相位調制技術在數位影像浮水印之應用

陳文淵
cwy@ncut.edu.tw

摘要

在數位影像中加入浮水印，包含 2 項要素:1).不能降低數位影像的品質，即加入浮水印資料後，數位影像仍需具有良好的品質。 2).浮水印必需具備強健性，不能輕易被破壞，基於這兩項要求，我們發覺現數位通信調制技術很適合引用在數位影像浮水印方面，原因是數位通信調制技術有強大的雜訊排除能力，且利用調制技術改變少數的影像內容。因此能保持良好的影像品質。本人採用相位調制技術作為數位影像嵌入浮水印的技術，經實驗證明，相位調制技術是一種有效的數位影像浮水印隱藏技術。

關鍵詞：相位調制技術，數位浮水印，影像品質，強健性浮水印

一、簡介

由於電腦與網路的普及，數位資料得以藉由網路的傳播，因此產生資料安全的問題 。在數位化的時代，未經授權的複製，對作者是很大的傷害力。目前大都採用數位浮水印的技術來保護數位智財權。數位浮水印是將智財擁有者的資訊嵌入到數位多媒體資料中，作為認證版權的依據。

數位浮水印在設計上需考慮下列因素： 1) 透明度 (Transparency)：在影像植入浮水印後，不能影響原影像品質。 2) 安全性 (Security)：所植入的浮水印不能被破解偵測而被移除。即使知道浮水印的演算法，使用者仍必須使用秘鑰 (secrete key) 才能取出浮水 印。3) 明確性(Unambiguous) :浮水印必須清楚確認版權所有人。4) 強健性 Robustness： 具浮水印之影像經過攻擊後，浮水印不能被破壞。 5) 容量 (Capacity)：在原影像中，能加入浮水印的資料量。好的浮水印技術能使原始影像中容納更多的浮水印資訊。 6) 是否需有來源資料比對 (Blindness)： 在抽取浮水印時，是否需要使用來源資料作比對。

常用被使用作為浮水印攻擊的方式有: 1)數位類比轉換法（A/D,D/A conversion），2) 旋轉攻擊法（rotation），3)放大縮小破壞法（scaling），4) 切割改變法（cropping），5) 壓縮還原法（compression）， 6) 再量化處理法（requantization），7) 再取樣分配法（resample）。

影像浮水印技術通常是更改影像中的資料來嵌入浮水印數據，有兩個主要的運作領域:A.空間域（時間域）法: 早期影像浮水印技術主要是在空間域發展，以灰階影像為例，每個像素點（pixel）以八個位元來表示，資料位元的重要性由最高位元 MSB 向最

低位元 LSB，因此更改像素點中敏感度最低的 LSB 來嵌入浮水印資料，以獲得較高的隱密性。缺點是容易被惡意破壞，難以抵抗各種破壞攻擊。B.頻率域法:在頻域中的浮水印技術是將原始影像轉換到頻域，然後加入浮水印資料，將浮水印藏匿在不同頻率成份訊號中，將資料嵌入至高頻訊號中，較不容易被人眼察覺，嵌入至低頻成份訊號中，則不容易被破壞。

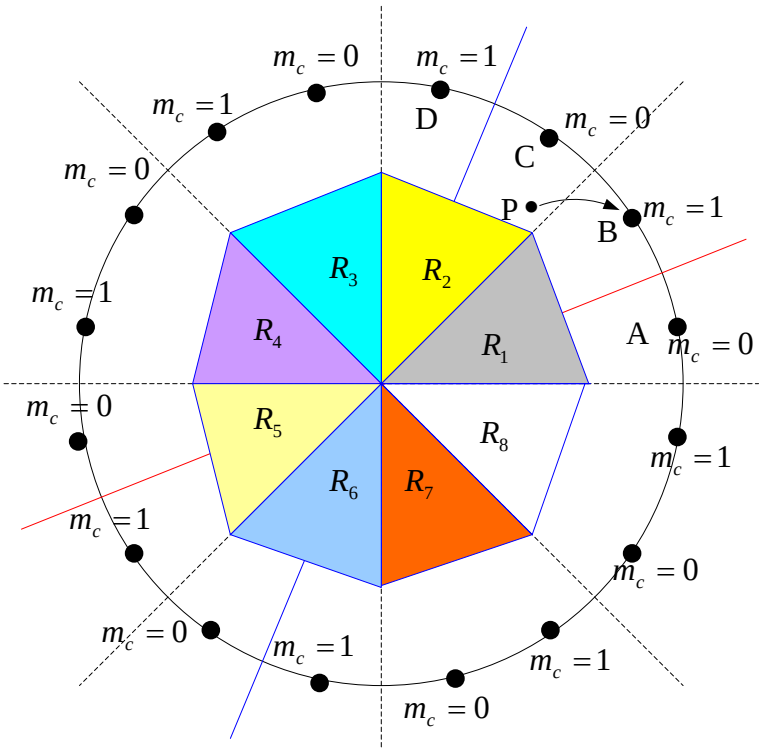
Hsu 和 Wu [3]發表一種使用數位餘弦轉換 DCT 技術結合區塊處理的數位浮水印隱藏技術。 經實驗結果證實有良好的效果。Wu 和 Hsieh [10]使用零樹結構法在數位餘弦轉換 DCT 作出類似在小波領域的多解析度分析法來嵌入數位浮水印。 Ruanaidh 等人[6]發表在數位傅立葉領域以相位角的浮水印隱藏技術，經實驗證明該演算法最能抵檔旋轉性的破壞攻擊。Solachidis 和 Pitas [7] 發表一款將圓對稱的浮水印隱藏在二維的數位傅立葉轉換領域中，而獲得良好的數位浮水印隱藏效果 。

二、相移鍵控技術之相位角選擇

為了保持被嵌入秘密資料之影像品質，一種最近接相位角選擇法 nearest phase selection (NPS)被採用在本論文中。在相位角調制的過程中，任何信號的相位的角度會依秘密資料的位元值來改變信號的相位角度至幾個固定點，如圖一所示。圖一是相位調制強度為s=1/8 的信號星座圖，每一信號的相位角度被分為 8 個區域R_1-R_8。每一個區域依據秘密資料的值為 0 或 1 分別對應到不同的相位角度。例如圖中的R_2區域，若秘密資料的值為 1， ($m_c=1$)，則信號點 p 會被強制改變至圖中的 D 點。若秘密資料的值為 0，($m_c=0$)，則信號點 p 會被強制改變至圖中的 C 點.但假如信號點 p，其秘密資料的值為 1，($m_c=1$)，照規則信號 p 應更改為 D，但實際上信號 p 應更改為 B 才對，因為 B 點與 P 點的距離比 D 點與 P 的距離近。換言之改變信號的角度較小，造成影像品質劣化的程度會較小。在圖 1 中將相位角的區域分為 8 段，因此每區段的角度為 45 度。在 45 度中又分為$m_c=1$與$m_c=0$等 2 種，因此真正改變信號的角度必定小於 22.5 度。若雜訊干擾的角度大於 11.25 度才可能造成解調制時的資料錯誤，相位制的數學公式如下所示。

$$P=\begin{cases} B \quad , \quad if \quad (\angle P-\angle B)<(\angle D-\angle P) \\ D \quad , \quad if \quad (\angle P-\angle B)\geq(\angle D-\angle P) \end{cases} \tag{1}$$

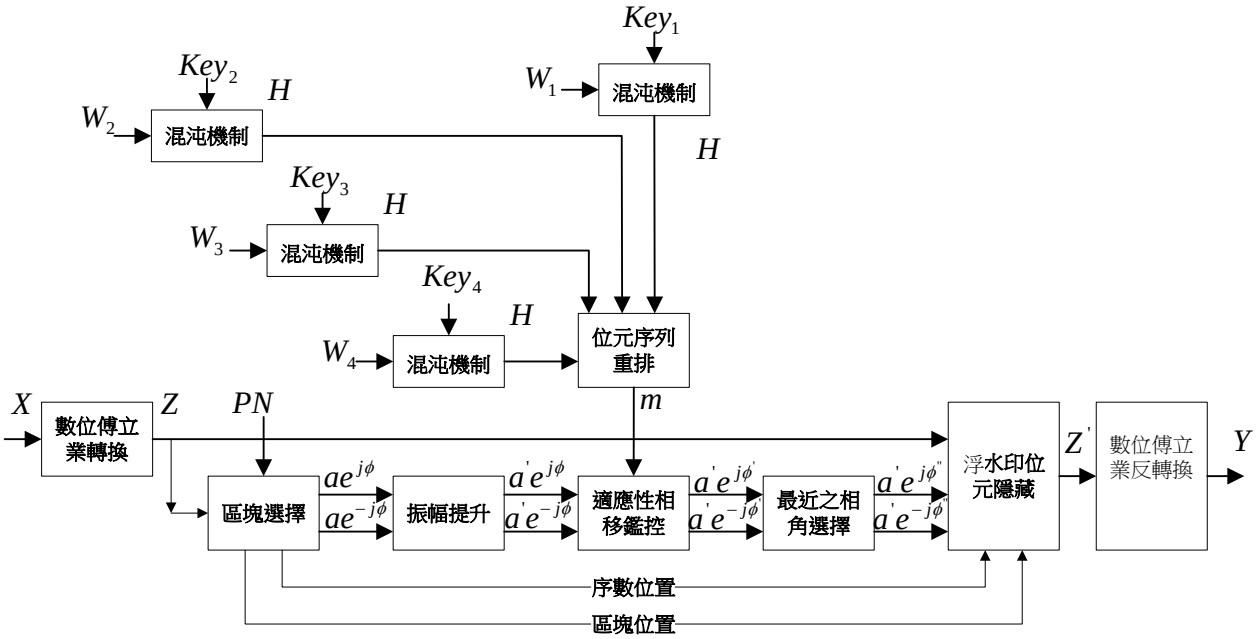
其中$\angle P$是 p 點的角度， $\angle B$是 B 點的角度，$\angle D$ 是 D 點的角度。



圖一、最近接相位角選擇法示意圖

三、嵌入浮水印演算法

一種強健的浮水印技術必須要能夠在各種攻擊後，仍然保有影像品質，且要保證在安全性方面的祕密鑰匙不能被惡意攻擊者破解。本研究的浮水印隱藏架構如圖二所示， 四個浮水印 $W_1 \sim W_4$ 首先經由混沌機構 chaotic mechanism (CM) 將資料打亂。並註記為 H 。混沌機構採用亂數序列 PN_3 及密秘鑰匙 Key 來完成 。四種浮水印 $W_1 \sim W_4$ 經由混沌機構後轉換為二元性質的位元串輸出 $\{m\}$ 作為相位調制的信號來源。另一方面，主要影像 X 經由數位傅立葉轉換後註記為 Z 。數位傅立葉轉換後的區塊 Z 經由亂數序列 PN_2 的選擇作為秘密資料的隱藏區塊。被選擇出的兩個區塊序數 $ae^{j\phi}$ 與 $ae^{-j\phi}$ 是共軛複數，將經由振幅提升機構提升振幅從 a 提升為 a' 。在適應性相移鍵控方面，相位角 ϕ 是依信號振幅及 m 調制為 ϕ' 。實際上的信號成為 $a'e^{j\phi'}$ 與 $a'e^{-j\phi'}$ ，其中的相位角 ϕ' 已經隱藏了密秘資料。上述的工作一直重複直到將所有秘密資料都完成隱藏，此影像註記為 Z' ，再經由數位傅立葉反轉換將資料轉換成影像格式後註記為 Y ，才算完成藏入數位浮水印工作，詳細的作法將簡略說明於後。



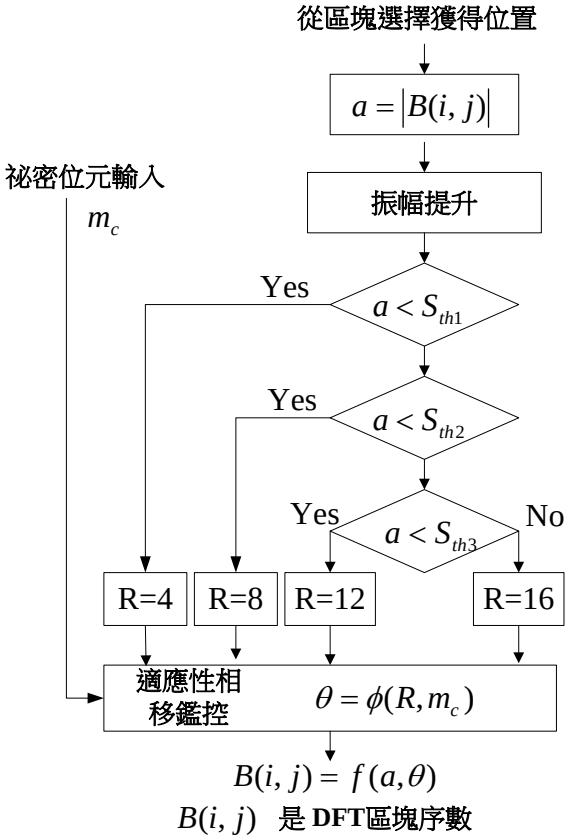
圖二、 數位浮水印的隱藏流程圖

(一)適應性相移鍵控

適應性相移鍵控是將信號相位依振幅大小自動改變的一種機制。在我們的方法中，四種調制強度被用來作為秘密資料的隱藏。詳細過程如圖三所示。在適應性相移鍵控方面。秘密資料位元與信號序數是輸入參數，而調制後的序數是輸出。在開始進行調制時，使用跳頻方法先選擇被調制的區塊，再選擇係數的振幅a。然後再檢查振幅，假如振幅值小於門檻值S_{th1}，然後振幅提升機構 AB 將信號振幅提升至S_{th1}，因為這種振幅才能抵抗雜訊的干擾。在相位調制方面，我們將振幅分為 4 種等級($R=4$, $R=8$, $R=12$ 與 $R=16$)作為相位($s=1/2$, $s=1/4$, $s=1/6$ 與 $s=1/8$)調制使用。至於如何找到最佳的門檻值就如圖三所示，依據圖三的流程就很容易的找到門檻值與振幅，相位角之間的相關性。當所有區塊的係數都調制完成後，則適應性相移鍵控的資料隱藏工作才算完成。所使用的數學公式如公式(2)-(3) 所示。

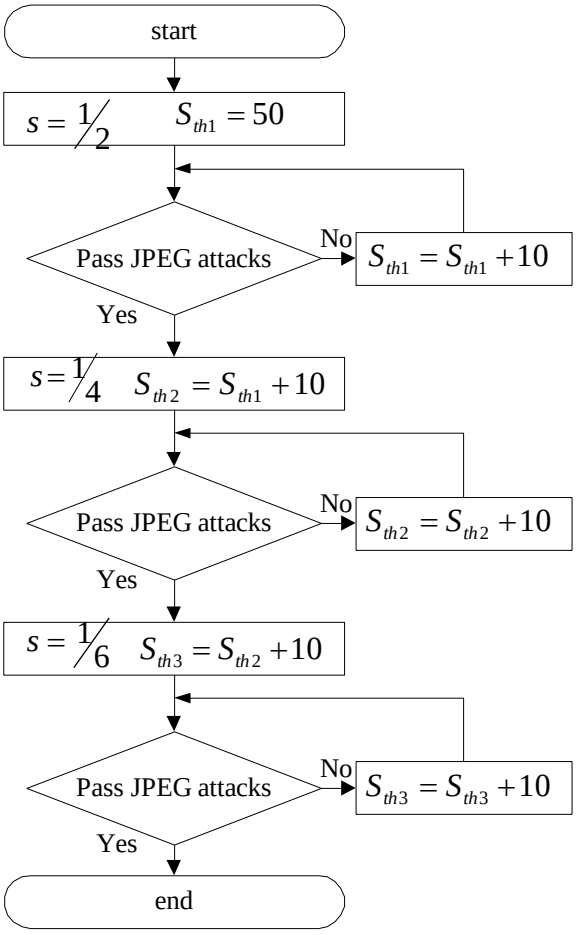
$$\angle\theta = \phi(R, m_c) \tag{2}$$

$$B(i, j) = a \cdot e^{j\theta} \tag{3}$$



圖三、適應性相移鍵控流程圖

圖四是相位範圍參數設定流程圖，流程圖中清楚看出一開始時將S_{th1}設為 50，並將 S 設為 1/2，若門神值越高則 S 值就設為較低，如此可達到最佳的影像品質效果。又能將相位角依秘密資料位元來改變。最後達成 S 分為 4 種類別的效果，詳細流程請看圖四中的說明。



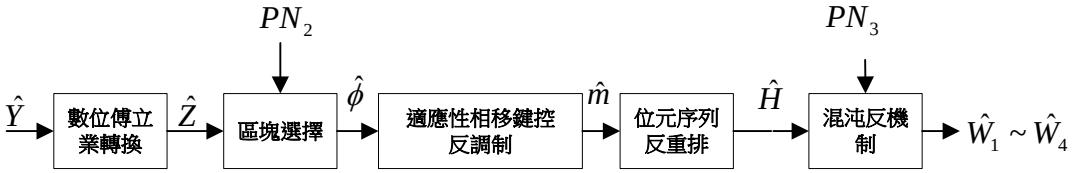
圖四、相位範圍參數設定流程圖

四、擷取浮水印演算法

(一) 浮水印擷取流程

在浮水印隱藏步驟中，為保存數位影像的品質，我們採用適應性相移調制技術及最近接角度選擇法。為了達成浮水印的安全性我們使用了混沌機制，搭配亂數系列，使惡意攻擊者無法破壞。在浮水印擷取步驟中，其方法是與浮水印隱藏時採用相同方法，只是步驟倒反而已。圖五是數位影像浮水印擷取流程圖。首先將已隱藏之數位浮水印影像 $\hat{Y}$ 經由數位傅立葉轉換產生 $\hat{Z}$ 資料.在 $\hat{Z}$ 資料中使用相同於浮水印嵌入時的亂數系列 PN_2 找出正確的區塊。在正確的區塊中使用適應性相移鍵控反調制技術 APSK demodulation 取出隱藏在相位角 $\hat{\phi}$ 中的秘密位元資料 $\hat{m}$ 。繼續的步驟是將秘密位元資料

重新排序，使其依照嵌入時的格式 $\hat{H}$ 。最後再經由反混沌機制還原出正確的浮水印 $\hat{W}_1 \sim \hat{W}_4$。讀者只需詳細推敲圖五的方塊圖即可了解浮水印的擷取過程。



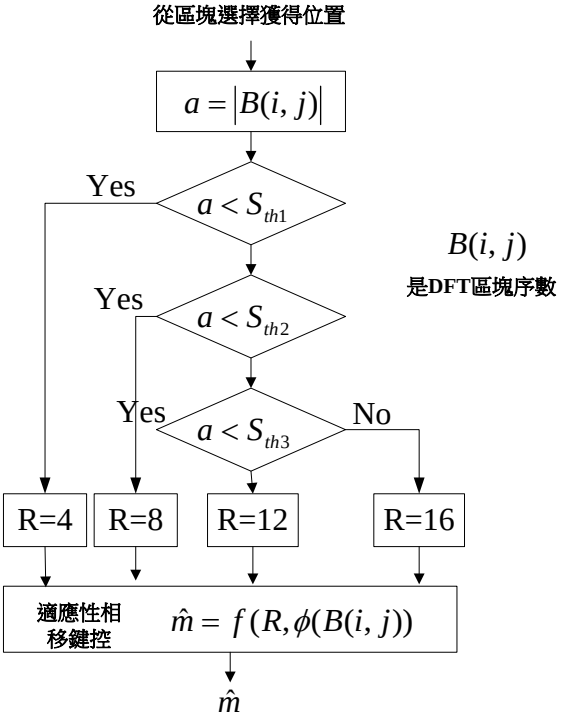
圖五、數位影像浮水印擷取流程圖

(二) 適應性相移鍵控反調制流程

適應性相移鍵控反調制流程是與調制作業順序相反，首先數位影像必須經傅立葉轉換後，依與浮水印嵌入時相同的順序區塊 $B(i, j)$。從區塊中取出對應於嵌入時的係數振幅 a，再經由檢驗 a 是落在那個門檻值的範圍，即可知是下列 4 種類別之一;(R=4, R=8, R=12,及 R=16) 。最後經由適應性相移鍵控反調制的數學式就可獲得秘密位元資料。適應性相移鍵控反調制的數學式如公式(4)所示，圖六是適應性相移鍵控反調制流程圖，從圖中讀者可以看出適應性相移鍵控反調制取出秘密資料的詳細過程。

$$\hat{m} = f(R, \phi(B(i, j))) \qquad (4)$$

其中 R 表示信號振幅的強度範圍。$\phi(B(i, j))$ 表示信號 $B(i, j)$ 的相位角。



圖六、適應性相移鍵控反調制流程圖

五、實驗結果

(一) 實驗環境設定

不可感知性對數位浮水印的影像隱藏是一項重要的因子，為了檢測本研究的隱藏效果，本研究以 PSNR 作為判斷影像品質的依據。PSNR 的數學公式如公式(5)所示。

$$PSNR = 10\log_{10} \frac{255^2}{\frac{1}{N \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (X(i, j) - Y(i, j))^2} \qquad (5)$$

其中 $X(i, j)$ 和 $Y(i, j)$，表示原始影像及已藏入數位浮水印影像在相對區塊中的係數 (i, j) 的灰階值，其尺寸大小為 $n = N \times N$。

在測試模擬中我們採用多個尺寸大小為512×512的影像做為測試影像，但由於篇幅限制的關係，我們只秀出一種影像的測試結果，在浮水印的選擇方面，本研究採用 4 種浮水印。資料顯示於下:1.是勤益科大的 Logo 尺寸為(32×32)。2.使用英文字符號 VR LAB (32×32)。 3.使用英文字 NCIT IEE (32×32)。 4.第四種是使用中文字"電子系的圖像。在信號振幅的門檻值判斷上設定為: S_{th1}=260，S_{th2}=350 ，S_{th3}=410 。

(二) 實驗結果

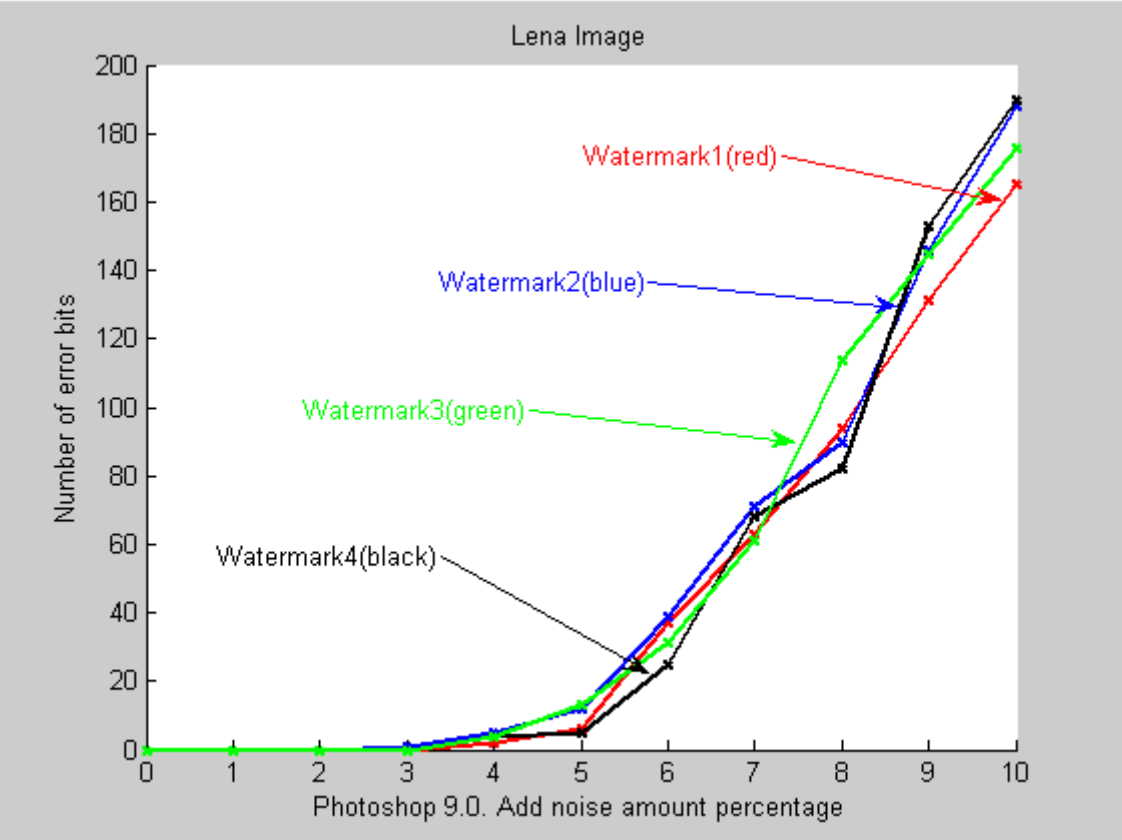
圖七是浮水印的攻擊測試圖，圖七(a)是 90 度旋轉攻擊測試影像圖，圖七(b)是改變影像大小之攻擊測試影像，圖七(c)是挖除測試影像的部份區域之攻擊測試圖，圖七(d)是塗抹部份測試影像之區域作為攻擊測試的情形，圖七(e)是將測試影像加入雜訊之攻擊測試圖。圖七(f)是將測試影像作糢糊化處理後之攻擊測試圖。表一是針對圖七影像攻擊測試後所獲得之浮水印與原始浮水印比對之錯誤位元表，從表一中我們可以清楚看出本研究方法所取回的 4 個浮水印都能清楚呈現，這表示錯誤率很低，由表中可以看出最大錯誤位元是 83，其錯誤率為 83/1024=0.081，只有百分之 8，很小，因此本方法是一種有效的浮水印演算法。

圖八是使用 photoshop 軟體所獲得之雜訊量與取回浮水印之錯誤位元數之曲線圖。圖八的水平軸表示將雜訊加入數位影像中作為一種破壞攻擊量，最右邊是加入百分之十的雜訊量。垂直軸表示取回之浮水印，其資料位元的錯誤量，最頂端表示值為 200。圖中的 4 條曲線代表 4 個被嵌入影像中的浮水印。

圖七、浮水印的攻擊測試;(a) 90 度旋轉攻擊測試，(b) 改變影像大小之攻擊測試, (c) 挖除部份區域之攻擊測試, (d) 塗抹部份區域之攻擊測試, (e) 加雜訊之攻擊測試,, (f) 糢糊影像之之攻擊測試

表一、針對圖七影像攻擊測試後所獲得之浮水印與原始浮水印比對之錯誤位元表

item	the rotated	the resized	the cropped	the painted	the noised	the blurred
W1						
W2						
W3						
W4						
W1 err. bits	0	37	77	67	59	6
W2 err. bits	0	55	78	71	62	3
W3 err. bits	0	43	83	80	72	2
W4 err. bits	0	59	71	64	73	5



圖八、使用 photoshop 軟體所獲得之雜訊量與取回浮水印之錯誤位元數之曲線圖

五、結論

數位通信調制技術有強大的雜訊排除能力。數位浮水印的機制是要能夠抵抗各式攻擊破壞，因兩者的物理現象相同。所以可以引用數位通信調制技術至數位浮水印演算法中會有良好的效果。

本研究採用適應性相位調制技術及發展出一種最近接相位角選擇法 nearest phase selection (NPS)作為數位浮水印的隱藏法，經過多種測試影像的模擬實驗結果。證實適應性相位調制技術能達成透明度 (Transparency)及強健性(Robustness) 。

參考文獻

[1] F. Alturki and R.Mersereau, "An Oblivious Robust Digital Watermark Technique for Still Image Using DCT Phase Modulation," *IEEE Int'l Conf. on Acoustic, Speech, and Signal Processing*, Vol.4,pp. 1975-1978,2000.

[2] W. Y. Chen and C. H. Chen, "A Robust Watermarking Scheme Using Phase Shift Keying with the Combination of Amplitude Boost and Low Amplitude Block Selection," *Pattern Recognition*, 38, 587-598 (2005).

[3] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images," *IEEE Trans. on Image Processing*, 8 (1) (1999) 58-68.

[4] N. Kaewkamnerd and K. R. Rao, "Wavelet Based Image Adaptive Watermarking Scheme," *Electronic Letters*, 36 (4) (2000) 312-313.

[5] G. C. Langelaar and R. L. Lagendijk, "Optimal Differential Energy Watermarking of DCT Encoded Images and Video," *IEEE Trans. on Image Processing*, 10 (1) (2001) 148-158.

[6] J. J. K. Q Ruanaidh, W. J. Dowling and F. M. Boland, "Phase Watermarking of Digital Images," *IEEE International Conference on Image Processing*, 3, 1996, pp. 239-242.

[7] V. Solachidis and I. Pitas, "Circularly Symmetric Watermark Embedding in 2-D DFT Domain," *IEEE Trans. On Image Processing*, 10 (465) (2001) 1741-1753.

[8] M. J. Tsai, K. Y. Yu and Y. Z. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking," *IEEE Trans. on Consumer Electronics*, 46 (1) (2000) 241-245.

[9] S. Voloshynovskiy, S. Pereira, T. Pun, J. Eggers and J. K. Su, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks," *IEEE Communications Magazine*, August 2001.

[10] C. F. Wu and W. S. Hsieh, "Digital Watermarking Using ZeroTree of DCT," *IEEE Trans. on Consumer Electronics*, 46 (1) (2000) 87-94.

作者簡介

陳文淵 Wen-Yuan Chen 教授任職於國立勤益科技大學電子工程系。早期主要研究數位浮水印技術，密碼學及資料壓縮技術。自 2007 年起亦同時研究影像辨識技術。