Journal of Information Security and Applications 35 (2017) 119–127

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A novel pseudo random sequence generator for image-cryptographic applications

Rafik Hamza*

LAMIE Laboratory, Department of Computer Science, University of Batna 2, Batna, Algeria

ARTICLE INFO

Article history:

Keywords:
Pseudo random sequence generator
Cryptographic keys
Probability distribution
Images security
Chen chaotic system

ABSTRACT

In this paper, we propose a novel algorithm for pseudo random number sequence generator based on the samples of Chen chaotic system. The proposed algorithm can be used to generate cryptographic keys for digital images among the cryptography applications. Moreover, our pseudo random number generator solves the problem of the non-uniform probability distribution of sequence generated directly by the Chen chaotic system. The various statistical tests such as Diehard battery test and NIST SP 800-22 randomness test verify that the sequences generated by our proposed scheme have good statistical properties. The experimental results of the security analysis validate the high capability of the proposed method to withstand various attacks.

1. Introduction

Cryptography applications should be resistant to different types of cryptanalysis attacks. The cryptographic keys have a very important role in cryptography applications. These keys should be infeasible to find or estimate without the exact secret keys due to the fact that the security depends only on keeping the secret keys secretly [1]. The cryptographic keys require numerous properties such as statistical randomness, and avoid the short periodic and predictable non-randomness keys. The pseudo random number algorithms can propose a good solution to generate a cryptographic key for digital images. As we know, digital images are high sensitivity data that can present a lot of information. Thus, the visual data plays a vital role in different areas such as social networking [2,3], and medical fields [4]. Security of this specific data has become a major concern, which is evident from the recent studies [5–7].

The chaotic maps can be distinguished by a discrete-time such as the logistic map [8], or a continuous-time like Chen chaotic system [9]. The logistic map is one of the famous chaotic systems, considered as a prelude into the chaotic systems. This map proved its importance in several fields, especially with cryptography applications including light-weight image encryption algorithms [10,11], and watermarking algorithms [12–14], and true or pseudo random number generator [15–18]. For example, in our previous work [19], we presented a novel encryption scheme that employed 2D Zaslavsky chaotic map only with the P-box processes, where we permute the pixels based on the indexes sort of the chaotic map directly. García-Martínez et al. [16] proposed a pseudo-random bit generator based on lag time series of the logistic map. Authors used the positive and negative values of this logistic map in the bifurcation parameter with some of a delay in the generation of time series. Franois et al. [20] proposed a novel algorithm to produce a random sequence that consists of mixing three chaotic maps produced from an input initial vector and the generator can resist some attacks such as differential attack and exhaustive attacks. Hu et al. [21] presented a pseudo random sequence generator based on Chen's chaotic system with highly capable of withstanding attacks. Öztürk et al. [22] presented a novel method based on the differential equation from chaotic systems to produce a new pseudo random numbers generator.

In the last two decades, researchers in the field of nonlinear dynamics have become aware of relationship between the chaotic maps and cryptography [16]. The chaotic systems produce good pseudo-stochastic sequences that can be applied to design the cryptography keys [23], due to their valuable properties such as sensibility and large space of the initial values and controlling parameters. The idea of using a chaotic system as pseudo-random is about the ability to propose a dynamic algorithm to produce a sequence of numbers, which are random in their nature. In fact, the former algorithms of the pseudo-random number generator (PRNG) have been proved their ability to be very useful and have been applied accurately with numerous fields, especially with

* Corresponding author.
E-mail addresses: rafik.hamza.uob@gmail.com, r.hamza@univ-batna2.dz, rafik.hamza@hotmail.com

http://dx.doi.org/10.1016/j.jisa.2017.06.005

cryptographic applications, where the keys-cryptographic are very required in image encryption algorithm [24–27].

Recently, some security issues have been presented with the encryption schemes based on chaos [28–31], mainly from three reasons: key space, the structures algorithmic and their combination. For example, Lambić et al. [29] showed some issues on the image encryption algorithm presented in [32] using the weakness of the cryptographic keys. Authors in [30,31] established equivalent keys for most ciphers using some arithmetic operations such as XOR, and modulo Addition. In Özkaynak et al. [33], authors analyzed a security weaknesses of the pseudo sequence generator above-mentioned [21], with total break and exposure the security problems to retrieve the sequence generated with a complexity lower than a brute force attack. The authors in [33] relied on the subordination of output values of a chaotic system that yield a smaller key space, which exploited with a complexity lower than a brute force attack.

The most important problem in chaos-based cryptography is the selection of the chaotic system to generate the pseudo random bits [29,34]. The chaotic maps are defined on real numbers, while almost all cryptographic applications are defined on finite numbers. These defects import some difficulties for the chaos-based image encryption methods, due to round-off errors in real number quantization, which may lead to irreversible functions for encryption and make the decryption process impossible [35]. In addition, chaotic maps in low dimension (eg., 1D or 2D) may lose its chaotic nature completely and become periodic with dynamical degradation when it is discretized in finite precision computation [35]. One dimension logistic map has periodic windows in bifurcation diagrams [36], and other low dimensional chaotic maps such as the piecewise linear chaotic map [37–39]. The lower chaotic maps along with some low spatiotemporal maps are more exposed to the problem of degradation during the finite precision computations. Indeed, the complexity of a chaotic map with high-dimensions is more secure than any lower chaotic map, and can improve the security of the pseudo random number generator. Thus, it is adequate to construct PRNG by high-dimensional chaotic systems to produce digital stream keys.

In this paper, we propose a new effective and secure pseudo-random sequence generator based on Chen chaotic system. The major contributions of this work are given as follows.

(1) We propose a secure pseudo-random sequence generator based on a combination of the three coordinates of the Chen chaotic orbits. We overcome the weaknesses of the former PRNG based on Chen chaotic map [21,33].
(2) The proposed PRNG solves the problem of non-uniform distribution of the sequences generated directly by Chen chaotic system.
(3) The properties of the high-dimensional Chen chaotic map have been used with the average function of the samples by multiplication and applying arithmetic modular. Herein, we have avoided the problem of degradation during the finite precision computations by using a high-dimension map with cascading and mixing the orbit samples.
(4) The proposed algorithm provides various advantages such as the large key space and a complex dynamic of the generated binary sequence. Moreover, the PRNG sequences are verified with two famous statistical packages (NIST, and DIEHARD tests) using several sequences up to 8 million bits, to demonstrate that the proposed system is highly secure and can provide good statistical characteristics.

The rest of the paper is organized as the follows. We introduce the nonlinear dynamic “Chen” in Section 2. The overall architecture of the proposed algorithm is presented in Section 3. The experimental results and the security performance are well discussed in Section 4. Finally, the conclusion is presented in the last section.

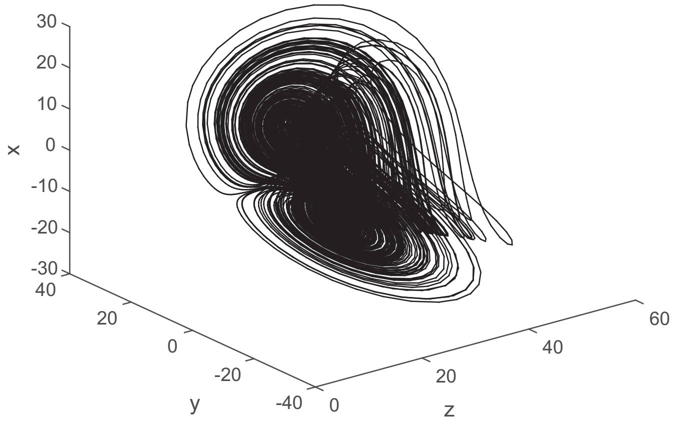

Fig. 1. Chaotic behavior of Chen’s system.

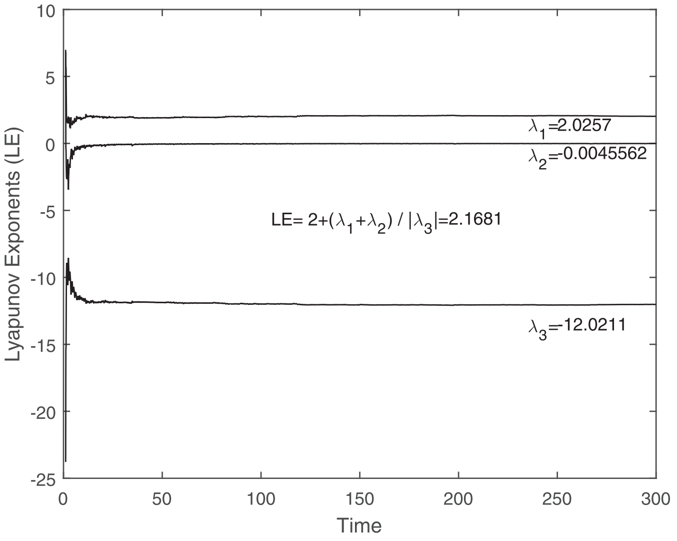

Fig. 2. Lyapunov exponents of Chen’s chaotic system.

2. Chen chaotic system

Chen chaotic system was introduced by Chen [40] with an extension of the three-dimensional orbit. This map is also called Lorenz-like systems, which means it is similar as the chaotic system Lorenz [9,41]. In recent years, these systems have been well studied and applied in several areas [9,21,33].

The complex dynamical behaviors of Chen chaotic system can be elaborated in Fig. 1. Chen’s chaotic system can be represented mathematically by the following equations:

$$\begin{cases} \dot{x} = ay - ax \\ \dot{y} = cx - ax + cy - xz \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

where x, y and z are the samples of this system while a, b, and c are the control parameters.

Fig. 2 shows dynamics of Lyapunov exponents of system chaotic Chen. The Lyapunov exponents of system (1) are found to be $\lambda_1 = 2.02,\ \lambda_2 = -0.004\ ,\ \lambda_3 = -12.02$. The fractal dimension of Chen chaotic system is 2.1681, which is large and not the most widely used compared to the rest of chaotic systems.

Figs. 3, 4, and 5 show the forms of the distributions for the orbits (x, y, z) sequentially using different seeds (initial values). The