

行政院國家科學委員會專題研究計畫 成果報告

頻域上應用人類視覺系統之適應性影像浮水印技術

計畫類別：個別型計畫

計畫編號：NSC94-2622-E-029-005-CC3

執行期間：94年05月01日至95年04月30日

執行單位：東海大學資訊工程與科學系

計畫主持人：林正基

共同主持人：蔡清欉

計畫參與人員：柯朝輝、林家福

報告類型：精簡報告

處理方式：本計畫為提升產業技術及人才培育研究計畫，不提供公開查詢

中 華 民 國 95 年 6 月 12 日

國科會補助提升產業技術及人才培育研究計畫成果報告

頻域上應用人類視覺系統之適應性影像浮水印技術

計畫編號：NSC 94-2622-E-029-005-CC3

執行期限：94年5月1日至95年4月30日

主持人 ： 林正基 東海大學資訊工程與科學系講師
共同主持人 ： 蔡清欉 東海大學資訊工程與科學系副教授

一、中文摘要

由於網際網路的普及，使用者可以透過網路輕易取得這些數位資料並加以修改，使得資料擁有者的著作權受到很大的威脅。為了保護網路多媒體的智慧財產權，一種能將版權宣告訊息藏入多媒體資料中的版權保護機制數位浮水印便應運而生。

本文針對頻域嵌入技術來探討，頻域的嵌入技術雖然強健性 (robustness) 較高但是較難評估是否合乎隱藏性 (imperceptibility) 的要求。本文嘗試克服上述困難，所提出的作法是利用人類視覺系統的特性估測的恰可視誤差 (just noticeable distortion, JND) 值作為影像中灰階值可以承受的最大修改量。如此將經模擬攻擊後的影像映至頻域藉以獲得頻域係數的變化量，並依此作為嵌入浮水印資訊量的最大強度。而選擇嵌入浮水印之頻域係數是依據頻率位置、係數值及加入資訊量的多寡三個因素。此外，我們考慮影像性質將影像分割成互不相重疊的影像區塊，然後根據區塊分類不同的特性來決定頻域係數嵌入浮水印時符合該區塊之最大隱藏的資訊量，藉以提高浮水印的強健性。

總而言之，本論文將人類視覺系統的特性應用到頻域來，而且能確保嵌入的浮水印在空間域中是不可見的。此外，並提出位置強度模型使嵌入的浮水印具有高度的強健性可以抵抗人為的攻擊破壞。根據實驗的結果顯示，本文所提出的浮水印系統具有高度的強健性，它能抵抗 JPEG 壓縮、部份影像擷取、雜訊、模糊等各類訊號處理的攻擊。

關鍵詞：數位浮水印，人類視覺系統，離散餘弦轉換，恰可視誤差，智慧財產權保

護

Abstract

Due to the prevalence of Internet, the various information is digitizing rapidly and can be accessed easily. Users can reproduce and manipulate these digital data without granting appropriate credit to the owner. How to protect data is one the important issue they should face. One promising solution for the copyright protection of digital images is a so-called watermarking technique. The watermarking technique can hide an invisible signature or code in digital image to indicate the image owner or recipient.

Although the frequency domain techniques can provide more efficient and robust method, it is difficult for them to evaluate the requirement of imperceptibility. For the purpose of overcoming above-mentioned objection, we adopt the method of simulating attack to simulate signal-processing operations that modify the grayscale value of the image in spatial domain. Because of the imperceptible limitation, we use a just-noticeable distortion (JND) based on human visual model in spatial domain to check out the maximal intensity of simulating attack. Thus the image operated by simulating attack is transformed to the frequency domain and is able to obtain the change of amount for each frequency component. The choice of embedding the watermark into DCT coefficient is exactly depended on the three factors - the frequency position, the

magnitude of DCT coefficient and the amount of embedding information. Besides, we should consider the existence of the image content features, and then we divide the image into non-overlapped blocks. According to the block content analysis, we can decide the maximal amount of embedding information to enhance the robustness.

In summary, our watermarking scheme applies human visual system to frequency domain and makes sure that embedded watermark into images is invisible in spatial domain. Besides, we propose the location strength model to make the embedded watermark high in robustness to resist artificial attacks. Experiment results show that the proposed scheme provides good performance of robustness against image processing attacks such as JPEG compression, cropping, adding noise and blurring.

Keywords: digital watermark, human visual system, Discrete Cosine Transform, Just-Noticeable-Distortion, copyright protection

二、緣由與目的

近年來，由於網際網路的蓬勃發展，加速了多媒體資料數位化的趨勢。數位化的優點就是資料傳輸與複製非常地方便，使用者可以透過網路輕易取得這些數位資料；但相對的不管合法與不合法，任何人都可以輕易地複製、散播這些數位資訊，甚至將數位資訊加以修改，然後宣稱是自

己的資料以進行圖利的商業行為。這種隨著數位化趨勢所帶來的問題，使得資料擁有者的著作權受到很大的威脅，造成許多人對於將自己的數位作品公開散佈裹足不前，阻礙了數位媒體的發展。因此，為了保護智慧財產權，讓數位資料的版權擁有者放心地將他的作品公開地散佈，一種良好的版權保護機制是迫切需要的。在現實生活中，人們通常在其作品上以蓋章、簽名或浮水印的方式來宣告其擁有權，因此有人想到是否可以利用相同的方式將其簽名加入數位資料中，於是便發展出數位浮水印的技術。通常在現實世界中浮水印大都屬於可見的，但數位化的浮水印卻分為可見與不可見兩種。以可見的浮水印加註資料可讓使用者可以很清楚知道版權擁有者屬誰，以防止使用者挪用於其他用途，但是由於浮水印是清晰可見的所以會破壞影像的品質。不可見的浮水印它應用了資料隱藏的觀念，利用特殊的演算法將版權訊息嵌入數位資料上，又不影響數位資料的品質，一但發生版權爭議時，只有資料的擁有者才能偵測並將浮水印顯現出來，以證明其為資料合法的擁有者。由於不可見的浮水印具有保持原始數位資料品質的特性，所以目前浮水印的技術大都趨向於不可見的浮水印為研究目標。

一個有效而且不可見的浮水印技術必須滿足下列的基本需求[1, 2]：(1) 隱藏性 (imperceptibility) (2) 強健性 (robustness) (3) 安全性 (security) (4) 容量性 (capacity) (5) 明確性 (unambiguity)。目前的浮水印技術依其嵌入浮水印的方式來看可以分為兩大類，一類屬於在空間域上[5-8, 19-23]嵌入浮水印，此法係直接修改影像中的像素值來達成嵌入浮水印的目的。這類方法的優點容易將人類視覺系統的特性應用於嵌入的

技術上，因此易於估量嵌入後的影像是否合乎隱藏性的要求。但較不容易抵抗各類訊號處理的破壞。另一類則是將浮水印加到頻域上[9-18]，此法是先將影像轉換(如離散餘弦轉換、小波轉換等)至頻域後，藉由改變轉換後所得的係數值來達到嵌入浮水印的目的。這種作法的優點可將加入的浮水印散佈在整張影像上，具有較佳抵抗訊號處理破壞的能力，但是需要大量的運算而且難以評估是否合乎浮水印的隱藏性。

由現有文獻的浮水印技術的研究中我們發現空間域的嵌入技術易於達到隱藏性的要求但是強健性不高，頻域的嵌入技術通常強健性較高但是較難評估是否合乎隱藏性的要求。本計畫結合了空間域和頻域浮水印的優點，為了提昇浮水印系統的強健性並同時兼顧隱藏性，就必須同時考慮到嵌入資訊量的多寡與嵌入位置的選擇，因此本計畫提出模擬攻擊的方式來得到離散餘弦轉換(DCT)頻域上可嵌入的最大資訊量且能保證嵌入的浮水印仍合乎類視覺系統之察覺性。前述之浮水印技術，對於嵌入位置的選擇大都侷限在低頻、中頻幾個固定位置或是選擇係數值較大的作為嵌入位置，並未對嵌入位置強健性作一整體性的分析。因此本計畫亦提出一個位置強度作為浮水印嵌入位置的選擇依據，此模型能從影像中挑選最合適嵌入浮水印的位置藉以增加浮水印之強健性。在使用區塊分類嵌入浮水印的做法，重新歸類四類的區塊分類法對嵌入資訊量以準確掌握，以求得每個分類所能放入最大資訊量。

總而言之，本計畫考慮人類視覺系統中的特性，來對影像品質及浮水印強健性之間的取捨，分別提出全新而有效的頻域浮水印嵌入方法，我們希冀計畫的執行與實驗結果能確實顯現其抵抗 JPEG 壓縮、

部份影像擷取、雜訊、模糊等各類訊號處理的攻擊能力。

三、研究方法與成果

通常浮水印系統的強健性必須同時考慮到嵌入資訊量的多寡與嵌入位置的選擇，而嵌入資訊量是直接影響到浮水印系統強健性與隱藏性的重要因素。嵌入資訊量過多則會嚴重影響影像的品質，反之嵌入太少的資訊量則會使浮水印容易被破壞。因此本章結合 Chou 等人[31] 在空間域上提出的 JND 模型，採用模擬攻擊的方式發展出在 DCT 頻域上新的 JND 模型。根據此模型所計算出的 JND 值，能將浮水印加在整張影像所有係數上且不會被人類視覺系統所察覺。此外，目前的浮水印技術中，對於嵌入位置的選擇大都侷限在低頻或中頻幾個固定位置或是選擇係數值較大的作為嵌入位置，並未對嵌入位置強健性作一整體性的分析，因此我們提出位置強健性模型作為浮水印嵌入位置的選擇依據。本章所提出的數位浮水印系統同時具有高度的強健性及隱藏性。下一節將介紹本浮水印系統所使用的技術。

3.1 模擬攻擊單元

本章所採用的模擬攻擊，主要是模擬訊號處理所造成影像內容的更改且在不造成影像可視的失真的前提下，預估影像的內容可以承受多大的修改量。我們的作法是在空間域中採用模擬非平衡攻擊的方式對原影像分別做類似負數攻擊與正數攻擊，然後將受攻擊後的影像經 DCT 轉換後所得係數值與原影像經 DCT 轉換後所得係數值相減，藉以求出每個係數值所能修改的資訊量(圖 3.1)。基於受模擬攻擊

後的影像與原影像品質的差異必須讓人類視覺系統無法察覺的限制下，因此我們利用空間域上 JND 模型所求得每個像素所能修改的 JND 值作為模擬攻擊的強度評估，以保證受模擬攻擊後所造成的影像失真是讓人類視覺系統無法察覺出來。模擬攻擊詳細介紹如下：

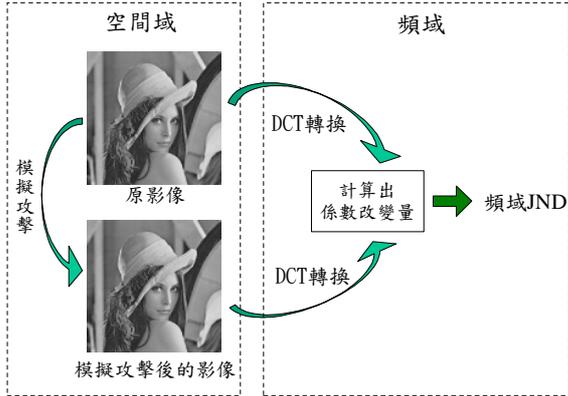


圖 3.1 頻域 JND 計算示意圖

3.1.1 模擬負數攻擊行為

首先將影像分割成互不相重疊 8×8 大小的影像區塊，並計算出每個區塊中像素灰階平均值 \bar{P}_j 及每個像素的 JND 值 $JND_j(x, y)$ ，其中 j 表示影像中第 j 個區塊。然後將每個區塊中的像素灰階值 $P_j(x, y)$ 向區塊像素灰階平均值 \bar{P}_j 做調整，這種調整方式類似對影像做模糊處理，因此可以用來模擬負數攻擊的行為，每個像素灰階值所能調整的最大資料量為 $JND_j^w(x, y)$ 但調整後的灰階值以不超過區塊灰階平均值 \bar{P}_j 為原則，其中 $JND_j^w(x, y)$ 是將原像素 JND 值 $JND_j(x, y)$ 乘上對應的加權因子 $WM(x, y)$ (圖 3.2) 所得。

也就是說，當像素灰階值 $P_j(x, y)$ 大於區塊灰階平均值 \bar{P}_j 則將像素灰階值

$P_j(x, y)$ 減去 $JND_j^w(x, y)$ 後，若所得之像素灰階值 A 小於區塊灰階平均值 \bar{P}_j 則受模擬攻擊後的像素灰階值 $P_j^-(x, y)$ 等於區塊灰階平均值 \bar{P}_j 反之 $P_j^-(x, y)$ 等於像素灰階值 A ；當 $P_j(x, y)$ 小於 \bar{P}_j 則將 $P_j(x, y)$ 加上 $JND_j^w(x, y)$ 後，若所得之值 A 大於 \bar{P}_j 則受模擬攻擊後 $P_j^-(x, y)$ 等於 \bar{P}_j 反之 $P_j^-(x, y)$ 等於 A ，式 (3.1) - (3.4) 為詳細運算式。

$$P_j^-(x, y) = \begin{cases} \max(A, \bar{P}_j), & \text{if } P_j(x, y) > \bar{P}_j \\ \min(A, \bar{P}_j), & \text{otherwise} \end{cases} \quad (3.1)$$

$$A = P_j(x, y) + B * JND_j^w(x, y) \quad (3.2)$$

$$B = \begin{cases} -1, & \text{if } P_j(x, y) > \bar{P}_j \\ +1, & \text{otherwise} \end{cases} \quad (3.3)$$

$$JND_j^w(x, y) = JND_j(x, y) * WM(x, y) \quad (3.4)$$

0.3	0.6	0.3	0.6	0.3	0.6	0.3	0.6
0.6	0.8	0.5	0.8	0.5	0.8	0.5	0.3
0.3	0.5	1	1	1	1	0.8	0.6
0.6	0.8	1	1	1	1	0.5	0.3
0.3	0.5	1	1	1	1	0.8	0.6
0.6	0.8	1	1	1	1	0.5	0.3
0.3	0.5	0.8	0.5	0.8	0.5	0.8	0.6
0.6	0.3	0.6	0.3	0.6	0.3	0.6	0.3

圖 3.2 加權因子 $WM(x, y)$ 。

3.1.2 模擬正數攻擊行為

相對的，模擬正數攻擊的行為是將每個像素值向區塊像素平均值反向做調整，這種調整方式類似對影像做加強對比的處理，因此可以用來模擬增加轉換後係數值的行為。其作法亦是先將影像分割成互不相重疊 8×8 大小的影像區塊，並計算

出每個區塊的像素灰階平均值 $\overline{P_j}$ 及每個像素的 JND 值 $JND_j(x, y)$ 。然後將每個區塊中的像素灰階值 $P_j(x, y)$ 向區塊像素灰階平均值 $\overline{P_j}$ 反向調整來模擬正數攻擊的行為，每個像素灰階值所能調整的最大資料量為 $JND_j^w(x, y)$ 但調整後的灰階值以不超過 0 或 255 原則。

也就是說，當像素灰階值 $P_j(x, y)$ 大於 $\overline{P_j}$ 則將像素灰階值 $P_j(x, y)$ 加上 $JND_j^w(x, y)$ 後作為受模擬攻擊後的像素灰階值 $P_j^+(x, y)$ ，但若像素灰階值 $P_j^+(x, y)$ 大於 255 則 $P_j^+(x, y)$ 為 255；當 $P_j(x, y)$ 小於 $\overline{P_j}$ 則將 $P_j(x, y)$ 減去 $JND_j^w(x, y)$ 後作為受模擬攻擊後的像素灰階值 $P_j^+(x, y)$ ，但若像素灰階值 $P_j^+(x, y)$ 小於 0 則 $P_j^+(x, y)$ 為 0，式 (3.5) - (3.7) 為詳細運算式。

$$P_j^+(x, y) = \begin{cases} \min(A, 255), & \text{if } P_j(x, y) > \overline{P_j} \\ \max(A, 0), & \text{otherwise} \end{cases} \quad (3.5)$$

$$A = P_j(x, y) + B * JND_j^w(x, y) \quad (3.6)$$

$$B = \begin{cases} +1, & \text{if } P_j(x, y) > \overline{P_j} \\ -1, & \text{otherwise} \end{cases} \quad (3.7)$$

此模擬攻擊方法，根據式 (3.8) 可保證修改的資訊量不會被人類視覺系統所察覺。

$$|P_j^*(x, y) - P_j(x, y)| \leq JND_j(x, y) \quad (3.8)$$

3.1.3 頻域 JND 計算單元

根據上一節將受模擬攻擊後的影像經 DCT 轉換後所得的係數值與原影像經 DCT 轉換後所得的係數值相減，來求得頻域上每個係數所能修改的資訊量，即

JND 值。(圖 3.3) 為計算 DCT 頻域 JND 值的流程圖。

也就是將受模擬負數攻擊後的影像經 DCT 轉換後所得的係數值 $c_j^-(u, v)$ 與原影像經 DCT 轉換後所得的係數值 $c_j(u, v)$ 相減取絕對值得到 $dctjnd_j^-(u, v)$ ，式 (3.9)。

$$dctjnd_j^-(u, v) = \text{abs}(c_j^-(u, v) - c_j(u, v)) \quad (3.9)$$

同時將受模擬正數攻擊後的影像經 DCT 轉換後所得的係數值 $c_j^+(u, v)$ 與原影像經 DCT 轉換後所得的係數值 $c_j(u, v)$ 相減取絕對值得到 $dctjnd_j^+(u, v)$ ，式 (3.10)。

$$dctjnd_j^+(u, v) = \text{abs}(c_j^+(u, v) - c_j(u, v)) \quad (3.10)$$

接著在 $dctjnd_j^+(u, v)$ 與 $dctjnd_j^-(u, v)$ 中取其最小值即為所求之頻域 JND 值 $dctjnd_j(u, v)$ ，式 (3.11)。

$$dctjnd_j(u, v) = \min(dctjnd_j^+(u, v) + dctjnd_j^-(u, v)) \quad (3.11)$$

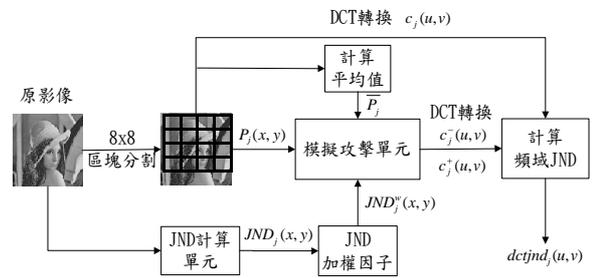


圖 3.3 頻域 JND 計算流程圖

3.2 位置強度模型

以往的研究中，對於嵌入浮水印位置的選擇並未做整體性的分析。他們對嵌

的大小為 2×2 的區塊 $w_j(x, y)$ ，其中 $j=1, 2, 3, \dots, 4096$ 、 $x, y=1, 2$ 。

步驟五：經式 (3.13) 浮水印強度模型選擇出要嵌入的位置。因為要將浮水印中每個 2×2 的區塊 $w_j(x, y)$ 嵌入 8×8 大小的影像區塊中，因此每個影像區塊有四個位置要嵌入浮水印，所以我們取浮水印強度值最大的前四個作為嵌入位置 (圖 3.6)。

步驟六：如果 $w_j(i) = 1$ 則根據式 (3.14) 修改加入浮水印的係數，否則依據式 (3.15) 修改對應的係數值。其中 $c_j(i)$ 表示經修改後的係數值。

$$c_j(i) = \begin{cases} \text{abs}(c_j(i)) + \text{dctjnd}_j(i) & \text{if } c_j(i) \geq 0 \\ (\text{abs}(c_j(i)) + \text{dctjnd}_j(i)) * -1 & \text{otherwise} \end{cases} \quad (3.14)$$

$$c_j(i) = \begin{cases} \text{abs}(c_j(i)) - \text{dctjnd}_j(i) & \text{if } c_j(i) \geq 0 \\ (\text{abs}(c_j(i)) - \text{dctjnd}_j(i)) * -1 & \text{otherwise} \end{cases} \quad (3.15)$$

步驟七：經 IDCT 轉換成加入浮水印後影像。

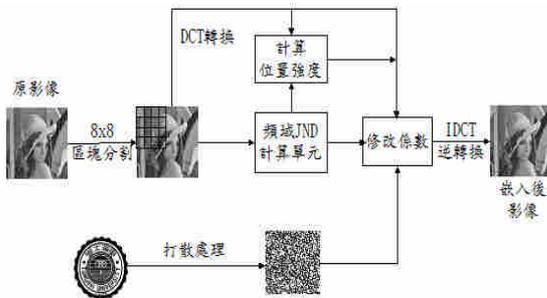


圖 3.5 浮水印的嵌入流程圖

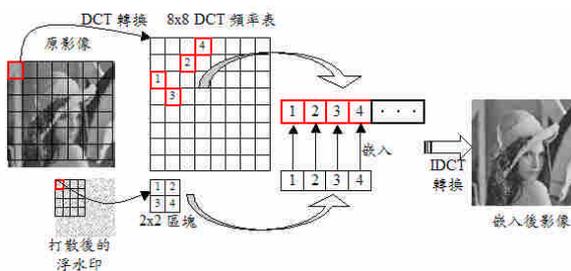


圖 3.6 浮水印的嵌入示意圖

我們用 512×512 的 Lena 影像作為測試影像嵌入東海校徽，東海校徽先經環型

曲線同構法打散成 128×128 的雜訊影像如圖 3.7，其中 $n=19, k=11, N=128$ ，加入浮水印後 Lena 影像的 PSNR 為 57.95 如圖 3.8 所示與原影像在品質上沒有什麼差異。

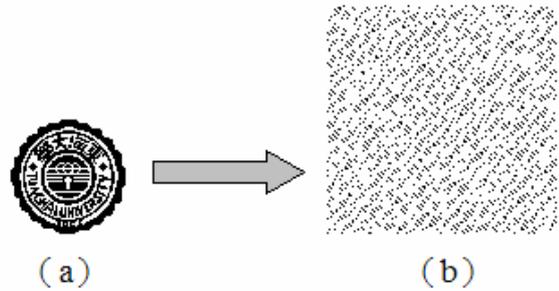


圖 3.7 (a)為東海校徽(b)東海校徽打散成 128×128

的雜訊影像



圖 3.8 (a) 為原 Lena 影像 (b) 為嵌入浮水印後 Lena 影像，其 PSNR 值為 57.95

3.4 取出浮水印演算法

(圖 3.9) 為浮水印取出流程，演算法描述如下：

輸入：受攻擊的影像。

輸出：浮水印。

演算法：

步驟一：同嵌入演算法的步驟一~步驟五，求得浮水印嵌入的位置。

步驟二：將受攻擊的影像經 DCT 轉換求得係數 $c_j^*(i)$ 。

步驟三：將原影像經 DCT 轉換求得係數 $c_j(i)$ 。

步驟四：將 $c_j^*(i)$ 與 $c_j(i)$ 相減，如果 $c_j(i) \geq 0$ 則根據式 (3.16) 來判斷浮水印的二元值，否則依據式 (3.17) 判斷之。

$$w_j(i) = \begin{cases} 1 & \text{if } c_j^*(i) - c_j(i) \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (3.16)$$

$$w_j(i) = \begin{cases} 1 & \text{if } \text{abs}(c_j^*(i)) - \text{abs}(c_j(i)) \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (3.17)$$

步驟五：經環型曲線同構法週期運算的性質還原浮水印。

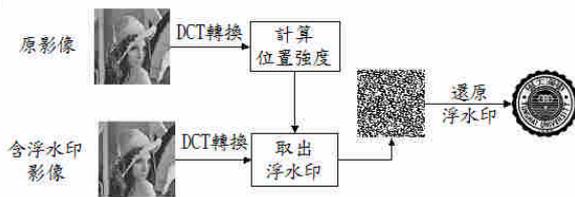


圖 3.9 浮水印的取出流程圖

3.5 基於區塊分類的浮水印技術

此節中我們改進了上面的作法，我們將影像先經區塊分類單元分成：平坦區塊 (plain)、邊緣區塊 (edge)、平滑區塊 (smooth) 及紋理區塊 (texture) 四類，然後根據區塊的特性，將模擬攻擊的方式所計算出的頻率 JND 值乘上對應的參數來決定嵌入的資訊量，藉以提高浮水印系統的強健性。

3.5.1 區塊分類

本章所採用區塊分類的方法是根據 [32] 的區塊分類的方法加以改良而來的。因為其使用 8×8 大小的影像區塊符合我們浮水印系統的影像分割方式，且他是針對區塊中係數的頻率位置及係數值的大小加以分析來分類區塊所以計算快速。其作法是先將區塊中的 64 個係數分成四區域，並將各區域的係數值取絕對值相加分別以 DC、L、E、H 表示，其中 L 表示低頻區塊位置，E 表示邊緣區塊位置，H 表

示高頻區塊位置。經其實驗證明， $\frac{L+E}{H}$

與 $\frac{L}{E}$ 的強度可用來決定邊緣區塊， $E+H$ 的大小可以用來決定紋理區塊。因此將其改進細分成平坦區塊、邊緣區塊、平滑區塊及紋理區塊四類。其流程圖如 (圖 3.10)。

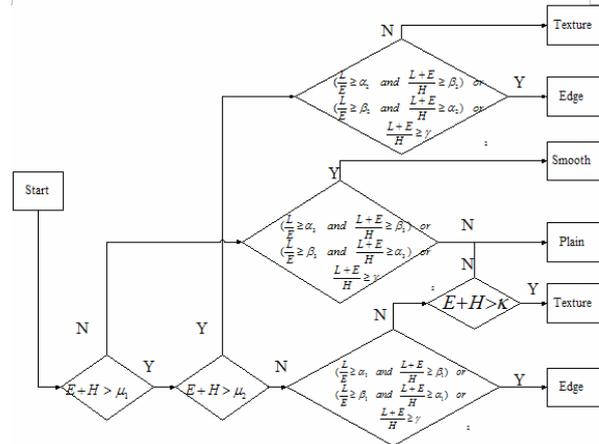


圖 3.10 區塊分類流程圖

3.5.2 重估可修改的資訊量

根據上一節區塊的特性分析，我們了解紋理區塊 區塊中每個係數所能修改的資訊量最多，而平滑區塊 區塊中每個係數所能修改的資訊量最少。因此我們將平坦區塊、邊緣區塊、平滑區塊及紋理區塊四類區塊中每個係數所對應的 JND 值，分別乘上 β_1 、 β_2 、 β_3 、 β_4 四種參數，來重新評估每個區塊係數修改的資訊量 (表 3.1)。根據實驗的分析 β_1 、 β_2 、 β_3 與 β_4 分別為 1.2、1.5、1 與 2 所產生的影像較為人類視覺系統所接受。

表 3.1 各類區塊係數修改的資訊量

紋理區塊	$mcoef_j(x, y) = 2 \times dctjnd_j(x, y)$
邊緣區塊	$mcoef_j(x, y) = 1.5 \times dctjnd_j(x, y)$
平坦區塊	$mcoef_j(x, y) = 1.2 \times dctjnd_j(x, y)$
平滑區塊	$mcoef_j(x, y) = 1 \times dctjnd_j(x, y)$

3.5.



DC

學自

海大
為數



L 表示低頻區塊位置



E 表示邊緣區塊位置

位浮水印，其大小為 64×64 的二元影像，嵌入的影像大小為 512×512 。圖 3.11 為浮水印的嵌入流程圖，演算法描述如下：

輸入：原始影像與浮水印。

輸出：嵌入浮水印的影像。

演算法：

步驟一：將原影像以 8×8 大小做非重疊的區塊分割，然後計算出每個區塊的像素平均值 $\overline{P_j}$ 及經 DCT 轉換的頻率係數值 $c_j(u, v)$ ，其中 $j=1,2,3,\dots,4096$ 、 $x,y,u,v=1,2,3,\dots,8$ 。

步驟二：利用空間域上 JND 計算模型，求得原影像中每個像素的 JND 值 $JND_j(x, y)$ ，其中 $x,y=1,2,3,\dots,8$ 。

步驟三：將每個區塊影像經模擬攻擊單元，求得頻域係數的 JND 值 $dctjnd_j(u, v)$ 。

步驟四：將原影像經過區塊分類單元分成平坦區塊、邊緣區塊、平滑區塊及紋理區塊，根據區塊的特性將 JND 值乘上表 3.1 相對應的參數求得係數可修改的資訊量 $mcoef_j(u, v)$ 。

步驟五：將 64×64 浮水印經環型曲線同構法打散成 128×128 的雜訊影像，並分割成同步驟一的影像區塊數目，在此分割的大小為 2×2 的區塊 $w_j(x, y)$ ，其中 $j=1,2,3,\dots,4096$ 、 $x,y=1,2$ 。

步驟六：經式 (3.13) 浮水印強度模型選擇出要嵌入的位置。因為要將浮水印中每個 2×2 的區塊 $w_j(x, y)$ 嵌入 8×8 大小的影像區塊中，因此每個影像區塊有四個位置要嵌入浮水印，所以我們取浮水印強度值最大的前四個作為嵌入位置。

步驟七：如果 $w_j(i) = 1$ 則根據式 (3.18) 修改加入浮水印的係數，否則依據式 (3.19) 修改對應的係數值。其中 $c_j(i)$

表示經修改後的係數值， $mcoef_j(i)$ 表示加入的資訊量。

$$c'_j(i) = \begin{cases} abs(c_j(i)) + mcoef_j(i) & \text{if } c_j(i) \geq 0 \\ (abs(c_j(i)) + mcoef_j(i)) * -1 & \text{otherwise} \end{cases} \quad (3.18)$$

$$c'_j(i) = \begin{cases} abs(c_j(i)) - mcoef_j(i) & \text{if } c_j(i) \geq 0 \\ (abs(c_j(i)) - mcoef_j(i)) * -1 & \text{otherwise} \end{cases} \quad (3.19)$$

步驟八：經 IDCT 轉換成加入浮水印後影像。

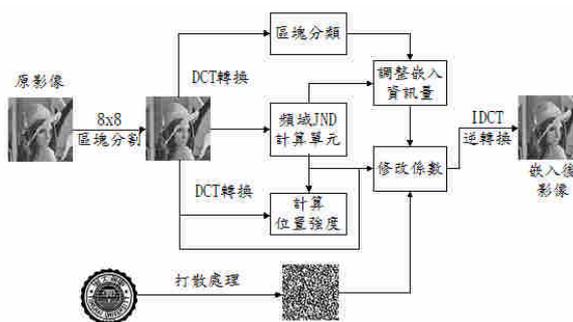


圖 3.11 浮水印的嵌入流程圖

3.5.4 取出浮水印演算法

取出浮水印演算法與本章 3.4 節相同。

四、實驗結果與討論

4.1 基於模擬攻擊的浮水印技術

我們對所加入的浮水印影像進行各類影像處理的攻擊破壞，來分析遭受各類影像處理攻擊後浮水印的存活率。各類影像處理的攻擊包含：JPEG 壓縮、模糊 (blurring)、銳化 (sharpening)、加入雜訊 (noise adding)、擷取 (cropping) 等攻擊。

4.1.1 JPEG 壓縮攻擊測試。

將嵌入東海校徽後的 Lena 影像經過不同壓縮品質的 JPEG 壓縮攻擊之後的測試結果如圖 4.1。由圖 4.1 中，壓縮品質為 50% 的壓縮攻擊下取出的浮水印其相似度 NC 值大約保持在 0.8，可以明顯的看出在壓縮品質 50% 以上的 JPEG 壓縮攻擊下幾乎對浮水印沒有影響。在壓縮品質

為 20%時，取出的浮水印 NC 值大約在 0.5 左右，我們依然可以辨識出浮水印。所以在較高壓縮比的 JPEG 壓縮攻擊下，此時影像品質與原影像已有明顯的差異，我們的浮水印依然可以辨識出來。



圖 4.1 JPEG 壓縮攻擊測試的結果，其中 (a) ~ (d) 為 JPEG 壓縮攻擊後的 Lena 影像，壓縮品質依序為 90%、70%、50%、20%。PSPNR 依序為 33.62、32.99、32.57、31.54；(e) ~ (f) 為 (a) ~ (d) 中取出之浮水印，其相似度 NC 值依序為 0.91、0.87、0.79、0.53。



4.1.2 模糊攻擊測試。

將嵌入東海校徽後的 Lena 影像經過不同程度的模糊化攻擊之後的測試結果如圖 4.2。



	(f)	(g)	(h)	(i)	(j)
取出的浮水印					
PSPNR	24.59	22.46	22.34	22.15	21.96
PSNR	22.38	20.32	20.22	20.05	19.89
NC	0.86	0.68	0.44	0.38	0.34

圖 4.2 模糊攻擊測試的結果，其中 (a) ~ (e) 為不同程度的模糊化處理後的 Lena 影像；(f) ~ (j) 分別為 (a) ~ (e) 的 PSPNR 及 PSNR 與取出之浮水印及其相似度 NC 值

4.1.3 雜訊攻擊測試。

將嵌入東海校徽後的 Lena 影像分別加入變異數為 3、5、10、15、20、25 的變動性分佈的雜訊之後的測試結果如圖 4.3。

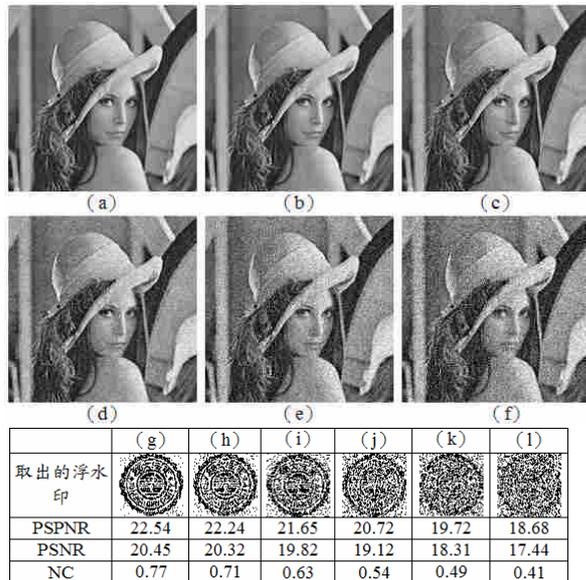


圖 4.3 雜訊攻擊測試的結果，其中 (a) ~ (f) 為加入不同程度的雜訊後的 Lena 影像；(g) ~ (l) 分別為 (a) ~ (f) 的 PSPNR 及 PSNR 與取出之浮水印及其相似度 NC 值

4.1.4 銳利化攻擊測試

將嵌入東海校徽後的 Lena 影像經過不同程度的銳利化攻擊後的測試結果如圖 4.4。

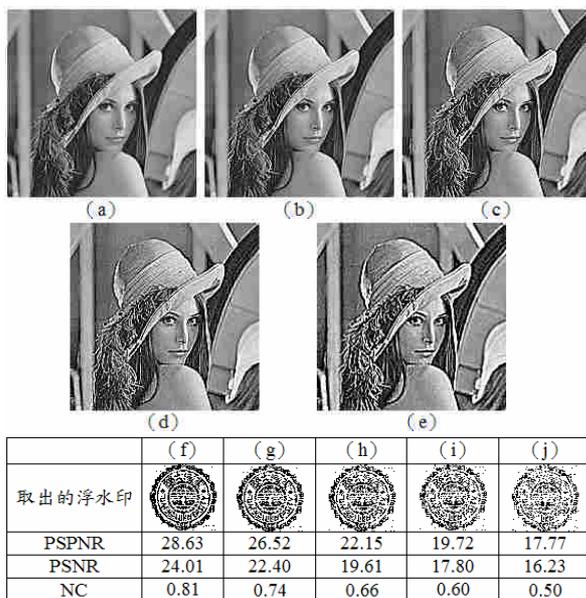


圖 4.4 銳利化攻擊測試的結果，其中 (a) ~ (e) 為不同程度的銳利化處理後的 Lena 影像；(f) ~ (j) 分別為 (a) ~ (e) 的 PSPNR 及 PSNR 與取出之浮水印及其相似度 NC 值。

4.1.5 擷取攻擊測試

將嵌入東海校徽後的 Lena 影像分別擷取不同資料量的測試結果如圖 4.5。

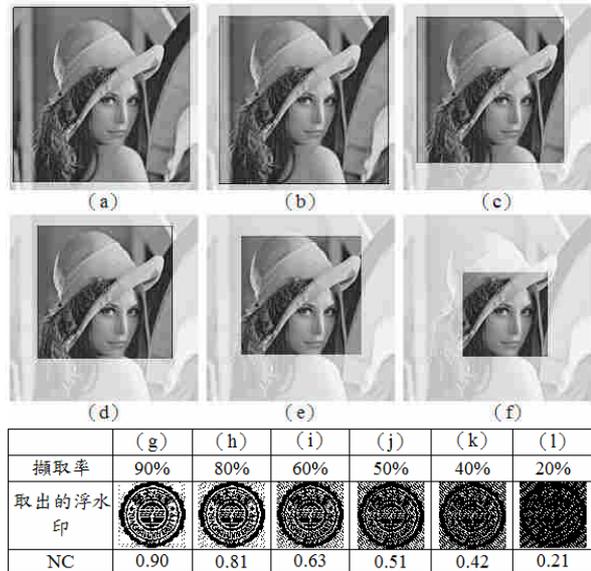


圖 4.5 擷取攻擊測試的結果，其中 (a) ~ (f) 為擷取 Lena 影像 90%、80%、60%、50%、40%、20% 之資料量；(g) ~ (l) 分別為 (a) ~ (f) 取出之浮水印及其相似度 NC 值

4.2 基於區塊分類的浮水印技術

我們對所加入的浮水印影像進行與 4.1 節中相同程度的攻擊破壞，來分析比較兩種方法遭受各類影像處理攻擊後浮水印的存活率。

4.2.1 JPEG 壓縮攻擊測試

我們將經區塊分類的浮水印技術與基於模擬攻擊的浮水印技術的結果做比較並繪成圖 4.6，從圖中可以明顯的看出測試影像為 Lena 在任何壓縮品質攻擊下，使用區塊分類的浮水印技術取出的浮水印其相似度 NC 值均比基於模擬攻擊的浮水印技術的相似度 NC 值略有提昇。在壓縮品質 10% 以下的 JPEG 壓縮攻擊下我們取出的浮水印雖然可以隱約的辨識出來但效果仍不盡理想。

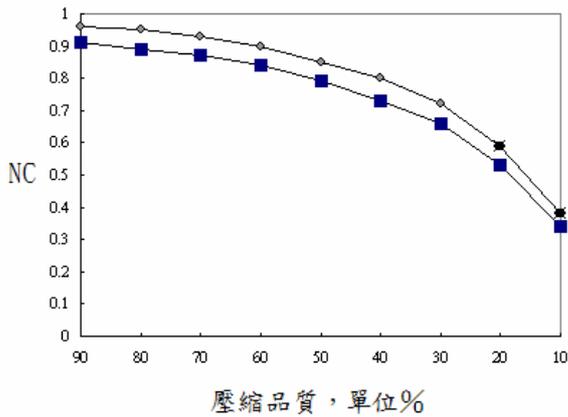


圖 4.6 Lena 為測試影像之相似度 NC 值對 JPEG 壓縮品質的曲線圖，其中”●”為使用區塊分類的浮水印技術；”■”為無區塊分類的浮水印技術。

4.2.2 模糊攻擊測試。

我們將經區塊分類的浮水印技術與基於模擬攻擊的浮水印技術的結果做比較並繪成圖 4.7，由圖中分析使用區塊分類的浮水印技術取出的浮水印其相似度 NC 值與基於模擬攻擊的浮水印技術的相似度 NC 值比較，雖然略有提昇但對於高強度的模糊攻擊本章的作法對於浮水印的強健性助益有限。

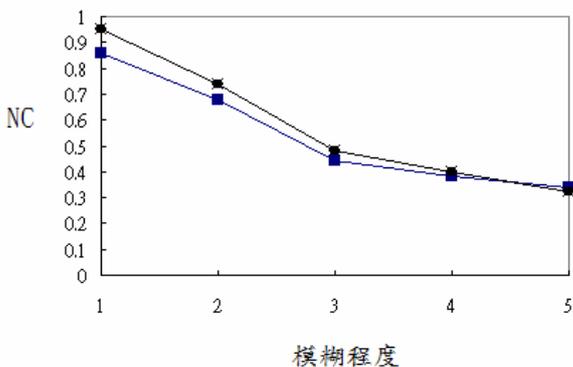


圖 4.7 Lena 為測試影像之相似度 NC 值對模糊程度的曲線圖，其中”●”為使用區塊分類的浮水印技術；”■”為無區塊分類的浮水印技術。

4.2.3 雜訊攻擊測試。

我們將經區塊分類的浮水印技術與基於模擬攻擊的浮水印技術的結果繪成圖 4.8 以茲比較。由圖中分析，以相似度 NC 值比較來看，使用區塊分類的浮水印技術取出之浮水印的相似度 NC 值確實比

基於模擬攻擊的浮水印技術的相似度 NC 值略有提昇；但若以視覺來看，對於較程度的雜訊攻擊如 (c)、(d)，浮水印幾乎完全被破壞了。

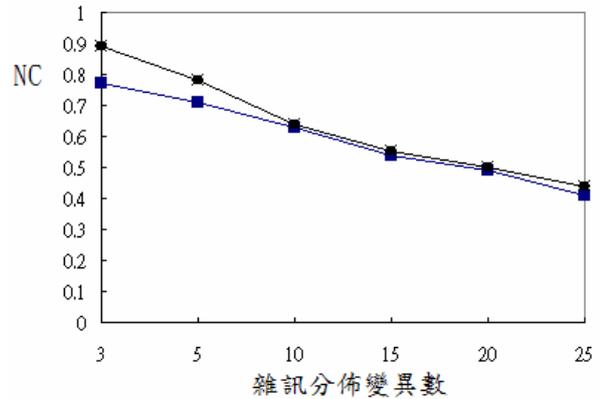


圖 4.8 Lena 為測試影像之相似度 NC 值對雜訊分佈變異數的曲線圖，其中”●”為使用區塊分類的浮水印技術；”■”為無區塊分類的浮水印技術。

4.2.4 銳利化攻擊測試

我們將經區塊分類的浮水印技術與基於模擬攻擊的浮水印技術的結果繪成圖 4.9 以茲比較。由圖中分析，無論從相似度 NC 值或視覺比較來看，使用區塊分類的浮水印技術取出之浮水印的強健性確實比上基於模擬攻擊的浮水印技術的來的好。經不同程度的銳利化攻擊後的影像，我們取出的浮水印其相似度 NC 值大約保持在 0.8 與 0.5 之間，我們依然可以辨識出浮水印。基本上對於銳利化攻擊，我們浮水印系統有較佳的抵抗能力。

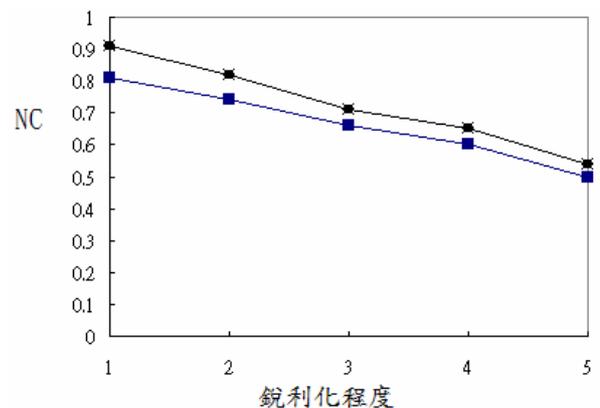


圖 4.9 Lena 為測試影像之相似度 NC 值對銳利化程度的曲線圖，其中”●”為使用區塊分類

的浮水印技術；”■”為無區塊分類的浮水印技術。

4.2.5 擷取攻擊測試。

我們將經區塊分類的浮水印技術與基於模擬攻擊的浮水印技術的結果繪成圖 4.10 以茲比較。由圖中分析，無論是使用區塊分類或不經區塊分類的浮水印技術對於擷取性的攻擊，兩種作法擷取的資訊量是相同的，因此取出的浮水印及相似度 NC 值也相同。

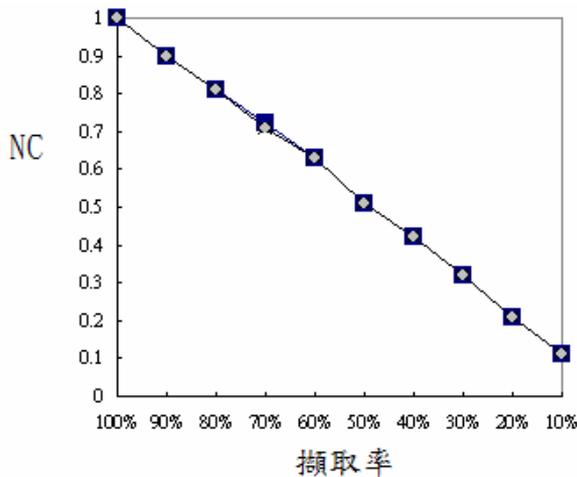


圖 4.10 Lena 為測試影像之相似度 NC 值對擷取率的曲線圖，其中”●”為使用區塊分類的浮水印技術；”■”為無區塊分類的浮水印技術。

五、結論

由實驗結果顯示出，本文中所提出的兩種浮水印技術結合空間域和頻域兩種嵌入方法的優點，將人類視覺系統的特性應用到頻域來，能保證嵌入浮水印後的影像品質，並提出位置強度模型使嵌入浮水印更具有高度的強健性可以抵抗更嚴重的攻擊破壞。根據實驗結果分析，無論使用所提出的哪種浮水印技術，只要受攻擊後影像不被破壞到視覺上嚴重失真的程度，都能辨識出浮水印的存在。尤其在 JPEG 壓縮攻擊下，壓縮品質 20% 以上的 JPEG 壓縮攻擊我們仍然可以取出浮水印，相當於可以抵抗 29 倍 JPEG 壓縮攻擊。

目前有許多浮水印技術的研究，大都針對不需要原始影像的輔助來偵測浮水印的存在。一般而言，浮水印偵測時不需原始影像的輔助，其強健性較低，尤其對嵌入的浮水印為二元影像時便無法抵抗影像部分擷取的攻擊。雖然有許多這方面的研究都宣稱其可以抵抗擷取性的攻擊，但其基本上都假設知道擷取出的子影像與原影像的相對位置，這種假設實在有可議之處。而且以保護智慧財產權來考量而言，為了節省原影像的儲存空間而降低了浮水印系統的強健性是否本末倒置呢？

本文所提出位置強度模型，目前只實作於 DCT 轉換上且有很好的效果，並且其他同是 DCT 轉換的浮水印系統亦可以使用此位置強度模型來提昇其浮水印系統的強健性。我認為此位置強度模型應該可以推展至小波轉換浮水印系統甚至空間域浮水印系統上，這是一個在未來可以研究的方向。

六、參考文獻

- [1] F. Hartung, and M. Kutter, "Multimedia Watermarking Techniques," Proceedings of the IEEE, Vol. 87, No. 7, pp. 1079-1107, July 1999.
- [2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding-A Survey," Proceedings of the IEEE, Vol. 87, No. 7, pp. 1062-1078, July 1999.
- [3] C.I. Podilchuk and W. Zeng, "Image-Adaptive Watermarking Using Visual Models," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 525-539, May 1998.
- [4] S. Craver, N. Memon, B.-L. Yeo, M.M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," IEEE Journal on Selected Areas in Communications, Vol. 16, No.4, pp. 573-586, May 1998.
- [5] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, "A Digital

- Watermark," IEEE Int. Conf. on Image Proc., Vol. 2, pp. 86-94, 1994.
- [6] F. Hartung and B. Girod, "Watermarking of Uncompressed and Compressed Video," Signal Processing, Vol. 66, No. 3, pp. 283-301, 1998.
- [7] G. Voyatzis and I. Pitas, "Applications of Topral Automorphisms in Image Watermarking," IEEE Int. Conf. on Image Proc., pp. 237-240, 1996.
- [8] N. Nikolaidis and I. Pitas, "Robust Image Watermarking in the Spatial Domain," Signal Processing, Vol. 66, No.3, pp. 385-403, 1998.
- [9] I.J. Cox, J. Kilian, F.T. Leighton and T. Shamon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687, Dec. 1997.
- [10] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT-domain System for Robust Image Watermarking," Signal Processing, Vol. 66, No. 3, pp. 357-372, 1998.
- [11] C. T. Hsu and J. L. Wu, "Digital Watermarking for Images and Videos Engineer," doctor Thesis in National Taiwan University, Taiwan, R.O.C., 1997.
- [12] F. Hartung, B. Girod, "Digital Watermarking of MPEG-2 Coded video in the Bitstream Domain," IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), pp. 2621-2624, 1997.
- [13] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent Robust Image Watermark," IEEE Int. Conf. on Image Proc., Vol. 3, pp. 211-214, 1996.
- [14] M.D. Swanson, B. Zhu and A.H. Tewfik, "Multiresolution Scene-Based Video Watermarking Using Perceptual Models," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 540-550, May 1998.
- [15] J.F. Delaigle, C. D. Vleeschouwer and B. Macq, "Watermarking Algorithm based on a Human Visual Model," Signal Processing, Vol. 66, No. 3, pp. 319-335, 1998.
- [16] J.O. Rusanidh and T. Pun, "Rotation, Scale and Translation Invariant Spread Spectrum," Signal Processing, Vol. 66, No. 3, pp. 303-317, 1998.
- [17] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images," IEEE Transactions on Image Processing, Vol. 8, No. 1, pp. 58-68, Jan. 1999.
- [18] E. Koch and J. Zhao, "Towards Robust and Hidden Image Copyright Labeling," Proceedings of 1995 IEEE workshop on Nonlinear Signal and Image Processing, 1995.
- [19] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding," Pro. of the SPIE Conference on Storage and Retrieval for Image and Video Databases III, Vol. 2420, pp. 164-173, Feb 1995.
- [20] G. Voyatzis and I. Pitas, "Chaotic Watermarks for Embedding in the Spatial Domain," In Proceedings of ICIP'98, Chicago, USA, Oct 1997.
- [21] G. Voyatzis and I. Pitas, "Digital Image Watermarking using Mixing Systems," Computer & Graphics, Elsevier, Vol. 22, No. 4, pp. 405-416, 1998.
- [22] M. Kutter, F. Jordan, and F. Bossen, "Digital Watermarking of Color Images using Amplitude Modulation," Journal of Electronic Imaging, Vol. 7, No. 2, pp. 326-332, Apr 1998.
- [23] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust Data Hiding for Images," IEEE Digital Signal Processing Workshop, (Loen, Norway), pp. 37-40, Sep 1996.
- [24] C. I. Podilchuk and W. Zeng, "Image Adaptive Watermarking using Visual Models," IEEE Journal on Selected Areas in Communication, Vol. 16, pp. 523-539, 1998.
- [25] A. B. Watson, "DCT Quantization Matrices Visually Optimized for Individual Images," Proc. SPIE conf. Human Vision, Visual Processing, and Digital Display IV, pp. 202-216, 1992.
- [26] S.W. Kim, S. Suthaharan, H.K. Lee and K.R. Rao, "Image Adaptive Watermarking Scheme using Visual Model and BN Distribution," Elec. Lett., 4th, Vol. 35, Issue 3, Feb 1999.
- [27] S. Suthaharan and S. Sathanathan, "Transform Domain Technique: Robust Watermarking for Digital

- Images," Southeastcon 2000. Proceedings of the IEEE, pp. 407-412, 2000.
- [28] C. H. Lee; H. S. Oh; Y. Baek; H. K. Lee, "Adaptive Digital Image Watermarking using Variable Size of Blocks in Frequency Domain," TENCON 99. Proceedings of the IEEE Region 10 Conference, Vol. 1, pp. 702-705, 1999.
- [29] N. B. Nill, "A Visual Model Weighted Cosine Transform for Image compression and Quality Assessment," IEEE Transactions on communications, Vol. Com-33, No. 6, pp. 551-557, June 1985.
- [30] H.A. Peterson, A.J. Ahumada, Jr. and A. B. Watson, "Improved Detection Model for DCT coefficient Quantization," Proc. SPIE Conf. Human Vision, Visual Processing, and Digital Display IV, Vol. 1913, pp. 191-201, Feb. 1993.
- [31] C.H. Chou and Y. C. Li, "A perceptually tuned subband image coder based on the measure of just-noticeable-distortion profile," IEEE Transactions on Circuit and Systems for Video Technology, Vol. 5, Issue. 6, pp. 467-476, Dec. 1995.
- [32] J. Park, "Some Adaptive Quantizers for HDTV Image Compression," Signal Processing of HDTV, V. 1994.
- [33] F. Hartung, J. K. Su, and B. Girod, "Spread Spectrum Watermarking: Malicious Attacks and Counter Attacks," Security and Watermarking of Multimedia Contents, Proc. SPIE 3657, Jan. 1999.
- [34] F. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Attacks on Copyright Marking Systems," 2nd Workshop on Information Hiding, USA, pp. 218-238, 1998.
- [35] T.D. Tran and R. Safranek, "A Locally Adaptive Perceptual Masking Threshold Model for Image Coding," IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, Vol. 4, pp. 1882-1885, 1996.
- [36] Jiwu Huang; Li Chen; Shi, Y.Q. "An Integrated Classifier in Classified Coding," Proceedings of the 1998 IEEE International Symposium on, Vol. 4, pp. 146-149, 1998.
- [37] Jiwu Huang and Shi, Y.Q. "Segmentation-based Hybrid Coding using Luminance Masking," Electronics Letters, Vol. 34, Issue. 8, pp. 750-751, Apr 1998.
- [38] H.H.Y. Tong, and A.N. Venetsanopoulos, "A Perceptual Model for JPEG Applications Based on Block Classification, Texture Masking, and Luminance Masking," IEEE Int. Conf. on Image Processing (ICASSP), pp. 428-432, 1998.
- [39] J. Fridrich, "Combining Low-frequency and Spread Spectrum Watermarking," Proc. SPIE Int. Symposium on Optical Science, Engineering, and Instrumentation, San Diego, July 19-24, 1998.
- [40] C. S. Lu, H. Y. Mark Liao, S. K. Huang, and C. J. Sze, "Highly Robust Image Watermarking Using Complementary Modulations," to appear in 2nd International Information Security Workshop, Malaysia, Nov. 6-7, 1999.
- [41] C. S. Lu, H. Y. Mark Liao, S. K. Huang, and C. J. Sze, "Cocktail Watermarking on Images," to appear in 3rd International Workshop on Information Hiding, Dresden, Germany, Sept. 29-Oct. 1, 1999.
- [42] R. B. Wolfgang and J. Delp, "A Watermark for Digital Image", IEEE Int. Conf. Image Processing, Vol. 3, pp. 219-222, Sept. 1996.
- [43] Y. C. Hou, P. M. Chen and Y. F. Chiao, "Steganography: An Efficient Data Hiding Method," in Proc. of CVPRIP'98, Vol.4, pp. 211-214, Durham, Oct., 1998.
- [44] P. M. Chen, "A Robust Digital Watermarking based on A Statistic Approach", IEEE Int. Conf. on Information Technology: Coding and Computing, pp. 116-121, 2000.