УДК 004.056

О.В. Гресь, В.М. Косован, М.І. Скрипський, Г.М. Розорінов, П.М. Шпатар

АНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ХАОТИЧНИХ ВІДОБРАЖЕНЬ

В даній роботі запропонований модифікований алгоритм шифрування інформації, з використанням ключових послідовностей генерованих на основі хаотичних відображень. Також запропоновано удосконалення перетворення дифузії, що підвищує чутливість алгоритму до вхідних параметрів. Дослідження алгоритму на криптостійкість підтверджують можливість використання такого алгоритму для шифрування інформації.

Ключові слова: дифузія, генератор, псевдовипадкова послідовність, нормальний розподіл, хаотичне відображення, криптостійкість.

Вступ

Швидкий розвиток інтернет – технологій, засобів телекомунікаційвимагає забезпеченнявисокоїприхованості таконфіденційностіінформації, що передається по каналах зв'язку. Забезпечення конфіденційності інформації сучасних телекомунікаційних систем можливе шляхом її шифрування інформації за допомогою хаотичних послідовностей. Тому в останній час широкого розвитку набули криптографічні методи захисту інформації, що ґрунтуються на теорії динамічних систем [1,2].

Найкращим способом захисту інформації, з точки зору швидкості та складності обчислень, є побітове додавання по модулю 2 вхідної інформаційної послідовності з певною ключовою послідовністю, що може бути сформована наприклад генератором хаотичних послідовностей. В якості ключових послідовностей можуть використовуватися псевдохаотичні послідовності, алгоритми генерування яких реалізовані на базі явища динамічного хаосу , що є чутливим до зміни початкових умов.Чим більша подібність генерованого потоку випадковому, тимбільше часу необхідно затратити криптоаналітику для розкриття шифру [1,2].

1. Алгоритм шифрування

В даній роботі проведено дослідження та модифікування алгоритму шифрування інформації, з використанням генераторів псевдовипадкових послідовностей на основі дискретних одномірних відображень [2,3].

Алгоритм генерування ключа базується на використанні роботи двох незалежних генераторів псевдовипадкових послідовностей з рівномірним розподілом, лінійного конгруентного генератора (1), та генератора на основі логістичного відображення (2), що працюють з різними початковими умовами [3]:

$$x_{n+1} = (a_1 \cdot x_n + d_1) \bmod N , \qquad (1)$$

де x_n, x_{n+1} – значення системи на n-й та $n+1$ -й ітерації; N –натуральне число;
$x_0, a, d \in \{0,1,\ldots,\mathrm{N}-1\}$ – параметри системи;

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

де a_1, d_1 , λ, x_0- початкові умови для генерування послідовностей.

Вихідні послідовності цих генераторів за допомогою алгоритму Бокса-Мюллера перетворюються в нормально розподілену послідовність (за законом Гауса) [4].

Блок-схема алгоритму шифрування приведена на рис. 1.

Рис. 1. Блок-схема алгоритму шифрування

2. Практична реалізація алгоритму

Практична реалізація алгоритму здійснена в програмному середовищі Delphi 7.0.

Вигляд ключової послідовності, (утвореної після перетворення Бокса-Мюллера), що використовується для шифрування приведена на рис. 2.

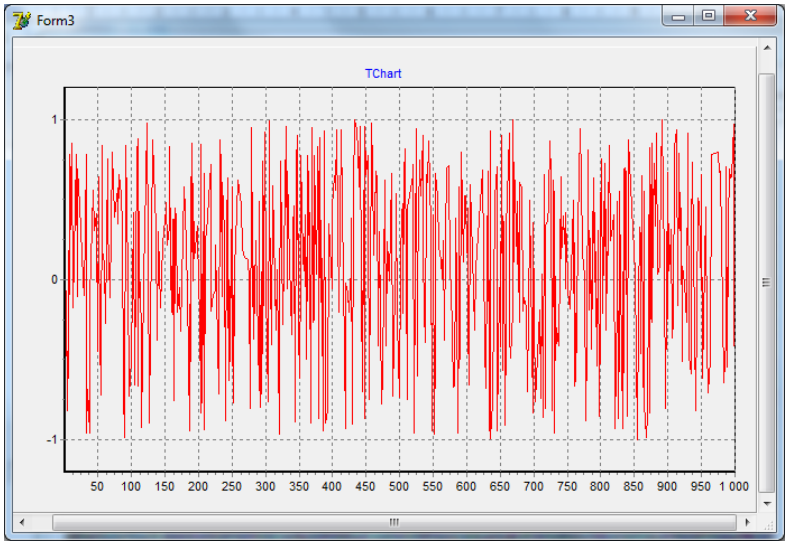


Рис.2. Вигляд ключової послідовності,
що використовується для шифрування

Шифрування інформації, здійснюється за схемою, наведеною на рис. 3.

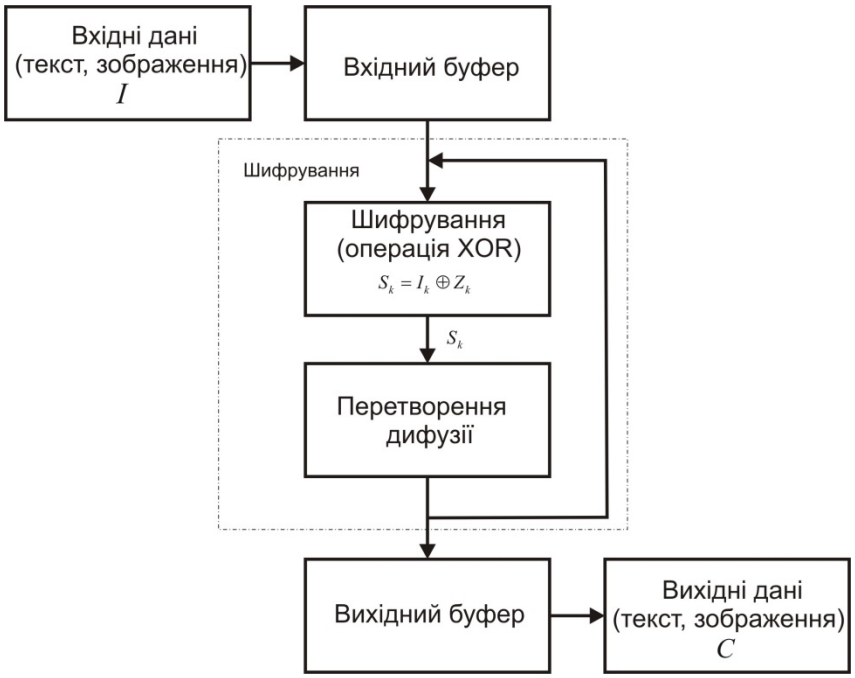


Рис.3. Схема роботи алгоритму

Роботу алгоритму розглянемо на прикладі шифрування текстових повідомлень. У випадку шифрування тексту процес проходить побайтово. Вихідне повідомлення перетворюється в 8-и бітові числа згідно ASCII коду, утворюючи множину I.

Згенерована ключова послідовність дійсних чисел перетворюється в двійкове 8-и бітове представлення за допомогою наступної формули [5]:

$$z_n = 2^{-1} b_{n1} + 2^{-2} b_{n2} + ... + 2^{-L} b_{nL}, \quad (3)$$

де: L– розрядність двійкового представлення.

Кількість згенерованих ключів шифрування рівна кількості символів в повідомленні.

Множина Z утворюється як послідовність біт $\{b_{n1}, b_{n2} ... b_{nL}\}$. Елементи інформаційного повідомлення i_k додаються з елементами псевдовипадкової послідовності z_k з використанням операції XOR [5]:

$$s_k = m_k \oplus z_k \quad (4)$$

Даний алгоритм шифрування є симетричним, тому процес розшифрування здійснюється в оберненому порядку при тих самих початкових умовах та параметрах що використовувались при шифруванні.

Алгоритм дозволяє шифрувати не тільки текстові повідомлення, а й зображення. В такому випадку з кожного пікселя зображення зчитуються градації R,G,B-кольорів, що представляються двійковими 8-и бітовими числами, утворюючи множину I.

Для збільшення ефекту впливу змін вихідних даних на зашифровані, використаємо механізм дифузії, запропонований в [3,6]. Для випадку шифрування повідомлень даний механізм зв'язує значення шифрованих байтів з наступними байтами шифротексту. Механізм дифузії здійснюється за наступною формулою:

$$C(k) = \phi(k) \oplus \{[S(k) + \phi(k)] \bmod N\} \oplus C(k-1), \quad (5)$$

де $C(k-1)$ та $C(k)$ – попередній та наступний байти шифротексту, $S(k)$– байт вихідного тексту, $\phi(k)$ – хаотична функція, в якості якої запропоновано логістичне відображення:

$$\phi(k+1) = 3{,}95\phi(k)[1-\phi(k)]. \quad (6)$$

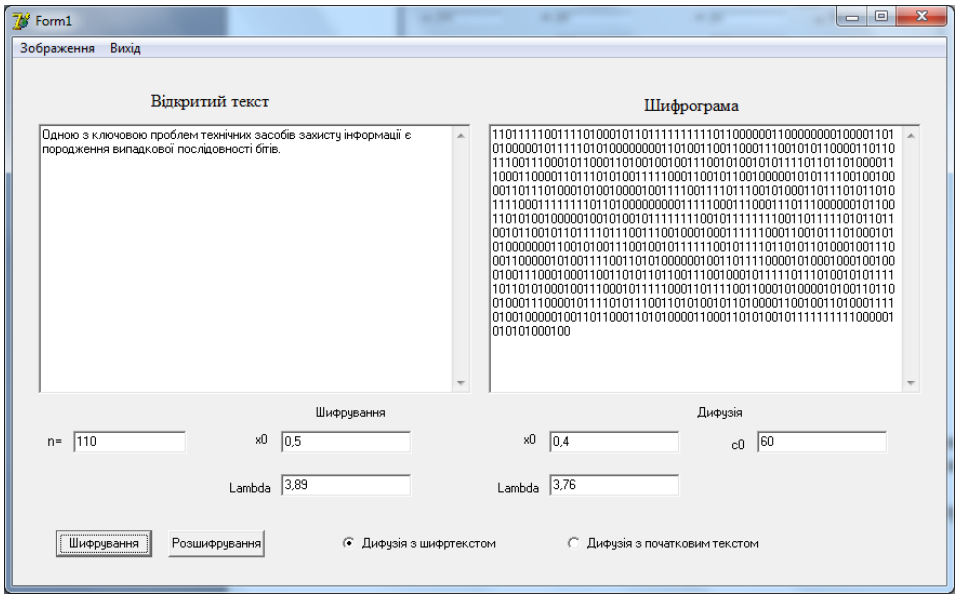
Оберенене перетворення дифузії описується формулою:

$$S(k) = \{\phi(k) \oplus C(k) \oplus C(k-1) + N - \phi(k)\} \bmod N \qquad (7)$$

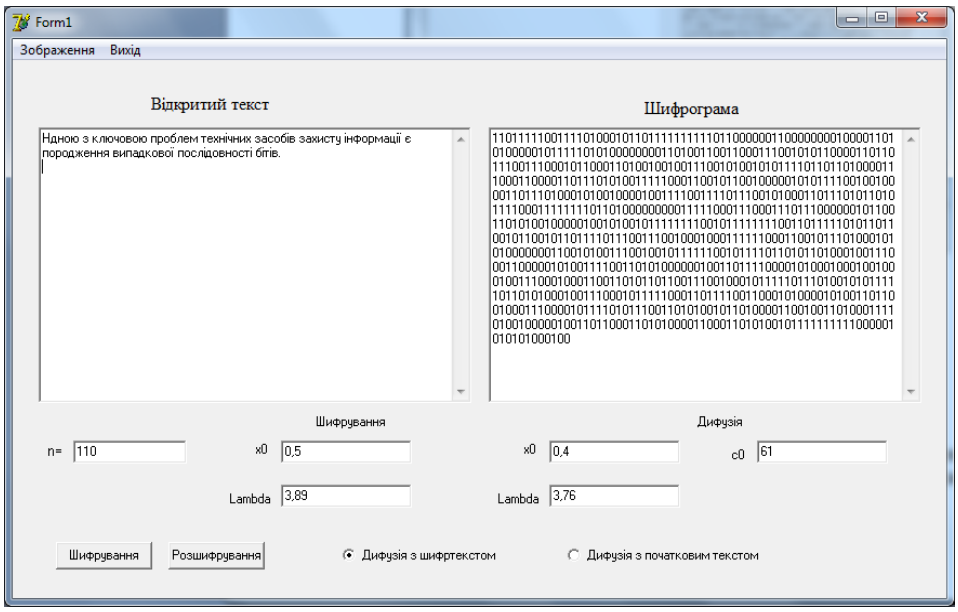
Параметрами перетворення дифузії є два початкові значення: $C(0)$ та $\phi(0)$. Ці параметри є додатковим ключем для алгоритму шифрування.

3. Дослідження роботи алгоритму та його модифікація

В результаті дослідження процесу шифрування з використанням даного перетворення дифузії (5) було встановлено, що *C(0)* не може являтись додатковим параметром шифрування, оскільки при оберненому перетворенні дифузії, що описується формулою (7) елементи початкового тексту, починаючи із другого символу, не залежать від вибору *C(0)*. Результати досліджень на прикладі шифрування текстового повідомлення приведені на рис. 4.



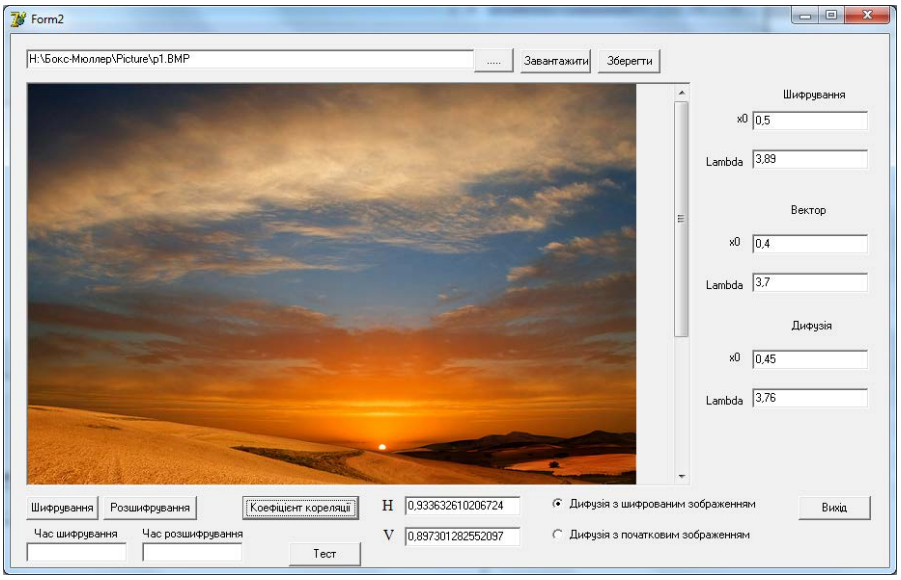
а)



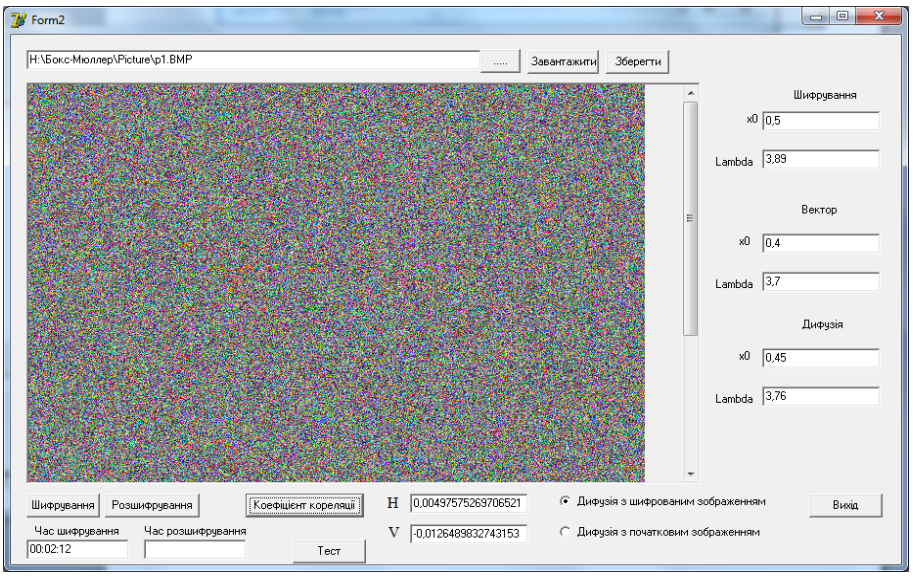
б)

Рис. 4. Результати шифрування повідомлень при різних значеннях параметру *C(0)*: а) шифрування при *C(0)*=60; б) розшифрування при *C(0)*=61

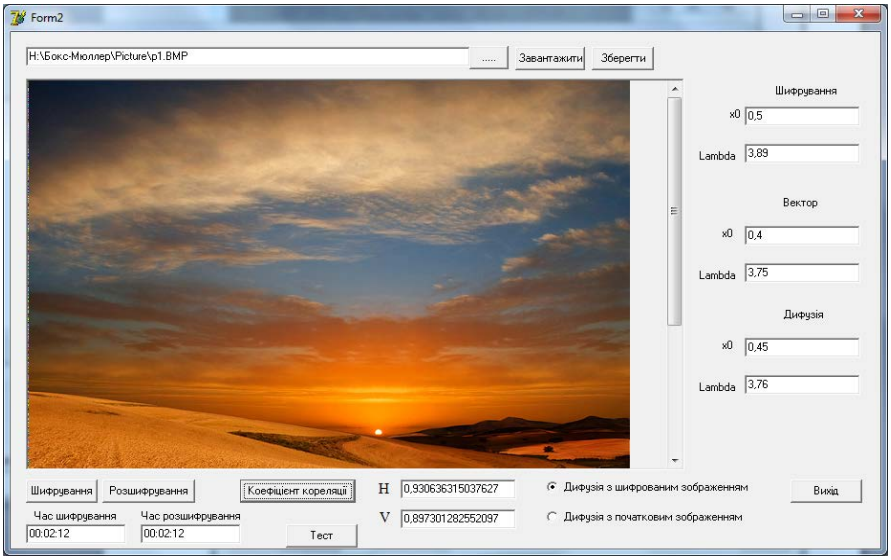
З рис.4 видно, що при зміні *C(0)* не розшифровується тільки перший символ, інші символи, починаючи з 2-го, розшифровуються однозначно. Подібний процес відбувається і при шифруванні зображень. При розшифруванні з іншим початковим параметром *C(0)* залишається нерозшифрованим перший стовпчик зображення (рис. 5 в, г). У випадку шифрування зображень запропоновано формувати значення *C(i)* для кожного рядка на основі одномірного дискретного відображення, що описується формулою (2), в якій в якості початкових умов виступають значення λ та x_0 (рис. 5).



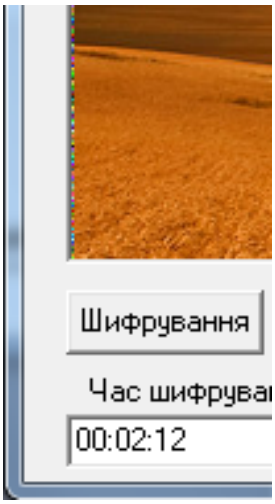
а)



б)



в)



г)

Рис.5. Результати шифрування зображення при різних значеннях параметру *C(0):* а) вихідне зображення, б) шифрування при λ=3,7; в) розшифрування при λ=3,75; г)фрагмент розшифрованого зображення

Авторами запропонована модифікація формули перетворення дифузії (5), (7) шляхом заміни $C(k-1)$ (попереднього байту шифротексту) на $I(k-1)$ (попередній байт вихідного тексту). Тоді формула (5) перепишеться у наступному вигляді:

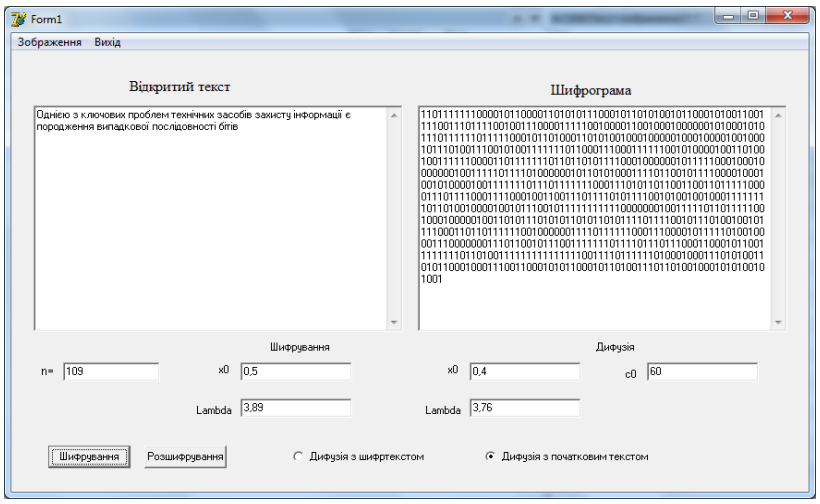
$$C(k) = \phi(k) \oplus \{[S(k) + \phi(k)] \bmod N\} \oplus I(k-1), \quad (8)$$

де $I(k-1)$ - попередній байт початкового тексту (при k=1 замість $I(k-1)$ беремо відповідне значення *C(0)*, $\phi(k)$ – хаотична функція, в якості якої запропоновано логістичне відображення (6).

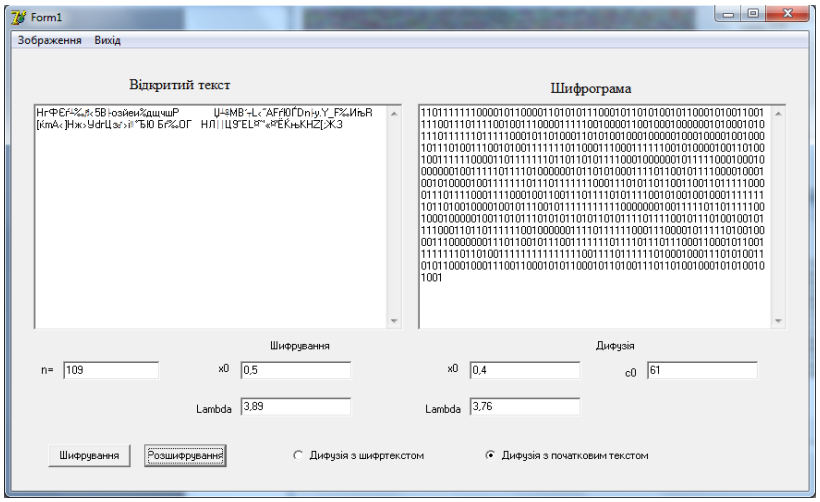
Оберенене перетворення дифузії описується формулою:

$$S(k) = \{\phi(k) \oplus C(k) \oplus I(k-1) + N - \phi(k)\} \bmod N \quad (9)$$

Робота алгоритму з модифікованим перетворенням дифузії була досліджена на прикладі шифрування текстових повідомлень та зображень. Результати шифрування наведені на рис. 6 та 7, відповідно.

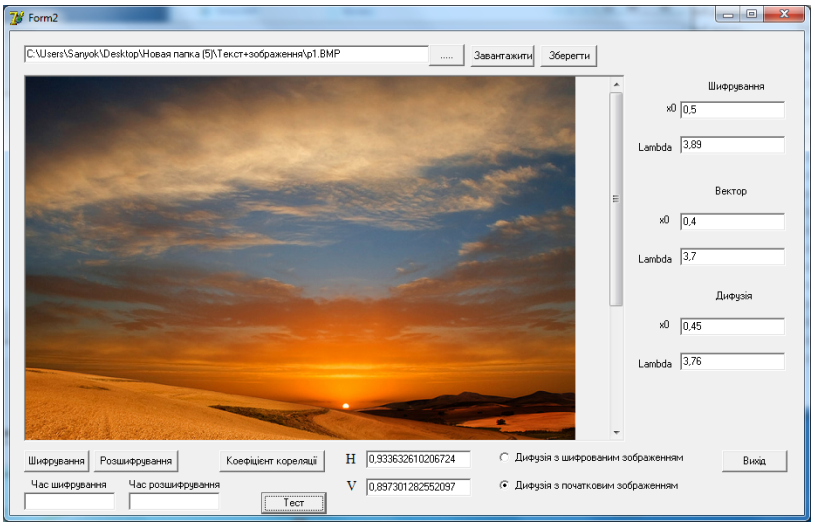


а)

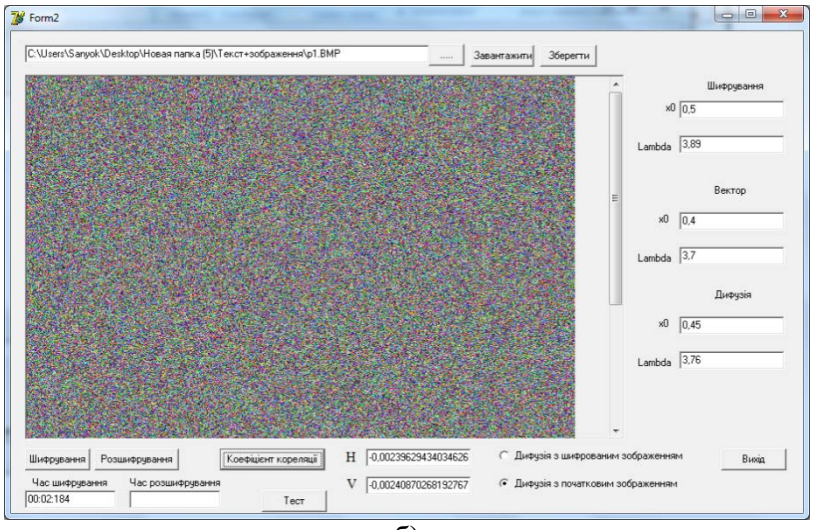


б)

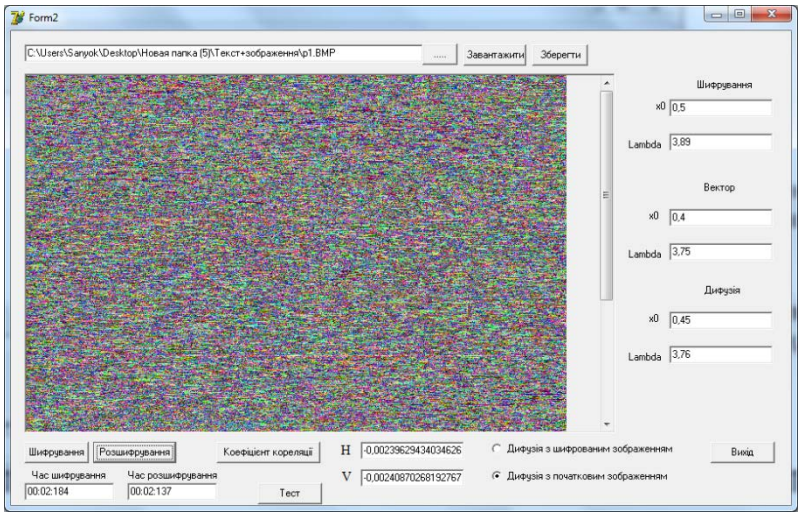
Рис.6. Результати шифрування повідомлень модифікованим алгоритмом: а) шифрування при *C(0)*=60; б) розшифрування при *C(0)*=61



а)



б)



в)

Рис. 7. Результати шифрування зображення модифікованим алгоритмом:
а) шифрування при λ=3,7, б) розшифрування при λ=3,75

З отриманих досліджень можна зробити висновок, що в модифікованому варіанті перетворення дифузії, що описується формулами (8), (9) додатковим ключем є два початкові значення $C(0)$ і $\phi(0)$.

4. Тестування алгоритму

Запропонований модифікований алгоритм може використовуватись для шифрування будь-якого виду інформації. Одним з найскладніших видівінформації для шифрування є графічна інформація. Тому в роботі проводиться тестування алгоритму на прикладі шифрування кольорових зображень.

Швидкість шифрування. В даній роботі проводилось порівняння часу, що витрачається на шифрування зображень різного розміру наступними алгоритмами: запропонованого модифікованого алгоритму, алгоритму на основі стандартного відображення [10], на основі комбінації стандартного та кубічного відображень [11] та на основі комбінації логістичного та кубічного відображень [12]. Порівняння проводилось з використанням комп'ютера з наступними параметрами Celeron M 1,6 GHz CPU з 2Гб ОЗП. Результати порівняння наведені на рис. 8.

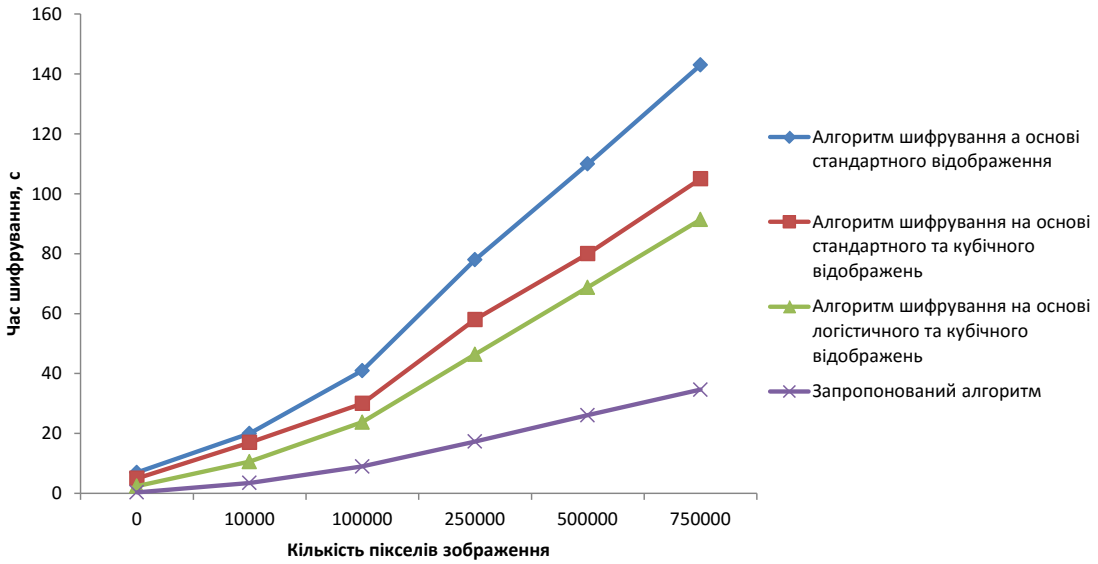
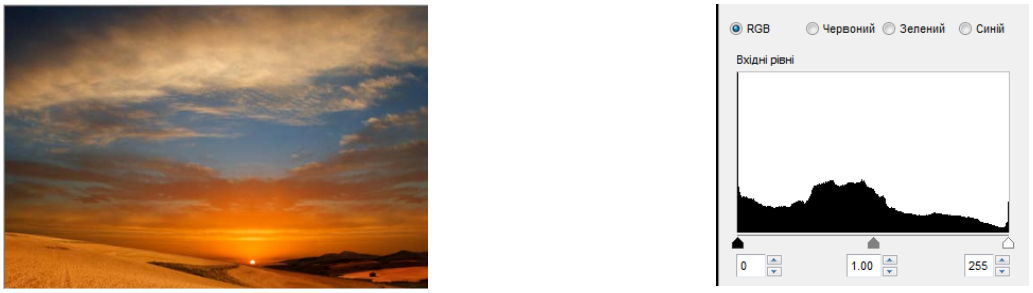


Рис. 8. Порівняльний аналіз швидкості шифрування алгоритмів

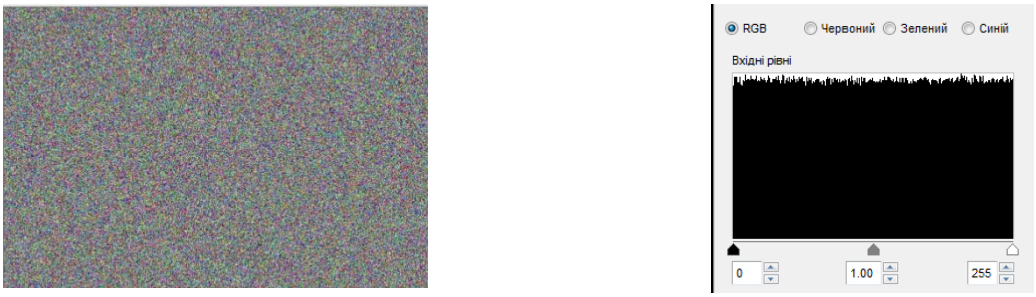
Із отриманих залежностей можна зробити висновок, що швидкість шифрування розробленим алгоритмом є вищою, ніж в інших алгоритмах шифрування на основі хаотичних систем.

Оцінка ефективності алгоритму. Для підтвердження ефективності алгоритму шифрування був проведений гістограмний та кореляційний аналіз. Результати гістограмного аналізу, який демонструє розподіл кольорів пікселів для вихідного та зашифрованого зображень, приведені на рис. 9 та 10, відповідно.



а) б)

Рис. 9. Вихідне зображення (а) та гістограма розподілу кольорів пікселів (б)



а) б)

Рис.10 Зашифроване зображення (а) та гістограма розподілу кольорів пікселів (б)

З отриманих результатів досліджень можна зробити висновок, що на відміну від гістограми кольорів пікселів вихідного зображення гістограма кольорів пікселів зашифрованого зображення носить рівномірний характер.

Оцінка ефективності алгоритму шифрування здійснювалась на прикладі шифрування зображень за значенням коефіцієнта кореляції між суміжними пікселями для вихідного та зашифрованого зображень [7-9]. Для вихідних зображень коефіцієнт кореляції між пікселями становить 0,94…0,98, а для зашифрованих запропонованим алгоритмом не перевищував 0,01…0,05.

Отже практичне тестування алгоритму показало придатність алгоритму для шифрування інформації.

Висновки

В роботі запропоновано модифікований алгоритм шифрування інформації на основі хаотичних відображень. Запропонована модифікація формули перетворення дифузії шляхом заміни попереднього байту шифротексту на попередній байт вихідного тексту, що підвищило чутливість алгоритму до вхідних параметрів. В модифікованому варіанті перетворення початкові параметри виступають додатковим ключем алгоритму шифрування. Крім шифрування текстових даних даний алгоритм також може шифрувати будь-які інші файли, наприклад графічні.

Результати практичного тестування алгоритму показали, що:

– швидкість шифрування розробленим методом є вищою, ніж в інших алгоритмах шифрування на основі хаотичних систем;

– в зашифрованих зображеннях не прослідковується ніяких структур;

– розподіл кольорів пікселів для зашифрованих зображень є однорідним.

Отримані результати вказують на високу криптостійкість розробленого алгоритму.

Література

1. Долгов В.А. Криптографические методы защиты информации. Курс лекций. / В.А. Долгов, В.В. Анисимов. – Хабаровск.: Издательство ДВГУПС, 2008. – 155с.

2. Політанський Р.Л. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей / Політанський Р.Л., Шпатар П.М., Гресь О.В., Ляшкевич В.Я. // «Восточно-европейский журнал передовых технологий». 2012 №6/11(60) С8-10.

3. Гресь О.В. Алгоритм шифрування інформації з використанням псевдовипадкових послідовностей / Гресь О.В., Політанський Р.Л., Шпатар П.М., Верига А.Д. // Науково-виробничий збірник «Наукові записки українського науково-дослідного інституту зв'язку». 2013 №1(25) С88-93.

4. Преобразование Бокса-Мюллера. Доступно на: http://ru.wikipedia.org

5. Болтенков В.А. Анализ алгоритмов хаотического шифрования изображений / Болтенков В.А., Никольский Е.С. // Цифрові технології/ № 7 – 2010 – С. 61-66.

6. Chen Guanrong, Mao Yaobin, Chui Charles K. A Symmetric Image Encryption Scheme based on 3D Chaotic Cat maps // Chaos, Solitons and Fractals. 2004. V. 21, N 3. P. 749–761.

7. Pareek N.K Image encryption using chaotic logistic map/ Pareek N.K., Vinod Patidara, Sud K.K. // Image and Vision Computing 24 – 2006 – Pp. 926–934.

8. Pareek N.K. Cryptography using multiple one-dimensional chaotic maps/ Pareek N.K., Patidar V, Sud K.// Commun. Nonlinear Sci. Numer. Simul./ №10(7) – 2005 – Pp.715–723.

9. Liu S.An Improved Image Encryption Algorithm Based on Chaotic System / Liu S., Sun J., Xu Zh.// Journal of Computers./ №11.Vol.4 – 2009 – Pp. 1091-1100.

10. Shiguo Lian. A block cipher based on a suitable use of the chaotic standard map / Shiguo Lian, Jinsheng Sun, Zhiquan Wang // Chaos, Solitons and Fractals, №26 – 2005 – Pp. 117-129.

11. Krulikovskyi Oleh V. Image encryption algorithm based on chaotic maps / Oleh V. Krulikovskyi, Petro M. Shpatar, Leonid F. Politanskyi // Eastern European Scientific Journal. – 2014. – №6. – P. 362-366 .

12. Гресь.О.В. Блочне шифрування інформації з використанням детермінованих хаотичних систем / Гресь О.В., Косован Г.В., Шпатар П.М., Ластівка Г.І. // «Науковий вісник Чернівецького університету. Серія: Комп'ютерні системи та компоненти». 2011–Т. 2. Вип. 3–С. 85-91

Надійшла 18.08.2015 р. Рецензент: д.т.н., проф. Дудикевич В.Б.