International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2016; 1(6): 27-39

www.mathsjournal.com
Received: 15-09-2016
Accepted: 17-10-2016

Abdellatif JarJar
Moulay Rachid High School,
Taza, Morocco

New chaotic map and its application in encrypted color image

Abdellatif JarJar

Abstract
This paper traces the process of constructing a new one-dimensional chaotic map, and will provide a simple application in color image encryption. The use of Sakovskii's theorem will make it possible to determine the existence of chaos and restrict all conditions to ensure the existence of this new sequence. In addition, the sensitivity to initial conditions will be proved by Lyapunov's index value. Similarly, the performance of this new chaotic map will be illustrated graphically and compared with other chaotic maps most commonly used in cryptography. Finally, a humble color image encryption application will show the power of this new chaotic map.

$$Abreviation \begin{cases} I = [0\ 1] \\ f: continuous\ function\ over\ I \\ f^k(x) = \underbrace{fofof \ldots \ldots \ldots of(x)}_{k\ instances} \\ G_n = \mathbb{Z}/_{n\mathbb{Z}}\ Ring \end{cases}$$

Keywords: Chaotic function, Lyapunov's exponent, Sarkovskii's theorem

Introduction
Chaos is a phenomenon very close to randomness, which occupies an important position in cryptography, but determinism and dynamics distinguish it from randomness. In the past three decades, chaos has swept through most sciences (mathematics, physics, biology). It is defined by a nonlinear equation that is very sensitive to initial conditions. The expansion of chaos theory is closely related to the development of computer science and new mathematical advances (modeling, simulation, etc.). Like all new theories, chaos theory is still the subject of many controversies. Various forms of disputes have caused disputes over legal opinions and interpretations. Will science be able to explain it more and more, or is it impossible to understand the world by accident? In fact, for scientists, this is a matter of defining the complexity of the phenomenon they are studying. Chaos as understood by scientists does not mean that there is no order. In fact, this is related to unpredictability, because the final state is very sensitive to the initial state, so long-term evolution cannot be predicted. We believe that the difference between chaos and randomness is the most important point for understanding chaos. Indeed, there is always a tendency to believe that a phenomenon is unpredictable due to the large number of parameters involved. In his description, this prompted us to give a probabilistic method, which by definition can satisfy a certain degree of freedom completely satisfactorily. Randomness. As far as chaos is concerned, this is actually not the case, and the behavior of the chaotic system seems to be random. But in reality, this behavior is described in a deterministic way by fully deterministic nonlinear equations, that is, in particular using mathematics that allow accurate and deterministic methods. To explain with a famous advertisement, a person can write: "Looks like an opportunity, tastes like an opportunity, but not accidental. With the passage of time, people have made several attempts to build a chaotic graph, and realized the password A large number of chaotic graphs used in learning. Domain [1]. Other technologies use chaotic maps to construct hash functions [2]. On the other hand, other technologies use chaotic cards in symmetric encryption systems [3].

Corresponding Author:
Abdellatif JarJar
Moulay Rachid High School,
Taza, Morocco

There are also some the technology combines several chaotic maps to improve performance. Their system [4-6]. In the absence of any deterministic formula for generating random numbers, tables of such numbers appeared.

1. Pseudo-random number generator

Finding that they were unable to master random numbers, researchers quickly turned to the generation of pseudo-random numbers defined by mathematical relationships that produce the same sequence under the same conditions. Among all these technologies, we mentioned the most important ones

2. Von Neumann Generator

In 1946 Von Neumann proposed the following pseudo-random number generator

- Take an integer (x_0) of n digits
- Calculate $(x_1 = x_0^2)$
- Take the (n) middle digits
- Restart

3. Linear congruence generator

The linear congruential generator was introduced by Lehmer, and is still popular in today's methods for generating pseudorandom numbers quickly. The sequence of random numbers (x_n)*is created as follows:*

$$Equation\ 9 \begin{cases} x_0 \in \mathbb{Z}/n\mathbb{Z} \\ x_{n+1} = (ax_n + c) \bmod n \end{cases}$$

In order to be able to choose a seed x_0 without constraints between 0 and $n - 1$, it is necessary to try to maximize the generator period. However, it turns out that the values of a and c are known, which makes it possible to obtain a maximum period (equal to n).

The period of a linear congruential generator is maximum if and only if:

- if $c \neq 0$ then c is prime with n. $\mathrm{Pgcd}(c, n) \Longrightarrow c \wedge n = 1$.
- For each prime number p dividing n, $(a - 1)$ is a multiple of p.
- $(a - 1)$is a multiple of 4 if n is one

II. Selected popular chaotic maps

Functions that generate chaotic sequences can be divided into two categories: one-dimensional sequences and multi-dimensional sequences. Chaotic functions are rare in the literature, and there are only a dozen functions used in cryptography.

1. One-dimensional chaotic map

a. Logistic recurrence

Logistic recursion [7] is a simple example of nonlinear sequence. It is defined by a simple relation managed by a second order polynomial described by the following recurrence relation

$$\text{Equation 1} \begin{cases} u_0 \in]0{,}5\ 1[, \mu \in [3{,}75\ 4] \\ u_{n+1} = \mu u_n(1 - u_n) \end{cases}$$

b. The Skew Tent Map

The Skew tent map [8] will be redefined as the equation below

$$\text{Equation 5} \begin{cases} v_0 \in]0\ 1[\ p \in]0{,}5\ 1[\\ v_{n+1} = \begin{cases} \dfrac{v_n}{p} \text{ if } 0 \prec v_n \prec p \\ \dfrac{1 - v_n}{1 - p} \text{ if } p \prec v_{n<1} \end{cases} \end{cases}$$

c. PWLCM Map

It is a real linear sequence [9] by pieces defined by the equation below

$$\text{Equation 6 } w_n = f(w_{n-1}) = \begin{cases} \dfrac{w_{n-1}}{d} \text{ if } 0 \leq w_{n-1} \leq d \\ \dfrac{w_{n-1} - d}{0.5 - d} \text{ if } d \leq w_{n-1} \leq 0.5 \\ f(1 - w_{n-1}) \text{ else} \end{cases}$$

The simplicity and robustness of this card encourages researchers to use it in cryptography.

III. Recommended knowledge

Before revealing the structure of this new map, it is necessary to define some basic properties. Let (f) be a continuous function over the interval(I) and defined by the equation

Equation11 $\begin{cases} f: I \rightarrow I \\ x \rightarrow f(x) \end{cases}$

We are going to give some definitions to clarify all the points of the article

1. Trajectory

Let (x) be an element of (I), we call the trajectory of x the set of iterates of(x) by the function (f). This set is defined by

Equation 12 $\Gamma_x = \{x, f(x), f^2(x), \dots \dots .. f^k(x), \dots\}$

2. Periodicity

We say that $x \in I$ is periodic if there is an integer (r) such that

Equation 13 $f^r(x) = x$

In that case we'll have

Equation 14 $\Gamma_x = \{x, f(x), f^2(x), \dots \dots .. f^k(x), \dots, f^{r-1}(x)\}$

3. Period

The (l) period of an element $x \in I$ is the smallest integer r such that

Equation 16 $l = \underbrace{Min}_{r \in \mathbb{N}} \ f^r(x) = x$

We notice that if (l) is the period of element (x) then

Equation 17 $\forall r \in \mathbb{N}: f^r(x) = x$ then $\exists q: r = ql$

4. Transitive topology

Let (f) be a continuous function on I. We say that (f) is topologically transitive if: Equation 18 $\forall (U, V)$Ouverts $\subset I$; $\exists (x, p) \in U x \mathbb{N} \ / f^p(x) \ \in V$

5. Density

It is said that(f) is dense in (I)if: Equation 19 $\forall (x, y) \ \in IxI$; $\exists (\alpha, p) \in Ix\mathbb{N} \ / f^p(\alpha) \ \in [x\ y]$

6. Initial Condition Sensitivity

It is said that(f) is sensible to the initial conditions if

Equation 20 $\exists \rho > 0, \forall\ x \in I, \forall\ \mu > 0, \exists (y, p) \in Ix\mathbb{N} \begin{cases} |x - y| < \mu \\ \text{Then} \\ |f^p(x) - f^p(y)| > \rho \end{cases}$

In other words For $\rho \in I$ and $\rho^* = \rho + \epsilon$: $\in \sim 10^{-32}$ then $\Gamma_{\rho \neq} \Gamma_{\rho+\epsilon}$

7. Fixed points nature

a. Definition

(x) is a fixed-point if Equation 21 $(f(x) = x)$ here are two types of fixed points

b. Attractive fixed point

(x) is an attractive fixed point if and only if Equation 22 $\exists (\alpha_n = f^n(\alpha_0))$ that $\lim(\alpha_n) = x$

c. repulsive fixed point

(x) is a repulsive fixed point if it is not attractive.

i. Property

If function (f) is derivable then

Equation 23 $\begin{cases} |f'(x)| > 1 \text{ then x attractive fixed point} \\ |f'(x)| < 1 \text{ then x repulsive fixed point} \\ |f'(x)| = 1 \text{ then ambiguity} \end{cases}$

IV. New chaotic function design

1. Chaotic function

a. Definition

(f) is a chaotic function if and only if:

- the set of periodic points is dense in (I)
- f is transitive topologically
- f shows sensitivity to initial conditions

Let (f) be a continuous function over the interval I and defined by the equation

Equation 24 $$\begin{cases} f: I \to I \\ \text{Let } (p > 0 \\ f(x) = \begin{cases} p^2 x \text{ if } 0 \le x \le \dfrac{1}{1+p} \\ p - px \text{ if } \dfrac{1}{1+p} \le x \le 1 \end{cases} \end{cases}$$

1. Graphic representation of the function (f)

The function (f) defined by the equation can be represented by the following figure

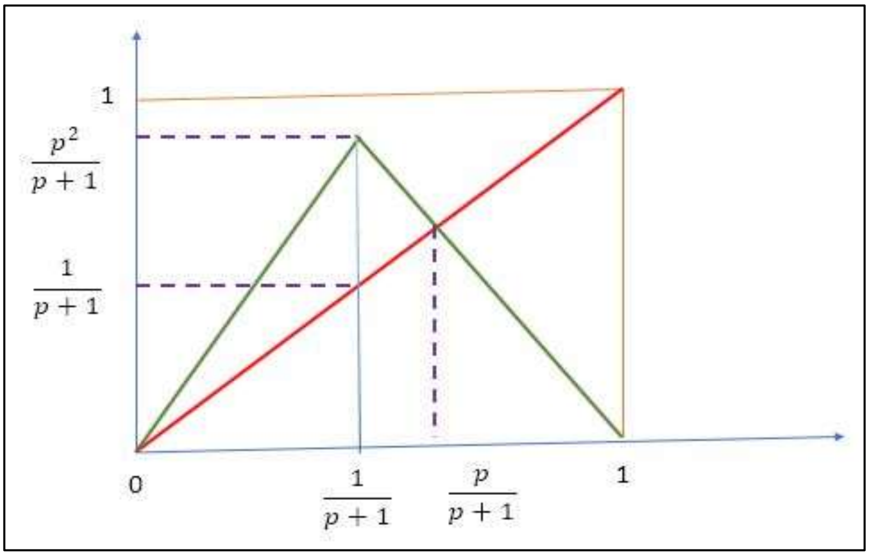


Fig 1: Basic function graph

2. Existence domain of function f

For the sequence (x_n) to exist it is necessary that $f(I) \subset I$. So, it is necessary that

Equation 25 $$\begin{cases} \dfrac{p^2}{1+p} < 1 \\ \text{So} \\ p^2 - p - 1 < 0 \end{cases}$$

Let's put $\varphi = \frac{1+\sqrt{5}}{2}$ (Gold – Number) **So** Equation 26 $p \in [0\ \varphi\ ]$

3. Derived from f

The function (f) is continuously derivable and its derivative is given by the expression

Equation 27 $$\begin{cases} f'(x) = p^2 \text{ if } 0 \le x \le \dfrac{1}{1+p} \\ f'(x) = -p \text{ if } \dfrac{1}{1+p} \le x \le 1 \end{cases}$$

4. (f) fixed points

The two stationary points of (f) are

Equation 28 $\begin{cases} \alpha = 0 \\ \beta = \dfrac{p}{1+p} \end{cases}$

5. Fixed points nature

We have

Equation 29 $\begin{cases} |f'(\alpha)| = p^2 \\ |f'(\beta)| = \begin{cases} p^2 \text{ if } 0 \le \beta \le \frac{1}{1+p} \\ p \text{ if } \frac{1}{1+p} \le \beta \le 1 \end{cases} \end{cases}$ **So** Equation 30 $\begin{cases} \text{if } p < 1 \text{ then } \alpha \text{ is attractive fixed point} \\ \text{if } p > 1 \text{ then } \alpha \text{ is repulsive fixed point} \end{cases}$

Therefore, Preliminary positioning of control parameters (p)Equation31 $p \in [1\ \varphi]$

V. Chaotic sequence building

The sequence (x_n) is defined by the following expression

Equation 32 $\begin{cases} x_0 \in [0\ 1]\ p \in [1\ \varphi] \\ f(x_n) = x_{n+1} \begin{cases} p^2 x_n \text{ if } 0 \le x_n \le \dfrac{1}{1+p} \\ p - p x_n \text{ if } \dfrac{1}{1+p} \le x_n \le 1 \end{cases} \end{cases}$

1. Initial Condition Sensitivities

To measure the sensitivity to the initial conditions of the sequence (x_n) defined by function (f), we have to calculate the Lyapunov exponent

Equation 33 $\lambda = \lim_{n\to\infty} \left(\frac{1}{n}\right) \sum_{k=0}^{n} \mathrm{Log}_2 |f'(x_k)|$

In our case, we notice that

Equation 34 $\lambda \gg \lim_{n\to\infty} \left(\frac{1}{n}\right) \sum_{k=0}^{n} \mathrm{Log}_2 |f'(x_k)| = \lim_{n\to\infty} \left(\frac{1}{n}\right) \sum_{k=0}^{n} \frac{3}{2} \mathrm{Log}_2(p) \approx \frac{3}{2} \mathrm{Log}_2(p) > 0$

We can conclude from the value of the Lyapunov exponent that the sequence (x_n) defined by the function (f) is sensitive to the initial conditions. This value is higher than the value of the logistics diagram, indicating that it is highly sensitive to initial conditions and control parameters.

Fig 2: Lyapunov exponent variation with p

The logarithmic scale plot shows that the distance between two very close initial conditions varies according to an exponential law.

2. Sarkovskii's Theorem

Order of Sarkovskii

$$\begin{cases} 3 \succ 5 \succ 7 \succ 9 \succ 11 \succ \cdots\cdots \\ 3*2 \succ 5*2 \succ 7*2 \succ 9*2 \succ \cdots\cdots \\ 3*2^2 \succ 5*2^2 \succ 7*2^2 \succ 9*2^2 \succ \cdots \\ \vdots \\ \vdots \\ 3*2^n \succ 5*2^n \succ 7*2^n \succ 9*2^n \succ \cdots \\ \vdots \end{cases}$$

All-natural integers are represented in this Sarkovskii order.

- The first line represents odd numbers
- The row line (n) represents the numbers $2^{n-1}(2k+1)$

a. Theorem

Let f: I $\rightarrow$ I continue. Suppose that (f) has a periodic point of period(k). If $(k \succ \ell)$ according to Sarkovskii's order, then f also has a periodic point of period (ℓ).

b. Corollary (Lie and York)

If (f) admits an item from period 3, then it admits an item of any order. As a result, the function has a chaotic appearance.

i. Search for a period point 3

Let

Equation 35 Let $x^* = \dfrac{p}{1+p^5} \in I$

Let's demonstrate that $(x^*)$is a point of period 3

Let's prove that

Equation 36 $\dfrac{p}{1+p^5} < \dfrac{1}{1+p} \Longrightarrow p^5 - p^2 - p + 1 > 0$ for $p \in [1\ \varphi]$

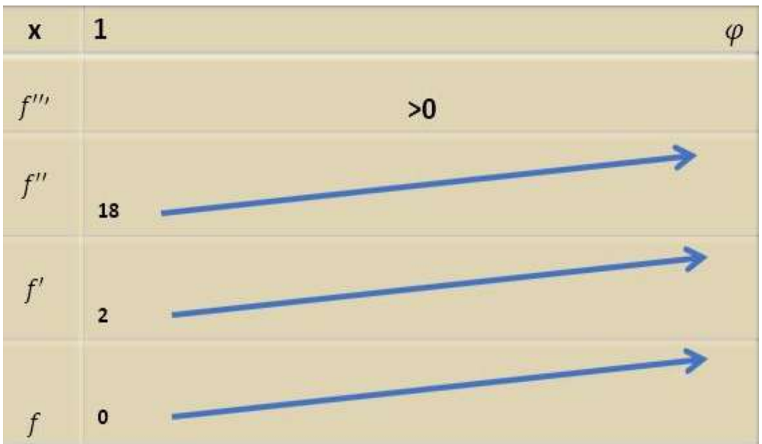
Let's put

Equation 37 $f(p) = p^5 - p^2 - p + 1$

Therefore

Equation 38 $\begin{cases} f'(p) = 5p^4 - 2p - 1 \\ f''(p) = 20p^3 - 2 \text{ So } f^{(3)}(p) = 60p^3 > 0 \end{cases}$

The following table gives the variations of the functions



So

$\forall p \in [1\ \varphi]\ \dfrac{p}{1+p^5} < \dfrac{1}{1+p}$

Therefore

$$\text{Equation 40}\begin{cases} f(x^*) = \dfrac{p^3}{1+p^5} \\ \text{Let's compare } \dfrac{p^3}{1+p^5} \text{ and } \dfrac{1}{1+p} \end{cases}$$

Let's look at the sign of the function (f) defined by

$$f(p) = p^5 - p^4 - p^3 + 1$$

According to a rough calculation we have For $p \in [1{,}47\ \varphi]$ $f'p) > 0$ So

$$\text{Equation 41}\begin{cases} \text{For } p \in [1{,}47\ \varphi] \text{ We have} \\ f(x^*) = \dfrac{p^3}{1+p^5} \\ f^{(2)}(x^*) = \dfrac{p^5}{1+p^5} > \dfrac{1}{(1+p)} \\ f^{(3)}(x^*) = p - p\dfrac{p^5}{1+p^5} = \dfrac{p}{1+p^5} = x^* \end{cases}$$

$x^* = \frac{p}{1+p^5}$ is a periodic point of period 3, therefore(f)is a chaotic function according to Sarkovskii's corollary. This period point 3 is illustrated by the following figure

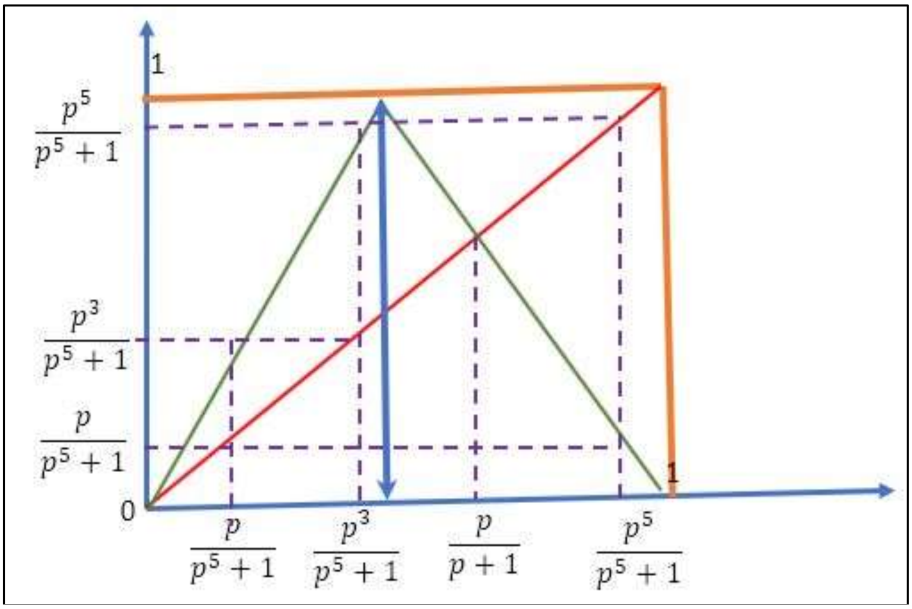


Fig 3: Period point 3

3. Initial sequence values

Period doubling

We know that the only fixed points are

$$\text{Equation 42}\begin{cases} \alpha = 0 \\ \beta = \dfrac{p}{1+p} \end{cases}$$

searches for points (x_0) for which there is a k such that

$$f^k(x_0) = \beta$$

If there is such a point (x_n) then the sequence (x_n) is stationary. For $(k = 1)$, we have

$$\text{Equation 43} \quad \begin{cases} f(x_0) = \beta = \dfrac{p}{1+p} \\ \text{So} \\ x_0 = \dfrac{1}{p(1+p)} \end{cases}$$

For $(k = 2)$, we have

$$\text{Equation 44} \quad \begin{cases} f^2(x_0) = \beta = \dfrac{p}{1+p} \\ \text{So} \\ x_0 = \dfrac{1}{p^3(1+p)} \end{cases}$$

By recurrence, we obtain For $(k = n)$, we have

$$\text{Equation 45} \quad \begin{cases} f^n(x_0) = \beta = \dfrac{p}{1+p} \\ \text{So} \\ x_0 = \dfrac{1}{p^{2n-1}(1+p)} \end{cases}$$

If there is (n) such that the initial condition $x_0 = \frac{1}{p^{2n-1}(1+p)}$, then the sequence would be stationary from the n iteration onwards. Then the sequence is no longer chaotic. We construct a sequence (y_n) defined by:

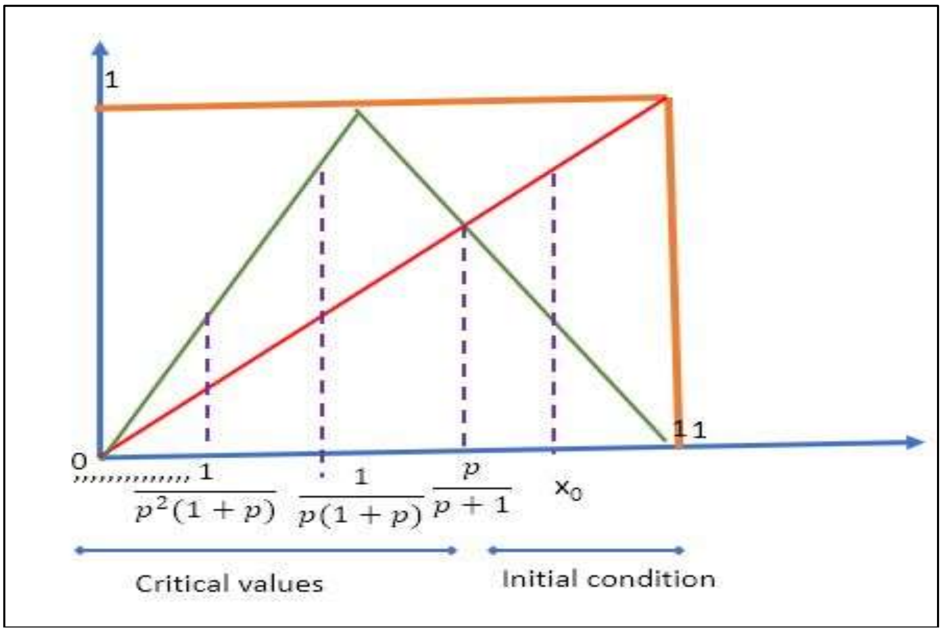
$$\text{Equation 46} \quad \begin{cases} n \geq 1 \\ \text{We have} \\ y_n = \dfrac{1}{p^{2n-1}(1+p)} \sim \dfrac{1}{p^{2n}} \end{cases}$$

(y_n) is a decreasing sequence minus 0, converging donations, and we have the following equation;

$$\text{Equation 47} \quad \text{For } p > 1 \text{ we have } \lim_{n\to\infty}(y_n) = 0$$

Finaly

$$\text{Equation 48} \quad \begin{cases} x_0 > \dfrac{1}{(1+p)} \quad p \in [1{,}47\ \varphi] \\ f(x_n) = x_{n+1} \begin{cases} p^2 x_n \text{ if } 0 \leq x_n \leq \dfrac{1}{1+p} \\ p - p x_n \text{ if } \dfrac{1}{1+p} \leq x_n \leq 1 \end{cases} \end{cases}$$



The sequence (x_n) defines is a chaotic sequence under the specified conditions.

We are looking for an element $x_0 > \frac{1}{(1+p)}$ such as

$$\exists\, k \in \mathbb{N} \text{ such as } f(x_0) = x_k = \frac{1}{p^{2k-1}(1+p)} < \frac{1}{(1+p)}$$

If such a point exists then two situations present themselves

$$x_0 > \frac{p}{(1+p)} \text{ or } x_0 \in \left[\frac{1}{(1+p)}, \frac{p}{(1+p)}\right]$$

Situation 1

$$\text{if } x_0 \in \left[\frac{1}{(1+p)}, \frac{p}{(1+p)}\right] \text{ then } f(x_0) > \frac{p}{(1+p)}$$

Situation 2

$$\text{if } x_0 > \frac{p}{(1+p)} \text{ then } f(x_0) < \frac{p}{(1+p)}$$

$$\text{So} \begin{cases} p - px_0 = \dfrac{1}{p^{2k-1}(1+p)} \\ \text{So} \\ x_0 = \dfrac{p^{2k-1}(1+p) - 1}{p^{2k-1}(1+p)} < \dfrac{1}{(1+p)} \end{cases}$$

In this case the sequence would be stationary from iteration (k)

$$f^k(x_0) = \frac{p}{1+p}$$

Moreover, we have,

$$\forall\, k \in \mathbb{N}: \frac{p^{2k-1}(1+p) - 1}{p^{2k-1}(1+p)} > \frac{p}{1+p}$$

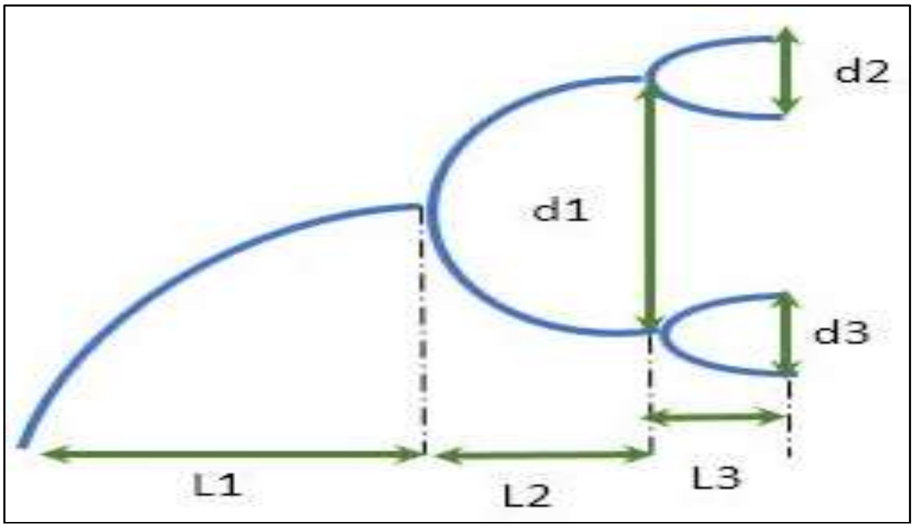
Finally

$$\text{Equation 34} \begin{cases} x_0 \in \left[\dfrac{1}{(1+p)}, \dfrac{p}{(1+p)}\right] \; p \in [1{,}47\ \varphi] \\ f(x_n) = x_{n+1} \begin{cases} p^2 x_n \text{ if } 0 \le x_n \le \dfrac{1}{1+p} \\ p - px_n \text{ if } \dfrac{1}{1+p} \le x_n \le 1 \end{cases} \end{cases}$$

This sequence is chaotic

4. Feigenbaum's Constants - Renormalization –

In 1975 the physicist Feigenbaum noticed that the general pattern of the logistic sequence was repeated at each bifurcation to within a factor of scale. He then used a process of renormalization. This involves enlarging smaller and smaller parts of the graph and comparing these magnifications to the original pattern. When the enlarged pattern reproduces the first pattern, it is called self-simulation. As it grows to infinity, the general structure repeats itself. If globally, the duplications are not the same, they keep the same ratios



The first constant intervening horizontally

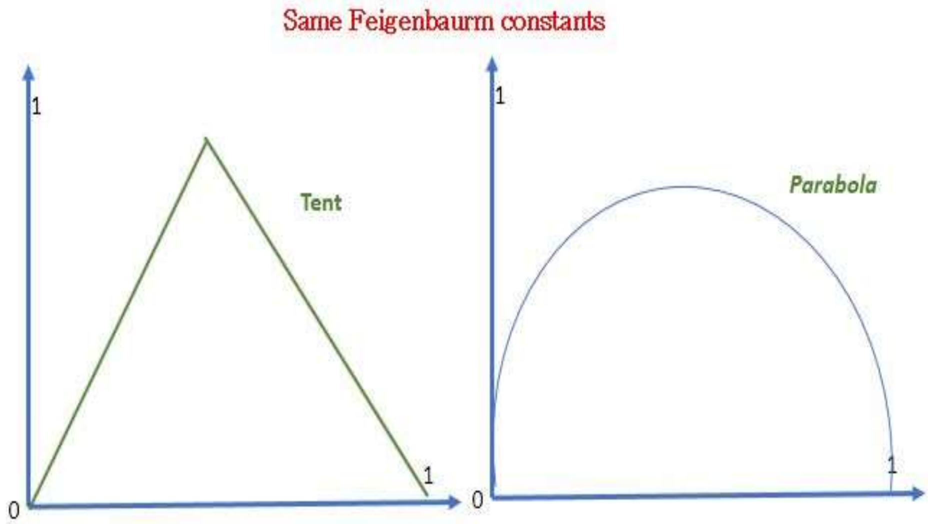
$$\frac{L_1}{L_2} \approx \frac{L_2}{L_3} \approx 4{,}57$$

The second constant occurring vertically

$$\frac{d_1}{d_2} \approx \frac{d_2}{d_3} \approx 2{,}5$$

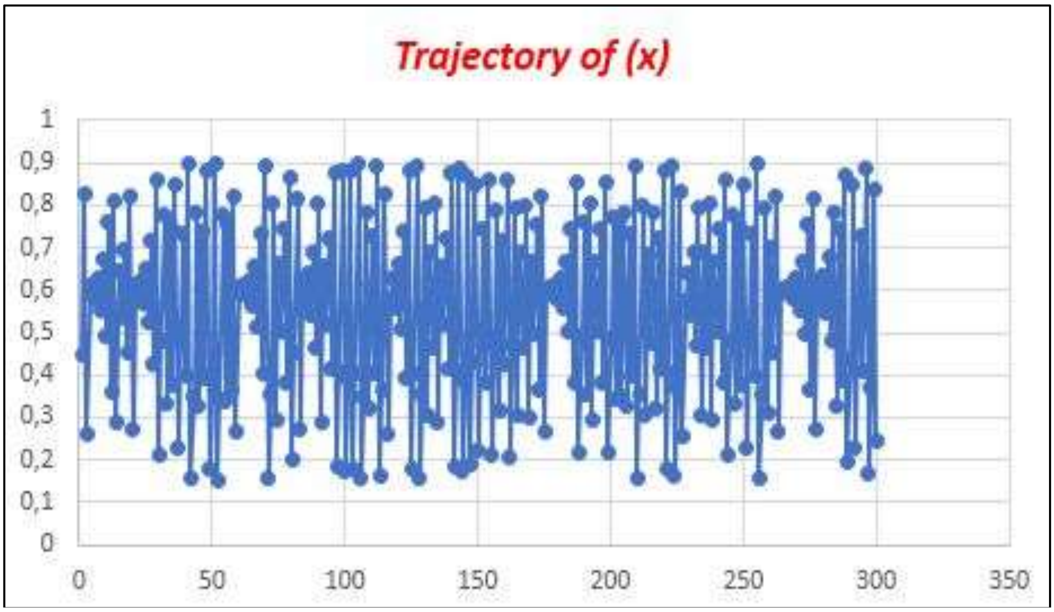
5. Universality

The same sequence, but defined by another function (f) defines single hump type has the same properties



6. Some simulations

$$\begin{cases} x_0 = 0{,}45 \\ p = 1{,}5 \end{cases}$$



The trajectory seems to be random

a. Deviation

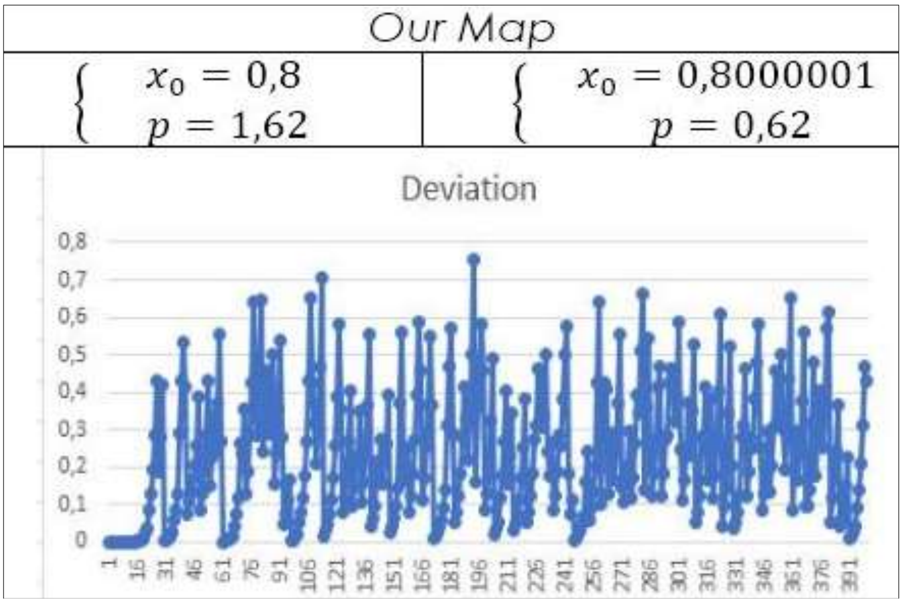


Fig 5: We have noticed that small disturbances under initial conditions will greatly deviate from the trajectory.

VI. Cryptography application

We will introduce the improvement of Hill's classic method using the new chaotic map as the private key to illustrate the performance of our new chaotic map. After reading the original image and switching to the vector, a chaotic vector of the same size is generated from the new map (in the simulation, we take $p = 1.54, x_0 = 0.623$)

- Our algorithm
- Subdivision of the image vector into blocks of three pixels, as well as the chaotic vector.
- Calculation of the initialization vector
- Modification of the priming block
- Application of Hill's improved method.
- application of dissemination
- reconstruction of the encrypted image

The encryption process is as follows

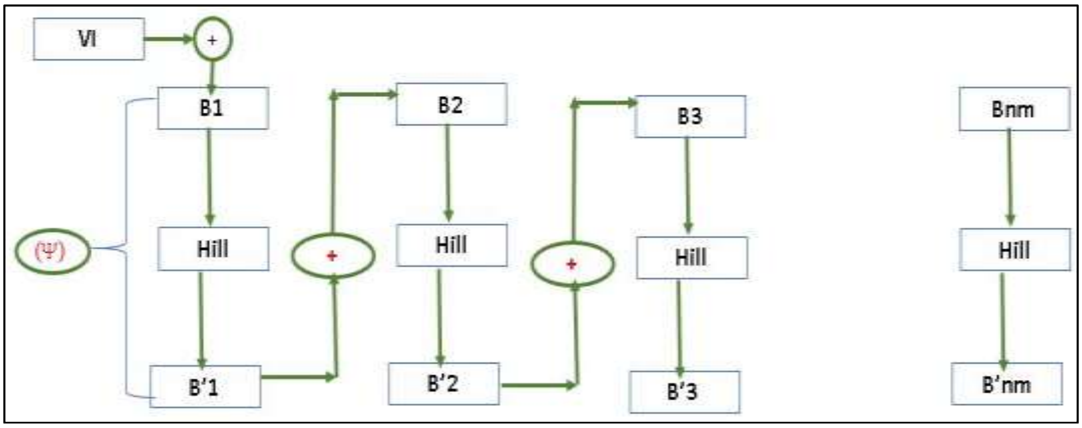


Fig 3: Encryption process

The encryption function is defined by

$$\text{Algorithm1}\begin{cases} B_1 = IV \oplus B_1 \\ \Psi(B_1) = B_1' = HB_1 \oplus TV1 \\ \text{for } i = 2 \text{ to nm} \\ B_i = B_{i-1} \oplus B_i \\ \Psi(B_1) = B_1' = HB_1 \oplus TVi \\ \text{Next } i \end{cases}$$

The use of vector (Tvi) aims to overcome the linearity problem of classical systems.
Construct the encryption key matrix from the new chaotic map by the following expression

$$H = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & q \end{pmatrix} \text{ With a, d, q } \epsilon \left(\mathbb{Z}/256\mathbb{Z}\right)^* \text{and b, c, e } \mathbb{Z}/256\mathbb{Z}$$

After the simulation is complete, we get

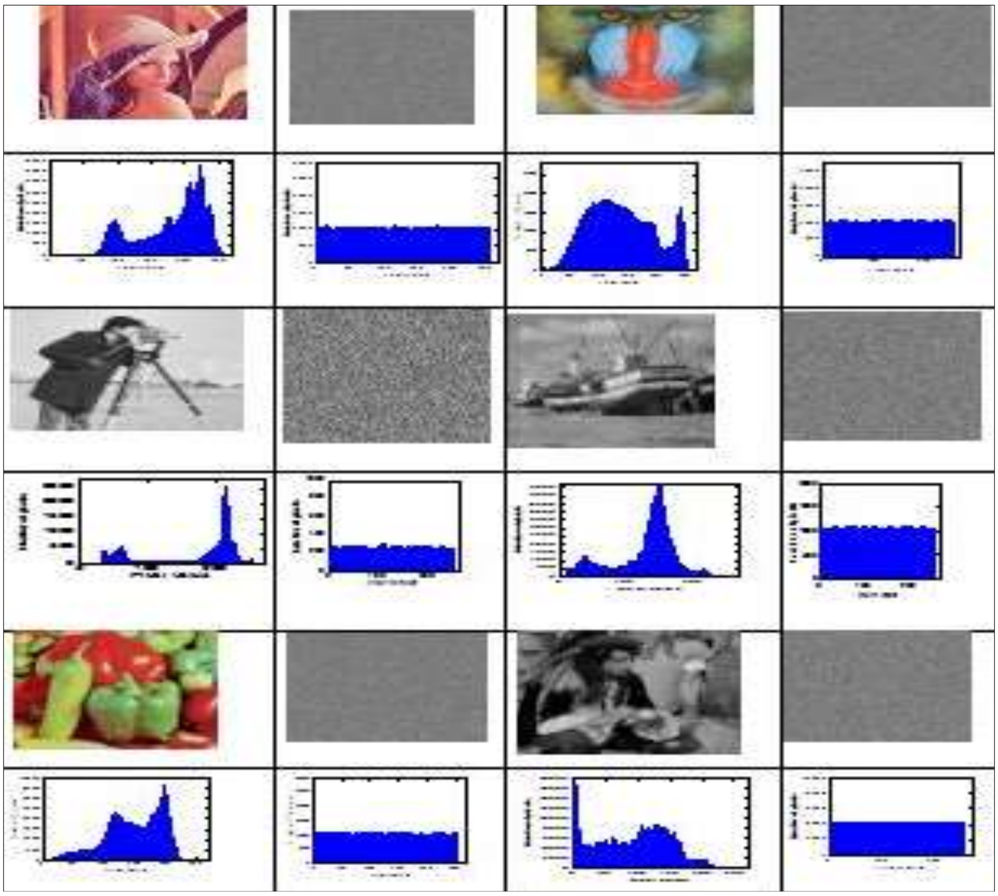


Table 3: Encrypted image histogram

Conclusion

Faced with various difficulties in constructing random numbers, researchers are committed to using generators that follow simple mathematical formulas to create pseudo-random numbers. With the passage of time, chaos theory suddenly appeared, and due to the need to use passwords with such numbers to create private encryption keys, chaos was born. We have witnessed the emergence of some chaotic maps in color image encryption. Our article contributed to the creation of a new chaotic map, and implemented the chaotic map in the color image encryption example by enhancing the classic Hill function. The proof of chaos is proved using Sarkovskii's theorem and the inference of Lie and York. The map will be added to the list of existing maps on the market to increase this range.

References

1. Abdullah G¨ul University, Kayseri 38080, Turkey" Chaotic Map Construction from Common Nonlinearities and Microcontroller Implementations" International Journal of Bifurcation and Chaos 2016;26(7):1650121. (11 pages)
2. Author links open overlay panel Huaqian Yang abKwok- Wo Wong b Xiao feng Liaoc Yong Wang dDegang Yang "One-way hash function construction based on chaotic map network" Chaos, Solitons & Fractals 2009;41(5):2566-2574.
3. Yantao Li, Shao jiang Deng, Di Xiao. "A novel Hash algorithm construction based on chaotic neural network" Neural Computing and Applications 2011;20:133-141.
4. Nicolas Bierne John Welch Etienne Loire François Bonhomme Patrice David » The coupling hypothesis: why genome scans may fail to map local adaptation genes" Wilyu online library First published 2011.
5. Jacques Patarin. Security of Random Feistel Schemes with 5 or More Rounds »Annual International Cryptology Conference CRYPTO 2004: Advances in Cryptology – CRYPTO 2004, 106-122| Cite as
6. Author links open overlay panel Sahar Mazloom Amir Masud Eftekhari-Moghadam » Color image encryption based on Coupled Nonlinear Chaotic Map" Chaos, Solitons & Fractals 2009;42(3):1745-1754.
7. Xiao Feng, Xiaolin Tian § Shaowe iXia, "An Improved Image Scrambling Algorithm Based On Magic Cube Rotation and Chaotic Sequences", IEEE press,4th International Congress on Image and Signal Processing, 2011, 1021-1024.
8. Hraoui S, Gmira F, Jarar AO, Satori K, Saaidi A. Benchmarking AES and chaos based logistic map for image encryption. Computer Systems and Applications (AICCSA), ACS International Conference 2013.
9. Jarjar A. Improvement of hill's classical method in image cryptography » International Journal of Statistics and Applied Mathematics 2017;2(3), Part A.
10. Pisarchik AN, Flores-Carmona NJ, Carpio-Valadez M. Encryption and decryption of images with chaotic map lattices" AIP Chaos 2006;16:033118.