5. Самойчук К. О. Аналітичні дослідження умов диспергування жирової фази молока в пульсаційному гомогенізаторі / К. О. Самойчук, Л. В. Левченко // Вісник Дніпропетровського державного аграрно-економічного університету: Дніпропетровськ – 2016. – № 1(39). – С. 64–67.

6. Дейниченко Г. В. Аналітичні дослідження енерговитрат пульсаційного гомогенізатора молока / Г. В. Дейниченко, К. О. Самойчук, Л. В. Левченко // Прогресивні техніка та технології харчових виробництв ресторанного господарства і торгівлі. Наукові праці ХДУХТ: Харків – 2016. – Вип. 1(23). – С. 170–181.

Гаврилко Ю.В.

студент;

Вовк Р.Б.

кандидат технічних наук, доцент,

Івано-Франківський національний технічний університет нафти і газу

ОПИС АЛГОРИТМУ ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ МЕТОДУ ДНК ТА ГІПЕРХАОТИЧНОЇ СИСТЕМИ РІВНЯНЬ РОССЛЕРА

З розвитком інформаційних технологій зростає обсяг інформації, яка передається, зокрема у вигляді цифрових зображень, а тому зростає потреба у забезпеченні її конфіденційності. В основному існують два типи шифрування: з симетричним ключем, яке використовує один ключ для шифрування й дешифрування; та асиметричним – один ключ для шифрування інший для дешифрування [1]. Для цих типів реалізовано багато різноманітних алгоритмів і в залежності від них визначається безпека даних, і у випадку коли витрати на декодування даних переважають самі дані по значимості то алгоритм шифрування вважається безпечним [2].

Суть методу шифрування зображення полягає в тому, щоб зашифрувати інформацію у вихідному зображенні для того, щоб ніхто не міг отримати вмістиме зображення без ключа розшифрування. Традиційні алгоритми шифрування, такі як DES, IDEA і AES не годяться для шифрування зображень через їх повільну швидкість роботи на реальних масштабах даних та недостатню точність і різне форматування даних. В даний час використовуються нові методи шифрування такі як, наприклад, ДНК шифрування, яке є перспективним в області шифрування інформації [3]. До переваг ДНК шифрування можна віднести паралелізм обчислень, високу щільність інформації та швидкість обчислень, що робить цей метод придатним для шифрування зображень [2]. В даному методі для шифрування використовується формальна модель ДНК, яку можна сформулювати наступним чином: послідовності ДНК включають чотири основи нуклеїнових кислот C (цитозин), T (тимін), A (аденін), G (гуанін), де допускається об’єднання між A і T та C і G. Чотири основи нуклеїнової кислоти C, T, A і G позначають значеннями двійкової системи числення 00, 01, 10, 11, а кожен піксель растрового чорно-білого зображення може бути представлений як

8-бітове двійкове число [1]. Таким чином, можна отримати 24 види об єднань, але оскільки вони повинні відповідати правилам спарювання, тобто А повинен бути спарений з G, а Т з С, тобто ефективними є лише 8 типів об'єднань, які подані в таблиці 1. Наприклад, якщо значення пікселю чорно-білого растрового зображення відповідає 183, то можна представити це значення в двійковій системі: $183_{10} = 10110111_2$, і використовуючи другий спосіб представлення в формі послідовності ДНК з таблиці 1, отримано послідовність «CTGT».

Таблиця 1

Правила кодування ДНК послідовностей

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0_{10}	00_2-A	00_2-A	00_2-C	00_2-C	00_2-G	00_2-G	00_2-T	00_2-T
1_{10}	01_2-C	01_2-G	01_2-A	01_2-T	01_2-A	01_2-T	01_2-C	01_2-G
2_{10}	10_2-G	10_2-C	10_2-T	10_2-A	10_2-T	10_2-A	10_2-G	10_2-C
3_{10}	11_2-T	11_2-T	11_2-G	11_2-G	11_2-C	11_2-C	11_2-A	11_2-A

В таблицях 2 і 3 представлені правила операцій додавання й віднімання для другого способу з таблиці 1.

Таблиця 2

Операція додавання ДНК послідовностей для варіанту 2

+	**A**	**C**	**T**	**G**
A	A	C	T	G
C	C	A	G	T
T	T	G	C	A
G	G	T	A	A

Таблиця 3

Операція віднімання ДНК послідовностей для варіанту 2

-	**A**	**C**	**T**	**G**
A	A	C	G	T
C	C	A	T	G
T	T	G	A	C
G	G	T	C	A

Для представлення значення пікселя X зображення для шифрування у вигляді послідовності ДНК використаємо наступні рівняння:

$$m_1 = X \bmod N$$
$$m_2 = (X/N) \bmod N$$
$$m_3 = (X/N^2) \bmod N \quad (1)$$
$$\dots$$
$$m_N = (X/N^{N-1}) \bmod N$$

де N це деяке значення, N < X; X – число, яке розкладається; $\{m_1, m_2, \dots, m_n\}$ – коефіцієнти. Невід'ємне ціле число X може бути представлене

у вигляді набору з N констант. Звідси X можна представити за допомогою формули (2).

$$X = \left(\left(\left(\left(\frac{X}{N^N}\right) * N + m_n\right) * N + \ m_{N-1}\right) \ldots\right) * N + \ m_1 \tag{2}$$

Також застосуємо хаотичні системи рівнянь для забезпечення більшої надійності. Відомо, що хаос це розповсюджене явище в детермінованих нелінійних системах, які проявляють високу чутливість до початкових умов і мають випадкове поводження. Для створення хаотичного потоку шифру, необхідно щоб випадковий потік бітів був створений за допомогою хаотичної системи. Основна ідея полягає в тому, щоб взяти невелику випадкову послідовність і розширити її до послідовності більшої довжини, таким чином, щоб не можна було ефективно розрізняти вихідну послідовність і випадкову послідовність. Відповідно, це означає можливість застосування системи шифрування зображень на хаотичних системах. В розробці алгоритму використовується гіперхаотична система рівнянь Росслера, яка описується наступним чином:

$$\begin{gathered} \dot{x} = -(\mathrm{y} + z) \\ \dot{y} = \mathrm{x} + \mathrm{ay} + \mathrm{w} \\ \dot{z} = \mathrm{b} + \mathrm{xz} \\ \dot{w} = -\mathrm{cz} + \mathrm{dw} \end{gathered} \tag{3}$$

де a, b, c, d, k – параметри системи; генеруються чотири хаотичні послідовності, $\dot{x}$, $\dot{y}$, $\dot{z}$, $\dot{w}$ – вихідні параметри для значень для значень квадрантів зображення [4].

Процес шифрування починається з розділення вхідного зображення A (m, n) на чотири частини (квадранти), в яких значення пікселів перетворюються згідно формули (1), внаслідок чого створюється чотири матриці RA, RB, RC, RD. Після цього кожна матриця кодується в ДНК послідовність EA, EB, EC, ED з використанням правил таблиці 1. Потім генеруються чотири хаотичні послідовності $x = (x_1, x_2 \ldots, x_n)$, $y = (y_1, y_2 \ldots, y_n)$, $z = (z_1, z_2 \ldots, z_n)$, $w = (w_1, w_2 \ldots, w_n)$, допомогою гіперхаотичної системи рівнянь Росслера з вхідними x_0, y_0, z_0, w_0 і системними параметрами a, b, c, d. Далі значення пікселя змінюється за наступними правилами:

$$\begin{gathered} EA(i,j) = \ EA\ (fx(i), fy\ (i)) \\ EB(i,j) = \ EB\ (fy(i), fz(i)) \\ EC(i,j) = \ EC\ (fz(i), fq\ (i)) \\ ED(i,j) = \ ED\ (fq(i), fx\ (i)) \end{gathered} \tag{4}$$

де $i = 1, 2..m, j = 1, 2..n$.

Аналогічно використовується операція додавання ДНК послідовностей для квадрантів й будуються матриці SA, SB, SC, SD. Відповідно MA, MB, MC, MD послідовності отримуються в процесі обробки колонок SA, SB, SC, SD за допомогою наступної операції:

$$\begin{cases} MA\{i\} \leftrightarrow MB\{i\}, \text{якщо } x(i) + \ y(i) < 1 \\ \qquad \text{без операції, інакше} \end{cases}$$
$$\begin{cases} MC\{i\} \leftrightarrow MD\{i\}, \text{якщо } z(i) + \ w(i) < 1 \\ \qquad \text{без операції, інакше} \end{cases} \tag{5}$$

Послідовності MA, MB, MC, MD шифруються за допомогою правил ДНК шифрування і отримуються матриці DA, DB, DC, DD,значення яких змінюються за формулою 2, в наслідок чого отримується зашифроване зображення.

Процес розшифрування є зворотнім до процесу шифрування і відрізняється тільки заміною операції додавання на віднімання послідовностей ДНК [5].

Отже, розглянутий алгоритм є досить стійким і надійним серед більшості інших криптографічних алгоритмів, оскільки при такому підході ключ генерується з використанням гіперхаотичної системи рівнянь Росслера, і застосуванням алгоритму ДНК заміщення.

Список використаних джерел:

1. Patel D. K. Image Encryption Using Different Techniques: A Review / Patel D. K., Belani S.; International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol. 1, Issue 1, November 2011. – Pp. 30-34.

2. Kwok H. S. A Fast Image Encryption System based on Chaotic Maps with Finite Precision Representation 32 / Kwok H. S., Tang W. K. S.; Chaos Solitons and Fractals, 2007. – Pp. 1518–1529.

3. Soni R. An Encryption and Decryption Algorithm for Image Based on DNA / Soni R. Johar, A., Soni V.; International Conference on communication systems and network technologies (CSNT), April 2013. – Pp. 478-481,

4. Rössler O. E An equation for hyperchaos; Physics Letters A, 1979. – Pp. 155-157.

5. Niu H. Splicing model and hyper-chaotic system for image encryption / Niu H., Zhou C., Wang B., Zheng X., Zhou S.; Journal of Electrical Engineering. Volume 67, Issue 2 May 2016. – Pp. 78–86.

Даниляк В.І.
студент;
Науковий керівник: **Вовк Р.Б.**
кандидат технічних наук,
Івано-Франківський національний технічний університет нафти і газу

ОПИС ТА КЛАСИФІКАЦІЯ ОСНОВНИХ МЕРЕЖЕВИХ АТАК ТА МЕТОДІВ ЗАХИСТУ ВІД НИХ

Мережевий захист – це динамічна галузь, яка стрімко розвивається, проте, не дивлячись на це, все частіше в заголовках новин зустрічається термін «мережеві атаки». Мережеві атаки – це певні дії, метою здійснення яких є отримання контролю над комп'ютерною системою або порушення її роботи, а також захоплення даних користувача. Актуальність захисту пристроїв у мережі з плином часу лише зростає, так згідно зі статистикою Qrator Labs [1] кількість лише DDoS-атак в першій половині 2015 становила 9347 в порівнянні з 2715 у 2014 році за аналогічний період.

Існує багато видів мережевих атак і захисту від них, вибір способу захисту залежить від багатьох факторів, таких як топологія мережі, протокол з'єднання та інше. Сьогодні багато людей, незалежно від їх сфер діяльності перебувають