UDC 004.056.55, 004.942

# PROPERTIES OF GENERATORS OF PSEUDO-RANDOM SEQUENCES CONSTRUCTED USING FUZZY LOGIC AND TWO-DIMENSIONAL CHAOTIC SYSTEMS

**Kushnir M. Ya.** – PhD, Associate Professor, Associate Professor of the Department of Radio Engineering and Information Security. Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine.

**Kosovan Hr. V.** – PhD, Assistant of the Department of Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine.

**Kroyalo P. M.** – Postgraduate student, Department of Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine.

## ABSTRACT

**Context.** The problem of generating pseudo-random sequences of bits using the rules of fuzzy logic and two-dimensional chaotic systems is considered.

**Objective.** Pseudo-random sequences generators built using two-dimensional chaotic systems and fuzzy logic. The purpose of the work is to develop and implement pseudo-random bit sequences generators based on the rules of fuzzy logic and two-dimensional chaotic systems and to evaluate the statistical characteristics of the generated sequences using statistical tests of National Institute of Standards and Technology.

**Method.** A method for generating pseudo-random bit sequences is proposed, which allows form bit sequences with characteristics that meet the requirements of secure communication systems and cryptographic protection of information based on the rules of fuzzy logic and two-dimensional chaotic systems. In the process of studying the operation of generators, histograms of the distribution of output values were constructed, which allows to clearly determine whether the entire range of output values of the two-dimensional system could be used to generate pseudo-random bit sequence or only part of it. A study of the statistical characteristics of the generated sequences using a set of statistical tests was also performed.

Results. Bit sequences formed using fuzzy logic rules and two-dimensional chaotic systems can be used to transmit information in secure communication systems.

**Results.** The proposed generators were implemented in software, histogram analysis and evaluation of compliance with the criteria for a set of statistical tests of National Institute of Standards and Technology.

**Conclusions.** The experiments confirmed the ability of the proposed generators to generate bit sequences with good statistical characteristics, which allows them to be recommended for use in practice in solving problems of cryptographic protection of information and secure transmission of information over open communication channels. Prospects for further research may be to create cryptographic methods of information protection based on the proposed pseudo-random bit sequences generators, the implementation of secure communication systems.

**KEYWORDS:** generator, chaos, two-dimensional system, pseudo-random sequence, fuzzy logic, statistical tests.

## ABBREVIATIONS

FFT is a fast Fourier transform;

NIST is a statistical tests suite of National Institute of Standards and Technology;

PFMM-CLM is a parallel fuzzy multimodule chaotic logistic mapping;

PRB is a pseudo-random bits;

PRS is a pseudo-random sequence.

## NOMENCLATURE

$x_0$ is an initial condition of the two-dimensional Hénon system;

$y_0$ is an initial condition of the two-dimensional Hénon system;

$x_{n+1}$ is an output value of the two-dimensional Hénon system;

$y_{n+1}$ is an output value of the two-dimensional Hénon system;

$a$ is a control parameter of the two-dimensional Hénon system;

$b$ is a control parameter of the two-dimensional Hénon system;

$c_0$ is an initial condition of the two-dimensional Lozi system;

$d_0$ is an initial condition of the two-dimensional Lozi system;

$c_{n+1}$ is an output value of the two-dimensional Lozi system;

$d_{n+1}$ is an output value of the two-dimensional Lozi system;

$\alpha$ is a control parameter of the two-dimensional Lozi system;

$\beta$ is a control parameter of the two-dimensional Lozi system;

$p_0$ is an initial condition of the two-dimensional cross-chaotic system;

$r_0$ is an initial condition of the two-dimensional cross-chaotic system;

$p_{n+1}$ is an output value of the two-dimensional cross-chaotic system;


DOI 10.15588/1607-3274-2022-1-5

$r_{n+1}$ is an output value of the two-dimensional cross-chaotic system;

$\mu$ is a control parameter of the two-dimensional cross-chaotic system;

$k$ is a control parameter of the two-dimensional cross-chaotic system;

$n$ is a number of iterations of chaotic system;

$x_{\min}$ is a minimum of range of output values of the two-dimensional Hénon system;

$x_{\max}$ is a maximum of range of output values of the two-dimensional Hénon system;

$P_{value}$ is a criterion for passing the statistical test NIST.

## INTRODUCTION

A method of generating pseudo-random sequence (PRS) bits using multidimensional chaotic systems and fuzzy logic rules for the formation of pseudo-random bit sequences with their further verification for compliance with the criteria of statistical tests suite of National Institute of Standards and Technology (NIST) is suggested in this article [1–8]. A number of multidimensional chaotic systems, such as two-dimensional Hénon, Lozi maps, and cross-chaotic maps, are used as mathematical functions for the formation of initial values.

Fuzzy logic in the sense of deterministic chaos is a section of mathematical logic designed to solve the problem of fuzzy decision making by assigning a certain bit value to a fuzzy range of initial values of a chaotic system to obtain the most accurate result possible [9–14]. Fuzzy logic is designed to solve the problem of generating bits by considering all available information and making the best possible decision from the generated initial value of the chaotic system. To verify the effectiveness of this method of generating PRS, the latter should be tested for compliance with the criteria of NIST statistical tests, which will confirm the effectiveness of encoders and cryptographic methods based on such generators for processing, transmitting or storing confidential information [15–19].

A large number of different PRS bit generators are known from the literature that both use threshold methods to generate bit sequences and generate sequences by converting a decimal value into a bit representation [6–8]. We suggest to use the rules of fuzzy logic to form pseudo-random bit sequences.

**The object of study** is the process of pseudo-random bit sequence generation using two-dimensional chaotic systems and fuzzy logic.

**The subject of study** is the combination of chaos theory and fuzzy logic rules to form a new approach to creating secure data transmission systems.

**The purpose of the work** is to develop and implement PRS bit generators based on the rules of fuzzy logic in two-dimensional chaotic systems and to evaluate the statistical characteristics of the generated sequences using statistical tests NIST.

## 1 PROBLEM STATEMENT

To generate PRS bits, we selected three two-dimensional chaotic mappings using fuzzy logic, namely the Hénon (1), Lozi (2) maps, and cross-chaotic (3) maps [1, 3].

$$\begin{aligned} x_{n+1} &= y_{n+1} - ax_n^2, \\ y_{n+1} &= bx_n^2, \end{aligned} \tag{1}$$

where $x_0 \in (-1;1)$ and $y_0 \in (-0.4;0.4)$ are the initial states of Hénon chaotic systems, $a \in (0;2]$, $b \in (-0.5;0.5]$ are control parameters.

$$\begin{aligned} c_{n+1} &= 1 - \alpha|c_n| + d_n, \\ d_{n+1} &= \beta c_n, \end{aligned} \tag{2}$$

where $c_0 \in (-2;2)$ and $d_0 \in (-2;2)$ are the initial states of chaotic systems, $a \in (1.3;1.8)$ and $b \in (0.3;0.6)$ are control parameters.

$$\begin{aligned} p_{n+1} &= 1 - \mu r_n^2, \\ r_{n+1} &= \cos\left(k \cos^{-1} p_n\right), \end{aligned} \tag{3}$$

where $p_0 \in (-1;1)$ and $y_0 \in (-1;1)$ – are the initial states of chaotic systems, $\mu \in (1,4;2]$ and $k \in (0,3)$ are control parameters.

Depending on how the control parameter of the chaotic system is selected a different range of initial values is obtained, and the formation of bit sequences will be done in a different way. Therefore, in order to be able to form a bit sequence, it is necessary to adapt the rules of fuzzy logic to make them suitable for a bit sequence formation.

Histograms of distribution of initial values of two-dimensional chaotic systems, as well as results of the NIST statistical tests will serve as the criteria of the formed sequences estimation.

## 2 REVIEW OF THE LITERATURE

Chaos theory is used in numerous applications, namely in cryptography, secure communications, technology, physics, economics, robotics, control and many others [1, 3, 5, 12]. Chaotic systems are deterministic ones with high sensitivity to initial conditions and changes in control parameters and are therefore constitute an excellent basis for effective modeling of complex natural phenomena. These features allow using the chaotic systems to build secure communication systems.

Due to the above characteristics of chaotic systems, there is a constant demand for the introducing new appli-


DOI 10.15588/1607-3274-2022-1-5

cations of chaotic systems in secure communication systems. Usually new applications are implemented by either modifying the existing chaotic system, or by slightly changing the equations describing chaotic systems, or adding another equation to the system and increasing its dimension, or proposing a new application of an already well-studied chaotic system.

Logistic map [7] is one of the most well-known one-dimensional discrete time chaotic systems and one of the most heavily modified chaotic systems [7, 8, 12, 15]. The map has only one parameter and a simple structure, which makes it suitable for many applications. Many modifications of the classical logistic map have been proposed in the literature. One of such modifications is the use of a fuzzy triangular number to change the behavior of the logistic map. The idea of passing the logistic map values through a fuzzy number is mathematically simple, but it leads to a significant improvement in the behavior of chaotic map.

Fuzzy logic and a fuzzy sets themselves are a large field of research and have found their application in technology. Specifically, in dynamical systems fuzzy sets are combined with chaotic systems and form the so-called fuzzy dynamical systems [9–14]. In one of the proposed modifications of the logistic map, its values at each iteration are passed through a triangular fuzzy number, which is a simple linear function that takes values in the interval [0, 1]. The resulting map demonstrates a more unpredictable behavior associated with chaos compared to the classical map, and reaches a higher value for its Lyapunov exponent. In addition, to demonstrate the applicability of the map in chaos-related software applications, the problems of generating pseudo-random values are described in [17–19], and the process of image encryption based on such systems is presented in [19]. It can be seen that a sequence of bits formed from a modified mapping using a simple rule passes all 15 tests of the NIST statistical test suite [15,18]. Further, the generated bit sequence is used to implement the image encryption process, and the resulting encrypted image is analyzed for security using methods such as histogram analysis, correlation and information entropy.

It should be noted that the approach of combining fuzzy logic and chaotic systems can be easily applied to any chaotic system and further modified by considering different types of fuzzy numbers, such as trapezoidal, Gaussian, quadratic, exponential ones or combinations thereof. Thus, the combination of fuzzy logic and chaos is quite promising for the development of new PRS bit generators and their application in cryptography and secure communication systems.

## 3 MATERIALS AND METHODS

To implement the PRS bit generator, we used the following fuzzy logic rule:

1. First, we divide the range of initial values of each of the chaotic systems into 10 intervals.
2. Each of these intervals is divisible by 25 subintervals except the last one; it is divisible by 30.
3. The size of each of the intervals is determined depending on the selected values of the control parameters of chaotic systems, and they will differ from each other for both systems.

First, we selected four two-dimensional chaotic maps, such as Hénon (1), Lozi (2), and a cross-chaotic map (3) to test the efficiency of such generators.

Fuzzy logic rule for a two-dimensional Hénon map with the values of the control parameter a = 1.40 and b = 0.3035 and the range of change of output values [–1.297; 1.276] is as follows:

If the input = –1.297 – –1.0397, the output = 0–25
If the input = –1.0397– –0.7824, the output = 26–50
If the input = –0.7824 – –0.5251, the output = 51–75
If the input = –0.5251– –0.2678, the output = 76–100
If the input = –0.2678 – –0.0105, the output =101–125
If the input = –0.0105 – 0.2468, the output = 126–150
If the input = 0.2468 – 0.5041, the output = 151–175
If the input = 0.5041 – 0.7614, the output = 176–200
If the input = 0.7614 – 1.0187, the output = 201–225
If the input = 1.0187 – 1.276, the output = 226–255.

Similarly, the original ranges of Lozi maps and the cross-chaotic map are broken and PRS bits are formed. Fig. 1 shows a block diagram of a PRS bit generator using fuzzy logic and two-dimensional chaotic systems.

## 4 EXPERIMENTS

In the process of studying the statistical characteristics of bit sequences, PRS bits were formed separately for each two-dimensional map with different initial conditions and control parameters. Their initial conditions and control parameters, under which the best results of statistical tests were obtained, are presented in Table 1. In addition, since the system is very sensitive to the values of initial conditions and control parameters, it is necessary to choose the values of control parameters so that the range of initial values of chaotic systems is fully completed.

## 5 RESULTS

To check whether the whole range of initial values is really completed, it is necessary to build a histogram of the initial values distribution. Since the fuzzy logic rule used for generating bit sequences is divided into 256 intervals, the volume of the histogram will also be confined to 256 intervals. Fig. 2 presents a histogram of the initial values distribution of the Hénon map. The range of output values was from $x_{\min} = -6.3722$ to $x_{\max} = 6.3699$, which was divided into 256 intervals. Here, the abscissa axis shows the division of the range of the initial values into 256 intervals, and the ordinate axis – the number of values that fall into the corresponding interval.


DOI 10.15588/1607-3274-2022-1-5

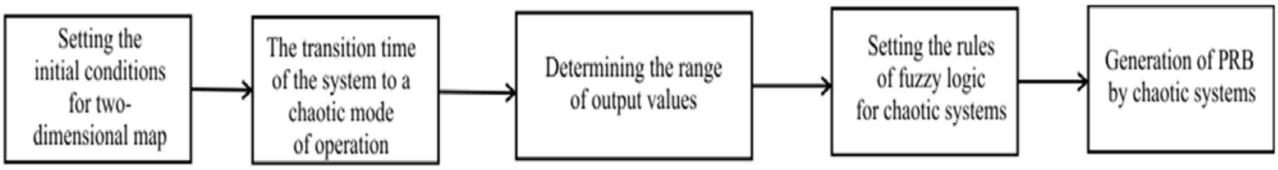


Figure 1 – Block diagram of the PRS bit generator using fuzzy logic and two-dimensional chaotic system

Table 1 – Values of initial conditions and control parameters of two-dimensional chaotic systems

| Two-dimensional chaotic map | Henon | Lozi | Cross-chaotic |
|---|---|---|---|
| Initial conditions | $x_0$ =0.254 | $c_0$ =0.173 | $p_0$ =0.324 |
| | $y_0$ =0.321 | $d_0$ =0.255 | $r_0$ =0.651 |
| Control parameters | $a$=0.0413 | $\alpha$ =1.6113 | $\mu$ =2.81 |
| | $b$=0.99991 | $\beta$ =0.5202 | $k$ =7.73 |

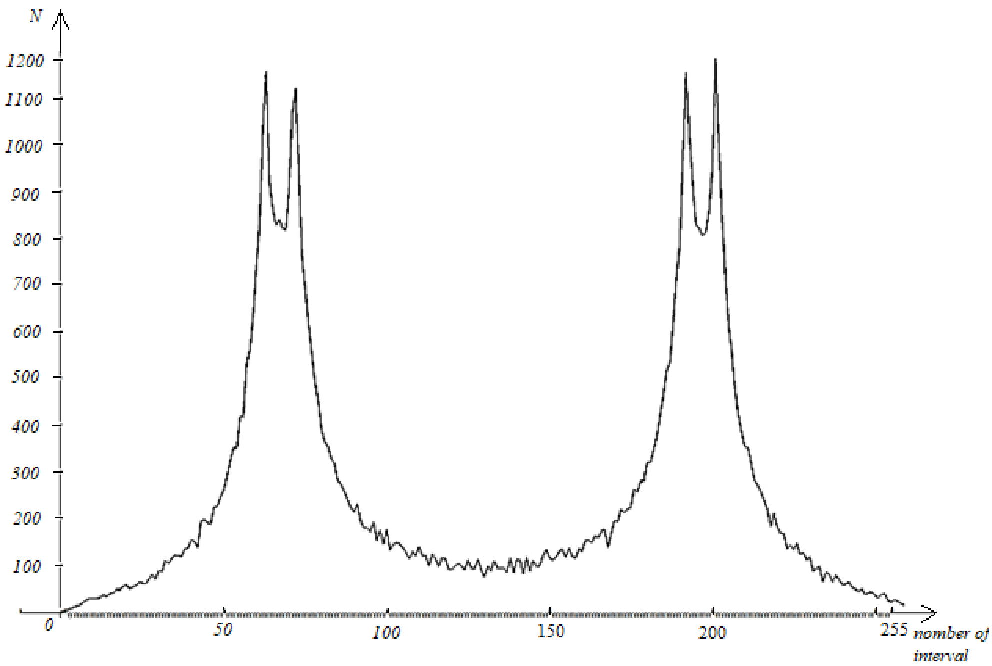


Figure 2 – Histogram of the distribution of the output values of the Henon mapping for 65,000 iterations

It can be seen from the obtained histogram that two areas predominate in the number of values that fall there. The greater number of values falling in a certain area in terms of statistical research or application in cryptography is rather considered a disadvantage. Therefore, to generate PRS bits, it is advisable to use not the entire range of initial values, but only a part of it with uniform distribution of the number of values falling into it.

Fig. 3 presents a histogram of the initial values distribution of the Lozi map. The range of output values was from $x_{\min} = -1.2236$ to $x_{\max} = 1.38$ and was also divided into 256 intervals. It follows from the obtained histogram that the distribution of the initial values is almost uniform, and this enables to generate PRS bits. Uniformity of distribution also determines the use of PRS bit generator based on fuzzy logic in cryptographic and secure communication systems.

The histogram of the initial values distribution for two-dimensional the cross-chaotic map is presented in Fig. 4. The range of output values was from $x_{\min} = -1.1$ to $x_{\max} = 0.96$ and was divided into 256 intervals.

It can be seen from the obtained histogram that, similarly to the case of the Hénon map, there are two areas predominating in the number of values that fall there. Therefore, to generate PRS bits, it is advisable to use not the entire range of the initial values, but only a part of it with the best uniform distribution.

The results of studying the PRS bits for compliance with the criteria of statistical tests formed by the Hénon, Lozi and cross-chaotic maps are presented in Tables 2, 3 and 4.


DOI 10.15588/1607-3274-2022-1-5

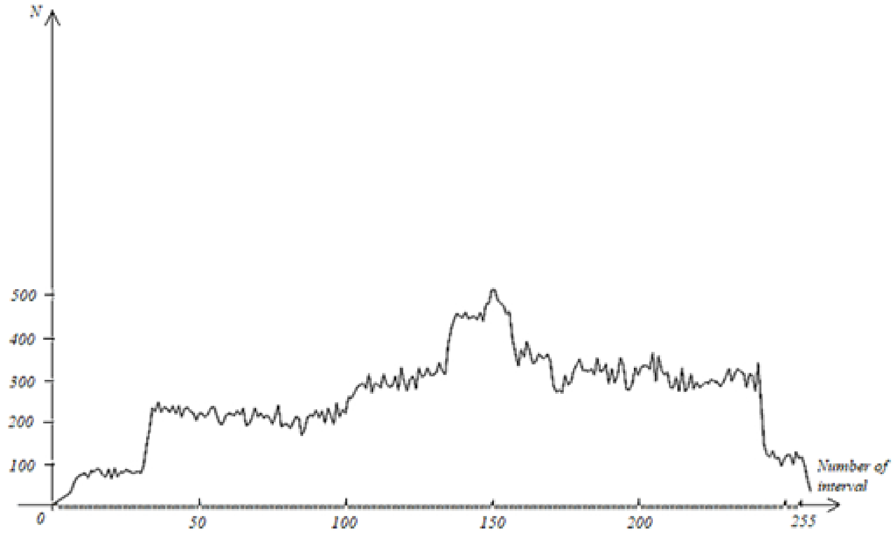


Figure 3 – Histogram of the distribution of the output values of the Lozi mapping for 65,000 iterations

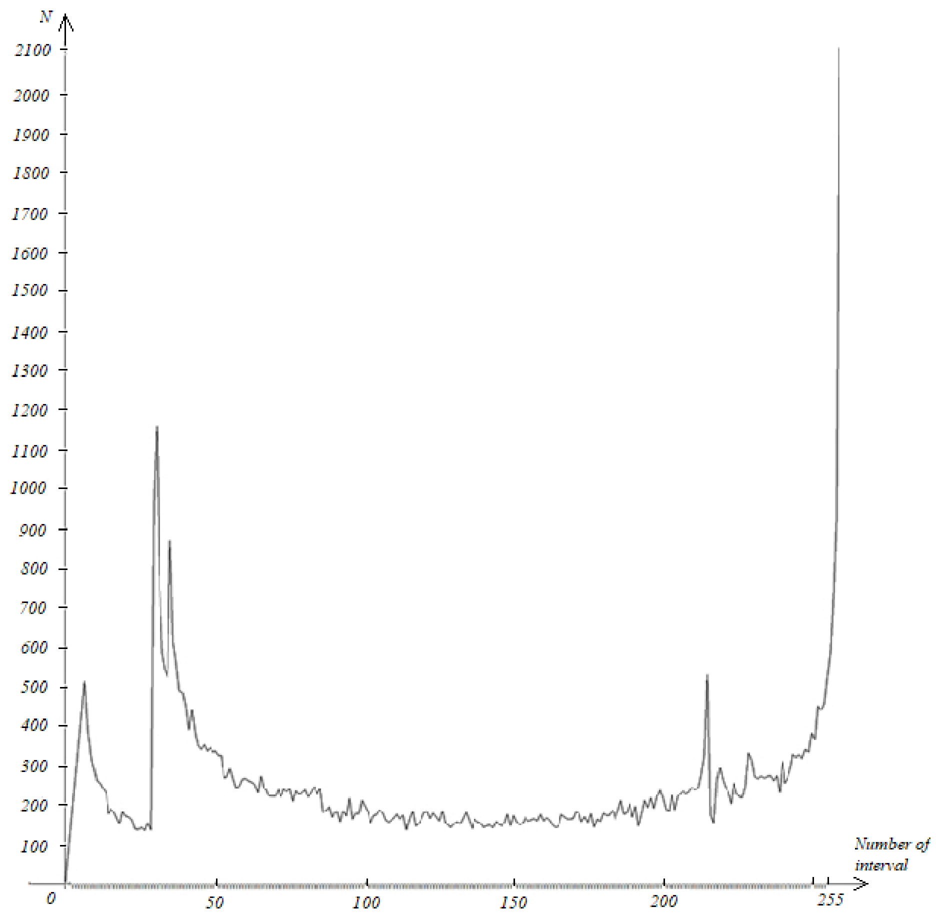


Figure 4 – Histogram of the distribution of the output values of two-dimensional cross-chaotic mapping for 65,000 iterations


DOI 10.15588/1607-3274-2022-1-5

Table 2 – Test results of the generated sequence formed by the Henon mapping

| Statistical test type | The obtained $P_{value}$ | Proportion |
|---|---|---|
| Frequency | 0.991 | 0.980 |
| Block Frequency | 0.992 | 1,0 |
| Runs | 0.872 | 0.962 |
| Longest Run | 0.895 | 0.941 |
| Rank | 0.992 | 0.854 |
| FFT | 0.990 | 0.268 |
| Non-Overlapping Template | 0,383827 | 0.980 |
| Overlapping Template | 0.987 | 0.252 |
| Universal | 0.963 | 0.106 |
| Linear Complexity | 0.971 | 1.0 |
| Serial | 0.987 | 0.670 |
| Approximate Entropy | 0.989 | 0.959 |
| Cumulative Sums | 0.108791 | 1.0 |
| Random Excursions | 0.203 | 0.643 |
| Random Excursions Variant | 0.213 | 1.0 |

Table 3 – Test results of the generated sequence formed by the Lozzi mapping

| Statistical test type | The obtained $P_{value}$ | Proportion |
|---|---|---|
| Frequency | 0.258 | 1.0 |
| Block Frequency | 0.687 | 1.0 |
| Runs | 0.697 | 0.960 |
| Longest Run | 0.253 | 0.960 |
| Rank | 0.799 | 0.66 |
| FFT | 0.547 | 0.91 |
| Non-Overlapping Template | 0.350 | 1.0 |
| Overlapping Template | 0.358 | 0.180 |
| Universal | 0.451 | 0.960 |
| Linear Complexity | 0.366 | 0.970 |
| Serial | 0.783 | 1.0 |
| Approximate Entropy | 0.687 | 0.980 |
| Cumulative Sums | 0.316 | 1.0 |
| Random Excursions | 0.857 | 0.960 |
| Random Excursions Variant | 0.751 | 0.857 |

Table 4 – Test results of the generated sequence formed by cross-chaotic mapping

| Statistical test type | The obtained $P_{value}$ | Proportion |
|---|---|---|
| Frequency | 0.138 | 0.980 |
| Block Frequency | 0.113 | 0.970 |
| Runs | 0.380 | 1.0 |
| Longest Run | 0.575 | 0.960 |
| Rank | 0.789 | 0.990 |
| FFT | 0.474 | 1.0 |
| Non-Overlapping Template | 0.321 | 0.980 |
| Overlapping Template | 0.574 | 0.990 |
| Universal | 0.525 | 0.960 |
| Linear Complexity | 0.883 | 1.0 |
| Serial | 0.116 | 0.960 |
| Approximate Entropy | 0.233 | 0.980 |
| Cumulative Sums | 0.178 | 0.83 |
| Random Excursions | 0.037 | 1.0 |
| Random Excursions Variant | 0.745 | 0.980 |

## 6 DISCUSSION

We also compared the results with the results of other studies. In [20], a method for generating PRB sequences using fuzzy logic rules and based on chaotic one-dimensional mappings is proposed. The three most well-known one-dimensional mappings were used in the study, namely logistic, square and cubic. As a result of the inspection, it was found that the PRB generated by such mappings meet the conditions of the tests from the NIST set in part. Therefore, it is not desirable to use only one one-dimensional chaotic mapping to form bit sequences using fuzzy logic rules. To solve this problem, in the same work [20], it was proposed to implement a PVP bit generator using two one-dimensional chaotic systems, namely logistic and cubic mappings. As a result, much better results were obtained, namely, the generated sequences correspond to most of the tests from the NIST set.

In [21], one-dimensional logistic mapping was modified using fuzzy triangular numbers. The result is a new modified logistics mapping. Then this mapping was used to generate pseudo-random bits, which gave high positive


DOI 10.15588/1607-3274-2022-1-5

results. Pseudo-random bits were created by comparing the obtained number with the threshold value selected at 0.5. The value of bit 1 was generated if the number is greater than or equal to the threshold, and the value of bit 0 was obtained otherwise.

A set of statistical tests from the National Institute of Standards and Technology NIST 800-22 was also used to verify that the generated sequence was pseudorandom. The obtained results showed that the sequence generated by the modified logistic mapping passes all tests.

In addition, a new parallel fuzzy multimodule chaotic logistic mapping (PFMM-CLM) was proposed in [22]. In the process of research, logistic mapping was used several times with changed control parameters. In this case, fuzzy set theory is used as a fuzzy logic selector to generate pseudo-random bit sequences. As a result of modeling and performance analysis of the proposed pseudo-random bit generator based on PFMM-CLM, high chaotic properties were obtained, such as a reliable bifurcation diagram and a high value of the Lyapunov exponent. Checking the compliance of statistical tests showed that the sequences generated by such a generator are completely satisfactory to all tests.

As a result of analysis and comparison of all considered results it was found that our proposed pseudo-random bit generator has improved statistical properties in comparison with PVP bit generators based on one-dimensional chaotic systems. In addition, it also has a number of advantages, namely:

– the use of two-dimensional display increases the number of initial conditions and control parameters, and, as a consequence, improves the security of information transmission systems;

– does not require additional modifications;

– does not require multiple use of the same display with different values of control parameters and, as a result, our proposed generator will be fast enough.

## CONCLUSIONS

**The scientific novelty.** The method for generating PRS bit sequences using fuzzy logic rules and based on two-dimensional chaotic maps is proposed in this article. Since two-dimensional maps are very sensitive to the values of control parameters, it was first checked whether all the intervals formed by the rules of fuzzy logic are attended by the initial values of chaotic systems. To check that, the histograms of the initial values distribution were built, and the parts with the most uniform distribution were selected from them to form the PRS bits. After obtaining the best histograms, the pseudo-random bit sequences were generated and further verified for compliance with the NIST test criteria.

**The practical significance.** The sequences verification was performed both for each of the equations of two-dimensional systems separately and after superimposing the initial values using the XOR operation. Due to verification it was found that, when generating sequences by the Hénon map, the sequence formed by the variable y corresponded better to the conditions of the statistical tests. For the sequence formed by the Lozi map, it was the sequence formed by the first equation of the system, and for the cross-chaotic map the first equation shows the best results. PRSs formed in this way satisfy the conditions of the tests from the NIST suite.

**Prospects for further research.** PRS bits generated using fuzzy logic rules and two-dimensional chaotic systems can be used to develop methods for encrypting information based on them and to create secure telecommunications systems.

## ACKNOWLEDGEMENTS

The work is supported by the state budget scientific research project of Yuriy Fedkovych Chernivtsi national university “Methods of forming signal structures and information processes of software and hardware interaction of broadband telecommunication systems and the Internet of Things” (state registration number 0121U 112870).

## REFERENCES

1. Kocarev L. Chaos-based cryptography: A brief overview, *IEEE Circuits and Systems Maganize*, 2001, Vol. 1, pp. 6–21. DOI:10.1109/7384.963463.
2. Semenko A., Kushnir N., Bokla N., Kosovan Hr. Features of creating based on chaos pseudo-random sequences. Modern Problems of Radio Enginiring, Telecommunications, and Computer Science, *XIIth International Conference TCSET’ February 20–24 2018: proceedings*. Lviv-Slavsco, Ukraine. 2018, pp. 338–342. DOI:10.20535/2411-2976.22018.
3. Mira C. and all. Chaotic dynamics in two-dimensional noninvertible maps, *World Scientific Series on Nonlinear Science,* 1996, *Series A*, Vol. 20, pp. 185–337. https://doi.org/10.1142/2252.
4. Hénaff S., Taralova I., Lozi R. Dynamical Analysis of a new statistically highly performant deterministic function for chaotic signals generation, *International Conf. on Physics and Control (PhysCon): proceedings*. Catania, Sicily, September 2009, P. 10. HAL Id: hal-00623064.
5. Strogatz S.H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering. CRC Press, Boca Raton, FL, USA, 2018, P. 532. ISBN 9780813349107.
6. Huang X., Liu L., Li X., Yu M., Wu Z. New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics, *Complexity,* 2019, № 44, pp. 1–9. https://doi.org/10.1155/2019/6567198.
7. Wang Y., Liu Z., Ma J., He H. A pseudorandom number generator based on piecewise logistic map, *Nonlinear Dyn.* 2016, No. 83, pp. 2373–2391. https://doi.org/10.1007/s11071-015-2488-0.
8. Murillo-Escobar M., Cruz-Hernández C., Cardoza-Avendaño L., Méndez-Ramírez R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map, *Nonlinear Dyn.* 2017, No. 87, pp. 407–425. https://doi.org/10.1007/s11071-016-3051-3.
9. Zimmermann H.J. Fuzzy Set Theory – And Its Applications. Springer Science & Business Media. *Berlin. Germany,* 2011, Vol. 21, 525 p. DOI: 10.1007/978-94-015-8702-0.
10. Chakraverty S., Sahoo D. M., Mahato N. R. Concepts of Soft Computing: Fuzzy and ANN with Programming. Springer: Berlin/Heidelberg, Germany, 2019, 198 p. DOI 10.1007/978-981-13-7430-2.
11. Hanss M. Applied Fuzzy Arithmetic: An Introduction with Engineering Applications. Springer, Berlin/Heidelberg, Germany, 2005, 270 p. DOI: 10.1007/b138914.


DOI 10.15588/1607-3274-2022-1-5

12. Li Z., Zhang X. On Fuzzy Logic and Chaos Theory: from an Engineering Perspective. In Fuzzy Logic, *A Spectrum of Theoretical & Practical Issues; Springer*. Berlin/Heidelberg, Germany, 2007. pp. 79–97. ISSN: 1434-9922.
13. Porto M., Amato P. A fuzzy approach for modeling chaotic dynamics with assigned properties, *Ninth IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2000: proceedings.* San Antonio, TX, USA, 7–10 May 2000, Vol. 1, pp. 435–440. DOI: 10.1109/FUZZY.2000.838699.
14. Stefanini L., Sorini L., Guerra M. L. Simulation of fuzzy dynamical systems using the LU-representation of fuzzy numbers, *Chaos Solitons Fractals,* 2006, No. 29, pp. 638–652. https://doi.org/10.1016/j.chaos.2005.08.096.
15. Patidar V., Sud K. K., Pareek N. K. A pseudo random bit generator based on chaotic logistic map and its statistical testing, *Informatica,* 2009, No. 33, pp. 441–452.
16. Stojanovski T., Kocarev L. Chaos-based random number generators-part I: analysis [cryptography], *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, 2001, No. 48, pp. 281–288. DOI: 10.1109/81.915385.
17. François M., Grosges T., Barchiesi D., Erra R. Pseudo-random number generator based on mixing of three chaotic maps, *Commun. Nonlinear Sci. Numer. Simul.,* No. 19, pp. 887–895. https://doi.org/10.1007/978-3-319-06089-7_16.
18. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E. A statistical Test Suite for Random and Pseudorandom Number Generators for cryptographic Applications, *Technical Report; Booz-Allen and Hamilton Inc.* Mclean, VA, USA, 2001. DOI: 10.3390/sym12081202.
19. Alvarez G., Li S. Some basic cryptographic requirements for chaos-based cryptosystems, *Int. J. Bifurc. Chaos,* 2006, No. 16, pp. 2129–2151. DOI: 10.1142/S0218127406015970.
20. Kushnir M., Kosovan Hr., Kroialo P., Komarnytskyy A. Encryption of the Images on the Basis of Two Chaotic Systems with the use of Fuzzy Logic, *15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering TCSET 2020: proceedings.* Lviv-Slavsco, Ukraine. February 25–29, 2020, pp. 610–613. DOI: 10.1109/TCSET49122.2020.235504.
21. Moysis L., Volos Ch., Jafari S. et al. Modification of the Logistic Map Using Fuzzy Numbers with Application to Pseudorandom Number Generation and Image Encryption, *Entropy*, 2020, Vol. 22, 474 p. DOI: 10.3390/e22040474.
22. Gad M., Hagras E., Soliman H. et al. A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption, *The International Arab Journal of Information Technology*. March 2021, Vol. 18, No. 2, pp. 227–236. https://doi.org/10.34028/iajit/18/2/12.

Received 21.11.2021.
Accepted 27.01.2022.

УДК 004.056.55, 004.942

## ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ПОБУДОВАНИХ ІЗ ВИКОРИСТАННЯМ НЕЧІТКОЇ ЛОГІКИ ТА ДВОВИМІРНИХ ХАОТИЧНИХ СИСТЕМ

**Кушнір М. Я.** – канд. фіз.-мат. наук, доцент, доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, Чернівці, Україна.

**Косован Г. В. –** канд. техн. наук, асистент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, Чернівці, Україна.

**Крояло П. М. –** аспірант кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, Чернівці, Україна.

### АНОТАЦІЯ

**Актуальність.** Розглянуто задачу генерування псевдовипадкових послідовностей (ПВП) бітів із застосуванням правил нечіткої логіки та двовимірних хаотичних систем. Об’єктом дослідження є генератори псевдовипадкових бітових послідовностей побудовані із застосуванням двовимірних хаотичних систем. Мета роботи – розроблення та реалізація генераторів ПВП бітів на основі правил нечіткої логіки та двовимірних хаотичних систем та оцінка статистичних характеристик сформованих послідовностей за допомогою статистичних тестів NIST.

**Метод.** Запропоновано спосіб генерування псевдовипадкових послідовностей бітів, що дозволяє сформувати бітові послідовності із характеристиками, що задовольняють вимогам захищених систем зв’язку та криптографічного захисту інформації на основі правил нечіткої логіки та двовимірних хаотичних систем. В процесі дослідження роботи генераторів побудовано гістограми розподілу вихідних значень, що дозволяє чітко встановити, чи весь діапазон вихідних значень двовимірної системи може бути використаний для генерування ПВП бітів чи тільки його частина. Також проведено дослідження статистичних характеристик генерованих послідовностей за допомогою набору статистичних тестів.

**Результати.** Послідовності бітів сформовані із застосуванням правил нечіткої логіки та двовимірних хаотичних систем можуть бути використані для передачі інформації в захищених системах зв’язку.

**Висновки.** Проведені експерименти підтвердили здатність запропонованих генераторів генерувати бітові послідовності із хорошими статистичними характеристиками, що і дозволяє їх рекомендувати для використання на практиці при вирішенні задач криптографічного захисту інформації та захищеної передачі інформації по відкритих каналах зв’язку. Перспективи подальших досліджень можуть полягати в створенні криптографічних методів захисту інформації на основі запропонованих генераторів ПВП бітів, реалізації захищених систем зв’язку.

**КЛЮЧОВІ СЛОВА:** генератор, хаос, багатовимірна система, псевдовипадкова послідовність, нечітка логіка, статистичний тест.

УДК 004.056.55, 004.942

## ИССЛЕДОВАНИЕ СВОЙСТВ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКОЙ ЛОГИКИ И ДВУМЕРНЫХ ХАОТИЧЕСКИХ СИСТЕМ

**Кушнир Н. Я. –** канд. физ.-мат. наук, доцент, доцент кафедры радиотехники и информационной безопасности. Черновицкого национального университета имени Юрия Федьковича, Черновцы, Украина.

**Косован Г. В. –** канд. техн. наук, ассистент кафедры радиотехники и информационной безопасности Черновецкого национального университета имени Юрия Федьковича, Черновцы, Украина.

**Крояло П. М. –** аспирант кафедры радиотехники и информационной безопасности Черновицкого национального университета имени Юрия Федьковича, Черновцы, Украина.


DOI 10.15588/1607-3274-2022-1-5

## АННОТАЦИЯ

**Актуальность.** Рассмотрена задача генерирования псевдослучайных последовательностей битов (ПСП) с применением правил нечеткой логики и двумерных хаотических систем. Объектом исследования являются генераторы псевдослучайных битовых последовательностей построенных с применением двумерных хаотических систем. Цель работы – разработка и реализация генераторов ПСП бит на основе правил нечеткой логики и двумерных хаотических систем и оценка сформированных последовательностей с помощью статистических тестов NIST.

**Метод.** Предложен способ генерирования псевдослучайных последовательностей битов, позволяет сформировать битные последовательности с характеристиками, удовлетворяющими требованиям защищенных систем связи и криптографической защиты информации на основе правил нечеткой логики и двумерных хаотических систем. В процессе исследования работы генераторов построены гистограммы распределения выходных значений, позволяет четко установить, весь диапазон выходных значений двумерной системы может быть использован для генерирования ПСП битов или только его часть. Также проведено исследование статистических характеристик генерируемых последовательностей с помощью набора стать-соприкасающихся тестов.

**Результаты.** Последовательности битов сформированы с применением правил нечеткой логики и двумерных хаотических систем могут быть использована для передачи информации в защищенных системах связи.

**Выводы.** Проведенные эксперименты подтвердили способность предложенных генераторов генерировать битные последовательности с хорошими статистическими характеристиками, что и позволяет их рекомендовать для использования на практике при решении задач криптографической защиты информации и защищенной передачи информации по открытым каналам связи. Перспективы дальнейших исследований могут заключаться в создании криптографических методов защиты информации на основе предложенных генераторов ПСП битов, реализации защищенных систем связи.

**КЛЮЧЕВЫЕ СЛОВА:** генератор, хаос, многомерная система, псевдослучайная последовательность, нечеткая логика, статистический тест.

## ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Kocarev L. Chaos-based cryptography: A brief overview / L. Kocarev // IEEE Circuits and Systems Maganize. – 2001. – Vol. 1. – P. 6–21. DOI:10.1109/7384.963463.
2. Features of creating based on chaos pseudo-random sequences. Modern Problems of Radio Enginiring, Telecommunica-tions, and Computer Sciens / [A. Semenko, N. Kushnir, N. Bokla, Hr. Kosovan] // XIIth International Conference TCSET' February 20–24 2018: proceedings. – Lviv-Slavsco, Ukraine. 2018. – P. 338–342. DOI:10.20535/2411-2976.22018.
3. Mira C. Chaotic dynamics in two-dimensional noninvertible maps / C. Mira and all // World Scientific Series on Nonlinear Science, Series A. – 1996. – Vol. 20. – P. 185–337. https://doi.org/10.1142/2252.
4. Hénaff S. Dynamical Analysis of a new statistically highly performant deterministic function for chaotic signals generation / S. Hénaff, I. Taralova, R. Lozi // International Conf. on Physics and Control (PhysCon): proceedings. – Catania, Sicily, September 2009. – P. 10. HAL Id: hal-00623064.
5. Strogatz S. H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering / S. H. Strogatz. – CRC Press: Boca Raton, FL, USA, 2018. – P. 532. ISBN 9780813349107.
6. New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics / [X. Huang, L. Liu, X. Li et al.] // Complexity. – 2019. – № 44. – P. 1–9. https://doi.org/10.1155/2019/6567198.
7. A pseudorandom number generator based on piecewise lo-gistic map / [Y. Wang, Z. Liu, J. Ma, H. He] // Nonlinear Dyn. – 2016. – № 83. – P. 2373–2391. https://doi.org/10.1007/s11071-015-2488-0.
8. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map / [M. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, R. Méndez-Ramírez] // Nonlinear Dyn. – 2017. – № 87. – P. 407–425. https://doi.org/10.1007/s11071-016-3051-3.
9. Zimmermann H. J. Fuzzy Set Theory – And Its Applications / H. J. Zimmermann // Springer Science & Business Media : Berlin, Germany. – 2011. – Vol. 21. – 525 p. DOI: 10.1007/978-94-015-8702-0.
10. Chakraverty S. Concepts of Soft Computing: Fuzzy and ANN with Programming / S. Chakraverty, D. M. Sahoo, N. R. Mahato // Springer : Berlin/Heidelberg, Germany, 2019. – 198 p. DOI 10.1007/978-981-13-7430-2.
11. Hanss M. Applied Fuzzy Arithmetic: An Introduction with Engineering Applications / M. Hanss. – Springer : Berlin/Heidelberg, Germany, 2005. – 270 p. DOI: 10.1007/b138914.
12. Li Z. On Fuzzy Logic and Chaos Theory: from an Engineer-ing Perspective. In Fuzzy Logic / Z. Li, X. Zhang. – A Spec-trum of Theoretical & Practical Issues; Springer : Ber-lin/Heidelberg, Germany, 2007. – P. 79–97. ISSN: 1434-9922.
13. Porto M. A fuzzy approach for modeling chaotic dynamics with assigned properties / M. Porto, P. Amato // Ninth IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2000: proceedings. – San Antonio, TX, USA, 7–10 May 2000. – Vol. 1. – P. 435–440. DOI: 10.1109/FUZZY.2000.838699.
14. Stefanini L. Simulation of fuzzy dynamical systems using the LU-representation of fuzzy numbers / L. Stefanini, L. Sorini, M. L. Guerra // Chaos Solitons Fractals 2006. – № 29. –P. 638–652. https://doi.org/10.1016/j.chaos.2005.08.096.
15. Patidar V. A pseudo random bit generator based on chaotic logistic map and its statistical testing / V.Patidar, K. K. Sud, N. K. Pareek // Informatica. – 2009. – № 33. – P. 441–452.
16. Stojanovski T. Chaos-based random number generators-part I: analysis [cryptography] / T. Stojanovski, L. Kocarev // IEEE Trans. Circuits Syst. I Fundam. Theory Appl. – 2001. – № 48. – P. 281–288. DOI: 10.1109/81.915385.
17. Pseudo-random number generator based on mixing of three chaotic maps / [M. François, T. Grosges, D. Barchiesi, R. Erra] // Commun. Nonlinear Sci. Numer. Simul. – № 19. – P. 887–895. https://doi.org/10.1007/978-3-319-06089-7_16.
18. A statistical Test Suite for Random and Pseudorandom Number Generators for cryptographic Applications / [Rukhin A., Soto J., Nechvatal J., Smid M. et al.] // Technical Report; Booz-Allen and Hamilton Inc.: Mclean, VA, USA. – 2001. DOI: 10.3390/sym12081202.
19. Alvarez G. Some basic cryptographic requirements for chaos-based cryptosystems / Alvarez G., Li S. // Int. J. Bifurc. Chaos. – 2006. – № 16. – P. 2129–2151. DOI: 10.1142/S0218127406015970.
20. Encryption of the Images on the Basis of Two Chaotic Sys-tems with the use of Fuzzy Logic / [M. Kushnir, Hr. Kosovan, P. Kroialo, A. Komarnytskyy] // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering TCSET 2020: proceedings. – Lviv-Slavsco, Ukraine. February 25–29, 2020. – P. 610–613. DOI: 10.1109/TCSET49122.2020.235504.
21. Modification of the Logistic Map Using Fuzzy Numbers with Application to Pseudorandom Number Generation and Image Encryption / Moysis L., Volos Ch., Jafari S. et al. // Entropy. – 2020. – Vol. 22. – 474 p. DOI:10.3390/e22040474.
22. A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption / Gad M., Hagras E., Soliman H. et al. // The International Arab Journal of Information Technology. – March 2021. – Vol. 18, No. 2. – P. 227–236. https://doi.org/10.34028/iajit/18/2/12.


DOI 10.15588/1607-3274-2022-1-5