

色彩科學導論與應用

Determining Secret Keys for 2D Arnold Cat Map

授課教師：王宗銘

2021/05/11

Assignment 10

請寫一個 python 程式讀入輸入檔案，計算變數後，產出輸出檔案。這些變數稍後可以當成 Arnold Cat Map 之參數來加密影像。這個程式可以由 Assignment 09 修改。

輸入檔案：input10.txt

第 1 行 x_0 r_x
第 2 行 y_0 r_y
第 3 行 seed N
第 4 行 L

輸出檔案：output10.txt

第 1 行 x_0 r_x
第 2 行 y_0 r_y
第 3 行 seed N
第 4 行 L
第 5 行 R1 R2 R3
第 6 行 x_5 y_{18}
第 7 行 a b

其中，第 1-4 行與輸入檔案內容相同，第 5-7 行為由程式計算得出。

1. 由輸入檔 input10.txt 讀入第 1 行與第 2 行之 (x_0, r_x) 、 (y_0, r_y) ，並當成 2 個 Logistic maps 之初始值。精準度為小數後 21 位。

$$x_{n+1} = r_x x_n (1 - x_n),$$

$$y_{n+1} = r_y y_n (1 - y_n).$$

假設

$$x_0 = 0.3999940013885498046875,$$

$$r_x = 3.3999940013885498046875,$$

$$y_0 = 0.389999999999999999999999,$$

$$r_y = 3.389999999999999999999999$$

2. 讀入第 3 行 seed、整數 N、間格長度 L。以 seed 當成亂數種子，隨機產生 3 個介於 1 與 N 之整數，分別為 R1, R2, R3。

假設 seed=100, N=50, L=0.02。產生的 3 個隨機變數為 R1=5, R2=18, R3=23。

3. 依據 R1=5，使用第 1 個 Logistic Map，產出第 5 個 logistic 數值(以 x_5 表示之)，數值取到小數後 21 位，如無法取得，至少需要小數後 6 位。同理，根據 R2=18，使用第 2 個

Logistic Map，產出第 18 個的 logistic 數值(以 y_{18} 表示之)。

假設產出之兩數分別為

$x_5=0.254896756412598754123$ $y_{18}=0.789561451289745620124$ 。

4. 計算 x_5 所在之間格： x_5 落在第 $\left\lceil \frac{x_5}{L} \right\rceil = 13$ 個間格，故計算出變數 $a=5+13=18$ 。同理， y_{18} 落在第 $\left\lceil \frac{y_{18}}{L} \right\rceil = 40$ 個間格，故計算出變數 $b=18+40=58$ 。

5.將上述輸入參數寫入輸出檔案的第 1、2、3、4 行。將計算得出之 R1, R2, R3 寫在輸出檔案的第 5 行，取得的 logistic 數值寫在輸出檔案的第 6 行，最後，將計算得出的 a 與 b 寫在第 7 行。

7. 將取得之參數依序寫入檔案 output10.csv，成為輸出檔案。

輸入範例

第 1 行 0.399940013885498046875 3.399940013885498046875

第 2 行 0.38999999999999999999 3.38999999999999999999

第 3 行 100 50

第 4 行 0.02

輸出範例

第 1 行 0.399940013885498046875 3.399940013885498046875

第 2 行 0.38999999999999999999 3.38999999999999999999

第 3 行 100 50

第 4 行 0.02

第 5 行 5 18 23

第 6 行 0.254896756412598754123 0.789561451289745620124

第 7 行 18 58

Program:

The python program, “學號-10-IMG_SEC.py, reads an input file, **input10.txt**, and produces the output, **output10.txt**.

Submission:

Please submit the following **THREE files**.

1. 學號-10-IMG_SEC.py
2. Input10.txt
3. Output10.txt