具自身可逆性的重曝隱藏機制

蘇昱嘉、李榮三
逢甲大學資訊工程系所
cancer1986627@gmail.com、leejs@fcu.edu.tw

摘要

基於網際網路技術的蓬勃發展，多樣化的網路服務推陳出新，使得人們可透過網際網路快速取得豐富的資訊內容。其中地理資訊更是近年來熱門的巨量資料服務類別，透過龐大數量的地圖與地理屬性收集與彙整，輔助人們了解並分析地球複雜的空間資訊。空照圖資訊服務提供人們查詢目標地點周遭的地形地貌資訊，然而網際網路的環境是公開且透明的，若地圖中部分地理資訊隸屬國防的重要軍事機密，則存在極大的洩漏風險，如何提供便利卻又不危害國家安全的地理資訊服務，為本論文所要探討的議題。

本論文設計一個重曝資料隱藏機制，可針對機密影像的重點區域予以隱藏至其他部位。實驗結果顯示，本研究可確實隱密空照圖機密地帶，兼具確保國家重要軍事地點隱蔽性與提供便民的地理資訊服務。此外，合法授權者可無失真的還原既有的機密地帶影像。

關鍵詞：地理資訊、影像修補、隱像術、秘密、重曝

壹、緒論

有鑑於智慧型手持裝置的崛起與行動上網的便利性，人們的生活模式也隨之演進。透過智慧型手機或平板電腦可隨時隨地上網獲取大量資訊服務，其中地理資訊系統(GIS)整合了地圖圖資與地理相關屬性資料，搭配全球衛星定位系統技術(GPS)，可提供人們諸多便利的 LBS(Location Based Services)地理資訊服務[3]如：消防救災救護派遣、路線導航、鄰近大眾運輸查詢、空照圖地圖資訊等諸多便民的資訊服務。而政府近年來也逐步開放全國公部門所管理及生產的巨量地理空間資料(例如：全國門牌、路燈、管線、人手孔、道路等)與航拍圖資，並以開放資料的方式公開提供給民間機構做查詢、管理、規劃、決策分析等業務上的使用。然而政府在推動釋出有助於社會整體進步的地理資訊服務的同時，亦須考量其相關的資訊是否涉及國防機密資訊，如有涵蓋的部分，要如何同時滿足民眾的資訊需求與不洩漏國家重要軍事地點是一件難以達成的任務。以空照圖資訊服務為例，該涉及國防軍事地點的影像圖資，若未進行影像的降解析度或模糊化影像處理，有心人士即可從該影像窺探其內部的建築架構與軍事設備內容，亦可提取其相對應經緯度座標，進行軍事戰略的佈局，對國家安全無疑是一大隱憂。目前市面上所提供的空照圖資訊服務中，雖已針對機密地點所做了影像處理的保護，仍具有下列威脅隱憂：

1) 機密地帶的察覺：由於該影像處理的方式，會造成該區域與周遭紋理特性截然不同的視覺效果，反而更易引起有心人士的關注。

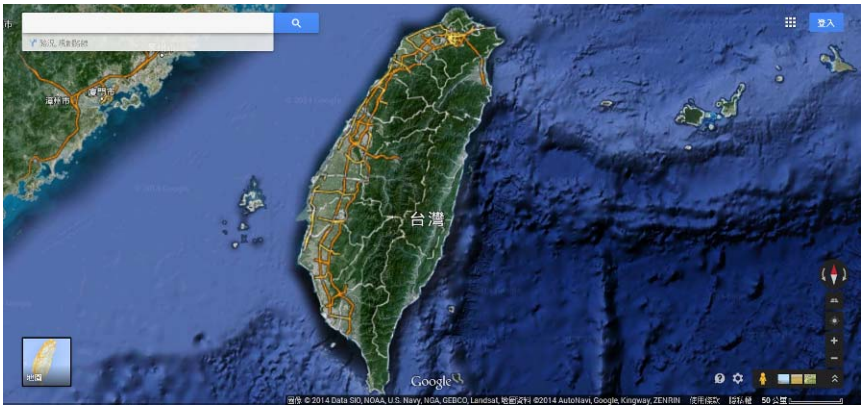
2) 未有權限控管機制：對於隸屬國防機密地點的影像區域，一般民眾皆可一覽無遺，應建立權限機制予以控管。

上述的威脅，主要的癥結點在於機密地帶能被普羅大眾所識別出來，進而擷取其相關地理屬性資訊，造成國安危機。現階段針對機密影像地帶所進行的影像處理方式為：使該影像內容無法辨識，而並非隱藏該內容。這種方式雖然使得有心人士無法進行觀測、窺探機密區域內部的建築結構與設備內容，然而有心人士依舊能從該區域是否具有模糊化、馬賽克、與該週遭紋理不連續性等視覺效果，進而推測出該區域隸屬機密地帶。本研究提供一重曝資料隱藏機制，利用影像修補的方式將機密地帶的影像紋理填補為與週遭地形地貌相同的紋理結構，令其機密影像區塊偽冒成週遭的地形地貌紋理，藉以矇騙有心人士的視覺感受，而原先的機密內容則利用資料隱藏方法藏匿至該張影像中，以便後續具有授權的對象，能從該張影像中取回並還原機密地帶的影像內容。

本論文架構分別以下列各章節詳述之。第壹章緒論，說明該研究的動機與目的。第貳章介紹空照圖影像服務。第參章說明空照圖影像服務洩漏國防機密的隱憂。第肆章先備知識介紹包含影像修補與資料隱藏技術。第伍章介紹我們的研究-自身可逆性的重曝隱藏機制，用來解決線上圖資國防機密地點曝光的問題。第陸章實際實作我們的研究方法於空照圖影像。第柒章為結論。

貳、空照圖影像服務

圖一為知名企業 google 所提供的 google map 空照圖影像服務[9]，該項服務可提供民眾瀏覽全球世界各地的高解析度空照影像圖，就猶如搭乘直升機翱翔天際般地探索世界的各個角落，且使用者可透過簡單的介面輸入地址即可存取地理編碼服務(Geocoding)[6]，定位至相對應的空照圖所在地，檢視該位置週遭的地形地貌影像。該項地理資訊服務已融入一般民眾的生活，無論是出遊要查詢目的地址的導航路線(底圖資訊具有道路圖層)，或是查詢目標地址週遭的熱門景點(底圖資訊具有熱門景點圖層)，都可透過該項便利的地理資訊服務幫你規劃路線，擺脫迷路的窘境。**圖二**說明迷路時，如何利用該項服務了解周遭路網分布與景點分布，進而順利抵達目的地。當位處人生地不熟的環境中，如何得知當地熱門的景點，或是如何規劃路線前往目的地，以往都是透過旅遊書、地圖的輔助，然而受惠於智慧型手持裝置的普及與行動上網的便利性，透過 GPS 定位將目前位置展點標示於線上地圖，藉由瀏覽線上地圖了解相對應週遭的地理資訊，再者透過導航服務，標示出指引目的地的路線圖。



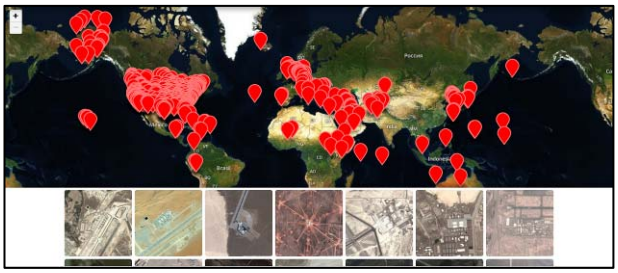
圖一：google map 空照圖影像服務圖[3]

圖二：google map 圖資服務使用說明圖

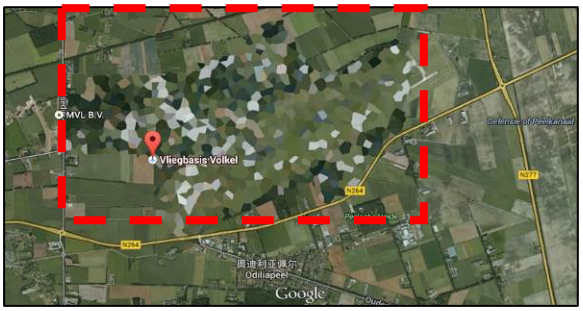
參、國防機密洩漏的隱憂

近年來由於手持裝置的盛行與行動上網的便利性，民眾可隨時隨地存取網路資訊服務，其中高解析度衛星影像的可辨識率範圍甚至可達 0.6 至 1 公尺，然而由於對比 30 公尺的範圍即可辨識出港口、船艦、基地等大範圍目標物，該解析度的精細度已足以構成軍事國防的威脅，若有心人士利用該項服務刻意於軍事機密地點存取空照圖影像服務，藉以觀測其禁區內部建築結構與設備內容，抑或是透過瀏覽空照圖影像服務來探索各軍事機密地點的經緯度座標值，這些行為都會造成國家安全的威脅。最近美國數據專家 Josh Begley 僅透過 google map 的空照圖影像服務[9]，便識別出美國部屬全球各地 600 多處的軍事地點如**圖三**，該結果再再凸顯現階段空照圖影像服務所存在之威脅[10]。而現階段商業公司 google 所提供的 google map 空照圖影像服務[9]，針對上述之威脅的應對方式為：對機密區域進行遮蔽如**圖四**紅色框選的迷彩遮蔽區塊、模糊化如**圖五**及馬賽克如**圖六**，上述方式雖可防止有心人士窺探機密區域內容，然而卻無法隱密其地理位置資訊例如：經緯度座標，實例說明：有心人士瀏覽空照圖影像服務時，若發覺該影像中部分區塊紋理與周遭影像內容不連續，即可推測其區塊隸屬機密地帶，進而提取相對應的經緯

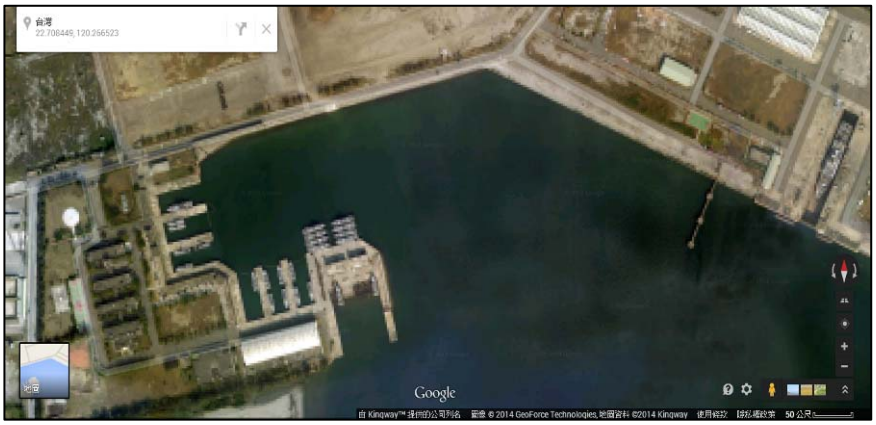
度座標，甚至撰寫程式去識別該紋理性質的地點，造成國防機密洩漏的危機。透過實作我們的方法，將機密地帶的影像內容偽冒為與周遭環境相同紋理，藉以矇騙有心人士的視覺感受，可解決上述機密地帶易被識別出的問題。



圖三：美國軍事地點位置圖[10]



圖四：google 遮蔽方式圖[9]



圖五：模糊化方式圖[9]

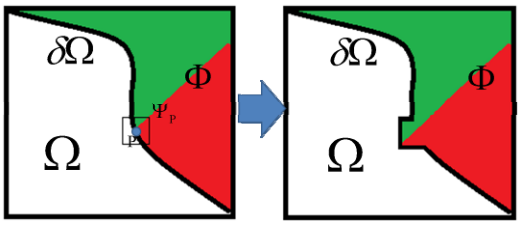
圖六：馬賽克方式圖[9]

肆、先備知識

這裡我們要介紹的先備知識，包含用來修復移除秘密區塊的影像修補技術以及將秘密區塊藏到其他部位的差異擴張隱藏技術。

影像修補

影像修補技術可用來移除數位影像中不想要保留的部分，或用來修補照片因折損而產生的摺痕，而處理過後的結果要符合人眼視覺的不可察覺性，在 M. Ashikhmin 學者提出的影像修補方法[1]與 L. Y. Wei 和 M. Levoy 等學者所提出的影像修補方法[8]，都可以成功地修補大範圍破損的影像區塊，然而卻無法保留原有影像中結構性的紋理特性，有別於以上紋理合成式的修補方法，2004 年 A. Criminisi, P. Perez 和 K. Toyama 等人提出一個基於範例型 patch 區塊的影像修補方法[5]，該方法除了能修補大面積的紋理範圍亦可處理小範圍面積結構型的物件(例如：線段、邊緣)的方法。2010 年 Agrawal 學者等人又根據該方法改善其填補效果，使得結果更符合紋理合理性[2]。研究中作者提及，填補 patch 的優先順序，為影響其線性結構可否較為合理化填補的關鍵因素如**圖七**所示，填補邊界中，有線結構通過的 patch 擁有較高的填補優先權，可延續保留既有的線性結構，其中符號代表涵義請參閱**表一**。

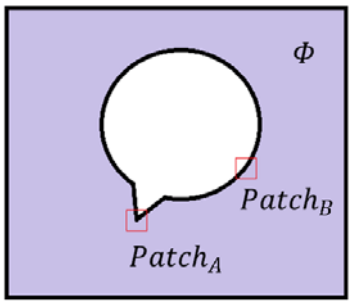


圖七：線結構優先權說明圖

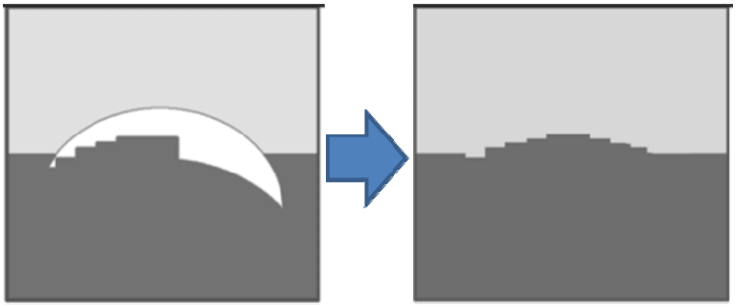
表一：符號定義表

Ω	填補區域	$C(p)$	P點中心點patch的信賴值，值越大代表遺留的Φ畫素越多
δΩ	填補邊界	$D(p)$	P點中心點patch中，含有線性結構的比例
Φ	資源區域	α	正規化參數(例:灰階圖為255)
Ψ_p	以P點為中心點的填補patch	$\nabla I_p^{\perp}$	通過P點的線向量
$P(p)$	P點中心點patch的權重值，值越大越先被填補	n_p	正交於P點的單位向量

該演算機制中的優先填補順序規則如下，以位居填補區域輪廓線上的 patch 中，遺留最多信賴值 $C(p)$ 的 patch 相對優先，藉以優先填補掉相對較往資源區域 Φ 突出的形狀如**圖八**所示，圖中由於 $Patch_A$ 的資源區域遠比 $Patch_B$ 多，所以其信賴值 $C(A) > C(B)$，以減少**圖九**所示一般填補順序所產生的不自然效果。



圖八：信賴值說明圖



圖九：不自然填補說明圖

Agrawal 學者等人所提方法[2]的整體演算法的運作步驟如**表二**敘述，分別詳述如下：

表二：Agrawal 等人方法[2]的演算步驟

	輸入:I(欲填補影像)、(填補的patch大小) 輸出:I^C(填補後的影像)
步驟一	**計算輪廓線上的所有點位的patch優先順序$P(p)$**
步驟二	**填補階段**
步驟三	**重新計算信賴值**

步驟一 ：研究中顯示優先的權重值$P(p)$如**公式 1** 會受兩大因素所影響，一為具有較高的信賴值$C(p)$如**公式 2**(代表該 patch 遺留較多的資源區域的畫素) ，該公式中$|\psi_p|$表目前 patch 面積，另一因素則為計算該 patch 擁有線性結構(如邊)的比例如**公式 3**，藉以延續保留該線性結構。

步驟二 ：更進行實際的填補作業，由上階段所計算出的優先權重值$P(p)$，取其最大值的點 p Patch 為欲填入的$\psi_{\hat{p}}$Patch，並以歐基里德距離**公式 4** 尋找其最接近的$\psi_{\hat{q}}$ Patch 取代之。

步驟三 ：更新上階段所填補的 Patch 中隸屬$\psi_{\hat{p}} \cap \Omega$的權重值**公式 5**，以表示其畫素若是經由填補的，其權重值必須衰減，間接影響其週遭附近的 Patch 優先權。

經由上述的步驟執行，直到所有填補區域Ω均已填補，則完成該張影像的修補。

上述演算法中所述公式如下：

$$P(p) = C(p)D(p) \qquad \text{(公式 1)}$$

$$C(p) = C\left(\frac{\sum_{q \in \psi_p \cap (I-\Omega)} C(q)}{|\psi_p|}\right) \qquad \text{(公式 2)}$$

$$D(p) = \frac{|\nabla I_p^{\perp} \cdot n_p|}{\alpha} \qquad \text{(公式 3)}$$

$$\psi_{\hat{q}} = \arg\min_{\psi_q \in \Phi} d\left(\psi_{\hat{p}}, \psi_q\right) \qquad \text{(公式 4)}$$

$$C(p) = C(\hat{p}), \forall p \in \psi_{\hat{p}} \cap \Omega \qquad \text{(公式 5)}$$

差異擴張法

2003 年由 Jun 及 Tian 等人所提出[7]的資料隱藏方法，藉由在嵌入階段將機密訊息藏入圖片中，以該張圖片作為媒介建立一秘密訊息傳遞通道，而在還原階段將接收到的圖片擷取出隱藏其中的秘密資訊並藉此還原原圖。其嵌入階段的方法概念主要透過一組像素值 X,Y 之間的差異量 d 擴展兩倍後，將機密資訊 $m \in [0,1]$ 隱藏於其中，並形成相對應的偽裝像素組 X',Y'。而還原階段，則透過計算一組偽裝像素值 X',Y' 的差異量 d' 及其平均值 l 即可還原原本 X,Y 像素與取出嵌入的機密資訊 m。該資料隱藏方法的特點為可無失真地還原藏匿秘密訊息過後的影像，因此可應用於醫學、軍事這些須高精準度且無失真的影像，其演算方法細節下列詳述之。

嵌入階段：

將圖片依兩畫素 X,Y 切分為多個畫素群組，計算個畫素群組的差異值 $d = |X - Y|$ 及其整數的平均值 $l = \lfloor d/2 \rfloor$，再依**條件一**判斷其畫素群組是否可藏入機密資訊 $m \in [0,1]$；其中滿足條件一代表該群組為可擴增群組，滿足**條件二**即為可改變群組，皆可藏入機密資訊；反之則為不可改變群組，無法用來藏入機密資訊，因此該方法會產生額外的對照表資訊來記錄像素群組是否有嵌入的資訊。若該畫素群組可嵌入資訊，則計算嵌入後的像素差異值 $d' = 2 \times d + m$，其載圖像素群組修正為 $X' = l + \lfloor (d' + m)/2 \rfloor$、$Y' = l - \lfloor d'/2 \rfloor$。

$$\text{條件一}: 0 \le l - (2 \times d + m) \le 255 \text{ and } 0 \le l + (2 \times d + m) \le 255,\ m \in [0,1]$$

$$\text{條件二}: 0 \le l - (2 \times \left\lfloor \frac{d}{2} \right\rfloor + m) \le 255 \text{ and } 0 \le l + (2 \times \left\lfloor \frac{d}{2} \right\rfloor + m),\ m \in [0,1]$$

還原階段：

同樣將圖片依兩兩畫素切分為多個畫素群組，根據嵌入階段所產製的對照表資訊判斷目前的像素群組是否有嵌入機密資訊，若有則計算其像素差異值 $d' = |X' - Y'|$、整數的平均值 $l = \lfloor (X' + Y')/2 \rfloor$，接著計算出嵌入的機密資料 $m = d' \bmod 2$ 和原始的像素差異值 $d = \lfloor d'/2 \rfloor$，再還原原圖的像素值 $X = l + \lfloor (d + m)/2 \rfloor$ 與 $Y = l - \lfloor (d + m)/2 \rfloor$。

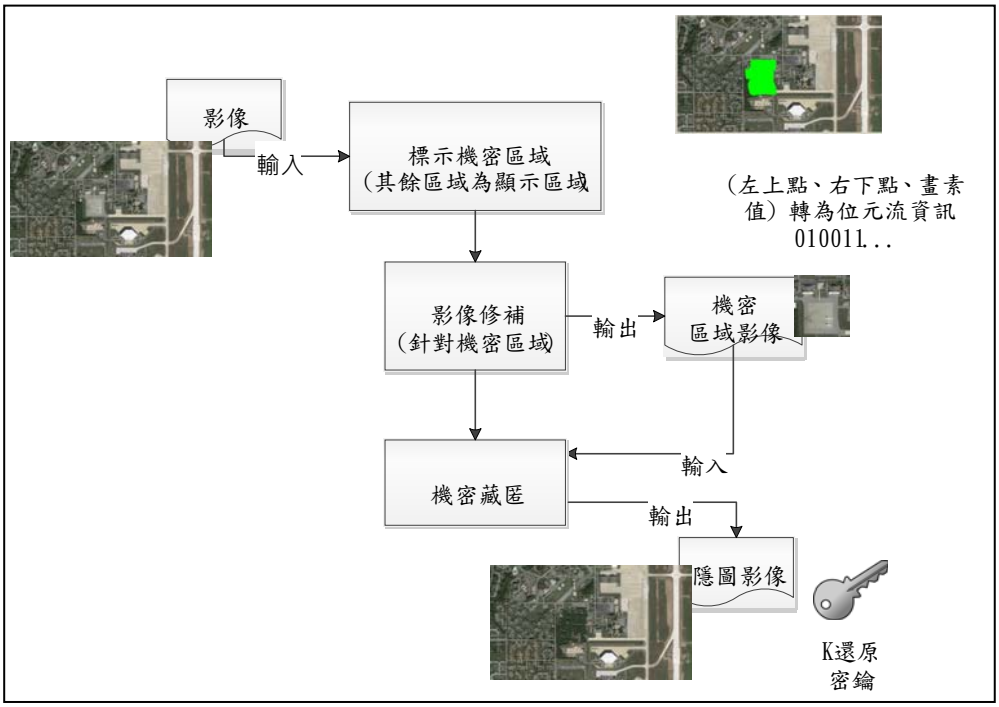
伍、自身可逆性的重曝隱藏機制

本研究取其攝影技法「重曝」一詞，藉以描述在同一張影像中，存有可將偽裝的機密區域還原的資訊，猶如攝影技法，單張照片具備兩個不同的紋理影像。本研究將一張影像區分為 S 機密區域(機密區域顧名思義即為重要區塊要予以藏匿的部分)與 O 顯示區域(整張圖像中不屬於 S 機密區域的部分即為顯示區域)，一開始先將原本的機密區域內容複製暫存，再針對機密區域的範圍進行影像修補，形成偽裝的區域 F，藉以矇騙攻擊者。在傳送之前將原本的機密區域像素值與起訖的位置座標結合成位元流，並進行加密，

再利用差異值擴增法嵌入於填補好的整張影像中；該方法即便攻擊者發現其嵌入的方法進而擷取出嵌入的資訊，也因缺乏正確的解密資訊而無法獲取機密區域的內容為何。

重曝隱藏演算法(嵌入步驟)：

為了將機密地帶的影像偽裝為其他區域的畫素值，又能確保授權者能從該張偽裝的影像中還原機密地帶，因此必須先將機密地帶內容的畫素值、位置等資訊轉為位元流，並利用差異擴張法[7]分別將每個位元嵌入於該張影像中，其嵌入演算流程如**圖十**所示，輸入欲處理的影像於本系統中，接著分別經由標示機密區域、影像修補、及機密藏匿三個階段的處理，產出一個偽裝影像Φ^c與還原密鑰K，流程步驟內容分別於下列詳述之，演算過程所使用的符號代碼涵義請參閱**表三**。



圖十：編碼嵌入流程圖

表三：符號定義表

Φ	整張原圖影像	Φ^c	藏匿後的偽裝影像
w	原圖影像的寬度	h	原圖影像的高度
H	自訂擾亂因子（實驗中取一8位元數）	K	還原密鑰(含H、R)
R	壓縮分割規則	S	機密區域
O	顯示區域	S_{start}	機密區域的左上點座標值
Φ'	經影像修補過的原圖影像	S_{end}	機密區域的右下點座標值

輸入：Φ(原圖影像)、H(自訂擾亂因子)
輸出：Φ^c(藏匿後的偽裝影像)、K(還原密鑰)

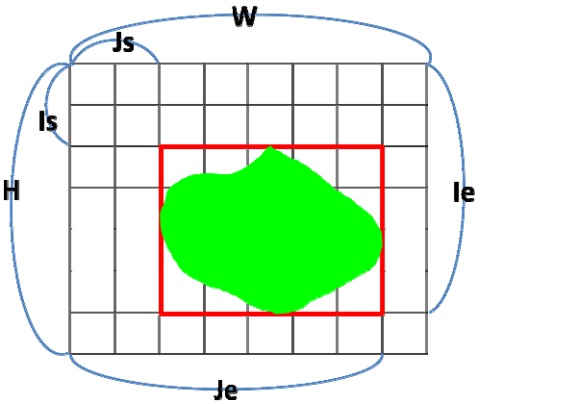
階段一(標示機密區域)：將欲傳輸的圖檔Φ載入，並標示其中欲隱藏的機密區域S，剩餘區塊則為顯示區域O，如**圖十一**所示，紅色虛線所標示區域表機密區域S，剩餘區域則屬O，為顯示區域。

圖十一：區域識別圖

階段二(影像修補)：將上階段所標示出的機密區域S，先複製一份便於後續嵌入用，該階段使用 Agrawal 學者等人[2]的影像修補方法，針對所標示的機密區域進行修補，產出Φ'圖。

階段三(機密藏匿)：將上階段所複製的機密區域S，轉換為位元流並與擾亂因子H進行簡易的 exclusive-or 邏輯運算加密$H \oplus S$、$H \oplus S_{start}$、$H \oplus S_{end}$，其中座標轉換為單一數值紀錄如**圖十二**所示，S_{start}以最大值$H \times W$為例，將其轉為二進制則$\lfloor \log_2(h \times w) \rfloor + 1$個位元數即可代表該數值(舉例:該影像大小為$16 \times 16 = 256$，則需$\lfloor \log_2 256 \rfloor + 1 = 9$個位元來表示該座標，意即稍後需嵌入 9 個位元至影像中)，將運算結果經由 RLE(run lenth encoding)[4]的壓縮以減少嵌入量，再使用差異擴張法[7]嵌入填補好的Φ'圖中，產生Φ^c偽圖影像。由於機密區域S的正確位置，與畫素值都透過擾亂因子H的邏輯運算加密且壓縮過，其中壓縮的方式與產製出的壓縮分割規則R如**圖十三**所示，圖中的 RLE function 表 Rum Length Encoding[4]的壓縮方式，圖中將機密的數值資訊M先轉為二進制，以便後續使用差異擴張法[7]將各個 bit 的位元資訊嵌入

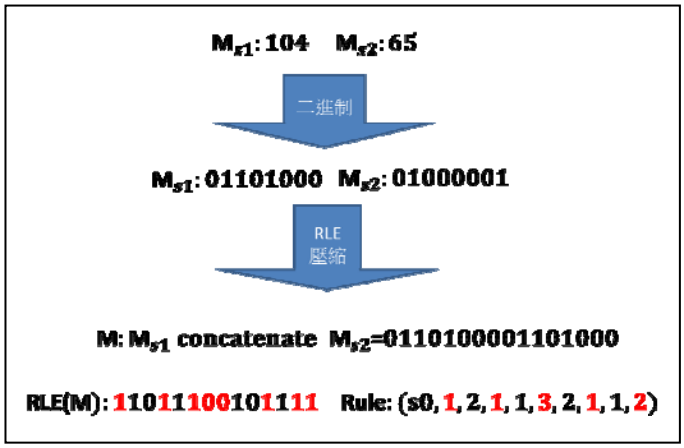
各組畫素組裡，在嵌入之前將其經由 RLE[4]壓縮過，並將其壓縮分割的規則 R (圖中 S0 代表開始的二元碼為 0)視為解密的重要參數透過安全通道傳給收方；換句話說，唯有取得正確擾亂因子 H 且知道壓縮分割規則 R 的一方(這裡我們將擾亂因子 H 與壓縮分割規則 R 視為一把私鑰 K)，才可進而還原原圖影像。



$S_{start}: Js \times H + Is, \in [0, H \times W]$ 原本(2,2) ➔ (14)

$S_{end}: Je \times H + Ie, \in [0, H \times W]$ 原本(6,7) ➔ (55)

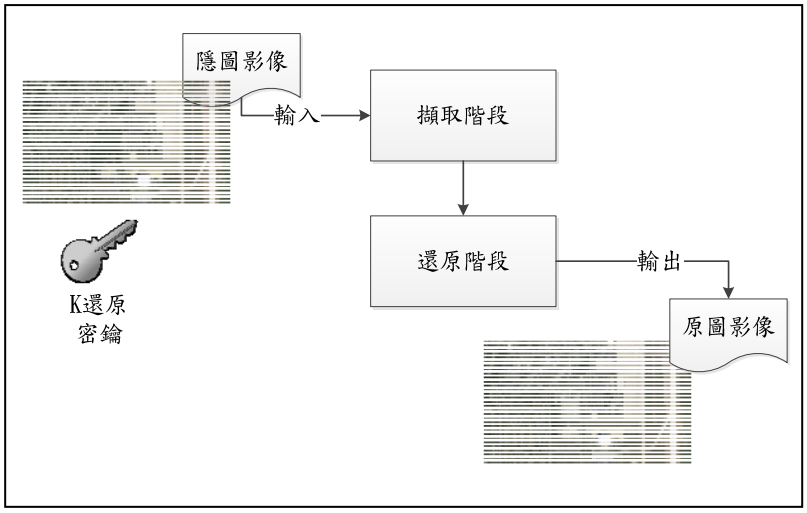
圖十二：機密區域座標換算圖



圖十三：機密內容壓縮示意圖

重曝隱藏演算法(擷取步驟)：

其嵌入演算流程如**圖十四**所示，將含有秘密訊息的隱圖影像，透過差異擴張法[7]取回秘密訊息並還原修補後的Φ'圖，由於取回的秘密訊息中含有機密地帶的位置與畫素值資訊，再依據機密地帶的位置資訊以取回的畫素質內容取代Φ'圖相對應位置的畫素值，即可還原原圖Φ。流程步驟內容分別於下列詳述之。



圖十四：還原流程圖

輸入：Φ^c(藏匿後的偽裝影像)、K(還原密鑰)
輸出：Φ(無失真的原圖影像)

階段一(擷取階段)：先從Φ^c圖中利用差異擴張法[7]，擷取壓縮過的$H \oplus S$、$H \oplus S_{start}$、$H \oplus S_{end}$。

階段二(還原機密區域)：利用傳送方所賦予的還原密鑰K(該密鑰包含自訂擾亂因子H與壓縮分割規則R資訊)，有了壓縮分割規則R可進而解回原先的$H \oplus S$、$H \oplus S_{start}$、$H \oplus S_{end}$，再透過擾亂因子H，解回S_{start}與S_{end}可得知機密區域的範圍，並以S畫素值取代，即可無失真的還原整張原圖影像Φ。

陸、實驗結果

實驗過程中我們實際採用空照圖影像，以佐證我們的機制可運行於該類型的影像上。而我們系統環境架構採用個人電腦，CPU規格為Intel Pentium4 3.0GHz搭配1G的記憶體，而作業系統為Windows Server 2003，軟體撰寫語法則採用微軟的C#語法做開發。

下列兩小節中，我們分別針對圖片嵌入機密區域相關訊息後的填補效果來做測試，是否能符合人眼辨識的不可察覺性，以證明我們的機制可確實隱匿機密地帶，達到矇騙有心人士的目的，進而確保國家機密軍事地點的隱密性。另一小節證明我們的方法具備權限控管的機制，唯有擁有授權的密鑰才可還原機密地帶的影像內容。

機密區域嵌入實驗：

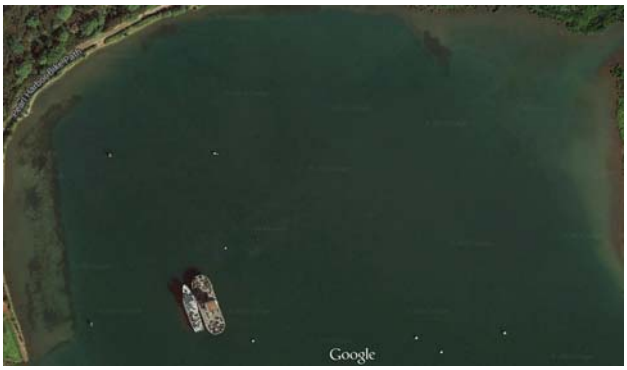
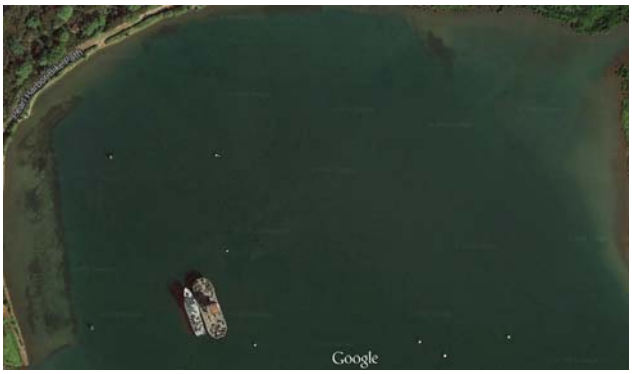
本篇論文實驗採用google map的空照圖及一般照片做為測試影像，空照圖我們選用紋理性質較為複雜如**表四**中的 **A1 圖**所示的機場空照圖實驗之。在**表四**中，我們將機場中的一處停機棚視為機密地帶，以綠色區塊將之框選如**表四**中的 **A2 圖**所示，透過我們的方法實作，可將原本的停機棚藏匿成一座樹林區域，如**表四**中的 **A3 圖**所示，由實驗結果可得知，藏匿後的載圖影像如**表四**中的 **A3 圖**，並無明顯不正常紋理性或模糊化效果，符合人類視覺系統的不可察覺性，且具有還原金鑰的合法授權者，可無失真的還原回原本加密的區域如**表四**中的 **A4 圖**，藉以實施權限控管的機制。

表四：紋理複雜隱匿表

	
A1 原圖影像圖	A2 標示範圍圖
	
A3 載圖影像圖	A4 還原影像圖

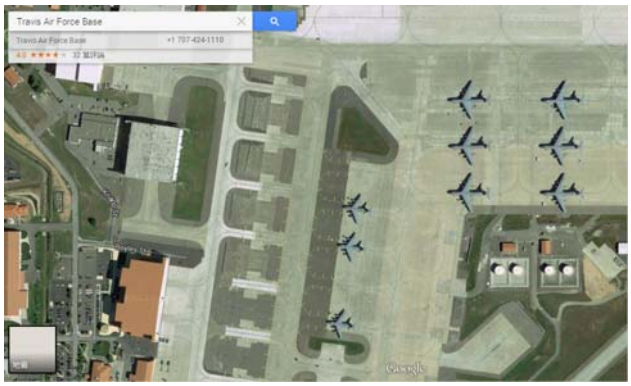
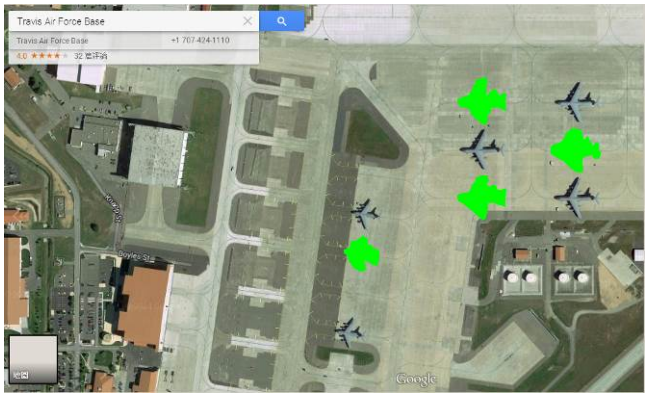
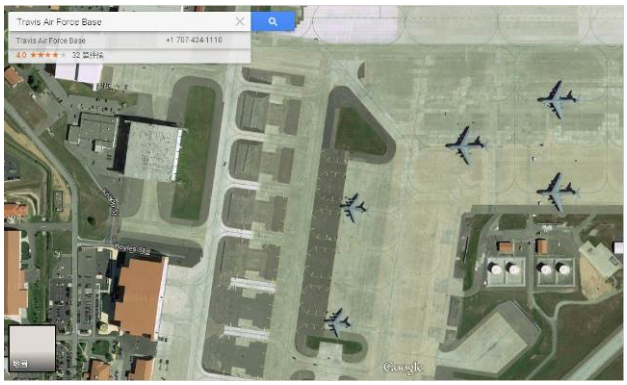
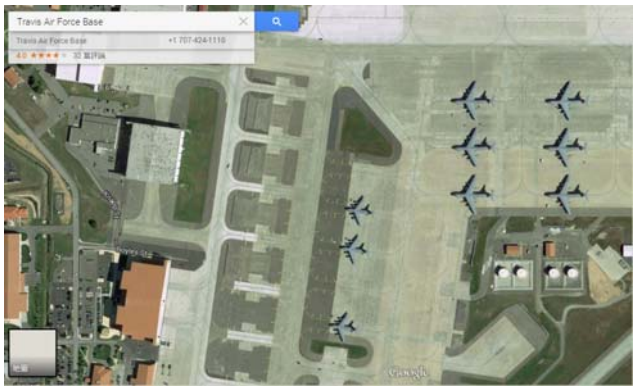
實驗中我們也選用紋理性質較為平滑如**表五**中的 **B1 圖**所示，如**表五**中的 **B2 圖**所示，我們將海灣中的兩艘軍艦視為機密地帶，並以綠色區塊框選之，經過我們的方法實作可將原本圖中的兩艘軍艦藏匿起來，形成一片海灣如**表五**中的 **B3 圖**所示，透過這種方式可以隱匿軍艦的蹤跡藉以防範軍港地點的曝光，且具有還原金鑰的合法授權者，可無失真的還原回原本加密的區域如**表五**中的 **B4 圖**。

表五：紋理平滑隱匿表

	
B1 原圖影像圖	B2 標示範圍圖
	
B3 載圖影像圖	B4 還原影像圖

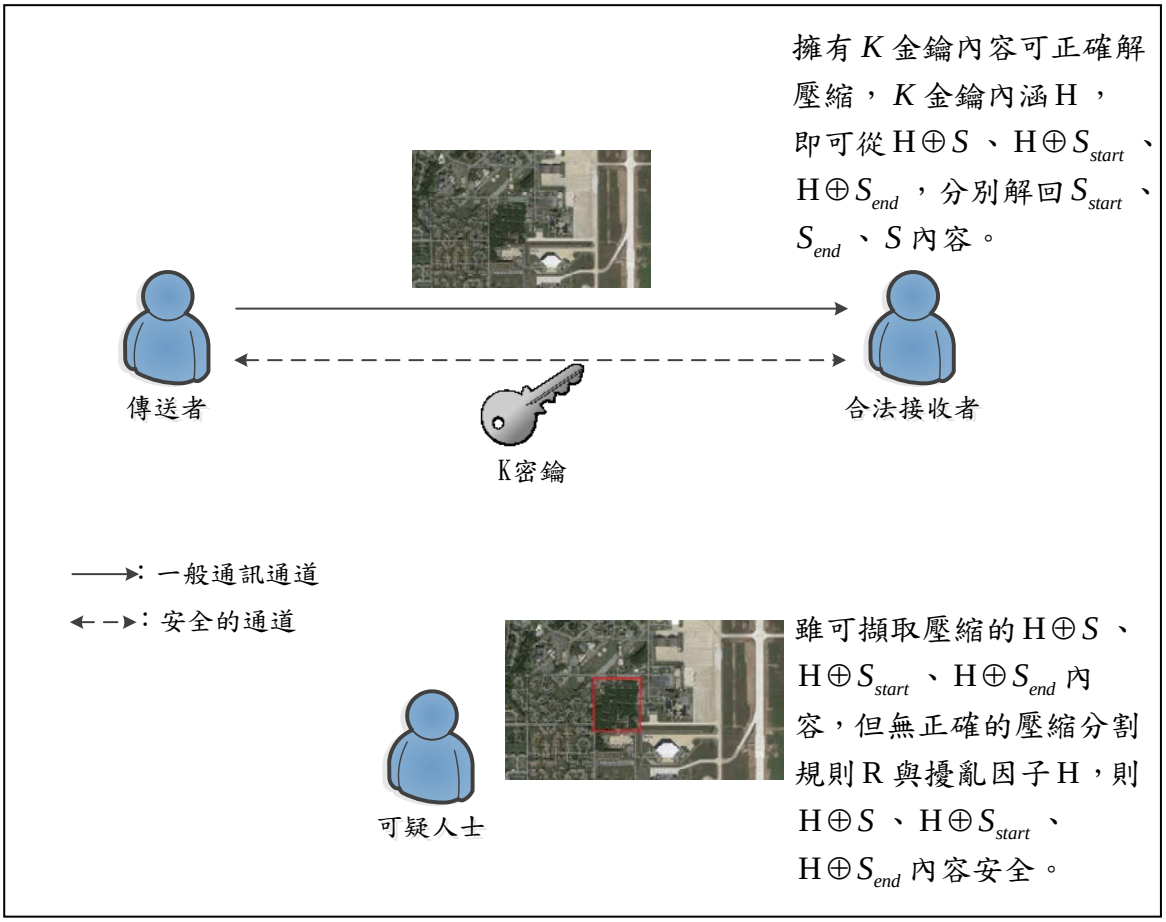
實驗中我們也針對多項欲隱藏的機密地帶如**表六**中的 **C1 圖**所示，我們選取多架戰鬥機為欲藏匿的機密地帶，並以綠色區塊框選之如**表六**中的 **C2 圖**所示，將原先九架戰鬥機其中的四架藏匿起來，藏匿的效果如**表六**中的 **C3 圖**所示，無存在不合理的紋理性，因此可有效矇騙有心人士，具有還原金鑰的合法授權者，可無失真的還原回原本加密的區域如**表六**中的 **C4 圖**。

表六：多機密地帶隱匿表

	
C1 原圖影像圖	C2 標示範圍圖
	
C3 載圖影像圖	C4 還原影像圖

權限控管機制：

在我們的方法中，將機密資訊嵌入時會經由一個使用者自定義的擾亂因子 H 做 exclusive-or 邏輯運算加密，且透過壓縮以降低嵌入量，而我們將擾亂因子 H 與壓縮分割規則 R 視為金鑰的內容透過安全的通道傳送給授權者，換句話說唯有擁有金鑰的授權者才可順利解回原先的機密資訊內容，未授權的一方即便發覺該圖藏有機密訊息，也因無法得知嵌入的方法以及金鑰內容解回原圖如**圖十五**所示，藉此達到權限的控管。



圖十五：嵌入內容安全性示意

柒、結論

我們的機制應用於空照圖影像服務是一項新的嘗試，空照圖影像服務是彙整全球衛星空拍圖及多項地理屬性資料的龐大資料集合，透過該項服務即可探索世界各個地點的空拍景色，然而這也延伸出機密軍事地點曝光的國防危機，本研究我們結合影像修補的技術與資料隱藏的概念，提出一個新型的影像秘密分享機制，我們方法針對空照圖影像服務做重點式的影像偽冒，經由實驗結果證實該方法藏匿的機密影像可符合人眼視覺的不可察覺性，矇騙有心人士，進而確保軍事地點的隱密性，在我們的方法中也結合權限控管機制，唯有合法授權者可無失真的還原機密地帶的影像資訊。

參考文獻

[1] M. Ashikhmin, "Synthesizing natural textures," *in Proceedings of the 2001 symposium on Interactive 3D graphics*, pp. 217-226, 2001.

[2] A. Agrawal, P. Goyal, and S. Diwakar, "Fast and enhanced algorithm for exemplar based image inpainting," *in Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on*, pp. 325-330, 2010.

[3] L. Barkuus and A. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns," *in 9th IFIP TC13 International Conference on Human-Computer Interaction*, pp.709 -712, 2003.

[4] J. Capon, "A probabilistic model for run-length coding of pictures," *Information Theory, IRE Transactions on*, vol. 5, no. 4, pp. 157-163, 1959.

[5] A. Criminisi, P. Perez, and K. Toyama, "Region filling and object removal by exemplar-based image inpainting," *Image Processing, IEEE Transactions on*, vol. 13, no. 9, pp. 1200-1212, 2004.

[6] M. J. Hutchinson, "Developing an agent-based framework for Intelligent geocoding," thesis, Curtin University of Technology, 2010.

[7] J. Tian, "Reversible data embedding using a difference expansion," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 13, no. 8, pp. 890-896, 2003.

[8] L. Y. Wei and M. Levoy, "Fast texture synthesis using tree-structured vector quantization," *in Proceedings of the 27th annual conference on Computer graphics and interactive techniques*, pp. 479-488, 2000.

[9] https://www.google.com.tw/maps/preview?hl=zh-TW

[10] http://empire.is/about

[作者簡介]

蘇昱嘉，就讀於逢甲大學資訊工程學系碩專班，現任於坤眾科技 GIS 工程師，主要研究領域為影像處理、網路安全、地理資訊。

李榮三，目前為逢甲大學資訊工程學系副教授，研究領域包含網路安全、影像處理、無線通訊。