ЗМІСТ

Секція 1
Інтелектуальні інформаційні технології

Григорович В.Г. ПРОБЛЕМИ ПОБУДОВИ СЕМАНТИЧНИХ ВІДНОШЕНЬ ТА МЕТРИКИ ДЛЯ ОЦІНЮВАННЯ КОНЦЕПТІВ В ОНТОЛОГІЯХ ……... **6**

Клапата Н.І., Лучкевич М.М. СИСТЕМА ІДЕНТИФІКАЦІЇ ВІДБИТКІВ ПАЛЬЦІВ ЛЮДИНИ …..……..……... **9**

Секція 2
Моделювання та дослідження складних систем

Бурда Ю.Р. РОЗРОБЛЕННЯ ДОДАТКУ «МАСАЖНИЙ САЛОН» ……..….. **15**

Дорошенко М.В. ЦИФРОВА ОБРОБКА ЗОБРАЖЕНЬ ЗАСОБАМИ ПАКЕТУ WAVELET TOOLBOX ……. **18**

Красиленко В.Г., Нікітович Д.В. ВДОСКОНАЛЕННЯ ТА МОДЕЛЮВАННЯ МЕТОДУ ГЕНЕРУВАННЯ ПОТОКУ МАТРИЧНИХ ПЕРЕСТАНОВОК ЗНАЧНОЇ РОЗМІРНОСТІ ……. **23**

Krasilenko V.G., Lazarev A.A., Nikitovich D.V. DEVELOPMENT AND SIMULATION ARRAY OF DEVICES BASED ON THE FPGA FOR PARALLEL CALCULATION OF NORMALIZED EQUIVALENCES OF THE REFERENCE FILTERS WITH THE CURRENT PROCESSED FRAGMENT OF THE IMAGE ……..…. **37**

Лазурчак Л.В. СЕРЕДОВИЩЕ РОЗРОБКИ RAD STUDIO ДЛЯ СТВОРЕННЯ ВЛАСНИХ ПРОЕКТІВ …….. **51**

Макарова Л.М., Торопов В.М. ЙМОВІРНІСНІ МОДЕЛІ РОЗПОДІЛУ ЧАСУ НАПРАЦЮВАННЯ МІЖ ВІДМОВАМИ БАНКОМАТІВ ……..….. **53**

Пелещак Р.М., Даньків О.О., Кузик О.В., Михавчак Г.В. МОДЕЛЮВАННЯ ПЕРЕБУДОВИ ЗОННОЇ СТРУКТУРИ НАПІВПРОВІДНИКА ПІД ВПЛИВОМ ЛАЗЕРНОГО ОПРОМІНЕННЯ …….. **58**

*Приходько С.Б., Книрік К.О.*НЕЛІНІЙНА РЕГРЕСІЙНА МОДЕЛЬ ДЛЯ ОЦІНЮВАННЯ ТРУДОМІСТКОСТІ РОЗРОБКИ МОБІЛЬНИХ ЗАСТОСУНКІВ НА ПОЧАТКОВОМУ ЕТАПІ ПРОЕКТУВАННЯ …… **64**

Приходько С.Б., Приходько Н.В., Місюра А.О. ПОБУДОВА НЕЛІНІЙНОЇ РЕГРЕСІЙНОЇ МОДЕЛІ ДЛЯ ОЦІНЮВАННЯ РОЗМІРУ PHP-ЗАСТОСУНКІВ З ВІДКРИТИМ КОДОМ ЗА МЕТРИКАМИ ДІАГРАМИ КЛАСІВ ……..……... **67**

Сікора О.В., Жидик В.Б. ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ УДОСКОНАЛЕННЯ ПРОЦЕСУ КОНДУКТИВНОГО СУШІННЯ ПОЛІГРАФІЧНИХ МАТЕРІАЛІВ ……..… **71**

Ших Н.В., Шаклеіна Н.В. АНАЛІЗ ПОПУЛЯРНИХ СЕРЕДОВИЩ КРОС-ПЛАТФОРМНОЇ РОЗРОБКИ МОБІЛЬНИХ ДОДАТКІВ ……..... **74**

Секція 3
Інформаційні технології соціокомунікаційних систем та мереж

Васьків Н.Ф. РОЗРОБЛЕННЯ ВЕБ-ПЛАТФОРМИ «FREELANCE» ……... **79**
Мартинов С.В. РОЗРОБЛЕННЯ МОБІЛЬНОГО ДОДАТКУ «АВТООРГАНАЙЗЕР» ……..…… **72**
Моржин А.Ю. РОЗРОБЛЕННЯ КЛІЄНТСЬКОЇ ЧАСТИНИ СТРІМІНГОВОГО ВІДЕО-СЕРВІСУ ……..…… **85**
Собків Р.А. ІГРОВИЙ ДОДАТОК "WHAT IS THIS SONG?" ……..… **88**

Секція 4
Інформаційно-комунікативні технології в освіті та наукових дослідженнях

Вдовичин Т.Я. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІКТ УЧАСНИКАМИ ОСВІТНЬОГО ПРОЦЕСУ ЗВО ……..…… **91**
Воронка Н.В. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ДИФЕРЕНЦІЙОВАНОГО НАВЧАННЯ НА УРОЦІ ІНФОРМАТИКИ В ПОЧАТКОВІЙ ШКОЛІ …….. **93**
Гальчишак М.Р. ОСОБЛИВОСТІ МИСЛЕННЄВОЇ ДІЯЛЬНОСТІ МОЛОДШИХ ШКОЛЯРІВ НА УРОЦІ ІНФОРМАТИКИ В ПОЧАТКОВІЙ ШКОЛІ ……..…… **97**
Гарбич-Мошора О.Р. ПЕРСПЕКТИВИ ВИКОРИСТАННЯ MEGAPOLIS.DOCNET ……..…….. **102**
Григорович А.Г., Сосяк Р.М., Хевпа Д.Я. СИСТЕМА ДИСТАНЦІЙНОГО НАВЧАННЯ ОСНОВАМ ПРОГРАМУВАННЯ ……..... **104**
Гринько В.О. РЕАЛІЗАЦІЯ НАВЧАЛЬНО-ДОСЛІДНИЦЬКОГО ПРОЕКТУ НА ОСНОВІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ……..….. **108**
Дорошенко М.В., Шаповаловський А.О. ДИСТАНЦІЙНЕ ВИВЧЕННЯ ДИСЦИПЛІНИ «МЕТОДИ ОБ'ЄКТНО-ОРІЄНТОВАНОГО ПРОГРАМУВАННЯ» НА ОСНОВІ ПЛАТФОРМИ EFRONT ……..... **112**
Здобиляк У.М., Василиків І.Б. ЗАСТОСУВАННЯ PLICKERS НА УРОКАХ МАТЕМАТИКИ В ПОЧАТКОВІЙ ШКОЛІ ……..…. **115**
Кобильник Т.П. СТАТИСТИЧНЕ СЕРЕДОВИЩЕ R ЯК ЗАСІБ НАВЧАННЯ ДИСЦИПЛІНИ «ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ» …… **118**
Когут У.П. ВПРОВАДЖЕННЯ КВЕСТ-ТЕХНОЛОГІЇ В ОСВІТНІЙ ПРОЦЕС **120**
Кутняк О.А. СТВОРЕННЯ МУЛЬТИМЕДІЙНИХ ДИДАКТИЧНИХ МАТЕРІАЛІВ ЗАСОБАМИ LEARNINGAPPS ……... **123**
Мойко О.С. ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В СИСТЕМІ ВИЩОЇ ШКОЛИ ……... **125**
Сікора О.В., Когут У.П., Вдовичин Т.Я. ПРОЕКТУВАННЯ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ СТУДЕНТІВ …… **130**
ВІДОМОСТІ ПРО АВТОРІВ …… **133**

ВДОСКОНАЛЕННЯ ТА МОДЕЛЮВАННЯ МЕТОДУ ГЕНЕРУВАННЯ ПОТОКУ МАТРИЧНИХ ПЕРЕСТАНОВОК ЗНАЧНОЇ РОЗМІРНОСТІ

Красиленко В.Г., Нікітович Д.В.

Вінницький національний технічний університет

krasvg@i.ua

Вступ. Суттєве зростання у інформаційних потоках частки різноманітних текстово-графічних документів (ТГД) з візами, підписами, різноманітного формату кольорових та багато-спектральних зображень (З), таблиць, діаграм, 2D, 3D і вище масивів даних, тощо, сприяло появі нового класу криптосистем матричного типу (МТ) [1-4], що реалізуються на основі алгоритмів і матрично-алгебраїчних моделей (МАМ) криптографічних перетворень (КП) та мають ряд суттєвих переваг, які були продемонстровані у роботах [5-10]. Узагальнені МАМ, матричні афінні та афінно-перестановочні шифри, їх модифікації також досліджувались та використовувались при створенні сліпих та інших цифрових підписів у [11-14], включаючи покращені [15]. Вони краще відображаються на матричні цифрові архітектури при їх апаратних реалізаціях, мають покращені показники крипто-стійкості та гістограмно-ентропійного аналізу, дозволяють перевіряти наявність перекручувань у криптограмах чорно-білих, кольорових зображень, цілісність криптограм [5,7], мають розширені функціональні можливості, що сприяють створенню блокових [6], багатофункціональних параметричних [8] і багатосторінкових [9] моделей, дослідженню їх стійкості [10]. Базовими операціями МАМ є по-елементні множення, додавання за модулем матриць та матричні моделі перестановок (ММ_П) з процедурами множення матриць. Для реалізації КП необхідно матриці байтів зліва та справа множити на матриці перестановок (МП), матрицю з рядків, колонок, векторів, що в унітарних кодах відображають символи, коди, байти, теж замінювати, переставляти за допомогою перестановок. Процедури переставляння бітів, байтів чи їх груп є найбільш поширеними та обов’язковими практично для всіх

відомих та новостворюваних алгоритмів та шифрів. Для змін гістограми, збільшення ентропії криптограми З при їх КП на основі ММ_П необхідні декомпозиція R,G,B складових і їх бітових зрізів та декілька матричних ключів (МК) і векторних (ВК) [3-5]. А для маскування відео-файлів чи потоку блоків необхідна низка псевдовипадкових МК, які повинні відповідати вимогам та швидко генеруватись. Тобто для МАМ є гостра необхідність формування цілої низки МП з головного МК, які б задовольняли ряду вимог. Оскільки в [16,17] розглядались питання узгодження лиш головного МК загального виду, а не низки (потоку) МП, а в [18] розглядались методи генерування потоку матричних ключів перестановок, але тільки для бітових МП розміром 256*256, то метою роботи є спроба вдосконалити метод генерації низки МП, покращити та адаптувати вид, структуру, опис МП до формату З і до швидких апаратних рішень, суттєво розширити межі розмірності МП, промоделювати та дослідити процес формування потоку МП для МАМ КП у системах МТ, перевірити властивості генерованих МП. Виклад основного матеріалу. 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 колосальні значення. Але кожну 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 любу 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 Програмний модуль 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. Таким чином, любу МП можна однозначно представити

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 (З) повторюється рівно по 256 раз.

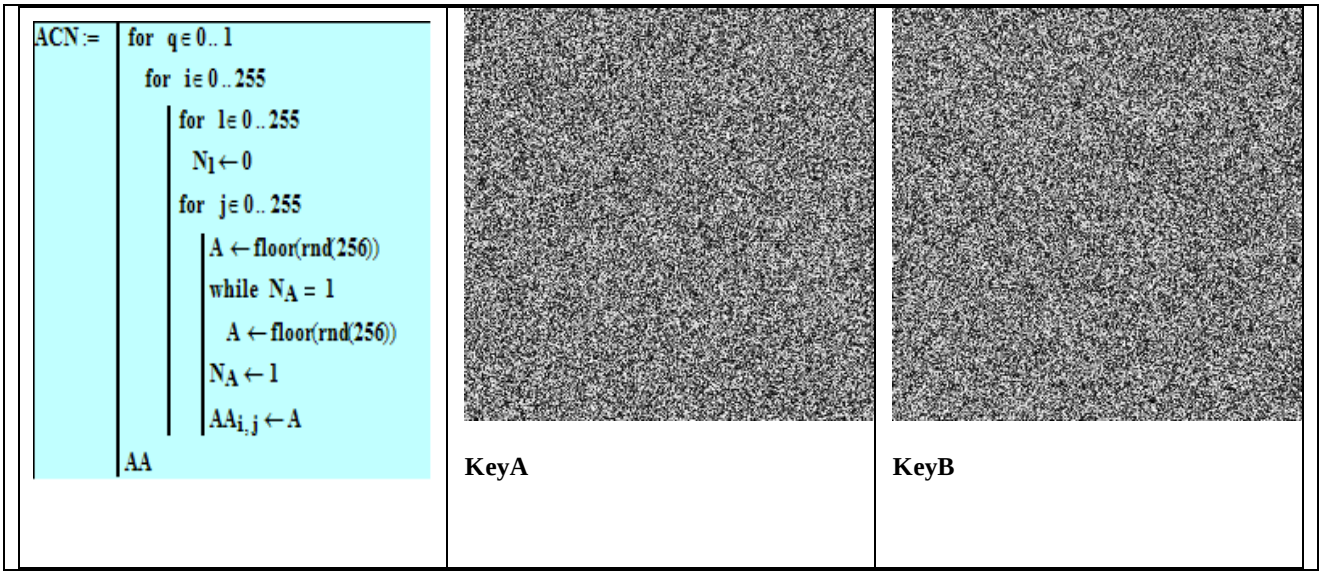


Рис. 1. Програмний модуль для генерування базового (головного) МК (МП) та вигляд складових KeyA та KeyB у форматі двох чорно-білих зображень

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, матричним афінно-перестановним шифром (МАПШ) при використанні МП та тих же наявних її складових KeyA та KeyB.

Результати моделювання КП З (Im) МАПШ за допомогою пропонованої МП у Mathcad з формулами, що відповідають перестановці та афінним КП, та матрицями (З) явного З, його криптограм та перевірними показані на рис.3, 4.

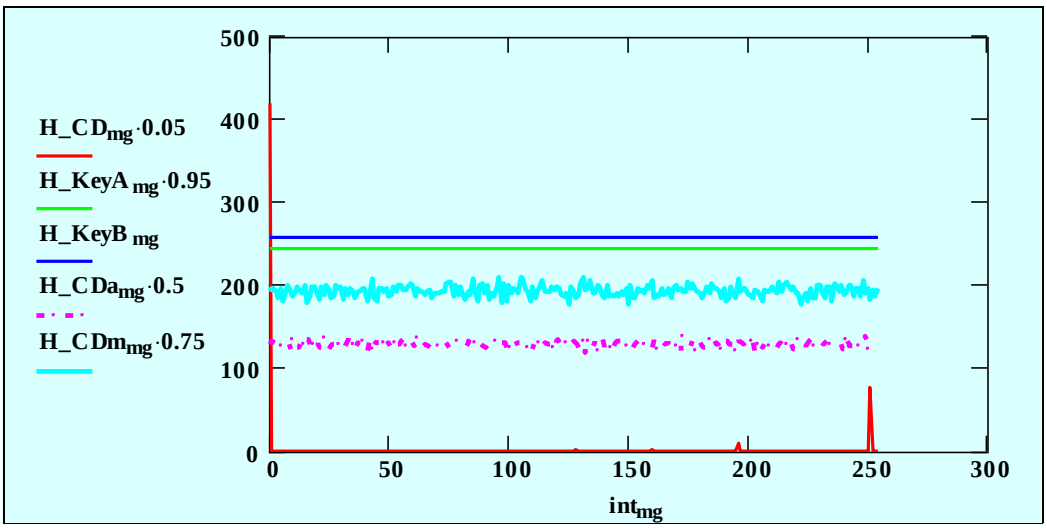


Рис. 2. Гістограми H_KeyA та H_KeyB відповідно складових KeyA та KeyB МП, гістограма H_CD криптограми явного З (співпадає з гістограмою З), відповідні гістограми H_CDa та H_CDm криптограм після адитивної та мультиплікативної афінних КП З за допомогою тих же KeyA та KeyB

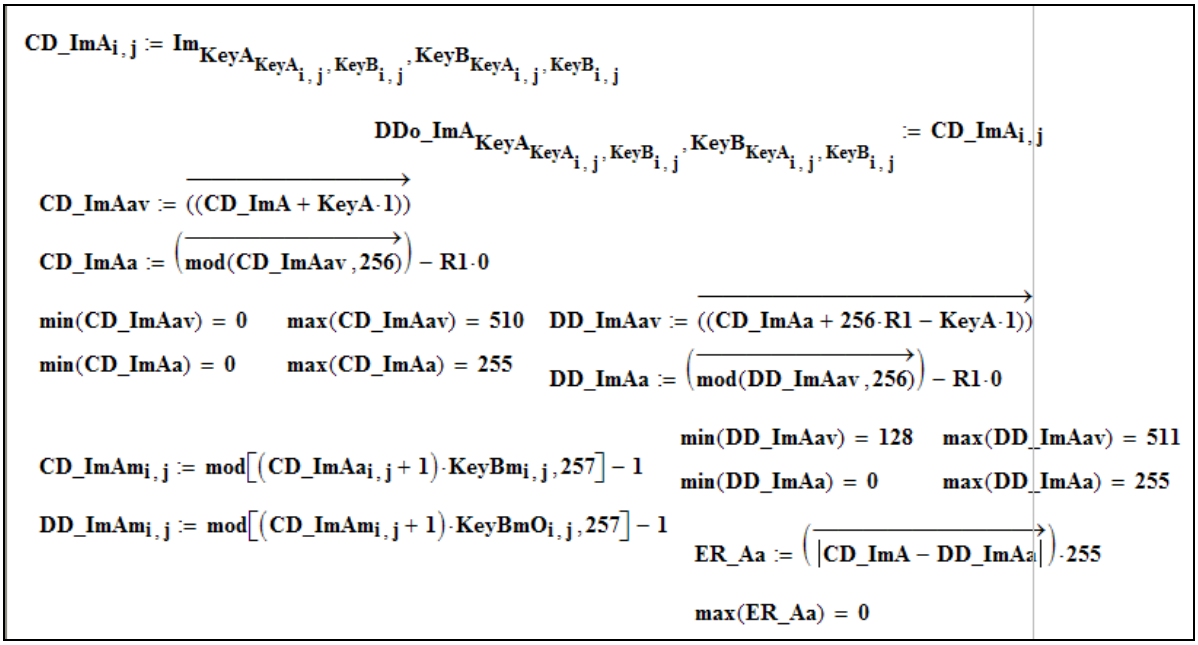


Рис. 3. Фрагмент вікна Mathcad з формулами для моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК

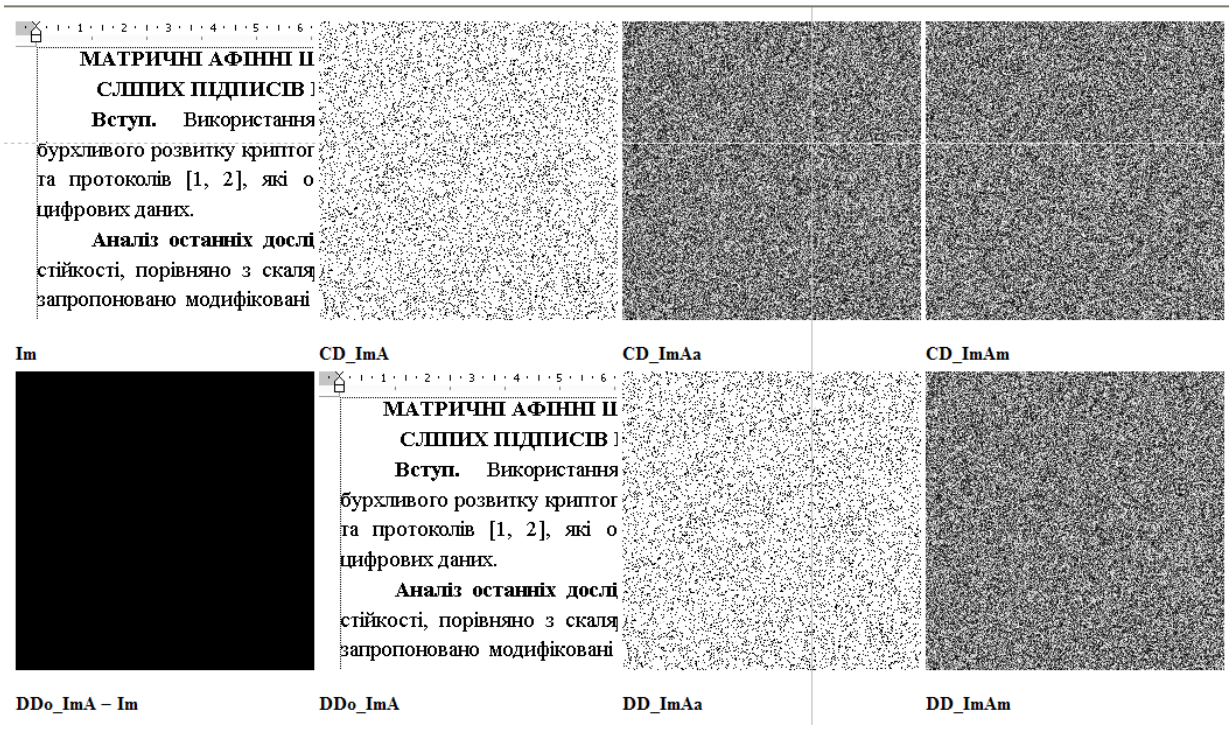


Рис. 4. Результати моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК

Як видно з рис.4 та рис.2, після перестановки байтів зображення Im отримана криптограма CD_ImA не змінює свою гістограму, але після 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. Програмний модуль Mathcad для розрахунку ентропії З та побудови гістограм показано на рис. 5, а на рис.6 – 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. Вони свідчать теж про достовірну якісну роботу шифру при застосуванні пропонованих представлень МП та багатокрокових МАПШ.

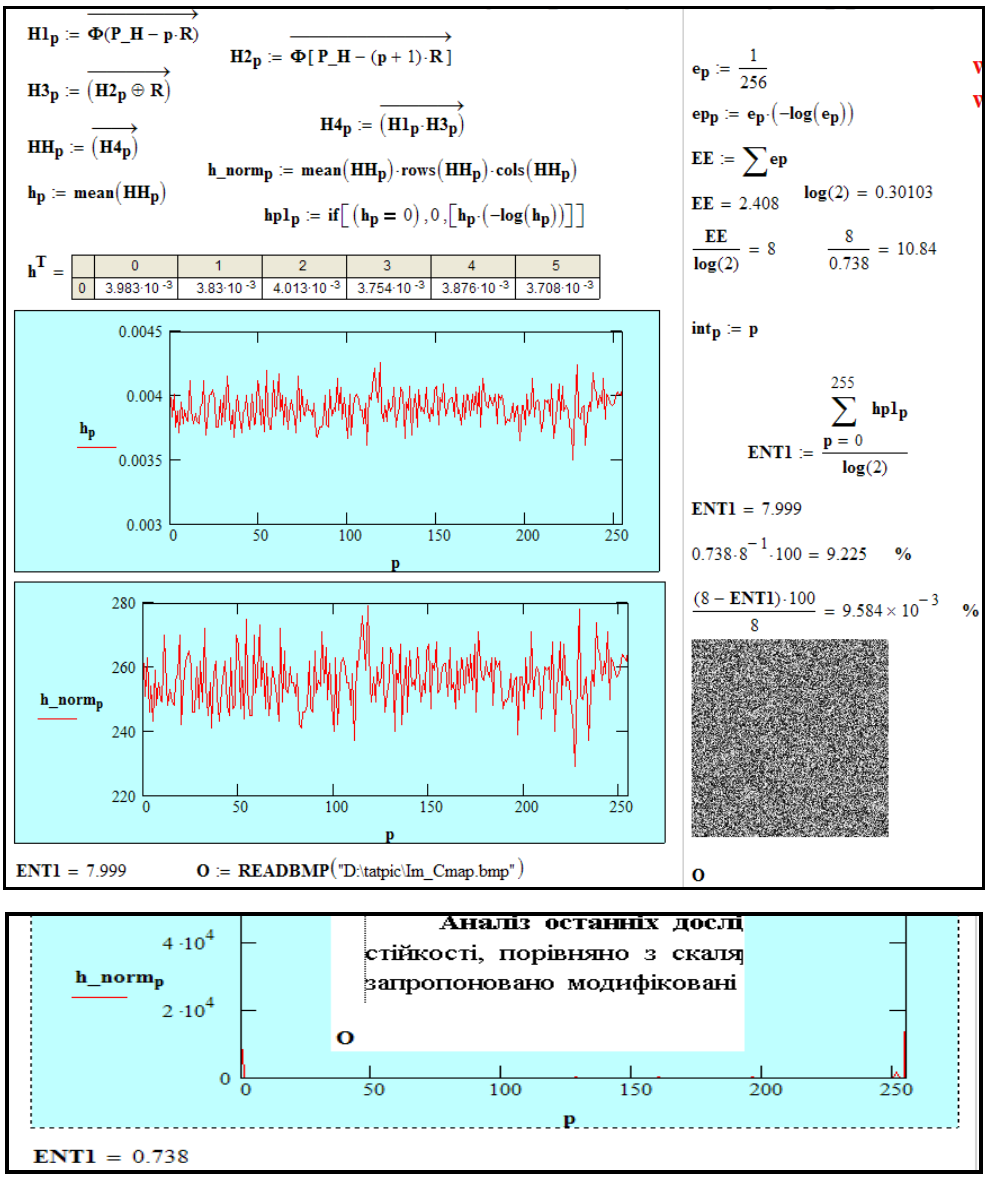


Рис. 5. Програмний модуль Mathcad для розрахунку ентропії З, гістограм

Оскільки для багатокрокових, декількох раундових, циклових КП кожного поточного блоку чи спектральних складових кольорових, багато-спектральних З бажано, з метою збільшення стійкості МАПШ, мати низку неповторюваних МК, генерованих з головного МК, наприклад, з такої ж МП, то, з урахуванням вимог до крипто-статистичних характеристик МК, стає актуальною задача дослідження процесів швидкого надійного генерування послідовності таких МП.

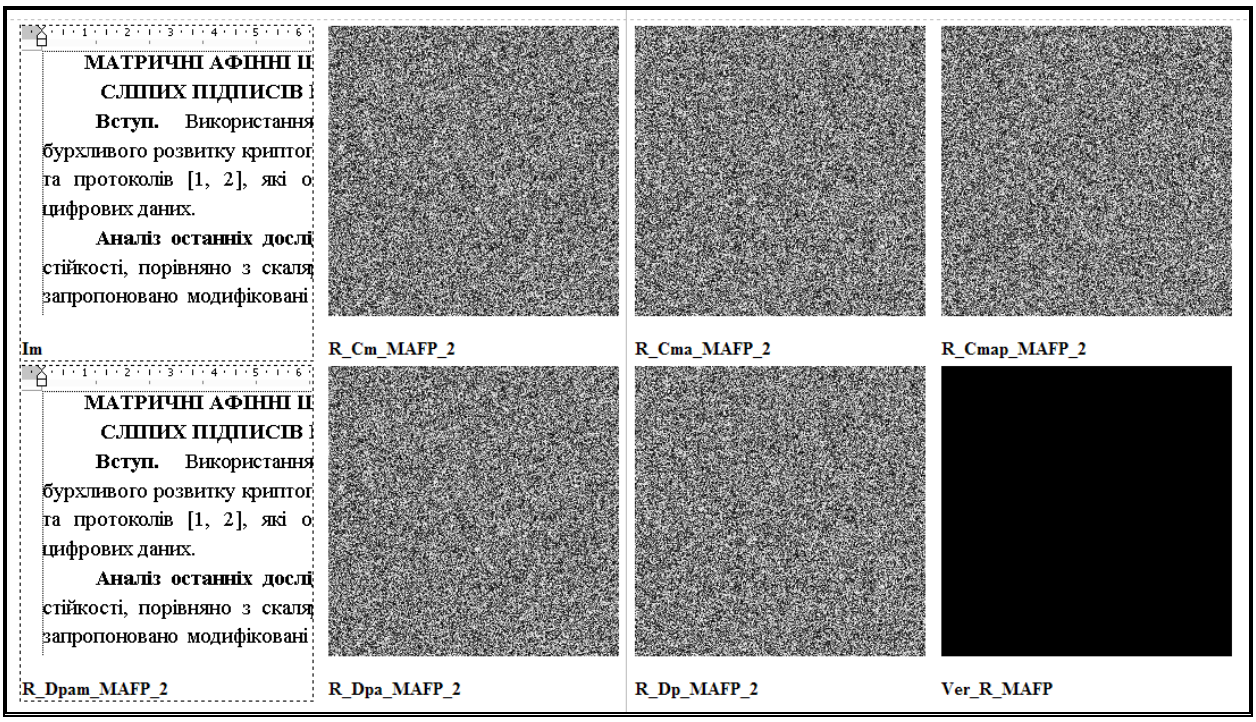


Рис. 6. Результати моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК

Одним з підходів, по аналогії з [18], є використання деяких, узгоджених сторонами скалярів ха та xm (одного чи двох), як ключів для КП (зашифрування) ними складових KeyA та KeyB головної МП (ГМП) за допомогою афінного шифру з операціями за модулем 257. Утворені з них криптограми, їх пара, будуть складовими нової МП, повністю будуть зберігати всі необхідні властивості ГМП, мати аналогічні гістограми та відповідати вимогам. При відкиданні значень «0» та «1» для ха та xm оцінки показують, що число різних таких пар скалярів може бути 254*254, а кількість можливих переставлять цих пар у їх послідовній множині оцінюється величиною (254*254)!, що є досить значною, тобто можна створювати низки МК (МП) значної розмірності. Для практичних застосувань навіть одного мультиплікативного афінного (лінійного) КП достатньо, щоб з множини 256-ти значень xm створювати, крім того, й без повторів, значну кількість випадкових векторів довжиною 256, а саме 256!, для формування цим узгодженим вектором послідовності необхідних МП у вигляді двох його складових виду 3, тобто блоків байтів. Результати моделювання

процесів генерування МК KeyM, як першої складової нової МП, з KeyA складової МП для такої ситуації у Mathcad з формулами та матрицями KeyM для xm = km=17 показані на рис.7. Генерування другої складової виконується з тим же km=17, але від KeyB.

$$\mathbf{KeyM}(\mathbf{km},\mathbf{KeyA}) := \left| \begin{array}{l} \textbf{for}\ \ i \in 0..255 \\ \quad \textbf{for}\ \ j \in 0..255 \\ \quad\quad W_{i,j} \leftarrow \mathbf{mod}\left[\left(\mathbf{KeyA}_{i,j}+1\right)\cdot \mathbf{km}, 257\right]-1 \\ W \end{array} \right.$$

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) =

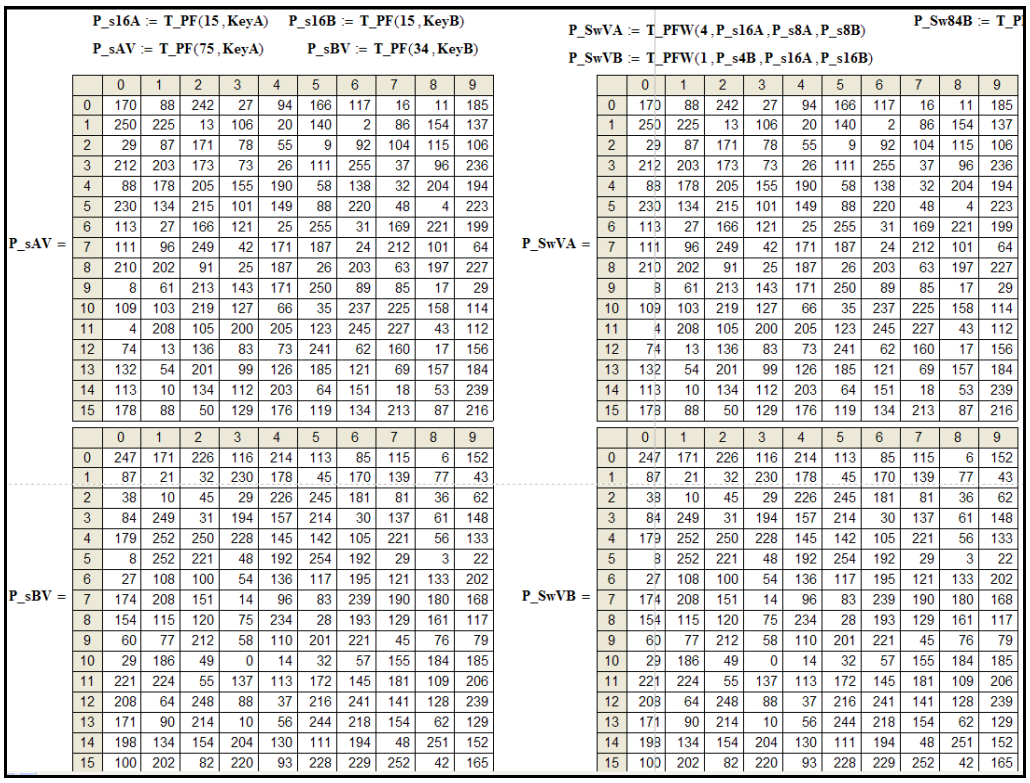
	0	1	2	3	4	5	6	7	8	9
0	201	128	218	79	195	71	175	159	86	115
1	6	170	118	190	169	16	246	216	48	46
2	26	205	35	29	173	141	90	34	240	183
3	10	69	46	150	45	28	48	172	191	43
4	73	65	139	94	230	105	84	59	87	162
5	124	19	204	43	5	220	142	78	57	45
6	21	96	223	232	31	233	158	91	41	40
7	223	22	66	90	129	151	118	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. 7. Формули та вигляд (2D) генерованого МК з ГМП простим лінійним КП та функціональним параметричним

Гістограми всіх цих векторів з елементами, що не повторюються, також є горизонтальними лініями, як і обох складових всіх генерованих за їх допомогою перестановок, що відображаються у вигляді і-тих криптограм складових KeyA та

KeyB ГМП та утворюються за допомогою афінного шифру, пари і-их компонентів векторів (адитивна і мультиплікативна складові) чи лише однієї і-тої компоненти з них. Пари цих криптограм і є і-ими поточними матричними перестановками, що однозначно відображаються і у вигляді двох матриць розмірністю (256*256). Оскільки гістограми складових МП та випадкових векторів є горизонтальними лініями, а їх ентропія рівна 8 біт, то крипто-аналіз на їх основі унеможливлюється. Крім того, ГМП, 2 (1) узгоджені допоміжні векторні ключі є секретними, що дозволяє лише сторонам процесу КП створювати чи мати цю низку МК (МП). В принципі, секретною може бути лише ГМП, або узгодженими лише вищезгадані векторні ключі.

Другим способом генерування поточних (на і-тому кроці) МП є однакові циклічні зсуви складових ГМП по х та у координатах на відповідні вибрані (узгоджені сторонами) значення з діапазону 1-254. З урахуванням обмежень, тут моделювання цього способу 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. Отже, третій спосіб 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 способом потоку МП при його моделюванні у Mathcad показані на рис.8, 9 та підтверджують його адекватність, коректність, відповідність вимогам та досягнення суттєвих переваг за рахунок як значних прискорень обчислення степенів ГМП, так і простоти можливих реалізацій і зменшення затрат на відображення ГМП.



P_s16A := T_PF(15, KeyA) P_s16B := T_PF(15, KeyB)

P_sAV := T_PF(75, KeyA) P_sBV := T_PF(34, KeyB)

P_SwVA := T_PFW(4, P_s16A, P_s8A, P_s8B) P_Sw84B := T_P

P_SwVB := T_PFW(1, P_s4B, P_s16A, P_s16B)

P_sAV =

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

P_SwVA =

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

P_sBV =

	0	1	2	3	4	5	6	7	8	9
0	247	171	226	116	214	113	85	115	6	152
1	87	21	32	230	178	45	170	139	77	43
2	38	10	45	29	226	245	181	81	36	62
3	84	249	31	194	157	214	30	137	61	148
4	179	252	250	228	145	142	105	221	56	133
5	8	252	221	48	192	254	192	29	3	22
6	27	108	100	54	136	117	195	121	133	202
7	174	208	151	14	96	83	239	190	180	168
8	154	115	120	75	234	28	193	129	161	117
9	60	77	212	58	110	201	221	45	76	79
10	29	186	49	0	14	32	57	155	184	185
11	221	224	55	137	113	172	145	181	109	206
12	208	64	248	88	37	216	241	141	128	239
13	171	90	214	10	56	244	218	154	62	129
14	198	134	154	204	130	111	194	48	251	152
15	100	202	82	220	93	228	229	252	42	165

P_SwVB =

	0	1	2	3	4	5	6	7	8	9
0	247	171	226	116	214	113	85	115	6	152
1	87	21	32	230	178	45	170	139	77	43
2	38	10	45	29	226	245	181	81	36	62
3	84	249	31	194	157	214	30	137	61	148
4	179	252	250	228	145	142	105	221	56	133
5	8	252	221	48	192	254	192	29	3	22
6	27	108	100	54	136	117	195	121	133	202
7	174	208	151	14	96	83	239	190	180	168
8	154	115	120	75	234	28	193	129	161	117
9	60	77	212	58	110	201	221	45	76	79
10	29	186	49	0	14	32	57	155	184	185
11	221	224	55	137	113	172	145	181	109	206
12	208	64	248	88	37	216	241	141	128	239
13	171	90	214	10	56	244	218	154	62	129
14	198	134	154	204	130	111	194	48	251	152
15	100	202	82	220	93	228	229	252	42	165

Рис. 8. Формули та частина цифрових масивів генерованого МК з ГМП шляхом ітераційних чи послідовних фіксованих перестановок

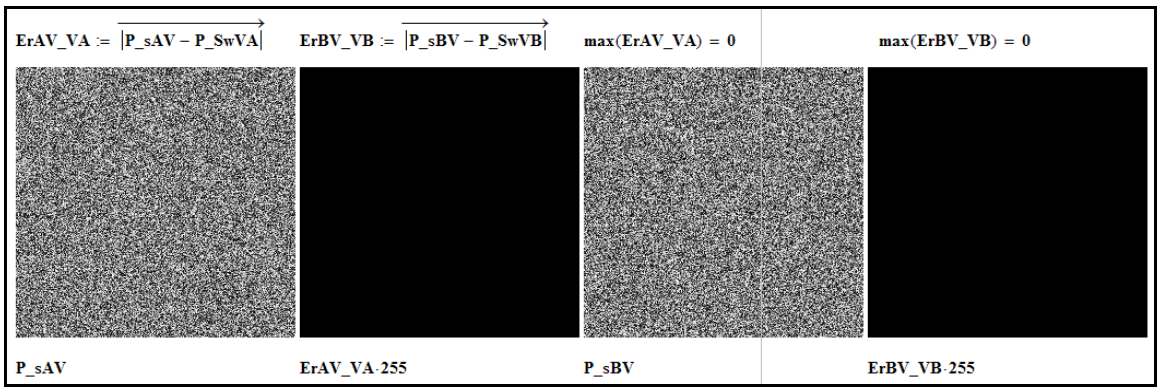


Рис. 9. Формули для перевірки (порівняння) та вигляд генерованих МК з ГМП

Використовуючи показані на рис.10 функціональні параметричні моделі КП на основі генерованих МП, 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 КП: криптограми, відновлені З, явні та різницеві показані на рис.11.

Висновок. Вдосконалений і промодельований метод генерації низки МП значної розмірності, розглянуто 3 його модифікації. Результати експериментів, оцінки стійкості підтвердили якість МП, адекватність функціонування моделей та пропонованих методів генерування МП, їх переваги та перспективність.

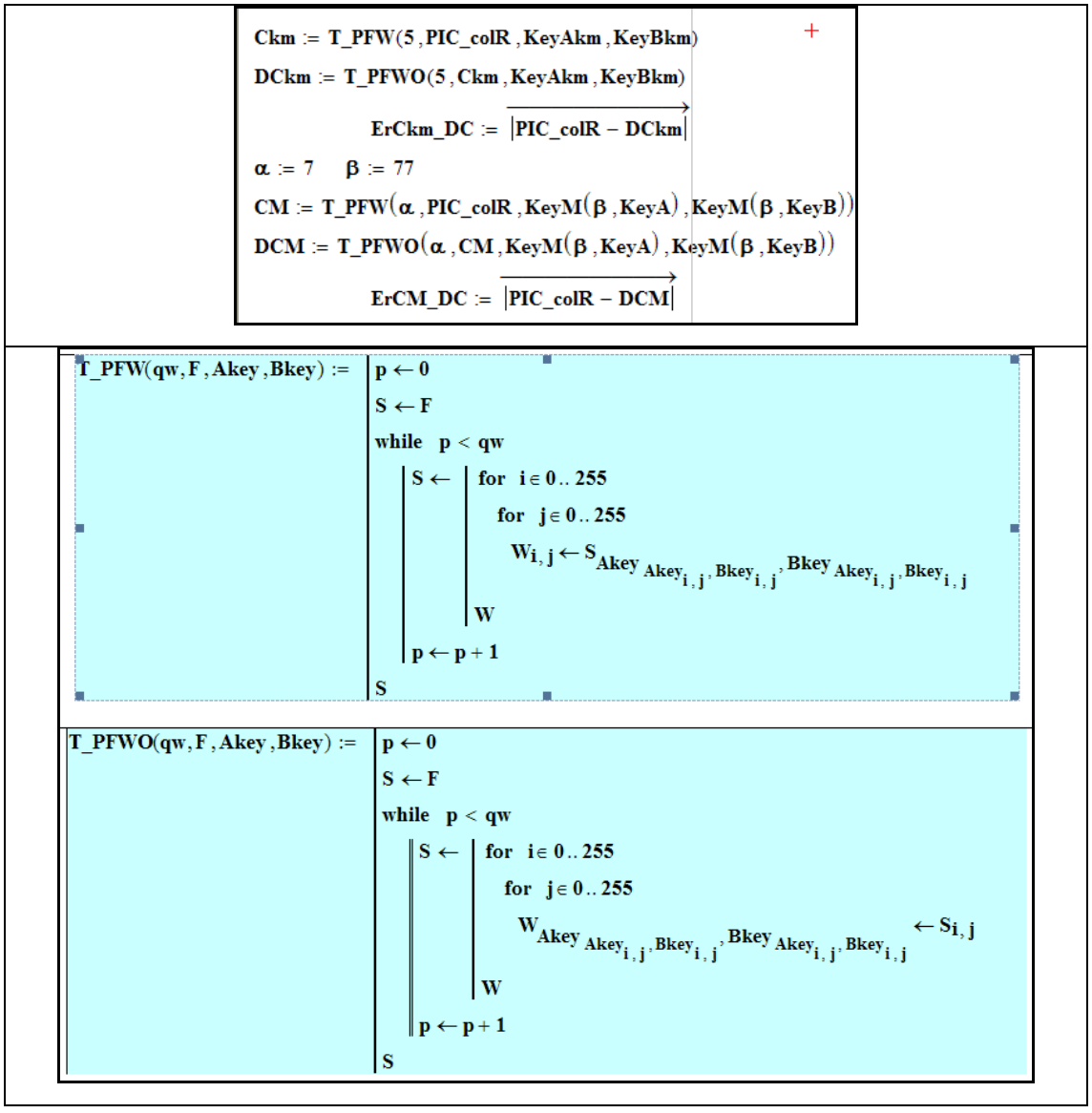


Рис. 10. Функціональні параметричні моделі КП на основі генерованих МП

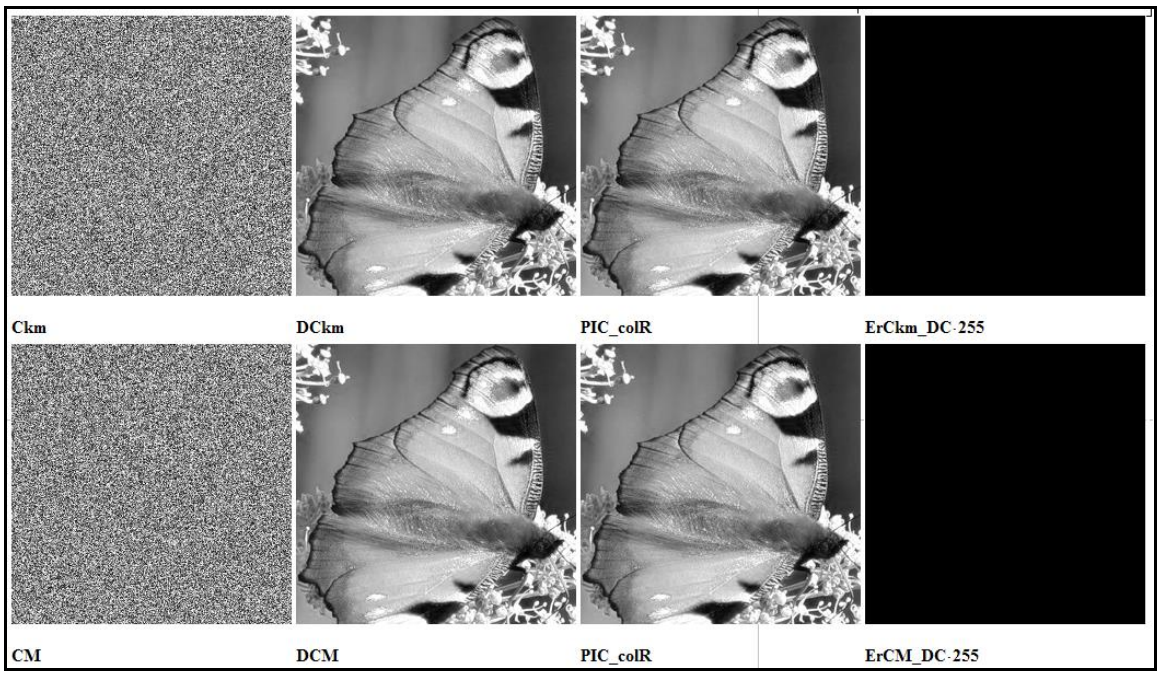


Рис. 11. Пряме та зворотне КП 3 на основі генерованих МП

Список використаних 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-бітовозрізовою 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-зрізовою 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-бітовозрізової 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 (МАМ) 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 IX 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 III 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. Тріфонова, // 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 текстографічних 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.

DEVELOPMENT AND SIMULATION ARRAY OF DEVICES BASED ON THE FPGA FOR PARALLEL CALCULATION OF NORMALIZED EQUIVALENCES OF THE REFERENCE FILTERS WITH THE CURRENT PROCESSED FRAGMENT OF THE IMAGE

Krasilenko V.G., Lazarev A.A., Nikitovich D.V.
Vinnytsia National Technical University;
krasvg@i.ua

Introduction, purpose and objectives of the work. The basis of most known methods, algorithms and means, including models of neural networks (NNs), for the recognition and clustering of images in the biometric, machine vision systems is to compare two different images of the same object or its fragments [1, 2]. Discriminant measure of compared reference and current fragments is often a mutual two-