DOI 10.15276/imms.v14.no3.154
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 3, pp. 154-162

ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК АЛГОРИТМУ ПЕРЕМІШУВАННЯ ЕЛЕМЕНТІВ ДВОВИМІРНИХ МАТРИЦЬ ЯК ОСНОВА ДЛЯ ФОРМУВАННЯ ЗМІННИХ S-БЛОКІВ

Г.В. Ахмаметьєва[1], А.І. Гарбуз[2]

[1] Національний університет «Одеська юридична академія»
28,. Рішельєвська вул, Одеса, 65000, Україна
[2] ВСП «Фаховий коледж вимірювань» ДУІТЗ
13, Спиридонівська вул., Одеса, 65020, Україна
Emails: anna.odessitka@gmail.com[1], garbuzartem@okv.suitt.edu.ua[2]

Наводиться опис та аналіз структури алгоритму формування стеганографічного ключа, основою якого є перемішування рядків і стовпців двовимірної матриці, що містить неповторювані числові значення як послідовність вибору пікселів/блоків зображення для вбудовування повідомлення. Охарактеризована структура алгоритму з точки зору застосування перемішаних двовимірних матриць для формування змінних S-блоків в криптографічному перетворенні, виявлені переваги і недоліки структури та можливі напрями удосконалення процедури перемішування і підвищення швидкодії алгоритму. Проведено тестування експериментальних S-блоків розміром 16×16, що здійснюють заміну 8-бітових блоків новим 8-бітовим значенням, статистичними тестами NIST, яке показало, що більшість сформованих таблиць відповідає вимогам надійних псевдовипадкових послідовностей. З метою подальшого застосування розробленого раніше алгоритму перемішування двовимірної матриці для задач криптографічних перетворень були розраховані статистичні властивості S-блоків - алгебраїчна степінь нелінійності, відстань нелінійності, коефіцієнти кореляції S-блоку, лавинні властивості S-блоку, період повернення S-блоку. Результати експерименту показали, що майже для всіх таблиць досягається значення алгебраїчної степені нелінійності 7, що теоретично дозволяє використання алгоритму перемішування для формування змінних S-блоків, але коливання інших показників вимагає подальшої модифікації алгоритму та дослідження впливу параметрів алгоритму на статистичні характеристики сформованих матриць замін.

Ключові слова: стеганографічний ключ, перемішування, двовимірна матриця, криптографічне перетворення, S-блок заміни, статистичні властивості, псевдовипадкова послідовність

Вступ. Сучасні технології та Інтернет-комунікації сприяють миттєвому обміну інформацією між користувачами різних країн світу. Засобами вебсайтів, електронної пошти, месенджерів, файлообмінників, хмарних сховищ можна передавати будь-які дані, як то текстові документи, аудіозаписи, фото, відео, тощо. Однак далеко не всі інструменти Інтернет-комунікації є безпечними. За умови передачі несекретної та загальнодоступної інформації існуючі системи моніторингу не створюють особливих проблем, хоч і можуть відслідковувати активність та зацікавленість користувачів. А ось необхідність відправити конфіденційну інформацію при відсутності захищених каналів зв’язку створює велику загрозу збереженню в таємниці персональної або комерційної інформації.

Вирішити цю задачу дозволяє застосування методів стеганографії, які забезпечують приховану передачу конфіденційних даних всередині нічим не примітного на перший погляд контейнеру. В якості контейнерів найбільш розповсюдженими є зображення, аудіо та відео через наявність в них надмірної інформації, що дозволяє забезпечити високу пропускну спроможність прихованого каналу зв’язку, тобто можливість вбудовування в контейнер значний обсяг даних.

Переваги використання стеганографії полягають в широкому виборі методів та їх програмних реалізацій, переважна більшість яких здійснює вбудовування секретної інформації в цифрові зображення. В більшості стеганографічних застосунків не приділяється увага формуванню стеганографічного ключа - послідовності вибору елементів контейнера для занурення в нього даних. Іноді стеганографічне перетворення поєднують з криптографічним закриттям конфіденційних даних [1-3]. У зв'язку з чим в роботі [4] були проаналізовані підходи до формування стеганографічних ключів інших авторів [5-12] та розроблено алгоритм формування стеганографічного ключа на основі перемішування рядків і стовпців двовимірної матриці. В роботі [13] було проведено дослідження характеристик перестановки графічними тестами, які показали достатньо надійний псевдовипадковий розподіл числових елементів на площині та якісні характеристики автокореляційної функції.

Метою даної роботи є проведення більш детального дослідження статистичних характеристик розробленого в [4, 13] алгоритму, в основу якого покладено перемішування рядків і стовпців двовимірної матриці.

Задачами статті є:

1. Визначити переваги і недоліки в структурі алгоритму формування стеганографічного ключа;
2. Провести дослідження якості перестановок при застосування оригінального алгоритму [4] статистичними тестами NIST [14];
3. Проаналізувати можливість використання основи алгоритму стеганографічного ключа для формування змінних S-блоків для криптографічних перетворень.

Основна частина. Алгоритм формування стеганографічного ключа [4] передусім спрямований на те, щоб задати псевдовипадкову послідовність вибору елементів контейнеру (блоків, пікселів) для вбудовування повідомлення, а з цього випливає, що елементи такої послідовності не можуть повторюватись, оскільки перезапис нового біту повністю видаляє попередній, що припускає можливість застосування даного алгоритму для формування змінних S-блоків заміни для криптографічних перетворень. Крім того, алгоритм побудований таким чином, що не потребує збереження матриці ключа окремим файлом, оскільки його можна відтворити на основі секретного паролю та вхідних параметрів, що забезпечує неможливість відтворення секретного ключа без знання паролю.

В роботі [4] описано послідовність обчислень та пояснення щодо математичних операцій, однак не наведено основні кроки алгоритму, які в повній мірі задають перемішування елементів матриці. Для подальшого розуміння структури алгоритму та виявлення його недоліків наведемо основні кроки алгоритму [13].

Крок 1. Отримання вхідних даних:

- розмір зображення-контейнера $H \times W$,
- розмір блоку $m \times n$,
- пароль key (послідовність з не менш як восьми символів),
- алгоритм хешування $algorithm$ (за умовчанням MD5),
- кількість перемішувань $perturbations$ (за умовчанням 30).

Крок 2. Підготовка матриці стеганографічного ключа.

2.1. Обчислення розміру матриці стеганографічного ключа

$$M = \left\lfloor \frac{H}{m} \right\rfloor, N = \left\lfloor \frac{W}{n} \right\rfloor,$$

де $\lfloor \bullet \rfloor$ - округлення до найменшого цілого.

2.2. Заповнення матриці послідовністю чисел від 1 до MN

$$table_{i,j} = j + (i-1)N.$$

Крок 3. Формування додаткових ключів.

3.1. Отримання результату хешування паролю key

$$hash_l = algorithm(key), \overline{l = 1, L},$$

$$algorithm \in \{MD5, SHA1, SHA256, SHA384, SHA512\},$$

де $hash$ - вектор з десятковими значеннями хеш-функції.

3.2. Обчислити:

$$t_k = \left\lfloor \frac{L}{Z_k} \right\rfloor \text{ або } t_k = \left\lceil \frac{L}{Z_k} \right\rceil,$$

де L - довжина вектору $hash$, $\lfloor \bullet \rfloor$ - округлення до найменшого цілого, $\lceil \bullet \rceil$ - округлення до найбільшого цілого, $Z_k \in \square$, $Z_k > 1, k = \overline{1,8}$.

3.3. Визначити значення додаткових ключів:

$$key1 = \left| \left(hash_{t_8} - hash_{t_6} \right) \left(hash_{t_1} + hash_{t_5} \right) \right|,$$

$$key2 = \left| \left(hash_{t_2} - hash_{t_7} \right) \left(hash_{t_3} + hash_{t_8} \right) \right|,$$

$$key3 = \left| \left(hash_{t_7} - hash_{t_4} \right) \left(hash_{t_5} + hash_{t_2} \right) \cdot hash_{t_6} \cdot hash_{t_1} \right|,$$

$$key4 = \left| \left(hash_{t_2} - hash_{t_1} \right) \left(hash_{t_7} + hash_{t_6} \right) \cdot hash_{t_4} \cdot hash_{t_3} \right|.$$

Крок 4. Формування параметрів лінійного конгруентного генератора і генерація псевдовипадкових послідовностей $SeqI$ і $SeqJ$.

4.1. Обчислити модулі

$$p_1 = M \cdot perturbations,$$

$$p_2 = N \cdot perturbations.$$

4.2. Визначення параметрів двох лінійних конгруентних генераторів.

4.2.1. Для модулів p_1 і p_2 визначити прості дільники.

4.2.2. Обчислити добуток унікальних простих дільників, де під унікальними простими дільниками розуміємо такі значення, що не повторюються. Результат - A_1, A_2.

4.2.3. Якщо $p_1 \equiv 0 (\mathrm{mod}\, 4)$, то $A_1 = 2A_1 + 1$, інакше $A_1 = A_1 + 1$.

Якщо $p_2 \equiv 0 (\mathrm{mod}\, 4)$, то $A_2 = 2A_2 + 1$, інакше $A_2 = A_2 + 1$.

4.2.4. Обчислити $B_1 = \mathrm{mod}(p_1 \cdot X, Y)$ і $B_2 = \mathrm{mod}(p_2 \cdot X, Y)$, де $X, Y \in \square$.

4.2.5. Якщо $(B_1, p_1) = 1$, то $B_1 = B_1$, інакше доки $(B_1, p_1) \neq 1$, $B_1 = B_1 - 1$.

Якщо $(B_2, p_2) = 1$, то $B_2 = B_2$, інакше доки $(B_2, p_2) \neq 1$, $B_2 = B_2 - 1$.

4.3. Генерація псевдовипадкових послідовностей

$$prg_i^1 = A_1 prg_{i-1}^1 + B_1 (\mathrm{mod}\, p_1), \overline{i = 1, p_1}, prg_0^1 = key1,$$

$$prg_j^2 = A_2 prg_{j-1}^2 + B_2 (\mathrm{mod}\, p_2), \overline{j = 1, p_2}, prg_0^2 = key2.$$

Крок 5. Перемішування матриці *table*.

Для $\overline{i = 1, p_1}$, $\overline{j = 1, p_2}$:

5.1. Визначення номеру рядка і стовпця:

$$x = \mathrm{mod}(prg_i^1, M), y = \mathrm{mod}(prg_j^2, N).$$

5.2. Визначення величини циклічного зсуву рядка і стовпця:

$$shiftI = rezI(\mathrm{mod}\, N),\ rezI = XOR^{mod}(prg_i^1, key3, mn),$$
$$shiftJ = rezJ(\mathrm{mod}\, M),\ rezJ = XOR^{mod}(prg_j^2, key4, nn),$$

де XOR^{mod} - операція складання за модулем mod, $mod = mn$ - максимальна цифра у prg_i^1, $mod = nn$ - максимальна цифра у prg_j^2.

5.3. Циклічний зсув рядка і стовпця матриці $table$:

$$table_{i,:} = circshift(table_{i,:}, shiftI),$$
$$table_{:,j} = circshift(table_{:,j}, shiftJ),$$

де $circshift$ - операція циклічного зсуву.

Результат – матриця $table$ з перемішаними номерами блоків $m \times n$ для зображення розміром $H \times W$.

В даному алгоритмі слід детально пояснити сутність операції XOR^{mod}, оскільки вона є нестандартною та не використовується в криптографічних та стохастичних алгоритмах. Операція XOR^{mod} передбачає порозрядне сумування двох десяткових цифр *x* та *y* за модулем деякої третьої цифри *w*, де значення *w* становить максимальну цифру числа псевдовипадкової послідовності. Наприклад, маємо число псевдовипадкової послідовності $X = \{x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0\}$ та ключ $Y = \{y_7, y_6, y_5, y_4, y_3, y_2, y_1, y_0\}$. Нехай максимальною цифрою у X є x_5, тоді порозрядним модулем буде $w = x_5$. Тоді результатом операції XOR^{mod} буде число $Z = \{z_7, z_6, z_5, z_4, z_3, z_2, z_1, z_0\}$, кожний розряд якого обчислюється за формулою

$$z_i = x_i + y_i \left(\mathrm{mod}\, w\right), i = \overline{0,7}.$$

І оскільки псевдовипадкове число *X* змінюється на кожній ітерації алгоритму, то і модуль *w* буде змінним, що забезпечує певну непередбачуваність у величинах зсуву рядків та стовпців.

Послідовність і взаємозв'язок обчислень алгоритму можна подати у вигляді схеми, наведеної на рис.1 [13, 15], де скорочення ППВЧ означає послідовність псевдовипадкових чисел, суцільна лінія стосується обчислень для циклічного зсуву рядків, пунктирна лінія – для стовпців.

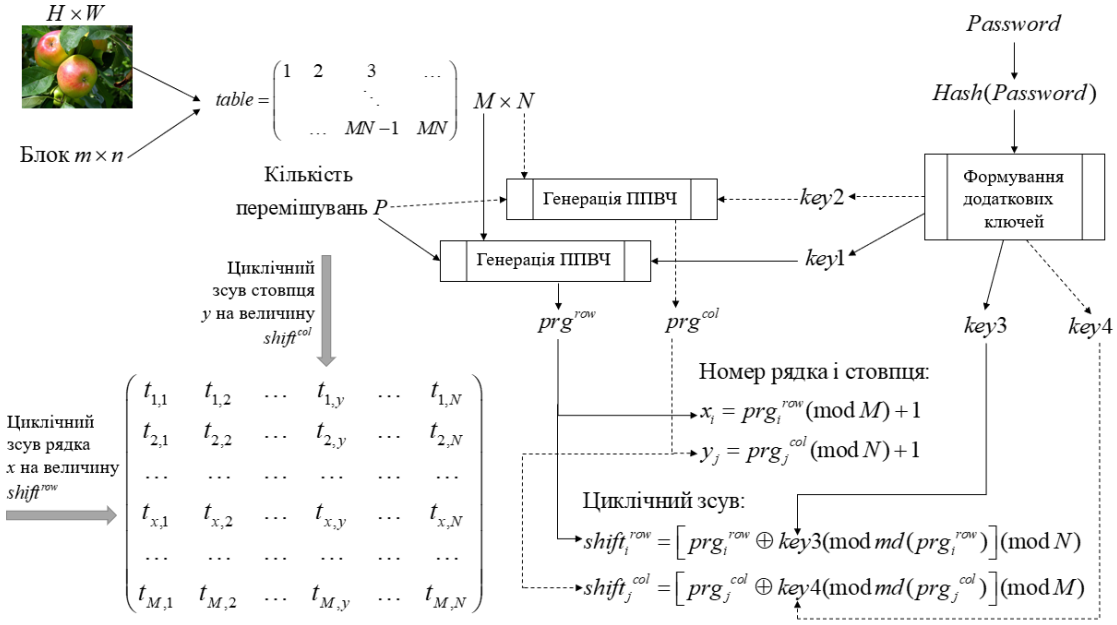

Рис.1. Структурна схема алгоритму формування стеганографічного ключа

Слід зазначити, що в алгоритмі міститься багато переваг, які дозволяють гарантувати захищеність стеганографічного ключа та можливість його відтворення на основі знання секретного паролю та параметрів перетворення, зокрема:

– в перемішуванні двовимірної матриці відбувається циклічний зсув як рядків, так і стовпців, причому змінними є як величина зсуву для кожного рядку/стовпця на кожному кроці, так і вибір самого рядка/стовпця, який задається псевдовипадковою послідовністю;

– всі внутрішні параметри прив'язані до секретного ключа –хеш-значення паролю та числа перемішувань P, тобто заміна ключа призводить до повної зміни результатів перестановки та гарантує непередбачуваний характер процедури перемішування;

– використання нестандартної операції модульного порозрядного сумування XOR^{mod} з одного боку є перевагою, з іншого недоліком, оскільки обмежує можливість реалізації алгоритму лише програмними засобами та потребує обчислень в десятковій системі числення, що вимагає більших обчислювальних затрат порівняно з двійковою системою числення та негативно впливає на швидкодію;

– запропонований алгоритм забезпечує рівномірний розподіл перших 5-10% елементів з послідовності від 0 до MN–1 по всій матриці [4] вже при $P = 10$.

До недоліків (з погляду адаптації алгоритму до задачі формування змінних S-блоків заміни криптографічних перетворень) можна віднести наступні:

– занадто складна процедура обчислення додаткових ключів (крок 3) містить константи, які задають вибір складових хешу, та подальше обчислення математичних виразів, обґрунтування яких в [4, 13] не наводиться;

– на кроці 4 при підборі параметрів лінійних конгруентних генераторів для забезпечення максимального періоду слід вірно підібрати константи A і B, для яких необхідно розкласти числа p_1 і p_2 на прості множники, тобто слід застосувати обчислювально складні операції факторизації складених чисел.

В сучасних криптографічних алгоритмах приділяється увага формуванню надійних S-блоків заміни, які забезпечують нелінійний шар криптографічного перетворення, що в значній мірі ускладнює можливість застосування диференціального, лінійного та інших методів криптоаналізу. В більшості алгоритмів S-блоки заміни є складовою частиною структури і є незмінними, деякі передбачають можливість використання сторонніх таблиць заміни, зокрема національний стандарт шифрування ДСТУ 7624:2014 [16, 17].

Оскільки S-блок представляє собою бієктивну матрицю заміни, де кожному входу єдиним способом ставиться у відповідність вихідний елемент, тобто S-блок суть є перестановкою значень від 0 до 2^N–1, поданої у вигляді квадратної матриці, а отже описаний вище алгоритм можна адаптувати та використовувати для формування змінних S-блоків в криптографічних шифрах.

З метою подальшої модифікації алгоритму перестановки для задач формування змінних S-блоків криптографічних перетворень, проаналізуємо статистичні властивості двовимірних матриць, отриманих запропонованим в [4] алгоритмом. Оскільки сучасні криптографічні стандарти, зокрема AES та ДСТУ 7624:2014, здійснюють байтові заміни, будемо розглядати S-блоки розміром 16×16, елементами якого є числа від 0 до 255.

За допомогою описаного вище алгоритму формування стеганографічного ключа було сформовано 1024 S-блоків розміром 16×16, з яких 512 з використанням хеш-функції SHA-256 та 512 з використанням хеш-функції SHA-256 при числі перемішувань $P = 12$. Отримані матриці подані для тестування статистичними тестами NIST [14], результати яких наведено в таблиці 1.

З таблиці 1 видно, що більшість послідовностей, отриманих перемішуванням запропонованим алгоритмам, проходять статистичні тести та можуть бути використані в

задачах криптографії для формування змінних S-блоків або для генерування псевдовипадкових послідовностей для потокових шифрів.

З'ясуємо, чи можна розглянутий алгоритм (можливо з деякими модифікаціями) використовувати як основу для перемішування даних в S-блоках заміни. Для цього був проведений обчислювальний експеримент на основі:

– група 1 – 512 S-блоків розміром 16×16, отриманих 12-ми циклами перемішування рядків і стовпців матриці з використанням хеш-функції SHA-256;

– група 2 – 512 S-блоків розміром 16×16, отриманих 18-ми циклами перемішування рядків і стовпців матриці з використанням хеш-функції SHA-256;

– група 3 – 512 S-блоків розміром 16×16, отриманих 12-ми циклами перемішування рядків і стовпців матриці з використанням хеш-функції SHA-512;

– група 4 – 512 S-блоків розміром 16×16, отриманих 18-ми циклами перемішування рядків і стовпців матриці з використанням хеш-функції SHA-512.

Таблиця 1.

Результати стохастичних тестів NIST

№	Тест	S-блоки (SHA-256)		S-блоки (SHA-512)		Кількість S-блоків, що пройшли тест, %	
		P-value	Pass rate	P-value	Pass rate	S-блоки (SHA-256)	S-блоки (SHA-512)
1	Monobit test	1	+	1	+	100	100
2	Frequency within block test	0,073	+	0,435	+	99,4	99,6
3	Runs test	0,979	+	0,731	+	100	100
4	Longest run ones in a block test	0,857	+	0,219	+	100	99,4
5	Binary matrix rank test	0,412	+	0,718	+	99,4	98,6
6	DFT test	0,096	+	0,882	+	99,02	99,2
7	Non overlapping template matching test	1	+	0,999	+	100	100
8	Overlapping template matching test	0,707	+	0,998	+	99,8	99,6
9	Maurers universal test	0,444	+	0,162	+	99,6	99,8
10	Linear complexity test	0,507	+	0,179	+	99,2	98,8
11	Serial test	0,991	+	0,964	+	100	100
12	Approximate entropy test	0,999	+	0,998	+	100	100
13	Cumulative sums test	0,719	+	0,784	+	100	100
14	Random excursion test	0,065	+	0,321	+	97,2	96,1
15	Random excursion variant test	0,046	+	0,088	+	98	97,1

Для кожної групи були обчислені показники алгебраїчної степені нелінійності, відстань нелінійності, коефіцієнти кореляції S-блоку, лавинні властивості S-блоку, та період повернення S-блоку, наведені в таблиці 2.

З таблиці 2 видно, що експериментальні набори S-блоків задовольняють показникам алгебраїчної степені нелінійності, де майже всі S-блоки мають значення 7, та коефіцієнтам кореляції S-блоку, де всі коефіцієнти наближені до 0. Значення показників відстані нелінійності для значної кількості матриць не досягають 100, яке на практиці вважають орієнтиром, а лавинні властивостей S-блоку мають достатньо значні відхилення від 128. Період повернення S-блоку також є різним для експериментальних

блоків, і така помітна різниця пояснюється використанням великого числа псевдовипадкових чисел в структурі алгоритму та нерівномірним розподілом перестановок.

Таблиця 2.

Оцінка статистичних властивостей S-блоків

Показник	Значення показника	Кількість S-блоків з відповідними значеннями показників, %			
		Група 1	Група 2	Група 3	Група 4
Алгебраїчна степінь нелінійності	7 6	99.6% 0.4%	99.4% 0.6%	99.2% 0.8%	100% 0%
Відстань нелінійності	$x<96$ $96<=x<100$ $x>=100$	6.4% 36.1% 57.5%	7.2% 36.5% 56.3%	6.6% 38.3% 55.1%	4.7% 35.7% 59.6%
Коефіцієнти кореляції S-блоку	середнє значення	від -0.0237 до 0.0244	від -0.0227 до 0.0222	від -0.0249 до 0.0222	від -0.0205 до 0.0273
Лавинні властивості S-блоку	середнє значення	від 124 до 132.625	від 124 до 132.375	від 123.8125 до 132.8125	від 124.875 до 133.25
Період повернення S-блоку	середнє значення	4834855.51	15072582.9	37296991.63	13132147.81

Висновки. Незважаючи на певні просідання в значеннях окремих показників та тестів, вважаємо доцільними подальші дослідження розглянутого алгоритму перемішування за умови певних модифікацій в його структурі, а саме:

– замість секретного паролю та його хеш-значення використовувати повноцінний ключ довжиною не менше 256 бітів;

– розроблення зрозумілої та обґрунтованої процедури розширення ключа для отримання величин зсуву рядків і стовпців матриці;

– спрощення порядку вибору рядків і стовпців матриці та використання обчислювально легких операції для збільшення швидкодії перемішування.

Також має сенс дослідити мінімальну кількість ітерацій перемішування, яка забезпечувала б відповідність всім показникам статистичних властивостей S-блоків.

Оскільки в більшості криптографічних алгоритмах використовується більше однієї таблиці замін, а принаймні чотири, то слід провести дослідження властивостей комплексу, який включає від чотирьох і більше S-блоків. Також можливим є використання алгоритму перемішування в потоковому шифруванні для генерації гами за умови забезпечення високої швидкодії процедури перемішування. В подальших публікаціях означені питання будуть розглянуті більш детально.

Список літератури

1. Abbas Z., Saeed M.Q. Image Steganography using Cryptographic Primitives. *International Conference on Cyber Warfare and Security (ICCWS).* 2021, P 124-131. DOI: 10.1109/ICCWS53234.2021.9703017.
2. Alanzy M.; Alomrani R.; Alqarni B.; Almutairi S. Image Steganography Using LSB and Hybrid Encryption Algorithms. *Appl. Sci*. 2023, No.13. P. 11771. URL: https://doi.org/10.3390/app132111771
3. Bahaddad A.A., Almarhabi K.A. Sayed Abdel-Khalek. Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption. *Alexandria*

Engineering Journal. 2023. V. 75, P.41-54. URL: https://doi.org/10.1016/j.aej.2023.05.051

4. Ахмаметьєва Г.В., Бойко Н.В. Розробка алгоритму формування стеганографічного ключа для цифрових зображень. *«Шляхи розвитку науки в сучасних кризових умовах»: І Міжнародна науково-практична інтернет-конференція.* 2020. Т.1. С.32-35.
5. Vinodhini R.E., Vimalkumar K., Malathi P., Gireeshkumar T. A Highly Secured Image Steganography using Bernoulli's Chaotic Map and Binary Hamming Code. *International Journal of Pure and Applied Mathematics*. 2018. V. 118. No. 7. P.159-164.
6. Sahil, Sinwar D. A Steganography Technique based on chaos for Pseudo-Random LSB Images. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*. 2018. V. 6. No. II. P.436-440.
7. Al-Bahadili H.. A secure block permutation image steganography algorithm. *International Journal on Cryptography and Information Security (IJCIS)*. 2013. V.3. No. 3. P.11-22.
8. Sunder R., Eswaran P., Nagalinga R. A. High capacity image steganography in the spatial domain using Lehmer code. *International Journal of Advance Research In Science And Engineering (IJARSE)*. 2015. V.4. No.5. P.91-99.
9. Nagalinga R., Sunder R. Hiding text in digital images using permutation ordering and compact key based dictionary. *ICTACT Journal on Image and Video Processing*. 2017. V.7. No.4. P.1497-1504.
10. Bassam H.S., Elsamani A.E.A., Gafar Z.A.S., Abdelmajid H.M. A Spatial Domain Image Steganography Technique Based on Pseudorandom Permutation Substitution Method using Tree and Linked List. *International Journal of Engineering Trends and Technology* (IJETT). 2015. V.23. No 4. P.209-217.
11. Nazari S., Eftekhari-Moghadam A.M., Mohammad-Shahram M. A novel image steganography scheme based on morphological associative memory and permutation schema. *Security and Communication Networks*. 2015. No.8. P.110–121.
12. Shakir M. Hussain, Naim M. Ajlouni. Key Based Random Permutation (KBRP). *Journal of Computer Science*. 2006. No. 2 (5). P.419-421.
13. Бойко Н.В. Удосконалення стеганографічного методу для цифрових зображень. Розробка алгоритму формування стеганографічного ключу: квал. роб. бак. Одеса: НУ «одеська політехніка», 2020. 67 с.
14. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. *NIST Special Publication 800-22.* 2001.
15. Ахмаметьєва Г. Дослідження алгоритму формування стеганографічного ключа для побудови змінних криптографічних S-блоків. *Міжнародна науково-практичної конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика»*. 2023. С. 13-17.
16. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. К.: Мінекономрозвитку України, 2015.
17. Горбенко І. Д., Олійников Р.В., Казимиров О.В., Руженцев В.І., Кузнєцов О.О., Горбенко Ю.І., Дирда О.В., Долгов В.І., Пушкарьов А.І., Мордвінов Р.І. Симетричний блоковий шифр «Калина» – новий національний стандарт України. *Радіотехніка*. 2015. Вип. 181. С. 5–22.

RESEARCH OF THE STATISTICAL CHARACTERISTICS OF THE ALGORITHM FOR SHUFFLING THE ELEMENTS OF TWO-DIMENSIONAL MATRICES AS A BASIS FOR THE FORMATION OF VARIABLE S-BLOCKS

A.V. Akhmametieva[1], A.I. Garbuz[2]

[1] National University «Odesa Law Academy»
28, Rishilievska str., Odesa, 65000, Ukraine
[2] SSS «Professional College of Measurements of State University of Intellectual Technologies and Communications»
13, Spiridonivs'ka str., Odesa, 65020, Ukraine
Emails: anna.odessitka@gmail.com[1], garbuzartem@okv.suitt.edu.ua[2]

The article provides a description and analysis of the structure of the algorithm for formation of the steganographic key. Proposed algorithm is based on the shuffling of rows and columns of a two-dimensional matrix containing unique numerical values as a sequence of image pixel/block selection for embedding of the secret message. The structure of the algorithm was characterized from the point of view of the using of mixed two-dimensional matrices for the formation of variable S-blocks in cryptographic transformation. The advantages and disadvantages of the algorithms structure, possible directions for improving the mixing procedure and increasing the speed of the algorithm are revealed. Experimental S-blocks of size 16×16, which replace 8-bit blocks with new 8-bit values, were tested by NIST statistical tests, which showed that most of the formed tables meet the requirements of reliable pseudo-random sequences. In order to further apply the previously developed two-dimensional matrix shuffling algorithm for cryptographic transformation problems, the statistical properties of S-blocks were calculated - the algebraic degree of nonlinearity, the distance of nonlinearity, correlation coefficients of the S-block, avalanche properties of the S-block, and the return period of the S-block. The results of the experiment showed that for almost all tables, the value of the algebraic degree of nonlinearity is 7, which theoretically allows the use of the shuffling algorithm for the formation of variable S-blocks, but the fluctuation of other indicators requires further modification of the algorithm and the study of the influence of the algorithm parameters on the statistical characteristics of the formed substitution matrices.

Keywords: steganographic key, shuffling, two-dimensional matrix, cryptographic transformation, S-block of substitution, statistical properties, pseudorandom sequence.