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 multinode 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;
$r_{n+1}$ 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.

## 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].

\[
x_{n+1} = y_{n+1} - ax_n^2,
\]

\[
y_{n+1} = bx_n^2,
\]

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.

\[
c_{n+1} = 1 - \alpha |c_n| \cdot d_n,
\]

\[
d_{n+1} = \beta c_n,
\]

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.

\[
p_{n+1} = 1 - \mu n^2,
\]

\[
r_{n+1} = \cos(k \cos^{-1} p_{n}),
\]

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.

## 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-
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 used 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 $x_{\text{min}} = -6.3722$ to $x_{\text{max}} = 6.3699$, 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.
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

<table>
<thead>
<tr>
<th>Two-dimensional chaotic map</th>
<th>Henon</th>
<th>Lozi</th>
<th>Cross-chaotic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial conditions</td>
<td>$x_0 = 0.254$</td>
<td>$c_0 = 0.173$</td>
<td>$p_0 = 0.324$</td>
</tr>
<tr>
<td></td>
<td>$y_0 = 0.321$</td>
<td>$d_0 = 0.255$</td>
<td>$r_0 = 0.651$</td>
</tr>
<tr>
<td>Control parameters</td>
<td>$a = 0.0413$</td>
<td>$\alpha = 1.6113$</td>
<td>$\mu = 2.81$</td>
</tr>
<tr>
<td></td>
<td>$b = 0.99991$</td>
<td>$\beta = 0.5202$</td>
<td>$k = 7.73$</td>
</tr>
</tbody>
</table>

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 $x_{\text{min}} = -1.2236$ to $x_{\text{max}} = 1.38$ 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 $x_{\text{min}} = -1.1$ to $x_{\text{max}} = 0.96$ 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.
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
Table 2 – Test results of the generated sequence formed by the Henon mapping

<table>
<thead>
<tr>
<th>Statistical test type</th>
<th>The obtained $P_{value}$</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.991</td>
<td>0.980</td>
</tr>
<tr>
<td>Block Frequency</td>
<td>0.992</td>
<td>1.0</td>
</tr>
<tr>
<td>Runs</td>
<td>0.872</td>
<td>0.962</td>
</tr>
<tr>
<td>Longest Run</td>
<td>0.895</td>
<td>0.941</td>
</tr>
<tr>
<td>Rank</td>
<td>0.992</td>
<td>0.854</td>
</tr>
<tr>
<td>FFT</td>
<td>0.990</td>
<td>0.268</td>
</tr>
<tr>
<td>Non-Overlapping Template</td>
<td>0.383827</td>
<td>0.980</td>
</tr>
<tr>
<td>Overlapping Template</td>
<td>0.987</td>
<td>0.252</td>
</tr>
<tr>
<td>Universal</td>
<td>0.963</td>
<td>0.106</td>
</tr>
<tr>
<td>Linear Complexity</td>
<td>0.971</td>
<td>1.0</td>
</tr>
<tr>
<td>Serial</td>
<td>0.987</td>
<td>0.670</td>
</tr>
<tr>
<td>Approximate Entropy</td>
<td>0.989</td>
<td>0.959</td>
</tr>
<tr>
<td>Cumulative Sums</td>
<td>0.108791</td>
<td>1.0</td>
</tr>
<tr>
<td>Random Excursions</td>
<td>0.203</td>
<td>0.643</td>
</tr>
<tr>
<td>Random Excursions Variant</td>
<td>0.213</td>
<td>1.0</td>
</tr>
</tbody>
</table>

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

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

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

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

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...
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


Accepted 27.01.2022.
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 битовые 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 стат-соприкасающихся тестов.

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

Выводы. Проведенные эксперименты подтвердили способность предложенных генераторов генерировать битовые 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, псевдослучайность, нечеткая логика, статистический тест.

ЛИТЕРАТУРА