Праці Одеського політехнічного університету, 2025. Вип. 2(72)
ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

UDC 004.056

V. Khamitov,
S. Antoshchuk. DSc, Prof.
Odessa Polytechnic National University, Shevchenko Ave. 1, Odesa, Ukraine, 65044, e-mail: asg@op.edu.ua

APPLICATION OF NONLINEAR DISCRETE MAPS TO CONSTRUCT PSEUDO-CHAOTIC CRYPTOSYSTEMS

В. Хамітов, С. Антощук. **Використання нелінійних дискретних відображень для побудування псевдохаотичних криптосистем**. Стаття присвячена використанню нелінійних дискретних динамічних систем у комп'ютерній криптографії. Основою багатьох потокових схем шифрування є псевдохаотичні послідовності, що генеруються за допомогою деякої обраної траєкторії дискретної динамічної системи. Основна проблема використання псевдохаотичних динамічних систем у комп'ютерних обчисленнях полягає в тому, що кількість різноманітних станів у комп'ютері скінчено, отже, кожна побудована траєкторія є періодичною, причому довжина періоду може бути невеликою. Крім того, різні платформи (апаратні та програмні) використовують різні алгоритми обчислення математичних функцій та зберігають проміжні результати з різною точністю, тому результати, отримані на різних платформах, можуть суттєво відрізнятися. Для подолання зазначених проблем пропонується використати нову динамічну систему, а саме узагальнене відображення Тент з керуванням, яке стабілізує цикли заданої довжини. Ці цикли залежать від параметрів системи та початкового значення; ці величини є коротким ключем для генерації довгої псевдохаотичної послідовності. У статті наводиться найпростіший статистичний аналіз перевірки некорелювання ключової послідовності, а також графічний тест. Експерименти показують відсутність значної кореляції. Також досліджено чутливість елементів ключової послідовності до варіації параметрів ключа. Як приклад роботи алгоритму розглянуто завдання шифрування зображень.

Ключові слова: псевдохаотичні послідовності, шифрування зображень, криптосистеми, захист інформації від несанкціонованого доступу, апаратно-програмна платформа, статистичний аналіз, дискретні динамічні системи, нестійкі періодичні орбіти, стабілізація періодичних орбіт

V. Khamitov, S. Antoshchuk. **Application of nonlinear discrete maps to construct pseudo-chaotic cryptosystems**. The article is devoted to the application of nonlinear discrete dynamical systems in computer cryptography. The basis of many stream encryption schemes is pseudo-chaotic sequences, which are generated using a certain selected trajectory of a discrete dynamical system. The main problem with using pseudo-chaotic dynamical systems in computer calculations is that the number of all possible states in a computer is finite, therefore, every constructed trajectory is periodic, and the period length can be small. In addition, different platforms (hardware and software) use different algorithms for calculating mathematical functions and store intermediate results with different precision, so the results obtained on different platforms can differ significantly. To overcome these problems, it is proposed to use a new dynamical system, namely the generalized Tent map with control, which stabilizes cycles of a given length. These cycles depend on the system parameters and the initial value; these values are a short key (seed) for generating a long pseudo-chaotic sequence. The article provides a simple statistical analysis to check the uncorrelation of the key sequence, as well as a graphical test. The experiments show the absence of significant correlation. The sensitivity of the elements of the key sequence to the variation of the key parameters was also investigated. As an example of the algorithm's operation, the problem of image encryption is considered.

Keywords: pseudo-chaotic sequences, image encryption, cryptosystems, protection of information from unauthorized access, hardware-software platform, statistical analysis, discrete dynamical systems, unstable periodic orbits, stabilization of periodic orbits

Introduction

One of the main problems of digital data processing is the problem of unauthorized access to information. To protect data in a digital environment, cryptographic methods are used. Cryptographic transformations can be conditionally divided into two types: classical methods or alphabetic ciphers, and arithmetic transformations, in which transformation operations occur on the bit (decimal) representation of data. In modern cryptography, methods of the second type are used. Symmetric and asymmetric encryption schemes are distinguished. Another well-known classification distinguishes between block and stream ciphers. A stream cipher converts a stream of text characters into a stream of ciphertext, and the transformation depends on the state of the system. Identical text characters will be encrypted into different ciphertext characters. There is extensive literature on various aspects of cryptography, for example, [1, 2, 3].

Many stream encryption schemes can be viewed from the point of view of nonlinear dynamics. A feature of these schemes is the use of the values of a certain selected trajectory of a discrete dynamical system, i.e., constructed for some given initial conditions and system parameters. A similar way can be used to obtain a sequence of decimal digits or a bit sequence. This sequence is then used as a key to transform the original sequence (the source message) into an encrypted one (ciphertext). The process is

DOI: 10.15276/opu.2.72.2025.19

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

carried out by linear operations modulo (for example, two or ten) of the elements of the source and key sequences. The simplest stream cipher is the Vernam cipher [4].

A stream encryption scheme is considered secure if the key sequence is truly random and its length is equal to the length of the original message [5]. However, in practice, it is difficult to generate and transmit such keys. Instead, pseudo-random (pseudo-chaotic) sequences are used, generated by some deterministic generator from a short key (seed), using a discrete dynamical system [6-9].

However, at the stage of modeling dynamical systems on modern computers, fundamental problems arise. For example, in [10] it is noted that computer calculations necessarily require additional special confirmation of the results. The main computational problem is that in computers, numbers are stored in registers and memory cells with a limited number of bits, as a result of which the system of real numbers representable in a machine is discrete and finite. To trace what consequences may arise as a result of this, let's consider the simplest example of calculating an iterated sequence using the standard Tent function $f(x) = 2(1/2 - |x - 1/2|)$ in the EXEL software environment. Let's choose the starting point $x_0 = 2/3$. Then theoretically it should be $f^{(k)}(x_0) = x_0$, $k = 1, 2, \ldots$ (here and below the notation $f^{(1)}(x) = f(x)$, $f^{(k}(x) = f(^{(k-1)}(x))$ is used). However, the calculations give different results: $f^{(53)}(x_0) = 1$, $f^{(54)}(x_0) = 0$. One can choose other initial values for x_0, and again we will get $f^{(54)}(x_0) = 0$. The reason for such incorrect calculations is explained by the fact that a number from the interval $[0, 1]$ is represented in a computer in the binary number system by a finite sum of numbers of the form $\alpha_j / 2^j$ ($\alpha_j \in \{0,1\}$), i.e., they are binary-rational numbers, it is equal to $A/2^m$ (A is an integer and $0 \le A \le 2^m$). The number m is called the order. But then $f(A/2^m) = A_1/2^{m-1}$ (A_1 is an integer and $0 \le A_1 \le 2^{m-1}$), $f^{(2)}(A/2^m) = A_2/2^{m-2}$, … , $f^{(m+1)}(A/2^m) = 0$. On computers where the iterated sequence was calculated, the maximum order was 53.

Let's turn again to the Tent map. We will carry out the calculations in the MAPLE package with a decimal representation with the value of the variable *Digits*:=25. We generate the sequences $\{x_k = f^{(k)}(x_0)\}$, $\{y_k = f^{(k)}(y_0)\}$, $k = 1, 2, \ldots$, where $x_0 = 1/1001$, $y_0 = evalf(1/1001)$, and construct the sequence $\{x_k - y_k\}$. It can be seen that, starting from the 80th step, the behavior of this sequence is quasi-chaotic.

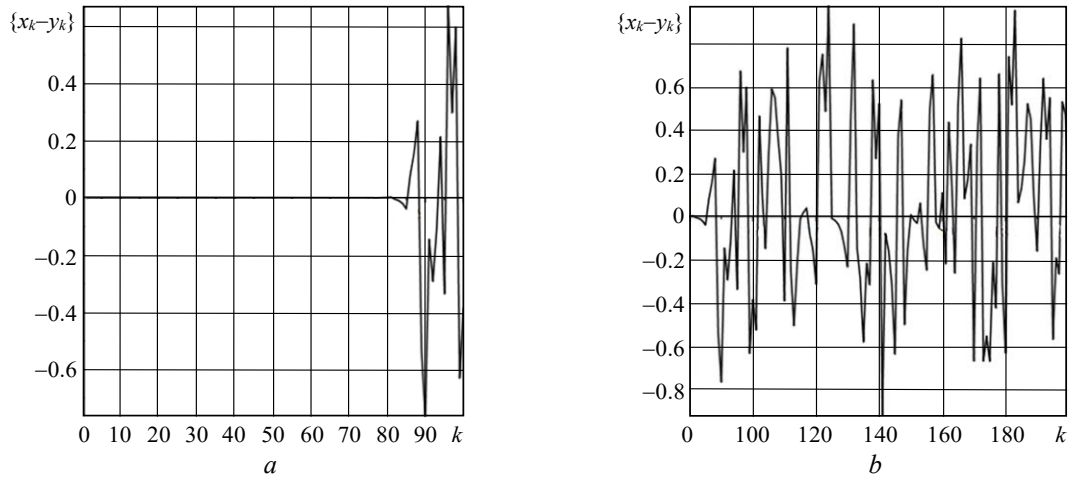


Fig. 1. Graphical representation of the sequence $\{x_k - y_k\}$: *a* – *for* $k = 1, \ldots, 100$; *b* – *for* $k = 80, \ldots, 200$

Similar examples can be constructed further. However, the examples given above clearly show that a researcher can never be sure of the correctness of calculations performed on a computer. That is, to the question of *R. Lozi* [10] (about trust in numerical results), the answer is,

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

unfortunately, negative. This once again proves the need to develop mathematical methods that allow correcting computer calculations.

Another problem may arise when the orbit of a discrete dynamical system becomes cyclic, and the cycle length turns out to be quite small, for example, due to an unsuccessfully chosen initial value. It is also possible that as a result of rounding values, the trajectory will become cyclic, again, with a small cycle length. The point here is that the variables that determine the state of the system can have close, but not equal values; and when rounded, the chaotic behavior ceases. In these cases, it is impossible to construct a correct key sequence.

The next problem is related to the fact that different platforms (hardware and software) use different algorithms for calculating mathematical functions and store intermediate results with different precision. Since chaotic generators are extremely sensitive to precision and error, it is very likely that the same encryption algorithms implemented on different platforms will lead to different results.

Thus, the property of chaoticity of dynamical systems turns out to be dual: on the one hand, it provides the properties of confusion and diffusion absolutely necessary for cryptography (relative to the text and the key) [11], on the other hand, it causes inconvenience of use associated with high sensitivity to disturbances and rounding.

The purpose of this article is to construct a new discrete dynamical system with which you can generate long pseudo-chaotic sequences; in this case, the system parameters and initial values are used as a seed (key). Requirements for the seed: the seed should consist of a small number of elements. Requirements for the algorithm: the algorithm should not depend on the hardware and software.

Literature Review

A significant number of works are devoted to the use of chaotic systems in cryptanalysis, for example, [12 – 15]. The importance of the problem of the performance of chaotic cryptosystems is noted [17, 18, 19]. Discrete dynamic systems of small dimensions have obvious advantages over high-dimensional systems: these systems are easier to implement in software, and the time costs for generating a pseudo-chaotic sequence are less, which allows encrypting large amounts of data in real time [20]. Therefore, the development of effective models of one-dimensional discrete chaotic systems for constructing encryption algorithms is an actual task [21, 22, 23].

Preliminary results

The mathematical basis for constructing new algorithms for generating pseudo-chaotic cryptosystems is the one-dimensional Tent mapping with additional predictive control.

Following [24], let's consider a nonlinear equation with discrete time:

$$x_{n+1} = f(x_n), \quad n = 1, 2, \dots , \tag{1}$$

where:

$$f(x) = H(1/2 - |x - 1/2|) = \begin{cases} H\,x, x \le 1/2; \\ H(1-x), x > 1/2, \end{cases} \tag{2}$$

$x \in (-\infty, +\infty)$, $H \ge 2$.

The map (2) is called the generalized Tent map.

A set U is called invariant for equation (1) if for any $x_0 \in U$ it follows that $f^{(k)}(x_0) \in U$, $k = 1, 2, \dots$. It can be shown that for $H > 2$ in equation (1) the invariant set will be a *Cantor*-type set: closed, continuum power, with zero *Lebesgue* measure. Note that each point of the invariant set is representable in the form $\sum_{j=1}^{\infty} \frac{\alpha_j}{H^j}$, where $\alpha_j \in \{0, H-1\}$. This set includes a countable subset of all periodic points of the map (2). If x_0 does not belong to the invariant set, then

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

the corresponding sequence $\{f^{(k)}(x_0)\}_{k=1}^{\infty}$ tends to $-\infty$. Such invariant sets are called repellers of the map (2).

The set $\{\eta_1, \dots, \eta_T\}$ is called a T - cycle of the map (2) if the numbers $\eta_1, \dots, \eta_T$ are different and $\eta_{j+1} = f(\eta_j)$, $j = 1, \dots, T-1$, $\eta_1 = f(\eta_T)$, while each point of the T – cycle is called a T – periodic point. The multiplier of the cycle of equation (1) is determined by the formula $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$, i.e. $\mu = \pm H^T$.

As is known [25], the local asymptotic stability of a cycle is determined by the condition (sufficient): the multiplier in absolute value is less than one. Since $|\mu| = H^T > 1$, any cycle of equation (1) is unstable. In addition, if $H > 2$, then for almost any initial point, the corresponding trajectory goes to infinity.

Along with equation (1), let's consider the equation:

$$x_{n+1} = F(x_n), \quad n = 1, 2, \dots, \tag{3}$$

where: $F(x) = f(\vartheta x + (1-\vartheta) f^{(T)}(x))$, ϑ – is some real number, called the control parameter and subject to determination. Equation (3) is called the control system for equation (1). Let $\{\eta_1, \dots, \eta_T\}$ be a cycle of equation (1).

Since $\vartheta \eta_k + (1-\vartheta) f^{(T)}(\eta_k) = \eta_k$, then $F(\eta_k) = f(\eta_k)$, this means that the cycle of equation (1) will also be a cycle of equation (3). Note that the converse is not true in the general case.

The multiplier λ of this same cycle $\{\eta_1, \dots, \eta_T\}$ but for equation (3) can be found from [26]:

$$\lambda = \mu(\vartheta + (1-\vartheta)\mu)^T.$$

Two cases are possible: $\mu > 0$ and $\mu < 0$. The condition for local asymptotic stability of a T - cycle of equation (3) for $\mu = H^T$: $|\lambda| = \left|H^T (\vartheta + (1-\vartheta) H^T)^T\right| < 1$, whence:

$$\frac{H^T - \frac{1}{H}}{H^T - 1} < \vartheta < \frac{H^T + \frac{1}{H}}{H^T - 1}. \tag{4}$$

If $\mu = -H^T$, then the condition for local asymptotic stability of the cycle of equation (5): $|\lambda| = \left|H^T (\vartheta - (1-\vartheta) H^T)^T\right| < 1$, whence:

$$\frac{H^T - \frac{1}{H}}{H^T + 1} < \vartheta < \frac{H^T + \frac{1}{H}}{H^T + 1}. \tag{5}$$

***Theorem* 1** [24]. If inequalities (4) are satisfied, then any solution of equation (3) is bounded (i.e., for any initial point $x_0 \in (-\infty, +\infty)$ the corresponding trajectory is bounded). Moreover, any T – cycle $\{\eta_1, \dots, \eta_T\}$ of this equation, for which the value $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$ is positive, is locally asymptotically stable.

***Theorem* 2** [24]. If inequalities (5) are satisfied, then the set $[0, H/2]$ is an invariant set of equation (1) (i.e., for any initial point the corresponding trajectory is bounded by the values 0 and $H/2$). Moreover, any T – cycle $\{\eta_1, \dots, \eta_T\}$ of this equation, for which the value $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$ is negative, is locally asymptotically stable.

Main result

To generate a pseudo-chaotic sequence, it is proposed to use a dynamical system (3), in which ϑ satisfies condition (4) or (5). In this case, the sequence itself is determined through the T periodic points $\{\eta_1, \dots, \eta_T\}$. Here T – is a sufficiently large number. In order to exclude

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

short subcycles, the number T must be taken to be simple. In total, there are $\frac{2^{T-1}-1}{T}$ cycles of length T, i.e., for sufficiently large lengths T the total number of cycles will be very large (exponential growth in T), i.e., the probability of guessing a specific cycle that is realized is negligible. Due to the chaotic nature of the dynamical system (1), a long cycle will be practically indistinguishable from an arbitrary bounded non-cyclic trajectory. Note, however, that in practice for $H > 2$ any trajectory of equation (1) will go to infinity due to rounding of results. Fig. 2 shows typical T - periodic trajectories of equation (1) for $T = 223$, $H = 2.070801$, $x_0 = 0.9$.

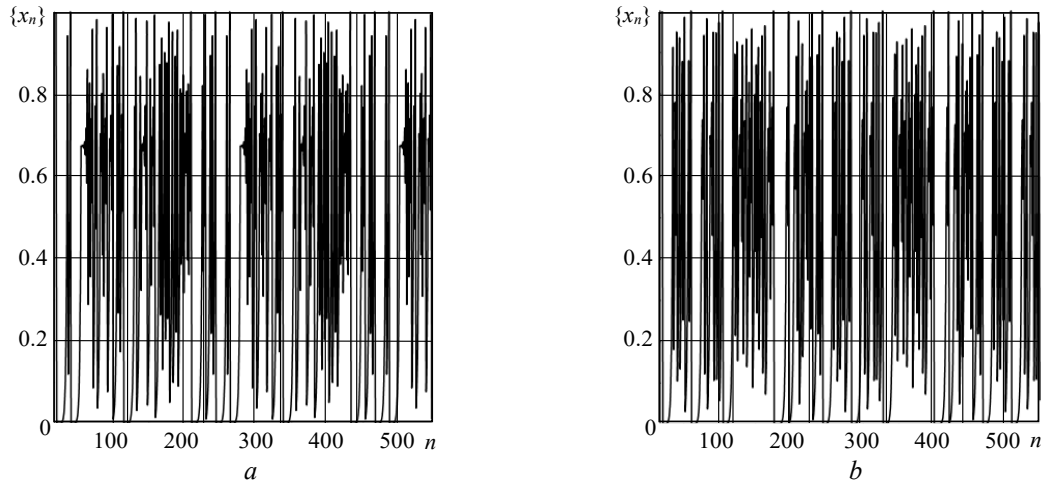


Fig. 2. T – periodic trajectories of equation (1) for $T = 223$, $H = 2.070801$, $x_0 = 0.9$: a – the value $\mu = f'(\eta_T)\cdot\ldots\cdot f'(\eta_1)$ is negative; b – the value $\mu = f'(\eta_T)\cdot\ldots\cdot f'(\eta_1)$ is positive

For things to work practically, you need to use equation (3). Then the found cycle will depend on the initial point $x_0 \in (0,1)$, on the number T and on the parameters H and ϑ, which may contain a sufficient number of decimal places. Such a complex dependence will in fact make the cycle parameters non-obvious for a cryptanalyst.

This cycle is locally asymptotically stable. This means that the resulting trajectory does not depend on minor disturbances, inaccuracies in calculations and rounding. Moreover, one can expect that for different but close values of x_0, T, H, ϑ different cycles will be obtained on the same computers. The main question is the speed of convergence (i.e., the number of correct decimal places). Roughly speaking, this speed must be sufficient for the length of the cycle. Experiments show [24] that the accuracy should be chosen at least $1.05 \cdot T \lg(H)$.

However, the sequence $\{\eta_1, \ldots, \eta_T\}$ is not pseudo-random –the order of elements is fully determined. So an extra trick is needed. The point is that as a result of the calculation, we need to guarantee q correct decimal places in the cycle $\{\eta_1, \ldots, \eta_T\}$, where q denotes the number of decimal places. In this case, we have $T \cdot q$ decimal digits, from which we can build a pseudo-chaotic sequence. For example, in the following way: let's take the numbers T_0, T_1, and computational precision should be taken $q = T_1 + 2T_0$ $(T_1 + 2T_0 > 1.05 \cdot T \lg(H))$.For each number η_j take decimal digits of the fractional part starting from digit number $T_0 + 1$, ending with number $T_1 + T_0$. Denote these sets $\{\eta_{j1}, \ldots, \eta_{jT_1}\}$, $j = 1, \ldots, T$. For the formation of the key sequence, we obtained $T \cdot T_1$ decimal digits. The key sequence itself can have, for example, the form:

$$I_1 = \{\eta_{11}, \eta_{12}, \ldots, \eta_{1T_1}, \eta_{21}, \ldots, \eta_{2T_1}, \ldots, \eta_{T1}, \ldots, \eta_{TT_1}\} \quad (6)$$

or

$$I_2 = \{\eta_{11}, \eta_{21} \ldots, \eta_{T1}, \eta_{12}, \ldots, \eta_{T2}, \ldots, \eta_{1T_1}, \ldots, \eta_{TT_1}\}. \quad (7)$$

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

You can form the sequence in other ways.

Choice of key parameters

The seed for generating a pseudo-chaotic sequence is the key $Key = [T, H, \pm\alpha, x_0]$. Here the numbers α or $-\alpha$ are used to calculate the control parameter $\vartheta = \dfrac{H^T + \alpha\dfrac{1}{H}}{H^T - 1}$ or $\vartheta = \dfrac{H^T - \alpha\dfrac{1}{H}}{H^T + 1}$ respectively.

The closer α is to zero, the closer the cycle multiplier is to zero, the faster the initial point will be attracted to this cycle. Therefore, it is advisable to take $0 < \alpha < 0.005$. Practical experiments show that with such α , the initial point falls into the cycle in no more than 20 iterations. This means that the number T_0 in the formula $q = T_1 + 2T_0$ can be taken equal to 20. In this case, the number T_1 can be taken simply equal to T. The period T must be a prime number in the range between 100 and 500. Large numbers lead to a sharp increase in calculation time. The initial point x_0 must be chosen from the interval $(0, 1)$.

Periodic trajectories are sensitive to changes in key parameters. Let's take, for example, $x_0 = 0.9$, $T = 223$, $\vartheta = \dfrac{H^T + 0.001 \cdot 1/H}{H^T - 1}$, $H \in \{2.070801, 2.0708011\}$, i.e. $Key = [223, \{2.070801, 2.0708011\}, 0.001, 0.9]$. Let's calculate the two corresponding periodic trajectories and their difference z_n. Let's plot the resulting trajectory in Fig. 3.

Due to the high sensitivity, the parameter H can be chosen quite close to two, for example, $H \in (0, 2.2)$, and the whole uncertainty can be put into the following significant decimal places.

Let's take the key: $Key = [223, 2.0708011, \{0.001, -0.001\}, 0.9]$. Let's calculate the two corresponding periodic trajectories and their difference z_n. Let's plot the resulting trajectory in Fig. 4.

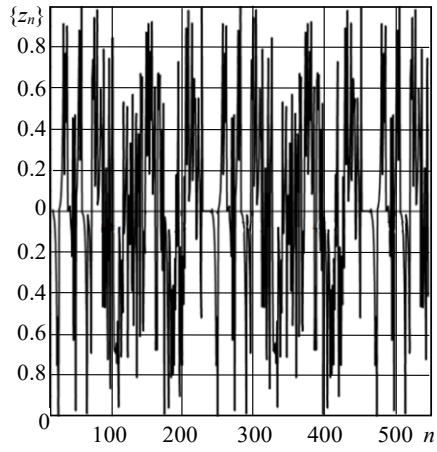


Fig. 3. The difference of two T – periodic trajectories of equation (3) for $Key = [223, \{2.070801, 2.0708011\}, 0.001, 0.9]$

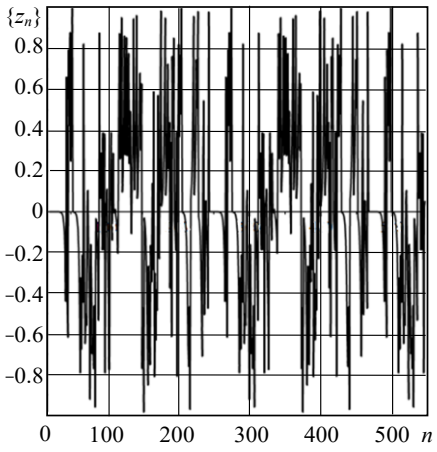


Fig. 4. The difference of two T – periodic trajectories of equation (3) for $Key = [223, 2.0708011, \{0.001, -0.001\}, 0.9]$

Similarly, we construct the difference of trajectories for $Key = [223, 2.0708011, \{0.001, 0.0011\}, 0.9]$ (Fig.5), $Key = [223, 2.0708011, 0.001, \{0.9, 0.9001\}]$ (Fig.6)

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

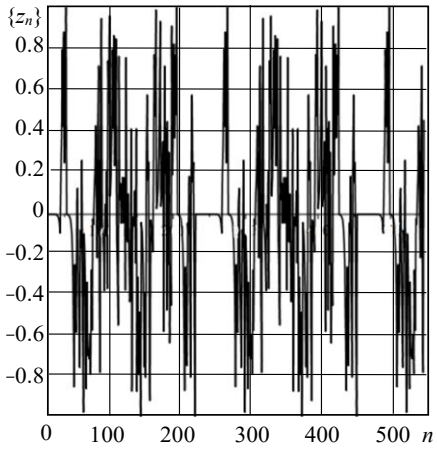


Fig. 5. The difference of two T – periodic trajectories of equation (3) for $Key = [223,\ 2.0708011, \{0.001, 0.0011\}, 0.9]$

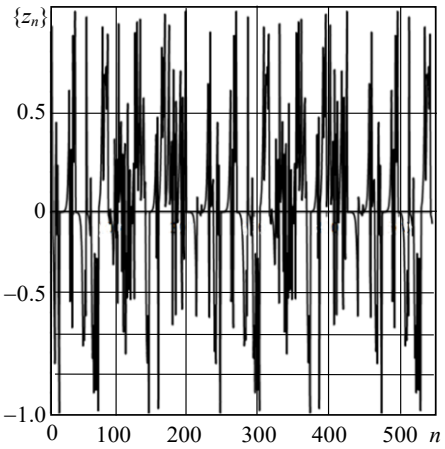
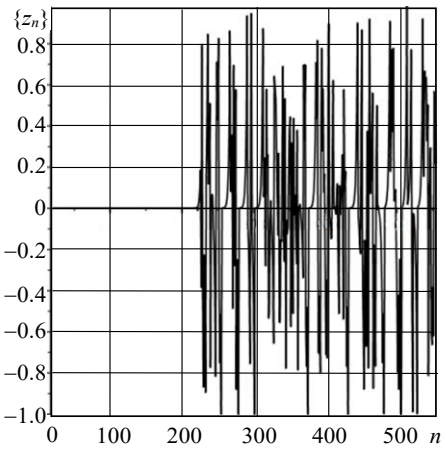
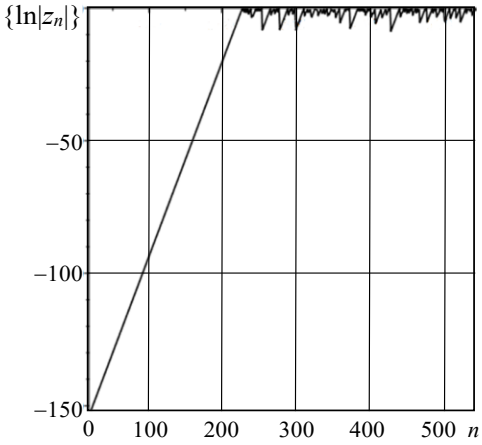


Fig. 6. The difference of two T – periodic trajectories of equation (3) for $Key = [223, 2.0708011, 0.001, \{0.9, 0.9001\}]$

Let's consider the sensitivity of the key sequence to the parameter T (period), i.e., let's calculate two corresponding periodic trajectories x_n and y_n (constructed for $T = 223$ and $T = 227$ respectively) and their difference z_n for the key: $Key = [\{223, 227\}, 2.0708011, 0.001, 0.9]$. Let's plot the resulting trajectory in Fig. 7-*a*). In Fig. 7-*b*) we plot the points of the sequence $\{\ln(|z_n|)\}$.



a



b

Fig. 7. The difference of two periodic trajectories of equation (3) for $Key = [\{223, 227\}, 2.0708011, 0.001, 0.9]$: *a* – the sequence $\{z_n\}$; *b* – the sequence $\{\ln(|z_n|)\}$

Analysis of the results shows that for $n < 210$ the values of the two trajectories x_n and y_n are close to each other, in particular $|z_n| < 10^{-50}$ for $n < 74$. For $230 < n < 440$ the values x_n and y_{n+4} will be close; further, for $460 < n < 670$ the values x_n and y_{n+8}, will be close, and so on. Conclusion: variation of the parameter T does not give the necessary divergence of the key sequences.

The essential parameters of the key are the values H, α, x_0. If these parameters are determined by at least ten decimal places, then the number of all possible variants of the keys will be of the order of 10^{30}, i.e., about 100 bits. If necessary, you can increase the cryptographic strength of the algorithm by using several keys in series.

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

Statistical analysis

Let's investigate some statistical characteristics of pseudo-chaotic sequences (6) and (7) for the $Key = [223, 2.070811, 0.001, 0.9]$. Let's construct a histogram and determine the mean and standard deviation. Let's start with sequence (6). The sequence contains T^2 elements. In our case, 49729 elements. The mean is $S = 4.4795...$, which deviates insignificantly from the theoretical mean of 4.5 of a uniformly distributed discrete random variable. The standard deviation is the theoretical one is 2.8722... Let's construct histograms for the first 1000 elements of the sequence, for elements with numbers from 2000 to 3000, for all elements (Fig. 8).

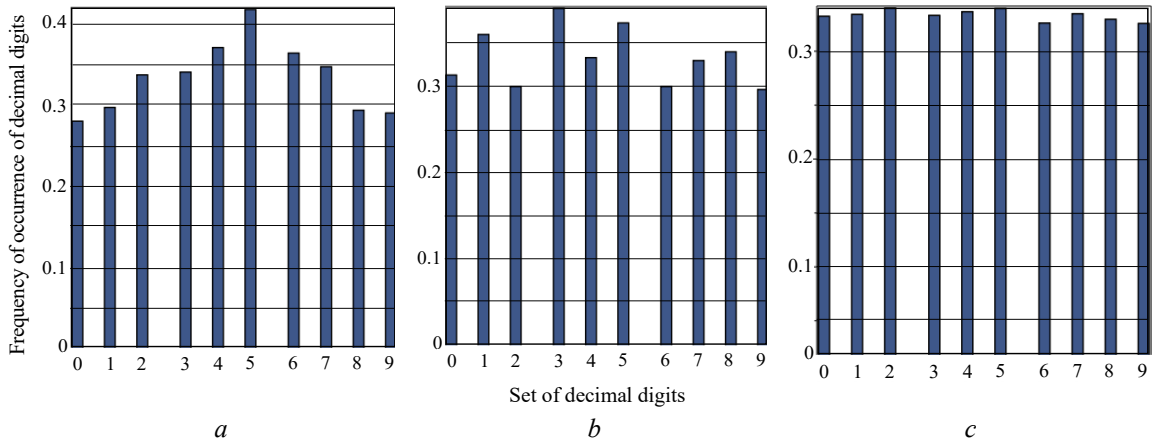


Fig. 8. Histogram for the sequence: $a - [\mathrm{I}_1[j]: j = 1..1000]$; $b - [\mathrm{I}_1[j]: j = 2000..3000]$; $c - [\mathrm{I}_1[j]: j = 1..49729]$, constructed for $T = 223$, $H = 2.0708011$, $\vartheta = \dfrac{H^T + 0.001 \cdot 1/H}{H^T - 1}$, $x_0 = 0.9$

We see that individual sections of the sequence do not have a strictly uniform distribution, although their distributions are close to uniform.

For further analysis of the properties of the sequence $[\mathrm{I}_1[j]: j = 1..49729]$ let's define three quantities: the cumulative mean $\overline{\mathrm{I}}_1(k) = \dfrac{1}{k}\sum_{j=1}^{k} \mathrm{I}_1[j]$, $k = 1, \ldots, T^2$; the cumulative standard deviation $\delta_1(k) = \dfrac{1}{k-1}\sum_{j=1}^{k} (\mathrm{I}_1[j] - \overline{\mathrm{I}}_1(k))^2$; the cumulative variance $\sigma_1(k) = \sqrt{\delta_1(k)}$, $k = 2, \ldots, T^2$. It is clear that the usual sample mean is equal to $\overline{\mathrm{I}}_1(T^2)$, and the sample variance is $\sigma_1(T^2)$.

To construct graphs of the cumulative mean and variance, we derive recurrent formulas for these quantities. Since $\overline{\mathrm{I}}_1(k) = \dfrac{k-1}{k}\dfrac{1}{k-1}\sum_{j=1}^{k-1} \mathrm{I}_1[j] + \dfrac{1}{k}\mathrm{I}_1[k]$, then

$$\overline{\mathrm{I}}_1(k) = \frac{k-1}{k}\overline{\mathrm{I}}_1(k-1) + \frac{1}{k}\mathrm{I}_1[k], \ \overline{\mathrm{I}}_1(1) = \mathrm{I}_1[1]. \tag{8}$$

Further, $(\mathrm{I}_1[j] - \overline{\mathrm{I}}_1(k))^2 = (\mathrm{I}_1[j])^2 - 2\mathrm{I}_1[j]\overline{\mathrm{I}}_1(k) + (\overline{\mathrm{I}}_1(k))^2$, whence

$$\delta_1(k) = \frac{1}{k-1}\sum_{j=1}^{k} (\mathrm{I}_1[j])^2 - \frac{2}{k-1}\overline{\mathrm{I}}_1(k)\sum_{j=1}^{k} \mathrm{I}_1[j] + \frac{k}{k-1}(\overline{\mathrm{I}}_1(k))^2 = \frac{1}{k-1}\sum_{j=1}^{k} (\mathrm{I}_1[j])^2 - \frac{k}{k-1}(\overline{\mathrm{I}}_1(k))^2.$$

Let's denote:

$$\overline{\mathrm{I}}_1^{(2)}(k) = \frac{1}{k-1}\sum_{i=1}^{k} (\mathrm{I}_1[j])^2,$$

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

then $\overline{\mathrm{I}}_1^{(2)}(k)=\frac{k-2}{k-1}\frac{1}{k-2}\sum_{j=1}^{k-1}(\mathrm{I}_1[j])^2+\frac{1}{k-1}(\mathrm{I}_1[k])^2=\frac{k-2}{k-1}\overline{\mathrm{I}}_1^{(2)}(k-1)+\frac{1}{k-1}(\mathrm{I}_1[k])^2$. Thus, the following recursive relation is valid:

$$\begin{cases}\delta_1(k)=\overline{\mathrm{I}}_1^{(2)}(k)-\frac{k}{k-1}(\overline{\mathrm{I}}_1(k))^2;\\ \overline{\mathrm{I}}_1^{(2)}(k)=\frac{k-2}{k-1}\overline{\mathrm{I}}_1^{(2)}(k-1)+\frac{1}{k-1}(\mathrm{I}_1[k])^2.\end{cases} \tag{9}$$

In this case, $k=3,\dots,N$, and $\overline{\mathrm{I}}_1^{(2)}(2)=(\mathrm{I}_1[1])^2+(\mathrm{I}_1[2])^2$.

The graphs of the quantities $\{\overline{\mathrm{I}}_1(j)\}_{j=1}^{500}$, $\left\{\overline{\mathrm{I}}_1(j)\right\}_{j=1}^{T^2}$ are shown in Fig. 9. The graphs of the quantities $\left\{\sigma_1(j)\right\}_{j=1}^{500}$, $\{\sigma_1(j)\}_{j=1}^{T^2}$ are shown in Fig. 10.

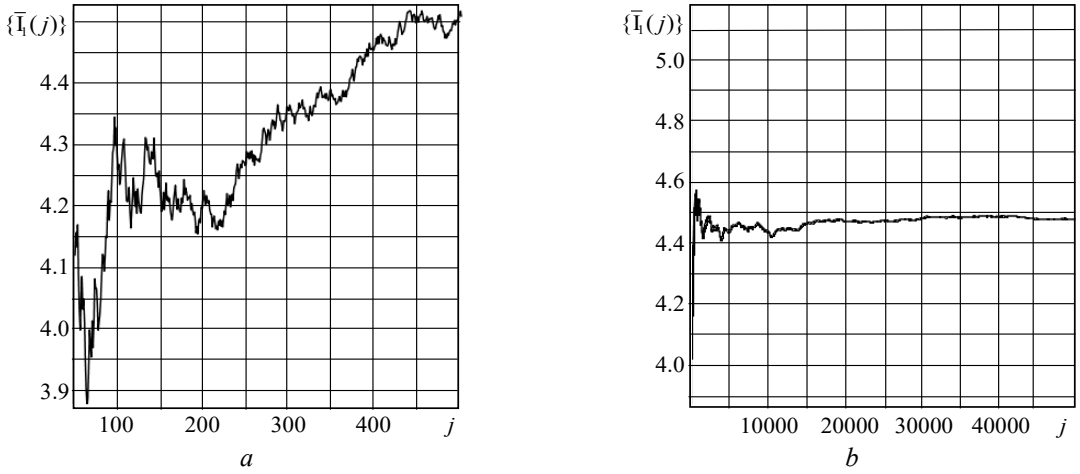


Fig. 9. Graphs of the quantities: *a* – $\{\overline{\mathrm{I}}_1(j)\}_{j=1}^{500}$; *b* – $\{\overline{\mathrm{I}}_1(j)\}_{j=1}^{T^2}$

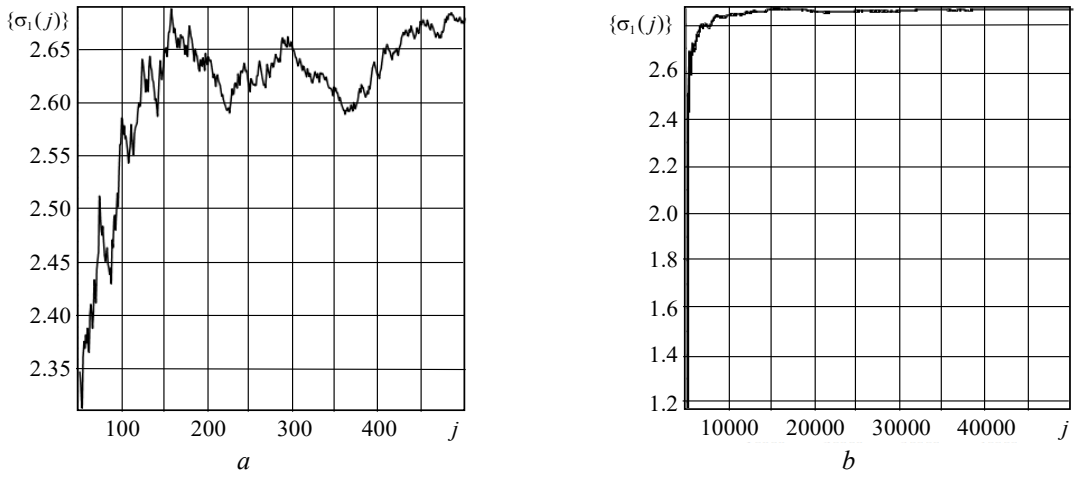


Fig. 10. Graphs of the quantities: *a* – $\{\sigma_1(j)\}_{j=1}^{500}$; *b* – $\{\sigma_1(j)\}_{j=1}^{T^2}$

The absence of periodicity in the behavior of the graphs of the cumulative mean and variance indicates the absence of regularities between individual parts of the sequence, which may indicate its pseudo-stochastic nature.

Let's carry out a similar analysis for sequence (7). In this case, we note that in formulas (8), (9) the index 1 must be replaced by 2. The corresponding graphs are given below (Fig. 11–13).

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

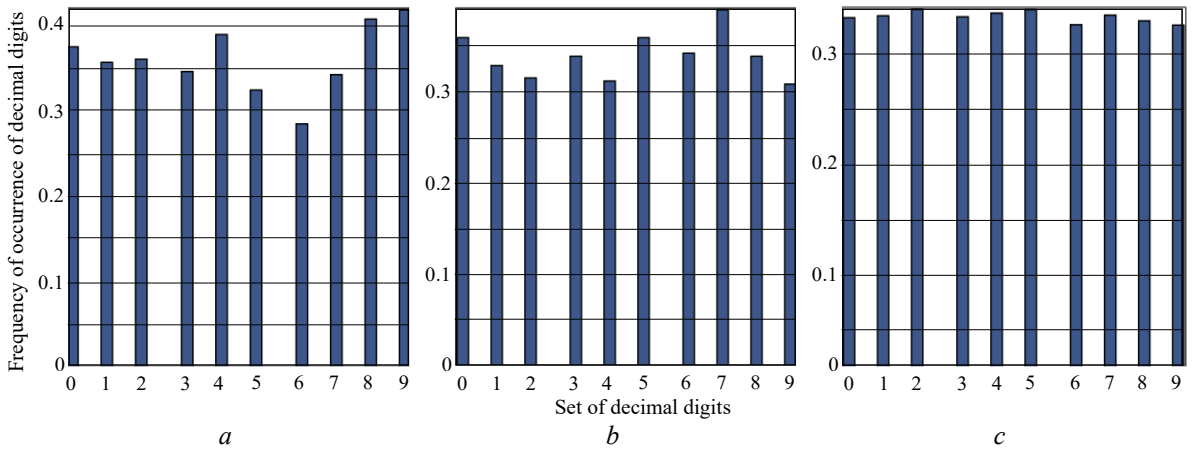


Fig. 11. Histogram for the sequence: *a* – $[\mathrm{I}_2[j]: j=1..1000]$; *b* – $[\mathrm{I}_2[j]: j=2000..3000]$; *c* – $[\mathrm{I}_2[j]: j=1..49729]$, constructed for $T=223$, $H=2.0708011$, $\vartheta=\dfrac{H^T+0.001\cdot 1/H}{H^T-1}$, $x_0=0.9$

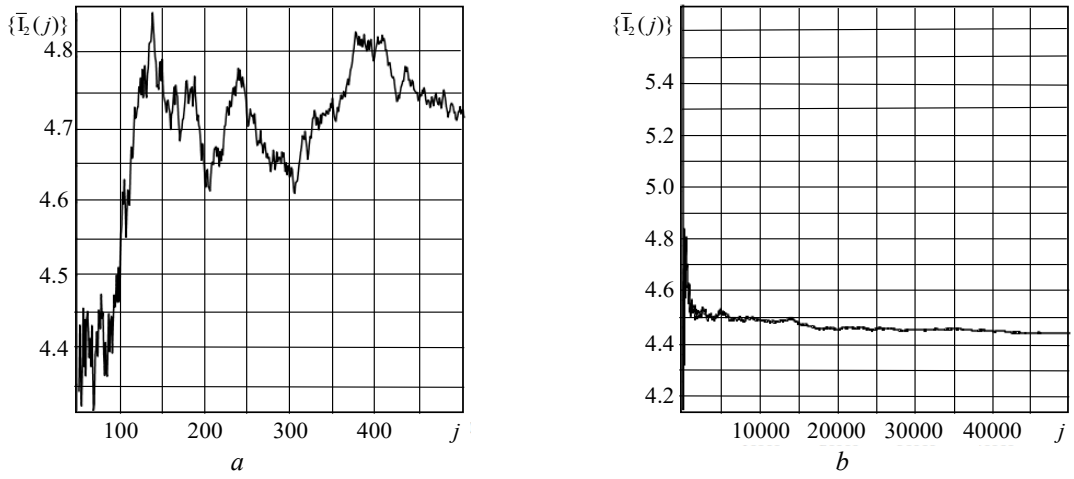


Fig. 12. Graphs of the quantities: *a* – $\{\bar{\mathrm{I}}_2(j)\}_{j=1}^{500}$; *b* – $\{\bar{\mathrm{I}}_2(j)\}_{j=1}^{T^2}$

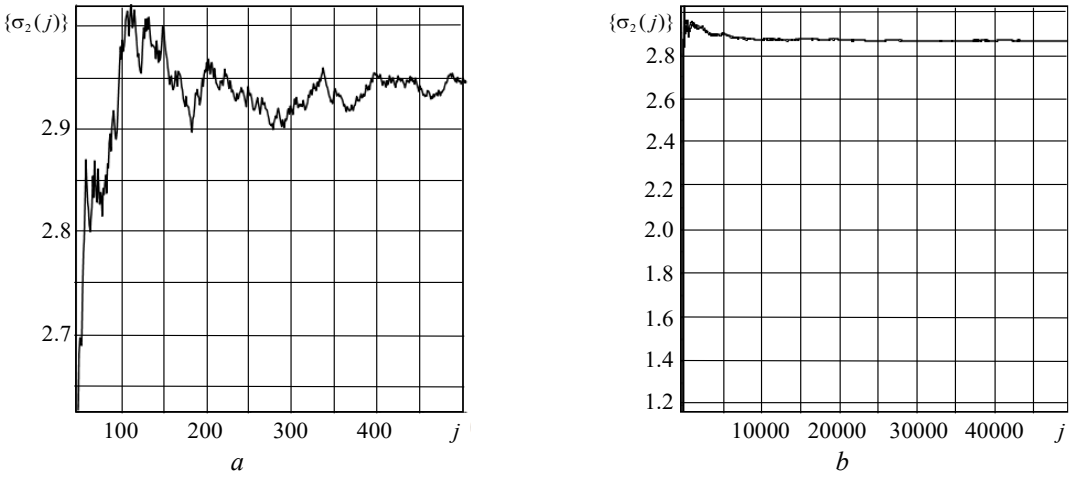


Fig. 13. Graphs of the quantities: *a* – $\{\sigma_2(j)\}_{j=1}^{500}$; *b* – $\{\sigma_2(j)\}_{j=1}^{T^2}$

Праці Одеського політехнічного університету, 2025. Вип. 2(72)
ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

Graphical testing method

There is a known problem in testing a pseudo-chaotic sequence for uncorrelation, which is that the use of point characteristics (mean, variance), as well as correlation functions or even functions that depend on higher-order moments, can be ineffective.

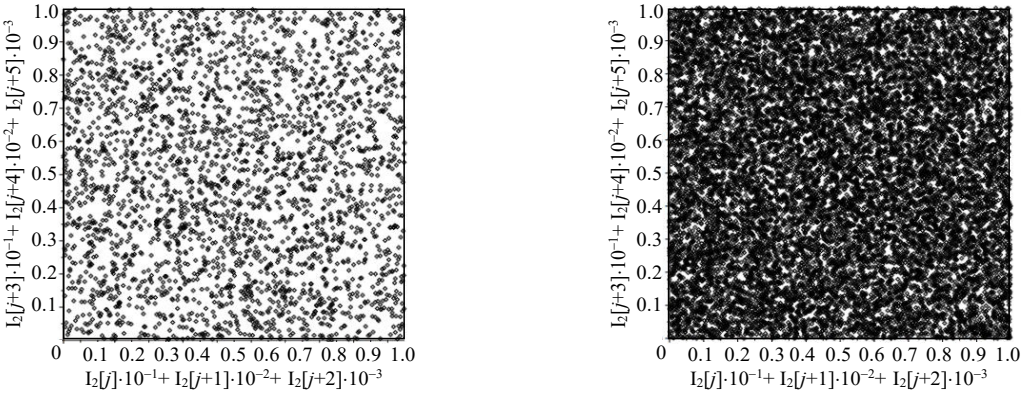
Therefore, we will additionally apply a graphical testing method. Let's break down the sequence $[\mathrm{I}_1[j]: j = 1..49729]$ into elements consisting of consecutive triples of decimal numbers, and divide the resulting three-digit numbers by 10^3. We get a new sequence:

$$[\mathrm{I}_1[j]\cdot 10^{-1} + \mathrm{I}_1[j+1]\cdot 10^{-2} + \mathrm{I}_1[j+2]\cdot 10^{-3} : j = 1..49727],$$

consisting of decimal numbers, which are determined by the first three digits. Let's plot the points with coordinates on the plane:

$$\{\mathrm{I}_1[j]\cdot 10^{-1} + \mathrm{I}_1[j+1]\cdot 10^{-2} + \mathrm{I}_1[j+2]\cdot 10^{-3}, \mathrm{I}_1[j+3]\cdot 10^{-1} + \mathrm{I}_1[j+4]\cdot 10^{-2} + \mathrm{I}_1[j+5]\cdot 10^{-3}\}. \quad (10)$$

The resulting image will allow us to assess the chaotic nature of consecutive triples of numbers. In Fig. 14, the points with coordinates (10) are shown for $j = 1..3000$ and $j = 5000..20000$.

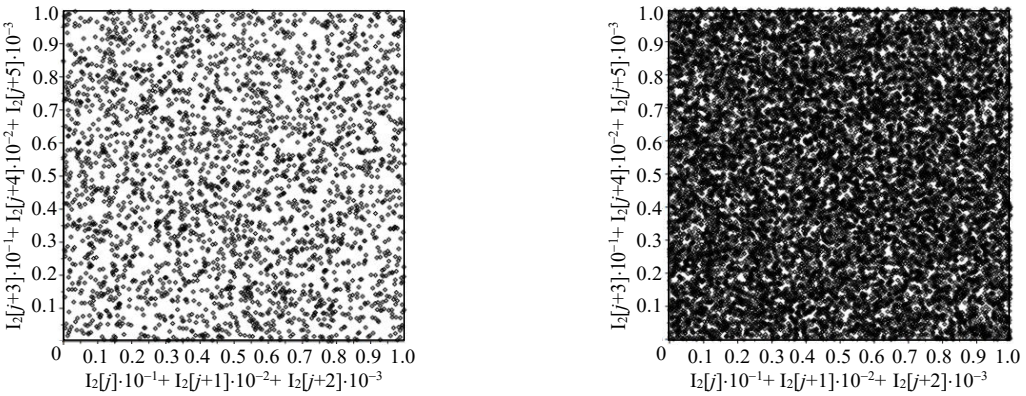


a *b*

Fig. 14. Points with coordinates (10) for: *a* – $j = 1..3000$ and *b* – $j = 5000..20000$, generated by sequence (6)

for $T = 223$, $H = 2.0708011$, $\vartheta = \dfrac{H^T + 0.001\cdot 1/H}{H^T - 1}$, $x_0 = 0.9$

One can see the absence of explicit correlation in sequence (6). For sequence (7), the results of the corresponding constructions are shown in Fig. 15.



a *b*

Fig. 15. Points with coordinates (10) (with the replacement of index 1 by 2) for: *a* – ; *b* – $j = 5000..20000$, generated by sequence (6) for $T = 223$, $H = 2.0708011$, $\vartheta = \dfrac{H^T + 0.001\cdot 1/H}{H^T - 1}$

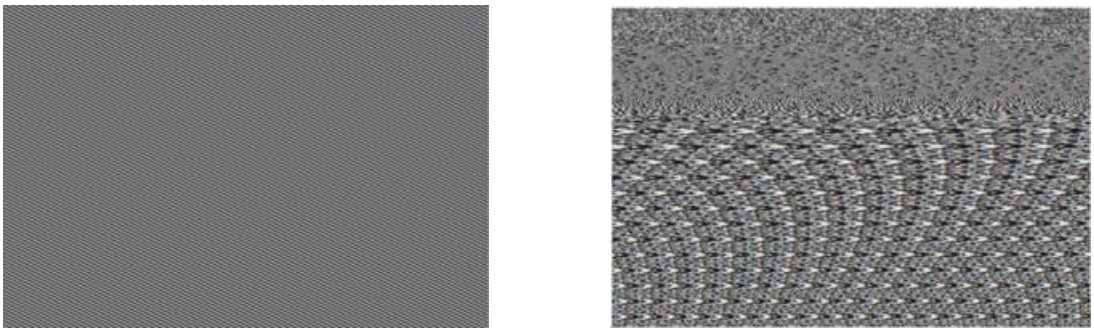
ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

Visual analysis of the corresponding graphs shows that sequence (7) may be more uncorrelated than (6). However, sequence (6) is constructed sequentially with the calculation of the cycle points $\{\eta_1, \dots, \eta_T\}$, while for the construction of sequence (7) it is necessary to know the entire cycle at once, which leads to a decrease in the speed of the algorithm and an increase in the memory used.

The graphical test used above can be modified. For a more effective check of the correlation of the sequence, instead of a two-color image, one can consider a color one. To do this, three sequences are generated from the sequence $[\mathrm{I}[j]: j=1..N]$: $R=[0.1\cdot \mathrm{I}[j]: j=1..N]$, $G=[0.1\cdot \mathrm{I}[j+1]: j=1..N]$, $B=[0.1\cdot \mathrm{I}[j+2]: j=1..N]$. Further, for each pixel, the color in RGB format is determined using the generated sequences R, G, B.

Let's take, for example, an image height of $h=438$ pixels, a width of $w=648$ pixels. A total of 279936 pixels are used. Let's generate the sequence $[j \bmod 10: j=1..N]$ (the number N must be chosen not less than 279938), which is clearly correlated. In this case, the histogram, mean and variance of this sequence will be, as for a uniformly distributed one. For comparison, let's generate a sequence of the first digits of the fractional part of the expression $\sin(j^2+1)$, $j=1..N$. Let's construct images of these sequences in RGB format (Fig. 12).

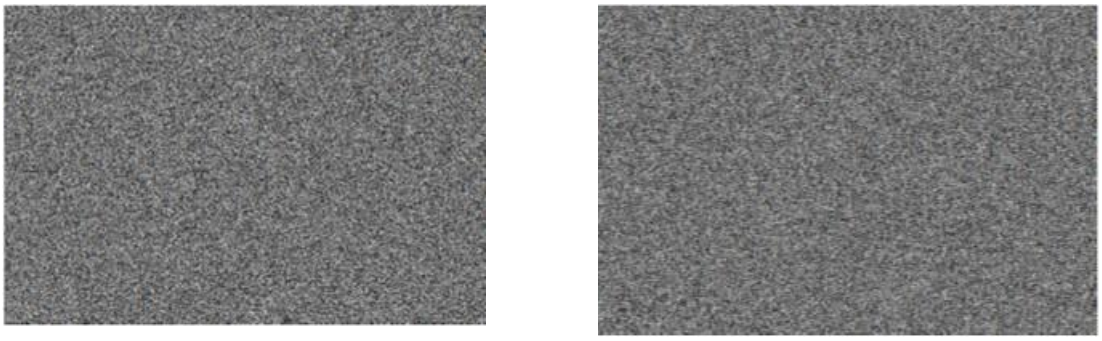
Since any correlation should manifest itself in the form of visual regularity, it can be argued that the sequences that generate the images in Fig. 16 are strongly correlated.



a *b*

Fig. 16. Images in RGB format for the sequences: *a* – $[j \bmod 10: j=1..N]$;
b – $[trunc(10\cdot \sin(j^2+1)): j=1..N]$

Let's construct a similar image for sequences (6) and (7) (Fig. 17).



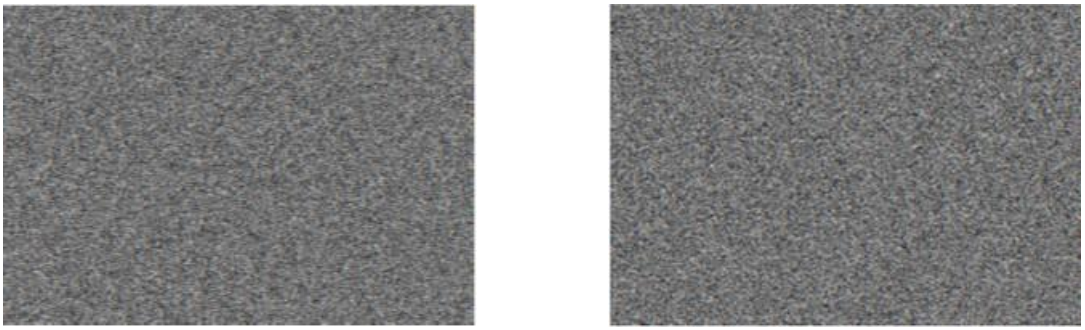
a *b*

Fig. 17. Image in RGB format for sequences (6) (case *a*) and (7) (case *b*)

For these sequences, the regular structure is not visually traced.

For comparison, we give an image in RGB format for the sequence of the first 286000 decimal digits of the numbers π and e (Fig. 18).

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)



a *b*

Fig. 18. Image in RGB format for the sequence of the first 286000 decimal digits of the numbers: $a - \pi$; $b - e$

Image encryption

Let's apply the above algorithm to image encryption. An image with a height of h pixels and a width of w pixels consists of $n = h \cdot w$ pixels. That is, it is considered as an array of n elements, to each of which a three-dimensional vector of decimal numbers is assigned. These numbers have 15 digits and are enclosed between zero and one. The vector (0, 0, 0) defines a black pixel, and the vector (1, 1, 1) a white pixel. The coordinates characterize the shades of red, green and blue, respectively. Sometimes a fourth coordinate is also considered, which characterizes the transparency of the color.

To encrypt an image, you need to generate a pseudo-chaotic sequence whose elements are enclosed between zero and one, and add it element-wise modulo 1 with the sequences R, G and B. It is clear that instead of one pseudo-chaotic sequence, you can generate three different similar sequences.

Let the sequence $[\mathrm{I}[j]: j = 1..N]$ be generated according to rule (6) or (7) with the corresponding key: $Key = [T, H, \pm\alpha, x_0]$. Let's define the sequence:

$$[\sum_{k=1}^{p} \mathrm{I}[j+k-1] \cdot 10^{-k} : j = 1..N+1-p], \tag{11}$$

where $1 \le p \le 15$ (experiments show that it is sufficient to take $p = 2$ or 3). If T is such that N is less than n, then it is necessary to generate several key sequences (with different keys). Let r – i-th element of the sequence R, α – i-th element of the key sequence. Then the encrypted element $\hat{r}$ in the simplest case will be calculated by the formula:

$$\hat{r} = \{r + \alpha\}, \tag{12}$$

where the function $\{\cdot\}$ means the integer part of the number.

Formula (12) allows for the reverse:

$$r = \begin{cases} \hat{r} - \alpha, & \hat{r} - \alpha > 0; \\ 1 + \hat{r} - \alpha, & \hat{r} - \alpha < 0. \end{cases} \tag{13}$$

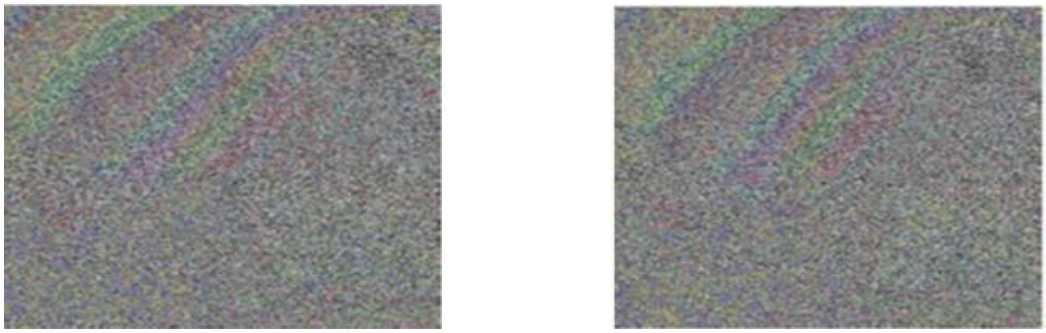
Formula (13) allows you to uniquely restore the value of the original pixel from the encrypted value in all cases, except for $\hat{r} - \alpha = 0$. In this case, two options are possible $r = 0$ or 1. In order to exclude ambiguity, you can perform rescaling of the sequences R, G and B: $X \to (1 - \varepsilon)X$, where ε — is a small number, greater than 10^{-15}. Then in the case of $\hat{r} - \alpha = 0$ it is necessary that $r < 1$, i.e. $r = 0$. Physically, rescaling means the absence of pure white. For small ε, this fact practically does not change anything. It is clear that if necessary, you can perform the reverse rescaling $X \to X/(1 - \varepsilon)$.

Let's consider the image presented in Fig. 19. It consists of 238572 pixels ($h = 423$, $w = 564$). For encryption, let's take the key $Key = [223, 2.070811, 0.001, 0.9]$ and generate the key

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

sequence. It contains 49729 elements. It is necessary to generate additional sequences. Let's do this by choosing the keys $Key_j = [223, 2.07081j,\ 0.001,\ 0.9]$, $j = 2..6$. The combined key sequence contains $49729 \cdot 6 = 298374$ elements, which is sufficient to perform the encryption process. The results of the encryption process using sequences (6), (7). The image encrypted in this way is presented in Fig. 20.

Fig. 19. Test image for encryption



a *b*

Fig. 20. Encrypted test image using sequence (6) (case *a*) and (7) (case *b*)

A regular structure is traced on the encrypted images. If you use a modified version (14), then already for $p = 2$ the encrypted images look without a visible regular structure (Fig. 21).

a *b*

Fig. 21. Encrypted test image using modification (14) for $p = 2$ for sequences: (6) (case *a*) and (7) (case *b*)

Let's consider one more example (the test image is shown in Fig. 22).

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

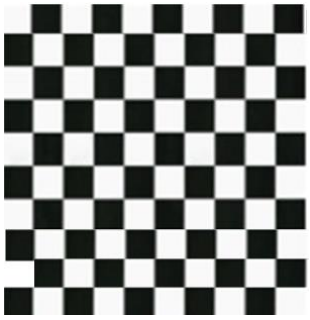


Fig. 22. Test image for encryption

The encryption results are presented in Fig. 23. It can be seen that the simple use of sequences (6) and (7) leads to a regular structure (cases *a*) and *b*). With modification (14) ($p = 2$), the visible regularity of the encrypted image disappears.

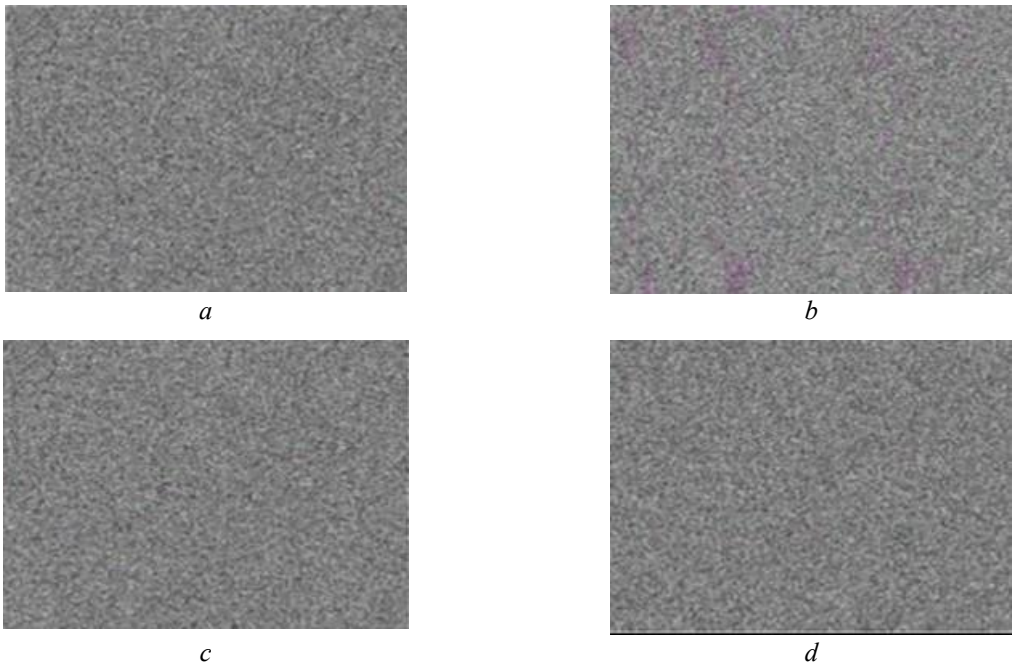


Fig. 23. Encrypted test image for sequences (6) and (7): without modification (cases *a* and *b*); with modification (14) for $p = 2$ (cases *c* and *d*)

Concluding remarks

This paper proposes a new discrete dynamical system for generating long pseudo-chaotic sequences. The system can be used for data encryption, for example, images and information protection from unauthorized access. The advantage of the proposed solution is the short key length and the independence of the algorithm from the hardware and software platform used.

The algorithm for constructing pseudo-chaotic sequences proposed in the article, of course, needs further testing. It is necessary to conduct a detailed correlation analysis of the sequence, an approximate entropy analysis, a statistical test (National Institute of Standards and Technology, USA), etc. It is necessary to additionally conduct an analysis of the security of the keys, an analysis of the statistical histograms of encrypted messages (images), an analysis of sensitivity, an analysis of robustness, an analysis of complexity, etc. [27].

It is also interesting to consider other schemes for stabilizing cycles, for example, [28, 29, 30] and compare them with the scheme proposed in the article.

These are all tasks for further research.

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

Література

1. Stinson D. R. Cryptography: Theory and Practice. 3rd ed. Boca Raton : Chapman and Hall/CRC, 2006. 593 p.
2. Mao W. Modern Cryptography: Theory and Practice. Upper Saddle River : Pearson Education, 2003. 755 p.
3. Bauer F. L. Decrypted Secrets: Methods and Maxims of Cryptology. 4th ed. Berlin : Springer, 2007. 487 p. DOI: https://doi.org/10.1007/978-3-540-48121-8.
4. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptology. Boca Raton : CRC Press, 1996. 780 p. URL: https://cacr.uwaterloo.ca/hac.
5. Shannon C. E. A mathematical theory of communication. *Bell System Technical Journal*. 1948. Vol. 27, no. 4. P. 379–423, 623–656. DOI: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.
6. Zhu C. X. A novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications*. 2012. Vol. 285, no. 1. P. 29–37. DOI: https://doi.org/10.1016/j.optcom.2011.08.079.
7. Lu Q., Yu L., Zhu C. Symmetric Image Encryption Algorithm Based on a New Product Trigonometric Chaotic Map. *Symmetry*. 2022. Vol. 14, no. 2. Art. 373. DOI: https://doi.org/10.3390/sym14020373.
8. Zhang W., Zhu Z., Yu H. A symmetric image encryption algorithm based on a coupled logistic-Bernoulli map and cellular automata diffusion strategy. *Entropy*. 2019. Vol. 21, no. 5. Art. 504. DOI: https://doi.org/10.3390/e21050504.
9. An Intelligent Session Key-Based Hybrid Lightweight Image Encryption Algorithm Using Logistic-Tent Map and Crossover Operator for Internet of Multimedia Things / M. Gupta et al. *Wireless Personal Communications*. 2021. Vol. 121. P. 1857–1878. DOI: https://doi.org/10.1007/s11277-021-08713-3.
10. Lozi R. Can we trust in numerical computations of chaotic solutions of dynamical systems? *Topology and Dynamics of Chaos* / eds. Ch. Letellier, R. Gilmore. World Scientific, 2013. Vol. 84. P. 63–98. DOI: https://doi.org/10.1142/9789814434928_0003.
11. Shannon C. E. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. 1949. Vol. 28, no. 4. P. 656–715. DOI: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.
12. Malik D. S., Shah T. Color multiple image encryption scheme based on 3D-chaotic maps. *Mathematics and Computers in Simulation*. 2020. Vol. 178. P. 646–666. DOI: https://doi.org/10.1016/j.matcom.2020.07.011.
13. Öztürk İ., Kılıç R. Utilizing true periodic orbits in chaos-based cryptography. *Nonlinear Dynamics*. 2021. Vol. 103. P. 2805–2818. DOI: https://doi.org/10.1007/s11071-021-06275-w.
14. Image encryption scheme based on blind signature and an improved Lorenz system / G. Ye et al. *Expert Systems with Applications*. 2022. Vol. 205. Art. 117709. DOI: https://doi.org/10.1016/j.eswa.2022.117709.
15. Zhu S., Wang G., Zhu C. A Secure and Fast Image Encryption Scheme based on Double Chaotic S-Boxes. *Entropy*. 2019. Vol. 21, no. 8. Art. 790. DOI: https://doi.org/10.3390/e21080790.
16. An image encryption scheme based on multi-objective optimization and block compressed sensing / X. Chai et al. *Nonlinear Dynamics*. 2022. Vol. 108. P. 2671–2704. DOI: https://doi.org/10.1007/s11071-022-07331-5.
17. Liu L., Wang J. A cluster of 1D quadratic chaotic map and its applications in image encryption. *Mathematics and Computers in Simulation*. 2023. Vol. 204. P. 89–114. DOI: https://doi.org/10.1016/j.matcom.2022.07.027.
18. Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system / H. Zhu et al. *Mathematics and Computers in Simulation*. 2022. Vol. 198. P. 188–210. DOI: https://doi.org/10.1016/j.matcom.2022.02.027.
19. A New One-Dimensional Compound Chaotic System and Its Application in High-Speed Image Encryption / S. Zhu et al. *Applied Sciences*. 2021. Vol. 11, no. 23. Art. 11206. DOI: https://doi.org/10.3390/app112311206.
20. Complexity analysis of chaotic pseudo-random sequences based on spectral entropy algorithm / K. H. Sun et al. *Acta Physica Sinica*. 2013. Vol. 62, no. 1. Art. 010501. DOI: https://doi.org/10.7498/aps.62.010501.
21. A new hybrid digital chaotic system with applications in image encryption / M. Alawida et al. *Signal Processing*. 2019. Vol. 160. P. 45–58. DOI: https://doi.org/10.1016/j.sigpro.2019.02.016.
22. Adleman L. M. Molecular computation of solutions to combinatorial problems. *Science*. 1994. Vol. 266, no. 5187. P. 1021–1024. DOI: https://doi.org/10.1126/science.7973651.
23. Midoun M. A., Wang X., Talhaoui M. Z. A sensitive dynamic mutual encryption system based on a new 1D chaotic map. *Optics and Lasers in Engineering*. 2021. Vol. 139. Art. 106485. DOI: https://doi.org/10.1016/j.optlaseng.2020.106485.
24. Search for invariant sets of the generalized tent map / K. Ayers et al. *Journal of Difference Equations and Applications*. 2023. Vol. 29, no. 9-12. P. 1156–1183. DOI: https://doi.org/10.1080/10236198.2024.2307521.

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

25. Elaydi S. N. Discrete Chaos: With Applications in Science and Engineering. 2nd ed. Boca Raton : Chapman & Hall/CRC, 2007. 440 pDmitrishin D., Stokolos A., and Iacob J., Average predictive control for nonlinear discrete dynamical systems, Adv. Syst. Sci. Appl. 20(1) (2020), pp. 27 – 49.
26. Dmitrishin D., Stokolos A., Iacob J. Average predictive control for nonlinear discrete dynamical systems. *Advances in Systems Science and Applications*. 2020. Vol. 20, no. 1. P. 27–49. DOI: https://doi.org/10.25728/assa.2020.20.1.848.
27. Teh J. S., Alawida M., Sii Y. C. Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*. 2020. Vol. 50. Art. 102421. DOI: https://doi.org/10.1016/j.jisa.2019.102421.
28. Biham O., Wenzel W. Characterization of Unstable Periodic Orbits in Chaotic Attractors and Repellers. *Physical Review Letters*. 1989. Vol. 63, no. 8. P. 819–822. DOI: https://doi.org/10.1103/PhysRevLett.63.819.
29. A new method for finding cycles by semilinear control / D. Dmitrishin et al. *Physics Letters A*. 2019. Vol. 383, no. 16. P. 1871–1878. DOI: https://doi.org/10.1016/j.physleta.2019.03.018.
30. Miller J. R., Yorke J. A. Finding all periodic orbits of maps using Newton methods: sizes of basins. *Physica D: Nonlinear Phenomena*. 2000. Vol. 135, no. 3-4. P. 195–211. DOI: https://doi.org/10.1016/S0167-2789(99)00114-1.

References

1. Stinson, D. R. (2006). *Cryptography: Theory and Practice* (3rd ed.). Chapman and Hall/CRC.
2. Mao, W. (2003). *Modern Cryptography: Theory and Practice*. Pearson Education.
3. Bauer, F. L. (2007). *Decrypted Secrets: Methods and Maxims of Cryptology* (4th ed.). Springer. https://doi.org/10.1007/978-3-540-48121-8.
4. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptology*. CRC Press. https://cacr.uwaterloo.ca/hac/.
5. Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, *27*(4), 379–423, 623–656. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.
6. Zhu, C. X. (2012). A novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications*, *285*(1), 29–37. https://doi.org/10.1016/j.optcom.2011.08.079.
7. Lu, Q., Yu, L., & Zhu, C. (2022). Symmetric Image Encryption Algorithm Based on a New Product Trigonometric Chaotic Map. *Symmetry*, *14*(2), 373. https://doi.org/10.3390/sym14020373.
8. Zhang, W., Zhu, Z., & Yu, H. (2019). A symmetric image encryption algorithm based on a coupled logistic-Bernoulli map and cellular automata diffusion strategy. *Entropy*, *21*(5), 504. https://doi.org/10.3390/e21050504.
9. Gupta, M., Gupta, K. K., Khosravi, M. R., Shukla, P. K., Kautish, S., & Shankar, A. (2021). An Intelligent Session Key-Based Hybrid Lightweight Image Encryption Algorithm Using Logistic-Tent Map and Crossover Operator for Internet of Multimedia Things. *Wireless Personal Communications*, *121*, 1857–1878. https://doi.org/10.1007/s11277-021-08713-3.
10. Lozi, R. (2013). Can we trust in numerical computations of chaotic solutions of dynamical systems? In Ch. Letellier & R. Gilmore (Eds.), *Topology and Dynamics of Chaos* (Vol. 84, pp. 63–98). World Scientific. https://doi.org/10.1142/9789814434928_0003.
11. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.
12. Malik, D. S., & Shah, T. (2020). Color multiple image encryption scheme based on 3D-chaotic maps. *Mathematics and Computers in Simulation*, *178*, 646–666. https://doi.org/10.1016/j.matcom.2020.07.011.
13. Öztürk, İ., & Kılıç, R. (2021). Utilizing true periodic orbits in chaos-based cryptography. *Nonlinear Dynamics*, *103*, 2805–2818. https://doi.org/10.1007/s11071-021-06275-w.
14. Ye, G., Wu, H., Liu, M., & Shi, Y. (2022). Image encryption scheme based on blind signature and an improved Lorenz system. *Expert Systems with Applications*, *205*, 117709. https://doi.org/10.1016/j.eswa.2022.117709.
15. Zhu, S., Wang, G., & Zhu, C. (2019). A Secure and Fast Image Encryption Scheme based on Double Chaotic S-Boxes. *Entropy*, *21*(8), 790. https://doi.org/10.3390/e21080790.
16. Chai, X., Fu, J., Gan, Z., Lu, Y., & Zhang, Y. (2022). An image encryption scheme based on multi-objective optimization and block compressed sensing. *Nonlinear Dynamics*, *108*, 2671–2704. https://doi.org/10.1007/s11071-022-07331-5.

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)
Proceedings of Odessa Polytechnic University, Issue 2(72), 2025

1. Liu, L., & Wang, J. (2023). A cluster of 1D quadratic chaotic map and its applications in image encryption. *Mathematics and Computers in Simulation*, *204*, 89–114. https://doi.org/10.1016/j.matcom.2022.07.027.
2. Zhu, H., Ge, J., Qi, W., Zhang, X., & Lu, X. (2022). Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system. *Mathematics and Computers in Simulation*, *198*, 188–210. https://doi.org/10.1016/j.matcom.2022.02.027.
3. Zhu, S., Deng, X., Zhang, W., & Zhu, C. (2021). A New One-Dimensional Compound Chaotic System and Its Application in High-Speed Image Encryption. *Applied Sciences*, *11*(23), 11206. https://doi.org/10.3390/app112311206.
4. Sun, K. H., He, S. B., He, Y., & Yin, L. Z. (2013). Complexity analysis of chaotic pseudo-random sequences based on spectral entropy algorithm. *Acta Physica Sinica*, *62*(1), 010501. https://doi.org/10.7498/aps.62.010501.
5. Alawida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A new hybrid digital chaotic system with applications in image encryption. *Signal Processing*, *160*, 45–58. https://doi.org/10.1016/j.sigpro.2019.02.016.
6. Adleman, L. M. (1994). Molecular computation of solutions to combinatorial problems. *Science*, *266*(5187), 1021–1024. https://doi.org/10.1126/science.7973651.
7. Midoun, M. A., Wang, X., & Talhaoui, M. Z. (2021). A sensitive dynamic mutual encryption system based on a new 1D chaotic map. *Optics and Lasers in Engineering*, *139*, 106485. https://doi.org/10.1016/j.optlaseng.2020.106485.
8. Ayers, K., Dmitrishin, D., Radunskaya, A., Stokolos, A., & Stokolos, K. (2023). Search for invariant sets of the generalized tent map. *Journal of Difference Equations and Applications*, *29*(9-12), 1156–1183. https://doi.org/10.1080/10236198.2024.2307521.
9. Elaydi, S. N. (2007). *Discrete Chaos: With Applications in Science and Engineering* (2nd ed.). Chapman & Hall/CRC.
10. Dmitrishin, D., Stokolos, A., & Iacob, J. (2020). Average predictive control for nonlinear discrete dynamical systems. *Advances in Systems Science and Applications*, *20*(1), 27–49. https://doi.org/10.25728/assa.2020.20.1.848.
11. Teh, J. S., Alawida, M., & Sii, Y. C. (2020). Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, *50*, 102421. https://doi.org/10.1016/j.jisa.2019.102421.
12. Biham, O., & Wenzel, W. (1989). Characterization of Unstable Periodic Orbits in Chaotic Attractors and Repellers. *Physical Review Letters*, *63*(8), 819–822. https://doi.org/10.1103/PhysRevLett.63.819.
13. Dmitrishin, D., Skrinnik, I., Lesaja, G., & Stokolos, A. (2019). A new method for finding cycles by semilinear control. *Physics Letters A*, *383*(16), 1871–1878. https://doi.org/10.1016/j.physleta.2019.03.018.
14. Miller, J. R., & Yorke, J. A. (2000). Finding all periodic orbits of maps using Newton methods: sizes of basins. *Physica D: Nonlinear Phenomena*, *135*(3-4), 195–211. https://doi.org/10.1016/S0167-2789(99)00114-1.

Хамітов Віталій Миколайович; Vitalii Khamitov, ORCID: https://orcid.org/0009-0005-3494-8304,
Антощук Світлана Григорівна; Svitlana Antoshchuk, ORCID: https://orcid.org/0000-0002-9346-145X

Received October 03, 2025

Accepted November 21, 2025