Generalized logistic map and its application in chaos based cryptography

Generalized logistic map and its application in chaos based cryptography

M Lawnik
Faculty of Applied Mathematics, Silesian University of Technology, ul. Kaszubska 23, 44-100 Gliwice, Poland

E-Mail: marcin.lawnik@polsl.pl

Abstract. The logistic map is commonly used in, for example, chaos based cryptography. However, its properties do not render a safe construction of encryption algorithms. Thus, the scope of the paper is a proposal of generalization of the logistic map by means of a well-recognized family of chaotic maps. In the next step, an analysis of Lyapunov exponent and the distribution of the iterative variable are studied. The obtained results confirm that the analyzed model can safely and effectively replace a classic logistic map for applications involving chaotic cryptography.

1. Introduction

Chaotic maps are widely used in many science branches, e.g. [1-4]. One of the most commonly used chaotic dynamical system in practice is the logistic map (LM) given by the following expression:

$$x_{k+1} = 4qx_k(1-x_k), \tag{1}$$

where $q \in [0,1]$ and $x \in [0,1]$. Its universal nature is certified by many applications, among others, in cryptography based on chaos theory, e.g. [5,6]. Chaos based cryptography regards chaotic maps as generators of pseudo-random numbers, and the values of their initial conditions and parameters as the secret keys. From such point of view, recurrence (1) has many disadvantages, which were indicated in professional publications [7]. They include, among others, a small space of allowable values of parameter q, not uniform distribution of the iterative variable, or unstable value of Lyapunov exponent. The Lyapunov exponent denotes the sensitivity of dynamical system $x_{k+1} = f(x_k)$ to changes in the initial conditions and is calculated in accordance with the dependence:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} \ln\left|f'(x_k)\right|. \tag{2}$$

In the above-mentioned applications, it is definitely recommended that the values of parameter q of (1) are close to 1. This results from its distribution, which for such set of values is flat in the middle, and determined by the density function:

$$\rho(x) = \frac{1}{\pi\sqrt{x(1-x)}} \tag{3}$$

Furthermore, for $q = 1$ the Lyapunov exponent for (1) reaches the maximum value equal to $\lambda = \ln 2$ among all allowable values of parameter q. The above results show that the admissible values of parameter q are considerably limited. This has a negative impact on the safety of algorithms and may

lead to successful brutal attack. In view of this, the designation of a chaotic map that could combine the simplicity of (1) and , at the same time, render much better properties, seems relevant.

In [8] the following family of chaotic functions was presented:

$$x_{k+1}=\begin{cases} q\left(1-\left|\dfrac{p-x_k}{p}\right|^r\right), & 0<x<p \\ q\left(1-\left|\dfrac{p-x_k}{1-p}\right|^r\right), & p\le x<1 \end{cases}, \tag{4}$$

where p,q,r represents parameters.

If $p=0.5$, $r=2$ and $q\in[0,1]$, map (4) may be reduced to LM (1). Thus, LM is a special case of (4). In [8] only for selected values of parameters p,q and r an casual analysis of Lyapunov exponent of (4) was presented, indicating the domains for which it has a positive value. From the point of view of above mentioned applications, such analysis is insufficient.

2. The generalized logistic map

The generalized logistic map (GLM) can be given by the formula:

$$x_{k+1}=\begin{cases} \dfrac{-q}{p^2}(p-x_k)^2+q, & 0\le x_k\le p \\ \dfrac{-q}{(1-p)^2}(p-x_k)^2+q, & p<x_k\le 1 \end{cases}, \tag{5}$$

where $p\in(0,1)$ and $q\in[0,1]$.

GLM (5) is a specific case of (4) for the parameter value $r=2$.

3. Analysis

In figure1, the graph of Lyapunov exponent for the values of parameters p and q is presented. As shown in the graph, a large range of the domain $[0.89,1]\times[0,1]$ has a positive value of Lyapunov exponent. Furthermore, it may be reasoned that for the value of parameter q close to 1 and the entire variation range of parameter p, the GLM (5) has a positive Lyapunov exponent, as shown in detail in figure 2. Accordingly, the analysis of Lyapunov exponent for this map renders a considerably wider range of the allowable values in comparison with a LM (1).

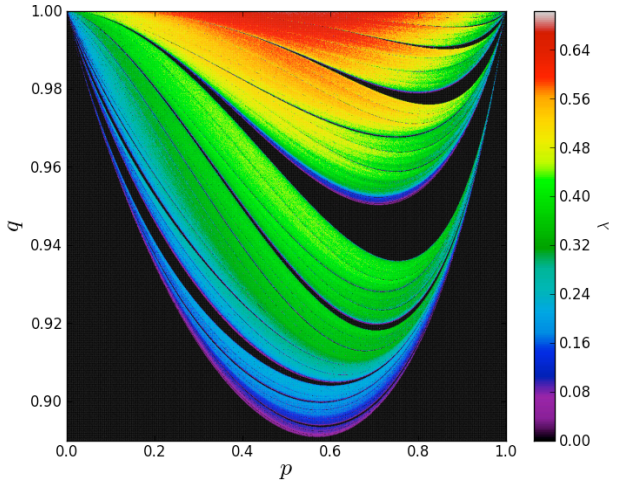

Figure 1. Graph of the Lyapunov exponent of GLM (5). The non-positive value of the exponent is marked in black.

As indicated in figure 2 the value of Lyapunov exponent is stable for parameter q close to 1. This means that Lyapunov time, which determines the number of iterations that the system requires to forget the initial condition, is also stable. In applications, Lyapunov time determines how many initial iterations of the system must be rejected, in order to obtain a chaotic solution, which has also an impact on the calculations effectiveness of the algorithms involving cryptography.

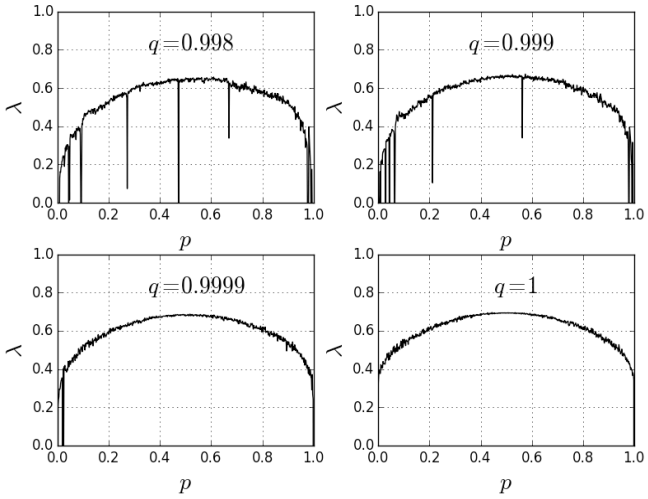

Figure 2. The graph of the Lyapunov exponent of the GLM (5) for values of parameter q close to 1.

The distribution of the iterative variable for the value of parameter q close to 1 is flat in the middle (figure 3), just as in a LM (1). However, in the discussed example, the distribution is the same for the entire variation of parameter p, and not only for one value. This significantly extends the range of the allowable parameters, and, at the same time, enhances the safety of the algorithm - see figure 4.

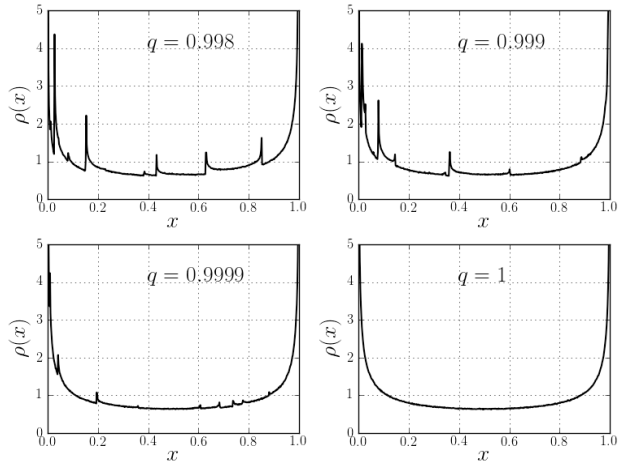

Figure 3. Distributions of the GLM (5) obtained in a numerical way for values of parameter q close to 1 and $p = 0.4$.

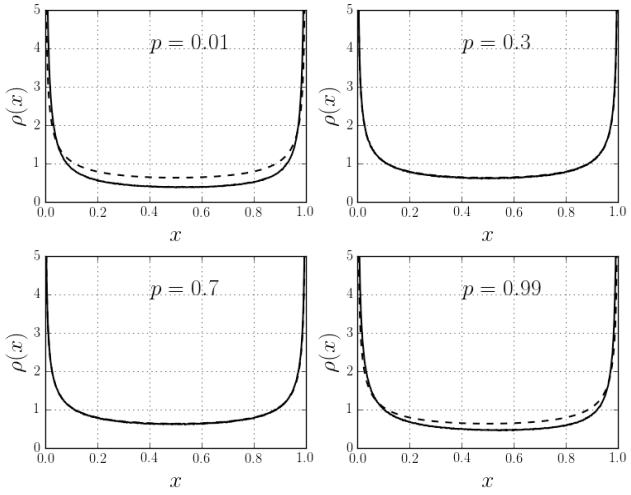

Figure 4. Distribution of GLM (5) obtained in a numerical way for set values of parameter p and $q = 1$ (continuous line). The broken line marks density function (3).

4. Conclusions

The analysis of the generalized logistic map with the use of function family (4) was conducted. The presented calculations indicated that the analyzed model has much better properties than a classic logistic map, such as wider range of the allowable parameters with a positive value of Lyapunov exponent and flat distribution of the iterative variable in the middle part. From the point of view of cryptography based on the chaos theory, the properties of the analyzed function provide its successful application. On the other hand, the analyzed model combines the simplicity of its classic correspondent. This should lead to the replacement of a logistic map by its generalized form in cryptography applications.

References

[1] Berezowski M and Lawnik M 2014 Identification of fast-changing signals by means of adaptive chaotic transformations *Nonlinear Analysis: Modelling and Control* **19(2)** 172–177
[2] Lawnik M and Berezowski M 2014 Identification of the oscillation period of chemical reactors by chaotic sampling of the conversion degree *Chem. Process Eng.* **35(3)** 387–393
[3] Lawnik M 2014 Generation of numbers with the distribution close to uniform with the use of chaotic maps *Proceedings of the 4th International Conference on Simulation and Modeling Methodologies, Technologies and Applications* pp 451–455
[4] Lawnik M 2014 The approximation of the normal distribution by means of chaotic expression *Journal of Physics: Conference Series* **490** 012072
[5] Baptista M S 1998 Cryptography with chaos *Physics Letters A* **240** 50–54
[6] Pareek N K, Vinod Patidar and Sud K K 2006 Cover image Image encryption using chaotic logistic map *Image and Vision Computing* **24(9)** 926–934
[7] Arroyo D, Alvarez G and Fernandez V 2008 *On the inadequacy of the logistic map for cryptographic applications* eds. L Hernandez A Martin X Reunin (Espa˜nola sobre Criptolog´ıa y Seguridad de la Informaci´on) pp 77–82
[8] Skrobek A 2007 *Metoda projektowania dyskretnych chaotycznych szyfrów strumieniowych oparta na kryptoanalizie* Phd thesis (in polish)