Combined logistic and tent map

Marcin Lawnik
Silesian University of Technology, Faculty of Applied Mathematics, Kaszubska 23, 44-100
Gliwice, Poland
E-mail: marcin.lawnik@polsl.pl

Abstract. In this paper the combination of logistic and tent map is discussed. Some basic properties of the new dynamical system like Lyapunov exponent and density of the iterated variable are analyzed. Furthermore, applications of the discussed model in chaos based cryptography are presented.

1. Introduction
Chaotic maps constitute the backgrounds for chaos based cryptography due to the fact that chaotic transformations are sensitive to changes in the initial conditions and generate solutions similar to random ones. Such approach to data securing means that the parameter values and the initial conditions values are used as the secret keys.

One of the measures determining if the transformation in the form of

\[ x_{k+1} = f(x_k) \] (1)

generates a chaotic solution is the Lyapunov exponent expressed as

\[ \lambda = \lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln |f'(x_i)|. \] (2)

Its positive value is a necessary condition for a chaotic solution, otherwise, the solution is stable.

However, relaying only on chaotic property of the solution does not suffice safe data encryption. The distribution of the iterative valuable, i.e. its invariant density, is also very important, and, as such, may be derived from Frobenius-Perron equation given as [1]

\[ \rho(x) = \sum_{i=1}^{k} \frac{\rho(y_i)}{|f'(y_i)|}, \] (3)

where \( y_i \) is the \( i \)-th inverse image of point \( x \) (\( \forall i = 1, 2, \ldots, k, \ f(y_i) = x \)). Equation (3) is hard to solve, so the invariant density of (1) can be analytically determined only in very few cases.

Transformations used for data encryption are extensively discussed in professional publications, where two most commonly examined solutions are logistic and tent map. The logistic map is described by the following expression:

\[ x_{k+1} = ax_k(1 - x_k), \] (4)
where \( a \in [0, 4] \) and \( x \in [0, 1] \). The chaotic solutions generated from the above transformation are in the range of \([3.57, 4]\) with the exclusion of the so called periodic windows, where Lyapunov exponent of the map is negative. However, the function does not render solutions from the uniform distribution. The density of (4) for values of \( a \) that generate chaotic solutions can only be determined for \( a = 4 \) [2]

\[
\rho(x) = \frac{1}{\pi \sqrt{x(1-x)}}. \tag{5}
\]

The tent map is described by the following expression

\[
x_{k+1} = \begin{cases} 
    \frac{x_k}{p}, & 0 < x_k \leq p \\
    \frac{1-p}{1-p} x_k, & p < x_k < 1
\end{cases}, \tag{6}
\]

where \( p \in (0, 1) \). For each value of \( p \) transformation (6) is chaotic and its invariable density is equal to 1. Its Lyapunov exponent is given by [3]

\[
\lambda = -p \ln p - (1-p) \ln(1-p). \tag{7}
\]

By comprising the properties of the logistic and tent map from the point of view of cryptography, the following conclusions are drawn:

- (4) generates non-uniform distribution values;
- (4) has a too narrow range in which the transformation generates chaotic solution;
- (4) and (6) have unstable and small value of Lyapunov exponent.

Because in professional publications the above-mentioned properties of the chaotic transformations are considered as unsuitable for data securing, it is essential to find a chaotic transformation that can provide better properties [4, 5].

In this paper a combined logistic and tent map is presented. Furthermore its properties are discussed, especially in term of chaos based cryptography.

2. Model

The combined logistic and tent map is in the form

\[
x_{k+1} = \begin{cases} 
    \frac{x_k}{p}, & 0 \leq x_k < p \\
    \frac{x_k - T}{p - T}, & p \leq x_k \leq T \\
    a \frac{x_k - T}{1 - T} \left( 1 - \frac{x_k - T}{1 - T} \right), & T \leq x_k \leq 1
\end{cases}, \tag{8}
\]

where \( p, T \) and \( a \) are parameters that fulfill \( p \leq T \), \( T \in [0, 1] \) and \( a \in [0, 4] \). An exemplary transformation of (8) is presented in Fig. 1.

If \( T = 0 \), (8) becomes the logistic map given by expression (4); whereas, if \( T = 1 \), (8) becomes the tent map in the form of (6).

3. Analysis

The analysis of transformation (8) is divided into two parts: the analysis of Lyapunov exponent and the analysis of the density of the iterated variable. Both parts contain references to possible applications in chaotic cryptography.
3.1. Lyapunov exponent

The Lyapunov exponent of (8) for a given value of parameter $p$ is plotted in Fig. 2. The graph indicates that for a wide range of the examined parameters, the value of the Lyapunov exponent is positive, which is very advantageous for chaotic cryptography. Furthermore, the part of the graph for values of the parameter $a$ close to 4 and for values of $T$ close to 1 is very appealing. Exemplary values of Lyapunov exponent for those parameter values are presented in Fig. 3.

3.2. Density of the iterated variable

The density of transformation (8) similarly to logistic map (4) is difficult to determine by means of analytical determinations. Numerical analyses rendered several interesting cases—see Fig. 4. The two upper graphs present the density for $a = 2$ with $p = 0.15$, $T = 0.3$ and, respectively, for $p = 0.25$, $T = 0.5$. As indicated, starting with a certain value of $x$ the density stabilizes and is close (for $x > 0.5$) to uniform distribution. The second case, where the left part of the density for $x < 0.5$ is of special interest, as it is similar to the graph of density (5). Likewise, the same structure of the density is preserved in the course of adjusting the values of parameter $p$.

The lower part of the graph is derived for $a = 4$ with $p = 0.05$, $T = 0.1$, and, respectively, $p = 0.45$, $T = 0.9$. The two cases give the image of the transfer of the density of (5) with $T = 0$.
Figure 3. Lyapunov exponent of (8) for the value of parameter $a$ close to 4 (two upper graphs) and for $T$ close to 1 (lower graphs).

Figure 4. The chaotic transformation (in blue) and its density (in black) for selected values of $p$, $a$ and $T$.

to a uniform distribution for $T = 1$. A similar result is derived while adjusting the values of parameter $p$.

Due to their uniform distribution, the two cases discussed above may be considered as sets of values of parameters of (8) suitable for encryption.

4. Conclusions
A new chaotic dynamical system that generalizes the logistic and tent map is discussed in the paper. In the next step, Lyapunov exponent and the density of the iterated variable are analyzed. The results confirm the usability of the proposed model for cryptography based on the theory of chaos.

References
[1] Bohr T and Tél T 1988 The Thermodynamics of Fractals Directions in Chaos Volume 2 ed Hao Bai-Lin (Singapore: World Scientific) pp 194-237
[2] Boyarsky A and Gra P 1997 Laws of Chaos Invariant Measures and Dynamical Systems in One Dimension (New York: Springer Science+Business Media)

[3] Anikin V M, Arkadaksky S S, Kuptsov S N, Remizov A S and Vasilenko L P 2008 Lyapunov exponent for chaotic 1D maps with uniform invariant distribution Bulletin of the Russian Academy of Sciences: Physics 72 (12), 1684-1688

[4] Arroyo D, Amigo-Garcia J M, Li S and Alvarez G 2010 On the inadequacy of unimodal maps for cryptographic applications (RECSI Tarragona Spain ISBN 9788469333044)

[5] Lawnik M 2017 Generalized logistic map and its application in chaos based cryptography Journal of Physics: Conference Series 936 012017