Міністерство освіти і науки України
Черкаська обласна державна адміністрація
Черкаський національний університет імені Богдана Хмельницького
Національна академія наук України
Національний авіаційний університет
Національний технічний університет України «КПІ»
Одеський державний екологічний університет
Одеський національний університет імені І.І.Мечнікова
Чернігівський національний технологічний університет
Jan Dlugosz University in Czestochowa
Wroclaw University of Science and Technology
Opole University

МАТЕРІАЛИ

другої міжнародної науково-практичної конференції

Інформаційні моделюючі технології, системи та комплекси

(ІМТСК-2020)

27-29 травня 2020 року
Черкаси, Україна

ЗМІСТ

Моделювання поблокових матричних афінно-перестановочних шифрів з ізоморфними представленнями блоків і ключів зображеннями

Красиленко В.Г., Нікітович Д.В. Вінницький національний технічний університет, Вінниця, Україна, krasvg@i.ua, nikitovych@i.ua

Modeling of blocked matrix affinity permutations ciphers with isomorphic block representations and key images

Krasilenko V., Nikitovich D. Vinnitsa National Technical University, Vinnitsa, Ukraine, krasvg@i.ua, nikitovych@i.ua

Abstract

First, we will give a brief overview of the proposed multifunctional parametric block MAPSs, their subspecies of vector affine permutation ciphers (VAPSs), and show that to achieve the goal it is advisable to use the isomorphism of various representations of permutations (matrices or vectors), which act as the main and block-wise, vector matrix keys. Modeling confirms the adequacy of the proposed block ciphers (MAPS) with isomorphic representations of the MP of significant dimensions and blocks and their good characteristics, their advantages, including increased stability and enhanced functionality. The processes of crypto-transformations, generation of MP, main MP and turn-key processes, their advantages are clearly shown by a number of model experiments. The models are simple, convenient, adaptived for multi-format and color images, implemented by matrix processors, have high efficiency, stability, and speed.

Розвиток електронних комунікацій, інформаційних технологій, стрімкий ріст об’ємів різноманітних чорно-білих, кольорових, багато-спектральних зображень (З), текстово-графічних документів (ТГД) з таблицями, формулами, малюнками, графіками, діаграмами, підписами, резолюціями, які є 2-D зображеннями, в тому числі і таких ТГД, які є конфіденційними або з обмеженим ступенем доступу, 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» любого файлу представляється байтами, як і елементи З, а тому актуальною і необхідною стає задача КП З (блоків), що враховують специфіку їх форматів, статистичні особливості. Серед значного числа публікацій, присвячених КП З, є низка робіт [1-3], що зорієнтовані суто на матричні моделі (ММ) і засоби паралельної обробки. Матричні афінні шифри (МАШ), їх ММ та різновиди, узагальнення до матричних афінно-перестановочних шифрів (МАПШ) з аналізом їх можливостей, переваг і застосувань досліджені, промодельовані та висвітлені у [1, 2]. Основною складовою цих і 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) [3-5] 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 в [3], КП З на основі простих ММ_П не змінюють гістограми З, 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, З, файлів значного розміру є потреба окремо опрацьовувати їх блоки та ще й різними під-ключами Рі для збереження стійкості КП, а кількість узгоджених ключів максимально скоротити, аж до ГМК і в той же час розмір Р значно збільшити для суттєвого зростання потужності множини можливих Рі, як МК. Тому актуальним є завдання пошуку подальших вдосконалень, досліджень шифрів МТ, МАПШ, особливо на основі перестановок, з метою розширення їх ММ та застосувань на випадок потокових сторінкових (по-блокових) КП цілісних значних масивів, кольорових великорозмірних зображень, а також їх моделювання у програмному середовищі Mathcad, демонстрація утворених криптограм, їх гістограм, ентропій, що дозволить оцінити стійкість, деякі функціональні характеристики, особливості і сфери застосувань шифрів.

Спочатку ми зробимо короткий огляд запропонованих багатофункціональних параметричних блочних МАПШ, їх підвидів векторних афінно-перестановочних шифрів (ВАПШ), та покажемо, 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 З полягає в декомпозиції З на блоки, наприклад, на 256-байтні вектори (в нашому експерименті рядки/стовбці З 256*256 ел.) для першого випадку та блоки-матриці у вигляді чорно-білих З 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, серед яких дуже зручним є використання Labview. Деякі з можливих варіантів при використанні Mathcad для цих цілей показані на рис. 1-2 та будуть обговорюватись у доповіді. 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 Р (її степені !) чи ізоморфні їм вектори. Зазначимо, що 256-байтні вектори успішно можна представити З розміром 16*16 ел., тобто Р 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.2-7. 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, що на рис. 3, створювала всі необхідні для контролю процесів КП кольорові зображення, дивись рис. 4, 5.

Експериментом, аналізом ентропій і гістограм деяких ТГД (кольоровий малюнок з текстом), З (метелик) 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, як видно з рис. 5, 7 використання низки ПК, що створюються з ГК, успішно вирішує цю проблему. Гістограми утворених криптограм, показані на рис. 5, підтверджують збільшення міри невизначеності (ентропії), практично аж до 7,5-7,8 біт.

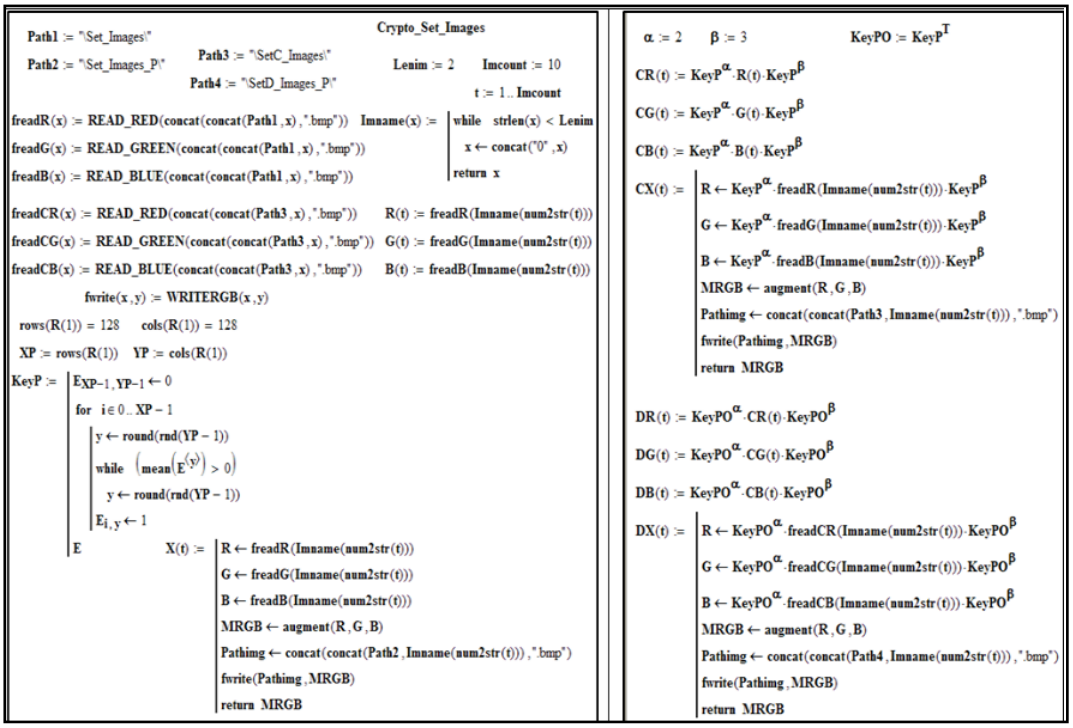

Рисунок. 1. Програмні модулі (вікна Mathcad) для моделювання блокових (сторінкових) КП кольорових зображень на основі ММ перестановок. Ліворуч:формування МК, спектральна декомпозиція-композиція, запис-читання. Праворуч: зашифрування, розшифрування, конкатенації для поєднання R,G,B, імен фреймів та їх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

Без знання ГК неможливо відновити З, і як було показано в [2], уже при розмірності ГК, рівній 32*32, можна забезпечити стійкість МАПШ моделей. Проте, не всі МП, наприклад, циклічного зсуву, а лише частка з їх множини відповідають вимогам. Якщо частка є навіть декілька відсотків, а потужність множини МП при N=32 оцінюється величиною 32!=1035, а вже при N=128 - величиною 128!=10215 , то оскільки в нас P має 256*256 а N=256, то ми маємо колосальне зростання оцінки потужності множини МП (P) аж до 256!, що дає запас.

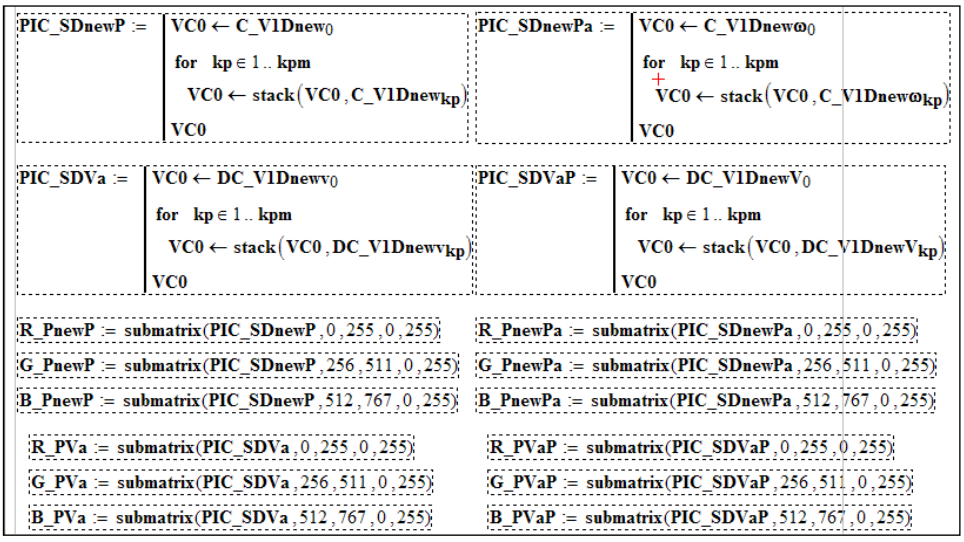

Рисунок. 2: Вікно Mathcad: Формули для конкатенації блоків, формування спектральних складових криптограми, відновлених розшифрованих З.

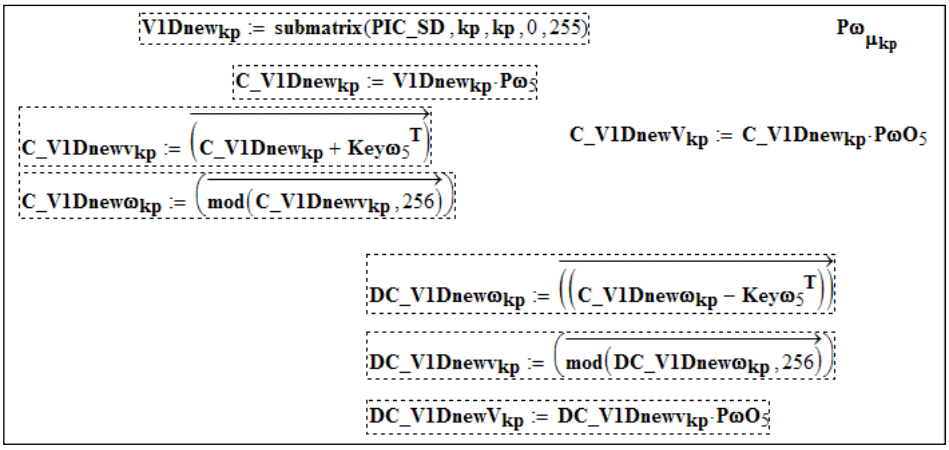

Рисунок. 3. Вікно Mathcad з формулами для прямого та оберненого по-блокового на основі ВАПШ КП З, де Keyw5 – векторний ПК, що відповідає матриці перестановок Pw5.

Розглянемо результати другого експерименту та 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, а потім чи до афінні перетворення. В цьому випадку МП в загально прийнятому вигляді повинна бути квадратною з N*N елементами («0» чи «1»), де N=216, 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. 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. Суттєвим моментом тут є і той факт, що для по-компонентних (Pixel-by-Pixel) 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 значної розмірності, як ключ.

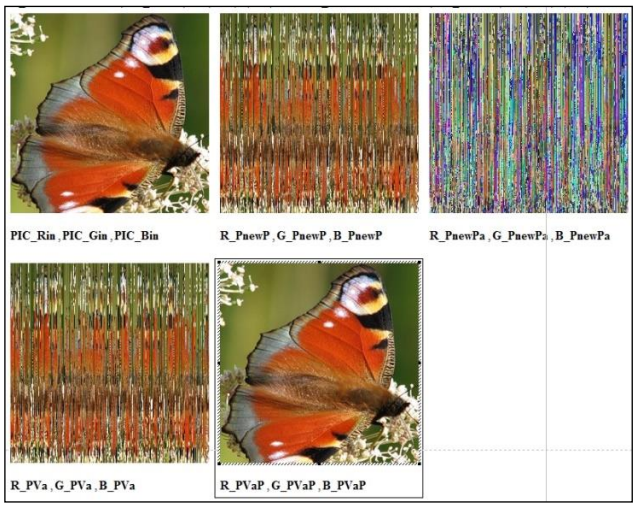

Рисунок. 4. Верхній ряд, зліва направо: явне, після перестановки (1-ий крок), криптограма після ВАПШ; Нижній ряд: відновлене проміжне та рівне явному розшифроване З.

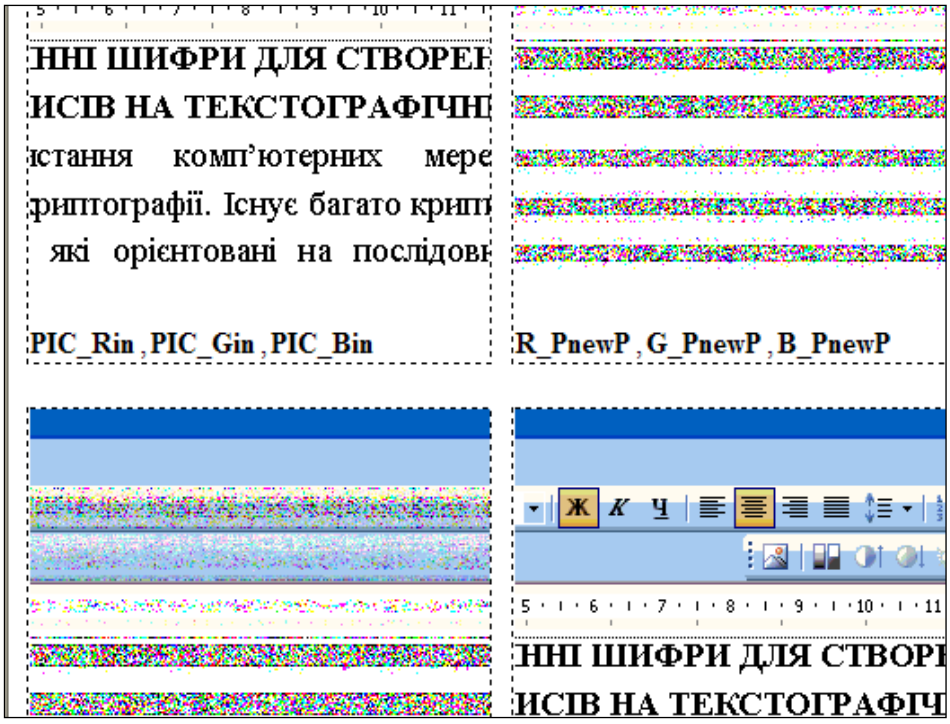

Рисунок. 5. Результати для випадку різних ПК для блоків (низка генерованих у потоці). Верхній ряд, зліва направо: явне, після перестановки (1-ий крок), криптограма після ВАПШ; Нижній ряд: відновлене проміжне та розшифроване зображення ТГД.

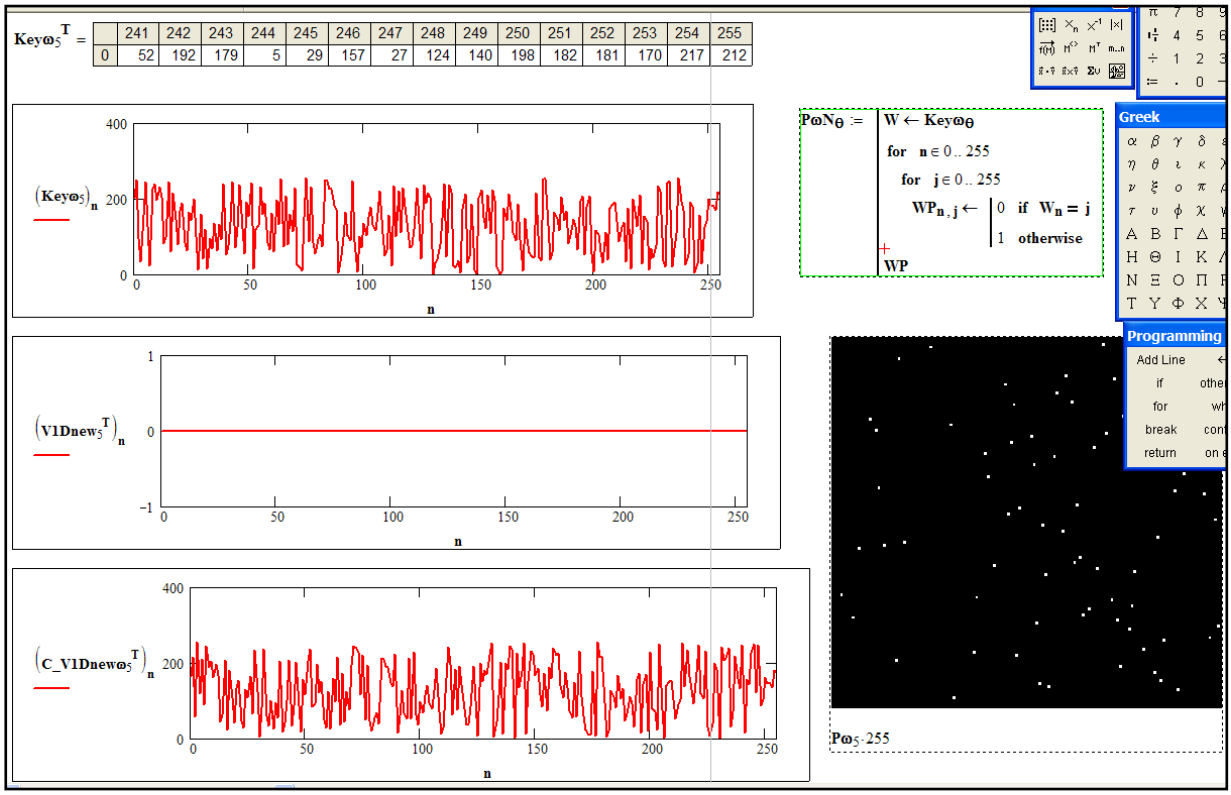

Рисунок. 6. Вигляд ПК у векторному цифровому (вгорі), графічному та матричному (праворуч матриця Pw5 з формулою ізоморфного переходу), вектора даних та його криптограми.

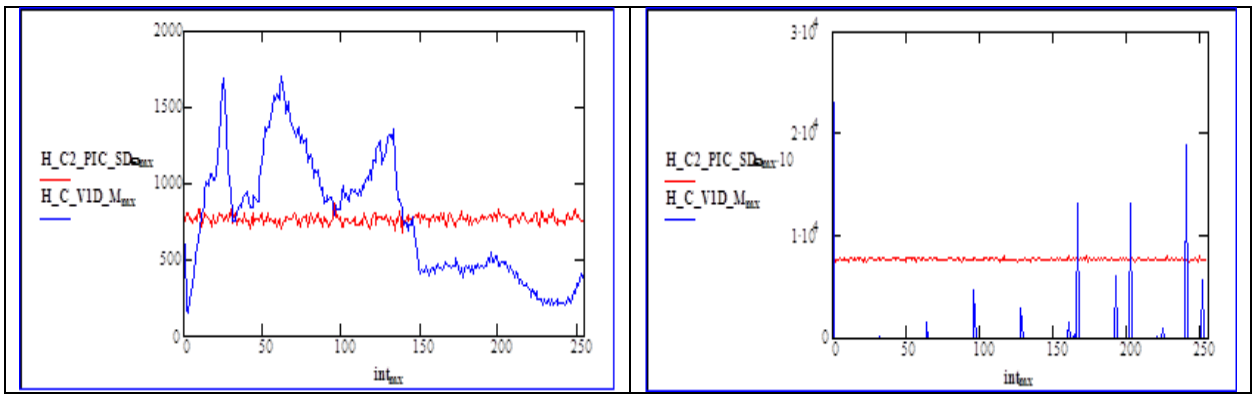

Рисунок. 7. Аналіз гістограм 1-го (метелик) та 2-го (ТГД) явних зображень (сині лінії) та гістограм їх криптограм (червоні лінії), що мають майже рівномірний розподіл!

Вигляд програмного модуля у Mathcad для генерування базового (головного) МК (МП) та вигляд його складових KeyA та KeyB у форматі двох чорно-білих зображень показано на рис.8. Отже, любу МП можна однозначно відобразити двома матрицями розміром 256*256, елементи яких приймають значення з діапазону 0-255, з тією особливістю, що кожна з 256 їх градацій інтенсивності в кожній з цих двох матриць (3) повторюється рівно по 256 раз.

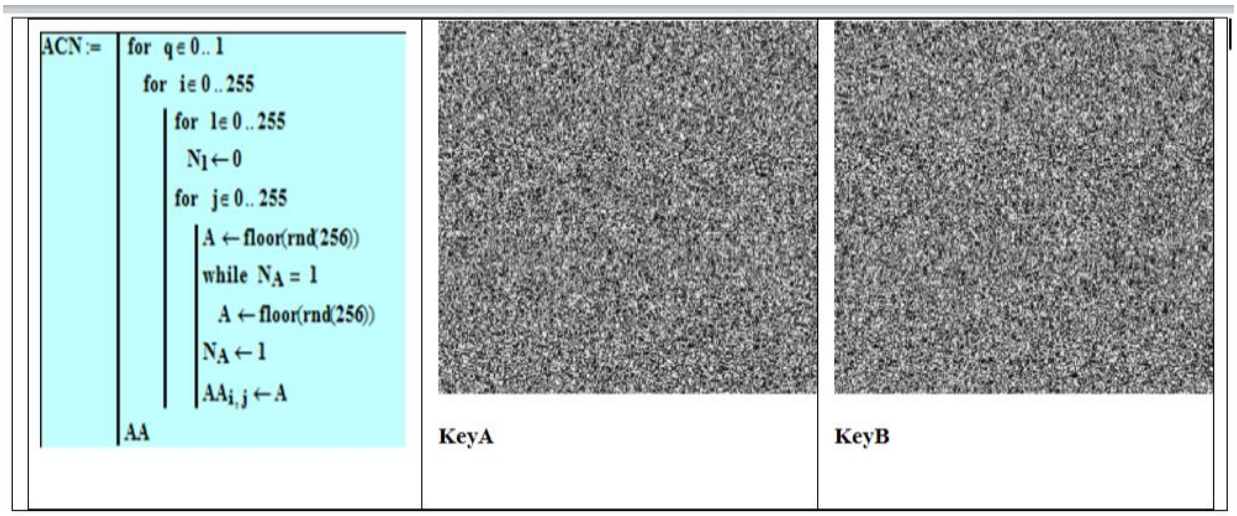

Рисунок. 8. Програмний модуль для генерування базового (головного) МК (МП) та вигляд складових KeyA та KeyB у форматі двох чорно-білих зображень (Вікно Mathcad).

Гістограми складових KeyA та KeyB МП зображені на рис.9 та мають вигляд горизонтальних ліній, як і очікувалось. Відмітимо, що таке ізоморфне у вигляді двох зображень представлення МП дає нам можливість використати ці складові KeyA та KeyB, про що вище згадувалось, у якості двох секретних МК загального типу, наприклад, як адитивний та мультиплікативний ключі у МАПШ чи іншій МАМ. Результати КП МАПШ зображення (Im) за допомогою пропонованої МП та її складових, як ключів, що показані на рис. 10 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, що зображені на рис.9.

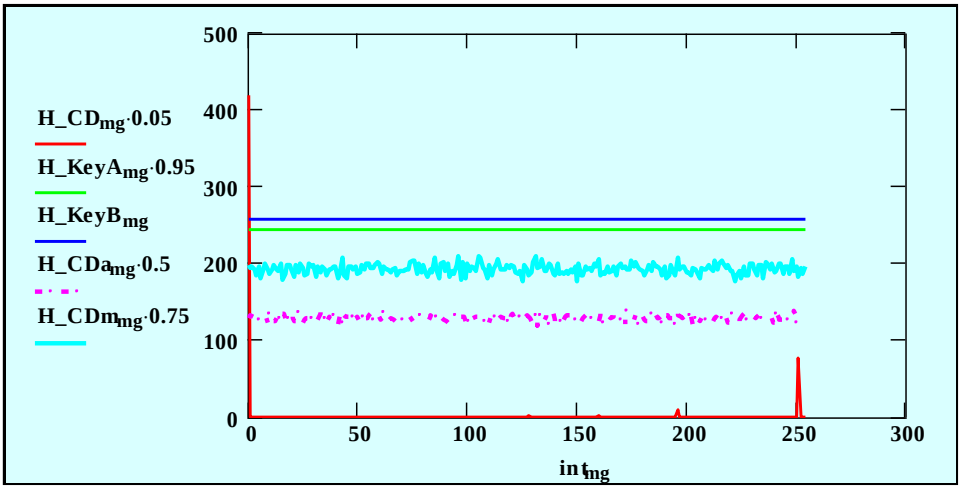

Рисунок. 9. Гістограми H_KeyA та H_KeyB відповідно складових KeyA та KeyB МП, гістограма H_CD криптограми явного З (співпадає з гістограмою З), відповідні гістограми H_CDa та H_CDm криптограм після адитивної та мультиплікативної афінних КП З за допомогою тих же KeyA та KeyB (Вікно Mathcad).

Ці модельні експерименти підтвердили, що КП МАПШ наявними 2-ма складовими МП дають якісні криптограми CD_ImAa та CD_ImAm, гістограми яких H_CDa та H_CDm настільки близькі до рівномірного закону розподілу, що навіть для З (Im) з ентропією 0,738 ентропія криптограм відрізняється від теоретично максимальної (8 біт) всього на долі відсотка, збільшуючись аж до 7,99. Результати моделювання МАПШ та багатокрокових МАПШ для різних випадків, коли спочатку виконуються складові афінних перетворень і у іншій послідовності та різними чи одним МК від МП, а потім перестановка за допомогою МП, чи навпаки, також засвідчили подібні якісні КП при застосуванні пропонованих ізоморфних представлень МП. Узагальнюючи наш підхід, можна стверджувати, що для синтезу ГМП зі ще більшою розмірністю останні можна також однозначно представити за допомогою 3, 4 і т.д. зображень-матриць чи блоків з байтів, аналогічних вищевказаним складовим KeyA та KeyB. Покращення всіх модифікацій МАМ при застосуванні саме таких (ізоморфно представлених З) МП забезпечується тим, що потужність множини МП оцінюється значною величиною N!=(256*256)!, крім того, є досить гарні перспективи швидких формувань похідних під-ключів, як елементів поля від узгодженої сесійної секретної ГМП. Тому, саме на ці аспекти будуть спрямовані наші подальші дослідження.

Використовуючи розроблені нами функціональні параметричні ММ МАПШ для КП З (блоків), у яких від деяких значень компонент векторного ключа залежать алгоритм та процес вибору-генерації під-ключів для поточних блоків і послідовність афінних і перестановочних кроків КП цього блоку, було виконано перевірку правильного до вимог синтезу ПК та адекватності різновидів моделей МАПШ шляхом прямого та зворотного КП З, що було частково показано вище та буде детально демонструватись у доповіді. Отримані результати підтвердили правильність концепції та досягнення більшої стійкості.

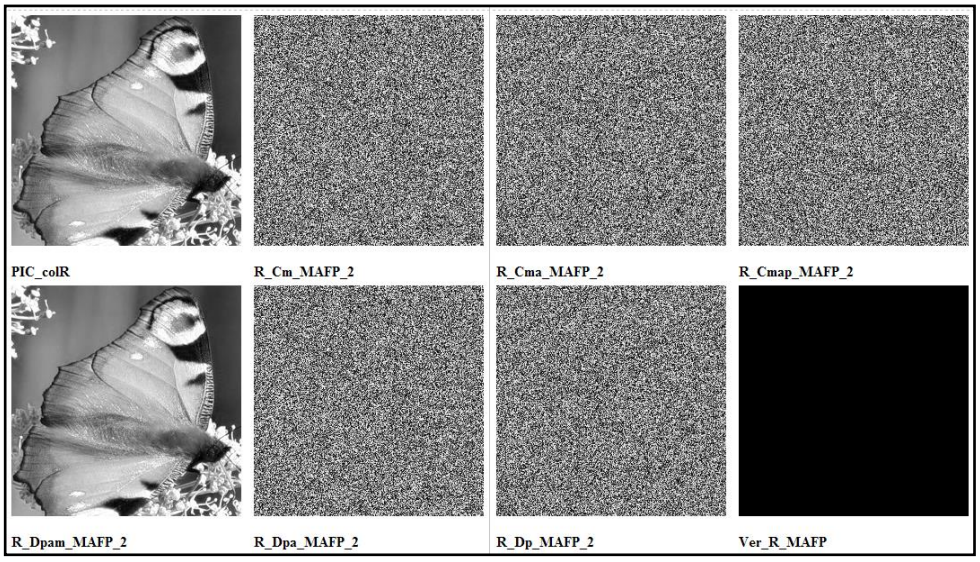

Рисунок. 10. Результати моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК. Верхній ряд, зліва направо: явне, після перетворень, криптограма після МАПШ; Нижній ряд: відновлене, проміжні та різницеве (праворуч) зображення ТГД.

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. 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.
2. Красиленко В.Г. Матричні афінно-перестановочні шифри для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. - Х.: ХУПС, 2012. – Вип. 3 (101).-т. 2. – С. 53-62.
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 Хмельницького НУ. Технічні науки. - 2014. - № 1. - С. 74 -79.
4. 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. - С. 151-157. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2017_3_32
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