

邏輯映射串流加密器

國中組 第一名

縣 市：台北市

校 名：中正國中

作 者：呂任棠、唐維澤、陳 毅

指導教師：李柏翰



我是唐維澤，今年14歲。從小就對理化、生物、地球科學、歷史，有很濃厚的興趣。在父母親的引導下，我廣泛地閱讀各種不同主題的書籍，並常利用圖書館、書店和網際網路搜集資訊。曾隨父母到澳洲住過兩年，後又至香港、新加坡、加拿大及日本等地旅遊，對各地的人文及都市管理有深刻的體認。我期許自己在未來的人生道路上，秉持著自律與毅力，善盡地球公民的責任。

呈任棠，民國75年2月2日生「琴棋書畫樣樣精，優點多得數不清，聰明優秀人人愛，短小精悍是辯才」，這是在金華國小競選自治市長時，班上同學推薦給全校同學的競選標語。金華國小畢業時，獲陳水扁市長親頒市長獎。進入中正國中後成績優異，曾兩次在段考時得到全校第一名(男生)，亦參加合唱團，兩次代表學校參加全國比賽，獲得優等。八十九年科展以「邏輯映射串流加密器」獲全國科展第一名，並因全科展優異表現獲李總統接見，更被遴選為總統頒獎時之全體受獎代表。

陳毅，1986生於臺北。1991舉家至德國求學，1995返國銜接國小三下課程。不擅辭令，然開朗樂觀的個性，使學習路上充滿豐沛的生命力。喜好音樂，尤其對數理的興趣及執著更是”一路走來，始終如一”！期望在資訊的國度裡一展所長。

關鍵詞：邏輯映射(logistic map)

一、研究動機

自從看了電影“駭客任務(MATRIX)”後，就深深為其動人的劇情所吸引，震撼之深非筆墨所能言喻。故事內容大約如下:二十二世紀的地球已被電腦進化成有生命的電腦人

(agent)所控制主宰，人類大部分都活在agent設計的虛擬夢幻世界中，而實際上是熟睡在保育箱中，成為agent所飼養的“動物”，只有一小部份人類是清醒並躲入地下伺機而動，在女主角崔妮蒂的帶領下，男主角尼歐結識了一群抵抗agent電腦王國的自由鬥士，那時活在地底下的人類生活行動是依賴一部“錫安”電腦主機來掌控，“錫安”電腦主機是由人類所操控，藉著其強大的密碼系統抵抗保衛agent的入侵，最後終因密碼系統的強固以及密碼(password)沒有外洩的情形下，爭取到時間使得尼歐領悟電腦電子世界的奧秘，進而消滅了電腦人。

這部令人想一看再看的電影深深吸引著我，因而有個念頭也想設計出強大而無法被人破解的密碼系統，可以抵抗未來agent的入侵。

二、研究目的

機緣巧合下在接觸到天下文化出版社所發行的“渾沌(chaos)”以及楊吳泉先生所著的“現代密碼學入門與程式設計”兩本書，反覆熟讀思索，發現在現在熱門的非線性科學“渾沌(chaos)”中，有一種稱為邏輯映射圖(Logistic map)的一元二次方程式，其形式非常簡單，適當的參數控制下，其迭代軌跡會出現渾沌現象，所以想利用電腦程式演算此軌跡圖形，利用數論中的模運算來取得加解密所需要的亂數，配合密碼學中串流加密的方式(Stream Ciphers)，是可以發展出一套安全性高的加解密軟體系統，媲美“錫安”電腦主機密碼系統來抵抗agent的入侵。

三、研究設備器材：

(一)pentium(k) 450 個人電腦，Win98作業平台：1台；

(二)Visual C++6.0 版軟體:1套;

(三)Matlab5.1 版軟體:1套;

(四)PUTeX 論文編輯軟體:1套;

四、研究過程或方法:

(一)研究過程:

1.渾沌理論:

邏輯映射圖(Logistic map)方程式:

$$X_{n+1} = \mu * X_n(1-X_n), X_n \in [0,1], \quad (1)$$

邏輯映射圖在 $\mu=3.569946$ 開始出現渾沌，其分析圖形如下:

圖(2):

$X_{n+1}=0.4 X_n (1- X_n)$, $X_0=0.8$, 幾次迭代後很快進入固定點0不再改變，屬於週期數為1的邏輯映射圖。

圖(3):

$X_{n+1}=2 X_n (1- X_n)$, $X_0=0.2$, 幾次迭代後很快進入固定點0.5不再改變，屬於週期數為1的邏輯映射圖。

圖(4):

$X_{n+1}=3.3 X_n (1- X_n)$, $X_0=0.2$ 幾次迭代後很快進入兩個固定點0.48和0.83，屬於週期數為2的邏輯映射圖。

圖(5):

$X_{n+1}=3.53 X_n (1- X_n)$, $X_0=0.37$ 幾次迭代後很快進入四個固定點0.37、0.52、0.83、0.88，屬於週期數為4的邏輯映射圖。

圖(6):

$X_{n+1}=3.9 X_n (1- X_n)$, $X_0=0.2$ 很多幾次迭代後仍無法進入固定點，屬於週期數為 ∞ 的邏輯映射圖，此時已出現渾沌現象。

圖(7):

$\mu = 1 \sim 4$ ，倍週期分叉到混沌映射圖，其中 $\mu = 3.5699456 \sim 4$ 的黑色區域表示渾沌現象。

圖(8):

$\mu = 3 \sim 4$ 倍週期分叉到混沌映射圖，其中黑色區域中三條白紋表示再次出現穩定倍週期現象。

2.密碼學:

串流加密方式如下，今有明文(plaintext)P:八個位元;亂數(random number)R:八個位元;欲產生密文(ciphertext)C:八個位元，如下所示，方程組(2)為互斥運算:

$$P \oplus R \equiv C$$

$$C \oplus R \equiv P$$

(2)

(二) Return map 檢測:

Return map(遞迴映射)是一種可以測量出亂數序列週期性的測量方法，舉例說明:今有一數字序列為 $(X_1, X_2, \dots, X_n)$, 遞迴映射檢測方式為: X_i 對 X_{i+1} 作圖，其中 $1 \leq i \leq (n-1)$ ，若數字序列是週期性，則遞迴映射將出現一些固定點圖，若數字序列是非週期性，則遞迴映射圖將出現一些複雜的圖形。

(三) FIPS PUB 140-1亂數檢測方式:

FIPS PUB 140-1是美國聯邦資訊處理標準公告(Federal Information Processing Standards Publication)對密碼模組的秘密安全規定(Security Requirements for Cryptographic Modules)，其中所包含對密碼模組亂數檢測方式如下:

1.單一位元測試(Monobit Test):

亂數產生器產生20,000個連續位元(0或1)，將20,000個連續位元相加總數定義為X，若 $9,654 < X < 10,346$ ，則此項亂數測試通過。

2. 撲克測試(Poker Test):

亂數產生器產生20,000個連續位元，將此20,000個位元切割成連續5,000個4位元整數，此整數之數值範圍為0-15。定義 $f(i)$ 為整數 i 出現之次數，而 i 的範圍為 $0 \leq i \leq 15$ ，計算下列數值：

$$X = \frac{16}{5000} \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000$$

(3)

若 $1.03 < X < 57.4$ ，則此項亂數測試通過。

3. 位元重複值測試(Runs Test):

“位元重複值”定義為連續20,000亂數位元中所出現的連續為1的長度或連續為0的長度，統計累積此數值，不論是1或是0的位元，“位元重複值”的長度對統計數值大小需符合下表(1)累積數之範圍，共計12項測試(包含1和0的測試)，若不符合其中一項，則此項亂數測試不通過。

位元重複值	累積數
1	2,267 – 2,733
2	1,079 – 1,421
3	502 – 748
4	223 – 402
5	90 – 223
≥ 6	90 – 223

4. 長位元重複值測試(Long Run Test):

“長位元重複值”定義為連續20,000亂數位元中所出現的連續為1的長度為34或34以上，或連續為0的長度為34或34以上，統計累積此“長位元重複值”，共計2項測試(包含1和0的測試)，若此兩項統計值其中一項不為0，則此項亂數測試不通過。

五、研究結果

以實際例子來說:輸入密碼為: chaos

輸入明文

為: Quantum mechanics is the basis for all modern descriptions of the structure and behaviour of matte

(一)加密:

假設尼歐欲加密一段明文 $m(k) = (m_1, m_2, \dots, m_k)$ 給崔妮蒂，並且輸入密碼 $h(i) = (h_1, h_2, \dots, h_k)$ ，在此 $5 \leq i \leq 200$ ； h_i 代表 ASCII 電腦字元碼，進入電腦LSC密碼系統，其運算過程如下:

1.取得初值:

password= "chaos " , h1 代表 c(99) , h_2 代表 h(104) , h3代表 a(97) , h4代表 o(111) , h5代表s(115) 。

$$\begin{aligned}(((99)^{104})^{97})^{111})^{115} &\equiv 64492 \pmod{65537} \\ 99 * 104 * 97 * 111 * 115 &\equiv 39292 \pmod{65537} \\ 64492 * 39292 &\equiv 90 \pmod{109} \\ 99 + 104 + 97 + 111 + 115 &\equiv 109 \pmod{139} \\ 64492 + 39292 &\equiv 5 \pmod{13}\end{aligned}$$

2.取得明文m(k) 和明文長度k=800 。

3.取得邏輯映射初值條件 。

$$\begin{aligned}X_0 &= 0.1 + 0.00001 * 64492 = 0.74492 \text{ (} 0.1 \sim 0.75537 \text{)} \\ Y_0 &= 0.1 + 0.00001 * 39292 = 0.49292 \text{ (} 0.1 \sim 0.75537 \text{)}\end{aligned}$$

$$\begin{aligned}\mu_x &= 3.63 + 0.001 * 90 = 3.72 \text{ (} 3.63 \sim 3.74 \text{)} \\ \mu_y &= 3.86 + 0.001 * 109 = 3.969 \text{ (} 3.86 \sim 4.0 \text{)} \\ t_0 &= 10 + 5 = 15 \text{ (} 10 \sim 22 \text{)}\end{aligned}$$

如圖(9):

$X_{n+1}=3.72 X_n(1-X_n)$, $X_0=0.74492$ 很多幾次迭代後仍無法進入固定點，屬於週期數為 ∞ 的邏輯映射圖，此時出現渾沌現象。

如圖(13):

$Y_{n+1}=3.969Y_n(1-Y_n)$, $Y_0=0.49292$ 很多幾次迭代後仍無法進入固定點，屬於週期數為 ∞ 的邏輯映射圖，此時出現渾沌現象。

4.得到亂數序列。讓邏輯映射軌跡從t=0開始演化直到 $t \geq 15$, 開始取出x,y變數值。亂數序列表示為 $U(800)=U_1,U_2, \dots U_{800}$ 。

$$\begin{aligned}10^7 * X_n &\equiv T_x(n) \pmod{2^8} \\ 10^7 * Y_n &\equiv T_y(n) \pmod{2^8} \\ T_x(n) \oplus T_y(n) &\equiv H(n) \\ H(1) &\equiv U_1, U_2, \dots U_8 \\ H(2) &\equiv U_9, U_{10}, \dots U_{16} \\ &\text{生的亂數序列。}\end{aligned} \tag{4} U_1, U_2 \cdots U_{800} \text{ 爲產}$$

5.產生密文 C_k .

$$m^k \oplus U_k \equiv C_k$$

(二)解密:如上述加密的步驟。

六、討論

(一)FIPS PUB 140-1亂數檢測:

1.邏輯映射圖 $X_{n+1} = \mu X_n(1-X_n)$ ， $X_0=0.2$ 在經由FIPS PUB 140-1亂數檢測，如圖(17)， $\mu = 3.5$ 到4，共16項亂數測試全部通過為 $T=16$ 或 $T=-16$ (一項測試通過為1，二項測試通過為2, ..., $T=-16$ 和 $T=16$ 意義相同，方便圖形對稱比較)，明顯看出有四區可以通過測試， $\mu = 3.55$ 到4三條測試不過範圍，表示再次出現穩定倍週期現象，故無法通過亂數測試。

2.邏輯映射圖在單一位元總和亂數測試，如圖(18): $\mu = 3.5$ 到4，明顯看出有三條測試不過範圍，表示再次出現穩定倍週期現象，故無法通過亂數測試， $9,654 < X < 10,346$ 。

3.邏輯映射圖在撲克亂數測試，如圖(19): $\mu = 3.5$ 到4，明顯看出有四區可以通過測試，三條測試不過範圍，表示再次出現穩定倍週期現象，故無法通過亂數測試， $1.03 < X < 57.4$ 。

4.亂數映射遞迴圖如圖(12)，混亂而無法辨別軌跡，可以確保LSC系統的安全性。

(二)邏輯映射圖固定點穩定性分析及倍週期分叉圖米範圍計算:

1.邏輯映射圖方程式及微分後斜率 m 方程式如下:

$$\begin{aligned} f(X_n) &= X_{n+1} = \mu * X_n(1-X_n), X_n \in [0,1], \mu \in [0,4] \\ f(X_n)' &= X_{n+1}' = \mu - 2\mu X_n \end{aligned} \quad (5)$$

2.固定點穩定性分析:

定義固定點為 X_f

$$\begin{aligned} x_f &= f(x_f) = \mu * x_f(1-x_f) \\ x_f &= 0 \text{ 或 } x_f = 1 - \frac{1}{\mu} \end{aligned} \quad (6)$$

$$\text{當 } x_f = 0, f'(0) = \mu$$

$$f'(0) = \mu \leq 1 \text{ 是穩定, 而 } \mu > 1 \text{ 是不穩定}$$

$$\text{當 } x_f = 1 - \frac{1}{\mu}, f'(x_f) = 2 - \mu$$

$$|2 - \mu| \leq 1 \text{ 是穩定, 且 } 1 \leq \mu \leq 3$$

$$|2 - \mu| > 1 \text{ 是不穩定, 且 } \mu > 3 \quad (7)$$

3. 倍週期分叉圖 μ 範圍計算:

定義2次迭代為 $f^2(x_n)$, 為四次方程式如下:

$$\begin{aligned} f^2(x_n) &= f(f(x_n)) = \mu^2 x_n(1-x_n)[1 - \mu * x_n(1-x_n)] \\ &= \mu^2 x_n[1 - (1+\mu)x_n + 2\mu x_n^2 - \mu x_n^3] \end{aligned} \quad (8)$$

倍週期分叉分析固定點 x_f :

$$f^2(x_f) = x_f, \text{立刻得到1根 } x_f=0 \text{ 及}$$

$$\mu^3 x_f^3 - 2\mu^3 x_f^2 + (1+\mu)\mu^2 x_f + (1-\mu^2) = 0$$

故, 定義此方程式三根為 $\alpha\beta\gamma\mu$

$$\gamma = 1 - \frac{1}{\mu}, \text{因為1次迭代2個解已知}$$

$$\alpha + \beta + \gamma = 2 = \alpha + \beta + (1 - \frac{1}{\mu})$$

$$\alpha\beta\gamma = -\frac{1-\mu^2}{\mu^2} = \alpha\beta(1 - \frac{1}{\mu})$$

$$\alpha + \beta = 1 + \frac{1}{\mu}$$

$$\alpha\beta = \frac{\mu^2 + 1}{\mu^2} \quad (9)$$

由得到的 α, β 兩根可得到新的2次方程式:

$$\mu^2 x_f^2 - \mu(\mu+1)x_f + (1+\mu) = 0$$

$$x_f = \frac{(\mu+1) \pm \sqrt{(\mu+1)(\mu-3)}}{2\mu} \quad (10)$$

如圖(4): $x_{n+1}=3.3 x^n(1-x_n)$, $x_0=0.2$ 幾次迭代後很快進入固定點 x

$$x_f = \frac{(\mu+1) \pm \sqrt{(\mu+1)(\mu-3)}}{2\mu}$$

$$\mu = 3.3$$

$$x_f = \frac{(3.3+1) \pm \sqrt{(3.3+1)(3.3-3)}}{2 \times 3.3}$$

$$x_f = 0.83 \text{ 和 } 0.48 \quad (11)$$

所以圖(4),屬於週期數為2的邏輯映射圖($x_f=0.48$ 和 0.83)。倍週期分叉 μ 出現範圍分析:

4.定義倍週期斜率 m ,兩個固定點為 p, q :

$$m = \frac{d}{dx} f(f(x))_{x=p} = f'(f(p))f'(q)$$

$$m = \mu^2(1-2p)(1-2q) \quad (12)$$

將方程式(17)之固定點帶入方程式(19),可得

$$m = \mu^2(1-2p)(1-2q) = \mu^2[1-2(p+q)+4pq]$$

$$m = -\mu^2 + 2\mu + 4$$

$$|m| \leq 1, |-\mu^2 + 2\mu + 4| \leq 1$$

$$3 \leq \mu \leq 1 + \sqrt{6}$$

$$3 \leq \mu \leq 3.4494897 \quad (13)$$

由上可知,2倍週期分叉出現範圍為 $3 \leq \mu \leq 3.4494897$,如圖(8): 2倍週期分叉出現在 $\mu = 3 \sim 3.45$,且固定點有兩個。

(三)邏輯映射串流加密系統(LSC)加解密速度分析:

如下表,加解密速度最快約為19456bytes/s,也就是155648 bites/s,也等於152 kbits/s。

CPU	作業平台	加密	解密
Pentium(k)450	Windows98	152	152

(四)Return map 檢測:

1 · 圖(11):

代表方程式 $X_{n+1}=3.72 X_n(1-X_n)$, $X_0=0.74492$ 之 X_n 遞迴映射圖,由圖形可知 X_n 序列會分布在拋物線上。

2 · 圖(12):

代表在上述方程式下, $R(n) \equiv X(n) \pmod{256}$,在經過模運算後所得亂數序列 $R(n)$ 遞迴映射圖,由圖形可發現亂數序列 $R(n)$ 沒有一定之週期。

3 · 圖(15):

代表方程式 $y_{n+1}=3.969 y_n(1-y_n)$, $y_0=0.49292$ 之 y_n 遞迴映射圖,由圖形可知 y_n 序列會分布在拋物線上。

4 · 圖(16):

代表在上述方程式下, $R(n) \equiv y(n) \pmod{256}$,在經過模運算後所得亂數序列 $R(n)$ 遞迴映射圖,由圖形可發現亂數序列 $R(n)$ 沒有一定之週期。

(五)LSC密碼系統抵抗“暴力攻擊法”數值值域範圍:

以輸入密碼字數而言,LSC可輸入密碼字數為5 ~ 200個字(猜出password:機率約 $1/2^{1600}$,顯然優於傳統4 ~ 6字元機率約 $1/2^{48}$,而以輸入起始值參數範圍為五次模運算中質數相乘之乘積 $65537*65537*109*139*13$,猜出起始值機率約為 $1/2^{50}$,一般來說LSC加解密系統是已經編譯成電腦執行檔,所以使用者使用時並須先面對輸入密碼的檢測,是以LSC仍優於傳統密碼系統加解密的方式。

七、結論

一個渾沌系統意謂著在相空間中的數值軌跡演化會展現非週期性、複雜、和對初值敏感的現象。根據邏輯映射圖的渾沌性質,我們詳述一個簡單的亂數產生器,利用適當的模運算,乘法運算,截掉小數處理,LSC系統所產生之亂數可用來當作加解密金鑰(key)。在本文中,我們示範遞迴運算(return map)分析邏輯映射圖並了解其無週期性,再利用FIPS PUB 140-1亂數檢測方式證明亂數具有高度的安全性。LSC加解密系統可適用於任何文件之加解密,如各式中英文檔案,圖形檔,執行檔等,使用LSC加解密系統有容易完成、高隱密性、高效率、安全性高可抵抗竊密者等優點。

八、參考資料及其他

(一)參考資料:

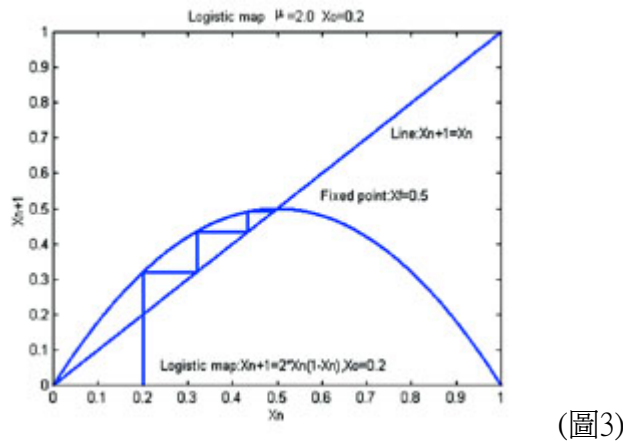
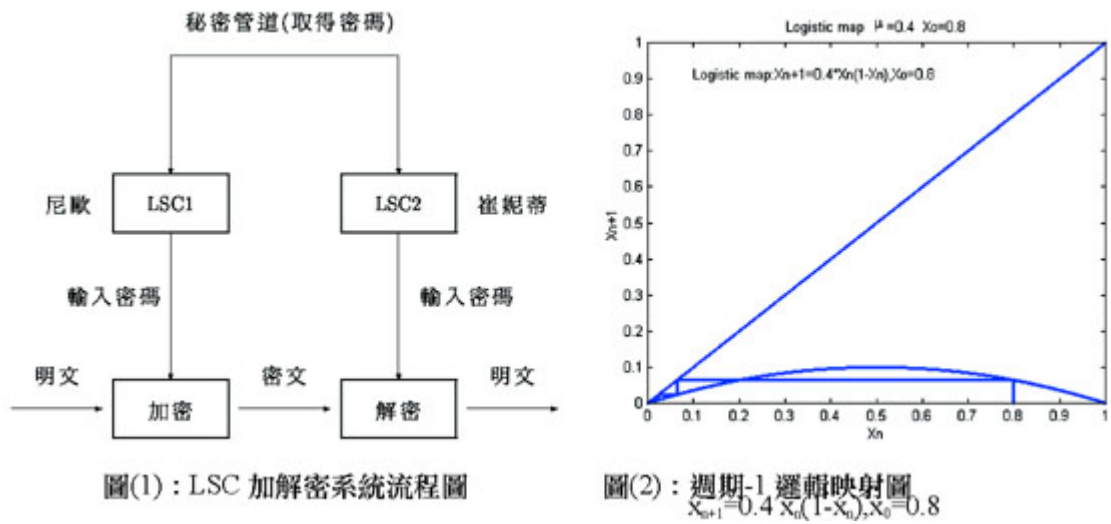
- (1)楊吳泉.現代密碼學入門與程式設計.全華出版社.1996
- (2)James Cleick , 林和 譯.渾沌.天下文化.1997
- (3)閔嗣鶴,嚴士健.初等數論.凡異出版社.1993
- (4)美國密碼模組(FIPS 140-1)檢驗認證講習會手冊.中華民國資訊安全學會.1999年四月.
- (5)劉秉正,非線性動力學與渾沌基礎},徐氏基金會.1994
- (6)E. Ott {Chaos in Dynamical Systems}. Cambridge Univ. Press. 1993.
- (7)Brauce Schneier {Applied Cryptography:Protocols,Algorithms, and Source Code in C,seconded. John Wiley & Sons, New York, 1996.
- (8)R.A. Rueppel {Analysis and Design of Stream Ciphers. Springer-Verlag Berlin, Heidelberg. 1986.

評語

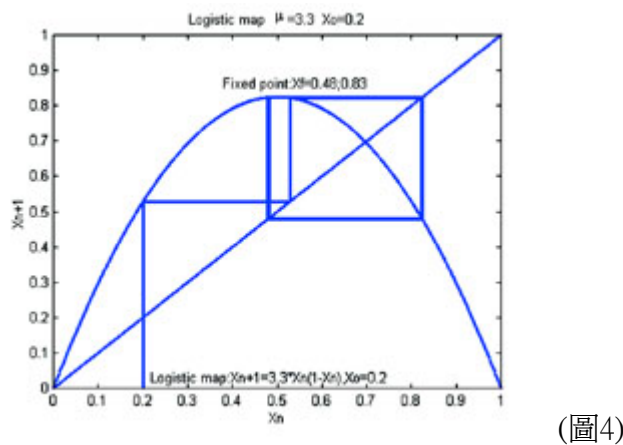
該作品以數學渾沌理論中的邏輯映射方程式，應用到密碼系統之中，以達成加密與解密的作用。此方法雖在文獻中有提出過，然而實做方法完整且有創新，同時作者對整個系

統的理論與應用有非常深刻的了解。在程式設計方面(有附原始程式碼)不但了解，且超過同年齡之程度。總體而言，相當符合科學研究的方法與精神，故推薦之。

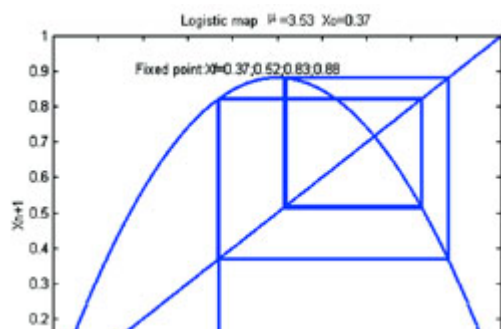
(二)圖形說明:

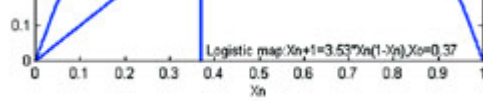


圖(3):週期-1 邏輯映射圖, $x_{n+1}=2 \ x_n(1-x_n),x_0=0.2$



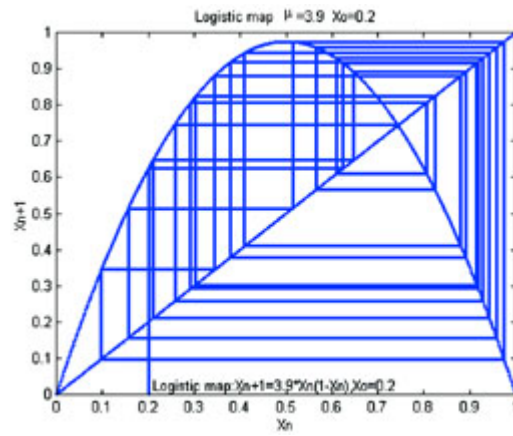
圖(4):週期-2 邏輯映射圖, $x_{n+1}=3.3 \ x_n(1-x_n),x_0=0.2$





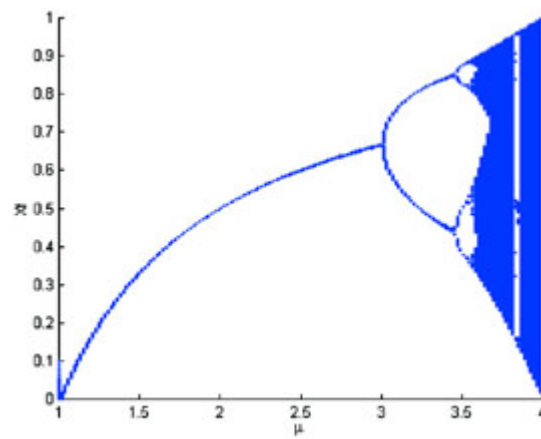
(圖5)

圖(5):週期-4 邏輯映射圖, $x_{n+1}=3.53 x_n(1-x_n)$, $x_0=0.37$



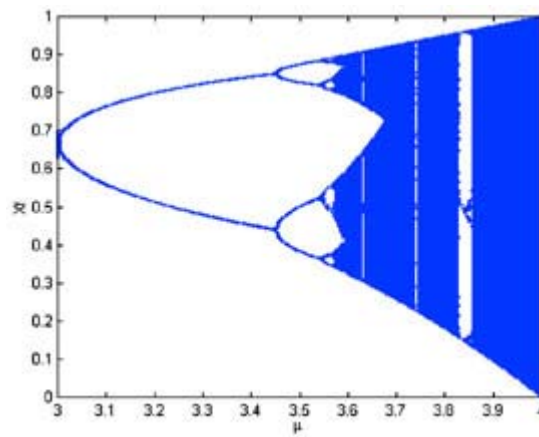
(圖6)

圖(6):週期- ∞ 邏輯映射圖, $x_{n+1}=3.9x_n(1-x_n)$, $x_0=0.2$



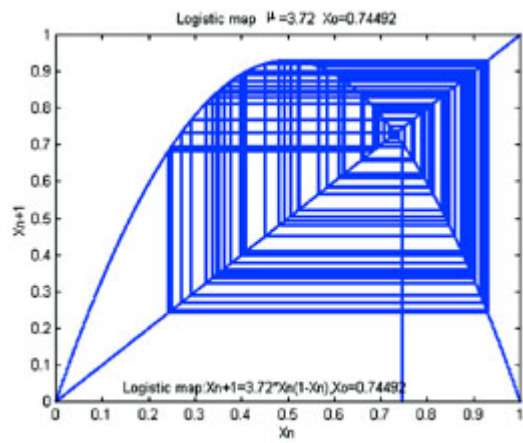
(圖7)

圖(7): μ 到 4, 倍週期分叉到混沌映射圖



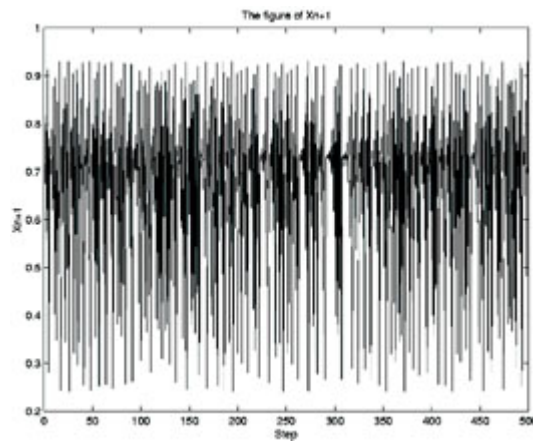
(圖8)

圖(8): μ 到 4, 倍週期分叉到混沌映射圖



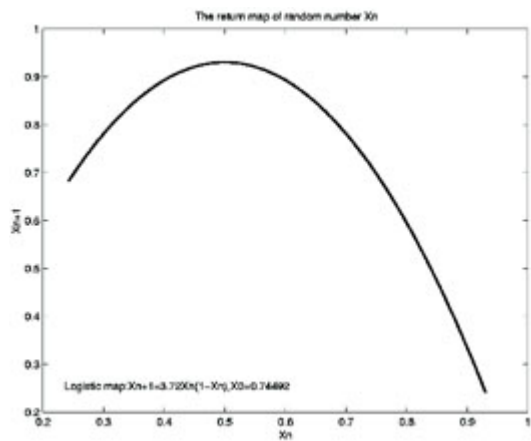
(圖9)

圖(9): 週期- ∞ 邏輯映射圖, $x_{n+1}=3.72x_n(1-x_n)$, $x_0=0.74492$ 。



(圖10)

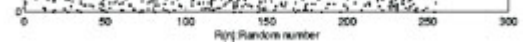
圖(10):邏輯映射圖中 $x_{n+1}=3.72x_n(1-x_n)$, $x_0=0.74492$, x_{n+1} 震盪圖。



(圖11)

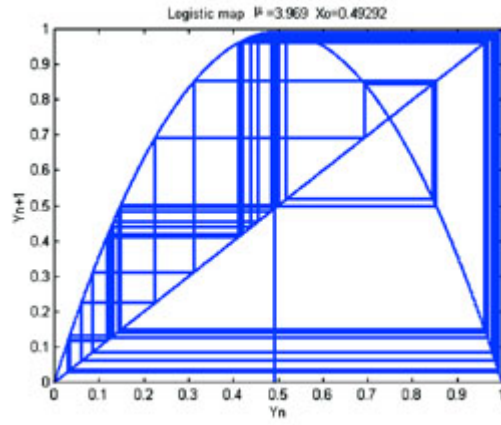
圖(11): x_n 遞迴映射圖， $x_{n+1}=3.72x_n(1-x_n)$, $x_0=0.74492$ 。





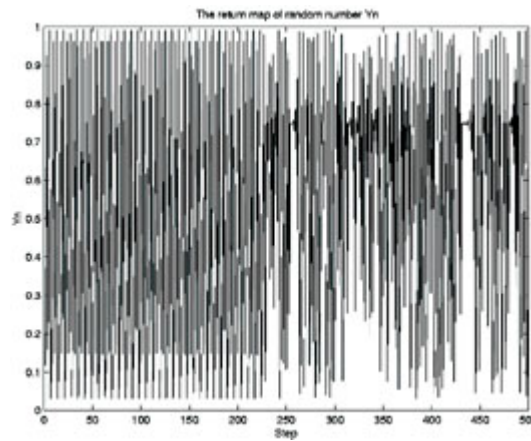
(圖12)

圖(12): $R(n)$ 亂數映射遞迴圖， $x_{n+1}=3.72x_n(1-x_n)$, $x_0=$



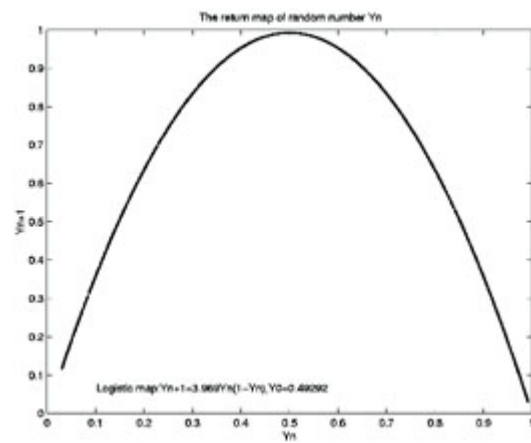
(圖13)

圖(13):週期- ∞ 邏輯映射圖, $y_{n+1}=3.969y_n(1-y_n)$, $y_0=0.49292$ 。



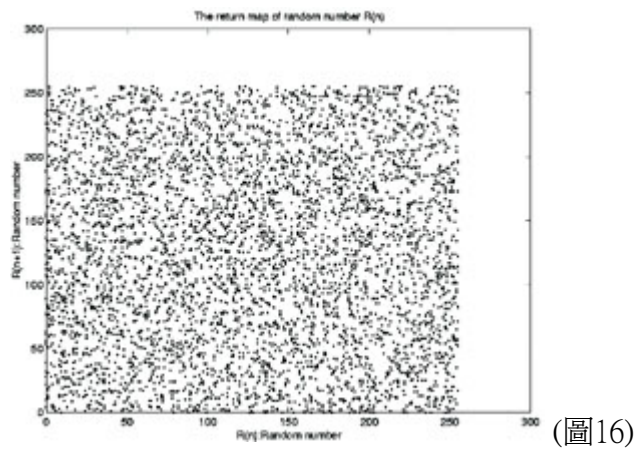
(圖14)

圖(14):邏輯映射圖中 $y_{n+1}=3.969y_n(1-y_n)$, $y_0=0.49292$, y_n 震盪圖。

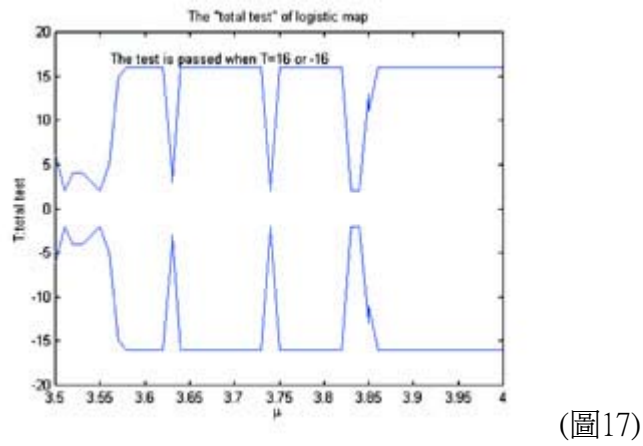


(圖15)

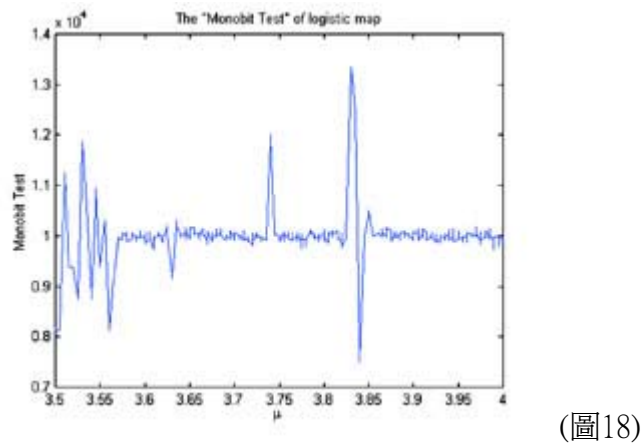
圖(15): y_n 遞迴映射圖， $y_{n+1}=3.969y_n(1-y_n)$, $y_0=0.49292$ 。



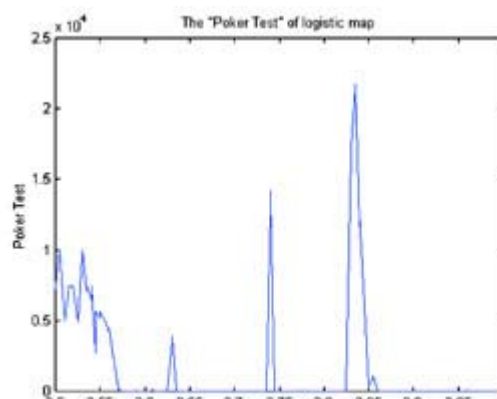
圖(16): $R(n)$ 亂數遞迴映射圖， $y_{n+1}=3.969y_n(1-y_n), y_0$



圖(17): $\mu=3.5$ 到 4, 16項亂數測試圖。



圖(18): $\mu=3.5$ 到 4, 單一位元總和亂數測試圖



3.5 3.55 3.6 3.65 3.7 3.75 3.8 3.85 3.9 3.95 4
 μ

(圖19)

圖(19): $\mu = 3.5$ 到 4, 樸克亂數測試圖。

[回到目錄頁](#) [../Index.htm](#)