Image Encryption SINE - MAP

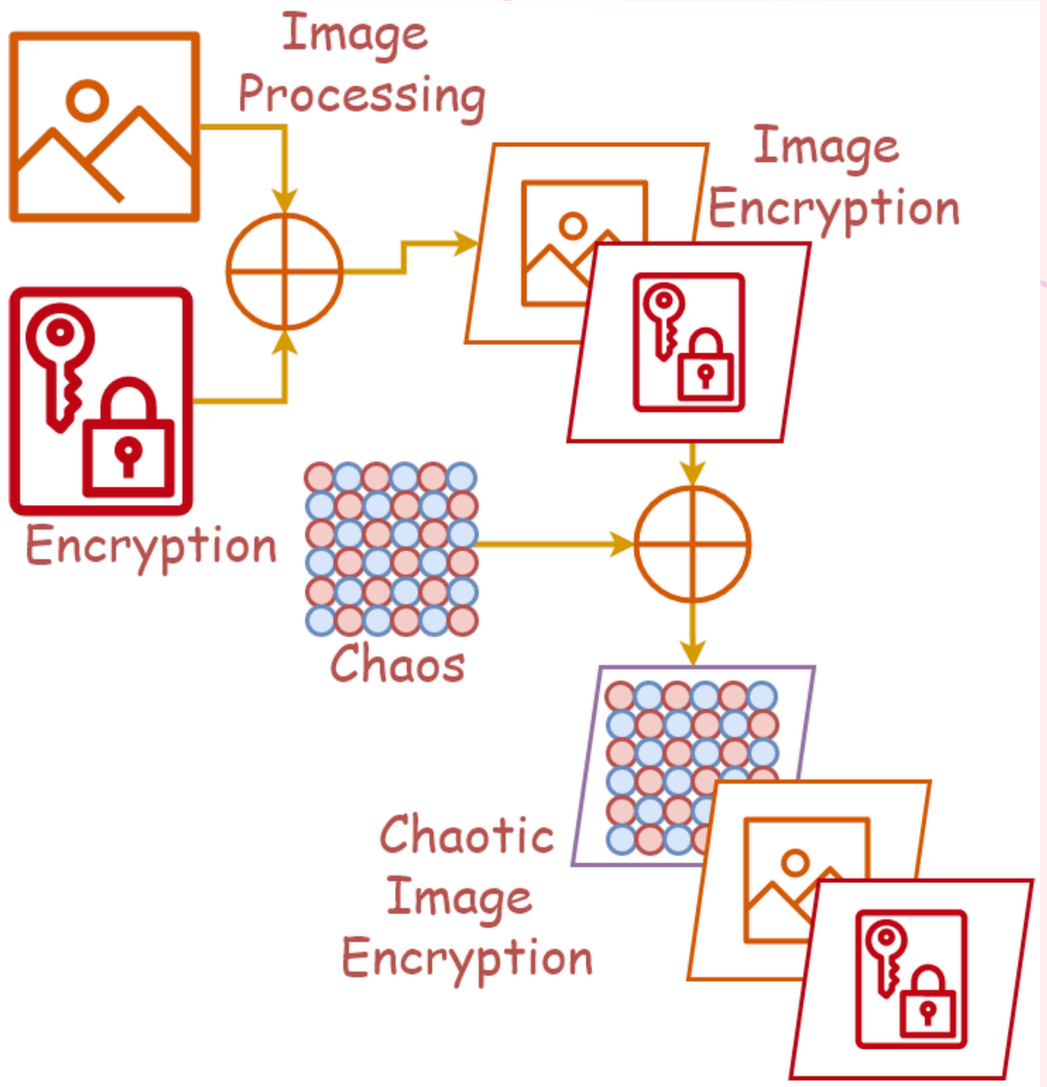
Group - 4 **Cryptography Project Class**

Abdul Fikih Kurnia - 2106731200
Laode Alif Ma'sum -

Apa itu Enkripsi Image??

Enkripsi image dengan menggunakan fungsi chaos adalah teknik kriptografi yang digunakan untuk mengamankan citra digital. Proses ini melibatkan penggunaan algoritma chaos, yang dikenal karena sifatnya yang sangat sensitif terhadap kondisi awal, untuk mengacak atau mengubah citra asli menjadi bentuk yang tidak dapat dikenali atau "blur".

Fungsi chaos digunakan untuk menentukan urutan pengacakan piksel pada citra. Piksel-piksel dalam citra asli diacak berdasarkan urutan yang dihasilkan oleh algoritma chaos, sehingga citra tersebut menjadi tidak dapat dikenali.



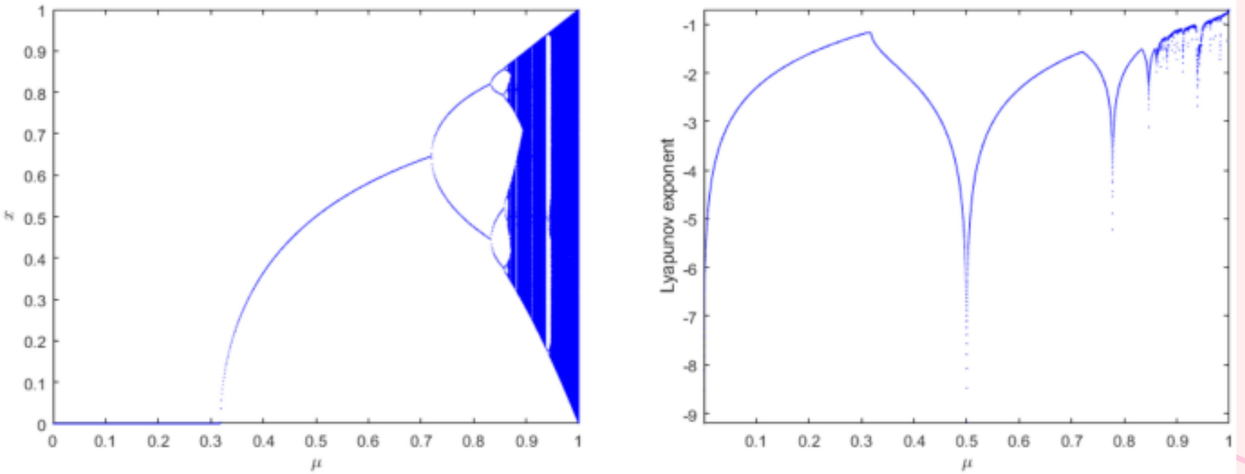
Apa itu SINE MAP??

Fungsi ini adalah jenis peta iteratif yang menunjukkan sifat chaos, di mana hasil dari satu iterasi digunakan sebagai input untuk iterasi berikutnya.

$$x_{n+1} = sin(\pi a(y_n + 3)x_n(1 - x_n))$$

$$y_{n+1} = sin(\pi a(x_n + 1 + 3)y_n(1 - y_n))$$

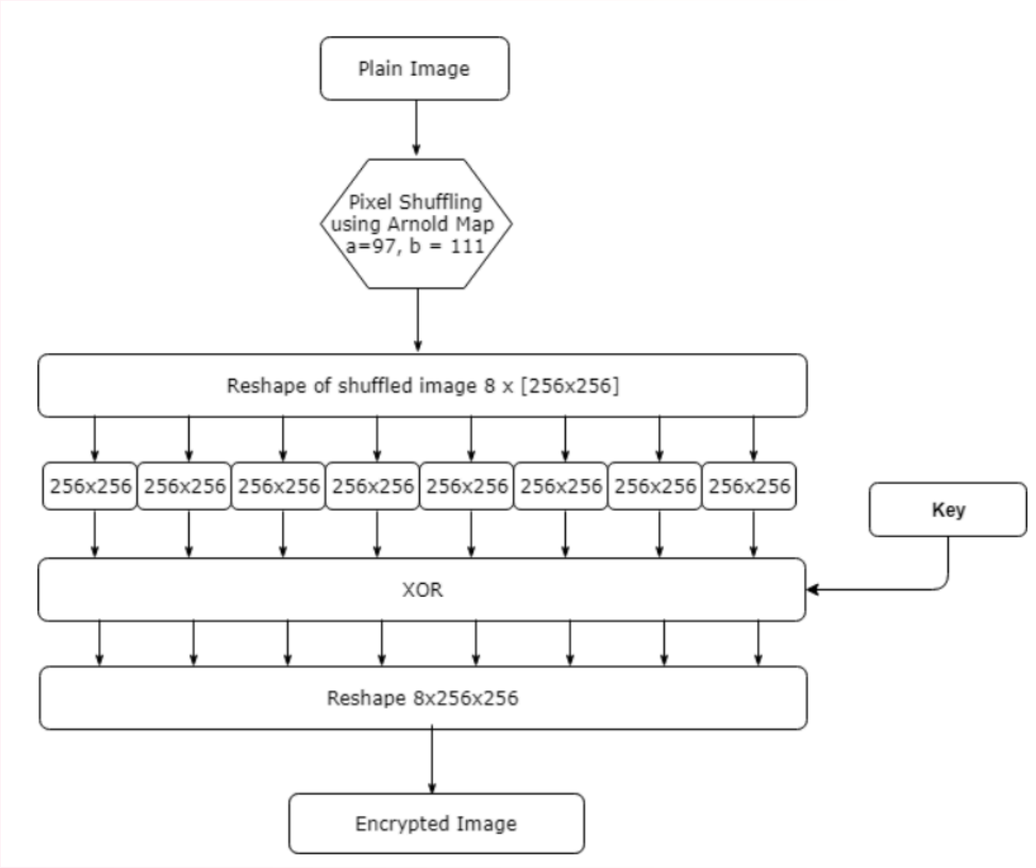
dimana nilai a ∈ [0,1], xn, yn merupakan output sequence yang akan digunakan pada key. Nilai I dan x pada fungsi sine map digunakan sebagai key dalam proses enkripsi dan dekripsi.



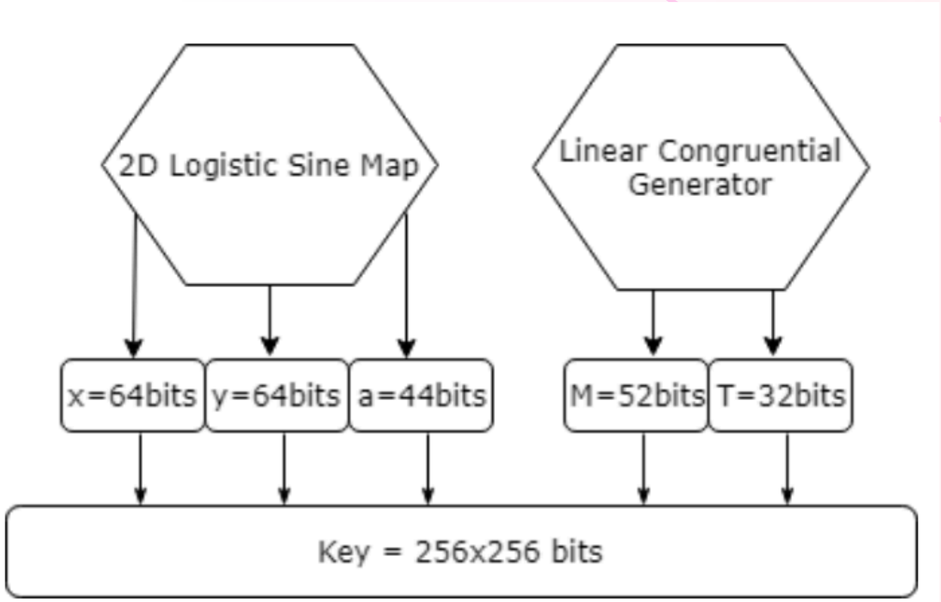
(a) Bifurcation Diagram (b) Lyapunov exponent

- **Pemilihan Kondisi Awal**: Nilai awal x0x0 dan parameter kontrol rr dipilih sebagai bagian dari kunci enkripsi.
- **Iterasi Sine Map**: Sine map diiterasikan untuk menghasilkan urutan nilai yang tampak acak.
- **Pengacakan Piksel**: Urutan nilai ini digunakan untuk mengacak posisi atau nilai piksel dalam citra, menghasilkan citra yang terenkripsi.

Proses Enkripsi & Dekripsi

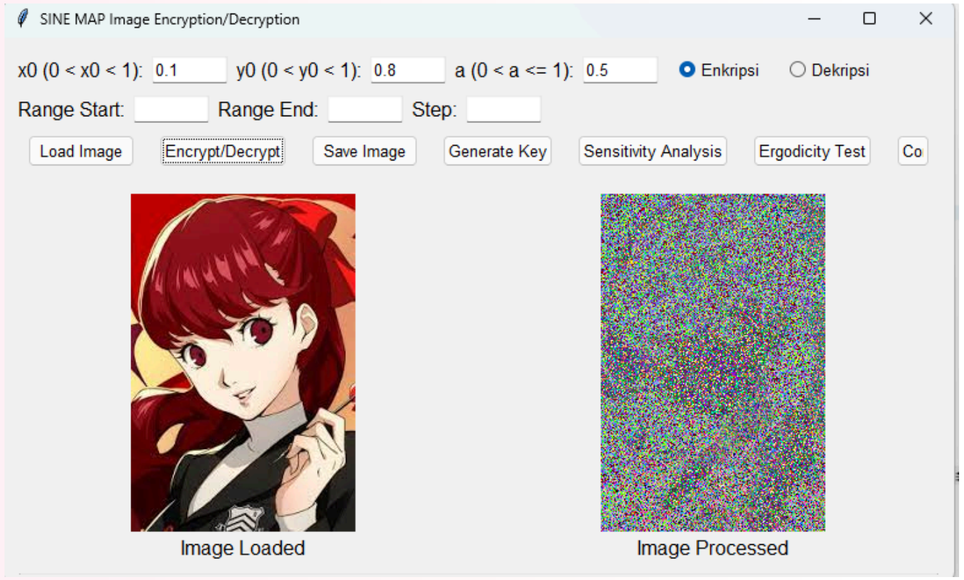


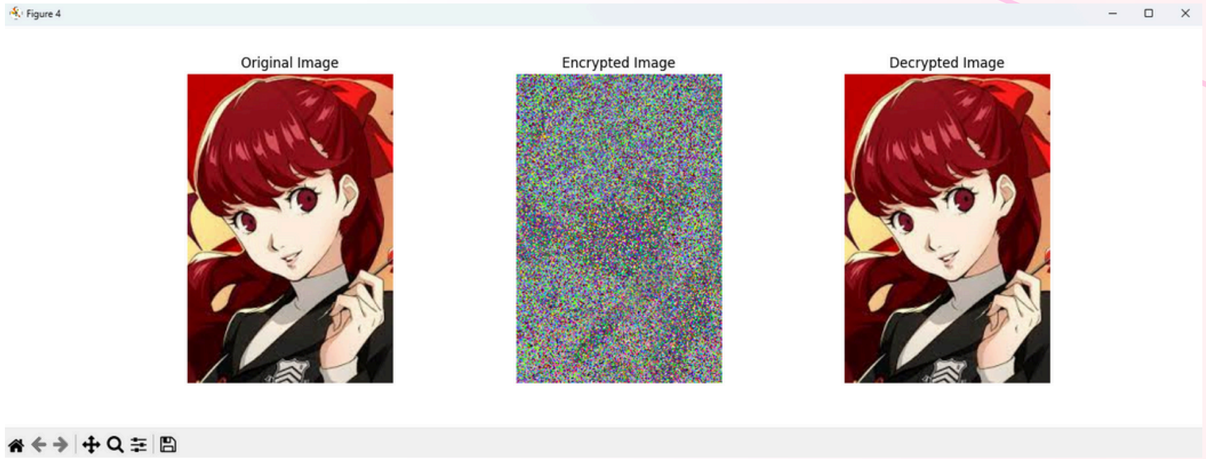
Algoritma Enkripsi



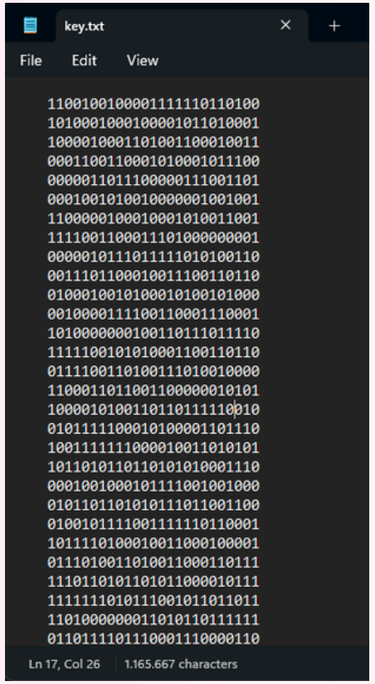
Key Generation

Hasil GUI Aplikasi





Analisis [Uji keacakan stream : NIST]

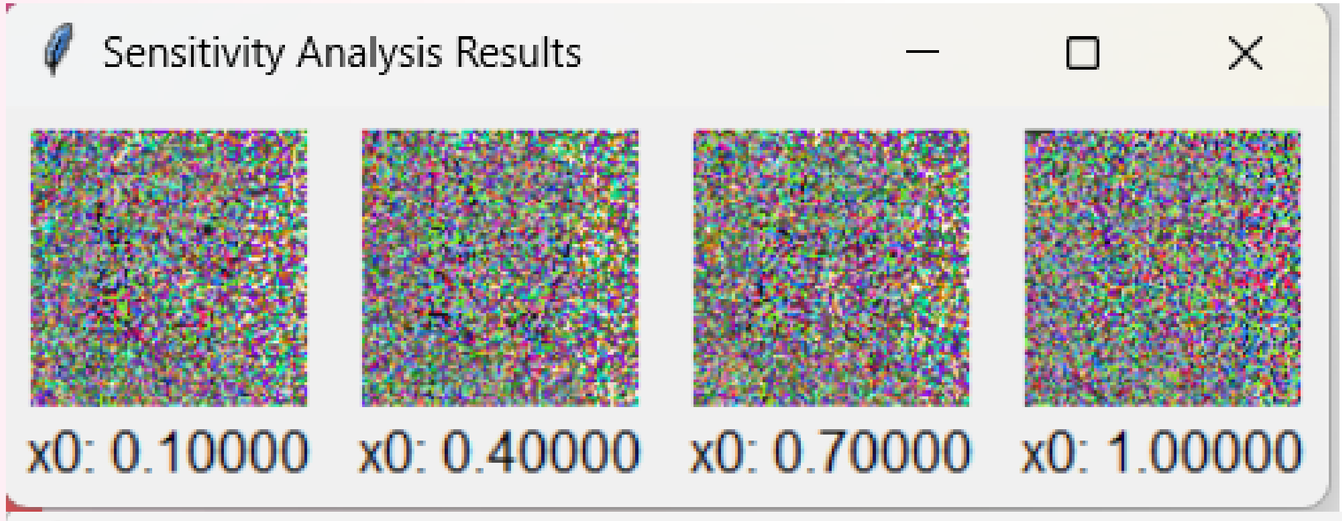



```
alif5@DESKTOP-J6UP6T5 /cygdrive/c/Users/alif5/Documents/Kuliah/Semester 6/Kripto/sts-2.1.
2
$ ./assess 10000
         G E N E R A T O R   S E L E C T I O N
         -------------------------------------

   [0] Input File                 [1] Linear Congruential
   [2] Quadratic Congruential I   [3] Quadratic Congruential II
   [4] Cubic Congruential         [5] XOR
   [6] Modular Exponentiation     [7] Blum-Blum-Shub
   [8] Micali-Schnorr             [9] G Using SHA-1

  Enter Choice: 0


            User Prescribed Input File: key.txt

            S T A T I S T I C A L   T E S T S
            ---------------------------------

   [01] Frequency                       [02] Block Frequency
   [03] Cumulative Sums                 [04] Runs
   [05] Longest Run of Ones             [06] Rank
   [07] Discrete Fourier Transform      [08] Nonperiodic Template Matchings
   [09] Overlapping Template Matchings  [10] Universal Statistical
   [11] Approximate Entropy             [12] Random Excursions
   [13] Random Excursions Variant       [14] Serial
   [15] Linear Complexity

        INSTRUCTIONS
           Enter 0 if you DO NOT want to apply all of the
           statistical tests to each sequence and 1 if you DO.

  Enter Choice: 1

       P a r a m e t e r   A d j u s t m e n t s
       -----------------------------------------
   [1] Block Frequency Test - block length(M):         128
   [2] NonOverlapping Template Test - block length(m): 9
   [3] Overlapping Template Test - block length(m):    9
   [4] Approximate Entropy Test - block length(m):     10
   [5] Serial Test - block length(m):                  16
   [6] Linear Complexity Test - block length(M):       500

  Select Test (0 to continue): 0

  How many bitstreams? 25

  Input File Format:
   [0] ASCII - A sequence of ASCII 0's and 1's
   [1] Binary - Each byte in data file contains 8 bits of data

  Select input mode:  0

    Statistical Testing In Progress.........

    Statistical Testing Complete!!!!!!!!!!!
```

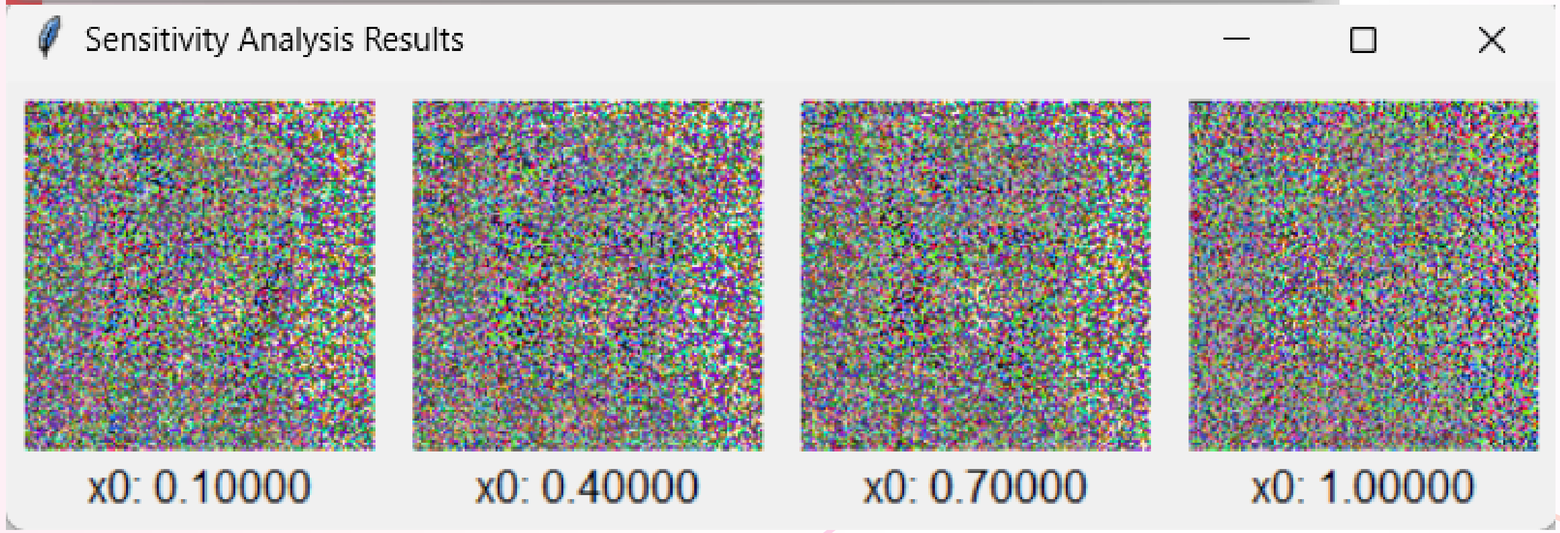
```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <key.txt>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
  4   1   4   4   1   2   1   5   1   2 0.186566     24/25     Frequency
  1   3   3   2   2   8   2   3   0   1 0.007422     25/25     BlockFrequency
  5   1   3   1   4   4   0   0   2   5 0.029796     25/25     CumulativeSums
  4   2   2   1   1   2   4   1   3   5 0.311542     24/25     CumulativeSums
  4   1   4   0   1   4   2   5   3   1 0.105618     25/25     Runs
  1   3   0   3   2   4   3   1   3   5 0.242986     25/25     LongestRun
  4   3   1   7   3   1   0   1   3   2 0.021262     25/25     Rank
  2   2   3   2   3   4   2   3   0   4 0.585209     25/25     FFT
```

if P-value > 0.01 --> Random sequence

Analisis [Uji sensitivitas nilai awal = 1]

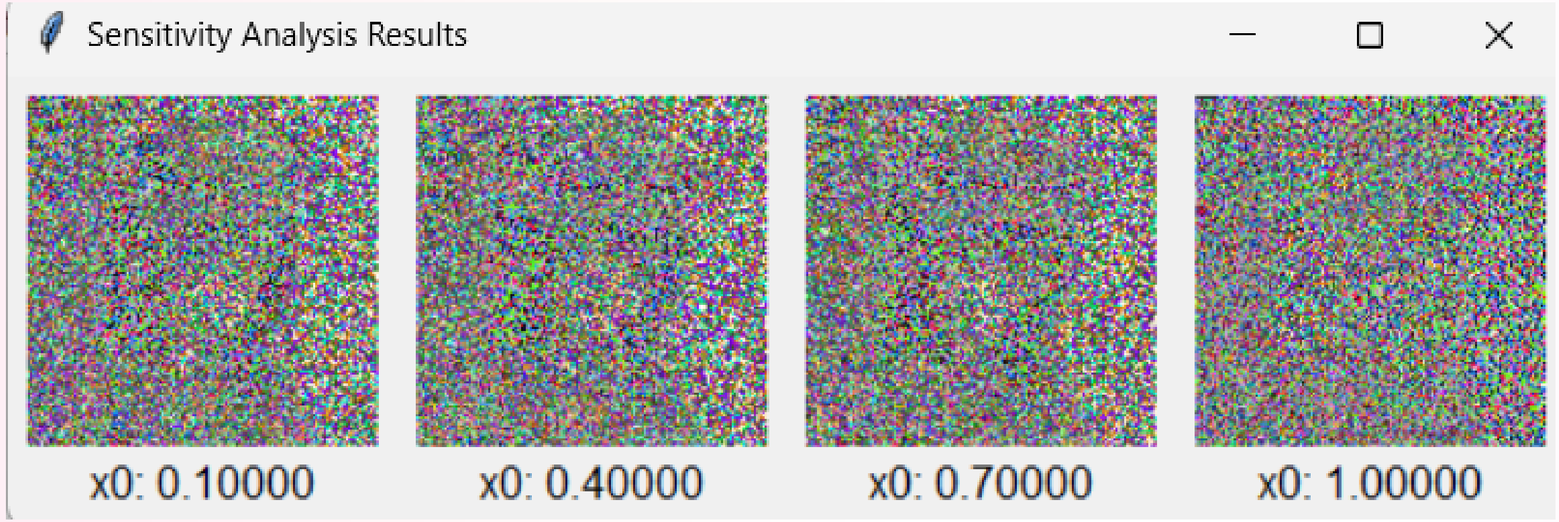


Pixel : 80 x 80

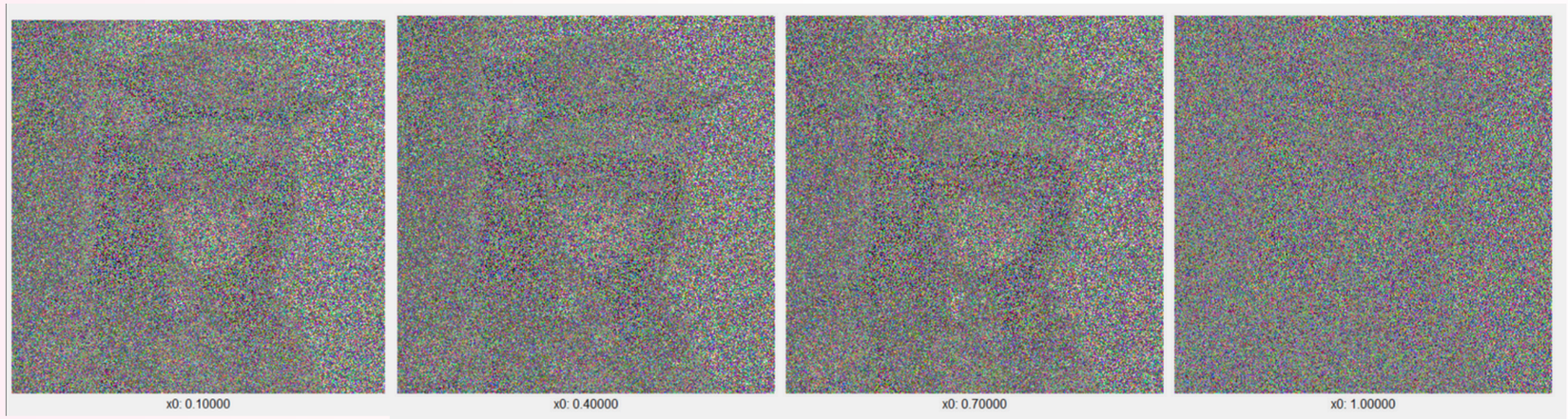


Pixel : 128 x 128

Analisis [Uji sensitivitas nilai awal = 1]

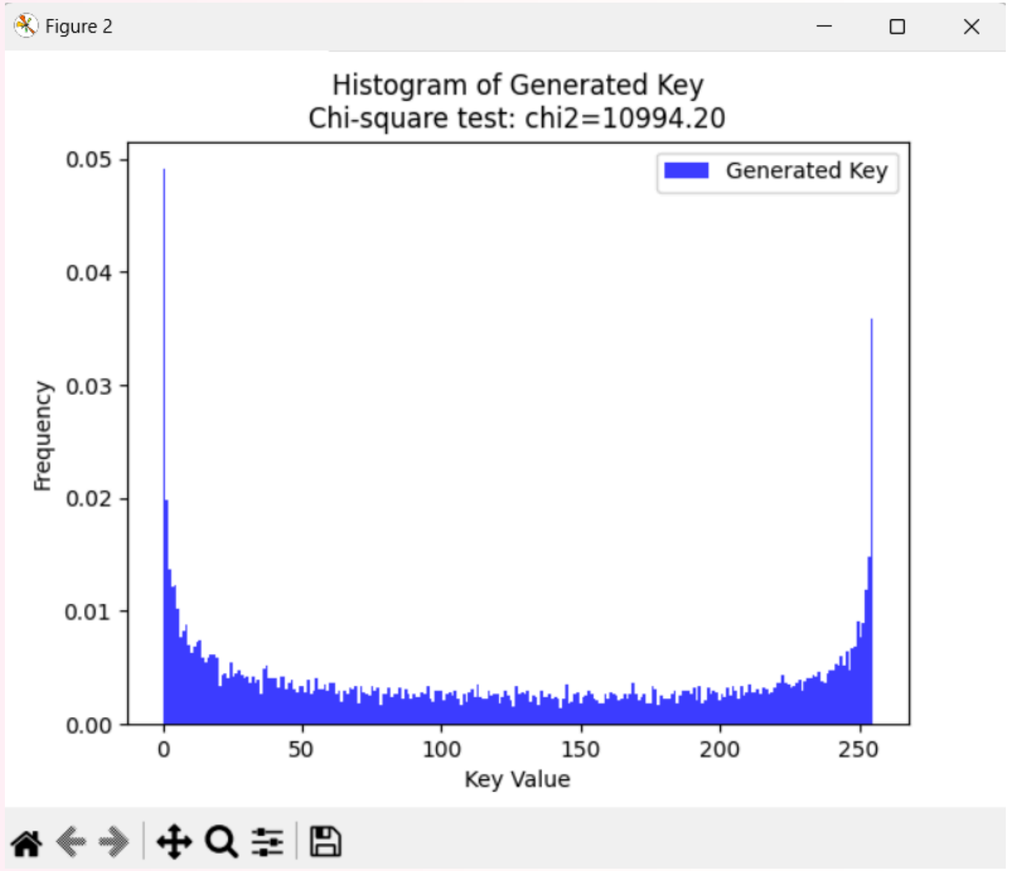


Pixel : 480 x 480

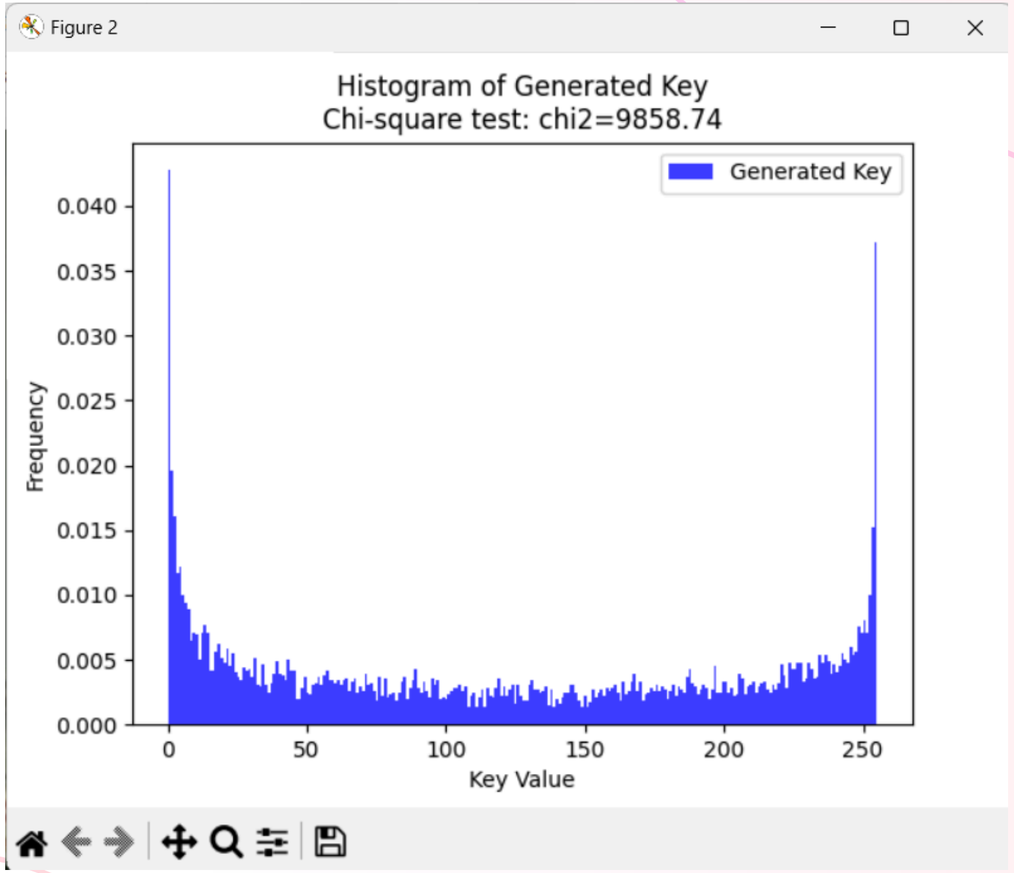


Pixel : 720 x 720

Analisis [Uji ergodisity a = 1]

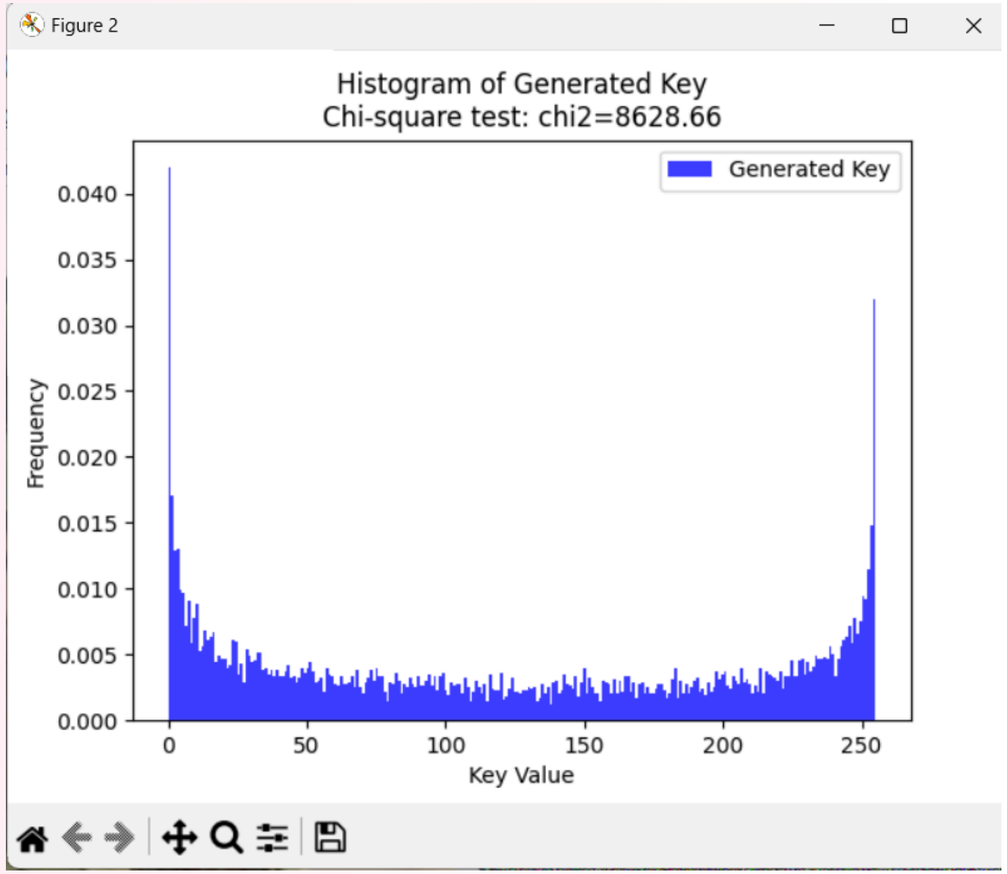


X0 = 0.1

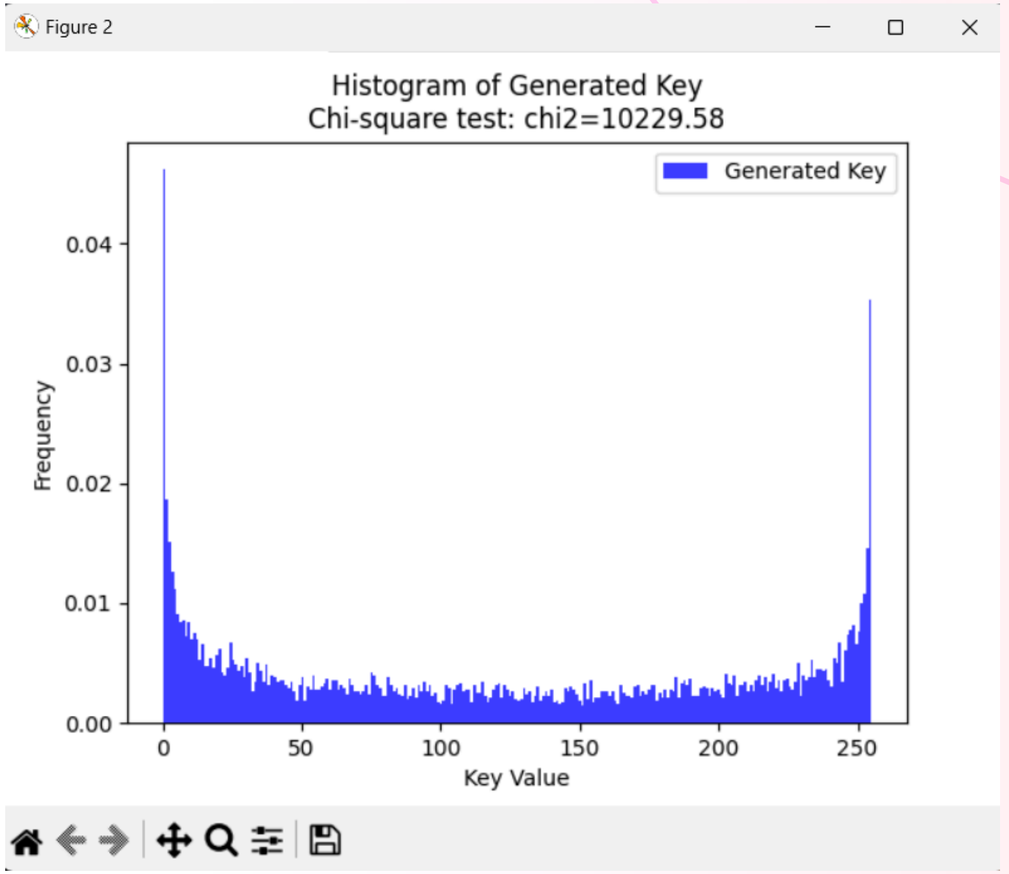


X0 = 0.4

Analisis [Uji ergodisity a = 1]

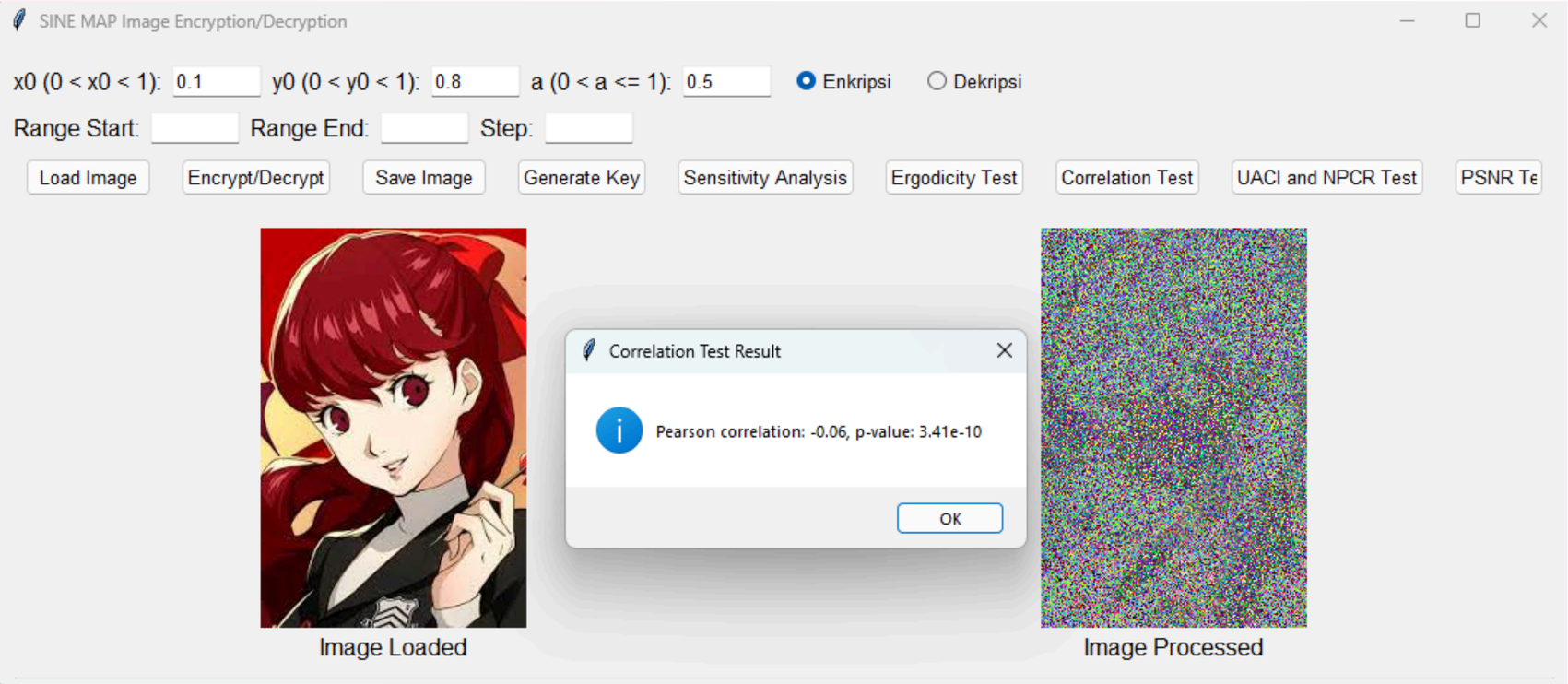


X0 = 0.7

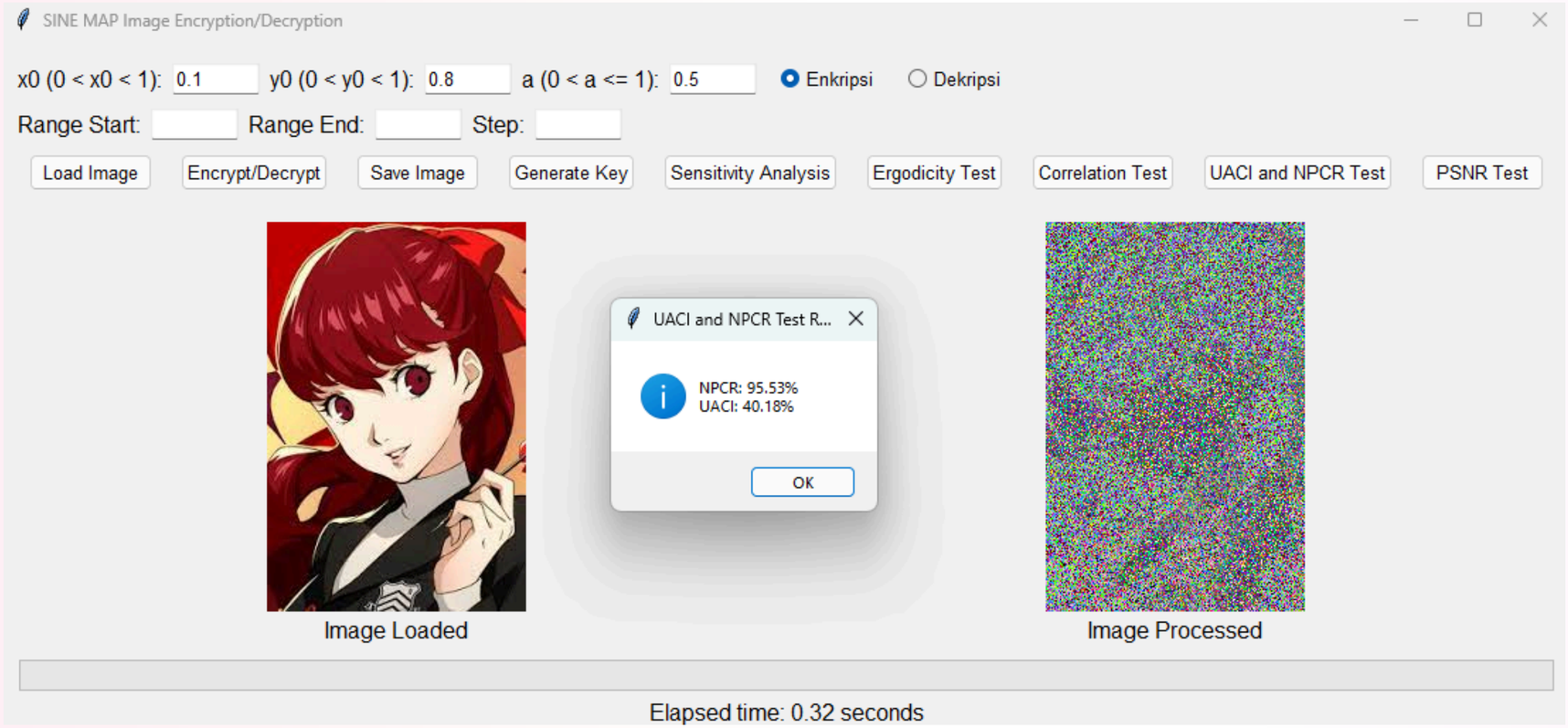


X0 = 1

Analisis [Uji korelasi]



Analisis [Uji UACI dan NPCR]



Analisis [Rata-Rata Waktu Proses]

No	Pixel	Waktu Enkripsi (s)	Waktu Dekripsi (s)
1	80 x 80	0.03	0.03
2	128 x 128	0.07	0.07
3	480 x 480	1.05	1.05
4	720 x 720	2.16	2.13
5	1080x 1080	4.56	4.69
6	1920 x 1920	13.92	14.15

Get protected today!

Link Github:

https://github.com/Abdfikih/Sine-Map-Encryption.git