

Секція 1. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тузенко О.А., Балалаєва О.Ю., Хижняк А.Ю., Кулішова К.О.	Розробка програмного забезпечення для підвищення якості роботи муніципальних транспортних служб	3
Хомутовський А.А., Болотіна В.В.	Система управління товарами для магазину розетка	5
Генвальдт А.С., Болотіна В.В.	Розробка web-орієнтованої системи Freelance біржи	6
Грабар О.І., Лисогор Ю.І., Скачков В.О.	Аналіз методів опису текстур для веб-сервісу візуального розпізнавання сортів рослин	8
Мельников О.Ю.	Прогнозування результату команди в грі «Що? Де? Коли?» за допомогою штучних нейронних мереж	10
Мельников О. Ю., Кадацький М. А.	Задачі визначення дальності польоту ядра шляхом нейромережевого моделювання з урахуванням параметрів спортсменів та додаткових факторів	12
Василевський В.О., Романюк О.В.	Недоліки використання модульного тестування як основної технології тестування	14
Яремчук С.І., Шупіков О.А., Корнєєв А.А.	Другий алгоритм Гоморі в розв'язанні мінімаксної задачі розміщення джерел	16
Турчин М.Б., Чижмотря О.В.	Інформаційно-довідкова система пошуку медикаментів	18
Мощицький Р.Ю., Чижмотря О.В.	Інструментальні засоби для розробки комп'ютерних ігор	19
Василишин М.І., Чижмотря О.Г.	Мобільний додаток «AR меню для харчового закладу»	21
Стахівський Т.І.,	Web-орієнтована система типу «со-	23

ЗМІСТ

Чижмотря О.В.	ціальна мережа»	
Цукрук В.І., Романюк О.В.	Розрахунок бойових характеристик персонажів ігрового Telegram-боту	25
Котлярчук Д.В., Романюк О.В.	Аналіз методу чек-лістів для тестування графічного інтерфейсу	27
Мельниченко М.В., Чижмотря О.Г.	Система розпізнавання облич	30
Дашкевич В.В., Марчук Г.В.	Сервіс для керування тренажерним залом, клієнтська частина	32
Безкоровайна Ю.М.	Верифікація та валідація програмного забезпечення замовником	33
Безуглий В.О., Петросян Р.В.	Сучасні сайти як прогресивні веб-додатки	35
Сікайло В.О., Марчук Г.В.	Дослідження процесів використання патернів проектування при розробці ігор	37
Красиленко В.Г., Нікітович Д.В.	Протоколи узгодження секретних ключів у вигляді матричних перестановок значної розмірності для криптографічних перетворень	39
Пулеко І.В., Свінцицька О.М.	Програмне забезпечення моделювання динаміки рухливих об'єктів на основі кватерніонів	50
Голубенко О.І., Грищенко О.О., Дударєва Г.О.	Аналіз ефективності використання вектора показників зсуву кільцевого коду	52
Марчук Г.В., Лисогор Ю.І., Мисливий М.В.	Розпізнавання монет України з використанням компютерного зору	54
Грищенко В.О., Марчук Г.В.	Екосистема для пошуку тимчасової роботи, або робітника	56

Секція 2. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Бидюк П.И., Гамидов Г.И., Кязимов Т.Г., Гасанов А.С.	Информационные технологии моделирования и прогнозирования нелинейных нестационарных процессов	58
Завертайло К.С., Хошаба О.М.	Управление процессами взаимных блокировок в операционной системе Unix	60
Мірошніченко С.І., Байдацький Й.С.	Інформаційна система ведення обліку кадрів військової частини	62
Свінцицька О.М.	Інформаційні технології в управлінні внутрішніми комунікаціями ІТ-проектів	64
Пількевич І.А., Мудрик В.В.	Інформаційна система електронного документообігу військової частини	66
Хошаба О.М.	Решение некоторых проблем балансировщиков нагрузки	68
Чумакевич В.О., Погрібний А.П., Чумакевич В.В.	Визначення тиску ґрунтів та побудова геологічного розрізу на будівельному майданчику	70
Пількевич І.А., Мірошніченко С.І., Гаряжа Д.В.	Інформаційна система обліку майна служби озброєння військової частини	72
Абрамчук М.В., Сугоняк І.І., Ковальчук В.Н.	Веб-додаток для розпізнання рукописного тексту онлайн	74
Левківський В.Л.	Дослідження алгоритмів інтелектуального аналізу статистичних даних медичного спрямування	76
Ячменьов Я.О., Панаріна І.В.	Система інтеграції Magento 2 у WordPress	78
Ткаченко О.М., Підмогильний О.О.	Інтервальні нейронні мережі як детектори нестабільності для реконструкції астрономічних зображень екзопланет	80
Чумакевич В.О.,	Застосування технологій 3D скану-	82

Остапов В.В., Мальчишин П.І.	вання для контролю якості будівельних робіт	
Вишнівський В.В., Серих С.О.	Реалізації мереж SDN обладнанням Hewlett Packard Enterprise	84
Катков Ю.І., Зінченко О.В.	Застосування системи керування контейнерами операційними системами для розгортання критичних мікросервісних додатків	86

Секція 3. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА

Байлюк Є.М., Непша І.О.	Аналіз протоколу DNS over HTTPS	88
Філатов К.А., Покотило О.А.	Розробка локальної мережі в межах офісу	90
Кобрин А.Г., Оринчак І.А.	Навчально-тренувальний комплекс «IPTester»	92
Горбенко А.А.	Кібербезпека освітнього середовища в умовах карантину	94
Сіденко В.П., Андрієвич В.М.	Системи єдиного часу на базі платформи Arduino	97
Околита Д.О., Вакалюк Т.А.	Охоронна система безпеки для квартир	99
Lobanchukova N., Kreditsar S.	Methodology For Perimeter Security Systems Creation	101

Секція 4. ЦИФРОВА ОБРОБКА ЗОБРАЖЕНЬ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Чан А. Л. В., Романюк О. Н.	Аналіз моделі відбивної затності поверхні Кука-Торренса	103
Sergey Vyatkin, Romaniuk O.N., Romaniuk O.V.	Face Recognition Based On Binocular Stereo Reconstruction	105
Романюк О.Н., Кокушкін В.М., Чехместрук Р.Ю.,	Методи реконструкції зображень обличчя	108

Перун І.В.		
Вяткин С.И., Романюк О.Н., Денисюк А.В., Кокушкін В.М.	Метод активной модели внешнего вида	111
Sergey Vyatkin, Romaniuk O. N., Romaniuk O. V.	Method For Calculating The Depth Map From a Stereo Pair	113
Романюк О.Н., Мельник О.В., Панфілова Ю.О.	Деякі застосування гексагональної моделі пікселя	116
Лугових О.О.	Розробка системи для визначення параметрів руху технологічного обладнання	118
Подчашинський Ю.О. Воронова Т.С. Шавурська Л.Й.	Моделювання системи вейвлет-стиснення для відеозображень з вимірювальною інформацією структур природного походження в автоматизованих системах управління	120
Древа С.В., Лугових О.О.	Автоматизована система охорони для офісного приміщення	122
Безвесільна О.М., Чепюк Л.О.	Фільтрація вихідного сигналу струнного гравіметра	124
Олійник М.В., Лугових О.О.	Автоматизована система контролю серцебиття для пацієнтів лікарні	127
Подчашинський Ю.О., Чепюк Л.О.	Порівняння фрактального і вейвлетного підходів до стиснення зображень	129
Майданюк В.П.	Двовимірна апроксимація при фрактальному ущільненні зображень	131
Чепюк Л.О.	Визначення оптимальних параметрів цифрових обчислювальних пристроїв для визначення геометричних ознак виробів з природного каменю	133

**Секція 5. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ.
ПРИЛАДОБУДУВАННЯ**

Zosimovych N.	Uav Autopilot Controller With Test Dynamics Model Platform	135
Безвесільна О.М., Ткачук А.Г., Кравчук А.Р.	Жорсткість та демпфування систем стабілізації озброєння легкої броньованої техніки	139
Гурковская С.С.	Математическое моделирование напряженно-деформированного состояния обечаек при их формовке	141
Рафальська М.В., Ткачук А.Г., Безвесільна О. М.	Аналіз факторів впливу на точність стрільби озброєння легкої броньованої техніки	143
Ткачук А.Г., Янчук В.М., Кузьменко К.В.	Автоматизовані приводи наведення озброєння легкої броньованої техніки у горизонтальній площині	145

**Секція 6. БІОТЕХНІЧНІ ТА МЕДИЧНІ АПАРАТИ, СИСТЕМИ
ТА ТЕХНОЛОГІЇ**

Сілі І.І.	Розрахунок усередненого електромагнітного поля в рослинному середовищі картоплі	147
Ткачук А.А., Ткачук Р.А., Яненко О.П.	Автоматизована система тестування імплантатів для регулювання внутрішньоочного тиску	149
Яненко О.П., Перегудов С.М., Шевченко К.Л., Грубник Б.П.	Мікрохвильві випромінювання природних матеріалів для фізіотерапії	151
Хоменко Ж.М.	Дослідження оптичних властивостей біологічних тканин і практичне застосування результатів в спектрофотометрії	153
Коренівська О.Л., Шпак О.О.	Теоретичні засади вимірювання швидкості осідання еритроцитів	155
Коломієць Р.О.,	Схемотехнічні принципи побудови	157

Нікітчук Т.М., Морозов Д.С.	генераторів холодної плазми для медичного застосування	
Петров М.Ю., Чухов В.В., Мартинчук П.П.	Лабораторний макет для дослідження оптрона із зовнішнім фотонним зв'язком	159
Косюк І.Г., Чухов В.В., Мартинчук П.П.	Лабораторний макет для дослідження тахометричного перетворювача на оптроні із зовнішнім фотонним зв'язком	161
Коренівська О. Л. Бенедицький В. Б. Маляренко Н. П	Система моніторингу якості повітря в палатах та відкритих просторах	163
Секція 7. ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА		
Семенов А.О., Квітчук Я.В., Савчук П.П.	Дослідження хаотичної динаміки мікрохвильових радіотехнічних пристр-роїв на основі одиничного переходу Джозефсона	165
Семенов А.О., Куляс Р.О., Пінаєв Б.О.	Дослідження характеристик базових логічних пристроїв мікрохвильового діапазону на основі резонансно-ту- нельних діодів	167
Березовська В.О., Бондарчук В.В.	Особливості частотно - територіального планування систем мобільного зв'язку	169
Письменник О.В., Романчук С.Ю.	Використання високошвидкісних технологій бездротового зв'язку для передачі даних з безпілотного літального апарату	171
Ципоренко В.В., Іщук Т.Г., Скочко А.Я.	Дослідження антенної системи пеленгаторів комплексу радіомоніторингу	173
Ципоренко В.В., Міткевич Б.А., Кравченко Є.В.	Дослідження ширококутового прий- мального радіомодуля	175
Ципоренко В.Г., Ващенко М.А.,	Програмно-конфігурована система моніторингу стрілецького полігону	177

Меньшикова І.В.		
Ципоренко В.В., Рябченко В.О.	Розробка пристрою дистанційного керування	179
Ципоренко В.Г., Мартинюк Р.П., Сиротюк С.С.	Система спостереження з адаптивною топологією	181
Ципоренко В.Г., Матвійчук А.С., Сергійчук М.І.	Автоматизована система охорони вантажів потягу	183
Дубина О.Ф., Якобчук Д.Р., Дрозд П.А.	Аналіз камер відеоспостереження	185
Дубина О.Ф., Предчук Т.В., Сергійчук М.І.	Вплив ракурсу відеоспостереження на інформативність зображення	187

Секція 8. ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ В ОСВІТІ

Ткачук Г.В., Стеценко В.П., Стеценко Н.М.,	Особливості проведення онлайн-занять засобами сервісу Zoom в умовах дистанційного навчання студентів	189
Присяжнюк Г.Є., Кот Н.С., Сербин В.М.	Використання Learning Apps у навчанні математики	191
Усенко А.А., Вакалюк Т.А.	Автоматизована інформаційна система обліку успішності	193
Побідаш Д.С., Вакалюк Т.А.	Розробка web-орієнтованої навчальної системи	195
Баранов С.С.	Про актуальність розробки класифікації засобів навчання освітньої робототехніки	197
Сергієнко О.М.	Смарт-технології як засіб підготовки майбутніх педагогів з інформатики та комп'ютерної техніки	199

ЗМІСТ

Василенко А.С.	Комбінування засобів ІКТ в умовах дистанційного навчання	202
Кулімова Ю.Г.	Google-сервіси у процесі фахової освіти майбутніх учителів школи I ступеня	204
Мельников О.Ю., Сокольский О.С.	Функціональне проєктування інформаційно-навчальної системи для демонстрації і порівняння алгоритмів сортування та пошуку даних	206
Мар'єнко М.В.	Психолого-педагогічні особливості формування хмаро орієнтованої системи підготовки вчителів природничо-математичних предметів до роботи в науковому ліцеї	208
Черниш А.В., Бабюк Н.П., Большаков В. Н., Лефтеров А. В., Федосеев А. И.	Розробка алгоритму генерації кросвордів у заданій сітці	210
	Реберные точки субъектных компетенций	212
Ткачук Г.В.	До питання формування комунікативних умінь майбутніх учителів інформатики в умовах розвитку інформаційно-освітнього середовища	214
Джога Д.С.	Дистанційна освіта як новітня інформаційна технологія	216
Ярошик Я.В.	Інноваційні технології в системі освіти України	218
Дмитрієнко О.О.	Використання сервісу Zoom у дистанційному навчанні	220
Колеснікова І.В.	Цифрова трансформація сучасного освітнього процесу	222
Троян С.О.	Засоби навчання для забезпечення організаційно - педагогічних умов формування готовності до проєктної діяльності студентів педвузу на основі Java - технології	224

ЗМІСТ

Кривцова О.П.	Технологія візуального програмування в підготовці студентів	226
Кисельова О.Б.	Використання хмар слів в освітньому процесі	228
Ксензук Д.І., Коротун О.В.	Використання смартфонів для вивчення англійської мови у закладах загальної середньої освіти	230
Луцевич О.О., Сугоняк І.І., Ковальчук В.Н.	Освітня платформа для дітей дошкільного та молодшого шкільного віку	232
Замора Я.П.	Педагогічні програмні засоби ІКТ	234
Головня О.С.	Застосування електронного дистанційного курсу NDG Linux Essentials у навчанні операційних систем Unix/Linux	236
Сухіх А.С.	Здоров'язбережувальні умови використання програмно-апаратних засобів школярами під час дистанційного навчання	240

ПРОТОКОЛИ УЗГОДЖЕННЯ СЕКРЕТНИХ КЛЮЧІВ У ВИГЛЯДІ МАТРИЧНИХ ПЕРЕСТАНОВОК ЗНАЧНОЇ РОЗМІРНОСТІ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Вступ. Узагальнення відомих криптосистем з форматами даних скалярного типу на випадки матрично-тензорних форматів, поява та дослідження нового класу криптосистем матричного типу (КМТ) [1-4] на основі їх матрично-алгебраїчних моделей (ММ) криптографічних перетворень (КП) 2D(3D) - масивів, зображень (З), які мають ряд суттєвих переваг, сприяла інтенсифікації досліджень КМТ, ММ та демонстрації цілої низки нових їх покращень та застосувань [5-10]. Узагальнені ММ, матричні афінні та афінно-перестановочні шифри (МАПШ), їх модифікації досліджувались та використовувались при створенні сліпих та інших покращених цифрових підписів у [11-15]. ММ при їх апаратних реалізаціях легше відображаються на матричні процесори, мають розширені функціональні можливості, покращену крипто-стійкість, дозволяють перевіряти цілісність криптограм чорно-білих, кольорових зображень і наявність у них перекручувань [5,7], створювати блокові [6], параметричні [8], багатосторінкові [9] моделі з їх значною стійкістю [10]. Для КП у матричних моделях перестановок (ММ_П), з їх базовими процедурами множення матриць та деякими іншими по-елементними операціями за модулем над матрицями, матриці байтів, утворених з ряд-ків, колонок, векторів, що в унітарних чи інших кодах відображають символи, коди, байти, необхідно множити на матриці перестановок (МП). Процедури переставляння бітів, байтів чи їх груп є найбільш поширеними та обов'язковими практично для всіх відомих та новостворюваних алгоритмів та шифрів. Для збільшення ентропії криптограм З при їх КП на основі ММ_П та зміни їх гістограм необхідні декомпозиція R,G,B складових і їх бітових зрізів та декілька матричних ключів (МК) типу МП [3-5]. Низка таких псевдовипадкових (поточних, покрокових, по-фреймових) МК, які б відповідали вимогам, швидко генерувались, потрібна і для маскуванню, КП відео-файлів чи потоку блоків з файлів, зображень при їх значних розмірах. Постановка задачі. Таким чином, для ММ є необхідність формування низки МП, які б задовольняли ряду вимог, з головного МК. Оскільки питання узгодження головного МК загального виду, але не послідовності МП розглядалися в [16,17], а методи генерування потоку МК перестановок з головного МК частково розглядалися в [18], але тільки для бітових МП невеликих розмірів (256*256), то метою роботи є спроба запропонувати та дослідити протокол узгодження секретного (головного) МК у вигляді МП значної розмірності, тобто ГМП, удосконалити та адаптувати вид, структуру ГМП такої чи ще значнішої розмірності до формату З і до швидких апаратних рішень, промодельовати цей протокол та процес формування потоку МП з такої ГМП для ММ КП у системах МТ.

Виклад основного матеріалу та результатів дослідження. Огляд МТ шифрів, особливо багатофункціональних параметричних блочних [4], їх аналіз показують, що доцільно використовувати для досягнення мети ізоморфність різних представлень перестановок (матриць чи векторів), що виступають у ролі головного ключа (ГК) та по-блокових чи покрокових, раундових МК типу МП, тобто під-ключів (ПК), що являють собою матриці перестановок Р (її степені !) чи ізоморфні їм вектори. З робіт [6,8,9] відомо, що при КП на основі МАПШ, ВАПШ криптограми для деяких видів текстово-графічних документів (ТГД) і З, особливо для поблочних ММ, при використанні одного ПК для всіх блоків є недостатніми по стійкості, та попри це низка ПК, що створюються з ГК, вирішує цю проблему. А тому важливим є аспект узгодження секретного ГК типу МП значної розмірності. Розглянемо ситуацію, коли для КП блоків довжиною 256*256 байтів, що представлені у вигляді матриці чорно-білого зображення необхідно переставити всі байти у відповідності до МП. В цьому випадку МП в загально прийнятому вигляді повинна бути квадратною з $N*N$ елементами («0» чи «1»), де $N=2^{16}$. Потужність множини можливих таких МП, тобто їх кількість оцінюється, як $N!$, що дає для цього N колосальні значення. Але кожен адресу байту блоку можна представити і за допомогою двох байтів, що вказують дві координати (рядок та стовпчик) блоку. Це дає нам можливість двома блоками (256*256 елементів) байтів представляти любую перестановку, ставлячи в кожній однаковій адресі цих блоків відповідну старшому байту (в першому блоці) та молодшому байту (в другому блоці) координати нової адреси вибраного для перестановки байту. Вигляд програмного модуля у Mathcad для генерування базового (головного) МК (МП) та вигляд його складових KeyA та KeyB у форматі двох чорно-білих зображень показано на рис.1. Отже, любую МП можна однозначно відобразити двома матрицями розміром 256*256, елементами яких приймають значення з діапазону 0-255, з тією особливістю, що кожна з 256 їх градацій інтенсивності в кожній з цих двох матриць (З) повторюється рівно по 256 раз. Гістограми складових KeyA та KeyB МП зображені на рис.2 та мають вигляд горизонтальних ліній, як і очікувалось. Відмітимо, що таке ізоморфне у вигляді двох зображень представлення МП дає нам можливість використати ці складові KeyA та KeyB у якості двох секретних МК загального типу, наприклад, як адитивний та мультиплікативний ключі у МАПШ чи іншій ММ. Про це свідчать результати моделювання КП зображення (Im) МАПШ за допомогою запропонованої МП та її складових, як ключів, що показані на рис. 3 з матрицями явного З (Im), проміжних, його криптограм (Сmap) та перевірних З [19]. А гістограми явного З, його криптограм після кожного КП афінними складовими цієї МП зображені на рис.2.

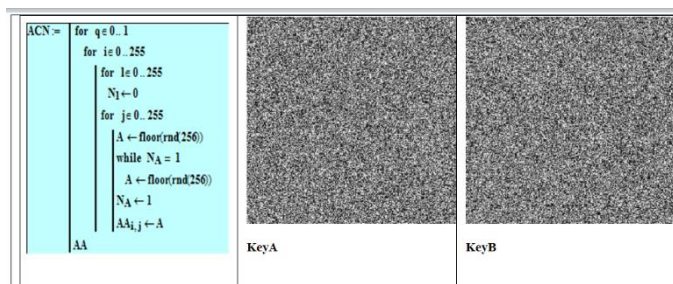


Рис. 1. Програмний модуль для генерування базового (головного) МК (МП) та вигляд складових KeyA та KeyB у форматі двох чорно-білих зображень (Вікно Mathcad).

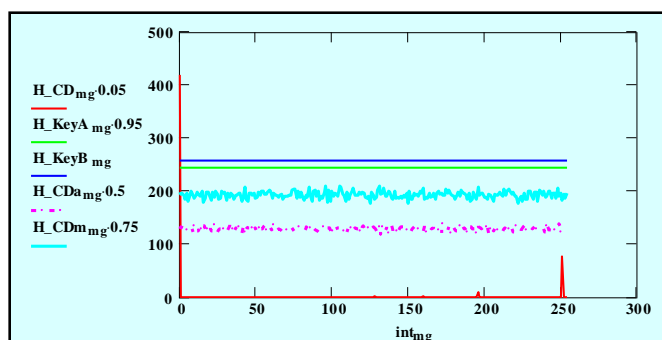


Рис. 2. Гістограми H_{KeyA} та H_{KeyB} відповідно складових KeyA та KeyB МП, гістограма H_{CD} криптограми явного З (співпадає з гістограмою З), відповідні гістограми H_{CDa} та H_{CDm} криптограм після адитивної та мультиплікативної афінних КП З за допомогою тих же KeyA та KeyB (Вікно Mathcad).

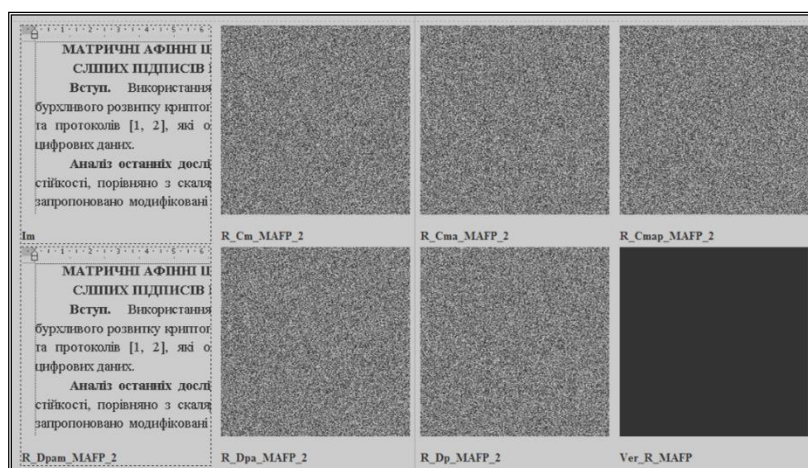


Рис. 3. Результати моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК. Верхній ряд, зліва направо: явне, після перетворень, криптограма після МАПШ; Нижній ряд: відновлене, проміжні та різницеве (праворуч) зображення ТГД.

Ці модельні експерименти підтвердили, що КП МАПШ наявними 2-ма складовими МП дають якісні криптограми CD_{ImAa} та CD_{ImAm} , гістограми яких H_{CDa} та H_{CDm} настільки близькі до рівномірного закону розподілу, що навіть для З (Im) з ентропією 0,738 ентропія криптограм відрізняється від теоретично максимальної (8 біт) всього на долі відсотка, збільшуючись аж до 7,99. Результати моделювання МАПШ та багатокрокових МАПШ для різних випадків, коли спочатку виконуються складові афінних перетворень і у іншій послідовності та різними чи одним МК від МП, а потім перестановка за допомогою МП, чи навпаки, також засвідчили подібні якісні КП при застосуванні пропонованих представлень МП. Але для всіх модифікацій МАМ при таких МП, потужність множини яких оцінюється значною величиною $N! = (256 \cdot 256)!$, є надважливим питання узгодження сесійної секретної ГМП. А тому, узагальнюючи наш підхід, можна стверджувати, що для синтезу ГМП зі значно більшою розмірністю останні можна також однозначно представити за допомогою З, 4 і т.д. зображень-матриць чи блоків з байтів, аналогічних вищевказаним складовим KeyA та KeyB.

Розглянемо сутність самого протоколу узгодження ГМП сторонами. Нехай є сторони: x (Alisa) та y (Bob). Допустимо, що відома одна МП з множини допустимих у вигляді складових KeyA та KeyB, що показана на рис. 4. Крім того, завжди існує МП зворотної перестановки, що для вибраного представлення має вигляд 2-х З KeyAO та KeyBO. Кожна з сторін на першому кроці підносить ізоморфно ГМП у вибрану ними свою

секретну степінь (у нас 11 та 17 для прикладу!), пересилає нову МП іншій стороні та на другому кроці сторону отримані нові МП аналогічно підносять їх у ті ж свої випадкові секретні степені. Тут аналогія з протоколом Діффі-Хелмана. На рис. 5-8 показані результати моделювання цих двох кроків протоколу узгодження секретного МК у Mathcad, а на рис.9-10 вигляд отриманих проміжних та результативної секторної ГМП у ізоморфному представленні 3. Сторони не знають степені іншої сторони, але отримані ними МП є ідентичними, що видно з рис. 10.

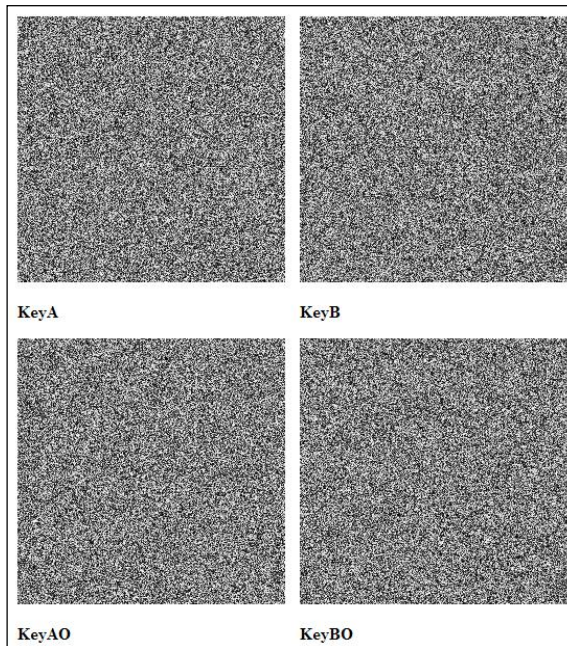


Рис. 4. Вигляд (2D) відомих генерованих МП: вгорі (пряма), внизу (зворотна) перестановки.

Таким чином піднесення МП ($N*N$ бінарних, де $N=2^{16}$) еквівалент-но замінюється швидкими перестановками, які до того ж можуть бути ще більш прискореними при значних степенях за рахунок використання деякого базового набору фіксованих (фіксовані степені ГМП) та специфічної їх послідовності, що дає досягнення суттєвих переваг за рахунок прискорень обчислення степенів ГМП, простоти можливих реалізацій і зменшення затрат.

```

Alisa_xc := 11
Ax_P(Alisa_x) :=
p ← 0
S ← KeyA
while p < Alisa_x
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,jKeyB1,jKeyBKeyAi,jKeyBi,j
      W
  p ← p + 1
S

Bx_P(Alisa_x) :=
p ← 0
S ← KeyB
while p < Alisa_x
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,jKeyB1,jKeyBKeyAi,jKeyBi,j
      W
  p ← p + 1
S
  
```

Рис. 5. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (11!) стороною x (Alisa).

```

Bob_yc := 17

Ay_P(Bob_y) :=
p ← 0
S ← KeyA
while p < Bob_y
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,j,KeyB1,j · KeyBKeyAi,j,KeyB1,j
    W
  p ← p + 1
S

By_P(Bob_y) :=
p ← 0
S ← KeyB
while p < Bob_y
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,j,KeyB1,j · KeyBKeyAi,j,KeyB1,j
    W
  p ← p + 1
S

```

Рис. 6. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (17 !) стороною у (Bob).

```

Axy_P(Alisa_x) :=
p ← 0
S ← Ay_P(Bob_yc)
while p < Alisa_x
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,j,KeyB1,j · KeyBKeyAi,j,KeyB1,j
    W
  p ← p + 1
S

Bxy_P(Alisa_x) :=
p ← 0
S ← By_P(Bob_yc)
while p < Alisa_x
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,j,KeyB1,j · KeyBKeyAi,j,KeyB1,j
    W
  p ← p + 1
S

```

Рис. 7. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в отриманій від у новій МП, ізоморфних піднесенню у потрібну степінь (11 !) стороною x (Alisa).

```

Ayx_P(Bob_y) :=
p ← 0
S ← Ax_P(Alisa_xc)
while p < Bob_y
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,j,KeyB1,j · KeyBKeyAi,j,KeyB1,j
    W
  p ← p + 1
S

Byx_P(Bob_y) :=
p ← 0
S ← Bx_P(Alisa_xc)
while p < Bob_y
  S ←
  for i ∈ 0..255
    for j ∈ 0..255
      Wi,j ← SKeyAKeyAi,j,KeyB1,j · KeyBKeyAi,j,KeyB1,j
    W
  p ← p + 1
S

```

Рис. 8. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в отриманій від x новій МП, ізоморфних піднесенню у потрібну степінь (17 !) стороною у (Bob).

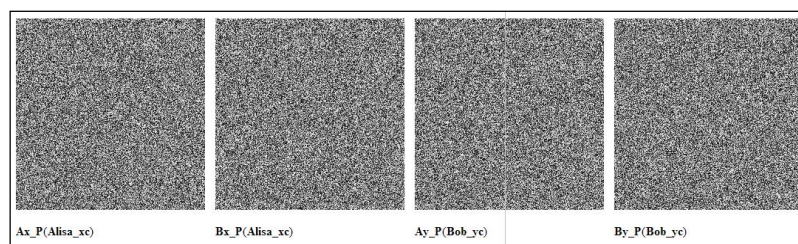


Рис. 9. Отримані сторонами нові МП (кожна у вигляді їх двох складових) після першого кроку протоколу, ті що пересилаються іншій стороні.

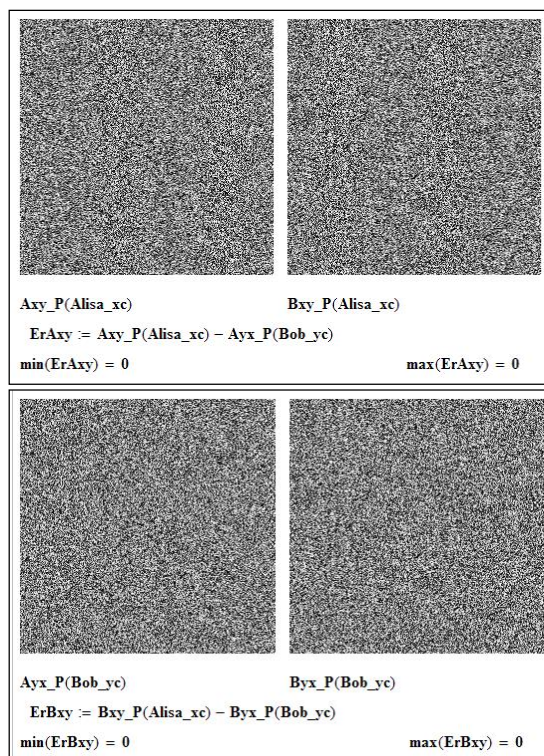


Рис. 10. Отримані сторонами ідентичні нові МП (кожна у вигляді їх двох складових) після другого кроку протоколу, тобто секретна МП.

Використовуючи розроблені функціональні параметричні моделі КП за допомогою узгодженого пропонуваного протоколом секретного МК, що показані вище, було виконано перевірку правильного до вимог їх синтезу та адекватності моделей шляхом прямого та зворотного КП З, що було показано на рис. 1-3. Отримані моделюванням у Mathcad результати підтверджують правильність протоколу, а аналіз стійкості, що буде представлений детальніше у доповіді, показує неможливість здійснення атак внаслідок величезної множини можливих МП.

Висновки. Запропоновано протокол узгодження секретного ключа у вигляді ізоморфних представлень МП значних розмірностей, виконано модельні експерименти, що підтвердили адекватність функціонування моделей та пропонуваного протоколу і методів генерування МП, їх переваги. Моделі прості, зручні, адаптуються для різноформатних та кольорових зображень, реалізуються матричними процесорами, мають високі ефективність, стійкість, швидкодію.

Список літературних джерел

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. НУ "Львів. політехніка". - 2009. - № 658. - С. 59-63.
2. 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
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 Хмельн. НУ. Технічні науки. - 2014. - № 1. - С. 74-79.
4. 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> .

5. 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

6. Красиленко В.Г. Моделі блокових матричних афінно-перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження / В.Г. Красиленко, Д.В. Нікітович // 72 НТК: матеріали конференції (13-15 грудня 2017 р.). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.117-122.

7. 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. НПК– К., 2010. – С.120-124.

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

9. Красиленко В.Г. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей ІХ Міжнародної НТК, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 73-77.

10. Красиленко В.Г. Дослідження покращеного багатокрокового 2D RSA шифру та його гістограмно-ентропійних характеристик / В.Г. Красиленко, Д.В. Нікітович // «Інформаційна безпека та комп'ютерні технології»: Збірник тез доповідей ІІІ Міжнародної НПК, 19-20 квітня 2018 року. – Кропивницький: ЦНТУ, 2018. – С. 78-82. Режим доступу: <http://it-kntu.kr.ua/wp-content/uploads/2015/01/Zbirnyk-tez-InfoSecCompTech-2018.pdf>

11. 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.

12. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р.О. Яцковська, Ю.М. Тріфонова. // Системи обробки інформації. – 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

13. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції «Інформаційні управлінські системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: «ВидавІнформ НУ «ОМА», 2017. - С. 312 -318.

14. Красиленко В.Г. Моделювання покращених сліпих електронних цифрових підписів 2D типу / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей ІХ Міжнародної науково-технічної конференції, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 78-82.

15. Красиленко В.Г. Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису / В.Г. Красиленко, Д.В. Нікітович, Р.О. Яцковська, В.І. Яцковський // Системи обробки інформації: збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2019. – Вип. 1 (156). – С. 92-100. – [Електронний ресурс]. – Режим доступу: <https://doi.org/10.30748/soi.2019.156.12>

16. 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.

17. Красиленко В.Г. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: ЛНТУ, 2017. – Вип. 26. – С 111-120. - Режим доступу: <http://ki.lutsk-ntu.com.ua/node/134/section/27> .

18. Красиленко В.Г. Моделювання процесів генерування матричних ключів / В.Г. Красиленко, Д.В. Нікітович // «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2018): Збірник тез доповідей ІV Міжнародної науково-практичної конференції, 17-18 травня 2018 року.–Черкаси: ЧДТУ, 2018. – С. 32-35. Режим доступу: <https://chdtu.edu.ua/itont-2018/materiali-konferentsiji>

19. Красиленко В.Г. Моделювання методів генерування потоків матричних перестановок значної розмірності для криптографічних перетворень зображень // В.Г. Красиленко, Д.В. Нікітович // Тези доповідей ІІ Всеукраїнської науково-технічної конференції Комп'ютерні технології: інновації, проблеми, рішення (14 – 15 листопада 2019 р.) . – Житомир: Житомирська політехніка, 2019. – С. 67-77. – Режим доступу: <https://conf.ztu.edu.ua/wp-content/uploads/2019/12/67-1.pdf>