



ISBN 978-1-968285-23-4

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

SCIENCE, EDUCATION, INNOVATIONS, AND SOCIETY: STRATEGIC PRIORITIES FOR SUSTAINABLE DEVELOPMENT

Book of abstracts



November 29, 2025

**Seattle,
USA**



CONTENTS

SECTION 1. PEDAGOGICAL SCIENCES.....	8
Дешко Н. В., Іваничко І. І., Раїнчук В. А. ТОЛЕРАНТНІСТЬ І НЕНАСИЛЬНИЦЬКЕ СПІЛКУВАННЯ ЯК УМОВИ ФОРМУВАННЯ ЕМОЦІЙНОГО ІНТЕЛЕКТУ СТУДЕНТІВ....	8
Риндюк В. В. ОРГАНІЗАЦІЯ САМОСТІЙНОЇ ПІЗНАВАЛЬНОЇ ДІЯЛЬНОСТІ СТАРШОКЛАСНИКІВ З ВИКОРИСТАННЯМ НАВЧАЛЬНИХ ПЛАТФОРМ	14
SECTION 2. EDUCATION (PRESCHOOL, PRIMARY, SECONDARY, VOCATIONAL AND SPECIAL EDUCATION)	18
Адамовська М. С. КУЛЬТУРОЛОГІЧНА КОМПЕТЕНТНІСТЬ СТУДЕНТІВ ДИЗАЙНЕРСЬКИХ СПЕЦІАЛЬНОСТЕЙ: ІННОВАЦІЙНІ СТРАТЕГІЇ ТЮТОР-КРЕЙТОРА В КОНТЕКСТІ СТАЛОГО РОЗВИТКУ	18
Іноземцев С. А. ВИКОРИСТАННЯ ПРОЄКТНИХ ТЕХНОЛОГІЙ У ФОРМУВАННІ ЕКОЛОГІЧНОЇ КОМПЕТЕНТНОСТІ МОЛОДШИХ ШКОЛЯРІВ У ЗАКЛАДАХ ПОЗАШКІЛЬНОЇ ОСВІТИ	22
Nuzhna S. A., Domin Y. O. FLIPPED LEARNING IN COMPUTER SCIENCE: USING MODERN CLOUD TECHNOLOGIES AND ONLINE PLATFORMS.....	25
SECTION 3. PHILOLOGICAL SCIENCES	30
Avazneli M., Koberidze M. ETHNOGRAPHY OF SPEECH	30
Baratashvili M., Koberidze M. THE PLACE OF DIALECT AND SOCIOLECT IN SOCIETY (JARGON, ARGO, SLANG).....	32

Gvimradze S., Koberidze M. THE IMPORTANCE OF CONTEXT FOR TEXT	34
Доній Т. М., Бугрій А. В. ПЕРЕКЛАДАЦЬКІ ТРАНСФОРМАЦІЇ У ВІДТВОРЕННІ УРБАНІСТИЧНИХ РЕАЛІЙ ПОСТМОДЕРНІСТСЬКОЇ ПОЕЗІЇ.....	37
Muzashvili S., Koberidze M. SYNTACTIC DISTRIBUTION IN GEORGIAN.....	40
Черняк С. В. ІЗ СПОСТЕРЕЖЕНЬ НАД СПОСОБАМИ НОМІНАЦІЇ ТРАДИЦІЙНОГО ОДЯГУ ПОДОЛЯН.....	43
SECTION 4. PHYSICAL CULTURE AND SPORTS.....	49
Мерзлікіна О. А., Сущенко Л. П., Кондрин А. В. СУЧАСНІ ПІДХОДИ ДО ФІЗКУЛЬТУРНО-СПОРТИВНОЇ РЕАБІЛІТАЦІЇ ВІЙСЬКОВОСЛУЖБОВЦІВ З БОЛЯМИ У СПИНІ В УМОВАХ РЕАБІЛІТАЦІЙНИХ ЗАКЛАДІВ.....	49
Приймак М. М. РОЛЬ ТРЕНЕРА ТА СПОРТИВНОЇ КОМАНДИ У СОЦІАЛЬНІЙ АДАПТАЦІЇ ТА ОСОБИСТІСНОМУ РОЗВИТКУ СПОРТСМЕНА.....	53
Тимошенко О. В., Качур Є. Ю., Юрченко К. С. ФІЗКУЛЬТУРНО-СПОРТИВНА РЕАБІЛІТАЦІЯ ЖІНОК 40-45 РОКІВ З ТРАВМОЮ ПЛЕЧА.....	57
SECTION 5. LAW	60
Ільїна О. В., Ткаченко В. В. ПОНЯТТЯ ОСУДНОСТІ ТА ОСОБЛИВОСТІ ВПЛИВУ ОБМЕЖЕНОЇ ОСУДНОСТІ НА КРИМІНАЛЬНУ ВІДПОВІДАЛЬНІСТЬ	60

SECTION 6. ECONOMICS AND MANAGEMENT 64

Vasiltsova O.

INTERNATIONAL EXPERIENCE OF ECO-MANAGEMENT AS A
PREREQUISITE FOR ECOLOGICAL CAPITALIZATION IN FOOD
ENTERPRISES 64

Єлецьких С. Я., Колюбаєва К. П., Маматов А. М.

РЕСУРСНИЙ ПОТЕНЦІАЛ ЯК ОСНОВА ДОСЯГНЕННЯ
СТРАТЕГІЧНИХ І ТАКТИЧНИХ ЦІЛЕЙ ДІЯЛЬНОСТІ
ПІДПРИЄМСТВА 69

Семенча І. Є., Кісін Б. О.

АКТУАЛЬНІ ПИТАННЯ ОРГАНІЗАЦІЇ УПРАВЛІННЯ ЗБУТОВОЮ
ДІЯЛЬНІСТЮ ПІДПРИЄМСТВ В СУЧАСНІЙ УКРАЇНІ 72

SECTION 7. FINANCE, ACCOUNTING, BANKING, INSURANCE 76

Безпаленко О. В., Ліщинський В. В.

ВИЗНАЧЕННЯ ОПТИМІЗАЦІЇ СТРУКТУРИ КАПІТАЛУ НА ОСНОВІ
МІНІМІЗАЦІЇ СЕРЕДНЬОЗВАЖЕНОЇ ВАРТОСТІ КАПІТАЛУ 76

Довгань О. І.

ВІДКРИТИЙ БАНКІНГ ЯК ДРАЙВЕР ЦИФРОВОЇ
ТРАНСФОРМАЦІЇ ФІНАНСОВОГО РИНКУ УКРАЇНИ 80

**SECTION 8. PUBLIC MANAGEMENT, ADMINISTRATION AND
PUBLIC ADMINISTRATION 82**

Калюжний В. В.

ПЕРСПЕКТИВИ РОЗВИТКУ НОРМАТИВНОЇ, ІНСТИТУЦІЙНОЇ ТА
ІНФРАСТРУКТУРНОЇ БАЗИ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ У
СФЕРІ ПРИКОРДОННОЇ БЕЗПЕКИ 82

Крушельницька Т. А., Конівець Т. Є., Хорошун К. С.

ЕКОЛОГІЧНІ МЕХАНІЗМИ В СИСТЕМІ ЖИТЛОВО-
КОМУНАЛЬНОГО ГОСПОДАРСТВА ВЕЛИКИХ МІСТ СВІТУ ТА
МОЖЛИВОСТІ ЇХ АДАПТАЦІЇ В МІСТІ ДНІПРІ 85

Чумак А. В. МОЛОДЬ ЯК СПЕЦИФІЧНА СОЦІАЛЬНО-ДЕМОГРАФІЧНА ГРУПА І ОБ’ЄКТ КРИМІНОЛОГІЧНОГО ДОСЛІДЖЕННЯ.....	90
SECTION 9. PSYCHOLOGICAL SCIENCES.....	94
Гамма Т. В., Горошко В. І., Старик Р. М. КОМПЛЕКСНА РЕАБІЛІТАЦІЯ ЯК ЗАСІБ ЗАПОБІГАННЯ ТРИВОЖНИМ РОЗЛАДАМ У СТУДЕНТІВ В УМОВАХ ХРОНІЧНОГО СТРЕСУ	94
Melnychuk D., Furman O. PSYCHOLOGICAL SUPPORT OF FAMILIES WITH CHILDREN WITH SPECIAL EDUCATIONAL NEEDS	97
SECTION 10. TECHNICAL SCIENCES, PRODUCTION AND TECHNOLOGY	100
Гануліч Б. К. ВАРІАНТ ОПИСУ КВАЗІКРИХКОГО РУЙНУВАННЯ	100
Шлюнь Н. В., Шевчук Л. В., Шевчук А. В. КЕЛЬТСЬКИЙ КАМІНЬ ЯК МАТЕМАТИЧНА МОДЕЛЬ КОЛИВАНЬ КРУЖЛЯННЯ ДОЛОТА.....	104
SECTION 11. ARCHITECTURE AND CONSTRUCTION	107
Племенник І. В. ПРИНЦИПИ ПРОЄКТУВАННЯ БАГАТОФУНКЦІОНАЛЬНИХ ЖИТЛОВИХ КОМПЛЕКСІВ	107
SECTION 12. INFORMATION TECHNOLOGY AND CYBERNETICS.....	111
Boiarynova Yu., Odnoraz A. COMPARATIVE ANALYSIS OF TOOLS FOR CREATING AND COMPILING UNIT TESTS FOR CODE WRITTEN IN C/C++	111

Красиленко В. Г., Нікітович Д. В. ВЕЛИКОБЛОКОВІ МАТРИЧНІ АФІННО-ПЕРЕСТАНОВОЧНІ ШИФРИ З ІЗОМОРФНИМИ ПРЕДСТАВЛЕННЯМИ БЛОКІВ І КЛЮЧІВ.....	115
Кут В. І., Пайдич М. В. ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ПЕРСОНАЛЬНОЇ РЕАБІЛІТАЦІЇ, ТРЕНУВАНЬ ТА ОЗДОРОВЛЕННЯ	121
SECTION 13. GEOGRAPHICAL AND GEOLOGICAL SCIENCES	124
Kravtsova I. V., Melnychenko P. A., Kasianenko S. P. MONITORING AND ASSESSMENT OF ANTHROPOGENIC IMPACTS ON URBAN LANDSCAPES: A CASE STUDY APPROACH	124
SECTION 14. TOURISM AND HOTEL AND RESTAURANT BUSINESS	128
Chernykhivska A. STRATEGIC PRIORITIES FOR SUSTAINABLE DEVELOPMENT OF THE HOTEL-RESTAURANT BUSINESS AND TOURISM.....	128

УДК 004.056.55: 004.032: 004.93

Красиленко В. Г.

к.т.н., доцент кафедри комп'ютерних наук та цифрової економіки,
Вінницький національний аграрний університет,

Нікітович Д. В.

аспірантка,

Вінницький національний технічний університет

ВЕЛИКОБЛОКОВІ МАТРИЧНІ АФІННО-ПЕРЕСТАНОВОЧНІ ШИФРИ З ІЗОМОРФНИМИ ПРЕДСТАВЛЕННЯМИ БЛОКІВ І КЛЮЧІВ

Розвиток електронних комунікацій, ріст об'ємів різноманітних чорно-білих, кольорових, багато-спектральних зображень (З), текстографічних документів (ТГД) з таблицями, формулами, малюнками, діаграмами, підписами, резолюціями, які є 2-D З, в тому числі і таких ТГД, які є конфіденційними або з обмеженим доступом, викликали гостру необхідність у криптографічних перетвореннях (КП) З, ТГД для їх безпечного зберігання, передачі, для створення, наприклад, електронних цифрових підписів (ЕЦП). В той же час, «тіло» всіх файлів представляється байтами, як і елементи З, а тому актуальною і необхідною стає задача КП З (блоків), що враховують специфіку їх форматів, їх особливості. Серед публікацій, присвячених КП З, є низка робіт [1; 2; 3], що зорієнтовані суто на матричні моделі (ММ) і засоби паралельної обробки. Матричні афінні шифри (МАШ), їх ММ і різновиди, узагальнення до матричних афінно-перестановочних шифрів (МАПШ) з аналізом їх можливостей, переваг і застосувань досліджені та висвітлені у [1; 2]. Складовою багатокрокових МАПШ є ММ перестановок (ММ_П), які мають наочну простоту. Ці роботи спричинили активізацію досліджень і у напрямку створення ЕЦП, і протоколів узгодження матричних ключів (МК), і нових більш досконалих та експериментально більш досліджених модифікацій шифрів матричного типу (МТ) [3; 4] на низці З, але як окремих матриць, а не їх сукупностей, що обмежувало узагальнення, вимагало вирішення проблеми зменшення кількості матричних ключів (МК) при збільшенні їх розміру, вирішення задачі генерування під-ключів для ітераційних крокових чи циклових КП. Для шифрів з вищезгаданих робіт основними МК є матриці перестановок Р, їх низка, які з початкової їх множини чи з одного головного МК створені операціями над ними, як елементами у полі. Проте, як показано нами, КП З на

основі простих ММ_П не змінюють гістограми Z , ТГД, а запропоновані модифіковані ММ_П з декомпозицією бітових зрізів хоч і усувають цей недолік, потребують крім двох МК ще й двох векторних (ВК). В той же час для ІО, Z , файлів значного розміру є потреба окремо опрацьовувати їх блоки та ще й різними під-ключами P_i для збереження стійкості КП, а кількість узгоджених ключів максимально скоротити, аж до ГМК і в той же час розмір P значно збільшити для суттєвого зростання потужності множини можливих P_i , як МК. Тому актуальним є завдання пошуку подальших удосконалень, досліджень шифрів МТ, МАПШ, особливо на основі перестановок, з метою розширення їх ММ та застосувань на випадок поточкових (великоблокових) КП цілісних значних масивів, великорозмірних зображень, а також їх моделювання у програмному середовищі Mathcad з демонстрацією криптограм, їх гістограм, ентропій, що дозволить оцінити стійкість, деякі функціональні характеристики, особливості і сфери застосувань шифрів.

Виклад основного матеріалу, результатів дослідження. Огляд запропонованих багатофункціональних параметричних блочних МАПШ, їх підвидів векторних афінно-перестановочних шифрів (ВАПШ) показав, що для досягнення мети доцільно використовувати ізоморфність різних представлень перестановок (матриць чи векторів), що виступають у ролі головного та по-блокових, векторно-матричних ключів (ВМК) та не є скалярними. Сутність поблочних КП Z полягає в декомпозиції Z на блоки, наприклад, на 256-байтні вектори (в нашому експерименті рядки/стовбці Z 256×256 ел.) для першого випадку та блоки-матриці у вигляді чорно-білих Z такого ж розміру з кодуванням значень елементів байтами у другому випадку. Аналогічні підходи можна застосувати до «тіла» файлів любого типу з метою їх декомпозиції на блоки. Ми продемонструємо можливості застосування для цієї процедури різних програмних середовищ та інструментів. Деякі з можливих варіантів при використанні Mathcad для цих цілей показані на рис. 1-3.

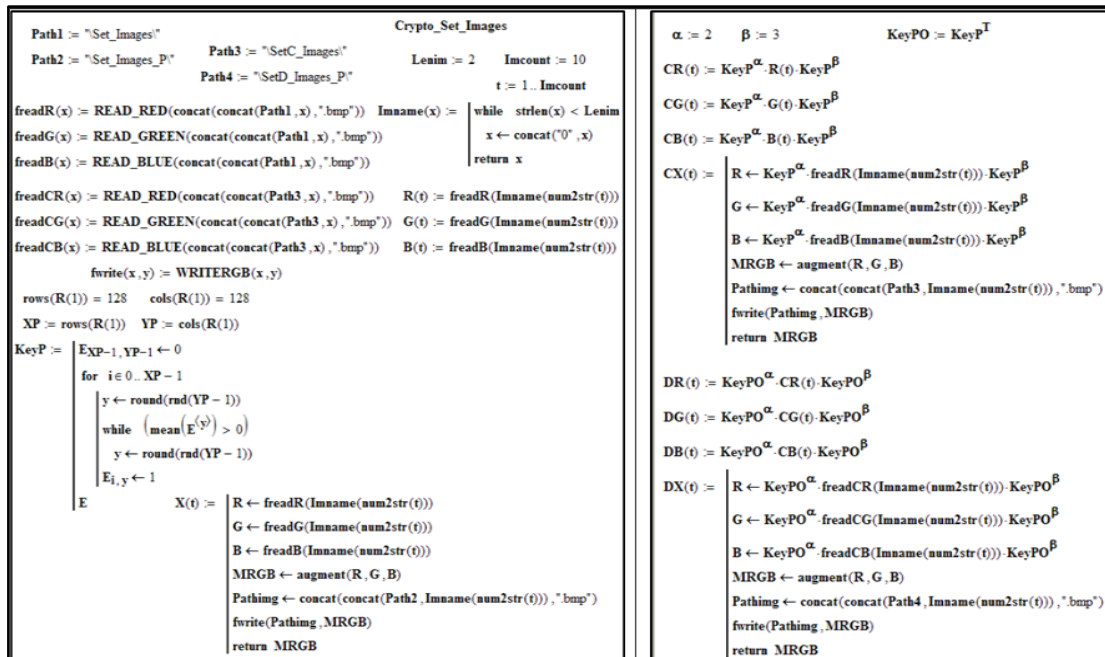


Рис. 1. Програмні модулі (вікно Mathcad) для моделювання блокових (сторінкових) КП кольорових зображень на основі ММ перестановок. Ліворуч: формування МК, спектральна декомпозиція-композиція, запис-читання. Праворуч: зашифрування, розшифрування, конкатенації для поєднання R,G,B, імен фреймів, їх введення-виведення (авторами створене).

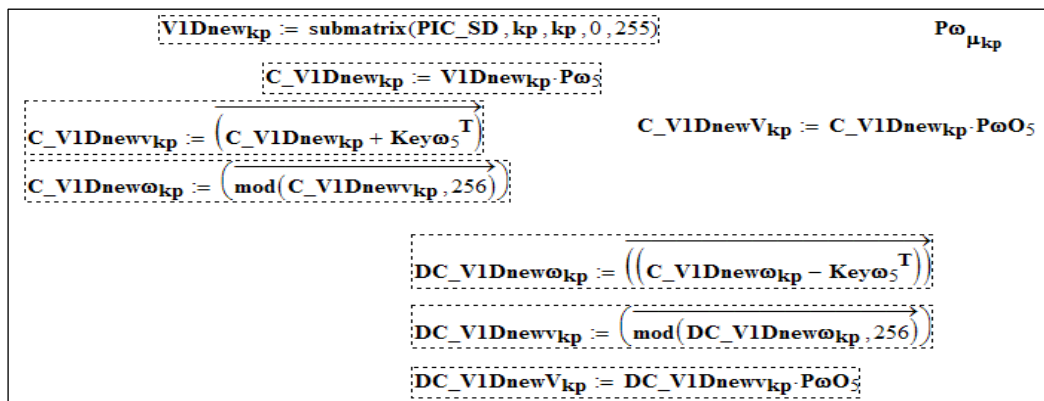


Рис. 2. Вікно Mathcad з формулами прямого та оберненого поблокового КП 3 на основі ВАПШ, де Key_w5 – векторний ПК, що відповідає перестановці Pw5. (авторами створене).

У першому випадку до кожного блоку для прямого та оберненого КП застосовувався ВАПШ, що є підвидом МАПШ, та один зі створюваних з головного ключа (ГК) під-ключів (ПК), що являють

собою матриці перестановок P (її степені!) чи ізоморфні їм вектори. Зазначимо, що 256-байтні вектори успішно можна представити з розміром 16×16 ел., тобто матрицею, розміри якої аналогічні розмірам матриці P . Спочатку виконується перестановка байтів блока, а потім тим же ПК (вектором) на основі ВАПШ адитивне (в загальному адитивно-мультиплікативне) КП байтів блока. Результати моделювання у Mathcad поблочних КП явних кольорових зображень PIC_SD (256×256 ел.) модифікованим ВАПШ показані на рис.2-3.

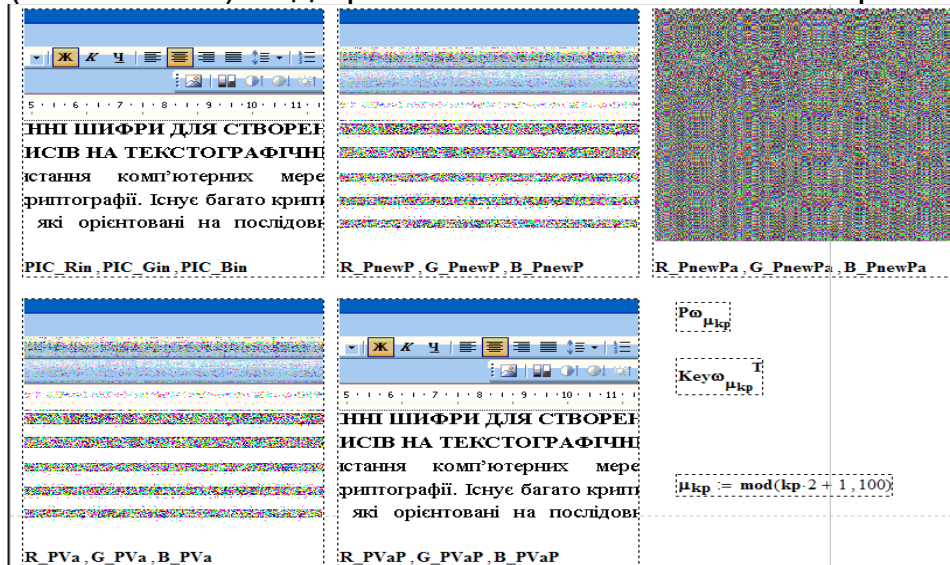


Рис. 3. Результати для випадку різних ПК для блоків (низка генерованих у потоці). Верхній ряд, зліва направо: явне, після перестановки (1-ий крок), криптограма після ВАПШ; Нижній ряд: відновлене проміжне та розшифроване зображення ТГД. (авторами створене).

Використовуючи формули для прямого та зворотного КП, кожен kp -ий блок з перетворювався у блоки проміжної, вихідної криптограм, відновлених з, а їх конкатенація за допомогою формул, створювала всі необхідні для контролю процесів КП кольорові зображення, дивись рис.3. Експериментом, аналізом ентропій і гістограм деяких ТГД (кольоровий малюнок з текстом на рис.3) та інших було встановлено, що для забезпечення крипто-стійкості та якості криптограм недостатньо лише одного адитивного афінного кроку та однакових ПК для всіх чи частини блоків, особливо для ТГД з малою кількістю значень рівнів у їх гістограмах, що видно і візуально. Та попри це ми експериментально довели, що використання низки ПК, які створюються з ГК, успішно вирішує цю проблему. Гістограми утворених криптограм, показані на рис. 3, підтверджують збільшення міри невизначеності (ентропії), практично аж до 7,5-7,8 біт.

Розвиваючи наш підхід ми показуємо, що для КП блоків довжиною 256×256 байтів, що представлені у вигляді матриці чорно-білого зображення, ми можемо переставляти всі байти у відповідності до МП, а перед тим чи після виконувати афінні перетворення. В цьому випадку МП в загально прийнятому вигляді повинна бути квадратною з $N \times N$ елементами («0» чи «1»), де $N=2^{16}$, або ізоморфним до неї N -компонентним вектором зі значеннями, закодованими двома байтами. Відмітимо, що потужність множини можливих таких МП, тобто їх кількість оцінюється, як $N!$, що дає для цього N колосальні значення. Суттєвим моментом тут є і той факт, що для по-компонентних матричних афінних КП потрібні дві (адитивна та мультиплікативна) аналогічного розміру випадкові матриці-ключі, тобто МК. Значить, замість них ми можемо застосувати два блоки (зображення), що ізоморфно представляють вищевказану, узгоджену секретну МП, як ключ. Тобто таке ізоморфне представлення МП дає нам можливість використати ці два З (складові KeyA та KeyB) у якості двох секретних МК загального типу, наприклад, як адитивний та мультиплікативний ключі у МАПШ чи іншій МАР. Результати КП МАПШ зображення (*Im*) за допомогою пропонованої МП та її складових, як ключів, що показані на рис. 4 з матрицями явного З (*Im*), проміжних, його криптограм (*Cmap*) та перевірних З свідчать про адекватну та якісну роботу наряду з гістограмами явного З, його криптограм після кожного КП афінними складовими цієї МП.

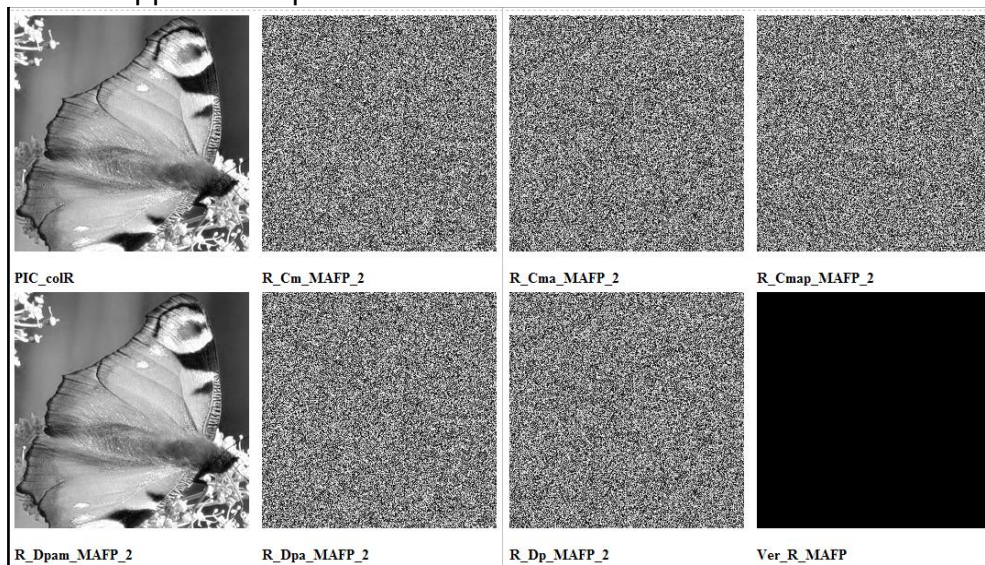


Рис. 4. Результати моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК. Верхній ряд, зліва направо: явне, після перетворень, криптограма після МАПШ; Нижній ряд: відновлене, проміжні та різницеве (праворуч) зображення ТГД. (авторами створене).

Ці модельні експерименти підтвердили, що КП МАПШ наявними 2-ма складовими МП дають якісні криптограми, гістограми яких настільки близькі до рівномірного закону розподілу, що навіть для 3 (*Im*) з ентропією 0,738 ентропія криптограм відрізняється від теоретично максимальної (8 біт) всього на соті долі відсотка, збільшуючись аж до 7,999.

Висновки. Моделювання підтверджують адекватність запропонованих блокових шифрів (МАПШ) з ізоморфними представленнями МП значних розмірностей та блоків та їхні гарні характеристики, їх переваги, в тому числі збільшення стійкості та розширення функціональних можливостей. Наочно показано низкою модельних експериментів процеси крипто-перетворень, генерування МП, головної МП та під-ключів, їх переваги. Моделі прості, зручні, адаптуються для різноформатних та кольорових зображень, реалізуються матричними процесорами, мають високі ефективність, стійкість, швидкодію.

Список літератури

1. Krasilenko V.G., Grabovlyak S.K. Matrix affine and permutation ciphers for encryption and decryption of images. *Systems of information processing*. - Kh., 2012. - Vol. 3 (101). - P. 53-62.

2. Krasilenko V.G., Nikitovich D.V. Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-map decompositions. *Computer-integrated technologies: education, science, production: sciences*. Journ. - Lutsk: LNTU, - 2016. - Vol. 23. - P. 31-36.

3. Красиленко В.Г., Нікітович Д.В. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал*. – Луцьк: ЛНТУ, 2017. – Вип. 26. – С 111-120.

4. Krasilenko V.G., Nikitovich D.V. Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity. *Electronics and Information Technologies*. - Lviv: National University, 2016. - Vol. 6. - P. 111-127. URL: http://elit.lnu.edu.ua/pdf/6_12.pdf