

# 具高容量的向量地圖資訊偽裝演算法

## A High Capacity Steganography Algorithm for Vector Map

陳凱威 王聖銘 張聖杰 王宗銘 鄭友銘 蔡淵裕 王鵬程  
中興大學資訊科學所  
kidd32pg@hotmail.com

### 摘要

本篇論文係針對一新興的圖形格式：向量地圖，提出一個高容量資訊偽裝演算法。我們模擬病毒感染擴散的方法快速地決定嵌入順序，並透過 QIM 概念的延伸於轉換域嵌入秘密訊息，達到高隱藏量的同時仍能保有良好的視覺效果。實驗結果顯示：我們提出的演算法不需原始向量地圖與記錄額外資訊，即可達到近似於向量地圖頂點個數二倍的高資訊嵌入量及低變形程度的目的。此外，我們的方法亦可有效抵抗平移、旋轉、等向縮放及頂點重排攻擊。證實此法可適用於向量地圖資訊偽裝之領域。

**關鍵詞：**向量地圖、資訊偽裝、轉換域。

### Abstract

This paper regards a new graphic format: vector map. We propose a high capacity steganography algorithm for the vector map. We simulate the contagious diffusion method to rapidly decide the embedded order, and through the advancing of the QIM method in the transfer domain, embed secret messages. It thereby results in high hidden capacity yet retaining well visual effects. The results indicate: Our proposed method doesn't need the original vector map and extra recorded data during the extraction procedure. It rapidly embeds messages about twice the amount of the vertices of vector maps and still preserves well visualization of a vector map. Furthermore our method can also work effectively against translation, rotation, uniform scale and vertices reorder. This proves that this method is applicable to the field of vector maps and steganography algorithm.

**Keywords:** vector map, steganography, transfer domain.

### 1. 簡介

隨著科技的進步，舉凡文字、靜態影像、動態影像到音訊等資料，皆以數位化的方式呈現與保存，加上網際網路的普及，使得這些資訊可以迅速且大量的在全世界流通，因此人們可以輕易

地從網路上竊取資料並重製散播，故引發了許多智慧財產及資訊安全相關的問題。為了保護著作權及維護資訊安全，已有許多的學者專家投身於資訊隱藏(Information Hiding)的研究中。

資訊隱藏包含兩大議題：浮水印(Watermarking)與資訊偽裝(Steganography)。浮水印演算法是將代表性的文字或影像，稱之為浮水印(Watermark)，嵌入(Embed)於需要受保護的數位媒體之中，用以驗證著作權；資訊偽裝演算法則是將欲傳送的重要訊息(Message)嵌入在不受人注意的掩護(Cover)媒體，藉此迷惑竊取者的注意力，達到秘密通訊的目的。進一步以嵌入方式區分，兩者皆可以分類為空間域(Spatial Domain)及轉換域(Transform Domain)兩種方式。空間域的優點為速度快但強韌性較差，嵌入資料造成的變形量(Distortion)是獨立的；相較於空間域，轉換域的嵌入方式需要經過大量的運算，故較為費時，但強韌性佳且能分散變形量，使人不易察覺。本篇論文係針對向量地圖(Vector Map)，此一新興的媒體，從事轉換域資訊偽裝的研究。

向量地圖為近年來相當受歡迎的圖形格式，舉凡網路地圖、全球定位系統(Global Position System, GPS)、汽車導航(Car Navigation)等，應用層面相當廣泛。向量地圖利用點與邊所構成的多邊形描述地圖上的地理特徵，故處理放大縮小、旋轉等操作時不會引響其品質，相較於傳統的圖形格式，向量地圖擁有更良好的視覺效果。有鑑於向量地圖的快速發展及其便於在網路上流通使用，我們認為可將向量地圖視為負載秘密訊息的媒介，透過向量地圖來進行秘密的通訊，故我們針對向量地圖提出一套資訊偽裝的演算法，其演算法的特性為具高資訊隱藏容量且低失真變形，能保留良好的地圖品質以達到資訊偽裝的目的。

本論文架構如下：第二節探討相關研究；第三節詳述我們提出的資訊偽裝演算法；實驗結果與數據分析呈現於第四節；最後第五節為結論。

### 2. 相關研究

截至目前為止，向量地圖的資訊隱藏研究大部分著重於浮水印[2, 5, 6, 7, 8, 9, 11, 12, 14, 15, 16, 17, 18, 19]，尚無關於資訊偽裝方面的文獻。由於向量地圖的組成元素僅為點與邊，與三維模型極

為類似，故我們將介紹部份向量地圖浮水印的演算法，及相關的三維模型資訊偽裝方法。

向量地圖的浮水印演算法依其嵌入方式可以分為空間域與轉換域。空間域的方法，如 2001 年，Hwan 學者利用簡單的遮罩以及 2002 年 Ohbuchi 學者利用四元樹分割，兩者皆透過移動分割區塊中的點座標、位置來嵌入浮水印。不同於空間域，轉換域上的浮水印演算法不直接透過點座標、位置的改變來嵌入浮水印，而是經過數學的轉換程序，轉換的方式諸如傅利葉轉換(Fourier Transform)[5, 8, 16, 17]，小波轉換(Wavelet Transformation)[7]，離散餘弦轉換(Discrete Cosine Transform)[18]，光譜係數(Spectral Coefficient)[12]等，皆將向量地圖上的頂點資訊透過數學定義及運算轉為各種係數值，再依浮水印位元調整係數值來嵌入秘密訊息。

三維模型的資訊偽裝同樣區分為空間域[3, 21, 22, 23]與轉換域[1, 10, 20]兩大類。空間域方面，Cayre 學者在 2003 年針對由三角片所組成的三維模型，利用尋訪三角片的方法並同時運用 QIM (Quantization Index Modulation)的觀念改變三角片上頂點座標的狀態來嵌入秘密訊息。隨後在 2005 年 Wang 學者針對 Cayre 所提出的方法在提出更高容量，更有效率的改進策略。轉換域方面則以 2000 年，Wagner 學者依模型拓樸關係定義屬於各頂點的頂點向量[20]，利用此頂點向量的轉換完成轉換域的浮水印演算法，隨後 Aspert 學者則在 2002 年進一步將 Wagner 的方法運用於三維模型的資訊偽裝[1]，而 Maret 學者則提出改良的方法提高資訊嵌入量[10]。

總結上述轉換域資訊偽裝演算法，皆是利用頂點向量的轉換嵌入秘密訊息，本篇論文也植基於此轉換域提出適用於向量地圖的資訊偽裝法。

### 3.演算法

我們針對向量地圖提出植基於轉換域且具有高資訊隱藏容量的演算法。 $n$  個頂點的向量地圖可藏入  $2(n-1)$ 位元的訊息，其演算法流程如圖 1。

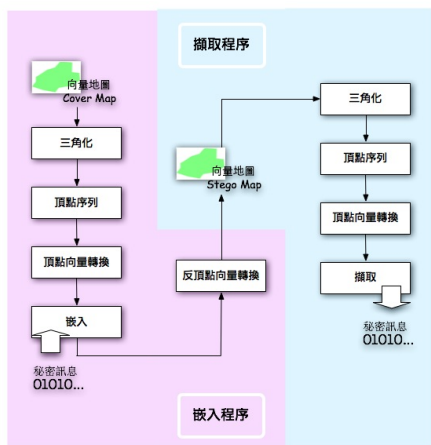


圖 1 資訊偽裝演算法流程

在嵌入的程序中分為五個步驟：首先將掩護的向量地圖經過三角化，建立一虛擬三角片網格 (Triangle Mesh)，使地圖所有的頂點互相連通；隨後在第二步驟，頂點序列，決定出稍後訊息嵌入的順序；接下來的第三步驟，我們利用頂點向量轉換將地圖的頂點座標資訊轉換到轉換域上；然後在四步驟中將秘密訊息透過 QIM 概念的延伸嵌入掩護地圖中；最後透過反頂點向量轉換產生一已嵌入訊息的掩護地圖。相同的概念，在擷取訊息的程序中也同樣將向量地圖先經過三角化，頂點序列，頂點向量轉換等步驟，最後，利用 QIM 的概念來擷取出已藏入的秘密訊息。

### 3.1 訊息嵌入流程

以下將針對我們提出的演算法的嵌入程序，依照流程逐一說明解釋。

#### 3.1.1 三角化

向量地圖利用點和邊構成的多邊形描述地表面的物件或特徵，由於島嶼等型態之地圖的分布特性，造成向量地圖中頂點與頂點間未必存在路徑，故並非所有頂點都有邊互相連通(connect)。為了取得唯一的嵌入順序及分散變形量，在此我們使用迪勞內三角化演算法(Delaunay meshing)[4]，將地圖中所有的頂點互相連通，使地圖形成由許多三角片所構成的網格，如圖 2 所示。

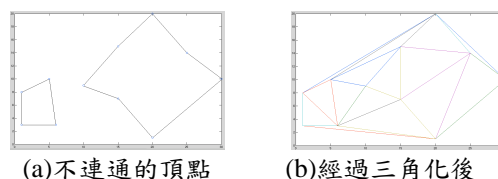


圖 2 不連通的頂點經過三角化後形成三角片組成的網格

#### 3.1.2 頂點序列

對向量地圖嵌入訊息前，必須先決定訊息嵌入的順序。此嵌入順序的產生必須是唯一的，同時滿足在嵌入與擷取兩個程序中必須能產生相同的順序，才能確保正確地擷取出已藏入的秘密訊息。在此，我們模擬病毒傳染擴散 (Contagious Diffusion) 的方式尋訪地圖上的三角片，尋訪三角片的過程可以依序蒐集到地圖上所有的頂點，並將其紀錄在頂點序列中，以此序列中頂點的先後順序作為稍後嵌入訊息時的順序，以下我們將詳述此病毒傳染擴散的三角片尋訪方法。

首先，我們將地圖上的三角片定義為兩種狀態：受感染的三角片與健康的三角片。其中受感染的三角片也稱之為病源，可以感染與其相鄰的健康三角片使其成為另一個具有傳染擴散能力的病源，同時受感染的三角片將具有免疫的特性，不會再被其他病源所感染，相對的，健康的三角片則不具備任何抵抗能力，若其相鄰的三角片為病源時，則很容易遭受感染。

藉由此法，我們必須先在皆為健康三角片的向量地圖定義一起始三角片  $T_{initial}$ ，做為病源，此  $T_{initial}$  的選取是依據向量地圖重心坐落的三角片決定。隨後，利用向量地圖的主成份分析(Principal component analysis, PCA)[12]決定  $T_{initial}$  的三個頂點紀錄的先後順序。我們對向量地圖所有的頂點座標做主成份分析得到兩個互相正交的主軸：第一主軸及第二主軸，其中第一主軸表向量地圖頂點分佈的主要情形，再將  $T_{initial}$  上的三個頂點座標投影到第一主軸上，由小到大可以為  $T_{initial}$  上的三個頂點做出排序並依序紀錄在頂點序列中，如圖 3 所示，並將這三個頂點依順序紀錄在頂點序列中。

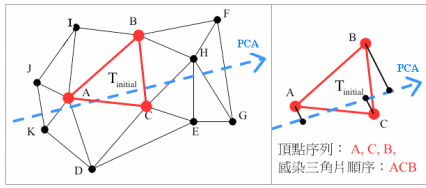


圖 3  $T_{initial}$  的選取與各標記的定義

隨後再由  $T_{initial}$  向外搜尋與其相鄰的三角片，搜尋相鄰三角片可以藉由  $T_{initial}$  上的三個頂點在頂點序列中紀錄的順序分為兩個方向：順方向(由 A 開始往 B 到 C)與逆方向(由 A 開始往 C 到 B)。如何決定順方向搜尋或逆方向搜尋，我們可以由使用者利用密鑰產生一連串的 0、1 序列，並定義 1 為逆方向，0 為順方向，如此一來，透過此一連串的 0、1 序列可以分別指定每個三角片的搜尋方向，提高頂點序列的安全性。

以圖 4 為例，假設三角片 ACB 為  $T_{initial}$  且將  $T_{initial}$  的三個頂點依其對主成分分析投影的排序結果紀錄在頂點序列中，隨後以  $T_{initial}$  為病源向外傳染擴散。由 0、1 序列的第一個位元：0，可以決定此次搜尋方向為逆方向，由 A 往 C 到 B，依此順序我們可以感染 ADC、CHB、BIA 三個健康三角片，並在頂點序列中依序紀錄下 D、H、I 三個頂點，此時三角片 ADC、CHB、BIA 皆受到  $T_{initial}$  的感染轉變成病源。

我們再分別以三角片 ADC、CHB、BIA 為病源向外傳染，依照順序先由三角片 ADC 往外搜尋與其相鄰的三角片，在此我們利用 0、1 序列的第二個位元來決定搜尋方向，可以讓我們依序搜尋到三角片 AKD、DEC 及 ABC，由於三角片 ABC 已經免疫，故只感染其餘兩個三角片並取得 K、E 兩點，同樣的，我們也依序分別對三角片 CHB、BIA 向外搜尋並傳染取得點 F、J。在此我們又成功感染了四個健康的三角片，AKD、DEC、HFB 與 IJA，並再以此四個三角片為病源向外傳染，透過不斷的搜尋病源的相鄰三角片並使之感染，直到所有頂點皆被取得紀錄在頂點序列中，而稍後，我們將對頂點序列中所紀錄的頂點，依序將其轉換到轉換域。

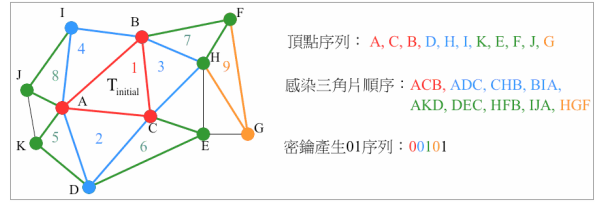


圖 4 模擬病毒傳染擴散

### 3.1.3 頂點向量轉換

在此，我們先定義何謂頂點向量(Vertex vector)[1, 10, 20]，隨後加以說明如何將地圖上的頂點資訊轉換至屬於頂點向量的轉換域。

根據 Wagner 學者所定義的頂點向量[20]，我們使用與其相同的定義。定義一平面  $M$ ， $M$  中包含兩個集合，分別為  $P$  和  $C$ 。其中  $P$  表示平面  $M$  上所有頂點的集合， $C$  則表示平面上頂點與頂點間的連接關係，其關係如下所示：

$$M = \{P, C\}$$

$$P = \{p_i\}_{i=0, \dots, n}, \quad p_i = (x_i, y_i)$$

$$C = \{\{i, j_k\}\}_{k=0, \dots, m}, \quad 0 \leq i_k \leq n, 0 \leq j_k \leq n.$$

在這個平面  $M$  上的每個頂點  $p_i$  皆可以透過式 1 計算出其頂點向量。其中  $S_i$  為一純量，表示與  $p_i$  有邊相連的頂點個數，如式 2 所示：

$$n_i = \frac{1}{|S_i|} \sum_{j \in S_i} (p_j - p_i) \quad (1)$$

$$S_i = \{j | \{i, j\} \in C\}, \quad i = 0, \dots, n \quad (2)$$

隨後，依頂點序列中頂點的先後順序對每個頂點  $p_i$ ，藉由三角化步驟產生的拓樸關係求出其頂點向量  $n_i$ ，將向量地圖所有頂點資訊轉換到頂點向量的轉換域上，對於轉換後所得的每個頂點向量  $n_i$  都可透過式 3 及式 4 求出其長度  $r_i$  與角度  $\theta_i$ ，再利用  $r_i$ 、 $\theta_i$  及式 5，我們可得到各頂點向量對應的弧長  $L_{\theta_i}$ 。其中  $r_i$ 、 $\theta_i$  及  $L_{\theta_i}$  將為我們嵌入訊息時重要的資訊，除了  $n_i$  中最小的頂點向量  $n_{\min}$  所對應的  $r_{\min}$  和  $\theta_{\min}$  不能嵌入資訊外，其餘的  $(n-1)$  個頂點向量，都可對其  $r_i$  及  $\theta_i$  嵌入訊息。

$$r_i = \sqrt{x_i^2 + y_i^2} \quad (3)$$

$$\theta_i = \tan^{-1} \left( \frac{y_i}{x_i} \right) \quad (4)$$

$$L_{\theta_i} = r_i' \cdot \theta_i \quad (5)$$

### 3.1.4 嵌入訊息

我們將 QIM 的概念運用於嵌入資訊，依序對  $r_i$  及  $\theta_i$  各嵌入一個位元的訊息。首先，先將長度  $r_i$  分為兩種狀態： $M_0$  及  $M_1$ ，如圖 5 所示。

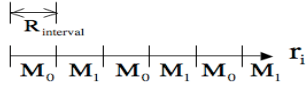


圖 5 將  $r_i$  分成兩種狀態  $M_0$  及  $M_1$

其中  $M_0$  與  $M_1$  區間的大小為  $R_{interval}$ ， $R_{interval}$  可由式 5 求得。式 6 中的  $D_r$  為使用者所自訂的參數，根據不同的向量地圖會有不同的適用  $D_r$  參數。若  $D_r$  選取的較大會使得地圖嵌入前後變形較大，失去偽裝的意義；若是  $D_r$  取的太小容易造成  $R_{interval}$  過小，使得擷取有誤差，故我們將  $R_{interval}$  的有效小數點位數控制在一範圍內，如式 7 所示，藉此來決定  $D_r$  的範圍，使得擷取訊息時不會照成誤差且保持良好的變形。其中， $f$  為地圖頂點座標中有效的小數點位數。

$$R_{interval} = \frac{n_{min}}{D_r} \quad (6)$$

$$\frac{n_{min}}{1 \times (0.1)^{f-1}} < D_r < \frac{n_{min}}{\sqrt{2} \times (0.1)^f} \quad (7)$$

嵌入訊息時，根據我們欲隱藏的訊息位元是 0 或 1 兩種狀態移動  $r_i$  的長度到正確的狀態。在這裡令  $r_i$  的狀態為  $P(r_i)$ ，欲嵌入的訊息為  $b$  ( $b=0$  或  $b=1$ )，若  $P(r_i) \in M_b$ ：移動  $r_i$  長度到區間  $M_b$  的中間；若  $P(r_i) \notin M_b$ ：移動  $r_i$  長度為  $r'_i$ ，使得  $P(r'_i) \in M_b$  且落在最鄰近的  $M_b$  區間的中間，並滿足  $r'_i$  不會小於  $n_{min}$  的長度；運用相同的概念，我們也將隨後依序對  $\theta_i$  所對應的弧長  $L_{\theta_i}$  做嵌入。

我們將弧長  $L_{\theta_i}$  也分為兩種狀態  $M_0$  及  $M_1$ ， $M_0$  與  $M_1$  區間的大小為  $L_{interval}$ 。 $L_{interval}$  的求法同  $R_{interval}$ ，由使用者自訂一參數  $D_L$  來決定，如式 8 所示。同樣地，我們一樣以式 7 限制  $D_L$  的範圍。根據我們要嵌入的訊息改變弧長的長度使其弧長落在正確的區間中，再根據式 4 反推嵌入後的  $\theta_i$ 。由於在嵌入過程中， $r_i$  的長度改變會影響到  $\theta_i$ ，所以對每個頂點向量做嵌入時，必須先對  $r_i$  做完嵌入動作後才可以對  $\theta_i$  做嵌入。

$$L_{interval} = \frac{n_{min}}{D_L} \quad (8)$$

透過上述方法，除了最短的頂點向量  $n_{min}$  不能隱藏外，其餘  $(n-1)$  個頂點向量皆可隱藏 2 位元的資訊。是故，一個擁有  $n$  個頂點的向量地圖，可以隱藏  $2(n-1)$  位元的資訊。

### 3.1.5 反頂點向量轉換

嵌入訊息後，頂點向量會因為  $r_i$  與  $\theta_i$  被嵌入訊息而有所變動，欲求得偽裝地圖的頂點資訊時，我們必須利用嵌入訊息後的頂點向量與三角

化所產生各頂點的拓樸關係，透過式 9 將轉換域上的頂點向量反轉換至空間域中的頂點座標。其中  $\tilde{p}_i$  及  $\tilde{p}_j$  是偽裝地圖的頂點座標，而  $n_i$  為頂點向量，由這些資訊帶入式 9 中，可以透過解聯立方程式求出  $\tilde{p}_i$  及  $\tilde{p}_j$ ，得到嵌入後的偽裝地圖，完成所有的嵌入程序。

$$n_i = \frac{1}{|S_i|} \sum_{j \in S_i} (\tilde{p}_j - \tilde{p}_i) \quad (9)$$

## 3.2 擷取訊息

為了成功擷取出秘密訊息，我們必須紀錄嵌入程序中的一些資訊，其中包含頂點序列的使用者秘鑰及決定嵌入區間長度的  $D_r$  與  $D_L$ 。擷取秘密訊息時，與嵌入程序一樣，先將偽裝地圖做三角化，使其產生一三角化的網格，再利用偽裝地圖重心所在的三角片作為起始三角片。以此為病源搭配使用者秘鑰產生的 0、1 序列向外感染其他三角片，在擴散感染其他三角片的過程，可以得到與嵌入時相同的頂點序列。再依序將其頂點資訊轉換至頂點向量轉換域，最後，利用 QIM 的概念判斷各頂點向量的狀態擷取出正確的訊息，完成擷取秘密訊息的程序。

## 4、實驗結果與分析

我們實作的環境為 Mac OSX，PowerPC G4 1.33GHz 中央處理器，1GB 記憶體。

表 1 為我們實作的向量地圖的一些特性及其可嵌入的訊息數與變形量。由實驗的數據可以得知，在  $n$  個頂點的向量地圖上，我們可以藏入  $2(n-1)$  位元的秘密訊息，隱藏量近乎頂點數量的 2 倍。

以變形量部分而言，由於我們的資訊偽裝方法屬於轉換域的方式，故會將嵌入時所造成的變形量散佈在地圖上的各頂點。從圖 6 可以發現，掩護地圖與偽裝地圖其差異程度無法以肉眼判斷，此外，我們亦以量化的變形數據作為佐證，分析嵌入前後向量地圖的變形程度。在此，我們使用 RMSE(Root Mean Square Error) 與 GL(Geometric Laplacian) 作為測量的工具。其中，RMSE 的測量方法可由式 10 計算求得，透過掩護地圖與偽裝地圖兩者間相對應頂點座標的歐基里得距離來評估差異程度；GL 則是加入了頂點間的拓樸關係作為考量，我們可由式 11 計算得之。其中  $v_i$  表示掩護模型， $\hat{v}_i$  表示偽裝模型； $l_{ij}$  為頂點  $i$  與相連頂點  $j$  的幾何距離， $n(i)$  為與頂點  $i$  有連接關係的頂點集合，其兩種方式的測量結果皆紀錄在表 1。由表 1 可以顯示我們提出的方法在嵌入大容量訊息的同時，也可以達到低變形量，保持良好的地圖視覺效果。

$$RMS = \sqrt{\sum_{i=1}^n (\hat{x}_i - x_i)^2 + (\hat{y}_i - y_i)^2} / N$$

$$RMSE = RMS / \text{Bounding Box} \quad (10)$$

$$GL(v_i) = v_i - \frac{\sum_{j \in n(i)} l_{ij}^{-1} v_j}{\sum_{j \in n(i)} l_{ij}^{-1}}$$

$$\text{Mean of } GL = \sum_{i=1}^N \left( \|GL(\hat{v}_i) - GL(v_i)\| \right) / N \quad (11)$$

強韌性方面，資訊偽裝不同於浮水印的地方在於其目的不同，資訊偽裝著重在偽裝，而浮水印主要目的則是為了保護智慧財產權。從不同的目的上來分析，資訊偽裝通常不考慮其強韌性。但因為向量地圖相對於傳統影像地圖的優點在於對其放大、縮小不會造成視覺上的失真，且地圖不可避免的可能會被使用者旋轉或是平移，所以我們的資訊偽裝方法對於這些地圖常見的操作行為皆視為非蓄意性的攻擊：旋轉、平移、等比例縮放，故我們認為需要具備抵抗相似轉換的能力。我們延伸 QIM 的概念並以區間比例的方式進行嵌入與擷取，有效抵抗旋轉、平移、等比例縮放的攻擊。此外，我們在嵌入資訊前利用三角片感染擴散得到一頂點序列作為嵌入訊息時的順序，故當向量地圖遭受重排攻擊時，我們仍可順利的擷取出正確的秘密訊息。

安全性分析方面，在搜尋病源相鄰的三角片時，我們利用秘鑰產生一組 0、1 的序列決定搜尋方向，竊取者對於每一三角片皆僅有二分之一的機會預測搜尋方向，故竊取者成功預測頂點序列的機率僅為  $(0.5)^T$ ，其中 T 為三角片總數。以台東線地圖為例，竊取者成功預測頂點序列的機率僅為  $0.5^{5340}$ ，其成功率近乎於零。此外，竊取者仍需取得嵌入步驟中的  $D_r$  與  $D_L$  才可正確擷取秘密訊息，故由上述分析可以得知我們提出的資訊偽裝演算法具有良好的安全性。

時間分析方面，反頂點向量轉換較為複雜耗時，見表 2。由於反頂點向量轉換需藉由解聯立方程式，其複雜度為  $O(n)^2$ ，所以對於點數較多的向量地圖會較為耗時。雖然轉換域需耗費較長的時間取得轉換後的數值以供嵌入資訊，但是，卻可有效分散向量地圖變形程度，避免地圖輪廓局部之突兀變形。

## 5、結論

本論文係針對一個新興的圖形格式：向量地圖，提出一套具高容量的向量地圖資訊偽裝演算法。我們改變頂點向量的長度及其對應之弧長嵌入資訊，在  $n$  個頂點的向量地圖中可嵌入  $2(n-1)$  位元的秘密訊息，達到高資訊嵌入量的目的。此外，我們利用轉換域的特性分散其變形量，使偽裝向量地圖仍保有良好的地圖外觀，達到偽裝的訴求。總結本研究：我們提出的演算法可以在向量地圖嵌入大量資訊的同時亦能維持向量地圖良好的視覺效果，促使其應用範疇更為廣泛。

未來工作方面，我們希望針對反頂點向量轉換提出最佳化，利用小波轉換或模型切割提升演算法效率，並期待以自動化方式選取  $D_r$  與  $D_L$ ，提高演算法的便利性。

## 參考文獻

- [1] N. Aspert, E. Drelie, Y. Maret, and T. Ebrahimi, "Steganography for Three-Dimensional Polygonal Meshes," *Proceedings of SPIE 47th Annual Meeting*, Vol. 4790, pp. 705-708, 2002.
- [2] M. Bami, F. Bartolini, V. Cappellini, A. Piva and F. Salucco, "Text-based Geometric Normalization for Robust Watermarking of Digital Maps," *Proceedings of the 2001 IEEE International Conference on Image Processing*, Vol. 1, pp. 1082-1085, 2001.
- [3] F. Cayre and B. Macq, "Data hiding on 3-D triangle meshes," *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, pp. 939-949, 2003.
- [4] M. de Berg, M. van Kreveld, M. Overmars and O. Schwarzkopf, "Computational Geometry: Algorithms and Application," 2nd edition, Springer, 2000.
- [5] A. Giannoula, N. Nikolaidis and I. Pitas, "Watermarking of Sets of Polygonal Lines Using Fusion Techniques," *Proceedings of IEEE International Conference on Multimedia and Expo*, Vol. 2, pp. 549-552, 2002.
- [6] Kang Hwan II, Kab II Kim and Jong Uk Choi, "A Vector Watermarking Using the Generalized Square Mask," *Proceedings of IEEE International Symposium on Industrial Electronics*, Vol. 1, pp. 56-58, 2001.
- [7] I. Kitamura, S. Kanai, and T. Kishinami, "Watermarking Vector Digital Map using Wavelet Transformation," *Proceedings of Annual Conference of the Geographical Information Systems Association (GISA) 2000*, Vol. 9, pp. 417-4, 2000.
- [8] I. Kitamura, S. Kanai and T. Kishinami, "Copyright Protection of Vector Map using Digital Watermarking Method based on Discrete Fourier Transform," *Proceedings of IEEE 2001 International Geoscience and Remote Sensing Symposium*, Vol. 4, pp. 11-13, 2001.
- [9] M. Kurihara, N. Komatsu and H. Arita, "Watermarking Vector Digital Maps," *Proceedings of IPSJ*, Vol. 9, No. 36, 2000.
- [10] Y. Maret and T. Ebrahimi, "Data hiding on 3D polygonal meshes," *Proceedings of the 2004 workshop on Multimedia and security*, Magdeburg, Germany, pp. 68-74, 2004.
- [11] Ryutarou Ohbuchi, Hiro Ueda and Shu Endoh, "Robust Watermarking of Vector Digital Maps," *Proceedings of IEEE Conference on Multimedia and Expo 2002 (ICME 2002)*, Vol. 1, pp. 577-580, 2002.
- [12] Ryutarou Ohbuchi, Hiro Ueda and Shu Endoh, "Watermarking 2D Vector Maps in the Mesh-Spectral Domain," *Proceedings of the Shape Modeling International 2003*, pp. 6-225, 2003.

- [13] Alvin C. RENCHER : *Methods of Multivariate Analysis*. Second Edition, Wiley, New York, 2002.
- [14] Gerrit Schulz and Michael Voigt, "A High Capacity Watermarking System for Digital Maps," *Proceedings of the 2004 workshop on Multimedia and security*, pp. 180-186, 2004.
- [15] Cheng Yong SHAO, Hai Long WANG, Xia Mu NIU and Xiao Tong WANG, "A Shape-Preserving Method for Watermarking 2D Vector Maps Based on Statistic Detection," *Proceedings of IEICE Transactions on Information and Systems 2006*, Vol. E89-D, No. 3, pp. 1290-1293, 2006.
- [16] V. Solachidis, N. Nikolaidis and I. Pitas, "Fourier Descriptors Watermarking of Vector Graphics Images," *Proceedings of IEEE International Conference on Image Processing*, Vol. 3, pp. 9-12, 2000.
- [17] V. Solachidis, N. Nikolaidis and I. Pitas, "Watermarking Polygonal Lines using Fourier Descriptors," *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'2000)*, Vol. 6, pp. 55-58, 2000.
- [18] Michael Voigt, Bian Yang and Christoph Busch, "Reversible Watermarking of 2D-Vector Data," *Proceedings of the 2004 workshop on Multimedia and security*, pp.160-165, 2004.
- [19] Michael Voigt and Christoph Busch, "Feature-based watermarking of 2D-Vector Data," *Proceedings of SPIE, Security and watermarking of Multimedia Content*, pp. 359-366, 2003.
- [20] M. G. Wagner, "Robust Watermarking of Polygonal Meshes," *Proceedings of Geometric Modeling and Processing 2000*, 2000, pp. 201-208.
- [21] C.-M. Wang and Y.-M. Cheng, "An Efficient Information Hiding Algorithm for Polygonal Models," *Computer Graphics Forum*, Vol. 24, No. 3, pp. 591-600, 2005.
- [22] C.-M. Wang and P.-C. Wang, "Data Hiding Approach for Point-Sampled Geometry," *IEICE Transactions on Communications*, Vol. E88-B, No. 1, pp. 0-4, 2005.
- [23] C.-M. Wang and P.-C. Wang, "Steganography on Point-sampled Geometry," *Computers & Graphics*, Vol. 30, No. 2, pp. 244-254, 2006.

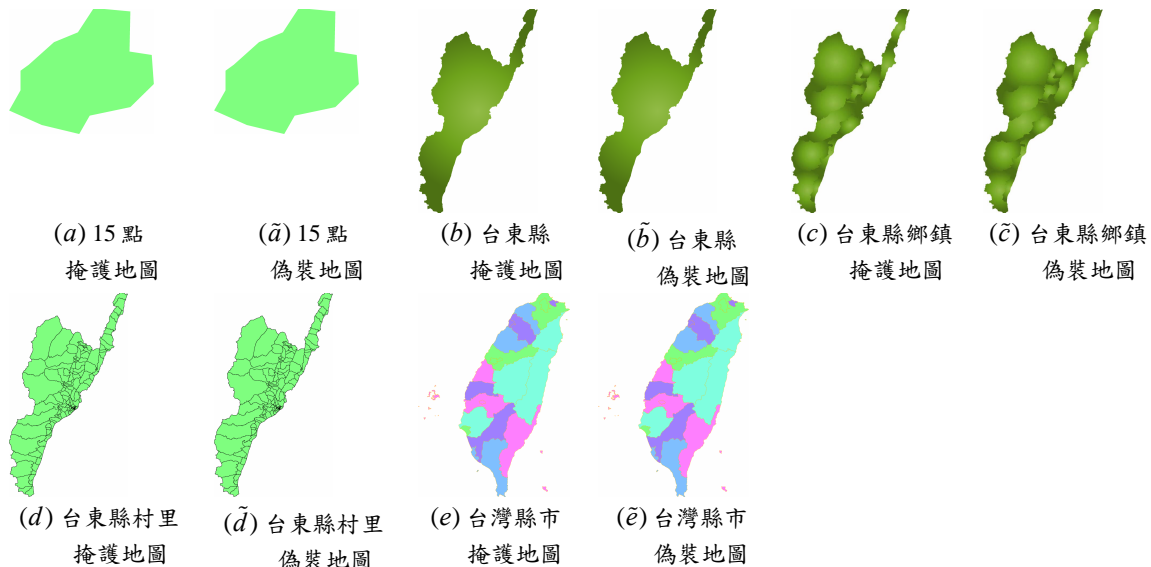


圖 6 掩護地圖與偽裝地圖的視覺化

表 1 向量地圖的特性與嵌入訊息量變型量時間

| 向量地圖 | 頂點個數  | 嵌入訊息量 (Bits) | Bounding Box 斜對角線長 | $D_r$ | $D_L$ | RMSE   | GL     | 嵌入程序總時間 (秒) | 反頂點向量轉換時間 (秒) |
|------|-------|--------------|--------------------|-------|-------|--------|--------|-------------|---------------|
| (a)  | 15    | 28           | 65623.409463       | 30000 | 30000 | 0.0303 | 0.0371 | 1           | < 1           |
| (b)  | 2685  | 5368         | 155127.288406      | 30000 | 30000 | 0.0041 | 0.0030 | 2.7         | 1             |
| (c)  | 7393  | 14784        | 155127.288406      | 30000 | 30000 | 0.0183 | 0.0223 | 4.8         | 2.4           |
| (d)  | 9199  | 18396        | 155127.288406      | 10000 | 10000 | 0.0033 | 0.0080 | 11.3        | 4.9           |
| (e)  | 14840 | 29678        | 465553.936370      | 30000 | 30000 | 0.0087 | 0.0512 | 53.6        | 43.5          |