УДК 621.391
М.О. Слободян, М.О. Лівчук, С.К. Підченко, докт. техн. наук, проф.
Хмельницький національний університет, Україна

АЛГОРИТМ ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ ДИСКРЕТНИХ ХАОТИЧНИХ ПОСЛІДОВНОСТЕЙ

M.O. Slobodian, M.O. Livchuk, S.K. Pidchenko, Dr., Prof.

DATA ENCRYPTION ALGORITHM USING DISCRETE CHAOTIC SEQUENCES

Важливими аспектами проектування та розробки телекомунікаційних систем є захист та конфіденційність інформації. В роботі запропоновано алгоритм шифрування вихідного байтового масиву хаотичними числовими послідовностями, отриманими за допомогою дискретної моделі динамічної системи Лоренца [1, 2].

Дискретно-часова система Лоренца може бути задана у вигляді системи нелінійних дискретних відображень:

$$\begin{cases} x(n+1)=\sigma\big(y(n)-x(n)\big)\Delta t+x(n) \\ y(n+1)=\big(x(n)\big(r-z(n)\big)-y(n)\big)\Delta t+y(n), \\ z(n+1)=\big(x(n)\,y(n)-bz(n)\big)\Delta t+z(n) \end{cases} \quad (1)$$

де $\sigma=10$, $r=28$, $b=8/3$ – параметри системи, Δt – час дискретизації.

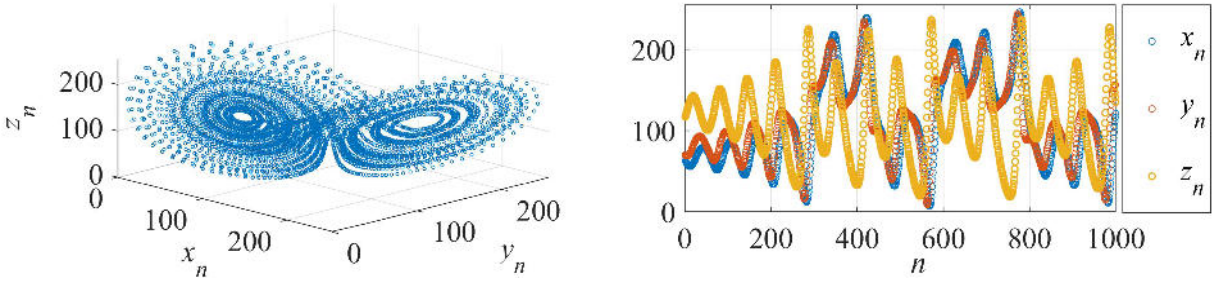
Для вказаних значень параметрів система (1) демонструє нестійкість фазових траєкторій та сильною залежністю від початкових умов, про що свідчить додатне значення старшого показника Ляпунова $\lambda_0>0$ [1, 2].

Отримані в результаті ітеративної процедури псевдовипадкові числові послідовності перетворюються в цілі двійкові числа згідно виразу:

$$w(n)=\left\lfloor \big(x(n)-l\big)/\big(h-l\big)\cdot\big(2^k-1\big)\right\rfloor, \quad (2)$$

де k – розрядність двійкового представлення цілого числа,
h, l – відповідно максимальне та мінімальне значення послідовності x.

Фазовий портрет системи та діаграма хаотичних послідовностей показані на рис. 1.



а) б)

Рисунок 1. Фазовий портрет атрактора (а), та діаграми хаотичних послідовностей (б)

Вихідний байтовий масив b, що представляє собою інформаційне повідомлення, побітово сумується за модулем 2 з хаотичною послідовністю w. Отриманий в результаті шифрування код передається захищеним або відкритим каналом зв'язку та дешифрується на приймальній стороні аналогічним чином. Ключем шифру є дійсний вектор початкових значень $K=\big[x(0),y(0),z(0)\big]$. Криптографічна стійкість системи залежить від кількості можливих ключів шифрування [3]. Наприклад, дійсні числа,

представлені у форматі з плаваючою комою подвійної точності мають 15 значущих цифр [4], тоді кількість ключів становитиме приблизно:

$$N_K \approx \left(10^{15}\right)^3 = 10^{45} \tag{3}$$

Операції шифрування та дешифрування виконуються однією процедурою, блок-схема алгоритму якої зображена на рис. 2.

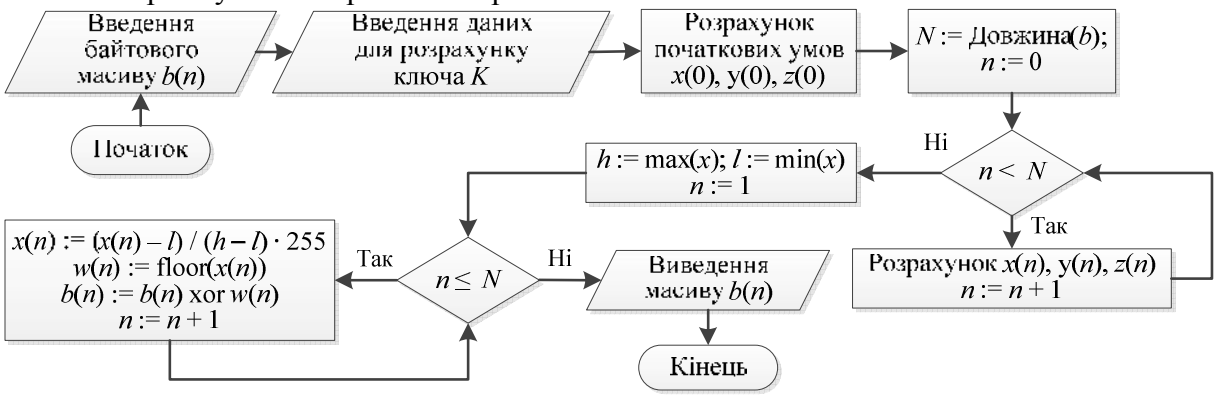
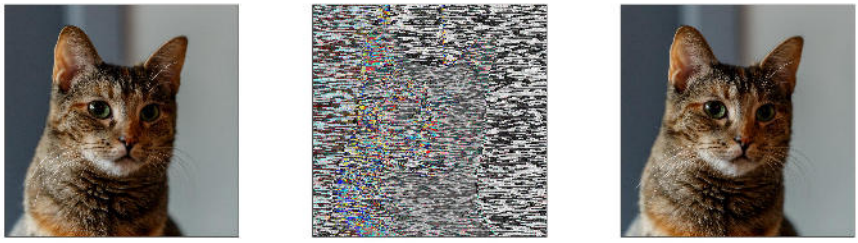


Рисунок 2. Алгоритм шифрування/дешифрування вихідного байтового масиву *b*

Описаний алгоритм шифрування (рис. 2) був реалізований на мові програмування Python 3. На рис.3 показано результат роботи програми на прикладі шифрування та дешифрування растрового зображення у форматі .jpeg розміром 1000×1000 пікселів.



а) б) в)

Рисунок 3. Результат роботи програми шифрування:
вихідне зображення (а), після шифрування (б), після дешифрування (в)

В результаті науково-практичного дослідження можна зробити наступні висновки:

1. Математичні моделі нелінійних систем із хаотичною динамікою можуть бути ефективно використані в якості генераторів послідовностей псевдовипадкових чисел в алгоритмах шифрування. Сильна чутливість до початкових умов забезпечує високу криптостійкість систем, побудованих на їх основі.

2. Описаний алгоритм шифрування даних за допомогою дискретних хаотичних послідовностей, згенерованих на основі динамічної системи Лоренца, дозволяє здійснювати шифрування і дешифрування довільних байтових послідовностей та може бути застосований в конфіденційних системах зв'язку, в тому числі телемедичних.

Література

1. Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А.С. Дмитриев, А.И. Панас. – М. : Изд-во Физико-математической литературы, 2002. – 252 с.

2. Прикладне застосування теорії хаотичних систем у телекомунікаціях: монографія / [Ю.Я. Бобало, С.Д. Галюк, М.М. Климаш, Р.Л. Політанський]; Нац. ун-т «Львів. політехніка». – Львів: Коло, 2015. – 178 с.

3. Политанский Р.Л. Система передачи данных с шифрованием хаотическими последовательностями / Р.Л. Политанский, М.П. Шпатарь, А.В. Гресь, А.Д. Верига // Технология и конструирование в электронной аппаратуре. – 2014. – № 2-3. – С. 28–32.

4. Генри С. Уоррен. Числа с плавающей точкой // Алгоритмические трюки для программистов = Hacker's Delight. — М.: Вильямс, 2007. – С. 288.