Applied Mathematics and Computation 270 (2015) 413–424

Contents lists available at ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

Hyperchaotic encryption based on multi-scroll piecewise linear systems

M. García-Martínez[a,d,*], 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, San Luis Potosí, 78216, 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, Czech Academy of Sciences, Pod vodarenskou vezi 4, Prague, 18208, Czech Republic*

[d] *Colegio de la Frontera Sur CHETUMAL, Av. del Centenario Km. 5.5, Chetumal, 77900, Q. Roo, México*

ARTICLE INFO

Keywords:
Hyperchaotic encryption
Piecewise linear systems
Stream cipher
Pseudo-random bit generator
Chaos theory
Multi-scroll attractors

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 conjugate eigenvalues with positive real part. Thus, the encryption quality is evaluated depending on the variation of the number of scrolls.

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 [6–8].

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.

* Corresponding author. Tel.: +5244442685656.
E-mail 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).

http://dx.doi.org/10.1016/j.amc.2015.08.037
0096-3003/

- 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 [10–13]. More recently, the scientific community has started to implement continuous time systems as cryptosystems, see [14–18] and the references therein. However, some approaches [19–22] 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, $\mathbf{A} = [a_{ij}] \in \mathbf{R}^{4\times 4}$, $i, j = 1, 2, 3, 4$, 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 $\Lambda = \{\lambda_i\}, i = 1, \ldots, 4$ 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: