A Realizable Modified Tent Map for True Random Number Generation

Hamid Nejati, Ahmad Beirami, and Yehia Massoud

Electrical and Computer Engineering Department, Rice University, Houston TX 77005

(massoud@rice.edu)

Abstract—Tent map is a discrete-time piecewise-affine I/O characteristic curve, which is used for chaos-based applications, such as true random number generation. However, tent map suffers from the inability to maintain the output state confined to the input range under noise and process variations. In this paper, we propose a modified tent map, which is interchangeable with the tent map for practical applications. In the proposed modified tent map, the confinement problem is solved while maintaining the functionality of the tent map. We also demonstrate simulation results for the circuit implementation of the presented modified tent map for true random number generation.

I. INTRODUCTION

Certain nonlinear dynamical systems can demonstrate non-periodic, long-term non-predictive behaviors, known as chaos. Chaotic behavior results from the high sensitivity of the system to the initial state, which is never exactly known in practice. Any small perturbation can grow exponentially with time within the system leading to a non-predictive behavior of chaotic systems [1], [2]. Chaotic waveforms have been extensively used in various research areas such as the modeling of the behavior of human organs [3]–[5] as well as the modulation of signals and chaotic encryption of telecommunication data [1]. Truly Random Number Generators (TRNG) can be utilized in cryptographic systems. A TRNG is a number generator that is capable of producing uncorrelated and unbiased binary digits through a nondeterministic and irreproducible process [7]. A TRNG requires a high entropy source, which can be provided by uncertain chaotic sources [7].

A discrete-time chaotic map, formed by the iteration of the output value in a transformation function, can be used for the generation of random numbers. Simple piecewise affine input-output (I/O) characteristics have been extensively used for the generation of random bits, e.g., the Bernoulli map [7], and the tent map [8]. The entropy source of a chaotic map is the inherent noise of the system, which is amplified in the positive gain feedback loop by the iteration of the output signal in the map function [7]. High Speed, capability of integration, and the high quality of the generated bits make the discrete-time chaotic maps very good candidates for high speed embeddable random number generation.

The practical application of both the tent map and the Bernoulli map can be hindered by noise and implementation errors, where they are unable to maintain the state of the system confined [7]. In this paper, we present a modified tent map that can be interchanged with the tent map in practical applications.

The rest of this paper is organized as follows. In Section II, the fundamentals of discrete-time chaotic maps are reviewed, and the practical problems of the tent map are pointed out. In Section III, we present the modified tent map and investigate its chaotic characteristics. In Section IV, we demonstrate the feasibility of implementing the presented modified tent map for true random number generation. Section V concludes the paper.

II. TENT MAP: FUNDAMENTALS AND HISTORY

In this section, after a brief introduction to discrete-time chaotic maps, we review the tent map and the previously proposed implementations. Discrete-Time Markov chaotic sources are a subclass of discrete-time chaotic nonlinear dynamical systems. A discrete-time chaotic system is formed by the iteration of the output signal through a transformation function $M(x)$ as given by

$$x_{n+1} = M(x_n) = M^n(x_0). \tag{1}$$

In this equation, n represents the time step, x_0 is the initial state of the system, and x_n is the state of the system at time step n.

The tent map function $M(x) : (0,1) \rightarrow (0,1)$, shown in Figure 1 (a), is given by

$$M(x) = \begin{cases} 2x & 0 < x \leq \frac{1}{2}, \\ 2(1-x) & \frac{1}{2} < x < 1. \end{cases} \tag{2}$$
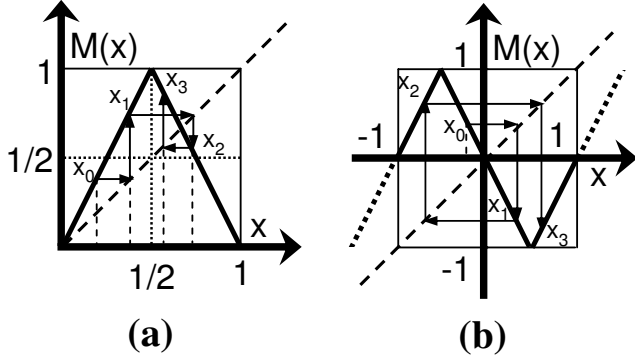
Fig. 1. (a) The tent map. (b) The presented modified tent map.

It can be shown that after several iterations, the density of states in the tent map asymptotically follows a uniform distribution, i.e., the state of the system is uniformly distributed in $(0, 1)$ and the asymptotic density distribution $f(x)$ for the tent map satisfies $f(x) = 1$ [9].

The Lyapunov exponent of a discrete-time map can be calculated from [2]

$$\lambda = \int \ln |M'(x)| f(x) dx, \qquad (3)$$

where $M'(x)$ is the derivative of the map function $M(x)$ and $f(x)$ is the asymptotic density distribution. A positive Lyapunov exponent implies the chaotic behavior in the system. The rate of the separation between the trajectories of very close initial states is given by λ. For tent map, $|M'(x)| = 2$ and $f(x) = 1$, which result in $\lambda = \ln 2$.

Tent map circuit implementation has been proposed in [8], [10]. These circuit implementations suffer from the confinement problem in practice, i.e., the output value of the map can be trapped in a point outside the map due to noise or implementation errors [7], [11]. A tailed tent map has been presented in [11] to solve the problem. The tailed tent map maintains the uniform asymptotic density distribution of the states, while not disturbing characteristics of the tent map. For example, the utilization of the tailed tent map for true random number generation results in the generation of correlated output binary sequence. In [12], a hardware implementation has been proposed for the tent map based on reducing the slope, which will change the characteristics of the map and degrade the quality of the generated binary sequence in terms of the statistical characteristics.
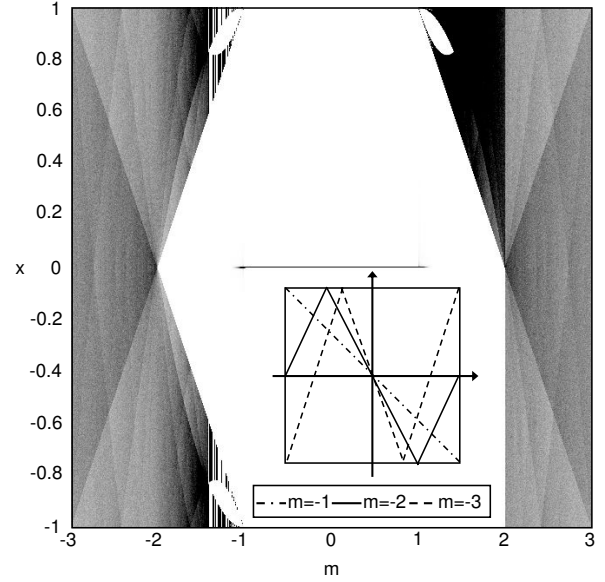

Fig. 2. Bifurcation diagram of the modified tent map with bifurcation parameter m, defined in (5). The generalized modified tent map with three different values of m (-1, -2, and -3) is shown in the inset.

III. THE PRESENTED MODIFIED TENT MAP

In this section, we present the modified tent map and investigate its chaotic behavior. The presented modified tent map function $M(x) : (-1, 1) \rightarrow (-1, 1)$, shown in Figure 1 (b), is given by

$$M(x) = \begin{cases} 2x + 1 & -1 < x \leq -\frac{1}{2}, \\ -2x & -\frac{1}{2} < x < \frac{1}{2}, \\ 2x - 1 & \frac{1}{2} \leq x < 1. \end{cases} \qquad (4)$$

In the modified tent map, the sign of the output value alternates in each iteration, i.e, $x_n x_{n+1} < 0$. Suppose x_1^a, x_2^a, and x_3^a are the abscissa of three successive output values of the tent map, and x_1^b, x_2^b, and x_3^b are the output values of the modified tent map. If $x_1^a = x_1^b$, we have $x_2^a = -x_2^b$ and $x_3^a = x_3^b$, as shown in Figure 1 (a,b). In other words, for an equal initial state, the absolute value of the output sequence is equal for both the tent map and the modified tent map while the output of the modified tent map alternates between positive and negative values. Since the output values of the tent map and the modified tent map have equal absolute values, the Lyapunov exponent of the modified tent map is equal to that of the tent map, which was shown to be $\ln 2$.

In order to further investigate the presented modified tent map, we generalize the map function by introducing

a slope parameter m, where $m \in (-3, 3)$, as given by

$$M(x) = \begin{cases} -m(x + \frac{2}{|m|}) & -1 < x \leq -\frac{1}{|m|}, \\ mx & -\frac{1}{|m|} < x < \frac{1}{|m|}, \\ -m(x - \frac{2}{|m|}) & \frac{1}{|m|} \leq x < 1. \end{cases} \quad (5)$$

Here, $m = -2$ represents the modified tent map, as given by equation (4). Figure 2 shows the bifurcation diagram of the generalized map function as a function of the bifurcation parameter m. A bifurcation diagram is obtained by following the output trajectory to find the possible long-term states of the system. Under certain conditions, the bifurcation diagram can also represent the density of the states due to the ergodicity [9], [15]. In this diagram, the density of the states is proportional to the darkness, i.e. darker regions have higher density of states. This diagram is obtained assuming that the inherent initial noise is a very small positive value, i.e., $x_0 = 0^+$.

For $|m| > 3$, the system could not maintain the state in the input range, which could not be used for chaotic applications. For $2 < m < 3$, the system is chaotic and the bifurcation diagram represents the steady state density distributions. Chaotic behavior can also be observed for $1 < m \leq 2$. Since the initial state of the system is assumed to be positive, the output is confined in positive values. For $|m| \leq 1$, the system does not demonstrate chaotic behavior. Regardless of the initial state of the system, the output will ultimately settle in zero. For $-2 \leq m < -1$, the system also shows chaotic behavior. In this mode, the output alternates between positive and negative values with each iteration. In this region, the system does not have an asymptotic density distribution. For $-3 < m < -2$, the system is chaotic and the bifurcation diagram represents its asymptotic density distribution.

For $m = 2$, equation (5) represents a map that is given by

$$M(x) = \begin{cases} -2x - 1 & -1 < x \leq -\frac{1}{2}, \\ 2x & -\frac{1}{2} < x < \frac{1}{2}, \\ -2x + 1 & \frac{1}{2} \leq x < 1. \end{cases} \quad (6)$$

As the equation shows, this is exactly like the tent map for $x > 0$. Here, if m is a little bit greater than 2, the system could still maintain the state confined in the system since the output could jump to the negative side of the map, which is the fundamental difference between this map and the tent map. In the tent map, if the slope is more than 2, the system could not maintain the state confined. Therefore, the tent map could not be used for practical applications under process variations and noise.

Although in the neighborhood of $m = -2$, the asymptotic density distribution does not exist, the modified tent map could be used in practical applications such as true random number generation based on the principles explained earlier.

IV. IMPLEMENTATION AND DISCUSSIONS

In this section, we propose the utilization of a current mode circuit implementation for the presented modified tent map. In current mode circuits, the signal is represented by the branch current instead of the node voltage in the voltage mode circuits. Current mode circuits have recently attracted great attention because of their capability of very low supply voltage operation [13]. While scaling the feature size, the supply voltage is scaled more rapidly than the threshold voltage, which in turn decreases the overdrive voltage of the transistors and limits the voltage swing. In current mode circuits, high current gains can be achieved while the nodal voltages are floating [13], [14]. Current mode circuits will be playing an important role in the future deep submicron technologies, e.g., telecommunications, analog signal processing, and multiprocessors [13].

The presented modified tent map is a *continuous* piecewise affine map, where we implemented it by the affine interpolation of the value at the breakpoints, proposed in [15]. In this method, the affine partitions are implemented using elementary blocks based on the detection of the breakpoints. Therefore, it is straightforward to detect whether the output value is within a certain affine partition of the map, and generate a binary output sequence. We performed HSPICE simulations in TSMC 0.18 μm technology for the modified tent map circuit. The I/O characteristic curve of the map is shown in Figure 3(a), where the input and output range are equal to $6\mu A$. Investigating the transient response of the circuit with an input current pulse, we demonstrated that at the worst case the output would settle within 1% of its final value in less than 25 ns. Therefore, the circuit could be utilized at operation frequencies as high as 20 MHz.

We demonstrate the feasibility of binary generation from the presented modified tent map. In Figure 4(a), the partition $|x| < 1/2$ is represented by state A, and the partitions $-1 < x < -1/2$ and $1/2 < x < 1$ are represented by the states B_1 and B_2, respectively. In order to generate a binary output, the states B_1 and B_2 are combined in a macro-state B. The state A corresponds to the bit 1 and the state B corresponds to the bit 0. As discussed earlier, the binary sequence generated from a modified tent map is exactly the same as the binary sequence
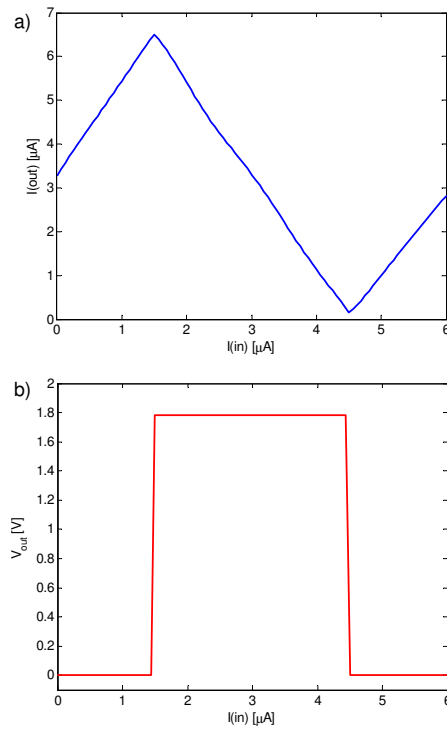
Fig. 3. (a) The I/O current characteristics of the modified tent map. (b) Output bit-generation pattern.

Fig. 4. (a) The modified tent map and the corresponding affine partitions (b) The Markov chain of states for true random number generation.

generated from a tent map due to the symmetry of the bit-generation process around the origin. Therefore, the bit-generation process can be modeled as a Markov chain similar to the tent map, as shown in Figure 4(b) [7]. In this Figure, p is the probability of the generation of 1 when the latest generated bit is 1. q is the probability of the generation of a 0, when the previous bits is 0. Since the functionality of the map is similar to the tent map, we have $p = q = 1/2$ and the generated bits are truly random. In Figure 3(b), the simulation result for the bit-generation circuit is presented, where it demonstrates very good agreement with the desired bit-generation pattern.

V. CONCLUSION

The tent map suffers from the inability to maintain the state confined in the input range of the map under noise and implementation errors. This fundamental issue limits the practical application of the tent map. In this paper, we presented a modified tent map, which can solve the state confinement problem of the tent map. The presented modified tent map could be used in all practical applications instead of the tent map. We demonstrated that the presented map could be used for true random number generation.
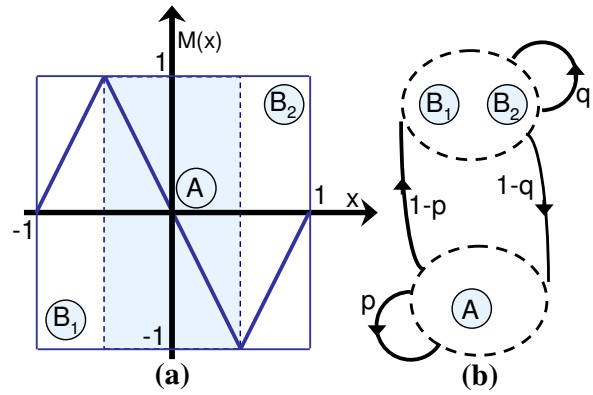
REFERENCES

[1] P. Stavroulakis, *Chaos Applications in Telecommunications.* CRC Press, 2006.
[2] E. Ott, *Chaos in dynamical systems.* Cambridge university press, 2002.
[3] K. Kaneko and I. Tsuda, *Complex systems: chaos and beyond: A constructive approach with applications in life science.* Springer, 2001.
[4] I. Tsuda, "toward an interpretation of dynamic neural activity in terms of chaotic dynamical systems," *Behav. Brain Sci.*, vol. 24, pp. 793–810, 2001.
[5] G. Chen and T. Ueta, *Chaos in circuits and systems.* World scientific publishing Co., 2002.
[6] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.* CRC Press Series on Discrete Mathematics and Its Applications, 1997.
[7] S. Callegari, R. Rovatti, and G. Setti, "Embeddable adc-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos," *IEEE Trans. Signal Processing*, vol. 53, no. 2, pp. 793–805, February 2005.
[8] J. Bean and P. J. Langlois, "A Current Mode Analog Circuit for Tent Maps Using Piecewise Linear Functions," in *IEEE ISCAS*, 1994, pp. 125–128.
[9] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise: Stochastic Aspects of Dynamics.* Springer-Verlag, 1994.
[10] T. Morie, S. Sakabayashi, M. Nagata, and A. Iwata, "Cmos circuits generating arbitrary chaos by using pulsewidth modulation techniques," *IEEE Trans. Circuits Syst. I*, vol. 47, no. 11, pp. 1652–1657, November 2000.
[11] S. Callegari, G. Setti, and P. J. Langlois, "A CMOS Tailed Tent Map for the Generation of Uniformly Distributed Chaotic Sequences," in *IEEE ISCAS*, 1997, pp. 781–784.
[12] S. Callegari, R. Rovatti, and G. Setti, "First direct implementation of a true random source on programmable hardware," *Int. J. Circuit Theory Apllicat.*, vol. 33, no. 1, pp. 1–16, January 2005.
[13] F. Yuan, *CMOS current-mode circuits for data communications.* Springer, 2007.
[14] G. Roberts and A. Sedra, "All current-mode frequency selective circuits," *Electron. Lett.*, vol. 25, pp. 759–761, 1989.
[15] R. Rovatti, N. Manaresi, G. Setti, and E. Franchi, "A current-mode circuit implementing chaotic continuous piecewise-affine markov maps," *International Conference on Microelectronics for Neural, Fuzzy and Bio-Inspired Systems*, pp. 275–282, 1999.