УДК 004.056.55

МОДЕЛЮВАННЯ МАТРИЧНИХ АФІННИХ ШИФРІВ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ЗОБРАЖЕНЬ

В.Г. Красиленко, *к.т.н., с.н.с., доц., проф.,* ***Д.В. Нікітович,*** *н.с.*
krasilenko@mail.ru

Розглянуто результати моделювання матричних афінних удосконалених шифрів для крипто-перетворень чорно-білих та кольорових зображень зі зменшеною вдвічі кількістю матричних ключів. На основі експериментів у Mathcad з різними зображеннями показано, що запропоновані модифікації таких шифрів є зручними для використання та дозволяють навіть збільшити їх крипто-стійкість і функціональні можливості

Krasilenko V.G., Nikitovich D.V. Considered the results of the simulation of superior matrix affine ciphers for crypto-transformation gray-scale and color images with the twice reduced set of matrix keys. Based on experiments in Mathcad with various images show, that the proposed modifications of these ciphers are convenient to use and allow even increase their crypto-stability and functionality.

Ключові слова: МАТРИЧНИЙ АФІННИЙ ШИФР, КРИПТО-ПЕРЕТВОРЕННЯ ЗОБРАЖЕНЬ, МАТРИЧНІ КЛЮЧІ.

Keywords: MATRIX AFFINE CIPHER, IMAGES CRYPTO-TRANSFORMATIONS, MATRIX KEYS.

Вступ, огляд, аналіз публікацій та постановка проблеми. Для захисту цілісності інформаційних об’єктів (ІО) та їх стійкості до потенційних загроз застосовують криптографічні методи та засоби. Зростає доля специфічних ІО у вигляді малюнків, діаграм, підписів, резолюцій, які є зображеннями і які потрібно передавати чи засвідчувати їх цифровими підписами. Більшість методів, моделей та засобів криптографічних перетворень (КП) ІО чи зображень, протоколів формування ключів зорієнтовані на послідовну скалярну обробку блоків. Поява паралельних алгоритмів і матричних процесорів, сприяла переорієнтації КП

на ці засоби та створенню моделей матричного типу (МТ) [1-4]. У роботі [1] були продемонстровані переваги КП моделями МТ на основі узагальнених матричних афінних шифрів (МАШ), а в [2] показані можливості створення на їх основі сліпих цифрових підписів. Ще більш узагальнені матричні афінно-перестановочні шифри були досліджені в [3], а в [4] МАШ були застосовані для КП кольорових зображень. Алгоритми формування матричних ключів (МК) для таких моделей МТ, МАШ та КП зображень на їх основі наведені в [5]. Проте недолік МАШ та їм подібних полягає у необхідності застосування як мінімум 2-ох МК, якщо реалізувати у моделі МТ і мультиплікативну і адитивну матричну складові. Тому удосконалення МАШ, направлені на зменшення кількості МК при збереженні стійкості та інших характеристик матричних моделей (ММ), їх експериментальна перевірка на різних зображеннях є актуальним завданням. ***Метою роботи*** є дослідження та моделювання таких модифікацій МАШ з метою їх використання для КП зображень.

Моделювання *МАШ* проводилось у Mathcad з використанням зображень (З) різної розмірності. Процес КП 2-ох З (256*256 ел.) з М-ключом Key_GC показано на рис. 1. Ліворуч у 1, 2-у рядах криптограми, у центрі – розшифровані, вони ж початкові, праворуч – різницеві (нульові). На рис.2 показано одне з вікон з

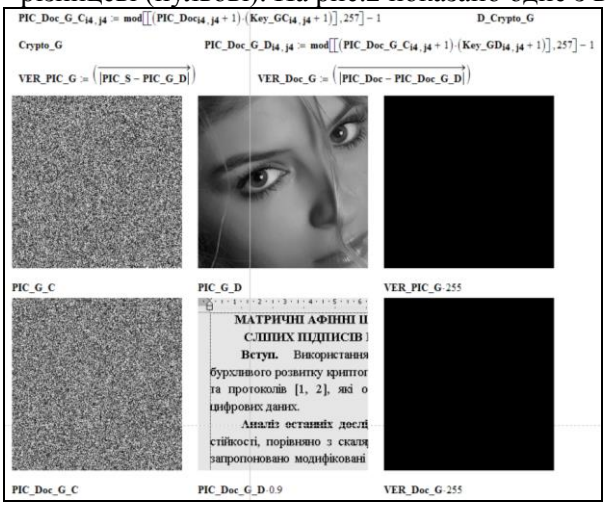

Рис. 1. Результати моделювання МАШ для 2-ох зображень.

формулами, що були використані для генерування ключів, прямих та обернених до них за модулем 257, зашифрування та розшифрування кожної R,G,B_pic складової З (600*549 ел.) трьома МК Key_C_(R,G,B) та Key_D_(R,G,B) відповідно.

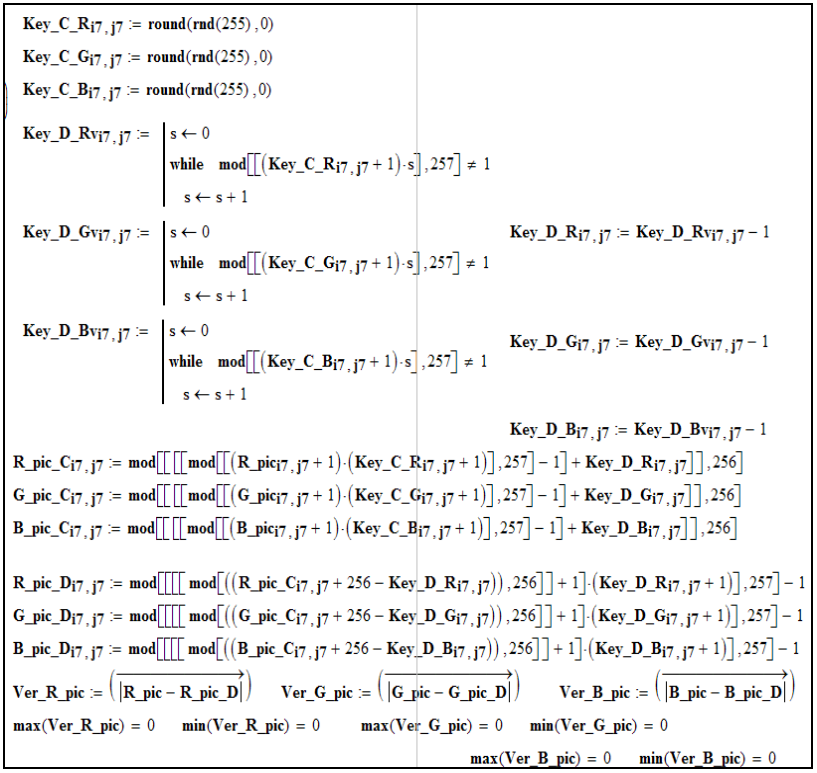

Рис. 2. Вікно з формулами для КП кольорового зображення.

На рис. 3 показані результати КП на основі МАШ лише з одним МК для кожної складової: кольорові вихідне З, МК (1ряд, праворуч), криптограма (2 ряд, ліворуч) та розшифроване З. Тут зауважимо, 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 до прямого за модулем є по суті адитивною складовою МАШ. Використання скалярних ключів та процедур по-елементного піднесення у степінь за модулем

кожного МК дає реалізацію багатокрокових МАШ **[1-3].** З урахуванням обмежень для тез низку інших експериментів ми тут не демонструємо.

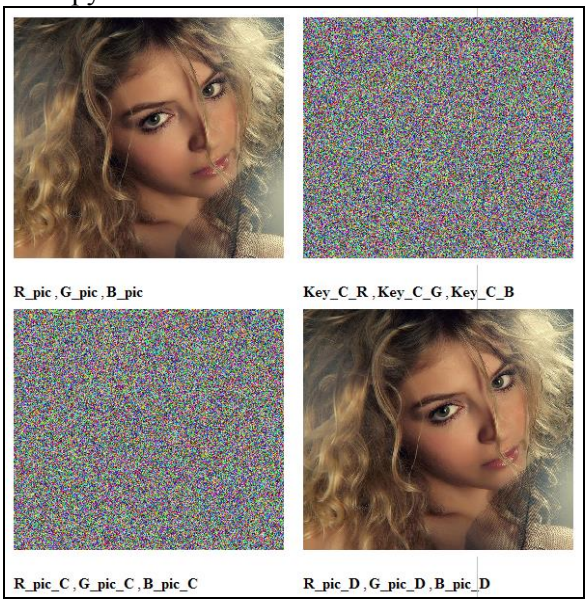

Рис. 3. Фрагмент вікна Mathcad з результатами КП зображення.

Висновки. Моделювання підтвердили правильну роботу моделей та удосконалень матричних афінних шифрів.

Література

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка» «Комп'ютерні системи та мережі», 2009 - № 658. – С. 59-63.
2. 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.
3. 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.
4. 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. наук.-пр. конф. – К., 2010. – С.120-124.
5. 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.