дополнительного параметра a, изменение которого возможно в пределах малого отклонения от значения 3,9.

Результаты проверки работоспособности различных генераторов хаоса показали, что в пределах одного миллиарда формируемой числовой последовательности $\{x_i\}$ периодичность не была обнаружена.

Выводы. Предложенный метод WEP-шифрования на основе динамического хаоса предотвращает процесс повторения гамма-последовательности. Обеспечивается это за счет инициализации нового внутреннего состояния генератора хаоса через интервалы, не превышающие 2^w комбинаций, где w - длина ключа. Выбор значений ключей w_i по параметрам генератора a_i и x_i дает неограниченную возможность по созданию новых траекторий хаотического процесса, что является одним из важных условий генерирования гамма-последовательностей с большим периодом. Это обеспечивает существенное снижение уязвимости радиосетей стандарта IEEE 802.11.

Список литературы

1. Лунтовський А.О. Мультисервісні мобільні платформи / А.О. Лунтовський, М.В. Захарченко, А.І. Семенко – К.: ПВП «Задруга», 2014. – 214 с.
2. Шахтарин Б.И. Генераторы хаотических колебаний / Шахтарин Б.И. – М. : Гелиос АРВ, 2007. – 248 с.
3. Корчинський В.В. Підвищення прихованості передачі в системі зв'язку з кодовим розділенням каналів на основі динамічного хаосу / В. В. Корчинський, В. Й. Кільдішев // Матеріали міжнародної наук.-практ. конф. [«Перспективні напрями захисту інформації – 2017»], (Київ, 25-26 травня 2017 р.) – Київ: «Державна служба спеціального зв'язку та захисту інформації України»: 2017 р. – Вип. 19. – С. 48.

Красиленко В.Г., Нікітович Д.В.
Вінницький національний технічний університет

МОДЕЛІ БЛОКОВИХ МАТРИЧНИХ АФІННО-ПЕРЕСТАНОВОЧНИХ ШИФРІВ (МАПШ) ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ТА ЇХ ДОСЛІДЖЕННЯ

*Анотація. В роботі запропоновані та промодельовані нові параметричні матрично-алгебраїчні моделі (МАМ) блокових МАПШ для КП, в тому числі зображень. Результати їх моделювання на прикладі прямих та обернених КП зображень свідчать про їх коректну роботу, зручність (лише матричні процедури та 1 МК, параметричне по суті управління перестановками байтів у матрицях-блоках та при формуванні ключів), адаптованість до форматів, багатофункціональність (поєднання операцій створення та обробки блоків, афінних перетворень байтів у блоках з процесом утворення поточних блокових ключів, взаємозамінність циклових ітераційних процедур та матричних піднесень у степінь), ефективність (орієнтація на матричні процесори). Розглянуті різновиди блокових МАПШ, матричних алгебраїчних КП процедур на основі операцій за модулем і параметричних процедур синтезу необхідних матричних ключів (МК). Показані експерименти зашифрування та розшифрування чорно-білих та кольорових зображень (256*256 елементів) і текстово-графічних документів (ТГД) у програмному середовищі Mathcad.*

Вступ, аналіз досліджень і публікацій, визначення мети та завдань. Розвиток інформаційних технологій, електронних та мережних комунікацій за умов супутнього зростання кількості інформаційних загроз і вразливості ресурсів потребує вирішення проблем інформаційної безпеки та захисту інформації державного, комерційного та приватного змісту. Одним з напрямків вирішення цих проблем є застосування криптографії. Як показує аналіз відомих типових криптографічних систем і алгоритмів, більшість з них

орієнтовані на послідовну обробку скалярних даних чи у кращому випадку блоків, довжина яких не перевищує 256 бітів (AES, тощо), і лише для найновіших їх версій може досягати 1024 біти. Для багатьох задач, наприклад, розпізнавання та біометричного контролю, електронного підписування, необхідно здійснювати криптографічні перетворення (КП) над багатовимірними сигналами, серед яких є напівтонові та кольорові зображення чи інша конфіденційна інформація (підписи, візи, резолюції) на текстово-графічних документах (ТГД). Поява паралельних алгоритмів, а особливо матриць багатопроцесорних засобів, потребує створення відповідних матрично-алгебраїчних моделей (МАМ), систем матричного типу (МТ) для КП. Переваги КП ТГД, чорно-білих, кольорових зображень (З) узагальненими матричними афінними і афінно-перестановочними шифрами (МАПШ), в тому числі при створенні сліпих цифрових підписів були продемонстровані у роботах [1-4]. Їх базовими операціями є по-елементні множення, додавання за модулем матриць та матричні моделі перестановок (ММ_П) з процедурами множення матриць. Але недоліком цих робіт є значні розміри матричних ключів (МК) і відсутність демонстрації їх ефективної роботи з блоками у вигляді матриць, на які розбиваються багатосторінкові дані. У деяких МАМ на основі ММ_П необхідні декомпозиція біт-зрізів та крім 2-х МК ще й два векторних (ВК) для збільшення ентропії та зміни гістограми З при їх КП [5-6]. Перспективність МАМ та їх модифікацій для КП засвідчується можливістю перевіряти цілісність (Ц) криптограм зображень та наявність у них перекручувань, дивись [7-8], збільшенням крипто-стійкості та розширенням їх функціональності при збереженні уніфікованих матричних операцій, процедур навіть для дуже специфічних (з характерними гістограмами) сканованих ТГД, як експериментально показано в [9]. Узагальнення МАМ до матрично-блокового виду є необхідними з точки зору універсальності блокових алгоритмів та незалежності від об’ємів даних. Тому удосконалення МАПШ, направлені на зменшення кількості МК при збереженні стійкості та інших характеристик матричних моделей (ММ), їх експериментальна перевірка на різних зображеннях є актуальним завданням. Таким чином, **метою роботи** та актуальною є розробка блокових модифікацій МАПШ з щонайменшою довжиною 2048 бітів, з можливістю вибору його параметрів і циклових чи блокових ключів аналогічної довжини, їх моделювання на реальних інформаційних об’єктах (ІО) та демонстрація, оцінювання їх переваг, характеристик та стійкості, можливостей застосувань.

Виклад матеріалу та результатів дослідження. Пропонований алгоритм КП при зашифруванні складається з таких етапів: 1) розбиття ІО (З) на блоки (Б) у вигляді матриць з розмірністю 2^m*2^m, де m=4, 5, 6,… та з елементами-байтами у цифровому форматі, що при m=4 еквівалентно довжині блока 256*8=2024 бітів, 2) перестановка байтів кожного поточного Б за допомогою поточного ключа (ПК), що формується синхронно як степінь з головного у відповідності до параметричної моделі, аргументом якої є індекс Б, 3) матричні афінні чи афінно-перестоновочні перетворення (МАПП) матриць байтів Б поточними ключами, тими ж, що на етапі 2 чи аналогічними, але по іншій параметричній моделі, 4) конкатенація отриманих блоків для формування криптограми ІО. Процес розшифрування має етапи: 1) розбиття криптограми на Б, 2) обернені МАПП блоків на основі обернених поточних ключів, 3) обернені перестановки байтів Б поточними ключами (оберненими), 4) конкатенація перетворених блоків у відновлений ІО. Моделювання блокових МАПШ проводилось у Mathcad з використанням чорно-білих та кольорових зображень (З) різної розмірності для наглядної демонстрації. Вікна Mathcad з формулами для моделювання КП зображень алгоритмом блокового МАПШ для 2-ох чорно-білих З (256*256 ел.) з М-ключом M_V (КРХ) показані на рис. 1, а на рис.2 показані результати КП та вигляд ключів, блоків до і після КП, різницеві верифікаційні матриці-блоки. Результати КП цих З зображені на рис.3.

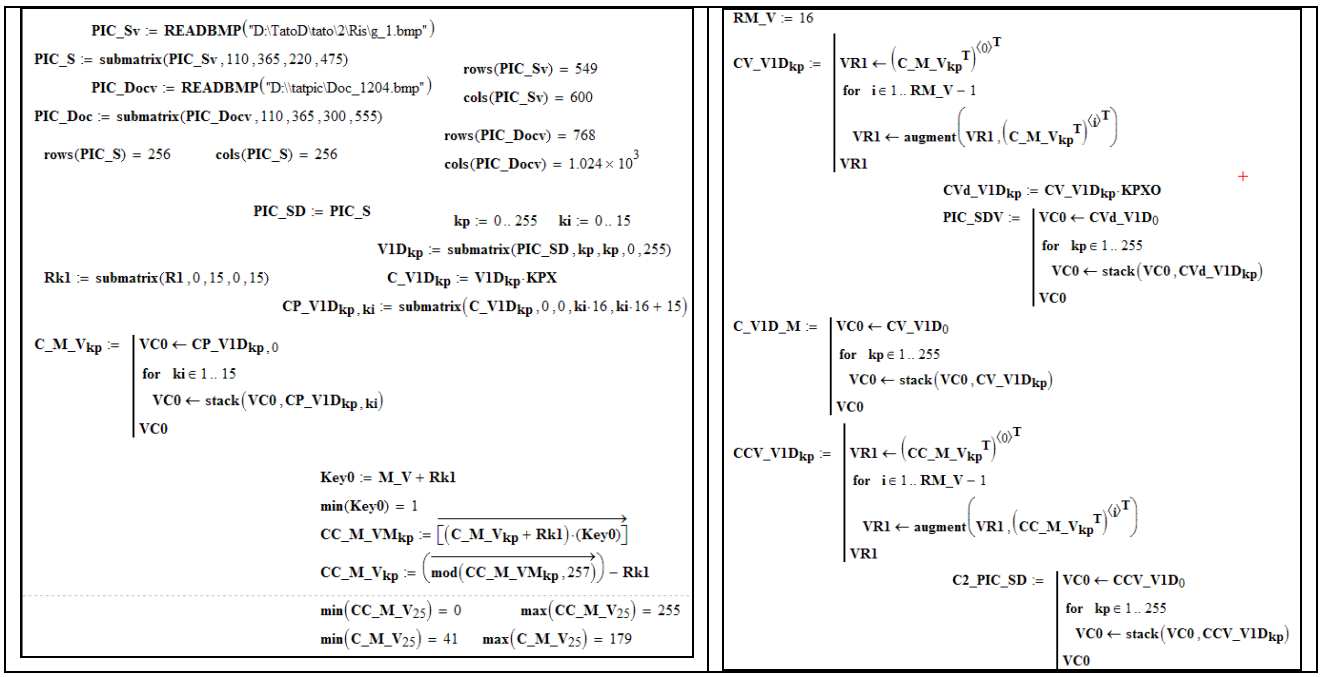

Рис.1. Фрагменти з вікон Mathcad з формулами для формування (конкатенації) блоків, зашифрування, розшифрування зображень алгоритмом блокового МАПШ і верифікації.

Сформована любим способом випадкова бітова матриця КРХ (256*256*1) перестановок використовується для перестановок байтів у кожному kp-ому Б (256 компонентний вектор VID (C_VID) чи матриця C_M_V (16*16) з 8-розрядними числами). ЇЇ можна однозначно представити і у вигляді матриці M_V (16*16) байтів, яка або її параметрична (степенева) модель і використовується для МАПП на наступному етапі. Сутність МАПП полягає у застосуванні до матриць-Б, як сукупностей байтів (8-бітних зображень (PIC_S, PIC_Doc, дивись рис.1), процедур по-елементного матричного множення на відповідні 8-бітні МК (прямі та обернені до них) тієї ж розмірності (Key0, Key0_O чи Key_C(qa), Key_C(qo), Key_CN(qs), що залежать від параметрів та модулі формування яких показані на рис. 4,5 !) з використанням операцій множення та додавання за модулем. Як видно з рис. 3 і 6 результати моделювання процесів прямого та оберненого КП ТГД і З (і кольорового) розмірністю 256*256 ел. підтвердили коректну роботу моделей.

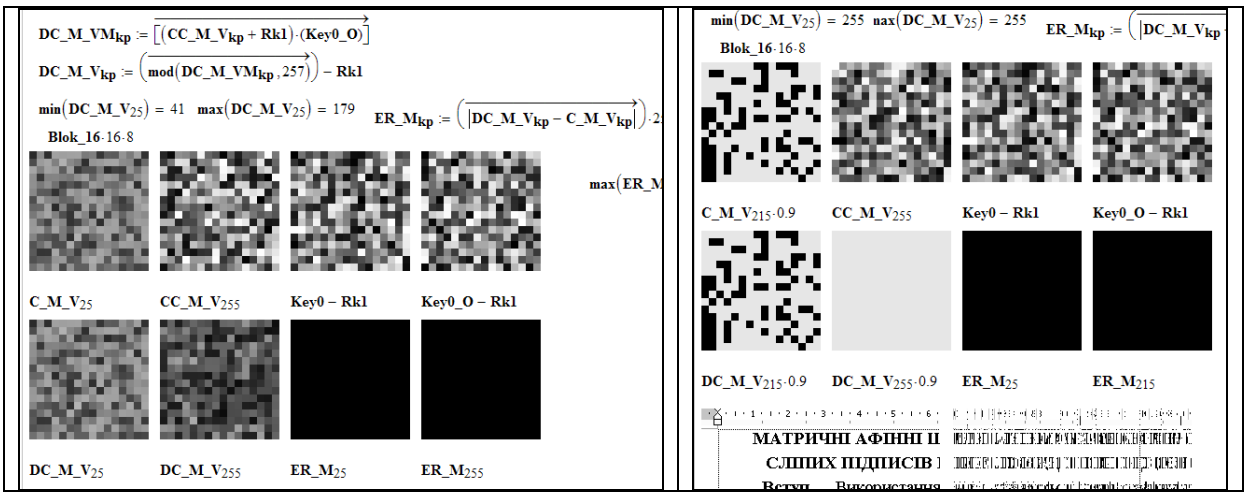

Рис.2. Результати КП та вигляд поточних ключів, блоків до і після КП, різницеві верифікаційні матриці-блоки: ліворуч-для 1-го З, праворуч – для ТГД.

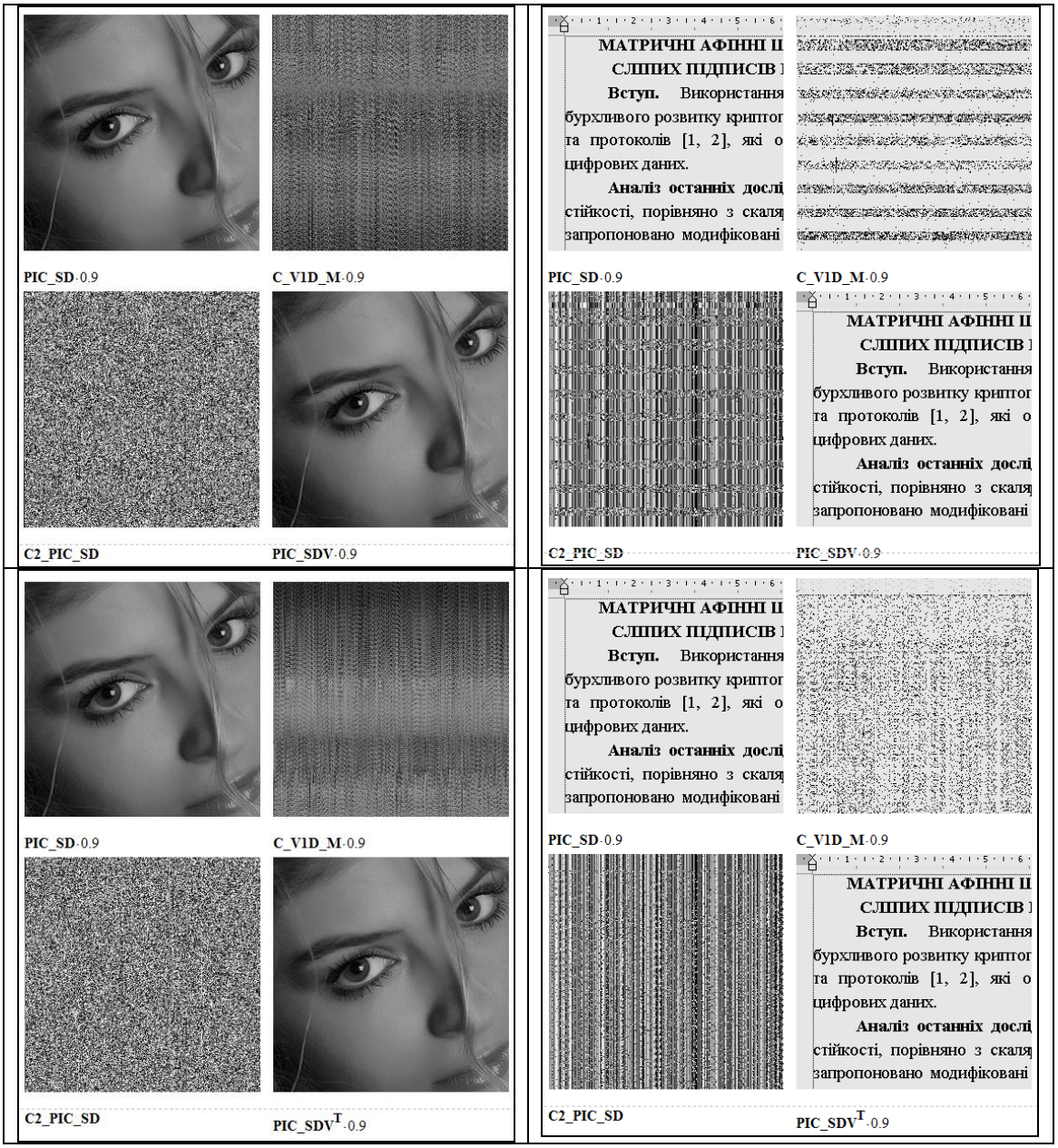

Рис.3. Фрагменти вікон Mathcad з результатами моделювання КП блоковими МАПШ.

Криптографічна обробка блоків при їх виділенні супроводжується одночасним перемішуванням їх елементів та наступними їх замінами МАПП, але, як буде показано нами у доповіді, аналіз ентропій, гістограм З, ТГД та їх криптограм, як видно з рис.3, показує, що для ТГД, на відміну від зображення особи, декількох ітераційних множень матриці даних (МД) на МК зліва чи справа може бути недостатньо, тим більше при застосуванні того ж МК. Тому для покращення алгоритму ми пропонуємо застосовувати для блоків різні поточні МК, оскільки процес їх генерування може бути зведений до простих параметричних моделей.

Key_C(qa) := **p ← 1** **S ← Key0** **while p < qa** **S ← [(S)·(Key0)]** **S ← (mod(S, m1))** **p ← p + 1** **S**	**Key_C_O(qo) :=** **p ← 1** **S ← Key0_O** **while p < qo** **S ← [(S)·(Key0_O)]** **S ← (mod(S, m1))** **p ← p + 1** **S**
Модуль генерації поточних МК	Генерація поточних обернених МК

Рис.4. Фрагменти з вікон Mathcad з модулями формування МК.

Key_CN(qs) := **p ← 1** **S ← Key0N** **while p < qs** **S ← [(S)·(Key0N)]** **S ← (mod(S, 257))** **p ← p + 1** **S**	$\mu_{kp} := mod(kp, 5) + 3$ $CC\_M\_VM_{kp} := [(C\_M\_V_{kp} + Rk1)\cdot(Key\_C(\mu_{kp}))]$ $CC\_M\_V_{kp} := (mod(CC\_M\_VM_{kp}, 257)) - Rk1$ Формули для прямого КП параметричними МК $DC\_M\_VM_{kp} := [(CC\_M\_V_{kp} + Rk1)\cdot(Key\_C\_O(\mu_{kp}))]$ $DC\_M\_V_{kp} := (mod(DC\_M\_VM_{kp}, 257)) - Rk1$ $ER\_M_{kp} := (\lvert DC\_M\_V_{kp} - C\_M\_V_{kp}\rvert)\cdot 255$
Модуль генерації МК з КРХ	Для оберненого КП параметричними МК

Рис.5. Фрагменти з вікон Mathcad з модулями формування МК та формулами КП.

Параметричні блокові МАПШ КП, ідея яких базується на використанні залежностей від індексів блоків і додаткових скалярно-векторних ключів (ВК) і в якості параметрів, що впливають на степені матриць МД та МК за модулем у моделях їх матричного множення та степінь і вид матриць перестановок. Для різних Б та ітераційних кроків беруться різні МК.

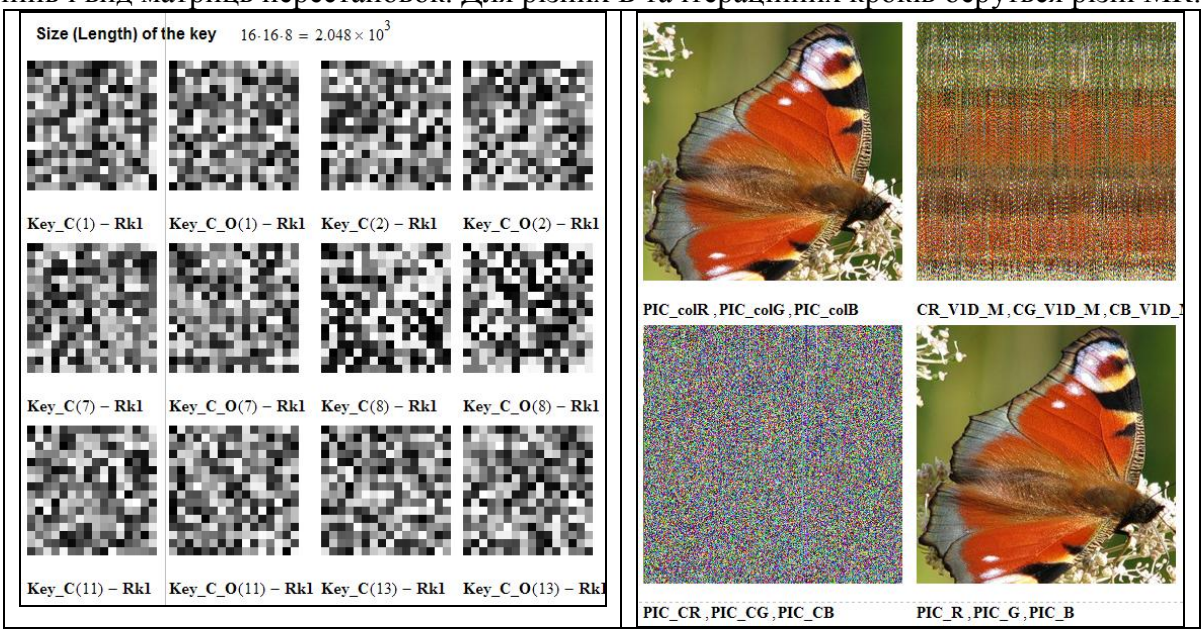

Рис.6. Вигляд параметричних поточних МК (праворуч) та КП кольорового З (ліворуч).

Аналіз гістограм до та після КП підтверджує, що запропоновані моделі дають кращі результати. Ентропія ТГД складала 0,738, а ентропія криптограми ТГД зросла в 10,62 рази та стала рівною 7,837. Ентропії криптограм З стали майже рівними 8 біт на ел.: 7,997 (-0,04% !). Без знання МК неможливо відновити МД і, як було показано в [3-4], уже при розмірності 32*32 МК виду Р, забезпечується стійкість моделей, а в нас ключі 16*16 не 1-бітних, а 8-бітних елементів, що навіть для Р (256!) дає суттєвий запас! Потужність множини можливих ключів зросла на порядки (більше ніж 10^{300} !!). Тому стійкість моделей суттєво зросла.

Висновки. Запропоновані та промодельовані нові параметричні матрично-алгебраїчні моделі (МАМ) блокових МАПШ для КП. Наводяться результати їх моделювання на прикладі прямих та обернених КП зображень, що свідчать про їх коректну роботу та ефективність. Розглянуті аспекти створення поточних МК. Моделі реалізуються як програмно так і матричними процесорами, мають високі швидкість і стійкість перетворень.

Список літератури

1. Красиленко В.Г. Моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // Інформатика та системні науки (ІСН-2017): матеріали VIII Всеукраїнської НПК, (м. Полтава, 16–18 березня 2017 року) / за ред. О.О.Ємця – Полтава: ПУЕТ, 2017. – Режим доступу: http://dspace.puet.edu.ua/handle/123456789/5558

2. 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: ЛНУ імені Івана Франка, 2017. – Вип. 7. – С 20-42. – Режим доступу: http://elit.lnu.edu.ua/issue.php?lang=&number=7

3. 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.

4. 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.

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 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

7. 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. Режим доступу: http://ddpu.drohobych.net/wp-content/uploads/2016/04/material_konf.pdf

8. 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: збірник наукових праць. – Львів: Львівський НУ імені Івана Франка, 2016. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf

9. Красиленко В.Г. Криптографічні перетворення (КП) кольорових зображень на основі матричних моделей з операціями за модулем / В.Г. Красиленко, Д.В. Нікітович // Сучасні методи, інформаційне та програмне забезпечення систем управління організаційно-

технічними комплексами: збірник тез доповідей всеукраїнської науково-практичної інтернет-конференції (11 травня 2016 року). – Луцьк: РВВ Луцького НТУ, 2016. – С. 41-43.

Красиленко В.Г., Нікітович Д.В.
Вінницький національний технічний університет

БАГАТОФУНКЦІОНАЛЬНІ ПАРАМЕТРИЧНІ МАТРИЧНО-АЛГЕБРАЇЧНІ МОДЕЛІ (МАМ) КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ (КП) З ОПЕРАЦІЯМИ ЗА МОДУЛЕМ ТА ЇХ МОДЕЛЮВАННЯ

*Анотація. В роботі запропоновані та розглянуті нові моделі з операціями за модулем для КП, в тому числі зображень. Наводяться результати їх моделювання на прикладі прямих та обернених КП зображень, що свідчать про їх коректну роботу, зручність (всього 1 матрична процедура та 1 МК!), адаптованість до форматів, багатофункціональність (поєднання операцій матричних блокових замін з перестановками, як самих блоків так і елементів блоків, взаємозамінність циклових ітераційних процедур та матричних піднесень у степінь за модулем зі зручними і простими вибором параметрів та управлінням ними перетвореннями, формуваннями ключів), ефективність (орієнтація на матричні процесори). Розглянуті аспекти багатокрокових матричних алгебраїчних КП процедур на основі операцій за модулем і параметричних різновидів синтезу необхідних матричних ключів (МК). Показані експерименти зашифрування та розшифрування зображень (256*256 елементів) і текстово-графічних документів (ТГД) у програмному середовищі Mathcad.*

Вступ, аналіз досліджень і публікацій. На відміну від типових послідовних скалярних алгоритмів, моделей криптосистем поява нових паралельних алгоритмів, а особливо матриць багатопроцесорних засобів, потребує створення відповідних матрично-алгебраїчних моделей і систем матричного типу (МТ). Переваги КП ТГД у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій, тощо, чорно-білих і кольорових зображень (З) матричними алгоритмами на основі узагальнених матричних афінних і афінно-перестановочних шифрів, в тому числі при створенні сліпих цифрових підписів були продемонстровані у роботах [1-4]. Їх базовими операціями є по-елементні множення, додавання за модулем матриць та матричні моделі перестановок (ММ_П) з процедурами множення матриць. Для збільшення ентропії та зміни гістограми З при їх КП на основі ММ_П необхідні декомпозиція бітових зрізів у модифікованих моделях та крім двох МК ще й два векторних (ВК) [5-6]. Модифікації вищезгаданих моделей дозволяють при КП перевіряти цілісність (Ц) криптограм та наявність у них перекручувань, що було показано в [7-8], як для чорно-білих так і кольорових зображень. Але, як засвідчили експерименти, деякі специфічні ТГД, наприклад скановані документи, мають значні по розмірах області з майже однаковою інтенсивністю пікселів, малу кількість градацій і дуже характерні гістограми, що потребує для їх КП збільшення крипто-стійкості шляхом пошуку вдосконалень МАМ, в тому числі і за рахунок розширення їх функціональності при збереженні уніфікованих матричних операцій, процедур [9]. Таким чином, метою роботи та актуальною є спроба розробок і подальшої модифікації, універсалізації та узагальнення МАМ для КП з метою покращення їх характеристик та стійкості, а моделювання та перевірка створених моделей на реальних інформаційних об’єктах (ІО) дозволить оцінити їх параметри, можливості та особливості застосувань.

Виклад матеріалу та результатів дослідження. Сутність запропонованих МАМ для КП полягає у застосуванні до матриць розмірністю N*N, як сукупностей байтів чи 8-бітних зображень (PIC_S, PIC_Doc, дивись рис.1), процедур матричного множення на відповідні 8-бітні МК тієї ж розмірності (KLC256, KLD256) з використанням операцій множення та додавання за модулем. Як видно з рис. 1-5, результати моделювання процесів прямого та оберненого КП ТГД і З розмірністю 256*256 ел. підтвердили коректну роботу моделей при застосуванні правильних ключів (рис.4) так і неправильних (рис.5). МК мали ієрархічну