Hyperchaotic encryption based on multi-scroll piecewise linear systems

M. García-Martínez[a,*], L.J. Ontañón-García[b], E. Campos-Cantón[a], S. Čelikovský[c]

[a] División de Matemáticas Aplicadas,
Instituto Potosino de Investigación Científica y Tecnológica A.C.
Camino a la Presa San José 2055 col. Lomas 4a Sección, 78216,
San Luis Potosí, SLP, México

[b] Coordinación Académica Región Altiplano Oeste,
Universidad Autónoma de San Luis Potosí,
Kilometro 1 Carretera a Santo Domingo, 78600,
Salinas de Hidalgo, San Luis Potosí, México

[c] Institute of Information Theory and Automation,
Academy of Sciences of the Czech Republic
Pod vodarenskou vezi 4, 182 08 Prague, Czech Republic

Abstract

A hyperchaotic multi-scroll piecewise linear system in $\mathbf{R}^4$ is binarized to generate a pseudo-random sequence which encrypt a grayscale image via symmetric-key algorithm. The sequence is analyzed throughout statistical tests according to the National Institute of Standards and Technology (NIST) specifications. The scrolls of the system are the result of a switching law that changes between the saddle hyperbolic equilibria of piecewise linear systems with eigenvalues as follows: two negative real and one pair of complex

*Corresponding author
Email addresses: moises.garcia@ipicyt.edu.mx (M. García-Martínez), luisjavier.ontanon@gmail.com (L.J. Ontañón-García), eric.campos@ipicyt.edu.mx (E. Campos-Cantón), celikovs@utia.cas.cz (S. Čelikovský)

conjugate eigenvalues with positive real part. Thus, the encryption quality is evaluated depending on the variation of the number of scrolls.
Keywords: Hyperchaotic encryption; piecewise linear systems; stream cipher; pseudo-random bit generator; chaos theory; multi-scroll attractors.

1. Introduction

The idea of transmitting sensitive information in a secure way, safely hidden to potential hackers and eavesdroppers, has generated really strong impact in the scientific community inspiring nowadays many researchers to combine a great variety of approaches in order to tackle this challenging issue. Several methods that mask the transmitted information have been proposed during recent years. These encryption methods are based on many different techniques, for example, partial encryption [1], scan patterns [2], cellular automata [3, 4] and splay trees [5] among others [6, 7, 8].

One of the areas that has begun to caught attention in cryptography is chaos. This is due to the intrinsic dynamics of this type of systems and the relationship between chaos and cryptography. In [9], Alvarez and Li determined that many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems, for example:

- Ergodicity and confusion: The output has the same distribution for any input.
- Sensitivity to initial conditions and diffusion with a small change in the plaintext: A small deviation in the input can cause a large change at the output.

- Deterministic dynamics and deterministic pseudo-randomness: A deterministic process can cause a random-like (pseudo-random) behavior.
- Structure complexity and algorithm complexity: A simple process has a very high complexity.

Approaches based on discrete-time systems (maps) have been commonly used during the last decade to encrypt images using block and stream cipher cryptosystems [10, 11, 12, 13]. More recently, the scientific community has started to implement continuous time systems as cryptosystems, see [14, 15, 16, 17, 18] and the references therein. However, some approaches [19, 20, 21, 22] have not demonstrated the statistical properties of the pseudo-random generators and some others [23, 24] have already been proven to be unsafe for encryption.

Recently, some encryption theories have implemented 2D continuous systems whose solutions result in multi-scroll attractors generated through hysteresis [25]. Taking in consideration all these approaches, a new Pseudo-Random Bit Generator (PRBG) based on hyperchaotic multi-scroll piecewise linear (PWL) systems is presented. Whose dynamics in addition to live in a space with four degrees of freedom are also safe to be used in cryptography.

Among all the theories on generating multi-scroll attractors, for example: extension of the Chua's diode, saturation and hysteresis among others [26], here, the generation of multi-scroll by PWL systems with unstable dissipative equilibria [27, 28] is considered. One of the advantages of unstable dissipative systems is that with a corresponding switching law the resulting trajectory between two of these systems may be contained in a double-scroll attractor. The number of scrolls is given by the number of saddle equilibrium points of

each unstable subsystem. These equilibria are characterized by fast stable eigendirection and a complex unstable spiral-like eigenplane corresponding to appropriate eigenvalues. The relation between the number of scrolls and the resulting pseudo-random sequence will be analyzed throughout by some statistical tests.

The article is organized as follows: Section 2 introduces the theoretical basis for the hyperchaotic multi-scroll systems; while Section 3 derives the PRBG along with some statistical tests showing that its use is safe in cryptography according to the National Institute of Standards and Technology (NIST). Furthermore Section 4 applies a scheme for grayscale image encryption based on the symmetric key stream cipher using the generator like a keystream. Section 5 endorses the method proposed by some security analysis and finally some conclusions are drawn in Section 6.

2. Hyperchaotic multi-scroll attractors

Continuing the work based on PWL systems in $\mathbf{R}^3$ by [27, 29] and extending to $\mathbf{R}^4$ as described in [28], we consider the class of affine linear system given by:

$$\dot{\mathbf{X}} = \mathbf{A}\mathbf{X} + \mathbf{B}, \tag{1}$$

where $\mathbf{X} = [x_1, x_2, x_3, x_4]^T \in \mathbf{R}^4$ is the state vector, $\mathbf{A} = [a_{ij}] \in \mathbf{R}^{4\times4}$, $i, j = 1, 2, 3, 4$, denotes a real matrix and $\mathbf{B} = [B_1, B_2, B_3, B_4]^T \in \mathbf{R}^4$ stands for a real vector. We are interested in a dissipative system having a hyperbolic equilibrium point at $\mathbf{X}^*$, i.e. $\mathbf{A}\mathbf{X}^* + \mathbf{B} = 0$. The corresponding set of eigenvalues $\Lambda = \{\lambda_i\}, i = 1, ..., 4$ of $\mathbf{A}$ are as follows: two λ_i are negative real

eigenvalues, and two λ_i are complex conjugate eigenvalues with positive real part $Re\{\lambda_i\} > 0$. In order to assure dissipativeness of (1), these eigenvalues are assumed to satisfy $\sum_{i=1}^{4} \lambda_i < 0$.

Nevertheless, the system given by Eq. (1) is unstable, therefore, we need to consider a switching system in order to generate bounded trajectories as follows:

$$\dot{\mathbf{X}} = \mathbf{A}\mathbf{X} + \mathbf{B}(\mathbf{X}),$$

$$\mathbf{B}(\mathbf{X}) = \begin{cases} B_1, & \text{if } \mathbf{X} \in \mathcal{D}_1; \\ B_2, & \text{if } \mathbf{X} \in \mathcal{D}_2; \\ \vdots & \vdots \\ B_k, & \text{if } \mathbf{X} \in \mathcal{D}_k, \end{cases} \tag{2}$$

where $\mathbf{R}^4 = \cup_{i=1}^{k} \mathcal{D}_i$. The system given by Eq. (2) has the equilibria $\mathbf{X}_1^* \in \mathcal{D}_1, \ldots, \mathbf{X}_k^* \in \mathcal{D}_k$ with $\mathbf{A}\mathbf{X}_i^* + B_i = 0, i = 1, \ldots, k$. The goal is to choose vectors B_i, in such a way that system (2) becomes chaotic. Namely, for any initial condition $\mathbf{X}_0$ the trajectory converges to some chaotic strange attractor presenting strong dependance on initial conditions, recurrence behavior and topological transitivity. To achieve that, a collection of heteroclinic orbits $\phi(\mathbf{X}_0)$ trapped in a hyperchaotic attractor $\mathfrak{A}$ is needed, upon defining at least two vectors B_1 and B_2 connecting neighboring equilibria. Note that all these heteroclinic connections would be structurally stable, as it will be shown later for a 2-dimensional stable and 2-dimensional unstable manifolds in a transversal way. Thanks to these heteroclinic connections, each trajectory is taken from the domain corresponding to one of the equilibria to the

next domain, thereby visiting all domains in a topologically transitive way. Besides, heteroclinic orbits are known to indicate chaos existence.

The system generated by this method can display k multi-scroll attractors as a result of a combination of several unstable "one-spiral" trajectories, where k is the number of subsystems introduced.

The location of the scrolls occurs in one direction grid (1D-grid) in which the equilibrium points of the subsystems are introduced. Although many systems may satisfy the discussion aforementioned, the matrix $\mathbf{A}$ and the vector $\mathbf{B}$ will be defined as follows:

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1.5 & -1 & -1 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 0 \\ 0 \\ B_3 \\ B_4 \end{pmatrix}. \tag{3}$$

The case of $B_3 = B_4$ is considered throughout the paper. For this particular case of matrix $\mathbf{A}$ and vector $\mathbf{B}$, the equilibrium points (obtained from $\mathbf{X}^* = -\mathbf{A}^{-1}\mathbf{B}$) are displaced in 1D-grid onto the plane (x_1, x_4). By considering a different matrix $\mathbf{A}$ and a different vector $\mathbf{B}$, the displacement can be made in different directions inside a n-dimensional grid. For example the case of $\mathbf{B} = (0, B_3, B_3, 0)^T$ will result in a displacement along 1D-grid onto the (x_1, x_3) plane.

For the sake of simplicity and in order to understand the 2-dimensional stable and 2-dimensional unstable manifolds of the system given by (3), consider the linear transformation $T : \mathbf{R}^4 \to \mathbf{R}^4$ with the following transformation of coordinates:

$$\dot{\mathbf{Y}} = \hat{\mathbf{A}}\mathbf{Y} + \hat{\mathbf{B}}. \tag{4}$$

Here $\mathbf{Y} = \mathbf{Q}^{-1}\mathbf{X}$, where $\mathbf{Q}$ is an invertible matrix that satisfies $\hat{\mathbf{A}} = \mathbf{Q}^{-1}\mathbf{A}\mathbf{Q}$ and $\hat{\mathbf{B}} = \mathbf{Q}^{-1}\mathbf{B}$, taking the following values:

$$\begin{aligned} \hat{\mathbf{A}} &= \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0.1020 + 1.1115i & 0 & 0 \\ 0 & 0 & 0.1020 - 1.1115i & 0 \\ 0 & 0 & 0 & -1.2041 \end{pmatrix}, \\ \hat{\mathbf{B}} &= B_3 \begin{pmatrix} 3 \\ 0.4223 + 0.3434i \\ 0.4223 - 0.3434i \\ 2.1329 \end{pmatrix}. \end{aligned} \tag{5}$$

Therefore, the set of eigenvalues of the system given by Eq. (3) results in $\Lambda = diag(\hat{\mathbf{A}}) = \{-1.0000, 0.1020 \pm 1.1115i, -1.2041\}$, according to the saddle hyperbolic equilibrium point of the unstable system required.

Now, a switching law depending on the value of x_1 that results in a double-scroll attractor is defined as follows:

$$B_3(x_1) = \begin{cases} 0.9, & \text{if } x_1 \geq 0; \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

The system given by Eq. (3) with the switching law given by Eq. (6) presents the following equilibrium points: $\mathbf{X}_1^* = (0, 0, 0, 0)^T$ and $\mathbf{X}_2^*$ =(0.6, 0, 0, 0.9)^T. Since $\mathbf{R}^4$ is divided in two domains so two subsystems are needed to

determine the dynamics of the system. Each subsystem introduces an equilibrium point in its corresponding domain and a scroll emerges in the overall attractor. The projection of the double-scroll attractor onto the (x_1, x_2) plane with initial condition $\mathbf{X}_0 = (1, 0, 0, 0)^T$ depicts a double-scroll (Figure 1 a)).

Now, if the switching law is designed considering more subsystems commuting B_3, then more scrolls can be obtained in the resulting attractor. For example, to obtain a 4-scroll attractor, B_3 can be given as follows:

$$B_3 = \begin{cases} 1.8, & \text{if } x_1 \geq 0.9; \\ 0.9, & \text{if } 0.3 \leq x_1 < 0.9; \\ 0, & \text{if } -0.3 < x_1 < 0.3; \\ -0.9, & \text{if } x_1 \leq -0.3, \end{cases} \tag{7}$$

this switching law introduces two additional subsystems with corresponding equilibrium points located at $\mathbf{X}_3^* = -\mathbf{X}_2^*$ and $\mathbf{X}_4^* = (1.2, 0, 0, 1.8)^T$. The projection of the 4-scroll attractor onto the (x_1, x_2) plane given by the switching law (7) with initial condition $\mathbf{X}_0 = (1, 0, 0, 1)^T$ is shown in (Figure 1 b)). Now, by means of adding 6 subsystems results in the case of a 10-scroll attractor given by the following switching law:

$$B_3 = \begin{cases} 4.5, & \text{if } x_1 \geq 2.7; \\ 3.6, & \text{if } 2.1 \leq x_1 < 2.7; \\ 2.7, & \text{if } 1.5 \leq x_1 < 2.1; \\ 1.8, & \text{if } 0.9 \leq x_1 < 1.5; \\ 0.9, & \text{if } 0.3 \leq x_1 < 0.9; \\ 0, & \text{if } -0.3 \leq x_1 < 0.3; \\ -0.9, & \text{if } -0.9 \leq x_1 < -0.3; \\ -1.8, & \text{if } -1.5 \leq x_1 < -0.9; \\ -2.7, & \text{if } -2.1 \leq x_1 < -1.5; \\ -3.6, & \text{if } x_1 \leq -2.1. \end{cases} . \tag{8}$$

The 10-scroll attractor given by the switching law (8) with initial condition $\mathbf{X}_0 = (4, 0, 0, 1)^T$ can be appreciated from the projection of the attractor onto the (x_1, x_2) plane as Figure 1 c) depicts. The positive Lyapunov exponents of the system are $(0.136181, 0.135918)$, indicating that the system is hyperchaotic. These exponents remain the same regardless of the number of scrolls presented in the attractor. The integration of these systems was considered by a fourth order Runge Kutta method with a 0.01 integration step.

3. Pseudo Random Bit Generator

This generator is based on the time series obtained from the hyperchaotic multi-scroll system states given by Eq. (2) with (3) for different number of scrolls (2, 4, or 10).

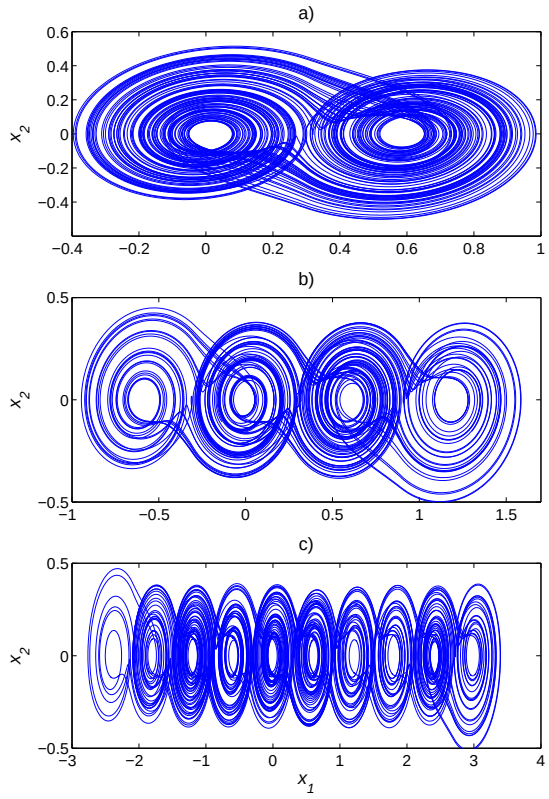


Figure 1: Projection of the attractor given by Eq. (2) with (3) onto the (x_1, x_2) plane for different switching laws: a) 2 scrolls with Eq. (6); b) 4 scrolls with Eq. (7); c) 10 scrolls with Eq. (8).

The idea is to iterate the system n times to obtain a sequence $\mathbf{X}$ after 1000 iterations of the transient state. Taking advantage of the sensitivity to initial conditions in chaotic systems, it is considered that each set of initial conditions $\mathbf{X}_{0p}$ with $p \in \mathbf{Z}^+$ results in p different time series, where $\mathbf{X}_{01} \neq \ldots \neq \mathbf{X}_{0p}$. Therefore, each $\mathbf{X}_{0p}$ can be considered as a key to the cipher, if the number of scrolls is augmented then the dynamics of the system is more complex and the encryption quality is increased.

Thereupon the PRBG is defined as follows

$$\kappa_i = \left\lfloor \sum_{j=1}^{4} x_j(i) \cdot 10^{14} \right\rfloor \ mod\ 256. \tag{9}$$

Here $\kappa_i \in \{0, 1, 2, \ldots, 255\}$ and $i = 1, \ldots, n$, where $n = l \times m$ with l, m accordingly to the size of the grayscale image to be encrypted. The operation $\lfloor \cdot \rfloor$ stands for the floor function, namely $\lfloor x \rfloor \in \mathbf{Z}$, s.t. $\lfloor x \rfloor \leq x \leq \lfloor x \rfloor + 1$. Since the numerical simulator works with floating point and double precision, the sum can be scaled to 10^{14}. Thus each i-th value of κ is an integer number which can be represented by 8 bits sequence, resulting in an overall binary κ sequence of $8n = l \times m \times 8$ bits.

First the correlation coefficient is determined by two sequences with nearby keys and the sensitivity to initial conditions is analyzed. The correlation coefficients $\mathfrak{C}_{\mathcal{E},\mathcal{F}}$ for each pair of sequences $\mathcal{E} = [e_1, ..., e_N]$ and $\mathcal{F} = [f_1, ..., f_N]$ are computed as follows [30]:

$$\mathfrak{C}_{\mathcal{E},\mathcal{F}} = \frac{\sum_{i=1}^{N} (\mathcal{E}_i - \bar{\mathcal{E}})(\mathcal{F}_i - \bar{\mathcal{F}})}{\left[\sum_{i=1}^{N} (\mathcal{E}_i - \bar{\mathcal{E}})^2\right]^{1/2} \left[\sum_{i=1}^{N} (\mathcal{F}_i - \bar{\mathcal{F}})^2\right]^{1/2}}, \tag{10}$$

where $\bar{\mathcal{E}} = \frac{1}{N} \sum_{i=1}^{N} \mathcal{E}_i$ and $\bar{\mathcal{F}} = \frac{1}{N} \sum_{i=1}^{N} \mathcal{F}_i$ are the mean values of $\mathcal{E}$ and $\mathcal{F}$, respectively. The coefficients $\mathfrak{C}_{\mathcal{E},\mathcal{F}}$ are computed for each pair of generated sequences with nearby initial conditions, *i.e.*, $\mathbf{X}_0$ and $\mathbf{X}'_0 = \mathbf{X}_0 + \delta$, this has been done for every state of the system $(x_i, i = 1, \ldots, 4)$ and for 2, 4 and 10 scrolls. The corresponding data with $\delta = 1 \times 10^{-15} \cdot (1, 1, 1, 1)^T$ demonstrates that $\mathfrak{C}_{\kappa_i \kappa'_i} \approx 0$ (Table 1), meaning that there is no correlation between the generated sequences with nearby initial conditions. This value decreases when the number of scrolls is increased, for example, from 2 scrolls to 4 scrolls the percent of decrease is of 55.3%, and from 2 to 10 scrolls is

Table 1: Correlation coefficients of pseudo-random sequences with nearby initial conditions.

Number of scrolls	$\mathbf{X}_0$	$\mathfrak{C}_{\mathcal{E},\mathcal{F}}$
2 scrolls	0.05624	$\mathfrak{C}_{\mathcal{E}_1,\mathcal{F}_1} = 0.1754$
	0.14957	$\mathfrak{C}_{\mathcal{E}_2,\mathcal{F}_2} = 0.2262$
	0.49637	$\mathfrak{C}_{\mathcal{E}_3,\mathcal{F}_3} = 0.2284$
	0.32378	$\mathfrak{C}_{\mathcal{E}_4,\mathcal{F}_4} = 0.1624$
	κ_i	$\mathfrak{C}_{\kappa_i,\kappa_i'} = -0.0103$
4 scrolls	0.93147	$\mathfrak{C}_{\mathcal{E}_1,\mathcal{F}_1} = 0.2833$
	0.13678	$\mathfrak{C}_{\mathcal{E}_2,\mathcal{F}_2} = 0.1789$
	0.71548	$\mathfrak{C}_{\mathcal{E}_3,\mathcal{F}_3} = 0.1401$
	0.05621	$\mathfrak{C}_{\mathcal{E}_4,\mathcal{F}_4} = 0.2877$
	κ_i	$\mathfrak{C}_{\kappa_i,\kappa_i'} = -0.0046$
10 scrolls	0.35489	$\mathfrak{C}_{\mathcal{E}_1,\mathcal{F}_1} = 0.3696$
	0.18957	$\mathfrak{C}_{\mathcal{E}_2,\mathcal{F}_2} = 0.2969$
	0.75621	$\mathfrak{C}_{\mathcal{E}_3,\mathcal{F}_3} = 0.2791$
	0.42687	$\mathfrak{C}_{\mathcal{E}_4,\mathcal{F}_4} = 0.3707$
	κ_i	$\mathfrak{C}_{\kappa_i\kappa_i'} = -0.0008$

92.2%.

In order to determine whether or not the series generated by Eq.(9) possess the same statistical properties as a truly random sequence, first they must be analyzed through statistical tests to demonstrate that they are suitable to be used in cryptography.

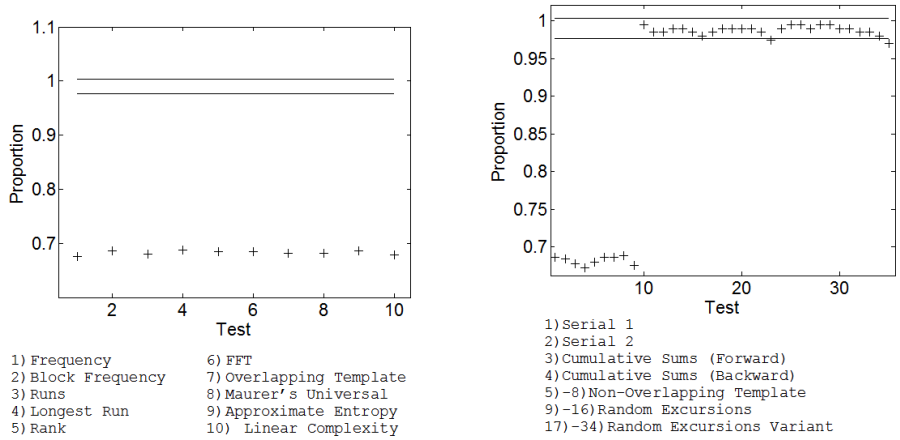
Among some of the possible tests [31, 32, 33], here, the statistical tests proposed by NIST [34] were implemented, which describe a combination of tests that detect any deviation from randomness. The idea is to define a significance level σ, typically chosen between 0.001 and 0.01. For example, considering a value of $\sigma = 0.01$ which indicates that 1 out of 100 sequences may be rejected by the tests in the case of having a random sequence.

The NIST has adopted two ways to interpret empirical results: (1) the examination of the proportion of sequences that pass statistical tests and (2) the distribution of P-values to check for uniformity, only the examination of the proportion of sequences that pass a statistical tests will be considered. For this, it is necessary to define a confidence interval as:

$$(1-\sigma) \pm 3\sqrt{\frac{\sigma}{\theta}}, \tag{11}$$

where $\theta = 500$ is the sample size of sequences, i.e. the amount of sequences that were checked and each of this sequences has 1×10^6 elements. This statistical suite of tests is applied to different sequences which are generated by hiperchaotic systems with different number of scrolls. By means of equation (11), the confidence interval is given by 0.99 ± 0.01342, thus, if the statistic test result is within this interval then it is considered that passed the test, and the result is success (S), otherwise fail (F), as is shown in the tables 2 and 3.

For a generated series with a double scroll hyperchaotic system, the proportion is outside of the confidence interval for 20 of the tests (Figures 2 (a) and (b)), meaning that the hyperchaotic system with 2 scrolls is not useful to cipher information. Similar results have been obtained for a 3 scroll attractor, so this number of scrolls is also unsafe for encryption. If the hyperchaotic attractors present 4 and 10 scrolls then the sequences result is inside the confidence interval, (see Figures 3 (a),(b) and Figures 4 (a),(b)). Hence the sequences are generated by hyperchaotic attractors with 4 and 10 scrolls therefore, they are safe to be used like a keystream.



(a) Part 1 (b) Part 2

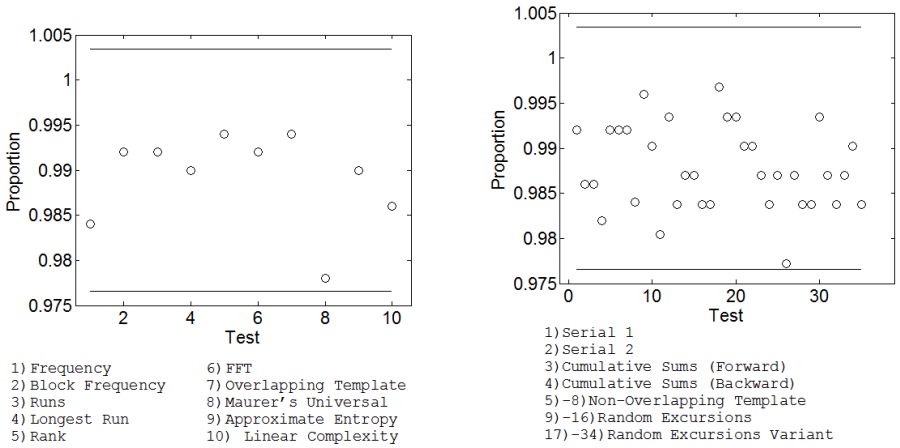
Figure 2: Part 1 and 2 of the results of the sequences with 2 scrolls according to the suite of statistical tests of the NIST using the confidence interval given by (11).

4. Design of the encryption and decryption scheme

After proving that sequences generated by hyperchaotic systems with four or more scrolls are safe as PRBG for cryptography, we encrypt the image using a similar stream cipher as the ones reported in [6, 35, 36]. The purpose of ciphering information with the proposed PRBG is to demonstrate that sequences with different number of scrolls generate different cipher image i.e., the encryption quality is improved if the number of scrolls is increased. The process for cipher the image is pixel by pixel in the following way:

$$\begin{cases} C_1 = P_1 \oplus \kappa_1 \oplus IV; \\ C_i = P_i \oplus \kappa_i \oplus C_{i-1}. \end{cases} \tag{12}$$

Where C_i and P_i with $i = 2, \ldots, n$ are the pixels of the cipher image and the plain image, respectively. To improve security in the process, a



(a) Part 1 (b) Part 2

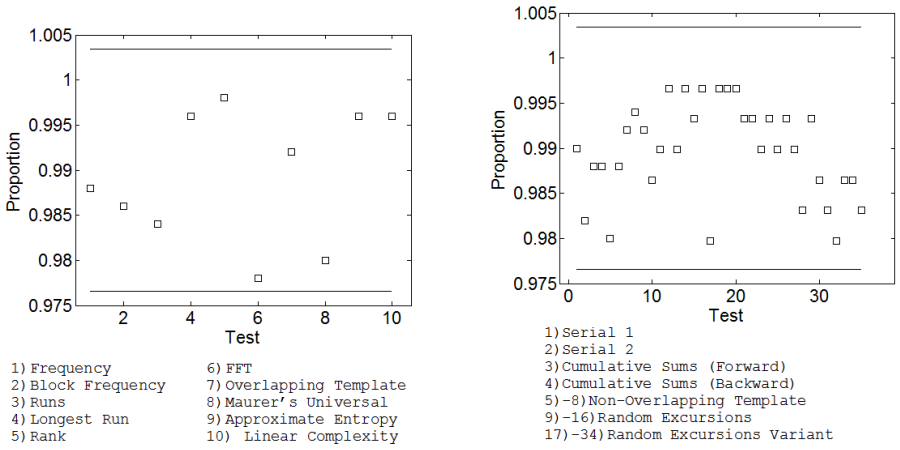
Figure 3: Part 1 and 2 of the results of the sequences with 4 scrolls according to the suite of statistical tests of the NIST using the confidence interval given by (11).

feedback in the encryption (C_{i-1}) and an initial vector are considered, where IV $\in \{0, 1, \ldots, 255\}$ is an initialization vector used once, κ_i is the pseudo-random bit sequence, the symbol $\oplus$ is the XOR operation, which is executed bit by bit in the block of 8 bits by pixel.

In order to decrypt the image correctly the receiver must have the same keystream (formed by the initial conditions $\mathbf{X}_0$, the initialization vector IV and the decryption function). This function takes the following form:

$$\begin{cases} P'_1 = C_1 \oplus \kappa_1 \oplus IV; \\ P'_i = C_i \oplus \kappa_i \oplus C_{i-1}. \end{cases} \tag{13}$$

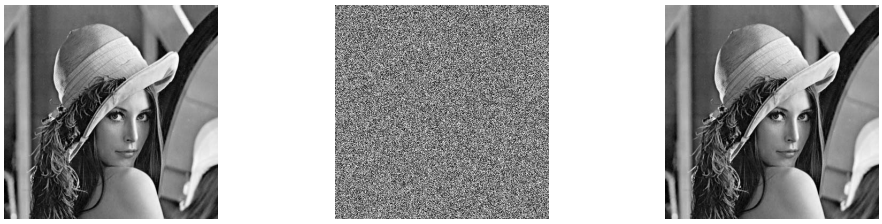
If the correct key κ_i and the correct initialization vector IV are used, then the original image will be obtained correctly, i.e., $P'_i = P_i$. In order to prove the encryption–decryption method, the common grayscale image of Lenna



(a) Part 1 (b) Part 2

Figure 4: Part 1 and 2 of the results of the sequences with 10 scrolls according to the suite of statistical tests of the NIST using the confidence interval given by (11).

was considered, thus Figure 5 (a) shows the plain image; the cipher image is presented in Figure 5 (b) and the decrypted image is shown in Figure 5 (c).



(a) (b) (c)

Figure 5: Image of Lenna: (a) Original; (b) Encrypted; (c) Decrypted.

Table 2: Part 1 of results from statistical suite of tests. F=Fail;S=Success

Test name	2 scrolls		4 scrolls		10 scrolls	
	Portion passing	Result	Portion passing	Result	Portion passing	Result
Frequency test	0.6760	F	0.9840	S	0.9880	S
Frequency test within a block	0.6860	F	0.9920	S	0.9860	S
Runs test	0.6800	F	0.9920	S	0.9840	S
Test for the longest run	0.6880	F	0.9900	S	0.9960	S
Binary matrix	0.6840	F	0.9940	S	0.9980	S
Discrete fourier transform	0.6840	F	0.9920	S	0.9760	S
Overlapping template matching test	0.6820	F	0.9940	S	0.9920	S
Maurer's universal statistical test	0.6820	F	0.9780	S	0.9780	S
Approximate entropy	0.6860	F	0.9900	S	0.9960	S
Linear complexity	0.6780	F	0.9860	S	0.9960	S

5. Security analysis

The proposed algorithm can successfully encrypt and decrypt the image. However, it is imperative to verify the security of the cryptosystem in order to detect if the scheme is robust against any statistical attack. To do so six security tests were implemented: i) Key space analysis; ii) the histogram analysis; iii) entropy; iv) calculation of the correlation coefficients of adjacent pixels; v) encryption quality and vi) security test against differential attack.

5.1. Key space analysis

A good encryption algorithm must have a key space large enough to make brute-force attacks infeasible. The key space for a cryptographic algorithm should not be less than 2^{128} to resist brute force attacks [38]. For the proposed image encryption algorithm the key is given by the initial condition $\mathbf{X}_0$, where each state has a double precision. Here, a system with 4 states is

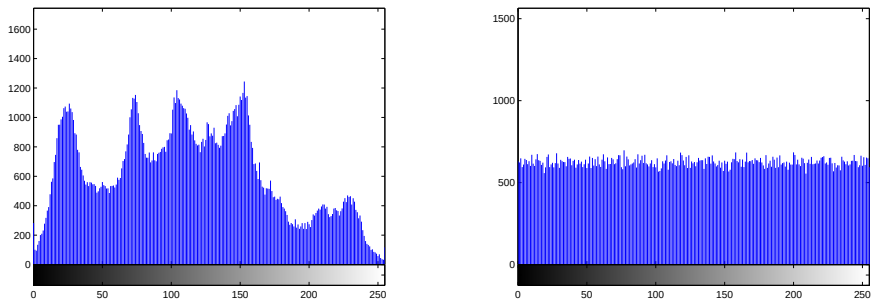
Table 3: Part 2 of results from statistical suite of tests. F=Fail; S=Success.

Test name	2 scrolls		4 scrolls		10 scrolls	
	Portion passing	Result	Portion passing	Result	Portion passing	Result
Serial test 1	0.6860	F	0.9920	S	0.9900	S
Serial test 2	0.6840	F	0.9860	S	0.9820	S
Cumulative sums test						
a) Forward	0.6780	F	0.9860	S	0.9880	S
b) Backward	0.6720	F	0.9820	S	0.9880	S
Non-overlapping template matching test						
a)	0.6800	F	0.9920	S	0.9800	S
b)	0.6860	F	0.9920	S	0.9880	S
c)	0.6860	F	0.9920	S	0.9920	S
d)	0.6880	F	0.9840	S	0.9940	S
Random excursions test						
a) -4	0.9950	S	0.9935	S	0.9865	S
b) -3	0.9849	S	0.9902	S	0.9899	S
c) -2	0.9849	S	0.9805	S	0.9966	S
d) -1	0.9899	S	0.9837	S	0.9899	S
e) 1	0.9899	S	0.9870	S	0.9966	S
f) 2	0.9849	S	0.9870	S	0.9932	S
g) 3	0.9799	S	0.9837	S	0.9966	S
h) 4	0.9849	S	0.9837	S	0.9797	S
Random excursions variant test						
a) -9	0.9899	S	0.9967	S	0.9966	S
b) -8	0.9899	S	0.9935	S	0.9966	S
c) -7	0.9899	S	0.9935	S	0.9966	S
d) -6	0.9899	S	0.9902	S	0.9932	S
e) -5	0.9849	S	0.9902	S	0.9932	S
f) -4	0.9749	F	0.9870	S	0.9899	S
g) -3	0.9899	S	0.9837	S	0.9932	S
h) -2	0.9950	S	0.9870	S	0.9899	S
i) -1	0.9950	S	0.9739	S	0.9932	S
i) 1	0.9899	S	0.9870	S	0.9899	S
k) 2	0.9950	S	0.9837	S	0.9831	S
l) 3	0.9950	S	0.9837	S	0.9932	S
m) 4	0.9899	S	0.9935	S	0.9865	S
n) 5	0.9899	S	0.9870	S	0.9831	S
o) 6	0.9849	S	0.9837	S	0.9797	S
p) 7	0.9849	S	0.9870	S	0.9865	S
q) 8	0.9799	S	0.9902	S	0.9865	S
r) 9	0.9698	F	0.9837	S	0.9831	S

considered. According to the IEEE floating-point standard [37] the computational precision of the 64-bit double-precision number is about 10^{-15}, thereby the total space is $\simeq 6.582\text{x}10^{63} \simeq 2^{212}$, therefore the algorithm exceeds the standard for 2^{84}.

5.2. Histogram analysis

The histogram depicts how pixels are distributed in an image. It plots the number of pixel according to the grayscale level. A property that should satisfy an encryption system is that the histogram of the encrypted image presents a uniform distribution. Therefore, the histograms between the original image and the encrypted image must be completely different. Figure 6 depicts both histograms, Figure 6 (a) shows the histogram of the original image and Figure 6 (b) of the encrypted image. Notice that the latter depicts a uniform distribution as expected.



(a) (b)

Figure 6: Histogram of the images of Lenna: (a) Original image; (b) Encrypted image.

Table 4: Correlation coefficients of two adjacent pixels.

	Plain image	Cipher image with 2 scrolls	Cipher image with 4 scrolls	Cipher image with 10 scrolls
Lenna				
Vertical	0.9829	0.0207	0.0306	-0.0343
Horizontal	0.9687	-0.0515	0.0044	0.0017
Diagonal	0.9520	0.0284	-0.0146	0.0013
Einstein				
Vertical	0.9832	0.0450	0.0086	0.0082
Horizontal	0.9795	-0.0205	0.0168	0.0152
Diagonal	0.9677	-0.0440	-0.0258	-0.0206
Baboon				
Vertical	0.8186	0.0184	0.0179	0.0001
Horizontal	0.8641	-0.0333	0.0201	0.0055
Diagonal	0.7766	0.0253	-0.0175	0.0018

5.3. Correlation Analysis

It is well known that adjacent image pixels are highly correlated in vertical, horizontal and diagonal directions. This property can be quantified by means of the correlation coefficient, between adjacent pixels using Eq. 10. Now, $\mathcal{E}$ and $\mathcal{F}$ denote the intensity value pixels which are adjacent, N is the total number of duplets $(\mathcal{E}, \mathcal{F})$ which for this particular case $N = 2000$. A plain image is expected to present a value of 1, meaning that every pixel is highly correlated and the image transitions result smoother. On the other hand an encrypted image is expected to present values equal to zero, assuring that there is no relation between the pixels in any vertical, horizontal and diagonal direction. The result of this test is shown in Table 4, Figure 7 and Figure 8.

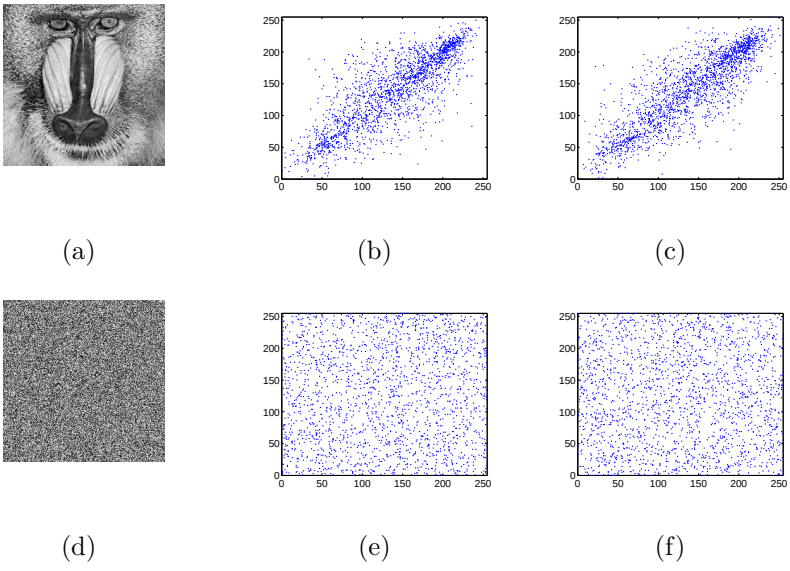


Figure 7: (a) Plain image Baboon; (b) Correlation in vertical direction of plain image; (c) Correlation in horizontal direction of plain image; (d)Encrypted image Baboon; (e) Correlation in vertical direction of encrypted image; (f) Correlation in horizontal direction of encrypted image.

5.4. Information Entropy

Entropy is one of the most significant features of randomness [39], it can be used to characterize the texture of and image and is defined as follows:

$$E(s) = -\sum_{i=0}^{2^M-1} Pr(s_i) log_2 Pr(s_i), \tag{14}$$

where M is the number of bits to represent a symbol $s_i \in s$, and $Pr(s_i)$ represents the probability of a symbol s_i, therefore the entropy is expressed in bits. For a cipher grayscale image with 256 levels, the entropy should ideally be $E(s) = 8$.

The entropies for plain image and cipher images using different number

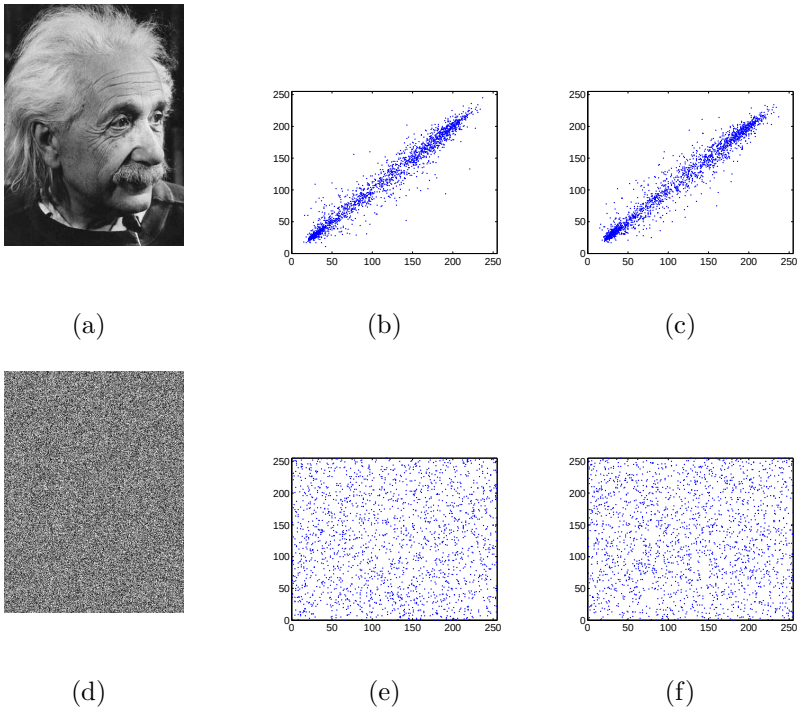


Figure 8: (a) Plain image Einstein; (b) Correlation in vertical direction of plain image; (c) Correlation in horizontal direction of plain image; (d) Encrypted image Einstein; (e) Correlation in vertical direction of encrypted image; (f) Correlation in horizontal direction of encrypted image.

of scrolls are calculated and listed in Table 5. Notice that in the cipher image for any number of scrolls the entropy is close to the ideal value.

5.5. Encryption Quality

The encryption creates large changes in the amount of pixels which should be completely different from the original image. These changes are irregular and more changes in the value of pixels show more effectiveness of encryption algorithm and thus better quality. The encryption quality represents the

Table 5: Entropy for plain image and cipher image with 2, 4 and 10 scrolls.

Entropy	Plain image	2 scrolls	4 scrolls	10 scrolls
Lenna	7.8059	7.9986	7.9989	7.9989
Einstein	7.4913	7.9988	7.9989	7.9989
Baboon	7.7091	7.9967	7.9973	7.9973

Table 6: Encryption quality for cipher images with 2, 4 and 10 scrolls.

Encryption quality	2 scrolls	4 scrolls	10 scrolls
Lenna	271.1094	271.5391	271.6563
Einstein	314.4609	314.6250	314.8906
Baboon	118.6953	119.7188	119.9688

average number of changes to each gray level according to [40] and it can be expressed as:

$$Q = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256}, \tag{15}$$

where L's are the gray levels of the images, $H_L(C)$ and $H_L(P)$ are the number of repetition from each gray value in the original and the encrypted image, respectively. The results of this test are shown in Table 6 where it is possible to see if the number of scrolls increases then the encryption quality of the cipher image is increased.

5.6. Differential attack

In the differential attack the opponent may perform a slight change modifying only one pixel of the original image to observe the changes on the corresponding cipher image, trying to find a relationship between the plain image and the cipher image. To make this attack practically useless the encryption algorithm should be such that a small change in the plain image

produces a significant change in the cipher image. Usually, in this attack the first pixel is changed, in this work this is the case. Nevertheless if the last pixel is modified, in the cipher image only one pixel is modified, it is possible to avoid such situation with a second round encryption. This property can be measured by two criteria, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI).

The NPCR measures the number of different pixels between two cipher images.

$$NPCR = \frac{\sum_{i,j} \delta_a(i,j)}{\nu} \times 100\%; \tag{16}$$

$$\delta_a(i,j) = \begin{cases} 0 & \text{if } C(i,j) = C'(i,j); \\ 1 & \text{if } C(i,j) \neq C'(i,j). \end{cases} \tag{17}$$

Where ν is the total number of pixels in the image, C and C' are the cipher images with one modified pixel in the original image.

The second criterion, UACI can be defined as:

$$UACI = \frac{1}{\nu} \left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{2^8 - 1} \right]. \tag{18}$$

Results of these tests are shown in Table 7. These results show that the scheme is very sensitive with respect to small changes in the plain text and the two cipher images C and C' behave like two random images.

5.7. General specifications and extension of the work

In order to use the presented approach, some specification need to be established. First of all, the same integration method and step must be

Table 7: Correlation coefficients of two adjacent pixels.

	Proposed scheme
NPCR	99.6078
UACI	33.4182

considered in order to encrypt and decrypt. This work may also be extended to audio, video and text signals if the information to be ciphered is arranged as a matrix of size $l \times m$. The numerical simulation regarding this matter will be studied and reported elsewhere.

6. Conclusions

Based on the intrinsic property of sensitiveness to initial conditions, a new PRBG capable of generating binary sequences using the four states of a multi-scroll hyperchaotic system was presented. The trajectory of these complex systems based on PWL systems can result in any number of scrolls with a correct switching law. It has been demonstrated that the number of scrolls on the system affects the properties of the sequences, allowing them to pass the statistical test of the NIST. The pseudo-random sequence is used like keystream to encrypt grayscale image using the XOR operation. The encrypted image has been proved to pass several security tests assuring that it is safe to use in encryption. Moreover the results show that increasing the number of scrolls improve the encryption quality of the image.

Acknowledgments

M. García-Martínez is doctoral fellow of the CONACYT in the Graduate Program on control and dynamical systems at DMAp-IPICYT. L.J.

Ontañón-García acknowledges the FAI-UASLP financial support through project No. C15-FAI-04-80.80. E. Campos-Cantón acknowledges the CONACYT financial support through project No. 181002. S. Čelikovský was supported by the Czech Science Foundation through the research grant No. 13-20433S.

References

[1] H. Cheng, Partial Encryption of Compressed Images and Videos, IEEE Transactions on Signal Processing. 48 (8) (2000) 2439-2451.

[2] N. Bourbakis, C. Alexopoulos, Picture data encryption using scan patterns, Pattern Recognition. 25 (6) (1992) 567-581.

[3] S. Wijaya, S. K. Tan, S. U. Guan, Permutation and sampling with maximum length CA or pseudorandom number generation, Applied Mathematics and Computation. 185 (1) (2007) 312-321.

[4] A. M. Del Rey, J. P. Mateus, G. R. Sánchez, A secret sharing scheme based on cellular automata, Applied Mathematics and Computation. 170 (2) (2005) 1356-1364.

[5] D. Jones, Applications of splay trees to data compression, Communications of the ACM. 31 (8) (1988) 996-1007.

[6] H.S. Kwok, W.K.S. Tang, A fast image encryption system based on chaotic maps with finite precision representation, Chaos, Solitons and Fractals. 32 (4) (2007) 1518-1529.

[7] T. Uehara, R. Safavi-Naini, P. Ogunbona, Securing Wavelet Compression with Random Permutations, The First IEEE Pacific-Rim Conference on Multimedia. (2000) 332-335.

[8] H.K.C. Chang, J.L. Liu, A linear quadtree compression scheme for image encryption, Signal Processing: Image Communication. 10 (4) (1997) 279-290.

[9] G. Alvarez, S. Li, Some Cryptographic requirements for Chaos-Based cryptosystems, International Journal of Bifurcation and Chaos. 16 (8) (2006) 2129-2151.

[10] M. Gotz, K. Kelber, W. Schwar, Discrete-Time Chaotic Encryption Systems Part I: Statistical Design Approach, IEEE Transactions on Circuits and Systems I. 44 (10) (1997) 963-970.

[11] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons and Fractals. 21 (3) (2004) 749-761.

[12] L. Kocarev, G. Jakimoski, Logistic map as a block encryption algorithm, Physics Letters A, 289 (4-5) (2001) 199-206.

[13] S. Mazloom, A. M. Eftekhari-Moghadam, Color image encryption based on Coupled Nonlinear Chaotic Map, Chaos, Solitons and Fractals. 42 (3) (2009) 1745-1754.

[14] S. Čelikovský, V. Lynnyk, Desynchronization chaos shift keying method based on the error second derivative and its security analysis, International Journal of Bifurcation and Chaos. 22 (9) (2012) 1250231.

[15] H. Hermassi, R. Rhouma, S. Belghith, Improvement of an image encryption algorithm based on hyper-chaos, Telecommunication Systems. 52 (2) (2013) 539-549.

[16] H. Liu, X. Wang, Color image encryption based on one-time keys and robust chaotic maps, Computers and Mathematics with Applications. 59 (10) (2010) 3320-3327.

[17] M. Khan, T. Shah, H. Mahmood, M.A. Gondal, An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dynamics. 71 (3) (2013) 489-492.

[18] M. Khan, T. Shah, H. Mahmood, M.A. Gondal, I. Hussain, A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dynamics. 70 (3) (2012) 2303-2311.

[19] O. Mirzaei, M. Yaghoobi, H. Irani, A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dynamics. 67 (1) (2012) 557-566.

[20] T. Gao, Z. Chen, A new image encryption algorithm based on hyper-chaos, Physics Letters A. 372 (4) (2008) 394-400.

[21] X. Y. Wang, X. J. Wang, Chaotic encryption based on Lorenz system, International Journal of Modern Physics B. 26 (32) (2012) 1250209.

[22] X. Y. Wang, L. Yang, R. Liu, A. Kadir, A chaotic image encryption algorithm based on perceptron model, Nonlinear Dynamics. 62 (3) (2010) 615-621.

[23] Y. Zhang, C. Li, Q. Li, D. Zhang, S. Shu, Breaking a chaotic image encryption algorithm based on perceptron model, Nonlinear Dynamics. 69 (3) (2012) 1091-1096.

[24] X. Wang, L. Liu, Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos, Nonlinear Dynamics. 73 (1-2) (2013) 795-800.

[25] F. Han, J. Hu, X. Yu, Y. Wang, Fingerprint images encryption via multi-scroll chaotic attractors, Applied Mathematics and Computation. 185 (2) (2007) 931-939.

[26] J. Lü, G. Chen, Generating multiscroll chaotic attractors: Theories, methods and applications, International Journal of Bifurcation and Chaos. 16 (4) (2006) 775-858.

[27] E. Campos-Cantón, J. G. Barajas-Ramírez, G. Solís-Perales, R. Femat, Multiscroll attractors by switching systems, Chaos. 20 (1) (2010) 013116.

[28] L.J. Ontañón-García, E. Jiménez-López, E. Campos-Cantón, M. Basin, A family of hyperchaotic multi-scroll attractors in $\mathbf{R}^n$, Applied Mathematics and Computation. 233 (2014) 522-533.

[29] E. Campos-Cantón , R. Femat, G. Chen, Attractors generated from switching unstable dissipative systems, Chaos. 22 (3) (2012) 033121.

[30] M. Franois, T. Grosges, D. Barchiesi, R. Erra, Pseudo-random number generator based on mixing of three chaotic maps, Communications in Nonlinear Science and Numerical Simulation. 19 (4) (2014) 887-895.

[31] Beker H, Piper F. Cipher systems: the protection of communications, New York, Van NostrandReinhold, 1982.

[32] H. Gustafson, E. Dawson, L. Nielsen, W. Caelli, A computer package for measuring the strength of encryption algorithms, Computers and Security. 13 (8) (1994) 687-697.

[33] G. Marsaglia, DIEHARD Statistical Tests: http://www.stat.fsu.edu/pub/diehard/.

[34] A. Rukhin et al, A Statistical test suite for random and pseudo-random number generators for cryptographic applications, NIST special publication (800-22) (2010).

[35] H. Liu, X. Wang, A. Kadir, Color image encryption using Choquet fuzzy integral and hyper chaotic system, Optik. 124 (18) (2013) 3527-3533.

[36] X. Wang, X. Wang, J. Zhao, Z. Zhang, Chaotic encryption algorithm based on alternant of stream cipher and block cipher, Nonlinear Dynamics. 63 (4) (2011) 587-597.

[37] IEEE Computer Society, IEEE Standard for Binary Floating-Point Arithmetic, ANSI/IEEE Std 754 (1985).

[38] Europan Network of Excellence in Cryptology, ECRYPT II Yearly Report on Algorithms and Keysizes (2012).

[39] Shannon C., Communication Theory of Secrecy Systems, Bell System Technical Journal. 28 (1949) 656-715.

[40] H.E.D.H. Ahmed, H.M. Kalash and O.S. Farag Allah, Encryption quality analisys of the RC5 block cipher algorithm for digital images, Optical Enginnering. 45 (10) (2006) 107003.