Красиленко В. Г., к.т.н., с.н.с., доц.,
Нікітович Д. В.,
Вінницький національний технічний університет

ПОБЛОЧНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ВЕКТОРНИХ АФІННО-ПЕРЕСТАНОВОЧНИХ ШИФРІВ ТА ЇХ МОДЕЛЮВАННЯ

Вступ. Використання електронних комунікацій викликало гостру необхідність опрацьовувати, передавати специфічні текстово-графічні документи (ТГД) з таблицями, формулами, малюнками, графіками, діаграмами, підписами, резолюціями, які є 2-D зображеннями. Багато з них містять інформацію з обмеженим доступом, яку як звітність треба надавати у державні органи та засвідчувати їх цифровими підписами. Для цього використовуються методи криптографічних перетворень (КП) інформаційних об'єктів (ІО), зображень (З), шифри і протоколи формування для них ключів. Більшість КП зорієнтовані на послідовну скалярну обробку блоків ТГД. Поява паралельних алгоритмів та матричних багатопроцесорних засобів потребує створення і відповідних моделей матричного типу (МТ) для КП [1-3]. А тому **актуальним є завдання пошуку** нових матричних моделей (ММ) та засобів для КП З. Можливості запропонованих узагальнених матричних афінних шифрів (МАШ), матричних афінно-перестановочних шифрів (МАПШ) та їх переваги і застосування висвітлені у [1, 2]. Основною складовою останніх є матричні моделі перестановок (ММ_П), які мають наочну простоту. 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 матричних ключів (МК) ще й двох векторних (ВК). В той же час для ІО, З, файлів значного розміру є потреба окремо опрацьовувати їх блоки, а кількість та розміри ключів максимально скоротити, але без втрати стійкості КП. **Постановка задачі.** Таким чином є актуальною подальша модифікація відомих МАПШ, ММ_П для КП З з метою їх спрощення, покращення, розширення їх функціональних можливостей та перевірка нових шифрів, моделей шляхом моделювання останніх у програмному середовищі Mathcad та оцінювання якості, стійкості моделей.

Виклад основного матеріалу та результатів дослідження. Короткий огляд МТ шифрів, запропонованих багатофункціональних параметричних блочних шифрів [4], який ми зробимо спочатку, 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 З полягає в декомпозиції З на блоки, наприклад на 256-байтні вектори (в нас рядок З). До кожного блоку для прямого та оберненого КП застосовуємо векторний афінно-перестановочний шифр (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. Спочатку виконується перестановка байтів блока, а потім тим же ПК (вектором) на основі ВАПШ адитивне (в загальному адитивно-мультиплікативне) КП байтів блока. На рис. 1-4 зображені результати моделювання у Mathcad поблочних КП на основі модифікованих ВАПШ для деяких видів зображень.

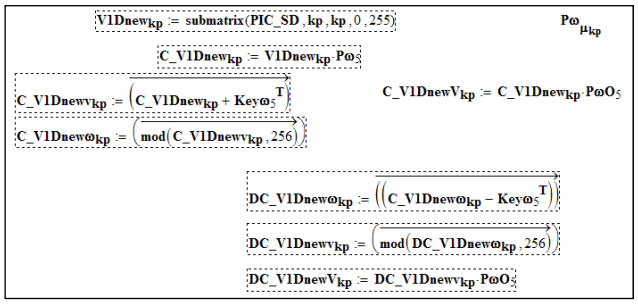

Рис. 1. Вікно Mathcad з формулами для прямого та оберненого по-блокового на основі ВАПШ КП З, де $Keyw_5$ – векторний ПК, що відповідає матриці перестановок Pw_5 .

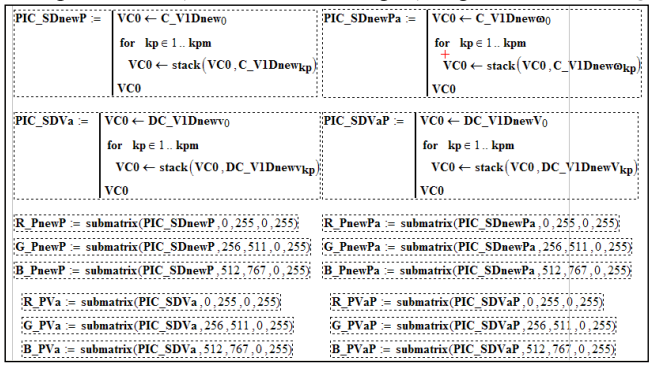

Рис. 2: Вікно Mathcad: Формули для конкатенації блоків, формування спектральних складових криптограми, відновлених розшифрованих З.

Використовуючи як явне кольорове зображення PIC_SD (256*256 ел.), дивись на рис.1 а, формули для шифрування і дешифрування, кожен *kp*-ий блок З перетворювався у блоки проміжної, вихідної криптограм,

відновлених З, а їх конкатенація за допомогою формул, що на рис. 2, створювала всі необхідні для контролю процесу КП кольорові зображення, дивись рис.3. Як видно, явне З після КП шифром дало якісну криптограму, ентропійно-гістограмний аналіз якої, про що буде доповідатись, підтвердив достатність для такого типу З навіть лише одного адитивного афінного кроку та однакових ПК для блоків. Проте, як видно нз рис. 4, 5 криптограми деяких ТГД при використанні одного ПК для всіх блоків є недостатніми по стійкості, що видно і візуально, та попри це низка ПК, що створюються з ГК, вирішує цю проблему.

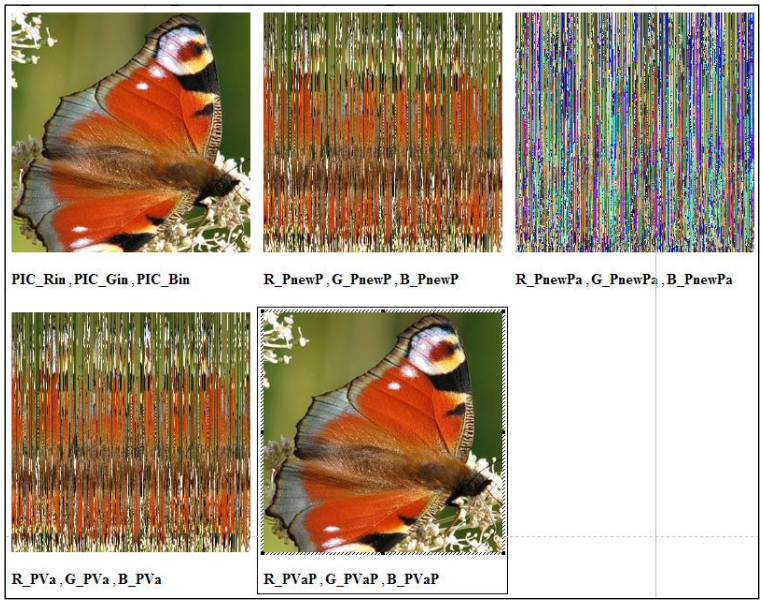

Рис. 3. Вікно Mathcad 1. Верхній ряд, зліва направо: явне, після перестановки (1-ий крок), криптограма після ВАПШ; Нижній ряд: відновлене проміжне та рівне явному розшифроване зображення.

Гістограми утворених криптограм, показані на рис. 6, підтверджують збільшення міри невизначеності (ентропії), практично аж до 7,5-7,8 біт. Без знання ГК неможливо відновити З, і як було показано в [2], уже при розмірності ГК, рівній 32*32, забезпечується на сьогодні стійкість МАПШ моделей, бо в нас Р має 256*256, а ВК має 256*8 біт!

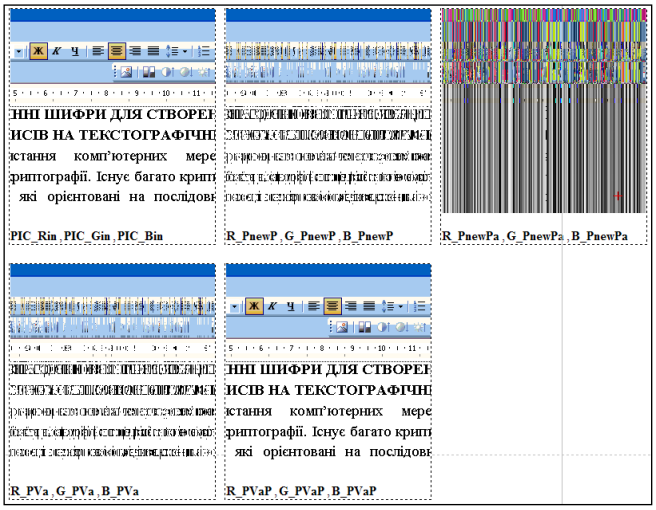

Рис. 4. Вікно Mathcad 2. Верхній ряд, зліва направо: явне, після перестановки (1-ий крок), криптограма після ВАПШ; Нижній ряд: відновлене проміжне та рівне явному розшифроване зображення ТГД.

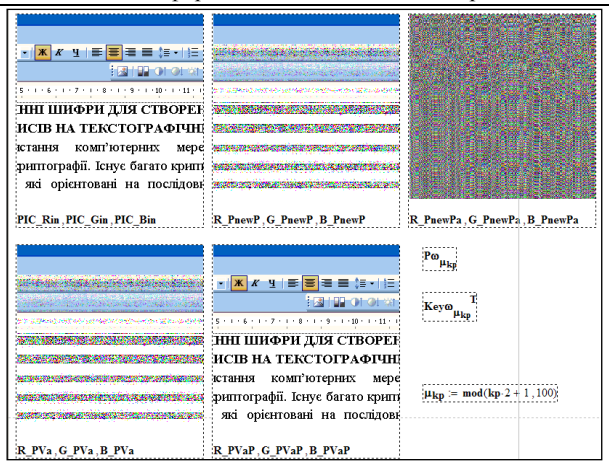

Рис. 5. Результати для випадку різних ПК для блоків (низка генерованих у потоці). Верхній ряд, зліва направо: явне, після перестановки (1-ий крок), криптограма після ВАПШ; Нижній ряд: відновлене проміжне та рівне явному розшифроване зображення ТГД.

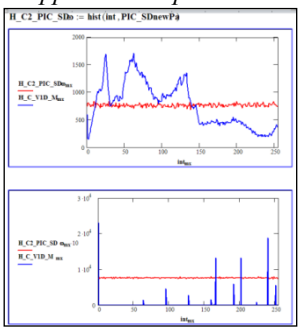

Рис. 6. Аналіз гістограм 1 та 2 явних З (сині лінії) та гістограм криптограм (червоні лінії), що мають майже рівномірний розподіл!

Висновки. Результати моделювання підтверджують адекватність запропонованих шифрів та їхні гарні характеристики. При цьому фактично ми використовуємо лише один 256*8=2024-бітний ключ, за допомогою якого формується низка необхідних якісних з точки зору стійкості ПК. Моделі реалізуються матричними процесорами та адаптуються для різноформатних та кольорових зображень, зручні для використання, мають високі ефективність, стійкість, швидкодію.

Література:

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