УДК 681.3.05

В.Г. Красиленко, С.К. Грабовляк

Вінницький соціально-економічний інститут університету «Україна», Вінниця

МАТРИЧНІ АФІННО-ПЕРЕСТАНОВОЧНІ АЛГОРИТМИ ДЛЯ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ

В статті на основі аналізу публікацій та теоретичних основ матричних афінних шифрів, включаючи їх багатокрокові модифікації, розгляду математичних моделей шифрів перестановок з оцінками їх стійкості пропонуються матричні афінно-перестановочні алгоритми для криптографічних перетворень зображень, як вдосконалення та шлях покращення стійкості матричних афінних шифрів шляхом доповнення їх матричними моделями перестановок. Наведені формули та алгоритмічні кроки процедур і конкретних результатів шифрування та дешифрування великорозмірних чорно-білих та кольорових зображень. Показані на прикладах особливості множини матриць-перестановок з операцією їх множення, як алгебраїчної групи. Визначені оцінки стійкості та часу зламування у таких алгоритмах. Продемонстровані можливості та переваги таких модифікацій алгоритмів для обробки зображень модельними експериментами у програмному середовищі Mathcad Professional.

Ключові слова: *криптографічні перетворення, матричний афінно-перестановочний алгоритм, матриця перестановок, алгебри, групи, шифрування, дешифрування, зображення, стійкість, час атаки.*

Вступ

Постановка проблеми. Стрімкий розвиток ІТ-інфраструктури підприємств, організацій та установ, електронних комунікацій та мережевих технологій призводить до зростання кількості інформаційних загроз і вразливості інформаційних ресурсів. В таких умовах зростає актуальність та важливість забезпечення необхідного рівня захисту інформації державного, військового, комерційного та приватного змісту. Одним з напрямків вирішення проблеми інформаційної безпеки та захисту інформаційних ресурсів в інформаційних системах є застосування методів та засобів криптографії, як напрямку, що останні 2-3 десятиліття розвивається бурхливими темпами. Аналіз відомих існуючих методів та засобів шифрування-дешифрування даних, криптографічних алгоритмів та протоколів, що використовуються для захисту інформації [1, 2], показує, що більшість з них орієнтовані на послідовну обробку скалярних даних. При цьому для криптографічних перетворень різних інформаційних блоків найчастіше використовується один і той самий підключ або ключ, в результаті чого такі алгоритми послідовної обробки блоків є нестійкими. Важливим елементом сучасних криптографічних систем та фундаментальною основою, особливо для асиметричних алгоритмів, є довжина ключа і діапазон модулів (чисел), які використовуються для визначення розмірностей скінченних полів, параметрів криптографічних систем та реалізації процедур генерування ключів, формування шифрограм, криптоперетворень, автентифікації та верифікації цифрових підписів. В той же час з'являється все більше і більше задач, в яких необхідно виконувати криптографічні

© В.Г. Красиленко, С.К. Грабовляк

перетворення над багатовимірними сигналами, серед яких особливе місце займають двовимірні масиви, а також багатоградаційні та кольорові зображення. До них належать і біометричні системи, в яких необхідно обробляти та зберігати велику кількість різноманітних зображень, наприклад, відбитки пальців, зображення рухомих об'єктів, обличчя, райдужної сітківки ока тощо. Вся ця інформація часто є конфіденційною, а тому є гостра необхідність в її криптографічному перетворенні з метою захисту від несанкціонованого доступу. Використання для шифрування зображень традиційних та модифікованих підходів та методів, що базуються на відомих алгоритмах, наприклад, RSA [3, 4], показує, що виконувати криптографічні перетворення необхідно для деякої сукупності чи масиву (вікна) пікселів (рядок, кілька рядків, тощо) і бажано застосовувати різні підключі. В той же час, в таких роботах мало приділялось уваги комплексному підходу і аналізу таких криптоалгоритмів комплексним критерієм та частковими, наприклад такими як час та обчислювальні ресурси для виконання криптографічних процедур. На наш погляд, суперечливим є також питання, що в сучасних умовах важко зберігати та створювати за допомогою відповідних протоколів та процедур ключі, які є великої розмірності, і є не тільки скалярними величинами, а представлені і формуються у вигляді багатовимірних масивів даних, наприклад, матриць великої розмірності чи зображень. Вибрати з бази зображень потрібне та передати його чи інше зображення, яке створене шляхом криптоперетворень, на електронну адресу особи, з якою планується створити захищений канал передачі інформації (шляхом її шифрування-дешифрування) на сьогоднішній день не складає ніяких труднощів. Вибравши відповідні формати представлення зображень, наприклад, bmp чи інші, їх легко та швидко (в реальному масштабі часу) ввести, обробити у відповідному програмному середовищі (MathCad, тощо), записати та вивести і передати у вигляді файлу. Головним питанням, що є важливим для забезпечення стійкості пропонованих підходів та методів залишається вирішення задачі створення ефективних та криптостійких протоколів формування матричних ключів, тобто ключів, що є фактично зображеннями великої розмірності.

Аналіз останніх досліджень і публікацій. Для забезпечення більшої стійкості алгоритмів у порівнянні з скалярними криптографічними перетвореннями у роботах [5, 6] було запропоновано модифіковані матричні алгоритми криптографічних перетворень 2-D масивів і зображень, що базуються на модифікації відомих афінних шифрів [1]. У статті [7] було представлено також результати моделювання модифікованого алгоритму створення 2-D ключа, в основу якого покладено математичні моделі та протокол Діффі-Хелмана. Результати моделювання процесів криптоперетворень багатоградаційних та кольорових зображень на основі запропонованих матричних алгоритмів та моделей, що наведені в цих роботах, показують їх суттєві переваги порівняно з традиційним афінним асиметричним шифром. У роботі [8] на основі матричних афінних шифрів розглядається процес створення сліпого цифрового підпису на текстографічні документи, що представлені у вигляді багатоградаційних зображень, та наводяться результати моделювання реально розробленої і практично перевіреної програми для реалізації процедур формування та верифікації цього підпису.

В роботах [5, 9, 10] розглядались нові алгоритми та практично реалізована на їх основі мовою Delphi програма CryptoFax та її експериментальні випробовування та дослідження. Цими роботами була вирішена задача захисту інформації в текстографічних документах при їх передаванні електронними мережами чи факсимільним способом. Було показано, що розроблені криптографічні методи, в основу яких покладено матричні перестановки та використання надлишковості при представленні даних у вигляді текстографічних зображень, є стійкими до впливу завад та різних спотворень, що виникають під час передавання документів. При дії завад з втратами до 30% від загальної кількості (біт) інформації, що передається, програма показала можливе ефективне дешифрування та відтворення переданої інформації. Програма дозволяла працювати із зображеннями розміром 787×1130 точок, що відповідають формату аркуша паперу А4 при роздільній здатності 100 точок на дюйм та розмірі полів по 5 мм (зображення являє собою матрицю розмірністю 787×1130). Суть методу кодування полягала у керованій перестановці місцями елементів матриці, при цьому повна кількість можливих перестановок оцінювалася величиною (787·1130)!=889310!, що навіть з урахуванням обмежень реалізацій та вибраної довжини ключа забезпечувала достатню криптостійкість. Недоліком роботи з програмою CryptoFax є те, що при такому методі перетворень розподіл яскравостей пікселів зображень залишається незмінним.

Вище розглянуті алгоритми описуються математичними суто матричними моделями, тому поява спеціалізованих швидкодіючих, високопродуктивних матричних процесорів та систем паралельної обробки, що працюють з матричними картинними операндами і матричними логіками, дозволяє легше та ефективніше відобразити такі матричні криптографічні моделі, алгоритми на матричні структури і реалізувати на їх основі криптосистеми з обчислювальною продуктивністю на рівні $10^9 – 10^{15}$ операцій за секунду та суттєвим зменшення часу обробки чи криптоперетворення.

Постановка завдання. Тому метою роботи є покращення стійкості матричних афінних алгоритмів криптоперетворень зображень шляхом допов-

нення їх матричними моделями перестановок, створення на цій основі матричних афінно-перестановочних алгоритмів та демонстрація можливостей таких модифікацій для практичних застосувань модельними експериментами у програмному середовищі MathCad Professional.

Основна частина

Короткі відомості про теоретичні основи матричних афінних шифрів. Суть узагальнених матричних афінних шифрів, що належать до асиметричних систем та алгоритмів [5,6], полягає в наступному: створюємо матрицю N, всі елементи якої однакові і дорівнюють простому великому числу n. Далі вибираємо два матричні ключі відповідної розмірності **A** та **S**, елементи яких є числами з діапазону 1÷(n-1). Для того, щоб створити ключі дешифрування, які представляються як матриці **AD** та **SD** такої ж розмірності як і **A** та **S**, необхідно:

1) для кожного елемента $a_{i,j}$ матриці **A** знайти обернене за модулем n число $a_{i,j}^{-1}$, сукупність яких і представлятиме матрицю **AD**.

2) для визначення матриці **SD** знайти значення кожного елемента sd_{ij} за відомим виразом (1):

$$sd_{ij} = -a_{ij}^{-1} \cdot s_{ij} \mod n \qquad (1)$$

або у матричному вигляді(2):

$$\mathbf{SD} = \left(-\mathbf{AD} \underset{N}{\Theta} \mathbf{S} \right), \qquad (2)$$

де символом $\left(\underset{N}{\Theta} \right)$ позначено поелементне множення за модулем n матриць **AD** та **S**.

Процеси шифрування та дешифрування для матричного повідомлення **M** та криптограми **C** виражаються формулами (3), (4), де символом $\left(\underset{N}{+} \right)$ позначено поелементне додавання за модулем n матриць:

$$\mathbf{C} = \left(\mathbf{M} \underset{N}{\Theta} \mathbf{A} \underset{N}{+} \mathbf{S} \right); \qquad (3)$$

$$\mathbf{M} = \left(\mathbf{C} \underset{N}{\Theta} \mathbf{AD} \underset{N}{+} \mathbf{SD} \right). \qquad (4)$$

Якщо до створеного за формулою 2 закритого повідомлення C застосувати аналогічну процедуру шифрування з тими ж ключами β разів, то будемо мати, так званий, багатокроковий матричний афінний шифр [5]. Аналогічно до вище сказаного, процес дешифрування за формулою (4) також повторюватиметься β разів. У цьому випадку узагальнені формули прямого та оберненого криптоперетворень для такого багатокрокового матричного афінного шифру будуть мати відповідно вигляд (5) та (6):

$$\mathbf{C} = \underbrace{\left(\left(\mathbf{M} \underset{N}{\Theta} \mathbf{A} \underset{N}{+} \mathbf{S} \right) \underset{N}{\Theta} \mathbf{A} \underset{N}{+} \mathbf{S} \right) \ldots \underset{N}{+} \mathbf{S} \Big)}_{\beta}; \qquad (5)$$

$$\mathbf{M} = \underbrace{\left(\left(\mathbf{C} \underset{N}{\Theta} \mathbf{AD} \underset{N}{+} \mathbf{SD} \right) \underset{N}{\Theta} \mathbf{AD} \underset{N}{+} \mathbf{SD} \right) \ldots \underset{N}{+} \mathbf{SD} \Big)}_{\beta}. \qquad (6)$$

Специфіка зображень та кодування яскравості піксела напівтонового зображення (або однієї з RGB складових кольорового) байтом дозволяє шляхом додавання фону (+ 1 градація) перетворити діапазон значень елементів матриць M, A, AD, тощо, який є рівним 0÷255, в діапазон 1÷256. При цьому n = 257, і є простим числом, а тому може бути використаним у запропонованих таких шифрах.

Основи матричних моделей шифрів перестановки. Якщо вхідне повідомлення представити у вигляді вектора, елементами якого є числа з обраного діапазону, то використовуючи матриці перестановок та векторно-матричні процедури можна переставляти місцями компоненти вектора. При множенні матриці, що відповідає явному вхідному зображенню, зліва та справа на відповідні матриці перестановок відбувається перемішування відповідно стовпців та рядків такої матриці. При такому варіанті представлення шифрів перестановки забезпечується не найбільша можлива кількість перестановок, оскільки елементи рядків чи стовпців перемішуються за тими самими правилами. Перестановки можуть бути описані і іншими моделями [1], але, на наш погляд, найбільш зручними та адекватними при описуванні криптоперетворень зображень шляхом перестановок їх пікселів є саме матричні моделі типу **SPXY=KPX·SI·KPY**, де **SI** – матриця вхідного повідомлення заданої розмірності, **KPX** та **KPY** – квадратичні матриці перестановок по одній та відповідно другій координатах з розмірностями матриць узгодженими з кількістю рядків та стовпців. Основу цих моделей складають матриці перестановок **P**, тобто матриці, в яких в кожному стовпчику і в кожному рядку є лише один елемент, який дорівнює 1, а всі інші дорівнюють 0 [9,11]. Потужність множини всіх можливих матриць **P** розмірністю k×k оцінюється величиною **K** = f(k) = k!. Набір всіх можливих матриць розмірністю 4×4 показаний на рис. 1. Для даного випадку кількість матриць буде дорівнювати 4!=1·2·3·4=24.

Вивчення властивостей матриць **P** показує, що множина цих матриць із асоціативною операцією (·) їх множення (наприклад **P3·P4=P19** або **P10·P16=P13**, дивись рис. 2) є групою, оскільки в ній є нейтральний елемент, одинична матриця (**P1**), а для кожного елемента існує обернений (**P23** є оберненим до **P19,** бо **P23·P19= P1),** крім того, операція (·) є «некомутативною», оскільки **P3·P4** не дорівнює **P4·P3.**

Можна помітити, що з даного матричного набору матриця **P1**, що є одиничною, та матриця **P24**, яка є її дзеркальним відображенням, на відміну від інших, перестановок не роблять. Отже, не всі матриці з даної множини можуть бути використані.

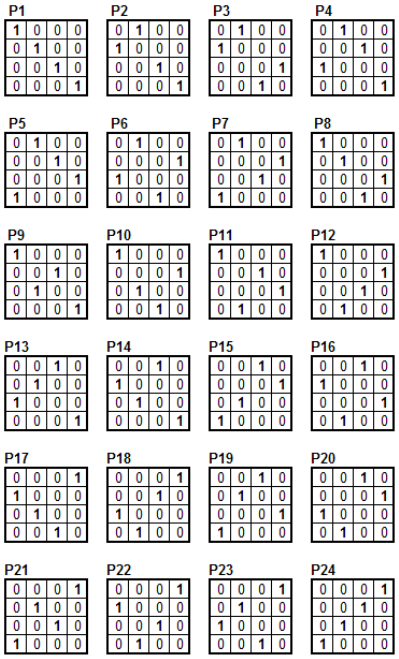

Рис. 1. Набір всіх можливих матриць-перестановок розмірністю 4×4 матриць з набору

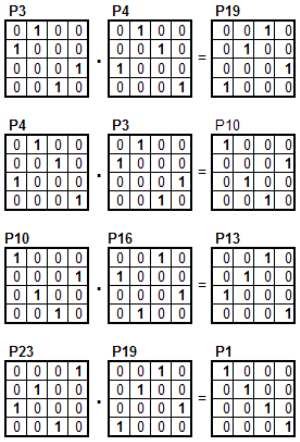

Рис. 2. Приклад перемножування матриць з набору

Для оцінювання потужності множини можливих матриць перестановок як функції **K**=f(k)=k!, нами були проведені відповідні розрахунки [11] кількості матриць перестановок при різних розмірностях матриць k, які представлені в табл. 1. В ній проміжні значення скорочені у зв'язку з обмеженням обсягу статті.

Таблиця 1

k	16	32	56	64
K=f(k)	$2{,}092\cdot10^{13}$	$2{,}631\cdot10^{35}$	$7{,}11\cdot10^{74}$	$1{,}269\cdot10^{89}$

З цієї таблиці видно, що кількість перестановок, при розмірності матриці k = 16, досягає $2{,}092\cdot10^{13}$, при k = 64 аж $1{,}269\cdot10^{89}$.

Сучасні технічні засоби, а особливо супер-ПЕОМ, дозволяють працювати з великою продуктивністю обробки даних (10^{12} –10^{15} операцій за секунду і більше). У зв'язку з цим, не дивлячись на таку велику кількість перестановок, при відповідному нарощуванні мережевих ресурсів, час перебору може бути не таким значним, а тому бажано зробити хоча б грубі оцінки часу атаки (перебору в таких алгоритмах).

Як функція від розмірності k матриць перестановок нами використовувалась нижче наведена формула (7) для визначення часу перебору **T** = φ(k). В ній було враховано, що одна матриця-перестановки заданої розмірності k×k з будь-яким навіть значним k, може бути згенерована за наносекунду, а оскільки хвилина має 60 секунд, година – 60 хвилин, доба – 24 години, а рік – 365 діб, то використовуючи вираз для значення потужності множини матриць перестанвок **K** = f(k), час брутальної атаки був визначений шляхом поділу величини **K** на кількість створених матриць за рік при вказаній вище продуктивності ПЕОМ. Вираз (7) дозволяє оцінити час (в роках), що необхідний для перебору матриць. Оцінки при різних значеннях k матриць показані в табл. 2:

$$\mathbf{T} = \frac{\mathbf{K}}{10^9 \cdot 60 \cdot 60 \cdot 24 \cdot 365}. \qquad (7)$$

Таблиця 2

k	16	24	32	56	64
T	$6{,}635\cdot10^{-4}$	$1{,}967\cdot10^{7}$	$8{,}344\cdot10^{18}$	$2{,}255\cdot10^{58}$	$4{,}024\cdot10^{72}$

З таблиці видно, що при розмірності матриці k = 16 час для перебору дорівнює $6{,}635\cdot10^{-4}$, отже він досить малий, а при розмірності k = 32 становить $8{,}344\cdot10^{18}$, тобто, в даному випадку перебір займе досить значний час. Отже, з даних розрахунків випливає, що матриці розмірністю 24×24 чи 32×32 забезпечують достатню стійкість.

Матричні афінно-перестановочні алгоритми. В даній статті ми не зупиняємось на процесі формування ключів, це буде розглянуто в наступних роботах. Тут нами розглядаються саме матричні афінно-перестановочні алгоритми, результати їх дослідження та моделювання.

Поєднання матричних афінних шифрів з математичними моделями шифрів перестановок дозволяє створити групу матричних афінно-перестановочних алгоритмів для криптоперетворень зображень, які в загальному випадку можуть бути представлені у вигляді процедур шифрування-дешифрування на основі нижче наведених формул (8), (9):

$$\mathbf{C}_{\text{МАПА}} = \underbrace{\mathbf{KPX}\cdot\mathbf{M}\cdot\mathbf{KPY}\ \underset{N}{\Theta}\mathbf{A}\underset{N}{+}\mathbf{S}\ \ldots\underset{N}{+}\mathbf{S}}_{\beta}; \qquad (8)$$

$$\mathbf{M}'_{\text{МАПА}} = \mathbf{KPX}^{-1}\cdot\underbrace{(\mathbf{C}_{\text{МАПА}}\underset{T}{\Theta}\mathbf{AD}\underset{N}{+}\mathbf{SD})\ldots\underset{N}{+}\mathbf{SD})}_{\beta}\cdot\mathbf{KPY}^{-1}. \qquad (9)$$

Можливий і нижченаведений спосіб (10), (11):

$$\mathbf{C}_{\text{МАПА}} = \mathbf{KPX}\cdot\underbrace{(\mathbf{M}\underset{N}{\Theta}\mathbf{A}\underset{N}{+}\mathbf{S})\ldots\underset{N}{+}\mathbf{S})}_{\beta}\cdot\mathbf{KPY}; \qquad (10)$$

$$\mathbf{M}'_{\text{МАПА}} = \underbrace{(\mathbf{KPX}^{-1}\cdot\mathbf{C}_{\text{МАПА}}\cdot\mathbf{KPY}^{-1})\underset{N}{\Theta}\mathbf{AD}\underset{N}{+}\mathbf{SD})\ldots\underset{N}{+}\mathbf{SD})}_{\beta}. \qquad (11)$$

Для проведення експериментальних досліджень матричних афінно-перестановочних алгоритмів для криптоперетворень зображень ми використовуємо лише один ключ в афінному перетворенні, а саме його мультиплікативну складову, а параметр β обрали рівним 1 (що відповідає однокроковому варіанту). За допомогою програмного середовища MathCad ми згенерували дві матриці перестановки **KPX** та **KPY** розмірністю 256×256 (рис. 3, 4). (На рис. 4 для кращого сприйняття ми показуємо негатив **KPX** та **KPY**, тобто одиниці відображаються чорними точками).

Об'єктом першого експерименту [12] було обране напівтонове текстографічне зображення **SI** з яскравістю пікселів в діапазоні 0÷255 (Рис. 5a) розмірністю 256×256. Оскільки для афінного шифру (лінійного) достатньо одного, відповідним чином згенерованого матричного ключа [6], нами використовувався в якості ключа **A** ключ шифрування **G** (відповідне йому зображення **GV1** на рис. 5c) та в якості ключа **AD** взаємопов'язаний з ним ключ дешифрування **OG** (зображення **OG**1 на рис. 5e), елементи якого визначаються як обернені за модулем до елементів матриці **G.**

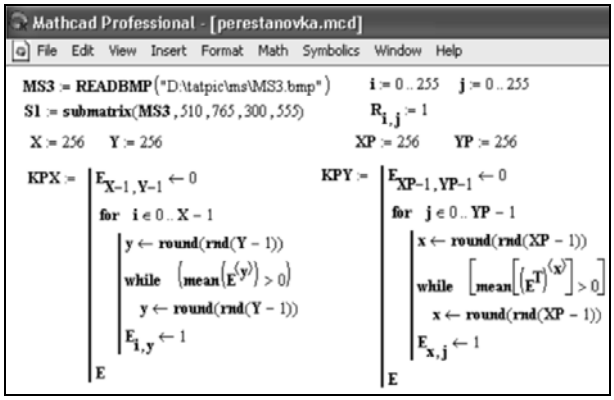

Рис. 3. Формули для генерування матриць перестановок

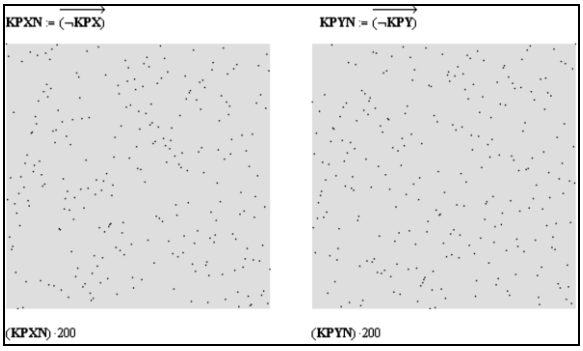

Рис. 4. Матриці перестановок

Процес шифрування здійснюється за допомогою таких кроків:

1) перемішування елементів вхідного зображення **SI**, що підлягало шифруванню у відповідності до формул матричних моделей перестановок (12):

$$\mathbf{SPXY} = \mathbf{KPX} \cdot \mathbf{SI} \cdot \mathbf{KPY}; \qquad (12)$$

2) формування зміщення по інтенсивності пікселів масивів шляхом додавання матриці **R**, всі елементи якої дорівнюють "1" (формули (13), (14), (15):

$$\mathbf{G} = \mathbf{GV1} + \mathbf{R}; \qquad (13)$$

$$\mathbf{OG} = \mathbf{OG1} + \mathbf{R}; \qquad (14)$$

$$\mathbf{SPR} = \mathbf{SPXY} + \mathbf{R}; \qquad (15)$$

3) закриття матриці **SPR** ключем **G** за формулою (16) і отримання матриці **SPG**, яка будучи зміщеною шляхом віднімання від неї матриці **R** (формула (17)), дає матрицю-криптограму зображення **CS**, що є зашифрованим представленням текстографічного документа (зображення на рис. 5, f):

$$\mathbf{SPG} = \mathbf{SPR} \underset{N}{\Theta} \mathbf{G}; \qquad (16)$$

$$\mathbf{CS} = \mathbf{SPG} - \mathbf{R}. \qquad (17)$$

Процес дешифрування відбувається в такій послідовності:

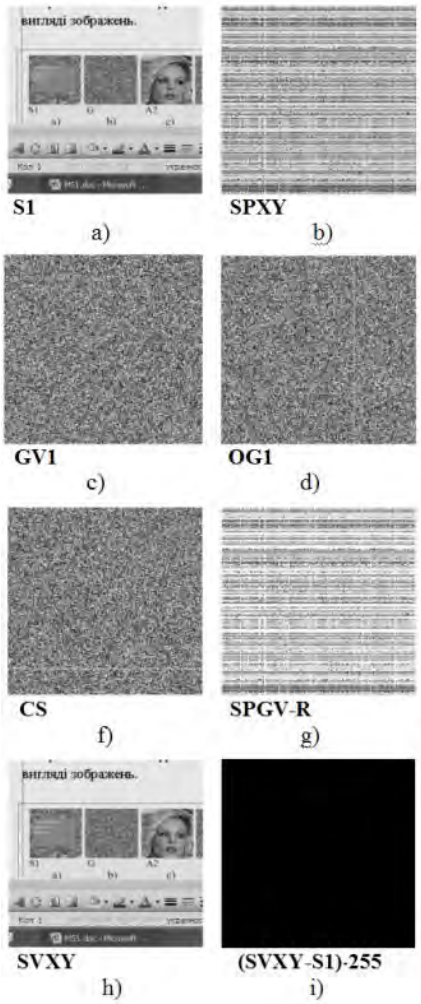

Рис. 5. Результати шифрування зображення на базі матричного афінно-перестановочного алгоритму: a – вхідне зображення для моделювання; b – проміжне зображення після перемішування пікселів за допомогою матриць перестановок; c – зображення ключа шифрування; d – зображення ключа дешифрування; f – криптограма; g – проміжне відновлене зображення з переставленими пікселями; h – повністю відновлене зображення; i – різницеве зображення

1) зміщення криптограми **CS** та її розкриття матричним ключем **OG** у відповідності до формул (18), (19), та отримання матриці відновленої **SPGV**:

$$\mathbf{SPG'} = \mathbf{CS} + \mathbf{R}\ ; \qquad (18)$$

$$\mathbf{SPGV} = \left(\mathbf{SPG'} \underset{\mathrm{N}}{\Theta} \mathbf{OG} \right); \qquad (19)$$

2) зміщення матрицею **R** матриці **SPGV** та отримання відновленого зображення з переставленими пікселями (рис. 5, g);

3) обернене перемішування елементів (точок) та утворення за допомогою формули (20) з зображення **(SPGV-R)** відновленого **SVXY** початкового явного зображення:

$$\mathbf{SVXY} = \mathbf{KPX}^{\mathbf{T}} \cdot \ \mathbf{SPGV} - \mathbf{R}\ \cdot \mathbf{KPY}^{\mathbf{T}}. \qquad (20)$$

В цій формулі замість обернених матриць $\mathbf{KPX}^{-1}$ та $\mathbf{KPY}^{-1}$ використовуються транспоновані ($\mathbf{KPX}^{\mathbf{T}}$ та $\mathbf{KPY}^{\mathbf{T}}$), оскільки для такого виду матриць перестановок **P** обернені до них дорівнюють транспонованим.

Різницеве зображення між вхідним зображенням та розшифрованим (рис. 5, i) підтверджує правильну роботу запропонованого матричного афінно-перестановочного алгоритму для шифрування та дешифрування зображень.

Для оцінювання якості закриття документів при їх шифруванні запропонованим алгоритмом, нами розроблена підпрограма в MathCad, яка дозволяє розраховувати та будувати гістограми розподілу яскравостей та обчислювати середню ентропію на 1 піксель конкретних зображень. Деякі фрагменти гістограми показані на рис. 6. На цьому малюнку показані результати обробки зображень розмірністю 256×256, які отримані в процесі шифрування. Як видно з гістограмних розподілів гістограми **SI** та **SPXY** одинакові, розподіл **KPX** та **KPY** передбачуваний, гістограми **GV1** та **OG1** мають майже рівномірний розподіл, і забезпечують цим отримання майже найкращого розподілу в криптограмі **CS**. Про це свідчать і відповідні ентропії: ентропія початкового текстографічного документа **SI** дорівнює 5,512; ентропія матриці **KPX** – 0,037; зображення **SPXY** – 5,512; ентропія зображення ключа шифрування **GV1** – 7,997; зображення ключа дешифрування **OG** – 7,997; та ентропія зашифрованого зображення **CS** = 7,998, тобто є дуже близькою до максимально можливої 8. А як відомо, чим більша ентропія зашифрованого зображення, тим більша міра невизначеності відповідного зображення і тим складніше провести брутальну атаку на даний алгоритм.

Для наглядного представлення результатів моделювання процесу шифрування текстографічного документу матричним афінно-перестановочним алгоритмом в програмному середовищі MathCAD та визначення часу криптоперетворень здійснено ще одне шифрування вхідного зображення **SI** розмірністю 704×572 (рис. 9, a), відповідно використовуючи ключ **G** (зображення **GV1** на рис. 9, c) для шифрування та ключ **OG** (зображення **OG1** на рис. 9, d) для дешифрування, а також згенеровані нами матриці перестановок **KPX** та **KPY** (рис. 7, 8), що мають різні розмірності для узгодження з розмірами **SI**.

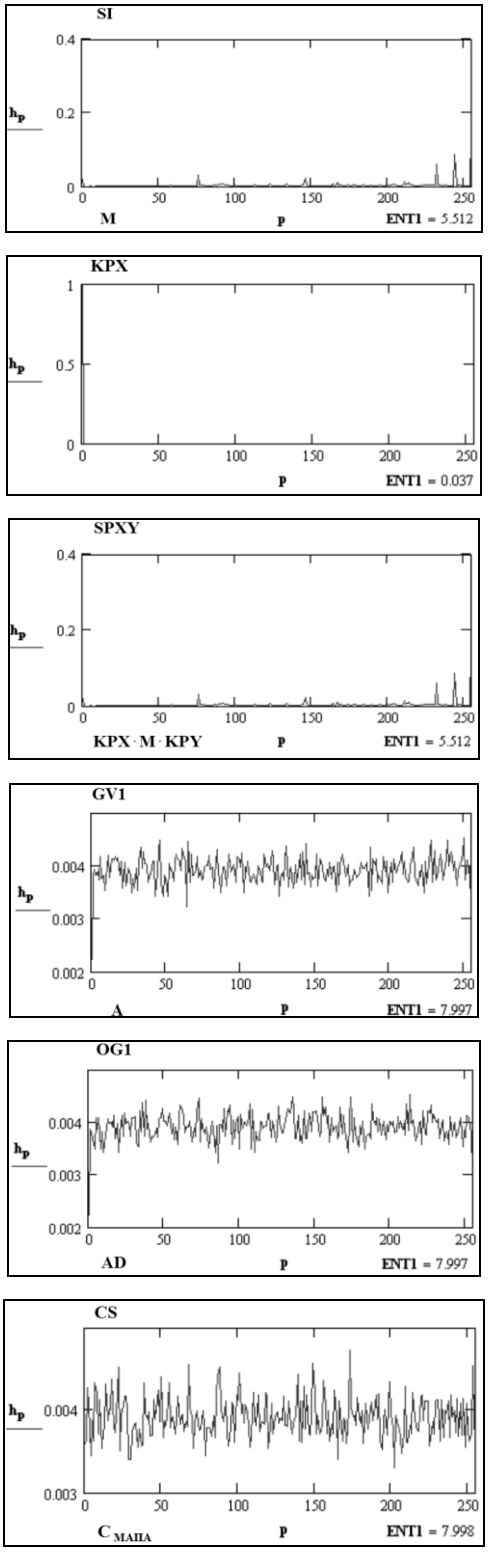

Рис. 6. Гістограми розподілу яскравостей

Порядок шифрування аналогічний попередньому. Після перестановки пікселів вхідного тексто-

графічного документу множенням матриці зображення **SI** на матриці перестановок **KPX** та **KPY** утворюється матриця **SPXY**, що показана як зображення на рис. 9, b. В якості ключа **A** використовувалось випадкове зображення **GV1** (рис. 9, c), де піксель має випадкове значення яскравості.

Додаванням до нього матриці **R** був отриманий ключ шифрування **G** та взаємопов'язаний з ним ключ дешифрування **OG**. (На рис. 9, c показано **OG1=OG-R).** Після шифрування отримали зображення **CS** (рис. 9, d) зашифрованого текстографічного документу.

При дешифруванні зображення спочатку матриця **SPG** розкривається за допомогою ключа **OG,** в результаті чого утворюється матриця **SPGV**. Після оберненого переставляння пікселів шляхом віднімання від матриці **SPGV** матриці **R** (рис. 9, f) та множення її на транспоновані матриці $\mathbf{KPX}^{\mathbf{T}}$ та $\mathbf{KPY}^{\mathbf{T}}$ зліва та справа утворюється зображення **SVXY** (рис. 9, g), яке повністю відповідає вхідному зображенню. Правильність роботи алгоритму підтверджує рис. 9, h. Повний алгоритм дій та формули для моделювання процесів криптографічних перетворень зображень запропонованим алгоритмом в MathCad показані на рис. 10.

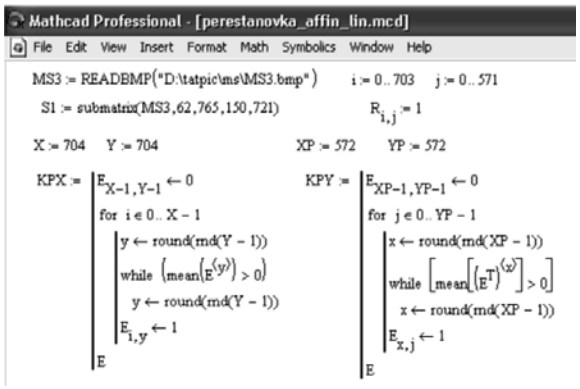

Рис. 7. Формули для генерування матриць перестановки

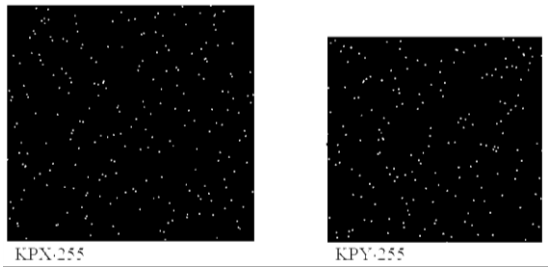

Рис. 8. Матриці перестановки 704×704 та 572×572

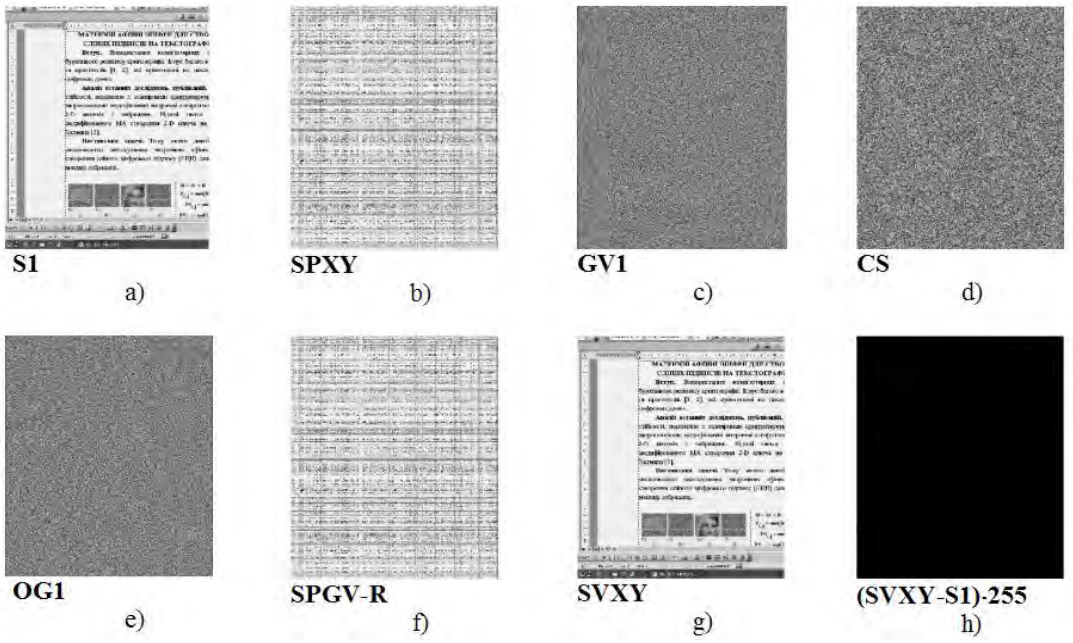

Рис. 9. Результати процесу шифрування та дешифрування текстографічних документів МАПА: a – вхідне зображення для моделювання; b – вхідне зображення після перемішування пікселів за допомогою матриць перестановок; c – зображення ключа шифрування; d – криптограма; e – зображення ключа дешифрування; f – відновлене зображення з переставленими точками; g – повністю відновлене зображення; h – різницеве зображення

Результати модельних експериментів у середовищі MathCad при шифруванні кольорових зображень розмірністю 256×256 у форматі RGB за допомогою МАПА показані на рис. 11 (три складових початкового, проміжне, зашифроване та розшифроване зображення у кольоровому форматі) [12].

На рис. 12 зображені гістограми розподілу яскравостей пікселів у відповідних трьох складових R,G,B, отриманої кольорової криптограми.

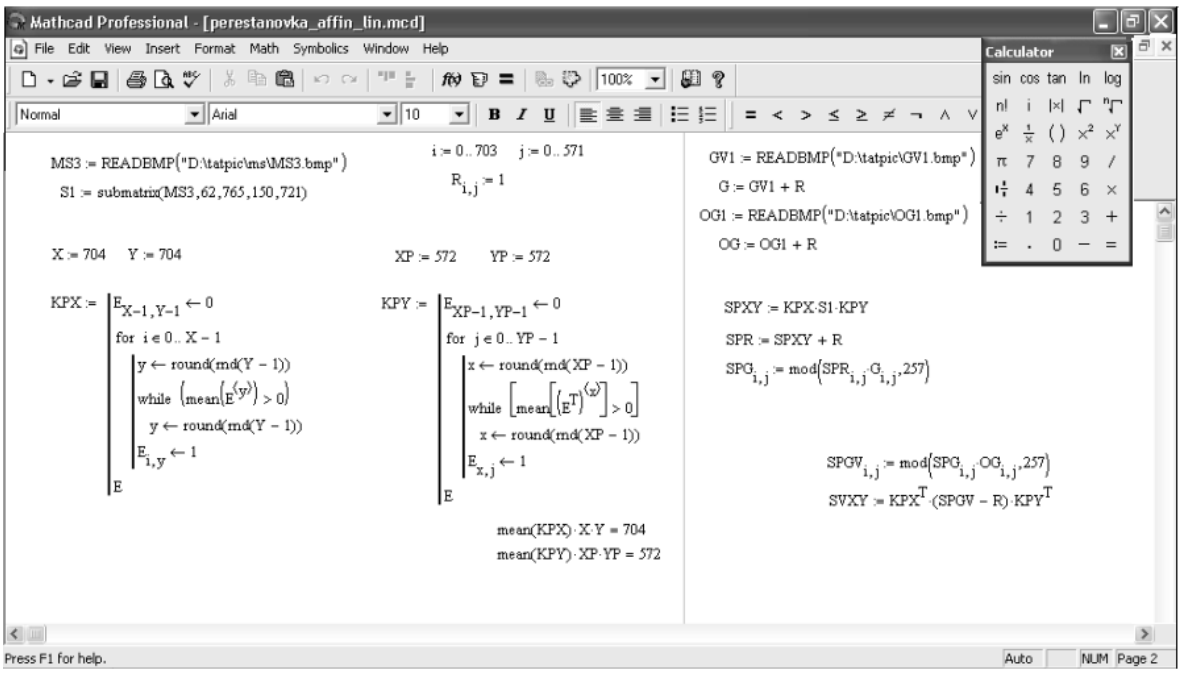

Рис. 10 Формули для моделювання процесів криптографічних перетворень зображень матричним афінно-перестановочним алгоритмом в MathCad

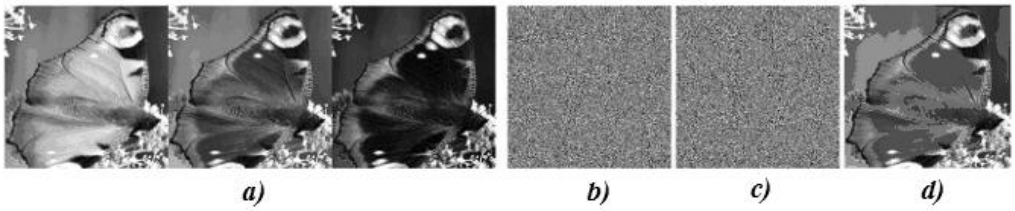

Рис. 11. Результати шифрування кольорових зображень у форматі RGB:
a– три RGB складові вхідного зображення у відтінках сірого; b – проміжне зображення;
c – криптограма; d – відновлене зображення в кольоровому форматі

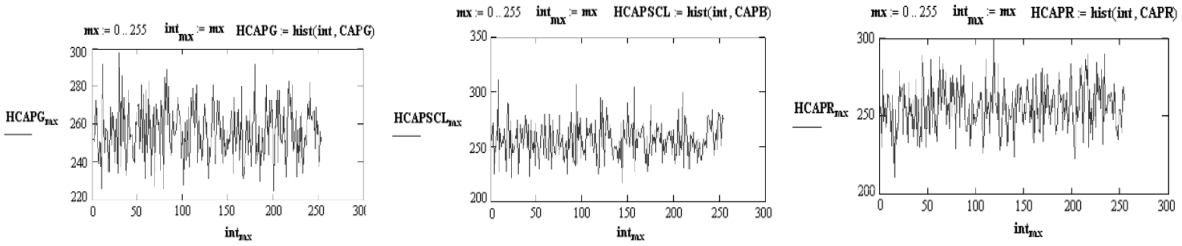

Рис.12. Гістограми розподілу яскравостей у трьох складових отриманої криптограми

Висновки

Таким чином, нами запропоновані матричні афінно-перестановочні алгоритми для шифрування-дешифрування текстографічних документів як вдосконалення та узагальнення матричних багатокрокових афінних шифрів. Вони відносяться до симетрично-асиметричних алгоритмів та криптосистем. Наведені формули для здійснення всіх алгоритмічних кроків та процедур. Модельними експериментами в програмному середовищі MathCad продемонстровано його дію та правильність функціонування на трьох прикладах криптоперетворення напівтонового зображення розмірністю 256×256, чорно-білого зображення розмірністю 704×572 (реального документу) та кольорового зображення розмірністю 256×256 у форматі RGB. Визначено стійкість та час зламування у матричних перестановочних та афінно-перестановочних алгоритмах. Показано, що забезпечити необхідну стійкість таких алгоритмів до атак можливо при розмірностях матриць перестановок не менше 24×24. Встановлено, що матриці перестановок мають тісний зв'язок з цікавими алгебраїчними структурами, групами та півгрупами.

Для оцінювання якості закриття документів при їх шифруванні, була розроблена підпрограма для обчислення середньої ентропії на 1 точку конкретних зображень та побудови гістограм розподілу яскравостей. Час криптоперетворень реальних документів формату А4 не перевищує півхвилини.

З отриманих результатів можна стверджувати, що запропоновані алгоритми можуть бути реалізо-

ваними на основі спеціалізованих матричних пристроїв, матричних перемножувачів, які складаються з масиву одночасно працюючих процесорів і дозволяють виконувати процедури поелементних множення та додавання матриць за модулем паралельно та ефективніше.

Список літератури

1. Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.: іл.

2. Хорошко В.О. Методи та засоби захисту інформації: навч. посібник / В.О. Хорошко, А.О. Четков. – К.: Юніор, 2003. – 502 с.

3. Ковальчук А. Підвищення стійкості системи RSA при шифруванні зображень / А. Ковальчук // Технічні вісті. – 2009. – № 1-2. – С. 70-71.

4. Рашкевич Ю.М. Афінні перетворення в модифікаціях алгоритму RSA шифрування зображень / Ю.М. Рашкевич, А.М. Ковальчук, Д.Д. Пелешко // Автоматика. Автоматизация. Электротехнические комплексы и системы. – 2009. – № 2 (24). – С. 59-66.

5. 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.

6. Красиленко В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В.Г. Красиленко, К. Огородник, Ю. Флавицька // Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. наук.-пр. конф. – К., 2010. – С. 120-124.

7. Красиленко В.Г. Моделювання модифікованого алгоритму створення 2-D ключа в криптографічних застосуваннях / В.Г. Красиленко, О.І. Нікольський, О.О. Лазарєв // Наука і навчальний процес: науково-методичний збірник науково-практичної конференції. – Вінниця, 2008. – С. 107-109.

8. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 7 (97). – С.60-63.

9. A noise-immune cryptographic information protection method for facsimile information transmission and the realization algorithms / V.G. Krasilenko, V.F. Bardachenko, A.I. Nikolsky, et. al. // Proc.SPIE. – 2006. – Vol. 6241. – P. 316-322.

10. Красиленко В.Г. Розробка методу криптографічного захисту інформації текстографічного типу / В.Г. Красиленко, С.А. Свіренюк // Наука і навчальний процес: науково-методичний збірник науково-практичної конференції. – Вінниця, 2006. – С. 73-74.

11. Красиленко В.Г. Оцінювання стійкості та часу зламування у матрично-перестановочних алгоритмах криптоперетворень / В.Г. Красиленко, С.К. Грабовляк // Наука і навчальний процес: науково-методичний збірник матеріалів науково-практичної конференції ВСЕІ Університету "Україна". – Вінниця, 2012. – С. 173-174.

12. Красиленко В.Г. Моделювання матричного афінно-перестановочного алгоритму для криптоперетворень зображень / В.Г. Красиленко, С.К. Грабовляк // Наука і навчальний процес: науково-методичний збірник матеріалів науково-практичної конференції ВСЕІ Університету "Україна". – Вінниця, 2012. – С. 171-172.

Надійшла до редколегії 9.03.2012

Рецензент: д-р техн. наук, проф. В.А. Лужецький, Вінницький національний технічний університет, Вінниця.

МАТРИЧНЫЕ АФФИННО-ПЕРЕСТАНОВОЧНЫЕ АЛГОРИТМЫ ДЛЯ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ ИЗОБРАЖЕНИЙ

В.Г. Красиленко, С.К. Грабовляк

В статье на основе анализа публикаций и теоретических основ матричных аффинных шифров, включая их многошаговые модификации рассмотрения математических моделей шифров перестановок оценкам их устойчивости предлагаются матричные аффинно-перестановочное алгоритмы криптографических преобразований изображений, как совершенствование и путь повышения устойчивости матричных аффинных шифров путем дополнения их матричными моделями перестановок. Приведенные формулы и алгоритмические шаги процедур и конкретных результатов шифрования и дешифрования крупноразмерных черно-белых и цветных изображений. Показаны на примерах особенности множества матриц-перестановок с операцией их умножения, как алгебраической группы. Определены оценки устойчивости и времени взлома в таких алгоритмах. Продемонстрированы возможности и преимущества таких модификаций алгоритмов обработки изображений модельными экспериментами в программной среде Mathcad Professional.

Ключевые слова: *криптографические преобразования, матричный аффинно-перестановочных алгоритм, матрица перестановок, алгебры, группы, шифрования, дешифрования, изображения, устойчивость, время атаки.*

MATRIX AFFINE-PERMUTATION ALGORITHMS FOR ENCRYPTION AND DECRYPTION IMAGES

V.G. Krasilenko, S.K. Grabovlyak

The article is based on an analysis of publications and the theoretical foundations of the matrix affine ciphers, including multistep modification, review of mathematical models cipher permutations with estimates of their stability offered by affinity-matrix permutation algorithms for encryption of images as a way to improve and improve the stability of the matrix affine cipher by supplementing their matrix model permutations. These formulas and algorithmic steps and procedures for concrete results encryption and decryption of large black and white and color images. Illustrated by the particular set of permutations of the matrix multiplication operation it as an algebraic group. The estimation of stability and time of cracking in these algorithms. Demonstrated features and benefits of such modifications of algorithms for image processing model experiments in the software environment Mathcad Professional.

Keywords: *cryptographic transformation, matrix affinity-commutative algorithm, matrix permutation, algebra, group encryption, decryption, image stability, the attack.*