Microelectronic Engineering xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Microelectronic Engineering

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

Digital noise produced by a non discretized tent chaotic map

L. Palacios-Luengas [a], G. Delgado-Gutiérrez [a], M. Cruz-Irisson [a], J.L. Del-Rio-Correa [b], R. Vázquez-Medina [a,*]

[a] Instituto Politécnico Nacional, ESIME-Culhuacan, Santa Ana 1000, 04430 D.F., Mexico
[b] Universidad Autónoma Metropolitana Iztapalapa, San Rafael Atlixco 186, 09340 D.F., Mexico

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Inverted tent chaotic map
Pseudorandom noise generator
Chaotic noise generator
Binary sequences uniformly distributed

ABSTRACT

This paper shows a digital electronic system that produces uniformly distributed binary sequences using the inverted tent chaotic map (*ITCM*) without the scaling and discretization processes. The proposed system has been developed considering a numerical representation of floating point with a 64-bit precision format according to the standard IEEE-754. The proposed system has four important advantages: (i) the produced binary sequences are uniformly distributed and they satisfy 10 randomness tests defined in the NIST 800-22SP guide, (ii) the statistical behavior of the *ITCM* is not affected by the scaling and discretization processes; therefore, the chaotic map used is not modified, (iii) the statistical behavior of the *ITCM* does not have stability islands inside the chaotic region, although its control parameter is changed, as it occurs with the logistic chaotic map and (iv) the statistical behavior of the binary sequences is conducted by the control parameter and the skeleton of the bifurcation diagram of the *ITCM*, which can be considered as the security keys of the system.

1. Introduction

A pseudorandom noise generator (PRNG) can be implemented in hardware or software in order to generate analog or digital signals. These noise generators can be used in different applications and areas [1,2]. In the case of cryptographic systems, it is desirable to produce digital signals with apparently uniform statistical distributions, which have the largest period possible, and must satisfy the randomness tests proposed by the NIST 800-22SP guide [3]. The digital noise generation produces a great interest to investigate mathematical models that generate unpredictable and aperiodic signals whose statistical distribution can be similar to a uniform distribution. Some reported works related with the design of *PRNG* can be revised in [4–5]. The different alternatives to produce digital noise for cryptographic applications can be divided mainly into five types, and they are based on: (a) Linear Congruential [6], (b) Linear Feedback Shift Register [7], (c) cryptosystems [8] and cryptographic primitive functions [9,10], (d) combinations relatively complex of the above alternatives, and (e) chaotic maps [11–14].

In this paper, the used alternative to produce digital noise is based on chaotic maps. In particular, the inverted tent chaotic map (*ITCM*), described in Section 2 has been used in the structure of a generator of pseudorandom binary sequences (*PBS*). The *ITCM* is a function that produces real numbers sequences, which must be converted into binary sequences using some specific strategy. Particularly in this case, the used strategy does not consider the scaling and discretization processes over the chaotic map, because these processes allow generating binary sequences through a non chaotic function, which is an approximation to the chaotic function. This approximation will be good or bad according with the discretization level. In this work, the scaling and discretization processes are avoided in order to conserve the statistical properties of the generated sequences, which, once they are generated with the desired statistical distribution function are converted into a binary format. Thus, the proposed system is considered an improvement regarding traditional techniques because it avoids the scaling and discretization processes.

The strategy used to convert real numbers into binary numbers consists in defining a statistical partition which resolution depends on the number of bits used to convert each real number. This strategy is described in Section 3. In this paper the *ITCM* is used because it does not have stability islands as it occurs with the logistic chaotic map, therefore, when the chaotic region is reached the *ITCM* produces pseudorandom number sequences even when the control parameter changes. Section 4 shows the hardware implementation of the PBS generator. Finally, in Section 5, the statistical features of the binary sequences produced by the proposed system are evaluated using the randomness tests described in the NIST 800-22SP guide [3].

2. Tent chaotic map

There are several 1-D chaotic maps such as the logistic map [11], tent map [12], sine map [13], and Bernoulli map [14], which can be used to produce binary sequences. These maps are chaotic

* Corresponding author. Tel./fax: +52 55 5656 2058.
E-mail address: ruvazquez@ipn.mx (R. Vázquez-Medina).

0167-9317/$ - see front matter © 2013 Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.mee.2013.03.127

dynamic systems (*CDS*) that can be built with iterated functions. A typical 1-D chaotic map is the tent map, which is the kind of piecewise linear chaotic maps that has been extensively studied and used since it has great mathematical simplicity [15]. The classical iterated function governing this CDS is,

$$x_{n+1} = f(\mu, x_n) = \begin{cases} 2\mu\, x_n + \left(\frac{1-\mu}{2}\right) & , a \leqslant x_n \leqslant \frac{1}{2} \\ -2\mu\, (x_n - 1) + \left(\frac{1-\mu}{2}\right) & , \frac{1}{2} < x_n \leqslant b \end{cases}, \quad (1)$$

where x_n and x_{n+1} are the current and next values in the produced real numbers sequence; μ is the control parameter and x_0 is the initial condition, both are chosen arbitrarily but known and defined in the interval $[a, b]$ in R.

There are different variants of the tent chaotic map, some of these can be found in [16,17]. In particular, in this paper the variant used has been inspired in the research work of Nejati et al. [12]. In this work, the used alternative is named the inverted tent chaotic map (*ITCM*), which is a variant of the typical tent chaotic map and is described by Eq. 2 (see Fig. 1a),

$$x_{n+1} = \tau(\mu, x_n) = \tau^n(\mu, x_0) = \mu\left(2\left|x_n - \frac{1}{2}\right|\right) + \left(\frac{1-\mu}{2}\right). \quad (2)$$

where $\tau\,(\mu, x_n)$: $(0, 1) \rightarrow (0, 1)$ considering that n represent the iteration step, x_0 is the initial condition, x_n is the real number produced by the *ITCM* at the iteration n, $\mu \in (0, 1)$ in R (see Fig. 1a) and $\tau^n\,(\mu, x_0)$ represents n iterations of $\tau\,(\cdot)$ applied on x_0.

According to the iterated function expressed by Eq. 2, the *ITCM* produces sequences whose behavior is dependent on the initial conditions and the control parameter. If the initial condition or the control parameter are changed, the produced sequence will be very different. This is a condition of the chaotic systems. In this context, the statistical distribution of a produced sequence by the *ITCM* can be determined by finding the frequency with which the different regions are visited. For this, the histogram of the sequence is calculated and this constitutes an approximation to the statistical distribution of the produced sequences. However, if a sequence of great length is considered, then a stationary statistical distribution can be obtained, which does not depend on the initial condition, and it only depends on the control parameter. Precisely, this is what is observed in a bifurcation diagram.

The *ITCM*, being a chaotic dynamical system, has high dependence on initial conditions. Additionally, depending on the value of μ, the *ITCM* can have two types of behavior, stable and unstable.

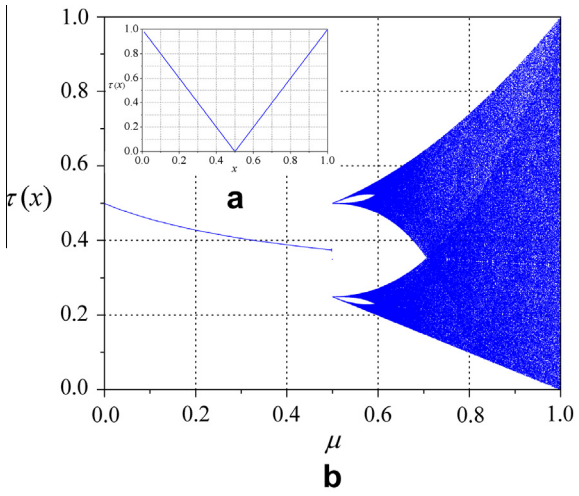

Fig. 1. (a) Graphic expression of the *ITCM* considering $x \in (0,1)$ and (b) bifurcation diagram of the *ITCM* considering $\mu \in (0,1)$.

In the stable behavior, the *ITCM* always generates the same value, which also depends on μ. In the unstable or chaotic behavior, the *ITCM* generates aperiodic numbers sequences with random appearance.

The *ITCM* has a chaotic behavior if $0.5 < \mu < 1$ and it has a stable behavior if $\mu < 0.5$. These behavior regions are shown by the bifurcation diagram in Fig. 1b. A bifurcation diagram, also named Feingenbaum's diagram, is a tool that shows the behavior of the possible sequences that can be generated by a chaotic map as a function of its control parameter and it not considers the transient of the sequences. The bifurcation diagram is a tool derived from Chaos Theory, which shows a graph that illustrates the changes in the dynamic behavior of the chaotic map, demonstrating the phenomenon by which it comes to chaos. With this tool the regions of periodic or chaotic behavior are identified for the chaotic map [18]. The bifurcation diagram represents a summary of the statistical distribution functions of the number sequences generated by chaotic map as a function of μ [19]. Now, to build a bifurcation diagram, the chaotic map is iterated considering different values of μ in (0, 1) with a defined step $\Delta\mu$. A simple procedure that explains how to build a bifurcation diagram, avoiding the transient of the generated sequence, is the following: (a) define $\mu = 0.0$, (b) randomly selects an initial condition x_0 in (0, 1) and the chaotic map must be iterated N times (e.g. $N = 1000$) to calculate the sequence $\{x_1, x_2, x_3, ..., x_N\}$, (c) The first 100 values of the sequence are discarded to ensure that the transient has been exceeded, (d) the remaining values of the sequences $\{x_{101}, x_{102}, x_{103}, ..., x_N\}$ are plotted, (e) Increase the value of μ a step $\Delta\mu$, that is, $\mu \leftarrow \mu + \Delta\mu$ and the procedure must be repeated from (*b*) until $\mu = 1.0$.

In this paper, the interest region happens when $\mu \in (0.7, 1.0)$ because for these values of μ, the *ITCM* has only one interval in which the number sequence is produced. Whenever $\mu \in (0.5, 0.7)$ there is more than one interval where the produced sequence is concentrated (see Fig. 1b). Real number sequences with a good statistical distribution function can be produced by Eq. 2. If $\mu \rightarrow 1$, then the expected statistical distribution function of the produced number sequences will be very close to a uniform distribution function. Considering that the *ITCM* is a chaotic system and consequently it has high dependence on initial conditions, then the produced sequences will be different if the used initial condition is changed, but its statistical distribution function is the same at long term.

A digital implementation of the *ITCM* is possible, several authors have proposed schemes that include the scaling and discretization processes over chaotic maps defined in the real numbers set, R, and the result of these processes is a new map defined in the natural numbers set, N, which is a non chaotic function [20,21]. That alternative produces binary sequences, which do not have a statistical behavior that is congruent with the one of the original chaotic map, since the rounding of numbers produced by the discretization process induces an error. The error is propagated and increased when the new map is iterated, and then the statistical behavior of the resulting sequence of real numbers is strongly affected [22]. The proposed system overcomes this problem.

3. Proposed system

The proposed system is a hardware electronic device that generates digital noise sequences using the *ITCM*. These sequences are transmitted to a PC using the USB port, and for this process the next aspects need to be considered: (a) a secret key k_μ, which is formed by the concatenation of the control parameter μ and the initial condition x_0, (b) L_B, the length of the binary sequence that will be produced, and (c) S_c, the starting command in its binary format (0111001). k_μ has a length of 128 bits conformed by 16 blocks of 8 bits each one, L_B has a variable length that can take