*Journal of Multimedia Information System VOL. 8, NO. 2, June 2021 (pp. 131-142): ISSN 2383-7632 (Online)*
http://doi.org/10.33851/JMIS.2021.8.2.131

# New chaotic map development 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 Sarkovskii'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.

**Key Words**: Chaotic function; Lyapunov's exponent; Sarkovskii's theorem.

## I. 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. The large number of chaotic graphs used in learning [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]. There are also some the technology combines several chaotic maps to improve performance. Their systems [4], [5], [6] were in the absence of any deterministic formula for generating random numbers, tables of such numbers appeared.

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

**Pseudo-random number generator**

Finding that they were unable to master random numbers, researchers quickly turned to the generation of pseudo-

**Manuscript received March 01, 2021; Revised June 09, 2021; Accepted June 15, 2021. (ID No. JMIS-21M-03-009)**
Corresponding Author (*): Abdellatif JarJar, Moulay Rachid High School, Taza Morocco, abdoujjar@gmail.com

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.

### 1.1. Von Neumann Generator

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

1. Take an integer $(x_0)$ of n digits
2. Calculate $(x_1 = x_0^2)$
3. Take the $(n)$ middle digits
4. Restart

### 1.2. 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:

| Linear congruence generator | |
|---|---|
| $x_0 \in \mathbb{Z}/_{n\mathbb{Z}}$ | (1 |
| $x_{n+1} = (ax_n + c)\ mod\ n$ | ) |

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:

1. $if\ c \neq 0\ \ then$ c is prime with n.
   $Namely, it\ means\ Pgcd(c,n)$=1.
2. For each prime number $p\ dividing\ n$,
   $(a-1)\ is\ a\ multiple\ of\ p.$
3. $(a-1) is\ a\ multiple\ of\ 4\ if\ n\ is\ one$

### 1.3. 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.

### 1.4. One-dimensional chaotic map

*1.4.1 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.

| Logistic recurrence | |
|---|---|
| $u_0 \in ]0,5\ \ 1[\quad ,\ \mu \in [3{,}75\quad 4]$ | (2) |
| $u_{n+1} = \mu u_n(1-u_n)$ | |

*1.4.2. The Skew Tent Map*

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

| The skew tent map | |
|---|---|
| $v_0 \in ]0\ \ 1[\quad p \in ]0,5\ \ 1[$ | |
| $v_{n+1} = \begin{cases} \frac{v_n}{p} & if\ \ 0 \prec v_n \prec p \\ \frac{1-v_n}{1-p} & if\ p \prec v_{n<1} \end{cases}$ | (3) |

*1.4.3. PWLCM Map*

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

| PWLCM | |
|---|---|
| $w_n = f(w_{n-1})$ | |
| $= \begin{cases} \frac{w_{n-1}}{d} & if\ \ 0 \le w_{n-1} \le d \\ \frac{w_{n-1}-d}{0.5-d} & if\ d \le w_{n-1} \le 0.5 \\ f(1-w_{n-1}) & else \end{cases}$ | (4) |

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

## II. 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.

| continuous function | |
|---|---|
| $f:\ \ I \to I$ | (5) |
| $x\ \to\ f(x)$ | |

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

### 2.1. 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

| Trajectory | |
|---|---|
| $\Gamma_x = \{x, f(x), f^2(x), \ldots\ldots f^k(x), \ldots\}$ | (6) |

### 2.2. Periodicity

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

| Periodicity |
|---|

*Journal of Multimedia Information System VOL. 8, NO. 2, June 2021 (pp. 131-142): ISSN 2383-7632 (Online)*
http://doi.org/10.33851/JMIS.2021.8.2.131

$$\exists\, r \in \mathbb{N};\ f^r(x) = x \qquad (7)$$

In that case we'll have

$$\Gamma_x = \{x, f(x), f^2(x), \dots\dots f^k(x), \dots, f^{r-1}(x)\} \qquad (8)$$

### 2.3. Period

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

| Period | |
|---|---|
| $l = \underbrace{Min}_{r\in\mathbb{N}}\ f^r(x) = x$ | (9) |

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

### 2.4. Transitive topology

Let $(f)$ be a continuous function on I. We say that $(f)$ is topologically transitive if:

| Transitive topology | |
|---|---|
| $\forall (U,V) Ouverts \subset I;\ \exists (x,p) \in UxN\ / f^p(x) \in V$ | (10) |

### 2.5. Density

It is said that $(f)$ is dense in $(I)$ if:

| Density | |
|---|---|
| $\forall (x,y)\ \in IxI;\ \exists (\alpha,p) \in IxN\ / f^p(\alpha)\ \in [x \quad y]$ | (11) |

### 2.6. Initial Condition Sensitivity

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

| Initial condition sensitivity | |
|---|---|
| $\exists \rho > 0\ , \forall\ x \in I, \forall\ \mu > 0, \exists (y,p) \in IxN \begin{cases} \lvert x-y\rvert < \mu \\ Then \\ \lvert f^p(x) - f^p(y)\rvert > \rho \end{cases}$ | (12) |
| In other words, | |
| $For\ \rho \in I\ and\ \rho^* = \rho + \epsilon:\ \in \sim 10^{-32}\ \ then\ \Gamma_{\rho \neq} \Gamma_{\rho+\epsilon}$ | |

### 2.7. Fixed points nature

*2.7.1. Definition*

$(x)$ *is* a fixed-point if

| Fixed point | |
|---|---|
| $(f(x) = x)$ | (13) |

here are two types of fixed points

*2.7.2. Attractive fixed point*

$(x)$ is an attractive fixed point if and only if

| Attractive fixed point | |
|---|---|
| $\exists \big(\alpha_n = f^n(\alpha_0)\big)\ that\ lim(\alpha_n) = x$ | (14) |

*2.7.3. repulsive fixed point*

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

*2.7.4. Property*

If function $(f)$ is derivable then

| Property | |
|---|---|
| $\lvert f'(x)\rvert > 1\ then\ x\ attractive\ fixed\ point$<br>$\lvert f'(x)\rvert < 1\ then\ x\ repulsive\ fixed\ point$<br>$\lvert f'(x)\rvert = 1\ then\ ambiguity$ | (15) |

## III. NEW CHAOTIC FUNCTION DESIGN

### 3.1. Chaotic function

*3.1.1. Definition*

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

the set of periodic points is dense in $(I)$

1. f is transitive topologically
2. f shows sensitivity to initial conditions
3. Let $(f)$ be a continuous function over the interval I and defined by the equation

| Chaotic function design | |
|---|---|
| $f:\ I \to I$<br>$Let\ \ (p > 0$<br>$f(x) = \begin{cases} p^2 x & if\ \ 0 \le x \le \frac{1}{1+p} \\ p - px & if\ \ \frac{1}{1+p} \le x \le 1 \end{cases}$ | (16) |

### 3.2. Graphic representation of the function $(f)$

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

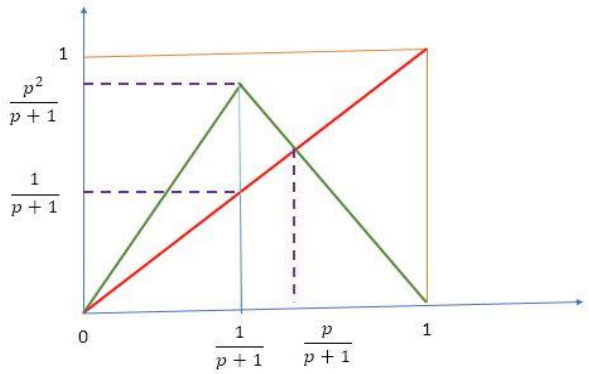



Fig. 1. Basic function graph.

### 3.3. 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

| Existence domain |
|---|

$$\begin{cases} \frac{p^2}{1+p} < 1 \\ So \\ p^2 - p - 1 < 0 \end{cases} \quad (17)$$

Let's put $\varphi = \frac{1+\sqrt{5}}{2}$ $(Gold - Number)$

$So \quad p \in [0 \quad \varphi\,]$

### 3.4. Derived from f

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

Derived from f

$$\begin{cases} f'(x) = p^2 \quad if \quad 0 \le x \le \frac{1}{1+p} \\ f'(x) = -p \quad if \quad \frac{1}{1+p} \le x \le 1 \end{cases} \quad (18)$$

### 3.5. $(f)$ fixed points

The two stationary po

$$\boldsymbol{(f)fixed\ point}$$

$$\begin{cases} \alpha = 0 \\ \beta = \frac{p}{1+p} \end{cases} \quad (19)$$

*3.5.1. Fixed points nature*

We have

Fixed point nature

$$\begin{cases} |f'(\alpha)| = p^2 \\ |f'(\beta)| = \begin{cases} p^2 \quad if \quad 0 \le \beta \le \frac{1}{1+p} \\ p \quad if \quad \frac{1}{1+p} \le \beta \le 1 \end{cases} \end{cases} \quad (20)$$

So

$$\begin{cases} if\ p < 1\ then\ \alpha\ is\ attractive\ fixed\ point \\ if\ p > 1\ then\ \alpha\ is\ repulsive\ fixed\ point \end{cases}$$

Therefore, Preliminary positioning of control parameters $(p)$

$$p \in [1 \quad \varphi] \quad (21)$$

### 3.6. Chaotic sequence building

The sequence $(x_n)$ is defined by the following expression

Chaotic sequence building

$$\begin{cases} x_0 \in [0 \quad 1] \quad p \in [1 \quad \varphi] \\ f(x_n) = x_{n+1} \begin{cases} p^2 x_n \quad if \quad 0 \le x_n \le \frac{1}{1+p} \\ p - p x_n \quad if \quad \frac{1}{1+p} \le x_n \le 1 \end{cases} \end{cases} \quad (22)$$

### 3.7. 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

Lyapunov exponent

$$\lambda = \lim_{n\to\infty} \left(\frac{1}{n}\right) \sum_{k=0}^{n} Log_2 |f'(x_k)| \quad (23)$$

In our case, we notice that

$$\lambda \gg \lim_{n\to\infty} \left(\frac{1}{n}\right) \sum_{k=0}^{n} Log_2 |f'(x_k)| = \lim_{n\to\infty} \left(\frac{1}{n}\right) \sum_{k=0}^{n} \frac{3}{2} Log_2(p) \approx \frac{3}{2} Log_2(p) > 0 \quad (24)$$

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.

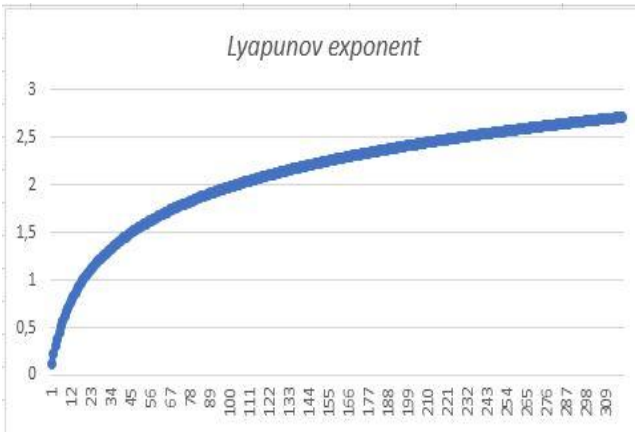



Fig. 2. Lyapunov exponent variation with p.

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

### 3.8. Sarkovskii's Theorem

Order of Sarkovkii

Sarkovskii's Theorem

$$\begin{cases} 3 \succ 5 \succ 7 \succ 9 \succ 11 \succ \cdots\cdots \\ 3*2 \succ 5*2 \succ 7*2 \succ 9*2 \succ \cdots\cdots \\ 3*2^2 \succ 5*2^2 \succ 7*2^2 \succ 9*2^2 \succ \cdots \\ \vdots \\ \vdots \\ 3*2^n \succ 5*2^n \succ 7*2^n \succ 9*2^n \succ \cdots \\ \vdots \end{cases} \quad (25)$$

All-natural integers are represented in this Sarkovkii order.

The first line represents odd numbers

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

*3.8.1. Theorem*

Let $f: I \to I$ 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 $(\ell)$.

*3.8.2. Corollary (Lie & 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.

Search for

*3.8.3. period point 3*

Let

Period point 3

$$Let\ x^* = \frac{p}{1+p^5} \in I \qquad (26)$$

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

Let's prove that

$$\frac{p}{1+p^5} < \frac{1}{1+p} \Rightarrow p^5 - p^2 - p + 1 > 0 \quad for \quad p \in [1 \quad \varphi] \qquad (27)$$

Let's put

$$f(p) = p^5 - p^2 - p + 1 \qquad (28)$$

Therefore

$$\begin{cases} f'(p) = 5p^4 - 2p - 1 \\ f''(p) = 20p^3 - 2 \; So \; f^{(3)}(p) = 60p^3 > 0 \end{cases} \qquad (29)$$

The following table gives the variations of the functions

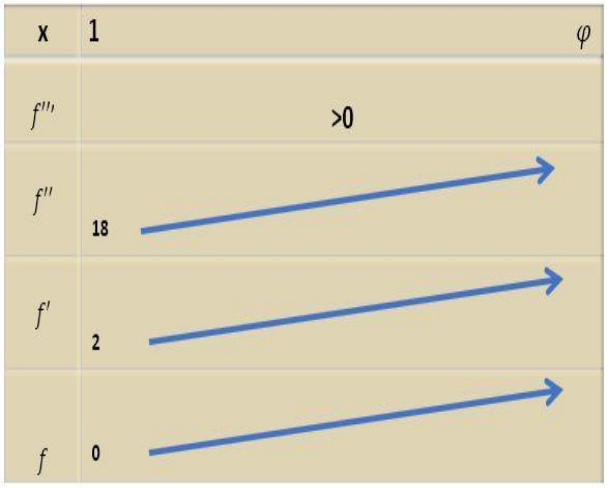



Fig. 3. Location of the period 3 point.

So

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

Therefore:

$$\begin{cases} f(x^*) = \dfrac{p^3}{1+p^5} \\ Let's\ compare \quad \dfrac{p^3}{1+p^5} \ and \ \dfrac{1}{1+p} \end{cases} \qquad (30)$$

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

$$f(p) = p^5 - p^4 - p^3 + 1 \qquad (31)$$

According to a rough calculation we have

$$For\ p \in [1{,}47 \quad \varphi] \quad f'p) > 0$$

$$\begin{cases} For\ p \in [1{,}47 \quad \varphi] \quad We\ have \\ f(x^*) = \dfrac{p^3}{1+p^5} \\ f^{(2)}(x^*) = \dfrac{p^5}{1+p^5} > \dfrac{1}{(1+p)} \\ f^{(3)}(x^*) = p - p\dfrac{p^5}{1+p^5} = \dfrac{p}{1+p^5} = x^* \end{cases} \qquad (32)$$

$x^* = \frac{p}{1+p^5}$ 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

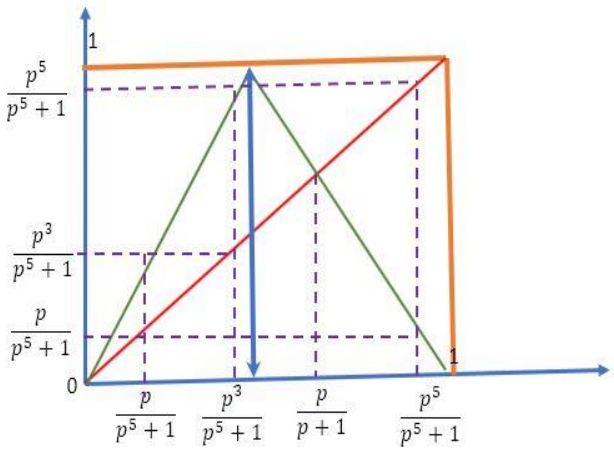



Fig. 4. Period point 3.

### 3.9. Initial sequence values

*3.9.1. Period doubling*

We know that the only fixed points are

Period doubling

$$\begin{cases} \alpha = 0 \\ \beta = \dfrac{p}{1+p} \end{cases} \quad (33)$$

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

$$\begin{cases} f(x_0) = \beta = \dfrac{p}{1+p} \\ So \\ x_0 = \dfrac{1}{p(1+p)} \end{cases} \quad (34)$$

For $(k = 2)$, we have

$$\begin{cases} f^2(x_0) = \beta = \dfrac{p}{1+p} \\ So \\ x_0 = \dfrac{1}{p^3(1+p)} \end{cases} \quad (35)$$

By recurrence, we obtain

For $(k = n)$, we have

$$\begin{cases} f^n(x_0) = \beta = \dfrac{p}{1+p} \\ So \\ x_0 = \dfrac{1}{p^{2n-1}(1+p)} \end{cases} \quad (36)$$

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:

$$\begin{cases} n \geq 1 \\ We\ have \\ y_n = \dfrac{1}{p^{2n-1}(1+p)} \sim \dfrac{1}{p^{2n}} \end{cases} \quad (37)$$

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

$$For\ p > 1\ we\ have\ \lim_{n\to\infty}(y_n) = 0 \quad (38)$$

Finally

$$\begin{cases} x_0 > \dfrac{1}{(1+p)} \qquad p \in [1{,}47 \quad \varphi] \\ f(x_n) = x_{n+1} \begin{cases} p^2 x_n & if \quad 0 \leq x_n \leq \dfrac{1}{1+p} \\ p - p x_n & if \quad \dfrac{1}{1+p} \leq x_n \leq 1 \end{cases} \end{cases} \quad (39)$$

This is illustrated by the following curve

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

$$\exists\ k \in \mathbb{N}\ such\ as\ f(x_0) = x_k = \frac{1}{p^{2k-1}(1+p)} < \frac{1}{(1+p)} \quad (40)$$

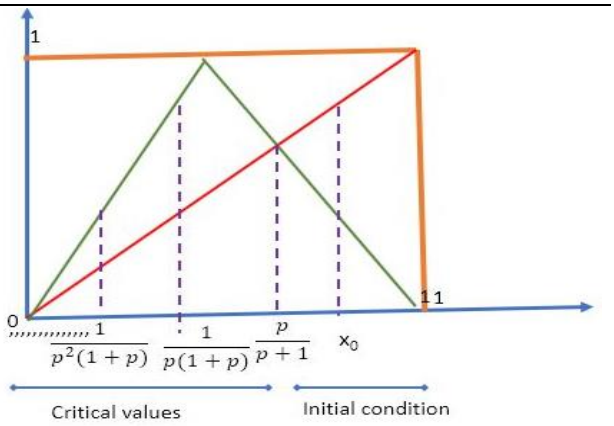



Fig. 5. Initial value.

If such a point exists then two situations present themselves

$$x_0 > \frac{p}{(1+p)} \quad or\ x_0 \in \left[\frac{1}{(1+p)} \quad \frac{p}{(1+p)}\right] \quad (41)$$

Situation 1

$$if\ \ x_0 \in \left[\frac{1}{(1+p)} \quad \frac{p}{(1+p)}\right]\ then\ \ f(x_0) > \frac{p}{(1+p)} \quad (42)$$

Situation 2

$$if\ \ x_0 > \frac{p}{(1+p)}\ \ then\ \ f(x_0) < \frac{p}{(1+p)} \quad (43)$$

So

$$\begin{cases} p - p x_0 = \dfrac{1}{p^{2k-1}(1+p)} \\ So \\ x_0 = \dfrac{p^{2k-1}(1+p) - 1}{p^{2k-1}(1+p)} < \dfrac{1}{(1+p)} \end{cases} \quad (44)$$

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

$$f^k(x_0) = \frac{p}{1+p} \quad (45)$$

Moreover, we have,

$$\forall k \in \mathbb{N} : \frac{p^{2k-1}(1+p)-1}{p^{2k-1}(1+p)} > \frac{p}{1+p} \quad (46)$$

Finally

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

This sequence is chaotic.

### 3.10. 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

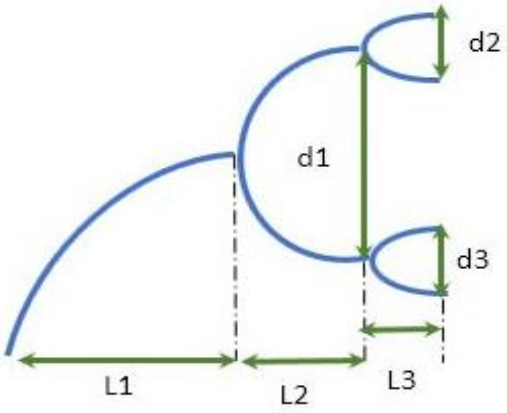



Fig. 6. Feigenbaum's Renormalization.

The first constant intervening horizontally

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

The second constant occurring vertically

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

#### *3.10.1. Universality*

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

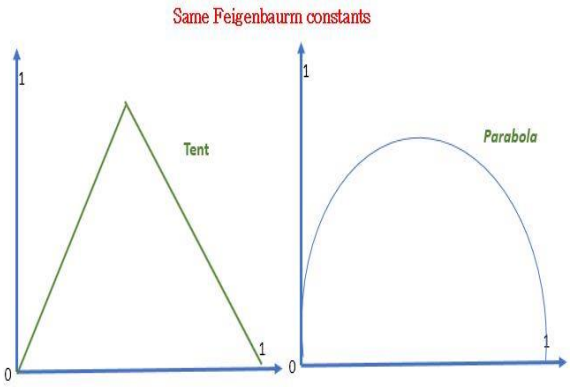



Fig. 7. Universality.

### 3.11. Some simulations

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

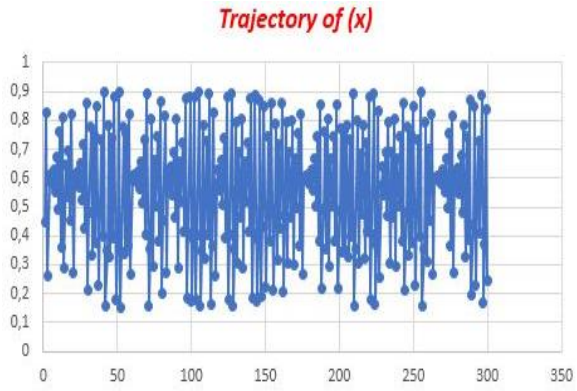



Fig. 8. Trajectory of x.

The trajectory seems to be random

#### *3.11.1. Deviation*

For two very close values of the initial conditions attached to the same control parameter (p) we see the deviation of the trajectories, this is due to the strong sensitivity to the initial conditions provided by the value of the Lyapunov exponent.

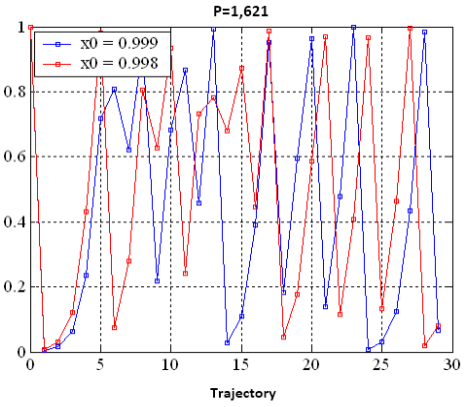



Fig. 9. Sensitivity.

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

The sensitivity to initial conditions of a chaotic map measures its robustness against abrupt attacks. Our map is one-dimensional, a comparison with the most used maps is given by the following table.

Table 1. Lyapunov exponent.

| Chaotic map | Lyapunov exponent |
|---|---|
| Logistic Map | Ln (2) |
| PWLCM | Ln (2) |
| Tent Map | Ln (2) |
| Our Map | $3/2\mathrm{Ln(p)} >> \mathrm{Ln(2)}$ |

## IV. 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 $(in\ the\ simulation, we\ take\ p = 1.54,\ x_0 = 0.623)$.

### 4.1. Our algorithm

1. Subdivision of the image vector into blocks of three pixels, as well as the chaotic vector.
2. Calculation of the initialization vector
3. Modification of the priming block
4. Application of Hill's improved method.
5. Application of dissemination
6. Reconstruction of the encrypted image
7. The encryption process is as follows

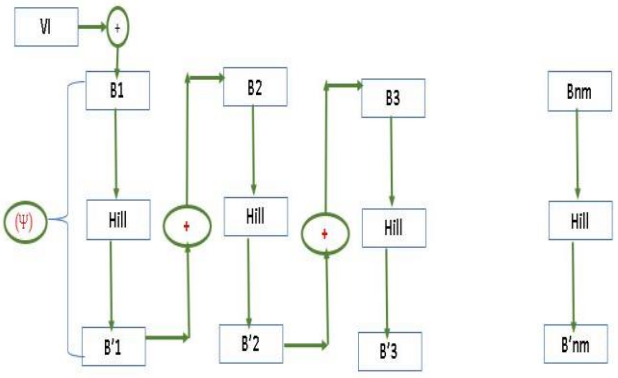



Fig. 10. Encryption process.

The encryption function is defined by

***Encryption process***

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

The use of vector $(Tvi)$ aims to overcome the linearity problem of classical systems.

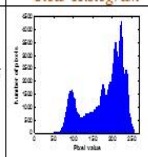
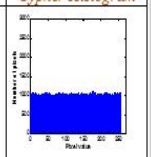
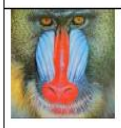
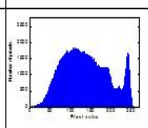
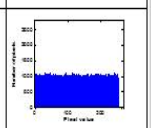
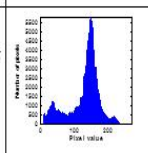
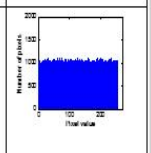
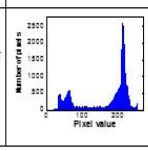
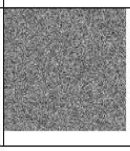
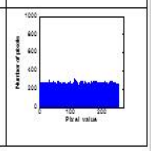
Construct the encryption key matrix from the new chaotic map by the following expression.

$$H = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & q \end{pmatrix}$$

$$With\ \ a, d, q\ \epsilon \left(\mathbb{Z}/_{256\mathbb{Z}}\right)^{*} and\ b, c, e\ \mathbb{Z}/_{256\mathbb{Z}}$$

After the simulation is complete, we get

Table 2. Encrypted image histogram.

| Clear Image | Size | Clear Histogram | Cypher Image | Cypher Histogram |
|---|---|---|---|---|
|  | 256x256 |  |  |  |
|  | 512x512 |  |  |  |
|  | 256x256 |  |  |  |
|  | 256x256 |  |  |  |

All images tested by our algorithm generate encrypted images with uniform and flattened histograms of pixel distribution. These histograms give an entropy value very close to the maximum value (8). This ensures a strong protection of our new technology against any entropy attack. The calculation of the entropy value is given by the table below

Table 3. Calculated entropy.

| Image | Size | Cypher | Entropy |
|---|---|---|---|
|  | 256x256 |  | 7,9993 |
|  | 512x512 |  | 7,9998 |
|  | 512x512 |  | 7,9997 |
|  | 1024x1024 |  | 7,9999 |
|  | 256x256 |  | 7,9991 |

The use of the encryption mode provides strong protection for our system against differential attacks. The table below illustrates the different values of the differential statistical constants.

Table 4. Differential parameters.

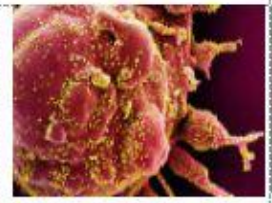
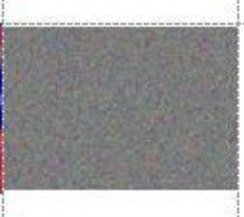
| Image | Size | NPCR | UACI | PSNR |
|---|---|---|---|---|
|  | 256x256 | **99,92** | **33,35** | **8,36** |
|  | 512x512 | **99,67** | **34,23** | **8,65** |
|  | 1024x1024 | **99,96** | **33,37** | **8,10** |

*4.1.1. Avalanche effect*

Our algorithm uses a strong link between encrypted pixels and pixels with clear policies. As a result, as data propagates through the structure of the algorithm, gradual changes become increasingly important. The avalanche effect is the number of bits that have been changed if a single bit in the original image is changed. The mathematical expression of this avalanche effect is given by

$$AE = \left(\frac{\sum_i bit\ change}{\sum_i bit\ total}\right) * 100. \quad (48)$$

Table 5. Avalanche effect.

| Original Image | Cypher Image | AE |
|---|---|---|
|  |  | 78,25 |
|  |  | 77,04 |
|  |  | 76,26 |

The high sensitivity of our new chaotic map makes our algorithm immune to brute force attacks. This sensitivity is illustrated by the following figure

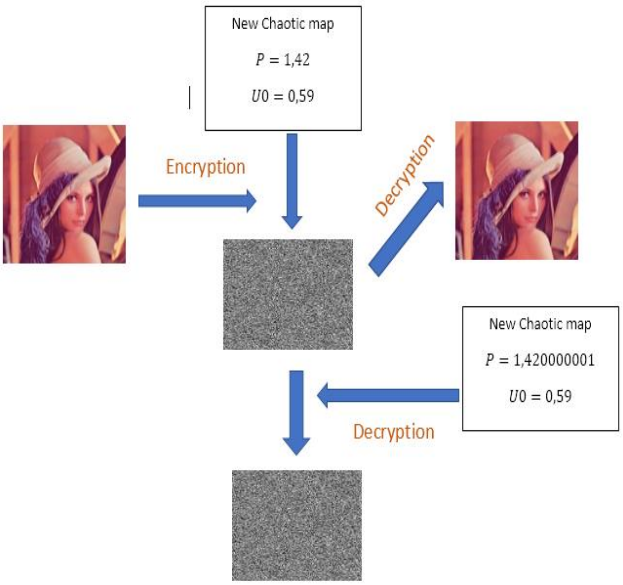



Fig. 11. Key sensitivity.

A rapid comparison between our example using a chaotic map with an enhanced Vigenere and other techniques. This minimal comparison, illustrated in the following table, highlights the complexity of our system, devoted by the new chaotic map.

Table 6. Comparison of our scheme with other methods.

| Measure | Image Name | Our Method | Method [12] | Method [8] | Method [ 7] |
|---|---|---|---|---|---|
| Entropy | Baboon (512×512) | 7.9998 | 7.9944 | --- | 7.9987 |
| | Peppers (512×512) | 7.9998 | 7.9973 | --- | 7.9992 |
| | Lena (256×256) | 7.9992 | 7.9969 | 7.9967 | 7.9991 |
| | Cameraman (256×256) | 7.9991 | 7.9976 | --- | 7.9991 |
| NPCR | Baboon (512×512) | 99.654 | --- | ---- | 99.63 |
| | Peppers (512×512) | 99.745 | 99.63 | ---- | 99.60 |
| | Lena (256×256) | 99.634 | 66.63 | 99.61 | 99.57 |
| | Cameraman (256×256) | 99.632 | 99.54 | ---- | 99.56 |
| UACI | Baboon (512×512) | 334.541 | ---- | ---- | 33.40 |
| | Peppers (512×512) | 33.784 | 30.89 | ---- | 33.17 |
| | Lena (256×256) | 33.545 | 30.47 | 33.51 | 33.35 |
| | Cameraman (256×256) | 33.541 | 31.76 | ---- | 33.59 |

## V. 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 attack. Using logarithms and discrete exponents and translation vectors to overcome linear problems will increase the complexity of our method.

## CONFLICT OF INTEREST

I am the alone author of this article, and therefore no conflict.

To finalize this document, I did not receive any assistance funds from any organization. This document does not contain any studies or experiments on animals.

Ethical approval: This article does not contain any studies with animals performed by any of the authors.

(Or) Ethical approval: This article does not contain any studies with human participants or animals performed by any of the author.

### REFERENCES

[ 1 ] Günyaz Ablay, "Chaotic Map Construction from Common Nonlinearities and Microcontroller Implementations," *International Journal of Bifurcation and Chaos*, vol. 26, no. 7. 2016.

[ 2 ] Kwok-Wo Wong, Xiao feng Liao, Yong Wang, Degang Yang, "One-way hash function construction based on chaotic map network," *Chaos, Solitons & Fractals*, vol. 41, no. 5, pp. 2566-2574, 2009.

[ 3 ] Yantao Li, Shao jiang Deng, and Di Xiao "A novel Hash algorithm construction based on chaotic neural network," *Neural Computing and Applications*, vol. 20, pp. 133-141, 2011.

[ 4 ] Nicolas Bierne, John, Welch , Etienne Loire , François Bonhomme, and Patrice david, "The coupling hypothesis: why genome scans may fail to map local adaptation genes," *Molecular Ecology*, vol. 20, no. 11, pp. 2044–2072, 2011.

[ 5 ] Jacques Patarin, "Security of Random Feistel Schemes with 5 or More Rounds," in *Proceeding of Annual International Cryptology Conference*, pp 106-122, 2004.

[ 6 ] Sahar Mazloom, Amir Masud, and Eftekhari-Moghadam, "Color image encryption based on Coupled Nonlinear Chaotic Map," *Chaos, Solitons & Fractals,* vol. 42, no. 3, pp. 1745-1754. 2009.

[ 7 ] Xiao Feng, Xiaolin Tian, and Shaowe iXia, "An Improved Image Scrambling Algorithm Based On Magic Cube Rotation and Chaotic Sequences," in *Proceeding of IEEE the 4-th International Congress on Image and Signal Processing*, pp.1021-1024, 2011

[ 8 ] Hraoui S., Gmira F., Jarar A. O., Satori. K., Saaidi A., "Benchmarking AES and chaos based logistic map for image encryption," in *Proceeding of International Conference on Computer Systems and Applications (AICCSA)*, pp. 1-4, 2013.

[ 9 ] A. Jarjar, "Improvement of hill's classical method in image cryptography," *International Journal of Statistics and Applied Mathematics*, vol. 2, no. 3, Part A, 2017.

[10] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices," *AIP Chaos*, vol. 16, 033118 (2006)

[11] Noshadian S., Ebrahimzade A., and Kazemitabar S. J., "Breaking a chaotic image encryption algorithm," *Multimedia Tools and Applications*, vol. 79, no. 35, pp. 25635-25655, 2020.

[12] Niu Y., Zhou Z., and Zhang X., "An image encryption approach based on chaotic maps and genetic operations," *Multimedia Tools and Applications*, vol. 79, no. 35, pp. 25613-25633, 2020.

[13] Ghazvini M., Mirzadi M., and Parvar N., "A modified method for image encryption based on chaotic map and genetic algorithm," *Multimedia Tools and Applications*, vol. 79, no. 37, pp. 26927-26950, 2020.

## Acknowledgement

This article is not subsidized by any public or private organization. It is a personal work.

## Author

**Mr. Abdellatif JarJar** is the alone author of this article, and therefore no conflict. To finalize this document, I did not receive any assistance funds from any organization. This document does not contain any studies or experiments on animals. This article does not contain any studies with animals performed by any of the authors. This article does not contain any studies with human participants or animals performed by any of the author.