

高藏入效率的雙影像可逆式資訊隱藏技術

呂慈純
朝陽科技大學
資訊管理系副教授
tclu@cyut.edu.tw

許永明
朝陽科技大學
資訊管理系研究生
persevere1104@gmail.com

黃英軒
國立中興大學
資訊科學與工程學系研究生
phd9807@cs.nchu.edu.tw

摘要

近年來，許多專家學者提出可逆式資訊隱藏技術來保護資料，如：Lee 和 Huang 學者於 2011 年提出了一個雙影像可逆式資訊隱藏技術，該技術進行藏入動作時，僅會對像素進行加減 1 之修改，故可得到一張高品質的偽裝影像，然而，此方法每四個像素僅能藏入五個機密位元，藏入量仍有改善的空間，因此本論文提出一個高藏入效益的雙影像技術方法，所提方法對每個像素可藏入 T 個機密位元，其中 T 為一個自適應的門檻值，故能藉由 T 控制藏入量和偽裝影像品質。實驗結果顯示所提方法除了達到 T 位元的藏入效益外，所產生的偽裝影像品質也優於 Lee 和 Huang 的方法。

關鍵詞：雙影像可逆式資訊隱藏技術、偽裝影像、藏入量、自適應門檻值。

Abstract

In recent years, many scholars have proposed the reversible information hiding methods to protect the confidential data. For example, Lee and Huang proposed a reversible information hiding method in 2011. They modify the pixel by adding or subtracting one to embed secret data. Consequently, the quality of stego image obtained by the above modification rules is excellent. However, in their method, each set of four pixels can be used to embed five secret bits, thereby the rule restricting the hiding capacity. In this paper, we proposed a reversible information hiding method with high embedding rate to improve the drawback of Lee and Huang's method. In our method, each pixel can embed T secret bits, where T is an adaptive threshold and is used to control the image quality and hiding capacity. Experimental results show that the embedding rate of the proposed method achieves T bpp, which is better than that of the recently proposed methods.

Keywords: reversible information hiding method, stego image, hiding capacity, adaptive threshold

1. 前言

資訊隱藏(Data Hiding)是將機密資訊(Secret Data)藏入掩蔽影像(Cover Image)中，以得到一張偽裝影像(Stego Image)，由於偽裝影像與掩蔽影像是相似的，故人眼無法分辨影像是否攜帶機密資訊，因此該技術可有效保護資料。資訊隱藏技術可分為不可逆式資訊隱藏(Non-Reversible Data Hiding)[1-3]與可逆式資訊隱藏(Reversible Data Hiding) [4-8]，不可逆式資訊隱藏技術可有效藏入與取出機密資訊，但無法還原掩蔽影像；相反地，可逆式資訊隱藏技術除了可藏入與取出機密資訊，亦能無失真地還原掩蔽影像，故可逆式的資訊隱藏技術可應用於不容許失真的領域，如國防的機密文件、醫學影像及高價值文物保存等。

一個好的資訊隱藏技術須滿足三個要點：安全性(Security)、不可察覺性(Imperceptivity)和高資訊負載量(Payload)之要求。安全性意指除了擁有金鑰者，其他人無法從偽裝影像中取得機密資訊。不可察覺性是指偽裝影像不能有嚴重的像素失真問題，以避免惡意人士的懷疑與攻擊，換言之，不法第三者(Third Party)無從鑑別出偽裝影像與原始影像的差異。高資訊負載量是指在一個高水準的偽裝影像品質要求下，盡可能藏入機密資訊。

2003 年，Tian 等學者提出了一個差值擴張(Difference Expansion, DE)的可逆式資訊隱藏技術 [7]，該技術首先計算兩個相鄰像素 a 和 b 的平均值 m 和差值 d ，即 $m = \lfloor (a+b)/2 \rfloor$ 和 $d = a - b$ 。接下來，將差值 d 擴張成 2 倍，並將機密位元 s 嵌入於兩倍擴張後的差值中，即 $d' = 2d + s$ ，其中 $s \in \{0, 1\}$ 。最後，使用修改後的差值 d' 與平均值 m 計算出偽裝像素 (a', b') ，即 $a' = m + \lfloor (d'+1)/2 \rfloor$ 和 $b' = m - \lfloor d'/2 \rfloor$ 。此方法雖然簡單，然而，在差

值 d 擴張為 2 倍時，較大的差值會產生嚴重的失真，導致像素可能有溢位或下溢問題 (Overflow or Underflow Problem)，故該方法須要一張位置圖 (Location Map) 以紀錄二個像素是否擴張方式藏入訊息。該位置圖須嵌入於影像中，導致藏入量和偽裝影像品質同時下降。

為了解決上述問題，2006 年 Ni 等學者提出一個植基於像素直方圖 (Pixel Histogram) 之可逆式資訊隱藏的方法 [6]。該方法根據原始影像的像素值出現次數來製成一張直方圖，並於直方圖中尋找峰值 (Peak Point)，以藏入機密資訊。該方法當像素峰值出現次數不高時，便無法藏入大量機密資訊。

為了解決上述問題，Lee 和 Huang 學者於 2011 年提出一個雙影像可逆式資訊隱藏的方法 [5]。該方法先將掩蔽影像複製一份，依據欲藏入的機密資訊和事先建立的藏入規則來修改像素，即完成藏入機密資訊。此方法在藏入機密資訊的過程中，僅進行加減 1 之修改，故可得到高品質的偽裝影像。然而此方法對四個像素僅能藏入五個機密位元，藏入量仍有改善空間。

為了改善 Lee 和 Huang 學者的方法，本論文提出一個高藏入效益的雙影像可逆式資訊隱藏方法，本方法能藏入 T 個機密位元於像素中，其中 $1 \leq T \leq L$ ， L 為像素的位元數目，當門檻值 T 愈大時，可藏入的機密數量愈大；反之，當 T 愈小時，可藏入的機密數量愈小，然而其偽裝影像品質可大幅提升。如上所述，所提方法因此擁有自適性門檻值、高藏入效率及良好的偽裝影像品質等效能。

2. 文獻探討

本章節闡述近期學者所提的無失真資訊隱藏方法，包含差值擴張技術 [7]、Lee 和 Huang 的雙影像藏入方法 [5]、直方圖的藏入方法 [6]。

2.1 差值擴張技術 [7]

Tian 學者於 2003 年提出了一個差值擴張的可逆式資訊隱藏方法，該方法屬於空間域 (Spatial Domain) 的隱藏技術，其藏入演算法如下所示：

步驟 1: 取出二個相鄰的掩蔽像素 (a, b)。

步驟 2: 計算二個掩蔽像素 (a, b) 的平均值 m ，

$$\text{即 } m = \left\lfloor \frac{a+b}{2} \right\rfloor。$$

步驟 3: 計算二個掩蔽像素的差值 d ，其公式為 $d = a - b$ 。

步驟 4: 擴張差值 d 成兩倍，再將機密資訊 s 嵌入於擴張後的差值中，即 $d' = 2d + s$ ，其中 $s \in \{0, 1\}$ 。

因擴張二倍後的差值必為偶數，故機密資訊“0”嵌入於偶數時，其值會維持為偶數；若嵌入的機密資訊為“1”時，差值就會被修改為奇數。故在取出階段時，接收者只需計算兩個相鄰像素之差值的最不重要位元 (Least Significant Bit, LSB)，便能得到所嵌入的機密訊息。

步驟 5: 將平均值 m 和藏入機密資訊後的差值 d' 代入公式

$$a' = m + \left\lfloor \frac{d'+1}{2} \right\rfloor \text{ 和 } b' = m - \left\lfloor \frac{d'}{2} \right\rfloor。 \quad (1)$$

，以得到二個偽裝像素 a' 和 b' 。

2.2 直方圖的可逆式資訊隱藏技術 [6]

Ni 等人於 2006 年提出一個直方圖可逆式資訊隱藏技術，該技術統計掩蔽像素的出現次數，並根據像素的出現次數製成一張直方圖。在直方圖中，他們找出多個峰值和零點 (Zero Point) 配對，其中峰值 p 是掩蔽影像中出現最多的像素值，零點 z 是掩蔽影像中出現最少次的像素值。為了騰出一個空間用來藏機密資訊，當 $p < z$ 時，將所有界於 $p+1$ 至 z 的像素皆向右位移一個單位，換言之，該步驟是將像素值進行加 1 之修改；當 $p > z$ 時，界於 $p-1$ 和 z 的像素值皆向左位移一個單位，即像素值進行減 1 之修改。完成上述步驟後，等於峰值的像素可用來藏機密資訊，當機密資訊 s 為 1 時，則像素值加 1 (或減 1)，否則，當機密資訊 s 為 0 時，像素則維持不變。

直方圖隱藏技術的演算法如下所示：

步驟 1: 統計原始影像 I 中的像素值 x 出現次數，以產生一張像素直方圖 $H(x)$ ，其中像素值 $x \in \{0, 1, \dots, 255\}$ 。

步驟 2: 在直方圖 $H(x)$ 中，尋找一個峰值 p 和零點 z ，其中 $p, z \in \{0, 1, \dots, 255\}$ 。

步驟 3: 修改界於峰值 p 至零點 z 之間的像素值 x ，其公式如下: (a) 若 $p > z$ 且 $p < 0$ ，則表示峰值位於零點之右方，則 $x = x - 1$ ；(b) 若 $p < z$ 且 $p \geq 0$ ，則表示峰值在零點之左方，則 $x = x + 1$ 。

步驟 4: 將機密訊息藏入等於峰值 p 的像素中，其藏入方法如下：如果藏入資訊 s 為 0，則像素值 x 不進行任何修改；

反之，若藏入資訊 s 為 1 且 $p < z$ ，則像素值 x 加 1，即 $x = x + 1$ ；否則，若藏入資訊 s 為 1 且 $p > z$ ，則像素值 x 減 1，即 $x = x - 1$ 。

步驟 5: 輸出偽裝影像 I' 、峰值 p 及零點 z 。

2.3 雙影像可逆式資訊隱藏技術 [5]

Lee 和 Huang 學者[5]在 2011 年提出一個雙影像的可逆式資訊隱藏方法，其藏入演算法如下所示。

步驟 1: 將 n 個機密位元 $\{s_1, s_2, \dots, s_n\}$ 轉換為十進制值 V ，其中 n 的初始值被設為 5。若 $V > 24$ ，則 $n = n - 1$ 。

步驟 2: 將十進制值 V 轉換為二個五進制值，即 v_1 和 v_2 ，其中 v_1 和 v_2 即為要藏入的機密符號。

步驟 3: 從掩蔽影像中取出二個像素(即 a 和 b)，並將該像素複製一份，即 $a1 = a$ 和 $b1 = b$ 。

步驟 4: 使用藏入規則將 v_1 和 v_2 嵌入於四個像素中($a, b, a1, b1$)，其藏入規則如表 1 所示，其中 a' 和 b' 為第一張偽裝影像的二個像素值； $a1'$ 和 $b1'$ 為第二張偽裝影像的二個像素值。

我們以一個例子來說明，假設欲藏入的機密資訊 $w = (17)_{10}$ ，將 w 轉成五進制的值得到 $V = (17)_{10} = (32)_5$ ，第一個數值即為 $v_1 = 3$ ，第二個數值為 $v_2 = 2$ 。若掩蔽影像的像素值為 $(a, b) = (93, 76)$ ，則將像素值複製一份得到 $(a1, b1) = (93, 76)$ ，則第一個機密符號為 $v_1 = 3$ ，由表查出 v_1 為 3 時， $a' = a + 1$ ， $b' = b + 1$ ，在 $v_1 = 3$ 的情況下， $v_2 = 2$ 時， $a1' = a - 1$ ， $b1' = b$ ，因此， $a' = 93 + 1 = 94$ ， $b' = 76 + 1 = 77$ ， $a1' = 93 - 1 = 92$ ， $b1' = 76$ 。

3. 所提方法

Lee 和 Huang 學者的雙影像資訊隱藏方法 [5] 每 4 個掩蔽像素最多能嵌入 5 個機密位元，故該方法的最大藏入率和藏入量分別為 $\frac{5}{4}$ (Bit

Per Pixel, bpp) 和 $2 \times \frac{5}{4} \times W \times H$ 個位元，其中 W

和 H 分別為影像的寬和高。若欲藏入的機密資訊大於最大藏入量，則該方法為了藏入機密資訊會額外產生 $2k$ ($2 \leq k < \infty$) 張偽裝影像，導致偽裝影像的數量增加，故本研究提出一個高藏入量的可逆式資訊隱藏方法來解決此問題，所

提方法對每個掩蔽像素能嵌入 T 個位元，其中 $0 \leq T \leq L$ ， L 為像素的位元數目。此外，所提方法處理像素溢位問題的機制是利用 Lee[5] 等學者所提方向進一步發展而成的，該機制之優點是無須記錄位置圖 (Location Map) 和額外資訊 (Extra Data)，故所提方法可達到高藏入率。

本章節架構茲分述如下：子章節 3.1 和 3.2 分別闡述藏入演算法與取出和還原演算法；子章節 3.3 說明像素溢位問題和解決機制。

3.1 藏入演算法

輸入：掩蔽影像 I 、機密資訊 S 及門檻值 T 。

輸出：二張偽裝影像 ($SI-1$ 和 $SI-2$)。

步驟 1: 從機密資訊 S 取出 T 個機密位元 s_l ($l = 1, 2, \dots, T$)，並將其轉換成 10 進制之值 V 。

步驟 2: 從掩蔽影像 I 取出一個像素 $x_{(i,j)}$ ，其中 $1 \leq i \leq W$ 、 $1 \leq j \leq H$ 及 W 和 H 分別表示影像之寬和高。

步驟 3: 藉由公式 $x1'_{(i,j)} = x_{(i,j)} - \lfloor V/2 \rfloor$ 和 $x2'_{(i,j)} = x_{(i,j)} + \lceil V/2 \rceil$ ，得到二個偽裝像素 $x1'_{(i,j)}$ 和 $x2'_{(i,j)}$ 。

假設掩蔽影像 I 為 $\{91, 90\}$ 、機密資訊 S 為 $\{0, 1, 1, 0\}$ 及門檻值 T 為 2。首先，我們取出二個機密位元 $\{0, 1\}$ ，將其轉成十進制之機密資訊 $V = (01)_2 = (1)_{10}$ ，接下來，我們將第一個掩蔽像素 $x_{(1,1)} = 91$ 和十進制之機密資訊 $V = 1$ 代入公式 $x1'_{(1,1)} = 91 - \lfloor 1/2 \rfloor = 91$ 和 $x2'_{(1,1)} = 91 + \lceil 1/2 \rceil = 92$ ，得到二個偽裝像素 $x1'_{(1,1)} = 91$ 和 $x2'_{(1,1)} = 92$ 。第 3 至第 4 個機密位元為 $\{1, 0\}$ 和其轉換後的十進制值為 $V = 2$ ，我們將第二個掩蔽像素 $x_{(1,2)} = 90$ 和十進制的機密資訊 $V = 2$ 代入公式以求得偽裝像素，即 $x1'_{(1,2)} = 90 - \lfloor 2/2 \rfloor = 89$ 和 $x2'_{(1,2)} = 90 + \lceil 2/2 \rceil = 91$ 。經過上述藏入過程後，我們可得到二張偽裝影像 $SI-1 = \{91, 89\}$ 和 $SI-2 = \{92, 91\}$ 。

表 1 Lee 和 Huang 學者所提的藏入規則

| v_1 | a' | b' | v_2 | $a1'$ | $b1'$ |
|-------|-------|-------|-------|-------|-------|
| 0 | a | b | 0 | a | b |
| | | | 1 | $a-1$ | $b-1$ |
| | | | 2 | $a-1$ | $b+1$ |
| | | | 3 | $a+1$ | $b+1$ |
| | | | 4 | $a+1$ | $b-1$ |
| 1 | $a-1$ | $b-1$ | 0 | a | $b+1$ |
| | | | 1 | $a-1$ | b |
| | | | 2 | $a+1$ | $b+1$ |
| | | | 3 | $a+1$ | b |
| | | | 4 | $a+1$ | $b-1$ |
| 2 | $a-1$ | $b+1$ | 0 | $a+1$ | b |
| | | | 1 | $a+1$ | $b-1$ |
| | | | 2 | a | $b+1$ |
| | | | 3 | a | $b-1$ |
| | | | 4 | $a-1$ | $b-1$ |
| 3 | $a+1$ | $b+1$ | 0 | a | $b-1$ |
| | | | 1 | $a-1$ | $b-1$ |
| | | | 2 | $a-1$ | b |
| | | | 3 | $a+1$ | b |
| | | | 4 | $a-1$ | $b+1$ |
| 4 | $a+1$ | $b-1$ | 0 | $a-1$ | b |
| | | | 1 | $a-1$ | $b+1$ |
| | | | 2 | a | $b+1$ |
| | | | 3 | $a+1$ | $b+1$ |
| | | | 4 | a | $b-1$ |

3.2 取出和還原演算法

輸入：二張偽裝影像($SI-1$ 和 $SI-2$)和門檻值 T 。

輸出：掩蔽影像 I 和機密資訊 S 。

步驟 1：從二張偽裝影像分別取出一個像素，即 $x1'_{(i,j)}$ 和 $x2'_{(i,j)}$ 。

步驟 2：計算二個偽裝像素的絕對差值，以取出十進制之機密資訊 V ，即

$$V = |x1'_{(i,j)} - x2'_{(i,j)}|。$$

步驟 3：將十進制的機密資訊 V 轉換成 T 個機密位元 S_i 。

步驟 4：計算二個偽裝像素的平均值，以還原掩蔽像素 $x_{(i,j)}$ ，即 $x_{(i,j)} = \lfloor (x1'_{(i,j)} + x2'_{(i,j)})/2 \rfloor$ 。

沿續藏入的例子，二張偽裝影像分別為 $SI-1 = \{91, 89\}$ 和 $SI-2 = \{92, 91\}$ 及門檻值 T 為 2。首先，我們取出二張偽裝影像的第一個像素，其值分別為 $x1'_{(1,1)} = 91$ 和 $x2'_{(1,1)} = 92$ ，接下來，我們計算二個像素的絕對差值，以取出十進制之機密資訊，即 $V = |x1'_{(1,1)} - x2'_{(1,1)}| = |91 - 92| = 1$ ，再將十進制之機密資訊 $V = 1$ 轉換成 2 個機密位元 $\{0, 1\}$ 。另一方面，為了還原掩蔽像素，我們計算二個偽裝像素的平均值，即 $x_{(1,1)} = \lfloor (91 + 92)/2 \rfloor = 91$ 。二張偽裝影像的第二個像素分別為 $x1'_{(1,2)} = 89$ 與 $x2'_{(1,2)} = 91$ ，其絕對差值即為十進制之機密資訊，即 $V = |89 - 91| = 2$ ，接下來，我們將十進制之機密資訊 $V = 2$ 轉成 2 個機密位元 $\{1, 0\}$ ，便完成取出機密位元之過程。最後，為了還原掩蔽像素 $x_{(1,2)}$ ，我們計算二個偽裝像素的平均值 $x_{(1,2)} = \lfloor (89 + 91)/2 \rfloor = 90$ 。經由上述取出和還原過程，我們可得到掩蔽影像 $I = \{91, 90\}$ 與加密後的機密資訊 $S = \{0, 1, 1, 0\}$ 。

3.3 溢位問題處理機制

在藏入機密資訊的過程中，每個像素進行減 $\lfloor V/2 \rfloor$ 或加 $\lceil V/2 \rceil$ 之修改，故掩蔽像素若界於 $[0, \lfloor V/2 \rfloor]$ 和 $[255 - \lceil V/2 \rceil, 255]$ 二區間時，則可能會產生像素溢位問題。若發生此問題時，則像素不藏入任何機密資訊，並且讓 $x1'_{(i,j)}$ 等於原始像素值 $x_{(i,j)}$ ，而 $x2'_{(i,j)}$ 則視 $x_{(i,j)} + \max\{V\} + 1$ 是否會大於 255，若 $x_{(i,j)} + \max\{V\} + 1$ 小於 255，則 $x2'_{(i,j)} = x_{(i,j)} + \max\{V\} + 1$ ，否則 $x2'_{(i,j)} = x_{(i,j)} - \max\{V\} - 1$ 。

當我們收到偽裝像素 $x1'_{(i,j)}$ 和 $x2'_{(i,j)}$ ，若 $|x1'_{(i,j)} - x2'_{(i,j)}| = \max\{V\} + 1$ ，則我們得知該像素無藏入任何機密資訊，此外， $x1'_{(i,j)}$ 即為原始像素。

4. 實驗結果

我們實作了 Lee 等學者的方法[4]、Lee 和 Huang 學者的方法[5]、Ni 等學者的方法[6]及 Tsai 等學者的方法[8]，為了比較其效能，我們分別採用嵌入率(Embedding Rate, ER)和高峰影像信號雜訊比(Peak Signal to Noise Ratio, PSNR)來評估藏入量和偽裝影像品質，其公式如下：

$$ER = \frac{\text{\# of secret data}}{W \times H}, \quad (2)$$

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right) \text{ (dB)}, \quad (3)$$

$$MSE = \frac{1}{W \times H} \sum_{i=1}^H \sum_{j=1}^W (x'_{(i,j)} - x_{(i,j)})^2 \text{ (bpp)}, \quad (4)$$

其中，MSE 為偽裝影像與原始影像的均方誤差 (Mean Squared Error)、 H 和 W 分別為影像的高

和寬。

圖 1 顯示當門檻值 T 設為 4 時，每張偽裝影像品質皆大於 34 dB，且在視覺上，偽裝影像與掩蔽影像是相似的，此外，無論平滑影像 (例如：Lena 和 F-16) 或複雜影像 (Baboon 和 Barbara)，其藏入率皆可達到 1.99 bpp，故所提方法有良好的藏入率和偽裝影像品質。圖 2 (a)-(d) 顯示當門檻值愈大時，可藏入的機密資訊數量愈大，然而，當藏入量相同時，較小的門檻值可得到較好的偽裝影像品質，這是因為高門檻值僅使用圖像的一部份便完成藏入資訊，因此容易產生嚴重的像素失真問題，換言之，低門檻值是將機密資訊有效藏入至整張影像中，故像素破壞程度較小和偽裝影像品質較好。



掩蔽影像

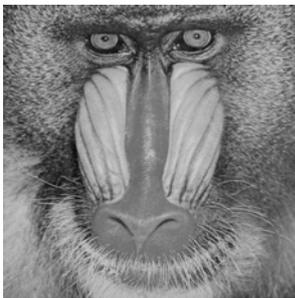


第一張偽裝影像
(2 bpp 和 35.688 dB)

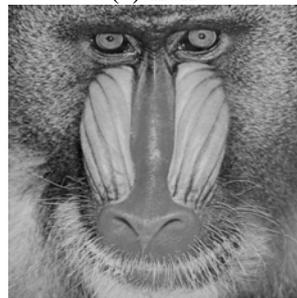


第二張偽裝影像
(2 bpp 和 34.792 dB)

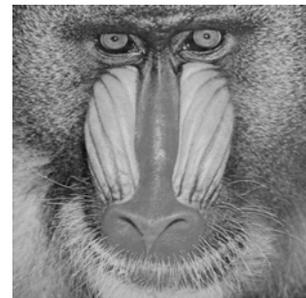
(a) Lena



掩蔽影像



第一張偽裝影像
(1.99 bpp 和 35.690 dB)



第二張偽裝影像
(1.99 bpp 和 34.797 dB)

(b) Baboon



掩蔽影像



第一張偽裝影像
(2 bpp 和 35.696 dB)



第二張偽裝影像
(2 bpp 和 34.798 dB)

(c) F-16



掩蔽影像



第一張偽裝影像
(2 bpp 和 35.699 dB)
(d) Barbara



第二張偽裝影像
(2 bpp 和 34.805 dB)



掩蔽影像



第一張偽裝影像
(2 bpp 和 35.709 dB)
(e) Boat



第二張偽裝影像
(2 bpp 和 34.815 dB)



掩蔽影像



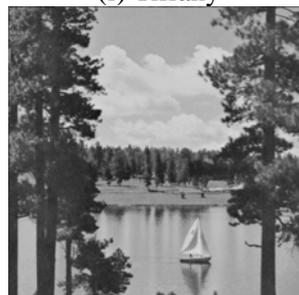
第一張偽裝影像
(2 bpp 和 35.687 dB)
(f) Tiffany



第二張偽裝影像
(2 bpp 和 34.794 dB)



掩蔽影像



第一張偽裝影像
(2 bpp 和 35.688 dB)
(g) Sailboat



第二張偽裝影像
(2 bpp 和 34.798 dB)



掩蔽影像



第一張偽裝影像
(2 bpp 和 35.699 dB)
(h) Goldhill



第二張偽裝影像
(2 bpp 和 34.803 dB)



掩蔽影像



第一張偽裝影像
(2 bpp 和 35.703 dB)
(i) Zelda



第二張偽裝影像
(2 bpp 和 34.811 dB)



掩蔽影像

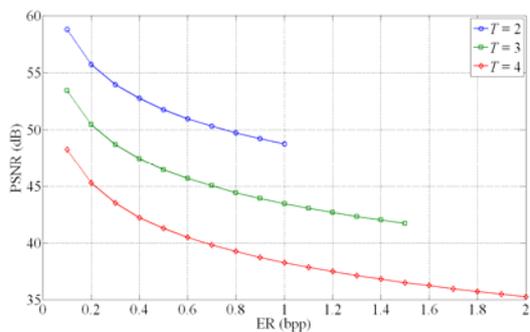


第一張偽裝影像
(1.99 bpp 和 35.698 dB)
(j) Pepper

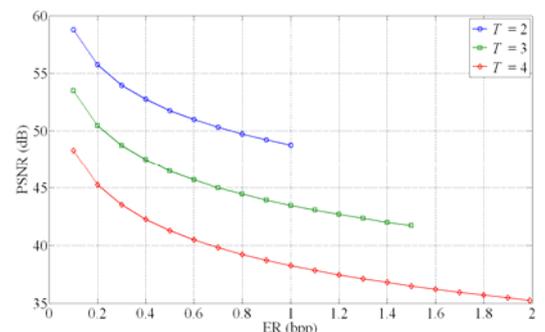


第二張偽裝影像
(1.99 bpp 和 34.744 dB)

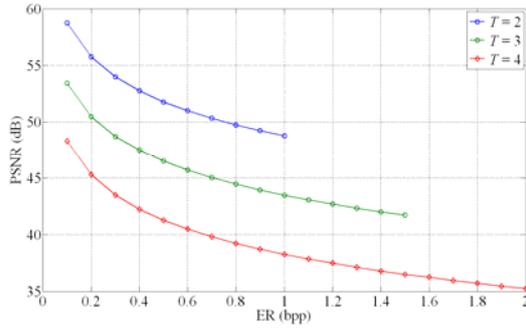
圖 1 掩蔽影像和偽裝影像



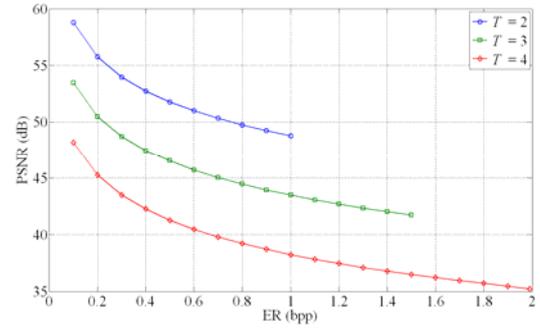
(a) Lena



(b) Baboon

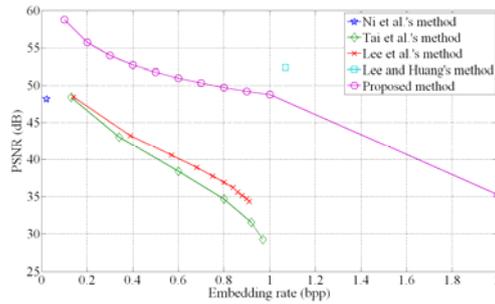


(c) Barbara

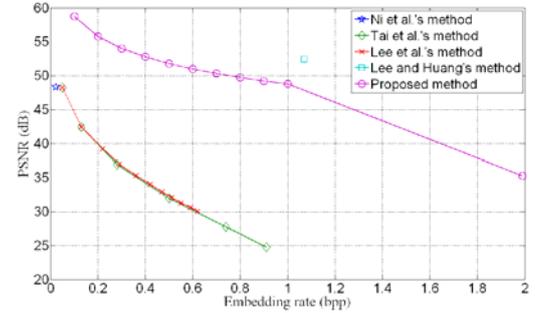


(d) Pepper

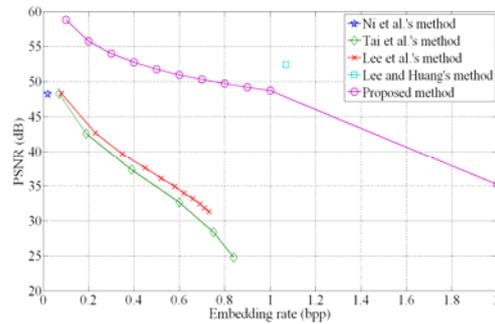
圖 2 不同門檻值所對應的可藏入量和偽裝影像品質



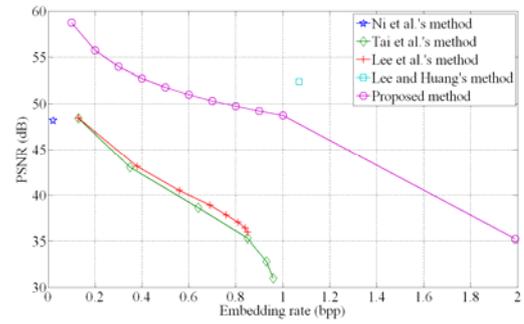
(a) Lena



(b) Baboon



(c) Barbara



(d) Pepper

圖 3 所提方法與近年來的方法之效能比較可藏入量和偽裝影像品質

圖 3(a)-(d)說明了所提方法的偽裝影像品質與藏入率皆優於 Lee 等學者方法 [4]和 Tai 等學者的方法[8]，這是因為他們的方法在藏入機密資訊過程中，將像素與其相鄰像素的差值擴張成 2 倍，故產生嚴重像素失真問題。另一方面，所提方法的影像品質和藏入量也高於像素直方圖方法[6]，其主要原因是像素直方圖方法僅使用等於峰值的像素來藏機密資訊，因而限制了藏入效率，同時，無法隱藏資訊的像素也須進行修改，進而降低了偽裝影像品質。在相同的藏入率下，所提方法的偽裝影像品質比 Lee 和 Huang 學者方法[5]的偽裝影像品質差，然而，我們方法的最大嵌入率比 Lee 和 Huang 學者方法高 0.92 bpp。綜合上述所言，所提方法具有高影像品質和藏入效益。

5. 結論

本文提出一個高藏入效率的雙影像可逆式資訊隱藏技術，該技術所產生的偽裝影像和可藏入量比近年來學者提出的方法好。本文所提出的方法對每個像素能藏入 T 個機密位元，其中 $1 \leq T \leq L$ ， L 為像素位元的數目，當門檻值 T 愈大時，可藏入的機密數量愈大；反之，當 T 愈小時，可藏入的機密數量愈小，然而偽裝影像品質較好，故所提方法擁有自適性門檻值、高藏入率及良好的偽裝影像品質等效能。

參考文獻

- [1] Chan, C. K. and Cheng, L. M., "Hiding Data in Images by Simple LSB Substitution,"

- Pattern Recognition*, Vol. 37, No. 3, pp. 469-474, 2004.
- [2] Kieu, T. D. and Chang, C. C., "A Steganographic Scheme by Fully Exploiting Modification Directions," *Expert Systems with Applications*, Vol. 38, pp. 10648-10657, 2011.
- [3] Lin, C. C., "An Information Hiding Scheme with Minimal Image Distortion," *Computer Standards & Interfaces*, Vol. 33, No. 5, pp. 477-484, 2011.
- [4] Lee, C. F., Chen, H. L. and Tso, H. K., "Embedding Capacity Raising in Reversible Data Hiding Based on Prediction of Difference Expansion," *Journal of Systems and Software*, Vol. 83, No. 10, pp. 1864-1872, 2010.
- [5] Lee, C. F. and Huang, Y. L., "Reversible Data Hiding Scheme Based on Dual Stegano-images Using Orientation Combinations," *Telecommunication Systems*, pp. 1-11, 2011.
- [6] Ni, Z. C., Shi, Y. Q., Ansari, N. and Su, W., "Reversible Data Hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 3, pp. 354-362, 2006.
- [7] Tian, J., "Reversible Data Embedding Using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890-896, 2003.
- [8] Tai, W. L., Yeh, C. M. and Chang, C. C., "Reversible Data Hiding Based on Histogram Modification of Pixel Differences," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 19, No. 6, pp. 906-910, 2009.