

植基於模式函數之適應性區塊預測資訊影藏技術

曾顯文

朝陽科技大學

Email:

hwtseng@cyut.edu.tw

鄭聚賦

Email:

jyufu.cheng@gmail.com

摘要

資訊隱藏(Information hiding)技術主要是利用有意義圖像作為載體，將機密訊息嵌入到掩護的影像(Cover image)，有義意圖像在現今資料數位化時代中極為普遍而不易引起不法的第三方所注意，藉此藏入機密訊息以規避惡意的偵測或剽竊機密訊息，而達成資訊隱藏之目的。本文中，我們參考由 Chang 學者等人所提出的拓展全向性模式函數資訊隱藏方法(Fully Exploiting Modification Directions)，並利用鄰近影像複雜度，在影像複雜、平滑區，依據人類視覺感知能力的不同，進行適應性的機密訊息嵌入，藉以提升偽裝影像(Stego-image)整體的機密訊息載入量，並維持良好的影像視覺品質。

關鍵詞：資訊隱藏、模式函數、適應性

1. 前言

近年來隨著日新月異的科技及網際網路發展，使用者之間可以透過公開的網際網路空間便捷的傳遞訊息，因此訊息在傳遞過程當中，容易引起不法的第三方覬覦而遭竊取、竄改；為解決這些資訊安全上的問題，學者們提出了資訊隱藏(Information Hiding)技術將重要的機密訊息嵌入到媒體中再傳送到收方，使重要資訊能不被不法的第三方直接竊取而達到資訊隱藏之目的。資訊隱藏著重：安全性(Security)、不可察覺性(Imperceptibility)、高負載量(High Payload)。

資訊隱藏技術中最廣為人知且最簡單的方法為最低位元取代法(least significant bit)[1]其優點在於藏入的機密訊息只需依序取代影像中每一個像素值的最後一個位元即可完成藏入操作。在影像中鄰近像素值差異越大可歸類於邊緣區反之則為平滑區，人類肉眼對於邊緣區變動的察覺能力相較於平滑區低；故為了提升 LSB 整體機密訊息嵌入量便有學者提出以連續兩像素差異值作為參考，定義像素最大的可嵌入量[2][3]。近年來有越來越多資訊隱藏研究的提出是針對邊緣偵測[4]、人類視覺系統所發展[5]作為判斷影像複雜度之依據。

模式函式(modulus function)為基礎的資訊隱藏方法[6]。像素值更動的方式主要就是依據學者們所定義出的函式做為依據；因像素組所對應的函數值

為循環數，所以像素組與函數運算結果可以預先被儲存；而像素組更動的方式可以在預先的結果中搜尋並取代，這具有向的特性故模式函數的資訊隱藏方法也被稱做拓展方向性資訊隱藏方法 EMD(exploiting modification direction)。學者們提出各種拓展模式函數中的基底方法[7][8][9][10][11]，是為讓原始像素值在預先儲存的像素組中搜尋較少像素修改的像素組。學者們為了要提升模式函數的機密訊息嵌入量，更提出以像素差異值為參考決定機密訊息嵌入[12]。

本研究針對人類視覺的特性，以滑動窗口計算鄰近影像複雜度，作為新像素組影像複雜度的預測，預測數值越高則新像素組嵌入較多機密訊息，反之則嵌入較少的機密訊息，以維持良好的視覺品質。實驗結果顯示，依據影像複雜度所作的適應性嵌入，證明本研究在相同嵌入量下，能夠提供更好的偽裝影像品質。

2. 相關工作

Chang 學者等人所提出的研究，首先定義一張灰階影像 X ，影像大小為 $H \times W$ ，像素值介於 $[0,255]$ ，使用者預先切割後的機密訊息藏入到連續且不重疊的掩護像素組 (x_i, x_{i+1}) ， $i = \{1,3,5 \dots H \times W - 1\}$ ，藏入機密訊息後的偽裝像素組為 (y_i, y_{i+1})

Chang 學者所使用的模式函數公式如公式(1)所示：

$$F = [x_i \times (S - 1) + x_{i+1} \times S] \bmod S^2 \quad (1)$$

公式中 x_i, x_{i+1} 即代表影像連續且不重疊像素組，參數 S 的大小係由使用者決定，而參數 S 影響像素組的機密訊息嵌入量。掩護像素組函數式的運算結果只落在 $0 \leq F \leq S^2$ ，這意味著像素組所包含的像素值經過函數運算對應到單一的函數值，且為一個不大於 S^2 的循環數，所以在像素組嵌入機密訊息前，會先以使用者所提供的參數，將像素與各函數式運算結果對應到 $2D$ 的函數矩陣中，作為嵌入機密訊息時，替代像素的參考。

機密訊息嵌入長度，是依照使用者定義的參數 S ，將隨機產生的二元機密訊息切割而來。在嵌入時會將二進制機密訊息轉換為以 S 基底的十進制數字，如此一來機密訊息就被限定為 $2^S \leq S^2$ ，換句話說機

密訊息也為一個不大於 S^2 循環的數字，另一方面像素組會對應到該組像素差異值所使用的 $2D$ 函數矩陣中，若像素組的函數運算值恰好與轉換後的機密訊息數字相同，即代表該組像素不需修改像素組即為藏入機密訊息的偽裝像素組；若函式運算結果與機密訊息不相同，則像素組在 $2D$ 函數矩陣中所對應的數字即為函式運算結果，此時在 $2D$ 函數矩陣中以掩護像素組為中心，向搜索半徑內搜尋與機密訊息轉換的數字相同的像素組，並作為可替代像素組的候選像素組。可替代像素組在搜尋範圍內最少存在一組，所以為了選擇較好的替代像素組，在候選像素組內，會以歐基里德距離計算候選像素組與原始像素組的差距，並挑選其中差距小的候選像素組作為最後嵌入之結果。

在取出機密訊息部分，收方收到偽裝影像後根據使用者所使用的參數 S ，將像素組以公式(1)運算，所得之函數值即為藏入的機密訊息數字，最後將取出的函數值由十進制轉為對應參數 S 長度的二進制，即為藏入的機密訊息，依序計算各個連續但不重疊的像素組，便可取出完整的機密訊息。

當像素組鄰近灰階值的邊界即 x_i, x_{i+1} 趨近於灰階值 0 或 255 時，像素組就會產生上溢或下溢的問題，為了解決這問題 Chang 學者等人將搜尋時會產生溢位問題的像素值強制更動，也就是說若像素組中的 x_i 在搜索替代像素值的過程中，產生上溢問題則依據搜索半徑的變數 r 將像素值 x_i 強制定義在 $255 - r$ 的像素值以避免在搜索過程中產生上溢問題，反之若產生下溢問題則將 x_i 定義為 $0 + r$ 的像素值；像素組中的 x_{i+1} 亦遵照同樣的規範。

Chang 學者等人所提出的研究，簡而言之係將機密訊藏入到連續兩像素值餘數當中，而像素組機密訊息的藏入量則由使用者在一開始便定義，也就是說每組像素組每次藏入的機密訊息量是相同，但自然影像中，可區分為平滑、及複雜的區域，所以此方法並未考量到影像視覺特性。

3. 研究方法

本文所提出的研究，主因係近年來有越來越多的資訊隱藏技術是針對影像的邊緣偵測，簡單的說鄰近像素差異值越大，表示該區域為邊緣區的可能性提高，而針對邊緣區作修改的對於人類視覺特性而言，是相對比較不容易發現其間的差距。

本研究主要參考 Chang 學者等人所提出的研究所使用的模式函數公式，並進一步提出以鄰近影像複雜度預測，於機密訊息嵌入時，以適應性區間表作為藏入量的依據，達到提升整體機密訊息嵌入量之結果。

3.1 嵌入流程

本文提出一套資訊隱藏技術為一植基於模式函數之適應性區塊預測。本研究提出以鄰近像素預測影像複雜度，並利用鄰近像素組複雜度的預測結果，將機密訊息以適應性嵌入到掩護像素組中。本研究的嵌入流程如圖 1 所示：

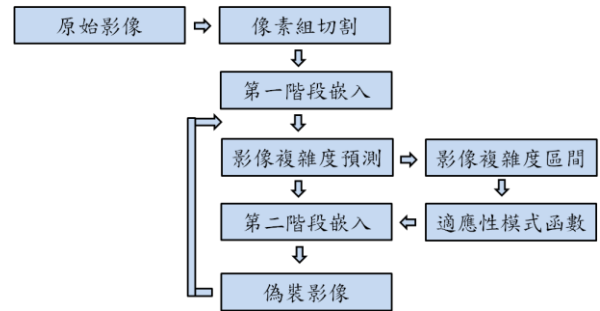


圖 1 嵌入方法流程圖

步驟一：切割掩護影像

首先我們將一張像素值介於 $[0,255]$ 尺寸為 $H \times W$ 的原始影像 Y ，以連續且不重疊的兩像素切割為一組並視為區塊 $b_{(i,j)}$ ， $i = \{1,2,3 \dots \frac{W}{2}\}$ ， $j = \{1,2,3 \dots H\}$ ；而個別區塊中則包含連續的兩像素則定義為 $p_{(2i-1,j)}, p_{(2i,j)}$ 。定義完影像中的區塊及像素位置，接著區分為如圖 2 的灰色部分係作為第一階段嵌入的像素組區塊；以及圖 2 右下部分作為第二階段嵌入的像素組區塊。

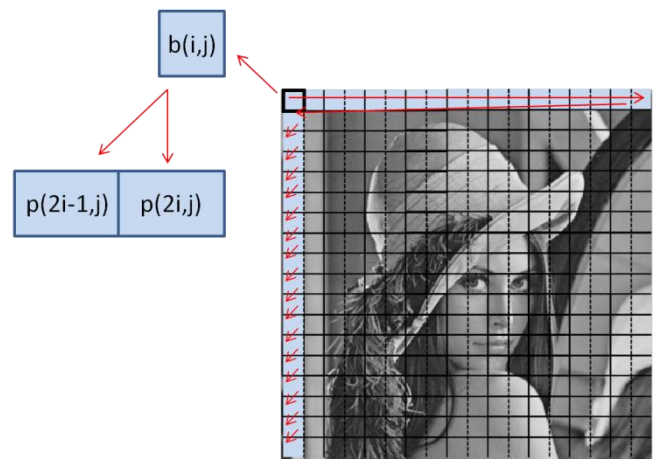


圖 2 掩護影像切割及第一階段嵌入

步驟二：第一階段嵌入

在第一階段機密訊息嵌入，主要是為預測影像複雜度衡量而操作，所以機密訊息嵌入量並不是此階段主要考量，因此我們在第一階段的機密訊息嵌

入時應盡可能減少原始影像的修改。圖 2 中灰色區域為第一階段的嵌入，即影像中最左側與最上層的區塊，嵌入演算法為公式(2)，將連續且不重疊的像素組，以每組掩護像素嵌入 2 位元機密訊息，也就是參數 $S = 2$ ，藉此減少第一階段在嵌入時對原始影像的修改程度。

$$F = [p_{(2i-1,j)} \times (S - 1) + p_{(2i,j)} \times S] \bmod S^2 \quad (2)$$

第一階段所進行的嵌入，是將像素組中的連續兩像素 $p_{(2i-1,j)}, p_{(2i,j)}$ 對應到如圖 3 作為中心點，並根據半徑公式(3)向鄰近像素組中建立可替代像素組範圍

$$C = \left\lfloor \frac{S + S - 1}{2} \right\rfloor \quad (3)$$

建立的搜尋範圍以公式(4)表示，其中 $p_{(2i-1,j)}, p_{(2i,j)}$ 即為搜索範圍的中心點

$$W_{(2 \times C + 1) \times (2 \times C + 1)}(S, (p_{(2i-1,j)}, p_{(2i,j)}), C) \quad (4)$$

在搜尋範圍內，為了保持良好影像品質我們將候選的像素組與原始像素組利用公式(5) 即歐基里德距離公式，計算選取的候選像素組與原始像素組差異，當選取最小差異的像素組時令該組為偽裝像素組 $(p'_{(2i-1,j)}, p'_{(2i,j)})$ 。嵌入機密訊息後的偽裝像素組區塊定義為 $b'_{(i,j)}$ 至此完成第一階段的嵌入機密訊息操作；而未嵌入機密訊息的區塊與偽裝像素組區塊暫存保留在一起。

$$dist = \min \left\{ |p'_{(2i-1,j)} - p_{(2i-1,j)}|^2 + |p'_{(2i,j)} - p_{(2i,j)}|^2 \right\} \quad (5)$$

	0	1	2	3	4	5	...	255	$p_{(2i,j)}$
0	0	2	0	2	0	2	...		
1	1	3	1	3	1	3	...		
2	2	0	2	0	2	0	...		
3	3	1	3	1	3	1	...		
4	0	2	0	2	0	2	...		
5	1	3	1	3	1	3	...		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	...		
255									

$p_{(2i-1,j)}$

圖 3 參數 $S=2$ 的函數矩陣圖

步驟三：區塊影像複雜度預測

在區塊影像複雜度的預測如圖 5 所示，我們由影像中最左上角以 2×2 區塊遮罩，開始選取並定義為 $B_{(i,j)}$ ， $i = \{1, 2, 3 \dots \frac{W}{2}\}$ ， $j = \{1, 2, 3 \dots H - 1\}$ ；而區塊遮罩 $B_{(i,j)}$ 中包含在已嵌入機密訊息的像素組區塊

$\{b'_{(i,j)}, b'_{(i+1,j)}, b'_{(i,j+1)}\}$ ，是作為影像複雜度判斷的運算。 $\{b_{(i+1,j+1)}\}$ 則為未嵌入機密訊息的掩護像素，該區塊依據影像複雜度運算結果，進一步利用使用者定義的適應性區間，決定該區塊機密訊息嵌入量；意即第二階段的嵌入，是由鄰近區塊的影像複雜度決定機密訊息嵌入量。

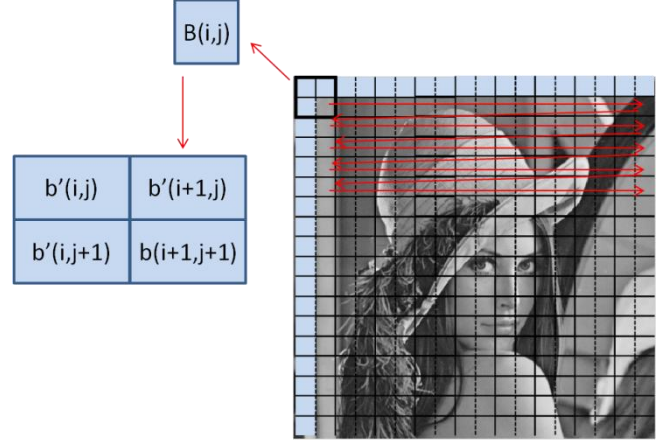


圖 4 影像複雜度預測

本研究對於區塊影像複雜度的預測是以標準差作為評估的方法；原因在於若鄰近區塊中像素組的像素值離散程度越大，代表在該區域內像素變動程度越大，也就越有可能是影像的邊緣區，所以我們就進一步針對遮罩範圍內，預測影像複雜度的像素組，進行樣本標準差的估算如公式(6)所示

$$\hat{B}_{(i,j)} = \sqrt{\frac{(b'_{(i,j)} - \bar{B})^2 + (b'_{(i+1,j)} - \bar{B})^2 + (b'_{(i,j+1)} - \bar{B})^2}{6}} \quad (6)$$

其中 \hat{B} 代表影像複雜度預測後之運算值， \bar{B} 代表的是預測像素組的像素平均值， \bar{B} 如公式(7)所示

$$\bar{B}_{(i,j)} = \left\lfloor \frac{1}{6} (b'_{(i,j)}, b'_{(i+1,j)}, b'_{(i,j+1)}) \right\rfloor \quad (7)$$

預測區塊影像複雜度的操作結束後，根據使用者預先定義的影像複雜度區間如表 1，依嵌入量調整模式函數所使用之參數，對遮罩內 $\{b_{(i+1,j+1)}\}$ 的區塊作適應性嵌入。

在接下來的第二階段機密訊息嵌入時，遮罩範圍內只選取影像中 $\{b_{(i+1,j+1)}\}$ ，作為機密訊息嵌入的目標，該組像素，而 $\{b'_{(i,j)}, b'_{(i+1,j)}, b'_{(i,j+1)}\}$ 只作為影像邊緣預測之使用，不再作第二階段嵌入。

表 1 為參考 Chang 者等人所提出之研究，本研究調整預設的影像複雜度門檻值 \hat{B} 、像素組嵌入量 L 、嵌入機密訊息所使用之參數 S ，並套用到公式(8)依序完成第二階段的機密訊息嵌入。

表 1 影像複雜度區間表 I

\hat{B}	L	Q
$0 \leq \hat{b} \leq 10$	2	2
$11 \leq \hat{b} \leq 25$	3	3
$\hat{b} \geq 26$	4	4

$$F = [p_{(2u-1,v)} \times (S - 1) + p_{(2u,v)} \times S] \text{mod} S^2 \quad (8)$$

在公式(8)中所使用變數 $u = i + 1$ 、 $v = j + 1$ ；第二階段嵌入候選像素的距離公式也改以公式(9)計算：

$$\text{dist} = \min \left\{ |p'_{(2u-1,v)} - p_{(2u-1,v)}|^2 + |p'_{(2u,v)} - p_{(2u,v)}|^2 \right\} \quad (9)$$

步驟四：第二階段機密訊息嵌入

依據區塊複雜度預測結果，針對 $\{b_{(i+1,j+1)}\}$ 以表 1 複雜度區間表做適應性嵌入， $\{b_{(i+1,j+1)}\}$ 區塊所包含的像素組透過公式 1 做運算並執行機密訊息嵌入。我們以圖 5 舉例機密訊息的嵌入過程

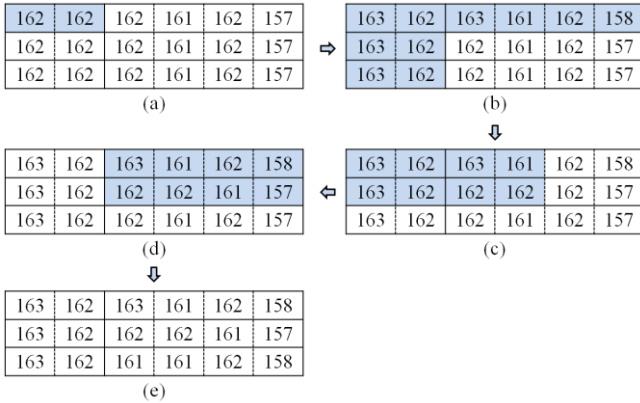


圖 5 掩護影像切割及第一階段嵌入

首先第一階段機密訊息嵌入，只針對影像中最左側與最上層的像素區塊作機密訊息嵌入，如圖 5(a) 所示，以連續且不重疊的兩像素為一區塊， $b_{(i,j)} = b_{(1,1)}$ 所包含的兩像素 $p_{(2i-1,j)}, p_{(2i,j)} = (162,162)$ ，將第一組像素代入公式(1)運算則 $F = [162 \times 1 + 162 \times 2] \text{mod} 2^2 = 2$ ，假設嵌入的二元機密訊息為 11 機密訊息轉換後為 3，因嵌入的機密訊息數字與模式函數運算結果並不相等，我們進一步在預先儲存的 2D 函數矩陣中，搜尋可替代像素組。搜尋的方式如圖 6 所示：

	160	161	162	163	164	165	...	255	$P_{(2i,j)}$
160	0	2	0	2	0	2	...		
161	1	3	1	3	1	3	...		
162	2	0	2	0	2	0	...		
163	3	1	3	1	3	1	...		
164	0	2	0	2	0	2	...		
165	1	3	1	3	1	3	...		
...		
255									

圖 6 像素組取代參考

掩護像素(162,162)在 2D 函數矩陣中，可找到函式運算結果為 $F = 2$ ，但嵌入的二元機密訊息為 11，此時以掩護像素為中心點，搜尋半徑參考公式(3)為 $C = 1$ ，則搜索範圍為 $W_{3 \times 3}(2, (162,162), 1)$ ，在此範圍中函數值若為 3 的將被選取為候選像素組，候選像素組與掩護像素組最後透過歐基里德距離公式計算並選取差異最小的一組，藏入機密訊息的偽裝像素組以該組取代，所以掩護像素(162,162)最後取代為(163,162)即 $b'_{(1,1)}$ ；如圖 5(b)依序將影像中最上層與最左側的掩護像素嵌入機密訊息完成第一階段的嵌入。

第二階段的嵌入則依據第一階段嵌入機密訊息的偽裝像素區塊作為影像複雜度預測，並進一步決定第二階段嵌入機密訊息的區塊，嵌入機密訊息的多寡。如圖 5(c)所示 $B_{(i,j)} = B_{(1,1)}$ 包含了第一階段已嵌入機密訊息的像素組區塊 $\{b'_{(i,j)}, b'_{(i+1,j)}, b'_{(i,j+1)}\}$ 及未嵌入機密訊息的掩護像素 $\{b_{(i+1,j+1)}\}$ 。透過公式(7)計算該遮罩內的像素平均值並進一步利用公式(6)計算影像複雜度，以 $B_{(i,j)} = B_{(1,1)}$ 如圖 5(c)使用 $\{b'_{(1,1)}, b'_{(2,1)}, b'_{(1,2)}\}$ 以藏入機密訊息的三個像素區塊作為影像複雜度預測，並決定未藏入機密訊息的區塊 $\{b_{(2,2)}\}$ 機密訊息嵌入量。 $b'_{(1,1)} = (163,162)$ 、 $b'_{(2,1)} = (163,161)$ 、 $b'_{(1,2)} = (163,162)$ ，利用公式(7)計算該遮罩內的像素平均值則 $\bar{B}_{(1,1)} = 162$ ，並進一步利用公式(6)計算該區域的影像複雜度 $\hat{B}_{(i,j)} = 0$ ，利用使用者預先定義的影像複雜度區間表即表 1 決定 $b_{(2,2)}$ 的機密訊息嵌入量，本例子中影像複雜度預測結果為 $\hat{B}_{(i,j)} = 0$ 則 $b_{(2,2)}$ 該區塊嵌入 2 位元的機密訊息，此時依據表 1 的區間表將 $b_{(2,2)}$ 代入到公式(8)則函數運算結果為 $F = [162 \times 1 + 162 \times 2] \text{mod} 2^2 = 2$ ，假設藏入的二元機密訊息為 10 經轉換後為機密訊息數字 2，在函數運算結果與機密訊息相同的情況，像素值不需取代即嵌入機密訊息並更新 $b_{(2,2)} = b'_{(2,2)} = (162,162)$ 。

第二階段嵌入遮罩選取範圍是重疊的，如圖 5(d)所示，在 $B_{(i,j)} = B_{(2,1)}$ 包含已嵌入機密訊息的像素區塊

$\{b'_{(2,1)}, b'_{(3,1)}, b'_{(2,2)}\}$ 及未嵌入機密訊息的掩護像素區塊 $\{b_{(3,2)}\}$ ，依此不斷更新遮罩所選取範圍完成機密訊息的嵌入如圖 5(e)所示。

3.2 提取流程

本研究在提取機密訊息與嵌入流程相似，第一階段嵌入的部分是固定以參數 $S = 2$ 的模式函數作嵌入；第二階段藏入的機密訊息則由鄰近像素組區塊影像複雜度預測結果提取機密訊息，提取流程如圖 7 所示：

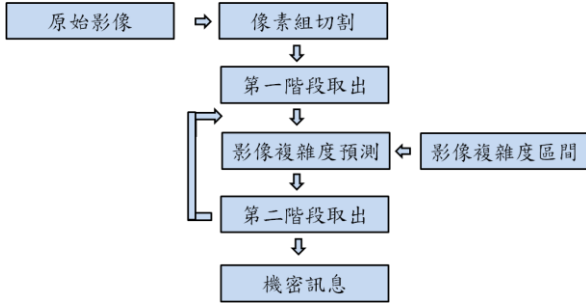


圖 7 提取方法流程圖

首先第一階段嵌入機密訊息的偽裝像素組，及偽裝影像中最左側與最上層的像素組，經參數 $S = 2$ 的模式函數運算，將嵌入的機密訊息數字取出，並轉換為長度為二位元的機密訊息，即取出第一階段所嵌入的機密訊息。

針對第二階嵌入機密訊息的偽裝像素組，首先利用鄰近像素組進行影像複雜度的運算並將運算結果，依使用者預先定義的影像複雜度區間，判別模式函數所使用的參數 S ，接著將第二階段嵌入機密訊息的像素組，依照區間表提供的參數 S 進行模式函數運算，進一步取出的機密數字，並轉換為相對應長度 L 的二元機密訊息，依序完成二元機密訊息提取，原始的機密訊息即可完整取出。

3.3 溢位處理

當機密訊息嵌入過程中，像素組鄰近灰階值的邊界即趨近於灰階值 0 或 255 時，像素組就會產生上溢或下溢的問題，為了解決這問題 Chang 學者等人將搜尋時會產生溢位問題的像素值強制更動，也就是說若像素組中的 x_i 在搜索的過程中，產生上溢問題則強制定義該像素值為 $255 - C$ ，反之若產生下溢問題則將像素值定義為 $0 + C$ 在本研究沿用這項修改方式

3.4 實驗結果

實驗結果我們將偽裝影像中的各個像素 $p'_{i,j}$ 及原始影像中的各像素 $p_{i,j}$ 以峰值信噪比 PSNR(peak signal-to noise ratio)計算，作為評定影像品質的工具，一般而言人類視覺難以辨別出測定數據大於 35 的影像與原始影像之間差別。PSNR 值定義如下：

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (8)$$

其中 MSE(mean a-square error)的計算公式為：

$$MSE = \left[\frac{1}{M \times N} \right] \sum_{i=1}^M \sum_{j=1}^N (p'_{i,j} - p_{i,j})^2 \quad (9)$$

表 2 實驗結果 I

偽裝影像	Chang之藏入量 (Capacity)	Chang之影像品質 (PSNR)	本研究之藏入量 (Capacity)	本研究之影像品質 (PSNR)
Lena	262144	52.39	266151	52.28
Baboon	262144	52.40	276366	52.04
Tiffany	262144	52.39	263727	52.35
Peppers	262144	52.38	265407	52.29
Babara	262144	52.39	276652	52.01

表 2 實驗結果是利用表 1 之影像複雜度區間表，所進行的適應性嵌入，結果顯示本研究能夠提高整體機密訊息的嵌入量，並且保持良好的偽裝影像品質，此外，在越複雜的影像如：Baboon、Babara 越能顯示在複雜影像中，本方法能嵌入更多的機密訊息

表 3 影像複雜度區間表 II

\hat{B}	L	Q
$0 \leq \hat{B} \leq 10$	3	3
$11 \leq \hat{B} \leq 25$	4	4
$\hat{B} \geq 26$	5	6

表 4 實驗結果 II

偽裝影像	Chang之藏入量 (Capacity)	Chang之影像品質 (PSNR)	本研究之藏入量 (Capacity)	本研究之影像品質 (PSNR)
Lena	393216	49.88	396473	49.76
Baboon	393216	49.89	406689	49.42
Tiffany	393216	49.89	394019	49.84
Peppers	393216	49.89	395710	49.77
Babara	393216	49.89	406922	49.41

表 5 影像複雜度區間表 III

\hat{B}	L	Q
$0 \leq \hat{B} \leq 10$	4	4
$11 \leq \hat{B} \leq 25$	5	6
$\hat{B} \geq 26$	6	8

表 6 實驗結果 III

偽裝影像	Chang之藏入量 (Capacity)	Chang之影像品質 (PSNR)	本研究之藏入量 (Capacity)	本研究之影像品質 (PSNR)
Lena	524288	46.75	526769	46.60
Baboon	524288	46.74	537051	46.22
Tiffany	524288	46.74	524345	46.69
Peppers	524288	46.74	526032	46.62
Babara	524288	46.75	537225	46.21

表 6 之實驗結果參照表 5 之影像複雜度適應性區間，透過影像複雜度門檻值大小進一步調整各區間的機密訊息嵌入量。

表 7 影像複雜度區間表 IV

\hat{B}	L	Q
$0 \leq \hat{B} \leq 10$	5	6
$11 \leq \hat{B} \leq 25$	6	8
$\hat{b} \geq 26$	7	12

表 8 實驗結果 IV

偽裝影像	Chang之藏入量 (Capacity)	Chang之影像品質 (PSNR)	本研究之藏入量 (Capacity)	本研究之影像品質 (PSNR)
Lena	655360	43.29	657080	43.21
Baboon	655360	43.29	667371	42.97
Tiffany	655360	43.30	654641	43.27
Peppers	655360	43.30	656336	43.23
Babara	655360	43.30	667558	42.96

表 8 之實驗結果參照表 5 之適應性區間表。在本研究中，我們固定各個區間的門檻植，實際上使用者可以依據機密訊息量調整區間大小，以上實驗結果皆顯示我們所提出的研究與 Chang 學者等人所提出之研究都能夠提供良好的偽裝影像品質，而本研究相較之下能夠提供更多的機密訊息負載量。

4. 結論

本研究所提出改良方法，參考了 Chang 學者等人所提出的模式函數式，本研究特色在於以鄰近區塊複雜度作為適應性嵌入原則，且影像複雜度是以預測的方式產生，有別於目前模式函數藏匿法的改進方式都在於修改模式函數的基底公式；此外透過影像複雜度區間的控制可提高機密訊息負載量。

本研究提出了一個較新穎方式包含了預測、以及適應性嵌入，並提高機密訊息藏入量，在未來研究上展望於更好的預測方法，使得預測結果越準確，讓偽裝影像品質能有所提升。

參考文獻

- [1] C. K. Chan and L. M. Cheng, "Hiding data in image by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.
- [2] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letter pp.1613-1626, June, 2003.
- [3] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement method," IEE Proceedings – Vision Image and Signal Processing 152 (October), pp.611-615, 2005.
- [4] W. J. Chen, C. C. Chang, T. Hoang, N. Le, "High payload steganography mechanism using hybrid edge detector," Journal of system with applications, vol.37, no. 7, pp.3292-3301, April, 2010
- [5] S. W. Jung, L. H. Le, S. J. Ko, "A new histogram modification based reversible data hiding algorithm considering the human visual system," IEEE signal processing letters, vol. 18, no.2, Feb, 2011.
- [6] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Communications Letters, vol. 10, no. 1, pp.781-783, 2006.
- [7] R. M. Chao, H. C. Wu, C. C. Lee, amd Y. P. Chu, "A novel image data hiding scheme with diamond encoding," EURASIP Journal on Information Security, Mar 2009.
- [8] 張真誠、陳國男, "如何在影像中藏入秘密資訊", 逢甲大學資訊工程學系電子報, 第二期, 9月, 2010年。
- [9] C. F. Lee, C. C. Chang, and K. H. Wang, "An improvement of EMD embedding method for large payload by pixel segmentation strategy," Image

and Vision Computing, vol. 26, no. 12, pp.1670-1676, Dec 2008

[10] D. Kieu, C. C. Chang, "A steganography scheme by fully exploiting modification directions," Expert System with Applications, vol. 38, no. 8, pp.10648-10657, Aug 2011.

[11] C. F. Lee and H. L. Chen, "A novel data hiding scheme based on modulus function," Journal of

Systems and Software, vol. 83, no. 5, pp.832-843, May 2010

[12] C. M. Wang, N. I. Wu. C. S. Tsai, and M. S. Hwang "A high quality steganographic method with pixel-value differencing and modulus function," Journal of System and Software, Jan 2007.