植基於整數轉換函式之可逆式資訊隱藏技術

呂慈純
朝陽科技大學資訊管理學系
e-mail：
tclu@cyut.edu.tw

蔡承翰
朝陽科技大學資訊管理學系
e-mail：
s9614632@cyut.edu.tw

摘要

本篇論文提出一個有效的可逆式資訊隱藏技術，所提出的方法主要改進 Alattar 等學者提出的整數轉換函式藏入法需要額外傳送對應表(Location Map)的缺點，利用鄰近的 4 個像素為一個區塊，計算每一個像素之間的差異值，再將機密訊息藏入。

關鍵詞：資訊隱藏，對應表，可逆式差異擴張技術。

Abstract

This paper proposes an efficiency reversible hiding scheme to improve Alattar et al.'s integer transform function hiding scheme, which needs a location map to recover the original image.

The proposed scheme uses four pixels in the nearby area to embed three message bits. The differences between neighboring pixels are expended to conceal the secret bits.

Keywords: Information Hiding, Location Map, secret message

1. 前言

由於數位科技與網際網路技術的蓬勃發展，世界已經走入了數位化的年代，網際網路的便利，帶動了數位資訊的交流，各種資訊以數位化的形式，透過網際網路可以迅速的傳送到世界各地，但是由於網際網路的發達，也帶來了許多安全上的新議題，例如：資料的竊取與竄改，智慧財產權的侵犯等，因此資訊安全的議題日漸受到重視，要如何確保數位資訊在網路上傳送時的安全性，已成為數位時代中的一項重要議題。

在資訊安全的領域中，資訊隱藏(Information Hiding)是除了資料加密技術之外，另一項保護數位資料傳輸安全的技術。資訊隱藏技術可以分為六大類[1]，其中包括了隱密通道(Cover Channels)、匿名(Anonymity)、隱藏學(Steganography)及著作權標記(Copyright Marking)，其中隱藏學主要是由希臘文字中的 Steganos 與 Graphein 兩個字結合而成，Steganos 所代表的意義是隱藏、遮蔽(Covered)，Graphein 則是有寫入的意思，兩個文字結合起來則有「隱藏所寫入的文字」之意義。由於資訊藏入的動作對於偽裝影像會造成影像品質的失真，因此學者提出了無失真資訊隱藏技術(Lossless Information Hiding)改善失真問題，此項技術又稱為可逆式資訊隱藏(Reversible Data Embedding)，常用於軍事以及醫學影像領域。Alattar 學者提出一個可逆式資訊隱藏技術，然而，由於他們的方法在復原影像時需要額外記錄資訊，造成傳輸上的負擔，因此本篇研究改進了 Alattar 學者的方法，利用像素之間的差異擴張計算藏入機密訊息(Secret Message)，需要的額外資訊較 Alattar 學者的方法少。

2. 相關技術

Celik等學者於 2002 年提出一個廣義最低位元藏入法(Generalized Least Significant Bit，G-LSB) [3]，將機密訊息藏入遮蔽影像中以產生偽裝影像。G-LSB在藏入機密訊息前，會先將原始影像經過公式

$$\hat{S}_i = \left\lfloor \frac{S_i}{q} \right\rfloor \times q \qquad (1)$$

進行量化，其中 S_i 為第 i 個像素，q 為量化間距，$\hat{S}_i$ 為量化後的像素。如圖1為遮蔽影像 S，經過量化後的量化影像 $Q(S)$ 如圖2。

32	37	28	26
21	30	11	17
29	15	9	24
33	27	31	20

圖 1 遮蔽影像 S

30	35	25	25
20	30	10	15
25	15	5	20
30	25	30	20

圖 2 量化影像 $Q(S)$

接著將機密訊息 W 表示為小數，再轉成十進制得到 W'。例如，機密訊息 $W=(1101)_2$，將 W 表示為小數位數 0.1101，再轉為十進制表示得到 $W'=(0.1101)_2=(0.8125)_{10}$。G-LSB藏入時需要一個區間量表進行資訊隱藏，區間量表是將 0 到 1 的數值平均切割為 5 個等份，如圖3所示，其中 R_0 為第 0 個區間，R_1 為第 1 個區間，以此類推。

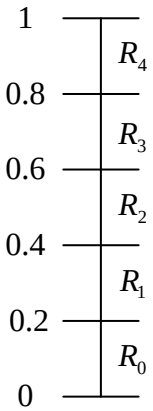

圖 3 比例區間量表

得到區間量表後，將機密訊息 W' 投入區間量表中，找出 W' 坐落的區間。上例中，$W'=(0.8125)_{10}$ 落在 R_4 區間中，偽裝影像將量化後的像素加上區間號碼。例如，原始影像中的第一個像素為 32，設量化間距為 5，像素量化後得到 30，加上機密訊息 W' 落在 R_4 區間，因此 $S_1'=30+4=34$。接著再以 R_4 區間為中心，平均切割為五個等份，如圖4，再將 W' 投入新的比例區間圖中，W' 落在 R_{40} 區間，第二個像素量化後為 35，因此，$S_2'=35+0=35$，以此類推，最後得到的偽裝影像 S'，如圖5所示。

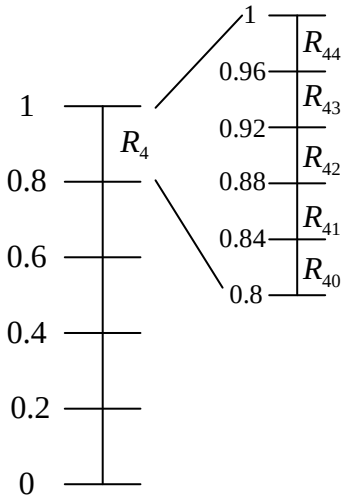

圖 4 R_4 的比例區間圖

34	35	26	27
20	30	10	15
25	15	5	20
30	25	30	20

圖 5 偽裝影像 S'

G-LSB藏入技術為失真式資訊隱藏技術，為了讓G-LSB達到無失真，Celik[2]等學者於 2005 年提出一個延伸G-LSB的無失真廣義最低位元藏入法(Lossless Generalized Least Significant Bit， Lossless G-LSB)。其方法是將G-LSB因為量化產生的失真記錄下來，即將遮蔽影像 S 與量化後的遮蔽影像 $Q(S)$ 相減，得到 S 與 $Q(S)$ 之間的差異 R，如圖6所示。

2	2	3	1
1	0	1	2
4	0	4	4
3	2	1	0

圖 6 S 與 $Q(S)$ 的差異圖 R

接著利用算術編碼壓縮法(Arithmetic Coding)將 R 壓縮成 $Comp(R)$ [5]， $Comp(R)$ 與機密訊息一併利用G-LSB的方法藏入遮蔽影像中。算術編碼壓縮 R 的過程中，需要先求出 R 中各數值出現的機率，再利用得到的機率進行編碼。由上例中得到的差異 R，可以算出各數值出現的機率如表1。

表 1 差異圖中各數值比例分析

數值	出現次數	機率
0	3	0.1875
1	4	0.25
2	4	0.25
3	2	0.125
4	3	0.1875

接著以每一數值出現的機率做成區間比例圖，如圖7，並將差異 R 中的值帶入比例區間圖中。圖6中第一個像素值為 2，為第二個區間 R_2，因此將 R_2 區間再以表1的機率分割為五份，將圖6中第二個像素值 2 帶入 R_2 區間，再進行分割，以此類推。假設做到第三次切割時停止，則從第三次切割的 R_3 區間中，任意挑選一個實數，設得到的數為 $(0.10365)_{10}$，將 $(0.10365)_{10}$ 轉為二進制得到 $(0.0001101)_2$，此即為壓縮結果。將得到的壓縮結果串接到機密資訊後，並以G-LSB的方式藏入遮蔽影像中。

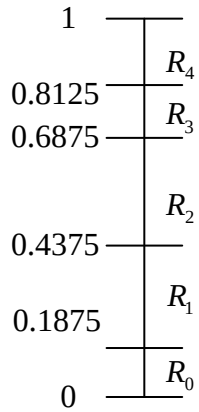

圖 7 R 的比例區間圖

接收方在得到偽裝影像後，首先進行量化的動作，接著將偽裝影像和量化後的影像相減，即可得到藏入偽裝影像的機密訊息以及壓縮過後的差異，接著利用區間比例圖可以還原原始的差異，利用差異即可還原原始遮蔽影像。

差異擴張法(Difference Expansion)為Tian所提出[4]，延伸G-LSB的可逆式資訊隱藏方法，其以兩個相鄰像素藏入一個位元。假設兩個相鄰像素為 $A=42$ 與 $B=32$ 藏入的機密訊息為 $W=1$。首先算出兩個像素的差異值 d 以及平均值 l，其計算式為 $d=A-B=42-32=10$，$l=\left\lfloor\frac{A+B}{2}\right\rfloor=\left\lfloor\frac{42+32}{2}\right\rfloor=37$。

接著將差異值擴張成二倍並將 W 藏入得到 d'，$d'=2\times d+W=2\times 10+1=21$，最後得到偽裝影像，$A'=l+\left\lfloor\frac{d'+1}{2}\right\rfloor=37+\left\lfloor\frac{21+1}{2}\right\rfloor=48$，$B'=l-\left\lfloor\frac{d'}{2}\right\rfloor=37-\left\lfloor\frac{21}{2}\right\rfloor=27$。當接收方要取出機密信息及還原像素值時，先計算相鄰偽裝像素值 A' 與 B' 之間的差異值 d' 與平均值 l，$d'=A'-B'=48-27=21$ 和 $l=\left\lfloor\frac{A'+B'}{2}\right\rfloor=\left\lfloor\frac{48+27}{2}\right\rfloor=37$，接著計算原始差異值 $d=\left\lfloor\frac{d'}{2}\right\rfloor=\left\lfloor\frac{21}{2}\right\rfloor=10$，找出原始差異值 d 後，可以用 d' 與 d 找出嵌入的機密訊息 $W=d'-d\times 2=21-20=1$，最後再將原始像素 A 與 B 還原，$A=l+\left\lfloor\frac{d+1}{2}\right\rfloor=37+\left\lfloor\frac{10+1}{2}\right\rfloor=42$、$B=l-\left\lfloor\frac{d}{2}\right\rfloor=37-\left\lfloor\frac{10}{2}\right\rfloor=32$。若能順利嵌入機密訊息的像素值稱為可擴張，然而，有些相鄰像素可能超過 255 或小於 0，此時則改以 $d'=2\times\left\lfloor\frac{d}{2}\right\rfloor+W$ 的方式將機密訊息藏入，若還是超過 255 或小於 0，則判斷為不可藏入。這三種不一樣的狀況分別稱為：可擴張的(Expandable)、可改變的(Changeable)以及不可改變的(Non-changeable)。當機密資訊藏入遮蔽影像後，需要產生一個對應表(Location Map)來記錄這三種不同的狀況，以還原原始像素，因此最後藏入遮蔽影像的內容，除了機密訊息

外，另外還需要藏入壓縮後的對應表。為了提高藏入量，Tian 採用多重藏入的方式，如此可提高資訊藏入量。實驗結果顯示，Tian 的方法在藏入量以及偽裝影像的品質都比 Lossless G-LSB 來的好。

2004 年，Alattar[1]為了提升Tian所提方法的資訊負載量，提出了一個可逆式整數轉換函式隱藏法(Generalized Integer Transform)，此方法運用四個鄰近像素藏入三個機密訊息。假設四個像素值分別為$u_1=11$、$u_2=15$、$u_3=16$以及$u_4=12$，機密訊息分別為$W_1=1$、$W_2=0$和$W_3=1$，首先計算權重平均值(Weighted Averages)v_1、v_2、v_3和v_4，其計算式為：

$$v_1=\left\lfloor\frac{a_1u_1+a_2u_2+a_3u_3+a_4u_4}{a_1+a_2+a_3+a_4}\right\rfloor$$
$$=\left\lfloor\frac{1\times11+2\times15+2\times16+1\times12}{1+2+2+1}\right\rfloor,$$
$$=14$$

$v_2=u_2-u_1=15-11=4$，

$v_3=u_3-u_1=16-11=5$ 和

$v_4=u_4-u_1=12-11=1$，

上述計算式中的a_1、a_2、a_3、a_4為四個常數值，本例中假設$a_1=1$、$a_2=2$、$a_3=2$和$a_4=1$，接著利用機密訊息調整權重平均值，

$\tilde{v}_1=v_1=14$，

$\tilde{v}_2=2\times v_2+W_1=2\times4+1=9$，

$\tilde{v}_3=2\times v_3+W_2=2\times5+0=10$ 和

$\tilde{v}_4=2\times v_4+W_3=2\times1+1=3$。

偽裝像素的計算為

$$u_1'=\tilde{v}_1-\left\lfloor\frac{a_2\tilde{v}_2+a_3\tilde{v}_3+a_4\tilde{v}_4}{a_1+a_2+a_3+a_4}\right\rfloor=8,$$

$u_2'=\tilde{v}_2+u_1'=9+8=17$，

$u_3'=\tilde{v}_3+u_1'=10+8=18$ 和

$u_4'=\tilde{v}_4+u_1'=3+8=11$。

在取出過程中，首先計算偽裝像素的平均值及差異值，

$$\hat{v}_1=\left\lfloor\frac{a_1u_1'+a_2u_2'+a_3u_3'+a_4u_4'}{a_1+a_2+a_3+a_4}\right\rfloor$$
$$=\left\lfloor\frac{1\times8+2\times17+2\times18+1\times11}{1+2+2+1}\right\rfloor$$
$$=14$$

$\hat{v}_2=u_2'-u_1'=17-8=9$，

$\hat{v}_3=u_3'-u_1'=18-8=10$ 和

$\hat{v}_4=u_4'-u_1'=11-8=3$。

由平均值找出機密訊息，

$W_1=\hat{v}_2-\left\lfloor\frac{\hat{v}_2}{2}\right\rfloor=9-8=1$，

$W_2=\hat{v}_3-\left\lfloor\frac{\hat{v}_3}{2}\right\rfloor=10-10=0$ 和

$W_3=\hat{v}_4-\left\lfloor\frac{\hat{v}_4}{2}\right\rfloor=3-2=1$。

還原原始像素則計算權重平均值，

$v_1=\hat{v}_1=14$，

$v_2=\left\lfloor\frac{\hat{v}_2}{2}\right\rfloor=\left\lfloor\frac{9}{2}\right\rfloor=4$，

$v_3=\left\lfloor\frac{\hat{v}_3}{2}\right\rfloor=\left\lfloor\frac{10}{2}\right\rfloor=5$ 和

$v_4=\left\lfloor\frac{\hat{v}_4}{2}\right\rfloor=\left\lfloor\frac{3}{2}\right\rfloor=1$，

再利用v_1、v_2、v_3和v_4還原原始像素值，

$$u_1=v_1-\left\lfloor\frac{a_2v_2+a_3v_3+a_4v_4}{a_1+a_2+a_3+a_4}\right\rfloor=11,$$

$u_2=v_2+u_1=4+11=15$，

$u_3=v_3+u_1=5+11=16$ 和

$u_4=v_4+u_1=1+11=12$。

此方法同樣會面臨有些像素無法擴張的問題，而必須改用可改變的方式藏入資訊或根本無法藏入。因此，Alattar 所提出的方法也必須使用對應表來記錄哪些像素可以擴張，比較 Tian 的方法，Alattar 的方法能夠藏入更多的機密訊息，而偽裝影像的品質也較 Tian 的方法好。

3. 四倍差異擴增技術

為了改善 Alattar 需要對應表的缺點，本研究提出了一個利用奇偶數來判斷是否藏入隱藏訊息的方法，用以減少需額外傳送對應表的

缺點。詳細的嵌入與取出步驟，將於 3.1 節以及 3.2 節中介紹。

3.1 嵌入過程

步驟 1：將遮蔽影像(Cover Image)切割為 2×2 大小的遮蔽矩陣 I，如圖8，每一個像素分別設為 A、B、C、D。

A	B
C	D

圖 8 矩陣 I

步驟 2：利用 A、B、C、D，進行差異擴張算出 $\overline{A}$、$\overline{B}$、$\overline{C}$ 和 $\overline{D}$，其運算式如下：

$$\overline{A}=4\times A-(B+C+D),$$
$$\overline{B}=4\times B-(A+C+D),$$
$$\overline{C}=4\times C-(A+B+D),$$
$$\overline{D}=4\times D-(A+B+C), \quad (1)$$

接著再利用產生出來的差異值，以 $\overline{A}$ 為基底分別與 $\overline{B}$、$\overline{C}$、$\overline{D}$ 相減，產生 $\overline{A}$ 與 $\overline{B}$、$\overline{C}$、$\overline{D}$ 之間的差異值 T_1、T_2、T_3，運算式如下：

$$T_1=\left|\overline{A}-\overline{B}\right|,$$
$$T_2=\left|\overline{A}-\overline{C}\right|,$$
$$T_3=\left|\overline{A}-\overline{D}\right|. \quad (2)$$

步驟 3：利用得到的 T_1、T_2、T_3 進行判斷，φ 定義為一門檻值 (Threshold)，若 $\varphi<T_1$、T_2、T_3，此矩陣 I 不能藏機密訊息，則將 A' 設為奇數 $A'=2\times\left\lfloor\frac{A}{2}\right\rfloor+1$，並且

$$B'=B,$$
$$C'=C,$$
$$D'=D. \quad (3)$$

接著把原始像素 A 的最低有效位元 (Least Significant Bit，LSB)記錄起來，令Original LSB為 A 的LSB。A'、B'、C'、D' 為偽裝像素，形成偽裝矩陣 I'，如圖9。回到步驟一繼續下一個矩陣

A'	B'
C'	D'

圖 9 矩陣 I'

步驟 4：若矩陣符合 $\varphi>T_1$、T_2、T_3，則判斷 A、B、C、D 之中是否有偶數存在，假使其中有一個或以上的偶數，則將機密訊息 W_1、W_2、W_3 藏入 $\overline{A}$、$\overline{B}$、$\overline{C}$ 和 $\overline{D}$ 中，得到 A'、B'、C'、D'，

$$A'=2\times\left\lfloor\frac{\overline{A}}{2}\right\rfloor,$$
$$B'=2\times\left\lfloor\frac{\overline{B}}{2}\right\rfloor+W_1,$$
$$C'=2\times\left\lfloor\frac{\overline{C}}{2}\right\rfloor+W_2 \text{ 和}$$
$$D'=2\times\left\lfloor\frac{\overline{D}}{2}\right\rfloor+W_3. \quad (4)$$

若 A、B、C、D 皆為奇數，則直接將機密訊息藏入原始遮蔽影像像素值的 LSB，得到 A'、B'、C'、D'，運算式如下：

$$A'=A,$$
$$B'=2\times\left\lfloor\frac{B}{2}\right\rfloor+W_1,$$
$$C'=2\times\left\lfloor\frac{C}{2}\right\rfloor+W_2 \text{ 和}$$
$$D'=2\times\left\lfloor\frac{D}{2}\right\rfloor+W_3. \quad (5)$$

步驟 5：利用步驟 4 得到的 A'、B'、C'、D' 判斷是否大於 255 或者小於 0，並代入取出步驟，計算是否能夠順利取出。

- 若 A'、B'、C'、D' 皆未大於 255 與小於 0，並能夠順利取出，則將 A'、B'、C'、D' 當作嵌入最後結果；
- 若 A'、B'、C'、D' 的值大於 255 或小於 0，且不能順利取出，則將此區塊當作不能藏，跳回步驟 3，將區塊利用步驟 3 做計算。

詳細的取出步驟將在下一節作介紹。

步驟 6：回到步驟 1 繼續下一個矩陣，直到完成所有矩陣。

再舉一個例子，說明嵌入過程。假設要藏入的訊息為，$W_1=1$、$W_2=1$、$W_3=0$，門檻值為 $\varphi=20$，2×2 的矩陣 I 如圖10。

26	31
41	36

圖 10 2×2 範例矩陣 I

利用 A、B、C、D 進行差異擴張的運算得到

$$\overline{A}=4\times32-(33+35+34)=26,$$

$$\overline{B}=4\times33-(32+35+34)=31,$$

$$\overline{C}=4\times35-(32+33+34)=41 \text{ 和}$$

$$\overline{D}=4\times34-(32+33+35)=36。$$

再利用 $\overline{A}$ 為基底分別與 $\overline{B}$、$\overline{C}$、$\overline{D}$ 相減，產生差異值 T_1、T_2、T_3，

$$T_1=|26-31|=5,$$

$$T_2=|26-41|=15 \text{ 和}$$

$$T_3=|26-36|=10。$$

判斷 T_1、T_2、T_3 是否大於門檻值 φ，此例中，我們假設門檻值為 20，則 $20>T_1$、T_2、T_3。接著分析矩陣內是否有偶數存在，因為 A 和 D 為偶數，因此將機密訊息 W_1、W_2、W_3 藏入 $\overline{B}$、$\overline{C}$、$\overline{D}$ 中得到 A'、B'、C'、D'，再將 $\overline{A}$ 轉為偶數，表示矩陣內至少有一個數值為偶數，

$$A'=2\times\left\lfloor\frac{26}{2}\right\rfloor=26,$$

$$B'=2\times\left\lfloor\frac{31}{2}\right\rfloor+1=31,$$

$$C'=2\times\left\lfloor\frac{41}{2}\right\rfloor+1=41 \text{ 和}$$

$$D'=2\times\left\lfloor\frac{36}{2}\right\rfloor+0=36。$$

接著判斷 A'、B'、C'、D' 是否大於 255 或者小於 0，並代入取出步驟；結果顯示 A'、B'、C'、D' 並未大於 255 或者小於 0，且可順利取出，因此得到矩陣 I'，如圖11。

32	33
35	34

圖 11 2×2 矩陣 I'

3.2 取出過程

步驟 1：首先將得到的偽裝影像，切割成為同等大小 2×2 的矩陣 I'。

步驟 2：判斷 A' 為奇數或偶數。

步驟 3：若 A' 為奇數表式有二種可能，第一種表示該矩陣無法藏入，第二種可能表示該矩陣內的像素皆為奇數。先將 A'、B'、C'、D' 轉成偶數，算出 $\tilde{A}$、$\tilde{B}$、$\tilde{C}$、$\tilde{D}$，運算式如下：

$$\tilde{A}=2\times\left\lfloor\frac{A'}{2}\right\rfloor,$$

$$\tilde{B}=2\times\left\lfloor\frac{B'}{2}\right\rfloor,$$

$$\tilde{C}=2\times\left\lfloor\frac{C'}{2}\right\rfloor \text{ 和}$$

$$\tilde{D}=2\times\left\lfloor\frac{D'}{2}\right\rfloor。 \quad (6)$$

步驟 4：接著進行差異擴張運算，計算出 $\overline{A}$、$\overline{B}$、$\overline{C}$、$\overline{D}$，運算式如下：

$$\overline{A}=4\times\tilde{A}-(\tilde{B}+\tilde{C}+\tilde{D}),$$

$$\overline{B}=4\times\tilde{B}-(\tilde{A}+\tilde{C}+\tilde{D}),$$

$$\overline{C}=4\times\tilde{C}-(\tilde{A}+\tilde{B}+\tilde{D}),$$

$$\overline{D}=4\times\tilde{D}-(\tilde{A}+\tilde{B}+\tilde{C})。 \quad (7)$$

接著利用產生出來的差異值 $\overline{A}$、$\overline{B}$、$\overline{C}$、$\overline{D}$，以 $\overline{A}$ 為基底分別與 $\overline{B}$、$\overline{C}$、$\overline{D}$ 相減，產生 $\overline{A}$ 與 $\overline{B}$、$\overline{C}$、$\overline{D}$ 之間的差異值 T_1、T_2、T_3，運算式如下：

$$T_1=|\overline{A}-\overline{B}|,$$

$$T_2 = \left|\overline{A} - \overline{C}\right| ,$$

$$T_3 = \left|\overline{A} - \overline{D}\right| 。 \quad (8)$$

步驟 5：利用得到的 $\overline{A}$ 、$\overline{B}$ 、$\overline{C}$ 、$\overline{D}$ 以及 T_1 、T_2 、T_3 進行比較。其中 φ 定義為一門檻值(threshold)：

- 若 $252 < \overline{A}$ 、$\overline{B}$ 、$\overline{C}$ 、$\overline{D}$ 或 $3 > \overline{A}$ 、$\overline{B}$ 、$\overline{C}$ 、$\overline{D}$ 或 $\varphi < T_1$ 、T_2 、T_3 ，表示沒有藏入機密訊息，則還原像素值，

$$A = 2 \times \left\lfloor \frac{A'}{2} \right\rfloor + \text{Original LSB} 。 \quad (9)$$

表示將原始 LSB 加到 A' 的 LSB，並且 $B = B'$ ，$C = C'$ 和 $D = D'$ 。回到步驟 1 繼續下一個矩陣。

- 若不符合條件，表示有藏入機密訊息，則取出 B' 、C' 、D' 的 LSB，得到機密訊息 W_1 、W_2 、W_3 ，

$$W_1 = LSB(B') ,$$

$$W_2 = LSB(C') ,$$

$$W_3 = LSB(D') , \quad (10)$$

$LSB(x)$ 函式表示取出 x 值的 LSB。接著以 A' 、B' 、C' 、D' 還原原始像素，其運算如下：

$$A = A' ,$$

$$B = 2 \times \left\lfloor \frac{B'}{2} \right\rfloor + 1 ,$$

$$C = 2 \times \left\lfloor \frac{C'}{2} \right\rfloor + 1 \text{ 和}$$

$$D = 2 \times \left\lfloor \frac{D'}{2} \right\rfloor + 1 。 \quad (11)$$

步驟 6：若 A' 為偶數，則 $\hat{A} = A'$ ，另外可以直接將機密訊息取出，$W_1 = LSB(B')$ ，$W_2 = LSB(C')$ ，$W_3 = LSB(D')$ 。接著將 B' 、C' 、D' 轉成偶數得到 $\hat{B}$ 、$\hat{C}$ 、$\hat{D}$ ，運算式如下：

$$\hat{B} = 2 \times \left\lfloor \frac{B'}{2} \right\rfloor ,$$

$$\hat{C} = 2 \times \left\lfloor \frac{C'}{2} \right\rfloor ,$$

$$\hat{D} = 2 \times \left\lfloor \frac{D'}{2} \right\rfloor 。 \quad (12)$$

利用 $\hat{A}$ 、$\hat{B}$ 、$\hat{C}$ 、$\hat{D}$ ，還原 A 、B 、C 、D ，

$$A = \left\lceil \frac{2 \times \hat{A} + \hat{B} + \hat{C} + \hat{D}}{5} \right\rceil ,$$

$$B = \left\lceil \frac{2 \times \hat{B} + \hat{A} + \hat{C} + \hat{D}}{5} \right\rceil ,$$

$$C = \left\lceil \frac{2 \times \hat{C} + \hat{A} + \hat{B} + \hat{D}}{5} \right\rceil \text{和}$$

$$D = \left\lceil \frac{2 \times \hat{D} + \hat{A} + \hat{B} + \hat{C}}{5} \right\rceil 。 \quad (13)$$

我們以 3.1 節中，圖11的 2×2 矩陣 I' 為例說明取出的步驟，首先，判斷 A' 為奇數或偶數，在本例中，$A' = 26$ 為偶數，則 $\hat{A} = A' = 26$ ，並直接從 B' 、C' 、D' 的LSB中，取得機密訊息，得到 $W_1 = LSB(31) = 1$ ，$W_2 = LSB(41) = 1$ ，$W_3 = LSB(36) = 0$ 。接著將 B' 、C' 、D' 轉為偶數，得到 $\hat{B}$ 、$\hat{C}$ 、$\hat{D}$ ，

$$\hat{B} = 2 \times \left\lfloor \frac{31}{2} \right\rfloor = 30 ,$$

$$\hat{C} = 2 \times \left\lfloor \frac{41}{2} \right\rfloor = 40 \text{ 和}$$

$$\hat{D} = 2 \times \left\lfloor \frac{36}{2} \right\rfloor = 36 。$$

利用得到的 $\hat{A}$ 、$\hat{B}$ 、$\hat{C}$ 、$\hat{D}$ 進行還原，其計算如下：

$$A = \left\lceil \frac{2 \times 26 + 30 + 40 + 36}{5} \right\rceil = 32 ,$$

$$B = \left\lceil \frac{2 \times 30 + 26 + 40 + 36}{5} \right\rceil = 33 ,$$

$$C = \left\lceil \frac{2\times 40 + 26 + 30 + 36}{5} \right\rceil = 35 \quad 和$$

$$D = \left\lceil \frac{2\times 36 + 26 + 30 + 40}{5} \right\rceil = 34 \text{。}$$

4. 實驗結果

本研究利用 Lena、Airplane 和 Barbara 三張大小為 512×512 的圖形做為測試影像，並以亂數產生器產生機密訊息。第一個實驗為針對不同的門檻值設定，求出三張影像的機密訊息藏入量(Capacity)、平均藏入位元(Bits Per Pixel, Bpp)以及偽裝影像品質，其中偽裝影像品質以影像信號雜訊比(Peak Signal to Noise Ratios, PSNR)作為測量準則。

實驗結果如表2所示，實驗的門檻值分別設為 20、30 和 40，其中當門檻值越小時，PSNR 值越高，平均藏入位元越低。反之，門檻值越高，PSNR值越低，平均藏入位元越高。圖12 (a)為原始Lena影像，圖12 (b)、圖12 (c)和圖12 (d)分別為門檻值設為 20、30 以及 40 時之偽裝影像。以人眼觀查，藏入機密訊息過後的偽裝影像與原始影像的差異不大，不容易遭第三方查覺。此外，嵌入過後的機密訊息可以完全取出，偽裝影像也可順利還原成原始影像。

表 2 實驗結果

(a) 門檻值：20

Image	Lena	Airplane	Barbara
Capacity	50,847	112,254	35,667
Bpp	0.1940	0.4282	0.1361
PSNR	40.09	39.22	41.55

(b) 門檻值：30

Image	Lena	Airplane	Barbara
Capacity	93,243	135,945	64,755
Bpp	0.3557	0.5186	0.2470
PSNR	34.78	36.18	36.41

(c) 門檻值：40

Image	Lena	Airplane	Barbara
Capacity	121,764	148,041	83,955
Bpp	0.4645	0.5647	0.3203
PSNR	32.00	34.28	33.62

(a) 原始 Lena 影像

(b) 門檻值 20，PSNR：40.09

(c) 門檻值 30，PSNR：34.78

(d) 門檻值 40，PSNR：32.00

圖 12 原始影像與嵌入後的影像

5. 結論

本研究提出了一個有效的可逆式資訊隱藏技術，利用奇偶數來判斷藏入資訊的內容，並利用整數轉換函式及差異擴張方法來藏入機密訊息，除了能夠有效減少需要對應表進行還原過程的負擔外，也可以成功的回復原始遮蔽影像，偽裝影像與原始影像之間的失真，也在容許的範圍內，由於可以成功的復原原始影像，因此也能夠對同一張遮蔽影像，進行多次藏入的動作，以提升資訊藏量。

未來的研究方向，將針對不能藏入機密訊息的矩陣，運用其他藏入技術，使得機密訊息的藏入量能有效的增加，以期望有更高的負載量，並嘗試能夠將此方法運用於彩色影像上。

參考文獻

[1] Alattar, A. M., “Reversible Watermark Using the Difference Expansion of Generalized Integer Transform,” ***IEEE Transactions on Image Processing***, Vol. 13, No. 8, pp. 1147-1156, 2004.

[2] Celik, M. U., Sharma, G., Tekalp, A. M., and Saber, E., “Lossless Generalized-LSB Data Embedding,” ***IEEE Transactions on Image Processing***, Vol. 14, No. 2, pp. 253-266, 2005.

[3] Celik, M. U., Sharma, G., Tekalp, A. M., and Saber, E., “Reversible Data Hiding,” ***Proceedings of IEEE International Conference on Image Processing***, Vol. II, pp.157-160, 2002.

[4] Tian, J., “Reversible Data Embedding Using a Difference Expansion,” ***IEEE Transactions on Circuits and System for Video Technology***, Vol. 13, No. 8, pp. 831-841, 2003.

[5] Witten, I. H., Radford, M., and Cleary, J. G., “Arithmetic Coding for Data Compression,” ***Communications on ACM***, Vol. 30, No. 6, pp. 520-540, 1987.