戰場情資傳遞機制強化之研究

文／林志麟 少校・婁德權 上校

提要

黃石公說：「用兵之要，必先察敵情」。正意謂「情報是先戰之戰」，是全勝的基礎。在兩軍交戰之時，能先獲知正確的戰場訊息的一方，往往也佔有較高的勝算，戰場情資傳遞之重要性也就不言可喻。在資訊化的現代戰爭中，人們運用大量的高科技設備來蒐集各種有用的情報及資訊，並透過各種的通訊設施及設備來進行傳遞。但要如何確保情報資料在傳遞過程中之安全性，亦為國軍所不能輕視的議題。現行戰場資訊傳遞過程中，多半運用密碼學的加(解)密技術來保證訊息的安全性。但在情資傳遞的過程中，傳遞行為的公開化本身也是一個潛在的危險；因此若能將情報資訊在敵人無法察覺的狀態下予以傳遞，將能大幅提昇戰場機密情資傳遞之安全性。

前言

黃石公說：「用兵之要，必先察敵情」。正意謂「情報是先戰之戰」，是全勝的基礎。在兩軍交戰之時，能先獲知正確的戰場訊息的一方，往往也佔有較高的勝算，戰場情資傳遞之重要性也就不言可喻①。秘密的訊息傳遞之歷史非常悠遠，遠在西元前五世紀時就有秘密訊息傳遞技術運用之記載。希羅多德於「歷史(The Histories)」一書中，就說明此一技術讓希臘人得以免於遭受波斯暴君塞奇斯(Xerxes)征服的危機。被祖國驅逐至波斯境內的希臘人狄馬拉圖斯(Demaratus)於發現塞奇斯欲發動大規模突襲的整軍備武之行為，其將訊息刻於木製寫字版上再用一層臘將訊息蓋住，藉以躲過波斯守衛的攔截，得以將塞奇斯的突襲行動順利的通知希臘，也讓希臘人得以從容的準備以抵抗波斯的入侵，有效避免被塞奇斯征服的厄運。此種掩飾訊息存在的保密通訊法稱為資訊隱藏技術(Steganography)。此後各式各樣的隱藏技術也不斷地被發展出來，以滿足各種不同狀況下之機密訊息傳遞需求，如：中國古代將訊息寫在絲布，揉成球狀後並用臘覆蓋，交由信差吞入腹中以傳遞訊息；十六世紀的義大利科學家喬凡尼波塔(Giovanni Porta)運用明礬與醋的混合溶液，得以將訊

① 徐學謙，戰爭的智慧（高雄：派色文化出版社，1995年），頁161。

息寫入煮熟的雞蛋中，並且不改變蛋殼的顏色；或是西元一世紀時老蒲林尼(Pliny)就曾說明某些植物汁液風乾後會具透明的特性，可作爲隱形墨水來使用。機密資訊傳遞方式也隨時代的演進而有不同的發展，如各種的隱形墨水、微縮影片的標示點(microdot)等作法，都是現代情報作戰中相當常見的作法②。

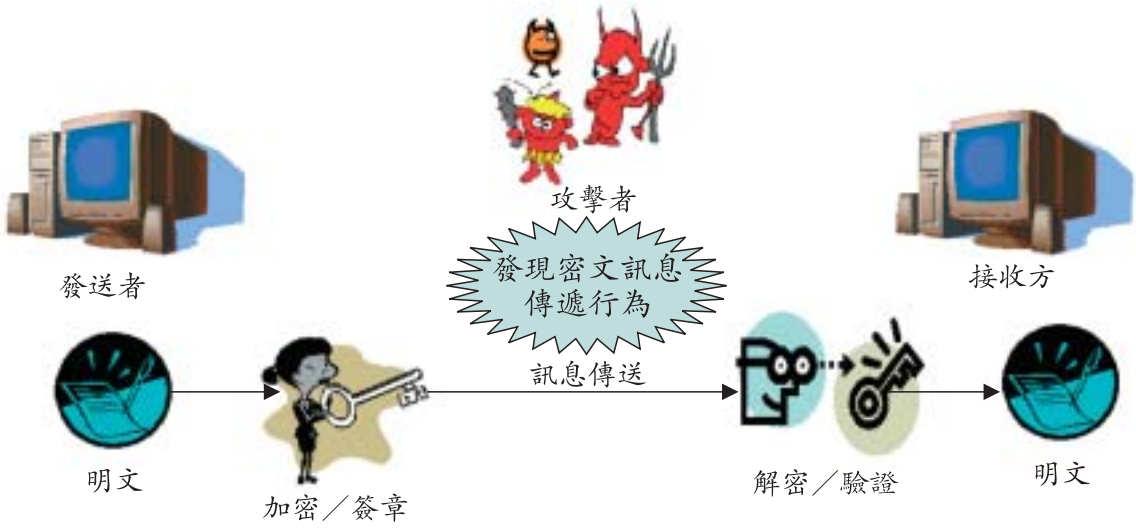
在電腦科技高速成長，資訊技術大量被運用的現代社會中，情報作戰中的訊息傳遞作法亦隨之不斷推陳出新。爲保護機密訊息在傳輸過程中之安全性，現代密碼學的加（解）密技術提供了一個有效的解決方法。訊息發送者可將欲傳送之明文訊息透過現代密碼學的加密及簽章技術處理，轉換成密文訊息，再將密文訊息傳送給接收者。接收者在收到密文訊息後，同樣利用密碼學技術進行解密及驗證的動作，如此即可確保訊息之安全，如圖一所示。

將明文訊息經過密碼技術處理後，將會形成亂碼格式的密文，雖可有效避免敵人的窺視與竄改。但是此一特性，也讓戰情資料傳遞的過程無法避免地爲有心人士起疑而遂行窺視，容易形成情資傳遞機制的漏洞。且密文訊息的傳遞量與次數，亦會成爲敵人情資蒐集參考的素材。如二次大戰時的太平洋戰場，美軍根據短期內截收到大量的日軍密電傳遞，因而判斷日軍將有大規模軍事行動，並運用情報手法而探知日軍之攻擊目標，從而締造著名於世的「中途島之役」。美軍在此役中不僅重創日軍，並也扭轉了整個戰場的局勢。因此若能將實際的戰場情資，運用資訊隱藏的技術嵌入在一般的傳播媒體中，透過日常的傳播模式來進行傳遞，如此將使敵人無法瞭解機密情資的存在，進而達到安全傳遞之目的。

一、密碼技術與資訊隱藏技術

㈠密碼技術簡介

密碼技術可分爲移位法(transposition)與替代法(substitution)兩大類，移位法是將訊



圖一　以密碼學技術進行訊息傳遞示意圖

② 賽門辛著，劉燕芬譯，碼書（台北：台灣商務印書館，2000年），頁1-50。

息裡的字母調動其順序，使訊息呈現無法解讀的狀態，只有知道調動順序的人，才能正確解讀出訊息的內容。如西元前五世紀的斯巴達密碼棒，在密碼棒上纏繞一條皮革，發訊者在密碼棒上橫向寫入訊息，當解下皮帶時，則原本訊息已被攪亂，唯擁有相同密碼棒的收訊者，才能解回原本的訊息。密碼技術的另一類作法是替代法，發訊者將原始訊息的字母用另一個字母來取代，如此也是只有知道字母取代規則的收訊者才能正確解出訊息。而替代式密碼法於軍事上的首次運用出現在凱薩大帝的高盧戰役(Gallic Wars)，凱薩在傳送訊息之過程中用希臘字母取代羅馬字母，使訊息成爲敵人無法解讀的符號，順利的阻止考慮投降的西賽羅②。

雖然傳統密碼技術爲秘密通訊提供了數世紀的安全保障，但在各式各樣的密碼分析技術被提出後，其安全度即受到質疑。當密碼技術大量的運用於各種機密訊息傳遞的場合中，而密碼分析學(cryptanalysis)也正隨著密碼學的普及應用而逐步發展。十六世紀著名的「貝平頓陰謀」展現了密碼分析學的重要性。蘇格蘭瑪莉(Mary Stuart)女王在遭受英格蘭伊莉莎白女王的監禁時，其追隨者密謀要刺殺伊莉莎白女王以解救她。在雙方通訊的過程中，雖然運用密碼技術來加密，但是卻遭到英格蘭解密學家菲力普(Philip)的破解。因此在瑪莉女王回覆同意相關刺殺行動時，就等於簽下自己的死刑判決書。瑪莉女王的密件回函經菲力普解密後，即變成法庭上不容抵賴的證據②。因此傳統密碼學的加解密技術並無法確保訊息的安全性。

密碼技術在面臨密碼分析技術的挑戰下，也不斷進步與成長。工業革命後機械化技術的迅速發展，促成各種半自動化密碼機的誕生。例如二次大戰期間，德軍的“Enigma”密碼機就在德軍初期的戰利中扮演相當重要的角色。但是破密的技術也是不斷地演進，盟軍的“ULTRA”行動，成功的破解德軍機密訊息傳遞所倚賴的密碼機；日軍大將山本五十六亦因日軍密電被美軍破解，導致其赴前線鼓舞士氣的行蹤洩漏而死於美軍的刺殺行動中③。但是相關的加密與破密的戰爭，並未隨二次大戰的結束而稍有停歇。

在二次大戰期間德國的“Enigma”密碼機每天都需要更換乙組新的密鑰，而密鑰的傳送即形成一個相當重要的問題。迪菲(Diffie)與黑爾曼(Hellman)提出一個有效解決金鑰分配問題的公開金鑰密碼(Public Key)機制④。而現代密碼技術的研究區分爲二大類。

1.公開金鑰系統

加密者與解密者分別持有各自的公鑰與私鑰，加密者以解密者的公鑰加密後，僅有解密者能還原此密文。

2.私密金鑰系統

加密與解密者擁有共同的金鑰，加密者以共同金鑰加密後，解密者使用相同的（共同）金鑰予以解密。

現代密碼學運用數論爲基礎，將破密的問題提昇至數學理論的層次。在資訊社會資

③ 山本的結局，http://hk.geocities.com/lxxsxxxxxpxx21888/youknow/sb.htm。

④ W. Diffie, M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, (1976), pp. 644-654.

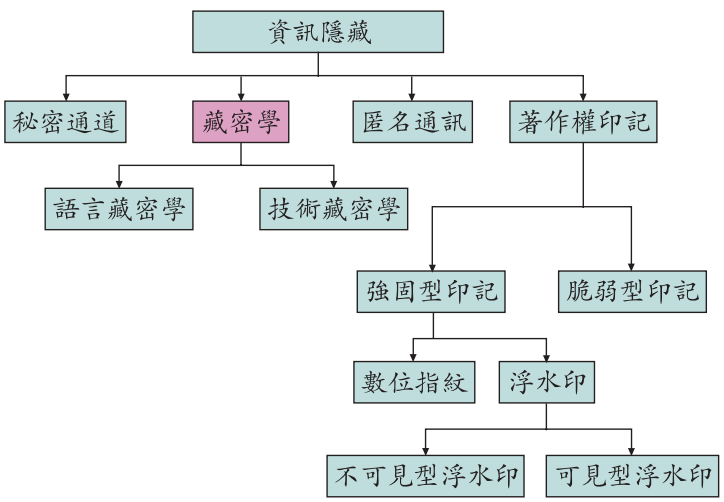
訊服務迅速發展的同時，現代密碼學也是資訊安全確保的重要屏障。但是明文訊息經過加密後，仍是會以亂碼形式存在，雖然破密者未必能有效破解出其潛藏的機密，但是卻能清楚的辨識出機密存在之訊息，無法避免地提供破密者一個可供研究之線索。

㈡資訊隱藏技術介紹

所謂的資訊隱藏，顧名思義就是將資訊隱藏在另一份媒體之中，通常我們稱這個媒體爲掩護載體(Cover-Media)，隱藏的動作叫做嵌入(embedding)，掩護載體被嵌入資訊後便成爲一份僞裝載體(Stego-Media)，而取出(extraction)或偵測(detection)的動作則是用來還原隱藏在僞裝媒體中的資訊⑤。

1.資訊隱藏技術的區分

資訊隱藏技術是將所欲傳遞的機密資料，透過隱藏處理的方式將其嵌入在一般常見的資料中，使敵人無法發覺機密訊息存在的方法。Fabien將資訊隱藏技術依照研究方向區分爲以下幾類⑥，如圖二所示：



圖二　資訊隱藏技術的分類

⑴隱匿通道(Covert Channel)

利用攻擊者無法察覺的通道來進行資料的傳遞。

⑵匿名(anonymity)

讓使用者無須洩漏自己的身份但又能得到合法認證之匿名傳遞機制，如電子選舉或是電子現金的使用等。

⑶著作權印記(Copyright Marking)

著作權的擁有者將著作標誌嵌入在傳播媒體上，在必要的時候能有效證明其所擁有之著作權。

⑷藏密學(steganography)

將機密資料以模擬一般資料的形式來傳遞，使攻擊者無法察覺機密訊息的存在，如藏頭詩、微縮影片的針孔標註或影像的訊息嵌入等方法。此爲本文機密資訊傳遞時所運用的方法，以下僅就此項技術進行介紹。

其中可用於機密訊息傳遞的技術有：隱匿通道及藏密學等兩項。其中藏密學的技術可分爲語言藏密與技術藏密等兩大類，語言藏密技術的使用需要相當程度的文學造詣，且所能藏入的資料多爲文字形式，不適合多樣化戰情資料之傳遞，所以本文將以技術藏密作爲研究重點。另依戰場情況搭配藏密學技術之設計需求

⑤ W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3&4, (September-December, 1996), pp. 313-336.

⑥ P. Fabien, R. Anderson, and M. Kuhn, "Information Hiding - A Survery," Proceedings of IEEE, vol. 87, no. 78, (July 1999), pp. 1062-1078.

與特性，會因應用領域的不同而有所變化。

2.資訊隱藏技術的要求

一個可信賴之資訊隱藏技術應該要盡可能達到以下要求。

⑴不可察覺性(imperceptibility)

嵌入之資訊必須爲人類感官所難以察覺，對於掩護媒體品質的影響應減至最低，使得攻擊者無法察覺，如此才能達到隱藏的目的。換而言之，隱藏之資訊對原始媒體具有良好的通透性(transparency)。

⑵不可偵測性(Undetectability)

利用藏密技術進行秘密通訊時，即便嵌入的資訊無法被人類感覺所察知，並不代表安全無虞，因爲媒體本身具有一些與媒體內容相關的性質，當資訊嵌入時將異動部分特性，導致其無法抵抗統計方式分析與偵知，曝露秘密通訊的行爲。

⑶安全性(security)

嵌入之資訊必須能抵抗攻擊者的偵測與分析，不能讓攻擊者從掩護媒體中移除或竄改，即使已知有資訊隱藏的情況下，仍然要保證資訊的安全。

⑷容量(capacity)

藏密技術對於資訊的隱藏容量愈大愈好，較大的容量也表示有較佳的隱藏性，即在相同的不可察覺性下，能嵌入更多的資訊是較佳的隱藏方法。

⑸有效及簡易性(efficiency)

嵌入技術之設計要簡單且有效率，資訊的藏入與取出要快速及便利。同時系統的執行時間和維護成本要盡可能降低。

然而上述需求，在實際應用時彼此會有些衝突。例如說提高隱藏資料的容量，即會降低資料的隱蔽性、不可察覺性及安全性。因此在藏密技術的應用上，必須考量隱藏的容量與其他因素來作比較與取捨。發展可以同時滿足上述各項要求的隱藏技術，是目前研究者的最大挑戰之一。一般而言，機密資訊的隱藏容量對於安全性與不可察覺性是處於互補及交換的情況②。只有在這兩個因素之間取得平衡，才有最佳之藏密效果與應用之處。

3.資訊隱藏技術的作法

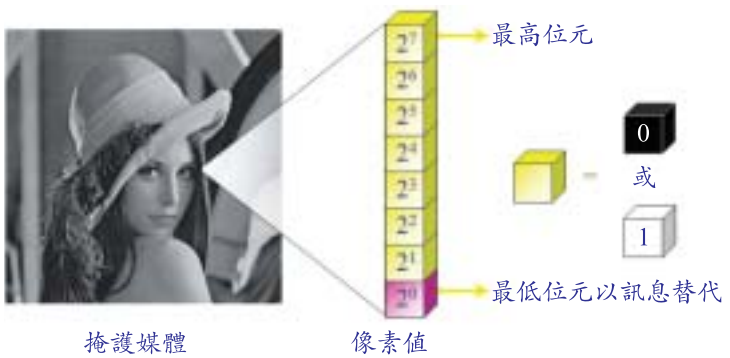
資訊隱藏技術的研究可區分空間域及頻率域兩大族群，作法說明如後。

⑴空間域

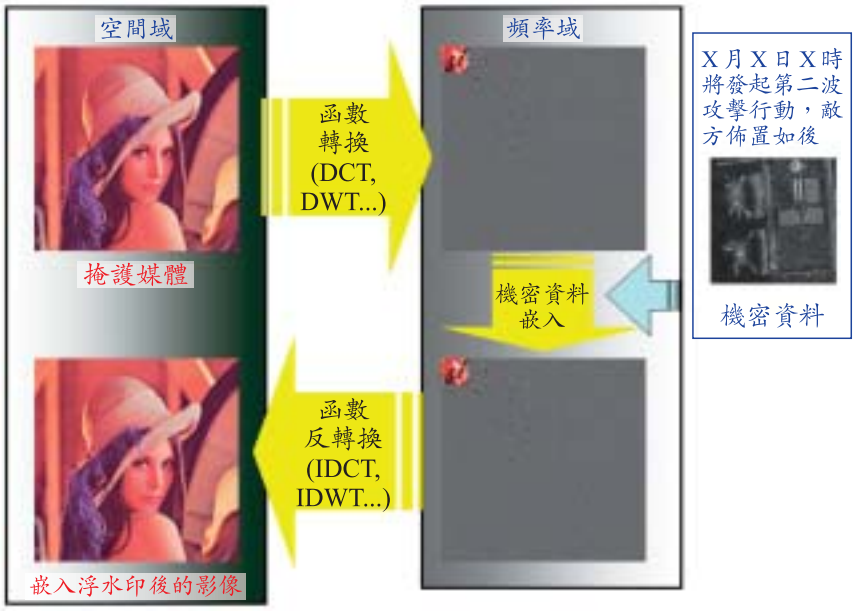
將機密資料直接藏於僞裝媒體中，如常見之最低位元(Least Significant Bit, LSB)藏密法，運作方式如圖三所示。此技術把資訊藏於最低位元，對掩護媒體(Cover Media)的影響較小，所以具有極佳的通透性。

⑵頻率域

在頻率域上的藏密作法是先將掩護媒體透過各種轉換函數，把空間域的資料轉至頻率域，完成資料藏入後再轉換回空間域，如此處理可以把嵌入資訊平均分散於掩護媒體，因此比較不容易被察覺，如圖四所示



圖三　最低位元藏密法



圖四　頻率域藏密技術

。例如：離散餘弦⑦(Discrete Cosine Transform, DCT)或離散小波(Discrete Wavelet Transform)等頻率域轉換之藏密方式，因能掌握整體之能量分佈情形，故所嵌入的機密較不易被察覺。

美國911恐怖攻擊事件發生前，美國今日報(USA Today)曾指出：「恐怖組織可能利用資訊隱藏技術，進行相關攻擊指令的下達，以避免國家安全單位的稽查。」⑧但是想要在現今網際網路中超過百億筆的影像資料與數十億個網站中，透過逐一分析並找到有隱藏資訊的圖片，幾可說是一件不可能的任務。Provos與Honeyman的研究中⑨，曾針對網路上近兩百萬張的圖片進行偵知與破密，並未能發現有嫌疑的圖片，即可見一斑。在Provos與Honeyman的結論中也提到雖針對已知的藏密工具予以分析，但也無法斷言這些實驗的圖片絕對沒有機密訊息隱藏其中，故可知道破解影像藏密工作的困難度之高。

二、強化戰場情資傳遞機制

現行之戰情傳遞機制係藉由現代密碼學技術的保護，雖不至於讓機密情資內容外洩於敵人，但是其密文情資傳遞的行爲仍是一大隱憂。因此我們可透過資訊隱藏技術的結合，將戰場情報運用資訊隱藏技術嵌入一般常見之媒體中。再將僞裝載體混入資訊網路上大量使用的資訊中，讓敵人無法察覺訊息的傳遞行爲。讓所需傳遞的重要情資能獲得更安全的保護，甚或是在敵人無法察覺的情形下，完成定期的戰情傳遞任務。

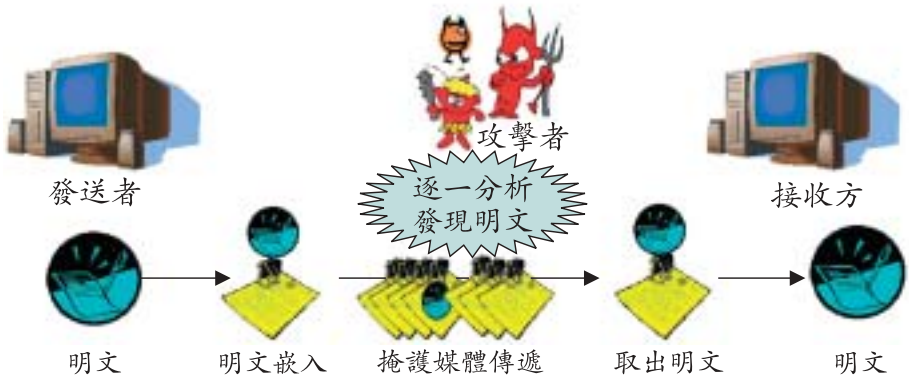
但若僅使用資訊隱藏技術來進行戰場情資資訊傳遞，則在攻擊者具備對所有傳遞資訊進行分析之能力時，我方隱藏重要戰場情資訊所使用之僞裝媒體，還是有可能在敵人進行暴力攻擊下被發現，而嵌入其間的機密也將爲敵人所知悉，如圖五所示。

綜觀國軍重要情資之傳遞，若將機密訊

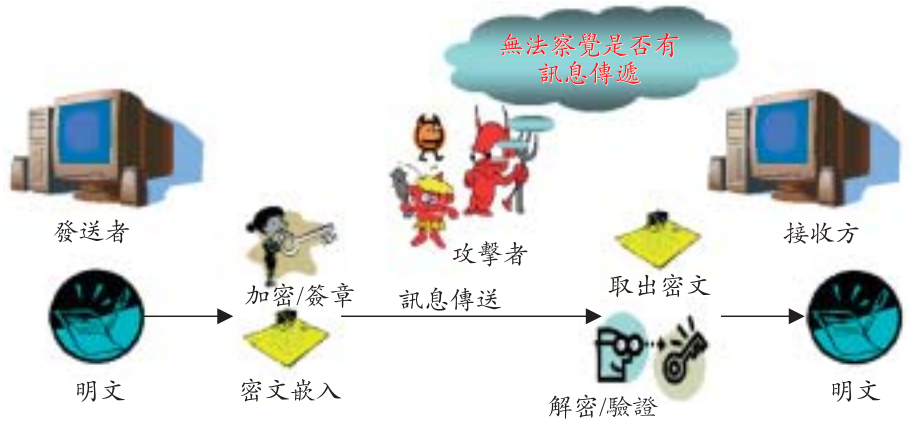
⑦ I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, (December 1997), pp. 1673-1687.

⑧ K. Jack, "Terror groups hide behind Web encryption," USA Today, (2001), http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm.

⑨ N. Provost and P. Honeyman, "Detecting steganographic content on the internet," Proceedings of the Network and Distributed Systems Security Symposium, (Feburary 2002).



圖五　僅以資訊隱藏技術進行訊息傳送示意圖



圖六　結合資訊隱藏與密碼學技術進行訊息傳遞示意圖

息加密後傳遞，固然可以防範敵人知曉情資的內容，但亂碼形式的密文傳遞過程，將成爲傳輸安全上的一大漏洞；若僅運用資訊隱藏技術來架構一個情資傳遞之機制，卻會在敵人的暴力攻擊(Brute-force Attack)下暴露出相關的訊息。所以在考量戰場各式情報資訊之高安全性需求下，可將資訊隱藏技術結合密碼學技術，來建立一套完整且具高安全性之國軍戰場情資傳遞機制。讓重要的情報資訊先經過密碼技術加密後，再透過資訊隱藏技術嵌入一般媒體中，如此則可大幅提昇機密訊息傳遞之安全性，達到在敵人不知不覺的情形下，完成情資傳遞的目的，如圖六所示。

結論

在國軍積極推動與強化指、管、通、資、情、監、偵 (C^4ISR) 系統的同時，相關戰情資訊傳遞之安全性也相形重要，本文建議運用資訊隱藏技術，以彌補現行運用密碼學技術來進行訊息傳遞時無法隱藏傳遞行爲之盲點，並提出一個可有效強化國軍情資傳遞安全之機密情資傳遞機制。在未來資訊化戰場中，若能妥當運用資訊隱藏與現代密碼學的技術來進行戰情傳遞，將能有效的整合戰場各式情資之傳遞，並且大幅提昇國軍機密戰場情報及資訊傳遞時之安全性。

作者簡介

林志麟少校，中正理工學院資訊系84年班、國防大學國防管理學院資訊所90年班，曾任保修官、通信官、隊長、連長，現就讀國防大學中正理工學院國防科學所博士班。

婁德權上校，中正理工學院76年班電機系、國立中山大學電研所碩士、國立中正大學資工所博士。曾任排長、裝載官、助教、講師、副教授。現任國防大學中正理工學院電機系教授兼電算中心主任。