В даній роботі запропонований алгоритм шифрування інформації з використанням послідовностей псевдовипадкових дійсних чисел, підпорядкованих розподілу Гауса. Дослідження алгоритму на криптостійкість підтверджують можливість використання такого алгоритму для шифрування інформації

Ключові слова: псевдовипадкова послідовність, генератор, розподіл Гауса, криптостійкість

В данной работе предложен алгоритм шифрования информации с использованием последовательностей псевдослучайных действительных чисел, подчиненных распределению Гаусса. Исследование алгоритма на криптостойкость подтверждает возможность использования такого алгоритма для шифрования информации

Ключевые слова: псевдослучайная последовательность, генератор, распределение Гауса, криптостойкость

УДК 621.391

ШИФРУВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПСЕВДОВИПАДКОВИХ ГАУСОВИХ ПОСЛІДОВНОСТЕЙ

Р.Л. Політанський
Кандидат фізико-математичних наук, доцент*
Контактний тел.: (03722) 4-24-36
E-mail: polroos@mail.ru
П.М. Шпатар
Кандидат технічних наук, доцент*
Контактний тел.: (03722) 4-24-36
О.В. Гресь
Аспірант*
*Кафедра радіотехніки та інформаційної безпеки**
Контактний тел.: (03722) 4-24-36
E-mail: alexgs85@ukr.net
В.Я. Ляшкевич
Кандидат технічних наук, доцент
Кафедра комп'ютерних систем та мереж**
Контактний тел.: (0372) 52-64-46
E-mail: vaslya@chnu.edu.ua
**Чернівецький національний університет ім. Юрія Федьковича
вул. Коцюбинського, 2, м. Чернівці, Україна, 58012

1. Вступ

Швидкий розвиток електронних засобів телекомунікацій сприяв розробленню принципово нових методів кодування, шифрування та передавання інформації, зокрема криптографічних методів, що ґрунтуються на теорії динамічних систем з притаманними їм властивостями хаосу. Криптографічні методи захисту інформації при її передаванні залишаються найбільш стійкими і захищеними.

У більшості методів та алгоритмів шифрування, особливо потокових шифрах, використовуються генератори ключової послідовності, що видає потік бітів, що може бути точно відтвореним одержувачем інформації, а для стороннього спостерігача є випадковим. Чим більше подібність генерованого потоку випадкому, тим більше часу необхідно затратити криптоаналітику для злому шифру.

Генератори випадкових чисел використовуються для моделювання випадкових даних відповідно до заданої функції розподілу. Послідовності випадкових чисел застосовують в обчислювальних алгоритмах (метод Монте-Карло), комп'ютерному моделюванні, кодуванні інформації. Маючи випадкову послідовність із заданим розподілом, можна моделювати помилки вимірювань, варіації природних факторів, тощо [1].

Побудова генератора випадкової послідовності з заданою функцією розподілу здійснюється шляхом перетворення рівномірно розподілених на відрізку [0,1] чисел. Рівномірно розподілену випадкову послідовність можна отримати, використовуючи лінійний генератор.

2. Алгоритм шифрування

В даній роботі запропонований алгоритм шифрування інформації, з використанням послідовностей псевдовипадкових дійсних чисел, розподілених за законом Гауса, що є хорошою моделлю шуму.

Блок-схема алгоритму шифрування приведена на рис. 1.

Алгоритм шифрування базується на псевдовипадковому генераторі ключа, основою яких є два лінійних конгурентних генератори псевдовипадкових послідовностей.

Одним із поширених алгоритмів, формування псевдовипадкової послідовності є формування послідовності бітів, значення яких визначається належністю певного числа до однієї з двох підмножин $\left[0;\frac{1}{2}\right]$, $\left(\frac{1}{2};\ 1\right]$, множини дійсних чисел [0;1].

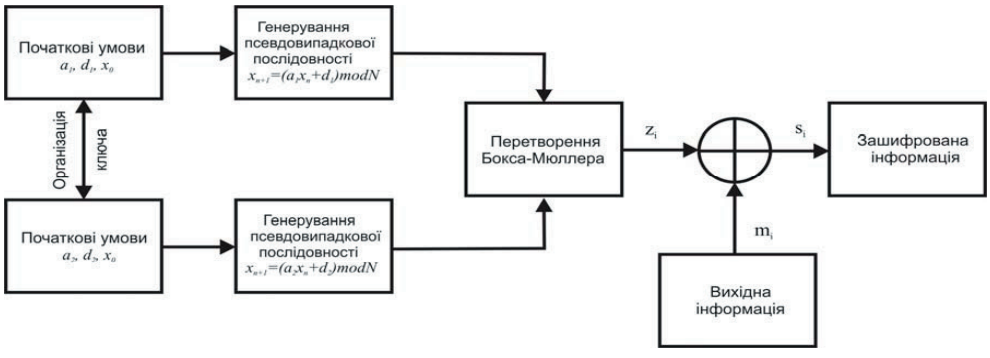


Рис. 1. Блок-схема алгоритму шифрування

В загальному випадку схема генерування псевдовипадкових послідовностей чисел описується виразом [2]:

$$x_{n+1}=(a\cdot x_n+d)\bmod N, \quad (1)$$

де x_n, x_{n+1} – значення системи на n-ій та n+1-ій ітерації; N – натуральне число, x_0, a, d $\in \{0, 1, \ldots, N-1\}$ – параметри системи, а «mod» означає арифметичний оператор знаходження залишку від результату ділення цілих чисел.

Такий генератор є лінійним та періодичним. Максимальне значення на його виході досягається за умови, що числа d і N є взаємно простими; якщо деяке просте число p є дільником N, та число a–1 повинно бути кратним числу p.

Схема генерування ключа використовує два лінійні генератори псевдовипадкових послідовностей, які працюють з різними початковими умовами:

$$x_{n+1}=(a_1\cdot x_n+d_1)\bmod N,\ x_{n+1}=(a_2\cdot x_n+d_2)\bmod N, \quad (2)$$

де a_1, d_1, a_2, d_2 - початкові умови для генерування послідовностей.

Вихідні послідовності цих генераторів перетворюються за допомогою алгоритму Бокса-Мюллера (3) в послідовність псевдовипадкових дійсних чисел, що належать інтервалу [-1;1], розподілених за законом Гауса. В основу алгоритму Бокса-Мюллера закладені наступні співвідношення [2]:

$$\nu=x_1^2+x_2^2,\ y_1=x_1\cdot\sqrt{\frac{-2\log(\nu)}{\nu}},\ y_2=x_2\cdot\sqrt{\frac{-2\log(\nu)}{\nu}}, \quad (3)$$

де x_1, x_2 два числа, отримані від генератора випадкових чисел, а y_1, y_2 - два псевдовипадкових нормально розподілених числа. Якщо при цьому сума квадратів чисел x_1 та x_2 є більшою за 1, тобто $\nu=x_1^2+x_2^2$, то даний результат пропускається та вибирається наступне випадкове число.

Роботу алгоритму розглянемо на прикладі шифрування зображень. Алгоритм шифрування здійснюється наступним чином. З кожного пікселя зображення зчитуються градації R,G,B-кольорів, що представляються двійковими 8-и бітовими числами, утворюючи множину M_n. Згенерована послідовність дійсних чисел перетворюється в двійкове 8-и бітове представлення за допомогою наступної формули:

$$z_n=0,b_{n1},b_{n2}\ldots b_{nL}=2^{-1}b_{n1}+2^{-2}b_{n2}+\ldots+2^{-L}b_{nL}, \quad (4)$$

де L – розрядність двійкового представлення.

Множина Z_n утворюється як послідовність біт $\{b_{n1},b_{n2}\ldots b_{nL}\}$. Елементи інформаційного повідомлення m_i сумуються з елементами псевдовипадкової послідовності z_i з використанням операції XOR:

$$s_i = m_i \oplus z_i. \quad (5)$$

Дешифрування здійснюється аналогічно завдяки зворотності операції XOR [3].

3. Реалізація алгоритму

Практична реалізація алгоритму здійснена в програмному середовищі Delphi 7.0.

Часова залежність псевдовипадкової ключової послідовності, розподіленої за законом Гауса, що використовується для шифрування приведена на рис. 2

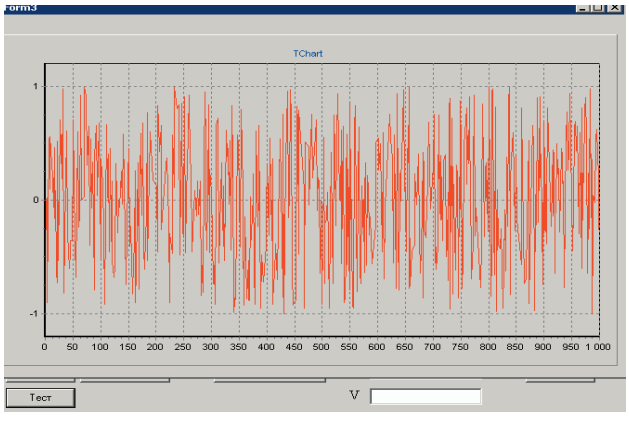


Рис. 2. Псевдовипадкова ключова послідовність

На рис. 3. приведене вихідне та зашифроване зображення. Шифрування здійснюється за описаним алгоритмом.

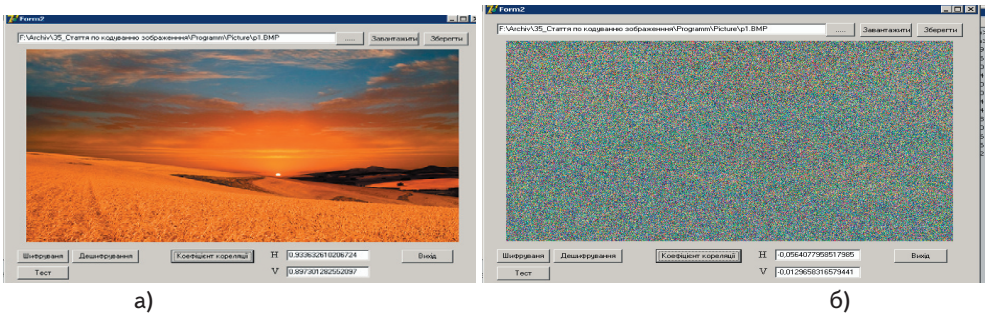
Оцінка ефективності алгоритму шифрування здійснювалась за значенням коефіцієнта кореляції між суміжними пікселями вихідного та зашифрованого зображень [3,4].

Коефіцієнт кореляції між суміжними пікселями зображення визначається за наступною формулою:

$$C_p=\frac{N\sum_{j=1}^{N}x_jy_j-\sum_{j=1}^{N}x_j\sum_{j=1}^{N}y_j}{\sqrt{N\left\{\sum_{j=1}^{N}x_j^2-\left(\sum_{j=1}^{N}x_j\right)^2\right\}}\sqrt{N\left\{\sum_{j=1}^{N}y_j^2-\left(\sum_{j=1}^{N}y_j\right)^2\right\}}}, \quad (6)$$

де x,y- значення градацій кольорів для двох суміжних пікселів зображення,

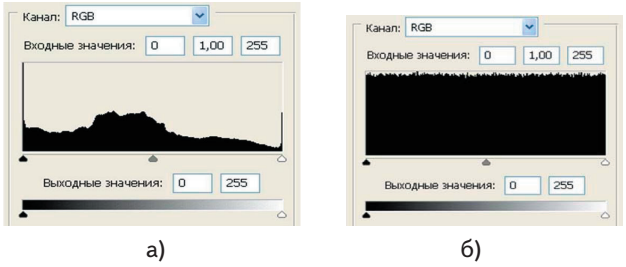
N- число пікселів зображення які вибрані для розрахунку коефіцієнту кореляції.



а) б)

Рис. 3. Вихідне а) та зашифроване б) зображення

Для вихідного зображення коефіцієнт кореляції становить 0,85...0,98. Проведені експерименти з різними зображеннями показали, що коефіцієнт кореляції між суміжними пікселями зображень, зашифрованих запропонованим алгоритмом не перевищував 0,01...0,06. Отримані результати підтверджують криптостійкість шифрування зображень за запропонованим алгоритмом.



а) б)

Рис. 4. Гістограми для вихідного а) та зашифрованого б) зображень

Також для даного алгоритму був проведений гістограмний аналіз, який демонструє розподіл пікселів в кожному рівні інтенсивності кольору (рис. 4) [5,6].

На рис. 4а зображена гістограма оригінального кольорового зображення, а на рис. 4б відповідна гістограма для зашифрованого зображення.

Крім шифрування зображення, даний алгоритм також може шифрувати будь-які інші файли, наприклад, текстові.

4. Висновки

В роботі продемонстровано алгоритм шифрування інформації, що базується на використанні в якості ключа двох генераторів псевдовипадкових послідовностей, вихідні послідовності яких підпорядковуються розподілу Гауса.

Ефективність алгоритму була перевірена за допомогою кількісного показника коефіцієнта кореляції, який для зашифрованого зображення знаходиться в межах 0,01÷0,06.

Отримані результати вказують на високу криптостійкість запропонованого алгоритму.

Література

1. Долгов, В.А. Криптографические методы защиты информации. Курс лекцій [Текст] / В.А. Долгов, В.В. Анисимов. – Хабаровск.: Издательство ДВГУПС, 2008. – 155с.
2. Преобразование Бокса-Мюллера. Доступно на: http://ru.wikipedia.org
3. Pareek, N.K Image encryption using chaotic logistic map [Текст] / Pareek N.K., Vinod Patidara, Sud K.K. // Image and Vision Computing 24 – 2006 – Pp. 926–934.
4. Болтенко, В.А. Анализ алгоритмов хаотического шифрования зображений [Текст] / Болтенков В.А., Никольский Е.С. // Цифрові технології/ № 7 – 2010 – С. 61-66.
5. Pareek, N.K. Cryptography using multiple one-dimensional chaotic maps [Текст] / Pareek N.K., Patidar V, Sud K.// Commun. Nonlinear Sci. Numer. Simul./ №10(7) – 2005 – Pp.715–723.
6. Liu, S.An Improved Image Encryption Algorithm Based on Chaotic System [Текст] / Liu S., Sun J., Xu Zh.// Journal of Computers./ №11.Vol.4 – 2009 – Pp. 1091-1100.
7. Іванюк, П.В. Дослідження хаотичних процесів, генерованих системою Лю [Текст] / П.В. Іванюк, Л.Ф. Політанський, Р.Л. Політанський // Восточно-Европейский журнал передовых технологий. – 2011. – №4/9(52). – С. 11 – 15.

Abstract

The rapid progress of the electronic telecommunications has contributed to the development of the innovative methods of encoding, encryption and transmission of information, including the cryptographic techniques. The cryptographic techniques of information security in its transmission are the most stable and secure.

The article suggests an algorithm of the information encryption using sequences of pseudorandom real numbers distributed according to Gauss law, which is a good model of noise. The encryption algorithm is based on the pseudorandom key guns, which are based on two linear congruous generators of pseudorandom sequences.

Practically, the algorithm was implemented in the software environment Delphi 7.0. The effectiveness of the algorithm was tested using a quantitative index of the correlation coefficient, the range of which is 0,01 ÷ 0,06 for the encrypted image. The results indicate the high cryptographic security of the suggested algorithm

Keywords: *pseudorandom sequence, generator, Gaussian distribution, cryptographic security*