Number generation based on the chaotic sequences

Yelena Kozmina[1*], Alytis Gruodis[2]

[1]***ISMA,*** *1 Lomonosova Str., build. 6, LV-1019 Riga, Latvia*
[2]***Vilnius Business College, Kalvarijų 129-401, LT-08221 Vilnius, Lithuania***

**Corresponding author's e-mail: jelena.kozmina@isma.lv*

Abstract

Several classical algorithms for generation the recurrent chaotic sequences are observed and discussed in the framework of cryptographic usage for learning purposes.

Keywords: Verhulst equation, discrete chaos

1 Introduction

Information hiding technologies must be treated as the important tool for different tasks in the contemporary world. Traditional encryption/decryptions techniques (for example AES, DES-3, IDEA) are oriented for data transmission between the correspondents, otherwise, the usage of digital multimedia requires the new approach for security. In that case, chaotic encryption systems are useful for solving problems related to authorisation, copyright [1].

This work is devoted to the observing the most popular number generation techniques in information systems, where chaotic sequences play the role of cryptographic keys.

2 Overview

Generation of chaotic sequences is grounded on the 'randomness' behaviour. Two criteria are very important in order to estimate the 'quality' of sequence: uniform distribution and independence [2]. Uniform distribution allows controlling the sequence behaviour. Occurrence of each state with the same or approximately the same frequency must be realized for all sequences. Independence could be titled as a sophisticated parameter, some sort of the 'state of art': no one sequence value can be generated from the other values. Unpredictability of the sequence members could be distinguished using following criterion: each number must be statistically independent of neighbour numbers and generally of other numbers.

Logistic growth model is known as the simplest model of a discrete chaos. In the middle of XIX century, population growth was studied by Pierre Verhulst [3]. Nowadays, *logistic map* could be titled as the simplest system for describing the chaos as a determined system in recurrent form. For *t*=0,1,2,… sequence x_t represents the current value related to the certain state, $x_t \in (0;1)$, and *r* represents the system parameter:

$$x_{t+1} = r x_t (1 - x_t). \tag{1}$$

Figure 1 represents the one-dimensional chaotic distribution x_t, when *t* varies from 0 to 500 with step 1. Detail description of solutions of Verhulst equation in differential and discrete form is presented in [4]. Also, two-dimensional dynamic system described by Duffing's equation [5] could be used for number generation.

In [6], several recurrent routines for generation purposes are proposed:

$$x_{t+1} = 1 - (1.5 + r) x_t^2, \tag{2}$$

$$x_{t+1} = (3.5 + r) x_t^3 - (2.5 + r) x_t, \tag{3}$$

$$x_{t+1} = \cos\big((2 + 100r) \arccos(x_t)\big), \tag{4}$$

where *r* represents the system parameter in interval (0÷0.5), and $x_t \in (-1;1)$.
One-dimensional chaotic sequences are vulnerable to attacks of the phase space reconstruction [6]. According to this circumstance, additional routines were used. Equations (2), (3), (4) represent the chaotic sequences with *logistic map* [3], *cubic map* [7] and *Chebyshev map* [8] respectively.

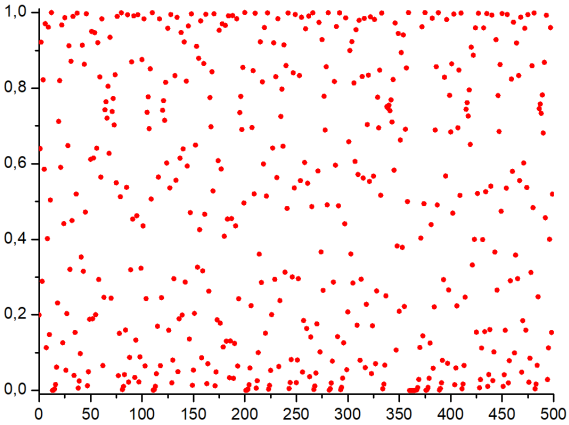

FIGURE 1 Distribution of x_t, $t \in [0;500]$, r=4.0, according to (1)

In [7], properties of sequences generated by cubic equation were described, where *a* represents the system parameter in interval $0 < a \leq 4$:

$$x_{t+1} = a x_t^3 + (1 - a) x_t. \tag{5}$$

In [8], novel image encryption algorithm based on two generators is presented. Algorithm consisting of two parts (*Chebyshev map* based as well as rotation equation based) demonstrates an excellent level of security. Rotation equations are presented below:

$$x_{t+1} = -a - (x_t - a)\cos\theta + (y_t \sin\theta)/r_t, \tag{6}$$

$$y_{t+1} = -x_t\, r_t\, \sin\theta - y_t \cos\theta, \quad (7)$$

$$r_t = \sqrt{0.5\left(x_t^2 + \sqrt{x_t^4 + 4y_t^2}\right)}, \quad (8)$$

where θ=2 and a=2.8.

In [9], an idea of linear congruential generators was proposed firstly. Sequence is described by following equation:

$$x_{t+1} = (a\, x_t + c)\, mod\ m, \quad (9)$$

where *m>0* represents modulus, *c* represents increment in the range $0 \le c < m$, initial value x_0 must be selected from interval $0 \le x_0 < m$. It is necessary to point out, that selection of values for *a, c*, *m* is critical for generation of statistically independent numbers.

3 Conclusion

Several techniques for number generation could be used in order to receive the statistically independent number sequences like chaotic [2]. Statistical tests allow estimating the quality of generated sequence in order to avoid the predictability [8].

References

[1] Pianhui Wu 2013 *Research on digital image watermark encryption based on hyperchaos* PhD thesis. – Derby

[2] William Stallings 2005 Cryptography and Network Security *Principles and Practices, Fourth Edition* Prentice Hall 592

[3] Bacaer N 2011 *A Short History of Mathematical Population Dynamics* Springer-Verlag London Limited DOI 10.1007/978-0- 85729-115-8-6

[4] Kozmina Ye 2018 Discrete Analogue of the Verhulst Equation and Attractors. Methodological Aspects of Teaching *Innovative Infotechnologies for Science, Business and Education* **1**(24) 3-12

[5] Roda Fernando, Lara Luis 2010 Chaotic Cipher Using the Duffing Equation *Information Security Journal: A Global Perspective* **19**(6) 320-7

[6] Changci Wen, Qin Wang, Xianghong Liu, Fumin Huang. An Image Encryption Algorithm Based on Scrambling and Chaos 2013 *Journal of Information & Computational Science* **10**(17) 5725-33

[7] Rogers T D, Whitley D C 1983 Chaos in the cubic mapping *Mathematical Modelling* **4** 9-25

[8] Stoyanov B, Kordov K 2015 Image Encryption Using Chebyshev Map and Rotation Equation *Entropy* **17** 2117-39

[9] Lehmer D 1951 Mathematical Methods in Large-Scale Computing *Proceedings of 2nd Symposium on Large-Scale Digital Calculating Machinery* Cambridge: Harvard University Press