資訊隱藏技術之研究

陳文淵 卓江南

國立勤益技術學院電子工程系

e-mail : cwy@chinyi.ncit.edu.tw jnj@chinyi.ncit.edu.tw

摘要

古往今來國家安全與軍事機密，都有賴於秘密通信機制而得到保障。工業上機器的結構與製造技術或處理流程，商業上的交易價格，售與對向與個人創作的智慧財產等都需要有安全，秘密的通信技術來保護。由於有急迫的需要性，因此各種秘密通信技術接連的被開發出來。近代密碼學技術有了重大的突破，使得在文字上的秘密通信得到保障，因此網路交易成為可行。但另一方面，e 世代的影音多媒體取代了傳統的文字，圖形界面(graphics user interface, GUI)更增進了人與機器的距離，使得電腦與網路更普遍，成為生活上的必需品。因多媒體商機升起，也形成駭客竊取與破壞的目標。如何保護多媒體產品，成為當務之急，而密碼技術又無法達成保障多媒體產品的功能，因此資訊隱藏技術也就運應而生了。資訊藏密系統 (steganography)，提供秘密資訊的隱藏，且秘密的不對外公開。這類型式的架構分為 2 種：其一為語言上的資訊藏密系統 (linguistic steganography)，這是利用語言上文字的佈置技巧所達成的一種資訊隱藏技術。其二為利用數位信號處理與影像處理的技術所研發出來的藏密系統 (technical steganography)，這是近代科學的成果，可以達成高難度的藏密要求。

所有權(copyright)的保護系統(copyright marking)可分為：易碎的數位浮水印技術(fragile watermarking)，用來認證(authentication)或驗證(verification)資料的正確性，防止資料被竄改(tamper)之用。強健的數位浮水印技術(robust watermarking)，用來隱藏一個版權資訊(一串文字，一個公司的 mark，或是特別的一個影像，聲音等)於多媒體的產品中，而當遭受破壞後，仍然保有此聲明版權的浮水印資料。這類的浮水印技術又可分為指紋密碼技術(Fingerprinting)，可見的數位浮水印技術(visible watermarking)及不可見的數位浮水印技術(imperceptible watermarking)。在本文中將完整介紹這些技術及其應用領域。

關鍵詞：影像藏秘機制(image steganography)，數位餘弦轉換(Discrete Cosine Transform，DCT)，展頻技術(Spread Spectrum，SS)，數位浮水印(digital watermarking)，靜態壓縮標準(Joint Photographic Experts Group，JPEG)。

1. 前言

自有人類以來，資訊往來是人與人之間必要的事務，而傳達資訊被稱為通信。通訊在人類的生活上是無所不在的，行動電話在我們的手上，電視在我們的客廳，電腦與網際網路在我們的辦公室，email 可在家中接收，由此可見通信對人類來說是時時刻刻都需要的。

由於秘密通信從古至今都有極大的需求，國家安全與軍事機密，都有賴於秘密通信機制而得到保障。工業技術，商業機密與個人創作的智慧財產等都需要有安全秘密的通信技術來保護。尤

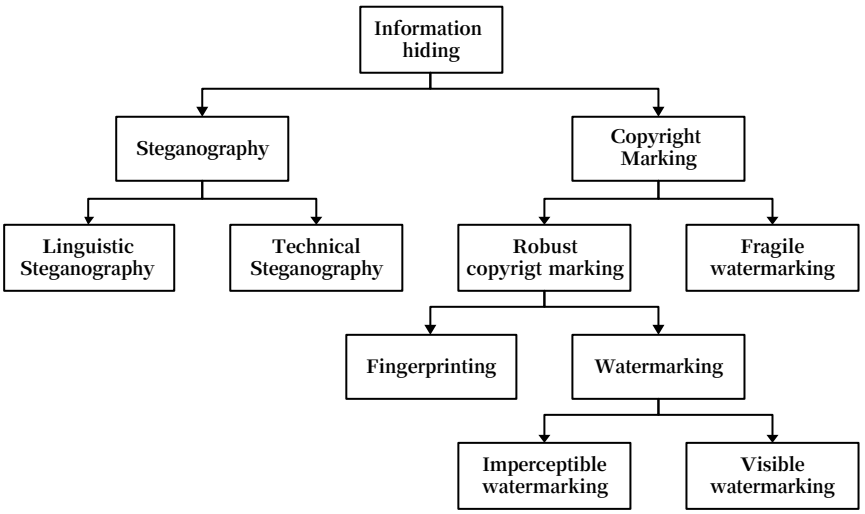
其是自由貿易的商業時代，網際網路拉近了地球村的距離，許多交易都在網路上進行，更為駭客大開竊取，破壞，篡改等不法行徑的大門。因此資訊隱藏技術與數位浮印技術是被用來作為秘密通信及保護私密資料，防止駭客的有效法門。

現代化的社會人人都有秘密通信的自由，擁有私有財產的自由及擁有私密資訊不為人知的自由。但通信會被竊聽，私有的智慧財產會被駭客盜取，私密資訊會被狗仔隊偵測而曝光，要如何落實這些自由？我們的祖先發明了隱形墨水，需經特殊的處理後才能使秘密文字現形。

現代的科技，利用密碼學的原理，設計許多加密解密及數位簽章的軟體被廣泛的使用在網際網路(internet)上，使得網路上的商業交易得以安全及保障。科技公司也將這些密碼學的理論轉化成實用的密碼 IC，而使自動提款機上所輸入的任何資料給予立即的加密保障而不怕駭客在傳輸途中的竊取與破壞。可是在多媒體所掌控的 e 世代，一切都以圖形介面，一切都是以影音取代文字，尤其是具有廣大商機的多媒體產品，經由廉價的多媒體設備可任易的複制，修改，傳播，使得產品的著作權及所有權遭到嚴重的破壞，而密碼學的技術只適合文字的處理，對於影像資料卻無能為力，因此發展影像資訊隱藏技術及所有權保障的技術，就顯得重要而不可缺了。

2. 資訊隱藏技術之分類

圖(1)是資訊隱藏技術階層圖 [1]，其中影像隱藏技術方面稱為 Steganography 是一種隱藏資料而又秘密的不對外公佈的隱藏技術。可分為 2 類：一類是利用語言上的知識將秘密資料隱含其中而字面上卻不被發覺的技術，稱為 Linguistic Steganography。另一類是利用數位影像與數位信號處理的技術，將秘密資料隱含其中而無降低封面影像(Cover Image)的品質稱為 Techincal Steganography。 在所有權保護方面，有一種易碎的浮水印技術稱為 Fragile Watermarking，專門用來作為防止竄改(tamper)與作驗証(verification)之用。另外強健性的所有權保護技術(Robust Copyright Markng)又分為專門用在點對點分佈系統用來驗証隱藏字串資料的浮水印稱為 Fingerprinting 浮水印技術。浮水印專門應用在影像方面可分為可見的浮水印技術(在封面影像上看得到浮水印)和不可見的浮水印技術(在封面影像上看不到浮水印)。為了使讀者容易了解資訊隱藏技術的分類與其特性，我們將以實例來說明其不同點。



圖(1)：資訊隱藏技術階層圖[1]。

2.1 語言式藏密法 (Linguistic Stganography)

下述書信是摘錄自霹靂布袋戲 [2] 的一篇書信，信上表面上看起來是稱頌被推薦者多才多藝，而實際上隱藏了求救的信息，明白的表達了已被軟禁的窘境(吾被禁)。這種利用語言上的技巧來傳達秘密信息而不被發現稱為語言藏密法(Linguistic Steganography)。

夜修羅管主大鑒:

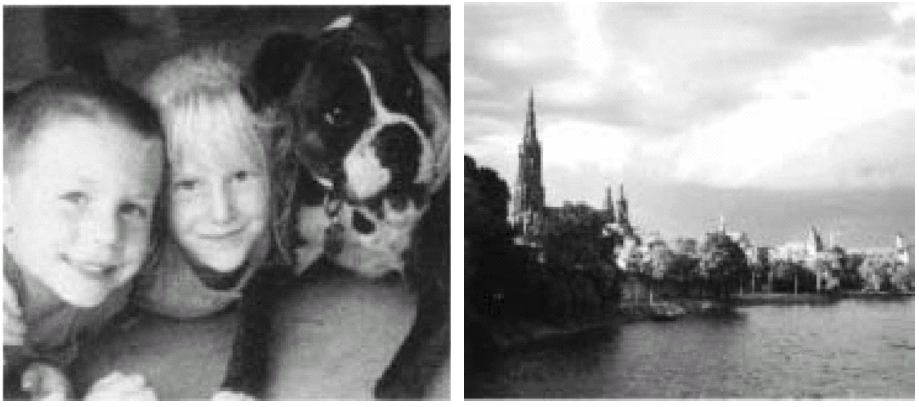
吾經天子，欲推薦一身懷大志之士；鬼王棺。此人被魔劍道納為軍師，乃因經通謀略之學，擅長詭奇禁術。更有驚人之武學造詣實為難得之輩。今日以魔劍道軍師之位，欲與貴界合作，謀取天下。吾深信以雙方之能，必能馬到成功。

玉指聖顏經天子親筆

2.2 技術式藏密法 (Technical Steganography)

利用數位影像與數位信號處理的技術將秘密資料隱含其中而無降低封面影像(Cover Image)的品質稱為 Techincal Steganography。這種技術是機密的，不對外公開所用的藏密方法，可藏任何形式的資訊(文字，影像，圖形)，可藏少量的秘密資訊或大量的影像。通常要藏匿大的影像時，都先以影像壓縮技術將資料量降低後，再搭配錯誤控制碼(Error Control Code)來降低取回秘密資料時的錯誤率。在進行資料隱藏時，通常有 2 種技術：空間域(spatial domain)與轉換域(transform domain)用來完成埋入程序而使人無法感知到有秘密資訊隱藏其中。一般而言轉換域的藏匿效果較佳。

圖(2)是 Technical Steganography 的一種應用範例，大圖藏大圖。其中圖 2(a)是秘密影像(secret image)藏入封面影像(cover image)後的影像，被稱為 stego-image。圖 2(b)是從 stego-image 中利用 technical steganography 的偵測技術所重建的秘密影像(secret image)。這種 technical steganography 的技術，不管是藏入資訊後的封面影像(stego image)，或是取回的秘密影像(secret image)，都擁有很高的影像品質，是人眼所無法察覺出來的，如同圖(2)所示。



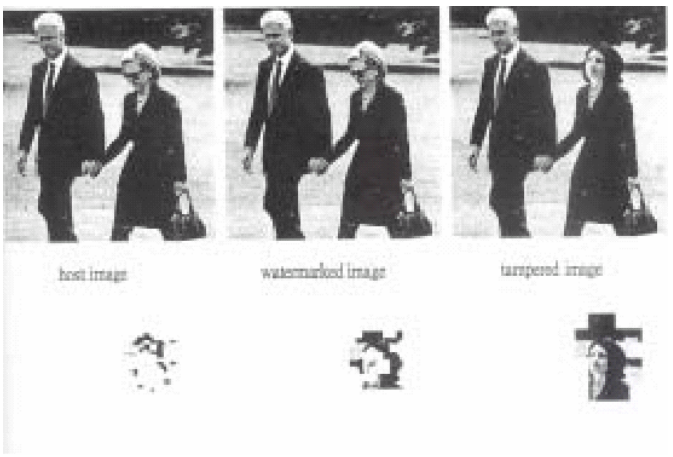
(a) (b)

圖(2)：Technical Steganography (a) 藏入秘密影像後的 Stego-image
(b) 取回後的 secret image.

Chen [3] 利用向量量化(VQ)技術並結合密碼學中的(DES)技術，發表一篇大圖藏大圖的影像藏密技術，使得秘密影像藏入封面影像的VQ索引中，而人眼無法查覺有秘密影像藏匿其中，且取回的秘密影像也和原始影像一模一樣具有高的影像品質。

2.3 易碎的浮水印技術 (Fragile Watermarking)

易碎的浮水印(Fragile Watermarking)，是專門設計來保護影像的完整性，防止駭客與非法份子對於影像資料進行竄改，例如使用影像處理軟體如 photoshop 或 photoimpact 都很容易完成剪貼、破壞、竄改等改變。假如影像有經過易碎浮水印的處理，則任何剪貼、破壞、竄改都會被偵測出來。如下圖所示，圖中的女主角被竄改了，但是經由浮水印偵測後便得知那些位置是假的、是被竄改的，會被清楚的標示出來，因此使原始影像得到保護。

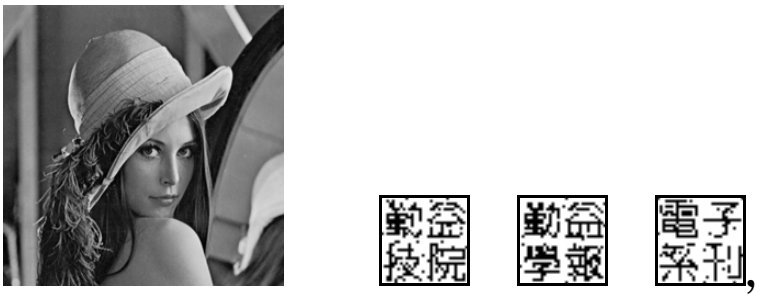


圖(3)：易碎的浮水印可以偵測出被竄改的地方與還原真實影像[4]。

Wu and Liu [5] 將封面影像利用數位餘弦轉換(DCT)轉換到頻率域，再製作一個浮水印隱藏用的對照表，利用查表的方式將密秘資料隱藏其中，而完成一種影像認證防止資料被竄改的易碎數位浮水印系統。

2.4 不可見強健性數位浮水印 (Invisible robust watermarking)

不可見強健性數位浮水印，是用來保護著作權及所有權，而又不會破壞原始影像的技術。這種技術將商標、產品序號，或是其它形式的 LOGO 等浮水印，隱藏至多媒體的產品中(包括聲音 audio、影像 image、影集 video、本文 text)，經由各種破壞測試(加雜訊 noising、模糊化處理 blurring、塗繪 painting、局部挖除 cropping、局部旋轉 rotating、放大縮小 resizing、改變亮度 lighting 及 JPEG 壓縮解壓縮處理)等都無法將浮水印移除。這種強健性數位浮水印具有多種特性如(1) 強健性(robustness)，可抵檔各式各樣的破壞(attacks)仍無法將其消除。(2)安全性(security)，浮水印資料(watermark)以極安全的方式藏入，使得駭客無法破解而取得。(3)不模糊性(unambiguous)，浮水印資料經由各種破壞後，仍能清楚的辨識出浮水印的內容，除非該多媒體資料或影像已經被破壞到失去價值的程度。圖(4)是不可見強健性數位浮水印的範例，圖 4(a)是已經藏入浮水印後的影像 host-image，圖 4(b)是從 host-image 取回的浮水印。



(a) (b)

圖(4)：不可見強健性數位浮水印 (a)原始影像 (b)取出的浮水印。

Hsu and Wu [6] 選取數位餘弦轉換後的中頻係數將具有視覺可辨識圖訊的數位浮水印隱藏其中，而完成一種不可見強健性的數位浮水印系統。Kii et al. [7]利用統計學上一種稱為拼湊法(patchwork)技術將數位浮水印藏入封面影像中，這種方法對於 JPEG 的壓縮破壞攻擊，特別有抵擋的能力。

2.5 可見強健性數位浮水印 (visible robust watermarking)

可見強健性數位浮水印，是用來保護著作權及所有權的技術之一，這種技術直接將商標、產品序號，或是其它形式的 LOGO 直接加到原始影像中，使得人眼可以隱約的看到浮水印的存在，就如同紙本的浮水印一樣是可看得見的。這種浮水印是以最直接的方式來宣告版權，如在電視 CNN 頻道上畫面的左上角，都有 CNN 字樣，這就是典型的可見的數位浮水印。圖(5)是可見強健性浮水印的範例，圖 5(a)是浮水印影像，圖 5(b)是藏入浮水印後的原始影像(host-image)，在圖 5(b)中可以隱約的看到浮水印的存在。

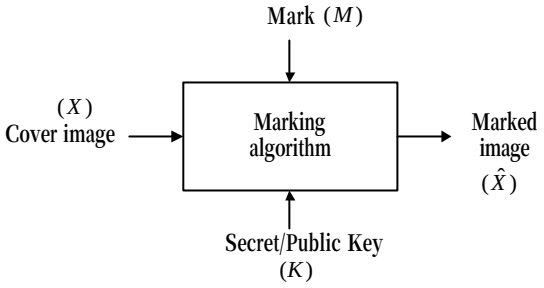
(a) (b)

圖(5)：可見強健性浮水印(a)浮水印影像 (b)藏入浮水印的封面影像[8]。

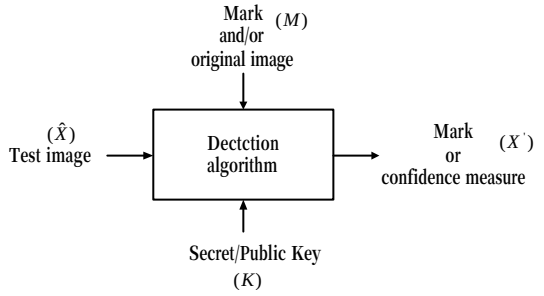
3. 資訊隱藏技術

資訊隱藏技術由 2 種程序來完成：(1)資訊藏入的流程如圖 6(a)所示。圖中我們將多媒體產品（智慧財產）簡稱為封面影像(cover image)，將所要藏入的商標、產品序號，或是其它形式的 LOGO 稱為標示(mark)，運用一種安全的一組秘密鑰匙或公開鑰匙(secret/public key)來作安全性的防範，然後以資訊隱藏演算法將 mark 資料藏入 cover image 中，產生已被標示的影像稱為 marked image。(2)資訊取出的流程如圖 6(b)所示。圖中我們將測試影像，原始影像或 mark 資料及藏入時所用的

同一支鑰匙(secret/public key)，再運用資訊隱藏偵測法將 mark 資料取出。我們將繼續介紹資訊隱藏技術的方法。



(a) 隱藏程序



(b)取出程序

圖(6)：資訊隱藏的示意圖 (a)資訊藏入示意圖 (b)資訊取出示意圖。

3.1 空間域的浮水印技術 (watermarking scheme in Spatial Domain)

資訊隱藏技術應用在空間域(spatial domain)具有大量的隱藏位置及容易隱藏，處理簡單等優點。其缺點是與轉換域的浮水印技術比較起來，其強健性(robustness)稍差一些。但只要設計得宜還是有很好的隱藏效果。空間域的資訊隱藏技術大都建立在人類的視覺系統(human vision system, VHS)的基礎上。根據 VHS，建立一套正好察覺失真程度(just noticeable distortion, JND)的公式來判斷可藏入的資料量，而又不會破壞原始影像的品質。一般常使用在空間域的浮水印技術有，類神經網路技術(neural network)，統計學技術(statistic)，展頻技術(spread spectrum)及密碼學技術(cryptography)，向量量化(VQ)，碎形編碼法(fractal)等。有時為了增加其強健性，這些空間域的技術會混合(hybrid)轉換域的技術來使用。

3.1.1 人類的視覺系統 (Human Vision System)

Wu and Tsai [9] 根據人類視覺系統，計算封面影像及數位浮水印間的像素位階(gray level) 差距值來判斷該封面影像的圖素可藏入多少個位元數(bit)，而不會影響視覺品質，發表一篇數位浮水印系統。

Lie and Chang [10]跟據大的灰階值可藏匿較多的位元數，在依人類視覺系統來計算將封面影

像的圖素值分為 4 類，每類分別隱藏不同的像素值，如此不僅不會增加額外的資料負擔(overhead)，且可隱藏大量的資料，依此方法建構了一種高品質的浮水印系統。

3.1.2 展頻技術 (Spread Spectrum)

展頻技術(Spread Spectrum)是隨機的(random)擴充一資訊位元成多個位元。其資訊位元值為高位元(Hi)的擴充位元與資訊位元值為低位元(Lo)的擴充位元成為反相狀態。為了產生隨機的擴充一資訊位元，一種稱為亂數數列(pseudorandom number sequence, PN)被用來完成該項任務。首先將數位浮水印資料傳換成位元序列 $d(j)$， $j=1,2,3...n$. 對於每個 $d(j)$，對映到一亂數序列 $r_j(i), i=1,2,3...l$，將兩者相乘即可得到展頻後的資料位元如下面公式所示。

$$m_j(i)=d(j)\cdot r_j(i),\quad i=1,2,3...l,\quad j=1,2,3...n. \tag{1}$$

由於浮水印資料在藏入封面影像前已先經由展頻技術調制，所以要取回浮水印資料也必需經由反展頻的技術才能正確的取回浮水印。反展頻是利用如下所示的公式來完成

$$d'(j)=\begin{cases}1, & if \quad \sum_{i}^{l} m_j'(i)\oplus r_j(i) < \dfrac{l}{2}\\ 0, & if \quad \sum_{i}^{l} m_j'(i)\oplus r_j(i) \geq \dfrac{l}{2}\end{cases} \qquad j=1,2,...n \tag{2}$$

其中 $m_j'(i), i=1,2,3...l$ 是由封面影像中取回的資料， $r_j(i), i=1,2,3...l$ 是展頻擴充時所使用的亂數序列， $\oplus$ 是互斥或(xor)運算。

3.1.3 向量量化與碎形編碼法(VQ and Fractal)

向量量化(VQ)是一種高壓縮比的影像壓縮技術，由於浮水印技術必須要能夠經得起(JPEG)壓縮的破壞才是有用的技術，因此將 VQ 技術引用到數位浮水印技術是正確的作法。

碎形編碼利用仿射轉換(affine transform)及區域疊代法(local iterated function system, IFS) 能夠有效的壓縮自然影像，如風景影像，海岸影像，或天空景像等。自從 jacquin 發表應用在資料壓縮的演算法後，碎形編碼技術就被大量的使用在影像處理的領域，因此引用在數位浮水印技術上，應該是合適的方法。

Bas et al. [11] 使用碎形編碼技術及在碎形編碼中的 domain pool 進行量化來藏入秘密資料發表強健性數位浮水印技術。為了防止方塊效應，每個 rang block 的動態值($\hat{R}$)小於 20 及 domain block 動態值介於 50-100 者才被選為藏匿浮水印的方塊，在其演算法中，其所藏入浮水印所使用的公式為:

$$\hat{R}=d*S*\frac{D}{\max(D)}+\overline{R} \tag{3}$$

其中 $\overline{R}$ 是 R 的平間均值,而且

$$d=\begin{cases}+1 & if \quad the \quad embedded \quad bit=1\\ -1 & if \quad the \quad embedded \quad bit=0\end{cases}$$

這種浮水印技術經由實驗測試，對於幾何破壞(geometric attack)如平移，旋轉，放大，縮小等特別有抵擋的能力。

3.2 轉換域的浮水印(Watermarking scheme in Transform Domain)

3.2.1 離散餘弦轉換法(discrete cosine transform, DCT)

離散餘弦轉換法(DCT)，將影像資料由空間域(spatial domain)轉換至頻率域(frequency domain)。一般最常用的是將原始影像分割成無數個不重疊的 8×8 區塊。每個區塊的 DCT 係數可分為直流值(DC)，低頻帶(low frequency band)，中頻帶(middle frequency band)，高頻帶(high frequency band)。若要獲得強健性的浮水印架構就必須將資料藏在低頻帶如下圖所示有標示 p 的區域。

DC		P+3	P+4	P+12			
	P+2	P+5	P+11				
P+1	P+6	P+10					
P+7	P+9						
P+8							

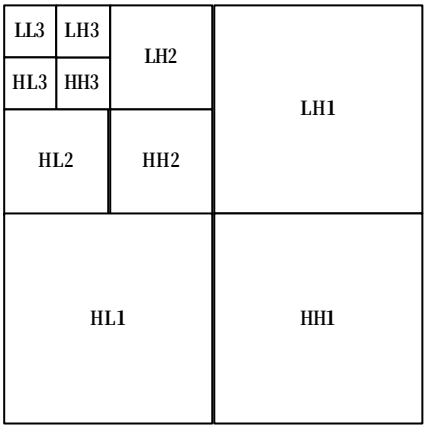
圖(7)：適合藏匿浮水印 DCT 係數的低頻帶。

Langelaar and Lagendijk [12]使用多個 DCT 區塊來隱藏一個位元，使用較低品質的 JPEG 因子來對抗重複編碼的破壞，及使用所謂在 DCT 係數鋸齒式掃描最小截斷索引(minimal cutoff index in zigzag scanned fashion of the DCT coefficient)等 3 種參數來建構出一種數位浮水印技術。

Lu et al. [13] 提出一種雞尾酒式的數位浮水印技術，其演算法中同時藏入 2 個浮水印，一個採用所謂的正性調制技術(Modu(+,+)或 Modu(-,-)，專門抵擋如 sharpening 或 histogram equalization 的破壞，另一個採用所謂的負性調制技術(Modu(+,-)或 Modu(-,+)，專門抵擋如 compression 或 blurring 的破壞.完成一種強健性高的數位浮水印技術。

3.2.2 離散小波轉換法(discrete wavelet transform, DWT)

離散小波轉換法，具有將原始影像能量集中及產生不同頻率帶的功能，因此被大量的使用在影像處理方面。最有名的頻率分解法稱為多解析度分析(Multi-Resolution Analysis, MRA)，如圖(8)所示。其中 LH1 是水平方向的邊影像，HL1 是垂直方向的邊影像，HH1 是對角方向的邊影像，LL1 則是原始影像縮小圖。以藏密的角度來看，LH3, HL3, HH3, LH2 HL2, HH2 等是較佳的隱藏地點，既不會降低封面影像的品質，又具有相當好的強健性，不會因受攻擊(attacks)時浮水印就被破壞。



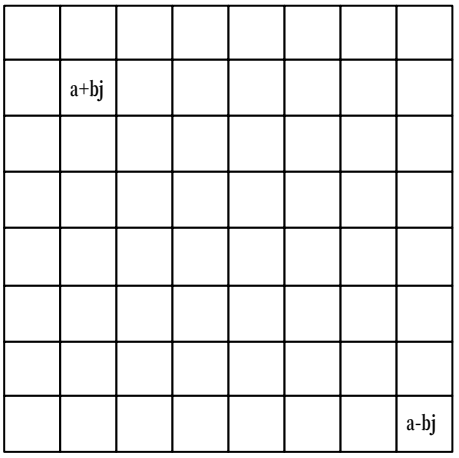
圖(8)：離散小波的多解析度分解示意圖。

C. S. Lu and H. Y. Liao [14] 利用量化原始影像的 DWT 轉換後的係數及使用雞尾酒式 2 個互補式的浮水印技術完成一種同時擁有易碎浮水印技術的認證功能及強健性浮水印技術的保護功能。

Wei et al. [15] 控制小波係數使得浮水印雜訊值小於人類視覺系統中的 JND(just-noticeable difference)值，建構出一種強健性的數位浮水印技術。

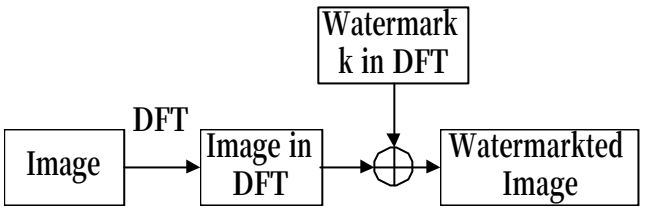
3.2.3 離散傅立葉轉換法(discrete fouries transform, DFT)

傅立葉轉換法(DFT)也是一種好的頻率轉換法。有 2 種藏密的方式，一種是將資料藏在振幅(amplitude)稱為振幅調制(amplitude modulation)，另一種是藏在相角(phase)稱為相位調制(phase modulation)。尤其以相位角的方式來藏匿浮水印時，就必須以 DFT 來轉換，因為 DFT 轉換後的係數是 a+bj 及 a-bj 的型態，而且是以對稱的方式出現，由這些係數中很容易就可取出相位資料，進一步的將資料隱藏其中。下圖即為 DFT 的係數，很清楚的看出其係數是對稱的。



圖(9)：傅立葉轉換後的係數藏匿區示意圖。

Premaratne and Ko [16] 將浮水印及原始影像同時都經由 DFT 轉換後才進行隱藏程序,而穫致一種強健性的數位浮水印技術,其方塊圖如(10)所示。

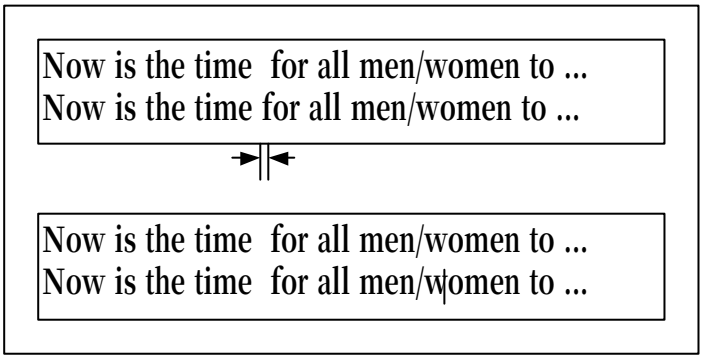


圖(10)：使用 DFT 轉換的浮水印藏入程序圖.

4. 應用領域

4.1 文件 (Documentation)

文件資料亦可用來隱藏秘密資料, 只是能隱藏的資料量較少而已。一般而言文件資料的隱藏方法有(1)行移編碼(Line-Shift Coding):利用調整文章前行與後行之間距來隱藏秘密資料的編碼.(2)字移編碼(Word-Shift Coding):將一個字輕微的向右或向左移動位置,而其鄰近的 2 個字保持不變的方式來將秘密資料編碼,這種編碼方式每一行的第一字或最後一字是不能所被選來隱藏資料的. 如下圖即是一種利用改變文字間的間距來隱藏資料的方法。



圖(11)：文件檔案的資料隱藏示意圖。

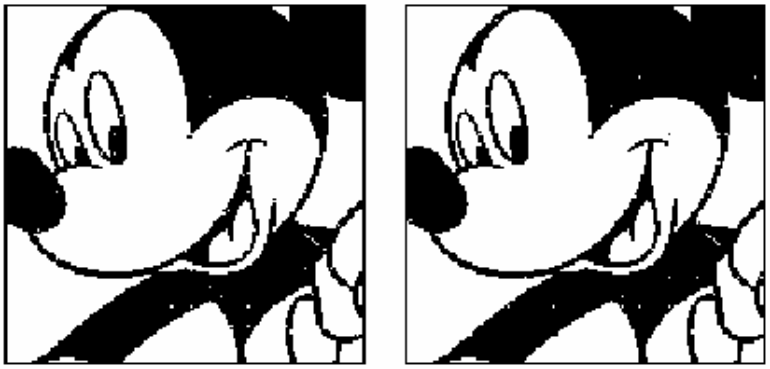
Kuo and Chen [17] 認為大部份的文件檔案都是利用 PDL(PostScript Page Description Language)來傳輸或儲存,因此將秘密資料隱藏在文件的 PDL 中。在演算法中一個前處理程序用來剖析原始文章中任何 2 字的間距(space),然後利用一組新的字體(token)來取代原來的字,以達到調整字的間距,達成藏入 0,1 的目地。該演算法的前處理還可以調整字距使其一致並避開每行必需對齊的問題,更好的是在取回秘密資料時並不需使用原始文件.

4.2 黑白影像(Binary Image)

黑白影像是一種藝術, 且所佔用的記憶體空間極小, 是灰階影像的 1/8, 彩色影像的 1/24, 有其存在的價值。如圖(12)所示, 黑白影像的資料隱藏最佳地點是影像的邊, 若資料不是隱藏在邊的位置時, 就會出現如圖(12)黑色部份出現白點, 白色部份出現黑點的現象, 既破壞畫面又被

知道有藏匿秘密資訊。黑白影像的藏匿法可分為 2 類：一類是改變個別的圖素來隱藏資料(individual pixels),另一類是改變一群圖素來隱藏資料(a group of pixels)，前者較為容易處理，且可以藏匿較多的資料。

Wu et al. [18] 基於改變個別圖素來隱藏資料的理念，將原始影像分割成無數個不重疊區塊，再以計算連續性及均勻性來評估該圖素是否適合用來隱藏資料，並以混亂原始影像機制(shuffling mechanism)來增大可隱藏區塊，而達成一個高影像品質且隱藏量大的資料隱藏系統。



圖(12)：黑白影像的資料隱藏示意圖[18]。

4.3 灰階影像 (Grayscale Image)

灰階影像的資料量較彩色影像較少，其影像品質與內容都相當美好，是重要的多媒體資料，大多數的影像處理技術都以灰階影像來測試發展。圖(13)是以勤益技術學院的標章當浮水印藏入灰階影像的一個範例。

圖(13)：灰階影像與其浮水印影像。

灰階影像的浮水印演算法相當多，在空間域(spatial domain)是以基於人類視覺系統(HVS)及展頻技術(Spread Spectrum)為最多。在轉換域(Transform Domain)則以 DCT 及 DWT 所搭配一些策略所建構出的系統最多。其中同位法(parity check bits)，加權法(weighting)，密碼法(cryptography)，補綴法(patchwork)，錯誤更正法(Error correction code)，互補式隱藏法(complementary)，查表法(look-up table)，群組法(group set)，人類視覺系統(VHS)，展頻技術(SS)，振幅調變技術(AM)，相位調變技術(PM)．．．等都是常用的轉換域搭配策略。

4.4 彩色影像 (Color Image)

彩色影像是重要的多媒體資料，現在我們所見所用的影像，大都是彩色影像。圖(14)是以勤益技術學院的標章當浮水印藏入彩色影像的一個範例。在彩色影像處理時通常將彩色影像由(RGB)平面轉換至 YUV 平面來處理，因為 Y 平面將包含有 93%，U 平面將包含有 5%，V 平面將包含有 2%的彩色影像的能量。當影像處理完後再經由 YUV 平面轉換回原來的 RGB 平面。

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.30 & 0.59 & 0.11 \\ -0.15 & -0.29 & -0.44 \\ 0.61 & -0.52 & 0.1 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{4}$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.01 & 0.007 & 1.14 \\ 0.994 & -0.381 & -0.583 \\ 1.000 & 2.02 & 0.006 \end{bmatrix} \begin{bmatrix} Y \\ U \\ V \end{bmatrix} \tag{5}$$

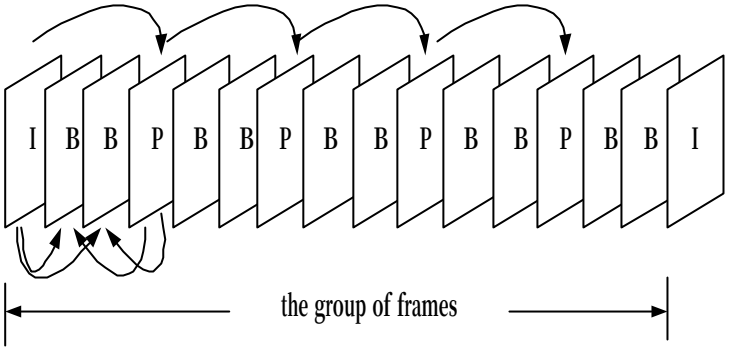
圖(14)：彩色影像與其浮水印影像。

Puertpan and Amornraksa [19] 基於高斯圖素加權遮罩(Gaussian pixels-weighting marks)的理念，將彩色影像轉換至 YUV 平面，然後將自己圖素及鄰近圖素的明亮度加權平均後，再以振幅調變技術將浮水印資料藏入影像中。在偵測浮水印時，經由平均加權該圖素及鄰近圖素的技術，可以不用原始影像而順利的取出浮水印。

4.5 影集 (Video)

影集(video)是由一連串的影像集合而成。影集是動畫，每秒鐘有 30 個影像畫面，資料量大得驚人，因此經由動態影像壓縮是必要的。MPEG-1 是現行 VCD 所採用的壓縮標準(standard)，MPEG-2 是 DVD 所採用的壓縮標準，在這標準之下資料量可降低千倍而仍有良好的畫質，這是由於 MPEG-2 會消除時間上的累贅(temporal redundancy)而得的壓縮效果。同樣的原理，若資料要

隱藏在 video 中，就必需考慮 MPEG-2 的壓縮原理(畫面分為 Intra, bi-directional, Predictive, IBP)，將資料隱藏在 I 畫面才能獲得強健性。圖(15)是影集的資料畫面，我們可以清楚的知道秘密資料在 video 中的最佳藏匿地點了。



圖(15)：MPEG video 影像的時間軸示意圖。

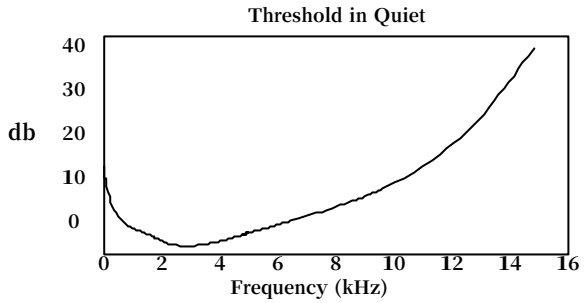
Liu et al. [20] 利用 4 種策略：(1)將資料隱藏在 LL^3 子頻帶； (2) 使用 BCH 碼來降低取回資料的錯誤率；(3) 使用 3-D interleaving 技術來更正 bursts；(4) 發展出一個有效的時間同步技術 (temporal synchronization technique)在數位小波轉換域(DWT)建構出一個 Video 浮水印系統。

Hsu and Wu [21] 基於 MPEG 的位元資料流(bitstreams)結構將浮水印隱藏在 intraframe 的中頻範圍及 non-intraframe 的動作估測向量中，而建構出一種 Video 浮水印系統。

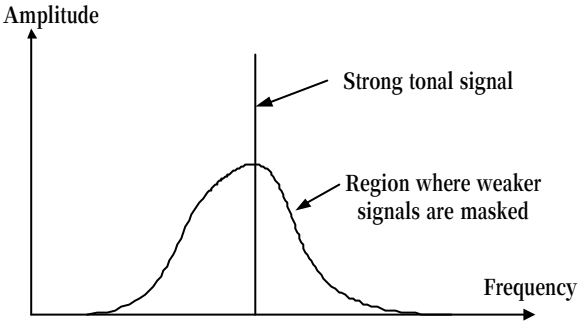
4.6 聲音 (audio)

多媒體影音資料是現代化生活的必需品，我們每天都從電視及其它媒體獲得許多資訊，其中聲音是重要的一種。我們聽的音樂與廣播，或其它的有聲書都是屬於智財產都需要保護。聲音的浮水印或聲音的藏密機制是重要而必需的。聲音的藏密機制通常可分為時間域(time domain)及頻率域(frequency domain)兩種模式，在頻率域又以 DFT 轉換為主。在聲音浮水印的處理技術方面大都以人類聽覺系統 human auditory system (HAS)為基礎。由於人類耳朵對於聲音的敏感性很高，不像人類的眼睛對於影像的敏感性較低，使得設計聲音浮水印的處理技術較為困難，而且聲音的檔案資料較影像檔案小很多，使得強健性的聲音浮水印更難達成。

人類的聽覺效應是隨著不同的頻率有不同的靈敏度，如圖(16)所示，人類的耳朵對於頻率範圍在 2k-4k 中的聲音特別靈敏，只要有一點小聲音，立即會被查覺，而其它頻率則依圖(16)曲線而各不相同了。在人類的聽覺效應中，強的聲音會遮蔽弱的聲音，稱為遮蔽效應，其強弱如圖(17)所示。例如在一個特別大的聲音中，會聽不到其它較弱的聲音。 這些聽覺特性是設計聲音浮水印者必需考慮的因素。



圖(16)：人耳聽覺臨界絕對值



圖(17)：人類聽覺的遮蔽效應.

Pei and Tai [22] 利用人類聽覺系統(HAS)建構了一套強健性的聲音浮水印系統。這個系統可以隱藏兩種不同的浮水印, 一種是字串形態的浮水印另一種是聲音形態的浮水印。在這論文中也祥述了各種原理，現象，及解決方法，是從事聲音浮水印研究者一篇很好的參考資料。

5. 結論

綜合前面的分析，對於不同的藏密需求, 有不同的演算法來達成任務，只是這些功能的完美程度不同而已。時代在進步，產品日新月異，功能與使用方式, 外表包裝都是一日千里，所以資訊隱藏技術也都紛紛的被發展出來，但是精益求精，發展更完美、更快速、更有效、更強健的資訊隱藏技術，是所有從事科技工作者的努力目標與責任。

參考資料

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, “Information Hiding – A Survey,” Proceeding of the IEEE, Vol. 87, No. 7, pp. 1062-1078, 1999.

[2] 霹靂布袋戲雜誌, 2002.

[3] T. S. Chen, C. C. Chang and M. S. Hwang, “A Virtual Image Cryptosystem Based upon Vector Quantization,” IEEE Trans. on Image Processing, Vol. 7, No. 10, pp.1485-1488, Oct 1998.

[4] 呂俊賢與廖弘源, “Cocktail Watermarking on Image,” 影像與識別 2000, Vol. 6, No. 1, pp28-36, 2000.

[5] M. Wu and B. Liu,” Watermarking for Image Authentication,” IEEE Conference, pp. 437-441, 1998.

[6] C. T. Hsu and J. L. Wu, “Hidden Digital Watermarks in Images,” IEEE Trans. on Image Processing, Vol. 8, No. 1, pp. 58-68, Jan 1999.

[7] H. Kii, J. Onish and S. Ozawa, “The Digital Watermarking Method by Using Both Patchwork

and DCT," IEEE conference, pp. 895-899, 1999.

[8] P. M. Chen, "A Visible Watermarking Mechanism Using a Statistic Approach, " Proceeding of ICSP, pp. 910-913, 2000.

[9] D. C. Wu and W. H. Tsai, "Spatial-Domain Image Hiding Using Image Differencing," IEE Proc.-Vis. Image Signal Process, Vol. 147, No. 1, Feb. 2000

[10] W. N. Lie and L. C. Chang, "Data Hiding in Images with Adaptive Numbers of Least Significant Bits Based on the Human Visual System," IEEE conference, pp.286-290, 1999.

[11] P. Bas, J. M. Chassery and F. Davoine, "Using the Fractal Code to Watermark Images," IEEE conference, pp. 469-473, 1998.

[12] G. C. Langelaar and R. L. Lagendijk, "Optimal Differential Energy Watermarking of DCT Encoded Images and Video," *IEEE Trans. on Image Processing*, Vol. 10, No. 1, pp. 148-158, 2001.

[13] C. S. Lu, S. K. Huang, G. J. Sze and H. Y. Liao, "Cocktail Watermarking for Digital Image Protection," IEEE Trans. on Multimedia, Vol. 2, No. 4, pp.209-224, Dec. 2000.

[14] C. S. Lu and H. Y. Liao, "Multipurpose Watermarking for Image Authentication and Protection," IEEE Trans. on Image Processing, Vol. 10, N. 10, pp.1579-1592, Oct 2001.

[15] Z. H. Wei, P. Qin and Y. Q. Fu, "Perceptual Digital Watermark of Images Using Wavelet Transform," *IEEE Trans. on Consumer Electronics*, Vol. 44, No. 4, pp.1267-1272, 1998.

[16] P. Premaratnee and C. C. Ko, "A Novel Watermark Embedding and Detection Scheme for Image In DFT Domain," Image Processing and its Application, Conference Publication No. 465, IEE, pp. 780-783, 1999.

[17] C. H. Kuo and L. H. Chen, "A Study on Data Hiding for PostScript File," The 13th IPPR Conference on CVGIP, pp. 340-347, 2000.

[18] M. Wu, E. Tang and B. Liu, "Data Hiding in Digital Binary Image," IEEE Conference, pp.393-396, 2000

[19] R. Puertpan and T. Amornraksa, "Gaussian Pixel Weighting Marks in Amplitude Modulation of Color image Watermarking", IEEE ISSPA, Kuala Lumlur, Malaysia, pp.19197, Aug. 2001.

[20] H. Liu, N. Chen, J. Huang, X. Huang and Y. Shi, "A Robust DWT-Based Video Watermarking Algorithm", IEEE Conference, pp. III-631-III-634, 2002.

[21] C. T. Hsu and J. L. Wu, "DCT-Based Watermaking for Video", IEEE Trans. on Consumer Electronics, Vol. 44, No. 1, pp. 206-216,Feb. 1998.

[22] S. Pei and Y. H. Tai, "Digital Audio Watermarking Techniques Utilizing Human Auditory System", **影像與識別** 2000, Vol. 6,No.1 , pp.49-78, 2000