

以小波轉換與灰階浮水印為基礎的所有權保護方法

Wavelet-Based Ownership Protection Scheme for Gray-Level Watermarks

許慶昇

銘傳大學資訊管理系

cshsu@mcu.edu.tw

李奕煌

銘傳大學資訊管理系

pilicatmax@gmail.com

摘要

隨著科技的進步，許多影像檔案均已透過數位化而成為數位影像。由於數位影像具備容易複製及散佈的特性，因此常常衍生出數位影像智慧財產權的爭議問題。為了解決此問題，近年來許多數位浮水印機制相繼被提出，其作法就是在數位影像之中，藏入足以辨識影像所有權的數位訊號。本文中將提出一個以小波轉換為基礎的灰階數位浮水印機制，為了提升浮水印的強韌性，我們將浮水印的灰階值轉換為三種不同重要性的位元，並以不同的方法將此三種位元藏入原始影像中，使較重要的位元資料能得到較佳的保護，而影像的破壞程度則控制在人眼所無法察覺的狀態之下。由實驗結果顯示，本研究所提出的方法對於一些常見的影像攻擊具有相當程度的強韌性。

關鍵詞：數位浮水印、離散小波轉換、著作權保護

Abstract

With the explosive growth of digital technologies, more and more images are transformed into digital formats. Therefore, it is very easy to duplicate or distribute digital images in an unauthorized manner. Recently, more and more watermarking

schemes are proposed to protect intellectual property rights of digital images. However, only a few of them take into account the issue of gray-level watermarks. This paper proposes an ownership protection scheme based on discrete wavelet transformation (DWT) for gray-level watermarks. To embed a gray-level watermark, we distinguish the gray-levels of the watermark into three kinds of bits according to their importance levels, and embed them into the original image by different methods. Thus, we can increase the survival rate of significant bits under attacks. In addition, the scheme requires neither the original watermark nor the original image during the ownership identification phase. Experimental results show that our scheme can resist many common attacks.

keywords : digital watermarking, discrete wavelet transformation, copyright protection

一、簡介

隨著科技的進步，許多影像檔案均已透過數位化而成為數位影像。除了能永久保存檔案之外，數位影像最大的特色在於能輕易地複製或散佈。數位化後的影像檔

案具備了許多一般傳統影像檔案所沒有的優點。因此，數位影像已逐漸取代了一般傳統影像而成為現今社會的主流。但是，在複製數位影像的過程之中，往往會牽涉到數位影像的智慧財產權爭議。因此，如何能在不破壞數位影像的原貌的前提下，進而保護影像的智慧財產權乃是目前急需解決的議題。

解決數位影像智慧財產權問題的方法之一，就是數位浮水印機制。所謂的數位浮水印機制，就是利用特定的方法將足以代表影像所有權的數位浮水印藏入數位影像之中，若之後遇到版權、所有權的爭議時，則可取出藏在影像之中的數位浮水印，進而驗證數位影像的所有權。一般來說，藏入影像中的數位浮水印可以分成兩大類[4]：

1、 虛 擬 隨 機 亂 數 (Pseudo-Random Gaussian Sequence)

此類型的數位浮水印是利用一個虛擬隨機亂數種子產生一連串數字，而該串數字是由 1 與 -1 所組成。以此類型的浮水印藏入影像後，日後若要從影像中取出浮水印以驗證影像所有權時，取出的浮水印需要與原始的浮水印進行比對並利用原始浮水印與取出的浮水印兩者之間的相似度進而驗證該數位影像的所有權。

2、 影 像 式 浮 水 印 (Binary Image or Gray Scale Image Watermarks)

此類型的數位浮水印通常是一張具有意義的影像，由於影像本身即具備辨識數位影像所有權的相關資訊，因此，此類型的浮水印藏入影像後，日後若遇到所有權的爭議時，即可利用取出的數位浮水印證明該影像的所有權。

數位浮水印機制乃是利用藏在數位影像之中的數位浮水印進而驗證影像的所有權，而一個有效的數位浮水印應具備不易

察覺性(imperceptibility)、強韌性(robustness)及明確性(unambiguousness) [1]。

藏入數位浮水印的方法可以分成兩大類，一種是藉由直接調整數位影像的像素值(Pixel)來藏入浮水印的空間域(Spatial Domain)的方法，另一種則是利用特定的數學公式將數位影像的像素值轉換成頻率域係數，再藉由修改該係數以藏入數位浮水印的頻率域(Frequency Domain)的方法。而常見的轉換方式有「快速傅利葉轉換(Fast Fourier Transformation, FFT)」、「離散餘弦轉換(Discrete Cosine Transformation, DCT)」與「離散小波轉換(Discrete Wavelet Transformation, DWT)」等。

近年來，以離散小波轉換為基礎的數位浮水印機制已被廣泛地討論。一張原始影像經過離散小波轉換後可以區分出低頻帶、中頻帶及高頻帶三種不同的頻帶係數，不同的頻帶代表著對影像不同的重要性，而修改不同的頻帶係數也會對影像造成不同的失真程度。低頻帶代表一張影像中最重要的部分，若將數位浮水印藏在低頻帶中，將會造成影像較大的失真程度，然而，藏在此頻帶的浮水印則具有較佳的強韌性；相反地，若將數位浮水印藏在高頻帶中，其對影像造成的失真程度較小，但其浮韌性也較為脆弱[10]。因此，為了能平衡對原始影像造成的失真程度及數位浮水印的強韌性，中頻帶通常是隱藏浮水印較佳的選擇[8]。

一般來說，數位浮印機制能依照取出浮水印所需的資訊的多寡，而分為私有的(private)、半私有的(semi-private)及公開的(public)浮水印架構[7]。在私有的浮水印架構裡，取出浮水印的過程中需要利用原始影像才能從取出浮水印，但是，由於在某些實際情況之中，原始影像的取得並不是相當方便，因此，需要原始影像才能取出

數位浮水印的架構是較不切合實際的應用情況[7]。

在 Tsai[3]一文中，提出了結合空間域與頻率域兩種方法的數位浮水印機制。數位浮水印在藏入原始影像中之前，先利用混沌擾亂法(Toral Automorphisms)將數位浮水印打亂，接者，再利用頻率域的方法將打亂後的數位浮水印藏入影像之中，而所謂的打亂數位浮水印所指的是將數位浮水印的座標重新排列。混沌擾亂法最大的特色在於經過固定的週期轉換後，可以將座標還原為原始座標。也就是說，假設週期大小為 T ，則原始座標 (x, y) 執行 T 次混沌擾亂法的運算後，就會原還到原始座標 (x, y) 。在藏入數位浮水印之前，先執行 t ($t < T$) 次的混沌擾亂法打亂數位浮水印，之後，若從一張藏有浮水印的影像中取出浮水印時，只需將取出的雜訊圖再執行 $(T-t)$ 次的運算即可將浮水印還原成具有義意的數位浮水印。

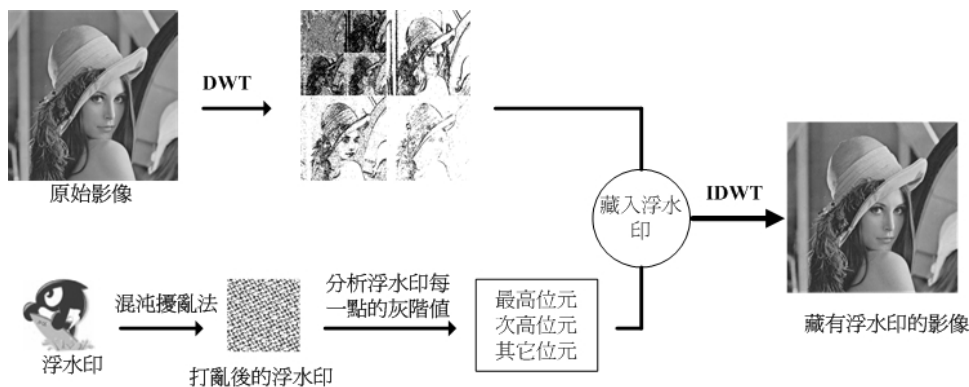
一般來說，影像式浮水印大多是以黑白影像為主，以灰階影像為浮水印的架構較為少見。在[9]一文中，原始影像與浮水印皆為一張灰階影像，其藏入的方法是先利用離散小波轉換將原始影像及灰階浮水印進行三階小波轉換，並區分出不同的頻率係數。接著，將浮水印的各頻帶之小波係數藏入相對應的原始影像之各頻帶之中。在浮水印的偵測過程中，該方法卻需

要利用原始影像及原始浮水印才能從影像之中取出浮水印。

在本研究中，我們的方法是以離散小波轉換為基礎並以灰階影像與灰階數位浮水印進行探討。為了取得影像失真程度與數位浮水印強韌性之間的平衡，我們將數位浮水印藏在離散小波係數的中頻帶，而在藏入數位浮水印之前，會先將浮水印座標重新排列、打亂。在藏入浮水印的過程中，由於我們藏入的是一張灰階數位浮水印，其每一點的灰階值是以八個位元所組成，且其每一位元的重要性均不同，因此，在藏入的過程中，我們將會針對不同重要性的位元採用不同的藏入方法，以期能確保較重要的位元能獲得較大的保護，進而增加浮水印的強韌性，而在浮水印的偵測過程中，我們的方法完全不需要利用原圖及原浮水印即可進行影像所有權的辨識。

二、 浮水印的隱藏

在本研究中，我們假設原圖及浮水印皆為灰階影像。為了能針對不同重要性的位元進行不同的隱藏方法，我們將浮水印每一個灰階值，區分成三種不同重要性的位元：最高位元、次高位元及其它位元。接著，再以不同的隱藏方法將此三種位元分別藏入影像中，其浮水印的隱藏流程如圖一所示。



圖一：浮水印隱藏流程

在藏入浮水印的過程中，我們以第三階的中頻帶(LH₃, HL₃)、第二階的中頻帶(LH₂, HL₂)以及另一個大小為四倍浮水印大小的面積為藏入的位置。為了能增加浮水印的安全性，在藏入浮水印之前，我們先執行 t 次的混沌擾亂法將浮水印影像座標重新排列、打亂。其公式如下[6]：

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

其中， k 為一個控制變數， N 為浮水印的長與寬， (x, y) 代表原始的座標，而 (x', y') 則代表轉換後的新座標。

在浮水印隱藏的過程中，不同重要性的位元會採用不同的隱藏方法。就最高位元而言，由於該位元是屬於最重要的位元，若此位元產生錯誤將會造成浮水印嚴重的失真。因此，為了能提升此位元的安全性，我們將此位元隱藏於第三階中頻帶HL₃及LH₃中。而在藏入最高位元的方法中，首先，在LH₃中選取一個小波係數 v_1 ，接著，在HL₃中選取另一個小波係數 v_2 ，接著，利用下列的演算法將浮水印藏入所選出的小波係數組合 (v_1, v_2) 之中。

Algorithm Embedding1(v_1, v_2, R)

```

 $f = |v_1| \bmod R$ 
 $r = |v_2| \bmod R$ 
 $\Delta(v_1) = v_1 - S(v_1) \times f$ 
 $\Delta(v_2) = v_2 - S(v_2) \times r$ 
if  $w==1$  then
     $f = (3 \times R) / 4$ 
     $r = R / 4$ 
else
     $f = R / 4$ 
     $r = (3 \times R) / 4$ 
 $v'_1 = \Delta(v_1) + S(v_1) \times f$ 

```

$$v'_2 = \Delta(v_2) + S(v_2) \times r$$

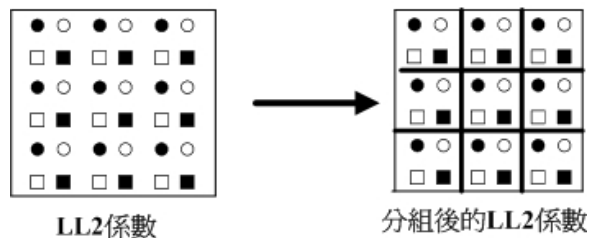
其中

$$S(v_i) = \begin{cases} 1 & \text{if } v_i \geq 0 \\ -1 & \text{otherwise} \end{cases}, i \in \{1, 2\}.$$

在上述的演算法中，首先，利用模數運算求出 v_1 及 v_2 除以 R 後的餘數 f 與 r ，並計算出 v_1 及 v_2 減去餘數後的 $\Delta(v_1)$ 及 $\Delta(v_2)$ 。接著，藉由最高位元判別 f 及 r 所要修改的數值。最後，將修改後的 f 與 r 計算出藏有浮水印後的小波係數 (v'_1, v'_2) 。

對次高位元而言，其重要性雖然不及最高位元來的重要，但其對數位浮水印的灰階值也有一定的影響力。因此，我們將次高位元隱藏在第二階中頻帶HL₂及LH₂中，而隱藏的方法如同藏入最高位元一般，是以 **Embedding1** 為藏入的方法。不同的是，所選取出來的係數組合 (v_1, v_2) 是在HL₂及LH₂兩個中頻帶所選取，且其修改的參數 R 也較最高位元來的小。

在其它位元的部分，我們先將剩餘的六個位元以兩兩為一組，並將每一組的位元轉換為介於0~3的十進位數值，也就是說，每一個灰階值的其它位元部分我們可以再分解成三個0~3的整數值。接著，將所選取的範圍裡的小波係數切割成不重疊的 2×2 區塊(如圖二)。



圖二：小波係數的切割圖

在隱藏其它位元的方法中，我們藉由修改[3]所提出的方法，使其能符合我們要藏入介於0至3之間的數值。在我們的方

法中，藉由增加第三個參數 T_3 使其在一定數值 S 之間產生四個區間，也就是 $0 \sim T_1$ 、 $T_1 \sim T_2$ 、 $T_2 \sim T_3$ 及 $T_3 \sim S$ ，各個區間分別代表 0 至 3 的整數。接著，在各個 2×2 的區塊中以 K 為一虛擬隨機亂數種子，並隨機挑選出三個小波係數，並分別以 **Embedding2** 將三整數藏入影像中。

Algorithm Embedding2(v, S)

```

 $f = |v| \bmod S$ 
 $\Delta(v) = v - S(v) \times f$ 
if  $w == 0$  then
     $f = \frac{T_1}{2}$ 
else if  $w == 1$  then
     $f = \frac{(T_1 + T_2)}{2}$ 
else if  $w == 2$  then
     $f = \frac{(T_2 + T_3)}{2}$ 
else
     $f = \frac{(T_3 + S)}{2}$ 
 $v' = \Delta(v) + S(v_1) \times f$ 

```

其中，

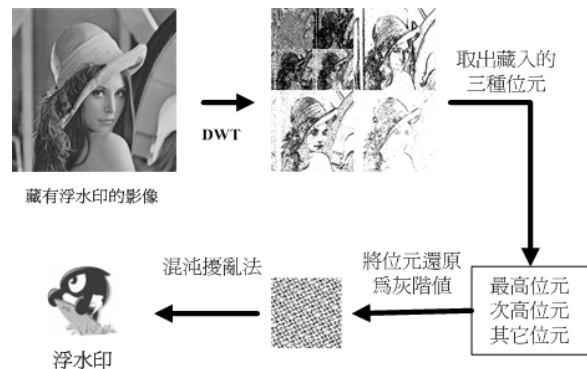
$$S(v_i) = \begin{cases} 1 & \text{if } v_i \geq 0 \\ -1 & \text{otherwise} \end{cases}, i \in \{1, 2\}.$$

在上述的演算法中，首先以模數運算求出小波係數除以參數 S 後的餘數： f ，並計算出其小波係數減掉餘數後的值 $\Delta(v)$ ，接著，利用調整 f 以藏入我們要藏入的整數。在各區間中，其中間位置的安全性最好[5]，因此，藉由要藏入的整數，進而修改 f 到代表該整數的區間，並將之修改為此區間的中間位置，以期獲得較佳的安全性。最後，利用修改過的 f 與調整後的小波係數 $\Delta(v)$ 進行運算，以計算出藏有浮水印的小波係數 v' 。演算法中 T_1 、 T_2 及 T_3

分別代表 $S/4$ 、 $S/2$ 及 $3S/4$ 。

三、 浮水印的偵測

浮水印的偵測流程如圖三所示，而在取出浮水印的過程中，所需的資訊有： k 、 t 、 R 、 S 及 K 。由於藏入浮水印時，是以不同的方法藏入不同重要性的位元，因此，在取出浮水印時，首先要先依不同的方法取出三種不同的位元，接著，利用各別的方法取出最高位元、次高位元及三個代表其它位元的三個整數，並依其順序重新還原為灰階值，最後，再利用混沌擾亂法將浮水印重新還原。



圖三：浮水印的偵測流程

在取出浮水印時，最高位元及次高位元是以 **Extracting1** 演算法取出。在此方法中，首先利用模數運算求出 v'_1 及 v'_2 除以 R 後的餘數 f 及 r' ，接著，根據 f 及 r' 兩者之間的大小判斷藏入的最高位元或次高位元的值為 1 或 0。

Algorithm Extracting1(v'_1, v'_2, R)

```

 $f = |v'_1| \bmod R$ 
 $r' = |v'_2| \bmod R$ 
if  $f \geq r'$  then
     $w' = 1$ 
else
     $w' = 0$ 

```

在其它位元的部分中，要取出所藏入的三個整數則是以 **Extracting2** 取出。在演算法中，首先利用模數運算求出餘數 f' ，接著，藉由判斷 f' 所在的區間進而判斷所藏入整數為何。最後，我們先將代表其它位元的三個整數分別轉換為兩兩一組的位元組，然後，再依相同的順序將最高位元、次高位元及三組位元組重新組合並轉換成灰階值。為了還原浮水印的位置，我們再利用原來的 k 及 t 執行混沌擾亂法($T-t$)次，將打亂的浮水印還原為原始的浮水印。

Algorithm Extracting2(v', S)

```

 $f' = |v'| \bmod S$ 
if  $f' \geq T_1$  then
     $w' = 0$ 
else if  $f' > T_1$  and  $f' \leq T_2$  then
     $w' = 1$ 
else if  $f' > T_2$  and  $f' \leq T_3$  then
     $w' = 2$ 
else
     $w' = 3$ 

```

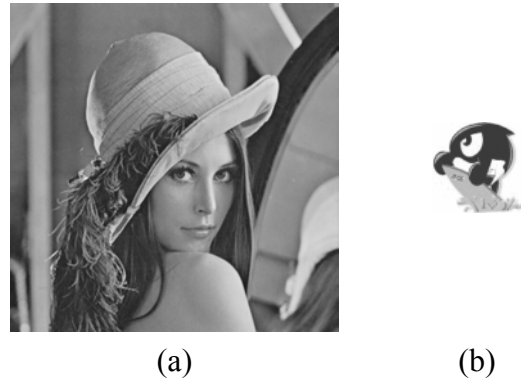
四、 結果與討論

在我們研究中，我們以 *PSNR* (Peak Signal to Noise Ration)來衡量藏入浮水印後的影像品質，其公式如下，其中 $X_{i,j}$ 表示原始影像中的像素值，而 $X'_{i,j}$ 則表示藏入浮水印後的影像像素值， m 與 n 則分別代表影像的寬與長。

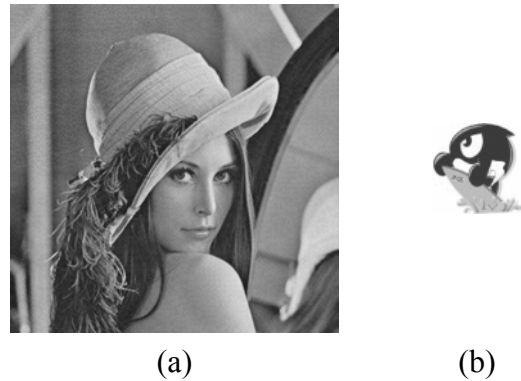
$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{ (dB)} \quad (2)$$

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (X_{i,j} - X'_{i,j})^2 \quad (3)$$

在本研究中，我們分別以一張 512×512 pixels(圖四(a))及一張 64×64 pixels 的灰階影像作為原圖及浮水印(圖四(b))，並利用 PhotoImpact 12 做為模擬影像攻擊的工具。在未受任何影像攻擊之前，藏入浮水印的影像如圖五(a)所示，其 *PSNR* 值為 35.73，取出的浮水印如圖五(b)所示。在接下來的實驗中，我們將會針對下列幾種影像攻擊進行浮水印強韌性的探討：



圖四: (a)原始影像；(b)浮水印









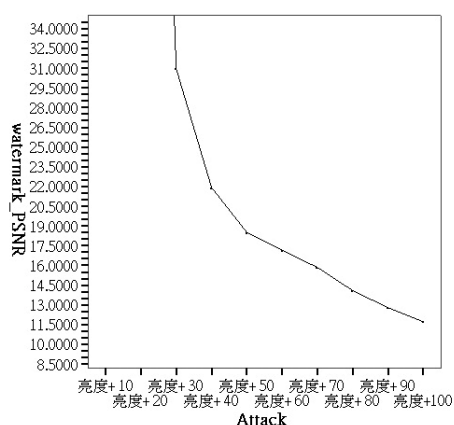
圖五: (a)藏有浮水印影像；(b)取出的浮印

1. 亮度改變

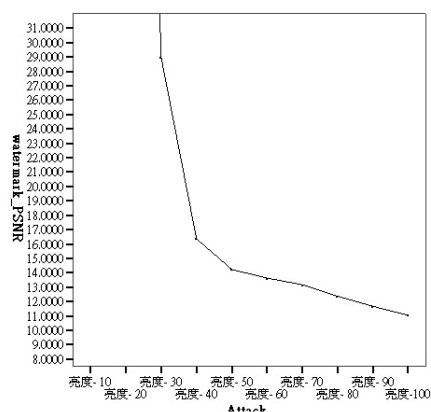
亮度改變的實驗結果如表一、圖六與圖七所示。由實驗結果可以，在我們的方法中，即使面對亮度調整的最大化攻擊，取出的浮水印依然清晰可見，因此，我們的方法中面對亮度改變的攻擊具有相當的強韌性。

表一：亮度改變後的實驗結果表

亮度 改變	影像的 PSNR	取出的 浮水印	亮度 改變	影像的 PSNR	取出的 浮水印	亮度 改變	影像的 PSNR	取出的 浮水印
+100	7.03		+50	12.16		+10	26.38	
-10	25.75		-50	12.20		-100	7.38	



圖六：變亮攻擊的實驗結果








圖七：變暗攻擊的實驗結果

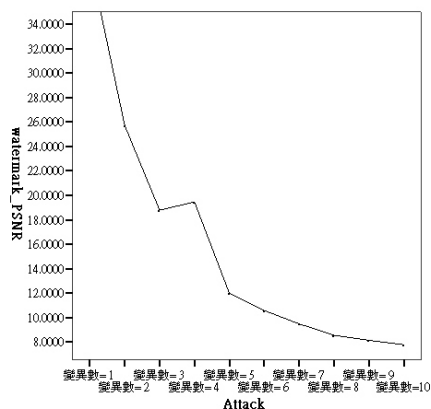
2. 加雜點

利用 PhotoImpact 12 可以在影像之中加入雜點，而可調整的參數是以變異數為主。在此實驗中，我們進行了變異數範圍

為 1 至 10 的攻擊。其實驗結果如表二及圖八所示。就實驗結果來看，變異數的值設定在 5 以下所取出的浮水印都依然是清晰可見。

表二：加雜點後的實驗結果表

變異數	影像的 PSNR	取出的浮水印
1	35.55	
3	34.10	
5	32.04	
7	30.11	
10	27.60	








圖八：加雜點後的實驗結果

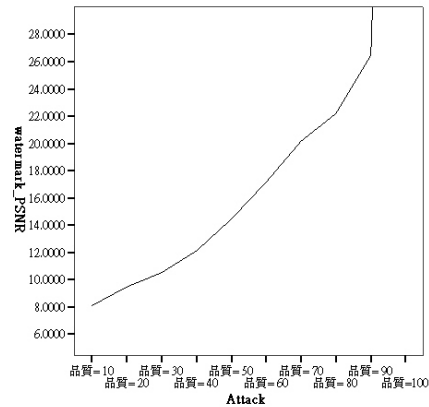
3. JPEG 壓縮

由實驗結果(表三及圖九)可知，即使將壓縮品質降為 50 後，取出的浮水印依然

可以辨識。因此我們的方法對 JPEG 壓縮的攻擊是具備相當不錯的抵抗力。

表三： JPEG 壓縮的實驗結果表

品質	影像的 PSNR	取出的浮水印
100	35.71	
80	35.00	
50	34.07	
30	33.41	
20	32.44	








圖九： JPEG 壓縮的實驗結果

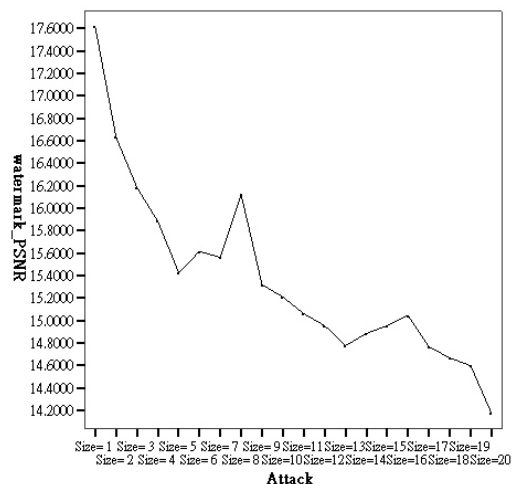
4. Jitter Attack

在本實驗中，我們是以(50, 0)的位置為起點座標，將寬度為 20 個像素的一行從起點座標抽出，再將之插入起點座標為

(100, 0)的位置。由實驗結果(表四及圖十)得知，我們的方法對於 Jitter Attack 的攻擊，具備相當程度的強韌性。

表四： Jitter Attack 的實驗結果表

寬度	影像的 PSNR	取出的浮水印
20	22.17	
15	22.52	
10	23.62	
5	26.20	
1	32.12	












圖十： Jitter Attack 的實驗結果

5. 其它攻擊

表五為其它影像攻擊情況之下的實驗結果。在改變大小的影像攻擊中，取出的浮水印雖然可以大致看出其原始浮水印的外貌，但其影像並不是相當地清晰。因此，我們的方法在目前的參數設定下，對改變大小的影像攻擊僅有較脆弱的抵抗力。在模糊攻擊中，其模糊程度可區分為弱、中及強，就實驗結果而言，取出的浮水印依然清晰可見，因此，本研究的方法

對於模糊攻擊是具備一定程度的強韌性。最後，在影像剪裁的攻擊中，為了能測試我們的方法能抵抗剪裁的攻擊，因此，我們將剪裁的範圍擴大到影像的一半，也就是說，我們會分別剪裁掉影像的上半部、下半部、左半部及右半部。由實驗結果可知，即使影像被剪裁掉一半，本研究的方法依然能取出浮水印，且能明確地看出浮水印的原貌。因此，在我們的方法中，其抵抗影像剪裁攻擊的效果相當不錯。

表五： 其它攻擊的實驗結果表

影像攻擊	影像 PSNR 值	取出的浮水印	影像攻擊	影像 PSNR 值	取出的浮水印
改變大小 256 × 256	33.54		剪裁 上	8.60	
改變大小 128 × 128	28.31		剪裁 下	9.24	
模糊 弱	37.50		剪裁 左	9.91	
模糊 中	35.95		剪裁 右	8.09	
模糊 強	32.73				

五、 結論

在本研究中，我們提出一個以離散小波轉換為基礎的灰階數位浮水印機制，在藏入灰階浮水印的過程中，我們會依其位元的重要性進而以不同的方法藏入原始影像之中，以期能盡可能提昇較重要的位元的強韌性，進而提升浮水印的強韌性，而且藏入浮水印後對影像所造成的破壞程度是人眼所無法察覺的。在取出浮水印的過程中，我們的方法完全不需利用原始影像即可成功取出浮水印。由實驗結果得知，本研究的方法對於調整亮度、影像模糊、

影像剪裁、JPEG 失真壓縮及 Jitter Attack 等影像攻擊是具備相當不錯的抵抗力。

致謝

本研究係由國家科學委員會工程處專題研究計畫經費補助。專題研究計畫編號：NSC 96-2221-E-130-018。

參考文獻

- 1、Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T., "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, Vol. 6, pp.1673-1687, 1997.
- 2、Kutter, M. and Petitcolas, F.A.P., "Fair benchmark for image watermarking systems," *Proceedings of SPIE - The International Society for Optical Engineering*, Vol. 3657, pp.226-239, 1999.
- 3、Tsai, M.-J., Yu, K.-Y., and Chen, Y.-Z., "Joint wavelet and spatial transformation for digital watermarking," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp.241-245, 2000.
- 4、Potdar, V.M., Han, S., and Chang, E., "A survey of digital image watermarking techniques," *IEEE International Conference on Industrial Informatics*, pp.709-716, 2005.
- 5、Tsai, M.-J. and Hung, H.-Y., "Wavelet transform based digital watermarking for image authentication," *Fourth Annual ACIS International Conference on Computer and Information Science*, pp. 408-411, 2005.
- 6、Voyatzis, G. and Pitas, I., "Applications of toral automorphisms in image watermarking," *International Conference on Image Processing*, Vol. 2, pp 237-240. 1996.
- 7、Wang, Y.-L. and Pearmain, A., "Blind image data hiding based on self reference," *Pattern Recognition Letters*, Vol. 25, No. 15, pp.1681-1689, 2004.
- 8、Wu, G.-D. and Huang, P.-H., "Image Watermarking Using Structure Based Wavelet Tree Quantization," *IEEE/ACIS International Conference on Computer and Information Science*, pp. 315-319, 2007.
- 9、Niu, X.-M., Lu, Z.-M. and Sun, S.-H., "Digital image watermarking based on multiresolution decomposition," *Electronics Letters*, Vol. 36, No. 13, pp.1108-1110, 2000.
- 10、Hu, Y.-P. and Han, D.-Z., "Wavelet -based readable watermarking algorithm using adaptive quantization," *International Conference on Machine Learning and Cybernetics*, Vol. 7, pp. 4076-4080, 2004.