УДК 004.056.55+003.26.09

Старший викладач Копичко С.М., студент Легеза Д.В.

Національний технічний університет України
«Київський політехнічний інститут»

МОДЕЛЬ ШИФРУВАННЯ ІЗ ЗАСТОСУВАННЯМ ТЕОРІЇ ХАОСУ

Abstract

Sergiy M. Kopychko, senior lecturer; Dmytro V. Legeza, student
Encryption model based on chaos theory

In this work the method of encryption based on chaos theory was formulated. Encryption algorithm based on chaos theory was created and tested on cryptostability. These results indicate the adequacy of the proposed method and the potential to use it for encrypting data.

Вступ

Шифрування є криптографічним методом, що найбільш широко використовується для збереження конфіденційності інформації, він захищає дані від несанкціонованого доступу до них.

Криптографічні методи можуть бути класифіковані різним чином.

Один із методів класифікації полягає у поділі в залежності від кількості ключів, які використовуються у відповідному криптоалгоритмі [1-4]:

1. Безключові, в яких не використовуються будь-які ключі;
2. Одноключеві (симетричні) – в них використовується якийсь додатковий ключовий параметр - зазвичай це секретний ключ;
3. Двохключеві (асиметричні), які використовують у своїх обчисленнях два ключі: закритий і відкритий.

У роботі розглядаються одноключеві методи шифрування. Існуючі криптометоди є дієвими, хоча й використовують класичні математичні методи (гамування складними алгебраїчними функціями). Саме тому існує нагальна необхідність вдосконалення або створення нових алгоритмів шифрування на основі сучасного математичного апарату.

У роботі описується новий криптоалгоритм, що використовує у вигляді математичного апарату методики детермінованого хаосу.

Постановка задачі

Мета роботи – аналіз методів шифрування на основі хаосу, розробка нового алгоритму шифрування із застосуванням теорії хаосу або вдосконалення вже існуючого та дослідження його на стійкість.

Термінологічний словник

Гамма – псевдовипадкова послідовність байтів, що додається до вихідних даних за модулем 2 з метою усунення в них можливих статистичних залежностей.

Гамування – метод шифрування, що оснований на «накладанні» гаммапослідовності на відкритий текст. У більшості випадків використовується додавання у певному скінченному полі (у полі GF(2) таке додавання перетворюється в операцію виключаючого АБО – XOR). Для розшифрування інформації операція гамування проводиться ще раз.

Шифртекст – інформація, до якої застосована операція шифрування.

Відмінність методу шифрування за допомогою теорії хаосу від традиційних методів шифрування

У роботі пропонується підхід до використання фрактальних ітераційних функцій в шифруванні інформації. Запропонований підхід є варіантом гамування – процесу "накладання" гаммапослідовності на відкриті дані, де в якості гаммапослідовності (послідовності псевдовипадкових елементів) використовується фрактальна послідовність.

Ключовою проблемою технічних засобів захисту інформації є породження випадкової послідовності бітів. Ідея застосування фрактальних сигналів як псевдовипадкових послідовностей виходить з припущення можливості описання поведінки фізичних та природних систем за допомогою фракталів [5].

Принцип роботи методу наведено на рис. 1 [6]. Як видно із схеми, спочатку за допомогою функції гамування створюється гамма послідовність, яка залежить від параметра *K*. Після цього до вихідного сигналу та отриманої гамми застосовується операція *mod2*.

Початкові параметри ітераційної функції, що забезпечують вибір одного перетворення із сукупності можливих для даного алгоритму, є криптографічним ключем. Ітераційна функція, що породжує фрактальну послідовність, є обчислювально незворотною функцією. Іншими словами, обчислення зворотного перетворення не може бути зроблено більш

ефективним способом, ніж перебором по множині можливих значень початкових параметрів функції.

Аналіз результатів роботи алгоритму шифрування

В ролі нелінійного елемента запропоновано використовувати асиметричне відображення, яке називається «наметове» (tent):

$$x_{n+1} = \begin{cases} \dfrac{x_n}{\mu}, x_n \in [0, \mu) \\ \dfrac{1 - x_n}{1 - \mu}, x_n \in [\mu, 1] \end{cases}, \quad \text{де } \mu \in (0,1),$$

де μ – параметр відображення; x_n – базова, а x_{n+1} – шукана точки перетворення.

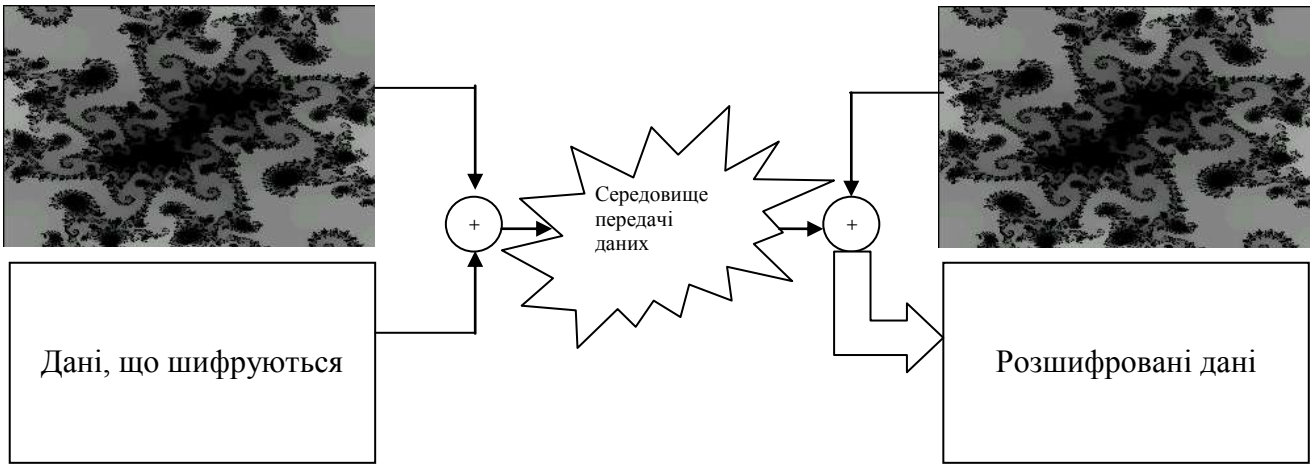

Рис.1. Принцип роботи методу шифрування на основі хаосу

В якості базового модуля алгоритму обрана схема з нелінійним підмішуванням інформаційного сигналу в хаотичний (рис. 2).

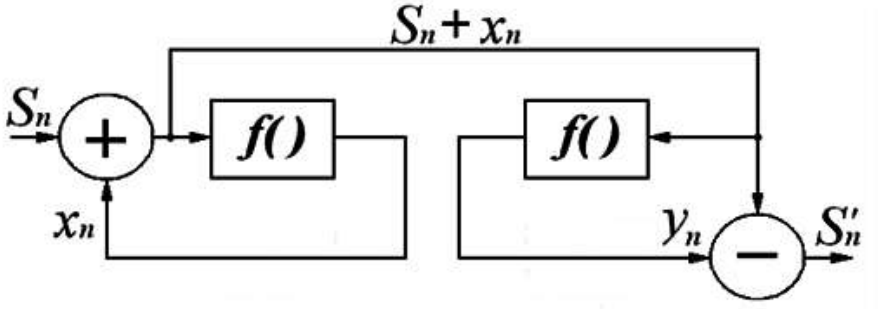

Рис. 2. Схема кодування інформації з нелінійним підмішуванням інформаційного сигналу

Тут S_n – вхідний інформаційний сигнал; x_n, y_n - хаотичний сигнал; S_n' - розшифрований сигнал; S_n+x_n – зашифрований сигнал.

Отримана таким чином схема шифрування може використовуватися для кодування будь-якого виду інформації. Одним з найскладніших видів сигналів для кодування є графічна інформація. Тому в роботі розглядається кодування зображень (рис.3, 4).

В якості тестового вибрано чорно-біле зображення розміром 257 × 350 пікселів з 256 градаціями сірого. Зображення і його спектр наведено на рис. 4 і рис. 5 відповідно.

Рис. 3. Вихідне зображення

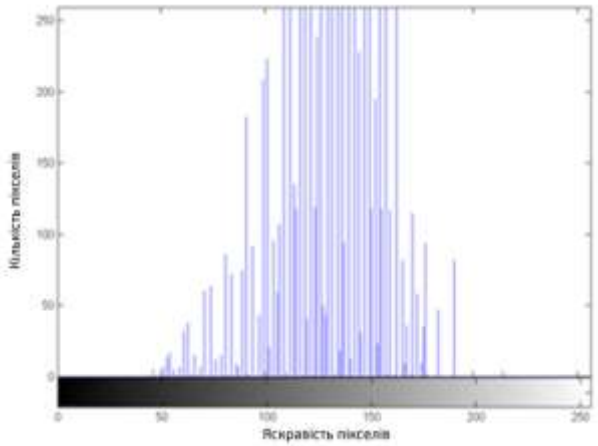

Рис. 4. Спектр яскравості кольорів пікселів зображення на рис. 3

Перші тести по застосуванню цього алгоритму для шифрування інформації показали його потенційну придатність для криптографічного кодування. У зашифрованому зображенні не виявлено ніяких структур (рис. 5), і його спектр яскравості кольорів пікселів став однорідним (рис. 6).

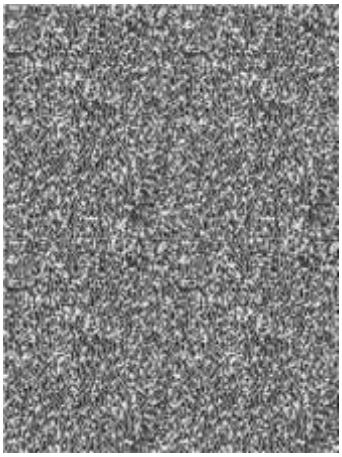

Рис. 5. Результат кодування тестового зображення при значенні параметра $\mu = 0.4$

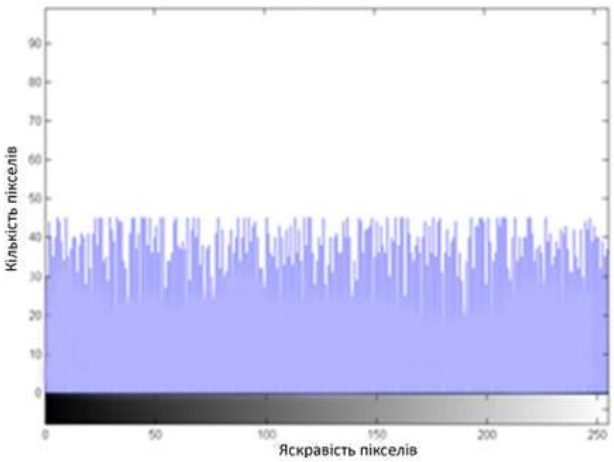

Рис. 6. Спектр яскравості кольорів пікселів шифрованного зображення на рис. 5

1) даний криптоалгоритм підтвердив потенційну можливість його використання для шифрування інформації;
2) унеможливлюється використання візуального криптоаналізу для дешифрації інформації, оскільки у зашифрованій інформації не виявлено ніяких структур, крім того спектр яскравості пікселів зображення став однорідним;
3) при найменших змінах параметрів та початкових умов (зміни $>10^{-9}$), отримано абсолютно різні шифри;
4) при розшифруванні інформації спотворені біти даних у шифртексті позначаються локально і не впливають на всю зашифровану інформацію.

Література

1. *Баричев С. В.* Криптография без секретов. – М.: Наука, 1998. – 120 с.
2. *Диффи У.* Первые десять лет криптографии с открытым ключом // ТИИЭР – 1988 – т. 76 – С. 54-74.
3. Панасенко С.П. Назначение и структура алгоритмов шифрования //Русский Bugtraq. – 2002. [Електронний ресурс]. URL: http://www.ixbt.com/soft/alg-encryption.shtml (12.02.2011).
4. Панасенко С.П. Применение шифрования и стойкость RSA // IXBT. – 2006. [Електронний ресурс]. URL: http://www.bugtraq.ru/library/crypto/rsa.html (14.02.2011).
5. *Александров В. В.* Развивающиеся системы. В науке, технике, обществе и культуре: учебное пособие. – СПб: СПбГТУ, 2000. — 243 с.

6. *Гуляев Ю. В.* Математика и физика фракталов: теоремы, модели, некоторые результаты / Никитов С.А., Матвеев Е.Н., Потапов А.А. // Праці XLVI наукової конференції МФТИ «Современные проблемы фундаментальных и прикладных наук». – М.: Долгопрудный: МФТИ (ГУ). Частина V «Квантовая и физическая электроника». - 2003. – С.103-104.