Hindawi Publishing Corporation
Advances in Multimedia
Volume 2014, Article ID 409586, 15 pages
http://dx.doi.org/10.1155/2014/409586

Research Article

A New One-Dimensional Chaotic Map and Its Use in a Novel Real-Time Image Encryption Scheme

Radu Boriga,[1] Ana Cristina Dăscălescu,[1] and Adrian-Viorel Diaconu[2]

[1] *Faculty of Computer Science, Titu Maiorescu University, 040051 Bucharest, Romania*
[2] *IT & C Department, University of South-East Europe Lumina, 021187 Bucharest, Romania*

Correspondence should be addressed to Radu Boriga; radu.boriga@prof.utm.ro

Received 15 January 2014; Revised 16 April 2014; Accepted 27 April 2014; Published 2 June 2014

Academic Editor: Stefanos Kollias

We present a new one-dimensional chaotic map, suitable for real-time image encryption. Its theoretical analysis, performed using some specific tools from the chaos theory, shows that the proposed map has a chaotic regime and proves its ergodicity, for a large space of values of the control parameter. In addition, to argue for the good cryptographic properties of the proposed map, we have tested the randomness of the values generated by its orbit using NIST statistical suite. Moreover, we present a new image encryption scheme with a classic bimodular architecture, in which the confusion and the diffusion are assured by means of two maps of the previously proposed type. The very good cryptographic performances of the proposed scheme are proved by an extensive analysis, which was performed regarding the latest methodology in this field.

1. Introduction

Image encryption schemes have been increasingly studied in order to ensure real-time secure images transmission through the Internet or through the communication networks. To meet this challenge, many new encryption schemes based on classical algorithms (e.g., Blowfish, AES, DES, etc.) have been proposed in the last years [1–5]. Starting from 1989, when Robert Matthews proposed the first chaos-based cryptosystem, in which he used the logistic map, chaotic maps have become a new direction to develop image encryption schemes which have, in many aspects, similar properties to the conventional ones [6–10]. Recently, many researchers have proposed different encryption schemes based on chaotic maps, being encouraged by the chaotic properties of dynamical systems such as high sensitivity to the initial conditions, ergodicity, and topological transitivity [11–17].

It is well known that a good encryption algorithm should be sensitive to the secret key, and the key space should be large enough to make brute-force attacks infeasible [18, 19]. In-based encryption schemes, the secret key space is defined by the control parameters and/or the initial conditions of the maps underling chaos. For some of the proposed chaos-based encryption schemes it was proved that an incorrect selection of the initial condition or the use of chaotic maps which have a small range of the control parameters or an uneven values distribution leads to a weak security [19–25].

In this sense, we proposed in [26] a new chaotic map with large interval of parameters values for which the chaos is fulfilled, obtained by compounding a periodic real map with a bounded real map. Using specific mathematical and numerical tools from chaos theory and statistics, we proved that the proposed map has very good cryptographic properties. Then, the proposed map was used to design a new PRNG/PRBG model, based on a well-known binary operation [26]. In this paper, we have extended our work by studying not only theoretically but also only numerically the behavior of another map designed in the same manner. Thus, we used the topological conjugacy mechanism with logistic map, in order to study the behavior of the proposed map. Also, we have calculated the analytic form of Lyapunov exponent, which allows us to prove theoretically that the proposed map is chaotic for a large interval of parameters values. Moreover, the proposed chaotic map is used in a new real-time image encryption scheme, in which the confusion property is ensured by a new algorithm for generating random permutations, while the diffusion property is achieved using a new efficiently XOR-scheme.

The paper is organized as follows: in Section 2 we present the design of the newly proposed chaotic map, including its chaotic behavior assessment. Section 3 showcases the detailed and comprehensive randomness' testing process of sequences generated by the orbit of the new chaotic map. Section 4 presents a new image encryption scheme based on the map proposed in Section 2. Section 5 presents the performance analysis of the proposed image encryption scheme. Finally, Section 6 concludes the work carried out so far.

2. The Proposed Chaotic Map

In any encryption system, the basic issue is the selection process of the secret keys. According to the principle postulated by Menezes et al. [18], the security of the cryptosystem must depend only on the secret key. Even if an encryption algorithm is well designed, if the secret key is incorrectly chosen or the key space size is small, the security is endangered. Chaotic-based cryptosystems proposed so far have not defined a clear set of rules to be followed in the selection process of the secret key [27]. In many cases, the idea that the secret key is constituted by the control parameters and/or the initial condition of the map for which this is chaotic and ergodic was implicitly admitted. Most used maps in chaos-based encryption schemes proposed so far, respectively, the logistic map, tent map, and Hénon map, have small ranges of the parameters' values, for which the two requirements are achieved, that is, intervals (3.999, 4], (0.999, 1), and [1.1, 1.4]. Due to the discretization (i.e., implementation of the real numbers is realized with a finite precision in computers), the key space size of a cryptosystem based on chaotic map will actually collapse to a finite and a small set of numbers [6, 19, 24, 25, 28, 29].

The new chaotic map proposed in this paper uses (1) as model. Here, whilst g represents a periodic real map (selected so as to ensure a large phase space), h represents a bounded real map (which, by an appropriate selection, restricts the phase space to a closed interval in which the map has good chaotic properties):

$$x_{n+1} = h\left(g\left(x_n\right)\right). \tag{1}$$

Therefore, the proposed one-dimensional chaotic map, which is defined with respect to (1), is given by

$$\begin{gathered} x_{n+1} = f\left(x_n\right), \\ f : [-1,1] \longrightarrow [-1,1], \qquad f\left(x\right) = \frac{2}{\pi}\arcsin\left(\sin\left(\pi x\right)\right). \end{gathered} \tag{2}$$

The behavior of a map can be easily studied using the mechanism of topological conjugacy with a map whose behavior is already known; thus it established an equivalent relationship between their dynamics [30, 31]. So, we have determined the topological conjugacy between the proposed map f and the logistic map, whose properties are already well-known.

Proposition 1. *The $f : [-1,1] \rightarrow [-1,1]$ map given by relation* (2) *and the logistic map g extended on the interval $[-1,1]$ given by*

$$\begin{gathered} g : [-1,1] \longrightarrow [-1,1], \\ g\left(x\right) = \begin{cases} 4x\left(1+x\right), & x \in [-1,0), \\ 4x\left(1-x\right), & x \in [0,1], \end{cases} \end{gathered} \tag{3}$$

are topologically conjugated through the homeomorphism

$$\begin{aligned} h : [-1,1] \longrightarrow [-1,1], h\left(x\right) \\ = \begin{cases} -\dfrac{1}{\pi}\arccos\left(1+2x\right), & x \in [-1,0) \\ \dfrac{1}{\pi}\arccos\left(1-2x\right), & x \in [0,1]. \end{cases} \end{aligned} \tag{4}$$

Once the conjugation map h (between maps f and g) is determined, the study of the evolution in time of an orbit $\{x_0, f(x_0), f^2(x_0), \ldots, f^k(x_0)\}$, of period k and belonging to f map, can be realized through the analysis of the behavior of an orbit $\{x_0, g(x_0), g^2(x_0), \ldots, g^k(x_0)\}$, of period k, of and belonging to g map, using the bijection h.

Proof. To prove that the f_N and f_L maps are topologically conjugated through the homeomorphism h, we check that the following condition is satisfied:

$$\left(f_N \circ h\right)\left(x\right) = \left(h \circ f_L\right)\left(x\right). \tag{5}$$

For $x \in [-1,0]$ the left term from (5) becomes

$$\begin{aligned} \left(f_N \circ h\right)\left(x\right) &= \frac{2}{\pi}\arcsin\left(\sin\left(-\arccos\left(1+2x\right)\right)\right) \\ &= -\frac{2}{\pi}\arcsin\left(\sqrt{1-\left(1+2x\right)^2}\right). \end{aligned} \tag{6}$$

For $x \in [-1,0]$ the right term from (6) becomes

$$\left(h \circ f_l\right)\left(x\right) = -\frac{2}{\pi}\arccos\left(1-4x\left(1+x\right)\right). \tag{7}$$

Substituting the relations (6) and (7) in (5), we obtain

$$-\frac{2}{\pi}\arcsin\left(\sqrt{1-\left(1+2x\right)^2}\right) = -\frac{2}{\pi}\arccos\left(1-4x\left(1+x\right)\right) \tag{8}$$

which is equivalent with

$$1-\sin^2\left(\arcsin\left(\sqrt{1-\left(1+2x\right)^2}\right)\right) = 1-4x\left(1+x\right) \tag{9}$$

and hence

$$1+8x+8x^2 = 1+8x+8x^2. \tag{10}$$

Summing up, condition (5) is satisfied.

In a similar manner, condition (5) was proven for $x \in [0,1]$, which concludes the proof of the proposition. □

Theorem 2. *The f map, given by relation* (2)*, has chaotic orbits on the interval* $[-1, 1]$.

Proof. In order to study the asymptotic behavior of an orbit $\{x_0, x_1, \ldots, x_k\}$ of the chaotic map f, in the phase space, which starts from an initial point $x_0 \in [-1, 1]$, we will use a strong instrument from the chaos theory, such as the Lyapunov exponent λ_f [31], given by the relation

$$\lambda_f = \lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} \ln \left| f'(x_i) \right|. \tag{11}$$

The maps f and g are topologically conjugated through the conjugation map h given by relation (4); thus, after applying the derivation rule of the continue maps, we obtain

$$f'(h(x)) \cdot h'(x) = h'(g(x)) \cdot g'(x) \tag{12}$$

from which it results that

$$g'(x) = \frac{f'(h(x)) \cdot h'(x)}{h'(g(x))}. \tag{13}$$

Therefore, we obtain the relation

$$\begin{aligned} &\ln \left| g'(x_1) g'(x_2) \cdots g'(x_k) \right| \\ &\quad = \sum_{i=1}^{k} \ln \left| \frac{f'(h(x_i)) \cdot h'(x_i)}{h'(x_{i+1})} \right| \\ &\quad = \sum_{i=1}^{k} \ln \left| \frac{h'(x_i)}{h'(x_{i+1})} \cdot f'(h(x_i)) \right| \\ &\quad = \ln \left| h'(x_1) \right| - \ln \left| h'(x_{k+1}) \right| + \sum_{i=1}^{k} \ln \left| f'(h(x_i)) \right|. \end{aligned} \tag{14}$$

Dividing the last relation by k, we obtain

$$\begin{aligned} &\frac{1}{k} \sum_{i=1}^{k} \ln \left| g'(x_i) \right| \\ &\quad = \frac{1}{k} \left[\ln \left| h'(x_1) \right| - \ln \left| h'(x_{k+1}) \right| + \sum_{i=1}^{k} \ln \left| f'(h(x_i)) \right| \right]. \end{aligned} \tag{15}$$

Appling the limit after k in the last relation, we obtain the following relation:

$$\lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} \ln \left| g'(x_i) \right| = \lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} \ln \left| f'(h(x_i)) \right|. \tag{16}$$

The Lyapunov exponent of the logistic map is given by the relation [31]

$$\lambda_g = \lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} \ln \left| g'(x_i) \right| = \ln 2. \tag{17}$$

Relation (16) shows that the Lyapunov exponent of the orbits corresponding to the f map is identical with the g map one, so we obtain

$$\lambda_f = \ln 2. \tag{18}$$

Due to the fact that the Lyapunov exponent is positive, the asymptotic behavior of any orbit of the f map is chaotic [30, 32, 33].

The next objective is to determine a statistical image of the f map dynamics, in the phase space, using the same mechanism of topologic conjugation, through theoretical results postulated by Grossman and Thomae in [30]. □

Proposition 3. *The f map given by relation* (2) *conserves an absolute invariant density function that is continuous on the interval* $[-1, 1]$ *and is equal to 1.*

Proof. Let ρ_f and ρ_g be the probability densities of the maps $f$and g. Because these maps are topologically conjugated through conjugation map h, applying the Grossman-Thomae theorem [30], we obtain the relation

$$\rho_f = \rho_g \left(h^{-1}(x) \right) \left| \frac{dh^{-1}(x)}{dx} \right|. \tag{19}$$

For $x \in [0, 1]$, conjugation map h is given by the relation

$$h(x) = \frac{1}{\pi} \arccos(1 - 2x). \tag{20}$$

Thus, we obtain that

$$h^{-1}(x) = \frac{1 - \cos \pi x}{2}. \tag{21}$$

The invariant density function of the logistic map has the following analytical expression [33]:

$$\rho = \frac{1}{\pi \sqrt{x(1 - x)}}. \tag{22}$$

So, relation (19) becomes

$$\begin{aligned} \rho_f &= \rho_g \left(\frac{1 - \cos \pi x}{2} \right) \left| \pi \sin \pi x \right| \\ &= \frac{\pi \sin \pi x}{2\pi \sqrt{((1 - \cos \pi x)/2)((1 + \cos \pi x)/2)}} = 1. \end{aligned} \tag{23}$$

From (23) we conclude that the density function of probability of the$f$ map is equal to 1, for any $x \in [0, 1]$. In the same manner, we can prove that the probability density function of the f map is equal to 1, for any $x \in [-1, 0]$, which concludes the proof of the statement. □

2.1. The Parameterization of the Proposed Dynamic System. From the theoretical results, that is, the ones presented above, we can conclude that the map f has a chaotic behavior and an invariant probability measure on the interval $[-1, 1]$.

The chaotic maps used as base of cryptosystems are defined in a parametric way; for example, their dynamics depend on one or several control parameters. Moreover, those chaotic systems show a chaotic behavior for certain values of the associated control parameters. Therefore, the design of a cryptosystem based on any of those dynamical systems must be done by guaranteeing the use of a set of values for the control parameters leading to chaos.

Following the method described by Fridrich in [34], we parameterized f map, as follows:

$$\begin{gathered} x_{n+1} = f_r(x_n) \\ f_r : [-1,1] \longrightarrow [-1,1], \\ f_r(x) = \frac{2}{\pi} \arcsin(\sin(\pi r x)), \end{gathered} \tag{24}$$

where $r > 0$ is the control parameter of the map.

The behavior, in time, of the discreet system $x_{n+1} = f_r(x_n)$, depends both on the control parameter r and on the initial condition x_0.

First, we analyze the stability of the fixed points in order to determine the sensitivity level of the system to the initial conditions. The map f_r has the following fixed points:

$$x_k^1 = \frac{4k}{2r-1}, \qquad x_k^2 = \frac{2(2k+1)}{2r+1}, \quad k \in \mathbb{Z}. \tag{25}$$

According to the theorem of fixed points [31], the points x_1 and x_2 are attractors if the following condition is fulfilled:

$$\left| f_r'(x_i) \right| < 1, \quad i = \overline{1,2} \tag{26}$$

which implies that the control parameter r must fulfill the condition

$$r < \frac{1}{2}. \tag{27}$$

The map f_r is defined on the interval $[-1,1]$; therefore, from condition (24), it results that the fixed point $x_k^2 \notin [-1,1]$ for any $k \in \mathbb{Z}$ and the fixed point $x_k^1 \in [-1,1]$ only for $k = 0$. So, for values of the parameter $r < 1/2$, any trajectory which starts from any initial point $x_0 \in [-1,1]$ converges in time to the attractor point $x_0^1 = 0$. After the value of the parameter r exceeds the value $1/2$, the fixed point x_0^1 loses its stability and another instable fixed point $x_0^2 = 2/(2r+1)$ appears. The trajectory with the initial condition x_0 converges, at the beginning, in the neighborhood of x_0^2, and then leaves it, entering into a chaotic regime. The stability of the fixed points of the map f_r is also emphasized through the bifurcation diagram presented in Figure 1.

It can be observed that for a value of the parameter $r > 1/2$ the f_r map has an instable behavior and for the parameter $r > 1$ the map enters in a complete chaotic regime.

The road to chaos of the f_r map with parameter $r > 1/2$ is not achieved through the doubling process of the period, specific to some chaotic maps [31], but is induced by the existence of a dense set of periodic orbits of any period in the interval $[-1,1]$.

The sensitivity of the f_r map to infinitesimal changes of the initial conditions is illustrated in Figures 2 and 3. In Figure 2, two orbits of the map f_r with fixed control parameter $r = 5$ starting from two very close initial points in phase space are plotted, while in Figure 3 two orbits generated by two maps which start from the same initial point x_o whose control parameters differ by 10^{-6} are plotted. It can be noticed, in both figures, that, after some iterations, the orbits have a completely different behavior, becoming divergent by an exponential law in time.

Next, using the Lyapunov exponent we proved that the orbits of the map f_r have a chaotic behavior on the interval $(-1,1)$ for values of the control parameter $r > 1/2$.

Theorem 4. *The orbits of the map f_r given by relation* (24) *have a chaotic behavior on the interval* $(-1,1)$ *for values of the control parameter $r > 1/2$.*

Proof. The sensitivity level to the initial conditions of a periodic orbit $\{x_1, x_2, \ldots, x_k\}$ generated by f_r map is determined using the Lyapunov exponent:

$$\begin{aligned} \lambda_f &= \lim_{k \to \infty} \frac{1}{k} \sum_{i=1}^{k} \ln \left| f_r'(x_i) \right| \\ &= \lim_{k \to \infty} \frac{1}{k} \sum_{i=1}^{k} \ln \left| 2r \frac{\cos \pi r x_i}{\left| \cos \pi r x_i \right|} \right| = \ln 2r. \end{aligned} \tag{28}$$

The orbit $\{x_1, x_2, \ldots, x_k\}$ is chaotic if the Lyapunov exponent λ_f is positive, so we obtain the relation $\ln 2r > 0$, which is equivalent to $r > 1/2$. □

Figure 4 represented the Lyapunov exponent, numerically calculated using Wolf's algorithm [35], according to the control parameter $r \in [0,10]$. It can be observed that for values of the parameter $r > 1/2$ the orbits of the map f_r are chaotic.

Following on, the analysis of the shape of a dynamical system attractor can provide information about its behavior in time for certain values of its parameters. The attractor of a dynamical system with a periodic behavior has a regular shape, while the one corresponding to chaotic dynamical system has a complex structure, of fractal type, and it is called strange attractor. The attractor of the f_r map for $r = 7$ is represented in Figure 5.

The fractal structure of an attractor is indicated by a fractional value of its fractal dimension, which is a ratio providing a statistical index of complexity comparing how details in a pattern change with the scale at which they are. Several types of fractal dimension can be estimated theoretically and empirically, such as box-counting dimension, Hausdorff dimension, Minkowski-Bouligand dimension, information dimension, and correlation dimension [36–38]. Using the plots from Figure 6, we established that the attractor of the f_r map has a box-counting dimension $D_b = 0.97863$ and a correlation dimension $D_c = 0.97064$.

The fractional values of both estimated fractal dimensions allow us to conclude that the proposed map f_r has a strange attractor, which indicates a chaotic behavior.

In the next stage of our analyses we tested the ergodicity property. The ergodic property is a basic requirement for

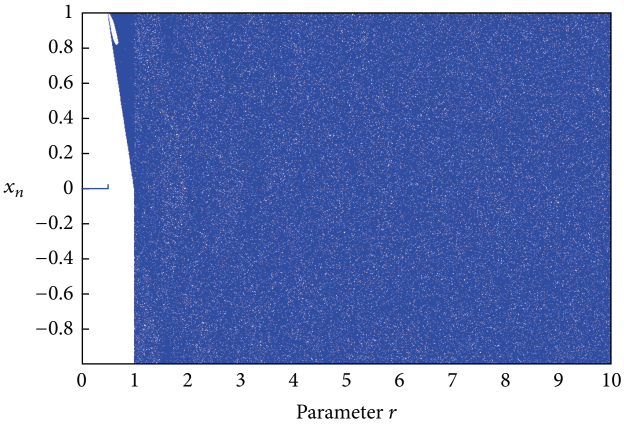


Figure 1: The bifurcation diagram of the f_r map for $r \in [0, 10]$.

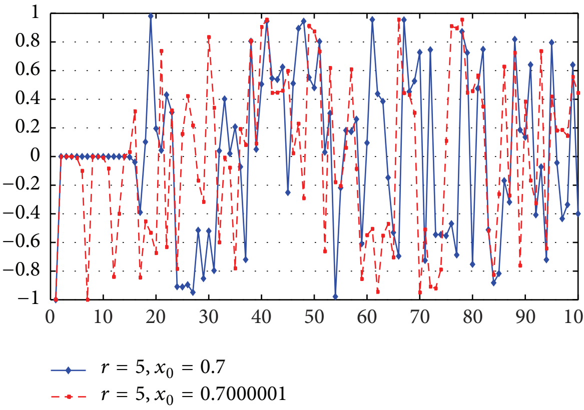


Figure 2: The sensibility of the f_r map to changes of the initial point x_0.

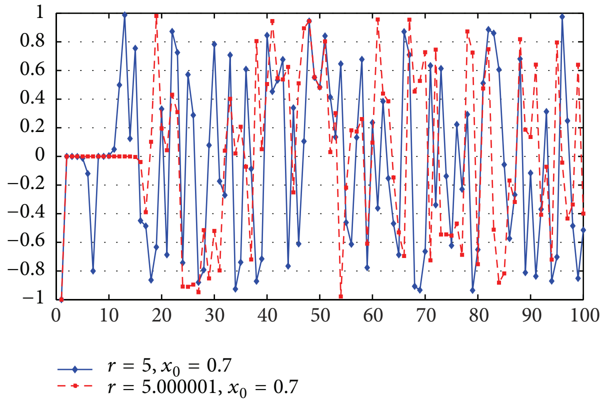


Figure 3: The sensibility of the f_r map to changes of the control parameter r.

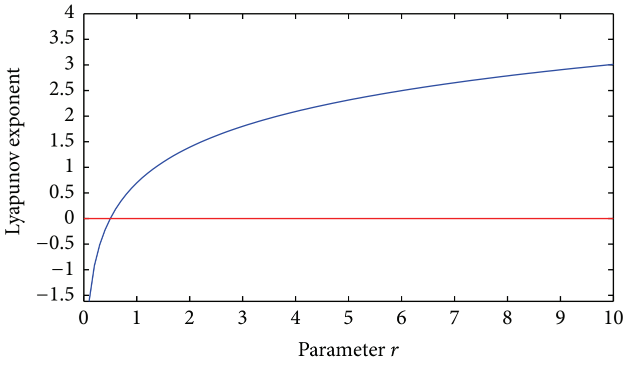


Figure 4: The Lyapunov exponent of the f_r map for $r \in [0, 10]$.

the use of a dynamical system as a base of an encryption scheme. This property implies that the state space cannot be nontrivially divided into several parts. Therefore, a trajectory starting from a point never localizes in a smaller region, so the plain-text space which corresponds to a given cipher will not be restricted to a "smaller" subspace.

Indeed, if a dynamical system is ergodic, the long-term behavior of its orbits is independent of the initial condition and can be studied using statistical analysis. Using Birkhoff's theorem [30, 31] in conjunction with Kolmogorov-Smirnov test [39] we proved that the dynamical system f_r is ergodic for $r > 1$. The Kolmogorov-Smirnov test is applied on two series of experimental independent data $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$, corresponding to the measurements of two random variables X and Y. The random variable X is obtained iterating for n times the f_r map using a fixed parameter $r > 1$ and an initial condition $x_0 \in [-1, 1]$. The second random variable Y is obtained by selecting the values extracted from n distinct orbits of the f_r map at a moment k, orbits that start from n initial points of the interval $[-1, 1]$, using the same fixed parameter. The moment $k = 100$ is chosen from the stationary zone of f_r , previously established using Kolmogorov-Smirnov test described in [39, 40].

Due to the fact that the random variables X and Y correspond to time average of f_r after time n and space average, respectively,, the purpose of the test is to establish if the two experimental sets of data derive from populations with the same distribution or not, in respect to Birkhoff's theorem. The analysis is based on the experimental distribution functions Fe_X and Fe_Y of the two random variables X and Y.

The hypotheses of the Kolmogorov-Smirnov test are as follows:

(i) H_0: both variables X and Y have the same probability law;

(ii) H_1: both variables X and Y have different probability laws.

The Kolmogorov-Smirnov test is applied as follows.

(1) The δ test value is calculated; that is, the maximum absolute difference between the two experimental distribution functions is

$$\delta = \max_u \left| Fe_X(u) - Fe_Y(u) \right|. \qquad (29)$$

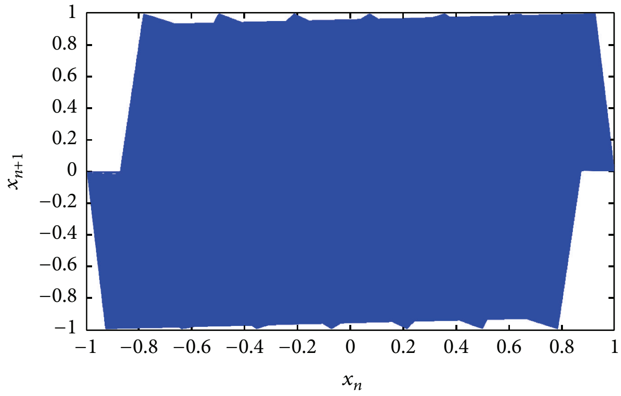


Figure 5: The attractor of the f_r map for $r = 7$.

Table 1: The results of ergodicity property testing for f_r map.

Number	Parameter value	KS-Test value	Result
1	5.429208420782631	0.958	SUCCESS
2	9.119643904063768	0.944	SUCCESS
3	9.982798857377562	0.958	SUCCESS
4	6.478547914065082	0.952	SUCCESS
5	8.101080150367013	0.954	SUCCESS
6	4.183180696373615	0.948	SUCCESS
7	7.066962832367738	0.968	SUCCESS
8	4.985348171318265	0.934	SUCCESS
9	5.068908118426080	0.942	SUCCESS
10	3.072806838451141	0.958	SUCCESS

(2) For a chosen α significance level, Δ_α is calculated, where α is the quantile of the probability law of the random value Δ; that is, $P(\Delta > \Delta_\alpha) = \alpha$,

$$\Delta_\alpha \cong \sqrt{\frac{n+m}{nm}}\sqrt{\frac{1}{2}\ln\frac{2}{\alpha}}. \quad (30)$$

(3) If $\delta \leq \Delta_\alpha$, the hypothesis H_0 is accepted. In other words, if the absolute maximum distance between the two experimental distribution functions is lower than a certain accepted value Δ_α, then it will be decided if the random variables X and Y have the same probability law. Otherwise, if $\delta > \Delta_\alpha$, the test rejects the H_0 hypotheses for the chosen level; that is, the two sets of experimental data come from random variables with different probability laws [40].

The Kolmogorov-Smirnov test was performed for a sample of $n = m = 100000$ and a significance level $\alpha = 0.05$. The decision regarding the ergodicity can be based on a Monte Carlo analysis, which evaluates the ability of the Kolmogorov-Smirnov test to accept bad data as good data. For example, the above experiment can be repeated 500 times, finally recording the acceptance proportion of the hypothesis H_0, which is [0.93, 097].

The overall results are summarized in Table 1. One can observe that, in case of all values selected for r parameter, with $r \in (1, 10]$, the acceptance proportion of H_0 hypothesis lies within the confidence interval. Thus, ergodicity of the proposed chaotic map is confirmed over the entire interval of interest of the parameter r.

Based on the results numerically obtained, using instruments from the chaos theory, it can be concluded that the f_r map has a chaotic behavior, without intermittent scenarios, for values of the control parameters $r > 1$. Therefore, the dynamical system can be successfully used to build strong cryptographic applications, because of the very large space of the keys that ensures a high level of security and also due to the ergodicity property which ensures the efficiency of the diffusion process.

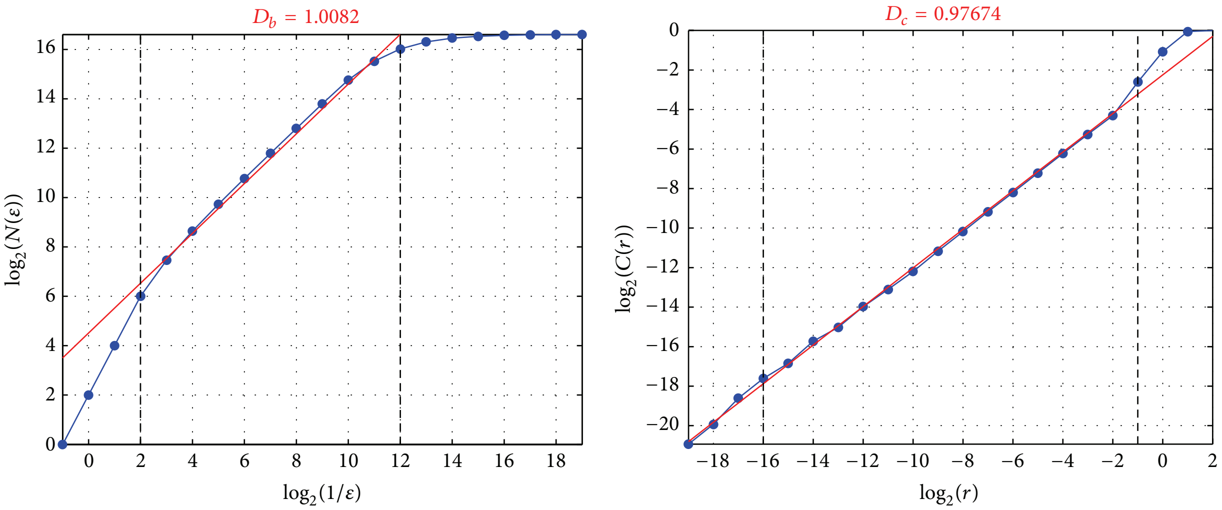
According to Theorem 4, the map f_r is sensitive to the initial conditions on interval $[-1, 1]$, for values of the parameter $r > 1/2$, and it becomes chaotic and ergodic for $r > 1$. Because the control parameter of a chaotic map defines the corresponding cryptosystem's key space, the fact that map f_r can be used for the construction of robust encryption scheme is confirmed.

3. Randomness Analysis

Evaluation process in terms of cryptographic properties of a dynamical system must include, in addition to the study of the chaotic behavior, a statistical analysis of the randomness of the values generated, in order to determine the security level of the system against some statistics cryptanalytic attacks. There are several options available for analyzing the randomness of a new developed pseudorandom bit generator. The most popular suites of statistical tests for randomness are NIST [41] and DIEHARD [42].

Chaotic cryptography deals with real numbers; thus, in order to use the NIST statistical suite, we firstly apply a computationally method to transform a chaotic sequence of real number into a bitstream. The used discretization method has consisted of the extraction of the first 15 digits from the fractional part of the real numbers generated by the chaotic f_r map. For the numerical experimentations we have generated $m = 2000$ different binary sequences from 500 randomly chosen orbits, each sequence having a length of $n = 1000000$ bits, and computed the P value corresponding to each sequence for all the 15 tests of the NIST suite.

The significance level of each test in NIST is set to 1%, which means that 99% of test samples pass the tests if the random numbers are truly random. The acceptance region of the passing ratio is given by $[p - 3\sqrt{(p(1-p))/m}, p + 3\sqrt{(p(1-p))/m}]$, where m represents the number of samples tested and $p = 1 - \alpha$ is the probability of passing each test. For $m = 2000$ and the probability $p = 0.99$ (corresponding to the significance level $\alpha = 0.01$), we obtained the confidence interval $[0.983, 0.996]$. In the second column of Table 2 we have summarized the results obtained after applying nonparameterized and parameterized tests of the NIST suite on the binary sequences produced by the discrete orbit of the proposed map. The computed proportion for each test lies inside the confidence interval. Hence, the tested binary sequences are random according to all tests of NIST suite [41].



(a) The box-counting dimension

(b) The correlation dimension

FIGURE 6: The fractal dimensions of the attractor of the f_r map.

TABLE 2: The results of the NIST tests.

Test name	Passing ratio of the test	Uniformity P value	Result
Frequency	0.992	0.602803	SUCCESS
Block frequency	0.990	0.748891	SUCCESS
Cumulative sums	0.991	0.090388	SUCCESS
Runs	0.990	0.939005	SUCCESS
Longest run	0.989	0.592443	SUCCESS
Rank	0.991	0.840367	SUCCESS
FFT	0.989	0.242363	SUCCESS
Nonoverlapping template	0.983	0.761719	SUCCESS
Overlapping template	0.983	0.230755	SUCCESS
Universal	0.987	0.050629	SUCCESS
Approximate entropy	0.988	0.959347	SUCCESS
Random excursions	0.987	0.614382	SUCCESS
Random excursions variant	0.984	0.830939	SUCCESS
Serial	0.986	0.209392	SUCCESS
Linear complexity	0.989	0.764655	SUCCESS

If the tested sequences are truly random, then P values would be uniformly distributed in the interval $[0, 1)$. NIST recommends to apply a χ^2-*test* in which the interval $[0, 1)$ is divided into 10 subintervals. Defining F_i as number of occurrences of P value in ith interval, then the χ^2 statistic is $\chi^2 = \sum_{i=1}^{10} (F_i - (m/10))^2/(m/10)$. NIST recommends to set its significance level to 0.01%, so the acceptance region of statistics is $\chi^2 \leq 33.72$. The P value corresponding to the uniformity of the P values is calculated as igamc $(9/2, \chi^2/2)$, so it must be greater than 0.0001 to ensure that the P values could be considered uniformly distributed. The results from the third column of Table 2 lead us to the conclusion that the P values for each statistical test are uniformly distributed.

The calculating method of the total test passing ratio of total test and the uniformity P value of total test samples follows the same methodology described above. In this case, we considered the number of samples $m = 30000$, so the acceptance region is $[0.988, 0.992]$. For the passing ratio of the total test we obtained the value 0.988 and the P value corresponding to the uniformity of the P values from the total test was 0.294808. Thus, the pseudorandom bit sequences obtained by discretization of the f_r orbits passed the total test.

4. Description of the Proposed Cryptosystem

The proposed cryptosystem is a symmetric one and has a bimodular architecture, in which one of the modules performs the diffusion process using a random permutation generated by a chaotic map f_1 of type (24), while the second one performs the confusion process by modifying pixel values using a deterministic algorithm which implies another map f_2 of type (24).

Assuming that the pixels of a RGB image with size $n = W \times H$ pixels are numbered on rows, from top to down and from left to right on each row, we denote the plain image by $P = \{p_0, p_1, \ldots, p_{n-1}\}$ and the corresponding encrypted one by $C = \{c_0, c_1, \ldots, c_{n-1}\}$, both of the same size n. Also, both in the encryption and in decryption process, we will use an auxiliary image of size n, too, denoted by $A = \{a_0, a_1, \ldots, a_{n-1}\}$.

Next, we will describe in detail the implementation and functionality of each module of the proposed cryptosystem.

4.1. The Secret Key.

4.1. The Secret Key. The secret key of the proposed cryptosystem, shared by the emitter and the receiver, consists of

(i) two real numbers $r_1$and r_2 representing the parameters of the maps f_1 and f_2 chosen so that both maps might be in a chaotic and ergodic regime (i.e., $r_1, r_2 > 1$);

(ii) two real numbers x_0^1 and x_0^2 representing the initial conditions of the maps f_1 and f_2, chosen from the interval $[-1, 1]$;

(iii) two unsigned integers m_1 and m_2 representing the preiterations numbers of the maps f_1 and f_2, required to assure a chaotic and ergodic behavior (we recommend to choose $m_1, m_2 \geq 100$);

(iv) an unsigned integer iv, representing the initial value used to encrypt/decrypt the first pixel of the plain/encrypted image.

4.2. The Encryption Process

4.2.1. The Diffusion Process. In a bimodular image encryption/decryption scheme, the diffusion process consists of the pixels permutation from the plain image, so that the default redundancy of the image might be distributed throughout the encrypted image [34]. In [43], we proposed a fast algorithm for generating random permutations with a high shift factor, suitable for image scrambling.

The algorithm combines the use of random values, generated by a chaotic map, with the use of nonrandom ones, determined algorithmically. Practically, a permutation $q = (q_1, q_2, \ldots, q_n)$ of degree n is constructed element by element, as follows: a random value between 1 and n, obtained by discretization of a real value generated by the f_1 map, is assigned to the current element and then it is checked if the value was previously used; if not, the maximum unused value is assigned to it. In this way, it is clear that a part of the elements from the beginning of the permutation will have large values and a part of the elements from the end of the permutation will have small ones, so the shift factor of the permutation will be high.

Using the chaotic map f_1 and the recurrence $x_{k+1}^1 = f_1(x_k^1)$, where $x_0^1 \in [-1, 1]$, firstly we discard the preiterated values $\{x_1^1, \ldots, x_{m_1}^1\}$ and we construct an orbit $\{x_{m_1+1}^1, \ldots, x_{m_1+n}^1\} \subset \mathbb{R}$ of length n. Next, we construct a discretized sequence $\{d_1, d_2, \ldots, d_n\}$ of unsigned integers by extracting the first 15 digits from the fractional part of each real number from the orbit $\{x_{m_1+1}^1, \ldots, x_{m_1+n}^1\}$, that is, $d_i = \text{floor}(10^{15} \times x_{i+m_1}^1)$ for any $i \in \{1, 2, \ldots, n\}$.

The proposed algorithm for generating a random permutation $q = (q_1, q_2, \ldots, q_n)$ of degree n, starting from the sequence $\{d_1, d_2, \ldots, d_n\}$ and using a labeling array L of dimension n (i.e., $L[i]$ is equal to 1 if a value $i \in \{1, 2, \ldots, n\}$ is used in permutation q; else $L[i]$ is equal to 0), is as follows [43].

Input. Unsigned integers are $n, d_1, d_2, \ldots, d_n$.

Output. Random permutation is $q = (q_1, q_2, \ldots, q_n)$.

```
(1) For $i$ from 1 to $n$ do the following.
    (1.1) Set $L[i] \leftarrow 0$.
(2) Set max $\leftarrow n + 1$ (variable max stores the maximum
    unused value between 1 and $n$ in permutation $q$).
(3) For $i$ from 1 to $n$ do the following.
    (1) Set $q[i] \leftarrow 1 + d[i] \bmod n$.
    (2) If $L[q[i]] = 1$, then go to step 3, else go to step 7.
    (3) Set $k \leftarrow \max - 1$.
    (4) If $L[k] = 1$, then go to step 5; else go to step 6.
    (5) Set $k \leftarrow k - 1$ and go to step 4.
    (6) Set $q[i] \leftarrow k$ and max $\leftarrow k$.
    (7) Set $L[q[i]] \leftarrow 1$.
(4) Return $(q)$.
```

In [43] we proved that the proposed algorithm has an almost linear complexity if the used map is chaotic and ergodic, condition satisfied by the f_1 map.

In the encryption process, the pixels from the plain image P are shuffled using the following algorithm, based on the permutation $q = (q_1, q_2, \ldots, q_n)$.

Input. This includes plain image $P = \{p_0, p_1, \ldots, p_{n-1}\}$ and the permutation q of degree n.

Output. Shuffled image is $A = \{a_0, a_1, \ldots, a_{n-1}\}$.

```
(1) For $i$ from 0 to $n - 1$ do the following.
    (1.1) Set $a_{q_{i+1}-1} \leftarrow p_i$.
(2) Return $(A)$.
```

4.2.2. The Confusion Process. In an image encryption/decryption scheme, the confusion process tries to hide the correlations between the plain image, the encrypted image, and encryption key, usually by substitutions of the values of all pixels in a deterministic way [34].

As we mentioned above, the confusion process is based on one chaotic map f_2 of type (24), used in conjunction with the recurrence $x_{k+1}^2 = f_2(x_k^2)$, where $x_0^2 \in [-1, 1]$. The preiterated values $\{x_1^2, \ldots, x_{m_2}^2\}$ are discarded and we construct an orbit $\{x_{m_2+1}^2, \ldots, x_{m_2+n}^2\} \subset \mathbb{R}$ of length n. Next, we construct the keystream as a discretized sequence $\{k_0, k_1, \ldots, k_{n-1}\}$ of unsigned integers by extracting the first 15 digits from the fractional part of each real number from the orbit $\{x_{m_2+1}^2, \ldots, x_{m_2+n}^2\}$, that is, $k_i = \text{floor}(10^{15} \times x_{i+m_2+1}^2)$ for any $i \in \{0, 1, \ldots, n - 1\}$ (function floor(x) returns the nearest integer less than or equal to x).

To ensure a high level of security against differential attacks, we alter the value of a pixel a_i from the shuffled image $A = \{a_0, a_1, \ldots, a_{n-1}\}$, before XOR-ing it with the keystream and the value of the previously encrypted pixel, by the sum s_i of the three values corresponding to the color channels RGB of the pixels previously encrypted. Assuming that a pixel c_i from the encrypted image is a triplet $c_i = (c_i^R, c_i^G, c_i^B)$, then we define s_i as

$$s_i = \sum_{j=0}^{i-1} \left(c_j^R + c_j^G + c_j^B\right) \tag{31}$$

for any $i \in \{1, \ldots, n-1\}$ and $s_0 = 0$.

Thus, the values of the pixels from the encrypted image are obtained according to the following formula:

$$\begin{gathered} c_0 = a_0 \oplus iv \oplus k_0 \\ c_i = \left(\left(a_i + s_i\right) \bmod 256\right) \oplus c_{i-1} \oplus k_i, \quad 1 \le i \le n-1. \end{gathered} \tag{32}$$

4.3. The Decryption Process. Due to the fact that the proposed cryptosystem is a symmetric one, in the decryption process the same secret key is used, which leads to the same keystream $\{k_0, k_1, \ldots, k_{n-1}\}$. The decryption process consists of next two steps.

Step 1. On the pixels of the encrypted image $C = \{c_0, c_1, \ldots, c_{n-1}\}$, we apply the inverse transformation of (24), obtaining the auxiliary image $A = \{a_0, a_1, \ldots, a_{n-1}\}$:

$$\begin{gathered} a_0 = c_0 \oplus iv \oplus k_0, \\ a_i = \left(c_i \oplus c_{i-1} \oplus k_i + 256 - s_i\right) \bmod 256, \quad 1 \le i \le n-1, \end{gathered} \tag{33}$$

where s_i is defined by (23).

Step 2. On the pixels of the auxiliary image $A = \{a_0, a_1, \ldots, a_{n-1}\}$, we apply the inverse q^{-1} of the permutation q, obtaining the plain image $P = \{p_0, p_1, \ldots, p_{n-1}\}$.

5. Performances of the Proposed Cryptosystem

5.1. Security Analysis of the Proposed Cryptosystem. A strong encryption scheme should resist against known cryptanalytic attacks, such as known-plain-text attack, cipher-text only attack, statistical attack, differential attack, and various brute-force attacks. For the proposed image encryption system we performed standard security analysis, such as key space analysis, statistical analysis, and differential analysis. Thus, several specific statistical tests were performed, such as image pixels distribution, the correlation between adjacent pixels of the image encrypted, entropy, the correlation between original image and the encrypted one, NPCR, and UACI. The performances of the proposed cryptosystem were evaluated using 10 various standard test images from USC-SIPI Image Database [44], Kodak Digital Camera Sample Pictures [45], personal photos, and so forth. All the pictures used were 24 bit-color bitmaps, with different dimensions varying from 256 × 256 to 3000 × 4000 pixels. All tests were performed for each of the three color channels (red, green, and blue) in order to achieve a rigorous and detailed analysis of proposed cryptosystem performance.

5.2. Key Space Analysis. A secure image encryption algorithm should have enough large key space to resist against brute-force attacks.

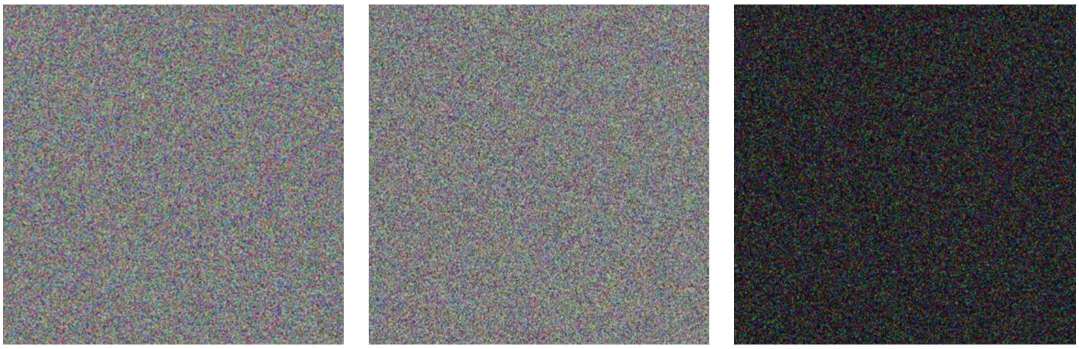
The secret key of the proposed cryptosystem contains 4 real numbers and 3 unsigned integers. The real numbers must be stored and transmitted using a real data type with high precision to prevent them from negative effects caused by the discretization. If the implementation of the cryptosystem is done using a programming language that complies with *IEEE Standard 754-2008*, then it is recommended to use the double data type, which stores real numbers on 8 bytes, with an accurate 15 decimal places. In this case, the secret key length will be 352 bits, which means that the size of the secret key space will be equal to $2^{352} \approx 9.17 \times 10^{105}$, a value large enough to prevent guessing the secret key in a reasonable time, using exhaustive search.

5.3. Key Sensitivity Analysis. A secure image cryptosystem should be sensitive to any small change in the secret key, so the use of two secret keys which are very small different one from another leads to two completely different encrypted images. In Figure 7, 2 images are shown obtained by encrypting Lena image using 2 secret keys which has only a double data type component different by 10^{-12}, along with the difference image.

In our key sensitivity analysis, we considered 10 plain images and 10 corresponding secret keys. Each plain image was encrypted using 7 secret keys, which differ from the initial one by 10^{-12} on components of double data type or by one bit on components of unsigned integer data type, and the 7 encrypted images obtained were compared with the image obtained by encrypting the plain image using the initial secret key. In all the 70 cases, we obtained a correlation coefficient very close to 0, which confirms that the encrypted images are completely different.

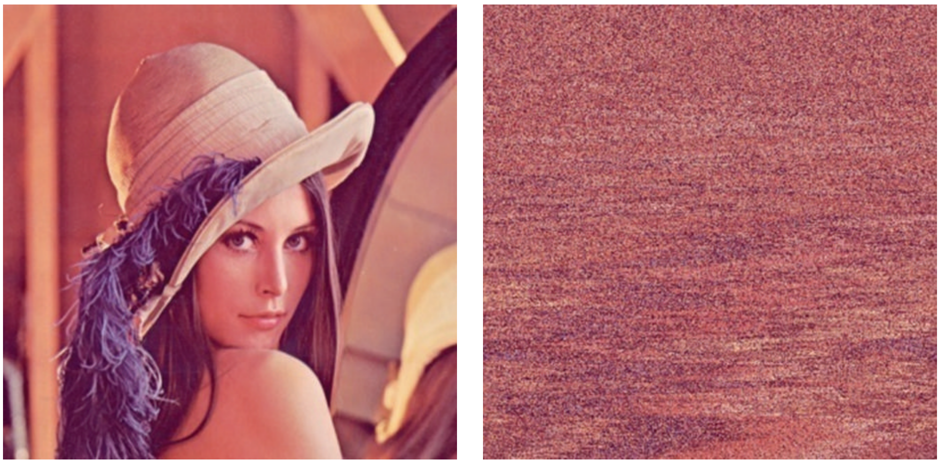
Furthermore, the sensitivity to any small change in the secret key must be present in the decryption process, too. So, the use of a secret key which is different in very few respects from the original one must lead to a decrypted image completely different from the initial plain one. Figure 8 shows an image obtained by decrypting the encrypted Lena image using a secret key which has only one double data type component different by 10^{-12} from the original secret key. Note that the image is totally different from the plain-image Lena and, moreover, the decrypted image seems to be a noise.

In this step of our key sensitivity analysis, we considered 10 plain images and 10 corresponding secret keys, too. Each plain image was encrypted using the corresponding secret key and the encrypted image obtained was decrypted using 7 secret keys, which differ from the initial one by 10^{-12} on components of double data type or by one bit on components of unsigned integer data type, and all the 7 decrypted images obtained were compared to the initial plain image. In all 70



(a) Lena image encrypted with the first secret key (b) Lena image encrypted with the second secret key (c) The difference image of the two encrypted images

Figure 7: Images that resulted from encrypting the Lena image using two secret keys which differ by 10^{-12} on a single double data type component.



(a) Decrypted using the original secret key (b) Decrypted using an altered secret key

Figure 8: Images that resulted from decrypting the encrypted Lena image.

cases, we obtained a correlation coefficient very close to 0, which confirms that the decrypted images are completely different from the initial plain images.

So, we can conclude that the proposed encryption algorithm is very sensitive to the key, because a small change in the secret key will generate a completely different decrypted image and cannot obtain the correct plain image.

5.4. Statistical Analysis.

In his most famous work, "*Communication Theory of Secrecy Systems*" [46], Shannon said that "*It is possible to solve many kinds of ciphers by statistical analysis.*" In this sense, he suggested two methods of diffusion and confusion in order to crack the attacks based on statistical analysis.

In order to prove that the proposed image encryption system has a superior confusion and diffusion properties, we performed tests on the histograms and entropies of the encrypted images, along with a statistical test on the correlations between adjacent pixels in the encrypted image.

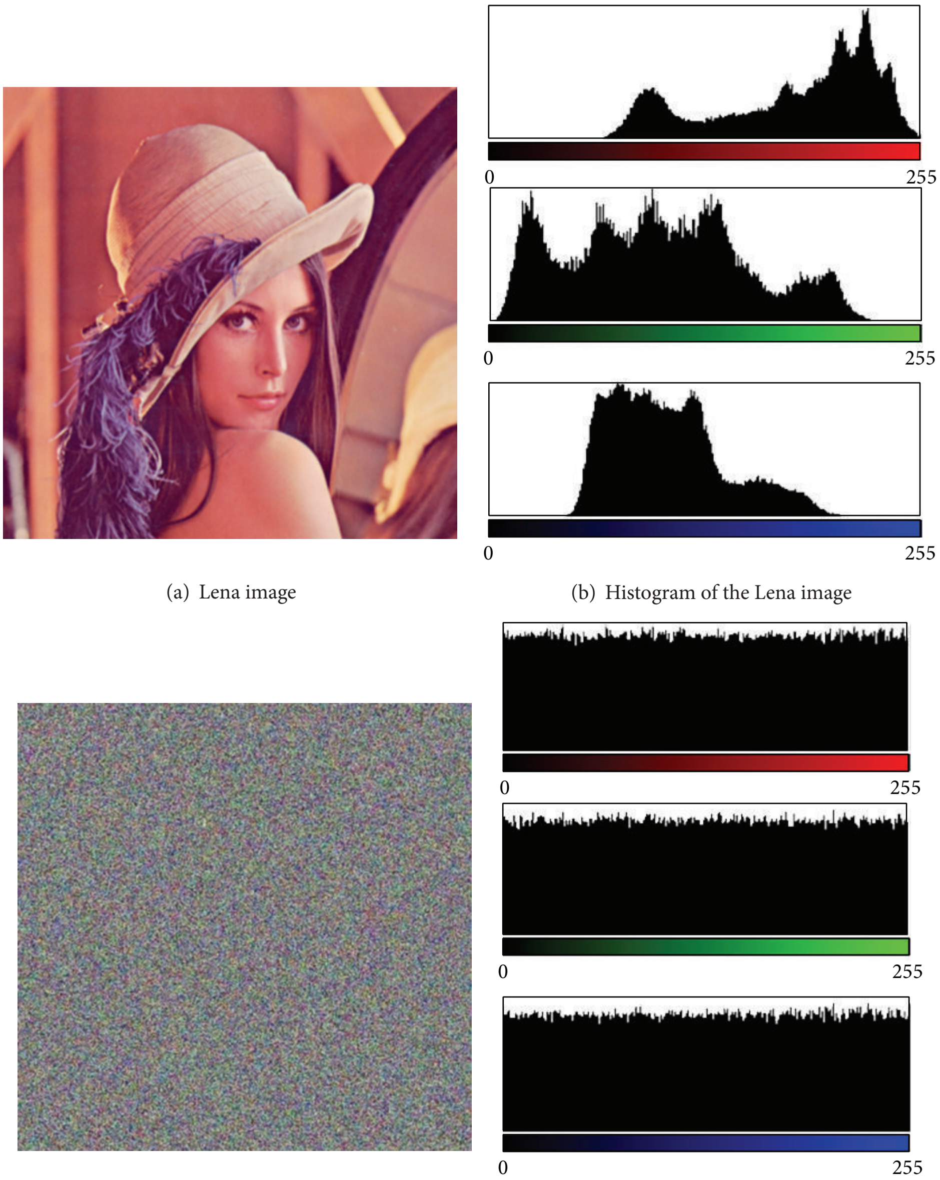
5.4.1. Histogram of the Encrypted Images.

A cryptosystem with high security level needs to produce encrypted images with a uniform distribution of pixels in each color channel, in order to hide the uneven distribution from the plain image.

The most often used visual analysis tool to study the distribution of a color image of pixel values is the *color histogram*, in which the pixel values frequencies are plotted separately for each color channel. Figure 9 contains a pair of plain image, encrypted image, along with the associated color histograms.

Note that, after the encryption of Lena image, which has a strong color uneven distribution (Figure 9(a)), we obtained an image with a uniform distribution of pixel values (Figure 9(d)) for each color channel, so an attacker cannot extract statistical information about the plain image or about the encryption key used.

To analyze the distribution of pixel values for a large number of encrypted images, we used the χ^2 test [47].



(a) Lena image

(b) Histogram of the Lena image

(c) Encrypted Lena image

(d) Histogram of Lena encrypted image

Figure 9: Analysis of the standard image Lena.

The value of the χ^2 test for an encrypted image of dimension $m \times n$ is given by the following formula:

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0}, \qquad (34)$$

where v_i is the observed frequency of a pixel value i $(0 \leq i \leq 255)$ and v_0 is the expected frequency of a pixel value i, so $v_0 = (m \times n)/256$.

The results obtained by applying the χ^2 test on 10 encrypted images can be summarized as follows: for 9 images the values of the χ^2 test obtained were lower than the critical value $\chi^2_{255,0.05} = 293.25$ and for one image the value obtained was 294.68, which is very close to the critical value $\chi^2_{255,0.05} = 293.25$. Thus, we conclude that the distribution of pixel values is uniform in the encrypted image, which demonstrates that the proposed cryptosystem is able to resist against statistical attacks.

5.4.2. Entropy. Considering the pixel values as a quantification of the information contained in an image, we can estimate the uncertainty of its content through the notion of *entropy*, defined by Shannon [46]. The entropy $H(S)$ of an image source S can be calculated as

$$H(S) = -\sum_{i=0}^{255} P(i) \log_2 P(i), \qquad (35)$$

where $P(i)$ represents the probability of a pixel value i $(0 \leq i \leq 255)$ from a color channel RGB of an image and the entropy is expressed in bits.

The 10 plain images used in the testing process had entropy values between 5.762235 and 7.752217. Through the encryption process images with entropies between 7.999330 and 7.99986 were obtained, being very close to the maximal theoretical value of 8, so that the information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

5.4.3. Correlation of Adjacent Pixels. In an ordinary image, each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical, or diagonal directions [9, 48, 49] which is indicated by a value of Pearson's correlation coefficient very close to 1 [47].

In order to analyze the encryption quality of the proposed algorithm, the correlation coefficient was used to evaluate the correlations between adjacent pixels of the plain/encrypted images. Firstly, we randomly selected 1000 pairs of two adjacent pixels from plain/encrypted image, and, using the values from each color channel RGB, we constructed two series of data $X = \{x_1, x_2, \ldots, x_{1000}\}$ and $Y = \{y_1, y_2, \ldots, y_{1000}\}$. Then, we calculated the correlation coefficient between X and Y using the following formula:

$$\rho_C(X, Y) = \frac{\operatorname{cov}(X, Y)}{\sqrt{D(X)}\sqrt{D(Y)}}, \tag{36}$$

where C is the color channel, $D(\cdot)$ denotes the variance of a random variable, and $\operatorname{cov}(\cdot, \cdot)$ denotes the covariance of two random variables [47].

In Figure 10(a) we plotted the value of the pixel at the position (x, y) versus the value of the pixel at the position $(x+1, y)$ from the Lena image, while in Figure 10(b) we plotted them from the encrypted Lena image. We repeated the same plotting for vertically adjacent pixels (Figures 10(c) and 10(d)), respectively, for diagonally adjacent pixels (Figures 10(e) and 10(f)).

For all the 10 pairs of plain/encrypted test we obtained average values of the correlation coefficient from the interval $[-0.00915, 0.010345]$, very close to 0, which confirms that the encryption process eliminates the inherent strong correlation existing between the pixels of the plain image. This fact proves, once again, that the proposed system will resist against cryptanalytic attacks of statistical type.

5.5. Differential Attacks Analysis. Testing the security of a cryptosystem against differential attacks is necessary to evaluate how a minor change in the plain image is reflected upon the encrypted image. For this purpose, we consider two plain images $P_1 = \{p_0^{(1)}, p_1^{(1)}, \ldots, p_{n-1}^{(1)}\}$ and $P_2 = \{p_0^{(2)}, p_1^{(2)}, \ldots, p_{n-1}^{(2)}\}$ which differ by the value of a single pixel in a RGB color channel and their corresponding encrypted images $C_1 = \{c_0^{(1)}, c_1^{(1)}, \ldots, c_{n-1}^{(1)}\}$ and $C_2 = \{c_0^{(2)}, c_1^{(2)}, \ldots, c_{n-1}^{(2)}\}$.

To test the influence of one-pixel change in the plain image on the whole encrypted image using the proposed encryption scheme, two common measures are used: *number of pixels change rate* (NPCR) and *unified average changing intensity* (UACI) [49].

The NPCR indicator measures the percentage of different pixel numbers between the encrypted images C_1 and C_2 and it is defined as follows:

$$\text{NPCR} = \left(\frac{1}{n}\sum_{i=0}^{n-1} d_i\right) \times 100\%, \tag{37}$$

where $d_i = 0$ if $c_i^{(1)} = c_i^{(2)}$ and $d_i = 1$ if $c_i^{(1)} \neq c_i^{(2)}$ for any $i \in \{0, 1, \ldots, n-1\}$.

The UACI indicator measures the average intensity of differences between the encrypted images C_1 and C_2 and it is defined as follows:

$$\text{UACI} = \left(\frac{1}{n}\sum_{i=0}^{n-1} \frac{\left|c_i^{(1)} - c_i^{(2)}\right|}{255}\right) \times 100\%. \tag{38}$$

Considering two random images, the maximum expected value of NPCR is found to be 99.609375%, while the maximum expected value of UACI is 33.463541% [49]. Using the proposed cryptosystem, 10 tests were performed, achieving values of the NPCR indicator between 98.78% and 99.16% and between 32.77% and 33.14% for the UACI indicator, which confirms that the proposed cryptosystem will withstand to the differential attacks.

5.6. Quality of the Decryption Process. Within the cryptosystem performances evaluation, the quality of the decryption process should be also checked. Basically, this consists in testing that the image obtained after decryption process coincides with the plain one.

In this sense, we evaluated the *mean squared error* (MSE) between a plain image $P = \{p_0, p_1, \ldots, p_{n-1}\}$ and the corresponding decrypted one $D = \{d_0, d_1, \ldots, d_{n-1}\}$, on each RGB color channel, using the following formula [47]:

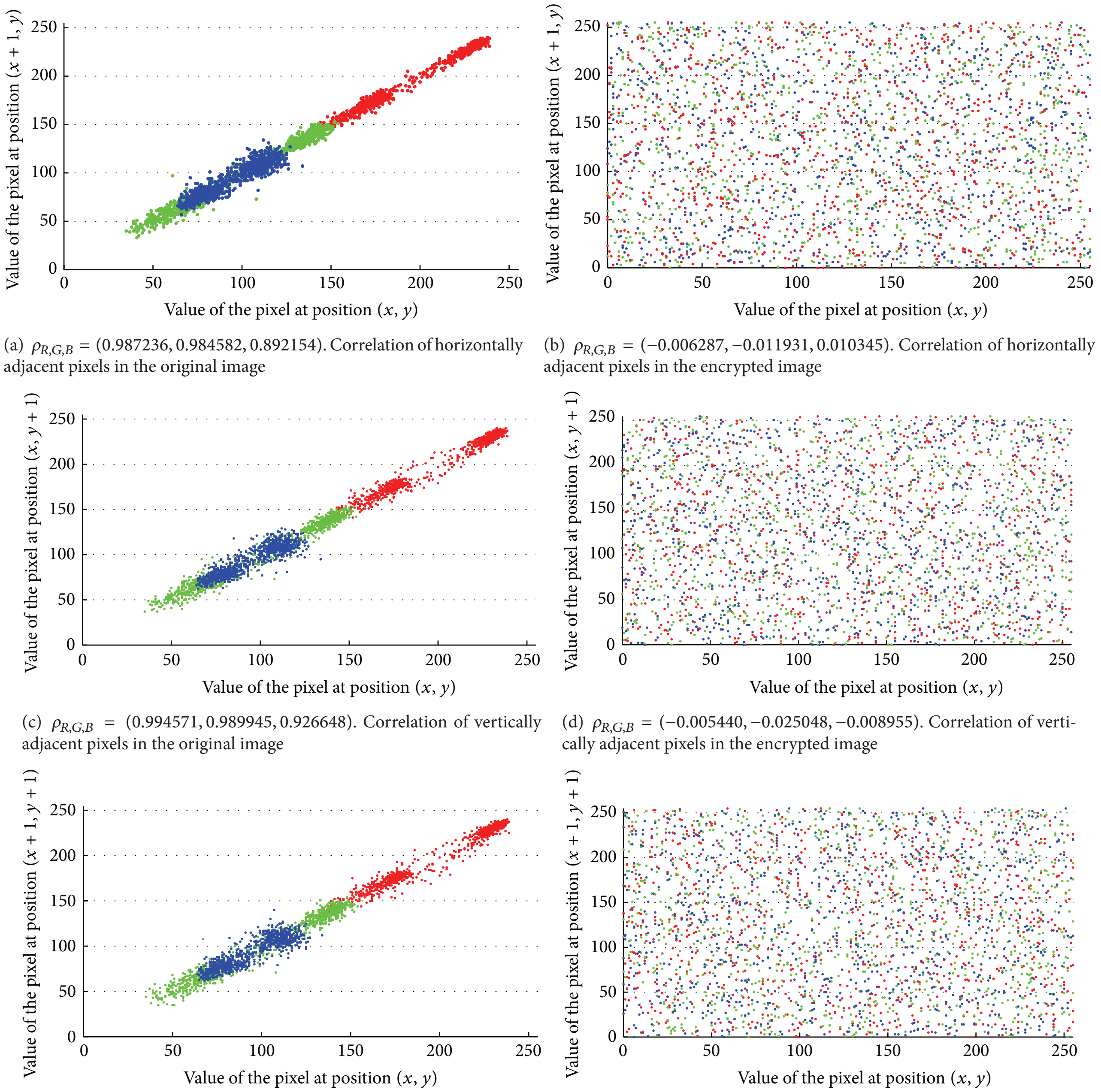
$$\text{MSE}(P, D) = \frac{1}{n}\sum_{i=0}^{n-1}(p_i - d_i)^2. \tag{39}$$

A value close to 0 of MSE indicates a good quality of the decryption process, while other values indicate the occurrence of errors in this process.

In all 10 tests performed, the value of MSE was 0 for each RGB color channel, which indicates that decryption is carried out without any loss of information.

5.7. Speed Performance. Another important factor to consider when analyzing the efficiency of a cryptosystem is its speed. In this sense, we run the proposed algorithm implemented in C language (MinGW compiler) under Windows 7, using a PC with Intel(R) Core (TM) i3 @2.53 GHz CPU and 3 GB RAM. We used 10 standard test bitmaps (256×256) with sizes of 256 × 256, 512 × 512, 720 × 576, 1024 × 1024, and 3000 × 4000 [44, 45]. The mean speeds obtained are summarized in Table 3.

Analyzing the mean speeds from Table 3, we can conclude that the proposed algorithm is faster than the ones presented in [50–52], having a mean encryption/decryption speed about 4 MB/s, being suitable for real-time image encryption.



(a) $\rho_{R,G,B} = (0.987236, 0.984582, 0.892154)$. Correlation of horizontally adjacent pixels in the original image

(b) $\rho_{R,G,B} = (-0.006287, -0.011931, 0.010345)$. Correlation of horizontally adjacent pixels in the encrypted image

(c) $\rho_{R,G,B} = (0.994571, 0.989945, 0.926648)$. Correlation of vertically adjacent pixels in the original image

(d) $\rho_{R,G,B} = (-0.005440, -0.025048, -0.008955)$. Correlation of vertically adjacent pixels in the encrypted image

(e) $\rho_{R,G,B} = (0.984270, 0.981644, 0.889881)$. Correlation of diagonally adjacent pixels in the original image

(f) $\rho_{R,G,B} = (\ 0.005888, -0.007541, -0.010945)$. Correlation of diagonally adjacent pixels in the encrypted image

Figure 10: Correlation of adjacent pixels from Lena plain/encrypted image.

5.8. Performances' Comparison with Other Image Encryption Schemes. Furthermore, we present below the results obtained by comparing the performances of the proposed system to other new similar encryption schemes [50–52]. Table 4 shows a summary of the mean values obtained for correlation coefficient of adjacent pixels (CCAP), NPCR, UACI, and speed.

Taking into account the results from Table 4, it can be seen that the proposed image encryption scheme has similar results regarding the level of security with other recent proposed schemes [50–52], but our scheme is much faster than all of them, so it is suitable for real-time image encryption.

6. Conclusions

Development of new chaotic maps which meet the current demands of security is an actual research direction in the field of chaotic cryptography. The main objective was to obtain a large key space, induced by the control parameter

Table 3: Speed performance of the proposed cryptosystem (encryption/decryption).

Image size (pixels)	Image size (MB)	Mean time (s)	Mean speed (MB/s)
256 × 256	0.19	0.05	3.80
512 × 512	0.75	0.17	4.41
720 × 576	1.19	0.28	4.25
1024 × 1024	3.00	0.75	4.00
3000 × 4000	34.30	8.85	3.88

Table 4: Performances' comparison.

Indicator	Stoyanov and Kordov [50]	Pareek et al. [51]	Ghebleh et al. [52]	Our scheme
NPCR	99.61	99.46	99.61	99.16
UACI	33.45	N/A	33.72	33.14
CCAP				
Horizontal	−0.0006	0.0083	−0.0043	−0.0058
Vertical	0.0008	−0.0162	0.0049	−0.0046
Diagonal	0.0013	0.0078	0.0057	0.0029
Speed (MB/s)	1.11	0.37	2.4	4

and/or initial conditions, for which the map is chaotic and ergodic. In this respect, in this paper we have developed a new one-dimensional map that meets these requirements. Using specific mathematical tools from chaos theory and the mechanism of topological conjugation, we proved, by Propositions 1 and 3 and Theorems 2 and 4, the very good cryptographic properties of the proposed map. In addition, to argue for the good cryptographic properties of the proposed map, we tested the randomness of the values generated by its orbit, using the NIST statistical suite. Using the proposed map we designed a new image encryption scheme. The confusion property is ensured by an algorithm that generates a random permutation for shuffling the pixels of plain image and the diffusion property is ensured by a new XOR-scheme. Through the experimental tests performed, we demonstrated that the new image encryption scheme is fast and has a high level of security, being suitable for real-time image encryption.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "A hash-based image encryption algorithm," *Optics Communications*, vol. 283, no. 6, pp. 879–893, 2010.

[2] F. Riaz, S. Hameed, I. Shafi, R. Kausar, and A. Ahmed, "Enhanced image encryption techniques using modified advanced encryption standard," *Communications in Computer and Information Science*, vol. 281, pp. 385–396, 2012.

[3] S. Dey, "SD-AEI: an advanced encryption technique for images: an advanced combined encryption technique for encrypting images using randomized byte manipulation," in *Proceedings of the 2nd International Conference on Digital Information Processing and Communications (ICDIPC '12)*, pp. 68–73, Klaipeda, Lithuania, July 2012.

[4] S. M. Seyedzade, R. E. Atani, and S. Mirzakuchaki, "A novel image encryption algorithm based on hash function," in *Proceedings of the 6th International Conference on Machine Vision and Image Processing (MVIP '10)*, pp. 1–6, Isfahan, Iran, October 2010.

[5] V. M. Silva-García, R. Flores-Carapia, and C. Rentería-Márquez, "Triple-DES block of 96 bits: an application to colour image encryption," *Applied Mathematical Sciences*, vol. 7, no. 21-24, pp. 1143–1155, 2013.

[6] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[7] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Physics Letters A*, vol. 372, no. 15, pp. 2645–2652, 2008.

[8] H. Yang, X. Liao, K.-W. Wong, W. Zhang, and P. Wei, "A new cryptosystem based on chaotic map and operations algebraic," *Chaos, Solitons and Fractals*, vol. 40, no. 5, pp. 2520–2531, 2009.

[9] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[10] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[11] A.-V. Diaconu and K. Loukhaoukha, "An improved secure image encryption algorithm based on rubik's cube principle and digital chaotic cipher," *Mathematical Problems in Engineering*, vol. 2013, Article ID 848392, 10 pages, 2013.

[12] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos," *Nonlinear Dynamics*, vol. 67, no. 1, pp. 557–566, 2012.

[13] C. K. Huang, C. W. Liao, S. L. Hsu, and Y. C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *Telecommunication Systems*, vol. 52, no. 2, pp. 563–571, 2013.

[14] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized arnold map," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 2079–2087, 2012.

[15] G. Ye and K.-W. Wong, "An image encryption scheme based on time-delay and hyperchaotic system," *Nonlinear Dynamics*, vol. 71, no. 1-2, pp. 259–267, 2013.

[16] X. Tong and M. Cui, "Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation," *Science in China F: Information Sciences*, vol. 53, no. 1, pp. 191–202, 2010.

[17] Z.-X. Zhang and T. Cao, "A chaos-based image encryption scheme with confusion-diffusion architecture," *Communications in Computer and Information Science*, vol. 152, no. 1, pp. 258–263, 2011.

[18] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[19] D. Arroyo, G. Alvarez, S. Li, C. Li, and J. Nunez, "Cryptanalysis of a discrete-time synchronous chaotic encryption system," *Physics Letters A*, vol. 372, no. 7, pp. 1034–1039, 2008.

[20] C. Li, L. Y. Zhang, R. Ou, K.-W. Wong, and S. Shu, "Breaking a novel colour image encryption algorithm based on chaos," *Nonlinear Dynamics*, vol. 70, no. 4, pp. 2383–2388, 2012.

[21] F. Huang and Y. Feng, "Security analysis of image encryption based on twodimensional chaotic maps and improved algorithm," *Frontiers of Electrical and Electronic Engineering in China*, vol. 4, no. 1, pp. 5–9, 2009.

[22] J. Wang, G. Jiang, and B. Lin, "Cryptanalysis of an image encryption scheme with a pseudorandom permutation and its improved version," *Journal of Electronics*, vol. 29, no. 1-2, pp. 82–93, 2012.

[23] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 372, no. 38, pp. 5973–5978, 2008.

[24] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of an ergodic chaotic cipher," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 311, no. 2-3, pp. 172–179, 2003.

[25] D. Arroyo, J. M. Amigoy, S. Li, and G. Alvarez, "On the inadequacy of unimodal maps for cryptographic applications," in *XI Reunion Espanola sobre Criptologia y Seguridad de la Informacion (XI RECSI)*, pp. 37–42, Universitat Rovira i Virgili, Tarragona, Spain, 2010.

[26] A. C. Dăscălescu, R. E. Boriga, and A. V. Diaconu, "Study of a new chaotic dynamical system and its usage in a novel pseudorandom bit generator," *Mathematical Problems in Engineering*, vol. 2013, Article ID 769108, 10 pages, 2013.

[27] C. Li, S. Li, G. Alvarez, G. Chen, and K.-T. Lo, "Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations," *Physics Letters A: General, Atomic and Solid State Physics*, vol. 369, no. 1-2, pp. 23–30, 2007.

[28] V. Patidar, K. K. Sud, and N. K. Pareek, "A pseudo random bit generator based on chaotic logistic map and its statistical testing," *Informatica*, vol. 33, no. 4, pp. 441–452, 2009.

[29] M. Hénon, "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics*, vol. 50, no. 1, pp. 69–77, 1976.

[30] S. Grossmann and S. Thomae, "Invariant distributions and stationary correlation functions of one-dimensional discrete processes," *Zeitschrift fur Naturforschung*, vol. 32, pp. 1353–1363, 1977.

[31] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos: An Introduction to Dynamical Systems*, Springer, 1st edition, 1996.

[32] M. T. Rosenstein, J. J. Collins, and C. J. De Luca, "A practical method for calculating largest Lyapunov exponents from small data sets," *Physica D: Nonlinear Phenomena*, vol. 65, no. 1-2, pp. 117–134, 1993.

[33] H. G. Schuster, *Deterministic Chaos: An Introduction*, Wiley-VCH, 3rd edition, 1995.

[34] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[35] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Physica D: Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.

[36] P. Grassberger and I. Procaccia, "Measuring the strangeness of strange attractors," *Physica D: Nonlinear Phenomena*, vol. 9, no. 1-2, pp. 189–208, 1983.

[37] J. D. Farmer, E. Ott, and J. A. Yorke, "The dimension of chaotic attractors," *Physica D: Nonlinear Phenomena*, vol. 7, no. 1–3, pp. 153–180, 1983.

[38] J. Theiler, "Estimating fractal dimension," *Journal of the Optical Society of America A*, no. 7, pp. 1055–1079, 1990.

[39] L. I. Shujun, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 15, no. 10, pp. 3119–3151, 2005.

[40] A. Luca, A. Vlad, B. Badea, and M. Frunzete, "A study on statistical independence in the tent map," in *Proceedings of the International Symposium on Signals, Circuits and Systems (ISSCS '09)*, pp. 1–4, Iași, Romania, July 2009.

[41] A. Rukhin, J. Soto, J. Nechvatal et al., "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," NIST Special Publication 800-22, 2010.

[42] http://www.stat.fsu.edu/pub/diehard/.

[43] A. C. Dăscălescu and R. E. Boriga, "A novel fast chaos-based algorithm for generating random permutations with high shift factor suitable for image scrambling," *Nonlinear Dynamics*, vol. 74, no. 1-2, pp. 307–318, 2013.

[44] USC-SIPI Image Database, University of South California, Signal and Image Processing Institute, http://sipi.usc.edu/database/database.php.

[45] Kodak Digital Camera Sample Pictures, Kodak, http://www.kodak.com/digitalImages/samples/samples.shtml.

[46] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[47] D. R. Cox and C. A. Donnelly, *Principles of Applied Statistics*, Cambridge University Press, 2011.

[48] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons and Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[49] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons and Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[50] B. Stoyanov and K. Kordov, "Novel image encryption scheme based on Chebyshev polynomial and Duffing map," *The Scientific World Journal*, vol. 2014, Article ID 283639, 11 pages, 2014.

[51] N. K. Pareek, V. Patidar, and K. K. Sud, "Substitution-diffusion based Image Cipher," *International Journal of Network Security and Its Applications (IJNSA)*, vol. 3, no. 2, pp. 149–160, 2011.

[52] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 618–627, 2014.

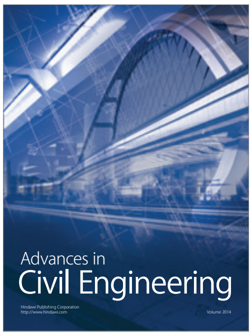
Journal of
Engineering

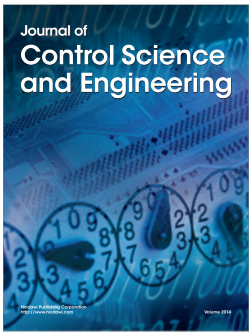
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

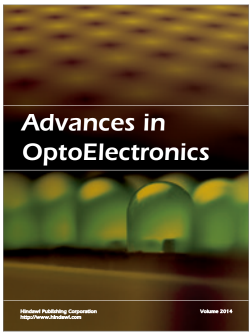
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

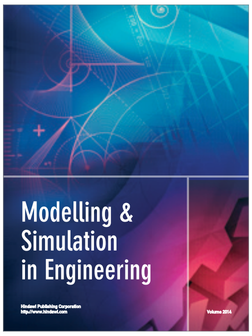
Journal of
Robotics

Journal of
Electrical and Computer Engineering

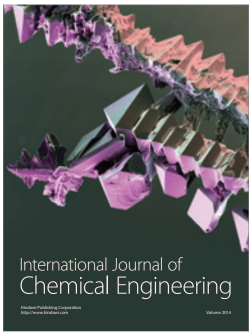

Advances in
OptoElectronics

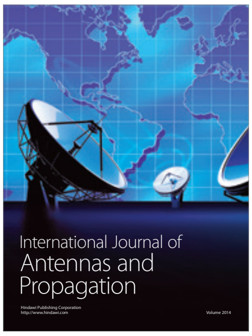
VLSI Design

International Journal of
Navigation and Observation

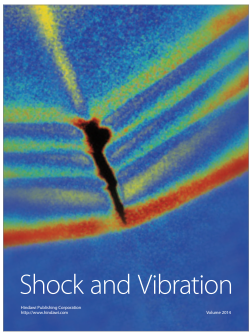

Modelling & Simulation in Engineering

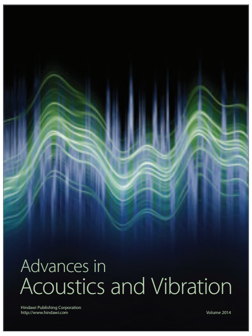
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration