Chaotic stream ciphers using logistic map

使用邏輯映射之渾沌串流密碼

陳毅
臺北市立建國高中
臺北縣永和市永和路二段 14 號 5 樓
huei7777@ms31.hinet.net

李柏翰
台灣大學物理研究所
臺北市杭州南路二段 52 號 3 樓
leepohan@ms17.hinet.net

摘要

使用一維渾沌系統來產生渾沌式串流密碼(chaotic stream ciphers)計劃已經被提出。此計劃在加密大量資料如數位元影像及資料庫等展現高度安全性以及很難破解之特性。在本論文中，我們將介紹一個新的方法藉由渾沌系統來產生令人信賴之亂數。我們的方法是利用在渾沌系統中的數值軌跡來產生亂數，此軌跡在相空間中會展現非週期性、複雜、和對初值敏感的現象。為了證明亂數的強固性，我們利用標準亂數檢測方式證明亂數 CSC 具有高度的安全性。透過檢測，我們發現 CSC 在特殊參數條件下可通過測試，因此我們可說 CSC 密碼有容易完成、高隱密性、高效率及安全性高可抵抗竊密者等優點。

關鍵詞:
二分法(bisection method)
邏輯映射(logistic map)
渾沌式串流密碼(chaotic stream ciphers, CSC)

一、簡介

在渾沌理論中稱為邏輯映射圖(Logistic map)的一元二次方程式在適當的參數控制下，其迭代軌跡會出現渾沌現象，此方程式已有很多人研究過，並利用其渾沌性質來做資料加解密。如 Bianco 等利用二分法(Bisection Method)的分類定義使 Logistic map 去產生一系列的浮點數，然後透過二分法的定義轉換成一個二進位序列的亂數，以此亂數可和明文互斥產生密文，其所提出二分法是將 logistic map 分成 2 個相鄰間隔範圍(不需要包含全部 logistic map 的範圍)，當迭代數值落於左邊部份編碼為 0，落於右邊一部份編碼為 1，作者宣稱此亂數非常強固，且這個過程不易逆轉，而使得此一過程不易被逆運算，我們會在後面利用亂數統計測試來分析此一亂數產生方式，並與我們的 CSC 加以比較其優缺點。當然利用 Logistic map 產生亂數的研究還有很多，如 Fridrich、Phatak 等，其產生亂數的方式更有特殊的演算法，為了方便比較起見，則不在本論文比較討論之列。

二、產生亂數的演算法

(一) Bianco 等人使用的二分法

$$X_{n+1} = mX_n(1-X_n) \qquad (1)$$

其中 X_n 介於 0 到 1 之間。

當取 $\begin{cases} X_l \text{ 代表低臨界值} \\ X_m \text{ 代表中點} \\ X_u \text{ 代表高臨界值} \end{cases}$

當 X_n 迭代進入 $X_l < X_n < X_m$，則亂數為 0，當 X_n 迭代進入 $X_m < X_n < X_u$，則亂數為 1，如圖(1)所示。

(二)CSC 亂數產生方式:

1.利用方程式(1)，以初值 X_0 代入方程式中求得 X_1，如此不斷迭代得到一亂數序列:(X_1， X_2，…， X_n)，再利用模運算(mod operation)取得我們所要的亂數(二進位制)序列。

$$R_n \equiv AX_n \pmod{S} \qquad (2)$$

其中 $R_n \in Z^+$。

2.舉例來說，如果我們取

$A=10^7, S=256, m=3.9, X_0=0.1$，則

$$X_1 = 3.9X_0(1-X_0) = 0.351$$
$$X_2 = 3.9X_1(1-X_1) = 0.8884161$$
$$X_3 = 3.9X_2(1-X_2) = 0.3866184397\,17$$
$$\vdots$$
$$X_{99} = 3.9X_{98}(1-X_{98}) = 0.2057258234\,97$$
$$X_{100} = 3.9X_{99}(1-X_{99}) = 0.6373705652\,70$$

所以我們要產生的 CSC 亂數如下

$$R_1 \equiv 10^7 X_1 \pmod{256} \equiv 240$$
$$R_2 \equiv 10^7 X_2 \pmod{256} \equiv 193$$
$$R_3 \equiv 10^7 X_3 \pmod{256} \equiv 72$$
$$\vdots$$
$$R_{99} \equiv 10^7 X_{99} \pmod{256} \equiv 42$$
$$R_{100} \equiv 10^7 X_{100} \pmod{256} \equiv 73$$

3.加解密使用:

利用此一無序之亂數及電腦中的數值運算 Exclusive-or 之方法，我們可以用此亂數來做資料加解密的處理，或者是可當作亂數產生器來產生社會科學中統計測量所需要的亂數序列。

三、亂數檢測

(一) 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 20000 個連續位元(0 或 1)，將 20000 個連續位元相加總數定義為 X，若 $9654 < X < 10346$，則此項亂數測試通過。

2.樸克測試(Poker Test):

亂數產生器產生 20000 個連續位元，將此 20000 個位元切割成連續 5000 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 $0 \le i \le 15$，計算下列數值:

$$X = \frac{16}{5000}\left(\sum_{i=0}^{15} f(i)^2\right) - 5000 \qquad (3)$$

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 20000 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	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
≧6	90-223

(表格 1: 位元重複值累積數)

4.長位元重複值測試(Long Run Test):

“長位元重複值”定義為連續20000亂數位元中所出現連續為 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。總計此 FIPS PUB 140-1 之亂數檢測共計 16 項，16 項全部通過才算通過，我們用 16 代表全部通過，0 代表全部不通過，3 代表 3 項通過，其餘依此類推。

(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，…，X_n)，遞迴映射檢測方式為: X_i 對 X_{i+1} 作圖，其中 $1 \le i \le (n-1)$，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。利用此法，可將亂數的週期性加以分析。

四、實驗與討論

(一) Bianco 的二分法亂數統計測試

FIPS PUB 140-1 之亂數檢測總共 16 項，全部通過為 16，其中有一項不過，則亂數不通過測試。如圖(2)所示:

$X_l = 0.4, X_m = 0.5, X_u = 0.6$，$m = 3.5 \sim 4$，間隔為 0.001，$X_0 = 0.1$，亂數統計測試為

$$\text{正確率} = \frac{55}{501} = 0.1098 = 10.98\%$$

$$\text{誤差率} = \frac{446}{501} = 0.8902 = 89.02\%$$

(二)CSC 的亂數統計測試

1.如表格 2 所示:

$A = 10^3 \Rightarrow 10^{10}, m = 3.5 \sim 4.0$，$m$之間隔分別為 0.001、0.0001、0.00001，分別累計總測試次數為 501、5001、50001 次，且模運算 $S = 256$，起始值 $X_0 = 0.1$，正確數代表通過統計測試次數、正確率代表通過統計測試占總測試次數之比率，錯誤數代表無法通過統計測試次數、錯誤率代表無法通過統計測試占總測試次數之比率。表格 3 則為 $S = 2$，其他條件與表格 2 同的情形。

A	統計	0.001	0.0001	0.00001
10^3	正確數	8	66	704
	錯誤數	493	4935	49297
	正確率	0.0160	0.0132	0.0141
	錯誤率	0.9840	0.9868	0.9859
10^4	正確數	288	2928	29331
	錯誤數	213	2073	20670
	正確率	0.5749	0.5855	0.5866
	錯誤率	0.4251	0.4145	0.4134
10^5	正確數	382	3758	37715
	錯誤數	119	1243	12286
	正確率	0.7625	0.7514	0.7543
	錯誤率	0.2375	0.2486	0.2457
10^6	正確數	385	3850	38472
	錯誤數	116	1151	11529
	正確率	0.7685	0.7698	0.7694
	錯誤率	0.2315	0.2302	0.2306
10^7	正確數	388	3876	38660
	錯誤數	113	1125	11341
	正確率	0.7745	0.7750	0.7732
	錯誤率	0.2255	0.2250	0.2268
10^8	正確數	390	3895	38770
	錯誤數	111	1106	11231
	正確率	0.7784	0.7788	0.7754
	錯誤率	0.2216	0.2212	0.2246
10^9	正確數	391	3907	38916
	錯誤數	110	1094	11085
	正確率	0.7804	0.7812	0.7783
	錯誤率	0.2196	0.2188	0.2217
10^{10}	正確數	392	3917	38967
	錯誤數	109	1084	11034
	正確率	0.7824	0.7832	0.7793
	錯誤率	0.2176	0.2168	0.2207

(表格 2: 亂數統計測試結果; (mod 256))

表格 2:的三條正確率曲線圖如圖(3)所示。

A	統計	0.001	0.0001	0.00001
10^3	正確數	257	2953	26020
	錯誤數	244	2048	23981
	正確率	0.5130	0.5905	0.5204
	錯誤率	0.4870	0.4095	0.4796
10^4	正確數	367	3624	36296
	錯誤數	134	1377	13705
	正確率	0.7325	0.7247	0.7259
	錯誤率	0.2675	0.2753	0.2741
10^5	正確數	381	3831	38269
	錯誤數	120	1170	11732
	正確率	0.7605	0.7660	0.7654
	錯誤率	0.2395	0.2340	0.2346
10^6	正確數	386	3857	38544
	錯誤數	115	1144	11457
	正確率	0.7705	0.7712	0.7709
	錯誤率	0.2295	0.2288	0.2291
10^7	正確數	387	3864	38613
	錯誤數	114	1137	11388
	正確率	0.7725	0.7726	0.7722
	錯誤率	0.2275	0.2274	0.2278
10^8	正確數	387	3867	38638
	錯誤數	114	1134	11363
	正確率	0.7725	0.7732	0.7727
	錯誤率	0.2275	0.2268	0.2273
10^9	正確數	388	3868	38915
	錯誤數	113	1133	11085
	正確率	0.7745	0.7734	0.7783
	錯誤率	0.2255	0.2266	0.2217
10^{10}	正確數	387	3869	38662
	錯誤數	114	1132	11339
	正確率	0.7725	0.7736	0.7732
	錯誤率	0.2275	0.2264	0.2268

(表格 3: 亂數統計測試結果; (mod 2))

表格 3:的三條正確率曲線圖如圖(4)所示。

2.如圖(5) 所示:

$A = 65537, m = 3.5 \sim 4$，**間隔 0.00001，** $S = 256, X_0 = 0.1$

正確率 $= \frac{37328}{50001} = 74.65\%$

錯誤率 $= \frac{12673}{50001} = 25.35\%$

如圖(6) 所示: ，

$A = 1801982953$ **(一個大質數)** , $m = 3.5 \sim 4$，**間隔 0.00001，** $S = 256, X_0 = 0.1$

正確率 $= \frac{38955}{50001} = 77.91\%$

錯誤率 $= \frac{11046}{50001} = 22.09\%$

如圖(7) 所示:

$A = 10^{10}, m = 3.5 \sim 4$ **，間隔 0.00001，** $S = 2, X_0 = 0.1$

正確率 $= \frac{38662}{50001} = 77.32\%$

錯誤率 $= \frac{11339}{50001} = 22.68\%$

由上述亂數統計測試數據可發現，CSC 的方法優於 Bianco 的二分法而且可以產生令人信賴的亂數。

(三)用 Return Map 檢測 CSC:

如圖(8) 所示，發現圖形混亂無法辨識，可判定為非週期性的亂數。

(四)邏輯映射圖固定點穩定性分析及倍週期分叉圖 m 範圍計算之討論:

1. 方程式(1)微分後斜率 m 方程式如下:

$$f'(X_n) = X'_{n+1} = m - 2mX_n \qquad (4)$$

2.固定點穩定性分析:

定義固定點為 X_f

$$X_f = f(X_f) = mX_f(1 - X_f) \quad (5)$$

則 $X_f = 0$ 或 $X_f = 1 - \frac{1}{m}$

當 $X_f = 0$， $f'(0) = m$

而 $m \le 1$ 時穩定， $m > 1$ 時不穩定

當 $X_f = 1 - \frac{1}{m}$， $f'(X_f) = 2 - m$

$|2 - m| \le 1$ 穩定，則 $1 \le m \le 3$

$|2 - m| > 1$ 不穩定，則 $m > 3$ (6)

3.倍週期分叉圖 m 範圍計算:

定義 2 次迭代為 $f^2(X_n)$ 為四次方程式如下:

$$\begin{aligned} f^2(X_n) &= f(f(X_n)) \\ &= m^2 X_n(1 - X_n)[1 - mX_n(1 - X_n)] \\ &= m^2 X_n[1 - (1+m)X_n + 2mX_n^2 - mX_n^3] \end{aligned} \quad (7)$$

倍週期分叉分析固定點 X_f:

$f^2(X_f) = X_f$，立刻得到 1 根

$X_f = 0$ 及

$$m^3 X_f^3 - 2m^3 X_f^2 + (1+m)m^2 X_f + (1 - m^2) = 0$$

故，定義此方程式三根為 $a\ b\ g$，

$g = 1 - \frac{1}{m}$，因為 1 次迭代的 2 個解已知

$$\begin{aligned} a + b + g &= 2 = a + b + \left(1 - \frac{1}{m}\right) \\ abg &= -\frac{1 - m^2}{m^3} = ab\left(1 - \frac{1}{m}\right) \\ a + b &= 1 + \frac{1}{m} \\ ab &= \frac{m+1}{m^2} \end{aligned} \quad (8)$$

由得到的 α，β 兩根可得到新的二次方程式:

$$\begin{aligned} m^2 X_f^2 - m(m+1)X_f + (1+m) &= 0 \\ X_f &= \frac{(m+1) \pm \sqrt{(m+1)(m-3)}}{2m} \end{aligned} \quad (9)$$

4.倍週期分叉 m 出現範圍分析:

定義倍週期斜率 m，兩個固定點為 p，q:

$$\begin{aligned} m &= \frac{d}{dx} f(f(x))_{x=p} = f'(f(p))f'(p) \\ m &= m^2(1 - 2p)(1 - 2q) \end{aligned} \quad (10)$$

將方程式(8)之固定點帶入方程式(10)，可得

$$\begin{aligned} m &= m^2(1 - 2p)(1 - 2q) \\ &= m^2[1 - 2(p+q) + 4pq] \\ m &= -m^2 + 2m + 4 \\ |m| &\le 1, \ |-m^2 + 2m + 4| \le 1 \\ 3 &\le m \le 1 + \sqrt{6} \\ 3 &\le m \le 3.4494897 \end{aligned}$$

由上可知，2 倍週期分叉 m 出現範圍為 $3 \le m \le 3.4494897$。

(五)利用 CSC 來作圖形加密

Lena 圖形為圖(9)，利用方程式(2)，其中 $A = 10^7, m = 3.98$、$S = 256, X_0 = 0.1$ 所產生 CSC 加密之後所得圖形為圖(10)，由圖所示，可發現已加密成混亂的無法辨識之密文，輸入正確的密碼後解密之圖形為圖(11),又恢復成

原圖相同之圖形。

五、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方式，利用適當的模運算，乘法運算，截掉小數處理，所產生之亂數可用來加解密。在本文中，我們示範遞迴運算(return map)分析邏輯映射圖並瞭解其無週期性，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。CSC 亂數可適用於任何文件之加解密，如各式圖形檔，執行檔等，使用 CSC 亂數加解密有容易完成、高效率、安全性高可抵抗竊密者等優點。

六、誌謝

特別感謝台大物理系陳義裕教授在渾沌理論上的解析，也要感謝成大電機博士候選人楊吳泉先生提供美國密碼模組(FIPS 140-1)檢驗認證的方法，才能使本論文能克服困難而順利產生。本論文為中華民國國科會研究計劃所支助，編號為 NSC89-2112-M-002-057 以及 NSC90-2112-M-002-020。

七、參考文獻

[1] 中華民國資訊安全學會，"美國密碼模組(FIPS 140-1)檢驗認證講習會手冊"，4月，1999.

[2] 李柏翰，"渾沌式擬亂數產生器"，中華民國專利，Patent No. 088111987，9月19，2001.

[3] B. Schneier "Applied Cryptography'', seconded. John Wiley and Sons, Inc. 1994.

[4] D.E. Knuth, "The Art of Computer Programming", vol. 2, third, Addison and Wesley, 1997.

[5] E. Ott, " Chaos in Dynamical Systems'', Cambridge Univ. Press. 1993.

[6] I. Niven , H. S. Zuckerman and H. L. Montgomery, "An Introduction to the theory of numbers", fifth, John Wiley and Sons, Inc.,1991.

[7] J. Fridrich, and J. Geer, " Secure Image Ciphering Based on Chaos'', Final Technical Report (USAF, Rome Laboratory, New York), 1997.

[8] M. Andrecut,"Logistic map as a random number generator", Int. J. of Morden Phys. B, vol. 12, No.9, pp. 921-930, 1998.

[9] M. E. Bianco and G. L. Mayhew, "High Speed Encryption System and Method'', US Patent No.5365588, Nov. 15, 1994.

[10] M. E. Bianco, and D. A. Reed, "Encryption System Based on Chaos Thoery'', US Patent No. 5048086, Sept. 10, 1991.

[11] P. -H. Lee, "Implementation of chaotic stream ciphers using chaotic pseudo-random number generator", Dept. of Physics , NTU, master thesis, 1999.

[12] S. C. Phatak and S. S. Rao,"Logistic Map: A possible random-number generator", Phys. Rev. E, vol. 51, No.4, pp. 3670-3678, 1995.

[13] Security Requirements for Cryptographic Modules, "FIPS PUB 140-1", Federal Information Processing Standards Publication, 1994.

[14] Y.-Y. Chen, "Masking messages in chaos", Europhysics Letters, vol. 34, No.4, pp. 245-250, 1996.

八、圖形說明:

圖(1): Bianco 二分法的說明

圖(2): Bianco 二分法的亂數的檢測結果,
$X_l = 0.4, X_m = 0.5, X_u = 0.6$,
$m = 3.5 \sim 4$ **間隔為 0.001,** $X_0 = 0.1$。

圖(3): 表格 2 中模運算 $S = 256$ **亂數統計測試的正確率曲線圖。**

圖(4): 表格 3 中模運算 $S = 2$ **亂數統計測試的正確率曲線圖。**

圖(5): $A = 65537, m = 3.5 \sim 4$ **,間隔 0.00001,** $S = 256, X_0 = 0.1$ **的 CSC 檢測結果。**

圖(6): $A = 1801982953, m = 3.5 \sim 4$ **,間隔 0.00001,** $S = 256, X_0 = 0.1$ **的 CSC 檢測結果。**

圖(7): $A = 10^{10}, m = 3.5 \sim 4$ **,間隔 0.00001,** $S = 2, X_0 = 0.1$ **的 CSC 檢測結果。**

圖(8): Return Map 檢測:
$X_{n+1} = 3.72X_n(1 - X_n), X_0 = 0.74492$

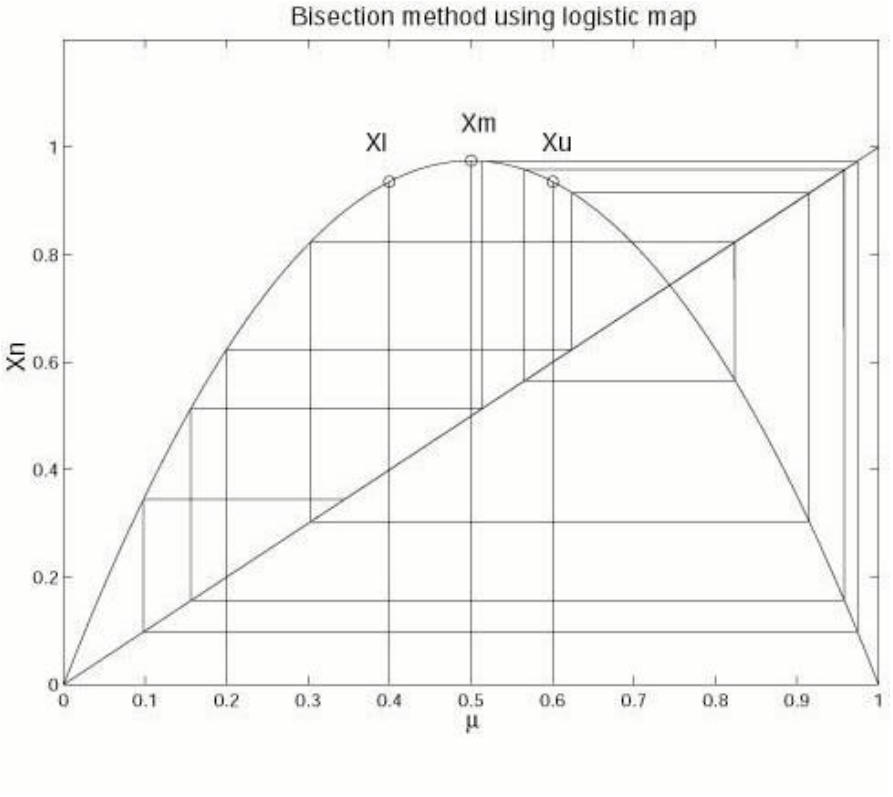
圖(9): Lena 原圖

圖(10): Lena 經由 CSC 加密後的圖

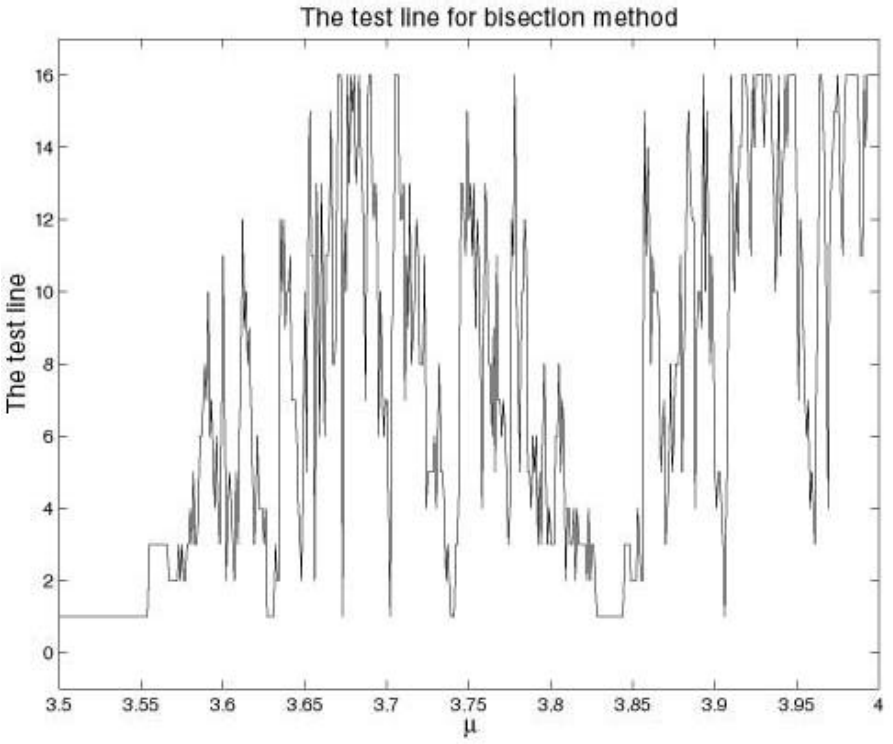
$A = 10^7, S = 256$, $X_0 = 0.1, m = 3.98$

圖(11): Lena 經 CSC 解密後的圖

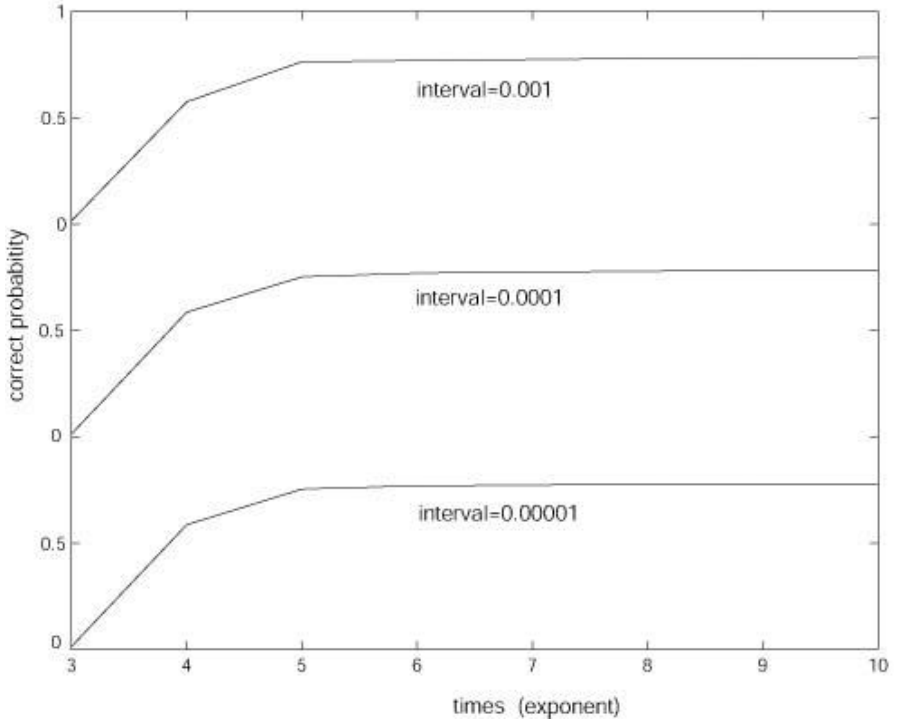
$A = 10^7, S = 256$, $X_0 = 0.1, m = 3.98$ 。



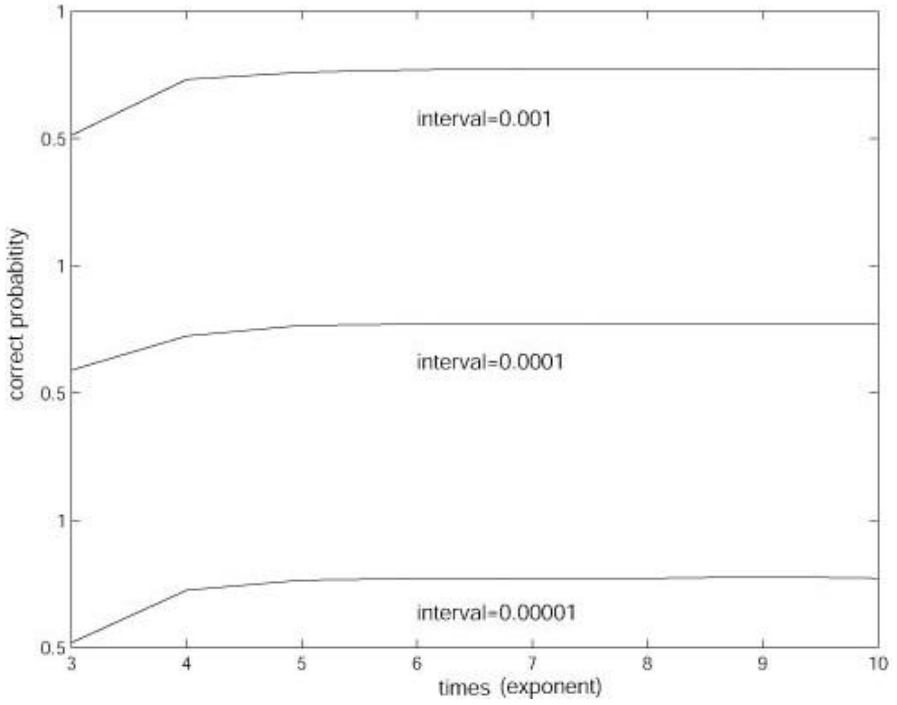
圖(1)：Bianco 二分法的說明



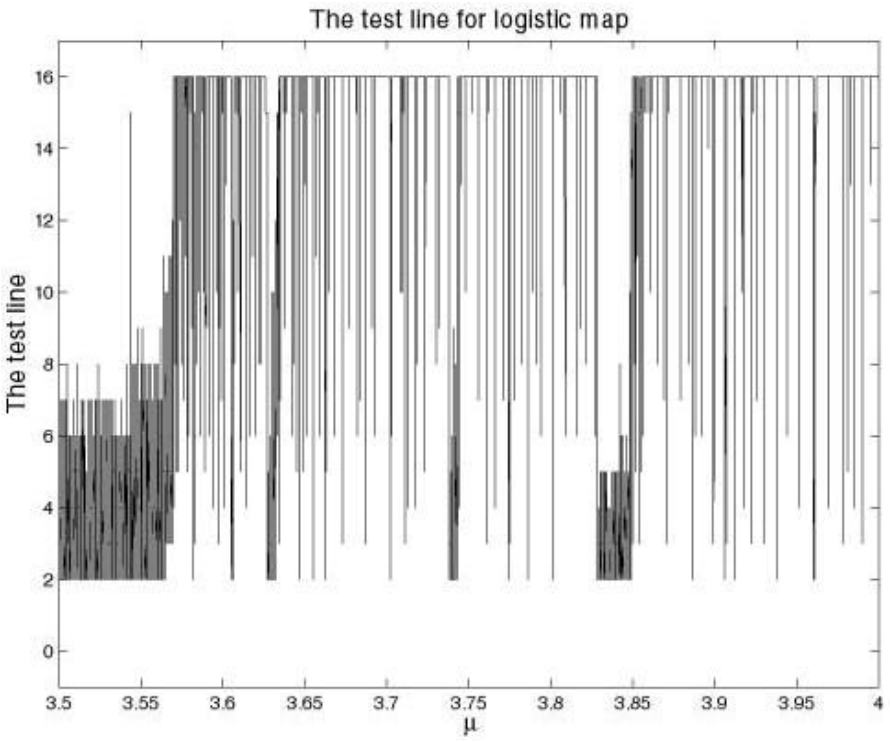
圖(2)：Bianco 二分法的 FIPS PUB 140-1 的檢測結果。



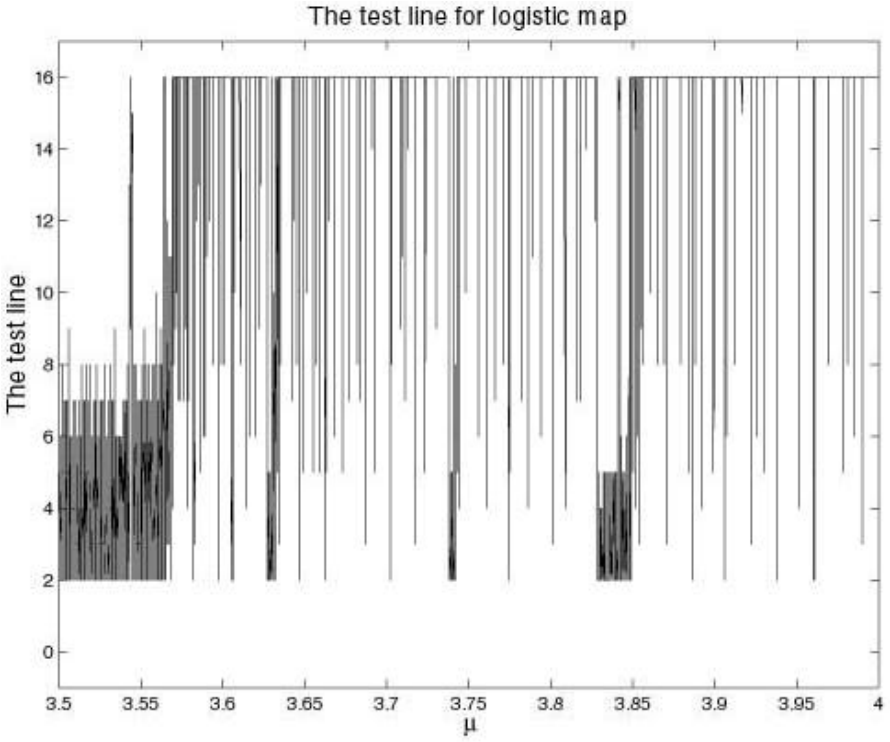
圖(3)：表格 2 中 $S = 256$ 亂數統計測試的正確率曲線圖



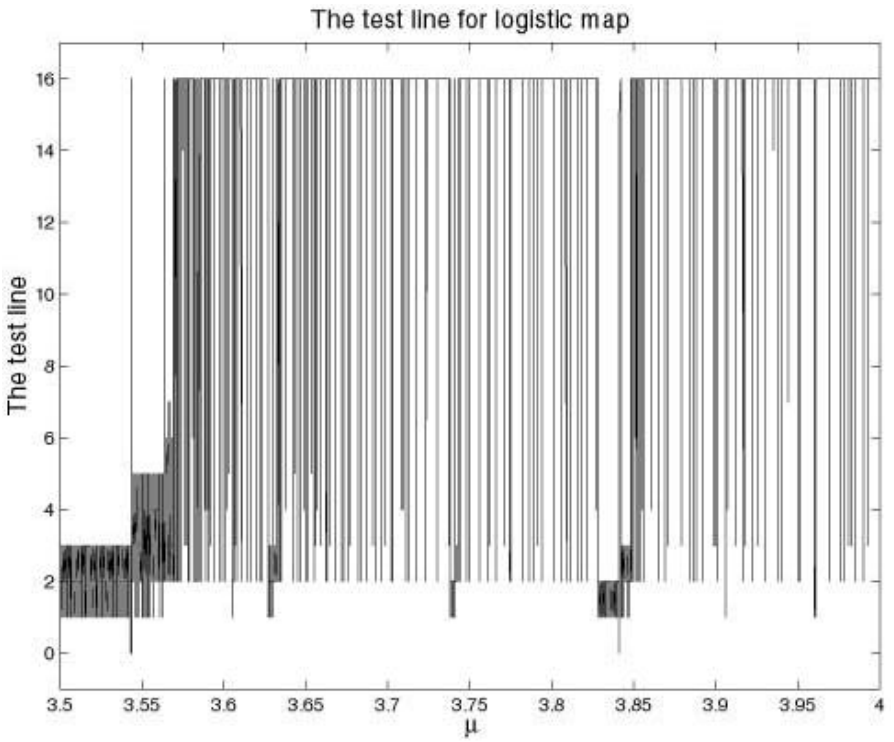
圖(4)：表格 3 中 $S = 2$ 亂數統計測試的正確率曲線圖



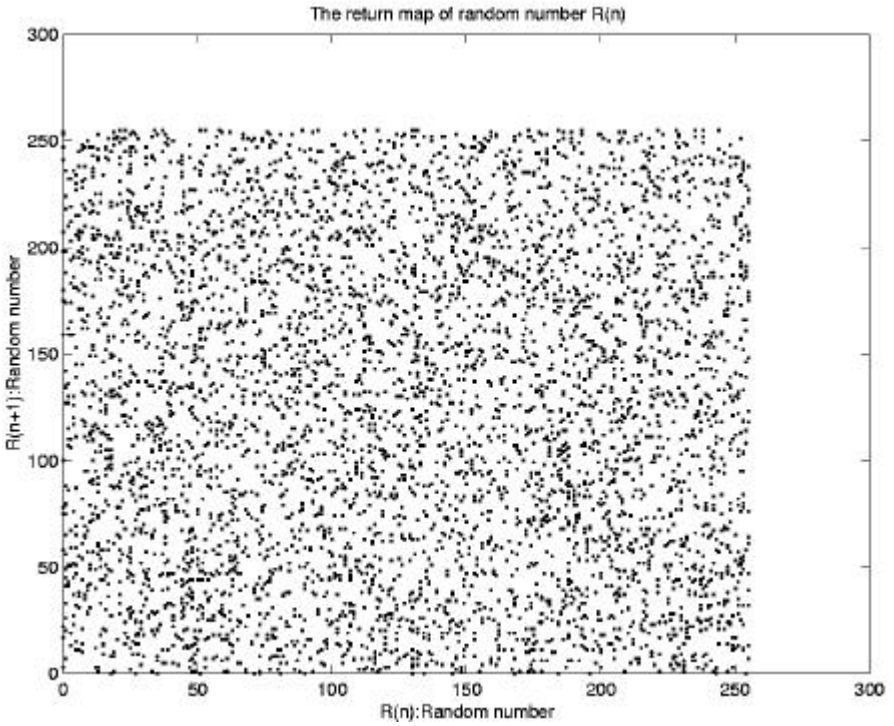
圖(5)： $A=65537, m=3.5\sim 4$ **，間隔 0.00001，** $S=256, X_0=0.1$**的檢測結果。**



圖(6)： $A=1801982953, m=3.5\sim 4$ **，間隔 0.00001，** $S=256, X_0=0.1$**的檢測結果。**

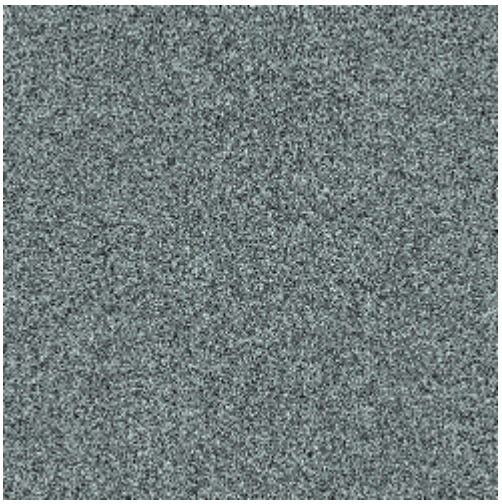


圖(7)： $A=10^{10}, m=3.5\sim 4$ **，間隔 0.00001，** $S=2, X_0=0.1$ **的檢測結果。**



圖(8): Return Map 檢測 $X_{n+1}=3.72X_n(1-X_n),\ X_0=0.74492$

圖(9)：Lena 原圖



圖(10)：Lena 經由 CSC 加密後的圖

圖(11)：Lena 經 CSC 解密後的圖