植基於 LSB 與 PVD 空間域藏密法之效能分析

作者/劉興漢、許孟華

提要

一、近年來網路蓬勃發展，提升資訊傳遞速度與品質，而網路便利同時也帶來了更重要的資訊安全需求。因此，在政府機關和軍事單位的實務應用，除了使用密碼學作為第一層保護之外，還可以運用日益成熟之資訊隱藏技術來實現更完善的資訊防護。

二、本研究藉由修正 Liu 等學者於 2020 年提出之改良 LSB/PVD 藏密法，提出修正改良 LSB/PVD 藏密法。藉由修正藏密使用之像素差值區間及嵌入密文量，並有效利用未藏密的最後 2 行像素，分別使用 LSB、PVD、Modules PVD 及 3-bitLSB/PVD 藏密技術，分析其藏密後的藏密量與偽裝影像品質。

三、根據實驗結果，相較於其他基於 PVD 藏密法，修正改良 LSB/PVD 藏密法在保持影像品質的同時，可顯著提高藏密量（最佳為 17.2%）。研究結果證實本法的可行性，並為軍事通信實務提供可行之大量機敏訊息傳遞技術。

關鍵詞：資訊隱藏、最低有效位元取代法、像素差值藏密法。

前言

隨著網際網路普及和通訊媒體多樣化，以及資訊科技的進步，資訊交換變得更加容易和頻繁。但如果資訊傳遞時沒有伴隨著嚴謹的資訊安全觀念，可能於資訊傳遞途中被有心人士攔截與不法使用，對個人和組織造成嚴重傷害。隨著資訊傳遞速度提升和電子化社會之形成，保護資訊的驗證和保密技術變得越來越重要。儘管資訊技術的發展帶來了便利性，但人們也必須確保資訊安全性，以保護個人隱私和敏感資料。因此，資訊安全重要性日益提高，並需要相應的技術和措施來確保資訊之機密性、完整性和可用性。[1]

政府機關與軍事單位的機敏資訊傳遞時，若將機密訊息採明文方式於網際網路上公開傳遞，是極其不安全之運送選擇。因為有心人士可能會中途攔截這些資訊，試圖窺探其機密內容或進行後續的破壞與中間人攻擊。因此，為了保障機密資訊的安全，政府機關與軍事單位在實務應用中不僅可以使用密碼學作為第

1 李南逸、溫翔安、葉禾田、張智超、林峻立、王智弘，《網路安全與密碼學概論》(臺北市：美商麥格羅希爾國際股份有限分司臺灣分公司，2014)。

一層保護，還可以運用成熟資訊隱藏技術進行更全面的資訊防護。密碼學是廣泛應用於資訊安全實務領域的應用科學，主要使用數學和各類演算法來加密和解密數據，以確保傳輸過程中之機密性和完整性。[2]通過使用加密技術，政府機關與軍事單位可以將機密資訊轉換為密文，以防止未經授權的存取。

而資訊隱藏技術也為機敏資訊的保護，提供第二層保護。資訊隱藏是一種將機密資訊嵌入至看似尋常載體（如相片、影片或音訊）內的技術，使其於資訊傳遞時，不會引人注意。例如，可以將機密資訊嵌入到圖像、音頻或視頻文件中，使其在傳輸過程中顯示為正常的媒體內容，但只有授權人才能提取和解讀其中之機密信息。其中，數位多媒體成為資訊隱藏最常運用的載體。[3]綜合使用密碼學和資訊隱藏技術，政府機關與軍事單位可以建立一個更堅固的資訊防護系統。這樣系統不僅可以加密數據，防止未經授權的存取，還可以將機密資訊隱藏在其他載體內，降低被攔截或識別風險。這樣的結合可確保敏感資訊在傳輸和儲存過程中之安全性和可靠性。

藏密演算法不同於加密演算法，加密演算法需使用金鑰對機敏訊息加密與解密，而藏密技術是將機敏訊息嵌入至各種不同的載體(圖片、音訊及影片)。藏密技術之安全性在於即使不法人士攔截疑似藏密後的偽裝影像，因不知偽裝影像使用何種藏密演算法所產生，亦不知機敏訊息藏在載體影像的那幾個像素(Pixel)，故無法正確取得隱藏於影像內的機敏訊息。故藏密演算法沒有存放加解密金鑰等密鑰管理之問題。

圖 1 說明資訊隱藏技術可分成四大類，包含隱密通道、藏密學、匿名與著作權標記。至目前為止，國內外有多位學者投入資訊隱藏技術之研究，而藏密學（或稱為藏密技術）廣泛應用於國防實務、學術研究和資訊安全等方面。若將欲傳送的秘密訊息嵌入至載體影像後，產生內含密文的偽裝影像，而偽裝影像於網際網路傳遞過程中，由於人類視覺難以察覺偽裝影像中細微改變之像素，故可在不易察覺的情況，進行秘密訊息傳送。即使被不法人士竊取，通常只會視為一般多媒體的傳輸和交換，並不容易察覺其內部隱藏了機密資訊。因此，這種技術能夠提供相對高的安全性，在不受阻礙或破壞情況下，讓接收者只需透過特定方式提取秘密訊息，達到秘密訊息傳遞之目的。

2 婁德權，〈古法新煉的資訊安全技術：藏密學〉《資通安全專論，國家實驗研究院科技政策研究與資訊中心》，2006。

3 婁德權，〈藏密學發展現況〉《資通安全專論，國家實驗研究院科技政策研究與資訊中心》，2006。

圖 1 資訊隱藏技術分類圖

資料來源：Petitcolas et al., 1999。[4]

資訊隱藏技術的 SWOT 分析(如表 1 所示)，將其區分為優勢、劣勢、機會與威脅等四個面向進行說明。

表 1 資訊隱藏技術的 SWOT 分析

優勢(Strengths) **(1)隱匿性：藏密技術能將機敏資訊隱藏在不同的媒體中，使其不易被人類視覺系統察覺，強化了機敏資訊之隱匿性。** **(2)應用靈活：藏密技術可應用於多種載體，如圖片、音頻、視頻等，且可視不同場景調整使用，具應用靈活之優勢。**	**劣勢(Weaknesses)** **(1)影像失真：將機敏資訊隱藏在載體影像內，會導致載體影像的失真。** **(2)高複雜性：某些藏密技術的演算法可能很複雜，且需要大量計算資源。**
機會(Opportunities) **(1)新技術發展：隨著科技進步，新的藏密技術和改進方法持續發展，提供更多應用機會。** **(2)防止數據洩露：隨著藏密技術的進步，軍事單位可藉此技術保護和敏感資訊，減少洩露風險。**	**威脅(Threats)** **(1)敵對攻擊：不法人士可利用藏密技術來傳遞惡意程式碼或隱藏惡意訊息，對國軍單位造成風險。** **(2)人工智慧：隨著人工智慧的發展，新的藏密分析技術會破解藏密技術的隱匿性，從而暴露隱藏的機敏訊息。**

資料來源：作者研究整理

接著以 SWOT 衍伸出 SO(積極性進攻)、ST(差別化策略)、WT(迴避危機)、

4 Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G., "Information hiding-a survey" Proceedings of the IEEE, Vol. 87, No. 7(1999), pp. 1062~1078

WO(階段化策略)來分析資訊隱藏技術。

• SO（積極性進攻）策略：利用資訊隱藏技術優勢，可以積極採取進攻性行動，例如研究創新或整合資訊隱藏方法，以增加隱藏容量，提高資訊隱藏的效率。資訊隱藏技術亦可提供國軍單位更高的情報傳遞安全性，使其能夠積極地進行攻擊行動與隱藏國軍行動意圖，而無需擔心敵方監測和截取。

• ST（差別化策略）策略：利用資訊隱藏技術特點來實施差別化策略，例如提供國軍單位高安全性之資訊隱藏演算法，強化機敏訊息的強韌性。

• WT（迴避危機）策略：針對劣勢，可以採取迴避危機的策略，例如設計與實作資訊隱藏技術時，強調演算法之穩定性和可靠性，減少國軍單位使用資訊隱藏技術時，因未預期之突發狀況而可能導致的問題。

• WO（階段化策略）策略：設計資訊隱藏技術時，可以採取階段化策略，例如透過不斷創新或與人工智慧及物聯網相結合，開發高效靈活的資訊隱藏技術，以滿足國軍不同單位需求。亦可結合資訊隱藏技術與其他軍事技術（如電子戰），可以創建更完整的戰術解決方案。

國外軍事運用資訊隱藏技術實例，其一是發現研判策劃美國911恐攻的蓋達組織，利用藏密技術傳送情報之可能性很高。其二是德國政府逮捕的不法人士，從其電腦內之偽裝色情檔案，發現上百份國際恐怖組織欲隱藏的秘密文件。廣義而言，不法人士之恐怖攻擊可視為軍事活動運用資訊隱藏等技術之案例。[5]而國外軍事運用資訊隱藏等技術與DARPA（美國國防高等研究計畫局）前瞻研究的專案亦有關聯。以生成操作通信通道（Generating Communication Channels to Operate,GeCCO）[6]專案為例，其旨在通過使用靈活的通信架構來部署虛擬網路服務，從而通過防止生命模式分析(pattern-of-life analysis)來保護隱私，從而在允許環境中為軍事應用提供安全通信。如今，遍佈全球的分散式行動需要較小之後勤足跡，以便與任務合作夥伴開展協作，同時還能保護通信隱私。GeCCO將通過安全使用已經普及的蜂窩網路來克服這一挑戰，從而減輕部署軍事系統之後勤負擔。與當今的戰術無線電網路相比，GeCCO將利用虛擬化和軟體程式設計性來創建保護隱私所需網路服務，同時提高服務品質。因資訊隱藏技術的目的是確保安全地通信，故與DARPA之GeCCO專案研究宗旨相同。

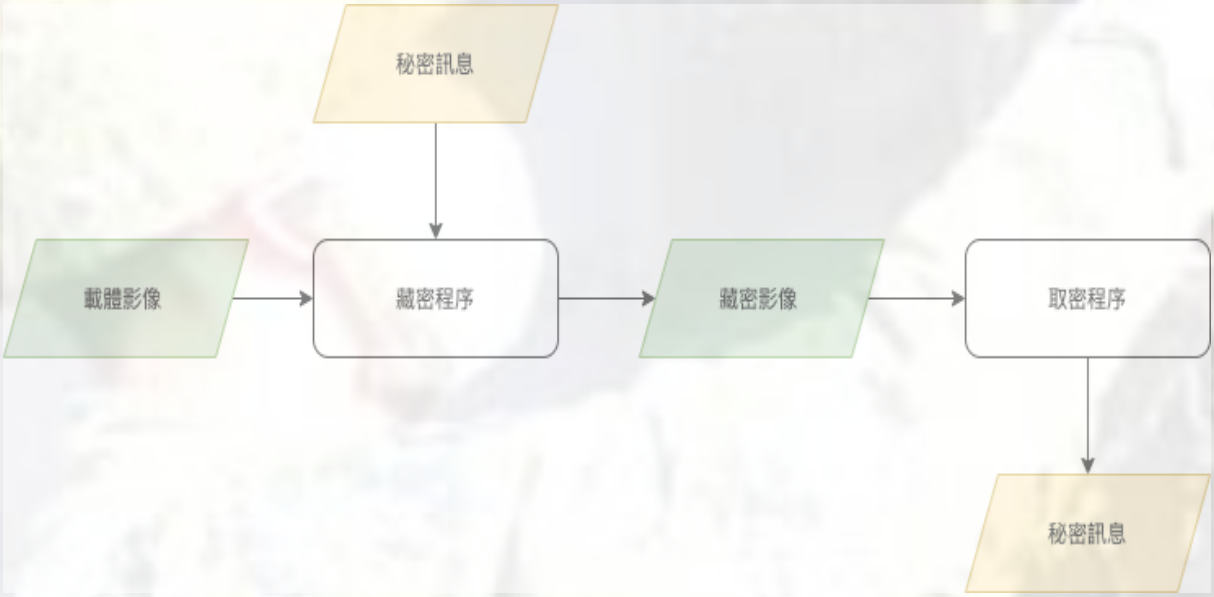
特別是涉及國軍年度各項演訓課目、流程與兵力與武器配置等軍事機密的

5 劉興漢，〈植基於直方圖特徵之數位影像藏密分析技術研究〉，國防大學理工學院國防科學研究所博士學位論文，2013。

6 Schurgot, M. R., “Generating Communication Channels to Operate (GeCCO),” Defense Advanced Research Projects Agency, Retrieved from https://www.darpa.mil/program/generating-communication-channels-to-operate, 2008,(2023/7/27).

國防領域中，如何應用資訊隱藏相關技術，保護其機敏資訊之安全性至關重要。而資訊隱藏技術常使用多媒體型式（例如數位影像、聲音和視訊等）[7]，作為秘密訊息嵌入的載體，其中以數位影像最為主要。主要原因為社群媒體（Facebook、Instagram 及 Youtube）的普及和流行，使得數位媒體交流更加頻繁，而數位影像傳遞成為最常分享的方式。個人或家庭旅行、聚餐與休閒活動，經常以數位影像在各大社群平台上進行分享。而由於數位影像容易取得，因此成為主要的資訊隱藏應用載體。而後續研究將運用數位影像作為載體影像，進行資訊隱藏，而資訊隱藏之藏密和解密基本流程可參考圖 2。

圖 2 資訊隱藏之藏密與取密基本流程圖



資料來源：作者研究整理

雖然資訊隱藏技術可以隱藏機敏訊息的存在，但若有心人士利用藏密技術來傳遞不法行為之相關訊息，會對國土安全造成極大影響。而藏密分析技術(Steganalysis)可檢測是否不法使用藏密技術。藏密分析技術依偵測藏密法的種類不同，可區分為特定藏密分析和通用藏密分析兩種技術。

特定藏密分析針對已知藏密法所產生的特徵進行設計，由於明瞭藏密演算法於嵌入過程對載體影像產生影響，故特定藏密分析技術偵測正確率極高。而通用藏密分析技術則在未知所使用藏密演算法的情況下，將受測影像從空間域之像素轉換至頻率域的係數，或是透過各類直方圖分析，尋找具有區別力的特徵，

7 吳南益、傅國欽、王宗銘，〈植基於像素差值與模數函數之新型灰階影像資料隱藏技術〉《網際網路技術學刊》第11卷第4期，2010，頁1071～1081。

將所得特徵藉由機器（深度）學習進行訓練與測試，故通用藏密分析技術可提供不錯之偵測正確率。

從事資訊隱藏學者主要實踐的目標，其一為提升可嵌入藏密量（Capacity），其二為嵌入大量之密文後，能維持偽裝影像的品質。1996 年 Bender 等學者提出最低有效位元（Least-Significant-Bit, LSB）取代法，[8]2003 年 Wu 等學者提出植基於像素差值（Pixel-Value Differencing, PVD）的藏密技術，[9]分別以單一像素值或 1×2 個連續且不重疊之像素區塊，透過各自藏密演算法將密文嵌入載體影像。

為增加藏密方法的多樣性，陸續有學者結合 LSB 取代法與 PVD 藏密法，並進行相關研究。2005 年 Wu 等學者[10]首先提出結合 LSB 與 PVD 的資訊隱藏技術，而 2010 年 Yang 等學者[11]也提出基於 LSB 與 PVD 結合演算法，藉以改善 Wu 等學者方法之藏密量及偽裝影像品質。2012 年 Khodaei 與 Faez 學者[12]研究中，提出使用 1×3 的像素區塊進行藏密，亦可有效地提高偽裝影像藏密量。而 2020 年 Liu 等學者[13]研究中，結合改良式 LSB 取代法與 2008 年 Wang 等學者[14]所發表基於模數函數（Modulus Function）的 PVD 藏密法，可大幅提升藏密量，並維持人類視覺可接受的偽裝影像品質。但 Liu 等學者的藏密法將載體影像區分成 1×3 個連續且不重複像素區塊進行藏密，而實驗使用之載體影像之長寬為 512×512，會使載體影像中仍有最後 2 行像素（512 mod 3 = 2 ）未使用，造成藏密空間浪費。故本研究將修正 Liu 等學者藏密法的像素差值區間及區間嵌入密文數量等參數，並有效利用最後 2 行像素，分別使用 LSB、PVD、Modules PVD 及 3-bit LSB/PVD 藏密技術，完善利用 512×512 大小之載體影像，並分析其藏密後的偽裝影像之藏密量與藏密後的影像品質。

文獻探討

8 Bender, W., Gruhl, D., Morimoto, N., and Lu, A., “Techniques for Data Hiding,” IBM Systems Journal, Vol.35, No. 3-4(1996), pp. 313~336.

9 Wu, D. C., and Tsai, W. H., “A steganographic method for images by pixel-value differencing” Pattern Recognition Letters, Vol. 24(2003), pp.1613~1626.

10 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“ Proceeding of IEE Inst. Elect. Eng., Vis. Image Signal Process, Vol. 152, No. 5(2005), pp.611~615.

11 Yang, C. H., Weng, C. Y., Wang, S. J., and Sun, H.-M., “Varied PVD+LSB evading detection programs to spatial domain in data embedding systems“ Journal of Systems and Software, Vol. 83, No. 10(2010), pp.1635~1643.

12 Khodaei, M., and Faez, K., “New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing” IET Image Processing, Vol. 6, No. 6(2012), pp. 677~686.

13 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 System, Vol. 14, No. 11(2020), pp. 4537~4556.

14 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(2008), p.p150-158.

一、藏密技術衡量標準

資訊隱藏技術必須滿足下述三項衡量標準：

• 安全性（Security）：除了合法影像擁有者和相對應的授權使用者外，旁人無法從偽裝影像中擷取密文。

• 不可察覺性（Imperceptibility）：載體影像經嵌入密文後，產生之偽裝影像不可嚴重失真，即影像品質需保持可接受的水準，避免影像過度失真，進而引起第三者注意。

• 高藏密量（Payload）：於可接受偽裝影像品質要求下，儘量多嵌入密文，藉此提高影像像素的可嵌入容量。

在資訊隱藏領域中，通常無法完全兼顧偽裝影像品質和藏密量。隨著藏密量的增加，對影像品質之破壞也會增加。因此，如何在偽裝影像的品質和藏密量之間找到平衡點，成為一個重要實務議題。為了評估偽裝影像的品質好壞，可以使用兩種量化衡量標準，即峰值訊號雜訊比（Peak Signal-to-Noise Ratio, PSNR）值和結構相似性指標（Structural Similarity Index, SSIM）。這兩種指標可以用來定義偽裝影像的品質。接下來，將對這兩種衡量標準進行介紹。

• 即峰值訊號雜訊比

PSNR 是由 Zhou 和 Bovik 學者[15]在 2002 年提出的客觀影像品質評估標準。一般而言，根據公式(1)計算的 PSNR 值較高，代表藏密後之影像品質較好。[16]然而，當 PSNR 值低於 30dB 時，表示影像品質已達到人眼無法接受的程度。因此，在評估藏密後影像之品質時，常要求 PSNR 值必須大於 30dB。儘管如此，高 PSNR 值並不一定表示影像品質更好，仍需搭配人眼視覺觀察的輔助來判斷藏密演算法優劣。

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right) \tag{1}$$

$$MSE = \frac{\sum_{n=1}^{FrameSize}(I_n - P_n)^2}{FrameSize}$$

15Zhou, W., and Bovik, A. C., “A universal image quality index” IEEE Signal Processing Letters, Vol. 9, No. 3(2002), pp.81~84.

16廖健宇，〈植基於隨機嵌密順序之具安全性影像藏密技術〉，國防大學管理學院資管系碩士論文，2016。

• 結構相似性指標

Zhou 等學者[17]於 2004 年提出結構相似性指標（SSIM），藉此衡量兩張數位影像之間的類似程度。自然影像通常具有高度結構性，也就是說，其中相鄰像素間存在著強烈的相關性，其蘊含了影像中像素之結構性。由於視覺系統在檢視影像時已經熟練地提取這種結構性，故與傳統的影像品質衡量指標（如 PSNR）相比較，SSIM 更能符合人眼對影像品質之評估。公式(2)用於比較兩張影像的亮度，公式(3)用於比較對比度，公式(4)則用於比較結構性，而 SSIM 的計算公式如公式(5)所示。

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

$$c(x,y)=\frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2} \quad (3)$$

$$s(x,y)=\frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3} \quad (4)$$

$$\boldsymbol{SSIM}=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (5)$$

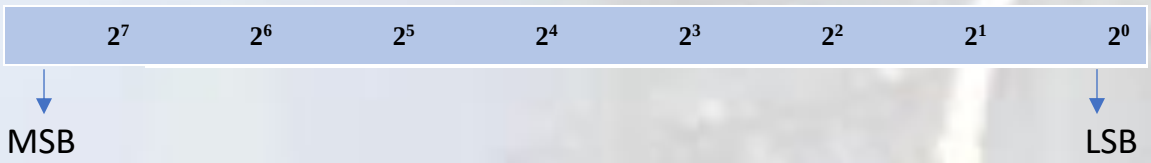
二、最低有效位元取代法

最低有效位元取代法是由 Bender 等學者 1996 年提出的一種方法，用於將秘密訊息直接嵌入影像像素之最低有效位元中。該方法的核心思想是利用最低有效位元，它對像素值的影響較小，將秘密訊息隱藏其中（如圖 3 所示的位置）。以本研究實驗所用灰階影像為例，每個像素的亮度分量使用 8 位元（bits）表示，範圍從 0 到 255（2^8-1），其值為 0 時表示為黑色，若值為 255 時表示為白色，改變每個位元會產生不同的亮度分量值。若更改最高有效位元（Most-Significant-Bit, MSB）的值，亦即從 0 變為 1 或從 1 變為 0，亮度分量會增加或減少 128，對像素值影響很大；而當 LSB 從 0 變為 1 或從 1 變為 0，亮度分量只增減 1，對像素值影響很小。LSB 具有高嵌入量和失真低的優點，以下是 LSB 嵌入密文的

17Zhou, W., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P., "Image quality assessment: from error visibility to structural similarity" IEEE Transactions on Image Processing, Vol. 13, No. 4(2004), pp.600~612.

步驟說明。

圖 3 影像像素最低與最高有效位元位置示意圖



資料來源：Bender et al., 1996。

步驟一：以 C 代表載體影像，其為包含 $M_c \times N_c$ 個像素之 8 位元的灰階影像，以公式(6)表示。

$$C = \{p_{ij} | 0 \le i < M_c, 0 \le j < N_c, p_{ij} \in \{0,1,\ldots,255\}\} \quad (6)$$

步驟二：n-bits 密文以 b 表示，如公式(7)。

$$b = \{b_i | 0 \le i < n, b_i \in \{0,1\}\} \quad (7)$$

步驟三：從 C 依一組設定完成序列，從中選取出n'個像素$\{p_1, p_2, \ldots, p_{n'}\}$，再運用 b 替換 p_i 的 k 個 LSBs，來完成嵌入過程。完成藏密之像素，如公式(8)所示。

$$p'_i = p_i - p_i \bmod 2^k + b \quad (8)$$

LSB 法秘密訊息取出步驟如下：

步驟一：使用與嵌入步驟等同序列，並從偽裝影像 S 內取出嵌入密文的集合 $\{p'_1, p'_2, \ldots, p'_n\}$。

步驟二：針對嵌入密文的集合，擷取每組像素的 k 個 LSBs，藉以取出秘密訊息，如公式(9)。

$$b'_i = p'_i \bmod 2^k \quad (9)$$

LSB 藏密法在最差狀況下，當 $k \geqq 4$ 時，偽裝影像的品質會顯著下降。表 2 列出

當 k 為 1, 2, 3, 4, 5 時，最差狀況下的 PSNR 值。

表 2 LSB 取代法之最差狀況下 PSNR 值表

k	1	2	3	4	5
PSNR	48.13	38.59	31.23	24.61	18.30

資料來源：Bender et al., 1996。

三、像素差值藏密法

2003 年 Wu 和 Tsai 學者基於人類視覺系統的特性，提出 PVD 藏密法。其核心概念為人眼能察覺平滑區域之失真，但對於邊緣區域的失真則相對不容易發現。PVD 藏密法利用像素與鄰近像素之差值來決定嵌入的密文量後，然後調整 1×2 不重疊區塊之像素值，藉以嵌入密文。PVD 藏密法藏密步驟說明如下：

步驟一：將載體影像採 Z 字形掃描，分別區分為 1×2 相鄰且不重疊的像素區塊，其像素以$[p_i, p_{i+1}]$表示，以$d = |p_{i+1} - p_i|$計算像素差值，而 $p_i, p_{i+1} \in [0, \ldots, 255]$。

步驟二：根據表 3 決定像素差值 d 屬於區間 R_k。表 3 相關參數定義如下，l_k 表示區間下限，u_k 表示區間上限，而區間寬度為 $w_k = u_k - l_k + 1$。

表 3 像素差值區間對應表

R_k	像素差值區間 (k)					
	1	2	3	4	5	6
l_k	0	8	16	32	64	128
u_k	7	15	31	63	127	255
n	3	3	4	5	6	7

資料來源：Wu and Tsai, 2003。

步驟三：以$\lfloor \log_2(w_k) \rfloor$ 計算嵌入位元數 n，並從欲嵌入的密文內取出 n 位元後，計算十進位數值 b。

步驟四：使用公式(10)計算新像素差值d'，而d'必須與 d 屬於相同區間。

$$d' = \begin{Bmatrix} l_k + b, \text{if } d \geq 0 \\ -(l_k + b), \text{if } d < 0 \end{Bmatrix} \tag{10}$$

依據公式(11)計算偽裝影像的像素值(p'_i, p'_{i+1})。而若偽裝像素值發生溢位，即不屬於[0-255]之像素值範圍，則此區塊將會進行溢位處理，小於 0 的偽裝像素值設定為 0，而大於 255 的偽裝像素值設定為 255。

$$(p'_i, p'_{i+1}) = \begin{Bmatrix} \left(p_i - \left\lceil \frac{d'-d}{2} \right\rceil\right), \left(p_{i+1} + \left\lfloor \frac{d'-d}{2} \right\rfloor\right), \text{if } d \text{ is odd} \\ \left(p_i - \left\lfloor \frac{d'-d}{2} \right\rfloor, \left(p_{i+1} + \left\lceil \frac{d'-d}{2} \right\rceil\right)\right), \text{if } d \text{ is even} \end{Bmatrix} \tag{11}$$

而 PVD 藏密法則依公式(12)取出密文 b。

$$b = \begin{Bmatrix} d' - l_k, \text{if } d' \geq 0 \\ -d' - l_k, \text{if } d' < 0 \end{Bmatrix} \tag{12}$$

四、植基於模運算之像素差值藏密法

2008 年 Wang 等學者基於模數函數運算的特性，提出模運算像素差值藏密法(Modulus PVD, MPVD)，藉由模數函數之雙向調整特性，減少偽裝影像的失真，並優化偽裝影像品質，其密文嵌入載體影像之步驟如下：

步驟一：比照 PVD 藏密法，將載體影像區分成相鄰且不重複的 1×2 像素區塊，其像素值分別為 Pi 及 Pi+1，以$d = |P_i - P_{i+1}|$計算像素差值，並依表 3 判斷差值 d 屬於那個區間，可得密文嵌入數 n。

步驟二：以公式(13)計算 P_i 及 P_{i+1} 之和與 mod 2^n 的餘數值 F_{rem}。

$$F_{rem} = (P_i + P_{i+1}) \bmod 2^n \quad (13)$$

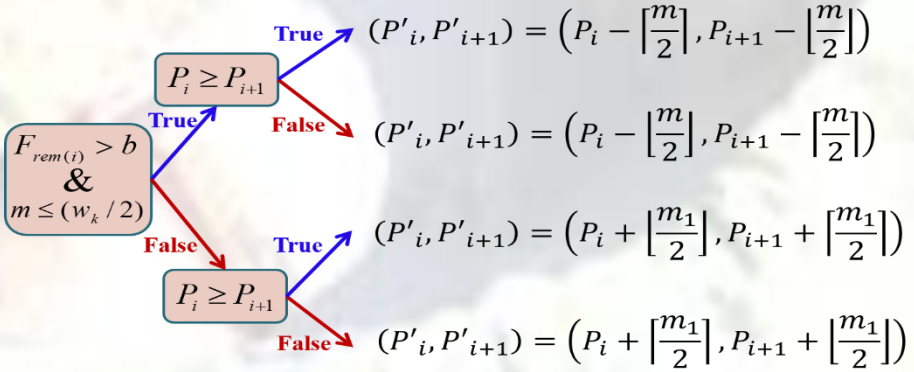
步驟三：以 b 代表欲嵌入密文之十進位值，使用公式(14)及公式(15)計算 m 與 m_1 值

$$m = |F_{rem} - b| \quad (14)$$

$$m_1 = 2^n - |F_{rem} - b| \quad (15)$$

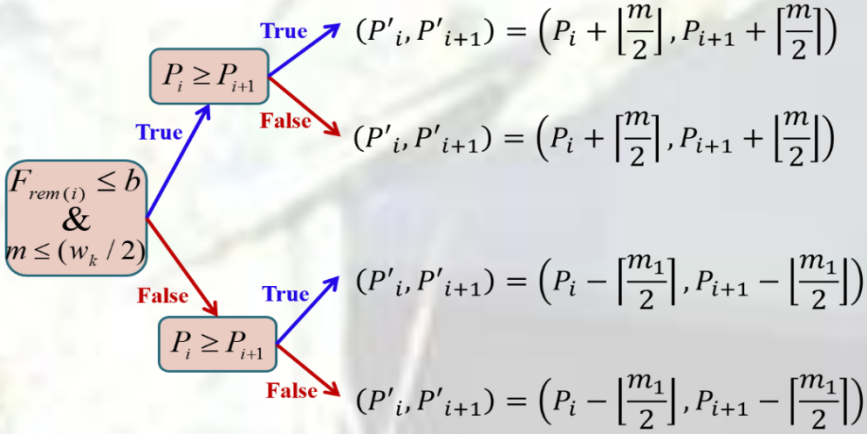
步驟四：依照 F_{rem}、m 與 m_1 值的大小，進行偽裝像素值調整，如圖 4 與圖 5 之說明

圖 4 模運算像素差值藏密法嵌密情況（一）



資料來源：Wang et al., 2008。

圖 5 模運算像素差值藏密法嵌密情況（二）



資料來源：Wang et al., 2008。

步驟五：若偽裝像素值發生溢位狀況，而像素差值若小於 128 時，依公式(16)與公式(17)進行調整：

Case1：$P_i \geq 0$且$P_{i+1} \geq 0$且（$P'_i < 0$或$P'_{i+1} < 0$）

$$(P''_i, P''_{i+1}) = (P'_i + 2^n/2, P'_{i+1} + 2^n/2) \quad (16)$$

Case2：$P_i \leq 255$且$P_{i+1} \leq 255$且（$P'_i > 255$或$P'_{i+1} > 255$）

$$(P''_i, P''_{i+1}) = (P'_i - 2^n/2, P'_{i+1} - 2^n/2) \quad (17)$$

步驟六：若偽裝像素值發生溢位狀況，而像素差值若大於 128 時，依公式(18)進行調整：

$$(P''_i, P''_{i+1}) = \begin{cases} (0, P'_i + P'_{i+1}), \text{if } P'_i < 0 \text{ and } P'_{i+1} \geq 0 \\ (P'_i + P'_{i+1}, 0), \text{if } P'_i \geq 0 \text{ and } P'_{i+1} < 0 \\ \left(255, P'_i + (P'_{i+1} - 255)\right), \text{if } P'_i > 255 \text{ and } P'_{i+1} \geq 0 \\ \left(P'_i + (P'_{i+1} - 255), 255\right), \text{if } P'_i \geq 0 \text{ and } P'_{i+1} > 255 \end{cases} \quad (18)$$

MPVD 藏密法取出密文時，針對偽裝影像區分成 1×2 不重複的像素區塊後，計算像素差值d'。並依表 3 判斷差值d'屬於那個區間，取得嵌入密文之位元數 n，並計算出區塊像素之和後，再模運算 2^n，其餘數即為所嵌入的密文。

2012 年劉江龍等三位學者[18]提出改進論點，指出 MPVD 藏密演算法有無法正確取出密文的情況，進一步提出改良式 MPVD 藏密法，藉此修正 MPVD 異常藏密分析特徵，並同步改善上述密文取出不正確的狀況。

改良式 MPVD 藏密法主要是在使用 MPVD 藏密法嵌入密文後，修正偽裝像素差值為區間上限 u_k 之區塊的指定位元值，藉以分別其藏密前之像素差值區間。其詳細步驟為挑出像素差值為 u_k ($k \geq 1$)的偽裝像素區塊，假設與其相應之載體像素區塊中像素差值為下一個區間之下限值為 l_{k+1} 時，則把偽裝像素區塊中 2 個像素的第 n+1 個位元值都修正成 1，假設與其相應之載體像素區塊中像素差值為 u_k，則將 2 個像素的第 n+1 個位元值都修正成 0。

而改良式 MPVD 藏密法於密文提出的程序如下，當偽裝像素區塊中像素差值為 u_k($k \geq 1$) 時，假設 2 個像素的第 n+1 個位元值是 1，則可把載體像素區塊中之像素差值設定為 l_{k+1}，假設 2 個像素的第 n+1 個位元值是 0，可判斷其載體像素區塊中像素差值為 u_k。決定 2 個像素所屬之正確藏密區間後，後續則可使用 MPVD 藏密法取密步驟，取出正確密文。

密文嵌入過程說明，若載體像素區塊為（50, 66），且要嵌入的密文為 7。故

18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，2012。

可計算出像素差值 d=16 及 n=4。使用 MPVD 藏密法嵌入密文後，偽裝像素區塊中的像素值將成為（57, 72），此時差值d'=15。根據表 3 像素差值區間的定義，可決定出 n=3，這可能導致後續提取秘密訊息時出現跨區間取密錯誤。

因此，改良 MPVD 方法調整 2 個像素的第 4 個位元值，於取出密文時也針對第 4 個位元進行判斷。若第 4 個位元值等於 1，則使用 2^4 進行模運算；若等於 0，則使用 2^3 進行模運算，這樣的改進可以解決秘密訊息提取錯誤的問題。

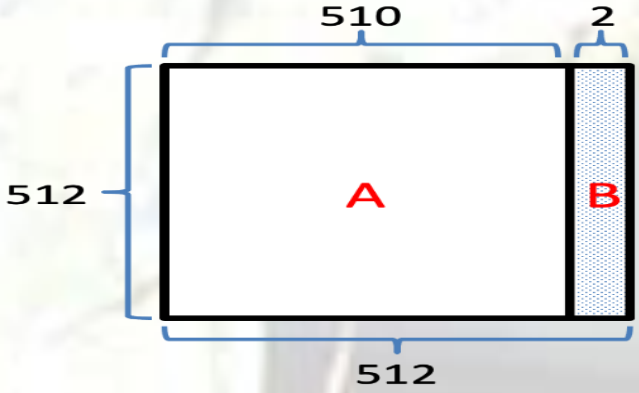
植基於 LSB 與 PVD 空間域藏密法之效能分析

一、系統架構設計

本研究的改良式藏密法是修正 Liu 等學者於 2020 年提出之改良式 LSB/PVD 藏密法，修正藏密區間與所嵌入的密文數，並將未藏密之像素區塊，分別使用 LSB、PVD、Modules PVD 及 3-bit LSB/PVD 藏密技術進行，分析其藏密後的偽裝影像藏密量與品質，本研究系統架構設計說明如下。

先將 512×512 載體影像分割為 1×3 個相鄰且不重複像素之區塊，後續嵌入密文的過程先針對圖 6 之載體影像 A 區塊進行藏密後，再針對圖 6 之載體影像 B 區塊 2×512 個像素進行 LSB、PVD、Modules PVD 及 3-bit LSB/PVD 藏密，後續針對各個藏密法進行效能分析。藉由有效利用載體影像藏密空間前提下，測試不同之藏密技術所帶來的影響。並儘可能地保持偽裝影像品質，有效提升本研究之藏密量。表 4 說明使用之藏密技術，表 5 說明本研究使用之符號。

圖 6 載體影像藏密示意圖



資料來源：作者研究整理。

表 4 本研究之改良式資訊隱藏技術結合之各藏密法表

項目	藏密法
1	3, 4, 5-bits LSB
2	PVD
3	MPVD
4	3-bit LSB/PVD

資料來源：作者研究整理。

表 5 本研究方法符號說明表

項目	符號	說明
1	C、S	載體影像、偽裝影像
2	c_i、s、k	大小為 1×3 像素之區塊、嵌入之二進位秘密訊息、最低有效位元取代法的置換量
3	P_{ic}、P_{i1}、P_{i2}	基底像素、基底像素左邊像素、基底像素右邊像素
4	LSB_i	基底像素中最低 3 個有效位元轉換成十進位的值
5	s_{ic}	藏入基底像素之秘密訊息轉換成十進位的值
6	d_{ic}	LSB_i 與 s_{ic} 的差值
7	d_{i1}、d_{i2}	左邊像素與藏密後基底像素的差值、右邊像素與藏密後基底像素的差值
8	R_j	像素差值所屬區間
9	n	嵌入秘密訊息的位元數
10	F_{remL}、F_{remR}	P_{i1} 及 P_{i2} 分別與P'_{ic}之和 mod 2^n 的餘數值
11	b_{iL}、b_{iR}	嵌入 P_{i1} 及 P_{i2} 之秘密訊息的十進位值

資料來源：作者研究整理。

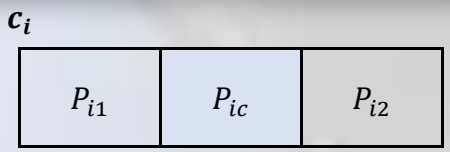
二、本研究藏密程序

藏密流程如下說明，各個方程式內所使用變數之定義，請參閱表 5：

步驟一：針對欲嵌入密文之載體影像 C，分為包含 510×512 像素 A 及包含 2×512 像素 B，並先執行 A 部分之藏密步驟，將載體影像 C 進行 zig-zag 掃描，各別形成 1×3 個相鄰且不重複像素的區塊。

步驟二：P_{ic} 為區塊的中間像素，於本研究定義為基底像素（如圖 7）。

圖 7 基底像素選定示意圖



資料來源：作者研究整理。

步驟三：定義本研究使用 LSB 之取代量為 3 bit（k = 3），使用 3 bit 二進位密文置換 P_{ic} 二進位基底像素的最低 3 位元，可得已藏密之基底像素P'_{ic}。把原基底像素 P_{ic} 的最低 3 位元轉成十進位數值 LSB_i，並把剛嵌入基底像素之密文轉成十進位值 s_{ic}。

步驟四：以公式(19)計算 LSB_i 與 s_{ic} 的差值 d_{ic}。

$$d_{ic} = LSB_i - s_{ic} \tag{19}$$

步驟五：以公式(20)之最佳像素調整程序（OPAP）調整基底像素P'_{ic}。

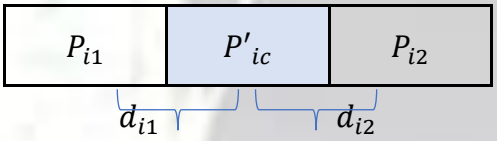
$$P'_{ic} = \begin{cases} P'_{ic} + 2^k, \text{if } d_{ic} > 2^{k-1} \text{ and } 0 \le P'_{ic} + 2^k \le 255 \\ P'_{ic} - 2^k, \text{if } d_{ic} < -2^{k-1} \text{ and } 0 \le P'_{ic} - 2^k \le 255 \\ P'_{ic}, \text{otherwise} \end{cases} \tag{20}$$

步驟六：分別以公式(21)與公式(22)計算像素 P_{i1} 與 P_{i2} 與藏密後基底像素P'_{ic}的差值 d_{i1} 和 d_{i2}，圖 8 為 2 組像素差值計算示意圖。參考圖 9 之區間設定，可得欲嵌入密文的位元數 n。本研究修正原本 Liu 等學者設定的區間範圍與嵌入位元數（區間設定修正為[0-63]與[64-255]、嵌入位元數修正為 5 與 6 bits）。

$$d_{i1} = |P_{i1} - P'_{ic}| \tag{21}$$

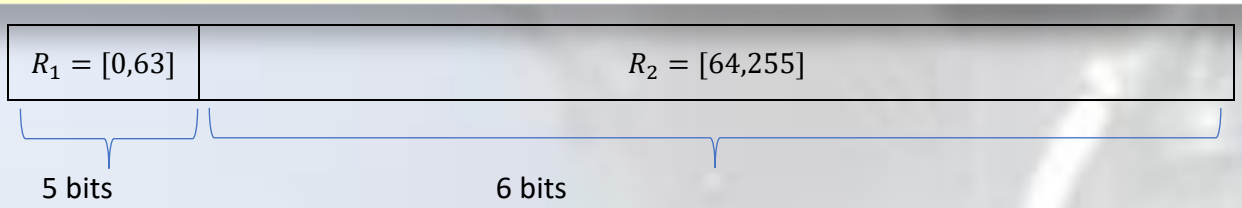
$$d_{i2} = |P_{i2} - P'_{ic}| \tag{22}$$

圖 8 像素差值示意圖



資料來源：作者研究整理。

圖 9 像素差值範圍區間設定圖



資料來源：作者研究整理。

步驟七：各別計算像素 P_{i1} 和 P_{i2} 與P'_{ic}之和，以公式(23)與公式(24)計算 mod 2^n 的餘數值 F_{remL} 和 F_{remR}。

$$F_{remL} = (P_{i1} + P'_{ic}) \bmod 2^n \tag{23}$$

$$F_{remR} = (P_{i2} + P'_{ic}) \bmod 2^n \tag{24}$$

步驟八：嵌入像素 P_{i1} 與 P_{i2} 之密文之十進位值分別為 b_{iL} 與 b_{iR}，兩者之 m_{ia} 與 m_{ib} 值可依公式(25)至(28)計算，分別表示為 m_{iaL} 與 m_{iaR}，以及 m_{ibL} 與 m_{ibR}：

$$m_{iaL} = |F_{remL} - b_{iL}| \tag{25}$$

$$m_{iaR} = |F_{remR} - b_{iR}| \tag{26}$$

$$m_{ibL} = 2^n - |F_{remL} - b_{iL}| \tag{27}$$

$$m_{ibR} = 2^n - |F_{remR} - b_{iR}| \tag{28}$$

步驟九：依 F_{remL}、F_{remR}、m_{iaL}、m_{iaR}、m_{ibL}、m_{ibR}的值，區分成 4 種狀況進行像素值計算，如公式(29)至(32)（公式內之 F_{rem} 為 F_{remL} 或 F_{remR}，m_{ia} 為 m_{iaL} 或 m_{iaR}，m_{ib} 為 m_{ibL} 或 m_{ibR}，b_i 為 b_{iL} 或 b_{iR}，P_i 為 P_{i1} 或 P_{i2}，而P'_i為P'_{i1}或P'_{i2}）：

Case1：$F_{rem} > b_i$ and $m_{ia} \leq (2^n/2)$

$$P'_i = P_i - m_{ia} \tag{29}$$

Case2：$F_{rem} > b_i$ and $m_{ia} > (2^n/2)$

$$P'_i = P_i + m_{ib} \tag{30}$$

Case3：$F_{rem} \le b_i$ and $m_{ia} \le (2^n/2)$

$$P'_i = P_i + m_{ia} \tag{31}$$

Case4：$F_{rem} \le b_i$ and $m_{ia} > (2^n/2)$

$$P'_i = P_i - m_{ib} \tag{32}$$

步驟十：若像素值在藏密後發生溢位情形，則依公式(33)進行調整，並完成載體影像 A 部分藏密。

$$P'_i = \begin{cases} P'_i + 2^n, \text{if } P_i \ge 0 \text{ and } P'_{ic} \ge 0 \text{ and } P'_i < 0 \\ P'_i - 2^n, \text{if } P_i \le 255 \text{ and } P'_{ic} \le 255 \text{ and } P'_i > 255 \end{cases} \tag{33}$$

步驟十一：分別使用 LSB（2-bit、3-bit、4-bit）、PVD、MPVD 及 3-bit LSB/PVD 等藏密法針對載體影像之 B 部分進行藏密，之後步驟僅就 PVD 藏密法進行說明，其餘步驟請參閱 2.3 章說明。

步驟十二：使用 Z 字形掃描載體影像 B 部分，區分為 1×2 相鄰且不重疊的像素區塊，其像素以$[p_i, p_{i+1}]$表示，以$d = |p_{i+1} - p_i|$計算這組 2 個像素的差值。

步驟十三：由表 6 決定 d 屬於那組 R_k 區間，可得區間寬度為 $w_k = u_k - l_k + 1$。

表 6 PVD 像素差值區間對應表

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

步驟十四：使用 $\lfloor \log_2(w_k) \rfloor$ 計算嵌入位元數 n，並從欲嵌入的密文內取出 n 位元後，計算十進位數值 b。

步驟十五：使用公式(34)計算新像素差值d'，而d'必須與 d 屬於相同區間。

$$d' = \begin{Bmatrix} l_k + b, \text{if } d \geq 0 \\ -(l_k + b), \text{if } d < 0 \end{Bmatrix} \quad (34)$$

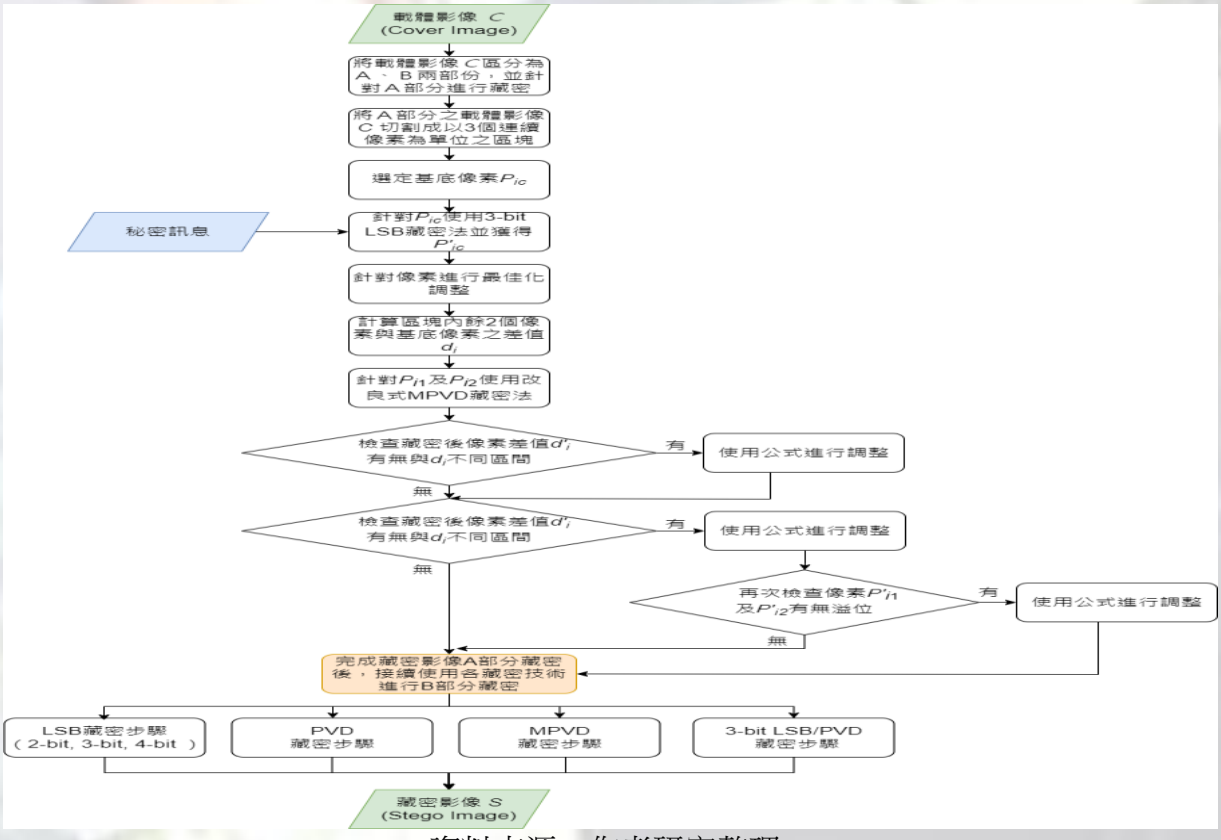
步驟十六：依據公式(35)計算偽裝影像的像素值(p'_i, p'_{i+1})。

$$(p'_i, p'_{i+1}) = \begin{Bmatrix} \left(p_i - \left\lceil \frac{d'-d}{2} \right\rceil\right), \left(p_{i+1} + \left\lfloor \frac{d'-d}{2} \right\rfloor\right), \text{if } d \text{ is odd} \\ \left(p_i - \left\lfloor \frac{d'-d}{2} \right\rfloor, \left(p_{i+1} + \left\lceil \frac{d'-d}{2} \right\rceil\right)\right), \text{if } d \text{ is even} \end{Bmatrix} \quad (35)$$

步驟十七：若偽裝像素值發生溢位，即不屬於[0-255]之像素值範圍，則此區塊將會進行溢位處理，小於 0 的偽裝像素值設定為 0，而大於 255 的偽裝像素值設定為 255，並完成載體影像 B 部分藏密。

本研究所提出之藏密方法，藏密完整流程如圖 10 所示。

圖 10 藏密流程圖



資料來源：作者研究整理。

三、取密程序

密文提取程序較藏密簡易，本研究之取密步驟如下說明：

步驟一：針對欲處理的偽裝影像，分為 A 及 B 兩個部分。

步驟二：將偽裝影像之 A 部分分割成包含 1×3 個區塊為單位之像素。

步驟三：指定基底像素為區塊的中間像素P'_{ic}，並取出基底像素的密文。

步驟四：針對左右 2 個像素與基底像素P'_{ic}的差值進行計算，依表 6 判斷差值所屬區間，並依序將十進位之密文 b_i 取出，並將其轉換為二進位值，如公式(36)所示。

$$b_i = (P'_i + P'_{ic}) \bmod 2^n \tag{36}$$

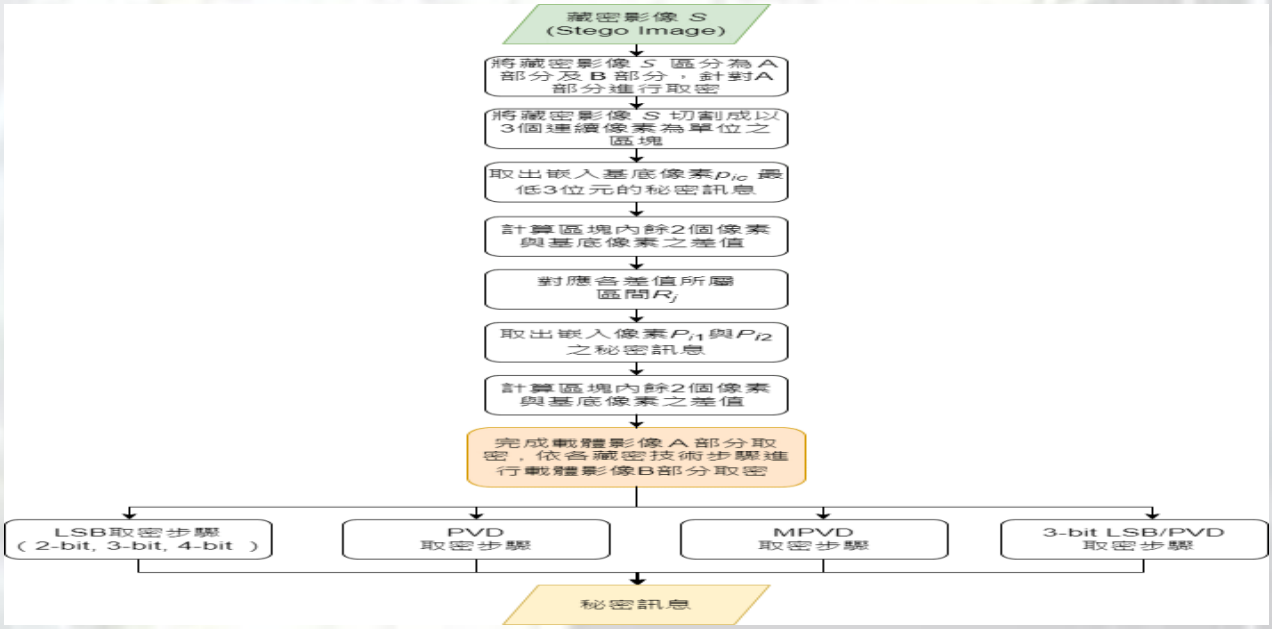
步驟五：偽裝影像之 A 部分成功取密後，接續依 LSB（2-bit、3-bit、4-bit）、PVD、MPVD 及 3-bit LSB/PVD 等藏密法取密步驟，將 B 部分偽裝影像之像素擷取密文，之後取密步驟僅就 PVD 藏密法進行說明，其餘步驟請參閱 2.3 章說明。

步驟六：偽裝影像之 B 部分使用 PVD 嵌入密文，而 PVD 藏密法則依公式(37)取出密文 b。

$$b = \begin{cases} d' - l_k, \text{if } d' \geq 0 \\ -d' - l_k, \text{if } d' < 0 \end{cases} \tag{37}$$

本研究提出之藏密方法，完整取密流程如圖 11 所示。

圖 11 取密流程圖



資料來源：作者研究整理。

實驗結果分析

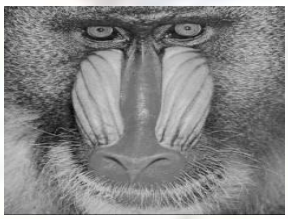
一、實驗環境

本研究實驗過程使用硬體環境為MacBook Pro 3.1GHz雙核心Intel Core i5 8GB RAM筆記型電腦，藉以執行上述藏密法嵌入與取出密文之程序與評量偽裝影像之藏密量與品質。而軟體環境為運用Pycharm CE應用程式，以Python實作修正改良式最低有效位元與像素差值法之藏密技術（後續稱為修正改良LSB/PVD）

二、實驗結果分析

本研究選用了Barbara等8張512x512灰階經典影像，這些影像在資訊隱藏領域中被廣泛使用，用作主要的測試影像（如圖12所示）。這些影像包含了各種紋理複雜和平滑區間的特徵，涵蓋了人像、風景照、物品和交通工具等多樣的影像類型，能夠代表大部分數位影像的內容。為評估偽裝影像品質，本研究使用PSNR值和SSIM值作為評量指標。

圖12 本研究使用之測試影像

			
Barbara	Boat	F16	Goldhill
			
Lena	Mandrill	Peppers	Tiffany

資料來源：作者研究整理。

依本研究提出參數修正與充分使用載體影像藏密空間之修正改良式LSB/PVD方法(修正改良LSB/PVD)之藏密步驟，與改良LSB/PVD(Liu et al., 2020)、LSB藏密法（Chan與Cheng, 2004）、PVD藏密法（Wu and Tsai, 2003）、MPVD藏密法（Wang et al., 2008）及3-bit LSB/PVD（Wu, H. C. et al., 2005）進行比較，其中修正改良式LSB/PVD藏密技術除了改變兩個區間的區間範圍與嵌入密文數(區間設定修正為[0-63]與[64-255]、嵌入位元數修正為5與6 bits）外，最後2欄像素使用LSB進行藏密。上述藏密技術實驗結果如表7至表9所示。其中，各種藏密法之藏密量比較如表7，PSNR值比較如表8，而SSIM值比較如表9所示

從表 7 針對藏密量的比較，可發現本研究（修正改良 LSB/PVD）針對載體影像的 A 部分先進行藏密，並調整其像素差值區間設定值 R_i 及可嵌入區間的秘密訊息位元數 n，原區間設定值 R_1 = [0-31] 及 R_2 = [32-255]，修正為 R_1 = [0-63] 及 R_2 = [64-255]，原 R_1 區間可嵌入密文位元數為 4 位元、R_2 區間可嵌入密文位元數為 5 位元。經本研究之參數修正後，R_1 區間調整至 5 位元、R_2 區間調整至 6 位元，而 B 部分採 LSB 進行藏密，其平均藏密量為 1,133,669 位元，與改良式 LSB/PVD 藏密法相較，可提升約 17.2%的藏密量。而載體影像 A 部分若使用改良 LSB/PVD 藏密法，在 B 部分分別結合 LSB、PVD、MPVD 及 3-bit LSB/PVD 等藏密法中，可發現 4-bit LSB 平均藏密量為 971,407 位元，與改良式 LSB/PVD 藏密法相較，可提升約 0.4%的藏密量，而 3bit LSB/PVD 藏密法平均藏密量為 970,407 位元，可提升約 0.3%的藏密量，接續為 MPVD 藏密法，平均藏密量為 969,016 位元，可提升約 0.18%藏密量，最後 PVD 藏密法平均藏密量為 968,903 位元，可提升約 0.17%藏密量

表 7 各方法藏密量比較表（位元數）

方法 / 影像	修正改良 LSB/PVD	改良 LSB/PVD (2020)	LSB(2004)			PVD (2004)	MPVD (2008)	3-bit LSB/PVD (2005)
			2-bit	3-bit	4-bit			
Barbara	1,139,491	983,749	985,734	986,808	987,849	985,191	985,213	986,719
Boat	1,133,128	965,941	968,009	969,041	970,065	967,650	967,664	968,849
F16	1,132,751	963,471	965,555	966,548	967,583	965,032	965,945	966,500
Goldhill	1,131,996	962,633	964,693	965,727	966,730	964,206	964,238	965,592
Lena	1,132,227	962,452	964,492	965,503	966,532	964,038	964,000	965,482
Mandrill	1,134,771	977,179	979,252	980,222	981,278	978,924	978,910	980,046
Peppers	1,132,615	961,563	963,606	964,628	965,659	963,158	963,145	965,572
Tiffany	1,132,376	961,449	963,513	964,498	965,560	963,024	963,012	964,497
Average	**1,133,669**	**967,305**	**969,357**	**970,372**	**971,407**	**968,903**	**969,016**	**970,407**

資料來源：作者研究整理。

從表 8 與 9 針對影像品質的比較，可發現本研究之修正改良 LSB/PVD 藏密法，於調整像素差值區間及嵌入區間的密文位元數與充分使用載體影像藏密空間後，平均 PSNR 值為 29.66 dB，SSIM 值平均為 0.704。在大幅提高藏密量的同時，偽裝影像品質亦即大幅下降（PSNR 值下降約 14.8%，而 SSIM 值下降約 18.1%），

但觀察 8 張測試影像經修正改良 LSB/PVD 藏密後之偽裝影像（如圖 13 所示）後，仍可接受其影像品質。故本研究提出之修正改良 LSB/PVD 藏密法，適用於需傳遞大量機敏訊息之情境。

表 8 各方法 PSNR 值比較表（dB）

方法 / 影像	修正改良 LSB/PVD	改良 LSB/PVD (2020)	LSB(2004)			PVD (2004)	MPVD (2008)	3-bit LSB/PVD (2005)
			2-bit	3-bit	4-bit			
Barbara	28.604	33.762	33.790	33.745	33.603	33.780	33.765	33.760
Boat	29.938	35.006	35.022	34.977	34.840	35.040	35.042	35.035
F16	30.210	35.335	35.332	35.274	35.062	35.331	35.332	35.340
Goldhill	30.312	35.313	35.249	35.239	35.057	35.315	35.294	35.288
Lena	30.182	35.354	35.357	35.312	35.122	35.348	35.38	35.360
Mandrill	29.537	33.934	33.859	33.814	33.704	33.922	33.915	33.895
Peppers	29.296	34.891	35.003	34.950	34.731	34.981	34.969	34.920
Tiffany	29.197	34.764	34.786	34.772	34.610	34.792	34.802	34.764
Average	**29.660**	**34.795**	**34.800**	**34.760**	**34.591**	**34.814**	**34.812**	**34.795**

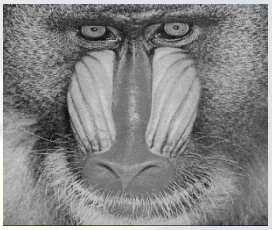
資料來源：作者研究整理。

表 9 各方法 SSIM 值比較表

方法 / 影像	修正改良 LSB/PVD	改良 LSB/PVD (2020)	LSB(2004)			PVD (2004)	MPVD (2008)	3-bit LSB/PVD (2005)
			2-bit	3-bit	4-bit			
Barbara	0.7675	0.918	0.9087	0.9088	0.9082	0.9092	0.9092	0.9086
Boat	0.7354	0.900	0.8946	0.8950	0.8943	0.8955	0.8950	0.8950
F16	0.7015	0.882	0.8807	0.8807	0.8800	0.8807	0.8810	0.8809
Goldhill	0.7789	0.920	0.9185	0.9188	0.9179	0.9188	0.9188	0.9184
Lena	0.7109	0.896	0.8878	0.8877	0.8867	0.8883	0.8880	0.8877
Mandrill	0.5717	0.956	0.6268	0.6266	0.6272	0.6619	0.6271	0.6279
Peppers	0.7044	0.900	0.8889	0.8890	0.8881	0.8890	0.8886	0.8887
Tiffany	0.6669	0.883	0.8725	0.8723	0.8714	0.8724	0.8721	0.8718
Average	**0.7047**	**0.907**	**0.8598**	**0.8599**	**0.8592**	**0.8645**	**0.8600**	**0.8599**
註：SSIM 值介於−1~1(1 代表與原始載體影像完全相同，0 則代表無結構相似度)								

資料來源：作者研究整理。

圖 13 測試影像經修正改良 LSB/PVD 藏密後之偽裝影像

			
Stego Barbara	Stego Boat	Stego F16	Stego Goldhill
			
Stego Lena	Stego Mandrill	Stego Peppers	Stego Tiffany

資料來源：作者研究整理。

而改良 LSB/PVD 在針對載體影像 B 部分結合各式藏密法進行藏密後，因具有較高的藏密量，故影像品質均略為下降。

結論

一、研究結論

本研究主要目標是有效利用改良 LSB/PVD 藏密法未用之 2×512 行的剩餘空間與修正藏密區間範圍與相對應之嵌入密文數，提出修正改良 LSB/PVD。經過多次實驗測試後，本研究調整區間範圍大小和秘密訊息藏入位元數來進行藏密。具體而言，實驗結果達到大幅提升藏密量目標，同時維持可接受之偽裝影像品質。

在資訊隱藏領域中，針對各種藏密方法所進行效益評估標準，其一為藏密量的大小，其二為偽裝影像品質是否可接受。本研究所提修正改良 LSB/PVD 藏密法可有效提升載體影像之藏密量，並略維持人眼可接受的影像品質。相較於改良 LSB/PVD 藏密法，本研究的修正改良 LSB/PVD 藏密法，包含改良 LSB/PVD 藏密法與分別結合 2-bit LSB 藏密法、3-bit LSB 藏密法、4-bit LSB 藏密法、PVD 藏密法、MPVD 藏密法及 3-bit LSB/PVD 藏密法，其藏密量分別提升 166,364 位元（17.2%）、2,052 位元（0.2%）、3,067 位元（0.3%）、4,102 位元（0.4%）、1,598 位元（0.2%），以及 3,102 位元（0.2%）。

而影像品質評量部分，修正改良 LSB/PVD 藏密法與其它藏密法相比較，其 PSNR 值除改良 LSB/PVD 藏密法、3-bits LSB 藏密法及 4-bits LSB 藏密法分別下降約 14.8%、0.1%及 0.5%外，其餘 2-bits LSB、PVD 藏密法、MPVD 藏密法

及 3-bitLSB/PVD 藏密法分別約可提升 0.5%、0.05%、0.05%及 0.001%。而 SSIM 值除 PVD 藏密法可提升 0.5%外，其餘改良 LSB/PVD 藏密法、2-bits LSB 藏密法、3-bits LSB 藏密法、4-bits LSB 藏密法、MPVD 藏密法及 3-bit LSB/PVD 藏密法分別下降約 18.06%、0.02%、0.02%、0.1%、0.01%、0.82%。實驗結果證明本研究提出之修正改良 LSB/PVD 藏密法，可在仍維持可接受偽裝影像品質的前提下，有效提升藏密量，適用於軍事通信實務領域需傳遞大量機敏資訊之情境。

現今 AI 影像辨識與偽冒相關技術日益成熟，對藏密技術發展也帶來影響。藏密技術(Steganography)旨在保護機密訊息於傳遞過程中，不被有心人士不當擷取、破壞與利用。而藏密分析技術(Steganalysis)則為與之相對抗的技術，其重點是找出於藏密過程改變原始影像之相關特徵，並搭配機器學習相關技術（如類神經網路、支援向量機），判斷受測影像是否有藏密。所以藏密技術與利用 AI 進行藏密分析或影像辨識的技術，兩者確實存在矛與盾關係。

而為避免藏密過程改變原始影像的相關特徵，進而被藏密分析技術判斷有藏密，可透過生成對抗網路（Generative Adversarial Network, GAN）等技術產生不被藏密分析技術偵測有嵌入機敏訊息之偽裝影像，加強藏密技術安全性。

二、研究建議與國防領域應用

本研究修正改良 LSB/PVD 藏密法可有效提升了藏密量，並結合了不同藏密法。在實際應用中，這些不同的藏密法能夠有效對抗藏密分析技術之偵測，增加有心人士破解密文的時間成本，從而提升傳遞秘密訊息安全性。這些相關的藏密演算法，平時國軍軍事情報單位可運用於相關情報資訊傳遞，亦可運用於各項年度演訓之情報通信環節，確保情報工作安全。

戰時則可以應用於國防軍事領域，以一個簡單的軍事應用情境為例，若戰場指揮官向他的部隊發送攻擊發起時間命令，若用明文傳遞，其洩密的風險極高。但指揮官利用加密技術傳送機密訊息，有心人士亦會察覺加密訊息，即使無法順利解密他可以從中破壞加密訊息，使訊息無法到達指揮官之所屬部隊。此時，指揮官可利用藏密演算法將該命令嵌入載體影像，使其成為一個偽裝影像。因人眼無法視覺判斷偽裝影像與一般影像之差別，故不法人士無法從中攔截。該偽裝影像被傳送到部隊後，部隊可以使用取密演算法從中提取出指揮官下達的攻擊發起時間命令。

在影像傳遞過程中，即使有心人士發現偽裝影像中包含機密資訊並試圖攻擊，因不知偽裝影像所使用的藏密演算法，故他們無法在有效時間內獲得取密演算法，且有心人士無法取得相同的載體影像，亦無法偽造影像進行傳送。因此可以有效提高安全性(上述流程如圖 14 所示)。

圖 14 情境模擬示意圖

資料來源：作者研究整理。

參考文獻

一、吳南益、傅國欽、王宗銘，〈植基於像素差值與模數函數之新型灰階影像資料隱藏技術〉《網際網路技術學刊》第 11 卷第 4 期，2010，頁 1071～1081。

二、李南逸、溫翔安、葉禾田、張智超、林峻立、王智弘，《網路安全與密碼學概論》(臺北市：美商麥格羅希爾國際股份有限分司台灣分公司，2014)。

三、婁德權，〈古法新煉的資訊安全技術：藏密學〉《資通安全專論，國家實驗研究院科技政策研究與資訊中心》，2006。

四、婁德權，〈藏密學發展現況〉《資通安全專論，國家實驗研究院科技政策研究與資訊中心》，2006。

五、廖健宇，〈植基於隨機嵌密順序之具安全性影像藏密技術〉，國防大學管理學院資管系碩士論文，2016。

六、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，2012。

七、劉興漢，〈植基於直方圖特徵之數位影像藏密分析技術研究〉，國防大學理工學院國防科學研究所博士學位論文，2013。

八、**Chan, C. K., and Cheng, L. M., "Hiding Data in Images by Simple LSB Substitution" Pattern Recognition, Vol. 37, No. 3(2004), pp.469~474**

九、**Khodaei, M., and Faez, K., "New adaptive steganographic method using least-**

significant-bit substitution and pixel-value differencing" IET Image Processing, Vol. 6, No. 6(2012), pp. 677~686.

十、Liu, H. H., Su, P. C., and Hsu, M. H., "An Improved SteganographyMethod Based on Least-Significant-Bit Substitution and Pixel-Value Differencing" KSII Transactions on Internet and Information System, Vol. 14, No. 11(2020), pp. 4537~4556.

十一、Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G., "Information hiding-a survey" Proceedings of the IEEE, Vol. 87, No. 7(1999), pp. 1062~1078.

十二、Schurgot, M. R., "Generating Communication Channels to Operate (GeCCO)," Defense Advanced Research Projects Agency, Retrieved from https://www.darpa.mil/program/generating-communication-channels-to-operate, 2008, (2023/7/27).

十三、Wu, D. C., and Tsai, W. H., "A steganographic method for images by pixel-value differencing" Pattern Recognition Letters, Vol. 24(2003),pp.1613~1626.

十四、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" Proceeding of IEE Inst. Elect. Eng., Vis. Image Signal Process, Vol. 152, No. 5(2005), pp.611~615.

十五、Wang, C. M., Wu, N. I., Tsai, C.-S., and Hwang, M.-S., "A high quality steganographic method with pixel-value differencing and modulusfunction" Journal of Systems and Software Vol. 81, No. 1(2008), p.p150-158.

十六、Yang, C. H., Weng, C. Y., Wang, S. J., and Sun, H.-M., "Varied PVD+LSB evading detection programs to spatial domain in data embedding systems" Journal of Systems and Software, Vol. 83, No. 10(2010), pp.1635~1643.

十七、Zhou, W., and Bovik, A. C., "A universal image quality index" IEEE Signal Processing Letters, Vol. 9, No. 3(2002), pp.81~84.

十八、Zhou,W., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P., "Image quality assessment: from error visibility to structural similarity" IEEE Transactions on Image Processing, Vol. 13, No. 4(2004), pp.600~612.

作者簡介

劉興漢，國防管理學院資訊管理系學士、世新大學資管系碩士、國防大學理

工學院國防科學研究所博士，歷經排長、程設官、中隊長、教官、助理教授，目前任職於國防大學管理學院資訊管理學系上校副教授。

許孟華，國防大學管理學院資管系學士、國防大學管理學院資管系碩士，歷經資通電軍資網官、通安官，目前任職於國防部資通電軍指揮部。