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

МОДЕЛЮВАННЯ СТОРІНКОВИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ МАСИВІВ КОЛЬОРОВИХ ЗОБРАЖЕНЬ НА ОСНОВІ МАТРИЧНИХ МОДЕЛЕЙ ТА ПЕРЕСТАНОВОК

Вступ, аналіз останніх досліджень, публікацій. В епоху сучасних електронних комунікацій, інформаційних технологій стрімко виросли об'єми різноманітних чорно-білих, кольорових, багато-спектральних зображень (З), текстово-графічних документів (ТГД), в тому числі і таких, які є конфіденційними або з різним ступенем обмеження доступу. Тому для їх безпечного зберігання, передачі, для створення, наприклад, електронних цифрових підписів (ЕЦП), засвідчення звітів, ТГД підписами відповідальних осіб, нотаріусів, є необхідність у криптографічних перетвореннях (КП) З, ТГД, масивів даних у різних форматах. В той же час, «тіло» любого файлу представляється байтами, як і елементи З, а тому актуальною і необхідною стає задача КП З, що враховують специфіку їх форматів, статистичні особливості. Суттєвий ріст числа публікацій, присвячених КП З, поява робіт [1-3], що зорієнтовані на матричні моделі (ММ) і засоби паралельної обробки, спричинили активізацію досліджень і у напрямку створення ЕЦП, і протоколів узгодження матричних ключів (МК), і нових модифікацій шифрів матричного типу (МТ) [4-8]. Матричні моделі (ММ) запропоновані в [1], а матричні афінні шифри (МАШ) та сліпі ЕЦП на їх основі в [2], які пізніше були узагальнені до багатокрокових матричних афінно-перестановочних шифрів (МАПШ) у роботі [3], де були розроблені, досліджені і промодельовані на зображеннях їх ММ. Пізніше вони були удосконалені, модифіковані та експериментально більш досліджені в [4-8] на низці З, але як окремих матриць, а не їх сукупностей, що обмежувало узагальнення, вимагало вирішення проблеми зменшення кількості матричних ключів (МК) та їх розміру, генерування під-ключів для ітераційних крокових чи циклових КП. Для шифрів з вищезгаданих робіт матриці перестановок **P**, їх низка, що створені операціями над ними, як елементами у полі, є основними МК. **Постановка задачі.** Тому **метою** роботи є подальше **вдосконалення**, дослідження шифрів МТ, МАПШ, особливо на основі перестановок, з метою **розширення** їх ММ та застосувань на випадок потокових сторінкових (блокових) КП цілісних масивів кольорових зображень, а також їх моделювання у Mathcad, демонстрація утворених криптограм, їх гістограм, ентропій, що дозволить оцінити стійкість, деякі характеристики, особливості і сфери застосувань таких шифрів.

Виклад основного матеріалу, результатів дослідження. Для моделювання ми використовували масив кольорових З різної розміру, ТГД розмірністю 704 × 572 елементи та формату А4. А для демонстрації, з урахуванням обмежень на обсяг тез, ми тут наводимо результати моделювання процесів КП масиву кольорових З, як блоків (сторінок) з розміром 128*128 ел. Відмітимо, що, з урахуванням 3-байтного представлення пікселів З такого розміру, блок (чи фрейм) має 384К бітів, тобто це порядки більше розмірів блоків у відомих шифрах. Крім того, для забезпечення необхідної стійкості потужність множини перестановок (МК) з такими розмірами буде зі значним запасом, бо пропорційна 128!, якщо навіть доля підходящих на рівні 1% від усіх можливих, дивись [3]. Нами було показано, що введення додаткових скалярних ключів, що використовуються як степені для піднесення матриць перестановок **P** у ці степені, можна легко створити низку похідних перестановок, використання яких суттєво розширює можливості для покращення якості, стійкості крипто-перетворень. Програмні модулі та результати моделювання показані на рис. 1-4.

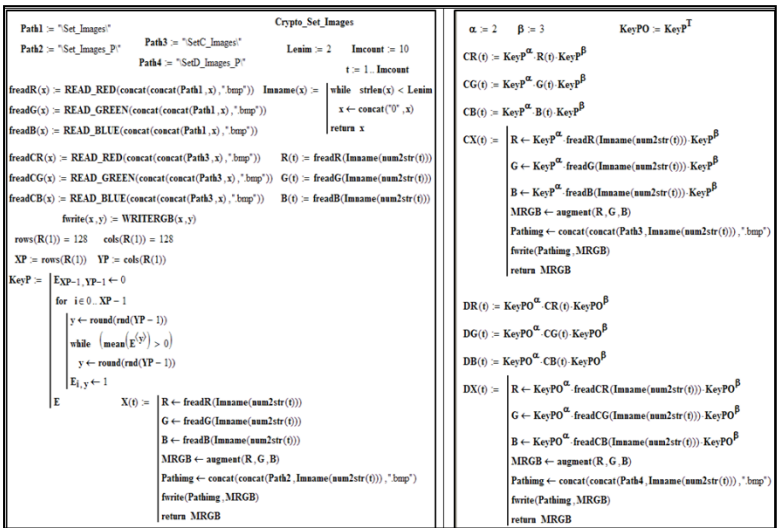

Рис.1 Програмні модулі (вікна Mathcad) для моделювання блокових (сторінкових) КП кольорових зображень на основі ММ перестановок. Ліворуч:формування МК, спектральна декомпозиція-композиція, запис-читання. Праворуч: зашифрування, розшифрування, конкатенації для поєднання R,G,B, імен фреймів та їх введення-виведення.

Основна концептуальна ідея параметричних процедур генерування низки МК базується на використанні додаткових векторних ключів (ВК) в якості параметрів, що впливають на степені матриць **P** та МК у моделях їх матричного множення чи піднесення у степінь, вид та розмір **P** чи їх блоків. На кожному ітераційному кроці в

залежності від ВК формуються різні МК. Процедури генерування послідовностей матриць **P** за відповідними погодженими сторонами ВК будуть розглянуті у доповіді наряду з протоколом узгодження головного МК. Узгодження МК загального типу розглядались у [9], а тому будуть висвітлені та продемонстровані лише у доповіді. Крім того, ми розглянемо як перестановки можуть використовуватись не лише для перемішувань елементів та блоків масивів, а й для заміни байтів, слів.

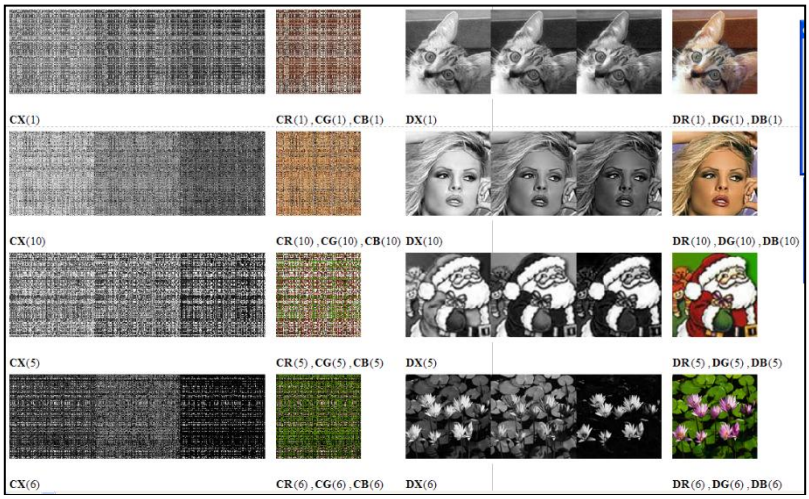

Рис.2. Результати моделювання. Утворені кольорові криптограми, їх R,G,B спектральні складові для кольорових зображень та відповідні їм розшифровані кольорові зображення та їх складові

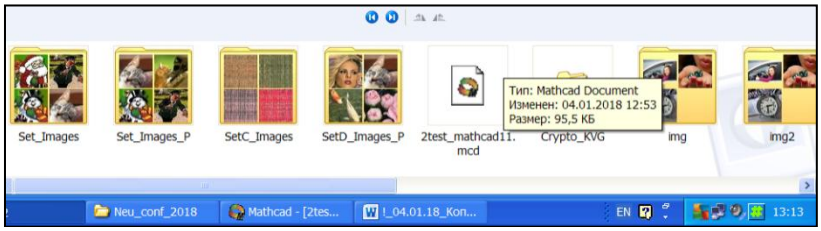

Рис.3. Результати моделювання: Набори сторінок (папки) явних зображень, відповідних їм криптограм, розшифрованих зображень, що демонструють правильну роботу ММ КП потокового (сторінкового) типу.

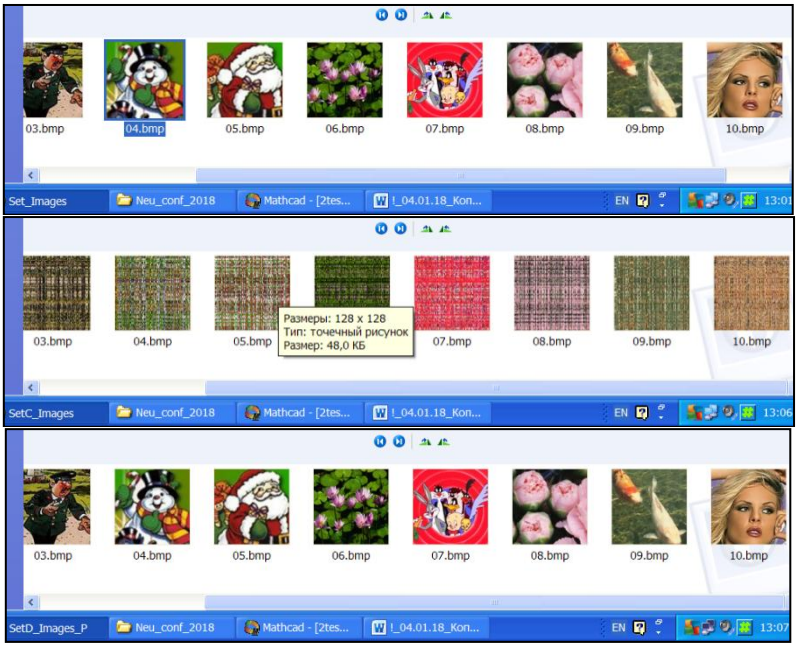

Рис.4. Матриці-зображення, що формувалися в експериментах (Mathcad), як сторінки (блоки) та підтверджують правильну роботу прямого та оберненого процесів КП ММ потокового (сторінкового) типу: Набори явних зображень, відповідних їм криптограм, розшифрованих зображень.

Висновки: Виконана демонстрація функціональних можливостей сторінкових (блокових) криптографічних перетворень масивів кольорових зображень на основі матричних моделей, матричних афінно-перестановочних

шифрів та матриць перестановок, як ключів. Наведені результати моделювання у Mathcad процесів прямих та обернених КП масивів великоформатних З, підтвердили адекватність, достовірне функціонування ММ, їх кращі гістограмно-ентропійні, часові характеристики (показано збільшення ентропії до 7,98 біт/ел.).

Список літератури

1. *Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. нац. ун-ту "Львів. політехнік".- 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 алгоритми для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. - 2012. - Вип. 3(2). - С. 53-61. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15*
4. *Красиленко В.Г. Удосконалення та моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології: збірник наукових праць. – Львів: Львівський національний університет імені Івана Франка, 2017. – Вип. 7. – С 20-42. – Режим доступу: http://elit.lnu.edu.ua/issue.php?lang=&number=7*
5. *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 національного університету. Технічні науки. - 2014. - № 1. - С. 74-79.*
6. *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*
7. *Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво : наук. журн. – Луцьк: Видавництво Луц. нац. техн. ун-т., - 2016. - № 23. - С. 31-36. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/132/section/9*
8. *Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень з верифікацією цілісності криптограм на основі матричних моделей перестановок/ В.Г. Красиленко, Д.В. Нікітович// Матеріали НПК «Проблеми моделювання та розроблення інформаційних систем». – Дрогобич : ДДПУ ім. І. Франка, 2016. – С. 128-136.*
9. *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 (149). – С 151-157.*