

УДК 004.056.55

ІНФОРМАЦІЙНА БЕЗПЕКА ХАОТИЧНИХ СИСТЕМ ЗВ'ЯЗКУ

DOI 10.36994/2707-4110-2019-1-22-13

Кушнір М. Я., к.ф.-м.н., доц., Чернівецький національний університет ім. Ю. Федьковича, Чернівці, Україна. kushnirnicks@gmail.com.

Семенко А. І., д.т.н., проф., Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. setel@ukr.net.

Косован Г. В., Чернівецький національний університет ім. Ю.Федьковича, Чернівці. kosovan.gregoriy@gmail.com

Бокла Н. І., к.т.н., Національний університет «Львівська політехніка», Львів, Україна. nataloshka_77@ukr.net.

Шестопад Є. О., Державний університет телекомунікацій, Київ, Україна. ie.shestopal@gmail.com.

Анотація. Побудова захищених систем зв'язку з використанням явища детермінованого хаосу є актуальним питанням на сьогоднішній день. Для досягнення поставленої мети необхідно виконати кілька основних етапів. Це забезпечення ступеня стійкості синхронізації між передавачем і приймачем відповідно, дослідження хаотичних коливань для оцінки схожості шуму і апаратне проектування системи зв'язку. Відомо, що режим стабільної синхронізації необхідний для рівня якості відновлення даних. Для побудови системи зв'язку з високим ступенем прикриття в першу чергу необхідно вибрати хаотичний сигнал несучої, спектральні та статистичні характеристики якого були би схожі з шумом. Значна увага в роботі приділена оцінюванню періодичності т.зв. псевдохаотичних коливань, які ми використовуємо при моделюванні. На основі отриманих результатів побудовано апаратний прототип прихованої системи зв'язку.

Ключові слова: хаос, псевдовипадкова послідовність, псевдохаотична послідовність, криптографія, конфіденційність передачі інформації.

INFORMATION SECURITY OF THE CHAOTIC COMMUNICATION SYSTEM

Nikoaj Kushnir, Ph.D., Ass. Prof, Chernivtsi National University Chernivtsi, Ukraine. kushnirnicks@gmail.com

Anatoly Semenko, Dr.habil., Prof, Open International University of Human Development «Ukraine», Kyiv, Ukraine. setel@ukr.net

Georgij Kosovan, Chernivtsi National University Chernivtsi, Ukraine. kosovan.gregoriy@gmail.com

Natalija Bokla, Ph.D., National University «of Lviv Polytechnic», Lviv, Ukraine. nataloshka_77@ukr.net

Yevhen Shestopal, State University of Telecommunications, Kyiv, Ukraine.
ie.shestopal@gmail.com

Abstract. *In telecommunications, a particular place belongs to systems with a wideband noise-free signal, the undisputed advantage of which is increased by both narrowband and wideband interference, confidentiality of information transmission, as well as electromagnetic compatibility with adjacent electronic devices. A wideband noise-free signal is formed using a number of known modulated sequences — m-, Kasam-, Gold sequences, typically by direct spreading. Systems using known pseudo-random sequences cannot be considered protected from unauthorized access. An effective way to increase the confidentiality of signal transmission in a noise-free TSC is to use a chaotic signal-based PVP. Pseudorandom sequence generators are based on one-dimensional chaotic reflections such as logistics, quadratic, and cubic. Researches have shown the undeniable advantage of logistical reflection.*

The construction of hidden communication systems using the deterministic chaos phenomenon is progressive issue nowadays. Several main stages should be carried out for achieving the goal. These are providing of the stability degree of synchronization between the drive and response generators of the transmitter and receiver respectively, investigation of chaotic oscillation to estimate the noise similarity and hardware design of communication system. It is known that the stable synchronization mode is needed for the quality level of data recovery. Therefore the basic conditions were computed for unidirectional coupled chaotic generators for the purpose of providing of generalized synchronization. To construct the communication system with high hiding degree first of all it is necessary to select the chaotic carrier signal the spectral and statistical characteristics of which were similar to noise. Using the obtained results the hardware prototype of hidden communication system was constructed.

Keyword: *chaos, pseudo-random sequence, pseudo-chaotic sequence, cryptography, confidentiality of information transfer.*

Вступ

В наш час активно продовжуються теоретичні та практичні дослідження систем зв'язку, побудованих з використанням детермінованого хаосу, як на програмному так і на апаратному рівнях. Дана робота є продовженням циклу робіт, виконуваних на кафедрі радіотехніки та інформаційної безпеки Чернівецького національного університету і присвячених аналізу безпечних хаотичних систем зв'язку.

Попередній аналіз хаотичних коливань, які планується використати в комунікаційних системах, виконується представленим в роботі дослідницьким комплексом. Він дає можливість оцінити ряд важливих параметрів — показники Ляпунова, перетин Пуанкаре, кореляційну розмірність та ін. і оцінити придатність використання досліджуваних хаотичних коливань для захисту інформації. Оскільки моделювання інформаційних процесів хаотичних систем відбувається з використанням псевдохаотичних коливань, то значна увага в роботі приділяється питанням границі між хаотичними та псевдохаотичними, випадковими та псевдовипадковими коливаннями.

Дослідження системи

Відкриття детермінованого хаосу [1] призвело до швидкого зростання фундаментальних і прикладних наукових досліджень, що дозволило описати поведінку цього нелінійного явища. Чутливість до початкових умов і можливість синхронізації хаотичних коливань [2] дозволяють використовувати детермінований хаос в інформаційних системах. З нашої точки зору, більшість робіт, пов'язаних з використанням хаосу в системах зв'язку, можна розділити на наступні чотири групи:

- загальні властивості хаотичних коливань — включають роботи, присвячені генераторам хаосу різних розмірностей і фундаментальні дослідження нових властивостей детермінованого хаосу;

- синхронізація і контроль хаосу — включають дослідження, що аналізують можливість синхронної хаотичної поведінки зв'язаних систем та керування ними;

- хаотична криптографія — включають дослідження з використанням хаотичної динаміки для створення криптосистем на основі хаосу: аналогового і цифрового. Першу хаотичну схему шифрування виконували на основі дискретної хаотичної системи (логістичної карти), що представлено в [3]. Сьогодні сучасні методи хаотичної криптографії використовують також для шифрування текстів, зображень і відео;

- інформаційні системи з детермінованим хаосом — включають всі види хаотичних систем зв'язку для аналогової та цифрової передачі. Деякі з них включають хаотичні системи зв'язку на основі символічної динаміки.

Аналіз останніх робіт, присвячених хаотичним інформаційним системам, дозволяє зробити кілька важливих висновків. По-перше, переважна кількість робіт включає дослідження хаотичної криптографії для систем інформаційної безпеки. По-друге, інтенсивно вивчаються схемотехнічні реалізації хаотичних систем зв'язку та їх основних апаратних засобів. По-третє, прямохаотичні системи зв'язку є особливо перспективними, де зміна параметра хаотичної системи передає інформацію.

І ще один важливий момент, який стосується природи хаотичних коливань. Реальні хаотичні коливання можуть бути реалізовані лише за умови повного врахування точних значень їх хаотичних часових рядів. Оскільки всі обчислювальні пристрої мають обмежену точність, то при вивченні хаотичних систем ми завжди маємо справу з псевдохаотичними флуктуаціями. Ми чітко розуміємо їх принципovu відмінність від псевдовипадкових коливань, що є чутливою залежністю від початкових умов хаотичних відображень. Попередні розрахунки показують, що в більшості випадків, якщо є точність 16 знаків після коми у комп'ютерному моделюванні, то можна говорити саме про хаотичні коливання [4].

В криптографії на основі хаотичних систем найчастіше використовуються логістичне, квадратне та кубічне одновимірні відображення. Їх використання обумовлене тим, що вони володіють хорошими криптографічними властивостями.

Відомо, що всі три відображення володіють екстремальною чутливістю до початкових умов та значень параметрів функцій відображення, і найменша їх зміна неминуче призводить до розходження генерованих ними траєкторій і, як наслідок, до генерації різних послідовностей бітів. Ця чутливість є настільки високою, що при генерації бітових послідовностей на двох різних персональних комп'ютерах при однакових початкових умовах можлива суттєва різниця між ними [5].

Усунення цього ефекту можливе шляхом обмеження точності обчислень, внаслідок чого можлива повторюваність в часі генерованих послідовностей. Тому є актуальним питання дослідження періоду повторення цих послідовностей.

Для дослідження були використані генеровані логістичним квадратним та кубічним відображеннями значення змінних із трьома довільно обраними ітераціями. При цьому задавалась точність обчислення в 15 знаків після коми.

Дослідження відбувалось наступним чином:

1. Вводились значення початкових умов та параметрів контролю для одновимірних відображень.

2. Вибиралось значення змінних відображень при трьох довільних ітераціях, що далі використовувались для дослідження періодичності.

3. При точності обчислення від другого до 15-го знаку після коми здійснювалось розв'язання рівнянь одновимірних відображень до повторення вибраного значення змінної.

Номер ітерацій, при якій мала місце повторна генерація заданого значення і є періодом повторення. В таблицях 1,2 приведені результати досліджень періоду повторення для логістичного, квадратного та кубічного відображень.

Всі три динамічні системи реалізовувались в програмному середовищі Delphi 7, що дозволяло дослідити періодичність одновимірних відображень при різних значеннях початкових умов та різній точності їх задавання. На рис. приведено зовнішній вигляд програми, де $N = 100000000$ — максимальна кількість ітерацій, що може виконувати програма; n — номер ітерації, значення якої використовувалось при дослідженні періодичності; n_i — номер ітерації, при якій мало місце повторення зазначеного значення змінної із заданою точністю обчислення.

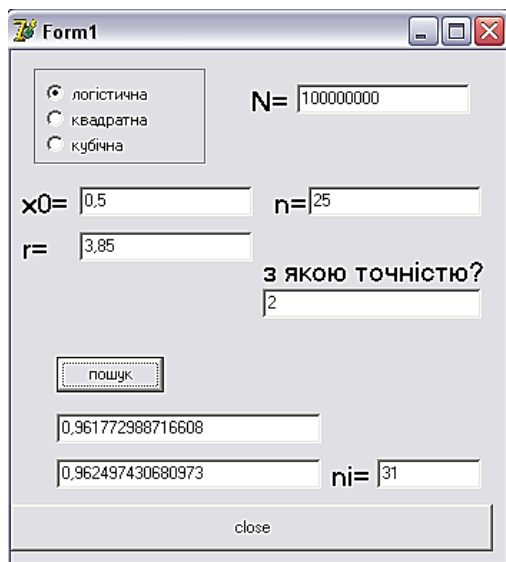


Рис.1. Вікно програми дослідження періодичності одновимірних відображень: x_0 — початкова умова, r — параметр контролю для логістичного відображення

Таблиця 1

**Результати досліджень періоду повторення значень
генерованих логістичним відображенням**

Кількість знаків після коми	$n_{25} =$ 0,961772988716608	$n_{30} =$ 0,499183081649421	$n_{100} =$ 0,959543174980258
	Період повторення (ітерації)	Період повторення (ітерації)	Період повторення (ітерації)
2	31	90	106
3	37	90	130
4	85	330	130
5	145	330	280
6	3625	810	880
7	3625	9390	880
8	9385	22890	9460
9	22885	22890	22960
10	22885	22890	22960
11	22885	209970	210040
12	22885	209970	210040
13	209965	>100000000	210040
14	>100000000		>100000000

Таблиця 2

**Результати досліджень періоду повторення значень генерованих
квадратним відображенням**

Кількість знаків після коми	$n_{25} =$ 0,950289744660889	$n_{30} =$ -0,521709464679855	$n_{100} =$ 0,994499522199194
	Період повторення (ітерації)	Період повторення (ітерації)	Період повторення (ітерації)
2	79	67	121
3	2390	187	169
4	8052	187	1094
5	205757	8057	16617
6	229084	137992	82586
7	630032	137992	6631556
8	79182518	46798393	>100000000
9	>100000000	>100000000	

Висновки

З отриманих результатів випливає, що період повторної генерації послідовностей з часом швидше зростає для послідовностей генерованих квадратним та кубічним відображенням при збільшенні точності обчислення. Періоди повторної генерації вибраних значень для одновимірного відображення, при використанні одних і тих самих початкових умов та параметрів керування відрізняється між собою, що являється підтвердженням нелінійності характеристик одновимірних відображень.

Література

1. E.N. Lorenz. Deterministic Nonperiodic Flow, *Journal of the atmospheric sciences*, vol. 20, pp. 130–141, 1963.
2. L.M. Pecora, T.L. Carroll. Synchronization in Chaotic Systems, *Physical Review Letters*, vol. 64, n. 8, pp. 821–825, 1990.
3. M.S. Baptista. Cryptography with chaos, *Physics Letters A*, 240, pp. 50–54, 1998.
4. M. Kushnir, S. Galiuk, V. Rusyn, G. Kosovan, D. Vovchuk. Computer modeling of information properties of deterministic chaos, *Imprint Proceedings of the 7th Chaotic Modeling and Simulation International Conference*, Lisbon, Portugal, 7–10 June, 2014, pp. 265–276. Published by: ISAST: International Society for the Advancement of Science and Technology. Editor: Christos H Skiadas.
5. Пат. UA 80695 U, МПК H04L 9/24, H03M 7/00 Спосіб шифрування зображення з використанням хаотичного відображення / Політанський Л.Ф. Кушнір М.Я., Косован Г.В.; власник Чернівецький національний університет імені Юрія Федьковича.-u2012 14061; подання заявки 10.12.2012; опубліковано 10.06.2013, Бул.№ 11

References

1. E.N. Lorenz. Deterministic Nonperiodic Flow, *Journal of the atmospheric sciences*, vol. 20, pp. 130–141, 1963.
2. L.M. Pecora, T.L. Carroll. Synchronization in Chaotic Systems, *Physical Review Letters*, vol. 64, n. 8, pp. 821–825, 1990.
3. M.S. Baptista. Cryptography with chaos, *Physics Letters A*, 240, pp. 50–54, 1998.
4. M. Kushnir, S. Galiuk, V. Rusyn, G. Kosovan, D. Vovchuk. Computer modeling of information properties of deterministic chaos, *Imprint Proceedings of the 7th Chaotic Modeling and Simulation International Conference*, Lisbon, Portugal, 7–10 June, 2014, pp. 265–276. Published by: ISAST: International Society for the Advancement of Science and Technology. Editor: Christos H Skiadas.
5. Pat. UA 80695 U, MPK H04L 9/24, H03M 7/00 Sposib shyfruvannya zobrazhen-nya z vykorystannyam khaotychnoho vidobrazhenya / Politans'kyi L.F. Kushnir M.YA., Kosovan H.V.; vlasnyk Chernivets'kyi natsional'nyy universytet imeni Yuriya Fed'kovy-cha. — u2012 14061; podannya zayavky 10.12.2012; opublikovano 10.06.2013, Byul.№ 11 **УДК 004.056.55**