



Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Інститут модернізації змісту освіти
Національний технічний університет України
«Київський політехнічний інститут» ім. І. Сікорського
Вінницький національний технічний університет
Житомирський державний університет ім. Івана Франка
Житомирський військовий інститут імені С.П. Корольова
Тернопільський національний технічний університет імені Івана Пулюя
Тернопільський національний економічний університет
Харківський національний університет радіоелектроніки
Уманський державний педагогічний університет імені Павла Тичини
Національний університет біоресурсів та природокористування України

ТЕЗИ ДОПОВІДЕЙ

II Всеукраїнської науково-технічної конференції

Комп'ютерні технології: інновації, проблеми, рішення

м. Житомир, 14-15 листопада 2019 р.

Житомир
2019

УДК 004.056.55

*Красиленко В.Г., канд. техн. наук., старш. наук. співроб., доцент,
Нікітович Д.В.*

¹ *Вінницький національний технічний університет*

МОДЕЛЮВАННЯ МЕТОДІВ ГЕНЕРУВАННЯ ПОТОКІВ МАТРИЧНИХ ПЕРЕСТАНОВОК ЗНАЧНОЇ РОЗМІРНОСТІ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ЗОБРАЖЕНЬ

Вступ. Поява нового класу криптосистем матричного типу (КМТ) [1-4], що базуються на основі матрично-алгебраїчних моделей (ММ) криптографічних перетворень (КП) 2D(3D) - масивів, зображень (З) та є узагальненням відомих криптосистем зі скалярними форматами даних на випадки матрично-тензорних форматів і які мають ряд суттєвих переваг, сприяла інтенсифікації досліджень КМТ, ММ та демонстрації цілої низки нових їх покращень та застосувань [5-10]. Узагальнені ММ, матричні афінні та афінно-перестановочні шифри, їх модифікації досліджувались та використовувались при створенні цифрових сліпих та інших покращених підписів у [11-15]. ММ при їх апаратних реалізаціях легше відображаються на матричні процесори, мають покращені крипто-стійкість та інші характеристики, дозволяють перевіряти цілісність криптограм чорно-білих, кольорових зображень і наявність у них перекручувань [5,7], мають розширені функціональні можливості за рахунок створення блокових [6], багатофункціональних параметричних [8] і багатосторінкових [9] моделей з їх значною стійкістю [10]. Матричні моделі перестановок (ММ_П) з процедурами множення матриць та деякими іншими по-елементними операціями за модулем над матрицями є одними з базових операцій, оскільки для реалізації КП необхідно матриці байтів зліва та справа помножити на матриці перестановок (МП), матрицю з рядків, колонок, векторів, що в унітарних кодах відображають символи, коди, байти, теж замінювати, переставляти за допомогою перестановок. Процедури переставлення бітів, байтів чи їх груп є найбільш поширеними та обов'язковими практично для всіх відомих та новостворюваних алгоритмів та шифрів. Для збільшення ентропії криптограм З при їх КП на основі ММ_П та зміни їх гістограм необхідні декомпозиція R,G,V складових і їх бітових зрізів та декілька матричних ключів (МК) типу МП [3-5]. Низка таких псевдовипадкових (поточних, покрокових, по-фреймових) МК, які б відповідали вимогам, швидко генерувались, потрібна і для маскування, КП відео-файлів чи потоку блоків з файлів, зображень при їх значних розмірах. **Постановка задачі.** Таким чином, для ММ є необхідність формування низки МП, які б задовольняли ряду вимог, з головного

МК. Оскільки питання узгодження головного МК загального виду, але не послідовності МП розглядались в [16,17], а методи генерування потоку МК перестановок частково розглядались в [18], але тільки для бітових МП невеликих розмірів ($256*256$), то **метою роботи** є спроба вдосконалити метод генерації низки МП, покращити та адаптувати вид, структуру, опис МП до формату 3 і до швидких апаратних рішень, суттєво розширити межі розмірності МП, промодельовати та дослідити процес формування потоку МП для МАР КП у системах МТ, перевірити властивості генерованих МП.

Виклад основного матеріалу та результатів дослідження. Огляд МТ шифрів, особливо багатофункціональних параметричних блочних [4], їх аналіз показують, що доцільно використовувати для досягнення мети ізоморфність різних представлень перестановок (матриць чи векторів), що вступають у ролі головного ключа (ГК) та по-блокових МК типу МП, тобто під-ключів (ПК), що являють собою матриці перестановок P (її степені !) чи ізоморфні їм вектори. З робіт [6,8,9] відомо, що для поблочних КП на основі МАПШ, ВАПШ криптограми деяких видів зображень та текстово-графічних документів (ТГД) при використанні одного ПК для всіх блоків є недостатніми по стійкості, та попри це низка ПК, що створюються з ГК, вирішує цю проблему. Розглянемо ситуацію, коли для КП блоків довжиною $256*256$ байтів, що представлені у вигляді матриці чорно-білого зображення необхідно переставити всі байти у відповідності до МП. В цьому випадку МП в загально прийнятому вигляді повинна бути квадратною з $N*N$ елементами («0» чи «1»), де $N=2^{16}$.

Потужність множини можливих таких МП, тобто їх кількість оцінюється, як $N!$, що дає для цього N колосальні значення. Але кожному адресу байту блоку можна представити і за допомогою двох байтів, що вказують дві координати (рядок та стовпчик) блоку. Це дає нам можливість двома блоками ($256*256$ елементів) байтів представляти любую перестановку, ставлячи в кожній однаковій адресі цих блоків відповідну старшому байту (в першому блоці) та молодшому байту (в другому блоці) координати нової адреси вибраного для перестановки байту. Вигляд програмного модуля у Mathcad для генерування базового (головного) МК (МП) та вигляд його складових $KeyA$ та $KeyB$ у форматі двох чорно-білих зображень показано на рис.1. Отже, любую МП можна однозначно відобразити двома матрицями розміром $256*256$, елементи яких приймають значення з діапазону 0-255, з тією особливістю, що кожна з 256 їх градацій інтенсивності в кожній з цих двох матриць (3) повторюється рівно по 256 раз. Узагальнюючи, можна стверджувати, що для ще більших за розміром МП останні можна

також однозначно представити за допомогою 3, 4 і т.д. блоків з байтів, аналогічних вищевказаним складовим KeyA та KeyB. Гістограми складових KeyA та KeyB МП зображені на рис.2 та, як і очікувалось, мають вигляд горизонтальних ліній. Там же показані і гістограми явного З та його криптограм після КП, наприклад, МАПШ при використанні такої МП.

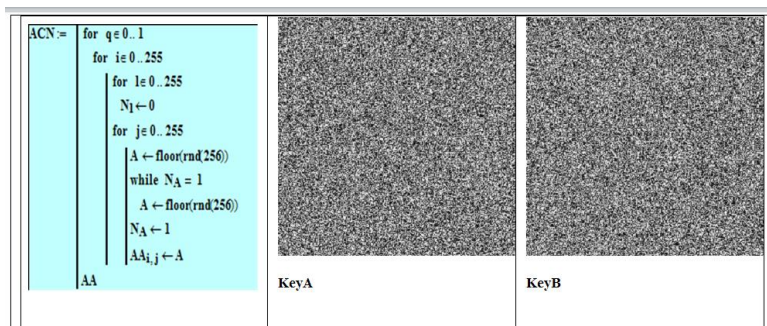


Рис. 1. Програмний модуль для генерування базового (головного) МК (МП) та вигляд складових KeyA та KeyB у форматі двох чорно-білих зображень (Вікно Mathcad).

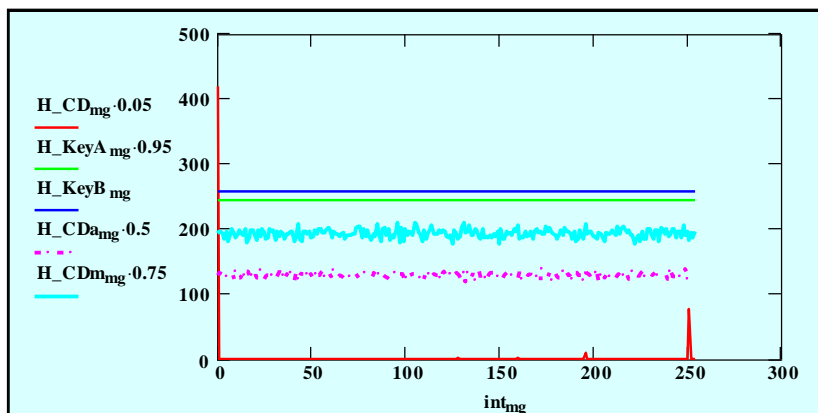


Рис. 2. Гістограми H_KeyA та H_KeyB відповідно складових KeyA та KeyB МП, гістограма H_CD криптограм явного З (співпадає з гістограмою З), відповідні гістограми H_CDa та H_CDm криптограм після адитивної та мультиплікативної афінних КП З за допомогою тих же KeyA та KeyB (Вікно Mathcad).

Результати моделювання КП зображення (Im) МАПШ за допомогою запропонованої МП та її складових, як ключів, з формулами, що відповідають перестановці та афінним КП, та матрицями явного З (Im), проміжних, його криптограми (Стар) та перевірними показані на рис.3, 4. Експериментами встановлено, що після додаткових афінних КП при використанні наявних 2-х складових МП ми отримуємо криптограми CD_ImAa та CD_ImAm, гістограми яких H_CDa та H_CDm настільки близькі до рівномірного закону розподілу, що навіть для Im з ентропією 0,738 ентропія криптограм збільшується аж до 7,99 та більше і відрізняється від теоретично максимальної (8 біт) всього на долі відсотка. Результати моделювання КП З (Im) МАПШ для випадку, коли спочатку виконуються складові афінних перетворень і у іншій послідовності та різними чи одним МК від МП, а потім перестановка за допомогою МП, дивись рис.4, також свідчать про достовірну якісну роботу шифру при застосуванні запропонованих представлень МП та багатокрокових МАПШ. З метою збільшення стійкості МАПШ при обробці файлів блоками для кожного поточного блоку бажано мати низку неповторюваних МК, генерованих з головного МК, наприклад, з такої ж МП, тому є актуальною задача дослідження процесів швидкого надійного генерування послідовності таких МП, з урахуванням вимог до їх крипто-статистичних характеристик.

$$\begin{aligned}
 CD_ImA_{i,j} &:= Im_{KeyA_{KeyA_{i,j}}, KeyB_{i,j}}^{KeyB_{KeyA_{i,j}}, KeyB_{i,j}} \\
 &\quad \xrightarrow{DDo_ImA_{KeyA_{KeyA_{i,j}}, KeyB_{i,j}}^{KeyB_{KeyA_{i,j}}, KeyB_{i,j}}} := CD_ImA_{i,j} \\
 CD_ImAav &:= ((CD_ImA + KeyA \cdot 1)) \\
 CD_ImAa &:= (\overrightarrow{\text{mod}(CD_ImAav, 256)}) - R1 \cdot 0 \\
 \min(CD_ImAav) &= 0 \quad \max(CD_ImAav) = 510 \quad DD_ImAav := (\overrightarrow{(CD_ImAa + 256 \cdot R1 - KeyA \cdot 1)}) \\
 \min(CD_ImAa) &= 0 \quad \max(CD_ImAa) = 255 \quad DD_ImAa := (\overrightarrow{\text{mod}(DD_ImAav, 256)}) - R1 \cdot 0 \\
 CD_ImAm_{i,j} &:= \text{mod}[(CD_ImAa_{i,j} + 1) \cdot KeyBm_{i,j}, 257] - 1 \quad \begin{array}{l} \min(DD_ImAav) = 128 \quad \max(DD_ImAav) = 511 \\ \min(DD_ImAa) = 0 \quad \max(DD_ImAa) = 255 \end{array} \\
 DD_ImAm_{i,j} &:= \text{mod}[(CD_ImAm_{i,j} + 1) \cdot KeyBmO_{i,j}, 257] - 1 \quad ER_Aa := (\overrightarrow{|CD_ImA - DD_ImAa|}) \cdot 255 \\
 &\quad \max(ER_Aa) = 0
 \end{aligned}$$

Рис. 3. Фрагмент вікна Mathcad з формулами для моделювання МАПШ на основі складових МП, як адитивного та мультиплікативного МК.

Першим методом, по аналогії з [18], є використання деяких, узгоджених сторонами скалярів ха та хп (одного чи двох), як ключів для

КП (зашифрування) ними складових Key_A та Key_B головної МП (ГМП) за допомогою афінного шифру з операціями за модулем 257. Пара, утворених з них криптограм будуть складовими нової МП, яка буде повністю зберігати всі необхідні властивості ГМП, мати аналогічні гістограми та відповідати вимогам.

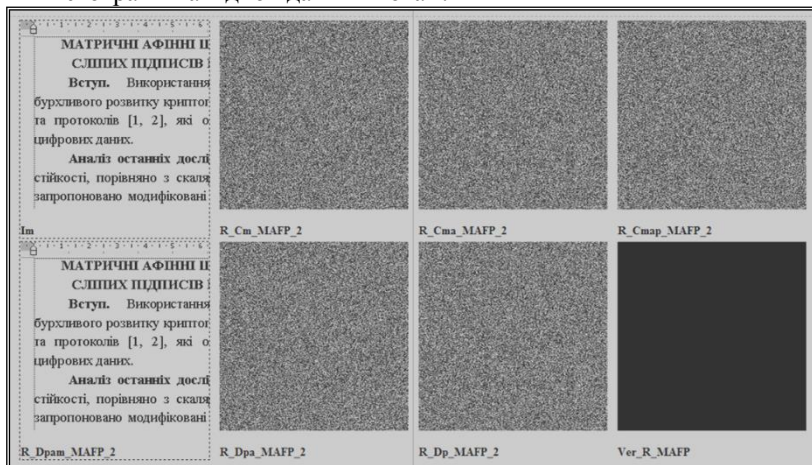


Рис. 4. Результати моделювання МАФШ на основі МП та її складових, як адитивного та мультиплікативного МК. Верхній ряд, зліва направо: явне, після перетворень, криптограма після МАФШ; Нижній ряд: відновлене, проміжні та різницеве (праворуч) зображення ТГД.

Оцінки показують, що число різних таких пар скалярів при відкиданні значень «0» та «1» для x та xm може бути $254 \cdot 254$, а кількість можливих переставлять цих пар у їх послідовній множині оцінюється значною величиною $(254 \cdot 254)!$, що дозволяє створювати низки МК (МП) значної довжини. Для практичних застосувань навіть одного мультиплікативного афінного (лінійного) КП достатньо, щоб з множини 254-ти значень xm створювати, крім того, й без повторів, значну кількість, а саме $254!$, узгоджених сторонами випадкових векторів довжиною 254 для формування ними послідовності таких МП у вигляді двох зображень.

На рис. 5 показані результати моделювання процесів генерування МК Key_M , як першої складової нової МП, з Key_A складової МП у Mathcad з формулами та матрицями Key_M для $xm = km = 17$. Генерування другої складової виконується з тим же $km = 17$, але від Key_B . Пари криптограм, утворених за допомогою афінного шифру зі складових Key_A та Key_B ГМП і є i -ими поточними матричними перестановками, що відображаються у вигляді двох матриць розмірністю

(256*256). Оскільки, ГМП та 2 (чи 1) узгоджені допоміжні векторні ключі (ВК) є секретними і відомі лише сторонам процесу КП, то цю послідовність МК (МП) створювати чи мати можуть лише вони, а за рахунок специфічності гістограм складових МП та їх ентропій (рівних 8 біт!) крипто-аналіз унеможлиблюється. Секретними, узгодженими можуть бути лише ГМП або ВК.

		$\text{KeyM}(km, \text{KeyA}) := \begin{array}{l} \text{for } i \in 0..255 \\ \quad \text{for } j \in 0..255 \\ \quad \quad W_{i,j} \leftarrow \text{mod}[(\text{KeyA}_{i,j} + 1) \cdot km, 257] - 1 \\ \quad W \end{array}$									
KeyAkm =		0	1	2	3	4	5	6	7	8	9
	0	201	128	218	79	195	71	175	159	86	115
	1	6	170	118	190	169	16	246	216	48	46
	2	26	205	35	29	173	141	90	34	240	183
	3	10	69	46	150	45	28	48	172	191	43
	4	73	65	139	94	230	105	84	59	87	162
	5	124	19	204	43	5	220	142	78	57	45
	6	21	96	223	232	31	233	158	91	41	40
	7	223	22	66	90	129	151	118	181	4	126
	8	206	232	1	175	98	199	19	200	228	238
	9	141	194	244	154	146	155	82	44	90	76
	10	224	216	152	80	169	213	99	88	39	107
	11	179	121	68	238	123	45	141	33	141	218
	12	194	86	82	163	198	8	36	38	136	46
	13	56	176	185	31	85	95	84	182	173	87
	14	202	207	35	119	6	218	43	172	30	111
15	104	81	62	0	56	196	27	5	171	15	
KeyM(17, KeyA) =		0	1	2	3	4	5	6	7	8	9
	0	201	128	218	79	195	71	175	159	86	115
	1	6	170	118	190	169	16	246	216	48	46
	2	26	205	35	29	173	141	90	34	240	183
	3	10	69	46	150	45	28	48	172	191	43
	4	73	65	139	94	230	105	84	59	87	162
	5	124	19	204	43	5	220	142	78	57	45
	6	21	96	223	232	31	233	158	91	41	40
	7	223	22	66	90	129	151	118	181	4	126
	8	206	232	1	175	98	199	19	200	228	238
	9	141	194	244	154	146	155	82	44	90	76
	10	224	216	152	80	169	213	99	88	39	107
	11	179	121	68	238	123	45	141	33	141	218
	12	194	86	82	163	198	8	36	38	136	46
	13	56	176	185	31	85	95	84	182	173	87

Рис. 5. Формули та вигляд (2D) генерованого МК з ГМП простим лінійним КП та функціональним параметричним.

Другим методом генерування поточних МП є застосування однокричлічних зсувів складових ГМП по x та y координатах на від-

повідні вибрані (узгоджені сторонами) значення (1-254). Моделювання цього методу тут, з урахуванням обмежень, не наводяться, але отримані результати також підтверджують забезпечення тих же можливостей, якостей та вищенаведених оцінок, що і для першого методу. Оскільки ці зсуви є одним з часткових видів загальних можливих перестановок, але елементів самих складових ГМП, то відкривається можливість, здійснюючи самою ГМП одноразову (багаторазову) перестановку байтів її складових відображень, отримувати нові МП, що будуть повністю відповідати вимогам. А тому, **третій метод** генерування полягає у піднесенні ГМП у степінь, що відповідає і-тій компоненті векторного ключа. Проте суть таких піднесень еквівалентно замінюється швидкими перестановками, які до того ж можуть бути ще більш прискореними при значних степенях за рахунок використання деякого базового набору фіксованих (фіксовані степені ГМП) та специфічної їх послідовності. Результати формування цим методом потоку МП при його моделюванні у Mathcad показані на рис.6 та підтверджують його адекватність, коректність, відповідність вимогам, досягнення суттєвих переваг за рахунок прискорень обчислення степенів ГМП, простоти можливих реалізацій і зменшення затрат.

P_s16A := T_FF(15, KeyA) P_s16B := T_FF(15, KeyB)										P_SwVA := T_PFW(4, P_s16A, P_s8A, P_s8B)										P_Sw84B := T_P												
P_sAV := T_FF(75, KeyA) P_sBV := T_FF(34, KeyB)										P_SwVB := T_PFW(1, P_s4B, P_s16A, P_s16B)																						
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9			
0	170	88	242	27	94	186	117	16	11	185	0	170	88	242	27	94	166	117	16	11	185	0	170	88	242	27	94	166	117	16	11	185
1	250	225	13	106	20	140	2	86	154	137	1	250	225	13	106	20	140	2	86	154	137	1	250	225	13	106	20	140	2	86	154	137
2	29	87	171	78	55	9	92	104	115	106	2	29	87	171	78	55	9	92	104	115	106	2	29	87	171	78	55	9	92	104	115	106
3	212	203	173	73	26	111	255	37	96	236	3	212	203	173	73	26	111	255	37	96	236	3	212	203	173	73	26	111	255	37	96	236
4	88	178	205	155	190	58	138	32	204	194	4	88	178	205	155	190	58	138	32	204	194	4	88	178	205	155	190	58	138	32	204	194
5	230	134	215	101	149	88	220	48	4	223	5	230	134	215	101	149	88	220	48	4	223	5	230	134	215	101	149	88	220	48	4	223
6	113	27	166	121	25	255	31	169	221	199	6	113	27	166	121	25	255	31	169	221	199	6	113	27	166	121	25	255	31	169	221	199
7	111	96	249	42	171	187	24	212	101	64	7	111	96	249	42	171	187	24	212	101	64	7	111	96	249	42	171	187	24	212	101	64
8	210	202	91	25	187	26	203	63	197	227	8	210	202	91	25	187	26	203	63	197	227	8	210	202	91	25	187	26	203	63	197	227
9	8	61	213	143	171	250	89	85	17	29	9	8	61	213	143	171	250	89	85	17	29	9	8	61	213	143	171	250	89	85	17	29
10	109	103	219	127	66	35	237	225	158	114	10	109	103	219	127	66	35	237	225	158	114	10	109	103	219	127	66	35	237	225	158	114
11	4	208	105	200	205	123	245	227	43	112	11	4	208	105	200	205	123	245	227	43	112	11	4	208	105	200	205	123	245	227	43	112
12	74	13	136	83	73	241	62	160	17	156	12	74	13	136	83	73	241	62	160	17	156	12	74	13	136	83	73	241	62	160	17	156
13	132	54	201	99	126	185	121	69	157	184	13	132	54	201	99	126	185	121	69	157	184	13	132	54	201	99	126	185	121	69	157	184
14	113	10	134	112	203	64	151	18	53	239	14	113	10	134	112	203	64	151	18	53	239	14	113	10	134	112	203	64	151	18	53	239
15	178	88	50	129	176	119	134	213	87	216	15	178	88	50	129	176	119	134	213	87	216	15	178	88	50	129	176	119	134	213	87	216

P_sAV := T_FF(75, KeyA) P_sBV := T_FF(34, KeyB)										P_SwVA := T_PFW(4, P_s16A, P_s8A, P_s8B)										P_Sw84B := T_P												
P_sAV := T_FF(75, KeyA) P_sBV := T_FF(34, KeyB)										P_SwVB := T_PFW(1, P_s4B, P_s16A, P_s16B)																						
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9			
0	247	171	226	116	214	113	85	115	6	152	0	247	171	226	116	214	113	85	115	6	152	0	247	171	226	116	214	113	85	115	6	152
1	87	21	32	230	178	45	170	139	77	43	1	87	21	32	230	178	45	170	139	77	43	1	87	21	32	230	178	45	170	139	77	43
2	38	10	45	29	226	245	181	81	36	62	2	38	10	45	29	226	245	181	81	36	62	2	38	10	45	29	226	245	181	81	36	62
3	84	249	31	194	157	214	30	137	61	148	3	84	249	31	194	157	214	30	137	61	148	3	84	249	31	194	157	214	30	137	61	148
4	179	252	250	228	145	142	105	221	56	133	4	179	252	250	228	145	142	105	221	56	133	4	179	252	250	228	145	142	105	221	56	133
5	8	252	221	48	192	254	192	29	3	22	5	8	252	221	48	192	254	192	29	3	22	5	8	252	221	48	192	254	192	29	3	22
6	27	108	100	54	136	117	195	121	133	202	6	27	108	100	54	136	117	195	121	133	202	6	27	108	100	54	136	117	195	121	133	202
7	174	208	151	14	96	83	239	190	180	168	7	174	208	151	14	96	83	239	190	180	168	7	174	208	151	14	96	83	239	190	180	168
8	154	115	120	75	234	28	193	129	161	117	8	154	115	120	75	234	28	193	129	161	117	8	154	115	120	75	234	28	193	129	161	117
9	60	77	212	58	110	201	221	45	76	79	9	60	77	212	58	110	201	221	45	76	79	9	60	77	212	58	110	201	221	45	76	79
10	29	186	49	0	14	32	57	155	184	185	10	29	186	49	0	14	32	57	155	184	185	10	29	186	49	0	14	32	57	155	184	185
11	221	224	55	137	113	172	145	181	109	206	11	221	224	55	137	113	172	145	181	109	206	11	221	224	55	137	113	172	145	181	109	206
12	208	64	248	88	37	216	241	141	128	239	12	208	64	248	88	37	216	241	141	128	239	12	208	64	248	88	37	216	241	141	128	239
13	171	90	214	10	56	244	118	154	62	129	13	171	90	214	10	56	244	118	154	62	129	13	171	90	214	10	56	244	118	154	62	129
14	198	134	154	204	130	111	194	48	251	152	14	198	134	154	204	130	111	194	48	251	152	14	198	134	154	204	130	111	194	48	251	152
15	100	202	82	220	93	228	229	252	42	165	15	100	202	82	220	93	228	229	252	42	165	15	100	202	82	220	93	228	229	252	42	165

Рис. 6. Формули та частина цифрових масивів генерованого МК з ГМП шляхом ітераційних чи послідовних фіксованих перестановок.

Використовуючи розроблені функціональні параметричні моделі КП за допомогою генерованих МП, що показані на рис.7, було виконано перевірку правильного до вимог їх синтезу та адекватності моделей шляхом прямого та зворотного КП З лише за допомогою цих МП. Отримані моделюванням у Mathcad результати, а саме: криптограми, відновлені, явні та різниці З, дивись рис.8, та дають такі висновки.

$\text{Ckm} := \text{T_PFW}(5, \text{PIC_colR}, \text{KeyAkm}, \text{KeyBkm})$ $\text{DCkm} := \text{T_PFWO}(5, \text{Ckm}, \text{KeyAkm}, \text{KeyBkm})$ $\text{ErCkm_DC} := \overline{ \text{PIC_colR} - \text{DCkm} }$ $\alpha := 7 \quad \beta := 77$ $\text{CM} := \text{T_PFW}(\alpha, \text{PIC_colR}, \text{KeyM}(\beta, \text{KeyA}), \text{KeyM}(\beta, \text{KeyB}))$ $\text{DCM} := \text{T_PFWO}(\alpha, \text{CM}, \text{KeyM}(\beta, \text{KeyA}), \text{KeyM}(\beta, \text{KeyB}))$ $\text{ErCM_DC} := \overline{ \text{PIC_colR} - \text{DCM} }$	
$\text{T_PFW}(qw, F, \text{Akey}, \text{Bkey}) :=$	<pre> p ← 0 S ← F while p < qw S ← for i ∈ 0..255 for j ∈ 0..255 W_{i,j} ← S_{Akey Akey_{i,j}, Bkey_{i,j}} · Bkey_{Akey_{i,j}, Bkey_{i,j}} W p ← p + 1 S </pre>
$\text{T_PFWO}(qw, F, \text{Akey}, \text{Bkey}) :=$	<pre> p ← 0 S ← F while p < qw S ← for i ∈ 0..255 for j ∈ 0..255 W_{Akey Akey_{i,j}, Bkey_{i,j}} · Bkey_{Akey_{i,j}, Bkey_{i,j}} ← S_{i,j} W p ← p + 1 S </pre>

Рис. 7. Функціональні параметричні моделі КП на базі створених МП

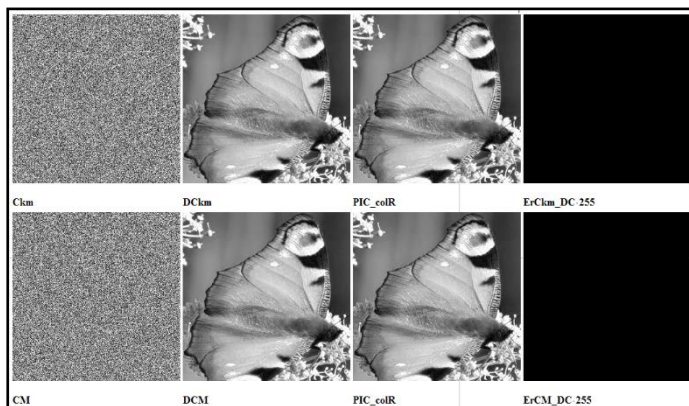


Рис. 8. Пряме та зворотне КПЗ на основі генерованих МП

Висновки. Запропоновано три вдосконалених метода генерації низької МП значної розмірності та їх модифікації. Результати експериментів, моделювання та оцінки стійкості підтвердили якість МП, адекватність функціонування моделей та запропонованих методів генерування МП, їх переваги. Моделі прості, зручні, адаптуються для різноформатних та кольорових зображень, реалізуються матричними процесорами, мають високі ефективність, стійкість, швидкодію.

Список літературних джерел:

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. НУ "Львів. політехніка". - 2009. - № 658. - С. 59-63.

2. Красиленко В. Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. - 2012. - Вип. 3(2). - С. 53-61. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

3. Красиленко В.Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрислою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельн. НУ. Технічні науки. - 2014. - № 1. - С. 74-79.

4. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрислою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво : наук. журн. – Луцьк: Видавництво Луц. нац. техн. ун-т., - 2016. - № 23. - С. 31-36. – Режим доступу: <http://ki.lutsk-ntu.com.ua/node/132/section/9> .

5. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-біговозрислової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології. – Львів: ЛНУ імені Івана Франка, 2016. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf

6. Красиленко В.Г. Моделі блокових матричних афінно-перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження / В.Г. Красиленко, Д.В. Нікітович // 72 НТК: матеріали конференції (13-15 грудня 2017 р.). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.117-122.

7. Красиленко, В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В. Г. Красиленко, К. В. Огородник, Ю.А.Флавицька // Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. НПК – К., 2010. – С.120-124.

8. Красиленко В.Г. Багатофункціональні параметричні матрично-алгебраїчні моделі (МAM) криптографічних перетворень (КП) з операціями за модулем та їх моделювання. / В.Г. Красиленко, Д.В. Нікітович. // 72 НПК: матеріали конференції (13-15 грудня 2017 року). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.123-128.

9. Красиленко В.Г. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей ІХ Міжнародної НТК, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 73-77.

10. Красиленко В.Г. Дослідження покращеного багатокрокового 2D RSA шифру та його гістограмно-ентропійних характеристик / В.Г. Красиленко, Д.В. Нікітович // «Інформаційна безпека та комп'ютерні технології»: Збірник тез доповідей ІІІ Міжнародної НПК, 19-20 квітня 2018 року. – Кропивницький: ЦНТУ, 2018. – С. 78-82. Режим доступу: <http://it-kntu.kr.ua/wp-content/uploads/2015/01/Zbirnyk-tez-InfoSecCompTech-2018.pdf>

11. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60 – 63.

12. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р.О. Яцковська,

Ю.М. Трифонова, // Системи обробки інформації. – 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

13. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстografічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: «ВидавІнформ НУ «ОМА», 2017. – С. 312 -318.

14. Красиленко В.Г. Моделювання покращених сліпих електронних цифрових підписів 2D типу / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної науково-технічної конференції, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 78-82.

15. Красиленко В.Г. Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису / В.Г. Красиленко, Д.В. Нікітович, Р.О. Яцковська, В.І. Яцковський // Системи обробки інформації: збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2019. – Вип. 1 (156). – С. 92-100. – [Електронний ресурс]. – Режим доступу: <https://doi.org/10.30748/soi.2019.156.12>

16. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації. – 2017. – Вип. 3 (149). – С 151-157.

17. Красиленко В.Г. "Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів" / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: ЛНТУ, 2017. – Вип. 26. – С 111-120. - Режим доступу: <http://ki.lutsk-ntu.com.ua/node/134/section/27> .

18. Красиленко В.Г. Моделювання процесів генерування матричних ключів / В.Г. Красиленко, Д.В. Нікітович // «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2018): Збірник тез доповідей IV Міжнародної науково-практичної конференції, 17-18 травня 2018 року. –Черкаси: ЧДТУ, 2018. – С. 32-35. Режим доступу: <https://chdtu.edu.ua/itont-2018/materiali-konferentsiji>

Секція 1. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Атоєв К.Л., Шпиґа С.П.	Математичне моделювання управління складними нелінейними системами	3
Барановський М.М., Кравченко С.М.	Тенденції розвитку штучного інтелекту в медицині	5
Галицький В. М., Галицький В. В.	Аналіз методів розпізнавання об'єктів на зображенні із застосуванням бібліотеки OPENCV	7
V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich	Design and modeling of digital multifunctional image processors based on the sorting node and method of processing weighting-selecting signals of rank differences	9
Зіньков Р.В., Марчук Г.В.	Принцип дії мурашиного алгоритму при вирішенні задачі Комівояжера	17
Лобанчикова Н.М., Лобач С.І.	Система управління освітленням офісного приміщення за допомогою веб-додатку	19
Лобанчикова Н.М., Мацюк К.О.	Веб-додаток управління припливно-витяжною вентиляцією у виробничому приміщенні	21
Лісовий Є. М., Левківський В.Л., Вакалюк Т.А.	Необхідність розробки додатку оптимізації вивезення побутових відходів	23
Любченко Д.В.	Система винагород і заохочень студентів закладів вищої освіти за допомогою віртуальної валюти	25
Каліберда С.С., Морозов А.В., Марчук Г.В.	Прогнозування хронічних захворювань	27
Пулеко І.В.	Принципи забезпечення функціональної стійкості інформаційних систем з розподіленими динамічними об'єктами управління	29
Пшеничний В.В.,	Використання Google Maps Platform	31

Кравченко С.М.	для відображення стану криміногенної ситуації на території України	
Романюк О. Н., Пивовар М.А., Перун І.В., Чехмestрук Р.Ю.	Аналіз алгоритмів пошуку осі дзеркальної симетрії обличчя людини	33
Романюк О.Н., Романюк О.В., Денисюк А.В.	Розподілення обчислювального процесу при реалізації зафарбовування в графічному процесорі	37
Туйчев В.В., Кательніков Д.І.	Розробка програмного забезпечення доповненої реальності для розпізнавання рухів з використанням технологій SWIFT, ARKIT, COREML	39
Ічанська Н. В., Улько С. І., Бережний А. В.	Розробка мобільного додатку для моніторингу стану тварин за допомогою фреймворку ANGULARJS	41
Постова С. А.	Моделювання роботи детермінованих одноканальних систем масового обслуговування за допомогою мови C++	43
Рокицький О.С., Сугоняк І.І.	Використання кластерного аналізу для сегментації користувачів	46
Семенець Б.С., Морозов А.В.	CRM-системи в структурі сучасних бізнес-зв'язків	48
Тимченко А.О., Кравченко С.М.	Дослідження процесів застосування згорткової нейронної мережі	50
Цюпа І.В., Сугоняк І.І.	Використання прогнозування в управлінні фінансами домашнього господарства	52
Погрібний А. П., Чумакевич В.В., Чумакевич В.О.	Особливості математичного моделювання геотехнічних ситуацій при дослідженні району будівництва	54
Чернишов К.А., Майданюк В.П.	Аналіз впровадження безготівкових транзакцій у вендингових пристроях	56
Головня С.А., Марчук Г.В.	Кластерний аналіз: ієрархічна кластеризація	58
Ісаєв А.М., Сугоняк І.І.	Розробка системи моніторингу стану автошляхів	60
Секція 2. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА		
Опанасюк Г.В., Єфіменко А.А.	Проект інформаційно-комунікаційної мережі спеціального призначення	63
Лоевський В.О.	Інформаційна система контролю тех-	65

	нічного стану комп'ютерів корпоративної мережі	
Красиленко В. Г., Нікітович Д. В.	Моделювання методів генерування потоків матричних перестановок значної розмірності для криптографічних перетворень зображень	67
Дрейс Ю.О., Лозова І.Л.	Розробка GDPR-моделі параметрів оцінювання наслідків витоку персональних даних	78
Криворучик Д.П.	Автоматизація за допомогою використання ботів	80
Кулініч І.Б.	Виклики глобального розвитку IoT, інновації і нові можливості в с/г	82
Дегтярьова А.А., Вакалюк Т.А.	Дослідження процесів захисту інформації в IoT	84
Бондарчук А.В., Єфіменко А.А.	Необхідність впровадження технології MPLS в мережах провайдерів та операторів зв'язку	88
Романченко Д.М., Єфіменко А.А.	Використання патернів проектування для підвищення ефективності автоматизації процесу тестування	90
Секція 3. ЦИФРОВА ОБРОБКА СИГНАЛІВ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ		
Бугайов. М.В.	Метод оцінювання завантаженості спектру для систем автоматичного радіоконтролю	92
Волотовська В.В.	Експериментальні дослідження датчика вологості ґрунту системи управління параметрами мікроклімату	94
Дончук М.О., Меленський В.Д.	Радіопеленгатор ультракороткохвильового діапазону на базі SDR приймача	96
Лугових О.О., Табалюк Д.С.	Використання вейвлет-фільтрації при дослідженні властивостей дизельного біопалива	98
Лугових О.О., Цвет Т.П.	Дослідження методів сегментації зображень для структурних елементів поверхні виробів з природного каменю	100
Подчашинський Ю.О.,	Дослідження методів фільтрації циф-	102

Шавурська Л.Й.	рових зображень, що містять вимірювальну інформацію	
Фірта Д.О., Воронова Т.С., Чепюк Л.О.	Системи розпізнавання мови	104

Секція 4. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ. ПРИЛАДОБУДУВАННЯ

Безвесільна О.М., Ткачук А.Г.	Автоматизований комплекс стабілізації озброєння	106
Бойко Л.К., Наумов Д.О.	Новітні методи виготовлення багат шарових друкованих плат з вбудованими електронними компонентами	108
Безвесільна О.М., Ткачук А.Г.	Двоканальний ємнісний мемс гравіметр	110
Богдановський М.В., Кузьменко К.В.	Перспективи та прогрес реалізації прототипу мобільної платформи на базі коліс Ілона для транспортних систем	112
Коваль А.В., Ткачук А.Г., Гриневич М.С.	Мобільна бездротова автоматизована система аналізу якості повітря	114
Безвесільна О.М., Ткачук А.Г.	Трикоординатний авіаційний гравіметр	116
Ізмайлов М.М., Сіротюк В.А., Рібоженко М.В., Держановський Б.І., Задорожня І.М.	шляхи оптимізації параметрів систем Автоматичного керування електроприводами важких машин на основі ефекту резонансної електромеханічної взаємодії	118
Ковальчук Р.Ю., Крижанівська І.В.	Автоматизована система відмикання-замикання гаражних воріт житлових будинків	120
Андреев П.І., Степаняк М.В.	Пристрій контролю та управління доступом до об'єкта	122

Секція 5. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТЕЛЕКОМУНІКАЦІЯХ ТА МЕДИЦИНІ

Говорадло П.П., Коломієць Р.О.	Дослідження процесів диференціації біосигналів для протезування верхніх кінцівок	124
Дубина О.Ф.	Визначення точності виміру паралакса при автоматичній обробці стереознімків	126

Сілі І.І.	Шляхи застосування вихрового ефекту та труби Ранка-Хілша у медицині	128
Ічанська Н. В., Улько С.І., Бережний А.В.	Розробка мобільного додатку для моніторингу стану тварин за допомогою фреймворку AngularJS	130
Андреев О.В., Білоцький М.О.	Дослідження точності місцевизначення з використанням GPS - трекера технології IoT	132
Ванельчук О.С., Корніюк А.В., Нікітчук Т.М.	Моделювання пульсової хвилі на вираженій ділянці променевої артерії	134
Левицький Б.В., Чухов В.В.	Дослідження виявлення дефектів графічної матриці при ультразвуковому дослідженні	136
Коренівська О.Л., Мартинчук П.П., Опанасюк Д.П.	Дослідження просторового розподілу іонів повітря від джерела аеронів	138
Секція 6. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ		
Бевз С.В., Войтко В.В., Бурбело С.М., Завальнюк Є.К., Козубенко М. В., Невський В.С., Пастух М.О.	Розробка інформаційно-комунікаційної технології з використанням квест-системи	140
Віров О.Ю. Семенець С.П.	Individualized adaptive learning Концептуальні засади використання засобів інформаційно-комунікаційних технологій в умовах компетентнісної математичної освіти	142 144
Вакалюк Т.А., Рантюк І.І.	Організаційні структури у ІТ компаніях	146
Декарчук С.О.	Законодавчі засади впровадження електронного підручника як інноваційного засобу навчання	148
Іщенко Г.В., Шумигай С.М.	Використання інтерактивних презентацій Prezi у підготовці майбутніх учителів математики	150
Мельник Н.В.	Активізація навчально-пізнавальної діяльності учнів у процесі навчання	152

Возносименко Д.А.	програмуванню Підготовка майбутніх учителів до використання QR-кодів у здо- ров'язберігаючій діяльності учнів на уроках математики	154
Плахотнюк І.М.	Цифровізація в сучасному вищому навчальному закладі	156
Решітник Ю.В.	використання ресурсу Wolfram Demon-?Trations Project під час лек- ційних занять із загальної фізики	158
Кривонос О.М., Кривонос М.П.	Огляд середовища для роботи з Arduino Fritzing	160
Іщенко Г.В., Дубовик В.В.	Використання системи Mathematica під час навчання лінійної алгебри	162
Ніжегородцев В.О., Нечепоренко А.О.	Інформаційні технології в системі підготовки фахівців державного пуб- лічного управління	164