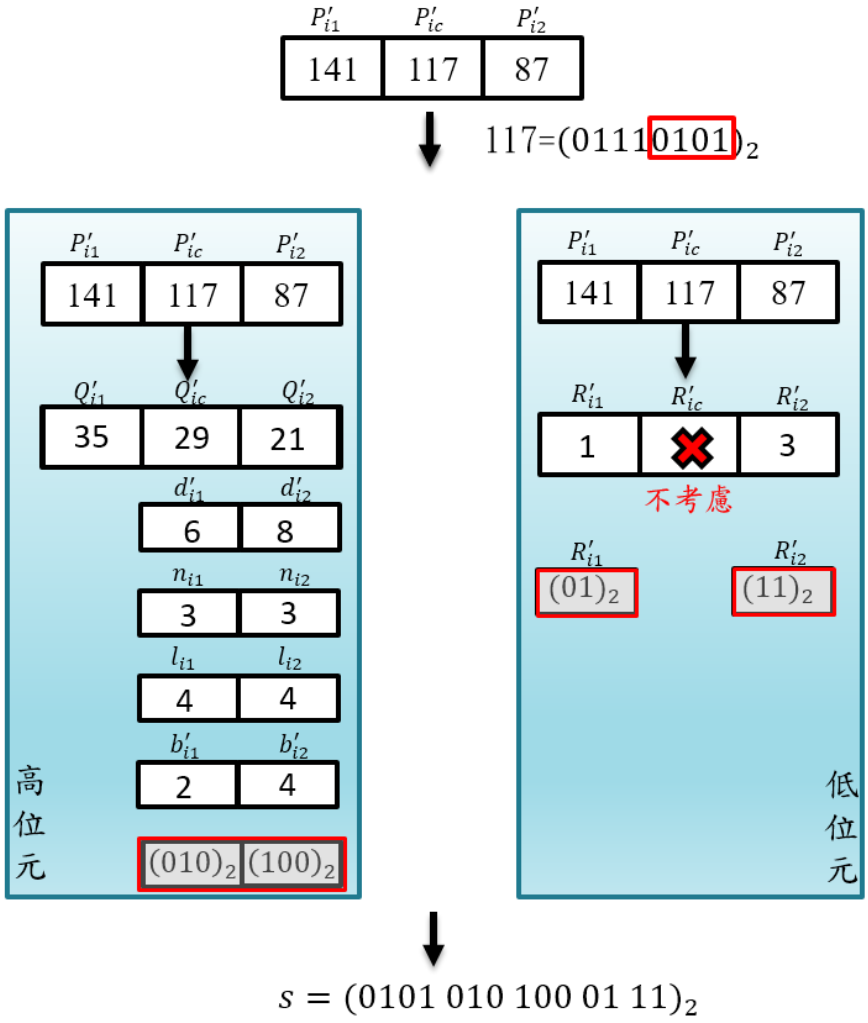


圖 6　本研究取密過程示意圖

因本研究旨在改善 Jung 學者所提藏密法於藏密後會產生溢位狀況，導致無法正確提取秘密訊息問題。而本研究之所以能解決溢位問題，主要在於藉由公式（21）重新調整藏密後的高位元像素值，使其值不會超過 63 或小於 0，故與低位元像素值結合後，不會產生溢位問題，本研究經實作表 3 所列程式後，所得各實驗影像溢位數量如下，證明本研究可改善溢位狀況。

表 3　溢位狀況統計表

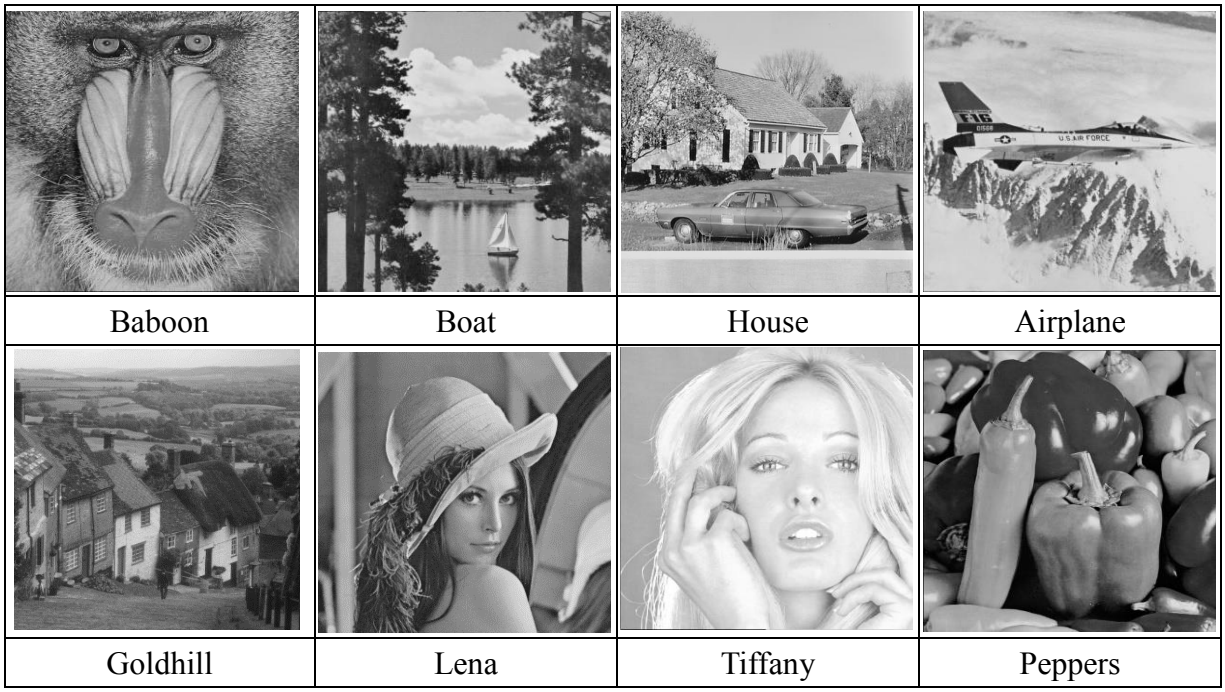
方法 / 影像	原始 PVD 2003	新式 LSB/PVD 2012	新式Side Match/PVD 2018	混合 LSB/PVD 2018	新式LSB/ MPVD 2020	本研究
Lena	0	7	0	0	0	0
Airport	11	0	0	0	0	0
Boat	37	4	0	41	0	0
Goldhill	1	0	0	0	0	0
Baboon	28	0	0	75	0	0
Tiffany	1110	1138	0	2534	0	0
House	45	12	0	5	0	0
Peppers	383	0	0	4113	0	0
Average	**201.87**	**145.12**	**0**	**529.5**	**0**	**0**

四、實驗結果

本節將對本研究所提出之改良混合最低位元取代法與像素差值之資訊隱藏技術與其他學者所提藏密法進行藏密量與偽裝影像品質比較，藉由實驗數據驗證本方法可行性。而為驗證本方法是否可抵抗藏密分析方法之偵測，以像素差值直方圖及內容選擇殘差分析技術進行偽裝影像偵測。

4.1 實驗環境

實驗影像以資訊隱藏經常使用的 Baboon、Boat、House、Airplane、Goldhill、Lena、Taffany、Peppers 等 8 張大小 512x512 的標準灰階影像進行測試（見圖 4），測試影像中包含平滑及粗糙紋理之影像。嵌入的秘密訊息以隨機亂數 0 或 1 的字串組成，實驗結果以藏密量、峰值信噪比（PSNR）及結構相似性（SSIM）作為衡量標準。



Baboon	Boat	House	Airplane
Goldhill	Lena	Tiffany	Peppers

圖 7　本研究使用之測試影像

4.2 實驗結果分析

本研究所提出之方法，分別與原始 PVD 藏密法（Wu & Tsai, 2003）、新式 LSB/PVD 藏密法（Khodaei & Faez, 2012）、新式 Side Match/PVD 藏密法（Liu et al., 2018）、混合 LSB/PVD 藏密法（Jung, 2018）、新式 LSB/MPVD 藏密法（Liu et al., 2020）進行比較，其藏密量比較結果見表 4、PSNR 與 SSIM 比較結果見表 5 所示。在表 4 針對各方法藏密量與嵌入率（bit per pixel, bpp）（括弧內的值）進行比較，可發現原始 PVD 藏密法，在藏密上因以單一藏密法為主，故藏密量與嵌入率相較低。而新式 LSB/PVD 藏密法、Side Match/PVD 藏密法與混合 LSB/PVD 藏密法和新式 LSB/MPVD 藏密法因結合了 2 種藏密方法，故相較原始 PVD 方法，具有較高的藏密量與嵌入率。而本研究提出的方法與混合 LSB/PVD 藏密法最大的不同，在於針對高位元採用改良新式 PVD 藏密法

及調整像素差值區間表，此步驟可有利於提高藏密量與嵌入率及維持可接受的影像品質。

表 4　各方法藏密量與嵌入率比較表（單位:bit）

方法 / 影像	原始 PVD 2003	新式 LSB/PVD 2012	新式Side Match/PVD 2018	混合 LSB/PVD 2018	新式LSB/ MPVD 2020	本研究
Lena	409,807 （1.56）	809,966 （3.09）	712,112 （2.72）	1,049,742 （4.00）	962,452 （3.67）	1,067,749 （4.07）
Airport	409,834 （1.56）	809,262 （3.09）	717,511 （2.74）	1,050,973 （4.01）	963,471 （3.68）	1,062,797 （4.05）
Boat	420,638 （1.60）	820,391 （3.13）	735,413 （2.81）	1,051,124 （4.01）	965,764 （3.68）	1,080,448 （4.12）
Goldhill	411,896 （1.57）	813,968 （3.11）	720,574 （2.75）	1,049,093 （4.00）	962,633 （3.67）	1,072,427 （4.09）
Baboon	457,105 （1.74）	886,516 （3.38）	808,760 （3.09）	1,054,327 （4.02）	977,179 （3.73）	1,113,184 （4.25）
Tiffany	407,365 （1.55）	806,847 （3.08）	709,764 （2.71）	1,049,513 （4.00）	961,484 （3.67）	1,062,916 （4.05）
House	420,123 （1.60）	818,580 （3.12）	729,785 （2.78）	1,051,474 （4.01）	965,871 （3.68）	1,074,960 （4.10）
Peppers	407,643 （1.56）	802,228 （3.06）	713,062 （2.72）	1,050,571 （4.01）	961,563 （3.67）	1,066,084 （4.07）
Average	**418,051** （**1.59**）	**820,970** （**3.13**）	**730,873** （**2.79**）	**1,050,852** （**4.01**）	**965,052** （**3.68**）	**1,075,071** （**4.10**）

表 5 針對衡量偽裝影像品質之 PSNR 及 SSIM 值（括弧內的值）進行比較，可察覺原始 PVD 藏密法、新式 LSB/PVD 藏密法、新式 Side Match/PVD 藏密法因藏密量較低，故偽裝影像品質較佳，而本研究藏密法的 PSNR 值平均約為 30.82 dB，與混合 LSB/PVD 藏密法相比，在藏密量提升 2.3%（約 24,219 位元），而偽裝影像品質 PSNR 值僅下降 6%（約 1.96 dB），SSIM 值下降約 0.013，實驗結果顯示本研究藏密法可提升藏密量，並維持可接受的影像品質（平均約 30.82 dB）。

為了驗證本研究所提出的藏密技術可應用於不同類型的廣泛性影像，針對 BossBase 影像資料庫（BOSSBases v0.93）10,000 張影像大小為 512×512 灰階影像進行藏密量及影像品質的計算，實驗結果見表 6 所示，本研究藏密技術藏密量平均約為 1,063,855 位元，PSNR 值平均約為 31.11dB，與混合 LSB/PVD 藏密法相比，藏密量提升 1.3%（約 14,210 位元），而影像品質 PSNR 值下降 4.2%（約 1.365 dB），SSIM 值下降約 0.013，實驗結果證實本研究方法與其他藏密技術進行數據比較，可具備較高藏密量，且維持可接受的影像品質。

表 5　各方法 PSNR 與 SSIM 比較表

方法 / 影像	原始 PVD 2003	新式 LSB/PVD 2012	新式Side Match/PVD 2018	混合 LSB/PVD 2018	新式LSB/ MPVD 2020	本研究
Lena	41.18 (0.978)	37.63 (0.936)	36.70 (0.929)	33.21 (0.805)	35.35 (0.896)	31.47 (0.801)
Airport	40.20 (0.973)	37.53 (0.931)	36.19 (0.923)	33.19 (0.787)	35.33 (0.882)	31.8 (0.797)
Boat	39.71 (0.981)	36.53 (0.941)	34.97 (0.941)	32.84 (0.846)	34.91 (0.918)	30.65 (0.829)
Goldhill	41.00 (0.983)	37.55 (0.944)	36.23 (0.944)	32.54 (0.859)	35.31 (0.920)	31.16 (0.843)
Baboon	36.96 (0.987)	36.29 (0.934)	32.04 (0.934)	31.74 (0.927)	33.93 (0.956)	29.67 (0.901)
Tiffany	40.89 (0.974)	37.79 (0.922)	36.84 (0.922)	32.47 (0.780)	34.76 (0.876)	30.37 (0.758)
House	39.15 (0.977)	36.44 (0.937)	35.47 (0.937)	32.73 (0.838)	34.96 (0.908)	30.96 (0.834)
Peppers	40.61 (0.978)	37.97 (0.927)	34.83 (0.927)	33.55 (0.806)	34.89 (0.900)	30.49 (0.785)
Average	**39.96 (0.978)**	**37.21 (0.932)**	**35.40 (0.932)**	**32.78 (0.831)**	**34.93 (0.907)**	**30.82 (0.818)**

表 6　BossBase 影像資料庫影像運算平均值

方法 / 影像	原始PVD 2003	新式 LSB/PVD 2012	新式Side Match/PVD 2018	混合 LSB/PVD 2018	新式 LSB/MPVD 2020	本研究
藏密量	409,780	805,717	719,708	1,049,645	962,718	1,063,855
PSNR	40.858	35.146	35.502	32.475	34.906	31.11
SSIM	0.969	0.919	0.909	0.783	0.878	0.77

4.3 安全性分析

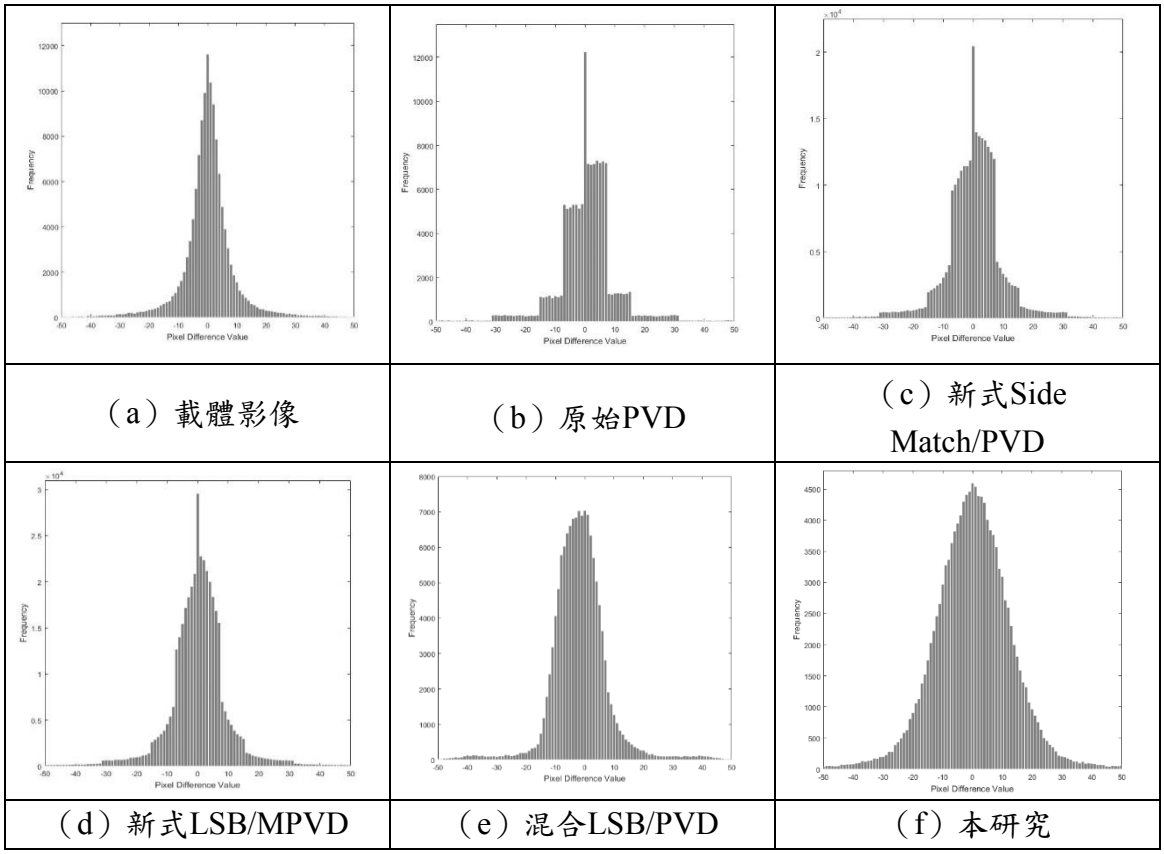
資訊隱藏技術的原則是指在網路上傳遞訊息時不被其他人察覺，而不可察覺除了要避免被人類視覺發現影像失真情形，也要避免被藏密分析技術偵測出異常狀況。本節將探討本研究所提出藏密技術是否可有效抵抗藏密分析方法偵測，採用空間域常見的像素差值直方圖（Pixel Difference Histogram, PDH）及內容選擇殘差（Content-Selective Residuals, CSR）兩種藏密的分析技術進行偽裝影像偵測。

4.3.1像素差值直方圖分析

一般灰階影像像素以 8 位元表示，其值介於 0 到 255 的範圍，表示灰色深淺。像素差值直方圖用來統計偽裝影像相鄰像素差值出現的次數，一般載體影像相鄰像素會呈現

常態分佈見圖 8（a）所示，直方圖橫軸為像素差值，縱軸為像素差值的統計量，影像經藏密演算法計算後會改變像素間彼此的相關性，像素差值直方圖會呈現不正常的分佈見圖 8（b）（c）（d）所示，若直方圖呈現不正常階梯狀的分佈狀態，此顯著分佈的差異變化容易成為藏密偵測特徵，可偵測出影像內是否隱藏秘密訊息。

本研究針對原始 PVD 藏密法、新式 Side Match/PVD 藏密法、混合 LSB/PVD 藏密法、新式 LSB/MPVD 及本研究所提出藏密方法分別進行藏密運算後所產生的像素差值直方圖進行安全性分析。（以 Lena 圖為例，掩護影像的像素直方圖見圖 8（a）所示，各方法藏密後所產生像素差值直方圖見圖 8（b）（c）（d）（e）（f）所示）。在圖 8（b）（c）（d）所示，原始 PVD 藏密法、新式 Side Match/PVD 藏密法與新式 LSB/MPVD 藏密法經藏密演算法運算後所產生像素差值直方圖明顯呈現不正常的階梯狀分佈，這類特徵容易遭藏密分析方法偵測。而圖 8（e）（f）所示，混合 LSB/PVD 藏密法與本研究所提藏密方法所產生的像素差值直方圖呈現常態分佈趨勢，較能有效抵禦像素差值直方圖藏密分析偵測。



（a）載體影像　（b）原始PVD　（c）新式Side Match/PVD

（d）新式LSB/MPVD　（e）混合LSB/PVD　（f）本研究

圖 8　各藏密方法之像素差值直方圖

4.3.2內容選擇殘差分析

內容選擇殘差（Content-Selective Residuals, CSR）影像藏密分析技術，是由 Denemark 等學者於 2014 年提出，針對測試影像擷取 1183 個藏密特徵，使用統計分析技術來判斷是否隱藏秘密訊息。本研究採用 BossBase 影像資料庫挑選 10,000 張影像大小為 512×512

灰階影像及經本研究藏密法藏密後影像進行偵測分析，最後藏密分析效能以類別預測最常用的評估指標準確率（Accuracy）計算，見公式（26）所示，準確率愈低表示藏密的安全性較高。其中正確分類區分二項分別為 TP（True Positive, TP）為實際偽裝影像預測為偽裝影像、TN（True Negative, TN）為實際掩護影像預測為掩護影像，錯誤分類區分二項分別為 FP（False Positive, FP）為實際為掩護影像預測為偽裝影像、FN（False Negative, FN）為實際為偽裝影像預測為掩護影像。

$$Accuracy = \frac{TN+TP}{TN+TP+FN+FP} \times 100\% \quad (26)$$

本研究針對新式 Side Match/PVD 藏密法、混合 LSB/PVD 藏密法、新式 LSB/MPVD 及本研究所提出藏密方法分別採用 CSR 影像藏密分析方法進行藏密偵測，實驗結果見表 7 所示，本研究所提出的藏密方法，所獲得的偵測正確率為 56.22%，雖然較新式 LSB/PVD、新式 Side Match/PVD 藏密法與混合 LSB/PVD 分別高出 2%、3.12%及 0.13%，但仍高於隨機判斷之機率 50%，根據實驗結果，本研究藏密方法可有效抵抗 CSR 影像藏密偵測，當藏密量愈高的藏密方法，在藏密後所產生的特徵值較高容易遭分析方法偵測。

因本研究所提藏密技術為藏密學（Steganography）之應用，而非屬於浮水印（Watermarking）的範疇，這二類技術應用範圍不同，所需抵抗之相關攻擊亦不同。故本研究乃針對相關藏密分析技術進行實驗與討論，而不針對浮水印技術所會遭受的攻擊（如胡椒鹽雜訊、高斯白雜訊、旋轉等）進行說明。

表 7　CSR 影像偵測結果

分類 / 方法	TP	TN	FP	FN	Accuracy（%）
新式 LSB/PVD	4999.1	423.2	4576.8	0.9	54.22%
新式 Side Match/PVD	5000	310.4	4689.6	0	53.10%
混合LSB/PVD	4996.8	611.8	4388.2	3.2	56.09%
新式 LSB/MPVD	5000	659.2	4340.8	0	56.6%
本研究	4999	623.3	4376.6	1	56.22%

五、結論與未來研究方向

5.1 結論

本研究中提出了高容量資訊隱藏技術，改良 Jung 學者的混合像素差值藏密法及最低位元取代藏密法，然而要提出一種高隱藏的容量的方法，相對的會降低不可察覺性及安全性，因此，經過反覆實驗後，決定將掩護影像分割成1×3不重疊的區塊大小，選定

區塊中間像素為基底像素，基底像素採用採用 LSB 及 OPAP 藏密法嵌入 4 位元的秘密訊息，其餘像素與藏密後的基底像素作差值計算，採用改良混合 LSB/PVD 法進行藏密，以達到提升藏密量為目的，同時維持可接受的影像品質。實驗影像以 Lena 等 8 張灰階影像進行測試，實驗結果顯示本研究的平均藏密量為 1,075,071 位元，與混合 LSB/PVD 藏密法相較，藏密量可提升約略 2.3%（約 24,219 位元），而偽裝影像品質 PSNR 值僅下降 6%（約 1.96 dB），SSIM 值下降約 0.013。

為驗證本研究所提出的藏密技術可應用於不同類型的廣泛性影像，針對 BossBase 影像資料庫 10,000 張影像大小為 512×512 灰階影像進行藏密量及影像品質的計算，藏密量平均約為 1,063,855 位元，PSNR 值平均約為 31.11 dB，與混合 LSB/PVD 藏密法相比，藏密量提升 1.3%（約 14,210 位元），而影像品質 PSNR 值下降 4.2%（約 1.365 dB），SSIM 值下降約 0.013，證明本研究藏密法可有效提升藏密量，同時能維持人眼難以察覺的範圍內。本研究安全性分析採用空間域常見的像素差值直方圖（PDH）及內容選擇殘差（CSR）兩種分析技術進行偵測，其分析結果證明本研究所提藏密技術之安全性。

5.2 未來研究方向

未來可以本研究為基礎探討與其他藏密技術的整合，若能依每種不同類型影像特性，如影像亮度、對比度等因素，若可動態調整每個像素適合嵌入的秘密訊息藏密量，可提升藏密的安全強度，是未來研究值得探討的方向。

5.3 國防領域之應用

近年來網路駭客攻擊及犯罪事件頻傳不斷，有心人士若運用資訊隱藏技術將不法資訊嵌入至灰階或彩色影像、視訊影片及音訊檔案內，提供恐怖份子執行非法的行為之依據，將可能對個人或國家安全造成損害的疑慮。所以身為國防資訊安全研究人員，必須熟悉相關資訊隱藏與資訊隱藏分析技術之方向。因此，本研究可提供國防資訊安全管理技術研究領域人員實務應用參考。

參考文獻

王旭正、翁麒耀、黃正達，2016。數位資訊@多媒體安全與應用。台北市：博碩文化。

劉江龍、賴泰宏、李翊豪，2012。可抵抗直方圖攻擊的像素差值藏密技術。第十一屆離島資訊技術與應用研討會。

Bender, W., Gruhl, D., Morimoto, N., and Lu, A., 1996. Techniques for data hiding. IBM Systems Journal, 35(3), 313-336.

BOSS Break Oure Steganographic System, BOSSBases (v0.93) (available online: http://agents.fel.cvut.cz/boss/index.php?mode=VIEW&tmpl=materials [visited on 2021/05/08]).

Chan, C. K. and Cheng, L. M., 2004. Hiding data in images by simple LSB substitution. Pattern Recognition, 37(3), 469-474.

Denemark, T., Fridrich, J., and Holub, V., 2014. Further study on the security of S–UNIWARD, SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics. International Society for Optics and Photonics, 9028, 902805.

Johnson, N. F. and Jajodia, S., 1998. Exploring steganography: Seeing the unseen, Computer, 31(2), 26-34.

Jung, K. H., 2018. Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane, J Real-Time Image Proc, 14(1), 127-136.

Khodaei, M. and Faez, K., 2012. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing, IET Image Processing, 6(6), 677-686.

Liu, H. H., Su, P. C., and Hsu, M. H., 2020. An Improved Steganography Method Based on Least-Significant-Bit Substitution and Pixel-Value Differencing, KSII Transactions on Internet and Information Systems, 14(11), 4,537-4,556.

Liu, H. H., Lin, Y. C., and Lee, C. M., 2018. A digital data hiding scheme based on pixel-value differencing and side match method, Multimedia Tools and Applications, 78(9), 12,157-12,181.

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G., 1999. Information hiding- a survey. Proceedings of the IEEE, 87(7), 1,062-1,078.

Wang, C. M., Wu, N. I., Tsai, C. S., and Hwang, M. S., 2008. A high quality steganographic method with pixel-value differencing and modulus function, The Journal of Systems and Software, 81, 150-158.

Wu, D. C. and Tsai, W. H., 2003. A steganographic method for images by pixel value differencing, Pattern Recognition Letters, 24, 1,613-1,626.

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, IEE Proc-Vis Image Signal Process, 152(5), 611-615.

Zhou, W., and Bovik, A. C., 2002. A universal image quality index, IEEE Signal Processing Letters, 9(3), 81-84.

Zhou, W., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P., 2004. Image quality assessment: from error visibility to structural similarity. IEEE Transactions on Image Processing, 13(4), 600-612.