

行政院國家科學委員會專題研究計畫成果報告

電子商務的數位影像浮水印，所有權資訊確認，

及壓縮技術整合之設計與研發

計畫編號：NSC88-2416-H009-021

執行期限：87 年 8 月 1 日至 88 年 7 月 31 日

主持人：蔡銘箴 國立交通大學資訊管理研究所

電子信箱：mjtsai@cc.nctu.edu.tw

一、中文摘要

數位資訊重製及改造的技術相當容易，使得數位影像在電子商務的應用中，衍生出對所有權保護及認證技術需求的日益迫切，交易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。因此，對數位影像加入不易察覺的標記－如浮水印，使得它能很容易地被所有權者加入或移除，由於有相當於私人簽章的加密，提供了保護的機置；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，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，以保障合法使用者的權益，使電子商務的安全性受到保障，接受度更為提高。本計畫的目的便是對電子商務的數位影像資訊所有權保護及認證的技術做深入而廣泛的研究，以提供解決的管理方式。

關鍵詞：數位浮水印，電子商務，專利所有權認證，數位影像處理，小波轉換。

Abstract

The techniques of the duplication and modification for digital data are comparatively simple. This situation has incurred the extreme need for the copy right protection and authentication for the digital image applications in electronic commerce.

The buyers and the sales must verify the integrity and status of the information source during the transaction. Therefore, to add the imperceptible digital watermarking into the digital image could meet the requirement. The owner of the digital image can very easily insert or extract the digital watermarking. The inserted information has the equivalent function of the private key encryption which offer the mechanism of protection. However, after deliberate manipulation like rotation, shifting, compression, zooming, transformation... etc. by the attackers, the watermark still exists and can offer the records as the reference. This makes the authentication mechanism available to verify the ownership attributes and also protect the normal usage for the legal users. The digital watermarking for the electronic commerce increases the reliability and safety which will improve the acceptance through the internet.

The goal of this research project will concentrate on the design and development of the ownership protection and authentication techniques for the digital image applications in electronic commerce. We expect to elaborate a manageable solution to fulfill the demands.

Keywords: digital watermark, electronic

commerce, copyright
authentication, digital image
processing, wavelet transform。

二、緣由與目的

緣由 - 由於網際網路的運用已蔚為風潮，使得網路資訊的交流，深入大眾的生活。而網路資訊的內容，已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，網路資源的持續擴充，吸引更多的使用者；一般家庭用戶，除了以最基本的電話網路登上網際網路外，有線電視頻道也以能直通網際網路為目標，期能更進一步打入消費者的生活，以擴展使用的範圍。網路資源的持續擴充與普及，吸引更多的使用者，也促進了商業行銷的契機。

而企業資訊網路的建製成本，由於技術的日益成熟，逐漸的降低；同時網際網路吸引了廣大消費者，基於經濟及實用性的考量，越來越多的商業交易也以數位化的格式來進行，使得電子商務[1, 2]的商業架構模式，已成為廠商行銷時不可缺少的重要管道；而商務多媒體如數位影像[3]的應用，使網頁的內容變得生動富有吸引力，更是網路資訊設計不可缺少的重要資料內容。

在瀏覽器內建功能的輔助下，網路數位資訊的重製相當容易，而影像處理軟體的操作容易，使得改造技術的取得，並不是件難事，這使得數位影像在電子商務的應用上，衍生出對所有權保護及認證技術[4]的需求，也就是交易的雙方必須對重要資訊來源的真實性及使用者的身份，提供確認。這一問題若沒有合理的解決途徑，廠商將不願將具有著作權的影像資訊放置在網際網路上，提供給消費者參考；流通資訊內容的缺乏，將阻礙了商務多媒體的應用，影響到整體電子商務的發展。

因此，對數位影像加入具有可資辨認的標記 - 如浮水印[5, 6, 7, 8]，使得它能很

容易地被所有權者加入或移除，但卻不易察覺；所傳遞的資訊，由於有相當於私人簽章的加密[9]，提供了保護的機置，使得未經授權的使用者，對數位影像經過各式的處理，如旋轉、平移、壓縮、放大、縮小、向量空間轉移 ... 等，浮水印的標記仍然保留，可供作證的參考，使驗證者可確保所有權的歸屬，以保障所有權擁有者及合法使用者的權益。

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，資料需經 Fast Fourier Transform 快速傅立葉轉換[3]、Discrete Cosine Transform 數位餘弦轉換[3]或是 Wavelet Transform 小波轉換[10, 11, 12]，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，將會是數位影像浮水印技術的主流。

目的 - 本計畫的目的便是對電子商務的數位影像資訊所有權保護及認證的技術做深入而廣泛的研究，以提供解決管理的方法。

譬如電子商務中，電子支票清單的列印、

傳送亦是銀行服務的項目之一。支票若未加註標記，傳遞過程中受到更改，或竄改支付金額，偽造簽名，不易確認其真實性；同時對電子數位支票加入浮水印標記，能使數位影像成為確認所有權的工具，以遏止非經授權的重製，及電子文件的分發。此技術除了在電子商務的應用外，對其他領域亦有相當重要的利用價值。例如，NII中的電子化政府，地籍圖資料具有公共參考的使用目的，加入浮水印，可確保地圖公正唯一性，以防未經授權的變造或竄改，使非法引用者無法遁形，且提供預警的效果。

三、結果與討論

本研究計劃已獲得相當豐富的研究成果，累積至今，已有兩篇會議論文的發表。第一篇是發表於1998年十一月二十日至二十一日於第四屆國際資訊管理研究暨實務研討會，地點是輔仁大學，論文內容請見[13]

第二篇則是發表於1999年六月四日至五日於第十屆國際資訊管理學術研討會，地點是中央警察大學，論文內容請見[14]及附件一。

四、計劃成果自評

本研究計劃研究成果，已獲得相當學術成果，對促進學術交流及發展，有豐碩及成熟的表現；除了將繼續做更深入的探討外，也積極參與相關學術研討及論文發表，以達到有效應用為目的。

五、參考文獻

- [1] Ravi Kalakota and Andrew B. Winston, *Frontiers of Electronic Commerce*, Addison-Wesley, 1996.
- [2] Ravi Kalakota and Andrew B. Winston, *Electronic Commerce: A Manager's Guide*, Addison-Wesley,

- 1997.
- [3] Anil K. Jain, *Fundamentals of Digital Image Processing*, Prentice-Hall, 1989.
- [4] E. Koch, J. Rindfrey, and J. Zhao, "Copyright protection for multimedia data," *Proc. Int. Conf. Digital Media and Electronic Publishing*, 1994
- [5] R.G. Schynde, A.Z. Tirkel, C.F. Osborne, "A digital watermark," *Proc. IEEE International Conference on Image Processing (ICIP'94)*, vol. 2, pp.86-90, 1994.
- [6] I.J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for image, audio and video," *Proc. IEEE International Conference on Image Processing (ICIP'96)*, vol.3, pp. 243-246, 1996
- [7] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *Proc. Infocom'94*, pp. 1278-1287.
- [8] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," *Proc. SPIE*, vol. 2420, p.40, Feb. 1995.
- [9] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21(2), pp. 120-126, Feb. 1978.
- [10] Daubechies, "Orthonormal bases of compactly supported wavelets," *Comm. Pure Appl. Math.*, vol. XLI, pp. 909-996, 1988.
- [11] S. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation", *IEEE Trans. Pattern Analysis Machine Intell.* 7:674-693, 1989.
- [12] M. Vitterli and C. Herley, "Wavelets

and filter banks: theory and design," *IEEE Trans. On Signal Processing*, vol. 40, pp. 2207-2232, Sep. 1992.

- [13] 蔡銘箴, 游光堯, "數位浮水印對電子商務影像資訊的所有權確認技術之研究", 第四屆國際資訊管理研究暨實務研討會, pp. 102-109, 輔仁大學, 1998.
- [14] 蔡銘箴, 游光堯, "可辨識的數位影像浮水印對所有權確認之研究", 第十屆國際資訊管理學術研討會, pp. 855-862, 中央警察大學, 1999.

附件一：可辨識的數位影像浮水印對所有權確認之研究¹

蔡銘箴 游光堯

交通大學資訊管理研究所

mjtsai@cc.nctu.edu.tw

u8634508@cc.nctu.edu.tw

摘要

對影像資訊而言，使用加解密的資訊安全的技術，仍不足以保障所有權人的認證，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，確認所有權擁有者的機制已經消失。然而，使用數位浮水印，將其嵌入資料當中，即使經過複製或有限度地破壞，數位浮水印仍存在於資料之中，可作為提供版權證明之證據，使得加密保護的工作更為完備。然而，具可辨識能力的數位浮水印，對所有權的確認，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，比以亂數產生的浮水印更有實際應用的參考性，對資訊安全及隱私權的保護，提供所有權辨認的不可否認性。本研究目前已成功地利用小波轉換(DWT)，設計出一套數位浮水印的架構，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。

關鍵字：數位浮水印、小波轉換、所有權確認、電子商務。

1.前言

網際網路的普及，提高了使用者對資訊技術的要求；在即時的線上傳輸資料中，影像資訊是最常被讀者所使用的多媒體資料型態。對影像資訊而言，使用加解密的資訊安全的技術，仍不足以保障所有權人的認證，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，使用數位浮水印，將其嵌入資料當中，即使經過複製或有限度地破壞，數位浮水印仍存在於資料之中，以作為提供版權證明之證據，可使得加密保護的工作更為完備。

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]-[4]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[5]-[9]，如[5]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。

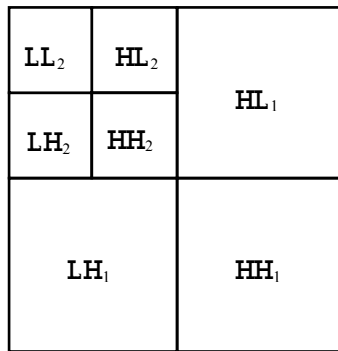
¹ 本文作者感謝國科會對本研究計畫的部分補助
(計畫編號：NSC88-2416-H009-021)

針對於目前提出的浮水印技術中[5]-[8]，所嵌入之數位浮水印大多為亂數產生的序列，如[5]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。

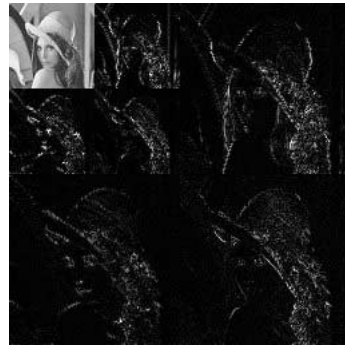
類似研究在[9]中有以DCT的步驟作比較，其方法是以類似JPEG的編碼，以事先預定的排列方式來加入浮水印，所採用的浮水印圖形幾佔原影像圖形之1/4，實不可不謂不大。由於浮水印本身太過龐大，致使影像的品質受到影響，連帶的使以[9]描述所製造的浮水印圖形其抵抗攻擊的能力，為之減

弱。

低頻-高頻波段(LH_1)等。

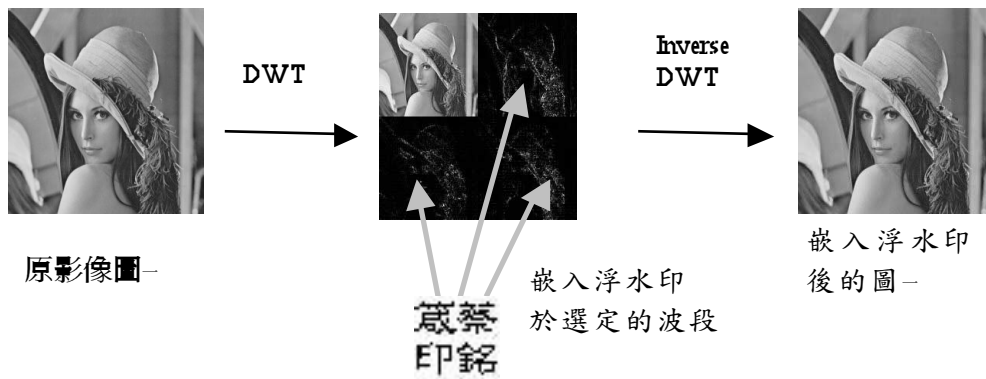


(a)



(b)

圖(一) 影像圖形之 DWT 金字塔結構分解圖 (a)示意圖(兩層的分解) (b)範例



圖(二) 數位浮水印的嵌入程序

本研究目前成功地利用小波轉換(DWT)，設計出一套數位浮水印的架構，以一視覺上可辨識的影像，作為嵌入圖形之數位浮水印。不同於[9]的，由於採用multi-resolution的方式，浮水印本身可以很小，使得其對於原影像圖形的影響降至最低。此外，此浮水印架構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)；同時，可在一影像資料中，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。

2.數位浮水印架構

在本研究中，我們利用小波轉換(Discrete Wavelet Transform, DWT)的技術，建構數位浮水印的架構。小波轉換基本的概念，是將訊號分離成高頻與低頻兩部分。對於二維的影像圖形，可將其分離成如(圖一)般的金字塔(pyramid)結構，其中為高頻-高頻波段(HH_1)、

因此，若將數位浮水印嵌入於影像的適當波段中，例如高頻-高頻(HH_1)波段，由於較高頻的波段是由圖形的稜角成分組成，嵌入浮水印於此僅會改變圖形的稜角色差，而人類的視覺系統對於高頻訊號的變化較不易感受，我們即可利用此特性來嵌入並偵測數位浮水印，達到嵌入浮水印不易受察覺的目的。

2.1 數位浮水印嵌入程序

數位浮水印的嵌入程序說明如下(圖二)：首先，將原始圖形經以小波轉換處理，將其分解成前述之金字塔結構；其次，選定欲嵌入數位浮水印的波段，將長度為P的數位浮水印，嵌入於影像中。在此，我們使用以下的公式：

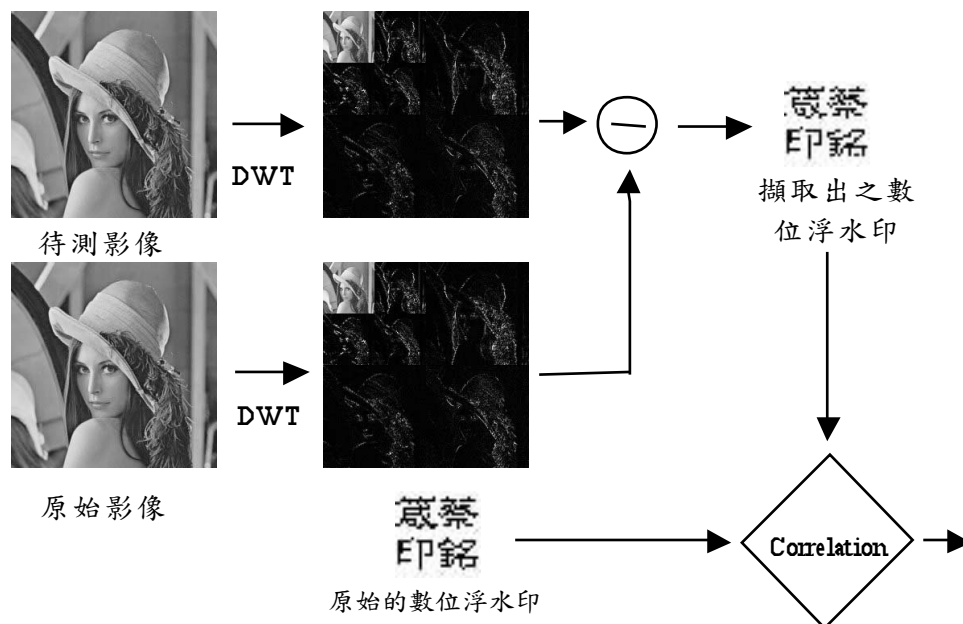
$$y'[m,n] = y[m,n](1 + \alpha \times N[m,n])$$

其中 $y[m,n]$ 與 $y'[m,n]$ 分別代表嵌入前、後，選定波段的 DWT 前 P 大的數值； $N[m,n]$

代表數位浮水印； α 則為強度參數，用以控制嵌入浮水印的強度。

最後，再將嵌入後的 DWT 數值 $y'[m,n]$ 取代原波段的數值 $y[m,n]$ 。再對整張圖形的訊號作 **Inverse DWT**，嵌入數位浮水印的程序即告完成。

2.2 數位浮水印擷取程序



圖(三) 數位浮水印偵測程序

偵測程序如圖(三)所示：首先，將待測之影像圖形與原始圖形分別做小波轉換處理；其次，將兩圖形之 **DWT** 係數相減。根據原始數位浮水印長度 p 與嵌入之波段，將待測圖形可能含有之數位浮水印擷取出來。最後，計算此擷取之數位浮水印與原始數位浮水印的相關程度(**Correlation**)，可得一反應常數。在此，計算相關程度所使用的公式如下：

$$\text{相關程度} = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2} \sqrt{\sum (y - \bar{y})^2}}$$

其中， x 代表自待測圖形中取出之數位浮水印， y 代表原始數位浮水印。而 $\bar{x}$ 與 $\bar{y}$ 則分別代表其平均值。相關程度的數值介於零與一之間，若其數值趨近於一，代表擷取之數位浮水印與原始浮水印非常相近。

3.實驗數據的探討

在本章節中，我們討論數位浮水印對影像品質的影響，以及浮水印在數種攻擊下的表現，最後則對嵌入數個浮水印(**Multiple Watermark**)進行討論。以下的實驗中，我們使用影像大小 512x512 像素的 **Lena** 圖形，作為嵌入的測試圖檔，嵌入的數位浮水印大小為 32x32 的 **binary image**，並且使用三層的 **DWT** 的分解結構。

3.1 數位浮水印對影像品質的影響

一般來說，嵌入影像圖形中的數位浮水印，強度越強，越能抵抗對於圖形的攻擊；但是嵌入過強的數位浮水印，可能會造成圖形視覺上的影響。因此，可動態地調整浮水

嵌入 波段	嵌入後圖 形 PSNR(dB)	偵測浮水 印 Correlation	浮水印 Error Points
HH ₁	60.59	0.995	0
LH ₁	56.62	0.998	0
HL ₁	51.68	0.999	0
HH ₂	51.17	0.998	0
LH ₂	49.15	0.999	0
HL ₂	45.12	0.999	0
HH ₃	46.03	0.999	0
LH ₃	45.86	0.999	0
HL ₃	40.79	0.999	0

表(一) 未受攻擊下，數位浮水印在不同波段的表現

印強度參數 α ，達到浮水印不易察覺的要求。本架構中，嵌入浮水印於較高頻的波段時，可使用數值較大的 α 值；於較低頻波段時，則改用強度較小的 α 。

3.2 數位浮水印在影像未受攻擊下的表現

表(一)為使用固定的浮水印強度參數 $\alpha=0.3$ ，將數位浮水印嵌入於圖形不同波段的表現。我們以擷取之數位浮水印與原始浮水印的相關係數，以及與原始浮水印的誤差點

數(**Error Points**：最小 0，最大 $32 \times 32 = 1024$ 點)作為評比的標準。在影像圖形未受攻擊下，偵測數位浮水印的相關程度非常地高，並且能夠正確無誤地被擷取出來(**Error Point=0**)。而嵌入浮水印於不同波段，對原圖形的影響可由表中的 **PSNR** 欄位看出，嵌入圖形越內層的波段(如 **HL₃**)，其 **PSNR** 數值越小，對圖形的影響較大。以圖(四)為例，嵌入浮水印於 **HL₃** 波段後，圖形的 **PSNR** 為 40.79，但在視覺上仍與原始圖形非常相似。



(a) (b) (c) (d)
圖(四) 在圖形未受攻擊下，嵌入數位浮水印於 HL_3 波段
(a)原始圖形 Lena (b)嵌入之數位浮水印
(c)Watermarked 影像 (PSNR=40.79dB) (d)擷取之數位浮水印

3.3 改變圖檔大小 (Bilinear Resizing) 的攻擊

改變圖檔大小的攻擊如圖(五)所示，將原始圖形由 512×512 像素，Bilinear Resizing 成 256×256 像素，此時，體積僅為原檔案的四分之一(用於偵測階段使用時，必須再將其放大回原始圖檔的大小)，也就是喪失了原圖形 75% 的資訊。經過此一攻擊，嵌入浮水印之圖形其 PSNR 下降至 30dB 左右。在此實驗

中，我們同樣使用固定的浮水印強度參數 $\alpha = 0.3$ ，而浮水印的反應如表(二)；我們發現，將數位浮水印嵌入越內層的波段，所擷取的浮水印相關程度越高，抵抗 Resizing 的能力越強。

3.4 JPEG 失真壓縮的攻擊

我們將嵌入數位浮水印的圖形經以 JPEG 失真壓縮，首先以不同的壓縮率加以測

嵌入波段	攻擊前圖形的 PSNR	攻擊後圖形的 PSNR	偵測浮水印的 Correlation	浮水印的 Error Points	擷取之數位浮水印
HH_1	60.91	31.53	0.009	293	
LH_1	57.35	31.53	0.039	313	
HL_1	52.35	31.53	0.025	331	
HH_2	50.96	31.49	0.901	80	
LH_2	49.38	31.47	0.951	25	
HL_2	44.87	31.37	0.948	23	
HH_3	45.71	31.39	0.927	29	
LH_3	45.79	31.39	0.969	3	
HL_3	41.12	31.12	0.978	2	

表(二) Bilinear Resizing 攻擊下，數位浮水印在不同波段的表現



(a)



(b)

圖(五) Bilinear Resizing 攻擊

(a) Resizing 前圖檔 512×512 pixels

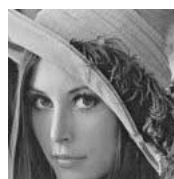
(b) Resizing 後圖檔 256×256 pixels

試。表(三)為嵌入浮水印於 LH_3 波段，使用強度參數 $\alpha=0.3$ 時的結果。在壓縮率低時，浮水印皆能清楚地被擷取出來；隨著壓縮率的提高，影像檔案失真的程度越嚴重，因此擷取出的數位浮水印的誤差會越大。我們若以偵測浮水印的相關程度大於 0.8，浮水印誤差點數不超過 50 點為可辨識的標準，嵌入浮水印於 LH_3 波段時，影像資料在經過 14.5:1 的失真壓縮率下，仍可辨識其中的數位浮水印；更高的失真壓縮，由於破壞太大，使其辨識能力大為降低。表(四)則說明在可辨識出數位浮水印的條件限制下，不同波段可達到的壓縮率與相關程度等表現。實驗數據顯示，將浮水印嵌入越內層的波段，可將影像壓縮的程度越高，使浮水印抵抗壓縮攻擊的能力增強。

3.5 Cropping 的攻擊



(a)



(b)

圖(六) Cropping 攻擊

(a) 去除外圍部分，僅保留影像中央部分

(b) 以未含數位浮水印的原始影像取代

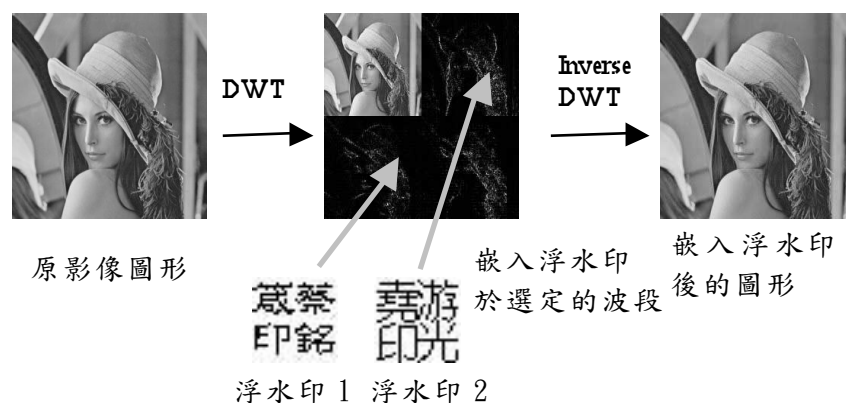
Cropping 的攻擊如圖(六)所示：只保留含數位浮水印的影像其中央部分；要擷取此部分的數位浮水印，該影像去除的部分則以尚未添加數位浮水印的原始影像取代。其實驗數據如表(五)所示：因為圖形的 3/4 部分被取代的關係，浮水印的相關係數降至約 0.6 上下；由於只剩下 1/4 的浮水印相關訊息，吾人可見其外圍部分幾乎喪失，這是由於 DWT 的 localization 的特徵所致，同時擷取出的數位浮水印只剩中間的圖形部分，其辨識程度受到影響，error points 的數目則較高，但仍有相當的資訊可供辨認及適當的參考。

3.6 嵌入數個數位浮水印

我們可利用先前數位浮水印的架構，同時嵌入數個浮水印於一影像圖形中。其示意圖如圖(七)。在此實驗中，我們以嵌入兩個

壓縮率 compression ratio	JPEG image 的 PSNR	偵測浮水印的 Correlation	浮水印的 Error points	擷取之 數位浮水印
8.9:1	36.69	0.968	0	
14.5:1	34.73	0.883	21	
21.9:1	32.72	0.706	129	
32.5:1	30.27	0.411	274	
70.8:1	17.94	0.041	344	

表(三) JPEG 失真壓縮攻擊下，數位浮水印在 LH_3 波段的表現



圖(七) 嵌入數個數位浮水印於影像圖形之示意

數位浮水印作為測試；同樣地對影像在未受攻擊、**Resizing** 攻擊以及 **JPEG** 失真壓縮攻擊下，進行實驗。在影像未受攻擊的情況下，數位浮水印皆能正確無誤地被辨識出來，而不會互相影響；在 **Resizing** 的攻擊下(表六)，由於兩浮水印選擇嵌入的波段不同，而會有不同的反應程度顯現：選擇嵌入於較內層的波段，其反應會比嵌入於外層的好，且影像的 **PSNR** 也較高，反應出較佳的影像品質。

在 **JPEG** 的攻擊中(表七)，我們選擇嵌入兩數位浮水印於 **LH₂**與 **LH₃**波段作為說明：在壓縮率低時，所擷取之兩浮水印可清楚辨識；當資料壓縮超過約 15:1，對於浮水印在視覺上才會造成顯著的影響。

4. 結論

具可辨識能力的數位浮水印，對所有權的確認，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

浮水印 嵌入波段	可達到的 壓縮率	JPEG image 的 PSNR	偵測浮水印的 Correlation	浮水印的 Error points	擷取之 數位浮水印
HH ₁	1.6:1	55.72	0.986	0	蔡銘光
LH ₁	2.9:1	43.50	0.927	7	蔡銘光
HL ₁	5.8:1	39.10	0.879	21	蔡銘光
HH ₂	6.9:1	38.28	0.81	43	蔡銘光
LH ₂	12.5:1	35.59	0.851	33	蔡銘光
HL ₂	15.7:1	34.35	0.849	36	蔡銘光
HH ₃	13.4:1	35.14	0.846	35	蔡銘光
LH ₃	17.3:1	33.95	0.823	47	蔡銘光
HL ₃	25.9:1	31.43	0.842	48	蔡銘光

表(四) 在可辨識條件限制下，**JPEG**失真壓縮攻擊下，數位浮水印在不同波段的表現

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，可提供進一步的版權證據。而增加浮水印辨別的能力，可藉由在影像資料中，同時加入數個數位浮水印來達成。本文章的實驗，證明在有限度的破壞攻擊下，具可辨識能力的數位影像浮水印，對資訊安全及隱私，提供所有權辨認的不可否認性，及更強的驗證能力。

5. 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] 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.
- [6] X. -G. Xia, C.G. Boncelet and G. R. Arce, "A Multiresolution Watermark for Digital Images", IEEE ICIP97, vol.1, June 1997.
- [7] W. Zhu, Z. Xiong, and Y. -Q. Zhang, "Multiresolution watermarking for images and video: A unified approach", IEEE ICIP98, vol. 1, October 1998.
- [8] R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images", IEEE ICIP98, vol. 2, October 1998.
- [9] Chiou-Ting Hsu, and Ja-Ling Wu, "Hidden Digital Watermarks in Images", IEEE Transactions on Image Processing, vol. 8, January 1999.

嵌入波段	攻擊前圖形的 PSNR	攻擊後圖形的 PSNR	偵測浮水印的 Correlation	浮水印的 Error Points	擷取之數位浮水印
HH ₁	60.91	63.60	0.663	132	
LH ₁	57.35	60.25	0.670	129	
HL ₁	52.35	55.74	0.679	132	
HH ₂	50.96	53.46	0.714	113	
LH ₂	49.38	52.18	0.708	126	
HL ₂	44.87	48.29	0.669	138	
HH ₃	45.71	48.53	0.641	180	
LH ₃	45.79	49.21	0.619	169	
HL ₃	41.12	45.19	0.596	199	

表(五) Cropping 攻擊下，數位浮水印在不同波段的表現

選定之嵌入波段		Resizing image 的 PSNR	浮水印 1 的 相關程度	浮水印 2 的 相關程度	浮水印 1 的 Error points	浮水印 2 的 Error points	擷取之 浮水印 1	擷取之 浮水印 2
浮水印 1	浮水印 2							
HH ₁	LH ₁	31.53	0.025	0.041	262	314		
LH ₁	HH ₂	31.49	-0.005	0.093	293	79		
HL ₁	LH ₃	31.39	0.031	0.931	303	26		
HH ₂	HL ₂	31.33	0.901	0.947	66	20		
LH ₂	LH ₃	31.33	0.948	0.969	24	2		
LH ₃	HL ₃	30.98	0.965	0.977	2	2		

表(六) 嵌入兩數位浮水印於選定的波段，在 Resizing 攻擊下的表現

壓縮率	JPEG image 的 PSNR	浮水印 1 的 相關程度	浮水印 2 的 相關程度	浮水印 1 的 Error points	浮水印 2 的 Error points	擷取之 浮水印 1	擷取之 浮水印 2
4.4:1	39.15	0.988	0.994	0	0		
10.9:1	35.76	0.880	0.941	18	3		
14.6:1	34.61	0.798	0.860	61	36		
22.1:1	32.65	0.554	0.672	179	134		
32.6:1	30.22	0.374	0.419	255	265		
70.8:1	17.95	-0.021	-0.013	360	390		

表(七) 嵌入數位浮水印 1 於 LH₂ 波段、嵌入數位浮水印 2 於 LH₃ 波段，
在 JPEG 失真壓縮攻擊下的表現