植基於邊緣偵測及最佳像素調整之資訊隱藏方法

劉興漢 [1*]　賀盛志 [2]　鄭岳原 [1]

[1] 國防大學資訊管理學系

[2] 德明財經科技大學資訊管理系

論文編號：NM-44-01-05

DOI：10.29496/JNDM.202405_45(1).0002

來稿2022年9月22日→第一次修訂2022年10月3日→第二次修訂2023年3月13日→

同意刊登 2023 年 4 月 10 日

摘要

本研究提出植基於邊緣偵測及最佳像素調整之資訊隱藏方法，首先利用中間邊緣偵測法用來區分目標像素是位於邊緣或是平滑區，據以判定秘密訊息的藏入量，基於人類視覺系統，若目標像素位於邊緣則以最低有效位元取代與最佳像素調整法嵌入較多的秘密訊息，若在平滑區則以相同方法嵌入較少的秘密訊息。實驗中，我們使用 Lena 等 8 張灰階影像進行測試，得到高藏密量且偽裝影像品質良好的效果。此項方法不需複雜的演算過程，透過現行基本的軟硬體設備，即可將機密資訊藏入影像中，並從偽裝影像取出隱藏訊息。此研究可提供國防資訊安全管理研究領域參考應用。

關鍵詞：中間邊緣偵測法、最低有效位元取代法、最佳像素調整法

[*]聯絡作者：劉興漢 email: liu.hansh@gmail.com

An Improved Steganographic Method Based on Median Edge Detection and Optimal Pixel Adjustment Process

Liu, Hsing-Han[1*] Ho, Sheng-Chih[2] Cheng, Yue-Yuan[1]

[1]Department of Information Management, National Defense University, *Taiwan, R.O.C*

[2]Department of Management Information System, Takming University of Science and Technology, *Taiwan, R.O.C*

Abstract

In this study, we propose an improved steganographic method based on median edge detection and optimal pixel adjustment process. At first, the median edge detection predictor distinguishes the target pixels located at the edge or those in the non-edge area, which determines the number of secret embedded data for each target pixel. According to the concept of human vision system, if the target pixel is located at the edge, the predicted value of the target pixel embeds more secret bits via the least-significant-bit substitution and optimal pixel adjustment process method. Contrarily, if the target pixel is located in the non-edge area, it embeds fewer secret bits via the same method. In this experiment, the modified method achieves a high capacity with better stego-image quality by using 8 grayscale images such as Lena, etc. This method does not require complex computational processes, but uses existing basic hardware and software to hide confidential information in the image and retrieve the hidden information from the stego-image. This study can provide reference applications in the field of defense information security management research.

Keywords: Median Edge Detection, Least-Significant-Bit Substitution, Optimal Pixel Adjustment Process

[*]Corresponding author: Liu, Hsing-Han email: liu.hansh@gmail.com

一、前言

通訊技術與生活便利性息息相關，愈新的通訊技術，在相同的時間內可以傳送愈多的資料量。若有適當的軟硬體配合，時間與空間對通訊終端方在事物的受用上，造成的限制亦隨之降低，學習、工作與生活的整體效率會隨之增加，相較過往通訊不便，現行通訊技術提升及行動網路普及，人們傳遞訊息所使用之文字、圖片、聲音、影片等傳輸媒介亦都數位化，數位資料的傳遞需求也隨之提高，然而當數位資料用來傳遞訊息愈便利，卻也增加了訊息內容遭惡意人士偽造、竊取的風險。因此，將傳遞之訊息「加密」或「隱藏」以確保數位資料傳遞之正確性、安全性，成為了值得探討研究之議題。訊息之「加密」或「隱藏」最大的不同：訊息「加密」是將要傳遞的原始資料「明文」，透過加密轉變為「密文」，將傳遞的訊息隱藏起來；而訊息「隱藏」則是將要傳遞的原始資料，運用方法或技術，儘可能使人無法察覺傳遞出去的訊息中，藏有真正要傳達的隱藏訊息(王旭正與柯宏叡，2006)。資料加密，如欲破解一份密文則必須去破解出其原始加密時所用之金鑰，才能取得原始之明文；但是對於資訊隱藏，其功能或原始意義不需被完全理解，只要隱藏之訊息被察覺，且被證明其存在，便是被破解(張凱崴，2013)。

資訊隱藏技術或可稱之為藏密學，於歷史上可說是五花八門，主要表達訊息中還有著「隱藏訊息」(王旭正等，2012)。歷史上，最早記載是在西元前五世紀，古希臘作家希羅多德(Herodotus)的著作史書(Histories)中提到，古希臘的統治者希斯提奧斯(Histiaus)，其將信任的奴隸頭髮剃光後，在奴隸頭皮上刻印祕密訊息，等到奴隸頭髮長出來，才派遣奴隸至目的地，此時對方只要把奴隸的頭髮剃光，即可得到被隱藏的秘密訊息，藉此傳達軍事訊息(婁德權，2006)。其他在軍事領域上運用資訊隱藏的案例，如傳送方使用隱形墨水，將軍隊動向、攻擊標的等重要軍事訊息，寫在信紙上，在不被敵人發現的狀況進行訊息傳遞，接收方透過將信紙加熱後，就能取得秘密訊息，隱形墨水是利用果汁、醋、牛奶等成分的化學變化來完成資訊隱藏目的；第二次世界大戰時，德國人將作工精細的微縮照片藏匿在普通訊息字句的標點符號內，藉此多次成功傳達軍事機密訊息。資訊隱藏應用方法多而廣泛，全取決於使用者的智慧及變化，隨著數位化時代到來，數位資料普及後，資訊隱藏技術亦被運用在確保數位資料傳輸之安全性。

資訊隱藏藉由通訊載體以達成嵌密之目的，其透由文字、影像、音訊、影片等數位傳輸媒介進行嵌密，現有研究提出嵌密於網路協定(network protocol)、DNA 等載體進行資料傳輸，但其中影像是最受歡迎也最常被使用的載體(Hussain et al., 2018)。數位影像具有下列優點：(一) 常見且取得容易；(二) 結構簡單易懂，可塑性極高；(三) 影像具成熟分析檢查技術，在數位影像上評估影像失真性是很容易的事情(吳南益等，2010)。資訊隱藏技術把秘密訊息嵌入掩護影像(cover image)之中，產生隱含機密訊息的偽裝影像(stego-image)，藉此避免秘密訊息被惡意者發現，以完成秘密通訊，其原理在於透過調整掩護影像的像素，將秘密訊息嵌入影像像素中，因為人類的視覺系統(Human Vision System; HVS)對影像微小的差異，幾乎無法察覺，藉此達到在不被惡意人士注意下，傳遞秘密訊息。

資訊隱藏的初衷不同於傳統密碼學，目標在於不被竊取者發現數位載體上藏有秘密

訊息，並根據資訊隱藏目的、技術，有以下特性：不可察覺性(imperceptibility)、強韌性(robustness)、安全性(security)、不可偵測性(undetectability)、效率性(efficiency)、高隱藏容量(high capacity)。一個安全又可靠的資訊隱藏技術，主要特性為以下三點：(一)不可察覺性：藏密過的數位資料不產生明顯之品質變化，符合人類視覺系統的特性狀態下，難以被人類感官所察覺。(二)高隱藏容量：資訊隱藏之目的，就是要在數位資料中藏入愈多秘密訊息。(三)強韌性：經過資訊隱藏的數位資料，須能被常見之非惡意方法處理後，隱藏資訊仍存在數位資料中，不會遭移除。(左豪官等，2007；陸哲明，2014)在各種特性間取得最佳平衡，儘可能發展同時滿足上述特性之資訊隱藏方法，是學者們持續努力的方向，也是最大的挑戰。

本研究將運用中間邊緣偵測法(Median Edge Detection; MED)預測掩護影像像素是否為邊緣，再以最低位元取代法(Least Significant Bit Substitution; LSB Substitution)結合最佳像素調整法(Optimal Pixel Adjustment Process; OPAP)的方式，將秘密訊息藏入掩護影像，本文之研究貢獻條列如下：

1. 軍事情資能在無人察覺的狀況下，安全地進行傳輸。
2. 實現一種具安全性、高藏密量、藏密過程不需複雜運算，並維持人類視覺可接受的影像品質之數位影像資訊隱藏技術。

本研究藏密方法最大可藏入 4.6bpp，且 PSNR 與 SSIM 值均位於人類視覺無法察覺之範圍，證明本研究藏密方法能有效提升藏密量，並維持一定的影像品質。

二、文獻探討

2.1 最低有效位元取代法

Bender et al.(1996)提出最低有效位元取代法，這個方法通常是研究空間域的資訊隱藏技術時，最先接觸到的一種方法。此概念是利用單個像素值當中最低的位元訊息，如圖 1 所示，直接嵌入秘密訊息，此作法對影像品質影響最小，因為人眼對微小差異無法察覺，此藏密法除操作容易外，也能滿足低處理效率的設備。但其缺點在於若欲增加藏密量，用來隱藏資料的位元數就必須增加，嵌入過多的秘密訊息時，會造成影像的失真，進而引起竊取者的注意。

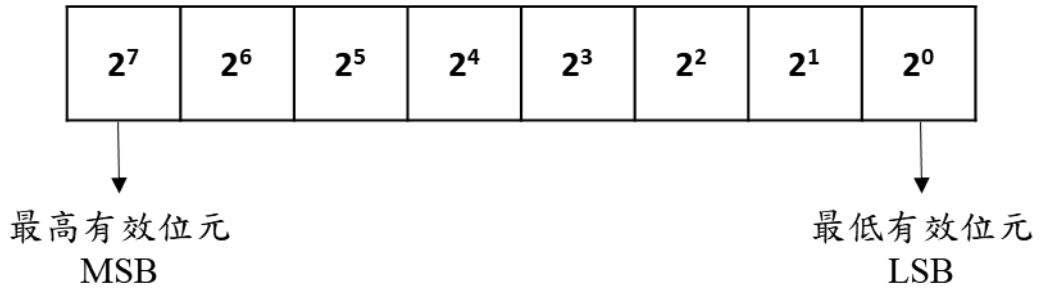


圖 1 像素值的二進位表示圖
資料來源：Chan and Cheng(2004)

以實際範例說明最低有效位元取代法，如圖 2 所示，掩護影像 C 為 2×2 之灰階影像，欲在 C 內嵌入$(11100100)_2$ 共計 8 個位元的秘密訊息 S，因為掩護影像 C 總共有 4 個像素，第一步先將 S 平均分割成 4 等份為 $s_1=(11)_2$、$s_2=(10)_2$、$s_3=(01)_2$、$s_4=(00)_2$，接續分別將 s_1、s_2、s_3、s_4 與掩護影像 C 中 4 個像素內的最低 2 個位元進行替換，完成取代程序後，原本掩護影像 C 的像素(128, 207, 227, 241)，調整成偽裝影像 C'的像素值為(131, 206, 225, 240)，即完成藏密程序，並得到已嵌入秘密訊息 S 的偽裝影像 C'。

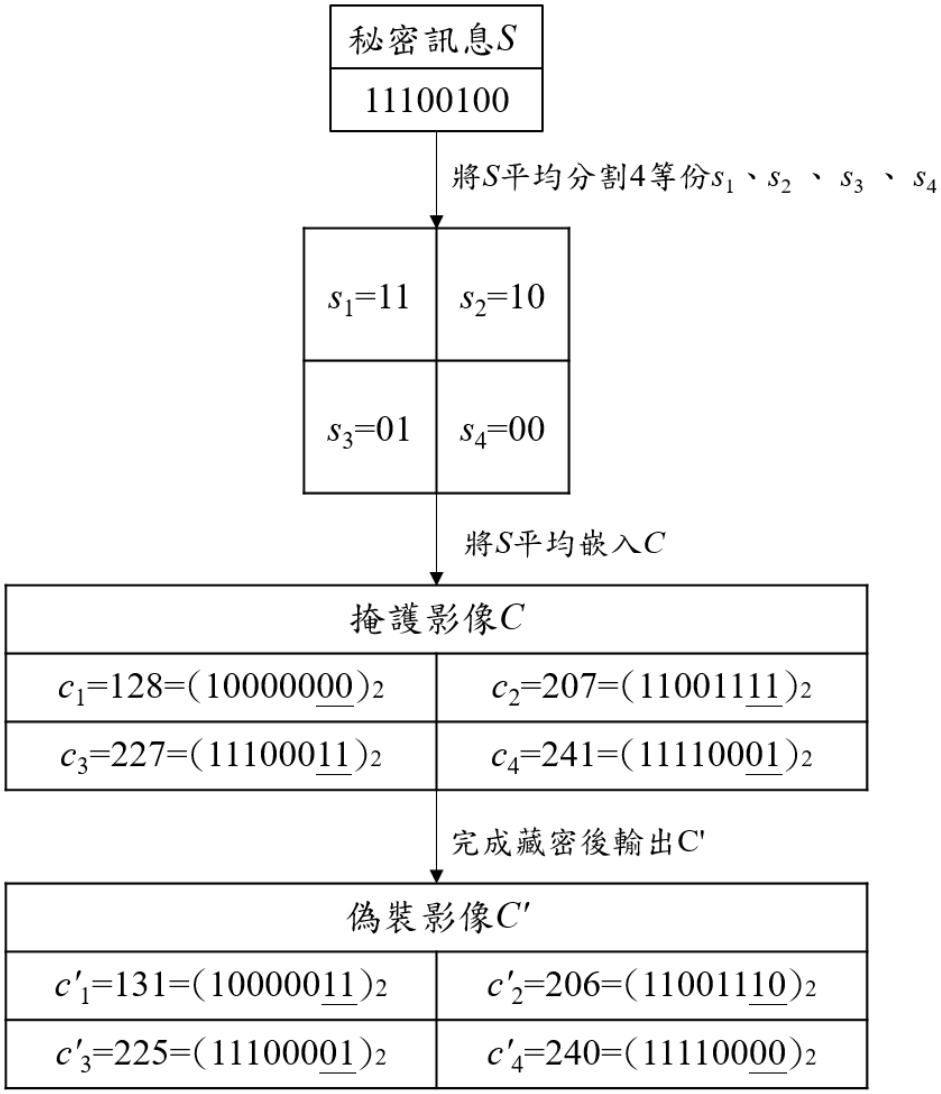


圖 2 最低有效位元取代法藏密步驟示意圖

將上述最低有效位元取代法以方程式來表示，假設 c_i 為掩護影像中其中一個像素值，s_i 為 S 之中一小段 k 位元的祕密訊息，此時要將 k 位元來嵌入 c_i 中，嵌入 k 位元後新像素值為 c'_i，上述嵌密的過程可以用公式(1)來表示：

$$c'_i = c_i - (c_i \ mod \ 2^k) + s_i \tag{1}$$

相反地，取密前只要知道嵌入的位元長度 k 為何，即可從 c'_i 取出秘密訊息 s_i，以公式(2)來表示如下：

$$s_i = c'_i \ mod \ 2^k \tag{2}$$

2.2 最佳像素調整法

Chan and Cheng(2004)提出基於 LSB 的改良方法，最佳像素調整技術，運用在影像經過 LSB 取代法後進行修正，藉由位元置換階層的調整，使像素差值最佳化，在嵌入相同藏密量的狀況下，獲得較佳影像品質，改善偽裝影像失真度。

假設秘密訊息 S，要將 k 位元嵌入掩護影像 C，嵌入後得到偽裝影像為 C'。而 c_i 為掩護影像 C 之像素值，c'_i 為利用 LSB 取代法嵌入秘密訊息後的像素值。另假設 d 為 c'_i 與 c_i 的差值，計算出 d 後，依據 d 的值可以區分三個區間，每個區間符合的條件都不相同，經過調整後得到 c''為經過最佳化調整後之像素值，三個區間分別如下：

區間一：$2^{k-1} < d < 2^k$，若$c'_i \geqq 2^k$則$c''_i = c'_i - 2^k$，否則$c''_i = c'_i$。

區間二：$-2^{k-1} \leq d \leq 2^{k-1}$，$c''_i = c'_i$。

區間三：$-2^k < d < -2^{k-1}$，若$c'_i < 256 - 2^k$則$c''_i = c'_i + 2^k$，否則$c''_i = c'_i$。

以實例說明 OPAP 的調整技術，如圖 3 所示，假設掩護影像 C 中某一像素值 c=168，轉換為二進位為 c=$(10101000)_2$，在這個像素中嵌入 k 為 3 位元之秘密訊息 S=$(111)_2$，得到新像素值 c'=$(10101111)_2$=175，此時計算兩個像素差值 d= c'-c=175-168=7，從上述 OPAP 調整區間可以判斷適用於區間一，且因為 c'=175≥2^3，得到經過最佳調整化過後的像素值 c''= $c' - 2^k$=175-8=167=$(10100111)_2$。原本 c'與 c 像素差值 d 為 7，經 OPAP 方法調整後 c'與 c 像素差值 d'減少為 1，進而提升偽裝影像品質。

反之，OPAP 方法的取密過程，只要藉由公式(2)之 LSB 取密方法即可完成。例如，調整後新像素值 c''為 167，利用公式(2)可以得到秘密訊息 S=167 mod 2^3＝7＝$(111)_2$，即為原本欲藏入 k=3 之秘密訊息 S。

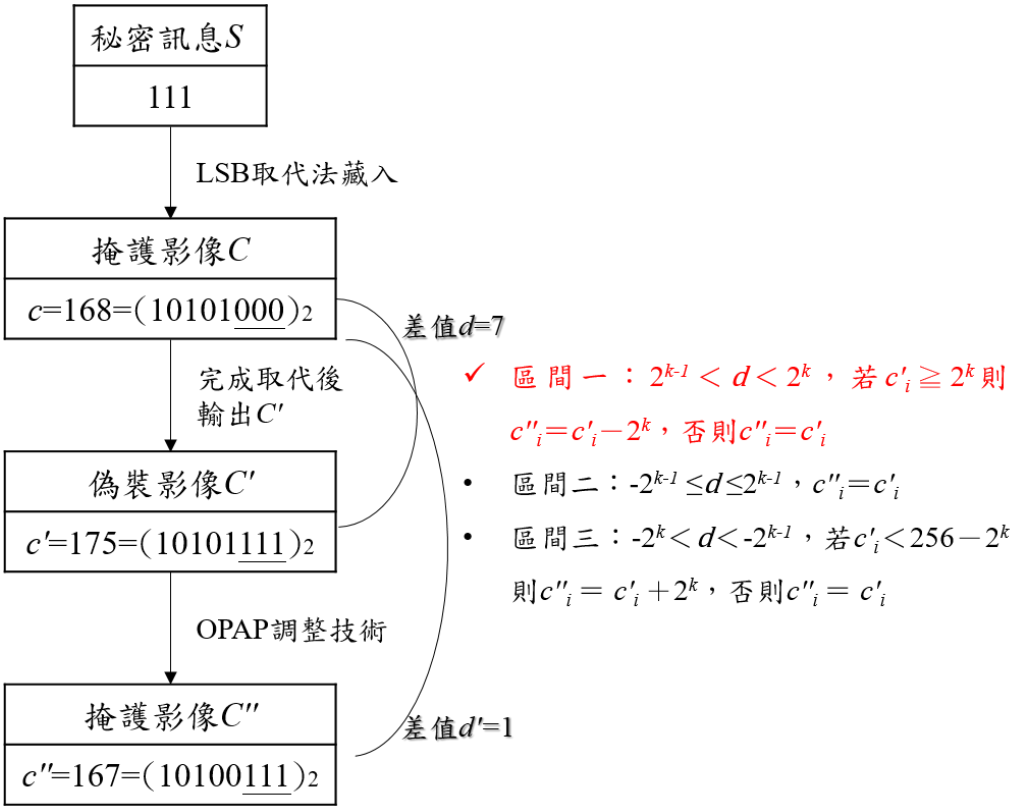


圖 3 最低有效位元取代法藏密步驟示意圖

2.3 中間邊緣偵測法

Martucci(1990)提出中間邊緣偵測法來預測像素的預測方法，該方法在邊緣明顯的影像中有較好的預測效果(Weinberger et al., 1996)。MED 每次進行預測時皆以 2×2 之區塊進行預測，假設預測像素值為 x，與 x 之相鄰像素值分別為 a 以及 b，非相鄰之像素值為 c，如圖 4 所示，預測值的計算如公式(3)說明，其中 $p(x)$為像素值之預測計算式，依像素值 c 符合判斷之狀況，選擇適合的運算式。

c	b
a	x

圖 4 預測像素 x 與其相鄰像素示意圖
資料來源：Weinberger et al.（1996）

$$p(x)=\begin{cases} min(a,b), if & c \geq max(a,b) \\ max(a,b), if & c \leq min(a,b) \\ a+b-c, & otherwise \end{cases} \quad (3)$$

Martucci 的方法預測效果很好，因此有許多研究都是以它為基礎(呂慈純等，2014)，本研究在預測部分亦採用 Martucci 提出的方法，判斷目標像素是否位於邊緣：若 $c \geq \max(a,b)$或 $c \leq \min(a,b)$，則 x 屬邊緣，否則為非邊緣，並稱之為平滑區。

2.4 改良後的中間邊緣偵測法

冷輝世等學者於 2013 年提出保留邊緣特性之改良後的中間邊緣偵測法(MMED)，假設在原始影像中 a、b、c 為目標像素 x 的鄰近像素(如圖 4 所示)，對於個別的影像特徵可找到一個門檻值 T，使其預測值在非邊緣區時更為準確，其預測值計算如公式(4)之說明。

$$p(x)=\begin{cases}\min(a,b), if\ \ c\geq\max(a,b)\\ \max(a,b), if\ \ c\leq\min(a,b)\\ \dfrac{a+b+c}{3}, \quad c\in(a,b), \left|c-\dfrac{a+b}{2}\right|<T, \quad T\in N\\ a+b-c, \quad otherwise\end{cases} \tag{4}$$

在公式(4)的計算過程中，先判斷目標像素是否位於邊緣或非邊緣區，如果 c 與 $(a+b)/2$ 的差小於個別影像特徵找到的門檻值 T，則預測值可設為 $(a+b+c)/3$，其餘預測值的設定與原始 MED 方法相同。修改後的 MMED 預測值經實驗證明，可準確判斷目標像素的特性，進而增加其資訊隱藏的容量。

2.5 藏密技術衡量標準

好的資訊隱藏技術通常需滿足安全性、不可察覺性、高藏密量等特性，但藏密影像品質與藏密量通常難以兼顧，當影像藏密量越大對其品質破壞也越大，因此在藏密影像品質與藏密量尋求最佳平衡點，成為資訊隱藏領域重要的研究議題，其中藏密量 bpp(Bit Per Pixel)表示每一像素值可藏入多少位元數，如公式(5)說明。接續將就峰值訊號雜訊比(Peak Signal to Noise Ratio, PSNR)與結構相似性指標(Structural Similarity Index Measure, SSIM) 2 種量化之衡量標準進行介紹。

$$bpp=\frac{Maximal\ \ Embedding\ \ bits}{m\ \times\ \ n} \tag{5}$$

公式(5)中的 m 與 n 分別代表受測影像的長與寬(單位為 pixel)。

2.5.1 峰值訊號雜訊比

Zhouc and Bovik(2002)提出一種對於影像品質的客觀判斷標準，以均方差(Mean Square Error, MSE)及峰值訊號雜訊比作為判定工具，均方差計算如公式(6)。

$$MSE=\frac{\sum_{i=1}^{m\times n}(C_i-C'_i)^2}{m\times n} \tag{6}$$

m 及 n 分別為影像之長、寬，於公式中相乘的分母表示影像之總像素值；C_i為掩護影像中的一個像素值、C'_i為掩護影像嵌密後的像素值，C_i與C'_i如果相差愈大，得到的均方差就愈大，表示掩護影像與嵌密後的影像差異愈大，愈容易被發現；反之，MSE 愈小、愈趨近於零，代表嵌密後的影像品質愈好、不可察覺性愈高。然而 MSE 將影響 PSNR 的值，其計算如公式(7)所示。

$$\mathrm{PSNR} = 10 \times \log\left(\frac{255^2}{MSE}\right) \quad (7)$$

一般灰階影像像素值以 8 位元表示，公式(7)中的 255 為灰階影像中最大的像素，倘若上述 MSE 的值愈小，PSNR(單位為 dB)就愈高，通常來說，人類的視覺在影像 PSNR 超過 30dB 時，就看不出藏密前後之差異性(陸哲明，2014)；PSNR 值小於 30dB 時，表示人類視覺看起來不能忍受的範圍，因此大部分 PSNR 值皆要大於 30dB，但 PSNR 值越高，不代表影像品質一定好，仍必須靠人的肉眼輔助來判斷影像的品質(王旭正等，2016)。

以圖 5 實例說明 PSNR 值大小與影像品質關係，圖 5(a)為 Lena 影像原圖、圖 5(b)為 Lena 影像 PSNR 值為 54.6dB 圖、圖 5(c)為 Lena 影像 PSNR 值為 31.02dB 圖、圖 5(d)為 Lena 影像 PSNR 值為 22.16dB 圖，圖 5(a)Lena 原圖與圖 5(b) Lena 影像 PSNR 值為 54.6dB 之圖相較之下，難以察覺差異，但當影像由左至右、PSNR 值愈來愈低，圖 5(c)及圖 5(d)影像以人眼即可察覺愈來愈顯粗糙。

(a)原圖

(b) PSNR:54.6dB

(c) PSNR:31.02dB

(d) PSNR:22.16dB

圖 5 PSNR 值實例影像圖

2.5.2 結構相似性指標

PSNR 值判定未列入人眼視覺特性，人眼對空間、亮度、區域對比度敏感度亦會影響感受，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 值判定結果與人眼主觀感受分歧的情況，自然影像是高度結構化的，亦即在自然影像相鄰像素之間有很強之關聯性。

因此 Zhou Wang et al.(2004)提出另一種符合人體直覺的影像質量評價標準，用以衡量 2 張數位影像相似程度之量化標準，稱結構相似性指標，主要測量掩護影像和偽裝影像之間結構相似大小，其值介於 0 到 1 之間，值愈大表示兩張影像的相似度愈高，SSIM 為 1 時，表示 2 張數位影像完全一致，SSIM 大於或等於 0.98 時，表示 2 張數位影像難以分辨，而 SSIM 為 0.95 時，表示大多數人對畫面看起來滿意，此數值可以視為及格的畫面，SSIM 為 0.9 時，表示瑕疵可能較 SSIM 為 0.95 時多一倍，人眼可察覺到明顯的畫面劣化。分別從公式(8)之影像亮度、公式(9)之對比度、公式(10)之結構等三方面度量影像相似性，而 SSIM 值計算方式如公式(11)所示。

$$l(x,y)=\frac{2\mu_x\mu_y+c_1}{\mu_x^2+\mu_y^2+c_1} \tag{8}$$

$$c(x,y)=\frac{2\sigma_x\sigma_y+c_2}{\sigma_x^2+\sigma_y^2+c_2} \tag{9}$$

$$s(x,y)=\frac{\sigma_{xy}+c_3}{\sigma_x\sigma_y+c_3} \tag{10}$$

$$SSIM=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{11}$$

其中，μ_x 及 μ_y、σ_x 及 σ_y 分別為 x 和 y 的平均值和標準差，σ_{xy} 為 x 和 y 的共變異數，c_1、c_2、c_3 皆為常數，用以維持$l(x,y)$、$c(x,y)$、$s(x,y)$的穩定。

三、研究方法

本研究利用 Martucci 學者提出的 MED 概念進行影像像素預測，每次預測以 2×2 個像素單位區塊進行預測，直接依照像素目標位置預測為邊緣或平滑區決定藏入量，若像素目標位置預測為邊緣，則藏入較多秘密訊息，若像素目標位置預測為平滑區，則藏入較少的秘密訊息，期藉以提升藏密效率，另為避免單純使用 LSB 取代法藏密後之偽裝影像具明顯特徵，可被現今許多藏密分析方法有效偵破，為了保有安全性，藉由 LSB 取代法結合 OPAP 調整法，調整像素差值，提高影像品質並改善偽裝影像失真度，進而取得偽裝影像，並能具有良好的抵抗藏密偵測之能力，本研究方法設計傳送概念圖如圖 6。

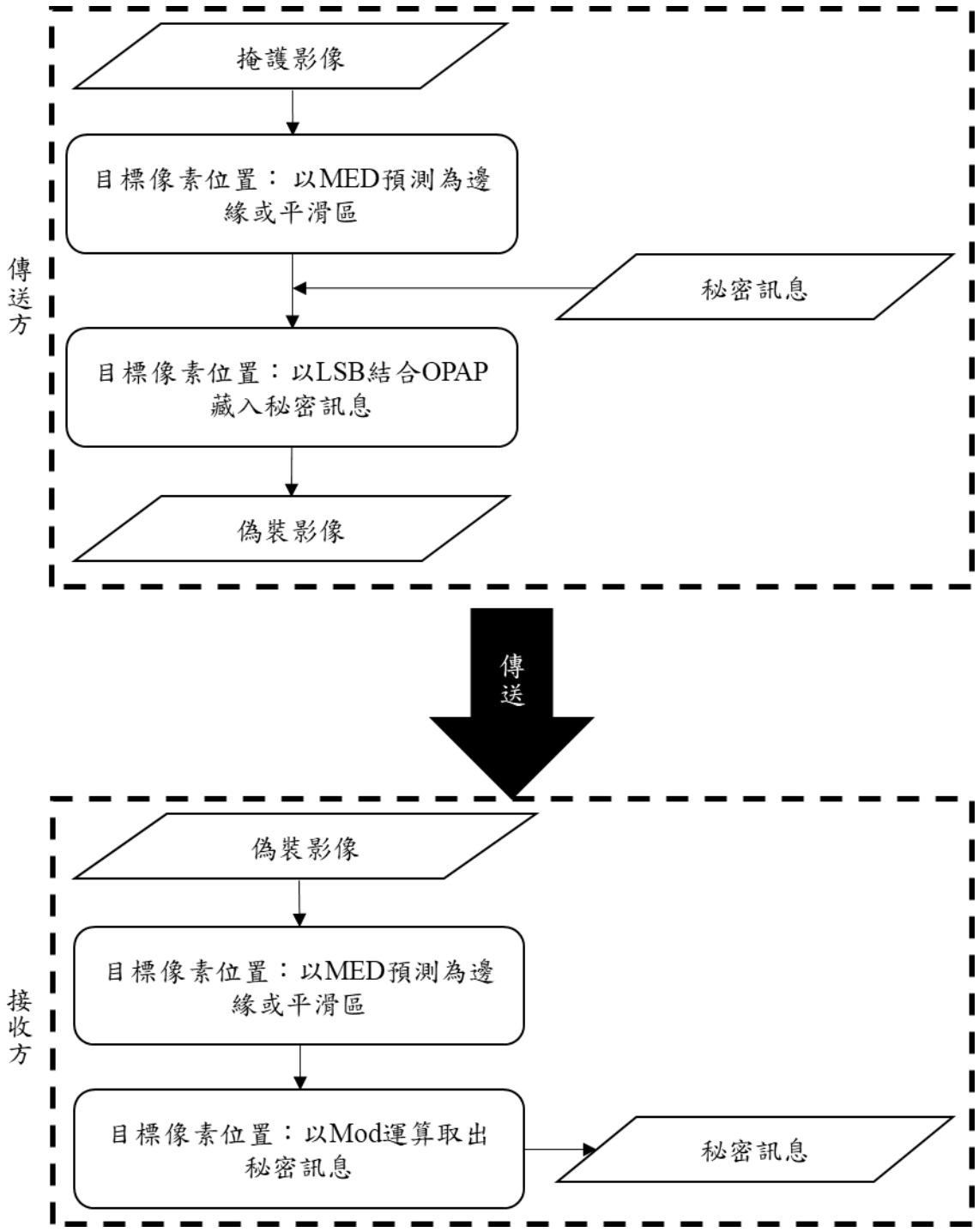


圖 6　本研究方法設計傳送概念圖

3.1 本研究方法之藏密程序

步驟一：以 512×512 大小之灰階影像 C 作為掩護影像，第一行與第一列中各 512 個像素作為參考值，均不藏入秘密訊息(如圖 7 斜線部分)。

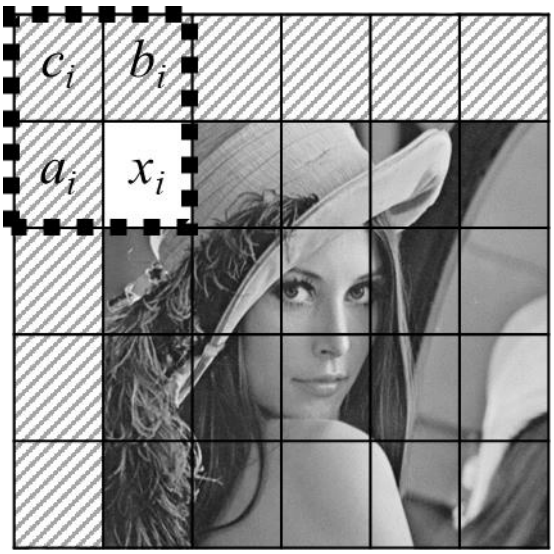


圖 7 掩護影像目標像素值位置示意圖

步驟二：除了步驟一之斜線部分作為參考值，如圖 7 所示，針對每一像素值，每次以 2×2 像素作為單位區塊進行邊緣預測，如圖 7 黑色粗體虛線框所示，以公式(12)判斷目標像素位置 x_i 屬邊緣或是平滑區，a_i 為目標像素位置 x_i 相鄰左側，b_i 為目標像素位置 x_i 相鄰上側，c_i 為目標像素位置 x_i 左上角相鄰位置。若 c_i 值大於或等於 a_i 與 b_i 的最大值，或 c_i 值小於或等於 a_i 與 b_i 的最小值，則目標像素位置 x_i 為邊緣，若 c_i 值介於 a_i 或 b_i 值之間，則目標像素位置 x_i 為平滑區。

$$c_i \geq max(a_i, b_i) \text{ or } c_i \leq \min(a_i, b_i) \tag{12}$$

步驟三：若目標像素位置 x_i 判定為邊緣(平滑)區塊，以公式(13)分別將目標像素位置 x_i 以 LSB 取代法藏入 k 位元秘密訊息(判定為邊緣區塊)或 k-1 位元秘密訊息(判定為平滑區塊)，而 s_i 為藏入秘密訊息之十進位值，亦會隨邊緣(平滑)區塊進行調整。

$$x'_i = x_i - (x_i \ mod \ 2^k) + s_i \tag{13}$$

步驟四：目標像素 x_i 以 LSB 取代法藏入後，以公式(14)計算目標像素 x'_i 與原本像素之差值d_i。

$$d_i = x'_i - x_i \tag{14}$$

步驟五：使用公式(15) 進行 OPAP 調整，針對 LSB 取代法藏入後目標像素位置 x'_i，得到目標像素位置 x''_i 。

$$x''_i = \begin{cases} x'_i + 2^k, if\ -2^{k-1} > d_i > -2^k \ and\ x'_i < 256 - 2^k \\ x'_i - 2^k, if\ 2^k > d_i > 2^{k-1} \ and\ x'_i \geq 2^k \\ x'_i\ , otherwise \end{cases} \quad (15)$$

步驟六：當單位區塊完成邊緣預測及秘密訊息嵌入後，整個黑色粗體虛線框向右位移 1 個像素，如圖 8 所示，進行下一個新的目標像素位置的邊緣預測及祕密訊息嵌入，以此類推，第一列執行完畢後，以 Z 字型方式換第二列類推，依序藏入秘密訊息，直至沒有下一個新的目標像素位置為止，即可獲得偽裝影像。

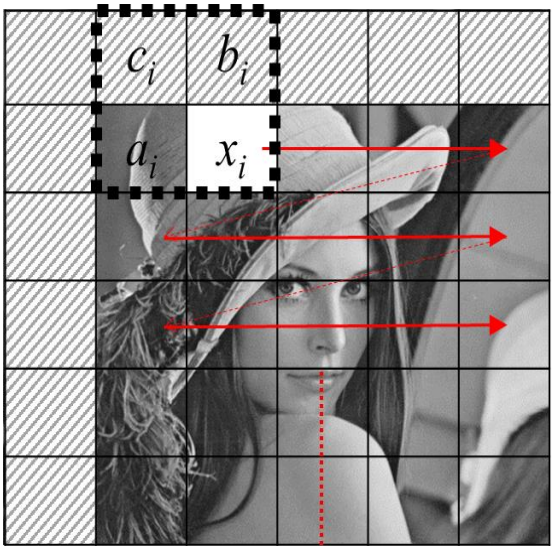


圖 8 掩護影像目標像素值位置位移示意圖

本研究方法藏密流程圖如圖 9 所示，因掩護影像為 512×512 之二維陣列，本研究提出之演算法須利用 2 層 for 迴圈控制其列與行之索引值，且第一列與第一行像素為 MED 預測保留區，故不列入計算，故其藏密演算法時間複雜度為 O(n^2)，其中 n 為影像之列(行)數。

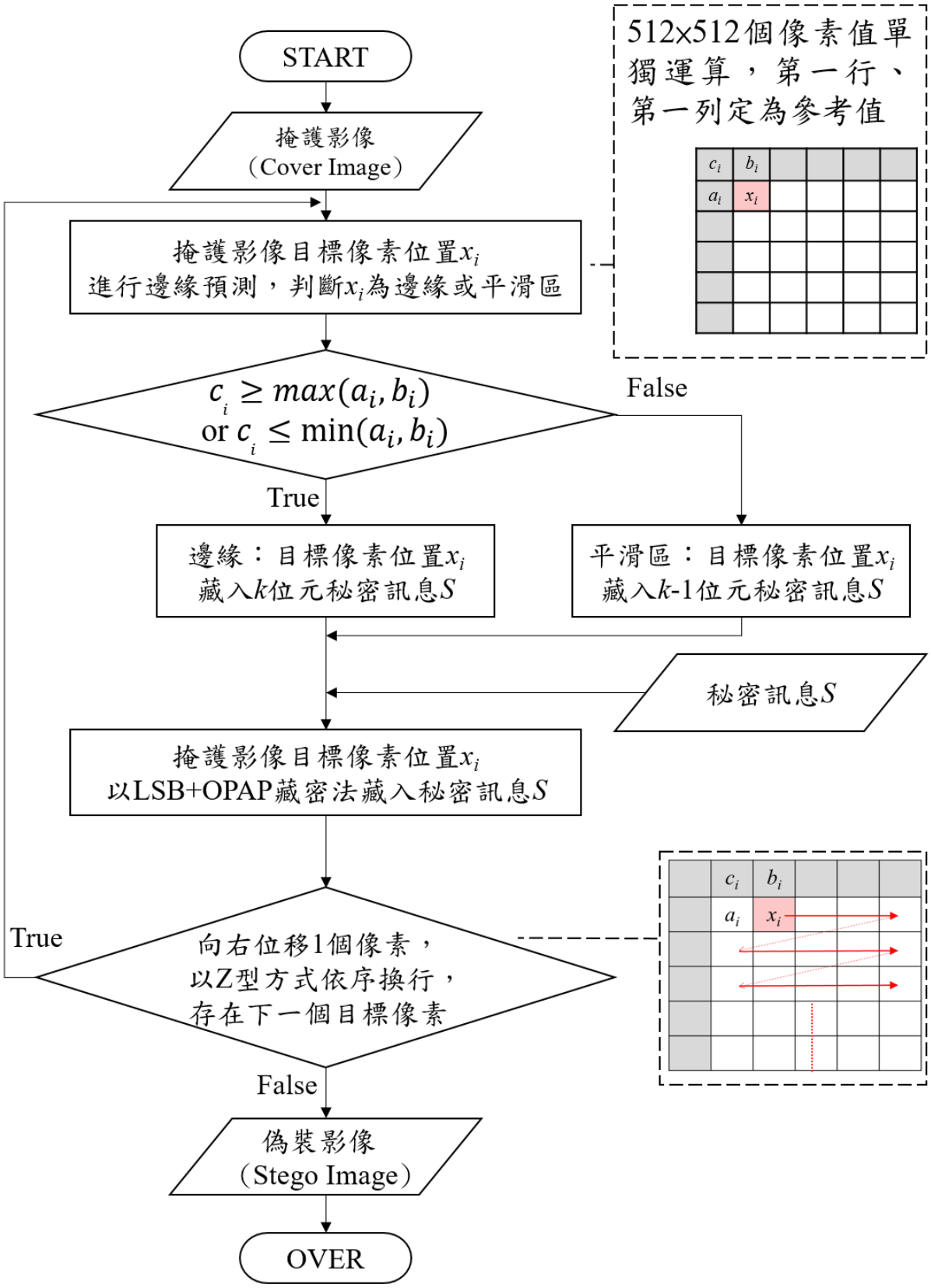
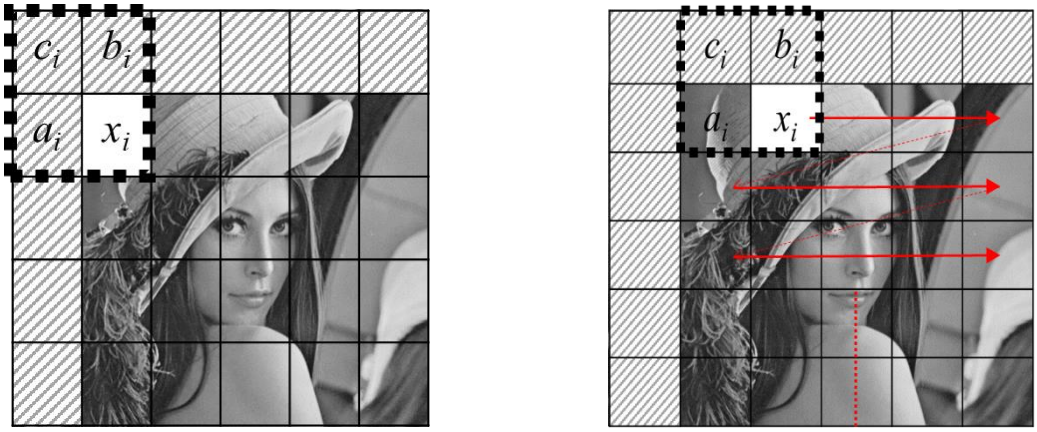

START
掩護影像
（Cover Image）
掩護影像目標像素位置x_i
進行邊緣預測，判斷x_i為邊緣或平滑區
512x512個像素值單獨運算，第一行、第一列定為參考值
c_i
b_i
a_i
x_i
$c_i \geq max(a_i, b_i)$
or $c_i \leq \min(a_i, b_i)$
False
True
邊緣：目標像素位置x_i
藏入k位元秘密訊息S
平滑區：目標像素位置x_i
藏入k-1位元秘密訊息S
秘密訊息S
掩護影像目標像素位置x_i
以LSB+OPAP藏密法藏入秘密訊息S
向右位移1個像素，
以Z型方式依序換行，
存在下一個目標像素
True
False
偽裝影像
（Stego Image）
OVER

圖 9 本研究藏密流程圖

3.2 本研究方法之取密程序

步驟一：藏密後之偽裝影像中，第一行與第一列中之各 512 個像素作為參考值，均不取出秘密訊息(如圖 10(a)斜線部分)。



(a) (b)

圖 10 偽裝影像目標像素值位置與位移示意圖

步驟二：除了步驟一之斜線部分作為參考值，如圖 10(a)所示，針對每一像素值，每次以 2×2 像素作為單位區塊進行邊緣預測，如圖 10(a)黑色粗體虛線框所示，以公式(12)判斷目標像素位置 x_i 屬邊緣區或是平滑區，a_i 為目標像素位置 x_i 相鄰左側，b_i 為目標像素位置 x_i 相鄰上側，c_i 為目標像素位置 x_i 左上角位置。若 c_i 值大於或等於 a_i 或 b_i 的最大值，或 c_i 值小於或等於 a_i 或 b_i 的最小值，則目標像素位置 x_i 為邊緣區，若 c_i 值介於 a_i 或 b_i 值之間，則目標像素位置 x_i 為平滑區。

步驟三：若目標像素位置 x'_i 判定為邊緣(平滑)區塊，以公式(16)分別將目標像素位置x'_i以模運算取出 k 位元秘密訊息(判定為邊緣區塊) 或 k-1 位元秘密訊息(判定為平滑區塊) ，而取出之 s_i 為藏入秘密訊息之十進位值。

$$s_i = \begin{cases} x'_i \bmod 2^k, if\ x'_i\ is\ located\ at\ the\ edge \\ x'_i \bmod 2^{k-1}, if\ x'_i\ is\ located\ in\ the\ non-edge\ area \end{cases} \quad (16)$$

步驟四：當單位區塊完成邊緣預測及秘密訊息取出後，整個黑色粗體虛線框向右位移 1 個像素，如圖 10(b)所示，進行下一個新的目標像素位置的邊緣預測及祕密訊息取出，以此類推，第一列執行完畢後，以 Z 字型方式換第二列類推，依序取出秘密訊息，直至沒有下一個新的目標像素位置為止，即可獲完整秘密訊息 S。

本研究方法之取密流程圖如圖 11 所示，因藏密影像為 512x512 之二維陣列，本研究提出之取密演算法須利用 2 層 for 迴圈控制其列與行之索引值，且第一列與第一行像素為 MED 預測保留區，故不列入計算，故其藏密演算法時間複雜度為 O(n^2)，其中 n 為

藏密影像之列(行)數。

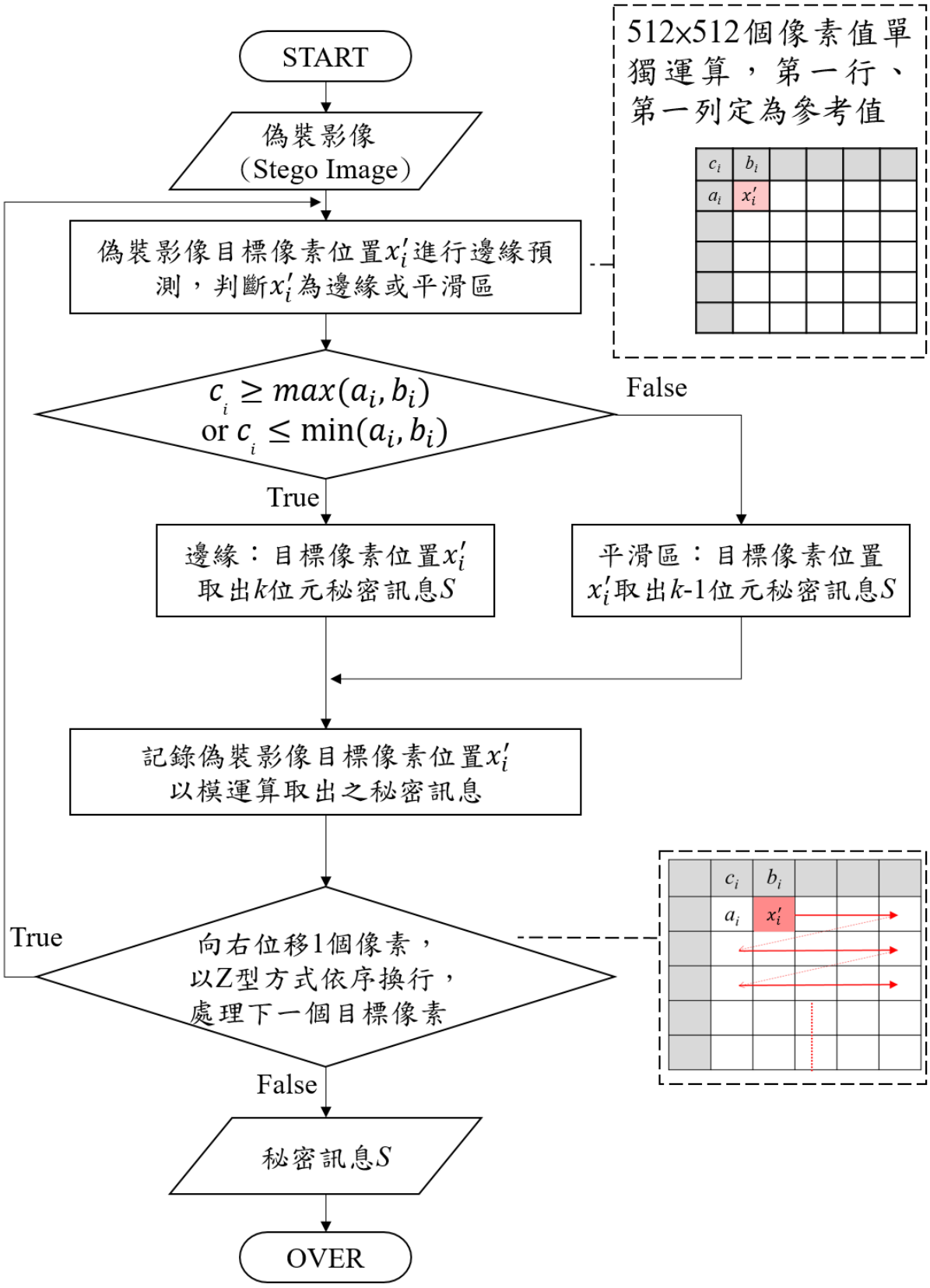


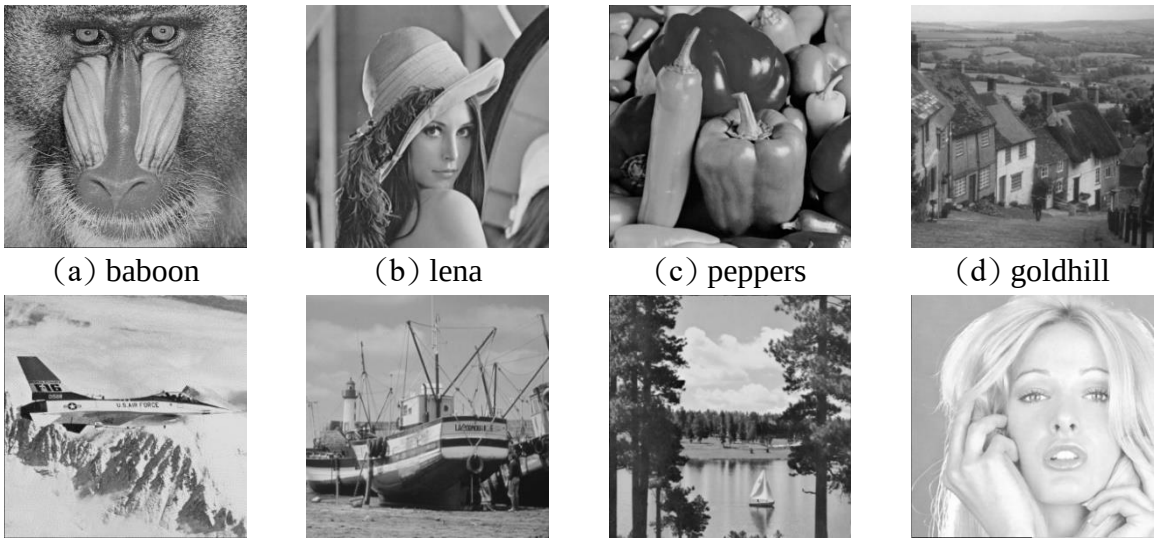
圖 11 本研究之取密流程圖

四、實驗結果與討論

4.1 實驗環境與素材

本研究使用筆記型電腦，作業系統為 MacOS 12.2.1、CPU Intel Core i5 2.0 GHZ，記憶體 16GB，以 Python 程式語言運用 Anaconda 中 Jupyter 進行程式撰寫，以驗證本研究提出的藏密及取密過程之正確性；並使用桌上型電腦，作業系統為 Windows 10、CPU Intel Core I5-6500 3.2 GHz，記憶體 16GB，採用 Matlab 進行安全性測試。

實驗過程運用資訊隱藏領域經常被廣泛使用之 Baboon 等 8 張 512×512 灰階測試影像為掩護影像(如圖 12)；其中包含紋理複雜影像及平滑影像，亦包含人像、風景照、物品及交通工具等影像，可用以代表大部分數位影像之內容。本研究嵌入的機密訊息以隨機亂數 0 或 1 的字串組成，實驗結果以藏密量、峰值訊號雜訊比(PSNR)及結構相似性指標(SSIM)作為衡量標準。



(a) baboon (b) lena (c) peppers (d) goldhill

(e) airplane (f) boat (g) lake (h) tiffany

圖 12 本研究使用之測試影像圖

4.2 實驗結果分析

實驗結果如表 1 所示，經對比 OPAP 藏密法及本研究所提出之藏密方法，在相同的圖片狀況下，OPAP 法僅能藏入 4bpp，本研究藏密方法最大可藏入 4.6bpp，且 PSNR 值均在人類視覺能夠忍受的範圍，證明本研究藏密方法能有效提升藏密量，並維持一定的影像品質。與近年 Liu 等學者於國際期刊所發表之高藏入量藏密法進行比較中，PVD 藏密法平均藏入量為 1.6bpp、平均 PSNR 值為 40.30dB，本研究藏密方法中，在 PSNR 值相當的狀況下，可藏入 2.7bpp(藏入值 k 為 3)；新式 LSB/PVD 藏密法平均藏入量為 3.1bpp、平均 PSNR 值為 37.16dB，本研究藏密方法中，在 PSNR 值相當的狀況下，可藏入 3.7bpp(藏入值 k 為 4)；以及 LSB/MPVD 藏密法平均藏入量為 3.7bpp、平均 PSNR 值為 34.84dB，本研究藏密方法中，在藏入量相當的狀況，平均 PSNR 值為 36.02(藏入值 k 為 4)。本研究所提之藏密方法產生之實驗結果與各方法比較值均較優，證明本研究藏密方法不只能維持較高的藏密量，同時能擁有較佳的影像品質。

表 1 本研究與其他方法之偽裝影像藏密量、PSNR 值比較表

測試影像	OPAP		PVD		New LSB/PVD		LSB/MPVD		本研究之方法					
	Chan and Cheng（2004）		Wu and Tsai（2003）		Khodaei and Faez（2012）		Liu et al.（2020）		*k*=5		*k*=4		*k*=3	
	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR
baboon	4	34.79	1.7	36.96	3.4	36.29	3.7	33.93	4.6	30.2	3.6	36.2	2.6	42.09
lena	4	34.84	1.6	41.18	3.1	37.63	3.7	35.35	4.7	30.03	3.7	35.98	2.7	41.85
peppers	-	-	1.6	40.61	3.1	37.97	3.7	34.89	4.7	29.72	3.7	35.86	2.7	41.78
goldhill	-	-	1.6	41.00	3.1	37.55	3.7	35.31	4.6	30.1	3.6	36.14	2.6	42.05
airplane	4	34.83	1.6	40.20	3.1	37.53	3.7	35.33	4.6	30.08	3.7	36.06	2.7	41.89
boat	-	-	-	-	-	-	-	-	4.6	30.1	3.7	36.07	2.7	41.9
lake	4	34.8	1.6	39.71	3.1	36.53	3.7	34.91	4.6	30.1	3.7	36.07	2.7	41.9
tiffany	-	-	1.6	40.89	3.1	37.79	3.7	34.76	4.7	29.57	3.7	35.78	2.7	41.72
average	4	34.81	1.6	40.30	3.1	37.16	3.7	34.84	4.6	29.99	3.7	36.02	2.7	41.9

本研究亦使用結構相似性指標(SSIM)作為衡量標準，SSIM 數值介於 0 至 1，越接近 1，兩影像越像似；如表 2 所示，本研究 k 值為 2,3,4 時，SSIM 值均接近 1，說明本研究藏密方法具有適應性強的特點，因此，偽裝影像和掩護影像之間的差異是微不足道的，雖然 SSIM 值在 k 值為 5 時差異較大，但在比較簡單的 Lena 圖和複雜的 Baboon 影像中，仍可存入穩定的藏密值，因此無論簡單或是複雜的影像，本藏密方法均能提供良好的藏密效果。

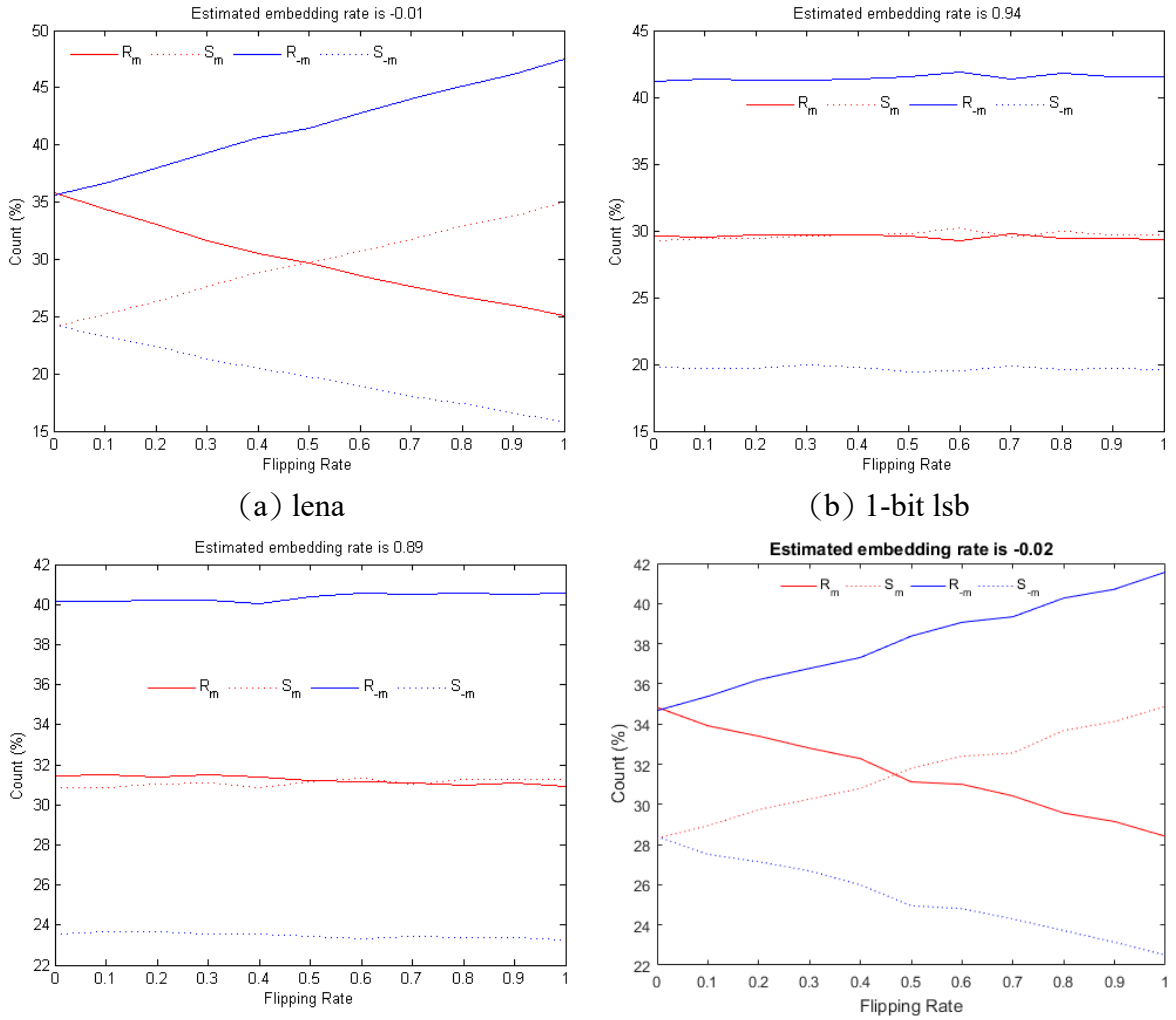
表 2 本研究偽裝影像與掩護影像 SSIM 值統計表

測試影像	*k*=5	*k*=4	*k*=3	*k*=2
	SSIM	SSIM	SSIM	SSIM
baboon	0.8774	0.9627	0.9901	0.9976
lena	0.6944	0.8893	0.9687	0.9923
peppers	0.6841	0.8885	0.9690	0.9922
goldhill	0.7684	0.9238	0.9795	0.9976
airplane	0.6764	0.8780	0.9647	0.9912
boat	0.7215	0.8973	0.9703	0.9925
lake	0.7590	0.9154	0.9759	0.9940
tiffany	0.6471	0.8732	0.9643	0.9912
average	0.7285	0.9035	0.9728	0.9936

4.3 安全性分析

資訊隱藏與密碼學研究，在秘密通訊應用上相輔相成，均是為了保障傳輸資料的安全，而密碼學之於破密，就如同資訊隱藏之於藏密偵知的關係，藏密偵知是利用偵測或分析技術，發現掩護媒體藏有秘密資訊就算成功。在藏密偵知的領域中，已有針對 LSB 取代法的影像隱藏偵測技術，經由統計方法計算影像像素對的特徵資料，即可有效偵測出藏密訊息長度的 RS 偵測技術(Fridrich, 2001)及卡方檢定法(Westfeld, 1999)。

本研究藏密方法是以 LSB 取代法為基礎將秘密訊息藏入掩護影像，為驗證本研究藏密方法之安全性，本研究採用 RS 偵測技術進行影像分析，獲得分析結果如圖 13 所示，圖 13(a)為 RS 偵測技術針對 Lena 原始影像之分析結果，圖 13 (b)與(c)分別針對使用 1-bit LSB 及 3-bits LSB 的 Lena 偽裝影像之分析結果，圖 13(d)為針對本研究藏密方法(k=4)所產生 Lena 偽裝影像之分析結果。從圖 13(a)-(d)之 RS 偵測結果可看出其所評估的藏密比率(embedding rate)分別為-0.01、0.94、0.89 及-0.02，表示 RS 偵測技術可有效偵測 LSB 藏密法，但無法有效偵測本研究藏密方法產生之偽裝影像，說明本研究所提植基於邊緣偵測及最佳像素調整的藏密法可有效抵抗 RS 偵測技術。



(a) lena　(b) 1-bit lsb

(c) 3-bit lsb　(d) 本研究偽裝影像(k=4)

圖 13 Lena 原圖、LSB 及本研究藏密產生偽裝影像之 RS 偵測分析圖

五、結論

本研究藉由簡化適性的高藏入量隱藏法，應用 MED 偵測法判定邊緣，並運用 LSB 與 OPAP 藏密法在平滑區嵌入較少秘密訊息、邊緣嵌入較多秘密訊息，藏密及取密演算過程簡易，能藏入高藏密量、維持一定的影像品質，與近年國際期刊所發表之高藏入量藏密法，在同樣的測試影像條件比較下，本研究提出之藏密方法，不只能維持較多的藏密量，產生之偽裝影像 PSNR 值亦較高，影像品質較佳，並通過 RS 偵測技術之安全性驗證，符合資訊隱藏技術特性中，效率性、不可察覺性、高隱藏容量、不可偵測性、安全性等目標。

資訊隱藏技術中重要之考量因素，其一是藏密量，其二為影像品質，此兩項往往是無法同時達成的。本研究尋求高藏密量的方法，並讓影像品質維持基本水準不失真的狀態，未來希望能夠依本研究成果為基礎，研究不同的邊緣偵測技術、調整藏入數量、更佳的像素調整方式，或可整合其他空間域之藏密技術，獲取更佳的藏密量或影像品質。

現代戰爭，將以資訊戰、不對稱作戰模式為主，在情報資訊掌握及傳達上，必需快速且準確，本研究提出透過簡單的邊緣偵測方法，達到高藏密量且不失真的資訊隱藏方式，且能避免運用統計分析技術，針對 LSB 取代法的影像偵測攻擊。此項藏密方法不需複雜的演算過程，透過國軍現行基本的軟硬體設備，即可將傳遞資訊藏入影像中，並從偽裝影像取出隱藏訊息，可提供國軍資訊安全管理技術研究領域參考應用。

參考文獻

王旭正、柯宏叡（2006）。資訊與網路安全－秘密通訊與數位鑑識新技法。新北：博碩文化。

王旭正、翁麒耀、林家禎（2012）。數位影像處理與應用。新北：博碩文化。

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

左豪官、戴鑑廷、盧嘉鴻、婁德權、劉江龍、吳嘉龍（2007）。資訊隱藏技術之研究。*黃埔學報*，52，9-16。

冷輝世、張維剛、曾顯文（2013）。基於預測值與鄰近像素差值的標準差的可逆式資訊隱藏。TANET2013 臺灣網際網路研討會論文集，1-6。

吳南益、傅國欽、王宗銘（2010）。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*，11（7），1071-1081。

呂慈純、冷輝世、黃俊智（2014）。植基於邊緣偵測法及鏡射三角定位概念之資訊隱藏技術。*資訊科技國際期刊*，8（2），35-41。

陸哲明（2014）。信息隱藏概論。北京：電子工業。

張凱崴（2013）。資訊隱藏技術於軍事運用之研究。*陸軍通資半年刊*，119，95-119。

婁德權（2006）。藏密學發展現況。資通安全專論，T95010。

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for Data Hiding. *IBM System Journal*, *35*(3.4), 313-336.

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

Fridrich, J., Goljan, M., & Rui, D. (2001). Detecting LSB steganography in color and gray-scale images. *Magazine of IEEE Multimedia Special Issue on Security*, *4*(4), 22-28.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46-66.

Khodaei, M., & 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., Su, P., & Hsu, M. (2020). An improved steganography method based on least-significant-bit substitution and pixel-value differencing. *KSII Transactions on Internet and Information Systems*, *14*(11), 4537-4556.

Martucci, S. A. (1990). Reversible compression of HDTV images using median adaptive prediction and arithmetic coding. *IEEE International Symposium on Circuits and Systems*, *8*(2), 1310-1313.

Weinberger, M., Seroussi, G., & Sapiro, G. (1996). LOCO-I: A low complexity, context-based, lossless image compression algorithm. *Proceedings of Data Compression Conference - DCC 96*, 140-149.

Westfeld, A., & Pfitzmann, A. (1999). Attacks on Steganographic Systems. *Proceedings of the Third International Workshop on Information Hiding*, Dresden, Germany, 61-75.

Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, *24*, 1613-1626.

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

Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, & Eero P. Simoncelli. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, *13*(4), 600−612.