

УДК 004.056.55

DOI: 10.31891/2219-9365-2020-65-1-10

ГРЕСЬ О. В.

Чернівецький національний університет імені Юрія Федьковича

РОЗОРІНОВ Г. М.

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

ПІЛЬКЕВИЧ Ю. Г.

Київський національний університет будівництва і архітектури

КОСТЯК М. Ю., ПАРХУЦЬ Л. Т.

Національний університет «Львівська політехніка»

ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПОТОКОВОГО ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ДИСКРЕТНИХ ВІДОБРАЖЕНЬ

У роботі запропоновано програмну реалізацію системи кодування-декодування інформації з додатковим поточним шифруванням псевдовипадковими послідовностями, що генеруються на основі логістичного відображення. Додаткове шифрування унеможливує розшифрування інформації, якщо третій стороні не відомі значення початкових умов логістичного відображення, що використовується для генерування послідовностей шифрування. Запропонована система була реалізована на програмному рівні з використанням сучасних програмних засобів, зокрема мови програмування C++. Робота системи досліджувалась на прикладі кодування текстової інформації. Результати тестування показали, що запропонована система має більшу швидкодію на 10 % порівняно з аналогічними системами стиснення та шифрування інформації на основі дискретних відображень

Ключові слова: псевдовипадкова послідовність, логістичне відображення, шифрування, кодування.

HRES O.

Yuriy Fedkovych Chernivtsi National University

ROZORINOV H.

National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute"

PILKEVICH Ju.

Kyiv National University of Construction and Architecture

KOSTIAK M., PARKHUTS L.

Lviv Polytechnic National University

SOFTWARE IMPLEMENTATION OF INFORMATION STREAM ENCRYPTION SYSTEM BASED ON DISCRETE MAPS

The paper proposes a system of encoding/decoding information with its additional stream encryption by elements of a chaotic sequence generated on the basis of discrete maps. The system consists of the following blocks: encoding / decoding unit, encryption/decryption unit, pseudorandom sequence generator, initial conditions task unit. The proposed system uses the method of adaptive arithmetic compression with additional streaming encryption of compressed information by pseudorandom sequences generated on the basis of discrete maps. A binary adaptive arithmetic encoder is used as the coding unit.

A modified diffusion transformation is used as the encryption method. At the output of the system, a compressed binary code message is generated, which is further encrypted by pseudorandom sequences. Additional encryption makes it impossible to decrypt the information unless the key to start the pseudorandom generator is known. The use of a modified diffusion transformation as an encryption method, which contains an additional parameter used as an additional key for encryption, can increase the impact of this parameter on the complexity of decrypting encoded data, as well as increase cryptographic and noise immunity of the system as a whole.

The proposed system was implemented at the software level using modern software, in particular the programming language C++.

The operation of the system was studied on the example of encoding text information.

The test results showed that the proposed system of encoding-decoding information with additional streaming encryption by pseudorandom sequences generated on the basis of discrete maps has 10 % higher speed than similar systems of compression and encryption of information on the basis of discrete maps and has increased cryptographic stability.

Keywords: pseudo-random sequence, logistic mapping, encryption, coding.

Вступ. Постановка задачі. Забезпечення захисту інформації в системах обміну інформацією є однією із складних проблем, для вирішення якої застосовують організаційні, технічні та криптографічні методи. Одним із напрямів вирішення проблеми захисту інформації є її криптографічний захист.

В наш час розроблено і використовується багато алгоритмів шифрування для криптографічного захисту. Найбільш поширений тип шифрів – це симетричні шифри, які розподіляються на два класи: блочні шифри, які мають високу стійкість до криптоатак, але не дуже велику швидкодію, та поточкові шифри, які мають дещо меншу криптостійкість, але більшу швидкодію, ніж блочні.

Достатньо ефективним засобом підвищення стійкості шифрування є комбіноване використання декількох різних способів шифрування, тобто послідовне шифрування вихідного тексту за допомогою двох або більше методів [1, 2].

Водночас з поширенням інтернет-технологій та розвитком безпілотних літальних апаратів, виникає проблема захищеності трафіка рухомих об'єктів, а саме, даних командної, аудіо- відео- та іншої інформації засобами малої обчислювальної потужності та високої швидкодії. Тому останнім часом стало поширеним використання поточкових методів шифрування інформації для захисту трафіка рухомих об'єктів з використанням інтернет-мереж.

У зв'язку з цим слід звернути увагу на математичний апарат теорії динамічного хаосу, що відкриває нові можливості для розроблення швидкодіючих шифрів з достатнім рівнем стійкості на основі генераторів псевдовипадкових послідовностей (ПВП) з дискретними функціями відображення. Непередбачуваність поведінки хаотичних систем є основною причиною їх використання при розробленні криптостійких генераторів ПВП, розробленні нових та підвищенні стійкості існуючих методів та систем поточкового шифрування інформації на основі дискретних відображень.

Аналіз основних публікацій. Над проблемою розроблення криптостійких генераторів ПВП на основі хаосу та їх застосування для шифрування інформації активно працюють ряд закладів та науковців як в Україні, так і за її межами. Аналіз публікацій останніх двох десятиліть, тема яких присвячена використанню хаосу у криптографії, та огляд сучасних швидкодіючих методів поточкового шифрування інформації на основі дискретних відображень для застосування в інформаційних системах показав, що проблема підвищення швидкодії криптографічних систем повністю не вирішена. Виходячи з цього, розроблення нових криптостійких та підвищення стійкості існуючих систем поточкового шифрування інформації на основі генераторів хаосу з дискретними функціями відображення із забезпеченням достатнього рівня швидкодії є актуальною задачею.

Основна частина. У системах з дискретним часом моделлю джерела хаотичних коливань в найпростішому випадку виступає різницеве рівняння першого порядку, що описується формулою [1, 2]:

$$x(k+1) = f[a(k), x(0), x(k)] \quad (1)$$

де $k=1, 2, 3, \dots$ – відліки дискретного часу,

Логістичне відображення є однією з найбільш відомих одномірних дискретних хаотичних систем для генерування ПВП, аналітичне представлення якого задається різницевою рівнянням [1, 2]:

$$x_{n+1} = \lambda x_n (1 - x_n), \quad (2)$$

де λ – параметр керування, x_n – початкове значення змінної, x_{n+1} – значення змінної.

Залежно від значення λ генеровані коливання можуть бути періодичними, квазі-періодичними або хаотичними. Встановлено, що для логістичного відображення при $\lambda \geq 3.56$ спостерігається режим хаотичних коливань [1, 2].

В роботі запропонована система кодування/декодування інформації з її додатковим шифруванням елементами хаотичної послідовності, генерованої на основі дискретних відображень [3, 4]. В основі системи лежить спосіб кодування-декодування інформації з додатковим шифруванням, запропонований в [3].

Система складається з наступних блоків: блок кодування/декодування, блок шифрування/розшифрування, генератор ПВП, блок завдання початкових умов. Схема реалізації системи кодування-декодування з додатковим поточковим шифруванням на основі дискретних відображень показана на рис. 1.

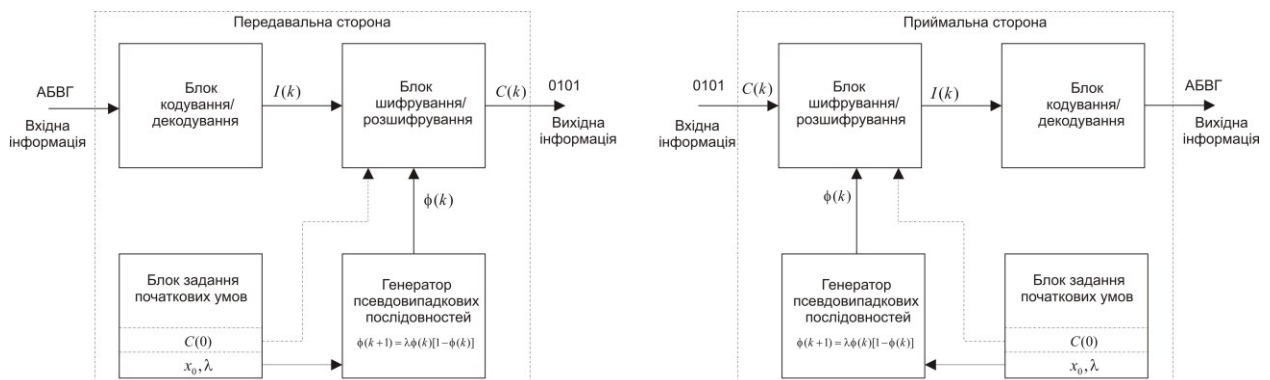


Рис. 1. Схема реалізації системи кодування-декодування з додатковим поточковим шифруванням на основі дискретних відображень

Запропонована система використовує метод адаптивного арифметичного стиснення з додатковим поточковим шифруванням стиснутої інформації псевдовипадковими послідовностями, генерованими на

основі дискретних відображень. Як блок кодування використовується двійковий адаптивний арифметичний кодер [3, 8].

Система працює наступним чином [3, 4] Інформація, що поступає на вхід системи (блоку кодування) на передавальній стороні, кодується та стискається за алгоритмом адаптивного арифметичного кодування, внаслідок чого формується двійкова послідовність (I), що представляє закодовану інформацію. Далі, закодована інформація надходить на вхід блоку шифрування, в якому зашифровується елементами псевдовипадкової послідовності, генерованої на основі логістичного відображення.

В якості методу шифрування використовується модифіковане перетворення дифузії, запропоноване [5]. Дане перетворення зв'язує значення поточних закодованих байтів інформації (тексту) $I(k)$ з наступними байтами інформації (тексту), отриманими після шифрування $C(k)$. Механізм дифузії описується наступною формулою:

$$C(k) = \phi(k) \oplus \{[I(k) + \phi(k)] \bmod N\} \oplus I(k-1), \quad (3)$$

де $C(k)$ – байти зашифрованої інформації (тексту), $I(k)$ – байт інформації (тексту), отриманої після стиснення; $I(k-1)$ – попередній байт інформації (тексту), отриманої після стиснення (з виходу блоку кодування) (при $k = 1$ замість $I(k-1)$ беремо відповідне задане нами значення $C(0)$, яке, зокрема, можна вважати додатковим ключем шифрування), $\phi(k)$ – байти псевдовипадкової послідовності, генерованої на основі логістичного відображення:

$$\phi(k+1) = \lambda \phi(k)[1 - \phi(k)]. \quad (4)$$

Обернене перетворення дифузії переписується у наступному вигляді:

$$I(k) = \{\phi(k) \oplus C(k) \oplus I(k-1) + N - \phi(k)\} \bmod N. \quad (5)$$

Таким чином, на виході системи утворюється стиснуте двійкове кодове повідомлення (C), що додатково зашифроване псевдовипадковими послідовностями. Додаткове шифрування унеможливує розшифрування інформації, якщо не відомий ключ для запуску генератора псевдовипадкової послідовності.

Як ключ для генератора на основі логістичного відображення виступають наступні параметри: початкова умова ϕ_0 та значення параметру керування λ (в нашому випадку $\lambda = 3,99$). На приймальній стороні розшифрування та декодування інформації здійснюється у зворотному порядку.

Використання в якості методу шифрування модифікованого перетворення дифузії, яке містить додатковий параметр, що застосовують як додатковий ключ для шифрування, дозволяє підвищити вплив цього параметру на складність розшифрування кодованих даних, а також підвищити крипто- та завадостійкість системи в цілому.

Для синхронізації передавальної та приймальної сторін можна використати, наприклад, спосіб синхронізації, запропонований в роботі [6]. Цей спосіб полягає у надсиланні через певні проміжки часу поточного значення змінної логістичного відображення, період надсилання значень якої визначається шляхом програмного знаходження часу встановлення синхронізації. Це дозволяє забезпечити однозначне розшифрування інформації в системах потокового шифрування та їх стабільну роботу.

Алгоритм роботи способу кодування – декодування інформації з додатковим потоковим шифруванням ПВП, генерованими на основі дискретних відображень, представлений на рис. 2.

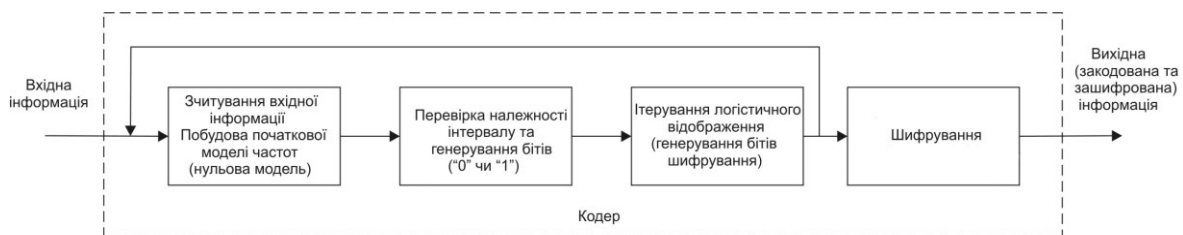


Рис. 2. Алгоритм роботи способу кодування-декодування інформації з додатковим потоковим шифруванням

Алгоритм обрахунку інтервалу та формування біту «0» або «1» наведений на рис. 3. Використовуючи значення параметру керування та початкової умови хаотичного коливання за якими здійснюється генерування псевдовипадкової послідовності на стороні кодера системи, аналогічну послідовність можна згенерувати на приймальній стороні системи.

Таким чином, на виході системи утворюється зашифроване хаотичними послідовностями стиснуте двійкове кодове повідомлення. Додаткове шифрування унеможливує розшифрування інформації, якщо третій стороні не відомі значення параметрів логістичного відображення та початкове значення хаотичного коливання x_0 , що використовується для генерування послідовностей шифрування.

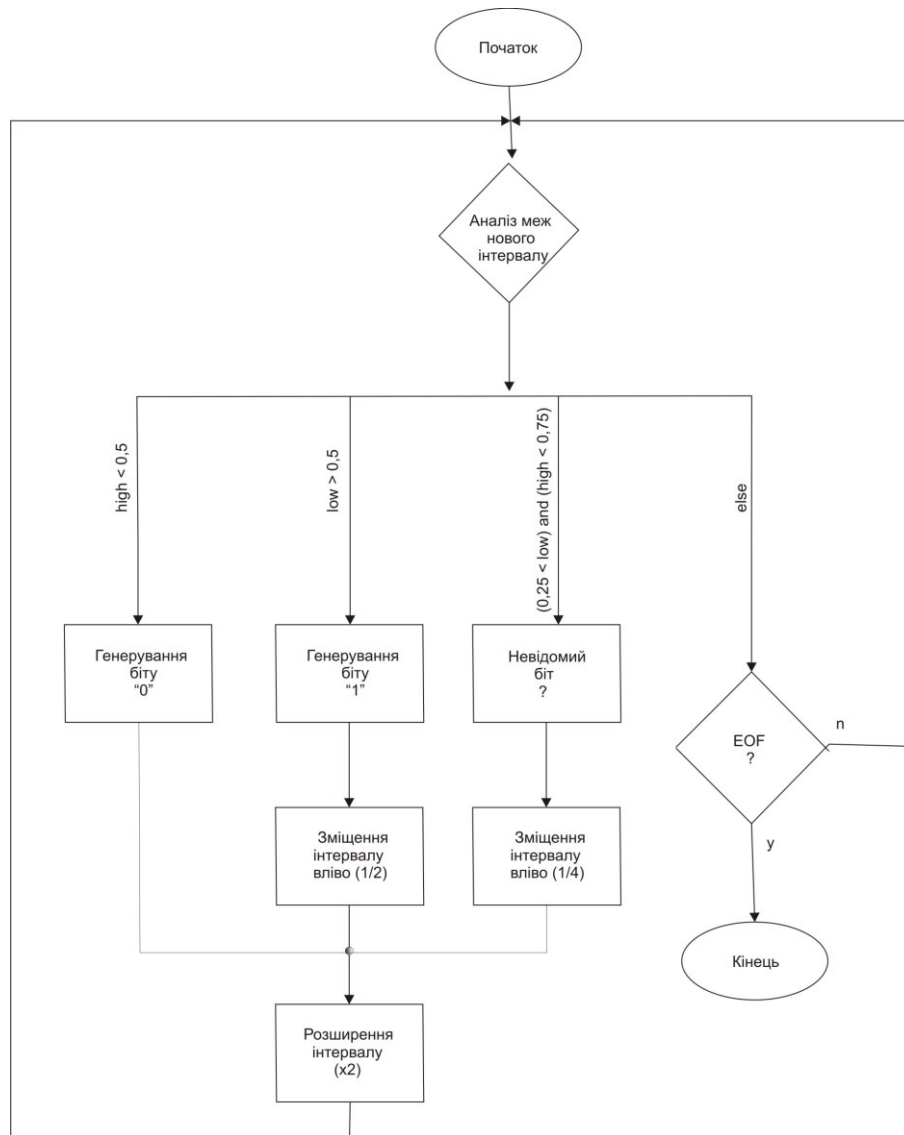


Рис. 3. Алгоритм генерування бітів «0» та «1» у системі стиснення інформації з поточним побітовим шифруванням

Ефективність процедури стиснення оцінюється коефіцієнтом стиснення, що визначається наступним чином:

$$k = \frac{L(S')}{L(S)} \quad (6)$$

де $L(S)$ – виражена в бітах довжина отриманого на виході кодера повідомлення в результаті стиснення рядка S ; $L(S')$ – довжина вхідного повідомлення в бітах.

Розшифрування та декодування інформації здійснюється у зворотному порядку. Стиснуте та зашифроване повідомлення надходить на вхід блоку розшифрування. В блоці розшифрування здійснюється побітове додавання інформації з елементами псевдовипадкової послідовності, генерованої при тих же умовах, що і послідовність в кодері. На виході блоку розшифрування утворюється стиснуте двійкове повідомлення (без шифрування), що поступає на вхід відповідного блоку декодування та перетворюється у вихідну інформацію.

Програмна реалізація системи. Елементи системи кодування-декодування даних з шифруванням може бути реалізований на апаратно-програмному рівні (можливе використання сучасних мікроконтролерів, ПЛІС, а також сучасних мов програмування, наприклад, C++). Запропонована система була реалізована на програмному рівні з використанням сучасних програмних засобів, зокрема мови програмування C++.

Інтерфейс програми, що реалізує розроблену систему кодування-декодування з поточним шифруванням інформації ПВП, генерованими на основі дискретних відображень, приведений на рис. 4. Початкова умова x_0 та параметр керування λ , які необхідні для генерування псевдовипадкової

послідовності для шифрування, вводяться у відповідні вікна програми. На рис. 4 показана робота системи на прикладі шифрування текстової інформації при значеннях початкової умови $x_0 = 0,5$ та параметру керування $\lambda = 3,87$. Дана програмна реалізація також може буди доповнена й іншими методами кодування, наприклад такими як Хаффмана, Шенона-Фано та ін. (рис. 4).

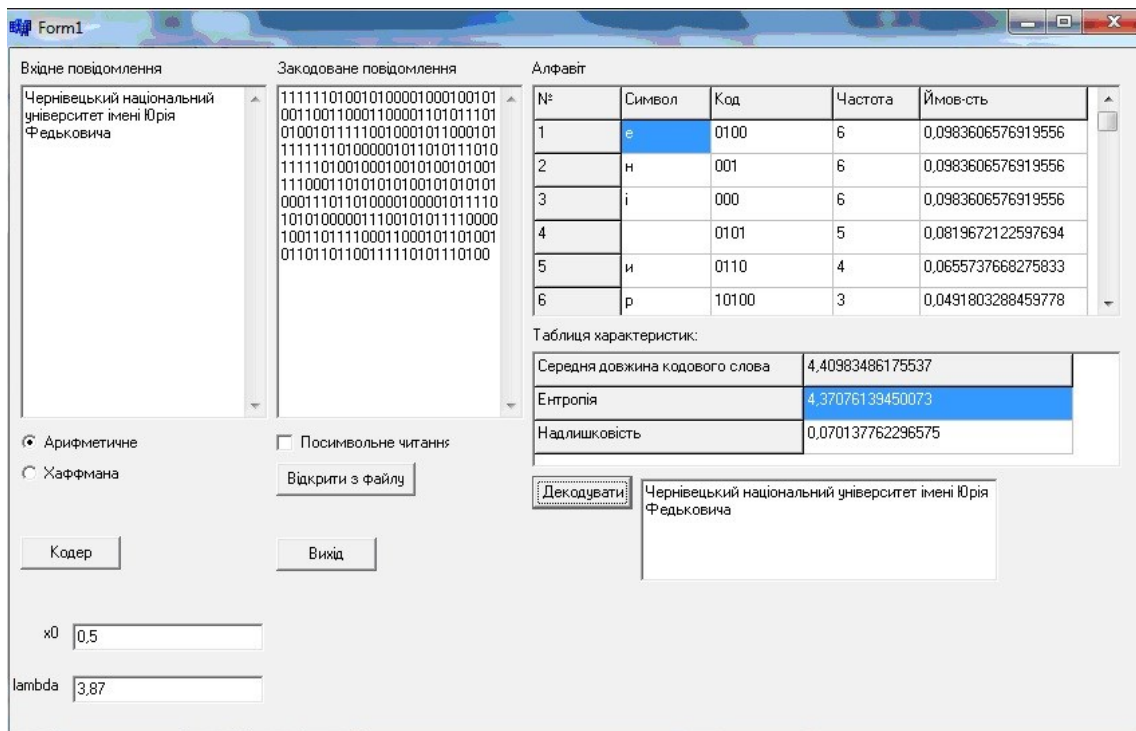


Рис. 4. Інтерфейс програми, що реалізує спосіб кодування-декодування з поточним шифруванням інформації ПВП, генерованими на основі дискретних відображень

Робота системи досліджувалась на прикладі кодування текстової інформації.

В таблиці 1 приведені результати роботи розробленої системи та інших систем кодування інформації з додатковим її шифруванням на основі дискретних відображень. Порівняння проводилось з використанням ноутбука з процесором марки Celeron M 1,6 GHz з 2Гб ОЗП.

Таблиця 1

Порівняльний аналіз розробленої системи з іншими системами кодування інформації з додатковим її шифруванням на основі дискретних відображень

Початковий розмір файлу, Кб	Система кодування-декодування інформації з додатковим шифруванням на основі дискретного відображення		Розроблена система		Відсоток підвищення швидкодії	
	Час кодування, мс	Час декодування, мс	Час кодування, мс	Час декодування, мс	кодування	декодування
1523	590	631	540	581	8,5	7,9
1443	570	601	515	549	9,6	8,7
1428	480	521	443	487	7,7	6,5

В таблиці 2 наведені результати порівняння результатів роботи запропонованої системи (на основі адаптивного арифметичного методу) із відомим методом стиснення LZW [7]. Із таблиці 2 випливає, що значення коефіцієнту стиснення інформації для LZW-кодера, в основному, є вищим, ніж арифметичного. Недоліками LZW-кодера є висока обчислювальна складність методу та менша швидкість стиснення. Швидкодія запропонованої системи стиснення є більшою за швидкодією відомих аналогів [8–10], і забезпечує при цьому захист інформації шляхом її шифрування ПВП.

Результати тестування показали, що запропонована система кодування-декодування інформації з додатковим поточним шифруванням псевдовипадковими послідовностями, генерованими на основі дискретних відображень, має на 10 % більшу швидкодію на відміну від аналогічних систем стиснення та шифрування інформації на основі дискретних відображень та володіє підвищеною криптостійкістю.

Таблиця 2

Порівняння результатів роботи запропонованої системи кодування-декодування інформації з шифруванням з LZW кодером

Розміри файлів, що підлягали стискуванню, Кб	Розміри стиснутих файлів, Кб (арифметичне кодування та шифрування)	Коефіцієнт стиснення	Розміри стиснутих файлів, Кб (LZW-кодер)	Коефіцієнт стиснення
1396	989	1,41	646,3	2,16
1403	1040	1,35	577,4	2,43
1428	946	1,51	631,85	2,26

Підвищення швидкодії запропонованої системи на відміну від аналогічних систем стиснення та шифрування інформації з використанням генераторів на основі дискретних відображень, у яких використовується процедура зміни інтервалів, що відображають символи, у відповідності із ключем шифрування на кожному кроці алгоритму арифметичного кодування, досягається за рахунок того, що шифрування відбувається за меншу кількість кроків. Також в запропонованій системі, на відміну від аналогічних, використовується один генератор ключових послідовностей, що використовуються для шифрування, та побітове шифрування здійснюється після кожної ітерації (тобто після кожного циклу генерування двійкового «0» або «1»).

Висновки. В роботі запропоновано програмну реалізацію системи кодування-декодування інформації з додатковим потоковим шифруванням псевдовипадковими послідовностями, що генеруються на основі логістичного відображення. Додаткове шифрування унеможливує розшифрування інформації, якщо третій стороні не відомі значення початкових умов логістичного відображення, що використовується для генерування послідовностей шифрування. Запропонована система була реалізована на програмному рівні з використанням сучасних програмних засобів, зокрема мови програмування C++. Робота системи досліджувалась на прикладі кодування текстової інформації. Також був проведений порівняльний аналіз швидкодії існуючих систем арифметичного кодування з наступним побітовим шифруванням та розробленої системи. Результати порівняння показали, що запропонована система має більшу швидкодію на 10 % на відміну від аналогічних систем стиснення та шифрування інформації на основі дискретних відображень. Підвищення швидкодії запропонованої системи зумовлене тим, що шифрування відбувається за меншу кількість кроків, в запропонованій системі для шифрування використовується один генератор ключових послідовностей а також стиснення та побітове шифрування здійснюється після кожної ітерації системи.

Література

1. Kocarev L. Pseudorandom bits generated by chaotic maps / L. Kocarev, G. Jakimoski // Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions. – 50(1). – 2003. – P. 123–126.
2. Pareek N.K. Cryptography using multiple one-dimensional chaotic maps / N.K. Pareek, Vinod Patidar, K.K. Sud // Commun. Nonlinear Sci. Numer. Simul. – 10(7). – 2005. – P.715–723.
3. Пат. на корисну модель 129426 Україна, МПК H03M 7/00, H03M 7/30 (2006.01) Спосіб кодування-декодування даних з шифруванням / О.В. Гресь, В.М. Косован, Г.М. Розорінов, А.П. Саміла. Заявники і патентовласники О.В. Гресь, В.М. Косован, Г.М. Розорінов, А.П. Саміла. – № u201805660; заявл. 22.05.2018; опубл. 25.10.2018, Бюл. № 20.
4. Гресь О.В. Дослідження генераторів псевдовипадкових послідовностей на основі дискретних відображень / О.В. Гресь, М.І. Скрипський, В.М. Косован, Г.М. Розорінов // Вісник Хмельницького національного університету. Технічні науки. – 2017. – №4. – С. 243–251.
5. Гресь О.В. Аналіз алгоритмів шифрування інформації на основі хаотичних відображень / О.В. Гресь, В.М. Косован, М.І. Скрипський, Г.М. Розорінов, П.М. Шпатар / Сучасний захист інформації. – 2015. – №3. – с. 49–58.
6. Политанский Р. Л. Система передачи данных с шифрованием хаотическими последовательностями / Р. Л. Политанский, П. М. Шпатар, А. В. Гресь, А. Д. Верига // Технология и конструирование в электронной аппаратуре. – 2014. – №2-3. – С. 28–32.
7. Somefun O. M. Evaluation of dominant text data compression techniques / O. M. Somefun, A. O. Adebayo // International Journal of Application or Innovation in Engineering & Management. – 2014. – Vol. 3, Issue 6. – Pp. 162 – 169.
8. Kwok-Wo Wong, Qiuzhen Lin, Jianyoung Chen "Simultaneous Arithmetic Coding and Encryption Using Chaotic Maps" // IEEE Transaction on Circuits and Systems II, Express Briefs, Vol.57, No.2, February, 2010. – Pp. 146–150).
9. Bose R. A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system / R. Bose, S. Pathak // IEEE transactions on circuits and systems—i: regular papers, . – april 2006 – Vol. 53, NO. 4. – pp. 848–857
10. Wang B. Encrypting the compressed image by chaotic map and arithmetic coding / B. Wang, X. Zheng, S. Zhou, C. Zhou, X. Wei, Q. Zhang, C. Che // Optik. – 2014. – Vol. 125 – pp. 6117–6122.

References

1. Kocarev L. Pseudorandom bits generated by chaotic maps / L. Kocarev, G. Jakimoski // Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions. – 50(1). – 2003. – P. 123–126.
2. Pareek N.K. Cryptography using multiple one-dimensional chaotic maps / N.K. Pareek, Vinod Patidar, K.K. Sud // Commun. Nonlinear Sci. Numer. Simul. – 10(7). – 2005. – P.715–723.
3. Пат. на корисну модель 129426 Україна, МПК H03M 7/00, H03M 7/30 (2006.01) Спосіб кодування-декодування даних з шифруванням / О.В. Гресь, В.М. Косован, Г.М. Розорінов, А.П. Саміла. Заявники і патентовласники О.В. Гресь, В.М. Косован, Г.М. Розорінов, А.П. Саміла. – № u201805660; заявл. 22.05.2018; опубл. 25.10.2018, Бюл. № 20.

4. Hres O.V. Doslidzhennia heneratoriv psevdovypadkovykh poslidovnostei na osnovi dyskretnykh vidobrazhen / O.V. Hres, M.I. Skrypskyi, V.M. Kosovan, H.M. Rozorinov // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – 2017. – №4. – S. 243-251.
5. Hres O.V. Analiz alhorytmiv shyfruvannia informatsii na osnovi khaotychnykh vdobrazhen / O.V. Hres, V.M. Kosovan, M.I. Skrypskyi, H.M. Rozorinov, P.M. Shpatar/ Suchasnyi zakhyst informatsii. – 2015. – №3. – s. 49-58.
6. Polytanskyi R. L. Systema peredachy dannykh s shyfrovanyem khaotycheskymy posledovatelnostiamy / R. L. Polytanskyi, P. M. Shpatar, A. V. Hres, A. D. Veryha // Tekhnolohiya y konstruyovanye v elektronnoi apparature. – 2014. – №2-3. – S. 28-32.
7. Somefun O. M. Evaluation of dominant text data compression techniques / O. M. Somefun, A. O. Adebayo // International Journal of Application or Innovation in Engineering & Management. – 2014. – Vol. 3, Issue 6. – Pp. 162 – 169.
8. Kwok-Wo Wong, Qiuzhen Lin, Jianyoung Chen "Simultaneous Arithmetic Coding and Encryption Using Chaotic Maps" // IEEE Transaction on Circuits and Systems II, Express Briefs, Vol.57, No.2, February, 2010. – PP. 146-150).
9. Bose R. A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system / R. Bose, S. Pathak // IEEE transactions on circuits and systems—i: regular papers, . – april 2006 – Vol. 53, NO. 4 . – pp. 848-857
10. Wang B. Encrypting the compressed image by chaotic map and arithmetic coding / B. Wang, X. Zheng, S. Zhou, C. Zhou, X. Wei, Q. Zhang, C. Che // Optik. – 2014 . – Vol. 125 – pp. 6117–6122.

Надійшла / Paper received: 12.02.2020

Надрукована / Paper Printed : 04.06.2020