第五章　與他人方法之比較

本章節一開始會先簡介 Tai, Wang, and Yu (2002)所提出之方法，接著說明選擇此篇論文來做為比較的原因，並在最後呈現本研究方法與 Tai 等人提出之方法比較後的結果。

第一節　Tai, Wang, and Yu 所提之方法

Tai, Wang, and Yu (2002)在“Visual Secret Sharing Watermarking for Digital Image”所提出的方法是利用視覺密碼技術將浮水印分成兩份分享影像，而原始影像經由離散餘弦轉換(discrete cosine transform, DCT)後取出其中頻帶，再將其中一份分享影像藏入中頻帶中，最後再將藏入浮水印的影像做離散餘弦轉換的轉回，即完成隱藏浮水印的動作，圖 5-1 為 Tai 等人所提之隱藏浮水印流程圖。在視覺密碼加密浮水印的部份，Tai 等人採用的是與本研究相同的加密規則，如表 2-2 所示。圖 5-2 為藏入浮水印的步驟，由此步驟可以得知 Tai 等人是將要被藏入浮水印的中頻帶以兩個係數為一組的方式來做配對，利用交換配對後組內係數的方式使得配對後的係數經由步驟六的判斷條件判斷後，與浮水印的像素值相同，藉此來將浮水印藏入原始影像中。

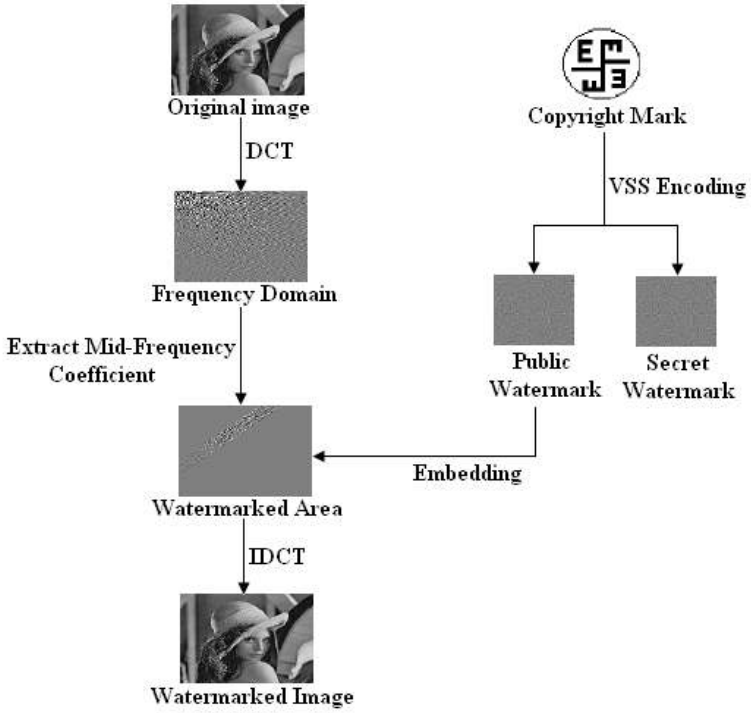


圖 5-1　Tai 等人所提之隱藏浮水印流程圖

步驟一：將取出的中頻帶放入一維陣列中，即：

$C = \{C_1, C_2 \ldots, C_{2\times 2k\times 2l}\}$

步驟二：將浮水印像素值取出放入一維陣列 $W(r)$中。

步驟三：將中頻帶 $C = \{C_1, C_2 \ldots, C_{2\times 2k\times 2l}\}$兩兩做不重複的配對，即：

$CP_i = (C_{2i-1}, C_{2i})$,　　$i = 1, 2 \ldots, 2k\times 2l$

步驟四：將 $W(r)$裡的值順序打亂，產生 $W(R_i) = \{R_1, R_2 \ldots, R_{2\times 2k\times 2l}\}$。

步驟五：執行下列判斷條件，

$$(C_{2i-1}, C_{2i}) = \begin{cases} 1 & if\ (C_{2i-1} > C_{2i}) \\ 0 & if\ (C_{2i-1} \le C_{2i}) \end{cases}$$

步驟六：執行下列判斷條件，

IF $\{W(Ri) \oplus (C_{2i-1}, C_{2i}) = 1\}$

THEN {swap the coefficient of C_{2i-1} and C_{2i}}

ELSE {no operation}

圖 5-2　Tai 等人所提之隱藏浮水印步驟圖

圖 5-3 為 Tai 等人(2002)所提之取出浮水印流程圖，首先將被浮水印影像做離散餘弦轉換後，取出轉換後影像的中頻帶，接者再透過比對的方式產生藏入的分享影像，最後將取出的分享影像與所有權人手中的分享影像做 OR 運算即可產生浮水印影像。圖 5-4 為取出浮水印的步驟，由此步驟可以得知在取出被藏入浮水印的中頻帶並以兩個係數為一組來做配對後，再利用步驟四的判斷條件做判斷後，即可取出藏入原始影像中的浮水印。

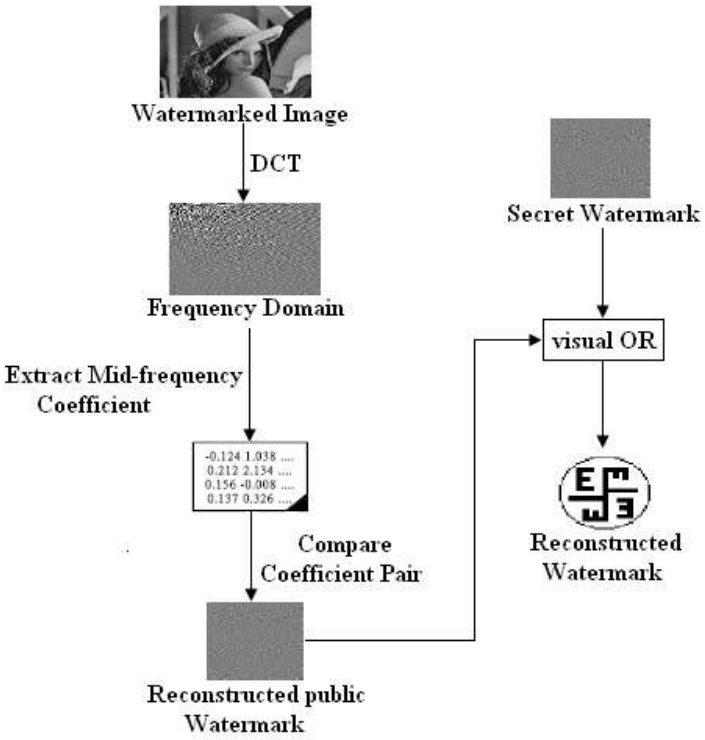


圖 5-3　Tai 等人所提之取出浮水印流程圖

步驟一：將取出的中頻帶放入一維陣列中，即：

$C' = \{C'_1, C'_2 \ldots, C'_{2\times 2k\times 2l}\}$

步驟二：將中頻帶 $C' = \{C'_1, C'_2 \ldots, C'_{2\times 2k\times 2l}\}$ 兩兩做不重複的配對，即：

$CP_i = (C'_{2i-1}, C'_{2i}), \quad i = 1, 2 \ldots, 2k\times 2l$

步驟三：利用 key 值產生原先打亂的集合 $W(R_i) = \{R_1, R_2 \ldots, R_{2\times 2k\times 2l}\}$。

步驟四：執行下列判斷條件，

$$W'_P(i) = \begin{cases} 1 & if\ (C'_{2i-1} > C'_{2i}) \\ 0 & if\ (C'_{2i-1} \le C'_{2i}) \end{cases}$$

圖 5-4　Tai 等人所提之取出浮水印步驟圖

由於 Tai 等人(2002)所提出的方法是透過視覺密碼的方法將浮水印分成兩份分享影像後，利用修改原始影像頻率域係數的方式來藏入其中一份，以達到保護原始影像著作權的目的，其作法與本研究相當類似，表 5-1 為兩方法相同與相異處之比較，因此本研究將以 Tai 等人所提出之方法做為比較對象。

表 5-1　本研究與 Tai 等人所提之方法比較

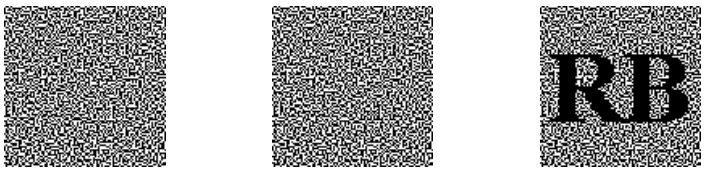
相同處	1. 皆使用視覺密碼的方法來對浮水印做分享 2. 皆使用轉換頻率域的方式來處理原始影像 3. 皆使用中頻帶為隱藏浮水印的位置 4. 皆以黑白浮水印及灰階原始影像來做實驗
相異處	1. 使用頻率域的方法 本研究：離散小波轉換 Tai 等人：離散餘弦轉換 2. 藏入浮水印的規則

第二節　兩方法比較結果

本研究在實驗本方法與 Tai 等人(2002)所提之方法的比較是以圖 5-5 (a)大小為 128 × 128 的灰階影像為原始影像，以圖 5-5 (b)大小為 50 × 50 的黑白影像為浮水印影像，圖 5-6 (a)和圖 5-6 (b)則是利用表 2-2 的視覺密碼方法所產生的浮水印分享影像 share1 及 share2，圖 5-6 (c)則是將 share1 和 share2 疊合後所產生之原始浮水印影像。本研究在實驗結果將以 *PSNR* 指標來衡量被浮水印影像與原始影像之間的差異，並以 *NC* 值來表示原始浮水印影像與受攻擊後取出的浮水印影像之間的差異。

(a) 原始影像　　(b) 浮水印影像

圖 5-5　比較實驗所使用之影像



(a) share1　　(b) share2　　(c) share1_2

圖 5-6　比較實驗所產生之影像

一、比較實驗結果

圖 5-7 為被浮水印影像及取出浮水印之實驗結果，由圖 5-7 (a)及圖 5-7 (c)為被浮水印影像在未受攻擊前所計算之 *PSNR* 值可看出，本研究所得到的 *PSNR* 值較 Tai 等人(2002)提出的方法來的高，因此可以確定本研究能夠產生品質較佳的被浮水印影像。從圖 5-7 (b)及圖 5-7 (d)為被浮水印影像在未受攻擊前取出浮水印所計算之 *NC* 值可以看出，由於 Tai 等人所使用之離散餘弦轉換是採用全域(full-frame)的方式，也就是未將原始影像做切割，因此在計算上除了相當耗費時間之外，同時也增加其誤差值(張真誠，黃國峰，陳同孝，2003；連國珍，1999)，因此取出的浮水印影像並無法達到與未藏入影像前的浮水印一模一樣的效果。

	被浮水印影像	浮水印影像
本研究方法		
	(a) *PSNR* = 32.77 dB	(b) *NC* = 1.00
Tai 等人所提之方法		
	(c) *PSNR* = 28.32 dB	(d) *NC* = 0.97

圖 5-7　兩種方法所產生之 *PSNR* 值及 *NC* 值

二、比較攻擊實驗結果

圖 5-8 為被浮水印影像在經過各種常見攻擊的實驗結果後，取出之浮水印影像之 *NC* 值長條圖，而其實驗結果如圖 5-9 所示，攻擊參數如表 5-2 所示。由圖 5-8 我們可以看出在不同類型的攻擊情況下，兩種方法所取出的浮水印皆能夠有一定的辨識程度，但本研究所計算出的 *NC* 值又較 Tai 等人(2002)提出的方法要高，因此顯示本研究所提出的方法的確能夠在被浮水印影像受攻擊後，取出品質較佳的浮水印影像。

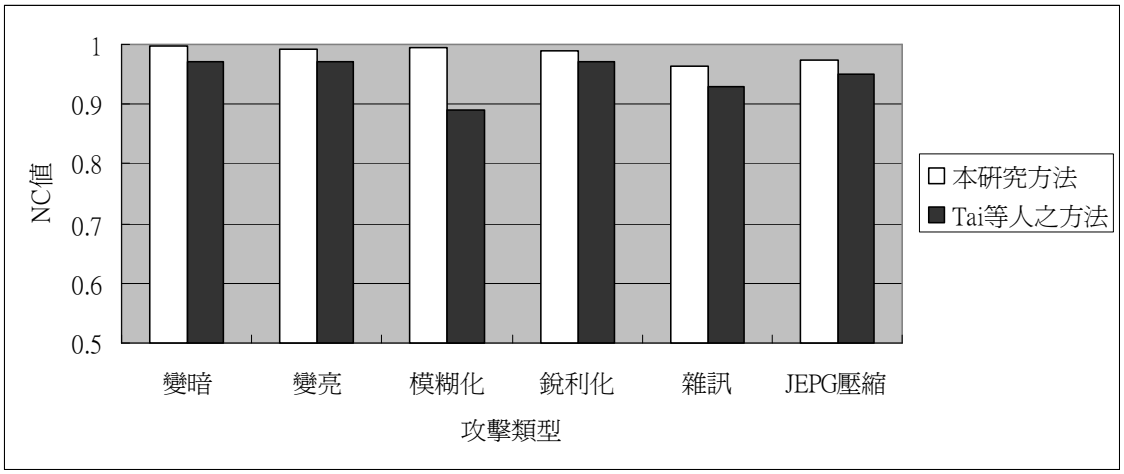


圖 5-8　不同攻擊類型之實驗結果

表 5-2　各類型攻擊參數說明

攻擊類型	參數
變暗	亮度：-25
變亮	亮度：+25
模糊化	智慧型模糊化，強度 20.0，臨界值 1.0
銳利化	智慧型銳利化，總量 15%，強度 4.0
雜訊	總量 3%
JPEG 壓縮	品質：8

攻擊類型	本研究方法	Tai 等人所提之方法
變暗		
	(a) *NC* = 0.99	(b) *NC* = 0.97
變亮		
	(c) *NC* = 0.99	(d) *NC* = 0.97
模糊化		
	(g) *NC* = 0.99	(h) *NC* = 0.89
銳利化		
	(i) *NC* = 0.98	(j) *NC* = 0.97
雜訊		
	(k) *NC* = 0.96	(l) *NC* = 0.93
JPEG 壓縮		
	(m) *NC* = 0.97	(n) *NC* = 0.95

圖 5-9　實驗結果取出之浮水印

三、總結比較實驗結果

經由以上之實驗結果可證實本研究所提出之方法的確較

Tai 等人(2002)提出之方法要來的好，其歸納幾點如下：

(一)被浮水印影像

從被浮水印影像之*PSNR*值可得知本研究所提出的方法在原始影像藏入浮水印影像後，較 Tai 等人(2002)所提出之方法不容易被人眼所發現，符合一個好的浮水印需要具備不可察覺性之特性。

(二)未受攻擊前所取出之浮水印影像

從未受攻擊前所取出之浮水印影像之*NC*值可得知本研究方法所取出的浮水印與未藏入前的浮水印是完全相同，而 Tai 等人(2002)由於使用的是全域的離散餘弦轉換，在公式的計算上會產生較大誤差值的問題，因此取出的浮水印無法達到與本研究相同的品質。

(三)受攻擊後所取出之浮水印影像

經由以上實驗結果可以得知，在受到不同類型的影像攻擊後，本研究所取出之浮水印品質較 Tai 等人(2002)所取出的略勝一籌，滿足一個好的浮水印應該滿足的明確性之條件。

(四)運算效率

由於 Tai 等人(2002)所提出之方法使用的是全域的離散餘弦轉換，因此在計算上需要二個迴圈的時間才能將原始影像轉換為頻率域，其時間複雜度為 $O(n^2)$，而本研究所採用的離散小波轉換在計算上只需要一個迴圈的時間便能將原始影像轉換為頻率域，其時間複雜度為 O(n)，因此在運算效率上 Tai 等人提出的方法是相當的慢。

(五)負載量

在藏入浮水印的過程中，本研究只需要一個頻率域係數便能藏入一個分解影像的位元，而 Tai 等人(2002)所提

出之方法則需要二個頻率域係數才能藏入一個分解影像的位元，因此在藏入相同大小浮水印的情況之下，本研究所修改的頻率域係數較 Tai 等人的要來的少，所產生的被浮水印影像便較不會被人眼所察覺其與原始影響之間的差異。