

結合邊緣特性與人類視覺系統的高藏量資訊隱藏法

冷輝世

國立彰化師範大學

lenghs@cc.ncue.edu.tw

張維剛

國立彰化師範大學

s9922119@mail.ncue.edu.tw

余奕憲

國立彰化師範大學

s9922117@mail.ncue.edu.tw

曾顯文

朝陽科技大學

hwtseng@cyut.edu.tw

摘要

數位化已是目前時代的潮流。因此，資訊安全亦受到重視。近年來許多學者從事資訊隱藏領域的研究，將機密訊息藏匿在媒介中。如何結合影像的特性以及符合人類視覺系統是一重要課題。本研究複製四份原始影像，再將這四份原始影像各別分割為 2×2 的區塊，分別使用MED邊緣檢測法判斷是否存在邊緣，進而以LSB結合OPAP的方式藏入機密訊息，最後再將四份藏入後的影像結合為偽裝影像。目的是儘可能在人類視覺系統可接受的影像品質下提高偽裝影像的藏量。實驗結果顯示本研究的方法不但符合邊緣特性且具有高藏量。

關鍵詞：人類視覺系統、MED邊緣檢測法、LSB、OPAP。

Abstract

Nowadays, digitization is the current trend. Therefore, information security was paid great attention. In recent years, many researchers focus on data hiding, and how to combine the image feature under the human vision system (HVS) is an important issue.

In this study, the proposed method makes the cover image into four copies. For each copy, divide into 2-by-2 blocks, applied median edge detection (MED) to detect whether there is an edge or not, and embedding secret messages by the LSB method and the OPAP process. Finally, combine this four copies into one stego image. The aim is to enlarge payload and keep the good image quantity under the human vision system. The experimental results show that the proposed method not only keep the edge feature of cover image but also has higher payload.

Keywords: HVS, MED, LSB, OPAP.

1. 前言

數位化時代的來臨造成大量的資訊在網路間傳遞。因此，資訊安全受到重視並進而發展出資訊隱藏科學。資訊隱藏是一門新興的資訊安全科學，將機密訊息嵌入媒介中(文字、圖形、影像等)，再傳送給接收方，接收方可藉由與傳送方協定的方法取出媒介中的機密訊息。由於圖形被廣泛的使用於網路上，且圖形具有龐大藏量的特性，所以大部份

的研究都以圖形為媒介。

資訊隱藏法又分為可逆式與不可逆式。可逆式可保持其原始媒體的完整性，主要有Tian學者(2007)[3]提出的差值擴張法、Ni學者(2006)[5]提出的直方圖位移法，通常無法藏入大量的機密訊息；不可逆式是指機密訊息取出後無法還原原始媒介，通常可藏入大量的機密訊息，以Chan等學者(2001)[1]提出的最小位元藏匿法(LSB)為一個普遍的藏匿技術，Chan等學者(2004)[2]對LSB另外提出了OPAP的最優化方法。

一般而言，人類視覺系統(HVS)對於影像平坦區內的變化之視覺敏感度高於複雜區的變化，且在PSNR值大於30dB時不具分辨性。本研究透過MED邊緣檢測法判別 2×2 區塊內是否有'edge'還是'non-edge'，並依上述的HVS特性決定藏入訊息的長度，利用LSB藏匿技術結合OPAP優化技術將機密訊息嵌入，使其偽裝影像在人類視覺系統可接受的範圍內(PSNR為30dB左右)，有較大的藏量及好的影像品質。

本文其餘的部分安排如下：第二章介紹相關研究，研究方法則在第三章說明，實驗結果在第四章說明，最後是結論。

2. 相關研究

在本章中將介紹：MED、Least Significant Bit (LSB)與Optimal pixel adjustment process (OPAP)。在底下的小節中，我們定義目標像素為 x ，如圖1，陰影區域代表是 x 的相鄰像素， a 為目標像素之水平鄰近像素、 b 為目標像素之垂直鄰近像素、 c 為目標像素之對角像素。

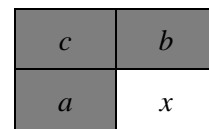


圖1 目標像素 x 與其相鄰像素

2.1 MED

Weinberger(2000)[4]所提出的MED預測法：假設在原始影像中 a 、 b 、 c 為目標像素 x 的鄰近像素(如圖1)。則其預測值為

$$\hat{x} = \begin{cases} \min\{a,b\}, & \text{if } c \geq \max\{a,b\} \\ \max\{a,b\}, & \text{if } c \leq \min\{a,b\} \\ a+b-c, & \text{otherwise} \end{cases}$$

其中若 $c \geq \max\{a,b\}$ 或是 $c \leq \min\{a,b\}$ 表示有'edge', 否則為'non-edge'。

2.2 LSB

Chan 等學者(2001)[1]提出 Least Significant Bit (LSB)藏匿法為一個普遍的藏匿技術，具有高藏量與低失真的特性，其方法如下：

設 P 為 8 位元像素的 $M \times N$ 原始影像的像素。

$$P = \{x_{ij} \mid 0 \leq i < M, 0 \leq j < N, x_{ij} \in [0, 255]\}$$

設 s 為 n 位元的機密訊息。

$$s = \{s_i \mid 0 \leq i < n, s_i \in \{0, 1\}\}$$

假設將 n 位元的機密訊息 s 嵌入於原始影像 C 的最右邊 k 位元，首先，將機密訊息 s 排置成 k 位元的 s' 。

$$s' = \{s'_i \mid 0 \leq i < n', m_i \in \{0, 1, \dots, 2^k - 1\}, n_i < M \times N\}$$

n 位元的機密訊息 $s = \{s_i\}$ 與嵌入訊息 $s' = \{s'_i\}$ 的關係如下：

$$s'_i = \sum_{j=0}^{k-1} s_{i \times k + j} \times 2^{k-1-j}$$

其中 n' 像素 $\{x_{i_1}, x_{i_2}, \dots, x_{i_{n'}}\}$ 從原始影像 C 預先定義的序列中選出。

嵌入過程：原始像素 x_{i_j} 嵌入 k 位元訊息 m'_i 後為隱蔽像素 x'_{i_j} ，則

$$x'_{i_j} = x_{i_j} - x_{i_j} \bmod 2^k + s'_i$$

取出過程：使用和嵌入過程中相同的序列，隱蔽像素 $\{x'_{i_1}, x'_{i_2}, \dots, x'_{i_{n'}}\}$ 含有嵌入的訊息，嵌入訊息 m'_i 可透過下面的式子取出：

$$s'_i = x'_{i_j} \bmod 2^k$$

2.3 Optimal pixel adjustment process

Chan 等學者(2004)[2]提出 LSB 技術最佳化的方法 OPAP (Optimal pixel adjustment process)，利用 LSB 藏匿機密訊息再加以最佳化以減少失真。

在原始影像 C 中，假設 p_i ， p'_i ， p''_i 為第 i 個相對應的像素，透過 LSB 的藏匿方法和 OPAP 得到偽裝影像 C' ，假設 d_i 為 p'_i 和 p_i 的嵌入誤差，在 2.2 節中， p'_i 是透過 LSB 取代 p_i 的 k 位元而得到的，因此， $-2^k < d_i < 2^k$ ， d_i 可再進一步地分成三個區間：

第一區間： $2^{k-1} < d_i < 2^k$

第二區間： $-2^{k-1} \leq d_i \leq 2^{k-1}$

第三區間： $-2^k < d_i < -2^{k-1}$

藉由三個不同的區間，將隱蔽像素 p'_i 透過 OPAP 修改為 p''_i ，敘述如下：

例一($2^{k-1} < d_i < 2^k$):

若 $p'_i \geq 2^k$ ， $p''_i = p'_i - 2^k$ ，否則 $p''_i = p'_i$ 。

例二($-2^{k-1} \leq d_i \leq 2^{k-1}$):

$p''_i = p'_i$ 。

例三($-2^k < d_i < -2^{k-1}$):

若 $p'_i < 256 - 2^k$ ， $p''_i = p'_i + 2^k$ ，否則 $p''_i = p'_i$ 。

假設 d'_i 為 p''_i 和 p_i 的嵌入誤差， d'_i 的計算如下：

例一($2^{k-1} < d_i < 2^k$ & $p'_i \geq 2^k$):

$$\begin{aligned} d'_i &= p''_i - p_i = p'_i - 2^k - p_i = d_i - 2^k \\ &\Rightarrow 2^{k-1} - 2^k < d'_i < 2^k - 2^k \\ &\Rightarrow -2^{k-1} < d'_i < 0 \end{aligned}$$

例二($2^{k-1} < d_i < 2^k$ & $p'_i < 2^k$):

$$\begin{aligned} d'_i &= p''_i - p_i = p'_i - p_i = d_i \\ &\Rightarrow 2^{k-1} < d'_i < 2^k \end{aligned}$$

例三($-2^{k-1} \leq d_i \leq 2^{k-1}$):

$$\begin{aligned} d'_i &= p''_i - p_i = p'_i - p_i = d_i \\ &\Rightarrow -2^{k-1} \leq d'_i \leq 2^{k-1} \end{aligned}$$

例四($-2^k < d_i < -2^{k-1}$ & $p'_i < 256 - 2^k$):

$$\begin{aligned} d'_i &= p''_i - p_i = p'_i + 2^k - p_i = d_i + 2^k \\ &\Rightarrow -2^k + 2^k < d'_i < -2^{k-1} + 2^k \\ &\Rightarrow 0 < d'_i < 2^{k-1} \end{aligned}$$

例五($-2^k < d_i < -2^{k-1}$ & $p'_i \geq 256 - 2^k$):

$$\begin{aligned} d'_i &= p''_i - p_i = p'_i - p_i = d_i \\ &\Rightarrow -2^k < d'_i < -2^{k-1} \end{aligned}$$

由上面五例可知經由 OPAP，可將原始影像與偽裝影像的嵌入誤差的絕對值限制於 $0 \leq |d'_i| \leq 2^{k-1}$ 。

3. 研究方法

本實驗中先將原始影像複製為四份相同的影像，再將這四張相同影像各別切割為 2×2 的區塊，這四張影像中的每個小區塊，分別在小區塊中的四個不同位置依 MED 邊緣偵測分為 'edge' 與 'non-edge'，並且依照特性決定藏入訊息的多寡，最後再將這四張影像合併為一張偽裝影像(如圖 2)。

3.1 複製影像與影像切割

本實驗中先將原始影像複製為四張相同的影像，再將這四張影像分割為 2×2 的小區塊，並且將這四張圖在小區塊中的四個不同位置分別藏入機密訊息，如圖 3、圖 4、圖 5 與圖 6 所示：

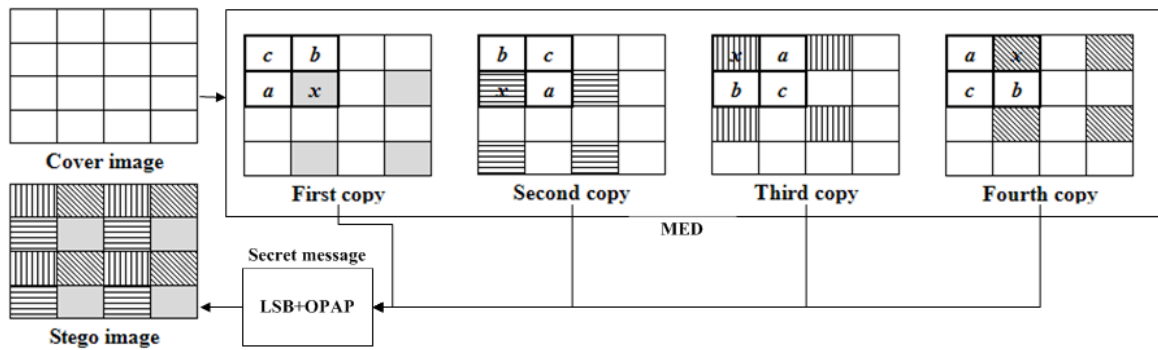


圖 2 藏入方法

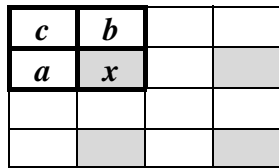


圖 3 First copy

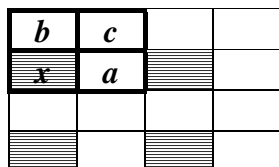


圖 4 Second copy

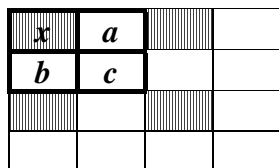


圖 5 Third copy

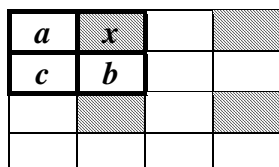


圖 6 Fourth copy

其中 x 為藏匿的目標像素， a 為目標像素的水平鄰近像素， b 為目標像素的垂直鄰近像素， c 為目標像素的對角鄰近像素。

3.2 藏匿方法與取出方法

將 2×2 區塊分為 'edge' 與 'non-edge'，並且根據其特性決定藏量大小。

判斷方法：

若 $c \geq \max\{a, b\}$ 或 $c \leq \min\{a, b\}$ ，則該區塊為 'edge'，否則為 'non-edge'。

依照人類視覺系統(HVS)，複雜區塊的改變較難察覺，因此在 'edge' 區藏入 n bits，在 'non-edge' 區藏入 $(n-1)$ bits。

藏匿方式使用 LSB+OPAP，如圖 3、圖 4、圖 5 與圖 6 之順序，依序藏入機密訊息。

藏匿方法：

對於目標像素 x 使用 LSB(n)+OPAP 藏入 n bits：

$$x_1' = [x - (x \bmod 2^n)] + s$$

$$x_2' = \begin{cases} [x - (x \bmod 2^n) + 2^n] + s & \text{if } \left\lfloor \frac{x}{2^n} \right\rfloor \in \text{even} \\ [x - (x \bmod 2^n) - 2^n] + s & \text{if } \left\lfloor \frac{x}{2^n} \right\rfloor \in \text{odd} \end{cases}$$

隱蔽像素 $x' = \begin{cases} x_1' & \text{if } |x_1' - x| \leq |x_2' - x| \\ x_2' & \text{if } |x_1' - x| > |x_2' - x| \end{cases}$ ，其中 s 為 n

bits 機密訊息。

四張圖接藏匿完成之後將藏匿完成的四張影像各自取其 x 像素，合併為一張偽裝影像(Stego image)，如圖 7：

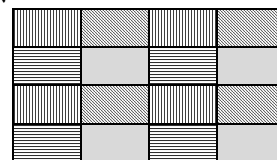


圖 7 Stego image

取出方法則是需要四張原始影像，並且將偽裝影像中每個小區塊的四個不同位置的像素，複製到四張原始影像中對應的位置，將偽裝影像還原回如圖 3、圖 4、圖 5 與圖 6，四張影像，接著將這四張影像依序使用 LSB 取出機密訊息(如圖 8)。

對於隱蔽像素 x' 使用 LSB(n) 取出 n bits：

$$\text{機密訊息 } s = x' \bmod 2^n。$$

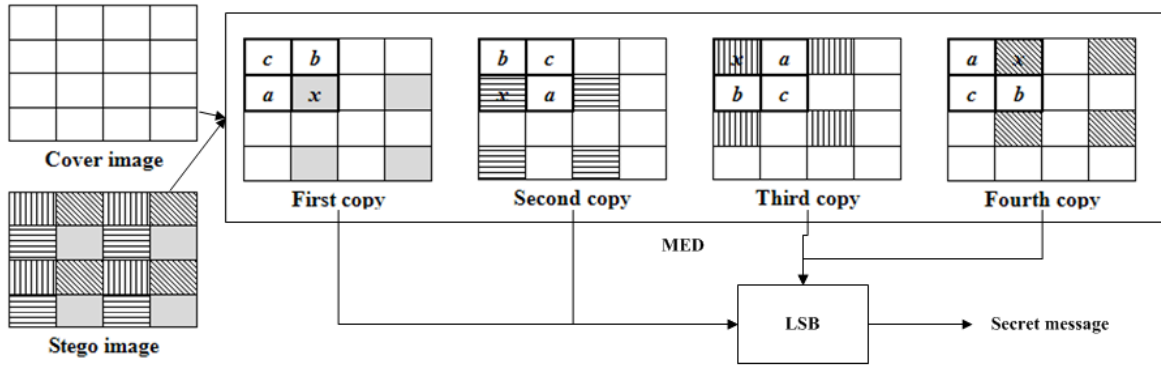


圖 8 取出方法

取出步驟：

將圖 10 的偽裝影像中每個小區塊的四個部分各自取出，並且替換掉四張原圖相對應位置(灰色部分)的像素值，如圖 11-14：

3.3 藏匿與取出範例

設 $n=5$ ，機密訊息串為 '101011010000010011'
以圖 9 為例：

80	179
78	178

圖 9 藏匿範例圖

藏匿步驟：

第一張圖：

目標像素 $x=178$ ，因為 $\min\{a,b\} < c < \max\{a,b\}$ 故藏入 4 bits, $s=0011_2=3$ ，則

$$x' = [178 - (178 \bmod 16)] + 3 = 179。$$

第二張圖：

目標像素 $x=78$ ，因為 $c \geq \max\{a,b\}$ 故藏入 5 bits $s=00001_2=1$ ，則

$$x' = [78 - (78 \bmod 32)] + 1 = 65$$

第三張圖：

目標像素 $x=80$ ，因為 $\min\{a,b\} < c < \max\{a,b\}$ 故藏入 4 bits, $s=1010_2=10$ ，則

$$x' = [80 - (80 \bmod 16)] - 16 + 10 = 74$$

第四張圖：

目標像素 $x=179$ ，因為 $c \leq \min\{a,b\}$ 故藏入 5 bits, $s=10101_2=21$ ，則

$$x' = [179 - (179 \bmod 32)] + 21 = 181$$

之後再將這四張圖有藏匿機密訊息的部分取出，合併為一張偽裝影像，如圖 10：

74	181
65	179

圖 10 藏匿完後的合併圖

80	179
78	179

圖 11 第一張替換圖

80	179
65	178

圖 12 第二張替換圖

74	179
78	178

圖 13 第三張替換圖

80	181
78	178

圖 14 第四張替換圖

第一張圖：

隱蔽像素 $x'=179$ ，因為 $\min\{a,b\} < c < \max\{a,b\}$ 故藏入 4 bits, $s = 179 \bmod 16 = 3 = 0011_2$ 。

第二張圖：

隱蔽像素 $x'=65$ ，因為 $c \geq \max\{a,b\}$ 故藏入 5 bits, $s = 65 \bmod 32 = 1 = 00001_2$ 。

第三張圖：

隱蔽像素 $x'=74$ ，因為 $\min\{a,b\} < c < \max\{a,b\}$ 故藏入 4 bits, $s = 74 \bmod 16 = 10 = 1010_2$

第四張圖：

隱蔽像素 $x'=181$ ，因為 $c \leq \min\{a,b\}$ 故藏入 5 bits

$$s = 181 \bmod 32 = 21 = 10101_2。$$

4. 實驗結果

本實驗使用 SIPI 影像圖庫裡的 'Tiffany'、'Baboon'、'Lena'、'Airplane'、'Scene' 與 'Peppers'，這六張圖為實驗樣本：

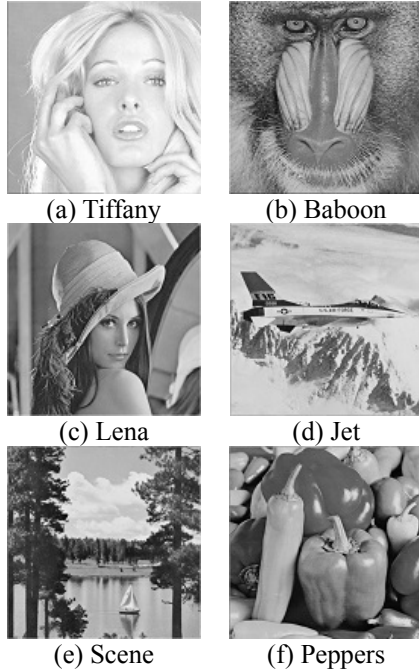


圖 15 六張原始影像

當 $n=5$ 與 $n=4$ 時，藏匿後的結果如圖 16、圖 17，由於 PSNR 值皆接近或大於 30dB，並無顯著差異：

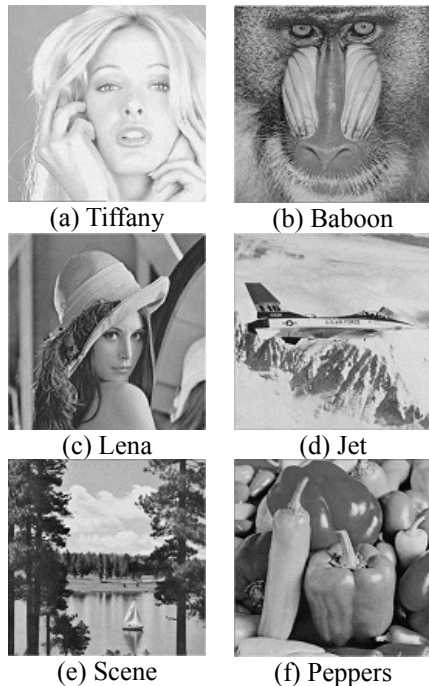


圖 16 $n=5$ 六張藏匿後的影像

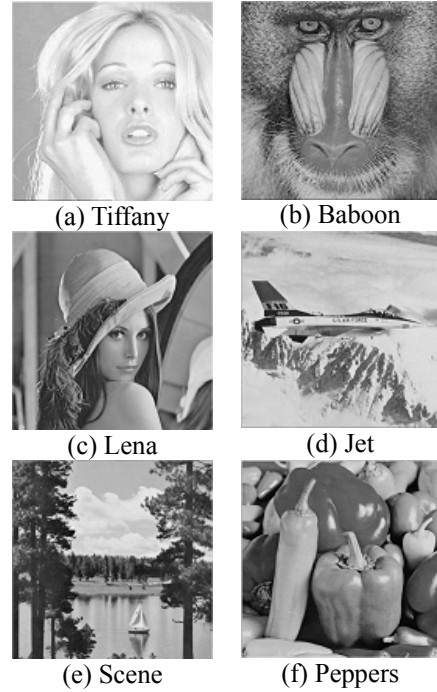


圖 17 $n=4$ 六張藏匿後的影像

由表 1、表 2 可知 $n=5$ 時，平均 PSNR 值約為 29.86dB，接近人類視覺系統可接受的影像品質，平均藏入率高達 4.69 bpp。若取 $n=4$ ，平均 PSNR 值約為 35.90dB，其平均藏入率亦高達 3.69 bpp。

表 1 $n=5$ 藏量表

	PSNR	Capacity	Payload
Tiffany	29.391660	1235456	4.712891
Baboon	30.215669	1214049	4.631229
Lena	29.957462	1229326	4.689507
Jet	29.891162	1233349	4.704853
Scene	29.930917	1230931	4.695629
Peppers	29.766402	1241229	4.734913

表 2 $n=4$ 藏量表

	PSNR	Capacity	Payload
Tiffany	35.697580	973312	3.712891
Baboon	36.197437	951905	3.631229
Lena	35.964673	967182	3.689507
Jet	35.894131	971205	3.704853
Scene	35.908862	968787	3.695629
Peppers	35.755626	979085	3.734913

5. 結論

本研究利用複製四份原始影像，再將這四份原始影像各別分割為 2×2 的區塊，分別使用 MED 邊緣檢測法判斷是否存在邊緣，進而以 LSB 結合 OPAP 的方式藏入機密訊息，最後再將四份藏入後

的影像結合為偽裝影像。由實驗結果可以知道可知當 $n=5$ 時，平均 PSNR 值約為 29.86dB，接近人類視覺系統可接受的影像品質，平均藏入率高達 4.69 bpp。

參考文獻

- [1] Chi-Kwong Chan, L.M. Cheng, "Improved hiding data in images by optimal moderately significant-bit replacement", IEEE Electron. Lett. 37 (16), pp1017-1018, 2001.
- [2] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.37, pp. 469-474, 2004.
- [3] Tian, J., "Reversible data embedding using a difference expansion." IEEE Transactions on Circuits and Systems for Video Technology, 16 (3), 721-730. 2007.
- [4] Weinberger MJ & Seroussi G, "The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS", IEEE Trans Image Process, 9(8), pp. 1309-1324, 2000.
- [5] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding." IEEE Transactions on Circuits and systems for video technology, Vol. 16, No. 3, March 2006