METHOD FOR ENCODING VIDEO INFORMATION SAFETY IMPROVEMENT AEROMONITORING EMERGENCY

A study of the conditions of operation using on-board video monitoring systems in the process of prevention and crisis management . Identifies the factors shaping the threat to disrupt the properties of availability and integrity of video aeromonitoring as categories of information security. This leads to the obsolescence of the information obtained , and the belated adoption of wrong decisions. Shows the actual increase security video aeromonitoring in the prevention and management of crisis situations. It is proved that the solution of this problem are encouraged to use compression for the video encoding technology. We justify the choice of image compression technology. It is shown that to avoid the disadvantages associated with a decrease in the lower limit of the differential Polyadic space required for perforating technology further consider the binary mask wavelet elements of the upper and lower levels. The principal stages of image coding method to improve the accessibility of video , which is based on : a differential representation of the images by a combined scheme , the organization perforation arrays in a two-dimensional representation of the differential Polyadic space , mask presentation of arrays of elements of the upper level of the perforation in the differential Polyadic space that provides an additional reduction of the combinatorial redundancy , one-dimensional coding block diagram. We present experimental evaluation of the effectiveness of the developed method with existing methods in the class of controlled loss of quality.

Keywords: differential representation, perforated polyadic space, combinatorial redundancy, the binary mask.

Бараннік Володимир Вікторович, доктор технічних наук, професор, начальник кафедри, Харківський університет Повітряних Сил імені Івана Кожедуба.
E-mail: Barannik_V_V@mail.ru
Баранник Владимир Викторович, доктор технических наук, профессор, начальник кафедры, Харьковский университет Воздушных Сил имени Ивана Кожедуба.
Barannik Vladimir, Doctor of Science (eng.), Professor, chief of chair, Kharkov University of Aircraft of the name of Ivan Kozhedub.

Куліца Олег Сергійович, ад'юнкт, Академія пожарной безпеки імені Героїв Чорнобиля, м. Черкаси.
E-mail: Barannik_V_V@mail.ru
Кулица Олег Сергеевич, адъюнкт, Академия пожарной безопасности имени Героев Чернобыля, г. Черкассы.
Kulitsa Oleg, associate, Academy of Fire Safety named Heroes of Chernobyl, Cherkasy.

УДК 621.391.7

АЛГОРИТМ ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ДВОХ ХАОТИЧНИХ ДИНАМІЧНИХ СИСТЕМ ДЛЯ ЗАХИЩЕНИХ СИСТЕМ ЗВ'ЯЗКУ

Григорій Косован, Микола Кушнір, Леонід Політанський

На сучасному етапі розвиток інформаційних технологій, засобів телекомунікацій та комп'ютерної техніки широко постає проблема захисту конфіденційної інформації від несанкціонованого доступу при її передаванні чи зберіганні. Щоб вирішити дану проблему часто звертаються до криптографічних методів захисту інформації. Крім методів шифрування, що базуються на алгебраїчних поняттях, проводяться розроблення алгоритмів на основі детермінованого хаосу. В даній роботі представлено алгоритм шифрування текстової інформації, що базується на використанні двох динамічних систем, системи Ресслера та кубічного відображення. Система Ресслера використовується для генерацій початкових умов, що використовується кубічним відображенням при шифруванні кожного окремого символу текстового повідомлення. В результаті роботи даного алгоритму символи вхідного повідомлення в результаті шифрування замінюються на цілі числа. В роботі також було проведено моделювання роботи динамічних систем в середовищі Matlab та приведено приклад роботи програми написаної на мові Delphi 7. В роботі також дано оцінку захищеності запропонованого алгоритму. Алгоритм володіє великою кількістю ключів шифрування, що робить процес їх підбору дуже складним. Використання двох динамічних систем ускладнює можливість статистичної атаки.

Ключові слова: *криптографія, шифрування, дешифрування, динамічна система, хаос, алгоритм, оцінювання рівня захищеності.*

Вступ. Розвиток інформаційних технологій та засобів телекомунікацій в значній мірі визначається закономірностями передавання даних по каналах цифрових систем зв'язку. Крім методів шифрування, що базуються на алгебраїчних поняттях, проводяться розроблення алгоритмів на основі детермінованого хаосу [1-4]. Відомі програмні реалізації схем шифрування, що основані на логістичному відображенні Арвінда, а також схеми генерації багаторазових ключів на

основі хаотичної функції Босе [1]. В літературі описана низка схем, що використовують хаотичні функції для прямого шифрування, роль ключів в яких відіграють параметри системи. Один з таких методів шифрування даних з використанням логістичного відображення $x_{n+1} = rx_n(1-x_n)$ запропонований Баптістою, алгоритм якого базується на властивості ергодичності динамічної системи [5].

В даній роботі запропоновано алгоритм шифрування, що поєднує динамічну систему Ресслера та кубічне відображення. Система Ресслера генерує початкові умови для кубічного відображення, що безпосередньо шифрує текстове повідомлення. При цьому збільшується кількість ключів шифрування, що значно підвищує криптостійкість алгоритму в порівнянні з алгоритмом Баптісти, описаному в [5-6]. Запропонований метод може використовуватись в телекомунікаційних системах зв'язку для передавання зашифрованих текстових повідомлень, що мають вигляд випадкового набору цифр.

Опис динамічних систем. Запропонований метод шифрування даних базується на використанні двох динамічних систем, а саме динамічної системи Ресслера, та кубічного відображення. Обидві динамічні системи є чутливими до початкових умов та володіють властивістю ергодичності [2, 7].

Система Ресслера, що задає початкові умови для кубічного відображення описується трьома диференційними рівняннями [1]

$$\begin{cases} \dot{x} = -y - z; \\ \dot{y} = x + py; \\ \dot{z} = q + z(x - r), \end{cases} \quad (1)$$

де змінні x, y, z – динамічні параметри системи; p, q, r – значення статичних параметрів системи. При $p = 0{,}2$, $q = 0{,}1$, $r = 4{,}5$ має місце хаотична динаміка.

Траєкторія системи Ресслера у фазовому просторі та часова залежність її динамічної змінної x, отримані в результаті моделювання в середовищі Matlab, приведені на рис. 1 та рис. 2 відповідно.

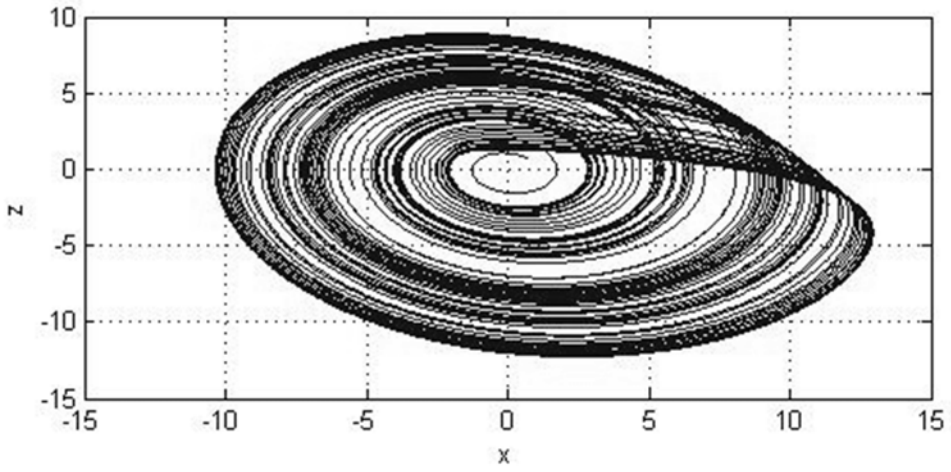


Рис. 1. Траєкторія стану системи Ресслера в фазовому просторі

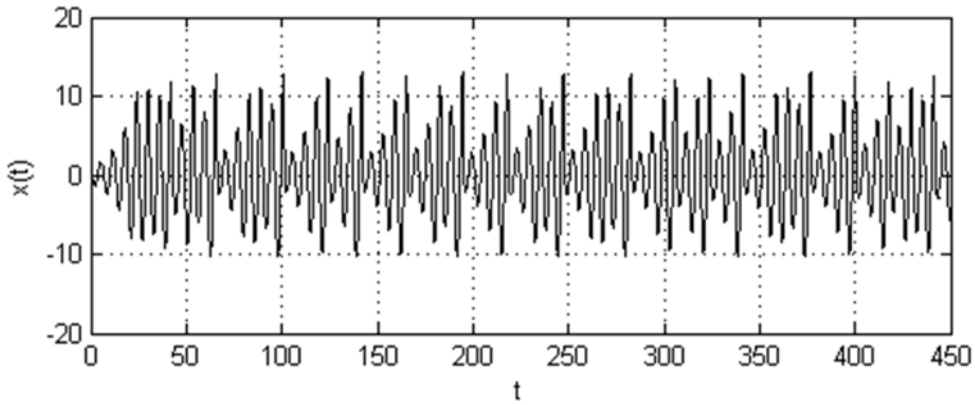


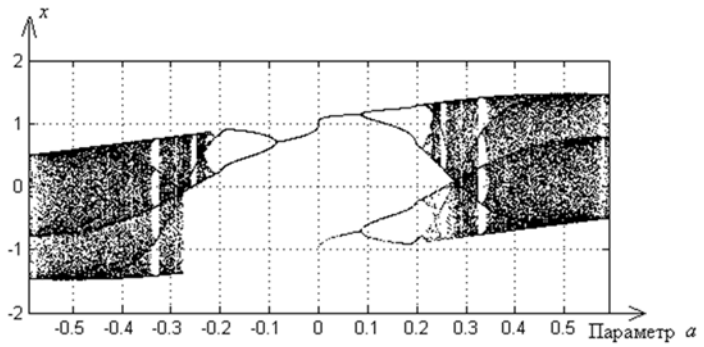
Рис. 2. Часова залежність змінної x хаотичної системи Ресслера

Математична модель кубічного відображення має наступний вигляд [2]:

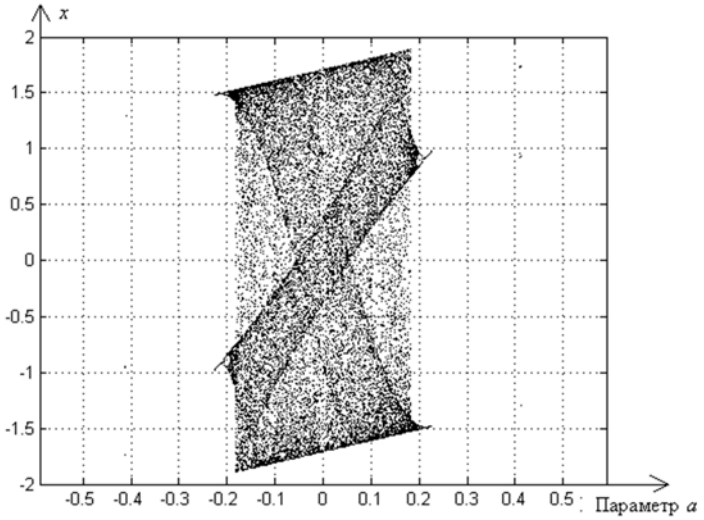
$$x_{n+1} = a - bx_n + x_n^3, \qquad (2)$$

де x – динамічна змінна, a та b – параметри системи, $n = 1,2,3,...$ – номер ітерації.

Результати математичного моделювання еволюційної поведінки кубічного відображення в програмному середовищі Matlab при різних значеннях параметрів системи $a \in [-0,6;0,6]$, $b \in [0,8;2,5]$, приведені на рис. 3 (а) та рис. 3 (б). З отриманих результатів випливає, що чим більше значеннях параметра b більш розвиненою є її хаотична динаміка.



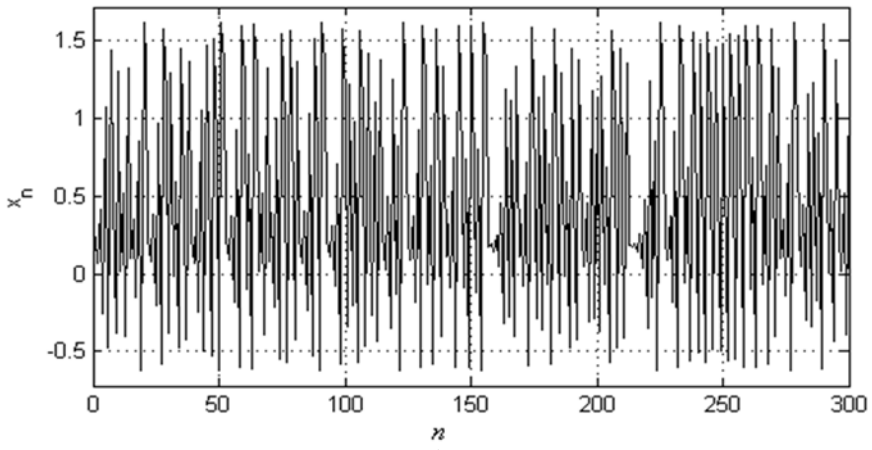
а)



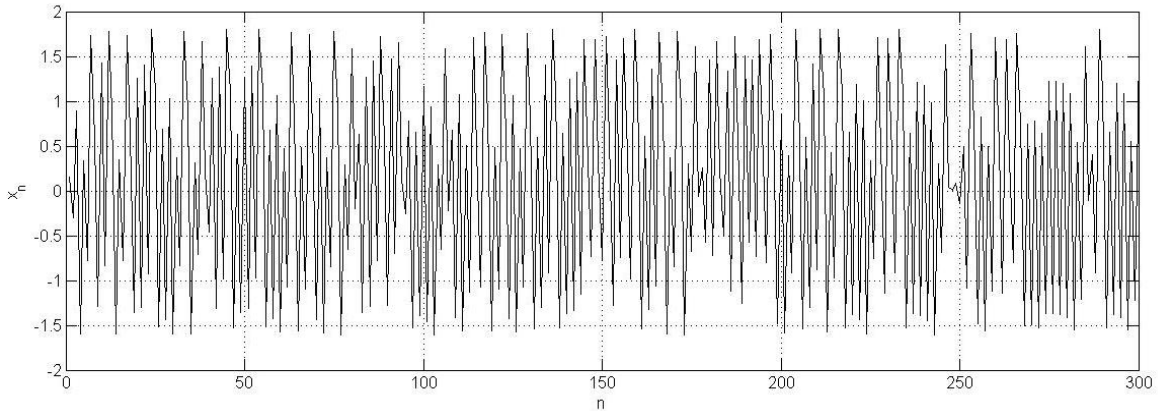
б)

Рис. 3. Біфуркаційна діаграма кубічного відображення:
а) при значенні параметрів $a = 0,55$ та $b = 2,1$, б) при $a = 0,18$ та $b = 2,7$

На рис. 4 приведено результат моделювання кубічного відображення для 300 ітерацій при різних значеннях параметрів.



а)



б)

Рис. 4. Залежність x_n від номера ітерацій n кубічного відображення при різних значеннях параметрів: а) при a=0,55, b=2,1 та x_0 =0,15, б) при a=0,1, b=2,7 та x_0 =0,15

Алгоритм шифрування-дешифрування. Алгоритм шифрування базується на використанні методики Баптісти [5-6], суть якої полягає в тому, що при заданих початкових умовах $x_0 \in [0;1]$ та значенні параметра системи r здійснюється генерація значень x_n, що шифрують повідомлення у відповідності з рівнянням $x_{n+1} = rx_n(1-x_n)$. В запропонованому нами алгоритмі, структурна схема якого приведена на рис. 5, система Ресслера слугує генератором початкових умов для кубічного відображення, що безпосередньо використовується для шифрування повідомлень.

Рис. 5. Структурна схема алгоритму шифрування

Алгоритм шифрування складається з наступних етапів:

Визначається загальну кількість символів у вхідному текстовому повідомленні N.

Вибираються початкові умови x_0, y_0, z_0 та значення параметрів p, q, r, що забезпечують роботу системи Ресслера в хаотичному режимі.

Розв'язується система Ресслера (1) $N+1000$ та формуємо траєкторію системи у фазовому просторі.

В якості початкових умов для кубічного відображення використовується $N+1000$ значень однієї із динамічних змінних x, y, z системи Ресслера.

Отримані значення однієї із змінних (наприклад x) перетворюються наступним чином $\tilde{x} = (x \bmod p)$, де $p=1$. Дане перетворення здійснюється для узгодження вихідних значень системи Ресслера з діапазоном вхідних значень кубічного відображення.

Вибираються значення параметрів a, b та початкова умова (пункти 4, 5) для кубічного відображення та генерується траєкторія кубічного рівняння (2) шляхом проведення послідовних ітерацій з наступним визначенням діапазону зміни значень кубічного відображення.

Робочий діапазон значень $x \in [x_{\min}, x_{\max}]$, що задається параметрами a та b розбиваємо на $S=256$ інтервалів шириною $\varepsilon = \dfrac{x_{\max}-x_{\min}}{S}$ у відповідності з алфавітом, що відповідає ASCII

коду. При цьому кожному з інтервалів ставиться у відповідність певний символ алфавіту.

В якості початкової умови для шифрування першого символу береться 1001-е узгоджене значення, що в якості початкової умови в рівняння (2). Кубічне відображення в свою чергу генерує значення, що порівнюються з діапазоном першого символу (рис. 6). Номер ітерації, при якому проітероване значення попало у відповідний діапазон слугує шифром цього символу. Процедура повторюється для кожного символу до повного шифрування повідомлення.

Дешифрування повідомлення здійснюється аналогічно шифруванню. При цьому замість символів повідомлення беруться номери інтервалів, що відповідають їх кількості, яку необхідно здійснити, щоб перевірити в який інтервал відповідає отриманому значенню. Отримавши інтервал встановлюється відповідний йому символ вхідного тестового повідомлення.

Внаслідок властивості ергодичності системи інтервалу, що відповідає кожному символу алфавіту буде відповідати певна кількість ітерацій. Отриманий в результаті моделювання частотний розподіл значень ітерацій кубічного відображення приведено на рис. 9.

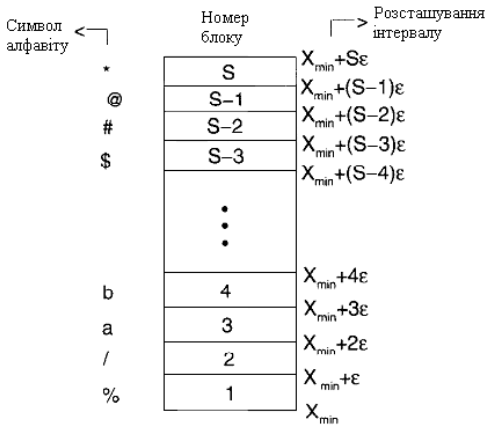


Рис. 6. Розбиття діапазону вихідних значень кубічного відображення на інтервали згідно вибраного алфавіту

Особливості реалізації алгоритму. Моделювання роботи алгоритму шифрування проведено в середовищі Matlab.

Часова залежність варіації змінних x, y і z (рис. 7) вказує на хаотичну поведінку системи Ресслера при зазначених параметрах $p = 0,2$, $q = 0,1$ та $r = 4,5$.

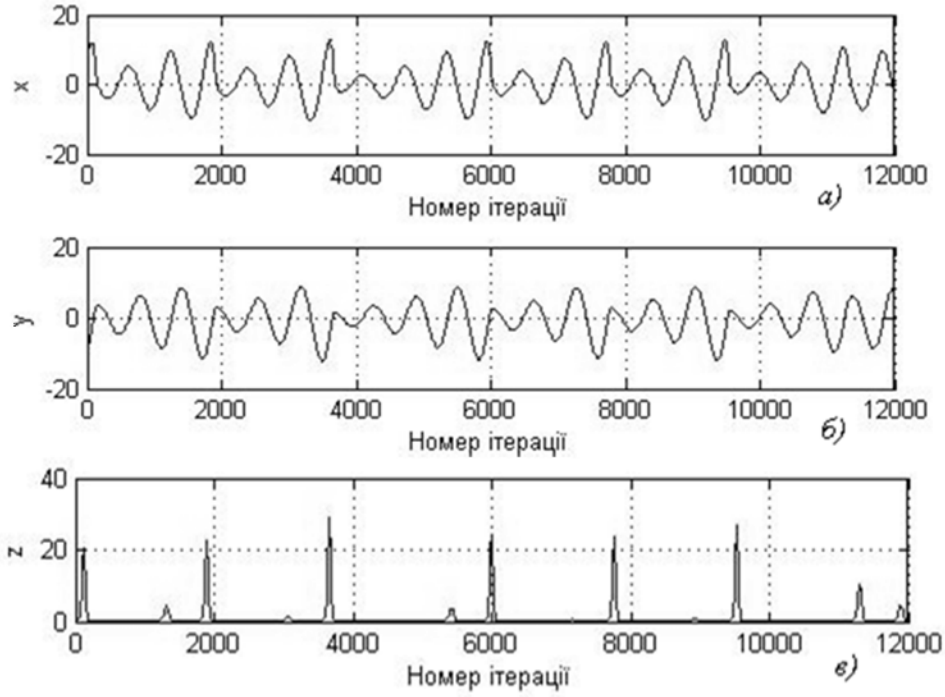


Рис. 7. Часові варіації змінних системи Ресслера: а) залежність зміни змінної x протягом часу, б) залежність зміни змінної y протягом часу, в)залежність зміни змінної z протягом часу

При використанні запропонованого методу шифрування необхідно узгодити вихідні значення вибраної змінної системи Ресслера з діапазоном вхідних значень кубічного відображення. Слід зауважити, що діапазон вихідних значень системи Ресслера є значно більшим у порівнянні з діапазоном вхідних значень кубічного відображення. Внаслідок цього узгодження діапазонів здійснюється відображенням значення змінних системи Ресслера на одиничний відрізок (0;1).

Внаслідок ергодичності системи кубічне відображення в кожен інтервал, що відповідає певному

символу алфавіту буде попадати значна кількість ітерацій (рис. 8).

При шифруванні кожного символу тексту генеруються значення ітерації для інтервалу довжиною $\varepsilon = \frac{x_{\max} - x_{\min}}{S}$, що відповідає символу з обраного алфавіту. Якщо отримане значення ітерації відповідає інтервалу, що відповідає певному символу, то порядковий номер ітерацій n приймається за шифр символу тексту.

Приклад практичної реалізації запропонованого алгоритму шифрування приведено на рис. 9. Програма реалізації алгоритму була написана на мові програмування Delphi 7. Для ілюстрації роботи алгоритму було вибране наступне повідомлення: «A first application of chaos for encryption messages using chaos was proposed Baptista».

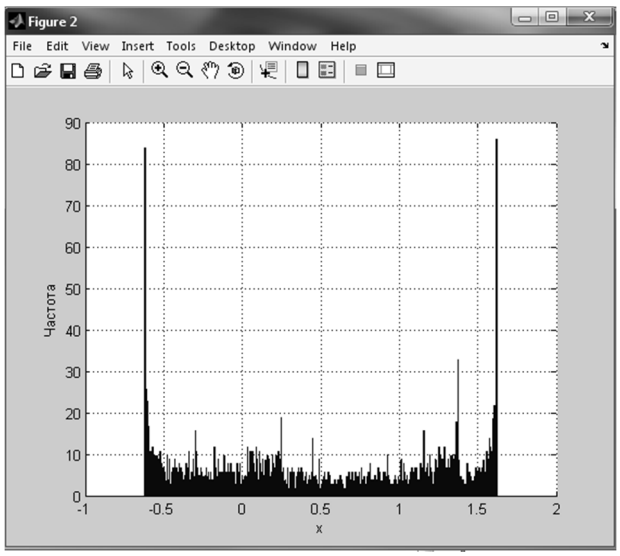


Рис. 8. Частотний розподіл змінної x кубічного відображення для 1000 ітерацій при значеннях параметрів системи при a=0,55, b=2,1 та початковій умові x_0 =0,15

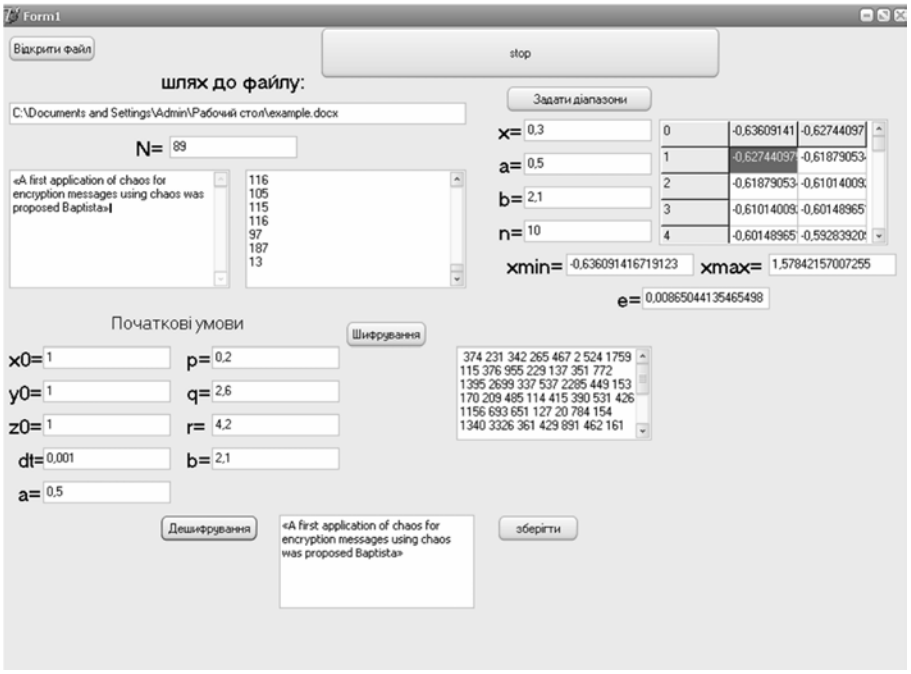


Рис. 9. Програмна реалізація алгоритму шифрування текстової інформації

У вікні програми (рис. 9) приведені всі важливі етапи процесу шифрування. В результаті шифрування було отримано наступне зашифроване повідомлення:

374 231 342 265 467 2 524 1759 115 376 955 229 137 351 772 1395 2699 337 537 2285 449 153 170 209 485 114 415 390 531 426 1156 693 651 127 20 784 154 1340 3326 361 429 891 462 161 716 1083 559 166 1512 415 38 712 145 520 1348 355 44 886 110 13 219 111 1735 751 455 315 665 601 334 76 29 215 813 281 109 623 874 666 23 182 296 448 293 31 517 830 584 775 95.

В процесі дешифрування (рис. 10) було отримано те саме вхідне текстове повідомлення.

Запропонований в роботі алгоритм є більш криптостійким в порівнянні з іншими відомими алгоритмами, наприклад алгоритмом Баптісти [5], що базуються на використанні однієї динамічної системи. В алгоритмі запропонованому в [5] використовується одна динамічна система (логістичне відображення) з однією початковою умовою та одним параметром керування. Таким чином в алгоритмі, запропонованим Баптістою, використовується три ключі шифрування (x_0, r та η). В запропонованому нами алгоритмі підвищення криптостійкості обумовлене використанням двох динамічних систем, що обумовлює збільшення кількості ключів

шифрування з трьох до восьми, а саме $x_0, y_0, z_0, p, q, r, a$ та b. Також використання однієї динамічної системи для генерування початкової умови для другої динамічної системи робить процес шифрування кожного окремого символу унікальним, тобто траєкторія, по якій проходить друга динамічна система, буде індивідуальною для кожного окремого символу. В алгоритмі [5] початковою умовою для шифрування наступного символу є значення змінної, що було отримано при шифруванні попереднього символу.

Висновки:

Збільшення кількості ключів та широкий діапазон їх значень, отриманих згідно запропонованого алгоритму, значно затрудняють підбір використаних в процесі шифрування початкових умов та параметрів систем. Зловмиснику доведеться застосувати всі можливі комбінації ключів $x_0, y_0, z_0, p, q, r, a$ та b, а комбінація двох динамічних систем разом з перетворенням параметрів ще більше ускладнює задачу.

Число часових кроків, що використовуються в якості шифру, не розкриває динаміку системи. Фактично вони не залежать від вибору параметрів. Тому атаку грубої сили здійснити надзвичайно важко. Таким чином, запропонована система забезпечує досить високий рівень захисту даних при передачі по каналах зв'язку.

Даний алгоритм також значно ускладнює можливість статистичного нападу, як форми розподілу частот символів шифрованого повідомлення, що не залежить від природи мови і виду повідомлення.

Запропонований алгоритм шифрування для захищеної системи зв'язку також має перевагу у порівнянні з апаратною реалізацією динамічних систем внаслідок усунення ефектів визваних дрейфом параметрів, стабільністю і т.д. Програмне забезпечення є гнучким щодо частої зміни ключів. Отримані результати показують, що шифрування і дешифрування є досить швидкими і цілком здійсненими.

Запропонований алгоритм представляє собою послідовне шифрування та здійснює вибір між траєкторіями змінних системи Ресслера, використовуючи той самий набір ключів. Таким чином передача даних може відбуватись по відкритих каналах зв'язку, так як її перехоплення і розшифрування вимагає значних апаратних та часових ресурсів. Для того щоб дізнатись який був переданий символ зловмиснику необхідно знати значення генероване кубічним відображенням при його шифруванні, при використанні обчислень з фіксованою точністю в 10 знаків після коми кількість можливих варіантів складає 10^{10} для окремого взятого символу. Тому атака грубої сили буде малоефективною для запропонованого алгоритму.

ЛІТЕРАТУРА

[1]. Шахтарин Б.И., Кобылкина П.И., Сидоркина Ю.А., Кондратьэв А.В., Митин С.В. Генераторы хаотических колебаний. Галилеос АРВ. – Москва. – 2007 – С. 247

[2]. Кузнецов А.П., Савин А.В., Тюрюкина Л.В.Введение в физику нелинейных от ображений // Саратов: изд-во «Научная книга». – 2010. – С. 134.

[3]. Pecora L.M. and Carroll T.L. Synchronization in Chaotic Systems // Phys. Rev Lett. - Vol. 64. – 1990. – P. 821.

[4]. Lawande Q.V., Ivan B. R. and Dhodapkar S. D. Chaos based cryptography: a new approach to secure comunication // BARC. – NEWSLETTER. – No. 258. – July 2005. – P. 1

[5]. Baptista M. S. Cryptography with chaos// Phys. Lett. – A 240. – 1998. – P. 50.

[6]. Arvind T., Chandana S. Nilavan and Prof. Prithviraj V. New approach to information security through nonlinear dynamics and chaos // National Workshop on Cryptology. - Oct. 16-18. – 2003. – Chennai.

[7]. May R.M. Simple mathematical model with very complicated dynamics // Nature 261. – 1976. – P. 459.

REFERENCES

[1]. Shahtarin B.I., Kobylkina P.I., Sidorkina Ju.A., Kondrat'jev A.V., Mitin S.V. Generatory haoticheskih kolebanij. Galileos ARV, Moskva, 2007, P. 247.

[2]. Kuznecov A.P., Savin A.V., Tjurjukina L.V.Vvedenie v fiziku nelinejnyh ot obrazhenij, Saratov: izd-vo «Nauchnaja kniga». 2010, P. 134.

[3]. Pecora L.M. and Carroll T.L. (1990) Synchronization in Chaotic Systems, Phys. Rev Lett., Vol. 64, P. 821.

[4]. Lawande Q.V., Ivan B.R. and Dhodapkar S.D. (2005) Chaos based cryptography: a new approach to secure communication, BARC, Newsletter, No. 258, P. 1.

[5]. Baptista M. S. (1998) Cryptography with chaos, Phys. Lett., A 240, P. 50.

[6]. Arvind T., Chandana S. Nilavan and Prof. Prithviraj V. (2003) New approach to information security through nonlinear dynamics and chaos, National Workshop on Cryptology, Chennai.

[7]. May R.M. (1976) Simple mathematical model with very complicated dynamics, Nature 261, P. 459.

АЛГОРИТМ ШИФРОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ ДВУХ ХАОТИЧЕСКИХ ДИНАМИЧЕСКИХ СИСТЕМ ДЛЯ ЗАЩИЩЕННЫХ СИСТЕМ СВЯЗИ

На современном этапе развитие информационных технологий, средств телекоммуникаций и компьютерной техники широко встает проблема защиты конфиденциальной информации от несанкционированного доступа при ее передаче или хранении. Чтобы решить данную проблему часто обращаются к криптографическим методам защиты информации. Кроме методов шифрования, основанные на алгебраических понятиях, проводятся разработки алгоритмов на основе детерминированного хаоса. В данной работе представлены алгоритм шифрования текстовой информации, основанный на использовании двух динамических систем, системы Ресслера и кубического отображения. Система Ресслера используется для генераций начальных условий, используется кубическим отражением при шифровании каждого отдельного символа текстового сообщения. В результате работы данного алгоритма символы входящего сообщения в результате шифрования заменяются целые числа. В работе также было проведено моделирование работы динамических систем в среде Matlab и приведены пример работы программы написанной на языке Delphi 7. В работе также дана оценка защищенности предложенного алгоритма. Алгоритм обладает большим количеством ключей шифрования, что делает процесс их подбора очень сложным. Использование двух динамических систем затрудняет возможность статистической атаки.

Ключевые слова: криптография, шифрование, дешифрование, динамическая система, хаос, алгоритм оценки уровня защищенности.

INFORMATION ENCRYPTION ALGORITHM BASED ON TWO CHAOTIC DYNAMIC SYSTEMS FOR SECURE COMMUNICATION SYSTEMS

At the present stage of development of information technology, telecommunication equipment and computer equipment commonly raises the problem of protecting confidential information against unauthorized access when it is transmitting or storing. To solve this problem often turn to cryptographic methods of information security. In addition to encryption methods based on algebraic concepts, conducted the development of algorithms based on deterministic chaos. In this paper presents an algorithm encrypt text data, based on the use of two dynamical systems, systems Roessler and cubic map. Ressler system used for generation of the initial conditions used cubic map when encrypting each character of message. As a result of this algorithm plaintext symbols incoming messages by encrypting replaced by integers. The work was also carried out modeling of dynamic systems in Matlab environment and given an example an example of the application written in Delphi 7. In this paper also assessed the security of the proposed algorithm. The algorithm has a large number of encryption keys, that making the process of their selection is very difficult. Using two dynamic systems complicates the possibility of statistical attacks.

Keywords: cryptography, encryption, decryption, dynamical systems, chaos, algorithm, evaluation of security.

Косован Григорій Васильович, аспірант кафедри радіотехніки та інформаційної безпеки Чернівецький національний університет імені Юрія Федьковича.
E-mail: spell1985@mail.ru
Косован Григорий Васильевич, аспірант кафедры радиотехники и информационной безопасности, Черновицкий национальный университет имени Юрия Федьковича.
Kosovan Gregorii, Postgraduate student, Department of the Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University.

Кушнір Микола Ярославович, кандидат фізико-математичних наук, доцент кафедри радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича.
E-mail: kushnirnick@gmail.com
Кушнир Николай Ярославович, кандидат фізико-математических наук, доцент кафедри радиотехники и информационной безопасности, Черновицкий национальный университет имени Юрия Федьковича.
Kushnir Mykola, docent, Department of the Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University.

Політанський Леонід Францович, доктор технічних наук, професор, завідувач кафедри радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича.
E-mail: spell1985@mail.ru
Политанский Леонид Францевич, доктор технических наук, професор, заведующий кафедры радиотехники и информационной безопасности, Черновицкий национальный университет имени Юрия Федьковича.
Politanskii Leonid, Professor, Department of the Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University.