A NEW CHAOTIC BIDIMENSIONAL MAP SUITABLE FOR IMAGES ENCRYPTION

Lect. Radu Boriga, PhD student

Titu Maiorescu University, Faculty of Computer Science, Bucharest

radu.boriga@utm.ro

Abstract

Chaotic bidimensional maps have aroused a great interest mainly in the encryption of images. Some maps of this type (Baker map, Cat map, etc.) have became a standard in the area of images encryption. In this letter, we propose a new kind of chaotic map based on the equation of a plane curve called the serpentine curve. We have studied the randomness of the keystreams generated by a PRNG based on the new function, both theoretically, using theory of discrete chaotic systems, and practically, using the DIEHARD battery of tests.

Keywords: chaotic systems**,** pseudo random, cryptography, stream cipher, transcendental equations

1. Introduction

The secret transmission of the visual information is necessary in many types of applications, such as commercial, military and medical applications. In this type of applications, to prevent an unauthorized access, the encryption of type image information is required before they are transmitted through the network. Through all times, a series of encryption algorithms based on the number theory and algebraic concepts has been proposed. In the last decade, the chaos is a new paradigm which seems to be promising. Thus, the chaos theory specific to nonlinear dynamic systems has received a lot of attention from the cryptographic community. A large number of algorithms based on chaotic systems have been proposed and analyzed in order to bring into effect the encryption of the messages for hardware and software equipment ([1],[6],[7]).

The chaotic cryptography is still at early stages and does not have an exact parallelism with concepts and ideas of classic cryptography. Nevertheless, the chaotic maps and classic algorithms have common proprieties: ergodicity, the system's sensitivity to the initial conditions/ parameter's values, mixing propriety, the deterministic dynamic and the complexity of the chaotic systems. These are similar with the proprieties given by the diffusion to minor changes plain/key text, the diffusion determined by a change in the plain block, the deterministic pseudo-randomness and the complexity of the algorithm from the encryption classic systems. So, a series of image encryption algorithms based on chaotic maps have been proposed. They are: logistic map [1], standard map, Hénon map [3], the Baker map [9], the PWNLCM [1], etc.

In this article we analyze the chaotic quality of a new bi-dimensional proposed map and the statistical results of a PRNG based on it.

2. Two-dimensional chaotic maps

A *discrete n-dimensional dynamic system* is an iterative map $f: \boldsymbol{R}^n \to \boldsymbol{R}^n$ of the form $x_{k+1} = f(x_k)$, where $k \in \mathbf{N}$ shows the dynamic in time of the system and $X \in \boldsymbol{R}^n$ is a state.

The *Hénon map* could be considered a representative example for the above described system. It was created by Michel Hénon as a simplification of the Poincaré section of the Lorenz system and since then has been studied. The two-dimensional chaotic systems are given by the two equations [3]:

$$x_{n+1} = -ax_n^2 + y_n + 1$$

$$y_{n+1} = bx_n \tag{1}$$

The Hénon map is an iterated discrete-time dynamical system that exhibit chaotic behavior. The bifurcation diagram for the parameters $a = 1.4$ and $b = 0.3$ is shown in the figure 1.

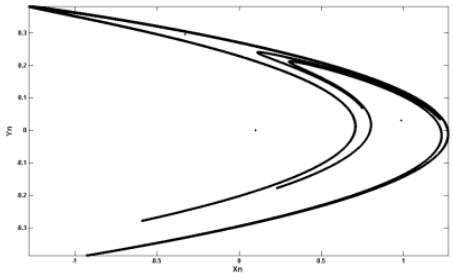

Figure 1. The Hénon attractor

In this diagram it can be observed the existence of a strange attractor, very popular, known under the name of *Hénon attractor*.

Another system that is analyzed and used in cryptographic applications is the discrete-time two-dimensional map called the *Ikeda map*, described by the following equations:

$$x_{n+1} = 1 + u(x_n cost_n - y_n sint_n)$$

$$y_{n+1} = u(x_n sint_n + y_n cost_n)\,, \tag{2}$$

where $t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2}$ and u is the parameter of the system [1].

For the value of the parameter $u = 0.92$, the discrete Ikeda map has a chaotic behavior (figure 2).

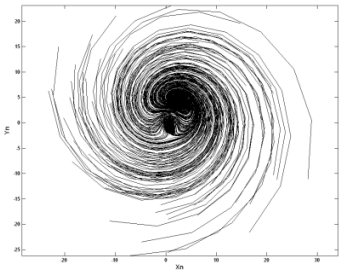

Figure 2. The Ikeda attractor

In the next chapter is presented the analysis performed using mathematically concepts from discrete dynamical nonlinear systems of the chaotic qualities for the proposed two-dimensional map which derives from the equations given by the *serpentine curve*.

3. The analysis of the new chaotic two-dimensional map

Over a period of sixteen years elliptic curve cryptography become important in several applied areas, including coding theory, pseudorandom number generation, and especially cryptography. In 1985 V. Miller and N. Koblitz proposed a completely different cryptographic use of elliptic curves constructing Diffie-Hellman type protocols using the group of points of an elliptic curve defined over a finite field rather than the multiplicative group of a finite field. An elliptic curve *E* can be given by the *Weierstrass equation*:

$$y^2 = x^3 + ax + b \tag{3}$$

The complete description of the applications based on elliptic curves can be found in [10].

Next, we intend to analyze the chaotic behavior of the two-dimensional map which derives from the equations of the *serpentine curve*:

$$\begin{aligned} x_n &= arctg(ctg(ry_n)) \\ y_n &= \sin(rx_n)\cos(rx_n) \end{aligned} \tag{4}$$

The behavior of the two-dimensional map given by the equation (4) depends in time by the system's parameter *r* and by the pair (x_0, y_0) which defines the initial condition (seed). From the bifurcation diagram, represented in figure 3, it can be observed that for a value of the parameter $r > 1$, the map's behavior is chaotic.

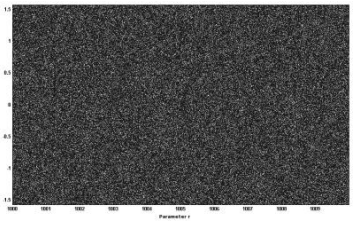

Figure 3. Bifurcation diagram for the serpentine

The chaotic state can be observed by the existence in the phase space of a chaotic attractor (figure 4) in which all the system trajectories evolve following a certain pattern but are never the same.

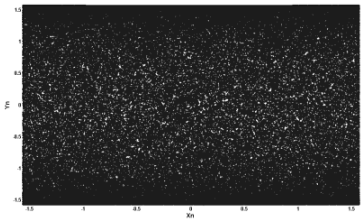

Figure 4. The serpentine attractor

The distribution probability of the maps' trajectories, which start from different initial conditions (x_0 si x_0'), with the system's parameter $r = 1000$, is represented in figure 5. It is obvious that the two maps are identical; therefore the map preserves an invariant density for values of the parameter $r \in [1000,1010]$.

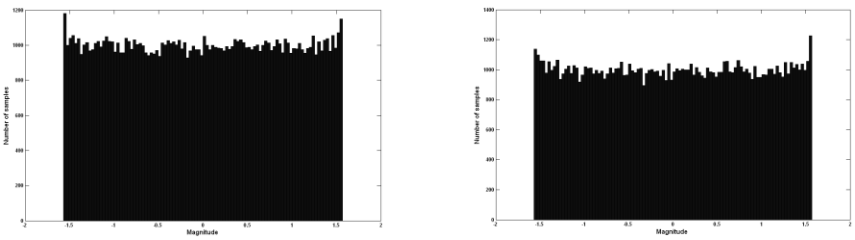

Figure 5. Histograms of the serpentine curve for $r = 1000$ and:
(a) $(x_0, y_0) = (-0.3, -1.1)$ (b) $(x_0', y_0') = (0.1, 1.3)$

According to the results described above, the two-dimensional map defined by the relation (4) has a chaotic behavior for a range of values of the system's parameter, preserves an invariant density making it to be successfully used in creating some pseudo-random number generator, strong from the cryptographic point of view.

4. The analysis of randomness for keystreams generated using the proposed function

The experimental testing of the randomness for keystreams generated using both of the new proposed function was performed using the automated system designed by authors and presented in [2]. The automated system is based on DIEHARD, a very well known battery for statistical testing of randomness of a PRNG, developed by George Marsaglia. For a certain input stream, DIEHARD performs more statistical tests to measure the quality of randomness of it and provides as output a set of 215 p-values. If a p-value, corresponding to a test, lies in the interval [0.001, 0.995], we can conclude that the input stream passed that test. For our experimental analysis of randomness, we have generated 1000 keystreams and we plotted the obtained results as a histogram of total number of passed tests versus number of keystreams which realized that number.

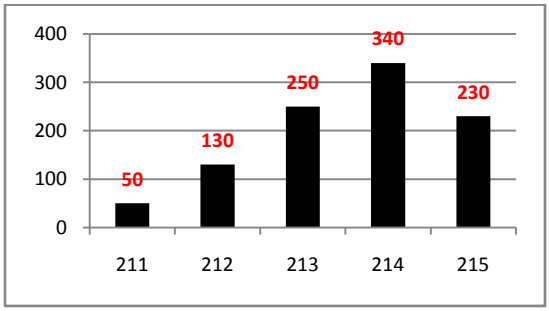

Figure 6. Histogram of the DIEHARD tests for the serpentine

Analyzing the histograms of serpentine, we can conclude that all generated files passed at least 98% of the tests. This entitles us to say that the proposed serpentine function has a very good randomness.

5. Conclusions

In the third chapter we theoretically have demonstrated, using instruments of the theory of nonlinear dynamic systems, that the proposed map has a good chaotic behavior. From the analysis of the experimental results, presented in chapter 4, we can conclude that the randomness of the sequences obtained using the PRNG based on serpentine curve has the required level to be used for the encryption of the images.

References

[1] N. K. Pareek , V. Patidar, K, "Block cipher using 1D and 2D chaotic maps", International Journal of Information and Comunication Tehnology, 2010.

[2] M. Sharma and M.K. Kowar, "Image Encryption Techniques Using Chaotic Schemes: a Review," International Journal of Engineering Science and Technology, vol. 2, no. 6, 2010, pp. 2359–2363.

[3] R. Forre, "The Hénon Attractor as Key Stream Generator," Abstracts of Eurocrypt 91, 1991, pp. 76–80.

[4] A.S. Alghamdi, H. Ullah, M. Mahmud, and M.K. Khan, "Bio-Chaotic Stream Cipher- Based Iris Image Encryption," Proceedings of the International Conference on Computational Science and Engineering, 2009, pp. 739–744.

[5] H.H. Ahmed, H.M. Kalash, and O.S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images," Journal of Optical Engineering, vol. 45, 2006.

[6] A.N. Pisarchik and M. Zanin, "Image Encryption with Chaotically Coupled Chaotic Maps," Physica D, vol. 237, no. 20, 2008, pp. 2638–2648.

[7] C. I. Rancu, A. Serbanescu "Chaos – Based Cryptography. A solution for information Security", Buletin of the Transilvania University of Brasov, 2009.

[8] R. Boriga, A.C. Dascalescu, "Automated system for testing the period and randomness of a pseudorandom number generator", Megabyte, 2010.

[9] A. Jolfaei and A. Mirghadri, "An Applied Imagery Encryption Algorithm Based on Shuffling and Baker's Map," Proceedings of the 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR- 10), Florida, USA, 2010, pp. 279–285.

[10]. G. Seroussi; CO. Hewlett-Packard , P Alto, "Elliptic curve cryptography", Information Theory and Networking Workshop, 1999 .