

灰階碎形影像與隱像術之研究

洪維恩

育達商業技術學院資訊管理
研究所助理教授
wienhong@ydu.edu.tw

許志維

育達商業技術學院資訊管理
研究所研究生
95104503@ydu.edu.tw

蔡雅純

育達商業技術學院資訊管理
研究所研究生
95104504@ydu.edu.tw

摘要

「碎形壓縮」是在影像壓縮技術之中，被廣為探討的一項議題。這項技術是運用影像的自我相似的原理，透過一系列的演算法，將原始影像進行壓縮，產生出較小的PIFS (Partition Iterated Function System) 碼，以降低影像儲存的空間。

傳統的隱像技術，多半是將資訊藏入原始影像的空間域，或者是頻率域上。此外；利用編碼方式來完成資訊藏入的技術，多集中在VQ (Vector Quantization) 的編碼，而使用碎形壓縮來達成隱像技術的研究並不多見。

本研究將要探討的內容，即是透過碎形壓縮技術來達到資訊隱藏的目的。其方法是使用碎形碼 (PIFS) 中的位置轉置參數，作為分群的依據，以便藏入大量的資訊。與傳統的方式比較起來，不但能夠藏入更多的資訊，還能維持影像的品質。

關鍵字：碎形壓縮、隱像術、資訊隱藏

1. 前言

隨著網際網路的成長，使用者能夠透過網路快速的重置、儲存或傳遞各種資料，卻也造成資訊安全性變得相當薄弱。以現今電腦使用者的習慣，依舊沒有辦法避免有關於網路侵權的問題發生。因此資訊隱藏便是為了提高其資訊安全性，進而確保重要資訊不落入駭客手中所發展的技術。而本研究要探討的主軸，即是該如何有效保護資訊的安全。

隱藏技術是將資訊藏入影像中，較不重要的區域，主要是確保資訊不會輕易的遭受竊取和破解，並且達到混淆第三者的視覺。這類技術運用在數位影像上的研究，大致上可分為兩種。一是在影像中嵌入數位浮水印，作為個人版權宣告的用途，藉以保護原擁有者的智慧財產權。這項技術多半著重於能夠抵抗外在的攻擊。另一種則是用於保密通訊，是將重要的資訊藏在數位影像中，使影像在外流的情況之下，資訊依然不會受到侵害。

其中保密通訊，也就是所謂的隱像術 (Image Hiding)。它是將資訊藏入一般的數位影像內容裡，讓擷取者認為該影像不具任何效益，便不加以破壞。一般來說這項技術不容易從視覺上查出藏入的資訊，因此可以在公用的平台上使用該影像，不須擔心藏入的資訊輕易的被第三者竊取。

1988年，Barnsley[1]率先開發碎形壓縮技術，但由於當時並沒有公開其作法，使得許多學者紛紛投入相關的技術研究，卻都沒有辦法完全瞭解其中的奧密。直到1990年Barnsley的學生Jacquin[2]發表了相關的論文，後人才能夠全盤瞭解碎形壓縮的技術，因此至今相關於碎形壓縮的學術研究都以此為基礎。

本研究所使用的是一般碎形壓縮技術，將會在第二節提出相關的作法。而有關於本研究提出的位置轉置參數分群法，將在第三節中做更詳細的說明與討論。

2. 文獻探討

1988 年，Barnsley 利用迭代函數系統 (Iterated Function System, IFS)，以影像的自我相似為基礎，將該影像壓縮並建立在碎形上。由於 Barnsley 宣稱能夠達到一萬倍的壓縮率，因此受到大家的重視，但有限於該演算法並未公開，於是各方學者無法瞭解其中的做法。

直到 1990 年，其學生 Jacquin 提出了分割迭代函數系統 (Partitioned Iterated Function System, PIFS)，並公開其相關演算流程，才使得碎形壓縮技術受到相當大的迴響。

2.1 灰階碎形壓縮影像

Jacquin 所提出的分割迭代函數系統 (PIFS) 是藉由影像區塊的自我相似性進行編碼。如圖 2.1，可發現在同一張影像裡，能夠找到大小不同，但其變化性幾乎相同的結構。

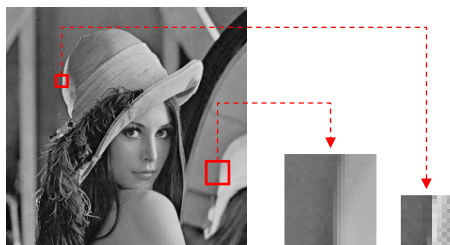


圖 2.1 相似的兩區塊

因此 Jacquin 將影像以不重疊的方式，分割成 $R \times R$ 的區塊，這些區塊 (Range Block) 統稱為值域 (Range Pool)。然後在同一張影像，以重疊的方式劃分 $D \times D$ 的區塊，所有的定義域區塊 (Domain Block) 統稱為定義域 (Domain Pool)。

為了方便計算通常會讓 $D_{size} = 2R_{size}$ ，使 $D_{size} > R_{size}$ 。接著值域裡的每一個區塊 R_i ，可以在定義域中找到最相近的 D_i ，如圖 2.2。

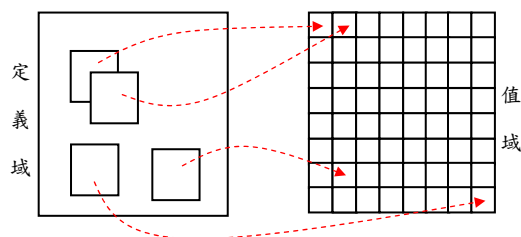


圖 2.2 值域與定義域之最相似區塊表示圖

利用自我相似的原理，讓所有的值域區塊 R_i 找到最契合的定義域區塊 D_i 。若以 3 維的座標來描述它， x 軸和 y 軸是用來表示影像上每個像素的位置， z 軸用來表示該像素的灰階值。根據 PIFS，可以得到如式 (2-1)。

$$W_i \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a_i & b_i & 0 \\ c_i & d_i & 0 \\ 0 & 0 & s_i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} e_i \\ f_i \\ o_i \end{bmatrix}, \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} = i_i \quad (2-1)$$

其中 s_i 為控制影像的對比度 (scaling)， o_i 則是明亮度， e_i 與 f_i 分別代表 R_i 與 D_i 的相對座標位置，而 i_i 則代表著控制區塊的形狀大小與旋轉角度。藉由這五項參數，記錄著轉換的規則，如收縮、平移、旋轉和灰階對應轉換，可寫成如式 (2-2)。

$$\hat{R}_k = s_i(i_i(A_i D_j)) + o_i \quad (2-2)$$

A_i 表示利用 e_i 與 f_i 所找到的定義域相對位置與收縮轉換。簡單的說，就是讓定義域區塊的大小收縮成與值域區塊的大小一樣。 i_i 為翻轉參數， s_i 為灰階對應轉換之斜率值，同前所述的控制影像轉換之對比度。 o_i 為此灰階對應轉換的 y 截距，同前所述的控制影像轉換之明亮度。

每一個值域區塊，在所有的定義域區塊中找到最契合的一個區塊時，通常會以最小距離求出兩者的誤差值，如式 (2-3)。數值越小表示該值域區塊與定義域區塊越接近。當找到誤

差為最小值時，即記錄當時轉換的參數，也就是 $[e_i, f_i, i_i, s_i, o_i]$ 五項參數來作為碎形碼。

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n (R - \hat{R}_k)^2 \quad (2-3)$$

相較於尋找最佳的碎形碼，解碼就容易多了，由於碎形擁有自我相似迭代的規則，因此利用此規則即可得到相似影像的原理。此外；還原影像並不需要任何原始影像的資訊，僅需同樣大小的圖形即可（全黑或全白影像亦可）。

透過式（2-2），利用自我相似的規則轉換之後，即可獲得一張較類似於原始圖片的影像。再經過數次的迭代還原，就能取得一張近似於原始圖的影像。

2.2 相關研究

由於本研究是以 Joan Puate 和 Fred Jordan[3]提出的演算法為基礎架構，因此特別說明其相關作法。[3]的演算法是透過區域搜尋（Local Searching Region, LSR）的概念，將資訊藏入位置轉置參數 e_i 與 f_i 。如圖2.3，值域區塊僅從自身周圍來搜尋最契合的定義域區塊。

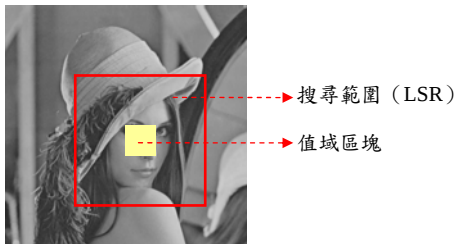


圖2.3 值域區塊搜尋的範圍

接著將搜尋範圍劃分出2個區域LSR-0和LSR-1，當嵌入的資訊為1時，就搜尋LSR-1的區域；反之當嵌入的資訊為0時，則由LSR-0的區域來搜尋，如圖2.4。

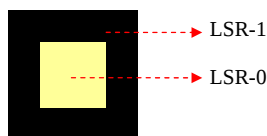


圖2.4 資訊嵌入的規則

如此在產生碎形碼 $[e_i, f_i, i_i, s_i, o_i]$ 之後， e_i 與 f_i 便帶有藏入的資訊。但由於 e_i 與 f_i 兩項參數容易遭到破解，所以只保留 i_i 、 s 與 o_i 作為金鑰，以避免重要資訊遭受竊取的問題發生。

在取出資訊時，則透過 i_i 、 s 與 o_i 三個金鑰，反推出 e_i 和 f_i 的值，再根據這兩項參數判斷其落點是位於哪一個區塊（即LSR-0或LSR-1）。如此一來，即可取出嵌入的資訊。

3. 研究方法

由於Joan Puate和Fred Jordan所提出的演算法能夠藏入的資訊量並不多，因此[3]的兩位作者將其應用在數位浮水印上。實際透過[3]的演算法，假設將一張 $M \times N$ 的影像，以不重疊和重疊的方式，劃分出 $R \times R$ 個值域區塊與 $D \times D$ 個定義域區塊，並按照[3]的方法來藏入的資訊。能夠發現資訊藏入的數目與值域區塊數目息息相關，和定義域區塊的數量就沒有直接的關係，此外定義域區塊的數量往往比值域區塊多上數十倍。所以若能夠利用以上的特點，將定義域作為資訊藏入的依據，即可讓嵌入的資訊量大大提升。

再者，位置轉置參數法的LSR區域並沒有依照圖片的特性，而是將影像分成LSR-0與LSR-1。所以當圖片的LSR-0與LSR-1區域反差相當高時，尋找最佳的定義域區塊，就會造成不夠客觀的問題發生，藏入資訊後的影像品質也會下降。

有鑑於此，本研究方法改良[3]的演算法，提升資訊能夠隱藏的數量，並且維持影像的品質。

3.1 位置轉置參數分群 (Position Classify Group)

本研究提出的位置轉置參數分群法 (Position Classify Group, PCG)，是將定義域劃分成若干個群組，再根據所嵌入的浮水印來決定搜尋的定義域為哪一個區域。

其分群的方式是依照定義域區塊座標的 e_i 與 f_i 。首先將 e_i 分群為 M_a ，其中 $a = \text{mod}(e_i, 16)$ ，如此可以得到 M_0 至 M_{15} ；而 f_i 分群為 N_b ，其中 $b = \text{mod}(f_i, 16)$ ，可得到 N_0 至 N_{15} 。接著將 M_a 與 N_b 交錯配對，產生出 256 個平面分群 $PCG(M_a, N_b)$ ，再讓 $PCG(M_a, N_b)$ 依序代表 0 到 255，如表 3.1。

表 3.1 以 2 維方式表示 PCG 的分群代號

	M00	M01	M02	M03	M04	M05	M06	M07
N00	000	016	032	048	064	080	096	112
N01	001	017	033	049	065	081	097	113
N02	002	018	034	050	066	082	098	114
N03	003	019	035	051	067	083	099	115
N04	004	020	036	052	068	084	100	116
N05	005	021	037	053	069	085	101	117
N06	006	022	038	054	070	086	102	118
N07	007	023	039	055	071	087	103	119
N08	008	024	040	056	072	088	104	120
N09	009	025	041	057	073	089	105	121
N10	010	026	042	058	074	090	106	122
N11	011	027	043	059	075	091	107	123
N12	012	028	044	060	076	092	108	124
N13	013	029	045	061	077	093	109	125
N14	014	030	046	062	078	094	110	126
N15	015	031	047	063	079	095	111	127

	M08	M09	M10	M11	M12	M13	M14	M15
N00	128	144	160	176	192	208	224	240
N01	129	145	161	177	193	209	225	241
N02	130	146	162	178	194	210	226	242
N03	131	147	163	179	195	211	227	243
N04	132	148	164	180	196	212	228	244
N05	133	149	165	181	197	213	229	245
N06	134	150	166	182	198	214	230	246
N07	135	151	167	183	199	215	231	247
N08	136	152	168	184	200	216	232	248
N09	137	153	169	185	201	217	233	249
N10	138	154	170	186	202	218	234	250
N11	139	155	171	187	203	219	235	251
N12	140	156	172	188	204	220	236	252
N13	141	157	173	189	205	221	237	253
N14	142	158	174	190	206	222	238	254
N15	143	159	175	191	207	223	239	255

一般來說，傳統的研究多半將搜尋區域劃分為二，並且藏入的資訊為 1 和 0 的二位元資料。當資訊為 1 時，則搜尋第一個區域，反之則由另一個區域搜尋。而本研究將搜尋區域分為 256 個群組，每一個分群代號皆為八個位元，因此藏入的資訊是以八個位元為一個單位。也就是說，每一個值域區塊能夠藏八個位元。

假設讓 e_i 和 f_i 的間隔變大，即可取得更多的群組，來增加資訊隱藏量。由此可印證，將定義域作為區域分群與資訊藏入的依據，就能大量提升嵌入的資訊量。

由於本研究藏入的資訊是以八個位元為一個單位，而灰階影像的每個像素值剛好為八位元，因此使用灰階影像作為藏入的資訊。

3.2 影像嵌入的演算法

完成分群後，便可依照想要藏入的資訊來做區域性搜尋。假設欲藏入的灰階影像之像素值為 0，就讓值域尋找最佳定義域的條件設為 $PCG(M_a, N_b) = 0$ ；若像素值為 2 時，定義域的條件則設為 $PCG(M_a, N_b) = 2$ ，由此推論就能夠完成影像嵌入的步驟，來取得資訊藏入之後的保護圖。

3.3 影像取出的演算法

在傳統的研究裡，為了避免全部的碎形碼外流讓資訊遭受竊取，通常只保留沒有嵌入資訊的碎形碼作為金鑰。但由於本研究劃分的群組比以往的研究多上數十倍，因此在嵌入資訊的 e_i 和 f_i 兩項參數中，選擇一項加入金鑰的行列。

假設隨機選一個 M_a ，讓 $PCG(M_a, N_{1 \sim 16})$ 的代碼轉為二進位型態，如圖 3.1，可以發現其變動都集中在後面四個位元（即 5 至 8 的位

元)。若隨機選擇任一個 N_b ，將 $PCG(M_{1\sim 16}, N_b)$ 轉為二進位型態後，可發現與前者不同的是位元變化集中在前面四個位元(即1至4的位元)。

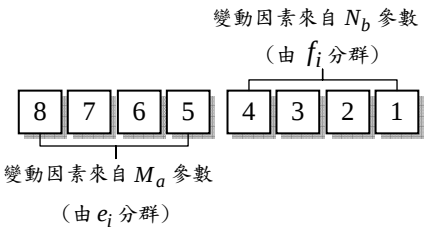


圖3.1 位置轉置參數與PCG代碼之二進位型態關係圖

由此可以發現， e_i 所藏入的資訊代表後面較重要的四個位元；而 f_i 則代表對影像較不重要的前面四個位元。即使 f_i 的資訊被竊取出來，也無法看出影像的概括，因此將 f_i 、 i_i 、 s 與 o_i 作為金鑰。如此可加快影像取出的速度。

從保護圖取出來嵌入的影像時，只需利用 $[f_i, i_i, s_i, o_i]$ 四個參數的金鑰，透過式 (2-3) 計算符合條件的定義域，求得最小誤差值之後，將 e_i 參數記錄下來，最後配合金鑰中的 f_i 參數，從 $PCG(M_a, N_b)$ 找出相對位置的分群代碼，即可依序取出影像。

4. 實驗結果與效能比較

本實驗先固定控制變因素，實驗圖像為 256×256 的灰階影像，每一個值域為 4×4 ，定義域為 8×8 ，而藏入的影像皆為 64×64 的灰階圖片。也就是說每一張 256×256 的灰階影像都藏入 $64 \times 64 \times 8$ 個位元數。

一般來說，影像品質的標準判定是使用 PSNR 值，如公式 (4-1)。

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (4-1)$$

其中在公式中的 MSE 代表的是均方差，通常 PSNR 的數值在 30 以上為影像可接受的品質範圍。

4.1 將 Elaine 與 Pepper 藏入 Lena

本實驗在 Lena 影像中，分別藏入的 Elaine 與 Pepper 影像，其原始影像與實驗後的結果，如下表所示：

表1 Lena與要藏入資訊的原始影像

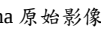
原始影像與隱藏影像	
	
	Elaine 原始影像
	
	Pepper 原始影像

表2 將Elaine藏入與取出的結果

藏入 Elaine 的 Lena 影像	取出的影像
	
PSNR : 31.33127dB	PSNR : 32.9292dB

表3 將Pepper藏入與取出的結果

藏入 Pepper 的 Lena 影像	取出的影像
	
PSNR : 31.40052dB	PSNR : 33.7672dB

從實驗結果來看，利用本研究的方法可以取出影像，而藏入影像的保護圖和取出後的影像，其PSNR值都可以高達30以上。

4.2 其他實驗

接著為了讓實驗更加公正，本研究在Pepper影像中分別藏入Lena與Elaine影像。而其控制變因素皆與先前的實驗相同。

表4 Pepper與要藏入資訊的原始影像

原始影像與藏影影像	
	
	Lena 原始影像
	
Pepper 原始影像	Elaine 原始影像

表5 將Lena藏入與取出的結果

藏入 Lena 的 Pepper 影像	取出的影像
	
PSNR : 32.24267dB	PSNR : 43.7375dB

表6 將Elaine藏入與取出的結果

藏入 Elaine 的 Pepper 影像	取出的影像
	
PSNR : 32.45799dB	PSNR : 34.7437dB

實驗後的結果PSNR仍在30以上，代表本研究的方法能夠有效的藏入與取出影像。

5. 結論

由實驗結果來看，本研究方法能夠有效的藏入一張灰階影像。無論是藏入資訊後的影像，或是取出來的資料，品質都在一定的水準上。

利用本法還有一項優點，就是傳統的碎形技術在壓縮時，需要耗費許多的時間，而利用本研究方法，將位置轉置參數分群後。值域在找最佳值時，能夠減少定義域的數目，不用搜尋全部的定義域，如此大大減少碎形在壓縮的時間。

而研究方法最大的貢獻是在於 e_i 和 f_i 的分群法，能夠藏入大量的資訊。只需要讓定義域的空間越大，所能藏入的資訊就越多。因此要在一張灰階影像藏入彩色圖片的資訊，也是有辦法達成。相關的問題都值得我們來做更深入探討。

6. 文獻探討

- [1] M.F. Barnsley ,“Fractals Everywhere,” Academic Press, San Diego, 1988.
- [2] A.E. Jacquin, “A Fractal Theory of Iterated Markov Operators with Applications to Digital Image Coding,”Ph. D. Thesis, Georgia Institute of Technology, 1989.
- [3] Joan Puate, Fred Jordan,“Using fractal compression scheme to embed a digital signature into an image,”in Proc. SPIE Photonics East Symp. Boston, MA, Nov 1996.
- [4] 廖思善，“碎形的魅力”，科學月刊，民國89年。
- [5] 蔡中緯，“數位影像驗證法”，朝陽科技大

- 學碩士論文，民國91年。
- [6] 高榮陽，“結合源端與通道碎形影像編碼之研究”，義守大學電子工程學系碩士論文，民國92年。
- [7] 李遠坤，陳玲慧，c位影像之資訊隱藏技術”，資訊安全通訊 第五卷 第四期，1999
- [8] 黃藝美，黃仁俊，“資料隱蔽技術”，資訊教育雜誌，2001
- [9] 楊文懿，“數位浮水印與影像隱藏技術研究”，屏東科技大學碩士論文，民國93年
- 陳仕政，“一個具有證証能力的安全影像隱藏機制”，逢甲大學碩士論文，民國92年
- [10] 國立中興大學物理系碎形研究室，
“<http://fractal.phys.nchu.edu.tw/index.htm>”
- [11] 張真誠，黃國峰，陳同孝，“電子影像技術”，旗標出版股份有限公司，民國92年。