ISSN 2224-087X. Електроніка та інформаційні технології. 2017. Випуск 7. С. 20–42
Electronics and information technologies. 2017. Issue 7. P. 20–42

УДК 004.056.55:004.032

УДОСКОНАЛЕННЯ ТА МОДЕЛЮВАННЯ МАТРИЧНИХ АФІННИХ ШИФРІВ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ЗОБРАЖЕНЬ

В. Красиленко, Д. Нікітович

Науково-дослідний відділ,
Вінницький соціально-економічний інститут університету "Україна",
вул. Келецька, 86/131, м. Вінниця, 21021, Україна
krasilenko@mail.ru

Наведено результати моделювання матричних афінних удосконалених шифрів для криптографічних перетворень чорно-білих та кольорових зображень зі зменшеною кількістю матричних ключів. Розроблено модифіковані моделі та алгоритмічні процедури процесів формування ключів, прямого та оберненого криптографічних перетворень, що зводяться до матрично-матричних поелементних операцій за модулем. Використання декомпозиції кольорових і багатоспектральних зображень на чорно-білі складові дало змогу уніфікувати процедури перетворень, використовувати лише один узгоджений матричний ключ та розширити види, формати даних і спектр застосувань шифрів. Як допоміжні похідні ключі використано степені головного ключа за модулем. На підставі низки експериментів у середовищі Mathcad з різними багатоградаційними та кольоровими зображеннями для їхнього шифрування та розшифрування за допомогою описаних моделей з'ясовано, що запропоновані удосконалення таких шифрів є адекватними, зручними для використання, мають переваги та дають змогу навіть збільшити їхні функціональні можливості.

Ключові слова: криптографічні перетворення зображень, матричний афінний шифр, матричні моделі, декомпозиція, криптограма, узгоджений ключ, матричні ключі, поелементна степінь за модулем матриці, матрично-матрична процедура.

Необхідність вирішення теоретичних і практичних завдань інформаційної безпеки та досягнення необхідного рівня захисту інформації державного, військового, комерційного та приватного змісту зумовила в епоху інформаційних технологій, комп'ютерних засобів, мереж та масових комунікацій і відповідний прискорений розвиток криптографії, споріднених та пов'язаних з нею нових наукових дисциплін. В епоху електронних комунікацій суттєво зросла потреба опрацьовувати та передавати специфічні текстово-графічні документи (ТГД) у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій тощо, які є, по суті, 2D масивами (зображеннями) значної розмірності. Крім того, збільшується частка нових задач, у яких необхідно виконувати криптографічні перетворення над багатовимірними сигналами, серед яких важливе місце посідають різноманітні напівтонові, кольорові багатоспектральні зображення, 2D, 3D та навіть 4D масиви [1–8]. У розпізнавально-ідентифікаційних, біометричних, навігаційно-моніторингових системах, робототехніці, інтелектуальному управлінні, у разі ухвалення рішень потрібно обробляти та передавати в зашифрованому вигляді велику

кількість різноманітних зображень, наприклад, відбитки пальців, фотографії осіб, зображення рухомих об'єктів, райдужної сітківки ока тощо. Розширення спектрального діапазону, що його сприймають сучасні багатосенсорні системи дистанційного зондування та моніторингу, зумовило необхідність оброблення значних масивів великорозмірних багато-спектральних зображень. Оскільки ця інформація часто конфіденційна, то є гостра потреба в її криптографічних перетвореннях для захисту від несанкціонованого доступу. Багато ТГД містять інформацію з обмеженим чи закритим доступом, яку треба надавати як звітність у податкові та інші державні органи, своєчасно та у зашифрованому вигляді передавати каналами зв'язку, забезпечуючи лише санкціонований доступ, засвідчувати їх цифровими підписами. Санкціонований доступ до багатьох інформаційних ресурсів, наприклад, бібліотечних, архівних та книжкових фондів, фондів наукових публікацій, патентних документів, що формуються в процесі діяльності суб'єктів інформаційної діяльності, можна забезпечити відповідними технологіями криптографії та заходами з видачею дозволів, сертифікатів і ключів доступу.

Для таких цілей захисту інформації використовують методи та засоби криптографічних перетворень (КП) інформаційних масивів чи зображень [1–10] та процедури і протоколи формування ключів і їхнього обміну [1, 11, 12], проте серед їхнього великого різноманіття [1-10] більшість з них орієнтована на послідовне скалярне оброблення блоків ТГД, перетворених у цифрові формати, і лише незначна частина присвячена методам та алгоритмам, орієнтованим на матричні моделі [14–22] та матричні спеціалізовані алгоритми і засоби. Водночас поява паралельних алгоритмів, а особливо матричних багатопроцесорних засобів, матричних лінійно-алгебричних, спеціалізованих багатоядерних, паралельних та матричного (картинного типу) процесорів [3, 9] сприяла переорієнтації під час дослідження КП зображень на ці нові засоби та створенню відповідних моделей матричного типу (МТ) [14–17]. Крім того, актуальність проблеми створення нових високоефективних моделей, алгоритмів, протоколів для оброблення та криптографічних перетворень зображень підтверджена і суттєвим зростанням за декілька останніх років частки праць, що присвячені шифруванню та розшифруванню зображень [4–8, 15, 17–25]. А тому пошук і дослідження нових матричних моделей (ММ) КП, удосконалення наявних матричних шифрів та засобів для їхньої реалізації є актуальним стратегічним завданням.

Результати моделювання процесів криптографічних перетворень зображень на основі запропонованих В. Красиленком та досліджених матричних алгоритмів і моделей криптографічного захисту засвідчують їхні переваги. Наприклад, у працях [10, 13] розглянуто матричні алгоритми та реалізацію мовою Delphi програми CryptoFax. Доведено, що розроблені методи перестановок є стійкими до впливу завад і різних спотворень. Недолік програми CryptoFax полягав у тому, що в разі перетворень залишалася незмінною гістограма перетворених зашифрованих зображень. Тому для усунення цього недоліку та поліпшення стійкості алгоритмів криптографічних перетворень зображень запропоновані узагальнення афінних шифрів та розширення їх на матричний випадок [17] і були експериментами в середовищі MathCad частково продемонстровані можливості й переваги для практичних застосувань матричних алгоритмів криптографічного захисту на основі більш узагальнених матричних афінних шифрів (МАШ). У працях [15, 16] запропоновано модифіковані та більш узагальнені матричні алгоритми криптографічних перетворень зображень і так звані матричні афінно-перестановочні алгоритми (МАПА) [18], що грунтуються на модифікації відомих афінних шифрів. Результати моделювання

[14–17] процесів криптографічних перетворень багатоградаційних та кольорових зображень [22] на основі таких моделей та алгоритмів засвідчили їхні суттєві переваги порівняно з традиційними скалярними афінними асиметричними шифрами, а саме: більша стійкість, збільшення швидкодії, можливість паралельно виконувати обчислювальні процедури та процеси й реалізовувати їх за допомогою паралельних проблемно-спеціалізованих засобів, матричних процесорів. У праці [16] на основі МАШ запропоновано алгоритм та процедуру створення цифрового сліпого підпису (ЦСП) на ТГД та наведено результати моделювання реально розробленої і практично перевіреної програми для формування та верифікації такого ЦСП. Такі матричні криптографічні моделі, алгоритми і криптографічні системи на їхній основі ліпше та ефективніше відображаються на повністю паралельні матричні обчислювальні засоби, оскільки описуються суто математичними матричними моделями, а це суттєво підвищує продуктивність оброблення в разі перетворень та зменшує час їхнього виконання.

Відомі також результати моделювання алгоритмів створення 2D ключа [11, 12], суть яких полягає в узагальненні відомих протоколів створення та генерування ключів на матричний випадок і формуванні та описі цих протоколів за допомогою матричних моделей. Створенню ЦСП на ТГД, однак на основі інших моделей матричного типу присвячена праця [14]. Однією з основних складових найбільш узагальнених матричних афінно-перестановочних шифрів чи МАПА, що запропоновані та досліджені в [18], є матричні моделі перестановок (ММ_П), які мають наочну простоту. Подальше застосування та вдосконалення шифрів матричного типу на основі таких ММ_П висвітлене в працях [19–21, 23, 24]. Проте, як наголошено в [20, 21], КП на їхній основі без додаткових операцій не змінюють гістограми зображень чи ТГД, а запропоновані в них модифіковані ММ_П з декомпозицією бітових зрізів усувають цей недолік, хоч і потребують у деяких випадках, крім двох матричних ключів (МК), ще й двох векторних ключів (ВК). Водночас у більшості згаданих вище праць є спільний суттєвий недолік, особливо праць, що стосуються МАШ [17, 22], МАПА [18] та подібних [14–16, 21, 23–25], який полягає потребі застосування мінімум двох МК, якщо реалізувати в моделях МАШ, МАПА, МТ і мультиплікативну й адитивну матричні складові. Проте МК, які застосовують, є двох типів: у вигляді випадкових зображень (головно, чорно-білих 8-бітних) для МАШ та квадратних матриць перестановок для реалізації ММ_П й алгоритмів на них [19–21]. Перший тип менше досліджений. Тому пошук способів удосконалення МАШ та особливо багатокрокових МАШ, МАПА [18] для зменшення кількості МК аж до одного зі збереженням стійкості та інших характеристик матричних моделей (ММ), їхня експериментальна перевірка на різних зображеннях є необхідним актуальним завданням і обґрунтовано наведеним вище оглядом публікацій.

Формулювання задачі. Необхідною й актуальною сьогодні є спроба подальшої модифікації та вдосконалення відомих МАШ зі спектральною декомпозицією для КП кольорових зображень з метою їхнього спрощення, поліпшення, дослідження моделей, що реалізують МАШ у різних середовищах, для виявлення специфічних особливостей конкретних застосувань та зі збереженням чи навіть розширенням їхніх функціональних можливостей. Перевірка створених моделей моделюванням, проведенням експериментів з реальними зображеннями різних форматів та розмірності дасть змогу оцінити їхню адекватність, характеристики, показники й особливості.

Тому наша мета – дослідження та моделювання в програмному середовищі Mathcad таких модифікацій та удосконалень МАШ з метою використання для КП як чорно-білих,

так і кольорових зображень, включаючи великорозмірні та багатоспектральні, у яких кількість необхідних матричних ключів для цих перетворень була б зменшена до одного, так званого головного, чи базового, зі збереженням тих самих функціональних можливостей. Одним з підзавдань є експериментальна перевірка правильності та якості роботи таких МАШ з різними типами та форматами, розмірами зображень для вивчення їхніх впливів на показники, характеристики шифрів, моделей та алгоритмів їхньої реалізації.

Опишемо деякі найпростіші теоретичні основи МАШ. Процеси зашифрування та розшифрування на основі МАШ для повідомлення у вигляді довільного різновиду й розміру матриці **M** та для створеної криптографічними перетвореннями відповідної криптограми **C** описують ММ, які виражають такими матричними формулами [17]:

$$\mathbf{C} = \left(\mathbf{M} \underset{N}{\otimes} \mathbf{A} \underset{N}{+} \mathbf{S} \right); \quad \mathbf{M} = (\mathbf{C} \underset{N}{\otimes} \mathbf{AD} \underset{N}{+} \mathbf{SD}),$$

де **A** та **S** – два ключі (мультиплікативна й адитивна складові) шифрування у вигляді матриць; **AD** та **SD** – ключі дешифрування, причому **AD** – мультиплікативна складова афінного шифру, **SD** – адитивна складова; **N** – матриця, усі елементи якої дорівнюють числу n (просте велике число), а компоненти всіх матриць вибрані з діапазону $1 – (n – 1)$, крім того, символами $\underset{N}{\otimes}$ та $\underset{N}{+}$ позначені, відповідно, поелементні множення та додавання матриць за модулем N.

Розглянемо сутність алгоритмів та МАШ на основі ММ зі спектральною декомпозицією. Модифікація ММ МАШ, яку ми пропонуємо, полягає у використанні, по суті, одного матричного ключа (МК) для відповідних мультиплікативного й адитивного прямого та оберненого перетворень, що є складовими одно- чи багатокрокових МАШ та реалізують криптографічні процедури для чорно-білого чи всіх спектральних складових кольорового зображень. Ідея полягає в тому, що до секретного МК, який вибирають чи генерують відомими способами у вигляді псевдовипадкового з відповідними до нього вимогами чорно-білого багатоградаційного зображення з розмірами, які дорівнюють розмірам вхідних зображень, завжди існує в разі виконання деяких простих додаткових умов обернений матричний ключ, який позначимо як МКо, а його елементи є оберненими за відповідним модулем до елементів МК.

Ця ідея та її пояснення запропоновані В. Красиленком та висвітлені в наших попередніх працях [17, 18], тому тут зазначимо лише, що в разі використання як модуля числа 257, що є простим, увесь діапазон 0–255 градацій 8-бітного зображення у випадку його зміщення в діапазон 1–256 матиме однозначні обернені значення з цього ж діапазону 1–256, а отже, у разі їхнього зворотного зміщення і в діапазоні 0–255, тобто матиме аналогічне 8-бітне зображення. Перш ніж перейти до деяких нових пропозицій та удосконалень, розглянемо результати моделювання найпростішого МАШ лише з однією мультиплікативною складовою, що є узагальненням скалярного лінійного шифру на матричний випадок. У першому з низки модельних експериментів з МАШ, які проводили в програмному середовищі Mathcad, ми відтворили прямий та обернений криптографічні процеси над двома різними зображеннями (З) (256*256 ел.) з використанням як МК Key_GC та пов’язаного з ним оберненого МКо Key_GD. Результати експерименту показані на рис. 1 та свідчать про правильну адекватну роботу моделей. Використані для перетворень формули відображені на рис. 1 спеціально в скалярному вигляді, а ті, які ви-

користовували для верифікацій, – у матричному. Ліворуч у першому–другому рядах – криптограми, у центрі – розшифровані, вони ж початкові, праворуч – різницеві (нульові).

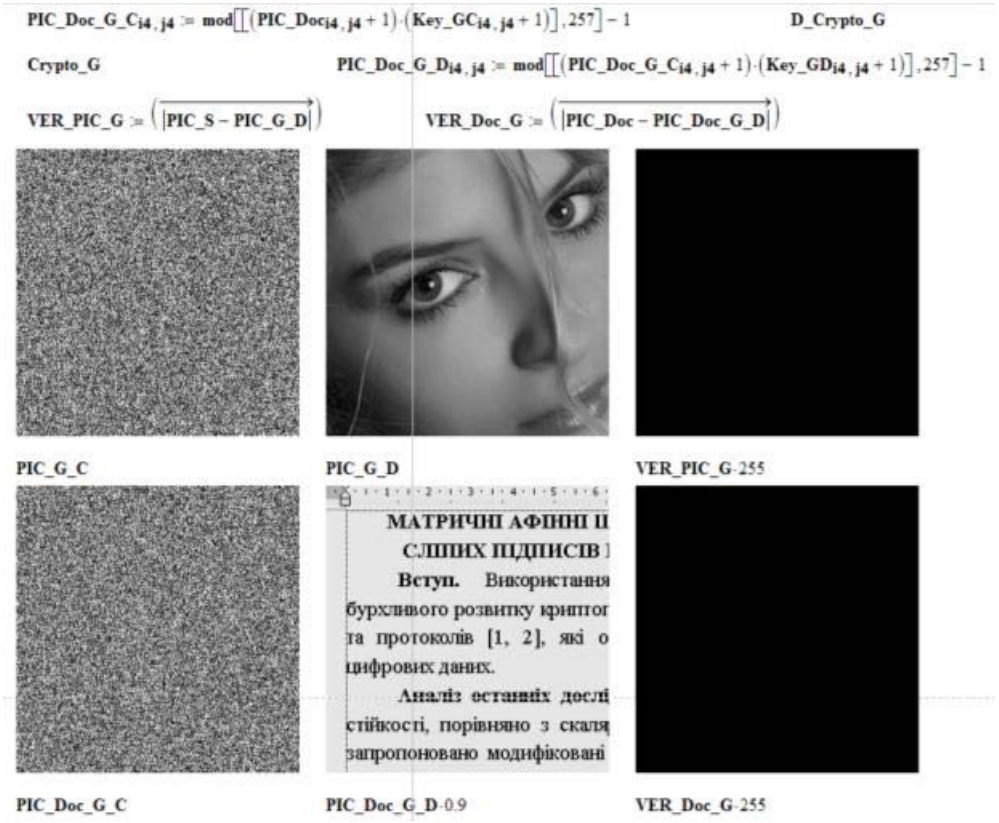


Рис. 1. Результати моделювання процесів прямого й оберненого криптографічних перетворень двох зображень матричним афінним шифром: використані формули для мультиплікативної складової КП МАШ, криптограма першого, розшифроване та різницеве між першим явним та розшифрованим зліва направо у верхньому ряду й відповідні криптограма другого, розшифроване друге та різницеве для нього у нижньому ряду.

Друга наша ідея полягає в тому, щоб для реалізації другого кроку, а саме – адитивної складової, прямого перетворення МАШ використати МКо, бо застосування МК є примітивним. А оскільки, по суті, і МК, і МКо є секретними та взаємно пов'язаними, то це призводить до необхідності двом сторонам процесу створення та передавання зашифрованих даних узгоджувати чи протокольно формувати лише один МК. Водночас не бажано в разі застосування МАШ для криптоперетворень кольорових зображень використовувати один і той самий МК.

Застосуємо другу ідею та перевіримо її на прикладі зашифрування й розшифрування кольорового зображення в разі використання для кожної його R,G,B складової свого МК, тобто трьох випадкових R,G,B складових, що еквівалентно одному МК у кольоро-

вому форматі. На рис. 2 показано одне з вікон з формулами, що використані для генерування ключів, прямих та обернених до них за модулем 257, зашифрування та розшифрування кожної R,G,B_pic складової 3 (600*549 ел.) трьома МК Key_C_(R,G,B) та Key_D_(R,G,B), відповідно.

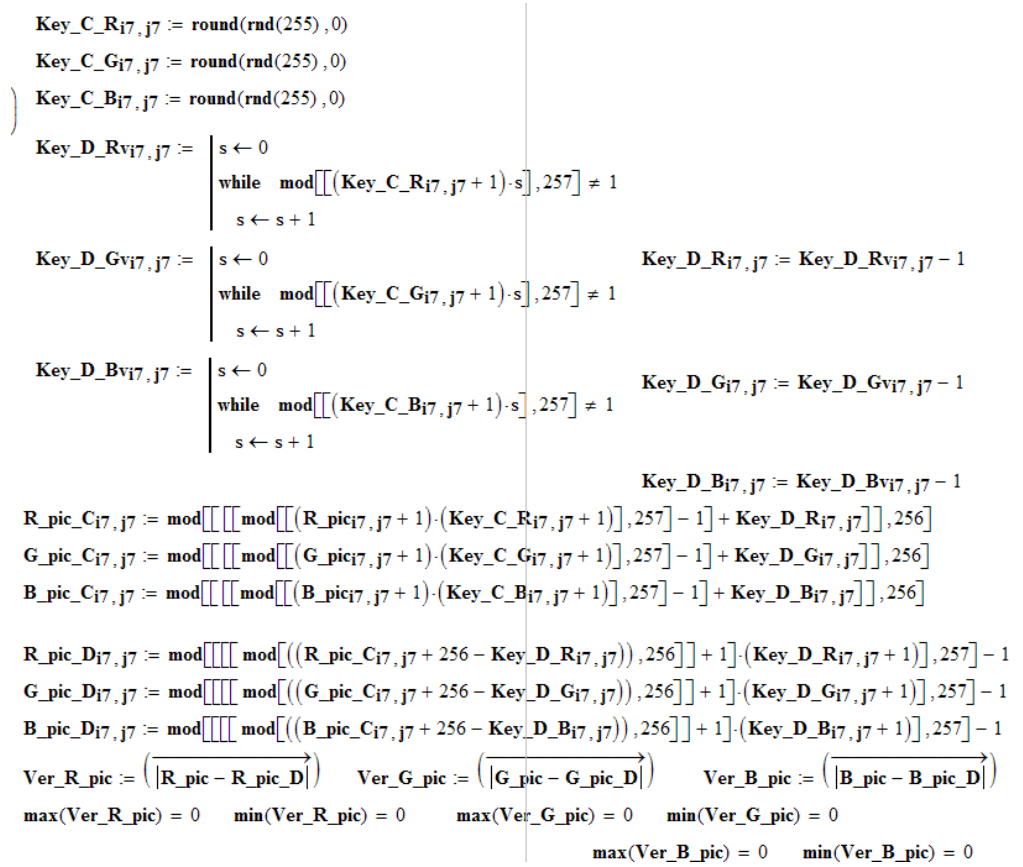


Рис. 2. Вікно Mathcad з формулами для КП кольорового зображення МАШ у разі використання для кожної спектральної складової свого, проте лише одного МК, яким виконується мультиплікативне пряме перетворення, а оберненим до нього МКо – обернене мультиплікативне та пряме й обернене адитивні перетворення.

На рис. 3 показано результати КП на основі МАШ лише з одним МК для кожної складової: кольорові вихідне зображення, МК (перший ряд, праворуч), криптограма (другий ряд, ліворуч) та розшифроване зображення. Вони свідчать про правильну роботу моделей для такої модифікації МАШ.

Зазначимо, що КП складових виконуються по-елементними матричними процедурами множення та додавання, відповідно, за модулями 257 та 256 з використанням практично одного відповідного МК, бо обернений МКо до прямого за модулем є, по суті, адитивною складовою МАШ.

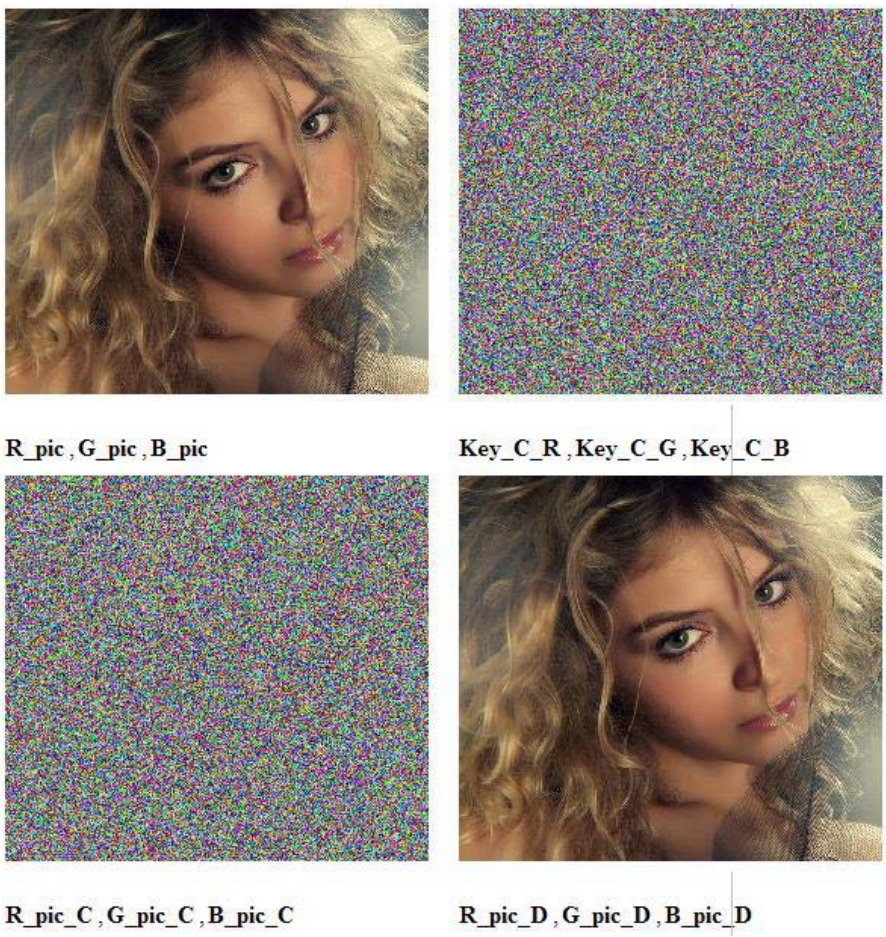
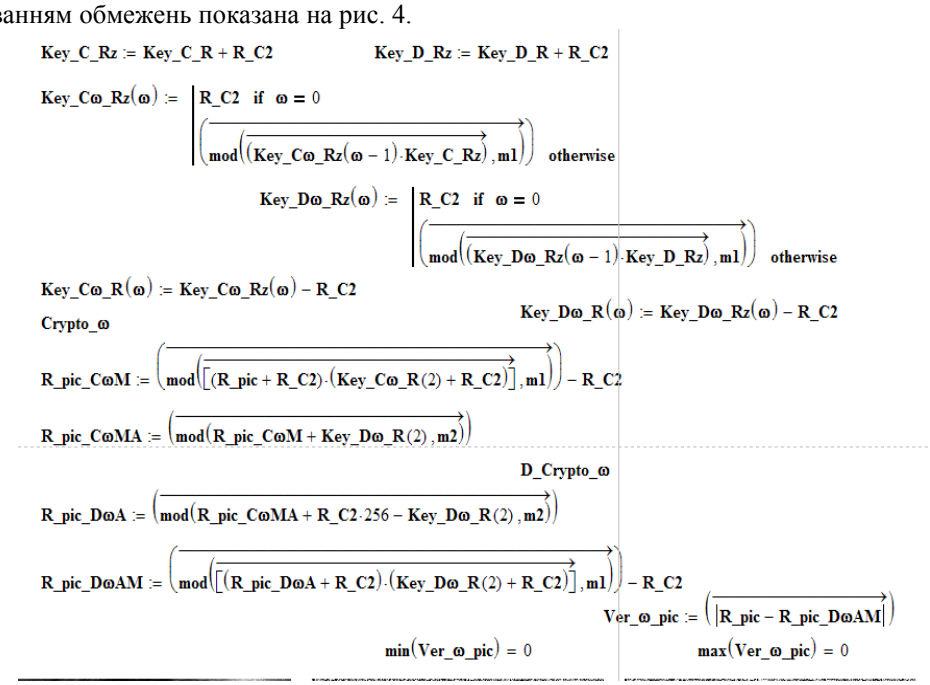


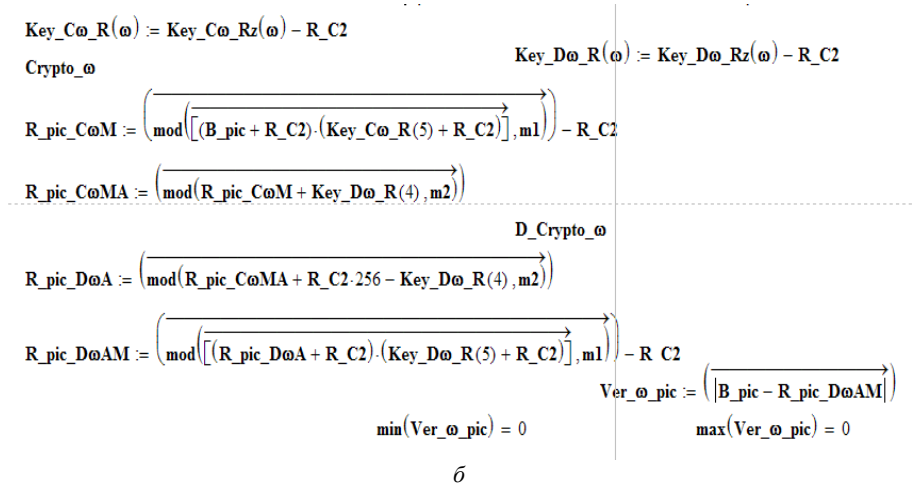
Рис. 3. Результати (фрагмент інтерфейсного вікна з Mathcad) моделювання процесів прямого та оберненого криптографічних перетворень матричним афінним шифром: зображення для шифрування, матричний ключ (набір трьох ключів), криптограма та розшифроване зображення у кольорових форматах.

Третя наша пропозиція полягає в тому, що можна необхідні для інших чи всіх спектральних складових, навіть не для кольорових, а багатоспектральних зображень чи 3D-масивів, матричні ключі формувати з одного головного чи базового ключа. Використання скалярних ключів та процедур поелементного піднесення у степінь за модулем кожного МК (навіть одного узгодженого ключа !) дає реалізацію одно- і багатокрокових МАШ [16–18] усього з одним секретним МК, з якого формуються інші похідні МК. Отже, третій наш експеримент полягав у розробці моделей та створенні процедури генерування низки МК як похідних від одного базового відповідно до узгодженої послідовності (вектора скалярних ключів з розмірністю рівній необхідній кількості матричних ключів з урахуванням кількості спектральних складових !) числових значень, що будуть взяті як степені в разі поелементних піднесень за модулем та у спробі здійснити КП на ос-

нові МАШ зображень різного формату. Цей модельний експеримент виконували на основі формул у матричному вигляді, частина з яких для достатнього розуміння та з урахуванням обмежень показана на рис. 4.



а



б

Рис. 4. Фрагмент вікна Mathcad з формулами, процедурами формування низки допоміжних прямих та обернених до них матричних ключів і формулами для мультиплікативної й адитивної складових прямого та оберненого криптографічних перетворень:
а – R-спектральної складової; *б* – B-спектральної складової кольорового зображення.

$Key\_C\_Rz := Key\_C\_R + R\_C2$

$\min(Key\_C\_R + R\_C2) = 1$ $\max(Key\_C\_R + R\_C2) = 256$

$Key\_C\_Rz =$

	590	591	592	593	594	595	596	597	598	599
533	197	58	7	91	71	176	26	62	65	151
534	158	32	199	136	28	197	175	42	70	247
535	96	182	95	114	112	134	200	24	177	192
536	106	200	199	90	145	23	155	83	21	139
537	210	134	186	54	20	21	170	233	218	119
538	195	239	16	15	49	250	39	11	162	148
539	225	43	30	96	40	123	81	105	161	56
540	165	234	27	117	160	229	216	153	5	100
541	189	204	120	206	9	128	59	116	79	38
542	114	182	74	126	243	240	34	114	186	243
543	253	60	159	137	123	146	202	16	152	15
544	245	247	232	71	161	222	91	46	172	227
545	161	241	82	192	173	199	76	107	150	103
546	99	250	40	19	141	27	194	141	41	124
547	16	15	53	204	53	223	244	218	206	76
548	85	179	35	78	254	184	131	123	231	174

а

$Key\_C\omega\_R(\omega) := Key\_C\omega\_Rz(\omega) - R\_C2$

$\min(Key\_C\omega\_Rz(1)) = 1$ $\max(Key\_C\omega\_Rz(1)) = 256$

$Key\_C\omega\_Rz(1) =$

	590	591	592	593	594	595	596	597	598	599
533	197	58	7	91	71	176	26	62	65	151
534	158	32	199	136	28	197	175	42	70	247
535	96	182	95	114	112	134	200	24	177	192
536	106	200	199	90	145	23	155	83	21	139
537	210	134	186	54	20	21	170	233	218	119
538	195	239	16	15	49	250	39	11	162	148
539	225	43	30	96	40	123	81	105	161	56
540	165	234	27	117	160	229	216	153	5	100
541	189	204	120	206	9	128	59	116	79	38
542	114	182	74	126	243	240	34	114	186	243
543	253	60	159	137	123	146	202	16	152	15
544	245	247	232	71	161	222	91	46	172	227
545	161	241	82	192	173	199	76	107	150	103
546	99	250	40	19	141	27	194	141	41	124
547	16	15	53	204	53	223	244	218	206	76
548	85	179	35	78	254	184	131	123	231	174

б

Рис. 5. Результати (інтерфейс-вікна Mathcad) формування базового МК

$\mathbf{Key\_C\omega\_R}(\omega) := \mathbf{Key\_C\omega\_Rz}(\omega) - \mathbf{R\_C2}$

$\min(\mathbf{Key\_C\omega\_Rz}(2)) = 1$ $\max(\mathbf{Key\_C\omega\_Rz}(2)) = 256$

$\mathbf{Key\_C\omega\_Rz}(2) =$

	590	591	592	593	594	595	596	597	598	599
533	2	23	49	57	158	136	162	246	113	185
534	35	253	23	249	13	2	42	222	17	100
535	221	228	30	146	208	223	165	62	232	113
536	185	165	23	133	208	15	124	207	184	46
537	153	223	158	89	143	184	116	62	236	26
538	246	67	256	225	88	49	236	121	30	59
539	253	50	129	221	58	223	136	231	221	52
540	240	15	215	68	157	13	139	22	25	234
541	255	239	8	31	81	193	140	92	73	159
542	146	228	79	199	196	32	128	146	158	196
543	16	2	95	8	223	242	198	256	231	225
544	144	100	111	158	221	197	57	60	29	129
545	221	256	42	113	117	23	122	141	141	72
546	35	49	58	104	92	215	114	92	139	213
547	256	225	239	239	239	128	169	236	31	122
548	29	173	197	173	9	189	199	223	162	207

в

$\mathbf{Key\_C\omega\_R}(\omega) := \mathbf{Key\_C\omega\_Rz}(\omega) - \mathbf{R\_C2}$

$\min(\mathbf{Key\_C\omega\_Rz}(7)) = 1$ $\max(\mathbf{Key\_C\omega\_Rz}(7)) = 256$

$\mathbf{Key\_C\omega\_Rz}(7) =$

	590	591	592	593	594	595	596	597	598	599
533	34	221	115	45	191	234	173	232	10	166
534	244	8	36	15	93	34	7	49	44	127
535	20	106	140	144	216	222	31	80	209	247
536	91	31	36	170	41	11	107	90	159	196
537	110	222	66	201	192	159	77	177	94	78
538	25	228	241	121	118	142	163	146	117	188
539	249	102	68	20	161	35	23	37	237	82
540	190	246	112	22	233	164	243	21	254	195
541	30	182	17	43	199	2	135	18	26	109
542	144	106	138	251	186	120	60	144	66	186
543	64	223	59	240	35	176	181	241	220	121
544	160	127	248	191	237	88	45	123	154	189
545	237	16	250	247	153	36	74	204	53	171
546	13	142	161	39	239	112	245	239	14	141
547	241	121	75	182	75	197	89	94	43	74
548	103	210	169	47	126	95	6	35	84	167

г

та його по-елементних степенів за модулем як допоміжних ключів з скалярними ключами.

На рис. 4 зображено копію фрагмента вікна Mathcad з формулами, процедурами формування низки допоміжних прямих та обернених до них матричних ключів і формулами для мультиплікативної й адитивної складових прямого та оберненого криптографічних перетворень. Як бачимо з рис. 4, *а*, похідні ключі Key_Cw_Rz(w) створюються рекурсивною процедурою поелементного піднесення у степінь за модулем попередніх МК, починаючи з базового, а степінь цих МК та відповідні їм матриці значень залежать від параметра w. Якщо ω = 0, то утворюється матриця Key_Cw_Rz(0), що дорівнює матриці R_C2, усі елементи якої є "1".

Деякі фрагменти-копії з вікон Mathcad цих МК з розмірами 600*549, що відповідали розмірам одного з низки зображень для КП, показані на рис. 5 у цифровому форматі, відповідають саме тим МК, що мають значення ω такі, як 1, 2, 7 . Узгоджений сторонами секретний ключ позначений як Key_C_R. Для відображення МК у форматі 8-бітних зображень виконується зміщення значень матриць МК відніманням від них матриці R_C2. Наголосимо, що перевірка засвідчує правильність потрапляння всіх значень елементів усіх матриць-ключів у необхідний діапазон. Результати цього експерименту в разі використання сформованих і показаних на рис. 5 ключів при КП кольорового зображення та його спектральних складових таким удосконаленим МАШ відображені на рис. 6–9. Вони свідчать про якісну правильну роботу моделей МАШ у разі застосування правильних ключів, неможливість розшифрувати без знання ключів і базового (не наводимо для неправильних ключів!).

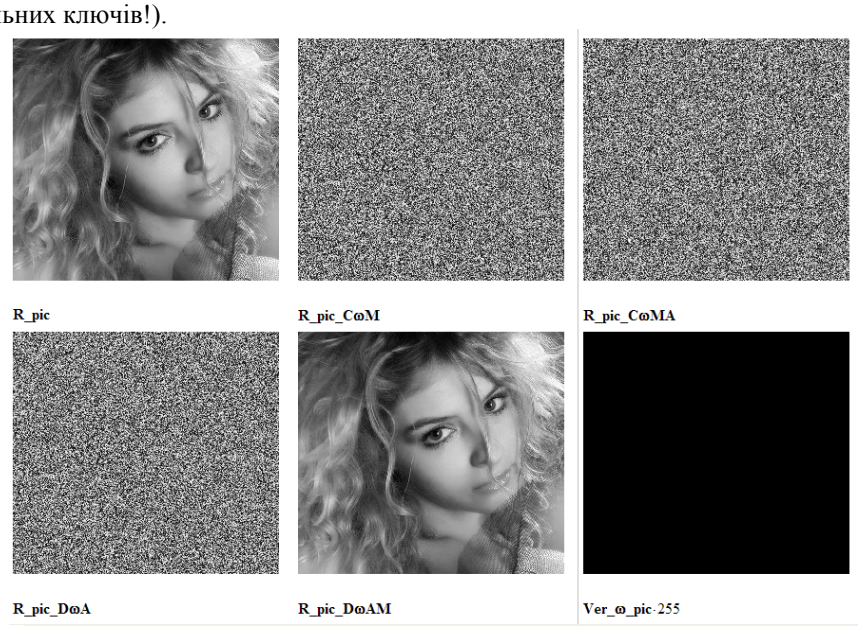


Рис. 6. Результати прямого й оберненого КП МАШ R складової кольорового зображення в разі використання для мультиплікативної та адитивної складових МАШ лише одного МК Key_Cw_R(2).

Ми також створили та експериментально перевірили підпрограму, що дає змогу відповідно до автоматично визначених розмірів вхідних масивів чи зображень формувати на основі висвітленого в працях [11,12] узагальненого на матричний випадок прото-

колу Діффі–Хелмана узгоджений сторонами захищеного передавання даних МК (МКо), робити їхню верифікацію та генерувати похідні від нього ключі.

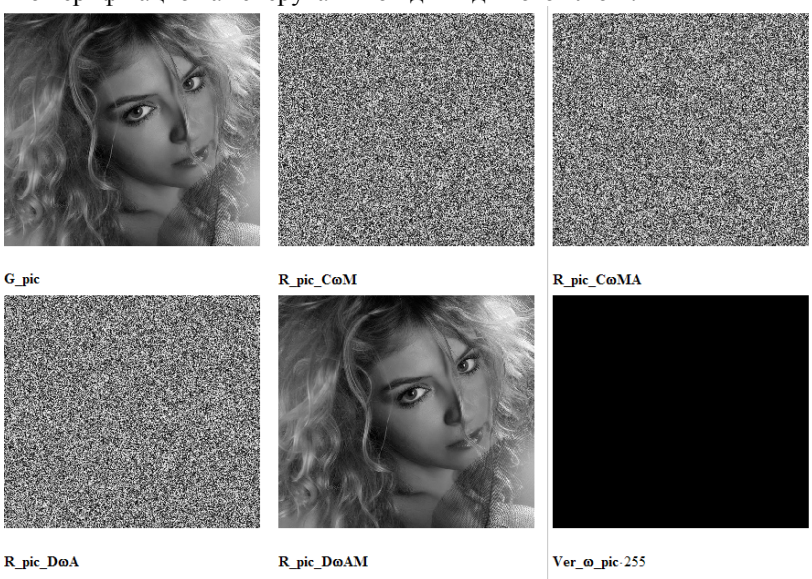


Рис. 7. Результати прямого та оберненого КП МАШ G складової кольорового зображення в разі використання для мультиплікативної та адитивної складових МАШ лише одного МК Key_Cw_R(7).

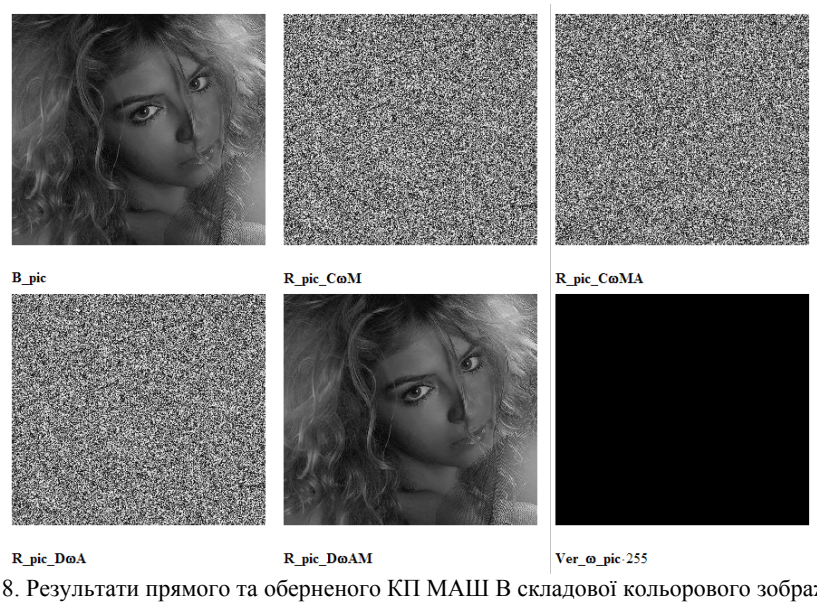


Рис. 8. Результати прямого та оберненого КП МАШ B складової кольорового зображення в разі використання для мультиплікативної та адитивної складових МАШ лише одного МК Key_Cw_R(5).

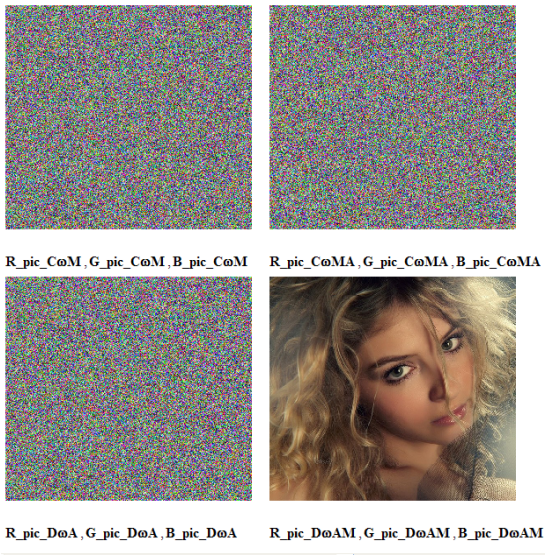


Рис. 9. Результати прямого та оберненого КП МАШ кольорового зображення в разі використання для мультиплікативної та адитивної складових шифру і для перетворень спектральних складових лише похідних від базового МК та параметричних скалярних ключів.

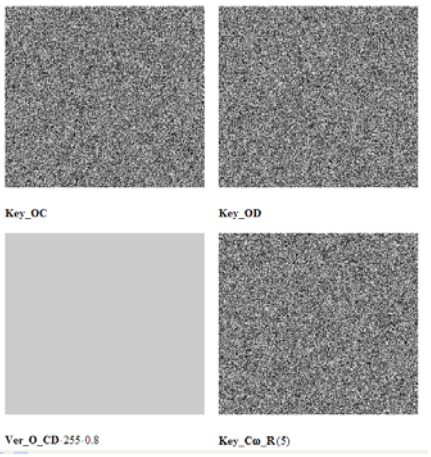


Рис. 10. Вигляд одного з базових матричних ключів **(Key_OC)**, оберненого до нього МКо **(Key_OD)**, допоміжного **(Key_Cw_R(5))** з параметром 5 та версифікаційної матриці **(Ver_O_CD)**, сформованих відповідно до вибраних параметрів та розмірності зображень, які шифрують. Фрагмент вікна та зображення зменшені!.

Створені підпрограмою ключі показані на рис. 10, а результати прямого й оберненого КП цими МК специфічного кольорового зображення природної сцени з фрагментами однакових значень інтенсивності за допомогою удосконалених МАШ – на рис. 11, 12. Аналогічні виконаним у працях [15, 17, 18, 21] гістограмний та ентропійний аналізи теж засвідчили хороші показники утворених криптограм і збільшення їхньої ентропії майже до 90–95 % від максимально можливої. Детальніше обговоримо ці питання нижче та покажемо деякі гістограми.

Для перевірки впливу розмірів, кількості спектральних складових, статистичних характеристик і структурно-текстурних особливостей зображень, що підлягають криптографічним перетворенням, на деякі показники роботи запропонованих удосконалених МАШ, а особливо на гістограмно-ентропійні та візуальні характеристики отриманих криптограм ми виконали інші експерименти.

Результати цих модельних експериментів з іншими зображеннями, включаючи кадри з відео-потоку, великорозмірні (640*1024) багатоспектральні (100 спектральних каналів) зображення та їхні складові, тексто-графічні документи в кольоровому форматі тощо, показані на рис. 13–17 та теж підтверджують правильне функціонування МАШ зі зменшеною кількістю ключів. Вони засвідчили, що тривалість виконання процедур КП не перевищує декількох секунд навіть для великорозмірних (640*1024) кольорових зо-

бражень у разі їхнього моделювання в середовищі Mathcad та використання широковживаних ПЕОМ з продуктивністю середнього класу.

Звичайно, що на загальну тривалість виконання необхідних процедур впливає і кількість спектральних каналів, і спосіб запису програмних модулів у разі емулювання моделей, і застосування векторних паралельних обчислень, а тому робити детальніші оцінки недоречно і тут ми лише зазначимо, що наші матричні моделі МАШ з декомпозицією мають внутрішній паралелізм, легше структурно відображаються на апаратні матричні засоби.

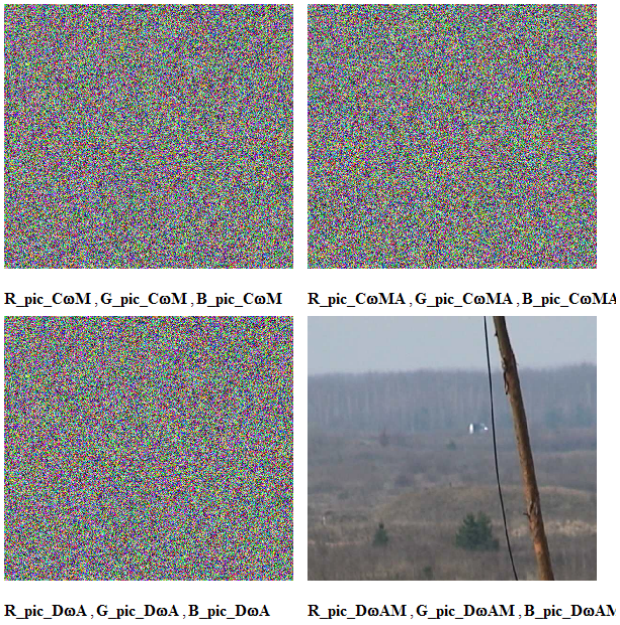


Рис. 11. Кольорові криптограми-зображення, отримані після мультиплікативного (ліворуч у верхньому ряду), мультиплікативного та адитивного (праворуч у верхньому ряду) прямих (зашифрування) та зворотних перетворень (розшифрування): адитивним (ліворуч у нижньому ряду) та мультиплікативним (розшифроване праворуч у нижньому ряду).

Візуальний аналіз отриманих під час моделювання та показаних на рис. 13–17 криптограм свідчить про якісне зашифрування та коректну роботу ММ прямого й оберненого криптографічних перетворень на основі МАШ у всіх випадках.

Для точнішого їхнього аналізу ми визначали ентропію зображень, ключів та криптограм та побудували за допомогою інструментів Mathcad їхні гістограми. Вони показані на рис. 18, 19. Як бачимо з рис. 18, 19, незважаючи на дуже специфічні гістограми складових зображення, гістограми складових криптограми суттєво змінилися, і не дають змоги за їхнім виглядом розпізнати можливий вигляд зображення чи прочитати повідомлення або зрозуміти ТГД.

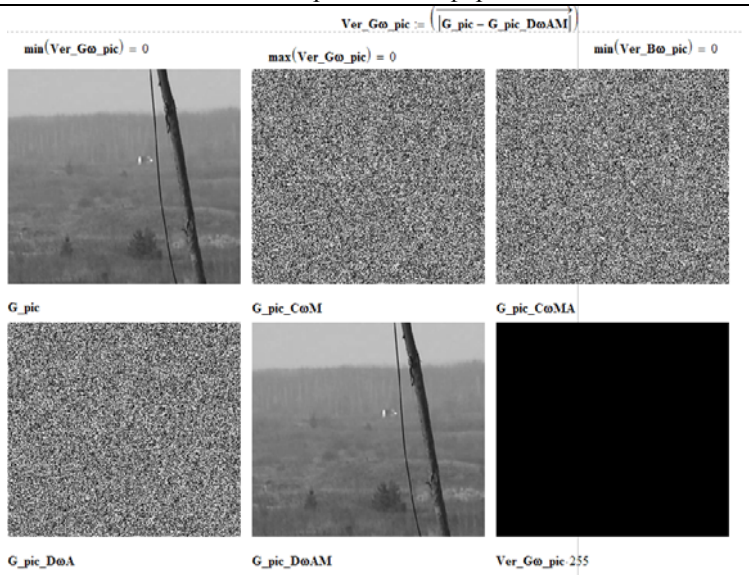


Рис. 12. Фрагмент інтерфейсного вікна, що демонструє процес прямого й оберненого криптографічних перетворень однієї, а саме – G, спектральної складової кольорового зображення, що показане на рис.12 та використане для модельних експериментів.

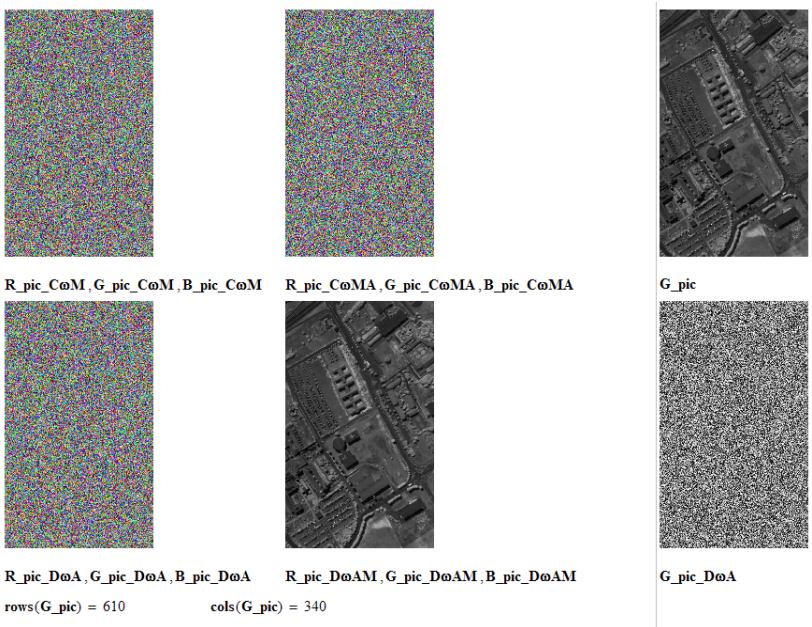


Рис. 13. Фрагмент вікна з криптограмами та розшифрованими зображеннями, що демонструє процес прямого й оберненого криптографічних перетворень складових великорозмірного багатоспектрального зображення, що отримане з літального пристрою дистанційного моніторингу та використане для модельних експериментів.

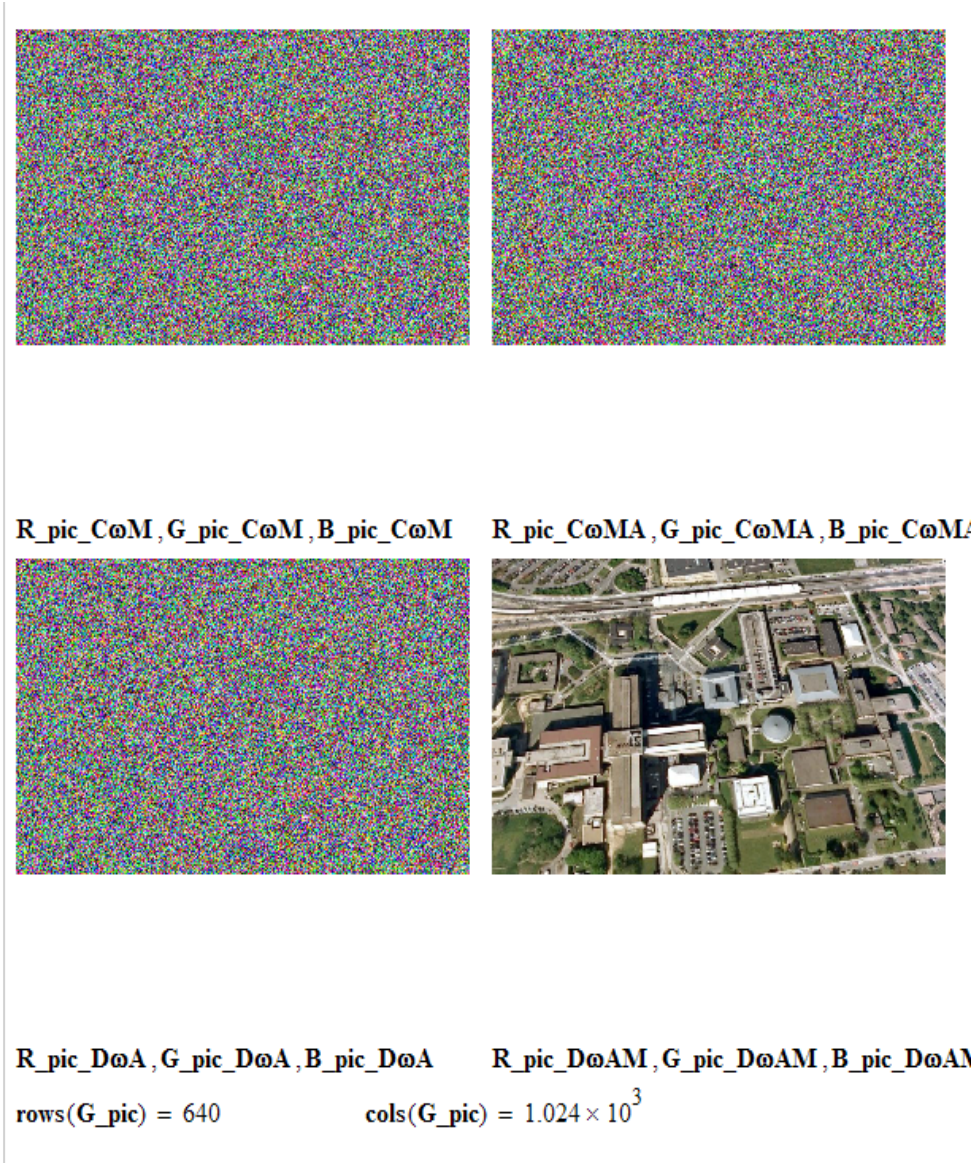


Рис. 14. Фрагмент вікна з криптограмами та розшифрованим зображенням (усі кольорові!), що демонструє процес прямого й оберненого криптографічних перетворень на основі удосконаленого МАШ великорозмірного зображення (640*1024 елементів), що використане для експериментів.

Для оцінювання якості закриття зображень чи документів у разі їхнього шифрування МАШ ми також використовували розроблену й висвітлену в [16] підпрограму у MathCad, яка дає змогу обчислити середню ентропію на 1 піксель конкретних зобра-

жень. Як бачимо з рис. 18, 19 та з гістограмних розподілів R,G,B складових явного кольорового зображення та як підтверджено визначенням ентропії, ентропія початкового явного зображення, а саме – його 8-бітових складових, є в межах 3–4 біт на піксель, а ентропія криптограм (її складових) для різних експериментів коливалась у межах 7,5–7,8 біт на піксель, тобто є дуже близькою до максимально можливої 8. Подібні значення ентропії мають і 8-бітні складові МК (див. рис. 18).

Зазначимо, що порівняння (з рис. 19) гістограм та ентропій складових криптограм, отриманих після мультиплікативного та мультиплікативного з подальшим адитивним перетвореннями дає змогу зробити висновок про незначні їхні відмінності. Ми також з'ясували, що багатораундові КП на основі МАШ практично мало поліпшують гістограмно-ентропійні характеристики, якщо базовий узгоджений ключ правильно вибраний чи генерований, відповідає необхідним вимогам і теж має наближену до максимально можливої ентропію.

Чим більша ентропія криптограми, тим більша міра невизначеності відповідного зображення і тим складніше провести атаку на цей алгоритм. Наголосимо на визначеному моделюванням факті, що всі похідні ключі мають необхідний гістограмний розподіл, який практично наближається до рівномірного розподілу, а отже, має і наближену до максимальної ентропію. Це дає змогу навіть за візуальним виглядом гістограми оцінювати якість як ключів, так і криптограм.

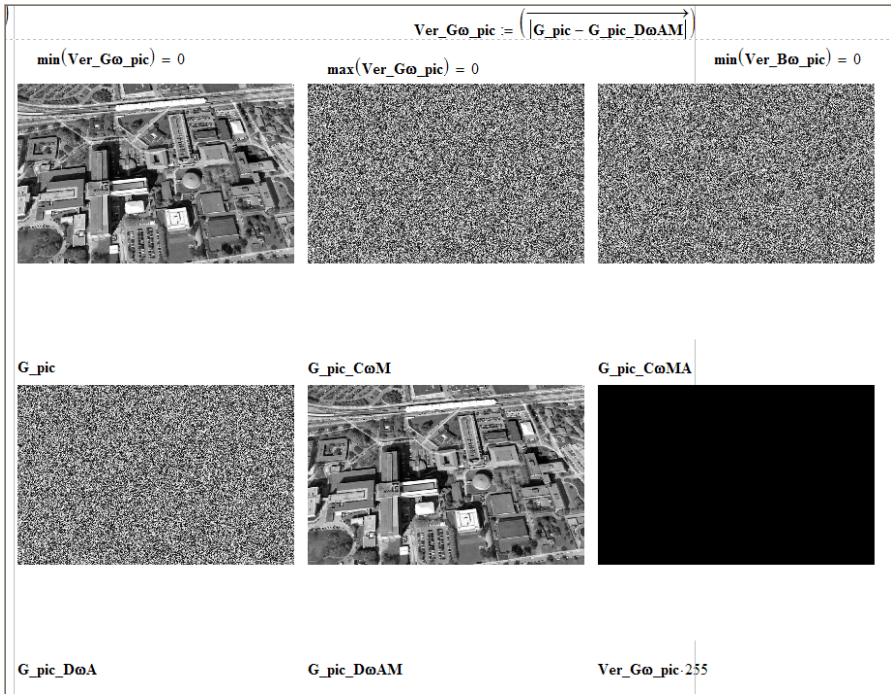


Рис. 15. Фрагмент інтерфейсного вікна, що демонструє деталі процесів прямого й оберненого криптографічних перетворень та їхньої верифікації однієї, а саме – G, спектральної складової кольорового зображення, що показане на рис. 14 та використане для моделювання удосконаленого МАШ зі зменшеною кількістю (один базовий!) МК.

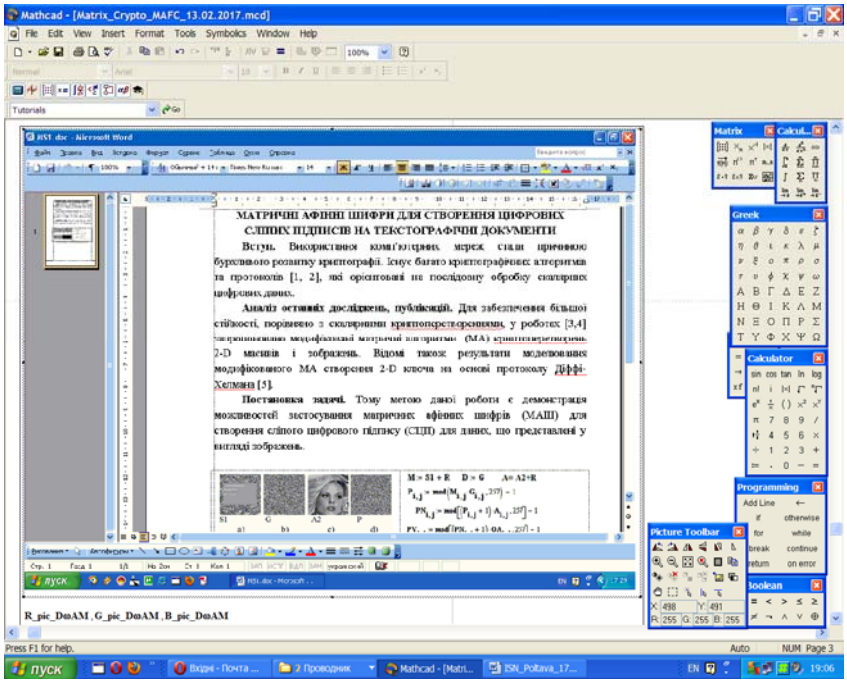


Рис. 16. Інтерфейс-вікно Mathcad (повністю) з інструментами та відображеним у його вікні кольоровим текстографічним документом (ТГД), що використаний для моделювання удосконалених МАШ, включаючи багатораундові.

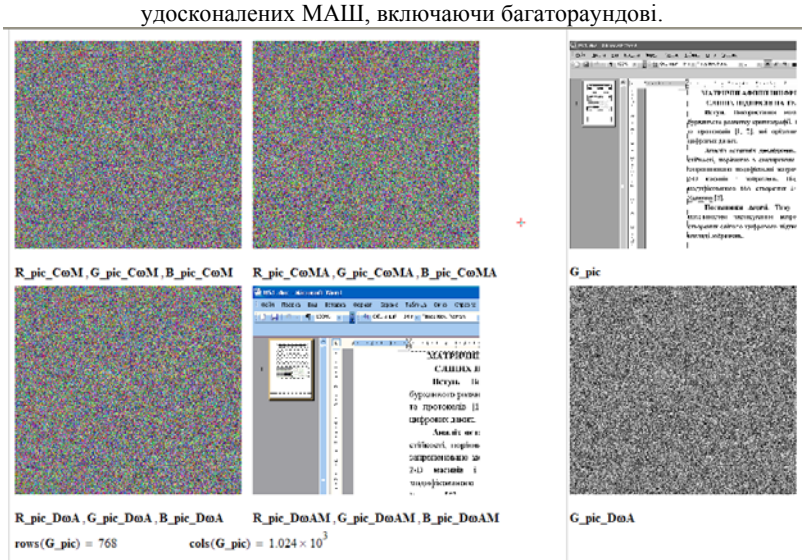


Рис. 17. Фрагмент вікна з фрагментами криптограм та розшифрованих зображень ТГД з рис. 16 (як кольорових у центрі та ліворуч, так і чорно-білих відповідних спектральних складових!), що демонструє правильність процесів прямого й оберненого криптографічних перетворень ТГД за допомогою удосконаленого МАШ.

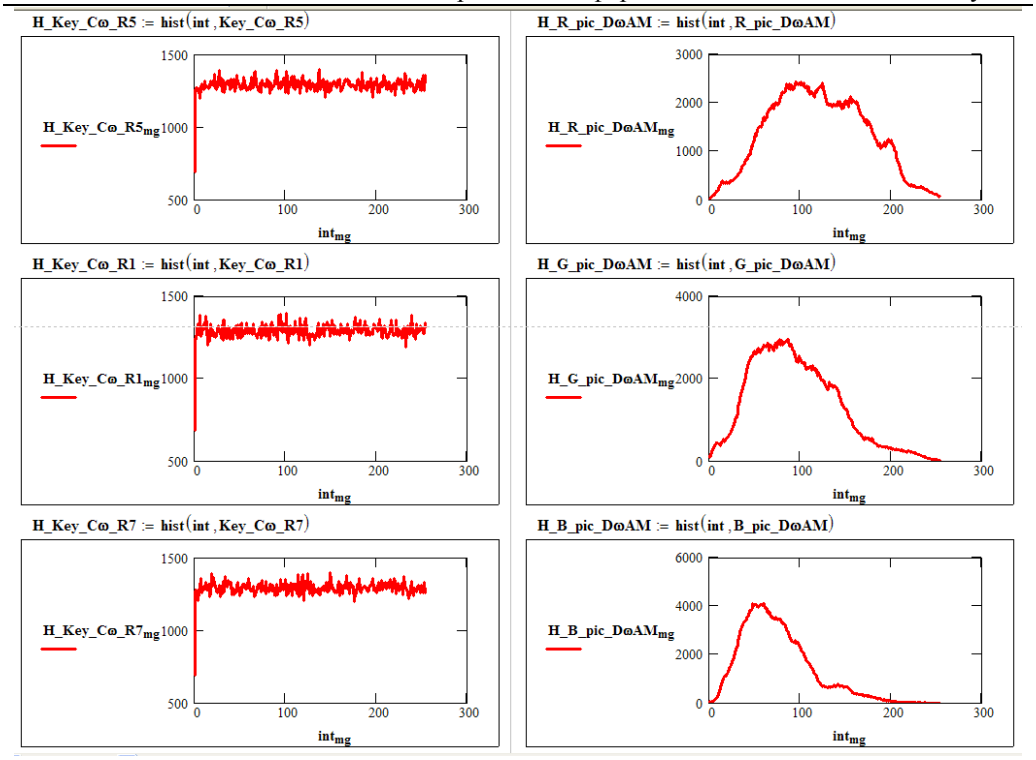


Рис. 18. Гістограми трьох сформованих з головного матричних ключів (ліворуч) та відповідних їм R,G,B спектральних складових (праворуч) кольорового зображення, над яким виконувались КП на основі МАШ та яке показане на рис. 9 праворуч у нижньому ряду.

Зазначимо, що використання спектральної декомпозиції та рекурсивних процедур формування набору МК, узгодженості між розмірами всіх матриць, цікавих зміщень діапазонів значень елементів матриць дає змогу застосовувати для КП на основі удосконаленого МАШ, по суті, лише один секретний матричний ключ, який, до речі, як і його похідні, теж легко подати у вигляді зображень. А маючи лише один такий МК, оскільки похідні від нього МК,як степені будуть різними і вибиратимуться на основі домовленостей про вектор скалярних ключів, можна реалізувати всі необхідні для конкретних застосувань та для різних видів даних надійні процедури КП МАШ.

Усі виконані експерименти та наведені тут їхні результати підтвердили коректну роботу запропонованих моделей та їхніх модифікацій, зручність їхньої адаптації до розмірів зображень чи їхніх фрагментів-блоків для криптографічних перетворень, зручність та простоту вибору необхідних ключів. З урахуванням обмежень тут ми не розглядаємо ефективні процедури, протоколи узгодження секретного ключа та їхній обмін, оновлення, оскільки ці питання висвітлюватимемо в нових статтях або ж вони частково розглянуті в [11, 12] для деяких загальніших видів.

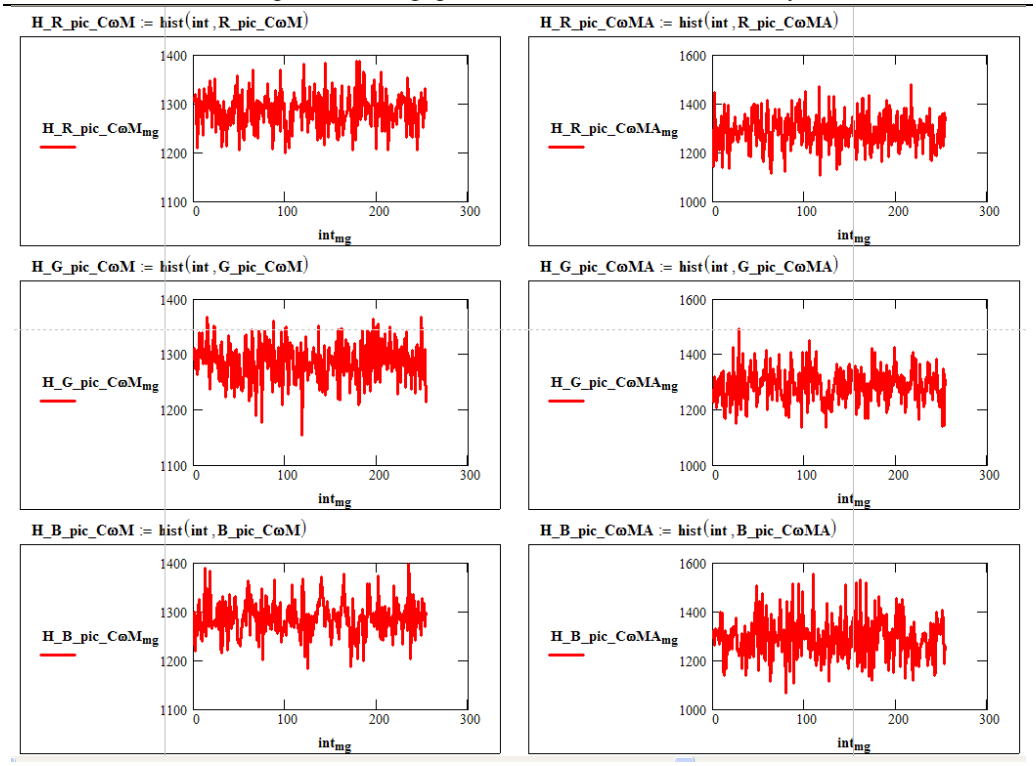


Рис. 19. Гістограми трьох R,G,B спектральних складових (ліворуч) отриманої криптограми після мультиплікативного КП та відповідних їм R,G,B спектральних складових (праворуч) отриманої криптограми після другого адитивного КП кольорового зображення, над яким виконувались КП на основі МАШ та яке показане на рис. 9 праворуч у нижньому ряду.

Отже, на підставі огляду й аналізу публікацій обґрунтовано перспективність та необхідність подальших досліджень і удосконалень матричних афінних шифрів та їхніх похідних. Запропоновано способи вдосконалення та наведено результати моделювання матричних афінних удосконалених шифрів для криптографічних перетворень чорно-білих і кольорових зображень зі зменшеною кількістю матричних ключів. Розроблено модифіковані моделі й алгоритмічні процедури процесів формування ключів, прямого та оберненого криптографічних перетворень, що зводяться до матрично-матричних поелементних операцій за модулем.

З'ясовано, що використання декомпозиції кольорових і багатоспектральних зображень на чорно-білі складові дало змогу уніфікувати процедури перетворень, використовувати лише один узгоджений матричний ключ та розширити види, формати даних і спектр застосувань шифрів. Запропоновано та підтверджено експериментально, що як допоміжні похідні ключі можна використовувати степені головного ключа за модулем. Доведено на підставі низки експериментів у середовищі Mathcad з різними багатоградаційними та кольоровими зображеннями для їхнього шифрування та розшифрування за допомогою розроблених моделей, що запропоновані удосконалення таких шифрів є ко-

ректними, адекватними, зручними для використання, мають переваги та дають змогу навіть збільшити їхні функціональні можливості. Визначено й оцінено гістограмно-ентропійні характеристики отриманих за допомогою МАШ криптограм, що також свідчать про їхні криптографічні властивості та стійкість.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Ємець В.* Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : БаК, 2003. – 144 с.
2. *Хорошко В. О.* Методи та засоби захисту інформації : [навч. посібник] / В. О. Хорошко, А. О. Четков. – К. : Юніор, 2003. – 502 с.
3. *Коркішко Т. А.* Алгоритми та процесори симетричного блокового шифрування : [наукове видання] / Т. А. Коркішко, А. О. Мельник, В. А. Мельник. – Львів : БаК, 2003. – 168 с.
4. *Ковальчук А.* Підвищення стійкості системи RSA при шифруванні зображень / А. Ковальчук // Технічні вісті. – 2009. – № 1–2. – С. 70–71.
5. *Рашкевич Ю. М.* Афінні перетворення в модифікаціях алгоритму RSA шифрування зображень / Ю. М. Рашкевич, А. М. Ковальчук, Д. Д. Пелешко // Автоматика. Автоматизация. Электротех. комплексы и системы. – 2009. – № 2 (24). – С. 59–66.
6. *Deergha Rao K.* A New and Secure Cryptosysyem for Image Encryption and Decryption / K. Deergha Rao, K. Praveen Kumar, P. V. Murali Krishna // IETE J. of research. – 2011. – Vol. 57. – Is. 2. – P. 165–171.
7. *Han Shuihua.* An Asymmetric Image Encryption Based on Matrix Transformation / Han Shuihua, Yang Shuangyuan // Ecti transactions on computer and information technology. – 2005. – Vol. 1, N 2. – P. 126–133.
8. *Chin-Chen Chang.* A new encription algorithm for image cryptosystems / Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen // The J. of Systems and Software. – 2001. – N 58. – P. 83–91.
9. *Красиленко В. Г.* Алгоритми та архітектури для високоточних матрично-матричних перемножувачів на основі оптичної чотирьохзначної знакозмінної арифметики / В. Г. Красиленко // Вимірювальна та обчислювальна техніка в технол. процесах. – 2004. – № 1. – С. 13–26.
10. *Krasilenko V. G.* A noise-immune cryptographic information protection method for facsimile information transmission and the realization algorithms / V. G. Krasilenko, A. I. Nikolsky, V. Bardachenko // Proc. SPIE. – 2006. – Vol. 6241. – P. 316–322.
11. *Красиленко В. Г.* Алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та їх моделювання / В. Г. Красиленко, В. І. Яцковський, Р. О. Яцковська // Системи обробки інформації. – 2012. – Вип. 8. – С. 107–110.
12. *Красиленко В. Г.* Моделювання модифікованого алгоритму створення 2-D ключа в криптографічних застосуваннях / В. Г. Красиленко, О. І. Нікольський, О. О. Лазарєв // Наука і навчальний процес. – Вінниця, 2008. – С. 107–109.
13. *Красиленко В. Г.* Розробка методу криптографічного захисту інформації текстографічного типу / В. Г. Красиленко, С. А. Свіренюк // Наука і навчальний процес. – Вінниця, 2006. – С. 73–74.

14. *Красиленко В. Г.* Моделювання сліпих електронних цифрових підписів матричного типу на конфіденційну текстографічну документацію / В. Г. Красиленко, Р. О. Яцковська, С. К. Грабовляк // І Міжнар. наук.-метод. конф. – Вінниця : ВНАУ, 2012. – С. 103–107.
15. *Красиленко В. Г.* Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. – 2012. – Вип. 8. – С. 102–106.
16. *Красиленко В. Г.* Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. – 2011. – Вип. 7(97). – С. 60–63.
17. *Красиленко В. Г.* Моделювання матричних алгоритмів криптографічного захисту / В. Г. Красиленко, Ю. А. Флавицька // Вісник НУ "Львів. політехніка". Комп'ютерні системи та мережі. – 2009. – № 658. – С. 59–63.
18. *Красиленко В. Г.* Матричні афінно-перестановочні шифри для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. – 2012. – Вип. 3 (101), т. 2. – С. 53–62.
19. *Красиленко В. Г.* Матричні моделі перестановок з матрично-бітовою декомпозицією для криптографічних перетворень зображень та їх моделювання [текст] / В. Г. Красиленко, В. М. Дубчак, О. В. Красиленко // Наука і навчальний процес. – Вінниця, 2013. – С. 90–92.
20. *Красиленко В. Г.* Матричні моделі криптографічних перетворень зображень з матрично-бітовозрізовою декомпозицією і перемішуванням та їх моделювання / В. Г. Красиленко, Д. В. Нікітович // Сучасні інформаційні системи і технології. Інформаційна безпека : Матеріали 68 НТК. – Одеса, ОНАЗ ім. О.С.Попова, 2013. – С. 139–143.
21. *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 Хмельницького нац. ун-ту. Технічні науки. – 2014. – № 1. – С. 74–79.
22. *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 доп. V Всеукр. наук.-практ. конф. – К., 2010. – С. 120–124.
23. *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 інформ. технології. – 2015. – Вип. 6. – С 111–127.
24. *Красиленко В. Г.* Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітовозрізовою декомпозиціями / В. Г. Красиленко, Д. В. Нікітович // Комп'ютерно-інтегровані технології : освіта, наука, виробництво. – 2016. – № 23. – С. 31–36.
25. *Красиленко В. Г.* Моделювання криптографічних перетворень кольорових зображень з верифікацією цілісності криптограм на основі матричних моделей перестановок / В. Г. Красиленко, Д. В. Нікітович // Проблеми моделювання та розроблення інформаційних систем : Матеріали наук.-практ. інтернет-конф. – Дрогобич : ДДПУ

ім. І. Франка, 2016. – С. 128–136. [Електронний ресурс]. – Режим доступу : http://ddpu.drohobych.net/wp-content/uploads/2016/04/material_konf.pdf37

Стаття: надійшла до редакції 13.03.2017,
доопрацьована 17.03.2017,
прийнята до друку 22.03.2017.

IMPROVEMENT AND MODELING OF MATRIX AFINE CIPHERS FOR IMAGES CRYPTOGRAPHIC TRANSFORMATIONS

V. Krasilenko, D. Nikitovich

Research Division,
Vinnitsa Social Economy Institute of University "Ukraine",
Keletskaya Str., 86/131, Vinnitsa, 21021, Ukraine
krasilenko@mail.ru

The paper presents the results of modeling matrix affine advanced ciphers for cryptographic transformations of grayscale and color images with a reduced number of matrix keys. Modified models and algorithmic procedures for the formation of keys, forward and reverse cryptographic transformations, which reduce to matrix-matrix element-by-element modulo operations, have been developed. The use of decomposition of color and multi-spectral images into their grayscale components made it possible to unify the transformation procedures, use only one matched key and expand the types, data formats and the range of applications of such ciphers. As auxiliary production keys, the master key degrees are used modulo. Based on a series of experiments in the Mathcad environment with various grayscale and color images for the purpose of encrypting and deciphering them using the proposed models, it is shown that the proposed improvements of such ciphers are adequate, convenient for use, have advantages and allow even to increase their functionality.

Key words: matrix affine cipher, cryptographic transformation of images, matrix models, decomposition, cryptogram, matched key, matrix key, element-by-element matrix-matrix ordering, matrix-matrix procedure.