強健性雙域數位影像浮水印
Rabust Two-Domain Digital Image Watermarking

郭偉晟Wei-Shen Kuo, 胡懷祖Hwai-Tsu Hu,李昱廷Li-Ting Lee
國立宜蘭大學電子工程所
Department of Electronic Engineering
National Ilan University
r9542012@niu.edu.tw, hthu@niu.edu.tw, r9642010@ms.niu.edu.tw

摘　要

現今許多影像浮水印技術大多難以兼顧一般攻擊與幾何攻擊，所以本文的研究動機在於技術的兼併整合，讓浮水印能夠承受各式各樣的攻擊。實際的做法則是應用雙頻率域處理的方式來達到抵抗一般攻擊與幾何攻擊。

文中的雙域處理是採用Discrete Wavelet Transform（DWT）與Discrete Fourier Transform（DFT）。由於DWT具有多解析頻帶特性，因此我們將浮水印嵌入在最不易受到破壞的低頻區。另一方面，DFT在幾何特性中是具有不變性的，因此可用於抵抗幾何攻擊，我們的作法是在DFT的振幅頻譜中嵌入一個Trial template，作為抽取時判斷遭到幾何失真的可能性。

此外，為了提高浮水印的隱蔽性與安全性，我們應用展頻技術與渾沌理論，實驗結果發現，我們的雙域浮水印架構較許多獨立浮水印架構技術來得優越，PSNR（Peak Signal-to-Noise Ratio）可達到45dB，並且有效的抵抗一般攻擊（如：椒鹽雜訊、高斯雜訊、Jpeg壓縮…等）與幾何攻擊（如：旋轉、縮放、剪裁），證實是一種非常具有實用價值的強健性技術。

關鍵字：浮水印、小波、傅立葉、展頻、渾沌理論。

Abstract

As many current image watermarking technologies have difficulty to cope with general and geometric attacks at the same time, the motive of this thesis is thus to integrate a variety of technologies to allow the watermark to survive under various malicious attacks. In actual practice, a dual-domain watermark embedding scheme is developed for such a purpose.

In our study, the dual-domain watermarking employs the Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). The DWT has multi-band resolution properties so that the watermark can be embedded in the low-frequency band that is less susceptible to damages. On the other hand, the DFT has the invariant geometric properties that can withstand geometric attacks. Our scheme is to embed a trial template in the amplitude DFT for judging the possibility of geometric distortion during the process of watermark extraction.

In addition, in order to enhance the obscurity and security of the watermarks, we have used the spread spectrum technique along with chaos theory. The experiment results show that our dual-domain watermark frame is superior to many others. Not only its PSNR can reach 45 dB, but it can effectively shield against general attacks (e.g. salt and pepper noise, Gaussian noise, JPEG compression, etc.) as well as geometric attacks (e.g. rotating, zooming, cropping, etc.). This study will prove that our scheme constitutes a very effective and robust watermarking algorithm.

Keywords: Watermark, DWT, DFT, Spread Spectrum, Chaos Theory.

1 引言

離散小波轉換（discrete wavelet transform, DWT）是近年來在數位訊號處理方面是非常重要的技術[1]，DWT 具有將影像中的高、中、低頻成份分離解析的能力，其中低頻訊號對一般攻擊的抵抗能力較高[2][3]，因此浮水印常嵌入低頻帶，以達到對一般攻擊的高強健性。

即使藏身於低頻區的浮水印能順利躲過一般攻擊，但對幾何攻擊（如：旋轉、縮放）仍舊束手無策，因此我們便藉助離散傅立葉轉換（discrete Fourier transform, DFT）的幾何不變特性[4]來克服這個問題，做法是在嵌入流程裡DFT的振幅頻譜中嵌入一個Trial template，此Template的Peak points能夠在抽取浮水印時判斷遭受何種幾何攻擊，並將影像還原，使得該架構在幾何攻擊下仍有極佳的強健性。

除了高強健性之外，此架構在隱蔽性與安全性方面也須考量，我們利用展頻（Spread Spectrum）以比較式的方式來嵌入浮水印[6][7]，如此便能大幅降低浮水印的嵌入強度，以使浮水印的隱蔽性提高。在安全性上我們則應用渾沌理論（Chaos theory）產生的亂數將浮水印打亂，以達到浮水印的安全性保護。

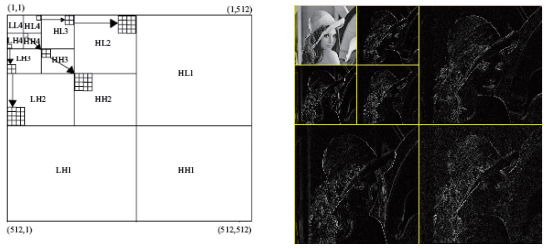
在上述的架構下，我們能有效解決其它論文無法同時抵抗一般攻擊與幾何攻擊的缺點，然其強健性與他人研發之方法相當，在PSNR（peak signal-to-noise ratio）上能高達45db。本文於第1節交代引言，第2節說明頻域處理，並簡介DWT、DFT，第3節討論安全性技術，同時介紹渾沌理論（Chaos theory）所產生的亂

數，第4節闡述展頻技術，第5節探討嵌入流程，第6節則說明抽取流程，第7節為實驗結果與數據，末了在第8節給予結論與未來展望。

2 頻域處理

2.1 Discrete Wavelet Transform（DWT）

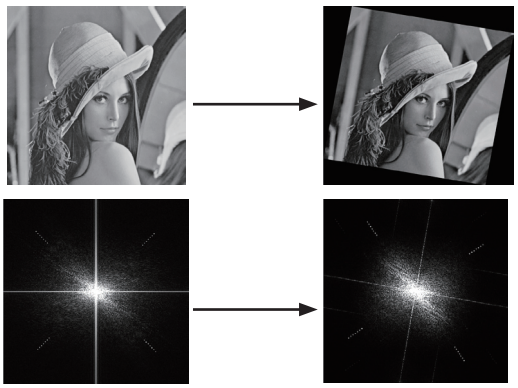
DWT具有濾波器特性，可對影像依高低頻做多層解析，圖一中將Lena圖分解為低頻帶LL，中頻帶LH、HL，高頻帶HH，在我們的架構中主要是將易於遭受破壞的高、中頻資訊分離，取低頻資訊來嵌入浮水印，以達到對一般攻擊的強健性[1-3]。



圖一　左圖為4階小波多解析，右圖為Lena的2階小波轉換示意圖

2.2 Discrete Fourier Transform（DFT）

DFT轉換在頻率域中是具有幾何不變性的，因此本篇論文對影像做DFT轉換後於振幅頻譜（Magnitude spectrum）中嵌入Peaks，在抽取架構中以判斷其Peak points來決定是否被旋轉、縮放，如圖二所示，當空間旋轉處理後，對應到的頻域仍是呈現相同的轉移（Translation）情況。文獻[4]對DFT的幾何特性有詳細敘述。



圖二　Lena空間域與頻率域旋轉示意圖

3 安全性技術

3.1 渾沌理論（Chaos theory）

在影像浮水印中浮水印的安全性是非常重要的，我們使用渾沌理論所產生的亂數來保護浮水印，因為在渾沌理論之下，分歧參數的些微改變即產生不同的亂數，如此即可當保護浮水印的key，在抽取過程中必須有此key才能還原浮水印，如此即可達到保護浮水印（令為W）。

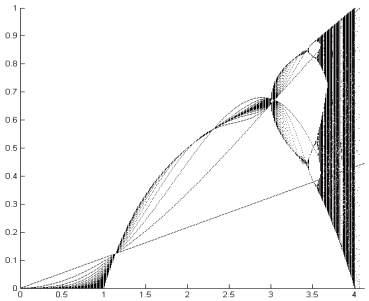
渾沌理論數學式如下：

$$x_{k+1}=\mu x_k(1-x_k) \quad (1)$$

其中x為系統狀態，介於0~1間，μ為分歧參數，n為離散時間。

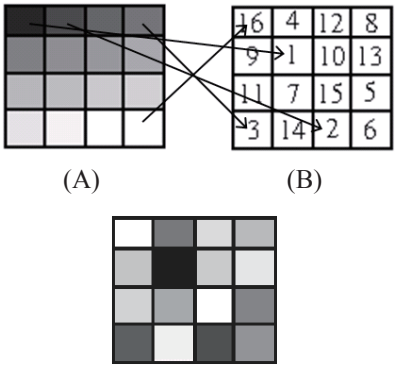
以下為渾沌亂數產生，例如我們可取初始值x_1=0.1234，分歧參數μ由μ=1依迴圈次數每次加0.01代入式(1)中，至μ=4.5，此為圖三之橫軸，每次μ值迴圈執行一次迭代3000次，經計算後得圖三渾沌亂數狀態圖。

由圖三中可以清楚發現當橫軸μ值約在3.57~4中有很明顯的亂數變化，因此我們將之運用到此浮水印的亂數處理。



圖三　渾沌亂數狀態圖（橫軸：μ值，縱軸：x值）

本文所取用的起始值x_1=0.5，μ=3.9996824，浮水印W大小為62*62，多次迭代直到產生不重覆之1~3844(62*62)的一維亂數矩陣，再將此矩陣轉換為二維矩陣，並將浮水印位置對應到亂數矩陣中，圖四為簡易說明圖。



圖四　(A)為預設浮水印矩陣，(B)為亂數矩陣，(C)為亂數處理浮水印

依上述方法所得之浮水印亂數如下，在此先將亂數處理後的浮水印定義為W_d，型如圖五所示。

圖五　原始W和亂數處理後之W_d

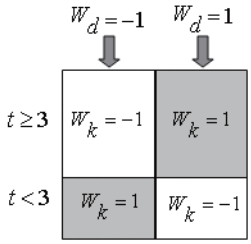
4 展頻技術

展頻技術（Spread spectrum）[7]之概念原應用於通訊領域，主要是利用雜訊產生器產生之雜訊，並將原易判斷之傳送資料隱入雜訊之中，因展頻後之訊號的能量較小，藏於雜訊中不易被察覺，也比較不會受到通訊干擾與惡意攻擊，而接收端必須使用與傳送端相同之雜訊產生器才可無誤擷取藏於雜訊中之訊號資料。

在我們的架構中，利用展頻技術嵌入浮水印的主要目的在於降低浮水印嵌入影像中的強度，如此便能提高浮水印的隱蔽性。做法如下：依展頻嵌入式(2)可發現當1 pixel大於等於周圍8 pixel 3次，且$W_d(i,j)$=1者，$W_k(i,j)$=1，反之$W_k(i,j)$=-1。

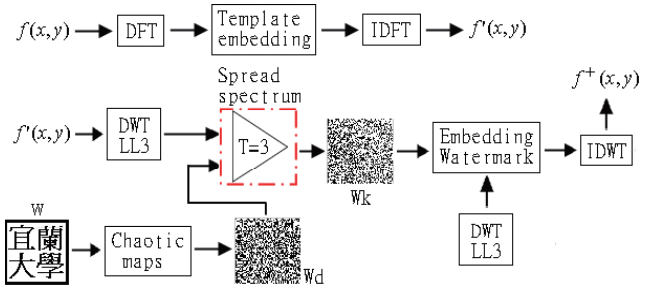
$$W_k(i,j)=\begin{cases}1 & if\,(t\geq 3\ and\ W_d(i,j)=1)\ or\\ & (t<3\ and\ W_d(i,j)=-1)\\ -1 & else\end{cases} \qquad (2)$$

其中t為LL3中每個pixel大於周圍8個pixel次數，式(2)處理過後的W_k即為展頻矩陣。經實驗得知，t值取2 or 3是有較佳的效果。

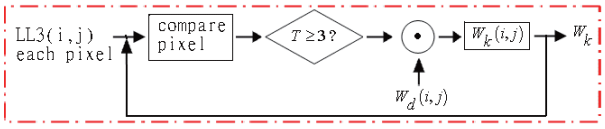


圖六　展頻示意圖

5 嵌入流程



圖七　嵌入架構圖

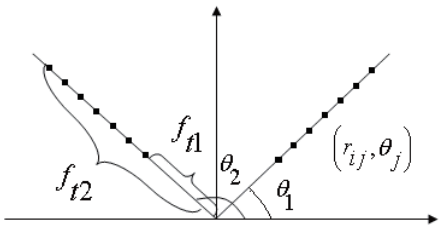


圖八　展頻嵌入示意圖

完整的浮水印嵌入動作如圖七所示，其執行步驟如下：

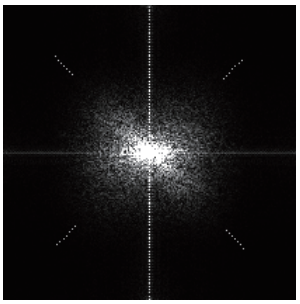
步驟一、將512*512 Lena原始影像補0至1024*1024後做DFT轉換，補0目的為提高DFT轉換後的頻譜解析度。

步驟二、取振幅頻譜中嵌入Template，示意圖如下：



圖九　Template model示意圖

產生一個不包含任何資訊的Template，並將其嵌入振幅頻譜中[5]，其中θ_1、θ_2為嵌入振幅的角度，在此皆取45°，f_{t1}、f_{t2}為振幅頻譜嵌入點的半徑範圍，取中頻嵌入可降低影像失真，在此f_{t1}取200，f_{t2}取305，r_{ij}為嵌入peak points位置，其半徑位置可由亂數產生峰值位置，或給定，在此給定每個峰值的r_{ij}距離為7，頻譜之上平面嵌入後下半平面亦對稱比照，取上下兩平面的原因在於傅立葉轉換有以中心點對稱的特性，因此必須以對稱方式嵌入，如圖十。



圖十　Template model 嵌入到振幅

再將嵌入Template之振幅做反傅立葉轉換（IDFT）後得空間域之$f'(x,y)$。

步驟三、將$f'(x,y)$透過DWT轉換後取LL3低頻帶當嵌入區域。我們將渾沌亂數產生之亂數浮水印W_d與LL3做頻譜擴展，展頻的嵌入方式如公式(2)所示。

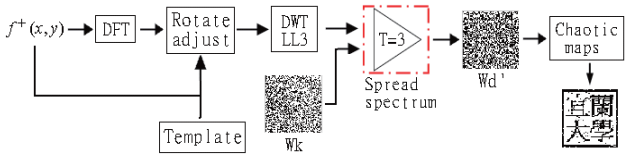
步驟四、將W_k嵌入至DWT LL3低頻帶中，嵌入式如下：

$$\hat{I}(i,j)=\tilde{I}(i,j)+\alpha\cdot W_k(i,j)\cdot\left|\tilde{I}(i,j)\right| \qquad (3)$$

$\hat{I}$：為已嵌入浮水印之DWT LL3係數
$\tilde{I}$：為原始DWT LL3係數
W_k：為展頻浮水印
α：為浮水印嵌入強度

步驟五、將嵌入後之係數$\hat{I}$放入LL3係數中後以IDWT還原為已嵌入浮水印之影像空間域。

6 抽取流程



圖十一　抽取架構圖

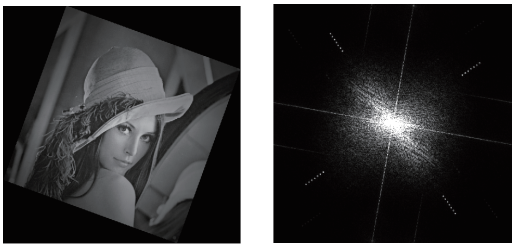
我們的影像浮水印架構是採雙域處理，當待測影像抽取浮水印時，會先經過DFT判斷是否遭到幾何攻擊，若無則再經由DWT程序抽取浮水印，因此在抽取架構中我們採用旋轉攻擊來說明此架構如何有效抵抗旋轉攻擊。

步驟一、$f^+(x,y)$為被旋轉攻擊之浮水印影像，將$f^+(x,y)$冠上Bartlett window產生一遮罩影像，式(4)為Bartlett window一維學數式。

$$w(n)=\frac{2}{N\text{-}1}\times\left(\frac{N\text{-}1}{2}-\left|n-\frac{N\text{-}1}{2}\right|\right) \tag{4}$$

我們先將影像$f^+(x,y)$每列像素做Bartlett window的加權乘機，再對其每行做相同處理，如此可得圖十二之左圖。

加Bartlett window的目的在於降低因DFT所造成的邊緣不連續誤差。接著再對周圍補0擴充至1024*1024，目的為提高解析度，之後再對該影像做DFT轉換後所得之振幅頻譜圖，如圖十二之右圖。



圖十二　左圖為被攻擊浮水印影像（Bartlett window處理），右圖為DFT振幅頻譜

步驟二、尋找Peaks峰值點，並記錄其角度θ_1，θ_2與半徑r_{ij}，與原Template比較後可得到被旋轉攻擊角度θ_{diff}後，對$f^+(x,y)$做-θ_{diff}旋轉，之後再去掉外圍黑框即可。對於縮放攻擊，則依抽取Peaks的r_{ij}與原Template model比較即可得知被縮放攻擊，我們只要再反縮放回來即可。

步驟三、將還原後的影像做DWT取LL3 subband，再取原展頻矩陣W_k做展頻抽取出浮水印，式子如下：

$$W'_d(i,j)=\begin{cases}1 & if\,(t'\geq 3\ and\ W_k(i,j)=1)\ or\\ & (t'<3\ and\ W_k(i,j)=-1)\\ -1 & else\end{cases} \tag{5}$$

步驟四、再對W'_d做反Chaotic maps還原為浮水印W'。

圖十三　抽取旋轉攻擊後之浮水印

7 實驗結果與數據

經研究結果發現我們的架構不僅能抵抗許多一般攻擊，同時也能抵抗幾何攻擊，我們將此架構與文獻[6]來比較，在一般攻擊的強健性相當，但在幾何攻擊（如：旋轉、縮放）則由本架構勝出。

在此我們以常見的攻擊類型來分別檢討，這包括椒鹽雜訊、高斯雜訊、Jpeg壓縮、馬賽克、低通濾波、扭曲、旋轉、縮放、剪裁等。未攻擊前的影像與浮水印如圖十四所示。

圖十四　原始影像512*512與浮水印62*62

嵌入後之浮水印影像PSNR=45.1144，隱蔽性相當高，當PSNR超過37人眼便難以判斷差異，一般影像浮水印相關研究PSNR約在40以上。就算式而言，PSNR計算如下：

$$RMSE=\left[\frac{\left[f(i,j)-f^+(i,j)\right]^2}{M*N}\right]^{1/2} \tag{6}$$

$$PSNR=20\log_{10}\left(\frac{255}{RMSE}\right)$$

其中M、N分別代表影像的長與寬。而Normalized Correlation（NC）則是常拿來判斷浮水印失真度：

$$NC=\frac{\sum_i\sum_j w(i,j)\,w^+(i,j)}{\sum_i\sum_j\left[w(i,j)\right]^2} \tag{7}$$

表1即各攻擊之測試結果，在實驗中，我們採用椒鹽雜訊、高斯雜訊、Jpeg壓縮、馬賽克、低通濾波、漩渦、旋轉、縮放、剪裁攻擊來做浮水印攻擊研究，這些攻擊是由較常用之Adobe Photoshop CS3以及Matlab所產生，其中馬賽克的攻擊類型為單元格，此單元格是將浮水印影像切割為N*N格，並計算每個N*N之平均值，然後將平均值放入N*N矩陣中，使N*N矩陣值皆相同，此N即為單元格。

表1　椒鹽、高斯、Jpeg壓縮、馬賽克攻擊結果圖

椒鹽雜訊	NC(*W*)	高斯雜訊	NC
雜訊度		雜訊度	
0.01	0.88	0.001	0.89
0.02	0.84	0.003	0.85
0.03	0.76	0.005	0.8
0.04	0.74	0.007	0.78
0.05	0.72	0.009	0.76
0.06	0.68	0.011	0.743
0.07	0.67	0.013	0.72
0.08	0.66	0.015	0.706
0.09	0.64	0.02	0.67

Jpeg壓縮	NC	馬賽克	NC
影像品質		單元格	
70	0.97	2	0.99
60	0.96	3	0.95
50	0.906	4	0.93
40	0.89	5	0.87
30	0.85	6	0.86
20	0.746	7	0.81
10	0.58	8	0.84
		9	0.74
		10	0.68

7.1 低通濾波

圖十五　低通濾波（NC=0.976）

在低通濾波攻擊中我們將待測影像中每點pixel含周圍8個pixel相加，之後取平均值再放入選取的pixel位置，如此處理後影像有如平滑處理一樣。

7.2 漩渦

圖十六　依中心漩渦角度=30°之結果

在漩渦攻擊上抵抗力稍弱，原因為以中心起始漩渦對外圍並無旋轉，但依然有30°的表現，此NC=0.7319。

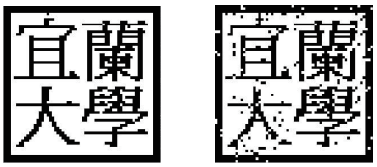
7.3 旋轉

表2　本架構與文獻[6]之旋轉攻擊結果

旋轉	本架構	文獻[6]
	NC(W)	NC(W)
角度		
2	0.877	0.42
5	0.876	0.374
10	0.877	0.307
15	0.867	0.234
35	0.878	0.1
-18	0.876	0.2
-30	0.875	0.13
-42	0.877	0.08

由表2可發現本文中運用了Template將Peak points嵌入DFT中，經比對後能夠有效計算出遭到旋轉攻擊，並將其還原，以解決旋轉攻擊，而文獻[6]的方法遭遇到些微角度的旋轉便無法抵抗攻擊，因此在旋轉攻擊方面由我們的架構勝出。

7.4 縮放



圖十七　左圖為放大攻擊（900*900）後所抽取之浮水印，右圖為縮小攻擊（200*200）後所抽取之浮水印。

在縮放攻擊中，我們透過Template的Peaks半徑r_{ij}可以有效且準確判斷影像浮水印是否遭到縮放，並且將影像浮水印還原，在文獻[6]中縮放攻擊是不被允許的，因為沒有可判斷縮放的技術，因此無法抵抗縮放攻擊。

縮小攻擊抵抗較差是因在影像內縮攻擊時遺失資訊較為嚴重，圖十七之左圖NC=0.9967，右圖NC=0.9058。

7.5 剪裁

圖十八　剪裁攻擊與結果

在剪裁攻擊上，由於我們在流程中應用渾沌理論將浮水印做亂數處理後再嵌入低頻區，因此當影像遭剪裁，浮水印仍能有效辨識。此NC=0.6538。

8 結論與未來展望

本文主要目標為透過雙域處理來達到一般攻擊與幾何攻擊上的兼顧，以提高影像浮水印面對許多攻擊上的強健性。

但在其它部分仍有待改進，未來可進一步在頻譜中結合錯誤更正碼，用以對遭破壞之浮水印進行還原，也可將嵌入方式改為影像特徵值方式來嵌入，可抵抗更多攻擊類型，更可加上著作財產權認證系統，將影像浮水印有效應用於生活上，以發揮數位影像浮水印之真正價值。

參考文獻

[1] G. Woods, *"Digital Image Processing 2/e* (*Chinese edition*),*"* pp.374-431.

[2] D. Lee, T. Kim, S. Lee, and J. Paik, *"A Robust Watermark Algorithm Using Attack Pattern Analysis*,*"* ACIVS 2006, LNCS 4179, 2006, pp.757-766,

[3] J. J. Chas, B. S. Manjunath, *"A Robust Embedded Data from Wavelet Coeffiients*,*"* Department of Electrical and Computer Engineering, PP.1-10.

[4] D. Zheng, J. Zhao, *"RST Invariant Digital Image Watermarking Based on Log-Polar Mapping and Phase Correlation*,*"* IEEE Transactions On Circuits And Systems For Video Technology, Vol. 13, No. 8, Aug. 2003, pp.753-765.

[5] X. Kang, J. Huang, *"A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression*,*"* Circutes and Systems For Video Technology, Vol. 13 No. 8, August 2003, pp.776-786.

[6] S. Mabtoull, E. Ibn-Elhaj, and D. Aboutajdinel, *"A Blind Chaos-Based Complex Wavelet-Domain Image Watermarking*,*"* IJCSNS International Journal, Vol. 6, No. 3, 2006, pp.134-139.

[7] Y. Yi Yang, D. Chun, and W. Wen Hsiang Tsai, *"Watermarking of Numerical Databases Using Spread Spectrum Techniques*,*"* pp.1-6.

[8] S. Pereira, T. Pun, *"Robust Template Matching for Affine Resistant Image Watermarks*,*"* IEEE Transaction On Processing, Vol. 9, No. 6, June 2000, pp. 1123-1129.

[9] Z. Dawei, C. Guanrong and L. Wenbo, *"A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm*,*"* Chaos, Solitons and Fractals, Vol. 22, Oct. 2004, pp. 47-54.

[10] A. McAndrew, *"Introduction to Digital Image Processing with MATLAB"* (Chinese).

作者簡歷

郭偉晟（Wei-Shen Kuo）（71-02-26），男，臺灣臺北市人，學生。碩士畢業於宜蘭大學，學士畢業於大華技術學院，專長為影像處理、數位訊號處理。

胡懷祖（**Hwai-Tsu Hu**）現為國立宜蘭大學電子工程學系教授。

photo not provided

李昱廷（**Li-Ting Lee**）現為國立宜蘭大學電子工程學系碩士班學生。