УДК 004.056.55

С.Д. ГАЛЮК, О.В. КРУЛІКОВСЬКИЙ, Л.Ф. ПОЛІТАНСЬКИЙ
Чернівецький національний університет імені Юрія Федьковича

ПОРІВНЯЛЬНИЙ АНАЛІЗ ДВОМІРНИХ ВІДОБРАЖЕНЬ ДЛЯ ПЕРЕСТАНОВОК ПІКСЕЛІВ

У статті наведено результати досліджень перестановок на основі дискретизованих двомірних хаотичних відображень: Кота, Бейкера, стандартного та відображення з двома нелінійностями. Проаналізовано простір ключів відображень і складність перестановок. Досліджено стійкість перестановок до кореляційної атаки. Показано, що використання відображення з двома нелінійностями унеможливлює кореляційну атаку після двох циклів перестановок та суттєво збільшує ключовий простір.

Ключові слова: перестановка пікселів, двомірні відображення, хаотичні шифри.

S.D. HALIUK, O.V. KRULIKOVSKYI, L.F. POLITANSKYI
Yuriy Fedkovych Chernivtsi National University

COMPARATIVE ANALYSIS OF TWO-DIMENSIONAL MAPS FOR PIXEL PERMUTATIONS

The article contains results of studies permutations based on discredited two-dimensional chaotic maps: Cat, Baker, standard, and map with two nonlinearities. The key space of maps and complexity of permutations are analyzed. Determined resistance of permutations to attacks based on the correlation between adjacent pixels. Also is shown, that using map with two nonlinearities prevents correlation attack after two cycles of permutations and significantly increases the key space.

Keywords –pixel permutations, two-dimensional chaotic map, chaotic ciphers.

Вступ

Починаючи з другої половини XX ст. в ході активного розвитку інформаційних технологій неперервно зростає багатогранність та складність проблем інформаційної безпеки [1]. Це підтверджується типовими і креативними атаками на бази даних і інформаційні системи державних, корпоративних та приватних користувачів. Для протидії цим атакам необхідно постійно вдосконалювати методи та засоби захисту інформації. Серед найбільш ефективних засобів захисту даних з обмеженим доступом є їх криптографічне шифрування. Постійне збільшення обчислювальної потужності ЕОМ та нових методів криптоаналізу зумовлює систематичне підвищення вимог до засобів безпеки інформації, що, в свою чергу, стимулює розвиток і дослідження нових напрямків в криптології.

Одним з перспективних напрямків досліджень є можливість використання теорії детермінованого хаосу для побудови інформаційно-комунікаційних систем [2, 3] та захисту інформації [4, 5]. Детерміновані хаотичні системи є чутливими до початкових умов і параметрів, а їхні траєкторії непередбачувані на великих часових інтервалах [6]. Використання цих властивостей є однією з необхідних умов для розробки нових криптографічних методів [7, 8].

Для розроблення криптографічних додатків можна використовувати аналогові [9], дискретні [10] хаотичні системи чи їх поєднання. З точки зору економічних і часових затрат кращими будуть дискретні рекурентні відображення, оскільки вони є простішими в реалізації та подібні до традиційних криптосистем. Надійний метод шифрування зображень повинен складатися з двох етапів [8]:

- перестановки пікселів,
- дифузії кольору пікселів.

На першому етапі здійснюється перетворення блоку інформації за допомогою дискретного двомірного хаотичного відображення. Метою перестановки є розрив взаємозалежності між послідовними пікселями зображення. При цьому розподіл градацій кольорів зображення не змінюється. Під час перестановки пікселів розмір блоку буде дорівнювати N^2.

Дифузія представляє собою зміну значень складових кольору пікселів за допомогою нелінійної детермінованої системи. Для дифузії розмір блоку визначатиметься типом використовуваної арифметики, розмірами зображення, кількістю двійкових розрядів для запису однієї з складових кольору пікселів. Наприклад, розмір блоку при дифузії для зображень формату RGB становитиме $\frac{24}{3}N^2 = 8N^2$ біт. Ключем дифузійного процесу є початкові умови і параметри функції дифузії. Дифузія чутлива до повідомлення при наявності зворотних зв'язків за шифротекстом у алгоритмі шифрування. Хаотичний потоковий шифр може містити тільки операції дифузії [11], які найчастіше полягають у додаванні за модулем два псевдовипадкової та інформаційної послідовності бітів.

В процесі перестановок чутливість до початкового значення відповідає чутливості до початкового положення пікселя. При зростанні чутливості покращується випадковість перестановки. Якість перестановки залежить від кількості циклів. Простором ключів буде область допустимих значень параметрів хаотичного відображення. Чутливість до ключа визначається чутливістю до параметрів хаотичного відображення та кількістю циклів. Недоліком перестановок є відсутність чутливості до повідомлення. Алгоритми шифрування, в яких використовуються тільки перестановки, легко зламуються атакою

відкритим текстом [12].

В [13] запропоновані модифікації стандартного відображення, призначені для виконання перемішування на етапі перестановки в шифрах на базі хаосу. В пропонованій роботі нами детально досліджено одну з модифікацій та здійснено порівняльний аналіз відомих двомірних дискретизованих хаотичних відображень.

Хаотичні відображення для перестановок

Для процесу перемішування можуть бути використані багато різних двомірних хаотичних відображень, наприклад, відображення Бейкера, відображення Кота, стандартне відображення (Чирікова), які дискретизовані по розміру зображення, дають змогу забезпечити перемішування всіх пікселів без втрат [8]. Для зображення розміром $N \times N$ пікселів дискретизовані відображення Чирікова, Кота і Бейкера описуються наступними системами рівнянь [8,14]:

$$\begin{aligned} x_{j+1} &= \left(x_j + y_j\right) \bmod N, \\ y_{j+1} &= \left(y_j + K \sin \frac{x_{j+1} N}{2\pi}\right) \bmod N, \end{aligned} \tag{1}$$

де K – параметр (ключ перестановки) стандартного відображення;

$$\begin{aligned} x_{j+1} &= \left(x_j + u y_j\right) \bmod N, \\ y_{j+1} &= \left(v x_j + (1 + uv) y_j\right) \bmod N, \end{aligned} \tag{2}$$

де u, v –параметри відображення Кота;

$$\begin{aligned} x_{j+1} &= \frac{N}{k_i}\left(x_j - N_i\right) + y_j \bmod \frac{N}{k_i}, \\ y_{j+1} &= \frac{k_i}{N}\left(y_j + y_j \bmod \frac{N}{k_i}\right) + N_i, \end{aligned} \tag{3}$$

де $k_1, k_2, \ldots, k_t$ – параметри відображення Бейкера, які задовольняють умови:

$$\begin{cases} k_1 + k_2 + \ldots k_t = N, \\ N = k_1 + \ldots + k_{i-1}, \\ N_i \le x_j < N_i + k_i, \\ 0 \le y_j < N. \end{cases}$$

Детально властивості, переваги та недоліки відображень (1)–(3) проаналізовані в [12–14].

В [15] запропоновано двомірне хаотичне відображення:

$$\begin{aligned} x_{j+1} &= \left(x_j + K_1 \sin \frac{y_j N}{2\pi}\right) \bmod N, \\ y_{j+1} &= \left(y_j + K_2 \sin \frac{x_{j+1} N}{2\pi}\right) \bmod N, \end{aligned} \tag{4}$$

де K_1 і K_2 – параметри системи.

Критерієм хаотичної поведінки нелінійної системи є швидкість розбігання близьких траєкторій, що таблично оцінюються значенням старшого показника Ляпунова [16]. Залежності показників Ляпунова для (4) від параметрів системи наведено на рис. 1. Розрахунок здійснено методом QR [17]. Як слідує з рис. 1, система (4) є хаотичною при заданих значеннях параметрів, сума показників Ляпунова дорівнює нулю, що є ознакою консервативності системи.

Значення якобіана системи (4) не залежить від значення параметрів K_1 і K_2:

$$D = \begin{vmatrix} \frac{\partial x}{\partial x} & \frac{\partial x}{\partial y} \\ \frac{\partial y}{\partial x} & \frac{\partial y}{\partial y} \end{vmatrix} = \begin{vmatrix} 1 & \frac{K_1 N}{2\pi} \cos \frac{yN}{2\pi} \\ \frac{K_2 N}{2\pi} \cos \frac{\left(x + K_1 \sin \frac{yN}{2\pi}\right) N}{2\pi} & 1 + \frac{K_1 K_2 N^2}{(2\pi)^2} \cos \frac{\left(x + K_1 \sin \frac{yN}{2\pi}\right) N}{2\pi} \cos \frac{yN}{2\pi} \end{vmatrix} = 1,$$

тобто відображення буде зберігати площу і є потенційно придатним для здійснення перестановок у хаотичних алгоритмах шифрування.

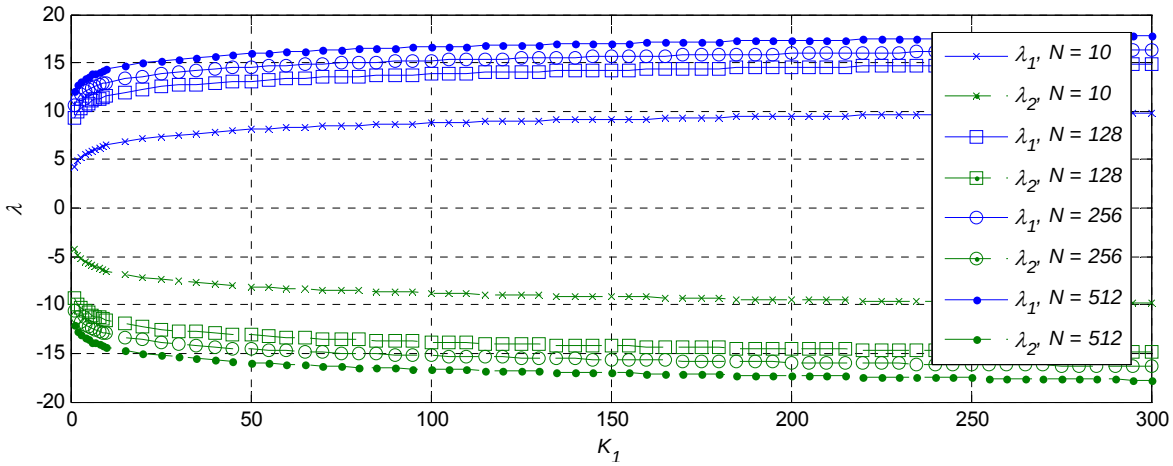
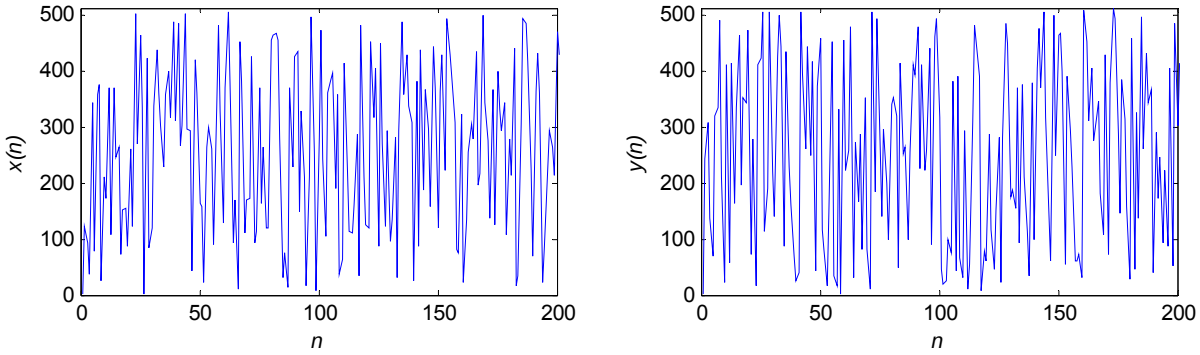


Рис. 1. Залежність показників Ляпунова для системи (4) від параметра K_1 і N при $K_1 = 100$

Приклади реалізації хаотичного процесу відображення (4) наведено на рис. 3. Всі ітераційні залежності схожі на випадкові коливання, але утворюються детермінованими системами.

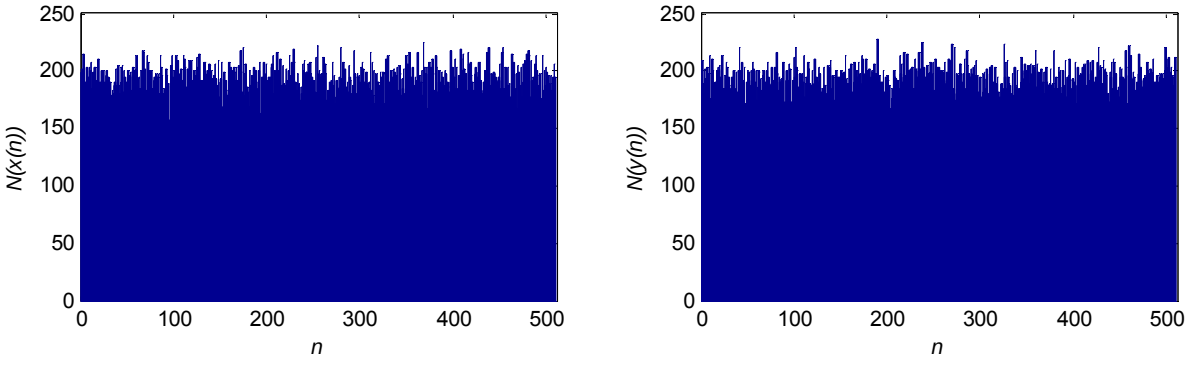


а **б**

Рис. 2. Приклади розв'язків системи (4): *а* – для змінної *x*, *б* – для змінної *y*

З точки зору обчислювальної складності система (4) є складнішою, порівняно з (1) тому що для розрахунку наступної ітерації необхідно двічі знаходити значення функції синуса. Враховуючи, що значення тригонометричних функцій у цифровій техніці обчислюються за допомогою розкладу в ряд Тейлора шуканих функцій, за кількістю необхідних часових ресурсів і/або об'єму пам'яті відображення Кота і стандартне є простішими та потребують виконання меншої кількості математичних операцій.

Гістограми розподілу розв'язків системи (4) характеризуються рівномірним розподілом (рис. 3), що найчастіше зустрічається в криптографії. Рівноймовірність розподілу обох змінних означає незалежність (в статистичному розумінні) між послідовними ітераціями хаотичного процесу.



а **б**

Рис. 3. Гістограми розподілу розв'язків системи (4): *а* – для змінної *x*, *б* – для змінної *y*

При виконанні перестановок пікселів у зображеннях системи рівнянь (1)–(4) пов'язують поточну та наступну координати пікселя з точністю до дробової частини. Дискретизоване за розміром зображення $N \times N$ відображення матиме вигляд

$$X_{j+1} = \left(X_j + K_1 sin \frac{Y_j N}{2\pi} \right) mod\, N,$$
$$Y_{j+1} = \left(Y_j + K_2 sin \frac{X_{j+1} N}{2\pi} \right) mod\, N, \quad (5)$$

де X_j, Y_j – початкові координати j-го пікселя, X_{j+1}, Y_{j+1} – координати j-го пікселя після перестановки; $\cdot$ – операція отримання цілої частини числа.

Обернене до (5) дискретизоване відображення застосовується для відновлення зображення після перестановки:

$$X_{j+1} = \left(X_j - K_1 sin \frac{Y_{j+1} N}{2\pi} \right) mod\, N,$$
$$Y_{j+1} = \left(Y_j - K_2 sin \frac{X_j N}{2\pi} \right) mod\, N. \quad (6)$$

При шифруванні та розшифруванні зображення в кілька циклів відповідну кількість раз необхідно застосовувати (5) і (6).

В порівнянні з дискретизованим стандартним відображенням [8] система (5) має дві нелінійності $K_1 sin \frac{y_j N}{2\pi}$ і $K_2 sin \frac{x_{j+1} N}{2\pi}$, і два параметри K_1 і K_2. Наявність двох незалежних рівноцінних параметрів квадратично збільшує ключовий простір системи. В роботі [15] показано, що для стандартного відображення можна ефективно застосувати кореляційну атаку, яка при одному або двох циклах перестановки дає змогу повністю дешифрувати зображення, не знаючи ключа *K*. Нелінійність у кожному рівнянні (5) вносить невизначеність в обидві змінні (координати), що покращує якість перестановки, і дає змогу усунути недоліки, характерні для стандартного відображення.

Порівняння ефективності перестановок

Розглянемо ефективність перестановок з використанням пропонованого та відомих відображень на прикладі зображення розміром 512×512 пікселів. Тестові зображення наведені на рис. 4 *а, е, м*.

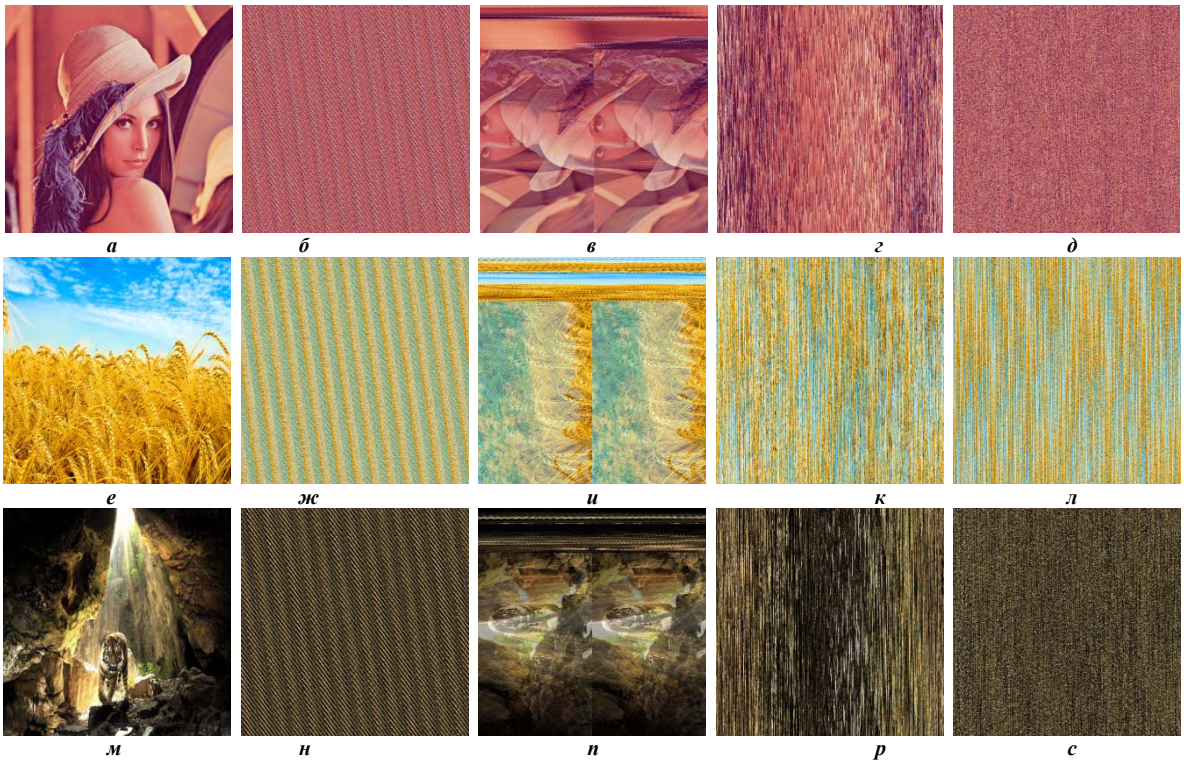


Рис. 4. *а, е, м* – оригінальні зображення, *б, ж, н* – після перестановки за допомогою (2), *в, и, п* – після перестановки за допомогою (3), *г, к, р* – після перестановки за допомогою (1, *д, л, с* – після перестановки за допомогою (4)

Після перестановки за допомогою відображення Кота (рис. 4 *б, ж, н),* незважаючи на відсутність контурів оригінального зображення в шифрованому, спостерігаються певні закономірності, що призводять до циклічності перестановки і можуть бути використані зловмисником. Застосування відображення Бейкера не дає змоги ефективно перемішати пікселі (рис. 4 *в, и, п*), зміст оригінального зображення можна легко

зрозуміти на основі шифрованого. Наші дослідження показують, що якість перестановок згідно (3) залежить від ключа і може мати малий період перестановки в декілька циклів.

Для перестановок пікселів в зображеннях на рис. 4 використовувались наступні параметри:

Таблиця 1

Використовувані параметри відображень для перестановок

Відображення	Параметри
Стандартне	K= 10000
Кота	v = 5677, u = 4359
Бейкера	{32, 4, 64, 2, 2, …, 2}
Пропоноване	K_1=K_2 = 10000

Один цикл перестановок за допомогою стандартного відображення теж не призводить до рівномірного розпорошення пікселів (рис. 4 *г, к, р*), тому для ефективного перемішування необхідно використовувати більшу кількість циклів. При використанні відображення (5), задовільне перемішування пікселів для заданих зображень можна отримати за один цикл перестановки (рис. 4 *д, л, с*).

Мірою взаємозв'язку між зображеннями є коефіцієнт кореляції. Чим менше значення модуля коефіцієнта кореляції, тим менш подібними будуть два зображення. Розглянемо, як змінюється кореляція між сусідніми пікселями по горизонталі і по вертикалі. Для розрахунку кореляції використаємо наступну формулу [18]:

$$C_r = \frac{N\sum_{j=1}^{N}\left(x_j \times y_j\right) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_j)^2) \times (N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \quad (7)$$

де x, y – значення градацій кольору двох сусідніх пікселів, N – кількість пікселів у зображенні.

Для оригінального зображення (рис. 4 *а*) значення коефіцієнта кореляції між сусідніми пікселями по горизонталі і вертикалі дорівнює 0,9759 та 0,9857 відповідно. Розраховані значення коефіцієнта кореляції після одного циклу перестановок наведені в Табл. 2. Серед досліджених систем найгірші кореляційні властивості перестановок забезпечує відображення Бейкера, для якого за один цикл перестановки кореляція пікселів по горизонталі майже не змінюється. Для стандартного відображення високим залишається значення коефіцієнта кореляції по вертикалі. Перестановки за допомогою (5) забезпечують найменшу кореляцію для всіх тестових зображень.

Таблиця 2

Кореляція пікселів зображення після одного циклу перестановок

Зображення	Кореляція пікселів	Відображення			
		Кота	Бейкера	Стандартне	Нове
Рис. 4 *а*	по горизонталі	-0,0796	0,9829	0,0972	-0,0011
	по вертикалі	0,1198	0,0433	0,9699	0,0375
Рис. 4 *е*	по горизонталі	-0,3555	0,9436	-0,0389	-0,0498
	по вертикалі	0,6639	-0,2540	0,9010	0,6258
Рис. 4 *м*	по горизонталі	0,1129	0,9673	0,0393	-0,0039
	по вертикалі	0,4548	0,1246	0,9468	0,0391

Для порівняння зазначимо, що в [14] для стандартного відображення рекомендується виконувати мінімум 4 цикли перестановок. Як випливає з аналізу, наведених в таблиці 3 значень коефіцієнтів кореляції при двох циклах перестановки, нове відображення володіє найкращими кореляційними властивостями.

Таблиця 3

Кореляція пікселів зображення після двох циклів перестановок

Зображення	Кореляція пікселів	Відображення			
		Кота	Бейкера	Стандартне	Нове
Рис. 4 *а*	по горизонталі	0,1083	0,0438	-0,0040	-0,0026
	по вертикалі	0,0099	0,0090	0,0969	-0,0029
Рис. 4 *е*	по горизонталі	-0,2535	-0,2552	$-1.0756*10^{-4}$	$7,4517*10^{-4}$
	по вертикалі	0,3038	0,4974	-0,0392	$-1,1870*10^{-4}$
Рис. 4 *м*	по горизонталі	0,1477	0,1219	-0,006	-0,0028
	по вертикалі	-0,1896	-0,1092	0,0396	$-6,5642*10^{-4}$

Оцінка часу перестановок

Безпека криптосистеми знаходиться в зв'язку з її обчислювальною складністю. В свою чергу

обчислювальна складність залежить від кількості циклів, складності хаотичного відображення і функції дифузії. Висока складність, зумовлена хаотичним відображенням або функцією дифузії, може бути зменшена шляхом вибору підходящого відображення. Оцінку обчислювальної складності проведемо за допомогою часу роботи алгоритму перестановки для різних відображень. Результати дослідження наведені в табл. 4. Для розрахунку використовувався ноутбук з Intel Corel Dual CPU 1,86 ГГц, 2ГБ ОЗУ.

Серед відображень Кота, стандартного та нового існує певна різниця в тривалості перестановки, проте не можна стверджувати, що вона є значною. Це пояснюється тим, що найбільше часу в процесі перестановки займає власне пошук і перемішання пікселя в матриці пікселів з одного положення в інше. При цьому час розрахунку значень наступного положення пікселя є малим в порівнянні з часом його переміщення.

Таблиця 4

Тривалість одного циклу перестановок для різних відображень

Зображення	**Відображення**			
	Кота	Бейкера	Стандартне	Нове
Рис. 6 *а*	0,913604	11,458918	0,935441	0,996236
Рис. 6 *е*	0,898154	11,360945	0,928541	0,993391
Рис. 6 *м*	0,887040	11,488943	0,937095	0,981561

В порівнянні з стандартним нове відображення характеризується більшою тривалістю циклу. Проте, якщо врахувати суттєве збільшення простору ключів та зменшення кількості циклів, необхідних для уникнення кореляції між сусідніми пікселями, його використання є повністю виправданим і доцільним.

Простір ключів

Оскільки в криптосистемах використовуються процеси перестановок і дифузії, тому ключовий простір криптосистеми дорівнює добутку кількості ключів цих процесів [14]. Нехай простір ключів при дифузії дорівнює $\boldsymbol{S}_1$, а для перестановок – $\boldsymbol{S}_2$; тоді для криптосистеми

$$\boldsymbol{S} = \boldsymbol{S}_1\boldsymbol{S}_2. \tag{8}$$

На практиці для різних циклів можуть використовуватися різні ключі. Якщо $\boldsymbol{n}$ – кількість циклів, тоді простір ключів

$$\boldsymbol{S} = (\boldsymbol{S}_1\boldsymbol{S}_2)^{\boldsymbol{N}}. \tag{9}$$

Із (9) випливає, що простір ключів $\boldsymbol{S}$ криптосистеми збільшується зі збільшенням простору ключів перестановок $\boldsymbol{S}_1$, області початкових значень ключів дифузії $\boldsymbol{S}_2$, або кількості циклів $\boldsymbol{n}$. Для різних хаотичних відображень розмір області значень ключа шифрування наведено в Табл. 5. Для нового відображення (5) два параметри K_1 і K_2 вносять невизначеність в перестановку. Зсув пікселя по горизонталі визначається значенням $\boldsymbol{d_x} = \left(\boldsymbol{K_1 sin}\dfrac{\boldsymbol{y_j N}}{2\boldsymbol{\pi}}\right)\boldsymbol{mod\, N}$, по вертикалі – $\boldsymbol{d_y} = \left(\boldsymbol{K_2 sin}\dfrac{\boldsymbol{x_{j+1} N}}{2\boldsymbol{\pi}}\right)\boldsymbol{mod\, N}$. В обох випадках існує N можливих варіантів зсуву по кожній координаті. Піксель після перестановки в залежності від значень ключів K_1 і K_2 може опинитися на будь-якій позиції $\boldsymbol{N}\times\boldsymbol{N}$ матриці пікселів. Піксель з координатами (0, 0), як і у випадку стандартного відображення, не змінюватиме свою позицію, незалежно від кількості циклів перестановки. Тому максимальний ключовий простір пропонованого відображення становитиме $(N^2\text{-}1)!$

Таблиця 5

Оцінка максимального простору ключів перестановки для зображення розміром $\boldsymbol{N\times N}$ з кількістю компонент кольору $\boldsymbol{L}$

Хаотичне відображення	**Простір ключів перестановки відображення, $\boldsymbol{S}_2$**	**Простір ключів перестановки (один ключ в різних циклах) для зображення, $\boldsymbol{S}_2$**	**Простір ключів криптосистеми (різний ключ в різних циклах) для зображення, $\boldsymbol{S}_2$**
Кота [8]	N^2	N^2L	$N^{2n}L^n$
Бейкера [8]	$2^{N\text{-}1}$	$2^{N\text{-}1}L$	$2^{n(N\text{-}1)}L^n$
Стандартне [13]	$N^{N\text{-}1}$	$N^{N\text{-}1}L$	$N^{n(N\text{-}1)}L^n$
Відображення з двома нелінійностями [15]	$N^2\text{-}1!$	$(N^2\text{-}1)!L$	$((N^2\text{-}1)!)^nL^n$

Оцінка ключів перестановки для (5) отримана при умові, що параметри K_1 і K_2 не обмежені за максимальним значенням. Реальний розмір ключів обмежиться мінімальним значенням добутку потужності

множин значень параметрів K_1 і K_2 і величиною (N^2-1)!, і залежатиме від прецизійності обчислень:

$$S_2 = \min\{card(K_1) * card(K_2),\ (N^2-1)!\}.$$

Ключовий простір збільшується, якщо в кожному циклі використати різні ключі. З таблиці 5 можна пересвідчитися, що пропоноване відображення має найбільший простір ключів, а відображення Кота – найменший.

Висновки

У роботі досліджено нове дискретне хаотичне відображення для перестановок пікселів в зображеннях $N \times N$ розмірності. Представлено порівняння якості перестановок пікселів новим відображенням з іншими відомими двомірними відображеннями. Досліджено швидкість перестановок, стійкість до кореляційної атаки. Встановлено, що при використані пропонованого відображення можна скоротити кількість циклів перестановки пікселів з врахуванням унеможливлення кореляційної атаки. З'ясовано, що потужність простору ключів перестановок є максимальною для растрових зображень $N \times N$ розмірності і становить $\left(N^2-1\right)!$ Відзначимо, що оцінка потужності простору ключів перестановок приймається на підставі умови абсолютної точності розрахунків. Вплив обмежень на потужність простору ключів є предметом подальших досліджень.

Література

1. Фомичев В. М. Дискретная математика и криптология / В. М. Фомичев. – М. : ДИАЛОГ-МИФИ, 2003. – 400 с.

2. Пивовар О. С. Моделювання випромінювання плат із вбудованими компонентами для передачі широкосмугових хаотичних сигналів / О. С. Пивовар, О. Б. Голевич // Вісник Хмельницького національного університету. Технічні науки. – 2014. – № 1. – С. 213–216.

3. Пивовар О.С. Дослідження впливу значення абсолютної похибки вирішення систем диференційних рівнянь на атрактори типу «ФОКУС» для генератора Чуа / О.С. Пивовар, О.Б. Голевич // Вісник Хмельницького національного університету. Технічні науки. – 2014. – № 6. – С. 243–246.

4. Гресь О.В. Алгоритм шифрування інформації з використанням псевдовипадкових послідовностей / О.В. Гресь, Р.Л. Політанський, П.М. Шпатар, А.Д. Верига // Наукові записки УНДІЗ. – 2013. – № 1.

5. Політанський, Р. Л. Моделювання схем шифрування інформації з використанням псевдовипадкових послідовностей / Р. Л. Політанський, Л.Ф. Політанський, П.М. Шпатар, О.В. Гресь // Восточно-Европейский журнал передовых технологий. – 2012. – Т. 57. – № 3/9. – С. 50–52.

6. Птицын Н. Приложение теории детерминированного хаоса в криптографии / Н. Птицын. – Москва : МГТУ им. Н. Э. Баумана, 2002. – 80 с.

7. Şefika Şule Erçetin Chaos, Complexity and Leadership 2013 / Şefika Şule Erçetin, Santo Banerjee – Ankara : Springer International Publishing, 2013. – 566 p.

8. Fridrich J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps / J. Fridrich // Inter. Journal of Bif. and Chaos. – 1998. – Vol. 8, No. 6. – P. 1259–1284.

9. Pareschi F. A Fast Chaos-based True Random Number Generator for Cryptographic Applications / F. Pareschi, G. Setti and R. Rovatti // Proceedings of the 32nd European Solid-State Circuits Conference. – Montreux, 2006. – P. 130–133.

10. Ljupco Kocarev Chaos-Based Cryptography Theory, Algorithms and Applications / L. Kocarev, S. Lian. – Berlin : Springer-Verlag Berlin Heidelberg, 2011. – 397 p.

11. Гресь О.В. Апаратна реалізація пристрою шифрування мовної інформації / О.В. Гресь, А.Д. Верига, Р.Л. Політанський, О.В. Дробик // Сучасний захист інформації. – 2014. – № 3. – С. 71–78.

12. Ercan Solak Cryptanalysis of fridrich's chaotic image encryption / Ercan Solak, Cahit okal, Olcay Taner Yildiz // International Journal of Bifurcation and Chaos. – 2010. – Vol. 20, No. 5. – P. 1405–1413.

13. Haliuk S. Analysis of Pixels Permutations Based on Discretized Chirikov Map / S. Haliuk, O. Krulikovskyi, L. Politanskyi // Proceedings of the XIIIth International Conference TCSET'2016, Lviv-Slavsko, Ukraine, February 23–26, 2016. – P. 519–521.

14. Lian S. Security analysis of a chaos-based image encryption algorithm / S. Lian, J. Sun, Z. Wang // Physica A: Statistical Mechanics and its Applications. – 2005. – Vol. 351, Is. 2–4. – P. 645-661.

15. Haliuk S. Two-dimensional map for permutations in chaotic ciphers / S. Haliuk, O. Krulikovskyi, L. Politanskyi // Conference PREDT 2016, 3–5 November 2016, Chernivtsi, Ukraine.

16. Генераторы хаотических колебаний / Б.И. Шахтарин, П.И. Кобылкина, Ю.А. Сидоркина, А.В. Кон-дратьэв, С.В. Митин. – М. : Галилеос АРВ, 2007. – 247 с.

17. Hubertus F. von Bremen An efficient QR based method for the computation of Lyapunov exponents / Hubertus F. von Bremen, Firdaus E. Udwadia, Wlodek Proskurowski // Physica D. – 1997. – № 101. – P. 1–16.

18. Jolfaei A. An image encryption approach using chaos and stream cipher / Alireza Jolfaei, Abdolrasoul Mirghadri // Journal of Theoretical and Applied Information Technology. – 2010. – Vol 19. No. 2.

Рецензія/Peer review : 27.1.2017 р. Надрукована/Printed :5.2.2017 р.
Рецензент : д.ф-м.н., проф. Махній В.П.