DOI: https://doi.org/10.15276/ict.02.2025.31
УДК 004.056

Використання нелінійних дискретних відображень для побудови псевдохаотичних криптосистем

Дмитришин Дмитро Володимирович[1)]
Д-р техніч. наук, професор каф. Прикладної математики та інформаційних технологій
ORCID: https://orcid.org/0000-0002-2291-2364; dmitrishin@op.edu.ua
Хамитов Віталій Миколайович[1)]
Аспірант кафедри Інформаційних систем
ORCID: https://orcid.org/0009-0001-3045-8245; khamitov@op.edu.ua
Болтьонков Віктор Олексійович[1)]
Канд. техніч.наук, доцент кафедри Інформаційних систем
ORCID: https://0000-0003-3366-974X; vaboltenkov@gmail.com
Антощук Світлана Григорієвна[1)]
Д-р техніч. наук, професор кафедри Інформаційних систем
ORCID: https://orcid.org/ 0000-0002-9346-145X; asg@op.edu.ua
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

Для вирішення проблеми несанкціонованого доступу до інформації використовуються методи криптографії. Аналіз показав, що перспективними в цьому плані є потокові схеми шифрування, які можна розглядати з погляду нелінійної динаміки. Особливістю таких схем є генерація деяким детермінованим генератором з короткого ключа (насіння) довгої псевдовипадкової послідовності з використанням дискретної динамічної системи. Однак хаотичності динамічних систем притаманне протиріччя: з одного боку вона дає абсолютно необхідні для криптографії властивості заплутування та розпилення (щодо тексту та ключа), з іншого боку викликає незручності використання, пов'язані з сильною чутливістю до обурень та округлень. Показано, що основна проблема використання псевдохаотичних динамічних систем пов’язана з особливостями комп’ютерних обчислень, а саме з тим, що кількість різних станів в комп’ютері кінцева, тобто будь-яка побудована траєкторія є періодичною з невеликою довжиною періоду. Також 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. Довжина цих циклів залежить від параметрів системи та початкового значення; ці величини є коротким ключем для генерації довгої псевдохаотичної послідовності.

Проведені дослідження запропонованого підходу показали, що знайдений цикл залежить від початкової точки, та від параметрів ключа. Це дозволяє забезпечити кількість можливих варіантів послідовностей більш ніж $10^{(3+p)m}$. Така складна залежність робить цикл практично необчислюваним для кібератак.

Ключові слова: захист даних; апаратне та програмне забезпечення, криптографічні перетворення; псевдохаотичні послідовності; нелінійна динаміка, .

Вступ. Однією з основних проблем аналізу та обробки даних є проблема несанкціонованого доступу до інформації. Для її вирішення у цифровому середовищі використовуються методи криптографії. Криптографічні перетворення можна умовно розділити на два типи: класичні методи або алфавітні шифри, арифметичні перетворення, в яких операції перетворення відбуваються над бітовим (десятковим) поданням даних. У сучасній криптографії використовують методи шифрування другого типу. Розрізняють симетричні та асиметричні схеми шифрування. Інша відома класифікація виділяє блокові та потокові шифри. Потокова схема перетворює потік символів тексту на потік шифротексту, причому перетворення залежить від стану системи. Ідентичні символи тексту будуть зашифровані у різні символи шифротексту. Існує численна література з різних аспектів криптографії, наприклад [1-3].

Потокові схеми шифрування можна розглядати з погляду нелінійної динаміки. Особливістю цих схем є використання значень деякої обраної траєкторії дискретної

динамічної системи, тобто. побудованої при деяких заданих параметрах системи та із заданим початковим значенням. Подібним щляхом можна отримувати послідовність десяткових цифр або бітову послідовність. Потім ця послідовність використовуються як ключ для перетворення вихідної послідовності (вихідного повідомлення) в зашифровану (шифротекст). Процес здійснюється шляхом лінійних операцій за модулем (два або десять) елементів вихідної та ключової послідовностей. Найпростішою потоковою схемою є шифр Вернама [4].

Потокова схема шифрування вважається безпечною, якщо ключова послідовність істинно випадкова та її довжина дорівнює довжині вихідного повідомлення [5]. Однак на практиці такі ключі генерувати та передавати важко. Замість них використовують псевдовипадкові (псевдохаотичні) послідовності, що згенеровані деяким детермінованим генератором з короткого ключа (насіння), з використанням дискретної динамічної системи [6-9]. Незважаючи на чисельні дослідження присвячені підвищенню криптостійкості методів шифрування на основі методів нелінійної динаміки, суттєвих недоліком останніх залишається їх залежність від апаратного та програмного забезпечення. На усунення цього недоліка націлені данні дослідження.

Аналіз поставленої задачі. Як довів аналіз літератури на етапі моделювання динамічних систем на сучасних обчислювальних засобах виникає ряд проблем. Наприклад, у [6] наголошується, що комп'ютерні обчислення обов'язково вимагають додаткового спеціального підтвердження результатів. Основна обчислювальна проблема пов'язана з тим, що в комп'ютерах числа зберігаються в регістрах і осередках пам'яті з обмеженою кількістю розрядів, внаслідок чого система дійсних чисел, що представлені в комп’ютері, є дискретною та кінцевою. Щоб простежити, які наслідки можуть виникнути в результаті цього, розглянемо найпростіший приклад обчислення ітерованої послідовності за допомогою стандартної функції Тент в програмному середовищі EXEL: $f(x) = 2(1/2 - |x - 1/2|)$.

Оберемо початкову точку $x_0 = 2/3$. Тоді теоретично повинно бути $f^{(k)}(x_0) = x_0$, $k = 1, 2, \ldots$ (тут і далі використовуються позначення $f^{(1)}(x) = f(x)$, $f^{(k)}(x) = f(f^{(k-1)}(x))$). Однак обчислення дають інші результати: $f^{(53)}(x_0) = 1$, $f^{(54)}(x_0) = 0$. Аналіз показав, що при виборі інших початкових значень для x_0, результат не змінюється, тобто будемо отримувати $f^{(54)}(x_0) = 0$.

Інша проблема може виникнути, коли орбіта зациклюється та довжина циклу виявляється досить малою. У цьому випадку використовувати ключову послідовність неможливо.

Наступна проблема пов'язана з тим, що різні платформи (апаратні та програмні) використовують різні алгоритми обчислення математичних функцій та зберігають проміжні результати з різною точністю. Так як хаотичні генератори вкрай чутливі до точності, дуже ймовірно, що одні й самі алгоритми шифрування, реалізовані на різних платформах, будуть призводити до різних результатів.

Таким чином, властивість хаотичності динамічних систем виявляється дуальною: з одного боку вона дає абсолютно необхідні для криптографії властивості заплутування та розпилення (щодо тексту та ключа) [7-11], з іншого боку викликає незручності використання, пов'язані з сильною чутливістю до обурень та округлень.

Метою представленого дослідження є побудова нової дискретної динамічної системи, що генерує довгі псевдохаотичні послідовності з використанням як насіння (ключа) параметрів системи та початкових значень. При цьому алгоритм не залежить від апаратного та програмного забезпечення.

Запропонований підхід. Розглянемо нелінійне рівняння з дискретним часом

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

де

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

$x\in(-\infty,+\infty)$, $H\ge 2$. Відображення (2) називається узагальненим відображенням Тент.

Множина $\{\eta_1,\dots,\eta_T\}$ називається T-циклом відображення (2), якщо числа $\eta_1,\dots,\eta_T$ різні та $\eta_{j+1}=f(\eta_j)$, $j=1,\dots,T-1$, $\eta_1=f(\eta_T)$, при цьому кожна точка T-циклу називається T-періодичною точкою. Мультиплікатор циклу рівняння (1) визначається формулою $\mu=f'(\eta_T)\cdot\ldots\cdot f'(\eta_1)$, тобто $\mu=\pm H^T$. Оскільки $|\mu|=H^T>1$, то будь-який цикл рівняння (1) нестійкий.

Наряду з рівнянням (1) розглянемо рівняння

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

де $F(x)=f\left(\vartheta x+(1-\vartheta)f^{(T)}(x)\right)$; ϑ – деяке дійсне число, яке зветься керуючим параметром і підлягає визначенню в подальшому.

Рівняння (3) будемо називати системою управління для рівняння (1).

Нехай цикл $\{\eta_1,\dots,\eta_T\}$ рівняння (1). Оскільки $\vartheta\eta_k+(1-\vartheta)f^{(T)}(\eta_k)=\eta_k$, тобто $F(\eta_k)=f(\eta_k)$, це означає, що цикл рівняння (1) також буде циклом рівняння (3). Слід відмітити, що зворотне твердження у загальному випадку невірне. Мультиплікатор λ цього ж циклу $\{\eta_1,\dots,\eta_T\}$ для рівняння (3) можна знайти з [13]: $\lambda=\mu\left(\vartheta+(1-\vartheta)\mu\right)^T$.

Тоді умова локальної асимптотичної стійкості циклу рівняння (3) при $\mu=H^T$: $|\lambda|=\left|H^T\left(\vartheta+(1-\vartheta)H^T\right)^T\right|<1$, звідки

$$\frac{H^T-\frac{1}{H}}{H^T-1}<\vartheta<\frac{H^T+\frac{1}{H}}{H^T-1}. \quad (4)$$

Якщо $\mu=-H^T$, умова локальної асимптотичної стійкості циклу рівняння (5): $|\lambda|=\left|H^T\left(\vartheta-(1-\vartheta)H^T\right)^T\right|<1$, звідки

$$\frac{H^T-\frac{1}{H}}{H^T+1}<\vartheta<\frac{H^T+\frac{1}{H}}{H^T+1}. \quad (5)$$

Можна довести таку теорему: якщо виконані нерівності (4), (5), то будь-яке рішення рівняння (3) обмежено. Більш того, будь-який T-цикл $\{\eta_1,\dots,\eta_T\}$ цього рівняння, для якого величина $\mu=f'(\eta_T)\cdot\ldots\cdot f'(\eta_1)$ позитивна/негативна, локально асимптотично стійкий.

Для генерації псевдостохастичної послідовності пропонується використовувати динамічну систему (3), у якій ϑ задовольняє умову (4) або (5).

При цьому сама послідовність визначається через T-періодичні точки $\{\eta_1,\dots,\eta_T\}$.

Тут T – досить велике число. Для того, щоб виключити короткі підцикли, число T потрібно брати простим. Усього існує $\frac{2^{T-1}-1}{T}$ циклів довжини T, тобто. великих T циклів дуже багато, отже ймовірність потрапити на конкретний цикл дуже мала. В силу хаотичності динамічної системи (1) довгий цикл практично не відрізняється від довільної нециклічної траєкторії. Цей цикл залежить від початкової точки $x_0\in(0,1)$, від числа T і

параметрів H і ϑ. Це фактично робить цикл необчислюваним для кібератак. Такий цикл є локально асимптотично стійким. Це означає, що отримана траєкторія залежить від незначних обурень, похибок обчислень і округлень. Більше того, можна очікувати, що при одних і тих же значеннях x_0, T, H, ϑ будуть виходити однакові цикли на різних комп'ютерах. Важливим питанням є питання точності обчислень. Загалом кажучи, ця точність повинна залежати від довжини циклу. Обчислювальні експерименти показують, що треба вибирати розрядність $Digits = T + 2(k_1 + k_2)$, $k_1, k_2 \approx 10-15$, $k_1 < k_2$. У цьому випадку можна використовувати всі значущі цифри чисел η_j для побудови ключової псевдохаотичної послідовності (для посилення хаотичності можна використовувати цифри з позиції k_1 до $T + k_1 - 1$). Початкових точок може бути кілька. Можна генерувати послідовності, змінюючи параметри T, H та ϑ.

Практичні рекомендації щодо вибору керуючого параметру:

$$\vartheta = \frac{H^T - \alpha_1 \frac{1}{H}}{H^T + 1} \text{ або } \vartheta = \frac{H^T + \alpha_2 \frac{1}{H}}{H^T - 1}, (0 < \alpha_1 < 0.001,\ 0 < \alpha_2 < 0.001).$$

Далі можна ще більше посилити хаотичність ключової послідовності: спочатку вибирати всі числа з послідовності $\{x_j\}_{j=T_0}^{T_0+T}$ (T_0 - деяке задане число), що стоять на k_1 місці після коми в кожному x_j, далі таким же чином вибирати числа, що стоять на $k_1 + 1$ місці тощо. Згенерована послідовність містить pT^2 елементів, де p – число початкових точок. Насінням генерації є ключ $Key = [T, H, \alpha_1, \alpha_2, \{x_0\}]$, де $\{x_0\}$ - множина початкових точок. Якщо параметри $H, \alpha_1, \alpha_2, \{x_0\}$ визначаються m цифрами, то можливих варіантів послідовностей більш ніж $10^{(3+p)m}$. Зламати такий ключ за розумний час неможливо.

Експериментальна перевірка. Припустимо, що існує наступний ключ:

$$Key = [419,\ H,\ 0.001,\ 0.001,\ \{0.9,0.01\}].$$

Розглянемо два випадки для різних значень параметру H: $H = 2.70801$, $H = 2.70800$.

Обчислимо елементи ключової послідовності з номера 1000 по 1050: отримаємо дві послідовності.

При $H = 2.70801$ - {1, 6, 6, 0, 8, 7, 5, 0, 7, 3, 6, 0, 4, 8, 3, 6, 7, 7, 7, 7, 9, 7, 6, 6 8, 3, 7, 9, 2, 6, 2, 3, 5, 7, 6, 0, 4, 7, 1, 7, 5, 6, 0, 1, 0, 2}

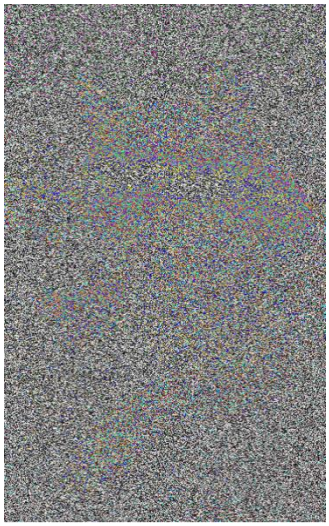
При $H = 2.70800$ -{6, 6, 7, 3, 5, 8, 3, 2, 3, 1, 4 4, 1, 4, 7, 1, 2, 7, 6, 1, 1, 2, 7, 7, 2, 3, 0, 2, 1, 7, 1, 0, 7, 5, 1, 0, 3, 4, 3, 3, 6, 8, 8, 9}

Також для перевірки задіяно графічний спосіб тестування. Розглянемо зображення, що зображене на рисунок,а. Для шифрування сформовано ключ та згенеровано ключову послідовність, як описано вище. Результати процесу шифрування зображення представлені на рис.,б.

Приклад демонструє працездатність алгоритму. Знайдений цикл залежить від початкової точки $x_0 \in (0,1)$ та від параметрів $H, \alpha_1, \alpha_2, \{x_0\}$, які можуть містити досить багато десяткових знаків. Така складна залежність робить цикл практично необчислюваним для кібератак.

Такий цикл локально асимптотично стійкий. Це означає, що отримана траєкторія не залежить від незначних обурень, похибок обчислень і округлень. Більше того, можна очікувати, що при одних і тих же значеннях параметрів $H, \alpha_1, \alpha_2, \{x_0\}$ будуть виходити однакові цикли на різних комп'ютерах.

а



б

Рисунок. **Тестові зображення**
а – вихідне; б – зашифроване

Висновки та подальші дослідження. Запропонований підхід показав хороші результати шифрування зображення, але він потребує подальшого тестування. Необхідно провести кореляційний аналіз послідовності, апроксимаційний ентропійний аналіз, статистичний тест (National Institute of Standards and Technology, USA), аналіз безпеки ключів, аналіз статистичних гістограм шифрованих закодованих повідомлень (образів), аналіз чутливості, аналіз робастності, аналіз складності тощо [12–14].

СПИСОК ЛІТЕРАТУРИ

1. Stinson D. R. “Cryptography Theory and Practice”. *Chapman and Hall/CRC, United Kingdom*. 2006. – URL: https://almuhammadi.com/sultan/crypto_books/Stinson.3ed.pdf.

2. Mao W. “Modern Cryptography: Theory and Practice, Pearson Education”. 2016. ISBN: 0-13-066943-1.

3. Bauer F.L. “Decrypted Secrets – Methods and Maxims of Cryptology”. *Springer*, 2007. ISBN: 978-3-540-60418-1.

4. Menezes A. J., van Oorschot P. C., Vanstone S. A. “Handbook of applied cryptology”. *CRC Press*, 1996. – URL: https://www.academia.edu/33795500/HANDBOOK_of_ APPLIED_CRYPTOGRAPHY.

5. Shannon C. E. “A mathematical theory of communication”. *Bell System Technical Journal*. 1948; 27 (4): 379–423, 623–526. – URL: https://people.math.harvard.edu/~ctm/ home/text/others/shannon/entropy/entropy.pdf.

6. Zhu C. X. “A novel image encryption scheme based on improved hyperchaotic sequences”. *Opt. Commun*. 2012; 285: 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; 14: 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 difusion strategy”. *Entropy*. 2019; 21: 504. DOI: https://doi.org/10.3390/e21050504.

9. Gupta M, Gupta K. K., Khosravi M. R., Shukla P. K., Kautish S., Shankar A. “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*. 2021; 121:1857–1878. – URL: https://www.mdpi.com/2078-2489/15/3/172.

10. Lozi R. “Can we trust in numerical computations of chaotic solutions of dynamical systems?” *Topology and Dynamics of Chaos, eds. Letellier, Ch. & Gilmore, R., World Scientific Series in Nonlinear Science Series A*. 2013; 84: 63–98. – URL: https://hal.science/hal-00682818v1/document.

11. “Communication Theory of Secrecy Systems”. *The Bell System Technical Journal*. 1949; 28 (4): 656–715. – URL: https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf.

12. Ayers K., Dmitrishin D., Radunskaya A., Stokolos A., Stokolos K. “Search for invariant sets of the generalized tent map”. *Journal of Difference Equations and Applications, Taylor & Francis Group*. 2023; 29 (9-12): 1156-1183. DOI: https://doi.rg/10.48550/arXiv.2111.08904.

13. Dmitrishin D., Stokolos A., and Iacob J. “Average predictive control for nonlinear discrete dynamical systems”. *Adv. Syst. Sci. Appl*. 2020; 20 (1): 27–49. DOI: https://doi.org/10.48550/arXiv.1906.02925.

14. Teh J. S., Alawida M., Sii Y. C. “Implementation and practical problems of chaos-based cryptography revisited”. *Journal of Information Security and Applications*. 2020; 50: 102421. DOI: https://doi.org/10.1016/j.jisa.2019.102421.

DOI: https://doi.org/10.15276/ict.02.2025.31
УДК 004.056

Using nonlinear discrete mappings to construct pseudo-chaotic cryptosystems

Dmytro V. Dmytryshyn[1)]
Doctor of Engineering Sciences,
Professor of the Department of Applied Mathematics and Information Technologies
ORCID: https://orcid.org/ 0000-0002-2291-2364; dmitrishin@op.edu.ua
Vitaliy M. Khamitov[1)]
Postgraduate studentof the Department of Information Systems
ORCID: https:///orcid.org/0009-0001-3045-8245; кhamitov@op.edu.ua
Viktor O.Boltenkov[1)]
PhD, Associate Professor, Associate Professor of the Department of Information Systems
ORCID: https:// 0000-0003-3366-974X; vaboltenkov@gmail.com
Svitlana G. Antoshchuk[1)]
Doctor of Engineering Sciences, Professor of the Department of Information Systems
ORCID: https://orcid.org/ 0000-0002-9346-145X; asg@op.edu.ua
[1)] Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine

ABSTRACT

Cryptographic methods are used to solve the problem of unauthorized access to information. Analysis has shown that stream encryption schemes, which can be considered from the perspective of nonlinear dynamics, are promising. A distinctive feature of such schemes is their generation by a deterministic generator from a short key (seed) using a discrete dynamic system. However, the chaotic nature of dynamic systems is inherently contradictory: on the one hand, it provides the properties of obfuscation and dispersion (by text and key) essential for cryptography; on the other, it causes inconveniences due to their strong sensitivity to fluctuations and rounding. It has been shown that the main problem with using pseudo-chaotic dynamic systems is related to the specifics of computer computations, namely, the fact that the number of different states in a computer is finite, meaning that any constructed trajectory is periodic with a short period. Furthermore, different platforms (hardware and software) use different algorithms for calculating mathematical functions and store intermediate results with varying accuracy, so the results obtained on different platforms can differ significantly. To overcome these problems, we propose using a new dynamic system, namely, a generalized Tent mapping with control, which stabilizes cycles of a given duration. These cycles depend on the system parameters and the initial value; these values represent a short key for generating a long pseudo-chaotic sequence.

Research into the proposed approach has shown that the resulting cycle will depend on the initial point and the key parameters. This allows for a number of possible sequence variants greater than $10^{(3+p)m}$. This complex dependence makes the cycle virtually uncomputable for cyberattacks.

Keywords: Data protection; hardware and software; cryptographic transformations; pseudo-chaotic sequences; nonlinear dynamics.