

改善 DLE 之高藏量資料隱藏法

李金鳳

朝陽科技大學
資訊管理學系副教授
lcf@cyut.edu.tw

趙宏林

朝陽科技大學
資訊管理學系研究生
s9614620@cyut.edu.tw

摘要

以影像做為隱蔽媒體，將機密資訊藏入隱蔽影像之中，只有接收者知道如何將機密資料從掩護媒體中擷取出來，而其他非法的竊取者誤以為掩護影像只是個普通的圖像，而不會有任何作為。Zhang *et al.* [7]運用最低位元取代技術 (Least Significant Bit, LSB) 及濕編碼 (Wet Paper Code, WPC) [2][3]提出一個雙層資料隱藏法(Double-layered Embedding, DLE)[6][7]。在 DLE 法中，欲嵌入一些機密資訊至灰階影像時，會先修改灰階像素值的第一層 LSB，並選擇加/減一個位元值來修改部份的第二層 LSB，以達到更多機密資訊藏入之目的。本論文提出一個改良式的 DLE 方法，並經實驗印証我們所提的方法可以達到比 DLE 更高的資料藏入量。

關鍵詞：資訊隱藏、最低位元取代法、濕編碼、雙層資訊隱藏。

Abstract

The steganographical techniques is to hide secret data into cover media like images as such that the illegal interceptors have no awareness of the in visual secret message, because the transmitted media between sender and receiver ends appear to be normal. Zhang *et al.*[7] a Double-layered Embedding (DLE) method [6][7] combining the steganographical methods of Least Significant Bit (LSB) with Wet Paper Code (WPC) [2][3] to embed the secret data into gray-level images. In the DLE method, the first LSBs of gray-level pixels might be changed by adding/subtracting one and the second LSBs of some pixels need to be altered if the first LSBs of these pixels have been altered. The DLE method improves the embedding efficiency of wet paper codes with a “double wet paper coding” scheme, and reaches the upper bound on that of LSB

steganography.

This paper advances the embedding capacity of the DLE method. The experimental results show that the proposed method achieves much better performance in the evaluation of embedding capacity but keeps the stego-image quality within a satisfactory degree.

Keywords: Information Hiding, Least Significant Bit, Wet Paper Code, Double-layered Embedding.

1. 前言

資訊隱藏這個議題可追溯自遠古時期的古希臘時代，這樣的一個技術至今仍不斷地被更新。尤其，在現今這個數位化的時代裡，各種資料都可以用數位的方式呈現(如文字、影像、聲音、視訊等)，而將機密資料隱藏在數位化的媒體中，已衍然成為現今資訊隱藏技術的新趨勢。因此，有效的將機密資訊隱藏到影像之中而不被第三者發現，並達到高資料藏入量(Embedding Capacity)是目前研究的重點方向。基於以上原因，許多資料隱藏技術[1]皆會根據下面兩個方向來開發隱藏的方法：

- (1)避免將資訊隱藏在隱蔽影像較為明顯的部份。
- (2)改善藏入時的效率，例如：隱藏更多的資訊到隱蔽媒體內。

Fridrich *et al.*提出植基於濕編碼(Wet Paper Code, WPC) [2]的影像隱藏技術，並非如以往 LSB 取式法[4]是以隨機方式來選取灰階影像之最低位元，以進行位元取代來藏入秘密資料，而是利用隱蔽影像像素及機密位元資料，達到避免將資訊隱藏在隱蔽影像較為明顯的部份。Zhang *et al.*於 2007 年所提出的加/減一的雙層資訊隱藏方法(DLE) [7]，主要的目的是原始的最低位元取代法容易經由統計分析工具分析出其藏入機密資訊的分佈，且直接採取最低位元取代法的安全性極低，所以他們提出雙層資訊隱藏的構想，可以增加機密資料的安全並且增加其隱藏的效率。本論文植基於 DLE，提出一個改良式的資料隱藏方法，以提昇 DLE 的資料藏入量。經實驗印証我們所提的方法可以達到比 DLE 更高的資料藏入量，然偽裝影像失真程度仍然在可容忍的範圍

內。本論文的組織架構為：第二節探討最低位元取代法及雙層資訊隱藏方法，第三節為本論文之研究方法介紹，第四節實驗分析及討論，第五節為結論。

2. 文獻探討

以下，我們將探討與本論文息息相關的兩種資料隱藏技術，分別為「最低位元取代法」及「雙層資訊隱藏方法」。

2.1 最低位元取代法 (Least Significant Bit, LSB)

最低位元取代法是利用改變數位媒體的最後一個位元值來進行資訊隱藏的動作。舉例來說，我們利用一張影像當成隱蔽媒體，將此影像的像素值轉換成二進制編碼，以相同的方式將所要隱藏的資訊轉換成二進制編碼。我們直接將所要隱藏資訊的二進制編碼值取代此影像像素值的最後一個位元值，將取代後的像素位元值轉換回十進制數值後並還原該影像，此影像稱之為偽裝影像。偽裝影像經傳輸後，當接收方收到此影像時，依照上述步驟將偽裝影像的像素值轉換成二進制編碼，並取出此編碼的最後一位元值，就可以得到原始傳送方想傳送的機密資訊。

範例 2-1：

假設影像 I 的像素值為 $I(15, 16, 17, 18)_{10}$ ，預藏入機密資訊 $S(1011)_2$ ，將其影像 I 轉換成二進制表示為 $(00001111, 00010000, 00010001, 00010010)_2$ ，將機密資訊 $S(1011)_2$ 直接覆蓋取代影像 I 的最後一位位元值，其結果為 $(00001111, 00010000, 00010001, 00010010)_2$ ，藏入後的偽裝影像 I' 為 $(15, 16, 17, 19)_{10}$ 。

當接收方收到偽裝影像後，將機密資訊取出方法是將偽裝影像 $I'(15, 16, 17, 19)_{10}$ 轉換成二進制值表示為 $(00001111, 00010000, 00010001, 00010010)_2$ ，直接取出每個像素值得最後一個位元值，其結果為 $(1011)_2$ 及為藏入的機密資訊。

2.2 雙層資料隱藏技術

Zhang *et al.* 於 2007 年所提出的加/減一的雙層資訊隱藏方法 [6][7]，主要的目的是原始的最低位元取代法容易經由統計分析工具分析出其藏入機密資訊的分佈，且直接採取最低位元取代法的安全性極低，所以他們提出雙層資訊隱藏的構想，解決以上兩個問題，並且增加其隱藏的效率。

根據 DLE 的概念，隱藏的動作會分成以下步驟進行，首先，將灰階影像以 $I_{(x_1, x_2, \dots, x_n)}$ 表示，其中 $x_1, x_2, \dots, x_n$ 表示灰階影像 I 的 n 個像素值，

$0 \leq x_i \leq 255$ 。機密資訊以 $S_{(b_1, b_2, \dots, b_m)}$ 表示之，其中 $b_1, b_2, \dots, b_m$ 表示機密資訊 S 中有 m 個機密位元， $b_i \in \{0, 1\}$ 。我們定義對原始像素值 x_i 作一階 LSB 取代法以 $LSB_1(x_i)$ 表示，對原始像素值 x_i 作二階 LSB 取代法以 $LSB_2(x_i)$ 表示之。若 $LSB_1(x_i)$ 值經位元運算後有改變，我們則以 $\overline{L_1(x_i)}$ 表示改變後的位元值；同理， $LSB_2(x_i)$ 值經位元運算後有改變，則以 $\overline{L_2(x_i)}$ 表示改變後的位元值。令 $L_1(x_i)$ 表示藏入機密位元到原始像素 x_i 後的之偽裝影像像素的第一階 LSB 位元值， $L_2(x_i)$ 為藏入機密位元資料後的偽裝影像像素之第二階 LSB 位元值。

先對影像 I 作一階 LSB 做 LSB 藏入法後，比較 S 與原始影像像素位元值是否相等，若相等則不進行第二階 LSB 藏入運算，即 $\overline{L_1(x_i)} = L_1(x_i)$ 。若 $LSB_1(x_i)$ 的位元值與原始影像像素位元值不相等，即 $\overline{L_1(x_i)} \neq L_1(x_i)$ ，則進行二階 LSB 藏入的工作。我們先將 $S(b_{m-n})$ 個機密資料經由一個傳送方與接收方事先定義好的密鑰方陣 $M_{k \times k}$ 進行轉置的動作，將轉置後的 $S(b_{m-n})$ 藏入二階 LSB 的位置，即完成藏入的動作。當接收方收到此影像時，依照上述步驟將偽裝影像的像素值轉換成二進制編碼，並取出此編碼的最後一位元值，以及取出不相等位置之機密資訊，將其以密鑰方陣 $M_{k \times k}$ 進行反轉置的動作，其結果與先前取出的最後一位元值合併及完成取出的動作。

3. 改善 DLE 之高藏量資訊隱藏法

本論文基於提昇資訊隱藏量及維持合理的影像品質將針對 Zhang *et al.* 學者於 2007 年所提出的加/減一的雙層資訊隱藏方法進行改善，並再以下說明之。

3.1 資料藏入

本研究基於 Zhang *et al.* 學者所提出的方法，利用第二層隱藏後所餘留的位置加以隱藏額外的資訊，以提升整體影像攜帶秘密資訊時的攜帶量。其方法如下述步驟：

首先取得一張灰階影像 $I_{(x_1, x_2, \dots, x_n)}$ ，機密位元字串 $S_{(b_1, b_2, \dots, b_m)}$ ，並與接收方制定一個大小為 $k \times k$ 的方陣 $M_{k \times k}$ 作為加解密的密鑰。同樣定義對原始像素值 x_i 作一階 LSB 取代法以 $L_1(x_i)$ 表示，對原始像素值 x_i 作二階 LSB 取代法以 $L_2(x_i)$ 表示

之。若 $L_1(x_i)$ 值經位元運算後有改變，我們則以 $\overline{L_1(x_i)}$ 表示改變後的位元值；同理， $L_2(x_i)$ 值經位元運算後有改變，則以 $\overline{L_2(x_i)}$ 表示改變後的位元值。令 $L'_1(x_i)$ 表示藏入機密位元到原始像素 x_i 後之偽裝影像像素的第一階 LSB 位元值， $L'_2(x_i)$ 為藏入機密位元資料後的偽裝影像像素之第二階 LSB 位元值。

step1. 將 $S_{(b_1, b_2, \dots, b_n)}$ 以一階 LSB 的方式藏入灰階影像 $I_{(x_0, x_1, \dots, x_n)}$ 中，即 $L'_1(x_i) = L_1(x_i) + b_i$ 。

step2. 判別藏入後的值是否與原始位元值相等，若不相等，則進行二階 LSB 藏入的工作。

$$L'_2(x_i) = \begin{cases} L_2(x_i), & \text{if } L'_1(x_i) = L_1(x_i) \\ L_2(x_i) + b, & \text{if } L'_1(x_i) = \overline{L_1(x_i)} \end{cases} \quad (1)$$

where $i = 1, 2, \dots, n$; $b \in S - \{b_1, b_2, \dots, b_n\}$.

為了方便下列藏入步驟之表示與說明，我們在此更進一步地重新定義，令有 h 個像素值都滿足 $L'_1(x_i) = L_1(x_i)$ ，所以為這 h 個像素重新排序值編號為 $(x_{a_1}, x_{a_2}, \dots, x_{a_h})$ st. $L'_1(x_{a_1}) = L_1(x_{a_1})$, $L'_1(x_{a_2}) = L_1(x_{a_2})$, $\dots$, $L'_1(x_{a_h}) = L_1(x_{a_h})$ 。同理也重新為剩下 $(n-h+1)$ 個像素值編號，這些它們都滿足 $L'_2(x_i) = \overline{L_2(x_i)}$ ，重新排序之編號為 $(x_{b_1}, x_{b_2}, \dots, x_{b_{n-h+1}})$ st. $L'_2(x_{b_1}) = \overline{L_2(x_{b_1})}$, $L'_2(x_{b_2}) = \overline{L_2(x_{b_2})}$, $\dots$, $L'_2(x_{b_{n-h+1}}) = \overline{L_2(x_{b_{n-h+1}})}$ 。那麼公式 (1) 就可以重寫成公式 (2)

$$\begin{cases} L'_2(x_{a_i}) = L_2(x_{a_i}), & \text{if } L'_1(x_{a_i}) = L_1(x_{a_i}) \\ \text{for } i = 1, 2, \dots, h. \\ L'_2(x_{b_i}) = L_2(x_{b_i}) + b_i, & \text{if } L'_1(x_{b_i}) = \overline{L_1(x_{b_i})} \\ \text{for } i = n+1, n+2, \dots, m. \end{cases} \quad (2)$$

且 $b_i \in S$ 。

step3. 將 $S_{(b_{n+1}, b_{n+2}, \dots, b_m)}$ 與一個轉置矩陣 $M_{k \times k}$ 進行轉置的動作。 $B^t = M \times b^t$ ，轉置後得到 B 矩陣。 B 矩陣乃是將 $b_{n+1}, b_{n+2}, \dots, b_m$ 透過轉置矩陣打亂每一個機密位元所重新排列的得到的機密位元矩陣。即 $B = M(S)$ 。

step4. 將不相等的位置記錄下來，並且進行二階 LSB 的藏入，即

$$L_2(x_{b_i}) = L_2(x_{b_i}) + b_i, b_i \in B$$

step5. 對一階 LSB 相等的位置，再次進行二階 LSB 藏入的工作，即

$$L_2(x_{b_i}) = L_2(x_{b_i}) + b_{m-i}, b_{m-i} \in B$$

3.2 資料取出

改善 DLE 藏入法取出程序如下：

step1. 第一階段先取出偽裝影像的第一階位元值，此為機密位元的前 n 個位元串，即

$$S(b_i) = L'_1(x_i), \text{ for } i = 1, 2, \dots, n.$$

step2. 第一階段再根據 location map 之指示，來取出在部份第二階的位元值，即為剩餘的 $m-n+1$ 的位元串。

$$B(b_i) = L'_2(x_i), \text{ for } i = n+1, n+2, \dots, m.$$

step3. 將非 location map 指示之第二階 LSB 位置值取出，並與 step3 取出之位元值合併。

step4. 然而這些位元串還需由 data receiver 透過方陣 M 來重排其順序。即

$$S(b_i) = MB(b_i), \text{ for } i = n+1, n+2, \dots, m.$$

step5. 將轉置後的位元值與 step1 取出之位元值合併，即的到原來所藏入之資料。

範例 3-1：

假設影像 I 的像素值為 $I(10, 11, 22, 13)_{10}$ ，欲藏入機密資訊 $S(10110111)_2$ ，將其影像 I 轉換成二進制表示為 $(00001010, 00001011, 00010110, 00001101)_2$ ，假設轉置矩陣 $M_{4 \times 4}$

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}_{4 \times 4} \quad \text{。首先，將影像 } I \text{ 作一階 LSB}$$

嵌入，嵌入機密位元資訊為 $(1011)_2$ ，其結果為 $(00001011, 00001010, 00010111, 00001101)_2$ ，接著判別原始資料值與嵌入資料是否相同，其中，像素值 10、11 和 22 經過機密位元資訊 $(1011)_2$ 的藏入後，其一階 LSB 會被修改，因此，這 3 個像素值（以 $DP = \{dp_1, dp_2, dp_3\}$ 表示之）將再進行二階 LSB 藏入的動作。對於沒有被修改的像素將之依序收集在集合 NP 中，以上例則 $NP = \{np_1\}$ ， $np_1 = 13$ 將機密資訊 S 剩餘的值 $B(0111)$ 與矩陣 $M_{4 \times 4}$ 進行運算，

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \text{ 將轉置過的值 } (1, 1, 1,$$

0) 取前三個值藏入 DP 的三個像素值（意即 dp_1, dp_2, dp_3 ）之二階 LSB 位置，其結果為 $(00001011,$

00001010, 00001011, 00001101)₂。

接著，將判別後未修改的二階 LSB 位置也進行藏入的動作，取出經轉置後未藏入剩餘的值 B (0)，藏入影像的 dp_1 (即 13) 之第二階 LSB 中，其結果為 (00001011, 00001010, 00001011, 00001101)₂。將其結果還原成十進制值，則偽裝影像 I' 為 (11, 10, 23, 13)。

當接收方收到偽裝影像 I' 後，將機密資訊取出的方式如下：首先，將偽裝影像 I' (11, 10, 23, 13) 轉換成二進制，其結果為 (00001011, 00001010, 00001011, 00001101)₂，接著直接取出像素值的最後一個位元值，取出結果 (1011)。再利用剛才所紀錄的位置 DP 集合中每一個像素值的第二階 LSB 所藏入的機密位元，其值為 (111)。接著再取出 NP 集合中每一個像素值的第二階 LSB 位置的位元值 (0)，利用事前與傳送方取得的密鑰 M 與二階 LSB 位置取出來的機密資訊做轉換，

$$\begin{bmatrix} 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \text{ 其藏入的資}$$

訊 S 為 (10110111)。

由計算結果可看出，不同於原始最低位元取代法，DLE 的方法至多會將每一個原始影像的像素值加/減 1，以本例來看，則只有三個原始影像的像素值有變動，且變動的幅度至多只有加/減 2，故偽裝影像的品質相對其他方法確實相當高。

4. 實驗分析及討論

本實驗使用 AMD Athlon™ 64×2 Dual Core Processor 3000+ 997MHz 的 CPU，960MB 的 RAM，使用的軟體為 MATLAB 7.1 版。我們使用大小為 512×512 的五張影像進行比較，並以影像信號雜訊比 (Peak Signal to Noise Ratio, PSNR) 作為影像品質評比的衡量基準。當我們使用 DLE 方法對影像進行藏入的動作，其平均藏入量為 393256bits，平均 PSNR 值為 46.3732dB。

本篇論文所提出之改善 DLE 之高藏量資料隱藏法對於這五張影像進行藏入，其平均藏入量為 524288bits，平均影像品質 PSNR 值為 40.0292dB。由實驗結果得知，當對於同一張影像進行藏入其藏量平均比 DLE 方法高出 131032bits 而 PSNR 值只減少了 6.344dB，對於視覺品質的影響甚微。其實驗比較結果如表 1 所示。

表 1、DLE Method 與 Proposed Method 比較表

方法 圖片	DLE Method		Proposed Method	
	PSNR	藏量	PSNR	藏量
Babala	46.3736	393444	40.0128	524288
GoldHill	46.3521	392797	40.0439	524288
Jet(F16)	46.3779	393338	40.0120	524288
Lena	46.3780	393295	40.0273	524288
Baboon	46.3846	393408	40.0502	524288
平均	46.3732	393256	40.0292	524288

其 DLE Method 與本篇論文所提出之改善 DLE 之高藏量資料隱藏法在嵌入資料後其影像結果如圖一所示。經由圖一可以看出在提升嵌入的資訊量後其影像的品質 (平均的 PSNR 值仍有 40dB 之高)，對於人類的眼睛而言，是無法分辨出影像中實則已因隱入機密資訊而造成的奇些微的變化，故此圖提供本方法實則具有良好的隱蔽效果。



(a) PSNR=46.3736dB



(b) PSNR=40.0128dB



(c) PSNR=46.3521dB



(d) PSNR=40.0439dB



(e) PSNR=46.3779dB



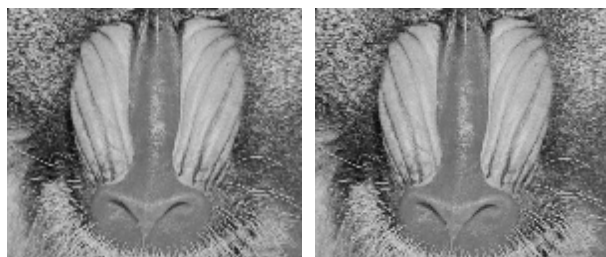
(f) PSNR=40.0120dB



(g) PSNR=46.3780dB



(h) PSNR=40.0273dB



(i) PSNR=46.3846dB (j) PSNR=40.0502dB
圖一、 DLE Method 與 Proposed Method 比較圖

5. 結論

影像的視覺品質及影像的資訊攜帶量一直是一個取捨的問題，對於 Zhang *et al.* 學者所提出的 DLE 方法進行改進。本研究提出的高藏量隱藏法，利用 DLE 方法藏入後所剩餘的藏入空間進行再次藏入的動作，有效的提高藏入量提高達約四分之一。對於這樣的提昇，影像的視覺品質並沒有損失太多，還在合理的人類視覺品質範圍之內。

參考文獻

- [1] 呂慈純、陸哲明、張真誠，*多媒體安全技術*，全華圖書股份有限公司，2007。
- [2] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE Transactions on*

Signal Processing, Vol. 53, No. 10, pp. 3923-3935, 2005.

- [3] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Wet paper codes with improved embedding efficiency," *IEEE Transactions on Information Forensics and Security*, Vol. 1 No. 1, pp. 102-110, 2006.
- [4] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, Vol. 13, No. 5, pp. 285-287, 2006.
- [5] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communication Letters*, Vol. 10, No. 11, pp. 781-783, 2006.
- [6] X. Zhang, W. Zhang, and S. Wang, "Efficient double-layered steganographic embedding," *Electronics Letters*, Vol. 43, No. 8, pp. 482-483, 2007.
- [7] W. Zhang, X. Zhang, and S. Wang, "A double layered "plus-minus one" data embedding scheme," *IEEE Signal Processing Letters*, Vol. 14, No. 11, pp. 848-851, 2007.