НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра обчислювальної техніки

«На правах рукопису»
УДК __004.052.42___

До захисту допущено:

Завідувач кафедри

_____*Сергій СТІРЕНКО*

«___»_____2021 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-науковою програмою «Комп'ютерні системи та мережі»

зі спеціальності 123 «Комп'ютерна інженерія»

на тему: "Метод гомоморфного шифрування зображень при їх віддаленій обробці "

Виконав:
студент VI курсу, групи ІВ- з01мп
Маслачков Олексій Юрійович _____

Керівник:
доц., к.т.н., доц.,
Марковський Олександр Петрович _____

Консультант з нормоконтролю:
професор, д.т.н., професор,
Кулаков Юрій Олексійович _____

Рецензент:
Декан ФПМ, д.т.н., професор
Дичка Іван Андрійович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет (інститут) *Інформатики та обчислювальної техніки*
(повна назва)

Кафедра *Обчислювальної техніки*
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-науковою програмою
Спеціальність *123. Комп'ютерна інженерія*
(код і назва)

Спеціалізація *123. Комп'ютерні системи та мережі*
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Стіренко С.Г.
(підпис) (ініціали, прізвище)
« » _____ 20***21*** р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Маслачкову Олексію Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема дисертації Метод гомоморфного шифрування зображень при їх віддаленій обробці

Науковий керівник дисертації доц.,к.т.н., доц. Марковський О.П.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «1» лютого *2021* р. № 3132-с

2. Строк подання студентом дисертації *26 квітня* 2021 *р*

3. Об'єкт дослідження *процеси гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах.*

4. Предмет дослідження *методи гомоморфного шифрування зображень під час їх середньоарифметичної фільтрації на віддалених комп'ютерних системах, які виключають можливість отримання несанкціонованого доступу до реальних даних зображень та дозволяють значно прискорити обробку зображень.*

5. Перелік завдань, які потрібно розробити: *Аналіз задач захищеної віддаленої обробки зображень та огляд існуючих методів їх гомоморфного шифрування. Розробка методу гомоморфного шифрування зображень при їх віддаленій середньоарифметичній фільтрації. Організація використання розробленого методу для захищеної фільтрації потоків зображень. Розробка програми моделювання процесів віддаленої обробки зображень з використанням гомоморфного шифрування.*

6. Консультанти розділів дисертації:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Кулаков Ю.А., професор		

7. Дата видачі завдання 01.02.2021

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів дисертації	Примітка
1.	*Затвердження теми роботи*	*10.09.2021-15.09.2021*	
2.	*Вивчення та аналіз завдання*	*15.09.2020-31.09.2021*	
3.	*Розробка архітектури та загальної структури системи*	*01.10.2021-10.10.2021*	
4.	*Розробка структур окремих підсистем*	*10.10.2021-8.11.2021*	
5.	*Програмна реалізація системи*	*9.11.2021-20.11.2021*	
6.	*Оформлення пояснювальної записки*	*20.11.2021-16.12.2021*	
7.	*Передзахист*	*16.12.2021*	
8.	*Захист*	*24.12.2021*	

Студент _____ О.Ю. Маслачков
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ О.П. Марковський
(підпис) (ініціали, прізвище)

РЕФЕРАТ

на магістерську дисертацію

виконану на тему: Метод гомоморфного шифрування зображень при їх віддаленій обробці

студентом: Маслачковим Олексієм Юрієвичем

Робота складається із вступу та 5 розділів. Загальний об'єм роботи: 99 аркушів основного тексту, 7 ілюстрації та 8 таблиць. Для виконання магістерської дисертації було використано інформацію з 77 літературних джерел.

Актуальність. В сучасних системах, що аналізують чи оброблюють зображення, надзвичайно поширеною є середньоарифметична фільтрації зображень. Зазвичай її виконують на початкових етапах обробки зображень з метою полішення їхньої якостза рахунок зменшення компоненти імпульсних завад. Висока ресурсоємність обробки зображень, що складаються з мільйонів пікселів, вказує на необхідність залучення потужних багатопроцесорних систем для виконання масової обробки зображень за допомогою фільтрації. Проте існують такі класи задач, при вирішенні яких Внаслідок цього виникає потреба розробки криптографічних методів захисту зображень в процесі їхньої віддаленої обробки на відкритих платформах. Основною вимогою, до них є високий рівень захищеності зображень як при передачі, так і в процесі самої обробки.

Таким чином, наукова задача забезпечення захисту зображень в процесі їх середньоарифметичної фільтрації на неконтрольованих віддалених обчислювальних системах великої потужності є актуальною та практично важливою для сучасного етапу розвитку комп'ютерних технологій.

Мета і завдання дослідження. Метою роботи є підвищення ефективності захищеної обробки зображень, зокрема їх середньоарифметичної фільтрації на віддалених обчислювальних потужностях за рахунок розробки перестановочного методу гомоморфного шифрування зображень.

Для досягнення поставленої мети було поставлено та вирішено такі завдання:

1. Аналіз обчислювальних операцій обробки зображень і зокрема середньоарифметичної фільтрації, пошук методів шифрування зображень, інваріантних до характеру обчислень при виконанні фільтрації. Обґрунтування критеріїв ефективності гомоморфних шифрів для середньоарифметичної фільтрації зображень.

2. Критичний огляд з позицій визначених критеріїв, існуючих методів гомоморфного шифрування зображень для їх захищеної обробки на віддалених обчислювальних системах.

3. Розробка методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на основі перестановочних шифрів.

4. Теоретична оцінка показників ефективності перестановочних гомоморфних шифрів для захисту зображень при середньоарифметичної фільтрації на віддалених обчислювальних системах.

5. Розробка програмних засобів для моделювання перестановочних гомоморфних шифрів для захисту зображень при середньоарифметичної фільтрації на віддалених обчислювальних системах. Експериментальне дослідження з використанням цих програмних засобів ефективності запропонованого методу гомоморфного шифрування зображень.

Об'єкт дослідження – є процеси гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах.

Предмет дослідження – методи гомоморфного шифрування зображень під час їх середньоарифметичної фільтрації на віддалених комп'ютерних системах, які виключають можливість отримання несанкціонованого

доступу до реальних даних зображень та дозволяють значно прискорити обробку зображень.

Методи дослідження базуються на теорії ймовірності та математичної статистики, теорії булевих функцій та комбінаторики, теорії організації обчислювальних процесів, а також на використанні методів моделювання.

Наукова новизна одержаних результатів полягає в наступному:

Теоретично обґрунтовано, розроблено та досліджено метод гомоморфного шифрування зображень для захисту їх під час середньоарифметичної фільтрації на віддалених комп'ютерних системах, відмінністю якого є використання в якості основного елементу захисту перемішування стовпців матриці зображень в секретному порядку. В рамках розробленого методу визначено процедури часткової середньоарифметичної фільтрації, яка здійснюється на віддалених системах, а також процедури завершальної фази фільтрації, яка виконується на обчислювальній платформі користувача після гомоморфного дешифрування отриманого із хмари зображення.

Практичне значення одержаних результатів роботи визначається тим, що їх використання забезпечує прискорення виконання задач фільтрації зображень за рахунок використання віддалених обчислювальних потужностей, забезпечуючи при практичну неможливість доступу до зображень. Це, в свою чергу, дозволяє значно підвищити оперативність обробки аерокосмічних зображень, організувати функціонування в захищеному режимі широкого класу роботизованих систем з функціями технічного зору в реальному часі.

Особистий внесок здобувача полягає в теоретичному обґрунтуванні одержаних результатів, їх експериментальній перевірці та дослідженні, а також у створенні програмних продуктів для практичного використання одержаних результатів.

Апробація результатів магістерської дисертації. Основні результати магістерської дисертації доповідались, обговорювались та отримали позитивну оцінку на семінарах кафедри обчислювальної техніки.

Ключові слова

Середньоарифметична фільтрація, захищені обчислення, захищена обробка зображень, хмарні обчислення, хмарні технології.

ЗМІСТ

Стр.

ВСТУП …….. 3

РОЗДІЛ 1. ……. 7

АНАЛІЗ ЗАДАЧ ЗАХИЩЕНОЇ ВІДДАЛЕНОЇ ОБРОБКИ ЗОБРАЖЕНЬ ТА ОГЛЯД ІСНУЮЧИХ МЕТОДІВ ЇХ ГОМОМОРФНОГО ШИФРУВАННЯ

1.1 Аналіз обчислювальних процедур обробки зображень ……..…. 8

1.2 Огляд сучасних схем гомоморфного шифрування даних ……..… 15

1.3 Аналіз існуючих гомоморфних шифрів для захисту ……... 20
зображень при їх віддаленій фільтрації

Висновки до розділу 1 ……... 24

РОЗДІЛ 2 ……..….. 26

РОЗРОБКА МЕТОДУ ГОМОМОРФНОГО ШИФРУВАННЯ

ЗОБРАЖЕНЬ ПРИ ЇХ ВІДДАЛЕНІЙ ФІЛЬТРАЦІЇ

2.1. Метод гомоморфного шифрування зображень для їх ……..... 27

захищеної середньоарифметичної фільтрації

2.2 Оцінка ефективності методу ……..……. 36

Висновки до розділу 2 ……...……. 44

Р О З Д І Л 3 …… 46
ОРГАНІЗАЦІЯ ВИКОРИСТАННЯ РОЗРОБЛЕНОГО МЕТОДУ ДЛЯ ЗАХИЩЕНОЇ ФІЛЬТРАЦІЇ ПОТОКІВ ЗОБРАЖЕНЬ

3.1 Організація захищеної групової середньоарифметичної фільтрації ….. 47

зображень з використанням перемішування стовпців

3.2 Оцінка ефективності …….. 51

Висновки до розділу 3 …… 53

РОЗДІЛ 4 …….. 54
РОЗРОБКА ПРОГРАМИ МОДЕЛЮВАННЯ ПРОЦЕСІВ ВІДДАЛЕНОЇ ФІЛЬТРАЦІЇ ЗОБРАЖЕНЬ З ВИКОРИТАННЯМ ГОМОМОРФНОГО ШИФРУВАННЯ

4.1 Організація даних програми ……..…… 55

4.2 Розробка процедур програми ……..……... 58

4.3 Експериментальне дослідження методу гомоморфного ……. 63
шифрування зображень при їх середньоарифметичній фільтрації
з використанням розробленої програми

Висновки до розділу 4 ……. 73

РОЗДІЛ 5 …….. 75

РОЗРОБЛЕННЯ СТАРТАП–ПРОЕКТУ

5.1. Опис проблеми …….. 75

5.2 Аналіз ринкових можливостей запуску стартап-проекту …….…….. 80

Висновки до розділу 5 …….…… 88

В И С Н О В К И ……..…….. 90

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ……..…… 93

Додаток А. Лістінги програми …….. 100

ВСТУП

Актуальність. Основна ціль комп'ютерної обробки зображень полягає в здійсненні їх автоматичного розпізнавання та аналізу. Цей процес включає в себе декілька етапів, які виконуються послідовно: один за одним. Важливим в цьому ряду є етап актуалізації зображення, тобто видалення з нього елементів, які не несуть корисної інформації для вирішення конкретної задачі аналізу зображення [33]. Основним елементом процесу актуалізації зображення виступає його фільтрація. Крім виконання задачі актуалізації, фільтрація зображень забезпечує підвищення їх якості шляхом видання завад, що утворилися під час одержання та в процесі передачі зображення [34].

В сучасних системах, що аналізують чи оброблюють зображення, надзвичано поширенною є середньоарифметична фільтрації зображень. Зазвичай її виконують на початкохи етапах обробки зображень з метою полішенн їхньої якостза рахунок зменшення компоненти імпульсних завад. Висока ресурсоємність обробки зображень, що складаються з мільйонів пікселів, вказує на необхідність залучення потужних багатопроцесорних систем для виконання масової обробки зображень за допомогою фільтрації. Проте існують такі класи задач, при вирішенні яких конфіденційність оброблюваних даних є ключовою. Зокрема, для деяких класів таких задач потребується обробка великої кількості зображень методом середньорифметичної фільтрації. Тобто цей клас задач не може бути розв’язаний з використанням відкритих багатопроцесорних систем. Внаслідок цього виникає потреба розробки криптографічних методів захисту зображень в процесі їхньої віддаленої обробки на відкритих платформах. Основною вимогою, до них є високий рівень захищеності зображень як при передачі, так і в процесі самої обробки.

Таким чином, наукова задача забезпечення захисту зображень в процесі їх середньоарифметичної фільтрації на неконтрольованих віддалених

обчислювальних системах великої потужності є актуальною та практично важливою для сучасного етапу розвитку комп'ютерних технологій.

Мета і задачі дослідження. Метою роботи є підвищення ефективності захищеної обробки зображень, зокрема їх середньоарифметичної фільтрації на віддалених обчислювальних потужностях за рахунок розробки перестановочного методу гомоморфного шифрування зображень.

Основні задачі дослідження у відповідності до поставленої мети полягають у наступному.

1. Аналіз обчислювальних операцій обробки зображень і зокрема середньоарифметичної фільтрації, пошук методів шифрування зображень, інваріантних до характеру обчислень при виконанні фільтрації. Обгрунтування критеріїв ефективності гомоморфних шифрів для середньоарифметичної фільтрації зображень.
2. Критичний огляд з позицій визначених критеріїв, існуючих методів гомоморфного шифрування зображень для їх захищеної обробки на віддалених обчислювальних системах.
3. Розробка методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на основі перестановочних шифрів.
4. Теоретична оцінка показників ефективності перестановочних гомоморфних шифрів для захисту зображень при середньоарифметичної фільтрації на віддалених обчислювальних системах.
5. Розробка програмних засобів для моделювання перестановочних гомоморфних шифрів для захисту зображень при середньоарифметичної фільтрації на віддалених обчислювальних системах. Експериментальне дослідження з використанням цих програмних засобів ефективності запропонованого методу гомоморфного шифрування зображень.

Об'єктом дослідження є процеси гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах.

Предметом дослідження є методи гомоморфного шифрування зображень під час їх середньоарифметичної фільтрації на віддалених комп'ютерних системах, які виключають можливість отримання несанкціонованого доступу до реальних даних зображень та дозволяють значно прискорити обробку зображень.

Методи дослідження базуються на теорії ймовірності та математичної статистики, теорії булевих функцій та комбінаторики, теорії організації обчислювальних процесів, а також на використанні методів моделювання.

Наукова новизна одержаних результатів полягає в наступному:

Теоретично обґрунтовано, розроблено та досліджено метод гомоморфного шифрування зображень для захисту їх під час середньоарифметичної фільтрації на віддалених комп'ютерних системах, відмінністю якого є використання в якості основного елементу захисту перемішування стовпців матриці зображень в секретному порядку. В рамках розробленого методу визначено процедури часткової середньоарифметичної фільтрації, яка здійснюється на віддалених системах, а також процедури завершальної фази фільтрації, яка виконується на обчислювальній платформі користувача після гомоморфного дешифрування отриманого із хмари зображення.

Практичне значення одержаних результатів роботи визначається тим, що їх використання забезпечує прискорення виконання задач фільтрації зображень за рахунок використання віддалених обчислювальних потужностей, забезпечуючи при практичну неможливість доступу до зображень. Це, в свою чергу, дозволяє значно підвищити оперативність обробки аерокосмічних зображень, організувати функціонування в захищеному режимі широкого класу роботизованих систем з функціями технічного зору в реальному часі.

Особистий внесок здобувача полягає в теоретичному обґрунтуванні одержаних результатів, їх експериментальній перевірці та дослідженні, а також у створенні програмних продуктів для практичного використання одержаних результатів.

Апробація результатів магістерської дисертації. Основні результати магістерської дисертації доповідались, обговорювались та отримали позитивну оцінку на семінарах кафедри обчислювальної техніки.

Р О З Д І Л 1

АНАЛІЗ ЗАДАЧ ЗАХИЩЕНОЇ ВІДДАЛЕНОЇ ОБРОБКИ ЗОБРАЖЕНЬ ТА ОГЛЯД ІСНУЮЧИХ МЕТОДІВ ЇХ ГОМОМОРФНОГО ШИФРУВАННЯ

Потреба у залученні значних за обсягом обчислювальних ресурсів характерна для практично всіх задач комп'ютерної обробки зображень. Значною мірою це зумовлено тим, що сучасні зображення складаються з мільйонів точок, а триваючий процес подальшого їх якості має наслідком збільшення кількості точок зображення. Крім того, сучасні алгоритми обробки зображень постійно ускладнюються.

Таким чином, тенденції використання комп’ютерного аналізу зображень у сучасних інформаційних технологіях вимагають значного збільшення обсягу обчислювальних ресурсів, темпи зростання яких значно випереджають прогрес потужності процесора [2].

Найбільш перспективний шлях кардинального прискорення комп’ютерної обробки зображень полігіє в залучення для вирішення прикладних завдань аналізу зображень практично необмежених обчислювальних ресурсів, що надають сучасні хмарні технології. Вони дозволяють інтегрувати потужності комп’ютерних систем в глобальному масштабі та надавати доступ до них широкому колу користувачів. З іншого боку, хмарні технології завдяки зазначеним вище чинникам забезпечують економічну ефективність суперкомп’ютерів за рахунок їх завантаження задачами користувачів з усього світу [3].

На сьогодні найбільшою перешкодою широкому впровадженню переваг технологій хмарних обчислень для обробки зображень є реальна загроза несанкціонованого доступу до них сторонніх осіб під час обробки на віддалених обчислювальних потужностях. Практично мова йде про обробку зображень користувача на обчислювальних системах, які не підконтрольні цим користувачам і є, відповідно, потенційно відкритими для несанкціонованого

доступу сторонніх осіб до зображень. Існуючий арсенал засобів шифрування інформації дозволяє забезпечити недоступність зображень лише в процесі їх передачі мережею Інтернет, але не забезпечує захищеності в процесі безпосередньої обробки зображень на віддалених комп'ютерних системах [4]. Для переважної більшості прикладних завдань комп'ютерного аналізу зображень питання недопущення до них сторонніх осіб є важливим.

Таким чином, наукова задача забезпечення захисту зображень у процесі їх дистанційної обробки, у тому числі фільтрації зображень на неконтрольованих користувачами віддалених комп'ютерних системах, є актуальною для сучасного етапу розвитку інформаційних та комп'ютерних технологій.

1.1 Аналіз обчислювальних процедур обробки зображень

На сьогоднішній день можна виділити доволі широкий клас прикладних задач, для вирішення яких здійснюється комп'ютерний аналіз та розпізнавання зображень. Для значної частини цих прикладних задач важливим є високий рівень оперативності обробки зображень та забезпечення конфіденційності. Це означає, що потрібно виключити можливість доступу до зображень сторонніх осіб. Зокрема це повною мірою стосується аерокосмічних зображень, баз даних портретів злочинців, зображень, пов'язаних з медициною та станом здоров'я людей.

Однім із найбільш дієвих шляхів досягнення можливості обробки в реальному часі полягає в використанні прогресивних хмарних технологій. Хмарні технології передбачають віддалене надання широкому колу користувачів,, на комерційній основі, певних ресурсів із загального в масштабах планети пулу. При цьому, в якості вказаних ресурсів можуть виступати обчислювальні потужності багатопроцесорних комп'ютерних систем, пам'ять глобальних сховищ інформації, а також програмне забезпечення. Надання користувачеві вказаних вище ресурсів реалізується виходячи з наявності вільних ресурсів у планетарному масштабі, так що користувач не знає

на яких обчислювальних потужностях вирішується його прикладне завдання або де зберігаються його персональні дані. Саме непрозорість для користувача процесу надання ресурсів і зумовила назву – хмарні технології.

Використання хмарних технологій значною мірою дозволяє вирішити проблему наявності певних обмежень в використанні наявних ресурсів для користувача: в рамках хмарних технологій кожному з них може бути надані значні за обсягом обчислювальні потужності сотень і тисяч процесорів сучасних багатопроцесорних комп'ютерних систем і суперкомп'ютерів, а також практично необмежений обсяг пам'яті для віддаленого зберігання його персональних даних.

Суттєвою перешкодою на шляху широкого використання можливостей хмарних технологій в плані підвищення продуктивності обробки даних користувачів і, зокрема, обробки зображень, постає відсутність до теперішнього часу ефективних механізмів захисту конфіденційних даних користувачів в процесі їх передачі та обробки на віддалених обчислювальних системах. Особливо гостро постає проблема захисту даних користувачів при їх обробці на віддалених і, відповідно, неконтрольованих обчислювальних системах. І якщо при передачі даних вони можуть бути захищені з використанням існуючих криптографічних механізмів шифрування, то при обробці проблема захисту даних користувачів і, зокрема, зображень, не знаходить прийнятного вирішення до теперішнього часу.

Швидкий розвиток інформаційних технологій стимулює стрімке і багатопланове розширення класу прикладних задач, вирішення яких передбачає комп'ютерний аналіз потоків зображень. В останні роки сильний поштовх розвитку технологій комп'ютерної обробки та аналізу зображень поява на ринку електронних пристроїв дешевих апаратних компонентів систем комп'ютерного зору [1] для робототехнічних систем. Це педалює прискорений прогрес системи, що мають функції технічного зору і працюють в режимі

реального часу. для застосувань цього класу висока швидкість комп'ютерної обробки зображень є важливим чинником ефективності.

Потреба в зростаючих обчислювальних ресурсах є характерною для всіх задачам комп'ютерної обробки зображень в силу того, що вони містять мільйони пікселів і подальше підвищення якості зображень прямо пов'язане зі збільшення кількості пікселів і ростом їх розрядності. Відмічається сталий процес ускладнення методів, процедур та алгоритмів обробки та комп'ютерного аналізу зображень.

Відповідно, тенденції використання комп'ютерної обробки і аналізу зображень в сучасних інформаційних технологіях потребують доручення дл вирішення цих задач значних за обсягом обчислювальних ресурсів. при цьому темпи росту потрібних для ефективної обробки зображень об'ємом обчислювальних ресурсів значно випереджають прогрес потужності процесорів [2].

До теперішнього часу виділяють ряд стандартизованих процедур комп'ютерної обробки зображень, які за цілями, що вони вирішують можна умовно розділити на наступні класи:

- процедури підвищення якості зображень, видалення імпульсних завад;
- процедури актуалізації зображень, тобто виділення інформації, потрібної для вирішення конкретної прикладної задачі;
- процедури перетворення зображень до виду, зручного для подальшого аналізу чи візуалізації:
- процедури аналізу зображень;
- процедури розпізнавання зображень.

До процедур підвищення якості зображень відносяться методи їх фільтрації: медіанна та середньоарифметична. Обидва згадані види фільтрації дозволяють підвищити якість зображень, шляхом видалення імпульсних шумів, що виникають в процесі формування та передачі зображень [1]. Суть цього виду обробки полягає в скануванні зображення квадратною апертурою

непарного розміру a з заміною центрального елемента поточної апертури на значення середнього арифметичного її точок при середньоарифметичній фільтрації або заміні середньої точки медіаною апертури при медіанній фільтрації.

Медіанна фільтрація - це специфічний вид цифрової обробки зображень , що має на меті зменшення або виключення імпульсних завад, в процесі якої здійснюються перетворення зображення, що підвищують його якість. Медіанна фільтрація, як вид обробки зображень відноситься до класу нелінійних фільтрів.

Середньоарифметична фільтрація, як і медіанна, спрямована на покращання якості зображень шляхом зменшення або повного видалення завад імпульсного характеру, які можуть виникати в процесі отримання або передачі зображення по ефірним зачумленим каналам. Принцип дії середньоарифметичної фільтрації полягає в тому, що зображення сканується квадратною апертурою визначеного розміру і в процесі сканування центральний елемент поточного квадрату апертури замінюється на код середнього арифметичного всіх точок поточної апертури. Відповідно, центральний елемент апертури стає фактично усередненням всіх точок апертури.

Зображення задається матрицею B з m рядків та m стовбців значень інтенсивності b_j, $0 < i \le n$, $0 < j \le n$,:

$$B = \begin{pmatrix} b_{11}\ b_{12} \ldots b_{1n} \\ b_{21}\ b_{22} \ldots b_{2n} \\ \ldots \\ b_{n1}\ b_{n2} \ldots b_{nn} \end{pmatrix}.$$

При виконанні середньоквадратичної фільтрації зображення B, кожний елемент c_{ij} відфільтрованого зображення C формується за формулою [5]:

$$\forall i \in \{\frac{a+1}{2}, \frac{a+1}{2}+1, ..., n-\frac{a-1}{2}\},$$
$$j \in \{\frac{a+1}{2}, \frac{a+1}{2}+1, ..., n-\frac{a-1}{2}\}: \quad (1.1)$$
$$c_{ij} = \frac{1}{a^2} \sum_{x=i-\frac{a-1}{2}}^{i+\frac{a-1}{2}} \sum_{y=j-\frac{a-1}{2}}^{j+\frac{a-1}{2}} b_{xy}.$$

Процес середньоарифметичної фільтрації зображень може бути ілюстровано наступним прикладом.

Нехай оригінальне зображення B з 6-ти рядків і 6-ти стовбців (n= 6) має наступний вигляд:

$$B = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1 & 1 & 2 & 5 & 9 \\ 1 & 5 & 2 & 3 & 2 & 7 \\ 1 & 1 & 2 & 3 & 2 & 8 \\ 1 & 2 & 3 & 4 & 1 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}.$$

В результаті середньоарифметичної фільтрації цього зображення апертурою 3 х 3 (a = 3) формується наступна матриця C відфільтрованого зображення:

$$C = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1{,}44 & 1{,}89 & 2{,}22 & 4{,}33 & 9 \\ 1 & 1{,}56 & 2{,}11 & 2{,}31 & 4{,}74 & 7 \\ 1 & 1{,}89 & 2{,}67 & 2{,}33 & 4{,}62 & 8 \\ 1 & 1{,}89 & 2{,}67 & 3{,}11 & 5 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}$$

Після округлення значень елементів матриця C відфільтрованого набуває наступного вигляду:

$$C = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1 & 2 & 2 & 4 & 9 \\ 1 & 2 & 2 & 2 & 5 & 7 \\ 1 & 2 & 3 & 2 & 5 & 8 \\ 1 & 2 & 3 & 3 & 5 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}.$$

При застосуванні апертури розміром 3 х 3 крайніми вважаються всі точки зображення першого і останнього стовпців матриці, а також першого та останнього рядків. Як видно з наведеного вище прикладу, при середньоарифметичній фільтрації, значення крайніх точок не змінюються.

Аналіз наведеної вище формули (1.1) показує, що для формування практично кожного (крім елементів, що лежать по краях зображення) елементу c_{ij} відфільтрованого зображення C при використанні апертури розміром a х a точок виконуються a^2 операцій додавання та одна операція ділення. Таким чином, час T_1 середньоарифметичної фільтрації одного зображення можна наближено оцінити як:

$$T_1 = n^2 \cdot (a^2 \cdot t_a + t_d), \qquad (1.2)$$

де t_a - час виконання операції цілочисельного додавання, та t_d - час виконання операції ділення з плаваючою точкою.

Існує більш ефективний алгоритм середньоарифметичної фільтрації [3], оснований на корегуванні, при переході в процесі сканування зображення від однієї апертури до сусідньої, суми її елементів шляхом віднімання значень інтенсивностей a точок, що належать попередній апертурі, але не належать наступній, і відповідно, додавання до поточного середнього значень інтенсивностей a точок, які є в поточній апертурі, але відсутні в попередній. Для цього алгоритму, час T_2 виконання середньоарифметичної фільтрації одного зображення обчислюється у вигляді:

$$T_2 = n^2 \cdot (2 \cdot a \cdot t_a + t_d). \qquad (1.3)$$

Для переважної більшості практичних застосувань комп’ютерної обробки зображень вирішується задача фільтрації не одного, а потоку зображень.

Відповідно, при використанні одного процесора темп фільтрації зображень співпадає з значеннями T_1 або T_2.

Як зазначалося вище, прискорення середньоарифметичної фільтрації потоку зображень може бути досягнуте за рахунок використання ресурсів потужних багатопроцесорних віддалених обчислювальних систем в рамках хмарних технологій. В силу того, що вказані комп'ютерні системи складаються з великої кількості процесорів, що вони здатні виконувати паралельну фільтрацію декількох зображень, темп обробки їх потоку практично визначається швидкістю мережевого каналу обміну даними з хмарою [15].

Для того, щоб здійснити криптографічний захист зображень за умови організації захищеної фільтрації потоку зображень з залученням віддалених комп'ютерних систем, на боці користувача мають здійснюватися обчислення, пов'язані з шифруванням зображень перед їх передачею в хмару, та дешифруванням отриманого результату.

Відповідно, в якості критеріїв ефективності методів гомоморфного шифрування зображень для їх захисту в процесі віддаленої обробки зображень доцільно розглядати [16]:

- Прискорення реалізації середньоквадратичної фільтрації, яке досягається за рахунок залученням віддалених комп'ютерних систем за умови захищеності зображення від стороннього доступу в процесі обробки. В якості такої міри прискорення реалізації середньоквадратичної фільтрації може слугувати коефіцієнт χ, що визначається співвідношення часу T фільтрації зображення користувачем і часу T_{cd} обчислень, які здійснюються їм для реалізації захисту:

$$\chi = \frac{T}{T_{ed}}. \qquad (1.4)$$

- Рівень захищеності зображень при використанні гомоморфного шифрування, в процесі їх передачі по відкритим каналам глобальних мереж та обробки в потенційно відкритому середовищі. Цей показник оцінюється об'ємом ресурсів, потрібних зловмиснику для здійснення незаконного доступу

до зображень користувача. В свою чергу, на практиці, в переважній більшості випадків, зазначений вище об’єм ресурсів оцінюється через об’єм перебору, який потрібно виконати зловмиснику для незаконної реконструкції оригінальних зображень.

1.2 Огляд сучасних схем гомоморфного шифрування даних

Проблема ефективного гомоморфного шифрування даних, що оброблюються в хмарах є вкрай актуальної, оскільки від її вирішення напряму залежить можливість використання віддалених комп’ютерних потужностей для багатьох практично важливих застосувань. Для цих застосувань неприпустимим є передача відкритих даних по мережах і обробка цих даних на непідконтрольних обчислювальних потужностях. Тому виникає задача шифрування даних таким чином, щоб вони не могли бути отримані в явному вигляді шляхом передачі в мережі та обробки на невідомій комп’ютерній системі.

Як уже зазначалося вище, основна проблема полягає в тому, що секретні дані мають оброблюватися на віддалених комп’ютерних потужностях. Зрозуміло, що при вирішенні різних практичних задач обчислення здійснюються різні. Відповідно до цього, всі існуючі системи гомоморфного шифрування можна розділити на два класи: шифрування, яке залежить від процедур обробки і шифрування, що не залежить від операцій, які виконуються на віддалених комп’ютерних потужностях. Реальне використання знаходить і гібридний підхід, який залежить від операцій віддаленої обробки лише частково [23]. Відповідно до цього, на рис.1.1 наведено схему класифікації існуючих систем гомоморфного шифрування даних.

Рис.1.1. Схема класифікації методів гомоморфного шифрування

В 1978 році Рівест [14] вперше запропонував схему універсального гомоморфного шифрування HE (Homomorphic Encryption), яка дозволяла проводити різні обчислення над зашифрованими даними з можливістю дешифрування отриманих результатів.

На практиці, до теперішнього часу найбільшого застосування отримали частково універсальні схеми PHE (Partial Homomorphic Encryption) та спеціалізовані схеми гомоморфного шифрування SWHE (Some what Homomorphic Encryption)) [16], [17], [18]. Значно рідше використовуються повністю універсальні схеми гомоморфного шифрування – FHE (Full Homomorphic Encryption) [9], [13]. Базовими характеристиками універсальних і часткового універсальних схем гомоморфного шифрування виступають глибина обчислень та потужність. Під глибиною обчислень розуміється

кількість вкладень операцій, яка допускає коректне дешифрування. Потужність – це ступінь перемішування даних при виконанні операцій, яка допускає коректне дешифрування.

Частково універсальне гомоморфне шифрування дозволяє виконувати операції додавання та множення з обмеженою глибиною обчислень. Повністю універсальне гомоморфне шифрування не накладає обмежень на глибину обчислень і при цьому забезпечує коректне дешифрування отриманого результату. В багатьох схемах універсального гомоморфного шифрування використовуються операції початкової загрузки [9, 19,20], які дозволяють частково знімати криптографічну складову в процесі обробки. Це, в свою чергу, чинить перепони нагромадженню криптографічної складової зі зростанням глибини обробки.

Часткове гомоморфне шифрування може допускати здійснення операцій гомоморфного множення або гомоморфного додавання з обмеженою глибиною обчислень. SWHE підтримує виконання операцій гомоморфного множення і додавання при наявності певних обмежень на глибину і складність таких обчислень. FHE підтримує довільний рівень глибини обчислень будь-якого типу в зашифрованому тексті з використанням початкової загрузки.

Широкого використання на практиці здобули реалізації методів гомоморфного шифрування даних BFV [16], [21], CKKS [22], BGV [18] та TFHE. Схеми гомоморфних обчислень BFV, CKKS та BGV будуються на основі навчання на кільці з помилками (R-LWE) [23], а TFHE в теоретичному плані базується на використання відомих технологій LWE та GSW [24]. Як технологія BFV, так і технологія BGV передбачають реалізацію гомоморфних обчислень над векторами елементів кінцевого поля, а схема CKKS дозволяє реалізувати наближені гомоморфне обчислення з реальними та комплексними числами.

Головними недоліками вказаних схем гомоморфних обчислень є потреба у значних часових ресурсах на навчання системи шифрування. Ефективність

таких схем гомоморфного шифрування залишається низькою в силу того, що значна частина обчислень приходиться на процеси шифрування та дешифрування. Під питанням залишається проблема рівня захищеності такого гомоморфного шифрування. Добре відомо [11], що криптографічні процедури, створені на основі сучасних засобів штучного інтелекту не відповідають критеріям лавинного ефекту. Це означає, що вони проявляють певну слабкість при застосуванні методів диференційного криптоаналізу.

В епоху хмарних обчислень та машинного навчання технології гомоморфного шифрування пропонують рішення для захисту користувачів, що передаються на аутсорсинг. Користувач завантажує зашифровані дані в хмарну службу без дешифрування, а служба хмари безпосередньо виконує складання та множення зашифрованого тексту. Інші обчислення з шифротекстом можуть бути побудовані з використанням гомоморфного складання та множення.

Досягнення в галузі інформаційних технологій та біоінформації змусили людей та установи використовувати сторонні хмарні платформи для зберігання та обробки даних, таких як онлайн-моніторинг стану здоров'я [25], діагностика захворювань [26] та внесення генотипу людини [11], [10]. Однак, як тільки користувачі завантажують дані у вигляді відкритого тексту на сторонню платформу, вони втрачають контроль над своїми конфіденційними даними. Будь-хто, хто має доступ до сторонньої платформи, може вкрасти генетичні дані користувачів. Навіть хмарні платформи з обмеженою довірою можуть розкривати генетичні дані користувачів, мотивовані вигодами.

Значною проблемою залишається організація гомоморфної обробки даних з залученням операцій з плаваючою точкою. Суть проблеми полягає в тому, що на різних обчислювальних платформах застосовуються різні системи округлення результатів обчислень. Зрозуміло, що це може призвести до відмінностях в зашифрованому тексті при використанні хмарними системи різних комп’ютерних платформ.

Для організації гомоморфної обробки даних з плаваючою точкою потрібно коректно представляти результат таким чином, щоб він міг бути адекватними чином відновлений. Для цього використовуються різноманітні методи лінійної регресіїї, які дозволяють автоматично відновлювати дані, пошкоджені в результаті округлення результатів при виконанні операцій з плаваючою точкою.

Суттєвим недоліком існуючих технологій гомоморфного шифрування універсального типу є мала обчислювальна ефективність. Тобто, об'єм обчислень, потрібних для виконання шифрування і особливо дешифрування може значно перевищувати об'єм обчислень, безпосередньо пов'язаних з виконанням завдання. Тому, до теперішнього часу подібні системи використовуються лише в теоретичному плані, активно досліджуються з перспективою подальшого практичного впровадження зі зміною технологічної ситуації.

Для обробки зображень взагалі і в тому числі середньоарифметичної фільтрації велике значення має характер операцій, з яких складається процедура обробки зображення.

Для досліджень, що проводяться в рамках магістерської дисертації дуже важливим є питання про нелінійність перетворень, що виконуються в рамках криптографічних алгоритмів гомоморфного шифрування. У цьому плані зручним є розділити всі криптографічні алгоритми на лінійні і нелінійні. Лінійні алгоритми, найвідомішим представником яких є Madriga [23] не становлять великого інтересу з погляду справжніх досліджень: їх порушення може бути здійснене шляхом аналітичних перетворень, які призводять до вирішення звичайної системи лінійних рівнянь. Більший інтерес з позицій гомоморфного шифрування представляють нелінійні алгоритми. Важливим є класифікувати криптографічні алгоритми виходячи з використовуваних механізмів формування нелінійності. На практиці у складі криптографічних алгоритмів використовуються такі класи нелінійних перетворень:

- табличні перетворення : цей метод забезпечує високу нелінійність перетворення в поєднанні з високою швидкістю реалізації нелінійних перетворень, хоча і вимагає пам'яті для зберігання таблиць - як наслідок цей спосіб використовується в більшості реальних алгоритмів гомоморфного шифрування;

- арифметичні операції додавання - нелінійні складові цього перетворення формуються у вигляді переносів, які включають операції кон'юнкції: так при арифметичному підсумовуванні розрядів a_{i-1} і b_{i-1} ($i>0$) з врахуванням переносу в (i-1) -й розряд, біт переносу p_{i-1} в наступний i-ий розряд формується у вигляді: $p_i = p_{i-1}\&a_{i-1} \& p_{i-1}\&b_{i-1}\&a_{i-1}\&b_{i-1}$.Аналіз показує, що такі операції малоефективні у плані реалізації перетворень з великою нелінійністю;

- операції множення та визначення залишку - нелінійні складові формуються у процесі виконання операцій множення. Цей шлях реалізації нелінійних перетворень отримав широке поширення через високу ефективність реалізації операцій множення в сучасних процесах в рамках багатьох алгоритмів гомоморфного шифрування;

- пряма реалізація нелінійних логічних операцій у криптографічних алгоритмах з використанням відповідних команд мікропроцесора або логічних елементів при апаратній реалізації.

Якщо аналізувати операції, які використовуються при здійсненні середньоарифметичної фільтрації, то це операції арифметичного додавання і нелінійна операція ділення. Тому, про операцію гомоморфного шифрування можна говорити як про процедуру нелінійного перетворення зображення.

1.3 Аналіз існуючих гомоморфних шифрів для захисту зображень при їх віддаленій фільтрації

До сьогоднішнього часу запроновано і активно використовуються ряд підходів до вирішення задачі захисту зображень в процесі їхньої віддаленої

середньоарифметичної фільтрації. Структурно вказані підходи до побудови гомоморфного шифрування можна розділи на два класи:

- гомоморфне шифри на основі використання адитивного маскування оригінального зображення;

- гомоморфне перестановочні шифри, які базуються на криптографії перемішування елементів оригінального зображення.

Ідея гомоморфних шифрів на основі адитивного маскування зображень базується на достатньо очевидному факті, який прямо випливає з формули (1.1) і полягає в наступному теоретичному положенні: результат середньоарифметичної фільтрації суми двох зображень дорівнює сумі відфільтрованих представлень цих двох зображень.

Відповідно, ідея гомоморфного шифрування на основі адитивного маскування полягає в арифметичному додаванні до матриці B оригінального зображення, яке має бути відфільтроване, матриці M зображення з формуванням замаскованого зображення D у вигляді суми B+M тобто виконання перетворення.

Отримане таким чином зображення D надсилається для фільтрації на віддалену комп'ютерну систему, яка формує відфільтроване зображення C . Оскільки зображення C являє собою суму відфільтрованого зображення B та M, то самий виконання гомоморфного дешифрування отриманого зображення зводиться до віднімання від відфільтрованого зображення C попередно відфільтрованого зображення маски$_j$.

В описаному вигляді ідея адитивного маскування запропонована в [17]. Основним недоліком гомоморфних шифрів на основі адитивного маскування є те , що вона потребує додаткової процедури фільтрування зображення-маски. В роботі [17] пропонується заздалегідь формувати певну множину таких зображень-масок та їх фільтрованих представлень. Фактично, ця множина являє собою множину ключів для шифрування і дешифрування зображень. За наявності вказаного набору маскуючи зображень та їх відфільтрованих

представлень для гомоморфного шифрування поточного зображення, тобто для його адитивного маскування вибирається випадковим чином одна з масок. Відповідно, процес гомоморфного шифрування полягає в додавання до зображення обраного маскую чого зображення, а для гомоморфного дешифрування використовується її фільтроване представлення цієї маски. Таким чином, маски та їхні відфільтровані відповідники заздалегідь формуються користувачем з залученням власних обчислювальних ресурсів та використовуються повторно.

В процесі гомоморфного шифрування віддаленої фільтрації за методом [17] користувач двічі виконує операцію арифметичного додавання (віднімання) замість обчислення середнього арифметичного a точок. Тобто замість a^2 операцій додавання і однієї операції ділення здійснюється лише дві операції додавання. Відповідно, значення коефіцієнту χ прискорення цього методу гомоморфного шифрування зображень визначається з наступної формули [17]:

$$\chi = \frac{a^2}{2} + \frac{t_d}{2 \cdot t_a}. \qquad (1.5)$$

Для практичних застосувань значення розміру апертури при фільтрації становить від 11 до 17 [4] з тенденцією до збільшення з ростом числа точок зображення. Співвідношення часу виконання операції ділення t_d та додавання t_a для сучасних процесорів Intel приблизно дорівнює 40 [8]. Таким чином, орієнтовне значення коефіцієнту χ становить 164.

Основним недоліком цього методу є низький рівень криптостійкості до спроб відновлення зашифрованого зображення шляхом статистичного аналізу.

Інший відомий метод гомоморфного шифрування зображень щляхом їх адитивного маскування [9] передбачає використання матриці M зображення-маски, елементи якої є кратними деякому секретному простому числу r, більшому за будь-який елемент матриці B: $\forall i \in \{1,2,\ldots,n\}, j \in \{1,2,\ldots,n\}$: $m_{i,j} \bmod$ $\forall i \in \{1,2,\ldots,n\}, j \in \{1,2,\ldots,n\}$: $m_{i,j} \bmod r = 0.$ $= 0, r > b_{i,j}$.

При використанні такого гомоморфного шифру оттримане після віддаленої обробки відфільтроване захищене зображення C дешифрується шляхом віднаходження залишку від ділення кожного його елементу c_{ij} на вибране користувачем секретне число r: $\forall i \in \{1,2,\ldots,n\}$, $j \in \{1,2,\ldots,n\}$: $q_{i,j} = c_{i,j} \bmod r$.

Головна перевага описаного методу гомоморфного шифруванні в порівнянні с простим адитивним маскуванням полягає в тому, що при нема необхідності в її фільтрації маскуючого зображення.

Висновки до розділу 1.

В результаті досліджень, направлених на аналіз задач організації захисту від несанкціонованого доступу зображень в процесі їх середньоарифметичної фільтрації на віддалених і потенційно доступних обчислювальних системах методами гомоморфного шифрування можуть бути зроблені наступні висновки:

1. Розширення класу прикладних задач обробки зображень, постійне зростання кількості їх точок, та вимог до оперативності їх обробки диктують необхідність використання для цього практично необмежених обчислювальних ресурсів, які надають сучасні хмарні технології за умови забезпечення надійного захисту від доступу з боку сторонніх осіб.

2. Найбільш доцільним засобом зображень в процесі їх обробки на віддалених комп'ютерних потужностях є гомоморфне шифрування, інваріанте до операцій обробки зображень і, зокрема операцій, які скидають процедуру середньоарифметичну фільтрацію зображень. Проведений аналіз операцій, що лежать в основі цього виду фільтрації зображень а також проведений огляд існуючих універсальних методів гомоморфного шифрування показали, що цей клас методів гомоморфного шифрування не забезпечує потрібної для задач практики ефективності захисту зображень в процесі їх середньоарифметичної фільтрації на віддалених комп'ютерних системах.

3. Проведений огляд існуючих спеціалізованих методів гомоморфного шифрування для захисту зображень під час їх середньоарифметичної фільтрації показав, що методи, які базуються на операціях адитивного маскування не забезпечують необхідного для задач практики рівня захищеності від атак на основі статистичного аналізу.

4. Проведений аналіз операцій, що лежать в основі процедур середньоарифметичної фільтрації зображень показав, що найбільш перспективним для реалізації гомоморфного шифрування є перестановочні шифри, які дозволяють забезпечити високий рівень захищеності від атак статистичним аналізом та дозволяє досягти високих характеристик часової

ефективності за рахунок того, що операції перемішування, якими реалізуються гомоморфні операції шифрування та дешифрування зображень можуть бути суміщені з операціями обміну зображеннями між обчислювальною платформою користувача та віддаленими потужними багатопроцесорними комп’ютерними системами.

РОЗДІЛ 2
РОЗРОБКА МЕТОДУ ГОМОМОРФНОГО ШИФРУВАННЯ ЗОБРАЖЕНЬ ПРИ ЇХ ВІДДАЛЕНІЙ ФІЛЬТРАЦІЇ

Основна ціль комп'ютерної обробки зображень полягає в здійсненні їх автоматичного розпізнавання та аналізу. Цей процес включає в себе декілька етапів, які виконуються послідовно: один за одним. Важливим в цьому ряду є етап актуалізації зображення, тобто видалення з нього елементів, які не несуть корисної інформації для вирішення конкретної задачі аналізу зображення [33]. Основним елементом процесу актуалізації зображення виступає його фільтрація. Крім виконання задачі актуалізації, фільтрація зображень забезпечує підвищення їх якості шляхом видання завад, що утворилися під час одержання та в процесі передачі зображення [34].

В сучасних системах, що аналізують чи оброблюють зображення, надзвичано поширенною є середньоарифметична фільтрації зображень. Зазвичай її виконують на початкохи етапах обробки зображень з метою полішенн їхньої якостза рахунок зменшення компоненти імпульсних завад. Висока ресурсоємність обробки зображень, що складаються з мільйонів пікселів, вказує на необхідність залучення потужних багатопроцесорних систем для виконання масової обробки зображень за допомогою фільтрації. Проте існують такі класи задач, при вирішенні яких конфіденційність оброблюваних даних є ключовою. Зокрема, для деяких класів таких задач потребується обробка великосї кількості зображень методом середньорифметичної фільтрації. Тобто цей клас задач не може бути розв’язаний з використанням відкритих багатопроцесорних систем. Внаслідок цього виникає потреба розробки криптографічних методів захисту зображень в процесі їхньої віддаленої обробки на відкритих платформах. Основною вимогою, до них є високий рівень захищенності зображень як при передачі, так і в процесі самої обробки.

На сьогодні найбільшою перешкодою для широкого використання переваг хмарних обчислень для організації відддаеної обробки зображень є їх вразливість до несанкціонованого доступу під час передачі та безпосередньої обробки на віддалених комп’ютерних потужностях. . Практично мова йде про обробку зображень користувача на комп'ютерних системах, які не підконтрольні їм, віддалено і потенційно відкриті для несанкціонованого доступу. Існуючі засоби шифрування інформації дозволяють забезпечити таємність зображень лише під час їх передачі через Інтернет, але не в процесі їх безпосередньої обробки на віддалених комп’ютерних системах [4]. Для переважної більшості прикладних завдань комп’ютерного аналізу зображень важливо дозволити лише обмежений доступ до них стороннім особам.

Таким чином, наукове завдання захисту зображень у процесі їх дистанційної обробки, у тому числі фільтрації на неконтрольованих користувачами комп’ютерних системах, є актуальним для сучасного етапу розвитку інформаційних технологій.

2.1. Метод гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації

Як зазначалося вище, одним із найбільш поширених видів комп'ютерної обробки зображень є середньоарифметична фільтрація. Ця операція дозволяє підвищити якість зображень, усуваючи імпульсні шуми, які виникають під час формування та передачі зображень [23]. Вище було показано, що суть цього виду обробки полягає в скануванні матриці зображення квадратною апертурою зі стороною непарного розміру, в ході якої здійснюється заміна центрального елемента поточної апертури на значення середнього арифметичного всіх її точок.

Базовими арифметичними операціями середньоарифметичної фільтрації зображень є операції обчислення середнього арифметичного точок зображення в межах поточної апертури. Вказана процедура складається з операцій

арифметичного додавання та подальшого ділення отриманої суми на розмір апертури.

При виконанні середньоарифметичної фільтрації розпаралелювання процесу обробки зображення може бути досягнуто як на рівні одночасної обробки групи зображень, так і на рівні одночасної обробки декількох апертур. Іншим варіантом є розбиття зображення на фрагменти і здійснення одночасної його фільтрації на рівні паралельної обробки вказаних вище фрагментів. Недоліком цього варіанту є те, що виникає потреба в додатковій фільтрації стиків фрагментів зображення. При цьому розмір стику визначається розміром обраної апертури.

Проведений в рамках оглядового розділу аналіз можливостей підвищення ефективності захищеної фільтрації зображень в хмарах дозволяє зробити однозначний висновок про те, що найбільш перспективний шлях досягнення поставленої в магістерській дисертації мети полягає в використання перемішування, яке не потребує значних обчислювальних ресурсів. На користь цього висновку говорить те, що значний об'єм інформації, що міститься в сучасних зображеннях робить перемішування достатньо ефективним засобом захисту від спроб реконструювання зображень технологіями направленого перебору або статистичного аналізу. Виходячи з цього висновку, в основу запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації покладено їх перемішування.

Розроблена та обґрунтована така процедура гомоморфного шифрування зображень при їх захищеній середньоарифметичній фільтрації. Оригінальне зображення Z трансформується в зашифроване зображення Q шляхом перестановки в певному порядку його стовпців. При цьому порядок перестановки стовпців матриці первинного зображення фактично виступає в ролі ключа гомоморфного шифрування цього зображення. Після описаного гомоморфного шифрування отримане зображення Q надсилається користувачем в хмару, яка розподіляє його обробку на віддаленій комп'ютерній

системі. Там зображення оброблюється, тобто здійснюється його часткова фільтрація. Результати обробки повертаються користувачеві у вигляді матриці *T*, над якою користувач виконує гомоморфне дешифрування, тобто здійснює зворотну перестановку стовпців та обчислення завершального етапу середньоарифметичної фільтрації. В узагальненому вигляді організація розробленого методу гомоморфного шифрування зображень при їх захищеній середньоарифметичній фільтрації представлена на рис.2.1.

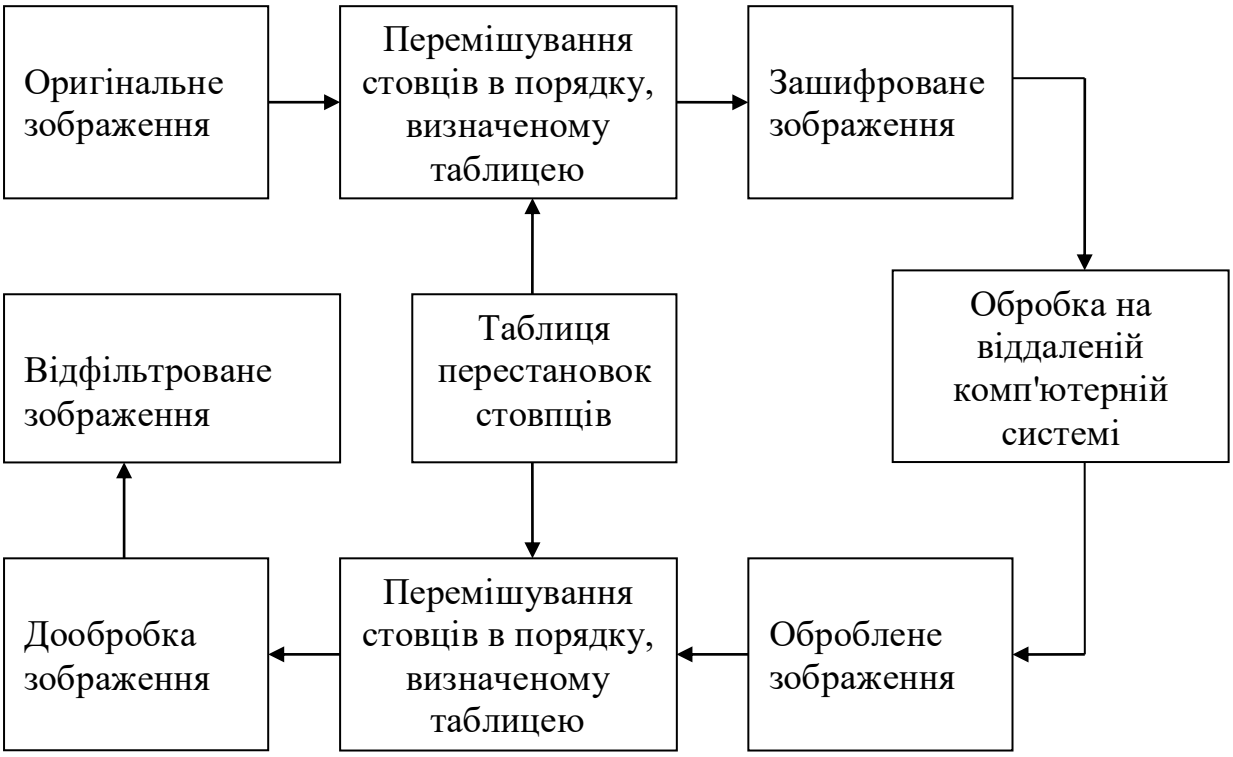

Рис.2.1 Загальна організація гомоморфного шифрування зображень при їх захищеній середньоарифметичній фільтрації

Запропонований метод гомоморфного шифрування зображень при їх захищеній середньоарифметичній фільтрації передбачає перемішування матриці зображення на рівні стовпців $z_1,z_2,\ldots,z_h$ матриці оригінального зображення Z :

$$Z=\{z_1,z_2,\ldots,z_h\}, \text{ де. } \forall j \notin \{1,2,\ldots,h\}: z_j=\{p_{1,j},p_{2,j},\ldots,p_{k,j}\}.$$

Порядок перемішування стовбців $z_1,z_2,\ldots,z_h$ матриці зображення вибирається користувачем довільно може бути представленим у вигляді

таблиці T_1 прямої перестановки. Фактично, таблиця T_1 являє собою секретний ключ користувача для виконання гомоморфного шифрування зображення. Кожній таблиці T_1 прямої перестановки відповідає одна таблиця T_2 зворотної перестановки. Кількість рядків таблиць T_1 і T_2 прямої та зворотної перестановки визначається числом h стовбців зображення. Важливим є те, що пропонований метод не накладає жодних обмежень на вибір таблиць T_1 і T_2 прямої та зворотної перестановки. Це означає, що перша з вказаних таблиць може генеруватися з використанням вбудованого генератора псевдовипадкових чисел.

При виконанні прямого перемішування з використанням таблиці T_1 задається номер x стовпця оригінального зображення Z, а вихідний код y являє собою позицію в перемішаному зображенні стовпця з номером x в оригінальному:

$$y = T_1(x).$$

При зворотному перемішуванні зображення, таблиця TR повертає позицію x в оригінальному зображенні стовпця з номером y в трансформованому зображенні, тобто:

$$x = T_2(y).$$

Тобто, для таблиць випадкових перемішувань T_1 і T_2 прямої та зворотної перестановки справедливо:

$$x = T_2(T_1(x)). \qquad (2.1)$$

При обробці потоків зображень користувач заздалегідь формує визначену наперед множину таблиць випадкових перемішувань T_1 і T_2 та використовує їх в якості ключів для компонування зображень, що передаються для віддалених обчислень з оригінальних зображень та компонування їх відфільтрованих зображень.

Формалізовано, розроблений метод гомоморфного шифрування зображень при їх захищеній середньоарифметичній фільтрації на віддалених обчислювальних системах містить в собі наступну послідовність дій:

1. Користувач випадковим чином, зокрема з використанням існуючих методів генерації псевдовипадкових чи випадкових чисел, формує таблицю T_1 прямої перестановки стовпців матриці заданого наперед розмірності.

2. Виходячи з отриманої описаним способом таблиці T_1 користувач формує таблицю T_2 відновлення оригінального порядку слідування стовпців матриці зображення, так, щоб виконувалися умова (2.1).

3. Користувач здійснює перестановку стовбців $z_1,z_2,\ldots,z_h$ матриці Z початкового зображення згідно даних таблиці T_1. В результаті виконання прямої перестановки формується гомоморфне зашифрована матриця Q:

$$Q = \begin{pmatrix} q_{11}\ q_{12} \ldots q_{1h} \\ q_{21}\ q_{22} \ldots q_{2h} \\ \ldots. \\ q_{k1}\ q_{k2} \ldots q_{kh} \end{pmatrix}.$$

В формалізованому представленні описана процедура послідовного формування зашифрованої матриці Q може бути описано наступним чином:

$$\forall l \in \{1, 2, ..., d\},\ j \in \{1, 2, ..., n\} : q_{ij} = p_{i,T1(j)}$$

4. Отримана в результаті описаного вище гомоморфного шифрування матриця G перемішаного зображення надсилається користувачем через хмару на віддалену комп'ютерну систему.

5 На віддаленій комп'ютерній системі, непідконтрольній користувачу реалізується часткова середньоарифметична фільтрація елементів матриці Q. Результат цієї операції формується у вигляді матриці D:

$$D = \begin{pmatrix} d_{11}\ d_{12} \ldots d_{1h} \\ d_{21}\ d_{22} \ldots d_{2h} \\ \ldots. \\ d_{k1}\ d_{k2} \ldots d_{kh} \end{pmatrix}.$$

В запронованому методі гомоморфного шифрування зображень на віддалених комп'ютерних системах виконується процедура часткової

фільтрації. Вказана процедура полягає в заміні кожного елемента матриці Q поділеною на k^2 сумою k елементів стовпчика, цент якого співпадає з вказаним елементом. Таким чином, при частковій фільтрації для кожного елементу матриці Q обчислюється сума, яка включає крім нього (k-1)/2 елементів вище і нижче його. Отримана сума ділиться на k^2 і результат ділення визначає нове значення поточного елементу частково відфільтрованого зображення.

У формальному вигляді описана вище процедура часткової фільтрації, тобто формування елементів матриці D, може бути представлено у наступному вигляді:

$$\forall i \in \{\frac{a+1}{2}, \frac{a+1}{2}+1, ..., k-\frac{a+1}{2}\},$$
$$j \in \{1, 2, ..., h\} : d_{ij} = \frac{1}{a^2} \sum_{x=i-\frac{a-1}{2}}^{i+\frac{a-1}{2}} q_{i,j}. \qquad (2.2)$$

Для забезпечення потрібної точності фільтрації, елементи матриці D обчислюються в форматі з плаваючою точкою.

6. Сформована, в результаті виконання на віддалених комп'ютерних системах описаної вище часткової середньоарифметичної фільтрації, матриця D повертається користувачеві по мережі Інтернет.

7. З отриманої матриці D користувач формує відфільтроване зображення V:

$$V = \begin{pmatrix} v_{11} & v_{12} \ldots v_{1h} \\ v_{21} & v_{22} \ldots v_{2h} \\ & \ldots. \\ v_{k1} & v_{k2} \ldots v_{kh} \end{pmatrix}$$

В теоретичному плані процес формування матриці V складається з двох етапів: зворотної перестановки стовпців матриці D з отриманням матриці V та заміни кожного елементу утвореної матриці V сумою групи розташованих в рядку a елементів з центром в цьому елементі. Другий етап гомоморфного

дешифрування виконується лише для елементів, що відстоять від країв зображення більш ніж (k-1)/2 точок.

Реально формування в явному вигляді матриці V не здійснюється: елементи групи, сума яких формує значення поточного елементу матриці D, вибираються з пам'яті матриці D з урахуванням зворотної перестановки рядків за допомогою таблиці T_2. Крайні точки зображення D, які не змінюються при середньоарифметичній фільтрації, прямо копіюються з оригінального зображення Q.

Для всіх інших точок процес формування елементів матриці Q з матриці D в формалізованому вигляді може бути описаний наступним чином:

$$\begin{aligned} &\forall l \in \{\frac{a+1}{2}, \frac{a+3}{2}, ..., k-\frac{a-1}{2}\}, \\ &h \in \{\frac{a-1}{2}, \frac{a+3}{2}, ..., h-\frac{a-1}{2}\}: \\ &v_{l,j} = \sum_{l=j-\frac{a-1}{2}}^{j+\frac{a-1}{2}} d_{l,T2(l)}. \end{aligned} \tag{2.3}$$

Задля прискорення гомоморфного дешифрування, тобто формування вихідної матриці Q відфільтрованого зображення пропонується здійснювати обчислення по формулі (2.3) тільки для елементів першого із не крайніх стовпців, тобто (a+1)/2 –го стовпця:

$$\begin{aligned} &\forall l \in \{\frac{a+1}{2}, \frac{a+3}{2}, ..., k-\frac{a-1}{2}\}, \\ &h = \frac{a+1}{2}: g_{l,h} = \sum_{l=h-\frac{a-1}{2}}^{h+\frac{a-1}{2}} r_{i,T1(l)}. \end{aligned} \tag{2.4}$$

Обчислення значень елементів всіх інших стовпців результуючої матриці V пропонується здійснювати рекурсивно з виконанням двох адитивних операцій: однієї операції додавання та однієї операції віднімання у згідно з наступною формулою:

$$\forall l \in \{\frac{a+3}{2}, \frac{a+5}{2}, ..., k-\frac{a-1}{2}\},$$
$$h \in \{\frac{a+1}{2}, ..., t-\frac{a-1}{2}\}: \qquad (2.5)$$
$$g_{l,h} = g_{l,h-1} - g_{l,T2(l-\frac{a+1}{2})} + g_{l,T2(h+\frac{a-1}{2})}.$$

Сформоване за описаною процедурою зображення V являє собою відфільтроване з заданим значенням апертури оригінальне зображення Q.

Розроблений метод гомоморфного шифрування зображень для захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах ілюструється прикладом віддаленої середньоарифметичної фільтрації зображення Q наведеного в оглядовій частині магістерської дисертації.

$$Q = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1 & 2 & 2 & 5 & 9 \\ 1 & 5 & 3 & 3 & 2 & 7 \\ 1 & 1 & 2 & 3 & 2 & 8 \\ 1 & 2 & 3 & 4 & 3 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}.$$

При виконання захищеної фільтрації зображення Q за розробленим методом, користувач довільним чином попередньо формує таблицю T_1 перестановок стовпців матриці зображень. Ця таблиця слугує в якості закритого ключа користувача для гомоморфного шифрування зображення. В рамках того прикладу, що розглядався в оглядовому розділі магістерської дисертації, таблиця T_1 має вигляд, представлений в таблиці 2.1.

Таблиця 2.1

Таблиця прямого перемішування стовпців TD

Номер стовпця матриці зображення	
Оригінального Q	Перемішаного G
1	4
2	6
3	5
4	1
5	4
6	2

Відповідно, таблиця T_2 зворотного перемішування або гомоморфного дешифрування має вигляд представлений в таблиці 2.1.

Таблиця 2.2

Таблиця T_2 зворотного перемішування стовпців

Номер стовпця матриці зображення	
Перемішаного	Оригінального
1	4
2	6
3	1
4	5
5	3
6	2

В рамках прикладу, що розглядається, з використанням таблиці T_1 гомоморфного шифрування зображення користувач формує перемішане (зашифроване) зображення *G*, матриця якого має наступний вигляд:

$$G = \begin{pmatrix} 2 & 6 & 1 & 4 & 2 & 1 \\ 2 & 9 & 2 & 5 & 1 & 1 \\ 3 & 7 & 1 & 1 & 3 & 5 \\ 3 & 4 & 1 & 1 & 2 & 1 \\ 4 & 8 & 1 & 3 & 3 & 2 \\ 4 & 9 & 2 & 5 & 3 & 2 \end{pmatrix}.$$

Отримана в результаті описаного гомоморфного шифрування матриця надсилається користувачем на хмару. На обраній хмарою віддаленій комп'ютерній системі виконується часткова середньоарифметична фільтрація перемішаного (гомоморфно зашифрованого) зображення з формуванням результуючої матриці *D*:

$$D = \begin{pmatrix} 2 & 6 & 1 & 4 & 1 & 1 \\ 0{,}76 & 2{,}47 & 0{,}34 & 1{,}11 & 0{,}33 & 0{,}78 \\ 0{,}89 & 2{,}77 & 0{,}43 & 0{,}78 & 0{,}44 & 0{,}76 \\ 1{,}11 & 2{,}56 & 0{,}33 & 0{,}56 & 0{,}67 & 0{,}89 \\ 1{,}22 & 2{,}78 & 0{,}43 & 1 & 0{,}88 & 0{,}56 \\ 4 & 9 & 2 & 5 & 3 & 2 \end{pmatrix}.$$

Зашифроване оброблене зображення з віддаленої комп'ютерної системи повертається користувачеві. Користувач копіює крайні точки оригінального

зображення Q в матрицю зображення V. Значення елементів другого стовпця (з другого по п'ятий в кожному стовбці матриці V обчислюється за формулою (2.4), а всіх інших – за формулою (2.5). В результаті користувачем отримується наступна матриця V:

$$V = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1{,}43 & 1{,}69 & 2{,}24 & 4{,}32 & 9 \\ 1 & 1{,}56 & 2{,}11 & 2{,}11 & 4{,}33 & 7 \\ 1 & 1{,}89 & 2{,}65 & 2{,}32 & 4{,}22 & 8 \\ 1 & 1{,}89 & 2{,}67 & 3{,}12 & 5 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}.$$

Після виконання округлення значень елементів матриці зображень, користувач отримує матрицю E відфільтрованого з заданим значенням апертури оригінального зображення:

$$E = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1 & 2 & 2 & 4 & 9 \\ 1 & 2 & 2 & 2 & 4 & 7 \\ 1 & 2 & 3 & 2 & 4 & 8 \\ 1 & 2 & 3 & 4 & 4 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}.$$

Цілком очевидно, що отримана в результаті запропонованої процедури гомоморфного дешифрування матриця є ідентичною з матрицею безпосередньої середньоарифметичної фільтрації.

2.2 Оцінка ефективності методу

Оцінку ефективності запропонованого методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації зображень доцільно здійснювати шляхом визначення і порівняння зазначених вище критеріїв:

- значення коефіцієнта μ прискорення фільтрації зображення за рахунок залучення до обчислень віддалених комп'ютерних систем;

- рівня захищеності зображень при їх передачі та в процесі віддаленої обробки на віддалених комп’ютерних системах, що не контролюються користувачем .

В запропонованому методі гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації зображень процес шифрування зображення перед передачею його на віддалені комп’ютерні системи не передбачає спеціальних обчислень і зводиться до перестановки стовпців матриці зображень. Таким чином, запропонований в магістерській дисертації методу гомоморфного шифрування за своєю сутністю відноситься до перестановочних методів шифрування. Такі типі шифрів відносяться до розряду класичних і широко використовуються як в минулих, так і в сучасних алгоритмах криптографічного шифрування даних [44]. На практиці, в рамках технології реалізації методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації зображень цей процес зводиться до зміни порядку передачі точок зображення в мережу в не потребує спеціального часу. Іншими словами процес гомоморфного шифрування зображення в реальності може бути суміщеним із процесом передачі даних з обчислювальної платформи користувача і віддалену комп’ютерну систему, на якій здійснюється часткова середньоарифметична фільтрація зображення.

Аналогічно процес гомоморфного дешифрування частково-відфільтрованого зображення, який зводиться до зворотного перемішування стовпців матриці пікселів зображення з використанням таблиці T_2, може бути суміщений з процесом передачі частково-відфільтрованого зображення з віддаленої комп’ютерної системи, на якій здійснювалась ця операція. Це означає, що в запропонованому методі гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації зображень процес дешифрування також не потребує додаткових часових ресурсів. Ця властивість перестановочного шифру в комбінуванні з віддаленим характером обробки зображень, яка потребує циклів передачі відповідних даних, значно підвищує

ефективність гомоморфного шифрування в порівнянні з іншими відомими методами спеціалізованого гомоморфного шифрування для обробки зображень і, зокрема, масочного або адитивного шифрування.

Після повернення частково-відфільтрованого зображення з віддаленої комп'ютерної системи, користувач в ході виконання завершальної фази фільтрації здійснює для всіх елементів матриці, крім першого не крайнього стовпця, одну операцію додавання і одну операцію віднімання. Для елементів першого не крайнього стовпця матриці зображень виконується *a* операцій додавання. Проте таких елементів відносно мало в складі сучасних зображень: їх питома вага становить менше 1/*x,* що для сучасних зображень складає менше 0.05%. Тобто, в рамках оціночних розрахунків показників ефективності є цілком прийнятним вважати, що час обробки користувачем однієї точки зображення в процесі завершальної фази середньоарифметичної фіотрацііі при використанні запропонованого методу фільтрації становить $2 \cdot t_a$. З цього випливає, що час *T* виконання користувачем на його власній обчислювальній платформі завершальної фази середньоарифметичної фільтрації визначається сумарним часом обробки всіх точок зображення:

$$T = k \cdot u \cdot 2 \cdot t_a \ . \qquad (2.6)$$

Відповідно, коефіцієнт μ прискорення середньоарифметичної фільтрації за рахунок залучення до обчислень віддалених комп'ютерних систем для запропонованого методу становить:

$$\mu = \frac{T_0}{T_1} = \frac{k \cdot u \cdot (a^2 \cdot t_a + t_e)}{k \cdot u \cdot 2 \cdot t_a} = \frac{a^2}{2} + \frac{t_e}{2 \cdot t_a} \ . \qquad (2.7)$$

Отримане значення практично збігається з оцінкою прискорення середньоарифметичної фільтрації (1.5) для найбільш швидкодіючого з відомих варіантів гомоморфного шифрування зображень з застосуванням адитивного маскування [17].

Фактично, в запропонованому методі гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на

обчислювальній платформі користувача виконується для кожної із точок зображень лише 2 адитивних операції: додавання результату часткової середньоарифметичної фільтрації для точки, що знаходиться праворуч (при скануванні зображення зліва направо), а також віднімання результату часткової середньоарифметичної фільтрації для точки, що знаходиться ліворуч від поточної точки зображення. Тобто мова йде лише про дві адитивних операції, виконання яких потребує, відповідно лише двох машинних команд: арифметичного додавання та арифметичного віднімання для чисел з плаваючою точкою.

Якщо говорити, про обробку точки зображення в процесі його часткової середньоарифметичної фільтрації на віддаленій комп'ютерній системі, то час, потрібний для обробки кожної точки зображення складається з часу виконання *a* операцій арифметичного додавання чисел з плаваючою точкою, а також часу здійснення операції ділення на розмір апертури отриманої суми з використанням однієї команди ділення над числами з плаваючою точкою. Іншими словами, питома вага χ операцій, що виконуються на обчислювальній платформі користувача при здійсненні завершальної фази середньоарифметичної фільтрації в загальному об’ємі операцій вказаного виду фільтрації визначається наступною формулою:

$$\chi = \frac{T_u}{T_s} = \frac{2 \cdot t_a}{a \cdot t_a + t_d}, \qquad (2.8)$$

де T_u- час виконання на обчислювальній платформі користувача обробки однієї точки зображення в процесі завершальної фази середньоарифметичної фільтрації; T_s - час виконання на віддалений комп’ютерній системі обробки однієї точки зображення в процесі часткової середньоарифметичної фільтрації зображення. Згідно з даними довідкових літературних джерел [56], час виконання на процесорах типу Intel команди ділення чисел з плаваючою точкою приблизно в сорок раз перевищує час виконання команд додавання віднімання з плаваючою точкою. З цього випливає, що для оціночних

розрахунків є цілком прийнятним вважати, що $t_d/t_a = 40$. З урахуванням цього, формула (2.8) може бути спрощена до наступного виду:

$$\chi = \frac{2 \cdot t_a}{a \cdot t_a + t_d} = \frac{1}{\frac{a}{2} + 20} \approx \frac{1}{25} = 0.04. \qquad (2.9)$$

Аналіз формули (2.9) показує, що в запропонованому методі гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації лише близько 4% об'єму обчислень, пов'язаних з фільтрацією здійснюється на обчислювальній платформі користувача, а, відповідно, 96% цих обчислень реалізується на віддалених комп'ютерних системах. Слід зазначити, що на відміну від обчислювальної платформи користувача, яка здебільшого являє собою звичайну робочу станцію, на віддалених комп'ютерних потужностях існують широкі можливості для розпаралелювання процесу часткової середньоарифметичної фільтрації. Теоретично, можна навіть розглядати варіант, за яким кожна точка зображення фільтрується на окремому процесорі. За цих умов процес фільтрації на віддалених багатопроцесорних комп'ютерних системах виконується гранично швидко. проте, проведений аналіз показав, що вказаний варіант не є найбільш ефективним: більш прийнятним з практичного боку, є залучення для часткової середньоарифметичної фільтрації не більше сотень процесорів [33].

Таким чином, проведений аналіз довів, що в порівнянні з іншими відомими методами гомоморфного шифрування зображень при їх віддалений середньоарифметичній фільтрації, запропонований метод, оснований на перестановках стовпців матриці зображень має значно кращі показники в плані значення питомої ваги операцій, що виконуються на обчислювальній платформі користувача при здійсненні завершальної фази середньоарифметичної фільтрації в загальному об'ємі операцій вказаного виду фільтрації. Зокрема, для широко відомого методу гомоморфного шифрування на основі адитивного маскування [24] цей показник має майже вдвічі більші

значення. Проведені експериментальні дослідження, результати яких детально наведені в четвертому розділі магістерської дисертації, в цілому підтверджують викладені вище теоретичні оцінки ефективності запропонованого методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації .

Таким чином, в результаті пильних студій часових характеристик технічної реалізації запропонованого методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації теоретично та експериментально доведено, що він забезпечує високі характеристики часової ефективності використання віддалених комп'ютерних потужностей. За значеннями цих характеристик запропонований метод не поступається відомим методам гомоморфного шифрування зображень при їх захищеній середньоарифметичній фільтрації.

Це досягнуто за рахунок того, що в основі запропонованого методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації лежать прості в плані технічної реалізації операції перестановки, які можуть бути на практиці суміщені з процесами передачі даних з обчислювальної платформи користувача на віддалені комп'ютерні системи і назад.

Проте в порівнянні з відомими методами гомоморфного шифрування зображень для їх захищеної фільтрації на віддалених комп'ютерних системах, пропоноване рішення забезпечує суттєво більший рівень захищеності від спроб незаконного відновлення зображення методами статистичного аналізу. Відомі методи гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації, зокрема, методи на основі адитивного маскування зображень, фактично мають використовувати для обробки зображень одну і ту ж саму маску, для якої на обчислювальній платформі користувача потрібно виконувати середньоарифметичну фільтрацію. Використання однієї маски для гомоморфного шифрування декількох зображень дозволяє виявити це методами

спектрального аналізу. відповідно, у супротивника з'являється можливість відновити маскуюче зображення і, відповідно, дешифрувати справжнє зображення в процесі його обробки на непідконтрольній користувачеві віддаленій комп'ютерній системі.

Рівень захищеності зображення може бути оцінено об'ємом ресурсів, потрібних зловмисникові для відновлення оригінального зображення. При використанні розробленого методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації кількість v можливих перестановок стовбців матриць дорівнює $u!$, що, за формулою Стірлінга, наближено становить:

$$v = (\frac{u}{e})^u \cdot \sqrt{2 \cdot \pi \cdot u} . \qquad (2.10)$$

Для реальних зображень найменша кількість u стовбців складає 1024, відповідно, кількість v варіантів перестановок стовбців такого зображення становить $6 \cdot 10^{2639}$. Зрозуміло, що аналіз такої кількості варіантів практично унеможливлює відновлення оригінального зображення шляхом підбору зворотної перестановки, оскільки перебір такої значної кількості варіантів далеко виходить за рамки сучасних можливостей технічної реалізації. Реалізація перебору такої великої кількості варіантів неможлива і найближчій перспективі 20-40 років навіть за умови використання можливостей квантових комп'ютерів.

Для певних класів контурних зображень об'єм розглянутого перебору може бути суттєвим чином скорочено за рахунок направленої реконструкції зображення. Ця технологія передбачає вибір стовбців таким чином, щоб два сусідніх мінімально відрізнялись один від одного. Проведені експериментальні дослідження показали, що для реальних контурних зображень об'єм перебору може бути таким чином зменшено на 2-3 порядки. Але цілком зрозуміло, що зменшення порядку перебору на 0.02% суттєвим чином не вливає на можливості технічної реалізації такого перебору сучасними комп'ютерними

засобами. Навіть при застосуванні описаної технології перебір такої значної кількості варіантів далеко виходить за рамки сучасних можливостей технічної реалізації. При захищеній обробці зображень цих класів з використанням розробленого методу рекомендується організовувати одночасну фільтрацію групи з n зображень. При цьому стовпці n обраних зображень перемішуються в межах групи. Кількість зображень в межах однієї групи не впливає на час виконання шифрування зображення перед передачею його в мережу та завершальну фазу фільтрації. Проте кількість варіантів перестановок збільшується до $(n \cdot u)!$, що суттєво підвищує рівень захищеності зображень.

Висновки до розділу 2

В результаті проведених в рамках другого розділу магістерської дисертації досліджень, націлених на підвищення оперативності обробки потоків зображень за рахунок використання хмарних технологій можуть бути зроблені наступні висновки:

1. В якості найбільш перспективного для задач забезпечення ефективного захисту зображень в процесі їх середньоарифметичної фільтрації на віддалених комп'ютерних системах обрано перестановочні гомоморфне шифри, які є інваріантними до операцій, які складають процедуру зазначеного вище виду фільтрації зображень.

2. Теоретично обґрунтовано, розроблено та досліджено метод гомоморфного шифрування зображень для захисту їх під час середньоарифметичної фільтрації на віддалених комп'ютерних системах, відмінністю якого є використання в якості основного елементу захисту перемішування стовпців матриці зображень в секретному порядку. В рамках розробленого методу визначено процедури часткової середньоарифметичної фільтрації, яка здійснюється на віддалених системах, а також процедури завершальної фази фільтрації, яка виконується на обчислювальній платформі користувача після гомоморфного дешифрування отриманого із хмари зображення.

3. Розроблений метод захищеної фільтрації на основі перемішування стовпців дозволяє, за рахунок використання віддалених обчислювальних потужностей, прискорити цю операцію на 1-2 порядки, що практично збігається з аналогічними показником найбільш швидкодіючого варіанту захисту зображень на основі адитивного маскування.

4. Основна перевага розробленого методу полягає в більш високому рівні захищеності від спроб, з використанням статистичного аналізу, отримати

незаконний доступ до зображень під час їх обробки на непідконтрольних користувачу віддалених комп’ютерних системах.

5. Запропонований метод гомоморфного шифрування зображень орієнтований на широке коло застосувань, пов’язаних з аналізом потоків зображень для підвищення оперативності їх обробки за рахунок використання можливостей сучасних хмарних технологій.

Р О З Д І Л 3
ОРГАНІЗАЦІЯ ВИКОРИСТАННЯ РОЗРОБЛЕНОГО МЕТОДУ ДЛЯ ЗАХИЩЕНОЇ ФІЛЬТРАЦІЇ ПОТОКІВ ЗОБРАЖЕНЬ

Переважна більшість прикладних задач, пов’язаних з обробкою зображень, в тому числі і із фільтрацією зображень з метою підвищення їх якості і актуалізації, орієнтовані на обробку не одиночних зображень, а потоків зображень. Для певних прикладних задач ці зображення пов’язані між собою, що має місце в задачах обробки аерокосмічних зображень, а також задачах медицинської діагностики та дистанційної дефектоскопії. В інших прикладних задачах зображення, що утворюють поті не пов’язані одне з одним. Відповідно, при обробці потоку зображень існує можливість реалізації перемішування, як засобі гомоморфного шифрування в значно більш широких межах ніж при організації захищеної обробки одиночного зображення. Крім того, в таких прикладних задачах об’єктивно існують умови для організації конвеєрної обробки зображень. Це означає, що під час віддаленої середньоарифметичної фільтрації поточного зображення, користувач може виконувати шифрування наступного. Це дозволяє значно підвищити ефективність використання обчислювальної платформи користувача, виключивши періоди простою з його функціонування. Зрозуміло, що за цих умов час, який витрачається користувачем безпосередньо для обробки кожного зображення згідно процедурою гомоморфного шифрування визначається часом його шифрування і дешифрування.

Для запропонованого методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп’ютерних системах організація обробка потоку зображень має свої особливості. Ці особливості полягають в тому, що розроблений у другому розділі магістерської дисертації метод гомоморфного шифрування відноситься до класу перестановочних шифрів і реалізація вказаних перестановок при шифруванні та дешифруванні може бути суміщена з процесами обміну зображеннями між

обчислювальною платформою користувача та віддаленою комп’ютерною системою. Друга важлива особливість запропонованого методу полягає в тому, що на віддаленій комп'ютерній системі не здійснюється в повному об’ємі середньоарифметична фільтрація – частина її реалізується в рамках так званої завершальної фази фільтрації, яка виконується безпосередньо на комп’ютерній платформі користувача після отримання частково обробленого на віддаленій системі зображення і його гомоморфного дешифрування.

3.1 Організація захищеної групової середньоарифметичної фільтрації зображень з використанням перемішування стовпців

Характерна особливість організації захищеної середньоарифметичної фільтрації зображень полягає в тому, що при збереженні в пам'яті системи матриці вихідного зображення і матриці результуючого зображення існують широкі можливості для паралельної фільтрації великої кількості точок зображення.

Як зазначалося вище, при виконанні обробки зображень для вирішення реальних прикладних задач часто вимагається середньоарифметична фільтрація не одиночного зображення, а потоку зображень. З формальної точки зору можна говорити, що в процесі вирішення прикладної задачі здійснюється середньоарифметична фільтрація деякої послідовності зображеньь $\Omega = \{B_1, B_2, B_3, \ldots, B_n\}$. Вказана особливість функціонування систем обробки зображень при вирішенні широкого спектру прикладних задач потенційно може бути використана для підвищення ефективності захисту зображень в процесі їх середньоарифметичної фільтрації на віддалених обчислювальних потужностях.

В результаті проведених досліджень виявлені можливості модифікації розробленого в другому розділі магістерської дисертації методу гомоморфного шифрування зображень для підвищення характеристик ефективності їх

захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах.

Зміст розробленої модифікації методу гомоморфного шифрування зображень для підвищення характеристик ефективності їх захищеної групової середньоарифметичної фільтрації на віддалених комп'ютерних системах полягає в здійсненні перемішувань стовпців не в рамках одного зображення а над групою зображень B_1,B_2,B_3, …,B_n. В результаті виконання таких транс перемішувань стовпців різних формально формується група з n гомоморфне зашифрованих зображень U_1, U_2, U_3…, U_n., які передаються на віддалені комп'ютерні потужності для здійснення над ними часткової середньоарифметичної фільтрації. На вказаних потужностях паралельна фільтрація цих надісланих гомоморфне зашифрованих зображень за викладеною вище методикою часткової середньоарифметичної фільтрації. В результаті виконання часткової середньоарифметичної фільтрації группі зображень U_1, U_2, U_3…, U_n формуються зображення Z_1, Z_2, Z_3…, Z_n, які являють собою частково відфільтровані зображення. Віддалена комп'ютерна система надсилає користувачеві кожне з вказаної групи Z_1, Z_2, Z_3…, Z_n зображень.

Відповідно, користувач, отримає групу Z_1, Z_2, Z_3…, Z_n зображень виконує їх гомоморфне дешифрування шляхом зворотної перестановки їх стовпців. Зрозуміло. що як при гомоморфному шифруванні, так і при гомоморфному дешифруванні перестановка стовпців здійснюється не в рамках одного зображення, в в рамках повної групи зображень. Це означає, наприклад, що перший стовпець першої в групі зображення може бути розміщений на місце 233-го стовпця п'ятого в групі зображення. Для дешифрування користувач виконує зворотну перестановку стовпців з використанням розширеної таблиці перестановок T'_2. В результаті користувач отримує групу з n зображень R_1, R_2, …, R_n. Над кожним з цих зображень окремо користувач здійснює фінальну фазу середньоарифметичної фільтрації у відповідності із формулою:

$$\begin{aligned}&\forall d \in \{\frac{a+3}{2}, \frac{a+5}{2}, ..., k-\frac{a-1}{2}\},\\ &\forall h \in \{\frac{a+1}{2}, ..., k-\frac{a-1}{2}\}:\\ &r_{d,h} = z_{d,hj-1} - z_{d,T(h-\frac{a+1}{2})} + z_{d,T(h+\frac{a-1}{2})}.\end{aligned} \quad . \qquad (3.1)$$

Отриманні в результаті фінальної фази середньоарифметичної фільтрації являють собою відфільтровані оригінальні зображення групи B_1, B_2, …, B_n.

Описана модифікація запропонованого методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп'ютерних може комбінуватись при цьому з адитивним маскуванням задля підвищення рівня захищеності при одробці певних груп зображень з характерними контурами.

При використанні модулярної арифметики [16], кожен з відліків $x_1,x_2,\ldots,x_n$ зображення X додається адитивна маска $g_1,g_2,\ldots,g_n$ так, що на віддалену систему передається множина адитивно замаскованих відліків: x_1+g_1, $x_2+g_2,\ldots,x_n+g_n$. При цьому значення масок вибираються як рішення такої системи рівнянь:

$$\begin{cases} g_1 \cdot a_{11} + g_2 \cdot a_{12} + ... + g_n \cdot a_{1n} = k_1 \cdot Z_1 \\ g_1 \cdot a_{21} + g_2 \cdot a_{22} + ... + g_n \cdot a_{2n} = k_2 \cdot Z_2 \\ \vdots \\ g_1 \cdot a_{n1} + g_2 \cdot a_{n2} + ... + g_n \cdot a_{nn} = k_n \cdot Z_n \end{cases} . \qquad (3.2)$$

де $Z_1,Z_2,\ldots,Z_n$ –закриті ключі гомоморфного шифрування. Тоді, при віддаленому виконанні середньоарифметичної фільтрації у відповідності з формулами (2.5 і 2.6) отримані результати можуть бути представлені наступним чином:

$$\begin{aligned}&\forall i \in \{1,2,...,n\} : r_i' = \sum_{l=1}^{n} (x_{il} + g_l) \cdot a_{il} = \sum_{l=1}^{n} x_{il} \cdot a_{il} + \sum_{l=1}^{n} g_l \cdot a_{il} =\\ &= r_i + k_i \cdot Z_i\end{aligned} , \qquad (3.3)$$

Відповідно, гомоморфне дешифрування отриманих даних здійснюється у наступному вигляді:

$$\forall i \in \{1,2,...,n\} : r_i = r_i' \bmod Z_i . \qquad (3.4)$$

Більш простий варіант полягає в тому, що використовується одне Z замість $Z_1, Z_2, \ldots, Z_n$.

При цьому значення масок вибираються як рішення такої системи рівнянь:

$$\begin{cases} g_1 \cdot a_{11} + g_2 \cdot a_{12} + ... + g_n \cdot a_{1n} = k_1 \cdot Z \\ g_1 \cdot a_{21} + g_2 \cdot a_{22} + ... + g_n \cdot a_{2n} = k_2 \cdot Z \\ \vdots \\ g_1 \cdot a_{n1} + g_2 \cdot a_{n2} + ... + g_n \cdot a_{nn} = k_n \cdot Z \end{cases} . \qquad (3.5)$$

Тоді, при віддаленому виконанні середньоарифметичної фільтрації у відповідності з формулами (2.5 і 2.6), отримані результати можуть бути представлені наступним чином:

$$\forall i \in \{1,2,...,n\} : r_i' = \sum_{l=1}^{n} (x_{il} + g_l) \cdot a_{il} = \sum_{l=1}^{n} x_{il} \cdot a_{il} + \sum_{l=1}^{n} g_l \cdot a_{il} = \\ = r_i + k_i \cdot Z \qquad (3.6)$$

Іншими словами, з формули (3.4) випливає, що результат віддаленої обробки являє собою суму реальної складової та деякого числа, яке націло ділиться на закритий ключ Z. Відповідно, дешифрування отриманих даних здійснюється у наступному вигляді:

$$\forall i \in \{1,2,...,n\} : r_i = r_i' \bmod Z . \qquad (3.7)$$

Проведений аналіз показав, що комбіноване використання різних методів гомоморфного шифрування даних для реалізації захищеної середньоарифметичної фільтрації групи зображень потребує значних додаткових обчислювальних ресурсів, хоча і забезпечує помітне зростання рівня захищеності в специфічних умовах чорно-білих зображень без напівтонів. Для таких зображень більш прийнятним варіантом гомоморфного шифрування виглядає використання чисто адитивних методів або гомоморфного модульного шифрування.

3.2. Оцінка ефективності

В якості критеріїв ефективності запропонованої модифікації методу гомоморфного шифрування груп зображень при їх середньоарифметичній фільтрації на віддалених обчислювальних потужностях доцільно розглядати:

- рівень захищенності зображень, що передаються потенційно відкритими каналами Інтернет на непідконтрольні користувачеві і потенційно відкриті для доступа стороннім особам віддалені комп'ютерні потужності;
- виграш в швидкості виконання середньоарифметичної фільтрації групи зображень за рахунок виконання більшої частини обчислень, пов'язаних з виконанням середньоарифметичної фільтрації на віддалених багато-процесорних комп'ютерних системах та кластерах.

Оцінка рівня захищеності групи зображень від несанкціонованого доступу до них з боку сторонніх осіб здійснюється через об'єм інформаційних та обчислювальних ресурсів, що витрачаються сторонніми особами для реалізації вказаного вище доступу.

Основний ефект від застосування описаної схеми організації гомоморфного шифрування при середньоквадратичній фільтрації зображень в груповому режимі полягає в тому, що це дозволяє суттєвим чином підвищити рівень захищеності при обробці окремих класів зображень, зокрема, контурних зображень.

Проведений аналіз показав, що найбільшу ефективність в плані підвищення рівня захищеності забезпечує комбіноване використання адитивного перемішування зі зсувом.

Суть такої технології полягає в тому, що стовпці групи зображень в процесі гомоморфного шифрування не тільки перемішуються, але і зсуваються. Відповідно, ускладнюється структура таблиці прямого перемішування стовпців для групи зображень.

Головною перевагою запропонованої модифікації методу гомоморфного шифрування групи зображень при їх середньоарифметичній фільтрації є

підвищення рівня захищеності за рахунок змішування не тільки стовпців одного зображення, але й стовпців різних зображень. Це різко збільшує кількість варіантів можливих перестановок і, відповідно утруднює процес відновлення порядку перестановки при виконанні дешифрування гомоморф-но зашифрованого зображення. Неважко показати, що кількість варіантів відновлення збільшується в n! раз при груповій обробці зображення. Часові характеристики ефективності запропонованого методу при організації групової обробки практично залишаються незмінними.

Висновки до розділу 3

В результаті досліджень, направлених на модифікацію запропонованого в другому розділі методу гомоморфного шифрування зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах, зокрема в умовах обробки не одиночних зображень, а їх потоків можуть бути зроблені наступні висновки:

1. Теоретично обґрунтовано та запропоновано модифіковану процедуру гомоморфного шифрування потоків зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах в рамках хмарних технологій. Відмінність запропонованої модифікації полягає в тому, що перемішування стовпців матриць зображень в процесі гомоморфного шифрування не обмежується рамками окремих зображень, а здійснюється в рамках групи зображень.

2. Головною перевагою запропонованої модифікації методу гомоморфного шифрування групи зображень при їх середньоарифметичній фільтрації є підвищення рівня захищеності за рахунок змішування не тільки стовпців одного зображення, але й стовпців різних зображень. Це різко збільшує кількість варіантів можливих перестановок і, відповідно утруднює процес відновлення порядку перестановки при виконанні дешифрування гомоморфно зашифрованого зображення. Теоретично та експериментально доведено, що часові характеристики гомоморфного шифрування та дешифрування при організації групової середньоарифметичної фільтрації не змінюються.

РОЗДІЛ 4

РОЗРОБКА ПРОГРАМИ МОДЕЛЮВАННЯ ПРОЦЕСІВ ВІДДАЛЕНОЇ ФІЛЬТРАЦІЇ ЗОБРАЖЕНЬ З ВИКОРИТАННЯМ ГОМОМОРФНОГО ШИФРУВАННЯ

Програма моделювання процесів захищеної віддаленої середньоарифметичної фільтрації зображень призначена для автоматизації експериментальних досліджень розробленого в другому розділі магістерської дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації.

Потреба в значних за обсягом обчислювальних ресурсах притаманна всім задачам комп'ютерної обробки зображень в силу того, що вони складаються з мільйонів точок і подальше підвищення їх якості педалює збільшення кількості точок. Крім того, постійно ускладнюються алгоритми обробки зображень.

Таким чином, тенденції використання комп'ютерного аналізу зображень в сучасних інформаційних технологіях потребують значного збільшення об'єму обчислювальних ресурсів, темпи росту яких помітно випереджають прогрес потужності процесорів [62].

Основна перевага розробленого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації полягає в більш високому рівні захищеності від спроб, з використанням статистичного аналізу, отримати незаконний доступ до зображень під час їх обробки на непідконтрольних користувачу віддалених комп'ютерних системах.

Запропонований метод гомоморфного шифрування зображень при їх середньоарифметичній фільтрації орієнтований на широке коло застосувань, пов'язаних з аналізом потоків зображень для підвищення оперативності їх обробки за рахунок використання можливостей сучасних хмарних технологій.

Важливою для цих застосувань характеристикою ефективності запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації виступає доля обчислень, які виконуються на

віддалених обчислювальних потужностей в співвідношенні до об’єму обчислень, які здійснюються на комп’ютерній платформі користувача. Зрозуміло, що ефективність віддаленої обробки зображень в хмарах тим вища, чим більша доля від загального об’єму обчислень здійснюється на віддалених комп’ютерних системах. Вважаючи на те, що обчислювальна потужність віддалених комп’ютерних систем теоретично можна вважати необмеженою, вказаний вище чинник реально визначає ступінь прискорення обробки потоку зображень.

Основною задачею експериментальних досліджень розробленого в другому розділі магістерської дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації є визначення часових характеристик, що дозволить експериментально перевірити отримані в другому розділі магістерської дисертації теоретичні оцінки часових характеристик розробленого методу.

Ціллю програми є перевірка ефективності запропонованого в магістерській дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації.

4.1 Організація даних програми

Виходячи з сформульованих вище основних задач експериментальних досліджень теоретично обґрунтованого та запропонованого в другому розділі магістерської дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації, програма має перевіряти правильність функціонування розробленого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації. При цьому потрібно експериментально довести правильність функціонування теоретично обґрунтованого та детально розробленого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації. Потрібно також визначити характеристики часової ефективності запропонованого методу та здійснити

порівняння з відомими методами захищеної фільтрації зображень. В якості основного показника ефективності реалізації середньоарифметичної фільтрації зображень на віддалених комп'ютерних потужностях з використанням хмарних технологій виступає доля обчислень, які виконуються на віддалених обчислювальних потужностей в співвідношенні до об'єму обчислень, які здійснюються на комп'ютерній платформі користувача.

Відповідно до викладених задач, які має досягати розроблене програмне забезпечення, при його створенні окремо організовані дані для виконання всіх етапів реалізації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації.

Зокрема, вихідне зображення, задане квадратною матрицею пікселів яскравості зберігається в матриці А цілих чисел, максимальним розміром 1024 х 1024. Введення даних в цю матрицю передбачається з спеціального файлу, або з використанням вбудованого генератора випадкових з чисел. При заповненні вхідної матриці зображення з спеціального файлу існує можливість досліджувати особливості реальних зображень, зокрема зображень з реальними спектральними характеристиками.

Для перевірки функціональної коректності роботи запропонованого в магістерській дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації в програмі передбачено виконання класичної середньоарифметичної фільтрації зображення, представленою матрицею А зі збереженням відфільтрованого зображення в матриці цілих чисел В.

Важливу роль в функціонуванні запропонованого в магістерській дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації відіграють таблиці шифрування та дешифрування. Ці таблиці створюються користувачем і виконують роль секретних ключів для гомоморфного шифрування та дешифрування зображень. Обидві таблиці представлені відповідно векторами Т1 і Т2 цілих чисел. в програмі передбачено, що вектор Т1 генерується випадковим чином, а вектор

T2 створюється спеціальним модулем розробленої програми на основі вектору T1.

Для фіксації результатів гомоморфного шифрування в розробленій програмі передбачено матрицю C реальних чисел, розмір якої співпадає з розмірами вихідної матриці A.

Зашифрована матриця C передається користувачем через механізми хмари на віддалену комп'ютерну багатопроцесорну систему, яка виконує часткову середньоарифметичну фільтрацію гомоморфне зашифрованого зображення.

Для зберігання та контролю правильності виконання на віддалених комп'ютерних системах часткової середньоарифметичної фільтрації в розробленій програмі передбачено використання спеціальної матриці D чисел з плаваючою точкою, розмірність якої співпадає з розмірністю матриці вихідного зображення. При виконанні часткової середньоарифметичної фільтрації вихідними даними для якої є матриця C результати фіксуються в матриці D. Це означає, що кожен відфільтрований піксель матриці D залежить тільки від поточної апертури матриці C.

Матриця D після завершення операції часткової середньоарифметичної фільтрації пересилається з віддалених обчислювальних потужностей на обчислювальну платформу користувача. Користувач здійснює гомоморфне дешифрування матриці D шляхом відновлення порядку слідування стовпців з використанням таблиці T_2. Результат гомоморфного шифрування фіксується в матриці E. В розробленій програмі здійснюється реальна перестановка стовпців матриці D. При реальній віддаленій обробці зміна порядку слідування стовпців відбувається в процесі передачі даних з віддаленої комп'ютерної системи на обчислювальну платформу користувача.

На обчислювальній платформі користувача здійснюється завершальна фаза середньоарифметичної фільтрації зображення, представленого в матриці E чисел з плаваючою точкою.

Після виконання користувачем завершальної фази середньоарифметичної фільтрації над матрицею E з отриманням матриці V, користувач здійснює округлення значень пікселів в цій матриці з отриманням в результаті матриці F повністю відфільтрованого зображення.

4.2 Розробка процедур програми

Розробка програми моделювання функціонування запропонованого в другому розділі магістерської дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації здійснюється на мові програмування високого рівня Пітон. Це дозволяє доволі оперативно створити програму, оперативно, в залежності від отриманих результатів моделювання вносити зміни в роботу програми. Ці можливості вкрай важливі для ситуації, коли програма створюється для всебічного дослідження нового методу організації обчислень і часто виникає потреба в зміні програми. В той же час не висувається жорстких обмежень, щодо часу роботи програми та об'єму задіяних нею ресурсів комп'ютерної системи. Наявні засоби цієї мови програмування дозволяють ефективно здійснювати заміри часових інтервалі роботи окремих фрагментів програми з використанням вбудованої мікросхеми таймеру.

Розроблена програма здійснює виконання наступної послідовності дій:

1. Випадковим чином згенерувати матрицю A 1024 x 1024 цілих чисел в діапазоні від 0 до 255. Для вирішення цієї задачі додатково створюються два вкладених цикли, обидва з яких мають ітерацію (-3,4). До індексу елементів матриці A додаються значення ітерацій. Таким чином отримується окремо індекс рядка і стовпця матриці. Матриця A заповнюється випадковим масивом цілих чисел,

2. Сформувати матрицю B розміром 1024 x 1024 як результат середньоарифметичної фільтрації матриці A з апертурою 7 x 7. Це означає, що кожен елемент b_{ij} матриці B обчислюється як округлене до цілого середнє

арифметичне квадратної підматриці розміром 7 х 7 матриці А. Центральний елемент цієї підматриці – a_{ij}. Індекси і та j лежать в інтервалах від 3-х до 1020 (при нумерації рядків і стовпців з нуля). Це означає, що крайні 3 стовпці зліва і справа, так же, як крайні три рядки знизу і зверху не оброблюються. Для виконання цього пункту завдання на розробку програмного забезпечння здійснюється сканування масиву від matrixA[row-3][column-3] і до matrixA[row+3][column+3]. Таким чином виділяється апертура в рамках якої здійснюється центрального елементу, який заповнюється значенням середньоарифметичного по апертурі (тобто сумою всіх елементів, поділеною на 49). В класі Polynom поліноми зберігаються порозрядно у вигляді масиву типу byte, індекс елемента в якому визначає його ступінь визнає степінь. При виконанні операцій над поліномом відповідні дії виконуються з представляючим його масивом, довжина масиву визначаються максимальним степенем поліному.

3. Випадковим чином сформувати таблицю T_1 із 1024 цілих чисел – вектор прямих перестановок. Кожен елемент вектору T_1 – числа від 0 до 1023, випадково розставлені на 1024 комірках вектору. Числа в таблиці T_1 – не повторюються. Для вирішення цієї задачі формується з використанням вбудованої функції random.sample таблиця в котрій міститься 1024 унікальних елемента від 0 до 1023. Створений метод, виконуючи операцію додавання поліномів як параметр отримує інший доданок, результат виконання повертається сума поліномів. Під час виконання, спершу визначається найбільша степінь результуючого поліному – найбільша зі степеней обох доданків, після чого створюється масив для результуючого поліному. Далі в циклі відбувається порозрядне заповнення масиву використовуючи виключне або вхідних масивів.

4. Сформувати таблицю T_2 із 1024 цілих чисел – вектор зворотних перестановок. Таблиця T_2 є зворотною по відношенню до T_1: якщо *j*-тий елемент таблиці T_1 дорівнює *k*, то *k*- тий елемент таблиці T_2 дорівнює *j*. Для

здійснення цієї задачі здійснюється ітерація до довжині створеної таблиці T1, при цьому отримується значення T1 при індексі в ітерації, відповідно, в таблицю T2 записується значення елементу індексу. При цьому новостворена таблиця T2 індексується значенням коду, що зчитується з таблиці T1.

5. Сформувати матрицю C, яка є результатом перестановки стовпців матриці A з використанням таблиці T_1. Наприклад, якщо $T_1[513] = 196$, то в 196-му стовпчику матриці C розміщається 513-й стовпчик матриці A. Для вирішеннія цього пункту завдання на проектування програмного забезпечення створюється пустий двовимірний масив C, повністю ідентичний масиву A. далі здійснюється ітерація по довжині таблиці T1. По значенню T1 по індексу, отримується номер стовпчика, який потрібно переставити із масиву A в масив C. Для копіювання елементів стовпця організується відповідний цикл ітерації. Цикл з використанням [i][column_index], де i - ітератор, а column_index – індекс зчитаний з таблиці T1. Для модуля, що формує матрицю C вхідними даними є матриця A та індекс стовпця цієї матриці. В модулі використовується лічильник *k*, якому на початку присвоюється нульове значення. Далі, при скануванні до лічильника додається одиниця k+=1, щоб ідти вниз по стовпчику матриці C. Для формування добутків використовується спеціально створена функція. Функції передається в якості вхідних даних поліном множника для виконання поліноміального множення. Максимальна степінь добутку дорівнює сумі ступінів множників, отже довжина результуючого масиву дорівнює сумі довжин вхідних масивів. Множення відбувається додаванням в циклі: перевіряється елемент масиву першого множника, якщо елемент не дорівнює нулю виконується додавання другого множника зсунутого на необхідну кількість розрядів.

6. Сформувати матрицю D реальних чисел, яка є результатом часткової фільтрації матриці C. Часткова фільтрація полягає в тому, що кожен елемент d_{ij} матриці D обчислюється як сума 7-ми суміжних елементів j-того стовпця матриці C, поділена на 49. Центральний елемент групи із згаданих 7-ми

елементів належить *i*-тому рядку матриці C. Виконання цього пункту завдання здійснюється в програмі за рахунок використання трьох вкладених циклів два перших з яких здійснюють сканування поля зображення. Для кожної із виділених в результаті такого сканування точок зображення в третьому циклі, який змінюється від -3 до +3 виконується обчислення суми елементів, які знаходяться відповідно вище і нижче активного елемента зображення, координати якого визначаються індексами сканування. Отримана сума цілиться в реальному форматі на 49 (розмір повною апертури) і результат розміщується в відповідній точці результуючої матриці D, координати цієї точки визначаються індексами сканування матриці C.

7. Сформувати матрицю E реальних чисел, яка є результатом зворотної перестановки (з використанням таблиці T_2) стовпців матриці D. Для реалізації цього пункту завдання на проектування програмного забезпечення створюється пустий двовимірний масив E, повністю ідентичний масиву D. Після цього здійснюється ітерація по довжині таблиці T2. По значенню T2 по поточному індексу, який приймає значення від 0 до 1023 отримується номер стовпчика, який потрібно переставити із масиву D в масив E. Для копіювання елементів стовпця організується відповідний цикл ітерації. Цикл з використанням [i][column_index], де i - ітератор, a column_index – індекс зчитаний з таблиці T2. Для модуля, що формує матрицю E вхідними даними є матриця D та індекс стовпця цієї матриці. В модулі використовується лічильник *k*, якому на початку присвоюється нульове значення. Далі, при скануванні до лічильника додається одиниця *k*+=1, щоб ідти вниз по стовпчику матриці D.

8. Сформувати матрицю F, кожен елемент якої f_{ij} формується як округлена сума 7-ми суміжних елементів i-того рядка матриці E, причому центральний елемент e_{ij} цієї групи з 7-ми елементів належить j-тому стовпцю матриці E.

9. Отримана матриця F має співпадати з матрицею B, сформованою в п.2. Для виконання цього пункту завдання на проектування програмного забезпечення організується цикл порівняння матриць F та B з урахуванням особливостей

округлення реальних чисел. Головна мета цього модуля програми полягає в контролі за правильністю розробленого програмного забезпечення з точки зору функціональної коректності процесів середньоарифметичної фільтрації.

10. В розробленій програмі здійснюється вимірювання часу виконання кожного із пунктів завдання з використанням вбудованого модулю Time. Це дозволяє сформувати результати експериментальних досліджень залежності ефективності запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації.

Розроблена програма функціонує в консольному інтерактивному режимі з виводом запрошень та меню для користувача. Результати роботи програми виводяться в файл, де зберігаються в текстовому форматі.

4.3 Експериментальне дослідження методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації з використанням розробленої програми

Основною задачею експериментальних досліджень теоретично обґрунтованого та запропонованого в другому розділі магістерської дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації є визначення часових характеристик, що дозволить експериментально перевірити отримані теоретичні оцінки часових характеристик розробленого методу.

В якості основного показника ефективності реалізації середньо-арифметичної фільтрації зображень на віддалених комп'ютерних потужностях з використанням хмарних технологій виступає доля обчислень, які виконуються на віддалених обчислювальних потужностей в співвідношенні до об'єму обчислень, які здійснюються на комп'ютерній платформі користувача.

В розробленій програмі досліджувався функціонал розробленого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації. Ціллю дослідження функціоналу є експериментальне доведення правильності функціонування теоретично обґрунтованого та детально розробленого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації.

На рис.4.1 наведено приклад матриці зображення розміром 16 х 16, над яким виконується операція середньоарифметичної фільтрації при використанні апертури 3 х 3. Розмір матриці вибрано виходячи з можливостей ефективного демонстрування функціоналу роботи методу. На практиці, розміри матриці зображень мають на порядки більше значення. з тією ж методу на наведеній матриці представлено напівтонове зображення, без актуалізації кольорової гами. Розрядність одного пікселя на наведеному на рис.4.1 зображенні складає один байт.

108	43	4	185	62	23	185	121	60	228	141	154	228	41	179	92
47	159	59	6	47	87	192	11	237	149	151	146	128	181	126	218
103	72	209	70	222	27	253	67	94	46	87	125	59	221	201	125
248	24	12	175	209	74	180	197	118	67	100	209	187	130	42	54
205	97	239	162	16	20	103	204	231	245	154	69	231	138	212	97
28	79	32	189	40	212	65	194	213	127	247	184	161	253	110	78
228	184	228	145	199	121	240	191	151	55	91	206	38	74	68	70
66	100	55	82	105	229	64	243	167	110	20	219	220	44	88	147
104	89	49	150	69	224	19	115	250	194	153	203	39	69	127	5
19	197	88	32	235	171	125	191	4	111	188	82	112	246	6	19
103	6	205	59	49	236	31	153	187	128	147	183	175	177	186	69
43	7	104	184	202	197	153	50	245	196	214	103	240	30	165	117
18	209	249	204	228	20	140	158	14	141	244	145	161	10	176	33
250	253	251	228	212	114	142	145	104	78	163	183	116	41	141	170
159	56	11	230	42	132	89	188	95	190	78	83	0	70	167	98
73	227	85	153	148	154	110	21	176	213	147	169	20	103	211	118

Рис.4.1 Приклад вихідної матриці A зображення розміром 16 x 16, над яким виконується операція середньоарифметичної фільтрації при використанні апертури 3 x 3.

На рис.4.2. представлено матрицю B після виконання класичної середньоарифметичної фільтрації зображення, представленою матрицею A.

0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.00	89.33	89.67	96.00	81.00	122.00	107.33	135.56	112.56	132.56	136.33	135.44	142.56	151.56	153.78	0.00
0.00	103.67	87.33	112.11	101.89	143.44	120.89	149.89	109.56	116.56	120.00	132.44	154.00	141.67	144.22	0.00
0.00	134.33	117.78	146.00	108.33	122.67	125.00	160.78	141.00	126.89	122.44	135.67	152.11	157.89	135.56	0.00
0.00	107.11	112.11	119.33	121.89	102.11	138.78	167.22	177.33	166.89	155.78	171.33	173.56	162.67	123.78	0.00
0.00	146.67	150.56	138.89	122.67	112.89	150.00	176.89	179.00	168.22	153.11	153.44	150.44	142.78	122.22	0.00
0.00	111.11	121.56	119.44	146.89	141.67	173.22	169.78	161.22	131.22	139.89	154.00	155.44	117.33	103.56	0.00
0.00	122.56	120.22	120.22	147.11	141.11	160.67	160.00	164.00	132.33	139.00	132.11	123.56	85.22	76.89	0.00
0.00	85.22	93.56	96.11	144.11	137.89	153.44	130.89	153.89	133.00	142.22	137.33	137.11	105.67	83.44	0.00
0.00	95.56	97.22	104.00	136.11	128.78	140.56	119.44	148.11	151.33	154.33	142.44	142.89	126.33	100.44	0.00
0.00	85.78	98.00	128.67	151.67	155.44	145.22	126.56	140.56	157.78	150.22	160.44	149.78	148.56	112.78	0.00
0.00	104.89	136.33	164.89	153.22	139.56	126.44	125.67	141.33	168.44	166.78	179.11	136.00	146.67	107.00	0.00
0.00	153.78	187.67	206.89	176.56	156.44	124.33	127.89	125.67	155.44	163.00	174.33	114.33	120.00	98.11	0.00
0.00	161.78	187.89	183.89	156.67	124.33	125.33	119.44	123.67	123.00	145.00	130.33	89.89	98.00	100.67	0.00
0.00	151.67	166.00	151.11	157.00	127.00	121.67	118.89	134.44	138.22	144.89	106.56	87.22	96.56	124.33	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Рис.4.2. Приклад матриці B відфільтрованого зображення з використанням апертури розміром 3 x 3.

Формування матриці B здійснюється згідно з планом експериментальних досліджень для перевірки правильності функціонування запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній

фільтрації , а також для експериментальної оцінки виникаючих при його практичному застосуванні похибок обчислення.

На рис.4.2. наведено згенеровану випадковим чином таблицю T_1 гомоморфного шифрування зображення розміром 16 х 16, яка виступає в ролі секретного ключа користувача.

13	15	9	7
0	11	10	3
2	12	14	6
1	4	8	5

Рис.4.3. Приклад таблиці T_1 прямої перестановки стовпців матриці зображення при його гомоморфному шифруванні.

На рис.4.4. наведено, в якості прикладу таблицю T_2 гомоморфного дешифрування обробленого на віддалених обчислювальних потужностях зображення розміром 16 х 16, яка також виступає в ролі секретного ключа користувача.

4	12	8	7
13	15	11	3
14	2	6	5
9	0	10	1

Рис.4.4. Приклад таблиці T_2 зворотньої перестановки стовпців матриці віддалено обробленого зображення для його гомоморфного дешифруванні.

Для фіксації результатів гомоморфного шифрування в розробленій програмі передбачено матрицю С цілих чисел, розмір якої співпадає з розмірами вихідної матриці А. Приклад такої матриці С, яка формується програмою в результаті гомоморфного шифрування вихідної матриці А (рис.4.1) з використанням таблиці перестановок Т1(рис.4.3) наведено на рис.4.5.

62	228	60	121	41	92	154	185	179	4	185	23	228	108	141	43
47	128	237	11	181	218	146	6	126	59	192	87	149	47	151	159
222	59	94	67	221	125	125	70	201	209	253	27	46	103	87	72
209	187	118	197	130	54	209	175	42	12	180	74	67	248	100	24
16	231	231	204	138	97	69	162	212	239	103	20	245	205	154	97
40	161	213	194	253	78	184	189	110	32	65	212	127	28	247	79
199	38	151	191	74	70	206	145	68	228	240	121	55	228	91	184
105	220	167	243	44	147	219	82	88	55	64	229	110	66	20	100
69	39	250	115	69	5	203	150	127	49	19	224	194	104	153	89
235	112	4	191	246	19	82	32	6	88	125	171	111	19	188	197
49	175	187	153	177	69	183	59	186	205	31	236	128	103	147	6
202	240	245	50	30	117	103	184	165	104	153	197	196	43	214	7
228	161	14	158	10	33	145	204	176	249	140	20	141	18	244	209
212	116	104	145	41	170	183	228	141	251	142	114	78	250	163	253
42	0	95	188	70	98	83	230	167	11	89	132	190	159	78	56
148	20	176	21	103	118	169	153	211	85	110	154	213	73	147	227

Рис.4.5. Приклад матриці C зображення після здійснення гомоморфного шифрування з використанням таблиці T_1.

Зашифрована матриця C передається користувачем через механізми хмари на віддалену комп'ютерну багатопроцесорну систему, яка виконує часткову середньоарифметичну фільтрацію гомоморфне зашифрованого зображення. Результат такої часткової фільтрації представлено в матриці D, показаної на рис.4.6.

0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
36.78	46.11	43.44	22.11	49.22	48.33	47.22	29.00	56.22	30.22	70.00	15.22	47.00	28.67	42.11	30.44
53.11	41.56	49.89	30.56	59.11	44.11	53.33	27.89	41.00	31.11	69.44	20.89	29.11	44.22	37.56	28.33
49.67	53.00	49.22	52.00	54.33	30.67	44.78	45.22	50.56	51.11	59.56	13.44	39.78	61.78	37.89	21.44
29.44	64.33	62.44	66.11	57.89	25.44	51.33	58.44	40.44	31.44	38.67	34.00	48.78	53.44	55.67	22.22
28.33	47.78	66.11	65.44	51.67	27.22	51.00	55.11	43.33	55.44	45.33	39.22	47.44	51.22	54.67	40.00
38.22	46.56	59.00	69.78	41.22	32.78	67.67	46.22	29.56	35.00	41.00	62.44	32.44	35.78	39.78	40.33
41.44	33.00	63.11	61.00	20.78	24.67	69.78	41.89	31.44	36.89	35.89	63.78	39.89	44.22	29.33	41.44
45.44	41.22	46.78	61.00	39.89	19.00	56.00	29.33	24.56	21.33	23.11	69.33	46.11	21.00	40.11	42.89
39.22	36.22	49.00	51.00	54.67	10.33	52.00	26.78	35.44	38.00	19.44	70.11	48.11	25.11	54.22	32.44
54.00	58.56	48.44	43.78	50.33	22.78	40.89	30.56	39.67	44.11	34.33	67.11	48.33	18.33	61.00	23.33
53.22	64.00	49.56	40.11	24.11	24.33	47.89	49.67	58.56	62.00	36.00	50.33	51.67	18.22	67.22	24.67
71.33	57.44	40.33	39.22	9.00	35.56	47.89	68.44	53.56	67.11	48.33	36.78	46.11	34.56	69.00	52.11
53.56	30.78	23.67	54.56	13.44	33.44	45.67	73.56	53.78	56.78	41.22	29.56	45.44	47.44	53.89	57.56
44.67	15.11	41.67	39.33	23.78	42.89	48.33	67.89	57.67	38.56	37.89	44.44	53.44	53.56	43.11	59.56
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Рис.4.6. Приклад матриці D результатів часткової фільтрації на гомоморфно защифрованим зображенням

Матриця D повертається з хмари користувачеві, який здійснює дешифрування цієї матриці з використання закритого ключа T_2 з отриманням матриці E, приклад якої показано на рис.4.7.

0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
28.67	30.44	30.22	29.00	36.78	15.22	70.00	22.11	43.44	47.00	42.11	47.22	46.11	49.22	56.22	48.33
44.22	28.33	31.11	27.89	53.11	20.89	69.44	30.56	49.89	29.11	37.56	53.33	41.56	59.11	41.00	44.11
61.78	21.44	51.11	45.22	49.67	13.44	59.56	52.00	49.22	39.78	37.89	44.78	53.00	54.33	50.56	30.67
53.44	22.22	31.44	58.44	29.44	34.00	38.67	66.11	62.44	48.78	55.67	51.33	64.33	57.89	40.44	25.44
51.22	40.00	55.44	55.11	28.33	39.22	45.33	65.44	66.11	47.44	54.67	51.00	47.78	51.67	43.33	27.22
35.78	40.33	35.00	46.22	38.22	62.44	41.00	69.78	59.00	32.44	39.78	67.67	46.56	41.22	29.56	32.78
44.22	41.44	36.89	41.89	41.44	63.78	35.89	61.00	63.11	39.89	29.33	69.78	33.00	20.78	31.44	24.67
21.00	42.89	21.33	29.33	45.44	69.33	23.11	61.00	46.78	46.11	40.11	56.00	41.22	39.89	24.56	19.00
25.11	32.44	38.00	26.78	39.22	70.11	19.44	51.00	49.00	48.11	54.22	52.00	36.22	54.67	35.44	10.33
18.33	23.33	44.11	30.56	54.00	67.11	34.33	43.78	48.44	48.33	61.00	40.89	58.56	50.33	39.67	22.78
18.22	24.67	62.00	49.67	53.22	50.33	36.00	40.11	49.56	51.67	67.22	47.89	64.00	24.11	58.56	24.33
34.56	52.11	67.11	68.44	71.33	36.78	48.33	39.22	40.33	46.11	69.00	47.89	57.44	9.00	53.56	35.56
47.44	57.56	56.78	73.56	53.56	29.56	41.22	54.56	23.67	45.44	53.89	45.67	30.78	13.44	53.78	33.44
53.56	59.56	38.56	67.89	44.67	44.44	37.89	39.33	41.67	53.44	43.11	48.33	15.11	23.78	57.67	42.89
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Рис.4.7. Приклад матриці E дешифрованих користувачем результатів часткової середньоарифметичної фільтрації

Над матрицею E користувач виконує операцію повної середньо-арифметичної фільтрації. Відповідний результат представлено у вигляді матриці V, яка представлена на рис.4.8.

0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.00	89.33	89.67	96.00	81.00	122.00	107.33	135.56	112.56	132.56	136.33	135.44	142.56	151.56	153.78	0.00
0.00	103.67	87.33	112.11	101.89	143.44	120.89	149.89	109.56	116.56	120.00	132.44	154.00	141.67	144.22	0.00
0.00	134.33	117.78	146.00	108.33	122.67	125.00	160.78	141.00	126.89	122.44	135.67	152.11	157.89	135.56	0.00
0.00	107.11	112.11	119.33	121.89	102.11	138.78	167.22	177.33	166.89	155.78	171.33	173.56	162.67	123.78	0.00
0.00	146.67	150.56	138.89	122.67	112.89	150.00	176.89	179.00	168.22	153.11	153.44	150.44	142.78	122.22	0.00
0.00	111.11	121.56	119.44	146.89	141.67	173.22	169.78	161.22	131.22	139.89	154.00	155.44	117.33	103.56	0.00
0.00	122.56	120.22	120.22	147.11	141.11	160.67	160.00	164.00	132.33	139.00	132.11	123.56	85.22	76.89	0.00
0.00	85.22	93.56	96.11	144.11	137.89	153.44	130.89	153.89	133.00	142.22	137.33	137.11	105.67	83.44	0.00
0.00	95.56	97.22	104.00	136.11	128.78	140.56	119.44	148.11	151.33	154.33	142.44	142.89	126.33	100.44	0.00
0.00	85.78	98.00	128.67	151.67	155.44	145.22	126.56	140.56	157.78	150.22	160.44	149.78	148.56	112.78	0.00
0.00	104.89	136.33	164.89	153.22	139.56	126.44	125.67	141.33	168.44	166.78	179.11	136.00	146.67	107.00	0.00
0.00	153.78	187.67	206.89	176.56	156.44	124.33	127.89	125.67	155.44	163.00	174.33	114.33	120.00	98.11	0.00
0.00	161.78	187.89	183.89	156.67	124.33	125.33	119.44	123.67	123.00	145.00	130.33	89.89	98.00	100.67	0.00
0.00	151.67	166.00	151.11	157.00	127.00	121.67	118.89	134.44	138.22	144.89	106.56	87.22	96.56	124.33	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Рис.4.8. Приклад матриці V зображення після виконання користувачем завершальної фази середньоарифметичної фільтрації над матрицею D.

Легко переконатися, що матриця V повністю відфільтрованого зображення за запропонованим гомоморфного шифрування зображень при їх

середньоарифметичній фільтрації практично повністю співпадає з матрицею B зображення, відфільтрованого у відповідності з класичним алгоритмом середньоарифметичної фільтрації.

Чільне місце в проведених експериментальних дослідженнях посідає визначення реальних часових характеристик ефективності запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації з використанням розроблених програмних засобів. В таблиці 4.1 наведені отримані експериментальним шляхом дані про час виконання основних обчислювальних процедур, передбачених запропонованим методом для апертури 3 x 3 та різних значень розміру зображення.

Таблиця 4.1

Час виконання основних процедур, передбачених розробленим методом гомоморфного шифрування для апертури 3 x 3

Розмір зображення	Час формування матриць в с.					
	A	B	C	D	E	F
16x16	0.002	0.00259	0.00035	0.00018	0.0	0.0
32x32	0.00599	0.01055	0.00094	0.00293	0.0	0.00195
64x64	0.01435	0.030652	0.001989	0.013868	0.0020444	0.006808
128x128	0.069407	0.132367	0.0098228	0.05337	0.00897	0.028566
256x256	0.216684	0.47862	0.03234	0.20133	0.035935	0.101108
512x512	0.855191	2.012119	0.1464588	0.8317465	0.1653213	0.433125
1024x1024	3.51835	8.245069	0.6290304	3.329616	0.686795	1.753675

В наведеній таблиці 4.1. показані часові характеристики формування базових матриць, які передбачені запропонованим в магістерській дисертації методом гомоморфного шифрування зображень при їх середньоарифметичній фільтрації.

Спеціальними експериментальними дослідженнями показано,що реально час формування матриць C та E, які співвідносяться з операціями гомоморфного шифрування та дешифрування зображень відповідно, практично співпадають з часом потрібним для пересилки по мережі Інтернет матриць зображень відповідного розміру. Це свідчить про те, що ці операції в реальних системах можуть бути суміщеними у часі і, таким чином, не займати часових ресурсів роботи обчислювальної платформи користувача.

В таблиці 4.2 наведені отримані експериментальним шляхом часові характеристики формування базових матриць у відповідності з процедурами, передбаченими методом гомоморфного шифрування зображень при їх середньоарифметичній фільтрації для апертури 5 х 5 та різних значень розміру зображення.

Таблиця 4.2

Час виконання основних процедур, передбачених розробленим методом гомоморфного шифрування для апертури 5 х 5

Розмір зображення	Час формування матриць в с.					
	A	B	C	D	E	F
16x16	0.00245	0.003956	0.0	0.00093	0.0	0.00098
32x32	0.00769	0.016223	0.0	0.00400	0.00099	0.00339
64x64	0.017818	0.062844	0.001996	0.01335	0.00206	0.00908
128x128	0.058768	0.24327	0.00997	0.054569	0.00792	0.035812
256x256	0.221704	0.99601	0.041805	0.227145	0.04514	0.151477
512x512	0.84267	4.63703	0.144129	0.879070	0.15498	0.654501
1024x1024	3.44627	17.35410	0.627648	3.50639	0.718754	2.722362

В наведеній таблиці 4.2. показані часові характеристики формування базових матриць, які передбачені запропонованим в магістерській дисертації методом гомоморфного шифрування зображень при їх середньоарифметичній фільтрації.

Для перевірки функціональної коректності роботи запропонованого в магістерській дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації в розробленій і представленій в доданках програмі передбачено програмне здійснення класичної процедури середньоарифметичної фільтрації зображення з різними значеннями апертур, представленою матрицею А зі збереженням відфільтрованого зображення в матриці цілих чисел В.

В таблиці 4.3 наведені отримані експериментальним шляхом часові характеристики формування базових матриць у відповідності з процедурами, передбаченими запропонованим у другому розділі магістерської дисертації методом гомоморфного шифрування зображень при їх середньоарифметичній фільтрації для апертури 7 х 7 та різних значень розміру зображення.

Таблиця 4.3

Час виконання основних процедур, передбачених розробленим методом гомоморфного шифрування для апертури 7 x 7

Розмір зображення	Час формування матриць в с.					
	A	B	C	D	E	F
16x16	0.001446	0.006247	0.0	0.0	0.00099	0.00158
32x32	0.00699	0.02776	0.00100	0.005	0.001	0.00302
64x64	0.01764	0.11655	0.002023	0.02027	0.003	0.0108
128x128	0.060857	0.44722	0.02786	0.0817	0.008	0.04177
256x256	0.22114	1.83616	0.03461	0.32314	0.03987	0.18982
512x512	0.854098	7.89993	0.14401	1.20527	0.16651	0.82228
1024x1024	3.468464	32.157763	0.608082	5.507016	0.782907	3.3709

Аналіз наведених в таблиці 4.3 даних дозволяє зробити висновки про те, що час виконання основних процедур, пов’язаних зі скануванням та обробкою точок зображення реально пропорційний об’єму зображень. Важливим результатом, який слідує із аналізу даних, наведених в таблиці 4.3 є те, що запропонований метод дозволяє зменшити об’єм обчислень навіть при виконанні середньоарифметичної фільтрації зображення на одному процесорі. Дійсно, не важко переконатися, що наприклад, як видно з останнього рядка таблиці 4.3, час формування матриці B за класичним алгоритмом складає 32.15 секунд (розмір зображення 1024 на 1024 точки). В той же час, сумарний час формування матриць D та E, який співвідноситься з часом часткової середньоарифметичної фільтрації та часом фінальної стадій такої фільтрації становить 6.28 секунд. Це означає, що навіть при виконання на одному процесорі, запропонований у другому розділі магістерської дисертації метод гомоморфного шифрування зображень при їх середньоарифметичній фільтрації дозволяє зменшити час фільтрації практично в 5 раз. Це досягається за рахунок спеціальної організації обчислювального процесу, яка виключає дублювання обчислень, притаманне класичному методу середньоарифметичної фільтрації.

При експериментальному дослідженні запропонованого методу з використанням віддалених обчислювальних платформ, які задіють до процесу часткової середньоарифметичної фільтрації 32 процесори, реальний час формування матриці D для зображень розміром 1024 x 1024 та апертурі 7 x 7

становить 0.48 секунд. Це означає, що при повному задіяні можливостей запропонованого в магістерській дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації на віддалених обчислювальних потужностях, прискорення виконання цього виду обробки зображень приблизно складає 30.

Аналіз експериментальних даних, наведених в таблицях 4.1 – 4.3 показують, що ефективність запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації на віддалених обчислювальних потужностях залежить від розміру апертури: чим більше розмір апертури, тим більш ефективним є розроблений метод, як в плані прискорення обробки зображення та і в плані зменшення питомої ваги обчислень, які здійснюються на обчислювальній платформі користувача в загальному об’єму обчислень.

За даними наведеними в таблицях 4.1 – 4.3 можна зробити висновки про зменшення питомої ваги обчислень, які здійснюються на обчислювальній платформі користувача. Результати відповідних обчислень, виконаним по даним таблиць 4.1 – 4.3 наведені в таблиці 4.4.

Таблиця 4.4

Залежність питомої ваги обчислень, які здійснюються на обчислювальній платформі користувача в залежності від розміру апертури.

Розмір апертури	Значення питомої ваги обчислень, які виконуються користувачем при реалізації середньоарифметичної фільтрації на віддалених комп’ютерних потужностей
3 x 3	0.12
5 x 5	0.10
7 x 7	0.09
9 x 9	0.07
11 x 11	0.05

Таким чином, для зображень реального розміру, за експериментальними даними прискорення середньоарифметичної фільтрації за рахунок використання розробленого методу з залученням віддалених обчислювальних потужностей складає близько 30 раз.

Висновки до розділу 4.

В результаті виконання досліджень, направлених на створення програмних засобів процесів захищеної віддаленої середньоарифметичної фільтрації зображень та здійснення експериментальних досліджень розробленого в другому розділі магістерської дисертації методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації можуть бути зроблені наступні висновки.

1. Розроблені програмні засоби для практичної реалізації та дослідження характеристик ефективності запропонованого нового методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації, зокрема для визначення часових характеристик об'єму обчислень, які виконуються на віддалених обчислювальних потужностях та об'ємів обчислень, які пов'язані з реалізацією функцій гомоморфного шифрування та дешифрування зображень і, відповідно, здійснюються на обчислювальній платформі користувача.

2. Експериментальні дослідження розроблено методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації повною мірою довели його функціональну працездатність.

3. Експериментальними дослідженнями доведено, що запропонований метод гомоморфного шифрування зображень при їх середньоарифметичній фільтрації дозволяє зменшити час фільтрації практично в 5 раз в порівнянні з класичним алгоритмом середньоарифметичної фільтрації навіть при використанні одного процесора. Це досягається за рахунок спеціальної організації обчислювального процесу в запропонованому методі, яка виключає дублювання обчислень, притаманне класичному методу середньоарифметичної фільтрації.

4. Проведені експериментальні дослідження з використанням розроблених програмних засобів показали, що для реальних зображень розміром 1024 х 1024 пікселів та апертурі 7 х 7 використання запропонованого в магістерській дисертації методу гомоморфного шифрування зображень при їх середньо-арифметичній фільтрації на віддалених обчислювальних потужностях, дозволяє

прискорити виконання цієї важливої в прикладному плані процедури приблизно в 30 раз.

5. Аналіз експериментальних даних показав, що ефективність запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації на віддалених обчислювальних потужностях залежить від розміру апертури: чим більше розмір апертури, тим більш ефективним є розроблений метод, як в плані прискорення обробки зображення та і в плані зменшення питомої ваги обчислень, які здійснюються на обчислювальній платформі користувача в загальному об’єму обчислень.

РОЗДІЛ 5
РОЗРОБЛЕННЯ СТАРТАП–ПРОЕКТУ

5.1. Опис проблеми

Потужний прогрес засобів передачі інформації та технологій глобальних мереж педалював появу і динамічний розвиток нової технології комп'ютерної обробки інформації - хмарних обчислень.

Хмарні технології передбачають віддалене надання широкому колу користувачів,, на комерційній основі, певних ресурсів із загального в масштабах планети пулу. При цьому, в якості вказаних ресурсів можуть виступати обчислювальні потужності багатопроцесорних комп'ютерних систем, пам'ять глобальних сховищ інформації, а також програмне забезпечення. Надання користувачеві вказаних вище ресурсів реалізується виходячи з наявності вільних ресурсів у планетарному масштабі, так що користувач не знає на яких обчислювальних потужностях вирішується його прикладне завдання або де зберігаються його персональні дані. Саме непрозорість для користувача процесу надання ресурсів і зумовила назву – хмарні технології.

Використання хмарних технологій значною мірою дозволяє вирішити одвічну проблему обмеженості наявних ресурсів для користувача: в рамках вказаних технологій кожному з них може бути надана обчислювальна потужність тисяч процесорів та практично необмежений обсяг пам'яті для віддаленого зберігання його персональні дані.

Разом з тим, поява та розширення практичного використання хмарних технологій істотним чином впливає на безпеку комп'ютерної обробки інформації у всіх галузях людської діяльності. Можливості використання потужних обчислювальних ресурсів сучасних суперкомп'ютерів, що надаються хмарними технологіями, дозволяють потенційним зловмисникам багатократно підвищити дієвість технологій порушення захисту існуючих систем інформаційної безпеки. переважна частина відомих методів порушення захисту в тій чи іншій формі застосовує перебір, який може бути ефективно

розпаралелений при використанні віддалених багатопроцесорних комп'ютерних системам, доступ до яких надають сучасні хмарні технології.

Суттєвою перепоною на шляху широкого використання можливостей хмарних технологій в плані підвищення продуктивності обробки даних користувачів і, зокрема, обробки зображень, постає відсутність до теперішнього часу ефективних механізмів захисту конфіденційних даних користувачів в процесі їх передачі та обробки на віддалених обчислювальних системах. Особливо гостро постає проблема захисту даних користувачів при їх обробці на віддалених і, відповідно, неконтрольованих обчислювальних системах. І якщо при передачі даних вони можуть бути захищені з використанням існуючих криптографічних механізмів шифрування, то при обробці проблема захисту даних користувачів і, зокрема, зображень, не знаходить прийнятного вирішення до теперішнього часу.

При реалізації середньоарифметичної фільтрації зображень на віддалених і непідконтрольних користувачеві комп’ютерних системах існує реальна небезпека несанкціонованого доступу до зображень конфіденційного характеру. Потенційно вразливими для незаконного доступу до зображення є канал Інтернету, в якому зображення можуть бути перехопленими та віддалені комп’ютерні система, на які власне здійснюється середньоарифметична фільтрація зображення.

Особливо гостро дана проблема стоїть для систем моніторингу об’єктів з космосу, адже вартість знімків є надзвичайно високою. Окрім цього існують системи контролю, які використовуються правоохоронними структурами. Для них захищенність даних є стратегічно важливою умовою.

Для виключення можливостей несанкціонованого доступу зловмисником до зображень, що передаються каналами Інтернет та оброблюються на віддаленій комп’ютерній системі за допомогою середньоарифметичної фільтрації з метою підвищення їхньої якості, пропонується метод віддаленої

захищенної середньоарифметичної фільтрації зображень з залученням хмарних технологій.

Таким чином, наукова задача забезпечення захисту зображень в процесі їх середньоарифметичної фільтрації на неконтрольованих віддалених обчислювальних системах великої потужності є актуальною та практично важливою для сучасного етапу розвитку комп'ютерних технологій.

Відповідна мета роботи полягає в підвищенні ефективності гомоморфного шифрування зображень під час їх віддаленої середньоарифметичної фільтрації на непідконтрольних комп'ютерних системах, за рахунок зменшення питомої ваги обчислень, що виконуються на обчислювальній платформі користувача.

На сьогодні найбільшою перешкодою для широкого використання переваг хмарних обчислень для організації віддаеної обробки зображень є їх вразливість до несанкціонованого доступу під час передачі та безпосередньої обробки на віддалених комп'ютерних потужностях. Існуючі засоби шифрування інформації дозволяють забезпечити таємність зображень лише під час їх передачі через Інтернет, але не в процесі їх безпосередньої обробки на віддалених комп'ютерних системах [4]. Для переважної більшості прикладних завдань комп'ютерного аналізу зображень важливо дозволити лише обмежений доступ до них стороннім особам.

В рамках представленої магістерської дисертації для досягнення сформульованої вище мети теоретично обґрунтовано, розроблено та досліджено метод гомоморфного шифрування зображень для захисту їх під час середньоарифметичної фільтрації на віддалених комп'ютерних системах, відмінністю якого є використання в якості основного елементу захисту перемішування стовпців матриці зображень в секретному порядку. В рамках розробленого методу визначено процедури часткової середньоарифметичної фільтрації, яка здійснюється на віддалених системах, а також процедури завершальної фази фільтрації, яка виконується на обчислювальній платформі користувача після гомоморфного дешифрування отриманого із хмари

зображення. Запропонований метод гомоморфного шифрування зображень для їх захищеної фільтрації на основі перемішування стовпців дозволяє, за рахунок використання віддалених обчислювальних потужностей, прискорити цю операцію на 1-2 порядки, що практично збігається з аналогічними показником найбільш швидкодіючого варіанту захисту зображень на основі адитивного маскування. Вагома перевага розробленого методу полягає в більш високому рівні захищеності від спроб, з використанням статистичного аналізу, отримати незаконний доступ до зображень під час їх обробки на непідконтрольних користувачу віддалених комп'ютерних системах.

Основні напрямки застосування розробленого методу гомоморфного шифрування зображень та вигоди користувачам від її практичного застосування зведені в таблицю 4.1.

Аналіз потенційних техніко-економічних переваг запропонованої методу гомоморфного шифрування зображень (чим відрізняється від існуючих аналогів та замінників) порівняно із пропозиціями конкурентів передбачає:

- визначення переліку техніко-економічних властивостей та характеристик ідеї ;
- визначення попереднього кола конкурентів (проектів-конкурентів) або товарів-замінників чи товарів-аналогів, що вже існують на ринку;
- проводиться збір інформації щодо значень техніко-економічних показників для ідеї власного проекту та проектів-конкурентів відповідно до визначеного вище переліку;
- проводиться порівняльний аналіз показників: для власної ідеї визначаються показники, що мають а) гірші значення (W, слабкі); б) аналогічні (N, нейтральні) значення; в) кращі значення (S, сильні).

Таблиця 5.1.

Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Гомоморфне шифрування зображень для захисту при їх обробці на віддалених комп'ютерних потужностях й	1. Для комп'ютерної обробки медицинських зображень в системах віддаленої діагностики захворювань	Зменшення часу обробки зображень, що дозволяє більш оперативно використовувати інформацію, що міститься в зображеннях. Збільшення об'ємом інформації, що оброблюються комп'ютерними засобами, що дозволяє приймати більш виважені рішення
	2. 2. Для організації комп'ютерної обробки аерокосмічних зображень з метою організації ефективного моніторингу стану природного середовища	Підвищення оперативності отримання інформації про стан природного середовища за рахунок прискорення комп'ютерної обробки .
	3. В системах комп'ютерної дефектоскопії	Збільшення об'ємів об'єктів діагностики при підвищенні надійності отриманих рішень.

5.2 Аналіз ринкових можливостей запуску стартап-проекту

Базовими показниками розробленого проекту організації гомоморфного шифрування зображень для захисту виконання над ними середньоарифметичної фільтрації на віддалених комп'ютерних системах підвищеної потужності при використані хмарних технологій можна вважати:

- Рівень захищеності від незаконних спроб отримання доступу до зображень користувачів під час обробки їх на непідконтрольних користувачам віддалених обчислювальних системах – вимірюється в витратах ресурсів на підбір таблиці перестановки стовпців матриці зображення, яке використовується в якості основного елементу гомоморфного шифрування зображень користувача.
- Рівень захищеності від несанкціонованих спроб відновлення базових елементів конфіденційних зображень через відновлення контурного представлення зображення – вимірюється в витратах ресурсів стороні, що здійснює таку спробу для проведення значних за обсягом обчислень пов'язаних з виконанням статистичного аналізу значної кількості гомоморфне зашифрованих зображень в процесі їх обробки них на непідконтрольних користувачам віддалених обчислювальних системах.
- Об'єм витрат обчислювальних ресурсів користувача на здійснення гомоморфного шифрування зображення та його гомоморфне дешифрування після обробки на віддалених комп'ютерних системах - вимірюється в процентному збільшенні/зменшенні часових затрат на реалізацію програм.
- Об'єм витрат пам'яті, потрібної для здійснення запропонованого методу гомоморфного шифрування зображень - вимірюється в об'ємі додаткових ресурсів пам'яті в Кбайтах.

В якості конкуруючих проектів можна розглядати проект СПЕКТР-4 для комп'ютерної обробки аерокосмічних зображень з використанням можливостей хмарних технологій [55]. В проекті здійснюється гомоморфне шифрування зображень для їх захистку при віддаленій реалізації медіанної фільтрації зображень. Технічна реалізація конкуруючого проекту передбачає плаваюче

сортування вибірки точок апертри і співставлення їм у відповідність проміжки фіксованого інтервального кодування. Таким чином здійснюється базова процедура медіанної фільтрації – збереження відношення порядку числа, що робить можливим подальше порівняння гомоморфно шифрованих зображень. Це забезпечує властивість зворотності гомоморфного дешифрування зображень.

Закритий характер трансформації зображення, яке виконуються в процесі інтервального гомоморфного шифрування зображень забезпечується за рахунок того, що таблиця інтервалів значень, що відповідають одному конкретному реальному значення генерується самим користувачем і використовується ним в якості секретного ключа гомоморфного шифрування зображень .

Представлений в розробці проект забезпечує більш високий рівень захисту від спроб незаконного відновлення конфіденційних зображень з використанням технологій статистичного аналізу, в порівнянні з конкуруючим проектом – СПЕКТ-4.

Другим конкуруючим проектом є HEKLA, в якому здійснюється гомоморфне шифрування зображень при їх середньоарифметичній фільтрації з використанням можливостей сучасних хмарних технологій [56]. В якості базового елементу гомоморфного шифрування використовується адитивне маскування. Гомоморфне дешифрування здійснюється через віднімання від зашифрованого зображення зашифрованого зображення маски. Тобто для гомоморфного дешифрування потрібно мати попередньо сформовані зображення масок та їх відфільтровані варіанти. підготовка таких елементів маскування потребує значних за обсягом комп’ютерних ресурсів що реалізуються на обчислювальній платформі користувача.

Представлений в рамках магістерської дисертації проєкт забезпечує вищий рівень захисту від незаконних спроб доступу до конфіденційних зображень, а також кращі часові характеристики у порівнянні з методом, реалізований в системі HEKLA.

В таблиці 4.2 наведено порівняльні характеристики представленого в магістерській дисертації проєкту з конкуруючими проектами, характеристики яких наведені вище.

Таблиця 5.2

Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ пп	Техніко-економічні характеристики ідеї	Оцінка концепції конкурентів			W	N	S
		Мій проект	СПЕКТ-4	HEKLA			
1	Об'єм ресурсів для незаконної гомоморфної дефрації зображень	2 880 000	67 000	88 000			+
2	Рівень захищеності від незаконних реконстру-ювання наближених контурів зображення	60 000	82 000	47 000		+	
3	Об'єм часових ресурсів на здійснення гомоморфного шифрування зображень	-120%	50%	67%			+
4	Об'єм ресурсів комп’ютерної пам'яті на реалізацію гомоморфного шифрування	120	80	35	+		

Таким чином, представлений в магістерській дисертації проєкт забезпечує помітне прискорення виконання процедур середньоарифметичної фільтрації зображень в порівнянні з конкурентами. Також, представлений проєкт забезпечує вищий рівень захищеності зображень конфіденційного характеру.

В зазначених вище в конкуруючих проектах захищеність зображень під час їх віддаленої обробки з використанням технологій гомоморфного шифрування реалізовано також на достатньо високому рівні, проте при їх використанні досягається помітно менша ефективність захищеної фільтрації зображень з точки зору швидкодії. Тобто, представлений в рамках магістерської дисертації проєкт забезпечує значно вищий рівень швидкості обчислювальної реалізації захищених обчислень на віддалених комп'ютерних потужностях.

Важливою ланкою розробки стартапу є аудит технології, за допомогою якої можна реалізувати ідею запропонованого в магістерській дисертації проєкту. Вихідним результатом проекту є програмне забезпечення. Визначення технологічної здійсненності ідеї запропонованого проєкту передбачає аналіз наступних компонентів:

- за якою програмною технологією буде реалізовано програмний продукт відповідно до запропонованої ідеї проєкту ?
- чи дотепер існують такі технології, чи, можливо, їх потрібно розробити/доробити ?
- чи доступні передбачені проектом технології авторам проєкту ?

Вихідним результатом проекту є програмне забезпечення, яке реалізує гомоморфне шифрування зображень при їх середньоарифметичній фільтраціх. Процедура середньоарифметичної фільтрації є стандартизованою, достатньо повно вивченою і всебічно дослідженою. Для практичної реалізації середньоарифметичної фільтрації створені відповідні програмні засоби, в тому числі і для багатопроцесорних комп'ютерних систем. Таким чином, розробка програмного забезпечення здійснюється за відомими технологіями програмної інженерії відповідними фахівцями. Тому можна вважати, що технології для реалізації ідей проєкту вже існують і вони є загальновідомими та загальнодоступними.

Наступним етапом стартапу є визначення ринкових можливостей програми, яка створена на основі проєкту. Ці можливості можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Дані про стан ринкового середовища зведено до таблиці 4.3.

Таблиця 4.3

Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	200
2	Загальний обсяг продаж, (для сектора)	80000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Значна конкуренція, велика кількість аналогів
5	Специфічні вимоги до стандартизації та сертифікації	Відсутні
6	Середня норма рентабельності в галузі (або по ринку), %	25%

З даних таблиці 4.3 слідує, що, в цілому, за проведеним попереднім оцінюванням, ринок програм для гомоморфного шифрування зображень при їх віддаленій середньоарифметичній фільтрації для поліпшення якості зображень та їх актуалізації є привабливим для входження.

Додаткової ринкової привабливості запропонованому проєкту додає розширення використання робототехнічних комплексів на основі концепції технічного зору та штучного інтелекту. За даними [34] створення таких

комплексів для масової заміни людьми роботизованими комплексами на основі технічного зору стане пріоритетним напрямком в найближче десятиліття. Важливе місце в цих системах відіграють системи комп'ютерної обробки та аналізу зображень, яке для портативних вбудованих мікроконтролерів може відбуватися в режимі реального часу за рахунок залучення можливостей хмарних технологій.

Ключовим етапом розробки стартапу є визначення потенційних клієнтів ринку программного забезпечення проєктного рішення. Відповідні розрахунки наведені в таблиці 4.4.

Проведений аналіз ринкової спроможності показав, що запропонований програмний продукт стимулює ринкову зацікавленість у значного числа державних установ та приватних, які є учасниками ринку. Найбільшу зацікавленість у розроблених програмних засобах мають лікарні та приватні медицинські компанії, що займаються віддаленою діагностикою різних захворювань з залученням інтерконтинетальних баз даних. Це пов'язано з потребою своєчасної обробки потоків з мільйонів зображень в межах жорстких часових обмежень. У разі неможливості забезпечення достатньої швидкості обробки віддаленої зображень, можуть виникнути помилки в діагностуванні хвороб або втрата оперативності процедур медицинської діагностиуки. Відповідно, в таких ситуаціях лікарні та приватні клініки нестимуть значні фінансові та репутаційні збитки через невиконання своїх основних задач.

Значну зацікавленість до прискорення фільтрації зображень проявляють машинобудівні підприємства та установи, що експлуатують авіаційний чи залізничний транспорт. Вони потребують оперативної обробки великої кількості зображень отриманих в результаті ультразвукової діагностики стану несучих конструкцій.

Таблиця 4.4

Аналіз ринку збуту

№ пп	Потреба, що формує ринок	Цільові сегменти ринку	Відмінності у поведінці різних потенційних цільових груп	Вимоги споживачів до товару
1	Потреба швидкої обробки потоків зображень медицинського характеру	Лікарні, приватні компанії, що займаються обстеженням та дослідженням захворювань	Необхідність швидкого порівняння великої кількості зображень для ефективності діагностики	Високий рівень захищеності зображень від незаконного доступу
2	Забезпечення високої надійності комп'ютерної дефектоскопії	Машинобудівні підприємства та установи, авіакомпанії та державна залізниця.	Високі вимоги щодо надійності контролю стану об'єктів дефектоскопії	Жорсткі вимоги до швидкості обробки зображень задля підвищення оперативності дефектоскопії
3	Обробка зображень аерокосмічного характеру	Деражавні та приватні підприємства, що займаються дис.-танційним зондуванням стану поверхні Землі	Активне втручання в роботу	Конфіденційність оброблюваних зображень в процесі їхньої віддаленої обробки та достовірність результатів

Іншою зацікавленою стороною є державні та приватні установи, що займаються моніторингом стану земної поверхні та природоохоронною діяльністю з використанням засобів дистанційного зондування поверхні Землі з використанням космічних апаратів чи спеціальних літаків Ан-30.

Для таких застосувань потрібно забезпечувати високу оперативність обробки зображень та їх секретність, пов’язану з великою вартістю залучення засобів отримання вказаних зображень.

Таким чином, розроблений проект задовільняє інтереси кілької маштабних груп-учасників ринку і, при цьому є конкурентноспроможним. В таблиці 4.5 представлено складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities).

Таблиця 4.5

SWOT- аналіз стартап-проекту

Сильні сторони: Проєкт забезпечує більший, в порівнянні з конкурентами рівень захисту зображень при їх віддалений обробці. Проєкт забезпечує більшу швидкість обробки потоків зображень	Слабкі сторони: Слабкою стороною є потреба в додаткових програмних ресурсіах на організацію поєднання пересилок зображень і перемішування їх стовпців.
Можливості: Розширення ринку збуту та закріплення проєкту як стандарту в віддаленої обробки зображень спрямованої на підвищенння їхньої якості, шляхом видалення імпульсних завад.	Загрози: Можливість появи в компанії джерела витоку секретної інформації щодо ключів, які використовуються для гомоморфного шифрування зображень

Висновки до розділу 5

Проведенні в рамках поточного розділу магістерської дисератації дослідження, спрямованні на виявлення і оцінку можливостей ринкового впровадження розробленого проєкту, дозволяють зробити такі висновки:

1. Розроблений програмний продукт та ідея гомоморфного шифрування зображень для їх захисту від несанкціонованого доступу під час реалізації на віддалених обчислювальних потужностях мають велику конкурентоздатність в силу того, що здатні забезпечити на порядок вищий рівнень ефективності з точки зору прискорення обробки зображень та надійності захисту віл спроб незаконного доступу до конфіденційних зображень. Тобто розроблений метод гомоморфного шифрування зображень конкурує з існуючими проектами в аспекті забезпечення захищенності оброблюваних даних. Зокрема, він забезпечує достатньо високий рівень захисту від незаконних спроб реконструювання контурів зображення методами статистичного аналізу. Таким чином, теоретично обґрунтований та детально розроблений в рамках магістерської дисертації метод гомоморфного шифрування зображень да захищеної середньоарифметичної фільтрації забезпечує більший рівень захищеності в порівнянні з конкуруючими проектами. Це досягнуто за рахунок використання перестановочних шифрів, інваріантних до характеру операцій, які застосовуються в процесі середньоарифметичної фільтрації зображень.

2. Доведене існування широкого кола потенційних покупців програмного забезпечення для захищеної обробки зображень з високим рівнем оперативності в режимі реального часу. До основних зацікавлених в запропонованій розробці учасників ринку відносяться фірми, що займаються моніторингом об’єктів з метою відслідковування загроз природних катаклізмів, підприємств, що займаються технічною дефектоскопією рухомих засобів, дослідницькі центри та компанії що працють в сфері медицини. Окрім цього, ринок збуту може бути розширено невеликими дослідницькими центрами та компаніями невеликого масштабу. Розробка може бути ефективно використана

в перспективних робототехнічних системах широкого застосування з функціями технічного зору, що працюють в режимі реального часу і реалізують функції сприйняття та розпізнавання зображень.

3. Проведений аналіз показав відносно невеликий рівень конкуренції в сфері оперативної захищенної обробки зображень з використанням хмарних технологій. Це пов’язано з тим, що існуючі дотепер проєкти не здатні забезпечити достатнього рівня захищеності, який задовільняє основних учасників ринку збуту, а саме компанії, що займаються моніторингом об’єктів, та організації, які зацікавленні в моніторингу природного середовища та медицинської віддаленої діагностики.

В И С Н О В К И

В результаті проведення комплексу науково-практичних досліджень, які складають магістерську дисертацію і направлені на підвищення ефективності захищеної обробки зображень, зокрема їх середньоарифметичної фільтрації на віддалених обчислювальних потужностях за рахунок розробки перестановочного методу гомоморфного шифрування зображень отримані результати, які можуть бути сформульовані у вигляді наступних висновків:

1. Найбільш доцільним засобом зображень в процесі їх обробки на віддалених комп'ютерних потужностях є гомоморфне шифрування, інваріанте до операцій обробки зображень і, зокрема операцій, які скидають процедуру середньоарифметичну фільтрацію зображень. Проведений аналіз операцій, що лежать в основі цього виду фільтрації зображень а також проведений огляд існуючих універсальних методів гомоморфного шифрування показали, що цей клас методів гомоморфного шифрування не забезпечує потрібної для задач практики ефективності захисту зображень в процесі їх середньоарифметичної фільтрації на віддалених комп'ютерних системах.

2. Проведений огляд існуючих спеціалізованих методів гомоморфного шифрування для захисту зображень під час їх середньоарифметичної фільтрації показав, що методи, які базуються на операціях адитивного маскування не забезпечують необхідного для задач практики рівня захищеності від атак на основі статистичного аналізу.

3. Теоретично обґрунтовано, розроблено та досліджено метод гомоморфного шифрування зображень для захисту їх під час середньоарифметичної фільтрації на віддалених комп'ютерних системах, відмінністю якого є використання в якості основного елементу захисту перемішування стовпців матриці зображень в секретному порядку. В рамках розробленого методу визначено процедури часткової середньоарифметичної фільтрації, яка здійснюється на віддалених системах, а також процедури завершальної фази фільтрації, яка виконується на

обчислювальній платформі користувача після гомоморфного дешифрування отриманого із хмари зображення.

4. Розроблений метод захищеної фільтрації на основі перемішування стовпців дозволяє, за рахунок використання віддалених обчислювальних потужностей, прискорити цю операцію на 1-2 порядки, що практично збігається з аналогічними показником найбільш швидкодіючого варіанту захисту зображень на основі адитивного маскування.

5. Основна перевага розробленого методу полягає в більш високому рівні захищеності від спроб, з використанням статистичного аналізу, отримати незаконний доступ до зображень під час їх обробки на непідконтрольних користувачу віддалених комп'ютерних системах.

6. Теоретично обґрунтовано та запропоновано модифіковану процедуру гомоморфного шифрування потоків зображень для їх захищеної середньоарифметичної фільтрації на віддалених комп'ютерних системах в рамках хмарних технологій. Відмінність запропонованої модифікації полягає в тому, що перемішування стовпців матриць зображень в процесі гомоморфного шифрування не обмежується рамками окремих зображень, а здійснюється в рамках групи зображень.

7. Розроблені програмні засоби для практичної реалізації та дослідження характеристик ефективності запропонованого нового методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації, зокрема для визначення часових характеристик об'єму обчислень, які виконуються на віддалених обчислювальних потужностях та об'ємів обчислень, які пов'язані з реалізацією функцій гомоморфного шифрування та дешифрування зображень і, відповідно, здійснюються на обчислювальній платформі користувача.

8. Експериментальні дослідження розроблено методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації повною мірою довели його функціональну працездатність.

9. Експериментальними дослідженнями доведено, що запропонований метод гомоморфного шифрування зображень при їх середньоарифметичній фільтрації дозволяє зменшити час фільтрації практично в 5 раз в порівнянні з класичним алгоритмом середньоарифметичної фільтрації навіть при використанні одного процесора. Це досягається за рахунок спеціальної організації обчислювального процесу в запропонованому методі, яка виключає дублювання обчислень, притаманне класичному методу середньоарифметичної фільтрації.

10. Проведені експериментальні дослідження з використанням розроблених програмних засобів показали, що для реальних зображень розміром 1024 х 1024 пікселів та апертурі 7 х 7 використання запропонованого в магістерській дисертації методу гомоморфного шифрування зображень при їх середньо-арифметичній фільтрації на віддалених обчислювальних потужностях, дозволяє прискорити виконання цієї важливої в прикладному плані процедури приблизно в 30 раз.

11. Аналіз експериментальних даних показав, що ефективність запропонованого методу гомоморфного шифрування зображень при їх середньоарифметичній фільтрації на віддалених обчислювальних потужностях залежить від розміру апертури: чим більше розмір апертури, тим більш ефективним є розроблений метод, як в плані прискорення обробки зображення та і в плані зменшення питомої ваги обчислень, які здійснюються на обчислювальній платформі користувача в загальному об’єму обчислень

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Russ J.C. The Image Processing Handbook. 7- Edition / J.C. Russ, F. Brent Neal // CRC Press.- 2016.- 1053 p.
2. Sathish V. Cloud-based Image Processing With Data Priority Distribution Mechanism / Sathish V.A. , Sangeetha T.A. // Journal of Computer Applications.- Vol.6, №1.- 2013.- P. 6-8.
3. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing/ N. Boroujerdi, S. Nazem // IJCSI International Journal of Computer Science Issues. – Vol. 9. – 2012. – №3. – P. 169-180.
4. Гуменюк І.О. Метод віддаленої середньоарифметичної фільтрації зображень / І.О. Гуменюк, О.Х. Слюсаренко // Альманах науки.- 2019.- № 11 (32).- С.40-43.
5. Грузман И.С. Цифровая обработка изображений в информационных системах / И. С. Грузман, В. Х. Киринчук – Новосибирск : НГТУ, 2002. − 352 с.
6. Xia Z.. Towards privacy-preserving content-based image retrieval in cloud computing / Z. Xia, X. Sun, Z.Qin, K. Ren // IEEE Trans. Cloud Comput. – 2018.- No.6,- PP. 276–286.
7. Markovskyi O.P. The method of accelerated secure image filtering on remote computer systems / O.P. Markovskyi, I.O.Gymenuk, Alireza Mirataei, J.I. Turoshanko, M.O. Voloshuk // Telecommunication and information technology.- 2019,- Vol.65.-no.4.- PP.99-110.
8. Бондарев В. Н. Цифровая обработка сигналов: методы и средства : учеб. пособие / В. Н. Бондарев, Г.П. Трестер, В. С. Чернега. – Севастополь : СевГТУ, 1999. − 398 с.
9. Ватолин Д.И. Методы сжатия данных / Д.И. Ватолин, А.Х. Ратушняк, М.П. Смирнов, В.Ю. Юкин. – М. : Диалог-Мифи, 2002. – 384 с.
10. Прэтт У. Цифровая обработка изображений / У. Прэтт. /– М. : Мир, 1982. – 480 с.

11. Марковський О.П. Захищена реалізація фільтрації зображень в GRID-системах / О.П. Марковський, М. О. Невдащенко, А.М. Білашевська // Вісник Національного технічного університету України ”КПІ” Інформатика, управління та обчислювальна техніка. – Київ: ВЕК+. – 2014. – № 61. – С. 105-109.
12. Bardis Nikolaos. Secure Implementation of Modular Exponentiation on Cloud Computing Resources / N.G. Bardis, O.P.Markovskyi // Proceeding of International Conference Applied Mathematics, Computational Science and Systems Engineering. Athens, Greece, October 6-8, - 2017. - P.90-96.
13. Лисицин В.Х. Практикум по фотограмметрии и дистанционному зондированию / В. Х. Лисицин. – Харьков : ХНАГХ, 2006. – 200 с.
14. Форсайт Д. Компьютерное зрение. Современный подход / Д. Форсайт, Р. Понс. – М. : Вильямс, 2004. – 928 с.
15. Шапиро Л. Компьютерное зрение / Л. Шапиро, Дж. Стокман. – М. : Бином. Лаборатория знаний, 2006. – 716 с.
16. Савиных В. П. Аэрокосмическая фотосьемка / В. П. Савиных, А. С. Кучко, А. Х. Стеценко. – М. : КартоГеоЦентр Геоиздат, 1997. – 378 с.
17. Буйбарова М.Ф. Метод захищеної реалізації перетворень Фур’є на віддалених розподілених комп’ютерних системах / М.Ф. Буйбарова, Ю.М. Виноградов, В.Х. Приймак // Вісник Національного технічного університету України “КПІ” Інформатика, управління та обчислювальна техніка. – К.: ТОО „ВЕК+”. – № 64. – 2016. – С. 64-71.
18. Анісімов А.В. Алгоритмічна теорія великих чисел / А.В. Анісімов. – К.: Академперіодијка. – 2001. – 153 с.
19. Березин А.С. Защита информации в открытых сетях / А.С. Березин, О.А. Петренко // Корпоративные системы. – 2001. – № 2. – С.65-69.
20. Бєйкер А. Введение в теорию чисел / А. Бєйкер. – Мн.: Вышєйш. шк. – 1999. – 340 с.

21. Бриль В.М. Сучасні методи та засоби криптографічного перетворення інформації з метою її захисту / В.М.Бриль. – К.: НТУУ “КПІ”. – 1999. – 83 с.
22. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing/ N. Boroujerdi, S. Nazem // IJCSI International Journal of Computer Science Issues. – Vol. 9. – Issue 4. – 2012. – №3. – PP. 169-180.
23. Гамаюн В.П. Квазиграфический метод преобразования многоразрядного кода / В.П. Гамаюн // Комп’ютерні засоби, мережі та системи. Зб.наукових праць. – К.: Ін-т кібернетики ім.В.М.Глушкова НАНУ. – 2002. – №1. – С.53-57.
24. Зима В.М. Безопастность глобальных сетевых технологий / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. – СПб.: БХВ-Петербург. – 2002. – 320 с.
25. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов. – М.:Кудиц-Образ. – 2001. – 368 с.
26. Can Xiang Verifiable and Secure Outsourcing Schemes of Modular Exponentiations Using One Untrusted Cloud Server and Their Application / Can Xiang // IACR Cryptology ePrint Archive 2014: P.500. –510.
27. Monjur Ahmed. Cloud Computing and Security Issues in the Cloud / Monjur Ahmed, Mohammad Ashraf Hossain // International Journal of Network Security & Its Applications (IJNSA).- Vol.6, №1.- 2014.- pp.25-36.
28. McIlvor S. Fast Montgomery Modular Multiplication and RSA Cryptographic Processor Architectures / S. McIlvor, T. McLoone, D. McCanny // IEEE Transaction on Computers. – Vol.42. – №7. – 2003. – P.693-699.
29. Янтуш Д. А. Дешифрирование азрокосмических снимков / Д. А. Янтуш. – М. : Недра, 1991. – 240 с.
30. Трифонов Т. А. Геоинформационные системы и дистанционное зондирование в экологических исследованиях / Т. А. Трифонов. − М. : Академический проект, 2005. − 252 с.

31. PengyaoWang. Rapid processing of remote sensing images based on cloud computing /PengyaoWang,JianqinWang, YingChen, Guangyuan Ni // Future Generation Computer Systems. – Vol.29.- № 8.-2013.- pp.1963-1968.
32. Markovskyi O.P. Secure Modular Exponentiation in Cloud Systems/ O.P. Markovskyi, N. Bardis, S.J. Kirilenko // Proceeding of the Congress on Information Technology. Computationnal and Experimental Physics (CITCEP 2015), 18-20 December 2015, Krakow. Poland. – PP.266-269.
33. Menezer A.J. Handbook of Applied Cryptography / A.J. Menezer, P.C. Van Oorschot, S.A. Vanstone. – CRC-Press. – 1997. – 780 с.
34. Вельшенбах М. Криптография на С и С++ в действии / М. Вельшенбах. – М.: Триумф. – 2004. – 460 с.
35. Гамаюн В.П. Квазиграфический метод вычисления остатка по модулю / В.П. Гамаюн //Проблеми інформатизації та управління. Зб.наукових праць. – К.: НАУ. – 2005. – Вип.3(14). – С.43-48.
36. ДСТУ 3396.0=96. Захист інформації. Технічний захист інформації. Основні положення. – К.: Держстандарт України. – 1997. – 14 с.
37. ДСТУ 3396.2-96. Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Держстандарт України. – 1997. – 11 с.
38. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99.
39. Reliher-Masoleh L. Fast Normal Basis Multiplication Using General Purpuse Processors / L. Reliher-Masoleh, M.A. Hasan // Proceedings of 8-th International Wordshop "Selected Areas in cryptography", LNCS 2259, Springer. – 2001. – P. 230-239.
40. Yen S.M. The fast cascade exponentiation algorithm and its application to cryptography / S.M. Yen, C.S. Laih // Proc. International Conference Asiacrypt-92. – 2009. – P.10-20.

41. Yen S.M. A note on multi-exponention / S.M. Yen, C.S. Laih, A.K. Lenstra // IEEE Proceeding, Computer and Digital Techniques. – V.141. – № 5. – 2004. – P.122-131.
42. ГОСТ Р.34.10-94. Системы обработки информации. Защита криптографическая. Алгоритм формирования цифровой подписи.
43. Домашнев А.В. Программирование алгоритмов защиты информации / А.В. Домашнев, М.М. Грунтович, В.О. Попов, Д.И. Правиков, А.Ю. Щербаков, И.В. Прокофьев. – М.: Нолидж. – 2002. – 409 с.
44. Задірака В.К. Комп'ютерна криптологія: Підручник / В.К. Задірака, О.С. Олексюк. – К.: Вища школа. – 2002. – 504с.
45. Taylor R. A high-performance flexible architecture for cryptography / R. Taylor, S. Goldstein // Proceedings of 1-th International Workshop "Cryptographic Hardware and Embedded Systems", LNCS 1717, Springer. – 1999. – P. 231-245.
46. Tenca A.F. High-Radix Design of a Scalabre Modular Multiplier / A.F. Tenca, G. Todorov, C.K. Koc // Cryptographic Hardware and Embedded System-CHES'2001. LNCS-2162, Springer-Verlag. – 2001. – P.185-196.
47. Xiaofeng Chen New Algorithms for Secure Outsourcing of Modular Exponentiations / Xiaofeng Chen, Jin Li, Jianfeng Ma3, Qiang Tang, Wenjing Lou // ESORICS 2012, LNCS 7459. – 2012. – PP. 541–556.
48. Костенко Ю. В. Метод защищенного модулярного экспоненцирования на удаленных компьютерных системах / Ю. В. Костенко, А.П. Марковский, О.В. Русанова // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка. – К.: ТОО „ВЕК+". – № 64. – 2016. – С. 51-54.
49. Молдовян А.А. Введение в криптосистемы с открытым ключом / А.А. Молдовян, Н.А. Молдовян. – С-Пб.: БХВ-Петербург. – 2004. – 322 с.
50. Мухин В.Е., Волков Е.Г. Повышение скорости шифрования при реализации алгоритма RSA для механизмов защиты информации / В.Е. Мухин, Е.Г. Волков // Вісник Національного технічного університету України "КПІ".

Інформатика, управління та обчислювальна техніка. № 39. – К.:ВІПОЛ. – 2002. – С.50-56.

51. Коблиц Н. Введение в эллиптические кривые и модулярные формы / Н. Коблиц. – М.:Мир. – 1988. – 320 с.
52. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М.: Постмаркет. – 2001. – 323.
53. Стіренко С.Г. Забезпечення безперервного відтворення потокового відео в однорангових мережах з використанням erasures кодів. / С.Г. Стіренко, А.В. Габінет, Ю.В. Костенко // Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка: збірник наукових праць. – К.: "Век+". – 2015. – № 62. – С. 105–110.
54. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс. – М.: Изд.дом.”Вильямс”. – 2001. – 621 с.
55. Brickell E.F. Fast exponentiation with precomputation / E.F. Brickell, D.M. Gordon, K.S. McCurlay, D.B. Wilson // Advances in cryptography –Proceeding of EUROCRYPT’12, LNCS-2059, Springer-Verlag. – 2012. – P. 200-207.
56. Kawamura S. A fast modular exponentiation algorithm / S. Kawamura, K. Takabayashi, A. Shimbo // IEEE Transaction on Information Theory. – Vol. 94. – № 6. – 2015. – P.2136-2142.
57. Sutton M. A. Image Correlation for Shape, Motion and Deformation Measurements (Basic Concepts, Theory and Applications)./ Sutton M. A., Orteu J. J., Schreier H. // – New York: Springer, 2009. – 364 p.
58. Malgouyres F. A noise selection approach of image restoration, Applications in signal and image processing IX / F. Malgouyres // Vol 4478. – 2001. – P. 34-41.
59. Задірака В.К. Комп’ютерна арифметика багато розрядних чисел: Наукове видання / В.К. Задірака, О.С. Олексик. – К.:Вища школа. – 2003. – 264 с.
60. Таненбаум Э. Компьютерные сети. 6-е изд / Э. Таненбаум. – М.:Питер. – 2013. – 991 с.

61. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. НД ТЗІ 1.1-001-99.
62. Кнут Д. Искусство программирования для ЭВМ. Т.2. Получисленные алгоритмы / Д. Кнут. – М.:Мир. – 1977.- 843 с.
63. Макконелл Д.Х. Основы современных алгоритмов / Д.Х. Макконелл. – М.: Вильямс. – 2004. – 512 с.
64. Haches G. Montgomery multiplication with no final subtraction / G. Haches, J.J. Quisquater // Cryptographic Hardware and Embedded System- CHES'2013. LNCS-2465, Springer-Verlag. – 2013. – P.293-301.
65. Марковський О.П. Метод резервування та прискореного відновлення даних в системах їх віддаленого зберігання / О.П. Марковський, Д. Г. Іванов, М.М. Великий, М.В. Невдащенко // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка. – Київ: ВЕК+. – 2014. – № 60. – С.46-54.
66. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК. – 2002. – 655 с.
67. Широчин В.П. Вопросы проектирования средств защиты информации в компьютерных системах и сетях / В.П. Широчин, В.Е. Мухин, А.В. Кулик. – К.: ВЕК++. – 2000. – 111 с.
68. Koc C.K. Montgomery Reduction with Even Modulus / C.K. Koc // IEEE Proceedings: Computers and Digital Techniques. – Vol.141. – 2004. – № 5. – P.314-316.
69. Jutla C.S. On finding small solution of modular multivariate polynomial equations / C.S. Jutla // Advances in cryptography // Proceeding of EUROCRYPT'98, LNCS-658, Springer-Verlag. – 1998. – P. 221-235.
70. Фомичев В.М. Дискретная математика и криптология / В.М. Фомичев. – М.: Диалог-МИФИ. – 2003. – 379 с.

71. Bos J.N. Additional chain heuristics / J.N. Bos, M. Coster // Cryptographic Hardware and Embedded System- CHES'2014. LNCS-2116, Springer-Verlag. – 2014. – P.143-151.
72. Харин Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание. – 2003. – 382 с.
73. Ростовцев А.Г. Алгебраические основы криптографии / А.Г. Ростовцев. – СПб.: Мир и семья. – 2000. – 353 с.
74. Сэвидж Д.Э. Сложность вычислений / Д.Э. Сэвидж. – М.: Факториал. – 1998. – 368 с.
75. Хамахер К. Организация ЭВМ / К. Хамахер, З. Вранешич, С. Заки. – К.:Питер. – 2003. – 845 с.
76. Брэй Б. Микропроцессоры Intel. Архитектура, программирование и интерфейсы. Восьмое издание / Б. Брэй; пер. с анг. А.В.Жукова.- Санк-Петербург: БХВ-Петербург, 2015.-1328 с.
77. Laszlo Hars Long Modular multiplication for Cryptographic Applications / Laszlo Hars //Cryptographic Hardware and Embedded System- CHES'2004. LNCS-3156, Springer-Verlag. – 2004. – P.45-61.

Додаток А. Лістінги програми

```
import time
import random
import numpy as np
import math

length_matrix = int(input("Введите рзамер матрицы: ")) #ввод размера матрицы
number_of_sum = int(input("Введите нечетную апертуру: ")) # ввод апертуры
(Только нечетное число больше 1)
number_from = -(math.floor(number_of_sum/2)) # получение числа для
фыльтрации массивов
number_to = (-number_from)+1 # получение второго числа для фыльтрации
массивов
middle_divisor = math.floor(math.sqrt(length_matrix)) #Получение среднего
делителя для таблицы
if middle_divisor % 2 ==1: #проверка на четность
    middle_divisor = middle_divisor-1 #уменьшение на 1 в случае нечетности

def create_a_matrix(): # функция которая создаёт матрицу A
    final_matrix = []
    for row in range(0,length_matrix): # цикл по рядам матрицы
        row_matrix = []
        for column in range(0,length_matrix): # цикл по столбцам матрицы
            row_matrix.append(random.randint(0,255)) # добавление случайного числа
от 0 до 255
        final_matrix.append(row_matrix)
    return final_matrix

def create_b_matrix(a_matrix): # создание матрицы B
    final_matrix = []
```

```
    for row in range (len(a_matrix)): # цикл по рядам матрицы
        row_matrix = []
        for column in range(len(a_matrix[row])): # цикл по столбцам матрицы
            average_num = 0  # итоговое число
            k = 0 # счетчик
            f = True
            for i in range(number_from,number_to): # цикл по рядам апертуры
                for j in range(number_from,number_to): # цикл по столбцам апертуры
                    index_column = column+i
                    index_row = row+j
                    if index_column<0 or index_column>=length_matrix or index_row<0 or
index_row>=length_matrix: # проверка на индекс
                        f = False # смена флага
                    else:
                        average_num += a_matrix[index_row][index_column] # добавление
к итоговому числу
                        k+=1
            if k!=0 and f==True: row_matrix.append(float(format(average_num/k))) #
проверка флага
            elif f==False: row_matrix.append(0)
        final_matrix.append(row_matrix)
    return final_matrix

def createt1Array():
    return random.sample(list(range(0,length_matrix)),length_matrix) # создание
таблицы T1 с случайномы числами по длине матрицы

def create_t2_array(t1_array):  # создание таблицы T1 по таблице T2
    t2_array = [0] * len(t1_array) # создание пустого массива
```

```
    for index in range(len(t1_array)): # обход T1
        element = t1_array[index]  # получение єлемента T1
        t2_array[element] = index # добавление елемента T2
    return t2_array


def create_reverse_matrix(a_matrix,t_array): # создание матрицы с перестановкой столбцов
    size_of_matrix = len(a_matrix)
    c_matrix = [[0 for x in range(size_of_matrix)] for y in range(size_of_matrix)] # создание пустой матрицы
    for i in range(len(t_array)): # обход таблицы
        matrix_element_by_index = t_array[i]
        array_to_put = get_matrix_column(a_matrix,i) #получении нужного столбца из первой матрицы
        put_in_column(c_matrix,array_to_put,matrix_element_by_index) # вставка столбца в другую матрицу
    return c_matrix


def put_in_column(matrix, array_to_put,column_index): # вставка столбца в матрицу
    k=0 # счетчик
    for element in array_to_put: # обход столбца
        matrix[k][column_index] = element # замена элементов в матрице
        k+=1
 def get_matrix_column(matrix,column_index): #получении нужного столбца из матрицы
    column_array = [] #создание пустого массива
```

```
    k = 0
    for length in range(len(matrix)): #обход матрицы
        column_array.append(matrix[k][column_index]) #добавления элементов
стобца в массив
        k+=1
    return column_array

def create_d_matrix(c_matrix): #создание матрицы D
    final_matrix = [] #создание пустой матрицы
    for row in range(len(c_matrix)): #обход ряда
        row_matrix = []
        for column in range(len(c_matrix[row])): #обход столбца
            d_number = 0 #итоговое число
            k = 0 #счетчик
            for i in range(number_from,number_to): #обход по столбцу
                index_row = row + i
                if index_row<0 or row>=(length_matrix+number_from): #проверка
индекса
                    break
                d_number+=c_matrix[index_row][column] #суммирование элементов
            row_matrix.append(float(format(d_number/(number_of_sum**2)))))
#добавление подходяещего элемента в массив
        final_matrix.append(row_matrix) #добавление массива в матрицу
    return final_matrix

def create_f_matrix(e_matrix): #создание матрицы F
    final_matrix = [] #создание пустой матрицы
    for row in range(len(e_matrix)):  #обход ряда
        row_matrix = []
```

```
        for column in range(len(e_matrix[row])):  #обход столбца
            d_number = 0  #итоговое число
            for i in range(number_from,number_to): #обход поряду
                index_column = column + i
                if index_column<0 or column>=(length_matrix+number_from): #проверка
индекса
                    break
                d_number+=e_matrix[row][index_column] #суммирование элементов
            row_matrix.append(round(d_number))  #добавление подходяещего
элемента в массив
        final_matrix.append(row_matrix) #добавление массива в матрицу
    return final_matrix

make_table = lambda list, slice: [list[i:i+slice] for i in range(0, len(list), slice)]
#Проебразование одномерного массива в двумерный

def main():
    start_time1 = time.time() #получение  времени до выполнение функции
    a_matrix = create_a_matrix()
    print("1: ",time.time()-start_time1) #получение и вывод времени выполнения
функции
    start_time2 = time.time()
    b_matrix = create_b_matrix(a_matrix)
    print("2: ",time.time()-start_time2)
    t1_array = createt1Array()
    start_time3 = time.time()
    c_matrix = create_reverse_matrix(a_matrix,t1_array)
    print("3: ",time.time()-start_time3)
    start_time4 = time.time()
```

```
    d_matrix = create_d_matrix(c_matrix)
    print("4: ",time.time()-start_time4)
    t2_array = create_t2_array(t1_array)
    start_time5 = time.time()
    e_matrix = create_reverse_matrix(d_matrix,t2_array)
    print("5: ",time.time()-start_time5)
    start_time6 = time.time()
    f_matrix = create_f_matrix(e_matrix)
    print("6: ",time.time()-start_time6)
    np.savetxt("A_matrix.csv", a_matrix, delimiter="|",fmt='%  4d')
    np.savetxt("B_matrix.csv", b_matrix, delimiter="|",fmt='%    1.2f')
    np.savetxt("T1_table.csv", make_table(t1_array,middle_divisor),fmt='%  5d')
    np.savetxt("T2_table.csv", make_table(t2_array,middle_divisor),fmt='%  5d')
    np.savetxt("C_matrix.csv", c_matrix, delimiter="|",fmt='%  4d')
    np.savetxt("D_matrix.csv", d_matrix, delimiter="|",fmt='%  1.2f')
    np.savetxt("E_matrix.csv", e_matrix, delimiter="|",fmt='%  1.2f')
    np.savetxt("F_matrix.csv", f_matrix, delimiter="|",fmt='% 4d')
if __name__ == "__main__":
    main()
```