適用於軍事地圖與衛星影像疊合之改良型 LSB 取代技術

李建中　劉江龍*

國防大學理工學院電機電子工程學系

摘　　要

本論文提出適用於軍事地圖與衛星影像疊合之藏密技術。本技術利用改良型簡單 LSB 取代技術將二值化地圖隱藏在衛星影像的最低位元平面，除保有簡單 LSB 取代技術的實作簡單及藏密量大等優點外，還可同時抵抗統計式分析之攻擊，具有比簡單 LSB 取代技術更安全的特性。因本藏密技術具有上述之優點，可在低頻寬及低運算能力設備上輕易達到影像與圖層疊合的效果。實驗結果顯示，本文所提的藏密技術具有良好的不可見性，並可有效抵抗卡方攻擊及 RS 偵測，非常適合數位化戰場的實務應用。

關鍵詞：衛星影像，地圖疊合，藏密學，最低位元取代，卡方攻擊，RS偵測

Modified Simple LSB Replacement Technique for Overlaying Military Map on Satellite Image

Chien-Chung Lee and Chiang-Lung Liu*

Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University

ABSTRACT

In this paper, we present a steganographic method for overlaying a military map on a satellite image. The proposed method uses a modified simple LSB replacement technique to embed a binary map in the least significant bit plane of a satellite image. The proposed method not only can maintain the properties of easy implementation and high capacity of the simple LSB replacement techniques, but also can resist the statistical attacks to gain the property of better security. Due to the above superiority, the proposed method can easily overlay a binary map on a satellite image on low-bandwidth and low-computational-power devices. Experimental results show that the proposed method have good imperceptibility and can resist Chi-square attack and RS steganalysis, and is practical for applications of digital battle fields.

Keywords: satellite image, map overlaying, steganography, LSB replacement, Chi-square attack, RS steganalysis

文稿收件日期 99.1.5; 文稿修正後接受日期 99.9.5; *通訊作者
Manuscript received January 5, 2010; revised May 5, 2010; * Corresponding author

一、前　言

以衛星系統進行地表遙感探測所生成的影像稱為衛星影像，最早起源於軍事上的應用，目的在觀測與記錄欲探索區域的氣象、水文、敵軍設施及行動佈署等情報資訊。由於衛星影像具有貼近真實的特性，因此對於精密的軍事任務而言，精確的地圖與衛星影像已是不可或缺的重要工具；而藉由地理資訊系統(Geographic Information System, GIS)的整合操作，地圖與衛星影像可以進行疊合(overlay)[1]，使地圖更容易被使用者判讀。

地理資訊系統是一套以電腦運算為基礎的空間資訊處理工具，能夠有效的將空間資料與外部資訊進行空間參照的資料處理，包括資料存取、管理、分析與輸出等，它解決了龐大的空間資料在管理與處理時所面臨時間與效率的挑戰[2]。

一般而言，地理資訊系統儲存兩種資料，分別為屬性資料與空間資料。屬性資料由數值、字元串及多維陣列所組成，儲存於資料庫。空間資料以網格(Raster)或向量(Vector)型式儲存，其中網格資料如同影像像素(Pixels)的排列方式展現，記錄著每個格點的屬性值；而向量資料則是由點、線段與多邊型等所組成。只要結合數值高程模型(Digital Elevation Model, DEM)、正交糾錯影像(Ortho-rectified Photo)及投影系統(Projection System)等三個分離儲存的檔案，即可呈現一個具空間立體概念的地圖。

在地理資訊系統軟體中，不論是原始資料或透過操作產生的資料集，都可視為某種型式的地圖，而為了更彈性的產生與使用空間資訊，不同的地圖層可以經由融合(Fusion)操作而同時呈現，此種結合兩個以上不同地圖資訊所產生新的地圖的操作又稱為地圖的疊合[3]。而對於不同應用目的使用者而言，疊合的圖層資訊往往更優於個別圖層資訊[4]，例如：將軍事地圖與衛星影像疊合後，可更具體地描述軍事任務的目標。

近來，許多新的運算技術、軟體、資料庫及網路科技導入地理資訊系統[5]，但是將空間資料視覺化的展現仍是一項困難與耗時的工程[6]。此外，空間資訊(如地圖)具有軍事上的重要性[7]，若經由通訊網路進行傳遞，則必須考量傳輸上的安全。GIS 的另一項限制，則是在主從(Client/Server)架構的地理資訊系統環境中[8]，空間資料視覺化的品質非常依賴資訊量、網路頻寬與遠端伺服器的資料傳輸速率 [9]，因此，對於移動式運算裝置而言，若無法提供可以處理多重資料的整合性系統，則即使在 GIS 系統中極為簡單的處理，也會成為高成本的工作[10]。例如移動式裝置就不適合即時將矩陣資料或向量資料以視覺化的方式展現，因為大量的空間資料所需的儲存空間及資料轉換的運算資源均可能超出設備所能提供的能力。

為解決上述地理資訊系統運用上可能遭遇的問題，本論文提出基於資訊隱藏技術的圖層疊合技術，將具有軍事用途的機敏資訊(例如座標、時間、高度、地物符號與標示等)巧妙嵌入在衛星影像中，若衛星影像不慎被非法截取，則可降低重要情報資訊洩露的風險。另外，在實際應用中，若將二值化後之軍隊符號或軍事地圖隱藏在衛星影像中，則可有效節省儲存空間及傳輸時間，而對於行動裝置的使用者而言，則可使用有限運算能力的設備，將隱藏在衛星影像中的祕密訊息萃取出來，並進一步與衛星影像進行視覺化疊合，以輔助地圖判讀與任務運用。

資訊隱藏技術中的簡單最低位元(Least Significant Bit, LSB)取代技術[11]因具有實作簡單及藏密量大的特性，有利於達成上述之目的。然而簡單 LSB 取代技術同時也暴露其獨特的統計特性，容易被統計分析攻擊，眾所知的卡方攻擊[12]及 RS 偵測法[13]可說是統計分析攻擊中的代表，均能有效偵測經簡單 LSB 取代技術所產生的藏密影像(Stego-image)。本文目的在提出適用於軍事地圖與衛星影像疊合之藏密技術，本技術利用改良型簡單 LSB 取代技術將二值化地圖資訊隱藏在衛星影像的，除繼承簡單 LSB 取代技術的實作簡單及藏密量大等優點外，還可同時抵抗卡方攻擊及 RS 偵測，具有比簡單 LSB 取代技術更安全的特性。

為完整說明本論文提出的技術，本論文其他段落安排如下：第 2 節為文獻探討，簡述資訊隱藏技術的概念，並說明最低位元取代技術及其面臨卡方攻擊及 RS 偵測法之弱點；第 3 節詳述我們提出的改良型 LSB 取代技術；第 4 節為與本技術相關之實驗結果；第 5 節則為本文之結論。

二、文獻探討

本節概述資訊隱藏技術，並說明最低位元取代技術的原理與安全性。

2.1 簡單 LSB 取代技術

資訊隱藏(Information Hiding)是一種隱匿資訊的技術[14]，這種起源於古老軍事情報傳遞的科學統稱為藏密學(Steganography)，主要作法是將欲傳遞的祕密訊息嵌入在掩護載體(Cover Carrier)中，以躲避第三者的察覺。藏密學與密碼學(Cryptography)的作法與要求不同，經密碼技術加密後的訊息在外觀上呈現無法理解的訊息，容易暴露其祕密通信的意圖，雖難以被第三者破解，但第三者卻可以干擾或破壞祕密通訊的進行；而藏密技術(Steganographic Technique)的提出，則是在隱藏祕密通訊的事實，提供另一層次的安全性。在實際應用上，我們會將欲傳遞的祕密訊息先行加密，再進行隱藏，如此，即使隱藏在掩護載體中的祕密訊息被第三者察覺，亦難以被破解。對於一個好的藏密技術而言，不可察覺性(Imperceptibility)與高藏密量(Capacity)是一般化的要求。所謂不可察覺性，就是人類視覺系統(Human Visual System)察覺不出藏密後的偽裝媒體(Stego-media)與原始掩護媒體(Cover-media)之間的區別；而高藏密量則是在不可察覺性的前提下，可夾帶大量的祕密訊息，以達到祕密通訊的目的

隨著資訊科技的普及，藏密技術也與時俱進，其中數位影像具有大量散佈、容易取得、及潛存龐大藏密空間等特性，已成為最普遍使用的掩護媒體[15]。數位影像藏密技術依儲存格式可區分為空間域(Spatial Domain)與轉換域(Transform Domain)兩類技術。一般來說，空間域技術比轉換域技術具有較高藏密量，而最低位元取代技術因具有實作簡單及藏密量大等特性，是最廣泛使用的藏密技術。最低位元取代技術的作法是將影像像素值(Pixel Value)的最低位元以祕密訊息來取代，由於像素值的最低位元可視為影像的冗餘部分，因此若以祕密訊息進行取代，並不會引起人類視覺系統的注意。

目前已有許多基於最低位元取代的藏密技術被提出來[16-24]，通稱為廣義LSB取代技術，其可進一步區為固定長度(Fixed-Length)與變動長度(Variable-Length)二類取代技術。固定長度取代技術是同步取代每個像素值固定n個最低位元以增加藏密量，也就是密文的取代僅會發生在固定的位元平面，因此又稱為簡單最低位元取代技術。由於人類視覺系統對於影像平滑區域的失真較複雜區域來得敏感，因此，若使用過多的固定位元進行藏密，在影像平滑區域易產生失真而暴露藏密的事實。變動長度取代技術的提出即在彌補這樣的缺失，其可依影像的特性而在不同影像特性的區域藏入不同位元的祕密訊息，期望在人類視覺的容許下盡可能達到高藏密量的目的。例如利用影像區塊複雜度的特性，在不同區塊中藏入不同數量祕密訊息位元的方法[16]；或利用人類視覺感知系統恰能察覺差異(Just Notice Difference, JND)模型，在不同像素中藏入不同數量祕密訊息位元的方法[17]；或利用藏密後與藏密前的像素值誤差距離，在不同像素中藏入不同數量祕密訊息位元的方法[24]等。為使藏密量與影像特性結合，這些方法需要額外的時間進行影像特性的計算，因此，不需要額外時間計算的簡單LSB取代技術則較適合將二值化的圖層資訊隱藏於衛星影像中。

簡單 LSB 取代技術並不會改變檔案的大小，只會造成影像最低位元平的改變，因此不會引起人類視覺系統的察覺，但由於簡單 LSB 取代技術的嵌入位置固定，且加密的訊息呈現雜亂的分佈特性，藏密後的影像會顯露出獨特的統計特性，例如產生像素對或破壞像素群組規律性等問題[12, 13]，容易為統計分析所攻擊，眾所知的卡方攻擊[12]及 RS 偵測法[13]等均能有效偵測經簡單 LSB 取代技術。

2.2 卡方攻擊技術

卡方攻擊是由 Westfeld [12]等學者所提出，由於加密後的位元串流中的 0 與 1 位元值近似均勻分布(Uniform Distribution)，因此，如果將這些密文位元串流以簡單 LSB 取代技術循序隱藏於影像最低位元平面，會導致藏密影像的像素對(Pixel Pairs of Values, PoVs)問題[12]。以 8 位元灰階影像為例，其像素值為 x，$0 \le x \le 2^8\text{-}1$。其像素對所成的集合為$\{(2i, 2i+1) \mid i \in \{0,1,\ldots, 2^{8-1}\text{-}1\}\}$，也就是共有 128 組像素對。令 f_i 為第 i 組像素對統計次數的平均值，

$f(2i)$及 $f(2i+1)$分別表示像素值 $2i$ 及 $2i+1$ 的統計次數。則經由簡單 LSB 藏密後，將造成像素值 x 由 $2i$ 變成 $2i+1$，或由 $2i+1$ 變成 $2i$，或是不變。這三種情況會使得 $f(2i)$約等於 f_i，而 Westfeld 等學者則利用這個統計特性來偵測祕密訊息存在的事實。偵測時，先找出藏密影像中可能成為像素對的總數 k，再以公式(1)估計第 i 組像素對的統計次數，接著以公式(2)計算在 k-1 自由度下的卡方統計量，最後利用卡方分佈的特性，以其機率密度函數(公式(3))推估 $f(2i)$等於 f_i 的機率 p。

$$f_i = \frac{f(2i)+f(2i+1)}{2} \tag{1}$$

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{\left(f(2i)-f_i\right)^2}{f_i} \ ; \tag{2}$$

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma\left(\frac{k-1}{2}\right)} \int_0^{\chi^2_{k-1}} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx \ 。 \tag{3}$$

假設使用簡單 LSB 取代技術連續嵌入訊息於影像前 50%像素。若使用卡方攻擊對上述藏密影像進行偵測，則結果如圖 1 所示，表示卡方攻擊可有效偵測出前 50%像素嵌有機密資訊，其中橫軸為影像的累積樣本資料量，縱軸代表累積樣本資料量中的藏密機率。

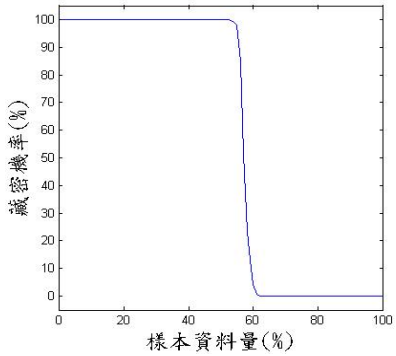


圖 1. 卡方偵測之偵測結果。

2.3 RS 偵測

RS 偵測是由 Fridrich[13]等學者所提出，他們利用翻轉函數(Flipping Function)與鑑別函數(Discrimination Function)將不重疊之連續 n 個相鄰像素群組區分為正常(Regular)、奇異(Singular)及無效(Unusable)等三種類型的群組。以 8 位元灰階影像為例，影像像素值所成的集合 x，$0 \le x \le 2^8$-1。令 $G=(x_1,x_2,\ldots,x_n)$ 表示 n 個相鄰像素群組，則鑑別函表示如下式：

$$f(G) = f(x_1,x_2,...,x_n) = \sum_{i=1}^{n-1} \left| x_{i+1} - x_i \right| \tag{4}$$

而翻轉函數是一項對像素群組 G 的置換，共有三種翻轉方式，分別為正翻轉、負翻轉與不翻轉等，分別定義如下：

正翻轉 $F_1(x)$：$2i \leftrightarrow 2i+1$，$i = 0 \ldots 2^{8-1}$-1；

負翻轉 $F_{-1}(x)$：$2i-1 \leftrightarrow 2i$，$i = 0 \ldots 2^{8-1}$；

不翻轉 $F_0(x)$：$x \leftrightarrow x$，$x = 0 \ldots 2^8$-1。

為方便翻轉操作，可以設計一個遮罩(*mask*)，並賦予翻轉值(例如：M=[1,0,0,1]，$-M$=[-1,0,0,-1])進行影像位元的翻轉操作，最後運用鑑別函數 f 與翻轉函數 F 在群組 G 進行 *mask* 翻轉，則依公式(5)、(6)、(7)計算得到三種類型群組統計量(式中 *mask* 屬於{M,$-M$})：

(1)正常群組(Regular Groups)：

$$R_{mask} = \sum G \mid f(F_{mask}(G)) > f(G) \tag{5}$$

(2)奇異群組(Singular Groups)：

$$S_{mask} = \sum G \mid f(F_{mask}(G)) < f(G) \tag{6}$$

(3)無效群組(Unusable Groups)：

$$f(F_{mask}(G)) = f(G) \tag{7}$$

一般而言，自然影像的正常群組數與奇異群組數的分佈呈現一種特殊的統計規律性。當影像無藏密時，正翻轉與負翻轉的正常群組數及奇異群組數約相等，且正常群組數大於異常群組數，其關係式下式所示：

$$R_M \cong R_{-M} > S_M \cong S_{-M} \ 。 \tag{8}$$

但對影像進行簡單 LSB 藏密後，隨著藏密量的增加，負翻轉的正常群組數(R_{-M})和正翻轉的奇異群組數(S_M)會增加，而正翻轉的正常群組數(R_M)和負翻轉的奇異群組數(S_{-M})會減少，利用此統計特性導出其交會的二次方程式，並精確估計出藏密量，除非藏密量低於 0.005 bpp (Bits Per Pixel)。

三、適用圖層疊合之改良型簡單LSB取代技術

如第二節所述，利用簡單 LSB 取代技術藏密後的影像會顯露出獨特的統計特性，容易為卡方攻擊及 RS 分析所偵測。最佳化(Optimal)LSB 取代技術[18-21]提出的目的之一即在改善簡單 LSB 取代技術易被偵測的問題。但嚴格來說，最佳化 LSB 取代技術不只會造成最低位元平面的改變，也會改變影像其他位元平面。以最低位元匹配法(LSB Matching)[25]為例，當祕密訊息位元與像素最低位元不同時，會隨機將像素值加 1 或減 1，也就是將 $2i$ 變成 $2i$-1，或將 $2i$+1 變成 $2i$+2，例如像素值為 128(10000000_2)且祕密訊息位元為 1 時，128 減 1 成為 127(01111111_2)。雖然此類方法增加了卡方攻擊的困難度及干擾 RS 分析的準確性，但也同時增加藏密技術運算的複雜度。

本節中，我們提出改良型簡單 LSB 取代技術(以下簡稱本藏密技術)，可將機敏資訊利用簡單 LSB 取代技術隱藏在影像的 LSB 中，除了可加速藏密時間外，還可有效抵抗卡方攻擊及 RS 偵測。本藏密技術主要是利用影像位元平面特性將欲隱藏的祕密訊息進行前置處理，再利用簡單 LSB 取代技術直接取代最低位元平面。影像位元平面特性及本藏密技術詳述於以下各小節。

3.1 影像位元平面特性

影像的低層位元平面與其上層位元平面息息相關。給定一張 $m\times n$ 大小的 8 位元灰階影像，我們定義 F 為影像複雜係數，其計算方式如公式(9)所示，其中 $X_{i,j}$ 表示影像第(i,j)位置的像素值，$1 \le i \le m$，$1 \le j \le n$。我們另定義函數 $f(k)$為影像第 k 位元平面的複雜係數，$1 \le k \le 8$，如公式(10)所示。其中 $B^k_{i,j} \in \{0,1\}$，表示第 k 個位元平面的第(i,j)位置的位元值(當 k = 1 為 LSB)。

$$F = \sum_{i=1}^{m}\sum_{j=1}^{n-1}\left|X_{i,j+1} - X_{i,j}\right| \tag{9}$$

$$f(k) = \sum_{i=1}^{m}\sum_{j=1}^{n-1}\left|B^k{}_{i,j+1} - B^k{}_{i,j}\right| \tag{10}$$

經實驗，我們歸納出一般自然影像的位元平面具有下列幾項特性：

性質一：影像的最低位元平面之位元值分佈看似散亂，實則與其他位元平面關聯，並具備某種程度的結構性。因此，若以擬亂分布的祕密訊息取代影像的最低位元平面，將破壞其結構性。

性質二：影像的各位元平面的複雜係數由最高位元平面向最低位元平面遞增。

性質三：對於影像的任二個相鄰位元平面，假設其中較平滑位元平面的複雜係數為 f_s，較複雜位元平面的複雜係數為 f_c，此二位平面進行互斥或(XOR)運算後所得的新位元平面的複雜係數為 f_n。由於影像各位元平面間具有某種關聯性，越相似的位元平面，其 f_n 愈趨近於 0，且不大於 f_c；反之，若位元平面越不相似，則 f_n 將愈趨近於 f_c。

性質四：若原始影像符合性質二，則藏密影像最低位元平面複雜係數 $f(1)$小於第 2 個位元平面複雜係數 $f(2)$，則可抵抗卡方攻擊；若原始影像不符合性質二，則祕密訊息與原始影像任一位元平面互斥或運算後，若其複雜係數小於第 2 個位元平面複雜係數，則以其取代原始影像的最低位元平面所得的藏密影像大多可抵抗卡方攻擊。

性質五：若藏密影像複雜係數 F 趨近於原始影像複雜係數，則可以抵抗 RS 偵測。

3.2 改良型簡單 LSB 取代技術

本小節利用上一小節所述之影像位元平面性質，提出改良型簡單 LSB 取代技術，以同時達到快速藏密與抵抗統計式攻擊的目的。改良型簡單 LSB 取代技術包括祕密訊息嵌入及祕密訊息取出與疊合兩個程序，分述於以下各小節。

3.2.1 祕密訊息嵌入程序

衛星感測影像在掃描過程中，因受大氣、地形、衛星本身系統、感測系統、地物反射變化及各種雜訊干擾，導致影像產生雜訊和扭曲，因此在將影像提供給用戶前，必須對衛星影像進行校正、消除雜訊、影像幅射值糾正、幾何校正、設定影像地理座標值與投影座

標系統等程序，而 GIS 系統的目的即在將衛星影像與地理資料(向量或矩陣)進行連結。然而，當使用者對疊合影像進行縮放操作時，有可能造成地圖與影像的位移現象，例如向量地圖縮放後可能發生道路疊合在溝渠上。為避免發生此現象，本藏密技術中所使用的圖層為二值化影像(Binary Image)。

本祕密訊息嵌入程序包括祕密訊息加密與自我相似性取代兩部分。祕密訊息加密主要結合位元攪亂(Disturbing)及區塊移位(Transposition)技巧，使加密後的祕密訊息仍保持一定的結構化，同時達到加密與抵抗統計式攻擊的效果；自我相似取代的目的在結合衛星影像本身紋理特性，使被祕密訊息取代後的最低位元平面仍具有衛星影像的結構特性，除可避免視覺攻擊(即被視覺輕易察覺)外，也可增強統計式攻擊抵抗的效果。位元攪亂、區塊移位、及自我相似取代詳細做法如下：

(1)位元攪亂

假設 *map* 表示 $m \times n$ 大小的二值祕密影像，首先在垂直方向以連續四個像素為區塊，並以區塊重疊(Overlapping)方式將祕密影像採由上而下、由左而右的順序進行初步攪亂處理。位元攪亂演算法如下：

```
for i = 1 to n
    for j = 1 to m-3
        if map(j,i) ≠ map(j+2,i)
            swap(map(j+1,i),map(j+3,i));
        endif
    end
end
```

其中 swap(*x*,*y*) 表示將 *x* 及 *y* 位置上的位元值進行交換，得到初步攪亂後之祕密訊息 *s_map*。

(2)區塊移位

將 *s_map* 區分成不重疊(Non-overlapping)且大小相同的 8×8 大小的像素區塊，再利用加密金鑰產生一隨機亂數，將上述之像素區塊進行重新排列，得到加密後祕密影像 *c_map*。

(3)自我相似取代

先將 RGB 色彩模式之測試影像轉換為 YUV 色彩模式(Y 表示色彩的亮度，而 U 及 V 表示色彩飽和度)，並將加密後的二值祕密影像 *c_map* 與轉換後的 Y 分量的高層位元平面進行互斥或運算，其結果再以簡單 LSB 取代法嵌入在影像的 Y 分量中，表示如下式：

$$Y_1 = c\_map \oplus Y_k \tag{11}$$

其中 Y_k 表示亮度分量的第 k 個位元平面，其 k 值並不具備加密效果，但其設定方式可比照加密金鑰的設定方式進行(例如事先約定)，而⊕表示位元方式互斥或運算。最後再將藏密後 Y 分量與 U、V 分量轉換至 RGB 色彩空間，形成藏密影像。

3.2.2 祕密訊息取出與疊合程序

本藏密技術之祕密訊息取出與疊合程序區分為自我相似萃取、祕密訊息解密、及圖形疊合三部分，其中祕密訊息解密部分又可細分為區塊復原及位元復原兩部分，自我相似萃取、區塊復原、位元復原、及圖形疊合等詳細做法如下：

(1)自我相似萃取

先將 RGB 色彩模式之藏密影像轉換為 YUV 色彩模式，並將 Y 分量中的 LSB 與第 k 個位元平面進行互斥或運算，如下式所示：

$$c\_map = Y_1 \oplus Y_k \tag{12}$$

其中 Y_k 表示亮度分量的第 k 個位元平面，⊕表示位元方式互斥或運算。

(2)區塊回復

先將上一步聚中所得的 *c_map* 區分成不重疊且大小相同的 8×8 大小的像素區塊，再利用解密金鑰產生一與嵌入程序相對順序的亂數，將上述之影像區塊進行重新排列，回復至原始之 *s_map*。

(3)位元回復

利用下列演算法將 *s_map* 回復至原始祕密圖層影像 *map*：

```
for i = 1 to n
    for j = m down to 4
        if s_map(j-3,i) ≠ s_map(j-1,i)
            swap(s_map(j,i),s_map(j-2,i));
        endif
    endfor
endfor
```

其中swap(*x*,*y*)表示將*x*及*y*位置上的位元值進行交換。

(4)圖形疊合

依下列演算法將已回復的二值祕密圖層影像疊合於衛星影像的 R、G、B 個別分量上：

```
for i = 1 to m
    for j = 1 to n
        if map(i,j) = 1
            C(i,j) = 255;
        endif
    endfor
endfor
```

其中C表示R、G、B其中一個分量。

四、實驗結果與討論

本節區分為三大部分以說明本文提出方法的有效性，分別為不可見性(Imperceptibility)測試、統計分析抵抗性測試、及實驗分析與討論等。

4.1 不可見性測試

為測試本藏密技術不可見性與一般簡單 LSB 取代技術同樣的優越，我們針對人類視覺系統分別進行主觀與客觀測試，其結果分述於以下各小節。

4.1.1 主觀測試

我們使用一張大小為 512×512 的 8 位元灰階影像作為測試衛星影像，並使用一張與測試衛星影像同樣大小的二值化地圖作為祕密訊息(分別如圖 2(a)與 2(b)所示)，並依照本文提出之祕密訊息嵌入程序將二值化地圖嵌入在測試衛星影像的 LSB 中，其結果如圖 3(a)所示。從視覺上來看，圖 3(a)與圖 2(a)幾乎沒有什麼差別，表示本文提出方法在主觀上具有良好的不可見性。而利用祕密訊息取出與疊合程序所產生之疊合衛星影像則如圖 3(b)所示，表示本方法可正確取出祕密訊息。

4.1.2 客觀測試

我們另以峰值信號雜訊比(Peak Signal to Noise Ratio, PSNR)作為藏密影像品質的客觀衡量，其計算公式如下：

$$\mathrm{PSNR} = 10 \times \log\left(\frac{255^2}{\mathrm{MSE}}\right)(\mathrm{dB})\ , \qquad (13)$$

其中 MSE 為均方差(Mean Square Error)，計算公式如下：

$$\mathrm{MSE} = \left(\frac{1}{m^2}\right)\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}(\alpha_{ij} - \beta_{ij})^2\ 。 \qquad (14)$$

在上式中，α_{ij} 及β_{ij} 分別表示原始影像及藏密影像在(i,j)位置的像素值。峰值信號雜訊比值越高，表示影像因藏密所產生的破壞越小，一般可以被人類視覺系統接受的信號雜訊比需要大於 30 dB。

我們先將圖 2(b)複製成四份，分別利用本文所提出的位元攪亂、位元攪亂+區塊移位、及位元攪亂+區塊移位+與圖 2(a)之第 6 位元平面進行互斥或運算等進行加密處理，其結果分別如圖 4(a)、4(b)及 4(c)所示。為與一般加密之結果對照，我們同時使用一般串流加密技術(Stream Cipher)對圖 2(b)加密，結果如圖 4(d)所示。經分別嵌入圖 2(a)後所得藏密影像之 PSNR 值如表 1 所示。

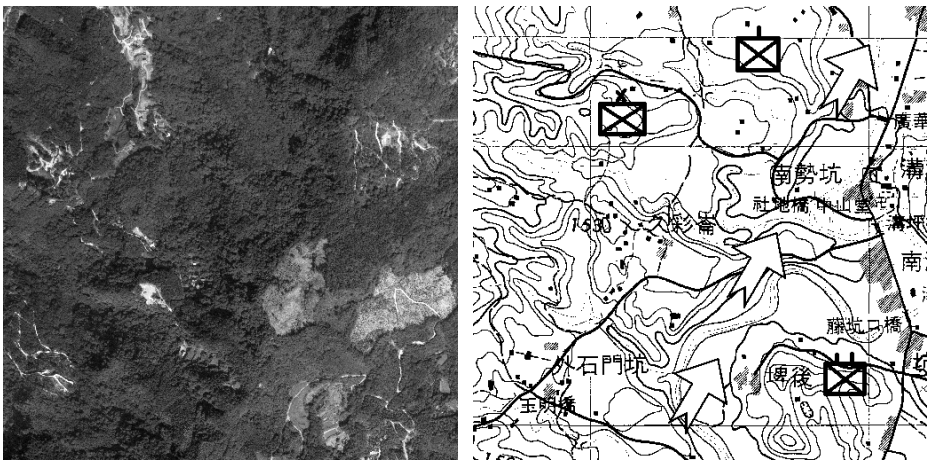
表 1. 不同藏密影像 PSNR 值

祕密訊息處理方式	PSNR(dB)
明文+簡單 LSB 取代	51.16
位元攪亂+簡單 LSB 取代	51.16
位元攪亂+區塊移位+簡單 LSB 取代	51.14
位元攪亂+區塊移位+自我相似取代	51.16
串流加密+簡單 LSB 取代	51.13

本藏密技術以祕密訊息取代影像最低位元平面。理論上，在最差情況下(均方差為 1)可確保其 PSNR 至少可達 48.13 dB 以上，而由表 1 的實驗結果顯示，利用本嵌入技術所得的藏密影像的 PSNR 值均大於 51 dB，與利用串流加密+簡單 LSB 取代技術所得之藏密影像同樣具有良好的不可見性。

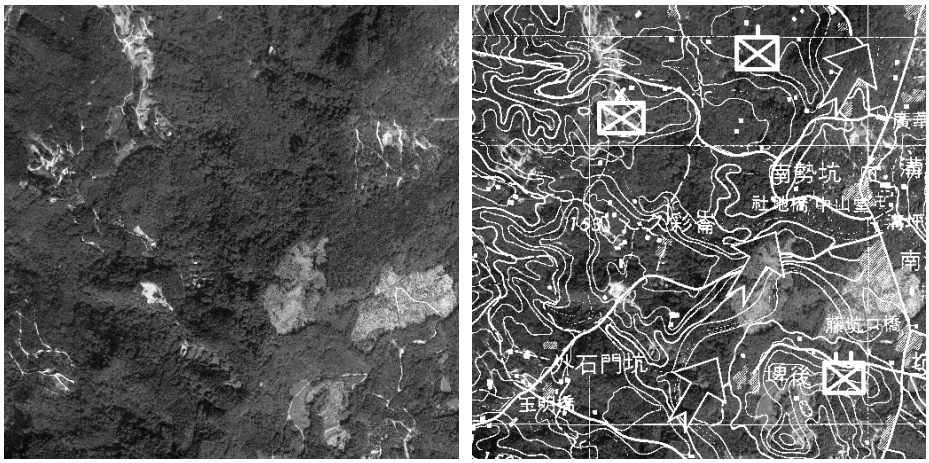
另從表 1 中我們可以發現，在所有祕密訊息處理方式中，因串流加密+簡單 LSB 取代之祕密訊息處理方式對原始影像 LSB 結構破壞最大，因此所得藏密影像的品質最差。另外，若以區塊移位後之攪亂祕密訊息取代原始影

像之 LSB，則因原始影像之 LSB 結構遭到較大的破壞，導致藏密影像的品質下降。但若以本文提出的自我相似 LSB 取代技術取代簡單 LSB 取代技術，則會改善上述之缺點，所得之藏密影像的品質與明文+簡單 LSB 取代處理方式所得之藏密影像的品質相當，同時又可獲得較好的安全性。



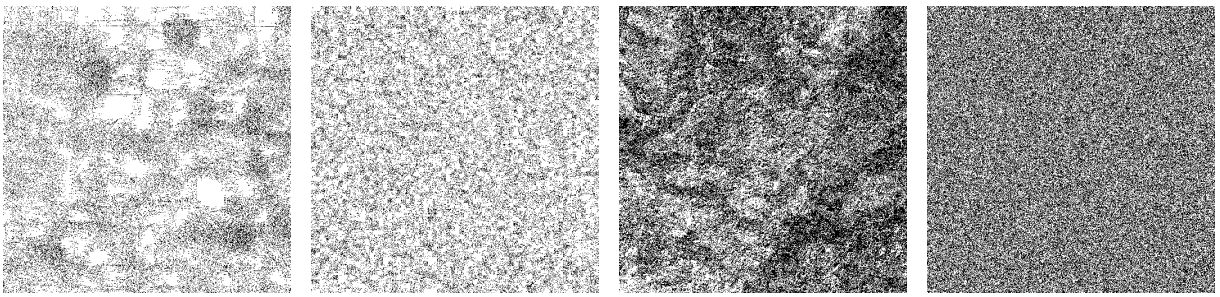
(a) (b)

圖 2. (a)未嵌入祕密訊息的測試衛星影像；(b)欲嵌入的祕密訊息。



(a) (b)

圖 3. (a)已嵌入祕密訊息的測試衛星影像；(b)經疊合後的衛星影像。



(a) (b) (c) (d)

圖 4. 祕密訊息經不同方法加密之結果：(a)位元攪亂；(b)位元攪亂+區塊移位；(c) 位元攪亂+區塊移位+與圖 2(a)之第 6 位元平面進行互斥或運算；(d)一般串流加密。

4.2 統計分析抵抗性測試

如上節所述，本藏密技術與一般簡單 LSB 取代技術一樣，均具有良好的不可見性。為驗證本藏密技術兼具更佳的安全性，本節進行本藏密技術對統計分析的抵抗性測試。本實驗所使用的測試影像為一組(8 張)512×512 大小之經典灰階影像(如圖 5 所示)及一組(8 張)512×512 大小之衛星影像(如圖 6 所示)。我們先利用不同加密與嵌入方式對祕密訊息進行處理，所得之藏密影像再分別針對知名的卡方攻擊及 RS 偵測技術進行抵抗性測試，其結果分述於以下各小節。

T1 T2 T3 T4

T5 T6 T7 T8

圖 5. 8 張經典測試影像。

S1 S2 S3 S4

S5 S6 S7 S8

圖 6. 8 張測試衛星影像。

4.2.1 卡方攻擊測試

為說明本藏密技術可有效抵抗卡方攻擊，我們在表 2 及表 3 分別列出 16 張原始測試影像各位元平面的複雜係數 $f(k)$及祕密訊息經不同方式處理後之藏密影像最低位元平面複雜係數 $f(1)$，為方便下面說明，我們在表 3 中同時列出藏密影像第 2 位元平面複雜係數 $f(2)$。

由於明文位元平面具相當結構化的紋理，因此具有最低的複雜係數(33231)；位元攪亂後之位元平面則具有較明文位元平面高的複雜係數(74479)；經位元攪亂+區塊移位處理後之位元平面又較前兩者具有更高的複雜係數(75384)；經位元攪亂+區塊移位+自我相似取代後的位元平面又較前三者具有更高的複雜係數。不管是採用上述那一種處理，處理後之位元平面複雜係數均小於第 2 位元平面複雜係數值 $f(2)$，因此用以取代原始影像的最低位元平面，並不會產生藏密影像像素對的統計特徵，均可滿足 3.1 節中性質四之要求，因此可抵抗卡方攻擊，此亦表示本文提出之藏密技術可有效抵抗卡方攻擊。

相反的，串流加密訊息的複雜係數(130804)均高於經典影像第 2 位元平面的複雜係數，因此若用以取代原始影像的最低位元平面，其藏密影像則無法躲過卡方攻擊。另外，雖然串流加密訊息的複雜係數與衛星影像的第 2 位元平面的複雜係數相近，但與衛星影像各位元平面間不具相關性，無法滿足 3.1 節中性質四之要求，因此亦無法躲過卡方攻擊。

圖 7 為 T1、T2、S1、S2 等四張測試影像經本藏密技術所得之藏密影像經卡方攻擊後之結果，其均無類似圖 1 之反應，表示本藏密技術可抵抗卡方攻擊。而圖 8 則是將串流加密後之二值地圖嵌入在上述四張測試影像，並利用卡方攻擊進行攻擊測試後之結果，顯示其無法躲過卡方攻擊。

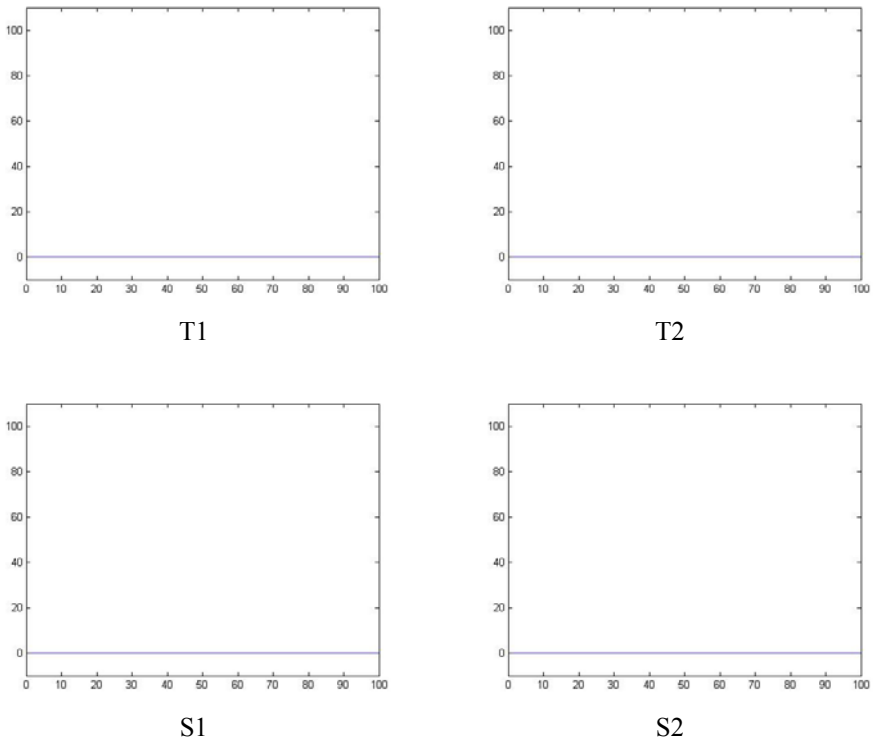


圖 7. 四張測試影像經本藏密技術所得之藏密影像經卡方攻擊後之結果。

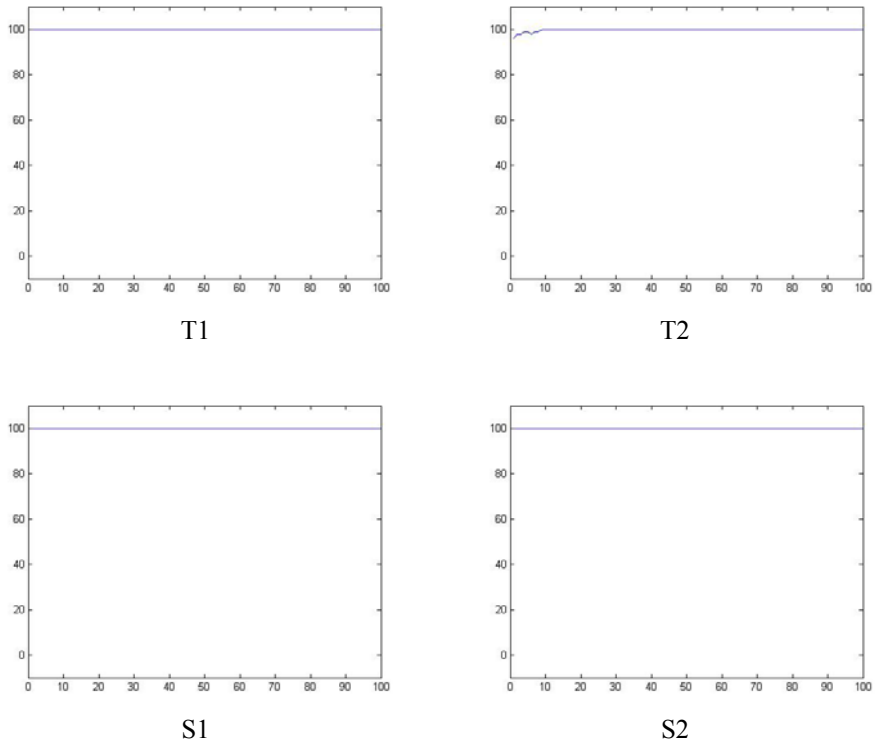


圖 8. 經串流加密後之二值地圖嵌入四張測試影像並利用卡方攻擊進行攻擊後之結果。

表 2. 原始測試影像各位元平面複雜係數值 $f(k)$

測試影像	位元平面(k)							
	1	2	3	4	5	6	7	8
T1	130703	130915	129008	112903	89547	70511	50024	31375
T2	130617	130651	124896	100982	76653	50549	23293	12780
T3	128647	124762	109936	82198	55114	32004	22448	8601
T4	120050	117236	108947	91112	66309	42172	22658	11873
T5	129954	130454	127269	107673	77387	45616	28374	13917
T6	130592	130490	130832	128609	116217	92497	61525	38716
T7	130489	130648	128596	114279	78590	47576	27248	9884
T8	130026	128109	122202	97334	68077	34668	14106	1817
S1	131029	129946	124292	108020	78756	48606	26903	21019
S2	130519	130907	131113	130641	128716	107603	64246	31191
S3	130492	130705	130230	126596	112809	79323	43143	13577
S4	130605	130326	129455	125741	113513	85184	51750	28137
S5	130221	130584	128694	121955	103179	70515	44206	4592
S6	131167	130723	130608	130511	128582	112729	69774	21179
S7	130414	129802	126197	113088	91216	68453	45491	24235
S8	130754	130371	130742	129624	121046	94776	57645	28058

表 3. 祕密訊息經不同方式處理後所得之藏密影像最低位元平面複雜係數值 $f(1)$

測試影像	$f(2)$	祕密訊息處理方式				
		明文 +簡單LSB取代	位元攪亂 +簡單LSB取代	位元攪亂 +區塊移位 +簡單LSB取代	位元攪亂 +區塊移位 +自我相似取代	串流加密 +簡單LSB取代
T1	130915	33231	74479	75384	105267	130804
T2	130651	33231	74479	75384	96545	130804
T3	124762	33231	74479	75384	78959	130804
T4	117236	33231	74479	75384	80459	130804
T5	130454	33231	74479	75384	81217	130804
T6	130490	33231	74479	75384	129751	130804
T7	130648	33231	74479	75384	79612	130804
T8	128109	33231	74479	75384	104463	130804
S1	129946	33231	74479	75384	84215	130804
S2	130907	33231	74479	75384	120727	130804
S3	130705	33231	74479	75384	109073	130804
S4	130326	33231	74479	75384	111554	130804
S5	130584	33231	74479	75384	77456	130804
S6	130723	33231	74479	75384	130118	130804
S7	129802	33231	74479	75384	123018	130804
S8	130371	33231	74479	75384	99785	130804

4.2.2 RS偵測抵抗性測試

表 4 列出祕密訊息經不同方式處理後之藏密影像複雜係數 F 及經 RS 分析之結果，其中括號內為 RS 分析所偵測出的藏密長度，單位為 bpp (Bits Per Pixel)，為方便下面之說明，表 4 中同時列出未藏密測試影像之複雜係數及經 RS 分析之結果。

如表 4 所示，由於不同影像有其不同的紋理結構與複雜度，即使在未藏密狀況下，RS 分析也可能偵測出少許藏密量，此即所謂的初始誤差。但一般而言，RS 分析對經簡單 LSB 取代所產生的藏密影像有很好的偵測效果[25]，尤其是可以有效偵測出藏密量。因此，對串流加密+簡單 LSB 取代處理所產生之藏密影像而言，RS 分析之偵測結果均接近 1 bpp，很接近真實藏密量(1 bpp)。

本藏密技術所使用的位元攪亂及區塊移位處理方式，可在結構化與複雜度之間取得平衡，因此，所產生的藏密影像複雜係數均較串流加密+簡單 LSB 取代處理所產生之藏密影像接近原始影像的複雜係數，可干擾 RS 鑑別函數對於異常群組數之統計，而導致其對藏密量錯誤之估測，因此，如同表 4 所示，RS 分析對本藏密技術所產生的藏密影像偵測之結果，均遠低於實際之藏密量(1 bpp)，此符合我們在 3.1 節中性質五對 RS 偵測抵抗性之描述。同理，本藏密技術所使用的自我相似取代方法可繼承原始影像的特性，可進一步降低藏密影像複雜係數，有效增強本藏密技術對 RS 偵測的抵抗性。

表 4. 祕密訊息經不同方式處理後所得之藏密影像複雜係數 F 及經 RS 分析之結果

測試影像	未藏密	祕密訊息處理方式				
		明文 +簡單LSB取代	位元攪亂 +簡單LSB取代	位元攪亂 +區塊移位 +簡單LSB取代	位元攪亂 +區塊移位 +自我相似取代	串流加密 +簡單LSB取代
T1	3712063 (0.0130)	3716437 (0.2096)	3721471 (0.4237)	3721004 (0.4041)	3719885 (0.3919)	3728154 (0.9985)
T2	1987299 (0.0175)	1992257 (0.1691)	1999535 (0.3897)	2000370 (0.4063)	1991639 (0.1819)	2009568 (0.9764)
T3	1443103 (0.0413)	1451061 (0.1715)	1462705 (0.3884)	1461804 (0.3721)	1456917 (0.2803)	1477330 (0.9892)
T4	1431120 (0.0011)	1439863 (0.1436)	1450219 (0.3301)	1451662 (0.3570)	1444253 (0.1981)	1466484 (0.9976)
T5	1694816 (0.0117)	1701099 (0.1997)	1707559 (0.4089)	1707340 (0.3997)	1698961 (0.1617)	1716550 (0.9553)
T6	3937290 (0.0176)	3938941 (0.1573)	3941955 (0.3874)	3942010 (0.4060)	3941773 (0.4624)	3945798 (0.9961)
T7	1684791 (0.0030)	1690137 (0.2044)	1696101 (0.4110)	1696084 (0.4177)	1690078 (0.2216)	1704388 (0.9981)
T8	1444532 (0.0069)	1451393 (0.1855)	1459975 (0.3955)	1460184 (0.4042)	1451909 (0.2396)	1471354 (0.9572)
S1	1701351 (0.0208)	1706075 (0.1420)	1713033 (0.3535)	1713086 (0.3630)	1700377 (0.1107)	1722652 (0.9531)
S2	4726289 (0.0235)	4728261 (0.1914)	4729359 (0.3715)	4729644 (0.3855)	4725709 (0.1620)	4731634 (1.0078)
S3	3321786 (0.0559)	3324575 (0.1542)	3328483 (0.4029)	3328366 (0.3831)	3323039 (0.0005)	3332476 (0.9318)
S4	3805889 (0.0173)	3808459 (0.1475)	3811831 (0.3614)	3812064 (0.3746)	3809010 (0.1469)	3816494 (0.9339)
S5	2534549 (0.0288)	2537513 (0.1526)	2542217 (0.3805)	2542214 (0.3736)	2539254 (0.2313)	2547676 (0.9844)
S6	5535921 (0.2863)	5535461 (0.1478)	5537091 (0.3619)	5537630 (0.3946)	5535212 (0.1203)	5539506 (0.8576)
S7	2992344 (0.0387)	2995963 (0.1740)	3001433 (0.3817)	3001676 (0.3917)	3000090 (0.3916)	3008578 (0.9603)
S8	3910474 (0.0013)	3912683 (0.1908)	3914901 (0.3863)	3915300 (0.3986)	3912937 (0.1796)	3918502 (0.9039)

4.3 實驗分析與討論

(1)根據 Kerchhoffs 原則[26]，由於位元攪亂並不使用金鑰，因此單獨用並不具安全性，但後續使用金鑰進行區塊移位處理則可使原先位元攪亂發揮加密的效果，此即所謂混合加密(Product Cipher)[27]，加上自我相似 LSB 取代處理，則可同時達到安全加密與隱藏祕密軍事圖層的目的。

(2)如上節所述，本藏密技術所使用之自我相似取代可有效增強本藏密技術對 RS 偵測的抵抗性。為進一步證明此效果，我們利用本藏密技術進行二值祕密地圖藏密，只是在自我相似取代階段，加密後之二值祕密地圖分別與原始影像不同位元平面進行互斥或運算，得到不同藏密影像複雜係數，如表 5 所示，其中 $k=0$ 表示原始影像；我們同時以 RS 分析對所有藏密影像進行藏密量偵測，其結果如表 6 所示。從表 5 及表 6 中可以發現，RS 分析所偵測之藏密量與藏密影像複雜係數有緊密的關係，以 S1 測試衛星影像為例，我們將其藏密影像複雜係數與 RS 偵測值繪製成折線圖，如圖 9 所示。從圖 9 中，我們可明顯看出，RS 偵測值幾乎與藏密影像複雜係數成正比，此證明我們在 3.1 節對抵抗 RS 偵測的性質敘述。

(3)理論上，若藏密影像複雜係數等於原始影像複雜係數時，可完全抵抗 RS 分析，但發生機率較低。若將最低位元平面均設定為 1

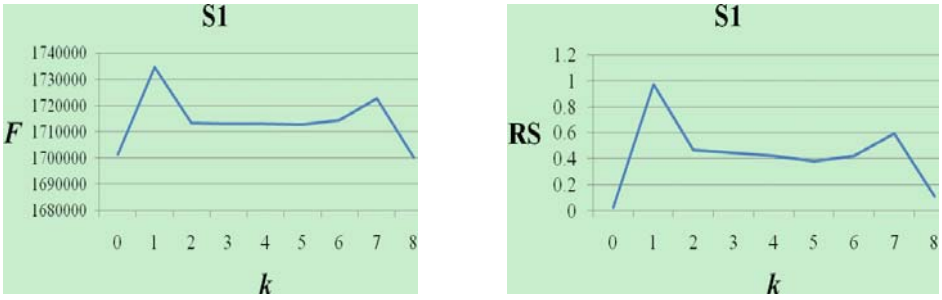
或 0，經 RS 分析所偵測的藏密量均接近 0，對簡單 LSB 取代而言，等於是無法進行藏密，因此，目前的簡單 LSB 取代技術幾乎無法抵抗 RS 分析。因此，在抵抗 RS 分析上，目的則在混淆 RS 分析對藏密量的估測值，而本藏密技術在此部分則有明顯的效果。

表 5. 以不同 k 值所得藏密影像之複雜係數

測試影像	k								
	0	1	2	3	4	5	6	7	8
T1	3712063	3737267	3720391	3722264	3722115	3722873	3719885	3723794	3701615
T2	1987299	2023471	2000273	1999546	2003278	1999979	1991639	2001147	1991890
T3	1443103	1493327	1460908	1459956	1461066	1457882	1465390	1458394	1456917
T4	1431120	1475438	1451144	1451707	1452216	1452807	1451346	1452308	1444253
T5	1694816	1729276	1707458	1707415	1710011	1704879	1711014	1706830	1698961
T6	3937290	3950424	3942084	3942110	3941773	3942409	3944395	3950957	3917992
T7	1684791	1714989	1695936	1695868	1696051	1697600	1697690	1691050	1690078
T8	1444532	1485130	1458733	1458560	1463178	1451909	1452932	1453202	1458299
S1	1701351	1734817	1713248	1712966	1713094	1712788	1714444	1722661	1700377
S2	4726289	4736037	4729879	4729773	4728889	4728364	4725709	4724678	4710167
S3	3321786	3339020	3327813	3327956	3327698	3321759	3323039	3317759	3319833
S4	3805889	3821939	3812216	3812123	3811041	3809703	3809010	3812118	3795255
S5	2534549	2555523	2541990	2541754	254945	2543557	2548107	2520282	2539254
S6	5535921	5542041	5536835	5538314	5536861	5535212	5527651	5516350	5524401
S7	2992344	3018152	3001234	3002213	3000090	3001244	3003407	3002397	2986077
S8	3910474	3923164	3914691	3914718	3914762	3914552	3913624	3912937	3897620

表 6. RS 分析對不同 k 值所得藏密影像之偵測結果

測試影像	k								
	0	1	2	3	4	5	6	7	8
T1	0.013	0.9871	0.5274	0.545	0.5134	0.4921	0.3919	0.4855	0.3819
T2	0.0175	0.9889	0.5329	0.4841	0.5225	0.4376	0.1819	0.4328	0.1685
T3	0.0413	0.9378	0.4649	0.4141	0.3997	0.326	0.4471	0.3077	0.2803
T4	0.0011	0.7948	0.433	0.4196	0.4052	0.4077	0.3752	0.3901	0.1981
T5	0.0117	0.9879	0.5333	0.4997	0.5263	0.3708	0.5013	0.3963	0.1617
T6	0.076	0.996	0.5439	0.4795	0.4624	0.4947	0.5736	0.8189	3.2415
T7	0.003	0.9879	0.55	0.5209	0.4896	0.5064	0.4842	0.2651	0.2216
T8	0.0069	0.9718	0.4952	0.4706	0.5214	0.2396	0.248	0.2486	0.3662
S1	0.0208	0.9767	0.4676	0.4457	0.419	0.3828	0.4194	0.5916	0.1107
S2	0.0235	0.9859	0.5317	0.5221	0.4214	0.3602	0.162	0.3561	3.2966
S3	0.0559	0.9995	0.4793	0.4594	0.4349	0.0872	0.0005	0.5251	0.2987
S4	0.0173	0.9735	0.4811	0.4599	0.3682	0.2779	0.1469	0.4146	1.4261
S5	0.0288	0.9865	0.4882	0.4566	0.4855	0.5118	0.6485	1.3021	0.2313
S6	0.2863	1.0049	0.4375	0.5752	0.4462	0.1203	1.6924	4.7274	2.1801
S7	0.0387	0.9778	0.5031	0.4942	0.3916	0.4109	0.4758	0.3821	0.3936
S8	0.0013	1.0104	0.5199	0.4767	0.4615	0.4	0.3043	0.1796	1.7237



(a) (b)

圖 9. 在不同 k 值下，以測試影像 S1 所得藏密影像之(a)複雜係數與(b) RS 偵測藏密量。

五、結論

本論文提出適用於軍事地圖與衛星影像疊合之藏密技術。為符合低頻寬傳輸與輕運算能力設備的作業需求，本技術利用改良型簡單 LSB 取代技術將二值化地圖經由特殊設計的加密法加密後隱藏在衛星影像的最低位元平面，合法接收者可將隱藏於衛星影像的祕密訊息或軍事圖層萃取出，經過解密後，疊合於衛星影像上。

實驗結果顯示，雖然本文提出之藏密技術作法簡單，但具有良好的不可見性，並可有效抵抗卡方攻擊及 RS 偵測，是一個兼具安全與實用之藏密技術，非常適合數位化戰場的實務應用。

誌謝

本文承行政院國科會提供經費補助(計畫編號(NSC 96-2623-7-606-020-D)，特此誌謝。

參考文獻

[1] Wang, Y., Ge, L., Rizos, C., and Babu, R., “Spatial Data Sharing on Grid,” Geomatics Research Australasia, No. 81, pp. 3-18, Dec. 2004.

[2] Cox, A. B., “An Overview to Geographic Information Systems,” The Journal of Academic Librarianship, Vol. 21, No.4, pp. 237-249, Jul. 1995.

[3] Waltz, E., “The Principles and Practice of Image and Spatial Data Fusion,” in Handbook of Multisensor Data Fusion, CRC Press, 2001.

[4] Nikander, J., Korhonen, A., Valanto, E., and Virrantaus, K., “Visualization of Spatial Data Structures on Different Levels of Abstraction,” Proceedings of the Fourth Program Visualization Workshop (PVW 2006), Vol. 178, pp. 89-99, Jul. 2007.

[5] Jiang, B., “Editorial: Some Thoughts on Geospatial Analysis and Modeling,” Computers, Environment and Urban Systems, Vol. 31, No. 5, pp. 477-480, Sep. 2007.

[6] Plaisant, C., “Information Visualization and the Challenge of Universal Usability,” in Exploring Geovisualization, Elsevier, Amsterdam, pp. 53-82, 2004.

[7] Wolthusen, S. D., “Secure Visualization of GIS Data,” Proceedings of the 2006 IEEE Workshop on Information Assurance, pp. 200-207. Jun. 2006.

[8] Aloisio, G., Cafaro, M., Conte, D., Fiore, S., Epicoco, I., Marra, G. P., and Quarta, G., “A Grid-enabled Web Map Server,” Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), Vol. 1, pp. 298-303, Apr. 2005.

[9] Komzak, J. and Slavik, P., “Scaleable GIS Data Transmission and Visualisation,” Proceedings of Seventh International Conference on Information Visualization (IV'03), Vol. 4, pp. 230- 236, Jul. 2003.

[10] Clegg, P., Bruciatelli, L., Domingos, F., Jones, R. R., Donatis, M. D., and Wilson, R. W., “Digital Geological Mapping with Tablet PC and PDA: A Comparison,” Computers & Geosciences, Vol. 32, No. 10, pp. 1682-1698, Dec. 2006.

[11] Bender, W., Gruhl, D., Morimoto, N., and Lu, A., “Techniques for Data Hiding,” IBM System Journal, Vol. 35, No. 3&4, pp.

313-336, 1996.
[12] Westfeld, A. and Pfitzmann, A., "Attacks on Steganographic Systems," Proceedings of 3rd International Workshop on Information Hiding, Dresden, Germany, 1999, pp. 61-76.
[13] Fridrich, J., Goljan, M., and Du, R., "Detecting LSB Steganography in Color and Gray-scale Images," IEEE Multimedia, Vol.8, No.4, pp. 22-28, Oct-Dec 2001.
[14] Petitcolas, F.A.P., Anderson, R.J., and Kuhn, M.G., "Information Hiding-A Survey," Proceedings of the IEEE, Vol. 87, No. 7, pp. 1062-1078, Jul. 1999.
[15] Rabah, K., "Steganography-The Art of Hiding Data" Information Technology Journal, Vol. 3, No. 3, pp. 245-269, 2004.
[16] Kawaguchi, W. and Eason, R. O., "Principle and Applications of BPCS-Steganography," Proceedings of SPIE, Vol. 3529, pp. 464-473, 1998.
[17] Lie, W.N. and Chang, L.C., "Data Hiding in Images with Adaptive Numbers of Least Significant Bits Based on the Human Visual System," Proceedings of IEEE International Conference on Image Processing, Vol. 1, Kobe, Japan, pp. 286-290, 1999.
[18] Wang, R.-Z., Lin, C.-F., and Lin, J.-C., "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," Pattern Recognition, Vol. 34, No. 3, pp. 671-683, Mar. 2000.
[19] Chang, C.-C., Hsiao, J.-Y., and Chan, C.-S., "Finding Optimal Least-Significant-Bit Substitution in Image Hiding by Dynamic Programming Strategy," Pattern Recognition, Vol. 36, No. 7, pp. 1583-1595, Jul. 2003.
[20] Yang, C.-H. and Wang, S.-J., "Weighted Bipartite Graph for Locating Optimal LSB Substitution for Secret Embedding," Journal of Discrete Mathematical Sciences & Cryptography, Vol. 9, No. 1, pp. 153-164, Apr. 2006.
[21] Mielikainen, J., "LSB Matching Revisited," IEEE Signal Processing Letters, Vol. 13, No. 5, pp. 285-287, May 2006.
[22] Zhang, H.-J. and Tang, H.-J., "A Novel Image Steganography Algorithm Against Statistical Analysis," Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, Vol. 7, pp. 3884-3888, 19-22, Aug. 2007.
[23] Yang, C.-H., "Inverted Pattern Approach to Improve Image Quality of Information Hiding by LSB Substitution," Pattern Recognition, Vol. 41, No. 8, pp. 2674-2683, Aug. 2008.
[24] Wang, C.-M., Wu, N.-I., Tsai, C.-S., Hwang, M.-S., "A High Quality Steganographic Method with Pixel-value Differencing and Modulus Function," Journal of Systems and Software, **V**ol. 81, No. 1, pp. 150-158, Jan. 2008.
[25] Manoharan, S., "An Empirical Analysis of RS Steganalysis," Proceedings of the Third International Conference on Internet Monitoring and Protection, June 29-July 5 pp. 172-177, 2008.
[26] Kerchhoffs, A., "La Cryptographie Militaire," Journal des Sciences Militaires, Vol. 9, pp. 5-38, Jan. 1883.
[27] W. Stallings, Cryptography and Network Security: Principles and Practice, third ed., Pearson Education, New Jersey, 2003.