МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

Кваліфікаційна наукова
праця на правах рукопису

КРУЛІКОВСЬКИЙ ОЛЕГ ВАЛЕРІЙОВИЧ

УДК 621.391.01

ДИСЕРТАЦІЯ

Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем

05.12.13 – радіотехнічні пристрої та засоби телекомунікацій
(шифр і назва спеціальності)

05 «Технічні науки»
(галузь знань)

Подається на здобуття наукового ступеня
кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ /О.В. Круліковський/

Науковий керівник:
Політанський Леонід Францович ,
доктор технічних наук, професор

Ідентичність всіх примірників дисертації
ЗАСВІДЧУЮ:
Вчений секретар спеціалізованої
вченої ради **/І.В. Демидов /**

Чернівці - 2018

АНОТАЦІЯ

Круліковський О.В. Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.12.13 «Радіотехнічні пристрої та засоби телекомунікацій» (172 Телекомунікації та радіотехніка). – Чернівецький національний університет імені Юрія Федьковича, Національний університет «Львівська політехніка» Міністерства освіти і науки України, Чернівці, 2018.

Сучасні телекомунікаційні мережі використовують відомі та добре вивчені сигнали (М-послідовності, коди Голда, послідовності Уолша, Баркера та ін.), які не можуть забезпечити необхідну структурну прихованість та конфеденційність процесу передавання. Формування сигналів довільної ємності є актуальним науково-практичним завданням при розробленні нових радіотехнічних пристроїв.

Розроблення генераторів сигналів з підвищеною інформаційною ємністю повинно базуватись на багатовимірних нелінійних системах, оскільки це значно утруднить їхню передбачуваність і розпізнавання та даватиме змогу отримати покращені статистичні властивості, порівняно із існуючими генераторами.

Використання сучасних програмованих логікових інтегральних схем (ПЛІС) уможливлює розроблення генераторів псевдовипадкових сигналів на основі багатовимірних НДС із кільцевим зв’язком, що дає змогу мінімізувати вплив обмеження точності обчислень при розрахунках та отримувати послідовності довільної довжини при врахуванні значень кореляційної розмірності системи.

У дисертаційній роботі представлено розв’язання важливої науково-практичної задачі синтезу та практичної реалізації генераторів псевдовипадкових та випадкових послідовностей на основі багатовимірних нелінійних динамічних систем.

У першому розділі приведено аналіз аспектів використання генераторів псевдовипадкових послідовностей, висвітлено основні положення теорії

нелінійних динамічних систем. Детально розглянуто властивості хаотичних систем, що обумовлюють їх використання у системах передавання інформації.

Проведено огляд методів розширення спектру та наведено переваги таких систем зв'язку. Розглянуто набори статистичних тестів для перевірки послідовностей на відповідність критеріям псевдовипадковості.

На основі аналізу літературних джерел за тематикою роботи сформульовано завдання дисертаційних досліджень.

Другий розділ присвячений питанням аналізу та синтезу генераторів псевдовипадкових послідовностей на базі нелінійних динамічних систем, з метою уможливлення їх застосування у пристроях формування та оброблення інформаційних сигналів.

Розглянуто на прикладі логістичного відображення розв'язання проблеми повторюваності псевдохаосу шляхом збільшення середньої довжини циклу та тривалості перехідного процесу за рахунок підвищення прецизійності обчислень та введення псевдовипадкових періодичних збурень, а також переходом до багатовимірних систем.

Показано, що у випадку, якщо тривалість циклу хаотичної системи становить одну ітерацію, то збурення з періодом повторення, більшим за середню тривалість перехідного процесу є недоцільними, оскільки при цьому має місце періодичне повторення частини однієї і тієї ж траєкторії. У результаті повторення колапсу хаотичної системи системи під впливом випадкового періодичного збурення через кожні 50 ітерацій при реалізації у арифметиці Q12.9 має місце короткотривалий перехідний процес, після якого система колапсує або виходить на періодичну орбіту.

Показано, що при виборі нелінійних динамічних систем в якості бази генератора випадкових та псевдовипадкових послідовностей перевагу слід надавати таким, що характеризуються суцільною біфуркаційною діаграмою без вікон періодичності.

Показано, що при кодуванні великих обсягів інформації, початкові умови є слабшим ключем, ніж значення параметру керування оскільки різні початкові

умови призводять до однакових циклів. Період повторення послідовностей, генерованих логістичним рівнянням є суттєво меншим за максимально можливий. Встановлено, що максимальна довжина перехідного процесу становить 16775 ітерацій а потужність множини різних початкових умов після перехідного процесу дорівнює сумі довжин всіх можливих циклів та становить 24797 $\approx 2^{14}$ при використані арифметики із фіксованою комою Q3.29.

Встановлено, що використання багатовимірних систем для розв'язання проблеми циклічності є найбільш доцільним, оскільки середні тривалості циклу та перехідного процесу при виході траєкторії на цикл залежать від кореляційної розмірності.

Показано, що збільшення середньої тривалості циклу шляхом збільшення кореляційної розмірності хаотичної системи при використані програмованих логікових інтегральних схем є доцільним. Кореляційна розмірність не перевищує розмірності фазового простору хаотичної системи. Тому збільшення періоду повторення псевдохаотичної послідовності можливе шляхом збільшення розмірності фазового простору хаотичної системи.

Проведено аналіз багатовимірних систем, що відповідають вищезазначеним критеріям та встановлено, що сімейство нелінійних динамічних систем Лоці та гіперхаотична система Тратаса можуть бути використанні в якості бази ГВП та ГПВП. Для реалізації ГПВП з великими значеннями їх періоду запропоновано метод синтезу псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком, що відрізняється від відомих використанням найменш значущих бітів, що відповідають критерію збалансованості. Набув подальшого розвитку метод збільшення періоду реалізації хаотичних систем шляхом підвищення їх розмірності, який на відміну від існуючих відрізняється врахуванням кореляційної розмірності нелінійної динамічної системи та уможливлює передбачення середньої тривалості періоду повторення послідовностей.

У третьому розділі роботи представлено апаратну реалізацію генераторів псевдовипадкових послідовностей на базі багатовимірних хаотичних систем та

результати дослідження генерованих ними послідовностей на відповідність критеріям псевдовипадковості згідно набору статистичних тестів NIST.

Виконано апаратну реалізацію на ПЛІС генераторів псевдовипадкових послідовностей на основі відображення Лоці та гіперхаотичної системи Тратаса. Генеровані послідовності відповідають критеріям псевдовипадковості згідно набору статистичних тестів NIST. ПЛІС реалізація генераторів при використані чотиривимірної системи Лоці забезпечує швидкість генерування ПВП до 19,2 Гбіт/с. Встановлено, що при реалізації на ПЛІС такі системи дозволяють отримати послідовності з рівномірним розподілом для широкого діапазону значень параметрів керування. Показано, що запропонована структура генератора забезпечує паралельний розрахунок змінних, що дозволяє збільшувати швидкість генерування без часових втрат.

За допомогою чисельних методів Ейлера та Рунге-Кутти досліджено математичну модель мемристивної хаотичної системи з використанням арифметики з фіксованою комою. Проведено порівняльний аналіз ефективності чисельних методів розв'язку нелінійних диференційних рівнянь, що описують хаотичні системи. Показано, що застосування методу Рунги-Кутти не призводить до збільшення періоду повторення псевдохаотичних рядів.

Розроблено апаратне рішення методу генерування псевдохаотичних послідовностей на основі математичних моделей неперервних хаотичних систем з використанням в якості нелінійного елементу мемристивної структури, що забезпечує незалежність середньої тривалості періоду повторення в межах $10^6 \div 2 * 10^6$ ітерацій від кроку дискретизації, що становить $\Delta t = 0,0005 \div 0,02$ при умові використання арифметики з фіксованою комою Q8.16.

Четвертий розділ дисертаційної роботи присвячений дослідженню динамічних режимів роботи та схемотехнічній реалізації генераторів випадкових послідовностей на базі хаотичних систем Тратаса і Лоці.

Реалізовано і експериментально досліджено двовимірну дискретну хаотичну систему Тратаса. Схема електрична принципова генератора складається з двох симетричних частин, з'єднаних кільцевим зв'язком. Керування

параметрами контролю для зміни динамічного режиму реалізовано на змінних резисторах.

Підтверджено, що генератор хаотичних сигналів на базі системи Тратаса генерує хаотичні та гіперхаотичні коливання в широкому неперервному діапазоні значень параметрів керування. При значені параметру керування $a \to 0$, $b = 2 - a \to 2$ показано, що генератор на базі системи Тратаса може генерувати послідовності з рівномірним розподілом значень

Розроблено та практично реалізовано макет генератора сигналів на базі двовимірної системи Лоці із кільцевим зв'язком. Встановлено, що внаслідок наявності розкиду значень номіналів елементів схеми спостерігаються викиди хаотичних сигналів за межі допустимих значень. Для хаотичних коливань генерованих на основі відображення Лоці здійснено оцифрування та тестування на випадковість згідно набору статистичних тестів NIST SP 800-22.

Розроблені генератори випадкових послідовностей складаються з двонапівперіодних випрямлячів, інвертуючих суматорів, пристроїв вибірки затримки та операційних підсилювачів. Експериментальні дослідження генераторів сигналів узгоджуються з результатами моделювання.

У п'ятому розділі проведено дослідження криптостійкості методу перестановок пікселів на основі відображення Чирікова.

Розроблено та досліджено нове дискретне хаотичне відображення для перестановок пікселів в зображеннях $N \times N$ розмірності.

Представлено порівняння якості перестановок пікселів новим відображенням з іншими відомими двомірними відображеннями. Досліджено швидкість перестановок, стійкість до кореляційної атаки.

Встановлено, що при використані пропонованого відображення можна скоротити кількість циклів перестановки пікселів з врахуванням унеможливлення кореляційної атаки. Доведено, що потужність простору ключів перестановок є максимальною для растрових зображень $N \times N$ розмірності і становить $(N^2 - 1)!$.

Проаналізовано та визначено недоліки методу шифрування растрових зображень з незалежними етапами дифузії і перестановки та показано можливість розкриття шифру.

Також розроблено метод захисту зображень на основі перестановок пікселів, що базуються на модифікованому відображенні Чирікова (14) та дифузії кольору пікселів шляхом шифрування бінарними ПВП, генерованими розробленими ГПВП.

Ключові слова: нелінійні динамічні системи, генерування псевдовипадкових послідовностей, відображення із кільцевим зв'язком, перестановки, збалансованість бітів, програмовані логікові інтегральні схеми.

Список публікацій здобувача:

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Галюк С.Д. Аналіз часових рядів генерованих гіперхаотичною системою Тратаса / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 4(251). – С. 187-192.

2. Галюк С.Д.Порівняльний аналіз двомірних відображень для перестановок пікселів / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 1(245). – С. 214-220.

3. Krulikovskyi Oleh V. Image encryption algorithm based on chaotic maps / Oleh V. Krulikovskyi, Petro M. Shpatar, Leonid F. Politanskyi // Eastern European Scientific Journal. – 2014. – №6. – P. 362-366.

4. Круліковський О.В. Особливості вибору хаотичних систем для побудови генераторів псевдовипадкових послідовностей / О.В. Круліковський, С.Д. Галюк, Л.Ф. Політанський // Телекомунікаційні та інформаційні технології. – 2017. – №2. – С. 64-67.

5. Krulikovskyi O.V. Testing timeseries ring-coupled map generated by on FPGA / O.V. Krulokovskyi, S.D. Haliuk, L.F. Politanskyi // Телекомунікаційні та інформаційні технології. – 2016. – №4(53). – С. 24-29

6. Krulikovskyi O.V. PRNG based on modified tratas chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Сучасний захист інформації. – 2016. – №2. – С. 69-77.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Corinto F. Memristor-based chaotic circuit for pseudo-random sequence generators / Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // Proceedings of the 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, April 18-20, 2016. (Індексується у Scopus).

8. Haliuk S. Analysis of Pixels Permutations Based on Discretized Chirikov Map / Sergiy Haliuk, Oleg Krulikovskyi, Leonid Politanskyi // Proceedings of the XIIIth International Conference TCSET'2016, Lviv-Slavsko, Ukraine, February 23 – 26, 2016. – pp. 519-521. (Індексується у Scopus).

9. Політанський Л.Ф. Циклічність послідовностей генерованих хаотичною системою / Л.Ф. Політанський, С.Д. Галюк, О.В. Круліковський // ІІ Міжнародна конференція з інформаційно-телекомунікаційних технологій та радіоелектроніки УкрМіКо 2017. – м. Одеса, 11-15 вересня 2017 р. – С. 545-548.

10. Krulikovskyi O. Development features of cryptographic means based on chaotic systems / Krulikovskyi Oleh, Haliuk Serhii // Proceeding of the Vth International Scientific Practical Conference "PREDT 2016", 3–5 November, 2016, Chernivtsi, Ukraine. - P.125.

11. Krulikovskyi O.V. Using PRNG based on multidimensional discrete hyperchaotic system for image encryption / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // IV Міжнародна науково-практична конференція «Напівпровідникові матеріали, інформаційні технології та фотовольтаїка»: тези доповідей, м. Кременчуг. 26-28 травня, 2016 р. – С. 234-235.

12. Krulikovskyi O.V. PRNG based on discrete hyper chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Проблеми інформатики та комп'ютерної техніки: Праці V-ї Міжнародної науково-практичної конференції ПІКТ – 2016, Чернівці, Україна, 21 – 24 травня, 2016. – С. 204.

13. Image encryption algorithm based on one-dimensional and two-dimensional maps / M.Ya. Kushnir, G.V. Kosovan, O.V. Krulikovskyi // Proceeding of the II International Scientific- Practical Conferences "PREDT -2012". – Chernivtsi, October 25-27, 2012. – p. 90-91.

14. Encryption algorithm based on two-dimensional standard map / O.V. Krulikovskyi , L. F. Politanskyi // Proceeding of the IV International Scientific-Practical Conferences "PREDT -2014". – Chernivtsi, October 23-25, 2014. – pp. 68-69.

15. Круліковський О.В. Рекурентний аналіз багатовимірних хаотичних систем / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Міжнародна науково-практична конференція "ОСНП - 2017"- м. Черкаси, 24-26 травня, 2017 р. – С. 94-96.

ABSTRACT

Krulikovskyi O.V. Synthesis of pseudorandom number generators based on multidimensional nonlinear dynamical systems. - Proficiency scientific treatise on the rights of the manuscript.

A thesis submitted in fulfillment of the Candidate of Engineering Science (PhD) degree in technical sciences on specialty 05.12.13 – «Radio Engineering Devices and Telecommunication Means» (172 - Telecommunications and radio engineering). – Chernivtsi National University, Lviv Polytechnic National University of Ministry for Education and Science of Ukraine, Chernivtsi, 2018.

Modern telecommunication systems use signals with a large information capacity. Formation of signals of arbitrary capacity is an actual scientific and practical task in the development of new radio engineering devices.

The development of signal generators with increased information capacity should be based on multidimensional nonlinear systems, since this would greatly impede their

predictability and recognition and will allow for improved statistical properties compared to existing generators.

The experimental method for generating signals is the use of programmable logic integrated circuits. Therefore, it is promising to develop generators of pseudorandom sequences based on multidimensional nonlinear dynamical systems with ring communication on programmable logic integrated circuits.

The dissertation is devoted to solving an important scientific and practical problem of synthesizing signal generators with increased information capacity on the basis of multidimensional nonlinear dynamical systems.

The first section presents an analysis of the aspects of the use of pseudorandom sequence generators on the basis of nonlinear dynamical systems, the main provisions of the theory of nonlinear dynamical systems are highlighted. The properties of chaotic systems that determine their use in information transmission systems are considered in detail.

The review of existing principles of construction of information transmission systems using pseudorandom sequence generators on the basis of nonlinear dynamic systems is presented.

On the basis of the analysis of literary sources, the problem of dissertation research is formulated.

The second section is devoted to the analysis and synthesis of generators of pseudorandom sequences on the basis of nonlinear dynamic systems, in order to enable their application in devices for the formation and processing of information signals.

It is well-known that deterministic chaos takes place in analog systems. When implementing generating systems based on the FPGA, "chaotic" is lost due to a decrease in the number of possible states. An example of a logistic representation of the solution of the problem of repetition of chaotic time series is considered by increasing the average cycle length and the duration of the transition process by increasing the precision of the calculations and the introduction of pseudorandom periodic perturbations, as well as the transition to multidimensional systems.

It has been established that the duration of the period of time series generated by the logistic map using fixed-point arithmetic Q3.29 is $\sim 2^{10} \div 2^{16}$.

It is shown that if the duration of the cycle of a chaotic system is one iteration, then perturbation with a duration period greater than the average duration of the transient process is not feasible, since there is a periodic repetition of part of the same trajectory. As a result of the duration of the collapse of the chaotic system of the system under the influence of random periodic perturbation, after each 50 iterations, in the implementation of Q12.9, there is a short-term transient process, after which the system collapses or goes into periodic orbit.

Since the chaotic systems feature is a visit to their trajectories of phase space regions, with fractional values of fractal dimensions with different frequencies, as a result of which the distribution of the values of sequences generated by such systems is uneven, the mechanism of elimination is considered by neglecting the part of the bits that do not correspond to the balance criterion.

It is shown that the deviation in the aspect ratio "0" and "1" for significant bits is due to the uneven distribution of the values generated by logistic map. Established that the least significant bits are a bit of timeseries are balanced when used with fixed-point arithmetic. In the case of calculations using floating point arithmetic of the least significant bits are unbalanced due to rounding features.

It is shown that in the choice of nonlinear dynamical systems as the basis of the generator of random and pseudorandom sequences, the advantage should be given to systems characterized by a continuous bifurcation diagram without windows of periodicity.

It is shown that when encoding large volumes of information, the initial conditions are a weaker key than the value of the control parameter, since different initial conditions lead to identical cycles. The period of repetition of the sequences generated by the logistic equation is substantially less than the maximum possible. It is established that the maximum length of the transition process is 16775 iterations and the power of a set of different initial conditions after the transition process is equal to the sum of the lengths of all possible cycles $24797 \approx 2^{14}$ using fixed-point arithmetic Q3.29.

It is shown that the use of multidimensional systems to solve the problem of cyclicity is the most expedient, since the average cycles and transient cycles during the trajectory exit cycle depend on the correlation dimension.

It is shown that increasing the average cycle duration by increasing the correlation dimension of the chaotic system using programmable logic integrated circuits is appropriate.

It has been established that the family of Lozi maps and the hyperhetotic system of Tratas can be used as a RNG and PRNG.

For the implementation of PRNGs with large values of their period, a method of synthesis of pseudorandom sequences based on multidimensional mappings with a ring coupling is proposed, which differs from the known use of the least significant bits corresponding to the balance criterion, using the bitwise addition of sequences by modulo 2 and registers of linear shift. This complicates the disclosure of the state and parameters of the generator, which allows the formation of large ensemble sequences, for use in radio engineering devices and telecommunications. It is established that when implementing on FPGA such systems allow to obtain sequences with even distribution for a wide range of values.

It is shown that the proposed structure of the generator provides a parallel calculation of variables, which allows to increase the speed of generation without time losses.

The hardware implementation of pseudo-random sequences generators on the FPGA based on the reflection of the locus and the hyperthatic system of Tratas is carried out. It is found that the generated sequences pass NIST statistical tests.

The method of increasing the period of the implementation of chaotic systems by increasing their dimension, which unlike the existings one, differs by considering of the correlation dimension of the nonlinear dynamic system and allows for predicting the average duration of the sequence repetition period.

The third section of the paper presents the hardware implementation of pseudorandom sequence generators on the basis of multidimensional chaotic systems

and the results of the study of the sequences generated by them in accordance with the pseudorandomity criteria according to the set of statistical tests NIST.

Using mathematical methods of Euler and Runge-Kutta, a mathematical model of a memristor based chaotic system using fixed-point arithmetic is investigated. A comparative analysis of the efficiency of numerical methods for the solution of nonlinear differential equations describing chaotic systems is carried out. It is shown that the use of Runge-Kutta method does not increase the period chaotic timeseries.

The use of the numerical method of Euler integration is substantiated in order to increase the pseudohaotic sequence generation rate on the basis of hardware realization of mathematical models of continuous chaotic systems while maintaining the same average length of the period and statistical characteristics.

In the fourth section of the dissertation, a study of dynamic regimes and schematic implementation of generators of random sequences based on chaotic systems of Tratas and Lozi was conducted.

A two-dimensional discrete chaotic Tratas system is investigated. It is established that the generator of chaotic signals based on the Tratas system generates chaotic and hyperhetotic oscillations in a wide continuous range of values of control parameters. It is shown that a generator based on a hyperhautic system can generate a sequence with a uniform distribution of values.

The model generator of signals based on the two-dimensional Tratas system is developed and practically implemented. Electric circuit of the generator consists from two ring-coupled symmetrical parts. Control of the control parameters for changing the dynamic mode is implemented on variable resistors.

The model generator of signals based on the two-dimensional case of the Lozi ring-coupled map has been developed and practically implemented. It is shown that the generator ensures the generation of sequences with a uniform distribution of values in a wide range of variable values of control parameters.

In the fifth section, the cryptographic stability of the method of pixel permutations on the basis of Chirikov's map is investigated.

Developed and explored new discrete chaotic map for permutations of pixels in images $N \times N$ dimensionality.

The comparison of the quality of permutations of pixels with a new map with other known two-dimensional map is presented. The velocity of permutations, resistance to correlation attack are investigated.

It is established that using the proposed map, can reduce the number of cycles of permutation of pixels, taking into account the impossibility of a correlation attack. It is found that the power of the permutation keys space is maximal for raster images $N \times N$ dimension and is $(N^2 - 1)!$.

Key words: nonlinear dynamical systems, generators of pseudorandom sequences, ring-coupled maps, permutations, bit balance, FPGA.

The list of author's publications:

Proceedings where basic scientific results of thesis are published:

1. Haliuk S.D. Analysis of timeseries generated by Tratas chaotic system / S.D. Haliuk, O.V. Krulokovskyi, L.F. Politanskyi // Herald of the Khmelnitsky National University series: Technical Sciences. – 2017. – № 4(251). – pp. 187-192.

2. Haliuk S.D. Comparative analysis of two-dimensional maps for pixel permutations / S.D. Haliuk, O.V. Krulokovskyi, L.F. Politanskyi // Herald of the Khmelnitsky National University series: Technical Sciences. – 2017. – № 1(245). – pp. 214-220.

3. Krulikovskyi Oleh V. Image encryption algorithm based on chaotic maps / Oleh V. Krulikovskyi, Petro M. Shpatar, Leonid F. Politanskyi // Eastern European Scientific Journal. – 2014. – №6. – pp. 362-366.

4. Krulikovskyi O.V. Features of choosing the chaotic systems for constructing generators of pseudo-random numbers / O.V. Krulokovskyi, S.D. Haliuk, L.F. Politanskyi // Telecommunication and information technologies. – 2017. – №2. – pp. 64-67.

5. Krulikovskyi O.V. Testing timeseries ring-coupled map generated by on FPGA / O.V. Krulokovskyi, S.D. Haliuk, L.F. Politanskyi // Telecommunication and information technologies. – 2016. – №4(53). – pp. 24-29.

6. Krulikovskyi O.V. PRNG based on modified tratas chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Modern information security. – 2016. – №2. – pp. 69-77.

Proceedings that certify an approvement of thesis materials:

7. Corinto F. Memristor-based chaotic circuit for pseudo-random sequence generators / Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // Proceedings of the 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, April 18-20, 2016.

8. Haliuk S. Analysis of Pixels Permutations Based on Discretized Chirikov Map / Sergiy Haliuk, Oleg Krulikovskyi, Leonid Politanskyi // Proceedings of the XIIIth International Conference TCSET'2016, Lviv-Slavsko, Ukraine, February 23 – 26, 2016. – pp. 519-521.

9. Politanskyi L.F. Cyclicity of timeseries generated by memristor based chaotic circuit / L.F. Politanskyi O.V, Haliuk, KrulokovskyiS.D. // II International Conference on Information and Telecommunication Technologies and Radio Electronics UkrMico 2017. – Odessa, September 11-15., 2017. – pp. 545-548.

10. Krulikovskyi O. Development features of cryptographic means based on chaotic systems / Krulikovskyi Oleh, Haliuk Serhii // Proceeding of the Vth International Scientific Practical Conference "PREDT 2016", 3–5 November, 2016, Chernivtsi, Ukraine. - P.125.

11. Krulikovskyi O.V. Using PRNG based on multidimensional discrete hyperchaotic system for image encryption / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // IV International scientific and practical conference «Semiconductor materials, information technologies and photovoltaics», may 26-28, 2016., Kremenchug. – pp. 234-235.

12. Krulikovskyi O.V. PRNG based on discrete hyper chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Problems of Informatics and

Computer Engineering: Proceedings of the 5th International Scientific and Practical Conference PICT – 2016, Chernivtsi, Ukraine, may 21 – 24, 2016. – p. 204.

13. Image encryption algorithm based on one-dimensional and two-dimensional maps / M.Ya. Kushnir, G.V. Kosovan, O.V. Krulikovskyi // II International Scientific-Practical Conferences “PREDT -2012”. – Chernivtsi, 2012. – p. 90-91.

14. Encryption algorithm based on two-dimensional standard map / O.V. Krulikovskyi , L. F. Politanskyi // IV International Scientific- Practical Conferences “PREDT -2014”. – Chernivtsi, 2014. – pp. 68-69.

15. Krulikovskyi O.V. Recurrent analysis of multidimensional chaonic systems / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // International Scientific- Practical Conference "OSNP - 2017" –Cherkasy, May 24-26, 2017.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CDMA – Code Division Multiple Access;

FPGA - Field-programmable gate array;

PRNG - Pseudorandom number generator;

RNG – Random number generator;

АКФ – Автокореляційна функція;

АЦП – Аналогово-цифровий перетворювач;

ВКФ – Взаємокореляційна функція;

ГВП – Генератор випадкових посліловностей;

ГПВП – Генератор псевдовипадкових посліловностей;

НДС – Нелінійна динамічна система;

ПВП – Псевдовипадкова посліловность;

ПЛІС – Програмована логікова інтегральна мікросхема;

СПІ – Система передавання інформації;

ТКС – Телекомунікаційна система.

ВСТУП

Актуальність теми.

У зв’язку з активним розвитком інформаційних технологій зростає багатогранність та складність проблем інформаційної безпеки, збільшуються обсяги передавання, оброблення та зберігання інформації з обмеженим доступом. Відомо, що найбільш ефективними засобами захисту конфіденційних даних є кодування та зашифрування. Однак постійне покращення методів і засобів криптоаналізу та радіорозвідки зумовлює систематичне підвищення вимог до комунікаційних систем. Сучасні телекомунікаційні мережі використовують відомі та добре вивчені сигнали (М-послідовності, коди Голда, послідовності Уолша, Баркера та ін.), які не можуть забезпечити необхідну структурну прихованість та конфеденційність процесу передавання інформації. Формування сигналів довільної ємності є актуальним науково-практичним завданням при розробленні нових радіотехнічних пристроїв. Підвищення вимог до кібербезпеки та електромагнітної сумісності вимагає розвитку нових областей дослідження та розробки генераторів сигналів з великою інформаційною ємністю.

Одним із перспективних напрямків досліджень є генератори випадкових (ГВП) та псевдовипадкових (ГПВП) послідовностей на основі нелінійних динамічних систем (НДС), спектральні і статистичні характеристики яких керуються параметрами компонентів їх електричних кіл.

Значний вклад у дослідження властивостей генераторів випадкових та псевдовипадкових послідовностей на базі нелінійних динамічних систем та розв’язання проблем їх застосування у радіотехнічних пристроях і засобах телекомунікацій належить зарубіжним і вітчизняним вченим Люпчо Коцареву, Рене Лоці, Джанлука Сетті, Матвійчуку Я.М., Скобелеву В.Г., Скобелеву В.В., Васюті К.С., Захарченко М.В., Костенко П.Ю. та іншим.

На сьогоднішній день запропоновано багато алгоритмів і методів побудови ГПВП і ГВП у яких використовуються дискретні одновимірні хаотичні системи. Проте нещодавно в роботах Васюти К.С. та інших показано, що послідовності, утворені за допомогою одновимірних хаотичних систем (логістичне, квадратичне,

тентове відображення та відображення Чебишева) не забезпечують необхідного рівня прихованості передавання, оскільки можуть бути розкриті застосуванням специфічних методів нелінійного аналізу (BDS- статистики, рекурентного аналізу, фрактальних розмірностей).

Для побудови системи зв'язку необхідно використовувати два ідентичних генератори хаотичних коливань. Однак, внаслідок впливу теплових шумів та технологічних обмежень на прецизійність елементів електричних кіл, виникає проблема встановлення стійкої синхронізації. Синхронізація генераторів хаотичних коливань забезпечується при розкиді параметрів електричних компонентів, що не перевищує 1%. Реалізація ідентичних генераторів можлива в інтегральному виконанні з лазерною підгонкою на інтегральній мікросхемі. Тому технологічна складність забезпечення ідентичності рознесених генераторів хаотичних коливань обмежує їх застосування в системах зв'язку, однак НДС можуть бути використані в якості бази ГВП.

Використання сучасних програмованих логікових інтегральних схем (ПЛІС) уможливлює розроблення генераторів псевдовипадкових сигналів на основі багатовимірних НДС із кільцевим зв'язком, що дає змогу мінімізувати вплив обмеження точності обчислень при розрахунках та отримувати послідовності довільної довжини при врахуванні значень кореляційної розмірності системи.

Науково-прикладним завданням, розв'язанню якого присвячена дисертаційна робота, є синтез та практична реалізація генераторів псевдовипадкових та випадкових послідовностей на основі багатовимірних нелінійних динамічних систем.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалася відповідно до наукового напряму кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича та в межах науково-дослідницьких робіт:

"Фізико-технологічні проблеми радіотехнічних пристроїв та засобів телекомунікацій і інформаційних технологій" (Держ. реєстр. №0111U000183,

2013-2015 рр.), а також “Методи та засоби передавання, оброблення і зберігання інформації в інфо-комунікаційних системах” (Держ. реєстр. №0116U001433, 2016-2017 рр.)

Мета і завдання дослідження. Метою дисертаційної роботи є аналіз та синтез генераторів великих ансамблів псевдовипадкових та випадкових послідовностей на основі нелінійних динамічних систем.

Для досягнення поставленої мети необхідно розв’язати наступні завдання:

1. Провести ретельний аналіз сучасного стану методів побудови ГПВП та ГВП на базі нелінійних динамічних систем.
2. Дослідити статистичні властивості часових рядів, генерованих логістичним відображенням.
3. Розробити генератори псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв’язком.
4. Дослідити статистичні властивості часових рядів, що генеруються з використанням математичних моделей нелінійних динамічних систем на основі мемристивних структур при реалізації на ПЛІС.
5. Розробити схемотехнічне рішення для генераторів випадкових коливань на базі відображень Тратаса та Лоці із неперервною біфуркаційною діаграмою. Провести аналіз часових рядів, що генеруються системою Тратаса.
6. Провести аналіз перестановок пікселів на основі стандартного відображення Чирікова-Тейлора та розробити відображення для змішування пікселів в растрових зображеннях $N \times N$ розмірності з потужністю простору ключів $(N^2 - 1)!$.

Об’єктом досліджень є процес формування псевдовипадкових послідовностей на базі нелінійних динамічних систем.

Предметом дослідження є генератори псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем для радіотехнічних та телекомунікаційних систем.

Методи дослідження. Під час розв'язання поставлених завдань у роботі використовувалися методи чисельного інтегрування систем нелінійних диференційних рівнянь, нелінійної динаміки (біфуркаційні діаграми, спектри показників Ляпунова, фазові портрети), методи теорії імовірності і випадкових процесів та елементи криптоаналізу, методи рекурентного аналізу та елементи теорії алгоритмів і комбінаторики.

Наукова новизна отриманих результатів:

– Вперше запропоновано метод синтезу псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком, що відрізняється від відомих використанням найменш значущих збалансованих бітів, що дало змогу формувати великі ансамблі послідовностей, які доцільно використовувати у радіотехнічних пристроях та засобах телекомунікацій;

– Вперше запропоновано метод збільшення періоду реалізацій хаотичних систем шляхом підвищення їх розмірності, який відрізняється від існуючих урахуванням кореляційної розмірності нелінійної динамічної системи та дає змогу передбачити середню тривалість періоду повторення послідовностей;

– Удосконалено метод генерування псевдохаотичних послідовностей на основі програмної реалізації математичних моделей мемристивних хаотичних систем, який відрізняється від існуючих обґрунтованим використанням чисельного методу інтегрування Ейлера, що дає змогу збільшити швидкість генерування цих послідовностей при збереженні однакової середньої довжини періоду повторення та статистичних характеристик;

– Удосконалено двовимірне відображення Чирікова шляхом введення додаткової нелінійності, що дало змогу збільшити потужність простору ключів перестановок від N^{N-1} до $(N^2-1)!$ для матриць розмірності $N \times N$.

Практичне значення одержаних результатів:

При виконанні дисертаційної роботи отримані наступні практичні результати:

– Схемотехнічно реалізовано генератори випадкових сигналів на основі двовимірних відображень Лоці та Тратаса із кільцевим зв'язком, зі швидкістю

генерування випадкових послідовностей 0,84 Мбіт/с для двовимірної системи з частотою тактового сигналу 30 кГц. Підвищення швидкодії може бути досягнуто за рахунок інтегрального виконання генератора, що уможливлює збільшення розмірності системи та її тактової частоти.

– Досліджено періодичність розв'язків логістичного відображення реалізованого на ПЛІС із використанням арифметики з фіксованою комою Q3.29. Показано, що потужність множини різних початкових умов після перехідного процесу дорівнює сумі довжин всіх можливих циклів та становить $24797 \approx 2^{14}$. Зокрема, модифіковане багатовимірне відображення в якості бази генератора псевдовипадкових послідовностей реалізованого на ПЛІС забезпечує збільшення середнього значення періоду повторення з 2^{14} до 2^{73} при використанні шестивимірної модифікації логістичного відображення.

– Розроблено та реалізовано апаратні рішення на базі ПЛІС для генерування псевдовипадкових послідовностей зі швидкістю до 19,2 Гбіт/с чотирьохвимірними хаотичними системами. Розроблена структура генератора уможливлює формування псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком довільної розмірності.

– Розроблено апаратне рішення методу генерування псевдо хаотичних послідовностей на основі математичних моделей неперервних хаотичних систем з використанням в якості нелінійного елементу мемристивної структури, що забезпечує незалежність середньої тривалості періоду повторення в межах $10^6 \div 2 * 10^6$ ітерацій від кроку дискретизації, що становить $\Delta t = 0,0005 \div 0,02$ при умові використання арифметики з фіксованою комою Q8.16.

Отримані в дисертаційній роботі наукові та практичні результати використовуються для формування цифрових хаотичних послідовностей на базі програмованих логікових мікросхем, зокрема для передавання інформаційних сигналів у системах зв'язку (ПАТ «Укртелеком»), при дослідженнях процесів формування хаотичних коливань на базі мемристивних структур (ОКБ «Рута»), а також впроваджені в навчальний процес на кафедрі радіотехніки та інформаційної

безпеки Чернівецького національного університету імені Юрія Федьковича, що підтверджується відповідними актами впровадження.

Достовірність отриманих результатів підтверджується узгодженістю теоретичних розрахунків та результатів моделювання із експериментально отриманими даними.

Апробація результатів дисертаційної роботи.

Основні результати дисертаційних досліджень були предметом обговорень на:

– наукових семінарах кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича;

– наукових семінарах дослідницької групи «Linear and Nonlinear Circuits & Systems» (Politecnico di Torino, Torino, Italy, 2015-2016);

– 18th «Mediterranean Electrotechnical Conference» (MELECON 2016), Limassol, Cyprus, 18-20 April 2016;

– XIII Inter. Conf. on «Modern Problems of Radio Engineering, Telecommunications and Computer Science» (TCSET'2016), Lviv-Slavske, 23-26 February, 2016;

– міжнародній науково практичній конференції «Проблеми інформатики та комп'ютерної техніки» (ПІКТ 2016), м. Чернівці, 21 - 24 травня 2016 року;

– міжнародній науково практичній конференції «Напівпровідникові матеріали, інформаційні технології та фотовольтаїка» (НМІТФ-2016), м. Кременчуг, 26 - 28 травня 2016 року;

– міжнародній науково практичній конференції «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки» (PREDT -2016). – м. Чернівці, 3- 5 листопада 2016 року;

– міжнародній науково-практичній конференції «Обробка сигналів і негаусівських процесів – 2017» (ОСНП-2017). – м. Черкаси, 24-26 травня 2017 р.;

– ІІ міжнародній конференції з інформаційно-телекомунікаційних технологій та радіоелектроніки «УкрМіКо 2017».– м. Одеса, – 11-15 вересня 2017 року.

Структура та обсяг дисертації. Дисертація складається зі вступу, 5 розділів, загальних висновків, бібліографічного списку використаних джерел, 2 додатків. Загальний обсяг роботи становить 156 сторінок друкарського тексту, із них 7 сторінок вступу, 118 сторінок основного тексту, 73 рисунки, 16 таблиць, список використаних джерел з 125 найменувань, 2 додатки на 5 сторінках.

РОЗЛІЛ 1.
ГЕНЕРАТОРИ СИГНАЛІВ НА БАЗІ НЕЛІНІЙНИХ ДИНАМІЧНИХ СИСТЕМ В РАДІОТЕХНІЧНИХ ПРИСТРОЯХ ТЕЛЕКОМУНІКАЦІЙ

Сучасні високошвидкісні телекомунікаційні системи, що забезпечують високу прихованість і завадостійкість передавання інформації з обмеженим доступом, ґрунтується на використанні ансамблів сигналів із великою інформаційною ємністю, що формуються ГПВП та ГВП. Генератори сигналів з підвищеною інформаційною ємністю повинні базуватись на багатовимірних нелінійних системах оскільки це значно утруднить їхню передбачуваність і розпізнавання та дозволить отримати покращенні статистичні властивості порівняно із існуючими генераторами. Тому перспективним напрямком досліджень є розробка генераторів сигналів на базі нелінійних динамічних систем, спектральні і статистичні характеристики яких керуються параметрами компонентів їх електричних кіл [9].

Використання детермінованого хаосу в радіотехнічних засобах зв'язку вимагає забезпечення високого рівня синхронізації та широкої смуги пропускання відповідних елементів системи. Це в свою чергу обмежується технологічною складністю застосування таких засобів зв'язку оскільки синхронізація генераторів хаотичних коливань забезпечується при розкиді параметрів електричних компонентів, що не перевищує 1% [16].

Для подальшого розвитку синтезу ГПВП на базі НДС для широкосмугових засобів передавання даних, розглянемо поетапно основні положення теорії НДС, переваги їх застосування у системах передавання інформації та проведемо огляд існуючих принципів побудови ГПВП і ГВП на базі НДС.

1.1. Генератори хаотичних коливань

Хаотичні коливання – окремий клас детермінованих сигналів, породжуються НДС [17-22]. З часу відкриття Пекори та Керола можливості синхронізації двох хаотичних генераторів [23-26] стало основою для дослідження

можливостей використання хаотичних коливань в якості носійних сигналів [27] для покращення завадостійкості та стеганографічних властивостей телекомунікаційних систем. Вивчення синхронізації генераторів хаотичних коливань отримало подальший розвиток в багатьох роботах з нелінійної динаміки, зокрема в [28-36]. Інтерес до систем зв'язку з використанням генераторів сигналів на базі НДС в основному обумовлений можливістю організації прихованого передавання інформації [37-46]. Крім забезпечення прихованості зв'язку, хаотичні коливання можуть бути використанні в системах множиного доступу де загальне середовище розповсюдження використовується багатьма абонентами [27].

Генератори хаотичних коливань можуть бути побудовані на базі НДС із неперервним або дискретним часом [17, 47]. Коротко розглянемо приклади та основні властивості таких систем.

1.1.1. НДС із неперервним часом

Динамічна система із неперервним станом та неперервним часом $S = \{X, K, \mathrm{F}\}$, що залежить від параметрів, може бути задана диференціальним рівнянням [48]:

$$\frac{dx}{dt} = F(x,k),\ x \in \mathrm{X} \subseteq \mathrm{R}^d, k \in K \subseteq R^{d_K}, \qquad (1.1)$$

де: $F : X \times K \to Y$ - гладка вектор-функція, X - множина станів, K - множина параметрів керування. Для кожної початкової умови x_0 система задовольняє умові існування і єдиності розв'язку $x(t, x_0)$, де $x(0, x_0) = x_0$ [48, 16]. Крива $\varphi_t(t, x_0)$, що відповідає цьому розв'язку називається траєкторією.

З точки зору телекомунікаційних систем найбільший інтерес викликають схемотехнічно нескладні радіотехнічні схеми в яких мають місце хаотичні коливання. Одними з детально вивчених таких систем є схема Чуа та генератор Колпітца [49-52].

Схема Чуа, є одним із найпростіших генераторів хаотичних коливань, який представляє собою автоколивальну систему з 1,5 степенями свободи, що

складається з коливного контуру з втратами rLC_2, інерційної ланки RC_1 та нелінійного елементу, приведеного на схемі в вигляді нелінійної провідності [53–61] (рис 1.1).

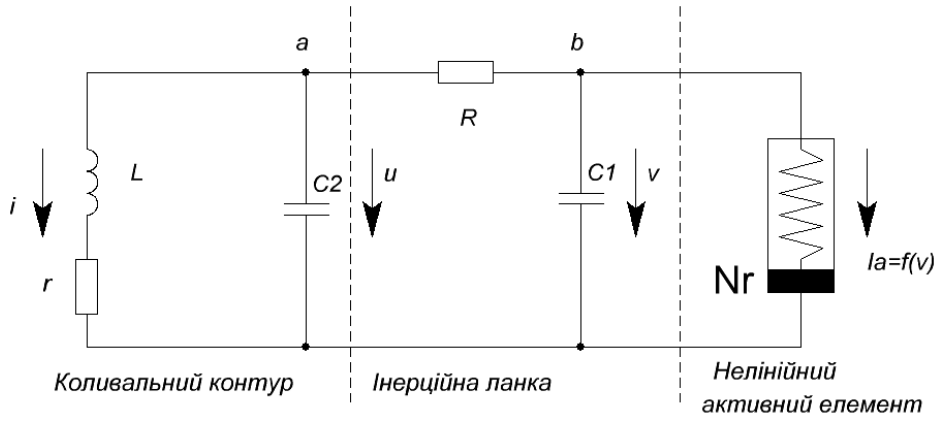


Рис. 1.1. Електрична схема генератора Чуа

Генеруючий резонансний коливний контур rLC_2 під'єднаний до активного нелінійного елементу через інерційну ланку RC_1. Поведінка системи визначається властивостями нелінійного елементу, що відіграє роль джерела живлення системи. При цьому нелінійність ВАХ (рис. 1.2) є необхідною, але недостатньою умовою для виникнення хаосу в системі.

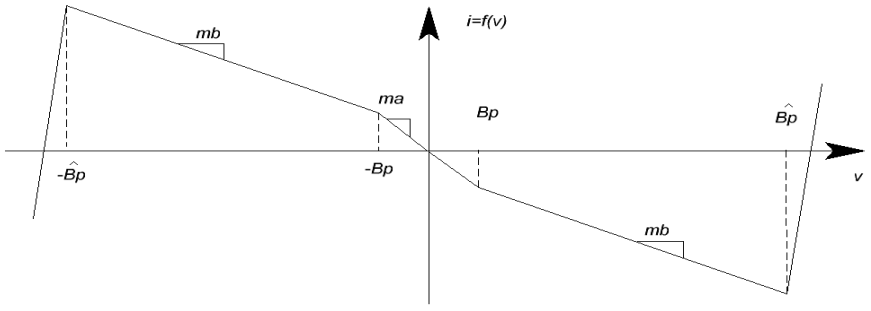


Рис.1.2. Вольт-амперна характеристика нелінійного елемента генератора Чуа

Характер хаотичних траєкторій обумовлений розсіюванням енергії на пасивних елементах R і r, що обмежує її зростання в коливному контурі. При цьому баланс енергії є досить нестійким, неперервно змінюється в часі і не повторюється як періодичне явище [62].

Складовими компонентів вектора стану системи є струм i в контурі, напруга u на ємності C_2 і напруга v на нелінійному елементі. Згідно законів Кірхгофа,

схему Чуа можна описати системою диференційних рівнянь [63]:

$$\begin{cases} L\dfrac{di}{dt} = -ri - u \\ C_2\dfrac{du}{dt} = i + \dfrac{v-u}{R} \\ C_1\dfrac{dv}{dt} = \dfrac{u-v}{R} - f(v) \end{cases} \tag{1.2}$$

де *f(v)* – значення струму, що протікає через нелінійний елемент при напрузі *v* і визначається кусково-лінійною функцією, що описує його ВАХ.

$$f(v) = m_b v + 0.5(m_b - m_a)[|v + Bp| - |v - Bp|] \tag{1.3}$$

де m_a, m_b – розмірні значення крутизни лінійних ділянок, $+Bp$, $-Bp$ – значення напруги в точках перегину нелінійної характеристики (рис. 1.2).

На базі схеми Чуа було розроблено схеми множиного доступу з кодовим розділенням (Code Division Multiple Acces - CDMA), де в якості несучих використано хаотичні коливання [64-67]. Також в роботах [64-67] показано, що сигнали генеровані такими системами крім широкосмуговості, володіють експоненціальною спадаючою кореляційною та взаємо-кореляційною функцією.

Більшість генераторів хаотичних коливань [68] із неперервним часом зокрема і схема Чуа відносяться до області частот генерування від 10 КГц до 100 МГц. Генератором хаотичних коливань, що дозволяє отримати хаотичні коливання в частотному діапазоні до декількох гігагерц відносяться триточкові схеми генераторів на біполярних транзисторах [69-75]. Однак технологічна складність забезпечення синхронізації та вимога наявності стійкого синхронізуючого сигналу для таких систем обмежжує їх застосування в телекомунікаційних системах [27]. Тому такі системи незважаючи на їх структурну простоту доцільніше використовувати в якості бази ГВП, що зокрема підтверджується нещодавно опублікованими роботами [76-78].

Зокрема в [76] запропоновано ГВП на базі широкосмугового хаотичного напівпровідникового лазеру який забезпечує швидкість генерування 640 Гбіт/с. Для формування псевдовипадкової послідовності використовувалися найменш значущі біти в бінарному представлені значень генерованих схемотехнічно

реалізованою НДС. В літературі в основному розглянуті ГВП на основі неперервних НДС. Тому в роботі проведено реалізацію ГВП на НДС із дискретним часом, оскільки вони є більш пріоритетними для цифрових інформаційно-комунікаційних систем.

1.1.2. НДС із дискретним часом

В системах дискретного часу моделю джерела хаотичних коливань в найпростішому випадку виступає різницеве рівняння першого порядку виду (1.4) [79-82]:

$$x(n+1) = f[a, x(0), x(n)] \tag{1.4}$$

де *n=0,1,2,3,...*- дискретний час, $f()$ нелінійна функція, що визначає тип відображення, a - параметр керування. Зауважимо, що (1.4) містить тільки один параметр керування хоча можливі двопараметричні одномірні відображення [79]. Дія функції $f\left[a(n), x(0), x(n)\right]$ на $x(0)$ називається ітерацією [18]. Послідовність $\{x(n)\} = \{f^n(x(0))\}$, де $n = 0,1,\ldots,\infty$ - номер ітерації, $f^n(x)$ - *n*-а ітерація функції, називають орбітою точки $x(0)$.

Для багатовимірних систем оператор відображення *T* переміщує фазову точку $x(n) = \left(x_n^{(1)}, x_n^{(2)}, \ldots, x_n^{(p)}\right)$ *p*- вимірного фазового простору в нове положення $x_n: x_n = Tx_n$. Для двовимірного відображення в декартових координатах вираз (1.4) можна записати у вигляді:

$$T_p : \begin{cases} x_{n+1}^{(1)} = f\left(x_n^{(1)}, x_n^{(2)}\right), \\ x_{n+1}^{(2)} = g\left(x_n^{(1)}, x_n^{(2)}\right) \end{cases} \tag{1.5}$$

Геометрично дискретне відображення характеризується функціональним визначником – якобіаном відображення [17]:

$$\mathbf{J_n} = \frac{\partial\left(x_{n+1}^{(1)}, x_{n+1}^{(2)}\right)}{\partial\left(x_n^{(1)}, x_n^{(2)}\right)} = \begin{vmatrix} \dfrac{\partial f(n)}{\partial x^{(1)}} & \dfrac{\partial f(n)}{\partial x^{(2)}} \\ \dfrac{\partial g(n)}{\partial x^{(1)}} & \dfrac{\partial g(n)}{\partial x^{(2)}} \end{vmatrix} \tag{1.6}$$

Якщо $|\mathbf{J}|=1$, то відображення зберігає площу, якщо $|\mathbf{J}|<1$ то відображення називають дисипативним, при $|\mathbf{J}|>1$ - розтягуючим.

НДС із дискретним часом в залежності від типу нелінійного перетворення, кількості параметрів керування, розмірності поділяються на:

- Одновимірні, що в свою чергу можуть бути одно параметричними, двопараметричними, гармонічного та поліноміального типів та відображення поліноміальних та гармонічних функцій (логістичне, кубічне, квадратичне, Бернулі, тентове і т.д.) [27];
- Багатовимірні (Пекаря, Кота, Чирікова-Тейлора, Лоці та інші) [17, 47].

Використання НДС із дискретним часом в цифрових системах зв'язку представляється зручним, оскільки дозволяє використовувати стандартні рішення на базі ПЛІС для оброблення і генерування хаотичних послідовностей.

1.2. Методи розширеного спектру

На даний час одним з найбільш перспективних напрямків досліджень є системи зв'язку із розширеним спектром [27]. Розширення спектру уможливлює збільшення бази сигналу та забезпечує підвищення ефективності передавання інформації за допомогою модульованих сигналів по каналу зв'язку із сильними завадами. Спочатку методи розширення спектру застосовувалися для військових систем управління і зв'язку та для боротьби із електромагнітними завадами. В подальшому розвиток методів розширення спектру отримав при розробці завадостійких систем зв'язку.

Суть методів розширеного спектру полягає у використані смуги передавання сигналу, набагато ширшої від мінімально необхідної для передавання інформації.

Система зв'язку називається системою з розширеним спектром в наступних випадках [83]:

1. Використовуванна смуга набагато більша мінімальної бази сигналу необхідної для передавання інформації.

2. Розширення спектру здійснюється за допомогою сигналу розширення, який не залежить від інформації.

3. Відновлення вихідних данник приймачем здійснюється шляхом співставлення отриманого сигналу і синхронізованої копії сигналу розширення.

В існуючих на сьогодні системах зв’язку із розширеним спектром використовують наступні методи:

- Псевдовипадкове переналаштування робочої частоти (*frequency-hopping spread spectrum*). Суть методу полягає в періодичній зміні значення несучої частоти згідно алгоритму відомому приймаючій та передавальній стороні. Такий метод використовуються в Bluetooth. Перевагою цього методу є простота реалізації, а недоліком затримка в потоці даних при кожній зміні несучої частоти.
- Розширення спектру методом прямої послідовності (*direct sequence spread spectrum*) Суть методу полягає в підвищенні тактової частоти модуляції, при цьому кожному символу повідомлення ставиться у відповідність відома псевдовипадкова послідовність. Метод використовується в системах стільникового зв’язку CDMA і Wi-Fi. По ефективності даний метод переважає метод розширення спектру за допомогою псевдовипадкового переналаштування робочої частоти.
- Розширення спектру методом лінійної частотної модуляції (*chirp spread spectrum*). Суть методу полягає в переналаштувані несучої частоти по лінійному закону. Даний метод використовується в радіолокації.

Переваги систем із розширеним спектром є:

- На сигнал слабо впливають завади.
- Розширення спектру дозволяє приховувати і шифрувати сигнали.
- Декілька користувачів можуть одночасно використовувати одну смугу частот.

Системи зв’язку з розширеним спектром із передаванням опорного сигналу можуть використовувати випадкові кодові сигнали розширення і стиснення, оскільки кодовий та модульований інформаційним кодовий сигнал одночасно передаються в різних областях спектру [83]. Метод зберігання опорного сигналу

не дозволяє отримувати істино випадкові сигнали, оскільки кодовий сигнал повинен зберігатися або генеруватися на приймальній стороні.

Розширюючі спектр послідовності сучасних систем зв’язку з множиним доступом є добре відомими (М-послідовності, коди Голда, послідовності Уолша, Баркера та ін.) поступово втрачають свою актуальність для забезпечення надійного конфіденційного зв’язку. Зростаючі вимоги до електромагнітної сумісності, кібербезпеки, тенденція до зменшення потужності джерел електромагнітного випромінювання обумовлюють доцільність поєднання етапів кодування і шифрування інформації з використанням ПВП. Джерелами таких послідовностей можуть бути неперервні або дискретні НДС.

1.3. Набір статистичних тестів NIST

Для дослідження статистичних властивостей генерованих послідовностей на відповідність критеріям псевдовипадковості використовують статистичні тести [84]. До статистичних тестів відносяться набори тестів розроблених Дональдом Кнутом, DIEHARD, NIST, FIPS та AIS [85, 86].

Статистичні тести використовують для перевірки певної нульової гіпотези H_0 щодо випадковості сформованої послідовності. З гіпотезою H_0 пов'язана альтернативна гіпотеза $H_{алт}$. про те, що послідовність не випадкова. Для кожного тесту, можна зробити висновок щодо прийняття чи відхилення нульової гіпотези, виходячи із сформованої генератором послідовності. При цьому для кожного тесту та послідовності має бути вибрана адекватна статистика випадковості, на основі якої може бути прийнято або відхилено нульову гіпотезу. Теоретично для нульової гіпотези розподілення статистики визначається математичними методами. При проведенні тесту розраховується значення тестової статистики, яке порівнюється з критичним. Якщо значення тестової статистики перевищує критичне, нульова гіпотеза відхиляється, в іншому випадку – приймається [87].

Зазвичай для тестування послідовностей використовують набори статистичних тестів FIPS та NIST SP 800-22. В переважній більшості робіт для

комплексного тестування послідовностей використовується набір статистичних тестів NIST SP 800-22. Такий вибір зумовлений тим, що даний набір пропонує критерії прийняття рішення відносно не тільки окремої послідовності, але й відносно всього ГПВП. Додатковим фактором вибору цієї методики є позитивний досвід її використання при дослідженні статистичних властивостей криптоалгоритмів, що висувалися на національний стандарт держав НАТО [86].

Набір статистичних тестів NIST розроблений Національним інститутом стандартизації США. Набір налічує 15 тестів. Якщо послідовність проходить всі тести, тоді вона вважається криптографічно стійкою [85].

Приведемо короткий огляд тестів [85].

1. Частотний (монобітний) тест.

Метою цього тесту є оцінка пропорції нулів та одиниць в заданій послідовності. У тесті здійснюється перевірка, чи буде кількість нулів та одиниць у досліджуваній послідовності приблизно така ж, як у справжньої випадкової послідовності. Тест оцінює чи кількість одиниць до близька до ½. Імовірність відхилення у пропорції одиниць оцінюється за допомогою критерію Пірсона (хі-квадрат статистики).

2. Частотний по блоковий тест.

Задачею тесту є оцінка співвідношення різних біт в М-бітових блоках. У тесті перевіряється, чи буде кількість одиниць в середині кожного блоку приблизно рівною М/2, як це повинно бути для справжньої випадкової послідовності.

3. Тест серій.

Серією називають неперервну послідовність з однакових бітів. У тесті здійснюється оцінка кількості різних серій в усій тестовій послідовності. Метою тесту є порівняння, кількості серій в досліджуваній та випадковій послідовності біт. Для проходження тесту наявні відхилення повинні знаходитися в допустимих межах. Також можна сказати, що цей тести виявляє швидкість і частоту коливань між нулями і одиницями в послідовності.

4. Пошук найдовшої серії з одиниць.

У тесті досліджуються М-бітові блоки, у кожному з яких шукається найдовша серія з одиниць. Результати порівнюються з очікуваними для дійсно випадкової послідовності.

5. Тест рангу бінарних матриць.

У тесті із заданої послідовності формуються квадратні бінарні матриці. Для кожної матриці шукається її ранг. Відомо, що ранг матриці є кількісною оцінкою лінійної залежності між її рядками. Якщо ранг матриці менший за кількість її рядків, тоді це означає що окремі рядки залежні між собою, а сама послідовність не є випадковою.

6. Тест на основі дискретного перетворення Фур'є.

У тесті виконується швидке перетворення Фур'є над вхідною послідовністю. Наявність у спектрі компонентів, що значно відрізняються за амплітудою говорить про ознаки періодичності тестової послідовності.

7. Тест шаблонів без перекриття.

У цьому тесті у послідовності шукається наперед заданий шаблон. Якщо послідовність бітів відповідає шаблону, то аналізуються наступні біти після нього. Якщо шаблон відрізняється від поточної послідовності, то пошук зсувається на один біт, і знову здійснюється порівняння, і т.д. Підрахована кількість співпадінь порівнюється з аналогічною для випадкової послідовності.

8. Тест шаблонів з перекриттям.

Від попереднього цей тест, відрізняється тим, що навіть при співпадінні шаблону вікно зсувається на один біт.

9. Універсальний тест Мауера.

Метою тесту є оцінка можливості стиснення послідовності шляхом підрахунку кількості біт між співпадаючими шаблонами. Якщо послідовність невипадкова – вона може бути значно стиснена без втрат.

10. Тест лінійної складності.

В тесті здійснюється розрахунок довжини лінійного регістра зсуву, який може згенерувати задану послідовність. Якщо послідовність є складною, то довжина регістра буде великою.

11. Тест серій.

У тесті серій обчислюється частота випадання усіх можливих m-бітних шаблонів з перекриттям. Для випадкової послідовності ця кількість буде приблизно рівно ймовірною.

12. Тест ентропії.

У тесті на ентропію підраховується частота випадання усіх можливих m та (m+1)-бітних шаблонів з перекриттям. Результати порівнюються з очікуваними для справжньої випадкової послідовності.

13. Тест накопичених сум.

В тесті початкова послідовність нулів і одиниць перетворюється на послідовність «1» і «-1». Далі розраховується починаючи з першого сума чисел і виявляються її максимальні значення. Для випадкової послідовності ці відхилення повинні бути невеликими.

14. Тест випадкових відхилень.

Тест подібний до попереднього з різницею в тому, що обчислюється кількість перетинів суми рівнів -4, -3, -2, -1, 1, 2, 3, 4 і порівнюється з очікуваною для випадкової послідовності.

15. Тест випадкових відхилень - 2.

Всі нулі у тестовій послідовності заміняються на мінус одиниці. Інтегральна сума послідовності вважається випадковим відхиленням. У тесті обчислюється кількість досягнень інтегральною сумою станів -9, -8, …, -1, 1, 2, …, 9 і порівнюється з очікуваною для випадкової послідовності.

1.4. ГПВП в телекомунікаційних системах

ГПВП використовуються в телекомунікаційних системах [83] для генерування псевдовипадкової гамми в блокових та потокових методах зашифрування, а також для формування широкосмугових сигналів [84].

Псевдовипадкові послідовності сучасних телекомунікаційних систем формуються апаратно реалізованими схемами, що базуються на:

- регістрах зсуву з лінійним оберненим зв'язком [83],
- лінійних конгруентних методах [84],
- методі Блюм-Блюм-Шуба [88],
- розв'язках системи нелінійних диференційних рівнянь (схема Чуа, система Лоренца і т.д.) [45];
- розв'язках системи одно- або багатовимірних рекурентних відображень (логістичне відображення, тентове, зсуву і т.д.) [45, 89-90].

Суть лінійного конгруентного методу полягає в обчислені послідовності псевдовипадкових чисел x_n за наступним рекурентним рівнянням [91]:

$$x_{n+1} = (ax_n + c) \bmod m \tag{1.7}$$

де m - модуль (натуральне число, відносно якого обчислюють остачу від ділення), a - множник, c - доданок. Числа c і m повині бути взаємопростими.

Хоча лінійні конгруентні методи дозволяють генерувати послідовності із хорошими псевдовипадковими властивостями, однак вони не є криптографічно стійкими. Генератори послідовностей на базі лінійного конгруентного методу були зламані Джимом Рідсом та вподальшому розширені на всі типи лінійних конгурентних методів [92].

Криптографічно стійким генератором псевдовипадкових послідовностей є метод Блюм-Блюм-Шуба. Суть даного методу полягає в обчислені послідовності чисел x_n за наступним рекурентним рівнянням [88, 92]:

$$x_{n+1} = x_n^2 \bmod M \tag{1.8}$$

де $M = pq$ - добуток двох великих простих чисел. Псевдовипадкова послідовність отримується на кожному кроці із x_n шляхом взяття біта парності або обного і більше найменш значущих бітів в бінарному представлені x_n. Числа p і q повинні прирівнюватися 3 по модулю 4. Основним обмежуючим фактором застосування цього генератора є його низька швидкодія, що обумовлена використанням великих чисел.

Серед систем генерування на базі НДС найбільш поширеними є генератори на основі одновимірних систем, зокрема логістичному відображенні, що задається ітераційним рівнянням [91]:

$$x_{n+1} = r x_n \left(1 - x_n\right) \tag{1.9}$$

де r — параметр керування, n – номер ітерації, x_{n+1} – змінна, яка може приймати значення з діапазону [0; 1]. На основі відображень такого типу способом отримання за допомогою псевдовипадкової послідовності є пороговий метод [95], згідно якому фазовий простір системи поділяється на дві незалежні області, що відповідають двійковим символам «0» або «1»:

$$X\left(n\right) = \begin{cases} 0, & x_n \le x_{П} \\ 1, & x_n > x_{П} \end{cases}, \tag{1.10}$$

де $x_{П}$ – порогове значення.

Отримана згідно (2.2) ПВП $X\left(n\right)$ є грубою оцінкою хаотичної траєкторії $x(n)$. Недоліком порогового методу є залежність статистичних характеристик послідовності $X\left(n\right)$ від вибору порогового значення $x_{П}$. В [93] пропонується вибирати $x_{П} = 0.5$. Проте в [94] показано, що внаслідок нерівності розподілу значень $x\left(n\right)$ такий вибір порогу $x_{П}$ не може забезпечити отримання збалансованих послідовностей і запропоновано використовувати динамічний режим вибору порогового значення в залежності від параметру керування. Також на основі розв’язків систем одно- або багатовимірних рекурентних відображень (логістичне відображення, тентове, зсуву і т.д.) запропоновано різноманітні методи захисту зображень шляхом переведення розв’язків системи із області дійсних чисел в діапазон восьмибітних цілих чисел [91].

Нещодавно показано, що врахування топологічних властивостей хаотичних коливань у фазовому просторі при використанні методів нелінійного аналізу (BDS- статистики, рекурентний аналіз, фрактальні розмірності) для одновимірних відображень уможливлює розрізнення хаотичного сигналу та встановлення параметрів системи [96-98].

Незважаючи на різноманіття не всі НДС можуть бути використані в якості бази ГПВП, що обумовлено наступними вимогами [17, 27]:

- простота реалізації для можливості використання різноманітних платформах. Наприклад, поліноміальні відображення, що використовують піднесення в дробові степені використовувати недоцільно через наявність складних арифметичних операцій;
- відсутність початкових умов які з часом призводять до до нульової реалізації вихідного сигналу. Тому тентове відображення і відображення зсуву не розглядалися [17];
- нелінійні функції відображень повині бути взаємно неоднозначними;
- хаотичні режими повині бути стійкими і виникати в незалежності від початкових умов.

Висновки до першого розділу

Синтез апаратних ГПВП на базі НДС та застосування їх для формування псевдовипадкових послідовностей і є актуальною задачею в радіотехнічних пристроях та засобах телекомунікацій. На базі проведеного аналізу науково-технічних публікацій та результатів експериментальних досліджень можна зробити наступні висновки:

1. З порівняльного аналізу генераторів сигналів на базі НДС випливає, що генератори сигналів на базі НДС можуть забезпечити синтез широкосмугових сигналів із покращеними статистичними характеристиками.

2. Більшість НДС не є придатними для використання в якості бази ГПВП. Тому затребуваним є синтез нових радіотехнічних НДС для систем передавання інформації.

3. Існують суттєві невирішені проблеми практичної реалізації систем передавання інформації на основі генераторів хаотичних коливань, повязанні із технологічною складністю забезпечення ідентичності параметрів електроних компонент приймальної і передавальної частини.

4. Послідовності генеровані регістрами зсуву з лінійним оберненим зв’язком є відомими, що обмежує їх застосування для телекомунікаційних систем.

5. Існує нагальна потреба в синтезі високошвидкісних ГПВП та ГВП на базі багатовимірних НДС для генерування ансамблів сигналів із підвищеною інформаційною ємністю.

Проаналізувавши літературні джерела, виявлено наступні задачі, що розглядаються і вирішуються в роботі:

1. Дослідити статистичні властивості часових рядів, генерованих логістичним відображенням.

2. Розробити генератори псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком.

3. Дослідити статистичні властивості часових рядів, що генеруються з використанням математичних моделей нелінійних динамічних систем на основі мемристивних структур при реалізації на ПЛІС.

4. Розробити схемотехнічне рішення для генераторів випадкових коливань на базі відображень Тратаса та Лоці із неперервною біфуркаційною діаграмою. Провести аналіз часових рядів, що генеруються системою Тратаса.

5. Провести аналіз перестановок пікселів на основі стандартного відображення Чирікова-Тейлора та розробити відображення для змішування пікселів в растрових зображеннях $N \times N$ розмірності з потужністю простору ключів $(N^2 - 1)!$.

РОЗДІЛ 2.
АНАЛІЗ ТА СИНТЕЗ ГПВП НА БАЗІ БАГАТОВИМІНИХ НДС

2.1. Дослідження дискретних детермінованих НДС в якості бази ГПВП

При переході до апаратно-програмної реалізації процесів на базі ЕОМ внаслідок зменшення множини можливих станів хаотичні системи втрачають «хаотичність», а їх реалізації є псевдохаотичними і циклічними [95]. Для мінімізації впливу цього фактору необхідно використовувати максимально можливу точність обчислень платформи та враховувати швидкодію таких рішень. Неповна відповідність базових програмно-апаратних носіїв часто призводить до неможливості відтворення ідентичних псевдохаотичних реалізацій на різних платформах (різні ОС, мови програмування, компілятори, різні виробники ПЛІС).

При виконанні арифметичних операцій над дійсними числами у арифметиці з плаваючою комою [47-48] має місце фактор різних значень похибки заокруглення, який внаслідок чутливості нелінійних систем призводить до розбігання траєкторій для різних програмно-апаратних засобів та компіляторів. Тому для уникнення різних похибок заокруглення доцільно використовувати для обчислень арифметику з фіксованою комою [48].

Апаратно реалізовані рішення з використанням арифметики з фіксованою комою уможливлюють рознесене отримання однакових значень хаотичних сигналів (у тому числі з довільними часовими затримками), що уможливлює синтез генераторів псевдовипадкових послідовностей для широкосмугових засобів зв’язку.

2.1.1. Розподіл хаотичних реалізацій

Особливістю хаотичних систем є різна частота відвідування їх траєкторіями різних областей фазового простору, що характеризується дробовими значеннями фрактальних розмірностей. Наслідком цього є нерівномірний розподіл значень послідовностей, генерованих такими системами.

На прикладі логістичного рівняння (1.9) вкажемо на проблемні питання використання одновимірних систем, як бази ГПВП. Гістограма розподілу значень

часових рядів, отриманих за допомогою (1.9) (рис. 2.1) є нерівномірною у всьому діапазоні значень параметру r, що є небажаним для реалізації якісних криптографічних засобів. Безпосереднє використання розв'язків (1.9) як псевдовипадкових чисел, обумовлює їх нестійкість до статистичних атак [99].

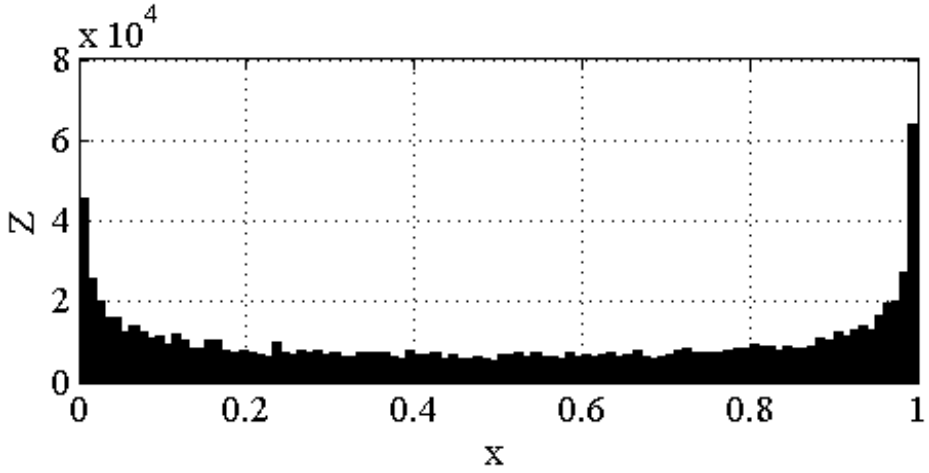


Рис. 2.1. Гістограма значень часових рядів генерованих (2.1) при $r = 3.999$, $n = 1000000$.

Найпростішим способом отримання за допомогою (1.9) псевдовипадкової послідовності є пороговий метод [93] згідно якому фазовий простір системи поділяється на дві незалежні області, що відповідають двійковим символам «0» або «1».

На рис. 2.2 приведено залежність відсотка символів «1» у послідовності, отриманій згідно (1.9) і (1.10) від значення параметру керування r.

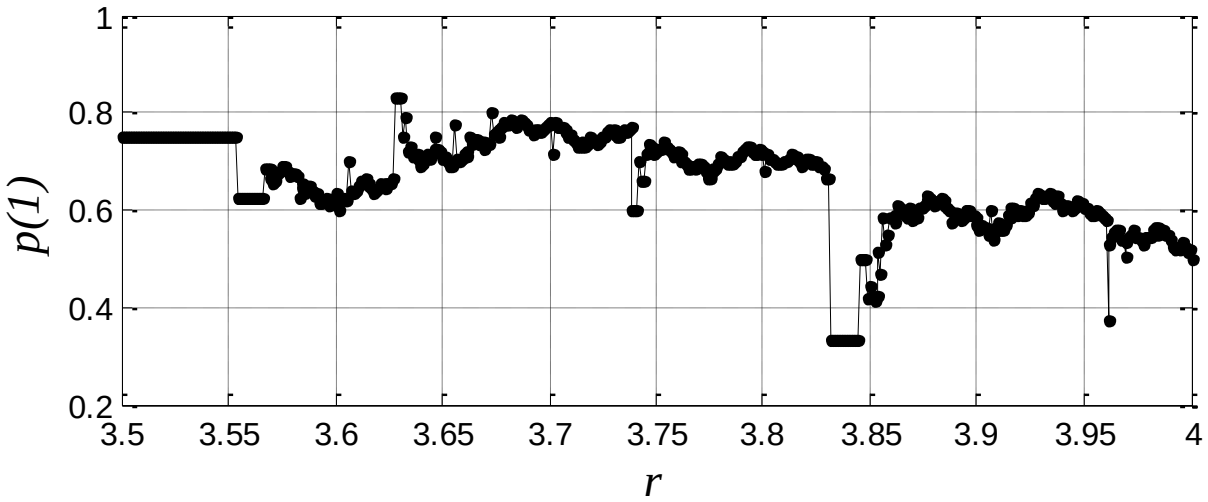


Рис. 2.2. Залежність ймовірності отримати символ «1» пороговим методом при $x_{П} = 0.5$ від параметру керування r.

Як бачимо, частки символів «0» і «1» при виборі порогу $x_{П} = 0.5$ значно різняться, що вказує на незбалансованість послідовності $X(n)$.

Усунути недолік порогового методу можна динамічним вибором порогу, як медіани розподілу при заданому значені параметру керування (рис. 2.3).

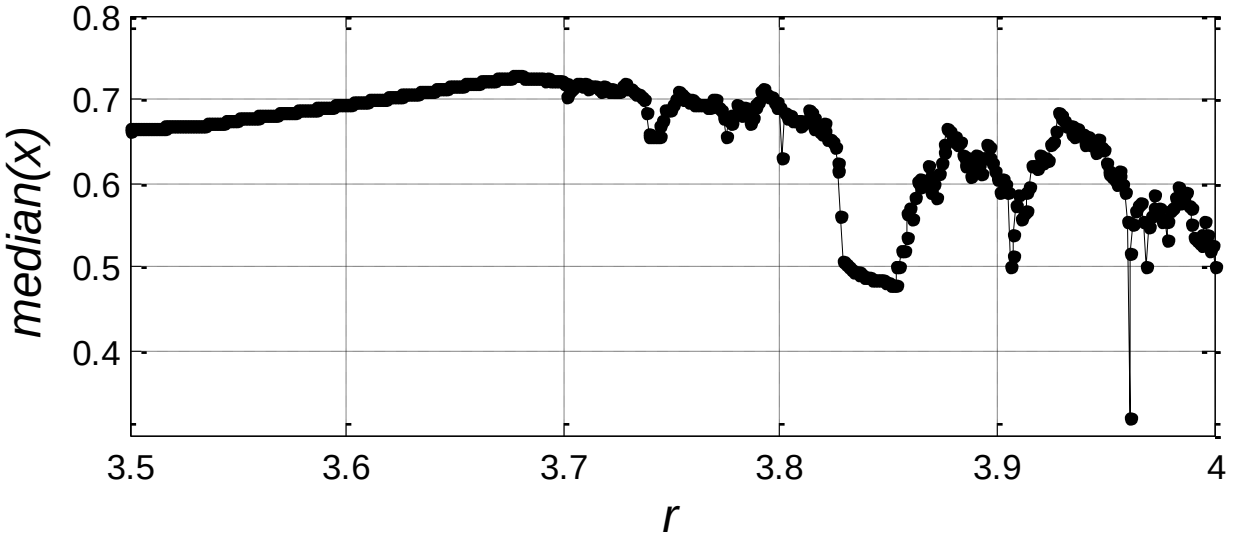


Рис. 2.3. Залежність медіани розподілу реалізацій системи (2.1) від параметру керування *r*.

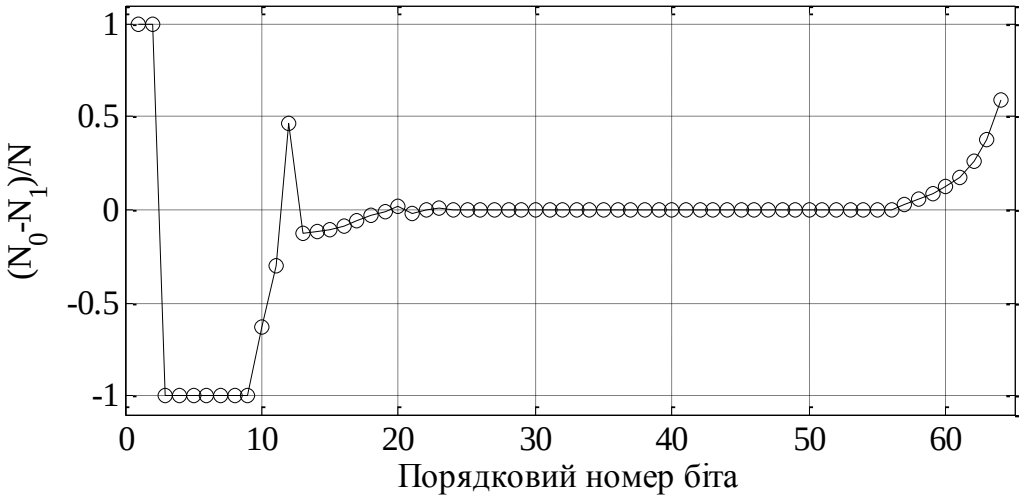
Недоліком порогового методу також є низька швидкість генерування ПВП, оскільки за одну ітерацію можливо отримати тільки один біт послідовності. Збільшити швидкість генерування ПВП можна шляхом бітового представлення хаотичних чисел.

Гістограму будь-якої хаотичної системи при програмній реалізації на ЕОМ формують значущі біти двійкового представлення даних. Відкинувши частину біт, що не відповідають критерію збалансованості, можна отримати послідовності з рівномірним розподілом. Розглянемо особливості бітового представлення чисел при розрахунках з фіксованою та плаваючою комою і подвійною точністю. Сформуємо матрицю з розмірністю $n \times m$ з елементами $l_{n,m}$.

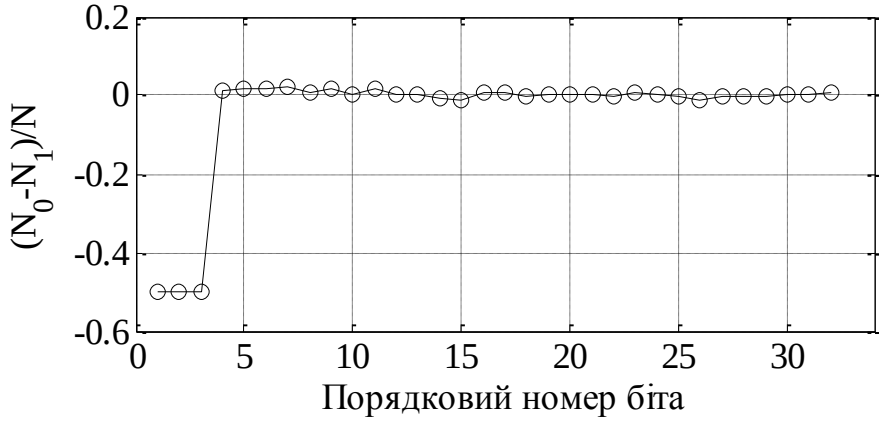
$$\begin{cases} l_{11} \; . \; l_{12} \; \ldots \; l_{1,\,m} \\ l_{21} \; . \; l_{22} \; \ldots \; l_{2,\,m} \\ \quad . \quad . \quad \ldots \quad . \\ l_{n,1} \; . \; l_{n,2} \; \ldots \; l_{n,\,m} \end{cases} \tag{2.1}$$

де n – номер ітерації x_n, а m – порядковий номер біта в бінарному представленні дійсного числа.

Для кожного стовпця обчислюється кількість нулів “0” - N_0 та одиниць “1” - N_1, $(N_0 + N_1 = N)$. Залежності відносної різниці кількості «0» і «1» від номера двійкового символу у числі приведено на рис. 2.4.



а



б

Рис. 2.4. Збалансованість послідовностей для логістичного рівняння при r = 3.999 для подвійної точності – *а*; арифметики Q3.29 – *б*.

Як випливає із рис. 2.4 *а*, для подвійної точності найбільш значущі біти, які формують хаотичний атрактор (2.1) є незбалансованими. Відхилення в пропорції «0» і «1» для найменш значущих бітів обумовлена особливостями округлення в арифметиці з плаваючою комою. Молодші біти збалансовані при реалізації логістичного відображення на ПЛІС та у комп’ютерних обчисленнях з

використанням арифметики з фіксованою комою (рис. 2.4 *б*). Приклад отримання рівномірного розподілу чисел, отриманих на основі реалізацій (2.1) шляхом відкидання старших 15 біт, приведено на рис. 2.5.

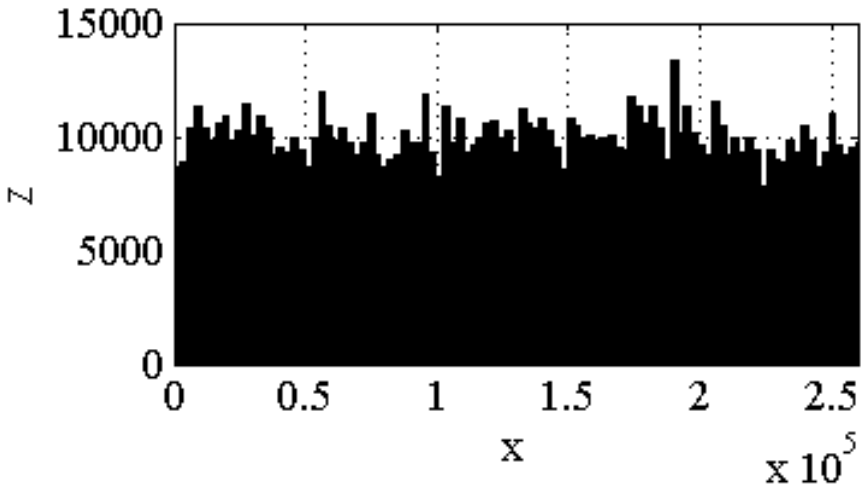


Рис. 2.5. Гістограма значень часових рядів генерованих (2.1) при r = 3.999, n=1000000 при відкиданні старших 15 біт при Q3.29.

Хаотичні сигнали можна отримати тільки в аналоговій динамічній системі [48]. При комп'ютерному моделюванні незалежно від формату обчислень, отримані реалізації хаотичних сигналів будуть псевдохаотичними, тобто будуть повторюватися (період повторення може бути великим) оскільки ЕОМ характеризуються скінченою кількість станів [95].

При великому періоді повторення розв'язки хаотичної системи зберігатимуть розмірність, ергодичність та властивості справжнього атрактора. Це дає змогу досліджувати хаотичні системи шляхом їх моделювання [17]. Кількість циклів при одному значенні параметру є обмеженою, внаслідок того що велика кількість траєкторій, формованих при різних початкових умовах, після закінчення перехідного процесу виходять на однакові дискретні періодичні орбіти [47]. Внаслідок циклічності псевдохаотичної послідовності об'єм інформації, що підлягає за шифруванню та простір ключів методу є обмеженими.

Вирішення проблеми усунення повторюваності псевдохаосу можливе за рахунок збільшення середньої довжини циклу і тривалості перехідного процесу, шляхом збільшення прецизійності обчислень, введенням псевдовипадкових періодичних збурень та переходом до багатовимірних систем.

Апаратне збільшення точності обчислень можливлене при використанні дорого вартісних пристроїв, що є суттєвим стримуючим фактором, а програмна реалізація вимагає збільшення часових затрат.

Ефективність періодичних збурень залежить від властивостей системи, до якої вони застосовуються, характеру збурень та частоти їх дії. Для прикладу розглянемо логістичного відображення (1.9), у випадку якщо тривалість циклу хаотичної системи становить одну ітерацію [100], збурення з періодом повторення більшим за середню тривалість перехідного процесу є недоцільні, оскільки вони призведуть до періодичного повторення частини однієї і тієї ж траєкторії. Часову реалізацію системи (1.9) у арифметиці Q12.9 під впливом випадкового періодичного збурення через кожні 50 ітерацій приведена на рис. 2.6.

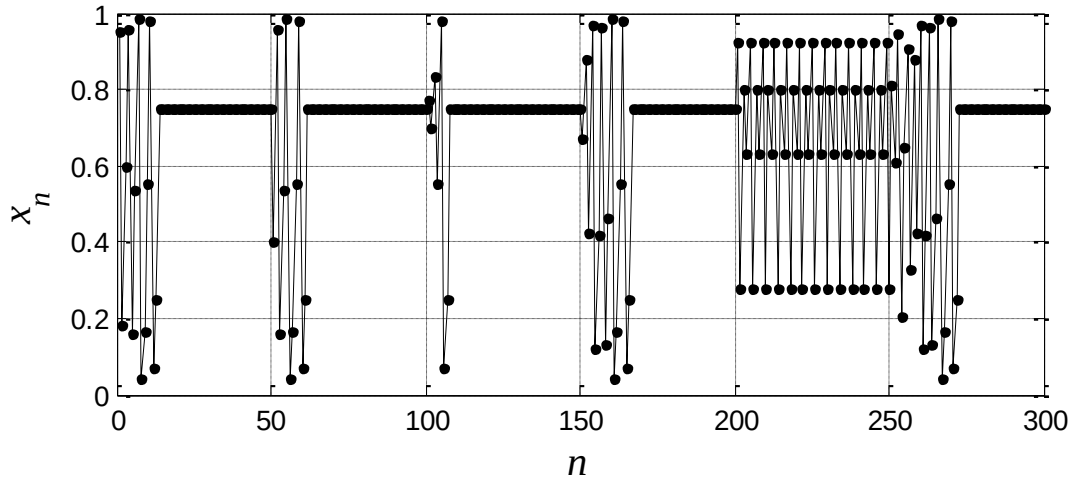


Рис. 2.6. Повторюваність колапсу при випадкових періодичних збуреннях через кожні 50 ітерацій

Із рис. 2.6 випливає, що дія збурення викликає короткий перехідний процес, після якого система колапсує або виходить на періодичну орбіту. Подібна ситуація матиме місце, у випадку, якщо середня тривалість циклів менша за період впливу збурення.

2.1.2. Періодичність часових рядів логістичного відображення при обмеженій точності обчислень арифметики Q3.29

Вплив точності представлення чисел на криптостійкість методів шифрування данних частково досліджено в роботі [101]. В [102] шляхом

чисельного моделювання показано, що заокруглення чисел при ітеруванні хаотичної системи призводить до виникнення періодичних коливань. При цьому період повторення є значно меншим за розмір множини можливих станів системи. Періодичність реалізацій оцифрованих хаотичних систем є причиною зменшення потужності множини значень початкових умов та параметрів керування.

При проведенні розрахунків у форматі з фіксованою комою множина розв'язків є кількістю чисел, що відрізняються не менше ніж в одному двійковому розряді, що дорівнює 2^{m+d}, де m і d – розрядність представлення відповідно дробової та цілої частини числа (включно зі знаком). Якщо розрахунки проводяться з плаваючою комою, то періодичність розв'язків залежатиме від особливостей апаратного і (або) програмного забезпечення.

Незважаючи на те, що проблема впливу прецизійності обчислень на властивості реалізацій хаотичних систем відома, часто вона не враховується при здійсненні оцінки криптостійкості пропонованих методів.

Результати дослідження періодичності для різних значень параметру керування r при використані арифметики з фіксованою комою Q3.29 приведено у табл. 2.1.

При моделюванні задано 10^5 випадкових початкових умов з рівномірним розподілом їх значень. Період повторення послідовностей генерованих (1.9) є суттєво меншим за максимально можливий. Після закінчення перехідного процесу при $m = 32$ кількість різних послідовностей які можна згенерувати за допомогою (2.1) обмежена і не залежить від початкових умов. Це означає, що використання початкових умов як ключа в окремих криптографічних алгоритмах не завжди доцільно.

Для різних значень r з табл. 2.1. випливає, що зміна параметру керування не призводить до суттєвої зміни періоду циклів, проте змінюється генерована послідовність. Якщо аналізувати хаотичну послідовність утворену за допомогою (2.1) після закінчення перехідного процесу, то більш інформативним буде значення параметру r, а не початкова умова $x(0)$.

Таблиця 2.1

Довжини періодів логістичного відображення

Значення параметра, *r* (у шістнадцятковій системі числення)	L	Кількість ПУ
80000000	6876	94672
	571	1086
	379	4206
	327	36
7fffffff	14561	58534
	4133	16435
	3331	18174
	1499	6442
	932	373
	193	34
	82	7
	13	1
7ffffffe	9215	97141
	4627	2091
	2564	680
	488	25
	300	42
	289	13
	136	3
	129	3
	17	2
7ffffffd	11078	51659
	3167	32673
	1230	651
	1177	14681
	362	317
	77	5
	29	2
	21	11
	13	1

Для систем з безмежною точністю обчислень чутливість до початкових умов і значень параметрів є рівнозначними в розумінні, що збурення обох призводять до різних реалізацій хаотичного процесу. При обмеженнях на точність обчислень з точки зору хаотичної криптографії можна зробити висновок, що чутливість до значень параметрів є вищою ніж до початкових умов. Це необхідно враховувати при розробленні хаотичних алгоритмів шифрування. Більше того, програмно

реалізовані хаотичні системи є нечутливими до початкових умов, що відрізняються на мінімально можливу величину 2^{-m} якщо після однієї чи кількох ітерацій їх траєкторії повністю співпадають.

Максимальна довжина перехідного процесу системи (1.9) при $r=4-2^{-29}$ та Q3.29 становила 16775 ітерацій (рис. 2.7).

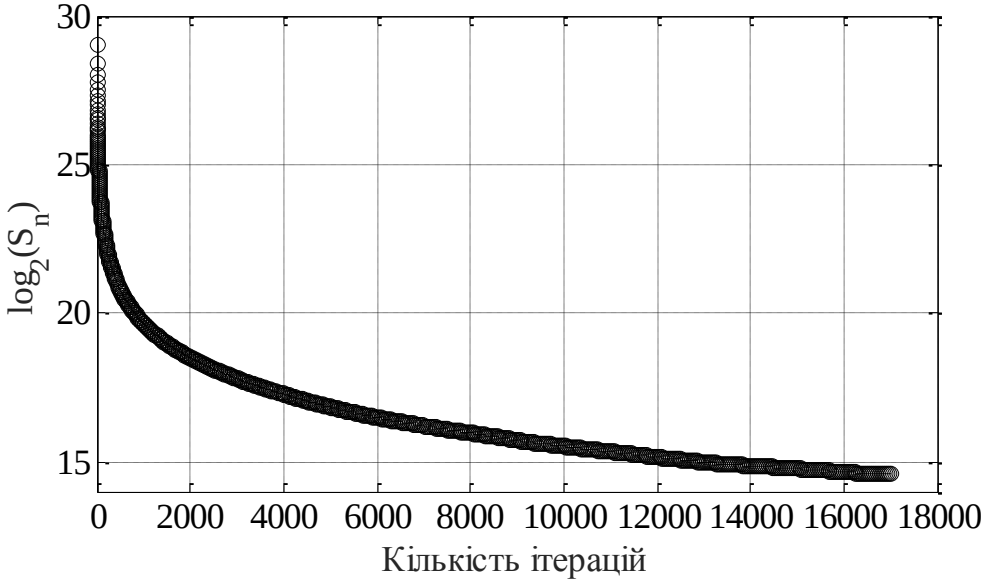
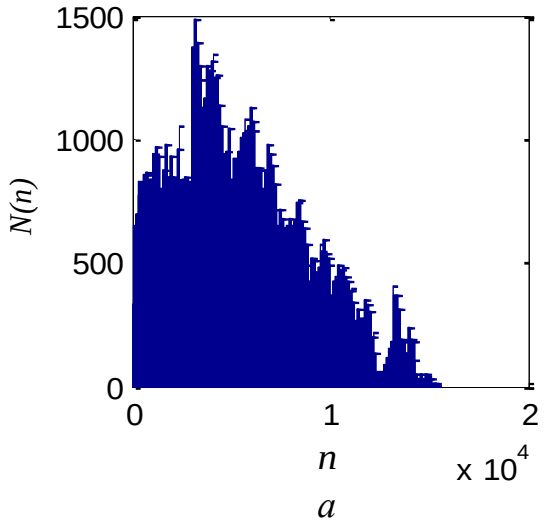
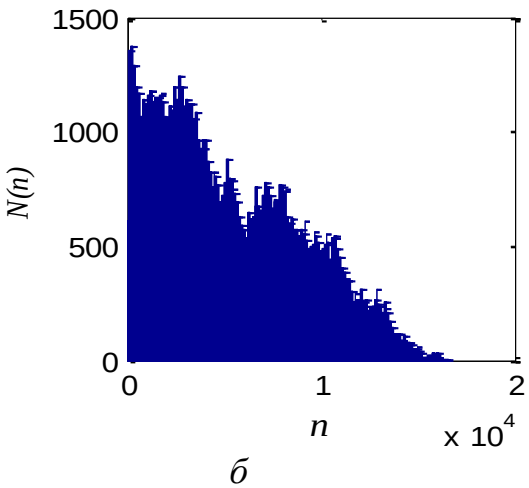


Рис. 2.7. Залежність потужності множини можливих станів логістичного рівняння від кількості ітерацій, *n*.

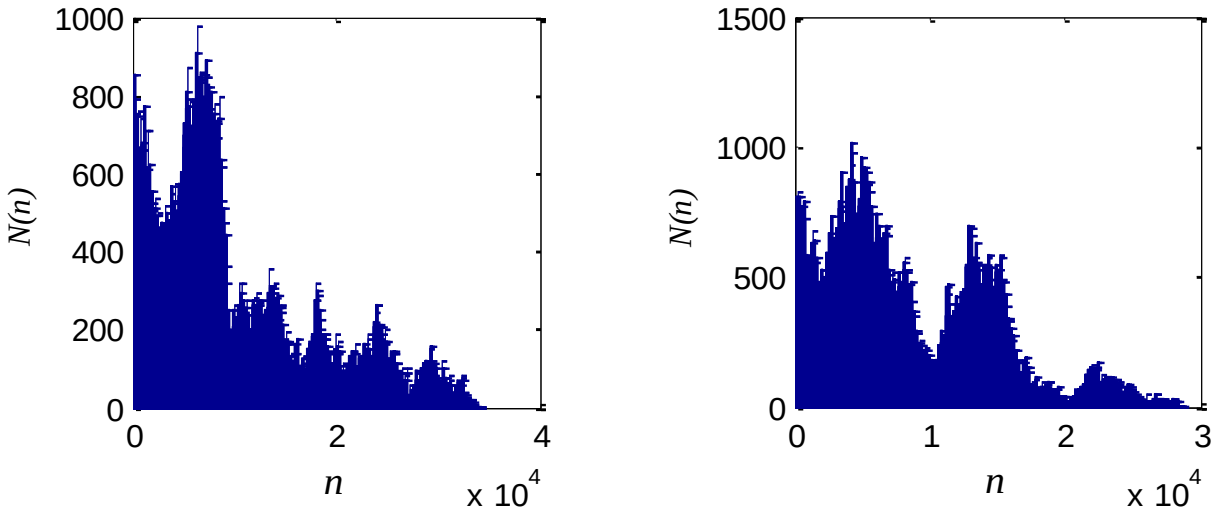
Внаслідок катастрофічної деградації потужність множини різних початкових умов у 2^{29} після перехідного процесу дорівнює сумі довжин всіх можливих циклів $24797 \approx 2^{14}$. Розподіл тривалості перехідного процесу залежить від значення параметру керування *r* і є нерівномірним (рис. 2.8). Із результатів моделювання слідує, що максимальна тривалість перехідного процесу обмежена як $2\text{-}4L_{max}$.



а



б



в *г*

Рис. 2.8. Гістограма розподілу тривалості перехідних процесів *а* – при r=4, *б* – при r=4-2^{-29}, *в* – при r=4-2×2^{-29}, *г* – при r=4-3×2^{-29}.

Згідно принципу Керкгофса зловмисник знає все про метод шифрування, крім ключів. Тому відкидання перехідного процесу для підвищення захищеності хаотичного шифру, як, наприклад, пропонується в піонерських роботах по криптографії на базі хаосу [47, 48] є беззмістовним. Якщо зловмисник ламає шифр атакою грубої сили, то ключем для нього будуть значення параметрів і початкові умови хаотичної системи в момент початку шифрування.

Як показано в роботах [100-103] (в більшості на якісному рівні) внаслідок динамічної деградації період повторення псевдохаосу є дуже малим в порівнянні з максимально можливим.

2.1.3. Періодичність часових рядів логістичного відображення при обмеженій точності обчислень арифметики з плаваючою комою

При реалізації математичних операцій на ЕОМ зазвичай використовують арифметику з плаваючою комою подвійної точності [104]. Це дозволяє забезпечити точність в 15—17 десяткових знаків і масштаб чисел в діапазоні від 10^{-308} до 10^{308}.

Число на ЕОМ представляється у вигляді знаку, експоненти та мантиси. Кінцеве значення числа визначається як:

$$\pm знак*(1+мантиса/\ 2^{52}) \times 2^{експонента-1023}.$$

Знак 0 відповідає додатнім числам, знак 1 відємним. Старший біт мантиси, який завжди рівний одиниці опускається. Експонента 0 записується, як 1023.

На ефективність використання арифметики з плаваючою комою впливають розміри області існування хаотичного атрактора та максимальне і мінімальне числа, якими оперує обчислювальна машина під час розрахунків.

Переваги арифметики з плаваючою комою можуть бути нівельовані, якщо розв'язки хаотичних систем не набуватимуть значень із всієї множини допустимих чисел.

Для системи (1.9) допустимі значення початкових умов з діапазону [0, 1], незалежно від значення параметру r. Проте розмах хаотичних реалізацій після закінчення перехідного процесу не виходитиме за межі деякого інтервалу $[x_{min}, x_{max}]$. Зі зміною параметру r будуть змінюватися розмах реалізацій і ключовий простір початкових умов. Легко показати, що:

$$x_{max} = f(r, 0{,}5) = \frac{r}{4},$$

$$x_{min} = f(r, x_{max}) = \frac{r^2}{4}\left(1 - \frac{r}{4}\right),$$

тоді послідовність розв'язків (2.1), стартуючи з довільної початкової умови з області (0,1) з часом обмежиться діапазоном $x(\mathrm{n}) \in \left[\frac{r^2}{4}\left(1-\frac{r}{4}\right), \frac{r}{4}\right]$, який задає область існування хаотичного атрактора системи (1.9).

Розглянемо вплив лінійних розмірів атрактора логістичного рівняння (після перехідного процесу) на ефективність використання арифметики для фіксованої і плаваючої коми. Під ефективністю використання арифметики ми розуміємо відношення потужності множини дозволених чисел арифметики N_0 до потужності множини яка належить атрактору системи N:

$$eff = \frac{N}{N_0} \tag{2.2}$$

Для арифметики з плаваючою комою при $r = 4$ мінімальне значення x_{min} вибиралося таке, щоб система (2.1) зберігала свою структуру, що рівноцінно значенню $x_{min} = 2^{-53}$ для подвійної точності і $x_{min} = 2^{-24}$ для одинарної точності.

Якщо значення $x(n) < 2^{-53}$ тоді $x(n)$ є машинним нулем в порівнянні з 1, тому $1 - x(n) = 1$. При цьому рівняння (1.9) еквівалентне наступному лінійному виразу

$$x(n+1) = rx(n) \tag{2.3}$$

Вплив лінійних розмірів атрактора логістичного рівняння (після перехідного процесу) на ефективність використання арифметики для фіксованої і плаваючої коми приведено в табл. 2.2.

Таблиця 2.2

Вплив лінійних розмірів атрактора логістичного рівняння на ефективність використання арифметики з фіксованою і плаваючою комою

Арифметика	Значення параметру *r*	x_{max}	x_{min}	Кількість різних чисел *N* в діапазоні від x_{min} до x_{max}	Кількість різних чисел N_0 для заданої арифметики	Ефективність, *eff*
Одинарна точність	3,75	0,9375 3f700000	0,2197265625 3e610000		$\approx 2^{32}$	
	4	1 3f800000	2^{-25} 33000000		$\approx 2^{32}$	
Подвійна точність	3,75	0,9375 3fee000000000000	0,2197265625 3fcc200000000000	$\approx 2^{53,06}$	$\approx 2^{64}$	$\approx 2^{-10,}$
	4	1 3ff0000000000000	2^{-54} 3c9000000000000	$\approx 2^{57,755}$	$\approx 2^{64}$	$\approx 2^{-6,2}$
Фіксована кома, 32 біти	3,75	0,9375 1e0000000000	0,2197265625 07080000	$\approx 2^{28,52}$	2^{32}	$\approx 2^{-3,4}$
	4	1 20000000	0 00000000	2^{29}	2^{32}	2^{-3}
Фіксована кома, 64 біти	3,75	0,9375 1e0000000000000000	0,2197265625 0708000000000000	$\approx 2^{60,52}$	2^{64}	$\approx 2^{-3,4}$
	4	1 2000000000000000	0 0000000000000000	2^{61}	2^{64}	2^{-3}

2.1.4. Механізм деградації та збільшення тривалості циклу

Зменшення потужності множини станів хаотичної системи зумовлене двома факторами:

1. За рахунок властивості перемішування різні області початкових умов після ітерацій потрапляють в одну. Наприклад, для логістичного відображення (рис. 2.9) два підінтервали відображаються в один:

$$S_{0,1} \to S'_{1,1}, S_{0.2} \to S'_{1,2} \,.\, S'_1 = \left(S_{1,1} \cup S_{1,2}\right) \to S'_1 = S'_{1,1} \cup S'_{1,2}. \qquad (2.4)$$

Якщо *r=4* отримаємо

$$S_1 = \left(0, \frac{1}{2}\right] \cup \left[\frac{1}{2}, 1\right) \to S'_1 = (0,1). \qquad (2.5)$$

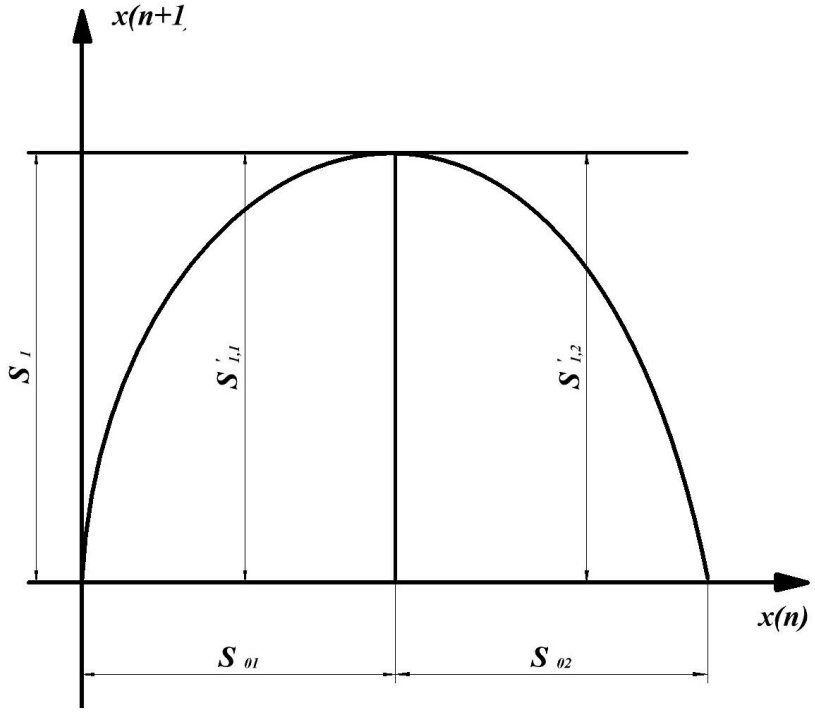


Рис. 2.9. Зменшення потужності множини станів хаотичної системи (1.9) ра рахунок властивості перемішування

Внаслідок перетворення потужність множини станів системи зменшується на кількість однакових елементів у $S_{1,1}$ і $S_{1,2}$.

2. За рахунок стиснення фазового об'єму в областях атрактора з від'ємним локальним показником Ляпунова. Для одномірних відображень ця область обмежена точками, в яких абсолютне значення похідної $\left|\frac{df(x)}{dx}\right| < 1$.

$$S_{2,1} \to S'_{2,1}, S_{2,2} \to S'_{2,2}\,.\, S'_2 = \left(S_{2,1} \cup S_{2,2}\right) \to S'_2 = S'_{2,1} \cup S'_{2,2}. \qquad (2.6)$$

Для логістичного відображення при $r = 4$ знайдемо, що $S_2 = \left(\frac{3}{8}, \frac{5}{8}\right)$. Після першої ітерації множина S_2 еволюціонує у $S'_2 = \left(\frac{15}{16}, 1\right)$ (рис. 2.10).

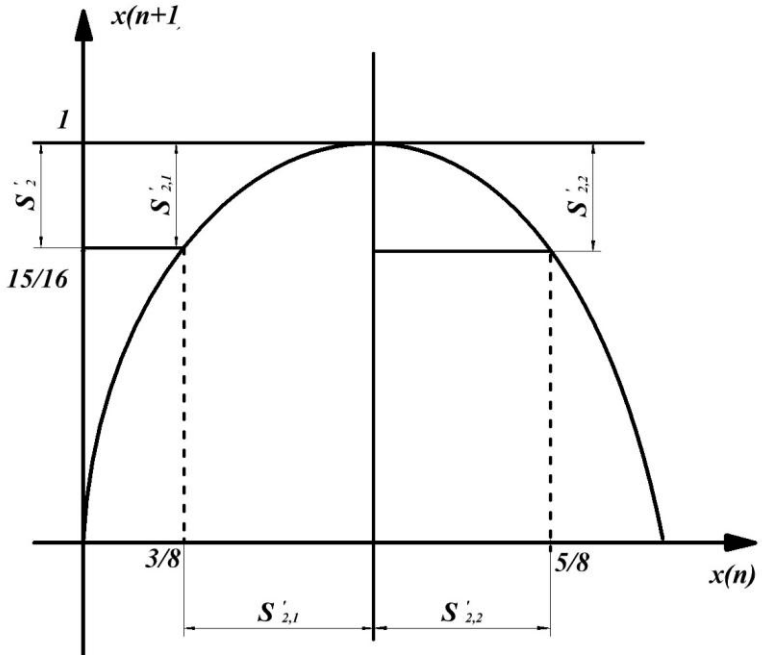


Рис. 2.10. Стиснення фазового об’єму в областях фазового простору логістичного відображення з від’ємним локальним показником Ляпунова.

В областях фазового простору з від’ємним локальним показником Ляпунова деградація відображення може відбуватися під впливом обох факторів.

Вплив ефекту стиснення фазового об’єму помітно впливає на деградацію при малих n. З ростом n внаслідок розрідження множини цей ефект зменшується, оскільки все менше і менше точок буде знаходитися достатньо близько щоб “збігтися” в одну.

Використання багатовимірних систем для вирішення проблеми циклічності є найбільш доцільним, оскільки середні тривалості циклу та перехідного процесу при виході траєкторії на цикл залежать від кореляційної розмірності d, наступним чином [18, 102, 103]:

$$\langle L \rangle \sim \varepsilon^{-\frac{d}{2}} \qquad (2.7)$$

де $\langle L \rangle$ - середнє значення тривалості циклу, ε - точність обчислень, що становить 2^{-29} для арифметики з фіксованою комою Q3.29. Для визначення кореляційної розмірності неперервна траєкторія дискретизується – заміною множини з N точок $\{\boldsymbol{X}_i\}$ в фазовому просторі. Потім вираховується відстань між парами точок $s_{ij} = |\boldsymbol{X}_i - \boldsymbol{X}_j|$, використовуючи звичайну евклідову міру відстані (квадратний корінь із суми квадратів компонент) , або іншу еквівалентну міру (наприклад суму абсолютних величин компонент вектора). Кореляційна функція визначається як:

$$C(\varepsilon) = \lim_{N\to\infty} \frac{1}{N^2} \left(\begin{matrix} \text{число пар } (i,j) \text{ для} \\ \text{яких відстань } s_{ij} < \varepsilon \end{matrix} \right). \qquad (2.8)$$

де N – кількість точок у фазовому просторі.

Із (2.7) випливає, що єдиним способом збільшення середньої тривалості циклу є збільшення кореляційної розмірності хаотичної системи. Кореляційна розмірність не перевищує розмірності фазового простору хаотичної системи. Тому збільшення періоду повторення псевдохаотичної послідовності можливе шляхом збільшення розмірності фазового простору хаотичної системи.

Загальна схема побудови багатовимірних відображень з використанням кільцевого зв’язку на рис. 2.11 [105].

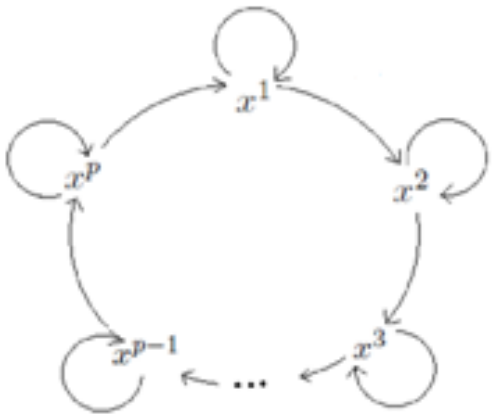


Рис. 2.11. Структура багатовимірного відображення із кільцевим звязком

Багатовимірне логістичне відображення із кільцевим зв’язком описується наступною системою рівнянь [94]:

$$\begin{cases} x_{n+1}^{(1)} = e * r * x_n^{(1)}(1 - x_n^{(1)}) + (1 - e) * x_n^{(p)} \\ x_{n+1}^{(2)} = e * r * x_n^{(2)}(1 - x_n^{(2)}) + (1 - e) * x_n^{(1)} \\ \cdots \\ x_{n+1}^{(p)} = e * r * x_n^{(p)}(1 - x_n^{(p)}) + (1 - e) * x_n^{(p-1)} \end{cases} \quad (2.9)$$

де – p розмірність системи, а e – коефіцієнт зв'язку.

Залежність значень кореляційної розмірності p для багатовимірного логістичного відображення з кільцевим зв'язком (2.9) приведено в табл. 2.3.

Таблиця 2.3.

Залежність значень кореляційної розмірності для відображення (2.9)

Розмірність системи, p	2	4	6	8	10	12	14	16	18	20
Кореляційна розмірність, d	1.75	3.5	5.06	6.23	7.86	8.88	9.97	11.41	12.42	14.47
$\langle L \rangle$ при $\varepsilon = 2^{-29}$	$43 * 10^6$	$1.8 * 10^{15}$	$1.2 * 10^{22}$	$1.5 * 10^{27}$	$2 * 10^{34}$	$2.5 * 10^{38}$	$3.2 * 10^{43}$	$6.3 * 10^{49}$	$1.6 * 10^{54}$	$1.4 * 10^{63}$

З таблиці 2.3 випливає, що використання багатовимірного відображення призводить до суттєвого зростання середньої тривалості періоду повторення часових в порівнянні із одновимірним випадком.

2.2. ГПВП на базі багатовимірних відображень із кільцевим звязком

2.2.1. Багатовимірна хаотична система Лоці

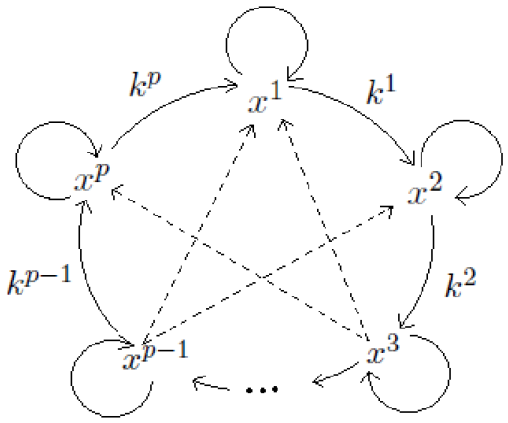
Сімейство систем Лоці належить до класу систем з дискретним часом і неперервною множиною значень [106-109]. Аналітично одне із сімейства відображень описується наступними рівняннями [107]:

$$\begin{cases} x_{n+1}^{(1)} = 1 - r_1 \left| x_n^{(1)} \right| + k_1 (\left| x_n^{(2)} \right| - (x_n^{(1)})^2) \\ x_{n+1}^{(2)} = 1 - r_2 \left| x_n^{(2)} \right| + k_2 (\left| x_n^{(3)} \right| - (x_n^{(2)})^2) \\ \cdots \\ x_{n+1}^{(p)} = 1 - r_p \left| x_n^{(p)} \right| + k_p (\left| x_n^{(1)} \right| - (x_n^{(p)})^2) \end{cases} \quad (2.10)$$

де – r та k – параметри керування системи, p – розмірність системи, $i = [1 \dots p]$, $\left|x_n^{(i)}\right|$ – абсолютне значення $x_n^{(i)}$.

Структурно систему (2.10) можна зобразити у вигляді графа наведеного на рис. 2.11.

Як випливає з рис. 2.11. багатовимірна система Лозі складається з сукупності послідовно з'єднаних у кільце підсистем. Альтернативним способом побудови системи Лозі є застосування пересічних з'єднань (рис. 2.12), що ускладнює завдання розкриття параметрів таких систем шляхом аналізу розподілу часових рядів [108].



б

Рис. 2.12. Варіанти структури багатовимірного відображення Лоці:
із кільцевим з'єднанням з пересіканням

Для того щоб значення розв'язків системи мали рівномірний розподіл і однаковою ймовірністю відвідували області фазового простору на p- розмірному торі $T^p = [-1,1]^p$ необхідно накласти обмеження на розмах значень змінних [106]:

$$\begin{aligned} &\text{якщо } 1 - r\left|x_n^{(i)}\right| + r(\left|x^{(i-1)}\right| - (x_n^{(i)})^2) < -1, \\ &\qquad x_{n+1}^{(i)} = x_{n+1}^{(i)} + 2, \\ &\text{якщо } 1 - r\left|x_n^{(i)}\right| + r(\left|x^{(i-1)}\right| - (x_n^{(i)})^2) > 1, \\ &\qquad x_{n+1}^{(i)} = x_{n+1}^{(i)} - 2, \end{aligned} \tag{2.11}$$

Застосування операцій (2.11) дає змогу покращити властивості псевдовипадковості при застосування системи (2,10) для генерування псевдовипадкових послідовностей, та уможливлює отримання часових рядів з рівно ймовірним розподілом.

Проведемо попереднє дослідження системи (2.11). Послідовність розв'язків для $x^{(1)}(n)$, приведена на рис. 2.13, свідчить про випадковий характер отриманої реалізації.

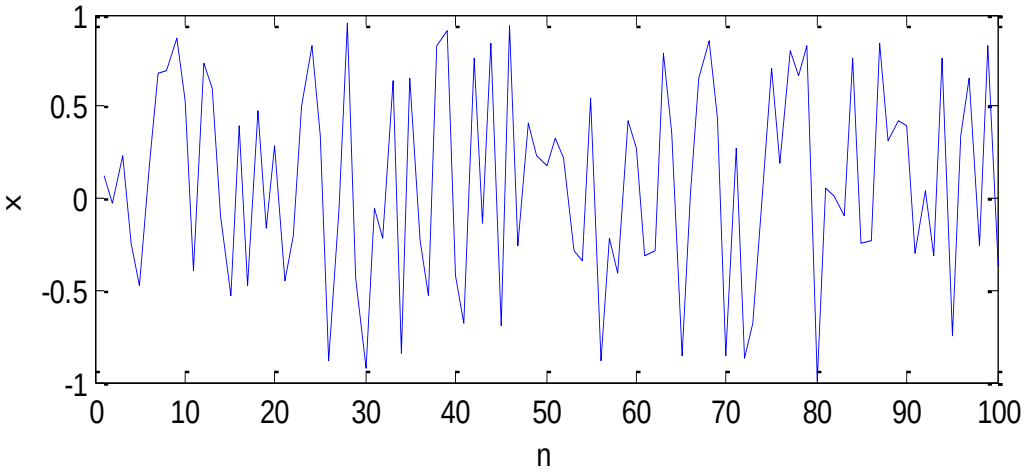


Рис. 2.13. Залежність змінної $x^{(1)}$ від номеру ітерації *n*.

Фазовий портрет для змінних $x^{(1)}$, $x^{(2)}$ і $x^{(3)}$ при $p = 4$ має вигляд рівномірно заповненого точками кубу, що говорить про слабку залежність відповідних змінних між собою (див. рис. 2.14).

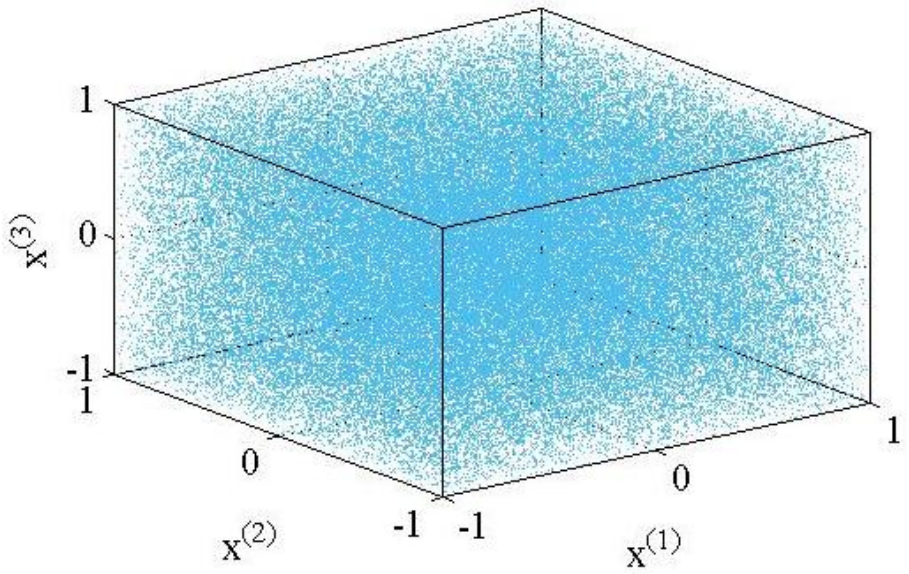


Рис. 2.14. Фазовий портрет системи Лоці $x^{(1)}$, $x^{(2)}$ і $x^{(3)}$ при $p = 4$.

Гістограми розподілу значень $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ і $x^{(4)}$, для 100000 ітерацій наведено на рис. 2.15. Для вихідних змінних діапазон значень сигналу було розбито на 100 піддіапазонів і пораховано кількість попадань в кожен з них.

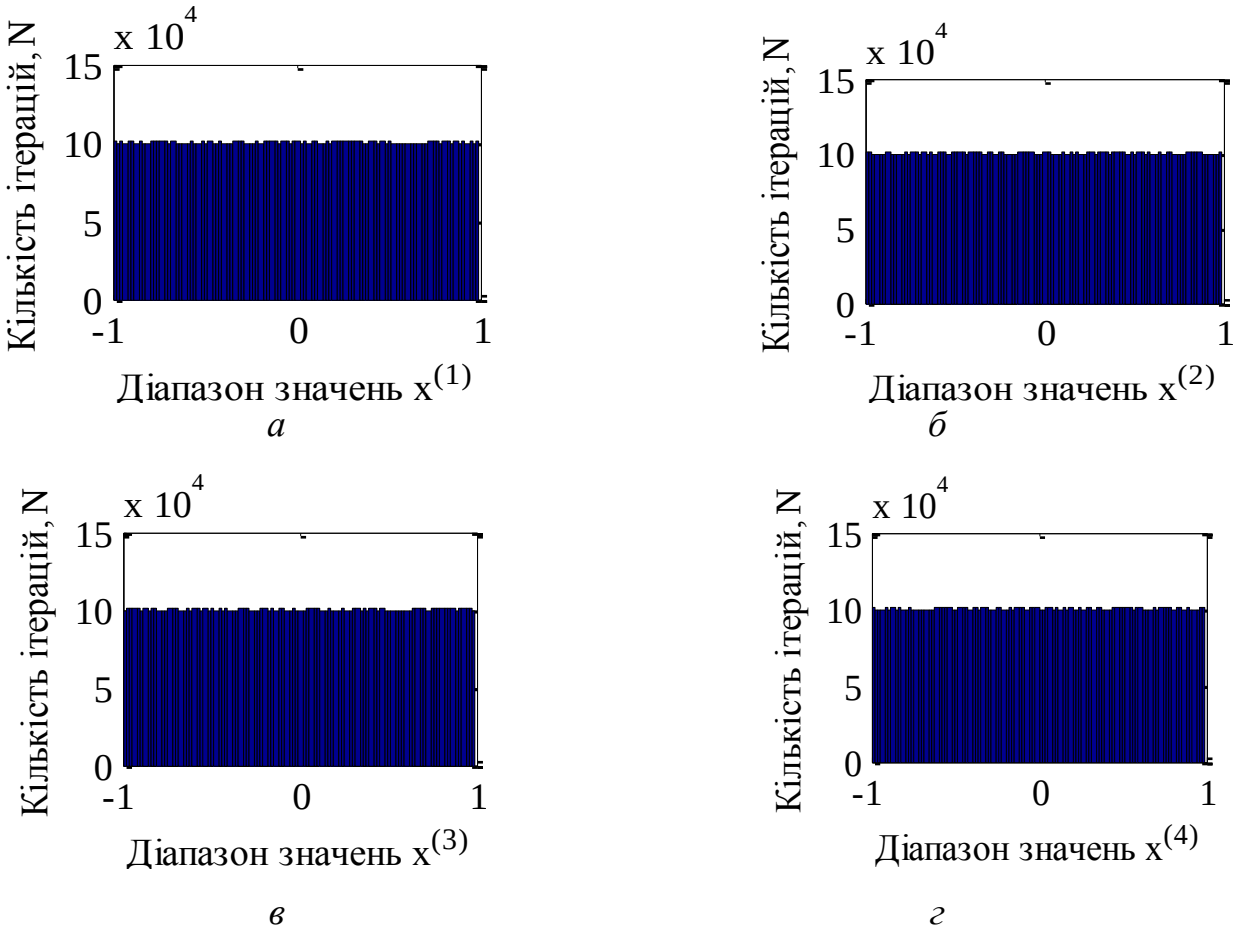


Рис. 2.15. Гістограми розподілу значень розв'язків чотиривимірної системи Лозі:

$x^{(1)}$ - *а*, $x^{(2)}$ -*б*, $x^{(3)}$ - *в*, $x^{(4)}$ - *г*

Як видно з рис. 2.15, у кожен із 100 піддіапазонів попадає приблизно 1000 точок, а розподіл близький до рівномірного. Рівномірний розподіл змінних $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ і $x^{(4)}$ означає, що у фазовому просторі траєкторія рівноймовірно відвідує кожну малу область. Це є перевагою відображення Лозі в порівнянні з іншими дискретними і неперервними системами у яких атрактор зосереджений в обмеженій області фазового простору. Залежність значень кореляційної розмірності *d* від розмірності системи *p* для багатовимірного відображення Лоці з кільцевим зв'язком (2.10) приведено в табл. 2.4.

Таблиця 2.4.

Залежність значень кореляційної розмірності d від розмірності системи p для багатовимірного відображення Лоці

Розмірність системи, p	2	4	6	8	10	12	14	16	18	20
Кореляційна розмірність, d	1.7407	3.7956	5.8643	7.5612	9.0311	10.823	12.838	13.902	15.191	17.638

З таблиці 2.4. випливає, що багатовимірне відображення Лоці володіє набагато кращими псевдовипадковими характеристиками ніж багатовимірне логістичне відображення. Тому таке відображення доцільніше використовувати в якості бази ГПВП.

2.2.2. Розробка структури ГПВП.

Оскільки сучасні методи криптоаналізу дозволяють легко розкрити структуру ГПВП на базі регістрів зсуву з лінійним оберненим зв'язком, доцільним є дослідження ГПВП на базі комбінації регістрів зсуву та багатовимірних НДС. Це в свою чергу дозволить ускладнити завдання розкриття параметрів та початкових умов таких генераторів. Тому пропонується використовувати схему генерування псевдовипадкових бітів, що наведена на рис. 2.16 [5]. На вхід поступає ключ, що представляє собою початкові умови, параметри керування та значення регістрів зсуву.

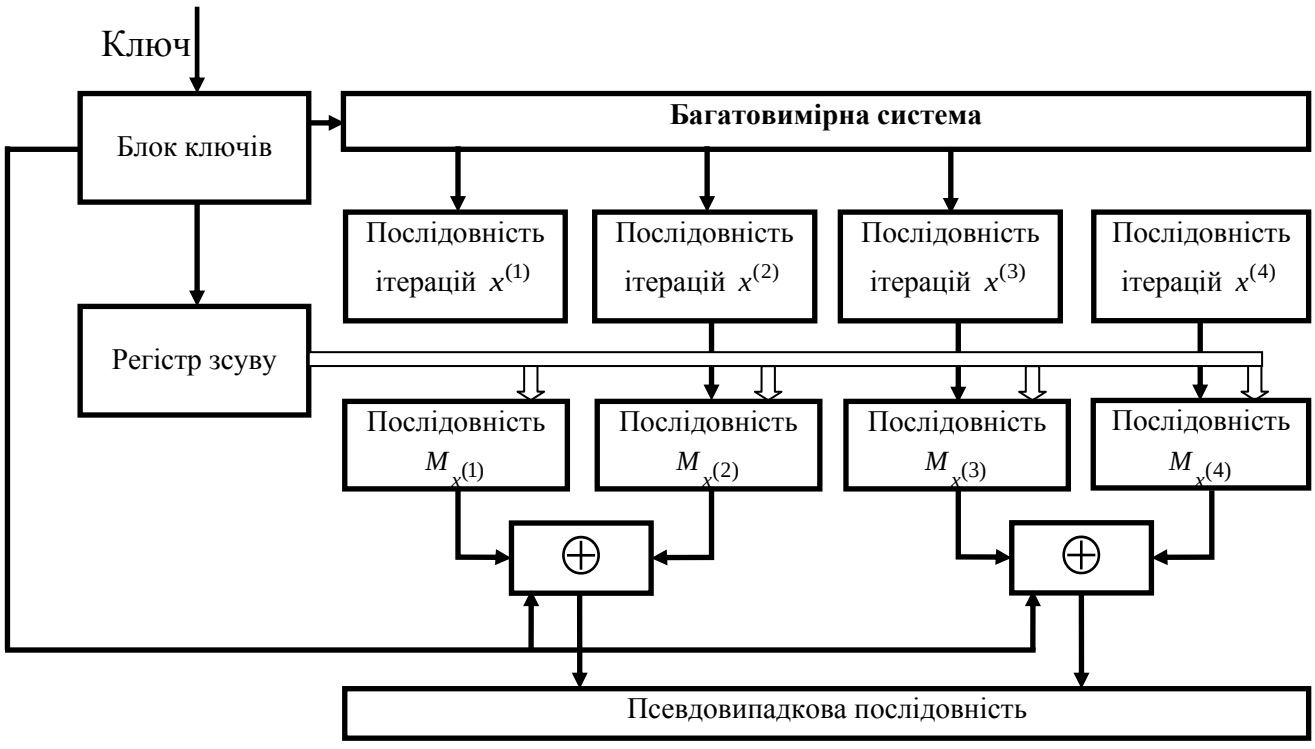


Рис. 2.16. Принцип побудови генератора псевдовипадкових послідовностей.

Розв’язки рівнянь (2.10) дають нам чотири різні хаотичні послідовності. Із кожної ітерації вибираються біти з 5 по 28. Вибір бітів обумовлюється їх збалансованістю згідно (2.1) і визначається для кожної системи окремо. Таким чином формуються чотири блоки по 24 біти. За одну ітерацію можна отримати послідовність довжиною 96 біт. При додавані за модулем 2 при $p = 4$ ми можемо використовувати одну з наступних можливих конфігурацій:

$$\begin{cases} M_{x^{(1)}} \oplus M_{x^{(2)}} \\ M_{x^{(3)}} \oplus M_{x^{(4)}} \end{cases}$$

$$\begin{cases} M_{x^{(1)}} \oplus M_{x^{(3)}} \\ M_{x^{(2)}} \oplus M_{x^{(4)}} \end{cases} \qquad (2.12)$$

$$\begin{cases} M_{x^{(1)}} \oplus M_{x^{(4)}} \\ M_{x^{(2)}} \oplus M_{x^{(3)}} \end{cases}$$

Тому доцільним є використання систем розмірність яких кратна 2. З чотирьох блоків по 24 біти по два додаються за модулем 2, в результаті отримаємо 48 псевдовипадкових біт.

При використанні чотиривимірної системи швидкість генерування псевдовипадкової послідовності бітів у випадку використання частоти PLL=50 МГц становитиме 48*50 000 000 = 2,4 ГГбіт/с. Збільшити швидкість генерації можна застосувавши хаотичну систему більшої розмірності.

Потенційна швидкість генерування псевдовипадкової послідовності з використанням чотривимірної системи при тактовій частоті 400 МГц становить 19,2 Гбіт/с.

Розроблена структура ГПВП дозволяє його застосовувати для будь-якого багатовимірного відображення із кільцевим зв’язком.

Відображення зсуву та тентове відображення також характеризуються неперервною біфуркаційною діаграмою. Однак ці системи володіють початковими умовами котрі з часом призводять до нульової реалізації вихідного сигналу [17]. Тому виходячи з цього дані відображення не розглянуто.

2.3. Генератор псевдовипадкових коливань на базі мемристивних хаотичних кіл

Як вже згадувалося, на базі схеми Чуа було запропоновано системи зв’язку із розширеним спектром для системи зв’язку CDMA. Однак не зважаючи на простоту схеми реалізація нелінійного елементу «діод Чуа» можлива тільки шляхом емулятора, що значно ускладнює побудову широкосмугових захищених систем зв’язку через проблему забезпечення завадостійкої синхронізації. Як один із шляхів вирішення даної проблеми було запропоновано замінити діод Чуа на мемристор або мемристивну структуру, оскільки їх характеристики також нелінійні [110, 111]. Мемристор є одним із останніх досягнень розробки та виготовлення нелінійних елементів з використанням інтегральної технології. Мемристор може бути виготовлений з використанням органічних та неорганічних матеріалів. Нелінійна динаміка мемристора може бути використана для реалізації малопотужних захищених систем зв’язку.

2.3.1. Генератор хаотичних коливань на базі мемристора

Один з найпростіших генераторів хаотичних коливань на базі мемристора описаний в [112] складається з трьох послідовно з'єднаних елементів: котушки індуктивності, конденсатора та мемристора (рис. 2.17).

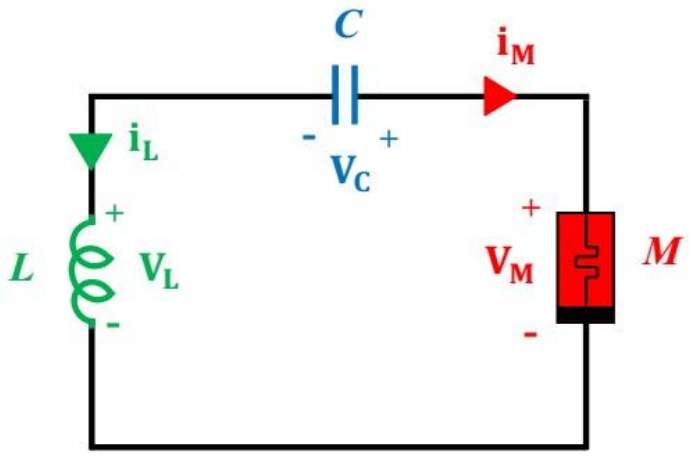


Рис. 2.17. Електрична схема хаотичної системи на базі мемристора

Використана модель мемристора є моделю узагальненого мемристивного пристрою [111] характеристики якого не відповідають характеристикам

ідеального мемристора введеного в [110]. Нелінійна характеристика мемристора описується рівнянням [20]:

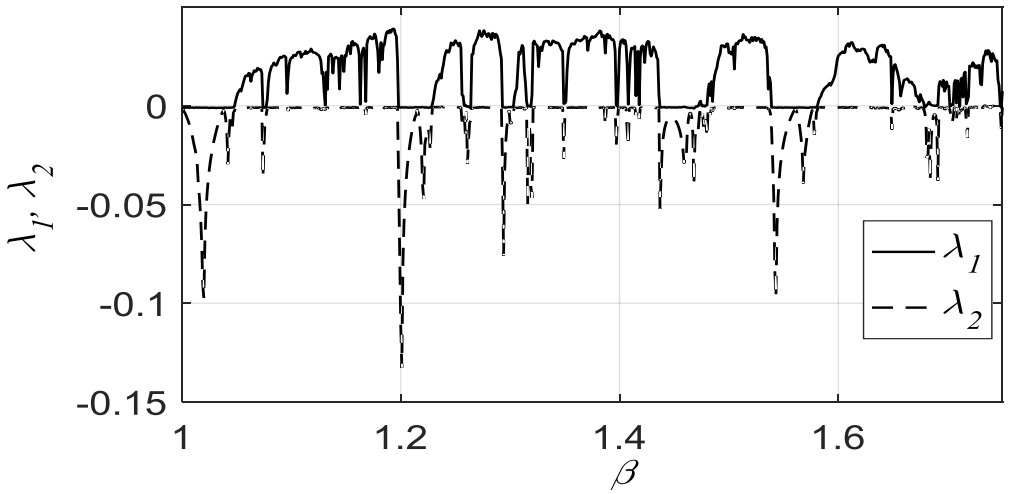
$$\begin{cases} V_{\text{м}} = \beta(x^2 - 1)\text{i}_M \\ \dot{x} = \text{i}_{\text{м}} - \alpha\text{x} - \text{i}_M\text{x} \end{cases} \tag{2.13}$$

Динаміка електронного кола (рис. 2.18.) описується системою рівнянь [4]:

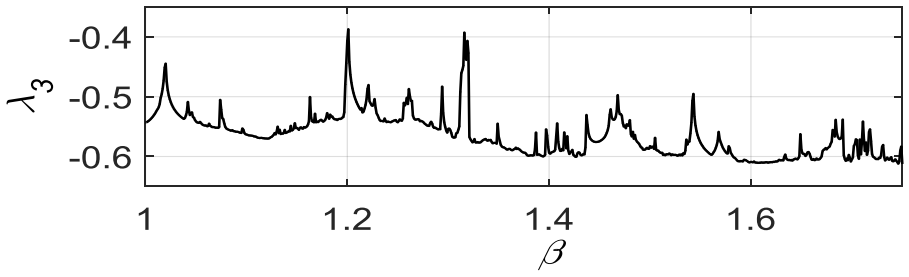
$$\begin{cases} \dot{x} = y/C \\ \dot{y} = -1/L\left[x + \beta(z^2 - 1)y\right] \\ \dot{z} = -y - \alpha z + yz \end{cases} \tag{2.14}$$

де α, β параметри керування, $C = 1$, $L = 3$.

Критерієм хаотичної поведінки є додатнє значення старшого показника Ляпунова. Визначена за допомогою методу Бенеттина [23], діаграма показників Ляпунова для системи (2.14) приведена на рис 2.18. При значеннях параметру $\beta \in [1; 1,7]$ в системі мають місце періодичні $(\lambda_1 = 0)$ і хаотичні $(\lambda_1 > 0)$ режими.



а



б

Рис. 2.18. Залежність показників Ляпунова від параметру β при $\alpha = 0,6$

Подальші дослідження проводилися для значень параметрів $\beta = 1{,}5$ та $\alpha = 0{,}6$. Із рис. 2.18. випливає, що при $\beta = 1{,}5$, один показник Ляпунова є додатнім, а сума показників Ляпунова є відємною, що вказує на хаотичну поведінку системи.

Більш детальне вивчення статистичних властивостей системи (2.14) приведено в розділі 3.2.

2.3.2. Розробка ГПВП на базі хаотичної системи з мемристивною структурою

Оскільки розподіл послідовностей генерованих системою (2.14) є нерівномірним то доцільним є відкидання старших бітів в бінарному представлені генерованих значень при використанні арифметики з фіксованою комою [7]. Це також утруднить розкриття поточного стану генератора. Блок схема методу генерування псевдовипадкових послідовностей на базі математичної моделі мемристивної хаотичної системи (2.14) приведена на рис. 2.19.

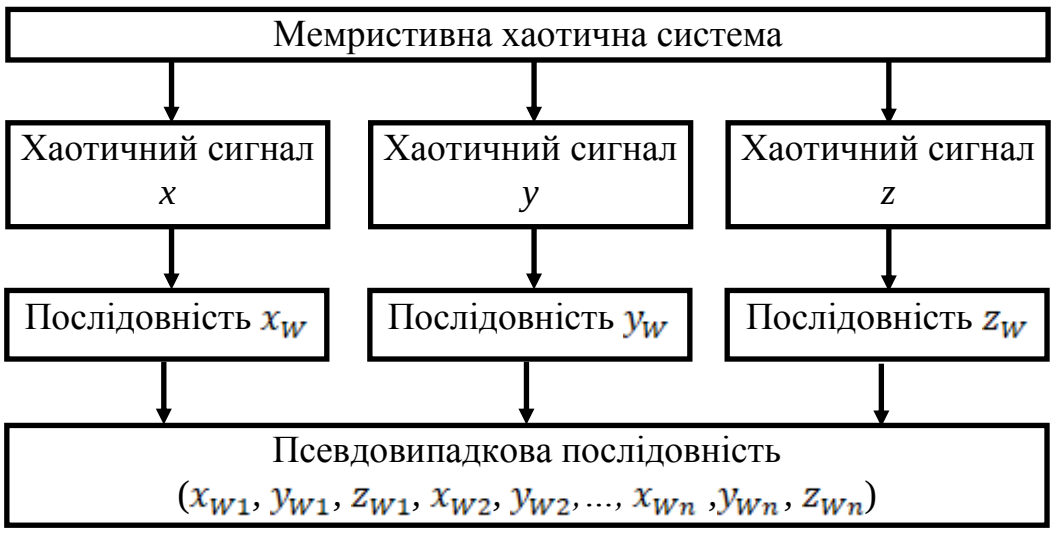


Рис. 2.19. Блок-схеми генератора псевдовипадкових послідовностей на базі мемристивної хаотичної системи третього порядку.

Як випливає із рис. 2.19 після відкидання старших бітів ми отримуємо послідовності x_W, y_W та z_W з яких формуємо псевдовипадкову послідовність типу $x_{W1}, y_{W1}, z_{W1}, x_{W2}, y_{W2}, \ldots, x_{Wn}, y_{Wn}, z_{Wn}$.

Оскільки така система при реалізації на ПЛІС також генеруватиме періодичні псевдохаотичні послідовності доцільним є використовувати декілька

електронних кіл з’єднаних між собою кільцевим зв’язком (Рис. 2.20) [108].

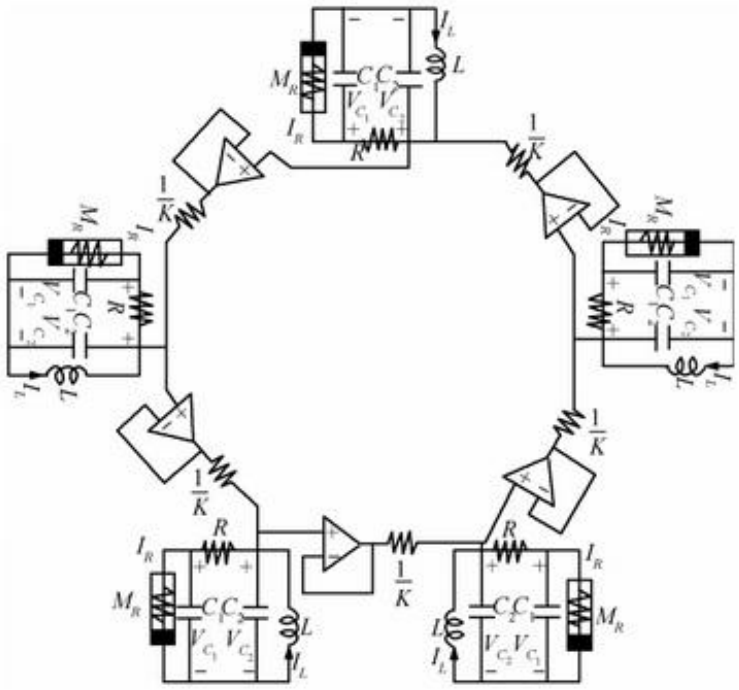


Рис. 2.20. Нелінійна динамічна система на базі неперервних хаотичних схем з’єднаних кільцевим зв’язком.

Використання кільцевого зв’язку при апаратній реалізації генератора псевдовипадкових послідовностей на базі математичної моделі такої системи дозволить збільшити середнє значення періоду повторюваності часових рядів та мінімізувати вплив явища колапсу хаосу. Також такий підхід цікавий з точки зору побудови неавтономних генераторів хаотичних коливань та їх реалізації на ПЛІС.

Висновки до другого розділу.

1. Досліджено періодичність розв’язків логістичного відображення при реалізації на ПЛІС з використанням арифметики з фіксованою комою. Q3.29. Показано, що після закінчення перехідного процесу при точності обчислень 2^{-29} кількість різних послідовностей, що можуть бути згенеровані логістичним відображенням обмежена і не залежить від початкових умов. Максимальна довжина перехідного процесу становила 16775 ітерацій. Показано, що потужність множини різних початкових умов після перехідного процесу дорівнює сумі

довжин всіх можливих циклів 24797 ≈ 2^{14}. Приведено залежність потужності простору початкових умов від кількості ітерацій.

2. Показано, що використання багатовимірних систем для вирішення проблеми циклічності є найбільш доцільним порівняно із періодичними збуреннями та підвищенням точності обчислень, оскільки середні значення тривалості циклу та перехідного процесу при виході траєкторії на цикл залежать від кореляційної розмірності.

3. Запропоновано генеротор псевдовипадкових послідовностей на базі багатовимірних відображень Лоці із кільцевим зв'язком. Показано, що при реалізації на ПЛІС такі системи дозволяють отримати послідовності з рівномірним розподілом для широкого діапазону значень параметрів керування . Для ускладнення розкриття поточного стану генератора та параметрів керування пропонується використовувати регістр зсуву і додавання за модулем 2 різних послідовностей.

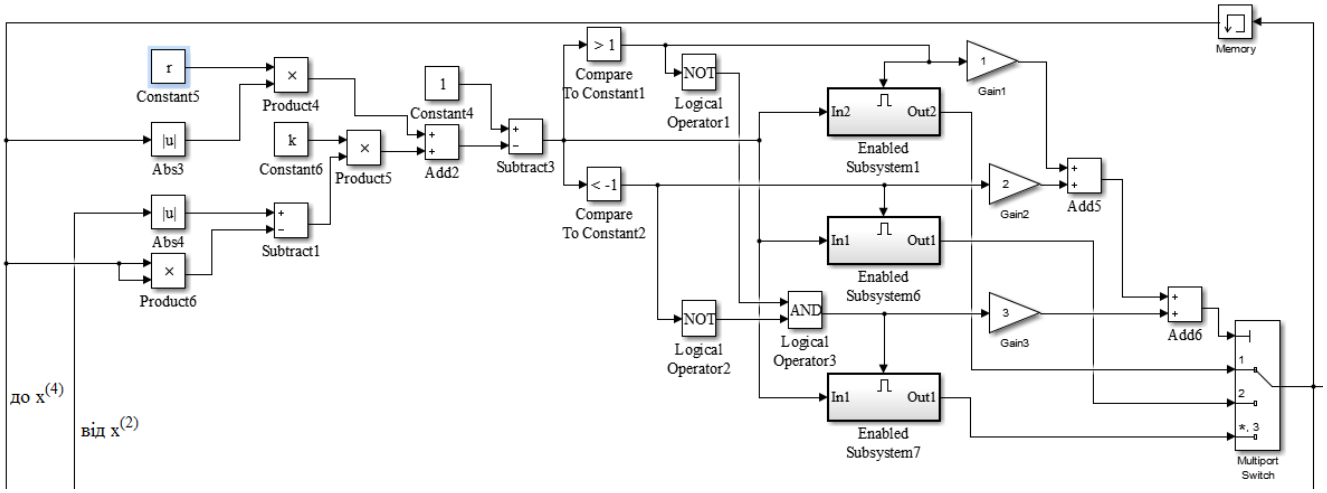
РОЗДІЛ 3.
АПАРАТНА РЕАЛІЗАЦІЯ ГПВП НА БАЗІ БАГАТОВИМІРНИХ НДС

3.1. Реалізація на ПЛІС генераторів ПВП на базі багатовимірних відображенн

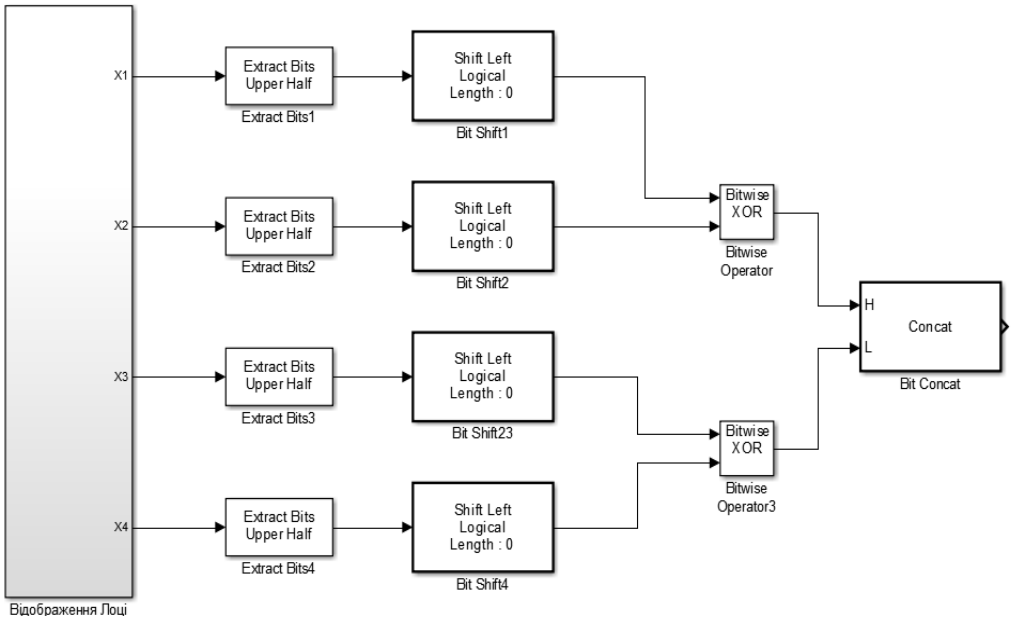
При розробці генераторів сигналів на базі спеціалізованих мікросхем доцільно проводити попередню реалізацію та верифікацію на базі програмованих логічних інтегральних схем. Це дозволяє в реальних умовах швидко провести дослідження генератора сигналів та легко вносити зміни в його конструкцію. Для апаратної реалізації відображень із кільцевим зв'язком ПЛІС є однією з найкращих платформ оскільки вони дозволяють реалізувати системи різної розмірності без втрати швидкодії шляхом паралельного обчислення змінних системи. Для експерименту використано ПЛІС Altera Cyclone *IV EP4CE115*.

Simulink - модель схеми, що обчислює $x_{n+1}^{(1)}$ у (2.10) із врахуванням (2.11) приведено на рис. 3.1 Елемент Memory необхідний для збереження минулого стану системи під час обчислення наступного.

Блок перевірки умов (2) нами побудовано на базі двох компараторів Comparator 1 і Comparator 2. Comparator 1 перевіряє умову $x_{n+1} > 1$. Якщо умова виконується тоді контрольний сигнал передається до підсистеми Subsystem 1 в якій здійснюється зменшення сигналу на 2. У блоці Comparator 2 виконується перевірка умови $x_{n+1} < -1$. У випадку позитивного рішення значення сигналу збільшується на 2. Якщо сигнал знаходиться в діапазоні [0, 1] тоді вихідні сигнали обох компараторів дорівнюють нулю. Два логічні елементи NOT, елемент AND, підсилювачі Gain1, Gain2, Gain3, суматори Add2 Add3 використані у схемі керування перемикачем MultiportSwith, який застосовується для вибору необхідного вихідного сигналу. Коефіцієнти підсилення підсилювачів Gain1, Gain2, Gain3 дорівнюють $1, 2, 3$ відповідно. Блок Constant 5 задає значення параметру $k^{(1)}$.



а



б

Рис. 3.1. Апаратна реалізація ГПВП приведеного на рис. 2.16 на базі системи 2.10 при $p = 4$: *а* - Simulink-модель схеми обчислення значення $x_{n+1}^{(1)}$, *б* загальний вид

Зміна стану дискретної системи відбувається під впливом тактового сигналу. Зміна стану дискретної системи відбувається під впливом тактового сигналу.

3.1.1. Дослідження збалансованості бітів генерованих відображенням Лоці

Надалі будемо використовувати наступне представлення чисел: 4 біта виділимо для цілої частини включаючи знаковий біт і 28 біт - для дробової

частини чисел. Таким чином про розрахунках отримуватимемо послідовність 32-бітових чисел. Однією з умов забезпечення високого показника випадковості послідовності бітів є їх збалансованість [83]. Кількість одиниць і нулів у послідовності повинна бути приблизно однаковою.

Для вибору частини бітів двійкового числа, які задовольняють вимогу збалансованості згенеровано 4 матриці типу (2.1) та визначено кількість символів "0" – N_0 і "1" – N_0 (рис. 3.2).

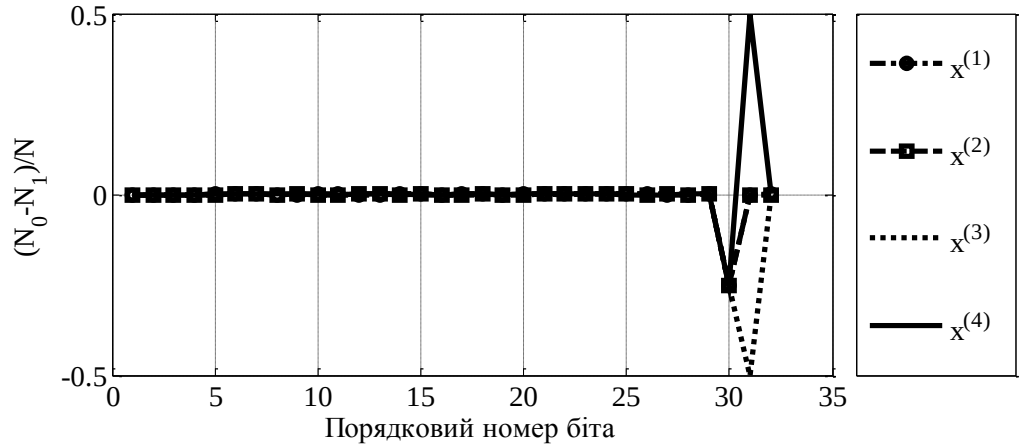


Рис. 3.2. Збалансованість бітів у бінарному представлені x^1

Із рис. 3.2 випливає, що біті які знаходяться в інтервалі від 1 до 29 можна вважати збалансованими. Кількість «0» і «1» для бітів з 30 по 32 значно відрізняється, тому вони є незбалансованими. У подальшому дослідження для побудови генератора псевдовипадкових послідовностей виберемо біти з 5 по 28 включно. Відкидання старших 4 біт кожного числа необхідно для ускладнення розкриття параметрів керування.

3.1.2. Експериментальне дослідження роботи хаотичної системи на ПЛІС

Для проведення експерименту систему (2.11) реалізовано у Simulink з використанням арифметики Q4.28. Далі з проекту у вигляді окремої підсистеми за допомогою HDL-coder згенеровано VHDL опис. Компіляція та присвоєння пінів проведено в середовищі Quartus II. Скомпільований проект в RTL Viewer для виводу сигналів $x^{(1)}$ та $x^{(2)}$ на екран цифрового осцилографа приведено на рис. 3.3.

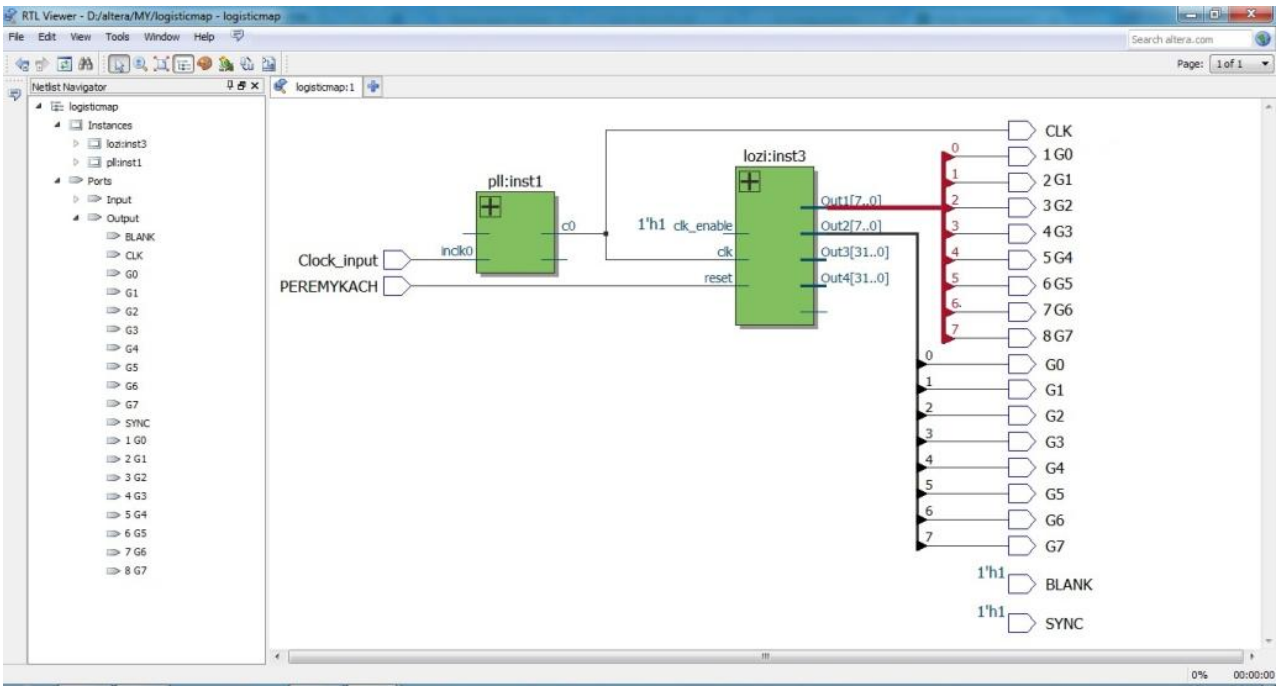


Рис. 3.3. Скомпільований проект в RTL Viewer

Для перетворення цифрового сигналу в аналоговий використано вбудований 8-бітний ЦАП. Значення змінних $x^{(p)}$ здіапазону [-1; 1] переведено в діапазон восьми бітних чисел [0; 256]. Далі восьмибітні числа подано на вхід чотирьохканального ЦАП. Дослідницький макет приведено на рис. 3.4.

Рис. 3.4. Проведення експерименту

При проведенні експерименту PLL налаштовано на частоту 1 МГц. Осцилограми часових рядів та фазового портрету системи (2.10) при реалізації на ПЛІС з арифметикою Q4.28 приведено на рис. 3.5 і рис. 3.6.

Як бачимо принцип паралельного обчислення що застосовується в ПЛІС дає змогу отримувати розв’язки хаотичної системи з частотою рівною частоті тактового сигналу.

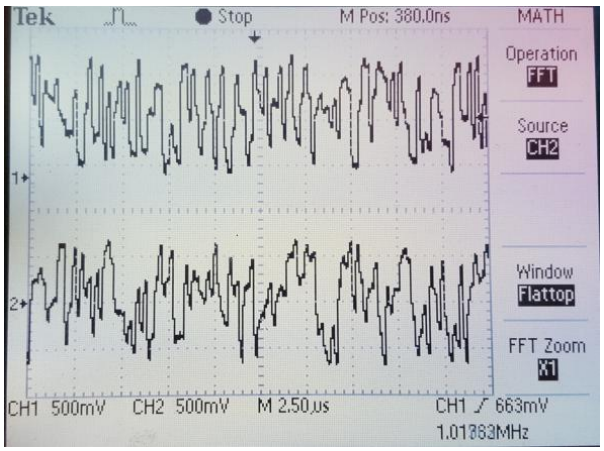


Рис. 3.5. Осцилограми вихідних сигналів x^1 та x^2 при реалізації на ПЛІС

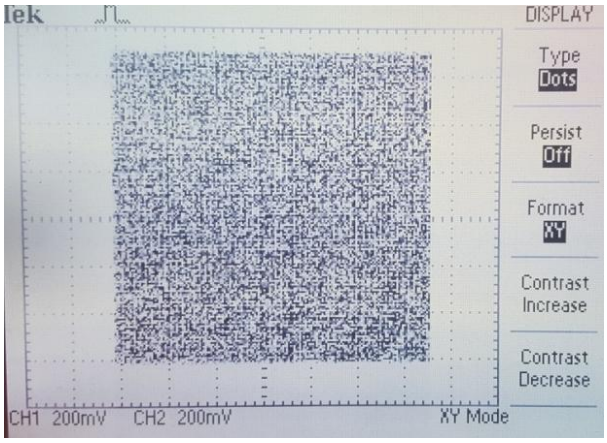


Рис. 3.6. Фазовий портрет хаотичної системи, реалізованої на ПЛІС

Спектр частот вихідного хаотичного сигналу схожий на спектр періодичної послідовності прямокутних імпульсів (рис. 3.7).

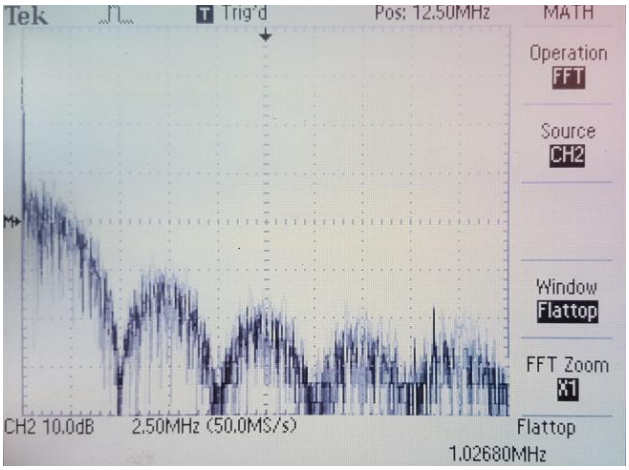


Рис. 3.7. Частотний спектр генерованого сигналу

Перший мінімум спектру співпадає з значенням тактової частоти, що зумовлено неперервним слідуванням хаотичних імпульсів.

Аналогічні результати були отримані при значенні тактової частоти 5, 25, 50

і 100 МГц. Технічні можливості використаної ПЛІС дозволяють задати максимальну тактову частоту в 400 МГц. Проте характеристики осцилографа та спотворення сигналів у каналі зв’язку унеможливили дослідження системи у вказаному діапазоні частот.

З порівняння результатів моделювання (рис. 2.13 і 2.14) та експериментального дослідження (рис. 3.5 і 3.6) випливає, що результати чисельного моделювання і експериментального дослідження повністю збігаються. Таким чином, можна зробити висновок, що розроблений генератор на ПЛІС та комп'ютерна модель реалізації системи Лозі працюють правильно. Параметри системи для отримання різних типів хаотичних сигналів в практичній реалізації можна задавати програмно. Така схема може генерувати необхідні хаотичні сигнали, які можна використати для утворення псевдовипадкових послідовностей. Отже, проведений експеримент підтвердив працездатність розробленої схеми.

3.1.3. Тестування ПВП генерованих відображенням Лоці

Таємними параметрами генератора є початкові умови: $x_0^{(1)}$, $x_0^{(2)}$, $x_0^{(3)}$, $x_n^{(4)}$ та параметри керування r і k в нашому випадку $r = 2$. Параметр керування k може приймає значення в діапазоні $k \in [1,\ 2]$. Вибір даного діапазону значень параметру обумовлений врахуванням вікон періодичності та наявністю хаосу в системі, що підтверджується біфуркаційною діаграмою системи (3) яка приведена на рис. 3.8.

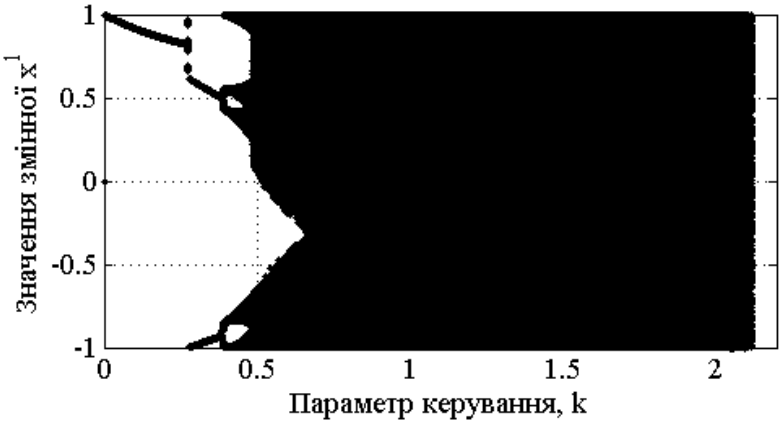


Рис. 3.8. Біфуркаційна діаграма системи (2.11) при $r = 2$

В табл. 3.1 приведені результати тестування за набором статистичних тестів NIST згенерованої послідовності довжиною 10^9 біт при наступних значеннях параметрів та початкових умов: $x_0^{(1)} = 0.292$, $x_0^{(2)} = -0.90258$, $x_0^{(3)} = 0.0258$, $x_n^{(4)} = 0.990258$, $k^{(1)}, k^{(3)}, k^{(2)}, k^{(4)}, r^{(1)}, r^{(3)}, r^{(2)}, r^{(4)} = 2$ та зсуві бітів рівним 0 для всіх M_x.

Таблиця 3.1.
Результати тестування за допомогою тестів NIST SP 800-22

Назва тесту	***P* - значення**	**Пропорція**	**Статус**
Частотний (монобітний) тест	0.958485	0.989	**Пройдено**
Частотний тест по блокам	0.377007	0.993	**Пройдено**
Тест на послідовність однакових бітів	0.281232	0.986	**Пройдено**
Тест на найдовшу послідовність одиниць в блоці	0.049984	0.993	**Пройдено**
Тест рангу бінарних матриць	0.231956	0.993	**Пройдено**
Тест на основі дискретного перетворення Фур'є	0.137282	0.983	**Пройдено**
Тест на співпадіння з шаблоном без перекриття	0.737915	0.990	**Пройдено**
Тест шаблонів з перекриттям	0.353733	0.993	**Пройдено**
Універсальний статистичний тест Маурера	0.450297	0.992	**Пройдено**
Тест лінійної складності	0.353733	0.983	**Пройдено**
Тест серій	0.056069	0.992	**Пройдено**
Тест на основі апроксимації ентропії	0.132640	0.988	**Пройдено**
Тест накопичених сум	0.672470	0.989	**Пройдено**
Тест випадкових відхилень	0.701024	0.990	**Пройдено**
Тест випадкових відхилень - 2	0.947142	0.992	**Пройдено**

Як випливає з табл. 3.1, що генеровані послідовності відповідають критеріям псевдовипадковості згідно набору статистичних тестів NIST SP 800-22. Також генеровані послідовності пройшли тести NIST SP 800-22 при інших значеннях параметрів керування та довжинах вибірок для тестування.

Приклади нормованої автокореляційної (АКФ) та взаємокореляційної (ВКФ) функції для послідовностей генерованих розробленим ГПВП на основі відображення Лоці (2.10) приведені на рис. 3.9.

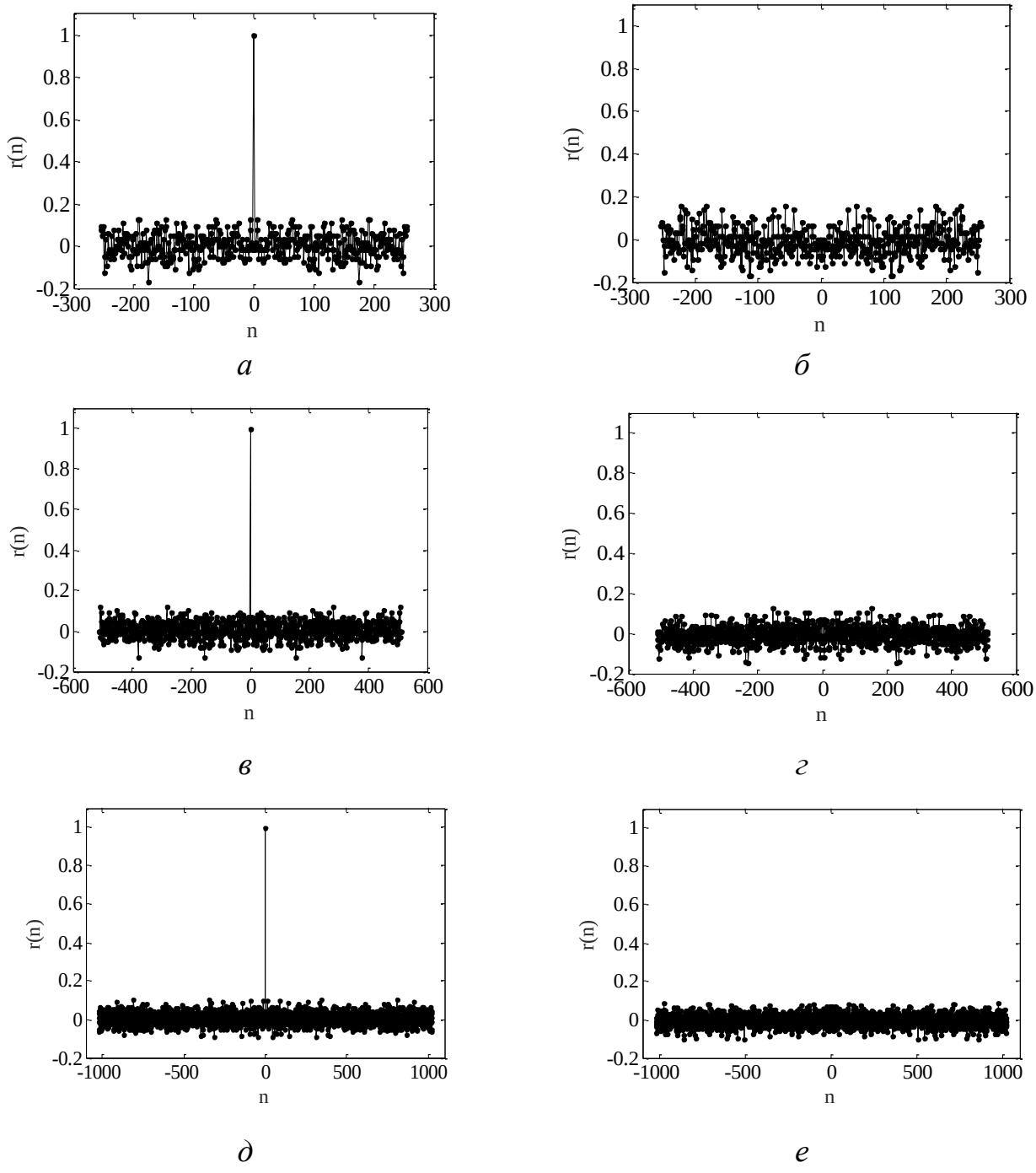


Рис. 3.9. Автокореляційна та взаємокореляційна функція для послідовностей генерованих розробленим ГПВП на основі відображення Лоці (2.10): *а,б* – 256 біт; *в,г* – 512 біт; *д,е* – 1024 біт.

З рис.3.9 випливає, що рівень бічних пелюсток нормованих АКФ та ВКФ не перевищує 0,15 для послідовності довжиною 256 біт та 0,1 для послідовностей довжиною 512 та 1024 біт відповідно.

3.1.4. Реалізація ГПВП на базі системи Тратаса

Структурно простішими багатовимірним відображеннямиз кільцевим зв'язком та неперервною біфуркаційною діаграмою, що не використовують механізмів рандомізації типу (2.11) є гіперхаотична система Тратаса, що описується наступною системою рівнянь [113]:

$$\begin{cases} x(n+1) = a_1 x(n) - b_1 |y(n)| + 1, \\ y(n+1) = a_2 y(n) - b_2 |x(n)| + 1, \end{cases} \tag{3.1}$$

де a_1, a_2, b_1 і b_2 - параметри керування. Система (3.1) детально описана та вивчена в розділі 4.1.

Залежність значень кореляційної розмірності d від розмірності системи p для багатовимірної системи Тратаса з кільцевим зв'язком (3.1) приведено в табл. 3.2.

Таблиця 3.2.
Залежність значень кореляційної розмірності d від розмірності системи p для багатовимірної системи Тратаса

Розмірність системи, p	2	4	6	8	10	12	14	16	18	20
Кореляційна розмірність, d	1.772	3.7228	5.591	7.0118	9.1844	9.889	10.85	11.95	12.636	14.916

З таблиці 3.2 випливає, що багатовимірна система Тратаса забезпечує середні кращі в порівнянні з логістичним відображенням псевдовипадкові характеристики і більші середні тривалості періодів повторення генерованих часових рядів при апаратній реалізації, однак поступається багатовимірному відображенню Лоці (2.10).

Оскільки послідовності генеровані ГПВП на базі двовимірної системи Тратаса при використанні арифметики з фіксованою точкою Q5.27 характеризуватимуться короткими циклами тому ми перетворимо систему Тратаса з двовимірної в шестивимірну згідно (рис. 2.12). Тоді (3.1) при $p = 6$ набуде вигляду:

$$\begin{cases} x_1(n+1) = a_1|x_1(n)| - b_1|x_2(n)| + 1 \\ x_2(n+1) = a_2|x_2(n)| - b_2|x_3(n)| + 1 \\ x_3(n+1) = a_3|x_3(n)| - b_3|x_4(n)| + 1 \\ x_4(n+1) = a_4|x_4(n)| - b_4|x_5(n)| + 1 \\ x_5(n+1) = a_5|x_5(n)| - b_5|x_6(n)| + 1 \\ x_6(n+1) = a_6|x_6(n)| - b_6|x_1(n)| + 1 \end{cases} \quad (3.2)$$

Розподіл значень послідовностей ітерацій x_1, x_2, x_3, x_4, x_5 і x_6 є нерівномірним і асиметричним оскільки бінарне представлення значень змінних x_1, x_2, x_3, x_4, x_5 і x_6 є незбалансованим. Для визначення діапазону збалансованих бітів обчислимо кількість “0” - N_0 і “1” - N_1, для кожного розряду так щоб $N_0 + N_1 = N$, результат приведений на рис. 3.10.

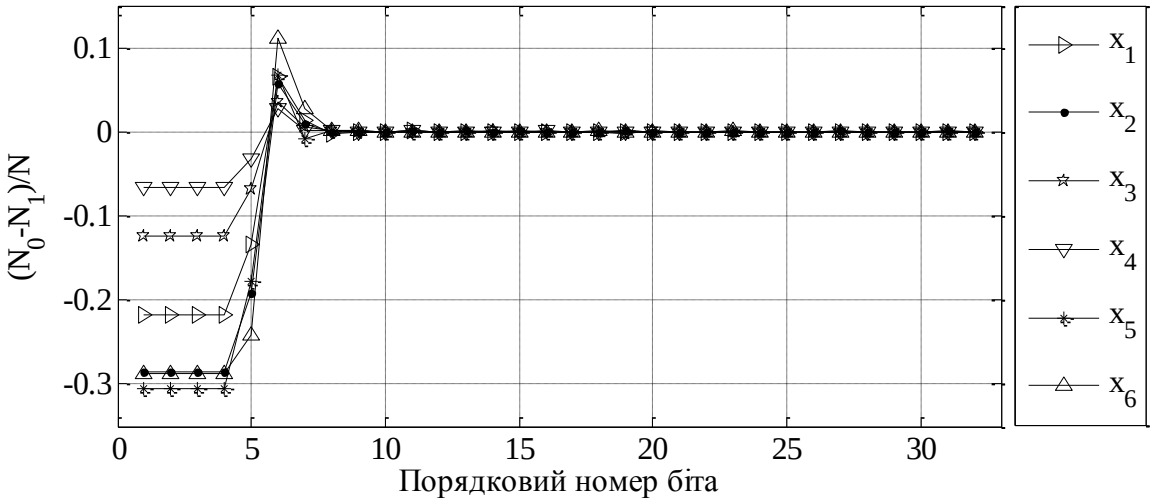


Рис.3.10. Збалансованість бітів генерованих системою Тратаса (3.1).

Для тестування послідовностей використаємо спрощену структуру генератора (рис. 2.16) приведену на рис. 3.11.

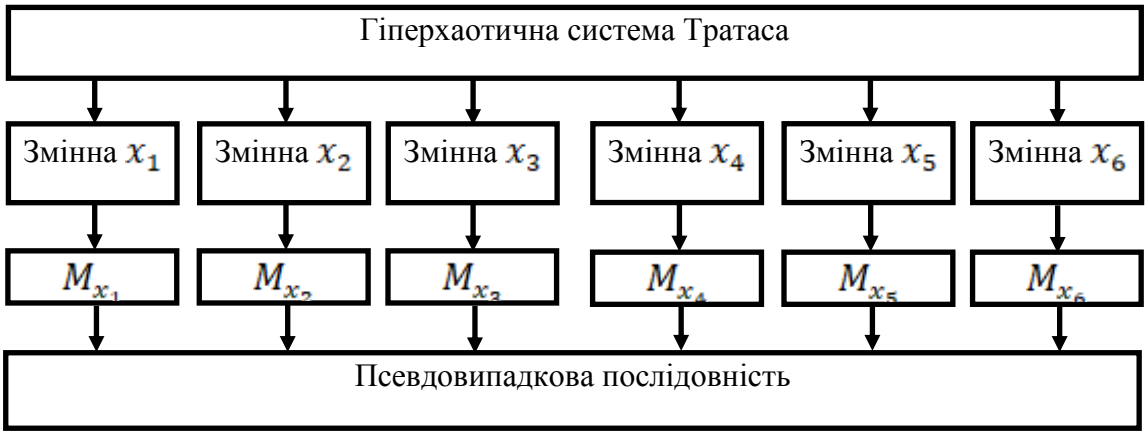
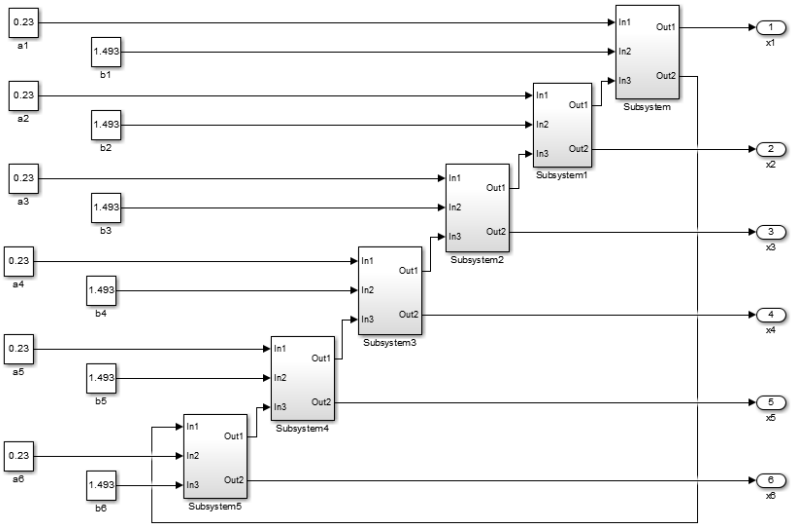


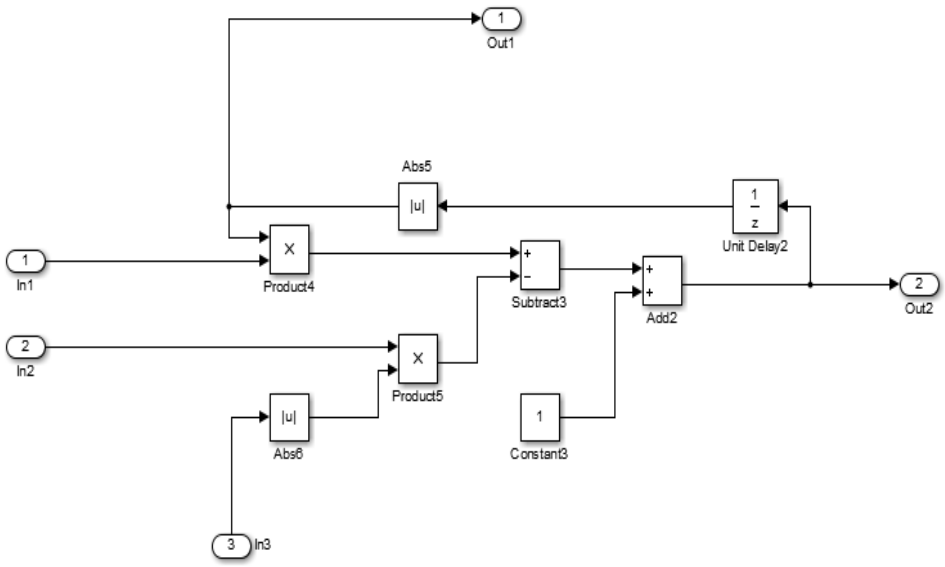
Рис. 3.11. Спрощенна блок-схема генератора ПВП.

При реалізації генератора використовуватимемо арифметику з фіксованою комою Q5.27. В блоці вибору збалансованих біт M_x ми вибираємо 16 бітів з кожного бінарного представлення значення змінних діапазоні від 11 до 27 біта. В результаті ми отримуємо 96 бітів з шести значень *x*.

Значення параметрів керування a_1, a_2, a_3, a_4, a_5, a_6, b_1, b_2, b_3, b_4, b_5, b_6 і початкових умов $x_1(0)$, $x_2(0)$, $x_3(0)$, $x_4(0)$, $x_5(0)$ і $x_6(0)$ будуть сеансовим ключем. Для апаратної реалізації розроблено Simulink модель системи (3.2) яка приведена на рис. 3.12 [6].



а



б

Рис. 3.12. Simulink модель системи Тратаса:

а - загальна структура, *б* – структура підсистеми

Результати тестування статистичних властивостей генерованих послідовностей приведено в таб. 3.3. Для тестування згенеровано послідовність довжиною 10^9 бітів яка при тестуванні була розділена на 1000 полсідовностей по 1 мільйону бітів кожна. При тестувані використано наступні параметри: $a_1 = 0{,}239$, $a_2 = 0{,}231$, $a_3 = 0{,}239$, $a_4 = 0{,}3$, $a_5 = 0{,}323$, $a_6 = 0{,}123$, $b_1 = 1{,}493$, $b_2 = 1{,}495$, $b_3 = 1{,}4931$, $b_4 = 1{,}9493$, $b_5 = 1{,}4493$, $b_6 = 1{,}3$, $x_1^0 = 0{,}2$, $x_2^0 = 0{,}5$, $x_3^0 = 1$, $x_4^0 = 0{,}25$, $x_5^0 = 1{,}5$, $x_6^0 = -0{,}9$.

Таблиця 3.3.

Результати тестування послідовностей статистичними тестами NIST

Назва тесту	***P* - значення**	**Пропорція**	**Статус**
Частотний (монобітний) тест	0,468595	1,000	**Пройдено**
Частотний тест по блокам	0,253551	0,978	**Пройдено**
Тест на послідовність однакових бітів	0,368773	0,989	**Пройдено**
Тест на найдовшу послідовність одиниць в блоці	0,189397	1,000	**Пройдено**
Тест рангу бінарних матриць	0,804337	0,989	**Пройдено**
Тест на основі дискретного перетворення Фур'є	0,579479	0,989	**Пройдено**
Тест на співпадіння з шаблоном без перекриття	0,368773	0,989	**Пройдено**
Тест шаблонів з перекриттям	0,879806	0,989	**Пройдено**
Універсальний статистичний тест Маурера	0,739918	0,967	**Пройдено**
Тест лінійної складності	0,694743	0,978	**Пройдено**
Тест серій	0,368773	0,989	**Пройдено**
Тест на основі апроксимації ентропії	0,602458	1,000	**Пройдено**
Тест накопичених сум	0,761937	0,989	**Пройдено**
Тест випадкових відхилень	0,517442	1,000	**Пройдено**
Тест випадкових відхилень - 2	0,392456	1,000	**Пройдено**

Як випливає з табл. 3.3, що генеровані послідовності відповідають критеріям псевдовипадковості згідно набору статистичних тестів NIST SP 800-22. Також генеровані послідовності пройшли тести NIST SP 800-22 при інших значеннях параметрів керування та довжинах вибірок для тестування.

3.2. Апаратна реалізація реалізація ГПВП на базі мемристивних хаотичних систем

3.2.1. Порівняння ефективності чисельних методів для реалізації на ПЛІС.

Розв’язки чисельними методами диференційних рівнянь відрізняються ступенем їх наближення до точних розв’язків системи [100]. Розв’язки отримані при моделюванні хаотичних систем з врахуванням їх чутливості до як завгодно малих відхилень початкових умов на великих проміжках часу значно відрізняються від точних розв’язків. Метою моделювання нелінійної системи є отримання реалізацій, що зберігають статистичні властивості ідеальних систем. Більшість хаотичних систем є ергодичними, тому їх дослідження можна проводити на основі однієї реалізації. Проте розв’язки отримані методом чисельного моделювання повинні зберігати поведінку хаотичного атрактора.

Суть чисельних методів полягає у представленні системи диференційних рівнянь у вигляді рекурентної залежності та розрахунку послідовності точок на траєкторії у дискретні моменти часу з кроком Δt.

Найбільш простим за обчислювальною складністю є метод Ейлера, в якому зв'язок між сусідніми точками траєкторій системи (2.14) описується наступною залежністю:

$$\begin{cases} x_{n+1} = f_1(t_n, y_n)\triangle t + x_n \\ y_{n+1} = f_2(t_n, x_n, y_n, z_n)\triangle t + y_n \\ z_{n+1} = f_3(t_n, y_n, z_n)\triangle t + z_n \end{cases} \tag{3.3}$$

де

$$\begin{cases} f_1 = \dfrac{y_n}{C} \\ f_2 = -\dfrac{1}{L}\left[x_n + \beta(z_n^2 - 1)y_n \right]. \\ f_3 = -y_n - \alpha z_n + y_n z_n \end{cases}$$

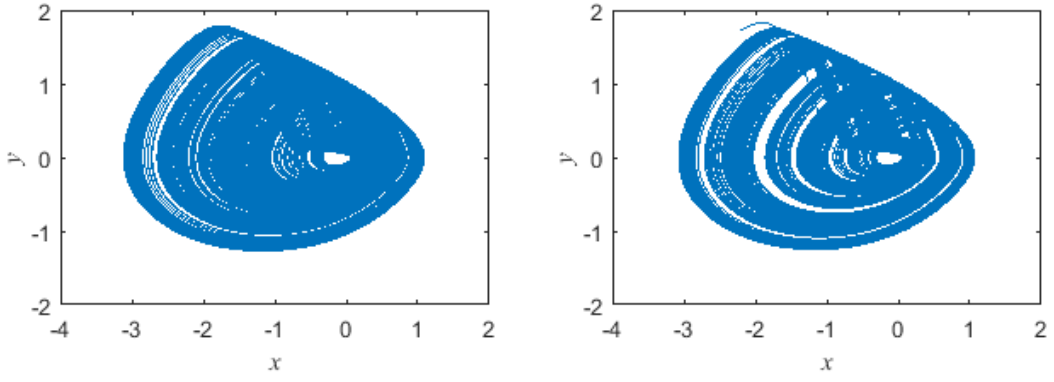
Широкого застосування набув метод Рунге-Кутти четвертого порядку, що характеризується вищою точністю розрахунків. Згідно цьому методу залежність між станами системи (2.14) у послідовні дискретні моменти часу є наступною:

$$
\begin{cases}
x_{n+1} = x_n + \dfrac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4), \\
y_{n+1} = y_n + \dfrac{1}{6}(m_1 + 2m_2 + 2m_3 + m_4), \\
z_{n+1} = z_n + \dfrac{1}{6}(l_1 + 2l_2 + 2l_3 + l_4),
\end{cases} \tag{3.4}
$$

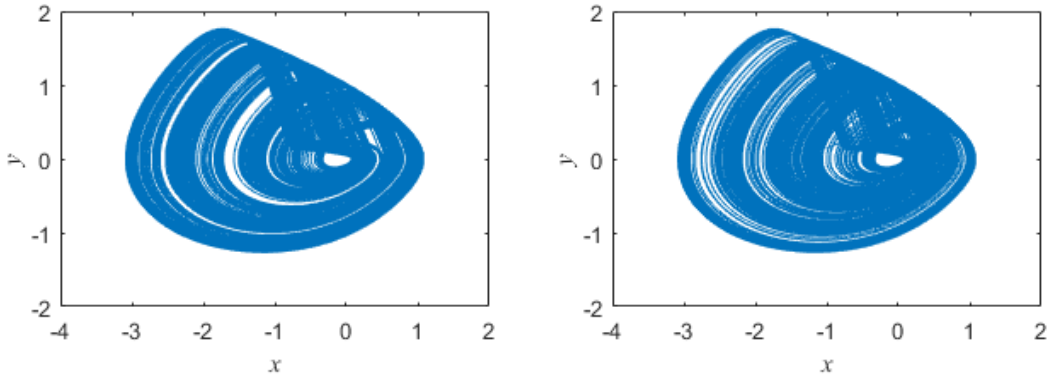
де

$$
\begin{aligned}
k_1 &= f_1(t_n, y_n)\triangle t, \\
m_1 &= f_2(t_n, x_n, y_n, z_n)\triangle t, \\
l_1 &= f_3(t_n, y_n, z_n)\triangle t, \\
k_2 &= f_1(t_n + \frac{\triangle t}{2}, y_n + \frac{m_1}{2})\triangle t, \\
m_2 &= f_2(t_n + \frac{\triangle t}{2}, x_n + \frac{k_1}{2}, y_n + \frac{m_1}{2}, z_n + \frac{l_1}{2})\triangle t, \\
l_2 &= f_3(t_n + \frac{\triangle t}{2}, y_n + \frac{m_1}{2}, z_n + \frac{l_1}{2})\triangle t, \\
k_3 &= f_1(t_n + \frac{\triangle t}{2}, y_n + \frac{m_2}{2})\triangle t, \\
m_3 &= f_2(t_n + \frac{\triangle t}{2}, x_n + \frac{k_2}{2}, y_n + \frac{m_2}{2}, z_n + \frac{l_2}{2})\triangle t, \\
l_3 &= f_3(t_n + \frac{\triangle t}{2}, y_n + \frac{m_2}{2}, z_n + \frac{l_2}{2})\triangle t, \\
k_4 &= f_1(t_n + \triangle t, y_n + m_3)\triangle t, \\
m_4 &= f_2(t_n + \triangle t, x_n + k_3, y_n + m_3, z_n + l_3)\triangle t, \\
l_4 &= f_3(t_n + \triangle t, y_n + m_3, z_n + l_3)\triangle t.
\end{aligned}
$$

Приклади портретів фазових атракторів отриманих при застосуванні методу Ейлера та Рунге-Кутти приведені на рис. 3.13. Рис. 3.13 *а* і *б* отримані з використанням арифметики Q24.16, а *в* і *г* з використанням арифметики Q32.24. Всі атрактори характеризуються однаковою структурою з однаковим розмахом реалізацій незалежно від точності розрахунків.



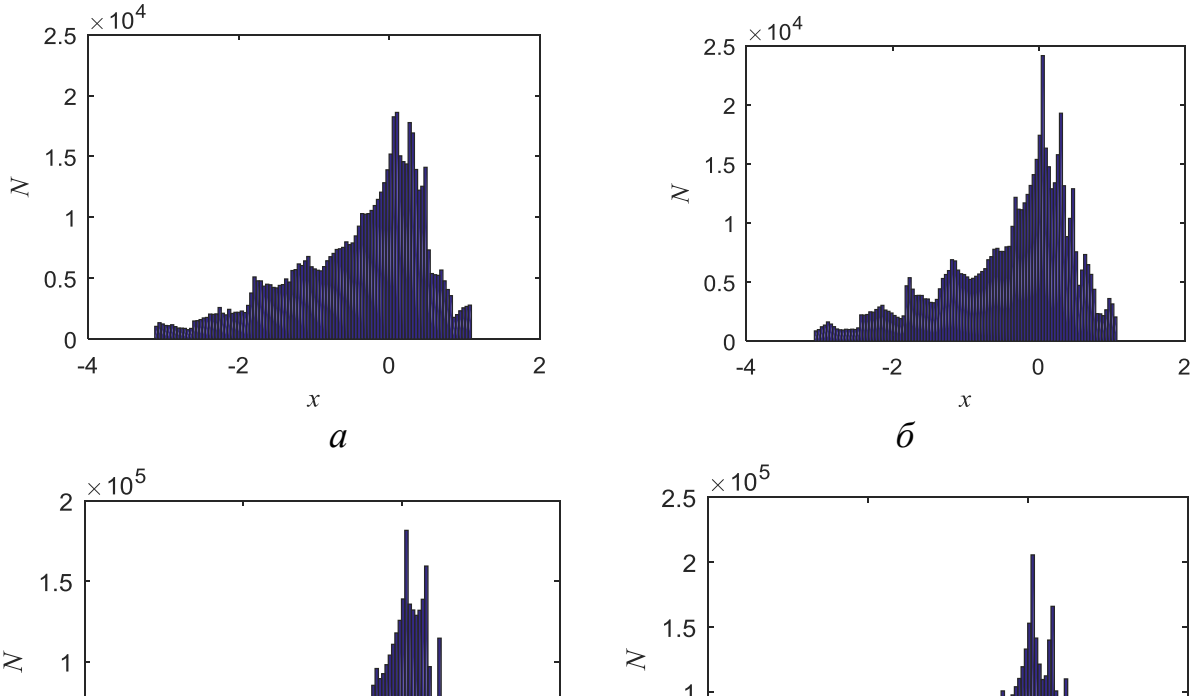
а *б*



в *г*

Рис. 3.13. Хаотичний атрактор системи (3.3) при $\Delta t = 0,001$ розрахунках методами Ейлера – *а, в*; Рунге-Кутти четвертого порядку – *б, г*.

Гістограми розподілу змінної *x* для різної точності та методів розрахунку є подібними (рис. 3.13), що вказує на збереження фрактальних розмірностей системи.



а *б*

в *г*

Рис. 3.14. Гістограми розподілу реалізацій змінної *x* системи (4.3) при $\Delta t = 0,001$ розрахунках методами Ейлера – *а, в*; Рунге-Кутти– *б, г*.

Рис. 3.13, 3.14 *а* і *б* отримані для арифметики Q24.16, *в* і *г* для арифметики Q32.24 З аналізу залежностей представлених на рис. 3.13 і рис. 3.14 випливає висновок про однакову результативність застосування методів Ейлера та Рунге-Кутти. Збереження комою Q8.16 з точністю 24 біти, з яких 16 біт відведено на дробову частину. Приклад реалізації (3.3) за допомогою методу Ейлера приведено на рис. 3.15.

У схемі використано стандартні засоби Simulink, операція інтегрування здійснюється блоками “Discrete-Time integrator”. При розрахунках проводилося заокруглення до меншого значення.

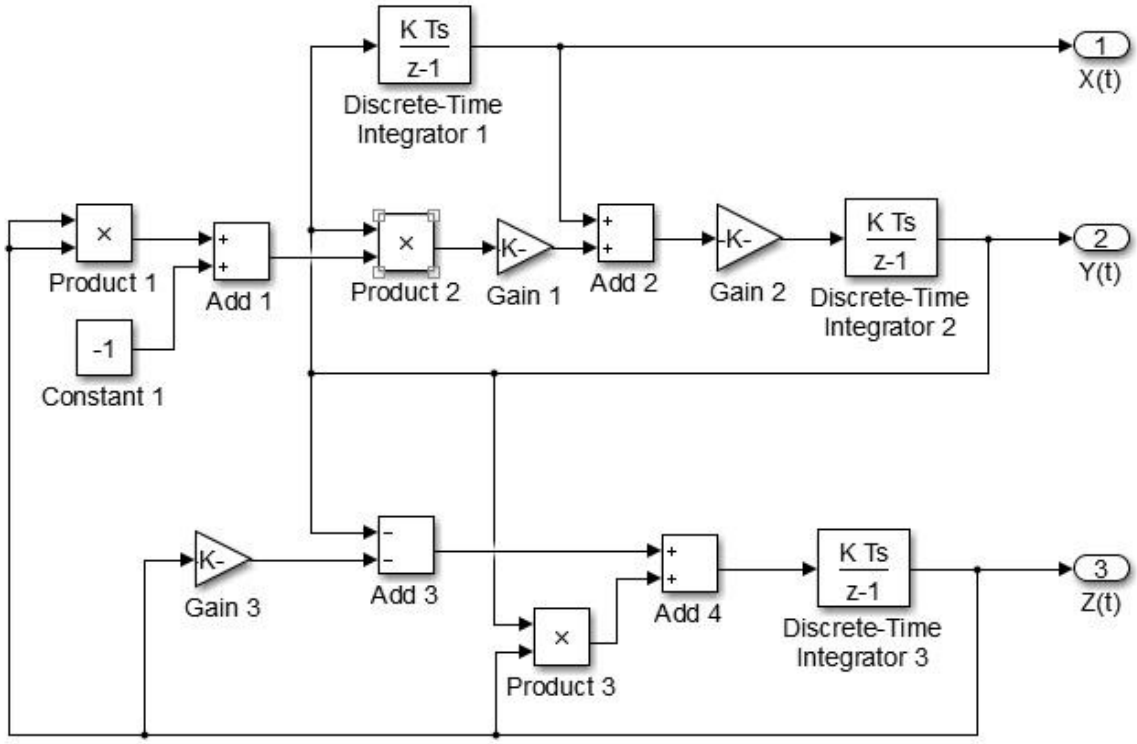


Рис. 3.15. Simulink-модель хаотичної системи для розрахунків методом Ейлера

Для 25 значень випадкових початкових умов, та 25 значень параметрів системи в околі $\beta = 1{,}5$ та $\alpha = 0{,}6$ залежність середнього періоду, що встановлюється внаслідок деградації хаотичної системи, від кроку по часу приведено на рис. 3.16.

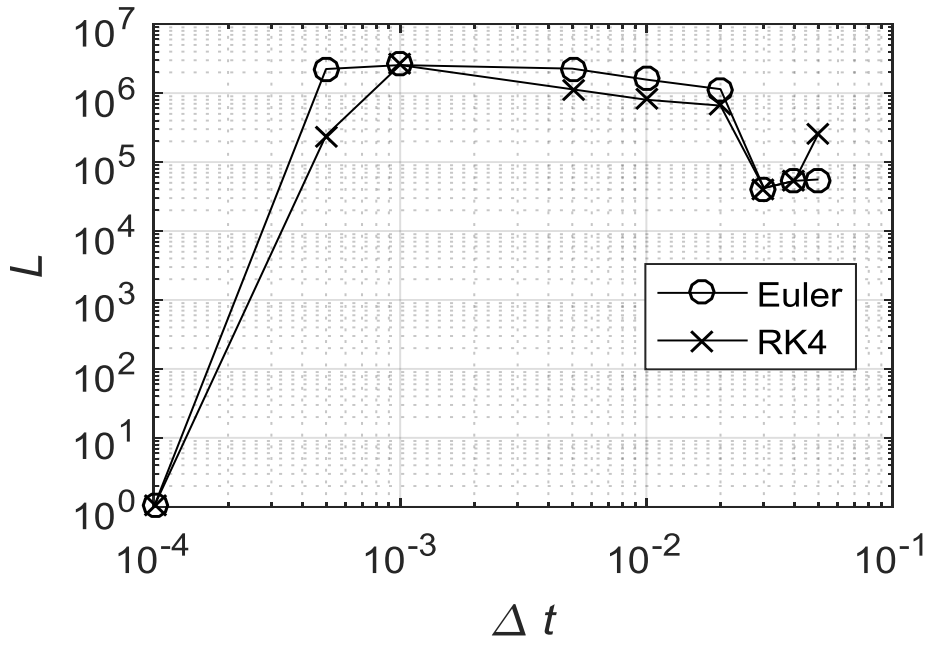


Рис. 3.16. Залежність середнього періоду від кроку по часу для методу Ейлера та Рунге-Кутти четвертого порядку.

З рис. 3.16 випливає, що збільшення складності розрахунків не призводить до збільшення тривалості періоду повторення реалізацій системи. Середня тривалість циклу знаходиться в межах $10^6 \div 2 \cdot 10^6$ ітерацій і не залежить від кроку дискретизації при $\Delta t = 0{,}0005 \div 0{,}02$. При $\Delta t = 0{,}0001$ для обох методів розрахунку спостерігається колапс хаосу. Після перехідного процесу система виходить на цикл довжиною одну ітерацію (рис. 3.17).

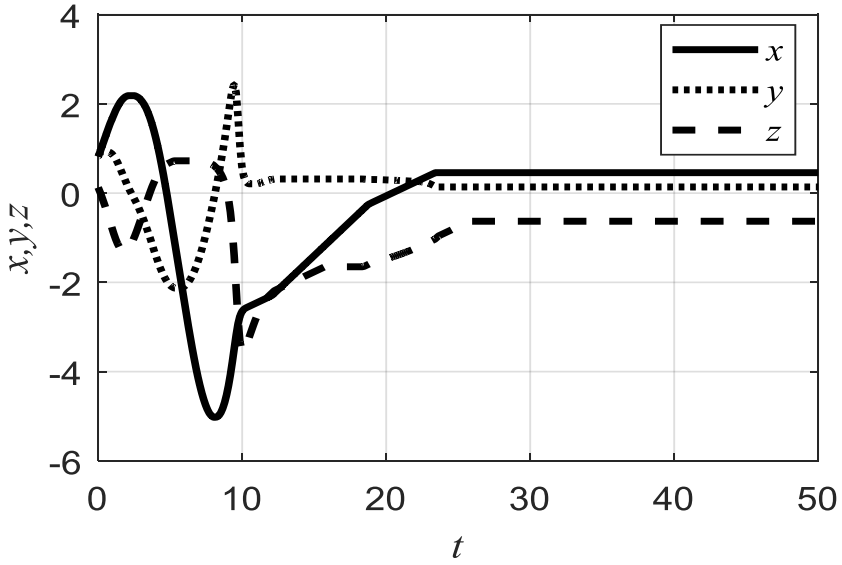


Рис. 3.17. Колапс хаотичної системи при $\Delta t = 0{,}0001$

У випадку зростання інтервалу дискретизації, при $\Delta t \geq 0,03$ середнє значення періоду повторення зменшується до $\sim 5 \cdot 10^4$, що може бути обумовлено зміною динаміки системи внаслідок лінеаризації на великому проміжку часу.

3.2.2. Генерування ПВП на базі схеми Чуа з мемристором

Щоб визначити діапазон бітів які необхідно використовувати для формування послідовностей обчислено збалансованість бітів (рис. 3.18) в бінарному представлені значень генерованих (3.3).

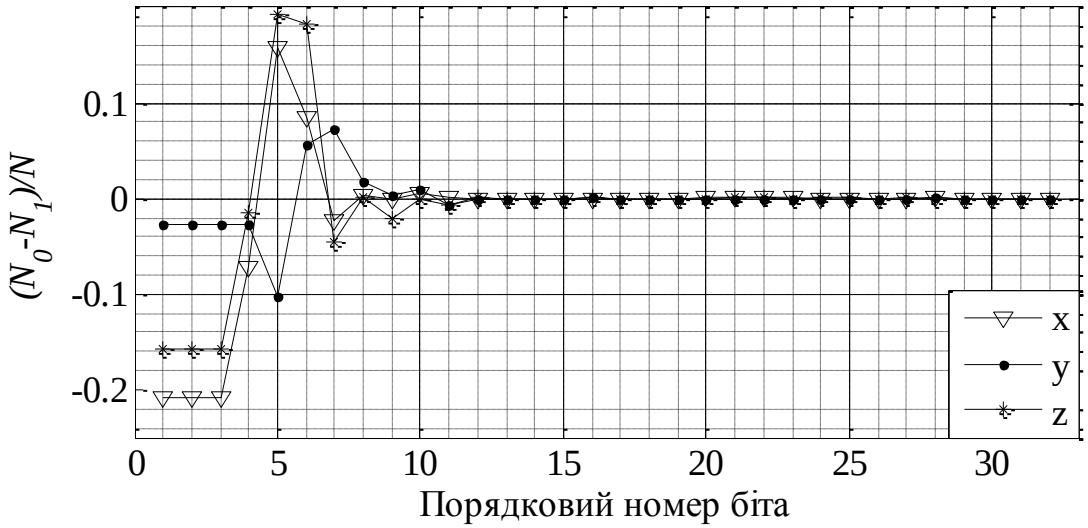
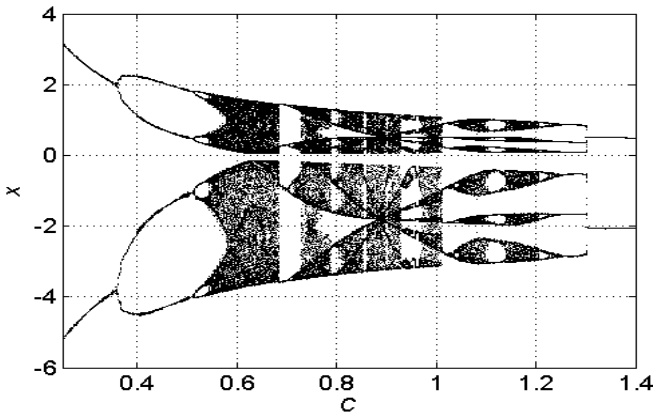
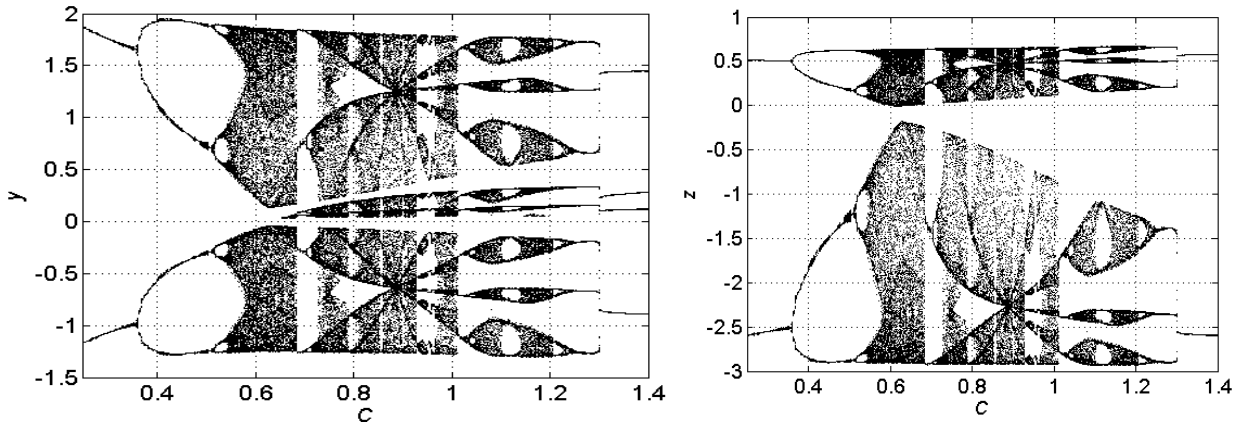


Рис. 3.18. Збалансованість бітів в бінарному представлені значень (3.4) при використані арифметики Q5.27.

Біфуркаційна діаграма системи (3.3) при фіксованих значеннях параметрів α і β для нелінійної частини приведена на рис. 3.19 і 3.20.

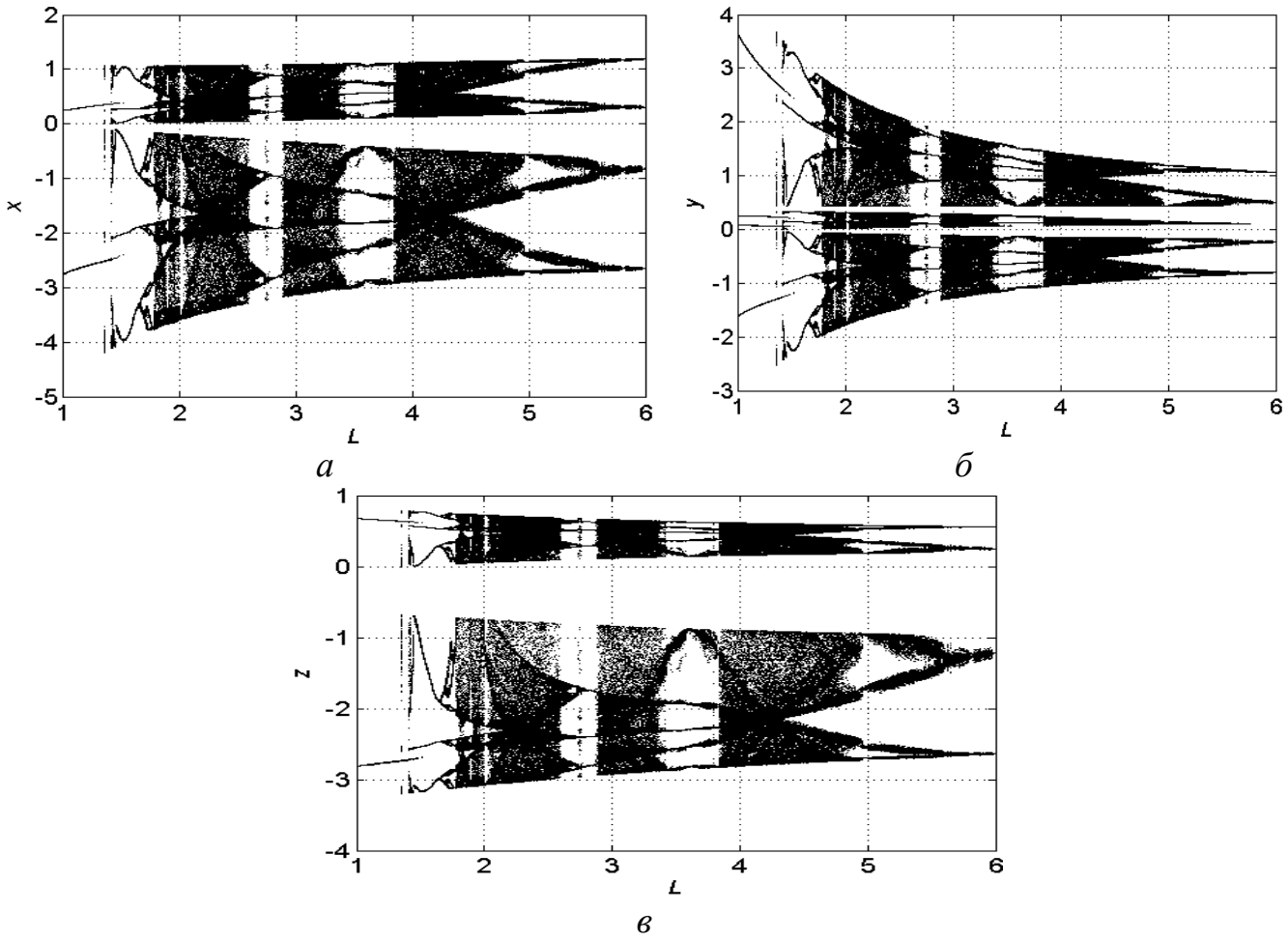


a



б *в*

Рис. 3.19. Біфуркаційна діаграма системи (3.4) при $\beta = 1.52,\ L = 3,\ \alpha = 0.6$: *а* – для сигналу *x*, *д* – для сигналу *y*, *в* – для сигналу *z*.

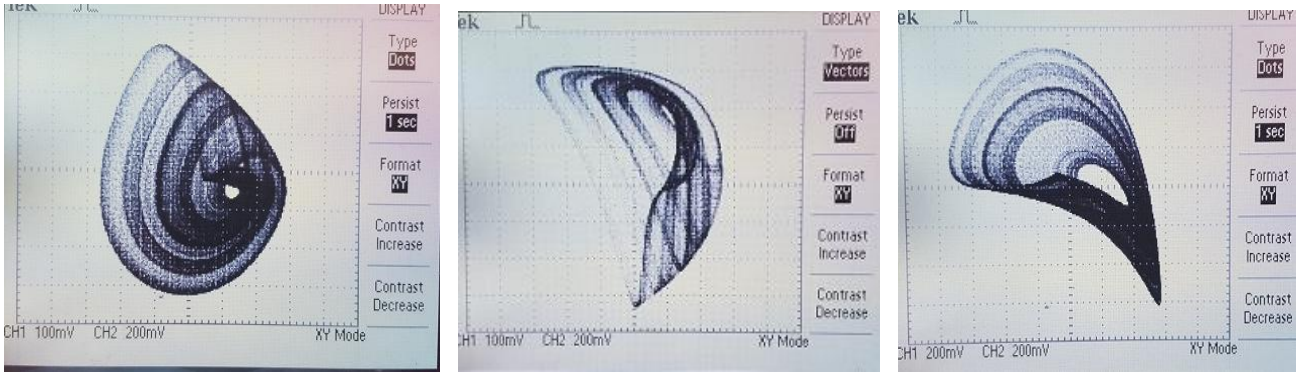


а *б* *в*

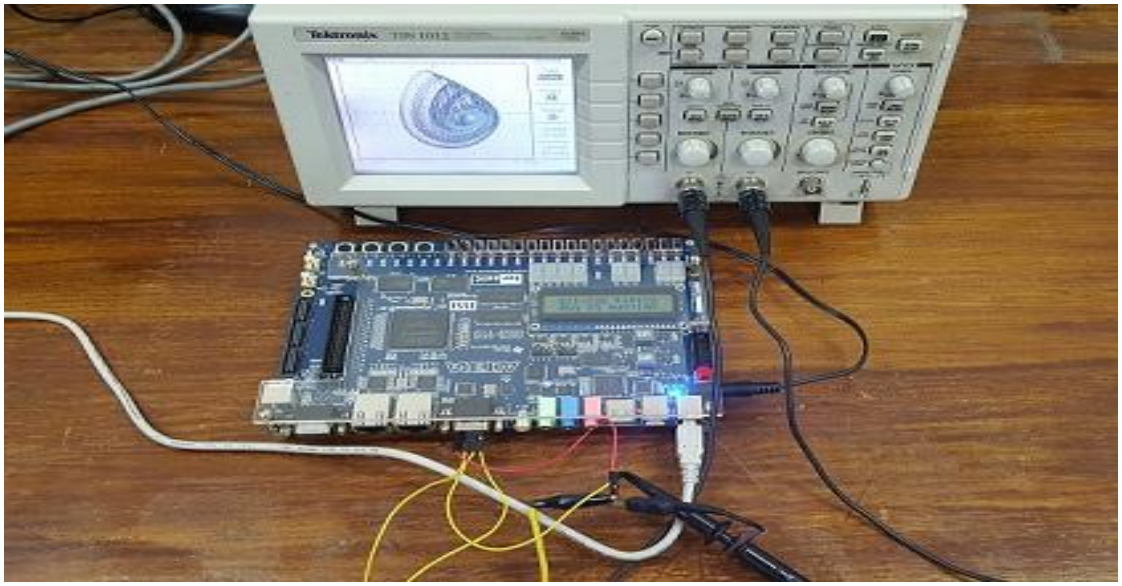
Рис. 3.20. Біфуркаційна діаграма системи (3.4) при $\beta = 1.52,\ C = 1,\ \alpha = 0.6$: *а* – для сигналу *x*, *д* – для сигналу *y*, *в* – для сигналу *z*.

З рис. 3.19 і 3.20 випливає, що система характеризується широкими неперервними діапазонами значень параметрів керування, за якими мають місце

хаотичні режими що уможливлює спрощення технологічних вимог до розкиду значень номіналів елементів схеми. Експериментально отримані фазові портрети при апаратній реалізації системи (3.3) із використанням арифметики із фіксованою комою Q8.24 приведені на рис. 3.21.



а *б* *в*



г

Рис. 3.21. Експериментально отримані фазові портрети при апаратній реалізації системи (3.3): *а- x(y), б- x(z), в- y(z), г-* проведення експерименту

Для формування псевдовипадкової послідовності вибираємо з кожної серії *x*, *y* та *z* 24 біти з діапазону від 18 до 27 згідно (рис. 3.18). В таб. 3.3 приведені результати тестування за набором статистичних тестів NIST згенерованої послідовності довжиною 10^9 біт при наступних значеннях параметрів: $\beta = 1.52,\ L = 3.0,\ \alpha = 0.6$.

Таблиця 3.4

Результати тестування послідовностей статистичними тестами NIST

Назва тесту	***P* - значення**	**Пропорція**	**Статус**
Частотний (монобітний) тест	0.616305	0.990	**Пройдено**
Частотний тест по блокам	0.202268	0.990	**Пройдено**
Тест на послідовність однакових бітів	0.304126	1.000	**Пройдено**
Тест на найдовшу послідовність одиниць в блоці	0.739918	1.000	**Пройдено**
Тест рангу бінарних матриць	0.350485	1.000	**Пройдено**
Тест на основі дискретного перетворення Фур'є	0.028817	1.000	**Пройдено**
Тест на співпадіння з шаблоном без перекриття	0.401199	0.980	**Пройдено**
Тест шаблонів з перекриттям	0.236810	1.000	**Пройдено**
Універсальний статистичний тест Маурера	0.699313	0.990	**Пройдено**
Тест лінійної складності	0.935716	0.970	**Пройдено**
Тест серій	0.145326	1.000	**Пройдено**
Тест на основі апроксимації ентропії	0.494392	1.000	**Пройдено**
Тест накопичених сум	0.236810	0.990	**Пройдено**
Тест випадкових відхилень	0.619772	0.985	**Пройдено**
Тест випадкових відхилень - 2	0.551026	0.985	**Пройдено**

Як випливає з табл. 3.4 послідовності генеровані ГПВП на основі мемристивної хаотичної системи відповідають критеріям псевдо випадковості згідно набору статистичних тестів NIST SP 800-22.

Висновки до третього розділу

1. За допомогою чисельних методів Ейлера та Рунге-Кутти досліджено математичну модель мемристивної хаотичної системи з використанням арифметики з фіксованою комою. Проведено порівняльний аналіз ефективності чисельних методів розв'язку нелінійних диференційних рівнянь, що описують

хаотичні системи. Показано, що застосування методу Рунги-Кутти не призводить до збільшення періоду повторення псевдохаотичних рядів.

2. Проведено апаратну реалізацію на ПЛІС генераторів псевдовипадкових послідовностей на основі відображення Лоці та гіперхаотичної системи Тратаса. Встановлено, що генеровані послідовності відповідають критеріям псевдовипадковості згідно набору статистичних тестів NIST.

3. Показано, що запропонована структура генератора забезпечує паралельний розрахунок змінних, що дозволяє збільшувати швидкість генерування без часових втрат.

4. За допомогою запропонованого ГПВП на основі системи Лоці потенційно можлива швидкість генерування ПВП при використанні чотиривимірної системи становить до 19,2 Гбіт/с.

РОЗДІЛ 4.
СХЕМОТЕХНІЧНА РЕАЛІЗАЦІЯ НДС ІЗ ДИСКРЕТНИМ ЧАСОМ

При виборі дискретної динамічної системи в якості бази генератора випадкових сигналів необхідно керуватися критеріями виборе відображення в якості бази ГПВП. Однак, складність реалізації систем у інтегральному виконані із заданим розкидом параметрів та прецизійності їх контролю обмежують кількість багатовимірних нелінійних динамічних систем, що можуть бути використані в якості бази генератора випадкових послідовнойстей при його схемотехнічній реалізації. Збільшення кількості елементів електронного кола призводить до ускладнення узгодження плечей кола у випадку використання багатовимірного відображення із кільцевим зв'язком. Для реалізації генератора на основі багатовимірних систем можуть бути використані сімейство хаотичних систем Лоці та гіперхаотична система Тратаса [109, 113], що мають неперервну біфуркаційну діаграму та здатні генерувати послідовності із рівномірним розподілом значень. Проведено дослідження динамічних характеристик вказаних систем.

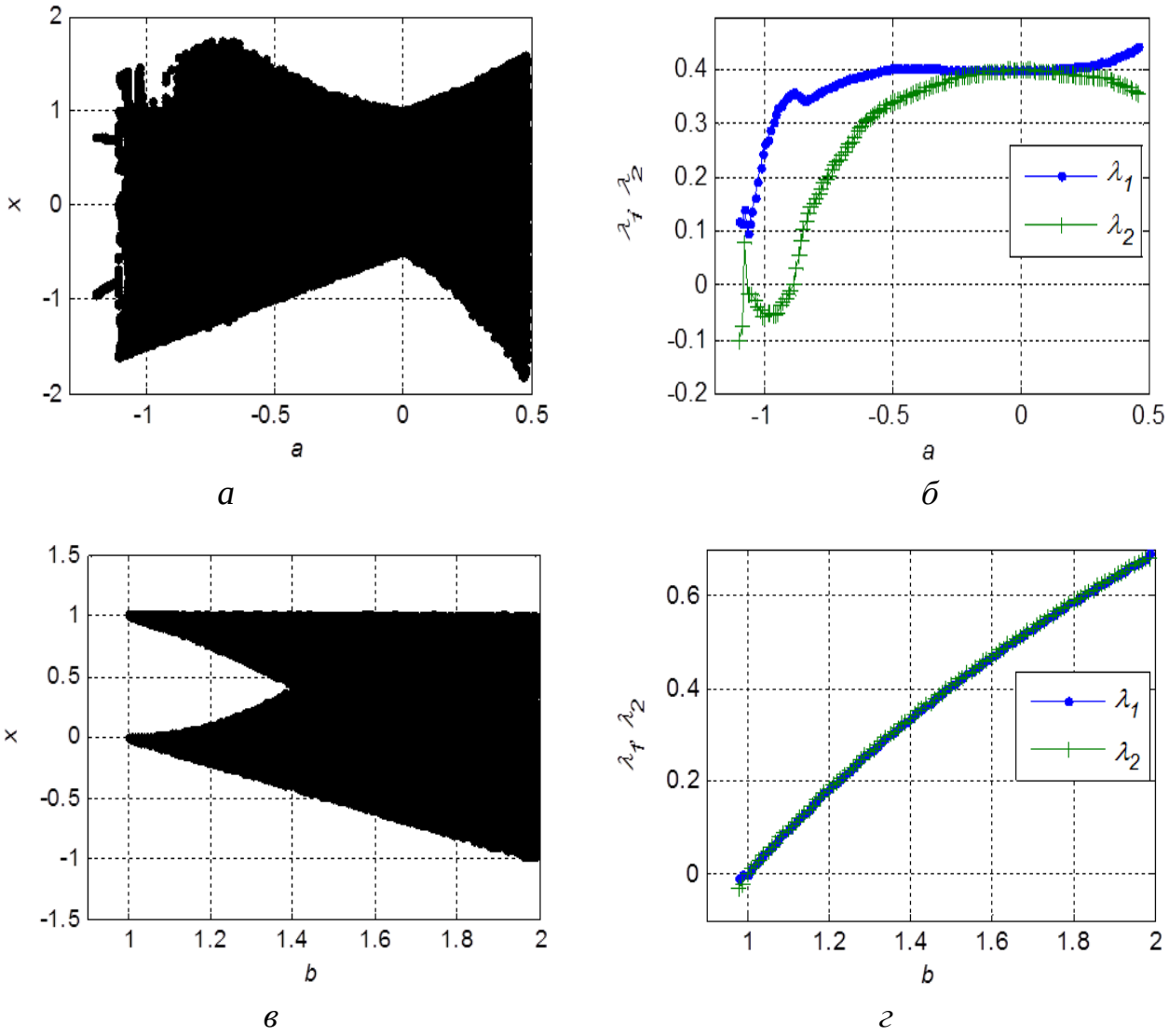
4.1. Багатовимірні НДС із неперервною біфуркаційною діаграмою

4.1.1. Система Тратаса

У системі Тратаса (3.1) в залежності від параметрів керування можуть виникати хаотичні або гіперхаотичні коливання [1]. Біфуркаційна діаграма та залежність значень показників Ляпунова від параметрів керування a та b приведені на рис. 4.1.

Із рис. 4.1 *а, в* випливає, що гіперхаотичні коливання у системі Тратаса мають місце в діапазоні значень параметрів керування $a \in [-0.8, 0.5]$ та $a \in (1, 2)$.

Для значень параметру керування $a = [-1;\ 0,48]$ та параметру $b = 1.493$ та значень параметру $b = [1,42;\ 1,989]$ при $a = [0.01]$ вікон періодичності в залежностях не виявлено.



а *б* *в* *г*

Рис. 4.1. Біфуркаційна діаграма – (*а*) та залежність значень показників Ляпунова від a при b=1,493 – (*б*); біфуркаційна діаграма – (*в*) та залежність показників Ляпунова від b при a=0,01 – (*г*)

4.1.2. Дослідження динамічних режимів роботи системи Тратаса

Розподіл значень хаотичних коливань генерованих (3.1) є неперервним між мінімальними та максимальними значенями. При розробці генераторів псевдовипадкових та випадкових послідовностей систему (3.1) необхідно трансформувати в багатовимірне відображення із кільцевим зв'язком:

$$\begin{cases} x_1(n+1) = a_1 |x_1(n)| - b_1 |x_2(n)| + 1 \\ x_2(n+1) = a_2 |x_2(n)| - b_2 |x_3(n)| + 1 \\ \cdots \\ x_d(n+1) = a_d |x_d(n)| - b_d |x_1(n)| + 1 \end{cases}, \qquad (4.1)$$

де d – розмірність системи.

Фазові портрети системи (3.1) в режимі неперіодичних автоколивань приведені на рис. 4.2. Із рис. 4.1 *б* випливає, що при $a = -0,95$; $b = 1,493$ один із показників Ляпунова системи є додатнім $\lambda_1 = 0,33$, а інший від'ємним $\lambda_2 = -0,048$, що підтверджує встановлення режиму хаотичних коливань в системі. Рівняння (3.1) описують дві незалежні системи із повною синхронізацією, оскільки їх коливання є ідентичними (рис. 4.2 *а*). Нелінійна функція перетворення $x(n+1) = f(x(n))$ є кусково лінійним відображенням, що складається із двох лінійних сегментів (рис. 4.3 *а*). Із збільшенням значень параметрів a і b до $-0,75$ та $1,493$ відповідно значеня показників Ляпунова є додатніми і становить $\lambda_1 = 0.369$, $\lambda_2 = -0.21$. Це вказує на встановлення в системі режиму гіперхаосу (рис 4.2 *б*). Для додатніх значень параметру a в системі мають місце гіперхаотичні коливання (рис. 4.2 *в*).

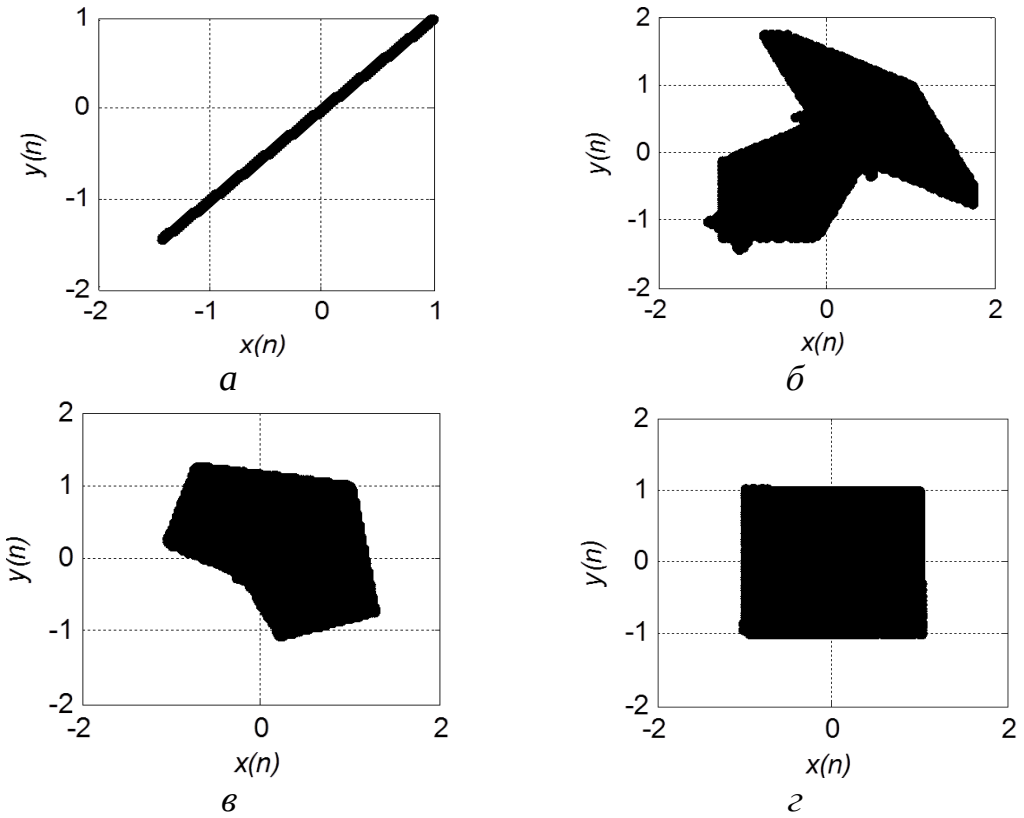
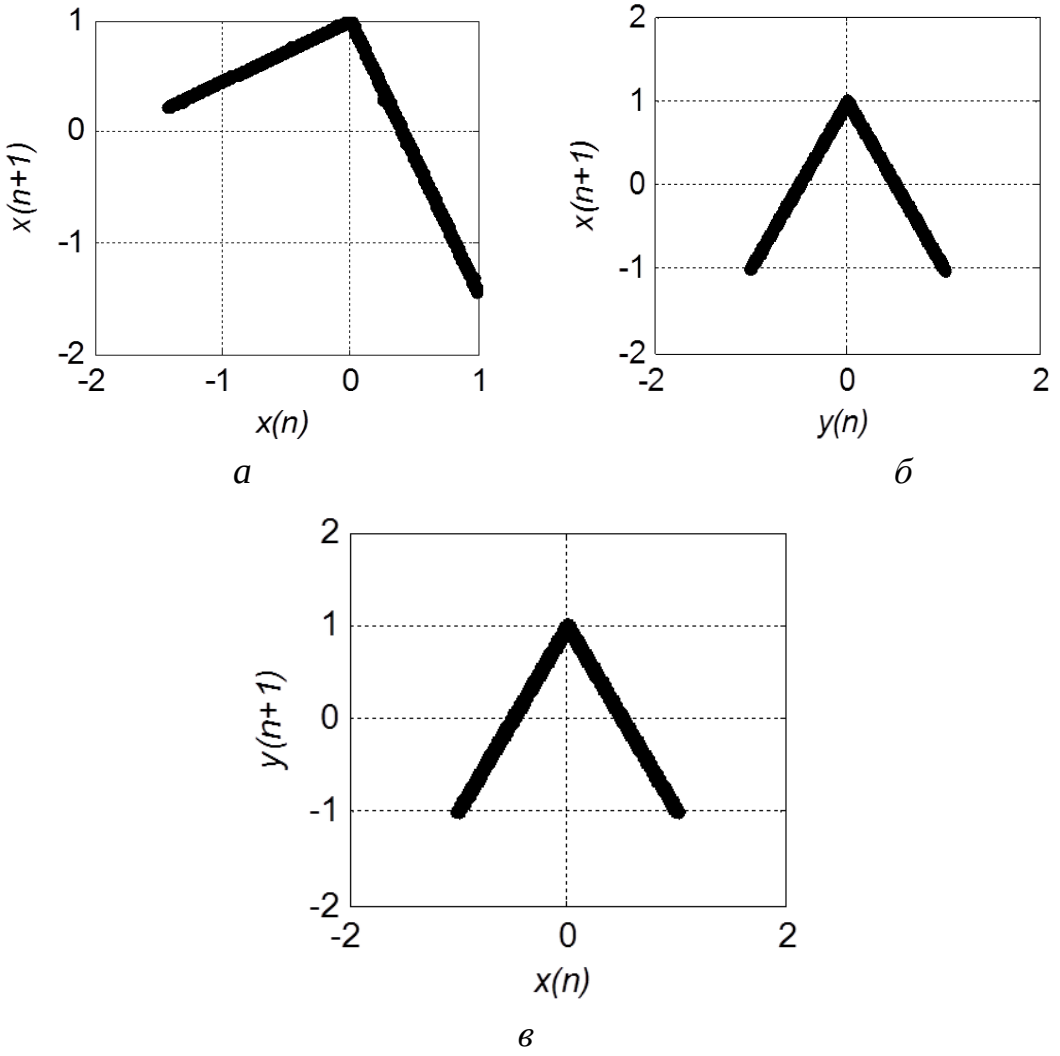


Рис. 4.2. Фазовий портрет відображення (3.1): хаотичний режим (*а*) при $a=-0.95$, $b=1,493$; гіперхаотичний режим (*б*): при $a=-0,75$, $b=1,493$; при $a=0,23$, $b=1,493$ – (*в*); при $a=0,01$, $b=1,98$ – (*г*).

При $a \to 0$, $b = 2 - a \to 2$ обидва показники Ляпунова приймають майже однакові значення, що прямують до $ln\,2$. На рис. 4.2 *г* фазовий портрет має форму квадрату в якому рівномірно розміщені точки, що свідчить про слабку статистичну залежність двох часових рядів $x(n)$ і $y(n)$.



а *б* *в*

Рис. 4.3. Графічне представлення функції нелінійного перетворення при $a = -0{,}95$, $b = 1{,}493$ – (*а*); $a = 0{,}01$, $b = 1{,}98$ – (*б*) і (*в*)

Детальний аналіз ітераційних діаграм (рис. 4.3 *б, в)* дозволяє зробити висновок, що система (4.1) за типом функції нелінійного перетворення еквівалентна двом тентовим відображенням які з'єднані слабким зворотнім зв'язком у формі доданків $ax(n)$ і $ay(n)$ [1]. Гістограми розподілу часових рядів системи (4.1) приведено на рис. 4.4.

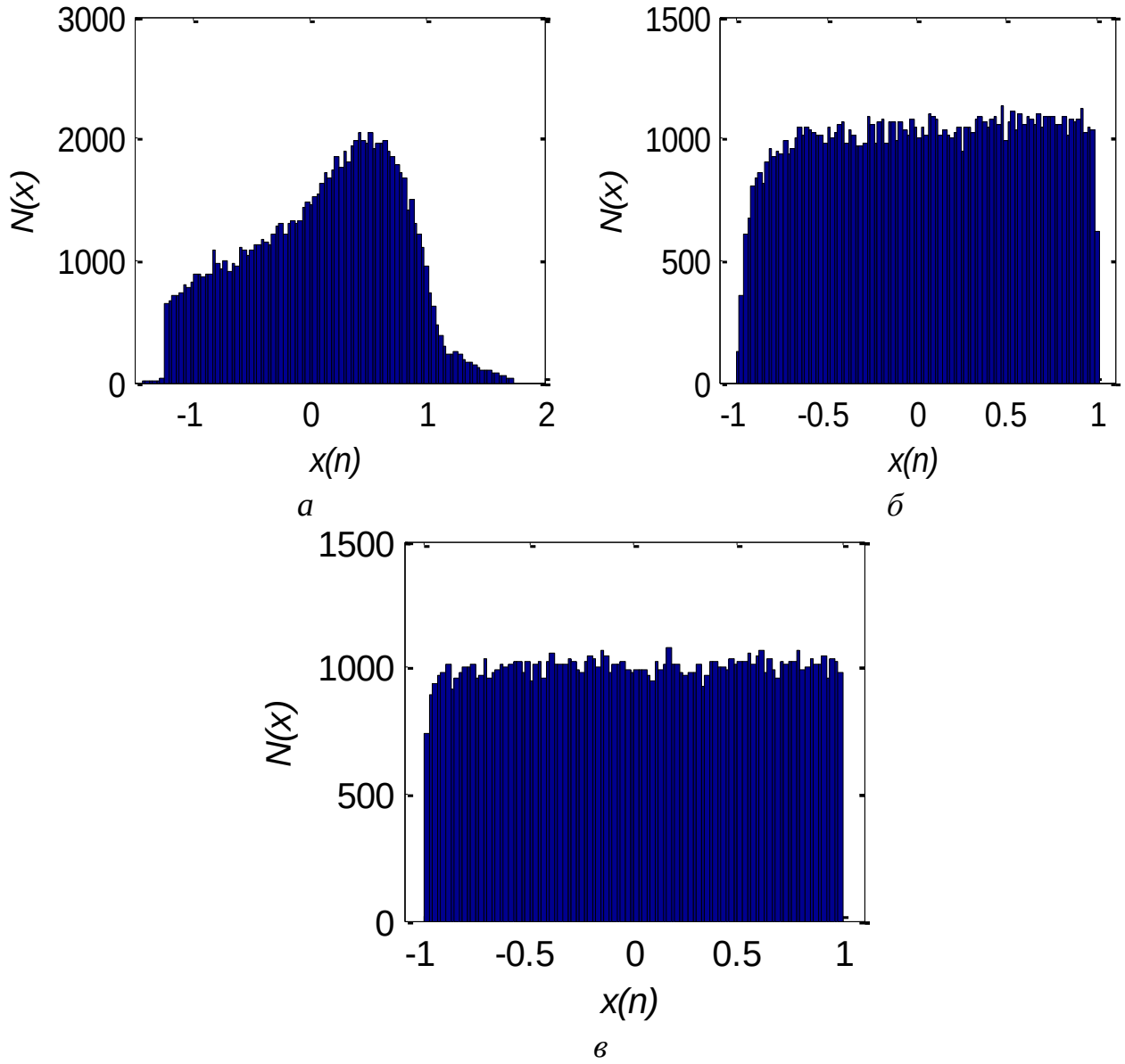


Рис. 4.4. Гістограма розподілу значень генерованих (3.1): при $a=-0,75$, $b=1,493$ - (*а*); при $a=0,01$, $b=1,98$ - (*б*); при $a=0,0001$, $b=1,998$ – (*в*);

Із рис. 4.4 випливає, що тільки при $a=-0,0001$ та $b=1,998$ гістограма розподілу є рівномірною (рис. 4.4 *в*).

4.1.3. Рекурентний аналіз часових рядів системи Тратаса

Рекурентний аналіз є одним з нелінійних методів дослідження експериментальних часових рядів [114-116], що дає змогу провести класифікацію процесів, виявити закономірності їх поведінки, оцінити складність і випадковість сигналів у телекомунікаційних системах. Суть аналізу полягає у побудові

спеціальних проекцій на двовимірну площину та чисельному оцінюванні отриманих геометричних структур.

Хаотичні системи еволюціонують в обмеженій області фазового простору тому характеризуються ергодичністю і частковим повторенням ділянок траєкторій, що можна виявити за допомогою рекурентного аналізу. Згідно теореми Танкеса на основі однієї часової реалізації $x=\{x_1,x_2,\ldots,x_N,\}$ можна побудувати траєкторію у псевдофазовому просторі розмірності m, що зберігає характеристики оригінальної системи, тобто:

$$\begin{aligned} x_1^m &= \{x_1,x_2,\ldots,x_{N-m},\} \\ x_2^m &= \{x_2,x_3,\ldots,x_{N-m+1},\} \\ &\ldots \\ x_m^m &= \{x_m,x_3,\ldots,x_N,\}. \end{aligned} \tag{4.2}$$

Проекція (4.2) на площину являє собою матрицю розміром $(n-m)\cdot(n-m)$ елементи якої характеризують відстань між траєкторією в моменти часу i і j. У найпростішому випадку матриця є бінарною і описується співвідношенням

$$R_{i,j}=\sigma\left(\varepsilon-\left|x_i-x_j\right|\right), i,j=1,2,\ldots N-m, \tag{4.3}$$

де ε – розмір околу навколо точки x_i в момент часу i, $\sigma(\bullet)$ – функція Хевісайда, $\|\cdot\|$ – Евклідова норма.

Для аналізу рекурентних діаграм використовують декілька оцінок [117-118], серед яких в роботі досліджено рекурентність, детермінізм і ентропію.

Рекурентність показує частку рекурентних точок, що потрапляють в інтервал радіусом ε

$$Rec=\frac{1}{N^2}\sum_{i,j}^{N-m}R_{i,j}. \tag{4.4}$$

Детермінізм показує частку точок, що утворюють діагональні структури, довжиною не менше l_{min} в загальній кількості рекурентних точок

$$Det=\frac{\sum_{l_{min}}^{l_{max}} l*P(l)}{\sum_{i,j}^{N-m}R_{i,j}}, \tag{4.5}$$

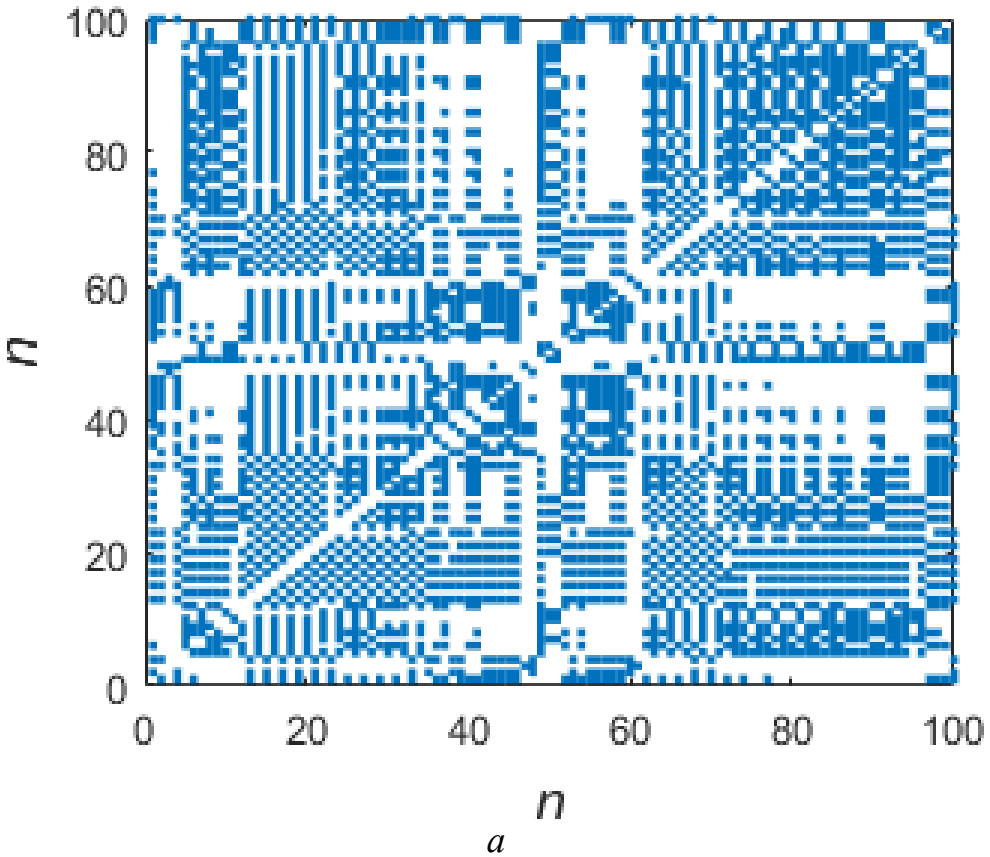
де $P(l)$ – ймовірність утворення діагоналі довжиною l.

Ентропія є оцінкою повторюваності частин траєкторії досліджуваного процесу.

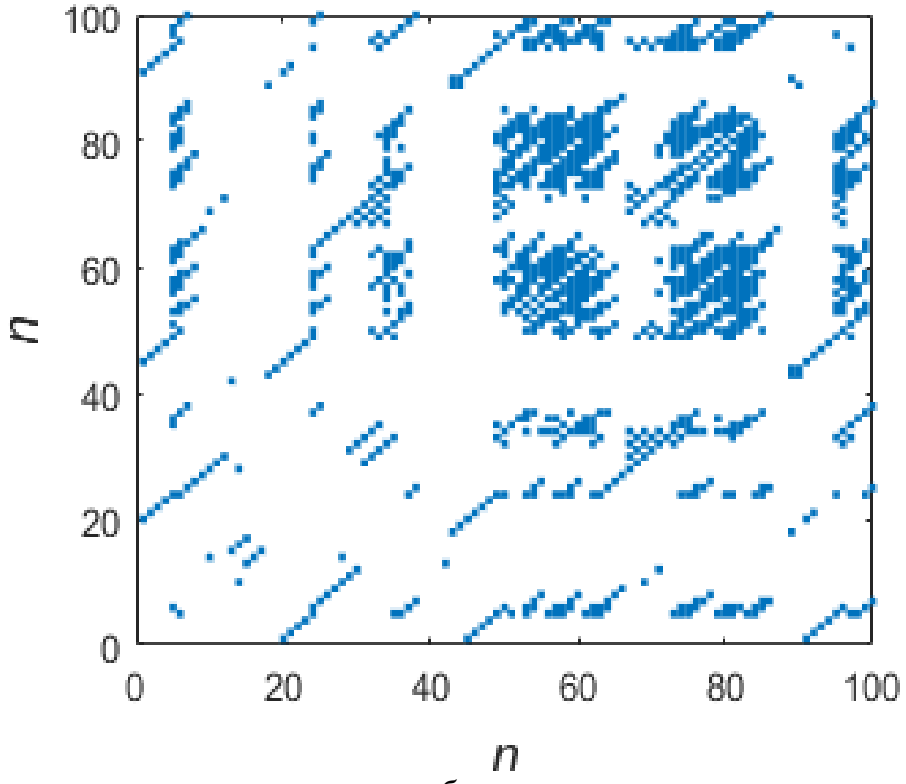
$$Entr = -\sum_{l_{min}}^{l_{max}} P(l) ln\left(P(l)\right). \tag{4.6}$$

В роботі поставлена задача оцінки можливостей рекурентного аналізу щодо визначення розмірності хаотичної системи, що актуально в контексті прихованості обміну даних в інформаційних та криптографічних застосуваннях, перевірки взаємозв'язку між розмірністю системи і псевдофазового простору та значеннями характеристик рекурентності. Для досліджень використаємо систему (4.1). Приклади рекурентних діаграм приведено на рис. 4.5.

Результати розрахунків характеристик рекурентних діаграм отримані для $N = 10000$ приведено на рис. 4.5. Рекурентність при постійній розмірності псевдо фазового простору не залежить від розмірності хаотичної системи.



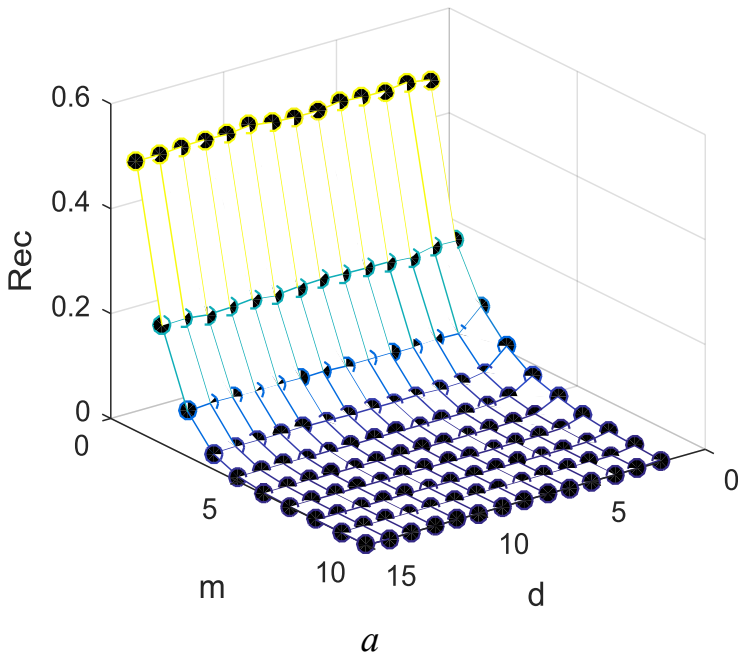
a



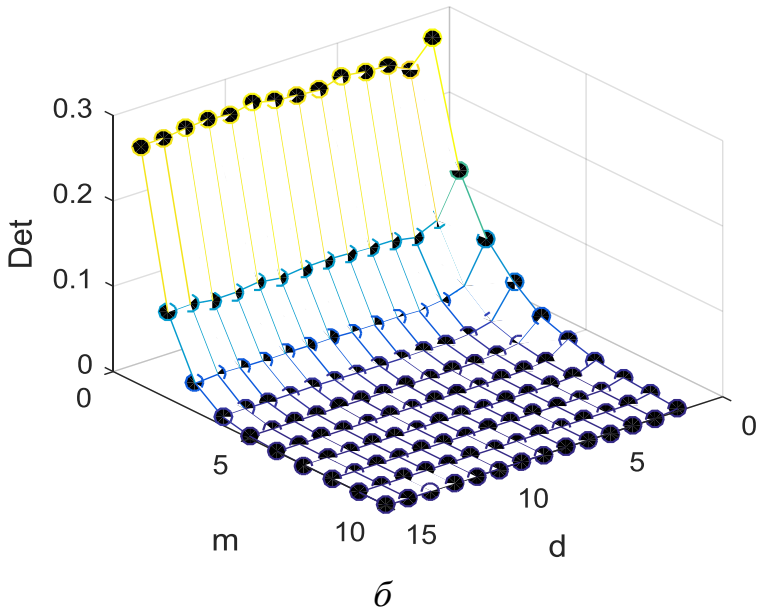
б

Рис. 4.5. Рекурентні діаграми системи (4.1) при $\varepsilon = 0{,}4$, $d = 2$ та розмірності псевдофазового простору $m = 1 - а$, $m = 5 - б$

При зростанні m рекурентність зменшується, що зумовлено зменшенням кількості точок які попадають в межі околу ε (рис. 4.6 *а*). Детермінізм зменшується при зростанні розмірності псевдофазового простору незалежно від розмірності системи (рис. 4.6 *б*).



а



б

Рис. 4.6. Залежності рекурентності, детермінізму та ентропії від розмірності системи та псевдо фазового простору при $\varepsilon = 0{,}4$, $l_{min} = 3$

На рис. 4.7 приведено залежність ентропії розподілу діагоналей від розмірності хаотичної системи та псевдофазового простору. Аналіз залежностей свідчить, що ентропія спочатку з ростом d зменшується, а потім її значення стабілізується. Така закономірність має місце при $m \le d-2$ і $m \in [1,5]$.

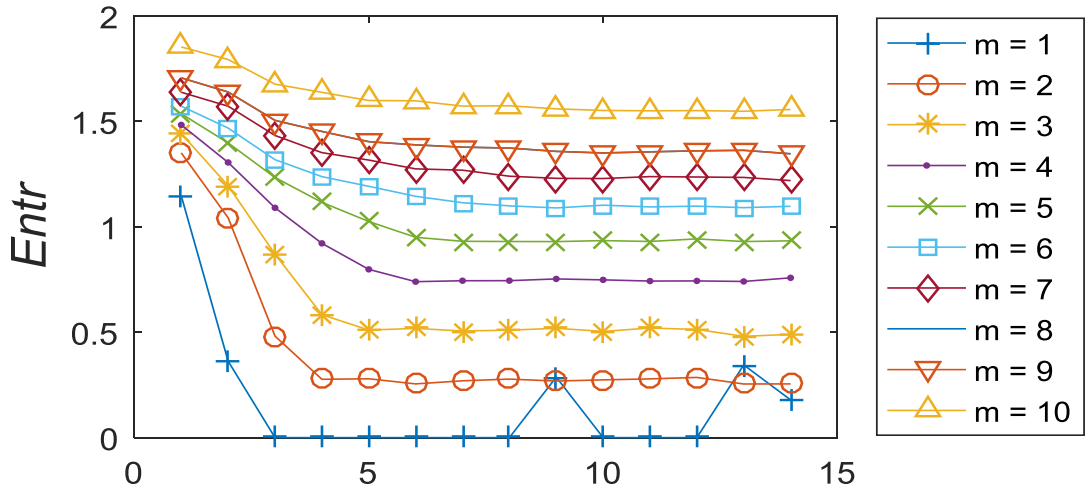


Рис. 4.7. Залежність ентропії від розмірності системи та псевдофазового $l_{min} = 3$ та $Rec = const$

При $m \ge 6$ перехід залежності $Entr(d,m)$ від спаду до постійного значення є плавним, а підтвердження вищенаведеної закономірності потребує подальших досліджень. З результатів проведеного дослідження слідує висновок, що

рекурентний аналіз дає змогу встановити нижню межу розмірності хаотичної системи.

4.1.4. Багатовимірне відображення Лоці із кільцевим зв'язком

Найпростіше багатовимірне відображення Лоці із кільцевим зв'язком, що дозволяє генерувати послідовності із рівномірним розподілом для неперервної множини значень параметрів керування описується [106]:

$$T_p:\begin{cases} x_{n+1}^{(1)} = 1 - a\left|x_n^{(1)}\right| + k^{(1)} \times x_n^{(2)} \\ x_{n+1}^{(2)} = 1 - a\left|x_n^{(2)}\right| + k^{(2)} \times x_n^{(3)} \\ \cdots \\ x_{n+1}^{(p)} = 1 - a\left|x_n^{(p)}\right| + k^{(p)} \times x_n^{(1)} \end{cases} \tag{4.7}$$

де параметр $k^{(i)} = (-1)^{i+1}$, $a \in (1, 2]$.

Для того щоб траєкторія системи рівноймовірно та щільно відвідува усі точки на p-вимірному торі $T^p = [-1,1]^p$ необхідно використовувати наступний механізм рандомізації [106]:

$$\begin{aligned} &\textit{якщо}\ \ x_{n+1}^{(j)} = 1 - 2\left|x_n^{(j)}\right| + k^{(j)} \times x_n^{(j+1)} < -1 \quad \textit{додати}\ \ 2 \\ &\textit{якщо}\ \ x_{n+1}^{(j)} = 1 - 2\left|x_n^{(j)}\right| + k^{(j)} \times x_n^{(j+1)} > 1 \quad\ \ \textit{відняти}\ \ 2 \end{aligned} \tag{4.8}$$

де $\left|x_n^{(j)}\right|$ позначає абсолютне значення $x_n^{(j)}$, та $j \in [1,\ p]$. Цей механізм дозволяє, отримати рівномірний розподіл генерованих часових рядів.

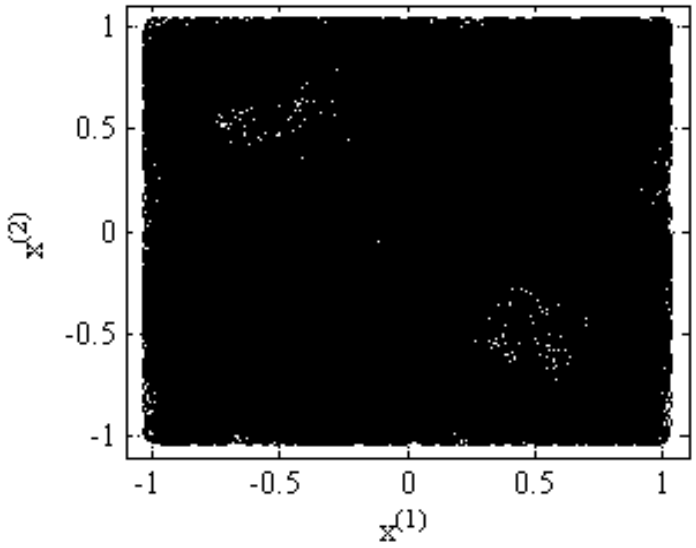
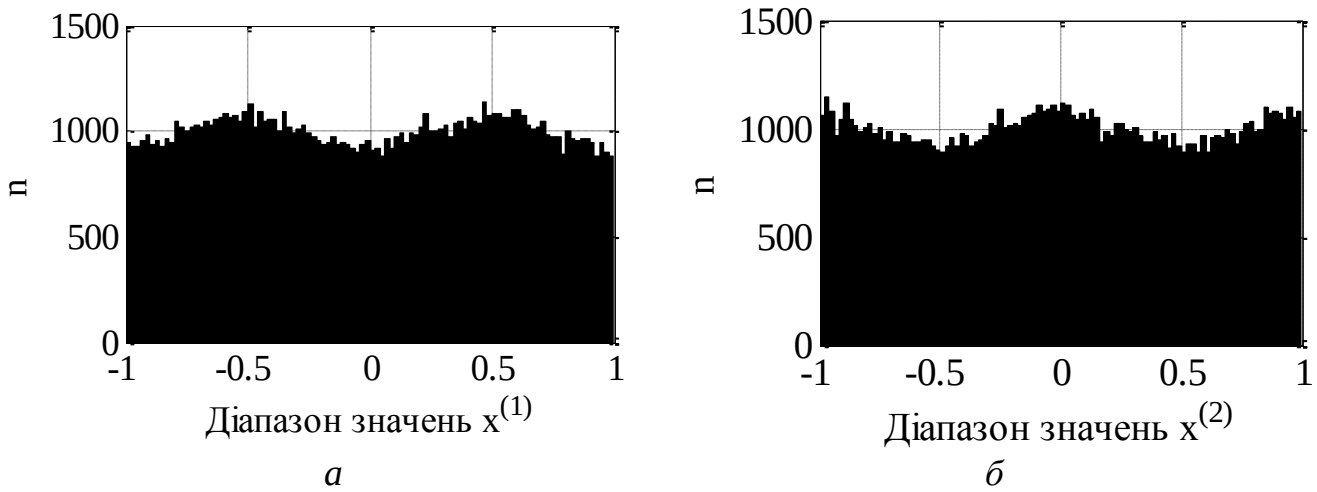


Рис. 4.8. Фазовий портрет системи (4.7) при p=2

Гістограма розподілу значень $x_n^{(1)}$ і $x_n^{(2)}$ для 20000 ітерацій при $a=2$, $k^{(1)}=-1$ та $k^{(2)}=1$ приведено на рис. 4.9.

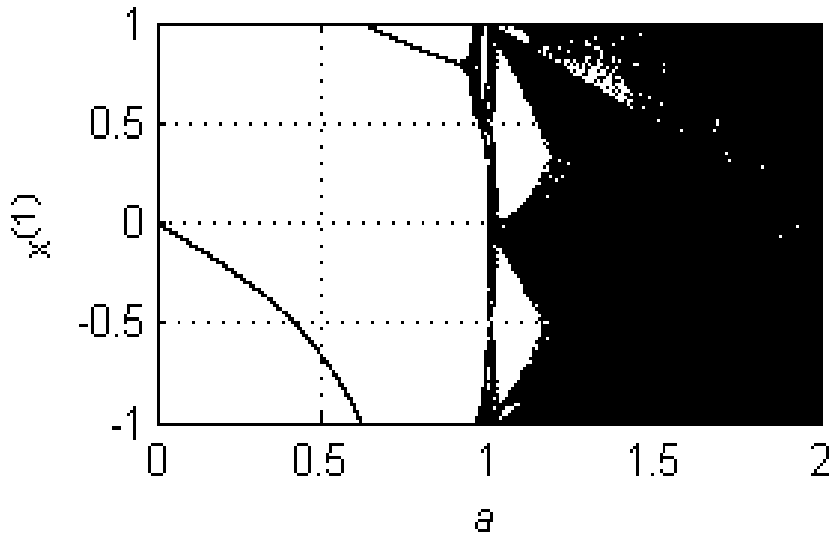


а *б*

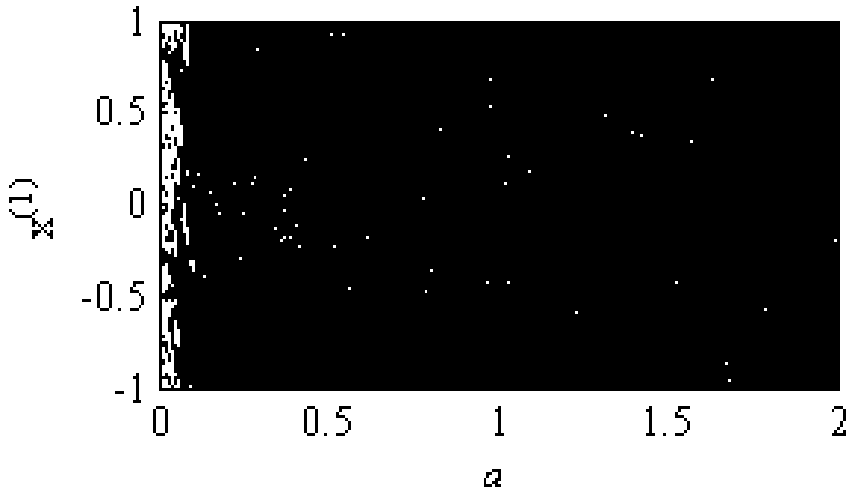
Рис. 4.9. Гістограма розподілу значень: *а* – змінна $x_n^{(1)}$, *б* – змінна $x_n^{(2)}$.

З рис. 4.8 і 4.9 випливає що траєкторії $x^{(1)}$ і $x^{(2)}$ мають близький до рівномірного розподіл значень. Для системи (4.7) рівномірний розподіл спостерігається при $p \geq 4$. Біфуркаційна діаграма відображення Лоці (4.7) для двовимірного та чотирьохвимірного випадку приведена на рис. 4.10.

З рис. 4.10. випливає, що при збільшені розмірності *p* системи (1) її псевдовипадкові характеристики покращуються і розподіл значень генерованих змінних $x^{(i)}$ є рівномірним а потужність простору значень параметру керування при якому є хаос зросла.



а



б

Рис. 4.10. Біфуркаційна діаграма для $x^{(1)}$: *а* – при *p*=2; *б* – при *p*=4.

З рис. 4.10. випливає, що при збільшені розмірності *p* системи (4.7) зростає потужність простору значень параметру керування при яких спостерігаються хаотичні коливання.

4.2. Схемотехнічна реалізація генераторів сигналів на базі двовимірних систем Тратаса та Лоці

4.2.1. Дослідження генератора хаотичних сигналів на базі системи Тратаса

Для схемотехнічної реалізації системи (3.1) у вигляді електронного кола необхідно перемасштабувати змінні наступною заміною:

$$\begin{aligned} u(n) &= Ex(n) \\ v(n) &= Ey(n) \end{aligned} \tag{4.9}$$

де $E > 0$.

Для роботи і додатніми значеннями параметра a необхідно ввести новий параметр A так щоб:

$$a = A - 1,\ A > 0. \tag{4.10}$$

Враховуючи (4.9) і (4.10) запишемо (3.1) в наступній формі:.

$$\begin{cases} u(n+1) = (A-1)u(n) - B|v(n)| + E \\ v(n+1) = (A-1)v(n) - B|u(n)| + E \end{cases}, \tag{4.11}$$

де *A,B* – нові параметри керування системою.

Як випливає із (4.11) за допомогою E можна керувати амплітудою генерованих сигналів. Електронне коло, що реалізовує (4.11) приведено на рис. 4.11.

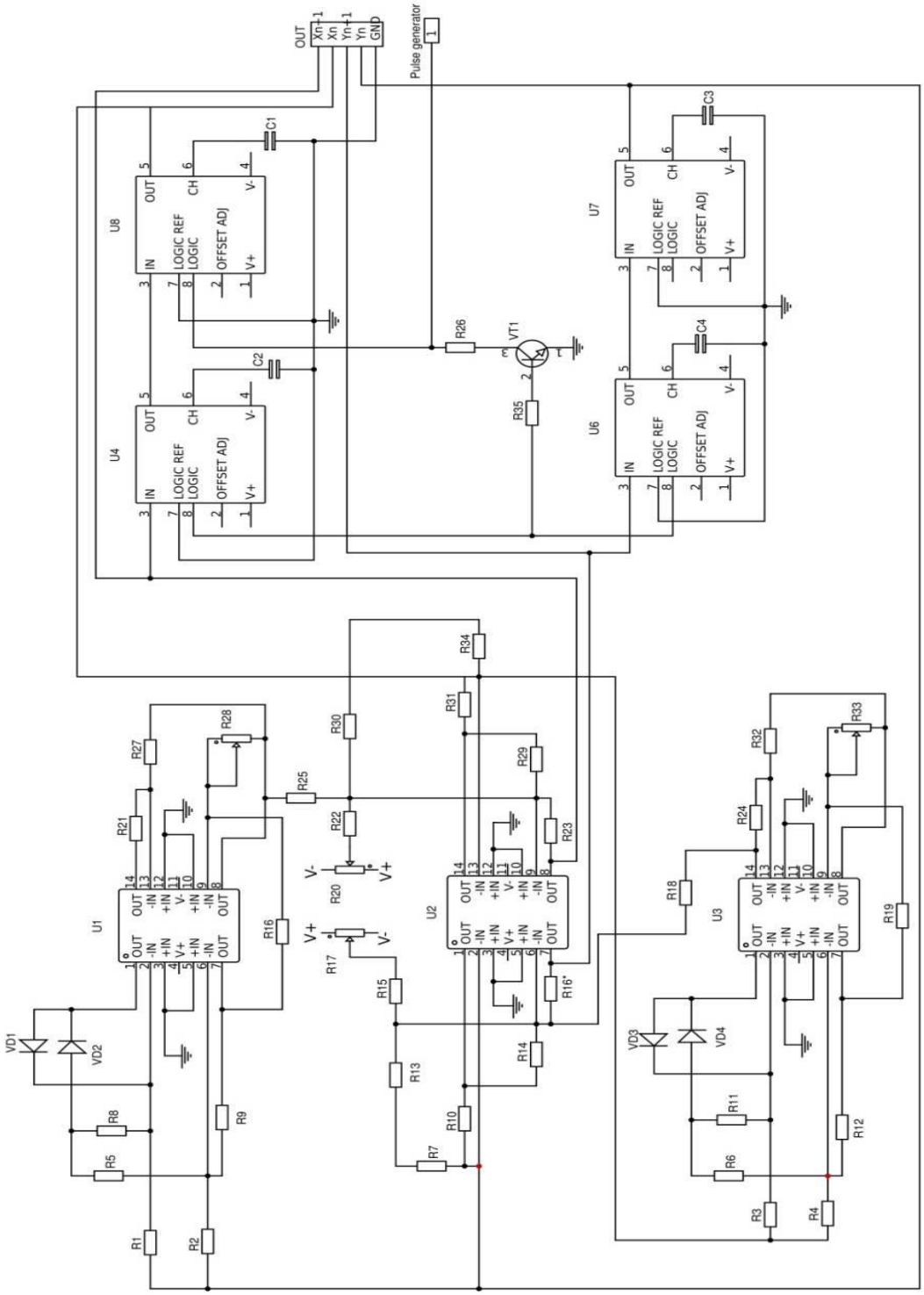


Рис. 4.11. Схемотехнічна реалізація системи (4.11)

Для визначення значення сигналу за модулем використано двонапівперіодний випрямляч на базі операційних підсилювачів та діодів VD1 і VD3. Затримку сигналу на один такт реалізовано на пристроях вибірки і затримки

LF398 - U4-7. На мікросхему U6 подається інвертований тактовий сигнал. При цьому на протязі першого напівперіоду заряджаються конденсатори C2 і C4, а значення попередньої ітерації зберігається на C1 і C3. На протязі другого напівперіоду заряджаються конденсатори C1 і C3, а C2 і C4 зберігають значення поточної ітерації.

Для експериментального дослідження електронного кола приведеного на рис. 4.11 розроблено макет (див. рис. 4.12).

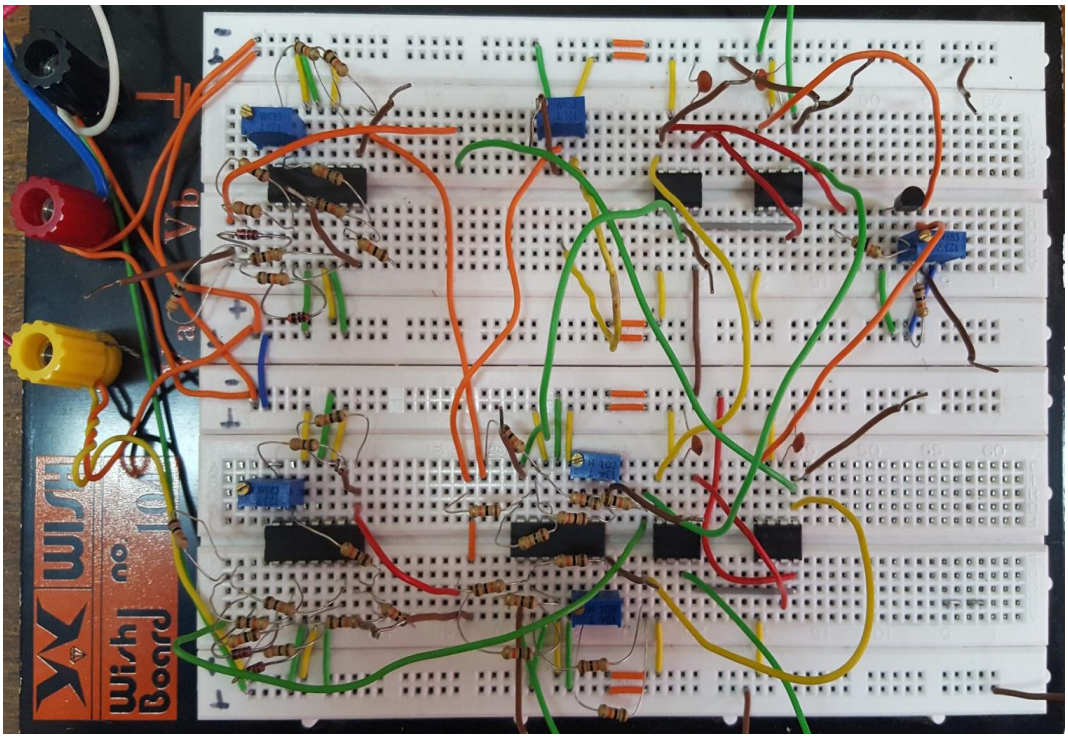


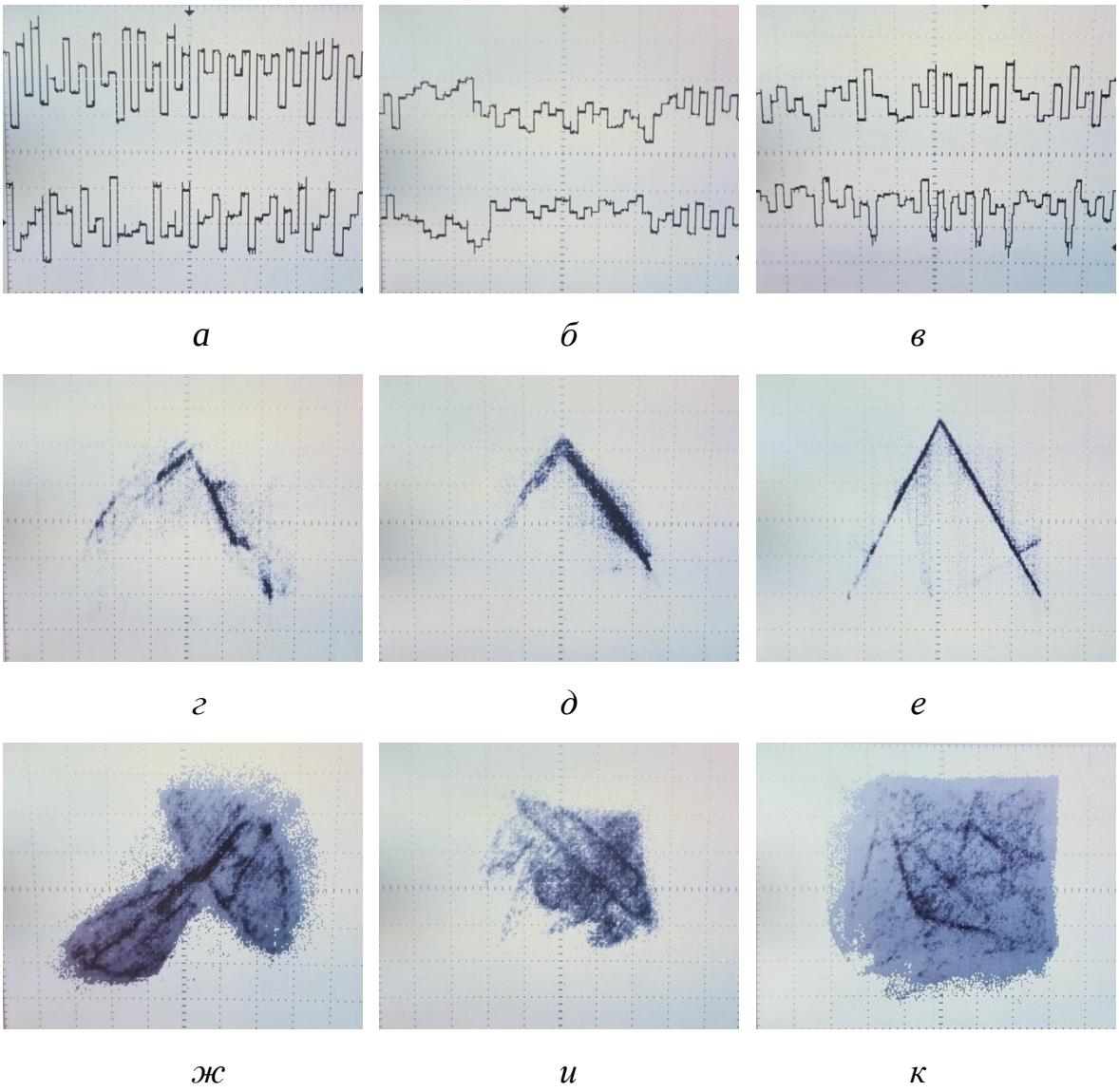
Рис. 4.12. Експериментальний макет

Значення номіналів елементів електронного кола приведено в табл. 4.1.

Таблиця 4.1.
Список компонентів та значення їх номіналів:

Елемент	**Специфікація**
Резистори R1-R12, R15-R28, R30-R33	10 кОм;
Резистори R13, R14	Змінні резистори 0-20 кОМ
Резистори R29 R34	Змінні резистори 0-20 кОМ
Резистори R35,R36	2.4 кОм
Діоди VD1-VD4	1N4001
Транзистор VT1	2N2222A
Конденсатори C1,C2	1 мкФ
C3,C4	10 нФ
U1-U3	TL084
U4-U7	LF398

Експерементально отримані осцилограми приведені на рис. 4.13. Значення параметрів керування *A* і *B* для коливань $u(n)$ і $v(n)$ є однаковими (рис. 4.13 *а, б, в*), функція нелінійного перетворення є кусочно лінійною, що підтверджується результатами експерименту (рис. 4.13 *г, д, е*). Фазові портрети, що відповідають гіперхаотичним режимам приведено на рис. 4.13 *ж, и, к.*



а *б* *в*

г *д* *е*

ж *и* *к*

Рис. 4.13. Гіперхаотичні коливання: сигнали *v(n)* і *u(n)* – (*а, б, в*); функція нелінійного перетворення *u*(*n*+1)=*f*(*u*(*n*)) – (*г, д, е*); фазовий портрет при R17=R22=2.5 кОм, R29=R32=14.93 кОм – (*ж*); R17=R22=12.3 кОм, R29=R32=14.93 кОм – (*и*); R17=R22=0.01 кОм, R29=R32=19.99 кОм – (*к*).

Оскільки напруга живлення рівна ±12 В тоді U_{reg} для генерованих коливань становить: рис. 4.13 *а, г, ж* – $U_{reg} = -2$ В; рис. 4.13 *б, д, и* $-U_{reg} = -4$В; рис. 4.13

в, *е*, *к* – $U_{reg} = -5{,}5\,\text{В}$. Частота тактового сигналу рівна 10 кГц. Результати експериментального дослідження узгоджуються із результатами моделювання. Однак, порівннюючи рис. 4.2 і 4.3 з рис. 4.13 можемо зробити висновок про наявність впливу розкиду параметрів елементів схеми відносно номінальних значень.

4.2.2. Схемотехнічна реалізація двовимірного відображення Лоці

Для реалізації генератора сигналів на базі системи (4.7) необхідно перемасштабувати змінні наступним чином:

$$\begin{aligned} u_n^{(i)} &= V x_n^{(i)} \\ u_n^{(i+1)} &= V x_n^{(i+1)} \end{aligned} \tag{4.12}$$

де $V > 0$.

Використовуючи (4.12) для двохвимірного випадку $p = 2$ ми можемо переписати (4.7) в наступному вигляді:

$$\begin{cases} u_{n+1}^{(i)} = V - a\left|u_n^{(i)}\right| + k^i \times u_n^{(i+1)} \\ u_{n+1}^{(i+1)} = V - a\left|u_n^{(i+1)}\right| + k^{i+1} \times u_n^{(i)} \end{cases} \tag{4.13}$$

тоді (4.13) набуде вигляду:

$$\begin{aligned} &\text{якщо } u_{n+1}^{(i)} < -V \qquad \text{тоді: } u_{n+1}^{(i)} = u_{n+1}^{(i)} + 2V \\ &\text{якщо } u_{n+1}^{(i)} > V \qquad \text{тоді: } u_{n+1}^{(i)} = u_{n+1}^{(i)} - 2V \end{aligned} \tag{4.14}$$

Змінюючи значення *U* можна керувати розмахом значень змінних $u^{(1)}$ та $u^{(2)}$, що прийматимуть значення з діапазону $u^{(1)}, u^{(2)} \in [-V, +V]$. Розроблена схема електрична принципова генератора випадкових сигналів на базі системи (4.15) приведена на рис. 4.14. В загальносу схема складається із двох ідентичних частин з'єднаних кільцевим зв'язком.

Для знаходження модуля значення сигналу $\left|u_n^{(1)}\right|$ та $\left|u_n^{(2)}\right|$ використано двонапівперіодний випрямляч на операційних підсилювачах.

Контроль зміни значень параметру керування *a* реалізовано на змінних резисторах RV1 та RV2 так, що:

$$a \approx \frac{R_{15}}{RV1} \approx \frac{R_{16}}{RV1}.$$

Для реалізації операторів умови (5) використано компаратори які керують нормально замкненими ключами.

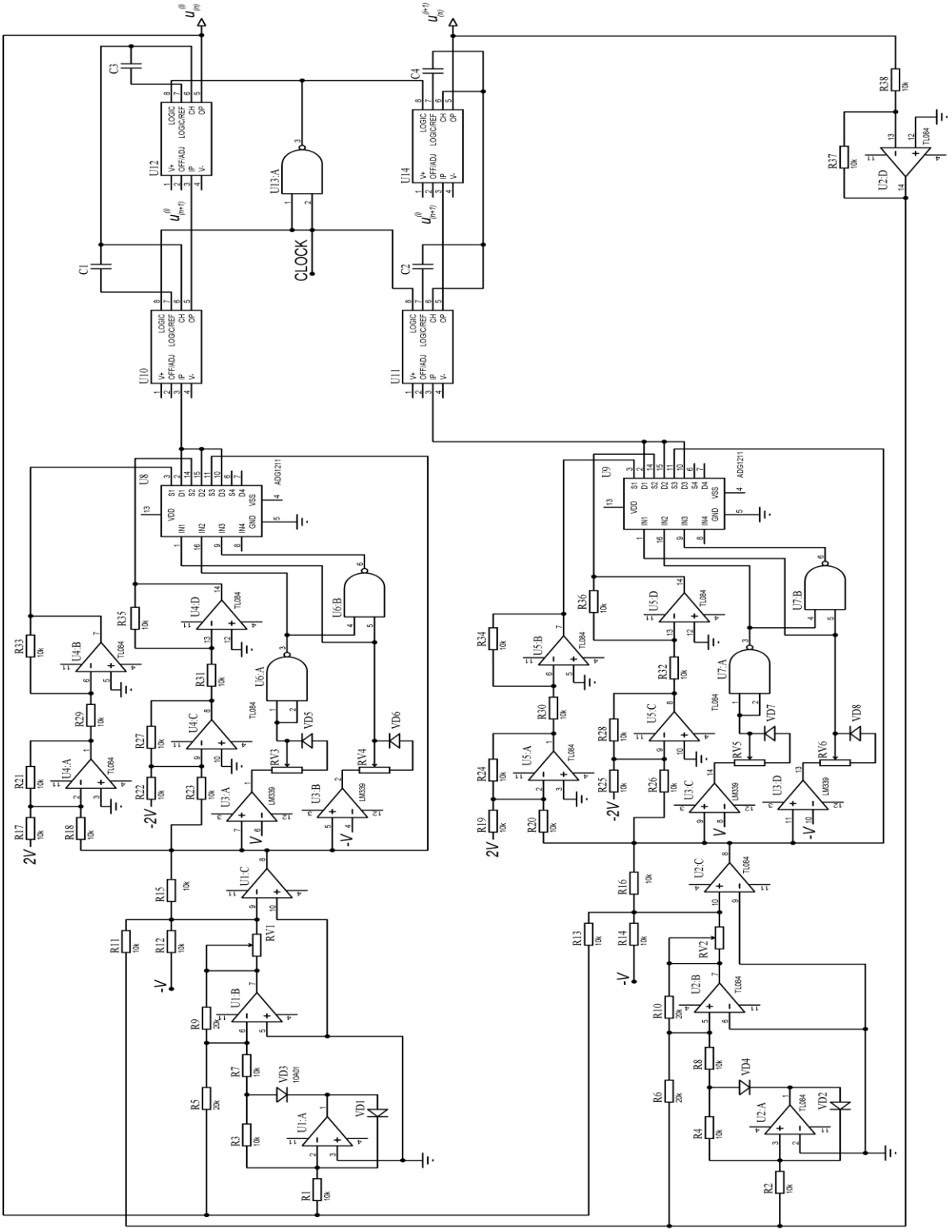


Рис. 4.14. Схема електрична принципова системи (4.14), враховуючи (4.14)

Затримку сигналів реалізовано на пристроях вибірки затримки LF398. На мікросхему U10 і U11 подається тактовий сигнал, на U12 і U14 подається

інвертований тактовий сигнал. Завдяки цьому тактовий сигнал заряджає конденсатори C1 і C2, конденсатори C3 і C4 зберігають значення попередньої ітерації. В другий на півперіод тактовий сигнал заряджає конденсатори C3 і C4, конденсатори C1 і C2 зберігають значення сигналу.

Для експериментального вивчення роботи системи приведеної на рис. 4.14 реалізовано дослідницький макет, який приведено на рис. 4.15.

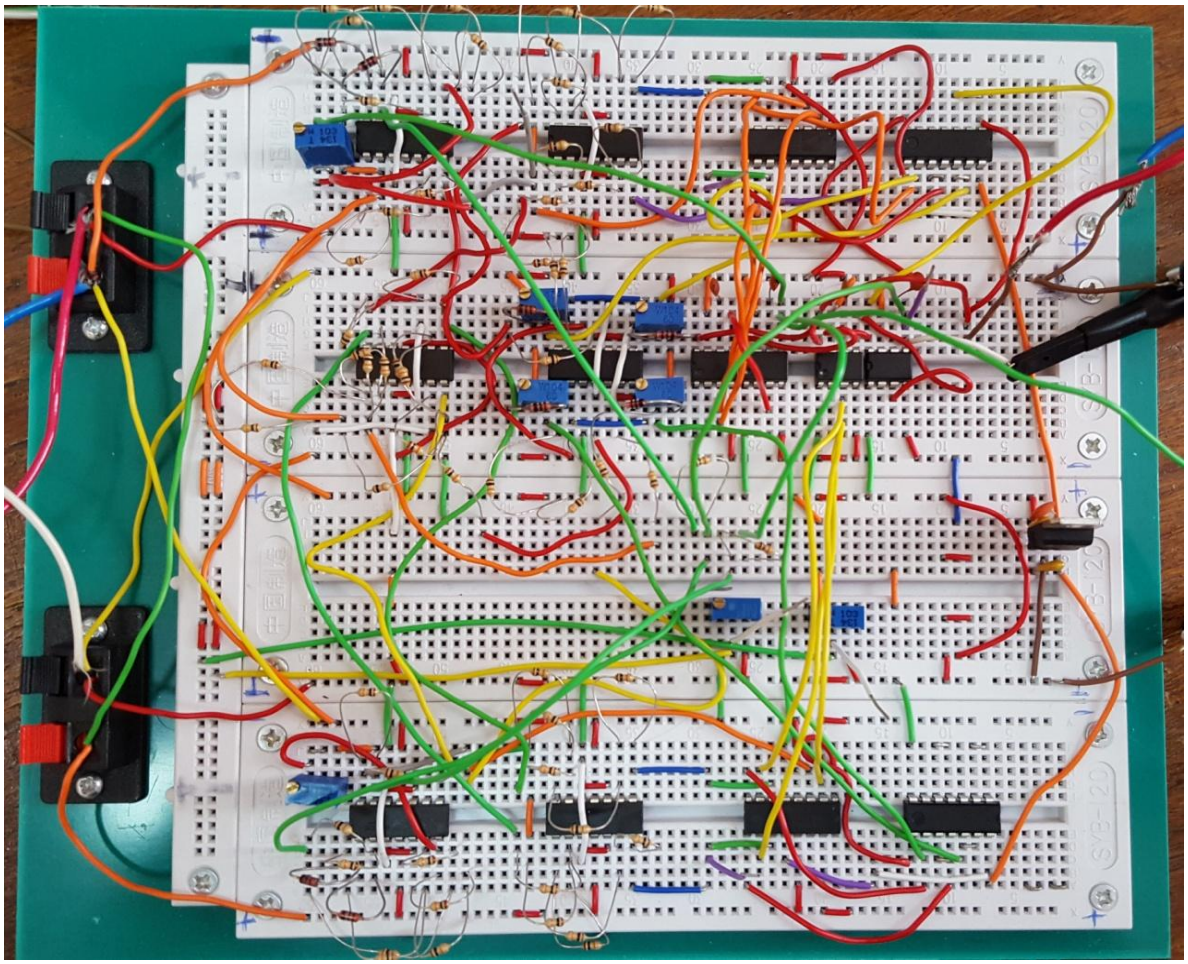


Рис. 4.15. Експериментальний макет генератора хаотичних сигналів на базі відображення Лоці.

Для досліджень розробленого макету значення частоту тактового сигналу встановлено на рівні 10 КГц. Значення параметра керування a встановлено за допомогою змінних резисторів:

$$a \approx \frac{R_{15}}{RV1} \approx \frac{R_{16}}{RV2} \approx 4.04.$$

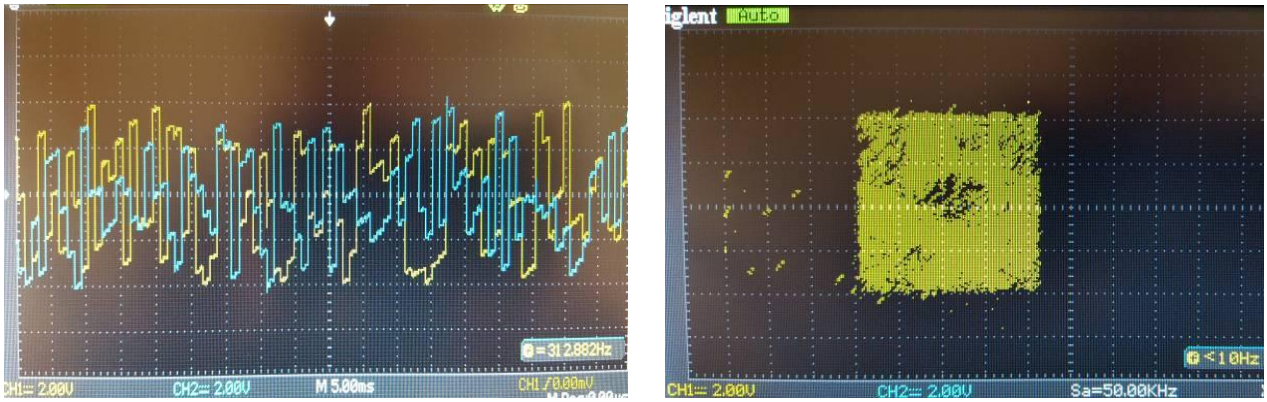
Значення номіналів елементів електронного кола (Рис. 4.14) приведено в табл. 4.2.

Таблиця 4.2.

Список компонентів та значення їх номіналів:

Елемент	Специфікація
Резистори R1-R12, R15-R28, R30-R33	10 кОм;
Резистори R13, R14	Змінні резистори 0-20 кОМ
Резистори R29 R34	Змінні резистори 0-20 кОМ
Резистори R35,R36	2.4 кОм
Діоди VD1-VD4	1N4001
Транзистор VT1	2N2222A
Конденсатори C1,C2	1 мкФ
C3,C4	10 нФ
U1-U3	TL084
U4-U7	LF398

Значення порогових напруг встановлено $V = 4$ В. Експериментально отримані осцилограми сигналів та фазовий портрет, що відповідає хаотичному режиму приведені на рис. 4.16. Спектр послідовності імпульсів $u^{(1)}$ приведений на рис. 4.17.



а *б*

Рис. 4.16. Експериментально отримані:

а- хаотичні коливання при $a \approx 4.04$, *б* -фазовий портрет

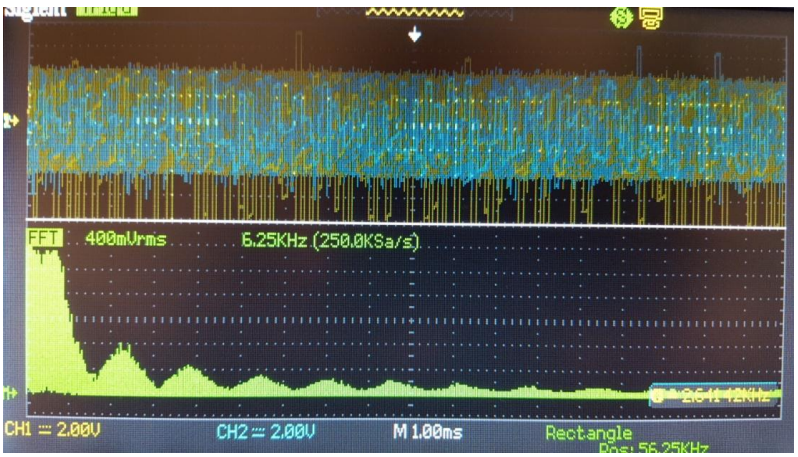


Рис. 4.17. Спектр сигналу $u^{(1)}$

Експериментально отримані дані корелюють із результатами моделювання. Однак, як випливає з рис. 4.17 має місце вплив дрейфу параметрів компонентів електронного кола відносно їх номінального значення. Тому ми спостерігаємо на фазовому портреті (рис. 4.16 *б*) значення сигналів більші $u^{(i)} > V$ та $u^{(i)} < -V$.

Для тестування послідовностей на відповідність критеріям випадковості було використано набір статистичних тестів NIST SP 800-22. Послідовність було оцифровано за допомогою 14-бітового аналого-цифрового перетворювача (АЦП). Для тестування згенеровано послідовність довжиною 10^8 бітів яку сформовано з 6-ти послідовностей згенерованих для випадкових початкових умов з діапазону [-V, V].

Висновки до четвертого розділу

1. Досліджено двовимірну дискретну хаотичну систему Тратаса. Встановлено, що генератор хаотичних сигналів на базі системи Тратаса генерує хаотичні та гіперхаотичні коливання в широкому неперервному діапазоні значень параметрів керування. Показано, що генератор на базі гіперхаотичної системи може генерувати послідовність з рівномірним розподілом значень

2. Розроблено та практично реалізова макет генератора сигналів на базі двовимірної системи Тратаса. Схема електрична принципова генератора складається з двох симетричних частин, з'єднаних кільцевим зв'язком. Керування параметрами контролю для зміни динамічного режиму реалізовано на змінних резисторах.

3. Розроблено та практично реалізовано макет генератора випадкових сигналів на базі двовимірного випадку системи Лоці із кільцевим зв'язком. Показано, що генератор забезпечує генерування послідовностей з розподілом близьким до рівномірного в широкому діапазоні неперервної змінни значень параметрів керування.

4. Розроблені генератори випадкових послідовностей складаються з двонапівперіодних випрямлячів, інвертуючих суматорів, пристроїв вибірки затримки та операційних підсилювачів. Експериментальні дослідження генераторів сигналів корелюють з результатами моделювання.

5. Встановлено, що на основі залежності ентропії розподілу діагоналей рекурентної діаграми модифікованої системи Тратаса можливо оцінити нижню межу розмірності фазового простору системи. Це дозволяє здійснювати підбір системи з розмірністю, при якій розкриття параметрів є ускладненим.

РОЗДІЛ 5.
РОЗРОБКА МЕТОДУ ЗАХИСТУ РАСТРОВИХ ЗОБРАЖЕНЬ НА ОСНОВІ МОДИФІКОВАНОГО ВІДОБРАЖЕННЯ ЧИРІКОВА-ТЕЙЛОРА

5.1. Аналіз перестановок на базі стандартного відображення Чирікова-Тейлора

Серед методів захисту інформації на базі детермінованого хаосу значну частину складають методи захисту зображень від несанкціонованого доступу. Як відомо одним з найбільш ефективних методів захисту інформації є її криптографічне за шифрування. Надійний метод зашифрування зображень повинен складатися з перестановки пікселів та дифузії кольору пікселів [119].

На етапі перестановки здійснюється перетворення блоку інформації за допомогою дискретного двомірного хаотичного відображення. Метою перестановки є розрив взаємозалежності між сусідніми пікселями зображення. При цьому розподіл градацій кольорів зображення не змінюється. При перестановці пікселів розмір блоку буде дорівнювати N^2.

Дифузія представляє собою зміну значень складових кольору пікселів за допомогою нелінійної детермінованої системи. Для дифузії розмір блоку визначатиметься типом використовуваної арифметики, розмірами зображення, кількістю двійкових розрядів для запису однієї з складових кольору пікселів. Наприклад, розмір блоку при дифузії для зображень формату RGB становитиме $\frac{24}{3}N^2 = 8N^2$ біт. Ключем дифузійного процесу є початкові умови і параметри функції дифузії. Дифузія чутлива до повідомлення при наявності зворотних зв'язків за шифротекстом у алгоритмі шифрування. Хаотичний потоковий шифр може містити тільки операції дифузії [117], які найчастіше полягають у додаванні за модулем два псевдовипадкової та інформаційної послідовності бітів.

В процесі перестановок чутливість до початкового значення відповідає чутливості до початкового положення пікселя. При зростанні чутливості

покращується випадковість перестановки. Якість перестановки залежить від кількості циклів. Простором ключів буде область допустимих значень параметрів хаотичного відображення. Чутливість до ключа визначається чутливістю до параметрів хаотичного відображення та кількістю циклів. Недоліком перестановок є відсутність чутливості до повідомлення. Алгоритми шифрування, в яких використовуються тільки перестановки, легко зламуються атакою відкритим текстом [8, 120], проте можуть бути використані як один з етапів у алгоритмах захисту даних.

5.1.1. Хаотичні відображення для перестановок

Для процесу перестановок зазвичай використовуються двовимірні хаотичні відображення, зокрема, відображення Бейкера, відображення Кота, стандартне відображення (Чирікова-Тейлора), які дискретизують по розміру зображення, що забезпечує коректне перемішування [121]. Для зображення розмірністю $N \times N$ пікселів дискретизовані відображення Чирікова-Тейлора, Кота і Бейкера описуються наступними системами рівнянь [120]:

$$\begin{aligned} x_{j+1} &= (x_j + y_j) \bmod N, \\ y_{j+1} &= \left(y_j + K\sin\frac{x_{j+1}N}{2\pi}\right) \bmod N, \end{aligned} \tag{5.1}$$

де K – параметр (натуральне число) стандартного відображення; x_{j+1} та y_{j+1} координати $j \in [0; N-1]$ пікселів по ширині або висоті растрового зображення розмірністю $N \times N$.

$$\begin{aligned} x_{j+1} &= (x_j + uy_j) \bmod N, \\ y_{j+1} &= (vx_j + (1+uv)y_j) \bmod N, \end{aligned} \tag{5.2}$$

де u, v –параметри відображення Кота;

$$\begin{aligned} x_{j+1} &= \frac{N}{k_i}(x_j - N_i) + y_j \bmod \frac{N}{k_i}, \\ y_{j+1} &= \frac{k_i}{N}\left(y_j + y_j \bmod \frac{N}{k_i}\right) + N_i, \end{aligned} \tag{5.3}$$

де $k_1, k_2, \ldots, k_t$ – параметри відображення Бейкера, які задовольняють умови:

$$\begin{cases} k_1 + k_2 + \cdots k_t = N, \\ N = k_1 + \cdots + k_{i-1}, \\ N_i \le x_j < N_i + k_i, \\ 0 \le y_j < N. \end{cases}$$

Детально властивості, переваги та недоліки відображеннь (5.2) та (5.3) проаналізовані в [120]. Однак в літературі не було проаналізовано особливості перестановок на базі відображення (5.1).

5.1.2. Особливості перестановок.

Властивості дискретизованого відображення (5.1) є не такими досконалими, як оригінального [120], але воно може бути застосовано на цілих значеннях інтервалів, що зменшує обчислювальну складність і уможливлює його використання для зашифрування інформації. Порядок дій при перестановці пікселів в растрових зображеннях розмірністю $N \times N$ для одного циклу є наступним:

1) Задаємо значення параметра K.
2) Для кожного пікселя x_j та y_j обчислюємо за допомогою (5.1) його нові координати x_{j+1} та y_{j+1} в зашифрованому зображені.
3) Переміщаємо пік сель згідно нових координат.
4) Операції 2) та 3) проводимо послідовно для кожного пікселя.

Розглянемо особливості перестановок на базі відображення (5.1).

Будь-яке растрове зображення з розмірністю $N \times N$ має $2N - 1$ діагоналей (рис. 5.1).

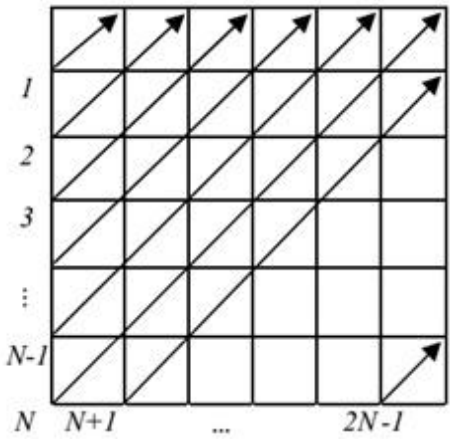


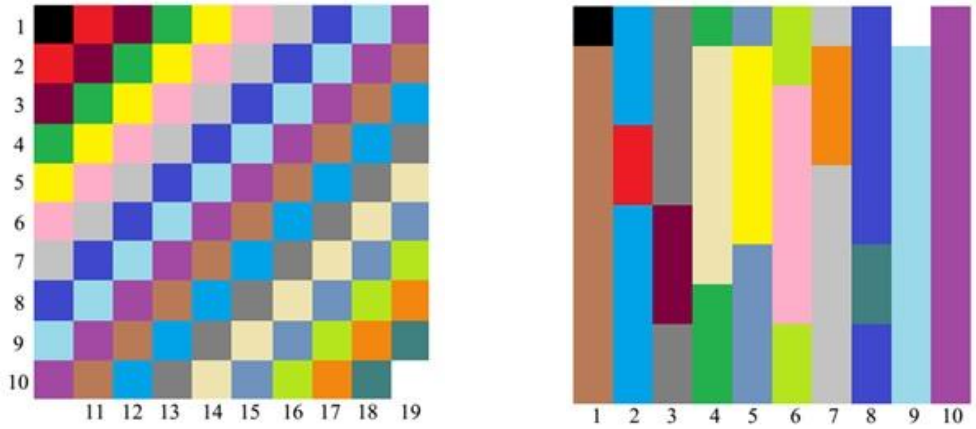
Рис. 5.1. Діагоналі в будь-якому зображені розмірності $N \times N$.

Як випливає з рис. 5.1 перша та остання діагоналі складаються з одного елемента (пікселя). Кількість елементів в діагоналі варіюється від 1 до N.

Перший елемент діагоналі є пікселем із найменшим значенням x_j. Перестановки на базі відображення (5.1) характеризуються наступними властивостями:

1. Піксель з координатами (0; 0) не змінює свого положення після будь-якої кількості циклів перестановки [120]. При побудові методів захисту інформації слід вводити механізми нівелювання даної вразливості, оскільки це може призвести до розкриття інформації.

2. Кожен стовпець після одного циклу перестановок складається із елементів двох діагоналей n та $N+n$, де $n \in [2; N-1]$. Останній стовпець складатиметься із елементів діагоналі N. Дані властивості приведені на рис. 5.2.



а *б*

Рис. 5.2. Результати одного циклу перестановки пікселів: *а* – оригінальне зображення (10×10), *б* – зображення після одного циклу перестановки.

На рис. 5.2 *а*. приведено тестове зображення розміром (10×10) пікселів. Як випливає з рис. 5.2 *б*, кожен стовпець складається з елементів двох діагоналей окрім останнього стовпця для яких в оригінальному зображенні справедливо:

$$(x_j + y_j) \bmod N = C = const, \tag{5.4}$$

де $V \in (0 \ldots N-1)$. Тоді рівняння для визначення y_{j+1} може бути записано, як:

$$y_{j+1} = (y_j + KC_1) \bmod N \tag{5.5}$$

де $C_1 = \sin(\frac{x_{j+1}N}{2\pi}) = \sin\frac{CN}{2\pi} = const$ і означає, що після перестановки пікселі координати яких відповідають (5.4) розміщені послідовно в одному стовпці, проте будуть зсунутими відносно початкової позиції, що залежить від параметрів K та C_1.

Пікселі для координат яких справедливо:

$$x_{j+1} = (x_j + y_j) \bmod N = 0 \tag{5.6}$$

завжди після циклу перестановки заходитимуться в першому стовпці. Вврахувуючи цю властивість та беручи до уваги (5.6) $x_{j+1} = 0$, $y_{j+1} = y_j$, згідно номеру стовпця може бути ідентифіковано діагоналі, з яких він сформований. Використовуючи властивості діагоналей (5.4-5.6), криптоаналітик може спробувати відновити зображення, переміщуючи пікселі в стовпцях на їх місце в діагоналях.

5.1.3. Потужність простору ключів.

Номер рядка в який може бути переміщений піксель після перестановки при $(x_j + y_j) \neq N$ та $(x_j + y_j) \neq 0$ залежить від значення параметру K та множника KC_1 в (5.5). Для елементів, що знаходяться в першому стовпці точно відомо їх позицію в оригінальному зображені. Два сусідніх стовпці містять пік селі двох сусідніх діагоналей. Тому можливо тільки N варіантів зсуву між елементами другого стовпця відносно першого. Знаючи, що пікселі двох сусідніх діагоналей слабо відрізняються між собою за значенням кольору, ми можемо знайти зсув між ними за допомогою максимального значення кореляційної функції. Враховуючи (5.4) та (5.5), кількість комбінацій для атаки грубою силою, необхідних для відновлення оригінального зображення після одного циклу перестановки становить N^{N-1}, що є значно менше $N^2!$ прийнятої в [119, 121].

Беручи до уваги інші властивості відображення (5.1), які можуть бути використані для зламу перестановок встановимо, що:

$$K_i = \mathrm{K}\sin(\frac{x_{j+1}N}{2\pi}).$$

Тоді при $x_{j+1} = const$ число K_i є ключем перестановок в діагоналі і в

стовпцях. В загальному буде N субключів, в той час деякі з них можуть бути однаковими.

З рис. 5.3 випливає, що кожен субключ K_i, при заданому K зустрічається обмежену кількість разів $m \leq N$, що зменшує потужність простору ключів перестановки в порівняні з N^{N-1}.

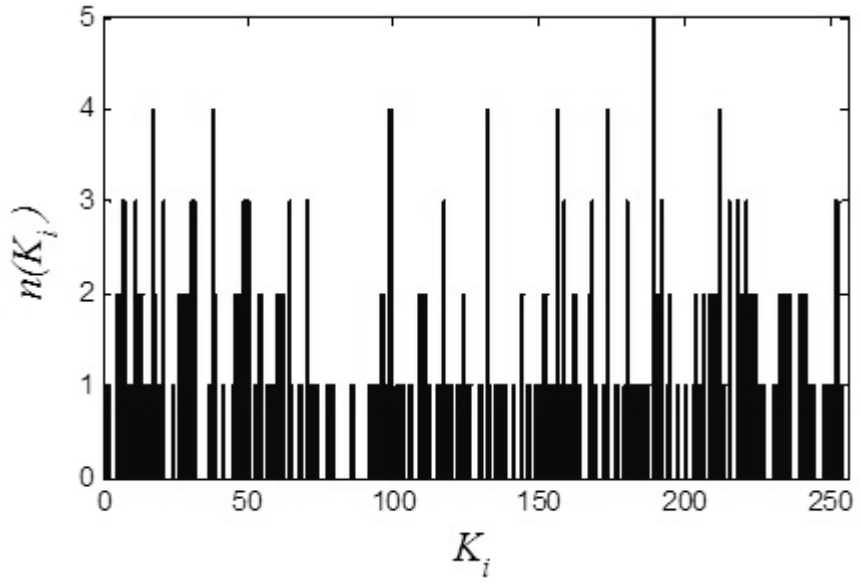


Рис. 5.3. Гістограма розподілу субключів для зображення розмірністю (256×256) при $K = 1000003$.

Приймаючи обмеженою кількість появи субключів перестановки K_i, оцінимо простір ключів для атаки грубою силою як кількість перестановок N різних елементів N, за умови, що кожен елемент зустрічається m разів [122]:

$$K = \sum_{\substack{n_1+n_1+n_N=N \\ n_i \leq m,\ i=1\ldots N}} \frac{N!}{n_1!n_2!\ldots n_N!} = \sum_{r_1=N-m}^{N} \sum_{r_2=r_1-m}^{r_1} \sum_{r_3=r_2-m}^{r_2} \ldots \sum_{r_1=N-m}^{r_{k-1}} C_N^{r_1} C_{r_1}^{r_2} C_{r_2}^{r_3} \ldots C_{k-1}^{r_k} \quad (5.7)$$

Таблиця 5.1

Зменшення простору ключів, %

N	m=3	m=5	m=7
64	72.6	3.2	0.046
128	93.1	6.81	0.11
256	99.6	13.7	0.11

Властивості субключів можуть бути використані зловмисником, щоб вибрати найбільш зручний ключ для початку атаки, і тим самим збільшити свої шанси на успіх.

При апаратній реалізації потужність множини станів хаотичної системи визначається прецизійністю обчислень [101]. Для перестановок з використанням (5.1), це також справедливо. Проведемо оцінку потужності простору ключів системи (5.1), за умови, що параметр K є додатнім цілим числом. При розрахунках із подвійною точністю на мантису виокремлено 52 біта. Послідовний діапазон цілих чисел, що може бути представлений у формі подвійної точності є $1 \dots 2^{53}$ [105]. Беручи до уваги можливі степені двійки, різних додатніх цілих чисел K є $2^{61,9}$. В [119] рекомендується використовувати для перестановок зображення розміром $N \geq 128$. Таким чином, можна сказати, що найбільш підходящим методом розкриття перестановок на базі стандартного відображення (5.1) є перебір всіх можливих значень ключа оскільки:

$$N^{N-1} = 128^{127} \cong 2^{894,6} \gg 2^{61,9}. \tag{5.8}$$

Дійсна потужність простору ключів для сучасних обчислювальних систем є малою в порівнянні з теоретичною. Зазначимо, що N^{N-1} є кількістю варіантів атаки грубою силою при різних можливих методах без урахування часових затрат для їх реалізації.

5.1.4. Криптографічна атака на базі кореляції між сусідніми пікселями

Беручи до уваги, що можливе існування тільки N варіантів зсуву елементів другого стовпця по відношенню до першого і враховуючи що пікселі в сусідніх діагоналях мало відрізняються між собою, можна визначити зсув між пікселями сусідніх стовпців за максимумом кореляційної функції.

Пропонована нами криптографічна атака на перестановки організовується наступним чином:

1. Для двох сусідніх стовпців, починаючи з першого та другого обчислюємо значення кросс-кореляційної функції [123]:

$$c_k = \sum_{k=0}^{N-1} (x_{i,n} - m_i)(x_{i+1,n+k} - m_{i+1}), \tag{5.9}$$

де $m_i = \frac{1}{N} \sum_{n=0}^{N-1} x_i, n.$ - математичне сподівання значення кольору зображення.

2. Знаходимо k для якого:

$$c_k = max\{c_0, c_1, \ldots, c_{n-1}\} \tag{5.10}$$

3. Зсуваємо $i + 1$ стовпець на K позицій вниз.

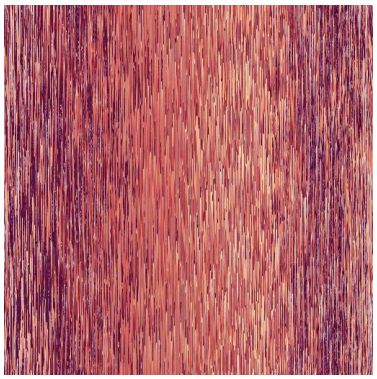
$$x_{x+1,n} = x_{i+1,(n+K) \mod N} \tag{5.11}$$

4. Повторяємо кроки 1, 2 і 3 для інших стовпців в зображенні.

Якщо на етапі виконання п. 2 отримуємо декілька рівних за значенням c_k, тоді здійснюємо розгалуження алгоритму. Алгоритм був протестований на зображенні приведеному рис. 5.4.

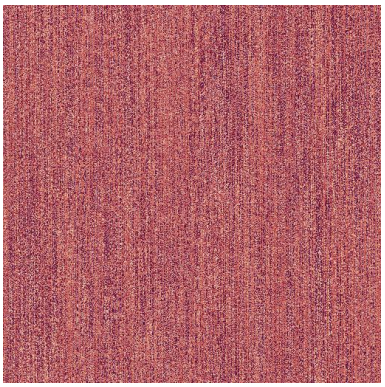
Рис. 5.4. Тестове зображення (512×512).

Результати тестування пропонованого алгоритму приведено на рис. 5.5.



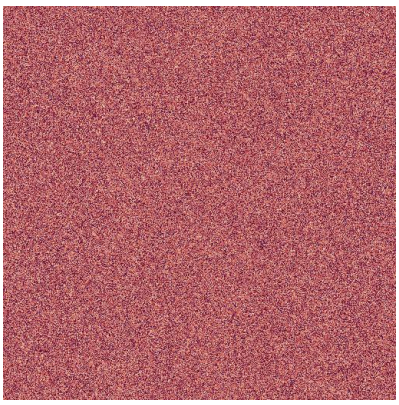
а

б

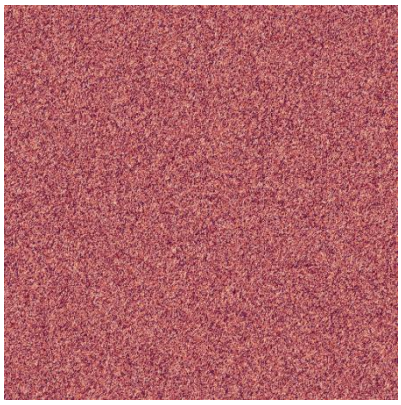


в

г



д



е

Рис. 5.5. *а*; *в*; *д* - зашифроване зображення після одного, двох та трьох циклів перестановки; *б*; *г*; *е* - відновлене.

Після першого і другого циклів перестановок вихідне зображення успішно відновлено (рис. 5.5 *б*, *г*). Тим не менш, спостерігаються спотворення. Після трьох циклів перестановок значення кореляції між сусідніми пікселями є малим і відновлення вихідного зображення за допомогою цього методу ускладнене. Таким чином, використовуючи представлену атаку перестановки можуть бути розкриті після двох циклів перестановок.

5.2.Модифікація стандартного відображення для цифрових систем зв'язку.

Для того щоб отримати максимальну потужність простору ключів для відображення (5.1) запропоновано ввести нелінійну функцію в зміну x_{j+1}. Тоді модифіковане відображення набуде вигляду:

$$x_{j+1} = \left(x_j + K_1 \sin\frac{y_j N}{2\pi}\right) mod\ N,$$
$$y_{j+1} = \left(y_j + K_2 \sin\frac{x_{j+1} N}{2\pi}\right) mod\ N, \qquad (5.12)$$

де K_1 і K_2 – параметри системи.

5.2.1. Властивості нового відображення

Критерієм хаотичної поведінки нелінійної системи є швидкість розбігання близьких траєкторій, що кількісно оцінюються значенням старшого показника Ляпунова [18]. Для (5.12) залежності показників Ляпунова від параметрів системи приведено на рис. 5.6. Розрахунок здійснено методом QR [124]. Як слідує з рис. 5.6, система (5.12) є хаотичною при заданих значеннях параметрів, сума показників Ляпунова дорівнює нулю, що є ознакою консервативності системи.

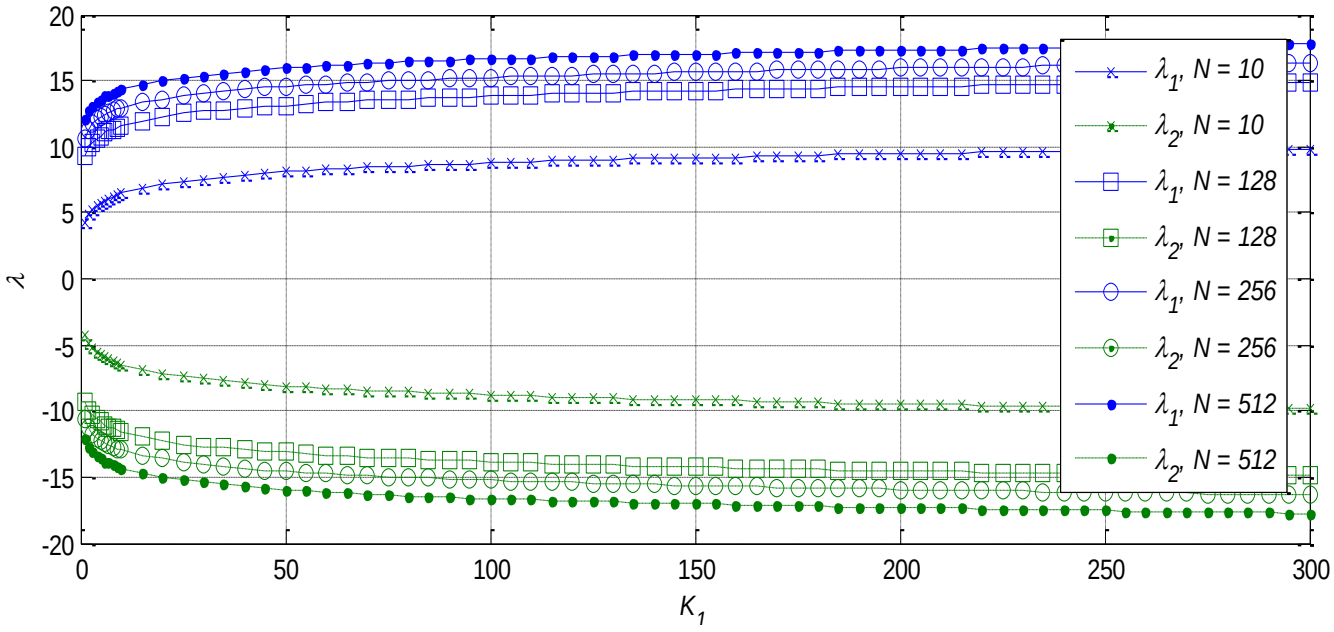


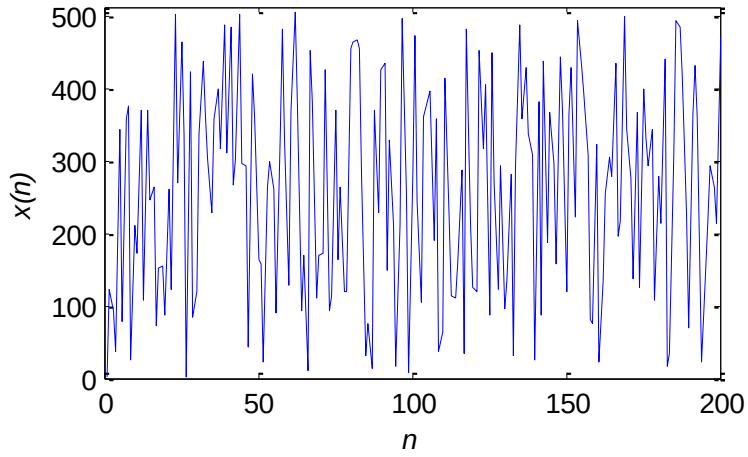
Рис. 5.6. Залежність показників Ляпунова для системи (5.12) від параметра K_1 і N при $K_1 = 100$

Значення якобіана системи (5.12) не залежить від значення параметрів K_1 і K_2:

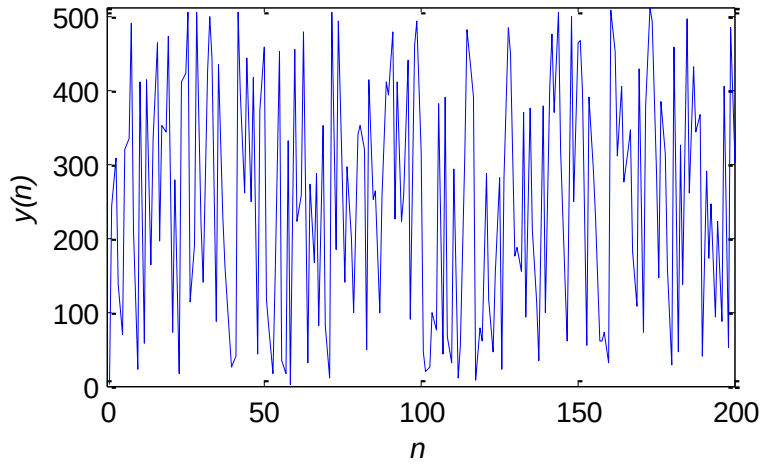
$$D = \begin{vmatrix} \frac{\partial x}{\partial x} & \frac{\partial x}{\partial y} \\ \frac{\partial y}{\partial x} & \frac{\partial y}{\partial y} \end{vmatrix} = \begin{vmatrix} 1 & \frac{K_1 N}{2\pi}\cos\frac{yN}{2\pi} \\ \frac{K_2 N}{2\pi}\cos\frac{\left(x + K_1 \sin\frac{yN}{2\pi}\right)N}{2\pi} & 1 + \frac{K_1 K_2 N^2}{(2\pi)^2}\cos\frac{\left(x + K_1 \sin\frac{yN}{2\pi}\right)N}{2\pi}\cos\frac{yN}{2\pi} \end{vmatrix} = 1,$$

тобто, відображення буде зберігати площу і є потенційно придатним для здійснення перестановок у хаотичних алгоритмах шифрування.

Приклади реалізації хаотичного процесу відображення (5.12) приведено на рис. 5.7.



а



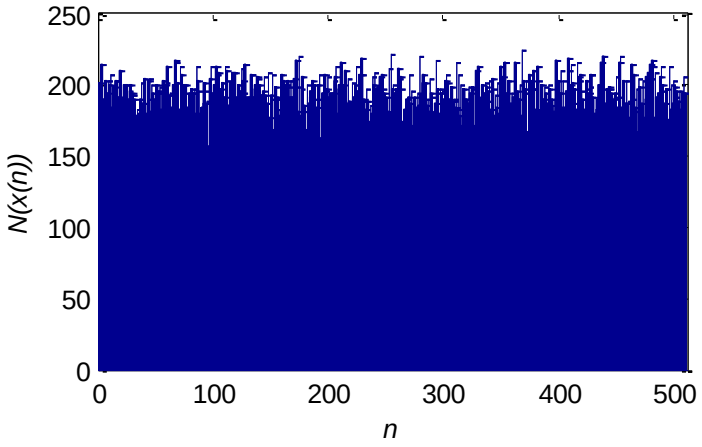
б

Рис. 5.7. Приклади розв’язків системи (5.12): *а* – для змінної *x*, *б* – для змінної *y*.

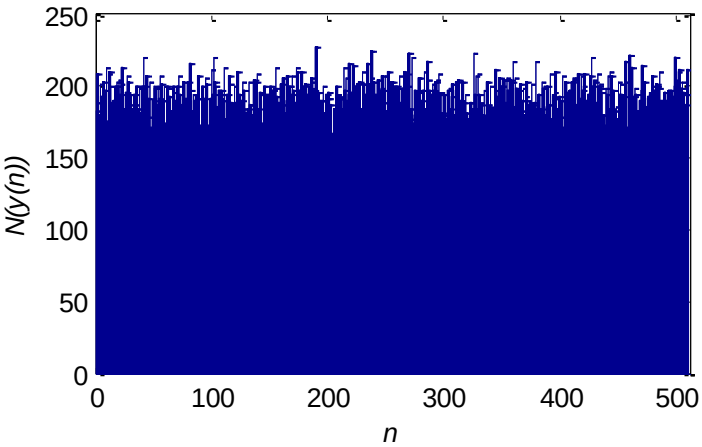
Всі ітераційні залежності мають вигляд на випадкових коливань, але утворюються детермінованими системами. З точки зору обчислювальної складності система (5.12) є складнішою, порівняно з (5.1) тому що для розрахунку наступної ітерації необхідно двічі знаходити значення функції синуса. Враховуючи, що значення тригонометричних функцій у цифровій техніці обчислюються за допомогою розкладу в ряд Тейлора шуканих функцій, за

кількістю необхідних часових ресурсів і/або об’єму пам’яті відображення Кота і стандартне є простішими та потребують виконання меншої кількості математичних операцій.

Гістограми розподілу розв’язків системи (5.12) характеризуються рівномірним розподілом (рис. 5.8), що найчастіше зустрічається в криптографії. Рівноймовірність розподілу обох змінних означає незалежність (в статистичному розумінні) між послідовними ітераціями хаотичного процесу.



а



б

Рис. 5.8. Гістограми розподілу розв’язків системи (5.12): *а* – для змінної *x*, *б* – для змінної *y*.

При виконанні перестановок пікселів у зображеннях системи рівнянь (5.1)-(5.3) і (5.12) пов’язують поточну та наступну координати пікселя з точністю до дробової частини. Дискретизоване по розміру зображення $N \times N$ відображення матиме вигляд

$$X_{j+1} = \left\lfloor \left(X_j + K_1 \sin \frac{Y_j N}{2\pi} \right) mod\ N \right\rfloor,$$
$$Y_{j+1} = \left\lfloor \left(Y_j + K_2 \sin \frac{X_{j+1} N}{2\pi} \right) mod\ N \right\rfloor, \quad (5.13)$$

де X_j, Y_j – початкові координати j- *го* пікселя, X_{j+1}, Y_{j+1} – координати j- *го* пікселя після перестановки; $\lfloor \cdot \rfloor$ – операція отримання цілої частини числа.

Обернене до (5.13) дискретизоване відображення застосовується для відновлення зображення після перестановки:

$$X_{j+1} = \left\lfloor \left(X_j - K_1 \sin \frac{Y_{j+1} N}{2\pi} \right) mod\ N \right\rfloor,$$
$$Y_{j+1} = \left\lfloor \left(Y_j - K_2 \sin \frac{X_j N}{2\pi} \right) mod\ N \right\rfloor, \quad (5.14)$$

При шифруванні та розшифруванні зображення в кілька циклів відповідну кількість раз необхідно застосовувати (5.13) і (5.14).

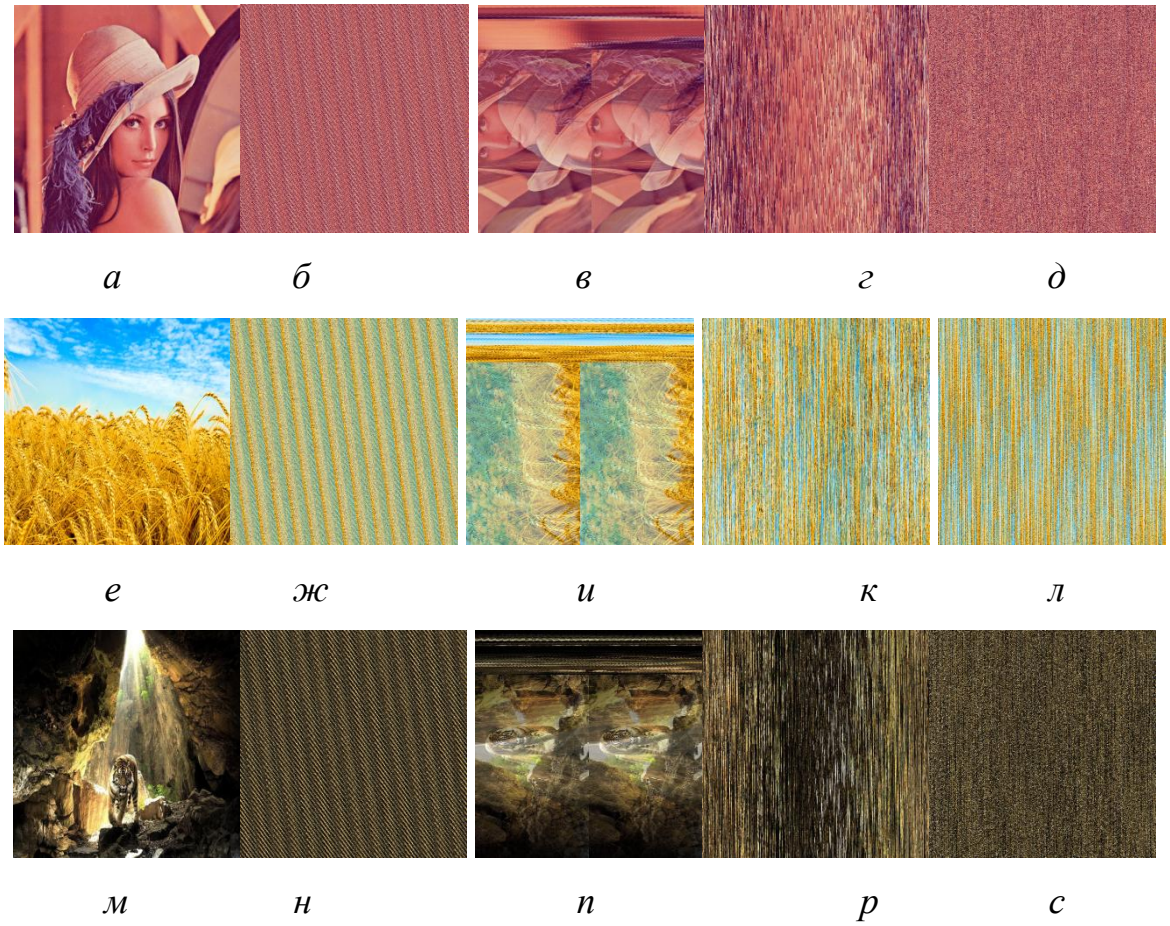
В порівнянні з дискретизованим стандартним відображенням [121] система (5.13) має дві нелінійності $K_1 \sin \frac{y_j N}{2\pi}$ і $K_2 \sin \frac{x_{j+1} N}{2\pi}$, і два параметри K_1 і K_2. Наявність двох незалежних рівноцінних параметрів квадратично збільшує ключовий простір системи. Оскільки для стандартного відображення можна ефективно застосувати кореляційну атаку, яка при одному або двох циклах перестановки дає змогу повністю дешифрувати зображення, не знаючи ключа *K*, нелінійність у кожному рівнянні (5.13) вносить невизначеність в обидві змінні (координати), що покращує якість перестановки, і дає змогу усунути недоліки, характерні для стандартного відображення.

5.2.2 Порівняння ефективності перестановок

Розглянемо ефективність перестановок з використанням пропонованого та відомих відображень на прикладі зображення розміром 512×512 пікселів. Тестові зображення наведені на рис. 5.9 *а, е, м*.

Після перестановки за допомогою відображення Кота (рис. 5.9 *б, ж, н),* незважаючи на відсутність контурів оригінального зображення в шифрованому, спостерігаються певні закономірності, що призводять до циклічності

перестановки і можуть бути використані зловмисником. Застосування відображення Бейкера не дає змоги ефективно перемішати пікселі (рис. 5.9 *в, и, п*), зміст оригінального зображення можна легко зрозуміти на основі шифрованого. Наші дослідження показують, що якість перестановок згідно (5.3) залежить від ключа і може мати малий період перестановки в декілька циклів.



а *б* *в* *г* *д*

е *ж* *и* *к* *л*

м *н* *п* *р* *с*

Рис. 5.9. *а, е, м* - оригінальні зображення, *б, ж, н* - після перестановки за допомогою (5.2), *в, и, п* - після перестановки за допомогою (5.3), *г, к, р* – після перестановки за допомогою (1, *д, л, с* - після перестановки за допомогою (5.4).

Для перестановок пікселів в зображеннях на рис. 5.9 використовувались наступні параметри приведені в табл. 5.2.

Таблиця 5.2.

Використовувані параметри відображень для перестановок

Відображення	Параметри
Стандартне	K= 10000
Кота	v = 5677, u = 4359
Бейкера	{32, 4, 64, 2, 2, …, 2}
Пропоноване	K_1=K_2 = 10000

Один цикл перестановок за допомогою стандартного відображення теж не призводить до рівномірного розпорошення пікселів (рис. 5.9 *г, к, р*), тому для ефективного перемішування необхідно використовувати більшу кількість циклів. При використанні відображення (5.13), задовільне перемішування пікселів для заданих зображень можна отримати за один цикл перестановки (рис. 5.9 *д, л, с*).

Мірою взаємозв'язку між зображеннями є коефіцієнт кореляції. Чим менше значення модуля коефіцієнта кореляції, тим менш подібними будуть два зображення. Розглянемо, як змінюється кореляція між сусідніми пікселями по горизонталі і по вертикалі. Для розрахунку кореляції використаємо наступну формулу [123]:

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j^{\,2} - (\sum_{j=1}^{N} x_j)^2) \times (N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \qquad (5.15)$$

де x, y – значення градацій кольору двох сусідніх пікселів, N – кількість пікселів у зображенні.

Для оригінального зображення (рис. 5.9 *а*) значення коефіцієнта кореляції між сусідніми пікселями по горизонталі і вертикалі дорівнює 0,9759 та 0,9857 відповідно. Розраховані значення коефіцієнта кореляції після одного циклу перестановок наведені в Табл. 5.3.

Таблиця 5.3.

Кореляція пікселів зображення після одного циклу перестановок

Зображення	Кореляція пікселів	Відображення			
		Кота	Бейкера	Стандартне	Нове
Рис. 5.9 *а*	по горизонталі	-0,0796	0,9829	0,0972	-0,0011
	по вертикалі	0,1198	0,0433	0,9699	0,0375
Рис. 5.9 *е*	по горизонталі	-0,3555	0,9436	-0,0389	-0,0498
	по вертикалі	0,6639	-0,2540	0,9010	0,6258
Рис. 5.9 *м*	по горизонталі	0,1129	0,9673	0,0393	-0,0039
	по вертикалі	0,4548	0,1246	0,9468	0,0391

Серед досліджених систем найгірші кореляційні властивості перестановок забезпечує відображення Бейкера, для якого за один цикл перестановки кореляція пікселів по горизонталі майже не змінюється. Для стандартного відображення високим залишається значення коефіцієнта кореляції по вертикалі. Перестановки за допомогою (5.13) забезпечують найменшу кореляцію для всіх тестових зображень (табл. 5.3).

Для порівняння зазначимо, що в [119] для стандартного відображення рекомендується виконувати мінімум 4 цикли перестановок. В таб. 5.4 приведені значення коефіцієнтів кореляції при двох циклах перестановки.

Таблиця 5.4.

Кореляція пікселів зображення після двох циклів перестановок

Зображення	Кореляція пікселів	Відображення			
		Кота	Бейкера	Стандартне	Нове
Рис. 5.9 *а*	по горизонталі	0,1083	0,0438	-0,0040	-0,0026
	по вертикалі	0,0099	0,0090	0,0969	-0,0029
Рис. 5.9 *е*	по горизонталі	-0,2535	-0,2552	$-1.0756*10^{-4}$	$7,4517*10^{-4}$
	по вертикалі	0,3038	0,4974	-0,0392	$-1,1870*10^{-4}$
Рис. 5.9 *м*	по горизонталі	0,1477	0,1219	-0,006	-0,0028
	по вертикалі	-0,1896	-0,1092	0,0396	$-6,5642*10^{-4}$

Як випливає з аналізу, приведених в табл. 5.4 значень коефіцієнтів кореляції при двох циклах перестановки, нове відображення володіє найкращими кореляційними властивостями.

5.2.3 Оцінка часу перестановок

Безпека криптосистеми знаходиться в зв’язку з її обчислювальною складністю. В свою чергу обчислювальна складність залежить від кількості циклів, складності хаотичного відображення і функції дифузії. Висока складність, зумовлена хаотичним відображенням або функцією дифузії, може бути зменшена шляхом вибору підходящого відображення. Оцінку обчислювальної складності проведемо за допомогою часу роботи алгоритму перестановки для різних відображень. Результати дослідження наведені в табл. 5.5. Для розрахунку використовувався ноутбук з Intel Corel Dual CPU 1,86 ГГц, 2ГБ ОЗУ.

Серед відображень Кота, стандартного та нового існує певна різниця в тривалості перестановки, проте не можна стверджувати, що вона є значною (таб. 5.5). Це пояснюється тим, що найбільше часу в процесі перестановки займає власне пошук і перемішення пікселя в матриці пікселів з одного положення в інше. При цьому час розрахунку значень наступного положення пікселя є малим в порівнянні з часом його переміщення.

Таблиця 5.5

Тривалість одного циклу перестановок для різних відображень, с

Зображення	Відображення			
	Кота	Бейкера	Стандартне	Нове
Рис. 5.9 *а*	0,913	11,458	0,935	0,996
Рис. 5.9 *е*	0,898	11,360	0,928	0,993
Рис. 5.9 *м*	0,887	11,488	0,937	0,981

В порівнянні з стандартним нове відображення характеризується більшою тривалістю циклу. Проте, якщо врахувати суттєве збільшення простору ключів та зменшення кількості циклів, необхідних для уникнення кореляції між сусідніми пікселями, його використання є повністю виправданим і доцільним.

5.2.4 Потужність простору ключів модифікованого відображення

Оскільки в криптосистемах використовуються процеси перестановок і дифузії, тому ключовий простір криптосистеми дорівнює добутку кількості ключів цих процесів. Нехай простір ключів при дифузії дорівнює S_1, а для перестановок – S_2; тоді для криптосистеми

$$S = S_1 S_2. \tag{5.16}$$

На практиці для різних циклів можуть використовуватися різні ключі. Якщо n – кількість циклів, тоді простір ключів становить:

$$S = (S_1 S_2)^N. \tag{5.17}$$

Із (5.17) випливає, що простір ключів S криптосистеми збільшується зі збільшенням простору ключів перестановок S_1, області початкових значень ключів дифузії S_2, або кількості циклів n. Для різних хаотичних відображень

розмір області значень ключа шифрування наведено в табл. 5.6. Для нового відображення (5.13) два параметри K_1 і K_2 вносять невизначеність в перестановку. Зсув пікселя по горизонталі визначається значенням $d_x = \left(K_1 sin\frac{y_j N}{2\pi}\right) mod\ N$, по вертикалі – $d_y = \left(K_2 sin\frac{x_{j+1} N}{2\pi}\right) mod\ N$. В обох випадках існує N можливих варіантів зсуву по кожній координаті. Піксель після перестановки в залежності від значень ключів K_1 і K_2 може опинитися на будь-якій позиції $N \times N$ матриці пікселів. Піксель з координатами (0, 0), як і у випадку стандартного відображення, не змінюватиме свою позицію, незалежно від кількості циклів перестановки. Тому максимальний ключовий простір пропонованого відображення становитиме (N^2-1)!.

Таблиця 5.6

Оцінка максимального простору ключів перестановки для зображення розміром $N \times N$ з кількістю компонент кольору L.

Хаотичне відображення	Простір ключів перестановки відображення, S_2	Простір ключів перестановки (один ключ в різних циклах) для зображення, S_2	Простір ключів криптосистеми (різний ключ в різних циклах) для зображення, S_2
Кота	N^2	N^2L	$N^{2n}L^n$
Бейкера	2^{N-1}	$2^{N-1}L$	$2^{n(N-1)}L^n$
Стандартне	N^{N-1}	$N^{N-1}L$	$N^{n(N-1)}L^n$
Відображення з двома нелінійностями (5.13)	N^2-1!	$(N^2$-1)!L	$((N^2$-1)!$)^nL^n$

Оцінка ключів перестановки для (5.13) отримана при умові, що параметри K_1 і K_2 не обмежені за максимальним значенням. Реальний розмір ключів обмежиться мінімальним значенням між добутком потужності множин значень параметрів K_1 і K_2 і величиною $(N^2 - 1)!$ та залежатиме від прецизійності обчислень:

$$S_2 = \min\{card(K_1) * card(K_2),\ (N^2 - 1)!\}. \qquad (5.18)$$

Ключовий простір збільшується, якщо в кожному циклі використати різні ключі. З таблиці 5.6 можна пересвідчитися, що пропоноване відображення має найбільший простір ключів, а відображення Кота – найменший.

5.3. Метод шифрування зображень із взаємозалежними етапами дифузії і перестановки

Одним з недоліків ряду алгоритмів шифрування растрових зображень на основі детермінованого хаосу є вразливість до ряду криптографічних атак, зокрема відкритим та вибраним відкритим текстом [99, 119]. Шифрування в таких алгоритмах складається з двох послідовних етапів дифузії і перестановки, що повторюються кілька раундів (рис. 5.10).

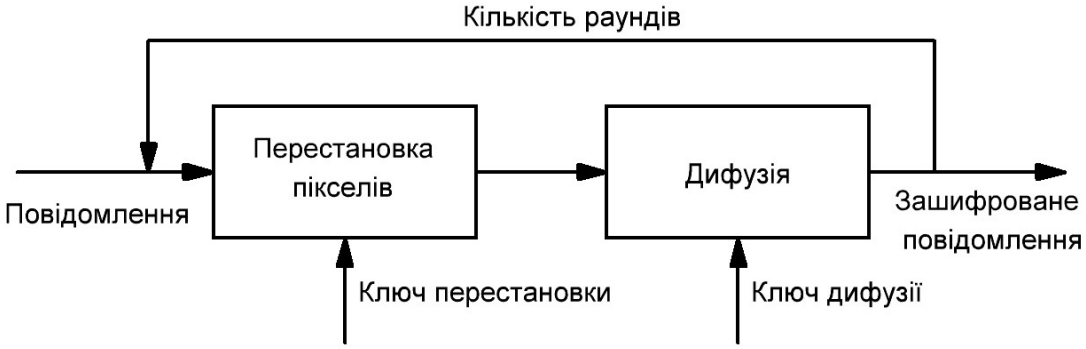


Рис. 5.10. Блок-схема методу шифрування зображень
на основі хаотичних систем

Із рис. 5.10 випливає, що результат операції дифузії залежить від перестановки пікселів. Однак дифузія не впливає на перестановку, що робить її статичною в межах одного ключа. Незалежно від початкового зображення, кожному його пікселю відповідатиме фіксована позиція у зашифрованому. Вказана вразливість уможливлює розкриття гамми шифрування, без знання ключа.

5.3.1. Атака вибраним відкритим текстом

Нами запропоновано та успішно проведено криптографічну атаку на шифроване зображення згідно [125] за наступним алгоритмом:

1. Задаємо зображення розміром $N * N$ з трьома градаціями кольору (RGB), для якого кожна складова кольору всіх пікселів дорівнює нулю, та шифруємо його згідно алгоритму [125]. В результаті отримаємо послідовність для дифузії

– матрицю D з елементами $d_{i,j,k},\ i,j=1..N,k=1..3.$

2. Довільно змінюємо значення кольору *n*-го пікселя зображення, шифруємо його, отримаємо матрицю P з елементами $p_{i,j,k}\ i,j=1..N,k=1..3.$

3. Порівнюючи матриці D і P, шукаємо елемент з різними значеннями кольору, координати якого відповідатимуть позиції *n*-го пікселя оригінального зображення у шифрованому.

4. Повторюємо п. 2-3 для всіх пікселів зображення і заповнюємо таблицю відповідності координат пікселів оригінального та шифрованого зображення.

Знаючи матрицю дифузії D та таблицю відповідності перестановки, дешифрування довільного зашифрованого зображення, що задане матрицею C з елементами $c_{i,j,k}\ i,j=1..N,k=1..3$ здійснюється за два етапи:

1. Обернена перестановка пікселів. Отримаємо матрицю C' з елементами $c'_{i,j,k}\ i,j=1..N,k=1..3.$

2. Операція дифузії, що полягає у побітовому додаванні за модулем 2 послідовності для дифузії та матриці C':

$$M=C'\oplus D. \tag{5.20}$$

Алгоритм вимагає виконання N^2 операцій шифрування заданого відкритого тексту, і дає змогу відновити послідовність для дифузії та таблицю для перестановок незалежно від використаних хаотичних систем.

Реалізувавши описаний алгоритм системі MatLab на ПК з IntelCore i7 3.4ГГц, ОЗУ 8Гб, нам вдалося дешифрувати зображення розміром 512*512 пікселів за 18,2 год.

5.3.2. Розробка методу шифрування зображень із взаємозалежними етапами дифузії і перестановки

Щоб згенерувати псевдовипадкову послідовність для дифузії використано тривимірну систему Лоці (4.7), для перестановки пікселів двовимірну систему (5.13). Проте, на практиці складно отримати однакові значення функції синуса використовуючи різні апаратні платформи. Тому необхідно використовувати

заздалегідь підготовлені таблиці значень або розробити відображення, що оперує цілими числами та зберігає площу.

Для реалізації хаотичної системи в цілочисельному діапазоні необхідно замінити нелінійні функції $\sin\frac{y_j N}{2\pi}$ та $\sin\frac{x_{j+1} N}{2\pi}$ на y_j^2 та x_{j+1}^2, відповідно. Тоді система (5.13) набуде вигляду:

$$\begin{cases} x_{j+1} = \left(x_j + K_1 y_j^2\right) mod\ N \\ y_{j+1} = \left(y_j + K_2 x_{j+1}^2\right) mod\ N \end{cases}, \qquad (5.21)$$

де K_1 і K_2 – параметри системи.

Один раунд шифрування RGB-зображення розміром $N*N$ виконується за наступним алгоритмом:

1. Задаємо ключ шифрування K довжиною 256 біт.

2. Розділяємо ключ К на вісім підключів $K_1 \ldots K_8$ довжиною в 32 біти кожен.

3. Задаємо для системи (4.8) початкові умови та значення параметрів як $x(0) = K_1 / 2\wedge 32,\ y(0) = K_1 / 2\wedge 32,\ \ z(0) = K_1 / 2\wedge 32,$ $a_1 = K_4 / 2\wedge 32 + 1, a_2 = K_5 / 2\wedge 32 + 1,\ a_3 = K_6 / 2\wedge 32 + 1$ Ітеруємо (2) N^2 раз. Отримаємо три послідовності чисел $\{x_1^{(1)}, x_2^{(1)}, \ldots x_{N^2}^{(1)}\}, \{x_1^{(2)}, x_2^{(2)}, \ldots x_{N^2}^{(2)}\},$ $\{x_1^{(3)}, x_2^{(3)}, \ldots x_{N^2}^{(3)}\}$. З кожного числа послідовностей вибираємо з 25 по 32 біти та перетворюємо їх у послідовності цілих чисел, формуємо матрицю $\mathbf{D} = \{d_{Ri,j,k}\}$ розміром $N*N*3,\ i, j = 1..N, k = 1..3.$

4. Виконуємо дифузію згідно:

$$\mathbf{D_R} = \mathbf{(M + D)} \bmod 256, \qquad (5.22)$$

де $\mathbf{M}$, $\mathbf{D}_R = \{d_{Ri,j,k}\}$ – матриці розміром $N*N*3$ 8-мибітних чисел, що дорівнюють значенням градацій кольору зображення перед та після операції дифузії, $i, j = 1..N, k = 1..3.$

5. Формуємо ключ для перестановок. Для кожного пікселя зображення ітеруємо систему (4.8) p раз з початковими умовами $\{d_{Ri,j,1} / 256, d_{Ri,j,2} / 256, d_{Ri,j,3} / 256\}$ та значеннями параметрів a_1, a_2, a_3. Після p

ітерацій кінцевим станом будуть дійсні числа $\{x^{(1)}(p), x^{(2)}(p), x^{(3)}(p)\}$ з яких вибираємо старші 32 біти і перетворюємо їх у послідовності цілих чисел, формуючи матрицю $\mathbf{Z} = \{z_{Ri,j,k}\}$ розміром $N*N*3$, $i, j = 1..N, k = 1..3.$

Знаходимо суми елементів $S_k^{'} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} z_{Ri,j,k}, k = 1,2,3,$ отримаємо три цілих числа $\{S'_1, S'_2, S'_3\}$.Для приховання значень $\{S'_1, S'_2, S'_3\}$система (4.8) ітерується m раз з початковими умовами $\{S'_1/2^{32}, S'_2/2^{32}, S'_3/2^{32}\}$.та значеннями параметрів a_1, a_2, a_3. Кінцевим станом (2) будуть три дійсних числа $\{x^{(1)}(m), x^{(2)}(m), x^{(3)}(m)\}$ з яких формуються підключі $\{S_1, S_2, S_3\} = \{\lfloor x^{(1)}(m) * 2^{32} \rfloor, \lfloor x^{(2)}(m) * 2^{32} \rfloor, \lfloor x^{(3)}(m) * 2^{32} \rfloor\}$, де $\lfloor \bullet \rfloor$ – ціла частина числа. Ключі для перестановки (параметри системи (5.21)) визначаються наступним чином:

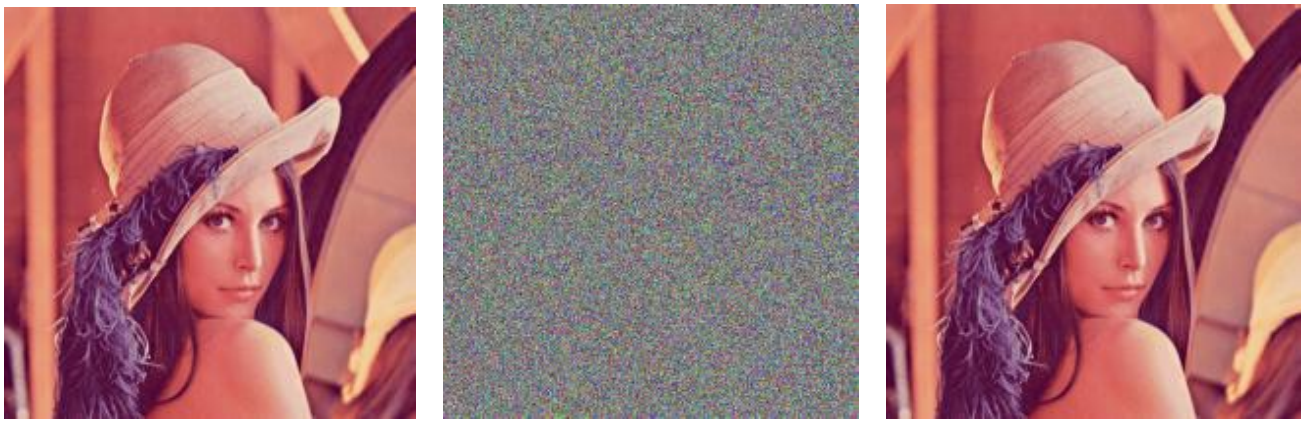
$$\begin{aligned} B_1 &= \left(K_7 S_1 + S_2 S_3\right) \bmod 2^{32}, \\ B_2 &= \left(K_8 S_2 + S_1 S_3\right) \bmod 2^{32}. \end{aligned} \tag{5.23}$$

Залежність ключа перестановки від результату операції дифузії унеможливлює атаку вибраним відкритим текстом.

Розшифрування зображення проводиться в оберненому порядку, оскільки метод шифрування є симетричним.

Результати описані далі отримані для одного раунду шифрування, при p = 5, m = 20.

Приклад зашифрованого і розшифрованого зображення наведено на рис. 5.10. Коефіцієнт кореляції між оригінальним та зашифрованим зображеннями становить $-1{,}31*10^{-4}$.



а *б* *в*

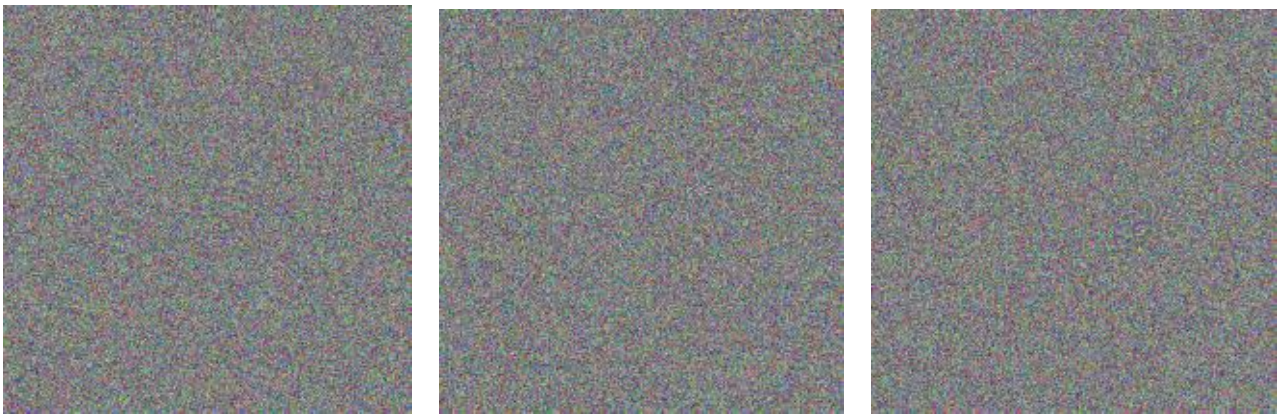
Рис. 5.11. Шифрування тестового зображення: *а* – оригінальне зображення, *б* – зашифроване зображення, *в* – розшифроване зображення

Результат перевірки чутливості запропонованого методу до ключа шифрування наведено на рис. 5.12. Два ключі шифрування:

$K^{(1)}$={D0E720E9A118478CF5F728F8F57CCC246BEA
CAF5A709D9EFADC1BE64A72BB408}

і $K^{(2)}$={42CC6EE92E432522DE948C25DA9F
598366133D1F2F3D6A0CE7F17D7D56E65E1C}

відрізнялися на 1 біт.



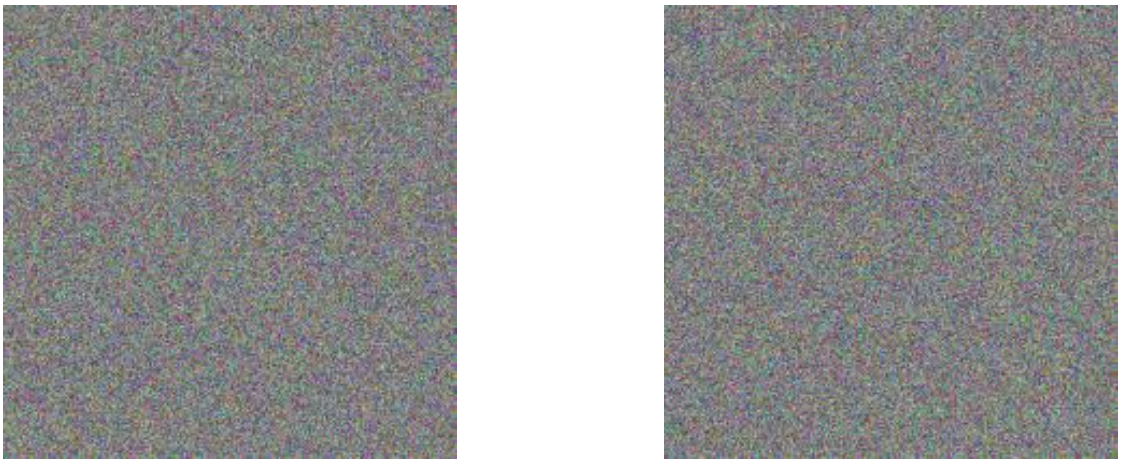
а *б* *в*

Рис. 5.12. Вигляд зашифрованого тестового зображення (рис. 5.10 *а*): *а* – зашифроване зображення для ключа $K^{(1)}$, *б* – зашифроване зображення для ключа $K^{(2)}$, *в* – зображення зашифроване за допомогою $K^{(2)}$ та розшифроване $K^{(1)}$

Кореляція між зашифрованими зображеннями (рис. 5.10 *а* і *б*) становить $5.37*10^{-4}$. Кореляція між зображенням зашифрованим ключем $K^{(2)}$ і розшифрованим за допомогою ключа $K^{(1)}$ (рис. 5.11 *в*) та оригінальним (рис. 5.10

а) була низькою і дорівнювала -1.4790*10^{-4}, що вказує на високу чутливість до ключа шифрування.

Для перевірки чутливості до повідомлення було змінено один біт колір останнього пікселя зображення (рис. 5.10 *а*), коефіцієнт кореляції між зашифрованими зображеннями після одного раунду шифрування (рис. 5.13) становить 0,0145.



а *б*

Рис. 5.13. Зашифроване тестове зображення *а* – оригінальне, *б* – зі зміненим останнім пікселем для ключа шифрування
42CC6EE92E432522DE948C25DA9F598366133D1F2F3D6A0C
E7F17D7D56E65E1C

Висновки до п’ятого розділу

1. Розроблено та досліджено нове дискретне хаотичне відображення для перестановок пікселів в зображеннях $N \times N$ розмірності.

2. Представлено порівняння якості перестановок пікселів новим відображенням з іншими відомими двомірними відображеннями. Досліджено швидкість перестановок, стійкість до кореляційної атаки.

3. Встановлено, що при використані пропонованого відображення можна скоротити кількість циклів перестановки пікселів з врахуванням унеможливлення кореляційної атаки. З’ясовано, що потужність простору ключів перестановок є максимальною для растрових зображень $N \times N$ розмірності і становить $(N^2 - 1)!$.

4. Проаналізовано та визначено недоліки методу шифрування растрових зображень з незалежними етапами дифузії і перестановки та показано можливість розкриття шифру. Запропоновано спосіб шифрування стійкий до атаки вибраним відкритим текстом, в якому ключ перестановки визначається результатом дифузії.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

У дисертаційній роботі розв’язано науково-прикладне завдання аналізу, синтезу та практичної реалізації генераторів псевдовипадкових та випадкових послідовностей на основі багатовимірних нелінійних динамічних систем. Основні результати дисертаційного дослідження викладені у висновках, що зводяться до наступних положень:

1. Проведено ретельний аналіз сучасного стану ГПВП та ГВП на базі нелінійних динамічних систем. Досліджено вплив обмеження точності обчислень на статистичні властивості логістичного відображення при його апаратній реалізації на базі ПЛІС з використанням арифметики з фіксованою комою Q3.29. Встановлено, що потужність множини різних початкових умов після перехідного процесу дорівнює сумі довжин всіх можливих циклів та становить $24797 \approx 2^{14}$. Визначено залежність потужності простору початкових умов для логістичного відображення від кількості ітерацій.

2. Досліджено двовимірну дискретну хаотичну систему Тратаса. Встановлено, що генератор хаотичних сигналів на базі системи Тратаса генерує хаотичні та гіперхаотичні коливання в широкому неперервному діапазоні значень параметрів керування. Запропоновано спосіб отримання випадкових сигналів на основі модифікованої багатовимірної системи Тратаса, що уможливлює формування сигналів із наперед заданим розподілом їх значень.

3. Схемотехнічно реалізовано генератор випадкових сигналів на базі відображення Лоці із кільцевим зв’язком, що може бути використаний для генерування випадкових сигналів із швидкістю 0,84 Мбіт/с при умові використання двовимірної системи та частоти тактового сигналу 30 кГц.

4. Встановлено, що на основі залежності ентропії розподілу діагоналей рекурентної діаграми модифікованої системи Тратаса можливо оцінити нижню межу розмірності фазового простору системи. Це дозволяє здійснювати підбір системи з розмірністю, при якій розкриття параметрів є ускладненим.

5. Запропоновано метод синтезу псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв’язком, з використанням

збалансованих найменш значущих бітів. Це ускладнює розкриття параметрів генератора, що дозволяє формувати великі ансамблі послідовностей з наперед заданими наборами довжин.

6. Проведено апаратну реалізацію запропонованих генераторів та показано, що при умові використання чотиривимірної системи потенційна швидкість формування ПВП становитиме до 19,2 Гбіт/с. Розроблена структура генератора уможливлює формування псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком довільної розмірності. Проведено тестування генерованих послідовностей на відповідність критеріям псевдовипадковості згідно набору статистичних тестів NIST SP 800-22.

7. Розроблено апаратне рішення методу генерування псевдохаотичних послідовностей на основі математичних моделей неперервних хаотичних систем з використанням в якості нелінійного елементу мемристивної структури, що забезпечує незалежність середньої тривалості періоду повторення в межах $10^6 \div 2 * 10^6$ ітерацій від кроку дискретизації, що становить $\Delta t = 0,0005 \div 0,02$ при умові використання арифметики з фіксованою комою Q8.16.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Галюк С.Д. Аналіз часових рядів генерованих гіперхаотичною системою Тратаса / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 4(251). – С. 187-192.

2. Галюк С.Д.Порівняльний аналіз двомірних відображень для перестановок пікселів / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 1(245). – С. 214-220.

3. Krulikovskyi Oleh V. Image encryption algorithm based on chaotic maps / Oleh V. Krulikovskyi, Petro M. Shpatar, Leonid F. Politanskyi // Eastern European Scientific Journal. – 2014. – №6. – P. 362-366.

4. Круліковський О.В. Особливості вибору хаотичних систем для побудови генераторів псевдовипадкових послідовностей / О.В. Круліковський, С.Д. Галюк, Л.Ф. Політанський // Телекомунікаційні та інформаційні технології. – 2017. – №2. – С. 64-67.

5. Krulikovskyi O.V. Testing timeseries ring-coupled map generated by on FPGA / O.V. Krulokovskyi, S.D. Haliuk, L.F. Politanskyi // Телекомунікаційні та інформаційні технології. – 2016. – №4(53). – С. 24-29.

6. Krulikovskyi O.V. PRNG based on modified tratas chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Сучасний захист інформації. – 2016. – №2. – С. 69-77.

7. Corinto F. Memristor-based chaotic circuit for pseudo-random sequence generators / Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // Proceedings of the 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, April 18-20, 2016. (Індексується у Scopus).

8. Haliuk S. Analysis of Pixels Permutations Based on Discretized Chirikov Map / Sergiy Haliuk, Oleg Krulikovskyi, Leonid Politanskyi // Proceedings of the

XIIIth International Conference TCSET'2016, Lviv-Slavsko, Ukraine, February 23 – 26, 2016. – pp. 519-521. (Індексується у Scopus).

9. Політанський Л.Ф. Циклічність послідовностей генерованих хаотичною системою / Л.Ф. Політанський, С.Д. Галюк, О.В. Круліковський // II Міжнародна конференція з інформаційно-телекомунікаційних технологій та радіоелектроніки УкрМіКо 2017. – м. Одеса, 11-15 вересня 2017 р. – С. 545-548.

10. Krulikovskyi O. Development features of cryptographic means based on chaotic systems / Krulikovskyi Oleh, Haliuk Serhii // Proceeding of the Vth International Scientific Practical Conference "PREDT 2016", 3–5 November, 2016, Chernivtsi, Ukraine. - P.125.

11. Krulikovskyi O.V. Using PRNG based on multidimensional discrete hyperchaotic system for image encryption / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // IV Міжнародна науково-практична конференція «Напівпровідникові матеріали, інформаційні технології та фотовольтаїка»: тези доповідей, м. Кременчуг. 26-28 травня, 2016 р. – С. 234-235.

12. Krulikovskyi O.V. PRNG based on discrete hyper chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Проблеми інформатики та комп'ютерної техніки: Праці V-ї Міжнародної науково-практичної конференції ПІКТ – 2016, Чернівці, Україна, 21 – 24 травня, 2016. – С. 204.

13. Image encryption algorithm based on one-dimensional and two-dimensional maps / M.Ya. Kushnir, G.V. Kosovan, O.V. Krulikovskyi // Proceeding of the II International Scientific- Practical Conferences "PREDT -2012". – Chernivtsi, October 25-27, 2012. – p. 90-91.

14. Encryption algorithm based on two-dimensional standard map / O.V. Krulikovskyi , L. F. Politanskyi // Proceeding of the IV International Scientific-Practical Conferences "PREDT -2014". – Chernivtsi, October 23-25, 2014. – pp. 68-69.

15. Круліковський О.В. Рекурентний аналіз багатовимірних хаотичних систем / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Міжнародна науково-практична конференція "ОСНП - 2017"- м. Черкаси, 24-26 травня, 2017 р. – С. 94-96.

16. Keuninckx Lars Encryption key distribution via chaos synchronization / Keuninckx Lars, Soriano Miguel C., Fischer Ingo, Mirasso Claudio R., Nguimdo Romain M., Van der Sande Guy // Scientific Reports. – 2017. – Vol. 7, Sp - 43428.

17. Шахтарин Б.И. Генераторы хаотических колебаний / Б.И. Шахтарин, П.И. Кобылкина, Ю.А. Сидоркина, А.В. Кондратьэв, С.В. Митин. Москва: Галилеос АРВ. –2007. – 247 с.

18. Мун Ф. Хаотические колебания: Вводный курс для научных работников и инженеров: пер. с англ. — М.: Мир, 1990. — 312 с.

19. Шустер Г. Детерминированный хаос: Введение: пер. з англ. —М.: Мир, 1988. —240 с

20. Неймарк Ю. И., Ланда П. С. Стохастические и хаотические колебания. — М.: Наука. 1987.—424 с.

21. Кроновер Р.М. Фракталы и хаос в динамических системах. Основы теории. Москва: Постмаркет, 2000.-352 с.

22. Заславский Г. М., Сагдеев Р. З., Усиков Д. А., Черников А. А. — Слабый хаос и квазирегулярные структуры. М.: Наука, 1991. — 240 с.

23. Ю.Pecora L., Carroll T. Synchronization of chaotic systems // Phys. Rev. Letters. 1990 Vol. 64. №8. p.821 -824

24. Carroll T., Pecora L. Synchronizing chaotic circuits // IEEE Trans. Vol CAS-38, №4,1991.p.453-456.

25. Pecora L., Caroll T. Synchronizing nonautonomous chaotic circuits // IEEE Trans. On Circuits and System — II :Analog and Digital Signal processing. №2, vol. 40,№ 10,1993.p.646.

26. Carol T.L., Pecora L.M. Synchronizing hiperchaotic volume-preserving maps and circuits // IEEE Trans, on CAS-1, Vol. 45, No. 6, 1998.p.656-659.

27. Морозов А. Г. Использование цифровых хаотических последовательностей для передачи информации : дис. канд. техн. наук : 05.12.04 / Морозов Андрей Геннадиевич – Москва, 2001. – 192 с.

28. Hasler M. Synchronization of chaotic systems and transmission of information // Intern. J. Of Bifurcation and Chaos, Vol.8, No.4, 1998. p.647-659.

29. Tang Y.S., Alistair I, Chua M&L. Synchronization and chaos // IEEE Trans. CAS, Vol.30, №9.

30. Wang X.F., Wang Z.Q. Synchronizing chaos and hiperchaos with any scalar transmitted signal // IEEE Trans, on CAS-1, Vol. 45, No.10. p.l 101-1103.

31. Hasler M., Maistrenko Yu.L. An introduction to the synchronization of chaotic systems: Coupled skew tent maps // IEEE Trans, on CAS-1, Vol. 44, No. 10, 1997.p.856-866.

32. Torikai S.H., Saito T. Synchronization of chaos and its itinerancy from a network by occasional linear connection // IEEE Trans, on CAS-1, Vol. 45, No.4,1998.p.l 101-1103.

33. Yang T., Chua L. Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication // IEEE Trans, on CAS-1, Vol. 44, No. 10,1997.p.976-988.

34. Panas A., Yang T. Chua L. Experimental results of impulsive synchronization between two Chua's circuits // International Journal on Bifurcation and Chaos, Vol.8, No 3, 1998.p.639-647.

35. Fradkov A.L., Markov A.Yu. Adaptive synchronization of chaotic systems based on speed gradient method and passification // IEEE Trans, on CAS-1, Vol. 44, №.l0,1997. p. 905-912.

36. Sushchik M.M. Jr., Rulkov N.F., Abarbanel H.D.I. Robustness and stability of synchronized chaos: An illustrative model // IEEE Trans, on CAS-1 Vol.44, No. 10, 1997.p.867-873.

37. Kolumban G., Kennedy M., Chua L. The role of synchronization in digital communications using chaos Part-I: Fundamental of Digital communications // IEEE Trans on CAS-44, №10, 1997. p.927-936

38. Kolumban G., Kennedy M., Chua L. The role of synchronization in digital communications using chaos Part-II: Chaotic Modulation and Chaotic Synchronization // IEEE Trans on CAS-45, №11, 1998. p. 1129-1140.

39. Endo N., Chua L. Synchronization of Chaos in Phase-Locked Loop // IEEE Trans. On Circuits and Systems, Vol. 38, №12, 1991. p.l580-1588.

40. Volkovski A. Synchronization of chaotic systems using phase control // IEEE Trans. CAS-44, No 10, 1997.p.913-917

41. Н.Дмитриев А.С., Панас А.И., Старков С.О. Динамический хаос как парадигма современных систем связи // Зарубежная Радиоэлектроника, №10, 1997, - с.4-26.

42. Вельский Ю.Л., Дмитриев А.С Передача информации с помощью детерминированного хаоса // Радиотехника и электроника, т.38, №7, 1993. с.1310-1315.

43. Дмитриев А.С., Кузьмин Л.В., Панас А.И., Старков С.О. Эксперименты по передаче информации с использованием хаоса через радиоканал // Радиотехника и Электроника, 1998, т.43, вып.9, с.l 115 -1128

44. Sato A., Endo T. Experiments of Secure Communications Via Chaotic Syncronization of Phase-Locked Loops // IEEE Trans Fundamental. Vol E78-A, No 10, Oct, 1995.p.l286-1290.

45. Kocarev Lj, Halle K.S., Eckert K., Chua L., Parlitz U. Experimental demonstration of secure communication via chaotic synchronization // International Journal on Bifurcation and Chaos, Vol.2, No 3,1992.p.709-713

46. Hasler M. Engineering Chaos for Encryption and Broadband Communication. // Philosophical Transaction of the Royal Society of London. Transaction A.353, 1995. p. 115-126.

47. Ljupco Kocarev Chaos-Based Cryptography Theory, Algorithms and Applications / L. Kocarev, S. Lian. Berlin: Springer-Verlag Berlin Heidelberg, 2011. - 397 pp.

48. Птицын Н. Приложение теории детерминированного хаоса в криптографии / Н. Птицын. – Москва: МГТУ им. Н. Э. Баумана, 2002. – 80 с.

49. *Kennedy M.* Chaos in Colpitts oscillator. IEEE Trans Circuits Syst I. –1994, –P. 771–774.

50. *Maggio G, Feo O, Kennedy M.* Nonlinear analysis of the Colpitts oscillator and applications to design. IEEE Trans Circuits Syst I. –1999. –P. 1118–1130.

51. *Wegener C, Kennedy M.* RF chaotic Colpitts oscillator. In: Proc 3rd Workshop NDES'95, –Dublin, Ireland, –July –1995. P. 255–258.

52. *Kennedy M.* On the relationship between the chaotic Colpitts oscillator and Chua's oscillator. IEEE Trans Circuits Syst I –1995. –P. 376–379.

53. Matsumoto T. A Chaotic Attractor from Chua's Circuit / T.A. Matsumoto // IEEE Transactions on Circuits & Systems. –1984. – Vol. CAS–31, № 12. – P. 1055 – 1058.

54. Matsumoto T. Birth and death of the double scroll / T. Matsumoto, L.O. Chua, M. Komuro // Physica D. –1986. – Vol. 24, № 1-3. – P. 13 – 18.

55. Zhong G.Q. Experimental Confirmation of Chaos from Chua's Circuit / G.Q. Zhong, F. Ayrom // International Journal of Circuit Theory & Applications. – 1985, – Vol. 13, № 1. – P. 93 – 98.

56. Zhong G.Q. Periodicity and chaos in Chua's circuit / G.Q. Zhong, F. Ayrom // IEEE Transactions on Circuits & Systems. –1985. – Vol. CAS-32, № 5. – P. 501 – 503.

57. Bartissol P. The Double Hook (Nonlinear Chaotic Circuits) / P. Bartissol, L.O. Chua // IEEE Transactions on Circuits & Systems. –1988. – Vol. 35, № 12. – P. 1512 – 1522.

58. Senani R. Implementation of Chua's chaotic circuit using current feedback op-amps / R. Senani, S.S. `Gupta // Electronics Letters. –1988. – Vol. 34, № 9. – P. 829 – 830.

59. Lakshmanan M. Chaos in Nonlinear Oscillators. Controlling and Synchronization / M. Lakshmanan, K. Murali. // World Scientific Series on Nonlinear Science, Series A. –1996. – Vol. 13. –P. 12–42.

60. Matsumoto T. Hyperchaos: Laboratory experiment and numerical confirmation / T. Matsumoto, L.O. Chua & K. Kobayashi // IEEE Trans. Circuits Syst. –1986. – Vol. 33. –P. 1143 – 1147.

61. Thamilmaran K. Hyperchaos in a Modified Canonical Chua's Circuit / K. Thamilmaran, M. Lakshmanan, A. Venkatesan // Int. J. Bifurcation and Chaos. – 2004. – Vol. 14, № 1. – P. 221 – 243.

62. Bilotta E.A. Gallery of Chua Attractor//World Scientific Series on Nonlinear Science, Series A. –2008. – Vol. 61. –P. 23–86.

63. Fortuna L. Chua's Circuit Implementation. Yesterday, Today and Tomorrow / L. Fortuna, M. Frasca, M.M. Xibilia. //World Scientific Series on Nonlinear Science, Series A. –2009.– Vol. 65. –P. 52–62.

64. Yang T., Chua L. Chaotic digital multiply access (CDMA) communication systems // International Journal of Bifurcation and Chaos. Vol.7, No 12,1997. p.2789-2805.

65. Yang T., Chua L.O. Application of chaotic digital code-division multiply access (CDMA) to cable communication systems // Intern. J. Of Bifurcation and Chaos, Vol.8, No.8,1998.p. 1657-1669.

66. Yang T., Chua L Error performance of chaotic digital code-division multiply access (CDMA) systems // International Journal on Bifurcation and Chaos. Vol.8, №10, 1998. p.2047-2059.

67. Rovatti R., Setti G., Mazzini G. Chaotic complex spreading sequences for asynchronous DS-CDMA Part-II: Some theoretical performance bounds // IEEE Trans, on CAS-1, Vol. 45, No.4.p.496-506.

68. Еліяшів О. М. Модифікування генераторів детермінованого хаосу для систем оброблення та передавання інформації: автореф. дис. канд. техн. наук: 05.12.13 / Олег Миронович Еліяшів . – Львів, 2015 . – 20 с.

69. Максимов, Н.А. Однотранзисторный генератор полосовых хаотических сигналов радиодиапазона / Н.А Максимов, А.И. Панас // Зарубежная радиоэлек- троника. Успехи современной радиоэлектроники. – 2000. – № 11. – С. 61–68.

70. Дмитриев А.С., Иванов В.П., Лебедев М.Н. Модель транзисторного генератора с хаотической динамикой // Радиотехника и электроника. –1988. Т.33, №5. –С. 1085–1088.

71. Кальянов Э.В., Иванов В.П., Лебедев М.Н. Экспериментальное иследование транзисторного автогенератора с запаздывающей обратной связью//Радиотехника и электроника. –1982. –Т.27, №5. –С. 982–986.

72. Кузьмин Л.В., Максимов Н.А., Панас А.И. Прецезионный гнератор хаотических колебаний скусочно линейной характеристикой нелинейного элемента // Известия Вузов.Прикладная нелинейная динамика. –1999. –№2,3. – С. 81–94.

73. Namajunas A., Tamasevicius A.Modified Wien-bridge oscillator for chaos//Electronics letters. –1995. –Vol.31. –P. 355,366.

74. Newcomb R.W., Sakham S. An RC–operational amplifier chaos generator //Electronics Letters. –1995. –Vol.31. –P. 335–336.

75. Zhang J., Chen X., Davis A High frequency chaotic oscillations in a transformer-coupled oscillator // Proceeding of NDES'99.–Ronne, Denmark. –1999. – P. 213–216.

76. Zhang, L. et al. 640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser. Scientific Reports 7, Article number: 45900 2017.

77. Naruse M., Kim S.-J., Aono M., Hori H., Ohtsu M. Chaotic oscillation and random-number generation based on nanoscale optical-energy transfer. Sci. Rep. 4, Article number: 6039, 2014.

78. Ultrafast photonic reinforcement learning based on laser chaos / M.Naruse, Y. Terashima, A. Uchida, K. Song-Ju. // Scientific Reports. – 2017. – №7, Article number: 8772.

79. Кузнецов А. П., Кузнецов С. П. Критическая динамика одномерных отображений. Часть 2. Двухпараметрический переход к хаосу // Изв. Вузов "ПНД". т1. №3,4, 1993.С.17-34.

80. Шарковский А.Н. Сосуществование циклов непрерывного отображения прямой в себя // Укр. Матем.Ж. 1961. Т.13, №3. с.86.

81. Шарковский А.Н., Майстренко Ю.Л., Романенко Е.Ю. Разностные уравнения и их приложения. Киев.:Наукова Думка. 1986.-280с.

82. Неймарк Ю.И. Метод точечных отображений в теории нелинейных колебаний. М:Наука, 1972.-472с.

83. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – Москва - Санкт-Петербург - Киев: Вильямс, 2007. – 1104 с.

84. Горбенко И.Д., Горбенко Ю.И. Прикладная Криптология. – Харьков. Форт. – 2012, – С. 867.

85. Ruhkin A.A. (2010). Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22rev1a.

86. Ю.І. Горбенко Т.О. Гріненко, О.П. Нарєжній Аналіз статистичних властивостей апаратного генератора випадкових послідовностей Збірник наукових праць Харківського університету Повітряних Сил // 2015. Вип. 4(45). ст. 74-77.

87. Дослідження впливу параметрів генератора Голлманна на статистичні характеристики вихідного сигналу / М.М. Мандрона, В. М. Максимович, Ю.М. Костів, О. І. Гарасимчук. // Вісник КрНУ імені Михайла Остроградського. – 2013. – №4. – С. 98–103.

88. Lenore Blum, Manuel Blum, and Michael Shub. «A Simple Unpredictable Pseudo-Random Number Generator», SIAM Journal on Computing, volume 15, pages 364—383, May 1986.

89. Gotz M., Kelber K., Schwartz W. Discrete-time chaotic encryption systems - Part I: Statistical design approach // IEEE Trans, on CAS-1, Vol. 44, No. 10,1997.p.963-970.

90. Dachselt F., Kelber K., Schwarz W. Discrete-time chaotic encryption systems Part III: Cryptographicak analysis // IEEE Trans, on CAS-1, Vol. 45, No.9.p983-988.

91. Розроблення завадозахищених систем передавання інформації на основі псевдовипадкових коливань та фрактальних сигналів : дис. докт. техн. наук : 05.12.02 / . – Львів, 2016, 300 с.

92. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.

93. Zhang Xuefeng Extended Logistic Chaotic Sequence and Its Performance Analysis / Zhang Xuefeng, Fan Jiulun // Tsinghua science and technology. – 2007. - Volume 12, Number S1. - pp156-161.

94. Галюк С.Д., Генерування псевдовипадкових послідовностей на базі дискретних хаотичних систем / С.Д. Галюк, Л.Ф. Політанський // Міжнародна науково-практична конференція «PREDT-2014 ». – Чернівці: 23-25 жовтня 2014 р. – с. 85-86.

95. Чорний А.О. Періодичність розв'язків хаотичних систем при обчисленнях з фіксованою комою / А.О. Чорний, С.Д. Галюк. // Проблеми інформатики та комп'ютерної техніки: Праці IV-ї Міжнародної науково-практичної конференції, 26 – 29 травня 2015р.: тези доп. – Чернівці, 2015. – С. 157-158.

96. Васюта К.С. Новий поход ц оценке параметров хаотических сигналов, наблюдадаємих на фоне шума, с использованием "нелинейной динамической статистики" / К.С. Васюта// Проблеми телекомуникаций. 2010. - №1(1). – С. 109-114.

97. Васюта К.С. Классификация процесов в инфокомуникационних радиотехнических системах с применением BDS- статистики / К.С. Васюта// Проблеми телекомуникаций. 2012. - №4(9). – С. 63-71.

98. Васюта К.С. Использование BDS-статистики для оценки параметров одномерных отображений по наблюдению хаотического временного ряда / К.С. Васюта// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2009. - №2(19). – С. 66-70.

99. Alvarez G. Some basic cryptographic requirements for chaos-based cryptosystems / G. Alvarez, Li S.J. // International Journal of Bifurcation and Chaos. – 2006. - 16 (8). - pp. 2129-2151.

100. Yuan G. Collapsing of chaos in one dimensional maps / G. Yuan, J.A. Yorke // Physica D: Nonlinear Phenomena. – 2000. - №136. – pp. 18-30.

101. Zhang Xuefeng Extended Logistic Chaotic Sequence and Its Performance Analysis / Zhang Xuefeng, Fan Jiulun // Tsinghua science and technology. – 2007. - Volume 12, Number S1. - pp156-161.

102. Harris Bernard Probability Distributions Related to Random Mappings / Bernard Harris // Ann. Math. Statist. – 1960. - Volume 31, Number 4. pp. 1045-1062.

103. Celso Grebogi Roundoff-induced periodicity and the correlation dimension of chaotic attractors / Celso Grebogi, Edward Ott, and James A. Yorke // Phys. Rev. – 1988. - A 38, 3688.

104. IEEE, "IEEE standard Floating-Point Arithmetic," IEEE Std 754-2008, pp. 1-58, Aug., 2008.

105. Garasym, Oleg, Taralova Ina and Lozi René. Key requirements for the design of robust chaotic PRNG. 11th International Conference for Internet Technology and Secured Transactions (ICITST 2016), 2016.

106. Oleg Garasym, Ina Taralova, Ren´e Lozi. Application of observer-based chaotic synchronization and identifiability to original CSK model for secure information transmission. indian Journal of Industrial and Applied Mathematics, 2015, 6 (1), pp.1-26.

107. Oleg Garasym, Ren´e Lozi, Ina Taralova. Robust PRNG based on homogeneously distributed chaotic dynamics. Journal of Physics: Conference Series, IOP Publishing, 2016, NOMA'15 International Workshop on Nonlinear Maps and Applications, 692, pp.012001.

108. Oleg Garasym, Ren´e Lozi, Ina Taralova. Exploring some topologies of coupled chaotic networks. Elena Blokhina, Orla Feely. NOMA'15, International Workshop on Nonlinear Maps and their Applications, Jun 2015, Dublin, Ireland, 2016, pp. 34-39.

109. Andrea Espinel Rojas, Ina Taralova, Ren´e Lozi. New alternate ring-coupled map for multirandom number generation. Journal of Nonlinear Systems and Applications, 2013, 4 (1), pp.64- 69.

110. Chua L.O. Memristor -The missing circuit element / Chua L.O. // IEEE Trans. Circuit Th. – 1971. - CT-18, pp. 507–519.

111. Chua L.O. Memristive devices and systems / L.O. Chua, S.M. Kang // Proc. IEEE. -1976. - № 64, pp. 209–223.

112. Muthuswamy B. Simplest chaotic circuit / Bharathwaj Muthuswamy, Leon O . Chua // Int. J. of Bif. and Chaos. -2010. - Vol.20, №. 5, pp. 1567–1580.

113. Тратас Ю.Г. Применение методов статистической теории связи к задачам приема хаотических колебаний // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. - 1998. - №11. – С. 57-80.

114. Кириченко Л.О. Анализ и распознавание реализаций сигналов, обладающих фрактальными свойствами / Л.О. Кириченко, Ю.А. Кобицкая, Н.А. Дёмина // БИОНИКА ИНТЕЛЛЕКТА. – 2015. – № 1 (84). – С. 49–55.

115. Людмила Кириченко, Лариса Чалая Комплексный подход к исследованию фрактальных временных рядов / Л. Кириченко, Л. Чалая // International Journal "Information Technologies & Knowledge". – Volume 8, Number 1. – 2014. Pp. 22-28.

116. Eckman J. P. Recurrence Plots of Dynamical Systems / J. P. Eckman, S.O. Kamphorst, D. Ruelle // Europhys. Lett. – 1987. – № 4 (9). – Pp. 973–977.

117. Joseph S. Iwanski Recurrence plots of experimental data: To embed or not to embed? / Joseph S. Iwanski and Elizabeth Bradley // Chaos. – 1998. – V. № 8. – Pp. 861-871.

118. Norbert Marwan Recurrence plots for the analysis of complex systems / Norbert Marwan, M. Carmen Romano, Marco Thiel, Jürgen Kurths // Physics Reports – 2007. – V. № 438 (5–6). – Pp. 237–329.

119. Shiguo Lian, Jinsheng Sun, Zhiquan Wang, Security analysis of a chaos-based image encryption algorithm, Physica A: Statistical Mechanics and its Applications, Volume 351, Issues 2–4, 15 June 2005, Pages 645-661.

120. Ercan Solak, Cahit Çokal and Olcay Taner Yildiz. Cryptanalysis of fridrich's chaotic image encryption. International Journal of Bifurcation and Chaos, Vol. 20, No. 5 (2010) 1405–1413.

121. Fridrich J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. Inter. Journal of Bif. and Chaos, Vol. 8, No. 6 (1998) 1259–1284.

122. Warren W. S. Hacker’s Delight Second Edition / Warren Warren. – New York: Addison-Wesley Professional, 2012. – 512 с.

123. Alireza Jolfaei, Abdolrasoul Mirghadri, An image encryption approach using chaos and stream cipher/ Journal of Theoretical and Applied Information Technology, Vol 19. No. 2 – 2010.

124. Hubertus F. von Bremen, Firdaus E. Udwadia, Wlodek Proskurowski. An efficient QR based method for the computation of Lyapunov exponents/ Physica D 101 (1997) 1-16.

125. Yuting Xi Color image encryption based on multiple chaotic systems / Yuting Xi, Xing Zang, Ruisong Ye // Int. J. of network securiry & its applications. – 2016. – V. 8. – № 5. – Pp. 39-50.

ДОДАТОК А. Акти впровадження результатів дисертаційної роботи

Публічне акціонерне товариство «Укртелеком»

Вул.Героїв Майдану,7
м.Чернівці,58001, Україна
Тел.: +380 372 534790
Факс: +380 372 533209

укртелеком
краще починається сьогодні

№02/05-17/_____
від «04» вересня 2017 р.

Акт

використання результатів дисертаційної роботи

Круліковського Олега Валерійовича

на тему

“Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем”

Даний акт складений в тому, що нукові та практичні результати дисертаційної роботи Круліковського О. В. “Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем” використані на ПАТ “Укртелеком”, Чернівецька філія, м. Чернівці рекомендовані для формування цифрових хаотичних послідовностей на базі програмованих логічних мікросхем для передавання інформаційних сигналів у системах зв”язку.

Начальник ЦТП
ЧФ ПАТ “Укртелеком” Микитин В.О.

Публічне акціонерне товариство«Укртелеком»

Вул. Героїв Майдану,7, м. Чернівці, 58001, Україна
р/р 26008476573 в АТ «Райффайзен Банк Аваль» м. Київ, МФО 380805, код ЄДРПОУ 22838086,індивідуальний податковий номер 215607626656, свідоцтво № 200016523, видане 02.01.2012 СДПІ у м. Києві по роботі з ВПП

Акт

використання результатів дисертаційної роботи

Круліковського Олега Валерійовича

на тему

“Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем”

Даний акт складений в тому, що наукові та практичні результати дисертаційної роботи Круліковського О.В. “Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем” впровадженні в ОКБ “Рута”, м.Чернівці при дослідженні процесів формування хаотичних коливань на базі мемристивних структур.

Директор “ОКБ”Рута А.Д. Кіцак

ЗАТВЕРДЖЕНО

Проректор з наукової роботи
Чернівецького національного університету
імені Юрія Федьковича
_____ П.М. Фочук
"05" ____09____ 2017 р.

А К Т

Впровадження результатів науково-дослідної роботи

Круліковського Олега Валерійовича

"Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем" у навчальний процес Чернівецького національного університету імені Юрія Федьковича

Комісія у складі:

Голова: директор інституту фізико-технічних та комп'ютерних наук проф., д. ф.-м. н. Ангельський Олег В'ячеславович
(посада, прізвище, ім'я, по батькові)

Члени комісії: 1. Завідувач кафедри радіотехніки та інформаційної безпеки, проф., д. т. н. Політанський Леонід Францович
(посада, прізвище, ім'я, по батькові)

2. Доцент кафедри радіотехніки та інформаційної безрики, к. ф.-м. н. Кушнір Микола Ярославович
(посада, прізвище, ім'я, по батькові)

3. Асистент кафедри радіотехніки та інформаційної безпеки, к. т. н. Галюк Сергій Дмитрович
(посада, прізвище, ім'я, по батькові)

Комісія встановила, що наукові та практичні результати дисертаційної роботи "Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем" впроваджені в навчальних курсах «Генерування і формування сигналів» та «Цифрові пристрої та мікропроцесори» на кафедрі радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича.

Голова комісії: О.В. Ангельський

Члени комісії: Л.Ф. Політанський
М.Я. Кушнір
С.Д. Галюк

"5" вересня 2017 р.

ДОДАТОК Б. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Галюк С.Д. Аналіз часових рядів генерованих гіперхаотичною системою Тратаса / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 4(251). – С. 187-192.

2. Галюк С.Д.Порівняльний аналіз двомірних відображень для перестановок пікселів / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 1(245). – С. 214-220.

3. Krulikovskyi Oleh V. Image encryption algorithm based on chaotic maps / Oleh V. Krulikovskyi, Petro M. Shpatar, Leonid F. Politanskyi // Eastern European Scientific Journal. – 2014. – №6. – P. 362-366.

4. Круліковський О.В. Особливості вибору хаотичних систем для побудови генераторів псевдовипадкових послідовностей / О.В. Круліковський, С.Д. Галюк, Л.Ф. Політанський // Телекомунікаційні та інформаційні технології. – 2017. – №2. – С. 64-67.

5. Krulikovskyi O.V. Testing timeseries ring-coupled map generated by on FPGA / O.V. Krulokovskyi, S.D. Haliuk, L.F. Politanskyi // Телекомунікаційні та інформаційні технології. – 2016. – №4(53). – С. 24-29

6. Krulikovskyi O.V. PRNG based on modified tratas chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Сучасний захист інформації. – 2016. – №2. – С. 69-77.

Наукові праці, які засвідчують апробацію матеріалів дисертації (очна участь здобувача):

7. Corinto F. Memristor-based chaotic circuit for pseudo-random sequence generators / Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // Proceedings of the 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, April 18-20, 2016.

8. Haliuk S. Analysis of Pixels Permutations Based on Discretized Chirikov Map / Sergiy Haliuk, Oleg Krulikovskyi, Leonid Politanskyi // Proceedings of the XIIIth International Conference TCSET'2016, Lviv-Slavsko, Ukraine, February 23 – 26, 2016. – pp. 519-521.

9. Політанський Л.Ф. Циклічність послідовностей генерованих хаотичною системою / Л.Ф. Політанський, С.Д. Галюк, О.В. Круліковський // II Міжнародна конференція з інформаційно-телекомунікаційних технологій та радіоелектроніки УкрМіКо 2017. – м. Одеса,11-15 вересня 2017 р. – С. 545-548.

10. Krulikovskyi O. Development features of cryptographic means based on chaotic systems / Krulikovskyi Oleh, Haliuk Serhii // Proceeding of the Vth International Scientific Practical Conference "PREDT 2016", 3–5 November, 2016, Chernivtsi, Ukraine. - P.125.

11. Krulikovskyi O.V. Using PRNG based on multidimensional discrete hyperchaotic system for image encryption / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // IV Міжнародна науково-практична конференція «Напівпровідникові матеріали, інформаційні технології та фотовольтаїка»: тези доповідей, 26-28 травня 2016 р., м. Кременчуг. – С. 234-235.

12. Krulikovskyi O.V. PRNG based on discrete hyper chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Проблеми інформатики та комп'ютерної техніки: Праці V-ї Міжнародної науково-практичної конференції ПІКТ – 2016, Чернівці, Україна, 21 – 24 травня, 2016. – С. 204.

13. Image encryption algorithm based on one-dimensional and two-dimensional maps / M.Ya. Kushnir, G.V. Kosovan, O.V. Krulikovskyi // II International Scientific-Practical Conferences "PREDT -2012". – Chernivtsi, 2012. – p. 90-91.

14. Encryption algorithm based on two-dimensional standard map / O.V. Krulikovskyi, L. F. Politanskyi // IV International Scientific- Practical Conferences "PREDT -2014". – Chernivtsi, 2014. – pp. 68-69.

15. Круліковський О.В. Рекурентний аналіз багатовимірних хаотичних систем / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Міжнародна науково-практична конференція "ОСНП - 2017" – м. Черкаси, 24-26 травня 2017 р.