國防科技學術合作協調小組研究計畫成果報告

數位國防影像及檔案資訊的網路安全傳輸

確認技術設計與研發 (II)

計畫編號： NSC90-2623-7-009-017

執行期間： 90 年 1 月 1 日至 90 年 12 月 31 日

計畫主持人：蔡銘箴 助理教授

執行單位： 國立交通大學資訊管理研究所

中華民國 90 年 12 月 31 日

目錄

1. 計畫目標：包括對象、緣起與目的

- 對象：網際網路的軍事應用。
- 緣起：

展望21世紀，以網際網路為通訊介面的應用，將是未來通訊發展的主要趨勢；網際網路的蓬勃發展已使得網路資訊的使用內容，從單純的文字檔案擴展到影像，聲音甚至動畫等的多媒體檔案；網路資源的擴充，吸引了更多的使用者，除了造就商業行銷的契機，基於經濟及實用性的考量，網際網路的軍事應用，也將是未來的趨勢。

- 目的：

網際網路的易受攻擊，如何保障數位國防影像之檔案資訊，能透過網路，安全地傳輸，辨識有否經過竄改，並做到確認傳送者，接收者的關鍵技術，是本計畫的目的。

根據前一年度計畫中，已經清楚描繪出多重浮水印架構，運用具可辨識能力的數位浮水印，對媒體文件責任區分的鑑定，不只提供數值上的相似性參考，在視覺主觀的認定上，更可以作為直接判斷的基礎；其效用比以亂數產生的浮水印更有實際應用的參考性，可提供進一步的證據。而媒體文件責任區分的能力，也可藉由在多重數位浮水印架構，於不同時加入多個數位浮水印來達成，這是有別於密碼學的加解密的機制。

而先前本研究的實驗，已證明在有限度的破壞攻擊（被攻擊後的圖形仍

具有使用價值）下，擷取多重具可辨識能力的數位影像浮水印，對資訊安全及隱私，提供媒體文件責任區分的鑑定及其不可否認性，及更強的驗證能力。

本計畫研究除以一般常用之影像圖形為研究對象外，並採用海軍所提供之空照圖為實驗圖形以為主要研究進行和探討目標，並針對偽造浮水印嵌入的問題提出相關因應的架構，以供貴單位參考使用。

2. 問題之背景、現況與需求定義

- 背景：

網際網路的普及，提高了使用者對資訊技術的要求，使用者對於媒體文件的取得與傳遞更是輕而易舉；然而在媒體文件即時的線上傳輸資料中，合法使用者僅使用加解密的資訊安全的技術，是不足以保障媒體文件之責任區分的確認，因為當數位資料傳送至接收端並完成解密動作後，加密的保護效果便不復存在。

- 現況：

由於數位資訊重製及改造的技術容易，使得數位影像之檔案資訊在應用上，衍生出對所有權保護及認證技術需求，傳送者及接收者的雙方必須對資訊來源的真實性及使用者的身份，提供認證。目前，可以公開金鑰的系統架構，來做加解密的保護，以供網路的安全傳輸。

此外，對數位影像之檔案資訊，做更積極的保護，則是對於數位影像之檔案資訊加入不易察覺的標記—如浮水印，使它能很容易地被傳送的所有權者加入或移除，由於有相當於私人簽章的加密，提供了保護的機制；但對未經授權的使用者而言，即使經過處心積慮的處理，如旋轉、平移、壓縮、放大、縮小、向量空間轉移....等等，浮水印標記仍然保留並且可供參考，使驗證者可確保所有權的歸屬，進而衍生出責任歸屬鑑定的問題。目前，這是相當重要的研究。

縱然有許多浮水印的研究持續進行，但是它仍有許多問題存在。例如：如何針對浮水印之所有權及浮水印之真偽爭議的研究（S. Craver..），仍有很大的空間，現今研究均專注於研究浮水印之嵌入與擷取，但這卻不能解決上述的問題，因為其中除了所有權人的嵌入和擷取的過程之外，非合法授權的使用者也可以做嵌入與擷取的動作，而這樣的行為會造成合法與非合法授權的使用者之浮水印的混淆，因此衍伸出有關浮水印之第三公正驗證中心的相關研究，如（G. Voyatxis..）提出了一套浮水印架構，來保護數位媒體資訊，透過 Watermark CA（浮水印認證中心）的架構來解決：1.偽造浮水印的缺點，2.原始檔案爭議的缺點；利用一經過註冊的 ID 去產生一個亂數序列當作浮水印，利用人類視覺系統（HVS）的特性來嵌入浮水印，擷取時確認這亂數序列經由 Similarity Test（相似度測試）來判斷是否有浮水印的嵌入。

- 需求定義：

如何將媒體文件如電子出版品或是國防機密影像檔案等加入浮水印，避免未經授權而欲將浮水印去除或將浮水印修改的事件發生。而必須使用數位浮水印，將其嵌入電子出版品或是國防機密影像檔案當中，因即使經過數次傳輸或有限度地破壞，出版商或是主管單位之數位浮水印仍存在於影像檔案資料之中，以作為提供媒體文件所有權界定或責任區分之證據，如此，可使得加密保護的工作更為完備。

3. 研究發現、成果與運用建議

- 研究發現

對於一般媒體文件交換系統而言，媒體文件的傳輸過程中，不外乎使用加解密的資訊安全的技術，但是單純的加解密不足以保障媒體文件之保管責任區分；因為當數位資料傳送至接收端並完成解密動作後，保密的效果便不復存在，也就是說，若媒體文件在經多次傳輸後，將很難追溯其發送者與接收者之責任。然而，若在媒體文件中，以影像圖形格式傳輸，使用數位浮水印，將其嵌入轉換後之媒體文件當中，即使經過數次傳輸、複製或有限度地破壞，各層級主管單位之數位浮水印仍存在於資料之中，可作為媒體文件責任證明之證據，使得加密保護的工作更為完備。如此，運用具可辨識能力的數位浮水印，對責任證明的確認，不只提供數值上的相似性參考，在視覺主觀的認定上，更可以作為直接判斷的基礎；其效用，比以不具參考價值的亂數產生的浮水印更有實際應用的效果，對資訊安全及隱私權的保護，提供責任證明辨認的不可否認性。本研究目前已成功地利用小波轉換 (DWT)，設計出一套多重數位浮水印的架構，可符合媒體文件在各單位傳送之需求，並能夠抵抗多種影像處理的攻擊，符合不易察覺(Imperceptible)、強韌性(Robust)以及明確性(Unambiguous)等要求。

- 研究成果

根據第一期的計畫所研究，可以得知嵌入單一數位浮水印在 JPEG 攻擊

大約 10:1 下依然可以維持在浮水印低於 5%的錯誤率，此時浮水印亦保持足夠的辨識程度可供主觀的參考。由此可知，具可辨識能力的數位浮水印，對媒體文件責任區分或所有權的鑑定，不只提供數值上的相似性參考，在視覺主觀的認定上，更可以作為直接判斷的基礎；其效用比以亂數產生的浮水印更有實際應用的參考性，可提供進一步的證據。這是有別於密碼學的加解密的機制。本研究的實驗，證明在有限度的破壞攻擊（被攻擊後的圖形仍具有使用價值）下，擷取多重具可辨識能力的數位影像浮水印，對資訊安全及隱私，提供媒體文件責任區分或所有權的鑑定及其不可否認性，及更強的驗證能力。

- 運用建議

而本研究所提出之驗證浮水印及嵌入浮水印的架構與上述不同之處在於本架構，可以輔助 CA 的架構，進一步提供公正的第三者能解決所有權確認的問題。此外本研究之浮水印架構適用於媒體文件交換系統中能夠抵抗多種影像處理的攻擊，如 JPEG 失真壓縮、剪裁攻擊（cropping）、加入雜訊...等攻擊。另用分解的方式，將浮水印分解為公開與私密兩部分，嵌入公開浮水印（Open Watermark）；驗證時，透過擷取出公開浮水印，和私密浮水印（Close Watermark）的結合成原始的浮水印，以達到所有權宣告之效果。因此，本架構不僅符合浮水印不易察覺（Imperceptible）的要求，更可以達成驗證出偽造浮水印。

4. 驗證方法與過程

由於相關的資料如文獻探討在前期計畫中有所涉獵，重要部分再度予以重述。

（一） 基本理論與假設

網際網路的普及，提高了使用者對資訊技術的要求，使用者對於媒體文件的取得與傳遞更是輕而易舉；然而在媒體文件即時的線上傳輸資料中，合法使用者僅使用加解密的資訊安全的技術，是不足以保障媒體文件之責任區分的確認，因為當數位資料傳送至接收端並完成解密動作後，加密的保護效果便不復存在。

經過詳細的研究，將媒體文件如電子出版品或是國防機密影像檔案等加入浮水印，如果未經授權而欲將浮水印去除或將浮水印取出會是相當不易，即使經過數次傳輸或有限度地破壞，出版商或是主管單位之數位浮水印仍存在於資料之中，以作為提供媒體文件責任區分之證據，使得加密保護的工作更為完備。因此，使用數位浮水印嵌入電子出版品或是國防機密影像檔案當中，是有其必要性的。

（二） 蒐集資料之正確性

- 數位浮水印

數位浮水印簡單的來說，是利用資料隱藏的技術，將一些具有代表性的資訊嵌入不同的數位媒體中。例如將作者的資訊、版權聲明、產品序號等

等，嵌入於聲音(audio)、影像(image)、視訊(video)等不同的數位媒體，以作為傳達所有權資訊、確認作品完整性等用途。與加密方法不同的，數位浮水印不預防不法的行動，但如其發生後，卻能提供證據以及相關的證明。

根據數位浮水印的特性，依其所顯示的圖像，可將其分類成可見(visible)與不可見(invisible)兩類，其作法與目的也各不相同。前者最常見的例子，可從有線電視(CATV)頻道上所傳送的視訊資料觀察，其螢幕的角落通常會有屬於該頻道特有的半透明商標(logo)，主要的用意乃在於嚇阻作用，以防止未經授權的非法盜用或翻拍，此浮水印雖然略為影響畫面的景觀，但卻無損於訂閱讀者的使用；只是在固定位置儲存的浮水印，仍然可借影像處理的方法來移除，並不可靠。較先進且牢靠的方式，則是具隱密性的不可見的浮水印(invisible watermarking)的技術，藉由將屬於原創作者的數位浮水印隱藏於數位資料中的不顯眼處，以人類肉眼(或其他感官)無法區別嵌入前後影像是否有差異為原則來為其加上浮水印，這些「識別碼」，便可作為版權證明的依據。有了如此的保護機置，創作者便可以不必公開原始作品，僅將加了浮水印的副本分送給使用者，達到保密與安全的功效；並可利用在圖片上加入不同的浮水印，給不同的使用者，以作為版權控制使用。

若以資料嵌入數位浮水印後，浮水印抵抗修改的能力，則可將浮水印分類為易碎(fragile)與強韌(robust)兩類。前類的數位浮水印對於抵抗訊號處理的能力非常脆弱，主要使用於證明資訊的完整性 (integrity)。而具有強韌性

的浮水印可抵抗訊號處理的攻擊，主要使用在所有權的宣告。

早期的數位浮水印技術，如[1]使用的 LSB (least significant bit) coding 方法，使嵌入浮水印具有不易察覺的特性。在[2]-[5]的文章則改進了[1]於抵抗影像壓縮、濾鏡處理(filtering)的缺點；但是在抵抗一般訊號處理的能力上，LSB coding 的方式仍有不足之處。針對此一缺點，目前的浮水印技術多採用 transform-domain 的方式[6]-[9]，如[6]使用數位餘弦轉換(DCT)，將浮水印嵌入於 DCT 係數的前 1000 大的數值當中，以抵抗訊號處理的攻擊。

所嵌入之數位浮水印大多為亂數產生的序列，如[6][14]使用的 Gaussian distributed random number。此類的浮水印只能在驗證程序中使用，在視覺上並不具備實質參考的意義；此外，其用作證明版權的方式，為計算待測圖形擷取之浮水印與原始嵌入浮水印的相關程度，以大於某一門檻值(threshold)說明此待測圖形為其所有。因此，若使用一視覺上可辨識的影像作為嵌入圖形之數位浮水印，如商標、或版權所有人的印章，在驗證浮水印相關程度的同時，能提供更進一步的版權證據。

類似研究在[10]中有以 DCT 的步驟作比較，其方法是以類似 JPEG 的編碼，以事先預定的排列方式來加入浮水印，所採用的浮水印圖形幾佔原影像圖形之 1/4，實不可謂不大。由於浮水印本身太過龐大，致使影像的品質受到影響，連帶地使以[10]描述所製造的浮水印圖形其抵抗攻擊的能力，為之減弱。而在[11]作者提到的方法是，在浮水印擷取的過程中不需要參考原

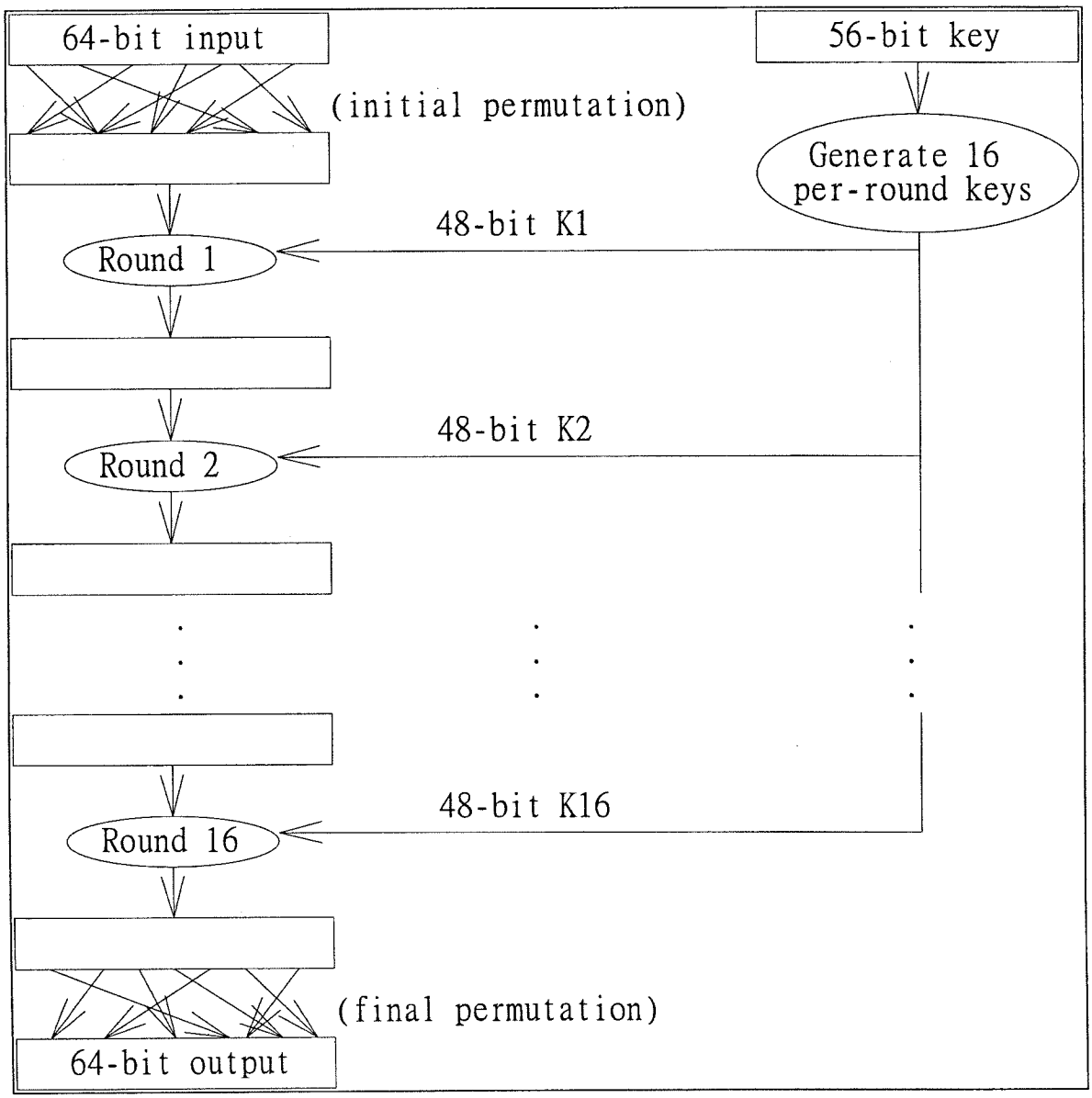
始的圖檔，即可把浮水印順利取出，這樣也方便了驗證的過程。

總括而言，目前最常使用的影像浮水印技術，基本上可分為 spatial domain時域空間及frequency domain頻率空間的處理方式。spatial domain採取的方法，選擇性地對數位影像的畫素 pixel 單位做處理，由於只有局部區域經過改變，若是已知修改的範圍，資料可以很輕易的做調換或更改，所提供的安全保護並不周密；而以 frequency domain 作為處理的運算空間，一般而言， Wavelet Transform 小波轉換[10-19]的效果較好，而經其在 frequency domain 處理後的資料，即使只有局部的修改，經由 inverse transform 後，浮水印的標記擴展到整張圖片，使得整張畫面都富含浮水印的標記；再加上利用分析 Human Visual System (HVS) 人體視覺系統所得到的知識，使加註的信號，無法查覺，並且不干擾到畫面的主題。所以，在 frequency domain 隱藏浮水印的信號，較 spatial domain 的處理有較高的安全保障。基於隱密性、安全性的考量，frequency domain 的處理模式，將會是影像浮水印技術的主流。

- **DES 加密**

DES(Data Encryption Standard)[20-25]是在 70 年代中期由美國 IBM 公司發展出來，且被美國國家標準局公佈為資料加密標準。迄今為止，在已知的公開文獻中，還是無法完全徹底的破解掉 DES。所以，DES 至今仍被認為是一種安全的加密方法。(目前最新的標準為 AES，其整體速度反應較慢但安全程度則較高)

下圖是 DES 的基本架構：



DES 是屬於區塊加密法（Block Cipher），所謂的區塊加密法就是對一定長度的明文 (Plaintext) 或密文 (Ciphertext) 來作加密或解密的動作。而在 DES 中，每次加密或解密的區塊大小都是 64bits。一般而言，資料長度通常都大於 64bits，因此我們只要將明文或密文每 64bits 切成一個區塊，再對每一區塊作加密或解密的動作即可。另一方面，DES 所用的加密金匙 (Enciphering Key) 或解密金匙 (Deciphering Key) 的長度也是 64 bits，但其中有 8 個 bits 是用來作 parity check 的，所以真正有效的金匙長度 (Key Length) 只有 56 bits。

其中 64 bits 的輸入是先經過一個初始置換 (initial permutation) 的運算，再經過 16 個回合的 f(ki)（i=1..16） 的運算，最後再做一個結尾置換 (final permutation) 的動作，即可得到一個區塊的輸出。而每個回合的 key length 是 48-bits， 是由原來的 56-bit Key 中取出不同的 48-bit 的子集合而來得。在 DES 的加密與解密是除了在 16 個回合所使用 Key 的順序不同外，其他部分則是完全相同的。

- **RSA 非對稱金鑰系統**

RSA[20-25]是以它的發明者 Rivest，Shamir 及 Adleman 的名字來命名的，它被證明是一個在 Open key encryption 及數位簽章中使用可靠度極高的理論。RSA 的安全性是來自於有關因數分解 large numbers 的問題。

RSA 所使用的 key 是從兩個很大的質數 p 和 q（p，q 的長度可能超過 200

digits)計算而來的，Open key 是由 n 和 e 兩組數字所構成的，其中 n = p x q；而 e 的值是一個隨機選取的數但須與 (p -1) x (q - 1)互質。Close key，d，是由 d = e^{-1}(mod (p -1) x (q - 1))所計算出來的，然後 p 和 q 即可毀去不用或要保密以保持 RSA 的安全性。

若 B 想祕密傳送 plaintext m（m 須小於n_A）給 A，則 B 先由公開檔案或由 A 提供，找出 A 的 Open key（e_A，n_A），B 接著執行加密動作：

$$C = Encrypt(m) = m^{e_A} (\mathrm{mod}\, n_A)$$

B 將 ciphertext C 送給 A，A 收到 C 後，利用其 Close key d_A來做解密的動作：

$$m = Decrypt(C) = C^{d_A} (\mathrm{mod}\, n_A)$$

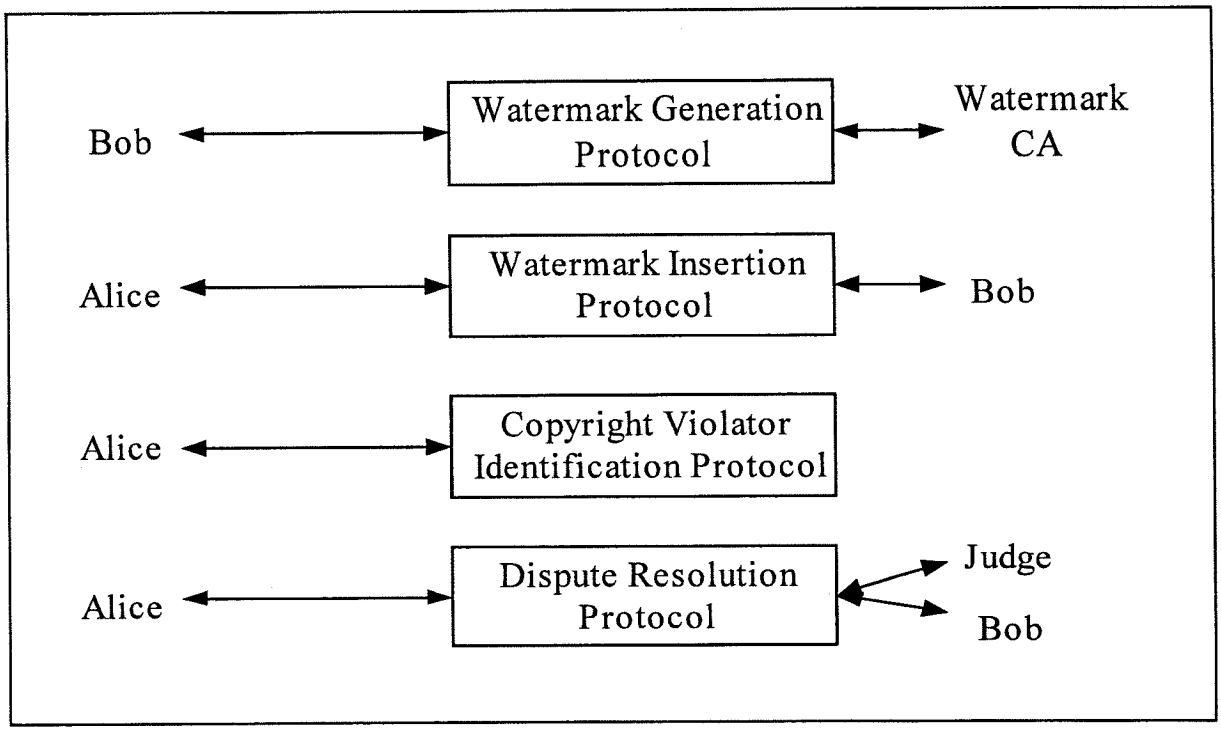
事實上 d 和 e 的值是可以互換的，所以 d 可以用來做加密而 e 可用來做解密的 key。

- **Buyer-Seller(B-S)** 浮水印協定

B-S 浮水印協定[27]是一個可解決浮水印爭議及如何確定非合法授權的複製品的一個機制，它建構在浮水印與 PKI 系統的安全機制上，另外在浮水印的確認部分，它需要一個可以產生浮水印的 CA 來作公正的第三者，而其中採用類似數位簽章的方式來確立浮水印的相關程序，以下即是相關步驟詳細介紹:

B-S 浮水印協定,主要分成四個部分 Watermark Generation Protocol，Watermark Insertion Protocol，Copyright Violator Identification Protocol，

Dispute Resolution Protocol 如圖:



(1) Watermark Generation Protocol:

此部份需要一個 CA，來作確認身分與公開 KEY 和私密 KEY 的產生，與浮水印的產生，首先，Bob 向 CA 作確認身分與公開金鑰的產生，與浮水印的產生，等 CA 收到確認後，它會傳回給 Bob 一 *EKB(W)*和一個數位牽章 *Signc(EKB(W))*而且 Bob 也將 E*KB* (W)送給 Alice.

(2) Watermark Insertion Protocol:

當 Alice 收到 *Signc(EKB(W))*後，和收到 *EKB(W)*後，作確認的動作，接著，先嵌入一個屬於 Alice 的浮水印，接著將 *EKB(W)*打散成 $\delta EKB(W)=EKB(\delta(W))$， 再嵌入於圖形中，後將圖形用 Bob 的 Open key 加密後傳送給 Bob，而 Alice 則需儲存這些相關資訊(ID,....)等

(3) Copyright Violator Identification Protocol:

經由擷取的演算法 D(X,Y)解出浮水印 U，比對這 U 和 V 有何不同，經由 TABLE 中抓取出 Bob 相對應資料。

(4) Dispute Resolution Protocol:

經由上一階段所獲得之資料來進行比對，若有比對資料符合，則屬於合法授權，另也比對 *Signc(EKB(W))*的部分，經由 CA 的確認使得 Bob 不得抵賴。

（三） 分析資料之正確性

本研究目前利用小波轉換 (DWT)的數位浮水印方法，設計出一套多重數位浮水印架構，以一視覺上可辨識的影像，作為嵌入圖形之數位浮水印。此外，此多重浮水印架構不僅適用在媒體文件交換系統中多次加入浮水印，且能夠抵抗多種影像處理的攻擊，如 JPEG 失真壓縮、改變圖檔大小(Resizing)；並且，可在一影像資料中，於不同時加入數個數位浮水印，增加辨別的能力。此架構符合不易察覺(Imperceptible)、強韌性(Robust)以及明確性(Unambiguous)等的要求。同時對安全的網路傳輸，作深入分析及研究。

（四） 成果與實用性

I. 多重數位浮水印架構

在前一期的研究中，本研究團隊利用[12][18]所發展的小波轉換(Discrete Wavelet Transform, DWT)的技術之數位浮水印；設計出一多重數位浮水印應用架構（圖 1）（圖 2），以因應媒體文件傳輸之責任區分之需求。

多重數位浮水印應用架構（圖 1）是建構在現行電子出版品遞送的過程上，其中存在這三種關係，如下：

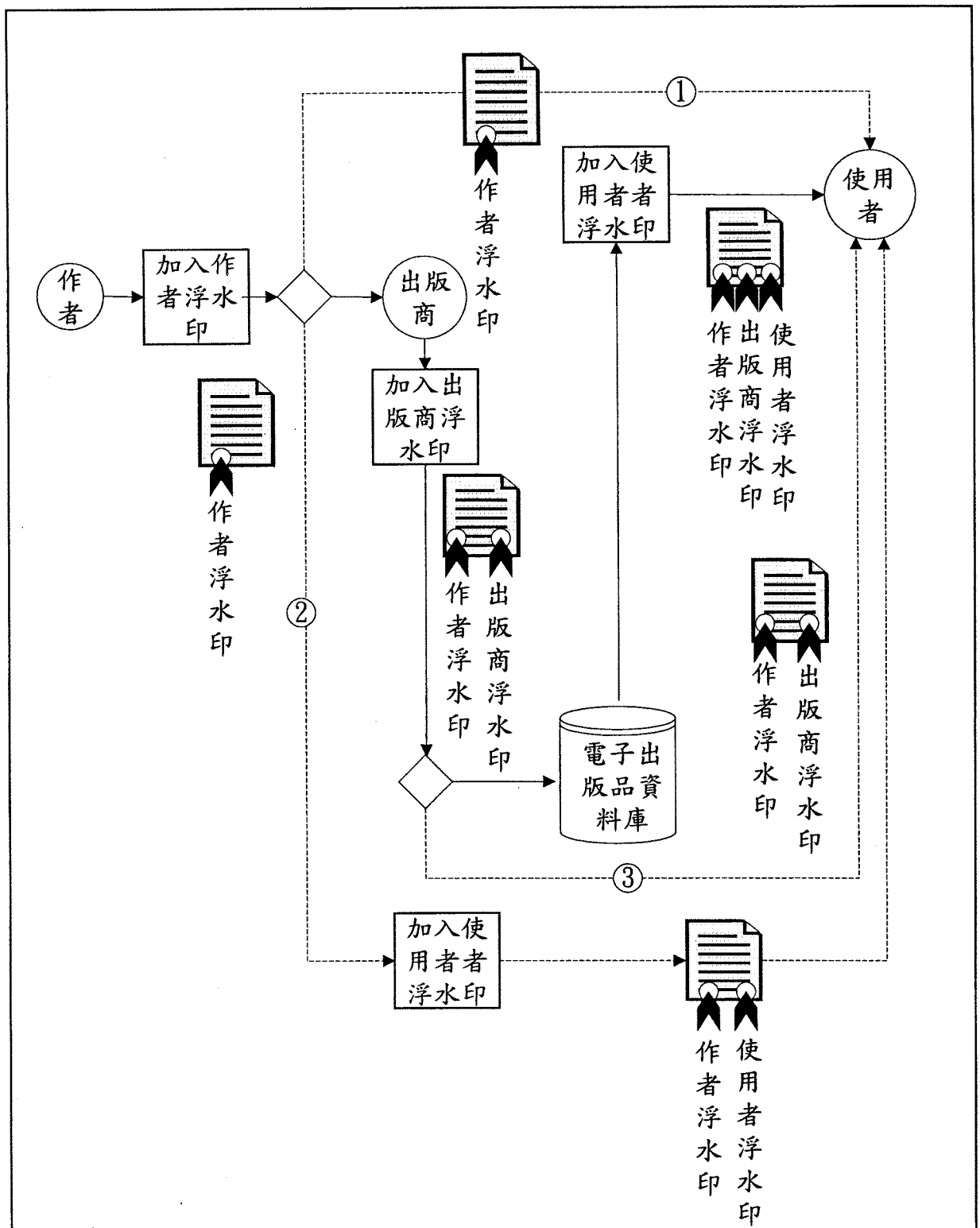
作者完成出版品後，加上自己的浮水印，不僅是對作品負責，也是保障自己的版權。

出版商和作者簽署合作契約後，在該電子出版品上加入出版商的浮水印，以證明是該出版商出品。完成本階段時，在出版商的電子出版品中均可偵測出出版商和作者的浮水印。

使用者經由購買獲得使用權：出版商將其出版之電子出版品中加入該使用者的浮水印，以證明該使用者的使用權。

以上是屬於合法正常的流程，其中作者和出版商扮演相當重要的角色。在虛線代表不合法的程序中表示：一旦作者未經出版商同意而私自將出版品任意翻印於他人時，這時的作品中，應該是不會有出版商的浮水印，而證明出此電子出版品的來源有問題。也就是說，媒體文件經過的單位就必

須加以該單位之浮水印，以對該文件負責。如路徑 2、3，都有相同類似的

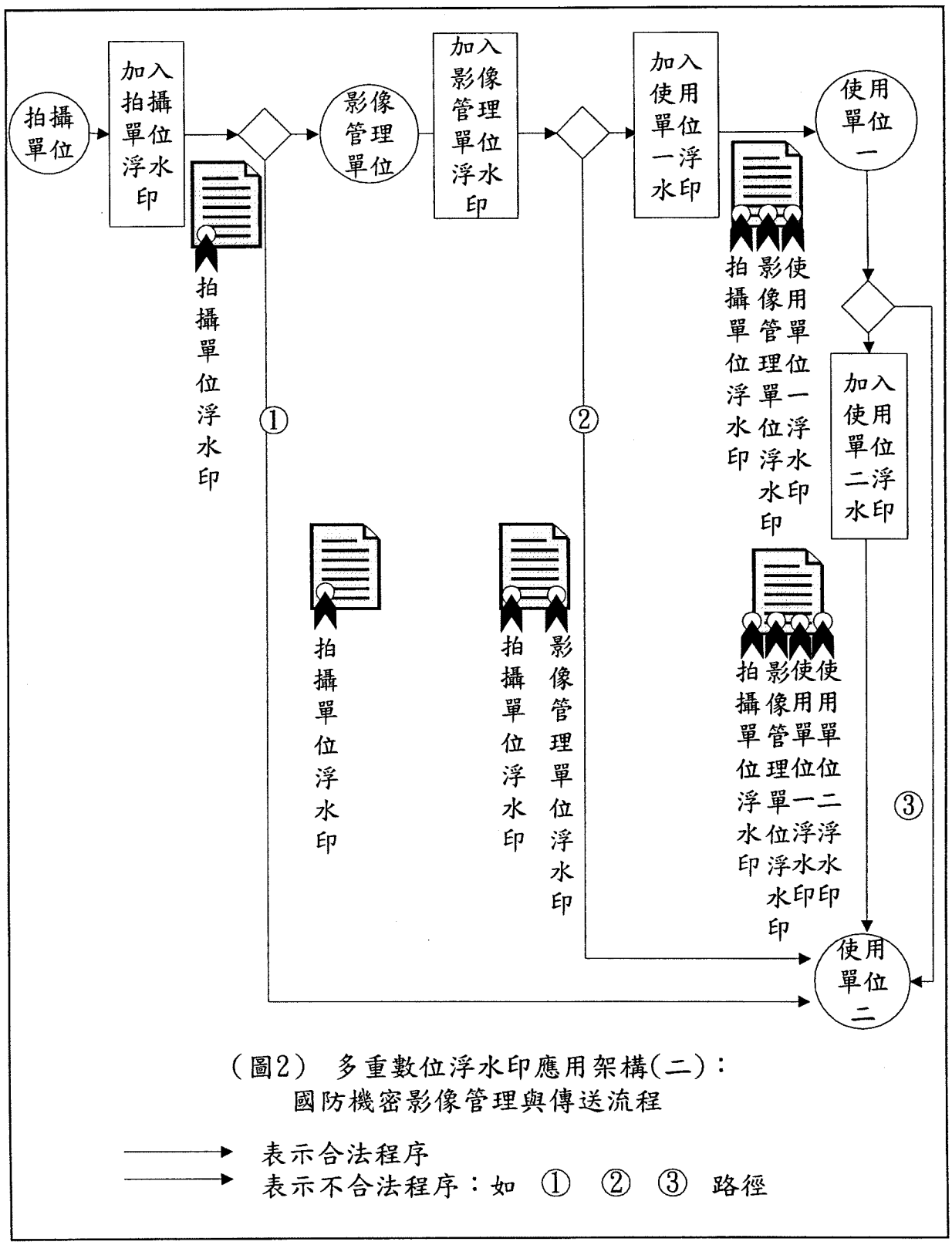


（圖 1） 多重數位浮水印應用架構(一)：
電子出版品之出版與販售流程

→ 表示合法程序
⇢ 表示不合法程序：如 ① ② ③ 路徑

問題，均因浮水印的不正常加入，而可以很容易的驗證和區分責任。

多重數位浮水印應用架構（圖 2）是建構在國防機密影像管理與傳送流



（圖2） 多重數位浮水印應用架構(二)：
國防機密影像管理與傳送流程

程，其中存在如下三種關係：

1. 拍攝單位將所製作之影像檔，加上自己的浮水印以示負責。
2. 影像管理單位在收到確認是某拍攝單位完成的影像文件後，證明該文件為非偽件後，再加上自己單位的浮水印而存入保管。以證明保管單位的責任。
3. 影像管理單位，在得到使用單位一的提出需求後，必須將所要求影像檔案加入單位一的浮水印，然後單位一才可以正式使用此檔案。
4. 當使用單位一將檔案傳送給使用單位二時，單位一也必須加入單位二的浮水印，以釐清檔案已經不再是使用單位一的責任。

在完成以上四個關係後，可以發覺：這機密影像如果從其中的某一個階段洩漏出去（如：路徑 1、2、3），可以追究相關單位的責任歸屬。譬如：在非合法流程中（疑似洩密動作），拿到一影像證物，經過偵測，只有拍攝單位之浮水印，這表示：該檔案文件，是從拍攝單位就洩漏了；若已有管理單位之浮水印，這表示：該檔案文件，是從管理單位洩漏了。經由這架構的推演，可以很有效率的追究相關單位的責任，這是有別於電子簽章又或是其他加解密的安全機制。

由此可知，多重數位浮水印架構能夠加強媒體文件之責任區分的能力，因此本研究是有其可行性及必要性。

II. Open-Close 浮水印架構

仿照 buyer-seller 的架構，本計畫研究小組設計了一個不需 CA 來做嵌入浮水印的架構。其主要的理由是方便性及實用性。

II.1 架構描述如下：

本架構分為四個步驟，步驟 1. 產生 Open Watermark，步驟 2. 嵌入浮水印，步驟 3. 擷取浮水印，步驟 4. 驗證浮水印，其詳細方法如下：

步驟 1. 產生 Open Watermark：如圖 3-(i)。

Function B（Function A（I）+W）➔K'

（I：Image，W：Watermark，K'：Open Watermark）

本階段藉由待嵌入圖（I）和可辨識浮水印（W）的輸入，產生出公開浮水印圖（K'）（Open Watermark）。

步驟 2. 嵌入浮水印：如圖 3-(ii)。

Embedding（I+K'）➔WI ；Attack（WI）=AI

（I：Image，WI：Watermarked Image，AI：Attacked Watermarked Image）

可運用任何浮水印嵌入方法，將公開浮水印圖（K'）嵌入圖形 I 中，而產生含浮水印圖形（WI）。

步驟 3. 擷取浮水印：如圖 3-(iii)。

Extracting（AI）➔K”

（K”：Extracted Open Watermark）

可採用任何浮水印擷取方法（需同嵌入方法），將待測圖（WI 或 AI）經由擷取浮水印的動作，擷取出 K”。

步驟 4. 驗證浮水印：如圖 3-(iv)。

Function B（Function A（I）+K”）➔W’

（K”：Extracted Watermark）

同步驟 1 之方法，產生該圖對應之私密浮水印圖（Close Watermark），再經運算後，計算還原出一驗證後的浮水印圖（W’）。

本架構經由步驟 1 和步驟 2，必須由圖形之所有權人所完成之動作，而步驟 3 可暴露在任何環境下，包括其嵌入之方法及其參數，以供他人擷取出相關浮水印（ Open Watermark），而完成所有權宣告的動作，且不會因為公布其方法或參數，而輕易的由大量模擬出找尋原始浮水印（W）的存在，因為步驟 3 所擷取出之類浮水印資料是公開浮水印圖 K’（ Open Watermark）而並不是原始浮水印（W），縱使駭客收集了大量 K’也無法計算出 W 的存在，因為 K’的產生，也都是由各個被嵌入圖形所計算出，而並不是由同一方法同一參數所產生，是故有其安全性。而且在實驗數據中，本研究採行 chaotic transformation 將可辨識之原始浮水印（W）轉換成無法辨識之公開

浮水印圖 K'（Open Watermark）。

而本研究在產生 Open Watermark 和 Close Watermark 階段採用之方法為以下幾個步驟：

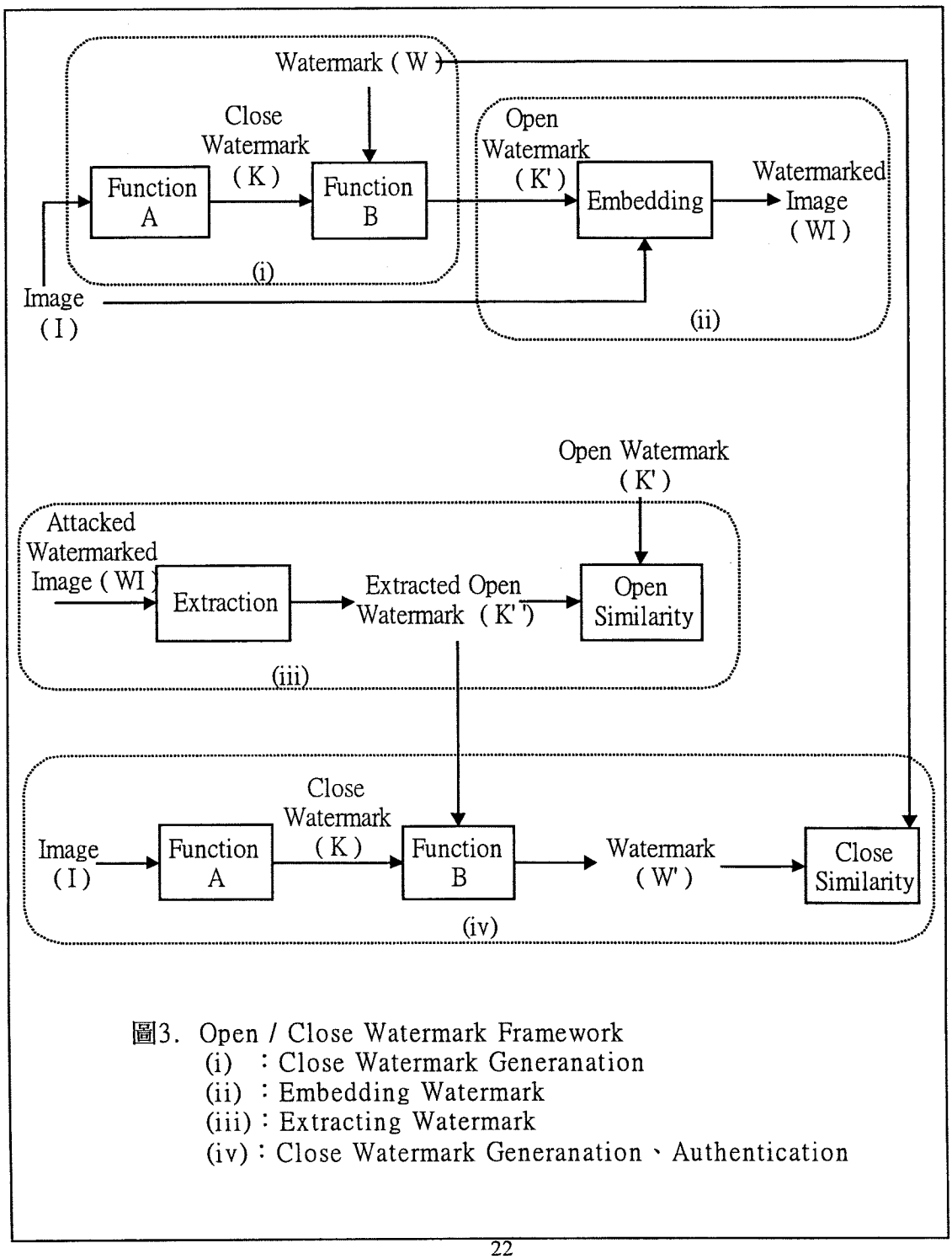


圖3. Open / Close Watermark Framework
(i) ：Close Watermark Generanation
(ii) ：Embedding Watermark
(iii)：Extracting Watermark
(iv)：Close Watermark Generanation、Authentication

1. 經原始圖形經過亂數公式（Function A）轉換。

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod} \quad N)$$

2. 將（1024*768）圖形分成，64*64 之區塊，每一區塊大小為 (1024/64)*(768/64)＝16*12。

3. 計算每一區塊之變異數(Vi)，共 64*64 個區塊。

4. 計算這 64*64 個變異數(Vi)之平均數 T，當成一個特徵值（門檻值，Threshold），（亦可取其他特徵值當門檻值）。

5. 經由下列規則產生出大小為 64*64 之私密浮水印（Close Watermark）。

   私密浮水印（Close Watermark）i= 1 ，if Vi>T

   私密浮水印（Close Watermark）i= 0 ，if Vi<T

6. 經由（Function B）

   （公開浮水印）==（私密浮水印）XOR（原始浮水印（W））

   而驗證浮水印階段之驗證出原始浮水印之 1-5 步驟，與上述相同，除第 6 步驟改為：

6. 經由（Function B）

   （原始浮水印（W'））==（私密浮水印）XOR（公開浮水印）

而嵌入與擷取浮水印階段，本階段研究採用先前發展之浮水印嵌入與擷取方法(請參見附錄一)，此階段亦可採用他種方法取代，根據本架構之模

擬：浮水印嵌入與擷取的效果取決於該階段方法的好壞；而在產生 Open Watermark 和 Close Watermark 和驗證浮水印階段的方法選擇，並不影響浮水印嵌入和擷取的效果，其數據將會在下一段落做討論。

II.2 實驗數據

針對上一階段之描述，本研究做出該雛形系統，並進行系統模擬，產生相對應之公開浮水印（Open Watermark）與私密浮水印（Close Watermark）後，另採用上一階段所開發之浮水印嵌入與擷取方法進行模擬，並以 JPEG，Blur，Adding Noise，Crop 等影像處理方法，作為攻擊的模式，來進行實驗數據，數據請參見附錄三。

其中，JPEG 壓縮至 3.2：1 時仍只有 10%的錯誤率，壓縮至 4：1 時，仍可感覺出擷取出之資訊與原始浮水印有相關之訊息，另外此方法也分別可經的起加入雜訊和剪裁攻擊等等，其中加入雜訊是採用 Paint Shop Pro 公司之功能透過參數的設定，可以依加入雜訊程度不同而做設定；另剪裁攻擊則是透過簡單的去除左上、右上、左下、右下四區塊來實驗，本研究發現，當剪裁範圍的比率大約是擷取後浮水印錯誤的比率，但在實用價值上，圖形一旦經過大幅修改，便已經失去使用價值，因此在此僅供數據上的討論。

本研究發現本研究之架構之浮水印效果，並不會因為增加了產生 Open Watermark 和 Close Watermark 和驗證浮水印階段的驗證工作，而使得嵌入

和擷取浮水印的效果變差（因為 K'.raw Error bits＝Seal.raw Error bits：表示所嵌入的 Close Watermark 的錯誤率，和 Original Watermark 的錯誤率相同；反而值得注意的是：嵌入和擷取浮水印之效果，可經由更換該部分之方法來增強浮水印的效果；而更換驗證浮水印階段的方法，可以適度增加其驗證之安全性。

討論

本研究所提出之驗證浮水印及嵌入浮水印的架構可以藉由一個類似 CA 架構的機制來驗證浮水印的動作，而能解決相同問題。在這部分先回顧本架構方法，再做詳細的分析，最後會有結論歸納與討論。

回顧：

1. 利用對於待嵌入圖以適當之運算（Function A：利用變異數 Var 當作

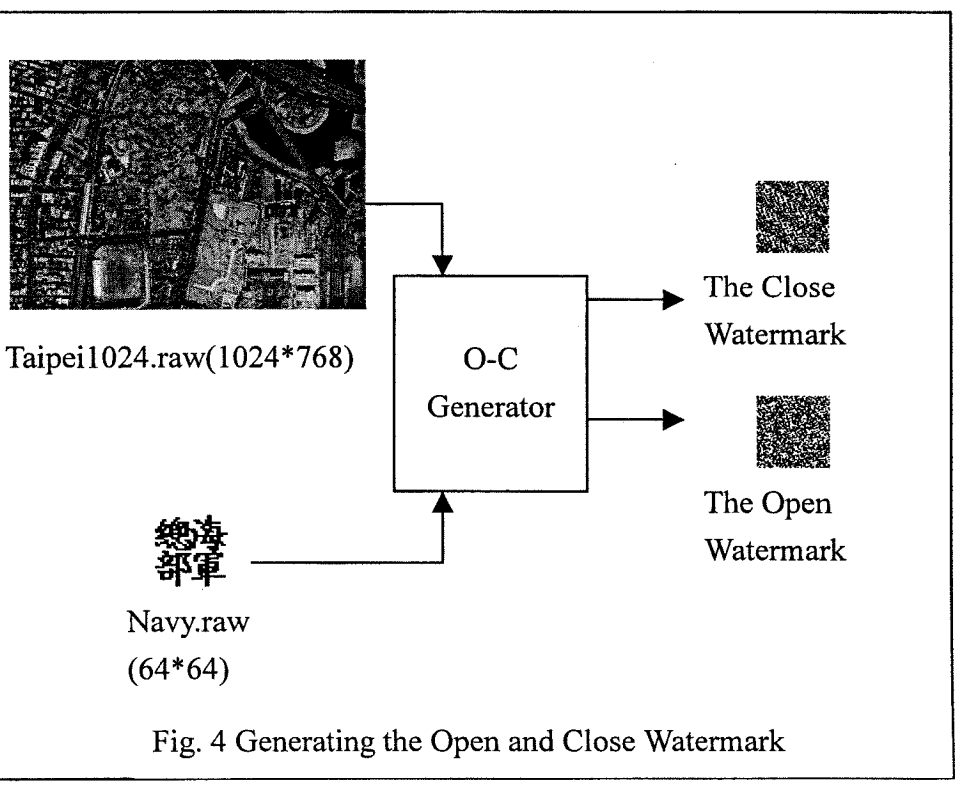


Fig. 4 Generating the Open and Close Watermark

門檻值等等）計算出浮水印之私密浮水印圖（Close Watermark），其中私密浮水印圖（Close Watermark），是一個經過運算而無視覺意義之浮水印，再利用這私密浮水印（Close Watermark）和一視覺上可辨識的影像（原始浮水印 Original Watermark）做運算產生之公開浮水印圖（Open Watermark）；

2. 利用小波轉換（DWT)的數位浮水印方法，以公開浮水印圖（Open Watermark）作為嵌入圖形之數位浮水印。

3. 為擷取出公開浮水印圖（K"）（Open Watermark）4：由這一公開浮水印圖(K")(Open Watermark)和重新運算後之私密浮水印圖(Close Watermark）來驗證出具視覺意義之原始浮水印的（Original Watermark）。

分析：

■ Open & Close Watermark Generator：

1. 由 Original Image、Original Watermark 運算出 Close Watermark 和 Open Watermark。

2. Open Watermark 被嵌入：意味 Open Watermark 是 User 擁有。

3. Close Watermark 可由 Author 持有或驗證時重新產生。

■ Authentication：

1. 經由擷取得到 Open Watermark ：意味 Open Watermark 來自於 User。

2. 由 Close Watermark、Open Watermark 合成出 Original Watermark。

歸納：

- 因為 Close Watermark 屬於 Author 所有。
- 因為 Open Watermark 來自於 User。
- 而且 Close Watermark ，Open Watermark 均是混亂無任何明顯資訊的浮水印：這意味 Close Watermark 、Open Watermark 兩者均不易偽造。
- 所以當 Close Watermark、Open Watermark 合成出 Original Watermark'時，
- Original Watermark' 確有某種意義的影像資訊呈現。
- 假設 Close Watermark 或 Open Watermark 有一造假。則 Original Watermark'便不可能有某種意義的影像資訊呈現。這是可預知的。
- 不可否認的：有某種意義的影像資訊呈現這不是巧合，因此這樣的驗證是有意義的。
- 而且雙方均不可抵賴這結果（巧合）。

經由上述討論可以清楚看出：本研究之方法利用所有權人所擁有的圖形和原始浮水印經由特定演算法產生一對公開浮水印浮水印（Open Watermark）和私密浮水印浮水印（Close Watermark），正如 Fig.4 所示；而所有權人持有的是一私密浮水印浮水印（Close Watermark），當需要驗證浮

水印時，必須和由嵌入圖形中的公開浮水印浮水印（Open Watermark）兩者合而為一，正如 Fig.5 所示，才能驗證出正確的浮水印；換句話說，當爭議產生需要驗證浮水印時，被驗證者與圖形所有權人都需提出該對應之浮水印，才能解出原始浮水印，而這代表的即是資訊來自於雙方缺一不可，所以雙方均不能抵賴驗證的結果，因此若有任一方偽造，在還原驗證原始浮水印時，便不能成功。因此這樣的機制，解決了兩個浮水印棘手的問題：

1. 圖形所有權人不能抵賴該驗證圖形，

2. 被驗證者不能抵賴該圖不是這所有權人的。

此外，此驗證與嵌入浮水印架構不僅適用在媒體文件交換系統中多次加入浮水印，且能夠抵抗多種影像處理的攻擊，如 JPEG 失真壓縮、剪裁（Cropping）、加入雜訊（Adding Noise）...等攻擊；而且更可以公開嵌入與

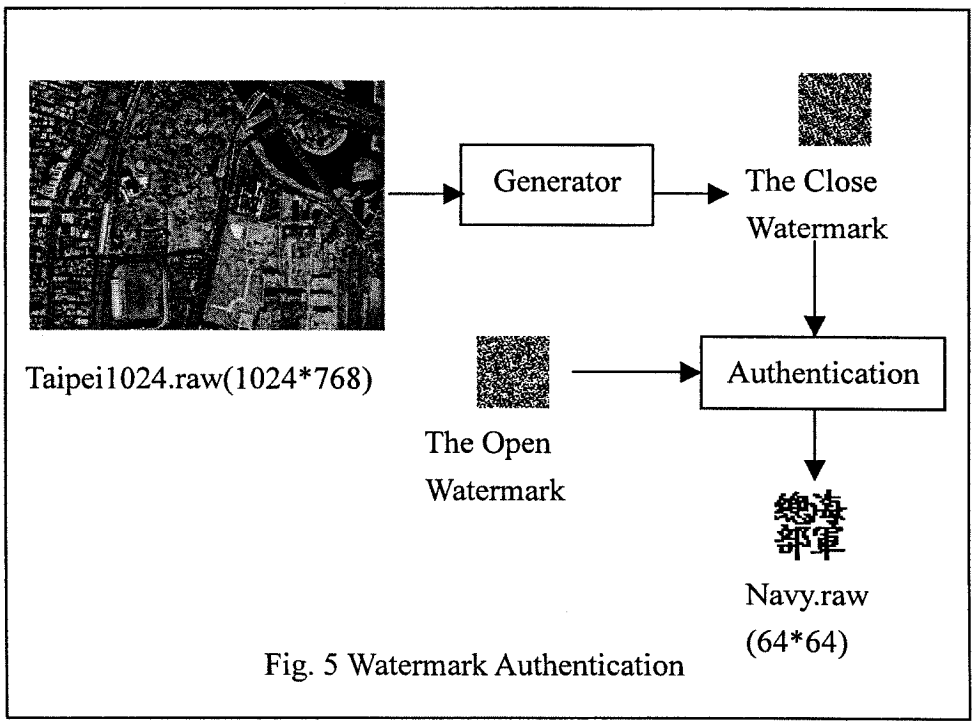


Fig. 5 Watermark Authentication

擷取之浮水印方法與參數，以供他人擷取出浮水印，以達到所有權宣告之效果。因此，本架構不僅符合浮水印之精神不易察覺(Imperceptible)、強韌性(Robust)以及明確性(Unambiguous)等的要求，更可以達成驗證偽造浮水印的嵌入與圖形所有權的確立。

實用性探討

(A)本階段研究乃鑑於浮水印之偽造的關鍵性議題，提出一類 CA 架構之解決方案，其不似 CA 之繁雜，不僅可輔助 CA 來作公正的第三者，又可達成驗證偽造浮水印之目的，而且本架構不影響任一種浮水印之嵌入或擷取方法的效果，經實驗模擬該系統架構確實可行；因此本浮水印架構之推行，不需有繁雜的確認動作，即可順利完成驗證偽造浮水印的動作，而日後之關於浮水印嵌入與擷取之研究，皆可應用至本架構之其中方法，所以本研究所提出之浮水印架構的確是一個可驗證偽造浮水印之方法。

(B)在網路傳輸的流程，將首先考慮以 PKI 金鑰管理的方式來做研究，步驟如下：

1. 先將影像及檔案資訊作加入數位浮水印的動作，如上頁所述。
2. 亂數產生一支 DES_KEY 做為網路傳輸加密用。
3. 將經過數位浮水印處理的影像資料及檔案，以 DES_KEY 作加密的動作。

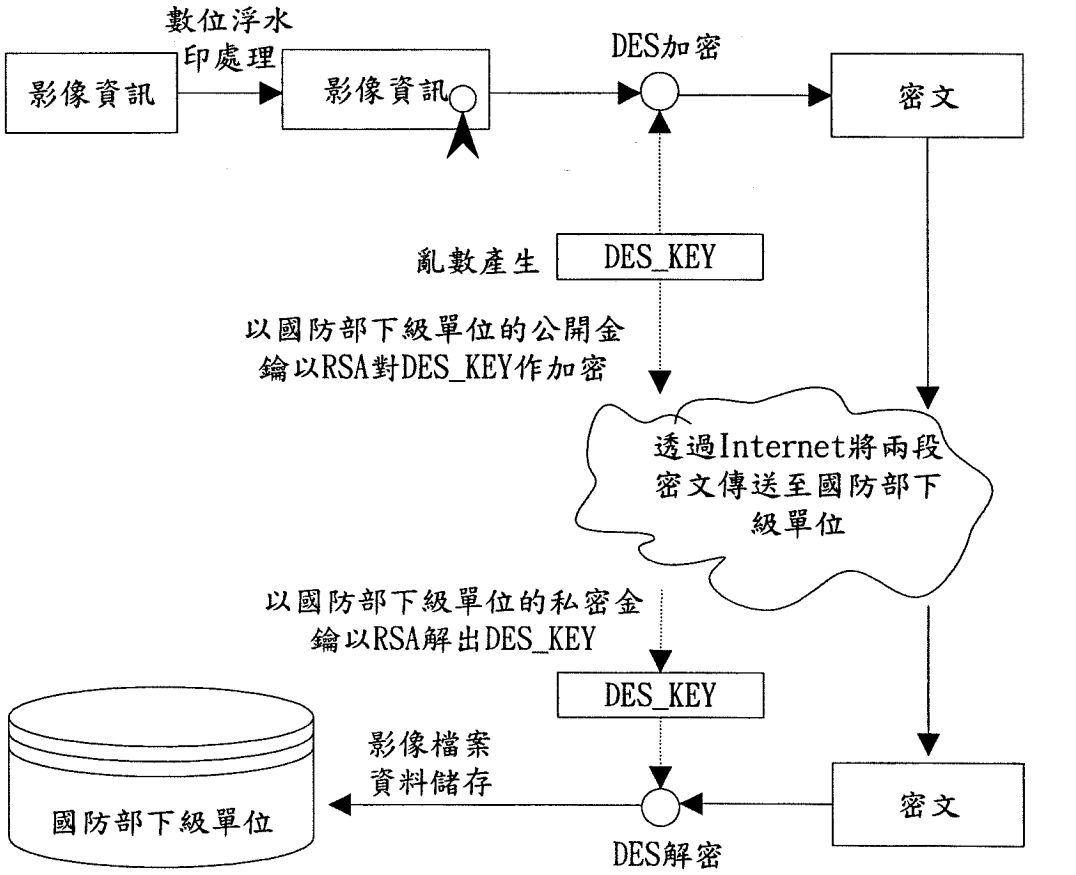
4. 在經過網路傳輸前，將此把 DES_KEY 以國防部的下級單位的公開金鑰（Open Key）作加密的動作。

5. 將兩筆密文經過網路傳輸至國防部的下級單位。

6. 國防部的下級單位接收到此兩筆密文，先以下級單位本身的私密金鑰（Close Key）作解密的動作，解出一支 DES_KEY。

7. 以這把 DES_KEY 對另一密文作解密的動作，解出所傳送的資料。

流程圖如下所示：



（圖6）網路傳輸流程

5. 完成項目

本研究完成進度及相關研究項目如下：

1. 對國防影像浮水印技術處理的各步驟，作詳細的系統分析與電腦模擬，設計出具體處理的技術。
2. 針對 attacker 的可能採取的偽造修改方式，做系統的模擬。
3. 對安全的網路傳輸，作深入分析及研究。
4. 承蒙合作單位之協調與安排，於１１月２３日，由計畫主持人率研究團隊赴基隆實地瞭解海軍數位影像的應用。對海事衛星有深刻之瞭解（請參見附錄四），實際參訪記錄及建議，請參見附錄五。
5. 承蒙合作單位及本計畫團隊之合作，上述相關進度與研究項目，均已如期完成。

6. 檢討與建議

在第一期的計畫中，可以得知多重數位浮水印架構在 JPEG 攻擊大約 8.3:1 下依然可以維持在浮水印低於 5%的錯誤率，此時浮水印亦保持足夠的辨識程度可供主觀的參考。

而在本期的研究中，綜合結論是具可辨識能力的數位浮水印，對媒體文件責任區分的鑑定，不只提供數值上的相似性參考，在視覺主觀的認定上，更可以作為直接判斷的基礎；其效用比以亂數產生的浮水印更有實際應用的參考性，可提供進一步的證據。而媒體文件責任區分的能力，可藉由在多重數位浮水印架構，於不同時加入多個數位浮水印來達成，這是有別於密碼學的加解密的機制。本研究的實驗，證明在有限度的破壞攻擊（被攻擊後的圖形仍具有使用價值）下，擷取多重具可辨識能力的數位影像浮水印，對資訊安全及隱私，提供媒體文件責任區分的鑑定及其不可否認性，及更強的驗證能力。

另外，在網路傳輸流程方面，透過 DES 和 RSA 的加解密機制，雙重加解密，可以保護密文及其加解密之金鑰，如此也可達成傳輸流程的安全性。

在實際應用探討中，相關建議請見附錄五。

參考文獻

[1]R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark", IEEE ICIP94, vol. 2, 1994.

[2]N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital images", IEEE Int. Conf. on Acoustics, Speech and Signal Processing, vol. 4, May 1996.

[3]R. Wolfgang and E. Delp, "A watermark for digital images", IEEE ICIP96, vol.3, September 1996.

[4]I. Pitas, "A method for signature casting on digital images", IEEE ICIP96, vol. 3, September 1996.

[5]G. Voyatzis and I. Pitas, "Applications of Toral Automorphisms in Image Watermarking", IEEE Int. Conf. on Image Processing, Vol. 2, pp. 237-240, September 1996.

[6]I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia" IEEE Transaction on Image Processing, Vol. 6, No. 12, Dec. 1997.

[7]X. -G. Xia, C.G. Boncelet and G. R. Arce, "A Multiresolution Watermark for Digital Images", IEEE ICIP97, vol.1, June 1997

[8]W. Zhu, Z. Xiong, and Y. -Q. Zhang, "Multiresolution watermarking for images and video: A unified approach", IEEE ICIP98, vol. 1, October 1998.

[9]R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-Based Scheme for

Watermarking Images", IEEE ICIP98, vol. 2, October 1998.

[10]Chiou-Ting Hsu, and Ja-Ling Wu, "Hidden Digital Watermarks in Images", IEEE Transactions on Image Processing, vol. 8, January 1999.

[11]W. Zeng and B. Liu, "A Stastical Watermark Detection Technique Without Using Original Images for Resolving Rightful Ownerships of Digital Images", IEEE Trans. On Image Processing, vol. 8, no.11, pp.1534-1548, Nov. 1999.

[12]M. Tsai, K. Yu and Y. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking" IEEE. Trans. On Consumer Electronics, vol. 46, No. 1, pp. 241-245, Feb, 2000.

[13]M. D. Swanson, M. Kobayashi and A.H. Tewfik, "multimedia Data-Embedding and Watermarking Technologies", Proceeding of the IEEE, Vol. 86, No. 6, June 1998.

[14]Daubechies, "Orthonormail bases compactly supported wavelets," Comm. Pure Appl. Math., Vol. XLI, pp. 909-996,1988.

[15]M.J. Tsai, J.D. Villasenor and F. Chen, "Stack-Run Image Coding", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 6, pp. 519-521, Oct. 1996

[16]M, Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet coefficients," IEEE Transactions on image Processing, Vol. 1, No. 2, pp. 205-220,Apr. 1992.

[17]M. Shapiro, "Embedded image coding using zerotrees of waveletecoefficients," IEEE Trans. On Signal Processing, Vol. 41, no. 12, pp.

3445-3462, Dec. 1993

[18]Min-Jen Tsai, Kuang-Yao Yu , and Yi-Zhang Chen, "Wavelet Packet and Adaptive Spatial Transformation of Watermark for Digital Image Authentication ",ICIP2000, vol. 1, Sep. 2000

[19]Ramarathnam Venkatesan, and Mariusz H. Jakubowski "Image Watermarking with Better Resilience",ICIP2000, vol. 1, Sep. 2000

[20]Charlie Kaufman, Radia Perlman, Mike Speciner "NETWORK SECURITY CLOSE Communication in a OPEN World" Prentice-Hall, Inc. 1995.

[21]Morrie Gasser, "Building A Secure Computer System", Van Nostrand Reinhold, 1988.

[22]Philip E. Fites, MBA, CDP and Martin P. J. Kratz, B. Sc., LLB, "Information Systems Security - A Practitioner's Reference", Van Nostrand Reinhold, 1993.

[23]Michel E. Kabay, Ph.D., "The NCSA Guide to Enterprise Security - Protecting Information Assets", McGraw-Hill, Inc., 1996.

[24]賴溪松，韓亮，張真誠,"近代密碼學及其應用", 松崗電腦圖書資料股份有限公司, 1996.

[25]B. Schneier, *Applied Cryptography*, 2nd Edition, John Wiley & Sons, Inc. 1996.

[26]D. Stinson, "Visual cryptography and threshold schemes", *IEEE Potentials*, vol. 18, No. 1, pp. 13-16, Feb.-March 1999.

[27]Nasir Memon, Ping Wah Wong, "A Buyer-Seller Watermarking Protocol" IEEE Transactions on Image Processing, Vol. 10, No. 4, pp. 643-649, Apr. 2001.

附錄一

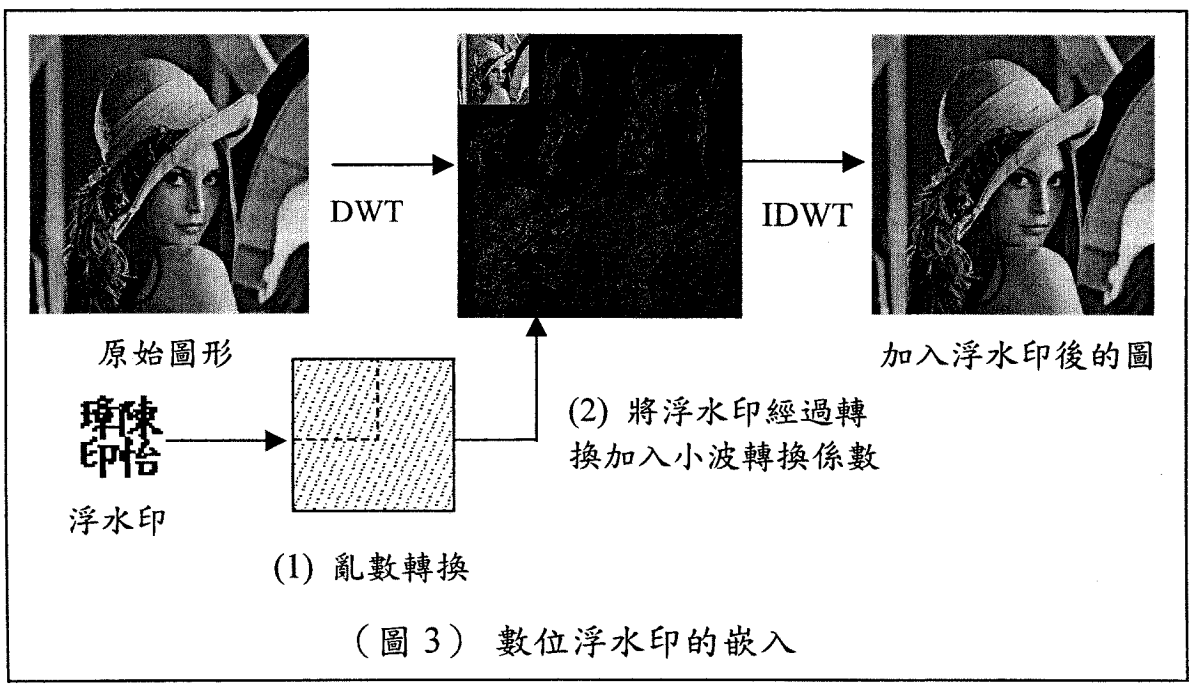
數位影像資訊利用小波轉換(DWT)的技術，運用在嵌入與擷取數位浮水印之程序。其中在擷取浮水印的過程中，必須使用與嵌入程序相同的 key，才能解出正確的資料。以下則介紹嵌入與擷取數位浮水印的做法。

- 數位浮水印嵌入程序

數位浮水印的嵌入程序(圖 3)可分成兩個步驟：(1)利用亂數轉換打散浮水印的地理相對位置。(2)將打散後的資料嵌入於原始圖檔的小波轉換係數中。其分項步驟說明如下：

(1) 亂數轉換(chaotic transformation)

我們參考[4]使用的亂數轉換系統，將大小為 m × m 的數位浮水印打散至 N × N 的矩陣中，配合以下的公式:



（圖 3） 數位浮水印的嵌入

$A_N(k)$： $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N}$

其中 k 代表控制參數、N 代表打散後的矩陣大小、(x , y)與(x' , y')分別代表 pixel 轉換前後的位置。假設公式 AN(k)的週期為 p，則(x , y)在經過 p 次的 AN(k)運算後，能返回原來的位置。

若某一點(i,j)經以 n 次的 AN(k)運算後(n < p)，需再經過 p－n 次的 AN(k)運算才能返回原點(i,j)。因此，若原作者將數位浮水印經過 n 次的 AN(k)運算，以打散數位浮水印，擷取時若使用不正確的參數 n 與 k，則無法還原出原始的數位浮水印。

(2) 將浮水印經過轉換加入特定區塊

在此步驟中，我們將原始圖檔經以小波轉換，產生如金字塔狀的分解圖形，於分解圖形中選出以(p1 , p2)為嵌入起始點、大小 N xN 的區域 B；其次，根據打散後數位浮水印的數值，嵌入此區域中相對應點的值(δ(i,j)－(T1，T2))；最後再執行 inverse DWT，數位浮水印的嵌入程序即告完成。

令數位浮水印打散的 N x N 矩陣為 A，矩陣 A 中浮水印形成的集合為 U；自分解圖形中選出的矩陣 B，而矩陣 C 之元素是來自於矩陣 B 和 U 運算的結果，即利用以集合 U 中元素的值為 B 的位址取出 B 值，放入矩陣 C 的相對應位置，其規則如下所述：

對矩陣 **A** 的集合 **U** 中所有點（**i**，**j**）：

1. 當 $A(i,j)=1$ 且 $B(i,j)\geqq 0$，

   則 $C(i,j)=C(i,j)-\delta(i,j)+T1$；

2. 當 $A(i,j)=0$ 且 $B(i,j)\geqq 0$，

   則 $C(i,j)=C(i,j)-\delta(i,j)+T2$；

3. 當 $A(i,j)=1$ 且 $B(i,j)<0$，

   則 $C(i,j)=C(i,j)+\delta(i,j)-T1$；

4. 當 $A(i,j)=0$ 且 $B(i,j)<0$，

   則 $C(i.j)=C(i,j)+\delta(i,j)-T2$；

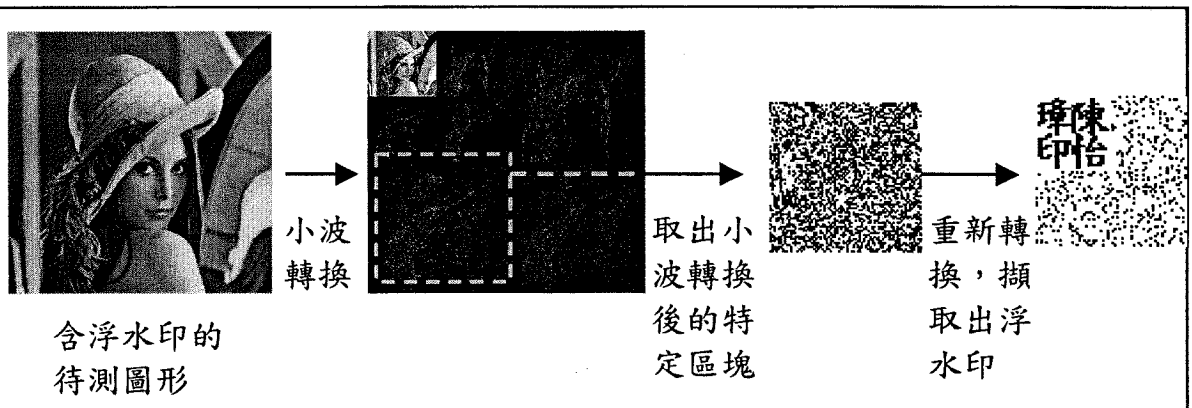
其中 $\delta(i,j)=C(i,j) \bmod s$

而 T1 與 T2 的值取決於 s 的大小，$T1=s/4$ ，$T2=3*s/4$。

因此，在嵌入程序中使用到的參數：n、 k、 p1、p2、N、s 構成 key。

- 數位浮水印擷取程序

數位浮水印的擷取程序如（圖 4），對待測圖形來說，擷取程序必須使用



（圖 4） 數位浮水印的擷取

以下的參數：n、 k、p1、p2、N、s (可以把以上參數視為一把鑰匙)。首先將待測圖形經以小波轉換後，根據 key 中的參數選取由起始點(p1 , p2)、大小為 N × N 的區塊所形成之矩陣 Y；其次，利用參數 s，另矩陣 θ 等於 Y 矩陣內元素除以 s 之餘數所成集合；再根據以下的規則決定嵌入的數值，組成矩陣 D：

對矩陣 **Y** 中所有點（**i**，**j**）

1. 當 **|θ(i,j)| ≧ s/2,** 則 **D(i,j) = '1';**
2. 當 **|θ(i,j)| < s/2,** 則 **D(i,j) = '0';**

最後根據 k 與 n，將矩陣 D 重新建構藉由 AN(k)做 p－n 次的轉換，即可得到嵌入的浮水印。

- 數位浮水印擷取程序

實驗數據探討，請見附錄二。

附錄二

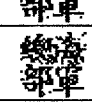
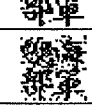
表 (1) 使用不同程度攻擊待測圖形，瞭解其對擷取單一浮水印的影響。

JPEG Image Quality	Compression Ratio	Error Points	Extracted Watermark
100%	1.41937	0	
90%	3.49181	0	
80%	5.07608	0	
70%	6.26225	0	
60%	7.34853	10	
50%	8.33394	32	
40%	9.52974	72	
30%	11.21088	166	
20%	14.55466	313	
10%	23.89209	446	
0%	70.37423	446	

表(2)使用不同程度攻擊待測圖形，瞭解其對擷取每一階段浮水印的影響。

JPEG Image Quality	Compression Ratio	擷取出第一個浮水印		擷取出第二個浮水印	
		Error Points	Extracted Watermark	Error Points	Extracted Watermark
100%	1.41746	0		0	
90%	3.48809	0		0	
80%	5.05552	0		0	
70%	6.23826	3		1	
60%	7.32880	11		21	
50%	8.29885	28		56	
40%	9.49109	85		115	
30%	11.20321	139		217	
20%	14.55385	286		362	
10%	23.85513	401		426	
0%	70.35534	420		451	

表 (4) 使用不同程度攻擊待測圖形，瞭解其對擷取單一浮水印的影響。本實驗使用「海軍總部」印作為嵌入之浮水印。

JPEG Image Quality	Compression Ratio	Error Points	Extracted Watermark
100%	1.60660	0	
90%	4.38588	0	
80%	6.83646	0	
70%	8.81216	1	
60%	10.67709	4	
50%	12.27496	26	
40%	14.24463	71	
30%	17.01019	150	
20%	21.65763	330	
10%	32.40346	479	
0%	70.77322	481	

表(5)使用不同程度攻擊待測圖形，瞭解其對擷取每一階段浮水印的影響。本實驗使用「海軍總部」及「資訊處印」作為第一階段及第二階段嵌入之浮水印。

JPEG Image Quality	Compression Ratio	擷取出第一個浮水印		擷取出第二個浮水印	
		Error Points	Extracted Watermark	Error Points	Extracted Watermark
100%	1.41667	0		0	
90%	3.48364	0		0	
80%	5.04366	0		0	
70%	6.22138	0		5	
60%	7.30165	12		19	
50%	8.27292	24		53	
40%	9.46949	72		115	
30%	11.17313	165		244	
20%	14.52401	314		375	
10%	23.85513	468		436	
0%	70.35534	482		477	

附錄三

Table 3 (JPEG 攻擊實驗)

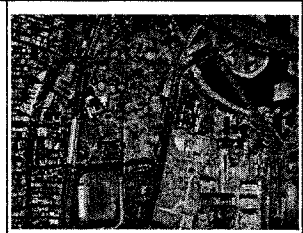
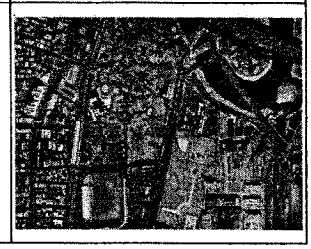
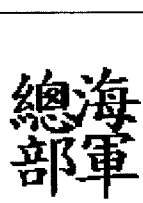
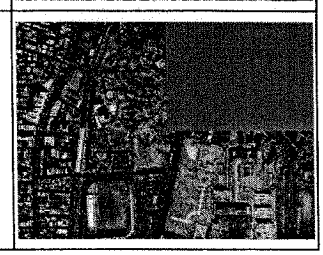
JPEG	K'.raw Error bits	Error ratio	Seal.raw Error bits	Com-pression ratio	Watermark	Attacked Image
100	0	0.00%	0	1.04		
90	11	0.27%	11	2.22		
80	418	10.21%	418	3.19		
70	951	23.22%	951	4.00		
60	1257	30.69%	1257	4.76		

Table 4 (模擬加入雜訊,剪裁攻擊)

Other attack	K'.raw Error bits	Error ratio	Seal.raw Error bits	Watermark	Attacked Image
Noise 1%	0	0.00%	0		
Noise 2%	0	0.00%	0		
Noise 3%	0	0.00%	0		
Noise 4%	6	0.15%	6		
Noise 5%	92	2.25%	92		
Crop 左上	1049	25.61%	1049		
Crop 右上	1013	24.73%	1013		

Crop 左下	876	21.39%	876		
Crop 右下	799	19.51%	799		

附錄四

INMARSAT 國際海事衛星

國際海事衛星(International Maritime Satellite，簡寫為 INMARSAT) 是全世界最早使用的全球衛星行動通信，截至目前為止仍舊是全世界僅有的一種商業化成熟的現代通信，能同時服務海上、陸上的機動用戶，以及飛行器與其他類型用戶。原先是由跨政府組織所組成以服務海上為主，運作約有 20 年光景，直到從 1999 年起 INMARSAT 成立股份有限公司，在更廣泛的市場範疇服務世人。在 1980 年代初期，用戶僅有 900 艘船，現在則已經擴大服務至船隻、車輛、飛機和手提終端機，數目超過 210,000 個用戶，不僅能傳達語音通話，也能傳真和數據通信，傳輸量高達 64Kbit/s。

INMARSAT 使用 C 和 L 頻段(其中船隻至衛星的上連為 1.6365-1.644GHz 右手圓形極化，陸岸至衛星的上連為 6.420-6.424GHz 右手圓形極化，衛星至船隻的下連為 1.535-1.5425GHz 右手圓形極化，衛星至陸岸的下連為 4.195-4.199GHz 左手圓形極化。指揮與測距使用 6.175GHz 水平極化，遙測信標有二分別為 3.945 和 3.9545GHz 左手圓形極化。) 。INMARSAT 系統包括三個次系統，分別是太空裝置、陸岸地球局(Coast Earth Stations，CES) 和船用地球局(Ship Earth Stations，SES)。所有岸至艦以及艦至岸通信必須經由一個陸岸地球局 CES 來路由，就好像一個集線器的節點。不經過一個 CES 的路由，一個船用地球局 SES 是無法與另一個 SES 建立直接的通信。

至於岸對艦通信方面，當一個 INMARSAT 陸岸用戶提出要求 CES 就呼叫這艘在海上的船隻。而每一個 INMARSAT 的 SES 都被分派一個識別碼，並且每一個海上分區也被分派一個區域碼。如此，CES 就能自動指派一個頻道給被呼叫的船隻，而建立一個通信電路。在艦對岸通信方面，當一個 INMARSAT SES 用戶要呼叫一個 INMARSAT 陸岸用戶時，SES 向 CES 提出建立連結的要求，CES 自動指派一個頻道並且回覆包含頻率選擇資訊給 SES。無論 SES 或 CES 都不需要任何人力來操作這些過程。

CES 是一個 C 波段的地球局，有一個 27 公尺碟形反射天線。陸岸至衛星的上連使用 6.4GHz，衛星至船隻的下連使用 1.5GHz。SES 是一個 L 波段的終端機，有一個 0.85 至 1.2 公尺的反射天線。現今總共有五種 INMARSAT SES 的標準機型，他們是 INMARSAT-A、INMARSAT-A64/A56、INMARSAT-C 、 INMARSAT-M 、和 INMARSAT-B 。INMARSAT-B 是 INMARSAT-A 的改良型，其服務運作是全雙工或半全雙工。最大傳輸頻寬

或速率為 64Kbit/s。

現今 INMARSAT 主要是由四個在地理同步軌道上運行的 INMARSAT-3(第三代)衛星所組成(另有在地理同步軌道上運行的一個第三代衛星和四個第二代衛星備援)，這些地理同步衛星在 35,600 公里的赤道上空，按照一個圓形軌道運行，就好像是在地表上選擇了一個點在那兒盤旋。這些衛星的主(全球) 波套能對除了極區以外的全部地球表面重疊涵蓋，其中 F1 涵蓋印度洋地區，F2 涵蓋大西洋東區，F3 涵蓋太平洋地區，F4 涵蓋大西洋西區。實際上祇需三個衛星就足以全球涵蓋，因此機動的用戶幾乎不需要從一個衛星轉換到另一個衛星。這些 INMARSAT-3 衛星能產生許多點波套或單一全球波套，點波套不僅能集中超功率在高需求區域，也使得一些較小、簡易型終端能獲標準化服務。此外，經由地面線路和蜂巢網路的延伸，INMARSAT 幾乎可通達地球上任何角落。

INMARSAT 的全球區域網(GAN) 是世界上首次將資訊技術網路與一個全球性行動通信網路統合，號稱在頻寬與速率上均能符合企業界嚴格的資訊需求。像是祇要需要就能從事遠端 LAN 的存取、e-mail、電子商務、企業網路存取、影像傳輸、以儲存並前送視訊，當然還有高品質的語言及傳真服務。INMARSAT 的全球區域網(GAN) 提供兩項功能強大和具彈性的服務，就是行動 ISDN 和行動封包資料(Mobile Packet Data)，以 64Kbit/s 高速服務延伸到區域和廣域網路達到客戶資訊傳輸需求。INMARSAT 的 GAN 是以其衛星網路提供虛擬的全球涵蓋，以陸岸地球局 CES 作為全球資訊網路的介面。未來，在行動衛星用戶的高速網際網路存取和多媒體通運需求持續成長下，將推出第四代衛星寬頻全球區域網(B-GAN)服務，預估 2004 年速率可達 432 Kbit/s，並能再加強隨選視訊(Video on Demand) 和視訊會議等服務。

參考資料：

1. John C. Kim & Eugen I. Muehldorf, "Naval Shipboard Communications Systems," Prentice Hall, 1995,Chap.13 pp288-293
2. http://www.inmarsat.com/about_inm.cfm
3. http://www.inmarsat.com/GAN/gan_index.htm
4. http://www.inmarsat.com/about_inm_satellite.cfm

附錄五

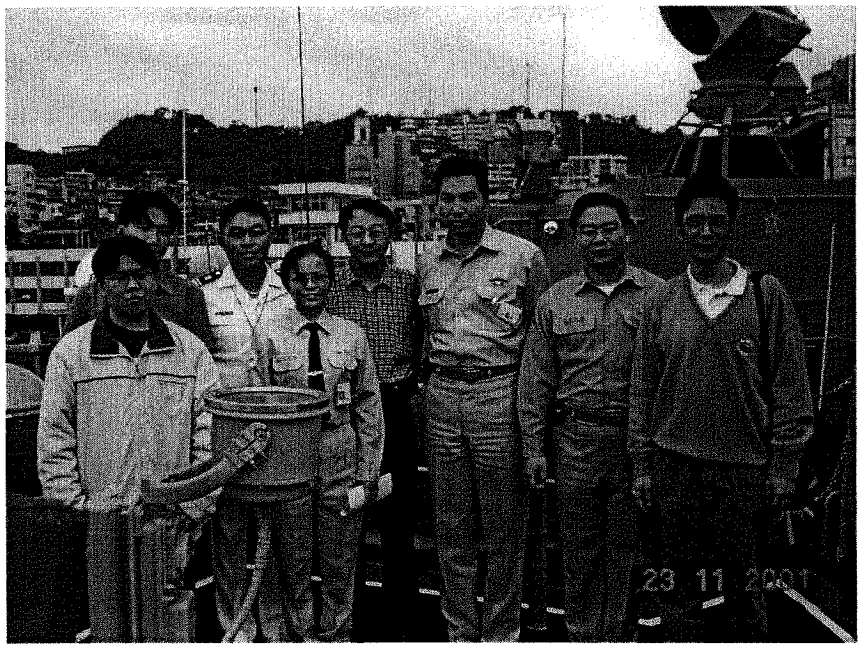
海軍衛星傳真設備參觀紀錄

時間：2001 年 11 月 23 日 13:30~15:30PM

地點：基隆海軍基地

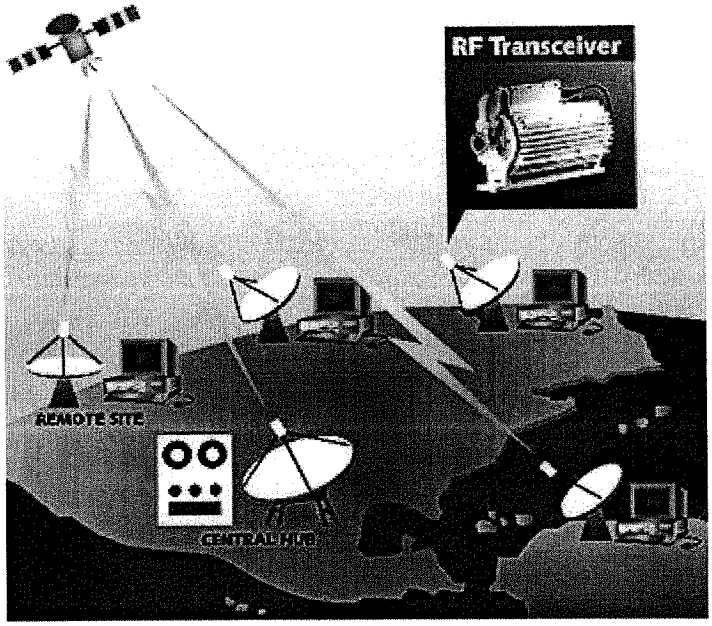
參加人員：蔡銘箴教授率計畫參與同學

當天中午 12 點從新竹交大出發，下午 1 點 25 分至基隆文化中心，與海軍總部承辦人員會合，於 1 點 30 分抵達海軍基隆軍港，隨後即登艦進行此次參觀活動。(附圖一)



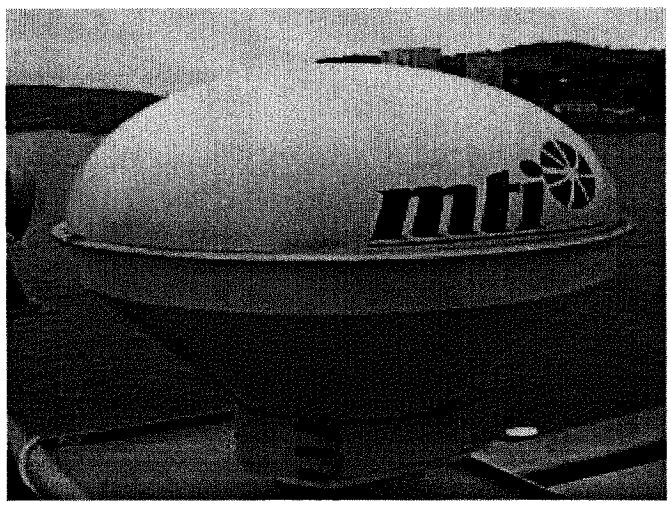
附圖一、參觀及接待人員

本次活動主要為瞭解海軍如何利用海事衛星通信機，做為視迅傳輸之運作過程。由於我國海軍並無直接可專用之通訊衛星，來做為海上偵搜戰情，或一般行政用途之視訊圖資傳輸之用，因此目前海軍乃藉助民間台揚公司所發展之衛星通信設備，透過國際海事衛星電話，來做為海上圖片資料之傳送，以達到在第一時間內，將有用之圖形資料，以傳真方式送回基地查閱參考。(附圖二)

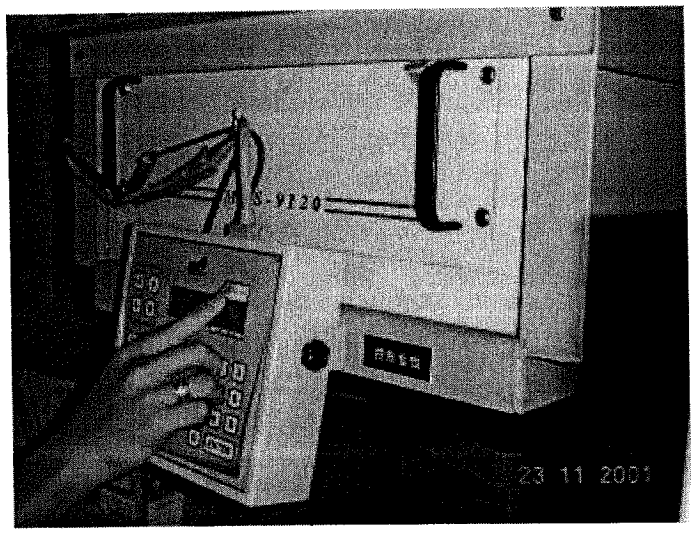


附圖二、台揚公司衛星傳送器

整套衛星相片傳真設備，包含一衛星收發天線（附圖三），控制面版（附圖四），電視螢幕、相片傳真數據機、電話、數位相機（附圖五），其系統運作流程如下：



附圖三、衛星收發天線



附圖四、控制面版

一、利用數位相機將圖形資料數位化後，儲存於相機記憶體之內。

二、將相機之 Video Out 端子，連線至影像傳真機之 Video In 接頭。

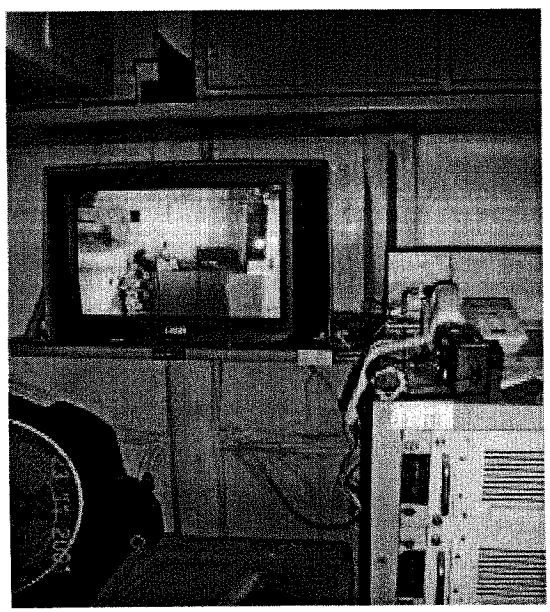
三、選擇欲傳送之相片於數位相機之 Review 位置。

四、打開衛星傳真機及系統之監視螢幕，並選擇遙控器上之 ACQ 按鈕，此時可檢視電視螢幕上之圖片，即為欲傳送之相片。

五、選定相片後，按下 ACQ 按鈕，將相片鎖定。

六、撥接電話至欲傳真之對方號碼，在電話不掛斷且對方電視螢幕未開機之情況下，按下遙控器上的 TX 鈕後，即完成影像傳輸之動作。

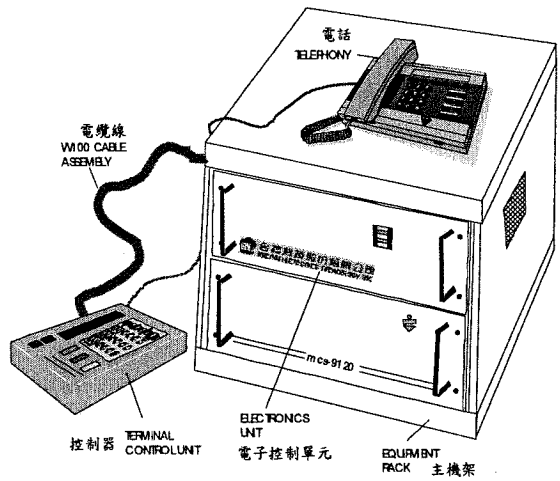
七、完成傳送後，對方打開電視螢幕，即可觀看該影像內容。



附圖五、電視螢幕、相片傳真數據機、電話、及數位相機

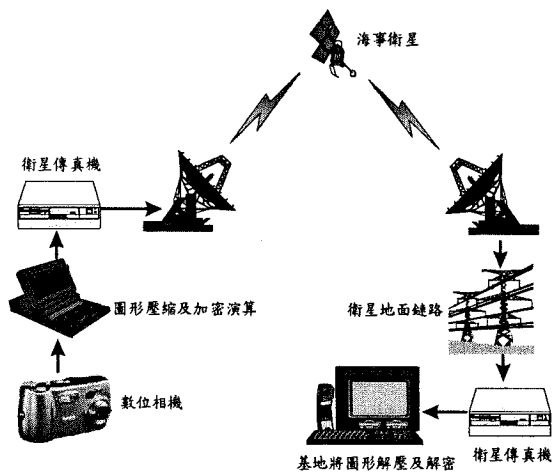
目前海軍使用之主機設備為台揚 MCS-9120 海事衛星通信機，如附圖五，由於海事

衛星使用民間頻道通訊，並透過國際海事衛星通信各鏈路，來傳送資料，因此幾乎沒有任何保密性，若使用此設備來傳送機密之數位圖形資料，非常容易遭到截收，因此基於保密問題，目前海軍很少使用此套設備來傳送圖資。另外，使用此設備需要撥打國際衛星傳真電話，來傳送圖形，而一般數位相機上之圖形，雖然已有壓縮，但效率仍嫌不足，因此需要多花費額外的電話費用來達成圖片傳真之目的。在操作上，也需要一張一張的圖形分別傳送，對於急速且多樣之戰情偵搜情況而言，可謂緩不濟急。



附圖六、**MCS-9120** 海事衛星通信機

本次參觀後的心得感想發現，若能透過一筆記型電腦設備，將數位相機上的照片一次下載至電腦硬碟中，然後利用加密壓縮的演算法，將所有的相片圖資都經過加密處理，並大大壓縮其容量，然後透過電腦內建的數據機，即可將所有相片直接連續的傳送至陸岸基地之相同環境設備上面（如附圖六）。另外配上一個簡單方便的照片圖資管理程式，可以很方便的翻頁、儲存、列印等，達到保密且快速的要求。如此一來，海軍各艦艇單位，即可方便地傳送各種相片，而不怕因為透過海事衛星，而有機密外洩之慮，且可因壓縮之後，更節省海事衛星通信費用。



附圖七、圖形壓縮及加密傳送